21. Routing statyczny a dynamiczny – różnice oraz wady i zalety.

#Zalety Statycznego:

- Router przesyła pakiety przez z góry ustalone interfejsy bez konieczności każdorazowego obliczania tras, co zmniejsza zajętość cykli procesora i pamięci.

- Informacja statyczna nie jest narażona na deformację spowodowaną zanikiem działania dynamicznego routingu na routerach sąsiednich.

- Dodatkowo zmniejsza się zajętość pasma transmisji, gdyż nie są rozsyłane pakiety rozgłoszeniowe protokołów routingu dynamicznego. zapewnia również konfigurację tras domyślnych, nazywanych bramkami ostatniej szansy (gateway of the last resort). Jeżeli router uzna, iż żadna pozycja w tablicy routingu nie odpowiada poszukiwanemu adresowi sieci docelowej, korzysta ze statycznego wpisu, który spowoduje odesłanie pakietu w inne miejsce sieci

#Wady Statycznego:

Routing statyczny wymaga jednak od administratora sporego nakładu pracy w początkowej fazie konfiguracji sieci, nie jest również w stanie reagować na awarie poszczególnych tras.

#Zalety Dynamicznego:

Adaptacja do zmiennych warunków w sieci. Oznacza to, że routery reagują na wszelkie nieprawidłowości oraz zmiany parametrów podczas pracy sieci, a więc informacje przechowywane w węzłach są bardziej adekwatne i ściślej opisują bieżącą topologię w sieci.

#Wady Dynamicznego:

Wymagania stawiane sprzętowym konfiguracjom węzłów sieci – mocy obliczeniowej oraz ilości pamięci, jak również dodatkowy ruch generowany w sieci na skutek wymiany informacji pomiędzy węzłami.

22. Pojęcie metryki routingu oraz dystansu administracyjnego.

Metryka trasowania - wartość używana przez algorytmy trasowania do określenia, która trasa jest lepsza. Brane są pod uwagę: szerokość pasma, opóźnienie, liczba przeskoków, koszt ścieżki, obciążenie, MTU, niezawodność, koszt komunikacji. Tylko najlepsze trasy przechowywane są w tablicach trasowania, podczas gdy inne mogą być przechowywane w bazach danych. Jeśli router korzysta z mechanizmów równoważenia obciążenia (ang. load balancing), w tablicy trasowania może wystąpić kilka najlepszych tras. Router będzie je wykorzystywał równolegle, rozpraszając obciążenie równomiernie pomiędzy trasami.
i – miara używana przez routery Cisco (i nie tylko), będąca liczbą naturalną z przedziału od 0 do 255, reprezentującą poziom zaufania (wiarygodności) w odniesieniu do źródła informacji o danej trasie. Zasada działania jest dość prosta – im mniejszy dystans administracyjny (mniejsza liczba), tym źródło danych o trasie jest bardziej godne zaufania.

23. Urządzenia sieciowe: hub, bridge, switch oraz router – charakterystyka działania

Koncentrator (hub) – urządzenie łączące wiele urządzeń sieciowych w sieci komputerowej o topologii gwiazdy. Koncentrator pracuje w warstwie pierwszej modelu ISO/OSI (warstwie fizycznej), przesyłając sygnał z jednego portu na wszystkie pozostałe. Nie analizuje ramki pod kątem adresu MAC oraz IP. Ponieważ koncentrator powtarza każdy sygnał elektroniczny, tworzy jedną domenę kolizyjną. Koncentrator przenosi sygnał z portu wejściowego na wszystkie porty wyjściowe bit po bicie, przełącznik(switch) natomiast ramka po ramce, co jest powodem wprowadzania dużych opóźnień (także dodatkowych, zmiennych, w zależności

od długości ramki). Jeżeli przesyłane mają być dane, dla których wspomniane zmienne opóźnienie jest niepożądane (np. streaming), koncentrator okaże się lepszym rozwiązaniem od przełącznika.

