TECHNOLOGIA

Mikro i makro świata sieci VLAN

netbloger
(wykładowca WSEI)

Wstęp

Cel i zakres publikacji

Celem poniższej publikacji jest przedstawienie jak na przestrzeni ostatnich kilkudziesięciu lat zmieniało się podejście do tzw. VLAN'ów jakie wynikały z tego problemy i jak je rozwiązywano.

Zacznijmy od podania definicji sieci VLAN. Jak podaje źródło Wikipedia w wersji angielskojęzycznej jest to:
„A virtual local area network (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).”[1],

Sieć VLAN rozumiemy jako logiczną reprezentację fizycznego obszaru sieci komputerowej, który jest ograniczony za pomocą tzw. domeny rozgłoszeniowej w drugiej warstwie modelu OSI.
Zwróćmy uwagę, że sieć VLAN nie jest ograniczona w żaden sposób przez medium, która je realizuje, ale tylko i wyłącznie przez tzw. domenę rozgłoszeniową, a ta z kolei jest zdefiniowana przez zbiór wzajemnie połączonych ze sobą urządzeń warstwy L1, L2; hubów, czy przełączników.

Rys historyczny

Na przestrzeni ostatnich kilkudziesięciu lat definicja VLAN'u oraz sposób podejścia do implementacji VLAN'u uległa radykalnym zmianom. Zanim przejdziemy do konkretnych przykładów chciałbym żebyśmy odpowiedzieli sobie na fundamentalne pytanie:

W jakim celu stosujemy sieci VLAN?

Są dwa powody. Po pierwsze aby zapewnić izolacje w warstwie drugiej modelu OSI pomiędzy tzw. sieciami/segmentami sieci. [2]
Po drugie aby ograniczyć rozmiar tzw. domeny rozgłoszeniowej [3].

Oba pojęcia wyjaśnię w dalszej części publikacji oraz przedstawię jaką odgrywają rolę z punktu widzenia sieci VLAN.

Musimy pamiętać, że do początku lat 80'ych ubiegłego wieku nie istniało pojęcie sieci VLAN, a co za tym idzie budowano sieci komputerowe bez ograniczenia ze względu na rozmiar domeny rozgłoszeniowej, gdyż fizycznie sieć realizowana była w oparciu o urządzenia warstwy pierwszej modelu OSI tzw. hub'y.

Dygresja: Można by stwierdzić odnosząc się do sieci z początku lat 80'tych, które chcielibyśmy zrealizować na współczesnym sprzęcie, że byłyby one oparte na jednym i jedynym VLAN'ie z punktu widzenia rozmiaru domeny rozgłoszeniowej.

Sieci w owym czasie budowano w zależności od liczby podpiętych urządzeń końcowych /ograniczmy się tutaj w naszych rozważaniach do sieci typu Ethernet/ w oparciu o grupy urządzeń warstwy L1 budując tzw. gwiazdę z centralnym węzłem lub tzw. Rozszerzoną gwiazdę z kilkoma węzłami centralnymi, ale zawsze węzłem centralnym był na owe czasy hub, który z racji swojej definicji pracował tylko i wyłącznie w warstwie fizycznej nie rozumiejąc wyższych warstw w szczególności warstwy drugiej czy trzeciej.
Oznacza to, że czysto teoretycznie rozważając można zbudować domenę rozgłoszeniową o nieograniczonym obszarze, a co za tym idzie nieograniczonej liczbie punktów końcowych.
Jeżeli pójdziemy dalej i pokryjemy hipotetycznych VLAN rozmiarem domeny rozgłoszeniowej to dostaniemy VLAN o nieograniczonym rozmiarze.

Co to oznacza?
Jeżeli nasze rozważania ograniczylibyśmy tylko i wyłącznie do warstwy drugiej modelu OSI i komunikacje w hipotetycznej sieci oparlibyśmy tylko i wyłącznie o adresacje w warstwie drugiej L2, czyli bazując na adresach MAC można by zbudować ogromną sieć z jedną ogromną domeną rozgłoszeniową. Jedynym wówczas ograniczeniem byłby dla nas unikalny adres MAC.

Jednakże chciałbym w tym momencie uwspółcześnić nasz rozważany model o warstwę trzecią modelu OSI i dodać do naszych rozważań adresacje IP.

Jeżeli dodamy drugi faktor w naszych rozważaniach, czyli adresacje IP i połączymy teraz oba elementy, czyli rozmiar domeny rozgłoszeniowej + adres IP dostaniemy nowy obszar dla zasięgu VLAN'ow, tym razem mocno zawężony przez liczbę możliwych unikalnych adresów IP dla danej klasy adresu IP.

