Міністерство освіти і науки України

КОМП’ЮТЕРНІ МЕРЕЖІ

Конспект лекцій для здобувачів першого (бакалаврського) рівня
вищої освіти освітньої програми «Комп’ютерна інженерія»
галузь знані 12 (F) Інформаційні технології
спеціальності 123 (F7) Комп’ютерна інженерія
денної та заочної форм навчання

Луцьк 2026

УДК 004.65(07)
Б17

Рекомендовано до видання вченою радою факультету КІТ ЛНТУ,
протокол № _____ від « _____ « _____ 20 26 року.

Голова вченої ради факультету КІТ _____ Інна КОНДІУС

Електронна копія друкованого видання передана для внесення в репозитарій ЛНТУ

Директор бібліотеки _____ Наталія ПОЛІЩУК

Розглянуто і схвалено на засіданні кафедри комп'ютерної інженерії та безпеки
ЛНТУ, протокол № _____ від « _____ « _____ 20 26 року.

Завідувач кафедри КІБ _____ Тарас ТЕРЛЕЦЬКИЙ

Укладач: _____ Наталія БАГНЮК, кандидат технічних наук,
доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ
_____ Дар'я ГОРДЄЄВА, кандидат економічних наук,
доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

Рецензент: _____ Олександр РОЙКО, кандидат технічних наук,
голова циклової комісії комп'ютерної та програмної інженерії
відокремленого структурного підрозділу «Волинський фаховий коледж
Національного університету харчових технологій»
Відповідальний за випуск: _____ Тарас ТЕРЛЕЦЬКИЙ, кандидат
технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

К17 Комп'ютерні мережі: конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Комп'ютерна інженерія» галузі знань 12 (F) Інформаційні технології спеціальності 123 (F7) Комп'ютерна інженерія денної та заочної форм навчання / уклад. Н. В. Багнюк, Д. В. Гордєєва. Луцьк: ЛНТУ, 2026 116 с.

Конспект лекцій з дисципліни «Комп'ютерні мережі» складено відповідно до діючої програми курсу.

Призначене для здобувачів вищої освіти спеціальності 123 (F7) Комп'ютерна інженерія освітньої програми «Комп'ютерна інженерія».

ЗМІСТ

ВСТУП

Конспект лекцій з дисципліни «Комп’ютерні мережі» розроблено відповідно до чинної освітньої програми підготовки здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 123 (F7) «Комп’ютерна інженерія». Матеріал конспекту спрямований на формування у студентів системного розуміння принципів побудови комп’ютерних мереж, їх архітектури, протоколів взаємодії, механізмів адресації, маршрутизації та комутації, а також засобів віртуалізації, автоматизації й мережевої безпеки.

Стрімкий розвиток інформаційних технологій, цифровізація суспільства та зростання обсягів передавання даних зумовили провідну роль комп’ютерних мереж у сучасному світі. Сьогодні мережеві технології є основою функціонування Інтернету, корпоративних інформаційних систем, хмарних сервісів, систем дистанційного навчання, електронного урядування та кіберфізичних систем. Уміння проєктувати, налаштовувати, адмініструвати й забезпечувати безпеку комп’ютерних мереж є однією з ключових компетентностей фахівця з комп’ютерної інженерії.

У конспекті послідовно розглянуто основні етапи розвитку комп’ютерних і телекомунікаційних мереж, класифікацію мереж, моделі OSI та TCP/IP, принципи фізичної й логічної адресації, топології мереж, роботу протоколів різних рівнів, особливості локальних, глобальних і бездротових мереж, технології VLAN, VPN, а також сучасні підходи до віртуалізації та автоматизації мережевої інфраструктури. Окрему увагу приділено питанням мережної безпеки, контролю доступу та захисту інформації.

Матеріал подано у логічно впорядкованому вигляді з урахуванням поступового ускладнення тем, що дає змогу студентам поетапно засвоювати теоретичні основи та готуватися до практичного застосування знань у лабораторних роботах і майбутній професійній діяльності. Конспект може бути використаний для підготовки до лекційних занять, самостійної роботи, виконання контрольних заходів і підсумкової атестації.

Тема 1 Вступ до мереж

Основні поняття та характеристики мереж. Етапи розвитку комп'ютерних та телекомунікаційних мереж. Класифікація комп'ютерних мереж. Загальні принципи побудови комп'ютерних мереж. Мережеві топології та їх характеристики. Поняття фізичної та логічної топології. Локальні мережі. Основні компоненти локальної мережі. Канали і лінії зв'язку. Кабельні системи. Характеристики ліній зв'язку. Мережеві пристрої.

Однією із суттєвих причин, які прискорили появу комп'ютерів, була потреба в розв'язуванні дуже широкого спектра задач. Між комп'ютерами, які розв'язували схожі завдання, досить часто виникали проблеми обміну даними. Як наслідок, з'явилася ідея об'єднати обчислювальні ресурси різних комп'ютерів, тобто ідея створення комп'ютерної мережі [1]..

Комп'ютерна мережа – це сукупність пристроїв, з'єднаних каналами передавання даних, для спільного користування апаратними, програмними та інформаційними ресурсами під керуванням спеціального програмного забезпечення.

Вузол мережі (англ. Node) – це пристрій, з'єднаний з іншими пристроями через мережу. Вузлами можуть бути комп'ютери, мобільні телефони, кишенькові комп'ютери та спеціальні мережні пристрої.

Призначенням комп'ютерних мереж є забезпечення [1].:

– швидкого обміну даними між окремими комп'ютерами мережі;

– спільного використання комп'ютерних програм і даних;

– спільної роботи користувачів над проєктами;

– віддаленого керування комп'ютерами;

– спільного доступу до периферійних пристроїв (принтерів, сканерів, зовнішньої пам'яті);

– спільного доступу до інформаційних ресурсів.

У комп'ютерній мережі комп'ютери можуть виконувати різні функції.

Комп'ютер, який керує розподілом ресурсів мережі, називають сервером (від англ. server − той, хто подає). Комп'ютери, які користуються ресурсами мережі, називають клієнтами або робочими станціями.

Залежно від завдань, які виконують комп'ютери, мережі розрізняють за територією, типом операційної системи, розподілом функцій, інфраструктурою та місцем розташування технічних засобів, які входять у мережу, та ін.

У 1961 році американський інженер українського походження Леонард Клейнрок запропонував ідею пакетної комутації, яка наразі є основою передавання даних мережею. А в 1964 році виклав основні принципи та розробив теорію.

Американського вченого Джозефа К. Р. Ліклайдера часто називають духовним батьком Інтернету. У 1962 році в низці статей він виклав свою концепцію «Галактичної мережі» − прообраз сучасного Інтернету.

Схему класифікації комп'ютерних мереж за різними ознаками наведено на рисунку 1.1.

Розглянемо класифікацію комп'ютерних мереж детально [1].

За територією мережі поділяються таким чином:

– персональні (PAN, від англ. Personal Area Network − мережа особистого простору, персональна мережа) − мережі для взаємодії пристроїв, що належать одній людині та об'єднують її власні електронні пристрої: персональні комп'ютери, ноутбуки, планшети, смартфони, комунікатори;

– локальні (LAN, від англ. Local Area Network − мережа локального простору) − з'єднують пристрої, розташовані на порівняно невеликій відстані один від одного, зазвичай у межах однієї або кількох сусідніх будівель, наприклад мережа навчального закладу;

– міські, регіональні (MAN, від англ. Metropolitan Area Network − мережа міського простору) − обласні й національні мережі;

– глобальні (WAN, від англ. Wide Area Network − мережа широкого простору) − об’єднують комп’ютерні мережі. Найвідомішою глобальною мережею є Інтернет [1].

Рисунок 1.1 – Класифікація мереж [1]

Сучасні операційні системи (ОС) поділяються на спеціалізовані та мережеві.

Спеціалізовані ОС призначені для роботи з мережевим обладнанням певної компанії. Так, Cisco IOS (англ. Internetwork Operating System − міжмережева ОС) працює виключно з маршрутизаторами й комутаторами компанії Cisco, а ZyNOS − ОС компанії ZyXEL, працює з маршрутизаторами Prestige [1].

За розподілом функцій між комп’ютерами мережі поділяють на однорангові й клієнт-серверні.

2. Мережеві топології

Комп’ютерні мережі поділяються також за топологією.

Мережна топологія визначає структуру мережі. В топології мережі можна виділити дві складові. Перша − це фізична топологія, яка визначає шлях прокладки кабелю та середовище передачі. Друга – це логічна топологія, що визначає, яким чином хости мають доступ до середовища передачі даних.

Існують три базові топології («загальна шина», «кільце», «зірка») та додаткові, що є модифікацією або поєднанням базових, наприклад топологію «дерево» можна розглядати як комбінацію декількох «зірок».

Кожна топологія накладає певні вимоги [1].

Топологія «загальна шина» передбачає використання одного кабелю, до якого під’єднуються всі комп’ютери мережі (рис. 1.2). Надіслане з будь-якого комп’ютера мережі повідомлення поширюється на всі інші комп’ютери мережі. Кожний із них перевіряє, кому адресовано повідомлення. Опрацьовує повідомлення лише той комп’ютер, якому воно адресоване. Комп’ютери можуть передавати дані лише послідовно, оскільки лінія зв’язку одна і спільна. Всі комп’ютери мають рівні права, все обладнання є ідентичним.

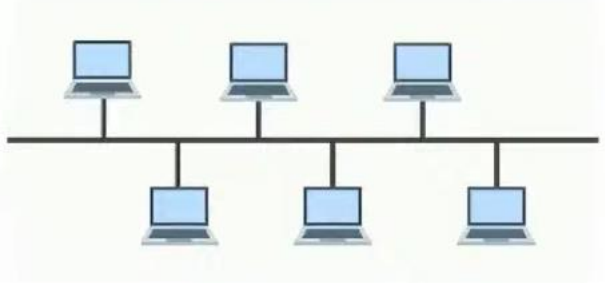

Рисунок 1.2 – Топологія шина

Топологія «кільце» − топологія, в якій кожен комп'ютер з'єднано лініями зв'язку лише з двома іншими (рис. 1.3): від одного він тільки отримує інформацію, а іншому тільки передає. Комп'ютери в «кільці» не є повністю рівноправними: одні обов'язково отримують інформацію від комп'ютера, який надсилає повідомлення в цей момент, раніше, а інші − пізніше.

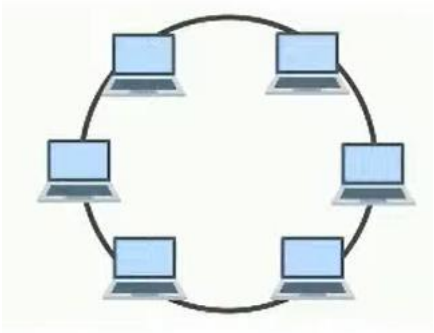

Рисунок 1.3 – Топологія кільце

У топології «зірка» всі комп'ютери мережі приєднано до центрального вузла (рис. 1.4), через який весь обмін інформацією йде від одного комп'ютера до іншого. Як центральний вузол можуть виступати концентратор чи комутатор − таку топологію називать пасивною «зіркою», або потужний комп'ютер, на який покладається дуже велике навантаження,− таку топологію називають активною «зіркою».

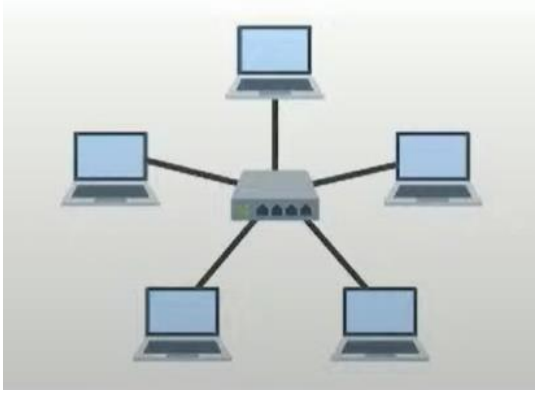

Рисунок 1.4 – Топологія зірка

Логічна топологія визначає як хости зв'язуються в мережі. Існує два основні види логічної топології: широкомовна (broadcast) та передача маркера (token passing) [2].

Broadcast в загальному розумінні означає, що кожен хост посилає дані, незалежно від інших хостів, в загальне мережеве середовище (моноканал), тобто випадково. Не існує порядку або правила, якому повинні слідувати робочі станції для використання мережі. Якщо першим відправив, то першим і обслуговується. Таким чином працює мережа Ethernet, яка розроблена компанією Xerox.

Другою логічною топологією є token passing. Token passing управляє доступом до мережі використовуючи електронні маркери, які передаються послідовно в одному напрямку від однієї робочої станції до іншої. Коли хост отримує маркер, то він починає передачу даних в мережу. Якщо, хост не готовий передавати інформацію, то у цьому випадку кадр маркера передається наступному хосту і процес знову повторюється. Прикладами мереж, які використовують маркерну передачу є : Token Ring (кільцева локальна мережа з маркерним доступом) та Fiber Distributed Data Interface (FDDI – оптоволоконний розподілений інформаційний інтерфейс, технологія побудови комп'ютерних мереж, що використовує для передачі сигналу оптоволоконний кабель).

Канали і лінії зв'язку. Кабельні системи. Характеристики ліній зв'язку.

Середовища передачі даних поділяються на [4]:

– середовища на мідній основі;

– оптоволоконні кабелі;

– безпровідні середовища.

До середовищ на мідній основі включають виту пару та коаксіальний кабель.

Вита пара − вид мережевого кабелю, з однією або декількома парами ізольованих провідників, скручених між собою (з невеликою кількістю витків на одиницю довжини) для зменшення взаємних наведень при передачі сигналу і покритих пластиковою оболонкою. Використовується для побудови мереж у багатьох технологіях, наприклад, Ethernet, ARCNet і Token ring. Останнім часом, завдяки своїй дешевизні й легкості установки, є найпоширенішим для побудови локальних мереж.

Підтримує передачу даних на відстань до 100 метрів. На більших відстанях сигнал через загасання не розпізнається; якщо передача даних на більшу відстань все ж таки необхідна, потрібно скористатися повторювачем, або ж задіяти коаксіальний кабель.

Залежно від наявності захисту − електрично заземленої мідної сітки або алюмінієвої фольги навколо скручених пар, визначають різновиди цієї технології:

1. Екранована вита пара (Shielded twisted pair, STP). Для захисту сигналу від шумів та спотворень використовується ефект взаємокомпенсації, екранування та попарне скручення проводів. Фізичні характеристики такого кабелю наступні:

– хвильовий опір − 150 Ом;

– пропускна здатність − до 100 Мб/с;

– рекомендована довжина фізичного сегменту − до 100 м.

Такий кабель забезпечує добрий захист від електромагнітних та радіочастотних наводок, але є порівняно дорогим та важким у прокладанні.

2. Екранована вита пара (Screened twisted pair, ScTP, Foiled twisted pair, FTP).

Володіє практично такими ж захисними властивостями, як і попередній. Фізичні характеристики:

– хвильовий опір 100-120 Ом;

– пропускна здатність до 100 Мб/с;

– рекомендована довжина фізичного сегменту − до 100 м.

Обидва вищеописані типи кабелю вимагають, щоб екрани були добре заземлені на обох кінцях, інакше замість екранування вони починають підсилювати зовнішні шуми.

3. Неекранована вита пара (Unshielded twisted pair, UTP).

Для зменшення впливу як зовнішніх так і внутрішніх шумів покладається лише на ефект взаємокомпенсації та попарне скручення проводів. Фізичні характеристики:

– хвильовий опір − 100 Ом;

– пропускна здатність − 100 і більше Мб/с (залежно від категорії кабелю);

– максимальна рекомендована довжина фізичного сегменту − до 100 м.

Перевагами використання цього кабелю є його дешевизна та легкість у прокладанні; недоліками − неможливість використання у зашумленому та агресивному середовищі.

Існує декілька категорій кабелю вита пара, які нумеруються від CAT1 до CAT7. Кабель вищої категорії зазвичай містить більше пар дротів і кожна пара має більше витків на одиницю довжини. Категорії неекранованої витої пари описуються в стандарті EIA/TIA 568 (Американський стандарт проводки в комерційних спорудах):

– CAT1 − телефонний кабель, всього одна пара. В США використовувався раніше, і провідники були скручені між собою. Використовується тільки для передачі голосу або даних за допомогою модему;

– CAT2 − старий тип кабелю з 2-х пар провідників, підтримував передачу даних на швидкостях до 4 Мбіт/с, використовувався в мережах token ring і ARCNet. Зараз іноді зустрічається в телефонних мережах;

– CAT3 − 2-парний кабель, використовувався для побудові локальних мереж 10BASE-T і token ring, підтримує швидкість передачі даних тільки до 10 Мбіт/с. На відміну

від попередніх двох, відповідає вимогам стандарту IEEE 802.3. Також дотепер зустрічається в телефонних мережах;

– CAT4 − кабель складається з 4-х скручених пар, використовувався в мережах token ring, 10BASE-T, 10BASE-T4, швидкість передачі даних не перевищує 16 Мбіт/с, зараз не використовується;

– CAT5 − 4-парний кабель, це і є те, що зазвичай називають кабель «вита пара». Завдяки високій швидкості передачі (до 100 Мбіт/с при використанні 2 пар і до 1000 Мбіт/с при використанні 4 пар) є найпоширенішим мережевим носієм, що використовується в ком-п'ютерних мережах дотепер. Для прокладки нових мереж користуються дещо вдосконаленим кабелем CAT5e, який краще пропускає високочастотні сигнали;

– CAT6 − Застосовується в мережах Fast Ethernet і Gigabit Ethernet, складається з 4 пар провідників і здатний передавати дані на швидкості до 10000 Мбіт/с. Доданий до стандарту в червні 2002 року, пропускає сигнали частотою до 200МГц. Існує категорія CAT6e, в якій збільшена частота сигналу, що пропускається, до 500МГц. За даними IEEE, 70% встановлених мереж у 2004 році використовували кабель категорії CAT6, проте, можливо, це просто данина моді, бо й кабелі CAT5 і CAT5e цілком справляються в мережах 10GBASE-T;

– CAT7 − Специфікація на цей тип кабелю поки що не затверджена, швидкість передачі даних − до 10000 Мбіт/с, частота сигналу, що пропускається, до 600-700 Мгц. Кабель цієї категорії екранований.

Вита пара широко застосовується в мережевих технологіях і комунікаціях; кабелем категорії 6 замінюють коаксіальний кабель. Незважаючи на велику захищеність екранованої витої пари, вона не набула широкого поширення через складність в установці − необхідне заземлення і кабель, порівняно з неекранованою звитою парою, жорсткіший.

Коаксіальний кабель

Коаксіальний кабель − електричний кабель із співвісними провідниками. На даний момент цей кабель вже досить рідко застосовується для прокладання комп'ютерних мереж, хоча широко використовується для інших технологій передачі даних (телебачення) [4].

Фізичні характеристики:

– хвильовий опір − 50 Ом;

– пропускна здатність − до 100 Мб/с;

– рекомендована довжина сегменту − до 185 м (тонкий коаксіал) та до 500 м (товстий коаксіал).

Мідне оплетення кабелю одночасно виступає і захисним екраном для центрального провідника, і другим провідником у кабелі. Він є досить дешевим, але вже не задовольняє сучасних вимог до комп'ютерних мереж через недосконалість фізичної топології, яку можна на ньому реалізувати.

Оптоволоконний кабель [4] служить середовищем передачі даних для модульованого електромагнітного випромінювання із певною, строго визначеною довжиною хвилі (світлових імпульсів). Його основною перевагою є значна швидкість передачі даних (до 10 Гб/с) та довжина фізичного сегменту (до 40 км) порівняно із середовищами на мідній основі, а також несприйнятливість до зовнішніх електромагнітних шумів. Однак цей кабель є значно дорожчим порівняно з іншими, а також більш складним у прокладанні.

Принципи передачі сигналу в оптоволоконному середовищі. Світло, яке є носієм сигналу у оптоволоконному середовищі − це один з видів електромагнітної енергії. Як відомо, ця енергія у формі хвиль може проходити через вакуум, повітря та через деякі матеріали − наприклад, скло. Важливою характеристикою будь-якої енергетичної хвилі є довжина. Довжина електромагнітної хвилі визначається частотою коливання електричного заряду, який генерує цю хвилю.

Для передачі інформації через оптоволокно використовуються електромагнітні хвилі із довжинами, що лежать поза межами видимого діапазону (400-700 нм). Як правило, це хвилі довжиною 850 нм, 1310 нм або 1550 нм. Ці довжини були вибрані, оскільки хвилі з такими параметрами проходять через оптоволокно краще, ніж хвилі з іншими параметрами.

Виходячи з джерела, електромагнітні хвилі розповсюджуються по прямій. Ці прямі лінії називають променями. У вакуумі світлові промені розповсюджуються на швидкості 300000 км/с. Але у середовищі (вода, скло) ці швидкості є меншими.

Коли світловий промінь потрапляє на межу розділу двох середовищ (падаючий промінь), частина світлової енергії відбивається назад (відбитий промінь). Та частина світлової енергії, яка не відбилася, буде поглинута іншим середовищем. Але через різницю оптичної густини падаючий промінь заломиться. Саме завдяки заломленню світлових променів на межі розділу середовищ можливе використання оптоволоконного кабелю для передачі інформації. Кут заломлення світлового променя залежить від оптичної густини матеріалу. Оптична густина визначає, наскільки швидкість розповсюдження світла у середовищі менша від швидкості розповсюдження світла у середовищі. Відношення швидкості світла у середовищі до швидкості світла у вакуумі називається індексом заломлення. Отже, мірою оптичної густини матеріалу є його індекс заломлення. Збільшити індекс заломлення матеріалу (наприклад, скла) можна, додаючи до нього певні хімічні елементи. Якщо падаючий промінь падає на межу розділу двох середовищ під кутом 90, промінь не заломлюється. Але якщо кут відмінний від 90, промінь заломлюється, причому кут заломлення залежить як від індексу заломлення середовищ, так і від кута падіння променя. Якщо світловий промінь переходить із середовища з меншим індексом заломлення у сере-довище з меншим індексом заломлення, заломлений промінь загинається у сторону нормалі. Якщо ж навпаки − заломлений промінь загинається у протилежний до нормалі бік. Кут падіння, при якому промінь при переході з більш оптично густого середовища у менш оптично густе вже не заломлюється, а повністю відбивається у середовище, називається критичним кутом.

Світловий промінь, який несе інформацію у оптоволокні, мусить залишатися всередині оптоволокна на всьому шляху від відправника інформації до отримувача. Він не повинен заломлюватися всередину матеріалу, який знаходиться навколо світловоду, оскільки через заломлення буде втрачатися частина енергії.

Закони відбивання та заломлення ілюструють, як спроектувати волокно, у якому світлова енергія буде втрачатися мінімально. Таке волокно повинно задовольняти двом умовам:

– центральна частина оптоволокна повинна мати більший індекс заломлення, ніж матеріал, який її оточує;

– кут падіння світлового променя повинен бути більшим за крити-чний кут для ядра та оболонки.

Коли обидві ці умови виконуються, падаючий промінь повністю за-лишається у волокні. Це явище називається повним внутрішнім відбиван-ням.

Першу умову виконати легко, підібравши відповідним чином мате-ріали для ядра та оболонки. Контролювати кут падіння променя дозво-ляють два фактори:

– числова апертура − межі кутів падіння променя, при яких він буде повністю відбиватися;

– мода − шлях проходження променя через оптоволокно.

Отже, світлові промені можуть увійти в ядро лише у тому випадку, якщо кут падіння лежить у межах числової апертури волокна.

Будова і особливості застосування оптоволоконного кабелю

Якщо діаметр волокна дозволяє, можна одночасно пропустити через нього кілька променів. Говорять, що таке волокно є багатомодовим на відміну від одномодового, у якому може проходити лише один промінь у певний момент часу.

Кожен волоконно-оптичний кабель, який використовується для пе-редачі інформації у мережах, складається з двох світловодів у спільній оболонці − для передачі інформації у двох напрямках.

Оскільки у оптоволоконному кабелі не виникає проблем, пов’язаних з перехресними наводками, немає потреби екранувати або перекручувати пари проводів. Тому один кабель може нести від 2 до 48 світловодів.

Як правило, волоконно-оптичний кабель має наступну будову:

– зовнішня оболонка;
– підсилюючий матеріал;
– буфер;
– оболонка;
– ядро.

Ядро оптоволокна виготовляється із світло провідного матеріалу − як правило, це скло, виготовлене з двоокису кремнію та інших матеріалів. Багатомодове оптоволокно використовує тип скла, який називають ступінчасто індексованим склом . У такого скла індекс заломлення зменшується у напрямку до зовнішнього краю ядра.

Оболонка навколо ядра виготовляється також з двоокису кремнію, але з меншим індексом заломлення, ніж ядро. Це дозволяє досягнути у ядрі ефекту повного внутрішнього відбивання. Як правило, стандартне багатомодове оптоволокно використовує 50-ти або 62,5-мікронне ядро та 125-ти мікронну оболонку. Це позначається як 62,5/125 μ або 50/125 μ оптоволокно.

В якості буферизуючого матеріалу, як правило ,використовується пластик. Він дозволяє убезпечити оболонку та ядро від пошкоджень. Для цього існує 2 види дизайну кабелю: із вільним положенням ядра та із жорстко закріпленим ядром. Як правило, у LAN використовується багатомодовий кабель із жорстко закріпленим ядром. Він призначений для прокладки всередині будівель, тоді як кабель із вільним положенням ядра використовується для зовнішніх робіт.

Підсилюючий матеріал навколо буферизуючого шару попереджає ушкодження кабелю у процесі інсталяції. Для його виготовлення, як правило, використовують кевлар.

Зовнішня оболонка використовується для попередження забруднення кабелю розчинниками, абразивними речовинами та іншим.

У якості джерела випромінювання у багатомодовому оптоволокні використовуються інфрачервоні фотодіоди (Light Emitting Diodes, LEDs) або лазери.Багатомодове оптоволокно можна використовувати для пере-дачі інформації на відстань до 2 км.

У одномодовому оптоволокні (9/125 μ) у якості джерела використовується інфрачервоні лазери. Одномодове оптоволокно можна використовувати для передачі інформації на відстань до 40 км.

Оскільки інформація у мережних вузлах представлена у вигляді електричних сигналів, необхідна наявність пристою для перетворення електричних сигналів у оптичні і навпаки. Для цього використовуються:

– фотодіоди, які можуть генерувати хвилі з довжиною 850 нм або 1310 нм. Для фокусування світла у ядро використовуються лінзи;

– лазери, які генерують вузький промінь когерентного випромінювання з довжиною 1310 нм або 1550 нм.

Для прийому інформації і її зворотнього перетворення використовуються фотоприймачі. Вони приймають світлові імпульси з чітко визначеною довжиною хвилі та конвертують їх у електричні сигнали.

Для приєднання кабелю до портів мережних пристроїв використовуються конектори: з багатомодовим оптоволокном − Subscriber Connector (SC-коннектор), з одномодовим − Straight Tip (ST-коннектор) (рис. 1.5).

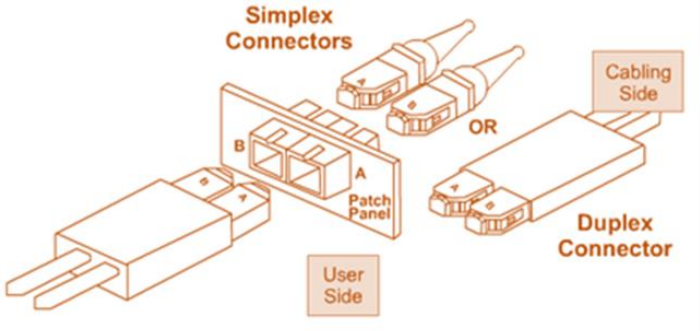

Рисунок 1.5 – Конектори [4]

Мережеві пристрої

Мережеве обладнання − пристрої, необхідні для роботи комп'ютерної мережі. Наприклад: маршрутизатор, комутатор, концентратор, патч-панель та ін. Зазвичай розрізняють активне та пасивне мережеве обладнання.

Активне мережеве обладнання має певні «інтелектуальні» можливості. До цього типу належать маршрутизатор, комутатор (світч).

Під пасивним мережним устаткуванням мається на увазі обладнання, не наділене «інтелектуальними» особливостями. Таким обладнанням вважається кабельна система, вилка/розетка, повторювач, патч-панель, концентратор (хаб), монтажні шафи, стійки.

Мережеві пристрої забезпечують транспортування даних між пристроями користувача. Вони подовжують і об'єднують кабельні з'єднання, перетворюють дані з одного формату в інший і керують передаванням даних.

До мережевих пристроїв належать:

– повторювач (англ. repeater) − це пристрій, призначений для підсилення мережевих сигналів, що дозволяє передавати їх середовищем на більшу відстань. Причому повторювач не переглядає іншу інформацію, яка міститься в пакеті;

– концентратор (англ. hub − центр уваги) − це один із видів мережевих пристроїв, які можна встановлювати на рівні доступу мережі Ethernet. На ньому є кілька портів для під'єднання вузлів до мережі;

– концентратор не визначає, якому вузлу призначено конкретне повідомлення. Він просто приймає електронні сигнали одного порту й відтворює їх для всіх інших портів. Для передавання та отримання повідомлень всі порти концентратора Ethernet під'єднуються до одного і того самого каналу;

– міст (англ. bridge − міст) − це пристрій, призначений для фільтрування потоків даних у локальній мережі для того, щоб локалізувати передавання даних і разом із тим зберегти можливість зв'язку з іншими частинами мережі для перенаправлення туди потоків даних. Міст збирає інформацію про те, на якому порті знаходиться конкретна MAC-адреса, і приймає рішення про пересилку даних на підставі відповідного списку MAC-адрес. Мости здійснюють фільтрацію потоків даних, базуючись лише на MAC-адресі вузлів, тому можуть швидко пересилати дані;

– комутатор (англ. switch − перемикач) − це пристрій, який можна назвати «розумним» концентратором, тому що він передає дані тільки безпосередньо отримувачу;

– маршрутизатори (англ. router) − це пристрої об'єднаних мереж, які пересилають пакети між мережами на основі адрес. Маршрутизатор здатний вибирати найкращий шлях у мережі для переданих даних.

Маршрутизатор може приймати рішення на основі мережевих адрес замість використання індивідуальних MAC-адрес другого рівня. Завдяки цій здатності маршрутизатори стали основною магістраллю глобальної мережі Internet.

Мережева карта (мережевий інтерфейс) − пристрій, яким оснащують комп'ютер для під'єднання до мережі за допомогою мережевого кабелю чи радіоканалу. Для під'єднання до бездротової мережі можуть використовуватися не тільки мережеві карти, а й спеціальні пристрої.

Мережеві інтерфейси виготовляють у вигляді плат або окремих пристроїв − для бездротових мереж. Тип мережевого інтерфейсу має відповідати типу середовища передавання.

Тема 2. Адресація в мережах

Адресація в комп'ютерних мережах: поняття адресації у мережах, роль адрес у маршрутизації та ідентифікації пристроїв. Фізична (MAC) адресація: призначення MAC-адреси, структура MAC-адреси (OUI та індивідуальна частина), особливості роботи на канальному рівні. Логічна адресація (IP-адреси): IPv4: структура та поділ на мережеву і хостову частину, класи IP-адрес та історичний підхід. IPv6: структура, скорочений запис, переваги. Мережеві маски та підмережі: призначення маски, CIDR (Classless Inter-Domain Routing), приклади розбиття на підмережі. Спеціальні та зарезервовані адреси: приватні адреси (RFC 1918), петльова адреса (loopback), широкомовні та мультикаст-адреси. Протоколи підтримки адресації: ARP (Address Resolution Protocol) у IPv4, NDP (Neighbor Discovery Protocol) у IPv6, DHCP як механізм автоматичного призначення адрес. Імена і служби адресації в Інтернеті: DNS як система відображення імен у IP-адреси, ієрархічна структура доменів, організації, що керують адресним простором (IANA, ICANN, RIR).Проблеми та виклики адресації: вичерпання IPv4, перехід на IPv6, використання NAT і PAT як тимчасове рішення. Принципи роботи та застосування NAT та PAT. Причини появи NAT: обмеженість IPv4-адресного простору.

Адресація в комп'ютерних мережах

Спробуємо розібратися, які саме вимоги можуть висуватися до мережевих адрес. Наприклад, було відправлено поштовий переказ на значну суму. Напевне, менш за все би хотілося, щоб у місті існувала ще одна вулиця, будинок, квартира і отримувач з точно такими ж даними, як Ваші. Тобто головною і обов'язковою вимогою до будь-якої адреси є її унікальність. Інакше грошовий переказ або дані можуть бути доставлені зовсім не тому, кому призначались. Також необхідно враховувати, що адреса передається разом з даними, тобто чим більше місця займатиме адреса, тим менше місця залишиться для даних. Окрім того, короткі адреси простіше аналізувати комутаційному обладнанню, тому наступною вимогою до адрес можна вважати компактність [5, 6].

Крім мережевого обладнання і обчислювальних пристроїв, адреси використовуються людьми. Поглянувши на дві адреси - ukr.net та 212.42.76.253, − зрозуміємо, що перша буде більш зручною для запам'ятовування. А отже, ще однією вимогою можна вважати зручність.

Уявімо, що адресою кожної окремої людини, наприклад в Україні, буде його ідентифікаційний код. Ідентифікаційний код є унікальним – розраховується за певним алгоритмом і не може повторюватися, компактним – складається з десяти цифр, частково зручним – так, можливо, запам'ятовувати коди всіх знайомих було б складно, проте цифровий код досить просто опрацьовувати. Проте як має виглядати доставка, наприклад, посилки, за такою адресою, враховуючи, що за ідентифікаційним кодом не можна вказати, в якому місті чи селищі мешкає людина? Якщо ж поглянути на адресу, яка використовуються для доставки пошти, то можна побачити, що вона складається з послідовних уточнень: країна, місто, вулиця, будинок. Тобто коли, наприклад, посилка відправляється з Франції, то перш за все вона направляється в країну доставки, потім відвозиться до певного міста. Якщо в місті декілька поштових відділень, то за назвою вулиці посилка направляється до відповідного поштового відділення і т.д. Можливість такого поетапного пошуку забезпечується існуванням ієрархічності адреси.

Отже, серед вимог, що висуваються до мережевих адрес, можна виділити:

– унікальність;

– компактність;

– зручність;

– ієрархічність.

Аналізуючи визначені вимоги, можна бачити, що деякі з них погано узгоджуються між собою. Так, наприклад, вимога унікальності і компактності можуть суперечити одна одній: максимально компактна адреса буде складатися з одного символу, але таких адрес буде досить мало. Така сама ситуація з компактністю та ієрархічністю – чим більш компактна адреса, тим менше нею може забезпечуватися ієрархічність.

Через подібні особливості в мережевих технологіях одночасно існують і використовуються різні адреси:

– фізичні, локальні, апаратні адреси (Physical, Local, Hardware Addresses);

– логічні, мережні адреси (Logical, Network Addresses);

– символьні, текстові адреси (Symbolic, Text Addresses).

Проте слід розуміти, що лише одна вимога має основне значення, і це − унікальність. Всі інші – не більш ніж побажання.

Для ідентифікації людини можна використати її відбитки пальців та поштову адресу. Зазвичай, відбитки пальців людини не змінюються, та за їх допомогою можна фізично ідентифікувати людину, де б вона не знаходилися. Інша справа − поштова адреса людини, яка залежить від місця її проживання, отже, може змінюватися упродовж життя.

Пристрої, що підключені до мережі, мають принаймні дві адреси, які аналогічні відбиткам пальців людини і її поштовій адресі. Це два типи адрес:

– MAC-адреса (Media Access Control) – адреса управління доступом до середовища передавання даних);

– IP-адреса (Internet Protocol) – адреса Інтернет-протоколу.

Мережевим вузлам потрібні обидві адреси для обміну даними мережею. MAC-адреса не змінюється при переміщенні пристрою з однієї мережі в іншу, оскільки вона призначається виробником мережевого інтерфейсу. IP-адреса може змінюватися в залежності від під'єднання пристрою до певної мережі, та призначається адміністратором мережі або відповідними службами мережі.

MAC-адреса (media access control address) – це унікальний ідентифікатор, що має мережевій адаптер, та застосовується у процесі передачі даних у межах локальної мережі (окремого канального сегменту мережі).

MAC-адреса має довжину 48 біт (6 байт). Для подання MAC-адреси використовується шістнадцятковий формат. Інших обмежень щодо подання не висувається, тому можна зустріти різні записи MAC-адрес, які відрізняються групуванням байтів та роздільними знаками:

00-50-56-BE-D7-87 – формат запису IEEE EUI-48.

00:50:56:BE:D7:87 – формат запису Unix Zero-Padded. 0050.56BE.D787 – формат запису Cisco.

Історично адреси прошивалися в ПЗУ чіпсету мережевої карти без можливості їх модифікації, але нині MAC-адреса може бути змінена програмно.

MAC-адреса складається з двох частин. Перша частина MAC-адреси вказує постачальника-виробника мережевого інтерфейсу. Ця частина MAC-адреси називається унікальним ідентифікатором організації (OUI – Organizationally Unique Identifier). Довжина OUI найчастіше складає 3 байти (24 біти), але може бути і 28 або 36 біт. Керування загальним адресним простором MAC-адрес здійснює Інститут інженерів електриків та електронників (IEEE – Institute of Electrical and Electronics Engineers). Отже, постачальник, який бажає виготовляти і продавати мережеві інтерфейси, повинен зареєструватися в IEEE, щоб йому надали ідентифікатор OUI.

Друга частина адреси (біти, що залишилися) − це унікальний ідентифікатор інтерфейсу (OUA – Organizationally Unique Address). Всі MAC-адреси, що починаються з однакового ідентифікатора OUI, повинні містити унікальні ідентифікатори інтерфейсів.

Тому в теорії MAC-адреси унікальні (подвійно унікальні), оскільки кожен з виробників зобов'язаний забезпечувати унікальність адреси для кожного виробленого ним пристрою. Однак деякі виробники для OUA встановлюють випадкове число, що може призводити до їх дублювання.

IP-адреса (Internet Protocol address) – це ідентифікатор, що призначається мережному адаптеру/інтерфейсу і використовується для адресації комп'ютерів чи пристроїв у мережах, побудованих з використанням протоколу TCP/IP. Важливою особливістю IP-адрес є їх ієрархічність, тобто IP-адреса ґрунтуючись на розміщення пристрою в мережі.

Існують четверта та шоста версії IP-адресації. Основним стандартом, у якому описуються вимоги до IP-адрес версії 4, є прийнятий у вересні 1981 року стандарт RFC-791

«Internet Protocol. DARPA Internet Program Protocol Specification». Основним стандартом, у якому описуються вимоги до IP- адрес версії 6, є прийнятий у грудні 1998 року стандарт RFC-2460 «Internet Protocol, Version 6 (IPv6) Specification». Пізніше ці стандарти були доповнені іншими стандартами RFC, що певною мірою стосуються питань IP-адресації. Тексти стандартів RFC, зокрема і зазначених вище стандартів, можна отримати на Web-сайті організації, що займається стандартизацією – Підрозділу інженерних розробок Інтернет (IETF, Internet Engineering Task Force).

IPv4: 32-бітна адреса. Записується в десятковому форматі чотирма числами, розділеними крапками. Наприклад, 192.168.10.10 (рис. 2.1).

IPv6: 128-бітна адреса. Записується в шістнадцятковому форматі (рис. 2.2).

Наприклад, 2001:0DB8:0000:ABCD:0000:0000:0000:1234.

Незважаючи на те, що IPv4-адреса записується в десятковому форматі, її опрацювання здійснюється в двійковому. Кожне число, відокремлене крапкою, називається октетом («ОКТО» − вісім), тому що містить 8 біт.

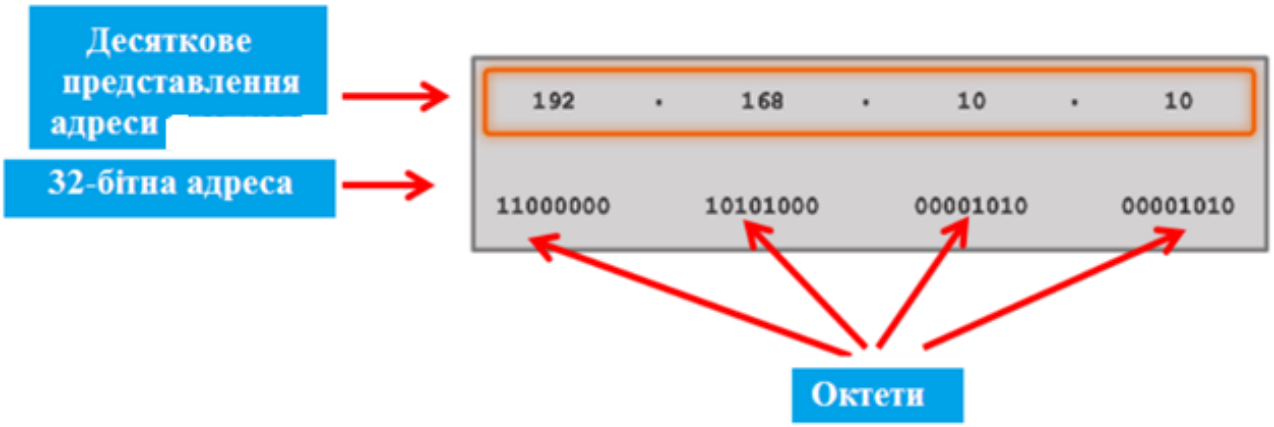

Рисунок 2.1 – Формат запису IPv4-адреси [6]

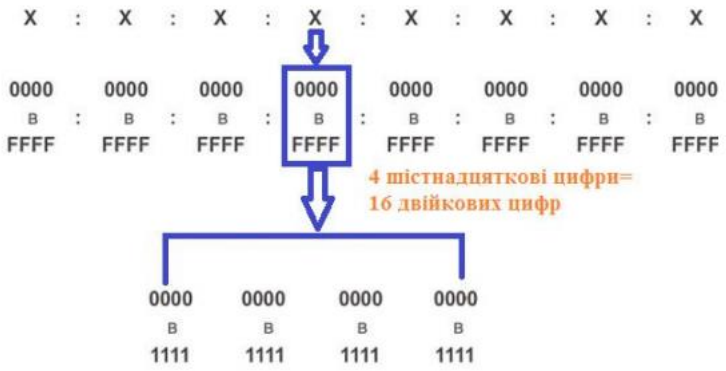

Рисунок 2.2 – Формат запису IPv6-адреси [6]

Таким чином, адреса 192.168.10.10 складається з чотирьох октетів. Кожен біт в октеті може бути 1 або 0. Тому кожен октет (8 біт) може містити десяткове значення від 0 до 255 включно (від 00000000 до 11111111).

Призначення мережевої маски

Мережева маска визначає, яка частина IP-адреси належить до мережі, а яка − до вузла (host).

Вона використовується для:

– ідентифікації межі між мережевим та хостовим простором;

– забезпечення маршрутизації пакетів у глобальній мережі;

– оптимізації використання адресного простору.

Наприклад, маска 255.255.255.0 (або /24) означає, що перші 24 біти адреси визначають мережу, а останні 8 − хост.

CIDR (Classless Inter-Domain Routing)

CIDR було запроваджено для подолання обмежень класової адресації (A, B, C).

Основні переваги CIDR:

– гнучкість у визначенні розміру підмережі;

– зменшення таблиць маршрутизації завдяки агрегації маршрутів;

– раціональне використання IPv4-адресного простору, що стало критично важливим у період його виснаження.

CIDR записується у форматі IP/префікс, де префікс вказує кількість бітів мережевої частини. Наприклад: 192.168.1.0/26.

Приклади розбиття на підмережі

Приклад 1: розбиття мережі /24. Мережа: 192.168.1.0/24 (256 адрес). Якщо розділити на підмережі /26: кожна підмережа матиме 64 адреси (62 доступні для хостів). Підмережі: 192.168.1.0/26, 192.168.1.64/26, 192.168.1.128/26, 192.168.1.192/26.

Приклад 2: Використання VLSM (Variable Length Subnet Masking). VLSM дозволяє застосовувати різні маски в межах однієї мережі. Наприклад, у мережі 10.0.0.0/24 можна виділити: /28 для невеликих сегментів (16 адрес), /30 для точка-точка з'єднань (4 адреси), /26 для більших сегментів (64 адреси).

Еволюція та сучасні тенденції:

– перехід від класової адресації до CIDR був ключовим етапом розвитку Інтернету;

– CIDR та VLSM забезпечили масштабованість та ефективність маршрутизації, особливо в умовах дефіциту IPv4;

– у сучасних мережах CIDR використовується також для IPv6, де префікси дозволяють створювати ієрархічну структуру адресного простору.

Мережеві маски є базовим інструментом для визначення структури IP-мережі:

– CIDR забезпечує гнучке та ефективне управління адресами;

– поділ на підмережі дозволяє оптимізувати використання ресурсів та підвищити безпеку мережі;

– використання VLSM дає можливість адаптувати розмір підмережі до конкретних потреб.

Приватні та публічні адреси

IPv4 використовує 32-бітну адресацію, що теоретично дозволяє створити приблизно 4,3 мільярда унікальних IP-адрес. На початковому етапі розвитку Інтернету така кількість вважалася надлишковою, однак історичні особливості розподілу адрес, зокрема класова адресація та виділення великих блоків організаціям без оптимального використання, суттєво зменшили ефективність цього простору. Згодом перехід до безкласової адресації CIDR лише частково розв'язав проблему, але не усунув її першопричину − обмежену довжину адреси [7].

IPv4 адреси бувають двох типів: публічні (public) і приватні (private) (рис. 2.3). Перші так само часто називають білими або зовнішніми, а другі − сірими або внутрішніми. У чому між ними різниця?

Публічні адреси є унікальними і не можуть повторюватися ніде і ніколи, що контролюється провайдером, який вам їх дав в оренду, а йому, у свою чергу дав їх в оренду інший провайдер або організація IANA, що стежить за розподілом адрес. А приватні, навпаки, можуть використовуватися ким завгодно і повторюватися скільки завгодно разів. Тобто, приватні адреси можуть повторюватися і не бути унікальними, але якою ціною? На них нічого не можна відправити з інтернету. Ніхто в інтернеті не знає маршруту до ваших приватних адрес, а так само що можливо тим же самими адресами, що використовується у вашого сусіда, а раз ніхто не знає, то яка різниця, повторюються вони чи ні? Іншими словами, за межами локальної мережі приватні адреси не маршрутизуються.

Характеристика	Приватні IP	Публічні IP
Унікальність	В межах мережі	Глобально
Доступність	Локальна мережа	Інтернет
Вартість	Безкоштовні	Платні

Рисунок 2.3 – Порівняння приват них і публічних адрес [6]

Приватних адрес не так багато − навіщо робити багато, якщо їх можна повторювати скільки завгодно разів (у різних локальних мережах, звичайно). Всього три діапазони приватних адрес (рис. 2.4) [8].

Клас A	10.0.0.0 - 10.255.255.255
Клас B	172.16.0.0 - 172.31.255.255
Клас C	192.168.0.0 - 192.168.255.255

Рисунок 2.4 – Діапазон приватних адрес [6]

Природно, що навряд чи знадобляться в чистому вигляді мережі таких великих розмірів, тому приватні адреси зазвичай розбивають на підмережі за допомогою більш довгого префікса, наприклад, з третього діапазону можна отримати 255 приватних підмереж по 254 хоста у кожній (рис. 2.5-2.6).

