Temat: Wirtualne Sieci Lokalne VLAN

Wirtualne sieci lokalne (Virtual Local Area Networks, VLANs) umożliwiają podział większej fizycznej sieci komputerowej na logiczne, odizolowane segmenty. Kształtowanie przepływu ruchu między sieciami VLAN odbywa się w warstwie 3. modelu OSI.

Virtual LAN (VLAN) dzieli fizyczne łącza na logiczne segmenty, ale sposób zaprojektowania wirtualnej sieci lokalnej zależy od administratora, a raczej przyjętych w organizacji założeń w zakresie kształtowania przepływu ruchu oraz wymaganego poziomu bezpieczeństwa. W ten sposób na jednym fizycznym przełączniku można utworzyć dwie (lub więcej) odizolowane od siebie sieci lokalne.

Tylko urządzenia przynależące do tej samej sieci VLAN mogą komunikować się ze sobą, każda sieć VLAN tworzy bowiem niezależną domenę rozgłoszeniową. Przełączniki przekazują ruch transmisji pojedynczej (unicast), grupowej (multicast) i rozgłoszeniowej (broadcast) tylko w ramach jednego segmentu sieci LAN. Poza izolacją segmentów sieci podejście to pozwala też ograniczyć zalewanie portów przełącznika rozgłoszeniami z protokołów ARP i DHCP, które nigdy nie przekraczają granic sieci VLAN.

Mechanizm routingu między VLAN, choć wymaga zastosowania dodatkowych urządzeń, pozwala kształtować przepływy ruchu między poszczególnymi segmentami sieci komputerowej. Mowa tutaj o kontroli dostępu, filtrowaniu ruchu na zaporze sieciowej czy zapewnianiu jakości usług (QoS).

Praktyczne zastosowania

Sieć VLAN może służyć do segmentacji według struktury organizacyjnej. W instytucjach publicznych komputery pracowników działów finansowych i HR nie powinny komunikować się ze względów bezpieczeństwa z urządzeniami pozostałego personelu biurowego. Z kolei w firmie produkcyjnej technologia VLAN może odizolować ruch sieci komputerowej udostępnianej pracownikom biurowym od sieci komputerowej wykorzystywanej w wydziałach produkcyjnych na potrzeby zbierania danych i sterowania maszynami.

Inne praktyczne zastosowanie sieci VLAN to segmentacja ruchu sieciowego ze względu na jego typ. Podejście to sprawdzi się w każdej instytucji, nawet gdy nie ma jawnej potrzeby izolowania ruchu według struktury organizacyjnej. Oddzielne VLAN stosuje się dla serwerów, punktów końcowych (stacje robocze, laptopy), drukarek, urządzeń mobilnych (strategia BYOD), telefonów VoIP, sieci Wi-Fi dla gości, sieci zarządzania (management) czy strefy DMZ.

Protokół IEEE 802.1Q

VLAN to wydzielona logicznie sieć komputerowa warstwy 2. (łącza danych) modelu OSI. Grupuje logicznie porty jednego lub wielu przełączników sieciowych niezależnie od ich położenia. Podstawowym, powszechnie stosowanym protokołem oznaczania ramek i trunkingu jest IEEE 802.1Q. Protokół ten, nazywany także Dot1q, stał się branżowym standardem definiującym sposób obsługi VLAN w sieciach Ethernet.

Działanie sieci VLAN bazuje na dodawaniu 4-bajtowych znaczników (tagów) wewnątrz nagłówka ramek Ethernet, które pozwalają urządzeniom sieciowym sterować przepływem ruchu. Znacznik ten, o nazwie 802.1Q Header, umieszczany jest między polem adresu źródłowego (Source MAC) a polem wskazującym na typ ramki/długość (EtherType/Size). Pierwsze dwa bajty tego znacznika (Tag Protocol ID, TPID) mają stałą wartość 0x8100 i umożliwiają przełącznikowi odróżnienie znakowanej ramki 802.1Q od ramki nieznakowanej, która w tym miejscu miałaby pole EtherType/Size. Pozostałe dwa bajty (Tag

Control Information, TCI) zawierają informacje służące do oznaczenia priorytetu ramki (definiowany w standardzie 802.1p), standardu sieci LAN (Ethernet lub Token Ring) oraz numeru wirtualnej sieci (VLAN ID), do której przynależy dana ramka. Wspomniane pole VLAN ID, stanowiące identyfikator sieci wirtualnej, ma długość 12 bitów i pozwala skutecznie przypisać ramkę do właściwego segmentu VLAN. W rezultacie na przełączniku można zdefiniować maksymalnie do 4096 sieci VLAN, z czego dwie są zarezerwowane do innych celów, a VLAN 1 pełni funkcję sieci natywnej.

W tym miejscu warto też wspomnieć o innym protokole znakowania i trunkingu. Inter-Switch Link (ISL) to własnościowy protokół Cisco używany w przełącznikach tej firmy. Oryginalna ramka Ethernet pozostaje niezmieniona, jest bowiem kapsułkowana w ramce ISL, której nagłówek zawiera znacznik VLAN ID. Protokół ISL został uznany za przestarzały, nie powinien być dalej używany. Co więcej, nie jest wspierany przez najnowsze przełączniki Cisco.

Punkty końcowe mogą komunikować się ze sobą w ramach jednej sieci VLAN. Przekazywanie ruchu sieciowego między sieciami VLAN wymaga zastosowania routera lub przełącznika działającego w warstwie 3. (sieci) modelu OSI.