МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Л.М. Олещенко

ОРГАНІЗАЦІЯ КОМП'ЮТЕРНИХ МЕРЕЖ

КОНСПЕКТ ЛЕКЦІЙ

*Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для студентів,
які навчаються за спеціальністю 121 «Інженерія програмного забезпечення», спеціалізацією «Програмне забезпечення комп'ютерних та інформаційно-пошукових систем»*

Київ
КПІ ім. Ігоря Сікорського
2018

Рецензенти: *Бідюк, П. І.*, д-р техн. наук, проф.
Стеценко, І. В., д-р техн. наук, проф.

Відповідальний редактор *Заболотня, Т. М.*, канд. техн. наук, доц.

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського
(протокол № 7 від 29.03.2018 р.)
за поданням Вченої ради факультету прикладної математики
(протокол № 8 від 26.03.2018 р.)

Електронне мережне навчальне видання

Олещенко Любов Михайлівна, канд. техн. наук

ОРГАНІЗАЦІЯ КОМП'ЮТЕРНИХ МЕРЕЖ

КОНСПЕКТ ЛЕКЦІЙ

Організація комп'ютерних мереж: конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спеціальності 121 «Інженерія програмного забезпечення», спеціалізації «Програмне забезпечення комп'ютерних та інформаційно-пошукових систем» / Л.М. Олещенко ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 3,32 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 225 с.

Навчальний посібник розроблено для вивчення студентами теоретичних відомостей з проектування та налаштування комп'ютерних мереж. Навчальне видання призначене для студентів, які навчаються за спеціальністю 121 Інженерія програмного забезпечення, спеціалізацією «Програмне забезпечення комп'ютерних та інформаційно-пошукових систем» факультету прикладної математики КПІ ім. Ігоря Сікорського.

ЗМІСТ

Вступ

Створення і об’єднання надійних мереж передачі даних є платформою, на якій відбуваються сучасні комунікації. Досягнення в мережевих технологіях є одними з найважливіших у світі. Завдяки мережам передачі даних межі країн, відстані і фізичні обмеження складають все менше перешкод. Глобальна мережа впливає на спосіб соціальної, комерційної, політичної і особистої взаємодії у суспільстві.

Учбова дисципліна «Організація комп’ютерних мереж» є нормативною і входить до складу циклу професійно-орієнтованих дисциплін навчального плану підготовки бакалаврів, що навчаються за спеціальністю 121 «Інженерія програмного забезпечення» спеціалізації «Програмне забезпечення інформаційно- пошукових систем».

Предметом дисципліни є теоретичні і практичні основи в області організації комп’ютерних мереж. Мета дисципліни – забезпечити знання теоретичних і практичних основ з організації та функціонування комп’ютерних мереж.

Метою конспекту лекцій є отримання необхідного рівня знань з теорії мережевих протоколів та засобів комунікацій, основних технологій передавання даних у локальних та глобальних мережах.

У даному конспекті лекцій студенти ознайомляться з правилами проектування локальних мереж, стандартами передачі даних, алгоритмами комутації та маршрутизації, методами захисту мереж від несанкціонованого доступу.

Курс лекцій з дисципліни «Організація комп’ютерних мереж» розрахований на 36 академічних годин аудиторних занять. Конспект лекцій складається з 18 розділів, кожен з яких присвячений одній лекції з дисципліни «Організація комп’ютерних мереж». У кожному розділі надаються теоретичні відомості з певної теми, контрольні питання для самоперевірки та список рекомендованої літератури.

Лекція 1. Тема: «Типи комп'ютерних мереж. Компоненти мережі. Мережеві протоколи і стандарти. Моделі OSI і TCP / IP»

План лекції

1.1. Типи комп'ютерних мереж.
1.2. Технології доступу в Інтернет.
1.3. Вимоги до мережі. Компоненти мережі.
1.4. Представлення мережі. Фізична та логічна топології мереж.
1.5. Хмарні обчислення. Центри обробки даних.
1.6. Мережеві протоколи і галузеві стандарти.
1.7. Моделі OSI і TCP/IP.
1.8. Порівняння моделей OSI і TCP/IP.

1.1. Типи комп'ютерних мереж

Існують мережі різного розміру, від простих мереж, що складаються з двох комп'ютерів, до систем, що сполучають мільйони пристроїв.

Мережі часто використовуються людьми, які працюють з будинку або віддаленого офісу і яким потрібне підключення до корпоративної мережі або інших централізованих ресурсів. Підприємці використовують мережі малого і домашнього офісу в рекламних цілях та для продажу продукції, замовлення витратних матеріалів і взаємодії з клієнтами.

На підприємствах і у великих організаціях мережі можуть використовуватися в ще більшому масштабі, щоб дозволити співробітникам збирати, зберігати і отримувати інформацію на мережевих серверах. Мережі дозволяють налагодити швидкий зв'язок у вигляді електронної пошти, обміну миттєвими повідомленнями, а також функцій спільної роботи між співробітниками.

Усі комп'ютери, що підключені до мережі та безпосередньо беруть участь в обміні даними, класифікуються як **вузли** або **кінцеві пристрої**. Вузли можуть приймати і відправляти повідомлення по мережі. У сучасних мережах комп'ютерні вузли можуть працювати як клієнт, сервер або як і те, і інше. Роль комп'ютера в мережі визначається програмним забезпеченням (ПЗ).

Сервери – це вузли зі встановленим ПЗ, що дозволяє надавати іншим мережевим вузлам інформацію (наприклад, доступ до електронної пошти або веб-сторінок). Для роботи кожної служби потрібне окреме серверне ПЗ. Наприклад, для роботи веб-служб в мережі на вузлі повинно бути встановлене ПЗ веб-сервера.

Клієнти – це комп'ютерні вузли зі встановленим ПЗ, що дозволяє просити і відображати отриману з сервера інформацію. Прикладом клієнтського ПЗ є веб-браузер, наприклад, Internet Explorer.

Комп'ютер з серверним ПЗ може одночасно обслуговувати один або декілька клієнтів. Крім того, на одному комп'ютері можна паралельно встановити декілька типів серверного ПЗ. У домашніх або невеликих корпоративних мережах одному комп'ютеру доводиться виступати файловим сервером, веб-сервером і сервером електронної пошти.

Крім того, на одному комп'ютері можна запускати декілька типів клієнтського ПЗ. Необхідно встановити клієнтське ПЗ для кожного сервісу. За наявності декількох клієнтів вузол зможе одночасно підключатися до декількох серверів щоб перевіряти електронну пошту, переглядати веб-сторінки, обмінюватися миттєвими повідомленнями, слухати інтернет-радіо тощо.

Зазвичай клієнтське і серверне ПЗ запускається на різних комп'ютерах, але таку функцію може виконувати і один комп'ютер. У невеликих корпоративних і домашніх мережах багато комп'ютерів працюють і як сервери, і як клієнти. Такі мережі називаються **одноранговими**.

Проста однорангова мережа складається з двох комп'ютерів, безпосередньо підключених один до одного за допомогою дротяного або безпровідного зв'язку.

Крім того, можна з'єднати декілька ПК і створити більшу однорангову мережу, але для цього знадобиться мережевий пристрій, наприклад, комутатор.

Основний недолік однорангового середовища полягає в тому, що при одночасній роботі клієнтом і сервером вузол працює повільніше.

Мережеві інфраструктури можуть значною мірою відрізнятися за критеріями:

- розмір обслуговуваної території;
- кількість підключених користувачів;
- число і типи доступних сервісів.

Локальна мережа (LAN, Local Area Network**)** – мережева інфраструктура, яка забезпечує доступ користувачам і крайовим пристроям в невеликій географічній області.

Основні компоненти LAN :

- локальні мережі зв'язують кінцеві пристрої в обмеженій області, наприклад, в будинку, школі, офісній будівлі або комплексі будівель;
- локальна мережа зазвичай адмініструється однією організацією або приватною особою, адміністратор управляє політикою безпеки і контролем доступу на мережевому рівні;
- локальні мережі надають високошвидкісний доступ до внутрішніх крайових і проміжних пристроїв.

Глобальна мережа (WAN, Wide Area Network**)** – мережева інфраструктура, яка охоплює велику географічну область. Управління глобальними мережами зазвичай здійснюється операторами зв'язку (**SP**, Service Provider) або Інтернет-провайдерами (**ISP**, Internet Service Provider).

Основні компоненти WAN:

- WAN зв'язують локальні мережі у великих географічних областях, таких як міста, регіони, країни або континенти;
- управління глобальними мережами зазвичай здійснюється різними операторами зв'язку;
- глобальні мережі зазвичай забезпечують більше низькошвидкісні з'єднання між локальними мережами.

Муніципальна мережа (MAN, Metropolitan area network**)** – мережева інфраструктура, яка охоплює фізичну область більшу, ніж LAN, але меншу глобальної мережі (наприклад, місто). Як правило, управління MAN здійснюється однією організацією, наприклад, великим підприємством.

Безпровідні локальні мережі (WLAN, Wireless Local Area Network**)** аналогічні мережам LAN, але сполучають користувачів і кінцеві пристрої невеликої географічної області за допомогою безпровідного зв'язку.

Мережа зберігання даних (SAN, Storage Area Network**)** – мережева інфраструктура, розроблена для підтримки файлових серверів і забезпечення зберігання даних, їх отримання з сховища і реплікації. Вона включає високопродуктивні сервери, дискові масиви і технологію з'єднань Fibre Channel.

Інтернет – найбільша мережа у всьому світі. Поняття «Інтернет» означає «мережу усіх мереж». Інтернет є об'єднанням підключених один до одного приватних і загальнодоступних мереж. Корпоративні мережі, мережі малого бізнесу і навіть домашні мережі зазвичай забезпечують загальний доступ до Інтернету. Це загальносвітовий конгломерат взаємозв'язаних мереж, що взаємодіють один з одним для обміну інформацією на основі загальних стандартів. Користувачі, що підключилися до Інтернету по телефонній лінії, оптоволоконному кабелю, безпровідному зв'язку або через супутник, можуть обмінюватися даними в найрізноманітніших формах.

Термін **«Інтранет» (внутрішні мережі)** використовується для позначення локальних і глобальних мереж, які належать організації і доступні лише її членам, співробітникам та іншим авторизованим особам. Внутрішні мережі є об'єднанням мереж, яке зазвичай доступні тільки у рамках організації. Організації можуть публікувати у внутрішніх мережах веб-

сторінки про внутрішні заходи, правила по техніці безпеки, повідомлення співробітників і корпоративні телефонні довідники. Внутрішні мережі можуть бути доступні для співробітників за межами організації з використанням безпечних підключень до внутрішньої мережі.

Організація може використовувати **Екстранет (зовнішні мережі)** для забезпечення захищеного і безпечного доступу співробітників, які працюють в різних організаціях і яким потрібні ці компанії. Приклади мережі Екстранет:

- лікарня, де використовується система запису до лікарів, які мають можливість призначати дату прийому пацієнтів;
- місцеве управління освіти, що надає школам свого району дані про розмір бюджету і кадри тощо.

1.2. Технології доступу в Інтернет

Існує багато різних способів підключення користувачів і організацій до Інтернету.

Домашні користувачі, дистанційні працівники (віддалені співробітники компаній) і малі офіси, як правило, для доступу в Інтернет потребують підключення до Інтернет-провайдера (ISP). Варіанти підключення істотно міняються залежно від Інтернет-провайдера і географічного місця розташування. Проте популярні варіанти включають широкосмугову кабельну мережу, широкосмугову цифрову абонентську лінію (**DSL**, Digital Subscriber Line), глобальні мережі (WAN) і сервіси мобільного доступу. Організаціям зазвичай потрібний доступ до інших корпоративних вузлів та Інтернету. Для бізнес-сервісів, у тому числі відеоконференцій, IP -телефонів, центрів обробки і зберігання даних потрібні швидкі з'єднання.

Розглянемо стандартні варіанти підключення для користувачів малих і домашніх офісів.

- **Кабельне підключення:** сигнал даних Інтернету передається по тому ж коаксіальному кабелю, який використовується для передачі сигналів кабельного телебачення. Цей спосіб забезпечує підключення до Інтернету з високою пропускною спроможністю і постійним доступом до мережі. Спеціальний кабельний модем відділяє сигнали Інтернет від інших, при цьому Ethernet -порт використовується для підключення комп'ютера або мережі LAN.
- **DSL:** цей спосіб забезпечує підключення до Інтернету з високою пропускною спроможністю і постійним доступом до мережі. При цьому способі підключення використовується високошвидкісний модем, що розділяє цифровий сигнал від телефонного, і Ethernet - з'єднання для підключення комп'ютера або мережі LAN. DSL працює по телефонній лінії, розділеній на три канали. Один канал використовується для телефонних викликів голосового зв'язку. Цей канал дозволяє приймати телефонні виклики без відключення Інтернету. Другий канал – швидший канал завантаження для отримання інформації з Інтернету. Третій канал використовується для відправки інформації. Цей канал, як правило, повільніший, ніж канал завантаження. Якість і оперативність DSL - з'єднання залежить в основному від якості телефонної лінії і відстані від центральної телефонної станції. Чим далі користувач знаходиться від центральної телефонної станції, тим повільніше з'єднання.
- **Стільниковий зв'язок:** для доступі в Інтернет використовується мобільна телефонна мережа. У будь-якій точці, де доступний стільниковий сигнал, можна дістати стільниковий доступ в Інтернет. Продуктивність буде обмежена можливостями телефону і базової станції, до якої він підключений. Доступність стільникового доступу в Інтернет – велика перевага в тих районах, в яких інакше не було б підключення до Інтернету, або для тих, хто постійно знаходиться в дорозі.
- **Супутниковий зв'язок:** є зручним варіантом для будинку або офісу, що не має доступу до цифрової абонентської лінії (DSL) або кабелю. Супутникові антени вимагають безперешкодної прямої видимості супутника і, отже, їх не бажано використовувати в

лісистих місцевостях або в місцях з наземними перешкодами. Швидкість відрізнятиметься залежно від умов договору, але вона, як правило, є оптимальною. Вартість устаткування і установки може бути високою з помірною щомісячною платою.

- **Телефонний комутований доступ:** недорогий спосіб, в якому використовується телефонна лінія і модем. Для підключення до Інтернет-провайдера користувач викликає телефонний номер доступу провайдера. Низька пропускна спроможність, що забезпечується підключенням по комутованій лінії, зазвичай недостатня для передачі даних. Модемне з'єднання має сенс розглядати тільки за відсутності варіантів швидшого з'єднання.

Багато будинків і невеликі офіси все частіше підключаються безпосередньо оптоволоконними кабелями. Це дозволяє Інтернет-провайдерам надавати вищі швидкості і пропускні здібності, а також підтримувати більше сервісів, наприклад Інтернет, телефон і телебачення.

- **Стандарт Metro Ethernet** зазвичай доступний від оператора до абонентського устаткування по виділених мідних або оптоволоконних лініях із швидкістю підключення (пропускною спроможністю) від 10 Мбіт/с до 10 Гбіт/с. Проте, Ethernet по мідному кабелю обмежений відстанню.

Постачальник безпровідних інтернет-послуг (WISP, wireless Internet service provider) підключає абонентів до точок доступу за допомогою безпровідних технологій. Частіше усього WISP зустрічаються в сільській місцевості, де цифрові абонентські лінії (DSL) або кабельні мережі недоступні.

Не дивлячись на те, що для антени може бути встановлена окрема вишка, зазвичай вона встановлюється на існуючих конструкціях, таких як водонапірна вежа або радіовежа. Невелика антена на даху у абонента знаходиться в зоні прийому передавача WISP. Блок доступу підключається до дротяної мережі в домашній мережі. З точки зору домашнього користувача, налаштування не відрізняється від DSL - ліній або кабельних ліній зв'язку. Головна відмінність полягає в тому, що підключення від будинку до оператора зв'язку є безпровідним замість фізичного кабелю.

1.3. Вимоги до мережі. Компоненти мережі

Мережі повинні підтримувати широкий набір додатків і сервісів, а також багато типів кабелів і пристроїв, з яких складається фізична інфраструктура. Термін «мережева архітектура» в цьому контексті відноситься до технологій, які підтримують інфраструктуру, а також до запрограмованих сервісів і правил, або протоколів, які переміщають повідомлення в мережі.

Мережі повинні відповідати чотирьом основним вимогам:

- стійкість до збоїв;
- масштабованість (можливість розширення мережі);
- якість обслуговування;
- безпека.

Відмовостійка мережа обмежує вплив збоїв так, щоб вони торкнулися найменшої кількості пристроїв. Вона також побудована так, щоб швидко відновлюватися при виникненні відмови. Ці мережі враховують наявність декількох шляхів між джерелом і місцем призначення повідомлення. Якщо один шлях недоступний, повідомлення можна негайно відправити по іншій лінії зв'язку. Наявність декількох шляхів до місця призначення називається **резервуванням.**

Щоб зрозуміти потребу в резервуванні, розглянемо роботу ранніх телефонних систем. Якщо користувач здійснював виклик за допомогою телефонного апарату, виклик спочатку проходив процес встановлення з'єднання. Цей процес встановлював місця комутації між абонентом (джерело) і телефонним апаратом (одержувач), що викликався. На час виклику створювався тимчасовий канал або лінія. Якщо доступ до будь-якого з ресурсів або пристроїв в каналі отримати не вдавалося, виклик скидався. Для повторного підключення

необхідно було зробити новий виклик з новим каналом. Цей процес встановлення з'єднання називається **процесом комутації каналів.**

Багато мереж з комутацією каналів надають пріоритет існуючим каналам підключення за рахунок нових запитів. Після того, як канал створений, і навіть якщо між абонентами на двох кінцях каналу не відбувається повідомлення, канал залишається підключеним, а ресурси зайнятими до тих пір, поки виклик не буде завершений однією із сторін. Через те, що число каналів обмежене максимально можливим, можна отримати повідомлення про те, що усі канали зайняті і виклик не може бути виконаний. Вартість для створення альтернативних маршрутів з достатньою пропускною спроможністю для підтримки великого числа одночасних каналів і технології, необхідні для динамічного відтворення розірваних каналів у разі збою, пояснюють, чому ця канальна технологія не стала оптимальною для Інтернету.

У пошуках відмовостійкої моделі мережі первинні розробники Інтернету звернули увагу на **мережі з комутацією пакетів**, де одне повідомлення можна розділити на декілька окремих блоків повідомлення, причому кожен з блоків повідомлення містить інформацію про адресацію, що ідентифікує початковий пункт і пункт призначення. Блоки сполучення з вбудованою інформацією називаються **пакетами**, які можуть бути відправлені через мережу по різних шляхах, а потім на місці отримання зібрані в початкове повідомлення.

Самі пристрої в мережі, як правило, не обізнані про вміст окремих пакетів. Їм видно лише адреси джерела і кінцевого місця призначення. Ці адреси називають **IP - адресами,** представленими в точково-десятковому форматі, наприклад: 10.10.10.10. Кожен пакет вирушає незалежно з одного місця розташування в інше. У кожному проміжному пункті приймається рішення про **маршрутизацію**, тобто про вибір шляху, який слід використовувати для передачі пакетів до місця призначення.

Якщо шлях, що раніше використався, більше недоступний, функція маршрутизації може динамічно вибрати наступний найбільш відповідний доступний шлях. Оскільки повідомлення вирушають по частинах, а не як одне ціле повідомлення, деякі з пакетів можуть бути втрачені, в цьому випадку їх можна повторно відправити до місця призначення по інших маршрутах. У багатьох випадках пристрій призначення не обізнаний про те, чи мали місце відмови або зміни маршруту. Необхідності єдиного зарезервованого шляху від початку до кінця не існує в мережі з комутацією пакетів. Будь-які частини повідомлення можна відправляти через мережу по будь-якому доступному шляху. Крім того, пакети з частинами повідомлень з різних джерел можуть передаватися по мережі в один і той же час. За рахунок реалізації способу динамічного використання надмірних маршрутів без втручання користувача Інтернет став відмовостійким видом зв'язку.

Не дивлячись на те, що мережі з комутацією пакетів без встановлення з'єднання є основою інфраструктури сучасного Інтернету, орієнтовані на підключення системи, такі як комутована телефонна мережа, мають свої переваги. Оскільки ресурси в різних місцях комутації орієнтовані на надання кінцевого числа каналів, можна гарантувати якість і узгодженість повідомлень в мережі з установкою з'єднань. Іншою перевагою є те, що постачальник послуг може виставити користувачеві мережі рахунок за час активного з'єднання. Можливість виставляти користувачам рахунок за активні з'єднання через мережу – фундаментальна основа галузі телекомунікаційних послуг.

Якість обслуговування (**QoS**, quality of service) сьогодні є однією з постійно зростаючих вимог до мережі. Нові додатки, доступні користувачам по Інтернету, наприклад, за допомогою передачі голосового зв'язку та відео в режимі реального часу, створюють вищі вимоги до якості сервісів.

Мережі повинні забезпечувати передбачуваний, вимірний, а іноді і гарантований рівень сервісів. Архітектура мережі з комутацією пакетів не гарантує, що усі пакети, з яких складається повідомлення, будуть доставлені в правильному порядку та що вони будуть доставлені без втрат. Крім того, мережам потрібні механізми управління переповненим мережевим трафіком. Пропускна спроможність мережі є мірою здатності мережі передавати дані. Пропускна спроможність мережі вимірюється у кількості біт, що передаються за одну

секунду, або в бітах в секунду (біт/с). При паралельних спробах передачі повідомлень по усій мережі попит на пропускну спроможність може перевищувати доступну величину, що створює перевантаження мережі. Мережа просто отримує більше біт, ніж смуга пропускання каналу зв'язку дозволяє доставити.

В більшості випадків, коли число пакетів перевищує можливості доставки по мережі, пристрої поміщають пакети в черги в пам'яті до тих пір, поки не будуть доступні ресурси передачі. Черги пакетів викликають затримки, оскільки нові пакети не можуть бути відправлені до тих пір, поки не відправлені попередні. Якщо кількість пакетів, поставлених в чергу, продовжує збільшуватися, черги в пам'яті заповнюються, і пакети відкидаються.

Мережева інфраструктура, сервіси і дані, що містяться в пристроях, підключених до мереж, представляють важливу складову особистих і ділових активів. Збиток для цілісності цих ресурсів може привести до серйозних наслідків, таким як:

- збої в роботі мережі, які не дозволяють здійснювати комунікації і транзакції, що приводить до упущення ділових можливостей;
- розкрадання і використання конкурентами інтелектуальної власності компанії (ідеї, патенти або дослідження);
- порушення конфіденційності і публікація без згоди користувача його особистої або приватної інформації;
- невірне використання і втрати особистих або корпоративних фінансових коштів;
- втрата даних, які вимагають істотних трудовитрат на відновлення або є незамінними.

Існує два типи проблем безпеки мережі: безпека мережевої інфраструктури та безпека інформації.

Забезпечення безпеки інфраструктури мережі включає забезпечення фізичної безпеки усіх пристроїв, які потрібні для мережевих підключень, і запобігання несанкціонованому проникненню в управляюче ПЗ.

Безпека інформації означає захист даних, що містяться в пакетах, що передаються по мережі, а також інформації, що зберігається на підключених до мережі пристроях.

Щоб досягти цілей безпеки мережі, існує три наступні основні вимоги.

1. **Забезпечення конфіденційності даних** означає, що тільки вказані і авторизовані одержувачі (співробітники, процеси або пристрої) можуть дістати доступ до даних. Це досягається за рахунок надійної системи аутентифікації користувачів, реалізації вимог до паролів, які складно підібрати, а також вимог частої зміни паролів. Шифрування даних, які міг би прочитати тільки вказаний одержувач, також входить в конфіденційність.
2. **Підтримка цілісності** означає забезпечення упевненості в тому, що інформація не була змінена в процесі передачі від початкового пункту до місця призначення. Цілісність даних може бути порушена, коли інформація пошкоджена, навмисно або ненавмисно. Цілісність даних забезпечується шляхом перевірки відправника і використання механізмів перевірки того, що пакет не змінився при передачі.
3. **Забезпечення доступності** означає засоби забезпечення своєчасного і надійного доступу до даних для авторизованих користувачів. Пристрої з мережевими екранами, а також з настільним і серверним антивірусним ПЗ дозволяють підвищити надійність і стійкість системи, виявляючи атаки і захищаючись від них. Створення повністю резервованих мережевих інфраструктур з малим числом точок відмови може зменшити наслідки цих погроз.

Інфраструктура мережі включає три **категорії компонентів мережі** (рис. 1.1):

- пристрої (Devices);
- середовище (Media);
- сервіси.

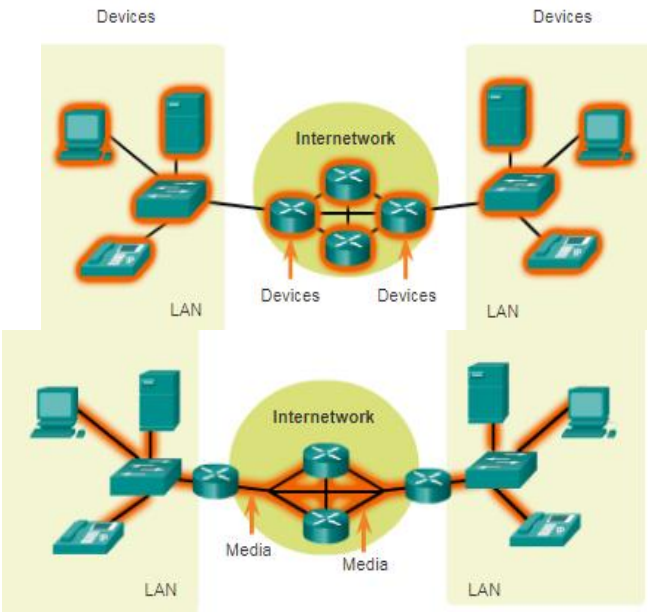


Рис.1.1. Пристрої та середовище передавання даних по мережі [1]

Пристрої і середовище – це фізичні елементи або устаткування мережі. Устаткування часто є видимою частиною мережевої платформи (ноутбук, ПК, комутатор, маршрутизатор, точка безпровідного доступу або кабелі тощо). Деякі компоненти є невидимими. У разі безпровідних мереж повідомлення передаються за допомогою невидимого радіочастотного або інфрачервоного випромінювання.

Компоненти мережі використовуються для надання **сервісів** і **процесів**. Це комунікаційні програми або ПЗ, які працюють на мережевих пристроях. **Мережевий сервіс** надає дані у відповідь на запит. Сервіси включають безліч мережевих застосувань, які люди використовують щодня, наприклад, сервіси електронної пошти і сервіси веб-хостингу для веб-сайтів тощо. **Процеси** забезпечують направлення і переміщення повідомлення в мережі. Процеси менш очевидні для нас, але критично важливі для роботи мереж.

Мережеві пристрої, з якими користувачі знайомі краще всього, називаються **кінцевим пристроями або вузлами**. Ці пристрої утворюють інтерфейс між користувачами і комунікаційною мережею, яка надає зв'язок.

До кінцевих (крайових) пристроїв відносяться:

- комп'ютери (робочі станції, ноутбуки, файлові сервери, веб-сервери);
- мережеві принтери;
- VoIP –телефони;
- термінальне устаткування TelePresence;
- камери відеоспостереження;
- пересувні кишенькові пристрої – смартфони, планшетні ПК, безпровідні зчитувачі дебетових/кредитних карт, сканери штрих-кодів тощо (рис. 1.2).

Рис. 1.2. Кінцеві (крайові) пристрої (end devices) [1]

Вузол є або джерелом, або адресатом повідомлення, що передається по мережі. Щоб відрізняти один вузол від інших, кожному вузлу в мережі призначена адреса. Коли вузол ініціює взаємодію, він використовує адресу вузла призначення, щоб визначити, куди має бути спрямоване повідомлення.

Проміжні пристрої служать для з'єднання крайових пристроїв. Ці пристрої забезпечують з'єднання, працюючи «за кулісами», здійснюючи передачу даних по мережі. Проміжні пристрої сполучають окремі вузли з мережею і можуть сполучати декілька окремих мереж для створення об'єднаної мережі.

До проміжних мережевих пристроїв відносяться (рис.1.3):

- пристрої доступу до мережі (комутатори і точки безпровідного доступу);
- пристрої мережевої взаємодії (маршрутизатори);
- пристрої безпеки (апаратні міжмережеві екрани).

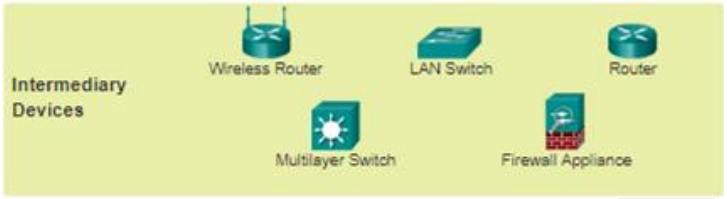


Рис.1.3. Проміжні мережеві пристрої (intermediary devices) [1]

До функцій проміжних пристроїв відноситься управління даними в процесі їх проходження через мережу. Ці пристрої використовують адресу вузла призначення у поєднанні з інформацією про зв'язки в мережі, щоб визначити шляхи для відправки повідомлень по мережі.

Процеси, запущені на проміжних мережевих пристроях, виконують наступні функції:

- регенерація і ретрансляція сигналів передачі даних;
- підтримка інформації про те, які шляхи передачі інформації є в мережі та між мережами;
- повідомлення інших пристроїв про помилки та збої зв'язку;
- напрям даних через альтернативний маршрут передачі при виході каналу з ладу;
- класифікація і передача повідомлень відповідно до пріоритетів якості обслуговування;
- дозвіл або заборона потоку даних на підставі налаштувань безпеки.

Для здійснення комунікації в мережі використовується **середовище передачі даних** (рис.1.4). Середовище надає канал, по якому повідомлення передається від джерела до адресата.

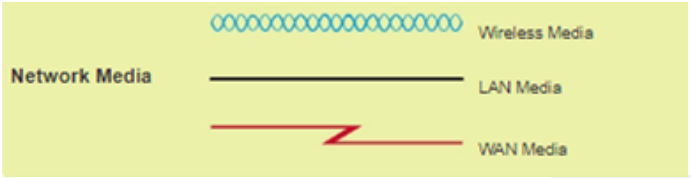


Рис.1.4. Середовище передачі даних по мережі (network media) [1]

У сучасних мережах використовуються три основні типи середовищ, що зв'язують пристрої і забезпечують шлях, по якому передаються дані:

- металеві дроти усередині кабелю;
- скляні або пластикові волокна (оптоволоконний кабель);
- радіопередача.

Кодування сигналу, яке потрібне для передачі, здійснюється по-різному залежно від типу середовища. У металевих дротах дані кодуються у вигляді електричних імпульсів, що відповідають певним шаблонам. Передача в оптоволоконних мережах відбувається у вигляді імпульсів світла, в діапазоні інфрачервоного випромінювання або видимого світла. При безпровідній передачі для опису різних значень бітів використовуються шаблони електромагнітного випромінювання.

1.4. Представлення мережі. Фізична та логічна топології мереж

При передачі складної інформації корисно використовувати візуальне представлення, що відображує усі пристрої і середовища у великій об'єднаній мережі. Схема забезпечує

наочний спосіб розуміння, яким чином пристрої у великій мережі пов'язані між собою. Така схема використовує символи для представлення різних пристроїв і каналів, з яких складається мережа. Цей тип зображення називається **схемою топології мережі.**

Як будь-яка інша мова, мова мережевих технологій використовує загальний набір знаків, щоб представляти різні кінцеві пристрої, мережеві пристрої і середовища. Здатність дізнаватися про логічні представлення фізичних мережевих компонентів має критичне значення для візуалізації організації і функціонування мережі. При обговоренні того, як кожен з пристроїв і середовище з'єднуються між собою, використовується спеціалізована термінологія.

- **Мережева інтерфейсна плата (NIC,** network interface controller/card) – адаптер локальної мережі (LAN), який забезпечує фізичне підключення до мережі на ПК або іншого пристрою. Середовище, що сполучає комп'ютер з мережевим пристроєм, під'єднується безпосередньо до мережевої плати.
- **Фізичний порт –** роз'єм або мережева розетка на мережевому пристрої, через який передавальне середовище підключене до ПК або іншого мережевого пристрою.
- **Інтерфейс –** спеціалізовані порти в мережевому пристрої, які підключаються до окремих мереж. Оскільки маршрутизатори використовуються для зв'язування мереж, порти відповідають мережевим інтерфейсам.

Схеми топологій забезпечують візуальну карту з'єднань в мережі. Існує два типи схем топології :

- **Схеми фізичної топології –** фізичне розташування проміжних пристроїв, налагоджених портів і прокладення кабелю (рис. 1.5).
- **Схеми логічної топології -** визначення пристроїв, портів і схеми IP –адресації.

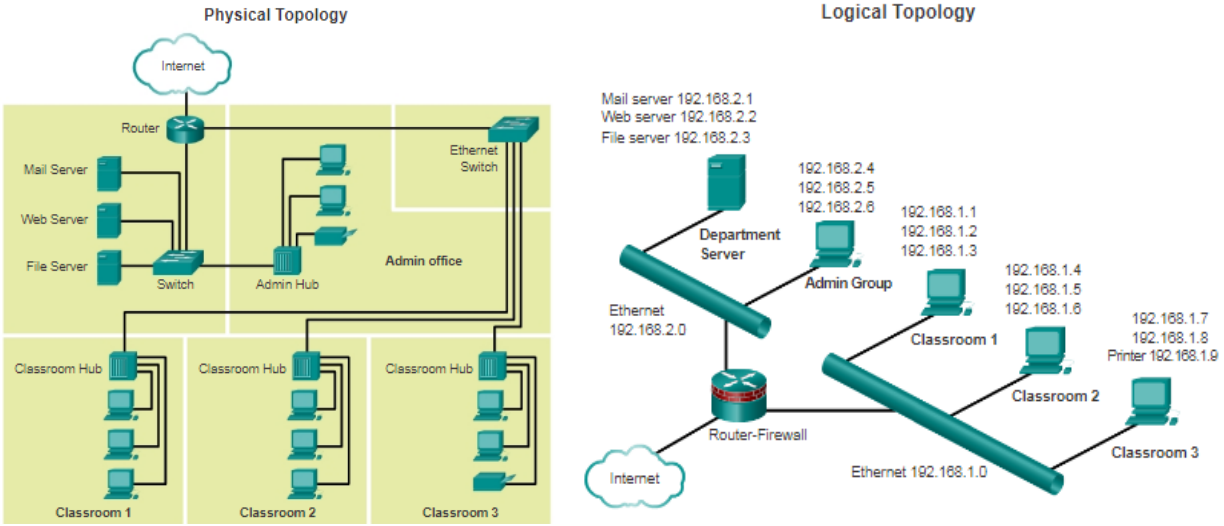


Рис. 1.5. Схема фізичної та логічної топології мережі [1]

1.5. Хмарні обчислення. Центри обробки даних

Хмарні обчислення – це використання обчислювальних ресурсів (устаткування і ПЗ), які надаються як послуга в мережі. Компанія використовує устаткування і ПЗ хмарних сервісів і вносить плату за послуги.

Локальним комп'ютерам більше не треба виконувати «важку роботу» для запуску мережевих додатків. Цим займається мережа комп'ютерів, з яких складається **хмара.** Знижуються вимоги користувача до устаткування і ПЗ. Комп'ютер користувача повинен взаємодіяти з хмарою за допомогою ПЗ, яке може бути браузером, а мережі хмарних сервісів виконують інші завдання.

Хмарні обчислення – це глобальна тенденція, яка змінює спосіб доступу і зберігання даних. Хмарні обчислення включають будь-який сервіс з підписки або з оплати за фактом використання в режимі реального часу через інтернет, дозволяють зберігати особисті файли

або цілий жорсткий диск на серверах в Інтернеті. Для підприємств хмара розширює ІТ-можливості, не вимагаючи при цьому великих капіталовкладень у створення нової інфраструктури, навчання нового персоналу або ліцензування нового ПЗ. Ці сервіси доступні за запитом і економічно доставляються на будь-який пристрій в будь-якій точці світу без зниження рівня безпеки і погіршення функціональності.

Термін «хмарні обчислення» означає обчислення, що виконуються в Інтернеті. Інтернет-банк, інтернет-магазини, скачування музики в Інтернеті є прикладами хмарних обчислень. Хмарні застосування зазвичай надаються користувачеві через веб-браузер. Користувачам не треба заздалегідь встановлювати на кінцеві пристрої ПЗ. Це дозволяє великому числу різних типів пристроїв підключатися до хмарних сервісів.

Хмарні обчислення пропонують наступні потенційні переваги.

- **Гнучкість організації:** користувачі можуть дістати доступ до інформації в будь-який час і в будь-якому місці за допомогою веб-браузеру.
- **Оперативність і швидке розгортання:** ІТ-відділ може сконцентруватися на інструментах з доставки, аналізу і спільного використання інформації з баз даних, файлів від інших користувачів.
- **Зниження витрат на інфраструктуру:** технологія переміщається з об'єкту до постачальника хмарних послуг, що знижує витрати на устаткування і застосування.
- **Переорієнтація ІТ-ресурсів:** засоби, заощаджені на устаткуванні і застосуваннях, можуть бути використані за іншим призначенням.
- **Створення нових бізнес-моделей**: додатки і ресурси легко доступні, тому компанії можуть швидко реагувати на потреби замовників. Це дозволяє їм проводити стратегію впровадження інновацій і досліджувати можливості проникнення на нові ринки.

Хмарні обчислення можливі завдяки центрам обробки даних.

Центр обробки даних (ЦОД) – це приміщення, в якому розташовуються комп'ютерні системи і відповідні компоненти, такі як:

- резервні сполучні кабелі для передачі даних;
- високошвидкісні віртуальні сервери (іноді їх називають серверними фермами або кластерами);
- резервні системи зберігання даних (зазвичай використовується технологія мережевої системи зберігання даних (**SAN**, Storage Area Network));
- джерела резервного електроживлення;
- елементи управління умовами робочого середовища (наприклад, системи кондиціонування повітря і пожежогасіння);
- пристрої забезпечення безпеки.

ЦОД може займати одне приміщення в будівлі, один або декілька поверхів або всю будівлю. Сучасні ЦОД використовуються для хмарних обчислень і віртуалізації, щоб зробити ефективною обробку великих масивів даних. Віртуалізація, або створення віртуальної версії чого-небудь, наприклад, апаратної платформи, операційної системи (ОС), пристрою зберігання мережевих ресурсів. Тоді як фізичний комп'ютер є фактичним фізичним пристроєм, віртуальна машина складається з набору файлів і програм, що працюють на фізичній системі. На відміну від багатозадачності, що полягає в тому, щоб запустити декілька програм на одній і тій же ОС, при використанні віртуалізації декілька різних ОС працюють паралельно на одному ЦП. Подібна схема значно зменшує витрати на адміністрування і накладні витрати.

ЦОД зазвичай дорого створювати і обслуговувати. З цієї причини тільки великі організації використовують спеціально створені ЦОД для розміщення корпоративних даних і сервісів для користувачів. Наприклад, велика медична установа може мати власний ЦОД, де історії хвороб пацієнтів ведуться в електронному вигляді. Невеликі організації, які не мають власного ЦОД, можуть понизити загальну вартість володіння за рахунок виділення сервера і сервісів зберігання даних у ЦОД більшої організації.

1.6. Мережеві протоколи і галузеві стандарти

Мережеві протоколи визначають загальний формат і набір правил для обміну повідомленнями між пристроями. Наприклад, протокол IP (Internet Protocol) визначає, яким чином пакет даних передається в межах мережі або у віддалену мережу. По протоколу IPv4 інформація передається в певному форматі так, щоб одержувач міг правильно її інтерпретувати. Прикладом використання набору протоколів в мережевому зв'язку є взаємодія між веб-сервером і веб-клієнтом. Ця взаємодія використовує ряд протоколів і стандартів у процесі обміну інформацією між ними. Різні протоколи взаємодіють один з одним, щоб гарантувати, що повідомлення будуть прийняті і зрозумілі обома сторонами. Прикладами протоколів є наступні.

- **Протокол прикладного рівня –** протокол передачі гіпертексту (**HTTP**, HyperText Transfer Protocol): визначає, яким чином взаємодіють веб-сервер і веб-клієнт. HTTP визначає зміст і формат запитів і відповідей, якими обмінюються клієнт і сервер. ПЗ і веб-клієнта, і веб-сервера реалізує HTTP як частина застосування. Для управління процесом передачі повідомлень між клієнтом і сервером HTTP звертається до інших протоколів.
- **Транспортний протокол –** протокол управління передачею (**TCP**, Transmission Control Protocol): управляє окремими сеансами зв'язку між серверами і клієнтами в Інтернеті. TCP ділить повідомлення HTTP на дрібніші частини – сегменти. Ці сегменти передаються між веб-сервером і клієнтськими процесами, запущеними на вузлі призначення. TCP також відповідає за управління розміром і швидкістю, з якою відбувається обмін повідомленнями між сервером і клієнтом.
- **Інтернет-протокол –** протокол IP: відповідає за прийом форматованих сегментів від TCP, інкапсуляцію їх в пакети, привласнення їм відповідних адрес і їх доставку по найкращому шляху до вузла призначення.
- **Протоколи мережевого доступу** описують дві основні функції **–** зв'язок по каналу передачі даних і фізична передача даних по мережевому середовищу. Протоколи управління каналами передачі даних приймають пакети від протоколу IP і форматують їх для передачі в середовищі. Стандарти і протоколи фізичної передачі даних управляють тим, як сигнали посилаються і як вони інтерпретуються клієнтами при отриманні. Одним з прикладів протоколу мережевого доступу є Ethernet.

Протоколи IP, HTTP і **DHCP** (Dynamic Host Configuration Protocol) є частиною набору протоколів Інтернет, який називається **протоколом управління передачею/протоколом IP (TCP/IP)**. Сімейство протоколів TCP/IP є відкритим стандартом, тобто ці протоколи знаходяться у вільному доступі для користувачів, і будь-який постачальник може впроваджувати ці протоколи на апаратних засобах або в ПЗ.

Протокол, заснований на стандартах, схвалюється у галузі мережевих технологій і затверджується організацією по стандартизації. Використання стандартів в розробці і реалізації протоколів гарантує, що продукти від різних виробників можуть взаємодіяти успішно. У передачі даних, наприклад, якщо одна сторона в сеансі зв'язку використовує протокол для управління одностороннім режимом зв'язку, а інша сторона використовує протокол двостороннього зв'язку, ймовірно, ніякого обміну даними не станеться.

Деякі компанії можуть працювати разом, щоб створити власний приватний протокол. Нерідко постачальник (чи група постачальників) розробляє приватний протокол для задоволення потреб своїх клієнтів, а потім сприяє тому, щоб ухвалити цей приватний протокол в якості відкритого стандарту. Наприклад, Ethernet був протоколом, спочатку розробленим Бобом Меткалфом (Bob Metcalfe) в дослідницькому центрі Palo Alto (PARC) компанії Xerox в 70-х рр. минулого століття. Заснувавши в 1979 році власну компанію 3Com, Боб Меткалф співпрацював з Digital Equipment Corporation (DEC), Intel і Xerox і просував стандарт «DIX» для Ethernet. У 1985 році Інститут інженерів з електротехніки і електроніки (IEEE) опублікував стандарт IEEE 802.3, який був майже ідентичний Ethernet. Сьогодні 802.3 є загальним стандартом, що використовується в локальних мережах (LAN).

Сімейство протоколів IP – це набір протоколів, необхідних для передачі і прийому інформації з використанням Інтернету. Цей протокол відоміший як TCP/IP, оскільки двома першими мережевими протоколами, визначеними для цього стандарту, були TCP і IP. Заснований на відкритих стандартах, TCP/IP замінив приватні набори протоколів окремих постачальників, такі як AppleTalk компанії Apple і Internetwork Packet Exchange (IPX/SPX) компанії Novell.

Першою мережею з комутацією пакетів і попередником сучасного Інтернету була Advanced Research Projects Agency Network (ARPANET), яка з'явилася в 1969 році за рахунок з'єднання базових ЕОМ в чотирьох місцях розташування. ARPANET фінансувався Міністерством оборони США і використовувався в університетах і науково-дослідних лабораторіях. Компанія Bolt, Beranek and Newman (BBN) виступала підрядчиком, виконавши основну частину первинної розробки ARPANET, включаючи створення першого маршрутизатора, який називався процесором інтерфейсних повідомлень (IMP).

У 1973 році Роберт Кан (Robert Kahn) і Винтон Серф (Vinton Cerf) почали роботу над протоколом TCP для розробки наступного покоління ARPANET. TCP був розроблений, щоб замінити програму мережевого управління (NCP) в мережі ARPANET. У 1978 році TCP був розділений на два протоколи: TCP і IP. Пізніше до набору протоколів TCP/IP були додані інші протоколи, включаючи Telnet, FTP, DNS і багато інших.

Сімейство протоколів TCP/IP реалізоване у вигляді стеку TCP/IP як на відправляючому, так і на приймаючому вузлах, і пов'язано з наскрізною доставкою цих застосувань по мережі. Протоколи 802.3 або Ethernet використовуються для передачі IP -пакета у фізичному середовищі передачі даних локальної мережі.

Відкриті стандарти заохочують конкуренцію та інновації. Крім того, вони гарантують, що продукт окремої компанії не зможе монополізувати ринок або отримати несправедливу перевагу в порівнянні з конкурентами. Відкриті стандарти також дозволяють клієнту з ОС OS X від компанії Apple завантажити веб-сторінку з веб-сервера під управлінням ОС Linux. Це пов'язано з тим, що обидві ОС використовують протоколи відкритих стандартів, наприклад, з набору протоколів TCP/IP.

Організації по стандартизації відіграють важливу роль в підтримці відкритого Інтернету з вільно доступною специфікацією і протоколами, які можуть бути реалізовані будь-яким постачальником. Організації по стандартизації зазвичай є нейтральними некомерційними організаціями, створеними для розробки і просування концепції відкритих стандартів.

Розглянемо наступні організації по стандартизації.

- Суспільство Інтернет (ISOC, Internet Society).
- Рада з архітектури Інтернету (IAB, Internet Architecture Board).
- Інженерна група по розвитку Інтернету (IETF, Internet Engineering Task Force).
- Інститут інженерів по електротехніці і електроніці (IEEE, Institute of Electrical and Electronics Engineers).
- Міжнародна організація по стандартизації (ISO, International Organization for Standardization).

Суспільство Інтернет (ISOC) відповідає за сприяння відкритій розробці, розвитку і використанню Інтернету у всьому світі. ISOC сприяє розвитку відкритих стандартів і протоколів для технічної інфраструктури Інтернету, у тому числі здійснює нагляд за радою з архітектури Інтернету (IAB).

Рада з архітектури Інтернету (IAB) відповідає за загальне керівництво і розробку інтернет-стандартів. IAB забезпечує нагляд за архітектурою протоколів і процедур в Інтернеті.

Місія IETF – розробка, оновлення і підтримка Інтернету, а також технологій TCP/IP. Одним з ключових обов'язків IETF є підготовка документів **Request for Comments (RFC)**, які є меморандумами протоколів, процесів і технологій для Інтернету.

IEEE є однією з провідних організацій у світі з розробки стандартів. Організація створює і підтримує стандарти в різних галузях, у тому числі в електроенергетиці, охороні здоров'я,

телекомунікаціях і мережевих технологіях. Сімейство стандартів IEEE 802 застосовується в локальних і міських мережах, включаючи дротяні і безпровідні.

Стандарти IEEE 802.3 і IEEE 802.11 є значущими стандартами IEEE в області комп'ютерних мереж. Стандарт IEEE 802.3 визначає управління доступом до середовища передачі даних (MAC) для дротяних мереж Ethernet. Як правило, ця технологія призначена для локальних мереж (LAN), але в ній також використовуються застосування глобальних мереж (WAN). Стандарт 802.11 визначає набір стандартів для реалізації безпровідних локальних мереж (WLAN). Цей стандарт визначає фізичний рівень і рівень каналу передачі даних OSI для безпровідних комунікацій.

У мережевих технологіях **організація ISO** найбільш відома завдяки створенню еталонної моделі **OSI** (Open System Interconnection) взаємодії відкритих систем. ISO опублікувала еталонну модель OSI в 1984 році в рамках розробки багаторівневої системи мережевих протоколів. Первинною метою цього проекту було не лише створити еталонну модель, але і закласти основу для комплексу протоколів, призначених для Інтернету. Такий комплекс протоколів дістав назву «набір протоколів OSI». При цьому у зв'язку із збільшенням популярності сімейства протоколів TCP/IP (розробленого Винтоном Серфом, Робертом Каном та іншими) набір протоколів OSI не був вибраний в якості набору протоколів для Інтернету. Замість нього було вибрано сімейство протоколів TCP/IP. Сімейство протоколів OSI було реалізоване на телекомунікаційному устаткуванні і використовується в телекомунікаційних мережах. Організація ISO також відповідає за створення стандартів для протоколів маршрутизації.

1.7. Еталонні моделі OSI і TCP/IP

При використанні багаторівневої моделі для опису мережевих протоколів і експлуатації існують певні переваги. Використання багаторівневої моделі :

- спрощує розробку протоколів, оскільки протоколи, що працюють на певному рівні, визначають формат оброблюваних даних і надають інтерфейс до верхніх і нижніх рівнів;
- сприяє створенню постачальниками конкуруючих продуктів уніфікованих рішень;
- унеможливлює зміни технологій або функцій одного рівня без урахування наслідків для верхніх і нижніх рівнів;
- надає спільну мову для опису функцій мережевої взаємодії.

Існує два основні типи моделей мережі.

- **Протокольна модель** відповідає структурі певного набору протоколів. Ієрархічний набір пов'язаних протоколів відповідає усім функціональним можливостям, необхідним для взаємодії мережі, що об'єднує людей, з мережею передачі даних. TCP/IP – протокольна модель, оскільки в ній описуються функції, які виконуються на кожному рівні протоколів, що входять в сімейство протоколів TCP/IP.
- **Еталонна модель** забезпечує послідовність в усіх мережевих протоколах і сервісах шляхом опису того, що необхідно зробити на певному рівні. Еталонна модель не використовується як специфікація для безпосередньої реалізації і не забезпечує достатній рівень деталізації, щоб точно визначити сервіси мережевої архітектури. Основна мета еталонної моделі – сприяти яснішому розумінню відповідних функцій і процесів.

Модель взаємодії відкритих систем (OSI) є найбільш відомою міжмережевою еталонною моделлю (див.табл.1.1). Вона використовується для проектування мереж, технічних вимог до операцій, для пошуку і усунення неполадок. Модель OSI представляє розширений список можливостей і сервісів, які можуть відбуватися на кожному рівні. Крім того, вона описує взаємодію кожного рівня з рівнями, розташованими поруч.

Примітка. Якщо рівні моделі TCP/IP позначаються тільки за назвою, то 7-рівнева модель OSI часто позначається за номером. Наприклад, фізичний рівень називається рівнем 1 моделі OSI.

Табл. 1.1. Призначення рівнів моделі OSI

Рівні моделі OSI	Призначення рівня моделі OSI
7. Рівень додатків **(Application layer)**	Забезпечує взаємодію мережі й користувача. Рівень дозволяє додаткам користувача доступ до мережевих служб, таких як обробник запитів до баз даних, доступ до файлів, пересиланню електронної пошти, відповідає за передачу службової інформації, надає додаткам інформацію про помилки.
6. Рівень представлення **(Presentation layer)**	Відповідає за перетворення протоколів і кодування/декодування даних. Запити додатків, отримані з прикладного рівня, він перетворить у формат для передачі по мережі, а отримані з мережі дані перетворить у формат, зрозумілий додаткам. На цьому рівні може здійснюватися стиснення/розпакування або кодування/декодування даних, а також перенапрямок запитів іншому мережевому ресурсу, якщо вони не можуть бути оброблені локально.
5. Сеансовий рівень **(Session layer)**	Відповідає за підтримку сеансу зв'язку, дозволяючи додаткам взаємодіяти між собою тривалий час. Рівень керує створенням/завершенням сеансу, обміном інформацією, синхронізацією завдань, визначенням права на передачу даних і підтримкою сеансу в періоди неактивності додатків.
4. Транспотрний рівень **(Transport layer)**	Призначений для доставлення даних без помилок, втрат і дублювання в тій послідовності, у якій вони були передані. При цьому немає значення, які дані передаються, звідки й куди, тобто він визначає сам механізм передачі. Блоки даних він розділяє на фрагменти, розмір яких залежить від протоколу, короткі об'єднує в один, довгі розбиває.
3. Мережевий рівень **(Network layer)**	Призначений для визначення шляху передачі даних. Відповідає за трансляцію логічних адрес й імен у фізичні, визначення найкоротших маршрутів, комутацію й маршрутизацію пакетів, відстеження неполадок і заторів у мережі.
2. Канальний рівень **(Data Link layer)**	Призначений для забезпечення взаємодії мереж на фізичному рівні та контролю за помилками, які можуть виникнути. Отримані з фізичного рівня дані він упаковує в кадри даних, перевіряє на цілісність, якщо потрібно – виправляє помилки й відправляє на мережний рівень.
1. Фізичний рівень **(Physical layer)**	Найнижчий рівень моделі, призначений безпосередньо для передачі потоку даних. Здійснює передачу електричних або оптичних сигналів у кабель і відповідно їхній прийом і перетворення в біти даних відповідно до методів кодування цифрових сигналів.

Протокольна модель мережевої взаємодії TCP/IP була створена на початку 70-х років і нерідко називається моделлю мережі Інтернет. Більшість протокольних моделей описують стек протоколів певного виробника. Оскільки модель TCP/IP є відкритим стандартом, жодна компанія не має права контролювати її визначення. Визначення і протоколи TCP/IP розглядаються на загальнодоступному форумі і визначаються в загальнодоступних

стандартах RFC. RFC містять як офіційні технічні характеристики протоколів обміну даними, так і ресурси, що описують застосування протоколів.

Табл. 1.2. Призначення рівнів моделі TCP/IP

Рівні моделі TCP/IP	Призначення рівня моделі TCP/IP
4. Рівень додатків	Представлення даних користувачу, кодування і управління діалоговими вікнами.
3. Транспортний рівень	Підтримка зв'язку між різними пристроями в різних мережах.
2. Міжмережевий рівень	Визначення оптимального шляху через мережу.
1. Рівень мережевого доступу	Управління пристроями і середовищами, що формують мережу.

1.8. Порівняння моделей OSI і TCP/IP

Сімейство протоколів TCP/IP може бути описане з точки зору еталонної моделі OSI. У моделі взаємодії відкритих систем (OSI) рівень доступу до мережі і рівень додатків в моделі TCP/IP додатково підрозділяються для опису окремих функцій, які реалізуються на цих рівнях.

На рівні доступу до мережі сімейство протоколів TCP/IP не визначає список протоколів для передачі по фізичному середовищу; воно описує тільки передачу з міжмережевого рівня фізичним мережевим протоколам (див.табл. 1.3).

Рівні 1 і 2 моделі OSI описують необхідні процедури для доступу до середовища передачі і фізичні засоби відправки даних по мережі.

Повний збіг двох мережевих моделей відбувається на рівнях 3 і 4 моделі OSI. Рівень 3 (мережевий рівень) зазвичай використовується для опису ряду процесів, які виникають в усіх мережах передачі даних при адресації і маршрутизації повідомлень в об'єднаній мережі. IP – це протокол з набору протоколів TCP/IP, що реалізує функціональність, описану на рівні 3 OSI.

Рівень 4 (транспортний рівень моделі OSI) описує загальні сервіси і функції, які надають впорядковану і надійну доставку даних між вузлами джерела і призначення. Ці функції включають підтвердження, усунення помилок і відновлення послідовності даних. На цьому рівні основні функції забезпечують протоколи TCP і UDP (протокол користувацьких датаграм) сімейства TCP/IP.

Прикладний рівень TCP/IP включає ряд протоколів, які надають певну функціональність різним застосуванням для кінцевих користувачів. Рівні 5, 6 і 7 моделей OSI використовуються в якості посилання для розробників і постачальників прикладного ПЗ у виробництві мережевої продукції.

Табл. 1.3. Порівняння моделей OSI та TCP/IP

Рівні моделі OSI	Основні протоколи	Рівні моделі TCP/IP
Рівень додатків Рівень представлення Сеансовий рівень	HTTP, DNS, DHCP, FTP	Рівень додатків
Транспотрний рівень	TCP, UDP	Транспотрний рівень
Мережевий рівень	IPv4, IPv6, ICMPv4, ICMPv6	Міжмережевий рівень
Канальний рівень Фізичний рівень	PPP, Frame Relay, Ethernet	Рівень мережевого доступу

Висновок до лекції 1

Існують мережі різного розміру, починаючи від простих мереж, що складаються з двох комп'ютерів, до систем, що сполучають мільйони пристроїв. Інтернет – найбільша мережа у всьому світі. Інфраструктура мережі – це платформа, що підтримує конкретну мережу. Вона виконує роль стабільного і надійного каналу для передачі даних. Вона складається з мережевих компонентів, до яких відносяться кінцеві пристрої, проміжні пристрої і засоби передачі даних. Мережі мають бути надійними. Це означає, що мережа має бути відмовостійкою, масштабованою, а також повинна забезпечувати якість обслуговування і безпеку інформації і ресурсів в мережі. Мережева безпека є невід'ємною частиною комп'ютерних мереж, незалежно від їх масштабів: починаючи з домашньої мережі, де до Інтернету підключений лише один ПК, до корпоративної мережі, що налічує тисячі користувачів.

Мережі передачі даних – це системи крайових і проміжних пристроїв, а також засобів передачі даних, що сполучають ці пристрої. Для успішного обміну даними ці пристрої повинні знати, як обмінюватися інформацією. Ці пристрої повинні відповідати правилам і протоколам, що регламентують процес обміну даними. TCP/IP – приклад набору протоколів. Більшість протоколів створюються організаціями по стандартизації, такими як Інженерна група по розвитку Інтернету (IETF) або Інститут інженерів по електротехніці і електроніці (IEEE). Інститут інженерів по електротехніці і електроніці – професійна організація для фахівців, що працюють в області електротехніки і електроніки. ISO, Міжнародна організація по стандартизації, є розробником міжнародних стандартів для широкого спектру продуктів і послуг.

Найбільш широко поширеними мережевими моделями є моделі OSI і TCP/IP. Зв'язування протоколів, які використовуються для передачі даних на різних рівнях цих моделей, корисно для визначення того, які пристрої і сервіси використовуються в певних точках, коли дані проходять через локальні і глобальні мережі. Модель OSI описує процеси кодування, форматування, сегментації і інкапсуляції даних для наступної передачі по мережі. Набір протоколів TCP/IP – це протокол відкритого стандарту, схвалений у галузі мережевих технологій, а також затверджений організацією по стандартизації.

Питання для закріплення

1. Які типи комп'ютерних мереж ви знаєте?
2. Які технології доступу в Інтернет ви знаєте?
3. Сформулюйте основні вимоги до комп'ютерної мережі.
4. Які компоненти мережі ви знаєте?
5. Поясність процес комутації каналів.
6. Поясніть принцип функціонування мереж з комутацією пакетів.
7. У чому полягає якість обслуговування комп'ютерної мережі?
8. Наведіть приклади кінцевих пристроїв комп'ютерної мережі.
9. Наведіть приклади проміжних пристроїв комп'ютерної мережі.
10. Що таке середовище передачі даних?
11. Для чого використовується фізична та логічна топології мереж?
12. Для чого використовується мережева інтерфейсна плата?
13. Що таке хмарні обчислення?
14. Які мережеві протоколи і галузеві стандарти ви знаєте?
15. Чим відрізняються протокольна та еталонна модель?
16. Яке призначення рівнів моделі TCP/IP?
17. Яке призначення рівнів моделі OSI?

Список рекомендованої літератури

1. CCNA R&S ITN Chapter 1: Exploring the Network // Електронний ресурс. Режим доступу: http://static-course-assets.s3.amazonaws.com
2. Комп'ютерні мережі та телекомунікації: навч. посіб. / В. А. Ткаченко, О. В. Касілов, В. А. Рябик. – Харків : НТУ «ХПІ», 2011. – 224 с.
3. Городецька О.С. Комп'ютерні мережі. Навчальний посібник / О. С. Городецька, В. А. Гикавий, О. В. Онищук. − Вінниця : ВНТУ, 2015. − 128 с.
4. Мережева модель OSI // Електронний ресурс. Режим доступу: http://bourabai.kz/lan/03.html

Лекція 2. Тема: «Мережева операційна система»

План лекції

2.1. Мережеві ОС.
2.2. Функції операційної системи IOS.
2.3. Метод консольного доступу.
2.4. Методи доступу за допомогою Telnet, SSH і AUX**.**
2.5. Програми емуляції терміналу.
2.6. Режими роботи операційної системи CISCO IOS.
2.7. Структура команд операційної системи IOS.
2.8. Основні команди налаштування і перевірки мережевих пристроїв.

2.1. Мережеві ОС

Операційні системи (ОС) використовуються на усіх кінцевих і мережевих пристроях, підключених до мережі Інтернет. При включенні комп'ютер завантажує ОС в оперативний запам'ятовуючий пристрій (ОЗП) з диску. Частина коду ОС, яка безпосередньо взаємодіє з апаратним забезпеченням комп'ютера, називається **ядром ОС**. Частина, яка забезпечує зв'язок між застосуваннями і користувачем, називається **оболонкою.** Користувач взаємодіє з оболонкою за допомогою **інтерфейсу командного рядка (CLI,** Command Line Interface**)** або **графічного інтерфейсу користувача (GUI,** Graphical User Interface**).**

При використанні інтерфейсу командного рядка відбувається безпосереднє звернення до системи в текстовому режимі методом введення команд з клавіатури в командний рядок. Система виконує команду, часто виводячи вихідні дані в текстовому форматі. GUI забезпечує взаємодію з системою в середовищі, де використовуються графічні зображення, мультимедіа і текст. Дії виконуються за допомогою зображень на екрані. GUI зручніший і не вимагає таких знань структури команд, як інтерфейс командного рядка. У більшості ОС є обидва інтерфейси.

Доступ до більшості операційних систем крайових пристроїв здійснюється за допомогою GUI, включаючи доступ до MS Windows, MAC OS X, ОС Linux, Apple iOS, Android.

ОС на домашніх маршрутизаторах зазвичай називається мікропрограмою. Найбільш поширений спосіб налаштування домашнього маршрутизатора – доступ до GUI через веб-браузер. На більшості домашніх маршрутизаторів при появі нових функцій або вразливих місць в безпеці активується оновлення мікропрограм.

Мережеві пристрої інфраструктури працюють на основі мережевої ОС. Мережева ОС, що використовується на пристроях Cisco, називається **операційною системою мережевої взаємодії Cisco (IOS).** Операційна система Cisco IOS використовується в більшості пристроїв Cisco, незалежно від їх типу і розмірів. Найбільш поширений спосіб доступу до цих пристроїв – використання інтерфейсу командного рядка (CLI).

Приховані функції комутаторів і маршрутизаторів дуже схожі. IOS на комутаторі або маршрутизаторі надає інтерфейс мережевому фахівцеві. Технічний фахівець може ввести певні команди, щоб налаштувати або запрограмувати пристрій для виконання різних мережевих функцій. Функціональні можливості IOS відрізняються на різних мережевих пристроях залежно від призначення пристроїв і підтримуваних функцій.

Розмір самого файлу IOS складає декілька мегабайт і зберігається в напівпостійній (флеш) пам'яті. Флеш пам'ять забезпечує незалежне зберігання даних. Це означає, що вміст пристрою зберігається, навіть якщо втрачено живлення. Не дивлячись на те, що вміст флеш пам'яті не втрачається під час втрати живлення, при необхідності його можна змінити або перезаписати. Завдяки цьому IOS можна оновлювати до новішої версії або додавати нові функціональні можливості без заміни устаткування. Флеш пам'ять можна використовувати для одночасного зберігання декількох версій ПЗ IOS.

У багатьох пристроях Cisco при підключенні до мережі IOS копіюється з флеш пам'яті в ОЗП. Потім, при роботі пристрою, IOS запускається з ОЗП, який забезпечує зберігання даних, які використовуються пристроєм для підтримки роботи мережі. Запуск IOS з ОЗП підвищує продуктивність пристрою, при цьому ОЗП вважається енергозалежною пам'яттю, оскільки дані втрачаються під час відключення живлення. Відключення живлення може відбуватися через випадкове або навмисне перезавантаження.

Кількість необхідної флеш пам'яті і оперативної пам'яті залежить від версії IOS. Для технічного обслуговування мережі і планування вкрай важливо визначити вимоги флеш пам'яті і ОЗП для кожного пристрою, включаючи максимальні конфігурації флеш пам'яті і ОЗП.

2.2. Функції операційної системи IOS

Фахівці в області мережевого проектування покладаються саме на функції маршрутизаторів і комутаторів Cisco IOS, щоб проектовані мережі функціонували належним чином. До найбільш значущих функцій маршрутизаторів або комутаторів Cisco відносяться:

- забезпечення безпеки мережі;
- IP -адресація віртуальних і фізичних інтерфейсів;
- можливість налаштування інтерфейсу для оптимізації підключення відповідного середовища передачі даних;
- маршрутизація;
- налаштування технологій якості обслуговування (QoS);
- підтримка технологій управління мережею.

Кожна функція або служба має відповідний набір команд конфігурації, які дозволяють мережевому фахівцеві її активувати.

Доступ до сервісів CISCO IOS зазвичай здійснюється за допомогою CLI.

2.3. Метод консольного доступу

Існує декілька способів доступу до середовища інтерфейсу командного рядка (CLI). Нижче приведені найбільш поширені методи.

- Консоль.
- Telnet або SSH.
- Порт AUX.

Консольний порт – це порт управління, що забезпечує можливість позасмугового доступу до пристрою Cisco. Позасмуговий доступ – це доступ через виділений адміністративний канал, який використовується виключно в цілях технічного обслуговування пристрою. Перевага використання порту консолі полягає в тому, що доступ до пристрою можливий навіть без налаштування мережевих послуг, наприклад, початкової конфігурації мережевого пристрою. При виконанні початкової конфігурації комп'ютер підключається до порту консолі пристрою за допомогою спеціального кабелю і запускається

програма емуляції терміналу для налаштування мережевого устаткування. Команди конфігурації для налаштування комутатора або маршрутизатора можна ввести на підключеному комп'ютері.

Консольний порт також можна використовувати, коли робота мережевих сервісів порушена і віддалений доступ до пристрою на базі CISCO IOS неможливий. В цьому випадку підключення до консольного порту дозволяє комп'ютеру визначати стан пристрою. За замовчуванням за допомогою консольного з'єднання можна спостерігати завантаження мережевого пристрою, здійснювати усунення неполадок, переглядати повідомлення про помилки. Після того, як мережевий фахівець підключився до пристрою, він може виконати усі необхідні команди конфігурації за допомогою сеансу консолі.

Для багатьох пристроїв IOS консольне підключення відбувається без використання технологій для забезпечення безпеки підключення. При цьому для запобігання несанкціонованому доступу до пристроїв доступ має бути захищений паролем. У разі втрати пароля існує цілий ряд заходів, що дозволяють дістати доступ до цього пристрою без пароля. Також пристрій повинен розташовуватися в закритому приміщенні або апаратній кімнаті для запобігання несанкціонованому фізичному доступу.

2.4. Методи доступу за допомогою Telnet, SSH і AUX

Telnet – це спосіб віддаленого встановлення сеансу інтерфейсу командного рядка (CLI) через віртуальний інтерфейс по мережі. На відміну від консольного підключення, для сеансів Telnet потрібні активні мережеві сервіси на пристрої. У мережевому пристрої має бути налагоджений хоча б один активний інтерфейс з інтернет-адресою, наприклад, з адресою IPv4. Пристрої CISCO IOS включають процес сервера Telnet, що дозволяє користувачам вводити команди конфігурації від клієнта Telnet. Окрім підтримки процесу сервера Telnet, пристрій CISCO IOS також містить клієнт Telnet. Це дозволяє адміністраторові мережі відправляти запит по протоколу telnet з інтерфейсу командного рядка (CLI) пристроїв Cisco будь-якому іншому пристрою з підтримкою процесу сервера Telnet.

Протокол Secure Shell (SSH) надає віддалений вхід в систему аналогічно Telnet, за винятком того, що він використовує безпечніші мережеві служби. Протокол SSH надає вищий рівень аутентифікації на основі пароля, ніж протокол Telnet, і при передачі інформації про сеанс використовує шифрування. Це захищає дані користувача, пароль і дані про сеанс управління. Рекомендується використовувати SSH замість протоколу Telnet.

Більшість версій CISCO IOS включають SSH -сервер. У деяких пристроях ця мережева служба за замовчуванням включена. У інших пристроях SSH -сервер вимагається включати вручну. Пристрої на базі Cisco IOS також містять SSH -клієнт, який можна використовувати для встановлення SSH -сеансів з іншими пристроями.

Застарілий метод встановлення сеансу інтерфейсу командного рядка (CLI) – **за допомогою комутованого з'єднання по телефону до допоміжного порту (AUX) маршрутизатора**. Аналогічно з підключенням консолі допоміжний метод також забезпечує позасмугове підключення і не вимагає налаштування або наявності яких-небудь мережевих сервісів. Якщо робота мережевих сервісів була порушена, віддалений адміністратор може дістати доступ до комутатора або маршрутизатора по телефонній лінії. Порт AUX може також використовуватися локально, як і консольний порт, з прямим підключенням до комп'ютера, на якому працює програма емуляції терміналу. При цьому консольний порт прийнятніше за порт AUX для пошуку і усунення неполадок, оскільки він за замовчуванням відображує повідомлення про запуск, усунення неполадок і помилки.

2.5. Програми емуляції терміналу

Існує багато програм емуляції терміналу, доступних для підключення до мережевого пристрою або послідовного підключення через консольний порт або з'єднання Telnet/SSH. До деяких з цих програм відносяться:

- PuTTY (мал. 2.1);
- Tera Term (мал. 2.2);
- SecureCRT (мал. 2.3);
- HyperTerminal;
- Terminal OS X.

Ці програми дозволяють максимально підвищити продуктивність роботи за рахунок регулювання розмірів вікна, зміни розміру шрифту і зміни комбінації кольорів.

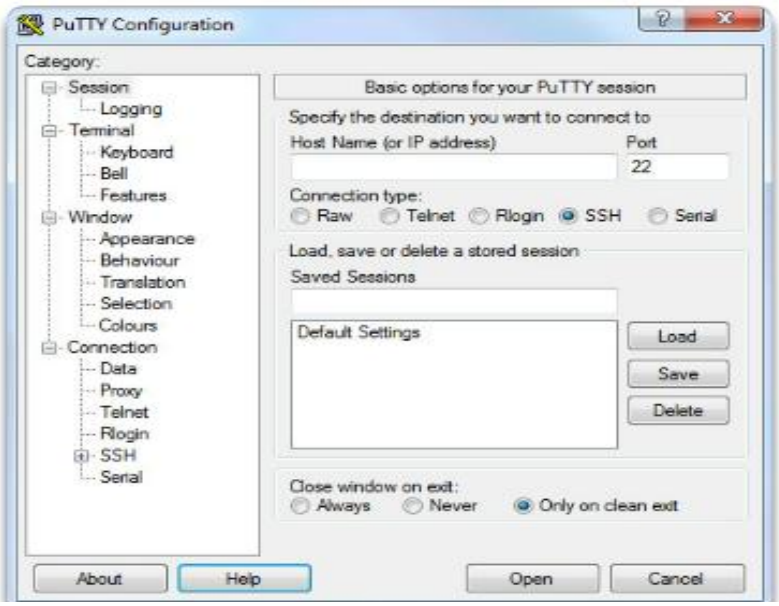


Рис. 2.1. Програма **PuTTY** [1]

Рис. 2.2. Програма **Tera Term** [1]

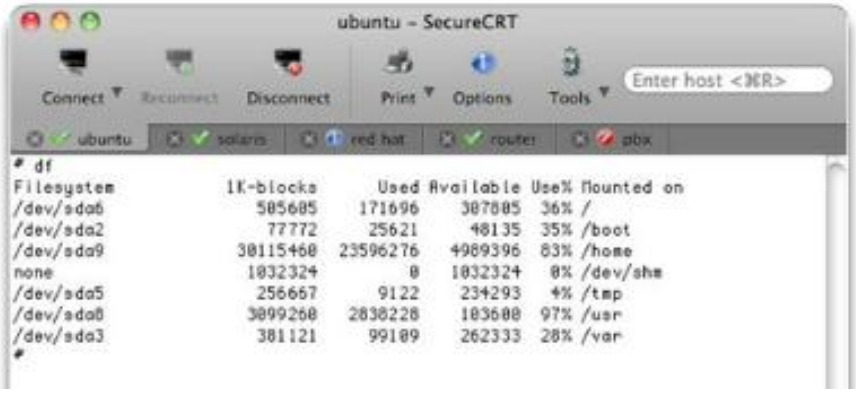


Рис. 2.3. Програма **SecureCRT** [1]

2.6. Режими роботи операційної системи CISCO IOS

Після того, як мережевий фахівець встановить з'єднання з пристроєм, він може почати його налаштування. Мережевий фахівець повинен перемикатися між різними режимами IOS. Режими CISCO IOS для комутаторів і маршрутизаторів дуже схожі. Інтерфейс командного рядка (CLI) використовує ієрархічну структуру для режимів.

У ієрархічному порядку режимів від базового до найбільш спеціалізованого основними режимами являються:

- користувацький режим;
- привілейований режим;
- режим глобальної конфігурації;
- інші спеціальні режими конфігурації, такі як режим конфігурації інтерфейсу.

У кожному режимі є відмінний командний рядок, який використовується для виконання певних завдань з певним набором команд, доступним тільки в цьому режимі. Наприклад, режим глобальної конфігурації дозволяє технічному фахівцеві задавати на пристрої загальні налаштування, наприклад, призначити пристрою ім'я. При цьому, якщо мережевому фахівцеві необхідно налаштувати, наприклад, параметри безпеки на конкретному порті комутатора, йому потрібно буде використовувати інший режим. В цьому випадку слід увійти до режиму конфігурації інтерфейсу для цього конкретного порту. Усі налаштування, що вводяться в режимі конфігурації інтерфейсу, застосовуються тільки до цього порту.

Для забезпечення безпеки можна налаштувати ієрархічну структуру. Для кожного режиму в ієрархії можуть вимагатися різні процедури аутентифікації. Це дозволяє контролювати рівень доступу, який мають мережеві фахівці.

Основними режимами є користувацький і привілейований. Здійснюючи функції захисту, ПЗ CISCO IOS розділяє сесії режимів на два рівні доступу. Привілейований режим має вищий рівень прав відносно можливостей використання пристрою.

Користувацький режим знаходиться на базовому рівні ієрархічної структури режимів. Це перший режим, в якому користувач починає роботу при вході в інтерфейс командного рядка (CLI) пристрою IOS. Користувацький режим дозволяє виконувати обмежену кількість базових команд. Цей режим часто називають «режимом для перегляду». У користувацькому режимі забороняється виконувати команди, які можуть змінити параметри пристрою.

За замовчуванням для входу в користувацький режим з консолі аутентифікація не потрібна. Проте під час початкової конфігурації рекомендується налаштувати процедуру аутентифікації.

Користувацький режим визначається за допомогою команди інтерфейсу командного рядка, що закінчується символом «>«. Наступний приклад демонструє символ «>« в командному рядку комутатора:

Switch>

Привілейований режим використовується для виконання команд конфігурації і управління мережевим пристроєм. Спочатку користувачеві треба увійти до користувацького режиму, а з нього – в привілейований режим.

Привілейований режим визначається командним рядком, що закінчується символом «#».

Switch#

Рекомендується переконатися в налаштуванні аутентифікації.

Привілейований режим відкриває доступ до режиму глобальної конфігурації і до усіх інших конкретніших режимів налаштування.

Режим глобальної конфігурації є основним режимом конфігурації. У режимі глобальної конфігурації виконуються зміни конфігурації інтерфейсу командного рядка (CLI) пристрою, що впливають на його роботу в цілому. Перед доступом до спеціалізованих режимів конфігурації треба увійти до режиму глобальної конфігурації.

Щоб перевести пристрій з привілейованого режиму в режим глобальної конфігурації і виконати введення команд конфігурації з терміналу, використовується команда інтерфейсу командного рядка:

Switch# configure terminal

Після введення команди командний рядок змінюється так, щоб показати, що він знаходиться в режимі глобальної конфігурації.

Switch(config)#

З режиму глобальної конфігурації користувач може перейти в різні режими конфігурації для підкоманд. Кожен з цих режимів дозволяє виконати налаштування параметрів конкретної області або функції пристрою з операційною системою IOS. Нижче приведені деякі з них.

- **Режим конфігурації інтерфейсу** призначений для налаштування одного з мережевих інтерфейсів (Fa0/0 або S0/0/0).
- **Режим конфігурації лінії** призначений для налаштування одного з фізичних або віртуальних ліній (консоль, AUX, VTY) (рис. 2.4).

```
Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)# line vty 0 4
Switch(config-line)# interface fastethernet 0/1
Switch(config-if)# end
Switch#
```

Рис. 2.4.Режим конфігурації віртуальних ліній VTY [1]

Щоб повернутися в режим глобальної конфігурації з конкретного режиму, використовується команда exit в командному рядку. Щоб остаточно вийти з режиму конфігурації і повернутися в привілейований режим, необхідно ввести end або скористатися комбінацією клавіш Ctrl - Z.

При використанні інтерфейсу командного рядка (CLI) режим визначається за командним рядком, який є унікальним для кожного режиму. За замовчуванням кожен командний рядок починається з імені пристрою. Після імені слідує залишок командного рядка, який визначає режим. Наприклад, запит за замовчуванням для режиму глобальної конфігурації на комутаторі виглядає так:

Switch(config)#

Команди enable і disable використовуються для перемикання інтерфейсу командного рядка між користувацьким і привілейованим режимами відповідно.

Щоб дістати доступ до привілейованого режиму, використовується команда enable. Іноді привілейований режим називають режимом включення (enable).

Синтаксис для введення enable виглядає так:

Switch> enable

Виконання цієї команди не вимагає якого-небудь параметра або ключового слова. Після натиснення клавіші Enter командний рядок зміниться так:

Switch#

Символ «#» у кінці командного рядка означає, що комутатор перемкнутий в привілейований режим.

Якщо в привілейованому режимі налагоджена аутентифікація паролем, IOS запросить пароль.

Наприклад:

Switch> enable

Пароль:

Switch#

Для повернення з привілейованого режиму в призначений для користувача використовується команда disable.

Наприклад:

Switch# disable

Switch>

Для виходу з режиму глобальної конфігурації і повернення в привілейований режим використовується команда exit.

Введення команди exit в привілейованому режимі призводить до закриття сеансу консолі. Це означає, що при введенні команди exit в привілейованому режимі ви побачите екран, який відкривається при першому запуску сеансу консолі. Для переходу з будь-якого підрежиму глобальної конфігурації в наступний режим ієрархії введіть команду exit.

Для переміщення з будь-якого підрежиму привілейованого режиму в привілейований режим введіть команду end або використовуйте поєднання клавіш Ctrl+Z.

Для переміщення з будь-якого підрежиму глобальної конфігурації в інший «актуальний» підрежим глобальної конфігурації просто введіть відповідні команди, які зазвичай вводяться в режимі глобальної конфігурації.

2.7. Структура команд операційної системи IOS

Кожна команда IOS має певний формат або синтаксис. Кожна команда виконується тільки з відповідного режиму. Загальний синтаксис команди – це команда, за якою йдуть відповідні ключові слова і параметри. Деякі команди складаються з ключових слів і параметрів, що забезпечують додаткові функціональні можливості. Команди використовуються для виконання яких-небудь дій, а ключові слова використовуються для визначення того, де і як треба виконати команду (рис.2.5).

Команда може мати один або декілька параметрів. На відміну від ключового слова, параметр, як правило, не є зумовленим словом. Параметр – це значення або змінна, визначена користувачем. Синтаксис забезпечує шаблон або формат, який необхідно використовувати при введенні команди.

Наприклад, для команди ping:

Синтаксис:

Switch> ping *ip - address*

Приклад зі значенням:

Switch> ping 10.10.10.5

Тут команда – ping, користувацький параметр - 10.10.10.5.

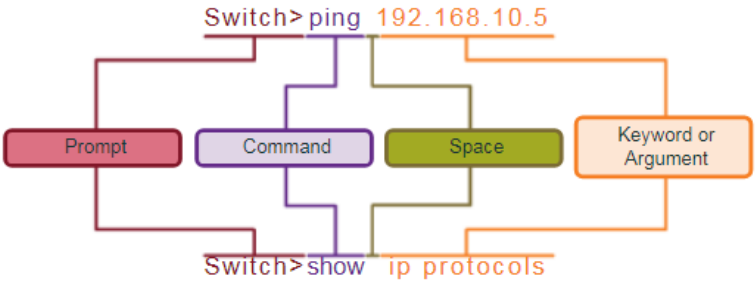


Рис. 2.5. Структура команд ОС IOS [1]

Контекстна довідка надає список команд і параметрів, пов’язаних з цими командами в контексті поточного режиму. Для доступу до контекстної довідки введіть знак (?) питання в будь-якому командному рядку. Послідує негайна відповідь навіть без натиснення клавіші Enter.

Контекстна довідка корисна для отримання списку доступних команд. Цей вид довідки можна використовувати в тих випадках, коли ви не знаєте імені команди або хочете дізнатися, чи підтримує IOS ту або іншу команду в певному режимі.

Наприклад, для отримання списку доступних команд в користувацькому режимі введіть знак (?) питання в командному рядку Switch>.

Крім того, контекстну довідку можна використовувати для відображення списку команд або ключових слів, які починаються з певного символу або символів. Якщо вказати знак питання без пропуску відразу після введення послідовності символів, IOS відобразить список команд або ключових слів для цього контексту, які починаються з вказаних символів.

Наприклад, введіть sh? для отримання списку команд, які починаються з поєднання символів sh.

Останній вид контекстної довідки використовується для визначення параметрів, ключових слів або параметрів, що співвідносяться з певною командою. При введенні команди введіть пропуск перед знаком ? , щоб визначити, що можна або треба ввести далі.

Інтерфейс командного рядка (CLI) IOS передбачає гарячі клавіші і клавіші швидкого виклику, які спрощують процес налаштування, моніторингу, пошуку і усунення неполадок.

Команди і ключові слова можна скоротити до мінімальної кількості символів, які залишаться унікальними. Наприклад, команду configure можна скоротити до conf, оскільки configure – це єдина команда, яка починається з символів conf. Скорочення con не підходить, оскільки з символів con починається декілька команд.

Ключові слова також можна скорочувати.

Наприклад, show interfaces можна скоротити таким чином:

Switch# show interfaces

Switch# show int

Можна скорочувати як команди, так і ключові слова. Наприклад:

Switch# sh int

2.8. Основні команди налаштування і перевірки мережевих пристроїв

Для перевірки і усунення неполадок в мережі слід перевірити роботу пристроїв. Базова команда для перевірки – show.

Існує багато різних варіантів цієї команди. Використовуйте команду show ? для отримання списку доступних команд у рамках вказаного контексту або режиму.

Типова команда show надає відомості про конфігурацію, експлуатацію і стан компонентів комутатора або маршрутизатора.

Досить поширена команда групи show – show interfaces. Ця команда служить для відображення статистичних відомостей за усіма інтерфейсами пристрою. Для відображення статистики певного інтерфейсу введіть команду show interfaces з вказівкою типу інтерфейсу і номера порту (слота). Наприклад:

Switch# show interfaces fastethernet 0/1

До додаткових команд show, часто використовуваним фахівцями мережі, відносяться:

show startup - config – відображує збережену конфігурацію, розташовану в NVRAM;

show running - config – відображує вміст файлу поточної конфігурації.

Коли команда показує більше вихідних даних, чим може відобразити екран, внизу екрану з’являється вікно More для перегляду наступної частини вихідних даних. Щоб проглянути тільки наступний рядок, натисніть клавішу Enter. При натисненні будь-якої іншої клавіші вихідні дані відміняються, а користувач повертається до командного рядка.

Команда

Switch# show version

відображує відомості про завантажену версію IOS, а також дані про пристрій і апаратне забезпечення. Якщо виконаний віддалений вхід в маршрутизатор або комутатор, команда

show version допоможе швидко дізнатися корисну інформацію про пристрій, до якого ви приєдналися. Ця команда виводить наступні дані:

- **Software version** - версія ПЗ IOS (зберігається у флеш пам'яті);
- **Bootstrap version** - версія програми початкового завантаження (зберігається в завантажувальному ПЗП);
- **System up - time** - час з моменту останнього перезавантаження;
- **System restart info** - спосіб перезапуску (наприклад, цикл включення-виключення, збій системи);
- **Software image name** - ім'я файлу образу IOS, що зберігається у флеш пам'яті;
- **Router type and processor type** - номер моделі і тип процесора;
- **Memory type and allocation (shared/main)** - ОЗП головного процесора і буферизація введення/виведення пакету;
- **Software features** - підтримувані протоколи/набори функцій;
- **Hardware interfaces** - доступні на пристрої інтерфейси;
- **Configuration register** - специфікації завантаження, налаштування швидкості консолі і інших параметрів.

Один з перших кроків при налаштуванні мережевого пристрою – це призначення унікального імені пристрою або вузла. Вузли відображуються у вікнах CLI і використовуються в різних процесах аутентифікації між пристроями. Їх треба використовувати в топологічних схемах. Імена вузлів настроюються на активному мережевому пристрої.

Відповідно до керівництва по позначенню імена повинні:

- починатися з букви;
- не містити пропусків;
- закінчуватися на букву або цифру;
- містити тільки букви, цифри і тире;
- містити не більше 64 символів.

У іменах вузлів на пристроях IOS, зберігаються усі прописні і рядкові символи. Цей метод відрізняється від більшості способів призначення імен в Інтернеті, в яких немає відмінностей між прописними і рядковими буквами.

Кожного разу, коли додається або змінюється пристрій, повинна оновлюватися документація. У цій документації пристроям мають бути присвоєне своє місце розташування, призначення і адреса.

Рекомендується фізично обмежувати доступ до мережевих пристроїв, розміщуючи їх в окремих приміщеннях або в закритих шафах. Проте, паролі залишаються основним засобом захисту від несанкціонованого доступу до мережевих пристроїв. На кожному пристрої, навіть на домашніх маршрутизаторах, мають бути встановлені паролі для обмеження доступу.

Для забезпечення безпеки пристрій IOS використовує ієрархічні режими. Для посилення захисту IOS може зажадати декілька паролів, щоб дозволяти доступ до різних рівнів ієрархії.

До приведених тут типів паролів відносяться:

- **пароль привілейованого режиму** - обмежує доступ в привілейований режим;
- **секретний пароль** - зашифрований пароль, що обмежує доступ в привілейований режим;
- **пароль консолі** - обмежує доступ до пристроїв через консольне підключення;
- **пароль для VTY** - обмежує доступ до пристроїв через Telnet.

Рекомендується використовувати різні паролі аутентифікації для кожного з рівнів доступу. Не дивлячись на те, що вхід в систему з декількома різними паролями незручний, це необхідний захід захисту інфраструктури мережі від несанкціонованого доступу. Використання ненадійних паролів або тих, які легко підібрати, як і раніше, представляє серйозну загрозу безпеки в багатьох сферах бізнесу.

Консольний порт мережевих пристроїв необхідно захистити як мінімум надійним паролем. Це знижує вірогідність доступу неавторизованих співробітників, які включають кабель і намагаються дістати доступ до пристрою.

Щоб встановити пароль для консолі рядка в режимі глобальної конфігурації, треба ввести наступні команди:

Switch(config)# line console 0

Switch(config - line)# password cisco

Switch(config - line)# login

У цьому прикладі у режимі глобальної конфігурації використовується команда line console 0, щоб увійти до режиму конфігурації рядка для консолі. Нуль використовується для позначення першого (а в більшості випадків – єдиного) інтерфейсу консолі. Друга команда – password cisco визначає пароль для консолі рядка. Команда login настроює комутатор для аутентифікації при вході в систему. Якщо включена процедура входу і налагоджений пароль, користувач консолі повинен буде ввести пароль, щоб дістати доступ до CLI.

Канали VTY (virtual terminal line) забезпечують доступ до пристроїв Cisco по протоколу Telnet. За замовчуванням багато комутаторів Cisco підтримують до 16 каналів VTY, пронумерованих від 0 до 15. Кількість каналів VTY, підтримуваних на маршрутизаторі Cisco, залежить від типу маршрутизатора і версії IOS. Але найчастіше встановлено п’ять каналів VTY. Ці канали пронумеровані від 0 до 4 за замовчуванням, хоча можна додавати додаткові канали. Пароль треба встановити для усіх доступних каналів VTY. Для усіх з’єднань можна встановити один пароль. При цьому часто виникає необхідність задати унікальний пароль для одного каналу, щоб забезпечити адміністраторові резервний доступ у тому випадку, якщо усі інші з’єднання зайняті.

Команди для призначення пароля каналів VTY:

Switch(config)# line vty 0 15

Switch(config - line)# password cisco

Switch(config - line)# login

Ще одна важлива команда, яка захищає пароль під час перегляду файлів конфігурації – service password - encryption. Ця команда шифрує паролі під час їх налаштування. Команда service password - encryption шифрує усі незашифровані паролі. Шифрування застосовується тільки до паролів у файлі конфігурації, але не до паролів, які відправлені по середовищу передачі даних. Ця команда не дозволяє неавторизованим співробітникам прочитати пароль.

Якщо виконати команди show running - config або show startup - config до виконання команди service password - encryption, то незашифровані паролі будуть видні у вихідних даних конфігурації. Потім можна виконати команду service password - encryption, після чого паролі будуть зашифровані. Після цього шифрування не можна буде відмінити.

Не дивлячись на те, що паролі захищають мережу від неавторизованих користувачів, необхідно використовувати повідомлення про те, що лише авторизованим користувачам можна дістати доступ до пристрою. Для цього треба додати **банер** у вихідні ці пристрої.

Банери можуть згодитися під час судового процесу, якщо користувач був звинувачений в недозволеному доступі. У деяких системах правосуддя не дозволено судове переслідування або стеження за користувачами без попередження.

Приклади формулювань, які можуть міститися в таких інформаційних банерах:

- «Доступ до пристрою дозволений тільки для авторизованих користувачів»;
- «Дії можуть відстежуватися»;
- «Будь-які спроби неавторизованого використання переслідуватимуться згідно з законом» тощо.

IOS надає безліч типів банерів. **Повідомлення поточного дня** (**MODT**, Message Of The Day) – досить поширений банер. Часто використовується для законного повідомлення, оскільки його бачать усі приєднані термінали.

Для налаштування повідомлення поточного дня в режимі глобальної конфігурації використовується наступний синтаксис:

Switch(config)# banner motd # message #

Після виконання команди банер буде показаний при усіх наступних спробах доступу до пристрою, поки він не буде видалений.

Файл поточної конфігурації відображає поточну конфігурацію, що функціонує на пристрої CISCO IOS. Він містить команди для визначення принципів роботи пристрою в мережі. Зміни поточної конфігурації негайно впливають на роботу пристрою.

Файл поточної конфігурації зберігається в робочій пам'яті пристрою або в ОЗП. Це означає, що файл поточної конфігурації тимчасово активний, коли працює пристрій (підключений до живлення). Проте при відключенні живлення пристрою або перезапуску пристрою усі незбережені зміни конфігурації будуть втрачені.

Після внесення змін у файл поточної конфігурації слід розглянути наступні варіанти дій.

- Повернути пристрій до початкової конфігурації.
- Видалити усі внесені зміни.
- Зробити змінену конфігурацію новою початковою конфігурацією.

Файл завантажувальної конфігурації відображує конфігурацію, яка буде застосована на пристрої після перезавантаження. Файл завантажувальної конфігурації зберігається в незалежній пам'яті (NVRAM). Після налаштування мережевого пристрою і зміни поточної конфігурації важливо зберегти ці зміни у файл завантажувальної конфігурації. Це запобігає втратам змін внаслідок збою живлення або випадкового перезавантаження.

Команду show running - config можна використовувати для перегляду файлу поточної конфігурації. Коли зміни перевірені, використовуйте команду copy running - config startup - config в командному рядку привілейованого режиму. Команда для збереження файлу поточної конфігурації у файл завантажувальної конфігурації виглядає так:

Switch# copy running - config startup - config

Після виконання команди файл поточної конфігурації оновлює файл завантажувальної конфігурації.

Якщо зміни, внесені в ході конфігурації, не принесли бажаного результату, можливо, знадобиться відновити попередню конфігурацію пристрою. Якщо ми не переписували початкову конфігурацію із змінами, поточну конфігурацію можна замінити початковою. Краще всього це здійснюється шляхом перезапуску пристрою і введення команди reload в командному рядку привілейованого режиму.

Виконуючи перезавантаження, IOS визначить, що змінена конфігурація не була збережена у файл початкової конфігурації. Якщо небажані зміни збережені у файл початкової конфігурації, можливо, знадобиться очистити усі конфігурації. Для цього треба видалити початкову конфігурацію і перезапустити пристрій.

Початкову конфігурацію можна видалити за допомогою команди erase startup - config.

Щоб видалити файл завантажувальної конфігурації, введіть команди erase NVRAM : startup - config або erase startup - config в командний рядок привілейованого режиму :

Switch# erase startup - config

Після введення команди з'явиться запит про підтвердження.

Примітка. Команду erase можна використовувати для видалення будь-якого файлу в пристрої. Неправильне використання цієї команди може привести до видалення самої IOS або інших важливих файлів.

Крім того, на комутаторі необхідно виконати команду delete vlan.dat на додаток до команди erase startup - config, щоб повернути конфігурацію, «вбудовану» за замовчуванням (що відповідає встановленою на підприємстві), :

Switch# delete vlan.dat

Delete filename [vlan.dat]?

Delete flash: vlan.dat? [confirm]

Switch# erase startup - config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

Switch#

Кожне посилання в мережі Інтернет не лише вимагає особливого типу середовища, але і окремої мережевої технології. Ethernet – найбільш поширена технологія локальної мережі (LAN) на сьогодні. Порти Ethernet можна знайти на пристроях кінцевих користувачів, комутаційних і інших мережевих пристроях, які можуть здійснювати фізичне підключення до мережі за допомогою кабелю. Щоб кабель міг сполучати пристрої за допомогою порту Ethernet, кабель має бути забезпечений правильним роз'ємом – RJ - 45.

Комутатори CISCO IOS не лише оснащені фізичними портами для пристроїв, але також одним або декількома віртуальними інтерфейсами комутаторів (**SVI**, Switch Virtual Interface). Такі інтерфейси називаються віртуальними, оскільки в пристрої немає пов'язаного з ними фізичного устаткування. Віртуальний інтерфейс створений в ПЗ та дозволяє віддалено управляти комутатором через мережу. Кожен комутатор поставляється з одним віртуальним інтерфейсом комутатора в конфігурації за замовчуванням. Віртуальним інтерфейсом за замовчуванням є VLAN1.