Przyjrzyjmy się teraz bliżej VLAN'om, ale z użyciem tzw. klasowych adresów IP i wynikające z tego ograniczenia.

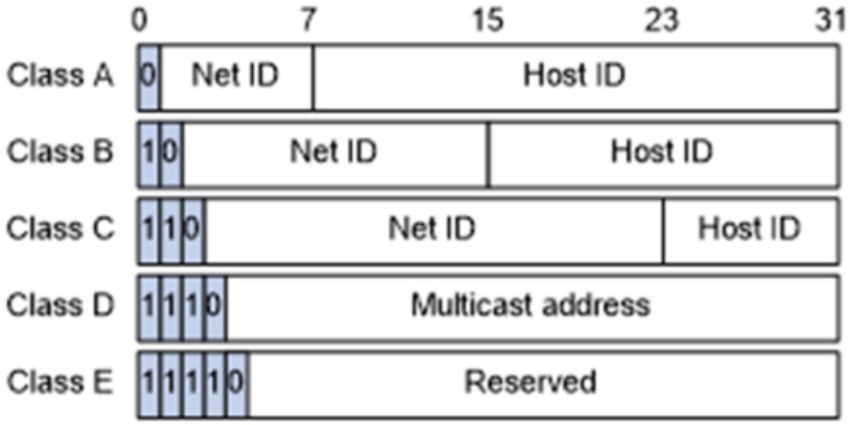
W przypadku użycia adresów IP klasy C do zbudowania sieci komputerowej możemy użyć maksymalnie 8 bitów do adresacji tzw. składowej hosta z adresu IP, co oznacza, że największa domena rozgłoszeniowa jaką możemy zbudować będzie się składała z 256 -2 = 254 hostów. Pamiętajmy, że w tym przypadku jako węzeł centralny użyjemy urządzeń, które pracują na warstwie pierwszej modelu OSI.

W przypadku użycia adresów IP klasy B do zbudowania sieci komputerowej możemy użyć maksymalnie 16 bitów do adresacji tzw. składowej hosta z adresu IP, co oznacza, że największa domena rozgłoszeniowa jaką możemy zbudować będzie się składała z 2^16 -2 hostów. Węzeł centralny zrealizowany j/w.

W przypadku użycia adresów IP klasy A do zbudowania sieci komputerowej możemy użyć maksymalnie 24 bitów do adresacji tzw. składowej hosta z adresu IP, co oznacza, że największa domena rozgłoszeniowa jaką możemy zbudować będzie się składała z 2^24 -2 hostów. Węzeł centralny zrealizowany j/w.

Możemy łatwo zaobserwować, że podczas nałożenia na VLAN adresacji IP w tym przypadku klasowej adresacji IP znacząco zawęziliśmy rozmiar domeny rozszerzeniowej, a co z tym idzie obszar pokrycia przez VLAN.

Podsumowując VLAN'y vs IP adresacje:
Jak można się domyślać obszar pokrycia VLAN'ów jest jedynie ograniczony poprzez urządzenia warstwy pierwszej, czy drugiej użyte do budowy sieci. Jeżeli nałożymy do tego kolejną warstwę w postaci adresacji IP dostajemy nowy obszar ograniczony w swoim zasięgu tak naprawdę przez rozmiar adresacji możliwy do pokrycie przez tzw. składową hosta w adresie IP



RYS.1. OBRAZUJĄCY ADRES IP DANEJ KLASY W KONTEKŚCIE LICZBY MOŻLIWYCH DO ZAADRESOWANIA HOSTÓW W SIECI, KTÓRA ODPOWIADA WPROST ROZMIAROWI TZW. DOMENY ROZGŁOSZENIOWEJ.

ŹRÓDŁO: HTTPS://TECHHUB.HPE.COM/EGINFOLIB/NETWORKING/DOCS/SWITCHES/5130EI/5200-3942_L3-IP-SVCS_CG/CONTENT/483572274.HTM

Dygresja: Podejście do adresacji sieci komputerowych z użyciem klasowych adresów IP w szczególności adresy klasy A może powodować w konsekwencji budowanie bardzo dużych domen rozgłoszeniowych [4].

Należy równocześnie mieć na uwadze fakt, że sieci Ethernet w szczególności IPv4 do pracy wymagają użycia tzw. broadcastów, a te z racji swojego specjalnego przeznaczenia będą się rozprzestrzeniać w granicach tzw. domeny rozgłoszeniowej. Sytuacja taka może doprowadzić w szczególności do znacznego przyrostu ruchu typu rozgłoszeniowego w stosunku do ruchu danych, co w konsekwencji spowoduje znaczny spadek wydajności sieci komputerowej.