Наступне важливе питання − припустимо, ми видали співробітникам в офісі багато приватних адрес, але як же вони зможуть вийти в інтернет? Вони будуть відправляти запити в мережу, а відповіді на ці запити повинні будуть повертатися на зворотні адреси, які в даному випадку приватні. Так як в інтернеті ніхто не знає маршрутів до приватних адрес, то це не можливо. Як правило така задача вирішується одним із двох способів:

1) у мережі використовується проксі-сервер. Цей сервер має інтерфейс у зовнішній мережі і може мати такий же інтерфейс в приватній. Користувачі звертаються до нього, а не до сайтів безпосередньо. Сервер «свій», тому він знає про свої приватні адреси. Він отримує з них запити, і для кожного запиту звертається в інтернет зі своєї публічної адреси. Коли він отримає відповідь, то перешле її в середину на приватну адресу запитувача;

2) на граничному маршрутизаторі можна налаштувати трансляцію адрес (NAT). І тоді при проходженні пакета з локальної мережі в інтернет, адреса відправника буде змінюватися: замість нікому невідомої приватної вписуватиметься публічна адреса з деякого пулу адрес, або публічна адреса самого маршрутизатора (тут можливі різні реалізації). На цю адресу і будуть приходити відповіді з інтернету. У відповідях відбуватиметься зворотня заміна: публічна адреса одержувача буде замінюватися на вихідну приватну адресу, після чого пакет повертається клієнтові, який робив запит.

Двійкове значення октету	Значення бітів октету	Десяткове значення октету
00000000	0	0
10000000	128	128
11000000	128+64	192
11100000	128+64+32	224
11110000	128+64+32+16	240
11111000	128+64+32+16+8	248
11111100	128+64+32+16+8+4	252
11111110	128+64+32+16+8+4+2	254
11111111	128+64+32+16+8+4+2+1	255

Рисунок 2.5 – Двійкова та десяткові значення деяких октетів

Двійкове значення октету	Значення бітів октету	Десяткове значення октету
11000101	128+64+0+0+0+4+0+1	197
11000110	128+64+0+0+0+4+2+0	198
11000111	128+64+0+0+0+4+2+1	199
11001000	128+64+0+0+8+0+0+0	200

Рисунок 2.6 – Приклад відповідності двійкового та десяткового значення октетів

На рисунку 2.7 показані зліва направо класи адрес − значення старших біт та десяткових значень першого октету в даному класі та доступна кількість мереж та вузлів, підтримуваних у даному класі.

Клас адреси	Старші біти	Діапазон десяткових значень першого октету	Доступна кількість мереж	Доступна кількість вузлів
Клас A	0	1–126	126	16 777 214
Клас B	10	128–191	16 384	65 534
Клас C	110	192–223	2 097 152	254

Рисунок 2.7 – Класи адрес та відповідні їм ідентифікатори мереж та вузлів

В адресах класу А перший октет представляє ідентифікатор мережі, в адресах класу В перші два актети використовуються для ідентифікатора мережі і нарешті в адресах класу С перші три октети використовується для ідентифікатора мережі. Таким чином кожну адресу можна розділити на два компоненти, як показано на рисунку 2.8.

Клас адреси	IP-адреса	Ідентифікатор мережі	Ідентифікатор вузла
Клас A	w.x.y.z	w	x.y.z
Клас B	w.x.y.z	w.x	y.z
Клас C	w.x.y.z	w.x.y	z

Рисунок 2.8 – Розподіл IP-адреси на компоненти відповідно до її класу

Локальні адреси IPv4 і IPv6

Локальні адреси каналу для IPv4 і IPv6 використовуються пристроєм для зв'язку з іншими комп'ютерами, підключеними до однієї мережі в межах одного діапазону IP адрес. Основна відмінність IPv4 від IPv6 полягає в наступному:

– пристрій IPv4 використовує локальну адресу каналу, якщо не може отримати IPv4 адресу;

– у IPv6-пристрою завжди має бути динамічно або вручну налаштована локальна адреса каналу.

Якщо комп'ютеру з ОС Windows не вдається зв'язатися з DHCP сервером і отримати адресу IPv4, то ОС Windows автоматично призначає адресу засобами автоматичного призначення приватних IP-адрес (Automatic Private IP Addressing, APIPA) [9]. Локальні адреси каналу знаходяться в діапазоні від 169.254.0.0 до 169.254.255.255.

IPv6 локальна адреса каналу

Як і IPv4, локальна адреса каналу IPv6 дозволяє пристрою обмінюватися даними з іншими пристроями з підтримкою IPv6 в одній мережі і тільки в ній. На відміну від IPv4, кожен пристрій з підтримкою IPv6 повинен мати локальну адресу каналу. IPv6 локальні адреси каналу знаходяться в діапазоні від fe80:: до febf::.

Примітка: На відміну від локальних IPv4-адрес каналу, локальні IPv6-адреси каналу використовуються в різних процесах, включаючи протоколи виявлення мереж і протоколи маршрутизації.

Загальне поняття спеціальних і зарезервованих IP-адрес

У процесі функціонування комп'ютерних мереж поряд із звичайними унікальними IP-адресами, що призначаються мережевим інтерфейсам вузлів, використовуються спеціальні та зарезервовані адреси. Вони мають визначене призначення та застосовуються для тестування, керування, маршрутизації трафіку, організації групової передачі даних і забезпечення службових функцій мережевих протоколів.

Спеціальні IP-адреси не можуть бути довільно призначені кінцевим вузлам для звичайного обміну даними в мережі Інтернет. Їхня поведінка суворо регламентована стандартами IETF (RFC) і реалізується на рівні мережевих протоколів та операційних систем.

До найважливіших категорій спеціальних і зарезервованих адрес належать петльова (loopback) адреса, широкомовні (broadcast) адреси та мультикаст-адреси.

Петльова адреса (Loopback Address)

Петльова адреса використовується для внутрішньої перевірки роботи мережевого стеку на одному й тому самому вузлі без передавання даних у фізичну мережу. Фактично пакети, надіслані на loopback-адресу, повертаються назад у межах операційної системи [11].

У протоколі IPv4 для петльового інтерфейсу зарезервовано весь діапазон адрес

127.0.0.0/8, тобто від 127.0.0.0 до 127.255.255.255. Найчастіше на практиці використовується адреса 127.0.0.1, яка має стандартну назву localhost.

У протоколі IPv6 для аналогічних цілей використовується адреса ::1/128, яка також ідентифікується ім'ям localhost.

Петльова адреса виконує важливі функції:

– тестування мережевого програмного забезпечення;

– перевірка роботи TCP/IP-стеку без доступу до зовнішньої мережі;

– забезпечення взаємодії між локальними сервісами (наприклад, веб-сервером і базою даних на одному сервері);

– підвищення безпеки, оскільки трафік не виходить за межі хоста.

Важливою особливістю loopback-адрес є те, що пакети з такими адресами ніколи не маршрутизуються та автоматично відкидаються маршрутизаторами.

Широкомовні адреси (Broadcast Addresses)

Широкомовні адреси призначені для одночасного передавання мережевих пакетів усім вузлам у межах однієї логічної мережі або підмережі. Такий механізм застосовується для виявлення пристроїв, службової взаємодії та початкової конфігурації мережі.

У протоколі IPv4 існують два основні типи широкомовних адрес. Обмежена широкомовна адреса має вигляд 255.255.255.255. Вона використовується для передавання повідомлень усім вузлам локального сегмента мережі, коли відправник ще не знає параметрів мережі. Такі пакети не передаються через маршрутизатори. Спрямована широкомовна адреса формується як остання адреса в конкретній підмережі, тобто адреса, у якій усі біти хостової частини дорівнюють одиниці. Наприклад, для мережі 192.168.1.0/24 широкомовною буде адреса 192.168.1.255.

Широкомовна передача широко використовується в таких протоколах і службах:

– ARP (визначення MAC-адреси за IP-адресою);

– DHCP (отримання IP-адреси клієнтом);

– деякі протоколи маршрутизації та виявлення сервісів.

– У протоколі IPv6 класичне широкомовлення відсутнє. Його функціональність замінена мультикаст-механізмом, що дозволяє зменшити навантаження на мережу.

Мультикаст-адреси (Multicast Addresses)

Мультикаст-адреси використовуються для передавання даних не всім вузлам мережі, а лише певній групі отримувачів, які підписалися на відповідну мультикаст-групу. Такий підхід є значно ефективнішим за широкомовлення, особливо в мережах із великою кількістю пристроїв.

У протоколі IPv4 мультикаст-адреси належать до діапазону 224.0.0.0 – 239.255.255.255, що відповідає класу D у класовій адресації. Цей діапазон поділяється на піддіапазони з різним призначенням:

– адреси 224.0.0.0/24 використовуються для локальних мережевих протоколів і не маршрутизуються;

– адреси 239.0.0.0/8 призначені для приватного мультикасту в організаціях.

У протоколі IPv6 всі мультикаст-адреси починаються з префікса FF00::/8. В IPv6 мультикаст є основним механізмом групової доставки трафіку та використовується, зокрема, для заміни ARP, служби виявлення сусідів і роботи мережевих сервісів.

Мультикаст-передача застосовується в таких сценаріях:

– потокове відео та аудіо (IPTV, відеоконференції);

– протоколи маршрутизації (OSPF, RIP);

– служби синхронізації та розповсюдження оновлень;

– корпоративні системи сповіщення.

Значення спеціальних адрес для адміністрування та безпеки мереж

Неправильне використання широкомовлення або мультикасту може призвести до перевантаження мережі, а некоректна фільтрація таких адрес − до уразливостей безпеки.

Зокрема, в системах мережевої безпеки (брандмауери, IDS/IPS) широко застосовуються правила контролю broadcast- та multicast-трафіку, а loopback-інтерфейс часто використовується для ізольованого розміщення критично важливих сервісів.

ARP (Address Resolution Protocol) у мережах IPv4 та NDP (Neighbor Discovery Protocol) у мережах IPv6

Загальні засади адресації та необхідність протоколів виявлення сусідів

Функціонування комп’ютерних мереж на основі стеку TCP/IP базується на використанні логічної IP-адресації та фізичної адресації канального рівня, зокрема MAC-адрес. Передавання даних у локальній мережі Ethernet фізично здійснюється за MAC-адресами, тоді як прикладні та транспортні протоколи оперують IP-адресами. Це зумовлює необхідність механізму динамічного зіставлення IP-адреси вузла з його MAC-адресою. У мережах IPv4 таку функцію виконує протокол ARP, а в мережах IPv6 − протокол NDP, який є складовою частиною ICMPv6.

Протокол ARP у IPv4

ARP (Address Resolution Protocol) − це допоміжний протокол мережевого рівня, призначений для визначення MAC-адреси вузла за відомою IPv4-адресою в межах однієї широкомовної доменної мережі [11].

Коли вузол IPv4 потребує передати пакет іншому вузлу в тій самій локальній мережі, він спочатку перевіряє власну ARP-таблицю (ARP cache). Якщо відповідність між IP- та MAC-адресою відсутня, ініціюється процедура ARP-запиту. ARP-запит передається у вигляді широкомовного Ethernet-кадру, адресованого на MAC-адресу FF:FF:FF:FF:FF:FF, і містить IP-адресу шуканого вузла. Вузол, IP-адреса якого збігається з адресою в запиті, формує ARP-відповідь, що надсилається уніфіковано безпосередньо ініціатору запиту. Отримавши відповідь, вузол зберігає пару IP-MAC у ARP-таблиці на обмежений час, після чого може здійснювати безпосереднє передавання кадрів Ethernet. ARP працює без механізмів автентифікації та цілісності, що робить його вразливим до атак типу ARP spoofing або ARP poisoning. Такі атаки широко використовуються в локальних мережах для реалізації перехоплення трафіку, атаки «людина посередині» (Man-in-the-Middle) та відмови в обслуговуванні. Саме тому ARP має важливе значення в курсах з мережевої безпеки та реагування на інциденти.

Попри простоту реалізації, ARP має низку архітектурних недоліків. Основними з них є використання широкомовних повідомлень, що негативно впливає на масштабованість мережі, а також відсутність вбудованих механізмів безпеки. У процесі проєктування IPv6 ці обмеження були враховані, що зумовило відмову від ARP на користь більш функціонального та гнучкого механізму − Neighbor Discovery Protocol (NDP).

Neighbor Discovery Protocol (NDP) у IPv6

Neighbor Discovery Protocol − це набір процедур і повідомлень, реалізованих у межах ICMPv6, які забезпечують виявлення сусідніх вузлів, визначення їх канальних адрес, контроль досяжності, автоматичну конфігурацію адрес і виявлення маршрутизаторів.

На відміну від ARP, NDP не використовує широкомовлення. Усі повідомлення передаються за допомогою багатоадресної (multicast) адресації, що суттєво зменшує навантаження на мережу. Для зіставлення IPv6-адреси з MAC-адресою використовуються повідомлення Neighbor Solicitation та Neighbor Advertisement. За своєю логікою вони є аналогами ARP-запиту та ARP-відповіді, проте функціонують у рамках ICMPv6.

Окрім вирішення адрес, NDP виконує низку додаткових функцій. Протокол забезпечує виявлення маршрутизаторів за допомогою Router Solicitation і Router Advertisement, підтримує Stateless Address Autoconfiguration (SLAAC), а також реалізує механізм Neighbor Unreachability Detection, який дозволяє визначати, чи доступний сусідній вузол у поточний момент часу. Таким чином, NDP поєднує функціональність ARP, ICMP Redirect та частково DHCP, що робить його ключовим елементом архітектури IPv6.

Хоча NDP є архітектурно досконалішим за ARP, він також не позбавлений вразливостей. Атаки типу Neighbor Spoofing, Rogue Router Advertisement або DoS через надмірні ICMPv6-повідомлення залишаються актуальними. Для підвищення рівня безпеки в IPv6 передбачено використання механізму Secure Neighbor Discovery (SEND), який базується на криптографічних підписах і сертифікатах, однак через складність реалізації він застосовується обмежено.

У практиці мережевого адміністрування безпека NDP часто забезпечується за допомогою фільтрації ICMPv6, контролю RA-повідомлень на комутаторах (RA Guard) та систем моніторингу мережевого трафіку.

Порівняльний аналіз ARP і NDP. ARP є простим, але обмеженим протоколом, призначеним виключно для зіставлення IPv4-адрес і MAC-адрес у локальній мережі. Він активно використовує широкомовлення та не має вбудованих засобів безпеки. NDP, навпаки, є комплексним механізмом IPv6, який використовує multicast, інтегрований з ICMPv6 та підтримує додаткові функції автоматичної конфігурації й виявлення маршрутизаторів.

З точки зору сучасних мереж, NDP краще відповідає вимогам масштабованості, автоматизації та керованості, однак потребує глибшого розуміння та ретельного налаштування з боку адміністратора.

ARP і NDP відіграють ключову роль у забезпеченні взаємодії між мережевим та канальним рівнями моделі TCP/IP. ARP залишається невід'ємною складовою IPv4-мереж, тоді як NDP є фундаментом функціонування IPv6.

Статична адресація

У невеликій мережі можна вручну налаштувати кожен пристрій з власною IP адресою. Ви призначаєте унікальну IP адресу кожному вузлу в одній мережі. Це процес відомий як статична IP адресація (рис. 2.1-2.2).

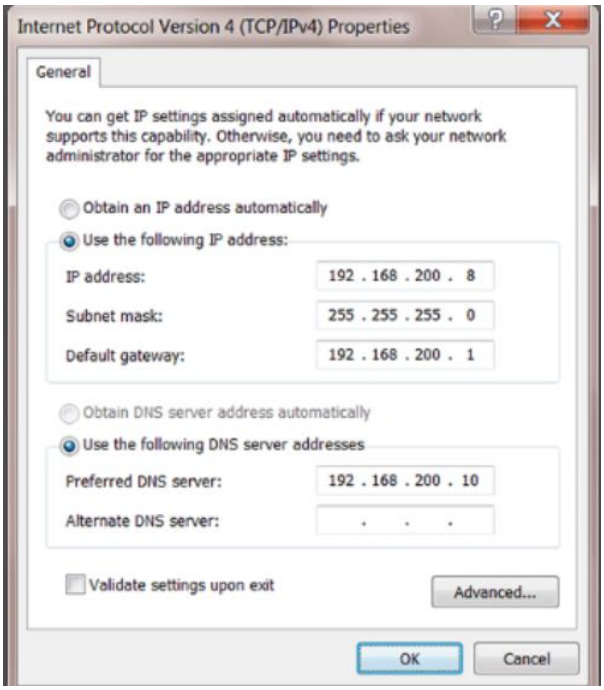

Рисунок 2.1 – Налаштування IPv4-адресації статично

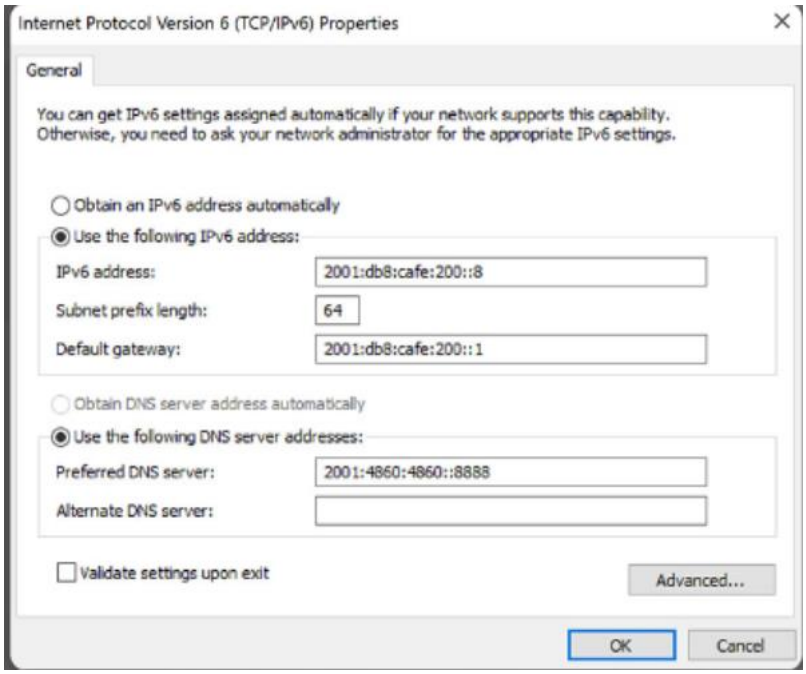

Рисунок 2.2 – Налаштування IPv6-адресації статично

На рисунку 2.2 показано, що на комп'ютері з ОС Windows можна призначити такі параметри IPv4 адреси вузла:

– IP адреса − ідентифікує пристрій у мережі;

– маска підмережі − використовується для ідентифікації мережі, до якої підключений даний пристрій;

– основний шлюз − визначає маршрутизатор, який цей пристрій використовує для доступу до Інтернету або іншої мережі

– необов'язкові параметри − наприклад, адреси основного та альтернативного DNS серверів

Динамічна адресація

Замість налаштування вручну кожного пристрою в мережі, можна скористатися перевагами реалізації сервера DHCP (Dynamic Host Configuration Protocol). DHCP сервер автоматично присвоює IP адреси, що спрощує процес адресації. Автоматичне налаштування деяких параметрів IP адресації також знижує можливість присвоєння повторних або недійсних IP адрес [12].

За замовчуванням більшість кінцевих пристроїв налаштовано на запит IP адреси з DHCP сервера. Налаштування за замовчуванням для комп'ютера з ОС Windows показані на рисунку. Якщо комп'ютер налаштовано на отримання IP адреси автоматично, усі інші поля IP адресації недоступні. Цей процес однаковий як для дротового, так і для бездротового мережевого адаптера.

DHCP сервер може автоматично встановлювати значення наступних налаштувань IPv4 адреси пристрою:

– IPv4 адреса;

– маска підмережі;

– основний шлюз (Default Gateway);

– необов'язкові параметри, наприклад адреса DNS сервера.

DHCP також доступний для автоматичного налаштування IPv6 адресації.

DHCP як механізм автоматичного призначення IP-адрес

У сучасних комп'ютерних мережах ефективне управління IP-адресним простором є критично важливим завданням, особливо в умовах великої кількості користувачів, динамічного підключення пристроїв та використання мобільних і віртуалізованих середовищ. Ручне призначення IP-адрес у таких умовах є неефективним, схильним до помилок і складним в адмініструванні. Саме тому широкого поширення набув протокол DHCP (Dynamic Host Configuration Protocol), який забезпечує автоматичне, централізоване та контрольоване призначення параметрів мережевої конфігурації клієнтам.

DHCP − це мережевий протокол прикладного рівня моделі TCP/IP, призначений для автоматичного надання клієнтським пристроям IP-адреси та супутніх параметрів конфігурації. До таких параметрів належать маска підмережі, адреса шлюзу за замовчуванням, адреси DNS-серверів, доменне ім'я, час оренди адреси та інші опції. DHCP є розвитком більш раннього протоколу BOOTP і зберігає з ним зворотну сумісність.

Основною ідеєю DHCP є використання централізованого сервера або групи серверів, які керують пулом IP-адрес та розподіляють їх клієнтам на певний проміжок часу, що називається орендою (lease).

У моделі OSI DHCP функціонує на прикладному рівні, однак для своєї роботи використовує транспортний протокол UDP. Обмін повідомленнями відбувається через порт 67 UDP на стороні сервера та порт 68 UDP на стороні клієнта. Використання UDP обумовлене необхідністю швидкого та простого обміну без встановлення з'єднання, а також можливістю широкомовної передачі.

Робота DHCP базується на клієнт-серверній архітектурі. Коли пристрій підключається до мережі та не має IP-адреси, він ініціює процес отримання конфігурації. Класичний алгоритм взаємодії між клієнтом і сервером описується моделлю DORA, яка включає чотири основні етапи: Discover, Offer, Request, Acknowledgment. На першому етапі клієнт надсилає широкомовне повідомлення DHCP Discover з метою виявлення доступних DHCP-серверів у мережі. Це повідомлення передається без IP-адреси відправника, оскільки клієнт ще не має власної адреси. На другому етапі один або кілька DHCP-серверів відповідають повідомленням DHCP Offer, у яких пропонують клієнту доступну IP-адресу та інші параметри конфігурації. На третьому етапі клієнт обирає одну з отриманих пропозицій і надсилає повідомлення DHCP Request, підтверджуючи бажання отримати конкретну адресу від конкретного сервера. На завершальному етапі сервер надсилає повідомлення DHCP

Acknowledgment (ACK), яким остаточно закріплює IP-адресу за клієнтом на визначений час оренди. Після цього клієнт може повноцінно функціонувати в мережі.

Оренда IP-адреси та її поновлення

IP-адреси в DHCP не призначаються назавжди, а надаються в оренду на певний час. Такий підхід дозволяє ефективно використовувати обмежений адресний простір. Протягом терміну оренди клієнт зобов'язаний періодично оновлювати її. Приблизно після половини часу оренди клієнт намагається поновити адресу, надсилаючи DHCP Request безпосередньо серверу, який її надав. Якщо сервер підтверджує поновлення, оренда продовжується без переривання мережевої роботи. У разі недоступності сервера клієнт може продовжити спроби поновлення або, після завершення терміну оренди, припинити використання IP-адреси та ініціювати новий цикл отримання конфігурації.

Статичні та динамічні призначення

DHCP підтримує як динамічне, так і умовно статичне призначення IP-адрес. Динамічне призначення передбачає видачу будь-якої вільної адреси з пулу. Умовно статичне призначення, відоме як резервування, базується на MAC-адресі клієнта: конкретному пристрою завжди видається одна й та сама IP-адреса. Такий підхід широко використовується для серверів, мережевих принтерів, IP-телефонів та іншого обладнання, яке повинно мати стабільну адресу, але при цьому керуватися централізовано.

DHCP Relay

У великих мережах, розділених на кілька підмереж або VLAN, широкомовні DHCP-повідомлення не проходять через маршрутизатори. Для вирішення цієї проблеми використовується механізм DHCP Relay. DHCP Relay-агент приймає широкомовні запити від клієнтів у локальній мережі та пересилає їх у вигляді унікаст-повідомлень на віддалений DHCP-сервер. Це дозволяє використовувати один або кілька централізованих серверів DHCP для обслуговування великої кількості сегментів мережі.

Безпека DHCP

Незважаючи на простоту та зручність, DHCP має низку вразливостей. Однією з основних загроз є атака типу rogue DHCP, коли в мережі з'являється несанкціонований DHCP-сервер, що роздає некоректні або шкідливі параметри конфігурації. Іншою загрозою є DHCP starvation − атака, спрямована на вичерпання пулу IP-адрес шляхом масових запитів з підробленими MAC-адресами. Для захисту використовуються такі механізми, як DHCP Snooping на комутаторах, обмеження кількості MAC-адрес на порт, сегментація мережі та використання автентифікації на рівні доступу.

Переваги та недоліки використання DHCP

Основними перевагами DHCP є зменшення навантаження на адміністратора, мінімізація помилок конфігурації, централізоване управління параметрами мережі та ефективне використання IP-адресного простору. Недоліками можна вважати залежність від доступності DHCP-сервера та потенційні ризики безпеки у разі неправильної конфігурації.

DHCP є базовим і невід'ємним компонентом сучасних IP-мереж. Його використання є стандартом де-факто як у корпоративних, так і в домашніх мережах.

DHCPv6 (Dynamic Host Configuration Protocol for IPv6)

Перехід від IPv4 до IPv6 зумовив необхідність адаптації базових мережевих сервісів, зокрема механізмів автоматичної конфігурації вузлів. Одним із ключових таких сервісів є DHCPv6 − протокол динамічної конфігурації хостів для мереж IPv6. DHCPv6 забезпечує централізоване та кероване надання параметрів мережевої конфігурації клієнтам, що є особливо важливим у корпоративних, операторських і хмарних середовищах.

На відміну від IPv4, у світі IPv6 поряд із DHCPv6 активно використовується механізм Stateless Address Autoconfiguration (SLAAC). Це призводить до необхідності чіткого розуміння ролей, переваг і обмежень кожного підходу, а також їх спільного використання.

DHCPv6 призначений для автоматичного надання вузлам мережі IPv6 таких параметрів: адрес IPv6 або префіксів; адрес DNS-серверів; імен доменів пошуку; адрес NTP-серверів; інших параметрів, визначених стандартами IETF. DHCPv6 не замінює повністю механізми IPv6, а доповнює їх. У типовій мережі IPv6 маршрутизатор відіграє ключову роль,

передаючи клієнтам інформацію про префікс і доступність DHCPv6 за допомогою Router Advertisement (RA) повідомлень.

Основні відмінності DHCPv6 від DHCP для IPv4

DHCPv6 має низку принципових відмінностей від DHCPv4. По-перше, DHCPv6 не використовує широкомовні повідомлення, оскільки IPv6 не підтримує broadcast. Натомість застосовується мультикаст, зокрема адреса ff02::1:2 для DHCPv6 серверів і ретрансляторів.

По-друге, у DHCPv6 ідентифікація клієнта не базується безпосередньо на MAC-адресі. Замість цього використовуються ідентифікатори DUID (DHCP Unique Identifier), що забезпечує стабільнішу ідентифікацію навіть при зміні мережевого інтерфейсу.

По-третє, DHCPv6 тісно інтегрований із механізмами IPv6 Neighbor Discovery та Router Advertisement, що визначають модель взаємодії клієнта, маршрутизатора і DHCPv6 сервера.

Архітектура DHCPv6 включає три основні компоненти: клієнт, сервер і ретранслятор. Клієнт − це вузол IPv6, який потребує конфігураційних параметрів. Сервер DHCPv6 зберігає політики адресації та параметрів і відповідає на запити клієнтів. Ретранслятор використовується в сегментованих мережах для передавання DHCPv6 повідомлень між клієнтами і сервером, якщо вони знаходяться в різних мережевих сегментах. Обмін повідомленнями відбувається поверх протоколу UDP із використанням порту 546 для клієнта та 547 для сервера.

На практиці IPv6 розрізняють три основні моделі конфігурації.

– у режимі Stateless DHCPv6 клієнт самостійно формує IPv6-адресу за допомогою SLAAC, а DHCPv6 використовується лише для отримання додаткових параметрів, таких як DNS;

– у режимі Stateful DHCPv6 сервер повністю відповідає за надання IPv6-адрес клієнтам, веде облік виданих адрес і контролює їх життєвий цикл;

– комбінований підхід передбачає одночасне використання SLAAC для адресації та DHCPv6 для сервісних параметрів, що є найпоширенішим варіантом у сучасних мережах.

Повідомлення та процес роботи DHCPv6

Робота DHCPv6 базується на обміні стандартизованими повідомленнями. Процес починається з повідомлення Solicit, яке клієнт надсилає для пошуку доступних серверів. Сервер відповідає повідомленням Advertise, інформуючи про можливість обслуговування клієнта.

Далі клієнт надсилає Request, обираючи конкретний сервер, а сервер підтверджує виділення параметрів повідомленням Reply. Для продовження терміну дії адреси використовуються повідомлення Renew і Rebind.

Час життя адрес і параметрів

DHCPv6 використовує поняття preferred lifetime і valid lifetime для керування життєвим циклом адрес. Preferred lifetime визначає період, протягом якого адреса є бажаною для нових з’єднань, тоді як valid lifetime визначає загальний час її придатності. Такий підхід дозволяє гнучко керувати перенумерацією мережі та поступовим виведенням адрес з експлуатації без порушення активних сесій.

Безпека DHCPv6 є критично важливою, оскільки зловмисний сервер може нав’язати клієнтам некоректні параметри мережі. Основними загрозами є підміна DHCPv6 сервера, атаки відмови в обслуговуванні та маніпуляції з конфігураційними параметрами. Для захисту використовуються механізми фільтрації DHCPv6 трафіку на комутаторах, функції DHCPv6 Guard, а також сегментація мережі. Додатково можливе застосування IPsec для захисту обміну повідомленнями.

SLAAC забезпечує простоту і мінімальну залежність від серверної інфраструктури, але обмежений у можливостях централізованого управління. DHCPv6, навпаки, дозволяє повністю контролювати процес конфігурації, вести облік клієнтів і реалізовувати політики безпеки. Вибір між SLAAC і DHCPv6 залежить від вимог до керованості, масштабу мережі та рівня безпеки. DHCPv6 широко використовують для централізованого управління IPv6-інфраструктурою, автоматизації адміністрування та забезпечення узгодженої роботи мережевих сервісів.

Ієрархічна структура доменів, організації, що керують адресним простором (IANA, ICANN, RIR).

Загальне керування адресним простором IP-адрес здійснює Адміністрація адресного простору Інтернет (IANA – Internet Assigned Numbers Authority), яка є підрозділом неприбуткової Інтернет-корпорації з призначення імен та адрес ICANN (Internet Corporation for Assigned Names and Numbers). IANA підпорядковуються регіональні Інтернет-реєстратори (RIR – Regional Internet Registries), яким, у свою чергу, підпорядковуються локальні Інтернет-реєстратори (LIR – Local Internet Registries) – провайдери послуг Інтернет. Регіональні Інтернет-реєстратори розподіляють IP-адреси як між кінцевими користувачами, так і між локальним Інтернет-провайдерами. Сфера впливу регіональних Інтернет-реєстраторів розповсюджується на певні регіони, а саме:

– RIPE NCC (Reseaux IP Europeens Network Coordination Centre) – Європа, Близький Схід та Центральна Азія;

– ARIN (American Registry for Internet Numbers) – Північна Америка;

– LACNIC (Latin American and Caribbean Internet Addresses Registry) – Південна Америка та басейн Карибського моря;

– APNIC (Asia-Pacific Network Information Centre) – Азійсько- Тихоокеанський регіон;

– AfriNIC (African Network Information Centre) – Африка.

Проблеми та виклики мережевої адресації: вичерпання IPv4, перехід на IPv6 та роль NAT і PAT

Стрімке зростання кількості підключених пристроїв, розвиток мобільних технологій, Інтернету речей та хмарних сервісів призвели до системної проблеми − вичерпання адресного простору IPv4.

Вичерпання пулів IPv4-адрес було офіційно зафіксоване регіональними реєстраторами, що означало неможливість подальшого виділення нових глобальних адрес у традиційному розумінні. Це стало серйозним викликом для операторів зв’язку, провайдерів інтернет-послуг та корпоративних мереж, оскільки модель прямої унікальної адресації кожного пристрою втратила масштабованість.

У відповідь на кризу адресації було запропоновано нову версію протоколу − IPv6. Він використовує 128-бітну адресацію, що забезпечує практично невичерпний адресний простір. IPv6 не лише вирішує проблему кількості адрес, але й спрощує маршрутизацію, підтримує автоматичну конфігурацію, покращує механізми безпеки та оптимізує обробку пакетів у мережевому обладнанні. Попри очевидні переваги, перехід на IPv6 відбувається повільно через необхідність модернізації інфраструктури, програмного забезпечення та підготовки фахівців. Більшість сучасних мереж змушені працювати в умовах співіснування IPv4 та IPv6, використовуючи перехідні механізми.

Одним із ключових тимчасових рішень проблеми вичерпання IPv4 стало використання технології трансляції мережевих адрес − NAT (Network Address Translation). Основна ідея NAT полягає у відокремленні внутрішнього адресного простору мережі від глобального адресного простору Інтернету. Для цього використовуються приватні IP-адреси, визначені стандартами, які не маршрутизуються в глобальній мережі. Пристрої у внутрішній мережі можуть мати однакові приватні адреси в різних організаціях, не створюючи конфліктів.

Принцип роботи NAT базується на зміні IP-адрес у заголовках пакетів під час їх проходження через маршрутизатор або міжмережевий екран. Коли внутрішній хост ініціює з’єднання із зовнішнім ресурсом, NAT-пристрій замінює його приватну IP-адресу на публічну адресу, що належить організації або провайдеру. У таблиці трансляції зберігається відповідність між внутрішньою та зовнішньою адресами, що дозволяє коректно обробляти зворотний трафік.

Подальшим розвитком і найбільш поширеною формою NAT є PAT (Port Address Translation), або трансляція адрес із використанням портів. У цьому випадку велика кількість внутрішніх хостів може одночасно використовувати одну публічну IP-адресу, а розрізнення з’єднань відбувається за номерами транспортних портів. Кожне активне з’єднання має

унікальну комбінацію зовнішньої адреси та порту, що дозволяє маршрутизатору правильно зіставляти пакети з відповідними внутрішніми пристроями.

Застосування NAT і PAT дало змогу суттєво продовжити термін використання IPv4, зменшити потребу в публічних адресах і спростити внутрішню організацію мереж. Водночас ці технології мають низку обмежень і недоліків. Вони порушують принцип наскрізної адресації, ускладнюють роботу деяких протоколів, зокрема тих, що потребують прямого встановлення з’єднання між хостами, та створюють додаткові труднощі для забезпечення прозорої безпеки. У контексті кібербезпеки NAT часто помилково сприймається як захисний механізм, хоча насправді він не замінює повноцінних засобів фільтрації та контролю доступу.

Таким чином, поява NAT була зумовлена насамперед обмеженістю IPv4-адресного простору та необхідністю зберегти працездатність Інтернету в умовах стрімкого зростання кількості підключень. Однак NAT і PAT слід розглядати лише як тимчасове рішення, яке не усуває фундаментальних обмежень застарілої архітектури. Стратегічним напрямом розвитку мереж залишається повноцінний перехід на IPv6, що відновлює початкову ідею глобальної унікальної адресації та створює основу для подальшого масштабування і розвитку цифрової інфраструктури.

Тема 3. Моделі та протоколи

Основи передавання даних. Еталонні моделі. Модель OSI: структура, рівні та функції. Модель TCP/IP: архітектура, подібності та відмінності від OSI. Порівняльний аналіз OSI та TCP/IP у практиці. Роль ISO, IEEE, ITU, IETF, ICANN. Поняття протоколу: правила, формати, послідовність дій. Інкапсуляція та декапсуляція даних. Класифікація протоколів за рівнями. Протоколи канального рівня (Ethernet, Wi-Fi). Протоколи мережевого рівня (IP, ICMP, ARP). Протоколи транспортного рівня (TCP, UDP). Прикладні протоколи (HTTP, FTP, SMTP, DNS, DHCP, DHCPv6.). Організації зі стандартизації. Інкапсуляція та доступ до даних. Механізм проходження даних через рівні моделі. Формування кадру, пакета, сегмента та повідомлення. IP-телефонія. Відстеження роботи протоколів у Wireshark. Візуалізація інкапсуляції даних у мережевих емуляторах.

Передавання даних у комп'ютерних мережах є основою сучасних інформаційних технологій і спрямоване на забезпечення логічної комунікації між системами, що можуть бути розташовані як у межах локальних мереж (LAN), так і глобальних мереж (WAN) або в Інтернеті. Функціонування мереж базується на розбитті початкового інформаційного блоку на менші одиниці (кадри, пакети, сегменти, повідомлення), передачі їх по фізичному середовищу, маршрутизації між вузлами та відновленні початкового об'єму даних у місці призначення. Цей процес опирається на множину еталонних моделей і протоколів, що визначають правила формування, адресації, маршрутизації та обробки даних.

Еталонні моделі передачі даних

Модель OSI [11, 16]є класичною еталонною моделлю взаємодії відкритих систем та описує процес мережевого взаємодію як послідовність функціональних рівнів. Вона була розроблена Міжнародною організацією зі стандартизації (ISO) у 1978 р., щоб уніфікувати підходи до побудови мережевих протоколів та взаємодії різних систем незалежно від виробника і технології. Кожен з семи рівнів цієї моделі має чітко визначені функції:

Рівень 1 − Фізичний: відповідає за передачу бітів через фізичні середовища (кабелі, радіохвилі).

Рівень 2 − Канальний: забезпечує організацію доступу до середовища і передачу кадрів між безпосередньо з'єднаними вузлами.

Рівень 3 − Мережевий: реалізує логічну адресацію та маршрутизацію пакетів через мережу.

Рівень 4 − Транспортний: забезпечує надійне передавання сегментів або датаграм між кінцевими вузлами.

Рівні 5–7 − Сеансовий, представлення та прикладний: відповідають за встановлення/закриття сеансів, представлення даних та надання сервісів для прикладних програм.

Модель OSI має важливе концептуальне значення, хоча безпосередньо не реалізується у сучасних мережах як повний стек протоколів. Проте вона лишається основою для розуміння структуризації мережевих функцій.

Модель TCP/IP є практичною архітектурою, на якій побудований Інтернет і більшість сучасних мереж. Ця модель виникла раніше за OSI та була розроблена як результат практичних потреб створення глобальної мережі з відкритою взаємодією пристроїв. На відміну від OSI, TCP/IP має чотири логічні рівні:

Рівень доступу до мережі (Network Access / Link Layer): включає фізичні та канальні протоколи, наприклад Ethernet, Wi-Fi − компоненти, що відповідають за передачу кадрів в межах однієї фізичної мережі.

Internet Layer (Мережевий): відповідає за логічну адресацію і маршрутизацію через протокол IP та пов'язані механізми, такі як ICMP і ARP.

Transport Layer (Транспортний): забезпечує передачу даних між кінцевими точками за допомогою TCP (надійне передавання) або UDP (ненадійне, але швидке).

Application Layer (Прикладний): включає сервіси, що надають прикладні функції, наприклад HTTP, FTP, SMTP, DNS та DHCP.

Ця архітектура віддзеркалює набір реальних протоколів, які взаємодіють для забезпечення передачі даних у глобальних мережах, і є основою для виконання мережевих сервісів.

Порівняльний аналіз OSI та TCP/IP у практиці

Порівняння моделей OSI та TCP/IP показує, що OSI слугує концептуальним еталоном, що розділяє мережеві функції на семи рівнях, тоді як TCP/IP − це практичний стек протоколів, що реалізує передачу даних у реальних мережах з меншим числом абстрактних рівнів та злитими функціями. Наприклад, у TCP/IP фізичний і канальний рівні OSI об'єднані у рівень доступу до мережі, а OSI-рівні представлення й сеансу функціонально входять у прикладний рівень TCP/IP. Попри ці відмінності, для аналізу мережевих проблем і проектування мереж часто користуються моделлю OSI як логічним каркасом, а TCP/IP − для практичної реалізації передачі даних.

У мережевих технологіях протокол − це формалізований набір прав, форматів, механізмів взаємодії і процедур, що визначають, як дані повинні бути передані між двома чи більше кінцевими точками у мережі. Протокол визначає:

Формати повідомлень (структури заголовків і полів) і синтаксис передачі;

Правила послідовності дій (коли і як ініціюються, підтримуються і завершуються обміни);

Механізми обробки помилок та контроль цілісності.

Ці визначення реалізуються на кожному рівні моделі OSI або TCP/IP, забезпечуючи чітке розмежування відповідальності між функціональними компонентами.

Протоколи класифікують за рівнями моделі OSI/TCP-IP:

Канальний рівень [18]: Ethernet, Wi-Fi − визначають формування і структуру кадрів у локальних мережах, доступ до фізичного середовища та MAC-адресацію.

Мережевий рівень [19]: IP − забезпечує логічну адресацію та маршрутизацію пакетів; ICMP − служить для контролю та обміну службовою інформацією про стан мережі; ARP − визначає відповідність між IP-адресою та MAC-адресою.

Транспортний рівень: TCP − забезпечує надійне передавання з контролем потоку і помилок; UDP − легкий, ненадійний протокол для швидких передач, де гарантована доставка не критична.

Прикладний рівень: HTTP, FTP, SMTP, DNS, DHCP (і його IPv6-версія DHCPv6) − реалізують прикладні сервіси користувача: веб-обмін, передавання файлів, електронна пошта, розв'язання доменних імен та автоматичне налаштування параметрів мережевих клієнтів.

Роль ISO, IEEE, ITU, IETF, ICANN у розвитку мережевих технологій

Розвиток комп'ютерних мереж і глобальних телекомунікацій був би неможливий без діяльності міжнародних організацій, які займаються розробленням стандартів, регулюванням і координацією технічних рішень. Найважливішу роль у цьому процесі відіграють ISO, IEEE, ITU, IETF та ICANN.

ISO (International Organization for Standardization) є міжнародною організацією зі стандартизації, що розробляє загальні стандарти для різних галузей, зокрема інформаційних технологій. У сфері комп'ютерних мереж ISO відома насамперед створенням еталонної моделі OSI, яка стала теоретичною основою для розуміння принципів мережевої взаємодії. Стандарти ISO сприяють сумісності обладнання та програмного забезпечення різних виробників і забезпечують єдиний підхід до проєктування систем.

IEEE (Institute of Electrical and Electronics Engineers) зосереджується на технічних стандартах у галузі електроніки, електротехніки та комп'ютерних мереж. Саме IEEE розробляє стандарти сімейства 802, до яких належать Ethernet (IEEE 802.3) та бездротові мережі Wi-Fi (IEEE 802.11). Ці стандарти визначають роботу фізичного та канального рівнів і є основою більшості сучасних локальних мереж.

ITU (International Telecommunication Union) є спеціалізованою установою ООН, що координує глобальні телекомунікації. Вона розробляє міжнародні рекомендації для телефонного зв'язку, передачі даних, радіозв'язку та супутникових систем. ITU також

відповідає за розподіл радіочастотного спектра і орбітальних позицій супутників, що має ключове значення для стабільної роботи світових систем зв'язку.

IETF (Internet Engineering Task Force) відіграє провідну роль у розвитку Інтернету. Це відкрита спільнота фахівців, яка розробляє та публікує стандарти у вигляді документів RFC (Request for Comments). Саме IETF створила ключові інтернет-протоколи, зокрема IP, TCP, UDP, HTTP, SMTP і DNS. Її діяльність забезпечує еволюцію Інтернету, зберігаючи сумісність і відкритість мережі.

ICANN (Internet Corporation for Assigned Names and Numbers) відповідає за координацію унікальних ідентифікаторів Інтернету. До її повноважень належать управління доменними іменами, IP-адресним простором і кореневими DNS-серверами. Завдяки ICANN забезпечується унікальність адрес і доменів, що є необхідною умовою стабільної та безперервної роботи глобальної мережі.

Таким чином, ISO, IEEE, ITU, IETF та ICANN виконують взаємодоповнювальні функції, формуючи технічну, організаційну та регуляторну основу сучасних комп'ютерних мереж і Інтернету.

Поняття протоколу в комп'ютерних мережах

Функціонування комп'ютерних мереж ґрунтується на чітко визначених правилах взаємодії між пристроями, незалежно від їх апаратної платформи, операційної системи чи виробника. Сукупність таких правил у теорії та практиці мережевих технологій отримала назву протоколу. Мережевий протокол − це формалізований опис правил, форматів і процедур, які визначають спосіб обміну даними між двома або більше вузлами мережі.

Протокол задає не лише форму передавання інформації, а й логіку взаємодії: коли і за яких умов відбувається передавання, як ініціюється з'єднання, яким чином підтверджується успішна доставка даних, як здійснюється контроль помилок і відновлення після збоїв. Без узгоджених протоколів взаємодія в мережі була б неможливою, оскільки кожен пристрій інтерпретував би дані по-своєму.

У структурі будь-якого протоколу можна виділити три базові складові: правила, формати та послідовність дій. Правила визначають допустиму поведінку учасників обміну даними, включно з ролями сторін, умовами початку й завершення сеансу зв'язку та реакцією на помилки. Формати описують структуру повідомлень, зокрема порядок розташування полів заголовка, довжину даних, способи кодування адресної та службової інформації. Послідовність дій регламентує часову логіку обміну, тобто визначає, які повідомлення і в якій черговості мають бути надіслані для коректної взаємодії.

Таким чином, протокол є основою сумісності мережевих пристроїв і програмних систем, а також гарантом надійності та передбачуваності передавання інформації.

Інкапсуляція та декапсуляція даних

Процес передавання даних у мережі відбувається поетапно і базується на принципі багаторівневої обробки інформації. Центральним механізмом цього процесу є інкапсуляція даних. Інкапсуляція полягає в послідовному додаванні службової інформації до користувацьких даних під час їх проходження через рівні мережевої моделі від прикладного рівня до фізичного.

На кожному рівні мережевої архітектури до даних додається власний заголовок, а в окремих випадках − і трейлер. Ці службові поля містять інформацію, необхідну для коректної доставки повідомлення, зокрема адреси відправника й отримувача, ідентифікатори протоколів, контрольні суми, номери портів або послідовності сегментів. У результаті первинні дані перетворюються на складну структуру, яка послідовно набуває форми сегмента, пакета, кадру або бітового потоку.

Протилежним процесом є декапсуляція, яка відбувається на стороні отримувача. Під час декапсуляції дані рухаються знизу вгору по рівнях мережевої моделі. Кожен рівень аналізує та обробляє відповідний заголовок, після чого видаляє його і передає корисне навантаження на вищий рівень. У кінцевому підсумку прикладна програма отримує дані в тому вигляді, в якому вони були сформовані відправником.

Інкапсуляція та декапсуляція забезпечують модульність мережевої архітектури, що дозволяє незалежно розвивати та вдосконалювати окремі протоколи без порушення роботи всієї системи.

Класифікація протоколів за рівнями мережевої моделі

Для систематизації протоколів і спрощення проектування мереж застосовується рівнева організація, найвідомішими реалізаціями якої є модель OSI та модель TCP/IP. Класифікація протоколів за рівнями дає змогу чітко визначити їх функціональне призначення та область відповідальності.

На прикладному рівні зосереджені протоколи, безпосередньо орієнтовані на взаємодію з користувачем або прикладними програмами. Вони забезпечують доступ до мережевих сервісів, таких як передавання файлів, електронна пошта, веб-доступ або служби каталогів. Ці протоколи не займаються доставкою пакетів у фізичному сенсі, а формують логіку прикладної взаємодії.

Транспортний рівень відповідає за наскрізне передавання даних між вузлами, контроль цілісності, управління потоком та, за потреби, надійність доставки. Протоколи цього рівня працюють із логічними з'єднаннями та забезпечують мультиплексування даних між кількома прикладними процесами.

На мережевому рівні функціонують протоколи, що забезпечують логічну адресацію та маршрутизацію даних між різними мережами. Саме на цьому рівні приймаються рішення щодо вибору маршруту, обробляються таблиці маршрутизації та реалізується доставка пакетів до кінцевого вузла через проміжні маршрутизатори.

Канальний рівень об'єднує протоколи, які регламентують передавання даних у межах одного фізичного сегмента мережі. Вони відповідають за формування кадрів, фізичну адресацію, виявлення помилок та управління доступом до середовища передавання.