Для віддаленого доступу до комутатора на віртуальному інтерфейсі комутатора треба налаштувати IP -адресу і маску підмережі :

- **IP -адреса –** з маскою підмережі ідентифікує крайовий пристрій в мережевій взаємодії;
- **маска підмережі –** визначає, яка частина великої мережі використовується IP – адресою;

Розглянемо команди для активації IP-з'єднання з комутатором S1 за допомогою IP -адреси 192.168.10.2:

- **interface vlan 1 –** застосовується для переходу в режим налаштування інтерфейсу з режиму глобальної конфігурації;
- **ip address 192.168.10.2 255.255.255.0 –** налаштовує IP -адресу і маску підмережі для комутатора (тільки одне з декількох можливих поєднань IP -адреси і маски підмережі);
- **no shutdown -** активує інтерфейс.

Після налаштування цих команд усі IP -елементи в комутаторі будуть готові для передачі даних по мережі.

Висновок до лекції 2

Технічний фахівець повинен знати команди, щоб налаштувати або запрограмувати мережевий пристрій для виконання різних мережевих функцій. Доступ до сервісів CISCO IOS здійснюється за допомогою інтерфейсу командного рядка (CLI), увійти до якого можна через консольний порт, порт AUX або використовуючи протоколи Telnet або SSH. Один раз підключившись до інтерфейсу командного рядка (CLI), мережеві фахівці можуть змінювати конфігурації пристроїв CISCO IOS. CISCO IOS розроблена як операційна система з режимами, тобто мережевий фахівець повинен уміти перемикатися між різними ієрархічними режимами IOS. Кожен режим підтримує різні команди IOS.

Довідкове керівництво CISCO IOS – це набір онлайн-документів, що детально описують команди IOS, які використовуються на на маршрутизаторах і комутаторах. Маршрутизатори і комутатори CISCO IOS підтримують подібну ОС з режимами, аналогічні командні структури і багато схожих команд. Крім того, при впровадженні цих двох пристроїв в мережу потрібно буде виконати однакові налаштування.

У цій лекції ми познайомилися з операційною системою CISCO IOS, розглянули різні режими CISCO IOS і вивчили основну командну структуру для налаштування цієї ОС. Крім того, отримали загальне уявлення про початкові параметри комутатора CISCO IOS, у тому числі про призначення імені, обмеження доступу до конфігурації пристрою, налаштування і збереження конфігурації.

Питання для закріплення

1. Наведіть приклади мережевих ОС.
2. Які функції операційної системи IOS?
3. У чому полягає метод консольного доступу до мережевого пристрою?
4. Які ви знаєте методи віддаленого доступу до мережевого пристрою?
5. Які програми емуляції терміналу ви знаєте?
6. Які режими роботи операційної системи CISCO IOS ви заєте?
7. Яка структура команд операційної системи IOS?
8. Наведіть основні команди налаштування і перевірки мережевих пристроїв.

Список рекомендованої літератури

1. CCNA R&S ITN Chapter 2: // Електронний ресурс. Режим доступу: https://341565113.netacad.com/courses/479164/pages/launch-chapter-2
2. Cisco IOS Technologies // Електронний ресурс. Режим доступу: https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-technologies/index.html

3. Cisco IOS Command Modes // Електронний ресурс. Режим доступу: www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/configuration/guide/ffun_c/fcf019.html
4. Початкове налаштування комутатора Cisco Catalyst 2960 на базі Cisco IOS // Електронний ресурс. Режим доступу: supportforums.cisco.com/document/147811

Лекція 3. Тема: « Фізичний та канальний рівень»

План лекції

3.1. Правила передавання даних у мережі.
3.2. Логічна та фізична адреса.
3.3. Основні принципи та засоби передачі даних фізичного рівня.
3.4. Характеристики мідних кабелів.
3.5. Особливості прокладення оптоволоконних кабелів.
3.6. Особливості безпровідного середовища.
3.7. Канальний рівень.
3.8. Найбільш поширені фізичні топології глобальної мережі.

3.1. Правила передавання даних у мережі

Протоколи, що використовуються у мережі зв’язку, і протоколи, що управляють успішними процесами комунікації, мають загальні основні характеристики. Окрім вказівки адреси джерела і призначення, мережеві протоколи визначають спосіб передачі повідомлення через мережу. Основними етапами передавання повідомлення є наступні:

- кодування повідомлення;
- форматування та інкапсуляція повідомлення;
- розмір повідомлення;
- часові параметри повідомлення;
- параметри доставки повідомлення.

Кодування повідомлення – один з перших етапів відправки повідомлення. Це процес перетворення інформації у форму, прийнятну для наступної передачі. Декодування – зворотний процес, в результаті якого інформація перетвориться в початковий вид. Кодування даних при обміні між вузлами повинне відповідати середовищу зв’язку. Передусім вузол-

відправник перетворить повідомлення в біти. Кожен біт кодується набором звуків, світлових хвиль або електричних імпульсів залежно від типу мережі. Вузол призначення приймає і декодує сигнали та інтерпретує повідомлення.

Форматування і інкапсуляція повідомлення. При відправці повідомлення від джерела до одержувача необхідно використовувати певний формат або структуру. Формат залежить від типу повідомлення і каналу доставки. Подібно до того, як вкладається в конверт лист, інкапсулюються комп'ютерні повідомлення. Для інкапсуляції кожного повідомлення комп'ютера перед відправкою по мережі використовується особливий формат, який називається **кадром**. Кадр діє приблизно так само, як і конверт: в ньому вказані адреси початкового вузла і призначення. Формат і вміст кадру залежать від типу повідомлення і каналу передачі. Вузол призначення не може успішно отримати і обробити повідомлення, що невірно відформатували.

Розмір повідомлення – ще одне правило комунікації. При передачі довгого повідомлення від одного вузла до іншого по мережі повідомлення поділяється на частини. Розміри цих частин, або кадрів, строго регулюються, вони залежать від використовуваного каналу. Занадто довгі або короткі кадри не доставляються. Обмеження за розміром кадрів примушують початковий вузол ділити довгі повідомлення на частини, що відповідають вимогам до мінімального і максимального розміру. Цей метод називається **сегментацією.** Кожна частина інкапсулюється з інформацією про адресу в окремий кадр і потім передається по мережі. Вузол-адресат розпаковує повідомлення і збирає їх разом для обробки і інтерпретації.

Часові параметри повідомлення. На якість прийому та інтерпретації повідомлення впливає час. Розрахунок часу дозволяє людям визначити, коли почати розмову, наскільки швидко або повільно говорити і скільки часу чекати відповіді. Це правила підтримки контакту. Метод доступу визначає, коли конкретна людина зможе відправити повідомлення. Вибір часу залежить від середовища. Наприклад, в деяких випадках говорити можна у будь-який момент, коли є що сказати. У такому середовищі треба дочекатися, поки інші припинять розмову, а потім почати говорити. Якщо дві людини починають говорити одночасно, відбувається **інформаційна колізія**, і обом доводиться починати спочатку. Комп'ютерам теж необхідно вибирати метод доступу. Щоб дізнатися, коли почати відправку повідомлень і як реагувати на помилки, вузлам в мережі треба визначити метод доступу.

Часові параметри впливають також на кількість інформації, що відправляється, і швидкість доставки. При відправці даних по мережі вузол-відправник може передавати повідомлення швидше, ніж вузол призначення їх приймає і обробляє. Управління потоком дозволяє вузлу-джерелу і вузлу призначення погоджувати час для успішного зв'язку.

Тайм-аут відповіді означає, що якщо людина ставить питання і не отримує відповіді за прийнятний час, вона припускає, що відповіді не буде, і реагує відповідним чином. Для мережевих вузлів також існують правила, що визначають час очікування відповіді і дії, що виконуються після закінчення цього часу. У деяких випадках відправнику треба переконатися, що повідомлення доставлене успішно. Для цього одержувач повинен відправити підтвердження доставки. Якщо підтвердження не потрібно, метод доставки повідомлення називається **непідтвердженим.**

Вузли в мережі використовують різні варіанти доставки повідомлень.

Варіант доставки «один до одного» називається **одноадресним (unicast)**. Це означає, що у повідомлення є тільки один адресат.

Якщо вузол розсилає повідомлення методом «один до багатьох», це називається **багатоадресною або груповою розсилкою (multicast).** Багатоадресна розсилка передбачає одночасну відправку одного і того ж повідомлення групі вузлів.

Якщо усім мережевим вузлам необхідно отримати повідомлення в один і той же час, використовується **широкомовна розсилка (broadcast).** Широкомовна розсилка є методом доставки повідомлень «один до усіх». Крім того, для вузлів передбачені правила розсилки сполучень з підтвердженням і без підтвердження.

При передаванні даних по мережі вони розділяються на дрібніші і керовані частини для передачі по мережі (процес сегментації**).** Сегментація повідомлення надає дві основні переваги:

- шляхом відправки невеликих окремих частин від джерела до одержувача в мережі можна підтримувати багато різних обмінів, що чергуються; процес доставки з чергуванням частин окремих обмінів повідомленнями в мережі називається **мультиплексуванням**;
- сегментація може підвищити надійність мережевої взаємодії, окремі частини кожного повідомлення не обов'язково слідують по одному шляху в мережі від джерела до одержувача. Якщо певний шлях буде переповнений трафіком або мережеве устаткування вийде з ладу, окремі частини повідомлення можуть бути відправлені до місця призначення по іншому шляху. Якщо яку-небудь частину повідомлення не вдається доставити до місця призначення, необхідно буде повторно передати тільки відсутні компоненти.

Недолік використання сегментації і мультиплексування для передачі повідомлень через мережу – рівень складності, яка додається до усього процесу. Уявіть собі, що необхідно відправити лист з 100 сторінок, але кожен конверт вміщує тільки одну сторінку. Процес написання адрес, маркування, отримання і відкриття усіх 100 конвертів віднімає багато часу у відправника і одержувача.

У області комунікацій усі сегменти повідомлення повинні пройти подібний процес, щоб повідомлення було доставлене до потрібного місця призначення і могло бути зібране в правильний вміст початкового повідомлення.

Різні типи пристроїв в мережі беруть участь в забезпеченні надійної доставки усіх частин повідомлення в місце призначення.

У міру того, як дані додатків передаються по стеку протоколів на шляху до передачі по мережевому середовищу, різні протоколи додають в них інформацію на кожному з рівнів. Форма, яку приймає масив даних на кожному з рівнів, називається **протокольними блоками даних (PDU,** Protocol Data Unit**)**. В ході інкапсуляції кожен наступний рівень інкапсулює PDU, отриманий від вищестоячого рівня відповідно до використовуваного протоколу. На кожному етапі процесу PDU отримує інше ім'я для віддзеркалення нових функцій:

- **дані** - загальний термін для позначення PDU прикладного рівня;
- **сегмент** - PDU транспортного рівня;
- **пакет** - PDU мережевого рівня;
- **кадр** - PDU рівня каналу даних;
- **біти** - PDU фізичного рівня, використовуваний при фізичній передачі даних по середовищу передачі.

Інкапсуляція даних – процес, який додає до даних вміст заголовка додаткового протоколу перед передачею. У більшості форм передачі даних первинні дані піддаються інкапсуляції декількох протоколів до початку передачі.

При відправці повідомлення по мережі стек протоколів на вузлі працює від верхнього рівня до нижнього.

Деінкапсуляція – процес, який виконується приймальним пристроєм, щоб видалити один або декілька заголовків протоколів. Дані деінкапсулюються у міру просування по стеку до додатків для кінцевих користувачів. Модель взаємодії відкритих систем OSI описує процеси кодування, форматування, сегментації та інкапсуляції даних для передачі по мережі.

Мережевий і канальний рівні відповідають за надання даних від відправляючого пристрою, або джерела, до приймаючого пристрою, або пристрою призначення. Протоколи на обох рівнях утримують адреси джерела і призначення, які мають різні цілі.

3.2. Логічна та фізична адреса

Логічна адреса мережевого рівня (рівень 3) містить інформацію, необхідну для доставки IP -пакета між пристроями. IP -адреса рівня 3 має дві частини: префікс мережі і вузлову частину. Префікс мережі використовується маршрутизаторами, щоб передати пакет

у відповідну мережу. Вузлова частина використовується останнім маршрутизатором для доставки пакету до пристрою призначення.

IP -пакет містить дві IP -адреси:

- **IP-адресу джерела** – IP -адресу відправляючого пристрою;
- **IP-адресу призначення** – IP -адресу приймаючого пристрою. IP -адреса призначення використовується маршрутизаторами для передачі пакету до місця призначення.

Фізична адреса канального рівня (рівень 2) дозволяє доставляти кадр каналу передачі даних з одного мережевого інтерфейсу на інший в одній і тій же мережі. Перш ніж IP -пакет можна буде відправити по дротяній або безпровідній мережі, його необхідно інкапсулювати в кадр каналу передачі даних для наступної передачі по фізичному середовищу реальної мережі. Локальні мережі Ethernet і безпровідні локальні мережі – два приклади мереж з різними фізичними носіями, кожна з яких має власний тип протоколу канального рівня.

IP -пакет інкапсулюється в кадр каналу передачі даних для доставки в мережу призначення.

Адреси мережевого рівня, або IP -адреси, є мережевими адресами джерела і призначення. Мережева частина адреси буде єдиною; відрізнятися буде тільки частина адреси, що описує окремий вузол або пристрій.

Якщо відправник і одержувач IP -пакета знаходяться в одній і тій же мережі, кадр каналу передачі даних вирушає безпосередньо приймаючому пристрою. У мережі Ethernet адреса каналу передачі даних називається **MAC -адресою Ethernet.**

MAC -адреси є 48-бітовими адресами, які фізично вбудовані на мережевій інтерфейсній платі Ethernet. MAC -адреса також називається **фізичною або апаратною адресою (BIA,** Burned In Address**).**

На рис. 3.1. MAC -адресою джерела ПК1 з IP-адресою 192.168.1.110 є MAC -адреса мережевої інтерфейсної плати Ethernet (NIC) ПК1 : 0A - AA - AA - AA - AA - AA.

MAC -адресою призначення є MAC -адреса FTP –сервера (IP-адреса 192.168.1.9): 0C - CC - CC - CC - CC - CC. Адреси джерела і призначення додаються в кадр Ethernet. Тепер кадр з інкапсульованим IP -пакетом можна передавати з ПК1 відразу на FTP -сервер.

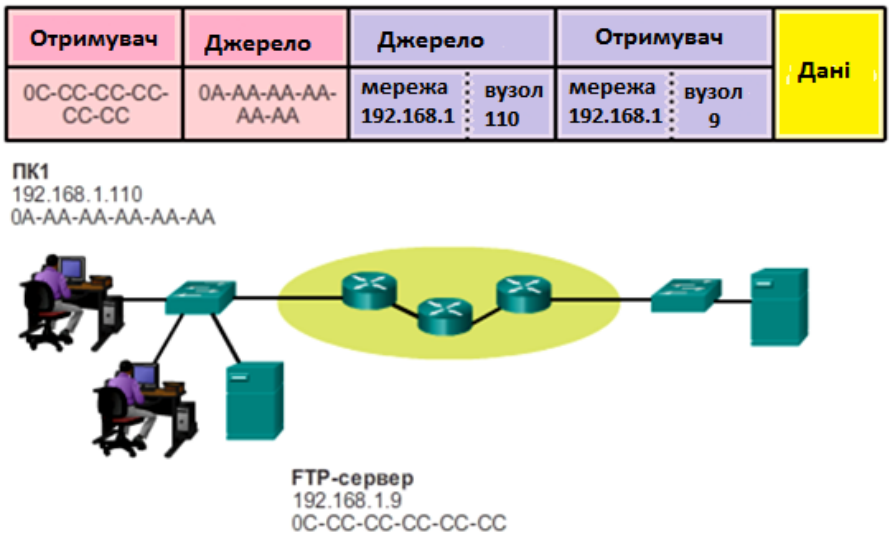


Рис. 3.1. Обмін даними в одній мережі ПК 1 з FTP-сервером [1]

Щоб відправити дані іншому вузлу в тій же локальній мережі, початковий вузол повинен знати фізичну і логічну адресу вузла призначення. Після цього він може створити кадр і відправити його по мережевому середовищу. Початковий вузол може упізнати IP -адресу призначення декількома способами. Наприклад, за допомогою Служби доменних імен (DNS, Domain Name System) або по тому, що адреса введена вручну (наприклад, якщо користувач вказує IP -адресу необхідного FTP -сервера). Але як вузол визначає MAC -адресу Ethernet іншого пристрою?

За допомогою IP -протокола, який називається **протоколом дозволу адрес (ARP,** Address Resolution Protocol), вузол визначає MAC -адресу будь-якого вузла в тій же локальній мережі. Передавальний вузол відправляє сполучення із запитом ARP по усій локальній мережі. ARP -запит є широкомовним повідомленням. ARP - запит містить IP -адресу пристрою призначення. Кожен пристрій у локальній мережі аналізує ARP - запит на предмет змісту своєї IP -адреси. Тільки пристрій з IP -адресою, представленою в ARP - запиті, повертає відповідь ARP. Відповідь ARP включає MAC-адресу, пов'язану з IP –адресою в ARP -запиті.

Метод, за допомогою якого вузол відправляє повідомлення адресата у віддалену мережу, відрізняється від методу відправки адресатові в тій же локальній мережі. При відправці вузлу, підключеному до тієї ж мережі, повідомлення спрямовується безпосередньо. Вузол за допомогою протоколу ARP визначає MAC -адресу вузла призначення. Він включає IP -адресу в заголовок пакету та інкапсулює пакет в кадр, де знаходиться MAC -адреса призначення, а потім передає його далі.

Якщо вузлу треба відправити повідомлення до віддаленої мережі, необхідно використовувати маршрутизатор, який також називається **шлюзом за замовчуванням.**

Шлюз за замовчуванням – це IP -адреса інтерфейсу маршрутизатора в тій же мережі, в якій знаходиться відправляючий вузол. Для кожного вузла в локальній мережі важливо правильно задати адресу шлюзу за замовчуванням. Якщо в налаштуваннях вузла TCP/IP адреса шлюзу за замовчуванням не вказана або вказана невірно, повідомлення, адресовані вузлам у віддалених мережах, доставлені не будуть.

3.3. Основні принципи та засоби передачі даних фізичного рівня

Мережеві інтерфейсні плати (NIC, network interface controller) служать для підключення пристрою до мережі. Мережеві інтерфейсні плати Ethernet використовуються для дротяного підключення, а мережеві інтерфейсні плати безпровідної локальної мережі – для безпровідного підключення. Пристрій кінцевого користувача може містити один або обидва типи інтерфейсних плат. Наприклад, мережевий принтер може бути оснащений тільки мережевою інтерфейсною платою Ethernet, тому йому необхідно підключатися до мережі за допомогою кабелю Ethernet. Інші пристрої, наприклад, планшетні ПК і смартфони, можуть бути оснащені тільки мережевою інтерфейсною платою безпровідної локальної мережі, при цьому потрібне використання безпровідного підключення.

Не усі фізичні з'єднання однакові з точки зору рівня продуктивності при підключенні до мережі. Наприклад, продуктивність безпровідного пристрою може знижуватися залежно від відстані до точки безпровідного доступу. Чим далі пристрій знаходиться від точки доступу, тим слабкіший сигнал, який вона отримує. Це може привести до зменшеної пропускної спроможності або втрати безпровідного підключення. Усі безпровідні пристрої повинні мати загальний доступ до радіоефіру точки безпровідного доступу. Це означає, що при одночасному підключенні великої кількості безпровідних пристроїв продуктивність мережі може знизитися. Дротяному пристрою не потрібний загальний доступ до мережі. Кожен дротяний пристрій має окремий канал зв'язку по окремих кабелях Ethernet. Це важливо при роботі з деякими додатками, наприклад з онлайн-іграми, потоковим відео і відеоконференціями, які вимагають вищої пропускної спроможності в порівнянні з іншими додатками.

Фізичний рівень OSI дозволяє передавати по мережевому середовищу біти, з яких складається кадр канального рівня. Цей рівень приймає увесь кадр від канального рівня і кодує його в серію сигналів, які передаються по локальному середовищу. Закодовані біти, з яких складається кадр, будуть отримані або крайовим, або проміжним пристроєм.

При переході від вузла джерела до вузла призначення дані піддаються наступному процесу (рис. 3.2).

- Дані для користувача розділяються на сегменти транспортним рівнем, розподіляються по пакетах мережевим рівнем, далі інкапсулюються в кадри канальним рівнем.
- Фізичний рівень кодує кадри і створює електричні, оптичні або радіохвилі, які представляють біти в кожному кадрі.
- Потім ці сигнали по черзі вирушають через середовище передачі даних.
- Фізичний рівень вузла призначення отримує ці окремі сигнали з середовища, відновлює їх до бітових представлень і передає біти до канального рівня у вигляді цілого кадру.

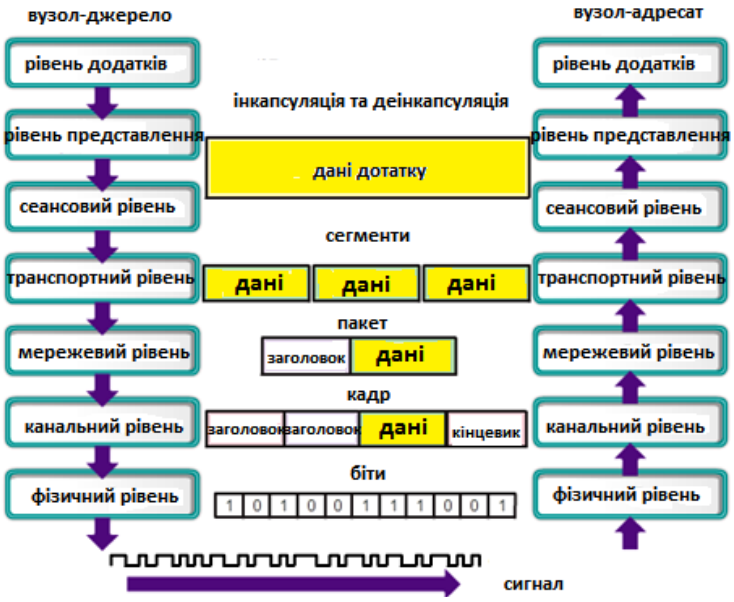


Рис. 3.2. Перетворення даних від джерела до адресата [1]

Існують три основні види середовищ передачі даних. Фізичний рівень створює представлення і групи бітів для кожного типу середовища, до яких відносяться наступні (рис. 3.3).

- **Мідний кабель:** сигнали є шаблонами електричних імпульсів.
- **Оптоволоконний кабель:** сигнали є світловими шаблонами.
- **Безпровідна мережа:** сигнали є шаблонами мікрохвильової передачі.

Для забезпечення функціональної сумісності на фізичному рівні усі аспекти цих функцій регламентуються організаціями по стандартизації.

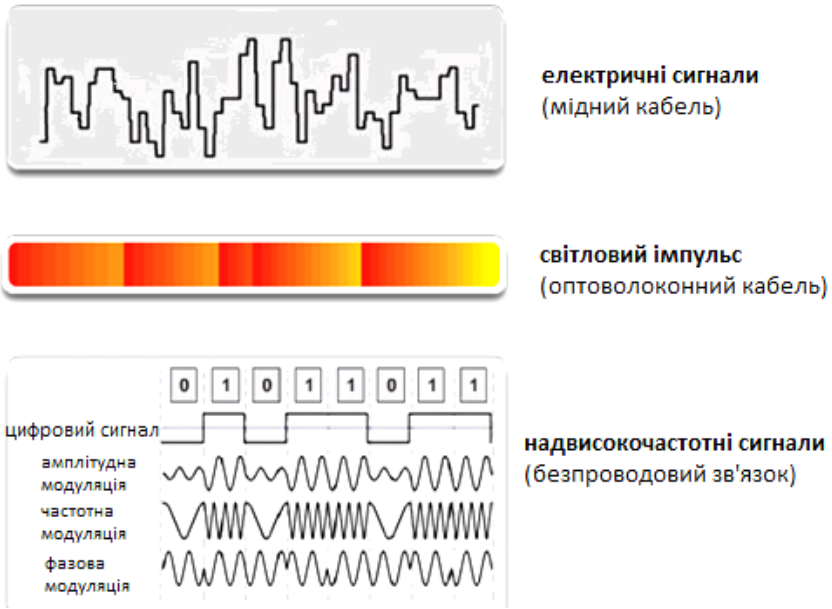


Рис. 3.3. Середовища передачі даних [1]

Фізичні компоненти мережі – це електронні апаратні пристрої, засоби передачі даних, а також інші блоки з'єднання, які передають і переносять сигнали для представлення бітів. Усі апаратні компоненти, такі як мережеві адаптери (NIC), інтерфейси і блоки з'єднання, кабельні матеріали і конструкції кабелів, вказані в стандартах, що відносяться до фізичного рівня.

Кодування або кодування каналу – це спосіб перетворення потоку біт в зумовлений «код». Коди – це групи біт, що використовуються для забезпечення заданого шаблону, який може розпізнати як одержувач, так і відправник. У мережі кодування визначається правилом зміни напруги або струму для представлення біт: нулів і одиниць. Різні фізичні середовища передачі даних підтримують різні швидкості передачі біт. Як правило, передача даних обговорюється з точки зору заявленої пропускної спроможності (bandwidth) і продуктивності (throughput).

Пропускна спроможність (bandwidth) – це здатність середовища передавати дані. Цифрова пропускна спроможність визначає об'єм даних, що передається з одного пункту в іншій за певний час. Зазвичай пропускна спроможність вимірюється в кілобітах в секунду (Кбіт/с) або мегабітах в секунду (Мбіт/с). Фактична пропускна спроможність мережі визначається сукупністю чинників:

- властивостями фізичного середовища;
- технологіями для передачі і виявлення сигналів в мережі.

Продуктивність (throughput) – це швидкість передачі бітів за вказаний проміжок часу. Через безліч чинників продуктивність (throughput) зазвичай не відповідає заявленій пропускній спроможності (bandwidth) в середовищах на фізичному рівні. На продуктивність (throughput) впливає ряд чинників, таких як об'єм та тип трафіку, час очікування, викликаний конфліктом декількох мережевих пристроїв між джерелом і призначенням.

Час очікування (latency) – це загальний час, який включає затримки (delays) для переміщення даних від однієї точки до іншої. При мережевій взаємодії або в мережі з декількома сегментами продуктивність (throughput) не може бути вища, ніж найповільніше з'єднання між джерелом і одержувачем. Навіть якщо усі або більшість сегментів мають високу заявлену пропускну спроможність (bandwidth), продуктивність усього каналу (throughput) визначається сегментом шляху з найнижчою продуктивністю, який створює вузьке місце для продуктивності усієї мережі.

3.4. Характеристики мідних кабелів

Мережі використовують мідні кабелі, тому що вони не вимагають великих витрат, зручні в установці і мають низький опір електричному струму. Проте мідні кабелі обмежені відстанню і перешкодами сигналу. Дані передаються по мідних кабелях у вигляді електричних імпульсів. Детектор в мережевому інтерфейсі цільового пристрою повинен отримати сигнал, який може бути легко розкодований для відповідності відправленому сигналу. Проте чим довше сигнал передається по мережі, тим швидше він затухає (attenuation – послаблення сигналу). Саме тому усе середовище передачі даних, засноване на мідному кабелі, повинне наслідувати строгі обмеження на відстані відповідно до стандартів. Значення розрахунку часу і напруги електричних імпульсів також залежать від двох аспектів. **Електромагнітні завади (ЕМЗ) або радіочастотні перешкоди (РЧП) -** сигнали ЕМЗ і РЧП можуть спотворювати і ушкоджувати сигнали даних, що передаються по мідному кабелю (рис. 3.4). Потенційні джерела ЕМЗ і РЧП включають радіохвилі і електромагнітні пристрої, наприклад, флуоресцентні лампи або електродвигуни**.**

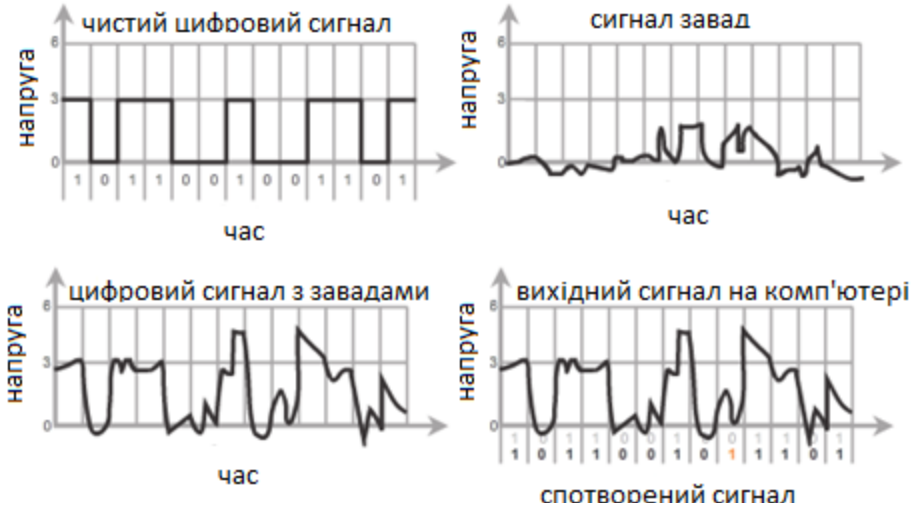


Рис. 3.4. Вплив завад на цифровий сигнал [1]

Перехресні перешкоди - це перешкоди, викликані електричними або магнітними полями сигналу на одному кабелі по відношенню до сигналу в суміжному кабелі. У телефонних каналах перешкоди можуть привести до того, що в одному каналі буде почута частина сторонньої розмови. Зокрема, коли електричний струм проходить через дріт, він створює невелике кругле магнітне поле навколо дроту, розмова на якому може бути почута на іншому дроті.

Для боротьби з небажаними наслідками ЕМЗ і РЧП деякі типи мідних кабелів обернуті в металевий захист і вимагають правильного заземляючого пристрою.

Для боротьби з небажаними наслідками перехресних перешкод деякі типи мідних кабелів мають дроти з протилежною течією струму перекручені між собою (говорять, що вони утворюють виту пару), що ефективно оберігає з'єднання від перешкод.

Опір мідних кабелів до електричного шуму може бути обмежений:

- вибором типу кабелю і категорії, відповідно до мережевого середовища;
- проектуванням інфраструктури кабелю для запобігання відомим і потенційним джерелам перешкод в структурі будівлі;
- використанням спеціальних методів прокладення кабелю.

У мережевих технологіях існують три основні типи мідних кабелів:

- неекранована вита пара (UTP);
- екранована вита пара (STP);
- коаксіальний кабель.

Ці кабелі використовуються для з'єднання вузлів в локальній мережі і пристроїв мережевої інфраструктури, таких як комутатори, маршрутизатори і точки безпровідного доступу. Кожен тип з'єднання і відповідні пристрої мають певні вимоги кабелів, передбачені стандартами фізичного рівня.

Кабель типу незахищена вита пара (UTP, Unshielded twisted pair**)** – найбільш поширене мережеве середовище. Кабелі UTP з роз'ємами RJ - 45 використовуються для зв'язку мережевих вузлів з проміжними мережевими пристроями, такими як комутатори і маршрутизатори. У локальних мережах кабель UTP складається з чотирьох пар дротів з кольоровою маркіровкою. Ці дроти перекручені між собою і захищені від невеликих фізичних ушкоджень гнучкою пластиковою оболонкою. Перекручення дротів захищає дроти від перешкод з боку інших дротів.

Кабелі на основі екранованої витої пари (STP, Shielded Twisted Pair **)** мають підвищений рівень захисту на відміну від кабелів на основі незахищеної витої пари (UTP). При цьому вони обходяться значно дорожче і складні в установці. Як і UTP, кабелі STP використовують роз'єм RJ - 45.

Кабелі типу захищена вита пара (STP) поєднують методи захисту від ЕМЗ і РЧП з перекрученням дротів. Більше того, такі кабелі мають бути оконцованы спеціальними захищеними роз'ємами STP.

Коаксіальний кабель називається так тому, що два провідники в нім використовують одну і ту ж вісь. Коаксіальний кабель складається з наступних елементів:

- мідний провідник для передачі електричних сигналів;
- мідний провідник, оточений ізоляцією з еластичного пластика;
- ізолюючий матеріал, оточений мідним обплетенням або металевою фольгою, який виступає другим дротом в каналі, а також екрану для внутрішнього провідника. Цей другий рівень, або екран, також знижує кількість зовнішніх електромагнітних завад.

Увесь кабель покритий кабельною оболонкою для захисту від невеликих фізичних ушкоджень. Усі три типи мідних засобів передачі вразливі до вогню і електричного струму. Загроза пожежі може виникнути через займистість кабельної ізоляції та екранів. При будівництві установ або організацій, можливо, потрібно буде обумовити стандарти безпеки для установки кабелів і відповідного устаткування.

Електричні характеристики мідних кабелів визначаються інститутом інженерів по електротехніці і електроніці (IEEE). IEEE класифікує кабелі незахищених витих пар (UTP) відповідно до продуктивності. Кабелі розділені на категорії відповідно до їх можливостей передачі на вищій швидкості. Наприклад, кабель категорії 5 (Cat5), як правило, використовується при установці FastEthernet 100BASE - TX. До інших категорій відносяться: розширений кабель категорії 5 (Cat 5e), категорії 6 (Cat6) і категорії 6a. Кабелі більше вищих категорій розроблені і сконструйовані для передачі даних на вищій швидкості. У міру розвитку і впровадження нових технологій Ethernet для гігабітних швидкостей передачі даних мінімально допустимим типом кабелів є Cat5e, а Cat6 рекомендується для прокладення нових мереж.

3.5. Особливості прокладення оптоволоконних кабелів

Оптоволоконні кабелі отримали велику популярність завдяки їх здатності об'єднувати мережеві пристрої інфраструктури. Їх застосування дозволяє передавати дані на великі відстані при вищій пропускній спроможності (швидкості передачі даних), ніж при використанні інших мережевих засобів передачі даних.

Оптичне волокно – це гнучкий, але дуже тонкий і прозорий кабель з чистого скла (кварцу) завтовшки з людську волосину. У оптоволоконному кабелі біти кодуються у вигляді світлових імпульсів. Оптоволоконний кабель діє як світлопровід, передаючи світло двома кінцями кабелю з мінімальною втратою сигналу.

На відміну від мідних дротів, оптоволоконний кабель може передавати сигнали при нижчому показнику послаблення, а також він абсолютно стійкий до дії електромагнітних і радіочастотних завад.

Нині оптоволоконні кабелі використовуються в чотирьох типах виробництва.

- **Корпоративні мережі.** Оптоволоконний кабель використовується для прокладення магістральної кабельної системи і зв'язку мережевих пристроїв, що реалізують інфраструктуру.
- **Технологія «оптоволокно до квартири» і мережі доступу.** Технологія «оптоволокно до квартири» (Fiber to the Home, FTTH) використовується для забезпечення постійного підключення мереж широкосмугового доступу для індивідуальних користувачів і невеликих підприємств. Технологія FTTH підтримує використання високошвидкісного доступу в Інтернет, а також дистанційної передачі даних, телемедицини та відео за запитом.
- **Мережі телекомунікацій.** Постачальники використовують наземні оптоволоконні мережі телекомунікацій для забезпечення міжнародного та міжміського з'єднання. Зазвичай ці мережі діють в діапазоні від декількох десятків до декількох тисяч кілометрів і підтримують швидкість до 10 Гбіт/с.

- **Підводні мережі.** Використовуються спеціальні оптоволоконні кабелі для забезпечення надійних високошвидкісних каналів з високою пропускною спроможністю, які здатні працювати у важких глибоководних умовах і пролягають через океани.

Хоча оптоволокно дуже тонке, воно складається з двох типів скла і захищене зовнішнім екраном. Зокрема, до компонент оптоволокна відносяться:

- **сердечник -** складається з прозорого скла і є частиною волокна, по якому проходить світло;
- **оболонка оптичного волокна -** скло, яке оточує серцевину і виступає дзеркалом. Світлові імпульси, які проходять по серцевині, відбиваються оболонкою. Завдяки цьому вони утримуються в серцевині волокна, будучи феноменом повного внутрішнього віддзеркалення.
- **Зовнішня оболонка -** як правило, виконана з полівінілхлориду (PVC), який захищає серцевину і оболонку кабелю. До складу оптоволокна також можуть входити зміцнюючі матеріали і буфер (обшивка), які захищають скло від подряпин і вологи.

Оптичне волокно пройшло ретельну виробничу перевірку. Було доведено, що оптоволокно витримує мінімум 20 тисяч кг на квадратний сантиметр. Оптичне волокно досить міцне, тому не ушкоджується під час установки і використання у важких природних умовах.

Світлові імпульси, які представляють дані у вигляді бітів в середовищі, генеруються за допомогою:

- лазерів;
- світловипромінюючих діодів;
- напівпровідникових пристроїв – фотодів, які визначають світлові імпульси і перетворять їх в електричні сигнали, які потім можуть бути перетворені в кадри даних.

Для швидкої і простої перевірки кабелю треба використовувати яскравий електричний ліхтар, направивши його в один кінець волокна і одночасно спостерігаючи за другим кінцем. Якщо світло видно, то волокно може передавати світло. Хоча така перевірка не вимірює продуктивність волокна, вона є швидким і недорогим способом виявити пошкоджене волокно.

Для перевірки оптоволоконних кабелів використовується оптичний тестер. Оптичний рефлектометр часової області (OTDR) можна використовувати для перевірки кожного сегменту оптоволоконного кабелю. Цей пристрій вводить тестовий імпульс світла в кабель, вимірюючи зворотне розсіювання і віддзеркалення світла залежно від проміжку часу. Оптичний рефлектометр розраховує приблизну відстань, на якій виявлені проблеми по усій довжині кабелю.

Використання оптоволоконних кабелів дає безліч переваг в порівнянні з мідними кабелями.

Оскільки волокна в оптоволоконному середовищі передачі даних не є провідниками струму, це середовище не схильне до електромагнітних завад і не проводить небажаний електричний струм завдяки заземленню. Оскільки оптичні волокна тонкі і відрізняються порівняно малою втратою сигналу, їх можна використовувати на набагато більших відстанях в порівнянні з мідним середовищем передачі даних, без необхідності відновлення сигналу. Деякі специфікації оптоволокна на фізичному рівні забезпечують передачу даних на декілька кілометрів.

Нині в більшості корпоративних середовищ для створення кабельної магістралі і забезпечення високошвидкісних з’єднань «точка-точка» між пристроями, а також для зв’язку в комплексі будівель переважно використовуються оптоволоконні кабелі. Оскільки оптоволоконний кабель не проводить електрику і відрізняється малою втратою сигналу, він оптимально підходить для таких цілей.

3.6. Особливості безпровідного середовища

На відміну від мідних і оптоволоконних кабелів, безпровідна мережа в якості мережевого середовища не обмежується провідниками або шляхами. Безпровідне середовище передачі даних характеризується найбільшою мобільністю. Крім того, кількість пристроїв безпровідного зв'язку постійно росте. Саме тому безпровідна мережа стала переважним середовищем для домашніх мереж. Також популярність безпровідних мереж швидко збільшується завдяки зростаючій пропускній спроможності мережі.

Проте безпровідна мережа має деякі проблемні області, до яких відносяться наступні.

- **Зона покриття.** Безпровідні технології передачі даних добре працюють у відкритих просторах. Проте деякі конструкційні матеріали, використовувані в будівлях і будовах, а також умови місцевості можуть обмежити зону покриття.
- **Перешкоди.** Безпровідна мережа сприйнятлива до перехресних перешкод, і її функціонування може бути порушене звичайними пристроями, наприклад, безпровідними телефонами, телевізійними приймачами, деякими типами флуоресцентних ламп, мікрохвильовими печами і іншими безпровідними комунікаціями.
- **Безпека.** Покриття безпровідного зв'язку не обмежується умовами доступу до середовища. Тому доступ до передачі можуть дістати неавторизовані користувачі і пристрої. Отже, засоби забезпечення мережевої безпеки є основною складовою адміністрування безпровідної мережі.

Телекомунікаційні і галузеві стандарти IEEE для безпровідної передачі даних покривають як канальний, так і фізичний рівні. До безпровідних мереж застосовано наступні три стандарти передачі даних.

- **Стандарт IEEE 802.11:** технологія безпровідних локальних мереж (WLAN), яка найчастіше називається Wi, - Fi, використовує конкуруючу або недетерміновану систему з множинним доступом (CSMA/CA).
- **Стандарт IEEE 802.15:** стандарт безпровідної персональної мережі, відоміший, як Bluetooth; для передачі даних на відстанях від 1 до 100 метрів вимагає близького розташування двох пристроїв.
- **Стандарт IEEE 802.16:** відоміший як протокол широкосмугового радіозв'язку (WiMAX); використовує топологію «точка-точка» для забезпечення безпровідного широкосмугового доступу.

У кожному з вказаних вище прикладів технічні характеристики фізичного рівня застосовані до наступних областей:

- кодування даних в радіосигнал;
- частота і потужність передачі;
- вимоги до прийому і декодування сигналу;
- проектування і структура антени.

Безпровідне з'єднання пристроїв до локальної мережі забезпечує безпровідну передачу даних. Зазвичай для встановлення безпровідної локальної мережі потрібні наступні мережеві пристрої.

- **Точка безпровідного доступу (AP,** Access Point**):** концентрує безпровідні сигнали від користувачів і за допомогою мідного кабелю підключається до наявної мережевої інфраструктури, наприклад, до Ethernet. Безпровідні маршрутизатори для будинку і малих підприємств поєднують функції маршрутизатора, комутатор і точки доступу в одному пристрої.
- **Безпровідні мережеві адаптери:** забезпечують безпровідний зв'язок для кожного мережевого вузла.

Переваги безпровідних технологій передачі даних очевидні, особливо відносно економії на дорогих дротах для приміщень і зручності мобільності вузла. Проте адміністраторам мережі необхідно розробляти і застосовувати суворі правила безпеки і процеси для захисту безпровідних локальних мереж від неавторизованого доступу і потенційного збитку.

З часом відбувається розвиток стандартів 802.11. Існують наступні стандарти.

- **IEEE 802.11a:** працює в частотному діапазоні від 5 ГГц і забезпечує швидкість до 54 Мбіт/с. Оскільки цей стандарт працює на вищих частотах, він має меншу зону покриття і менш ефективний усередині будівель. Пристрої, що працюють відповідно до цього стандарту, несумісні із стандартами 802.11b і 802.11g, описаними нижче.
- **IEEE 802.11b:** працює в частотному діапазоні від 2,4 ГГц і забезпечує швидкість до 11 Мбіт/с. Пристрої, що працюють відповідно до цих стандартів, мають більший діапазон і ефективніше працюють усередині будівель в порівнянні з пристроями стандарту 802.11a.
- **IEEE 802.11g:** працює в частотному діапазоні від 2,4 ГГц і забезпечує швидкість до 54 Мбіт/с. Пристрої, що працюють відповідно до аналогічного стандарту, працюють з тією ж радіочастотою і діапазоном, що і пристрої із стандартом 802.11b, але мають пропускну спроможність стандарту 802.11a.
- **IEEE 802.11n:** працює в частотних діапазонах 2,4 ГГц і 5 ГГц. Підтримує швидкість від 150 Мбіт/с до 600 Мбіт/с і працює в діапазоні до 70 метрів. Цей стандарт має зворотну сумісність з пристроями стандартів 802.11a/b/g.
- **IEEE 802.11ac:** працює в смузі частот 5 ГГц і забезпечує швидкість передачі даних від 450 Мбіт/с до 1,3 Гбіт/с (1300 Мбіт/с). Поєднаємо з колишніми версіями пристроїв 802.11a/n.
- **IEEE 802.11ad:** також називається «WiGig». Цей стандарт використовує зв'язок Wi - Fi з трьома частотними діапазонами: 2,4 ГГц, 5 ГГц і 60 ГГц, а також теоретично забезпечує швидкість передачі до 7 Гбіт/с.

У табл.3.1. виділені деякі відмінності стандартів 802.11.

Табл.3.1. Характеристики стандартів 802.11

Стандарт	Максимальна швидкість	Частота	Сумісність
802.11a	54 Мбіт/с	5 ГГц	нема
802.11b	11 Мбіт/с	2,4 ГГц	нема
802.11g	54 Мбіт/с	2,4 ГГц	802.11b
802.11n	600 Мбіт/с	2,4 ГГц або 5 Ггц	802.11a/b/g
802.11ac	1300 Мбіт/с (1,3 Гбіт/с)	2,4 ГГц і 5 Ггц	802.11a/n
802.11ad	7000 Мбіт/с (7 Гбіт/с)	2,4 ГГц, 5 Ггц і 60 ГГц	802.11a/b/g/n/ac

3.7. Канальний рівень

Канальний рівень відповідає за обмін кадрів між вузлами по фізичному середовищу. Він дозволяє верхнім рівням діставати доступ до середовища передачі даних, а також управляє способами розміщення і отримання даних в цьому середовищі.

Канальний рівень забезпечує два базові дві базові функції:

- приймає пакети рівня 3 і об'єднує їх в блоки даних, які називаються кадрами;
- контролює управління доступом до середовища і виконує виявлення помилок.

Канальний рівень ефективно приховує переходи пакету з одного середовища передачі даних в інше середовище від процесів на вищих рівнях мережевої моделі OSI. Канальний рівень отримує і відправляє пакети в протокол верхнього рівня. Протоколам верхнього рівня не вимагається знати, яке середовище використовуватиметься при передачі даних.

Канальний рівень ділиться на наступні два підрівні.

- **Управління логічним каналом (LLC,** Logical Link Control **):** це верхній підрівень, який визначає програмні процеси, що надають служби протоколам мережевого рівня. Він поміщає в кадрі інформацію, яка визначає, який протокол мережевого рівня використовується для цього кадру. Ця інформація дозволяє протоколам рівня 3, таким як IPv4 і IPv6, використовувати один і той же мережевий інтерфейс і один і той же засіб передачі даних.

- **Управління доступом до середовища передачі даних MAC:** це нижній підрівень, який визначає ключові процеси доступу до середовища передачі, що виконуються апаратним забезпеченням. Він забезпечує адресацію на канальному рівні і розподіл даних відповідно до фізичних вимог до сигналізації, а також тип використовуваного протоколу канального рівня.

Протоколи рівня 2 визначають інкапсуляцію пакету в кадр, а також методи отримання і відправки інкапсульованих пакетів по середовищах передачі даних. Технологія отримання і відправки кадру, називається **методом контролю доступу до середовища.**

При проходженні пакетів від вузла джерела до вузла призначення вони зазвичай проходять по різних фізичних мережах. Ці фізичні мережі можуть складатися з різних типів фізичних середовищ передачі даних, наприклад мідних і оптоволоконних кабелів, безпровідних мереж, що складаються з електромагнітних сигналів, радио- і мікрохвильових частот, а також супутникових каналів.

Пакети не мають прямого доступу до цих середовищ. Канальний рівень OSI готує пакети мережевого рівня для передачі і контролює доступ до фізичних середовищ. Способи управління доступом до середовища передачі даних, описані протоколами канального рівня, визначають процеси, за допомогою яких мережеві пристрої можуть дістати доступ до мережевого середовища і передавати кадри в різних мережевих середовищах.

Без канального рівня протоколи мережевого рівня, наприклад IP, повинні забезпечити з'єднання для кожного типу передавального середовища, які можуть знаходитися на шляху до тримання пакету. Більше того, протоколу IP необхідно кожного разу адаптуватися до нової мережевої технології або середовища. Цей процес утруднив би оновлення і розвиток мережевих середовищ передачі. Це головна причина використання багаторівневого підходу в мережі.

У рамках одного сеансу зв'язки можуть знадобитися різні методи управління доступом до середовища передачі даних. Кожне мережеве середовище, по якому проходять пакети впродовж передачі від локального до віддаленого вузла, може мати різні характеристики. Наприклад, локальна мережа Ethernet складається з безлічі вузлів, які борються за доступ до середовища передачі. Послідовні канали складаються з прямого підключення між двома пристроями, по яких слідують потоки даних у вигляді бітів.

Інтерфейси маршрутизатора інкапсулюють пакет у відповідний кадр. Для доступу до кожного каналу використовується відповідний спосіб контролю доступу до середовища передачі. У будь-якому обміні пакетами мережевого рівня може бути безліч переходів між канальним рівнем і середовищем. На кожному переході по дорозі маршрутизатор:

- приймає кадр від передавального середовища;
- деінкапсулює кадр;
- повторно інкапсулює пакет в новий кадр;
- передає новий кадр, який відповідає середовищу цього сегменту фізичної мережі.

Канальний рівень готує пакет для передачі по локальному середовищу передачі шляхом його інкапсуляції із заголовком і кінцевиком для створення кадру. Опис кадру – це ключовий елемент кожного протоколу канального рівня.

На відміну від інших протокольних блоків даних, кадр канального рівня складається з наступних елементів.

- **Заголовок:** містить контрольну інформацію (наприклад, адресація) і розташований на початку протокольного блоку даних.
- **Дані:** містить заголовок IP, заголовок транспортного рівня і дані.
- **Кінцевик:** містить контрольну інформацію для виявлення помилок, яка додана у кінці протокольного блоку даних.

Під час переміщення даних по середовищу передачі вони перетворяться в потік бітів, або одиниць і нулів. Якщо вузол отримує довгі потоки бітів, як він визначає кінець і початок кадру, а також які біти представляють адресу?

Кадрування ділить потік в групи, що піддаються розшифровці. Контрольна інформація поміщається в заголовку і кінцевику у вигляді значень у різних полях. Цей формат надає

фізичним сигналам структуру, яка може бути отримана вузлами і в місці призначення декодована в пакети.

Типи полів кадру складаються з наступних елементів.

- **Прапори початку і кінця кадру:** використовуються підрівнем MAC для визначення меж початку і кінця кадру.
- **Адресація:** використовується підрівнем MAC для визначення вузлів джерела і призначення.
- **Тип:** використовується управлінням логічного каналу для визначення протоколу рівня 3.
- **Управління:** визначає спеціальні служби управління потоком.
- **Дані:** містить корисне навантаження кадру (заголовок пакету, заголовок сегменту і дані).
- **Виявлення помилок :** розміщується після даних для створення кінцевика. Ці поля кадру використовуються для виявлення помилок.

Розміщення кадрів даних в середовищі контролюється підрівнем управління доступом до середовища передачі даних.

Протоколи канального рівня визначають правила доступу в різні середовища передачі даних. Деякі методи контролю доступу використовують ретельно відстежувані процеси для перевірки безпечного розміщення кадрів в середовищі. Ці методи задані складними протоколами, які вимагають механізми, що призводять до збільшення циркуляції службової інформації в мережі.

Серед різних варіантів реалізації протоколів канального рівня існують різноманітні способи управління доступом до такого середовища. Ці способи управління доступом до середовища визначають, чи використовують вузли це середовище спільно і яким чином це відбувається.

Вибір способу контролю доступу до середовища передачі залежить від наступних чинників.

- **Топологія**: як зв’язок між вузлами відображується для канального рівня.
- **Загальний доступ до середовища:** як здійснюється загальний доступ вузлів до середовища. Спільне використання середовища може здійснюватися з’єднанням «точка-точка», як в глобальній мережі, або може бути відкритий загальний доступ, як в локальних мережах.

3.8. Найбільш поширені фізичні топології глобальної мережі

Глобальні мережі часто підключені за допомогою наступних фізичних топологій.

- **Двоточкова топологія («точка-точка»):** це проста топологія, яка є постійним з’єднанням між двома кінцевими пристроями. Саме з цієї причини ця топологія найбільш поширена в глобальній мережі.
- **Топологія hub - and - spoke (зірка):** версія топології типу «зірка» для глобальної мережі, в якій центральний вузол підключає філії за допомогою двоточкових з’єднань.
- **Повнозв’язна (mesh) топологія:** ця топологія надає високу доступність, але вимагає, щоб кожна кінцева система була пов’язана з кожною іншою системою. Тому адміністративні і фізичні витрати можуть бути дуже значними. Кожен канал є двоточковим каналом для іншого вузла. Варіанти цієї топології включають сильносвязную (partial mesh) топологію, до якої підключені деякі, але не усі крайові пристрої.

Фізична двоточкова топологія («точка-точка»): двом вузлам не треба спільно використовувати одне середовище передачі з іншими вузлами. Крім того, вузлу не треба визначати, чи адресований вхідний кадр, саме для нього або адресований на інший вузол. Тому логічні протоколи канального рівня можуть бути дуже простими, тобто усі кадри в середовищі можуть бути спрямовані до двох вузлів або від них. Один вузол розміщує кадри на одному кінці, а інший вузол отримує ці кадри на іншому кінці двоточкового з’єднання.

Протоколи канального рівня можуть забезпечити складніші процеси управління доступом до середовища передачі даних для логічних двоточкових топологий, але це привело б до зайвих непродуктивних витрат протоколу.

Логічна топологія «точка-точка». Кінцеві вузли, що повідомляються по двоточковій мережі, можуть бути фізично підключені за допомогою декількох проміжних пристроїв. Проте використання фізичних пристроїв в мережі не впливає на логічну топологію.

Метод доступу до середовища визначається логічною двоточковою топологією, а не фізичною топологією. Це означає, що логічне двоточкове з'єднання між двома вузлами не обов'язково зв'язує два фізичні вузли на кожному кінці одного фізичного каналу зв'язку.

У двоточкових мережах дані передаються одним з двох наступних способів.

- **Напівдуплексна передача:** обидва пристрої можуть передавати і отримувати дані в середовищі, але не одночасно. Для вирішення конфліктів, що виникають у разі, коли відразу декілька станцій намагаються передати дані одночасно, в мережі Ethernet встановлені особливі правила.
- **Повнодуплексна передача:** обидва пристрої можуть одночасно передавати і отримувати дані в середовищі. На канальному рівні може відбуватися одночасна передача даних на обидва вузли. Тому на канальному рівні немає необхідності в особливих правилах.

Фізична топологія визначає, як фізично сполучені кінцеві системи. У локальних мережах з розподіленим середовищем передачі даних крайові пристрої можуть бути сполучені за допомогою наступних фізичних топологій.

- **Топологія типу «зірка»:** крайові пристрої підключаються до центрального проміжного пристрою. Колишні топології типу «зірка» сполучали крайові пристрої за допомогою концентраторів. Проте тепер в топологиях типу «зірка» використовуються комутатори. Топологія типу «зірка» – це найбільш поширена фізична топологія локальної мережі, головним чином тому, що вона проста в установці, модифікації (легко додавати і видаляти крайові пристрої) і зручна в усуненні неполадок.
- **Розширена зіркоподібна або гібридна.** У розширеній зіркоподібній топології центральні проміжні пристрої сполучають інші зіркоподібні топології. У гібридній топології зіркоподібні мережі можуть з'єднуватися з використанням топології шини.
- **Топологія шини:** усі кінцеві системи пов'язані один з одним загальною шиною (провідником, кабелем) і мають оконцовку на кінцях шини. Для з'єднання крайових пристроїв не потрібні комутатори. Шинні топології використовувалися в застарілих мережах Ethernet, оскільки були дешевими і легко встановлювалися.
- **Кільцева топологія:** кінцеві системи підключені до сусіднього вузла, формуючи зв'язок у формі кільця. На відміну від шинної топології, кільцева не вимагає оконцовки. Кільцеві топології використовувалися в застарілих мережах оптоволоконних ліній зв'язку (FDDI). Оптоволоконні лінії зв'язку (FDDI) використовують друге кільце для підвищення відмовостійкості і продуктивності.

На рис.3.5. показано, як крайові пристрої підключені в локальних мережах.

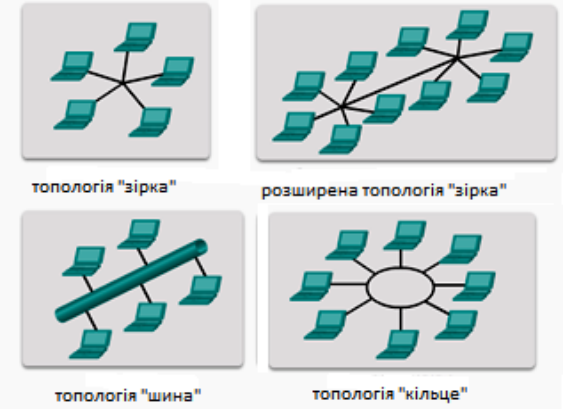


Рис. 3.5. Деякі фізичні топології мереж [1]

Для загального використання середовища існують два основні методи управління доступом.

- **Доступ на конкурентній основі (Contention - based access):** усі вузли конкурують за використання середовища, але мають особливий план дій у разі колізій.
- **Контрольований доступ (Controlled access):** кожен вузол використовує середовище в спеціально відведений час.

Протокол канального рівня визначає спосіб управління доступом до середовища передачі, що забезпечує необхідний баланс між управлінням кадром, захистом кадру і додатковими накладними витратами при передачі даних в мережі.

Асоціативний доступ. При використанні недетермінованого конкурентного методу мережевий пристрій може спробувати дістати доступ до середовища завжди, коли йому треба відправити дані. Для запобігання повній невпорядкованості в середовищі ці методи використовують процес множинного доступу з контролем несучої (**CSMA**, Carrier Sense Multiple Access), щоб спочатку виявити, чи передає середовище сигнал.

Якщо в середовищі виявлений сигнал несучої частоти, витікаючий від іншого вузла, це означає, що в даний момент інший пристрій здійснює передачу даних. Якщо середовище зайняте, коли пристрій намагається передати дані, воно почекає і спробує ще раз пізніше. Якщо сигнал несучої частоти, не виявлений, цей пристрій почне передачу даних. Конкурентний спосіб управління доступом до середовища передачі даних використовується безпровідними мережами і мережами Ethernet. Процес множинного доступу з контролем несучої (CSMA) може завершитися збоєм, через що два пристрої здійснюватимуть передачу одночасно, створюючи колізію даних. В цьому випадку дані, відправлені обома пристроями, будуть пошкоджені, через що знадобиться їх повторна відправка.

Конкурентні методи контролю доступу не мають яких-небудь додаткових механізмів контролю доступу. Механізм для відстежування черги доступу до середовища не потрібен. Проте асоціативні системи не відрізняються хорошою масштабованістю в умовах сильної завантаженості середовища. У міру збільшення інтенсивності навантаження і кількості вузлів знижується вірогідність дістати доступ до середовища без колізій. Крім того, пропускна спроможність середовища також зменшується, оскільки для виправлення помилок, викликаних такими колізіями, вимагається задіювати механізми відновлення.

Процес множинного доступу з контролем несучої (CSMA) зазвичай використовується спільно із способом вирішення конфліктів в середовищі. До двох найбільш широко поширеним методів відносяться наступні.

- **Множинний доступ з контролем несучої і виявленням колізій (CSMA/CD,** Carrier Sense Multiple Access with Collision Detection**):** крайовий пристрій відстежує сигнал даних в середовищі. Якщо сигнал даних не знайдений, і, отже, середовище вільне, той пристрій передає дані. Якщо пізніше виявляються сигнали про те, що в той же час передачу даних здійснював інший пристрій, передача даних на усіх пристроях уривається і переноситься на інший час. Цей метод використовується традиційними формами мереж Ethernet.
- **Множинний доступ з контролем несучої і запобіганням колізіям (CSMA/CA,** Carrier Sense Multiple Access With Collision Avoidance**):** крайовий пристрій вивчає сигнал даних в середовищі. Якщо середовище не завантажене, цей пристрій відправляє по середовищу повідомлення про намір використовувати її для передачі даних. Пристрій посилає дані після того, як середовище буде визнане незавантаженим. Цей спосіб використовується безпровідними мережевими технологіями стандарту 802.11.

Логічна топологія з множинним доступом дозволяє декільком вузлам обмінюватися інформацією один з одним за допомогою спільного доступу до середовища. Дані можуть бути розміщені в середовищі тільки з одного вузла одноразово. Кожен вузол бачить усі кадри в середовищі, але тільки той вузол, якому адресований кадр, обробляє вміст кадру.

Для контролю передачі даних і запобігання колізій між сигналами при підключенні до середовища відразу декількох вузлів потрібний метод контролю доступу до середовища передачі даних. При використанні контрольованого методу доступу мережеві пристрої

дістають доступ до середовища по черзі. Якщо крайовому пристрою не потрібен доступ до середовища, то можливість доступу переходить до наступного крайового пристрою. Цей процес здійснюється за допомогою маркера. Крайовий пристрій отримує маркер і розміщує кадр в середовищі. Жоден інший пристрій не має права виконувати цю дію до тих пір, поки кадр не буде отриманий і оброблений у вузлі призначення, після чого маркер буде знову доступний.

У логічній кільцевій топології кожен вузол у свою чергу отримує кадр. Якщо кадр не адресований вузлу, що отримав кадр, то цей вузол пересилає кадр наступному вузлу. Це дозволяє кільцевій мережі використовувати контрольований метод управління доступом до середовища передачі даних, який називається естафетною передачею.

Вузли в логічній кільцевій топології видаляють кадр з кільця, перевіряють адресу і відправляють його далі, якщо він адресований іншому вузлу. Усі вузли кільця перевіряють цей кадр (при пересилці між вузлом джерела і вузлом призначення по маршруту руху).

Існує багато методів управління доступом до середовища передачі даних, які можуть використовуватися з логічними кільцями залежно від необхідного рівня контролю. Наприклад, зазвичай одночасно по кільцю передається тільки один кадр. Якщо немає даних для передачі, то по кільцю по кругу передається порожній кадр (спеціальний сигнал), який називається маркером доступу. Вузол має право передавати дані, тільки якщо він отримав такий маркер.

Висновок до лекції 3

Рівень доступу до мережі на основі стеку протоколів TCP/IP еквівалентний канальному рівню OSI (рівень 2) і фізичному рівню (рівень 1). Фізичний рівень OSI дозволяє передавати по мережевому середовищу біти, з яких складається кадр канального рівня. Фізичні компоненти – це електронні апаратні пристрої, засоби передачі даних, а також інші блоки з'єднання, які передають і переносять сигнали для представлення бітів. Усі апаратні компоненти, такі як мережеві адаптери (NIC), інтерфейси і блоки з'єднання, кабельні матеріали і конструкції кабелів, вказані в стандартах, що відносяться до фізичного рівня. Стандарти фізичного рівня спрямовані на три функціональні області: фізичні компоненти, метод кодування кадру і спосіб передачі сигналів.

Використання відповідних засобів передачі даних є важливою частиною мережевої взаємодії. Без належного фізичного підключення, як дротяного, так і безпровідного, взаємодії між двома пристроями не станеться.

Дротяна взаємодія здійснюється за допомогою мідних і оптоволоконних кабелів. У мережах використовуються три основні типи мідних кабелі: незахищені виті пари (UTP), захищені виті пари (STP) і коаксіальний кабель. UTP -кабель – найбільш поширене середовище передачі даних на основі мідного дроту. Оптоволоконні кабелі отримали велику популярність завдяки їх здатності об'єднувати мережеві пристрої інфраструктури. Їх застосування дозволяє передавати дані на великі відстані при вищій пропускній спроможності (швидкості передачі даних), ніж при використанні інших мережевих засобів передачі даних. На відміну від мідних дротів, оптоволоконний кабель може передавати сигнали при нижчому показнику послаблення, а також він абсолютно стійкий до дії електромагнітних і радіочастотних завад.

За допомогою надвисоких частот безпровідні середовища передачі даних переносять електромагнітні сигнали, які представляють біти передаваної інформації. Кількість пристроїв безпровідного зв'язку продовжує збільшуватися. Саме тому безпровідна мережа стала пріоритетним середовищем для домашніх мереж і швидко набирає популярність в корпоративних мережах.

Канальний рівень відповідає за обмін кадрів між вузлами по фізичному мережевому середовищу. Він дозволяє верхнім рівням діставати доступ до середовища передачі даних, а також управляє способами розміщення і отримання даних в цьому середовищі.

Серед різних варіантів реалізації протоколів канального рівня існують різноманітні способи управління доступом до такого середовища. Ці способи управління доступом до середовища визначають, чи використовують вузли це середовище спільно і яким чином це відбувається. Вибір способу контролю доступу до середовища передачі залежить від топології і середовища. Топології локальної і глобальної мережі можуть бути фізичними або логічними. Саме логічна топологія впливає на тип мережевої синхронізації і використовуваний засіб управління доступом до середовища. Глобальні мережі зазвичай реалізуються за допомогою топологій типу «точка-точка» (point - to - point), «зірка» (hub - and - spoke) або повнозв'язній (mesh) топології. У спільно використовуваних локальних мережах крайові пристрої можуть бути сполучені за допомогою зіркоподібної, шини, кільцевої або гібридної (розширена зіркоподібна топологія) фізичних топологій.

Питання для закріплення

1. Які основні правила передавання даних у мережі?
2. Для чого використовується сегментація та мультиплексування даних?
3. Яке призначення одноадресної, багатоадресної та широкомовної розсилки?
4. Поясніть процеси інкапсуляції та деінкапсуляції.
5. Чим відрізняються логічна та фізична адреси?
6. Які основні принципи та засоби передачі даних фізичного рівня?
7. Які основні характеристики мідних кабелів?
8. Які особливості прокладення оптоволоконних кабелів?
9. Які особливості безпровідного середовища?
10. Назвіть найбільш поширені фізичні топології глобальної мережі.

Список рекомендованої літератури

1. CCNA R&S ITN Chapter 4: Network Access // Електронний ресурс. Режим доступу: http://static-course-assets.s3.amazonaws.com/IntroNet50ENU/module4/index.html
2. How Encapsulation Works Within the TCP/IP Model // Електронний ресурс. Режим доступу: http://learn-networking.com/tcp-ip/how-encapsulation-works-within-the-tcpip-model
3. Топології комп'ютерних мереж // Електронний ресурс. Режим доступу: http://comp-net.at.ua/index/topologija_komp_39_juternikh_merezh/0-6

Лекція № 4. Кодування інформації в локальних мережах

План лекції

4.1. Кодування з поверненням до нуля RZ.
4.2. Манчестерське кодування.
4.3. Кодування без повернення до нуля (NRZ).
4.4. Біфазний код.
4.5. Інші коди.
4.6. Аналогове кодування.
4.7. Методи передачі сигналу.
4.8. Типи модуляції сигналу.

4.1. Кодування з поверненням до нуля RZ

Кодування даних відбувається на фізичному рівні, також може створювати коди в цілях контролю, наприклад, для визначення початку і кінця кадру.

Інформація в кабельних локальних мережах передається в закодованому виді, тобто кожному біту передаваної інформації відповідає свій набір рівнів електричних сигналів в мережевому кабелі.

Модуляція високочастотних сигналів застосовується в основному в безкабельних мережах, в радіоканалах.

У кабельних мережах передача йде без модуляції або, як ще говорять, в основній смузі частот.

Правильний вибір коду дозволяє підвищити достовірність передачі інформації, збільшити швидкість передачі або понизити вимоги до вибору кабелю.

Наприклад, при різних кодах гранична швидкість передачі по одному і тому ж кабелю може відрізнятися в два рази. Від вибраного коду безпосередньо залежить також складність мережевої апаратури (вузли кодування і декодування коду).

Код повинен в ідеалі забезпечувати хорошу синхронізацію прийому, низький рівень помилок, роботу з будь-якою довжиною передаваних інформаційних послідовностей.

Деякі коди локальних мережах, показані на рис. 4.1.

Далі будуть розглянуті їх переваги і недоліки.

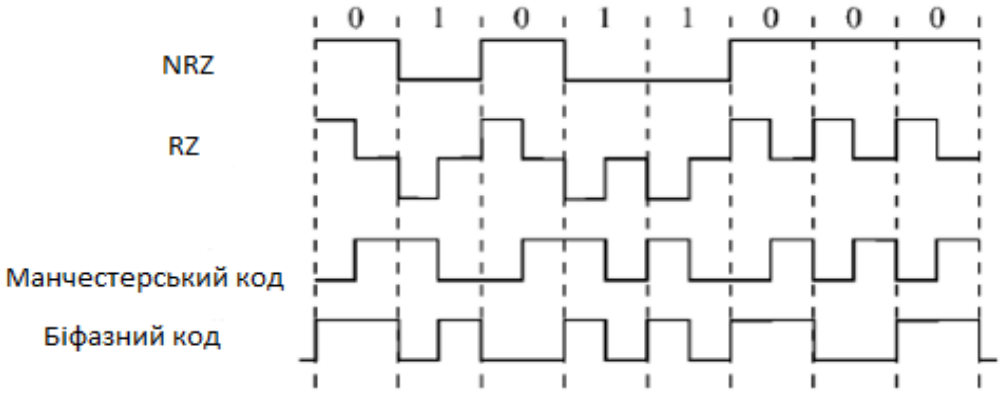


Рис. 4.1.Найбільш поширені коди передачі інформації

Код RZ (**Return to Zero** – з поверненням до нуля) – цей трирівневий код дістав таку назву тому, що після значущого рівня сигналу в першій половині бітового інтервалу слідує повернення до деякого «нульового», середнього рівня (наприклад, до нульового потенціалу). Перехід до нього відбувається в середині кожного бітового інтервалу. Логічному нулю, таким чином, відповідає позитивний імпульс, логічній одиниці – негативний (або навпаки) в першій половині бітового інтервалу.

У центрі бітового інтервалу завжди є перехід сигналу (позитивний або негативний), отже, з цього коду приймач легко може виділити синхроімпульс (строб). Можлива часова прив’язка не лише на початок пакету, як у разі коду NRZ, але і до кожного окремого біта, тому втрати синхронізації не станеться при будь-якій довжині пакету.

Ще одна важлива перевага коду RZ – проста часова прив’язка прийому, як на початок послідовності, так і до її кінця. Приймач просто повинен аналізувати, є зміна рівня сигналу впродовж бітового інтервалу або ні. Перший бітовий інтервал без зміни рівня сигналу відповідає закінченню послідовності біт, що приймається (рис.4.2). Тому в коді RZ можна використовувати передачу послідовностями змінної довжини.

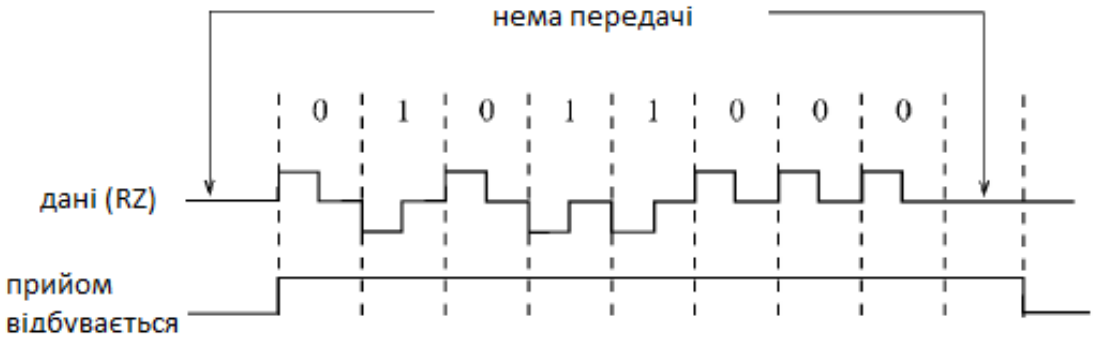


Рис. 4.2. Визначення початку і кінця прийому у коді RZ

Недолік коду RZ полягає в тому, що для нього потрібна удвічі більшу смуга пропускання каналу при тій же швидкості передачі в порівнянні з NRZ (оскільки тут на один бітовий інтервал доводиться дві зміни рівня сигналу). Наприклад, для швидкості передачі інформації 10 Мбіт/с потрібно пропускна спроможність лінії зв'язку 10 Мгц, а не 5 Мгц, як при коді NRZ (рис.4.3).

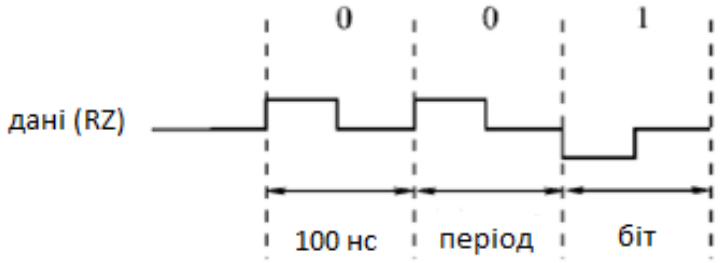


Рис.4.3. Швидкість передачі і пропускна спроможність при коді RZ

Інший важливий недолік – наявність трьох рівнів, що завжди ускладнює апаратуру як передавача, так і приймача. Код RZ застосовується не лише в мережах на основі електричного кабелю, але і в оптоволоконних мережах. Правда, в них не існує позитивних і негативних рівнів сигналу, тому використовується три наступні рівні: відсутність світла, «середнє» світло, «сильне» світло (рис. 4.4). Це дуже зручно: навіть коли немає передачі інформації, світло все одно є присутнім, що дозволяє легко визначити цілісність оптоволоконної лінії зв'язку без додаткових заходів.

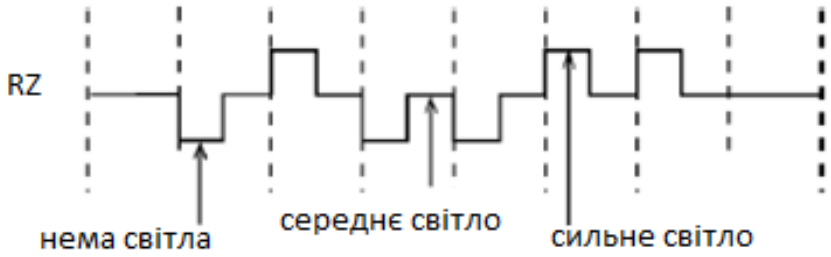


Рис.4.4. Використання коду RZ в оптоволоконних мережах

4.2. Манчестерське кодування

При манчестерському кодуванні нулі представлені переходом від високої до низької напруги; одиниці представлені переходом від низької до високої напруги. Цей тип кодування використовується в попередніх версіях Ethernet, RFID-пристроях і в технології Near Field Communication (NFC).

Манчестерський код є самосинхронізуючим, але на відміну від RZ має не три, а всього два рівні, що сприяє його кращій завадозахищеності і спрощенню приймальних і передавальних вузлів. Логічному нулю відповідає позитивний перехід в центрі бітового інтервалу (тобто

перша половина бітового інтервалу – низький рівень, друга половина – високий), а логічній одиниці відповідає негативний перехід в центрі бітового інтервалу (чи навпаки).

Як і в RZ, обов'язкова наявність переходу в центрі біта дозволяє приймачу манчестерського коду легко виділити з вхідного сигналу синхросигнал і передати інформацію скільки завгодно великими послідовностями без втрат через розсинхронізацію. Допустима розбіжність годинника приймача і передавача може досягати 25%.

Подібно до коду RZ, при використанні манчестерського коду потрібна пропускна спроможність лінії в два рази вища, ніж при застосуванні простого коду NRZ. Наприклад, для швидкості передачі 10 Мбіт/с потрібно смуга пропускання 10 Мгц (рис.4.5).

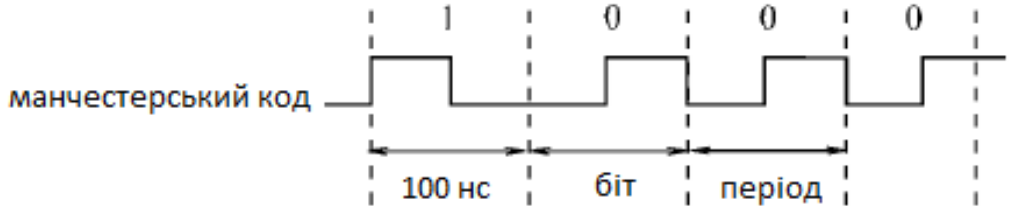


Рис. 4.5. Швидкість передачі і пропускна спроможність при манчестерському коді

Як і при коді RZ, в даному випадку приймач легко може визначити не лише початок передаваної послідовності біт, але і її кінець. Якщо впродовж бітового інтервалу немає переходу сигналу, то прийом закінчується. У манчестерському коді можна передавати послідовності біт змінної довжини (рис.4.6). Процес визначення часу передачі називають ще контролем несучої, хоча у явному вигляді несуча частота в даному випадку не присутня.

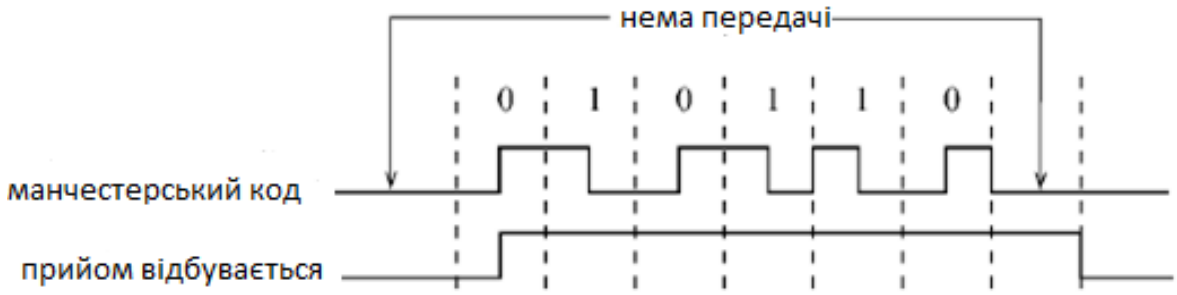


Рис. 4.6. Визначення початку і кінця прийому при манчестерському коді

Манчестерський код використовується як в електричних, так і в оптоволоконних кабелях (у останньому випадку один рівень відповідає відсутності світла, а інший – його наявності).

Основна перевага манчестерського коду – постійна складова в сигналі (половину часу сигнал має високий рівень, іншу половину – низький). Постійна складова дорівнює середньому значенню між двома рівнями сигналу.

Якщо високий рівень має позитивну величину, а низький – таку ж негативну, то постійна складова дорівнює нулю. Це дає можливість легко застосовувати для гальванічної розв'язки імпульсні трансформатори. При цьому не потрібне додаткове джерело живлення для лінії зв'язку, різко зменшується вплив низькочастотних перешкод, які не проходять через трансформатор, легко вирішується проблема узгодження.

Якщо ж один з рівнів сигналу в манчестерському коді нульовий (як, наприклад, в мережі Ethernet), то величина постійної складової впродовж передачі буде рівна приблизно половині амплітуди сигналу. Це дозволяє легко фіксувати зіткнення пакетів в мережі (конфлікт, колізію) за відхиленням величини постійної складової від встановлені межі.

Частотний спектр сигналу при манчестерському кодуванні включає тільки дві частоти: при швидкості передачі 10 Мбіт/с це 10 Мгц (відповідає передаваному ланцюжку з одних нулів або з одних одиниць) і 5 Мгц (відповідає послідовності з нулів, що чергуються, і одиниць: 1010101010..). Тому за допомогою простих смугових фільтрів можна легко позбавитися від усіх інших частот (перешкоди, наведення, шуми).

4.3. Кодування без повернення до нуля (NRZ)

Кодування без повернення до нуля NRZ (**Non Return to Zero** – без повернення до нуля) – це простий код, що є звичайним цифровим сигналом, поширений спосіб кодування даних, у якого є два стани, позначені «нулем» і «одиницею» без нейтрального або початкового положення. Нуль може бути представлений в середовищі передачі даних одним рівнем напруги; одиниці мають бути представлені іншим рівнем напруги.

Логічному нулю відповідає високий рівень напруги в кабелі, логічній одиниці – низький рівень напруги (чи навпаки, що не принципово). Рівні можуть бути різної полярності (позитивної і негативної) або ж однієї полярності. Впродовж бітового інтервалу (**bit time, BT**), тобто часу передачі одного біта ніяких змін рівня сигналу в кабелі не відбувається.

До безперечних достоїнств коду NRZ відносяться його досить проста реалізація (початковий сигнал не потрібно ні спеціально кодувати на передавальному кінці, ні декодувати на приймальному кінці), а також мінімальна серед інших кодів пропускна спроможність лінії зв'язку, потрібна пдля цієї швидкості передачі. Адже найбільш часта зміна сигналу в мережі буде при безперервному чергуванні одиниць і нулів, тобто при послідовності 1010101010.., тому при швидкості передачі 10 Мбіт/с (тривалість одного біта дорівнює 100 нс) частота зміни сигналу і, відповідно, необхідна пропускна спроможність лінії складе 1 / 200 нс = 5 Мгц (рис.4.7).

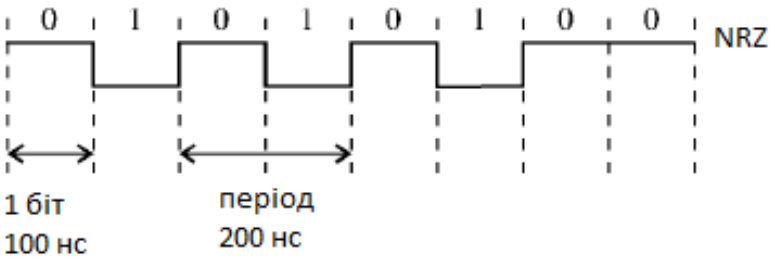


Рис. 4.7. Швидкість передачі і необхідна пропускна спроможність при коді NRZ

Найбільший недолік коду NRZ – це можливість втрати синхронізації приймачем під час прийому занадто довгих блоків (пакетів) інформації. Приймач може прив'язувати момент початку прийому тільки до першого (стартового) біта пакету, а впродовж прийому пакету він змушений користуватися тільки внутрішнім тактовим генератором (внутрішніми годинами). Наприклад, якщо передається послідовність нулів або послідовність одиниць, то приймач може визначити, де проходять межі бітових інтервалів, тільки по внутрішньому годиннику. І якщо годинник приймача розходиться з годинником передавача, то часове зрушення до кінця прийому пакету може перевищити тривалість одного або навіть декількох біт. В результаті станеться втрата переданих даних. Так, при довжині пакету в 10000 біт допустима розбіжність годинника складе не більше 0,01% навіть при ідеальній передачі форми сигналу по кабелю.

Для уникнення втрати синхронізації можна ввести другу лінію зв'язку для синхросигналу. Але при цьому необхідна кількість кабелю, число приймачів і передавачів збільшується в два рази. При великій довжині мережі і значній кількості абонентів це невигідно. У зв'язку з цим код NRZ використовується тільки для передачі короткими пакетами (зазвичай до 1 Кбіта).

Великий недолік коду NRZ полягає ще і в тому, що він може забезпечити обмін повідомленнями (послідовностями, пакетами) тільки фіксованої, заздалегідь обговореної довжини. За інформацією, що приймається, приймач не може визначити, чи йде ще передача або вже закінчилася. Для синхронізації початку прийому пакету використовується стартовий службовий біт, рівень якого відрізняється від пасивного стану лінії зв'язку (наприклад, пасивний стан лінії за відсутності передачі – 0, стартовий біт – 1). Закінчується прийом після відліку приймачем заданої кількості біт послідовності.

Найбільш відоме застосування коду NRZ – це стандарт RS232 - C, послідовний порт ПК. Передача інформації в ньому ведеться байтами (8 біт), що супроводжуються стартовим і стоповим бітами.

Три інші коди (RZ, манчестерський код, біфазний код) принципово відрізняються від NRZ тим, що сигнал має додаткові переходи (фронти) в межах бітового інтервалу. Це зроблено для того, щоб приймач міг підлаштовувати свій годинник під сигнал, що приймається, на кожному бітовому інтервалі. Відстежуючи фронти сигналів, приймач може точно синхронізувати прийом кожного біта. В результаті невеликі розбіжності годинника приймача і передавача вже не мають значення. Приймач може надійно приймати послідовності будь-якої довжини. Такі коди називаються самосинхронізуючими. Можна вважати, що самосинхронізуючі коди несуть в собі синхросигнал. Збільшення швидкості передачі даних вимагає складнішого кодування, наприклад, 4B/5B.

4.4. Біфазний код

Біфазний код часто розглядають як різновид манчестерського, оскільки їх характеристики практично повністю співпадають.

Цей код відрізняється від класичного манчестерського коду тим, що він не залежить від зміни місць двох дротів кабелю. Особливо це зручно у разі, коли для зв'язку застосовується вита пара, дроти якої легко переплутати. Цей код використовується в мережах Token - Ring компанії IBM.

Принцип цього коду простий: на початку кожного бітового інтервалу сигнал міняє рівень на протилежний попередньому, а в середині одиничних (і лише одиничних) бітових інтервалів рівень змінюється ще раз. Таким чином, на початку бітового інтервалу завжди є перехід, який використовується для самосинхронізації. Як і в разі класичного манчестерського коду, в частотному спектрі при цьому є присутньою дві частоти. При швидкості 10 Мбіт/с це частоти 10 Мгц (при послідовності одних одиниць: 11111111..) і 5 Мгц (при послідовності одних нулів: 00000000..).

Є також ще один варіант біфазного коду (його ще називають диференціальним манчестерським кодом). У цьому коді одиниці відповідає наявність переходу на початку бітового інтервалу, а нулю – відсутність переходу на початку бітового інтервалу (чи навпаки). При цьому в середині бітового інтервалу перехід є завжди, і саме він служить для побітової самосинхронізації приймача. Характеристики цього варіанту коду також повністю відповідають характеристикам манчестерського коду.

4.5. Інші коди

Усі коди, що розробляються останнім часом, покликані знайти компроміс між потрібною при заданій швидкості передачі смугою пропускання кабелю і можливістю самосинхронізації. Розробники прагнуть зберегти самосинхронізацію, але не ціною двократного збільшення смуги пропускання, як в розглянутих RZ, манчестерському і біфазному кодах.

Найчастіше для цього в потік передаваних бітів додають біти синхронізації. Наприклад, один біт синхронізації на 4, 5 або 6 інформаційних бітів або два біта синхронізації на 8 інформаційних бітів. Насправді кодування не зводиться до простої вставки в передавані даних додаткових бітів. Групи інформаційних бітів перетворяться в передавані по мережі групи з кількістю бітів на один або два більше. Приймач здійснює зворотне перетворення, відновлює початкові інформаційні біти. Досить просто здійснюється в цьому випадку і виявлення несучої частоти (детектування передачі).

Так, наприклад, в мережі FDDI (швидкість передачі 100 Мбіт/с) застосовується код 4B/5B, який 4 інформаційних біта перетворить в 5 передаваних бітів. При цьому синхронізація приймача здійснюється один раз на 4 біта, а не в кожному біті, як у разі манчестерського коду. Проте необхідна смуга пропускання збільшується у порівнянні з кодом NRZ не в два

рази, а лише в 1,25 разу (тобто складає не 100 Мгц, а усього лише 62,5 Мгц). За тим же принципом будуються інші коди, зокрема, 5B/6B, що використовується в стандартній мережі 100VG, AnyLAN, або 8B/10B, що використовується в мережі Gigabit Ethernet.

У сегменті 100BASE - T4 мережі Fast Ethernet використаний інший підхід. Там застосовується код 8B/6T, що передбачає паралельну передачу трьох трирівневих сигналів по трьох витих парах. Це дозволяє досягти швидкості передачі 100 Мбіт/с на дешевих кабелях з витими парами категорії 3, що мають смугу пропускання усього 16 Мгц. Правда, це вимагає більшої витрати кабелю і збільшення кількості приймачів і передавачів. До того ж принципово, щоб усі дроти були однієї довжини і затримки сигналу в них не занадто відрізнялися.

Іноді вже закодована інформація піддається додатковому кодуванню, що дозволяє спростити синхронізацію на приймальному кінці. Найбільшого поширення для цього набули 2-рівневий код NRZI, вживаний в оптоволоконних мережах (FDDI і 100BASE - FX), а також 3-рівневий код MLT - 3, використовуваний в мережах на витих парах (TPDDI і 100BASE - TX). Ці коди не є самосинхронізованими (рис. 4.8).

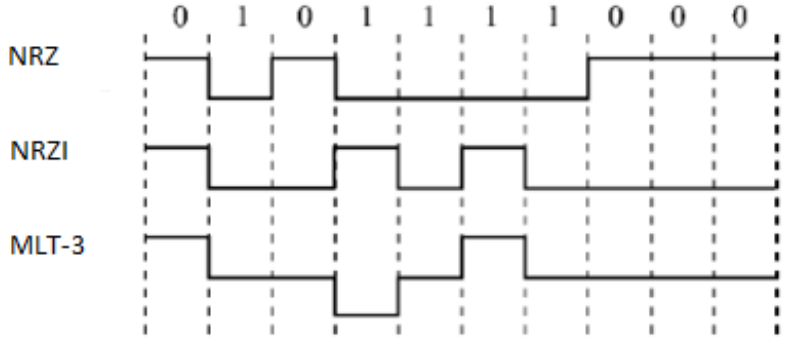


Рис. 4.8. Коди NRZI і MLT - 3

Код NRZI (без повернення до нуля з інверсією одиниць – **Non - Return to Zero, Invert to one**) припускає, що рівень сигналу змінюється на протилежний на початку одиничного бітового інтервалу і не змінюється при передачі нульового бітового інтервалу. При послідовності одиниць на межах бітових інтервалів є переходи, при послідовності нулів переходів немає. У цьому сенсі код NRZI краще синхронізується, ніж NRZ, оскільки там немає переходів ні при послідовності нулів, ні при послідовності одиниць.

Код MLT - 3 (**Multi - Level Transition - 3**) припускає, що при передачі нульового бітового інтервалу рівень сигналу не змінюється, а при передачі одиниці – змінюється на наступний рівень по такому ланцюжку: +U, 0, - U, 0, +U, 0, - U і так далі. Таким чином, максимальна частота зміни рівнів виходить вчетверо менше швидкості передачі в бітах (при послідовності суцільних одиниць). Необхідна смуга пропускання виявляється менше, ніж при коді NRZ.

Усі згадані коди передбачають безпосередню передачу в мережу цифрових двох- чи трирівневих прямокутних імпульсів.

4.6. Аналогове кодування

Проте іноді в мережах використовується і інший шлях – модуляція інформаційними імпульсами високочастотного аналогового сигналу (синусоїдального). Аналогове кодування дозволяє при переході на широкосмугову передачу істотно збільшити пропускну спроможність каналу зв’язку (в цьому випадку по мережі можна передавати декілька біт одночасно). До того ж, як вже відзначалося, при проходженні по каналу зв’язку аналогового синусоїдального сигналу не спотворюється форма сигналу, а тільки зменшується його амплітуда, а у разі цифрового сигналу форма сигналу спотворюється.

До найпростіших видів аналогового кодування відносяться амплітудна, частотна і фазова модуляція (рис.4.9) :

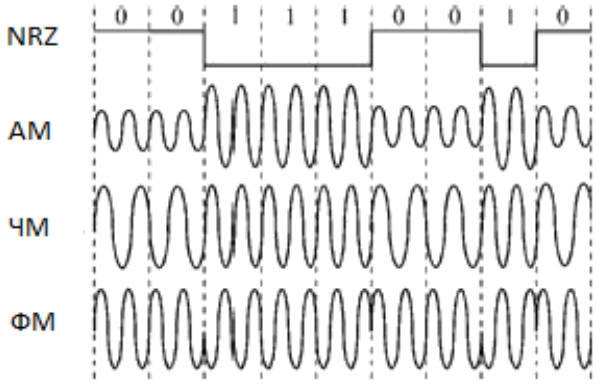


Рис. 4.9. Аналогове кодування цифрової інформації

4.7. Методи передачі сигналу

Фізичний рівень повинен створювати електричні, оптичні і безпровідні сигнали, які представляють в середовищі «1» і «0». Метод представлення бітів називається методом передачі сигналу. Стандарти фізичного рівня повинні визначати, який тип сигналу відповідає «1», а який тип відповідає «0». Це може бути просто зміною рівня напруги електричного сигналу або тривалості оптичного імпульсу. Наприклад, довгий імпульс може представляти 1, а короткий може представляти 0.

Це схоже на те, як використовується азбука Морзе для зв'язку. Азбука Морзе – один із способів передачі сигналів, який використовує звукові або світлові імпульси, кліки різної тривалості для відправки тексту по телефонних дротах або передачі сигналів між суднами в морі.

Сигнали передаються одним з двох способів.

- **Асинхронний:** сигнали передаються без відповідного тактового сигналу. Часові проміжки між символами або групами даних можуть бути довільними, тобто вони не мають стандартів. Тому для позначення початку і кінця кадру потрібні прапори.
- **Синхронний:** сигнали даних посилаються відповідно до тактового сигналу, який відміряє рівні проміжки часу, які називаються часом передачі біта.

4.8. Типи модуляції сигналу

Існує безліч способів передачі сигналів. Поширений метод відправки даних – із застосуванням технології модуляції.

Модуляція – це процес, при якому характеристика однієї хвилі (сигнал) змінює іншу хвилю (модульований сигнал). При передачі даних по середовищу поширені наступні методи модуляції.

Частотна модуляція (ЧМ): спосіб передачі, при якому несуча частота залежить від сигналу. Частотна модуляція (ЧМ, **FM – Frequency Modulation**), при якій логічній одиниці відповідає сигнал вищої частоти, а логічному нулю – сигнал нижчої частоти (чи навпаки). Амплітуда сигналу при частотній модуляції залишається постійною, що є великою перевагою в порівнянні з амплітудною модуляцією.

Амплітудна модуляція (АМ): спосіб передачі, при якому несуча амплітуда залежить від сигналу. Амплітудна модуляція (АМ, **AM – Amplitude Modulation**), при якій логічній одиниці відповідає наявність сигналу (або сигнал більшої амплітуди), а логічному нулю – відсутність сигналу (або сигнал меншої амплітуди). Частота сигналу при цьому залишається постійною. Недолік амплітудної модуляції полягає в тому, що АМ-сигнал сильно схильний до дії перешкод і шумів, а також пред'являє підвищені вимоги до загасання сигналу в каналі зв'язку. Переваги – простота апаратурної реалізації і вузький частотний спектр.

Фазова модуляція (ФМ, PM - Phase Modulation), при якій зміні логічного нуля на логічну одиницю і навпаки відповідає різка зміна фази синусоїдального сигналу однієї

частоти і амплітуди. Важливо, що амплітуда модульованого сигналу залишається постійною, як і у разі частотної модуляції.

Застосовуються і значно складніші методи модуляції, що є комбінацією перерахованих простих методів. Найчастіше аналогове кодування використовується при передачі інформації по каналу з вузькою смугою пропускання, наприклад, по телефонних лініях в глобальних мережах. Крім того, аналогове кодування застосовується в радіоканалах, що дозволяє забезпечувати зв'язок між багатьма користувачами одночасно. У локальних кабельних мережах аналогове кодування практично не використовується через високу складність і вартості як кодуючого, так і декодуючого устаткування.

Імпульсно-кодова модуляція (ІКМ): спосіб передачі, при якому аналоговий сигнал, наприклад голос, перетвориться в цифровий сигнал шляхом дискретизації амплітуди сигналу і вираженням амплітуд в двійковій системі. Частота дискретизації має бути як мінімум удвічі вище за максимальну частоту в спектрі сигналу.