Modele topologii

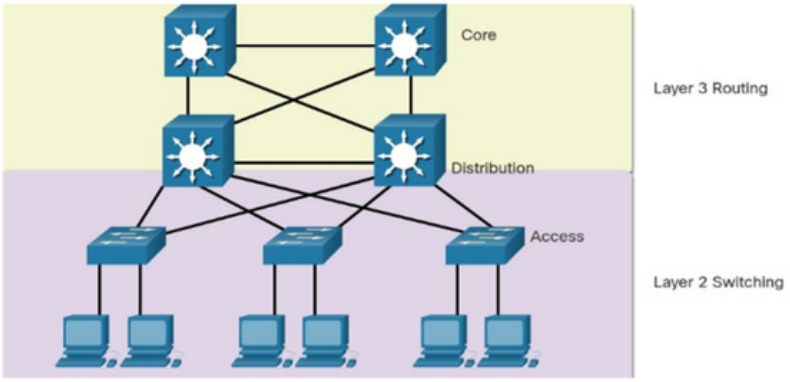
Jak wcześniej powiedzieliśmy istnieje ścisły związek pomiędzy VLAN'em, a klasą adresu użytego do adresacji hostów w sieci, a co za tym idzie pomiędzy ilością ruchu realizowanego w tzw. warstwie „Control Plane" oraz warstwie „Data Plane".

Chciałbym poniżej przedstawić przykłady, które są referencyjnymi modelami do realizacji fizycznych implementacji sieci LAN w kontekście VLAN'ów ich rozmiarów, a co za tym idzie rozmiarem domeny rozgłoszeniowej.

Dla każdego z poniżej wymienionych modeli skupmy się w szczególności na rozmiarze tzw. domeny rozgłoszeniowej. Wprowadźmy już tutaj pojęcie VLAN'ów, ale nasze rozważania uprośćmy tylko i wyłącznie na topologii z uwzględnieniem pojedyńczej sieci VLAN. Oczywiście pojęcie liczby VLAN'ów możemy ekstrapolować na większą ich liczbę bez zmiany warunków wejściowych, lecz ze względu na przejrzystość rozważanego zagadnienia ograniczę się tylko i wyłącznie do jednego VLAN'u.

Poniżej mamy pokazany tradycyjny hierarchiczny trzy warstwowy model sieci z wyodrębnionymi kolejno warstwami:
a) Core
b) Dystrybucji
c) Dostępu

Zwróćmy uwagę, że istniej wyraźnie określona granica, które urządzenia, jakiej warstwy i na jakiej warstwie realizują proces przełączania oraz proces rutowania. Jak widać poniżej routing oparty jest na urządzeniach warstwy Dystrybucji oraz Core, natomiast przełączanie jest oparte na urządzeniach warstwy Dystrybucji oraz Dostępu. Rozmiar i zasięg VLAN'u jest ściśle określony przez liczbę użytych urządzeń warstwy drugiej w warstwie dostępu.



RYS.2. TRADYCYJNY HIERARCHICZNY MODEL SIECI - THREE-TIER MODEL.

ŹRÓDŁO: MATERIAŁY SZKOLENIOWE CISCO CCNA

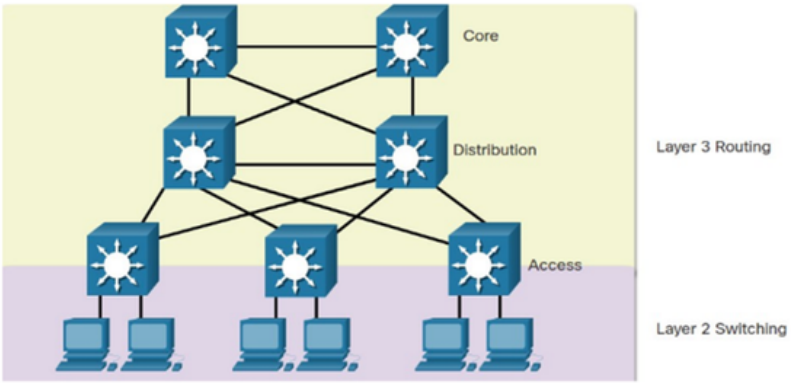
Zadajmy sobie kolejne pytanie już na konkretnym przykładzie:

Jak dla modelu powyżej wygląda obszar domeny rozgłoszeniowej?