Нарешті, фізичний рівень визначає електричні, оптичні або радіотехнічні характеристики передавання сигналів. Хоча формально він не оперує протоколами у класичному розумінні, саме цей рівень забезпечує фізичну можливість передавання бітів у середовищі зв'язку.

Узгоджена робота протоколів усіх рівнів формує єдину систему передавання даних, у якій кожен рівень виконує строго визначену функцію, не дублюючи і не підміняючи інші.

Мережеві протоколи є фундаментом сучасних комп'ютерних мереж, забезпечуючи стандартизовану, надійну та масштабовану взаємодію між пристроями. Поняття протоколу охоплює правила, формати та послідовність дій, необхідні для коректного обміну даними. Процеси інкапсуляції та декапсуляції реалізують багаторівневу обробку інформації, що дозволяє абстрагувати складність мережевих технологій. Класифікація протоколів за рівнями дає змогу структурувати мережеві рішення та ефективно проектувати, впроваджувати й аналізувати комп'ютерні мережі різного масштабу та призначення.

Протоколи канального рівня (Ethernet, Wi-Fi)

Канальний рівень [18] є другим рівнем еталонної семирівневої моделі OSI та відіграє ключову роль у забезпеченні надійної передачі даних між безпосередньо з'єднаними вузлами мережі. Саме на цьому рівні відбувається формування кадрів, фізична адресація пристроїв, виявлення помилок передавання та керування доступом до спільного середовища передавання даних. Протоколи канального рівня тісно взаємодіють із фізичним рівнем, використовуючи його для передачі бітів, але водночас забезпечують логічну структуру передавання інформації у вигляді кадрів.

Канальний рівень традиційно поділяється на два підрівні: підрівень логічного керування каналом (Logical Link Control, LLC) та підрівень керування доступом до середовища (Media Access Control, MAC). Підрівень LLC відповідає за ідентифікацію протоколів мережевого рівня та логічний контроль з'єднання, тоді як підрівень MAC реалізує механізми адресації та доступу до фізичного середовища передавання. Найпоширенішими технологіями канального рівня в локальних мережах є Ethernet та Wi-Fi, стандартизовані відповідно організацією IEEE у серіях стандартів IEEE 802.3 та IEEE 802.11.

Ethernet є базовою технологією дротових локальних обчислювальних мереж. Вона була розроблена для забезпечення простого, масштабованого та ефективного передавання

даних у середовищі спільного доступу. Класична модель Ethernet передбачала використання методу множинного доступу з виявленням колізій (CSMA/CD), за якого вузол перед початком передавання перевіряє, чи є середовище вільним, а у випадку одночасної передачі кількох станцій відбувається колізія, що виявляється та обробляється повторною передачею кадру. З розвитком комутованих мереж і повнодуплексного режиму роботи роль механізму CSMA/CD значно зменшилася, однак він залишається важливою частиною теоретичних основ Ethernet.

Кадр Ethernet має чітко визначену структуру, яка включає преамбулу та стартовий обмежувач кадру, MAC-адресу призначення, MAC-адресу джерела, поле типу або довжини, поле корисних даних та контрольну суму кадру (Frame Check Sequence, FCS). MAC-адреси в Ethernet є унікальними 48-бітними ідентифікаторами, що присвоюються мережевим інтерфейсам і забезпечують однозначну ідентифікацію вузлів у межах локального сегмента. Поле FCS використовується для виявлення помилок за допомогою циклічного надлишкового коду (CRC), що дозволяє приймальній стороні визначити факт спотворення даних під час передавання.

Ethernet підтримує різні швидкості та типи фізичного середовища, починаючи від класичних 10 Мбіт/с і завершуючи сучасними стандартами 10, 40, 100 Гбіт/с і більше. У практиці сучасних комп'ютерних мереж Ethernet є основою корпоративних, датацентрових та провайдерських інфраструктур завдяки своїй простоті, надійності та широкій підтримці обладнання.

На відміну від Ethernet, технологія Wi-Fi забезпечує бездротову передачу даних у локальних мережах і ґрунтується на використанні радіоканалу як середовища передавання. Wi-Fi також належить до стандартів сімейства IEEE 802, зокрема до серії IEEE 802.11, яка визначає фізичний і канальний рівні для бездротових мереж. Спільний характер радіоефіру та неможливість прямого виявлення колізій зумовили використання іншого механізму доступу до середовища − множинного доступу з уникненням колізій (CSMA/CA).

У Wi-Fi перед початком передачі станція не лише перевіряє зайнятість каналу, а й використовує випадкову затримку та механізми підтвердження доставки кадру. Кожен успішно прийнятий кадр підтверджується спеціальним керуючим повідомленням ACK, що підвищує надійність передавання, але водночас збільшує накладні витрати протоколу. За відсутності підтвердження кадр вважається втраченим і передається повторно.

Кадр Wi-Fi має складнішу структуру порівняно з Ethernet і може містити до чотирьох MAC-адрес, що пов'язано з особливостями бездротової архітектури, зокрема з використанням точок доступу та режимів ретрансляції. У протоколі передбачені різні типи кадрів: кадри даних, керуючі кадри та кадри управління, які використовуються для встановлення з'єднання, аутентифікації, асоціації клієнтів і керування енергоспоживанням.

Особливу увагу в технології Wi-Fi приділено питанням безпеки. На канальному рівні реалізуються механізми шифрування та автентифікації, зокрема стандарти WPA2 та WPA3, які забезпечують конфіденційність і цілісність переданих даних у бездротовому середовищі. Це є принциповою відмінністю від класичного Ethernet, де питання безпеки зазвичай вирішуються на вищих рівнях або за допомогою додаткових технологій, таких як VLAN, MAC-фільтрація чи мережевий контроль доступу.

Порівнюючи Ethernet і Wi-Fi, слід зазначити, що обидві технології реалізують однакові базові функції канального рівня, але адаптовані до різних фізичних середовищ. Ethernet забезпечує вищу стабільність, менші затримки та більшу пропускну здатність, тоді як Wi-Fi надає мобільність і гнучкість підключення за рахунок бездротового доступу. У сучасних мережах ці технології не конкурують, а взаємодоповнюють одна одну, формуючи єдину інфраструктуру доступу до мережевих ресурсів.

Таким чином, протоколи канального рівня Ethernet і Wi-Fi є фундаментом локальних комп'ютерних мереж. Їх розуміння є необхідним для ефективного проєктування, адміністрування та захисту мережевих систем, а також для подальшого вивчення протоколів вищих рівнів моделі OSI та сучасних мережевих технологій.

Протоколи мережевого рівня (IP, ICMP, ARP) та транспортного рівня (TCP, UDP)

Функціонування комп'ютерних мереж ґрунтується на ієрархічній організації протоколів, кожен з яких виконує чітко визначені завдання. У моделях OSI та TCP/IP ключову роль у передаванні даних між вузлами відіграють мережевий і транспортний рівні, які забезпечують адресацію, маршрутизацію, доставку та контроль передавання інформації.

Мережевий рівень та його протоколи

Мережевий рівень [19] відповідає за логічну адресацію вузлів, вибір маршруту передавання даних і доставку пакетів між різними мережами. Центральним протоколом цього рівня є Internet Protocol (IP), який працює разом із допоміжними протоколами ICMP та ARP.

Internet Protocol (IP) є базовим протоколом Інтернету та реалізує принцип best effort delivery, тобто не гарантує доставку пакетів, їх порядок чи відсутність дублювання. IP виконує фрагментацію даних, інкапсуляцію сегментів транспортного рівня в пакети та забезпечує їх маршрутизацію. Існують дві основні версії протоколу: IPv4, що використовує 32-бітну адресу, та IPv6, який застосовує 128-бітну адресацію й усуває низку обмежень IPv4, зокрема дефіцит адресного простору та залежність від NAT.

IP не здійснює контроль помилок на рівні доставки, однак забезпечує базову перевірку цілісності заголовка пакета. Вся відповідальність за надійність передавання покладається на транспортний рівень.

Internet Control Message Protocol (ICMP) використовується для передавання службових і діагностичних повідомлень. ICMP не призначений для транспортування прикладних даних, але відіграє важливу роль у керуванні мережею та виявленні помилок. За його допомогою вузли повідомляють про недоступність мережі або хоста, перевищення часу життя пакета (TTL), проблеми маршрутизації. Практичне значення ICMP проявляється в таких утилітах, як ping і traceroute, які застосовуються для діагностики стану мережі.

Address Resolution Protocol (ARP) забезпечує взаємозв'язок між логічною IP-адресою та фізичною MAC-адресою у локальній мережі. Оскільки передавання кадрів у канальному рівні відбувається за MAC-адресами, вузол повинен знати фізичну адресу отримувача. ARP працює шляхом широкомовного запиту, у відповідь на який вузол із відповідною IP-адресою надсилає свою MAC-адресу. Отримані відповідності зберігаються в ARP-кеші. У контексті кібербезпеки ARP має критичне значення, оскільки є вразливим до атак типу ARP-spoofing або ARP-poisoning.

Транспортний рівень та його протоколи

Транспортний рівень забезпечує логічну взаємодію між прикладними процесами на різних вузлах мережі. Основними протоколами цього рівня є Transmission Control Protocol (TCP) та User Datagram Protocol (UDP), які суттєво відрізняються за принципами роботи.

Transmission Control Protocol (TCP) є орієнтованим на з'єднання протоколом, який гарантує надійне та впорядковане доставлення даних. Перед початком обміну TCP встановлює з'єднання за допомогою триетапного рукостискання (three-way handshake), що забезпечує синхронізацію між відправником і отримувачем. TCP виконує контроль цілісності даних, керування потоком, повторну передачу втрачених сегментів та адаптацію швидкості передавання відповідно до завантаженості мережі.

Завдяки цим властивостям TCP широко використовується у сервісах, де критично важлива коректність і повнота передавання даних, зокрема у веб-з'єднаннях (HTTP/HTTPS), електронній пошті (SMTP, IMAP, POP3) та передаванні файлів (FTP).

User Datagram Protocol (UDP) є протоколом без встановлення з'єднання, який не гарантує доставку, порядок або відсутність дублювання пакетів. Основною перевагою UDP є мінімальні накладні витрати та висока швидкість передавання. Протокол не виконує керування потоком чи повторної передачі даних, що робить його ефективним для застосувань реального часу.

UDP широко використовується в потоковому відео та аудіо, онлайн-іграх, системах VoIP, а також у службових протоколах, таких як DNS і DHCP. Надійність у таких системах зазвичай реалізується на прикладному рівні.

Порівняльний аналіз та практичне значення

Мережевий і транспортний рівні взаємодіють між собою, утворюючи основу міжмережевої комунікації. IP забезпечує доставку пакетів між мережами, ICMP − діагностику та керування помилками, ARP − зв'язок між логічною та фізичною адресацією. TCP і UDP, у свою чергу, надають прикладним програмам різні моделі обміну даними, дозволяючи обирати між надійністю та швидкодією.

Прикладні протоколи комп'ютерних мереж

Прикладний рівень є верхнім рівнем як у моделі OSI, так і в архітектурі TCP/IP. Його основне призначення полягає у забезпеченні безпосередньої взаємодії мережевих сервісів з користувацькими застосунками. Саме на цьому рівні реалізуються протоколи, які визначають правила обміну даними між програмами, що працюють на різних вузлах мережі.

Протоколи прикладного рівня [20] не займаються маршрутизацією, фрагментацією або фізичною передачею сигналів. Вони використовують сервіси транспортного рівня (TCP або UDP) для доставки даних і зосереджуються на форматі повідомлень, логіці обміну та семантиці запитів і відповідей. До найпоширеніших прикладних протоколів належать HTTP, FTP, SMTP, DNS, DHCP та DHCPv6, які забезпечують функціонування веб-сервісів, передавання файлів, електронної пошти та автоматичну конфігурацію мережевих параметрів.

HTTP (HyperText Transfer Protocol) − це протокол прикладного рівня, призначений для передавання гіпертекстових документів у Всесвітній павутині. Він лежить в основі роботи веб-браузерів і веб-серверів та забезпечує доступ до веб-сторінок, зображень, відео, API-сервісів і хмарних застосунків.

HTTP є протоколом типу «клієнт–сервер». Клієнт, зазвичай веб-браузер, ініціює з'єднання та надсилає HTTP-запит, а сервер обробляє його і повертає HTTP-відповідь. Протокол є безстанним, тобто сервер не зберігає інформацію про попередні запити клієнта, якщо це не реалізовано додатковими механізмами, такими як cookies або сесії.

Основними методами HTTP є GET, POST, PUT, DELETE, HEAD та OPTIONS. Вони визначають тип дії, яку клієнт хоче виконати над ресурсом. Для передавання даних HTTP зазвичай використовує TCP-порт 80, а його захищена версія HTTPS, що працює з використанням TLS, − порт 443.

FTP (File Transfer Protocol) − це прикладний протокол, призначений для передавання файлів між клієнтом і сервером у мережі TCP/IP. Він широко використовувався для обміну файлами в локальних і глобальних мережах, хоча в сучасних системах часто замінюється більш безпечними рішеннями.

Особливістю FTP є використання двох з'єднань: керуючого та з'єднання для передавання даних. Керуюче з'єднання встановлюється через TCP-порт 21 і використовується для передавання команд, тоді як дані передаються через окреме з'єднання, параметри якого залежать від режиму роботи − активного або пасивного.

FTP не забезпечує шифрування облікових даних та передаваних даних, що є його суттєвим недоліком з точки зору безпеки. Для усунення цієї проблеми були розроблені розширення FTPS та альтернативний протокол SFTP, який працює поверх SSH.

SMTP (Simple Mail Transfer Protocol) − це прикладний протокол, призначений для передавання електронної пошти між поштовими серверами. Він забезпечує пересилання повідомлень від клієнта до сервера, а також між серверами електронної пошти.

SMTP використовує модель «store-and-forward», за якої повідомлення тимчасово зберігається на проміжних серверах до моменту доставки кінцевому адресату. Протокол працює поверх TCP і за замовчуванням використовує порт 25, а також порти 587 та 465 для захищеної передачі з використанням TLS.

SMTP відповідає лише за надсилання пошти. Для отримання повідомлень використовуються інші прикладні протоколи, зокрема POP3 та IMAP. У сучасних системах SMTP тісно інтегрується з механізмами автентифікації, шифрування та захисту від спаму.

DNS (Domain Name System) − це розподілена система імен, яка забезпечує перетворення символьних доменних імен у IP-адреси та навпаки. DNS є критично важливим

елементом функціонування Інтернету, оскільки дозволяє користувачам звертатися до ресурсів за зрозумілими іменами замість числових адрес.

DNS організований у вигляді ієрархічної розподіленої бази даних, що складається з кореневих серверів, серверів доменів верхнього рівня та авторитетних серверів доменів. Запити DNS зазвичай передаються з використанням UDP через порт 53, а у випадках великих відповідей або зонних трансферів використовується TCP.

DNS підтримує різні типи ресурсних записів, серед яких A, AAAA, MX, CNAME, NS та TXT. Кожен із них виконує конкретну функцію, наприклад, визначення IP-адреси вузла або поштового сервера домену.

DHCP (Dynamic Host Configuration Protocol) − це прикладний протокол, який використовується для автоматичної конфігурації мережевих параметрів вузлів у IP-мережах. Він дозволяє динамічно призначати IP-адреси, маски підмереж, шлюзи за замовчуванням, DNS-сервери та інші параметри без ручного втручання адміністратора.

DHCP працює за моделлю клієнт–сервер і використовує UDP-порти 67 для сервера та 68 для клієнта. Процес отримання адреси складається з чотирьох основних етапів: виявлення сервера, пропозиції адреси, запиту та підтвердження. Така послідовність відома як DORA-процес.

Завдяки DHCP значно спрощується адміністрування мереж, зменшується кількість помилок конфігурації та забезпечується ефективне використання адресного простору IPv4.

DHCPv6 є розвитком протоколу DHCP, адаптованим для роботи в мережах IPv6. Він призначений для автоматичної конфігурації параметрів IPv6-вузлів, зокрема адрес, префіксів, DNS-серверів та інших мережевих опцій.

На відміну від IPv4, у середовищі IPv6 можливе поєднання DHCPv6 з механізмом SLAAC, який дозволяє вузлам самостійно формувати адресу на основі оголошень маршрутизатора. DHCPv6 може працювати як у режимі повного керування адресацією, так і в режимі надання лише додаткових параметрів конфігурації.

Протокол використовує UDP-порти 546 для клієнта та 547 для сервера. DHCPv6 відіграє важливу роль у сучасних корпоративних і провайдерських мережах, де впроваджується IPv6-адресація.

Прикладні протоколи є ключовим елементом функціонування комп’ютерних мереж, оскільки саме вони забезпечують реалізацію мережевих сервісів, з якими безпосередньо взаємодіє користувач. HTTP, FTP, SMTP, DNS, DHCP та DHCPv6 охоплюють основні сценарії використання мереж − від доступу до веб-ресурсів і передавання файлів до електронної пошти та автоматичної конфігурації вузлів.

Організації зі стандартизації мережевих технологій

Ефективна робота глобальних мереж і взаємодія обладнання різних виробників можливі завдяки діяльності міжнародних організацій, що займаються узгодженням і стандартизацією мережевих протоколів і технологій.

International Organization for Standardization (ISO): добровільна міжнародна організація, що розробляє міжнародні стандарти, включно з OSI Reference Model, і забезпечує загальні правила та рекомендації для комунікаційних протоколів.

Institute of Electrical and Electronics Engineers (IEEE): професійне товариство, що розробляє технічні стандарти у галузі електротехніки та обчислювальної техніки. Комітет IEEE 802 стандартизує поширені локальні мережеві технології, зокрема Ethernet (802.3) та Wi-Fi (802.11).

International Telecommunication Union (ITU-T): сектор стандартів телекомунікацій, що видає рекомендації щодо цифрових телекомунікацій та мережевої взаємодії, включно з компонентами фізичного та канального рівнів мереж.

Internet Engineering Task Force (IETF): відкрита міжнародна спільнота інженерів і дослідників, яка розробляє стандарти для Інтернет-протоколів, описані у формі RFC (Request For Comments). На IETF лежить відповідальність за технічні специфікації основних протоколів стеку TCP/IP.

Internet Corporation for Assigned Names and Numbers (ICANN): неурядова організація, що координує розподіл IP-адрес, управління DNS (система доменних імен) та роботу кореневих серверів, що є критично важливими для функціонування глобального Інтернету.

Ці організації тісно взаємодіють між собою та підтримують розроблення відкритих стандартів, що забезпечують інтероперабельність мереж та пристроїв по всьому світу.

Механізм інкапсуляції − це процес, у якому кожен рівень моделі додає власний заголовок (інколи трейлер) до даних, що надходять із вищого рівня, формуючи відповідний PDU (Protocol Data Unit) − сегменти, пакети, кадри. У зворотному порядку декапсуляція відбувається при прийомі даних, коли кожен рівень видаляє свою обгортку та передає корисну інформацію вище.

Кадр (Frame) формується на канальному рівні, пакет (Packet) − на мережевому, сегмент (Segment) − на транспортному, а повідомлення (Message) − на прикладному рівні. Цей механізм дозволяє ізольовано обробляти мережеві функції на кожному рівні та забезпечує модульність дизайну мереж.

Механізм проходження даних через рівні моделі

Коли прикладна програма генерує дані (наприклад HTTP-запит), вони передаються вниз по стеку протоколів. На кожному рівні додається відповідний заголовок, що містить службову інформацію (адреси, номери портів, контрольні суми). Далі сформовані кадри передаються через фізичне середовище до приймача, де процес повторюється у зворотному порядку − заголовки видаляються, і корисна інформація передається вище. Цей послідовний «спуск» і «підйом» через рівні і є суттю логічної передачі даних.

Практичні аспекти: IP-телефонія, Wireshark, візуалізація інкапсуляції

IP-телефонія (VoIP) − приклад мережевого сервісу, де аудіо передається як цифрові пакети через IP-мережі, використовуючи транспортні протоколи (часто UDP для зменшення затримок), і прикладні протоколи сигналізації (наприклад SIP). Надійність і якість у VoIP залежать від правильного маршрутування, контролю потоку та мінімізації втрат пакетів.

Wireshark [11, 14] − це мережевий аналізатор, що дозволяє «перехоплювати» та візуально досліджувати трафік мережі. Використовуючи відстеження протоколів, можна бачити, як інкапсульовані дані проходять через рівні, а також аналізувати заголовки кадрів, пакетів і сегментів у реальному часі.

Емулятори мереж (наприклад GNS3, Packet Tracer) дозволяють візуалізувати процес інкапсуляції та траси даних між вузлами, що є корисним навчальним інструментом для розуміння мережевих моделей у практиці.

Тема 4. Принципи комутації та маршрутизації

Роль комутації та маршрутизації в мережах різних рівнів. Історичний розвиток технологій передавання даних. Основні поняття комутації. Методи комутації. Організація роботи комутаторів другого рівня (Layer 2 Switch). Забезпечення відмовостійкості (Spanning Tree Protocol).

Принципи маршрутизації. Визначення маршрутизації та її відмінність від комутації. Таблиці маршрутизації, метрики та алгоритми вибору шляху. Статична маршрутизація та її застосування. Динамічна маршрутизація: основні протоколи (RIP, OSPF, EIGRP, BGP). Маршрутизатори багаторівневі (Layer 3 Switch) та інтеграція з комутаторами. Порівняння комутації та маршрутизації: спільні риси та відмінності. Конфігурація комутатора та маршрутизатора у Cisco Packet Tracer. Значення принципів комутації та маршрутизації для розвитку сучасних мереж. Перспективи вдосконалення технологій (SDN, централізоване управління трафіком).

Комутація і сегментація мережі

Хоча для створення корпоративної мережі використовуються як комутатори, так і маршрутизатори, архітектура більшості корпоративних мереж у значній мірі ґрунтується на комутаторах. Вартість комутаторів з розрахунку на порт, нижча, ніж у маршрутизаторів, і вони забезпечують швидке пересилання кадрів зі швидкістю передачі даних по кабелю.

Комутатор – універсальний пристрій 2-го рівня, який використовується для з'єднання декількох вузлів. У більш складному варіанті комутатор підключається до одного чи декількох комутаторів для створення, контролю та обслуговування резервних каналів і з'єднань VLAN. Комутатор однаково обробляє всі типи трафіку, незалежно від їхнього призначення.

Комутатор передає трафік у відповідності до MAC-адрес. Кожен комутатор тримає таблицю MAC-адрес у високопродуктивній пам'яті, що називається асоціативною пам'яттю (CAM). Комутатор заново створює таблицю при кожній активації, використовуючи MAC-адреси джерела вхідних кадрів і номера портів, через які вони отримані. Комутатор видаляє запис з таблиці MAC-адрес, якщо вони не використовуються протягом визначеного періоду часу. Цей період називається таймером старіння (aging timer). Як тільки одноадресний кадр прибуває на порт, комутатор знаходить MAC-адресу джерела в кадрі. Потім він виконує пошук по таблиці MAC-адрес і знаходить запис, що відповідає адресі. Якщо MAC-адреса відсутня в таблиці, комутатор додає MAC-адресу і номер порту та активує таймер старіння. Якщо MAC-адреса джерела вже існує, комутатор скидає таймер старіння. Після цього комутатор шукає MAC-адресу призначення в таблиці MAC-адрес. Якщо запис існує, комутатор пересилає кадр на порт із відповідним номером. Якщо запису не існує, комутатор виконує лавинну маршрутизацію (floods) кадру через всі порти, крім порту, на якому він був прийнятий [11].

У корпоративному середовищі висока доступність, швидкість та смуга пропускання мережі мають першорядне значення. Розмір доменів широкомовного розсилання і доменів колізій впливає на потоки трафіку. Як правило, великі домени широкомовного розсилання і домени колізій погіршують ці критично важливі показники.

Якщо комутатор отримує широкомовний кадр, він розсилає його з усіх активних інтерфейсів так, як кадр із невідомою MAC-адресою призначення. Усі пристрої, що отримують широкомовне розсилання, складають домен широкомовного розсилання. При збільшенні числа з'єднаних комутаторів, розмір домену широкомовного розсилання також збільшується.

Домени колізій створюють аналогічну проблему. Чим більше пристроїв входить у домен колізій, тим частіше вони виникають. Комутатори використовують функцію мікросегментації, щоб зменшити розмір домену колізій до одного порту комутатора. Коли вузол підключається до порту комутатора, створюється виділене підключення. Коли два з'єднаних вузли взаємодіють один з одним, комутатор звертається до таблиці комутації і створює віртуальне підключення (мікросегмент) між портами.

Комутатор підтримує віртуальний канал (VC) до припинення сеансу. Кілька віртуальних каналів можуть бути активні одночасно. Мікросегментація покращує коефіцієнт використання смуги пропускання за рахунок зменшення кількості колізій і підтримки декількох паралельних підключень.

Комутатори можуть підтримувати симетричну та асиметричну комутацію. Комутатори, усі порти яких працюють на однаковій швидкості, називаються симетричними. Однак багато комутаторів мають два чи більше високошвидкісних порти. Ці високошвидкісні порти (порти для каскадування) використовуються для підключення до зон з більш високими вимогами до смуги пропускання. Сфери застосування таких портів:

– підключення до інших комутаторів;

– канали зв'язку з серверами;

– підключення до інших мереж.

Для з'єднання портів, що працюють на різних швидкостях, використовується асиметрична комутація. При необхідності комутатор зберігає інформацію в пам'яті, щоб створити буфер між портами з різними швидкостями. Асиметричні комутатори широко поширені в корпоративних середовищах.

Багаторівнева комутація

Традиційно мережі складалися з окремих пристроїв 2-го і 3-го рівнів. Кожен пристрій використовував різні методи обробки і пересилання трафіку.

Рівень 2. Комутатори рівня 2 є апаратними. Вони пересилають трафік зі швидкістю, що відповідає швидкості передачі середовища, використовуючи внутрішні схеми, що фізично з'єднують кожен порт з усіма іншими портами. Процес пересилання використовує MAC-адресу і наявність MAC-адреси призначення в таблиці MAC-адрес. Комутатор 2-го рівня пересилає трафік тільки всередині одного мережевого сегменту або підмережі.

Рівень 3. Маршрутизатори є програмними пристроями і використовують мікропроцесори для маршрутизації на основі IP-адрес. Маршрутизація 3-го рівня забезпечує пересилання трафіку між різними мережами та підмережами. Коли пакет приймається на інтерфейсі маршрутизатора, він використовує програмне забезпечення для пошуку IP-адреси призначення та вибору оптимального шляху до мережі призначення. Потім маршрутизатор передає пакет на потрібний вихідний інтерфейс. Багаторівневий комутатор поєднує функції комутатора 2-го рівня і маршрутизатора 3-го рівня. Комутація рівня 3 виконується в інтегральній схемі прикладної орієнтації (ASIC – Application-Specific Integrated Circuit). Для функцій пересилання кадрів і пакетів використовується одна мікросхема ASIC. Багаторівневі комутатори часто зберігають або додають у кеш дані маршрутизації по джерелу і призначенню, отримані з першого пакету в діалозі. Наступним пакетам не доводиться виконувати пошук у таблиці маршрутизації тому, що вони знаходять дані маршрутизації в пам'яті. Таким чином, кешування збільшує продуктивність цих пристроїв.

Типи комутації

Коли з'явилася комутація, комутатори підтримували два методи пересилання кадру з одного порту на інший: пересилання з буферизацією (store and forward) і комутація без буферизації (cut-through switching). Кожен з методів має свої переваги і недоліки.

Комутація з буферизацією. При використанні цього типу комутації повний кадр зчитується і зберігається в пам'яті перед передачею пристрою призначення. Комутатор перевіряє цілісність бітів в кадрі, обчислюючи значення циклічного контролю парності (CRC – Cyclic Redundancy Check). Якщо розраховане значення CRC збігається зі значенням у полі CRC кадру, комутатор пересилає кадр через порт призначення. Комутатор не пересилає кадри, якщо значення CRC не збігаються. Значення CRC знаходиться в полі контрольної послідовності кадру (FCS – Frame Check Sequence) в кадрі Ethernet.

Хоча цей метод дозволяє запобігти передачі пошкоджених кадрів в інші сегменти, він викликає значні затримки. Тому комутація з буферизацією в основному використовується в середовищах з високою імовірністю виникнення помилок, наприклад у середовищах, що часто піддаються впливу електромагнітних імпульсів.

Наскрізна комутація. Інший основний метод комутації – наскрізна комутація. Наскрізна комутація включає два методи: швидке пересилання і комутація з виключенням

фрагментів. При використанні обох методів комутатор пересилає кадр, не чекаючи його повного прийому. Оскільки комутатор не обчислює і не перевіряє значення CRC, можлива передача пошкоджених кадрів.

Швидке пересилання – найшвидший метод комутації. Комутатор пересилає кадри з порту призначення відразу після зчитування MAC-адреси. Цей метод характеризується найменшим запізненням, але може пересилати пошкоджені фрагменти. Цей метод комутації найкраще працює в стабільній мережі з невеликою кількістю помилок.

При комутації з виключенням фрагментів комутатор зчитує перші 64 байти кадру перед початком пересилання цього кадру з порту призначення. Мінімальний допустимий кадр Ethernet складає 64 байти. Кадри меншого розміру, як правило, є результатом колізій і називаються кадрами з недопустимо малою довжиною. Перевірка перших 64 байт гарантує, що комутатор не перенаправляє колізійні фрагменти.

Комутація з буферизацією має найбільшу затримку, швидке пересилання – найменшу. Затримки комутації з виключенням фрагментів лежать посередині між цими методами. Комутація з виключенням фрагментів є оптимальним методом у середовищах, в яких виникає багато колізій. У якісно спроектованій мережі колізії не є проблемою, тому кращим методом є швидка комутація.

В даний момент більшість комутаторів Cisco для локальних мереж використовують метод з буферизацією. Це пов’язано з тим, що нові технології і низький час обробки дозволяють комутаторам зберігати й обробляти кадри майже так швидко, як при наскрізній комутації, але без помилок. Крім того, багато функцій вищого класу, такі як багаторівнева комутація, використовують метод комутації з буферизацією.

Крім того, деякі нові комутатори 2-го і 3-го рівнів можуть змінювати метод комутації відповідно до зміни стану мережі. Ці комутатори виконують швидке пересилання кадрів, щоб забезпечити мінімальну затримку. Незважаючи на те, що комутатор не виявляє помилки перед пересиланням кадру, помилки розпізнаються, і їхня кількість зберігається в пам’яті. Число виявлених помилок порівнюється з попередньо заданим граничним значенням.

Якщо кількість помилок перевищує граничне значення, значить комутатор передав недопустиме число помилкових кадрів. У цьому випадку комутатор переключається на метод з буферизацією. Якщо кількість помилок опускається нижче граничного значення, комутатор повертається в режим швидкого пересилання. Цей режим називається адаптивною наскрізною комутацією.

Безпека комутаторів

Незалежно від методу комутації потрібно підтримувати безпеку мережі. Засоби мережевої безпеки часто зосереджуються на маршрутизаторах і блокуванні трафіку ззовні. Комутатори є внутрішніми пристроями організації і розроблені для зручного доступу, тому до них застосовуються тільки найпростіші заходи безпеки, або не застосовуються взагалі.

Потрібно використовувати наступні базові заходи безпеки комутатора, щоб доступ до нього могли отримати тільки авторизовані співробітники:

– захист фізичного доступу до пристрою;
– використання безпечних паролів;
– використовувати доступ через SSH;
– відслідковувати доступ і трафік;
– відключити доступ через http;
– відключити порти, що не використовуються;
– включити захист портів;
– відключити Telnet.

Використання Cisco IOS CLI

В CLI Cisco IOS [11] є безліч функцій, які допомагають викликати необхідні команди конфігурації. Наявність таких функцій пояснює, чому фахівці з обслуговування мереж воліють використовувати Cisco IOS CLI для налаштування комутаторів. При налаштуванні пристроїв особливо корисною є функція виклику контекстної довідки. Якщо ввести в командний рядок help або ?, то з’явиться короткий опис довідкової системи.

Switch# help

Контекстно-залежна довідка дозволяє отримати пропозиції по виконанню тих чи інших команд. Якщо відома не вся команда, а тільки кілька її перших символів, потрібно їх ввести, а після відомих символів поставити знак «?». Між символами команди та знаком «?» не повинно бути пробілу.

Крім того, щоб отримати список можливих параметрів для певної команди, потрібно ввести частину цієї команди, потім пробіл, а після нього знак «?». Наприклад, якщо ввести команду configure, потім пробіл і знак «?», то буде виведений список можливих варіантів продовження цієї команди. Щоб закінчити рядок команди, потрібно вибрати один з варіантів. Після завершення командного рядка з'явиться символ <cr>. Для введення команди потрібно натиснути клавішу Enter. Якщо знаку «?» не відповідає нічого із вмісту довідки, список буде порожнім. Це означає, що введена команда не підтримується.

Іноді користувачі вводять команди з помилкою. Якщо команда введена не повністю або її не вдається розпізнати, з'явиться відповідне повідомлення CLI. Символом «%» позначається початок повідомлення про помилку. Наприклад, якщо введено команду interface без додаткових параметрів, то з'явиться повідомлення про помилку, яке вказує, що команда введена не повністю:

% Incomplete command («Команда не завершена»)

Для отримання списку доступних параметрів потрібно використовувати символ «?».

Якщо команда введена неправильно, з'явиться таке повідомлення:

% Invalid input detected («Недопустима команда»)

Іноді важко помітити помилку в неправильно введеній команді, але в CLI є індикатор помилок. У тому місці стрічки команди, де перебуває неправильний або нерозпізнаний символ, з'являється знак вставки «^». Завдяки цьому, користувач може повернутися до потрібного місця та визначити правильну команду за допомогою функції довідки. Крім цього, в Cisco IOS CLI є функція виклику раніше введених команд. Ця функція особливо зручна при введенні довгих або складних команд.

Збереження історії введення команд включається за замовчуванням і система фіксує 10 записів командних рядків у буфері. Щоб змінити кількість командних рядків, які записуються системою протягом сеансу, можна використати команду terminal history size або history size. Максимальна кількість командних рядків - 256.

Для виклику з буфера останньої введеної команди можна використати клавіші Ctrl-P або клавішу зі стрілкою "вверх". Для виклику наступних команд потрібно повторити процедуру. Щоб повернутися до новішої команди з буферу, можна використати клавіші Ctrl-N або клавішу зі стрілкою "вниз". Для виклику наступних команд потрібно повторити процедуру.

CLI розпізнає частково введені команди, знаходячи перший унікальний символ. Наприклад, можна ввести «int» замість «interface». Якщо введено скорочену назву, наприклад «int», то при натисканні клавіші Tab запис команди буде автоматично доповнено до «interface».

В більшості комп'ютерів є додаткові функції вибору та копіювання за допомогою різних функціональних клавіш. Попередній рядок команди можна скопіювати та вставити як поточну команду.

Використання команд Show

Cisco IOS CLI дозволяє користуватися командами показу для відображення інформації про конфігурацію та режим роботи пристрою.

Адміністратори мережі широко користуються командами показу для перегляду файлів конфігурації, перевірки стану інтерфейсів пристроїв та поточних процесів, а також для контролю робочого стану пристроїв. Командами show можна користуватися незалежно від способу конфігурації пристрою - CLI або SDM.

За допомогою команди show можна відобразити стан практично будь-якого процесу або функції комутатора. Найбільш відомі команди show:

show running-config

show interfaces

show arp

show ip route
show protocols
show version

Базова конфігурація

У вихідну конфігурацію пристрою Cisco IOS входить призначення імені пристрою та паролів, які служать для контролю доступу до різних функцій пристрою.

Одним з перших завдань конфігурування є присвоєння пристрою унікального імені. Це завдання вирішується в режимі глобальної конфігурації за допомогою такої команди:

Switch(config)# hostname <ім'я>

При натисканні клавіші Enter ім'я вузла за замовчуванням - Switch - змінюється на нове, привласнене вузлу, ім'я.

Наступним кроком конфігурування є призначення паролів для запобігання несанкціонованого доступу до пристрою.

Для обмеження доступу до привілейованого режиму EXEC служать команди enable password та enable secret. Це не дає можливості змінювати параметри налаштування комутатора користувачам, які не мають відповідних прав доступу.

Switch (config)# enable password <пароль>

Switch (config)# enable secret <пароль>

Різниця між цими двома командами полягає в тому, що команда enable password за замовчуванням не є зашифрованою. Якщо після команди enable password вводиться команда enable secret <пароль>, то команда enable secret має перевагу перед enable password. Не зашифрований пароль можна відновити в режимі відновлення паролю.

До інших основних налаштувань комутатора належать налаштування баннера, включення синхронного ведення журналу та відключення пошуку домена.

Банери

Банер – це текст, який бачить користувач при вході в комутатор. Налаштування відповідного банера є частиною продуманого плану забезпечення безпеки. Банер повинен містити попередження щодо несанкціонованого доступу. Ніколи не встановлюйте банер у вигляді вітання для користувача, що не має відповідних прав доступу.

Існує два типи банерів: повідомлення дня (MOTD) та інформація для входу. Два окремих банери потрібні для того, щоб можна було замінити один з них, не зачіпаючи при цьому повідомлення банера цілком.

Для налаштування банерів служать команди banner motd й banner login. Для обох типів як роздільник на початку та наприкінці повідомлення використовується символ «#». Цей символ дозволяє користувачеві задати банер, що складається з декількох рядків.

Якщо задані обидва банери, то банер входу в систему з'являється після MOTD, але перед введенням облікових даних для входу.

Синхронне ведення журналу

Програма Cisco IOS часто надсилає повідомлення, наприклад, про зміну стану інтерфейсу, що конфігурується. Іноді це відбувається під час введення команди. Таке повідомлення не впливає на виконання команди, але дезорієнтує користувача, що вводить команду. Для того, щоб під час введення команди не з'являлися повідомлення, можна ввести команду logging synchronous в режимі глобальної конфігурації.

Відключення пошуку домена

За замовчуванням при введенні імені вузла в режимі включення комутатор інтерпретує це як спробу користувача підключитися до пристрою через Telnet. Комутатор намагається розв'язати невідомі імена, введені в режимі включення, шляхом відправлення їх на сервер DNS. Це відноситься до всіх введених слів, які комутатор не може розпізнати, включаючи неправильно введені команди. Якщо цього робити не потрібно, то за допомогою команди no ip domain-lookup можна відключити цю функцію, яка працює за замовчуванням.

Існує кілька способів підключитися до пристрою та налаштувати конфігурацію. Один з них - підключення комп'ютера до консольного порту пристрою. Цей тип підключення часто використовується для налаштування початкової конфігурації пристрою.

Встановлення паролю для доступу до консолі виконується в режимі глобальної конфігурації. Зазначені нижче команди запобігають несанкціонованому доступу до користувацького режиму з порту консолі.

Switch (config)# line console 0

Switch (config)# password <пароль>

Switch (config)# login

Якщо пристрій з'єднаний з мережею, то до нього можна отримати доступ через мережеве з'єднання. Такий варіант називається підключенням через віртуальний термінал або підключенням vty. Для віртуального порту (порту vty) потрібно призначити пароль.

Switch (config)# line vty 0 4

Switch (config)# password <пароль>

Switch (config)# login

Цифри 0 4 означають 5 одночасних внутрішньосмугових підключень. Можна для кожного підключення задати свій пароль, вказавши номери конкретних ліній, наприклад, line vty 0.

Для перевірки правильності призначення паролів можна використати команду show running-config. Паролі зберігаються у файлі поточної конфігурації, у форматі незашифрованого тексту. Можна включити шифрування всіх паролів, які зберігаються в пам'яті комутатора. Це створить додаткові труднощі у випадку несанкціонованого доступу.

Команда service password encryption, введена в режимі глобальної конфігурації, забезпечує шифрування всіх паролів.

Варто пам'ятати, що при зміні поточної конфігурації необхідно скопіювати її у файл початкової конфігурації. В протилежному випадку при вимиканні пристрою всі зміни будуть втрачені. Для копіювання поточної конфігурації у файл початкової конфігурації використовується команда: copy run start.

Конфігурація комутатора

Включення комутатора

Для включення комутатора необхідно виконати три основних кроки.

Крок 1. Перевірка компонентів.

Крок 2. Підключення кабелів до комутатора.

Крок 3. Запуск комутатора.

Після запуску комутатора починається його самотестування при включенні живлення (POST). У ході POST проводиться серія перевірок функцій комутатора. Індикатори мерехтять.

POST закінчується, коли світлоіндикатор SYST починає швидко мерехтіти зеленими кольорами. Якщо в процесі POST відбувається збій, індикатор SYST стає жовтим. Якщо комутатор не може виконати POST, необхідно відправити його для ремонту. Після завершення всіх стартових процедур можна приступати до налаштування комутатора Cisco 2960.

Початкова конфігурація комутатора

Існує кілька способів налаштування і керування комутатором Cisco у локальних мережах.

– Cisco Network Assistant (Мережевий помічник Cisco)

– Device Manager (SDM) (Диспетчер пристроїв Cisco)

– Інтерфейс командного рядка Cisco IOS

– Програма керування CiscoView

– Програмні продукти керування мережею SNMP

У деяких із цих способів для підключення до комутатора використовується IP-адресація або веб-браузер, що вимагає наявності IP-адреси. На відміну від інтерфейсів комутатора, портам комутатора не присвоюють IP-адресу. Щоб скористатися засобом керування на основі IP або відкрити сеанс Telnet для роботи з комутатором Cisco, потрібно налаштувати для керування IP-адресу комутатора.

Якщо в комутатора нема IP-адреси, варто підключитися безпосередньо до порту консолі та використати для налаштування емулятор терміналу.

Налаштування комутатора Cisco Catalyst 2960 виконується на заводі-виробнику. Перед підключенням до мережі необхідно задати тільки основну інформацію про безпеку.

Команди, що служать для налаштування на комутаторі імені вузла та паролів, є тими ж командами, які використовуються для налаштування ISR. Щоб працювати з комутатором Cisco через засоби керування на основі IP або Telnet, потрібно налаштувати для керування IP-адресу.

Для того, щоб призначити комутатору адресу, ця адреса має бути призначена інтерфейсу віртуальної локальної мережі VLAN. У мережі VLAN кілька фізичних портів можуть бути об'єднані логічно. За замовчуванням існує тільки одна мережа VLAN, що заздалегідь налаштована в комутаторі - VLAN1, і вона забезпечує доступ до функцій керування.

Щоб створити IP-адресу інтерфейсу керування VLAN1, потрібно перейти в режим глобальної конфігурації [12].

Switch>enable

Switch#configure terminal

Далі, увійти в режим конфігурації інтерфейсу для VLAN1.

Switch(config)#interface vlan 1

Задати IP-адресу, маску мережі та шлюз за замовчуванням для інтерфейсу керування. IP-адреса повинна перебувати в тій же локальній мережі, що й комутатор.

Switch(config-if)#ip address 192.168.1.2 255.255.255.0

Switch(config-if)#exit

Switch(config)#ip default-gateway 192.168.1.1

Switch(config)#end

Після цього зберегти конфігурацію за допомогою команди copy running-configuration startup-configuration.

Підключення комутатора до LAN

Підключення комутатора до мережі

Для підключення комутатора до маршрутизатора використовується прямий кабель. Світлоіндикатори на комутаторі та маршрутизаторі свідчать про успішність підключення.

Після з'єднання комутатора та маршрутизататора потрібно перевірити, чи можуть ці два пристрої обмінюватися повідомленнями.

Насамперед, потрібно перевірити налаштування IP-адреси. За допомогою команди show running-configuration потрібно переконатися в тому, що IP-адреса інтерфейсу управління комутатора мережі VLAN1 та IP-адреса безпосередньо під'єднаного інтерфейсу комутатора перебувають в одній локальній мережі.

Потім потрібно перевірити з'єднання за допомогою команди ping. Для цього з комутатора відправляється команда ping на IP-адресу безпосередньо під'єднаного інтерфейсу комутатора. Після цього потрібно повторити цей процес із комутатора, відправивши команду ping на IP-адресу інтерфейсу керування, призначену комутатору мережі VLAN 1.

Якщо ехо-запит виконати не вдалося, потрібно перевірити з'єднання та конфігурацію ще раз і переконатися в тому, що всі кабелі підключені правильно та надійно.

Коли між комутатором і маршрутизатором встановлений нормальний обмін даними, можна підключати до комутатора, за допомогою прямих кабелів, окремі ПК. Ці кабелі можуть прямо підключатися до ПК або вони можуть бути частиною структурованої кабельної системи, що йде до настінних розеток.

Порти комутатора можуть бути місцями несанкціонованого входу в мережу. Для запобігання цього комутатори підтримують функцію, що називається захистом портів. Ця функція обмежує кількість допустимих MAC-адрес на один порт. Порт не буде відправляти пакети з вихідними MAC-адресами, якщо вони не входять у групу заданих адрес. Існує три способи налаштування безпеки порту:

Статичний

MAC-адреси призначаються вручну, використовуючи команду налаштування інтерфейсу: switchport port-security mac-address <mac-адреса>

Статичні MAC-адреси зберігаються в таблиці адрес і додаються в поточну конфігурацію.

Динамічний

Динамічно отримані відомості про MAC-адреси зберігаються в таблиці адрес. Кількість отриманих адрес можна контролювати. За замовчуванням на один порт може бути отримано не більше однієї MAC-адреси. Отримані адреси видаляються з таблиці при вимиканні порту або при перезапуску комутатора.

Зв'язаний

Аналогічний динамічному, за винятком того, що адреси зберігаються ще й у поточну конфігурацію.

За замовчуванням безпека порту відключена. Якщо включити функцію безпеки порту, це приведе до несправності при відключенні порту. Наприклад, якщо включити функцію безпеки порту в динамічному режимі і на один порт може бути отримано не більше однієї MAC-адреси, то перша отримана адреса стає безпечною. Якщо інша робоча станція спробує одержати доступ до порту з іншою MAC-адресою, то відбудеться порушення безпеки і відповідний порт буде заблоковано. При цьому може надсилатись повідомлення про блокування порту. Порушення безпеки відбувається в кожній із зазначених нижче ситуацій:

– У таблицю адрес введена максимально можлива кількість безпечних MAC-адрес, і пристрій, адреси якого немає в таблиці адрес, намагається отримати доступ до інтерфейсу.

– Адресу, отриману або налаштовану на одному безпечному інтерфейсі, можна бачити на іншому безпечному інтерфейсі в тій же мережі VLAN.

Щоб можна було активувати функцію безпеки порту, необхідно перевести порт у режим доступу за допомогою команди switchport mode access.

Для перевірки налаштувань безпеки порту для комутатора або заданого інтерфейсу, використовується команда show port-security interface interface-id. На екрані з'являться такі вихідні дані:

– максимально допустима кількість безпечних MAC-адрес для кожного інтерфейсу;

– кількість безпечних MAC-адрес даного інтерфейсу;

– кількість порушень безпеки, що відбулися;

– режим порушення безпеки.

Крім цього, при введенні команди show port-security address відображаються безпечні MAC-адреси для всіх портів, а при введенні команди show port-security відображаються налаштування безпеки порту для комутатора.

Якщо включено функцію безпеки порту для статичного або зв'язаного режиму, то можна використати команду show running-config для перегляду MAC-адрес, пов'язаних з конкретним портом. Існує три способи видалення отриманої MAC-адреси, що була збережена у поточну конфігурацію:

– Використати команду clear port-security sticky interface <№ порту> access для видалення всіх отриманих адрес. Потім варто виключити порт, ввівши команду shutdown. Нарешті, потрібно знову включити порт за допомогою команди no shutdown.

– Для відключення режиму безпеки порту варто ввести з інтерфейсу команду no switchport port-security. Після відключення варто знову включити режим безпеки порту

– Перезавантажити комутатор.

Комутатор буде перезавантажуватися тільки в тому випадку, якщо поточна конфігурація не збережена у файл початкової конфігурації. Якщо ж поточна конфігурація була збережена у файл початкової конфігурації, то це виключає для комутатора можливість повторного отримання адрес при перезавантаженні системи.