Властивості фактичних сигналів, що представляють біти в середовищі передачі даних, залежатимуть від використовуваного способу передачі. Деякі із способів можуть використовувати один атрибут окремого сигналу для представлення нуля, а для представлення одиниці використовувати інший атрибут сигналу.

Висновок до лекції 4

Кодування даних відбувається на фізичному рівні, інформація в кабельних локальних мережах передається в закодованому виді, тобто кожному біту передаваної інформації відповідає свій набір рівнів електричних сигналів в мережевому кабелі. Модуляція високочастотних сигналів застосовується в основному в безкабельних мережах, в радіоканалах. У кабельних мережах передача йде без модуляції в основній смузі частот.

Правильний вибір коду дозволяє підвищити достовірність передачі інформації, збільшити швидкість передачі або понизити вимоги до вибору кабелю. Від вибраного коду безпосередньо залежить також складність мережевої апаратури (вузли кодування і декодування коду). Код повинен забезпечувати хорошу синхронізацію прийому, низький рівень помилок, роботу з будь-якою довжиною передаваних інформаційних послідовностей.

Найбільш поширеними методами кодування інформації в мережах передачі даних є манчестерське та біфазне кодування, коди RZ, NRZ та аналогове кодування, які мають свої переваги та недоліки. Усі коди, що розробляються, покликані знайти компроміс між потрібною при заданій швидкості передачі смугою пропускання кабелю і можливістю самосинхронізації. Розробники прагнуть зберегти самосинхронізацію, але не ціною двократного збільшення смуги пропускання, як в розглянутих RZ, манчестерському і біфазному кодах.

Питання для закріплення

1. На якому рівні моделі OSI відбувається кодування даних?
2. Поясніть процес кодування з поверненням до нуля RZ.
3. Поясніть принцип манчестерського кодування.
4. У чому полягає кодування без повернення до нуля (NRZ)?
5. Поясніть процес біфазного кодування.
6. У чому полягає аналогове кодування?
7. Які ви знаєте методи передачі сигналу?
8. Які типи модуляції сигналу ви знаєте?

Список рекомендованої літератури

1. Кодування сигналів // Електронний ресурс. Режим доступу: http://comp-net.at.ua/index/koduvannja_signaliv/0-20

2. Digital Communication Data Encoding Techniques // Електронний ресурс. Режим доступу: https://www.tutorialspoint.com/digital_communication/digital_communication_data_encoding_techniques.htm

3. Method of Unipolar Digital to Digital Encoding Data Transmission // Електронний ресурс. Режим доступу: http://www.sustech.edu/staff_publications/20140424053538550.pdf

Лекція 5. Тема: «Технології Ethernet»

План лекції

5.1. Підрівні канального рівня LLC і MAC.
5.2. Призначення і структура MAC-адреси.
5.3. Структура кадру Ethernet.
5.4. MAC і IP адреси.
5.5. Функції і принципи роботи роботи протоколу ARP.
5.6. Таблиця MAC -адрес комутатора.
5.7. Налаштування повнодуплексної та напівдуплексної передачі даних.
5.8. Порівняння комутації рівня 2 і рівня 3.

5.1. Підрівні канального рівня LLC і MAC

Фізичний рівень OSI дозволяє передавати по мережевому середовищу біти, з яких складається кадр канального рівня. На даний час Ethernet є основною у всьому світі технологією для локальних мереж. Ethernet функціонує на канальному і фізичному рівнях. Стандарти протоколів Ethernet визначають багато аспектів мережевого обміну даними, включаючи формат і розмір кадру, інтервал відправки і кодування. Коли підключені до мережі Ethernet вузли відправляють повідомлення, вони форматують їх відповідно до стандартів макету кадру (PDU).

Ethernet – це сімейство мережевих технологій, які регламентуються стандартами IEEE 802.2 і 802.3. Технологія Ethernet підтримує передачу даних на швидкостях:

- 10 Мбіт/с;
- 100 Мбіт/с;
- 1000 Мбіт/с (1 Гбіт/с);
- 10 000 Мбіт/с (10 Гбіт/с);
- 40 000 Мбіт/с (40 Гбіт/с);
- 100 000 Мбіт/с (100 Гбіт/с).

Стандарти Ethernet регламентують як протоколи рівня 2, так і технології рівня 1 OSI. Для протоколів другого рівня, як і у випадку з усіма стандартами групи IEEE 802, технологія Ethernet покладається на роботу цих двох окремих підрівнів канального рівня, а також на підрівні управління логічним каналом LLC і MAC.

Підрівень LLC (Logical Link Control**)** технології Ethernet забезпечує зв'язок між верхніми і нижніми рівнями. Як правило, це відбувається між мережевим ПЗ і апаратним забезпеченням пристрою. Підрівень LLC використовує дані мережевих протоколів, які зазвичай представлені у вигляді пакету IPv4, і додає управляючу інформацію, щоб допомогти доставити пакет до вузла призначення. LLC використовується для зв'язку з

верхніми рівнями застосувань і переміщає пакет для доставки на нижні рівні. LLC реалізований в ПЗ, і його застосування не залежить від устаткування. LLC для комп'ютера можна розглядати як ПЗ драйвера мережевої плати (NIC). Драйвер мережевої плати – це програма, яка безпосередньо взаємодіє з апаратними засобами комп'ютера на мережевій інтерфейсній платі для передачі даних між підрівнем MAC і фізичним середовищем.

Підрівень MAC (Media Access Control**)** є нижчим підрівнем канального рівня. MAC реалізується апаратно – зазвичай в мережевій інтерфейсній платі комп'ютера. Специфікації містяться в стандартах IEEE 802.3.

Підрівень MAC Ethernet виконує два основні завдання:

- інкапсуляція даних;
- управління доступом до середовища передачі даних.

Процес інкапсуляції даних включає зборку кадру перед його відправкою і розбирання кадру після його отримання. При формуванні кадру на рівні MAC до PDU мережевого рівня додаються заголовок і кінцевик.

Інкапсуляція даних забезпечує три основні функції.

- **Розподіл кадру.** Процес формування кадрів надає важливі роздільники, які використовуються для визначення групи бітів, що становлять кадр. Цей процес забезпечує синхронізацію між передавальними і одержуючими вузлами.
- **Адресація.** Процес інкапсуляції також забезпечує адресацію канального рівня. Кожен заголовок Ethernet, що додається в кадр, містить фізичну адресу (MAC -адресу), за допомогою якої кадр доставляється до вузла призначення.
- **Виявлення помилок.** Кожен кадр Ethernet містить кінцевик з циклічним контролем надмірності (CRC, Cyclic redundancy check) утримуваного кадру. Після прийому кадру одержуючий вузол створює CRC для порівняння з аналогічним параметром в кадрі. Якщо ці два розрахунки CRC співпадають, кадр може вважатися отриманим без помилок.

Використання кадрів допомагає при передачі бітів, оскільки вони поміщаються в середовище передачі даних, а також при групуванні бітів на приймаючому вузлі.

Другою функцією підрівня MAC є управління доступом до середовища передачі даних. Управління доступом до середовища передачі даних відповідає за розміщення кадрів в цьому середовищі і видалення з неї кадрів. Ця функція дозволяє управляти доступом до середовища передачі даних. Цей підрівень безпосередньо взаємодіє з фізичним рівнем.

Основна логічна топологія Ethernet – це шина з множинним доступом; отже, середовище передачі даних використовується усіма вузлами (пристроями) в одному сегменті мережі.

Ethernet – це спосіб асоціативного доступу організації мережі.

Метод асоціативного доступу (недетермінований метод) означає, що будь-який пристрій може постійно робити спробу передати дані в загальному середовищі за наявності у нього таких даних для відправки. При цьому якщо декілька пристроїв в одному середовищі почнуть разом передавати інформацію (подібно до того, як дві людини спробують розмовляти одночасно), то виникне конфлікт при передачі даних, який приведе до їх ушкодження і неможливості подальшого використання. Щоб не допустити подібної ситуації, Ethernet задіює метод множинного доступу з контролем несучої (CSMA) для управління загальним доступом вузлів.

Процес CSMA використовується для того, щоб спочатку визначити, чи передається сигнал в середовищі. Якщо в середовищі виявлений сигнал несучої частоти, витікаючий від іншого вузла, це означає, що в даний момент інший пристрій здійснює передачу даних. Якщо середовище зайняте, коли пристрій намагається передати дані, воно почекає і спробує ще раз пізніше. Якщо сигнал несучої частоти, не виявлений, цей пристрій почне передачу даних. Існує вірогідність виникнення збою процесу CSMA, внаслідок чого два пристрої передаватимуть дані одночасно. Це називається **колізією даних.** В цьому випадку дані, відправлені обома пристроями, будуть пошкоджені, через що знадобиться їх повторна відправка.

Способи контролю доступу до середовища передачі на основі асоціативного доступу не вимагають наявності механізмів для відстежування черговості доступу до середовища; отже, вони не мають навантаження на ресурси, властивого способам контрольованого доступу. Проте асоціативні системи не відрізняються хорошою масштабованістю в умовах сильної завантаженості середовища. У міру збільшення інтенсивності навантаження і кількості вузлів знижується вірогідність дістати доступ до середовища без колізій. Крім того, пропускна спроможність середовища також зменшується, оскільки для виправлення помилок, викликаних такими колізіями, вимагається задіювати механізми відновлення.

При **виявленні колізій CSMA (CSMA/CD)** пристрій перевіряє середовище на наявність в ньому сигналу даних. Якщо цей сигнал відсутній, вказуючи на те, що середовище передачі не завантажене, пристрій передає дані. Якщо пізніше виявляються сигнали про те, що в той же час передачу даних здійснював інший пристрій, передача даних на усіх пристроях обривається і переноситься на інший час.

У сучасних мережах широке застосування технологій комутації дозволило практично повністю виключити первинну потребу в CSMA/CD для локальних мереж. Майже усі дротяні з'єднання між пристроями в сучасних локальних мережах є повнодуплексними, тобто пристрої можуть одночасно відправляти і приймати дані. Це означає, що, не дивлячись на те, що мережі Ethernet розроблялися з урахуванням використання технології CSMA/CD, сучасні проміжні пристрої дозволяють усунути колізії, і процеси CSMA/CD вже не вимагаються.

Проте, для безпровідних з'єднань в середовищі локальної мережі можливість виникнення таких колізій все ще необхідно враховувати. Пристрої в безпровідній локальній мережі використовують метод доступу до середовища передачі даних з **контролем несучої і запобіганням колізіям (CSMA/CA).** При використанні CSMA/CA пристрій перевіряє середовище передачі даних на наявність в ньому сигналу даних. Якщо середовище не завантажене, цей пристрій відправляє по середовищу повідомлення про намір використовувати його для передачі даних. Потім пристрій відправляє дані. Цей спосіб використовується безпровідними мережевими технологіями стандарту 802.11.

5.2. Призначення і структура MAC-адреси

Як вже згадувалося раніше, основна логічна топологія Ethernet – це шина з множинним доступом. Кожен мережевий пристрій підключений до одного і того ж загального середовища передачі даних, і усі вузли отримують усі передавані кадри. Проблема полягає в тому, що якщо усі пристрої приймають усі кадри, як кожен окремий пристрій може визначити, чи являється він запланованим одержувачем, без додаткової необхідності в обробці і декапсуляції кадру для досягнення IP -адреси? Ситуація ускладнюється ще більше у великих мережах з великим об'ємом трафіку, в яких пересилається значна кількість кадрів.

Для запобігання надмірних навантажень, що виникають при обробці кожного кадру, був створений унікальний ідентифікатор – MAC -адреса, яка використовується для визначення фактичних вузлів джерела і призначення в межах мережі Ethernet. Незалежно від типу використовуваної мережі Ethernet MAC -адресація забезпечила метод ідентифікації пристроїв на нижчому рівні моделі OSI. **MAC -адреса Ethernet** – це 48-бітове двійкове значення, виражене у вигляді 12 шістнадцятиричних чисел (4 біта для кожної шістнадцятиричної цифри).

MAC -адреси мають бути унікальними в глобальному масштабі. Значення MAC -адреси – це безпосередній результат застосування правил, які розроблені інститутом IEEE для постачальників, щоб забезпечити глобальні унікальні адреси для кожного пристрою Ethernet. Відповідно до цих правил кожен постачальник, який займається реалізацією Ethernet -пристроїв, має бути зареєстрований в IEEE. IEEE привласнює постачальникові 3-байтний (24-бітовий) код, який називається **унікальним ідентифікатором організації (OUI,** organizationally unique identifier**).**

Інститут IEEE вимагає від постачальників дотримання двох простих правил:

1. усі MAC -адреси, що призначаються мережевій інтерфейсній платі або іншому пристрою Ethernet, повинні в обов'язковому порядку використовувати цей ідентифікатор OUI постачальника у вигляді перших 3 байтів;

2. усім MAC -адресам з одним і тим же ідентифікатором OUI має бути присвоєне унікальне значення (код виробника або серійний номер), яке вказується у вигляді останніх 3 байтів.

MAC -адресу часто називають **апаратною адресою (BIA)**, оскільки історично склалося так, що він записується в ПЗП (постійний запам'ятовуючий пристрій) на мережевій інтерфейсній платі. Це означає, що адреса вноситься в чіп ПЗП на апаратному рівні, і його зміна за допомогою ПЗ неможлива.

Примітка. Операційні системи і мережеві плати сучасних ПК підтримують можливість зміни MAC -адреси з використанням спеціальних програм. Це зручно при спробі діставання доступу до мережі, в якій використовується фільтрація на основі BIA; тобто фільтрація або відстежування трафіку на основі MAC -адреси більше не являється надійним способом.

MAC -адреси привласнюються робочим станціям, серверам, принтерам, комутаторам і маршрутизаторам – будь-якому пристрою, який повинен відправляти або отримувати дані в мережі. Усі пристрої, підключені до локальної мережі Ethernet, мають інтерфейси з використанням MAC -адрес. Різні виробники устаткування і ПЗ можуть представляти MAC -адресу в різних шістнадцятиричних форматах. Приклади форматів адрес:

- 00-000-05-9A-3C-78-00
- 0000:05:9 A :3 C :78:00
- 0000005.9A3C.7800

При запуску комп'ютера мережева плата спочатку копіює MAC -адресу з ПЗП в ОЗП. Якщо пристрій пересилає повідомлення в мережу Ethernet, він додає до пакету інформацію заголовка. Інформація заголовка містить MAC -адреси джерела і призначення. Початковий пристрій відправляє дані по мережі.

Кожна мережева плата в мережі переглядає інформацію (на підрівні MAC), щоб дізнатися, чи відповідає MAC -адреса призначення в кадрі MAC -адресі фізичного пристрою в ОЗП. Якщо не вдається виявити збіги, пристрій відхиляє кадр. Коли кадр досягає призначення, в якому MAC -адреса мережевої плати відповідає MAC -адресі одержувача кадру, мережева плата передає кадр на верхні рівні OSI, де відбувається процес деінкапсуляції.

5.3. Структура кадру Ethernet

На канальному рівні структура кадру практично ідентична для усіх швидкостей Ethernet. Структура кадру Ethernet додає заголовки і кінцевики PDU третього рівня для наступної інкапсуляції повідомлення, що відправляється.

Як заголовок, так і кінцевик Ethernet мають декілька розділів інформації, які використовуються протоколом Ethernet. Кожен розділ кадру називається полем. Існують два стилі формування кадрів Ethernet :

- стандарт Ethernet IEEE 802.3, який кілька разів оновлювався відповідно до нових технологій;
- стандарт Ethernet DIX, який тепер називається Ethernet II.

Відмінності між стилями формування кадрів мінімальні. Найбільш суттєвою відмінністю між цими двома стандартами є додавання в стандарті 802.3 начала роздільника кадру (SFD) і зміна поля «Тип» на полі «Довжина».

Ethernet II - це формат кадру Ethernet, використовуваний в мережах TCP/IP.

Основними полями кадру Ethernet є наступні (табл.5.1).

Табл. 5.1. Поля кадру Ethernet (IEEE 802.3)

Поле	Преамбула	Початок роздільника кадру	MAC-адреса призначення	MAC-адреса джерела	Довжина	Дані	Контрольна послідовність кадру
Кількість байт	7	1	6	6	2	46-1500	4

- **Поля «Преамбула» і «Початок роздільника кадру».** Поля «Преамбула» (7 байт) і «Початок роздільника кадру (SFD)», або «Початок кадру» (1 байт), використовуються для синхронізації відправляючих і одержуючих пристроїв. Ці перші 8 байт кадру потрібні для привертання уваги одержуючих вузлів. Перші декілька байт повідомляють одержувачам про необхідність приготуватися до вступу нового кадру.
- **Поле «MAC-адреса призначення».** Це поле (6 байт) є ідентифікатором для передбачуваного одержувача. Ця адреса використовується рівнем 2, щоб допомогти пристроям визначити, чи адресований кадр саме їм. Адреса в кадрі порівнюється з MAC - адресою в пристрої. У разі збігу пристрій приймає кадр.
- **Поле «MAC-адреса джерела».** Це поле (6 байт) визначає мережеву плату або інтерфейс пристрою, що відправив кадр.
- **Поле «Довжина».** У будь-якому стандарті IEEE 802.3, використовуваному до 1997 року, поле «Довжина» визначає точну довжину поля даних кадру. Пізніше воно використовується як частина контрольної послідовності кадру (FCS), щоб забезпечити правильність отримання повідомлення. У інших випадках це поле використовується, щоб описувати, який протокол більш високого рівня є присутнім. Якщо 2-октетне значення рівне або перевищує шістнадцятковий формат 0x0600 або десяткове число 1536, то вміст поля «Дані» декодується відповідно до вказаного протоколу EtherType. Якщо ж значення рівне або менше шістнадцятиричного формату 0x05DC або десяткового числа 1500, то поле «Довжина» дозволяє позначити використання формату кадру IEEE 802.3. Ось таким чином розрізняються кадри Ethernet II і 802.3.
- **Поле «Дані».** Це поле (46-1500 байт) містить інкапсульовані дані з більше високого рівня, який являється універсальним PDU рівня 3, або пакетом IPv4. Довжина усіх кадрів має бути не менше 64 байт. У разі інкапсуляції невеликого пакету використовуються додаткові біти, які називаються символами-заповнювачами, для збільшення розміру кадру до цього мінімального значення.
- **Поле «Контрольна послідовність кадру».** Поле «Контрольна послідовність кадру (4 байти) використовується для виявлення помилок в кадрі. У ньому використовується циклічний контроль надмірності (CRC). Відправляючий пристрій включає результати циклічного контролю надмірності в полі FCS кадру. Одержуючий пристрій приймає кадр і створює CRC для пошуку помилок. Якщо розрахунки співпадають, помилки відсутні. Неспівпадання розрахунків означає зміну даних; отже, кадр скидається. Дані можуть змінитися в результаті порушення електричних сигналів, які представляють біти.

На вузлі Windows MAC -адресу адаптера Ethernet можна визначити за допомогою команди ipconfig /all.

У мережі Ethernet різні MAC -адреси використовуються для одноадресної, багатоадресної і широкомовної розсилки рівня 2.

MAC -адреса одноадресної розсилки – це унікальна адреса, яка використовується при відправці кадру від одного передавального пристрою до одного пристрою призначення.

У пакеті **широкомовної розсилки** міститься IP -адреса призначення, у вузловій частині якого є присутніми тільки одиниці. Ця нумерація в адресі означає, що усі вузли в локальній мережі (домені широкомовної розсилки) отримають і оброблять пакет. Багато мережевих

протоколів, зокрема, DHCP і протокол дозволу адрес (ARP), використовують широкомовні розсилки.

Адреси багатоадресних розсилок дозволяють початковому пристрою розсилати пакет групі пристроїв. Пристрої, що відносяться до багатоадресної групи, отримують її IP -адресу. Діапазон адрес багатоадресних розсилок IPv4 – від 224.0.0.0 до 239.255.255.255. Оскільки адреси багатоадресних розсилок відповідають групам адрес (які іноді називаються групами вузлів), вони використовуються тільки як адресати пакету. У джерела завжди одноадресна адреса. Адреси багатоадресних розсилок використовуються, наприклад, в іграх з віддаленим підключенням, в яких беруть участь декілька учасників з різних місць. Крім того, такі адреси використовуються при дистанційному навчанні в режимі відеоконференції, коли декілька учнів підключені до одного і тому ж курсу.

Як і у випадку з адресами для одноадресної і широкомовної розсилки, IP -адресі для багатоадресної розсилки потрібна відповідна MAC -адреса, щоб фактично передавати кадри по локальній мережі. **MAC -адреса багатоадресної розсилки** – це особливе значення, яке в шістнадцятиричному форматі починається з 01-00-5E. Інша частина MAC -адреси багатоадресної розсилки створюється шляхом перетворення нижніх 23 біт IP -адреси групи багатоадресної розсилки в 6 шістнадцятиричних символів.

5.4. MAC і IP адреси

Головному пристрою привласнюються дві основні адреси:

- фізична адреса (MAC -адреса);
- логічна адреса (IP -адреса).

MAC - і IP -адреси функціонують спільно, щоб визначити пристрій в мережі. Процес використання MAC - і IP -адреси для пошуку комп'ютера подібно до використання імені і адреси окремої людини для відправки йому листи.

MAC -адреса на вузлі фізично впроваджена в мережеву плату вузла і залишається незмінною незалежно від розташування вузла в мережі.

IP -адреса залежить від фактичного розташування вузла. Використовуючи цю адресу, кадр може визначити місце, куди він має бути відправлений. IP -адреса, або мережева адреса призначається логічним шляхом. Така адреса привласнюється кожному вузлу мережевим адміністратором виходячи з параметрів локальної мережі, до якої підключений вузол.

Початковий пристрій відправить пакет, використовуючи IP -адресу. Одним з найбільш поширених способів, за допомогою якого початковий пристрій може визначити IP -адресу пристрою призначення, є використання сервісу доменних імен DNS, в якому IP -адреса прив'язана до імені домена. Наприклад, ім'я www.cisco.com пов'язане з адресою 209.165.200.225. Використовуючи цю IP -адресу, пакет буде доставлений в те місце в мережі, в якому знаходиться пристрій призначення. Саме цюя IP -адресу використовуватимуть маршрутизатори, щоб визначити найкращий шлях до вузла призначення. Іншими словами, IP -адресація дозволяє визначати поведінку IP -пакета при його проходженні від початкового вузла до кінцевого.

При цьому в кожному каналі на своєму шляху IP -пакет інкапсулюється в кадрі залежно від використовуваної технології каналу передачі даних, яка пов'язана з цим каналом, наприклад, технології Ethernet. Крайові пристрої в мережі Ethernet не приймають і не обробляють кадри на основі IP -адрес – замість цього кадр приймається і обробляється на основі MAC -адрес.

У мережах Ethernet MAC -адреси використовуються для визначення (на нижчому рівні) вузлів джерела і призначення. Коли підключений до мережі Ethernet вузол починає обмін даними, він розсилає кадри зі своєю MAC -адресою в якості джерела і MAC -адресою передбачуваного одержувача в якості призначення. Усі вузли, які отримують кадр, прочитуватимуть MAC -адресу призначення. Якщо MAC -адреса призначення співпаде з

MAC -адресою, встановленою на мережевій інтерфейсній платі вузла, тільки після цього вузол почне обробку повідомлення.

IP -адреси IP -пакетів в потоці даних асоціюються з MAC -адресами в кожному каналі на шляху до вузла призначення за допомогою протоколу дозволу адрес (ARP).

5.5. Функції і принципи роботи роботи протоколу ARP

Щоб відправляти дані, вузол повинен використовувати власні MAC- і IP -адреси в полях джерела, а також надати MAC- і IP -адреси для призначення. Не дивлячись на те, що IP -адреса призначення буде надана вищим рівнем OSI, відправляючому вузлу потрібний спосіб знайти MAC -адресу призначення для цього каналу Ethernet. У цьому полягає призначення протоколу ARP.

У своїй роботі ARP покладається на конкретні типи широкомовних і одноадресних повідомлень Ethernet, які також називаються **запитами і відповідями ARP.**

Протокол ARP виконує дві основні функції:

- зіставлення адрес IPv4 і MAC-адрес;
- збереження таблиці зіставлень.

Щоб кадр можна було помістити в середовще передачі даних локальної мережі, йому потрібна MAC -адреса призначення. Коли пакет вирушає до канального рівня для інкапсуляції в кадрі, вузол звертається до таблиці в його пам'яті, щоб знайти адресу канального рівня, яка зіставлена з IPv4 -адресою призначення. Ця таблиця називається **таблицею ARP або кешем ARP**. Таблиця ARP зберігається в оперативній пам'яті пристрою. Кожен запис або рядок в таблиці ARP зв'язує IP -адресу з MAC -адресою. Таблиця ARP тимчасово зберігає (кешує) зіставлення пристроїв в локальній мережі.

Таблиця ARP зберігається динамічно. Існують два способи, за допомогою яких пристрій може збирати MAC -адреси. Перший спосіб – **моніторинг трафіку**, який з'являється в сегменті локальної мережі. Коли вузол отримує кадри з середовища передачі даних, він може зареєструвати IP - і MAC -адреси джерела у вигляді зіставлення в таблиці ARP. У міру передачі кадрів по мережі пристрій заповнює таблицю ARP, додаючи пари адрес.

Другий спосіб отримання пари адрес для пристрою – **відправка запиту ARP**, що є широкомовною розсилкою рівня 2 на усі пристрої в локальній мережі Ethernet. Запит ARP містить IP -адресу вузла призначення і MAC -адресу широкомовної розсилки, FFFF.FFFF.FFFF. Оскільки це широкомовна розсилка, усі вузли в локальній мережі Ethernet отримають її і оброблять вміст. Відповідь поступить від того вузла, у якого IP -адреса співпадає з IP -адресою в запиті ARP. Відповідь буде представлена у вигляді кадру одноадресної розсилки, який містить MAC -адресу, відповідну IP -адресу в запиті. Потім ця відповідь буде використана для додавання нового запису в таблицю ARP відправляючого вузла.

Як поводиться вузол, коли йому необхідно створити кадр, а кеш ARP не містить зіставлення IP -адреса з MAC -адресом призначення? Він відправляє запит ARP!

Коли протокол ARP отримує запит на зіставлення адреси IPv4 з MAC -адресою, він звертається до своєї таблиці ARP для пошуку зіставлення, доданого в кеш. Якщо такий запис не знайдений, інкапсуляція пакету IPv4 буде неможлива, а процеси рівня 2 повідомлять протокол ARP про те, що йому потрібно зіставлення. Потім процеси ARP відправляють пакет запиту ARP, щоб знайти MAC -адресу пристрою призначення в локальній мережі. Якщо пристрій, що отримав цей запит, має IP -адресу призначення, він відправляє відповідь ARP. У таблицю ARP додається зіставлення. Тепер пакети для цієї адреси IPv4 можна інкапсулювати в кадрах.

Якщо на запит ARP не відповідає жоден пристрій, пакет відкидається, оскільки створення кадру неможливе. Інформація про цей збій інкапсуляції передається на верхні рівні пристрою. Якщо пристрій є проміжним (наприклад, маршрутизатором), верхні рівні можуть відправити відповідь на вузол джерела з помилкою в пакеті ICMPv4.

Усі кадри мають бути доставлені на вузол в сегменті локальної мережі. Якщо вузол призначення IPv4 знаходиться **в локальній мережі**, кадр використовуватиме MAC -адресу цього пристрою в якості MAC -адреси призначення.

Якщо вузол призначення IPv4 **не знаходиться в локальній мережі**, вузлу джерела необхідно доставити кадр до інтерфейсу маршрутизатора, який є шлюзом, або наступним переходом, що використовується для досягнення цього вузла призначення. Початковий вузол використовуватиме MAC -адресу шлюзу як адреси призначення для кадрів, які містять пакет IPv4, адресований вузлам в інших мережах.

Адреса шлюзу інтерфейсу маршрутизатора зберігається в IPv4 -конфигурації вузлів. Коли вузол створює пакет для адресата, він порівнює IP -адресу призначення і свою IP -адресу, щоб визначити, чи знаходяться ці дві IP -адреси в одній і тій же мережі рівня 3. Якщо вузол-одержувач знаходиться в межах іншої мережі, джерело використовує процес ARP для визначення MAC-адреси інтерфейсу маршрутизатора, що виступає шлюзом.

Для кожного пристрою таймер кеша ARP видаляє записи ARP, які не використовуються впродовж вказаного періоду часу. Цей період може бути різним залежно від пристрою і його ОС. Наприклад, деякі операційні системи Windows зберігають записи кеша ARP впродовж 2 хвилин. Якщо впродовж цього періоду запис використовується повторно, таймер ARP буде збільшений для неї до 10 хвилин. Крім того, можна використовувати деякі команди, щоб вручну видалити усе або деякі записи з таблиці ARP. Після видалення запису процес відправки запиту ARP і отримання відповіді ARP необхідно задіювати повторно, щоб зареєструвати зіставлення в таблиці ARP.

Для кожного пристрою передбачена команда, залежно від ОС, за допомогою якої можна видалити вміст кеша ARP. Ці команди не викликають виконання ARP. Вони тільки видаляють записи таблиці ARP. Служба ARP інтегрована усередині протоколу IPv4 і реалізується пристроєм.

На комп'ютерах під управлінням Windows 7 команда arp - a використовується для відображення таблиці ARP. На маршрутизаторі Cisco команда show ip arp використовується для відображення таблиці ARP, як показано на рис. 5.1.

```
Router#show ip arp

                     Age
Protocol  Address          (min)  Hardware Addr   Type   Interface
Internet  172.16.233.229    -    0000.0c59.f892   ARPA   Ethernet0/0
Internet  172.16.233.218    -    0000.0c07.ac00   ARPA   Ethernet0/0
Internet  172.16.168.11     -    0000.0c63.1300   ARPA   Ethernet0/0
Internet  172.16.168.254    9    0000.0c36.6965   ARPA   Ethernet0/0
```

Рис. 5.1. Таблиця ARP маршрутизатора [1]

Будучи кадром широкомовної розсилки, запит ARP виходить і обробляється усіма пристроями в локальній мережі. У стандартній корпоративній мережі такі широкомовні розсилки, швидше за все, не зроблять серйозного впливу на продуктивність мережі. Проте, якщо необхідно забезпечити живленням велику кількість пристроїв, і усі вони одночасно спробують дістати доступ до мережевих служб, це може на короткий період часу негативно вплинути на продуктивність роботи мережі.

В деяких випадках використання протоколу ARP може представляти певний ризик для безпеки. **ARP -спуфінг** (також званий «отруєнням» ARP -кеша) використовується зловмисниками, щоб за допомогою фальшивих запитів ARP додати в мережу свідомо неправильний зв'язок з MAC -адресою. Зловмисник фальсифікує MAC -адресу пристрою, після чого кадри можуть вирушати на неправильну адресу призначення.

Конфігурація статичних зв'язків ARP вручну – це один із способів запобігання ARP -спуфінгу. На деяких пристроях можна вказати допустимі MAC -адреси, і в результаті доступ до мережі зможуть отримати лше вказані пристрої.

Використовуючи сучасні комутатори, можна зменшити кількість проблем, пов'язаних з широкомовними розсилками і забезпеченням безпеки при роботі з протоколом ARP.

Комутатори забезпечують сегментацію локальної мережі, розділяючи її на декілька незалежних колізійних доменів. Кожним портом на комутаторі є окремий колізійний домен і забезпечує повну пропускну спроможність для одного або декількох вузлів, підключених до цього порту. Не дивлячись на те, що за замовчуванням комутатори не запобігають поширенню широкомовних розсилок на підключені пристрої, вони дійсно ізолюють одноадресні розсилки в мережі Ethernet так, щоб їх могли «почути» тільки пристрої джерела і призначення. Тому за наявності великої кількості запитів ARP кожна відповідь ARP передаватиметься тільки між двома пристроями.

5.6. Таблиця MAC -адрес комутатора

Комутатори використовують MAC -адреси для передачі даних по мережі через свою комутуючу матрицю на відповідний порт у напрямі вузла призначення. Комутуючі матриці є інтегрованими каналами і доповнюючими засобами машинного програмування, що дозволяє контролювати шляхи проходження даних через комутатор. Щоб комутатор зміг зрозуміти, який порт необхідно використовувати для передачі кадру одноадресної розсилки, спочатку йому необхідно дізнатися, які вузли є на кожному з його портів.

Комутатор визначає спосіб обробки вхідн кадрів, використовуючи для цього власну таблицю MAC-адрес. Він створює власну таблицю MAC -адрес, додаючи до неї MAC -адреси вузлів, які підключені до кожного з його портів. Після внесення MAC -адреси для того або іншого вузла, підключеного до певного порту, комутатор зможе відправляти призначений для цього вузла трафік через порт, який зіставлений з вузлом для наступних передач.

Якщо комутатор отримує кадр даних, для якого в таблиці немає MAC -адреси призначення, він пересилає цей кадр на усі порти, за винятком того, на якому цей кадр був прийнятий. Якщо від вузла призначення поступає відповідь, комутатор вносить MAC-адресу вузла в таблицю адрес, використовуючи для цього дані з поля адреси джерела кадру. У мережах з декількома підключеними комутаторами в таблиці MAC -адрес вносяться декілька MAC -адрес портів, що сполучають комутатори, які відбивають елементи за межами вузла. Як правило, порти комутатора, що використовуюься для підключення двох комутаторів, мають декілька MAC-адрес, внесених у відповідну таблицю.

5.7. Налаштування повнодуплексної та напівдуплексної передачі даних

Не дивлячись на те, що комутатори прозорі для мережевих протоколів і користувацьких додатків, вони здатні функціонувати в різних режимах, що може як позитивно, так і негативно відбитися на пересилці кадрів Ethernet по мережі. Одним з базових параметрів комутатора є дуплексний режим для кожного окремого порту, підключеного до кожного головного пристрою. Порт на комутаторі має бути налагоджений так, щоб співпадати з параметрами дуплексного режиму певного типу середовища передачі даних. Для обміну даними в мережах Ethernet використовуються два типи налаштувань дуплексного режиму: напівдуплексний і повнодуплексний.

Напівдуплексний зв'язок використовує однонапрямлений потік даних, коли відправка і отримання даних не виконуються в один і той же час. Це подібно до використання рації, коли одноразово може говорити тільки одна людина. Якщо хто-небудь намагається говорити під час розмови іншої людини, відбувається колізія. В результаті при напівдуплексному зв'язку використовується множинний доступ з контролем несучої і визначенням колізій, що дозволяє понизити вірогідність колізій і виявити їх у разі виникнення. При напівдуплексному зв'язку можливе зниження продуктивності, викликане постійним перебуванням в режимі очікування, оскільки дані можуть передаватися одночасно тільки в одному напрямі.

Напівдуплексні з'єднання, як правило, зустрічаються на старішому устаткуванні, наприклад на концентраторах.

При **повнодуплексному зв'язку** потік даних передається в обидві сторони, що дозволяє одночасно відправляти і отримувати інформацію. Підтримка двосторонньої передачі даних підвищує продуктивність за рахунок скорочення часу очікування між передачами. Більшість мережевих адаптерів Ethernet, що продаються сьогодні (Fast Ethernet і Gigabit Ethernet) працюють в повнодуплексному режимі. У повнодуплексному режимі детектор колізій відключений. При цьому унеможливлено зіткнення кадрів, що пересилаються двома пов'язаними кінцевими вузлами, оскільки ці вузли використовують два окремі канали зв'язку в мережевому кабелі. Кожне повнодуплексне з'єднання використовує тільки один порт. Повнодуплексним з'єднанням потрібен комутатор, який підтримує повнодуплексний режим, або пряме підключення, між двома вузлами, кожен з яких підтримує повнодуплексну передачу даних. Вузли, які безпосередньо підключені до виділеного порту комутатора за допомогою мережевих адаптерів, що підтримують повнодуплексний зв'язок, повинні підключатися до портів комутатора, налагоджених для роботи в повнодуплексному режимі.

5.8. Порівняння комутації рівня 2 і рівня 3

Комутатор LAN рівня 2 виконує комутацію і фільтрацію, використовуючи лше MAC - адресу (рівень 2) канального рівня OSI, і при цьому залежить від маршрутизаторів для передачі даних між незалежними IP -підмережами.

Комутатор рівня 3 (наприклад, Catalyst 3560) функціонує подібно до комутатора рівня 2 (наприклад, Catalyst 2960), але замість використання тільки однієї MAC -адреси рівня 2 для ухвалення рішень про пересилку комутатор рівня 3 може також використовувати також IP - адресу. Замість того щоб визначати, які MAC -адреси пов'язані з кожним з його портів, комутатор рівня 3 може також встановити, які IP -адреси пов'язані з його інтерфейсами. Це дозволяє комутатору рівня 3 перенаправляти трафік по мережі, також використовуючи дані про IP -адреси.

Комутатори рівня 3 також можуть виконувати функції маршрутизації рівня 3, тим самим знижуючи необхідність установки виділених маршрутизаторів в локальній мережі. Оскільки в комутаторах рівня 3 встановлено спеціальне апаратне забезпечення для комутації, вони, як правило, можуть направляти дані із швидкістю самої комутації.

Мережеві пристрої Cisco підтримують декілька різних типів інтерфейсів рівня 3. Інтерфейс рівня 3 підтримує пересилку IP -пакетів до кінцевого призначення на основі IP - адреси.

До основних типів інтерфейсів рівня 3 відносяться наступні.

- **Віртуальний інтерфейс комутатора (SVI)** - логічний інтерфейс на комутаторі, пов'язаний з віртуальною локальною мережею (VLAN).

1. **Порт, що маршрутизується, -** фізичний порт на комутаторі рівня 3, налаштований на роботу портом маршрутизатора.

- **EtherChannel рівня 3** - логічний інтерфейс на пристрої Cisco, який пов'язаний з групою портів, що маршрутизуються.

Порт комутатора можна налаштувати так, щоб він функціонував в якості порту 3 рівня, що маршрутизується, і діяв в режимі стандартного інтерфейсу маршрутизатора.

Висновок до лекції 5

На сьогодні Ethernet є найбільш використовуваною технологією для локальних мереж. Це сімейство мережевих технологій, які регламентуються стандартами IEEE 802.2 і 802.3. Стандарти Ethernet регламентують як протоколи другого рівня, так і технології першого рівня. Для протоколів другого рівня, як і у випадку з усіма стандартами групи IEEE 802, технологія Ethernet покладається на роботу підрівнів канального рівня, а також на підрівні управління логічним каналом (LLC) і MAC.

Адресація Ethernet рівня 2 підтримує одноадресний, багатоадресний і широкомовний режими передачі даних. Ethernet використовує протокол дозволу адрес (ARP) для визначення MAC -адрес і їх зіставлення з відомими адресами мережевого рівня.

У кожного вузла в IP -мережі є MAC- і IP -адреси. Вузол повинен використовувати власні MAC- і IP -адреси в полях джерела, а також надати MAC- і IP -адреси для призначення. Не дивлячись на те, що IP -адреса призначення буде надана вищим рівнем OSI, відправляючому вузлу необхідно знайти MAC -адресу призначення для цього каналу Ethernet. У цьому полягає призначення протоколу ARP.

У своїй роботі ARP покладається на конкретні типи широкомовних і одноадресних повідомлень Ethernet, які також називаються запитами і відповідями ARP. Протокол ARP перетворює адреси IPv4 в MAC-адреси і зберігає таблицю зіставлень.

У більшості мереж Ethernet крайові пристрої, як правило, підключаються до комутатора локальної мережі рівня 2 за принципом «точка-точка». Комутатор LAN рівня 2 здійснює комутацію і фільтрацію тільки на основі MAC-адреси канального рівня моделі OSI. Комутатор рівня 2 створює таблицю MAC-адрес, яку надалі використовує для ухвалення рішень про пересилку пакетів. В процесі передачі даних між незалежними IP -підмережами комутатори рівня 2 покладаються на маршрутизатори. Комутатори рівня 3 також можуть виконувати функції маршрутизації рівня 3, тим самим знижуючи необхідність установки виділених маршрутизаторів в локальній мережі. Оскільки в комутаторах рівня 3 встановлено спеціальне апаратне забезпечення для комутації, вони, як правило, можуть направляти дані із швидкістю самої комутації.

Питання для закріплення

1. Які підрівні канального рівня ви знаєте?
2. У чому полягають методи CSMA, CSMA/CD, CSMA/CA?
3. Яке призначення і структура MAC-адреси?
4. Які вимоги до створення MAC-адрес ви знаєте?
5. Який формат MAC-адреси?
6. Які ви знаєте типи MAC-адрес?
7. Яка структура кадру Ethernet?
8. Поясність призначення і структуру MAC і IP адреси.
9. Які функції і принципи роботи роботи протоколу ARP?
10. Що таке ARP –спуфінг?
11. Для чого використовується таблиця MAC -адрес комутатора?
12. Поясніть принципи повнодуплексної та напівдуплексної передачі даних.
13. У чому різниця комутації 2 рівня та 3 рівня?

Список рекомендованої літератури

1. CCNA R&S ITN Chapter 5: Ethernet // Електронний ресурс. Режим доступу: http://static-course-assets.s3.amazonaws.com/IntroNet50ENU/module5/index.html

2. MAC адреса - фізична адреса мережевого пристрою // Електронний ресурс. Режим доступу: https://hightech.in.ua/os-network/art-mac-address-physical-address

3. Атака ARP Spoofing, перехоплення пошти та пароля в локальній мережі // Електронний ресурс. Режим доступу: https://litl-admin.ru/xaking/ataka-arp-spoofing-perexvat-pochty-i-parolya-v-lokalnoj-seti.html

Лекція 6. Тема: «Мережевий рівень»

План лекції

6.1. Процеси і протоколи мережевого рівня.
6.2. Протокол IPv4.
6.3. Протокол IPv6.
6.4. Шлюз за замовчуванням.
6.5. Таблиці маршрутизації.
6.6. Будова і функції маршрутизатора.

6.1. Процеси і протоколи мережевого рівня

Мережеві застосування і сервіси на одному крайовому пристрої можуть взаємодіяти із застосуваннями і сервісами, запущеними на іншому пристрої. Яким чином забезпечується максимальна ефективність передачі цих даних по мережі?

Протоколи мережевого рівня моделі OSI визначають адресацію і процеси, які дозволяють упаковувати і передавати дані транспортного рівня. Інкапсуляція мережевого рівня забезпечує проходження даних по мережі до адресата (чи іншої мережі) з мінімальним навантаженням.

Мережевий рівень, або рівень 3 OSI, надає сервіси, що дозволяють крайовим пристроям обмінюватися даними по мережі. Для виконання такої наскрізної передачі в мережевому рівні використовуються чотири основні процеси.

- **Адресація крайових пристроїв:** крайовим пристроям необхідно призначити унікальну IP-адресу для можливості ідентифікації в мережі.
- **Інкапсуляція:** мережевий рівень отримує блок даних протоколу (PDU) від транспортного рівня. Під час виконання інкапсуляції мережевий рівень додає інформацію заголовка IP, наприклад IP -адресу вузла джерела (що відправляє) і вузла призначення (одержуючого). Після додавання в блок PDU інформації заголовка такий блок називатиметься **пакетом**.
- **Маршрутизація:** мережевий рівень надає сервіси, за допомогою яких пакети спрямовуються до вузла призначення в іншу мережу. Для переміщення до інших мереж пакет має бути оброблений маршрутизатором. Роль маршрутизатора полягає в тому, щоб вибрати шляхи для пакетів і направити їх до вузла призначення. Такий процес називається **маршрутизацією**. До того, як досягти вузла призначення, пакет може пройти через декілька проміжних пристроїв. Кожен маршрут на шляху пакету до вузла призначення називається **переходом**.
- **Деінкапсуляція:** після прибуття пакету на мережевий рівень вузла призначення цей вузол перевіряє IP -заголовок пакету. Якщо IP -адреса призначення в заголовку співпадає з його власною IP -адресою, заголовок IP видаляється з пакету. Після деінкапсуляції пакету, виконаною мережевим вузлом, отриманий блок PDU рівня 4 пересилається відповідній службі на транспортному рівні.

На відміну від транспортного рівня (рівень 4 OSI), який управляє передачею даних між процесами, запущеними на кожному вузлі, протоколи мережевого рівня вказують структуру пакету і тип обробки, які використовуються для переміщення даних від одного вузла до іншого.

Існує декілька протоколів мережевого рівня, але, як правило, використовуються лише наступні:

- протокол IP версії 4 (IPv4)
- протокол IP версії 6 (IPv6).

IP – це сервіс мережевого рівня, який реалізовується набором протоколів TCP/IP. До основних характеристик IP відносяться наступні.

- **Без встановлення з'єднання:** перед відправкою пакетів даних з'єднання з вузлом призначення не встановлюється.
- **Доставка з максимальними зусиллями (ненадійна):** доставка пакетів не гарантується.
- **Незалежність від середовища:** функціонує незалежно від середовища, в якому передаються дані.

Основна роль мережевого протоколу – пересилка пакетів між вузлами при найменшому навантаженні на мережу. Мережевий рівень не має відношення (і навіть не має якої-небудь інформації) щодо типу обміну даними, який міститься усередині пакету. IP є протоколом без встановлення з'єднання, це означає, що перед відправкою даних виділене наскрізне з'єднання не встановлюється. За своєю суттю обмін даними без встановлення з'єднання аналогічний відправці листа без попереднього повідомлення одержувача.

Протокол IP не використовує з'єднання і, отже, йому не потрібно первинний обмін контрольною інформацією для встановлення наскрізного підключення до початку пересилки пакетів. IP також не потребує додаткових полів в заголовку блоку даних протоколу (PDU) для підтримки встановленого з'єднання. Цей процес значно знижує навантаження IP. Проте, без заздалегідь встановленого наскрізного підключення відправникам невідомо, чи є пристрої-адресати і чи здатні вони функціонувати у момент відсилання пакетів, а також чи отримає пакет вузол призначення і чи зможуть пристрої-адресати дістати доступ до пакету і прочитати його.

IP часто називають ненадійним протоколом або протоколом доставки з максимальними зусиллями. Це не означає, що в деяких випадках протокол IP функціонує належним чином, а усю решту часу працює з помилками. «Ненадійний» протокол – той, який не здатний контролювати не доставлені або пошкоджені пакети і відновлюватися у разі їх появи. Це пов'язано з тим, що хоча пакети IP, що відправляються, і містять зведення про місце доставки, в них відсутня інформація, яку можна обробити, щоб повідомити відправника про успішно виконану доставку. Заголовок пакету не містить даних синхронізації для відстежування черговості доставки пакетів. Також не передбачені підтвердження доставки пакетів по IP і відсутні дані контролю помилок, за допомогою яких можна відстежити, чи доставлені пакети без ушкоджень. Пакети можуть прибути на вузол призначення пошкодженими або з порушеним порядком, або не прибути зовсім. У разі виникнення таких помилок інформація, яка міститься в заголовку IP, не дозволяє виконати повторну пересилку пакетів.

Якщо відсутність пакетів або недотримання черговості створює проблеми для застосувань, що використовують дані, сервіси верхнього рівня, наприклад TCP, повинні усунути ці проблеми. Це забезпечує високу ефективність роботи протоколу IP. Якщо навантаження надійності були включені в IP, то процеси обміну даними, для яких не потрібне підключення, або надійність можуть постраждати від зменшення пропускної спроможності і затримок, викликаних такими навантаженнями. У пакеті протоколів TCP/IP транспортний рівень може використовувати або TCP, або UDP, залежно від необхідності забезпечення надійності передачі даних. Якщо рішення про забезпечення надійності приймається на транспортному рівні, це дозволить IP швидше адаптуватися до різних типів передачі даних.

Мережевий рівень також не навантажується характеристиками даних середовища, в якому передаються пакети. Протокол IP діє незалежно від середовища, яке служить для передачі даних на нижніх рівнях стека протоколів.

Проте, існує одна важлива характеристика середовища передачі, яка враховується на мережевому рівні: максимальний розмір блоку PDU, який здатне переслати кожне середовище. Ця характеристика називається **максимальним розміром передаваного блоку даних (MTU,** Maximum Transmission Unit). Частина обміну контрольними даними між канальним рівнем і мережевим рівнем – це встановлення максимального розміру пакету. Канальний рівень передає значення MTU до мережевого рівня. Потім мережевий рівень

визначає розмір пакетів. В деяких випадках проміжний пристрій (як правило, це маршрутизатор) повинен розділити пакет під час його пересилки з одного середовища обробки даних в середовще з меншим максимальним розміром пакету. Цей процес називається **фрагментацією.**

Протокол IP інкапсулює, або упаковує, сегмент транспортного рівня шляхом додавання заголовка IP. Цей заголовок використовується для доставки пакету на вузол призначення. Заголовок IP залишається на місці з моменту відправки пакету з мережевого рівня вузла джерела до його прибуття на мережевий рівень вузла призначення.

Процес інкапсуляції даних рівень за рівнем забезпечує можливість сервісів розробляти і масштабувати на різних рівнях без впливу на інші рівні. Це означає, що сегменти транспортного рівня можна легко упакувати за допомогою протоколів IPv4 або IPv6 або будь-якого нового протоколу, який може бути створений в майбутньому.

6.2. Протокол IPv4

У 1983 році протокол IPv4 був уперше використаний в Мережі управління перспективних досліджень і розробок (ARPANET). IPv4 є найбільш поширеним протоколом мережевого рівня і широко застосовується в мережі Інтернет.

Пакет IPv4 складається з двох частин:

- **заголовок IP:** визначає характеристики пакету;
- **корисне навантаження:** містить інформацію сегменту 4 рівня і фактичні дані.

Серед найбільш важливих полів у заголовку IPv4 можна виділити наступні.

- **Версія:** включає 4-бітове двійкове значення, що визначає версію IP -пакета. Для пакетів IPv4 в цьому полі завжди вказано значення 0100.
- **Диференційовані сервіси (DS):** це 8-бітове поле для визначення пріоритету кожного пакету. Перші 6 біт визначають значення точки коду диференційованих сервісів, яке використовується механізмом забезпечення якості обслуговування (QoS). Останні 2 біта визначають значення явного повідомлення про перевантаження, яке можна використовувати для запобігання втрат пакетів під час перевантаження мережі.
- **Час існування (TTL,** Time to live**):** містить 8-бітове двійкове значення для обмеження часу існування пакету. Воно вказується в секундах, але зазвичай має на увазі кількість переходів. Відправник пакету встановлює початкове значення часу існування (TTL), яке зменшується на одиницю, або перехід в процесі кожної обробки пакету маршрутизатором. Якщо значення в полі TTL зменшується до нуля, маршрутизатор відкидає пакет і відправляє на IP -адресу джерела повідомлення про перевищення часу протоколу ICMP (управління повідомленнями в мережі). Команда traceroute задіює це поле, щоб визначити маршрути, використані між джерелом і призначенням.
- **Протокол:** 8-бітове двійкове значення, що вказує тип корисного навантаження даних, які переносить пакет, що дозволяє мережевому рівню пересилати дані на відповідний протокол більш високого рівня. Часто зустрічаються значення ICMP (1), TCP (6), і UDP (17).
- **IP -адреса джерела:** містить 32-бітове двійкове значення, яке представляє IP -адресу джерела пакету.
- **IP -адреса призначення:** містить 32-бітове двійкове значення, яке представляє IP -адресу призначення пакету.

Поля, що залишилися, використовуються для визначення і перевірки пакету або для переупорядковування фрагментованого пакету.

До полів, що використовуюься для визначення і перевірки пакету, відносяться наступні.

- **Довжина заголовка Інтернету:** містить 4-бітове значення, що визначає число 32-бітових слів у заголовку. Мінімальне значення цього поля – 5 (5×32 = 160 біт = 20 байт), а максимальне значення – 15 (15×32 = 480 біт = 60 байт).

- **Загальна довжина:** 16-бітове поле, визначає розмір усього пакету (фрагменту), включаючи заголовок і дані в байтах. Пакет мінімальної довжини складає 20 байт, максимальної – 65 535 байт.
- **Контрольна сума заголовка:** 16-бітове поле для перевірки помилок в заголовку IP. Контрольна сума заголовка розраховується повторно і порівнюється зі значенням в полі контрольної суми. Якщо значення не співпадають, пакет відкидається.

Упродовж багатьох років протокол IPv4 періодично оновлювався для вирішення нових завдань. Проте, навіть в результаті змін IPv4 як і раніше має три основні недоліки.

- **Нестача IP -адрес.** IPv4 може запропонувати лише обмежену кількість унікальних загальнодоступних IP -адрес. Не дивлячись на те, що існує приблизно 4 мільярди IPv4 -адрес, збільшення числа нових пристроїв, в яких використовується протокол IP, а також потенційне зростання менш розвинених регіонів привели до необхідності додатково збільшити кількість адрес.
- **Розширення таблиці інтернет-маршрутизації.** Таблиця маршрутизації використовується маршрутизаторами для визначення оптимальних шляхів пересилки даних. У міру збільшення кількості серверів (вузлів), підключених до Інтернету, також росте число мережевих маршрутів. Ці маршрути IPv4 споживають значну кількість пам'яті і ресурсів процесорів інтернет-маршрутизаторів.
- **Нестача наскрізних з'єднань.** Перетворення мережевих адрес (**NAT**, Network Address Translation) є технологією, яка зазвичай застосовується в мережах IPv4. NAT дозволяє різним пристроям спільно використовувати одну публічну IP -адресу. При цьому, оскільки публічна IP -адреса використовується спільно, IP -адреса вузла внутрішньої мережі прихована. Це може представляти проблему при використанні технологій, для яких потрібні наскрізні підключення.

6.3. Протокол IPv6

На початку 90-х років фахівці інженерної групи з розвитку Інтернету (IETF) підняли питання про недоліки протоколу IPv4 і почали пошуки альтернативних рішень. Результатом пошуків стала розробка протоколу IP версії 6 (IPv6). IPv6 допомагає здолати обмеження протоколу IPv4 і значно розширює доступні можливості, пропонуючи функції, які оптимально відповідають поточним і прогнозованим мережевим вимогам.

До поліпшень, які пропонує протокол IPv6, відносяться наступні.

- **Розширений адресний простір:** IPv6-адреси використовують 128-бітову ієрархічну адресацію, на відміну від протоколу IPv4, що використовує 32 біта. Це істотно збільшує кількість доступних IP -адрес.
- **Поліпшена обробка пакетів:** структура заголовка IPv6 була спрощена завдяки зменшенню кількості полів. Це підвищує обробку пакетів проміжними маршрутизаторами, а також надає підтримку розширень і додаткових параметрів, забезпечуючи підвищену масштабованість і довговічність.
- **Відсутність необхідності у використанні NAT:** завдяки великій кількості загальнодоступних IPv6 -адрес трансляція мережевих адрес (NAT) не потрібна. Клієнтські вузли, від найбільших підприємств до житлових будинків, можуть отримати загальнодоступну мережеву IPv6 -адресу. Це дозволяє усунути деякі проблеми, пов'язані з перетворенням мережевих адрес, які виникають при роботі додатків, що вимагають наявності наскрізного підключення.
- **Інтегрована безпека:** протокол IPv6 має засоби для аутентифікації і забезпечення конфіденційності. При використанні протоколу IPv4 для цього вимагалося реалізувати додаткові функції.

Адресний простір протоколу IPv4 – це 32-бітовий простір адрес, він передбачає приблизно 4 294 967 296 унікальних адрес. З цієї кількості можуть бути призначені тільки 3,7 мільярда,

оскільки система адресації IPv4 підрозділяє адреси на класи, резервуючи адреси для багатоадресних розсилок, тестування та інших цілей.

Адресний простір протоколу IP версії 6 підтримує 340 282 366 920 938 463 463 374 607 431 768 211 456 або 340 ундециліонів адрес, що приблизно дорівнює кількості піщинок на Землі.

Одним з основних конструктивних поліпшень протоколу IPv6 в порівнянні з IPv4 є спрощений заголовок IPv6.

Заголовок IPv4 складається з 20 октетів (до 60 байт), заголовок IPv6 складається з 40 октетів (головним чином через довжину адрес IPv6 джерела і призначення) і 8 полів заголовків (3 основні поля заголовків IPv4 і 5 додаткових полів). Крім того, в IPv6 додано нове поле, яке не використовується в протоколі IPv4.

Спрощений заголовок IPv6 пропонує ряд переваг в порівнянні з IPv4:

- підвищена ефективність маршрутизації для масштабованості продуктивності і швидкості пересилки;
- не потрібна обробка контрольних сум;
- спрощені і ефективніші механізми заголовків розширень;
- поле «Мітка потоку» призначене для обробки по потоках без необхідності відкривати транспортний внутрішній пакет для визначення різних потоків трафіку.

У заголовку пакету IPv6 використовуються наступні поля.

- **Версія:** поле, що містить 4-бітове двійкове значення, яке визначає версію IP -пакета. Для пакетів IPv6 в цьому полі завжди вказано значення 0110.
- **Клас трафіку:** 8-бітове поле, що відповідає полю «Диференційовані сервіси (DS)» в заголовку IPv4. Воно також містить 6-бітове значення точки коду диференційованих сервісів (DSCP), яке використовується для класифікації пакетів, а також 2-бітове значення явного повідомлення про перевантаження (ECN) для управління перевантаженнями трафіку.
- **Мітка потоку:** 20-бітове поле, що надає спеціальну службу для додатків реального часу. Використовуючи це поле, маршрутизаторам і комутаторам передається інформація про необхідність підтримувати один і той же шлях для потоку пакетів, що допоможе уникнути їх переупорядковування.
- **Довжина корисного навантаження:** 16-бітове поле, що відповідає полю «Загальна довжина» у заголовку IPv4. Воно визначає розмір усього пакету (фрагмента), включаючи заголовок і додаткові розширення.
- **Наступний заголовок:** 8-бітове поле, що відповідає полю «Протокол» у заголовку IPv4. Воно вказує тип корисного навантаження даних, які переносить пакет, що дозволяє мережевому рівню пересилати дані на відповідний протокол більше високого рівня. Це поле також використовується в тих випадках, коли в пакет IPv6 додаються додаткові заголовки розширень.
- **Межа переходу:** 8-бітове поле, замінююче поле «Час існування» (TTL) в IPv4. Це значення зменшується на одиницю кожним маршрутизатором, що пересилає пакет. Коли лічильник досягає 0, пакет відкидається, і на відправляючий вузол пересилається повідомлення ICMPv6, яке означає, що пакет не досяг свого призначення.
- **Адреса джерела:** 128-бітове поле, що визначає IPv6 -адресу приймаючого вузла.
- **Адреса призначення:** 128-бітове поле, що визначає IPv6 -адресу приймаючого вузла.

Пакет IPv6 також може містити заголовки розширень, які надають додаткову інформацію мережевого рівня. Заголовки розширень є додатковими і поміщаються між заголовком IPv6 і корисним навантаженням. Заголовки розширень використовуються для фрагментації, забезпечення безпеки, підтримки мобільності.

128-бітові IPv6 -адреси використовують шістнадцяткову систему числення, що спрощує представлення адрес. Для розподілу записів на серії 16-розрядних шістнадцятиричних блоків в IPv6 -адресах використовуються двокрапки.

6.4. Шлюз за замовчуванням

Шлюз за замовчуванням – цей пристрій, який направляє трафік з локальної мережі до пристроїв у віддалених мережах. У домашніх умовах або на малих підприємствах шлюз за замовчуванням часто використовується для підключення локальної мережі до Інтернету.

Якщо вузол відправляє пакет пристрою в іншу IP -мережу, то в цьому випадку він повинен пересилати пакет через проміжний пристрій до шлюзу за замовчуванням. Це пов'язано з тим, що головний пристрій не зберігає інформацію про маршрутизацію за межами локальної мережі, щоб досягти віддалених адресатів. Шлюз за замовчуванням, навпаки, зберігає таку інформацію. Шлюз за замовчуванням, в ролі якого найчастіше виступає маршрутизатор, зберігає таблицю маршрутизації.

Таблиця маршрутизації – це файл даних в ОЗП, який використовується для зберігання інформації про маршрути для безпосередньо підключених мереж, а також записів віддалених мереж, про які стало відомо пристрою. Маршрутизатор використовує інформацію в таблиці маршрутизації, щоб визначити найкращий шлях до вузлів призначення.

Яким чином вузол відстежує необхідність пересилки пакетів на шлюз за замовчуванням? На вузлах повинна зберігатися їх власна локальна таблиця маршрутизації, щоб пакети мережевого рівня гарантовано спрямовувалися до потрібної мережі призначення. Як правило, локальна таблиця вузла містить наступну інформацію.

- **Пряме підключення** - маршрут до інтерфейсу loopback (127.0.0.1).
- **Маршрут локальної мережі** - інформація про мережу, до якої підключений вузол, автоматично додається в таблицю маршрутизації вузла.
- **Локальний маршрут за замовчуванням** - це маршрут, який повинні пройти пакети, щоб досягти усіх віддалених мережевих адрес. Маршрут за замовчуванням створюється у тому випадку, коли на вузлі є адреса шлюзу за замовчуванням.

Адреса шлюзу за замовчуванням – це IP -адреса мережевого інтерфейсу маршрутизатора, підключеного до локальної мережі. Адресу шлюзу за замовчуванням можна налаштуватина вузлі вручну, або його можна отримати динамічно.

Шлюз за замовчуванням використовується тільки у тому випадку, якщо вузлу необхідно пересилати пакети до віддаленої мережі. В якості прикладу уявимо мережевий принтер або сканер. Якщо на мережевому принтері налагоджені IP -адреса і маска підмережі, то вузли можуть відправляти на принтер документи для друку. Крім того, принтер може переслати відскановані документи на будь-який локальний вузол. До тих пір, поки принтер використовується тільки локально, адреса шлюзу за замовчуванням не потрібна. Не налаштувавши на принтері адресу шлюзу за замовчуванням, ви фактично відхиляєте доступ до Інтернету, що може бути розумним рішенням з точки зору безпеки. Відсутність інтернет-підключення означає і відсутність зовнішніх загроз безпеки.

6.5. Таблиці маршрутизації

На вузлі під управлінням Windows для відображення таблиці маршрутизації вузла можна використовувати команду route print або netstat - r. Обидві команди видають однаковий результат.

Після введення команди netstat - r або команди route print будуть відображені наступні три розділи, що відносяться до поточних мережевих підключень TCP/IP.

- **Список інтерфейсів:** містить адресу управління доступом до середовища (MAC) і присвоєний номер інтерфейсу з підтримкою мережі на вузлі, включаючи адаптери Ethernet, Wi - Fi і Bluetooth.
- **Таблиця маршрутизації IPv4:** містить усі відомі маршрути IPv4, включаючи прямі підключення, локальні мережі і локальні маршрути, використовувані за замовчуванням.
- **Таблиця маршрутизації IPv6:** містить усі відомі маршрути IPv6, включаючи прямі підключення, локальні мережі і локальні маршрути, використовувані за замовчуванням.

Таблиця складається з п’яти стовпців, які містять дані про підключені мережі (рис. 6.1).