Biorąc pod uwagę fakt, że nasz wyimaginowany VLAN znajduje się na każdym przełączniku L2 warstwy dostępu oraz na przełącznikach L3 warstwy dystrybucji, domena rozgłoszeniowa pokrywa się z kolorem zaznaczonym na fioletowo. A zatem jej rozmiar może obejmować teoretycznie wszystkie urządzenia podpięte w warstwie dostępu.

Należy również pamiętać, że z uwagi na fakt występowania nadmiarowości w warstwie fizycznej dla obszaru fioletowego, domyślnie będzie tam uruchomiony na przełącznikach L2, L3 protokół drzewa opinającego z rodziny STP, który będzie starał się zapewnić nam nadmiarowe ścieżki bez możliwości występowania pętli w L2. Pamiętajmy, że protokoły rodziny STP nie posiadają żadnego wbudowanego mechanizmu zabezpieczającego nas w przypadku wystąpienia pętli L2, co jest bardzo niebezpieczne dla pracy sieci opartej na rodzinie STP.

Z tego też powodu obecnie chcemy minimalizować obszar użycia protokołów z rodziny STP zawężając maksymalnie jego pokrycie, co można zobaczyć na kolejnym przykładzie. Poniżej zmodyfikowany diagram sieci, gdzie proces routingu został poszerzony o warstwę dostępu. Jednocześnie zmniejszony został obszar użycia VLANów oraz protokołów z rodziny STP, która oczywiście realizuje też proces przełączania.



RYS.3. TRADYCYJNY HIERARCHICZNY MODEL SIECI - THREE-TIER MODEL.

ŹRÓDŁO: MATERIAŁY SZKOLENIOWE CISCO CCNA

Takie posunięcie spowodowało, że ograniczyliśmy w tym przypadku maksymalnie jak się da obszar użycia protokołów drzewa opinającego do minimum i dzięki temu zminimalizowaliśmy konsekwencje ewentualnego wystąpienia pętli warstwy drugiej na obszarze pojedynczego przełącznika L3 warstwy dostępu.

Czy można pójść jeszcze dalej w naszych rozważaniach i całkowicie usunąć definicje VLAN'u z naszej sieci?

Teoretycznie tak, jeżeli naszą komunikację w sieci oprzemy tylko i wyłącznie o protokół rutowania statycznego, czy może lepiej dynamicznego w komunikacji „end to end", ale stwarza to inny kolejny problem związany ze skalowalności naszej sieci np. kiedy system końcowy wspiera wirtualizacje, czy mikroserwisy.

Podsumowanie:

Artykuł ze względu na zamierzony rozmiar nie uwzględnił jeszcze jednego modelu stosowanego do budowy współczesnych sieci komputerowych dużej skali. Mam na myśli tutaj model „Spine and Leaf" stosowany w Chmurze Obliczeniowej.
Tej wielkości sieci i ich specyficzny charakter ze względu na pojęcie tzw. POD'u oraz wymogów co do charakteru określonego typu ruchu jak w poprzednich wymienionych modelach „North-South", ale również „East-West" wymagają przedefiniowania podejścia do zastosowanego modelu, który musi uwzględniać definicje tzw. „Sieci Overlay" oraz „Sieci Underlay", topologie „full mesh", VLAN'ów w rozszyciu na POD oraz pomiędzy POD'ami , skalowalności, nadmiarowości warstw L1, L2, L3 oraz agregacji połączeń w modelu.

Jak sądzę jest to doskonały materiał na kolejny artykuł i uzupełnienie wiedzy na temat jak budować nowoczesne sieci komputerowej dużej skali integracji.

zapraszam do kolejnej lektury
autor PP
adnotacja: dane autora znane redakcji

Spis obrazów:

Rysunek 1
https://techhub.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3942_l3-ip-svcs_cg/content/483572274.htm
Rysunek 2,3 - materiały szkoleniowe CISCO CCNA

[1] Definicja sieci VLAN
https://en.wikipedia.org/wiki/VLAN
[2] Segmentacji sieci
https://en.wikipedia.org/wiki/Network_segmentation
[3] Domena rozliczeniowa
https://en.wikipedia.org/wiki/Broadcast_domain
[4] Obecna technologia pozwala "rozszyć" domenę rozgłoszeniową nie tylko w ramach sieci lokalnych LAN, ale można rozciągnąć siec Ethernet poza obszar lokalny poprzez sieci WAN mówimy wtedy o technologii Ethernet WAN (Metro Ethernet), VxLAN czy L2TP