Protokół STP

Ustanawia węzeł główny, który jest nazywany mostem głównym. Protokół STP konstruuje topologię, w której do każdego węzła w sieci prowadzi dokładnie jedna ścieżka. Korzeniem drzewa jest most główny. Połączenia nadmiarowe, które nie są częścią drzewa o najkrótszych ścieżkach, są blokowane. Dzieje się tak, ponieważ zablokowanie pewnych ścieżek jest konieczne do uzyskania topologii pozbawionej pętli. Ramki danych odebrane na zablokowanych łączach są odrzucane. Protokół STP wymaga, aby urządzenia w sieci wymieniały komunikaty umożliwiające wykrycie pętli mostowania. Połączenia, które powodują powstanie pętli, przechodzą do stanu blokowania. Przełączniki wysyłają komunikaty nazywane jednostkami BPDU (ang. Bridge Protocol Data Unit) umożliwiające utworzenie topologii logicznej bez pętli. Jednostki BPDU są odbierane nawet na zablokowanych portach. Zapewnia to możliwość wyliczenia nowego drzewa opinającego w przypadku awarii urządzenia lub ścieżki aktywnej.

Jednostki BPDU

zawierają informacje, dzięki którym przełączniki mogą wykonywać określone zadania:
-Wybrać jeden przełącznik główny, który będzie pełnił rolę korzenia drzewa opinającego.
-Obliczyć najkrótszą ścieżkę od danego przełącznika do przełącznika głównego.
-W każdym segmencie sieci LAN wyznaczyć przełącznik, który w topologii będzie najbliżej przełącznika głównego. Przełącznik ten jest nazywany przełącznikiem wyznaczonym (ang. designated switch). Przełącznik wyznaczony obsługuje całą komunikację między daną siecią LAN a mostem głównym.
-Wybrać jeden ze swoich portów jako port główny (dla każdego przełącznika oprócz przełącznika głównego). Jest to interfejs, przez który prowadzi najlepsza ścieżkę do przełącznika głównego.
-Wybrać porty, które są częściami drzewa opinającego. Te porty noszą nazwę portów wyznaczonych (ang. designated ports). Porty inne niż porty wyznaczone są blokowane.

Działanie STP

Po ustabilizowaniu pracy sieci osiąga ona zbieżność i w każdej sieci istnieje jedno drzewo opinające. W wyniku tego we wszystkich sieciach przełączanych występują następujące elementy:
-jeden most główny w każdej sieci,
-jeden port główny w każdym moście oprócz mostu głównego,
-jeden port wyznaczony w każdym segmencie,
-porty nieużywane (takie, które nie zostały wyznaczone).

Porty główne i porty wyznaczone służą do przekazywania ruchu danych (są oznaczane skrótem F od ang. Forwarding Port).

Porty inne niż wyznaczone odrzucają ruch danych. Porty te są nazywane portami blokującymi lub portami odrzucającymi (są oznaczane skrótem B od ang. Blocking Port).

Wybór mostu głównego

Pierwszą decyzją, którą muszą podjąć wszystkie przełączniki w sieci, jest identyfikacja mostu głównego. Od lokalizacji mostu głównego w sieci zależy przepływ danych w tej sieci.
Po włączeniu przełącznika korzysta on z algorytmu STP, aby znaleźć most główny. Wysyłane są jednostki BPDU z identyfikatorem mostu BID. Na identyfikator BID składają się priorytet (domyślnie 32768) i adres MAC przełącznika. Domyślnie jednostki BPDU są wysyłane co dwie sekundy.

Kiedy przełącznik jest uruchamiany po raz pierwszy, zakłada on, że jest przełącznikiem głównym, i wysyła jednostki BPDU zawierające adres MAC tego przełącznika w identyfikatorach BID nadawcy i przełącznika głównego. Te jednostki BPDU są traktowane jako podrzędne, ponieważ są generowane przez wyznaczony przełącznik, który utracił połączenie z mostem głównym. Taki przełącznik

wyznaczony wysyła jednostki BPDU zawierające informacje, że jest on jednocześnie mostem głównym i mostem wyznaczonym. Te jednostki BPDU zawierają adres MAC przełącznika zarówno w identyfikatorze BID mostu głównego, jak i w identyfikatorze BID nadawcy. Identyfikatory BID są odbierane przez wszystkie przełączniki. Każdy przełącznik zastępuje w wysyłanych jednostkach BPDU wyższy identyfikator BID przełącznika głównego niższym identyfikatorem BID. Wszystkie przełączniki odbierają jednostki BPDU i ustalają, że przełącznik o najmniejszej wartości BID mostu głównego zostaje mostem głównym.