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.10.1   192.168.10.10      25
        127.0.0.0        255.0.0.0         On-link        127.0.0.1     306
        127.0.0.1  255.255.255.255         On-link        127.0.0.1     306
  127.255.255.255  255.255.255.255         On-link        127.0.0.1     306
     192.168.10.0    255.255.255.0         On-link    192.168.10.10     281
    192.168.10.10  255.255.255.255         On-link    192.168.10.10     281
   192.168.10.255  255.255.255.255         On-link    192.168.10.10     281
        224.0.0.0        240.0.0.0         On-link        127.0.0.1     306
        224.0.0.0        240.0.0.0         On-link    192.168.10.10     281
  255.255.255.255  255.255.255.255         On-link        127.0.0.1     306
  255.255.255.255  255.255.255.255         On-link    192.168.10.10     281
===========================================================================
```

Рис. 6.1. Таблиця маршрутизації IPv4 [1]

- **Network Destination (Мережа призначення):** список досяжних мереж.
- **Netmask (Маска мережі):** містить маску підмережі, яка повідомляє вузол, як визначати мережу і вузлові частини IP -адреси.
- **Gateway (Шлюз):** містить адресу, яка використовується локальним комп’ютером, щоб досягти віддаленого мережевого адресата. Якщо вузол призначення доступний безпосередньо, в цьому стовпці він буде відображений як «On-link» (Сполучено).
- **Interface (Інтерфейс):** містить адресу фізичного інтерфейсу, яка використовується для відправки пакету до шлюзу для досягнення мережевого адресата.
- **Metric (Метрика):** містить вартість кожного маршруту і використовується для визначення найкращого маршруту до адресата.

Що відбувається, коли пакет прибуває на інтерфейс маршрутизатора? Маршрутизатор перевіряє свою таблицю маршрутизації, щоб визначити місце пересилки пакету.

У таблиці маршрутизації маршрутизатора зберігається наступна інформація.

- **Маршрути з прямим підключенням:** надаються активними інтерфейсами маршрутизаторів. Маршрутизатори додають маршрут з прямим підключенням, коли інтерфейс настроюється за допомогою IP -адреси і активується. Кожен з інтерфейсів маршрутизатора підключений до різного сегменту мережі. Маршрутизатори зберігають інформацію про сегменти мережі, до якої вони підключені, в таблиці маршрутизації.
- **Віддалені маршрути:** надаються віддаленими мережами, підключеними до інших маршрутизаторів. Маршрути до цих мереж можуть бути налагоджені на локальному маршрутизаторі вручну мережевим адміністратором або призначені динамічно за допомогою локального маршрутизатора, який обмінюється даними маршрутизації з іншими маршрутизаторами, використовуючи для цього протоколи динамічної маршрутизації.

На рис. 6.2. показані мережі з прямим підключенням і віддалені мережі маршрутизатора R1. У даному пркладі маршрузаор R1 напряму підключений до мереж 192.168.10.0/24, 192.168.11.0/24, 209.165.200.224/30. R1 також має дві віддалені мережі, дані від них він може отримати від маршрузаора R1: 10.1.1.0/24 та 10.1.2.0/24.

Рис. 6.2. Мережі з прямим підключенням і віддалені мережі маршрутизатора R1 [1]

Таблиця маршрутизації вузла включає тільки інформацію про мережі з прямим підключенням. Для відправки пакетів віддаленому адресату вузлу потрібен шлюз за замовчуванням. Таблиця маршрутизації маршрутизатора містить подібну інформацію, але також дозволяє визначити конкретні видалені мережі.

Інтерфейси з прямим підключенням мають два коди джерела маршруту.

- **C:** означає мережу з прямим підключенням. Мережі з прямим підключенням створюються автоматично, коли інтерфейс настроюється за допомогою IP -адреси і активується.
- **L:** означає маршрут локального каналу. Маршрути локального каналу створюються автоматично, коли інтерфейс настроюється за допомогою IP -адреси і активується (рис.6.3).

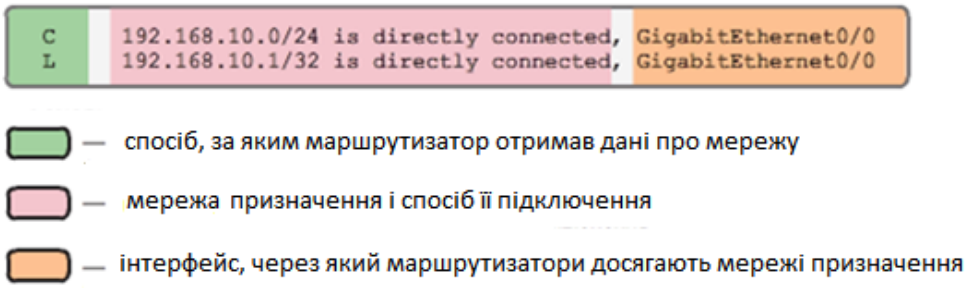


Рис.6.3. Інтерфейси маршрутизатора прямим підключенням [1]

Як правило, на маршрутизаторі налагоджено декілька інтерфейсів. У таблиці маршрутизації зберігається інформація як про маршрути з прямим підключенням, так і про віддалені маршрути. Як і для мереж з прямим підключенням, джерело маршруту визначає, яким чином був виявлений маршрут. Наприклад, до загальних кодів для віддалених мереж відносяться наступні.

- **S:** означає, що маршрут був створений вручну адміністратором, щоб досягти певної мережі. Такий маршрут називається **статичним.**
- **D:** означає, що маршрут був отриманий **динамічно** від іншого маршрутизатора з використанням протоколу EIGRP (вдосконаленого протоколу внутрішньої маршрутизації між шлюзами).
- **O:** означає, що маршрут був отриманий **динамічно** від іншого маршрутизатора з використанням протоколу маршрутизації OSPF (протоколу алгоритму найкоротшого шляху).

На рис.6.4. показаний запис таблиці маршрутизації на маршрутизаторі для маршруту до віддаленої мережі 10.1.1.0.

Рис.6.4. запис таблиці маршрутизації на маршрутизаторі для маршруту до віддаленої мережі 10.1.1.0 [1]

Запис містить наступну інформацію.

- **Джерело маршруту:** вказує спосіб отримання маршруту.
- **Мережа призначення:** вказує адреси віддаленої мережі.
- **Адміністративна відстань:** вказує достовірність джерела маршруту.
- **Метрика:** вказує значення, присвоєне для діставання доступу до віддаленої мережі. Менші значення означають пріоритетніші маршрути.
- **Наступний перехід:** вказує IP -адресу наступного маршрутизатора для пересилки пакету.
- **Відмітка часу маршруту:** вказує останню активність маршруту.
- **Вихідний інтерфейс:** вказує вихідний інтерфейс для пересилки пакетів до остаточного адресата.

Наступний перехід – це адреса пристрою, який оброблятиме наступний пакет. Для вузла в мережі адреса шлюзу за замовчуванням (інтерфейсу маршрутизатора) – це наступний перехід усіх пакетів, які необхідно відправити до іншої мережі. У таблиці маршрутизації маршрутизатора наступний перехід є для кожного маршруту до віддаленої мережі.

Коли пакет, призначений для віддаленої мережі, поступає на маршрутизатор, він порівнює мережу призначення з маршрутом, вказаним в таблиці маршрутизації. Якщо збіг знайдений, маршрутизатор пересилає пакет на IP -адресу маршрутизатора наступного переходу, використовуючи для цього інтерфейс, вказаний в записі маршруту.

Наступний перехід – це шлюз до віддалених мереж.

Мережі з прямим підключенням до маршрутизатора не мають адреси наступного переходу, оскільки маршрутизатор може пересилати пакети безпосередньо до вузлів в цих мережах за допомогою вказаного інтерфейсу.

Маршрутизатор не може пересилати пакети, якщо в таблиці маршрутизації відсутній маршрут для мережі призначення. Якщо маршрут, що означає мережу призначення, в таблиці не вказаний, пакет відкидається (тобто не пересилається).

Проте, оскільки вузол може використовувати шлюз за замовчуванням для пересилки пакету невідомому адресатові, маршрутизатор також можна нааштувати для використання статичного маршруту за замовчуванням, щоб створювати шлюз «останньої надії».

6.8. Будова і функції маршрутизатора

Незалежно від наявності функцій, розміру або складності усі моделі маршрутизаторів надзвичайно схожі з комп’ютерами. Як і комп’ютери, планшети та інтелектуальні пристрої, маршрутизатори містять наступні компоненти:

- операційна система (ОС);

- центральний процесор (ЦП);
- оперативний запам’ятовуючий пристрій (ОЗП);
- постійний запам’ятовуючий пристрій (ПЗП).

Маршрутизатор також оснащений спеціальною пам’яттю, яка включає флеш-память і незалежний запам’ятовуючий пристрій (NVRAM).

ЦП потрібна операційна система для виконання маршрутизації і комутації. ОС мережевої взаємодії Cisco (IOS) – це системне ПЗ, яке використовується для більшості пристроїв Cisco незалежно від їх розміру і типу. Вона є на маршрутизаторах, комутаторах для локальних мереж, невеликих точках безпровідного доступу, великих маршрутизаторах з великою кількістю інтерфейсів і на багатьох інших пристроях.

Не дивлячись на те, що існує декілька типів і моделей маршрутизаторів, кожен з них має ідентичні загальні апаратні компоненти.

Основні можливості маршрутизаторів:

- адресація;
- інтерфейси;
- маршрутизація;
- безпека;
- QoS;
- управління ресурсами.

Висновок до лекції 6

Мережевий рівень, або рівень 3 OSI, надає сервіси, що дозволяють крайовим пристроям обмінюватися даними по мережі. Щоб забезпечити таку передачу даних, мережевий рівень використовує чотири основні процеси: IP -адресацію крайових пристроїв, інкапсуляцію, маршрутизацію і деінкапсуляцію.

IPv4 є найбільш поширеним протоколом мережевого рівня і широко застосовується в мережі Інтернет. Пакет IPv4 містить IP -заголовок і корисне навантаження. При цьому у IPv4 є обмежена кількість доступних унікальних загальнодоступних IP -адрес. Це послужило причиною розробки IP версії 6 (IPv6). Спрощений заголовок IPv6 пропонує ряд переваг в порівнянні з IPv4, включаючи ефективнішу маршрутизацію, спрощені заголовки розширень і обробку кожного окремого потоку. Крім того, IPv6 -адреси використовують 128-бітову ієрархічну адресацію на відміну від адреси IPv4, що використовує 32 біта. Це істотно збільшує кількість доступних IP -адрес.

Мережевий рівень також відповідає за маршрутизацію. Вузлам потрібна локальна таблиця маршрутизації, щоб пакети спрямовувалися в потрібну мережу призначення. Локальна таблиця вузла, як правило, містить пряме підключення, маршрут локальної мережі та локальний маршрут за замовчуванням. Локальний маршрут за замовчуванням – це маршрут до шлюзу за замовчуванням.

Шлюз за замовчуванням – це IP -адреса інтерфейсу маршрутизатора, підключеного до локальної мережі. Коли вузлу необхідно переслати пакет на адресу призначення, яка не знаходиться в одній мережі з вузлом, пакет пересилається на шлюз за замовчуванням для подальшої обробки.

Коли маршрутизатор, такий як шлюз за замовчуванням, отримує пакет, він вивчає IP -адресу призначення для визначення мережі призначення. Таблиця маршрутизації маршрутизатора зберігає інформацію про маршрути з прямим підключенням і про віддалені маршрути. Якщо в таблиці маршрутизації є запис про мережу призначення, маршрутизатор відправляє пакет. Якщо ж подібний запис відсутній, то маршрутизатор може направити цей пакет по власному стандартному маршруту, якщо він є, або скине його.

Питання для закріплення

1. Які процеси і протоколи мережевого рівня в знаєте?
2. Які основні характеристики протоколу IPv4?
3. Які основні недоліки протоколу IPv4?
4. Які переваги протоколу IPv6?
5. Яка стуктура протоколу IPv6?
6. Що таке шлюз за замовчуванням, яке його призначення?
7. Яка структура таблиці маршрутизації
8. Яка будова і основні функції маршрутизатора?

Список рекомендованої літератури

1. CCNA R&S ITN Chapter 6: Network Layer // Електронний ресурс. Режим доступу: http://static-course-assets.s3.amazonaws.com/IntroNet50ENU/module6/index.html
2. The Internetwork Protocol (IP) // Електронний ресурс. Режим доступу: http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/ip.html
3. IPv6 // Електронний ресурс. Режим доступу: https://www.freebsd.org/doc/ru_RU.KOI8-R/books/handbook/network-ipv6.html
4. Провайдери з IPv6 // Електронний ресурс. Режим доступу: https://version6.ru/is

Лекція 7. Тема: «Транспортний рівень»

План лекції

7.1. Призначення транспортного рівня.
7.2. Протокол TCP.
7.3. Протокол UDP.
7.4. Адресація портів TCP і UDP.
7.5. Сегментація TCP і UDP.
7.6. Процеси і запити TCP –сервера.
7.7. Процеси і запити UDP –сервера.
7.8. Застосування, що використовують протоколи TCP та UDP.

7.1. Призначення транспортного рівня

Процеси, описані в транспортному рівні OSI, забезпечують прийом даних від рівня додатків і їх підготовку для пересилки на мережевому рівні. Транспортний рівень готує дані для передачі по мережі. Комп'ютер джерела встановлює зв'язок з приймаючим ПК, щоб визначити, як розділити дані на сегменти, як запобігти їх втратам і як перевірити, чи усі сегменти були доставлені.

Транспортний рівень відповідає за встановлення часового сеансу зв'язку і передачу даних між двома додатками. Додаток створює дані, які пересилаються із додатку на початковому вузлі додатку на вузлі призначення незалежно від типу вузла призначення, а також середовища, в якому повинні передаватися дані, маршрут, перевантаження каналу або розміру мережі.

Транспортний рівень забезпечує такий спосіб передачі даних по мережі, який гарантує, що на приймаючій стороні дані будуть скомпоновані без помилок. Транспортний рівень використовує розподіл даних на сегменти і пропонує елементи управління, необхідні для повторної зборки цих сегментів в різні потоки обміну даними.

У TCP/IP для виконання процесів сегментації і повторної зборки можна використовувати два абсолютно різних протоколу транспортного рівня – **TCP (**Transmission Control Protocol **, протокол управління передачею**) і **UDP (**User Datagram Protocol, **протокол користувацьких датаграм).**

Основні функції протоколів транспортного рівня:

- відстежування окремих сеансів передачі даних між додатками на вузлі-джерелі і вузлі-одержувачі;
- сегментація даних для управління ними, а також для їх повторного компонування в потоки прикладних даних на вузлі-адресатові;
- ідентифікація відповідного додатку для кожного потоку обміну даними.

На транспортному рівні кожен набір даних, що передаються між застосуванням джерела і застосуванням призначення, називається **сеансом зв'язку**. Вузол може мати декілька додатків, які одночасно обмінюються даними по мережі. Кожен з цих додатків взаємодіє з одним або декількома іншими додатками на одному або декількох віддалених вузлах. Транспортний рівень повинен підтримувати і відстежувати ці декілька сеансів зв'язку.

Дані необхідно підготувати для пересилки в середовищі у вигляді керованих частин. У більшості мереж існують обмеження на об'єм даних, які можуть бути включені в один пакет. Протоколи транспортного рівня мають сервіси, які розділяють дані застосувань на окремі блоки необхідного розміру. Такий сервіс включає інкапсуляцію, необхідну для кожної частини даних. Заголовок для повторної зборки додається до кожного блоку даних. Цей заголовок дозволяє відстежувати потік даних.

На вузлі призначення транспортний рівень має бути в змозі відновлювати окремі частини в один повний потік даних, який підходить для рівня застосувань. Протоколи на транспортному рівні описують, як використовується інформація у заголовку транспортного рівня, щоб повторно зібрати частини даних в потоки для подальшої передачі на рівень застосувань.

На кожному вузлі в мережі може бути запущено безліч застосувань або сервісів. Щоб переслати потоки даних відповідним застосуванням, транспортному рівню необхідно визначити цільове застосування. Для виконання цього завдання транспортний рівень привласнює кожному застосуванню окремий ідентифікатор. Цей ідентифікатор називається **номером порту**. Кожному програмному процесу, якому потрібно доступ до мережі, призначається номер порту, унікальний для цього вузла. Транспортний вузол використовує порти, щоб визначити відповідне застосування або сервіс.

При передачі по мережі даних деяких типів (наприклад, потокового відео) у вигляді одного повного потоку може використовуватися уся доступна смуга пропускання, що у свою чергу приведе до блокування інших процесів передачі даних, що виконуються в цей же час. Крім того, це ускладнює відновлення після помилок і повторну передачу пошкоджених даних.

Сегментація даних на дрібніші блоки дозволяє здійснювати чергування (мультиплексування) великої кількості різних процесів передачі даних між багатьма користувачами в одній і тій же мережі. Сегментація даних протоколами транспортного рівня також забезпечує можливості як для відправки, так і для отримання даних, коли на одному комп'ютері запущено декілька застосувань.

Без сегментації отримувати дані зможе тільки одне застосування. Наприклад, при передачі потокового відео усе середовище повністю використовуватиметься цим процесом, тому для інших застосувань воно буде недоступне. Робота з електронною поштою, використання програм для швидкого обміну повідомленнями або перегляду веб-сторінок одночасно з передачею відеозображення будуть неможливі.

Щоб визначити кожен сегмент даних, транспортний рівень додає до нього заголовок, який містить двійкові дані. Цей заголовок містить поля бітів. Саме значення в цих полях активують різні протоколи транспортного рівня для виконання різних функцій при управлінні передачею даних.

Транспортний рівень також відповідає за забезпечення надійності сеансу зв'язку. Різні застосування мають різні вимоги відносно надійності передачі даних.

IP -мережа відповідає тільки за структуру, адресацію і маршрутизацію пакетів. IP не визначає спосіб доставки або транспортування пакетів. Транспортні протоколи визначають спосіб передачі повідомлень між вузлами. TCP вважається надійним і повнофункціональним протоколом транспортного рівня, який забезпечує передачу усіх даних на вузол призначення. UDP на відміну від нього – дуже простий протокол транспортного рівня, що не гарантує надійність.

7.2. Протокол TCP

Як вже згадувалося раніше, TCP вважається надійним транспортним протоколом, а це означає, що він використовує процеси, які забезпечують надійну передачу даних між застосуваннями за допомогою підтвердження доставки. Передача з використанням TCP аналогічна відправці пакетів, які відстежуються від джерела до одержувача.

TCP використовує три основні операції для забезпечення надійності:

- відстежування переданих сегментів даних;
- підтвердження отриманих даних;
- повторна відправка усіх непідтверджених даних.

TCP розбиває повідомлення на фрагменти меншого розміру, які називаються **сегментами.** Цим сегментам привласнюються порядкові номери, після чого вони передаються IP - протоколу, який збирає їх в пакети. TCP відстежує кількість сегментів, відправлених на той або інший вузол тим або іншим застосуванням. Якщо відправник не отримує підтвердження впродовж певного періоду часу, то TCP розглядає ці сегменти як втрачені і повторює їх відправку. Повторно вирушає тільки втрачена частина повідомлення, а не усе повідомлення цілком. Протокол TCP на приймаючому вузлі відповідає за повторну зборку сегментів повідомлень і їх передачу відповідному застосуванню. Протокол передачі файлів (FTP) і протокол передачі гіпертексту (HTTP) – це приклади застосувань, які використовують TCP для доставки даних.

Спочатку протокол TCP був описаний в документі RFC 793. Окрім підтримки таких базових функцій, як сегментація даних і повторне компонування, протокол TCP також забезпечує:

- канали зв'язку зі встановленням з'єднання за допомогою встановлення сеансів;
- надійність доставки;
- відновлення послідовності даних;
- управління потоком.

TCP є протоколом зі встановленням з'єднання. Перед пересилкою будь-якого трафіку протокол зі встановленням з'єднання погоджує і настроює постійне з'єднання (чи сеанс) між пристроєм джерела і пристроєм призначення. Встановлення сеансу дозволяє підготувати пристрої до обміну даними один з одним. Сеанс дозволяє пристроям погоджувати об'єм трафіку, який можна переслати в заданий момент часу, а також дані, що пересилаються між ними двома, які можна безпосередньо обробити. Сеанс буде завершений тільки після виконання передачі усіх даних.

Протокол TCP може надати спосіб забезпечення надійної доставки даних. У мережевій термінології надійність означає доставку на вузол призначення кожної частини даних, відправленої вузлом джерела. Внаслідок багатьох причин при передачі по мережі одна з частин даних може бути пошкоджена або повністю втрачена. Використовуючи повторну відправку пошкоджених або втрачених даних, TCP може гарантувати, що дані повністю досягнуть свого призначення.

Оскільки в мережах можуть використовуватися декілька маршрутів з різними швидкостями передачі інформації, в процесі доставки даних їх порядок може змінитися.

Використовуючи нумерацію і впорядковування сегментів, TCP може гарантувати, що вони будуть зібрані в правильному порядку.

Такі ресурси мережевих вузлів, як пам'ять або смуга пропускання, досить обмежені. Коли протокол TCP отримує інформацію про те, що ці ресурси використовуються занадто активно, він може зажадати від відправляючого додатку зменшити швидкість потоку даних. Для цього TCP регулює кількість інформації, що передається джерелом. Управління потоком може запобігти втратам сегментів при їх проходженні по мережі і виключити необхідність повторної передачі даних.

Після того, як протокол TCP встановить сеанс, він зможе стежити за обміном даними, що відбувається у рамках цього сеансу. Завдяки здатності TCP відстежувати фактичні сеанси зв'язку він вважається протоколом з контролем стану. Протокол з контролем стану відстежує стан сеансу передачі даних. Наприклад, коли дані передаються по протоколу TCP, відправник чекає, що вузол призначення відправить підтвердження про отримання даних. TCP відстежує, яку інформацію він відправив і яка інформація була підтверджена. Якщо отримання даних не підтверджене, відправник вважає, що дані не досягли адресата, і повторює їх відправку. Сеанс зв'язку з контролем стану починається зі встановлення сеансу обміну даними і припиняється після його завершення.

Для обробки інформації про стан потрібні ресурси, які не потрібні протоколу без контролю стану, наприклад, UDP. При використанні цих функцій протокол TCP створює додаткове навантаження. Кожен сегмент TCP містить 20 додаткових байт в заголовку, інкапсулюючи дані рівня додатків. Це істотно перевищує значення сегменту UDP, в якому містяться 8 додаткових байт. Додаткове навантаження складається з наступних елементів.

- **Порядковий номер (32 біта):** використовується для повторного компонування даних.
- **Номер підтвердження (32 біта):** означає отримані дані.
- **Довжина заголовка (4 біта):** параметр, який також називається зміщенням даних. Означає довжину заголовка сегменту TCP.
- **Зарезервовано (6 біт):** поле, зарезервоване для наступного використання.
- **Біти управління (6 біт):** включає двійкові коди, або прапори, які вказують призначення і функцію сегменту TCP.
- **Розмір вікна (16 біт):** відображує кількість сегментів, які можна прийняти одноразово.
- **Контрольна сума (16 біт):** використовується для перевірки помилок заголовка і даних сегменту.
- **Терміновість (16 біт):** означає, чи є дані терміновими.

7.3. Протокол UDP

Тоді як функції надійності TCP забезпечують стабільнішу взаємодію між застосуваннями, вони також споживають більше ресурсів і можуть стати причиною затримок при передачі даних. Існує деякий компроміс між надійністю і тим навантаженням, яке вона представляє для мережевих ресурсів. Додаткове навантаження для забезпечення надійності деяких застосувань може понизити корисність самого застосування і навіть негативно позначитися на його продуктивності. У таких випадках використання протоколу UDP прийнятніше.

UDP забезпечує тільки основні функції для відправки сегментів даних між відповідними застосуваннями, при цьому використовуючи небагато ресурсів. UDP відомий як протокол негарантованої доставки даних. Стосовно комп'ютерних мереж негарантована доставка вважається ненадійною, оскільки при цьому відсутнє підтвердження про отримання відправлених даних на вузлі призначення. UDP не задіює процеси транспортного рівня, які повідомляють відправника про успішну доставку даних.

Протокол UDP подібний до того, начебто поштою відправляли звичайний незареєстрований лист. Відправник не знає, чи зможе адресат отримати лист, а поштове

відділення не несе відповідальності за відстежування листа або інформування відправника про те, чи доставлений лист за адресою.

Протокол UDP описаний в документі RFC 768. Це полегшений транспортний протокол, який пропонує таку ж сегментацію і повторну зборку даних, як і протокол TCP, але при цьому не забезпечує надійність і управління потоком, властиві TCP.

Наступні функції являються характерними для протоколу UDP.

- **Без встановлення з'єднання.** UDP не встановлює з'єднання між вузлами до того, як стануть можливими відправка і отримання даних.
- **Ненадійна доставка.** UDP не використовує сервіси, що забезпечують надійну доставку даних. Протокол UDP не використовує процеси, які вимагають від відправника повторної передачі втрачених або пошкоджених даних.
- **Без відновлення послідовності даних.** Періодично дані поступають не в тому порядку, в якому вони були відправлені. Протокол UDP не передбачає засобів для повторної зборки даних в їх початковій послідовності. Дані просто вирушають застосуванню в тій послідовності, в якій вони поступають.
- **Без управління потоком.** У UDP відсутні механізми для управління об'ємами даних, які пересилаються джерелом, для запобігання перевантаженням на пристрої призначення. Джерело відправляє дані. У разі надмірного використання ресурсів на вузлі призначення він, швидше за все, відхилятиме відправлені дані до тих пір, поки ресурси не стануть доступними. На відміну від TCP, протокол UDP не має механізмів повторної автоматичної передачі відхилених даних.

Фрагменти даних в протоколі UDP називаються **датаграмами**. Ці датаграми вирушають без гарантії доставки зусиллями протоколу транспортного рівня. Серед застосувань, які використовують протокол UDP, можна назвати службу доменних імен (DNS), передачу потокового відео і передачу голосової інформації по протоколу IP (VoIP).

Однією з основних вимог для передачі відео і голосу по мережі в режимі реального часу є наявність постійного високошвидкісного потоку. Застосування для передачі відео і голосу допускають втрати деякої кількості даних, які будуть ледве помітні або непомітні зовсім, і чудово підходять для використання протоколу UDP.

UDP – це протокол без контролю стану, а це означає, що ні клієнт, ні сервер не зобов'язані відстежувати стан сеансу зв'язку. Протокол UDP не забезпечує надійність або управління потоком. Дані можуть бути втрачені або отримані не по порядку, а UDP не має яких-небудь механізмів для відновлення або переупорядковування даних.

Як TCP, так і UDP є ефективними транспортними протоколами. Залежно від вимог застосувань можна використовувати будь-який з них (а в деяких випадках – навіть обоє). На підставі цих вимог розробники застосувань повинні визначити, який транспортний протокол підходить для них краще всього.

Деяким застосуванням необхідно, щоб сегменти передаваних даних поступали в строго певній послідовності, в якій вони можуть бути успішно оброблені. Іншим застосуванням потрібно, щоб усі дані були отримані повністю, інакше вони не вважатимуться придатними для використання. У обох цих випадках TCP використовується в якості транспортного протоколу. Наприклад, таким застосуванням, як бази даних, веб-браузери і клієнтські програми для роботи з електронною поштою необхідно, щоб усі відправлені дані поступили на вузол призначення у своєму первинному стані. Відсутність якої-небудь інформації може привести до ушкодження даних, які у такому разі будуть передані не повністю або будуть нечитаними. Тому ці застосування розроблялися виключно для роботи по протоколу TCP. Такі застосування створюють додаткове навантаження на мережу.

У інших випадках втрата деяких даних під час передачі по мережі може бути допустима для застосування, але при цьому затримки передачі є неприпустимими. Таким застосуванням краще використовувати протокол UDP, оскільки він задіює менше мережевих ресурсів. Протокол UDP прийнятніший для потокового відтворення аудіо, відео і передачі голосової

інформації по протоколу IP (VoIP). Підтвердження доставки тільки уповільнить процес передачі даних, але при цьому повторна доставка небажана.

Ще одним прикладом застосування, яке використовує протокол UDP, є інтернет-радіо. Якщо яке-небудь повідомлення загубилося в дорозі доставки по мережі, воно не вирушатиме повторно. Втрата декількох пакетів сприйматиметься слухачем як короткочасна втрата звуку. Якщо для цього використовувати протокол TCP, що передбачає повторну доставку втрачених пакетів, то процес передачі даних припиниться для прийому втрачених пакетів, що помітно погіршить якість відтворення.

7.4.Адресація портів TCP і UDP

У заголовку кожного сегменту або датаграми вказуються порти джерела і призначення. Номер порту джерела – це номер для цього обміну даними, пов'язаний з відправляючим застосуванням на локальному вузлі. Номер порту призначення – це номер для цього обміну даними, пов'язаний з приймаючим застосуванням на локальному вузлі.

При доставці повідомлення по протоколу TCP або UDP запрошувані протоколи і сервіси розпізнаються по номеру порту. **Порт** – це числовий ідентифікатор усередині кожного сегменту, який використовується для обліку окремих сеансів зв'язку і запрошених сервісів призначення. У кожному повідомленні, що відправляється з вузла, вказуються порт джерела і порт призначення.

Клієнт вказує номер порту призначення в сегменті, щоб повідомити серверу призначення інформацію про те, який сервіс проситься. Наприклад, порт 80 означає протокол HTTP або веб-сервіс. Сервер може надавати декілька сервісів одночасно. Наприклад, сервер може надавати веб-сервіс через порт 80 і одночасно послуги обміну файлами по протоколу FTP через порт 21.

Номер порту джерела випадково генерується пристроєм-відправником для ідентифікації сеансу зв'язку між двома пристроями. Це дозволяє встановлювати одночасно декілька сеансів зв'язку. Іншими словами, пристрій може передавати на веб-сервер декілька запитів сервісу HTTP в один і той же час. Окремі сеанси зв'язку відстежуються по номерах портів джерела.

Номери порту джерела і порту призначення записуються в сегмент. Потім ці сегменти інкапсулюються в пакеті IP. У пакеті IP записується IP –адреси джерела і призначення.

Комбінація IP -адрес джерела і призначення, а також номерів портів джерела і призначення називається **сокетом**. Сокет використовується для визначення сервера і сервісів, що просить клієнт. Щодня мільйони вузлів взаємодіють з тисячами різних серверів. Їх взаємодії визначаються за допомогою сокетів.

Сокет клієнта може мати вигляд 192.168.1.5:1099, де 1099 – це номер порту джерела.

Сокет веб-сервера може мати наступний вигляд: 192.168.1.7:80

Разом ці два сокети утворюють пару: 192.168.1.5:1099, 192.168.1.7:80

В результаті створення сокетів стають відомі кінцеві точки з'єднання, і дані можуть передаватися між застосуваннями на двох вузлах. Сокети дозволяють розрізняти декілька процесів, що виконуються на клієнтові, а також розпізнавати різні підключення до процесу сервера.

Запит клієнта порту джерела генерується випадково. Цей номер порту грає роль зворотної адреси для запрошуваного застосування. Транспортний рівень відстежує порт і застосування – джерело запиту, щоб після повернення відповіді його можна було переслати відповідному застосуванню.

Номери портів привласнюються Адміністрацією адресного простору Інтернет (IANA).

Існує декілька типів номерів портів.

- **Відомі порти (номери 0 - 1023).** Ці номери зарезервовані для сервісів і застосувань. Вони зазвичай використовуються для таких застосувань, як HTTP (веб-сервер), IMAP (протокол доступу до повідомлень в Інтернеті), SMTP (сервер електронної пошти) і Telnet.

Якщо ці загальновідомі порти визначаються серверними застосуваннями, то клієнтські застосування можна запрограмувати так, щоб вони просили підключення до цього конкретного порту і пов'язаним з нею сервісом.

- **Зареєстровані порти (номери 1024 - 49151).** Ці номери портів привласнюються процесам або застосуванням користувачів. Ці процеси в основному є окремими застосуваннями, встановленими користувачем, а не загальними застосуваннями, які могли б отримати загальновідомий номер порту. Якщо ці порти не використовуються для одного з ресурсів сервера, вони можуть бути вибрані клієнтом динамічно в якості свого порту джерела.
- **Динамічні або приватні порти (номери 49152-65535).** Як правило, ці порти, які також називаються тимчасовими, динамічно привласнюються клієнтським застосуванням, коли клієнт ініціює підключення до сервісу. Динамічний порт найчастіше використовується для визначення клієнтського застосування під час обміну даними, тоді як клієнт використовує загальновідомий порт, щоб визначити і встановити підключення до сервісу, який проситься на сервері. Клієнт рідко підключається до сервісу, використовуючи динамічний або приватний порт (хоча деякі програми для обміну файлами в однорангових мережах дійсно використовують ці порти).

7.5. Сегментація TCP і UDP

Розподіл даних на сегменти забезпечує пересилку даних в межах середовища та можливість мультиплексування різних застосувань в середовищі передачі.

Кожен заголовок сегменту TCP містить порядковий номер, який дозволяє функціям транспортного рівня на вузлі призначення повторно зібрати сегменти в тому порядку, в якому вони були відправлені. Це гарантує, що застосування призначення отримує дані точно в такій же формі, в якій вони були створені відправником.

Не дивлячись на те, що сервіси, які використовують протокол UDP, також відстежують сеанси зв'язку між застосуваннями, вони не враховують порядок, в якому інформація була передана, а також не забезпечують збереження підключення. У заголовку UDP порядковий номер не вказується. Протокол UDP має простішу конструкцію і створює менше навантаження в порівнянні з TCP, що дозволяє збільшити швидкість передачі даних.

Інформація може поступити в порядку, відмінному від переданого спочатку, оскільки різні пакети можуть проходити по різних маршрутах в мережі. Застосування, яке використовує протокол UDP, повинне допускати можливість вступу даних в іншому порядку.

7.6. Процеси і запити TCP-сервера

Процеси застосувань запускаються на серверах. На одному сервері одночасно можуть бути запущені декілька процесів застосувань. Ці процеси чекають, коли клієнт ініціює обмін даними, відправивши запит на отримання інформації або інших сервісів.

Кожен процес застосування, запущений на сервері, налаштовується на використання номера порту, встановленого за замовчуванням або введеного вручну системним адміністратором. На окремому сервері не можуть використовуватися два сервіси, яким призначений один і той же номер порту у рамках одних і тих же сервісів транспортного рівня. Застосування веб-сервера і застосування передачі файлів, які запущені на одному вузлі, не можуть бути налаштовані на використання одного і того ж порту (наприклад, TCP - порту 8080).

Активне серверне застосування, якому присвоєний який-небудь порт, вважається відкритим, що означає, що транспортний рівень може приймати і обробляти сегменти, що направляються на цей порт. Будь-який вхідній запит, який адресований правильному сокету, буде прийнятий, а дані будуть передані застосуванню сервера. Сервер може мати декілька

портів, відкритих одночасно, по одному для кожного активного застосування сервера. Як правило, сервер надає декілька сервісів одночасно (наприклад, веб-сервер і FTP -сервер).

Один із способів підвищити безпеку на сервері – надати доступ тільки до портів, пов'язаних з тими сервісами і застосуваннями, які мають бути доступні авторизованим сторонам.

У деяких країнах при зустрічі двох чоловіків прийнято обмінюватися рукостисканнями. Рукостискання розглядається обома сторонами як сигнал для дружнього вітання. Підключення в мережі здійснюються приблизно так же. При першому рукостисканні вирушає запит синхронізації. При другому рукостисканні первинний запит синхронізації підтверджується, після чого узгоджуються параметри підключення в протилежному напрямі. Третій етап рукостискання – це підтвердження, яке використовується для інформування вузла призначення про те, що обидві сторони згодні встановити підключення.

Якщо два вузли взаємодіють з використанням протоколу TCP, з'єднання встановлюється до того, як обмін даними буде можливий. Після закінчення обміну даними усі сеанси припиняються, а з'єднання уривається. Механізми підключення і здійснення сеансу зв'язку включають функції TCP, що забезпечують надійність.

Вузли відстежують кожен сегмент даних, що передаються під час сеансу, і обмінюються інформацією про отримані дані з використанням відомостей у заголовку TCP. TCP – це повнодуплексний протокол, в якому кожне з'єднання представляє два односторонні потоки обміну даними, або сеансу. Для встановлення зв'язку вузли використовують трибічне рукостискання. Біти управління в заголовку TCP означають етап і стан підключення. При трибічному рукостисканні виконуються наступні процеси.

- Спочатку встановлюється, чи є присутнім пристрій призначення в мережі.
- Потім перевіряється, чи є на пристрої призначення активний сервіс і чи приймає він запити на номер порту призначення, який клієнт, що ініціює, планує використовувати для сеансу.
- Далі пристрою призначення повідомляється, що клієнт джерела планує встановити сеанс зв'язку на цьому номері порту.

У процесі трибічного рукостискання заголовок сегменту TCP містить шість 1-бітових полів з контрольною інформацією, яка використовується для управління процесами TCP. Ці поля приведені нижче.

- **URG -** поле «Покажчик важливості» задіяно.
- **ACK -** поле «Номер підтвердження» задіяно.
- **PSH -** проштовхнути дані.
- **RST -** обірвати з'єднання.
- **SYN -** синхронізувати порядкові номери.
- **FIN -** більше немає даних від відправника.

Поля ACK і SYN мають відношення до даного аналізу трибічного рукостискання. На рис.7.2 наведено схема трибічного рукостискання TCP при взаємодії клієнта та сервера.

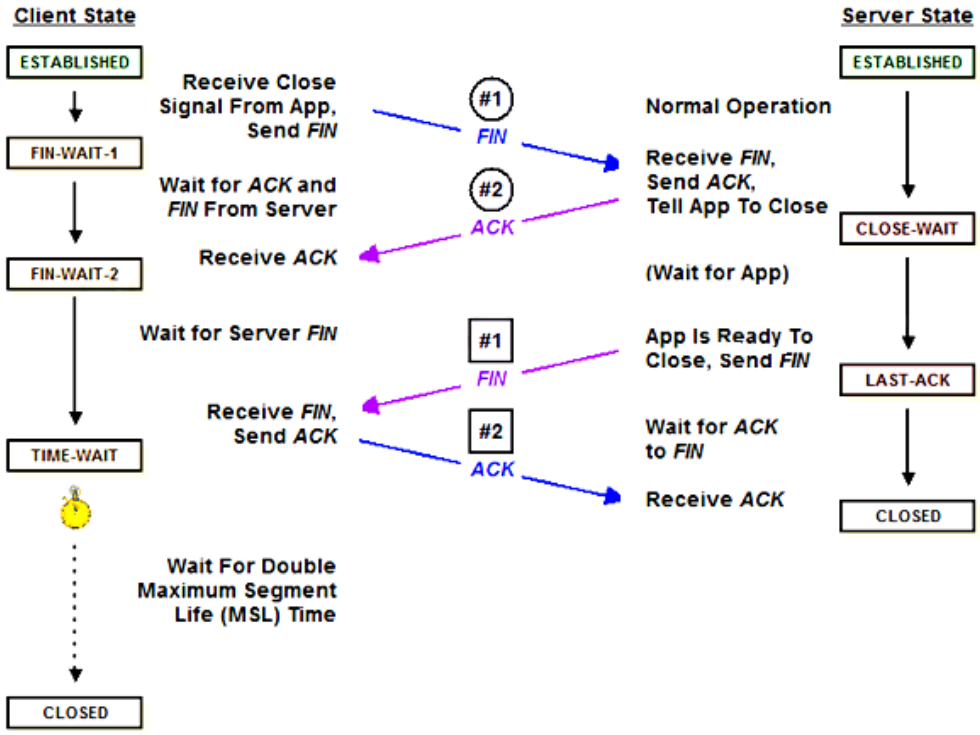


Рис. 7.2. Процес трибічного рукостискання TCP

Коли сервіси відправляють дані по протоколу TCP, сегменти можуть бути доставлені на вузол призначення у зміненому порядку. Щоб одержувач зміг розшифрувати первинне повідомлення, дані в цих сегментах повторно збираються у початковому порядку. Для цього в заголовку кожного пакету вказуються порядкові номери.

Під час налаштування сеансу зв'язку встановлюється початковий порядковий номер сеансу (ISN). Цей номер ISN представляє початкове значення байтів для цього сеансу, яке передається одержуючому застосуванню. У міру передачі даних під час сеансу порядковий номер збільшується на число переданих байт. Таке відстежування байтів даних дозволяє однозначно визначати і підтверджувати кожен сегмент, можна з'ясувати, які сегменти відсутні.

Порядкові номери сегментів забезпечують надійність, вказуючи, як необхідно повторно зібрати і переупорядкувати отримані сегменти.

TCP-процес поміщає дані з сегменту в одержуючий буфер. Сегменти розташовуються відповідно до порядкових номерів і після повторної зборки передаються на рівень застосувань. Усі сегменти, які поступають з невідповідними порядковими номерами, зберігаються для наступної обробки. Потім, поступаючи з відсутніми байтами, сегменти обробляються по порядку.

Однією з функціональних особливостей протоколу TCP є гарантія доставки кожного сегменту за призначенням. Сервіси TCP на вузлі призначення підтверджують дані, отримані їм від застосування джерела. Порядковий номер (SEQ) і номер підтвердження (ACK) використовуються спільно для підтвердження отримання байтів даних, які містяться в переданих сегментах. Порядковий номер SEQ означає відносне число байтів, переданих під час цього сеансу, включаючи байти в поточному сегменті. TCP використовує номер ACK, відправлений назад джерелу, щоб позначити наступний байт, який одержувач розраховує отримати. Це називається **очікуваним підтвердженням.**

Джерелу повідомляється, що вузол призначення отримав усі дані в цьому потоці до того байта (але не включаючи його), який позначений номером ACK. Передбачається, що передавальний вузол відправить сегмент, в якому використовується порядковий номер, рівний номеру ACK. Обмін номерами SEQ і ACK здійснюється в обох напрямах.

Кількість даних, яка може бути передана до отримання підтвердження, називається **розміром вікна.** Розмір вікна – це поле в заголовку TCP, за допомогою якого можна обробляти втрачені дані і управляти потоками.

Як би добре не була організована мережа, в ній час від часу трапляються втрати даних; з цієї причини протокол TCP передбачає способи управління цими втратами сегментів. Серед них – механізм для повторної передачі сегментів з непідтвердженими даними.

Сервіс вузла призначення, що використовує протокол TCP, зазвичай підтверджує тільки дані, що поступили в безперервній послідовності. У разі відсутності одного або декількох сегментів підтверджуються тільки дані в першій безперервній послідовності байтів. Наприклад, якщо були отримані сегменти з порядковими номерами від 1500 до 3000 і від 3400 до 3500, номером ACK буде 3001. Це пов'язано з тим, що є сегменти з номерами SEQ від 3001 до 3399, які не були отримані.

Якщо TCP на вузлі джерела не отримає підтвердження після закінчення встановленого періоду часу, він повернеться до останнього отриманого номера ACK і повторно перешле дані з цієї точки. При типовій реалізації протоколу TCP вузол може переслати сегмент, помістити копію сегменту в чергу для повторної передачі і запустити таймер. Після отримання підтвердження даних сегмент видаляється з черги. Якщо підтвердження не поступає до витікання часу таймера, сегмент пересилається повторно.

Протокол TCP також забезпечує механізми для управління потоком даних. Управління потоком дозволяє підтримувати надійність передачі по протоколу TCP шляхом регулювання швидкості потоку даних між вузлами джерела і напряму впродовж певного сеансу. Управління потоком здійснюється шляхом обмеження кількості сегментів даних, що передаються за один раз, а також запитів підтверджень отримання до відправки наступних сегментів.

Протокол TCP використовує розмір вікна, щоб спробувати управляти швидкістю передачі даних відповідно до максимального значення потоку, яке підтримується мережею і пристроєм призначення, одночасно з цим зменшуючи втрати даних і кількість їх повторних пересилок.

Ще одним способом управління потоком даних є використання динамічних розмірів вікон. Коли мережеві ресурси обмежені, TCP може зменшити розмір вікна, щоб зажадати частішого підтвердження отримання сегментів. Це дозволяє ефективно понизити швидкість передачі даних, оскільки джерело частіше чекає підтвердження їх отримання.

Приймаючий вузол посилає значення розміру вікна на відправляючий вузол, щоб вказати кількість байт, яку він готовий прийняти. Якщо вузлу призначення необхідно понизити швидкість передачі даних через обмежену пам'ять буфера, він може, наприклад, пересилати вузлу джерела менше значення розміру вікна як частину підтвердження.

7.7. Процеси і запити UDP -сервера

UDP – протокол, який забезпечує базові функції транспортного рівня. Він характеризується істотно меншими навантаженнями в порівнянні з протоколом TCP; він не використовує встановлення з'єднання і не пропонує складні механізми повторної передачі даних, впорядковування і управління потоком, які забезпечують надійність.

Це зовсім не означає, що застосування, які використовують UDP, завжди ненадійні, або що UDP – неповноцінний протокол. Це лише означає, що функції забезпечення надійності не реалізуються протоколом транспортного рівня і при необхідності мають бути реалізовані на інших рівнях.

Не дивлячись на те, що UDP-трафік зазвичай складає невелику долю загального мережевого трафіку, UDP використовуєть наступні важливими протоколи рівня застосувань:

- служба доменних імен (DNS)і
- простий протокол управління мережею (SNMP);
- протокол DHCP;

- протокол RIP;
- простий протокол передачі файлів (TFTP);
- IP -телефонія або передача голосової інформації по протоколу IP (VoIP);
- онлайн-ігри.

Оскільки UDP є протоколом без встановлення з'єднання, перед початком з'єднання сеанси зв'язку не встановлюються, як це відбувається у випадку з протоколом TCP. Вважається, що в основі протоколу UDP лежать транзакції; іншими словами, якщо у застосування є дані для відправки, воно просто посилає їх.

Коли на вузол призначення вирушають декілька датаграм, вони можуть використовувати різні шляхи і прибути в неправильному порядку. Протокол UDP не відстежує порядкові номери, як це робить TCP. Таким чином, протокол UDP просто повторно збирає дані в тому порядку, в якому вони були прийняті, і пересилає їх застосуванню. Якщо послідовність даних важлива для роботи застосування, воно повинне визначити правильну послідовність і вибрати оптимальний спосіб обробки даних.

Як і застосуванням, що використовують протокол TCP, серверним застосуванням на основі протоколу UDP привласнюються відомі або зареєстровані номери портів. Коли ці застосування або процеси запущені на сервері, вони приймають дані, що співпадають з присвоєним номером порту. Якщо UDP отримує датаграму, адресовану одному з цих портів, він пересилає ці застосування відповідному застосуванню виходячи з його номера порту.

Як і у випадку з TCP, обмін даними між клієнтом і сервером ініціюється клієнтським застосуванням, яке просить дані з серверного процесу. Процес UDP-клієнта випадковим чином вибирає номер порту з діапазону динамічних номерів портів і використовує його як порт джерела для сеансу зв'язку. Як правило, порт призначення – це відомий або зареєстрований номер порту, присвоєний процесу сервера.

Випадкові номери портів джерела також допомагають підвищити безпеку. За наявності передбачуваної моделі для вибору порту призначення зловмисникові простіше змоделювати доступ до клієнта, спробувавши підключитися до номера порту, який, найімовірніше, буде відкритий.

Оскільки при використанні протоколу UDP після підготовки даних до відправки і визначення портів сеанси не створюються, UDP може скласти датаграми і переслати їх на мережевий рівень для визначення адреси і пересилки по мережі. Після того, як клієнт вибрав порти джерела і призначення, ця ж пара портів буде вказана у заголовку усіх датаграм, які використовуються в процесі пересилки. Щоб сервер міг повернути дані клієнтові, номери портів джерела і призначення в заголовку датаграми вказуються в зворотному порядку.

7.8. Застосування, що використовують протоколи TCP та UDP

Багатьом застосуванням потрібна надійність та інші сервіси, які забезпечуються протоколом TCP. TCP краще всього підходить для застосувань, яким потрібна надійна передача даних і які допускають деякі затримки. Протокол TCP – це відмінний приклад того, як різні рівні набору протоколів TCP/IP можуть виконувати певні ролі. Оскільки протокол транспортного рівня TCP обробляє усі завдання, пов'язані з розподілом потоку даних на сегменти, забезпеченням надійності, управлінням потоком і повторним компонуванням сегментів, він звільняє застосування від виконання усіх цих завдань. Застосування може просто відправити потік даних протоколу транспортного рівня і використовувати сервіси TCP.

Можна виділити наступні приклади відомих застосувань, що використовують TCP (рис. 7.3):

- HTTP (протокол передачі гіпертексту);
- FTP (протокол передачі файлів);
- SMTP (протокол простої передачі електронної пошти);
- Telnet.

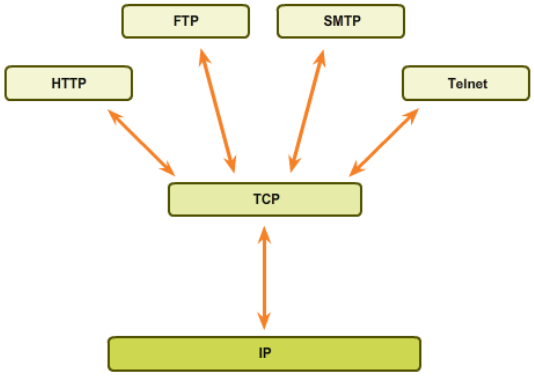


Рис. 7.3. Додатки, що використовують протокол TCP [1]

Існують три типи застосувань, які найбільш усього підходять для роботи з протоколом UDP,:

- застосування, які допускають втрату деяких даних, але для яких важлива невелика кількість затримок або повна їх відсутність;
- застосування з простими операціями відправки запитів і отримання відповідей;
- однонапрямлені потоки даних, при яких надійність не потрібна або може бути забезпечена застосуванням.

Протокол UDP використовують багато застосувань для передачі відео і мультимедійних даних, наприклад IP-телефонія та інтернет-телебачення. Ці застосування допускають втрати деякої кількості даних, які будуть ледве помітні або непомітні зовсім. Внаслідок використання механізмів забезпечення надійності, які передбачені в TCP, можливе помітне погіршення якості передаваного зображення і звуку. Інші застосування, які оптимально підходять для використання протоколу UDP, використовують прості операції по відправці запитів і отримання відповідей. Під цим розуміється ситуація, коли вузол відправляє запит, відповідь на який, можливо, поступить, а можливо, і ні. До таких застосувань відносяться (рис. 7.4):

- DHCP;
- DNS (може також використовувати TCP);
- SNMP;
- TFTP.

Деякі застосування забезпечують надійність самостійно. Таким застосуванням сервіси TCP не потрібен, і використання UDP в якості протоколу транспортного рівня для них буде прийнятнішим. TFTP – один з прикладів протоколу такого типу. Протокол TFTP має власні механізми для управління потоком даних, виявлення помилок і відновлення після них, а також відправки підтверджень. Він не потребує використання TCP для цих сервісів.

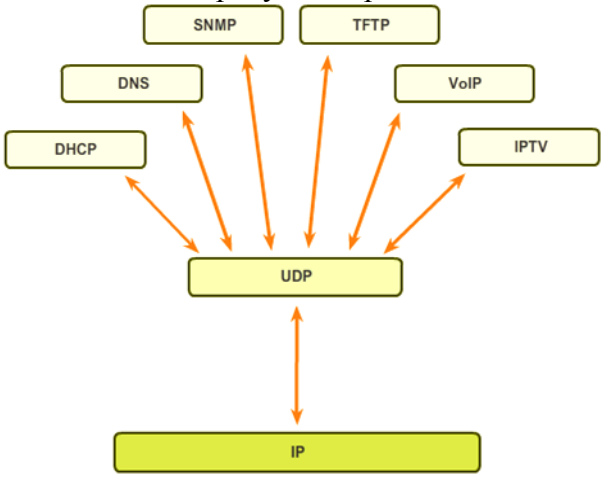


Рис. 7.4. Додатки, що використовують протокол UDP [1]

Висновок до лекції 7

Транспортний рівень надає сервіси для доставки даних, використовуючи наступні операції:

- розподіл на сегменти даних, отриманих від застосування;
- додавання заголовка для визначення кожного сегменту і управління ним;
- використання інформації у заголовку для повторної зборки сегментів в ці застосування;
- передача скомпонованих даних відповідному застосуванню.

UDP і TCP – це поширені протоколи транспортного рівня. Датаграми UDP і сегменти TCP мають заголовки, додані перед даними; вони включають номер порту джерела і номер порту призначення. Такі номери портів дозволяють направляти дані відповідному застосуванню, яке запущене на кінцевому комп'ютері. Протокол TCP не відправляє дані в мережу до тих пір, поки не отримає підтвердження готовності вузла призначення прийняти їх. Після цього TCP обробляє потік даних і повторно пересилає усі сегменти, які не були підтверджені як отримані вузлом призначення.

Щоб забезпечити надійність, TCP використовує процес рукостискання, таймери, повідомлення підтверджень і динамічну зміну вікна. Проте, забезпечення надійності призводить до додаткових навантажень на мережу, оскільки вимагає використання великих заголовків сегментів і пересилки більшої кількості трафіку між вузлами джерела і призначення.

Якщо потрібна швидка доставка даних застосування по мережі, або якщо пропускна спроможність мережі не в змозі підтримувати додаткове навантаження, пов'язане з пересилкою управляючих повідомлень, між системами джерела і призначення, тоді UDP буде прийнятнішим протоколом транспортного рівня для розробників. Оскільки UDP не відстежує або не підтверджує отримання датаграм на вузлі призначення (а просто передає отримані датаграми на рівень застосувань у міру їх поступання), він не відправляє втрачені датаграми повторно.

Питання для закріплення

1. Яке призначення та основні функції транспортного рівня?
2. Які переваги протоколу TCP?
3. Які переваги протоколу UDP?
4. Які особливості адресації портів TCP і UDP?
5. Які типи номерів портів ви знаєте?
6. Як відбувається сегментація TCP і UDP?
7. Які особливості процесів і запитів TCP –сервера?
8. Які особливості процесів і запитів UDP –сервера?
9. Назвіть застосування, що використовують протоколи TCP та UDP.

Список рекомендованої літератури

1. CCNA R&S ITN Chapter 7: Transport Layer // Електронний ресурс. Режим доступу: http://static-course-assets.s3.amazonaws.com/IntroNet50ENU/module7/index.html
2. Транспортний рівень. Функції та приклади протоколів // Електронний ресурс. Режим доступу: http://www.znanius.com/3592.html
3. What's the Difference Between TCP and UDP? // Електронний ресурс. Режим доступу: https://www.howtogeek.com/190014/htg-explains-what-is-the-difference-between-tcp-and-udp/

Лекція 8. Тема: «IP-адресація. Розбиття IP-мережі на підмережі»

План лекції

8.1. Мережева і вузлова частини IPv4 -адреси.
8.2. Побітова операція І.
8.3. Одноадресна, широкомовна та багатоадресна передача
8.4. Публічні та приватні IPv4 –адреси.
8.5. Застаріла класова адресація, її обмеження. Безкласова адресація.
8.6. Привласнення IP –адрес.
8.7. Потреба в IPv6. Представлення IPv6.
8.8. Розбиття мережі на підмережі

8.1 Мережева і вузлова частини IPv4 -адреси

Розуміння двійкової системи числення необхідне для того, щоб встановити, чи знаходяться два вузли в одній і тій же мережі. IP -адреса є ієрархічною адресою, яка складається з двох частин: мережевої і вузлової. У 32-бітовому потоці одна частина бітів складає мережу, а інша – вузол. Біти в мережевій частині адреси мають бути однаковими для усіх пристроїв, які знаходяться в одній і тій же мережі. Біти у вузловій частині адреси мають бути унікальними, щоб можна було визначити конкретний вузол в мережі. Незалежно від того, чи співпадають десяткові числа в двох IPv4 -адресах, якщо два вузли мають одну бітову комбінацію в певній мережевій частині 32-бітового потоку, то ці два вузли знаходяться в одній і тій же мережі.

При налаштуванні IP -вузла йому привласнюється не лише IP -адреса, але і маска підмережі. Як і IP -адреса, маска складається з 32 біт. Вона визначає, яка частина IP -адреси відноситься до мережі, а яка – до вузла. Маска порівнюється з IP -адресою побітно, зліва направо. У масці підмережі одиниці відповідають мережевій частині, а нулі – адресі вузла (рис. 8.1).

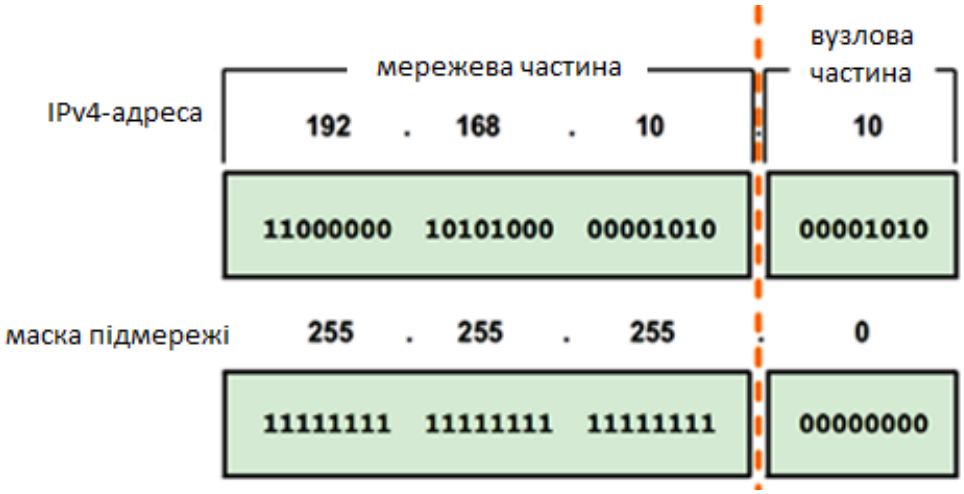


Рис. 8.1. Мережева і вузлова частини IP –адреси [1]

Як і IPv4 -адреса, маска підмережі для простоти використання представлена в десятковому форматі з розділовими крапками. Маска підмережі налагоджена на вузловому пристрої у поєднанні з IPv4 -адресою і потрібна для того, щоб вузол міг визначити, до якої мережі він належить. В табл.8.1. наведено допустимі маски підмережі для IPv4 -октета.

Табл. 8.1.Допустимі маски підмережі

Значення підмережі	Значення біта							
	128	**64**	**32**	**16**	**8**	**4**	**2**	**1**
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

Довжина префікса – це ще один спосіб представлення маски підмережі. Довжина префікса означає кількість біт, встановлених на одиницю (1) в масці підмережі. Вона позначається похилою риска вправо («/»), після якої йде набір одиниць. Наприклад, якщо маска підмережі 255.255.255.0, то в двійковій версії маски підмережі на одиницю налаштовані 24 біта, тому довжина префікса складає 24 біта або /24. Префікс і маска підмережі – це різні способи представлення одного і того ж – мережевої частини адреси.

Мережам не завжди призначається префікс /24. Залежно від кількості вузлів в мережі префікс може відрізнятися. Різний префікс призводить до зміни діапазону вузлів і широкомовної адреси для кожної мережі.

У діапазоні адрес кожної мережі IPv4 існують три типи адрес:

- мережева адреса;
- вузлові адреси;
- широкомовна адреса.

Мережева адреса – це стандартний спосіб позначення мережі. Маска підмережі або довжина префікса можуть використовуватися для позначення мережевої адреси. Для обміну даними по мережі кожному крайовому пристрою потрібна унікальна адреса. У IPv4 -адресах значення між мережевим і широкомовним адресами можуть бути призначені крайовим пристроям в мережі.

Широкомовна IPv4 -адреса – це особлива адреса для кожної мережі, яка здійснює зв'язок для усіх вузлів, розташованих в цій мережі. Для одноразової відправки даних на усі вузли в мережі вузол може відправити один пакет, призначений широкомовній адресі мережі, а кожен вузол в цій мережі, який отримає цей пакет, обробить його вміст.

Для широкомовної розсилки використовується найвища адреса діапазону мережі. У цій адресі усі частини вузла представлені одиницями. Сума одиниць октету в двійковій формі дорівнює значенню 255 в десятковому форматі. Вузлова частина не завжди представлена усім октетом цілком. Також цю адресу називають прямою **широкомовною розсилкою.**

Щоб упевнитися, що усім вузлам в мережі присвоєна унікальна IP -адреса усередині діапазону мережі, спочатку треба визначити адреси першого і останнього вузлів. У цьому діапазоні вузлам усередині мережі можуть бути присвоєні IP -адреси. Вузлова частина останньої адреси вузла міститиме усі одиниці з нулем в крайньому справа біті. Значення цієї адреси завжди на одиницю менше, ніж значення широкомовної адреси.

8.2. Побітова операція I

Якщо пристрою призначена IPv4 -адреса, то цей пристрій використовує маску підмережі, щоб визначити, до якої мережевої адреси він належить. Мережева адреса представляє усі пристрої в одній і тій же мережі.

При відправці даних по мережі пристрій використовує цю інформацію, щоб визначити, чи може він пересилати пакети локально, або він повинен відправляти пакети на шлюз за

замовчуванням для віддаленої відправки. Коли вузол відправляє пакет, він порівнює мережеві частини власної IP -адреси і IP -адреси призначення, яка залежить від маски підмережі. Якщо біти мережевої частини співпадають, значить, вузли джерела і призначення знаходяться в одній і тій же мережі, і пакет доставляється локально. Якщо біти не співпадають, відправляючий вузол передає пакет на шлюз за замовчуванням для відправки в іншу мережу.

Операція І – одна з трьох основних двійкових операцій в дискретній логіці. Крім того, існують операції АБО і НЕМАЄ. Хоча усі вони використовуються в мережах передачі даних, операція І використовується для визначення мережевої адреси. Логічна операція І – це порівняння двох бітів з наступними результатами:

1 І 1 = 1
0 0 І 1 = 0
0 0 І 0 = 0
1 І 0 = 0.

IPv4 -адреса вузла поступово, біт за бітом, пройшла операцію І, і її маска підмережі визначила мережеву адресу, з якою пов’язаний вузол. В результаті виконання побітової операції І між адресою і маскою підмережі створюється мережева адреса.

Будь-який біт адреси, що пройшов операцію І зі значенням біта 1 з маски підмережі, виводить початкове значення біта з адреси. Таким чином, 0 (з IPv4 -адреси) І 1 (з маска підмережі) дорівнює 0. 1 (з адреси IPv4) І 1 (з маски підмережі) дорівнює 1. Таким чином, усе, що проходить операцію І зі значенням 0, виводить 0. Ці властивості операції І використовуються з маскою підмережі, щоб «замаскувати» вузлові біти IPv4 -адреси. Кожен біт адреси проходить операцію І з відповідним бітом маски підмережі (рис. 8.2).

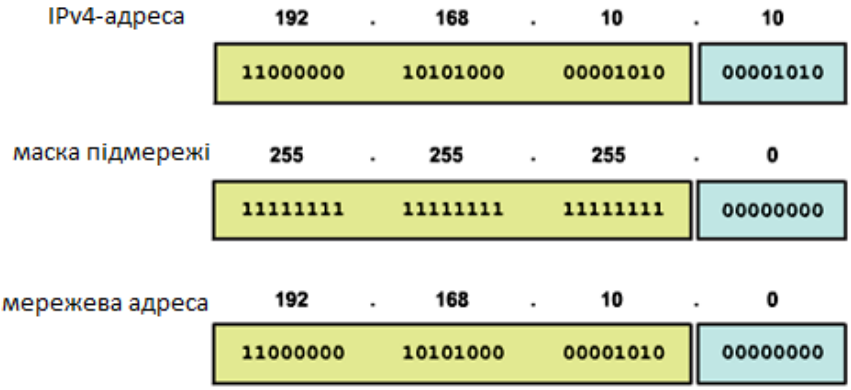


Рис. 8.2. Визначення мережевої адреси вузла [1]

Оскільки усі біти маски підмережі, що представляють вузлові біти, є нулями, вузлова частина виведеної мережевої адреси складається тільки з нулів. IPv4 -адреса з усіма нулями у вузловій частині представляє мережеву адресу. І навпаки, усі біти маски підмережі, які представляють мережеву частину, є одиницями. Коли кожна з цих одиниць проходить операцію І з відповідним бітом адреси, отримані в результаті операції біти ідентичні початковим бітам адреси.

Операцію І можна використовувати для визначення того, до якої підмережі належить адреса, а також того, які інші адреси відносяться до тієї ж підмережі. Якщо дві адреси знаходяться в одній і тій же мережі або підмережі, то один для одного вони є локальними і, отже, можуть взаємодіяти між собою безпосередньо. Адреси, що знаходяться в різних мережах або підмережах, є один для одного віддаленими, тому для їх комунікації потрібний пристрій рівня 3 (наприклад маршрутизатор або комутатор рівня 3).

При перевірці або діагностиці мережі часто доводиться визначати два вузли з однієї локальної мережі. Це визначення необхідно робити з точки зору мережевих пристроїв. Через неправильну конфігурацію вузол може бачити себе не в тій мережі. У більшості мереж

передачі даних багато вузлів представлено крайовими пристроями, такими як комп'ютери, смартфони, планшетні ПК, принтери і IP -телефони. Оскільки це основна частина пристроїв в мережі, найбільша кількість адрес має бути присвоєна саме цим вузлам. Таким вузлам привласнюються IP -адреси з діапазону доступних адрес в мережі. IP -адреса можна привласнювати статично або динамічно.

8.3. Одноадресна, широкомовна та багатоадресна передача

У IPv4 -мережі вузли можуть взаємодіяти одним з трьох наступних способів.

- **Одноадресна розсилка** - процес відправки пакету з одного вузла на індивідуальний.
- **Широкомовна розсилка** - процес відправки пакету з одного вузла на усі вузли в мережі.
- **Багатоадресна розсилка** - процес відправки пакету з одного вузла вибраній групі вузлів, можливо, в різних мережах.

Ці три типи зв'язку використовуються в мережах передачі даних для різних цілей. У усіх трьох типах IPv4 -адреса початкового вузла розміщена в заголовку пакету в якості адреси джерела.

Одноадресна передача використовується для звичайного обміну даними між вузлами як в мережі типу «клієнт/сервер», так і в одноранговій мережі. Для одноадресної розсилки пакетів в якості адреси призначення використовуються адреси цільового пристрою. Пакети можуть бути спрямовані через об'єднану мережу.

Трафік **широкомовної розсилки** використовується для відправки пакетів по усіх вузлах в мережі за допомогою групової адреси мережі. У пакеті широкомовної розсилки міститься IP -адреса призначення, у вузловій частині якої присутні тільки одиниці (1). Це означає, що пакети отримають і оброблять усі вузли в локальній мережі (домені широкомовної розсилки). Широкомовні розсилки передбачені в багатьох мережевих протоколах, наприклад в протоколі DHCP. Коли вузол отримує пакет, відправлений на мережеву широкомовну адресу, вузол обробляє цей пакет так само, як обробляє пакет, відправлений по одноадресній розсилці.

Використання широкомовної розсилки включає:

- проведення маршруту від адрес верхнього рівня до адрес нижнього рівня;
- запит адреси;
- на відміну від одноадресної розсилки, у разі якої пакети можуть бути відправлені по об'єднаній мережі, широкомовним пакетам заборонено проходити по локальній мережі. Це обмеження залежить від конфігурації маршрутизатора шлюзу і типу широкомовної розсилки.

Багатоадресна передача призначена для збереження пропускної спроможності IPv4 - мережі. Така передача скорочує трафік, дозволяючи вузлу відправляти один пакет вибраній групі вузлів, які є частиною групи мультисповіщення. Щоб досягти цільових вузлів за допомогою одноадресного зв'язку, вузол-джерело повиннен відправляти окремий пакет на кожну адресу. У випадку з багатоадресною розсилкою вузол-джерело може відправляти один пакет, який досягає декількох тисяч вузлів призначення. Мережева взаємодія дублює багатоадресні потоки, щоб вони досягали тільки вказаних одержувачів.

Багатоадресна передача включає:

- широкомовну передачу відео і аудіо;
- обмін даними маршрутизації протоколами маршрутизації;
- поширення ПЗ;
- гру віддаленим способом.

Протокол IPv4 має блок адрес, зарезервованих для груп мультисповіщення. Це діапазон адрес складає від 224.0.0.0 до 239.255.255.255. Діапазон групових адрес розділений на різні типи адрес: зарезервовані канальні і глобальні адреси.

Маршрутизатор, підключений до локальної мережі, розпізнає, що ці пакети адресовані локальній групі мультисповіщення, і не пересилає їх далі. Зазвичай зарезервовані локальні

адреси застосовуються в протоколах маршрутизації з використанням багатоадресної передачі для обміну даними маршрутизації.

Вузли, які отримують конкретні багатоадресні дані, називаються клієнтами багатоадресної розсилки. Клієнти багатоадресної розсилки використовують сервіси, запрошені програмою клієнта для підписки в групу мультисповіщення. Кожна група мультисповіщення представлена однією груповою IPv4 -адресою призначення.

8.4. Публічні та приватні IPv4 –адреси

Хоча велика частина вузлових IPv4 -адрес є **публічними**, тобто призначеними для використання в мережах, доступних через інтернет, існують блоки адрес, які використовуються в мережах, що вимагають обмеженого доступу в Інтернет або не вимагають його зовсім. Ці адреси називаються **приватними.**

Блоки приватних адрес:

10.0.0.0-10.255.255.255 (10.0.0.0/8)

172.16.0.0-172.31.255.255 (172.16.0.0/12)

192.168.0.0-192.168.255.255 (192.168.0.0/16)

Приватні адреси визначені в документі RFC 1918 «Привласнення адрес для приватного Інтернету». Іноді ці адреси називають адресами RFC 1918.

Вузли в різних мережах можуть використовувати одні і ті ж адреси приватного простору. Пакети, що використовують ці адреси як джерело або призначення, не повинні з’являтися в публічному Інтернеті. Маршрутизатор або пристрій міжмережевого екрану по периметру цих приватних мереж повинні блокувати або перетворювати ці адреси. Навіть якщо б пакети самі прокладали свій шлях через інтернет, у маршрутизаторів у будь-якому випадку не з’явилося б маршрутів для пересилки їх у відповідну приватну мережу.

Переважна більшість адрес в діапазоні вузлів одноадресної IPv4 -розсилки є публічними адресами. Ці адреси призначені для використання у вузлах з відкритим доступом з Інтернету.

Деякі адреси неможливо призначити вузлам. Також існують особливі адреси, які можуть бути призначені вузлам, але з обмеженнями того, як ці вузли можуть взаємодіяти в мережі.

Однією з зарезервованих адрес є **IPv4 -адреса логічного інтерфейсу loopback 127.0.0.1. Loopback** – це особлива адреса, яку використовують вузли, щоб направляти трафік самим собі. Адреса зворотного зв’язку дозволяє створювати прискорений метод взаємодії для застосувань і сервісів TCP/IP, які працюють на одному і тому ж пристрої. З використанням loopback -адреси замість призначеної IPv4 -адреси вузла два сервіси на одному вузлі можуть обійти нижні рівні стека протоколів TCP/IP. Для перевірки налаштування TCP/IP на локальному вузлі можна послати ехо-запит на loopback -адресу. Хоча використовується тільки адреса 127.0.0.1, резервуються адреси з діапазону 127.0.0.0 до 127.255.255.255. Будь-яка адреса з цього блоку дасть зворотний зв’язок з локальним вузлом. Жодна адреса з цього блоку не повинна з’являтися в якій-небудь мережі.

В якості **локальних адрес каналу** використовуються IPv4 -адреси в блоці адрес від 169.254.0.0 до 169.254.255.255 (169.254.0.0 /16). Ці адреси можуть бути автоматично присвоєні ОС локальному вузлу в середовищах, де налаштування IP -мережі недоступне. Вони можуть використовуватися в невеликій одноранговій мережі або для вузла, який не може автоматично отримати адресу від DHCP -сервера.

Комунікація за допомогою локальних IPv4 -адрес підходить тільки для обміну даними з іншими пристроями, підключеними до тієї ж мережі. Вузол не повинен відправляти пакет з локальною IPv4 -адресою призначення якому-небудь маршрутизатору для пересилки, а повинен задати час життя (TTL) IPv4 для цих пакетів в значенні 1.

Локальні адреси не надають сервіси за межами локальної мережі. Проте багато застосувань типу клієнт-сервер і однорангові застосування працюватимуть належним чином з локальними IPv4 -адресами.

8.5. Застаріла класова адресація, її обмеження. Безкласова адресація

Історично склалося так, що призначені адреси (RFC1700) згрупували одноадресні діапазони в адреси з особливими розмірами, які називаються адресами класу A, класу B і класу C. Крім того, були визначені адреси класу D (групові) і класу E (експериментальні). Згідно з індивідуальними адресами класів A, B і C визначені мережі особливого розміру і блоки особливих адрес для цих мереж. Компанії або організації призначається ціла мережа з блоків адрес класу A, B або C. Таке використання адресного простору називається **класовою адресацією**.

Блоки класу A

Блок адрес класу A розроблений для підтримки дуже великих мереж, що містять більш ніж 16 мільйонів адрес вузлів. Для позначення мережевої адреси IPv4 -адреси класу A використовували фіксований префікс /8 з першим октетом. Інші три октети використовувалися для адрес вузлів. Усі адреси класу A вимагають, щоб найбільший розряд старшого октету дорівнював нулю. Це означає, що існувало тільки 128 можливих мереж класу A, від 0.0.0.0/8 до 127.0.0.0 /8. Навіть якщо адреси класу A зарезервували половину адресного простору, у зв'язку з їх обмеженням до 128 мереж вони можуть бути призначені тільки приблизно 120 компаніям або організаціям.

Блоки класу B

Адресний простір класу B розроблений для підтримки потреб невеликих і великих мереж, що містять приблизно 65 000 вузлів. IP -адреса класу B використовувала два старші октети для позначення мережевої адреси. Два октети, що залишилися, визначали адреси вузлів. Як і у випадку з класом A, адресний простір для класів адрес, що залишилися, має бути зарезервованим. Для адрес класу B два найстарші розряди старшого октету дорівнюють 10. Це обмежує блок адрес для класу B від 128.0.0.0/16 до 191.255.0.0/16. Призначення адрес класу B більш ефективне в порівнянні з класом A, оскільки 25% його загального простору IPv4 -адрес було розділене серед приблизно 16 000 мереж.

Блоки класу C

Адресний простір класу C був доступний частіше за усі інші класи адрес. Це адресний простір призначений для надання адрес невеликим мережам з максимальною кількістю вузлів не більше 254. Блоки адрес класу C використовували префікс /24. Це означає, що мережа класу C використовувала тільки останній октет як адреси вузлів з трьома старшими октетами для позначення мережевих адрес. Блоки адрес класу C відділяли адресний простір за допомогою фіксованого значення 110 найстарших розрядів старшого октету. Це обмежило блок адрес класу C від 192.0.0.0/24 до 223.255.255.0/24. Хоча цей блок зайняв тільки 12,5 % від загального об'єму адресного IPv4 -простору, він надав адреси 2 мільйонам мереж.

Обмеження в системі класів

Не усі вимоги організацій відповідають цим класам. Класовий розподіл адресного простору часто призводить до втрати безлічі адрес, що негативним чином позначається на доступності IPv4 -адрес. Наприклад, компанії, в мережі якої знаходиться 260 вузлів, потрібні адреси класу B з більше 65 000 адресами.

Хоча ця класова система була практично забута у кінці 1990-х рр., нині як і раніше спостерігається її вплив. Наприклад, при призначенні комп'ютеру IPv4 -адреси ОС перевіряє привласнювану адресу, щоб визначити, до якого класу належить ця адреса: A, B або C. Потім ОС приймає префікс, використовуваний цим класом, і призначає маску підмережі за замовчуванням.

Безкласова адресація

Сьогодні використовується система, яка називається **безкласовою адресацією**, офіційна назва якої – безкласова міждоменна маршрутизація (**CIDR**, Classless Inter-Domain Routing). Класове призначення IPv4 -адрес з довжинами префіксів /8, /16 і /24, кожен з яких належав різному класу, було дуже неефективним. У 1993 р. організація IETF (Інженерна група по

розвитку Інтернету) створила нові стандарти, які дозволили операторам зв'язку призначати IPv4 -адреси в будь-яких бітових межах (мається на увазі довжина префікса) замість адрес класу A, B або C.

У IETF розуміли, що безкласова міждоменна маршрутизація (CIDR) була тільки тимчасовим рішенням і для підтримки швидкого розвитку кількості користувачів Інтернету потрібний новий IP -протокол. У 1994 р. в IETF почалися пошуки наступника IPv4. Ним став протокол IPv6.

8.6. Привласнення IP -адрес

Щоб мати в розпорядженні мережеві вузли, наприклад веб-серверами, компанії або організації потрібний блок призначених публічних адрес. Публічні адреси мають бути унікальними, а використання цих публічних адрес контролюється і призначається окремо для кожної організації. Це твердження є вірним відносно IPv4 - і IPv6 -адрес.

Адміністрація адресного простору Інтернет IANA (http://www.iana.org) регулює призначення IPv4 - і IPv6 -адрес. До середини 1990-х рр. управління усім адресним IPv4 -простором здійснювалося безпосередньо організацією IANA. Що у той час залишився адресний IPv4 -простір серед різних реєстраторів для полегшеного управління конкретними цілями і регіонами. Такі реєстраційні компанії називаються регіональними інтернет-реєстраторами (**RIR**, Regional Internet Registry). Основні реєстри:

- AfriNIC (Африканський мережевий інформаційний центр) – Африканський регіон http://www.afrinic.net.
- APNIC (Азіатсько-тихоокеанський мережевий інформаційний центр) – Азіатсько-тихоокеанський регіон http://www.apnic.net.
- ARIN (Американський реєстр інтернет-адрес) – Північноамериканський регіон http://www.arin.net.
- LACNIC (Латиноамериканський і Карибський мережевий інформаційний центр) – Латинська Америка і деякі острови Карибського моря http://www.lacnic.net.
- RIPE NCC (Координаційний центр європейської континентальної мережі) – Європа, Близький Схід і Азія http://www.ripe.net.

Регіональні інтернет-реєстратори відповідають за виділення IP -адрес інтернет-провайдерам (ISP). Більшість компаній або організацій отримують блоки IPv4 -адрес від інтернет-провайдерів. Зазвичай, окрім усіх інших послуг, провайдер надає своїм замовникам невелику кількість доступних IPv4 -адрес (6 або 14). Великі блоки адрес можна отримати відповідно до потреб і за додаткову плату.

По суті, провайдери позичають своїм клієнтам ці адреси. При зміні інтернет-провайдера новий постачальник послуг надає адреси зі своїх адресних блоків, а попередній отримує назад свої адреси і позичає їх іншому замовникові.

IPv6 -адреси можна отримати від інтернет-провайдера або, в деяких випадках, безпосередньо від інтернет-реєстраторів.

Для діставання доступу до послуг мережі Інтернет необхідно підключити мережу для передачі даних в Інтернет за допомогою інтернет-провайдера (ISP). У інтернет-провайдерів є свої мережі передачі даних для управління підключенням до Інтернету і надання послуг. Серед інших послуг, які інтернет-провайдери зазвичай надають своїм замовникам, існують сервіс DNS, сервіс електронної пошти і веб-сайти. Залежно від рівня необхідних і доступних послуг замовники звертаються до різних рівнів інтернет-провайдерів.

8.7. Потреба в IPv6. Представлення IPv6

Протокол IPv6 розроблений як наступник протоколу IPv4. У протоколі IPv6 більше 128-бітового адресного простору, що досить для 340 ундециліонів адрес (це число 340, за яким йде 36 нулів.) Проте IPv6 – не просто великі адреси. Коли фахівці IETF почали розробку

наступника IPv4, вони використовували цю можливість для усунення обмежень протоколу IPv4 і внесення додаткових поліпшень.

Скорочення адресного простору протоколу IPv4 – основний стимулюючий чинник для переходу до використання IPv6. У міру того як Африка, Азія і інші регіони планети все більше потребують підключення до мережі Інтернет, залишається все менше IPv4 -адрес для підтримки таких темпів розвитку. 31 січня 2011 р. Адміністрація адресного простору Інтернет IANA призначила останні 2 блоки IPv4 -адрес /8 регіональним інтернет-реєстраторам (RIR). Теоретична максимальна кількість IPv4 -адрес – 4,3 мільярда. Приватні адреси RFC 1918 у поєднанні з перетворенням мережевих адрес (NAT) служать для уповільнення виснаження адресного простору IPv4. Перетворення мережевих адрес (NAT) має обмеження, які перешкоджають одноранговому зв'язку.

Фахівці IETF створили різні протоколи та інструменти, які дозволяють мережевим адміністраторам поступово переводити свої мережі на протокол IPv6. Методи переходу можна розділити на 3 категорії.

- **Подвійний стек:** дозволяє протоколам IPv4 і IPv6 співіснувати в одній мережі. Пристрої з подвійним стеком одночасно працюють з протокольними стеками IPv4 і IPv6.
- **Тунелювання:** це спосіб транспортування IPv6 -пакетів через IPv4 -мережу. IPv6 – пакет інкапсулюється усередині IPv4 -пакета, як і інші типи даних.
- **Перетворення:** перетворення мережевих адрес 64 (NAT64) дозволяє пристроям під управлінням IPv6 обмінюватися даними з пристроями під управлінням IPv4 за допомогою методу перетворення, схожого на метод перетворення з NAT для IPv4. IPv6 -пакет перетворюється в пакет IPv4 -пакет і навпаки.

Довжина IPv6 -адрес складає 128 біт, написаних у вигляді рядка шістнадцятиричних значень. Кожні 4 біта представлені однією шістнадцятиричною цифрою, причому загальна кількість шістнадцятиричних значень дорівнює 32. IPv6 -адреси не чутливі до регістра, їх можна записувати як рядковими, так і прописними буквами.

Переважний формат для запису IPv6 -адреси: x: x: x: x: x: x: x: x, де кожен «x» складається з чотирьох шістнадцятиричних значень. Октети – це термін, який використовується для позначення 8 біт IPv4 -адреси. У IPv6 шістнадцятиричне число – це термін, використовуваний для позначення сегменту з 16 біт або чотирьох шістнадцятиричних значень. Кожен «x» - це одне шістнадцятиричне число, 16 біт або 4 шістнадцятиричних цифр. У переважному форматі IPv6 -адреса записана за допомогою 32 шістнадцятиричних цифр. Проте, це не найоптимальніший спосіб представлення IPv6 -адреси. Роглянемо два правила, які допоможуть скоротити кількість цифр, необхідних для представлення IPv6 -адреса.

Правило 1: пропуск початкових нулів

Перше правило для скорочення запису IPv6 –адрес – пропуск усіх ведучих 0 (нулів) в шістнадцятиричному записі. Наприклад:

- 001AB можна представити як 1AB;
- 009F0 можна представити як 9F0;
- 00A00 можна представити як A00;
- 0000AB можна представити як AB.

Правило 2: пропуск усіх нульових блоків

Друге правило для скорочення запису адрес IPv6 полягає в тому, що подвійна двокрапка (::) може замінити будь-який єдиний, суміжний рядок одного або декількох 16-бітових сегментів (хекстетів), що складаються з нулів.

Подвійна двокрапка (::) може використовуватися в адресі тільки один раз, інакше в результаті може виникнути декілька адрес. Поєднання цього правила з методом пропуску нулів допомагає значно скоротити запис IPv6 -адреса. Це називається **стислим форматом.**

Існує три типи IPv6 -адрес.

- **Індивідуальна:** служить для визначення інтерфейсу на пристрої під управлінням протоколу IPv6.

- **Групова:** використовується для відправки IPv6 -пакетів по декількох адресах призначення.
- **Довільна:** будь-яка індивідуальна IPv6 -адреса, яка може бути призначена декільком пристроям. Пакет, що відправляється на адресу довільної розсилки, спрямовується до найближчого пристрою з цією адресою.

На відміну від протоколу IPv4, IPv6 не використовує адресу широкомовної розсилки. Проте є групова IPv6 -адреса для усіх вузлів, який дає аналогічний результат.

Протокол IPv6 використовує довжину префікса для позначення частини префікса адреси. IPv6 не використовує для маски підмережі десяткове представлення з розділовими точками. Довжина префікса означає мережеву частину IPv6 -адреси за допомогою адреси або довжини IPv6 -префікса.

Діапазон довжини префікса може складати від 0 до 128. Традиційна довжина IPv6 -префікса для локальних та інших типів мереж – /64. Це означає, що довжина префікса, або мережева частина адреси, складає 64 біта, а що залишилися 64 біта залишаються для ідентифікатора інтерфейсу (вузлової частини) адреси.

Глобальні індивідуальні IPv6 -адреси унікальні по всьому світу і доступні для маршрутизації через інтернет IPv6. Ці адреси еквівалентні публічним IPv4 -адресам. Асоціація по привласненню імен і номерів Інтернету, оператор Адміністрації адресного простору Інтернет (IANA), виділяє блоки IPv6 -адрес п'яти регіональним інтернет-реєстраторам (RIR). Нині призначаються тільки глобальні індивідуальні адреси з першими трьома бітами 001 або 2000::/3. Це лише 1/8 від усього доступного адресного простору IPv6, за винятком дуже незначної кількості інших типів адрес індивідуальних і групових адрес.

Глобальна індивідуальна адреса складається з трьох частин:

- префікс глобальної маршрутизації;
- ідентифікатор підмережі;
- ідентифікатор інтерфейсу.

Префікс глобальної маршрутизації – це префіксна або мережева частина адреси, що призначається інтернет-провайдером замовникові або вузлу. Нині /48 є префіксом глобальної маршрутизації, який нині інтернет-реєстратори призначають своїм замовникам – корпоративним мережам та індивідуальним користувачам. Цього адресного простору більш ніж достатньо для більшості замовників.

Наприклад, IPv6 -адреса 2001:0 DB8: ACAD::/48 має префікс, який означає, що перші 48 біт (2001:0 DB8: ACAD) – це префіксна або мережева частина адреси. Подвійна двокрапка (::) перед довжиною префікса /48 означає, що інші адреси складаються з нулів.

SLAAC (Stateless address autoconfiguration) – це спосіб, який дозволяє пристрою отримати свій префікс, довжину префікса і адресу шлюзу за замовчуванням від маршрутизатора IPv6 без допомоги DHCPv6 -сервера. При використанні SLAAC для отримання необхідної інформації пристрою покладаються на повідомлення «Оголошення маршрутизатора ICMPv6».

8.8. Розбиття мережі на підмережі

Процес сегментації мережі шляхом розподілу її на дрібніші мережі називається **розбиттям на підмережі**. Ці дрібніші мережі називаються **підмережами**. Мережеві адміністратори можуть групувати пристрої і служби в підмережі за їх географічним місцем (наприклад, 3-й поверх будівлі) розташування, організаційному підрозділу (наприклад, відділ продажів) або за типом пристроїв (принтери, сервери, глобальна мережа) або за іншим значущим для мережі принципом. Розбиття на підмережі може понизити загальне навантаження на мережу і підвищити її продуктивність.

Маршрутизатор потрібний для взаємодії вузлів з різних підмереж. Пристрої в мережі використовують інтерфейс маршрутизатора, підключений до їх локальної мережі, в якості шлюзу за замовчуванням. Трафік, що відправляється на пристрій у віддаленій мережі, буде

оброблений маршрутизатором і відправлений у напрямі мережі призначення. Щоб визначити, чи є трафік локальним або віддаленим, маршрутизатор використовує маску підмережі.

Підмережі утворюють декілька логічних мереж з одного блоку адрес або мережевої адреси. Кожна підмережа розглядається як окремий мережевий простір. Пристрої в одній підмережі повинні використовувати адресу, маску підмережі і шлюз за замовчуванням тієї підмережі, до якої вони належать.

Трафік не може передаватися між підмережами без використання маршрутизатора. У кожного інтерфейсу маршрутизатора має бути IPv4 -адреса, що належить мережі або підмережі, до якої підключений цей інтерфейс.

Кожна мережева адреса містить допустимий діапазон адрес вузлів. Усі пристрої, підключені до однієї і тієї ж мережі, матимуть IPv4 -адресу вузла цієї мережі, а також загальну маску підмережі або префікс мережі.

Префікс і маска підмережі – це різні способи представлення одного і того ж – мережевої частини адреси. Для створення IPv4 -підмереж ми задіюємо один або декількох біт з вузлової частини в якості біт мережевої частини. Для цього ми розширюємо маску підмережі. Чим більше запозичено біт з вузлової частини, тим більше підмереж можна створити. Для кожного запозиченого біта кількість доступних підмереж подвоюється. Наприклад, якщо запозичувати один біт, можна створити дві підмережі. Для двох біт – 4 підмережі, для трьох біт – 8 підмереж і т. д. Проте з кожним запозиченим бітом зменшується кількість адрес вузлів в кожній підмережі.

Біти можуть бути запозичені тільки з вузлової частини адреси. Мережева частина адреси виділяється оператором зв'язку, і змінити її неможливо.

Для розрахунку **кількості підмереж** використовується формула:

2^n (де n = кількість запозичених біт).

Для розрахунку **кількості вузлів** в одній мережі використовується формула:

2^n -2 (де n = кількість біт, що залишилися у вузловій частині адреси).

Іноді потрібна конкретна кількість підмереж, а кількість адрес вузлів в кожній підмережі менш важлива. Наприклад, в організації потрібно розділити мережевий трафік згідно з внутрішньою структурою або при налаштуванні мережі в підрозділі. Наприклад, організація може прийняти рішення об'єднати в одну мережу усі пристрої для фахівців технічного відділу, а усі пристрої для керівництва винести в окрему мережу. В цьому випадку кількість підмереж має вищий пріоритет при визначенні кількості біт для запозичення.

Мережеві адміністратори повинні розробити схему міжмережевої адресації, щоб забезпечити максимальну кількість вузлів в кожній мережі. Кількість вузлів в кожному підрозділі повинна мати запас для збільшення в майбутньому.

У традиційному розбитті на підмережі кожній підмережі виділяється однакова кількість адрес. Якщо усі підмережі мають однакові вимоги до кількості вузлів, такі блоки адрес фіксованого розміру будуть ефективними.

Хоча традиційне розбиття на підмережі ділить адресний простір на достатню кількість підмереж, в ньому створюється значний об'єм невживаних адрес.

Наприклад, в кожній підмережі для кожного з трьох WAN –з'єднань потрібні тільки дві адреси. Оскільки в кожній підмережі доступні по 30 адрес, 28 з них не будуть використовуватися. Крім того, це обмежує можливості для майбутнього зростання, скорочуючи загальну кількість доступних підмереж. Таке неефективне використання адрес характерне для традиційного розбиття на підмережі з використанням класових мереж. Застосування традиційної схеми розбиття на підмережі в цьому варіанті є неефективним і даремним.

Розбиття підмережі на декілька підмереж з використанням маски підмережі змінної довжини (**VLSM**, variable length subnet mask) дозволяє розподіляти значно менше «зайвих» адрес.

Як показано на рис.8.3, при традиційному розбитті на підмережі створюються підмережі однакового розміру. У усіх підмережах в традиційній схемі використовується одна маска підмережі.

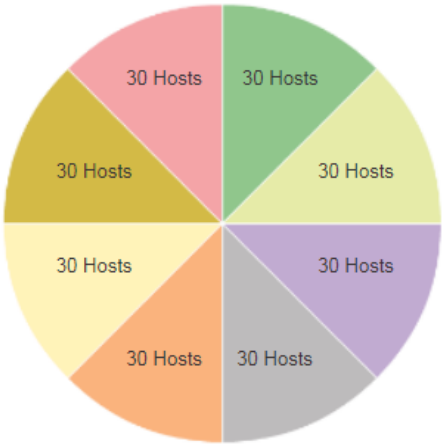


Рис.8.3. Традиційне розбиття на підмережі (створюються підмережі однакового розміру) [1]

Як показано на рис.8.4, VLSM -маска дозволяє розділити мережевий простір на нерівні частини. VLSM -маска підмережі може варіюватися залежно від кількості біт, які були запозичені для конкретної підмережі. Ці біти утворюють «змінну» частину маски.

Рис.8.4. Підмережі змінного розміру [1]

VLSM -розбиття на підмережі схоже на традиційне тим, що в ньому для створення підмереж запозичуються біти. Формули розрахунку кількості можливих підмереж і кількості вузлів в кожній підмережі також застосовні. Відмінність полягає в тому, що розбиття на підмережі виконується у декілька етапів. При використанні VLSM мережа спочатку розбивається на підмережі, а потім підмережі знову діляться на підмережі. Цей процес може повторюватися багато разів для створення підмереж різного розміру.

При плануванні виділення адрес в корпоративній мережі необхідно розглянути три основні моменти.

- **Запобігання дублюванню адрес:** кожен вузол в мережевій інфраструктурі повинен мати унікальну адресу. Без належного планування і документування адреса може бути призначена декільком вузлам, що приведе до проблем доступу до мережі цих вузлів.
- **Надання доступу і управління їм:** деякі вузли, такі як сервери, надають ресурси і внутрішнім, і зовнішнім вузлам. Призначену серверу адресу 3-го рівня можна

використовувати для управління доступом до цього сервера. Якщо адреса призначена випадковим чином і ніде не задокументована, управляти доступом буде складніше.

- **Моніторинг безпеки і продуктивності:** аналогічним чином необхідно контролювати безпеку і продуктивність вузлів мережі, а також усієї мережі в цілому. У рамках моніторингу мережевий трафік аналізується на наявність адрес, які генерують або отримують велике число пакетів. При належному плануванні і документуванні адресації в мережі проблемні пристрої можна легко виявити.

У мережі існують пристрої різних типів, включаючи наступні:

- клієнтські пристрої кінцевих користувачів;
- сервери і периферійні пристрої;
- вузли, доступні з Інтернету;
- проміжні пристрої;
- шлюз.

При проектуванні схеми IP -адресації зазвичай рекомендується використовувати готовий шаблон призначення адрес кожному типу пристроїв. Це допомагає адміністраторам додавати і видаляти пристрої, фільтрувати трафік на основі IP -адрес, а також спрощує документування.

Висновок до лекції 8

IP -адреса є ієрархічною структурою з мережевою частиною, маскою підмережі і вузловою частиною. IP -адреса може представляти усю мережу, певний вузол або мережеву адресу широкомовної розсилки.

Розуміння двійкової системи числення особливе важливе, щоб встановити, чи знаходяться два вузли в одній і тій же мережі. Біти в мережевій частині IP -адреси мають бути ідентичні для усіх пристроїв, які знаходяться в одній і тій же мережі. Маска підмережі або префікс використовується для визначення мережевої частини IP -адреси. IP -адреса можна привласнювати статично або динамічно. DHCP забезпечує автоматичне привласнення інформації про адресу, наприклад IP -адреси, маски підмережі, шлюзу за замовчуванням та інших параметрів.

IPv4 -вузли можуть обмінюватися даними за допомогою одного з трьох способів: одноадресної, широкомовної або багатоадресної розсилки. Блоки адрес, які використовуються в мережах, що вимагають обмеженого доступу в Інтернет або не вимагають його зовсім, називаються приватними адресами. Блоки приватних IPv4 -адрес: 10.0.0.0/8, 172.16.0.0/12 і 192.168.0.0/16.

Скорочення адресного простору протоколу IPv4 – основний стимулюючий чинник для переходу до використання IPv6. Кожна IPv6 -адреса має 128 біт замість 32 біт, як в протоколі IPv4. IPv6 не використовує для маски підмережі десяткове представлення з розділовими крапками. Довжина префікса використовується для позначення мережевої частини IPv6 -адреси за допомогою наступного формату: IPv6 -адрес/довжина префікса. Існує три типи IPv6 -адрес: індивідуальні, групові і довільні. Локальна IPv6 -адреса каналу дозволяє пристрою обмінюватися даними з іншими пристроями під управлінням IPv6 по одному і тому ж каналу і тільки по цьому каналу (підмережі). Пакети з локальною адресою каналу джерела або призначення не можуть бути спрямовані за межі того каналу, в якому пакет створюється.

Кожна мережева адреса містить допустимий діапазон адрес вузлів. Усі пристрої, підключені до однієї і тієї ж мережі, матимуть IPv4 -адресу вузла цієї мережі, а також загальну маску підмережі або префікс мережі. Вузли можуть безпосередньо обмінюватися трафіком, якщо вони знаходяться в одній підмережі. Трафік не може передаватися між підмережами без використання маршрутизатора. Щоб визначити, чи є трафік локальним або віддаленим, маршрутизатор використовує маску підмережі. Префікс і маска підмережі – це різні способи представлення одного і того ж – мережевої частини адреси.

Для створення IPv4 -підмереж ми задіюємо один або декількох біт з вузлової частини в якості біт мережевої частини. Два істотні чинники, які впливають на визначення блоку IP - адрес за допомогою маски підмережі, – це кількість необхідних підмереж і максимальна кількість вузлів, яка має бути в підмережі. Між кількістю підмереж і вузлів в них існує зворотна залежність. Чим більше біт запозичено для створення підмереж, тим менше залишиться біт у вузловій частині і, отже, тим менше вузлів буде доступні в кожній підмережі.

Для розрахунку кількості адрес, які будуть доступні в кожній підмережі, використовується формула 2^n (де n – кількість біт, що залишилися, у вузловій частині). Проте в цьому діапазоні мережева адреса і широкомовна адреса недоступні для використання, тому кількість доступних адрес розрахується за формулою 2^n - 2.

Розбиття підмережі на декілька підмереж або використання маски підмережі змінної довжини (VLSM) призначені для того, щоб уникнути створення непотрібних адрес. Розбиття IPv6 -мережі на підмережі має на увазі використання іншого підходу, ніж розбиття на підмережі IPv4 -мережі. Простір IPv6 -адрес розбивається не з метою економії адрес, а для забезпечення ієрархічної логічної структури мережі. Якщо IPv4 -мережі розбиваються на підмережі в основному для боротьби з нестачею адрес, то метою розбиття IPv6 -мережі на підмережі являється створенням ієрархії адрес на основі кількості маршрутизаторів і обслуговуваних ними мереж.

Для забезпечення найкращого використання схеми IP -адресації потрібно ретельне планування. В процесі планування адрес необхідно враховувати розмір, розташування, використання і вимоги до доступу. Після установки IP -мережі її необхідно протестувати для перевірки підключень і продуктивності.

Питання для закріплення

1. Для чого використовується мережева і вузлова частини IPv4 –адреси?
2. Що позначає довжина префікса?
3. Поясніть роль побітової операції I для мережевої адресації.
4. У чому полягає одноадресна, широкомовна та багатоадресна передача?
5. Чим відрізняються публічні і приватні IPv4 –адреси?
6. Назвіть блоки приватних адрес.
7. У чому полягають недоліки застарілої класової адресації?
8. Які переваги безкласової адресації?
9. Як відбувається привласнення IP –адрес?
10. Чому виникла в потреба в IPv6?
11. Яке представлення IPv6?
12. Як відбувається розбиття мережі на підмережі?
13. Для чого використовуються маски підмережі змінної довжини?

Список рекомендованої літератури

1. CCNA R&S ITN Chapter 9: Subnetting IP Networks // Електронний ресурс. Режим доступу: http://static-course-assets.s3.amazonaws.com/IntroNet50ENU/module9/index.html

2. Understanding IP Addresses, Subnets, and CIDR Notation for Networking // Електронний ресурс. Режим доступу: https://www.digitalocean.com/community/tutorials/understanding-ip-addresses-subnets-and-cidr-notation-for-networking

3. IP Addresses, Subnet Masks, and Default Gateways // Електронний ресурс. Режим доступу: http://www.networkcomputing.com/network-security/ip-addresses-subnet-masks-and-default-gateways/1835691346

4. IPv4 – VLSM // Електронний ресурс. Режим доступу: https://www.tutorialspoint.com/ipv4/ipv4_vlsm.htm

Лекція 9. Тема: «Протоколи та сервіси прикладного рівня»

План лекції

9.1. Функції і протоколи прикладного рівня TCP/IP.
9.2. Однорангові мережі.
9.3. Протоколи HTTP і HTTPS.
9.4. Протоколи SMTP, POP і IMAP.
9.5. Служба доменних імен.
9.6. Протокол динамічної конфігурації мережевого вузла.
9.7. Протокол передачі файлів (FTP).
9.8. Протокол обміну блоками серверних повідомлень.

9.1. Функції і протоколи прикладного рівня TCP/IP

Прикладний рівень або рівень застосувань ближче за усіх знаходиться до кінцевого користувача. Як показано на рис.9.1, на цьому рівні забезпечується взаємодія між застосуваннями для обміну даними, і базовою мережею, по якій передаються повідомлення. Протоколи рівня застосувань використовуються для обміну даними між програмами, що виконуються на вузлі-джерелі і вузлі-одержувачі.

Існує багато протоколів рівня застосувань, і постійно розробляються нові протоколи. До деяких з найбільш відомих протоколів рівня застосувань відносяться: протокол передачі гіпертексту (HTTP), протокол передачі файлів (FTP), простий протокол передачі файлів (TFTP), протокол доступу до повідомлень в Інтернеті (IMAP) і протокол служби доменних імен (DNS).

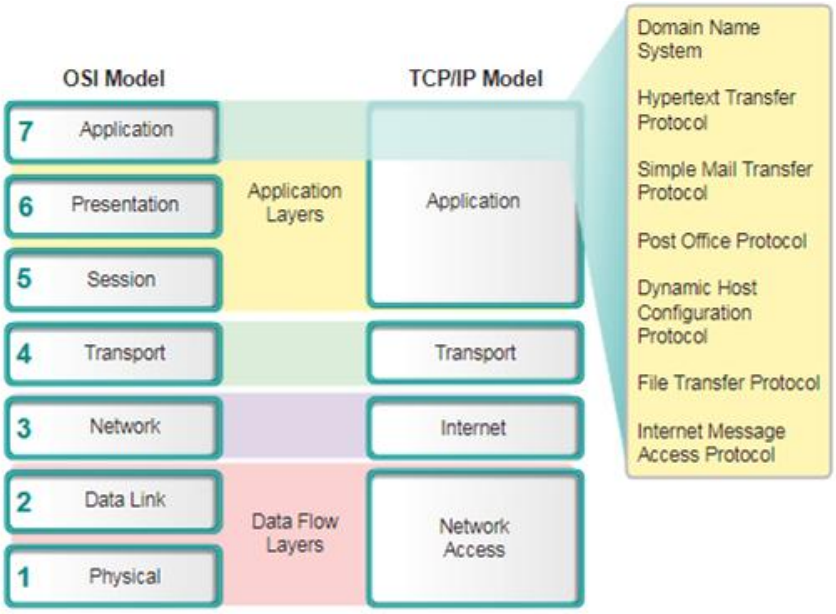


Рис. 9.1. Протоколи прикладного рівня [1]

Рівень представлення (Application layer) забезпечує три основні функції.

- Форматування або представлення даних з початкового пристрою у формі, відповідній для отримання пристроєм призначення.
- Стискування даних так, щоб їх можна було розпакувати на пристрої призначення.
- Шифрування даних для передачі і розшифровки даних після отримання на приймаючій стороні.

На рівні представлення форматуються дані рівня застосувань і встановлюються стандарти форматів файлів. До широко відомих форматів відеофайлів належать QuickTime і MPEG (рис.9.2).

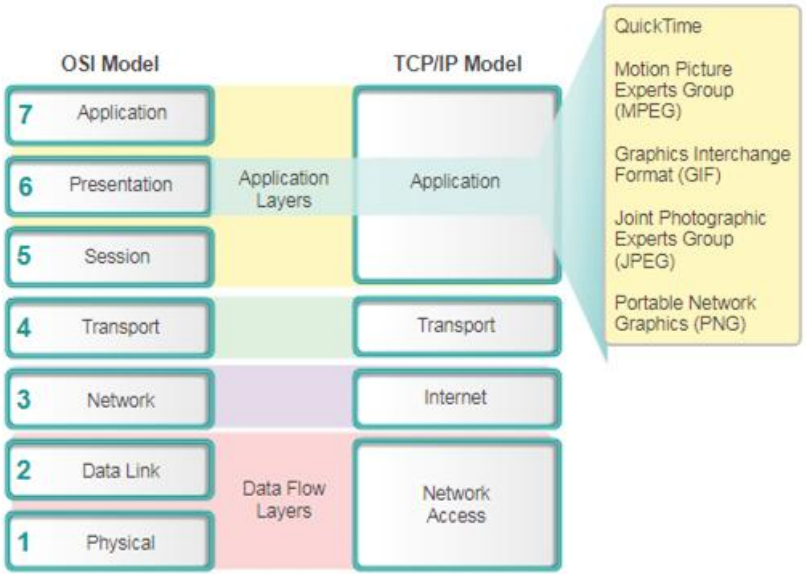


Рис. 9.2.Основні стандарти рівня представлення [1]

QuickTime – це стандарт комп'ютерів компанії Apple для роботи з відео і звуком, а MPEG (Moving Picture Experts Group) – це стандарт для стискування і кодування відео і звуку.

До деяких з найбільш відомих графічних форматів зображень, які використовуються в мережах, відносяться: формат обміну графічними даними (GIF, Graphics Interchange Format), стандарт цифрового стискування нерухомих відеозображень (JPEG, Joint Photographic Experts Group) і формат файлів для растрових графічних зображень (PNG, Portable Network Graphics). GIF і JPEG – це стандарти стискування і кодування для графічних зображень. Формат PNG був розроблений для подолання обмежень формату GIF, а також з метою його повної заміни.

Функції на сеансовому рівні створюють і обслуговують діалогові вікна між початковими і кінцевими застосуваннями. На сеансовому рівні відбувається обмін даними для створення діалогових вікон, підтримка їх в активному стані та для перезапуску сеансів, які були перервані або неактивні впродовж тривалого часу.

Хоча в моделі OSI функції рівня застосувань, рівня представлення і сеансового рівня відокремлені один від одного, найбільш відомі і широко використовувані застосування TCP/IP об'єднують в собі функції усіх трьох рівнів.

Протоколи прикладного рівня TCP/IP визначають формати і управляють даними, необхідними для багатьох поширених функцій обміну даними через інтернет. Нижче перераховані деякі з таких протоколів TCP/IP.

- **Служба доменних імен (DNS,** Domain Name System**):** використовується для перетворення імен інтернет-ресурсів в IP -адреси.
- **Telnet:** використовується для надання віддаленого доступу до серверів і мережевих пристроїв.
- **Простий протокол передачі електронної пошти (SMTP,** Simple Mail Transfer Protocol**):** використовується для передачі поштових повідомлень і вкладень.
- **Протокол динамічної конфігурації мережевого вузла (DHCP,** Dynamic Host Configuration Protocol**):** використовується для призначення вузлу IP -адреси, маски підмережі, шлюзу за замовчуванням та адрес DNS -серверів.
- **Протокол передачі гіпертексту (HTTP,** HyperText Transfer Protocol**):** використовується для передачі веб-сторінок з Інтернету.
- **Протокол передачі файлів (FTP,** File Transfer Protocol**):** використовується для передачі файлів між системами.
- **Простий протокол передачі файлів (TFTP,** Trivial File Transfer Protocol**):** використовується для передачі файлів без встановлення з'єднання.

- **Протокол BOOTP (**bootstrap protocol**).** Використовується для отримання даних про IP -адресу під час завантаження.
- **Поштовий протокол (POP,** Post Office Protocol **):** використовується поштовими клієнтами для отримання електронної пошти з віддалених серверів.
- **Протокол доступу до повідомлень в Інтернеті (IMAP,** Internet Message Access Protocol**):** використовується для клієнтського підключення до сервера електронної пошти і перегляду поштових повідомлень.

Протоколи рівня застосувань використовуються початковими і кінцевими пристроями під час сеансу зв'язку. Для успішного обміну даними протоколи рівня застосувань на початковому і кінцевому вузлах мають бути сумісними.

На сьогодні для робітників і розважальних цілей переважно використовуються три протоколи:

- HTTP (протокол передачі гіпертексту);
- SMTP (протокол простої передачі електронної пошти);
- поштовий протокол (POP).

Ці протоколи рівня застосувань дозволяють переглядати веб-сторінки, а також відправляти і приймати електронну пошту. Протокол HTTP використовується для підключення до веб-сайтів в Інтернеті. Протокол SMTP використовується для відправки електронної пошти. Протокол POP використовується для прийому електронної пошти.

Після введення в адресному рядку веб-адреси або уніфікованого покажчика ресурсу (URL -адреси) веб-браузер встановлює з'єднання по протоколу HTTP з веб-сервісом, запущеним на сервері. URL -адреса і уніфіковані ідентифікатори ресурсів – це назви, які більшість користувачів асоціюють з веб-адресами. http://www.cisco.com/index.html – приклад URL -адреси, яка вказує на певний ресурс – веб-сторінку з назвою index.html на сервері cisco.com.

Веб-браузери – це клієнтські застосування, за допомогою яких комп'ютер підключається до веб-сайтів і дістає доступ до ресурсів, розміщених на веб-серверах. Як і в більшості процесів сервера, веб-сервер працює у фоновому режимі і надає доступ до різних типів файлів.

Для доступу до вмісту веб-клієнти встановлюють підключення до сервера і просять необхідні ресурси. Сервер відповідає, відправляючи запрошені ресурси, а браузер інтерпретує отримані дані і представляє їх користувачеві.

Браузери можуть інтерпретувати і представляти багато типів даних (наприклад, простий текст або HTML -код – мова, на якій складаються веб-сторінки). Проте для інших типів даних може знадобитися інший сервіс або програма, які зазвичай називаються розширенням. Щоб допомогти браузеру визначити тип отримуваного файлу, сервер повідомляє, які дані містить файл.

Щоб краще зрозуміти взаємодію браузеру з веб-сервером розглянемо, як веб-сторінка (URL -адреса http://www.cisco.com/index.html) відкривається в браузері.

По-перше, браузер інтерпретує три частини URL -адреси:

1. http (протокол або схема);
2. www.cisco.com (ім'я сервера);
3. index.html (назва конкретного прошеного файлу).

Потім браузер перевіряє ім'я сервера www.cisco.com, щоб перетворити його в числову адресу, за якою встановлюється підключення до сервера. Згідно вимогами HTTP–протоколу, браузер відправляє GET -запит серверу і просить файл index.html. Сервер відправляє браузеру HTML -код цієї веб-сторінки. І нарешті, браузер декодує HTML -код і форматує сторінку у вікні браузеру.

9.2. Однорангові мережі

При доступі до даних на мережевому пристрої, підключеному до мережі (наприклад на ПК, ноутбуку, планшетному ПК, смартфоні), ці дані можуть не зберігатися фізично на цьому пристрої. В цьому випадку необхідно виконати запит на отримання даних з пристрою, на якому розміщені ці дані. У моделі однорангової мережі (P2P, peer-to-peer) дані просяться з рівноправного пристрою без використання виділеного сервера.

Мережева модель P2P полягає двох частин: P2P -мереж і P2P -додатків. Обидві частини мають схожі функції, але принцип їх роботи відрізняється.

У P2P -мережі два комп'ютери (чи більше двох) підключаються між собою по мережі і можуть відкривати доступ до своїх ресурсів (наприклад, до принтерів і файлів) без використання виділеного сервера. Кожен підключений до мережі крайовий пристрій може виконувати функції як сервера, так і клієнта. Один комп'ютер може грати роль сервера для однієї операції, одночасно виступаючи в ролі клієнта для інших операцій. Функції клієнта і сервера встановлюються за запитом.

У P2P -мережі використання ресурсів в мережі децентралізоване. Замість обміну файлами через виділені сервери дані можна розмістити в будь-якій теці на будь-якому підключеному пристрої. Більшість сучасних ОС підтримують відкриття загального доступу до файлів і принтерів без додаткового серверного ПЗ. Проте в P2P -мережах не ведеться централізоване управління обліковими записами користувачів і правами їх доступу. Тому в мережах, що містять велику кількість комп'ютерів, нелегко застосовувати політики безпеки і доступу. Облікові записи користувачів і права доступу повинні окремо настроюватися на кожному пристрої.

Однорангове застосування (P2P) дозволяє пристрою виступати в ролі як клієнта, так і сервера в межах одного сеансу зв'язку. У цій моделі кожен клієнт зв'язаний з серверним модулем, а кожен сервер має клієнтський модуль. Обоє з них можуть почати сеанс зв'язку і вважаються рівноправними в процесі обміну даними. Проте для P2P -додатків потрібно, щоб кожен крайовий пристрій надавав користувацький інтерфейс і запускав сервіс у фоновому режимі. P2P -додаток при запуску відкриває відповідний користувацький інтерфейс і запускає фонові сервіси. Після цього пристрою можуть обмінюватися даними безпосередньо.

У деяких P2P -додатках використовується гібридна система, де загальний доступ до ресурсів децентралізований, а індекси, що вказують на місця розташування ресурсів, зберігаються в центральному каталозі. У гібридній системі кожен вузол звертається до сервера індексації, щоб отримати місце розташування ресурсу, який зберігається на іншому вузлі. Сервер індексації також може допомагати вузлам підключатися один до одного, але після установки з'єднання вузли обмінюються даними без додаткового звернення до сервера.

P2P -додатки можуть використовуватися в однорангових мережах, в мережах моделі «клієнт-сервер» і в мережі Інтернет.

Усі комп'ютери в мережі, на яких запущено P2P -додатки, можуть виступати в ролі клієнта або сервера для інших комп'ютерів в мережі з цим же застосуванням. Найбільш поширені P2P -застосування:

- EDonkey;
- eMule;
- Shareaza;
- BitTorrent;
- Bitcoin;
- LionShare.

Деякі P2P -додатки засновані на протоколі Gnutella. Вони дозволяють відкривати доступ до файлів на жорстких дисках іншим користувачам. Клієнтське ПЗ, сумісне з протоколом Gnutella, дозволяє користувачам підключатися до сервісів Gnutella через інтернет, а також знаходити і використовувати ресурси, доступ до яких був відкритий іншими вузлами

Gnutella. Для доступу до мережі Gnutella існує безліч клієнтських застосувань, у тому числі: Gnucleus, BearShare, Morpheus, LimeWire, WinMX і XoloX.

Форум розробників Gnutella підтримує базовий протокол, тоді як постачальники застосувань нерідко створюють розширення для цього протоколу, щоб поліпшити його роботу зі своїми застосуваннями.

У більшості P2P -додатків для запису усіх файлів, доступних на однорангових пристроях, не використовується централізована БД. Замість цього кожен з цих пристроїв в мережі при отриманні відповідного запиту повідомляє інші, які файли доступні, і потім використовує протокол файлового обміну і аналогічні сервіси для допомоги при визначенні місцезнаходження ресурсів.

Процеси моделі типу «клієнт-сервер» відбуваються на рівні застосувань. Клієнт починає обмін даними, відправляючи запит на отримання даних з сервера, який у відповідь відправляє один або декілька потоків даних клієнтові. Протоколи рівня застосувань описують формат запитів і відповідей між клієнтами і серверами. На додаток до фактичної передачі даних для цього обміну даними також може знадобитися аутентифікація користувачів і ідентифікація передаваних файлів даних.

Одним з прикладів мережі типу «клієнт-сервер» є використання сервісу електронної пошти для відправки, отримання і зберігання повідомлень електронної пошти. Поштовий клієнт на домашньому комп'ютері відправляє запит серверу електронної пошти на отримання списку нових повідомлень. Сервер відповідає, відправляючи запрошене повідомлення клієнта. Потік даних може бути рівним в обох напрямах або бути більше в напрямі від клієнта до сервера. Наприклад, клієнт може передавати файл на сервер для зберігання.

9.3. Протоколи HTTP і HTTPS

Протокол HTTP призначений для передачі даних і є найбільш використовуваних протоколів рівня застосувань. Спочатку цей протокол розроблявся тільки для публікації і отримання HTML -сторінок. Проте завдяки своїй гнучкості він став найбільш важливим елементом в розподілених інформаційних системах.

Протокол HTTP заснований на механізмі «запит-відгук». Коли клієнт (зазвичай веб-браузер) відправляє запит веб-серверу, протокол HTTP визначає типи повідомлень для цієї взаємодії.

Три основні типи повідомлень: **GET, POST і PUT.**

GET – це запит даних клієнтом. Клієнт (веб-браузер) відправляє повідомлення GET веб-серверу, щоб запросити HTML -сторінки. Коли сервер отримує запит GET, він повертає рядок стану «HTTP/1.1 200 OK» і своє повідомлення. Відповідь сервера може містити запрошений HTML -файл (якщо він доступний) або повідомлення про помилку, наприклад: «The location of the requested file has changed».

Запити **POST і PUT** використовуються для відправки файлів даних на веб-сервер. Наприклад, якщо користувач вводить дані у форму, яка вбудована у веб-сторінку (наприклад при оформленні замовлення), веб-серверу вирушає повідомлення POST. Повідомлення POST містить дані, вказані користувачем у формі.

Запит PUT відправляє на веб-сервер ресурси або вміст. Наприклад, якщо користувач намагається відправити файл або зображення на веб-сайт, клієнт відправляє серверу PUT з вкладеним файлом або зображенням.

Не дивлячись на те, що протокол HTTP досить гнучкий, він не є безпечним. Повідомлення запитів передаються серверу відкритим текстом, який може бути перехоплений і прочитаний. Аналогічним чином, відповіді сервера (звичайно це HTML – сторінки) також передаються в незашифрованому виді.

Для захищеного двостороннього обміну даними з веб-серверами в Інтернеті використовується протокол HTTPS. HTTPS дозволяє використовувати аутентифікацію і

шифрування для захисту даних, що пересилаються між клієнтом і сервером. Протокол HTTPS визначає додаткові правила передачі даних між рівнем застосування і транспортним рівнем. У протоколах HTTPS і HTTP процеси «клієнт просить – сервер відповідає» аналогічні, але потік даних шифрується за допомогою SSL (Secure Sockets Layer) перед початком передачі по мережі. HTTPS створює додаткове навантаження і вимагає тривалішої обробки на сервері через необхідність шифрування і розшифрування трафіку.

При використанні моделі TCP/IP повний процес обміну даними складається з шести кроків.

Створення даних на рівні застосувань початкового крайового пристрою. В цьому випадку після створення запиту веб-клієнта (HTTP GET) ці дані будуть закодовані, стислі і, якщо необхідно, зашифровані. Цей процес виконується на рівні застосувань моделі TCP/IP, але до нього також відносяться функції, описані рівнем застосувань, рівнем представлення і сеансовим рівнем моделі OSI. Після рівня застосувань ці дані передаються у вигляді потоку на транспортний рівень.

Сегментація і інкапсуляція даних у міру їх проходження по стеку протоколів. На транспортному рівні повідомлення HTTP GET буде розбите на дрібніші, більш керовані частини, в кожну з яких буде доданий заголовок транспортного рівня. У заголовках транспортного рівня знаходяться індикатори, за якими можна буде відтворити повідомлення. У заголовок також додається ідентифікатор – номер порту 80. Він повідомляє кінцевий сервер, що повідомлення призначене для застосування веб-сервера. Також додається згенерований випадковим чином початковий порт, щоб клієнт зміг отримати повідомлення у відповідь і переслати його відповідному клієнтському застосуванню.

Далі в сегменти додаються ідентифікатори адреси. Завдання мережевого рівня – додати адресацію, щоб забезпечити передачу даних з початкового вузла на вузол, який їх використовує. На мережевому рівні це виконується шляхом інкапсуляції кожного сегменту в заголовок IP -пакета. Заголовок IP -пакета містить IP -адреси початкового і крайового пристроїв. (IP -адреса цільового пристрою, як правило, визначається службою доменних імен.)

Після додавання IP -адресації пакет передається на рівень мережевого доступу для генерації даних у фізичному середовищі. Для цього на рівні мережевого доступу пакет спочатку має бути підготовлений до передачі шляхом приміщення його в кадр із заголовком і кінцевиком. Цей кадр містить фізичну адресу початкового вузла, а також фізичну адресу наступного вузла на шляху до місця призначення. Це відповідає другому (чи канальному) рівню моделі OSI. Рівень 2 забезпечує доставку повідомлень в одній локальній мережі. Адреса рівня 2 є унікальною в локальній мережі і представляє адресу крайового пристрою у фізичному середовищі.

Кадр після підготовки на рівні мережевого доступу з додаванням IP -адрес джерела і призначення кодується в послідовність бітів, а потім - в електричні імпульси або спалахи світла, які передаються по кабелях мережі.

Якщо вузол призначення знаходиться в одній мережі з початковим вузлом, пакет передається між двома цими вузлами по локальному носію без маршрутизації. Проте якщо вузол призначення і початковий вузол знаходяться в різних мережах, пакети можуть передаватися в різних мережевих середовищах, по різних носіях і між багатьма маршрутизаторами. У міру проходження пакетів в мережі інформація в кадрах змінюється.

На межі кожної локальної мережі проміжний мережевий пристрій (маршрутизатор) витягає з кадру пакет, щоб прочитати в заголовку адресу вузла призначення. Маршрутизатори використовують мережеву частину адреси, щоб визначити, який шлях використовувати, щоб досягти вузла призначення. Після визначення шляху маршрутизатор інкапсулює пакет в новий кадр і пересилає його наступному вузлу на шляху до крайового пристрою призначення.

В результаті пристрій призначення отримує кадр. У міру зворотного проходження даних по стеку на кінцевому пристрої відбувається деінкапсуляція і повторна зборка даних. Дані

безперервно слідують вгору по рівнях з мережевого доступу на мережевий рівень до транспортного рівня, поки, нарешті, не досягнуть рівня застосувань, де їх можна буде обробити. Але як пристрій може переконатися в правильності визначення процесу застосування? На транспортному рівні дані в заголовку PDU визначають конкретний процес або сервіс, які запущені на пристрої вузла призначення і оброблятимуть дані. На вузлах, незалежно від того, чи являються вони клієнтами або серверами в Інтернеті, може бути одночасно запущено декількох мережевих застосувань. У користувачів, що працюють на ПК, часто можуть бути одночасно запущені поштовий клієнт, веб-браузер, програма обміну миттєвими повідомленнями, потокове мультимедіа або гра. Усі ці незалежно працюючі програми є прикладами окремих процесів.

При перегляді веб-сторінки активується як мінімум один мережевий процес. Перехід по гіперпосиланню примушує браузер встановити з'єднання з веб-сервером. В той же час у фоновому режимі поштовий клієнт може відправляти і приймати електронну пошту, а колега користувача може відправляти йому миттєве повідомлення.

9.4. Протоколи SMTP, POP і IMAP

Одна з основних послуг інтернет-провайдера – це розміщення серверів електронної пошти. Електронна пошта радикально змінила способи спілкування між користувачами завдяки її зручності і швидкості передачі даних. Але для того, щоб електронна пошта запрацювала на комп'ютері або іншому крайовому пристрої, потрібний ряд застосувань і сервісів.

Електронна пошта – це набір засобів для доставки, зберігання і пошуку електронних повідомлень в мережі. Повідомлення електронної пошти зберігаються на серверах електронної пошти в базах даних. Інтернет-провайдери часто встановлюють сервери електронної пошти, що містять облікові записи безлічі клієнтів.

Клієнти електронної пошти для відправки і отримання повідомлень звертаються до серверів електронної пошти. Сервери електронної пошти взаємодіють з іншими серверами електронної пошти для обміну повідомленнями між доменами. Поштовий клієнт не з'єднується безпосередньо з іншим поштовим клієнтом для відправки повідомлення. Обидва клієнти повинні довірити транспортування повідомлень сервера електронної пошти. Це вірно навіть у тому випадку, якщо обидва користувачі знаходяться в одному домені.

Клієнти електронної пошти відправляють повідомлення на сервер, вказаний в налаштуваннях застосування. Отримавши повідомлення, сервер перевіряє, чи є присутнім вказаний у ньому домен одержувача в локальній БД сервера. Якщо домен відсутній в БД, сервер відправляє запит DNS, щоб визначити IP -адресу поштового сервера пошти в домені одержувача. Електронна пошта потім пересилається на відповідний сервер.

Для роботи з електронною поштою використовуються три окремі протоколи: SMTP, POP і IMAP. В процесі рівня застосувань, при якому виконується відправка пошти, використовується протокол SMTP. Це відбувається при відправці повідомлень від клієнта на сервер, а також при відправці з одного сервера на інший.

Проте отримання електронної пошти клієнтом виконується по одному з двох протоколів рівня застосувань: POP або IMAP.

Протокол SMTP використовується для надійної і ефективної передачі електронної пошти. Для нормальної роботи SMTP-додатку потрібно, щоб поштові повідомлення були правильно відформатовані, а на клієнтові та сервері мають бути завантажені процеси SMTP.

У форматі SMTP повідомлення складається із заголовка і тіла повідомлення. Якщо тіло повідомлення може містити текст довільної довжини, то заголовок повинен містити адреси електронної пошти одержувача і відправника в правильному форматі. Усі інші елементи заголовка є необов'язковими.

Коли клієнт відправляє повідомлення електронної пошти, процес SMTP -клієнта підключається до процесу SMTP -сервера на широко відомому порту 25. Встановивши

з’єднання, клієнт намагається відправити по ньому повідомлення електронної пошти сервера. Коли сервер отримує повідомлення, він поміщає його в чергу повідомлень локального облікового запису або пересилає іншому серверу, виконавши такий же процес установки SMTP –з’єднання.

Цільовий сервер електронної пошти у момент доставки повідомлення може виявитися недоступним або перевантаженим. На цей випадок в SMTP передбачено тимчасове зберігання з’єднань з наступною повторною відправкою. Періодично сервер перевіряє чергу повідомлень і намагається відправити їх повторно. Якщо повідомлення не вдається доставити впродовж встановленого часу, воно повертається відправникові з повідомленням про неможливість доставки.

Протокол POP дозволяє робочим станціям отримувати повідомлення електронної пошти з серверів електронної пошти. При використанні протоколу POP повідомлення завантажуються клієнтом з сервера і віддаляються на сервері.

Мережевий сервіс POP на сервері пасивно чекає запитів підключення клієнтів до TCP - порту 110. Для використання цього мережевого сервісу клієнт просить TCP - з’єднання з сервером. Після установки з’єднання сервер POP посилає вітання. Потім клієнт і сервер POP обмінюються командами і відгуками, поки підключення не буде закрито або перерване.

Оскільки повідомлення електронної пошти завантажуються клієнтом і віддаляються з сервера, це означає, що вони не зберігаються централізовано. З цієї причини протокол POP недоцільний в рішенні для малого бізнесу з централізованим резервним копіюванням.

Протокол POP3 підходить для використання інтернет-провайдером, оскільки він знімає з нього відповідальність за зберігання великого об’єму даних на серверах електронної пошти.

Протокол доступу до повідомлень в Інтернеті (IMAP) передбачає інший метод витягання поштових повідомлень з сервера. Його відмінність від POP полягає в тому, що при підключенні користувача до сервера IMAP в клієнтське застосування завантажуються тільки копії повідомлень. Початкові повідомлення залишаються на сервері до тих пір, поки вони не будуть видалені вручну. Користувачі переглядають копії повідомлень в клієнтах електронної пошти.

Користувачі можуть організувати на сервері ієрархічну файлову структуру для впорядкування і зберігання пошти. Ця структура також дублюється клієнтом електронної пошти. Якщо користувач вирішує видалити повідомлення, воно синхронно видаляється з клієнта і з сервера.

Малим і середнім підприємствам протокол IMAP надає безліч переваг. IMAP забезпечує довгострокове зберігання поштових повідомлень на серверах електронної пошти і їх централізоване резервне копіювання. Він також дозволяє співробітникам працювати з повідомленнями з будь-якого місця, використовуючи різні пристрої і клієнтське ПЗ. Звична для користувача структура тек поштової скриньки не залежить від того, яким чином користувач звертається до поштової скриньки.

Для інтернет-провайдера протокол IMAP, можливо, не є кращим вибором. Можуть знадобитися істотні витрати на придбання і обслуговування великих дискових сховищ для великого об’єму кореспонденції. Крім того, якщо клієнти вимагають регулярного резервного копіювання своїх поштових скриньок, витрати інтернет-провайдера зростуть ще більше.

9.5. Служба доменних імен

У мережах передачі даних пристрою ідентифікуються за числовими IP -адресами для відправки і отримання даних. Більшість користувачів не в змозі запам’ятати ці числові адреси. Доменні імена були створені для того, щоб перетворити числову адресу в просте і легко таке, що запам’ятовується ім’я. У Інтернеті імена доменів, такі як http://www.cisco.com, легше запам’ятати, чим 198.133.219.25, який є фактичною адресою цього сервера в числовому виді. Якщо компанія Cisco вирішить змінити числову адресу www.cisco.com, це станеться непомітно для користувачів, оскільки ім’я домена залишиться без змін. Нова

адреса буде просто прив’язана до існуючого імені домена без порушення зв’язку з сервером. У невеликих мережах імена доменів було нескладно зіставляти їх з числовими адресами. У міру зростання мереж і кількості пристроїв це завдання стало практично неможливо виконувати вручну.

Служба доменних імен (DNS) була створена спеціально для перетворення доменних імен в адреси в таких мережах. У DNS використовується розподілена множина серверів для перетворення імен, пов’язаних з чисельними адресами. Протокол DNS визначає автоматизований сервіс, який зіставляє імена ресурсів з відповідними числовими мережевими адресами. У цьому протоколі описується формат для запитів, відповідей і самих даних. Такий формат повідомлення використовується для усіх типів запитів клієнта і відповідей сервера, повідомлень про помилки і передачі записів ресурсів між серверами.

DNS -сервер забезпечує дозвіл імен за допомогою програми для підтримки сервера імен доменів (**BIND**, Berkeley Internet Name Domain) або управляючі програми. Служба BIND була розроблена чотирма студентами Каліфорнійського університету в Берклі на початку 80-х років. Формат повідомлень DNS, в BIND є найпоширенішим форматом DNS в мережі Інтернет.

На DNS -серверах зберігаються різні типи записів ресурсів для дозволу імен. Ці записи містять ім’я, адресу і тип запису.

До деяких типів записи відносяться:

- **A** - адреса крайового пристрою;
- **NS** - довірений сервер імен;
- **CNAME** - повне доменне ім’я для канонічного імені; використовується, коли декілька сервісів мають одну мережеву адресу, але для кожного з них є окремий запис в DNS;
- **MX** - запис для обміну поштою; зв’язує ім’я домена із списком поштових серверів для цього домена.

Коли клієнт виконує запит, процес BIND сервера спочатку шукає це ім’я у своїх записах, щоб дозволити його. Якщо ім’я не вдалося дозволити по локальних записах, сервер звертається до інших серверів для дозволу імені.

Запит може пересилатися по декількох серверах, на що можуть знадобитися додатковий час і пропускна спроможність мережі. Числова адреса після знаходження повертається початковому серверу, який певний час зберігає цей запис у своїй кеш-пам’яті.

При повторному запиті цього ж імені перший сервер може повернути адресу, використовуючи значення, яке зберігається в кеші імен. Кешування знижує трафік DNS-даних в мережі і навантаження серверів на більш високому рівні в ієрархії. Служба «Клієнт DNS» на ПК з ОС Windows оптимізує продуктивність дозволу імен DNS, також зберігаючи раніше дозволені імена в пам’яті. На ПК з ОС Windows команда ipconfig /displaydns виводить на екран усі кешовані записи DNS.

У протоколі DNS використовується ієрархічна структура для створення БД і дозволу імен. Ця ієрархія виглядає як перевернуте дерево з коренем вгорі і гілками, що ростуть вниз (рис. 9.3).

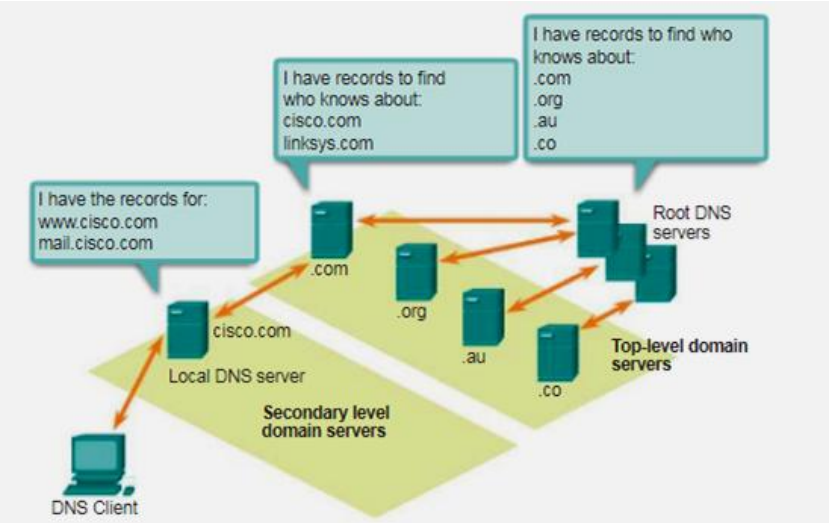


Рис. 9.3. Ієрархія DNS серверів (містить записи ресурсів, за якими імена співставляються з адресами) [1]

Ієрархічна структура DNS будується за іменами доменів і підрозділяється на невеликі керовані зони. У кожного DNS -сервера є окремий файл з базою даних. Сервер управляє прив'язкою імен до IP -адрес тільки в невеликій частині загальної структури DNS. Отримавши запит на перетворення імені, що не відноситься до власної зони DNS, DNS -сервер пересилає цей запит на обробку іншому DNS -серверу у відповідній зоні.

DNS – це масштабована служба дозволу імен вузлів, яка розподілена по множині серверів мережі.

Різні домени верхнього рівня представляють або певний вид організації, або країну походження. Приклади доменів верхнього рівня :

- **..au –** Австралія;
- **..co –** Колумбія;
- **..com -** комерційні або промислові підприємства;
- **..jp –** Японія;
- **..org -** некомерційні організації.

Під доменами верхнього рівня знаходяться домени другого рівня, а під ними – домени нижчих рівнів. Доменне ім'я – шлях в цьому перевернутому дереві, що починається від кореневого елементу. Наприклад, кореневий DNS -сервер може не знати про те, де знаходиться запис для поштового сервера mail.cisco.com, але у нього є запис для домена верхнього рівня com. Аналогічним чином, на серверах домена .com також може бути відсутнім запис вузла для mail.cisco.com, але при цьому міститиметься запис домена cisco.com. На серверах домена cisco.com є запис (точніше, запис MX) для mail.cisco.com.

Саме ця ієрархія децентралізованих серверів в системі DNS відповідає за зберігання і ведення записів ресурсів. Записи містять імена доменів, які може дозволити сервер, а також посилання на альтернативні сервери, які можуть також обробляти запити. Якщо на сервері є записи, які відповідають його рівню в ієрархії доменів, він вважається довіреним сервером для цих записів. Наприклад, сервер імен в домені cisco.netacad.net не буде довіреним сервером для запису mail.cisco.com, тому що цей запис зберігається на сервері більше високого рівня.

Служба DNS – це сервіс типу «клієнт-сервер», але вона відрізняється від інших сервісів. Якщо для інших сервісів використовується клієнт, що є застосуванням (наприклад веб-браузер, поштовий клієнт), то клієнт DNS працює як сервіс. Клієнт DNS, якого іноді називають перетворювачем (імен) DNS, забезпечує дозвіл імен для інших мережевих застосувань і сервісів, яким це потрібно.

При налаштуванні мережевого пристрою ми зазвичай вказуємо один або декілька адрес DNS -серверів, які клієнт DNS може використовувати для дозволу імен. Зазвичай адреси

DNS -серверів надаються інтернет-провайдером. Коли призначене для користувача застосування просить підключення до видаленого пристрою по його імені, клієнт DNS опитує один з цих серверів імен, щоб перетворити ім'я в числову адресу.

У ОС комп'ютерів зазвичай є програма **nslookup**, яка дозволяє користувачеві вручну опитувати сервери для дозволу імен. Цю програму можна також використовувати для усунення проблем з дозволом імен і для перевірки поточного стану серверів імен.

9.6. Протокол динамічної конфігурації мережевого вузла

Служба DHCP дозволяє пристроям в мережі отримувати IP –адреси та іншу інформацію з сервера DHCP. Ця служба автоматизує виділення IP -адрес, масок підмережі, шлюзу та інших параметрів IP-мережі. Такий процес називається **динамічною адресацією.** Альтернативою динамічній адресації є статична адресація. При використанні статичної адресації адміністратор мережі вручну вводить дані IP -адрес на вузлах мережі.

DHCP дозволяє вузлам динамічно отримувати IP -адреси при підключенні до мережі. Вузол зв'язується з сервером DHCP і просить адресу. DHCP сервер вибирає адресу із заданого діапазону адрес, який називається **пулом**, і призначає (здає в оренду) його вузлу на певний період часу.

У більших локальних мережах, а також в мережах з користувачами адреси, що часто міняються, переважно призначати за допомогою DHCP. Можуть з'явитися нові користувачі з ноутбуками, яким треба підключитися до мережі. А іншим користувачам можуть встановити нові робочі станції, які також треба підключити до мережі. Щоб кожної станції не доводилося вручну привласнювати IP -адреси, найпростіше це зробити автоматично за допомогою DHCP.

Адреси DHCP привласнюються вузлам не назавжди, а тільки на певний період часу. Якщо вузол вимикається або йде з мережі, його адреса повертається в пул для повторного використання. Це особливо корисно для мобільних користувачів, які то підключаються, то відключаються. Користувачі можуть вільно перейти на інше робоче місце і знову підключитися до мережі. Вузол може отримати IP -адрес після установки з'єднання в дротяній або безпровідній локальній мережі.

DHCP забезпечує доступ в Інтернет в зонах безкоштовного безпровідного доступу в аеропортах і кафе. Коли пристрій потрапляє в зону дії точки безпровідного доступу, DHCP -клієнт пристрою зв'язується через безпровідне з'єднання з локальним DHCP -сервером, який у свою чергу призначає пристрою IP -адресу.

Без DHCP для приєднання до мережі користувачі повинні вручну вказати IP -адресу, маску підмережі та інші мережеві параметри. Сервер DHCP обслуговує пул IP -адрес і видає тимчасові адреси усім клієнтам з налагодженим DHCP, коли клієнт включається. Оскільки IP -адреси є динамічними (надаються в оренду), а не статичними (призначаються назавжди), невживані адреси автоматично повертаються в пул для повторного призначення. У той час, коли пристрій з налагодженим DHCP завантажується і підключається до мережі, клієнт виконує широкомовну розсилку повідомлення виявлення DHCP (DHCPDISCOVER), щоб знайти в мережі усі доступні сервери DHCP. Сервер DHCP відповідає сполученням з пропозицією DHCP (DHCPOFFER), яка дозволяє клієнтові орендувати адресу. Сполучення з пропозицією містить IP-адресу і маску підмережі, IP -адресу DNS -сервера та IP -адресу шлюзу за замовчуванням. У пропозиції оренди також вказується її термін.

Клієнт може отримати декілька повідомлень DHCPOFFER, якщо в локальній мережі є декілька серверів DHCP. Тому клієнт повинен вибрати один з серверів, для чого він відправляє сполучення із запитом DHCP (DHCPREQUEST), в якому вказується конкретний сервер і пропозиція оренди, яка приймає клієнт. Клієнт також може запросити адресу, яка раніше була присвоєна йому сервером.

Якщо IP -адреса, що проситься клієнтом або пропонована сервером, як і раніше доступна, сервер повертає з'єднання з підтвердженням DHCP (DHCPACK), яке підтверджує клієнтові,

що оренда адреси була продовжена. Якщо пропозиція більше не дійсна (наприклад, витік час очікування або інший клієнт орендував адресу), вибраний сервер відповідає з'єднанням з негативним підтвердженням DHCP (DHCPNAK). Якщо повернено повідомлення DHCPNAK, процес вибору повинен початися повторно з відправкою нового повідомлення DHCPDISCOVER. Після того, як клієнт орендував адресу, оренду необхідно буде продовжити до закінчення терміну її дії за допомогою іншого повідомлення DHCPREQUEST.

DHCP - сервер забезпечує унікальність усіх IP -адрес (одна IP -адреса не може бути призначена одночасно двом різним мережевим пристроям). Використання протоколу DHCP дозволяє мережевим адміністраторам легко перенастроювати IP -адреси клієнтів без необхідності вручну робити зміни на клієнтах. Більшість інтернет-провайдерів використовують DHCP для виділення адрес своїм клієнтам, яким не потрібна статична адреса.

9.7. Протокол передачі файлів (FTP)

Протокол передачі файлів (FTP) – інший поширений протокол рівня застосувань. FTP був розроблений для передачі даних між клієнтом і сервером.

FTP -клієнт – це застосування, яке запускається на комп'ютері, а також відправляє і приймає дані з сервера, на якому запущена служба FTP.

Для передачі даних по FTP потрібно два з'єднання між клієнтом і сервером: одне для команд і відповідей, інше – для фактичної передачі файлів.

- Клієнт встановлює перше з'єднання з сервером для управління трафіком, який складається з команд клієнта і відповідей сервера.
- Потім клієнт встановлює друге з'єднання з сервером для безпосередньої передачі даних. Це підключення створюється для кожної передачі даних.

Дані можуть передаватися у будь-якому напрямі. Клієнт може завантажити (прийняти) дані з сервера або відправити дані на сервер.

9.8. Протокол обміну блоками серверних повідомлень

Протокол обміну блоками серверних повідомлень (**SMB**, Server Message Block) – це протокол обміну файлами між клієнтом і сервером, який був розроблений компанією IBM у кінці 1980-х років для опису структури загальних ресурсів мережі, таких як каталоги, файли, принтери і послідовні порти. Це протокол типу «запит-відповідь».

Протокол SMB описує доступ до файлової системи і спосіб запиту файлів клієнтами. Він також описує зв'язок між процесами SMB. Усі повідомлення SMB мають загальний формат. У цьому форматі використовується фіксована довжина заголовка, після якого слідує параметр змінного розміру і компонент даних.

За допомогою повідомлень SMB можна виконувати наступні дії:

- здійснювати запуск, аутентифікацію і завершення сеансів;
- управляти доступом до файлів і принтерів;
- дозволяти застосуванню відправляти повідомлення на інший пристрій і приймати їх.

Загальний доступ до файлів і служб друку на основі SMB є відмітною особливістю мереж Microsoft. Починаючи з серії систем Windows 2000, компанія Microsoft змінила базову архітектуру для використання протоколу SMB. У попередніх версіях продуктів Microsoft в службах SMB для дозволу імен використовувався протокол, відмінний від TCP/IP і не використовувався сервіс DNS. Починаючи з версії Windows 2000, в усіх наступних продуктах Microsoft використовується система імен DNS, яка дозволяє протоколам стека TCP/IP безпосередньо підтримувати загальні ресурси SMB. На відміну від обміну файлами по протоколу FTP, клієнти встановлюють довготривале підключення до серверів. Після установки з'єднання користувач може дістати доступ до ресурсів на сервері, якщо цей ресурс є локальним по відношенню до вузла клієнта.

Операційні системи LINUX і UNIX також дозволяють відкривати загальний доступ до ресурсів в мережах Microsoft, використовуючи версію SMB під назвою SAMBA. Операційні системи Apple Macintosh також підтримують роботу із загальними ресурсами по протоколу SMB.

Висновок до лекції 9

Рівень застосувань відповідає за прямий доступ до базових процесів, які управляють обміном даними в мережі. Цей рівень виконує роль джерела і одержувача повідомлень в мережах передачі даних. Застосування, сервіси і протоколи рівня застосувань дозволяють користувачам взаємодіяти з мережею передачі даних ефективним і зрозумілим чином.

- Застосування – це комп'ютерні програми, за допомогою яких користувач може почати процес передачі даних.
- Сервіси – це фонові програми, які забезпечують зв'язок між рівнем застосувань і нижчими рівнями мережевої моделі.
- Протоколи є структурою загальноприйнятих правил і процесів, за допомогою яких сервіси, що виконуються на одному пристрої, можуть обмінюватися даними з рядом різних мережевих пристроїв.

Дані можуть доставлятися по мережі за запитом клієнта до сервера або між пристроями, що працюють в одноранговій мережі P2P, де встановлені зв'язки типу «клієнт-сервер», згідно з якими пристрій є одночасно джерелом і одержувачем. Для установки і використання цих зв'язків служби рівня застосувань на усіх крайових пристроях обмінюються повідомленнями відповідно до специфікацій протоколу.

Наприклад, протоколи типу HTTP підтримують функцію доставки веб-сторінок на крайові пристрої. Протоколи SMTP і POP підтримують відправку і отримання електронної пошти. Протоколи SMB і FTP дозволяють користувачам відкривати доступ до своїх файлів.

P2P –додатки спрощують обмін файлами у розподіленій мережі. Служба DNS перетворить зручні для сприйняття людиною імена, що вказують на мережеві ресурси, в числові адреси в мережі.

Питання для закріплення

1. Які функції і протоколи прикладного рівня TCP/IP ви знаєте?
2. Для чого використовуються однорангові мережі?
3. У чому відмінності протоколів HTTP і HTTPS?
4. Яке призначення протоколів SMTP, POP і IMAP?
5. Для чого використовується служба доменних імен?
6. Для чого викоистовується протокол DHCP?
7. Для чого викоистовується протокол FTP?
8. Для чого викоистовується протокол SMB?

Список рекомендованої літератури

1. CCNA R&S ITN Chapter 10: Application Layer // Електронний ресурс. Режим доступу: http://static-course-assets.s3.amazonaws.com/IntroNet50ENU/module10/index.html

2. What Is P2P // Електронний ресурс. Режим доступу: http://www.openp2p.com/pub/a/p2p/2000/11/24/shirky1-whatisp2p.html

3. BIND Open Source DNS Server // Електронний ресурс. Режим доступу: https://www.isc.org/downloads/bind/

Лекція 10. Тема: «Засоби мережевої безпеки»

План лекції

10.1. Категорії погроз безпеки мереж.
10.2. Резервне копіювання, оновлення і установка виправлень.
10.3. Аутентифікація, авторизація і облік.
10.4. Міжмережеві екрани.
10.5. Захист крайових і мережевих пристроїв.
10.6. Включення протоколу SSH.
10.7. Використання спеціальних команд.
10.8. Основи безпеки безпровідних підключень.

10.1. Категорії погроз безпеки мереж

Мережева безпека є невід'ємною частиною комп'ютерних мереж, незалежно від їх масштабів: починаючи з домашньої мережі, де до Інтернету підключений лише один комп'ютер, до корпоративної мережі, що налічує тисячі користувачів. Забезпечення мережевої безпеки повинне брати до уваги існуюче середовище, інструменти і вимоги мережі. Воно повинне забезпечувати безпеку даних, і в той же час надавати якість обслуговування, відповідно до вимог до мережі.

До забезпечення безпеки мережі відносяться протоколи, технології, пристрої, інструменти і методи забезпечення безпеки даних і зниження наслідків погроз. Багато зовнішніх загроз для безпеки мережі сьогодні поширюються через інтернет. Найбільш поширены зовнішні загрози:

- **Віруси, черв'яки і «троянські коні»** - шкідливе ПЗ і довільний код, що працює на пристроях користувача.
- **Шпигунське і рекламне ПЗ** - ПЗ, встановлюване на пристрій користувача і таємно збираюче відомості про користувача.
- **Атаки нульового дня, також звані атаками нульової години,** - здійснюються в перший день, коли про уразливість стане відомо.
- **Хакерські атаки** - атаки, здійснювані користувачем, які має інформацію, що працює проти пристроїв кінцевих користувачів або мережевих ресурсів.
- **Атаки типу «відмова в обслуговуванні»** - атаки, розроблені для зниження продуктивності або аварійного завершення процесів на мережевому пристрої.
- **Перехоплення і розкрадання даних** - атака з метою збору приватної інформації з корпоративної мережі.
- **Крадіжка особистої інформації** - атака для розкрадання облікових даних користувача, щоб дістати доступ до даних приватного характеру.

Жодне подібне рішення по забезпеченню безпеки не в силах повністю узабезпечити мережу від численних сучасних погроз. Саме тому заходи по забезпеченню мережевої безпеки необхідно впроваджувати відразу на декількох рівнях, задіявши одночасно декілька рішень. Якщо один компонент безпеки не може визначити і захистити мережу, то інші з цими завданнями впораються.

Реалізації політики мережевої безпеки для будинку, як правило, досить прості. Вони зазвичай реалізовані на фізичних вузлах, що підключаються, а також на точці підключення до Інтернету, і можуть навіть покладатися на сервіси, що надаються за контрактом постачальником послуг Інтернету.

Реалізації політики мережевої безпеки для корпоративної мережі, навпаки, зазвичай включають безліч компонентів, вбудованих в мережі для контролю і фільтрації трафіку. У ідеалі передбачається, що усі компоненти працюють разом, що знижує об'єм обслуговування і підвищує безпеку.

Компоненти безпеки мереж для будинку або в мережах малих офісів повинні містити як мінімум:

- **антивірусне і антишпигунське ПЗ** - захист пристрою кінцевих користувачів від вірусів і від шкідливого ПЗ;
- **фільтрація на міжмережевому екрані** - блокування спроб несанкціонованого доступу до мережі Вони можуть включати систему реалізованих на вузлі міжмережевих екранів, яка використовується для запобігання несанкціонованому доступу до пристрою вузла, або базовий сервіс фільтрації на домашньому маршрутизаторі для запобігання несанкціонованому доступу із зовнішнього світу в мережу.

Окрім вищепереліченого, в більших мережах і корпоративних мережах часто є інші вимоги безпеки :

- **виділені системи міжмережевих екранів** - забезпечення досконаліших функціональних можливостей міжмережевого екрану, який може фільтрувати велику кількість трафіку з більшою деталізацією;
- **списки контролю доступу (ACL)** - подальша фільтрація доступу, а також забезпечення пересилки трафіку;
- **системи запобігання вторгненням (IPS)** - визначення погроз, що швидко поширюються, таких як атаки нульового дня або атаки нульової години;
- **віртуальні приватні мережі (VPN)** - забезпечення безпечного доступу для віддалених співробітників.

Вимоги безпеки повинні враховувати мережеве середовище, а також різні застосування і вимоги до обчислювальних пристроїв. І домашньому середовищу, і підприємствам необхідно забезпечувати безпеку своїх даних, але в той же час удосконалювати якість обслуговування, якого чекають користувачі кожної технології. Крім того, впроваджені рішення для забезпечення безпеки повинні легко адаптуватися до зростаючих тенденцій мережі, що змінюються.

Дротяні і безпровідні комп'ютерні мережі грають найважливішу роль в повсякденному житті. Фізичні особи і організації в рівній мірі залежать від своїх комп'ютерів і мереж. Несанкціоноване вторгнення в мережу може привести до надзвичайно витратних перебоїв і втрати важливих результатів роботи. Атака на мережу може мати руйнівні наслідки з втратою часу і засобів в результаті ушкодження або розкрадання важливої інформації і ресурсів.

Зловмисники можуть дістати доступ до мережі, використовуючи уразливості ПЗ, апаратні атаки, або шляхом підбору імені користувача і пароля. Зловмисники, які дістають доступ, змінюючи ПЗ або експлуатуючи уразливості в ПЗ, іменуються хакерами.

Хакер, що дістав доступ в мережу, відразу стає джерелом чотирьох видів погроз:

- розкрадання інформації;
- крадіжка особистої інформації;
- втрата даних або маніпуляція даними;
- припинення обслуговування.

Існує чотири класи фізичних погроз.

- **Погрози для апаратного забезпечення** - фізичне ушкодження серверів, маршрутизаторів, комутаторів, кабелів і робочих станцій.
- **Погрози з боку довкілля** - граничні температури (занадто високі або занадто низькі) або крайні значення вологості (занадто низька або занадто висока).
- **Електричні погрози** - зміни напруги, недостатня напруга в мережі (провали напруги), коливання напруги (шум) і повне відключення живлення.
- **Експлуатаційні погрози** - неналежне поводження з ключовими електричними компонентами (електростатичний розряд), нестача важливих запасних деталей, неправильне прокладення кабелів.

Деякі з цих проблем необхідно вирішувати за допомогою організаційних політик. Інші проблеми вирішуються за рахунок грамотного керівництва і управління в організації.

До атак з використанням шкідливого коду відноситься декілька типів комп'ютерних програм, створених з метою викликати втрату або ушкодження даних. Існує три основні типи атак з використанням шкідливого коду: віруси, троянські програми і черв'яки.

Вірус є шкідливою програмою, приєднаною до іншої програми з метою виконання певних небажаних функцій на робочій станції. В якості прикладу можна привести програму, приєднану до файлу command.com (основний командний інтерпретатор систем Windows); вона видаляє певні файли і заражає інші версії файлу command.com, які зможе виявити.

Троянська програма відрізняється тільки тим, що вона написана так, щоб бути схожою на іншу, а насправді є інструментом атаки. В якості прикладу троянської програми можна привести ПЗ, яке запускає просту гру на робочій станції. Поки користувач зайнятий грою, троянська програма відправляє по електронній пошті копію самій себе на кожну з адрес в адресній книзі користувача. Інші користувачі отримують гру і починають грати в неї, таким чином поширюючи троянську програму по адресах в кожній адресній книзі.

Вірусам, як правило, потрібно механізм передачі, свого роду вектор, наприклад ZIP -файл або будь-який інший виконуваний файл, приєднаний до повідомлення електронної пошти, який переносить код вірусу з однієї системи в іншу. Ключова відмінність комп'ютерного черв'яка від комп'ютерного вірусу полягає в тому, що для поширення вірусу потрібно взаємодію з користувачем.

Черв'яки – це незалежні програми, які атакують систему і намагаються використовувати визначені уразливості в цільовій системі. Після успішного використання уразливості черв'як копіює свою програму з атакуючого вузла в цільову систему, щоб запустити цикл повторно. Черв'як має наступну структуру:

- **активуюча уразливість -** черв'як встановлює свою програму, використовуючи відомі уразливості в системі, наприклад, розраховує на наївність кінцевих користувачів, які відкривають неперевірені виконувані файли у вкладеннях електронної пошти;
- **механізм поширення -** після діставання доступу до вузла черв'як копіює свою програму на цей вузол і вибирає нову мету;
- **корисне навантаження -** після зараження вузла черв'яком зловмисник дістає доступ до цього вузла (часто – доступ з правами привілейованого користувача). Зловмисники можуть використовувати локальне вторгнення, щоб підвищити права до рівня адміністратора.

Окрім атак з використанням шкідливого коду мережі також можуть стати метою різних мережевих атак. Мережеві атаки можна розділити на три основні категорії:

- **розвідувальні атаки -** несанкціоноване виявлення і зіставлення систем, служб або вразливостей;
- **атаки доступу -** несанкціоновані неправомірні дії з даними, доступ до системи або використання прав користувача;
- **відмова в обслуговуванні -** відключення або ушкодження мереж, систем або служб.

Зловмисники ззовні можуть використовувати інструменти Інтернету, наприклад програмні засоби nslookup і whois, які дозволяють легко визначити простір IP -адрес, призначений певній корпорації або юридичній особі. Після визначення простору IP -адрес зловмисник може виконати перевірку зв'язку із загальнодоступними IP -адресами, щоб виявити активні адреси. Для автоматизації цього етапу зловмисник може використовувати інструмент ехо-тестування адрес (наприклад, fping або gping), які систематично виконують перевірку зв'язку з усіма мережевими адресами в межах заданого діапазону або підмережі. Цей процес можна порівняти з переглядом розділу телефонної книги і дзвінком на кожного з номерів, щоб перевірити, хто відповість.

Атаки доступу використовують відомі уразливості в службах перевірки достовірності, службах FTP і веб-службах в цілях діставання доступу до облікових записів в Інтернеті, конфіденційних баз даних і іншої конфіденційної інформації. Атака доступу дозволяє зловмисникові дістати несанкціонований доступ до даних, для перегляду якого у нього немає прав.

Атаки доступу можна розділити на чотири типи. Один з найпоширеніших типів атак доступу – атака через підбір пароля. Атаки через підбір пароля реалізуються за допомогою використання аналізатора пакетів для збору облікових даних і паролів користувачів, що передаються у вигляді відкритого тексту. Атаками через підбір пароля можуть також називатися багатократні спроби входу на загальний ресурс (наприклад, сервер або маршрутизатор) для виявлення імені користувача, пароля або повних облікових даних. Такі багатократні спроби називаються словарними атаками або атаками методом грубої сили.

Відмова в обслуговуванні або DoS –атаки широко поширені, і їх наслідки усунути найважче. Навіть в межах співтовариства зловмисників DoS -атаки вважаються занадто банальними, і їх використання не вітається, оскільки для їх реалізації потрібно занадто мало зусилля. Проте зважаючи на простоту реалізації DoS -атак і потенційно істотної шкоди від них адміністратори безпеки повинні приділяти таким атакам особливу увагу. DoS -атаки можуть приймати різні форми. Такі атаки, споживаючи системні ресурси, заважають авторизованим користувачам використовувати сервіс.

10.2. Резервне копіювання, оновлення і установка виправлень

Антивірусне ПЗ може виявити велику частину вірусів і троянських програм, а також запобігти їх подальшому поширенню по мережі. Розгортання антивірусного ПЗ може виконуватися на рівні користувача і на рівні мережі.

Актуальні оновлення відповідно до новітніх розробок подібного роду атак також можуть забезпечувати ефективний захист від них. У міру випуску нових вірусів або троянських програм підприємствам рекомендується постійно стежити за оновленням антивірусного ПЗ до останніх версій.

Для зниження вірогідності атак вірусів-черв'яків потрібно увагу і обережність з боку як системних, так і мережевих адміністраторів. Нижче представлені рекомендовані кроки по зниженню вірогідності атак вірусів-черв'яків.

- **Стримування** означає стримування поширення черв'яків в межах мережі.
- **Протидія** - виправлення усіх систем і по можливості виконання сканування на предмет вразливостей в системі.
- **Карантин** - відстежування усіх заражених комп'ютерів в мережі.
- **Лікування** - очищення і виправлення усіх заражених систем. Для видалення деяких вірусів-черв'яків може знадобитися переустановлення усієї основної системи.

Найбільш дієвий метод мінімізації наслідків атаки вірусу-черв'яка – викачати оновлення для системи безпеки з сайту постачальника ОС і встановити відповідні виправлення на усі уразливі копії систем. Застосування цього методу відносно неконтрольованих призначених для користувача систем в локальній мережі представляє певну трудність. Управління декількома системами включає створення образу стандартного ПЗ (ОС і підтверджені застосування, авторизовані для використання в клієнтських системах), розгортання яких виконується в нових або оновлених системах. Проте, вимоги до безпеки міняються, і для розгорнутих систем може знадобитися установка оновлених виправлень безпеки. В якості одного з рішень управління критично важливими виправленнями системи безпеки можна створити центральний сервер виправлень, з яким взаємодіють усі системи після заданого періоду. Усі виправлення, які ще не були встановлені, автоматично завантажуються з сервера виправлень і встановлюються без участі користувача.

10.3. Аутентифікація, авторизація і облік

Такі служби забезпечення мережевої безпеки, як аутентифікація, авторизація і облік є базовою інфраструктурою, яка встановлює засоби контролю доступу на якому-небудь мережевому пристрої. Поєднання служб аутентифікації, авторизації і обліку – це метод, що дозволяє контролювати вхід дозволених користувачів (аутентифікація), які дії вони можуть виконувати, знаходячись в мережі (авторизація), а також стежити за їх діями під час доступу

до мережі (облік). Служби аутентифікації, авторизації і обліку (**AAA**, Authentication, Authorization, Accounting) забезпечують вищий рівень масштабованості на відміну від консолі, AUX, VTY і команди аутентифікації в привілейованому режимі.

Користувачі і адміністратори повинні підтвердити свою особу. Аутентифікація здійснюється за допомогою комбінацій імені користувача і пароля, методу ідентифікації типу «запит-відповідь», карт-маркерів і інших способів. У невеликій мережі часто використовується локальна аутентифікація. При локальній аутентифікації кожен пристрій використовує власну базу цих комбінацій імен користувачів і паролів. Проте за наявності великого числа облікових записів користувачів в локальній БД пристрою управління цими обліковими записами істотно ускладнюється. Крім того, у міру зростання мережі і додавання додаткових пристроїв в мережу підтримка локальної аутентифікації, а також її масштабування сильно ускладнене. Наприклад, за наявності 100 мережевих пристроїв усі облікові записи користувачів необхідно додати на усі 100 пристроїв.

У більших мережах рекомендується використовувати зовнішню аутентифікацію, оскільки вона забезпечує більше можливостей для масштабування. Зовнішня аутентифікація дозволяє усім користувачам проходити аутентифікацію за допомогою зовнішнього мережевого сервера. Два найбільш поширених варіанту зовнішньої аутентифікації користувачів - RADIUS і TACACS+:

- RADIUS є відкритим стандартом з низьким коефіцієнтом використання ресурсів ЦП і пам'яті. Цей стандарт використовується різними мережевими пристроями (наприклад, комутаторами, маршрутизаторами і безпровідними пристроями);
- TACACS+ є механізмом забезпечення безпеки, який дозволяє використовувати модульні служби аутентифікації, авторизації і обліку. Цей стандарт використовує службу TACACS+, запущену на сервері безпеки.

Після аутентифікації користувача служби авторизації визначають ресурси, до яких у користувача є доступ, і операції, які користувачеві дозволено виконувати. Наприклад, «Користувач «student» може здійснювати доступ до вузла serverXYZ, використовуючи тільки SSH».

Записи обліку дій користувача, включаючи об'єкти доступу, тривалість доступу до ресурсу і усі внесені зміни. Облік дозволяє відстежувати використання мережевих ресурсів. Концепція служб аутентифікації, авторизації і обліку (AAA) схожа на використання кредитної карти. Кредитна карта визначає, хто може нею користуватися, яку суму можна витратити, а також веде облік товарів, на які користувач витрачає гроші.

10.4. Міжмережеві екрани

Окрім захисту окремих комп'ютерів і серверів, підключених до мережі, необхідно контролювати проходження трафіку через мережу в різних напрямах.

Міжмережевий екран – один з найбільш ефективних засобів безпеки для захисту користувачів мережі від зовнішніх загроз. Міжмережевий екран розділяє дві або більше за мережу і здійснює контроль трафіку, що проходить між ними, одночасно запобігаючи спробам несанкціонованого доступу. У міжмережевих екранах використовуються різні методи визначення дозволеного і забороненого доступу до мережі. Ці методи перераховані нижче.

- **Фільтрація пакетів -** заборона або дозвіл доступу на основі IP - або MAC -адрес.
- **Фільтрація по застосуваннях -** заборона або дозвіл доступу для конкретних типів застосувань на основі номерів портів.
- **Фільтрація за URL -адресами -** заборона або дозвіл доступу до веб-сайтів на основі конкретних URL -адрес або ключових слів.
- **Аналіз пакетів з урахуванням станів з'єднань (SPI) -** пакети, що входять, мають бути легітимними відгуками на запити внутрішніх вузлів. Не запрошені пакети блокуються,

якщо вони не дозволені в явному виді. SPI також надає можливість розпізнавати і блокувати конкретні типи атак, наприклад атаку «відмова в обслуговуванні» (DoS -атака).

Міжмережеві екрани підтримують один або декілька подібних механізмів фільтрації і блокування. Крім того, міжмережеві екрани часто виконують перетворення мережевих адрес NAT. NAT переводить внутрішні IP -адреси і їх групи в зовнішні публічні IP -адреси, які передаються по мережі. При цьому внутрішні IP -адреси приховані від зовнішніх користувачів.

Розглянемо рішення для міжмережевих екранів надаються в різних типах пакетів.

- **Апаратні міжмережеві екрани -** це виділені пристрої, звані пристроєм захисту.
- **Серверні міжмережеві екрани** - це застосування міжмережевого екрану, що виконуються в мережевій операційній системі (NOS), наприклад UNIX, Windows або Novell.
- **Інтегровані міжмережеві екрани -** доповнює можливості існуючого пристрою (наприклад маршрутизатора) функціями міжмережевого екрану.
- **Персональні міжмережеві екрани -** розміщуються на вузлах і не розраховані на захист локальної мережі в цілому. Вони можуть бути реалізовані в ОС за замовчуваннямабо встановлені стороннім постачальником.

10.5 Захист крайових і мережевих пристроїв

Безпечна мережа захищена настільки, наскільки захищена її найуразливіша ланка. Найбільш значущими погрозами, які найчастіше обговорюються в ЗМІ, є зовнішні загрози (наприклад інтернет-черв'яки і DoS -атаки). Проте забезпечення безпеки внутрішньої мережі не менш важливе, чим захист периметра мережі. Внутрішня мережа складається з крайових мережевих. Крайовий пристрій, або вузол, є окремою комп'ютерною системою або пристроєм, який виступає в ролі мережевого клієнта. До найбільш поширених крайових пристроїв відносяться ноутбуки, настільні і планшетні ПК, сервери і смартфони. Якщо користувачі не забезпечують безпеку своїх крайових пристроїв, ніякі заходи безпеки не гарантують повного захисту мережі.

Захист крайових пристроїв – одне з найбільш складних завдань мережевого адміністратора, оскільки в даному випадку має значення людський чинник. Компанії необхідно розробити і ретельно задокументувати відповідні політики і ознайомити з ними співробітників. Співробітників необхідно навчити правильно використовувати мережу. Політики часто мають на увазі використання антивірусного ПЗ і міри запобігання несанкціонованому вторгненню на вузол. Комплексні рішення для захисту крайових пристроїв використовують функції контролю доступу до мережі.

У рамках захисту крайових пристроїв також потрібен захист пристроїв 2-го рівня у рамках мережевої інфраструктури, що дозволяє запобігти атакам 2-го рівня (наприклад, спуфінг-атаки з використанням MAC -адрес, атаки з використанням переповнювання таблиць MAC – адрес, атак за типом «мережевий шторм»). Така процедура називається мінімізацією ризику атаки.

При установці на пристрій нової ОС налаштуванням безпеки привласнюються значення за замовчуванням. В більшості випадків цей рівень безпеки є недостатнім.

Існує ряд простих кроків, які можна застосувати для більшості ОС:

- імена користувачів і паролі за замовчуванням необхідно негайно змінити;
- доступом до системних ресурсів повинні володіти тільки особи, наділені відповідними правами;
- будь-які незатребувані служби і застосування необхідно відключити або видалити.

Усі пристрої необхідно оновлювати, встановлюючи нові заходи безпеки у міру їх появи. Часто пристрої, отримані від виробника, до відвантаження зберігалися на складі впродовж певного періоду, і тому на них не встановлені актуальні виправлення. Також важливо перед впровадженням пристрою відновити усе ПЗ і встановити усі виправлення безпеки.

Для захисту мережевих пристроїв необхідно використовувати надійні паролі. Далі представлений ряд стандартних інструкцій.

- Використовуйте пароль завдовжки не менше 8 символів (переважно 10 і більше символів). Використовуйте довгі паролі (це впливає на їх надійність).
- Вибирайте складні паролі. Включайте в пароль комбінацію букв у верхньому і нижньому регістрі, цифр, спеціальних символів і пропусків (якщо допускається їх використання).
- Уникайте використання паролів, створених на основі повторень, звичайних слів із словника, послідовностей букв або цифр, імені користувача, імен родичів і домашніх тварин, біографічних даних (дата народження, ідентифікаційні номери, імена предків і інші дані, які легко з'ясувати).
- Допустіть в паролі навмисну помилку. Наприклад, Ivanov = Ivonov = 1vOnov або Security = 5ecur1ty.
- Періодично міняйте паролі. Якщо пароль був скомпрометований випадково, у будь-якому випадку це залишає зловмисникам мало можливостей для його використання.

Адміністратори повинні забезпечити використання в мережі надійних паролів. Для цього в цілях перевірки надійності пароля можна використовувати ті ж інструменти атаки методом грубої сили, які використовуються хакерами.

При впровадженні пристроїв важливо наслідувати усі інструкції з безпеки, діючі в організації. До таких інструкцій відноситься привласнення імен пристроям таким чином, яке забезпечує їх просте і зручне документування і відстежування, проте забезпечує при цьому певну міру безпеки. Не варто повідомляти в імені вузла зайву інформацію про використання пристрою.

Існує ряд дій, які можна виконати, щоб забезпечити збереження пароля в таємниці. Використання на мережевому пристрої команди глобальної конфігурації service password - encryption запобігає несанкціонованому доступу для перегляду паролів у вигляді звичайного тексту у файлі конфігурації. Ця команда виконує шифрування усіх незашифрованих паролів. Щоб усі налагоджені паролі мали довжину не менш заданого значення, слід використовувати команду security passwords min - length в режимі глобальної конфігурації.

Інший спосіб отримання зловмисниками паролів – проста атака методом грубої сили, тобто підбір паролів до тих пір, поки один з них не підійде. Для запобігання атак такого типу можна заблокувати спроби входу пристрій після певної кількості невдалих спроб в заданий період часу:

Router(config)# login block - for 120 attempts 3 within 60

Ця команда блокує спроби входу на 120 секунд, якщо впродовж 60 секунд виконано три невдалі спроби входу.

Банерні повідомлення важливі у рамках подання позову до суду відносно будь-кого, хто здійснив неправомірний доступ в систему:

Router(config)# banner motd #message#

Також рекомендується задати значення тайм-ауту по виконанню. Настроївши тайм-аут по виконанню, ви повідомляєте мережевому пристрою про необхідність відключення користувачів з лінії, якщо вони неактивні впродовж періоду, заданого значенням тайм-ауту по виконанню. Значення тайм-ауту по виконанню можна налаштуватина портах консолі, VTY і AUX. Наступна команда відключає користувачів після закінчення 10 хвилин:

```
Router(config)# line vty 0 4
Router(config - vty)# exec - timeout 10
```

10.6. Включення протоколу SSH

Застарілим протоколом для віддаленого управління пристроями є Telnet. Цей протокол не є безпечним. Дані в пакеті Telnet передаються в незашифрованому виді. Використовуючи

такі інструменти, як Wireshark, зловмисник може «проаналізувати» сеанс Telnet і отримати інформацію про пароль. З цієї причини в цілях забезпечення безпечного віддаленого доступу рекомендується використовувати на пристроях протокол SSH (Secure Shell). Налаштування підтримки протоколу SSH для мережевого пристрою виконується в чотири етапи:

Крок 1. Переконайтеся в тому, що маршрутизатору присвоєно унікальне ім'я вузла, після чого налаштуйте IP -доменне ім'я мережі, використовуючи команду ip domain - name domain - name в режимі глобальної конфігурації.

Крок 2. Необхідно створити односторонні секретні ключі для маршрутизатора для шифрування трафіку по SSH. Ключ є об'єктом, який фактично використовується для шифрування і розшифруваня даних. Для створення ключа шифрування використовується команда crypto key generate rsa general - keys modulus modulus - size в режимі глобальної конфігурації. Конкретне значення окремих фрагментів цієї команди відрізняється достатньою складністю, цей модуль визначає розмір ключа, і його можна налаштувати в діапазоні від 360 до 2048 біт. Чим більше модуль, тим вище рівень безпеки ключа, але тим більше часу займає шифрування і розшифрування даних. Мінімальна рекомендована довжина модуля – 1024 біт.

Router(config)# crypto key generate rsa general - keys modulus 1024

Крок 3. Створіть локальний запис імені користувача бази даних, використовуючи команду username name secret secret в режимі глобальної конфігурації.

Крок 4. Дозвольте використання сеансів SSH, що входять, для VTY за допомогою команд рядка VTY login local і transport input ssh.

Доступ до служби протоколу SSH на маршрутизаторі тепер можна здійснювати за допомогою ПЗ клієнта SSH.

10.7. Використання спеціальних команд

Після впровадження мережі мережевий адміністратор повинен мати можливість протестувати підключення до мережі, щоб підтвердити її працездатність. Крім того, мережевим адміністраторам рекомендується задокументувати мережу.

Команда ping надає ефективний спосіб перевірки підключення. Цю перевірку часто називають перевіркою стеку протоколів, оскільки команда ping переміщається від 3-го рівня моделі OSI до 2-го рівня, а потім - до 1-го рівня. Команда «ping» використовує для перевірки підключення протокол ICMP.

Команда ping не завжди дозволяє виявити характер проблеми, проте може допомогти визначити її джерело, що є першим важливим кроком на шляху до усунення неполадок у разі збою мережі.

Команда ping надає метод перевірки стеуа протоколів і конфігурації IPv4 -адреси на вузлі, а також перевірки підключення до локальних і віддалених вузлів призначення. Доступні також додаткові інструменти, які дозволяють отримати більше інформації, ніж команда ping, наприклад Telnet або Trace.

При запуску команди ping в IOS створюється ряд індикаторів для кожного відправленого ехо-запиту ICMP. Нижче представлені найпоширеніші індикатори.

! ! - вказує на отримання повідомлення ехо-відповіді від протоколу ICMP.

. . - показує час, що пройшов в очікуванні повідомлення ехо-відповіді від протоколу ICMP.

U - отримано повідомлення «Вузол призначення недосяжний».

««! (знак оклику) означає, що перевірка зв'язку успішно завершена, а також підтверджує підключення на 3-му рівні.

««. (точка) може вказувати на проблеми, що виникли в ході обміну даними. Цей індикатор вказує на проблеми підключення в якій-небудь точці шляху. Він також може вказувати на те, що маршрутизатор на шляху не містив маршруту до точки призначення і не відправив

повідомлення «Призначення ICMP недоступне». Крім того, він може вказувати на те, що команда «ping» заблокована системою безпеки пристрою.

Індикатор «U» означає, що маршрутизатор на шляху не утримував маршрут до адреси призначення або цей запит команди «ping» був заблокований, і у відповідь на нього відправлено повідомлення «Вузол призначення недосяжний».

Команда ping використовується для перевірки внутрішньої IP -конфигурації на локальному вузлі. Слід пам'ятати, що цей тест виконується за допомогою команди ping на зарезервованій адресі (loopback -адресі (127.0.0.1)). Ця команда перевіряє працездатність стеку протоколів від мережевого до фізичного рівня і назад без фактичної відправки сигналу в середовище.

Для перевірки loopback за допомогою команди ping використовується наступний синтаксис:

C:\> ping 127.0.0.1

Відповідь цієї команди виглядатиме приблизно таким чином:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli - seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

Результат свідчить про те, що чотири тестові пакети по 32 байти були відправлені і повернені вузлом 127.0.0.1 менш ніж за 1 мс. Абревіатура TTL означає «Time - to - Live» (час існування) і визначає кількість переходів, що залишилися у эхо-запроса до його скидання.

Команда «trace» повертає список переходів у міру маршрутизації пакету по мережі. Форма команди залежить від точки виконання команди. Для виконання трасування на комп'ютері з ОС Windows використовується команда tracert. При виконанні трасування з інтерфейсу командного рядка (CLI) маршрутизатора необхідно використовувати команду traceroute.

Як і команди ping, команди trace вводяться в командний рядок і приймають IP -адресу в якості аргументу.

Припускаючи, що команда буде запущена на комп'ютері Windows, можна використовувати форму tracert :

C:\> tracert 10.1.0.2

Tracing route to 10.1.0.2 over a maximum of 30 hops
1 2 ms 2 ms 2 ms 10.0.0.254
2 * * * Request timed out.
3 * * * Request timed out.
4 ^C

Час очікування для запитів трасування на адресу наступного переходу витік, а це означає, що маршрутизатор наступного переходу не відповідає. Результати трасування вказують на те, що збій стався у внутрішній мережі.

Щоб проглянути IP -адресу шлюзу за замовчуванням для вузла, можна запустити команду ipconfig в командному рядку комп'ютера під управлінням Windows.

Для перегляду MAC -адреси комп'ютера з детальними відомостями про адресацію пристрою 3-го рівня використовується інструмент ipconfig /all (рис. 10.1).

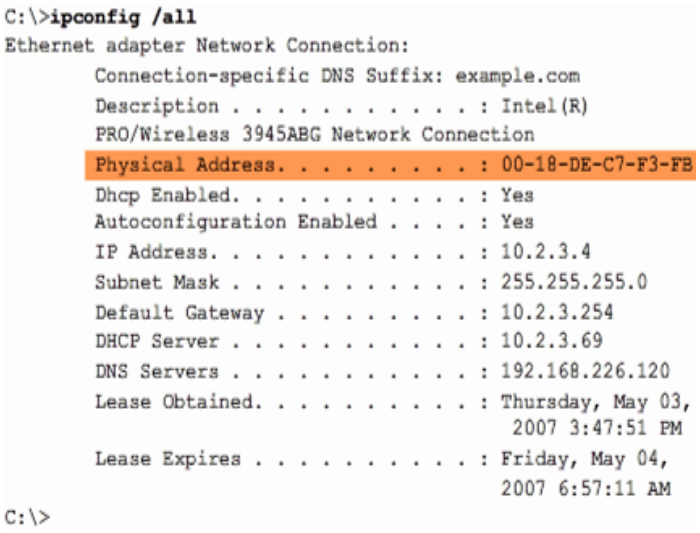


Рис. 10.1. Перегляд MAC -адреси комп'ютера за допомогою команди ipconfig /all [1]

Крім того, виробника мережевого інтерфейсу для комп'ютера можна визначити по частині OUI MAC -адреси. Ці відомості можна знайти в Інтернеті.

Клієнтська служба DNS на ПК з ОС Windows оптимізує продуктивність дозволу імен DNS за рахунок зберігання раніше дозволених імен в пам'яті. На ПК з ОС Windows команда ipconfig /displaydns виводить на екран усі кешовані записи DNS.

Команда arp робить можливим створення, редагування і відображення зіставлень фізичних адрес відомим IPv4 -адресам. Команда arp виконується в командному рядку Windows.

Щоб виконати команду arp, в командному рядку вузла введіть:

C:\host1> arp - a

Команда arp - a перераховує усі пристрої, які в даний момент представлені в ARP -кеші вузла, а також IPv4 -адресу, фізичну адресу і тип адресації (статична/динамічна) для кожного з пристроїв.

Кеш можна очистити за допомогою команди arp - d, якщо мережевому адміністраторові необхідно повторно заповнити кеш оновленими даними.

До найчастіше використовуваних команд відноситься команда show ip interface brief. Ця команда виводить вихідні дані в компактнішому форматі, ніж команда show ip interface. Вона надає відомості за ключовими даними для усіх мережевих інтерфейсів на маршрутизаторі.

Як і у випадку з будь-яким крайовим пристроєм, для перевірки працездатності 3-го рівня можна використовувати команди ping і traceroute. У цьому прикладі обидві команди ping і trace показують успішне підключення.

Комутатор також може перевірити підключення на 3-му рівні за допомогою команд show ip interface brief і traceroute. Важливо враховувати, що комутатору необов'язково потрібна IP -адреса для пересилки кадрів на 2-му рівні. IP -адреса потрібна тільки у тому випадку, якщо управління комутатором здійснюється по мережі за допомогою Telnet або SSH.

Якщо мережевий адміністратор планує віддалено підключатися до комутатора з розташування за межами локальної мережі LAN, необхідно також налаштуватишлюз за замовчуванням.

10.8. Основи безпеки безпровідних підключень

Заходи по забезпеченню безпеки мають бути сплановані і впроваджені до того, як точка доступу буде підключена до мережі або мережі інтернет-провайдера.

До стандартних заходів безпеки відносяться:

- зміна значень SSID (Service Set Identifier), заданих за замовчуванням, імен користувачів і паролів;
- відключення широкомовної розсилки SSID;

- налаштування шифрування з використанням WEP або WPA.

Шифрування – це процес перетворення даних таким чином, що навіть перехоплення інформації виявляється даремним.

Протокол WEP (Wired Equivalent Privacy) – це вдосконалений механізм безпеки, що дозволяє шифрувати мережевий трафік в процесі передачі. Протокол WEP використовує заздалегідь налагоджені ключі для шифрування і розшифрування даних.

WEP -ключ вводиться як рядок чисел і букв завдовжки 64 або 128 біт. В деяких випадках протокол WEP підтримує 256-бітові ключі. Для спрощення створення і введення цих ключів в багатьох пристроях використовуються фрази-паролі. Фраза-пароль – це простий засіб запам'ятовування слова або фрази при автоматичній генерації ключа.

Для ефективної роботи протоколу WEP точка доступу та кожен безпровідний пристрій, що має дозвіл на доступ до мережі, повинні використовувати загальний WEP -ключ. Без цього ключа пристрої не зможуть розпізнати дані, що передаються по безпровідній мережі.

Проте, протокол WEP також має свої слабкі сторони, одна з яких полягає у використанні статичного ключа для усіх пристроїв з підтримкою WEP. Існують програми, що дозволяють зловмисникові визначити WEP -ключ. Ці програми можна знайти в мережі Інтернет. Після того, як зловмисник отримав ключ, він дістає повний доступ до усієї передаваної інформації.

Одним із засобів захисту від такої уразливості є часта зміна ключів. Існує вдосконалений і безпечний засіб шифрування – протокол захищеного доступу до Wi - Fi (Wi - Fi Protected Access, **WPA**). У протоколі WPA використовуються ключі шифрування завдовжки від 64 до 256 біт. При цьому WPA, на відміну від WEP, генерує нові динамічні ключі при кожній спробі клієнта встановити з'єднання з точкою доступу. З цієї причини WPA вважається безпечнішим, ніж WEP, оскільки його значно важче зламати.

Існує ряд інших функцій забезпечення безпеки, які можна налаштувати для точки безпровідного доступу, включаючи фільтрацію за MAC -адресами, аутентифікацію і фільтрацію трафіку.

Висновок до лекції 10

В цілях відповідності вимогам користувачів необхідно ретельно планувати і проектувати навіть невеликі мережі. Планування дозволяє приділити належну увагу усім вимогам, витратам і способам впровадження. Важливими властивостями мережі є її надійність, масштабованість і доступність.

При плануванні впровадження мережі необхідно враховувати мережеві погрози і уразливості. Необхідно забезпечити безпеку усіх мережевих пристроїв. До таких пристроїв відносяться маршрутизатори, комутатори, крайові пристрої користувачів і пристрої забезпечення безпеки. Необхідно забезпечити захист мереж від шкідливого ПЗ (вірусів, троянських програм і черв'яків). Антивірусне ПЗ може виявити велику частину вірусів і троянських програм, а також запобігти їх подальшому поширенню по мережі. Найбільш дієвий метод мінімізації наслідків атаки вірусу-черв'яка - викачати оновлення для системи безпеки з сайту постачальника ОС і встановити відповідні виправлення на усі уразливі копії систем.

Необхідно також забезпечити захист мереж від мережевих атак. Мережеві атаки можна розділити на три основні категорії: розвідувальна атака, атака доступу і атака типу «відмова в обслуговуванні» (DoS -атака). Існує декілька способів захисту мережі від мережевих атак.

- Такі служби по забезпеченню мережевої безпеки, як аутентифікація, авторизація і облік є базовою інфраструктурою, яка встановлює засоби контролю доступу на якому-небудь мережевому пристрої. Поєднання служб аутентифікації, авторизації і обліку – це метод, що дозволяє контролювати вхід дозволених користувачів (аутентифікація), які дії вони можуть виконувати, знаходячись в мережі (авторизація), а також стежити за їх діями під час доступу до мережі (облік).

- Міжмережевий екран – один з найбільш ефективних засобів безпеки для захисту користувачів мережі від зовнішніх загроз. Міжмережевий екран розділяє дві або більше за мережу і здійснює контроль трафіку, що проходить між ними, одночасно запобігаючи спробам несанкціонованого доступу.
- Для захисту мережевих пристроїв необхідно використовувати надійні паролі. Крім того, при віддаленому доступі до мережевих пристроїв настійно рекомендується використовувати протокол SSH замість незахищеного протоколу Telnet.

Після впровадження мережі мережевий адміністратор повинен мати можливість здійснювати моніторинг і обслуговування мережевого підключення.

Питання для закріплення

1. Які категорії погроз безпеки мереж ви знаєте?
2. Для чого використовується резервне копіювання, оновлення і установка виправлень?
3. Для чого використовується аутентифікація, авторизація і облік?
4. Яке призначення міжмережевих екранів?
5. Які способи захисту крайових і мережевих пристроїв ви знаєте?
6. Який принцип роботи і основні функції SSH?
7. Які спеціальні команди діагностування стану мережі ви знаєте?
8. Які заходи безпеки безпровідних підключень ви знаєте?
9. Які відмінності між протоколами WPA та WEP?

Список рекомендованої літератури

1. CCNA R&S ITN Chapter 11: It's a Network // Електронний ресурс. Режим доступу: http://static-course-assets.s3.amazonaws.com/IntroNet50ENU/module11/index.html
2. The Secure Shell (SSH) Protocol Architecture // Електронний ресурс. Режим доступу: https://tools.ietf.org/html/rfc4251
3. Теорія і практика використання SSH (ssh crypt security) // Електронний ресурс. Режим доступу: http://www.opennet.ru/base/sec/ssh_intro.txt.html
4. The Difference Between WEP, WPA, and WPA2 Wi-Fi Passwords // Електронний ресурс. Режим доступу: https://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/

Лекція 11. Тема: «Локальні мережі. Технології комутації»

План лекції

11.1. Принципи роботи комутатора.
11.2. Методи пересилки на комутаторі.
11.3. Колізійні та широкомовні домени.
11.4. Зниження перевантажень мережі.
11.5. Базові налашування комутатора.
11.6. Неполадки на рівні мережевого доступу.
11.7. Поширені погрози безпеки.
11.8. Інструменти і тестування мережевої безпеки.

11.1. Принципи роботи комутатора

Різні пристрої повинні взаємодіяти один з одним для забезпечення швидкого, безпечного і надійного з'єднання між вузлами. Комутатори локальних мереж забезпечують підключення

кінцевих користувачів до корпоративної мережі та відповідають за управління інформацією усередині середовища LAN. Маршрутизатори забезпечують передачу інформації між мережами LAN і, як правило, не взаємодіють з окремими вузлами.

Концепція комутації і пересилки кадрів універсальна для мережевих і телекомунікаційних технологій. У локальній, глобальній і телефонній мережах використовуються різні типи комутаторів. Основна концепція комутації полягає в прийнятті пристроєм рішення на основі двох критеріїв:

- вхідний порт;
- адреса призначення.

Рішення про те, як комутатор пересилає трафік, приймається залежно від потоку трафіку. Термін «вхідною» використовується для опису порту, через який кадр входить в пристрій. Термін «вихідний» використовується для опису кадрів, які покидають пристрій з певного порту.

Рішення, що приймається комутатором, грунтується на даних про вхідний порт і адресу призначення цього повідомлення.

Інтелектуальні здібності комутатора LAN полягають в його здатності використовувати свою таблицю для пересилки трафіку на основі вхідного порту і адреси призначення повідомлення. У випадку з комутатором LAN є тільки одна таблиця комутації, яка описує строгий зв'язок між адресами і портами; тому сполучення з цією адресою призначення завжди покидає комутатор з одного і того ж вихідного порту, незалежно від порту, через який воно входить.

Комутатори використовують MAC-адреси для направлення мережевої передачі даних через комутатор до відповідного порту до місця призначення. Комутатор складається з об'єднаних мікросхем і відповідного ПЗ, за допомогою якого дані проходять через комутатор. Щоб комутатор знав, який порт використовувати для передачі кадру, він повинен спочатку дізнатися, які пристрої існують на кожному порту. У міру того, як комутатор дізнається відношення портів до пристроїв, він створює таблицю MAC-адрес або таблицю асоціативної пам'яті (CAM).

CAM (асоціативна пам'ять, англ. Content Addressable Memory) – це особливий тип пам'яті, що використовується в застосуваннях швидкого пошуку. Комутатори LAN визначають спосіб обробки вхідних кадрів шляхом ведення таблиці MAC-адрес. Комутатор створює свою таблицю MAC-адрес, записуючи MAC-адресу кожного пристрою, підключеного до кожного зі своїх портів. Комутатор використовує дані з таблиці MAC-адрес для відправлення кадрів, призначених для конкретного пристрою з порту, який був призначений цьому пристрою. Комутатор заповнює таблицю MAC-адрес на основі MAC-адрес джерела. Коли комутатор приймає вхідний кадр з MAC-адресою призначення, яка не міститься в таблиці MAC-адрес, комутатор пересилає кадр з усіх портів (лавинна розсилка), за винятком вхідного порту цього кадру. Коли пристрій призначення відповідає, комутатор додає MAC -адресу джерела кадру і порту, на якому був отриманий кадр, в таблицю MAC-адрес. У мережах з декількома сполученими комутаторами таблиця MAC-адрес містить декілька MAC-адрес для одного порту, підключеного до інших комутаторів.

11.2. Методи пересилки на комутаторі

Тоді як мережі підприємства розширюються, їх продуктивність помітно знижується. У зв'язку з цим в мережі були додані мости Ethernet (попередня версія комутатора) для обмеження розмірів колізійних доменів. У 90-х рр. розвиток технологій інтегральних мікросхем дозволив замінити мости Ethernet комутаторів для локальних мереж. Ці комутатори LAN могли передати ухвалення рішення про пересилку рівня 2 від ПЗ в спеціалізовані інтегральні мікросхеми (ASIC). ASIC скорочують час обробки пакетів в пристрої і дозволяють пристроям обробляти більше портів без зниження продуктивності.

Цей метод пересилки кадрів даних на рівні 2 назвали **комутацією з проміжним зберіганням** (режим «store - and - forward»). Цей термін протиставлений терміну «наскрізна комутація».

Комутація з проміжним зберіганням характеризується двома основними ознаками, які відрізняють її від наскрізної комутації,: виявленням помилок і автоматичною буферизацією.

Комутатор з проміжним зберіганням виявляє помилки у вхідному кадрі. Після отримання усього кадру на вхідному порту комутатор порівнює значення **FCS** (frame - check - sequence) в останньому полі датаграми з власними обчисленнями FCS.

FCS – це процес виявлення помилок, який дозволяє переконатися в тому, що кадр вільний від фізичних і канальних помилок. Комутатор пересилає кадр, якщо не виявив в нім помилок. Інакше кадр відкидається.

Процес буферизації на вхідному порту у комутаторах із проміжним зберіганням забезпечує гнучкість для підтримки будь-яких швидкостей Ethernet. Наприклад, обробка вхідного кадру передається в порт Ethernet 100 Мбіт/с і призначеного для відправки в інтерфейс 1 Гбіт/с, зажадає використання комутації з проміжним зберіганням. З будь-якою невідповідністю в швидкості між вхідним і вихідним портами комутатор зберігає увесь кадр в буфері, перевіряє FCS, пересилає його в буфер вихідного порту і потім відправляє його.

Комутація з проміжним зберіганням або комутація в режимі «store - and - forward», є основним методом комутації локальної мережі Cisco.

Комутатор з проміжним зберіганням відкидає кадри, які не пройшли перевірку FCS і таким чином не пересилає неприпустимі кадри. І навпаки, в режимі наскрізної комутації можлива пересилка неприпустимих кадрів, оскільки перевірка FCS не виконується.

Перевага **наскрізної комутації** полягає в здатності комутатора почати пересилку кадру раніше, ніж при комутації з проміжним зберіганням. Наскрізна комутація характеризується двома основними ознаками: швидкою пересилкою кадру і обробкою неприпустимих кадрів.

Комутатор з наскрізною комутацією може приймати рішення про пересилку відразу після знаходження MAC-адреси призначення кадру у своїй таблиці MAC-адрес. Комутатору не треба чекати іншої частини кадру, що поступає через вхідний порт, перш ніж прийняти рішення про пересилку.

З урахуванням сучасних контролерів і ASIC MAC, комутатор з наскрізною комутацією здатний швидко приймати рішення про те, чи треба йому перевіряти велику частину заголовків кадру в цілях додаткової фільтрації. Наприклад, комутатор може проаналізувати перші 14 байт (поля MAC -адреси джерела, MAC-адреси призначення і EtherType) і вивчити додаткові 40 байт, щоб виконати ускладнені функції по відношенню до рівнів 3 і 4 протоколи IPv4.

Наскрізна комутація не відкидає більшість неприпустимих кадрів. Кадри з помилками пересилаються іншим сегментам мережі. У разі високого коефіцієнта помилок (неприпустимих кадрів) в мережі наскрізна комутація може негативно позначитися на смузі пропускання, наповнюючи її пошкодженими і неприпустимими кадрами.

Безфрагментний режим комутації – це модифікована форма наскрізної комутації, при якій комутатор затримує пересилку пакету на час колізійного інтервалу (64 байт). Це означає, що кожен кадр буде обмежений полем даних для запобігання фрагментації. У безфрагментному режимі комутації помилки виявляються краще, ніж в режимі наскрізної комутації, при цьому затримка при передачі мінімальна. Завдяки найменшій величині затримки наскрізна комутація більше підходить для складних застосувань, що виконують високопродуктивні обчислення, для яких затримка між процесами повинна складати 10 мікросекунд або менше.

11.3. Колізійні та широкомовні домени

У сегментах Ethernet на основі концентраторів мережеві пристрої «борються» за контроль над середовищем передачі, оскільки пристрої повинні передавати дані по черзі. Сегменти мережі, які користуються загальною смугою пропускання, називаються **колізійними**

доменами, у випадках, коли два або більше за пристрої в межах одного сегменту пробують передавати дані одночасно, можуть виникнути колізії.

Проте можна використовувати інші мережеві пристрої (включаючи комутатори і маршрутизатори), що працюють на рівні доступу до мережі моделі TCP/IP і вище, для розподілу мережі на сегменти і зменшення кількості пристроїв, що конкурують за пропускну спроможність. У цьому випадку кожен новий сегмент стає новим колізійним доменом. Таким чином, пристрої у сегменті дістають більший доступ до смуги пропускання, тоді як колізії в одному домені не заважають роботі інших сегментів. Описаний процес також називають **мікросегментацією.**

Кожен порт комутатора підключений до одного ПК або сервера, є окремим колізійним доменом.

Не дивлячись на те, що комутатори фільтрують більшість кадрів на основі MAC-адрес, під фільтрацію не потрапляють кадри широкомовної розсилки. Для того, щоб кадри широкомовної розсилки отримували інші комутатори в локальній мережі, комутатори повинні розсилати ці кадри на усі порти. Сукупність сполучених комутаторів формує єдиний широкомовний домен. Тільки пристрій мережевого рівня, наприклад маршрутизатор, може розділити широкомовний домен 2 рівня. Маршрутизатори використовуються для сегментації як колізійних доменів, так і широкомовних доменів. Коли пристрій відправляє широкомовну розсилку рівня 2, MAC -адреса призначення в кадрі представлена одиницями у двійковому форматі. Кадр з MAC-адресою призначення з одиниць в двійковому форматі отримують усі пристрої в широкомовному домені.

Широкомовний домен 2 рівня називають широкомовним доменом MAC-адрес. У широкомовний домен MAC-адрес входять усі пристрої локальної мережі, які отримують кадри широкомовної розсилки від вузла. Коли комутатор отримує широкомовний кадр, він пересилає кадр з усіх своїх портів, за винятком вхідного порту, на якому широкомовний кадр був отриманий. Кожен пристрій, підключений до комутатора, отримує копію широкомовного кадру і обробляє її. В деяких випадках широкомовні розсилки потрібні для первинного місцезнаходження інших пристроїв і мережевих сервісів, але, крім цього, вони знижують ефективність мережі. Смуга пропускання мережі використовується для поширення широкомовного трафіку. Надмірна кількість широкомовних розсилок і навантаження трафіку в мережі можуть привести до перевантаження – зниження в продуктивності мережі. Коли два комутатори сполучено, широкомовний домен збільшується.

11.4.Зниження перевантажень мережі

Комутатори LAN мають певні характеристики, що дозволяють їм знижувати перевантаження мережі. По-перше, вони допускають сегментацію LAN в окремі колізійні домени. Кожен порт комутатора представляє окремий колізійний домен і забезпечує повну смугу пропускання для пристрою або пристроїв, підключених до цього порту. По-друге, вони забезпечують повнодуплексний зв’язок між пристроями. Повнодуплексне з’єднання дозволяє одночасно передавати і отримувати сигнал. Повнодуплексні з’єднання значно покращують продуктивність локальної мережі, крім того, вони потрібні для передачі даних із швидкістю 1 Гбіт/с Ethernet і вище. Комутатори сполучають сегменти LAN (колізійні домени), використовують таблицю MAC-адрес для визначення сегменту, якому треба відправити цей кадр, і можуть скоротити або повністю усунути колізії. Розглянемо характеристики комутаторів, які сприяють зниженню перевантаження мережі.

Висока щільність портів. Комутатори мають вищу щільність портів: часто висота комутаторів з 24 і 48 портами дорівнює мінімальній стандартній висоті нарощуваного пристрою (1,75’’), а швидкість їх може досягати 100 Мбіт/с, 1 Гбіт/с і 10 Гбіт/с. Комутатори великих підприємств можуть підтримувати декілька сотень портів.

Великі буфери кадрів. Можливість зберігати більше отриманих кадрів перед їх відкиданням дуже корисна, особливо за наявності переобтяжених портів, до яких підключені сервери або інші частини мережі.

Швидкість порту. Залежно від вартості комутатора можлива підтримка сукупності швидкостей. Найбільш поширені порти зі швидкостями 100 Мбіт/с, 1 або 10 Гбіт/с (швидкість 100 Гбіт/с також представляється можливою).

Швидка внутрішня комутація. Можливість швидкої внутрішньої пересилки забезпечує високу продуктивність. В якості методу можна використовувати швидку внутрішню шину або загальну пам'ять, яка впливає на загальну продуктивність комутатора.

Низька вартість кожного порту. Комутатори забезпечують високу щільність портів при мінімумі витрат. Саме тому комутатори LAN можуть забезпечувати проекти мереж з меншою кількістю користувачів для кожного сегменту, таким чином підвищуючи середню пропускну спроможність для кожного користувача.

Комутатори – це пристрої для з'єднання декількох пристроїв в одній мережі. У правильно спроектованій мережі комутатори локальної мережі відповідають за напрям потоку даних і управління ним на рівні доступу до мережевих ресурсів. Комутаторами можна управляти як локально, так і віддалено. Для віддаленого управління на комутаторі треба налаштувати IP -адресу і шлюз за замовчуванням.

11.5. Базові налаштування коммутатора

Щоб налаштувати на комутаторі можливість для віддаленого управління, на комутаторі потрібно налаштувати IP -адресу і маску підмережі. Для управління комутатором з віддаленої мережі для нього необхідно налаштувати шлюз за замовчуванням. Подібне налаштування мало чим відрізняється від налаштування інформації про IP -адреси на фізичних вузлах. Поняття SVI відноситься до мереж VLAN. Мережі VLAN – це пронумеровані логічні групи, яким можна присвоїти фізичні порти. Конфігурації і налаштування до VLAN також застосовуються до усіх портів, призначених для цієї VLAN. За замовчуванням комутатор налагоджений для управління через VLAN 1. За замовчуванням усі порти асоціюються з VLAN 1. В цілях безпеки не рекомендується використовувати мережу VLAN 1 як мережу управління VLAN. Розглянемо основні кроки з налаштування комутатора.

Крок 1. Налаштування інтерфейсу управління.

IP -адреса і маска підмережі налагоджені на SVI управління комутатора з режиму конфігурації інтерфейсу VLAN. Для входу в режим конфігурації інтерфейсу використовується команда interface vlan 99. Для налаштування IP -адреси використовується командаip address. Команда no shutdown активує інтерфейс. Інтерфейс SVI для мережі VLAN 99 не відображуватиметься як up/up, поки не буде створена VLAN 99 і не з'явиться пристрій, підключений до порту комутатора, пов'язаного з VLAN 99. Для того, щоб створити мережу VLAN з ідентифікатором 99 і прив'язати її до інтерфейсу, використовуються команди:

