projektowanie sieci komputerowych

wykład 2 część 1
projektowanie topologii sieci

zakres wykładu

- **Część II.**
  Logiczny projekt sieci

- projektowanie topologii sieci
- projektowanie strukturalnego modelu adresacji i nazewnictwa w sieci
- wybór technik mostkowania i komutacji oraz protokołów wyboru trasy
- ustalenie strategii bezpieczeństwa i zarządzania siecią

literatura podstawowa

Priscilla Oppenheimer

Top-Down Network Design

Third Edition

Cisco Press 2010

projektowanie topologii sieci

- topologia - jest mapą intersieci wskazującą segmenty sieci, punkty połączeń i grupy użytkowników
- celem topologii jest pokazanie *geometrii sieci* a nie jej fizycznej geografii czy implementacji
- w fazie tej, *identyfikuje się* sieci i punkty połączeń między nimi, rozmiary sieci i zakresy sieci oraz typy urządzeń sieciowych, ale nie konkretne urządzenia
- faza logicznego projektu *musi poprzedzać* projekt fizyczny, ze względu na spełnienie wymagań inwestora co do skalowalności i adaptowalności sieci

topologie sieci

- topologie hierarchiczne
- topologie nadmiarowe
- topologie bezpieczne

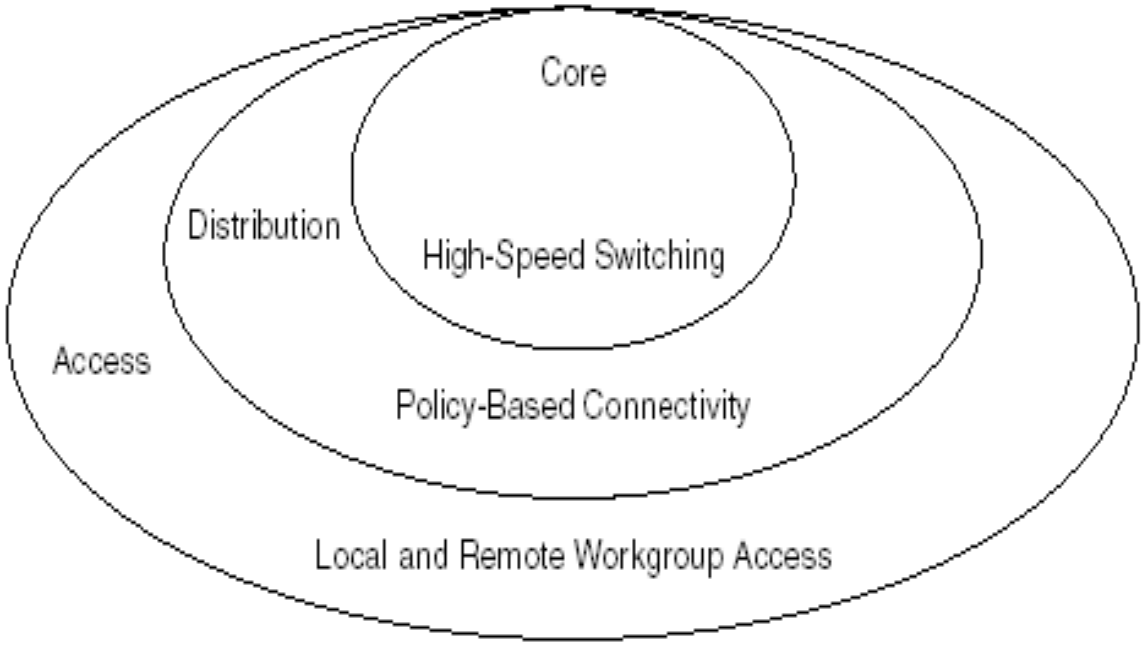
- po zapoznaniu się z materiałem wykładu, słuchacz będzie przygotowany do zaprojektowania hierarchicznej, nadmiarowej i bezpiecznej topologii sieci, spełniającej wymagania inwestora

zalety hierarchicznego projektu sieci

- projekt taki jest oszczędny co do kosztów, łatwy do zrozumienia, łatwo podlegający zmianom (skalowalny) i ułatwiający wykrywanie błędów

hierarchiczny projekt sieci

- ma trzy warstwy: rdzeń, warstwę dystrybucji i warstwę dostępu
- rdzeń: optymalny transport między stronami
- dystrybucja: łączność zgodnie z określoną polityką
- dostęp: użytkownika albo grupy do sieci