Stany STP

-W stanie blokowania (ang. blocking) porty mogą jedynie odbierać jednostki BPDU. Odrzucane są ramki danych i nie są zapamiętywane żadne adresy. Wychodzenie z tego stanu może trwać do 20 sekund.
-Ze stanu blokowania porty przechodzą do stanu nasłuchiwania (ang. listening). W tym stanie przełączniki ustalają, czy istnieją inne ścieżki do mostu głównego. Ścieżka, która nie jest ścieżką o najniższym koszcie prowadzącą do mostu głównego, przechodzi z powrotem do stanu blokowania. Okres nasłuchiwania jest nazywany opóźnieniem przesyłania i może trwać do 15 sekund. W stanie nasłuchiwania nie są przesyłane dane i nie są zapamiętywane adresy MAC. Jednostki BPDU są nadal przetwarzane.
-Ze stanu nasłuchiwania porty przechodzą do stanu zapamiętywania (ang. learning). W tym stanie dane nie są przekazywane, ale adresy MAC są odbierane i zapamiętywane. Stan zapamiętywania może trwać do 15 sekund i jest również nazywany opóźnieniem przesyłania. Jednostki BPDU są nadal przetwarzane.
-Ze stanu zapamiętywania porty przechodzą do stanu przekazywania (ang. forwarding). W tym stanie dane użytkowe są przekazywane, a adresy MAC są w dalszym ciągu zapamiętywane. Jednostki BPDU są nadal przetwarzane.
-Port może się znajdować w stanie wyłączenia (ang. disabled). Stan wyłączenia może wystąpić, gdy port zostanie wyłączony przez administratora lub ulegnie awarii.

Szybki protokół STP

Jest zdefiniowany przez standard IEEE 802.1w sieci LAN. W standardzie i w protokole zostały wprowadzone nowe funkcje:
-uporządkowanie ról i stanów portów;
-definicja zestawu typów łączy, które mogą szybko przejść do stanu przekazywania;
-zezwolenie przełącznikom na wysyłanie własnych jednostek BPDU po osiągnięciu zbieżności sieci, zamiast przekazywania jednostek BPDU wysyłanych przez most główny.
-Określenie stanu portu jako "blokujący" zostało zmienione na "odrzucający" (ang. discarding). Porty odrzucające pełnią rolę portów alternatywnych. Port odrzucający może stać się portem wyznaczonym, gdy port wyznaczony w tym segmencie ulegnie awarii.

VLAN

Sieć VLAN jest oparta na sieci przełączanej, która została logicznie posegmentowana. Do sieci VLAN można przypisać każdy z portów przełącznika. Porty przypisane do sieci VLAN odbierają i przekazują te same pakiety rozgłoszeniowe. Porty, które nie należą do tej sieci, nie przekazują tych pakietów. Zwiększa to wydajność sieci, ponieważ zmniejsza się ilość zbędnych pakietów rozgłoszeniowych. Sieci VLAN o członkostwie statycznym noszą nazwę sieci członkowskich VLAN opartych na portach (ang. port-centric). W momencie, gdy urządzenie jest dołączane do sieci, automatycznie przyjmuje ono członkostwo w sieci VLAN tego portu, do którego zostało podłączone.
Użytkownicy przyłączeni do tego samego współużytkowanego segmentu wspólnie korzystają z przepustowości tego segmentu. Każdy dodatkowy użytkownik przyłączony do wspólnego nośnika oznacza mniejszą przepustowość i spadek wydajności sieci. Sieci VLAN zapewniają użytkownikom większą przepustowość niż współużytkowane sieci Ethernet oparte na koncentratorach. Domyślną