```
S1(config)# vlan vlan_id
S1(config - vlan)# name vlan_name
S1(config - vlan)# exit
S1(config)# interface interface_id
S1(config - if)# switchport access vlan vlan_id
```

Крок 2. Налаштування шлюзу за замовчуванням.

У випадку, якщо вимагається управляти комутатором віддалено з мереж без прямого підключення, на комутаторі слід налаштувати шлюз за замовчуванням –маршрутизатор, до якого підключений комутатор. Комутатор пересилає IP -пакети з IP -адресами призначення за межі локальної мережі на шлюз за замовчуванням.

Для того, щоб налаштувати шлюз за замовчуваннямдля комутатора, використовується команда ip default - gateway. Введіть IP -адрес шлюзу за замовчуванням. Шлюз за замовчуванням – це IP -адреса інтерфейсу маршрутизатора, до якого підключений комутатор. Використовуйте команду copy running - config startup - config для створення резервної копії цієї конфігурації.

Крок 3. Перевірка конфігурації.

Команду show ip interface brief слід використовувати при визначенні стану як фізичних, так і віртуальних інтерфейсів. Показаний результат підтверджує, що для інтерфейсу VLAN 99 були задані IP -адрес і маска підмережі і що він знаходиться в робочому стані.

Команда show interfaces є ще однією поширеною командою, яка виводить дані про стан і статистику мережевих інтерфейсів комутатора. Командаshow interfaces часто використовується при налаштуванні і моніторингу мережевих пристроїв.

11.6. Неполадки на рівні мережевого доступу

Результат команди show interfacesможно використовувати для виявлення типових проблем середовища передачі даних. Найважливіші складові цих вихідних даних відображують стан протоколу канального рівня і протоколу каналу передачі даних.

Перший параметр (FastEthernet0/1 is up) відноситься до апаратного рівня і, по суті, вказує, чи отриманий інтерфейсом сигнал виявлення що несе від іншого крайового пристрою. Другий параметр (line protocol is up) відноситься до канального рівня. Він вказує, чи приймаються keepalive повідомлення протоколу канального рівня.

Використовуючи результат команди show interfaces, можна усунути можливі проблеми таким чином.

- Якщо інтерфейс включений, а канальний протокол не функціонує, існує проблема. Можлива невідповідність типу інкапсуляції, інтерфейс на іншому кінці міг бути вимкнений в результаті збою або могли виникнути проблеми з апаратним забезпеченням.
- Якщо протокол канального рівня (Line protocol) та інтерфейс відключені, можливо, не підключений кабель або існують інші проблеми з інтерфейсом. Наприклад, при з’єднанні двох пристроїв безпосередньо міг бути відключений інтерфейс на іншому кінці.
- Якщо інтерфейс відключений адміністратором, він був відключений вручну (за допомогою команди shutdown) в активній конфігурації.

В деяких випадках помилки середовища передачі даних не проявляються в достатній мірі, щоб привести до виходу з ладу з’єднання, але погіршують продуктивність мережі. «Помилки введення» – це сума усіх помилок в датаграмах, які були отримані при аналізі інтерфейсу. Вони включають карликові (runts) і гігантські (giants) кадри, помилки CRC, відсутність буфера, кадр, переповнювання і проігноровані пакети. До помилок введення, які можна виявити за допомогою команди show interfaces, відносяться наступні.

- **Карликові кадри (runt frames)** - кадри Ethernet, розмір яких не перевищує мінімально дозволені 64 байти. Карликові кадри найчастіше бувають викликані несправністю мережевої плати, але можуть бути обумовлені іншими причинами, наприклад, надмірно високим числом колізій.
- **Гігантські кадри (giants)** - кадри Ethernet, розмір яких перевищує максимальну довжину кадру. Наявність гігантських кадрів викликана тими ж причинами, що і наявність карликових.
- **Помилки CRC –** в Ethernet і послідовних інтерфейсах помилки CRC зазвичай свідчать про неполадки в середовищі передачі або кабелі. Частими причинами помилок є електричні наведення, погано закріплені або пошкоджені роз’єми, а також невірно вибраний тип кабелю. Велика кількість помилок CRC призводить до шуму на каналі, тому слід перевірити кабель на ушкодження і допустиму довжину. Також по можливості слід знайти і усунути джерела шуму.

«Помилки виводу» - це сума усіх помилок, які перешкоджали успішній передачі датаграм з інтерфейсу, що перевірявся. До помилок введення, які можна виявити за допомогою команди show interfaces, відносяться наступні:

- **Колізії** - колізії в напівдуплексному режимі є нормою, тому про них не варто турбуватися до тих пір, поки робота напівдуплексного режиму вас влаштовує. Проте в правильно спроектованій і налагодженій мережі з використанням повнодуплексного зв'язку колізій бути не повинно. Рекомендовано використовувати повнодуплексний зв'язок, за винятком випадків, коли ви працюєте із застарілим устаткуванням, що вимагає використання напівдуплексного режиму.
- **Пізні колізії** - це колізії, які відбуваються після передачі 512 біт кадру (преамбули). Найбільш поширена причина пізніх колізій – перевищення допустимої довжини кабелю. Неправильне налаштування дуплексного зв'язку також може викликати пізні колізії, наприклад, у разі, коли один кінець з'єднання налаштований на повнодуплексний режим, а інший – на напівдуплексний режим. Ви виявите пізні колізії на інтерфейсі, налаштованому на напівдуплексний режим. Для вирішення цієї проблеми необхідно налаштувати один і той же дуплексний режим на обох кінцях з'єднання. У правильно спроектованій і налагодженій мережі пізні колізії виникати не повинні.

Протокол **Secure shell** (SSH) – це протокол, який забезпечує безпечне (зашифроване) з'єднання для управління віддаленим пристроєм. Для безпечного управління віддаленими підключеннями рекомендується замінити протокол Telnet протоколом SSH. Telnet є більш раннім протоколом, що використовує небезпечну незашифровану передачу як даних, так і ідентифікаційної інформації (ім'я користувача і пароль) між взаємодіючими пристроями. SSH забезпечує захист віддалених з'єднань, надаючи надійне шифрування даних аутентифікації пристрою (ім'я користувача і пароль), а також даних, що передаються між пристроями. SSH використовує TCP -порт 22. Telnet використовує TCP -порт 23.

Для функціонування протоколу SSH на комутаторі Catalyst 2960 комутатор повинен використовувати версію ПЗ IOS з криптографічними функціями і можливостями (шифруванням). Використовуйте команду show version на комутаторі, щоб дізнатися, на якій версії IOS працює в даний момент комутатор. У випадку якщо ім'я ОС включає поєднання k9, то ця версія IOS здійснює підтримку криптографічних функцій і можливостей (шифрування).

Перед налаштуванням протоколу SSH на комутаторі треба налаштувати унікальне ім'я вузла і відповідні параметри мережевого підключення.

Крок 1. Перевірка підтримки протоколу SSH.

Щоб перевірити, чи підтримується протокол SSH, використовуйте команду show ip ssh. Якщо на комутаторі працює IOS, що не підтримує криптографічні функції, ця команда не буде розпізнана.

Крок 2. Налаштування домена IP.

Присвойте ім'я IP -домену мережі за допомогою команди режиму глобальній конфигурації ip domain - name ім'я домена.

Крок 3. Створення пар ключів RSA.

Не у всіх версіях IOS за замовчуванням використовується версія 2 протоколу SSH, а версія 1 SSH містить ряд відомих вразливостей. Для налаштування SSH версії 2 використовується команда режиму глобальної конфігурації ip ssh version 2. Створення пари ключів RSA автоматично включає протокол SSH. Використовуйте команду режиму глобальною конфигурації crypto key generate rsa, щоб включити сервер SSH на комутаторі та згенерувати пару ключів RSA. При створенні ключів RSA адміністраторові вимагається ввести довжину модуля. Рекомендований мінімальний розмір модуля 1024 біт. Довший модуль безпечніший, але його створення і використання вимагає більше часу.

Крок 4. Налаштування аутентифікації користувача.

SSH -сервер може аутентифікувати користувачів локально або за допомогою сервера аутентифікації. Для використання локального методу аутентифікації створіть пару «ім'я

користувача - пароль» за допомогою команди режиму глобальної конфігурації username ім'я_користувача secret password.

Крок 5. Налаштування каналів vty.

Включите протокол SSH на каналах vty за допомогою команди режиму конфігурації каналу transport input ssh. Діапазон каналів vty комутатора Catalyst 2960 складає від 0 до 15. Ця конфігурація запобігає підключенням по протоколах окрім SSH (наприклад Telnet) і дозволяє комутатору приймати підключення тільки по протоколу SSH. Використовуйте команду режиму глобальної конфігурації line vty, а потім команду режиму конфігурації каналу login local, щоб при підключеннях SSH була потрібна локальна аутентифікація з локальної бази цих імен.

Крок 6. Включите SSH версії 2.

За замовчуваннямSSH підтримує обидві версії (1 і 2). Якщо підтримуються обидві версії, результат команди show ip ssh повідомляє про підтримку версії 1.99. У версії 1 є ряд відомих вразливостей. З цієї причини рекомендується включати тільки версію 2. Включіть цю версію SSH, використовуючи команду режиму глобальною конфигурациир ssh version 2.

Для підключення до сервера SSH на ПК використовується SSH -клієнт, наприклад PuTTY.

Для відображення використовуваної версії і конфігурації для протоколу SSH на пристрої, який ви налаштували в якості сервера SSH, використовуйте команду show ip ssh.

11.7. Поширені погрози безпеки

Базова система безпеки комутатора не блокує шкідливі атаки. Система безпеки – це багаторівневий процес, що вимагає безперервного вдосконалення. Чим краще мережеві фахівці організації обізнані про погрози безпеки і можливі наслідки, тим вище рівень захисту. Далі описані деякі види погроз безпеки.

Лавинна атака таблиці MAC-адрес

Таблиця MAC-адрес комутатора містить MAC-адреси, які пов'язані з кожним фізичним портом і відповідною VLAN. Коли комутатор 2-го рівня отримує кадр, він шукає в таблиці MAC-адрес MAC-адресу призначення. Коли кадри прибувають на порти комутатора, MAC-адреси джерела реєструються в таблиці MAC-адрес. Якщо для цієї MAC-адреси існує запис, комутатор пересилає кадр у відповідний порт. У випадку якщо MAC -адреси немає в таблиці MAC-адрес, комутатор розсилає кадр з кожного порту, крім того, на якому цей кадр був отриманий.

Подібна поведінка комутатора відносно невідомих MAC -адрес може використовуватися для атаки на комутатор. Цей вид атаки називається **переповнюванням таблиці MAC-адрес**. Атаку переповнювання таблиці MAC-адрес іноді називають **лавинною атакою**, а також атакою **переповнювання таблиці CAM**.

Деякі засоби мережевої атаки можуть генерувати до 155 000 записів в таблиці MAC-адрес комутатора в хвилину. Максимальний розмір таблиці MAC-адрес може розрізнятися залежно від типу комутатора.

Один із способів понизити ризик від атаки переповнювання таблиці MAC-адрес – налаштуватифункцію безпеки порту.

DHCP - спуфінг

DHCP – це протокол, який автоматично призначає вузлу допустиму IP -адресу з пулу DHCP. DHCP використовується для виділення адрес клієнтам практично так давно, як і протокол TCP/IP. Можна виконати два типи атак DHCP: атаки виснаження ресурсів і DHCP – спуфінг.

При атаках виснаження ресурсів DHCP зловмисник створює лавинну розсилку з DHCP -запитів на DHCP -сервер, щоб використовувати усі доступні IP -адреси, які може призначити сервер DHCP. Після розподілу усіх IP -адрес, які можуть бути призначені DHCP -сервером, відбувається відмова в обслуговуванні (DoS -атака), оскільки нові клієнти не можуть дістати доступ до мережі. DoS -атака – це будь-яка атака, яка використовується для переповнення

конкретних пристроїв і мережевих сервісів несанкціонованим трафіком, внаслідок чого дозволений трафік не може дістати доступ до цих ресурсів.

При DHCP -спуфінгу зловмисник настроює в мережі несправжній DHCP -сервер, щоб видавати для клієнтів DHCP -адреси. Мета цієї атаки – змусити клієнтів використовувати помилкову службу доменних імен (DNS) і Windows -службу імен Internet (сервер WINS), а також вузол або пристрій зловмисника як шлюз за замовчуванням.

Перед DHCP -спуфінгом часто використовується атака виснаження ресурсів DHCP для відмови обслуговування санкціонованого DHCP -сервера, завдяки чому набагато простіше впровадити в мережу фіктивний DHCP -сервер.

Для зниження ризику атак DHCP слід використовувати функції відстежування DHCP і безпеці порту.

Використання вразливостей протоколу CDP

Протокол виявлення Cisco (CDP) – це запатентований протокол, який може бути налагоджений на будь-яких пристроях Cisco. CDP виявляє інші пристрої Cisco з прямим підключенням, завдяки чому пристрої можуть автоматично налаштовувати свої підключення. В деяких випадках це спрощує процедури налаштування та підключення.

За замовчуванням усі порти на більшості маршрутизаторів і комутаторів Cisco налагоджені для використання CDP. Інформація CDP вирушає в періодичних незашифрованих широкомовних розсилках і оновлюється локально в базі даних CDP кожного пристрою. Оскільки CDP є протоколом 2-го рівня, повідомлення CDP не поширюються маршрутизаторами.

CDP містить наступну інформацію про пристрій: IP -адреса, версію IOS, а також відомості про платформу, можливості та native VLAN. Цією інформацією може скористатися зловмисник для пошуку способів атаки мережі, як правило, у формі атаки DoS.

На пристроях або портах, де використання CDP не є необхідністю, рекомендується відключити цей протокол за допомогою команди режиму глобальної конфігурації no cdp run. CDP може бути відключений на кожному порту.

Атаки Telnet

Telnet – це незахищений протокол, який може бути використаний для отримання зловмисником віддаленого доступу до мережевого пристрою. Існують інструменти, що дозволяють зловмиснику почати атаку методом повного перебору проти каналів vty на комутаторі.

Атака методом повного перебору (метод грубої сили)

На першому етапі атаки методом повного перебору зловмисник використовує список поширених паролів і програму, розроблену для встановлення сеансу Telnet за допомогою усіх слів із списку. Якщо пароль не виявлений на першому етапі, починається другий етап, у якому зловмисник використовує програму, що створює послідовні поєднання символів, намагаючись підібрати пароль. Маючи достатню кількість часу, таким методом зловмисник може зламати практично усі використовувані паролі.

Для того, щоб понизити ризик такої атаки, необхідно використовувати надійні паролі і не забувати їх регулярно міняти. Надійний пароль повинен містити комбінацію символів верхнього і нижнього регістрів, а також числівники і символи (спеціальні знаки). Доступ до каналів vty також можна обмежити за допомогою списку контролю доступу (ACL).

DoS -атака протоколу Telnet

Telnet також може бути схильний до DoS -атаки. При атаках типу «відмову в обслуговуванні» (DoS –атаках, Denial of Service) зловмисник використовує уразливості серверного ПЗ Telnet, запущеного на комутаторі, що робить сервіс Telnet недоступним. Цей тип атак блокує віддалений доступ адміністратору до функцій управління комутатором. Такі атаки можуть бути об’єднані з іншими прямими атаками на мережу як частину скоординованої спроби закрити мережевому адміністратору доступ до базових пристроїв на час пролому в системі безпеки.

Для забезпечення безпеки мережі використовуйте наступні практичні рекомендації.

- Розробіть політику забезпечення безпеки для компанії.
- Відключите невживані сервіси і порти.
- Використовуйте надійні паролі і регулярно міняйте їх.
- Обмежте фізичний доступ до пристроїв.
- Уникайте використання стандартних ненадійних веб-сайтів HTTP, особливо для екранів входу в систему. Замість них використовуйте безпечніші HTTPS.
- Регулярно виконуйте резервне копіювання даних і перевіряйте резервні файли.
- Розкажіть співробітникам про технологію соціальної інженерії і розробіть політику перевірки ідентифікації людей по телефону, через електронну пошту і особисто.
- Зашифровуйте і захищайте паролем уразливі дані.
- Забезпечте безпеку на програмному і апаратному рівнях, наприклад, встановіть брандмауери.
- Регулярно оновлюйте ПЗ, щодня або щотижня встановлюючи виправлення безпеки.

Вищезгадані рекомендації є основами управління безпекою. Організації повинні забезпечувати безперервний захист від технологій злому, що постійно розвиваються. Для виміру уразливості поточної мережі використовуйте засоби мережевої безпеки.

11.8. Інструменти і тестування мережевої безпеки

Засоби мережевої безпеки дозволяють мережевому адміністратору перевіряти мережу на наявність слабких сторін. Деякі інструменти дозволяють адміністратору виступати в ролі зловмисника. За допомогою одного з таких інструментів адміністратор може виконати атаку мережі і перевірити результати, щоб якнайкраще врегулювати політику безпеки для зниження ризику цих типів атак. Аудит засобів захисту і тестування на проникнення – це дві основні функції, що виконуються інструментами мережевої безпеки.

Адміністратор може вручну запустити методи тестування безпеки мережі. Інші способи тестування є автоматизованими. Незалежно від типу тестування співробітники, що настроюють і контролюючі тестування безпеки, повинні мати глибокі знання в сферах безпеки і мережевих технологій. Передусім, вони повинні розбиратися в наступних областях:

- мережева безпека;
- міжмережеві екрани;
- системи запобігання вторгненням;
- операційні системи;
- програмування;
- мережеві протоколи (наприклад TCP/IP);
- засоби мережевої безпеки дозволяють адміністраторові виконувати аудит безпеки мережі. Аудит безпеки вказує на тип інформації, який може зібрати зловмисник, отримавши контроль над мережевим трафіком.
- Наприклад, засоби аудиту мережевої безпеки дозволяють адміністраторові перевантажувати таблицю MAC-адрес помилковими MAC-адресами. Після того, як комутатор починає лавинну розсилку трафіку з усіх портів, виконується перевірка портів комутатора. Під час аудиту санкціоновані зіставлення MAC-адрес застарівають, через що їх замінюють помилкові зіставлення MAC-адрес. Таким чином можна визначити, які порти схильні до ризику і не налагоджені належним чином для запобігання атакам цього типу.
- Облік часу є важливим чинником успішного проведення аудиту. Різні комутатори підтримують різну кількість адрес у своїй таблиці MAC-адрес. Визначення відповідної кількості «отруєних» MAC-адрес для відправки на комутатор може виявитися непростим завданням. Мережевий адміністратор також повинен враховувати період застарівання таблиці MAC-адрес. Якщо «отруєні» MAC-адреси починають застарівати під час проведення аудиту мережі, допустимі MAC-адреси починають заповнювати таблицю MAC-адрес і обмежувати дані, які можна перевірити за допомогою засобу аудиту мережі.

- Засоби мережевої безпеки можна використовувати для тестування на проникнення в мережу. Тестування на проникнення – це модельована атака на мережу, мета якої полягає у визначенні міри уразливості мережі до реальної атаки. Подібне тестування дозволяє мережевому адміністраторові виявити слабкі сторони в конфігурації мережевих пристроїв і внести зміни, щоб зробити пристрої стійкішими до атак. Адміністратор може виконати багато атак, і більшість інструментів поставляються разом з детальною документацією про синтаксис команд, необхідний для виконання бажаного типу атаки.
- Оскільки тестування на проникнення можуть негативно позначитися на мережі, вони виконуються в строгій відповідності з політикою забезпечення безпеки мережі.

Відключення невживаних портів

- Відключення невживаних портів – це простий спосіб захисту мережі від несанкціонованого доступу. Приміром, якщо комутатор Catalyst 2960 має 24 порти і при цьому використовуються три підключення Fast Ethernet, рекомендується відключити 21 невживаний порт. Перейдіть до кожного невживаного порту і введіть команду Cisco IOS shutdown. Якщо надалі порт необхідно знову включити, це можна зробити за допомогою команди no shutdown. Для того, щоб налаштувати діапазон портів, використовується команда interface range:
- Switch(config)# interface range введіть модуль/перший номер - останній номер.

Процес включення і виключення портів може зайняти багато часу, але він підвищує безпеку мережі і коштує витрачених зусиль.

Функція безпеки порту

Перед введенням комутатора в експлуатацію необхідно забезпечити безпеку усіх портів (інтерфейсів) комутатора. Один із способів захисту портів – використання функції безпеки портів (функція Port Security). Ця функція обмежує кількість допустимих MAC-адрес на один порт, а також дозволяє доступ для MAC-адрес санкціонованих пристроїв і забороняє доступ для інших MAC-адрес.

Для того, щоб дозволити доступ одному або декільком MAC-адресам, необхідно налаштувати функцію безпеки портів. У випадку якщо кількість дозволених MAC-адрес на порту обмежена до одного, до цього порту може підключитися тільки пристрій з цією конкретною MAC-адресою.

Якщо порт налагоджений як захищений і досягнута максимальна кількість MAC-адрес, будь-які додаткові спроби підключення з невідомих адрес приведуть до порушення безпеки.

Види захисту MAC-адрес

Існує багато способів налаштувати функцію безпеки порту. Залежно від конфігурації розрізняють наступні типи захищених адрес :

- **Статичний захист MAC-адреси** - MAC-адреси, які налагоджені на порту вручну за допомогою команди режиму конфігурації интерфейса switchport port, - security mac - address MAC-адреси. MAC-адреси, налагоджені таким чином, зберігаються в таблиці адрес і додаються в поточну конфігурацію комутатора.
- **Динамічний захист MAC-адреси** - MAC-адреси, які отримані динамічно і зберігаються в таблиці адрес. MAC -адреси, налагоджені таким чином, видаляються при перезавантаженні комутатора.
- **Захист MAC-адреси на основі прив'язки**- MAC-адреси, які можуть бути отримані динамічно або налагоджені вручну. Вони зберігаються в таблиці адрес і додаються в поточну конфігурацію.

Захист MAC-адреси на основі прив'язки

Для того, щоб налаштувати інтерфейс для перетворення динамічно отриманих MAC-адрес в прикріплені захищені MAC-адреси і додати їх в поточну конфігурацію, необхідно включити функцію sticky learning (розпізнавання прикріплених адрес). Функція sticky learning включається на інтерфейсі за допомогою команди режиму конфігурації інтерфейсу switchport port - security mac - address sticky.

Після введення цієї команди комутатор перетворить усі динамічно отримані MAC-адреси, включаючи адреси, які були отримані динамічно до включення цієї функції, в прикріплені захищені MAC-адреси. Усі прикріплені захищені MAC-адреси додаються в таблицю адрес і в поточну конфігурацію.

Також прикріплені захищені MAC-адреси можна задати вручну. Коли прикріплені захищені MAC-адреси налагоджені за допомогою команди режиму конфігурації інтерфейсу switchport port - security mac - address stickyMAC -адрес, усі вказані адреси додаються в таблицю адрес і поточну конфігурацію.

Якщо прикріплені захищені MAC-адреси зберігаються у файлі завантажувальної конфігурації, то після перезавантаження комутатора або відключення інтерфейсу не потрібне повторне отримання адрес. Якщо ж прикріплені захищені адреси не зберігаються, вони будуть втрачені.

При відключенні режиму sticky learning за допомогою команди режиму конфігурації інтерфейсу no switchport port - security mac - address sticky прикріплені захищені MAC-адреси залишаються в таблиці адрес, але видаляються з поточної конфігурації.

Порушення безпеки відбувається в будь-якій з вказаних нижче ситуацій:

- Додана максимальна кількість захищених MAC-адрес в таблицю адрес на інтерфейсі, і станція, MAC-адреса якої не зафіксована в таблиці адрес, намагається дістати доступ до інтерфейсу.
- Адреса, отримана або налагоджена на одному захищеному інтерфейсі, помічена на іншому захищеному інтерфейсі в тій же VLAN.

Інтерфейс можна налаштувати на один з трьох режимів реагування на порушення безпеки, який визначає дії, що робляться у разі порушення.

Захист. Коли кількість захищених MAC-адрес досягає межі дозволених адрес для порту, пакети з невідомими адресами джерела відкидаються, поки не буде видалено достатню кількість захищених MAC-адрес або не буде збільшено максимальну кількість дозволених адрес. Для цього режиму не передбачено повідомлення про порушення безпеки.

- **Обмеження.** Коли кількість захищених MAC-адрес досягає межі дозволених адрес для порту, пакети з невідомими адресами джерела відкидаються, поки не буде видалено достатню кількість захищених MAC-адрес або не буде збільшено максимальну кількість дозволених адрес. Для цього режиму передбачено повідомлення про порушення безпеки.
- **Виключення.** У цьому режимі (встановленому за замовчуванням) порушення безпеки порту викликає негайне відключення інтерфейсу унаслідок помилки і відключає індикатор порту. Для цього режиму передбачено збільшення значення лічильника порушень. При виключенні захищеного порту в результаті збою його можна знову включити, використовуючи команди режиму конфігурації інтерфейсу shutdown ино shutdown.

Щоб змінити режим реагування на порушення безпеки на порту комутатора, використовується команда режиму конфігурації інтерфейсу switchport port - security violation {protect |restrict | shutdown}.

Перевірка захисту MAC -адрес

Для відображення усіх безпечних MAC-адрес, налагоджених на усіх інтерфейсах комутатора або на вказаному інтерфейсі з інформацією старіння для кожного інтерфейсу, використовується команда show port - security address. Коли налагоджена функція безпеки порту, порушення безпеки може привести до відключення порту в результаті помилки. У випадку якщо порт вимкнений в результаті помилки, він не функціонує і не може відправляти або отримувати трафік. На консолі відображуються серії повідомлень, пов’язаних з функцією безпеки порту.

Перед повторним включенням порту адміністратор повинен виявити джерело порушення безпеки. Якщо до захищеного порту підключений несанкціонований пристрій, порт не можна включати, поки не усунена загроза безпеки. Для повторного включення порту використовується команда режиму конфігурації інтерфейсу shutdown. Для того, щоб порт почав функціонувати, використовуйте команду конфігурації інтерфейсу no shutdown.

При роботі з мережами необхідно стежити за правильним налаштуванням часу. Точні часові відмітки потрібні для відстежування подій в мережі, наприклад порушень системи безпеки. Синхронізація годинника має вирішальне значення для правильної інтерпретації подій у файлах даних системного журналу, так само як і для цифрових сертифікатів.

Протокол мережевого часу (NTP) – це протокол для синхронізації годинника обчислювальних систем в мережах передачі даних із змінною затримкою і з комутацією пакетів. NTP дозволяє мережевим пристроям синхронізувати свої налаштування часу з сервером NTP. Клієнти NTP, які отримують відомості про час і дату з одного джерела, використовуватимуть коректніші налаштування часу.

Для надійної синхронізації часу усередині мережі мережевим адміністраторам слід застосувати власний еталонний мережевий генератор часу, синхронізований по всесвітньому координованому часу (UTC) за допомогою супутника або радіосигналу. У випадку якщо мережеві адміністратори не хочуть застосовувати власний еталонний мережевий генератор часу зважаючи на надмірні витрати або з інших причин, в Інтернеті доступні інші джерела синхронізації. NTP може отримати правильний час з внутрішнього або зовнішнього джерела синхронізації, включаючи:

- локальний тактовий генератор;
- тактовий генератор в Інтернеті;
- GPS або атомний годинник.

Мережевий пристрій можна налаштуватияк NTP -сервер або як NTP -клієнт. Для того, щоб дозволити синхронізацію програмного годинника з сервером часу NTP, використовуйте команду ntp server ip - address в режимі глобальної конфігурації. Щоб налаштуватидля пристрою тактовий генератор NTP, з яким можуть синхронізуватися однорангові вузли, використовуйте команду ntp master [stratum] у режимі глобальної конфігурації.

Висновок до лекції 11

Для того, щоб дозволити віддалену конфігурацію комутатора, IP -адреса привласнюється інтерфейсу SVI, що входить у віртуальну локальну мережу управління VLAN. За допомогою команди ip default - gateway на комутаторі необхідно налаштувати шлюз за замовчуванням, що належить мережі управління VLAN. Якщо шлюз за замовчуванням налагоджений неправильно, віддалене управління неможливе. Для забезпечення безпечного (зашифрованого) підключення до віддаленого пристрою рекомендується використовувати протокол Secure Shell (SSH), який, на відміну від протоколу Telnet, дозволяє запобігти перехоплення незашифрованих імен користувачів і паролів.

Однією з переваг комутатора є те, що він підтримує повнодуплексний зв’язок між пристроями, що удвічі підвищує швидкість передачі даних. Незважаючи на те, що можна задати швидкість і режим дуплексного зв’язку інтерфейсу комутатора, рекомендується дозволити для комутатора автоматичне налаштування цих параметрів для запобігання появі помилок.

Функція безпеки порту комутатора потрібна для запобігання лавинної розсилки MAC-адрес і DHCP -спуфінга. Порти комутатора слід налаштовувати так, щоб доступ був дозволений тільки для кадрів з конкретними MAC-адресами джерела. Кадри від невідомих MAC-адрес джерела мають бути заборонені та викликати відключення порту для запобігання подальшим атакам.

Функція безпеки портів – це єдиний засіб захисту від зниження продуктивності мережі. Для забезпечення захисту мережі пропонуємо необхідно дотримуватися практичних рекомендацій:

- Розробіть політику забезпечення безпеки для компанії.
- Відключіть невживані сервіси і порти.
- Використовуйте надійні паролі і регулярно міняйте їх.
- Обмежте фізичний доступ до пристроїв.

- Уникайте використання стандартних ненадійних веб-сайтів HTTP, особливо для екранів входу в систему. Замість них використовуйте безпечніші HTTPS.
- Регулярно виконуйте резервне копіювання даних і перевіряйте резервні файли.
- Розкажіть співробітникам про технологію соціальної інженерії і розробіть політику перевірки ідентифікації людей по телефону, через електронну пошту і особисто.
- Зашифровуйте і захищайте паролем уразливі дані.
- Забезпечуйте безпеку на програмному і апаратному рівнях, наприклад, встановіть брандмауери.
- Регулярно оновлюйте ПЗ, щодня або щотижня встановлюючи виправлення безпеки.

Вищезгадані рекомендації є основами управління безпекою. Організації повинні забезпечувати безперервний захист від технологій злому, що постійно розвиваються.

Питання для закріплення

1. Які основні принципи роботи комутатора?
2. Які методи пересилки на комутаторі ви знаєте?
3. Що таке колізійні та широкомовні домени?
4. Назвіть характеристики комутаторів, які сприяють зниженню перевантажень у мережі.
5. Які ви знаєте базові налашування комутатора?
6. Які ви знаєте неполадки на рівні мережевого доступу?
7. Які ви знаєте поширені погрози безпеки?
8. Які ви знаєте інструменти і тестування мережевої безпеки?

Список рекомендованої літератури

1. CCNA R&S RSE Chapter 2: Basic Switching Concepts and Configuration // Електронний ресурс. Режим доступу: https://static-course-assets.s3.amazonaws.com/RSE50ENU/module2/index.html

2. Attacks – DHCP Server Spoofing // Електронний ресурс. Режим доступу: https://learningnetwork.cisco.com/docs/DOC-24355

4. The DDoS That Almost Broke the Internet // Електронний ресурс. Режим доступу: https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/

Лекція 12. Тема: «Проектування віртуальних локальних мереж»

План лекції

12.1. Призначення і переваги віртуальних локальних мереж.
12.2. Типи віртуальних локальних мереж**.**
12.3. Тегування кадрів Ethernet для ідентифікації мережі VLAN.
12.4. Діапазони VLAN на комутаторах.
12.5. Створення віртуальної локальної мережі.
12.6. Протокол DTP.
12.7. Проблематика VLAN.
12.8. Рекомендації з проектування VLAN.

12.1. Призначення і переваги віртуальних локальних мереж

У комутованих об'єднаних мережах мережі **VLAN** (Virtual Local Area Network) забезпечують гнучкість сегментації і організації. Мережі VLAN дозволяють згрупувати пристрої усередині локальної мережі.

Група пристроїв в межах мережі VLAN взаємодіє так, ніби пристрої підключені за допомогою одного дроту. Мережі VLAN грунтуються не на фізичних, а на логічних підключеннях (рис.12.1).

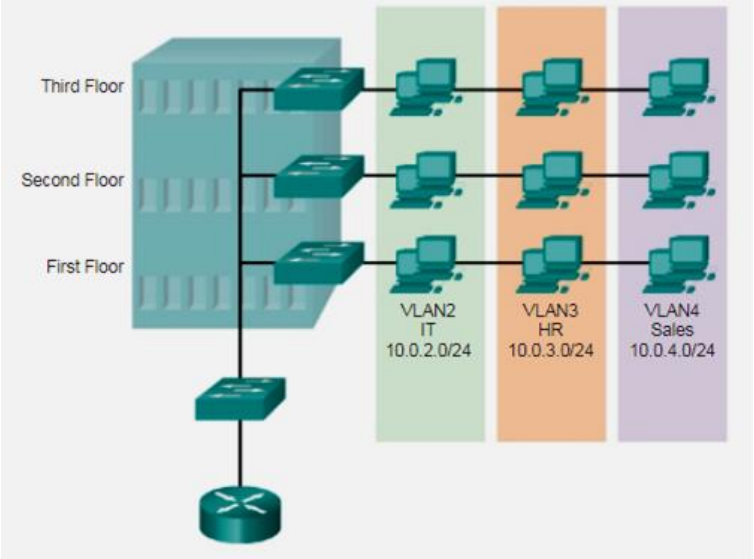


Рис. 12.1.Визначення груп віртуальної локальної мережі [1]

Мережі VLAN дозволяють адміністраторові проводити сегментацію за функціями, проектними групами або сферами застосування, незалежно від фізичного розташування користувача або пристрою. Пристрої в межах мережі VLAN працюють таким чином, ніби знаходяться у власній незалежній мережі, навіть якщо ділять одну загальну інфраструктуру з іншими VLAN. Будь-який порт комутатора може належати мережі VLAN. Одноадресні, широкомовні і багатоадресні пакети пересилаються і розсилаються тільки до кінцевих станцій у межах тієї мережі VLAN, яка є джерелом цих пакетів. Кожна мережа VLAN вважається окремою логічною мережею, і пакети, адресовані станціям, що не належать цій мережі VLAN, повинні пересилатися через пристрій, що підтримує маршрутизацію. Мережа VLAN створює логічний широкомовний домен, який може охоплювати декілька фізичних сегментів LAN. Розділяючи великі широкомовні домени на дрібніші мережі, VLAN підвищують продуктивність мережі. Якщо пристрій в одній мережі VLAN передає широкомовний кадр Ethernet, то цей кадр отримують усі пристрої у рамках цієї VLAN, пристрої ж в інших мережах VLAN цей кадр не отримують. Мережі VLAN дозволяють реалізовувати політику забезпечення доступу і безпеки, враховуючи інтереси різних груп користувачів. Кожен порт комутатора може бути призначений тільки одній мережі VLAN (за винятком порту, підключеного до IP -телефону або до іншого комутатора).

Мережі VLAN полегшують процес проектування мережі, що забезпечує допомогу у виконанні цілей організації. До основних переваг використання VLAN відносяться:

- **Безпека:** групи, що мають уразливі дані, відокремлені від іншої частини мережі, завдяки чому знижується вірогідність просочування конфіденційної інформації.
- **Зниження витрат:** завдяки економії на дорогих оновленнях мережевої інфраструктури і ефективнішому використанню наявної смуги пропускання і висхідних каналів відбувається зниження витрат.
- **Підвищення продуктивності:** розподіл однорідних мереж 2-го рівня на декілька логічних робітників груп (широкомовних доменів) зменшує кількість зайвого мережевого трафіку і підвищує продуктивність.

- **Зменшені широкомовні домени:** розподіл мережі на мережі VLAN зменшує кількість пристроїв в широкомовному домені.
- **Підвищення продуктивності IT-відділу:** мережі VLAN спрощують управління мережею, оскільки користувачі з аналогічними вимогами до мережі використовують одну і ту ж мережу VLAN. При введенні в експлуатацію нового комутатора на призначених портах реалізуються усі правила і процедури конкретної VLAN. Також IT-спеціалистам легше визначати функцію мережі VLAN, призначаючи їй відповідне ім'я.
- **Спрощене управління проектами і застосуваннями:** мережі VLAN об'єднують користувачів і мережеві пристрої для відповідності діловим або географічним вимогам мережі. Управління проектом і робота на прикладному рівні спрощені завдяки використанню розподілу функцій.

12.2. Типи віртуальних локальних мереж

Віртуальна локальна мережа для даних – це мережа VLAN, яка налагоджена спеціально для передачі користувацького трафіку. Мережа VLAN, що передає голосовий трафік або трафік управління, не є мережею VLAN для передачі даних. Рекомендується відділяти голосовий трафік від трафіку даних. VLAN для передачі даних іноді називають користувацькою мережею VLAN. Мережі VLAN для даних використовуються для розподілу мережі на групи користувачів або пристроїв.

Мережа VLAN за замовчуванням. Усі порти комутатора стають частиною VLAN за замовчуванням після первинного завантаження комутатора. Порти комутатора, що знаходяться в мережі VLAN за замовчуванням, є частиною одного широкомовного домена. Завдяки цьому будь-який пристрій, підключений до будь-якого порту комутатора, може обмінюватися даними з іншими пристроями на інших портах комутатора. Мережею VLAN за замовчуванням для комутаторів Cisco VLAN 1.

VLAN 1 підтримує усі функції будь-якої мережі VLAN, проте її не можна перейменувати або видалити. За замовчуванням увесь трафік 2-го рівня пов'язаний з мережею VLAN 1.

Мережа native VLAN. Мережа native VLAN призначена транковому порту 802.1Q.

Транкові порти – це канали між комутаторами, які підтримують передачу трафіку, пов'язаного з більш ніж однією мережею VLAN. Транковий порт 802.1Q підтримує трафік, що поступає від декількох VLAN (тегований трафік), а також трафік, який поступає не від VLAN (нетегований трафік). **Тегованим** називається трафік, для якого в початковий заголовок кадру Ethernet вставлений 4-байтовий тег, що визначає мережу VLAN, до якої відноситься цей кадр. Транковий порт 802.1Q розміщує нетегований трафік в мережі native VLAN, якою за замовчуванням є VLAN 1.

Мережі native VLAN визначені в специфікації IEEE 802.1Q для забезпечення зворотної сумісності з нетегованим трафіком, характерним для застарілих сценаріїв локальних мереж. Мережа native VLAN служить загальним ідентифікатором на протилежних кінцях транкового каналу.

Рекомендується налаштувати native VLAN як невживану VLAN, що відрізняється від мережі VLAN 1 та інших VLAN. Фактично прийнято виділяти фіксовану VLAN для виконання ролі мережі native VLAN для усіх транкових портів в комутованому домені.

Управляюча VLAN – це будь-яка мережа VLAN, налагоджена для доступу до функцій управління комутатора. Мережа VLAN 1 за замовчуванням є управляюча VLAN. Для створення управляючої VLAN інтерфейсу SVI комутатора цієї VLAN призначаються IP - адреса і маска підмережі, завдяки чому комутатором можна управляти через протоколи HTTP, Telnet, SSH або SNMP.

На рис. 12.2 усі порти призначені мережі VLAN 1 за замовчуванням. Жодна native VLAN не призначена явно, і жодна інша мережа VLAN не є активною. Таким чином, мережі native VLAN і VLAN, що управляє, співпадають. Подібне налаштування вважається загрозою безпеки.

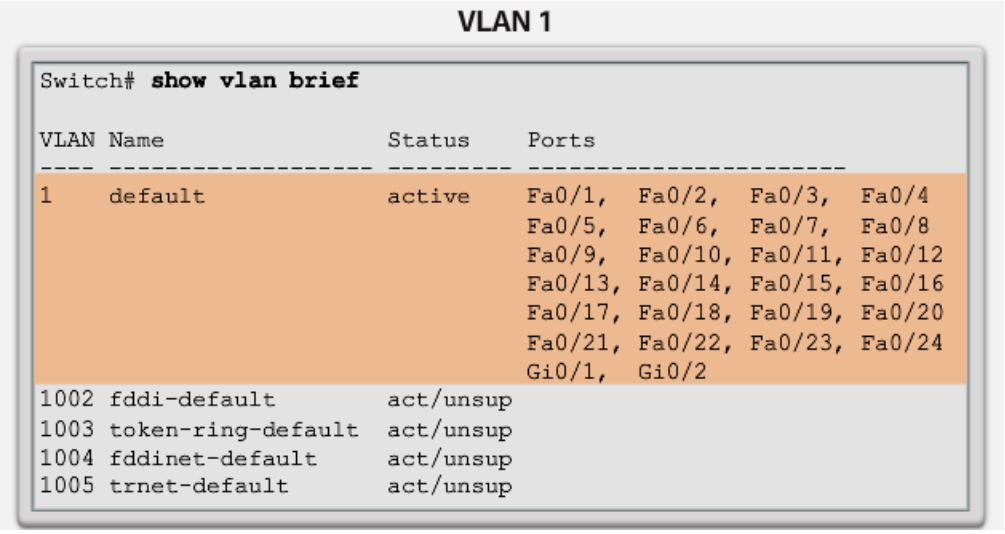


Рис. 12.2. Перегляд короткої інформації про VLAN на комутаторі [1]

Голосові мережі VLAN. Для підтримки передачі голосу по IP (VoIP) потрібно окрему мережу VLAN. Для VoIP -трафіка потрібні:

- гарантована смуга пропускання для забезпечення високої якості голосової передачі;
- пріоритет передачі перед іншими типами мережевого трафіку;
- можливість маршрутизації в обхід переобтяжених ділянок;
- затримка менше 150 мс по усій мережі.

Для того, щоб відповідати цим вимогам, уся мережа має бути спеціально спроектована для підтримки VoIP.

Транки віртуальних мереж – це канал типу «точка-точка» між двома мережевими пристроями, який підтримує більш ніж одну мережу VLAN. Транк віртуальних мереж розширює мережі VLAN по усій мережі. Використання мереж VLAN без транкових каналів істотно знижує корисні можливості VLAN. Транки віртуальних мереж забезпечують поширення усього трафіку VLAN між комутаторами так, щоб пристрої, що знаходяться в одній мережі VLAN, але підключені до різних комутаторів, могли обмінюватися даними без втручання маршрутизатора.

Транк віртуальних мереж не належить якій-небудь певній мережі VLAN, а, швидше, є «кабельним каналом» передачі багатьох VLAN між комутаторами і маршрутизаторами. Транк може також використовуватися між мережевим пристроєм і сервером або іншим пристроєм, оснащеним відповідним мережевим адаптером з підтримкою 802.1Q.

12.3. Тегування кадрів Ethernet для ідентифікації мережі VLAN

Стандартний заголовок кадру Ethernet не містить інформацію про VLAN, до якої відноситься кадр. Тому, коли кадри Ethernet розміщуються в транковому каналі, необхідно додати інформацію про мережі VLAN, яким вони належать. Цей процес називається **тегуванням** і виконується за допомогою заголовка IEEE 802.1Q, вказаного в стандарті IEEE 802.1Q. Заголовок 802.1Q містить тег розміром 4 байти, який додається в оригінальний заголовок кадру Ethernet та ідентифікує VLAN, до якої відноситься кадр.

Коли комутатор отримує кадр через порт, налагоджений в режимі доступу і призначений мережі VLAN, комутатор додає в заголовок кадру мітку VLAN, наново обчислює FCS і відправляє тегований кадр з транкового порту.

Поле тегу VLAN складається з поля типу, поля пріоритету, поля ідентифікатора канонічного формату і поля ідентифікатора VLAN.

- **Тип –** це 2-байтове значення, яке називається значенням ідентифікатора протоколу тегування (TPID). Значення для Ethernet має вигляд шістнадцятиричного числа 0x8100.

- **Пріоритет користувача –** це 3-бітове значення, яке підтримує реалізацію рівня або сервісу.
- **Ідентифікатор канонічного формату (CFI) –** це 1-бітовий ідентифікатор, який забезпечує передачу кадрів по каналах Ethernet.
- **VLAN -ідентификатор (VID) –** це 12-бітовий ідентифікаційний номер VLAN, який підтримує до 4096 ідентифікаторів VLAN.

Після того, як комутатор додасть поля типу та інформації управляючого тега, він перераховує значення FCS і додає в кадр нове значення FCS.

Деякі пристрої, що підтримують транковий зв'язок, додають мітку в трафік мережі native VLAN. Якщо транковий порт 802.1Q отримує тегований кадр з таким же ідентифікатором VLAN, як у мережі native VLAN, то він відкидає кадр.

Коли транковий порт комутатора Cisco отримує нетеговані кадри (які рідко зустрічаються в добре спроектованій мережі), він пересилає ці кадри в мережу native VLAN. Якщо з мережею native VLAN не пов'язані ніякі пристрої (що буває досить часто), а також немає інших транкових портів (що також часто трапляється), то кадр відкидається. Мережею native VLAN за замовчуванням є мережа VLAN 1. При налаштуванні транкового порту 802.1Q порту ідентифікатора VLAN за замовчуванням (PVID) привласнюють значення ідентифікатора мережі native VLAN. Увесь нетегований трафік, що поступає в порт 802.1Q або з нього, пересилається відповідно до значення PVID.

12.4. Діапазони VLAN на комутаторах

Різні комутатори Cisco Catalyst підтримують різну кількість мереж VLAN. Кількість підтримуваних мереж VLAN досить велика для задоволення потреб більшості організацій. Наприклад, комутатори Catalyst 2960 і 3560 здатні підтримувати більше 4 тисяч мереж VLAN. Віртуальні локальні мережі стандартного діапазону на цих комутаторах мають ідентифікатор від 1 до 1 005, а мережі VLAN розширеного діапазону – від 1 006 до 4 094.

Віртуальні локальні мережі стандартного діапазону

- Використовуються в малих і середніх мережах підприємств і організацій.
- Визначаються ідентифікатором VLAN від 1 до 1005.
- Ідентифікатори від 1002 до 1005 зарезервовані для мереж VLAN Token Ring і FDDI.
- Ідентифікатори 1 і ідентифікатори від 1002 до 1005 створюються автоматично і не можуть бути видалені.
- Конфігурації зберігаються у файлі бази даних VLAN під ім'ям vlan.dat. Файл vlan.dat розташований у флеш-памяти комутатор.
- Протокол VTP (транковий протокол VLAN), що допомагає управляти конфігураціями VLAN між комутаторами, може розпізнавати і зберігати тільки мережі VLAN стандартного діапазону.

Мережі VLAN розширеного діапазону

- Дозволяють операторам зв'язку розширювати свою інфраструктуру для великого числа клієнтів. Деяким великим міжнародним корпораціям потрібні ідентифікатори VLAN розширеного діапазону.
- Визначаються ідентифікатором VLAN від 1006 до 4094.
- Конфігурації мереж не записуються у файл vlan.dat.
- Підтримують менше функцій VLAN, чим мережі VLAN стандартного діапазону.
- За замовчуваннямзберігаються у файл поточної конфігурації.
- Протокол VTP не розпізнає мережі VLAN розширеного діапазону.

Примітка. 4096 – це максимальна кількість VLAN, доступних на комутаторах Catalyst, оскільки в полі ідентифікатора VLAN заголовка IEEE 802.1Q налічується 12 біт.

12.5. Створення віртуальної локальної мережі

При налаштуванні мереж VLAN стандартного діапазону відомості про конфігурацію зберігаються у флеш-пам'яті комутатора у файлі під ім'ям vlan.dat. Флеш-пам'ять є постійною, тому не вимагає виконання команди copy running - config startup - config. Проте, оскільки під час створення мереж VLAN на комутаторі Cisco часто необхідно настроювати інші параметри, рекомендується зберігати зміни поточної конфігурації в початкову завантажувальну конфігурацію.

Окрім введення одного ідентифікатора VLAN, можна ввести групу ідентифікаторів VLAN, розділених точками, або діапазон ідентифікаторів VLAN, розділених дефісами, за допомогою команди vlan vlan - id. Наприклад, для створення мереж VLAN 100, 102, 105, 106 і 107 використовується наступна команда:

S1(config)# vlan 100,102,105-107

Наступний крок після створення мережі VLAN – призначення портів мережам VLAN. Порт доступу може одночасно належати тільки одній VLAN. Єдиним виключенням з цього правила є порт, підключений до IP -телефону. В цьому випадку з портом пов'язані дві VLAN: одна для голосового зв'язку і одна для даних.

Примітка. Для одночасного налаштування декількох інтерфейсів використовується команда interface range.

Транк віртуальної мережі – це канал OSI 2-го рівня між двома комутаторами, який передає трафік в усі мережі VLAN (якщо список допустимих мереж VLAN не обмежений вручну або динамічно). Для того, щоб активувати транкові канали, необхідно налаштувати порти на будь-якому кінці фізичного каналу за допомогою паралельних наборів команд.

Щоб налаштувати порт комутатора на одному кінці транкового каналу, використовується команда switchport mode trunk. За допомогою цієї команди інтерфейс переходить в постійний транковий режим. На порту починається узгодження протоколу DTP для перетворення каналу в транковий, навіть якщо інтерфейс, підключений до нього, не погоджується на подібну зміну.

На рис. 12.3. порт F0/1 комутатора S1 налагоджений як транковый порт, в якості мережі native VLAN призначена VLAN 99, а магістральний канал налагоджений для передачі трафіку тільки для мереж VLAN 10, 20, 30 і 99.

```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30,99
S1(config-if)# end
```

Рис. 12.3. Приклад конфігурації транкового каналу [1]

На рис.12.4. показана конфігурація порту F0/1 на комутаторі S1. Конфігурацію можна перевірити за допомогою команди show interfaces interface - ID switchport.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```

Рис. 12.4.Перевірка конфігурації транкового каналу [1]

У верхній виділеній області показано, що адміністративний режим порту F0/1 налагоджений на trunk. Порт знаходиться в режимі транка. У наступній виділеній області видно, що мережа native VLAN - це VLAN 99. Далі в нижній виділеній області вихідних даних показано, що усе VLAN в транковом каналі активні.

12.6. Протокол DTP

Транкові інтерфейси Ethernet підтримують різні транкові режими. Інтерфейс може бути встановлений в транковий або нетранковий режим або налагоджений для узгодження транковго зв'язку з сусіднім інтерфейсом. Узгодження транкового каналу виконується протоколом динамічного створення транкового каналу (**DTP**, dynamic trunking protocol), який діє тільки за принципом наскрізного підключення між пристроями мережі.

Протокол DTP – запатентований протокол Cisco, який автоматично включений на комутаторах Catalyst 2960 і Catalyst 3560. Комутатори інших виробників не підтримують DTP. DTP управляє транковим узгодженням тільки у випадку, якщо порт сусіднього комутатора налагоджений у режимі транка, який підтримує DTP.

Деякі міжмережеві пристрої можуть пересилати кадри DTP неправильно, через що можуть виникнути помилки конфігурації. Щоб цього уникнути, необхідно відключити DTP на інтерфейсах комутатора, який підключений до пристроїв, що не підтримують DTP.

Для того, щоб включити транковий зв'язок від коммутатора до пристрою, який не підтримує DTP, використовується команда режиму конфігурації интерфейса switchport mode trunk та switchport nonegotiate. Команда перетворить інтерфейс в транковий канал, але не дозволяє йому створювати кадри DTP.

Інтерфейси Ethernet на комутаторах Catalyst 2960 і Catalyst 3560 підтримують різні транкові режими за допомогою протоколу DTP:

- **switchport mode access** - переводить інтерфейс (порт доступу) в постійний нетранковий режим і повідомляє, що канал перетворений в нетранковий канал. Інтерфейс стає нетранковим незалежно від того, чи являється сусідній інтерфейс транковим або ні.
- **switchport mode dynamic auto** - дозволяє інтерфейсу перетворювати канал в транковий канал. Інтерфейс стає транковим, якщо сусідній інтерфейс переведений в

транковий або рекомендований режим. Режим порту комутатора за замовчуванням для усіх інтерфейсів Ethernet - dynamic auto.

- **switchport mode dynamic desirable** - наказує інтерфейсу перетворювати канал в транковий канал. Інтерфейс стає транковим, якщо сусідній інтерфейс переведений в транковий, рекомендований або автоматичний режим.
- **switchport mode trunk** - переводить інтерфейс в постійний транковий режим і погоджує для перетворення сусіднього каналу в транковий канал. Інтерфейс стає транковим, навіть якщо сусідній інтерфейс не є таким.
- **switchport nonegotiate** - забороняє інтерфейсу створювати кадри DTP. Цю команду можна використовувати тільки тоді, якщо режим порту комутатора інтерфейсу знаходиться в режимі access або trunk. Щоб встановити транковий канал, необхідно вручну налаштувати сусідній інтерфейс в якості транкового інтерфейсу.

Щоб визначити поточний режим DTP, використовується команда show dtp interface.

12.7. Проблематика VLAN

Кожній VLAN повинна відповідати унікальна IP -підмережа. Якщо два пристрої в одній мережі VLAN мають різні адреси підмереж, вони не можуть обмінюватися даними. Ця невідповідність є поширеною проблемою, і для її вирішення треба виявити помилку в конфігурації і змінити адресу підмережі на правильний.

Якщо між пристроями в VLAN як і раніше немає з'єднання, але проблеми з IP -адресацією були усунені, необхідно виконати наступні дії.

1. Застосувати команду show vlan, щоб переконатися, що порт належить очікуваній VLAN. Якщо порт призначений невірною VLAN, використовуйте команду switchport access vlan для коригування приналежності VLAN. Використовуйте команду show mac address - table для перевірки адрес, отриманих на окремому порту комутатора і призначених VLAN цьому порту.

2. Якщо VLAN, яким призначений порт, видалена, порт стає неактивним. Використовуйте команду show vlan або show interfaces switchport.

Для відображення таблиці MAC-адрес використовуйте команду show mac - address - table. Кожен порт комутатора належить мережі VLAN. Якщо VLAN, якій належить порт, видалена, порт стає неактивним. Усі порти, що належать видаленій мережі VLAN, не зможуть взаємодіяти з іншими сегментами мережі. Для того, щоб перевірити, чи активний порт, використовуйте команду show interface f0/1 switchport. Якщо порт неактивний, він не працюватиме, поки за допомогою командыvlan vlan_id не буде створена відсутня VLAN.

Типовим завданням мережевого адміністратора є усунення неполадок при створенні транкового каналу або в каналах, які некоректно працюють в якості транкових. Іноді порт комутатора може працювати як транковий порт, навіть якщо він не налагоджений для цього. Наприклад, порт доступу може приймати кадри від мереж VLAN, до яких цей порт не призначений.

Для усунення неполадок при невдалому створенні транкового каналу необхідно виконати наступні дії.

Крок 1. Використати команду show interfaces trunk, щоб перевірити, чи співпадають локальна мережа і рівноправний вузол native VLAN.

Крок 2. Використати команду show interfaces trunk для перевірки встановлення транкового каналу між комутаторами.

Для того, щоб відобразити стан транка, мережі native VLAN, використовується команда show interfaces trunk. Якщо на одному кінці транкового підключення налагоджена мережа native VLAN 99, а на іншому – native VLAN 2, то кадр, відправлений з мережі VLAN 99 на одному кінці, буде отриманий в мережі VLAN 2 на іншому кінці. Трафік VLAN 99 потрапляє в сегмент VLAN 2.

CDP відображує повідомлення про неспівпадання native VLAN в транковому каналі таким повідомленням :

**Mar 1 06:45:26.232: %CDP-4 -NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (2), with S2 FastEthernet0/1 (99).

При виникненні неспівпадань native VLAN відбуваються проблеми з підключенням в мережі. Трафік цих мереж VLAN, окрім двох налагоджених мереж native VLAN, успішно проходить по транковому каналу, але дані, пов'язані з якою-небудь з цих двох native VLAN, не проходять по транковому каналу.

Причиною неполадок в транкових каналах зазвичай є неправильна конфігурація. При налаштуванні мереж VLAN і транкових каналів в комутованій інфраструктурі часто трапляються наступні типи помилок конфігурації.

- **Неспівпадання native VLAN:** транкові порти налагоджені з різними мережами native VLAN. При цій помилці конфігурації генеруються консольні повідомлення, а трафік, що управляє і адміністративний, вирушають в невірному напрямі. Це спричиняє за собою загрозу безпеки.
- **Неспівпадання транкового режиму:** для одного транкового порту налагоджений режим, невідповідний транковому режиму відповідного порту з іншого боку. При цій помилці конфігурації транковый канал перестає працювати.
- **Дозволені мережі VLAN в транкових каналах:** список мереж VLAN, дозволених в транку, не був оновлений відповідно до поточних вимог VLAN. В цьому випадку по мережі передається непередбачений трафік або ж зовсім порушується передача трафіку.

Якщо виявлена проблема з транковим каналом, а причина невідома, почніть усунення неполадок з перевірки неспівпадання транкових каналів для native VLAN. Якщо причина не в цьому, перевірте неспівпадання транкового режиму, потім перевірте список дозволених VLAN.

Транкові канали зазвичай настроюються статично за допомогою команди switchport mode trunk. Для успішної передачі трафіку з мережі VLAN по транку ця VLAN має бути дозволена на транковом каналі. Для цього використовуйте команду switchport trunk allowed vlan vlan -id.

У сучасних комутованих мережах існує безліч різних типів атак. Архітектура VLAN спрощує обслуговування мережі і підвищує продуктивність, проте також дає зловмисникам можливість для атаки. Необхідно розуміти як принцип дії різних типів атак, так і методи зниження ризику атак.

Атака VLAN hopping дозволяє сторонньою VLAN бачити трафік інший, VLAN, що атакується. **Спуфінг комутатора** – це тип атаки мережі VLAN, при якому використовується неправильно налагоджений транковий порт. За замовчуванням транкові порти мають доступ до усіх мереж VLAN і передають трафік для декількох VLAN через один і той же фізичний канал, як правило, між комутаторами.

У простому випадку спуфінг-атаки комутатора зловмисник у своїх інтересах користується тим, що порт комутатора за замовчуванням налаштований на динамічний автоматичний режим. Зловмисник конфігурує систему так, щоб вона поводилася як комутатор. Для такого спуфінга зловмисник повинен уміти імітувати повідомлення 802.1Q і DTP. Змусивши комутатор думати, що інший комутатор намагається створити транковий канал, зловмисник може дістати доступ до усіх мереж VLAN, дозволених на цьому транковому порті.

Кращий спосіб запобігти базовій спуфінг-атаку – відключити транковий зв'язок на усіх портах, за винятком тих, на яких транковий зв'язок потрібний. На потрібних транкових портах необхідно відключити DTP і вручну включити транковий зв'язок.

Інший тип атаки мережі VLAN – це **атака з подвійним тегуванням** (чи з подвійною інкапсуляцією). Цей вид атаки заснований на використанні принципів роботи апаратного забезпечення на більшості комутаторів. Більшість комутаторів виконують лише один рівень деінкапсуляції 802.1Q, що дозволяє зловмисникові вставляти в кадр приховану мітку 802.1Q. Мітка дозволяє пересилати кадр в мережу VLAN, яка не вказана первинною міткою 802.1Q.

Важлива властивість атаки з подвійною інкапсуляцією полягає в тому, що вона діє, навіть якщо транкові порти відключені, оскільки зазвичай вузол відправляє кадр в сегменті, який не є транковим каналом.

Атака VLAN hopping з подвійним тегуванням відбувається в три кроки:

1. Зловмисник відправляє на комутатор кадр з подвійним тегуванням 802.1Q. Зовнішній заголовок містить мітку мережі VLAN зловмисника, яка співпадає з native VLAN транкового порту. Передбачається, що комутатор обробляє отриманий від зловмисника кадр, ніби він знаходиться на транковому порті або порті з голосовою VLAN (комутатор не повинен отримувати тегований кадр Ethernet на порті доступу). В якості прикладу уявіть, що мережею native VLAN є VLAN 10. Внутрішній тег – це VLAN, підвладна атаці. В даному випадку – VLAN 20.

2. Кадр прибуває на комутатор, який перевіряє перші 4 байти тега 802.1Q. Комутатор бачить, що кадр призначений для VLAN 10, яка є мережею native VLAN. Видаливши мітку VLAN 10, комутатор пересилає пакет з усіх портів мережі VLAN 10. На транковому порті віддаляється мітка мережі VLAN 10, але пакет не тегується знову, оскільки він є частиною native VLAN. В цей час мітка мережі VLAN 20 як і раніше незаймана і не перевіряється першим комутатором.

3. Другий комутатор перевіряє тільки внутрішній тег 802.1Q, відправлений зловмисником, і бачить, що кадр призначений для мережі VLAN 20, що являється метою зловмисника. Другий комутатор відправляє кадр на порт, що атакується, або наповнює його лавинною розсилкою залежно від того, чи є в таблиці MAC-адрес запис для вузла, що атакується.

Цей вид атаки є однонапрямленим і працює, тільки якщо зловмисник підключений до порту, що знаходиться в тій же VLAN, що і мережа native VLAN транкового порту. Запобігти такій атаці не так легко, як зупинити звичайні атаки VLAN hopping.

Кращий спосіб зниження шкоди від атак з подвійним тегуванням – упевнитися, що мережа native VLAN транкових портів відрізняється від VLAN будь-яких користувацьких портів. Рекомендується використовувати фіксовану VLAN, яка відрізняється від усіх призначених для користувача VLAN в комутованій мережі, в якості мережі native VLAN для усіх транковых каналів 802.1Q.

12.8. Рекомендації з проектування VLAN

VLAN 1 є мережею Ethernet VLAN за замовчуванням. Найкращий метод забезпечення безпеки – налаштувати усі порти на усіх комутаторах так, щоб вони були пов’язані з мережами VLAN, виключаючи мережу VLAN 1. Для цього, як правило, треба налаштувати усі невживані порти в мережу VLAN «чорної діри», яка ніколи не використовується в мережі. Для запобігання несанкціонованому доступу рекомендується відключати невживані порти комутатора.

Також для забезпечення безпеки рекомендується відділяти адміністративний трафік від призначеного для користувача. VLAN, що управляє, встановлена за замовчуванням мережею VLAN 1, слід замінити на іншу VLAN. Для віддаленого управління комутатором Cisco комутатору потрібна IP -адреса, налагоджена на управляючій VLAN. Користувачі в інших мережах VLAN не зможуть встановлювати сеанси віддаленого доступу з комутатором, якщо вони не були маршрутизовані в управляючій VLAN із забезпеченням додаткового рівня безпеки. Крім того, комутатор слід налаштувати для прийому лише зашифрованих сеансів SSH віддаленого управління.

Протокол DTP пропонує чотири режими порту комутатора: режим доступу, транковий, динамічний автоматичний і динамічний рекомендований. Згідно загальної рекомендації, автоузгодження слід відключити.

Нарешті, голосовий трафік обмежується жорсткими вимогами QoS. Якщо призначені для користувача комп’ютери і IP -телефони знаходяться в одній мережі VLAN, кожен намагається використовувати доступну смугу пропускання, не зважаючи на інші пристрої.

Щоб уникнути таких конфліктів, рекомендується використовувати окремі VLAN для IP - телефонії і трафіку даних.

Висновок до лекції 12

Мережі VLAN грунтуються не на фізичних, а на логічних підключеннях. Мережі VLAN – це механізм, що дозволяє мережевим адміністраторам створювати логічні широкомовні домени, які здатні охоплювати один або декілька комутаторів незалежно від фізичної відстані. Ця функція корисна для зменшення розміру широкомовних доменів або для об'єднання груп або користувачів, які не обов'язково повинні знаходитися в одному місці.

Існує декілька типів мереж VLAN:

- мережа VLAN за замовчуванням;
- управляюча VLAN;
- native VLAN;
- призначена/для користувача VLAN для даних;
- VLAN «чорної діри»;
- голосова мережа VLAN.

У комутаторі Cisco VLAN 1 є мережею Ethernet VLAN за замовчуванням, мережею native VLAN за замовчуванням і управляючою VLAN за замовчуванням. Для забезпечення безпеки мережі native VLAN і керівники VLAN мають бути переміщені в іншу, окрему VLAN, а невживані порти комутатора мають бути переміщені в мережу VLAN «чорної діри».

Команда switchport access vlan використовується для створення мережі VLAN на комутаторі. Наступний крок після створення мережі VLAN – призначення портів мережам VLAN. Команда show vlan brief показує призначення VLAN і тип приналежності для усіх портів комутатора. Кожній VLAN повинна відповідати унікальна IP -підмережа. Якщо порт призначений невірною VLAN, використовуйте команду switchport access vlan для коригування приналежності VLAN. Використовуйте команду show mac address - table для перевірки адрес, отриманих на окремому порту комутатора і призначених VLAN цьому порту. Порт комутатора може працювати портом доступу або транковим портом. Порти доступу служать для передачі трафіку від певної VLAN, призначеної конкретному порту. Транковий порт за замовчуванням належить усім VLAN. Таким чином, він передає трафік в усі мережі VLAN. Транкові канали VLAN спрощують взаємодію між комутаторами, передаючи трафік, пов'язаний з декількома VLAN. Тегування кадрів IEEE 802.1Q дозволяє розрізняти кадри Ethernet, пов'язані з певними VLAN у міру їх проходження по загальних транковим каналах. Для того, щоб включити транкові канали, використовуйте команду switchport mode trunk. Узгодження транкового каналу виконується протоколом динамічного створення транкового каналу (DTP), який діє тільки за принципом наскрізного підключення між пристроями мережі.

Питання для закріплення

1. Яке призначення і переваги віртуальних локальних мереж?
2. Які типи віртуальних локальних мереж ви знаєте?
3. Яка відмінність між портами доступу і транковими портами комутатора?
4. Для чого використовується тегування кадрів Ethernet?
5. Які діапазони VLAN на коммутаторах?
6. Назвіть етапи створення віртуальної локальної мережі.
7. Для чого використовується протокол DTP?
8. Які проблеми виникають при використанні VLAN?
9. Назвіть основні рекомендації по проектуванню VLAN.

Список рекомендованої літератури

1. CCNA R&S RSE Chapter 3: VLANs // Електронний ресурс. Режим доступу: https://static-course-assets.s3.amazonaws.com/RSE50ENU/module3/index.html#3.1.1.1
2. Dynamic Trunking Protocol // Електронний ресурс. Режим доступу: http://www.ciscopress.com/articles/article.asp?p=2181837&seqNum=8
3. VLAN hopping // Електронний ресурс. Режим доступу: https://en.wikipedia.org/wiki/VLAN_hopping

Лекція 13. Тема: «Технології маршрутизації. Маршрутизація VLAN»

План лекції

13.1. Призначення маршрутизації.
13.2. Основні функції маршрутизаторів.
13.3. Налаштування основних параметрів маршрутизатора.
13.4. Таблиця і записи маршрутизації.
13.5. Статичні та динамічні маршрути
13.6. Маршрутизація VLAN.

13.1. Призначення маршрутизації

Комутатори Ethernet функціонують на канальному рівні, тобто 2-му рівні, і використовуються для пересилання кадрів Ethernet між пристроями в межах однієї мережі. Проте коли IP -адреса джерела і призначення знаходяться в різних мережах, кадр Ethernet необхідно відправити на маршрутизатор.

Маршрутизатор використовується для підключення однієї мережі до іншої. Маршрутизатор відповідає за доставку пакетів в різні мережі. Пунктом призначення для IP - пакета може бути веб-сервер, розташований в іншій країні, або сервер електронної пошти в локальній мережі.

Маршрутизатор використовує свою таблицю маршрутизації, щоб знайти оптимальний шлях для пересилки пакетів. Саме маршрутизатори забезпечують своєчасну доставку цих пакетів. Ефективність передачі даних між мережами залежить від можливості маршрутизаторів пересилати пакети по найбільш оптимальному шляху.

Коли вузол відправляє пакет пристрою в іншу IP -мережу, цей пакет пересилається на шлюз за замовчуванням, оскільки вузол не може безпосередньо взаємодіяти з пристроями, розташованими поза локальною мережею. Пунктом призначення в маршрутах трафіку з локальної мережі до пристроїв у віддалених мережах є шлюз за замовчуванням. Цей шлюз часто використовується для підключення локальної мережі до Інтернету.

Розглянемо ключові структури і властивості, пов’язані з продуктивністю мережі.

- **Топологія:** існують фізичні і логічні топології. Фізична топологія – схема розташування кабелів, мережевих пристроїв і кінцевих систем. У ній описується, як мережеві пристрої сполучені між собою за допомогою дротів і кабелів. Логічна топологія – це шлях, по якому дані передаються по мережі. У ній описується, як користувачі бачать з’єднання мережевих пристроїв.
- **Швидкість** - це кількість переданих даних по якому-небудь каналу мережі, вимірюється у бітах в секунду (біт/с).
- **Вартість** вказує загальні витрати на придбання компонентів мережі, установку і обслуговування мережі.

- **Безпека** вказує на міру захищеності мережі, у тому числі захищеності інформації, що передається по мережі. Чинник безпеки грає дуже важливу роль, тому технології і методи забезпечення безпеки постійно розвиваються. При будь-яких діях, які можуть вплинути на роботу мережі, необхідно звертати увагу на забезпечення безпеки.
- **Доступність** вказує на можливість використання мережі у момент звернення користувача.
- **Масштабованість** показує, наскільки легко мережа може вміщати більше число користувачів і відповідати вимогам передачі даних. Якщо проект мережі оптимізований тільки для виконання поточних завдань, то розширення мережі для відповідності зростаючим вимогам несе за собою великі труднощі і високі витрати.
- **Надійність** вказує на міру безвідмовності компонентів, з яких складається мережа,: маршрутизаторів, комутаторів, комп'ютерів і серверів. Надійність часто вимірюється як вірогідність збою або як середній час безвідмовної роботи (MTBF, Mean time between failures).

13.2. Основні функції маршрутизаторів

По суті, маршрутизатор – це спеціалізований комп'ютер. Для його роботи потрібні ЦП і пам'ять, в якій зберігаються дані для виконання інструкцій ОС, наприклад, ініціалізації системи, функцій маршрутизації і комутації.

Маршрутизатори зберігають дані, використовуючи наступні типи запам'ятовуючих пристроїв:

- **Оперативний апам'ятовуючий пристрій (ОЗП)** - забезпечує тимчасове зберігання даних для різних застосувань і процесів, включаючи поточну IOS, файл поточної конфігурації, різні таблиці (наприклад, таблицю IP -маршрутизації, таблицю ARP Ethernet) і буфери для обробки пакету. ОЗП є енергозалежною, оскільки при виключенні живлення вона втрачає свій вміст.
- **Постійний запам'ятовуючий пристрій (ПЗП)** - забезпечує постійне зберігання інструкцій завантаження, базового діагностичного ПЗ і IOS з обмеженими можливостями, що використовується у випадку, якщо маршрутизатор не зможе завантажити повнофункціональну IOS. ПЗП є вбудованою пам'яттю, яку називають незалежною, оскільки при виключенні живлення вона не втрачає свій вміст.
- **Незалежне ОЗП (NVRAM)** - забезпечує постійне зберігання файлу завантажувальної конфігурації (startup - config). NVRAM – це незалежна пам'ять, яка не втрачає свій вміст при виключенні живлення.
- **Флеш-пам'ять** забезпечує постійне зберігання даних для IOS та інших системних файлів. Під час процесу завантаження файли IOS копіюються з флеш-пам'яті в ОЗП. Флеш-пам'ять є незалежною і не втрачає свій вміст при відключенні живлення.

На відміну від комп'ютера, маршрутизатори не мають відео- і звукових карт. Замість цього маршрутизатори оснащені спеціалізованими портами і мережевими платами для підключення пристроїв до інших мереж.

Більшість користувачів не знають про наявність багатьох маршрутизаторів у власній мережі або в Інтернеті. Користувачі хочуть відкривати веб-сторінки, відправляти повідомлення електронної пошти і завантажувати музику незалежно від того, у власній або в іншій мережі знаходиться сервер, до якого вони дістають доступ. Мережеві фахівці знають, що саме маршрутизатор забезпечує пересилку пакетів з мережі в мережу, від першоджерела до кінцевого призначення.

Маршрутизатор сполучає багато мереж, і це означає, що він оснащений безліччю інтерфейсів, кожен з яких належить іншій IP -мережі. Коли маршрутизатор отримує IP -пакет на одному інтерфейсі, він визначає, який інтерфейс слід використовувати для пересилки пакету до місця призначення.

Інтерфейс, який використовує маршрутизатор для пересилки пакету, може бути кінцевою точкою маршруту, або ж мережею, підключеною до іншого маршрутизатора, використовуваного для досягнення мережі призначення.

Як правило, кожна мережа, до якої підключається маршрутизатор, вимагає окремого інтерфейсу. Ці інтерфейси використовуються для з'єднання як локальних (LAN), так і глобальних мереж (WAN). В більшості випадків, LAN – це мережі Ethernet, такі пристрої, що містять, як ПК, принтери і сервери. WAN використовуються для з'єднання мереж на великих територіях. Наприклад, підключення до WAN зазвичай використовується для підключення LAN до мережі інтернет-провайдера (ISP).

Основні функції маршрутизаторів :

- визначення оптимального шляху для передачі пакетів;
- пересилка пакетів до пункту призначення.

Маршрутизатор використовує свою таблицю маршрутизації, щоб знайти оптимальний шлях для пересилки пакетів. Коли маршрутизатор отримує пакет, він перевіряє адресу призначення пакету і використовує таблицю маршрутизації для пошуку оптимального шляху до потрібної мережі. Крім того, в таблиці маршрутизації враховується, який інтерфейс слід використовувати для пересилки пакетів в кожну відому мережу.

Якщо оптимальний маршрут знайдений, маршрутизатор інкапсулює пакет в кадр каналу передачі даних витікаючого або вихідного інтерфейсу і пересилає пакет до пункту призначення.

Маршрутизатор може отримувати пакет, який інкапсульований в кадр каналу передачі даних одного типу, і відправити пакет з інтерфейсу, який використовує інший тип кадру каналу передачі даних. Наприклад, маршрутизатор може отримати пакет на інтерфейсі Ethernet, але повинен переслати пакет з інтерфейсу, налагодженого за допомогою протоколу «точка-точка» (PPP). Інкапсуляція каналу передачі даних залежить від типу інтерфейсу маршрутизатора і типу передавального середовища, до якого він підключений. Різні технології каналу передачі даних, до яких може підключитися маршрутизатор, включають Ethernet, PPP, Frame Relay, DSL, кабельні і безпровідні мережі (802.11, Bluetooth).

Для забезпечення мережевого доступу на пристроях мають бути налагоджені такі параметри IP:

- **IP** -адреса - визначає унікальний вузол в локальній мережі;
- **маска підмережі** - визначає, з якою підмережею мережі вузол може обмінюватися даними;
- **шлюз за замовчуванням** - визначає, на який маршрутизатор слід відправляти пакет, коли пристрій призначення знаходиться в іншій підмережі локальної мережі.

Коли вузол відправляє пакет пристрою, який знаходиться в тій же IP -мережі, пакет просто пересилається з інтерфейсу вузла на пристрій призначення.

Коли вузол відправляє пакет пристрою в іншу IP -мережу, то пакет пересилається на шлюз за замовчуванням, оскільки пристрій вузла не може взаємодіяти безпосередньо з пристроями поза локальною мережею. Пунктом призначення в маршрутах трафіку з локальної мережі до пристроїв у віддалених мережах являється шлюз за умовчанням. Цей шлюз часто використовується для підключення локальної мережі до Інтернету.

Зазвичай шлюз за замовчуванням – це адреса інтерфейсу маршрутизатора, підключеного до локальної мережі. Маршрутизатор вносить записи в таблицю маршрутизації для усіх підключених мереж, так само як і для віддалених мереж, і визначає оптимальний маршрут для досягнення цих пунктів призначення.

При проектуванні нової мережі або зіставленні існуючої мережі потрібне документування мережі. Як мінімум, документація повинна визначати:

- імена пристроїв;
- інтерфейси, використовувані в проекті;
- IP -адреси і маски підмереж;
- адреси шлюзів за замовчуванням.

Цю інформацію можна зібрати шляхом створення двох корисних мережевих документів :

- **Схема топології** забезпечує візуальну інформацію, яка вказує на фізичні з'єднання і логічну адресацію 3-го рівня. Часто створюється за допомогою такого ПЗ, як Microsoft Visio.
- **Таблиця адресації,** в якій зібрані імена пристроїв, інтерфейси, IPv4 -адреса, маски підмережі і адреси шлюзів за замовчуванням.

13.3. Налаштування основних параметрів маршрутизатора

Однією з істотних відмінностей між комутаторами і маршрутизаторами є підтримувані пристроями типи інтерфейсів. Наприклад, комутатори 2-го рівня підтримують локальні мережі, у зв'язку з чим вони оснащені декількома портами FastEthernet або Gigabit Ethernet.

Маршрутизатори підтримують локальні і глобальні мережі, і можуть забезпечувати з'єднання між різними типами мереж. Таким чином, вони підтримують багато типів інтерфейсів.

Наприклад, маршрутизатори сімейства Cisco G2 SR використовують один або два інтегровані інтерфейси Gigabit Ethernet і роз'єми для високошвидкісних інтерфейсних карт WAN (HWIC) для підтримки різних типів мережевих інтерфейсів, включаючи послідовний, DSL і кабельний інтерфейси.

Щоб забезпечити доступність інтерфейсу, його необхідно:

- **налаштувати з адресою і маскою підмережі у разі використання IPv4:** використовуйте команду конфігурації інтерфейсу ip address ip - address subnet - mask.
- **активувати:** за замовчуванням інтерфейси мереж LAN і WAN не активовані (shutdown). Для включення інтерфейсу використовуйте команду активації no shutdown (аналогічно забезпеченню живлення на інтерфейсі). Також інтерфейс необхідно підключити до іншого пристрою (комутатору або іншому маршрутизатору) для активації фізичного рівня.

При необхідності інтерфейс також можна налаштувати з коротким описом. Рекомендується настроювати опис на кожному інтерфейсі. Текст опису може містити не більше 240 символів. У виробничих мережах опис може згодитися при пошуку і усуненні неполадок, оскільки в нім описується тип мережі, до якої підключений інтерфейс. Якщо інтерфейс підключається до інтернет-провайдера або оператора послуги, то рекомендується заповнити опис і контактну інформацію про третю сторону.

Інтерфейс loopback – це логічний інтерфейс усередині маршрутизатора. Він не призначається фізичному порту, тому його не можна підключити до іншого пристрою. Він вважається програмним інтерфейсом, який автоматично переводиться в стан UP під час роботи маршрутизатора.

Застосування інтерфейсу loopback може бути доцільним при тестуванні і управлінні мережевим пристроєм, оскільки він забезпечує доступність хоч би одного інтерфейсу. Його можна використовувати в цілях тестування – наприклад, для тестування внутрішніх процесів маршрутизації, шляхом імітації мереж за межами маршрутизатора.

Крім того, IPv4 -адреса, призначена loopback -интерфейсу, може бути потрібна для процесів маршрутизатора, в яких використовується IPv4 -адреса інтерфейсу в цілях ідентифікації. Один з таких процесів – алгоритм найкоротшого шляху (OSPF). При включенні інтерфейсу loopback для ідентифікації маршрутизатор використовуватиме завжди доступну адресу інтерфейсу loopback, ніж IP -адресу, призначену фізичному порту, робота якого може бути порушена.

Включення інтерфейсу і призначення loopback -адрес виконується за допомогою простого набору команд :