Przełącznik (switch) - urządzenie które łączy oddzielne sieci LAN oraz zapewnia filtrowanie pakietów między nimi. Switch LAN jest urządzeniem z pewną liczbą portów, z których każdy może współpracować z siecią Ethernet lub Token Ring. Chociaż zapewniają one takie same możliwości łączenia za pomocą kabli sieciowych jak koncentratory, to jednak przyczyniają się do zwiększenia wydajności całej sieci. Dzieje się tak wskutek rozszerzenia pasma transmisji danych (czyli maksymalnej pojemności sieci transmisji danych). Zamiast współdzielenia całego dostępnego pasma pomiędzy wszystkich użytkowników, tak jak w przypadku koncentratora, przełącznik przydziela każdemu podłączonemu urządzeniu sieciowemu określoną część pasma transmisyjnego. Na przykład, każdy koncentrator 10 Mb/s udostępni całe pasmo transmisyjne10 Mb/s wszystkim podłączonym urządzeniom. Odpowiedni przełącznik przydzieli takie pasmo każdemu urządzeniu z osobna, co znacznie zwiększy wydajność. Dalsze zwiększenie wydajności można uzyskać przez wprowadzenie przełączników pozwalających na obsługę połączeń dwukierunkowych. Działanie przełączników jest możliwe dzięki zapamiętaniu jednoznacznych adresów MAC każdego urządzenia pracującego w lokalnej sieci komputerowej i informacjom o tym, z którym portem komunikuje się dane urządzenie.

- Umieszczone w pobliżu szkieletu sieci likwidują "wąskie gardła" systemu transmisji danych i zwiększają przepustowość sieci;
- Mogą zwiększyć zasięg sieci, w której zainstalowano maksymalną dozwoloną liczbę połączonych szeregowo koncentratorów; używane jako urządzenia do podłączenia komputerów biurkowych, zapewniają ich użytkownikom najwyższą możliwą wydajność pracy.

Mostek (bridge) - urządzenie, które analizuje pakiety na poziomie warstwy łącza danych (ang. Data Link Layer – DLL) modelu OSI/ISO. W trakcie pracy analizuje stworzoną przez siebie tablicę forwardingu (ang. Forwarding DataBase – FDB lub MAC DataBase), zawierającą numery portów (interfejs E0/0, E0/1, itd...), do których przyłączone są urządzenia oraz adresy sprzętoweMAC. Mosty działają w trybie nasłuchu (ang. promiscuous mode) i odbierają dane krążące w medium transmisyjnym. Aby określić, jakie urządzenia znajdują się w poszczególnych segmentach sieci (skojarzonych z poszczególnymi portami), mosty odczytują źródłowe adresy MAC z ramek danych. Na tej podstawie tworzona jest tablica forwardingu (w wolnym tłumaczeniu "tablica mostowania"). Mosty, w przeciwieństwie do przełączników, mają oprogramowanie w formie programowej a nie sprzętowej, są więc od przełączników wolniejsze (przełącznik używa układu scalonego ASIC wspomagającego podejmowanie decyzji o filtrowaniu). Mosty mogą mieć tylko jedną instancję drzewa rozpinającego przypadającą na jeden port, przełączniki mogą mieć ich wiele. Podobnie mosty mogą mieć tylko do 16 portów, zaś przełączniki mogą mieć ich setki.

Ruter (router) – urządzenie sieciowe pracujące w trzeciej warstwie modelu OSI. Na podstawie informacji zawartych w pakietach TCP/IP jest w stanie przekazać pakiety z dołączonej do siebie sieci źródłowej do docelowej, rozróżniając ją spośród wielu dołączonych do siebie sieci. Proces kierowania ruchem nosi nazwę trasowania, routingu lub rutowania. Trasowanie musi zachodzić między co najmniej dwiema podsieciami, które można wydzielić w ramach jednej sieci komputerowej. Urządzenie tworzy i utrzymuje tablicę trasowania, która przechowuje ścieżki do konkretnych obszarów sieci oraz metryki z nimi związane (odległości od siebie licząc kolejne routery). Skuteczne działanie routera wymaga wiedzy na temat otaczających go urządzeń, przede wszystkim innych routerów oraz przełączników. Może być ona dostarczona w sposób statyczny przez administratora, wówczas nosi ona nazwę tablicy statycznej lub może być pozyskana przez sam router od sąsiadujących urządzeń pracujących w trzeciej warstwie, tablice tak konstruowane nazywane są dynamicznymi. Podczas wyznaczania tras dynamicznych router korzysta z różnego rodzaju protokołów trasowania i polega przede wszystkim na odpytywaniu sąsiednich urządzeń o ich tablice trasowania, a następnie kolejnych w zależności od zapotrzebowań ruchu, który urządzenie obsługuje.