siecią VLAN dla każdego portu przełącznika jest sieć VLAN zarządzania. Siecią VLAN zarządzania jest zawsze sieć VLAN 1. Sieci tej nie można usunąć. Aby móc zarządzać przełącznikiem, do sieci VLAN 1 musi być przypisany co najmniej jeden port. Wszystkie inne porty przełącznika mogą być przypisane do innych sieci VLAN.
Sieci VLAN z członkostwem dynamicznym są tworzone przez oprogramowanie zarządzające siecią. Dynamiczne sieci VLAN przyjmują członkostwo na podstawie adresu MAC urządzenia podłączonego do portu przełącznika. W momencie, gdy urządzenie jest podłączane do sieci, przełącznik, do którego jest ono podłączone, odpytuje bazę danych serwera konfiguracyjnego VLAN o członkostwo w sieci.
W członkostwie opartym na portach port jest przypisywany do konkretnej sieci VLAN niezależnie od użytkownika lub systemu podłączonego do portu. Gdy używana jest ta metoda członkostwa, wszyscy użytkownicy danego portu muszą być w tej samej sieci VLAN. Do portu może być podłączona dowolna liczba użytkowników, którzy nie zdają sobie sprawy, że sieć VLAN istnieje. Ułatwia to zarządzanie, ponieważ do segmentacji sieci VLAN nie są potrzebne złożone tablice wyszukiwania.
Administratorzy sieci odpowiadają zarówno za statyczną, jak i dynamiczną konfigurację sieci VLAN.

Zalety VLAN

Sieci VLAN umożliwiają administratorom sieci logiczne, zamiast fizycznego, organizowanie struktury sieci LAN. Jest to kluczowa zaleta tych sieci. Dzięki temu administratorzy mogą wykonywać następujące zadania:
-łatwo przenosić stacje robocze w sieci LAN;
-łatwo dodawać stacje robocze do sieci LAN;
-łatwo zmieniać konfigurację sieci LAN;
-łatwo nadzorować ruch w sieci;
-zwiększyć bezpieczeństwo.

Rodzaje sieci VLAN

Oparte na portach:
-Najczęściej stosowana metoda konfigurowania.
-Porty przypisane pojedynczo, w grupach, po kolei, w 2 lub wielu przełącznikach.
-Łatwe w użyciu.
-Często stosowane tam,gdzie do przypisania adresów IP do hostów w sieci używany jest protokół dynamicznej konfiguracji hostów (DHCP).
Adres MAC:
-Obecnie rzadko stosowane.
-Każdy adres musi byc ręcznie wprowadzony do przełącznika i skonfigurowany.
-Przydatne dla użytkowników.
-Trudne w administorwaniu, zarządzaniu i rozwiązywaniu problemów.
oparte na protokołach:
Konfigurowane podobnie jak adresy MAC, ale używany jest adres logiczny lub IP.
Obecnie rzadko używane, gdyż stosowany jest mechanizm DHCP.

Sieć VLAN typu end-to-end

ma następujące cechy:
-członkostwo użytkowników w sieci VLAN zależy od departamentu lub stanowiska, niezależnie od rozmieszczenia użytkowników;
-wszyscy użytkownicy w sieci VLAN muszą mieć taką samą charakterystykę przepływu 80/20;
-członkostwo w sieci VLAN nie powinno się zmieniać przy przenoszeniu się użytkowników w obrębie kampusu;
-każda sieć VLAN ma jeden zestaw wymagań dotyczących ochrony odnośnie wszystkich członków.

Konfigurowanie statycznych sieci VLAN

Switch#vlan database
Switch(vlan)#vlan numer_sieci_VLAN
Switch(vlan)#exit
Po wyjściu z tego trybu konfiguracja sieci VLAN zostanie zastosowana w przełączniku. Następnym krokiem jest przypisanie sieci VLAN do jednego lub wielu interfejsów
Switch(config)#interface fastethernet 0/9
Switch(config-if)#switchport access vlan numer_sieci_VLAN

VTP

Zadaniem protokołu VTP jest utrzymanie spójności konfiguracji sieci VLAN w całej określonej domenie administracyjnej sieci. VTP to protokół komunikacyjny, który umożliwia dodawanie, usuwanie i zmianę nazwy sieci VLAN w obrębie jednej domeny, używając do tego ramek łączy trunkingowych warstwy 2. Pozwala on również na scentralizowane wprowadzanie zmian, o których informacje są rozsyłane do wszystkich pozostałych przełączników w sieci. Komunikaty protokołu VTP są umieszczane w ramkach własnego protokołu Cisco — ISL lub protokołu IEEE 802.1Q, a następnie przekazywane za pośrednictwem łączy trunkingowych do kolejnych urządzeń. W ramkach protokołu IEEE 802.1Q ramki protokołu VTP są oznaczane za pomocą 4-bajtowych pól. W przypadku obu formatów ramki zawierają identyfikatory sieci VLAN. O ile porty przełączników standardowo są przypisywane tylko do jednej sieci VLAN, porty trunkingowe domyślnie przekazują ramki ze wszystkich sieci VLAN.