Однак отримані MAC-адреси будуть завжди пов'язані з конкретним портом доти, поки не буде зроблене очищення порту за допомогою команди clear port-security, або не буде відключений режим безпеки порту. Якщо це буде зроблено, потрібно перезаписати поточну конфігурацію у файл початкової конфігурації, щоб комутатор після перезавантаження не почав використовувати вихідні зв'язані MAC-адреси.

Якщо на комутаторі є порти, що не використовуються, рекомендується відключити їх з міркувань безпеки для обмеження можливості несанкціонованого доступу. Відключення

портів на комутаторі виконується просто. Переходячи до кожного порту, що не використовується, потрібно ввести команду shutdown. Якщо потім треба буде активувати цей порт, використовується команда no shutdown для відповідного інтерфейсу.

Крім включення режиму безпеки порту та відключення портів, які не використовуються, існують інші налаштування безпеки комутатора, які дозволяють встановлювати паролі на порти vty, застосовувати банери входу в систему та зашифровувати паролі за допомогою команди service password-encryption. Для зазначених конфігурацій використовуються ті ж команди інтерфейсу командного рядка Cisco IOS, які застосовуються для налаштування комутатора.

Мінімальний розмір кадрів Ethernet складає 64 байти, максимальний – 1518 байтів, однак розмір тегованого кадру Ethernet може досягати 1522 байти.

Кадри включають такі поля:

– MAC-адреси джерела і призначення;

– довжина кадру;

– корисні дані;

– контрольна послідовність кадру (FCS).

Поле FCS забезпечує виявлення помилок і гарантує цілісність всіх бітів в кадрі.

Мітка збільшує мінімальний розмір кадру Ethernet з 64 до 68 байт. Максимальний розмір збільшується з 1518 до 1522 байт. Комутатор перерозраховує FCS, тому що кількість бітів в кадрі збільшується.

Якщо порт, сумісний з 802.1q, підключений до іншого порту, також сумісного з 802.1q, дані маркування VLAN передаються між ними.

Якщо підключений порт несумісний з 802.1q, мітка VLAN буде видалена перш, ніж кадр досягне середовища передачі.

Якщо пристрій, або порт доступу без підтримки 802.1q отримує кадр 802.1q, то дані мітки ігноруються, а пакет комутується на рівні 2 як стандартний кадр Ethernet. Це дозволяє розміщувати на транковому маршруті 802.1q проміжні пристрої рівня 2, наприклад інші комутатори. Щоб обробити кадр із міткою 802.1q, пристрій повинен дозволяти MTU зі значенням 1522 або вище.

Призначення протоколу VTP

Автоматизація керування VLAN

Зі збільшенням розміру і складності мережі централізоване керування структурою VLAN стає критично важливим. Протокол VTP (VLAN Trunking Protocol) – це протокол обміну повідомленнями 2-го рівня, що надає метод керування базою даних VLAN з центрального сервера в мережевому сегменті. Маршрутизатори не пересилають оновлення VTP.

Без автоматизованого методу керування корпоративною мережею із сотнями VLAN потрібно було б вручну налаштувати кожну VLAN на кожному комутаторі. Будь-яка зміна структури VLAN потребувала б додаткового ручного налаштування. Один невірно набраний номер може стати причиною нестабільності з’єднань по всій мережі.

Щоб вирішити цю проблему, корпорація Cisco створила протокол VTP, що автоматизує багато задач конфігурації VLAN. VTP гарантує погоджене обслуговування конфігурації VLAN по всій мережі і зменшує необхідність у керуванні та моніторингу VLAN.

VTP являє собою протокол обміну повідомленнями між клієнтом і сервером, що дозволяє додавати, видаляти та перейменовувати VLAN в одному домені VTP. Усі комутатори під загальним керуванням є частиною домена. У кожного домена є унікальне ім’я. Комутатори VTP обмінюються повідомленнями VTP тільки з іншими комутаторами в домені.

Компоненти протоколу VTP

Ключовими компонентами протоколу VTP є:

VTP домен – складається з одного або декількох взаємопов’язаних комутаторів. Всі комутатори в домені діляться інформацією про деталі налаштування VLAN за допомогою

VTP оголошень. Маршрутизатор або комутатор третього рівня визначає межі кожного домену.

VTP оголошення – VTP використовує оголошення для поширення та синхронізації конфігурації VLAN по всій мережі.

Режими VTP – комутатор може бути налаштований на роботу в одному з трьох режимів: сервер, клієнт, або прозорий.

VTP сервер – VTP сервер поширює інформацію про VLAN іншим комуторам, що підтримують VTP, в тому ж VTP домені. VTP сервери зберігають інформацію про VLAN для всього домену в енергонезалежній пам'яті. На сервері VLAN можуть бути створені, видалені або перейменовані.

VTP клієнт – VTP клієнти працюють так само, як VTP сервери, але на них не можна створювати, змінювати, або видаляти VLAN. VTP клієнт зберігає інформацію про VLAN для всього домену лише в той час коли комутатор включений. Перезавантаження комутатора спричиняє видалення інформації про VLAN. Режим VTP клієнта на комутаторі необхідно налаштувати.

VTP прозорий – прозорий комутатор пересилає VTP повідомлення до VTP клієнтів та серверів. Прозорі комутатори не приймають участь в роботі VTP. Мережі VLAN, які створюються, перейменовуються або видаляються на прозорих комутаторах є локальними і відносяться лише до цього комутатора.

VTP Pruning(скорочення) – збільшує доступну смугу пропускання мережі шляхом обмеження поширення інформації про VLAN комутаторові у якого немає активних портів у відповідному VLAN, а також блокує широкомовний трафік на комутатор, якщо в ньому немає активних портів у тому ж VLAN з якого відправляється широкомовний трафік.

Структура VTP кадру

VTP оголошення (або повідомлення) поширюють ім'я домену VTP та зміни в конфігурації VLAN до комутаторів, які підтримують VTP.

VTP кадр складається з заголовка та повідомлення. VTP інформація вставляється в поле даних кадру Ethernet. Після цього Ethernet кадр інкапсулюється в транковий кадр 802.1q (або ISL кадр). Кожен комутатор в домені періодично надсилає повідомлення на кожен транковий на спеціальну групову адресу. Ці оголошення приймаються сусідніми комутаторами, які оновлюють свої VTP та VLAN конфігурації в міру необхідності.

Інкапсуляція VTP кадру в 802.1q кадр не є статичною. Зміст VTP повідомлення визначається наявними полями. Комутатори з підтримкою VTP шукають визначені поля та значення в кадрі 802.1q. В інкапсульованому у 802.1.q кадр VTP кадрі присутні наступні ключові поля:

Destination MAC address – MAC-адреса призначення, встановлена в значення 01-00-0C-CC-CC-CC, яке є зарезервованим значенням групової адреси для всіх VTP повідомленнь.

LLC (Logical link control) field – поле містить сервісну точку доступу призначення (destination service access point, DSAP) та сервісну точку доступу відправника (source service access point, SSAP) встановлені в значення AA.

SNAP (Subnetwork Access Protocol) field – поле з встановленим OUI в значення AAAA і встановленим типом 2003.

VTP header field – поле VTP заголовку, вміст змінюється в залежності від типу VTP повідомлення, але завжди містить такі поля VTP поля:

– Domain name – визначає адміністративний домен для комутатора;

– Domain name length – довжина доменного імені;

– Version – в-я, яку підтримує комутатор, встановлюється VTP 1, VTP 2, або VTP 3;

– Configuration revision number –поточний номер версії конфігурації на комутаторі.

VTP message field – значення залежить від типу повідомлення.

VTP Message Contents – VTP кадри містять наступну глобальну інформацію про домен фіксованої довжини:

– VTP domain name;

– ідентифікатор комутатора, що надіслав повідомлення та час його надсилання;

– MD5 значення VLAN конфігурації, включаючи максимальний блок передачі (maximum transmission unit, MTU) для кожноїVLAN;

– Формат кадру: ISL або 802.1q.

VTP кадри містять наступну інформацію для кожної налаштованої VLAN:

– VLAN IDs (IEEE 802.1q);

– VLAN name;

– VLAN type;

– VLAN state;

– Додаткова інформація про налаштування VLAN.

Режими роботи VTP

Існує дві різні версії VTP: 1 і 2. Версія 1 – версія за замовчуванням і вона несумісна з версією 2. На всіх комутаторах необхідно налаштувати однакову версію протоколу.

VTP використовує три режими: сервер, клієнт і прозорий пристрій. За замовчуванням усі комутатори є серверами. Рекомендується налаштувати хоча б два комутатори в мережі як сервери, щоб забезпечити резервування. Ці режими відрізняються тим, як вони використовуються для управління та надсилання повідомлень про VTPдомени та VLAN.

Режим сервер

В режимі сервера можна створювати, змінювати та видаляти VLAN для всього домену VTP. Режим VTP сервера використовується за замовчуванням на комутаторах Cisco. VTP сервери надсилають свої конфігурації VLAN на інші комутатори в тому ж домені VTP та синхронізують конфігурації VLAN з іншими комутаторами по магістральних каналах. VTP сервери відстежують оновлення через номер версії конфігурації. Інші комутатори в тому ж домені VTP порівнюють номер версії своєї конфігурації з номером ревізії, який було отримано з VTP сервера, щоб визначити чи вони повинні синхронізувати свою базу даних VLAN.

Режим клієнт

Якщо комутатор знаходиться в режимі клієнта, на ньому не можна створити, змінити або видалити VLAN. Крім того, інформацію про VLAN конфігурації VTP клієнт отримує від VTP сервера і вона зберігається в базі даних VLAN, а не в NVRAM. Завдяки цьому, VTP клієнти вимагають менше пам’яті, ніж VTP сервери. Після включення чи перезавантаження VTP клієнт надсилає запит на VTP сервер для оновлення інформації про конфігурацію VLAN. Комутатори налаштовані як клієнти зазвичай зустрічаються у великих мережах.

Прозорий режим

Комутатори налаштовані на прозорий режим роботи VTP пересилають VTP повідомлення, які вони отримують на магістральні порти на інші комутатори в мережі. Також вони не надсилають свою конфігурацію VLAN і не синхронізують конфігурацію VLAN з будь-яким іншим комутатором.

У прозорому режимі VLAN конфігурації зберігаються венергонезалежній пам’яті, тому конфігурація доступна після перезавантаження. Також це означає, що після перезавантаженнія комутатор не повернеться до режим VTP сервера pf замовчуванням, а залишається в прозорому режим VTP.

При використанні VTP кожен сервер посилає повідомлення через свої транкові порти. Повідомлення включають домен керування, номер версії конфігурації, відомі VLAN і параметри кожної VLAN. Кадри оголошень відправляються за адресою багатоадресної розсилки, тому їх отримують всі сусідні вузли.

Кожен комутатор VTP зберігає базу даних VLAN, що включає номер версії конфігурації, в енергонезалежній пам’яті (NVRAM). Якщо VTP отримує оновлення з більш високим номером версії, ніж номер у базі даних, комутатор додає нові дані у свою базу даних VLAN.

Номер зміни конфігурації VTP починається з нуля. При внесенні змін номер версії конфігурації збільшується на одиницю. Номер версії продовжує збільшуватися, поки не досягає 2 147 483 648. При досягненні цього значення лічильник скидається на нуль. Крім того, номер версії скидається при перезавантаженні комутатора.

Проблема, пов’язана з номером версії, може виникнути, якщо додати у мережу комутатор з більш високим номером версії. Оскільки за замовчуванням комутатор знаходиться в серверному режимі, нові, але невірні дані можуть перезаписати коректні дані VLAN на всіх інших комутаторах.

Один зі способів забезпечення захисту від цієї критичної ситуації полягає в заданні паролів VTP для перевірки комутаторів. Крім того, при додаванні комутатора в мережу, у якій уже є комутатор у серверному режимі, переконайтеся, що новий комутатор налаштований у прозорому або клієнтському режимі.

Повідомлення та налаштування VTP

Існує три типи повідомлень VTP: зведені оголошення, скорочені оголошення і запити оголошень.

Зведені оголошення

Комутатори Catalyst розсилають зведені оголошення кожні 5 хвилин, а також при зміні бази даних VLAN. Зведені оголошення містять поточне ім’я домена VTP і номер версії конфігурації.

При додаванні, видаленні або зміні VLAN сервер збільшує номер версії конфігурації і відправляє зведене оголошення.

При отриманні пакета зведеного оголошення комутатор порівнює ім’я домена VTP зі своїм ім’ям домену VTP. Якщо імена доменів збігаються, комутатор порівнює номер версії конфігурації зі своїм номером. Якщо отриманий номер менший, комутатор ігнорує пакет. Якщо номер версії вищий, відправляється запит оголошення.

Скорочені оголошення

Скорочене оголошення відправляється після зведеного оголошення. Скорочене оголошення містить список даних VLAN.

Скорочене оголошення містить нові дані VLAN, засновані на зведеному оголошенні. Якщо в мережі кілька VLAN, буде потрібно кілька скорочених оголошень. Причиною оновлення скороченого повідомлення може бути:

– створення або видалення VLAN;

– призупинення або активація VLAN;

– зміна імені VLAN;

– зміна MTU VLAN

Для повного оновлення інформації про VLAN потрібно використати декілька скорочених повідомлень.

Оголошення-запити.

VTP-клієнти використовують оголошення-запити, щоб запитати інформацію про VLAN. Оголошення-запити необхідні, якщо комутатор скинутий або змінене ім’я домена VTP. Комутатор отримує зведене оголошення VTP з більш високим номером версії конфігурації, ніж його власний.

Коли оголошення-запит надходить VTP серверу в тому ж VTP домені, VTP сервер відповідає, надсилаючи зведене оголошення, а потім скорочене оголошення.

Оголошення-запити направляються в таких випадках:

– після зміни імені VTP домену;

– при отримані комутатором зведеного оголошення з більш високим номером версії конфігурації ніж його власний;

– скорочене повідомлення втрачене з якихось причин;

– комутатор ресетувався.

За замовчуванням комутатори є VTP серверами. Якщо комутатор у серверному режимі відправляє відновлення з номером версії, що перевищує поточний номер версії, усі комутатори змінять свої бази даних відповідно до отриманого повідомлення.

При додаванні нового комутатора в існуючий домен VTP потрібно виконати наступні дії:

Дія 1. Налаштувати протокол VTP в автономному режимі (версію 1)

Дія 2. Перевірити конфігурацію VTP.

Дія 3. Перезавантажити комутатор.

При налаштуванні VTP можуть виникати певні проблеми.

Несумісність версій VTP – версії 1 та версії 2 несумісні одна з одною, тому старі комутатори, які підтримують тільки VTP версії 1 не можуть працювати у VTP домені поряд з комутаторами з версією 2. Якщо в мережі є комутатори, які підтримують тільки версію 1 потрібно вручну налаштувати комутатори з версія 2 для роботи в режимі версії 1

Неспівпадіння VTP паролів – при використанні VTP паролю для контролю участі в домені VTP, пароль повинен бути встановлений правильно на всіх комутаторах в домені VTP. На відміну від інших параметрів, які встановлюються автоматично піля отримання VTP повідомлення, комутатор не виконує автоматичне налаштування параметрів паролів.

Невірне ім’я VTP домену – ім’я домену VTP є ключовим параметром, який встановлюється на комутаторі. Неправильно налаштований VTP домен впливає на синхронізацію VLAN між комутаторами. Якщо комутатор отримує неправильне VTP оголошення, він його. Якщо відкинуте повідомлення містить інформацію про конфігурацію, комутатор не синхронізує свою базу данихVLAN, як очікувалося.

Щоб уникнути неправильного налаштування VTP домен, потрібно встановити ім’я VTP домену на комутаторі, який є VTP сервером. Всі інші комутатори в тому ж домені VTP будуть приймати та автоматично налаштувати їх VTP доменне ім’я, коли отримають перше зведене VTP оголошення. Всі інші комутатори можна встановити в режим VTP клієнтів. При цьому втрачається можливість для створення, видалення та управління VLAN в мережі. Оскільки комутатори в режимі VTP клієнта не зберігають інформацію про VLAN в енергонезалежній пам’яті, вони повинні оновити інформацію про VLAN після перезавантаження.

Щоб не втратити всі VLAN налаштування в VTP домені внаслідок випадкового переналаштування VTP сервера в режим VTP клієнта, можна налаштувати ще один комутатор в тому ж домені в режим сервера VTP.

Запобігання утворенню петель комутації

Резервування в мережі

Сучасні підприємства усе більше покладаються на мережі, іноді від мереж залежить саме їх існування. Мережа – життєво важлива комунікація для багатьох організацій. Простій мережі перетворюється у катастрофічні втрати для бізнесу і довіри замовників.

Відмова одного мережевого каналу, одного пристрою чи навіть важливого порта комутатора може стати причиною простою мережі. Щоб виключити критичні точки відмови і забезпечити високу надійність, у мережеву архітектуру необхідно ввести резервування. Резервування реалізується шляхом встановлення дубльованого обладнання та мережевих пристроїв на важливих ділянках.

Іноді повне резервування всіх каналів і пристроїв стає невиправдано дорогим. Мережеві інженери часто змушені шукати компроміс між витратами на резервування і вимогами до доступності мережі.

Резервування означає наявність двох різних шляхів до одного місця призначення. Якщо один шлях заблокований, другий залишається доступним.

Резервування комутаторів реалізується шляхом створення декількох каналів між ними. Резервні канали в мережі знижують перевантаження і підтримують високу доступність і розподіл навантаження.

Вплив режимів передачі трафіку

Однак з’єднання комутаторів може стати причиною проблем. Зокрема, широкомовна природа трафіку Ethernet приводить до утворення петель комутації. Широкомовні кадри циклічно поширюються у всіх напрямках, викликаючи «шторм» широкомовних пакетів. Широкомовні шторми займають усю доступну смугу пропускання, блокують створення нових мережевих підключень і розривають існуючі підключення.

Широкомовні шторми – не єдина проблема, що обумовлена резервними каналами в комутованій мережі. Кадри одноадресного пересилання можуть також викликати такі проблеми, як множинна передача кадрів і нестабільність бази даних MAC-адрес.

Множинна передача кадрів

Якщо вузол посилає одноадресний кадр вузлу призначення і MAC-адреса не представлена в жодній з таблиць MAC-адрес підключених комутаторів, усі комутатори виконують лавинне розсилання цього кадру з усіх портів. У мережі з петлями кадр може повернутися до вихідного комутатора. Цей процес повторюється, що приводить до утворення декількох копій кадру в мережі. В результаті вузол призначення отримує кілька копій кадру. Це стає причиною трьох проблем: неефективна витрата смуги пропускання, неефективна витрата циклів ЦП і дублювання трафіку.

Нестабільність бази даних MAC-адрес

Комутатори в резервованій мережі можуть отримувати невірні дані про місцезнаходження вузла через наявність петель комутаціїї. Якщо в мережі присутня петля, один комутатор може зв'язати MAC-адресу призначення з двома портами в своїй таблиці MAC-адрес. Це приведе до плутанини і неоптимального пересилання кадрів та збільшення завантаження каналів передачі даних і навантаження на комутатор.

Протокол STP забезпечує механізм відключення резервних каналів в комутованій мережі. STP дозволяє використовувати резервування, необхідне для надійної експлуатації, без створення петель комутації. STP ґрунтується на відкритих стандартах і використовується для створення логічної топології без петель комутації.

Протокол STP відносно самодостатній і вимагає мінімального налаштування. При першому включенні комутатори з підтримкою STP перевіряють мережу на наявність петель. Комутатори при виявленні петлі, блокують деякі з підключених портів, залишаючи інші порти активними для пересилання кадрів.

STP задає дерево, що охоплює всі комутатори в топології "розширена зірка". Комутатори постійно перевіряють мережу, щоб гарантувати відсутність петель і ефективну роботу всіх портів.

Щоб запобігти утворенню петель, протокол STP:

– переводить частину інтерфейсів в резервний або заблокований режим;

– залишає інші інтерфейси в режимі пересилки;

– переналаштовує мережу, активуючи відповідний резервний шлях, якщо шлях пересилки стає недоступним.

У термінології STP термін "комутатор" часто замінюється терміном "міст". Наприклад, кореневий міст – це основний міст або центральна вузол в топології STP. Кореневий міст взаємодіє з іншими комутаторами за допомогою блоків даних протоколу моста (bridge protocol data unit, BPDU). BPDU – це кадри, що розсилаються іншим комутаторам кожні 2 секунди. BPDU містять наступні відомості:

– ідентифікатор комутатора-джерела;

– ідентифікатор порту-джерела;

– сукупна вартість маршруту до кореневого моста;

– значення таймерів старіння;

– значення таймера "вітання".

При включенні комутатора кожен порт проходить через послідовність з 4 режимів: блокування, прослуховування, навчання і пересилання. П'ятий режим, "відключений", вказує на те, що адміністратор відключив порт комутатора.

Порт послідовно проходить через ці режими, при цьому колір світлодіодних індикаторів змінюється від мерехтливого жовтогарячого до немерехтливого зеленого. Проходження через режими STP може зайняти до 50 секунд, після чого комутатор буде готовий до пересилання кадрів.

При включенні комутатор переходить у режим блокування, щоб запобігти негайному утворенню петель. Потім він переходить у режим прослуховування, в якому приймає BPDU від сусідніх комутаторів. Після обробки цієї інформації комутатор визначає, які порти можуть пересилати кадри, не формуючи петлі. Якщо порт може пересилати кадри, він переходить у режим навчання, а потім у режим пересилання.

Алгоритм STP

Протокол STP використовує алгоритм сполучного дерева (Spanning Tree Algorithm, STA), щоб визначити, які порти комутатора в мережі мають бути заблоковані для

запобігання виникнення петель комтації. STA визначає один комутатор в якості кореневого мосту та використовує його в якості точки відліку для всіх розрахунку всіх шляхів.

Усі комутатори приймають участь в обміні кадрами BPDU щоб визначити, який комутатор має найнижчий bridgeID (BID) в мережі. Комутатор з найменшим значенням bridgeID автоматично стає кореневим мостом для розрахунків алгоритму STA.

Кожен BPDU містить BID, який ідентифікує комутатор, що надіслав BPDU. BID містить значення пріоритету, MAC-адресу комутатора-відправника та додаткові розширені ID системи. Найнижче значення BID визначається комбінацією цих трьох параметрів.

Після визначення кореневого мосту, STA розраховує найкоротший шлях до кореневого мосту. Кожен комутатор використовує STA щоб визначити, які порти заблокувати. Протягом часу визначення найкращих шляхів до кореневого мосту для всіх напрямків у широкомовному домені, весь трафік не має можливості передаватись по мережі.

Алгоритм STA визначає вартість шляху та вартість порту при визначенні шляху, який потрібно залишити розблокованим. Вартість шляху розраховується за вартістю порту, яка, в свою чергу, пов’язана зі швидкістю порту, для кожного порту комутатора для заданого шляху. Сума значень вартості портів визначає загальну вартість шляху до кореневого мосту. Якщо є більше ніж один шлях, STA вибирає шлях з найменшою вартістю шляху.

Коли STA визначив, які шляхи повинні залишатися доступними, він налаштовує різні ролі портам комутатора. Ролі портів описують зв’язок з кореневим мостом та можливість пересилання трафіку.

Всі комутатори в широкомовному домені беруть участь у виборчому процесі. Після включення комутатор надсилає BPDU кадри, що містять BID комутатора та rootID кожні 2 секунди. За замовчуванням, rootID відповідає BID для усіх комутаторів в мережі. RootID ідентифікує кореневий міст в мережі. Спочатку кожен комутатор ідентифікує себе як кореневий міст.

У кожній мережі працює тільки один кореневий міст, що вибирається на підставі ідентифікатора моста (BID, Bridge ID). BID дорівнює сумі значення пріоритету моста та його MAC-адреси.

Значення пріоритету моста за замовчуванням дорівнює 32 768. Якщо MAC-адреса комутатора AA-11-BB-22-CC-33, BID буде дорівнювати 32768:AA-11-BB-22-CC-33.

Міст із найменшим значенням BID стає кореневим. Оскільки комутатори, як правило, використовують однакове значення пріоритету за замовчуванням, комутатор з найменшою MAC-адресою стає кореневим мостом.

При включенні комутатор припускає, що є кореневим мостом, і розсилає кадри BPDU зі своїм ідентифікатором BID. Наприклад, якщо комутатор S2 повідомляє, що кореневий ідентифікатор менший, ніж ідентифікатор S1, S1 припиняє оголошення свого ідентифікатора моста і приймає кореневий ідентифікатор S2. S2 стає кореневим мостом.

Типи та стани портів в STP

STP використовує три типи портів: кореневі порти, призначені порти і заблоковані порти.

Кореневий порт

Порт із маршрутом оптимальної вартості до кореневого моста призначається кореневим. Комутатори обчислюють шлях з найменшою вартістю, використовуючи вартість смуги пропускання кожного каналу на шляху до кореневого моста.

Призначений порт

Призначений порт пересилає трафік до кореневого моста, але не підключений до шляху з найменшою вартістю.

Заблокований порт

Заблокований порт не пересилає трафік.

Перед налаштуванням STP мережевий адміністратор планує та оцінює мережу, щоб вибрати комутатор, який буде оптимальним кореневим мостом STP. Якщо кореневий міст буде обраний за мінімальною MAC-адресою, пересилання може бути неоптимальне.

В ролі кореневого мосту найкраще буде працювати комутатор, розташований у центрі мережі. Блокування порту, розташованого на периферії мережі, приведе до того, що трафік

буде передаватися до місця призначення по довшому маршруту, ніж при використанні комутатора в центрі мережі.

Щоб задати кореневий міст, для BID обраного комутатора налаштовується мінімальний пріоритет. Для налаштування пріоритету моста використовується команда bridge priority. Значення пріоритету може знаходитися в діапазоні від 0 до 65 535, але крок між значеннями складає 4 096. Значення за замовчуванням - 32 768.

Найкращий шлях до кореневого моста.

Після призначення кореневого мосту алгоритм STA починає процес визначення найкращого шляху до кореневого мосту з усіх напрямків в широкомовному домені. Оптимальний шлях визначається шляхом підсумовування вартості портів на шляху від призначення до кореневого мосту.

Вартість порту за замовчуванням визначається швидкістю, з якою працює порт. Так, наприклад, 10-Гбіт/с Ethernet порт має вартість 2, 1 Гбіт/с порт має вартість, 100 Мбіт/с порт має вартість 19 і 10 Мбіт/с Ethernet порт має вартість порту 100.

З появою нових, більш швидких технологій Ethernet, значення вартості шляху може змінитися.

Хоча порти комутатора мають вартість порту за замовчуванням, вартість порту можна змінити. Можливість налаштування вартості портів дозволяє адміністратору гнучко керувати шляхами сполучного дерева до кореневого мосту.

Для налаштування вартості порту потрібно ввести значення вартості за допомогою команди spanning-tree cost в режимі конфігурації інтерфейсу. Діапазон значень може бути від 1 до 200 000 000. Для повернення до стандартного значення використовується команда no spanning-tree cost.

Стани портів в STP.

STP визначає логічний маршрут без утворення петлі в межах широкомовного домену. Дерево будується на основі інформації, отриманої шляхом обміну BPDU кадрів між комутаторами. Кожен порт комутатора переходить через п’ять можливих станів порту і три BPDU таймери.

Побудова STP дерева розпочинається відразу після завершення завантаження. Якщо порт комутатора перейде від блокування безпосередньо в стан пересилання, порт може тимчасово створити петлю, якщо комутатор не володіє всією інформацією про топологію. З цієї причини в STP передбачено п’ять станів портів.

Blocking(блокування) – порт не є призначеним портом і не бере участі в передаванні кадрів. Порт отримує кадр BPDU, щоб визначити місце розташування root ID кореневого моста і який стан кожного порту комутатора повинен бути після завершення побудови активної STP топології.

Listening (прослуховування) – протокол STP встановив, що порт може приймати участь в пересиланні кадрів відповідно до попередньо отриманого кадру BPDU. Порт комутатора може не тільки отримувати кадри BPDU, але також і передавати свої власні кадри BPDU та інформувати сусідні комутатори, що порт комутатора готується до участі в активній топології.

Learning (навчання) – порт готується приймати участь в пересиланні кадрів і починається заповнення таблиці MAC-адрес.

Forwarding (пересилання) – порт вважається частиною активної топології і пересилає фрейми, а також відправляє і отримує кадри BPDU.

Disabled (відключений) – порт не приймає участі в Spanning Tree і не пересилає фрейми. Відключений стан встановлюється, коли порт комутатора відключений адміністративно.

BPDU таймери

Час, протягом якого порт залишається в різних станах, визначається BPDU таймерами. Тільки комутатор, який є кореневим мостом може відправляти інформацію по дереву для налаштування таймерів. Продуктивність STP і зміни стану визначають такі таймери:

– Hello time

– Forward delay

– Maximum age

Коли STP дозволений, кожен порт комутатора проходить через заблокований стан, проміжні стани прослуховування та навчання при включенні живлення. Порти потім стабілізуються в стані пересилання або блокування. Під час зміни топології, порт тимчасово реалізовує прослуховування і навчання на певний період, так званий інтервал затримки пересилання.

Ці значення інтервалів забезпечують адекватний час для збіжності в мережі з діаметром сім комтаторів. Це кількість комутаторів, які повинен пройти кадр з двох дальніх точок широкомовного домену. Діаметр на сім комутаторів – це найбільший дозволений діаметр, який забезпечує допустимий час збіжності протоколу STP. Конвергенція по відношенню сполучного дерева є часом, що витрачається на перерахунок сполучного дерева, якщо виникають проблеми з комутатором або лінією зв'язку.

Після визначення кореневого моста, а також кореневих, призначених та заблокованих портів, STP розсилає кадри BPDU по мережі із 2-секундним інтервалом. STP продовжує відслідковувати ці BPDU, щоб переконатися у відсутності каналів, які відмовили, і нових петель.

Якщо відбувається відмова каналу, STP перерозраховується шляхом:

– переведення деяких портів із заблокованого режиму в режим пересилання;

– переведення деяких портів з режиму пересилання в режим блокування;

– формування нового дерева STP для запобігання утворення петель у мережі.

Час очікування деяких прикладних програм може бути меншим періоду перерахунку, що може привести до зниження продуктивності. Частий перерахунок STP негативно впливає на час роботи систем.

Високопродуктивний корпоративний сервер підключається до порту комутатора. Якщо для цього порту виконується перерахунок через STP, сервер буде недоступний протягом хвилини. Важко уявити, яка кількість транзакцій може бути загублена за цей час.

У стабільній мережі перерахунки STP відбуваються рідко. Якщо мережа не стабільна, необхідно перевірити стабільність комутаторів та зміни їх конфігурацій. Одна з найпоширеніших причин перерахунків STP – несправне джерело живлення чи кабель живлення комутатора. Несправність джерела живлення викликає несподіване перезавантаження пристрою.

Ряд вдосконалень STP зводить до мінімуму час простоїв, викликаних перерахунком STP. До них належать режими роботи PortFast, UplinkFast і BackboneFast.

PortFast

STP PortFast негайно переводить порт доступу в режим пересилання, минаючи режими прослуховування і навчання. Застосування PortFast на портах доступу, підключених до однієї робочої станції чи сервера, дозволить їм негайно підключатися до мережі, не очікуючи конвергенції STP.

UplinkFast

STP UplinkFast прискорює вибір нового кореневого порту при відмові комутатора чи каналу, а також при перерахунку STP. Кореневий порт негайно переходить у режим пересилання, оминаючи режими прослуховування і навчання.

Протокол RSTP (Rapid Spanning Tree Protocol)

Коли інститут IEEE розробив оригінальний протокол STP (Spanning Tree Protocol) 802.1D, період відновлення розміром 1-2 хвилини був допустимим. Сьогодні комутація рівня 3 та удосконалені протоколи маршрутизації забезпечують більш швидкі альтернативні шляхи до місця призначення. Через потребу в передачі трафіку, чуттєвого до затримок, наприклад голосу і відео, мережі повинні підтримувати швидку конвергенцію, щоб задовольняти вимоги нових технологій.

Протокол Rapid Spanning Tree Protocol (RSTP), визначений у стандарті IEEE 802.1w, значно прискорює перерахунок STP. На відміну від функцій PortFast, UplinkFast і BackboneFast, протокол RSTP не є власністю однієї компанії.

Для забезпечення максимальної швидкості переконфігурації протокол RSTP вимагає повнодуплексного з'єднання "точка-точка" між комутаторами.

Переконфігурація зв'язного дерева при використанні протоколу RSTP займає менше однієї секунди, аналогічний процес протоколу STP займає близько однієї хвилини.

RSTP усуває потреби в таких функціях, як PortFast і UplinkFast. RSTP може переключатися в режим STP для обслуговування старого обладнання.

Для прискорення перерахунку число режимів портів протоколу RSTP зменшене до трьох: відхилення, навчання і пересилання. Режим відкидання аналогічний трьом оригінальним режимам STP: блокування, навчання і "відключений".

Крім того, у RSTP додана концепція активної топології. Усі порти, що не знаходяться в режимі відхилення, входять до складу активної топології і негайно переходять у режим пересилання.

Характеристики RSTP

RSTP забезпечує швидкий перерахунок зв'язного дерева: коли змінюється топологія мережі, RSTP може забезпечити збіжність в правильному налаштуванні мережі всього лише за кілька сотень мілісекунд. RSTP перевизначає тип портів та їх стан. Якщо порт налаштований як альтернативний або резервний порт він може відразу ж перейти в стан пересилання, не чекаючи збіжності мережі.

RSTP є найкращим протоколом для запобігання утворення петлі в комутованому мережевому середовищі. Такі удосконалення, як передавання в BPDU інформації про ролі портів тільки в сусідні комутатори, не вимагають додаткових налаштувань і в цілому виконується краще, ніж раніше в Cisco-пропрієтарних версіях. В даний час вони прозорі та інтегровані у функціонування протоколу.

Такі функції Cisco, як PortFast, UplinkFast і BackboneFast несумісні з протоколом RSTP.

В RSTP використовується поняття граничного порта по аналогії до механізму PortFast в протоколі STP. Це порт комутатора, який ніколи буде підключений до іншого комутатора. Такий порт після включення відразу ж переходить у стан пересилання.

Ні граничні порти, ні порти з підтримкою PortFast не спричиняють перегенерування змін в топології у випадку зміни свого стану.

На відміну від PortFast, граничний порт RSTP після отримання кадру BPDU втрачає статус граничного порту і негайно стає звичайним портом.

RSTP (802.1w) замінює STP (802.1D) при збереженні зворотньої сумісності. Основна частина термінології і більшість параметрів залишаються незмінними. Крім того, 802.1w здатен повертатись назад до 802.1D, для взаємодії з існуючими комутаторами. Наприклад, RSTP алгоритм вибирає кореневий міст аналогічно 802.1D.

RSTP (802.1w) використовує тип 2, версії 2 BPDU, завдяки чому RSTP міст може комунікувати з комутаторами, які використовують 802.1D. RSTP відправляє кадри BPDU і використовує поля flag в дещо інший спосіб, ніж STP.

Інформація протоколу визнається застарілою, якщо повідмлення-вітання не отримані протягом трьох послідовних діапазонів (протягом 6 секунд за замовчуванням, або якщо таймер max age завершився), що дозволяє швидко виявляти проблеми.

Стани портів та типи лінків в RSTP

Протокол RSTP забезпечує швидку збіжність при виникненні несправності або під час відновлення комутатора чи лінку. В протоколі RSTP роль порту відділена від стану порту. Наприклад, призначений порт може перебувати тимчасово в стані відхилення кадрів, хоча його кінцевим станом буде стан пересилання. В протоколі RSTP є три можливих стани портів: discarding (відхилення), learning (навчання) та forwarding (пересилання).

Тип лінку забезпечує класифікацію для кожного порту, який бере участь в RSTP. Тип зв'язку може визначати роль, яку відіграватиме порт при виконанні певних умов. Ці умови різні для прикордонних та неприкордонних портів. Неприкордонні порти поділяються на два типи лінків: точка-точка та спільні. Тип лінку визначається автоматично, але може бути переналаштований.

Прикордонні порти еквівалентні портам з підтримкою режиму PortFast, лінки типу точка-точка є кандидатами для швидкого переходу до стану пересилання. Однак, спочатку проткол RSTP повинен визначити роль портів, виходячи з того, що кореневі порти не використовують параметр “тип лінку”. Кореневі порти можуть зробити швидкий перехід в стан пересилання, як тільки порт засинхронізується.

Альтернативні та резервні порти не використовують параметр “тип лінку” в більшості випадків.

Призначені порти використовують параметр «тип лінку». Швидкий перехід в режим пересилання для призначених портів відбувається тільки, якщо тип лінку «точка-точка».

Керування трафіком в корпоративних мережах

Ієрархічні корпоративні мережі спрощують обмін інформацією. Інформація циркулює між мобільними співробітниками і філіями, а філії підключаються до офісів компанії в містах і країнах усього світу. В організації повинна бути створена ієрархія, що відповідає різним мережевим вимогам того чи іншого підрозділу компанії.

Як правило, найважливіша інформація і служби розміщуються вгорі ієрархії на захищених серверних фермах або у мережах збереження даних. Структура розгортається в безліч різних відділів, які утворюють нижню частину ієрархії.

Для взаємодії між рівнями ієрархії необхідне поєднання технологій LAN і WAN.

У корпоративних мережах необхідне керування трафіком, інакше вони не зможуть функціонувати. Маршрутизатори направляють трафік і запобігають засміченню основних каналів важливих служб широкомовними розсиланнями. Вони керують потоками трафіку між LAN так, що через мережу надходить тільки потрібний трафік.

Корпоративні мережі передбачають високий рівень надійності та обслуговування. Для цього використовується ряд заходів:

– передбачаються резервні канали на випадок відмови основного маршруту;

– впроваджуються служби QoS, щоб важливі дані оброблялися в першу чергу;

– використовується фільтрація пакетів, щоб виключити деякі типи пакетів, збільшити пропускну здатність каналу і захистити мережі від загрози атак.

Корпоративні топології

Правильний вибір фізичної топології дозволяє компанії розширити свої мережеві службибез зниження їхньої надійності та продуктивності. Мережеві проектанти приймають рішення про вибір топології на основі корпоративних вимог до продуктивності і надійності. В корпоративних середовищах зазвичай впроваджуються топологія типу “зірка” і топологія сітки.

Топологія типу “зірка”

Одна з найбільш розповсюджених фізичних топологій - топологія типу “зірка”. Центр “зірки” відповідає вершині ієрархії, що може представляти головне управління чи головний офіс компанії. Філії в тих чи інших місцях розташування з’єднуються з центром зірки.

Топологія типу “зірка” забезпечує централізоване керування мережею. Усі важливі служби і технічний персонал можна розташувати в одному місці. Топології типу “зірка” можна масштабувати. При додаванні нової філії додається ще одне з’єднання з центральною точкою “зірки”. Якщо у відділення з’являються кілька філій у своєму місці розташування, кожне з них може з’єднатися з центральним вузлом відділення, який в свою чергу підключається до головної точки центрального офісу. У цьому випадку проста “зірка” може розростися до розширеної зірки з малими “зірками” у головних філіальних відділеннях.

Топології типу “зірка” і “розширена зірка” утворять єдину точку відмови. Коміркові топології дозволяють усунути цю проблему.

Коміркові топології (топології сітки)

Кожне додаткове з’єднання дає альтернативний канал передачі даних і підвищує надійність мережі. В міру додавання з’єднань топологія стає комірковою із взаємозв’язаними вузлами. Кожне додаткове з’єднання збільшує собівартість і накладні витрати. Більш того, при цьому ускладнюється керування мережами.

Частково-коміркова

З додаванням додаткових з’єднань тільки у визначені області корпоративної мережі утвориться частково-коміркова топологія. Ця топологія відповідає вимогам надійності і доступності в таких критично важливих областях, як серверні ферми і мережі збереження даних. Інші області мережі як і раніше піддані відмовам. Таким чином, коміркову топологію необхідно розміщувати там, де це найбільш вигідно.

Повнозв’язна топологія

Якщо простої в роботі мережі недопустимі, тоді потрібна повнозв’язна топологія. У повнозв’язній топології кожен вузол з’єднується з усіма вузлами в компанії. Це найбільш відмовостійка топологія, але її впровадження вимагає найбільших витрат.

Мережа Інтернет – яскравий приклад коміркової топології. Керування пристроями в мережі Інтернет виконується не однією людиною або організацією. У результаті топологія мережі Інтернет постійно змінюється – деякі з’єднання стають активними, а інші неактивними. Додаткові з’єднання дозволяють збалансувати трафік і забезпечують надійний канал до адреси призначення.

Деякі з проблем мережі Інтернет постають і перед корпоративними мережами. Тому передбачені визначені процедури, що дозволяють пристроям адаптуватися до цих неперервно змінних умов і належним чином направляти трафік.

Статична та динамічна маршрутизація [21, 22]

Фізична топологія корпоративної мережі задає структуру для передачі даних. Маршрутизація забезпечує механізм її реалізації. У корпоративних мережах ускладнюється пошук оптимального маршруту до адреси призначення, оскільки в маршрутизатора може бути багато джерел інформації, на основі якої створюється таблиця маршрутизації.

Таблиця маршрутизації [11, 12] – це файл даних, що знаходиться в ОЗП і зберігає дані про підключення віддалених та безпосередньо під’єднаних мереж. У таблиці маршрутизації кожна мережа зв’язана або з вихідним інтерфейсом, або з наступним переходом.

Вихідний інтерфейс – це фізичний шлях, що використовується маршрутизатором для переміщення даних ближче до адреси призначення. Наступний перехід – це інтерфейс підключеного маршрутизатора, що переміщує дані ближче до адреси кінцевого призначення.

Крім того, у таблиці кожному маршруту призначається номер, що відображає ймовірність і точність джерела даних про маршрутизацію – адміністративна відстань. Маршрутизатори обслуговують дані про безпосередньо підключені, статичні та динамічні маршрути.

Маршрути з прямим підключенням

Безпосередньо підключена мережа підключається до інтерфейсу маршрутизатора. За допомогою налаштування інтерфейсу з IP-адресою та маскою інтерфейс стає вузлом у підключеній мережі. Адреса мережі і маска інтерфейсу разом з типом і номером інтерфейсу відображаються в таблиці маршрутизації як безпосередньо підключена мережа. У таблиці маршрутизації безпосередньо підключені мережі позначаються символом C.

Статичні маршрути

Статичні маршрути – це маршрути, що налаштовуються адміністратором мережі вручну. Статичний маршрут містить у собі адресу мережі і маску для мережі призначення разом з вихідним інтерфейсом або IP-адресою маршрутизатора наступного переходу. У таблиці маршрутизації статичні маршрути позначаються символом S. У статичних маршрутів найменша адміністративна відстань, оскільки вони стабільніші та надійніші за динамічні маршрути.

Динамічні маршрути

Протоколи динамічної маршрутизації також додають віддалені мережі в таблицю маршрутизації. Вони дозволяють маршрутизаторам спільно використовувати інформацію про надійність і статус віддалених мереж за допомогою виявлення мережі. Кожен протокол відправляє та отримує пакети даних, виконуючи пошук інших маршрутизаторів, оновлюючи та обслуговуючи таблиці маршрутизації. Маршрути, отримані за допомогою протоколів динамічної маршрутизації, визначаються протоколом. Наприклад, R позначається протокол RIP, а D – протокол EIGRP. Їм призначається адміністративна відстань протоколу.

Як правило, в корпоративній мережі використовуються і статичні, і динамічні маршрути. Статична маршрутизація спрямована на рішення конкретних мережевих задач. У залежності від фізичної топології за допомогою статичного маршруту можна керувати потоками трафіку.

Якщо обмежити трафік однією точкою входу/виходу, буде створена закрита мережа. У філіях деяких корпоративних мереж є тільки один можливий маршрут до іншої частини мережі. У цьому випадку кінцевий маршрутизатор не буде обтяжений відновленнями маршрутів і збільшенням навантаження через виконання протоколу динамічної маршрутизації, тому статична маршрутизація більш виграшна.

У залежності від розташування і функцій для деяких корпоративних маршрутизаторів можливе виникнення потреби використання статичних маршрутів. Прикордонні маршрутизатори використовують статичні маршрути для забезпечення безпечних стабільних маршрутів до ISP. Інші маршрутизатори використовують протоколи статичної, або динамічної маршрутизації відповідно до задач.

Маршрутизатори корпоративної мережі використовують пропускну здатність, пам’ять і обчислювальні ресурси для перетворення NAT/PAT, фільтрації пакетів і інших сервісів. Статична маршрутизація дозволяє виконувати пересилання, уникаючи навантаження, що пов’язане з більшістю протоколів динамічної маршрутизації.

Статична маршрутизація передбачає вищий рівень безпеки, ніж динамічна, оскільки не вимагає відновлення маршрутів. Хакер може перехопити відновлення динамічної маршрутизації, щоб отримати дані про мережу.

Проте, і при статичній маршрутизації можуть виникнути проблеми. Вона вимагає тимчасових витрат і точності з боку мережевого адміністратора, що змушений вручну вводити дані маршрутизації. Проста помилка в статичному маршруті може привести до простою мережі та втрати пакетів. Після зміни статичних маршрутів у мережі можуть виникнути помилки і збої маршрутизації в ході ручного переналаштування. З цих причин статична маршрутизація не підходить для повсякденного використання у великих корпоративних середовищах.

Налаштування статичних маршрутів

Глобальною командою для налаштування більшості статичних маршрутів є ip route з вказанням мережі призначення, маски та шляху до неї. Таким чином, команда наступна:

Router(config)#ip route [адреса мережі] [маска підмережі] [адреса наступного переходу або вихідного інтерфейсу]

За допомогою адреси наступного переходу, або вихідного інтерфейсу, маршрутизатор направляє трафік до потрібної адреси призначення. Однак ці два параметри діють по-різному.

Перед пересиланням маршрутизатором пакету процес у таблиці маршрутизації визначає вихідний інтерфейс для використання. Пошук у таблиці маршрутизації по статичних маршрутах, налаштованих для роботи з вихідними інтерфейсами, здійснюється лише один раз. Тоді як статичним маршрутам з налаштованим параметром наступного переходу доводиться звертатися до таблиці маршрутизації двічі, щоб визначити вихідний інтерфейс.

У корпоративній мережі статичні маршрути, налаштовані для роботи з вихідними інтерфейсами, ідеальні для з’єднань точка-точка, наприклад, для з’єднань між прикордонним маршрутизатором та ISP.

Статичним маршрутам, налаштованим для роботи з інтерфейсом наступного переходу, потрібно два кроки, щоб визначити вихідний інтерфейс. Це і є рекурсивний пошук. У ході рекурсивного пошуку:

– маршрутизатор співставляє IP-адресу призначення для пакету зі статичним маршрутом;

– далі він співставляє IP-адресу наступного переходу статичного маршруту з записами в таблиці маршрутизації, щоб визначити інтерфейс для використання.

Якщо відключений вихідний інтерфейс, статичні маршрути не будуть відображатися в таблиці маршрутизації. Після включення інтерфейсу маршрути будуть у ній перевстановлені.

Об’єднання декількох статичних маршрутів в один запис скорочує розмір таблиці маршрутизації і підвищує ефективність процесу пошуку. Цей процес називається сумуванням маршрутів.

Один статичний маршрут підсумовує кілька статичних маршрутів, якщо:

– мережі призначення об’єднані в єдину мережеву адресу;

– усі статичні маршрути використовують однакову IP-адресу вихідного інтерфейсу або наступного переходу.

Без сумарних маршрутів таблиці маршрутизації на магістральних маршрутизаторах мережі Інтернет стають некерованими. У корпоративних мережах виникають ті ж проблеми. Сумарні статичні маршрути – незамінне рішення в керуванні розмірами таблиць маршрутизації.

В залежності від корпоративних служб WAN статичні маршрути можуть забезпечувати резервне копіювання при відмові з’єднання основної WAN. У цьому випадку з метою резервного копіювання використовується функція плаваючих статичних маршрутів.