24. Idea wirtualnej sieci (VLAN)

Sieć VLAN (ang. Virtual LAN) to wydzielona logicznie sieć urządzeń w ramach innej, większej sieci fizycznej. Urządzenia tworzące sieć VLAN, niezależnie od swojej fizycznej lokalizacji (przełącznika do którego są podłączone), mogą się swobodnie komunikować ze sobą, a jednocześnie są odseparowane od innych sieci VLAN, co oznacza, że na poziomie przełącznika nie ma żadnej możliwości skomunikowania urządzeń należących do dwóch różnych sieci VLAN (dotyczy to także ramek rozgłoszeniowych). Sieci VLAN konfiguruje się w przełącznikach, urządzeniach sieciowych warstwy 2 modelu ISO/OSI. Jedna sieć VLAN może swym zasięgiem obejmować wiele przełączników, a w najprostszym przypadku tworzona jest w jednym przełączniku. Sieć VLAN identyfikowana jest poprzez liczbę całkowitą.
Ze stosowaniem sieci VLAN wiąże się kilka korzyści. Pozwalają one ograniczyć ruch rozgłoszeniowy, gdyż rozgłaszane ramki trafiają tylko do komputerów w obrębie danej sieci VLAN, nie „zalewają" całej sieci LAN. Ponadto, stosując sieci VLAN łatwo jest dostosować strukturę sieci do zmian w organizacji, ponieważ administrator może dokonać zmian topologii sieci programowo, a nie sprzętowo. Na przykład jeśli użytkownik należący do danej sieci VLAN zmienia stanowisko pracy, administrator po prostu konfiguruje przełącznik tak, by nowe stanowisko należało do odpowiedniej sieci VLAN. Do odzwierciedlenia zmiany administrator używa oprogramowania, a nie sprzętu (okablowania). Taka elastyczność jest szczególnie ceniona w dużych sieciach, w których często zachodzą zmiany w fizycznej topologii sieci. I wreszcie, podział sieci fizycznej na wiele sieci VLAN zwiększa bezpieczeństwo sieci komputerowej już z racji samej tylko separacji ruchu sieciowego w różnych sieciach VLAN

25. Połączenie typu TRUNK.

Gdy do sieci VLAN należą porty z różnych przełączników, konieczne jest skonfigurowanie specjalnego połączenia między przełącznikami (trunk), poprzez które przekazuje się informacje o sieciach VLAN - jest ono ustanawiane przez interfejsy Fast-Ethernet (100 Mb/s). Połączenia typu trunk między przełącznikami realizowane są z wykorzystaniem specjalnego protokołu, np. ISL (Inter-Switch Link) firmy Cisco, dostępnego między innymi na przełącznikach Catalyst 1900 (przełącznik 1900 faktycznie obsługuje protokół Dynamic ISL). ISL pracuje w warstwie drugiej modelu OSI, wymaga interfejsów FastEthernet i może być stosowany na połączeniach punkt-punkt między dwoma przełącznikami, między przełącznikiem a routerem, a także między przełącznikiem a serwerem wyposażonym w specjalną kartę sieciową obsługującą protokół ISL (np. firmy Intel). Protokół ISL hermetyzuje standardowe ramki Ethernet, dodając własny 26-bajtowy nagłówek oraz sumę kontrolną CRC. Protokół ten musi być obsługiwany przez obydwa końce połączenia, w przeciwnym razie taka ramka będzie nieczytelna dla strony odbiorczej. Jednym z podstawowych pól nagłówkowych jest 15-bitowe pole VLAN ID, w którym umieszczany jest identyfikator sieci VLAN (kolor). Dzięki temu możliwe jest identyfikowanie i przesyłanie ramek różnych sieci VLAN przez pojedyncze łącze trunk (p. rys.). Tylko 10 bitów pola VLAN ID jest w praktyce wykorzystywane, co pozwala obsługiwać maksymalnie 1024 sieci VLAN.