Tryby VTP

-Serwery VTP mogą tworzyć, modyfikować i usuwać sieci VLAN i ich parametry konfiguracyjne dla całej domeny. Serwery VTP zapisują informacje o konfiguracji sieci VLAN w pamięci NVRAM przełącznika. Serwery wysyłają komunikaty protokołu VTP na wszystkich portach łącza trunkingowego.
-Klienci VTP nie mogą tworzyć, modyfikować ani usuwać informacji o sieciach VLAN. Ten tryb jest przydatny w przypadku przełączników o ilości pamięci zbyt małej, aby przechowywać duże tablice informacji o sieciach VLAN. Jedynym zadaniem klientów VTP jest przetwarzanie zmian dotyczących sieci VLAN i wysyłanie komunikatów VTP na wszystkich portach łącza trunkingowego.
-Przełączniki pracujące w trybie przezroczystym protokołu VTP przekazują ogłoszenia tego protokołu, ale ignorują informacje zawarte w komunikatach. Po otrzymaniu aktualizacji nie modyfikują one swoich baz danych, jak również nie wysyłają aktualizacji wskazujących na zmianę stanu obsługiwanych przez siebie sieci VLAN. Z wyjątkiem przekazywania ogłoszeń VTP, pozostałe funkcje tego protokołu są wyłączone na przełącznikach pracujących w trybie przezroczystym.

Ogłoszenia VTP

-żądania od klientów, którzy chcą otrzymać informacje podczas swojego uruchamiania,
-odpowiedzi z serwerów.

Komunikaty VTP

-Za pomocą żądań ogłoszeń klienci wysyłają żądania podania informacji o sieciach VLAN.Serwer odpowiada ogłoszeniami skonsolidowanymi i szczegółowymi.
-Domyślnie przełączniki Catalyst działające w trybie serwera i klienta wysyłają ogłoszenia skonsolidowane co pięć minut. Serwery informują sąsiednie przełączniki, jaki ich zdaniem jest aktualny numer konfiguracji protokołu VTP. Jeśli nazwy domen są takie same, serwer lub klient porównuje otrzymany numer wersji konfiguracji z numerem posiadanych informacji.

Gdy przełącznik otrzyma numer wersji wyższy niż ten, który aktualnie posiada, wysyła żądanie nowych informacji o sieciach VLAN.
Ogłoszenia szczegółowe zawierają szczegółowe informacje o sieciach VLAN, takie jak numer wersji protokołu VTP, nazwa domeny wraz z polami pokrewnymi oraz numer wersji konfiguracji. Wysyłanie ogłoszeń szczegółowych może być wyzwalane przez następujące czynności:
-usunięcie lub dodanie sieci VLAN,
-zawieszenie lub aktywacja sieci VLAN,
-zmiana nazwy sieci VLAN,
-zmiana maksymalnej jednostki transmisyjnej MTU dla sieci VLAN.
Ogłoszenia mogą zawierać niektóre lub wszystkie z poniższych informacji:
-Nazwa domeny zarządzania — ogłoszenia zawierające inne nazwy domen są ignorowane.
-Numer wersji konfiguracji — wyższy numer oznacza nowszą konfigurację.
-MD5 (ang. *Message Digest 5*) — MD5 to klucz wysyłany przez protokół VTP w przypadku skonfigurowania hasła. Jeśli klucze są niezgodne, aktualizacja jest ignorowana.
-Tożsamość urządzenia aktualizującego — tożsamość urządzenia aktualizującego to tożsamość przełącznika, który wysyła ogłoszenie skonsolidowane protokołu VTP.