За замовчуванням адміністративна відстань статичного маршруту менша за адміністративну відстань маршруту, отриманого з використанням протоколів динамічної маршрутизації. Адміністративна відстань плаваючого статичного маршруту більша за адміністративну відстань маршруту, отриманого по протоколу динамічної маршрутизації. З цієї причини плаваючий статичний маршрут не відображається в таблиці маршрутизації. Запис плаваючого статичного маршруту буде відображений в таблиці маршрутизації, тільки якщо дані динамічних протоколів будуть втрачені.

Для створення плаваючого статичного маршруту потрібно додати значення для адміністративної відстані в кінці команди ip route:

Router(config)#ip route 192.168.4.0 255.255.255.0 192.168.9.1 200

Адміністративна відстань повинна бути більша AD, призначеної протоколу динамічної маршрутизації. Маршрутизатор використовує основний маршрут, поки він активний. Якщо основний маршрут стає неактивним, у таблиці буде встановлений плаваючий статичний маршрут.

Маршрути за замовчуванням

У таблицях маршрутизації не може бути маршрутів для всіх можливих вузлів мережі Інтернет. Зростання розмірів таблиць маршрутизації потребує більше ОЗП та обчислювальної потужності. Спеціальний тип статичного маршруту, названий маршрутом за замовчуванням, вказує який шлюз використовувати, якщо в таблиці маршрутизації немає шляху до адреси призначення. Звичайно маршрути за замовчуванням вказують наступний маршрутизатор на шляху до ISP. У складних корпоративних середовищах маршрути за замовчуванням виводять Інтернет-трафік з мережі.

Команда для створення маршруту за замовчуванням схожа з командою для створення звичайного чи плаваючого статичного маршруту. Мережева адреса і маска позначаються як 0.0.0.0, в результаті отримуємо маршрут чотирьох нулів. У команді використовується або адреса наступного переходу, або параметри вихідного інтерфейсу.

Нулі вказують маршрутизатору, що для використання цього маршруту біти збігатися не повинні. Якщо не існує більш оптимального маршруту, маршрутизатор буде використовувати статичний маршрут за замовчуванням.

Кінцевий маршрут за замовчуванням, розташований на пограничному маршрутизаторі, відправляє трафік до ISP. Цей маршрут позначає останній вузол в корпоративній мережі, як шлюз “останньої надії” для пакетів, що не вдається доставити. Ці дані відображаються в таблицях маршрутизації всіх маршрутизаторів.

Якщо в корпоративній мережі використовується протокол динамічної маршрутизації, пограничний маршрутизатор може відправляти маршрут за замовчуванням іншим маршрутизаторам у формі відновлення динамічних маршрутів.

Призначення протоколів динамічної маршрутизації

Протоколи маршрутизації використовуються для полегшення обміну інформацією про маршрутизацію між маршрутизаторами. Протоколи маршрутизації дозволяють

маршрутизаторам динамічно обмінюватися інформацією про віддалені мережі і автоматично додавати цю інформацію в своїх таблицях маршрутизації.

Протоколи маршрутизації визначають найкращий шлях до кожної мережі, який потім додається в таблицю маршрутизації. Одним з основних переваг використання протоколів динамічної маршрутизації є те, що маршрутизатори обмінюються маршрутною інформацією після зміни топології. Такий обмін дозволяє маршрутизаторам автоматично дізнаватися про нові мережі, а також знайти альтернативні шляхи, коли виникають проблеми з існуючим маршрутом.

В порівнянні зі статичною маршрутизацією, протоколи динамічної маршрутизації, вимагають менше затрат на адміністрування. Але відбувається це за рахунок використання частини ресурсів маршрутизатора для забезпечення роботи протоколів роботи (процесор, оперативна пам'ять) та пропускної здатності каналу зв'язку. Незважаючи на переваги динамічної маршрутизації, статична маршрутизація досі займає важливе місце в маршрутизації. Є моменти, коли статична маршрутизація є доцільнішою, хоча найчастіше ці типи маршрутизації поєднуються.

Протокол маршрутизації – це набір процесів, алгоритмів та повідомлень, які використовуються для обміну інформацією про маршрутизацію та заповнення таблиці маршрутизації та вибору найкращого маршруту. Протоколи маршрутизації забезпечують:

– виявлення віддалених мереж;

– підтримку актуальної інформації;

– вибір найкращого шляху до мережі призначення;

– можливість знайти новий кращий шлях, якщо поточний шлях більше недоступний.

Компонентами протоколу маршрутизації є:

– Структури даних – деякі протоколи маршрутизації використовують таблиці та/або бази даних для своїх операцій. Ця інформація зберігається в оперативній пам'яті.

– Алгоритм – це набір кроків, що використовується протоколами маршрутизації, обробки інформації про маршрутизацію та визначення найкращого маршруту.

– Повідомлення – протоколи маршрутизації використовують різні типи повідомлень для виявлення сусідніх маршрутизаторів, обміну інформацією про маршрутизацію, а також інші завдання для вивчення та підтримки іформації про мережу.

Всі протоколи маршрутизації мають однакову мету – дізнаватися про віддалені мережі та швидко адаптуватися до змін в топології. Методи, які використовують протоколи маршрутизації для досягнення цієї мети залежать від алгоритму, який використовується протоколом та характеристик самого протоколу.

Класифікація протоколів динамічної маршрутизації

Протоколи маршрутизації поділяються на групи в залежності від характеристик. Найбільш вживаними протоколами маршрутизації є:

RIP – дистанційно-векторний протокол внутрішньої маршрутизації.

IGRP – дистанційно-векторний протокол розроблений Cisco (застарілий на сьогоднішній день).

OSPF – внутрішній протокол стану каналу.

IS-IS – внутрішній протокол стану каналу.

EIGRP – покращений дистанційно-векторний протокол, розроблений Cisco.

BGP – протокол вектору шляху зовнішньої маршрутизації.

Протоколи IGP та EGP

Автономна система (AS - autonomous system), або домен маршрутизації – це набір маршрутизаторів під спільним адмініструванням. Типовими прикладами є внутрішні мережі компаній та мережі Інтернет-провайдерів. Оскільки Інтернет заснований на концепції автономної системи потрібні два типи протоколів маршрутизації: внутрішні та зовнішні. Цими протоколами є:

Внутрішні протоколи (IGP - Interior Gateway Protocols) використовуються для маршрутизації всередині автономної системи.

Зовнішні протоколи (EGP - Exterior Gateway Protocols) використовуються для міждоменної маршрутизації – маршрутизації між автономними системами.

Характеристики IGP та EGP протоколів маршрутизації

Протоколи внутрішньої маршрутизації використовуються в межах домену, який контролюється однією організацією. Автономна система зазвичай складається з безлічі окремих мереж, що належать компаніям, закладам, установам. Протоколи IGP використовуються для маршрутизації в межах автономної системи, а також для маршрутизації в межах окремих мереж. До протоколів IGP належать RIP, IGRP, EIGRP, OSPF та IS-IS.

Протоколи EGP призначені для використання між різними автономними системами, які знаходяться під контролем різних адміністрацій. На даний час BGP є єдиним життєздатним EGP протоколом маршрутизації, який використовується в Інтернет. BGP є протоколом вектора шляху та може використовувати багато атрибутів для оцінки маршрутів. На рівні провайдера, часто є більш важливі питання, ніж просто вибір найшвидшого маршруту. BGP зазвичай використовується між провайдерами, а іноді і між компанією та Інтернет-провайдером.

Конвергенція

Конвергенція (або збіжність) – це стан мережі, коли таблиці маршрутизації всіх маршрутизаторів знаходяться в стані узгодженості. Мережа конвергентна тоді, коли всі маршрутизатори мають повну і точну інформацію про мережу. Час збіжності – це час, який необхідний маршрутизаторам для обміну інформацією, обчислення найкращих маршрутів та оновлення таблиць маршрутизації. Мережа не є повноцінно робочою, поки не відбудеться конвергенція. Через це більшість мереж вимагають короткий час конвергенції.

Конвергенція характеризується швидкістю поширення маршрутної інформації та розрахунку оптимальних маршрутів. Протоколи маршрутизації можуть порівнюватись на основі швидкості збіжності. Швидша конвергенції характеризує кращий протокол маршрутизації.

Метрики

Є випадки, коли протокол маршрутизації дізнається про більш, ніж один маршрут до певного місця призначення. Щоб вибрати кращий шлях, протокол маршрутизації повинен вміти оцінити відмінності між доступними шляхами. Для цього використовується метрика. Метрика – це значення, яке використовується протоколами маршрутизації для визначення вартості доступу до віддалених мереж.

Різні протоколи маршрутизації використовують різні метрики. Метрики, що використовуються одним протоколом, відрізняються від метрик іншого протоколу. Два різних протоколи маршрутизації виберуть різні маршрути до одніє мережі призначення за рахунок використання різних метрик.

RIP буде вибирати шлях з найменшою кількістю стрибків, в той час як OSPF вибиратиме шлях з високою пропускною здатністю.

Протоколи маршрутизації використовують такі метрики:

Hop count (кількість переходів) – проста метрика, яка підраховує кількість маршрутизаторів, через які повинен пройти пакет.

Bandwidth (смуга пропускання) – вибір маршруту з врахуванням найвищої пропускної здатності.

Load (завантаження) – враховує завантаженість каналів передачі.

Delay (затримка) – враховує час проходження пакета по маршруту.

Reliability (надійність) – оцінює ймовірність збою каналу передачі, розраховується на основі помилок інтерфейсу або попередніх збоїв.

Cost (вартість) – вартість, визначається IOS або адміністратором мережі, щоб вказати перевагу маршруту. Вартість може представляти метрики, поєднання метрик чи політики.

Метриками для різних протоколів є:

RIP: кількість переходів – найкращим шляхом вибирається шлях з найменшою кількістю переходів.

IGRP та EIGRP: пропускна здатність, затримка, надійність та завантаження – найкращим шляхом вважається маршрут з найменшою композитною метрикою, обчисленою

з врахуванням цих параметрів. За замовчуванням використовується лише пропускна здатність та затримка.

IS-IS та OSPF: вартість – найкращим шляхом вибирається шлях з найменшою вартістю. Варіант реалізації OSPF компанією Cisco використовує пропускну здатність.

Балансування навантаження (Load balancing)

Протоколи використовують метрики для визначення найкращого шляху до віддаленої мережі. Але можлива ситуація, коли кілька маршрутів мають однакові значення метрики. В такому випадку маршрутизатор вибирає не один маршрут, а балансує навантаження між цими однаковими маршрутами. Пакети пересилаються з використанням рівноцінних маршрутів.

Протоколи динамічної маршрутизації поділяються на дві основні категорії: «вектор відстані» та «стану каналу».

Протоколи маршрутизації типу «вектор відстані»

Вектор відстані означає, що маршрути визначаються як вектори відстані та напрямку. Відстань визначається в термінах метрики, наприклад, як число переходів, а напрям – це маршрутизатор наступного пересилання або вихідний інтерфейс.

Протоколи векторів відстані зазвичай використовують алгоритм Беллмана-Форда для визначення кращого маршруту.

Деякі протоколи векторів відстані періодично відправляють повні таблиці маршрутизації до всіх підключених сусідів. У великих мережах такі оновлення маршрутів можуть створювати значні об’єми трафіку.

Хоча алгоритм Беллмана-Форда в кінцевому рахунку накопичує достатньо інформації, для підтримки бази даних досяжності мереж, алгоритм не дозволяє маршрутизатору знати топологію всієї мережі. Маршрутизатор знає тільки інформацію отриману від своїх сусідів.

Єдиною інформацією, якою володіє маршрутизатор про віддалену мережу, є відстань або метрика для досягнення цієї мережі, та інформація про те, який шлях або інтерфейс використовувати, щоб туди дістатися. Протоколи векторів відстані не мають фактичної карти топології мережі.

Протоколи векторів відстані працюють найкраще в таких умовах:

– мережа є простою та плоскою і не потребує спеціального ієрархічного дизайну;

– мережеві адміністратори не володіють достатніми знаннями для налаштування та діагностики протоколів стану каналу;

– в певних типах мереж, таких як зіркоподібні мережі (hub-and-spoke networks);

– час конвергенції мережі не має значення.

Динамічні протоколи маршрутизації допомагають мережевому адміністратору зекономити час на налаштування та обслуговування статичних маршрутів.

До протоколів векторів відстані належать протоколи:

– Routing Information Protocol (RIP);

– Interior Gateway Routing Protocol (IGRP);

– Enhanced Interior Gateway Routing Protocol (EIGRP).

RIP

Протокол RIP був описаний в RFC 1058. Він має такі основні характеристики:

– лічильник переходів використовується як метрика для вибору маршруту;

– якщо кількість переходів більше 15, RIP не може забезпечити маршрут до цієї мережі;

– оновлення інформації про маршрутизацію відбувається шляхом широкомовної або групової розсилки кожні 30 секунд, за замовчуванням.

IGRP

Протокол IGRP є власною розробкою компанії Cisco. IGRP має такі основні характеристики дизайну:

– пропускна здатність, затримка, надійність та завантаження використовуються для створення композитної метрики;

– оновлення інформації про маршрутизацію відбувається шляхом широкомовної розсилки кожні 90 секунд, за замовчуванням;

– IGRP є попередником EIGRP і на даний час не використовується.

EIGRP

Протокод EIGRP є власністю Cisco і має такі основні характеристики:

– він може виконувати балансування навантаження;

– він використовує алгоритму DUAL (Diffusing Update Algorithm) для розрахунку найкоротшого шляху;

– в ньому не використовуються періодичні оновлення. Оновлення маршрутної інформації здійснюється тільки тоді, коли відбуваються зміни в топології.

Як і всі протоколи маршрутизації, протоколи на основі векторів відстані використовують метрику для визначення оптимального маршруту. Протоколи на основі векторів відстані розраховують оптимальний маршрут, виходячи з відстані від маршрутизатора до мережі.

Протоколам, на основі векторів відстані, звичайно потрібно менш складне налаштування і керування в порівнянні з протоколами на основі стану каналу. Вони можуть виконуватися маршрутизаторами старіших моделей з меншою потужністю і вимагають меншого об’єму пам’яті та обчислень.

Маршрутизатори, що використовують протоколи на основі векторів відстані, виконують широкомовну чи багатоадресну розсилку всієї таблиці маршрутизації своїм сусідам через рівні інтервали часу. Якщо маршрутизатор отримує більше одного маршруту до адреси призначення, він розраховує і передає маршрут з найменшою метрикою.

Цей спосіб передачі даних маршрутизації у великих мережах відрізняється малою швидкістю. У визначений момент у деяких маршрутизаторів може не бути останніх відомостей про мережу. Це обмежує масштабованість протоколів і викликає проблеми, наприклад, петлі маршрутизації.

Періодичні оновлення та підтримка таблиць маршрутизації

Багато протоколів векторів відстані використовують періодичні оновлення для обміну маршрутною інформацією з сусідами та підтримування актуальної інформації в таблиці маршрутизації. Протоколи динамічної маршрутизації RIP та IGRP є прикладами таких протоколів.

Таймер оновлення інформації про маршрутизацію в таблиці маршрутизації оновлюється щоразу після отримання оновлення. Таким чином, інформація в таблиці маршрутизації може бути змінена при змінах в топології. Зміни можуть відбуватися з кількох причин, серед яких:

– відмова каналу зв’язку;

– додавання нового каналу зв’язку;

– відмова маршрутизатора;

– зміна параметрів каналу зв’язку.

Петлі маршрутизації (Routing Loop)

Петля маршрутизації – це ситуація, при виникненні якої пакет постійно передається між маршрутизаторами і ніколи не досягає своєї мережі призначення. Петля маршрутизації може виникнути у випадку, коли два або більше маршрутизаторів мають інформацію про маршрутизації, яка вказує, що існує шлях до недосяжної мережі.

Петля може виникнути в результаті:

– неправильно налаштованих статичних маршрутів;

– неправильно налаштованого перерозподілу маршрутів (route redistribution);

– непослідовності таблиць маршрутизації, яка виникає через повільну збіжність мережі.

Простота роботи протоколів типу вектора відстані є причиною такого недоліку, як петлі маршрутизації, хоча за певних умов петлі маршрутизації можуть виникати і в протоколах типу стану каналу.

IP-протокол має свій власний механізм для запобігання нескінченній передачі пакетів через мережу. Для цього використовується поле TTL (Time-to-Live). Його значення

зменшується на одиницю при проходженні через кожен маршрутизатор на шляху проходження від відправника до одержувача. Якщо TTL дорівнює нулю, маршрутизатор відкидає пакет.

Виникнення петель маршрутизації спричинює зниження продуктивності або, навіть, простій мережі.

Петлі маршрутизації виникають за певних умов:

– пропускна здатність каналу зв'язку буде використовуватися для передачі;

– процесор маршрутизатора буде завантажений циклічними пакетами;

– процесор маршрутизатора буде завантажений пересиланням непотрібних пакетів, що в свою чергу вплине на час збіжності мережі;

– оновлення маршрутизації можуть втрачатись або не оброблятись вчасно. Це створюватиме нові петлі маршрутизації, погіршуючи ситуацію загалом.

Для усунення петель маршрутизації використовується ряд механізмів, в першу чергу в протоколах вектора відстані. До цих механізмів належать:

– визначення максимальної метрики для запобігання нескінченної передачі;

– holddown timers (таймери утримання);

– split horizon(розділення горизонту);

– route poisoning or poison reverse (зворотнє виправлення);

– triggered updates (миттєве оновлення).

Встановлення максимальної метрики дозволяє після певної кількості переходів позначити мережу недосяжною та відкинути пакет.

Таймери утримання використовуються для запобігання оновленням з неналежно відновлених чи поганих маршрутів. Таймери визначають період, протягом якого маршрутизатори не проводять будь-які зміни. Якщо маршрут позначається як втрачений, або, як можливо втрачений, будь-яка інша інформація про цей маршрут, яка містить такий же статус, або гірший статус, ігнорується протягом певного періоду часу (період утримання). Це означає, що маршрутизатори залишають маршрут в таблиці маршрутизації позначеним як недосяжний протягом часу, достатнього для розповсюдження таблиць маршрутизації з останньою актуальною інформацією до всіх маршрутизаторів в мережі.

Правило розділення горизонту визначає, що маршрутизатор не повинен надсилати оновлення про мережу через інтерфейс, з якого надійшли оновлення. Split horizon може бути відключений адміністратором.

Route poisoning використовується для позначення маршруту, як недосяжного в оновленнях, які надсилаються на інші маршрутизатори. Недосяжність інтерпретується як метрика, яка встановлюється на максимум. Для RIP poisoned route має метрику 16.

Щоб пришвидшити процес конвергенції після зміни топології, RIP використовує миттєві оновлення. Миттєві оновлення оновлюють таблиці маршрутизації негайно у відповідь на зміну маршруту. Миттєві оновлення не чекають завершення таймера оновлення. Отримавши оновлення, маршрутизатор негайно відправляє повідомлення про оновлення на сусідні маршрутизатори.

Миттєві оновлення надсилаються у випадку:

– зміни стану інтерфейсу (up або down);

– маршрут став "недосяжним";

– маршрут додано в таблицю маршрутизації;

Використання миттєвих оновлень було б достатньо, якщо б існувала гарантія, що хвиля оновлення досягне всіх необхідних маршрутизаторів негайно. Проте, є дві проблеми з миттєвими оновленнями:

– пакети, що містять оновлення можуть бути видалені або пошкоджені;

– миттєві оновлення не відбуваються миттєво. Цілком можливо, що маршрутизатор, який ще не отримав миттєве оновлення надсилатиме регулярне оновлення у невідповідний час, що спричинить встановлення поганого маршруту в сусідньому маршрутизаторі, який вже отримав миттєве оновлення.

Критерії вибору протоколу

Приймаючи рішення, який протокол вектора відстані вибрати, необхідно враховувати декілька факторів:

– розмір мережі

– сумісність між моделями маршрутизаторів

– знання та вміння адміністратора

Протоколи RIP версії 1 і 2 є звичайними протоколами на основі векторів відстані, а протокол EIGRP – протоколом на основі векторів відстані з розширеними можливостями. Протокол RiPng, нова версія протоколу RIP, був спеціально розроблений для підтримки IPv6.

Протягом багатьох років протокол RIP перетворився з протоколу повнокласової маршрутизації (RIPv1) на протокол безкласової маршрутизації (RIPv2). RIPv2 – це стандартизований протокол маршрутизації, що працює на обладнанні різних виробників. Це один з найпростіших протоколів маршрутизації для налаштування, що робить його гарним вибором для невеликих мереж. Проте RIPv2 також має певні обмеження. Протоколи RIPv1 та RIPv2 використовують кількість переходів в якості метрики маршруту, з максимальним обмеженням в 15 переходів, що обмежує їх використання.

Особливості RIP:

– підтримуєм split horizon та split horizon з poison reverse для запобігання утворенню петель;

– забезпечує балансування навантаження з підтримкою до шести рівноцінних по вартості маршрутів. За замовчуванням використовується чотири рівноцінні маршрути.

В RIPv2 внесені такі вдосконалення:

– в оновлення включається маска підмережі;

– механізм аутентифікації для оновлення таблиці маршрутизації;

– підтримка маски змінної довжини (VLSM);

– використання групових адрес замість широкомовних;

– підтримка сумування маршруту.

Протокол EIGRP (Enhanced IGRP) був розроблений на базі протоколу IGRP. EIGRP безкласовий протокол типу вектора відстані з певними функціями схожими на функції протоколів стану каналу. Це є пропрієтарний протокол і працює лише на маршрутизаторах Cisco.

Основні характеристики EIGRP:

– миттєві оновлення (EIGRP не використовує періодичних оновлень);

– використовує таблицю топології для підтримки всіх маршрутів, отриманих від сусідів (не тільки кращих шляхів);

– створення суміжніх з’єднань з сусідніми маршрутизаторами, які використовують протокол EIGRP hello;

– підтримка VLSM та ручного сумування маршрутів.

Переваги EIGRP:

– хоча маршрути поширюються за принципом вектора відстані, метрика базується на мінімальній ширині смуги та затримці маршруту, а не кількості стрибків;

– швидка збіжність завдяки використанню алгоритму DUAL(Diffusing Update Algorithm) для обчислення маршруту. DUAL дозволяє вставляти в таблиці EIGRP топології резервні маршрути, які використовуються у випадку, якщо основний маршрут пошкоджується. Завдяки цьому перемикання на резервний маршрут відбувається негайно і не потребує жодних дій від будь-яких інших маршрутизаторів.

– обмежені оновлення означають, що EIGRP використовує менше пропускної здатності, особливо у великих мережах з великою кількістю маршрутів;

– EIGRP підтримує декілька протоколів мережевого рівня завдяки використанню незалежних модулів, які включають в себе підтримку IP, IPX та AppleTalk.

Характеристики протоколу RiPv1

Протокол RIP був першим протоколом маршрутизації на основі вектору відстані IP, стандартизованого у RFC (RFC1058 у 1988 році). Першу версію RIP тепер часто називають

RiPv1, щоб відрізняти її від згодом удосконаленої версії RiPv2, а також від версії IPv6 – RiPng.

Основні характеристики RIPv1

– повнокласовий протокол типу вектора відстані;

– в ролі метрики використовує кількість переходів;

– маршрути, з кількістю переходів понад 15, недосяжні;

– широкомовна розсилка оновлень кожні 30 секунд.

Дані RIP повідомлення інкапсулюються в UDP сегмент з номером порту відправника та отримувача 520. В заголовок IP та заголовок канального рівня додається широкомовна адреса призначення перед надсиланням через усі налаштовані інтерфейси.

RIP таймери

За замовчуванням протокол RiPv1 виконує широкомовну передачу оновлень маршрутів по всіх активних інтерфейсах кожні 30 секунд.

Крім таймеру оновлення, використовуються ще три таймери:

– Invalid

– Flush

– Holddown

Invalid timer. Якщо оновлення для існуючого маршруту не були отримані протягом 180 секунд (за замовчуванням), маршрут позначається як недійсний, і йому встановлюється метрика 16. Маршрут залишається в таблиці маршрутизації до моменту завершення flush таймера.

Flush timer. За замовчуванням, таймер встановлюється на 240 секунд, тобто на 60 секунд довше, ніж invalid таймер. Коли flush таймер завершується, маршрут видаляється з таблиці маршрутизації.

Holddown timer. Цей таймер стабілізує маршрутну інформацію та допомагає запобігати петлям маршрутизації в періоди здійснення конвергенції мережі. Як тільки маршрут позначається як недосяжний, він залишається в стані утримання протягом часу, достатнього для отримання усіма маршрутизаторами інформації про недоступність мережі. За замовчуванням таймер встановлюється на 180 секунд..

RiPv1 є протоколом повнокласової маршрутизації. Він автоматично підсумовує підмережі по класовій межі і не відправляє, у оновленні, дані про мережеву маску. Відповідно, RiPv1 не підтримує VLSM і CIDR. Маршрутизатор, що працює по протоколу RiPv1, або використовує задану для локального інтерфейсу мережеву маску, або застосовує мережеву маску на основі класу адреси, яка використовується по замовчуванню. Через це обмеження підмережі, що повідомляються протоколом RiPv1, не можуть бути несуміжними.

Наприклад, маршрутизатор із заданими інтерфейсами, як шлюзами для підмереж 172.16.1.0/24 і 172.16.4.0/24, при використанні протоколу RiPv1 буде повідомляти тільки мережу класу B 172.16.0.0. Відповідно, інший маршрутизатор, що отримує це поновлення, буде вказувати мережу 172.16.0.0 у своїй таблиці маршрутизації. Це означає, що пакети з фактичною адресою підмережі призначення 172.16.3.0 можуть бути помилково спрямовані на інший маршрутизатор і не прибудуть у потрібну підмережу призначення.

За замовчуванням RIP має адміністративну відстань 120.

Зупинка непотрібних оновлень RIP протоколу.

Для запобігання передачі оновлень через певні інтерфейси маршрутизатора використовується команда:

Router(config-router)#passive-interface interface-type interface-number

Ця команда зупиняє оновлення маршрутів із зазначеного інтерфейсу. Проте, мережа, до якої належить вказаний інтерфейс буде передаватись в оновленнях маршрутів, які відправляються з інших інтерфейсів.

Автоматичне сумування машрутів

Протокол RIP є повнокласовим протоколом, який автоматично сумує повнокласові мережі на кордоні мережі.

Правила обробки оновлень:

– якщо оновлення та інтерфейс, який їх приймає, належать до однієї і тієї ж мережі, тоді мережева маска інтерфейсу застосовується до мережі в оновленні

– якщо оновлення та інтерфейс, який їх приймає, належать до різних мереж, тоді повнокласова маска застосовується до мережі в оновленні

Переваги автоматичного сумування маршрутів.

Протокол RIP автоматично сумує повно класові мережі. Оскільки оновлення 172.30.0.0 надсилається через інтерфейс (Serial 0/0/1) в іншу повнокласову мережу (192.168.4.0), RIP надсилає повнокласову мережу замість окремих підмереж.

Це зменшує розмір оновлень та завантаженість каналів зв'язку (між R2 та R3 в даному прикладі).

R3 отримає один маршрут для мережі 172.30.0.0/16 незалежно від того, скільки є підмереж. Використання єдиного маршруту пришвидшує пошук в таблиці маршрутизації маршрутизатора R3.

Недоліки автоматичного сумування

Протоколи повнокласової маршрутизації не включають мережевої маски в оновлення. Мережі автоматично сумуються на границі мережі.

Наприклад маршрутизатори R1 та R3 мають підмережі з мережі 172.30.0.0/16, в той час як R2 не має. Отже, R1 та R3 є прикордонними маршрутизаторами для 172.30.0.0/16, оскільки вони розділені іншою мережею 209.165.200.0/24. Це розділення створює несуміжні мережі (discontiguous network), у вигляді двох груп підмереж 172.30.0.0/24, розділених іншою мережею. 172.30.0.0/16 є несуміжною мережею.

Навіть за умови правильного налаштування RIPv1 він не здатний визначити всі мережі в несуміжній топології. Так R1 не буде оголошувати 172.30.1.0 або 172.30.2.0 до R2 через мережу 209.165.200.0. Аналогічно R3 не буде оголошувати 172.30.100.0 або 172.30.200.0 до R2 через мережу 209.165.200.0. Хоча обидва маршрутизатори R1 та R3 будуть оголошувати 172.30.0.0.

Характеристики протоколу RiPv2

Протокол RIPv2 описаний в RFC 1723. Подібно до RIPv1, RIPv2 інкапсулюється в UDP сегмент використовуючи порт 520 і може переносити інформацію про 25 маршрутів. RIPv2 має такий самий формат повідомлення як RIPv1, але додаються два суттєві розширення.

Першим розширенням є поле мережевої маски, що дозволяє включати 32 бітну маску в запис маршруту. Завдяки цьому більше не існує залежності мережевої маски від вхідного інтерфейсу чи повно класової маски при визначенні маски маршруту.

Другим суттєвим розширенням формату повідомлення RIPv2 є додавання адреси наступного переходу (Next Hop Address). Ця адреса використовується для визначення кращої адреси наступного переходу ніж адреса маршрутизатора, який надсилає повідомлення. Якщо всі поля встановлені в нулі (0.0.0.0), адреса маршрутизатора, який надсилає повідомлення буде найкращою адресою наступного переходу.

У протоколу RiPv2 багато функцій, схожих з RiPv1. Крім того, він передбачає важливі удосконалення. RiPv2 – це протокол безкласової маршрутизації, що підтримує VLSM і CIDR. Поле маски включено в оновлення версії 2, що дозволяє використовувати несуміжні мережі. Крім того, протокол RiPv2 дає можливість відключити автоматичне підсумовування маршрутів.

Обидві версії протоколу RIP розсилають усю таблицю маршрутизації з усіх задіяних інтерфейсів у формі оновлень. RiPv1 виконує широкомовне розсилання цих новлень для 255.255.255.255. Це потребує обробки даних усіма пристроями широкомовної мережі (наприклад, мережа Ethernet). RiPv2 виконує багатоадресну розсилку своїх оновлень на адресу 224.0.0.9. Багатоадресна розсилка потребує меншої пропускної здатності, ніж широкомовні розсилки. Пристрої, не налаштовані для роботи з протоколом RiPv2, відхиляють багатоадресні розсилки на канальному рівні.

Зловмисники часто впроваджують неправильні оновлення, щоб маршрутизатор відправляв дані на помилкову адресу призначення або, щоб значно знизити продуктивність мережі. Неправильні відомості також можуть виявитися в таблиці маршрутизації через

помилкове налаштування чи несправну роботу маршрутизатора. Шифрування даних маршрутизації захищає вміст таблиці маршрутизації від маршрутизаторів, що не мають пароля та облікових даних. Протокол RiPv2 має механізм аутентифікації, а RiPv1 – не має.

Незважаючи на безліч удосконалень протоколу RiPv2, він не є зовсім іншим протоколом. Протокол RiPv2 має багато функцій RiPv1, наприклад:

– метрику числа переходів;

– максимальне число переходів, рівне 15;

– TTL, рівне 16 переходам;

– стандартний інтервал відновлення, рівний 30 секундам;

– заборона маршруту, зворотна заборона, поділ горизонту та утримання для уникнення петель;

– оновлення за допомогою UDP-порту 520;

– адміністративна відстань, рівна 120;

– заголовок повідомлення, що вміщує до 25 маршрутів без аутентифікації.

При запуску маршрутизатора кожен інтерфейс, налаштований для роботи з протоколом RIP, відправляє повідомлення-запит. Це повідомлення запитує у всіх сусідів, що працюють по протоколу RIP, відправку повних таблиць маршрутизації. Сусіди, що працюють по протоколу RIP, відправляють повідомлення-відповідь з відомими записами про мережу. Маршрутизатор, отримавши це повідомлення, оцінює кожен маршрут, виходячи з наступних умов:

– якщо запис маршруту новий, маршрутизатор встановлює маршрут у таблиці маршрутизації;

– якщо маршрут уже є в таблиці, а запис надійшов з іншого джерела, існуючий запис буде замінено в таблиці маршрутизації, якщо кількість переходів у новому записі краща;

– якщо маршрут уже є в таблиці і запис надійшов з того ж джерела, існуючий запис буде замінено, навіть якщо метрика не краща.

Запущений маршрутизатор потім відправляє поновлення при включенні з усіх інтерфейсів, що працюють по протоколу RIP і мають свої таблиці маршрутизації. Сусідів, що працюють по протоколу RIP, повідомляють про нові маршрути.

За умови, що маршрутизатори відправляють і обробляють належні версії оновлень маршрутів, протоколи RiPv1 і RiPv2 цілком сумісні. За замовчуванням протокол RiPv2 відправляє та отримує оновлення тільки версії 2. Якщо в мережі необхідно використовувати обидві версії протоколу RIP, адміністратор мережі налаштовує протокол RiPv2 для відправлення та отримання версій 1 і 2. За замовчуванням RiPv1 відправляє відновлення версії 1, а отримує версії 1 і 2.

Налаштування протоколу RiPv2

Перед налаштуванням RiPv2 необхідно призначити IP-адреси та маски всім інтерфейсам, задіяним у маршрутизації. При необхідності потрібно задати тактову частоту для послідовних каналів. Після завершення базового налаштування налаштовується протокол RiPv2.

Базове налаштування RiPv2 складається з трьох команд:

Router(config)#router rip – включення протоколу маршрутизації.

Router(config)#version 2 – визначення версії.

Router(config-router)#network [адреса мережі] – визначення всіх безпосередньо підключених мереж, яким потрібно повідомлення протоколом RIP.

За замовчуванням протокол RiPv2 буде підсумовувати всі мережі, які потрібно оголосити, по своїй класовій границі.

Для оголошень RiPv2 можна задати аутентифікацію.

Протокол RiPv2 поширює маршрут за замовчуванням сусіднім маршрутизаторам разом з оновленнями маршрутів. Для цього потрібно створити маршрут за замовчуванням і додати команду redistribute static у конфігурацію RiPv2

При використанні протоколу RIP може виникнути ряд проблем, пов’язаних із продуктивністю і безпекою. Перша проблема стосується точності таблиці маршрутизації.

Обидві версії протоколу RIP автоматично підсумовують підмережі на межі класу. Це означає, що протокол RIP розпізнає підмережі, як єдину мережу класу A, B чи C. У корпоративних мережах звичайно використовується безкласова IP-адресація і кілька підмереж, деякі з них не зв'язані між собою, у результаті чого утворються несуміжні підмережі.

На відміну від RiPv1, у протоколі RiPv2 функцію автоматичного підсумовування можна відключити. Якщо функція відключена, RiPv2 буде повідомляти про всі підмережі за рахунок використання мережевої маски. Це необхідно для забезпечення точності таблиці маршрутизації. З цією метою в конфігурацію RiPv2 потрібно додати команду no auto-summary.

Router(config-router)#no auto-summary

Інша проблема – широкомовний режим оновлень RIP. Як тільки конфігурація RIP видає команду network для тієї чи іншої мережі, протокол RIP відразу ж починає відправку повідомлень з усіх інтерфейсів, що входять у цю мережу. Ці оновлення можуть бути потрібні не на всіх ділянках мережі. Наприклад, інтерфейс локальної мережі Ethernet передає ці оновлення всім пристроям у своєму мережевому сегменті, що створює недоречний трафік. Оновлення маршрутів також може бути перехоплено будь-яким пристроєм, що робить мережу вразливою.

Команда passive-interface, відправлена в режимі інтерфейсу, відключає оновлення маршрутів у визначених інтерфейсах.

Router(config-router)#passive-interface тип_інтерфейсу номер_інтерфейсу

У складних корпоративних мережах, в яких задіяно більше одного протоколу маршрутизації, команда passive-interface визначає маршрутизатори для повідомлення про маршрути RIP. При обмеженні кількості інтерфейсів, що сповіщають про маршрути RIP, підвищується безпека і посилюється контроль над трафіком.

Мережі, яка використовує протокол RIP, потрібно час для конвергенції. Поки не будуть оновлені всі маршрутизатори і в них не буде того ж представлення мережі, деякі з них можуть містити в таблицях маршрутизації недопустимі маршрути.

Помилки у відомостях про мережу можуть викликати у оновленнях маршрутів і трафіку петлі, що ведуть до нескінченної передачі пакету між маршрутизаторами. У протоколі маршрутизації RIP встановлено обмеження на максимальне число переходів – 16.

Механізми уникнення петель маршрутизації протоколу RIP

Петлі маршрутизації негативно позначаються на продуктивності мережі. У протоколі RIP передбачено кілька функцій для усунення цієї проблеми. Ці функції часто поєднуються:

– зворотна заборона (poisoned reverse);

– поділ горизонту (split horizon);

– таймер утримання (holddown timer);

– оновлення при включенні (triggered updates).

Зворотна заборона визначає для метрики маршруту значення 16, і він стає недосяжний. Оскільки протокол RIP визначає нескінченність як 16 переходів, мережа понад 15 переходів недосяжна. Якщо мережа стає неактивною, маршрутизатор змінює метрику для цього маршруту на 16, щоб для всіх інших маршрутизаторів вона була недосяжною. Ця функція запобігає відправленню інформації протоколом маршрутизації по заборонених маршрутах.

Протипетлева функція в протоколі RIP збільшує його стабільність, але збільшує і час конвергенції.

Поділ горизонту запобігає утворенню петель. При передачі декількома маршрутизаторами один одному тих самих маршрутів у мережі можуть утворюватися петлі маршрутизації. Поділ обрію вимагає, щоб маршрутизатор, який отримує інформацію маршрутизації для інтерфейсу, не міг відправити оновлення для тієї ж мережі з цього ж інтерфейсу.

Таймер утримання стабілізує маршрути. Таймер утримання відмовляється приймати оновлення маршрутів з більшою метрикою для тієї ж мережі призначення на період, коли маршрут стає неактивним. Якщо протягом періоду утримання, вихідний маршрут знову стає

активним чи маршрутизатор отримує інформацію про маршрут з нижчою метрикою, маршрутизатор встановлює маршрут у таблиці маршрутизації і негайно починає ним користуватися.

Час утримання за замовчуванням дорівнює 180 секундам, у шість разів більше стандартного періоду оновлення. Значення за замовчуванням можна змінити. Однак, будь-який період утримання збільшує час конвергенції і негативно позначається на продуктивності мережі.

Маршрутизація за допомогою протоколу EIGRP

Протокол маршрутизації на основі векторів відстані простий у налаштуванні і вимагає мінімальну кількість ресурсів маршрутизаторів для роботи.

Однак спрощена метрика числа переходів, яка використовується протоколом RIP – це не найточніший спосіб визначення оптимального шляху в складних мережах. Крім того, через обмеження протоколу RIP у 15 переходів, віддалені мережі можуть буи недосяжними.

Протокол RIP виконує періодичні оновлення таблиці маршрутизації, займаючи смугу пропускання, навіть, якщо змін у мережі не було. Маршрутизатори повинні прийняти й обробити ці оновлення, щоб визначити, чи містять вони інформацію про оновлені маршрути.

Переданим від маршрутизатора до маршрутизатора оновленням потрібен час, щоб досягти всіх областей мережі. У результаті маршрутизатори можуть мати у своєму розпорядженні неточне уявлення про мережу. Через великий час конвергенції можуть утворюватися петлі маршрутизації, витрачаючи дорогоцінну пропускну здатність.

Перераховані властивості обмежують застосування протоколу маршрутизації RIP у корпоративному середовищі.

Обмеження RIP протоколу привели до розробки більш удосконалених протоколів з підтримкою VLSM і CIDR, легкою масштабованістю та малим часом конвергенції в складних корпоративних мережах.

Компанія Cisco розробила власний протокол маршрутизації на основі векторів відстані – протокол EIGRP (Enhanced Interior Gateway Routing Protocol). Він наділений розширеними можливостями, що усувають багато обмежень інших протоколів на основі векторів відстані. Крім ряду функцій, спільних з протоколом RIP, протокол EIGRP має багато удосконалених можливостей.

Незважаючи на відносно просте налаштування EIGRP, його функції і параметри носять складний характер. У нього входить безліч функціональних можливостей, що раніше не зустрічалися в жодному іншому протоколі маршрутизації. В силу всіх цих факторів протокол EIGRP – оптимальний вибір для великих багатопротокольних мереж, в яких, в основному, використовуються пристрої компанії Cisco.

Двома основними задачами протоколу EIGRP є забезпечення безпетлевої маршрутизації та швидкої конвергенції. Протокол EIGRP використовує відмінний від протоколу RIP спосіб розрахунку оптимального маршруту. EIGRP використовує складену метрику, яка, головним чином, базується на пропускній здатності та затримці. У порівнянні з числом переходів ця метрика більш точна у визначенні відстані до мережі призначення.

Алгоритм дифузійного відновлення (DUAL), який використовується у протоколі EIGRP, гарантує відсутність петель при розрахунку маршрутів. Коли в топології мережі відбувається зміна, алгоритм DUAL одночасно синхронізує всі пов’язані маршрутизатори. Завдяки цьому, адміністративна відстань для протоколу EIGRP рівна 90, а для протоколу RIP – 120. Менше значення відображає збільшення надійності протоколу EIGRP і підвищення точності метрики. Якщо маршрутизатор отримує маршрути до тієї ж адреси призначення і від RIP, і від EIGRP, він віддасть перевагу маршруту, визначеному протоколом EIGRP.

Протокол EIGRP позначає маршрути, отримані по іншому протоколу маршрутизації, як зовнішні. Оскільки інформація, яка використовується для розрахунку цих маршрутів, менш надійна, ніж метрика EIGRP, маршрутам привласнюється більша адміністративна відстань.

Протокол EIGRP – вдалий вибір для складних корпоративних мереж, в яких, в основному, використовуються маршрутизатори компанії Cisco. Максимальне число переходів протоколу, рівне 255 і дозволяє підтримувати великі мережі. Протокол EIGRP

може відображати більше однієї таблиці маршрутизації, оскільки він може збирати і зберігати дані маршрутизації для різних протоколів маршрутизації, наприклад, для IP і IPX. У таблиці маршрутизації EIGRP відображаються маршрути, отримані як всередині, так і зовні локальної системи.

На відміну від інших протоколів на основі векторів відстані протокол EIGRP не відправляє повні таблиці у формі своїх оновлень. EIGRP виконує багатоадресне розсилання часткових оновлень, що стосуються конкретних змін, тільки тим маршрутизаторам, яким ця інформація необхідна, а не всім маршрутизаторам області. Ці оновлення називаються частковими оновленнями, оскільки відображають конкретні параметри.

Замість відправлення періодичних оновлень маршрутів протокол EIGRP відправляє невеликі пакети-вітання для оновлення даних про своїх сусідів. Завдяки малому розміру та частковим оновленням зберігається пропускна здатність і при тому оновлюється інформація про мережу.

Термінологія і таблиці протоколу EIGRP

З метою збереження даних про мережу з оновлень і забезпечення швидкої конвергенції, протокол EIGRP веде ряд таблиць. Маршрутизатори EIGRP розміщують дані про маршрути і топології в ОЗП для забезпечення швидкості відгуку на зміни. Протокол EIGRP веде три взаємозалежні таблиці:

– таблицю сусідів;

– таблицю топології;

– таблицю маршрутизації.

Таблиця сусідів

Таблиця сусідів формує список, що містить дані про безпосередньо підключені сусідні маршрутизатори. EIGRP реєструє адресу виявленого сусіда і підключеного до нього інтерфейсу.

Коли сусід відправляє пакет вітання, він повідомляє про час утримання. Час утримання – проміжок часу, протягом якого маршрутизатор вважає сусіда досяжним. Якщо, протягом часу утримання, пакет-вітання не отриманий, відлік таймера завершується, і алгоритм DUAL виконує перерахунок топології.

Оскільки швидкість конвергенції залежить від точності даних про сусідів, ця таблиця вкрай важлива для роботи протоколу EIGRP.

Таблиця топології

Таблиця топології представляє, у вигляді списку, всі маршрути, отримані від кожного EIGRP-сусіда. Алгоритм DUAL отримує дані з таблиць сусідів і топологій та розраховує найбільш вигідні маршрути до кожної з мереж.

У таблиці топології визначаються до чотирьох основних безпетлевих маршрутів до адреси призначення. Ці кращі маршрути (successor route) відображаються в таблиці маршрутизації. Протокол EIGRP може розподіляти навантаження, тобто відправляти пакети за адресою призначення з допомогою декількох шляхів. Розподіл навантаження виконується за допомогою кращих маршрутів, що одночасно можуть бути з рівною вартістю і з нерівною вартістю. Ця функція дозволяє уникнути перевантаження пакетами того чи іншого маршруту.

Резервні маршрути, названі можливими спадкоємцями (feasible successor), відображаються в таблиці топології, але відсутні в таблиці маршрутизації. Якщо не діє основний маршрут, кращим маршрутом стає можливий спадкоємець. Це заміщення відбувається за умови, що оголошена відстань feasible successor менша допустимої відстані поточного successor до адреси призначення.

Таблиця маршрутизації

Якщо в таблиці топології розміщені дані про безліч різних маршрутів до мережі призначення, то в таблиці маршрутизації відображаються тільки оптимальні маршрути, які називаються кращими маршрутами (successor route).

Протокол EIGRP відображає інформацію про маршрути двома способами:

– у таблиці маршрути, отримані по протоколу EIGRP, позначаються символом D;

– EIGRP позначає динамічні і статичні протоколи, отримані від інших протоколів або не з мережі EIGRP, як D EX, або зовнішні, оскільки вони надійшли не від маршрутизаторів EIGRP цієї ж автономної системи.

Сусіди і суміжники EIGRP

Щоб протокол EIGRP зміг обмінюватись пакетами між маршрутизаторами, йому необхідно спочатку знайти своїх сусідів. Сусіди EIGRP – це інші маршрутизатори, що працюють по протоколу EIGRP у безпосередньо підключених мережах із загальним доступом.

Маршрутизатори EIGRP використовують пакети вітань для виявлення сусідів і встановлення примикань із сусідніми маршрутизаторами. За замовчуванням у каналах зі швидкістю більше T1 відбувається багатоадресна розсилка пакетів-вітань через кожні 5 секунд, а в каналах зі швидкістю T1 і менше – через кожні 60 секунд.

В IP-мережах адресою багатоадресної розсилки є 224.0.0.10. У пакет-вітання входять: інформація про інтерфейси маршрутизаторів і адреси інтерфейсів. Маршрутизатор EIGRP вважає, що поки надходять пакети-вітання від сусіда, сусід і його маршрути досяжні.

Час утримання – це період очікування протоколом EIGRP пакету-вітання. Звичайний час утримання в три рази більший від інтервалу вітання. Після закінчення часу утримання, алгоритм DUAL виконує перерахунок топології та оновлює таблицю маршрутизації.

Дані, виявлені за допомогою протоколу вітання, надходять у таблицю сусідів. У рядку з порядковим номером записується кількість останніх отриманих вітань від кожного сусіда і встановлюється мітка часу в момент надходження пакету-вітання.

Після встановлення сусідства протокол EIGRP використовує пакети різних типів для обміну і відновлення даних у таблицях маршрутизації. Сусіди отримують повідомлення про нові, недосяжні та знову виявлені маршрути шляхом обміну цими пакетами:

– підтвердження;

– оновлення;

– запит;

– відповідь.

При втраті маршруту він переходить в активний стан, а алгоритм DUAL виконує пошук нового маршруту до адреси призначення. Після виявлення маршруту він розміщується в таблиці маршрутизації і переходить у пасивний стан.

За допомогою цих пакетів алгоритм DUAL збирає дані, необхідні для розрахунку оптимального маршруту до мережі призначення.

Пакет підтвердження означає отримання пакету-оновлення або запиту відповіді. Пакети підтверджень – це невеликі пакети-вітання без даних. Ці типи пакетів завжди одноадресні.

Пакет-оновлення відправляє дані про топологію мережі своєму сусіду. Цей сусід оновлює свою таблицю топології. Для відправлення всіх даних про топологію новому сусіду іноді потрібно відправити кілька пакетів оновлення.