```
Router(config)# interface loopback number
Router(config - if)# ip address ip - address subnet - mask
Router(config - if)# exit
```

На маршрутизаторі можна активувати декілька інтерфейсів loopback. IPv4 -адреса для кожного інтерфейсу loopback має бути унікальною і не має бути задіяна іншим інтерфейсом.

Для перевірки роботи конфігурації інтерфейсу можна використовувати декілька команд show. Для того, щоб швидко визначити стан інтерфейсу, рекомендується використовувати наступні три команди:

- **show ip interface brief** - відображує коротку інформацію про усі інтерфейси, включаючи IPv4 -адресу інтерфейсу і поточний робочий стан.
- **show ip route** - відображує вміст таблиці маршрутизації IPv4, яка зберігається в ОЗП. У Cisco IOS 15 активних інтерфейсів мають бути вказані в таблиці маршрутизації з двома пов'язаними з ними записами, які визначені кодом «C» (підключений) або «L» (локальний). У попередніх версіях IOS з'являється тільки запис з кодом «C».
- **show running** - config interfaceinterface-id – відображує команди, налагоджені на вказаному інтерфейсі.

Для отримання додаткової інформації про інтерфейс використовуються наступні дві команди:

- **show interfaces** - відображує інформацію про інтерфейс і лічильник потоку пакетів для усіх інтерфейсів на пристрої.
- **show ip interface** - відображує інформацію про IPv4 для усіх інтерфейсів маршрутизатора.

Команди для перевірки налаштувань IPv6 на інтерфейсі схожі з командами для перевірки налаштувань IPv4.

Команда ping для IPv6 ідентична команді для IPv4, за винятком того, що використовується IPv6 -адреса.

13.4. Таблиця і записи маршрутизації

Основна функція маршрутизатора полягає у визначенні оптимального шляху для відправки пакетів. Для визначення оптимального шляху маршрутизатор шукає у своїй таблиці маршрутизації мережеву адресу, відповідну IP -адресу місця призначення пакету.

Результати пошуку можуть вивести один з трьох видів шляхів.

- **Мережа з прямим підключенням** - якщо IP -адреса призначення пакету належить пристрою в мережі з прямим підключенням до одного з інтерфейсів маршрутизатора, то цей пакет пересилається безпосередньо у пристрій призначення. Це означає, що IP -адреса призначення пакету - це вузлова адреса в тій же підмережі, що й інтерфейс маршрутизатора.
- **Віддалена мережа** - якщо IP -адреса призначення пакету належить віддаленій мережі, пакет пересилається на інший маршрутизатор. Відправити пакет до віддалених мереж можна тільки за допомогою пересилки на інший маршрутизатор.
- **Маршрут не визначений** - якщо IP -адреса призначення пакету не належить підключеній або віддаленій мережі, маршрутизатору треба визначити, чи доступний «шлюз останньої надії». «Шлюз останньої надії» задається, коли на маршрутизаторі налагоджений маршрут за замовчуванням. Якщо є маршрут за замовчуванням, то пакет пересилається на «шлюз останньої надії». Якщо маршрутизатор не має в розпорядженні маршруту за замовчуванням, то пакет відкидається. Якщо пакет відкинутий, маршрутизатор відправляє на IP -адрес джерела пакету ICMP -повідомлення про недоступність порту.

Визначення оптимального шляху має на увазі оцінку декількох шляхів в одну і ту ж мережу призначення і вибір оптимального або найкоротшого шляху для проходження цього маршруту. Коли існує декілька шляхів до однієї мережі, кожен шлях використовує різний вихідний інтерфейс маршрутизатора для досягнення мережі.

Протокол маршрутизації вибирає найкращий шлях, виходячи зі значення або метрики для визначення відстані до мережі. Метрика – це числове значення для виміру відстані до заданої мережі. Найбільш оптимальним шляхом до мережі є шлях з найменшою метрикою.

Протоколи динамічної маршрутизації зазвичай використовують власні правила і метрики для побудови і оновлення таблиць маршрутизації. Алгоритм маршрутизації генерує значення (чи метрику) для кожного шляху через мережу. Метрики можуть грунтуватися на одній або декількох характеристиках шляху. Деякі протоколи маршрутизації вибирають маршрут на основі декількох метрик, об'єднуючи їх в одну метрику.

Далі приведений список динамічних протоколів і використовуваних ними метрик.

- **Протокол RIP** - кількість переходів.
- **Протокол OSPF** («алгоритм найкоротшого шляху») – метрика, заснована на сумарній смузі пропускання від джерела до місця призначення**.**
- **Протокол EIGRP** (вдосконалений протокол внутрішньої маршрутизації між шлюзами, EIGRP) - пропускна спроможність, затримка, навантаження і надійність.

Що відбувається, коли в таблиці маршрутизації містяться два або більше за шлях з ідентичними показниками алгоритмів досягнення однієї і тієї ж мережі призначення?

Якщо маршрутизатор розташовує двома або більше шляхами до пункту призначення з метриками рівної вартості, він відправляє пакети по обох шляхах. Це називається **розподілом навантаження відповідно до рівної вартості**. Таблиця маршрутизації містить одну мережу призначення, але декілька вихідних інтерфейсів – по одному для кожного шляху з рівною вартістю. Маршрутизатор пересилає пакети через декілька вихідних інтерфейсів, вказаних в таблиці маршрутизації.

При правильній конфігурації розподіл навантаження може підвищити ефективність і продуктивність мережі. Розподіл навантаження з рівною вартістю можна налаштувати на використання як динамічних протоколів маршрутизації, так і статичних маршрутів.

Примітка. Тільки протокол EIGRP підтримує розподіл навантаження з нерівною вартістю.

Маршрутизатор можна налаштувати, використовуючи декілька протоколів маршрутизації і статичних маршрутів. В цьому випадку таблиця маршрутизації може містити декілька джерел маршруту для однієї мережі призначення.

Наприклад, якщо на маршрутизаторі налагоджені протоколи RIP і EIGRP, обидва протоколи маршрутизації можуть отримати одну і ту ж мережу призначення. Проте, виходячи з метрики протоколу маршрутизації, кожен протокол маршрутизації може вибирати різні шляхи для досягнення місця призначення.

Протокол RIP вибирає шлях, виходячи з кількості переходів, а протокол EIGRP керується відомостями про його складену метрику. Яким чином маршрутизатор вирішує, який маршрут використовувати?

В ОС Cisco IOS для визначення маршруту і занесення його в таблицю IP -маршрутизації застосовується так звана **адміністративна відстань (AD)**. Адміністративна відстань представляє «надійність» маршруту; чим менше його значення, тим більше надійним є джерело маршруту. Наприклад, значення AD статичного маршруту рівне 1, а значення AD маршруту, розрахованого по протоколу EIGRP, складає 90.

Маючи два різні маршрути до одного і того ж місця призначення, маршрутизатор вибирає маршрут з найменшим значенням AD. За умови вибору між статичним маршрутом і маршрутом, розрахованим по EIGRP, вибирається статичний маршрут.

Аналогічно, маршрут до мережі з прямим підключенням з AD, рівним 0, «виграє» у статичного маршруту з AD, рівним 1. У табл. 13.1.приведені різні протоколи маршрутизації і відповідні ним значення AD.

Табл. 13.1. Адміністративна відстань за замовчуванням

Джерело маршруту	Адміністративна відстань
Прямий	0
Статична	1
Сумарний маршрут EIGRP	5
Зовнішній BGP	20
Внутрішній EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
Зовнішній EIGRP	170
Внутрішній BGP	200

Таблиця маршрутизації маршрутизатора зберігає наступну інформацію.

- **Маршрути з прямим підключенням** - це маршрути, що поступають з активних інтерфейсів маршрутизатора. Маршрутизатори додають маршрут з прямим підключенням, коли інтерфейс налагоджений з IP -адресою і активований.
- **Віддалені маршрути** - це віддалені мережі, підключені до інших маршрутизаторів. Маршрути до цих мереж можуть бути налагоджені статично або динамічно з використанням протоколів динамічної маршрутизації.

Зокрема, таблиця маршрутизації є файлом даних в ОЗП для зберігання інформації про мережі з прямим підключенням і віддалені мережі. Таблиця маршрутизації містить асоціації з мережами або наступними переходами. За допомогою цих асоціацій маршрутизатор дізнається про те, що досягти конкретного місця призначення можна за допомогою відправки пакету на певний маршрутизатор, який є наступним переходом на шляху до пункту призначення. Також асоціація з наступним переходом може бути витікаючим або вихідним інтерфейсом для наступного призначення.

На маршрутизаторі Cisco IOS команда show ip route може бути використана для відображення таблиці IPv4 -маршрутизації. Маршрутизатор надає додаткову інформацію про маршрут, включаючи спосіб отримання маршруту, тривалість перебування маршруту в таблиці, а також відомості про конкретний інтерфейс, який слід використовувати для досягнення необхідного призначення.

У таблицю маршрутизації можуть бути додані наступні види записів.

- **Інтерфейси локального маршруту** - додаються, коли інтерфейс налагоджений і активний. Цей запис відображується тільки в IOS 15 або пізніших версіях для IPv4 - маршрутів і в усіх версіях IOS для IPv6 -маршрутів.
- **Інтерфейси з прямим підключенням** - додаються в таблицю маршрутизації, коли інтерфейс налагоджений і активний.
- **Статичні маршрути** - додаються, коли маршрут налагоджений вручну і активний вихідний інтерфейс.
- **Протокол динамічної маршрутизації**- додається, коли визначені мережі і реалізуються протоколи маршрутизації, які отримують інформацію про мережу динамічно, наприклад EIGRP або OSPF.

Джерела записів таблиці маршрутизації ідентифікуються за допомогою коду. Код визначає, яким чином був отриманий маршрут. До прикладів поширених кодів відносяться:

- **L** - вказує адресу, призначена інтерфейсу маршрутизатора. Цей код дозволяє маршрутизатору швидко визначити, що отриманий пакет призначений для інтерфейсу, а не для пересилки.
- **C** - визначає мережу з прямим підключенням.
- **S** - визначає статичний маршрут, створений для досягнення конкретної мережі.
- **D** - визначає мережу, динамічно отриману від іншого маршрутизатора за допомогою протоколу EIGRP.
- **O** - визначає мережу, динамічно отриману від іншого маршрутизатора за допомогою протоколу маршрутизатора OSPF.

13.5. Статичні та динамічні маршрути

Після того, як інтерфейси з прямим підключенням налагоджені і додані в таблицю маршрутизації, можна приступити до реалізації статичної або динамічної маршрутизації.

Статичні маршрути настроюються вручну. Вони визначають точний маршрут між двома мережевими пристроями. На відміну від протоколу динамічної маршрутизації, статичні маршрути не оновлюються автоматично, і при змінах в мережевій топології їх треба настроювати вручну. До переваг використання статичних маршрутів відносяться високий рівень безпеки і ефективність витрачання ресурсів. Статичні маршрути використовують вужчу смугу пропускання, чим протоколи динамічної маршрутизації; для розрахунку і зв'язку маршрутів цикли ЦП не використовуються. Основний недолік використання статичних маршрутів полягає у відсутності автоматичного налаштування при змінах в мережевій топології.

У таблиці маршрутизації представлено два поширені типи статичних маршруті:

- статичні маршрути в конкретну мережу;
- статичні маршрути за замовчуванням.

Статичний маршрут можна налаштуватидля досягнення конкретної віддаленої мережі. Статичні маршрути IPv4 налагоджені за допомогою команди глобальної конфигурації ip route network mask {next - hop - ip |exit - intf}. Статичний маршрут визначається в таблиці маршрутизації за допомогою коду «S».

Статичний маршрут за замовчуванням мало чим відрізняється від шлюзу за замовчуванням на вузлі. Якщо таблиця маршрутизації не містить шлях в мережу призначення, статичний маршрут за замовчуванням визначає вихідну точку, яку слід використовувати.

Статичний маршрут за замовчуванням є доцільним, коли маршрутизатор має в розпорядженні тільки одну вихідну точку в інший маршрутизатор, наприклад, коли маршрутизатор підключається до центрального маршрутизатора або оператора зв'язку.

Для того, щоб налаштувати статичний IPv4 -маршрут за замовчуванням, використовується команда глобальної конфігурації ip route 0.0.0.0 0.0.0.0 {exit - intf | next - hop - ip}.

Щоб налаштувати статичний маршрут за замовчуванням для IPv6, використовується команда глобальної конфігурації ipv6 route ::/0 {ipv6 - address | interface - type interface - number}.

Протоколи динамічної маршрутизації дозволяють маршрутизаторам спільно використовувати відомості про надійність і стан віддалених мереж. Протоколи динамічної маршрутизації виконують ряд операцій, включаючи виявлення мереж і ведення таблиць маршрутизації.

Під виявленням мереж мається на увазі здатність протоколу маршрутизації обмінюватися інформацією про відомі мережі з іншими маршрутизаторами, що використовують той же протокол маршрутизації. Протокол динамічної маршрутизації не залежить від вручну налагоджених статичних маршрутів до віддалених мереж на кожному маршрутизаторі, але

дозволяє маршрутизаторам автоматично дізнаватися про ці мережі від інших маршрутизаторів. Ці мережі, а також найкращі шляхи, до кожної з них додаються в таблицю маршрутизації і вказуються в якості мереж, отриманих конкретним протоколом динамічної маршрутизації.

В процесі виявлення мережі маршрутизатори обмінюються маршрутами і оновлюють свої таблиці маршрутизації. Маршрутизатор, що функціонує по протоколу динамічної маршрутизації, не лише забезпечує визначення оптимального шляху до мережі, а також визначає новий оптимальний шлях, якщо початковий шлях не можна використовувати (чи у разі зміни топології). З цих причин протоколи динамічної маршрутизації мають перевагу перед статичними маршрутами. Маршрутизатори, що використовують протоколи динамічної маршрутизації, автоматично обмінюються інформацією про маршрутизацію з іншими маршрутизаторами і виконують оновлення у разі яких-небудь змін в топології без участі мережевого адміністратора.

Щоб визначити, які протоколи маршрутизації підтримує IOS, використовується команда режиму глобальної конфігурації router ?.

Підтримка динамічних протоколів маршрутизації IPv6 залежить від устаткування і версії IOS. Більшість змін в протоколах маршрутизації призначені для підтримки довших IPv6 – адрес та інших структур заголовків. Щоб дозволити маршрутизаторам IPv6 пересилати трафік, необхідно виконати команду режиму глобальної конфигурації ipv6 unicast - routing.

13.6. Маршрутизація VLAN

VLAN ділять мережу на сегменти, для передачі трафіку між сегментами потрібен процес 3-го рівня. Процес маршрутизації на 3-му рівні можна здійснювати за допомогою маршрутизатора або комутатора 3-го рівня. Використання пристрою 3-го рівня забезпечує можливість управління передачею трафіку між сегментами мережі, у тому числі сегментами, які були створені за допомогою VLAN.

Мережа VLAN – це домен широкомовної розсилки, тому комп’ютери в різних мережах VLAN не можуть обмінюватися даними без допомоги пристрою маршрутизації. Будь-який пристрій, що підтримує маршрутизацію 3-го рівня, наприклад, маршрутизатор або багаторівневий комутатор, можна використовувати для виконання основних функцій маршрутизації. Незалежно від використовуваного пристрою, процес пересилки мережевого трафіку з однієї VLAN в іншу з використанням маршрутизації називають маршрутизацією між VLAN.

На відміну від традиційного методу маршрутизації між VLAN, який задіює декілька фізичних інтерфейсів на маршрутизаторі і комутаторі, сучасніший метод маршрутизації між VLAN цього не вимагає. Замість цього на деяких маршрутизаторах ПЗ дозволяє настроювати інтерфейс маршрутизатора в якості транка. Це означає, що для маршрутизації пакетів між декількома VLAN на маршрутизаторі і комутаторі потрібен тільки один фізичний інтерфейс.

Метод «router - on - a - stick» - це такий тип конфігурації маршрутизатора, при якому один фізичний інтерфейс маршрутизує трафік між декількома VLAN. Інтерфейс маршрутизатора настроюється для роботи транковим каналом і підключається до порту комутатора, який налагоджений в режимі транка. Маршрутизатор виконує маршрутизацію між VLAN, приймаючи на транковому інтерфейсі трафік з міткою VLAN, що поступає від суміжного комутатора, і потім за допомогою підінтерфейсів маршрутизуючи його між VLAN. Потім вже змаршрутизований трафік посилається з цього ж фізичного інтерфейсу з міткою VLAN, відповідною VLAN призначення.

Підінтерфейси - це програмні віртуальні інтерфейси, пов’язані з одним фізичним інтерфейсом. Підінтерфейси налаштовуються в ПЗ маршрутизатора, і кожному підінтерфейсу призначаються IP -адреса і VLAN. Для полегшення логічної маршрутизації підінтерфейси настроюються для різних підмереж, що відповідають призначеним їм VLAN. Після ухвалення рішення про маршрутизацію на основі мережі призначення VLAN кадрам

даних привласнюються мітки VLAN, після чого вони вирушають назад на фізичний інтерфейс.

Реалізація маршрутизації між VLAN з використанням методу router - on - a - stick вимагає тільки одного фізичного інтерфейсу на маршрутизаторі і одного інтерфейсу на комутаторі, що спрощує проведення кабелів для маршрутизатора.

Багаторівневі комутатори можуть працювати як на 2-му, так і на 3-му рівні, завдяки чому для виконання базової маршрутизації не вимагається додатково задіювати маршрутизатори. Багаторівневі комутатори підтримують динамічну маршрутизацію і маршрутизацію між VLAN.

Щоб багаторівневий комутатор виконував функції маршрутизації, на нім треба включити функцію IP -маршрутизації.

Багаторівнева комутація масштабується краще, ніж будь-яка інша реалізація маршрутизації між VLAN. Це пов’язано з тим, що маршрутизатори оснащені обмеженою кількістю портів для підключення до мереж. Крім того, інтерфейс, налагоджений в якості транка, має обмежену пропускну спроможність.

При використанні багаторівневого комутатора трафік маршрутизується усередині комутатора, і його не потрібно передавати по одному транку туди і назад, щоб перенести з однієї VLAN в іншу. Проте багаторівневий комутатор не може виконувати усі функції маршрутизатора. Маршрутизатори підтримують багато додаткових функцій, наприклад, дозволяють реалізовувати більше можливостей для забезпечення безпеки.

На перших порах розвитку комутаційних мереж комутація була швидкою (часто не відставала від швидкості роботи апаратного устаткування, тобто швидкість співпадала з часом, яке було потрібне для отримання і пересилки кадрів в інші порти), а маршрутизація була повільною (маршрутизації була реалізована програмно). Тому проектувальники мереж намагалися зробити максимально великою комутовану частину мережі. Рівні доступу, розподілу і ядра часто настроювалися для обміну даними на 2-му рівні. Це створювало проблеми з виникненням циклів. Для вирішення цієї проблеми і запобігання циклам використовувався протокол STP, що дозволяло зберегти гнучкість і можливість додавання резервних з’єднань між комутаторами.

Проте з розвитком мережевих технологій маршрутизація стала швидша і дешевша. Сьогодні маршрутизація здійснюється на швидкості апаратного забезпечення. Наслідком подібної еволюції стала можливість переходу маршрутизації на рівні ядра і розподілу без негативної дії на продуктивність мережі.

Багато користувачів знаходяться в окремих VLAN, а кожна мережа VLAN, як правило, є окремою підмережею. У зв’язку з цим, логічно настроювати комутатори розподілу в якості шлюзів 3-го рівня для користувачів кожної VLAN на комутаторі доступу. Це означає, що кожен комутатор розподілу повинен містити IP -адреси, що відповідають кожній мережі VLAN на комутаторі доступу.

Між рівнями ядра і розподілу, як правило, використовуються порти 3-го рівня (що маршрутизуються).

Ця мережева архітектура не залежить від роботи STP, оскільки у тієї частини топології, яка використовує 2-й рівень, немає фізичних петель.

Нижче наводиться декілька причин необхідності налаштування інтерфейсу SVI.

- Забезпечення шлюзу для мережі VLAN з метою маршрутизації трафіку у напрямку до або з цієї VLAN.
- Забезпечення на комутаторі IP – з’єднання 3-го рівня.
- Підтримка конфігурацій протоколу маршрутизації і режиму моста.

Далі приведені деякі з переваг інтерфейсів SVI (єдиний недолік полягає у високій вартості багаторівневих комутаторів).

- Цей вид маршрутизації набагато швидший за маршрутизацію з використанням методу router - on - a - stick, оскільки процеси комутації і маршрутизації здійснюються на базі апаратних засобів.

- Для маршрутизації не потрібні зовнішні канали від комутатора до маршрутизатора.
- Немає обмеження в один канал. Для підвищення пропускної спроможності між комутаторами можна використовувати канали EtherChannel 2-го рівня.
- Затримки набагато менше, оскільки трафік обробляється усередині комутатора.

Висновок до лекції 13

Маршрутизатор використовується для підключення однієї мережі до іншої. Маршрутизатор відповідає за доставку пакетів в різні мережі. Пунктом призначення для IP - пакета може бути веб-сервер, розташований в іншій країні, або сервер електронної пошти в локальній мережі.

Маршрутизатор використовує свою таблицю маршрутизації, щоб знайти оптимальний шлях для пересилки пакетів. Саме маршрутизатори забезпечують своєчасну доставку цих пакетів. Ефективність передачі даних між мережами залежить від можливості маршрутизаторів пересилати пакети по найбільш оптимальному шляху.

Маршрутизація між VLAN – це процес маршрутизації трафіку між мережами VLAN з використанням виділеного маршрутизатора або багаторівневого комутатора. Маршрутизація між VLAN спрощує обмін даними між пристроями, ізольованими межами VLAN.

Застарілий метод маршрутизації між VLAN обумовлений доступністю фізичного порту комутатора для кожної налагодженою VLAN. Цей метод був замінений на топологію router - on - a - stick, яка покладається на зовнішній маршрутизатор з підінтерфейсами, підключеними через транкові канали до комутатора 2-го рівня.

При використанні методу router - on - a - stick на кожному логічному підінтерфейсі необхідно налаштувати відповідні IP -адреси і параметри VLAN.

Питання для закріплення

1. Яке призначення маршрутизації?
2. Що таке адміністративна відстань та метрика мережі?
3. Які основні функції маршрутизаторів?
4. Які основні налаштування основних параметрів маршрутизатора?
5. Яке призначення таблиці маршрутизації?
6. Чим відрізняються статична та динамічна маршрутизація?
7. Як відбувається маршрутизація мереж VLAN?

Список рекомендованої літератури

1. CCNA R&S RSE Chapter 4: Routing Concept // Електронний ресурс. Режим доступу: https://static-course-assets.s3.amazonaws.com/RSE50ENU/module4/index.html
2. Маршрутизація: мета, основні задачі й протоколи // Електронний ресурс. Режим доступу: http://www.znanius.com/3820.html
3. Принцип роботи маршрутизатора // Електронний ресурс. Режим доступу: http://wiki.kspu.kr.ua/index.php

Лекція 14. Тема: «Статична та динамічна маршрутизація»

План лекції

14.1. Переваги та призначення статичної маршрутизації.
14.2. Налаштування статичного маршруту.
14.3. Статичний маршрут за замовчуванням.
14.4. Призначення та роль протоколів динамічної маршрутизації.
14.5. Принцип роботи протоколів динамічної маршрутизації.
14.6. Класифікація протоколів маршрутизації.
14.7. Дистанційно-векторні протоколи маршрутизації.
14.8. Протоколи маршрутизації за станом каналу.

14.1. Переваги та призначення статичної маршрутизації

Маршрутизація здійснює передачу даних шляхом перенесення інформації через об'єднану мережу від джерела до одержувача. Маршрутизатори є пристроями, що відповідають за передачу пакетів з однієї мережі в іншу.

Маршрутизатори отримують дані про віддалені мережі динамічно за допомогою протоколів маршрутизації або вручну – за допомогою статичних маршрутів. У багатьох випадках маршрутизатори одночасно використовують протоколи динамічної маршрутизації і статичні маршрути. Статичні маршрути дуже поширені, при цьому вони не вимагають такої ж кількості обчислень і операцій, як протоколи динамічної маршрутизації.

Маршрутизатор може дізнатися про віддалені мережі одним з двох способів:

- **вручну** - віддалені мережі вручну вводяться в таблицю маршрутизації за допомогою статичних маршрутів;
- **динамічно** - віддалені маршрути автоматично додаються за допомогою протоколу динамічної маршрутизації.

Мережевий адміністратор може вручну налаштувати статичний маршрут для доступу до конкретної мережі. На відміну від протоколу динамічної маршрутизації, статичні маршрути не оновлюються автоматично, і при змінах в мережевій топології їх необхідно повторно настроювати вручну. Статичні маршрути не змінюються до тих пір, поки адміністратор не перенастроюватиме їх вручну.

Розглянемо **переваги статичної маршрутизації** в порівнянні з динамічною маршрутизацією.

- Статичні маршрути не оголошуються по мережі, таким чином, вони безпечніші.
- Статичні маршрути використовують вужчу смугу пропускання, ніж протоколи динамічної маршрутизації. Крім того, для розрахунку і зв'язку маршрутів не використовуються ресурси ЦП.
- Шлях, використовуваний статичним маршрутом для відправки даних, відомий.

У статичної маршрутизації також є **недоліки:**

- Початкове налаштування і подальше обслуговування вимагають часових витрат.
- При налаштуванні часто допускаються помилки, особливо у великих мережах.
- Для внесення змін в дані маршруту потрібно втручання адміністратора.
- Недостатні можливості масштабування для зростаючих мереж, обслуговування при цьому стає досить трудомістким.
- Для якісного впровадження потрібно доскональне знання усієї мережі.

Статичні маршрути рекомендується використовувати в невеликих мережах, для яких заданий тільки один шлях до зовнішньої мережі. Вони також забезпечують безпеку у великих мережах з певним типом трафіку або в каналах до інших мереж, для яких потрібні розширені функції контролю. Важливо розуміти, що статична і динамічна маршрутизація не є взаємовиключними. У більшості мереж використовується комбінація протоколів динамічної маршрутизації і статичних маршрутів. Це може привести до того, що для

маршрутизатора задається декілька шляхів до мережі призначення за допомогою статичних маршрутів і динамічно отримуваних маршрутів. Проте адміністративна відстань (AD) статичного маршруту дорівнює 1. Тому статичний маршрут має пріоритет в порівнянні з усіма динамічно отримуваними маршрутами.

Статична маршрутизація має три основні призначення:

- Забезпечення спрощеного обслуговування таблиці маршрутизації в невеликих мережах, які не планується істотно розширювати.
- Маршрутизація до тупикових мереж і від них. **Тупикова мережа** є мережею, доступ до якої здійснюється через один маршрут, і маршрутизатор має тільки один сусідній пристрій.
- Використання маршруту за замовчуванням для представлення шляху до будь-якої мережі, точнішого збігу, що не має, з іншим маршрутом в таблиці маршрутизації. Маршрути за замовчуванням використовуються для відправки трафіку в будь-який пункт призначення за межами наступного маршрутизатора у висхідному напрямі.

Статичний маршрут за замовчуванням – це маршрут, якому відповідають усі пакети. Маршрут за замовчуванням ідентифікує IP -адресу шлюзу, на який маршрутизатор відправляє усі IP -пакети, для яких у нього немає відомого отриманого або статичного маршруту.

Статичний маршрут за замовчуванням – це статичний маршрут з IPv4 -адресою призначення рівною 0.0.0.0/0. При налаштуванні статичного маршруту за замовчуванням створюється «шлюз останньої надії».

Примітка. Усі маршрути, що визначають конкретне місце призначення з великим значенням маски підмережі, мають пріоритет в порівнянні з маршрутом за замовчуванням.

Статичні маршрути за замовчуванням використовуються в наступних випадках.

- За відсутності інших маршрутів в таблиці маршрутизації, що співпадають з IP -адресою призначення пакету – іншими словами, за відсутності точнішого збігу. Статичні маршрути часто використовуються при підключенні пограничного маршрутизатора компанії до мережі інтернет-провайдера.
- Якщо маршрутизатор підключений тільки до одного маршрутизатора. У такому разі використовується термін «тупиковий маршрутизатор».

Для зменшення числа записів в таблиці маршрутизації можна об’єднати декілька статичних маршрутів в один статичний маршрут. Це можливо за наступних умов:

- мережі призначення є суміжними і можуть бути об’єднані в одну мережеву адресу;
- усі статичні маршрути використовують один і той же вихідний інтерфейс або одну IP -адресу наступного переходу.

Ще одним типом статичного маршруту є плаваючий статичний маршрут. Плаваючі статичні маршрути – це статичні маршрути для надання резервного шляху основному статичному або динамічному маршруту на випадок збою в роботі каналу. Плаваючий статичний маршрут використовується тільки тоді, коли основний маршрут недоступний.

Для цієї мети плаваючий статичний маршрут настроюється з вищим значенням адміністративної відстані, чим основний маршрут. Слід пам’ятати, що адміністративна відстань вказує на надійність маршруту. За наявності декількох шляхів до адреси призначення маршрутизатор вибирає шлях з найнижчим значенням адміністративної відстані.

14.2. Налаштування статичного маршруту

Статичні маршрути настроюються за допомогою команди глобальної конфигурації ip route. Синтаксис команди :

Router(config)# ip route network - address subnet - mask { ip - address |interface - type interface - number [ip - address]} [distance] [namename] [permanent] [tag tag]

Для налаштування статичної маршрутизації обов’язково вказуються наступні параметри:

- network - address – адреса віддаленої мережі призначення, який необхідно додати в таблицю маршрутизації; цей параметр часто називають префіксом.
- subnet - mask – маска підмережі або просто маска віддаленої мережі, яку необхідно додати в таблицю маршрутизації. Маску підмережі можна змінити для об'єднання групи мереж.

Необхідно також використовувати один або обидва наступні параметри:

- ip - address – IP -адреса маршрутизатора, що підключається, використовується для пересилки пакетів у віддалену мережу призначення. Таку IP -адресу найчастіше називають **наступним переходом** або наступним вузлом.
- exit - intf – витікаючий інтерфейс, який використовується для передачі пакету на наступний перехід.

Найчастіше використовується наступний синтаксис команди : ip route network - address subnet - mask{ip - address | exit - intf}.

Параметр distance використовується для створення плаваючого статичного маршруту шляхом налаштування значення адміністративної відстані, що перевищує значення адміністративної відстані маршруту, що отримується динамічно.

Наступний перехід можна визначити за допомогою IP -адреси або вихідного інтерфейсу, а також обох параметрів відразу. Залежно від того, як вказано місце призначення, створюється один з трьох можливих типів маршруту.

- **Маршрут наступного переходу -** вказується тільки IP -адреса наступного переходу.
- **Безпосередньо підключений статичний маршрут –** вказується тільки вихідний інтерфейс маршрутизатора.
- **Повністю заданий статичний маршрут -** вказуються IP -адреса наступного переходу і вихідний інтерфейс.

У статичному маршруті наступного переходу вказується тільки IP -адреса наступного переходу. Вихідний інтерфейс визначається виходячи з наступного переходу.

Перед пересилкою маршрутизатором будь-якого пакету за допомогою таблиці маршрутизації визначається вихідний інтерфейс, який використовуватиметься для пересилки пакету.

Рекурсивний статичний маршрут є допустимим (тобто може бути доданий в таблицю маршрутизації), тільки якщо вказаний наступний перехід безпосередньо або побічно пов'язаний з допустимим вихідним інтерфейсом.

При налаштуванні статичного маршруту також можна використовувати вихідний інтерфейс для налаштування адреси наступного переходу.

Налаштування безпосередньо підключеного статичного маршруту з вихідним інтерфейсом дозволяє таблиці маршрутизації перетворити вихідний інтерфейс в ході одного процесу пошуку замість двох. Хоча запис в таблиці маршрутизації вказує на «пряме підключення», адміністративна відстань статичного маршруту як і раніше дорівнює 1. Тільки безпосередньо підключений інтерфейс може мати адміністративну відстань, рівну 0.

Примітка. Для інтерфейсів типу «точка-точка» можна використовувати статичні маршрути, що вказують на вихідний інтерфейс або адресу наступного переходу. Для багатоточкових або широкомовних інтерфейсів рекомендується використовувати статичні маршрути, що вказують на адресу наступного переходу.

У повністю заданому статичному маршруті вказуються і вихідний інтерфейс, і IP -адреса наступного переходу. Такий тип статичного маршруту використовується тоді, коли вихідний інтерфейс є інтерфейсом, підключеним до мережі з множинним доступом і є необхідність явно визначити наступний перехід. Наступний перехід має бути безпосередньо сполучений з вказаним вихідним інтерфейсом.

Припустимо, що канал мережі між маршрутизаторами R1 і R2 є каналом Ethernet і що інтерфейс GigabitEthernet 0/1 маршрутизатора R1 підключений до цієї мережі. Щоб виключити рекурсивний пошук, можна реалізувати безпосередньо підключений статичний маршрут, використовуючи наступну команду:

R1(config)# ip route 192.168.2.0 255.255.255.0 GigabitEthernet 0/1

Проте подібні дії можуть привести до непередбачених або суперечливих результатів. Відмінність між мережею Ethernet з множинним доступом і послідовною мережею типу «точка-точка» полягає в тому, що мережу «точка-точка» містить тільки один пристрій - маршрутизатор на іншому кінці каналу. Мережі Ethernet можуть містити багато різних пристроїв, що використовують одну мережу з множинним доступом, включаючи вузли і навіть декілька маршрутизаторів. Якщо вихідний інтерфейс Ethernet просто позначений в статичному маршруті, у маршрутизатора недостатньо даних, щоб визначити, який пристрій є пристроєм наступного переходу.

Можливість функціонування статичного маршруту визначається топологією і налаштуваннями на інших маршрутизаторах. Повністю заданий статичний маршрут рекомендується використовувати у разі, якщо вихідний інтерфейс є мережею Ethernet.

Разом з командами відправки эхо-запроса і трасування маршруту - ping itraceroute - існують інші корисні команди для перевірки статичних маршрутів :

- **show ip route**
- **show ip route static**
- **show ip route network.**

14.3. Статичний маршрут за замовчуванням

Статичний маршрут за замовчуванням – це маршрут, якому відповідають усі пакети. Замість зберігання усіх маршрутів до усіх мереж в таблиці маршрутизації маршрутизатор може зберігати один маршрут за замовчуванням, що представляє будь-яку мережу, відсутню в таблиці маршрутизації.

Маршрутизатори зазвичай використовують маршрути за замовчуванням, налагоджені локально або отримані від іншого маршрутизатора, за допомогою протоколу динамічної маршрутизації. Маршрут за замовчуванням використовується, якщо жоден з маршрутів в таблиці маршрутизації не співпадає з IP -адресою місця призначення пакету. Іншими словами, за відсутності точніших збігів в якості «шлюзу останньої надії» використовується маршрут за замовчуванням.

Статичні маршрути за замовчуванням зазвичай використовуються при підключенні:

- пограничного маршрутизатора до мережі інтернет-провайдера або
- тупикового маршрутизатора (маршрутизатора тільки з одним сусіднім маршрутизатором у висхідному напрямі).

Синтаксис команди для статичного маршруту за замовчуванням аналогічний синтаксису команди для будь-якого іншого статичного маршруту за винятком того, що адреса мережі вказується як 0.0.0.0, а маска підмережі – 0.0.0.0. Синтаксис основної команди статичного маршрутизатора за замовчуванням наступний:

ip route 0.0.0.0 0.0.0.0 { ip - address | exit - intf }

Ключем для цієї конфігурації виступає маска /0. Слід пам’ятати про те, що маска підмережі в таблиці маршрутизації визначає число бітів, які повинні співпасти між IP - адресою призначення пакету і маршрутом в таблиці маршрутизації. Двійкове значення 1 говорить про те, що потрібен збіг бітів. Двійкове значення 0 вказує, що збіг бітів не потрібно. Маска /0 в цьому записі маршруту вказує на те, що не потрібно збіг жодного з бітів. Статичний маршрут за замовчуванням зіставляє усі пакети, для яких не існує точнішого збігу.

Статичні маршрути для протоколу IPv6 налаштовуються за допомогою команди глобальної конфігурації ipv6 route:

Router(config)# ipv6 route ipv6 - prefix/prefix - length { ipv6 - address| exit - intf }

Більшість параметрів ідентичні параметрам команди для IPv4. Статичні маршрути IPv6 можна реалізувати як:

- стандартний статичний маршрут IPv6;

- статичний маршрут IPv6 за замовчуванням;
- сумарний статичний маршрут IPv6;
- плаваючий статичний маршрут IPv6.

Як і у випадку з IPv4, ці маршрути можна налаштувати як рекурсивні, підключені безпосередньо або повністю задані маршрути.

Для того, щоб маршрутизатор міг здійснювати пересилку пакетів для IPv6, необхідно налаштувати команду глобальної конфігурації ipv6 unicast - routing.

14.4. Призначення та роль протоколів динамічної маршрутизації

У великій мережі, що складається з декількох мереж і підмереж, налаштування і обслуговування статичних маршрутів між цими мережами вимагає частого адміністративного втручання і значних непродуктивних витрат. Непродуктивні витрати особливо зростають при необхідності внесення змін в мережу, наприклад, при збої в роботі каналу або реалізації нової підмережі. Використання протоколів динамічної маршрутизації може зменшити об'єм завдань з налаштування і обслуговування та забезпечити велику масштабованість мережі.

Протоколи динамічної маршрутизації використовуються в мережах з кінця 80-х рр. XX ст. Одним з перших протоколів маршрутизації був протокол маршрутної інформації (RIP). Перша версія протоколу RIP (RIPv1) була випущена в 1988 р., проте окремі базові алгоритми протоколу використовувалися ще в мережі ARPANET, створеній Агентством Міністерства оборони США по перспективних дослідженнях в 1969 р.

Разом з розвитком і ускладненням мереж, виникла необхідність в нових протоколах маршрутизації. Таким чином з'явилася оновлена версія протоколу маршрутизації RIP – RIPv2. Проте навіть оновлена версія RIP не надає можливостей масштабування при реалізації сучасних мереж більшого розміру. Відповідно до вимог мереж більшого розміру були розроблені два вдосконалені протоколи маршрутизації: протокол маршрутизації «алгоритм найкоротшого шляху» (OSPF) і протокол маршрутизації IS - IS. Компанія Cisco розробила внутрішній протокол маршрутизації шлюзів (IGRP) і вдосконалений протокол IGRP (EIGRP), які також забезпечують хорошу масштабованість при реалізації мереж більшого розміру.

Окрім перерахованих вимог, виникла необхідність в з'єднанні різних мереж і здійсненні маршрутизації між ними. Нині для зв'язку між мережами інтернет-провайдерів використовується протокол BGP. Протокол BGP також забезпечує обмін даними маршрутизації між інтернет-провайдерами і їх великими приватними клієнтами.

Протоколи маршрутизації спрощують обмін інформацією про маршрути між маршрутизаторами. Протокол маршрутизації є набором алгоритмів і повідомлень для обміну даними маршрутизації і наповнення таблиці маршрутизації оптимальними шляхами. Протоколи динамічної маршрутизації використовуються для вирішення наступних завдань:

- виявлення віддалених мереж;
- оновлення даних маршрутизації;
- вибір оптимального шляху до мереж призначення;
- пошук нового оптимального шляху у разі, якщо поточний шлях недоступний.

Протоколи динамічної маршрутизації включають наступні компоненти.

- **Структури даних** - як правило, для роботи протоколів маршрутизації використовуються таблиці або бази даних. Ця інформація зберігається в ОЗП.
- **Повідомлення протоколу маршрутизацію –** протоколи маршрутизації використовують різні типи повідомлень для виявлення сусідніх маршрутизаторів, обміну інформацією про маршрути і виконання інших завдань, пов'язаних з отриманням актуальної інформації про мережу.
- **Алгоритм.** Протоколи маршрутизації використовують алгоритми, що спрощують обмін даних маршрутизації і визначення оптимального шляху.

Протоколи маршрутизації дозволяють маршрутизаторам динамічно обмінюватися даними про видалені мережі і автоматично додавати ці дані у власні таблиці маршрутизації.

Протоколи маршрутизації визначають оптимальний шлях або маршрут до кожної мережі. Потім маршрут додається в таблицю маршрутизації. Основною перевагою протоколів динамічної маршрутизації є те, що вони забезпечують обмін даними маршрутизації між маршрутизаторами у випадках змін в топології. Подібний обмін даними дозволяє маршрутизаторам автоматично отримувати інформацію про нові мережі, а також знаходити альтернативні шляхи у разі збою каналу до поточної мережі.

В порівнянні із статичною маршрутизацією протоколи динамічної маршрутизації вимагають меншого втручання з боку адміністратора. Проте, до витрат використання протоколів динамічної маршрутизації можна віднести той факт, що частина ресурсів маршрутизатора виділяється для роботи протоколу (включаючи час ЦП і смугу пропускання мережевого каналу). Незважаючи на переваги динамічної маршрутизації, статична маршрутизація як і раніше знаходить застосування. В окремих випадках рекомендується використовувати саме статичну маршрутизацію, так само як і в інших прийнятніше вибрати динамічну маршрутизацію. Для мереж середнього рівня можна налаштувати як статичну, так і динамічну маршрутизацію.

Протоколи динамічної маршрутизації ідеально підходять для мереж будь-якого типу, що містять декілька маршрутизаторів. Протоколи забезпечують високий рівень масштабованості, а також автоматично визначають оптимальні маршрути при змінах в топології. Не дивлячись на те, що налаштування протоколів динамічної маршрутизації вимагає більше часових витрат, їх простіше налаштовувати у рамках великої мережі.

Для реалізації динамічної маршрутизації потрібні знання додаткових команд. Порівняно із статичною маршрутизацією динамічна маршрутизація демонструє нижчий рівень безпеки, оскільки інтерфейси, визначені протоколом маршрутизації, виконують відправку повідомлень про оновлення маршрутів. Маршрути можуть відрізнятися залежно від пакетів. Алгоритм маршрутизації використовує додаткові ресурси ЦП, ОЗП і смуги пропускання каналу.

14.5. Принцип роботи протоколів динамічної маршрутизації

Усі протоколи маршрутизації розроблені для отримання даних про віддалені мережі і швидку адаптацію до будь-яких змін в топології.

В цілому, роботу протоколу динамічної маршрутизації можна описати таким чином.

1. Маршрутизатор відправляє і приймає повідомлення маршрутизації на свої інтерфейси.
2. Маршрутизатор надає загальний доступ до повідомлень маршрутизації і даних про маршрути для інших маршрутизаторів, що використовують той же протокол маршрутизації.
3. Маршрутизатори здійснюють обмін даними маршрутизації для отримання інформації про видалені мережі.
4. При виявленні маршрутизатором змін в топології, протокол маршрутизації може оголосити цю зміну для інших маршрутизаторів.

Усі протоколи маршрутизації працюють за однією схемою.

При включенні живлення у маршрутизатора немає даних про топологію мережі. Крім того, у нього немає даних про наявність пристроїв на іншому кінці каналів. Маршрутизатору доступна лише інформація з його власного файлу конфігурації, збереженого в незалежному ОЗП (NVRAM). Після успішного завантаження маршрутизатор застосовує збережену конфігурацію. Якщо IP -адресація налагоджена вірно, спочатку маршрутизатор виконує виявлення безпосередньо підключених мереж.

Після початкового завантаження і виявлення джерел маршрутів, виконується оновлення таблиці маршрутизації з додаванням усіх безпосередньо підключених мереж та інтерфейсів, на яких розміщені ці мережі.

Якщо налагоджений протокол маршрутизації, на наступному етапі маршрутизатор починає обмін даними про коригування маршрутів для отримання інформації про усі віддалені маршрути.

Маршрутизатор відправляє пакет оновлення з усіх включених на ньому інтерфейсів. Оновлення містить дані з таблиці маршрутизації, в якій на даний момент є дані про безпосередньо підключені мережі.

В той же час маршрутизатор приймає і обробляє аналогічні пакети оновлень від інших підключених маршрутизаторів. Після отримання оновлення маршрутизатор перевіряє пакет на наявність даних про нові мережі. Він додає усі мережі, не прописані в таблиці маршрутизації.

На цьому етапі у маршрутизаторів є дані про власні безпосередньо підключені мережі, а також про підключені мережі найближчих до них сусідніх пристроїв. Продовжуючи процес збіжності, маршрутизатори виконують обмін періодичними оновленнями. Кожен з маршрутизаторів ще раз перевіряє оновлення на предмет наявності нових даних.

Дистанційно-векторні протоколи, як правило, запобігають появі петлі маршрутизації за допомогою методу розподілу горизонту. Метод розподілу горизонту забороняє відправку даних з того ж інтерфейсу, від якого вони були отримані. Наприклад, маршрутизатор R2 не відправляє оновлення, що містить мережу 10.1.0.0, з інтерфейсу Serial 0/0/0, оскільки маршрутизатор R2 отримав дані про мережу 10.1.0.0 через інтерфейс Serial 0/0/0.

Після завершення процесу збіжності маршрутизаторів в мережі, маршрутизатор може використовувати дані з таблиці маршрутизації для визначення оптимального шляху до адреси призначення. Різні протоколи маршрутизації використовують різні способи розрахунку оптимального шляху.

Збіжність мережі вважається досягнутою, коли усі маршрутизатори отримали повні і точні дані про усю мережу. **Час збіжності** – час, потрібний маршрутизатору для обміну даними, розрахунку оптимальних шляхів і оновлення таблиць маршрутизації. Мережа не являється повністю робочою до моменту повної збіжності. Таким чином, для більшості мереж має важливе значення час збіжності. Збіжність має на увазі як спільну, так і самостійну роботу пристроїв. Маршрутизатори обмінюються даними один з одним, проте вони повинні самостійно визначати вплив змін в топології на власні маршрути. Оскільки маршрутизатори реагують на зміни в топології незалежно один від одного, цей процес називають **збіжністю.**

До властивостей збіжності відносяться швидкість поширення даних маршрутизації і розрахунок оптимальних шляхів. Швидкість поширення співвідноситься з часом, необхідним для відправки інформації про маршрутизацію від маршрутизаторів усередині мережі.

Протоколи маршрутизації можна оцінювати за швидкістю збіжності - чим швидше виконується збіжність, тим більш ефективним є протокол маршрутизації. Як правило, більш ранні версії протоколів, наприклад, протокол RIP, відрізняються низькою швидкістю збіжності, тоді як сучасні протоколи, наприклад, EIGRP і OSPF, забезпечують швидшу збіжність.

14.6. Класифікація протоколів маршрутизації

Протоколи маршрутизації можна класифікувати за різними групами відповідно до їх характеристик. Зокрема, протоколи маршрутизації можна класифікувати за наступними ознаками:

- **Призначення -** протокол внутрішньої маршрутизації (IGP) або протокол зовнішньої маршрутизації (EGP)
- **Принцип роботи -** дистанційно-векторний протокол, за станом каналу або векторів маршрутів
- **Поведінка -** протоколи класової маршрутизації (застарілий метод) або безкласової маршрутизації

Наприклад, протоколи маршрутизації IPv4 можна класифікувати таким чином:

- **RIPv1 (застарілий)** - дистанційно-векторний класовий протокол внутрішньої маршрутизації;
- **IGRP (застарілий)** - дистанційно-векторний класовий протокол внутрішньої маршрутизації, розроблений компанією Cisco (не використовується після виходу IOS 12.2 і пізніших версій);
- **RIPv2** - дистанційно-векторний безкласовий протокол внутрішньої маршрутизації;
- **EIGRP** - дистанційно-векторний безкласовий протокол внутрішньої маршрутизації, розроблений компанією Cisco;
- **OSPF** - безкласовий протокол внутрішньої маршрутизації, за станом каналу;
- **IS - IS** - безкласовий протокол внутрішньої маршрутизації, за станом каналу;
- **BGP** - безкласовий протокол зовнішньої маршрутизації, по вектору маршруту.

Автономна система (AS) є системою маршрутизаторів, що управляються одним оператором, наприклад компанією або організацією. Автономну систему також називають **доменом маршрутизації**. До стандартних прикладів автономної системи можна віднести внутрішню мережу компанії та мережу інтернет-провайдера.

Мережа Інтернет заснована на концепції автономної системи, у зв'язку з чим вона вимагає використання протоколів маршрутизації двох типів.

1.Протоколи внутрішньої маршрутизації для маршрутизації усередині автономної системи. Цей тип маршрутизації також називають внутрішньою маршрутизацією автономної системи. Компанії, організації і навіть оператори зв'язку використовують протоколи внутрішньої маршрутизації у своїх внутрішніх мережах. До протоколів внутрішньої маршрутизації відносяться протоколи RIP, EIGRP, OSPF і IS - IS.

2.Протоколи зовнішньої маршрутизації для маршрутизації між автономними системами. Маршрутизацію цього типу також називають зовнішньою маршрутизацією автономної системи. Взаємодія між мережами операторів зв'язку і великих компаній може здійснюватися за допомогою протоколу зовнішньої маршрутизації. На даний момент протокол BGP є єдиним офіційним протоколом такої маршрутизації в мережі Інтернет.

Примітка. Оскільки протокол BGP є єдиним доступним протоколом зовнішньої маршрутизації, термін «протокол зовнішньої маршрутизації» використовується рідко. Замість цього терміну мережеві фахівці використовують термін протокол BGP.

Головна відмінність між класовими і безкласовими протоколами маршрутизації полягає в тому, що класові протоколи маршрутизації не відправляють дані про маску підмережі в оновленнях маршрутизації. Безкласові протоколи маршрутизації включають в оновлення маршрутизації дані про маску підмережі.

Спочатку було розроблено два протоколи маршрутизації IPv4 - RIPv1 і IGRP. Вони були створені в той час, коли мережеві адреси виділялися з урахуванням класу (наприклад класу A, B або C). У той час протоколу маршрутизації не вимагалося включати маску підмережі в пакет оновлень маршрутизації, оскільки маску мережі можна було визначити по першому октету мережевої адреси.

Примітка. До класових протоколів маршрутизації відносяться тільки протоколи RIPv1 і IGRP. Усі інші протоколи маршрутизації IPv4 і IPv6 є безкласовими протоколами. У протоколі IPv6 ніколи не використовувалася класова адресація.

Той факт, що протоколи RIPv1 і IGRP не включають дані про маску підмережі у свої оновлення, означає, що ці протоколи не можуть надавати маски підмережі змінної довжини (VLSM) і відповідно не можуть використовуватися в безкласовій міждоменній маршрутизації (CIDR).

Класові протоколи маршрутизації також створюють визначені в проблеми в «розірваних» мережах. Мережа вважається «розірваною» у тому випадку, коли підмережі у рамках однієї класової основної мережі розділені іншою класовою мережевою адресою.

У сучасних мережах класова IP -адресація більше не використовується, і маски підмережі неможливо визначити за значенням першого октету. Безкласові протоколи маршрутизації IPv4 (RIPv2, EIGRP, OSPF і IS - IS) включають в оновлення маршрутизації дані про маску

підмережі разом з мережевою адресою. Безкласові протоколи маршрутизації підтримують використання VLSM і CIDR.

Протоколи маршрутизації IPv6 є безкласовими. Розрізняти класові і безкласові протоколи маршрутизації має сенс тільки при використанні протоколів маршрутизації IPv4. Усі протоколи маршрутизації IPv6 вважаються безкласовими, оскільки включають довжину префікса разом з IPv6 -адресою.

Протоколи маршрутизації можна порівняти на основі наступних характеристик.

- **Швидкість збіжності** - визначає швидкість обміну даними маршрутизації і досягнення узгодженості даних між маршрутизаторами у рамках мережевої топології. Чим вища швидкість збіжності, тим прийнятніший протокол. Петлі маршрутизації можуть виникати у випадках, коли неузгоджені таблиці маршрутизації не оновлюються унаслідок повільної збіжності в мережі, що змінюється.
- **Масштабованість** - визначає максимально можливий розмір мережі з урахуванням використовуваного протоколу маршрутизації. Чим більший розмір мережі, тим більше можливостей для масштабування має бути передбачені протоколом маршрутизації.
- **Класові або безкласові протоколи (використання VLSM):** класові протоколи маршрутизації не включають маску підмережі і не підтримують використання VLSM. Безкласові протоколи маршрутизації включають в оновлення маску підмережі. Безкласові протоколи маршрутизації підтримують використання VLSM і забезпечують якісніше об'єднання маршрутів.
- **Споживання ресурсів** - включає такі вимоги протоколу маршрутизації, як об'єм пам'яті (ОЗП), споживання ресурсів ЦП і смуги пропускання каналу. Чим вищі вимоги до ресурсів, тим більше потужне апаратне забезпечення потрібно для підтримки роботи протоколу маршрутизації (окрім процесів пересилки пакетів).
- **Реалізація і обслуговування –** характеристика, що описує рівень знань, потрібний мережевому адміністраторові для реалізації і обслуговування мережі на базі розгорнутого протоколу.

В окремих випадках протокол маршрутизації отримує більше ніж один маршрут до однієї точки призначення. Для вибору оптимального маршруту протокол маршрутизації повинен уміти оцінювати і розрізняти можливі шляхи. Це завдання виконується за допомогою використання метрик маршрутизації.

Метрика є вимірюваним значенням, яке призначається протоколом маршрутизації різним маршрутам з урахуванням корисності того або іншого маршруту. У ситуаціях, коли доступні декілька маршрутів до однієї віддаленої мережі, метрики маршрутизації використовуються для визначення загальної «вартості» шляху від джерела до місця призначення. Протоколи маршрутизації визначають оптимальний шлях, виходячи з маршруту з найменшою вартістю.

Різні протоколи маршрутизації використовують різні метрики. Метрики одного протоколу маршрутизації не не можуть застосовуватися до іншого протоколу. Два різні протоколи маршрутизації можуть вибирати різні шляхи до однієї точки призначення.

14.7. Дистанційно-векторні протоколи маршрутизації

«Дистанційно-векторний» означає, що маршрути оголошуються шляхом вказівки двох характеристик:

- **відстань** - визначає віддаленість мережі призначення; грунтується на таких метриках, як число переходів, вартість, смуга пропускання, значення затримки тощо;
- **вектор** - визначає напрям маршрутизатора наступного переходу або вихідного інтерфейсу маршруту для доступу до адреси призначення.

Існує чотири дистанційно-векторні протоколи внутрішньої маршрутизації IPv4:

- **RIPv1** - застаріла версія протоколу першого покоління;
- **RIPv2** - простий дистанційно-векторний протокол;

- **IGRP** - запатентований протокол Cisco першого покоління (на сьогодні також застарілий, замінений протоколом EIGRP);
- **EIGRP** - розширена версія дистанційно-векторного протоколу.

Дистанційно-векторні протоколи здійснюють обмін оновленнями з сусідніми пристроями. До сусідніх пристроїв відносяться маршрутизатори, які спільно використовують канал і працюють на базі одного протоколу маршрутизації. Маршрутизатору відомі тільки мережеві адреси власних інтерфейсів і адреси віддалених мереж, доступ до яких він може здійснювати через сусідні пристрої. Маршрутизатори, що використовують дистанційно-векторну маршрутизацію, не мають даних про топологію мережі.

Деякі дистанційно-векторні протоколи регулярно відправляють оновлення. Наприклад, протокол RIP кожні 30 секунд відправляє оновлення усім сусіднім пристроям. Протокол RIP продовжує відправляти оновлення навіть у тому випадку, якщо топологія мережі не змінювалася. Протокол RIPv1 здійснює доступ до усіх сусідніх пристроїв за допомогою відправки оновлень на IPv4 -адреси усіх вузлів в мережі 255.255.255.255 (широкомовна розсилка).

Широкомовна розсилка регулярних оновлень не є ефективною, оскільки оновлення споживають смугу пропускання і ресурси ЦП мережевого пристрою. Кожен мережевий пристрій повинен обробити повідомлення широкомовної розсилки. У свою чергу, протоколи RIPv2 і EIGRP використовують групові адреси, тому оновлення отримують тільки ті сусідні пристрої, яким їх потрібно. Протокол EIGRP також може відправляти одноадресні повідомлення тільки тому сусідньому пристрою, який в цьому «зацікавлений». Крім того, протокол EIGRP відправляє оновлення тільки при необхідності, а не регулярно.

Існує два сучасні дистанційно-векторні протоколи маршрутизації IPv4: RIPv2 і EIGRP.

У основі дистанційно-векторного протоколу лежить алгоритм маршрутизації. Цей алгоритм використовується для розрахунку оптимальних шляхів і наступної відправки даних сусіднім пристроям.

Алгоритм протоколу маршрутизації визначає наступні процеси:

- механізм відправки і отримання даних маршрутизації;
- механізм розрахунку оптимальних шляхів і додавання маршрутів в таблицю маршрутизації;
- механізм виявлення і реагування на зміни в топології.

Різні протоколи маршрутизації використовують різні алгоритми для установки маршрутів в таблицю маршрутизації, відправки оновлень сусіднім пристроям і ухвалення рішень про визначення шляху. Розглянемо наступний приклад:

- Протокол RIP використовує алгоритм Беллмана-Форда як алгоритм маршрутизації. Він заснований на двох алгоритмах, розроблених в 1958 і 1956 рр. Річардом Беллманом (Richard Bellman) і Лестером Фордом-мл. (Lester Ford, Jr).
- Протоколи IGRP і EIGRP використовують алгоритм DUAL, розроблений доктором Дж. Дж. Гарсія-Луна-Асевес (SRI International).

Протокол RIP – протокол маршрутизації першого покоління для середовища IPv4, спочатку вказаний в RFC 1058. Налаштування цього протоколу досить просте, що робить його оптимальним протоколом для реалізації в невеликих мережах.

Протокол RIPv1 має наступні ключові характеристики:

- Широкомовна розсилка оновлень маршрутизації (255.255.255.255) виконується кожні 30 секунд.
- В якості метрики для вибору шляху служить число переходів.
- Число переходів, що перевищує 15, вважається нескінченним (тобто занадто видаленим). Маршрутизатор 15-го переходу не передає оновлення маршрутизації на наступний маршрутизатор.

У 1993 році протокол RIPv1 був оновлений в безкласовий протокол маршрутизації - протокол RIP версії 2 (RIPv2). У протоколі RIPv2 представлені наступні удосконалення:

- **Безкласовий протокол маршрутизації:** протокол підтримує використання VLSM і CIDR, оскільки включає маску підмережі в оновлення маршрутизації.
- **Підвищена ефективність:** протокол пересилає оновлення на групову адресу 224.0.0.9, а не на адресу широкомовної розсилки 255.255.255.255.
- **Менше число записів маршрутизації:** протокол підтримує ручне об'єднання маршрутів на будь-якому інтерфейсі.
- **Безпека:** протокол підтримує механізм аутентифікації, що забезпечує безпеку оновлень таблиць маршрутизації між сусідніми пристроями.

Оновлення протоколу RIP інкапсулюються в сегмент протоколу UDP, при цьому номери портів джерела і призначення налаштовані на порт UDP 520.

У 1997 р. була представлена версія протоколу RIP з підтримкою IPv6. У основі протоколу RIPng лежить протокол RIPv2. У протоколі досі діє обмеження в 15 переходів, а адміністративна дистанція дорівнює 120.

Внутрішній протокол маршрутизації шлюзів (IGRP) був першим запатентованим протоколом маршрутизації IPv4, розробленим компанією Cisco в 1984 р. Цей протокол має наступні характеристики:

- Для створення складеної метрики використовуються характеристики смуги пропускання, затримки, навантаження і надійності.
- Широкомовна розсилка оновлень маршрутизації виконується за замовчуваннямкожні 90 секунд.

У 1992 році протокол IGRP був замінений вдосконаленим протоколом IGRP (EIGRP). Як і в RIPv2, в протоколі EIGRP реалізована підтримка використання VLSM і маршрутизації CIDR. Протокол EIGRP забезпечує підвищену ефективність, скорочує об'єм оновлень маршрутизації і підтримує безпечний обмін повідомленнями.

Окрім іншого, протокол EIGRP демонструє наступні можливості:

- **Пов'язані оновлення по події:** протокол не відправляє регулярні оновлення. Поширенню підлягають тільки зміни в таблиці маршрутизації, що дозволяє понизити навантаження на мережу, пов'язану з роботою протоколу. Пов'язані оновлення з події вказують на те, що протокол EIGRP відправляє оновлення тільки тим сусіднім пристроям, яким вони потрібні. Такі оновлення використовують менший розмір смуги пропускання, особливо у великих мережах з множиною маршрутів.
- **Механізм keepalive (Hello):** виконується регулярна відправка і прийом невеликих повідомлень-вітань для підтримки стосунків суміжності з сусідніми маршрутизаторами. Тобто, на відміну від регулярних оновлень, механізм keepalive забезпечує низьке споживання ресурсів мережі.
- **Обробка таблиці топології:** обробка і збереження усіх маршрутів, прийнятих від сусідніх пристроїв (не лише оптимальних шляхів), в таблиці топології. Алгоритм DUAL може виконувати вставку резервних маршрутів в таблицю топології EIGRP.
- **Швидка збіжність:** в більшості випадків цей протокол є протоколом внутрішньої маршрутизації з найшвидшою збіжністю, оскільки він обробляє альтернативні маршрути, забезпечуючи практично миттєву збіжність. У разі збою основного маршруту маршрутизатор може використовувати вказаний альтернативний маршрут. Перемикання на альтернативний маршрут виконується негайно і не вимагає взаємодії з іншими маршрутизаторами.
- **Підтримка протоколів на декількох рівнях мережі:** протокол EIGRP використовує протоколозалежні модулі (PDM), тобто він є єдиним протоколом з підтримкою не лише IPv4 і IPv6, але й інших протоколів (наприклад, застарілих протоколів IPX і AppleTalk).

14.8. Протоколи маршрутизації за станом каналу

Протоколи маршрутизації за станом каналу також відомі як протоколи маршрутизації за найкоротшим шляхом. Ці протоколи використовують алгоритм маршрутизації найкоротшого шляху (SPF) Едсгера Дейкстри.

Протоколи маршрутизації IPv4 за станом каналу:

- алгоритм найкоротшого шляху (OSPF);
- протокол маршрутизації проміжних систем (IS - IS).

Протоколи маршрутизації за станом каналу вважаються складнішими, ніж дистанційно-векторні протоколи. Проте, базові функції і налаштування протоколів маршрутизації за станом каналу схожі.

Як і в протоколах RIP і EIGRP, базові операції в протоколі OSPF можна налаштувати за допомогою команд:

- **router ospf process - id** (команди глобальної конфігурації);
- **network** (команда оголошення мереж).

Для визначення сукупної вартості маршруту алгоритм Дейкстри використовує підсумовувану вартість усіх шляхів від джерела до місця призначення.

На відміну від маршрутизаторів, налагоджених для роботи дистанційно-векторного протоколу, маршрутизатори, що використовують протокол маршрутизації за станом каналу, можуть створювати повне представлення або топологію мережі шляхом збору даних від інших маршрутизаторів.

Використання протоколу маршрутизації за станом каналу схоже на використання детальної карти топології мережі. Вказівні знаки на шляху від джерела до пункту призначення не обов'язкові, оскільки усі маршрутизатори, що працюють з урахуванням стану каналу, використовують ідентичну карту мережі. Маршрутизатор на базі протоколу за станом каналу використовує дані про стан каналу для створення карти топології і вибору оптимального шляху до усіх мереж призначення в топології.

Маршрутизатори, що використовують протокол RIP, регулярно відправляють сусіднім пристроям оновлення своїх даних маршрутизації. Протоколи маршрутизації за станом каналу не використовують регулярні оновлення. Після закінчення збіжності мережі оновлення стану каналу вирушає тільки у разі змін у топології мережі.

Застосування протоколів маршрутизації за станом каналу є доцільним в наступних випадках:

- мережа має ієрархічну структуру, що, як правило, характерно для великих мереж;
- швидка збіжність мережі має критичне значення;
- адміністратори добре розбираються в роботі протоколу маршрутизації за станом каналу.

Існує два протоколи внутрішньої маршрутизації IPv4 за станом каналу:

- **OSPF -** широко використовуваний стандартний протокол;
- **IS - IS -** протокол, поширений в мережах операторів зв'язку.

При використанні протоколів цього типу канал є інтерфейсом на маршрутизаторі. Дані про стан цих каналів також називаються станом каналу.

Примітка. Цей процес однаковий для протоколів OSPF для IPv4 і протоколів OSPF для IPv6.

Процес маршрутизації за станом каналу починається з того, що кожен маршрутизатор дізнається про власні канали і безпосередньо підключені мережі. При налаштуванні інтерфейсу маршрутизатора з використанням IP -адреси і маски підмережі інтерфейс стає частиною цієї мережі.

Як і у випадку з дистанційно-векторними протоколами і статичними маршрутами, інтерфейс необхідно правильно налаштувати з використанням IPv4 -адреси і маски підмережі, а канал має бути в робочому стані до того, як протокол маршрутизації за станом каналу отримає дані про канал. Крім того, як і у випадку з дистанційно-векторними протоколами, інтерфейс також необхідно включити командою network при налаштуванні маршрутизатора, перш ніж він зможе брати участь в процесі маршрутизації за станом каналу.

Далі у рамках процесу маршрутизації за станом каналу кожен маршрутизатор відповідає за зв'язок з сусідніми пристроями в безпосередньо підключених мережах.

Маршрутизатори, що використовують маршрутизацію за станом каналу, використовують hello -протокол для виявлення сусідніх пристроїв на своїх каналах. Сусіднім пристроєм вважається будь-який маршрутизатор, налагоджений з використанням того ж протоколу маршрутизації за станом каналу.

На третьому етапі процесу маршрутизації за станом каналу кожен з маршрутизаторів створює пакет стану каналу, що містить дані про стан кожного безпосередньо підключеного каналу.

Після встановлення стосунків суміжності маршрутизатор може створювати пакети станів каналу, які містять дані про стан каналів цього маршрутизатора.

На четвертому етапі процесу маршрутизації за станом каналу кожен з маршрутизаторів виконує лавинну розсилку пакетів стану каналу усім сусіднім пристроям, які потім зберігають прийняті пакети в базу даних.

Кожен маршрутизатор виконує лавинну розсилку даних про стан каналу на усі маршрутизатори з маршрутизацією за станом каналу в зоні маршрутизації. Кожного разу при отриманні маршрутизатором пакету стану каналу від сусіднього пристрою маршрутизатор негайно відправляє такий пакет на усі інші інтерфейси, крім інтерфейсу, на який отриманий пакет стану каналу. Цей процес дозволяє виконати лавинну розсилку пакетів стану каналу від усіх маршрутизаторів по усій зоні маршрутизації.

Регулярна розсилка пакетів стану каналу не потрібна. Пакети стану каналу необхідно відправляти тільки в наступних випадках:

- під час початкового запуску протоколу маршрутизації на маршрутизаторі (наприклад, при перезавантаженні маршрутизатора);
- при змінах у топології (наприклад, у випадках деактивації або повторної активації каналу, встановленні або розриві стосунків суміжності з сусідніми пристроями).

Окрім даних про стан каналу в пакет стану каналу також включаються такі дані, як порядкові номери і відомості про час створення, що дозволяє управляти процесом лавинної розсилки. Ці дані використовуються кожним з маршрутизаторів, щоб визначити, чи був пакет стану каналу від іншого маршрутизатора отриманий раніше, або пакет містить свіжіші дані, ніж ті, що вже додані в БД про стан каналу. Цей процес дозволяє маршрутизатору зберігати найактуальнішу інформацію в БД про стан каналу.

На останньому етапі процесу маршрутизації за станом каналу кожен маршрутизатор використовує БД для побудови повної карти топології і обчислює оптимальний шлях до кожної з мереж призначення. Зрештою усі маршрутизатори отримують пакет стану каналу від усіх інших маршрутизаторів з маршрутизацією за станом каналу у рамках області маршрутизації. Ці пакети стану каналу зберігаються в базі цих станів каналів.

Кожен маршрутизатор в зоні маршрутизації використовує базу цих станів каналів і алгоритм пошуку найкоротшого шляху для побудови дерева найкоротших шляхів SPF.

Наприклад, використовуючи дані про стан каналу, отримані від усіх інших маршрутизаторів, маршрутизатор R1 може почати побудову дерева найкоротших шляхів SPF для цієї мережі. Спочатку алгоритм пошуку найкоротшого шляху інтерпретує пакет стану каналу кожного маршрутизатора, щоб визначити мережі та пов’язані вартості.

Кожен маршрутизатор створює власне дерево найкоротших шляхів SPF незалежно від інших маршрутизаторів. В цілях правильної маршрутизації, бази цих станів каналів для побудови таких дерев мають бути однаковими на усіх маршрутизаторах.

Протоколи маршрутизації за станом каналу надають ряд переваг у порівнянні з дистанційно-векторними протоколами.

- **Створення карти топології:** протоколи маршрутизації за станом каналу створюють карту топології або дерево найкоротших шляхів SPF мережевої топології. Оскільки протоколи маршрутизації за станом каналу обмінюються пакетами стану каналу, алгоритм пошуку найкоротшого шляху може створити дерево найкоротших шляхів SPF для мережі. Використовуючи дерево найкоротших шляхів SPF, кожен маршрутизатор може самостійно визначити найкоротший шлях до кожної з мереж.

- **Швидка збіжність:** при отриманні пакету стану каналу протоколи маршрутизації за станом каналу негайно виконують лавинну розсилку цього пакету з усіх інтерфейсів, окрім того інтерфейсу, з якого він був отриманий. Протокол RIP, навпаки, вимагається обробити кожне оновлення маршрутизації і оновлення таблиці маршрутизації до виконання лавинної розсилки з інших інтерфейсів.
- **Оновлення за подіями:** після початкової лавинної розсилки пакетів стану каналу протоколи маршрутизації розсилають пакети стану каналу тільки у разі змін у топології. Пакет стану каналу містить лише дані по задіяному каналу. На відміну від деяких дистанційно-векторних протоколів, протоколи маршрутизації за станом каналу не відправляють регулярні оновлення.
- **Ієрархічна структура:** протоколи маршрутизації за станом каналу використовують концепцію областей. Декілька зон складають ієрархічну структуру мереж, забезпечуючи оптимізовану агрегацію (об'єднання) маршрутів та ізолювання проблем маршрутизації в межах зони.

Протоколи маршрутизації за станом каналу також мають деякі недоліки порівняно з дистанційно-векторними протоколами.

- **Вимоги до пам'яті:** протоколи маршрутизації за станом каналу вимагають додаткових ресурсів пам'яті для створення і обслуговування бази цих станів каналів і дерева найкоротших шляхів SPF.
- **Вимоги до обробки:** протоколам маршрутизації за станом каналу також можуть знадобитися додаткові ресурси обробки ЦП. Алгоритму пошуку найкоротшого шляху потрібен триваліший час обробки ЦП, ніж для дистанційно-векторних алгоритмів (наприклад, алгоритм Белмана-Форда), оскільки протоколи маршрутизації за станом каналу виконують побудову повної карти топології.
- **Вимоги до смуги пропускання:** лавинна розсилка пакетів стану каналу може негативно позначитися на доступності смуги пропускання мережі. В більшості випадків це може статися під час першого запуску маршрутизаторів, але іноді може стати проблемою нестабільних мереж.

Сучасні протоколи маршрутизації за станом каналу орієнтовані на мінімальний вплив на ресурси пам'яті, ЦП і смуги пропускання. Використання і налаштування декількох зон дозволяє зменшити розмір баз цих станів каналів. Використання декількох зон також дозволяє скоротити об'єм даних про стан каналу, включених в лавинну розсилку в межах домена маршрутизації, і забезпечує можливість відправки пакетів стану каналу тільки на ті маршрутизатори, яким вони потрібні. При змінах в топології пакет стану каналу отримують тільки маршрутизатори області, яку зачіпає ця зміна, і тільки вони виконують алгоритм пошуку найкоротшого шляху SPF. Це дозволяє ізолювати нестабільний канал в окремій зоні домена маршрутизації.

Протокол OSPF був розроблений інженерною групою з розвитку Інтернету (IETF), що входить до робочої групи з розвитку OSPF. Розробка OSPF почалася в 1987 році, і на сьогодні використовується дві його версії:

- OSPFv2 - OSPF для мереж IPv4 (RFC 1247 і RFC 2328);
- OSPFv3 - OSPF для мереж IPv6 (RFC 2740).

Примітка. Завдяки функції сімейств адрес OSPFv3 протокол OSPFv3 забезпечує підтримку як IPv4, так і IPv6.

Протокол IS - IS розроблений міжнародною організацією з стандартизації (ISO) і задокументований у стандарті ISO 10589. Уперше цей протокол був реалізований корпорацією Digital Equipment Corporation (DEC); він носить назву DECnet Phase V. Протокол маршрутизації IS - IS розроблявся під керівництвом компанії Radia Perlman.

Спочатку протокол IS - IS створювався на базі пакету протоколу OSI, а не TCP/IP. Згодом в протокол Integrated IS - IS, також званий Dual IS - IS, була додана підтримка IP -мереж. Хоча протокол IS - IS відомий як протокол маршрутизації, використовуваний в основному

інтернет-провайдерами і операторами зв’язку, все більше корпоративних мереж переходить на його використання.

Протоколи OSPF і IS - IS багато в чому схожі один з одним, але між ними також існує безліч відмінностей. Користувачі OSPF і IS - IS не припиняють сперечатися з приводу переваг кожного з протоколів. Обидва протоколи маршрутизації забезпечують необхідні функції маршрутизації.

Таблиця маршрутизації є ієрархічною структурою, яка використовується для прискорення процедури пошуку маршрутів і пересилки пакетів. В межах цієї структури існує декілька ієрархічних рівнів.

Маршрути обговорюються з використанням наступних критеріїв:

- остаточний маршрут;
- маршрут 1-го рівня;
- батьківський маршрут 1-го рівня;
- дочірній маршрут 2-го рівня.

Остаточний маршрут є записом в таблиці маршрутизації, що містить або IPv4 -адресу наступного переходу, або вихідний інтерфейс. Безпосередньо підключені, динамічно отримувані і локальні маршрути є остаточними.

При вступі пакету на інтерфейс маршрутизатора маршрутизатор вивчає заголовок IPv4, визначає IPv4 -адресу і переходить до процедури пошуку маршруту.

Примітка. Маршрут, який посилається тільки на IP -адресу наступного переходу і не має певного вихідного інтерфейсу, має бути перетворений в маршрут із заданим вихідним інтерфейсом. На IP -адресі наступного переходу виконується рекурсивний пошук, поки маршруту не буде визначений вихідний інтерфейс.

Щоб IPv4 -адреса призначення пакету співпла з маршрутом в таблиці маршрутизації, потрібна мінімальна кількість збігів по крайніх лівих бітах в IPv4 -адресі пакету і маршруту в таблиці маршрутизації. Маска підмережі маршруту в таблиці маршрутизації використовується для визначення обов’язкового мінімального числа співпадаючих крайніх лівих бітів. Пакет IPv4 містить тільки IPv4 -адресу, а не маску підмережі.

Найкращим збігом є маршрут в таблиці маршрутизації, в якому максимальне число крайніх лівих бітів співпадає з IPv4 -адресою призначення пакету. Маршрут з найбільшим числом еквівалентних крайніх лівих бітів (щонайдовший збіг) завжди є переважним.

Висновок до лекції 14

Віддалені мережі є мережами, доступ до яких можливий тільки шляхом пересилки пакету на інший маршрутизатор. Статичні маршрути легко налаштувати. Проте у великих мережах виконання таких операцій вручну може бути занадто трудомістким. Статичні маршрути можна налаштувати з використанням IP -адреси наступного переходу, яка, як правило, являється IP -адресою маршрутизатора наступного вузла. Якщо використовується IP -адреса наступного переходу, процес таблиці маршрутизації повинен перетворити цю адресу у вихідний інтерфейс. На послідовних каналах із з’єднанням типу точка-точка прийнятніше налаштовувати статичний маршрут з вихідним інтерфейсом. У мережах з множинним доступом, наприклад Ethernet, можна одночасно налаштувати IP -адресу наступного переходу і вихідний інтерфейс на статичному маршруті.

Адміністративна відстань за замовчуваннямдля статичних маршрутів дорівнює 1. Адміністративна відстань також застосовується для статичних маршрутів, налагоджених як з використанням адреси наступного переходу, так і з вихідним інтерфейсом.

Статичний маршрут вноситься в таблицю маршрутизації тільки у разі, якщо IP -адресу наступного переходу можна визначити через вихідний інтерфейс.

Протоколи динамічної маршрутизації виконують наступні завдання: виявлення віддалених мереж, надання актуальних даних маршрутизації, вибір оптимального шляху до мереж призначення і можливість пошуку нового оптимального шляху у разі, якщо поточний

шлях недоступний. Не дивлячись на те, що протоколи динамічної маршрутизації вимагають меншого втручання з боку адміністратора, ніж статична маршрутизація, для їх роботи потрібна спеціально виділена частина ресурсів маршрутизатора, включаючи ресурси ЦП і смугу пропускання каналу.

У багатьох випадках мережі використовують комбінацію статичної і динамічної маршрутизації. Динамічна маршрутизація є оптимальним вибором для великих мереж, тоді як статична маршрутизація ідеально підходить для кінцевих тупикових мереж.

Протоколи маршрутизації відповідають за виявлення віддалених мереж, а також за надання точних даних про мережу. При зміні топології протоколи маршрутизації передають дані про зміни у рамках домена маршрутизації. Процес приведення усіх таблиць маршрутизації в узгоджений стан, в якому усі маршрутизатори в одному домені або області мають повні і точні дані про мережу, називається збіжністю. Деякі протоколи маршрутизації сходяться швидше, ніж інші.

Протоколи маршрутизації класифікуються як класові або безкласові, протоколи на базі векторів відстані або за станом каналу, а також як протоколи внутрішньої або зовнішньої маршрутизації. Дистанційно-векторні протоколи використовують маршрутизатори як вказівні знаки на шляху до кінцевої точки призначення. Єдині дані, які відомі маршрутизатору про віддалену мережу, - відстань або метрика до такої мережі, а також шлях або інтерфейс для доступу до неї. Дистанційно-векторні протоколи не мають фактичної карти топології мережі.

Маршрутизатори, що використовують протокол маршрутизації за станом каналу можуть створювати повне представлення топології мережі шляхом збору даних від усіх інших маршрутизаторів. Метрики використовуються протоколами маршрутизації для визначення оптимального або найкоротшого шляху для доступу до мережі призначення. Різні протоколи маршрутизації використовують різні метрики. Як правило, чим менше значення метрики, тим оптимальнішим вважається шлях. Метрики визначаються за числом переходів, пропускною спроможністю, затримкою, надійністю і навантаженністю.

Усі протоколи динамічної маршрутизації мають унікальне значення адміністративної дистанції разом із статичними маршрутами і безпосередньо підключеними мережами. Чим нижче значення адміністративної дистанції, тим більш переважним є джерело маршруту. Безпосередньо підключена мережа завжди є переважним джерелом. Другим джерелом після неї є статичні маршрути, і після них - різні протоколи динамічної маршрутизації.

При використанні протоколів маршрутизації за станом каналу (наприклад, OSPF) канал є інтерфейсом на маршрутизаторі. Дані про стан цих каналів також називаються станом каналу. Усі протоколи маршрутизації за станом каналу використовують алгоритм Дейкстри для обчислення оптимального шляху. Цей алгоритм зазвичай називають алгоритмом маршрутизації по найкоротшому шляху (SPF). Для визначення сукупної вартості маршруту алгоритм використовує підсумовувану вартість усіх шляхів від джерела до місця призначення.

Питання для закріплення

1. Які переваги та призначення статичної маршрутизації?
2. Як відбувається налаштування статичного маршруту?
3. Яке призначення та роль протоколів динамічної маршрутизації?
4. Який принцип роботи протоколів динамічної маршрутизації?
5. Яким чином класифікуються протоколи маршрутизації?
6. Який принцип роботи дистанційно-векторних протоколів маршрутизації?
7. Наведіть приклади дистанційно-векторних протоколів маршрутизації.
8. Як функціонують протоколи маршрутизації за станом каналу?
9. Наведіть приклади протоколів маршрутизації за станом каналу.

Список рекомендованої літератури

1. CCNA R&S RSE Chapter 6: Static Routing // Електронний ресурс. Режим доступу: https://static-course-assets.s3.amazonaws.com/RSE50ENU/module6/index.html
2. CCNA R&S RSE Chapter 7: Routing Dynamically // Електронний ресурс. Режим доступу: https://static-course-assets.s3.amazonaws.com/RSE50ENU/module7/index.html#7.0.1.1
3. How to configure Static Routing on wireless routers? // Електронний ресурс. Режим доступу: http://www.tp-linkru.com/faq-560.html
4. Dynamic Routing Protocols // Електронний ресурс. Режим доступу: http://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=4

Лекція 15. Тема: «Налаштування OSPF маршрутизації»

План лекції

15.1. Розвиток та характеристики протоколу OSPF.
15.2. Компоненти та принцип роботи протоколу OSPF.
15.3. OSPF для однієї та декількох областей.
15.4. Інкапсуляція та типи пакетів OSPF.
15.5. Встановлення стосунків суміжності з сусідніми пристроями.
15.6. Синхронізація баз даних OSPF.
15.7. Налаштування процесу OSPF.
15.8. Перевірка даних процесу OSPF.

15.1. Розвиток та характеристики протоколу OSPF

Протокол OSPF є протоколом маршрутизації за станом каналу, розробленим як заміна дистанційно-векторному протоколу (RIP). Протокол RIP був прийнятним протоколом маршрутизації на початкових етапах розвитку мережевих технологій і Інтернету. Проте використання протоколом RIP числа переходів як єдиної метрики для визначення оптимального маршруту незабаром привело до ряду труднощів. При використанні цього методу можливості масштабування великих мереж, що містять декілька шляхів з різними швидкостями, обмежені. Протокол OSPF має ряд значних переваг порівняно з протоколом RIP, забезпечуючи швидшу збіжність і можливість масштабування в цілях реалізації мереж більшого розміру.

Протокол OSPF є безкласовим протоколом маршрутизації, що використовує концепцію розподілу на області в цілях масштабованості.

Розробку OSPF в 1987 році почала робоча група OSPF у складі Інженерної групи по розвитку Інтернету (IETF). У той час Інтернет в основному використовувався в учбових закладах і дослідницьких центрах і фінансувався урядом США.

У 1989 році специфікація протоколу OSPFv1 була опублікована в запиті для коментарів (RFC) 1131. Було розроблено дві реалізації. Одна з них була розроблена для роботи з маршрутизаторами, а друга – з робочими станціями під управлінням UNIX. Друга реалізація перетворилася на поширений сервіс UNIX, відомий як GATED. OSPFv1 був експериментальним протоколом маршрутизації, і його розгортання не виконувалося.

У 1991 році Джон Мой представив протокол OSPFv2. Протокол OSPFv2 пропонував істотні технічні переваги порівняно з протоколом OSPFv1.

В той же час, коли був представлений протокол OSPF, робоча група ISO розробляла власний протокол маршрутизації за станом каналу – протоколу маршрутизації проміжних систем (IS - IS). Інженерна група по розвитку Інтернету (IETF) вибрала протокол OSPF в якості рекомендованого протоколу внутрішньої маршрутизації. У 1998 році специфікація

протоколу OSPFv2 була оновлена в запиті для коментарів (RFC) 2328, який до теперішнього часу залишається актуальним RFC для протоколу OSPF. У 1999 році протокол OSPFv3 для IPv6 був опублікований в RFC 2740. У 2008 році протокол OSPFv3 був оновлений в запиті для коментарів (RFC) 5340 як протокол OSPF для IPv6. Протокол OSPF має наступні властивості.

- **Безкласовість** - протокол розроблений як безкласовий, отже, він підтримує використання VLSM і маршрутизації CIDR.
- **Ефективність** - зміни маршрутизації запускають оновлення маршрутизації (без регулярних оновлень). Протокол використовує алгоритм пошуку найкоротшого шляху SPF для вибору оптимального шляху.
- **Швидка збіжність** - швидка трансляція змін мережі.
- **Масштабованість** - підходить для використання, як в невеликих, так і у великих мережах. Для підтримки ієрархічної структури маршрутизатори можна згрупувати в області.
- **Безпека** - підтримує аутентифікацію Message Digest 5 (MD5). Якщо ця функція включена, маршрутизатори OSPF приймають лише зашифровані повідомлення маршрутизації від рівноправних вузлів з однаковим заздалегідь заданим паролем.

Адміністративна дистанція (AD) є значенням надійності джерела маршруту.

15.2. Компоненти та принцип роботи протоколу OSPF

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

Протокол OSPF створює і обслуговує три БД:

- **БД суміжності** - створює таблицю сусідніх пристроїв;
- **БД про стан каналів (LSDB,** link state database**) -** створює таблицю топології;
- **БД пересилки** - створює таблицю маршрутизації.

Ці таблиці містять список сусідніх маршрутизаторів, між якими виконується обмін даними маршрутизації. Таблиці зберігаються і обробляються в ОЗП.

Протокол OSPF здійснює обмін повідомленнями для передачі даних маршрутизації, використовуючи для цього п’ять типів пакетів. До таких пакетів відносяться:

- пакет вітання (hello);
- пакет опису БД;
- пакет стану каналу;
- пакет оновлення стану каналу;
- пакет підтвердження стану каналу.

Ці пакети використовуються для виявлення сусідніх маршрутизаторів, а також для обміну даними маршрутизації в цілях надання точних даних про мережу.

ЦП обробляє таблиці сусідніх пристроїв і таблиці топології, використовуючи алгоритм пошуку найкоротшого шляху Дейкстри. Алгоритм пошуку найкоротшого шляху грунтується на даних про сукупну вартість доступу до точки призначення. Алгоритм пошуку найкоротшого шляху створює дерево найкоротших шляхів SPF шляхом розміщення кожного маршрутизатора у корені дерева і розрахунку найкоротших шляхів до кожного з вузлів. Після цього дерево найкоротших шляхів SPF використовується для розрахунку оптимальних маршрутів. Протокол OSPF вносить оптимальні маршрути в БД пересилки, яка застосовується для створення таблиці маршрутизації.

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

1. **Встановлення стосунків суміжності з сусідніми пристроями**: маршрутизатори з підтримкою OSPF повинні виконати виявлення один одного в мережі, щоб обмінюватися

даними. Маршрутизатор, що використовує OSPF, відправляє пакети вітання з усіх інтерфейсів з включеним OSPF для визначення усіх сусідніх пристроїв у межах цих каналів. За наявності сусіднього пристрою маршрутизатор, що використовує OSPF, намагається встановити з ним стосунки суміжності.

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

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

4. **Виконання алгоритму пошуку найкоротшого шляху SPF**. Після цього маршрутизатори виконують алгоритм пошуку найкоротшого шляху. Оптимальні маршрути вносяться в таблицю маршрутизації з дерева найкоротших шляхів SPF. Рішення з маршрутизації приймаються на основі записів в таблиці маршрутизації.

15.3. OSPF для однієї та декількох областей

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

Протокол OSPF можна реалізувати одним з наступних способів:

- **OSPF для однієї області** - усі маршрутизатори знаходяться в одній області, що називається **магістральною або нульовою областю (область 0).**
- **OSPF для декількох областей -** протокол OSPF реалізується за допомогою декількох областей в ієрархічному порядку. Усі області мають бути підключені до магістральної області (область 0). Маршрутизатори, за допомогою яких здійснюється з'єднання між областями, називаються **пограничними маршрутизаторами (ABR,** Area Border Router**).**

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

Кожного разу, коли маршрутизатор отримує нові дані про зміну топології в межах області (включаючи додавання, видалення або зміну каналу), маршрутизатор повинен повторно виконати алгоритм пошуку найкоротшого шляху, створити нове дерево найкоротших шляхів SPF і відновити таблицю маршрутизації. Алгоритм пошуку найкоротших шляхів споживає великий об'єм ресурсів ЦП; час, що витрачається на розрахунки, залежить від розміру області.

Примітка. Зміни топології розподіляються по маршрутизаторах в інших областях в дистанційно-векторному форматі. Тобто ці маршрутизатори оновлюють тільки свої таблиці маршрутизації і не повинні повторно виконувати алгоритм пошуку найкоротших шляхів.

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

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

- **Таблиці маршрутизації меншого розміру** - менше число записів в таблицях маршрутизації, оскільки мережеві адреси можуть об'єднуватися між областями. Функція об'єднання маршрутів відключена за замовчуванням.
- **Зниження навантаження, викликаного оновленнями стану каналу,** - мінімізація вимог до ресурсів процесора і пам'яті.
- **Зниження частоти розрахунків найкоротшого шляху** - локалізація дії змін топології в межах області. Таким чином, скорочується дія оновлень маршрутизації, оскільки лавинна розсилка оголошень LSA припиняється на межі області.

15.4. Інкапсуляція та типи пакетів OSPF

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

- **Заголовок кадру каналу даних Ethernet** - визначає групову MAC -адресу призначення 01-00-5E-00-00-05 або 01-00-5E-00-00-06.
- **Заголовок IP -пакета** - визначає поле 89 протоколу IPv4, що вказує, що цей пакет є пакетом OSPF. Він також визначає одну з двох групових адрес OSPF (224.0.0.5 або 224.0.0.6).
- **Заголовок пакету OSPF** - визначає тип пакету OSPF, ідентифікатор маршрутизатора і ідентифікатор області.
- **Дані залежно від типу пакету OSPF** - містять дані про тип пакету OSPF. Вміст може відрізнятися залежно від типу пакету. У даному випадку це заголовок IPv4.

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

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

- **Тип 1:** пакет вітання (hello) - використовується для встановлення і підтримки стосунків суміжності з маршрутизаторами OSPF.
- **Тип 2: пакет опису бази даних (DBD)** - містить скорочений список бази цих станів каналів відправляючого маршрутизатора. Використовується приймаючими маршрутизаторами для звіряння з локальною БД про стан каналу. Для побудови точного дерева найкоротших шляхів SPF маршрутизатори з маршрутизацією за станом каналу в межах області повинні використовувати ідентичну базу цих станів каналів.
- **Тип 3:** пакет запиту стану каналу (LSR) - приймаючі маршрутизатори можуть запросити додаткові дані про будь-який запис в пакеті опису БД (DBD), відправивши пакет запиту стану каналу (LSR).
- **Тип 4:** пакет оновлення стану каналу (LSU) - використовується для відправки відгуку на пакети запиту стану каналу (LSR) та оголошення нових даних. Пакети оновлення стану каналу (LSU) містять сім різних типів LSA.
- **Тип 5:** пакет підтвердження стану каналу (LSAck) - при отриманні LSU маршрутизатор відправляє LSAck для підтвердження прийому LSU. Поле даних LSAck є порожнім.

Пакет протоколу OSPF типу 1 – це пакет вітання або hello -пакет. Пакети вітання використовуються в наступних цілях:

- виявлення сусідніх пристроїв OSPF і встановлення стосунків суміжності з ними;
- оголошення параметрів, при яких два маршрутизатори зобов'язано погодитися встановити стосунки суміжності.

У мережах з множинним доступом (Ethernet і Frame Relay) необхідно вибрати виділений маршрутизатор (DR) і резервний виділений маршрутизатор (BDR). Для каналів типу «точка-точка» наявність DR або BDR не потрібно.

До найбільш важливих полів пакету вітання відносяться наступні:

- **Тип** - визначає тип пакету. Число 1 означає пакет вітання. Значення 2 означає пакет DBD, 3 - пакет LSR, 4 - пакет LSU, а 5 - пакет LSAck.

- **Ідентифікатор маршрутизатора - 32**-бітове значення, виражене в десятковому форматі з розподілом точкою (IPv4 -адрес), використовується для унікального позначення початкового маршрутизатора.
- **Ідентифікатор області -** область, в якій створений пакет.
- **Маска підмережі -** маска підмережі, пов'язана з відправляючим інтерфейсом.
- **Інтервал вітання (HelloInterval) -** інтервал (у секундах), після закінчення якого маршрутизатором вирушає наступний пакет вітання. У мережах з множинним доступом інтервал вітання за замовчуванням заданий зі значенням 10 секунд. У сусідніх маршрутизаторах повинен використовуватися один і той же таймер, інакше стосунки суміжності не встановлюються.
- **Пріоритет маршрутизатора -** використовується при виборі DR/BDR. За замовчуванням для усіх маршрутизаторів OSPF заданий пріоритет 1, проте його можна змінити вручну, вибравши значення в діапазоні від 0 до 255. Чим вище це значення, тим більше вірогідність того, що маршрутизатор використовуватиметься як виділений маршрутизатор (DR) на цьому каналі.
- **Інтервал простою (RouterDeadInterval) -** інтервал (у секундах) очікування маршрутизатором сигналу від сусіднього пристрою, після закінчення якого сусідній маршрутизатор оголошується «мертвим», тобто недіючим. Як правило, значення інтервалу простою дорівнює чотирикратному значенню інтервалу вітання. У сусідніх маршрутизаторах повинен використовуватися один і той же таймер, інакше стосунки суміжності не встановлюються.
- **Виділений маршрутизатор (DR) -** ідентифікатор маршрутизатора DR.
- **Резервний виділений маршрутизатор (BDR) -** ідентифікатор маршрутизатора BDR.
- **Список сусідніх пристроїв -** список, що визначає ідентифікатори усіх суміжних маршрутизаторів.

15.5. Встановлення стосунків суміжності з сусідніми пристроями

Якщо на інтерфейсі активований протокол OSPF, маршрутизатор повинен визначити наявність іншого сусіднього пристрою OSPF в каналі. Для цього маршрутизатор відправляє пакет вітання, що містить ідентифікатор маршрутизатора, з усіх інтерфейсів з підтримкою OSPF. Ідентифікатор маршрутизатора OSPF використовується процесом OSPF для унікальної ідентифікації кожного маршрутизатора в області OSPF. Ідентифікатором маршрутизатора є IP -адреса, призначена для ідентифікації конкретного маршрутизатора серед рівноправних вузлів OSPF.

Якщо сусідній маршрутизатор, на якому активований протокол OSPF, отримує пакет вітання з ідентифікатором маршрутизатора, який не включений в список його сусідніх пристроїв, приймаючий маршрутизатор намагається встановити з ініціюючим маршрутизатором стосунки суміжності.

В цілях оновлення даних маршрутизації виконується безперервний обмін пакетами вітання.

У мережах множинного доступу протокол OSPF може зіткнутися з двома проблемами, пов'язаними з лавинною розсилкою пакетів LSA.

- **Встановлення великої кількості стосунків суміжності -** мережі Ethernet потенційно можуть забезпечувати взаємодію багатьох маршрутизаторів OSPF за допомогою загального каналу. Встановлення стосунків суміжності з кожним маршрутизатором не потрібне і є небажаним, оскільки призводить до виникнення надмірної кількості пакетів LSA, якими маршрутизатори обмінюються в межах однієї мережі.
- **Надмірна лавинна розсилка пакетів LSA -** маршрутизатори з маршрутизацією за станом каналу виконують лавинну розсилку своїх пакетів LSA при кожній ініціалізації протоколу OSPF або у разі зміни топології. Подібна лавинна розсилка може стати надмірною.

Для будь-якого числа маршрутизаторів n в мережі множинного доступу існує n (n - 1) / 2 стосунків суміжності.

Може здатися, що це не так багато, проте у міру додавання маршрутизаторів в мережу число стосунків суміжності істотно зростає.

Проблема управління великою кількістю стосунків суміжності і лавинної розсилки пакетів LSA в мережі з множинним доступом вирішується за рахунок виділеного маршрутизатора (DR). У мережах множинного доступу протокол OSPF призначає виділений маршрутизатор (DR) як точку збору і поширення відправлених і прийнятих пакетів LSA. На випадок збою виділеного маршрутизатора (DR) також вибирається резервний виділений маршрутизатор (BDR). Усі інші маршрутизатори отримують статус маршрутизаторів DROthers. Маршрутизатор DROTHER - це маршрутизатор, який не є маршрутизатором DR або BDR.

15.6. Синхронізація баз даних OSPF

Після виходу із стану Two - Way маршрутизатори переходять в стан синхронізації БД. Пакет вітання використовується для встановлення стосунків суміжності з сусідніми пристроями, тоді як інші чотири типи пакетів OSPF використовуються в процесі обміну і синхронізації баз цих станів каналів.

В стані ExStart між маршрутизаторами і їх суміжними маршрутизаторами DR і BDR встановлюються відношення головного та підпорядкованого пристроїв. Маршрутизатор з вищим значенням ідентифікатора виступає в ролі провідного пристрою в стані Exchange.

Після того, як на усі пакети LSR для цього маршрутизатора відправлений відгук, суміжні маршрутизатори вважаються синхронізованими і переведеними в стан Full.

Поки сусідні маршрутизатори продовжують отримувати пакети вітання, дані про мережі, що містяться в переданих пакетах LSA, залишаються в БД топології. Після синхронізації топологічних БД пакети оновлень (LSU) вирушають сусіднім пристроям тільки в наступних випадках:

- отримання змін (інкрементні оновлення);
- після закінчення 30 хвилин.

15.7. Налаштування процесу OSPF

Команда network визначає інтерфейси, що беруть участь в процесі маршрутизації для області OSPF. Усі інтерфейси на маршрутизаторі, що відповідають мережевій адресі у рамках команди network, включені і готові до відправки і прийому пакетів OSPF. В результаті адреса мережі (чи підмережі) інтерфейсу включається в оновлення маршрутизації OSPF.

Базова команда синтаксису – network network - address wildcard - mask area area - id.

Синтаксис команди area area – id відноситься до області OSPF. При налаштуванні OSPF для однієї області на усіх маршрутизаторах необхідно налаштувати команду network з однаковим значенням area - id. Не дивлячись на те, що можна використовувати будь-який ідентифікатор області, для OSPF однієї області рекомендується використовувати ідентифікатор 0. Таке умовне позначення спрощує включення підтримки OSPF для декількох областей у разі змін мережі в майбутньому.

Для включення OSPF на інтерфейсах протокол OSPFv2 використовує комбінацію аргументів network - address wildcard - mask. OSPF є безкласовим протоколом, отже, завжди потрібна шаблонна маска або **wildcard -маска**. При визначенні інтерфейсів, що беруть участь в процесі маршрутизації, шаблонна маска, як правило, є зворотною величиною маски підмережі, налагодженої для цього інтерфейсу.

Шаблонна маска – це рядок з 32 двійкових цифр, що використовуєься маршрутизатором для визначення бітів адреси, які розглядатимуться на предмет збігу. У масці підмережі двійкове значення 1 дорівнює збігу, а двійкове значення 0 не є збігом. Відносно шаблонної маски вірно зворотне.

- Біт 0 шаблонної маски - співпадає з відповідним значенням біта в адресі.
- Біт 1 шаблонної маски - ігнорує відповідне значення біта в адресі.

Простий спосіб розрахувати шаблонну маску – відняти маску підмережі з 255.255.255.255.

Перевагою визначення інтерфейсу є те, що немає необхідності в розрахунку шаблонної маски. Протокол OSPFv2 використовує адресу інтерфейсу і маску підмережі для визначення оголошуваної мережі. У деяких версіях IOS можна вказати маску підмережі замість шаблонної маски. Після цього IOS перетворює маску підмережі у формат шаблонної маски.

За замовчуванням повідомлення OSPF пересилаються з інтерфейсів з включеним OSPF. Проте, насправді, необхідно, щоб ці повідомлення вирушали тільки з інтерфейсів, підключених до інших маршрутизаторів, що використовують протокол OSPF.

Протокол маршрутизації використовує метрику для визначення оптимального шляху пакету в мережі. Метрика означає навантаження, передбачуване при відправці пакетів через вказаний інтерфейс. Протокол OSPF використовує вартість як метрику. Шлях з нижчою вартістю є оптимальним в порівнянні з шляхом з вищою вартістю.

Вартість інтерфейсу обернено пропорційна до його пропускної спроможності. Отже, вища пропускна спроможність вказує на нижчу вартість. Вище навантаження і значення затримки за часом вказують на вищу вартість. Отже, лінія Ethernet 10 Мбіт/с має вищу вартість, ніж лінія Ethernet 100 Мбіт/с.

Формула розрахунку вартості OSPF:

- **Вартість = задана пропускна спроможність / пропускна спроможність інтерфейсу**

Задана пропускна спроможність рівна за замовчуванням10^8 (100000000). Таким чином, використовується наступна формула розрахунку :

- **Вартість = 100 000 000 біт/з /пропускна спроможність інтерфейсу (біт/с)**

Вартість маршруту OSPF є акумульованим значенням від одного маршрутизатора до мережі призначення.

OSPF використовує еталонну пропускну спроможність зі значенням 100 Мбіт/с для усіх каналів, швидкість яких рівна або вище за швидкість FastEthernet-з'єднання. Таким чином, значення вартості, призначене для інтерфейсу FastEthernet з пропускною спроможністю 100 Мбіт/с, дорівнюватиме 1.

Вартість = 100 000000 біт/з /100000000 = 1

Хоча цей розрахунок вірний для інтерфейсів FastEthernet, його використання для каналів, швидкість яких перевищує 100 Мбіт/с, проблематично, оскільки метрика OSPF використовує тільки цілі числа як остаточне значення вартості каналу. При отриманні в результаті розрахунку числа, яке менше цілого числа, протокол OSPF округлює його до найближчого цілого числа. З цієї причини, звертаючись безпосередньо до OSPF, інтерфейс з пропускною спроможністю 100 Мбіт/с (вартість 1) має таку ж вартість, як і інтерфейс з пропускною спроможністю 100 Гбіт/с (вартість 1).

Щоб протокол OSPF правильно визначив шлях, необхідно змінити еталонну пропускну спроможність, задавши вище значення з урахуванням мереж, що утримують канали, швидкість яких вище 100 Мбіт/с.

Зміна еталонної пропускної спроможності фактично не впливає на ширину смуги пропускання каналу. Подібна дія впливає лше на розрахунки при визначенні метрики. Для налаштування еталонної пропускної спроможності використовуєься команда конфігурації маршрутизатора auto - cost reference - bandwidth Mb/s (значення виражене в Мбіт/с). Цю команду необхідно налаштувати на усіх маршрутизаторах в домені OSPF. Отже, для налаштування інших значень використовуються наступні команди:

- **Gigabit Ethernet - auto - cost reference - bandwidth 1000**
- **10 Gigabit Ethernet - auto - cost reference - bandwidth 10000**

Для повернення до значення заданої пропускної спроможності за замовчуванням використовуйте команду auto - cost reference - bandwidth 100.

Для усіх інтерфейсів встановлені значення пропускної спроможності за замовчуванням. Як і у випадку із заданою пропускною спроможністю, значення пропускної спроможності

фактично не впливають на швидкість або місткість каналу. Ці значення використовуються протоколом OSPF для розрахунку метрики маршрутизації. Тому важливо, щоб значення пропускної спроможності відбивало фактичну швидкість каналу для того, щоб в таблиці маршрутизації містилися точні дані для вибору оптимального шляху.

Не дивлячись на те, що значення пропускної спроможності інтерфейсів Ethernet зазвичай відповідають швидкості каналу, у випадках з іншими інтерфейсами цього може не бути. Наприклад, фактична швидкість послідовних інтерфейсів часто відрізняється від значення пропускної спроможності за замовчуванням.

Замість налаштування пропускної спроможності за замовчуванням можна вручну налаштувати на інтерфейсі значення вартості, використовуючи команду конфігурації інтерфейсу ip ospf cost значення.

Перевага налаштування вартості порівняно з налаштуванням пропускної спроможності інтерфейсу полягає в тому, що маршрутизатору не вимагається розраховувати метрику. І, навпаки, якщо налашовується пропускна спроможність інтерфейсу, маршрутизатор повинен розраховувати вартість OSPF з урахуванням пропускної спроможності. Команду ip ospf cost рекомендується використовувати в неоднорідних середовищах, де маршрутизатори сторонніх виробників (не Cisco) можуть використовувати для розрахунку значень вартості OSPF метрику, відмінну від значення пропускної спроможності. Команди інтерфейсу bandwidth і ip ospf cost забезпечують однаковий результат, тобто надають точне значення, використовуване протоколом OSPF при визначенні оптимального маршруту.

15.8. Перевірка даних процесу OSPF

Команда show ip ospf використовується для перевірки ідентифікатора процесу OSPF і ідентифікатора маршрутизатора. Ця команда відображує області OSPF і показує час, коли останній раз виконувався алгоритм пошуку найкоротшого шляху.

Найшвидший спосіб перевірити налаштування інтерфейсу OSPF – використання команди show ip ospf interface. За допомогою цієї команди виводиться список для кожного інтерфейсу, що підтримує OSPF. Цю команду рекомендується використовувати, щоб перевірити правильність команд network.

Щоб отримати дані по усіх інтерфейсах, використовуючим OSPF, використовується команда show ip ospf interface brief (рис. 15.1).

```
R1# show ip ospf interface brief
Interface  PID   Area   IP Address/Mask   Cost   State   Nbrs F/C
Se0/0/1    10    0      192.168.10.5/30   15625  P2P     1/1
Se0/0/0    10    0      172.16.3.1/30     647    P2P     1/1
Gi0/0      10    0      172.16.1.1/24     1      DR      0/0
R1#
```

Рис. 15.1. Перевірка інтерфейсів OSPF маршрутизатора R1 [1]

Команда show ip protocols використовується для перевірки критично важливих даних конфігурації OSPF, включаючи ідентифікатор процесу OSPF, ідентифікатор маршрутизатора і мережі, що оголошуються маршрутизатором.

OSPFv3 активується не в режимі налаштування маршрутизатора, а на інтерфейсі. Для роботи протоколу OSPFv3 необхідно налаштуватиканали типу link - local. Для роботи OSPFv3 необхідно активувати одноадресну маршрутизацію IPv6. Для включення інтерфейсу OSPFv3 необхідно створити 32-бітовий ідентифікатор маршрутизатора.

Висновок до лекції 15

Протокол OSPF – безкласовий протокол маршрутизації зі значенням адміністративної дистанції за замовчуванням 110. Позначений в таблиці маршрутизації кодом джерела маршруту O.

Протокол OSPF активується за допомогою команди режиму глобальної конфигурації router ospf process - id. Значення process - id має локальну значущість, тобто воно необов'язково повинне співпадати зі значеннями на інших маршрутизаторах OSPF, щоб було можливе встановлення стосунків суміжності з цими пристроями.

Команда network в протоколі OSPF, виконує ту ж функцію, як і при використанні з іншими протоколами внутрішньої маршрутизації, але має дещо інший синтаксис. Значення wildcard - mask є зворотним значенням маски підмережі, а значення area - id має бути задане рівним 0.

За замовчуванням пакети вітання протоколу OSPF кожні 10 секунд вирушають до сегментів мереж типу «точка-точка» і мереж множинного доступу; і кожні 30 секунд – до сегментів не широкомовних мереж множинного доступу (Frame Relay, X.25, ATM). Ці пакети використовуються протоколом OSPF для встановлення стосунків суміжності. За замовчуванням інтервал простою дорівнює чотирикратному значенню інтервалу вітання.

Для того, щоб маршрутизатори встановили стосунки суміжності, їх інтервали вітання, інтервали простою, типи мереж і маски підмереж повинні співпадати. Команда show ip ospf neighbors використовується для перевірки стосунків суміжності OSPF.

OSPF вибирає виділений маршрутизатор (DR) як точку збору і поширення пакетів LSA, які вирушають і приймаються у мережі множинного доступу. Резервний виділений маршрутизатор (BDR) вибирається для виконання функцій виділеного маршрутизатора (DR) у разі його несправності. Усі інші маршрутизатори відомі як маршрутизатори DROthers. Маршрутизатори відправляють свої пакети LSA на виділений маршрутизатор, який потім виконує лавинну розсилку пакетів LSA на усі інші маршрутизатори в мережі множинного доступу.

Питання для закріплення

1. Які ви знаєте характеристики протоколу OSPF?
2. Які компоненти та принцип роботи протоколу OSPF?
3. Які особливості OSPF для однієї та декількох областей?
4. Як відбувається інкапсуляція пакетів OSPF?
5. Які є типи пакетів OSPF?
6. Як відбувається встановлення стосунків суміжності з сусідніми пристроями по протоколу OSPF?
7. Як відбувається синхронізація баз даних OSPF?
8. Як відбувається налаштування процесу OSPF?
9. Яка формула використовується для розрахунку вартості OSPF?
10. Як відбувається перевірка даних процесу OSPF?

Список рекомендованої літератури

1. CCNA R&S RSE Chapter 8: Single-Area OSPF // Електронний ресурс. Режим доступу: https://static-course-assets.s3.amazonaws.com/RSE50ENU/module8/index.html
2. Протокол маршрутизації OSPF // Електронний ресурс. Режим доступу: http://ciscotips.ru/ospf
3. OSPF. Поняття ABR і ASBR. Типи LSA // Електронний ресурс. Режим доступу: http://www.itkitchen.net/ospf

Лекція 16. Тема: «Списки контролю доступу»

План лекції

16.1. Визначення та завдання списків контролю доступу.
16.2. Сеанс зв'язку та обмін даними по протоколу TCP.
16.3. Стандартні і розширені ACL -списки.
16.4. Накладення шаблонної маски.
16.5. Рекомендації з використання ACL -списків.
16.6. Налаштування стандартних ACL -списків.
16.7. Використання ACL -списка для управління доступом до VTY.
16.8. Створення розширених ACL -списків.
16.9. Приклади пошуку і усунення поширених помилок ACL -списків.

16.1. Визначення та завдання списків контролю доступу

Фахівці з проектування мереж використовують міжмережеві екрани для забезпечення захисту мережі від несанкціонованого використання. Міжмережеві екрани або брандмауери є апаратними або програмними рішеннями, спрямованими на підвищення міри захищеності мережі. На маршрутизаторі можна налаштувати простий міжмережевий екран, який дозволяє фільтрувати трафік на базовому рівні за допомогою ACL -списків. Використання ACL -списків дозволяє адміністраторам зупиняти трафік або допускати в мережу тільки певний трафік.

Список контролю доступу (ACL, Access Control List**)** – це послідовний список правил дозволу або заборони, вживаних по відношенню до адрес або протоколів більш високого рівня. ACL -списки дозволяють ефективно контролювати вхідний та витікаючий трафік мережі. ACL -списки також можна налаштовувати для усіх протоколів, що маршрутизуються, мережі.

Найважливішою причиною для налаштування ACL -списка є забезпечення безпеки мережі.

ACL -список – це ряд команд IOS, що визначають, чи пересилає маршрутизатор пакети або скидає їх, виходячи з інформації в заголовку пакету. ACL -списки є однією з найбільш використовуваних функцій ОС Cisco IOS.

Залежно від конфігурації ACL -списки виконують наступні завдання.

- Обмеження мережевого трафіку для підвищення продуктивності мережі. Наприклад, якщо корпоративна політика забороняє відеотрафік в мережі, необхідно налаштувати і застосувати ACL -списки, що блокують цей тип трафіку. Подібні заходи значно знижують навантаження на мережу і підвищують її продуктивність.
- Друге завдання ACL -списків – управління потоком трафіку. ACL -списки можуть обмежувати доставку оновлень маршрутизації. Налаштування мережі в оновленнях маршрутизації дозволяє уникнути зайвого використання смуги пропускання.
- Списки контролю доступу забезпечують базовий рівень безпеки відносно доступу до мережі. ACL -списки можуть відкрити доступ до частини мережі одному вузлу і закрити його для інших вузлів. Наприклад, доступ до мережі відділу кадрів може бути обмежений і дозволений тільки авторизованим користувачам.
- ACL -списки здійснюють фільтрацію трафіку на основі типу трафіку. Наприклад, ACL -список може дозволяти трафік електронної пошти, але при цьому блокувати увесь трафік протоколу Telnet.
- Списки контролю доступу здійснюють сотування вузлів в цілях дозволу або заборони доступу до мережевих служб. За допомогою ACL -списків можна дозволяти або забороняти доступ до певних типів файлів, наприклад FTP або HTTP.

За замовчуванням ACL -списки не конфігуровані на маршрутизаторі, тому маршрутизатор не фільтрує трафік. Трафік, що поступає на маршрутизатор, маршрутизується виключно на

основі інформації таблиці маршрутизації. Проте якщо ACL -список використовується на інтерфейсі, маршрутизатор виконує додаткове завдання, оцінюючи усі мережеві пакети, що проходять через інтерфейс, з метою визначення дозволу пересилки пакету.

Окрім дозволу або заборони трафіку, ACL -списки можна використовувати для аналізу, пересилки або обробки окремих видів трафіку. Наприклад, за допомогою ACL -списків можна класифікувати трафік для включення обробки даних відповідно до пріоритету. Ця можливість ACL -списків аналогічна наявності VIP -пропуску на концерт. VIP -пропуск дає обраним гостям привілеї, недоступні володарям звичайних квитків, такі як пріоритет входу або доступ в закриту зону.

16.2. Сеанс зв'язку та обмін даними по протоколу TCP

ACL -списки дозволяють адміністраторам контролювати вхідний та витікаючий трафік. Подібний контроль може зводитися до простої заборони або дозволу трафіку на основі мережевих адрес або бути комплексом заходів з управління мережевим трафіком на основі запитів порту TCP. Зрозуміти, як ACL -список фільтрує трафік, буде легше, якщо розглянути діалог, що виникає при сеансі зв'язку по протоколу TCP, наприклад, при запиті веб-сторінки.

Коли клієнт просить дані від веб-сервера, протокол IP відповідає за взаємодію між комп'ютером (джерело) і сервером (призначення). Протокол TCP управляє обміном даних між браузером (застосування) і ПЗ мережевого сервера.

При відправці електронної пошти, перегляді веб-сторінки або завантаженні файлу протокол TCP відповідає за розбиття даних на сегменти для протоколу IP перед тим, як вони будуть відправлені. Протокол TCP також управляє збором даних, що поступили з сегментів. Дія протоколу TCP дуже схоже на розмову, в якій два мережеві вузли домовляються про передачу даних від одного вузла до іншого.

TCP забезпечує надійний сервіс передачі потоку байтів. Говорять, що протокол TCP орієнтований на встановлення з'єднання (connection - oriented protocol). Термін «зі встановленням з'єднання» означає, що два застосування повинні встановити TCP-з'єднання перед тим, як здійснювати обмін даними. TCP є повнодуплексним протоколом. Це означає, що кожне TCP- з'єднання підтримує пару потоків байтів, і кожен потік байтів слідує в одному напрямі. Протокол TCP включає механізм управління потоками для кожного потоку байтів, що дозволяє одержувачеві обмежувати об'єм даних, що передаються відправником. Протокол TCP також реалізує механізм відстежування перевантаження мережі.

Яким чином ACL -список використовує інформацію, передану в сеансі зв'язку по протоколу TCP/IP, для фільтрації трафіку?

За допомогою фільтрації пакетів, іноді званою статичною фільтрацією пакетів, здійснюється управління доступом до мережі шляхом аналізу вхідних та вихідних пакетів, і пропускання або відкидання пакетів на основі заданих критеріїв, наприклад, IP -адреси джерела, IP -адреси призначення і протоколу усередині пакету.

Маршрутизатор працює як фільтр пакетів, коли перенаправляє або відкидає пакети на основі правил фільтрації. Маршрутизатор, що фільтрує пакети, витягає певну інформацію з пакету, що поступає на нього. Використовуючи цю інформацію, маршрутизатор приймає рішення на основі встановлених правил фільтрації відносно того, чи можна пропустити пакет або його необхідно скинути. Маршрутизатор, що фільтрує пакети, використовує певні правила пропуску або відхилення трафіку. Маршрутизатор також може фільтрувати пакети на рівні 4 – транспортному рівні. Маршрутизатор може фільтрувати пакети на основі порту джерела і порту призначення сегменту TCP або UDP. Ці правила задаються за допомогою ACL -списків.

Список контролю доступу (ACL) – це послідовний список дозволяючих або забороняючих операторів, що називаються записами контролю доступу (ACE, access control entry). Записи контролю доступу також часто називають правилами ACL -списка. ACE -записи можна створити для фільтрації трафіку на підставі певних критеріїв, таких як адреса джерела,

адреса призначення, протокол і номери портів. При проходженні мережевого трафіку через інтерфейс, налагоджений з ACL -списком, маршрутизатор послідовно зіставляє інформацію усередині пакету з кожним записом ACE, визначаючи, чи відповідає пакет одному з правил. Якщо збіг знайдений, пакет обробляється відповідно до записів ACL -списка. Таким чином, ACL -списки можна налаштувати для управління доступом до мережі або підмережі.

Для оцінки мережевого трафіку, ACL -список витягає наступну інформацію із заголовка пакету рівня 3:

- IP -адреса джерела;
- IP -адреса призначення;
- тип повідомлення протоколу ICMP.

ACL -список також може витягати інформацію більше високого рівня із заголовка рівня 4, включаючи:

- порт джерела TCP/UDP;
- порт призначення TCP/UDP.

Списки контролю доступу визначають набір правил, що забезпечують додатковий контроль над пакетами, які приймаються інтерфейсами, транзитними пакетами, які передаються через маршрутизатор, а також пакетами, які вирушають з інтерфейсів маршрутизатора. Списки контролю доступу не застосовуються до пакетів, створених маршрутизатором.

ACL -списки конфігуровані для застосування до вхідного або вихідного трафіку.

- **Вхідні ACL-списки –** вхідні пакети, що обробляються перед відправкою на витікаючий інтерфейс. Вхідний ACL-список ефективний, оскільки він зберігає ресурси на пошук маршруту, якщо пакет скидається. Якщо пакет успішно проходить перевірку, він передається на обробку для подальшої маршрутизації. Вхідні ACL-списки є оптимальним рішенням для фільтрації пакетів, коли мережа, підключена до вхідного інтерфейсу, є єдиним джерелом пакетів, що вимагають аналізу.
- **Витікаючі ACL -списки** - пакети, що входять, маршрутизуються на витікаючий інтерфейс, а потім обробляються витікаючим списком контролю доступу. Витікаючі ACL -списки краще всього використовувати, коли однакові фільтри застосовуються до пакетів, що поступають з багатьох вхідних інтерфейсів перед виходом на той же витікаючий інтерфейс.

Останній запис будь-якого ACL -списка – це завжди «непряма відмова». Це правило автоматично вставляється в кінець кожного ACL -списка, хоча і не є присутнім в ньому фізично. Непряма відмова блокує увесь трафік. Унаслідок цієї неявної заборони ACL -список, що не містить хоч би одного дозволяючого правила, блокує увесь трафік.

16.3. Стандартні і розширені ACL -списки

Існує два типи ACL -списків для IPv4: стандартні і розширені ACL -списки.

Стандартні ACL -списки можна використовувати для дозволу або відхилення проходження трафіку тільки на основі IPv4 -адрес джерела. Призначення пакету і порти, що беруть участь в передачі даних, не оцінюються. Стандартні ACL -списки створюються в режимі глобальної конфігурації.

Розширені ACL -списки фільтрують IPv4 -пакети, виходячи з декількох ознак:

- тип протоколу;
- IPv4 -адреса джерела;
- IPv4 -адреса призначення;
- TCP або UDP порти джерела;
- TCP або UDP порти призначення;
- додаткова інформація про тип протоколу для оптимізованого контролю.

Розширені ACL -списки створюються в режимі глобальної конфігурації.

Стандартні і розширені списки контролю доступу можна створювати за допомогою номера або імені для ідентифікації ACL -списка і списку його правил.

Використання нумерованих ACL -списків - ефективний спосіб визначення типу ACL - списка в невеликих мережах, де в основному використовується трафік одного типу. Проте номер не містить інформації про призначення ACL -списка. З цієї причини, починаючи з операційної системи Cisco IOS версії 11.2, для визначення списків контролю доступу Cisco використовується присвоєне списку ім'я.

16.4. Накладення шаблонної маски

ACL -списки IPv4 використовують шаблонні маски. Шаблонна маска є рядком з 32 двійкових цифр, що використовуються маршрутизатором для визначення бітів адреси, які розглядатимуться на предмет збігів.

Примітка. На відміну від ACL -списків для IPv4, ACL -списки для IPv6 не використовують шаблонні маски. У протоколі IPv6 для вказівки того, яка частина IPv6 - адреса джерела або призначення повинна співпадати, використовується довжина префікса.

Як і у випадку з масками підмереж, цифри 1 і 0 в шаблонній масці визначають, як обробляти відповідні біти IP -адреси. Проте в шаблонній масці ці біти використовуються для інших цілей і наслідують інші правила.

У масках підмережі двійкові одиниці і нулі використовуються для визначення мережі, підмережі і вузлової частини IP -адреси. У шаблонній масці двійкові одиниці і нулі використовуються для фільтрації окремих IP -адрес або груп IP -адрес з метою дозволу або заборони доступу до ресурсів.

Шаблонні маски і маски підмереж розрізняються за правилами збігу двійкових одиниць і нулів. Для збігу двійкових одиниць і нулів в шаблонних масках використовуються наступні правила.

- Біт 0 в шаблонній масці означає, що біт в первинній адресі повинен співпадати з бітом в адресі результату.
- Біт 1 шаблонної маски означає, що відповідне значення біта в адресі може бути проігнороване.

Примітка. Шаблонну маску часто називають зворотною маскою. Ця назва пояснюється тим, що на відміну від маски підмережі, де двійкова одиниця дорівнює збігу, а двійковий нуль не є збігом, в шаблонній масці використовуються зворотні значення.

Розрахунок шаблонних масок може бути зв'язаний з певними складнощами. Простим способом являється віднімання маски підмережі з 255.255.255.255.

Розрахунок шаблонної маски. Приклад 1.

Припустимо, ви хочете дозволити доступ усім користувачам в мережі 192.168.3.0. Якщо маска підмережі 255.255.255.0, ви можете узяти 255.255.255.255 і відняти маску підмережі 255.255.255.0. В результаті виходить шаблонна маска 0.0.0.255.

Розрахунок шаблонної маски. Приклад 2.

Припустимо, ви хочете дозволити мережевий доступ для 14 користувачів в підмережі 192.168.3.32/28. Маска підмережі для IP -підмережі 255.255.255.240, отже, беремо 255.255.255.255 і віднімаємо маску підмережі 255.255.255.240. В результаті виходить шаблонна маска 0.0.0.15.

Розрахунок шаблонної маски. Приклад 3.

Припустимо, ви хочете вичислити шаблонну маску для відповідності мережам 192.168.10.0 і 192.168.11.0. І знову беремо 255.255.255.255 і віднімаємо маску підмережі, яка в даному випадку буде 255.255.252.0. У результаті виходить 0.0.3.255.

Подібний результат можна отримати за допомогою команд, представлених нижче:

R1(config)# access - list 10 permit 192.168.10.0

R1(config)# access - list 10 permit 192.168.11.0

Ефективнішим способом являється конфігурація шаблонної маски таким чином:

R1(config)# access - list 10 permit 192.168.10.0 0.0.3.255

Використовуйте приведену нижче конфігурацію для розрахунку шаблонної маски, що відповідає мережам в діапазоні між 192.168.16.0 і 192.168.31.0:

```
R1(config)# access - list 10 permit 192.168.16.0
R1(config)# access - list 10 permit 192.168.17.0
R1(config)# access - list 10 permit 192.168.18.0
R1(config)# access - list 10 permit 192.168.19.0
R1(config)# access - list 10 permit 192.168.20.0
R1(config)# access - list 10 permit 192.168.21.0
R1(config)# access - list 10 permit 192.168.22.0
R1(config)# access - list 10 permit 192.168.23.0
R1(config)# access - list 10 permit 192.168.24.0
R1(config)# access - list 10 permit 192.168.25.0
R1(config)# access - list 10 permit 192.168.26.0
R1(config)# access - list 10 permit 192.168.27.0
R1(config)# access - list 10 permit 192.168.28.0
R1(config)# access - list 10 permit 192.168.29.0
R1(config)# access - list 10 permit 192.168.30.0
R1(config)# access - list 10 permit 192.168.31.0
```

Приведені вище 16 команд конфігурації можна звести до однієї команди за допомогою правильної шаблонної маски, як показано нижче:

```
R1(config)# access - list 10 permit 192.168.16.0 0.0.15.255
```

Робота з десятковими представленнями бітів двійкової шаблонної маски може бути трудомісткою. Ключові слова host і any спрощують завдання, допомагаючи визначити найбільш часто використовувану шаблонну маску. Ці ключові слова виключають необхідність введення шаблонних масок при визначенні конкретного вузла або цілої мережі. Ці ключові слова полегшують читання ACL -списка, надаючи візуальні підказки відносно критеріїв джерела або призначення.

Ключове слово host застосовується для маски 0.0.0.0. Ця маска вказує, що повинні співпадати усі біти IPv4 -адреса, або співпадає тільки один вузол.

Ключове слово any застосовується для IP -адреси і маски 255.255.255.255. Ця маска вказує ігнорувати всю IPv4 -адресу або прийняти будь-яку адресу.

Примітка. Ключові слова host і anyтакже можна використовувати при конфігурації ACL -списка IPv6.

Складання ACL -списків може бути складним завданням. Для кожного інтерфейсу може існувати декілька правил, необхідних для управління типами трафіку, яким дозволено входити або виходити через цей інтерфейс. Маршрутизатор має два інтерфейси, конфігурованих для IPv4 і IPv6. Якщо для обох протоколів потрібні ACL -списки на обох інтерфейсах і в обох напрямах, то потрібно буде створити 8 окремих ACL -списків. Кожен інтерфейс матиме чотири ACL -списка: два списки для протоколу IPv4 і два - для протоколу IPv6. Для кожного протоколу потрібний один ACL -список для вхідного трафіку, і один - для витікаючого трафіку.

Примітка. Списки контролю доступу не вимагається конфігурувати на обидва напрями. Номери ACL -списків і їх напрями, вживані на інтерфейсі, залежать від заявлених вимог.

16.5. Рекомендації з використання ACL -списків

Приведемо декілька рекомендацій з використання ACL -списків.

- Використовуйте ACL -списки в міжмережевих екранах маршрутизаторів, розміщених між внутрішньою мережею і зовнішньою мережею, наприклад, Інтернетом.
- Для управління вхідним або вихідним трафіком в певній частині внутрішньої мережі використовуйте ACL -списки на маршрутизаторі, розташованому між двома частинами мережі.

- Конфігуруйте ACL -списки на пограничних маршрутизаторах, тобто маршрутизаторах, розташованих на межах мереж. Це забезпечить базовий буфер від зовнішньої мережі або між менш контрольованої і чутливішої областями мережі.
- Конфігуруйте ACL -списки для кожного протоколу мережі, налагодженого на інтерфейсі пограничного маршрутизатора.

Необхідно запам'ятати правило трьох «для», що становлять основні правила застосування ACL -списків на маршрутизаторі. Можна конфігурувати один список контролю доступу **для протоколу, напряму, інтерфейсу**:

- **Один ACL** -список для одного **протоколу** – для управління потоком трафіку на інтерфейсі ACL -список має бути визначений для кожного протоколу, діючого на інтерфейсі.
- **Один ACL** -список для одного **напряму** – ACL -списки одночасно контролюють трафік на одному напрямі одного інтерфейсу. Для управління витікаючим трафіком, що входить, мають бути створені два окремих ACL -списка.
- **Один ACL** -список для одного **інтерфейсу** – ACL -списки управляють трафіком на одному інтерфейсі, наприклад, GigabitEthernet 0/0.

Створення ACL -списків вимагає уваги до деталей і підвищеної обережності. Помилки можуть привести до серйозних наслідків і додаткових витрат, пов'язаних з простоями, пошуком і усуненням неполадок, а також некоректною роботою мережевих служб. Перед конфігурацією ACL -списка необхідно створити базовий план.

Правильне розміщення ACL -списка може підвищити ефективність мережі. ACL -список можна розмістити для мінімізації надмірного трафіку. Наприклад, трафік, який буде відхилений віддаленим місцем призначення, не повинен пересилатися за допомогою мережевих ресурсів за маршрутом до цього місця призначення.

Кожен ACL -список має бути розміщений там, де він може бути максимально корисний. Приведемо список базових правил розміщення ACL -списків:

- **Розширені ACL -списки** - розширені ACL -списки слід розміщувати максимально близько до джерела фільтрованого трафіку. Таким чином, небажаний трафік відхиляється близько до мережі-джерела, не перетинаючи інфраструктуру мережі.
- **Стандартні ACL -списки** - оскільки стандартні списки контролю доступу не визначають адреси призначення, їх розміщують максимально близько до місця призначення. Розміщення стандартного ACL -списка у джерела трафіку дозволяє запобігти досягненню цим трафіком інших мереж через інтерфейс, на якому застосований ACL -список.

Розміщення ACL -списка і, як наслідок, тип використовуваного ACL -списка може також залежати від наступних параметрів:

- **Сфера контролю мережевого адміністратора** - розміщення ACL -списка може залежати від того, чи управляє мережевий адміністратор і мережею-джерелом, і мережею призначення.
- **Пропускна спроможність задіяних мереж** - фільтрація небажаного трафіку у джерела запобігає передачі трафіку до того, як він знижує пропускну спроможність мережі на шляху до пункту призначення. Це особливо важливо в мережах з низькою пропускною спроможністю.
- **Простота конфігурації** - для заборони мережевим адміністратором трафіку, що поступає від декількох мереж, одним із способів може стати використання одного стандартного ACL -списка на найближчому до місця призначення маршрутизаторі. Недолік цього способу в тому, що трафік з цих мереж використовуватиме пропускну спроможність. Розширений ACL -список можна застосувати на кожному маршрутизаторі, з якого йде трафік. Це дозволить зберегти пропускну спроможність за допомогою фільтрації трафіку на джерелі, але для цього потрібно створення розширених ACL -списків на декількох маршрутизаторах.

Примітка. Розширені ACL -списки розміщуються як можна ближче до джерела, а стандартні ACL -списки – якомога ближче до місця призначення.

Стандартний ACL -список може фільтрувати трафік тільки за адресою джерела. Основне правило розміщення стандартного ACL -списка полягає в розміщенні списку як можна ближче до мережі призначення. Це дозволяє трафіку досягти усіх інших мереж, окрім мережі з фільтрацією пакетів.

Як і стандартний ACL -список, розширений список контролю доступу може фільтрувати трафік на основі адреси джерела. Проте, окрім цього, розширений ACL -список може фільтрувати трафік на основі адреси призначення, протоколу і номера порту. Ці додаткові можливості дають мережевим адміністраторам більше гнучкості при виборі типу трафіку, який можна відфільтрувати, і місця розміщення ACL -списка. Основним правилом розміщення розширеного ACL -списка є його розміщення максимально близько до джерела. Дотримання цього правила дозволяє запобігти відправці небажаного трафіку на первинному етапі, а не після проходження декількох мереж.

Мережеві адміністратори можуть розміщувати ACL -списки тільки на тих пристроях, які вони здатні контролювати. Тому місце розміщення визначається, виходячи з меж сфери контролю мережевого адміністратора.

Коли трафік поступає на маршрутизатор, він порівнюється із записами ACE в порядку, заданому в ACL -списку. Маршрутизатор продовжує обробку ACE, поки не виявить збіг. Маршрутизатор обробляє пакет на основі першого знайденого збігу, інші ACE -записи маршрутизатором не враховуються.

Якщо до кінця списку збігу не знайдені, маршрутизатор відхиляє трафік. Це пояснюється тим, що за замовчуванням у кінці кожного ACL -списка міститься команда заборони для трафіку, який не співпали ні з одним записом списку. Якщо ACL -список складається з однієї команди заборони, увесь трафік відхилятиметься. Таким чином, в списку має бути, принаймні, одна команда дозволу, оскільки інакше увесь трафік буде заблокований.

16.6. Налаштування стандартних ACL -списків

Для використання стандартних нумерованих ACL -списків на маршрутизаторі необхідно спочатку створити стандартний ACL -список і потім активувати його на інтерфейсі.

Команда глобальної конфігурації access - list визначає стандартний ACL -список з номером в діапазоні від 1 до 99. У ОС Cisco IOS версії 12.0.1 цей діапазон розширений; для стандартних ACL -списків можуть використовуватися номери від 1300 до 1999. Це дозволяє створити до 798 можливих стандартних ACL -списків. Додаткові номери посилаються на розширений ACL -список по протоколу IP.

Нижче наводиться повний синтаксис команди стандартного ACL -списка:

Router(config)# access - list access - list - number { deny | permit | remark} source [source - wildcard][log]

Записи ACE можуть дозволити або заборонити окремий вузол або діапазон адрес вузлів. Для створення в нумерованому ACL -списке 10 записів, що дозволяє певний вузол з IP - адресою 192.168.10.0, необхідно ввести наступну команду:

R1(config)# access - list 10 permit host 192.168.10.10

Для створення запису, який дозволить діапазон IPv4 -адрес в нумерованому ACL -списку 10, що дозволяє усі IPv4 -адреси в мережі 192.168.10.0/24, необхідно ввести наступну команду:

R1(config)# access - list 10 permit 192.168.10.0 0.0.0.255

Для видалення ACL -списка використовується команда глобальної конфігурації no access - list. Введення команди show access - list підтверджує видалення ACL -списка 10.

При перегляді конфігурації ACL -списка за допомогою команди show running - configтакже відображується відповідний коментар.

Cisco IOS застосовує внутрішній алгоритм в процесі прийому і обробки стандартних записів ACE. Як вже згадувалося раніше, записи ACE обробляються послідовно. Тому при введенні записів ACE важливо дотримувати певний порядок.

Після конфігурації стандартного ACL -списка, він прив'язується до інтерфейсу за допомогою команди режиму налаштування інтерфейсу ip access - group:

Router(config - if)# ip access - group {access - list - number | access - list - name } { in | out }

Для видалення усього ACL -списка з інтерфейсу спочатку слід ввести командуno ip access - group на інтерфейсі, а потім ввести глобальну команду no access - list.

Привласнення імен ACL -спискам спрощує розуміння функції того або іншого списку. Наприклад, ACL -списку, налагодженому для заборони FTP, можна присвоїти ім'я «NO_FTP». При привласненні ACL -списку імені замість номера, режим конфігурації і синтаксис команд змінюються.

Крок 1. Для створенням іменованого ACL -списка почніть з виконання команди режиму глобальної конфігурації ip access - list. Імена ACL -списків складаються з буквено-цифрових символів, вони чутливі до регістра і мають бути унікальними. Команда ip access - list standard name використовується для створення стандартного іменованого ACL -списка, тоді як команда ip access - list extended name застосовується для створення розширеного списку доступу. Після введення команди маршрутизатор входить в режим конфігурації стандартного іменованого ACL -списка, як вказано в командному рядку.

Примітка. Для нумерованих ACL -списків використовується команда глобальної конфігурації access - list, тоді як до іменованим ACL -спискам IPv4 застосовується команда ip access - list.

Крок 2. У режимі конфігурації іменованих ACL -списків застосуйте команди permit або deny, щоб задати одне або більше за умови визначення відправки або відхилення пакету.

Крок 3. Застосуєте ACL -список до інтерфейсу за допомогою команди ip access - group. Визначите, чи повинен ACL -список застосовуватися до пакетів, коли вони приходять на інтерфейс (in), або коли вони покидають його (out).

Вказувати імена ACL -списків заголовними буквами не обов'язково, але це робить їх помітнішими при перегляді вихідних даних поточної конфігурації. Це також знижує вірогідність випадкового створення двох різних ACL -списків з однаковими іменами, але що розрізняються використанням заголовних і рядкових букв.

Для додавання коментарів (зауважень) про записи будь-якого стандартного або розширеного ACL -списка можна використовувати ключове слово remark. Коментарі спрощують розуміння і перегляд ACL -списків. Довжина коментаря обмежена 100 символами.

Коментар можна додавати до або після команди permit або deny. Проте при додаванні коментарів слід використовувати систематичний підхід, щоб користувач завжди міг зрозуміти, до якої команди permit або deny відноситься той або інший коментар. Для додавання коментаря до нумерованого стандартного або розширеному ACL -списку IPv4 використовуйте команду глобальної конфігурації access - list access - list_number remarkremark. Щоб видалити коментар, використовуйте форму no цієї команди.

При налаштуванні стандартного ACL -списка в поточну конфігурацію додаються команди. Проте для цього не передбачена вбудована функція редагування, що дозволяє вносити зміни в ACL -список.

Існує два способи редагування стандартного нумерованого ACL -списка.

Метод 1.Використання текстового редактора

Після ознайомлення з процесами створення і редагування ACL -списків, простішим способом складання ACL буде використання текстового редактора, наприклад блокнот. Він дозволяє створювати або вносити зміни в ACL -список, а потім вставити його в маршрутизатор. Виконайте команду show running - config, щоб відобразити ACL -список, після чого список треба скопіювати, вставити в текстовий редактор, внести необхідні зміни і потім вставити його назад.

Необхідно пояснити, що при застосуванні команди no access - list, версії ОС IOS поводяться по-різному. Якщо ACL -список, який був видалений, все ще застосовується на інтерфейсі, деякі версії IOS діють, неначе немає ACL -списків, що захищають мережу, тоді

як інші версії блокують увесь трафік. З цієї причини рекомендується видалити посилання на списки доступу з інтерфейсу перед внесенням змін в список доступу. Також майте на увазі, що якщо в наново створеному списку виявлена помилка, список необхідно відключити для усунення проблеми. Знову ж таки, на час внесення змін мережа не матиме ACL -списка.

Метод 2. Використання порядкового номера

Наприклад, початкова конфігурація ACL 1 включає запис вузла для вузла 192.168.10.99. Цей запис помилковий. Вузол має бути конфігурований як 192.168.10.10. Щоб змінити список контролю доступу з використанням порядкових номерів, виконаєте наступні дії:

Крок 1. Ще раз відобразіть поточний ACL -список за допомогою команди show access - lists 1. Порядковий номер відображується на початку кожного запису. Порядковий номер автоматично привласнюється при додаванні запису в список. Зверніть увагу, що запис з неправильною конфігурацією має порядковий номер 10.

Крок 2. Введіть команду ip access - lists standard для конфігурації іменованого ACL - списка. Номер ACL -списка, 1, використовується як його ім'я. Спочатку необхідно видалити некоректно конфігурований запис за допомогою команди no 10, де 10 посилається на порядковий номер. Потім додайте новий запис з порядковим номером 10 за допомогою команди 10 deny host 192.168.10.10.

Примітка. Записи не можна перезаписати з тими ж порядковими номерами, що і у існуючих записів. Спочатку необхідно видалити поточний запис, а потім можна створювати нову.

Крок 3. Перевірте внесені зміни, використовуючи команду show access - lists.

Після застосування ACL -списка на інтерфейсі і завершення перевірки за допомогою команди show access – lists відображається статистика для кожного співпадаючого запису. Коли створюється трафік, який повинен відповідати якому-небудь запису ACL -списка, кількість збігів, що відображуються у вихідних даних команди show access - lists, повинно збільшитися. Наприклад, якщо ехо-запит виходить від PC1 до PC3 або PC4, вихідні дані покажуть збільшення кількості збігів для запису ACL 1, що містить заборону.

Записи дозволу і заборони відстежують статистику збігів, проте необхідно пам'ятати, що кожен список контролю доступу має непряму відмову в останньому рядку. Цей запис не відображується при виконанні команди show access - lists, отже, статистика його не враховує. Для перегляду статистики по непрямому запису «deny any», запис можна конфігурувати вручну, після чого вона з'явиться у вихідних даних. При ручній конфігурації команди «deny any» необхідно дотримуватися крайньої обережності, оскільки вона застосовується до усього трафіку. Якщо цей запис не конфігурований як останній запис ACL -списка, це може привести до несподіваних результатів.

Команда show running – config використовується для перевірки конфігурації ACL -списка. Зверніть увагу, що оператори перераховані в іншому порядку, ніж вони були введені.

Порядок, в якому перераховані стандартні ACE -записи, – це послідовність IOS при обробці списку. Записи згруповані в два розділи – оператори вузла слідують після операторів діапазону. Порядковий номер вказує порядок, в якому записи були введені, а не порядок, в якому вони оброблятимуться.

Оператори вузла перераховані першими, проте це не означає, що вони були додані в цьому порядку. IOS розташовує оператори вузлів за допомогою спеціальної функції розставляння (hash function). Отриманий порядок дозволяє оптимізувати пошук оператора вузла в ACL -списку.

Оператори діапазону відображуються після операторів вузла. Ці оператори розташовуються в тому порядку, в якому вони були введені.

Пам'ятайте, усі стандартні і нумеровані списки контролю доступу можна редагувати за допомогою порядкових номерів. Порядковий номер, вказаний у вихідних даних команди show access- lists, є номером, використовуваним при видаленні окремого запису із списку. При додаванні нового запису в ACL -список порядковий номер впливатиме тільки на місце

розташування в списку оператора діапазону. Оператори вузла завжди розташовуватимуться в певному порядку завдяки функції розставляння.

Примітка. Функція розставляння застосовується тільки до операторів вузла в стандартному списку контролю доступу IPv4. Алгоритм не застосовується для розширених ACL -списків IPv4 або IPv6. Це пов'язано з тим, що фільтр розширених і IPv6 ACL -списків більше, ніж просто одна адреса джерела.

16.7. Використання ACL -списка для управління доступом до VTY

Cisco рекомендує використовувати протокол SSH для адміністративних підключень до маршрутизаторів і комутаторів. Якщо образ Cisco IOS на маршрутизаторі не підтримує протокол SSH, можна підвищити безпеку адміністративних каналів шляхом обмеження доступу до VTY. Обмеження доступу до VTY – метод, що дозволяє визначити, якій IP - адресі дозволений доступ Telnet до процесу EXEC маршрутизатора. Можна проконтролювати, яка адміністративна робоча станція або мережа управляє маршрутизатором за допомогою ACL -списка і оператора access - class, конфігурованого на каналах VTY. Також можна використовувати цей метод з протоколом SSH для подальшого поліпшення безпеки адміністративного доступу.

Команда access - class, встановлена в режимі конфігурації каналу, обмежує вхідні та вихідні з'єднання між вказаним VTY (у пристрої Cisco) і адресами в списку доступу.

Стандартні і розширені списки контролю доступу застосовуються до пакетів даних, що передаються через маршрутизатор. Вони не призначені для блокування пакетів, що створюються усередині маршрутизатора. Розширений ACL -список по витікаючому протоколу Telnet не перешкоджає відкриттю Telnet -сесій, ініційованих маршрутизатором за замовчуванням.

Фільтрація трафіку Telnet або SSH, як правило, розглядається як розширена функція ACL -списка IP, оскільки має на увазі фільтрацію трафіку протоколу вищого рівня. Між тим, оскільки для фільтрації вхідного та вихідного трафіку Telnet/SSH використовується команда access - class, можна застосовувати стандартний ACL -список.

Синтаксис команди access - class вглядає так:

Router(config - line)# access - class access - list - number { in [vrf - also] | out }

Параметр in обмежує вхідні з'єднання між адресами в списку доступу і пристроєм Cisco, тоді як параметр out обмежує витікаючі з'єднання між окремим пристроєм Cisco і адресами в списку доступу.

Наступні положення повинні враховуватися при конфігурації списку доступу до каналів VTY.

- Тільки нумеровані списки доступу можуть застосовуватися до VTY.
- Однакові обмеження мають бути встановлені на усі канали VTY, оскільки користувач може спробувати підключитися до будь-якого з них.

16.8. Створення розширених ACL -списків

Для точнішого контролю над фільтрацією трафіку управління можна створити розширені списки контролю доступу IPv4. Розширені ACL -списки нумеруються від 100 до 199 і від 2000 до 2699, забезпечуючи 799 можливих розширених нумерованих ACL -списків. Розширеним ACL -спискам також можна привласнювати імена. Розширені ACL -списки використовуються частіше, ніж стандартні, оскільки вони забезпечують більший об'єм контролю. Як і стандартні, розширені ACL -списки перевіряють адреси джерел пакетів, а також адресу призначення, протоколи і номери портів (чи служб). Це забезпечує ширший спектр критеріїв, на яких можна будувати ACL -список. Наприклад, розширений ACL - список може дозволити трафік електронної пошти з мережі до певного місця призначення з одночасною забороною передачі файлів і переглядом веб-сторінок.

Перевірка портів і служб

Можливість фільтрації за протоколом і номером порту дозволяє мережевим адміністраторам створювати дуже специфічні розширені ACL -списки. Застосування визначається шляхом налаштування номера порту або імені відомого порту.

Послідовність кроків налаштування розширених ACL -списків така ж, як для стандартних ACL -списків. Спочатку розширений ACL -список налаштовується, а потім активується на інтерфейсі. При цьому слід враховувати, що синтаксис команди і параметри складніші для забезпечення підтримки додаткових функцій, що надаються розширеними ACL -списками.

Примітка. Внутрішній алгоритм застосовується для впорядкування записів стандартного списку контролю доступу і не застосовується для розширених ACL -списків. Записи відображуються і обробляються в тому порядку, в якому вони вводилися в процесі налаштування.

Характер протоколу HTTP вимагає, щоб трафік повертався назад в мережу від веб-сайтів, до яких зверталися внутрішні клієнти. Мережевий адміністратор хоче обмежити трафік, що повертається, до HTTP -обменів від прошених веб-сайтів, забороняючи увесь інший трафік. Це завдання виконує ACL 104, блокуючи увесь трафік, що входить, за винятком трафіку від раніше встановлених підключень. Запис permit в ACL 104 дозволяє вхідний трафік параметром established.

Параметр established дозволяє повернення в мережу 192.168.10.0/24 тільки того трафіку, який спочатку виходив з цієї мережі. Пакет задовольняє умовам, якщо зворотний сегмент протоколу TCP має біти ACK і RST, які вказують, що пакет належить існуючому підключенню. Без параметра established запису ACL -списка клієнт може послати трафік на веб-сервер, але не отримати зворотний трафік, що повертається від веб-сервера.

Якщо використовується номер порту замість імені порту, команди матимуть наступний вигляд:

access - list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20

access - list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21

Щоб виключити блокування усього трафіку командою deny any, представленою у вигляді непрямого запису у кінці кожного ACL -списка, необхідно додати команду permit ip any any. За відсутності, принаймні, одній дозволяючою команди permit в ACL -списку увесь трафік на інтерфейсі, де застосований ACL, буде скинутий. Іменовані розширені списки доступу створюються практично тим же способом, що й іменовані стандартні ACL -списки. Для створення розширеного ACL -списка з привласненням імені необхідно виконати наступні дії:

Крок 1. У режимі глобальної конфігурації виконати команду ip access - list extended name для визначення імені розширеного ACL -списка.

Крок 2. У режимі конфігурації іменованого ACL -списка вказати умови для permit або deny.

Крок 3. Повернутися в привілейований режим EXEC і перевірити ACL -список за допомогою команди show access - listsname.

Крок 4. Зберегти записи у файлі конфігурації командою copy running - config startup - config.

Для видалення іменованого розширеного ACL -списка виконати команду глобальної конфігурації no ip access - list extended name.

На відміну від стандартних списків контролю доступу, розширені ACL -списки не реалізують ту ж внутрішню логіку і функцію розставляння. Вихідні порядкові номери, що відображуються у вихідних даних команди show access, - lists, демонструють порядок, в якому були введені записи. Записи вузла не перераховуються автоматично перед записами діапазону.

Команда show ip interface використовується для перевірки ACL -списка на інтерфейсі і напряму, до якого був прив’язаний список. Вихідні дані цієї команди включають номер або ім’я списку доступу і напрям, до якого був прив’язаний ACL -список. Після перевірки конфігурації ACL -списка треба підтвердити, що ACL -списки працюють, як заплановано, тобто блокують і пропускають трафік згідно з вимогами. Внесення змін в розширений ACL -

список здійснюється по аналогії з внесенням змін в стандартний ACL -список. Розширений ACL -список можна змінити за допомогою наступних інструментів.

- **Метод 1.** ACL -список копіюється і вставляється в текстовий редактор, в якому проводяться зміни. Поточний список доступу відділяється командою no access - list. Відредагований ACL -список потім вставляється назад в конфігурацію.
- **Метод 2.** Порядкові номери використовуються для видалення або вставки запису ACL -списка. Команда ip access - list extended name застосовується для запуску режиму конфігурації іменованого ACL -списка. Якщо ACL -списку присвоєний номер, а не ім'я, номер ACL -списка використовується в параметрі name. ACE -записи можна вставити або видалити.

Розглянемо логіку роботи вхідного та вихідного ACL –списка. Якщо дані в заголовку пакету відповідають першому запису ACL -списка, інші записи списку опускаються, і пакет приймається або відхиляється, залежно від умови, з якою він співпав. Якщо заголовок пакету не відповідає першому запису ACL -списка, пакет перевіряється на відповідність наступного запису в списку. Цей процес повторюється до тих пір, поки не будуть перевірені усі записи списку.

Останнім записом у кінці кожного ACL -списка являється непряма команда «deny any». Цей запис не відображується у вихідних даних.

Команда «deny any» застосовується до усіх пакетів, що не задовольняють умовам перевірки. Остання умова перевірки відповідає усім пакетам, що залишилися, і ініціює в їх відношенні дію «заборонити». Маршрутизатор відкидає пакети, що залишилися, не передаючи їх на інтерфейс або з інтерфейсу. Останній запис списку часто називають «непрямою відмовою deny any» або командою «Заборонити увесь трафік». Через цю команду список контролю доступу повинен мати хоч би один дозволяючий запис, інакше увесь трафік блокуватиметься. Перш ніж пакет пересилається на витікаючий інтерфейс, маршрутизатор перевіряє таблицю маршрутизації, щоб визначити, чи підлягає пакет маршрутизації. Якщо пакет не підлягає маршрутизації, він відкидається і не перевіряється на відповідність записам ACE.

Наступним етапом маршрутизатор перевіряє, чи заданий витікаючий інтерфейс в списку контролю доступу. Якщо інтерфейс не заданий, пакет вирушає у вихідний буфер.

Розглянемо декілька прикладів принципу роботи витікаючого списку контролю доступу.

- **ACL** -список не застосований на інтерфейсі: якщо витікаючий інтерфейс не пов'язаний з витікаючим ACL, пакет відправиться безпосередньо на витікаючий інтерфейс.
- **ACL** -список застосований на интерфейсі: якщо витікаючий інтерфейс пов'язаний з витікаючим ACL, пакет не буде відправлений на витікаючий інтерфейс до тих пір, поки не буде перевірений комбінацією записів ACE, пов'язаних з цим інтерфейсом. Залежно від результату перевірки пакет приймається або відхиляється. Для витікаючих списків контролю доступу прийняття означає відправку пакету у вихідний буфер, а відхилення - відкидання пакету.

При отриманні пакету на інтерфейс маршрутизатора, процес маршрутизації залишається незмінним, незалежно від того, застосовуються ACL -списки або ні.

Оскільки кадр прибуває на інтерфейс, маршрутизатор перевіряє його на відповідність адреси призначення рівня 2 адресі інтерфейсу маршрутизатора рівня 2, і чи являється кадр кадром широкомовної розсилки.

Якщо адреса кадру прийнята, інформація кадру віддаляється, і маршрутизатор перевіряє наявність ACL -списка навхідному інтерфейсі. За наявності ACL -списка пакет зіставляється із записами в списку. Якщо пакет відповідає одному із записів, він приймається або відхиляється залежно від умови, з якою він співпав. Якщо пакет приймається, він перевіряється на наявність відповідного запису в таблиці маршрутизації з метою визначення інтерфейсу призначення.

Якщо для цього місця призначення існує запис в таблиці маршрутизації, пакет перенаправляється на вихідний інтерфейс, якщо запису немає – пакет відкидається.

Далі маршрутизатор перевіряє, чи є на вихідному інтерфейсі ACL -список. За наявності ACL -списка пакет зіставляється із записами в списку.

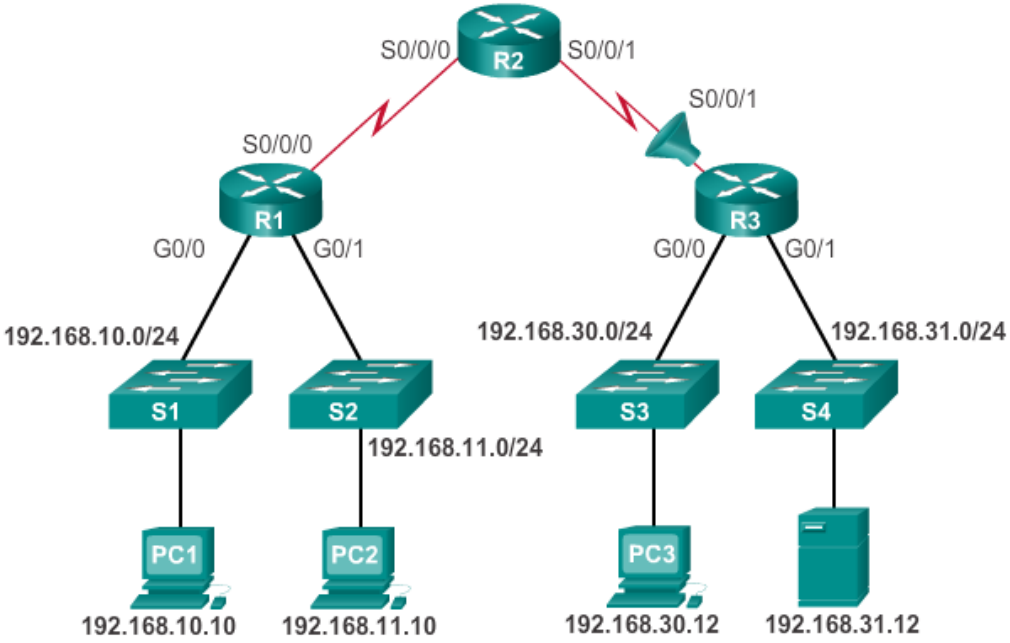
Якщо пакет відповідає одному із записів, він приймається або відхиляється залежно від умови, з якою він співпав. Якщо ACL -список відсутній, або пакету дозволено проходження, пакет інкапсулюється в новому протоколі рівня 2 і перенаправляється на інтерфейс наступного пристрою. Стандартні ACL -списки аналізують лише IPv4 -адрес джерела. Пункт призначення пакету і задіяні порти не розглядаються.

16.9. Приклади пошуку і усунення поширених помилок ACL -списків

Використання команд show дозволяють виявити більшість поширених помилок ACL -списка. До подібних помилок відносяться введення записів ACE в невірному порядку і застосування відповідних критеріїв до правил ACL -списка.

Приклад помилки 1.

Вузол 192.168.10.10 не може підключитися до 192.168.30.12 (рис.16.1). При перегляді вихідних даних команди show access - lists виявлені збіги для першого заборонного запису. Це вказує на те, що ця умова співпала по трафіку.




```
R3# show access-lists
Extended IP access list 110
    10 deny tcp 192.168.10.0 0.0.0.255 any (12 match(es))
    20 permit tcp 192.168.10.0 0.0.0.255 any eq telnet
    30 permit ip any any
```

Рис. 16.1. Перегляд вихідних даних команди show access - lists для виявлення збігів для першого заборонного запису для маршрутизатора R3 [1]

Рішення - перевірити порядок записів ACE. Вузол 192.168.10.10 не може підключитися до 192.168.30.12 через розташування правила 10 в списку доступу. Оскільки маршрутизатор обробляє списки контролю доступу, слідуючи зверху вниз, правило 10 забороняє вузол 192.168.10.10, тому для правила 20 може ніколи не знайтися збіг. Записи 10 і 20 слід поміняти місцями. Останній рядок дозволяє увесь інший трафік, відмінний від TCP, що відповідає протоколу IP (UDP, ICMP і так далі).

Приклад помилки 2

На рис.16.2 мережа 192.168.10.0/24 не може використовувати протокол TFTP для підключення до мережі 192.168.30.0/24.

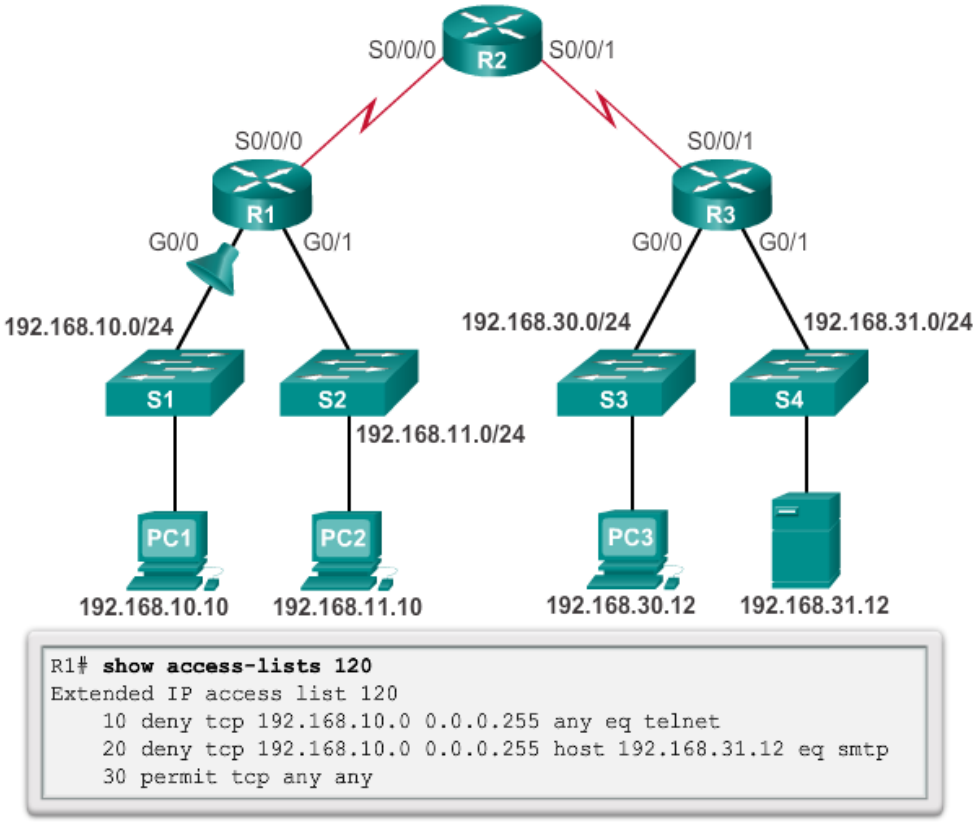


Рис. 16.2. Перегляд вихідних даних команди show access - lists 120 для маршрутизатора R1 [1]

Рішення - мережа 192.168.10.0/24 не може використовувати протокол TFTP для підключення до мережі 192.168.30.0/24, оскільки протокол TFTP використовує транспортний протокол UDP. Рядок 30 в списку доступу 120 дозволяє увесь трафік TCP.

Але оскільки TFTP використовує UDP замість TCP, він побічно заборонений. Непряма відмова «deny any» не відображується у вихідних даних команди show access - lists і, отже, збіги також не відображуються.

Запис 30 слід замінити на ip any any.

Приведений ACL -список працює незалежно від того, чи застосований він на G0/0 R1, S0/0/1 R3 або S0/0/0 R2 у вхідному напрямі.

Грунтуючись на правилі розміщення розширеного ACL -списка як можна ближче до джерела, найбільш оптимальним варіантом буде G0/0 R1, оскільки в даному випадку небажаний трафік буде фільтруватися без необхідності в проходженні через усю інфраструктуру мережі.

Приклад помилки 3

На рис.16.3 мережа 192.168.11.0/24 може використовувати протокол Telnet для з'єднання з 192.168.30.0/24, але відповідно до політики компанії, з'єднання цього типу заборонене.

Результати команди show access - lists 130 вказують на те, що знайдений збіг з дозволяючою умовою.

```
R1# show access-lists 130
Extended IP access list 130
    10 deny tcp any eq telnet any
    20 deny tcp 192.168.11.0 0.0.0.255 host 192.168.31.12 eq smtp
    30 permit tcp any any (12 match(es))
```

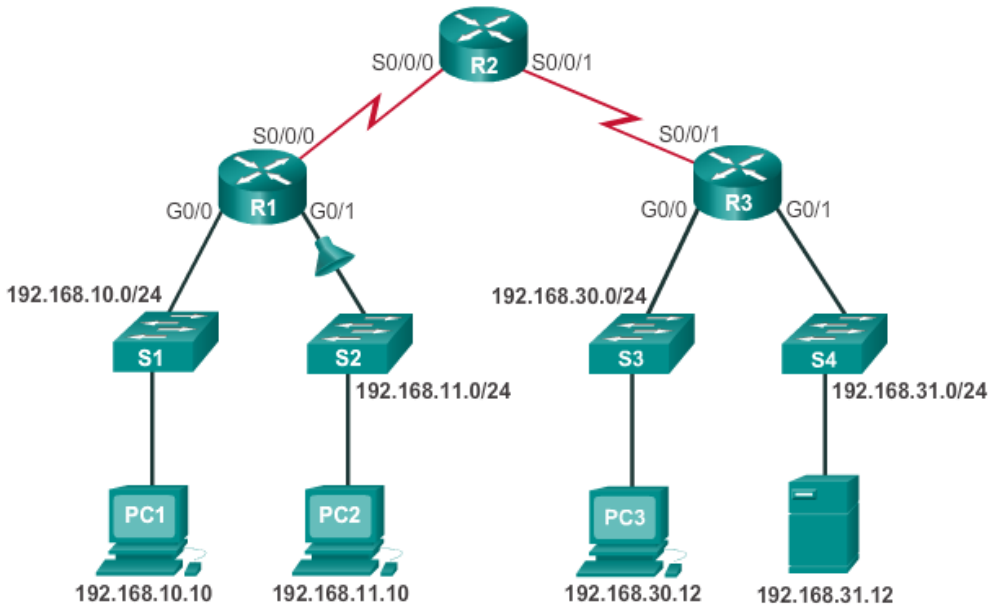


Рис. 16.3. Результати команди show access - lists 130 для маршрутизатора R1 [1]

Рішення - мережа 192.168.11.0/24 може використовувати протокол Telnet для підключення до мережі 192.168.30.0/24, оскільки номер порту протоколу Telnet в рядку 10 списку доступу 130 приведений в невірному місці запису ACL -списка. Нині рядок 10 забороняє будь-яке джерело пакету з номером порту, рівним Telnet. Щоб заборонити вхідний трафік Telnet на інтерфейсі G0/1, треба заборонити номер порту призначення, рівний Telnet, наприклад, deny tcp any any eq telnet.

Приклад помилки 4

На рис.16.4 вузол 192.168.30.12 має можливість використовувати Telnet для підключення до 192.168.31.12, але згідно політики безпеки компанії, подібне підключення має бути заборонене. Вихідні ці команди show access - lists 140 вказують на те, що знайдений збіг з дозволяючою умовою.

Рішення - вузол 192.168.30.12 може використовувати Telnet для підключення до 192.168.31.12, оскільки немає правил, що забороняють вузол 192.168.30.12 або його мережа в якості джерела. Рядок 10 списку доступу 140 забороняє інтерфейс маршрутизатора, через який трафік поступає на маршрутизатор. IPv4 -адресf вузла в записі 10 має дорівнювати 192.168.30.12.

```
R3# show access-lists 140
Extended IP access list 140
    10 deny tcp host 192.168.30.1 any eq telnet
    20 permit ip any any (5 match(es))
```

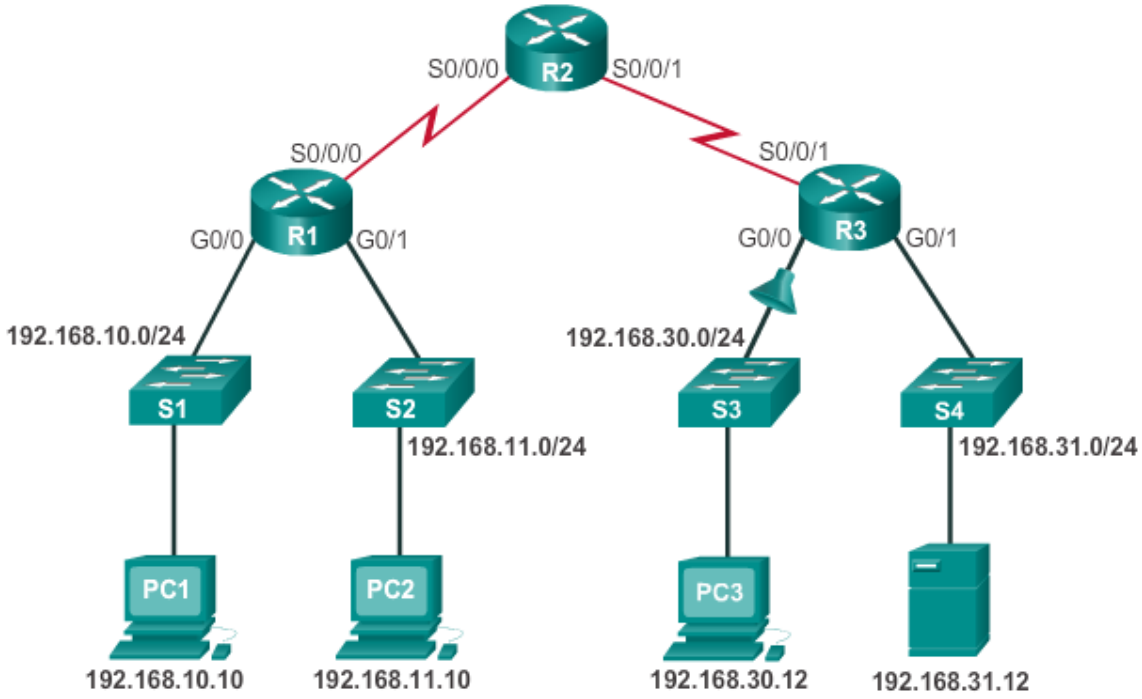


Рис. 16.4. Результати команди show access - lists 140 для маршрутизатора R3 [1]

Приклад помилки 5

На рис.16.5 вузол 192.168.30.12 може використовувати протокол Telnet для підключення до 192.168.31.12, але згідно політики безпеки, це підключення не може бути дозволене. Вихідні дані команди show access - lists 150 вказують на те, що, всупереч очікуванням, немає жодного збігу із заборонною умовою.

Рішення - вузол 192.168.30.12 може підключатися до 192.168.31.12 через протокол Telnet через напрям, у якому список доступу 150 застосований на інтерфейсі G0/1. Правило 10 забороняє будь-яку адресу джерела для підключення до вузла 192.168.31.12 з використанням telnet. Проте для коректної фільтрації цей фільтр має бути застосований на витікаючому G0/1.

```
R2# show access-lists 150
Extended IP access list 150
    10 deny tcp any host 192.168.31.12 eq telnet
    20 permit ip any any
```

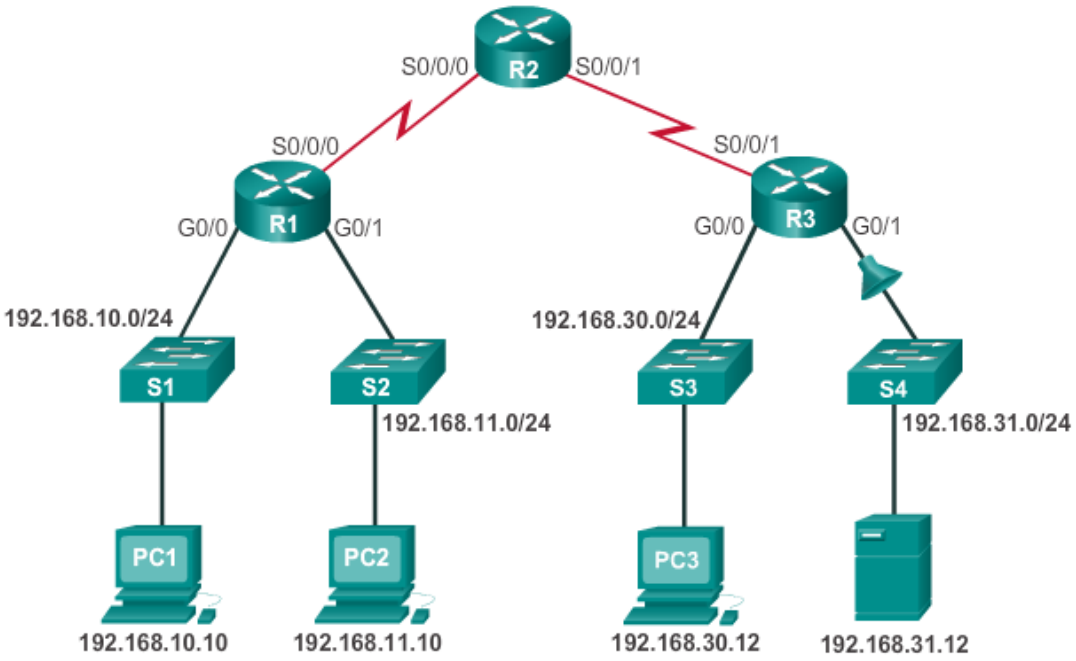


Рис. 16.5. Результати команди show access - lists 140 для маршрутизатора R2 [1]

Висновок до лекції 16

За замовчуванням маршрутизатор не фільтрує трафік. Трафік, що поступає на маршрутизатор, маршрутизується виключно на основі інформації таблиці маршрутизації.

За допомогою фільтрації пакетів здійснюється управління доступом до мережі шляхом аналізу пакетів, пропускання або відкидання пакетів на основі таких критеріїв, як IP -адреса джерела, IP -адреса призначення і протокол усередині пакету. Маршрутизатор, що фільтрує пакети, використовує певні правила пропуску або відхилення трафіку. Маршрутизатор також може фільтрувати пакети на транспортному рівні.

ACL -список є послідовним списком дозволяючих або забороняють умов. Останнім записом ACL -списка завжди є непряма відмова, що блокує увесь трафік. Для того, щоб відмінити дію непрямої відмови, присутньої у кінці будь-якого ACL -списка і що забороняє увесь трафік, можна додати дозволяючу команду permit ip any any.

При проходженні мережевого трафіку через інтерфейс, налагоджений за допомогою ACL -списку, маршрутизатор по порядку зіставляє інформацію усередині пакету з кожним записом списку, намагаючись знайти відповідність. Якщо збіг знайдений, пакет обробляється відповідно до записів ACL -списка.

Стандартні ACL -списки можна використовувати для дозволу або відхилення трафіку тільки з IPv4 -адрес джерела. Призначення пакету і порти, що беруть участь в передачі даних, не оцінюються. Основним правилом розміщення розширеного ACL -списка є його розміщення максимально близько до пункту призначення.

Розширені ACL -списки фільтрують пакети на основі декількох атрибутів: тип протоколу, IPv4 -адреси джерела або призначення і порти джерела або призначення. Основним правилом розміщення розширеного ACL -списка є його розміщення максимально близько до джерела.

Команда глобальної конфігурації access - list задає стандартний ACL -список з номером в діапазоні від 1 до 99 або розширений ACL -список з номером в діапазоні від 100 до 199 і від 2000 до 2699. Як стандартним, так і розширеним ACL -спискам можна привласнювати імена. Команда ip access - list standard name використовується для створення стандартного іменованого ACL -списка, тоді як команда ip access - list extended name використовується для створення розширеного списку доступу. ACL -списки IPv4 використовують шаблонні маски.

Після налаштування ACL -списка він підключається до інтерфейсу за допомогою команди ip access - group в режимі налаштування інтерфейсу. Не забувайте правило трьох «для» – лише один ACL -список передбачений для кожного протоколу, напряму та інтерфейсу.

Для видалення усього ACL -списка з інтерфейсу спочатку слід ввести командуno ip access - group на інтерфейсі, а потім ввести глобальну команду no access - list.

Для перевірки налаштування ACL -списка використовується команда show running - config і show access - lists. Команда show ip interface використовується для перевірки ACL -списка на інтерфейсі і напряму, до якого був прив'язаний список.

Команда access - class, введена в режимі конфігурації каналу, обмежує з'єднання між окремим VTY і адресами в списку доступу.

Як і у випадку з іменованими ACL -списками для IPv4, імена списків для IPv6 складаються з буквено-цифрових символів, вони чутливі до регістра і мають бути унікальними. На відміну від IPv4, стандартна або розширена опція не вимагаються.

Питання для закріплення

1. Які основні завдання списків контролю доступу?
2. Для чого використовуються стандартні і розширені ACL –списки?
3. Які особливості використання розширених ACL –списків?
4. Які основні рекомендації з використання ACL –списків?
5. Як відбувається налаштування стандартних ACL –списків?
6. Як налаштовується ACL -список для управління доступом до VTY?
7. Як налаштовуються розширені ACL –списки?
8. Назвіть приклади пошуку і усунення поширених помилок ACL –списків.

Список рекомендованої літератури

1. CCNA R&S RSE Chapter 9: Access Control Lists // Електронний ресурс. Режим доступу: https://static-course-assets.s3.amazonaws.com/RSE50ENU/module9/index.html
2. Access Control Lists // Електронний ресурс. Режим доступу: https://msdn.microsoft.com/en-us/library/windows/desktop/aa374872(v=vs.85).aspx
3. Configuring IP Access Lists // Електронний ресурс. Режим доступу: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html

Лекція 17. Тема: «Протокол DHCP»

План лекції

17.1. Призначення протоколу DHCP.
17.2. Операція DHCPv4.
17.3. Формат повідомлень DHCPv4.
17.4. Налаштування простого DHCPv4 –сервера.
17.5. DHCPv4-ретрансляція.
17.6. Налаштування маршрутизатора в якості DHCPv4-клієнта.
17.7. Пошук і усунення неполадок DHCPv4.
17.8. Перевірка налаштувань DHCPv4 на маршрутизаторі.

17.1. Призначення протоколу DHCP

Для кожного пристрою, підключеного до мережі, потрібна унікальна IP -адреса. Мережеві адміністратори привласнюють статичні IP -адреси маршрутизаторам, серверам, принтерам та іншим мережевим пристроям, чиє фізичне і логічне розташування, швидше за все, не зміниться. В більшості випадків йдеться про пристрої, що надають служби користувачам і пристроям в мережі; таким чином, привласнювані ними адреси мають бути постійними. Крім того, статичні адреси дозволяють адміністраторам управляти цими пристроями віддалено. Мережевим адміністраторам простіше дістати доступ до пристрою, якщо його IP -адресу легко визначити.

Проте в організації часто змінюється фізичне і логічне місце розташування користувачів і комп'ютерів. Привласнення нових IP -адрес при кожному переміщенні співробітника може бути складним і трудомістким процесом. При ручному налаштуванні параметрів мережі для співробітників, що працюють з віддалених місць, адміністратор також може зіткнутися з рядом труднощів. Крім того, привласнення IP -адрес вручну і налаштування іншої інформації про адресацію для настільних ПК також вимагає зусиль і витрат часу системного адміністратора, особливо у разі розширення мережі.

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

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

Протокол DHCP доступний як для IPv4 (DHCPv4), так і IPv6 (DHCPv6).

DHCPv4 привласнює IPv4 -адреси та інші мережеві параметри динамічно. Оскільки стаціонарні ПК зазвичай складають основну частину мережевих вузлів, протокол DHCPv4 є украй корисним інструментом, що дозволяє мережевим адміністраторам значно економити час.

Протокол DHCPv4 має 3 різні механізми призначення адреси, що забезпечують гнучкість при привласненні IP -адрес:

- **Ручний розподіл** - адміністратор привласнює пристрою-клієнтові заздалегідь виділену IPv4 -адресу, тоді як DHCPv4 тільки передає IPv4 -адресу до пристрою.
- **Автоматичний розподіл** - DHCPv4 автоматично привласнює пристрою постійну статичну IPv4 -адресу, вибираючи його з пулу доступних адрес. При автоматичному розподілі відсутнє поняття оренди, і пристрою виділяється адреса на постійне використання.
- **Динамічний розподіл** - DHCPv4 динамічно привласнює або видає в оренду IPv4 -адресу з пулу адрес на обмежений період часу – за вибором сервера або до тих пір, поки у клієнта є необхідність в адресі.

Протокол DHCPv4 зазвичай використовує механізм динамічного розподілу. При використанні динамічного розподілу клієнти орендують дані від сервера на заданий адміністратором термін. Адміністратори настроюють сервери DHCPv4 так, щоб термін оренди збігав в різний час.

Термін оренди зазвичай складає від 24 годин до тижня або більше. Після закінчення терміну оренди клієнт повинен запросити іншу адресу, хоча в більшості випадків клієнтові повторно призначається та ж адреса.

17.2. Операція DHCPv4

DHCPv4 працює згідно моделі «клієнт-сервер». Коли клієнт підключається до сервера DHCPv4, сервер привласнює або здає йому в оренду IPv4 -адресу. Клієнт з орендованою IP -адресою підключається до мережі до закінчення терміну оренди. Періодично клієнт повинен зв'язуватися з DHCP -сервером для продовження терміну оренди.

Завдяки подібному механізму клієнти, що «переїхали» або відключилися, не займають адреси, яких вони більше не потребують.

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

Первинна оренда

При початковому завантаженні клієнта (чи іншому способі підключення до мережі) починається 4-кроковий процес отримання адреси в оренду. Клієнт починає процес з повідомлення DHCPDISCOVER широкомовної розсилки зі своєї MAC -адреси з метою виявлення доступних DHCPv4 -серверів.

Виявлення DHCP (DHCPDISCOVER)

Повідомлення DHCPDISCOVER знаходить в мережі DHCPv4 -сервери. Оскільки під час завантаження у клієнта немає вірної IPv4 -інформації, для зв'язку з сервером використовуються широкомовні адреси рівня 2 і рівня 3.

Пропозиція DHCP (DHCPOFFER)

Коли сервер DHCPv4 отримує повідомлення DHCPDISCOVER, він резервує доступні IPv4 -адреси для видачі в оренду клієнтові. Сервер також створює запис ARP, що складається з MAC -адреси просячого клієнта і виданої клієнтові IPv4 -адреси. DHCPv4 -сервер посилає повідомлення прив'язки DHCPOFFER просячому клієнтові. Адресою джерела одноадресної розсилки повідомлення DHCPOFFER є MAC -адреса 2 рівня 2 сервера, адресою призначення - MAC -адреса 2 рівня клієнта.

Запит DHCP (DHCPREQUEST)

Коли клієнт отримує від сервера повідомлення DHCPOFFER, він відправляє у відповідь повідомлення DHCPREQUEST. Це повідомлення використовується як для первинної оренди адреси, так і для її продовження. Коли повідомлення використовується при первинній оренді, DHCPREQUEST служить повідомленням про прийняття пропозиції прив'язки до запропонованим сервером параметрам і непрямим відхиленням для усіх інших серверів, які могли надати клієнтові пропозицію прив'язки.

У корпоративних мережах часто використовується декілька DHCPv4 -серверів. Повідомлення DHCPREQUEST вирушає у формі широкомовної розсилки з метою інформування цього DHCPv4 -сервера та інших DHCPv4 -серверів про те, що пропозиція була прийнята.

Підтвердження DHCP (DHCPACK)

При отриманні повідомлення DHCPREQUEST, сервер перевіряє, чи не використовується видавана в оренду IP -адреса за допомогою відправки exo-запиту за протоколом ICMP на цю адресу. Після цього сервер створює новий запис ARP для клієнтської оренди і відповідає повідомленням одноадресної розсилки DHCPACK.

Повідомлення DHCPACK є копією повідомлення DHCPOFFER, за винятком зміни в полі типу повідомлення. При отриманні повідомлення DHCPACK клієнт завантажує інформацію про конфігурацію і виконує ARP -перевірку присвоєної адреси.

Якщо ARP -відповіді немає, значить, IPv4 -адреса доступна, і клієнт починає використовувати її як власну адресу.

Продовження оренди

Запит DHCP (DHCPREQUEST)

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

Підтвердження DHCP (DHCPACK)

При отриманні повідомлення DHCPREQUEST сервер підтверджує інформацію про оренду повідомленням у відповідь DHCPACK.

17.3. Формат повідомлень DHCPv4

Для усіх транзакцій DHCPv4 використовується однаковий формат повідомлень DHCPv4. Повідомлення DHCPv4 інкапсулюються у рамках транспортного протоколу UDP. Повідомлення DHCPv4 вирушають від клієнта через протокол UDP з порту джерела 68 в порт призначення 67.

Повідомлення DHCPv4 містить наступні поля:

- **Код операції (OP) –** вказує загальний тип повідомлення. Значення 1 означає повідомлення-запит; значення 2 – повідомлення-відповідь.
- **Тип устаткування** - визначає тип апаратного устаткування, що використовується в мережі. Наприклад, 1 – Ethernet, 15 – Frame Relay, 20 – послідовний канал. Ці ж коди використовуються в повідомленнях ARP.
- **Довжина фізичної адреси** - задає довжину адреси.
- **Переходи** - управління процесом пересилки повідомлень. Встановлюється клієнтом на 0 перед відправкою повідомлення-запиту.
- **Ідентифікатор транзакції** - використовується клієнтом для узгодження запиту з відповідями від DHCPv4 -серверів.
- **Секунди** - означають кількість секунд, пройдених з моменту, коли клієнт почав намагатися отримати або продовжити оренду. Використовується DHCPv4 -серверами для розставляння пріоритетності відповідей, у разі декількох клієнтських запитів.
- **Прапори** - застосовуються клієнтом, який не знає своєї IPv4 -адреси при відправленні запиту. Використовується тільки один з 16 біт, що є прапором широкомовної розсилки. Значення 1 в цьому полі повідомляє DHCPv4 -серверу або агентові-ретранслятору, що приймає запит, що відповідь має бути послана у формі широкомовної розсилки.
- **IP -адреса клієнта** - використовується клієнтом при оновленні адреси після закінчення терміну оренди, тобто коли клієнт має власну IP -адресу, але не в процесі первинного її отримання. Клієнт підставляє власну IPv4 -адресу в це поле тільки у разі, якщо у нього є діюча IPv4 -адреса, що співпадає з раніше призначеною; інакше значення поля встановлюється на 0.
- **IP -адреса сервера** - застосовується сервером для розпізнавання адреси сервера, який клієнт повинен використовувати для наступного кроку в процесі самоналаштування. Цей сервер може бути (чи не являтися) сервером, що посилає відповідь. Сервер, що посилає відповідь, завжди включає власну IPv4 -адресу в окреме поле – опцію Ідентифікатор сервера DHCPv4.
- **IP -адреса шлюзу** - направляє DHCPv4 -повідомлення при використанні агентів-ретрансляторів DHCPv4. Використання заданої адреси шлюзу спрощує передачу DHCPv4 -запитів і відповідей між клієнтом і сервером, які знаходяться в різних підмережах або мережах.
- **Фізична адреса клієнта** - вказує фізичний рівень клієнта.
- **Ім’я сервера** - використовується сервером, що відправляє повідомлення DHCPOFFER або DHCPACK. Це поле є необов’язковим для заповнення. Ім’ям сервера може бути простий текстовий псевдонім або доменне ім’я DNS -сервера, як наприклад dhcpserver.netacad.net.
- **Ім’я файлу завантаження** - опціональне поле, що використовує клієнт для запиту файлу завантаження певного типу за допомогою повідомлення DHCPDISCOVER. Застосовується сервером у повідомленні DHCPOFFER для точного завдання директорії файлу завантаження та імені файлу.
- **Опції DHCP** - поле включає опції DHCP, а також деякі параметри, необхідні для основних операцій протоколу DHCP. Довжина цього поля змінюється. Поле може використовуватися як клієнтом, так і сервером.

У випадку якщо до мережі хоче підключитися клієнт з налаштуваннями на динамічне отримання налаштувань IPv4, він просить значення адресації від DHCPv4 -сервера. Передача

клієнтом повідомлення DHCPDISCOVER в локальну мережу відбувається під час завантаження клієнта або при виявленні ним активного мережевого підключення.

Оскільки клієнт не може знати, до якої підмережі він відноситься, повідомлення DHCPDISCOVER є широкомовною розсилкою IPv4 (IPv4 -адреса призначення 255.255.255.255). Оскільки у клієнта ще немає налагодженої IPv4 -адреси, використовується IPv4 -адреса джерела – 0.0.0.0.

DHCPv4 -сервер відповідає на повідомлення DHCPDISCOVER повідомленням DHCPOFFER. Це повідомлення містить попередні налаштування для клієнта, включаючи IPv4 -адресу, запропоновану сервером, маску підмережі, термін оренди і IPv4 -адресу DHCPv4 -сервера, від якого виходить пропозиція.

Повідомлення DHCPOFFER може бути також налагоджене для утримання додаткових даних, таких як час оновлення оренди і адреса DNS -сервера.

17.4. Налаштування простого DHCPv4 -сервера

Маршрутизатор Cisco з ОС Cisco IOS можна налаштувати в якості DHCPv4 -сервера. DHCPv4 -сервер під управлінням Cisco IOS привласнює DHCPv4 -клієнтам IPv4 -адреси із заданого пулу адрес маршрутизатора і управляє цими адресами.

Крок 1. Виключення IPv4 -адрес

Маршрутизатор, що виконує функцію DHCPv4 -сервера, привласнює усі IPv4 -адреси з пулу DHCPv4 -адрес, якщо конфігурацією не передбачено виключення окремих адрес. Як правило, деякі IPv4 -адреси з пулу привласнюються мережевим пристроям для постійного використання. Отже, ці IPv4 -адреси не повинні привласнюватися іншим пристроям. Щоб виключити певні адреси, використовується команда ip dhcp excluded - address. Можна виключити одну адресу або діапазон адрес, задавши адреси нижнього і верхнього меж діапазону. До числа виключених адрес повинні входити адреси, присвоєні маршрутизаторам, серверам, принтерам і іншим пристроям, сконфігурованим вручну.

Крок 2. Налаштування адресного пулу DHCPv4

При виконанні налаштування DHCPv4 -сервера задається пул адрес, призначених для розподілу. Команда ip dhcp pool pool - name створює пул із заданим ім’ям і переводить маршрутизатор в режим конфігурації протоколу DHCPv4, який визначається рядком Router(dhcp - config)#.

Крок 3. Налаштування конкретних завдань

Пул адрес і основний шлюз маршрутизатора мають бути налагоджені. Використовуйте команду network для визначення діапазону доступних адрес.

Використовуйте команду default - router, щоб задати основний шлюз маршрутизатора. Шлюзом зазвичай виступає інтерфейс LAN маршрутизатора, найближчого до клієнтських пристроїв. Потрібен лише один шлюз, але за наявності декількох шлюзів можна перерахувати аж до 8 адрес.

Інші команди DHCPv4 -пула є додатковими. Наприклад, IPv4 -адреса DNS -сервера, доступна DHCPv4 -клієнту, налаштовується за допомогою команди dns - server. Для того, щоб задати доменне ім’я, використовуйте команду domain – name domain. Тривалість оренди протоколу DHCPv4 змінюється командою lease. За замовчуванням тривалість оренди дорівнює одному дню. Щоб задати сервер NetBIOS WINS, використовується команда netbios - name - server.

У версіях Cisco IOS, що підтримують використання DHCPv4, служба DCHPv4 за замовчуванням включена. Для того, щоб відключити службу, використовується команда в режимі глобальної конфігурації no service dhcp. Для відновлення роботи DHCPv4 -сервера використовується команда в режимі глобальної конфігурації service dhcp. У разі, якщо параметри не налагоджені, активація служби не має ефекту.

17.5. DHCPv4-ретрансляція

У складній ієрархічній мережі корпоративні сервери зазвичай розташовуються в серверній фермі. Ці сервери можуть надавати служби DHCP, DNS, TFTP і FTP. Клієнти мережі і сервери, як правило, знаходяться в різних підмережах. Для визначення місця розташування серверів і отримання послуг, клієнти часто використовують повідомлення широкомовної розсилки.

Налаштування допоміжної адреси дозволяє маршрутизатору пересилати широкомовні повідомлення DHCPv4 серверу DHCPv4. При пересилці запитів привласнення адреси/параметрів адреси маршрутизатор виступає агентом DHCPv4 -ретрансляції.

DHCPv4 - не єдина служба, на ретрансляцію якої може бути конфігурований маршрутизатор. За замовчуванням команда ip helper – address переадресовує наступні вісім служб UDP:

- Порт 37: Time
- Порт 49: TACACS
- Порт 53: DNS
- Порт 67: DHCP/BOOTP client
- Порт 68: DHCP/BOOTP server
- Порт 69: TFTP
- Порт 137: NetBIOS name service
- Порт 138: NetBIOS datagram service.

17.6. Налаштування маршрутизатора в якості DHCPv4-клієнта

В деяких випадках маршрутизатори Cisco в невеликих або домашніх офісах (SOHO) і філіях мають бути налагоджені в якості DHCPv4 -клієнтів аналогічно налаштуванню клієнтських комп'ютерів. Використовуваний метод залежить від інтернет-провайдера. У простій конфігурації для з'єднання з кабельним або DSL -модемом використовується Ethernet -інтерфейс. Для налаштування Ethernet -інтерфейса в якості DHCP -клієнта використовується команда режиму налаштування інтерфейсу ip address dhcp.

Припустимо, що інтернет-провайдер (ISP) на рис.17.1.налагоджений для надання вибраним споживачам IP -адрес з мережевого діапазону 209.165.201.0/27. Після налаштування інтерфейсу G0/1 за допомогою команди ip address dhcp, команди show ip interface g0/1 підтверджують, що інтерфейс включений, а адреса отримана від DHCPv4 -сервера.


```
SOHO(config)# interface g0/1
SOHO(config-if)# ip address dhcp
SOHO(config-if)# no shutdown
SOHO(config-if)#
*Jan 31 17:31:11.507: %DHCP-6-ADDRESS_ASSIGN: Interface
GigabitEthernet0/1 assigned DHCP address 209.165.201.12, mask
255.255.255.224, hostname SOHO
SOHO(config-if)# end
SOHO# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 209.165.201.12/27
  Broadcast address is 255.255.255.255
  Address determined by DHCP
```

Рис. 17.1. Налаштування маршрутизатора в якості DHCPv4-клієнта [1]

17.7. Пошук і усунення неполадок DHCPv4

Існує безліч причин виникнення проблем в роботі протоколу DHCPv4: несправності ПЗ ОС, драйверів мережевого адаптера або агентів DHCP -ретрансляції. Проте найбільш поширеною причиною неполадок є неправильна конфігурація. Через велику кількість потенційних проблемних областей при пошуку і усуненні несправностей потрібен систематичний підхід.

1. Вирішення конфліктів IPv4 -адрес

У клієнта, підключеного до мережі, може закінчитись термін оренди IPv4 -адреси. Якщо клієнт не відновить оренду, DHCPv4 -сервер може перепризначувати цю IPv4 -адресу іншому клієнтові. Після перезавантаження клієнт запросить IPv4 -адресу. Якщо DHCPv4 -сервер не дасть відповідь досить швидко, клієнт використовуватиме IPv4 -адресу, що використалась востаннє. Виникає ситуація, коли два клієнти використовують одну IPv4 -адресу, створюючи конфлікт.

Команда show ip dhcp conflict відображає усі конфлікти адрес, зареєстровані DHCPv4 -сервером. Для виявлення клієнта сервером використовується команда ping. Для виявлення конфлікту клієнт використовує протокол дозволу адрес (ARP). При виявленні конфлікту адреса видаляється з пулу і не привласнюється до усунення конфлікту адміністратором.

Вихідні дані відображують IP -адреси, DHCP, що конфліктують з сервером. У даних вказаний метод виявлення (detection method) і час виявлення (detection time) конфліктуючих IP -адрес, запропонованих сервером DHCP:

R1# show ip dhcp conflict

IP address Detection Method Detection time

192.168.10.32 Ping Feb 16 2017 12:28 PM

192.168.10.64 Gratuitous ARP Feb 23 2017 08:12 AM

2. Перевірка фізичного з'єднання

Спочатку необхідно застосувати команду show interfaces interface, щоб переконатися, що інтерфейс маршрутизатора, діючий в якості основного шлюзу для клієнта, функціонує. Якщо статус інтерфейсу відрізняється від статусу up, трафік (включаючи запити DHCP -клієнта) не проходить через порт.

3. Перевірка зв'язності з використанням статичної IP -адреси

При проведенні робіт з пошуку і усунення неполадок будь-якої несправності DHCPv4, необхідно перевірити зв'язність шляхом налаштування статичної IPv4 -адресації на клієнтській робочій станції. Якщо робочої станції не вдається отримати доступ до мережевих ресурсів, незважаючи на наявність статично налагодженої IPv4 -адреси, DHCPv4 не є джерелом проблеми. В цьому випадку необхідно провести перевірку мережевого підключення.

4. Перевірка налаштування порту комутатора

У випадку якщо DHCPv4 -клієнт не може отримати IPv4 -адресу від DHCPv4 -сервера при завантаженні, варто спробувати отримати IPv4 -адресу від DHCPv4 -сервера, вручну відправивши DHCPv4 –запит з пристрою-клієнта.

5. Діагностика роботи протоколу DHCPv4 в тій же підмережі або VLAN

Важливо розрізняти, чи правильно функціонує DHCPv4 в якості DHCPv4 -сервера, коли клієнт знаходиться в тій же підмережі або VLAN. У випадку якщо протокол DHCPv4 працює коректно за умови, що клієнт знаходиться в тій же підмережі або VLAN, проблема може полягати в агентові DHCP -ретрансляції. Якщо неполадки зберігаються навіть при перевірці роботи DHCPv4 в тій же підмережі або VLAN в якості DHCPv4 -сервера, проблема зазвичай полягає в DHCPv4 -сервері.

17.8. Перевірка налаштувань DHCPv4 на маршрутизаторі

Коли DHCPv4 -сервер розташований в окремій від клієнта LAN, інтерфейс маршрутизатора, що відповідає клієнтові, має бути налаштований на ретрансляцію DHCPv4 -запитів за допомогою конфігурації допоміжної IPv4 -адреси. Якщо допоміжна IPv4 -адреса налагоджена невірно, клієнтські DHCPv4 -запити не пересилатимуться на DHCPv4 -сервер.

Для перевірки налаштувань маршрутизатора використовуються наступні дії.

Крок 1. Переконатися, що команда ip helper - address виконана на правильному інтерфейсі. Команда має бути виконана на вхідному інтерфейсі LAN, містить робочі станції DHCPv4 -клієнта, і спрямована на вірний DHCPv4 -сервер. Команда show ip interface також може використовуватися для перевірки роботи DHCPv4 -ретрансляції на інтерфейсі.

Крок 2. Переконатися, що не була виконана команда глобальної конфігурації no service dhcp. Ця команда відключає усі функціональні можливості DHCP -сервера і ретрансляції на маршрутизаторі. Команда service dhcp не відображується при виведенні поточної конфігурації, оскільки є налагодженою за замовчуванням.

Команда show running - config | include no service dhcp підтверджує, що служба DHCPv4 запущена, оскільки немає збігів для команди show running - config | include no service dhcp. Якщо служба була відключена, командano service dhcp буде відображена у вихідних даних.

Якщо маршрутизатор, сконфігурований в якості DHCPv4 -сервера, не отримує запити від клієнта, процес DHCPv4 не може бути виконаний. Необхідно виконати одне із завдань по пошуку і усуненню неполадок для підтвердження того, що маршрутизатор отримує DHCPv4 -запит від клієнта.

Іншою корисною командою для пошуку і усунення неполадок в роботі DHCPv4 являється команда debug ip dhcp server events. Команда надає звіт про події сервера, таких як призначення адреси або оновлення БД. Також за допомогою цієї команди можна декодувати прийом і передачу DHCPv4.

Висновок до лекції 17

Для взаємодії з іншими пристроями усім мережевим вузлам потрібна унікальна IP -адреса. Статичне призначення даних IP -адресації у великій мережі призводить до адміністративного навантаження, якого можна уникнути, використовуючи протоколи DHCPv4 або DHCPv6 для динамічного привласнення IPv4, - і IPv6 -адрес відповідно.

Протокол DHCPv4 має 3 різні механізми призначення адреси, що забезпечують гнучкість при привласненні IP -адрес: ручний розподіл, автоматичний розподіл, динамічний розподіл. Динамічне виділення – це найчастіше використовуваний механізм DHCPv4, що дозволяє здійснювати обмін декількома різними пакетами між DHCPv4 -сервером і DHCPv4 -клієнтом, що призводить до оренди діючої інформації про адресацію на зумовлений період часу.

Повідомлення від клієнта (DHCPDISCOVER, DHCPREQUEST) є повідомленнями широкомовної розсилки, що дозволяє усім DHCPv4 -серверам в мережі дізнатися про запит клієнта і прийом клієнтом інформації про адресацію. Повідомлення від сервера DHCPv4 (DHCPOFFER, DHCPACK), посилаються як одноадресна розсилка безпосередньо клієнтові, що просить цю інформацію.

Якщо DHCP -сервер розташований в різних мережах з DCHP -клієнтом, необхідно налаштувати агент ретрансляції. Агент ретрансляції направляє спеціальні повідомлення широкомовною розсилкою з сегменту LAN на певний сервер, розташований в іншому сегменті LAN (в цьому випадку DHCP повідомлення широкомовної розсилки буде перенаправлене на сервер DHCP).

Пошук і усунення неполадок в роботі DHCPv4 і DHCPv6 включає однакові завдання:

- вирішення конфліктів адрес;
- перевірка фізичного з’єднання;

- перевірка зв’язності з використанням статичної IP -адреси;
- перевірка конфігурації порту комутатора;
- перевірка роботи протоколу в тій же підмережі або VLAN.

Питання для закріплення

1. Яке призначення протоколу DHCP?
2. У чому полягає операція DHCPv4?
3. Який формат повідомлень DHCPv4?
4. Як налаштувати простий DHCPv4 –сервер?
5. Що таке DHCPv4-ретрансляція?
6. Як налаштувати маршрутизатор в якості DHCPv4-клієнта?
7. Як відбувається пошук і усунення неполадок DHCPv4?
8. У чому полягає перевірка налаштувань DHCPv4 на маршрутизаторі?

Список рекомендованої літератури

1. CCNA R&S RSE Chapter 10: DHCP // Електронний ресурс. Режим доступу: https://static-course-assets.s3.amazonaws.com/RSE50ENU/module10/index.html#10.0.1.1
2. Автоматичне налаштування мережі (DHCP) // Електронний ресурс. Режим доступу: https://www.freebsd.org/doc/ru_RU.KOI8-R/books/handbook/network-dhcp.html
3. Протокол динамічного виділення адрес (DHCP) // Електронний ресурс. Режим доступу: http://help.ubuntu.ru

Лекція 18. Тема: «Технологія NAT»

План лекції

18.1. Визначення та необхідність використання технології NAT.
18.2. Термінологія NAT.
18.3. Механізми перетворення мережевих адрес.
18.4. Порівняння технологій NAT і PAT.
18.5. Переваги і недоліки NAT.
18.6. Налаштування статичного NAT.
18.7. Налаштування і перевірка динамічного NAT.
18.8. Налаштування та перевірка PAT.

18.1. Визначення та необхідність використання технології NAT

Усі публічні IPv4 -адреси, що підключаються до Інтернету, мають бути занесені в регіональний інтернет-реєстратор (RIR). Організації можуть орендувати публічні адреси у постачальника послуг, але тільки зареєстрований «власник» публічної інтернет-адреси може призначити цю адресу мережевому пристрою. Теоретично, максимально допустима кількість IPv4 -адрес складає 4,3 мільярда, що строго обмежує адресний простір IPv4. Коли в 1981 році Боб Кан (Bob Kahn) і Вінт Серф (Vint Cerf) розробили пакет протоколів TCP/IP, включаючи IPv4, вони не мали уявлення про те, на що перетвориться Інтернет.

З поширенням персональних комп’ютерів і настанням ери Всесвітньої мережі стало очевидно, що 4,3 мільярда IPv4 -адрес буде недостатньо. Поява протоколу IPv6 стала довгостроковим рішенням, проте разом з цим знадобилися швидші способи усунення

проблеми вичерпання адресного простору. IETF розробила ряд короткострокових рішень, у тому числі перетворення мережевих адрес (**NAT**, Network Address Translation) і приватні IPv4 -адреси відповідно до RFC 1918.

Кількості публічних IPv4 -адрес недостатньо, щоб призначити унікальні адреси усім пристроям, підключеним до Інтернету. В більшості випадків, мережі реалізуються з використанням приватних IPv4 -адрес відповідно до RFC 1918. Ці приватні адреси використовуються у рамках організації або об'єкту з метою забезпечення взаємодії пристроїв на локальному рівні. Але оскільки ці адреси не визначають конкретну компанію або організацію, приватні IPv4 -адреси не можна використовувати для маршрутизації через інтернет. Для того, щоб дозволити пристрою з приватною IPv4 -адресою доступ до пристроїв і ресурсів поза локальною мережею, приватну адресу спочатку необхідно перетворити в публічну адресу. NAT забезпечує перетворення приватних адрес в публічні адреси. Це дозволяє пристрою з приватною IPv4 -адресою діставати доступ до ресурсів поза своєю приватною мережею, включаючи ресурси, знайдені в Інтернеті. У поєднанні з приватними IPv4 -адресами, NAT продемонстрував свою доцільність відносно економії публічних IPv4 -адрес. Одна публічна IPv4 -адреса може спільно використовуватися сотнями, навіть тисячами пристроїв, для кожного з яких налагоджена унікальна приватна IPv4 -адреса.

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

Перетворення мережевих адрес NAT використовується в різних цілях, проте основним завданням цього механізму є збереження публічних IPv4 -адрес. Це досягається шляхом дозволу мережам використовувати приватні IPv4 -адреси для внутрішньої взаємодії і перетворення їх в публічні адреси тільки у разі потреби. Додаткова перевага NAT – підвищення міри конфіденційності і безпеки мережі пояснюється тим, що цей механізм приховує внутрішні IPv4 -адреси від зовнішніх мереж. Для маршрутизатора з підтримкою NAT можна налаштувати одну або декілька діючих публічних IPv4 -адрес. Ці публічні адреси відомі як **пул адрес NAT**. Коли внутрішній пристрій відправляє трафік за межі мережі, маршрутизатор з підтримкою NAT перетворює внутрішню IPv4 -адресу пристрою в публічну адресу з пулу NAT. Зовнішнім пристроям здається, що увесь трафік, що входить в мережу і виходить з неї, використовує публічні IPv4 -адреси з наданого пулу адрес.

Маршрутизатор NAT зазвичай працює на межі тупикової мережі. Тупикова мережа – це мережа, що використовує єдине з'єднання з сусідньою мережею, один вхдний маршрут і один витікаючий маршрут. Коли пристрою в тупиковій мережі потрібне з'єднання з пристроєм поза його мережею, пакет пересилається пограничному маршрутизатору. Пограничний маршрутизатор виконує процес NAT, перетворюючи внутрішню приватну адресу пристрою в публічну, зовнішню адресу, яка маршрутизується.

18.2. Термінологія NAT

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

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

У NAT передбачено 4 типи адрес:

- внутрішня локальна адреса;
- внутрішня глобальна адреса;
- зовнішня локальна адреса;
- зовнішня глобальна адреса.

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

- **Внутрішня адреса** - це адреса пристрою, що перетворюється механізмом NAT.
- **Зовнішня адреса** - це адреса пристрою призначення.

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

- **Локальна адреса** - це будь-яка адреса, що з'являється у внутрішній частині мережі.
- **Глобальна адреса** - це будь-яка адреса, що з'являється в зовнішній частині мережі.
- **Внутрішня локальна адреса** - це адреса джерела, видима з внутрішньої мережі.
- **Внутрішня глобальна адреса** - це адреса джерела, видима із зовнішньої мережі.
- **Зовнішня глобальна адреса** - це адреса призначення, видима із зовнішньої мережі. Це глобальна IPv4-адреса, що маршрутизується і призначена вузлу в Інтернеті.
- **Зовнішня локальна адреса** - це адреса призначення, видима з внутрішньої мережі.

18.3. Механізми перетворення мережевих адрес

Існують три механізми перетворення мережевих адрес.

- **Статичне перетворення мережевих адрес (статичний NAT)** - це взаємно-однозначна відповідність між локальним і глобальним адресами.
- **Динамічне перетворення мережевих адрес (динамічний NAT)** - це зіставлення адрес за схемою «багато до багатьох» між локальними і глобальними адресами.
- **Перетворення адрес портів (PAT)** - це зіставлення адрес за схемою «багато до одного» між локальними і глобальним адресами. Цей метод також називається NAT з перевантаженням.

Статичний NAT використовує зіставлення локальних і глобальних адрес за схемою «один в один». Ці відповідності задаються адміністратором мережі і залишаються незмінними.

Метод статичного перетворення мережевих адрес особливо корисний для веб-серверів або пристроїв, які повинні мати постійну адресу, доступну з Інтернету, – наприклад, для веб-сервера компанії. Статичний NAT також підходить для пристроїв, які мають бути доступні авторизованому персоналу, що працює поза офісом, але при цьому залишатися закритими для загального доступу через інтернет. Наприклад, мережевий адміністратор може з ПК підключитися за допомогою SSH до внутрішньої глобальної адреси 209.165.200.226. Маршрутизатор перетворить цю внутрішню глобальну адресу у внутрішню локальну адресу і підключає сеанс адміністратора до 209.165.200.226.

Для статичного NAT потрібна достатня кількість публічних адрес, доступних для загальної кількості одночасних сеансів користувачів.

Метод динамічного перетворення мережевих адрес (динамічний NAT) використовує пул публічних адрес, які привласнюються у порядку живої черги. Коли внутрішній пристрій просить доступ до зовнішньої мережі, динамічний NAT привласнює доступну публічну IPv4 -адресу з пулу.

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

За допомогою цього методу багато адрес можуть бути зіставлені одному або декільком адресам, оскільки кожна приватна адреса також відстежуються за номером порту. Якщо пристрій починає сеанс TCP/IP, він створює значення порту TCP або UDP для джерела, щоб унікальним чином визначити сеанс. Коли маршрутизатор NAT отримує пакет від клієнта, він використовує свій номер порту джерела, щоб унікальним чином визначити конкретне перетворення NAT.

PAT гарантує, що пристрої використовуватимуть різні номери портів TCP для кожного сеансу взаємодії з сервером в Інтернеті. При поверненні відповіді від сервера номер порту

джерела, яке стає номером порту призначення при зворотній передачі, визначає, якому пристрою маршрутизатор перешле відповідні пакети. Процес PAT також переконується в тому, що вхідні пакети дійсно були запрошені, підвищуючи таким чином міру безпеки сеансу.

18.4. Порівняння технологій NAT і PAT

Сформульовані нижче відмінності між NAT і PAT допоможуть зрозуміти особливості кожного з цих методів перетворення мережевих адрес. NAT перетворює IPv4 -адреси, виходячи з схеми 1:1 для приватних IPv4 -адрес і публічних IPv4 -адрес. В той же час, PAT міняє і адресу, і номер порту.

NAT пересилає вхідні пакети за їх внутрішнім призначенням, використовуючи IPv4 -адресу вхідного джерела, надану вузлом в публічній мережі. При використанні PAT зазвичай задіюється тільки одна або невелика кількість публічно представлених IPv4 -адрес. Вхідні пакети з публічної мережі спрямовуються адресатам в приватній мережі за допомогою таблиці маршрутизатора NAT. Ця таблиця відстежує пари публічних і приватних портів, що називається відстежуванням з'єднань. Що ж відбувається з пакетами IPv4, що передають дані, що не є сегментом TCP або UDP? Ці пакети не містять номера порту 4 рівня. PAT перетворить більшість основних протоколів, що передаються за допомогою IPv4 і що не використовують TCP або UDP, в протокол транспортного рівня. Найпоширенішим серед таких протоколів є протокол ICMPv4. Процес перетворення PAT обробляє кожен з цих протоколів по-різному. Наприклад, повідомлення запитів ICMPv4, exo-запити і exo-відповіді містять ідентифікатор запиту (Query ID). ICMPv4 використовує ідентифікатор запиту (Query ID), щоб визначити exo-запит з відповідною відповіддю. Ідентифікатор запиту збільшується з кожним відправленим exo-запитом. PAT використовує ідентифікатор запиту замість номера порту 4 рівня.

18.5. Переваги і недоліки NAT

NAT забезпечує багато переваг, у тому числі наступні.

- NAT зберігає офіційно зареєстровану схему адресації, дозволяючи приватне використання внутрішніх мереж. NAT економить адреси завдяки мультиплексуванню застосувань на рівні портів. При використанні NAT з перевантаженням внутрішні вузли можуть використовувати для усіх зовнішніх взаємодій одну публічну IPv4 -адресу. При цьому типі конфігурації для підтримки багатьох внутрішніх вузлів потрібна невелика кількість зовнішніх адрес.
- NAT підвищує гнучкість підключень до публічної мережі. Для забезпечення надійних підключень до публічної мережі можна створити множинні пули, резервні пули і пули розподілу навантаження.
- NAT забезпечує узгодженість схем внутрішньої мережевої адресації. Якщо в мережі не використовуються приватні IPv4 -адреси і NAT, зміна схеми публічних IPv4 -адрес зажадає зміни адрес усіх вузлів існуючої мережі. Витрати на зміну адресації вузлів можуть виявитися істотними. NAT дозволяє зберегти існуючу схему приватних IPv4 -адрес, одночасно підтримуючи простий перехід на нову схему публічної адресації. Це означає, що організація може змінити інтернет-провайдера, не міняючи налаштувань своїх внутрішніх клієнтів.
- NAT забезпечує безпеку мережі. Оскільки приватні мережі не оголошують ні свої адреси, ні внутрішню топологію, вони залишаються достатньо захищеними при використанні NAT для дістування керованого зовнішнього доступу. Проте, NAT не замінює міжмережеві екрани.

Перетворення мережевих адрес (NAT) має ряд недоліків. Той факт, що вузли в Інтернеті взаємодіють безпосередньо з пристроєм, що підтримує NAT, а не з фактичним вузлом приватної мережі, створює ряд проблем. Один з недоліків використання NAT пов'язаний з

продуктивністю мережі, особливо це стосується протоколів реального часу, таких як VoIP. NAT збільшує затримки комутації, оскільки перетворення кожної IPv4 -адреси в заголовках пакетів вимагає часу. Комутація першого пакету є програмним процесом – цей пакет завжди проходить повільнішим шляхом. Маршрутизатор повинен аналізувати кожен пакет, щоб вирішити, чи потрібно його перетворювати. Маршрутизатор повинен змінити заголовок IPv4 і, по можливості, змінити заголовок TCP або UDP. При кожному перетворенні має бути перерахована контрольна сума заголовка IPv4, а також контрольна сума TCP або UDP. Якщо в кеші є відповідний запис, інші пакети проходять по дорозі зі швидкою комутацією. Інакше вони теж затримуються. Іншим недоліком використання NAT є втрата наскрізної адресації. Багато інтернет-протоколів і застосувань залежать від наскрізної адресації від джерела до вузла призначення. Деякі застосування не сумісні з NAT. Наприклад, деякі застосування безпеки, такі як електронні підписи, не працюють з NAT, оскільки IPv4 -адреса джерела змінюється, перш ніж пакет встигає досягти вузла призначення. Застосування, що використовують фізичні адреси замість доменних імен, не можуть досягти вузлів призначення, при проходженні через маршрутизатор, що використовує NAT. В деяких випадках цієї проблеми можна уникнути за допомогою статичних зіставлень NAT.

Крім того, втрачається можливість трасування наскрізного з'єднання IPv4. Дуже сильно ускладнюється трасування пакетів, що піддаються численним змінам адреси пакету при проходженні декількох ділянок NAT, що, у свою чергу, утрудняє усунення неполадок.

Використання NAT також ускладнює протоколи туннелювання, такі як IPsec, оскільки NAT змінює значення в заголовках, що заважає перевіркам цілісності, що виконує протокол IPsec та інші протоколи тунелювання.

Робота служб, що вимагають ініціалізації з'єднань TCP із зовнішньої мережі або використовують протоколи без урахування стану, наприклад, на основі UDP, може бути порушена. Якщо на маршрутизаторі NAT не налагоджена підтримка таких протоколів, вхідні пакети не зможуть досягти свого призначення. Деякі протоколи можуть підтримувати один екземпляр NAT між вузлами-учасниками (наприклад, FTP в пасивному режимі), але не працюють, якщо обидві системи відокремлені від Інтернету за допомогою NAT.

18.6. Налаштування статичного NAT

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

Налаштування статичного NAT зв'язане з двома основними завданнями.

Крок 1. Першим завданням є створення відповідності між внутрішньою локальною і внутрішньою глобальною адресами.

Крок 2. Після налаштування відповідності інтерфейси, що беруть участь у перетворенні, налаштовуються як внутрішні або зовнішні відносно NAT.

На рис. 18.1. пакети, що поступають на внутрішній інтерфейс маршрутизатора R2 (Serial 0/0/0) від налагодженої внутрішньої локальної IPv4 -адреси (192.168.10.254) перетворяться, а потім передаються в зовнішню мережу. Пакети, що поступають на зовнішній інтерфейс маршрутизатора R2 (Serial 0/1/0), адресовані налагодженій внутрішній глобальній IPv4 -адресі (209.165.201.5), перетворяться у внутрішню локальну адресу (192.168.10.254) і потім передаються у внутрішню мережу.

```
Establishes static translation between an inside local address and
an inside global address.
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5

R2(config)# interface Serial0/0/0
R2(config-if)# ip address 10.1.1.2 255.255.255.252
Identifies interface serial 0/0/0 as an inside NAT interface.
R2(config-if)# ip nat inside
R2(config-if)# exit

R2(config)# interface Serial0/1/0
R2(config-if)# ip address 209.165.200.225 255.255.255.224
Identifies interface serial 0/1/0 as the outside NAT interface.
R2(config-if)# ip nat outside
```

Рис.18.1. Приклад конфігурації статичного NAT [1]

На рис.18.1 показані команди, необхідні для створення на маршрутизаторі R2 статичного зіставлення NAT для веб-сервера. У рамках показаної конфігурації R2 перетворить в пакетах, відправлених веб-сервером, адреси 192.168.10.254 в публічну IPv4 -адресу 209.165.201.5. Інтернет-клієнт направляє веб-запити на публічну IPv4 -адресу 209.165.201.5. Маршрутизатор R2 пересилає цей трафік веб-серверу за адресою 192.168.10.254.

Для перевірки роботи NAT використовується команда show ip nat translations. Ця команда відображає активні перетворення NAT. На відміну від динамічних перетворень, статичні перетворення завжди присутні в таблиці NAT. Якщо команда вводиться під час активного сеансу, вихідні дані також міститимуть адресу зовнішнього пристрою.

Іншою корисною командою є show ip nat statistics. Щоб переконатися у правильності роботи перетворення NAT, перед тестуванням рекомендується очистити статистику усіх попередніх перетворень за допомогою команди clear ip nat statistics.

До початку взаємодії з веб-сервером команда show ip nat statistics не повинна показувати які-небудь збіг. Після установки клієнтом сеансу з веб-сервером результат команди show ip nat statistics покаже збільшення кількості збігів до 5. Це підтверджує виконання статичного перетворення NAT на мапшрутизаторі.

18.7. Налаштування і перевірка динамічного NAT

Тоді як статичне перетворення NAT забезпечує постійну відповідність між внутрішньою локальною і внутрішньою глобальною адресою, динамічне перетворення NAT підтримує автоматичне зіставлення внутрішніх локальних адрес внутрішнім глобальним адресам. Ці внутрішні глобальні адреси зазвичай являються публічними IPv4 -адресами. Динамічний NAT використовує для перетворення групу або пул публічних IPv4 -адрес.

Для динамічного NAT, як і для статичного NAT, потрібне налаштування внутрішнього і зовнішнього інтерфейсів, що беруть участь в перетворенні NAT. Проте, якщо статичне перетворення NAT створює постійне зіставлення з однією адресою, для динамічного NAT використовується пул адрес.

Примітка. Перетворення між публічними і приватними IPv4 -адресами є найпоширенішим застосуванням NAT. Проте, перетворення NAT можуть виникати між будь-якими парами адрес.

Пул публічних IPv4 -адрес (пул внутрішніх глобальних адрес) доступний будь-якому пристрою у внутрішній мережі за принципом «першим прийшов – першим обслужили». При динамічному перетворенні NAT одна внутрішня адреса перетвориться в одну зовнішню адресу. Для цього типу перетворення в пулі має бути досить адрес, щоб охопити усі внутрішні пристрої, яким одночасно потрібен доступ до зовнішньої мережі. Якщо використані усіх адреси пулу, пристрій повинен дочекатися доступної адреси, щоб дістати доступ до зовнішньої мережі.

Крок 1. За допомогою команди ip nat pool необхідно створити пул адрес, які використовуватимуться для перетворення. Цей пул адрес зазвичай є групою публічних адрес. Ці адреси визначаються за допомогою вказівки початкового і кінцевого IP -адрес пулу. Ключове слово netmask або prefix - length вказує, які біти адреси відносяться до мережі, а які – до діапазону адрес вузлів.

Крок 2. Налаштувати стандартний ACL -список, щоб визначити (дозволити) тільки ті адреси, які мають бути перетворені. ACL -список із занадто великою кількістю дозволяючих команд може привести до непередбачуваних результатів. У кінці кожного ACL -списка знаходиться рядок deny all.

Крок 3. Виконати прив'язку ACL -списка до пулу. Команда ip nat inside source list access - list - number number poolpool name використовується для прив'язки списку до пулу. Ця конфігурація використовується маршрутизатором, щоб визначити, які пристрої (list) отримують які адреси (pool).

Крок 4. Визначити інтерфейси, що є внутрішніми по відношенню до NAT, тобто будь-який інтерфейс, підключений до внутрішньої мережі.

Крок 5. Визначити інтерфейси, що є зовнішніми відносно NAT, тобто будь-який інтерфейс, підключений до зовнішньої мережі.

Результати команди show ip nat translations відображають усі налагоджені статичні перетворення адрес і усі динамічні перетворення, створені в результаті обробки трафіку.

За замовчуванням термін дії записів перетворення збігає через 24 години, якщо налаштування таймерів не було змінене за допомогою команди ip nat translation timeout timeout - seconds в режимі глобальної конфігурації.

Для видалення динамічних записів до витікання їх часу дії використовується команда режиму глобальною конфигурації clear ip nat translation. При проведенні перевірки конфігурації NAT рекомендується видаляти динамічні записи. Цю команду можна використовувати з ключовими словами і змінними, щоб визначити записи, що видаляються. Конкретні записи можна видалити щоб уникнути збоїв активних сеансів. Щоб видалити з таблиці усі перетворення, використовується команда глобальної конфігурації clear ip nat translation.

Примітка. З таблиці віддаляються тільки динамічні перетворення. Статичні перетворення неможливо видалити з таблиці перетворень.

Команда show ip nat statistics виводить відомості про сумарну кількість активних перетворень, параметри конфігурації NAT, число адрес в пулі а число виділених адрес.

В якості альтернативи, можна скористатися командою show running - config і знайти команди NAT, ACL, інтерфейсу або пулу з потрібними значеннями.

18.8. Налаштування та перевірка PAT

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

Примітка. Сумарне число внутрішніх адрес, які можуть бути перетворені в одну зовнішню адресу, теоретично може досягати 65 536 на одну IP -адресу. Але число внутрішніх адрес, яким можна призначити одну IP -адресу, приблизно складає 4000.

Залежно від того, яким чином інтернет-провайдер виділяє публічні IPv4 -адреси, існує два способи налаштування PAT. У першому випадку інтернет-провайдер виділяє організації декілька публічних IPv4 -адрес, а в другому випадку виділяється єдина публічна IPv4 - адреса, необхідна організації для підключення до мережі інтернет-провайдера.

Якщо об'єкту було виділено декілька публічних IPv4 -адрес, то ці адреси можуть бути частиною пулу, що використовує PAT. Це аналогічно динамічному NAT, за винятком того, що публічних адрес недостатньо для створення взаємно-однозначних відповідностей внутрішніх і зовнішніх адрес. Невеликий пул адрес спільно використовується великим числом пристроїв.

Якщо доступна тільки одна публічна IPv4 -адреса, для конфігурації з перевантаженням зазвичай призначається публічна адреса зовнішнього інтерфейсу, яка підключається до інтернет-провайдера. Усі внутрішні адреси в пакетах, що виходять із зовнішнього інтерфейсу, перетворяться в одну IPv4 -адресу.

Процес перетворення NAT з перевантаженням є однаковим як при використанні пулу адрес, так і при використанні однієї адреси.

Для перевірки PAT використовуються ті ж команди, що і для перевірки статичного і динамічного NAT. Команда show ip nat translations виводить перетворення для трафіку від двох різних вузлів до різних веб-серверів.

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

Як правило, для роботи однорангових програм обміну файлами і виконання таких операцій, як веб-обслуговування і витікаючий FTP, вимагається, щоб порти маршрутизатора були переадресовані або відкриті. Оскільки NAT приховує внутрішні адреси, однорангові застосування працюють тільки зсередини – в цьому випадку NAT може зіставити вихідні запити і вхідні відповіді. Проблема полягає в тому, що NAT не дозволяє ініціювати запити зовні. Цю ситуацію можна вирішити за допомогою змін, внесених вручну. Можна налаштувати переадресацію портів, щоб визначити конкретні порти, які можуть бути переадресовані на внутрішні вузли.

Інтернет-застосування працюють з користувацькими портами, які мають бути відкриті або доступні цим застосуванням. Різні застосування використовують різні порти. Це дозволяє застосуванням і маршрутизаторам визначати мережеві сервіси. Якщо потрібно інший номер порту, його можна додати до URL -адреси, відокремивши двокрапкою (:). Наприклад, якщо веб-сервер прослуховує порт 8080, користувач повинен ввести http://www.example.com: 8080.

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

Реалізація переадресації портів за допомогою команд IOS аналогічна застосуванню команд налаштування статичного NAT. Переадресація портів фактично є статичним перетворенням NAT із заданим номером порту TCP або UDP.

Як і для інших типів NAT, для переадресації портів необхідно налаштувати як внутрішній, так і зовнішній інтерфейси NAT.

Аналогічно статичному NAT, для перевірки переадресації портів, можна використовувати команду show ip nat translations.

З початку 1990-х рр. пріоритетним завданням для IETF стало вирішення проблеми вичерпання адресного простору IPv4. Поєднання приватних IPv4 -адрес RFC 1918 і NAT стало інструментом, спрямованим на уповільнення процесу вичерпання. NAT має помітні

недоліки, і в січні 2011 IANA виділила для регіональних інтернет-реєстраторів свої останні IPv4 -адреси.

Однією з «ненавмисних» переваг NAT для IPv4 стало те, що ця технологія приховує приватні мережі від публічного Інтернету. Перевагою NAT є забезпечення очевидного рівня безпеки шляхом заборони комп'ютерам з публічного Інтернету доступу до внутрішніх вузлів. Але цю технологію не можна вважати заміною правильної мережевої безпеки, наприклад, як це забезпечує міжмережевий екран.

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

Унікальні локальні IPv6 -адреси (unique local addresses, ULA) схожі на приватні адреси RFC 1918 в IPv4, але при цьому істотно відрізняються від них. Мета унікальних локальних адрес – забезпечити простір IPv6 -адрес для взаємодії в межах локального об'єкту. Це не означає ні надання додаткового простору IPv6 -адрес, ні забезпечення рівня безпеки. Унікальна локальна адреса використовує префікс FC00::/7, і тому перший гекстет знаходиться в діапазоні від FC00 до FDFF. Якщо префікс призначається локально, наступний 1 біт встановлений рівним 1. Сенс значення 0 буде визначений пізніше. Наступні 40 бітів – це глобальний ідентифікатор, за яким йде 16-бітовий ідентифікатор підмережі. Ці перші 64 біта об'єднуються для створення префікса унікальної локальної адреси. Це залишає 64 біта для ідентифікатора інтерфейсу або, згідно термінології IPv4 – вузлової частини адреси. Унікальні локальні адреси визначені в RFC 4193. Унікальні локальні адреси також називаються локальними IPv6 -адресами (не слід плутати з локальними IPv6 -адресами типу link - local) і мають ряд характеристик:

- можливість об'єднувати або приватно сполучати об'єкти, без яких-небудь конфліктів адрес або необхідності в зміні нумерації інтерфейсів, що використовують ці префікси;
- незалежність від інтернет-провайдера і можливість застосування з метою взаємодії усередині об'єкту без необхідності в підключенні до Інтернету;
- неможливість маршрутизації через інтернет, проте при випадковому «витіку» через маршрутизацію або DNS конфлікт з іншими адресами відсутній.

Унікальні локальні адреси не настільки прості, як адреси RFC 1918. На відміну від приватних IPv4 -адрес, IETF не прагнула використовувати різновид NAT для перетворення між унікальними локальними адресами і глобальними індивідуальними адресами IPv6.

Реалізація і потенційні сфери застосування унікальних локальних IPv6 -адрес все ще вивчається інтернет-співтовариством. Наприклад, IETF аналізує можливість створення префікса унікальних локальних адрес локально, використовуючи FC00::/8, або призначення його автоматично сторонньою організацією, починаючи з FD00:: /8.

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

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

Подвійний стек застосовується, коли пристрої використовують протоколи, пов'язані як з IPv4, так і з IPv6. Тунелювання для IPV6 – це процес інкапсуляції пакетів IPv6 в пакети IPv4. Цей метод дозволяє передавати пакет IPv6 по мережі, в якій використовується тільки протокол IPv4.

NAT для IPv6 слід використовувати не як довгострокову стратегію, а як тимчасовий механізм, що допомагає перейти з IPv4 на IPv6. З часом з'явилося декілька типів NAT для IPv6, включаючи NAT - PT (Network Address Translation - Protocol Translation, перетворення мережевих адрес - перетворення протоколів). IETF визнала технологію NAT - PT застарілою і порекомендувала використовувати її заміну - NAT64.

Якщо в середовищі NAT виникають проблеми підключення IPv4, пошук причин неполадок часто виявляється складним завданням. Перший крок при усуненні проблеми – виключити NAT як причину. Розглянемо дії для перевірки правиьної роботи NAT.

Крок 1. Залежно від конфігурації чітко визначити цілі і завдання NAT. На цьому етапі ви можете виявити проблему, пов'язану з конфігурацією.

Крок 2. За допомогою команди show ip nat translations переконатися, що таблиця перетворень містить правильні перетворення.

Крок 3. Використати команди clear і debug, щоб переконатися, що NAT працює належним чином. Перевірити, чи створюються динамічні записи знову після їх видалення.

Крок 4. Детально вивчити, що відбувається з перетвореним пакетом, і переконатися, що маршрутизатори використовують правильні маршрути для передачі пакету.

У простому мережевому середовищі доцільно відстежувати статистику NAT за допомогою команди show ip nat statistics. Команда show ip nat statistics виводить відомості про сумарну кількість активних перетворень, параметри конфігурації NAT, число адрес в пулі і числі виділених адрес. Проте в складнішому середовищі NAT, у разі декількох перетворень, ця команда не дозволяє чітко визначити проблему. Команда debug ip nat використовується, щоб перевірити роботу NAT шляхом виведення відомостей про кожен пакет, перетворений маршрутизатором. Команда debug ip nat detailed виводить опис кожного пакету, що розглядається в якості кандидата на перетворення. Крім того, ця команда виводить відомості про конкретні помилки і виключення, таких як неможливість виділити глобальну адресу. Команда debug ip nat detailed видає більше службових даних, ніж команда debug ip nat, але вона може надати детальні відомості, які можуть бути потрібні для пошуку і усунення проблеми NAT.

Висновок до лекції 18

NAT для IPv4 дозволяє мережевим адміністраторам використовувати простір приватних адрес RFC 1918, одночасно надаючи підключення до Інтернету з використанням однієї публічної адреси або обмеженого числа публічних адрес. NAT економить простір публічних адрес і значно скорочує адміністративні витрати при додаванні, переміщенні і зміні адрес. NAT і PAT можуть використовуватися для економії простору публічних адрес і створення приватних захищених внутрішніх мереж, не впливаючи на підключення до мережі інтернет-провайдера. NAT має певні недоліки – ця технологія негативно впливає на продуктивність, безпеку і мобільність пристроїв, а також на можливість наскрізного підключення. Тому NAT слід використовувати як короткочасне рішення проблеми вичерпання адрес до впровадження довготривалого рішення, яким є IPv6.

Питання для закріплення

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

Список рекомендованої літератури

1. CCNA R&S RSE Chapter 11: Network Address Translation for IPv4 // Електронний ресурс. Режим доступу: https://static-course-assets.s3.amazonaws.com/RSE50ENU/module11/index.html
2. NAT на Cisco // Електронний ресурс. Режим доступу: https://habrahabr.ru/post/108931/
3. How Network Address Translation Works // Електронний ресурс. Режим доступу: http://computer.howstuffworks.com/nat.htm