Konfiguracja VTP

W celu przejścia do tego trybu i skonfigurowania numeru wersji protokołu VTP można użyć poniższych poleceń: 2
Switch#**vlan database**
Switch(vlan)#**vtp v2-mode**
Jeśli przełącznik jest pierwszym przełącznikiem w sieci, należy utworzyć domenę zarządzania. Jeśli domena zarządzania została zabezpieczona, należy dla niej skonfigurować hasło.
W celu utworzenia domeny zarządzania można użyć następującego polecenia: 3
Switch(vlan)#**vtp domain cisco**
W celu ustawienia właściwego trybu przełącznika można użyć następującego polecenia: 5
Switch(vlan)#**vtp {client | server | transparent}**

Dodanie klienta do VTP

Aby dodać klienta VTP do istniejącej domeny VTP, należy sprawdzić, czy jego numer wersji konfiguracji danych protokołu VTP jest niższy niż numer wersji konfiguracji pozostałych przełączników należących do domeny VTP. Służy do tego polecenie **show vtp status**. Przełączniki w domenie VTP zawsze używają informacji konfiguracyjnych sieci VLAN przełącznika o najwyższym numerze konfiguracji danych protokołu VTP. Jeśli zostanie dodany przełącznik, którego numer wersji jest wyższy niż numer aktualnie używany w domenie, może to spowodować usunięcie wszystkich informacji o sieciach VLAN z serwera VTP i domeny VTP

Łącze trunkingowe

to fizyczne i logiczne połączenie między dwoma przełącznikami, po którym odbywa się ruch w sieci. Jest to pojedynczy kanał transmisyjny między dwoma punktami. Punktami tymi są zazwyczaj centra przełączania. W sieci przełączanej łącze trunkingowe to łącze punkt-punkt, które może obsługiwać kilka sieci VLAN. Celem stosowania łączy trunkingowych jest zmniejszenie liczby wykorzystywanych portów podczas budowania połączeń między dwoma urządzeniami implementującymi sieci VLAN. Łącza trunkingowe pozwalają skonfigurować wiele łączy wirtualnych w jednym łączu fizycznym. Dzięki temu ruch z kilku sieci VLAN może być przekazywany za pośrednictwem jednego kabla poprowadzonego między przełącznikami.

Znakowanie ramek

System znakowania ramek w sieciach VLAN został opracowany specjalnie na potrzeby komunikacji w sieciach przełączanych. Znakowanie polega na umieszczeniu unikatowego identyfikatora w nagłówku każdej ramki podczas jej przesyłania w sieci szkieletowej. Identyfikator jest interpretowany i analizowany przez każdy przełącznik. Na tej podstawie przełącznik podejmuje decyzję o rozgłoszeniu lub przekazaniu ramki do innego przełącznika, routera lub stacji końcowej. Gdy ramka ma opuścić część szkieletową sieci, przełącznik usuwa z niej identyfikator, po czym wysyła ramkę do docelowej stacji końcowej. Znakowanie ramek funkcjonuje w warstwie 2 i nie wymaga wielu zasobów sieciowych ani działań ze strony administratora.

Filtrowanie ramek

Filtrowanie ramek bada konkretne informacje, związane z każdą ramką. Dla każdego switcha budowana jest tabela filtrowania. Zapewnia to administratorowi wysoki poziom kontroli, ponieważ pozwala na badanie wielu atrybutów każdej ramki. W zależności od stopnia zaaansowania technicznego danego switcha, użytkownicy mogą być grupowani w oparciu o adres MAC, lub tryb protokołu warstwy sieci. Switch porównuje filtrowaną ramkę z wpisami w tablicy filtrowania i na tej podstawie podejmuje odpowiednie działanie.

VTP Prunning

Dzięki niemu wykorzystanie przepustowości łącza trunkingowego jest efektywniejsze, gdyż zmniejsza niepotrzebne jego wykorzystanie. Broadcast i nieznane ramki unicast w sieci VLAN są przekazywane przez łącze trunkingowe tylko wtedy, gdy przełącznik na końcówce odbierającej łącza trunkingowego ma porty w tej sieci VLAN. VTP Prunning występuje jako dodatek do VTP w wersji 1, wykorzystując dodatkowy typ komunikatu. Gdy przełącznik Catalyst ma porty należące do sieci VLAN, przesyła ogłoszenie do sąsiednich przełączników, o tym, że posiada aktywne porty w tej sieci VLAN. Sąsiedzi zachowując tę informacje, mogą podjąć decyzję czy ruch ma być kierowany na łącze trunkingowe czy nie.