Кожного разу, коли алгоритм DUAL переводить маршрут в активний стан, маршрутизатор має відправити пакет запиту всім сусідам. Сусіди у свою чергу повинні відправити відповідь, навіть, якщо в ній буде зазначено, що про адресу призначення інформації немає. Дані кожного пакету-відповіді дозволяють алгоритму DUAL знайти кращий маршрут до мережі призначення. Запити можуть бути багатоадресними та одноадресними. Відповіді завжди одноадресні.

Пакети EIGRP використовують або TCP, або UDP протокол. Пакети оновлення, запиту і відповіді використовують службу типу TCP, а підтвердження і пакети-вітання – службу типу UDP.

Будучи протоколом маршрутизації, EIGRP функціонує незалежно від мережевого рівня. Компанія Cisco розробила власний протокол четвертого рівня – надійний транспортний протокол (RTP – Reliable Transport Protocol). RTP гарантує доставку та отримання пакетів EIGRP для всіх протоколів мережевого рівня. Оскільки у великих складних мережах може використовуватися ряд протоколів мережевого рівня, цей протокол забезпечує гнучкість і масштабованість EIGRP.

RTP можна використовувати одночасно і як транспортний протокол з гарантованою доставкою, і як транспортний протокол з негарантованою доставкою, подібно TCP і UDP. При RTP з гарантованою доставкою отримувач повинен відправити відправнику пакет підтвердження. Пакети оновлення, запиту і відповіді відправляються в режимі гарантованої доставки, а пакети-вітання і підтвердження – у режимі негарантованої доставки і не вимагають підтвердження. RTP використовує як одноадресні, так і багатоадресні пакети. Багатоадресні пакети EIGRP використовують зарезервовану адресу багатоадресної розсилки 224.0.0.10.

Кожен протокол мережевого рівня працює через протокол-залежний модуль (PDM – Protocol Dependent Module), відповідальний за конкретну задачу маршрутизації. Усі модулі PDM ведуть три таблиці. Наприклад, у маршрутизатора, на якому запущені IP, IPX і AppleTalk, є три таблиці сусідів, три таблиці топології і три таблиці маршрутизації.

Метрики і конвергенція протоколу EIGRP

Для визначення кращого маршруту до адреси призначення EIGRP використовує складене значення метрики. Ця метрика визначається на основі наступних значень:

– смуга пропускання;

– затримка;

– надійність;

– навантаження.

Ще одне значення – максимальний розмір переданого блоку даних (MTU) – входить у оновлення маршрутів, але не є метрикою маршрутизації.

У формулу складеної метрики входять коефіцієнти K: з K1 до K5.

За замовчуванням для K1 і K3 установлюється значення 1, а для K2, K4 і K5 – 0. Коефіцієнт 1 означає, що пропускна здатність і затримка мають однакову вагу при розрахунку складеної метрики.

Пропускна здатність

Метрика пропускної здатності є статичним значенням, відображається у Кбіт/с. У більшості серійних інтерфейсів значення пропускної здатності за замовчуванням дорівнює 1544 Кбіт/с. Ця метрика відображає пропускну здатність підключення T1.

Іноді значення пропускної здатності може не відображати фактичну фізичну пропускну здатність інтерфейсу. Пропускна здатність впливає на розрахунок метрики і, як наслідок, на вибір шляху EIGRP. Якщо в з'єднання з пропускною здатністю 56 Кбіт/с надходить повідомлення зі значенням 1544 Кбіт/с, воно може негативно позначитися на конвергенції, оскільки необхідно буде перебороти навантаження трафіку.

Іншими метриками, що використовує EIGRP для розрахунку вартості каналу, є затримка, надійність і навантаження.

Метрика затримки – статичне значення на основі типу вихідного інтерфейсу. Значення за замовчуванням дорівнює 20 000 мікросекунд для серійних інтерфейсів і 100 мікросекунд для інтерфейсів Fast Ethernet.

Метрика затримки не відображає фактичну кількість часу, що затрачають пакети, щоб досягти адреси призначення. При зміні значення затримки, пов'язаного з визначеним інтерфейсом, змінюється метрика, але це не має фізичного впливу на мережу.

Метрика надійності означає частоту помилок у каналі. На відміну від затримки метрика надійності оновлюється автоматично в залежності від умов каналу. Її значення дорівнює від 0 до 255. Надійність, рівна 255/255, показує канал зі стовідсотковою надійністю.

Навантаження відображає об'єм трафіку в каналі. Менше значення навантаження переважає високе. Наприклад, значення 1/255 означає канал з мінімальним навантаженням, а 255/255 – канал, завантажений на 100%.

У таблиці топології EIGRP метрики використовуються для розрахунку значень можливої відстані (FD) і оголошеної (AD) або заявленої відстані (RD). Алгоритму DUAL ці значення необхідні для визначення кращих шляхів і можливих спадкоємців (successors and feasible successors).

Можлива відстань (Feasible distance) – це краща метрика EIGRP по шляху до адреси призначення від маршрутизатора.

Оголошена відстань (Advertised distance) – це краща метрика, отримана від сусіднього маршрутизатора.

Безпетлевий маршрут з найменшою можливою відстанню стає кращим маршрутом (successor route). Можлива наявність декількох кращих маршрутів до адреси призначення в залежності від фактичної топології. Можливим спадкоємцем (feasible successor) є маршрут, оголошена відстань якого менша можливої відстані кращого маршруту.

Алгоритм DUAL виконує конвергенцію відразу ж після зміни топології. Алгоритм DUAL зберігає можливих спадкоємців у таблиці топології і відправляє в таблицю маршрутизації кращого з них, як кращий маршрут. При відсутності можливих спадкоємців вихідний маршрут переходить в активний режим, і відправляються запити на пошук нового спадкоємця.

Впровадження протоколу EIGRP

Налаштування протоколу EIGRP

Налаштування базового EIGRP відносно просте. Його налаштування багато в чому повторює протокол RiPv2.

Щоб почати процес маршрутизації EIGRP, використовуються два кроки.

Крок 1

Включити процес маршрутизації EIGRP.

Для включення процесу EIGRP необхідний параметр автономної системи. Цьому параметру AS можна призначити будь-яке 16-розрядне значення, і він визначає всі маршрутизатори однієї організації. Незважаючи на те, що EIGRP розглядає параметр, як номер автономної системи, він фактично виступає в ролі ідентифікатора процесу. Цей номер AS має тільки локальне значення і відрізняється від номера автономної системи, який видається і контролюється Комітетом з цифрових адрес в Інтернет (IANA –Internet Assigned Numbers Authority).

Номер AS у команді повинен збігатися для всіх маршрутизаторів, що беруть участь у процесі маршрутизації EIGRP.

Крок 2

Оголосити мережі, про які потрібно передати інформацію.

Команда network вказує протоколу EIGRP, які мережі та інтерфейси беруть участь у процесі EIGRP.

Щоб налаштувати EIGRP для передачі інформації лише про деякі підмережі, потрібно додати шаблонну маску (wildcard mask) після номеру мережі. Щоб визначити шаблонну маску, потрібно відняти мережеву маску з 255.255.255.255.

У деяких версіях Cisco IOS замість шаблонної маски можна вказати маску підмережі. Навіть при використанні звичайної маски, шаблонна маска буде відображена у вихідних даних команди show running-config.

Стандартну базову конфігурацію EIGRP завершують дві додаткові команди.

Команда eigrp log-neighbor-changes додається для перегляду змін сусідів. Ця функція дозволяє адміністраторам відслідковувати стабільність мережі EIGRP.

Для послідовних каналів, що не відповідають пропускній здатності EIGRP у 1,544 Мбіт/с, варто додати команду bandwidth з вказанням фактичної швидкості каналу (у Кбіт/с). Неточне задання пропускної здатності ускладнює вибір оптимального маршруту.

Після включення EIGRP усі маршрутизатори, налаштовані для роботи з EIGRP та заданим правильним номером автономної системи, працюють по EIGRP. Це означає, що маршрутизатори з іншою інформацією про маршрутизацію можуть негативно впливати і навіть зашкодити таблицям маршрутизації. Щоб цього уникнути, можна включити аутентифікацію в конфігурації EIGRP. Після налаштування аутентифікації маршрутизатор перевіряє достовірність джерела оновлень маршрутів перед тим, як їх прийняти.

Для аутентифікації EIGRP потрібно мати ключ. Протокол EIGRP дозволяє адміністраторам керувати ключами через ланцюжок ключів. Налаштування аутентифікації

EIGRP складається з двох кроків: створення ключа і включення аутентифікації з його використанням.

Створення ключа

Щоб створити ключ, потрібно виконати такі команди.

key chain ім’я ланцюжка

– команда глобального налаштування.

– вказується ім’я ланцюжка ключів і введення для неї режиму налаштування.

key ідентифікатор ключа

– визначення номеру ключа і введення режиму налаштування для цього ідентифікатору ключа.

key-string текст

– вказання рядка ключа або паролю. Це налаштування має збігатися у всіх маршрутизаторів EIGRP.

Включення аутентифікації

Ключ служить для включення аутентифікації MD5 для EIGRP за допомогою таких команд налаштування інтерфейсу:

ip authentication mode eigrp md5

– вказує на необхідність аутентифікації MD5 для обміну пакетами EIGRP.

ip authentication key-chain eigrp ім’я_ланцюжка AS

– AS позначає автономну систему конфігурації EIGPR.

Параметр імені ланцюжка вказує ланцюжок ключів, які були налаштовані раніше.

Підсумовування маршрутів EIGRP

Як і протокол RIP, EIGRP автоматично підсумовує на межі класу мережі з наявністю підмереж. Для сумарного маршруту EIGRP створює тільки один запис у таблиці маршрутизації. З сумарним маршрутом пов’язується оптимальний маршрут, або кращий маршрут (successor route). В результаті весь трафік, призначений для підмереж, надходить по цьому єдиному шляху.

У корпоративній мережі обраний шлях до сумарного маршруту може бути не оптимальним для трафіку, призначеного для тієї чи іншої окремої підмережі. Маршрутизатори можуть знайти оптимальні маршрути до кожної з окремих підмереж, тільки отримавши від сусідів інформацію про ці підмережі.

Якщо відключене підсумовування за замовчуванням, то оновлення будуть містити інформацію про підмережі. У таблиці маршрутизації будуть встановлені записи для кожної підмережі, а також запис для сумарного маршруту. Сумарний маршрут називається батьківським маршрутом, а маршрути підмереж – дочірніми маршрутами.

Для всіх батьківських маршрутів у таблиці маршрутизації EIGRP встановлює сумарний маршрут Null0. Інтерфейс Null0 означає, що це не фактичний маршрут, а деяке підсумовування з метою передачі даних про маршрутизацію. Якщо пакет відповідає одному з дочірніх маршрутів, він направляється з відповідного інтерфейсу. Якщо пакет відповідає сумарному маршруту і не відповідає жодному з дочірніх, він буде відхилений.

При використанні підсумовування за замовчуванням розміри таблиць маршрутизації скорочуються. Якщо підсумовування відключити, то розміри оновлень і таблиць будуть збільшуватися. Необхідність автоматичного підсумовування визначається, виходячи із загальної продуктивності мережі і моделей трафіку.

Для відключення підсумовування за замовчуванням, використовується команда no auto-summary.

Якщо автоматичне підсумовування відключити, то буде надходити інформація про всі підмережі. Адміністратор може зіштовхнутися із ситуацією, коли одним підмережам підсумовування необхідне, а іншим - непотрібне. Рішення про підсумовування приймається, виходячи з розташування підмереж. Наприклад, ізольовані підмережі, підключені до одного маршрутизатора, підходять для підсумовування.

Підсумовування вручну покращує керування маршрутами EIGRP. За допомогою цієї функції адміністратор визначає, які підмережі і на яких інтерфейсах повідомляти сумарними маршрутами.

Підсумовування вручну виконується на рівні інтерфейсу і наділяє адміністратора всією повнотою керування. Підсумований вручну маршрут відображається в таблиці маршрутизації у вигляді маршруту EIGRP на основі логічного (не фізичного) інтерфейсу:

D 192.168.0.0/22 is a summary, Null0

Перевірка роботи протоколу EIGRP

Незважаючи на відносну простоту налаштування протоколу EIGRP, він використовує складні технології, щоб перебороти обмежені можливості протоколів маршрутизації на основі векторів відстані. Щоб правильно перевірити, знайти та усунути помилки в конфігурації мережі, що працює по протоколу EIGRP, важливо розуміти ці технології. У число доступних команд перевірки входять такі команди.

show ip protocols

– Перевіряє, чи оголошені протоколом EIGRP відповідні мережі.

– Відображає номер автономної системи та адміністративну відстань.

show ip route

– Перевіряє наявність отриманих маршрутів EIGRP у таблиці маршрутизації.

– Позначає маршрути EIGRP символами D чи D EX.

– Відображає для внутрішніх маршрутів адміністративну відстань за замовчуванням, рівну 90.

show ip eigrp neighbors detail

– Перевіряє суміжні EIGRP форми.

– Відображає IP-адреси та інтерфейси сусідніх маршрутизаторів.

show ip route

– Відображає кращі маршрути і всіх можливих спадкоємців (successors and all feasible successors).

– Відображає можливу та оголошену відстань (feasible distance and reported distance).

show ip eigrp interfaces detail

– Перевіряє інтерфейси, що використовують EIGRP.

show ip eigrp traffic

– Відображає кількість і типи EIGRP пакетів, що відправляються та отримуються.

Однієї з основних задач цих команд show є перевірка правильності утворення EIGRP adjacencies і обміну пакетами EIGRP між маршрутизаторами. Робота EIGRP неможлива, якщо не сформовано adjacencies, тому їх потрібно перевірити до пошуку й усунення інших помилок.

Якщо з adjacencies все в порядку, а проблеми як і раніше залишаються, адміністратору варто почати пошук і усунення помилок за допомогою команд налагодження для перегляду інформації про роботу EIGRP на маршрутизаторі в режимі реального часу.

debug eigrp packet

– відображає передачу й отримання всіх пакетів EIGRP.

debug eigrp fsm

– відображає активність можливого спадкоємця, щоб визначити стан маршрутів (виявлені, установлені чи видалені протоколом EIGRP).

Операції налагодження вимагають значної пропускної здатності та обчислювальних потужностей маршрутизатора, особливо налагодження дуже складних протоколів типу EIGRP. Ці команди дозволяють визначити джерело втрати маршруту або відсутньої суміжності EIGRP, але продуктивність мережі при використанні таких команд може падати.

Проблеми й обмеження протоколу EIGRP

Хоча протокол маршрутизації EIGRP досить функціональний, проте , має деякі обмеження:

– не працює в середовищах різних провайдерів, оскільки є власним протоколом компанії Cisco;

– найоптимальніше функціонує в мережах плоского типу;

– у маршрутизаторів повинна збігатися автономна система, і його неможливо розділити на групи;

– може створювати дуже великі таблиці маршрутизації, що вимагають великих пакетів оновлень і пропускної здатності;

– використовує більший об’єм пам’яті та обчислювальних ресурсів у порівнянні з протоколом RIP;

– працює ефективно, якщо не змінювати параметри за замовчуванням;

– для його обслуговування необхідні адміністратори з поглибленими технічними знаннями.

Протокол EIGRP забезпечує оптимальну маршрутизацію на основі векторів відстані, використовуючи додаткові функції, звичайно характерні для протоколів маршрутизації на основі стану каналів, у тому числі, обмежені оновлення і суміжності сусідів. Для успішного впровадження багатьох функцій протоколу EIGRP потрібно ретельне налаштування, моніторинг, пошук і усунення помилок.

Основним питанням безпеки корпоративних мереж є баланс між двома важливими вимогами: необхідністю відкрити мережі для розвитку бізнес-можливостей та необхідністю захисту приватної, особистої та стратегічної бізнес-інформації.

Застосування ефективної політики безпеки є найбільш важливим кроком, який організація може зробити для захисту своєї мережі. Вона містить рекомендації про заходи, які будуть проводитися, та ресурси, які будуть використовуватися для захисту корпоративної мережі.

Значення та розміри комп’ютерних мереж швидко зростають в часі. Якщо не забезпечується безпека мережі, то це може мати дуже серйозні наслідки, такі як втрата конфіденційності, крадіжка інформації, несанкціонований доступ до ресурсів. Типи потенційних загроз для безпеки мережі постійно розвиваються, що ускладнює питання безпеки.

Розвиток електронного бізнесу, мобільної комерції та безпровідних мереж вимагає інтегрованих та гнучких рішенн безпеки, оскільки інструменти та методи мережевих атак також швидко розвиваються. Наприклад, в 1985 році зловмисник повинен був мати складний комп’ютер, мати знання програмування і мереж, щоб використовувати елементарні засоби та основні атаки. Проте, з часом методи та інструменти атак вдосконалювались, і сьогодні зловмисникам не потрібен такий же рівень складності знаннь. Люди, які раніше не брали участі в комп’ютерних злочинах, в даний час взмозі це зробити

Маршрутизація на основі стану каналу

На відміну від протоколів вектора відстані протоколи маршрутизації типу стану каналу можуть створити “повну картину”, або топологію мережі шляхом збору інформації від усіх інших маршрутизаторів.

Протоколи стану каналу використовують інформацію про стан каналу для створення топологічної карти та вибору найкращого шляху до всіх мереж призначення в топології.

Протоколи стану каналу не використовують періодичні оновлення. Після того, як наступила конвергенція мережі, оновлення надсилається тільки тоді, коли відбувається зміна в топології.

Корпоративні мережі і провайдери використовують протоколи на базі стану каналу, що пов’язано з їх ієрархічною структурою та можливістю масштабування для великих мереж. Протоколи маршрутизації на основі векторів відстаней не є правильним вибором для складної корпоративної мережі.

Протоколи маршрутизації на основі стану каналу, також відомі, як протоколи найкоротшого шляху побудовані на використанні алгоритму Дейкстри (Edsger Dijkstra’s shortest path first (SPF) algorit). До них належать:

– Open Shortest Path First (OSPF);

– Intermediate System-to-Intermediate System (IS-IS).

Алгоритм Дейкстри, або алгоритм коротшого шляху враховує вартість кожної ділянки шляху від відправника до отримувача.

Кожен маршрутизатор визначає вартість до кожного пункту призначення. Іншими словами, кожен маршрутизатор обчислює алгоритм SPF та визначає вартість із своєї власної точки зору.

Принцип роботи протоколів стану каналу такий:

1. Кожен маршрутизатор дізнається про свої безпосередньо підключені мережі. Це здійснюється завдяки виявленню, що інтерфейс знаходиться в активному стані.

2. Кожен маршрутизатор, несе відповідальність за роботу зі своїми сусідами з безпосередньо під'єднаних мереж. Як і в EIGRP, маршрутизатори стану каналу обмінюються пакетами-вітаннями з іншими маршрутизаторами, які підтримують протокол стану каналу.

3. Кожен маршрутизатор створює LSP пакет (Link-State Packet), що містить стан кожного безпосередньо під'єднаного каналу. Це здійснюється шляхом запису відповідної інформації про кожного сусіда, у тому числі його ідентифікатор (neighbor ID), тип каналу та пропускну здатність.

4. Кожен маршрутизатор розсилає пакети LSP до всіх сусідів, які зберігають всі отримані LSP в базі даних. Сусіди потім передають LSP пакети своїм сусідам. Таким чином всі маршрутизатори в домені протоколу отримають LSP пакети. Кожен маршрутизатор зберігає копію кожного LSP, отриманого від своїх сусідів у локальній базі даних.

5. Кожен маршрутизатор використовує базу даних, щоб побудувати повну карту топології і обчислити оптимальний шлях до кожної мережі призначення. Алгоритм SPF використовується для побудови карти топології та визначення найкращого шляху до кожної з мереж.

Канал (Link)

В протоколах маршрутизації стану каналу, link – це інтерфейс маршрутизатора. Як і в протоколах вектора відстані та статичній маршрутизації, інтерфейс повинен бути налаштований з правильною IP-адресою та мережевою маскою і повинен бути в піднятому стані, щоб протокол стану каналу міг дізнатися про link.

Стан каналу (Link-State)

Це інформація про стан каналу (link-states). Ця інформація включає в себе:

– IP-адресу інтерфейсу та маску підмережі.

– Тип мережі (Ethernet, Serial point-to-point link).

– Вартість каналу (cost of link).

– Сусідні (neighbor) маршрутизатори.

Протоколи маршрутизації на базі стану каналу мають ряд переваг в порівнянні з протоколами вектора відстані.

Будують топологічну карту.

Протоколи стану каналу створюють топологічну карту, або SPF дерево топології мережі. Протоколи вектора відстані не мають топологічної карти мережі. Маршрутизатори з підтримкою протоколу вектора відстані мають тільки список мереж, який включає в себе вартість (відстань) та маршрутизатори наступного переходу (напрям) до цих мереж. Оскільки протоколи стану каналу обмінюються повідомленнями про стан каналу, алгоритм SPF може побудувати SPF дерево мережі. Використовуючи дерево SPF, кожен маршрутизатор може самостійно визначити найкоротший шлях до будь-якої мережі.

Швидка конвергенція.

Отримавши LSP пакет протоколи стану каналу відразу ж відправляють LSP пакет через всі інтерфейси, крім інтерфейсу, з якого був отриманий LSP пакет. Протоколи вектора відстані повинні обробити кожне оновлення маршрутизації та оновити таблицю маршрутизації перед надсиланням на інші інтерфейси.

Оновлення по події.

Після початкового надсилання LSP, протоколи стану каналу відправляють LSP лише тоді, коли є зміни в топології. LSP містить інформацію лише про змінені стани каналів. Протоколи стану каналу не надсилають періодичних оновлень.

Ієрархічний дизайн.

Протоколи маршрутизації стану каналу використовують концепцію областей, що дозволяє створювати ієрархічний дизайн мереж для агрегації (сумування) маршрутів та ізолювати проблеми маршрутизації в межах однієї області.

Маршрутизація з використанням протоколу OSPF

Принцип роботи протоколу

Протокол OSPF (Open Shortest Path First) – приклад протоколу маршрутизації на базі стану каналу. Протокол OSPF – це відкритий стандарт протоколу маршрутизації, розроблений інженерною групою по розвитку Інтернет (IETF) для підтримки IP-трафіку.

Протокол OSPF є безкласовим протоколом внутрішніх шлюзів (IGP). Він поділяє мережу на різні секції, що називають областями. Даний поділ дає можливість більшого масштабування. Робота з декількома областями дозволяє адміністратору мережі вибірково включати підсумовування маршрутів та ізолювати проблеми з маршрутизацією в межах якої-небудь однієї області.

Протоколи маршрутизації на базі стану каналу, такі як OSPF, не надсилають періодичних розсилань повної таблиці маршрутизації. Замість цього після конвергенції мережі відправлення оновлення протоколом на базі стану каналу здійснюється тільки при якій-небудь зміні в топології мережі, наприклад, при відключенні каналу. Крім цього, кожні 30 хвилин протокол OSPF виконує повне оновлення.

Протоколи маршрутизації на базі стану каналу, такі як OSPF, працюють нормально у великих ієрархічних мережах, де важлива швидка збіжність.

У порівнянні з протоколами векторів відстані, для протоколів маршрутизації по стану каналу потрібно:

– більш складний процес планування і конфігурації мережі;

– збільшені ресурси маршрутизатора;

– більший об’єм пам’яті для збереження великої кількості таблиць;

– більш висока потужність процесора та обчислювальна потужність для складних розрахунків маршрутизації.

Однак при високій обчислювальній потужності маршрутизаторів, доступній в даний час, виконання цих вимог не є складним.

Маршрутизатори, на яких виконуються протоколи RIP, отримують оновлення від маршрутизаторів, що знаходяться в безпосередньому сусідстві, але без докладної інформації про всю мережу. Маршрутизатори, на яких виконуються протоколи OSPF, створюють повну карту мережі зі своєї точки зору. Дана карта дозволяє їм швидко визначати безпетлеві альтернативні маршрути у випадку відмови якого-небудь мережевого каналу.

Протокол OSPF використовує 5 типів LSP пакетів, кожен з яких має певне призначення в процесі роботи маршрутизації OSPF [21]:

1. Hello – Hello пакети використовуються для встановлення та керування суміжними відносинами з іншими OSPF маршрутизаторами.

2. DBD (The Database Description) – пакети містять скорочені списки бази даних стану лінків та використовуються при отриманні машрутизатором для звірки з локальною базою даних.

3. LSR (Link-State Request) – маршрутизатори можуть запитувати додаткову інформацію про записи в DBD шляхом надсилання запиту LSR.

4. LSU (Link-State Update) – пакети використовуються для відповіді на LSR запити, а також для оголошення нової інформації. LSU пакети містять сім типів оголошень LSA (Link-State Advertisements).

5. LSAck (Link-State Acknowledgement) – коли маршрутизатор отримує LSU він надсилає підтвердження про отримання LSAck.

Протокол OSPF не виконує автоматичного підсумовування на границях головної мережі. Крім того, у рішеннях по протоколах OSPF, пропонованих компанією Cisco, для визначення вартості каналу використовується пропускна здатність. Ця метрика вартості використовується протоколом OSPF для визначення найкращого маршруту. Канал з більш високою пропускною здатністю забезпечує нижчу вартість.

Для встановлення найкоротшого шляху маршрутизатор більше довіряє метриці, оснований на пропускній здатності, ніж метриці, оснований на числі переходів. Адміністративна відстань протоколу OSPF дорівнює 110, що менше, ніж для RIP, завдяки точності метрики.

Метрики і конвергенція протоколу OSPF

Протокол OSPF використовує метрику вартості для окремого каналу на основі його пропускної здатності або швидкості. Метрикою для конкретної мережі призначення є сума вартості всіх каналів шляху. Якщо існує кілька шляхів до мережі, кращим є шлях з найменшою вартістю, і він заноситься в таблицю маршрутизації.

Для розрахунку вартості каналу протоколу OSPF використовується рівняння:

вартість = 100 000 000 / пропускна здатність каналу в біт/с.

Значення пропускної здатності для рівняння дає пропускна здатність, що налаштовується в інтерфейсі. Пропускна здатність інтерфейсу визначається командою show interfaces.

При швидкостях каналу 100 Мбіт/с і вище, наприклад, як у каналів Fast Ethernet і Gigabit Ethernet, використання даного рівняння викликає труднощі. Незалежно від різниці у швидкості між цими двома каналами, вони обоє розраховуються до значення 1, тому, незважаючи на розходження цих каналів, вони будуть оброблятися однаково. Щоб це компенсувати, варто налаштувати значення вартості інтерфейсу вручну за допомогою команди ip ospf cost.

У межах однієї області маршрутизатори OSPF повідомляють інформацію про стан своїх з'єднань сусіднім маршрутизаторам. Для оголошення інформації про стан каналів використовуються повідомлення, що називаються оголошеннями про стан каналу (LSA).

Після отримання оголошень LSA з описом усіх каналів у межах відповідної області маршрутизатор OSPF використовує алгоритм SPF (алгоритм Дейкстри) для створення топологічної деревоподібної схеми, або карти мережі. Кожен маршрутизатор, на якому виконується даний алгоритм, визначає себе як кореневий елемент свого власного дерева SPF. Починаючи від кореневого елемента, дерево SPF визначає найкоротший шлях до кожного місця призначення і загальну вартість кожного шляху.

Інформація про дерево SPF зберігається в базі даних топології. Маршрутизатор заносить найкоротший шлях до кожної мережі в таблицю маршрутизації.

Конвергенція досягається, якщо всі маршрутизатори:

– отримають інформацію про кожне місце призначення в мережі;

– оброблять дану інформацію з використанням алгоритму SPF;

– обновлять свої таблиці маршрутизації.

При використанні протоколів OSPF оновлення інформації про стан каналів розсилаються з появою в мережі яких-небудь змін. Але яким чином маршрутизатор може довідатися про відмову сусіднього маршрутизатора? Маршрутизатори OSPF встановлюють і підтримують сусідські відносини, чи відносини суміжності, з іншими маршрутизаторами OSPF, підключеними до мережі. Суміжність – це покращена форма сусідських відносин між маршрутизаторами, що бажають обмінюватися інформацією про маршрутизацію. При ініціації маршрутизаторами відносин суміжності із сусідніми маршрутизаторами починається обмін оновленнями інформації про стан каналів. Маршрутизатори досягають стану суміжності FULL (повний), коли вони мають синхронізовані дані у своїй базі даних станів каналів.

Перед тим, як стати повністю суміжним із сусіднім маршрутизатором, той чи інший маршрутизатор проходить через кілька змін стану.

– Init (ініціація);

– 2-Way (двосторонній режим);

– Exstart;

– Exchange (обмін інформацією);

– Loading (завантаження);

– Full (повний).

У OSPF протокол-вітання використовується для початкового встановлення і ведення відносин суміжності. Протокол-вітання посилає дуже маленькі пакети-вітання до підключеного маршрутизатора OSPF на адресу багатоадресної розсилки 224.0.0.5. Пакети надсилаються кожні 10 секунд по каналах Ethernet і широкомовних каналах, та кожні 30 секунд по не широкомовних каналах. Пакети-вітання також містять у собі налаштування маршрутизатора. Налаштування містять інтервал вітання, паузу, тип мережі, а також тип

аутентифікації і дані аутентифікації, якщо вона налаштована. Для встановлення суміжності між будь-якими двома маршрутизаторами всі налаштування повинні збігатися. Маршрутизатор записує виявлені відносини суміжності між сусідніми маршрутизаторами в базу даних відносин суміжності.

Сусідні маршрутизатори OSPF та відносини суміжності

Стан Full є стандартним для маршрутизатора OSPF. Якщо маршрутизатор тривалий час знаходиться в іншому стані, це вказує на наявність якої-небудь проблеми, наприклад, розбіжності налаштувань. Єдиним виключенням є стан 2-way. У широкомовному оточенні маршрутизатор досягне стану full тільки з призначеним маршрутизатором (DR) і резервним призначеним маршрутизатором (BDR). Всі інші сусідні маршрутизатори будуть відображатися в стані 2-way.

Задачею маршрутизаторів DR і BDR є зниження кількості посилань оновлених даних, непотрібного трафіку і непродуктивних процесів на всіх маршрутизаторах. Це досягається шляхом відправлення на всі маршрутизатори запиту про прийом обновлених даних тільки від маршрутизатора DR. У широкомовних сегментах мережі є тільки по одному маршрутизатору DR і BDR. Всі інші маршрутизатори повинні мати з'єднання з маршрутизатором DR і BDR. При відмові якого-небудь каналу маршрутизатор, що має інформацію про даний канал, посилає інформацію на маршрутизатор DR, використовуючи адресу багатоадресної розсилки 224.0.0.6. Маршрутизатор DR відповідає за розсилання інформації про зміну на всі інші маршрутизатори OSPF за адресою багатоадресної розсилки 224.0.0.5. Крім зниження кількості оновлень, що розсилаються по мережі, цей процес також забезпечує отримання всіма маршрутизаторами однакової інформації в той самий час і з одного джерела.

Маршрутизатор BDR забезпечує відсутність яких-небудь критичних точок. Як і маршрутизатор DR, маршрутизатор BDR спостерігає за адресою 224.0.0.6 і отримує усі оновлення, що посилаються на маршрутизатор DR. При відмові маршрутизатора DR маршрутизатор BDR отримує функції маршрутизатора DR, і призначається новий маршрутизатор BDR. Будь-який маршрутизатор, не обраний як маршрутизатор DR чи BDR, називається маршрутизатором DROther.

Маршрутизатором DR призначається маршрутизатор з найвищим, у межах локальної мережі, ідентифікатором маршрутизатора. Маршрутизатором BDR призначається маршрутизатор з другим по величині ідентифікатором.

Ідентифікатором маршрутизатора є IP-адреса, що визначається таким чином:

1. Значенням, налаштованим з використанням команди router-id.

2. Якщо за допомогою команди router-id не встановлено ніякого значення, то вищою IP-адресою, налаштованою на loopback-інтерфейсі.

3. Якщо відсутній який-небудь налаштований loopback-інтерфейс, то вищою IP-адресою у будь-якому активному фізичному інтерфейсі.

Ідентифікатор маршрутизатора можна переглядати за допомогою наступних show команд:

show ip protocols, show ip ospf та show ip ospf interface.

У деяких випадках адміністратору може знадобитися можливість призначити в ролі маршрутизаторів DR і BDR які-небудь конкретні маршрутизатори. Це можуть бути маршрутизатори з більшою обчислювальною потужністю або з меншим завантаженням трафіку. Адміністратор може примусово призначити маршрутизатори DR і BDR шляхом налаштування пріоритету з використанням команди налаштування інтерфейсу:

ip ospf priority номер

За замовчуванням маршрутизатори OSPF мають значення пріоритету 1. При зміні значення пріоритету на якому-небудь маршрутизаторі, в ролі маршрутизатора DR буде обраний маршрутизатор з вищим налаштованим значенням пріоритету незалежно від вищого ідентифікатора маршрутизатора. Найвищим значенням для налаштування пріоритету маршрутизатора є значення 255. Значення 0 означає, що маршрутизатор не можна вибрати як маршрутизатор DR чи BDR.

Не для всіх типів каналів потрібно маршрутизатор DR чи BDR. Типи каналів, обумовлені протоколом OSPF, містять у собі:

Мережі із широкомовним розсиланням.

– Ethernet.

Мережі «точка-точка» (PPP).

– послідовні;

– T1/E1.

Нешироковомовні мережі множинного доступу (NBMA).

– Frame Relay;

– ATM.

У широкомовних мережах множинного доступу, таких як Ethernet, може з'явитися велике число сусідів, тому потрібно призначати маршрутизатор DR.

У мережах типу точка-точка встановлення відносин повної суміжності не є складним, оскільки, за визначенням, у цих мережах на каналі знаходиться тільки два маршрутизатори. Призначення маршрутизатора DR не є обов'язковим і не виконується.

У мережах NBMA маршрутизатор OSPF може працювати в двох режимах:

– симульоване широкомовне середовище: адміністратор може призначити тип мережі як широкомовний, при цьому мережа імітує широкомовну модель шляхом призначення маршрутизатора DR чи BDR. У даному оточенні звичайно рекомендується, щоб адміністратор вибирав маршрутизатор DR чи BDR шляхом налаштування пріоритету маршрутизатора. Це забезпечує наявність у маршрутизатора DR чи BDR можливості повної передачі даних на всі сусідні маршрутизатори. Сусідні маршрутизатори також визначаються статично за допомогою команди neighbor у режимі налаштування OSPF;

– багатоточкове середовище: у даному середовищі кожна нешироковомовна мережа розглядається як набір двоточкових каналів, при цьому маршрутизатор DR не призначається. Для цього середовища також потрібно, щоб сусідні маршрутизатори призначалися статично.

Області OSPF

Усі мережі OSPF починаються з області 0, яку називають областю магістралі. В міру розширення мережі можуть створюватися інші області, суміжні з областю 0. Цим іншим областям може призначатися будь-який номер до 65535.

Мережа OSPF має двохшарову ієрархічну структуру. Область 0 знаходиться вгорі, а всі інші області розташовані на наступному рівні. Усі немагістральні області повинні прямо з'єднуватися з областю 0. Ця група областей створює автономну систему OSPF (AS).

Процес роботи протоколу OSPF у межах якої-небудь області відрізняється від процесів, що виконуються між цією областю й областю магістралі. Звичайно між областями відбувається підсумовування мережевої інформації. Це дозволяє зменшити розмір таблиць маршрутизації в опорній мережі. За допомогою підсумовування також ізолюються зміни і нестабільності, чи биття, каналів до окремої області в домені маршрутизації. Якщо використовується підсумовування, то при якій-небудь зміні в топології отримують оголошення LSA і виконують алгоритм SPF тільки маршрутизатори, що знаходяться в області, де відбулася зміна.

Маршрутизатор, через який будь-яка область з'єднується з областю магістралі, називається прикордонним маршрутизатором області (ABR). Маршрутизатор, через який яка-небудь область з'єднується з іншим протоколом маршрутизації, таким як EIGRP, статичними маршрутами, які перерозподіляються в області OSPF, називається прикордонним маршрутизатором автономної системи (ASBR).

Впровадження протоколу OSPF

Налаштування протоколу OSPF в одній області [12]

Налаштування базового протоколу OSPF не є складною задачею і складається тільки з двох кроків. Перший крок – включення процесу маршрутизації OSPF. Другий крок – визначення мереж, що повинні бути оголошені.

Крок 1. Включення OSPF

router(config)#router ospf <ідентифікатор процесу>

Ідентифікатор процесу вибирається адміністратором, він може являти собою будь-яке число в діапазоні від 1 до 65535. Ідентифікатор процесу має тільки локальне значення і необов'язково повинен збігатися з ідентифікатором інших маршрутизаторів OSPF.

Крок 2. Оголошення мереж

Router(config-router)#network <адреса мережі> <шаблонна маска> area <ідентифікатор області>

Команда network має таку ж функцію, як в інших протоколах маршрутизації IGP. Цією командою визначаються інтерфейси, що можуть відправляти і приймати пакети OSPF. Дана інструкція визначає мережі, що включаються у оновлення маршрутизації OSPF.

У команді OSPF network використовується сполучення мережевої адреси і шаблонної маски. Мережева адреса, поряд із шаблонною маскою, вказує адресу інтерфейсу, чи діапазон адрес, що буде включений для OSPF.

Ідентифікатор області визначає область OSPF, що належить мережі. Навіть, якщо ніякі області не зазначені, повинна бути присутня яка-небудь область 0. В середовищі OSPF з однією областю, область завжди має ідентифікатор 0.

Команда OSPF network повинна використовувати шаблонні маски. При використанні для підсумовування мереж, чи організації супермереж, шаблонна маска є зворотньою мережевою маскою.

Щоб визначити шаблонну маску для підмережі, потрібно відняти десяткову мережеву маску для інтерфейсу від маски з усіма цифрами 255 (255.255.255.255).

Візьмемо наступний приклад: адміністратор хоче оголосити мережу 10.10.10.0/24 у протоколі OSPF. Маскою мережі для даного інтерфейсу Ethernet буде /24 чи 255.255.255.0. Потрібно відмінусувати маску від маски з усіма цифрами 255 для отримання шаблонної маски.

Отримане вираження OSPF network має вигляд:

Router(config-router)#network 10.10.10.0 0.0.0.255 area 0

Налаштування аутентифікації OSPF

Як і в інших протоколах маршрутизації, при налаштуванні за замовчуванням у протоколі OSPF обмін інформацією між сусідніми маршрутизаторами виконується простим текстом. У зв'язку з цим з'являється можлива загроза безпеці мережі.

Щоб усунути цю можливу проблему безпеки, потрібно налаштувати аутентифікацію OSPF між маршрутизаторами. Коли в якій-небудь області включена аутентифікація, маршрутизатори обмінюються інформацією тільки при співпадінні параметрів аутентифікації.

Використовуючи простий протокол аутентифікації по паролю, потрібно встановити на кожному маршрутизаторі ключ. Даний метод забезпечує тільки безпеку основного рівня, оскільки ключ передається між маршрутизаторами у вигляді простого тексту. Побачити ключ так просто, як і сам текст.

Більш безпечним методом аутентифікації є Message Digest 5 (MD5). При цьому методі на кожному маршрутизаторі необхідні ключ та ідентифікатор ключа. Маршрутизатор використовує алгоритм, за допомогою якого виконується обробка ключа, пакету OSPF та ідентифікатору ключа для створення зашифрованого числа. Зашифроване число міститься в кожному пакеті OSPF. Для отримання даного ключа неможливо використовувати програму перехоплення пакетів, оскільки ключ ніколи не передається.

Налаштування параметрів OSPF

Крім виконання базового налаштування протоколу OSPF потрібно налаштувати деякі його параметри.

Прикладом може служити ситуація, коли потрібно вказати, які маршрутизатори отримають функції маршрутизатора DR і BDR. Ця задача виконується шляхом встановлення пріоритету або інтерфейсу ідентифікатора маршрутизатора.

Маршрутизатор вибирає призначений маршрутизатор на підставі вищого значення кожного з наступних параметрів, у такій послідовності:

1. Пріоритет інтерфейсу. Встановлюється командою priority.
2. Ідентифікатор маршрутизатора. Задається командою OSPF router-id.

3. Вища адреса loopback інтерфейсу. За замовчуванням петлевий інтерфейс з вищою IP-адресою використовується як ідентифікатор маршрутизатора. Протокол OSPF підтримує петлеві інтерфейси, оскільки вони є не фізичними, а логічними. Логічні інтерфейси завжди мають пріоритет.

4. Вища адреса фізичного інтерфейсу. Як ідентифікатор маршрутизатора, маршрутизатор використовує вищу активну IP-адресу одного зі своїх інтерфейсів. Ця можливість викликає проблему, якщо інтерфейси припиняють роботу чи переналаштовуються.

Після зміни ідентифікатора маршрутизатора або пріоритету інтерфейсу, необхідно скинути значення відносин суміжності сусідніх маршрутизаторів. Для цього використовується команда clear ip ospf process. Цією командою вводяться в дію нові значення.

Ще одним параметром, що вимагає зміни, є пропускна здатність. На маршрутизаторах Cisco пропускна здатність більшості послідовних інтерфейсів за замовчуванням установлюється на швидкість 1,544 Мбіт/с, що відповідає швидкості стандарту T1. Значення пропускної здатності визначає вартість каналу, але фактично не впливає на швидкість каналу.

У деяких випадках провайдер послуг надає організації частину каналу T1, наприклад 384 Кбіт/с. Програмне забезпечення IOS робить припущення, що послідовні канали мають пропускну здатність T1, незважаючи на те, що інтерфейс фактично передає та отримує дані тільки зі швидкістю 384 Кбіт/с. Це припущення приводить до неправильного вибору шляху, оскільки протокол маршрутизації вирішує, що канал має більшу швидкість, ніж насправді.

Коли який-небудь послідовний інтерфейс фактично не працює зі швидкістю за замовчуванням T1, його потрібно налаштувати вручну (з обох сторін каналу на однакове значення).

У протоколі OSPF при налаштуванні інтерфейсу з використанням команди bandwidth чи ip ospf cost досягається однаковий результат. За допомогою обох команд вказується точне значення, яке OSPF використовує для визначення оптимального шляху.

Командою bandwidth змінюється значення пропускної здатності, що використовується для розрахунку метрики вартості протоколу OSPF. Щоб змінити вартість інтерфейсу, використовується команда ip ospf cost.

Ще одним параметром, зв’язаним з метрикою вартості OSPF, є еталонна пропускна здатність, що використовується для розрахунку вартості інтерфейсу, яку також називають вартістю каналу.

При розрахунку значення пропускної здатності кожного інтерфейсу використовується рівняння 100 000 000/пропускна здатність. Значення 100 000 000, чи 10^8, називається еталонною пропускною здатністю.

Існує певна складність з більш швидкісними каналами, такими як канали Gigabit Ethernet і 10Gbit Ethernet. Використання еталонної пропускної здатності за замовчуванням 100 000 000 дозволяє отримати інтерфейси зі значеннями пропускної здатності 100 Мбіт/с і вище, а також з однаковою вартістю OSPF зі значенням 1.

Для отримання більш точних розрахунків вартості може виникнути потреба підкоректувати значення еталонної пропускної здатності. Еталонна пропускна здатність змінюється використанням команди OSPF auto-cost reference-bandwidth.

При необхідності, ця команда, використовується на всіх маршрутизаторах, щоб метрика маршрутизації OSPF залишалася єдиною. Нова еталонна пропускна здатність вказується в мегабітах за секунду (Мбіт/с). Щоб встановити еталонну пропускну здатність на швидкість 10 Гбіт/с, використовується значення 10000.

Перевірка роботи протоколу OSPF

Після налаштування протоколу OSPF для перевірки правильності його роботи можна скористатися декількома командами.

Щоб у процесі пошуку та усунення несправностей у мережах OSPF перевірити, чи маршрутизатор створив відношення суміжності із сусідніми маршрутизаторами, використовується команда show ip ospf neighbor.

Якщо ідентифікатор сусіднього маршрутизатора не відображається або, якщо він не показує стан FULL, то обидва маршрутизатори не створили відносини суміжності OSPF. У випадку з маршрутизатором DROther відношення суміжності створене, якщо показується стан FULL чи 2WAY.

У мережі Ethernet із множинним доступом після стану FULL/ у колонку State (стан) відображаються значки DR і BDR.

Використання декількох протоколів маршрутизації

Налаштування і поширення маршруту за замовчуванням

Більшість мереж з'єднуються одна з одною по мережі Інтернет. Маршрутизатор OSPF надає інформацію маршрутизації про мережі в межах однієї автономної системи. Маршрутизатор OSPF також повинен надавати інформацію про доступність мереж за межами автономної системи.

Іноді адміністратори налаштовують статичні маршрути на маршрутизаторах таким чином, щоб вони надавали інформацію, що не виходить через протокол маршрутизації. Налаштування статичних маршрутів на всіх маршрутизаторах у великій мережі – процес трудомісткий. Більш легкий спосіб – налаштування маршруту за замовчуванням, що вказує на підключення до якої-небудь мережі через Інтернет.

За допомогою маршрутизатора OSPF адміністратор налаштовує даний маршрут на прикордонному маршрутизаторі автономної системи (ASBR). Маршрутизатор ASBR також часто називають маршрутизатором границі автономної системи. Маршрутизатор ASBR з'єднує мережа OSPF з якою-небудь зовнішньою мережею. Як тільки маршрут за замовчуванням буде внесений у таблицю маршрутизатора ASBR, його можна налаштувати таким чином, щоб він повідомляв цей маршрут для іншої частини мережі OSPF (default-information originate). Цей процес повідомляє маршрут за замовчуванням кожному маршрутизатору в межах автономної системи, що рятує адміністратора від роботи з налаштування статичних маршрутів на кожному маршрутизаторі в мережі.

Для налаштування маршрутизатора на розсилання маршруту за замовчуванням по мережі OSPF потрібно виконати наступні два кроки [12].

Крок 1

Налаштувати маршрут за замовчуванням на маршрутизаторі ASBR.

R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0

У команді статичного маршруту за замовчуванням можна вказати який-небудь інтерфейс чи IP-адресу наступного переходу.

Крок 2

Налаштувати на маршрутизаторі ASBR розсилання маршруту за замовчуванням на інші маршрутизатори. За замовчуванням маршрутизатор OSPF не включає маршрут за замовчуванням у свої оголошення навіть тоді, коли цей маршрут присутній у його таблиці маршрутизації.

R1(config)#router ospf 1

R1(config-router)#default-information originate

Тепер у таблицях маршрутизації інших маршрутизаторів в області OSPF має бути записаний шлюз останньої надії і вхід у мережу 0.0.0.0/0. Маршрут за замовчуванням включається в область OSPF і виглядає в таблицях маршрутизації інших маршрутизаторів просто як E2.

Налаштування підсумовування OSPF

Одним з методів, що забезпечують скорочення кількості оновлень маршрутів і розміру таблиці маршрутів OSPF, є підсумовування маршрутів. Маршрути можна підсумовувати в OSPF або між областями, що входять у ту ж мережу OSPF.

Коли маршрутизатор використовує сумарний маршрут, він використовує одну супермережеву адресу для представлення декількох маршрутів. Для оголошення сервером сумарного маршруту фактично активним має бути хоча б один з маршрутів, включених у сумарний маршрут.

Якщо нестабільні один чи декілька маршрутів, маршрутизатор продовжить повідомляти тільки стабільний сумарний маршрут. Він не відправляє оновлених даних про

окремі маршрутизатори. Усі пакети, спрямовані на нестабільний маршрут під час його неактивного стану, будуть просто скидатися на підсумовуючий маршрутизатор.

Щоб налаштувати маршрутизатор OSPF ASBR на підсумовування цих сегментів мережі в іншу область OSPF, у режимі налаштування маршрутизатора використовується команда, яка вказує область, де сумуються мережі, а також початковий номер мережі та маску:

area ідентифікатор_області range ip-адреса маска_ip-адреси

Обмеження протоколу OSPF

Протокол OSPF є масштабованим протоколом маршрутизації. Він має можливість швидкої конвергенції та роботи з дуже великими мережами. Однак при його використанні необхідно звертати увагу на деякі обмеження.

