Тема 18. Віртуальні мережі

VLAN (Virtual Local Area Network – віртуальна локальна комп'ютерна мережа) – є групою хостів з загальним набором вимог, що взаємодіють так, ніби вони приєднані до одного домену, незалежно від їх фізичного розташування. VLAN має ті самі атрибути, як і фізична локальна мережа, але дозволяє кінцевим станціям бути згрупованими разом, навіть якщо вони не перебувають на одному мережевому комутаторі. Реконфігурація мережі може бути зроблена за допомогою програмного забезпечення замість фізичного переміщення пристроїв.

VLAN, які створені, щоб забезпечити послуги сегментації, зазвичай надаються маршрутизаторами в конфігурації локальної мережі. VLAN, розглядають такі питання, як масштабованість, безпека та керування мережею. Маршрутизатори в топологіях VLAN забезпечують фільтрацію, безпеку, узагальнення адрес та керування трафіком. За визначенням, комутатори не можуть з'єднувати IP-трафік між мережами VLAN, оскільки це буде порушенням цілісності широкомовного домену VLAN.

Це також корисно, якщо хтось хоче створити кілька мереж 3-го рівня на тому ж комутаторі 2 рівня. Наприклад, якщо сервер DHCP (який буде перевіряти його наявність) підключений до комутатора він буде обслуговувати будь-який вузол, який налаштований на отримання свого IP від сервера DHCP. За допомогою віртуальних локальних мереж можна легко розділити мережу так, щоб вузли не використовували цей сервер DHCP і отримували локальні адреси, або отримували адресу з іншого серверу DHCP.

Віртуальні локальні мережі 2-го рівня конструкції є важливими, порівняно з IP-підмережами, які є конструкціями 3-го рівня. При використанні VLAN, можна керувати пакетами трафіку і швидко реагувати на переміщення. Мережі VLAN забезпечують гнучкість, щоб адаптуватися до змін у мережі вимогам і дозволяють спрощене адміністрування.

Можливості, які надають віртуальні мережі:

- логічний поділ комутатора на кілька мереж, що не об’єднані між собою.
- створення такого поділу на мережі з двома або більше комутаторами без вимоги проведення додаткових кабелів.
- асиметричні VLAN. У цьому випадку порт (не trunk, по кабелю рухаються кадри без тегу 802.1Q) підключений до однієї внутрішньої VLAN комутатора по вхідних кадрах (вона називається PVID), і до більш ніж однієї внутрішньої VLAN комутатора по вихідних кадрах. При цьому може бути не підключено вихідні кадри до PVID VLAN.
- через попередній пункт реалізується більш високорівнева абстракція – Promiscuous/Community/Isolated порти. У цьому випадку використовується логічне вкладення кількох вторинних VLAN в одну первинну.
- Promiscuous порт (порт на первинній VLAN) може спілкуватися з будь-яким Promiscuous/Community/Isolated портом як у первинній, і будь-якій вкладеній в неї вторинній VLAN.
- Community порт (порт на вторинній VLAN) може спілкуватися з будь-яким Promiscuous портом, а також з будь-яким Community портом в межах своєї вторинної VLAN.
- Isolated порт (також порт на вторинній VLAN, але це спеціальна isolated VLAN, яка може бути тільки одна в даній первинній VLAN) може спілкуватися тільки з Promiscous портами, і не може спілкуватися навіть з іншими Isolated портами (функціонал «всі клієнти бачать сервер і не бачать один одного», часто використовується в «гостьових» Wi-Fi мережах).
- дворівневе вкладення VLAN міток в кадр, а також трансляція значень міток «на льоту». Ця технологія називається QinQ, і підтримується не у всіх пристроях з підтримкою VLAN

У пристроях Cisco протокол VTP (VLAN Trunking Protocol) передбачає VLAN-домени для спрощення адміністрування. VTP також виконує «чистку»

трафіку, спрямовуючи VLAN трафік тільки на ті комутатори, які мають цільові VLAN-порти (функція VTP pruning). Комутатори Cisco в основному використовують протокол 802.1Q Trunk замість застарілого пропрієтарного ISL (Inter-Switch Link) для забезпечення сумісності інформації.

За замовчанням на кожному порті комутатора є мережа VLAN1 або VLAN керування. Мережа керування не може бути видалена, однак можуть бути створені додаткові мережі VLAN і цим альтернативним VLAN можуть бути додатково призначені порти.

Native VLAN – це параметр кожного порту, який визначає номер VLAN, який одержують усі непомічені (untagged) пакети.

В Cisco використовується наступна термінологія портів:

- access port – порт, що належить одній VLAN і передає нетегований трафік. За специфікацією cisco, access порт може належати лише одній VLAN, за замовчуванням це перша (нетегована) VLAN. Будь-який кадр, який проходить через access порт, позначається номером, що належить цій VLAN.
- trunk port – порт, що передає тегований трафік одного або декількох VLAN. Цей порт, навпаки, не змінює тег, лише пропускає кадри з тегами, які дозволено цьому порту.

Щоб передати через порт трафік кількох VLAN, порт переводиться у режим транка.

Режими інтерфейсу (за замовчуванням залежить від моделі комутатора):

- auto – порт знаходиться в автоматичному режимі і буде переведений у стан trunk тільки якщо порт на іншому кінці знаходиться в режимі on або desirable. Тобто якщо порти на обох кінцях знаходяться в режимі «auto», то trunk не застосовуватиметься.
- desirable – порт знаходиться в режимі «готовий перейти в стан trunk»; періодично передає DTP-кадри порту на іншому кінці, запитуючи віддалений порт перейти у стан trunk (стан trunk буде встановлено, якщо порт на іншому кінці перебуває у режимі on, desirable, чи auto).

– trunk – порт постійно знаходиться у стані trunk, навіть якщо порт на іншому кінці не підтримує цей режим.
– nonegotiate – порт готовий перейти в режим trunk, але не передає DTP-кадри порту на іншому кінці. Цей режим використовується для запобігання конфліктам з іншим не-cisco обладнанням. У цьому випадку комутатор на іншому кінці має бути вручну налаштований на використання trunk'a.

За промовчанням у транці дозволені всі VLAN. Для того, щоб через відповідний VLAN у транці передавалися дані, як мінімум, необхідно щоб VLAN був активним. Активним VLAN стає тоді, коли він створений на комутаторі і в ньому є хоча один порт в стані up/up.

Підтримка VLAN в Windows надається як частина Hyper-V (самі віртуальні машини створювати не обов'язково) або як частина технології NIC Teaming (також званої LBFO), яка аналогічна interface bonding в Linux.

Підтримка VLAN у Hyper-V:

– вимагає використання команд PowerShell, GUI для керування відсутня
– обов’язково використовує pseudo-Ethernet адаптери зі своїми «несправжніми» MAC-адресами, різні VLAN можуть бути виведені тільки на різні MAC-адреси.