NAT

NAT (skr. od ang. Network Address Translation, tłumaczenie adresów sieciowych; czasem Native Address Translation, tłumaczenie adresów rodzimych), znane również jako maskarada sieci lub IP (od ang. network/IP masquerading) – technika przesyłania ruchu sieciowego poprzez router, która wiąże się ze zmianą źródłowych lub docelowych adresów IP, zwykle również numerów portów TCP/UDP pakietów IP podczas ich przepływu. Zmieniane są także sumy kontrolne (tak IP jak i TCP/UDP), aby potwierdzić wprowadzone zmiany. Większość systemów korzystających z NAT ma na celu umożliwienie dostępu wielu hostom w sieci prywatnej do internetu przy wykorzystaniu pojedynczego publicznego adresu IP (zob.brama sieciowa). Niemniej NAT może spowodować komplikacje w komunikacji między hostami i może mieć pewien wpływ na osiągi.

Zastosowanie NAT:

Wraz ze wzrostem liczby komputerów w Internecie, zaczęła zbliżać się groźba wyczerpania puli dostępnych adresów internetowych IPv4. Aby temu zaradzić, lokalne sieci komputerowe, korzystając z tzw. adresów prywatnych (specjalna pula adresów tylko dla sieci lokalnych), mogą zostać podłączone do Internetu przez jeden komputer (lub router), posiadający mniej adresów internetowyc niż komputerów w tej sieci. Router ten, gdy komputery z sieci lokalnej komunikują się ze światem, dynamicznie tłumaczy adresy prywatne na adresy zewnętrzne, umożliwiając użytkowanie Internetu przez większą liczbę komputerów niż posiadana liczba adresów zewnętrznych. NAT jest często stosowany w sieciach korporacyjnych (w połączeniu z proxy) oraz sieciach osiedlowych.

Rodzaje NAT

- SNAT (Source Network Address Translation) to technika polegająca na zmianie adresu źródłowego pakietu IP na jakiś inny. Stosowana często w przypadku podłączenia siecidysponującej adresami prywatnymi do sieci Internet. Wtedy router, przez który podłączono sieć, podmienia adres źródłowy prywatny na adres publiczny (najczęściej swój własny).
Szczególnym przypadkiem SNAT jest maskarada, czyli sytuacja, gdy router ma zmienny adres IP (np. otrzymuje go w przypadku połączenia modemowego dodzwanianego). Wtedy router zmienia adre źródłowy na taki, jak adres interfejsu, przez który pakiet opuszcza router.
-DNAT (Destination Network Address Translation) to technika polegająca na zmianie adresu docelowego pakietu IP na jakiś inny. Stosowana często w przypadku, gdy serwer, który ma być dostępny z Internetu ma tylko adres prywatny. W tym przypadku router dokonuje translacji adresu docelowego pakietów IP z Internetu na adres tego serwera.

Konfiguracja NAT

Określenie które interfejsy są wewnętrzne a które zewnętrzne:
gw1-bogus(config-if)#ip nat inside
lub
gw1-bogus(config-if)#ip nat outside
np.:
gw1-bogus(config)#interface serial 2/0
gw1-bogus(config-if)#ip nat outside
gw1-bogus(config-if)#exit
gw1-bogus(config)#interface e0
gw1-bogus(config-if)#ip nat inside

NAT na bazie listy standardowej

Uwaga: Lista standardowa jest wystarczającym rozwiązaniem przy ustawianiu NAT-a obejmującego cały ruch wyjściowy. Jeśli chcemy wprowadzić ograniczenie NAT-a na podstawie adresów przeznaczenia, wówczas potrzebny jest NAT na bazie listy rozszerzonej – patrz następny rozdział !.
Ustawienie standardowego ACL-a który uruchamia NAT-a dla ruchu z wybranych sieci/hostów wewnętrznych (permit) lub blokuje NAT-a dla innych sieci/hostów wewnętrznych (deny):
gw1-bogus(config)#acces-list <ACL_1> permit <addres_sieci> <wildcard_bits>
np.
gw1-bogus(config)#acces-list 1 permit 192.168.1.0 0.0.0.255
Komenda włączająca NAT'a dla sieci wewnętrznej:
gw1-bogus(config)#ip nat inside source list <ACL_1> interface <interface> overload
i tak
- inside source – właczone NATowanie pakietów z wewnętrznych sieci (włączona zamiana pola source adress w nagłówku pakietu)
- <ACL_1> – nr ACL-a sterującego dostępem do NAT-a
- <interface> – nazwa interfejsu którego adres jest wstawiany w pole source address
- overload – zmiana wielu adresów na jeden – PAT (inaczej byłoby 1 w 1 - NAT)