Протокол OSPF підтримує кілька баз даних, тому вимагає більше пам'яті та обчислювальних потужностей, ніж протоколи маршрутизації на базі векторів відстані.

Алгоритм Дейкстри вимагає великої обчислювальної потужності для розрахунку найкращого маршруту. Якщо мережа OSPF є складною та нестабільною, даний алгоритм споживає значні об'єми ресурсів при частих перерахунках. Маршрутизатори, на яких виконується протокол OSPF, звичайно є більш потужними та дорогими.

Щоб уникнути надмірного використання ресурсів маршрутизатора, потрібно використовувати строгу ієрархічну структуру для поділу мережі на області меншого розміру. Всі області повинні підтримувати можливість зв'язку з областю 0. У протилежному випадку вони можуть втратити зв'язок з іншими областями.

Якщо мережа має великий розмір і складну структуру, процес налаштування протоколу OSPF може виявитися складним. Крім того, для інтерпретації інформації, що знаходиться в базах даних OSPF і таблицях маршрутизації, потрібно добре розуміння процесу.

Під час процесу початкового виявлення мережі протокол OSPF може виконувати лавинне розсилання по мережі повідомлень про стан каналу, істотно обмежуючи об'єм даних, що можуть бути передані по мережі. Лавинне розсилання у великих мережах з великою кількістю маршрутизаторів і маленькою смугою пропускання приводять до істотного зниження пропускної здатності мережі.

Незважаючи на проблеми і обмеження OSPF, він як і раніше є найбільш вживаним протоколом маршрутизації на базі стану каналу в середніх та великих корпоративних мережах.

Використання декількох протоколів

З багатьох причин організації можуть вибирати кілька протоколів маршрутизації.

Для різних розділів мережі мережевий адміністратор може вибрати різні протоколи маршрутизації в залежності від наявного застарілого обладнання та доступних ресурсів.

Можливі випадки злиття двох компаній, мережі яких були налаштовані з використанням різних протоколів маршрутизації, при цьому їм потрібно зв'язуватися один з одним по мережі.

Якщо на одному маршрутизаторі є кілька протоколів маршрутизації, то, можливо, що цей маршрутизатор буде дізнаватися про якого-небудь адресата з декількох джерел. Для маршрутизатора необхідний передбачуваний спосіб вибору кращого маршруту і запису його в таблицю маршрутизації.

Коли маршрутизатор довідається інформацію про одну мережу з декількох джерел, для визначення маршруту він використовує адміністративну відстань (Administrative Distance, AD). Всім методам отримання інформації про маршрутизацію програмне забезпечення Cisco IOS призначає визначену адміністративну відстань.

Якщо маршрутизатор дізнається про конкретну мережу за допомогою протоколів RIP та OSPF, для таблиці маршрутизації він вибере маршрут, повідомлений по протоколу OSPF. Його адміністративна відстань менша і тому більш бажана. Код на початку таблиці маршрутизації вказує джерело маршруту, або яким чином він був повідомлений. Кожен код асоціюється з конкретною адміністративною відстанню.

Якщо дві мережі мають однакову базову адресу і мережеву маску, маршрутизатор розглядає їх як ідентичні. Він розглядає підсумовану мережу та окрему мережу, що входить у цю сумарну мережу, як різні мережі.

Підсумована мережа 192.168.0.0/22 і окрема мережа 192.168.1.0/24 є окремими записами, незважаючи на те, що підсумована мережа містить цю окрему мережу. При виникненні цієї ситуації в таблицю маршрутизації заносяться обидві мережі. Вибір маршруту випадає на запис з найдовшим збігом префіксу.

Наприклад, маршрутизатор отримує пакет з IP-адресою призначення 172.16.0.10. Цьому пакету підходить три можливих маршрути: 172.16.0.0/12, 172.16.0.0/18 і 172.16.0.0/26. З усіх трьох маршрутів маршрут з адресою 172.16.0.0/26 має найдовший збіг. Щоб ці маршрути розглядалися як придатні, в мережевій масці маршруту повинна співпадати деяка кількість бітів.

Тема 5. Протоколи канального, мережевого та транспортного рівнів

Значення протоколів у моделі OSI та TCP/IP. Взаємодія рівнів і роль інкапсуляції даних. Протоколи канального рівня: основні функції канального рівня (адресація, контроль доступу до середовища, виявлення помилок). Ethernet як домінуючий стандарт локальних мереж. Технології бездротового доступу (Wi-Fi – IEEE 802.11). PPP та HDLC у каналах точка-точка. VLAN (IEEE 802.1Q) як розширення можливостей канального рівня. Протоколи мережевого рівня: призначення мережевого рівня (маршрутизація, логічна адресація). IPv4 та IPv6: структура адрес, основні відмінності. Протокол ARP і його роль у відображенні адрес. ICMP як інструмент діагностики та повідомлення про помилки.

Протоколи транспортного рівня: функції транспортного рівня (управління з'єднанням, контроль потоку, надійність). Порівняння TCP та UDP у прикладних сценаріях. Порти та сокети як механізм взаємодії з прикладними сервісами. Взаємодія протоколів різних рівнів. Приклади проходження даних крізь стек протоколів (інкапсуляція/декапсуляція). Приклади формування кадру, пакета та сегмента. Типові проблеми (затримки, втрата пакетів, дублювання) та методи їх усунення. Значення узгодженої роботи протоколів для функціонування глобальних мереж.

Значення протоколів у моделях OSI та TCP/IP

Протоколи є формалізованими правилами взаємодії між мережевими пристроями, які визначають формат даних, порядок обміну, способи виявлення та обробки помилок, а також механізми керування передаванням. Саме протоколи забезпечують сумісність обладнання та програмного забезпечення різних виробників і роблять можливим функціонування глобальних комп'ютерних мереж.

Еталонна модель OSI (Open Systems Interconnection) описує процес передавання даних у вигляді семирівневої ієрархії, де кожен рівень виконує чітко визначені функції та надає сервіси вищому рівню. Модель TCP/IP, що лежить в основі Інтернету, є більш практично орієнтованою і складається з чотирьох рівнів, які агрегують функції моделі OSI.

Попри різну кількість рівнів, обидві моделі ґрунтуються на однакових принципах: розподілі функцій, модульності та ієрархічній взаємодії протоколів.

Взаємодія рівнів і роль інкапсуляції даних

Передавання даних у мережі здійснюється завдяки процесу інкапсуляції. Дані, сформовані на прикладному рівні, послідовно передаються нижчим рівням, де кожен рівень додає власну службову інформацію у вигляді заголовка (а в деяких випадках і трейлера). У результаті на фізичному рівні передається бітовий потік.

На приймальному боці виконується зворотний процес − деінкапсуляція, під час якого кожен рівень аналізує та вилучає власний заголовок, передаючи корисні дані вищому рівню.

Такий підхід забезпечує:

– незалежність реалізації протоколів на різних рівнях;

– можливість модернізації окремих рівнів без зміни всієї системи;

– масштабованість і гнучкість мереж.

Канальний рівень: функції та протоколи

Канальний рівень відповідає за надійне передавання кадрів між безпосередньо з'єднаними вузлами мережі. Основні його функції полягають у фізичній адресації, контролі доступу до середовища передавання та виявленні помилок. На цьому рівні використовується MAC-адресація, яка ідентифікує мережеві інтерфейси. Контроль доступу до середовища (MAC − Media Access Control) визначає, який пристрій і в який момент часу має право передавати дані, що особливо важливо в мережах зі спільним середовищем. Для виявлення спотворень даних застосовуються контрольні суми та циклічні надлишкові коди (CRC), які дозволяють приймальній стороні визначити факт помилки та ініціювати повторне передавання кадру.

Ethernet (IEEE 802.3) є найпоширенішою технологією локальних мереж. Його домінування зумовлене простотою реалізації, високою масштабованістю та постійним зростанням пропускної здатності − від 10 Мбіт/с до сотень гігабіт за секунду.

Кадр Ethernet містить MAC-адреси відправника й отримувача, поле типу протоколу вищого рівня та контрольну суму. Сучасні Ethernet-мережі використовують комутацію замість спільного середовища, що практично усуває колізії.

Бездротові технології доступу: Wi-Fi (IEEE 802.11)

Стандарт IEEE 802.11 (Wi-Fi) реалізує канальний і фізичний рівні для бездротових локальних мереж. На відміну від Ethernet, Wi-Fi використовує механізми уникнення колізій (CSMA/CA), оскільки пристрої не завжди можуть «чути» один одного. Wi-Fi забезпечує мобільність користувачів, але є більш чутливим до завад, затримок і проблем безпеки, що зумовлює використання механізмів шифрування, автентифікації та керування доступом.

PPP та HDLC у каналах «точка-точка»

Протоколи PPP (Point-to-Point Protocol) та HDLC (High-Level Data Link Control) застосовуються в каналах з'єднання «точка-точка». Вони забезпечують інкапсуляцію мережевих протоколів, перевірку цілісності даних та, у випадку PPP, механізми автентифікації (PAP, CHAP). PPP широко використовується у з'єднаннях через WAN та VPN, тоді як HDLC часто застосовується у провайдерських мережах.

VLAN (IEEE 802.1Q) як розширення канального рівня

VLAN (Virtual Local Area Network) дозволяє логічно сегментувати фізичну мережу на окремі віртуальні домени широкомовлення. Стандарт IEEE 802.1Q реалізує тегування кадрів Ethernet, що дає змогу одному фізичному каналу обслуговувати декілька VLAN. Використання VLAN підвищує безпеку, керованість і ефективність використання мережевих ресурсів, особливо в корпоративних мережах.

Протоколи мережевого рівня

Мережевий рівень відповідає за логічну адресацію та маршрутизацію пакетів між різними мережами. IPv4 використовує 32-бітну адресу, що обмежує адресний простір і потребує застосування NAT. IPv6 використовує 128-бітну адресу, що практично усуває проблему дефіциту адрес і спрощує маршрутизацію, автоконфігурацію та безпеку. Основні відмінності між IPv4 та IPv6 полягають у структурі заголовка, механізмах адресації та підтримці сучасних мережевих сервісів.

ARP і ICMP

Протокол ARP (Address Resolution Protocol) забезпечує відображення логічних IP-адрес у фізичні MAC-адреси в локальній мережі.

ICMP (Internet Control Message Protocol) використовується для діагностики та повідомлення про помилки, зокрема у таких утилітах, як ping і traceroute.

Транспортний рівень: TCP та UDP

Транспортний рівень забезпечує логічний зв'язок між прикладними процесами.

TCP (Transmission Control Protocol) гарантує надійне передавання даних, контроль потоку та впорядкування сегментів, що робить його придатним для веб-сервісів, електронної пошти та передавання файлів.

UDP (User Datagram Protocol) є ненадійним, але швидким, що робить його ефективним для потокового відео, VoIP і онлайн-ігор.

Порти та сокети дозволяють ідентифікувати конкретні прикладні сервіси на вузлі та забезпечують мультиплексування з'єднань.

Проходження даних крізь стек протоколів

У процесі передавання інформації прикладні дані інкапсулюються у сегмент транспортного рівня, який далі поміщається в пакет мережевого рівня, а потім − у кадр канального рівня. На фізичному рівні кадр перетворюється на послідовність бітів.

Наприклад, HTTP-повідомлення інкапсулюється у TCP-сегмент, який передається у складі IP-пакета, що, своєю чергою, поміщається в Ethernet-кадр.

Типові проблеми передавання даних і методи їх усунення

До основних проблем належать затримки, втрата пакетів, дублювання та зміна порядку доставки. Вони усуваються завдяки механізмам повторного передавання, керування потоком, буферизації та маршрутизації.

Функціонування глобальних мереж можливе лише за умови узгодженої роботи протоколів усіх рівнів. Порушення або некоректна реалізація хоча б одного рівня призводить до деградації продуктивності або повної недоступності сервісів

Тема 6. Віртуальні локальні мережі та віртуальні приватні мережі

Актуальність технологій віртуалізації мережевих ресурсів. Віртуальні локальні мережі (VLAN): основні поняття та принципи роботи. Переваги використання VLAN: ізоляція трафіку, підвищення продуктивності та безпеки. Типи VLAN (на основі портів, MAC-адрес, протоколів). Механізм тегування кадрів (IEEE 802.1Q). Приклади конфігурації VLAN у мережевому обладнанні (комутатори Cisco, Mikrotik).

Віртуальні приватні мережі (VPN): основні поняття та призначення VPN. Основні архітектури VPN: site-to-site та remote access. Протоколи VPN (PPTP, L2TP, IPSec, SSL/TLS, OpenVPN, WireGuard). Використання VPN у корпоративних та хмарних середовищах. Використання VLAN і VPN для забезпечення сегментації та захисту корпоративних мереж. Практичні аспекти реалізації: налаштування VLAN у Cisco Packet Tracer. Створення простого VPN-з'єднання між віддаленими офісами. Типові проблеми та шляхи їх вирішення. Значення VLAN і VPN у сучасних інформаційно-комунікаційних системах. Перспективи розвитку технологій віртуалізації та безпечного віддаленого доступу.

Вузли і сервери, підключені до комутаторів 2-го рівня, вважаються частиною мережевого сегмента. Така організація характеризується двома серйозними проблемами:

– комутатори виконують лавинне розсилання широкомовних кадрів з усіх портів, що приводить до невиправданого використання смуги пропускання. Зі збільшенням числа пристроїв, підключених до комутатора, генерується більше широкомовного трафіку;

– всі пристрої, підключені до комутатора, можуть пересилати та отимувати кадри від всіх інших пристроїв на цьому комутаторі.

При проектуванні мережі рекомендується обмежувати широкомовний трафік областю мережі, у якій він необхідний. Існують причини організаційного характеру, коли одні вузли можуть отримувати доступ один до одного, а інші ні. Для обмеження широкомовних розсилань і об'єднання вузлів у групи створюються віртуальні локальні мережі (Virtual Local Area Networks, VLAN) [12].

VLAN – це логічний домен широкомовного розсилання, що може охоплювати кілька фізичних сегментів LAN. VLAN дозволяє адміністратору поєднувати станції по логічній функції незалежно від фізичного положення користувачів.

Кожна VLAN функціонує як окрема локальна мережа. VLAN може охоплювати один чи кілька комутаторів, що дозволяє вузлам працювати так, ніби вони знаходилися в одному сегменті.

VLAN виконують такі функції:

– обмеження широкомовних розсилань;

– об'єднання пристроїв у групи;

– пристрої, розташовані в одній VLAN, невидимі для пристроїв, розташованих в інший VLAN.

Для передачі трафіку між VLAN необхідний пристрій 3-го рівня.

Основними перевагами використання віртуальних локальних мереж є:

– безпека – віртуальні мережі дозволяють відокремити групи, які мають важливі дані від загальної частини мережі, зменшуючи ймовірність втрат конфіденційної інформації;

– зниження витрат – економія за рахунок ефективнішого використання пропускної здатності, up-лінків, зменшення потреб модернізації мережі;

– збільшення продуктивності – поділ мереж 2-го рівня на кілька логічних робочих груп (широкомовних доменів) зменшує зайвий трафік у мережі та підвищує продуктивність роботи;

– зменшення широкомовного шторму – поділ мережі на VLAN, знижує кількість пристроїв, які можуть брати участь в поширенні широкомовного шторму. Сегментація мережі запобігає поширенню широкомовного шторму на всю мережу;

– покращення ефективності роботи IT-персоналу – використання VLAN спрощує управління мережею, оскільки користувачі зі схожими вимогами до мережевих ресурсів знаходяться в одній VLAN. При додаванні нового комутатора всі політики і процедури, вже

налаштовані для конкретної VLAN, застосовуються при активації порта. Для певної VLAN можна задати відповідне ім’я з врахуванням їх призначення.

Пристрій можна призначити у VLAN відповідно до його розташування, MAC-адреси, IP-адреси або прикладних програм, які він використовує найчастіше. Адміністратори задають приналежність пристрою до VLAN статично або динамічно.

У випадку статичного призначення адміністратор повинен вручну призначити кожен порт комутатора у визначену VLAN. Наприклад, порт fa0/3 можна призначити в VLAN 20. Будь-який пристрій, що підключається до порту fa0/3, автоматично стає членом VLAN 20. Цей тип приналежності до VLAN найлегше налаштувати і він найпопулярніший, але додавання, переміщення і зміна пристроїв потребує постійного втручання адміністратора. Наприклад, переміщення вузла з однієї VLAN у другу потребує або ручного перепризначення порту комутатора в нову VLAN, або переключення кабелю робочої станції в інший порт комутатора, що відноситься до нової VLAN. Приналежність пристрою до VLAN цілком прозора для користувачів. Користувачі, які працюють із пристроєм, підключеним до порту комутатора, не знають, до якої VLAN вони належать.

Динамічна приналежність VLAN вимагає наявності сервера політик VLAN (VMPS − VLAN Management Policy Server). VMPS містить базу даних, що співставляє MAC-адреси з VLAN мережами. Коли пристрій підключається до порту, VMPS шукає його MAC-адресу у своїй базі даних і тимчасово призначає порт у відповідну VLAN. Динамічна приналежність VLAN вимагає більш складного налаштування й організації, але формує більш гнучку структуру, ніж статична приналежність VLAN. Переміщення, додавання і зміна компонентів виконується автоматично і не вимагає втручання адміністратора. Не всі комутатори Catalyst підтримують VMPS.

Типи VLAN

В мережі може існувати декілька типів VLAN. Деякі з них визначаються типом трафіку, що передається, інші визначаються функціями, що виконуються. Наприклад, у випадку статичного призначення порту у визначену VLAN, така VLAN називатиметься VLAN доступу(access VLAN).

Загалом розрізняють такі типии VLAN:

– Data VLAN;
– Default VLAN;
– Native VLAN;
– Management VLAN;
– Voice VLANs.

Data VLAN

VLAN даних – це VLAN налаштована для передавання лише користувацького трафіку. VLAN може передавати голосовий трафік, трафік для управління комутатором, але цей трафік не буде частиною Data VLAN. Це звичайна практика, щоб відокремити голосовий трафік та трафік управління від трафіку даних. VLAN даних іноді називають користувацькою VLAN.

Default VLAN

Всі порти комутатора стають членом VLAN за замовчуванням після початкового завантаження комутатора. Усі порти комутатора будучи членами Default VLAN знаходяться в одному домені широкомовної передачі. Це дозволяє будь-якому пристрою, підключеному до будь-якого порту комутатора, зв’язатись з іншими пристроями на інших портах комутатора. Для комутаторів Cisco Default VLAN є VLAN 1. VLAN 1 має всі функції VLAN, за винятком того, що її не можна перейменувати чи видалити. За замовчуванням, трафік 2-го рівня, такий як CDP чи STP пов’язаний з VLAN 1. З метою підвищення безпеки рекомендується змінити Default VLAN з VLAN 1 на будь-яку іншу VLAN, що в свою чергу вимагатиме налаштування всіх портів комутатора

Native VLAN

Native VLAN – це VLAN, який отримує всі кадри, які надсилаються без тега, або кадри з нерозподілених портів (не включених в жоден VLAN). 802.1q транковий порт підтримує трафік з багатьох VLAN (тегований трафік), а також трафік, який надходить не з

VLAN (нетегований трафік). Якщо комутатор отримує нетеговані кадри на транковому порті він автоматично передає їх в Native VLAN. В ролі Native VLAN рекомендується використовувати VLAN 1.

В термінології інших виробників можуть вживатися інші назви для такої VLAN. Наприклад untagged VLAN (3Com, Planet, D-link, Zyxel, HP).

Management VLAN

VLAN керування може бути будь-яка VLAN налаштована для доступу до функцій управління комутатором. VLAN 1 буде функціонувати як VLAN управління, якщо не призначити іншу VLAN в якості Management VLAN. Для VLAN керування призначається IP-адреса та маска підмережі. Керувати комутатором можна через HTTP, Telnet, SSH або SNMP.

Voice VLANs

Для передачі голосу по IP (VoIP) рекомендовано використовувати окремий VLAN, оскільки VoIP-трафік вимагає:

– гарантовану смуга пропускання для забезпечення якості передачі голосу;

– пріоритетності обслуговування в порівнянні з іншими типами трафіку;

– затримки менше 150 мілісекунд (мс) в мережі.

Для задоволення цих вимог вся мережа повинна бути призначена для підтримкиVoIP.

Ідентифікація та налаштування VLAN

Максимальне загальне число статичних і динамічних VLAN залежить від типу комутатора і версії IOS. За замовчуванням у якості VLAN керування застосовується VLAN1. Адміністратори використовують IP-адресу VLAN керування для віддаленого налаштування комутатора. Віддалений доступ до комутатора дозволяє адміністратору мережі налаштовувати та обслуговувати всі конфігурації VLAN. Крім того, VLAN керування використовується для обміну даними, наприклад трафіком протоколів CDP (Cisco Discovery Protocol) і VTP (VLAN Trunking Protocol), з іншими мережевими пристроями. При створенні віртуальної мережі їй призначається номер та ім’я. Номер VLAN – це будь-яке число з діапазону, доступного комутатору, крім VLAN1. Різні комутатори підтримують різну кількість VLAN. Найменування VLAN вважається рекомендованим методом керування.

Для налаштування VLAN використовуються наступні команди режиму глобальної конфігурації:

Switch(config)#vlan номер_vlan

Switch(config-vlan)#name ім’я_vlan

Switch(config-vlan)#exit

За замовчуванням всі порти належать до VLAN1. Порти можна призначати по одному чи діапазонами.

Для призначення окремих портів використовуються наступні команди:

Switch(config)#interface fa0/номер_порту

Switch(config-if)#switchport access vlan номер_vlan

Switch(config-if)# exit

Для призначення діапазонів портів використовуються наступні команди:

Switch(config)#interface range fa0/початок_діапазону - кінець_діапазону

Switch(config-if)#switchport access vlan номер_vlan

Switch(config-if)#exit

Для перевірки, обслуговування та усунення несправностей VLAN важливо знати основні команди show, доступні в Cisco IOS.

Для перевірки й обслуговування VLAN використовуються наступні команди:

– show vlan − виводить докладний список номерів та імен VLAN, активних на комутаторі, а також портів, призначених у кожну з них;

– show vlan brief − виводить зведений список, у якому відображаються тільки активні VLAN і їхні порти.

– show vlan id номер_ідентифікатора − виводить звіт про визначену VLAN за її ідентифікатором;

– show vlan name ім’я_vlan − виводить звіт про визначену VLAN за її ім’ям.

В організації працівники часто приходять, звільняються або переміщуються між відділами і проектами. Цей постійний рух вимагає обслуговування VLAN, включаючи їхнє видалення і перепризначення портів. Видалення VLAN і перепризначення портів в інші VLAN – це дві різні функції. Коли порт видаляється з визначеної VLAN, він повертається у VLAN1. При видаленні VLAN усі пов’язані порти деактивуються, оскільки вони більш незв’язані з жодною VLAN.

Видалення VLAN:

Switch(config)#no vlan номер_vlan

Видалення порту з визначеної VLAN:

Switch(config)#interface fa0/номер_порту

Switch(config-if)#no switchport access vlan номер_vlan

Пристрої, підключені до VLAN, взаємодіють тільки з іншими пристроями в цій VLAN, при цьому пристрої можуть бути підключені як до одного, так і до різних комутаторів.

Комутатор зв’язує кожен порт із визначеним номером VLAN. При прийомі кадру на порт комутатор додає ідентифікатор VLAN (VI) у кадр Ethernet. Додавання ідентифікатора VLAN у кадр Ethernet називається маркуванням кадру. Найпоширеніший стандарт маркування кадру – IEEE 802.1q. Стандарт 802.1q, що іноді скорочується до dot1q, має на увазі вставку 4-байтного поля мітки в кадр Ethernet. Ця мітка знаходиться між адресою джерела і полем type/length (тип/довжина). Мінімальний розмір кадрів Ethernet складає 64 байти, максимальний – 1518 байтів, однак розмір тегованого кадру Ethernet може досягати 1522 байти.

Кадри включають такі поля:

– MAC-адреси джерела і призначення;

– довжина кадру;

– корисні дані;

– контрольна послідовність кадру (FCS).

Поле FCS забезпечує виявлення помилок і гарантує цілісність всіх бітів в кадрі.

Мітка збільшує мінімальний розмір кадру Ethernet з 64 до 68 байт. Максимальний розмір збільшується з 1518 до 1522 байт. Комутатор перерозраховує FCS, тому що кількість бітів в кадрі збільшується. Якщо порт, сумісний з 802.1q, підключений до іншого порту, також сумісного з 802.1q, дані маркування VLAN передаються між ними. Якщо підключений порт несумісний з 802.1q, мітка VLAN буде видалена перш, ніж кадр досягне середовища передачі. Якщо пристрій, або порт доступу без підтримки 802.1q отримує кадр 802.1q, то дані мітки ігноруються, а пакет комутується на рівні 2 як стандартний кадр Ethernet. Це дозволяє розміщувати на транковому маршруті 802.1q проміжні пристрої рівня 2, наприклад інші комутатори. Щоб обробити кадр із міткою 802.1q, пристрій повинен дозволяти MTU зі значенням 1522 або вище.

VLAN для IP-телефонії та безпровідного доступу

Головне призначення VLAN – поділ трафіку на логічні групи. Трафік з однієї VLAN не впливає на трафік в іншій VLAN. Середовище VLAN ідеальне для трафіку, чуттєвого до тимчасових затримок, наприклад голосового. Голосовий трафік повинен отримувати пріоритет над звичайним трафіком даних, щоб уникнути перерв і джитера при розмові. Надання виділеної VLAN для голосового трафіку дозволяє голосовому трафіку не конкурувати з даними за доступну смугу пропускання.

IP-телефон, як правило, включає два порти – один для голосу, інший для даних. Пакети, передані між IP-телефоном і комп’ютером, використовують той же фізичний канал і той же порт комутатора. Для сегментації голосового трафіку потрібно активувати голосовий VLAN на комутаторі.

Безпровідний доступ – інший тип трафіку, що використовує переваги VLAN. Безпровідний доступ по своїй природі небезпечний та вразливий до хакерських атак. VLAN, створені для безпровідного доступу, ізолюють деякі з потенційних проблем. Загроза цілісності безпровідній VLAN не вплине на інші VLAN в організації. Більшість безпровідних

середовищ поміщають користувачів у VLAN за межами брандмауера для підвищеної безпеки. Користувачі повинні пройти аутентифікацію, щоб отримати доступ до внутрішньої мережі з безпровідної мережі. Крім того, багато організацій надають гостьовий доступ у свою безпровідну мережу. Гостьові облікові записи надають усім тимчасові безпровідні послуги, такі як веб-доступ, електронна пошта, ftp і SSH. Кількість активних облікових записів обмежується. Гостьові облікові записи включаються в безпровідну VLAN або групуються у власні VLAN.

Методи роботи з VLAN

При якісному плануванні та проектуванні VLAN забезпечується безпека, заощаджується смуга пропускання та локалізується трафік у корпоративній мережі. Усі ці функції поєднуються для покращення продуктивності мережі.

Деякі з методів налаштування, рекомендовані для VLAN у корпоративній мережі наводяться нижче:

– організація розміщення серверів;
– відключення портів, що не використовуються;
– налаштування VLAN керування з номером, відмінним від 1;
– використання протоколу VTP;
– налаштування доменів VTP;
– перезавантаження нових комутаторів перед їхнім додаванням в існуючу мережу.

В той же час VLAN не є відповіддю на всі проблеми.

Неправильне впровадження VLAN може привести до зайвого ускладнення мережі, що стане причиною зниження продуктивності мережі.

Транкінг та маршрутизація між VLAN

Режими роботи портів у VLAN

VLAN виконують три основні функції:

– обмеження розміру доменів широкомовних розсилань;
– підвищення продуктивності мережі;
– підвищення безпеки.

Щоб повною мірою скористатися перевагами VLAN, необхідно поширити їх на кілька комутаторів. Для портів комутатора можна задати дві різні ролі. Порт може бути визначений як порт доступу, або як транковий порт.

Порт доступу належить лише до однієї VLAN. Як правило, окремі пристрої, такі як комп'ютери і сервери, підключаються до портів такого типу. Якщо кілька комп'ютерів підключаються до одного порту доступу через концентратор, то всі пристрої, підключені до концентратора, будуть належати до однієї VLAN.

Транкінговий порт – це канал типу «точка-точка» між комутатором та іншим мережевим пристроєм. Транкові підключення служать для передачі трафіку декількох VLAN через один канал і забезпечують їм доступ до всієї мережі. Транкові порти необхідні для передачі трафіку декількох VLAN між пристроями при з'єднанні двох комутаторів, комутатора і маршрутизатора, комутатора і мережевого адаптера вузла з підтримкою транкінгу 802.1q. Без транкових портів для кожної VLAN було б потрібне окреме з'єднання між комутаторами. Наприклад, корпорації з 10 VLAN буде потрібно 10 каналів зв'язку. При такій організації мережа не масштабується належним чином. Транкові канали дозволяють вирішити цю проблему за рахунок передачі трафіку декількох VLAN через один канал. Для передачі трафіку декількох VLAN через один канал необхідна їх ідентифікація. Транковий порт підтримує маркування кадрів, яке дозволяє додати до кадру дані VLAN.

IEEE 802.1q – стандартний і затверджений метод маркування кадрів. Корпорація Cisco розробила власний протокол маркування кадрів з назвою міжкомутаторний канал (ISL, Inter-Switch Link). Комутатори вищого класу, такі як Catalyst 6500, підтримують обидва протоколи маркування, однак більшість комутаторів LAN, таких як Catalyst 2960, підтримують тільки 802.1q.

Налаштування режимів роботи портів

За замовчуванням порти комутатора працюють у режимі доступу. Щоб налаштувати порт комутатора в якості транкового порту, використовуються такі команди:

Switch(config)#interface fa0/номер_порту

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk encapsulation {dot1q | isl | negotiate}

Комутатори, що підтримують і 802.1q і ISL, вимагають останньої команди. Наприклад комутатор Catalyst 2960 не вимагає цієї команди, тому що підтримує тільки 802.1q.

Параметр узгодження використовується за замовчуванням на багатьох комутаторах Cisco. Він дозволяє пристрою автоматично виявляти тип інкапсуляції сусіднього комутатора.

Нові комутатори можуть виявляти тип каналу, заданий на протилежній стороні. У залежності від підключеного пристрою канал налаштовується в якості транкового порту або як порт доступу.

Switch(config-if)#switchport mode dynamic {desirable | auto}

У режимі desirable порт стає транковим, якщо порт на іншій стороні знаходиться в режимі trunk, desirable або auto.

У режимі auto порт стає транковим, якщо порт на іншій стороні знаходиться в режимі trunk чи desirable.

Щоб повернути транковий порт у режим доступу, використовуються такі команди:

Switch(config)#interface fa0/номер_порту

Switch(config-if)#no switchport mode trunk

або

Switch(config-if)#switchport mode access

Транкінг дозволяє декільком VLAN пересилати трафік між комутаторами, використовуючи один порт.

Транковий канал пропускає трафік з 4-байтним полем мітки в кадрі, якщо на обох сторонах налаштований протокол 802.1q. Мітка кадру містить ідентифікатор VLAN ID.

Коли комутатор отримує тегований кадр на транковому порту, він видаляє мітку перш, ніж переслати кадр із порту доступу. Комутатор пересилає кадр, тільки якщо порт доступу відноситься до тієї ж VLAN, що і тегований кадр. Однак деякі типи трафіку повинні проходити через канал 802.1q без ідентифікатора VLAN. Трафік без ідентифікатора VLAN називається нетегованим. Приклади нетегованого трафіку: CDP (Cisco Discovery Protocol), VTP і певні типи голосового трафіку. Нетегований трафік мінімізує затримку, пов’язану з перевіркою мітки ідентифікатора VLAN. Для підтримки нетегованого трафіку використовується спеціальна VLAN, що називається рідна (native VLAN).

Нетеговані кадри, прийняті на порту 802.1q, передаються у native VLAN. На комутаторах Cisco Catalyst в якості native VLAN за замовчуванням використовується VLAN 1. Будь-яку VLAN можна налаштувати в якості native VLAN. Native VLAN для транкового підключення 802.1q повинна бути однаковою на обох сторонах каналу. В протилежному випадку в топології STP можуть виникнути петлі. Для призначення ідентифікатора native VLAN фізичному інтерфейсу для транкового підключення 802.1q використовується команда:

Switch(config-if)#dot1q native vlan ідентифікатор_vlan

Хоча VLAN можуть охоплювати кілька комутаторів, тільки пристрої, що відносяться до однієї VLAN, можуть взаємодіяти один з одним. VLAN ізолюють визначені типи трафіку з міркувань безпеки. Для переміщення трафіку між VLAN необхідний пристрій мережевого рівня, що збільшує вартість впровадження і підвищує рівень затримок в мережі. Використання пристрою 3-го рівня для з’єднання між VLAN дозволяє адміністратору здійснювати контроль над трафіком, що передається з однієї VLAN в іншу.

Методи маршрутизації між VLAN

Один з методів маршрутизації між VLAN вимагає окремого підключення інтерфейсу до пристрою 3-го рівня для кожної VLAN. Інший метод з’єднання між VLAN вимагає функцій, що називаються субінтерфейсами. Субінтерфейси дозволяють логічно розділити один фізичний інтерфейс на кілька логічних шляхів. Для кожної VLAN налаштовується окремий шлях або субінтерфейс.

Взаємодія між VLAN з використанням субінтерфейсів вимагає налаштування як маршрутизатора, так і комутатора. Інтерфейс комутатора має бути налаштований в якості транкового каналу 802.1q.

Інтерфейс маршрутизатора (не нижче FastEthernet 100 Мбіт/с) має бути налаштований з підтримкою інкапсуляції 802.1q, крім того, для кожної VLAN налаштовується один субінтерфейс. Субінтерфейс дозволяє кожній VLAN мати власний логічний шлях і шлюз за замовчуванням до маршрутизатора. Вузол з передавальної VLAN пересилає трафік маршрутизатору, використовуючи шлюз за замовчуванням. Субінтерфейс VLAN визначає шлюз за замовчуванням для усіх вузлів цієї VLAN. Маршрутизатор визначає IP-адресу призначення і виконує пошук по таблиці маршрутизації. Якщо VLAN призначення відноситься до того ж комутатора, що і вихідна VLAN, маршрутизатор пересилає трафік назад до вихідного комутатора, використовуючи параметри субінтерфейсу та ідентифікатора VLAN призначення. Така конфігурація часто називається каскадом маршрутизаторів.

Якщо вихідний інтерфейс маршрутизатора сумісний з 802.1q, кадр зберігає 4-байтну мітку VLAN. Якщо вихідний інтерфейс несумісний з 802.1q, маршрутизатор відділяє мітку від кадру і повертає кадр в оригінальний формат Ethernet.

Налаштування маршрутизації між VLAN

Порядок налаштування маршрутизації між VLAN:

1. Налаштувати транковий порт на комутаторі.

Switch(config)#interface fa0/2

Switch(config-if)#switchport mode trunk

2. На маршрутизаторі налаштувати інтерфейс FastEthernet без IP-адреси та маски.

Router(config)#interface fa0/1

Router(config-if)#no ip address

Router(config-if)#no shutdown

3. На маршрутизаторі налаштувати один субінтерфейс з IP-адресою та маскою для кожної VLAN. Кожен субінтерфейс використовує інкапсуляцію 802.1q.

Router(config)#interface fa0/0.10

Router(config-subif)#encapsulation dot1q 10

Router(config-subif)#ip address 192.168.10.1 255.255.255.0

4. Перевірити конфігурацію і працездатність маршрутизації між VLAN за допомогою таких команд:

Switch#show trunk

Router#show ip interfaces

Router#show ip interfaces brief

Router#show ip route

Тема 7. Поняття мережної безпеки. Принципи роботи ACL

Роль ACL у забезпеченні контролю доступу та мережевої безпеки. Поняття та класифікація ACL. Визначення списків контролю доступу. Стандартні та розширені ACL. Нумеровані та іменовані ACL. Принципи функціонування ACL: логіка «permit» та «deny». Типові сценарії застосування ACL: фільтрація трафіку за IP-адресою джерела і призначення, контроль доступу за протоколами та портами, використання ACL для сегментації трафіку у VLAN, обмеження доступу до мережевих сервісів. Приклади налаштування ACL на мережевому обладнанні. ACL як базовий, але необхідний інструмент мережевої безпеки.

Фільтрація трафіку

Безпека в корпоративній мережі відіграє важливу роль. Важливо запобігти несанкціонованому доступу та захистити мережу від різного роду атак. У випадку несанкціонованого доступу зловмисники можуть змінити, знищити чи викрасти конфіденційні дані. DoS-атаки перешкоджають доступу легітимних користувачів до ресурсів.

Фільтрація трафіку дозволяє адміністратору контролювати трафік у різних сегментах мережі. Фільтрація являє собою процес аналізу вмісту пакету з метою дозволу або блокування його передачі. Фільтрація пакетів може бути простою чи складною і може забороняти або дозволяти трафік за такими критеріями, як: вихідна IP-адреса, IP-адреса призначення, MAC-адреса; протокол, тип додатку. Фільтрацію пакетів можна порівняти з фільтрацією небажаної електронної пошти. Багато поштових додатків дозволяють користувачу налаштовувати автоматичне видалення повідомлень, що приходять з визначеної вихідної адреси. Фільтрація пакетів може здійснюватися схожим чином шляхом налаштування маршрутизатора на визначення небажаного трафіку. Фільтрація пакетів дозволяє підвищити продуктивність мережі. Завдяки відхиленню небажаного чи забороненого трафіку близько до його джерела, трафік не передається по мережі і не споживає ресурси. Фільтрація пакетів, яку іноді називають статичною фільтрацією пакетів, контролює доступ до мережі шляхом аналізу вхідних і вихідних пакетів та їх передачі або блокування на основі встановлених критеріїв [24].

Маршрутизатор діє як фільтр пакетів, коли пересилає або забороняє передачу пакетів відповідно до правил фільтрації. Коли пакет прибуває на маршрутизатор, який здійснює фільтрацію пакетів, маршрутизатор аналізує певну інформацію із заголовку пакету та приймає рішення відповідно до правил фільтрації. Фільтрація пакетів здійснюється на мережевому рівні моделі OSI, або Інтернет-рівні моделі TCP/IP.

Маршрутизатор використовує правила, щоб визначити: передавати чи заборонити трафік залежно від IP-адрес джерела і призначення, порту джерела і порту призначення, протоколу пакету. Ці правила визначаються за допомогою списків контролю доступу, або ACL на основі:

– IP-адреси джерела;
– IP-адреси отримувача;
– типу ICMP повідомлення.

ACL може також проаналізувати інформацію вищого рівня та співставити зі своїми правилами. Інформація вищого рівня включає в себе:

– TCP / UDP порт джерела;
– TCP / UDP порт призначення.

До пристроїв, що найчастіше використовуються для фільтрації трафіку, входять:

– міжмережеві екрани, вбудовані в інтегровані маршрутизатори;
– виділені пристрої забезпечення безпеки;
– сервери.

Деякі з них фільтрують тільки трафік, що виникає у внутрішній мережі. Більш досконалі пристрої безпеки здатні розпізнавати і фільтрувати відомі типи атак із зовнішніх джерел.

Корпоративні маршрутизатори здатні розпізнавати шкідливий трафік і запобігати його проникненню в мережу та порушенню працездатності мережі. Практично всі маршрутизатори виконують фільтрацію трафіку по вихідних і кінцевих IP-адресах пакетів. Вони також фільтрують визначені додатки і протоколи, такі як IP, TCP, HTTP, FTP, Telnet та ін.

Списки контролю доступу

Одним з найбільш розповсюджених способів фільтрації трафіку є використання списків контролю доступу (ACL-списків). ACL-списки можна використовувати для керування вхідним і існуючим трафіком у мережі і його фільтрації.

ACL – це скрипт конфігурації маршрутизатора, який визначає, чи буде маршрутизатор дозволяти або забороняти передачу пакетів на основі критеріїв, які містяться в заголовку пакета. Списки ACL також використовуються для вибору типів трафіку, які будуть проаналізовані, передані чи оброблені іншими способами [24].

Кожен пакет проходить через інтерфейс з певними ACL. ACL перевіряються зверху вниз, рядок за рядком, перевіряючи співпадіння шаблону у пакетах. ACL забезпечує корпоративну політику безпеки, застосовуючи правила заборони/дозволу для визначення долі пакета. Розмір ACL-списку може змінюватись від однієї інструкції, по якій дозволяється або блокується трафік від одного джерела, до сотні інструкцій, що дозволяють або забороняють пакети з різних джерел. В основному, ACL-списки використовуються для визначення типів пакетів, які приймаються чи відхиляються.

ACL-списки визначають трафік для декількох цілей:

– вказання внутрішніх вузлів для NAT;

– виявлення і класифікації трафіку для забезпечення розширених можливостей, таких як QoS і організація черги;

– обмеження інформації про оновлення маршрутизації;

– контроль доступу віртуальних терміналів до маршрутизаторів.

За замовчуванням, маршрутизатор не має жодних списків ACL і тому не фільтрує трафік. Трафік, який надходить на маршрутизатор маршрутизується відповідно до таблиці маршрутизації. Якщо на маршрутизаторі не використовуються ACL списки, всі пакети проходять через маршрутизатор до наступного сегменту мережі.

Загалом на маршрутизаторі можуть застосовуватись три типи списків ACL, по одному відповідно до протоколу, до напрямку та до інтерфейсу:

– один ACL на протокол – для контролю потоків трафіку на інтерфейсі, тобто ACL повинні бути визначені для кожного протоколу на інтерфейсі;

– один ACL одному напрямку – ACL контролюють трафік в одному напрямку в один момент часу на інтерфейсі. Два роздільних списки контролю доступом мають бути створені для контролю вхідного та вихідного трафіку;

– один ACL на інтерфейс – ACL контролює трафіку для одного інтерфейсу.

Написання списків ACL може бути складним та комплексним завданням.

Використання ACL-списків може бути пов’язане з наступними потенційними проблемами:

– додаткове навантаження на маршрутизатор для перевірки всіх пакетів означає менший час на фактичне пересилання пакетів;

– погано організовані ACL-списки створюють ще більше навантаження на маршрутизатор і можуть порушити працездатність мережі;

– неправильно розміщені ACL-списки блокують дозволений трафік і дозволяють заборонений.

Типи і використання ACL-списків

Адміністратору доступно кілька варіантів створення списків контролю доступу. Складність вимог до структури визначає тип необхідного ACL-списку.

Існує три типи ACL-списків.

Стандартний ACL-список є найпростішим із трьох типів. При створенні стандартного ACL-списку для IP-протоколу, фільтрація по ACL-списках здійснюється на основі вихідної IP-адреси пакету. Адреса призначення пакету та порт не мають значення.

Стандартні ACL-списки визначають дозвіл пакетові на основі всього протоколу, такого як IP-протокол. Таким чином, при забороні вузлового пристрою стандартним ACL-списком, забороняються всі служби цього вузла. Такий тип ACL-списку корисний для дозволу доступу всіх служб визначеного користувача чи локальної мережі (LAN) через маршрутизатор із забороною доступу з інших IP-адрес.

Стандартні ACL-списки визначаються по номерах, які їм привласнюються. Номери з діапазону від 1 до 99 і від 1300 до 1999 привласнюються спискам доступу, що дозволяють або блокують IP-трафік.

Розширений ACL-список використовується для фільтрації не тільки по вихідній IP-адресі, а також по кінцевій IP-адресі, протоколу і номерах портів. Розширені ACL-списки використовуються частіше стандартних, оскільки вони є більш визначеними і забезпечують більш високий рівень контролю. Розширеним ACL-спискам привласнюються номери з діапазону від 100 до 199 і від 2000 до 2699.

Іменований ACL-список (NACL-список) має формат стандартного чи розширеного списку і позначається описовим ім'ям, а не номером. При налаштуванні іменованих ACL-списків, маршрутизатор IOS використовує режим підкоманди NACL.

Обробка ACL-списку

У списках контролю доступу міститься одна чи більше інструкцій. Кожна інструкція дає дозвіл, або забороняє трафік на основі зазначених параметрів. Трафік порівнюється з кожною інструкцією в ACL-списку одна за одною, поки не буде знайдене співпадіння, або не закінчиться список інструкцій.

Остання інструкція в ACL-списку завжди містить неявну заборону трафіку. Ця інструкція автоматично вставляється в кінець кожного ACL-списку, хоча і не є присутньою в ньому фізично. Неявна заборона блокує весь трафік. Ця можливість дозволяє запобігти випадковому проходженню небажаного трафіку.

Після створення списку контролю доступу, його необхідно застосувати до інтерфейсу, щоб задіяти його. ACL-список призначений для фільтрації вхідного або вихідного трафіку, що проходить через інтерфейс. Якщо пакет відповідає інструкції, що дозволяє проходження, то він пропускається маршрутизатором. Якщо ж пакет відповідає інструкції, що забороняє проходження, він зупиняється. ACL-список без жодної інструкції, що дозволяє проходження, приводить до блокування всього трафіку. Це пояснюється тим, що наприкінці кожного ACL-списку вказується неявна заборона. Таким чином, ACL-список буде перешкоджати проходженню всього трафіку, якщо не зазначені особливі дозволи.

Адміністратор може використовувати вхідний чи вихідний ACL-список для інтерфейсу маршрутизатора. Вхідний чи вихідний напрямок завжди розглядається з погляду маршрутизатора. Трафік, що надходить через інтерфейс, є вхідним, а трафік, який відправляється через інтерфейс – вихідним.

При отриманні пакету через інтерфейс маршрутизатор перевіряє такі параметри:

– наявність ACL-списку, пов'язаного з інтерфейсом;
– визначення типу ACL-списку (вхідний/вихідний);
– визначення відповідності трафіку умовам.

ACL-список, що використовується як вихідний до інтерфейсу, не діє для вхідного трафіку на тому ж інтерфейсі. Для кожного інтерфейсу маршрутизатор може мати один ACL-список для одного напрямку по кожному мережевому протоколу. Для IP-протоколу один інтерфейс може мати один вхідний і один вихідний ACL-список одночасно. ACL списки визначають набір правил, які дають додаткові можливості управління для пакетів, які надходять на вхідний інтерфейсу, пакетів, які передаються через маршрутизатор та пакетів, що виходять через вихідні інтерфейси маршрутизатора. ACL списки не діють на пакети, які виходять від самого маршрутизатора.

Вхідні ACL списки – вхідні пакети обробляються перед тим, як вони направляються на вихідний інтерфейс. Вхідні ACL є ефективними, оскільки економлять ресурси маршрутизатора, якщо пакет відкидається. Якщо пакет дозволений, потім він маршрутизується.

Вихідні ACL списки – вхідні пакети направляються на вихідний інтерфейс, а потім вони обробляються за допомогою вихідного ACL. Перед тим, як пакет направляється на вихідний інтерфейс, маршрутизатор перевіряє таблицю маршрутизації, щоб переконатися, що є маршрут для даного пакету. Якщо пакет не маршрутизується, він відкидається маршрутизатором. Потім маршрутизатор перевіряє, чи є ACL на вихідний інтерфейс. Для вихідних списків, «permit» означає послати пакет у вихідний буфер, а «deny» означає відкинути пакет.

ACL-списки, що застосовуються до інтерфейсу, створюють затримку трафіку. Навіть один довгий ACL-список може вплинути на продуктивність маршрутизатора [25].

Використання шаблонної маски

У простих ACL-списках вказується тільки одна дозволена чи заборонена адреса. Для блокування декількох адрес або діапазонів адрес необхідно кілька інструкцій або шаблонна маска. Використання IP-адреси мережі із шаблонною маскою забезпечує значно більшу гнучкість. За допомогою шаблонної маски можна блокувати діапазон адрес або всю мережу за допомогою лише однієї інструкції. У шаблонній масці використовуються символи «0» для вказівки частини IP-адреси, що повинна точно співпадати, і символи «1» – для частини IP-адреси, яка не повинна збігатися з визначеним номером. Шаблонна маска типу 0.0.0.0 вимагає точного співпадіння усіх 32 біт IP-адреси. Маска прирівнюється до використання параметра host. Шаблонна маска, яка використовується з функціями ACL-списків, аналогічна масці, що використовується в протоколі маршрутизації OSPF, але кожна маска має власну мету. При використанні з інструкціями ACL-списку шаблонна маска вказує вузол, або діапазон заборонених чи дозволених адрес. В інструкції ACL-списку IP-адреса та шаблонна маска утворюють поля, що порівнюються. Усі пакети, що входять або виходять через інтерфейс, порівнюються з кожною інструкцією ACL-списку для виявлення збігу. Шаблонна маска визначає, скільки біт вхідної IP-адреси відповідають порівнюваній адресі.

Наприклад: наступна інструкція дозволяє усі вузли мережі 192.168.1.0 і блокує інші:

access-list 1 permit 192.168.1.0 0.0.0.255

Шаблонна маска вказує, що повинні збігатися тільки перші три октети. Отже, якщо перші 24 біти вхідного пакету збігаються з першими 24 бітами порівнюваного поля, пакет дозволяється. Будь-який пакет з вихідною IP-адресою з діапазону 192.168.1.1 – 192.168.1.255 відповідає сполученню порівнюваної адреси і маски в зазначеному прикладі. Всі інші пакети забороняються ACL-списком за допомогою неявної інструкції deny any.

Оцінка результатів використання шаблонної маски

При створенні ACL-списку доступно два спеціальних параметри, які можна використовувати на місці шаблонної маски: host і any.

Параметр host

Для фільтрації одного визначеного вузла використовується шаблонна маска 0.0.0.0 після IP-адреси або параметр host перед IP-адресою.

R1(config)#access-list 9 deny 192.168.15.99 0.0.0.0

Що відповідає наступному:

R1(config)#access-list 9 deny host 192.168.15.99

Параметр any

Для фільтрації усіх вузлів використовуються всі параметри «1» шляхом налаштування шаблонної маски 255.255.255.255. При використанні шаблонної маски 255.255.255.255 вважається, що усі біти збігаються. Отже, IP-адреса, як правило, має вигляд 0.0.0.0. Іншим способом фільтрації усіх вузлів є використання параметра any.

R1(config)#access-list 9 permit 0.0.0.0 255.255.255.255

Що відповідає наступному:

R1(config)#access-list 9 permit any

Приклад, у якому забороняється визначений вузол і дозволяються всі інші:

R1(config)#access-list 9 deny host 192.168.15.99

R1(config)#access-list 9 permit any

Команда «permit any» дозволяє весь трафік, спеціально не заборонений ACL-списком. При такому налаштуванні, обробка пакетів не буде виконуватися до неявної команди deny any наприкінці ACL-списку.

У корпоративній мережі з ієрархічною схемою IP-адресації часто необхідна фільтрація трафіку підмережі.

Якщо 3 біти використовуються для розбивки мережі 192.168.77.0 на підмережі, маскою підмережі буде 255.255.255.224. У результаті вирахування маски підмережі з усіх значень маски 255 виходить шаблонна маска 0.0.0.31. Для дозволу вузлів у підмережі 192.168.77.32 використовується наступна інструкція ACL-списку:

access-list 44 permit 192.168.77.32 0.0.0.31

Перші 27 біт кожного пакету відповідають першим 27 бітам порівнюваної адреси. Загальний діапазон адрес, допустимих по цій інструкції, починається з 192.168.77.33 і закінчується 192.168.77.63. У нього входять всі адреси підмережі 192.168.77.32.

Створення правильних шаблонних масок для інструкцій ACL-списку забезпечує контроль, необхідний для точної оптимізації потоку трафіку.

Мережа 192.168.77.0 з маскою 255.255.255.192 чи /26 утворить наступні чотири підмережі:

192.168.77.0/26
192.168.77.64/26
192.168.77.128/26
192.168.77.192/26

Щоб створити ACL-список для фільтрації будь-яких з цих чотирьох підмереж, необхідно вирахувати маску підмережі 255.255.255.192 з усіх значень маски 255, у результаті чого вийде шаблонна маска 0.0.0.63. Щоб дозволити трафік з двох перших з цих підмереж, використовуються дві наступні інструкції ACL-списку:

access-list 55 permit 192.168.77.0 0.0.0.63
access-list 55 permit 192.168.77.64 0.0.0.63

Перші дві мережі в сумі утворять 192.168.77.0/25. У результаті вирахування підсумованої маски підмережі 255.255.255.128 зі значень маски 255 виходить шаблонна маска 0.0.0.127. Використання цієї маски дозволяє об’єднати ці дві підмережі в одній інструкції ACL-списку замість двох.

access-list 5 permit 192.168.77.0 0.0.0.127

Налаштування списків контролю доступу

Правильно складені списки контролю доступу позитивно позначаються на продуктивності та доступності мережі. Для досягнення максимальних результатів необхідне планування створення і розміщення списків контролю доступу.

Етап планування включає наступні дії:

1. Визначення вимог до фільтрації трафіку.

2. Вибір типу ACL-списку, який найкраще відповідає вимогам.

3. Визначення маршрутизатора та інтерфейсу, на якому буде застосовуватися ACL-список.

4. Вибір напрямку фільтрації трафіку.

Крок 1. Визначення вимог до фільтрації трафіку.

Список вимог до фільтрації трафіку, складається на основі опитування в кожному підрозділі підприємства. Ці вимоги різні для різних підприємств і ґрунтуються на потребах клієнтів, типах і об’ємах трафіку, а також задачах безпеки.

Крок 2. Вибір типу ACL-списку, що відповідає вимогам.

Вибір стандартного або розширеного ACL-списку обумовлений поточними вимогами до фільтрації. Вибір типу ACL-списку може вплинути на гнучкість фільтрації по ACL-списку, а також на продуктивність маршрутизатора і пропускну здатність мережі.

Стандартні ACL-списки легко створювати і впроваджувати. Однак фільтрація по стандартних ACL-списках можлива тільки на основі вихідної адреси і застосовується до всього трафіку без врахування його типу чи призначення. При маршрутизації в кілька мереж занадто близьке розміщення стандартного ACL-списку до джерела може ненавмисно

блокувати допустимий трафік. Отже, важливо розміщувати стандартні ACL-списки якнайближче до вузла призначення. У випадку більш складних вимог до фільтрації варто використовувати розширений ACL-список. Розширені ACL-списки дають більший контроль, ніж стандартні. Вони допускають фільтрацію по вихідних і кінцевих адресах. Ці списки також забезпечують фільтрацію по протоколу мережевого рівня, протоколу транспортного рівня і номерах портів, якщо це необхідно. Така, більш точна, фільтрація дозволяє адміністратору мережі створювати ACL-списки, що відповідають визначеним потребам плану по забезпеченню безпеки. Розширений ACL-список розміщується ближче до адреси джерела. Завдяки аналізу по вихідній і кінцевій адресі, ACL-список дозволяє блокувати пакети, що направляються у визначену кінцеву мережу перш, ніж вони залишать вихідний маршрутизатор. Пакети фільтруються перед тим, як вони перетнуть межі мережі, що допомагає підтримувати пропускну здатність.

Крок 3. Визначення маршрутизатора та інтерфейсу, для якого буде використовуватися ACL-список.

ACL-списки розміщуються на маршрутизаторах на рівні доступу або розподілу. Адміністратор мережі повинен мати контроль над цими маршрутизаторами і можливість реалізації політики безпеки. Без доступу до маршрутизатора адміністратор мережі не зможе налаштувати на ньому ACL-список. Вибір відповідного інтерфейсу залежить від вимог до фільтрації, типу ACL-списку і місця розташування призначеного маршрутизатора. Найкраще організовувати фільтрацію трафіку перш, ніж він досягне послідовного каналу з меншою пропускною здатністю.

Крок 4. Вибір напрямку фільтрації трафіку

При виборі напрямку, для якого буде використовуватися ACL-список, необхідно розглядати потік трафіку з погляду маршрутизатора. Вхідний трафік – це трафік, що надходить в інтерфейс маршрутизатора ззовні. Маршрутизатор порівнює вхідний пакет з ACL-списком перед пошуком мережі призначення в таблиці маршрутизації. Пакети, що відкидаються в цій точці, дозволяють виключити зайві операції пошуку маршрутизатора. Це робить вхідний список контролю доступу більш ефективним для маршрутизатора, ніж вихідний. Вихідний трафік проходить через маршрутизатор по інтерфейсу. Для вихідного пакету маршрутизатор уже здійснив пошук по таблиці маршрутизації і переключив пакет на правильний інтерфейс. Пакет порівнюється з ACL-списком безпосередньо перед виходом з маршрутизатора.

Налаштування ACL-списку

Після визначення вимог, планування списку контролю доступу і визначення розташування ACL-список необхідно налаштувати. Для кожного ACL-списку необхідний унікальний ідентифікатор. Ідентифікатор може бути числом або описовим ім’ям. У нумерованих списках контролю доступу, номер визначає тип створюваного ACL-списку:

– стандартним ACL-спискам для IP-протоколу привласнюються номери з діапазону від 1 до 99 і від 1300 до 1999;

– розширеним ACL-спискам для IP-протоколу привласнюються номери з діапазону від 100 до 199 і від 2000 до 2699.

Можна також створювати ACL-списки AppleTalk і IPX.

Обмеженням для будь-якого маршрутизатора є один ACL-список для протоколу і напрямку. Якщо на маршрутизаторі IP-протокол виконується в монопольному режимі, кожен інтерфейс може обробляти максимум два ACL-списки: один для вхідного й один для вихідного трафіку. Оскільки кожен ACL-список виконує порівняння кожного пакету, що проходить через підключення, використання ACL-списків створює затримку. Налаштування списку контролю доступу охоплює два етапи: створення і застосування.

Створення списку здійснюється в режимі глобальної конфігурації. За допомогою команди access-list вводяться інструкції списку контролю доступу. Поки список контролю доступу не буде готовий всі інструкції вводяться з однаковим номером ACL-списку.

Синтаксис стандартного ACL-списку наступний:

access-list [номер списку доступу] [deny|permit] [адреса джерела] [шаблонна маска джерела][log]

Оскільки кожен пакет порівнюється з інструкцією ACL-списку до знаходження співпадіння, порядок розміщення інструкцій у ACL-списку може впливати на створювану затримку. Тому інструкції потрібно розташовувати таким чином, щоб умови, які співпадають частіше в ACL-списку передували тим, які співпадають рідше. Наприклад, інструкції зі співпадінням по найбільшому об'єму трафіку необхідно розміщувати на початку ACL-списку. При цьому варто пам'ятати, що при співпадінні пакет більше не порівнюється з іншими інструкціями в ACL-списку. Це означає, що якщо один рядок дозволяє пакет, а наступний рядок у ACL-списку забороняє його, пакет буде дозволений. Тому варто планувати ACL-список таким чином, щоб інструкції з більш визначеними вимогами розташовувалися перед інструкціями з більш загальними вимогами. Іншими словами, забороняйте доступ визначеному вузлу в мережі, дозволяючи доступ іншим у всій мережі.

Для опису функції кожного розділу або окремої інструкції ACL-списку використовується команда remark:

access-list [номер списку] remark [текст]

Для видалення ACL-списку використовується команда:

no access-list [номер списку]

Зі стандартного або розширеного ACL-списку не можна видалити один рядок. ACL-список видаляється цілком і його необхідно замінити.

Фільтрація по ACL-списку неможлива до його застосування або призначення інтерфейсу.

ACL-список потрібно присвоїти одному або кільком інтерфейсам, вказавши вхідний чи вихідний трафік. Стандартний ACL-список потрібно використовувати якнайближче до адреси призначення.

R2(config-if)#ip access-group номер списку доступу [in | out]

Наступні команди дозволяють помістити список доступу access-list 5 для інтерфейсу Fa0/0 маршрутизатора R2 з фільтрацією вхідного трафіку:

R2(config)#interface fastethernet 0/0

R2(config-if)#ip access-group 5 in

За замовчуванням ACL-список на інтерфейсі застосовується на вихідний напрямок. Незважаючи на те, що вихідний напрямок встановлений за замовчуванням, дуже важливо вказувати напрямок для уникнення плутанини і для забезпечення фільтрації трафіку в правильному напрямку. Щоб видалити ACL-список з інтерфейсу без зміни самого ACL-списку, використовується команду no ip access-group інтерфейс. Деякі команди ACL-списку дозволяють оцінити правильність синтаксису, порядок інструкцій і розміщення на інтерфейсах:

– show ip interface – виводить інформацію про IP-інтерфейс та присвоєні ACL-списки;

– show access-lists [номер списку доступу] – дозволяє вивести вміст всіх ACL-списків маршрутизатора. Ця команда також виводить на екран число співпадінь по кожній інструкції з моменту застосування ACL-списку. Щоб вивести визначений список, потрібно додати ім'я ACL-списку або номер як параметр команди;

– show running-config – виводить на екран усі налаштовані ACL-списки маршрутизатора, навіть якщо вони в даний момент не застосовані до інтерфейсу.

При використанні нумерованих ACL-списків інструкції, що вводяться після створення ACL-списку, додаються в кінець. Такий порядок може не дати очікуваних результатів. Щоб вирішити цю проблему, потрібно видалити вихідний ACL-список та створити його заново.

Часто рекомендують створювати ACL-списки в текстовому редакторі. Це дозволить легко змінювати і вставляти ACL-список у конфігурацію маршрутизатора. Однак варто пам'ятати, що при копіюванні і вставці ACL-списку важливо спочатку видалити поточний ACL-список. В протилежному випадку всі інструкції будуть додані в кінець.

Налаштування нумерованих розширених ACL-списків

Розширені ACL-списки забезпечують більші можливості контролю в порівнянні зі стандартними. Розширені ACL-списки використовуються для дозволу або заборони трафіку по IP-адресі джерела, IP-адресі призначення, типу протоколу і номерах портів. Оскільки

розширені ACL-списки можуть бути точно визначеними, їхній розмір, як правило, швидко росте. Чим більше інструкцій містить ACL-список, тим складніше ним керувати.

Для розширених ACL-списків використовуються номери списку доступу з діапазонів від 100 до 199 і від 2000 до 2699. Правила, що діють для стандартних ACL-списків, також дійсні для розширених ACL-списків:

– в одному ACL-списку варто вказувати кілька інструкцій;

– кожна інструкція повинна мати той же номер ACL-списку;

– для представлення IP-адрес варто використовувати ключові слова host чи any.

Основною відмінністю синтаксису розширеного ACL-списку є необхідність вказувати протокол після умови дозволу або заборони. Це може бути IP-протокол із вказівкою всього IP-трафіку чи фільтрації визначеного IP-протоколу, такого як TCP, UDP, ICMP, OSPF.

Часто, поставлені вимоги можна виконати багатьма різними способами.

Наприклад, у компанії є сервер з адресою 192.168.3.75. Встановлено такі вимоги:

– дозволяти доступ до вузлів у локальній мережі 192.168.2.0;

– дозволяти доступ до вузла 192.168.1.66;

– блокувати доступ до вузлів у локальній мережі 192.168.4.0;

– дозволяти доступ до інших адрес у компанії.

Для задоволення цих вимог існують, як мінімум, два рішення. При плануванні ACL-списку потрібно намагатись зменшити кількість інструкцій, якщо це можливо.

Для зменшення числа інструкцій і скорочення навантаження на обробку маршрутизатором, можна використати наступні рекомендації:

– забезпечте виявлення прохідного трафіку великого об’єму і заборону трафіку, що блокується в початкових інструкціях ACL-списку, що дозволить уникнути порівняння пакетів з інструкціями далі за списком;

– об’єднуйте декілька інструкцій в одну інструкцію за допомогою діапазонів;

– намагайтеся блокувати доступ визначеної групи замість того, щоб дозволяти його іншій групі з більшою кількістю користувачів.

Налаштування іменних ACL-списків

Програмне забезпечення Cisco IOS версії 11.2 і вище дозволяє створювати іменовані ACL-списки (NACL-списки). У NACL-списку описове ім’я замінює числові діапазони, необхідні для стандартних і розширених ACL-списків. Іменовані ACL-списки мають можливості і переваги стандартних і розширених ACL-списків, при їхньому створенні відрізняється тільки синтаксис.

Ім’я ACL-списку є унікальним. Використання прописних букв в імені дозволяє зробити список легко впізнаваним у вихідних даних команд маршрутизатора і при рішенні проблем.

Для створення іменованого ACL-списку використовується команда:

ip access-list {standard | extended} ім’я

Після виконання цієї команди маршрутизатор переключається в режим підкоманди конфігурації NACL. Після вказівки початкової команди іменування необхідно ввести по одній всі інструкції. У NACL-списках використовується синтаксис команд стандартного, чи розширеного ACL-списку з інструкцією, що дозволяє або забороняє, на початку.

Іменований ACL-список застосовується до інтерфейсу аналогічно як застосовуються стандартні чи розширені ACL-списки.

При підключенні мережевого адміністратора до віддаленого маршрутизатора за допомогою протоколу Telnet на маршрутизаторі запускається вхідний сеанс. Telnet і SSH являють собою засоби внутрішньосмугового керування і використовують IP-протокол та мережеве підключення до маршрутизатора.

Метою обмеження доступу до віртуального терміналу (VTY) є підвищення рівня безпеки мережі. Зловмисники ззовні можуть спробувати отримати доступ до маршрутизатора. Якщо на порту віртуального маршрутизатора відсутній список контролю доступу, то кожен, хто зможе визначити ім’я користувача і пароль Telnet, отримає доступ до маршрутизатора. Якщо ACL-список застосувати до порту vty-маршрутизатора, по якому

дозволяється підключення тільки з визначених IP-адрес, то будь-якому користувачу, що намагається ввійти в маршрутизатор з IP-адреси, не дозволеного ACL-списком, буде відмовлено в доступі. При цьому варто пам’ятати, що можуть виникнути труднощі, якщо адміністратору доводиться підключатися до маршрутизатора з різних місць з різних IP-адрес.

Створення списку контролю доступу для віртуального терміналу здійснюється аналогічно списку для інтерфейсу. Однак для застосування ACL-списку до каналів VTY служить інша команда. Замість команди ip access-group використовується команда access-class.

При налаштуванні списків доступу для каналів віртуального терміналу, необхідно дотримуватись наступних рекомендацій:

– для каналів віртуального терміналу варто застосовувати не іменовані, а нумеровані ACL-списки;

– створювати однакові обмеження для всіх каналів віртуального терміналу, оскільки відсутня можливість контролювати канал, який використовує користувач.

Сеанси підключення до віртуального терміналу встановлюються між клієнтським ПЗ Telnet і кінцевим маршрутизатором. Мережевий адміністратор встановлює сеанс із кінцевим маршрутизатором, вводить ім’я користувача та пароль і вносить зміни в конфігурацію.

Тема 8. Бездротові мережі

Значення бездротових технологій у сучасному суспільстві. Порівняння дротових і бездротових мереж: переваги та обмеження. Основи бездротової передачі даних: радіохвилі та принципи їх поширення, спектри частот і методи модуляції, проблеми інтерференції та завадостійкості. Класифікація бездротових мереж: PAN (Personal Area Network): Bluetooth, ZigBee, WLAN (Wireless Local Area Network): Wi-Fi, MAN (Metropolitan Area Network): WiMAX, WWAN (Wireless Wide Area Network): стільникові мережі (3G, 4G, 5G, перспективи 6G).

Стандарти IEEE 802.11 (Wi-Fi): основні версії стандартів (802.11a/b/g/n/ac/ax), механізми доступу до середовища (CSMA/CA), архітектура Wi-Fi: точки доступу, клієнти, контролери. Мобільні мережі: принципи роботи стільникових мереж, архітектура 4G та 5G, особливості використання мобільного Інтернету для IoT. Бездротові технології для IoT: LoRaWAN, NB-IoT, ZigBee.

Безпека бездротових мереж: типові загрози (перехоплення, підробка точок доступу), методи захисту: WEP, WPA, WPA2, WPA3, використання VPN у бездротовому середовищі.

Значення бездротових технологій у сучасному суспільстві

Бездротові технології стали однією з ключових основ цифрової трансформації сучасного суспільства. Вони забезпечують мобільність користувачів, гнучкість розгортання інформаційно-комунікаційної інфраструктури та масштабованість сервісів. Саме бездротовий доступ зробив можливими такі явища, як масове використання смартфонів, розвиток хмарних сервісів, Інтернет речей (IoT), розумні міста, телемедицина, дистанційне навчання та віддалену роботу [26].

У промисловості бездротові мережі використовуються для моніторингу технологічних процесів, збору телеметрії та побудови систем автоматизації. У транспорті вони забезпечують навігацію, керування потоками, взаємодію між транспортними засобами (V2V, V2X). У побуті бездротові технології інтегровані в розумні будинки, носимі пристрої та мультимедійні системи.

Таким чином, бездротові технології є фундаментом для формування цифрової економіки та інформаційного суспільства, де доступ до мережі та даних можливий у будь-який час і в будь-якому місці.

Порівняння дротових і бездротових мереж

Дротові та бездротові мережі мають різні характеристики, що визначають сфери їх ефективного застосування.

Дротові мережі традиційно забезпечують високу пропускну здатність, стабільність з'єднання та низькі затримки. Вони менш схильні до зовнішніх завад і простіші з точки зору забезпечення фізичної безпеки. Водночас їхніми обмеженнями є висока вартість прокладання кабелів, складність масштабування та відсутність мобільності.

Бездротові мережі, навпаки, характеризуються швидким розгортанням, гнучкістю та підтримкою мобільних користувачів. Вони не потребують фізичного підключення кожного пристрою, що особливо важливо для тимчасових або динамічних середовищ. Основними обмеженнями бездротових мереж є залежність якості зв'язку від умов середовища, обмеженість радіочастотного спектра, вплив інтерференції та підвищені вимоги до криптографічного захисту.

На практиці сучасні мережі здебільшого є гібридними, поєднуючи дротову магістральну інфраструктуру з бездротовими сегментами доступу.

Основи бездротової передачі даних

Бездротова передача даних ґрунтується на використанні електромагнітних хвиль, зокрема радіохвиль. Радіохвилі поширюються у просторі зі швидкістю світла та можуть відбиватися, заломлюватися, дифрагувати або поглинатися перешкодами. Якість зв'язку залежить від відстані між передавачем і приймачем, потужності сигналу, частоти, а також від характеристик навколишнього середовища [13, 27].

У реальних умовах поширення сигналу супроводжується багатопроменевістю, коли сигнал доходить до приймача кількома шляхами з різними затримками, що може спричиняти інтерференційні спотворення.

Радіочастотний спектр є обмеженим ресурсом і регулюється на міжнародному та національному рівнях. Для бездротових мереж використовуються як ліцензовані, так і неліцензовані діапазони. Наприклад, Wi-Fi працює переважно в неліцензованих діапазонах 2,4 ГГц, 5 ГГц та 6 ГГц.

Для передавання інформації застосовуються різні методи модуляції, зокрема амплітудна, частотна та фазова модуляція, а також їхні цифрові різновиди, такі як QPSK, QAM різних порядків. Сучасні системи використовують ортогональне частотне мультиплексування (OFDM), що дозволяє підвищити спектральну ефективність і завадостійкість.

Інтерференція виникає внаслідок накладання сигналів від різних джерел, що працюють в одному або суміжних частотних діапазонах. Для підвищення завадостійкості застосовуються методи кодування з виправленням помилок, адаптивний вибір модуляції та потужності, просторове різноманіття і технології MIMO.

Класифікація бездротових мереж

PAN – персональні мережі. Персональні бездротові мережі призначені для з'єднання пристроїв на невеликих відстанях. Технологія Bluetooth широко використовується для підключення гарнітур, периферійних пристроїв та носимої електроніки. ZigBee орієнтована на енергоефективні сенсорні мережі та автоматизацію, зокрема в системах «розумного дому».

WLAN – локальні бездротові мережі. WLAN, реалізовані на основі технології Wi-Fi, забезпечують бездротовий доступ до локальних і глобальних мереж у межах будівель або кампусів. Вони є основою корпоративних і домашніх мереж доступу.

MAN – міські мережі. MAN охоплюють значні території міста або регіону. Прикладом є технологія WiMAX, яка розроблялася для широкосмугового бездротового доступу на великих відстанях.

WWAN – глобальні бездротові мережі. WWAN базуються на стільникових технологіях. Мережі 3G забезпечили мобільний доступ до Інтернету, 4G (LTE) значно підвищили швидкість і зменшили затримки, а 5G орієнтовані на ультранизькі затримки, високу щільність підключень та підтримку IoT. Перспективи 6G пов'язані з використанням терагерцового діапазону, інтеграцією штучного інтелекту та підтримкою голографічних і тактильних сервісів.

Стандарти IEEE 802.11 (Wi-Fi)

Сімейство стандартів IEEE 802.11 визначає фізичний і канальний рівні WLAN. Початкові версії 802.11a/b/g забезпечували швидкості до десятків Мбіт/с. Стандарти 802.11n і 802.11ac запровадили MIMO та ширші канали, а 802.11ax (Wi-Fi 6) орієнтований на ефективну роботу в умовах високої щільності клієнтів.

Доступ до середовища реалізується за допомогою механізму CSMA/CA, який мінімізує колізії шляхом прослуховування каналу та використання випадкових затримок. Архітектура Wi-Fi мереж включає точки доступу, клієнтські пристрої та, у корпоративних середовищах, бездротові контролери для централізованого управління.

Мобільні мережі та IoT

Стільникові мережі базуються на поділі території на комірки, кожна з яких обслуговується базовою станцією. У 4G архітектура спрощена та орієнтована на пакетну передачу даних. 5G вводить сервісно-орієнтовану архітектуру, мережеву віртуалізацію та механізм network slicing.

Для IoT особливо важливими є технології з низьким енергоспоживанням і великим радіусом дії. До них належать LoRaWAN, NB-IoT та ZigBee, які дозволяють підключати тисячі сенсорів і пристроїв з мінімальними витратами енергії.

Бездротові мережі є більш уразливими до атак через відкритість середовища передавання. Типові загрози включають перехоплення трафіку, підробку точок доступу, атаки типу «людина посередині».

Для захисту використовуються криптографічні механізми. Ранні стандарти WEP виявилися ненадійними. WPA та WPA2 значно підвищили рівень безпеки, а WPA3 забезпечує захист від перебору паролів і покращене шифрування. Додатковим рівнем захисту є використання VPN, що забезпечує конфіденційність і цілісність даних у бездротовому середовищі.

Бездротові технології є невід'ємною складовою сучасних комп'ютерних мереж. Їх розвиток визначає можливості мобільного доступу, масштабування сервісів та впровадження нових цифрових рішень.

Тема 9. Глобальні мережі

Поняття глобальних мереж та їхня відмінність від локальних і регіональних мереж. Історичні передумови розвитку глобальних мереж (ARPANET, NSFNET, Internet). Архітектура та основні принципи побудови глобальних мереж. Базові компоненти: маршрутизатори, магістральні канали, точки обміну трафіком. Принцип багаторівневої ієрархії у структурі Інтернету. Провайдери та автономні системи. Технології глобальних мереж. Волоконно-оптичні лінії та підводні кабелі. Супутникові системи зв'язку. Мобільні технології (4G, 5G, перспективи 6G). Хмарні інфраструктури та розподілені обчислення як частина глобальних мереж. Протоколи та стандарти глобальних мереж. TCP/IP як універсальна основа. BGP (Border Gateway Protocol) і його роль у маршрутизації між автономними системами. DNS як глобальна служба імен. Системи управління адресним простором (IANA, ICANN, RIR). Забезпечення якості та безпеки у глобальних мережах. QoS (Quality of Service) у глобальних каналах. Загрози і виклики безпеці (DDoS-атаки, міжмережеві атаки, проблеми конфіденційності). Засоби захисту: VPN, шифрування, міжмережеві екрани, глобальні системи моніторингу. Концепція «Інтернету майбутнього». Інтернет речей (IoT) на глобальному рівні. Використання штучного інтелекту в управлінні глобальними мережами. Роль глобальних мереж у сучасному інформаційному суспільстві.

Глобальні комп'ютерні мережі є фундаментальною складовою сучасної інформаційної інфраструктури, що забезпечує об'єднання мільярдів пристроїв, користувачів і сервісів у єдиний комунікаційний простір. Вони суттєво відрізняються від локальних і регіональних мереж не лише за масштабами, а й за принципами побудови, управління, протоколами та соціально-економічною роллю.

Під глобальними мережами розуміють мережі зв'язку, які охоплюють значні географічні простори − країни, континенти або всю планету − і забезпечують передачу даних між віддаленими вузлами з використанням різноманітних телекомунікаційних технологій. На відміну від локальних мереж (LAN), що функціонують у межах будівлі або кампусу та перебувають під управлінням однієї організації, і регіональних або міських мереж (MAN), які обслуговують обмежену територію, глобальні мережі не мають єдиного централізованого власника чи адміністратора. Їхня робота ґрунтується на взаємодії багатьох незалежних операторів, провайдерів і автономних систем, об'єднаних спільними протоколами та правилами маршрутизації.

Історичні передумови розвитку глобальних мереж пов'язані з потребами наукових і військових структур у надійних системах обміну інформацією. Першим прообразом сучасного Інтернету стала мережа ARPANET, створена наприкінці 1960-х років у США в рамках проєктів Агентства передових оборонних досліджень (ARPA). Основною ідеєю ARPANET було впровадження пакетної комутації, що дозволяло зберігати працездатність мережі навіть у разі виходу з ладу окремих вузлів. У 1980-х роках подальший розвиток отримала мережа NSFNET, яка об'єднала університетські та дослідницькі центри і стала основною магістраллю для академічного Інтернету. Саме на базі цих ініціатив сформувався Internet − глобальна мережа мереж, що використовує єдиний стек протоколів TCP/IP і згодом стала доступною для комерційного та масового використання.

Архітектура глобальних мереж характеризується високим рівнем децентралізації та масштабованості. Її основу становить ієрархічна модель, у якій виділяють рівні доступу, агрегації та магістралі. На рівні доступу розташовані кінцеві користувачі та корпоративні мережі, які підключаються до провайдерів через різні технології − оптоволоконні, бездротові чи мобільні. Рівень агрегації об'єднує трафік від численних мереж доступу, оптимізує маршрути та забезпечує резервування каналів. Магістральний рівень формують високопродуктивні маршрутизатори та канали зв'язку надвисокої пропускної здатності, які передають дані між регіонами та континентами.

Ключовими компонентами глобальних мереж є маршрутизатори, що виконують інтелектуальну пересилку пакетів між мережами, магістральні канали зв'язку, здебільшого побудовані на основі волоконно-оптичних технологій, а також точки обміну інтернет-

трафіком (IXP). Останні відіграють особливо важливу роль, оскільки дозволяють провайдерам обмінюватися трафіком без залучення сторонніх магістральних операторів, зменшуючи затримки та фінансові витрати.

Структура Інтернету базується на концепції автономних систем − логічно та адміністративно незалежних мереж, кожна з яких має унікальний ідентифікатор ASN і власну політику маршрутизації. Автономні системи можуть належати інтернет-провайдерам, великим корпораціям, хмарним платформам або державним установам. Взаємодія між ними забезпечується спеціальними міждоменними протоколами, що дозволяють координувати маршрути передачі даних у глобальному масштабі.

Технологічною основою глобальних мереж є передусім волоконно-оптичні лінії зв'язку, які забезпечують надзвичайно високу пропускну здатність, низький рівень затримок і стійкість до електромагнітних завад. Особливе значення мають підводні оптичні кабелі, що з'єднують континенти та забезпечують основний обсяг міжконтинентального трафіку. Доповненням до них є супутникові системи зв'язку, які застосовуються для покриття віддалених або важкодоступних регіонів, а також у мобільних і резервних каналах передачі даних. У сучасних умовах важливу роль відіграють мобільні технології четвертого та п'ятого поколінь, які забезпечують високошвидкісний доступ до глобальних мереж з мінімальною затримкою. Перспективи розвитку 6G пов'язують із подальшим зростанням швидкостей, інтеграцією штучного інтелекту та підтримкою масових кіберфізичних систем.

Суттєвим елементом глобальних мереж стали хмарні інфраструктури та розподілені обчислення. Великі дата-центри, географічно розподілені по всьому світу, формують глобальні платформи зберігання та обробки даних, забезпечуючи доступність сервісів незалежно від місця перебування користувача. Хмарні сервіси тісно інтегровані з мережевою інфраструктурою та фактично є її логічним продовженням.

Функціонування глобальних мереж неможливе без уніфікованих протоколів і стандартів. Стек TCP/IP є універсальною основою Інтернету, забезпечуючи адресацію, маршрутизацію та надійну передачу даних. Особливе місце посідає протокол BGP, який використовується для обміну маршрутною інформацією між автономними системами та визначає шляхи поширення трафіку у глобальному масштабі. Не менш важливою є система доменних імен DNS, що реалізує розподілену ієрархічну службу перетворення символьних імен у IP-адреси. Управління адресним простором і доменними зонами здійснюється міжнародними організаціями IANA та ICANN у взаємодії з регіональними інтернет-реєстрами.

Одним із ключових викликів для глобальних мереж є забезпечення якості обслуговування та безпеки. QoS у глобальних каналах передбачає механізми пріоритизації трафіку, керування затримками, втратами пакетів і пропускною здатністю, що особливо важливо для мультимедійних та критично важливих сервісів. Водночас глобальні мережі є мішенню для численних загроз, зокрема розподілених атак відмови в обслуговуванні, міжмережевих атак і порушень конфіденційності даних. Для протидії цим загрозам застосовуються VPN-технології [28], криптографічні методи шифрування, міжмережеві екрани, системи виявлення вторгнень і глобальні платформи моніторингу мережевого трафіку.

Перспективи розвитку глобальних мереж пов'язують із концепцією «Інтернету майбутнього», що передбачає інтеграцію мільярдів пристроїв Інтернету речей на глобальному рівні, розвиток кіберфізичних систем і використання штучного інтелекту для автоматизованого управління мережами. Алгоритми машинного навчання вже сьогодні застосовуються для прогнозування перевантажень, оптимізації маршрутизації та виявлення аномалій у мережевому трафіку.

Таким чином, глобальні мережі відіграють ключову роль у сучасному інформаційному суспільстві, забезпечуючи основу для цифрової економіки, науки, освіти, державного управління та міжнародної комунікації. Їхній розвиток визначає не лише технічний прогрес, а й трансформацію соціальних процесів, формуючи нову глобальну інформаційну реальність.

Тема 10. Віртуалізація та автоматизація роботи мережі

Потреба у віртуалізації та автоматизації в умовах зростання складності мереж. Еволюція від традиційних до програмно-керованих мереж. Поняття віртуалізації мереж: віртуалізація як відокремлення апаратного та логічного рівнів, Network Functions Virtualization (NFV): заміна апаратних рішень віртуальними функціями, віртуалізація мережевих пристроїв: віртуальні маршрутизатори, комутатори, міжмережеві екрани. Технології віртуалізації мереж: віртуальні локальні мережі (VLAN) та оверлейні мережі (VXLAN), віртуальні приватні мережі (VPN) як форма віртуалізації каналів зв'язку, використання гіпервізорів та контейнерних платформ (VMware, KVM, Docker, Kubernetes). Програмно-конфігуровані мережі (SDN): архітектура SDN: контрольний і дата-площини, контролери SDN (OpenDaylight, Ryu, ONOS), протокол OpenFlow як основа для централізованого управління.

Потреба у віртуалізації та автоматизації в умовах зростання складності мереж [29]

Сучасні комп'ютерні мережі зазнають стрімкого ускладнення внаслідок зростання обсягів переданих даних, кількості підключених пристроїв, поширення хмарних сервісів, мобільних технологій та Інтернету речей. Традиційні підходи до проєктування та адміністрування мереж, засновані на ручному налаштуванні фізичного обладнання, дедалі частіше виявляються недостатньо гнучкими, масштабованими та економічно ефективними. У таких умовах виникає об'єктивна потреба у впровадженні механізмів віртуалізації та автоматизації, які дозволяють зменшити залежність мережевих сервісів від апаратної інфраструктури, підвищити швидкість розгортання нових послуг і забезпечити централізоване управління мережею.

Автоматизація мережевих процесів зумовлена необхідністю мінімізації людського фактора, зменшення кількості помилок конфігурації та підвищення оперативності реагування на інциденти. Віртуалізація, у свою чергу, створює передумови для логічного поділу мережі на ізольовані сегменти, ефективного використання ресурсів та швидкого масштабування без фізичної модернізації обладнання.

Еволюція від традиційних до програмно-керованих мереж

Традиційні мережі будувалися за принципом тісної інтеграції апаратного та програмного забезпечення. Мережеві пристрої, такі як маршрутизатори й комутатори, поєднували в собі функції керування та пересилання даних, що ускладнювало централізоване управління та автоматизацію. Кожен пристрій конфігурувався окремо, що при великих масштабах мережі призводило до значних витрат часу та ресурсів.

Подальша еволюція мережевих технологій зумовила перехід до концепції програмно-керованих мереж, у яких логіка управління відокремлюється від процесів передачі даних. Це дозволило реалізувати нові підходи до адміністрування, засновані на централізованому контролі, політиках та програмному інтерфейсі управління мережею.

Поняття віртуалізації мереж

Віртуалізація мережі полягає у відокремленні логічного рівня мережевих функцій від фізичної апаратної інфраструктури. Такий підхід дає змогу створювати декілька логічно ізольованих мереж поверх спільних фізичних ресурсів. Кожна віртуальна мережа може мати власну топологію, адресний простір, правила маршрутизації та політики безпеки.

Ключовою ідеєю мережевої віртуалізації є абстрагування апаратних компонентів, що спрощує управління мережею та дозволяє швидко адаптувати її до змінних вимог бізнесу або навчального середовища.

Network Functions Virtualization (NFV)

Технологія Network Functions Virtualization спрямована на заміну традиційних апаратних мережевих рішень програмними реалізаціями, які виконуються у віртуальному середовищі. До таких функцій належать маршрутизація, міжмережеве екранування, балансування навантаження, системи виявлення вторгнень та інші мережеві сервіси.

NFV дозволяє розгортати мережеві функції у вигляді віртуальних машин або контейнерів на стандартному серверному обладнанні. Це значно знижує капітальні витрати, підвищує гнучкість масштабування та спрощує оновлення мережевих сервісів.

Віртуалізація мережевих пристроїв

Віртуалізація мережевих пристроїв передбачає створення програмних аналогів фізичних маршрутизаторів, комутаторів і міжмережевих екранів. Віртуальні маршрутизатори забезпечують маршрутизацію трафіку між логічними сегментами мережі, підтримуючи стандартні протоколи динамічної маршрутизації. Віртуальні комутатори виконують функції комутації на другому рівні моделі OSI та широко використовуються у хмарних і віртуалізованих середовищах. Віртуальні міжмережеві екрани дозволяють реалізувати політики безпеки без прив'язки до конкретного фізичного пристрою.

Технології віртуалізації мереж

Однією з базових технологій мережевої віртуалізації є віртуальні локальні мережі (VLAN), які дозволяють логічно сегментувати мережу на рівні канального шару незалежно від фізичного розташування пристроїв. VLAN забезпечують ізоляцію трафіку та підвищують рівень безпеки і керованості мережі.

Оверлейні мережі, зокрема VXLAN, розширюють можливості VLAN, дозволяючи створювати віртуальні мережі поверх IP-інфраструктури з підтримкою значно більшої кількості сегментів. VXLAN інкапсулює кадри другого рівня в пакети третього рівня, що робить можливим масштабування мереж у хмарних дата-центрах.

Віртуальна приватна мережа

Віртуальні приватні мережі VPN (скорочення від англ. virtual private network) є формою віртуалізації каналів зв'язку та забезпечують захищене передавання даних через публічні мережі. VPN дозволяють логічно об'єднувати віддалені сегменти мережі, створюючи ілюзію єдиного захищеного середовища.

Використання гіпервізорів і контейнерних платформ

Гіпервізори, такі як VMware ESXi або KVM, забезпечують виконання декількох віртуальних машин на одному фізичному сервері, що є основою для реалізації NFV та віртуальних мережевих пристроїв. Контейнерні платформи, зокрема Docker і Kubernetes, дозволяють розгортати мережеві сервіси у вигляді легковагових ізольованих контейнерів, що підвищує швидкість запуску та ефективність використання ресурсів.

Kubernetes відіграє важливу роль в автоматизації управління контейнеризованими мережевими функціями, забезпечуючи масштабування, балансування навантаження та відмовостійкість.

Програмно-конфігуровані мережі (SDN)

Програмно-конфігуровані мережі є логічним продовженням ідей віртуалізації та автоматизації. Основною особливістю SDN є розділення контрольної площини та площини передачі даних. Контрольна площина відповідає за прийняття рішень щодо маршрутизації та політик, тоді як дата-площина здійснює безпосередню пересилку пакетів.

Централізований SDN-контролер керує мережею через програмні інтерфейси, забезпечуючи глобальне бачення топології та стану мережі. До найпоширеніших контролерів належать OpenDaylight, Ryu та ONOS, які використовуються як у навчальних, так і в промислових середовищах.

Протокол OpenFlow

Протокол OpenFlow є одним з ключових елементів архітектури SDN і забезпечує взаємодію між SDN-контролером та мережевими пристроями. За допомогою OpenFlow контролер може динамічно змінювати правила обробки трафіку в комутаторах, визначати шляхи проходження пакетів та реалізовувати складні політики управління мережею.

Застосування OpenFlow дозволяє реалізувати централізоване, програмне та гнучке управління мережею, що є критично важливим для сучасних хмарних і масштабованих інфраструктур.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Класифікація комп'ютерних мереж URL: https://mozok.click/736-klasifkacya-kompyuternih-merezh.html (дата звернення: 15.03.2025).
2. Мережні топології. StudFiles. URL: https://studfile.net/preview/7446861/page:9/ (дата звернення: 22.03.2025).
3. Dr. Y Mohana Roopa Mr. P Ravinder Ms. N M Deepika URL: http://surl.li/eoivu (дата звернення: 30.03.2025)
4. Інформаційний портал Технічного фахового коледжу. URL: https://e-tk.lntu.edu.ua/pluginfile.php/26868/mod_resource/content/0/Тема%202.%20Середовища%20передачі%20даних%20в%20комп'ютерних%20мережах.pdf (дата звернення: 30.03.2026).
5. Tanenbaum A. et al. Computer Networks Title: Computer Networking: A Top-Down Approach. URL: https://csc-knu.github.io/sys-prog/books/Andrew%20S. %20Tanenbaum%20-%20Computer%20Networks.pdf (дата звернення: 04.04.2025).
6. Костюченко А.О., Цибко Г.Ю. Адресація в комп'ютерних мережах: навчально-методичний посібник. URL: http://erpub.chnpu.edu.ua:8080/jspui/bitstream/
123456789/7842/1/Adresatsiia_v_kompjuternykh_merezhakh_2021.pdf (дата звернення: 05.04.2025).
7. Комп'ютерні мережі. Книга 1: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. Львів: «Магнолія 2006», 2023. 256 с.
8. Комп'ютерні мережі. Книга 2: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. Львів: «Магнолія 2006», 2023. 312 с.
9. Буров Є.В., Митник М.М. Комп'ютерні мережі. Підручник. Том 1. Львів: «Магнолія 2006», 2021. 340 с.
10. Комп'ютерні мережі. Підручник. Том другий /Є.В. Буров, М.М. Митник/ Львів: Видавництво ПП «Магнолія 2006», 2024. 204 с.
11. Курс Мережевої академії Cisco CCNA: Introduction to Networks URL: https://www.netacad.com/courses/networking/ccna-introduction-networks (дата звернення: 10.04.2025).
12. Курс Мережевої академії Cisco CCNA: Switching, Routing, and Wireless Essentials URL: https://www.netacad.com/courses/networking/ccna-switching-routing-wireless-essentials (дата звернення: 18.04.2025).
13. Курс Мережевої академії Cisco CCNA: Enterprise Networking, Security, and Automation URL: https://www.netacad.com/courses/ccna-enterprise-networking-security-automation?courseLang=en-US (дата звернення: 25.04.2025).
14. Wireshark User's Guide. Wireshark. Go Deep. URL: https://www.wireshark.org/docs/wsug_html_chunked/?utm_source=chatgpt.com (date of access: 26.04.2025).
15. Computer networking: a top-down approach / James F. Kurose, University of Massachusetts, Amherst, https://networking.harshkapadia.me/files/books/computer-networking-a-top-down-approach-8th-edition.pdf (дата звернення: 27.04.2025)
16. Задерейко О. В., Багнюк Н.В., Толокнов А. А. Комп'ютерні мережі: навчально-методичний посібник для підготовки здобувачів вищої освіти галузі знань 12 «Інформаційні технології». 2023. URL: http://hdl.handle.net/11300/25951 (дата звернення: 30.04.2025).
17. NetAcademy - Networking101Lite Перша сесія «Модель OSI/Мережі/Базові налаштування обладнання». URL: http://surl.li/eoiux (дата звернення: 03.05.2025)
18. Networking101Lite Друга сесія «Другий (канальний) рівень OSI моделі. Ethernet. Комутація. VLAN». URL: http://surl.li/eoiuy (дата звернення: 05.05.2025)
19. Networking101Lite Третя сесія «Третій (мережевий) рівень OSI моделі. IP. Маршрутизація». URL: http://surl.li/eoiuz (дата звернення: 09.05.2025)
20. Networking101Lite Сесія №4 «Динамічне назначення IP адрес. DHCP». URL: http://surl.li/eoivc (дата звернення: 12.05.2025)
21. Networking101Lite Сесія №9 «Динамічна маршрутизація/OSPF URL: http://surl.li/eoivq (дата звернення: 23.05.2025)

22. Networking101Lite Сесія №10 «Динамічна маршрутизація/bgp». URL: http://surl.li/eoivr (дата звернення: 27.05.2025)

23. Networking101Lite Сесія №5 «Мережева взаємодія. Сокети. Утиліти для мережевого інженера». URL: http://surl.li/eoive (дата звернення: 15.05.2025)

24. Networking101Lite Сесія №6 «Контроль трафіку. Списки доступу. Налаштування контролю». URL: http://surl.li/eoivg (дата звернення: 18.05.2025)

25. Networking101Lite Сесія №7 «Трансляція IP адрес. Доступ в Інтернет. NAT». URL: http://surl.li/eoivi (дата звернення: 20.05.2025)

26. Все, що потрібно знати про бездротові мережі WLAN: побудова, безпека та керування - Netwave - Netwave. Netwave. URL: https://netwave.ua/blog/vse-shcho-potribno-znaty-pro-bezdrotovi-merezhi-wlan-pobudova-bezpeka-ta-keruvannya/ (дата звернення: 20.05.2025).

27. Бездротові методи передачі інформації. StudFiles. URL: https://studfile.net/preview/14570700/ (дата звернення: 21.05.2025).

28. Networking101Lite Сесія №8 «VPN/Захист даних при передачі/IPSec». URL: http://surl.li/eoivm (дата звернення: 21.05.2025)/

29. Що таке віртуалізація?, 2023. YouTube. URL: https://www.youtube.com/watch?v=wZxgSPICJVI (дата звернення: 23.05.2025).

Для нотаток

К17 Комп’ютерні мережі: конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Комп’ютерна інженерія» галузі знань 12 (F) Інформаційні технології спеціальності 123 (F7) Комп’ютерна інженерія денної та заочної форм навчання / уклад. Н. В. Багнюк, Д. В. Гордєєва. Луцьк: ЛНТУ, 2026. 116 с.

Конспект лекцій з дисципліни «Комп’ютерні мережі» складено відповідно до діючої програми курсу.

Призначено для здобувачів вищої освіти спеціальності 123 (F7) Комп’ютерна інженерія освітньої програми «Комп’ютерна інженерія».

Комп’ютерний набір Н. В. Багнюк

Редактор Н. В. Багнюк

Підп. до друку «___» _____ 2026р.

Формат 60х84/16. Папір офс. Гарнітура Таймс.

Ум. друк. арк. ____. Тираж 10 прим. Зам. ____

Відділ іміджу та промоцій

Луцького національного технічного університету

43018, м. Луцьк, вул. Львівська, 75