np.
gw1-bogus(config)#ip nat inside source list 1 interface e0 overload

NAT na baize listy rozszerzonej

Uwaga: Lista rozszerzona pozwala wyłączyć z NAT-a ruch wyjściowy na podstawie adresu przeznaczenia. Tego typu NAT jest nieodzowny np. przy ustawianiu zdalnego dostępu

klientów VPN – wówczas ruch skierowany do zdalnych klientow VPN nie powinien być NAT-owany. Zakładamy, że ustawiono rozszerzonego ACL-a nr 199, który uruchamia (permit) lub blokuje (deny) NAT-a.
W kolejnym kroku konfigurujemy mapę routingu (router-map) obejmującą ruch zdefiniowany przez rozszerzonego ACL-a nr 199:
gw1-bogus(config)#route-map <route-map-name> permit 10
gw1-bogus(config-route-map)#match ip address <extended_ACL_for_NAT>
np.
gw1-bogus(config)#route-map make_nat permit 10
gw1-bogus(config-route-map)#match ip address 199
Komenda włączająca NAT'a dla sieci wewnętrznej:
gw1-bogus(config)#ip nat inside source route-map <route-map-name> interface <interface> overload
i tak
- inside source – właczone NATowanie pakietów z wewnętrznych sieci (włączona zamiana pola source adress w nagłówku pakietu)
- <router-map-name> – nazwa mapy routingu sterującej dostępem do NAT-a
- <interface> – nazwa interfejsu którego adres jest wstawiany w pole source address
- overload – zmiana wielu adresów na jeden – PAT (inaczej byłoby 1 w 1 - NAT)

np.
gw1-bogus(config)#ip nat inside source route-map make_nat interface e0 overload

NAT - Translacja Statyczna i Dynamiczna

Translacje NAT mogą być dokonywane statycznie (dokonywane ręcznie) lub dynamicznie. W pierwszym przypadku przydział adresu NAT-IP. Dla oryginalnego adresu IP jest jednoznaczny w drugim nie jest. W statycznym NAT pewien stały źródłowy adres IP jest zawsze translowany do tego samego adresu NAT-IP i żaden inny adres IP nie będzie translowany do tego samego adresu NAT-IP. Natomiast w przypadku translacji dynamicznej NAT, adres NAT-IP jest zależny od różnorodnych warunków działania i może być kompletnie inny dlakażdej pojedyńczej sesji.

NAT i PAT

NAT może dokonać konwersji na dwóch różnych poziomach adresowania pakietu:
1. na poziomie warstwy sieciowej: adres IP - NAT
2. na poziomie warstwy transportowej: socket (adres IP i numer portu) - NAPT (PAT)

Rozpatrzmy powyższe dwie metody translacji NAT i NAPT (PAT).
1. Pierwsza metoda (NAT) dokonuje translacji tylko adresu IP prywatnego hosta.
Informacja adresowa wygląda następująco:
(adres IP źródła : numer portu źródłowego;
adres IP przezn. : numer portu przeznaczenia)
pakiet, który wychodzi w kierunku Internetu jest translowany do postaci:
(adres IP źródła : numer portu źródłowego;
adres IP przezn. : numer portu przeznaczenia)
2. W drugim przepadku modyfikacji (NAPT, PAT) podlegają zarówno adres IP jak i numer portu TCP/UDP.
Informacja adresowa wygląda następująco:
(adres IP źródła : numer portu źródłowego;
adres IP przezn. : numer portu przeznaczenia)
pakiet, który wychodzi w kierunku Internetu jest translowany do postaci:
(adres IP źródła : numer portu źródłowego;
adres IP przezn. : numer portu przeznaczenia)

Dla pakietów w kierunku odwrotnym, czyli z Internetu do sieci prywatnej, dokonywane są podobne modyfikacje, ale na polach przeznaczenia.

NAT – Wady i Zalety

Wady:
-nie można na własnym komputerze uruchomić serwera dostępnego w Internecie bez zmian wymagających interwencji administratora;
-utrudnione korzystanie z sieci P2P i bezpośrednie wysyłanie plików.
Zalety:
-większa anonimowość gdyż serwery, z którymi nastąpiło połączenie nie mogą zidentyfikować konkretnego hosta po samym adresie IP
-oszczędzanie publicznych adresów IP

Frame Relay

Podobnie jak X.25, Frame Relay opisuje komunikację na styku między klientem a dostawcą usług sieci WAN. Urządzeniem klienckim DTE moze być na przykład router Cisco, natomiast urządzeniem aktywnym DCE będzie zwykle przełącznik w sieci dostawcy.

Komunikacja między dwoma urządzeniami DTE realizowana jest poprzez zestawienie połączenia logicznego zwanego obwodem wirtualnym. Obwody **PVC (Private Virtual Circuit)** zestawia się między urządzeniami DTE na stałe i nie rozłącza przy braku transmisji, natomiast obwody SVC (Switched Virtual Circuit) zestawia się na żądanie i rozłącza po określonym okresie bezczynności. **Specyfikacja Frame Relay, w przeciwieństwie do X.25,** opisuje komunikację sieciową w obrębie tylko dwóch pierwszych warstw modelu sieciowego OSI (fizycznej i łącza danych). Zakłada ona przełączanie pakietów o zmiennej części informacyjnej wzdłuż obwodów wirtualnych, ale w praktyce stosowaną jednostką informacyjną jest ramka (warstwa druga). Za kontrolę przepływu danych oraz wykrywanie błędów odpowiedzialne są warstwy wyższe modelu OSI. Węzły sieci Frame Relay sprawdzają tylko sumę kontrolną CRC w odebranych ramkach, ale nie wymuszają retransmisji uszkodzonych ramek na poziomie warstwy drugiej. Typowe medium transmisyjne to skrętka miedziana lub światłowód, a prędkość przesyłania danych do 44,736 Mbps. Protokół Frame Relay jest protokołem warstwy łącza danych, natomiast w warstwie fizycznej stosowane mogą być protokoły RS232, RS449, V.35 bądź X.21. Do identyfikacji poszczególnych obwodów służą numery **DLCI (Data-Link Connection Identifier)** - mają one znaczenie lokalne i w różnych częściach sieci Frame Relay mogą być podłączone do niej routery korzystające z tych samych numerów DLCI. Numer DLCI zapisywany jest w ramce Frame Relay w polu nagłówkowym o długości 10 bitów, moŜliwe są więc 1024 różne identyfikatory. W praktyce pewne numery DLCI zarezerwowane są do specjalnych celów (od 0 do 15 i od 1008 do 1023) i standardowo wykorzystuje się tylko zakres od 16 do 1007. Protokół LMI opisuje sposób sygnalizacji (między urządzeniem DTE- routerem i DCE - przełącznikiem Frame Relay) stosowany do zarządzania połączeniem i przesyłania komunikatów informujących o stanie urządzenia. Obecnie uzywane są trzy implementacje protokołu LMI:
-standard ANSI (T1.617, Annex D),
-standard międzynarodowej unii telekomunikacyjnej ITU?T (Q.933, Annex A),
-protokół LMI opracowany przez firmy "grupy czterech" (DEC, Northern Telecom, Cisco, Stratacom).

Podinterfejsy Frame Relay

Podinterfejsy dzielą fizyczny interfejs na logiczne części, dzięki którym mozliwe jest podłączenie kilku obwodów PVC (sieci) do jednego fizycznego interfejsu routera. Uaktualnienia routingu mogą być rozsyłane przez podinterfejsy tak samo jak gdyby były one niezaleznymi interfejsami fizycznymi.

Kazdy podinterfejs ma unikatowy numer DLCI i traktowany jest jako niezalezna sieć. Przy tworzeniu podinterfejsów naleŜy usunąć adres dla interfejsu głównego, w przeciwnym wypadku lokalne podinterfejsy nie będą mogły odbierać danych. W routingu Frame Relay obowiązuje zasad podzielonych sieci, zabezpieczająca przez zapętleniami. Polega ona na tym, ze zabronione jest wysyłanie uaktualnień na ten sam interfejs, z którego ono nadeszło. Podinterfejsy mozna skonfigurować do obsługi połączeń Dwupunktowych i Wielopunktowych.