rdzeń

- *szkielet sieci*, wykorzystujący techniki szybkiego przełączania, nieodzowny dla łączności w firmie
- *cechy*: wysoka niezawodność, nadmiarowość, tolerancja na błędy, adaptowalność do zmian, niewielkie opóźnienia, dobra zarządzalność, unikanie czasochłonnego operowania na pakietach i filtrowania, ze *średnicą* (tzn. liczbą etapów od jednego krańca do drugiego) ograniczoną i spójną (taką samą między różnymi parami komputerów)
- ograniczenie średnicy intersieci daje przewidywalną wydajność sieci i łatwiejsze szukanie błędów

funkcje warstwy dystrybucji

- polityka
- bezpieczeństwo
- agregacja adresów
- dostęp z oddziału albo grupy użytkowników
- określenie domeny rozgłaszania i rozsyłania
- wybór trasy między wirtualnymi sieciami lokalnymi
- translacja między sieciami lokalnymi (Ethernet i TR)
- redystrybucja pomiędzy domenami wyboru trasy (między różnymi protokołami wyboru trasy)
- granica między statycznym a dynamicznym protokołem wyboru trasy

implementacja polityki

cechy systemu operacyjnego IOS na ruterze Cisco pozwalają na implementację polityki, w tym na:

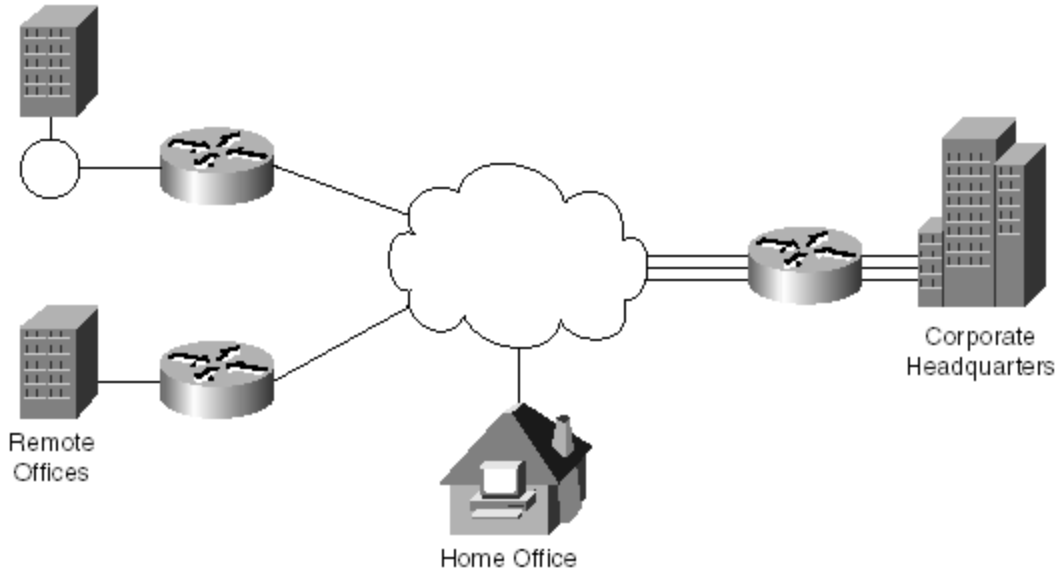
- filtrowanie adresem nadawcy albo adresem odbiorcy
- filtrowanie na portach wejściowych i wyjściowych
- ukrycie wewnętrznych numerów sieci za pomocą filtrowania trasy
- statyczny wybór trasy
- wprowadzenie mechanizmów jakości usług

warstwa dostępu

- zapewnia dostęp użytkownikowi do lokalnego segmentu sieci
- realizowana jest przez komutowaną sieć LAN o dzielonej szerokości pasma na obszarze kampusu
- mikrosegmentacja za pomocą komutatorów LAN, zapewnia dużą szerokość pasma grupom użytkowników, za pomocą podziału domeny kolizji w segmentach Ethernetu albo redukcji liczby stacji przechwytujących znacznik w sieciach TR
- dla małych biur (SOHO), zapewnia zdalny dostęp stosując technologie sieci WAN: ISDN, Frame Relay i linie dzierżawione

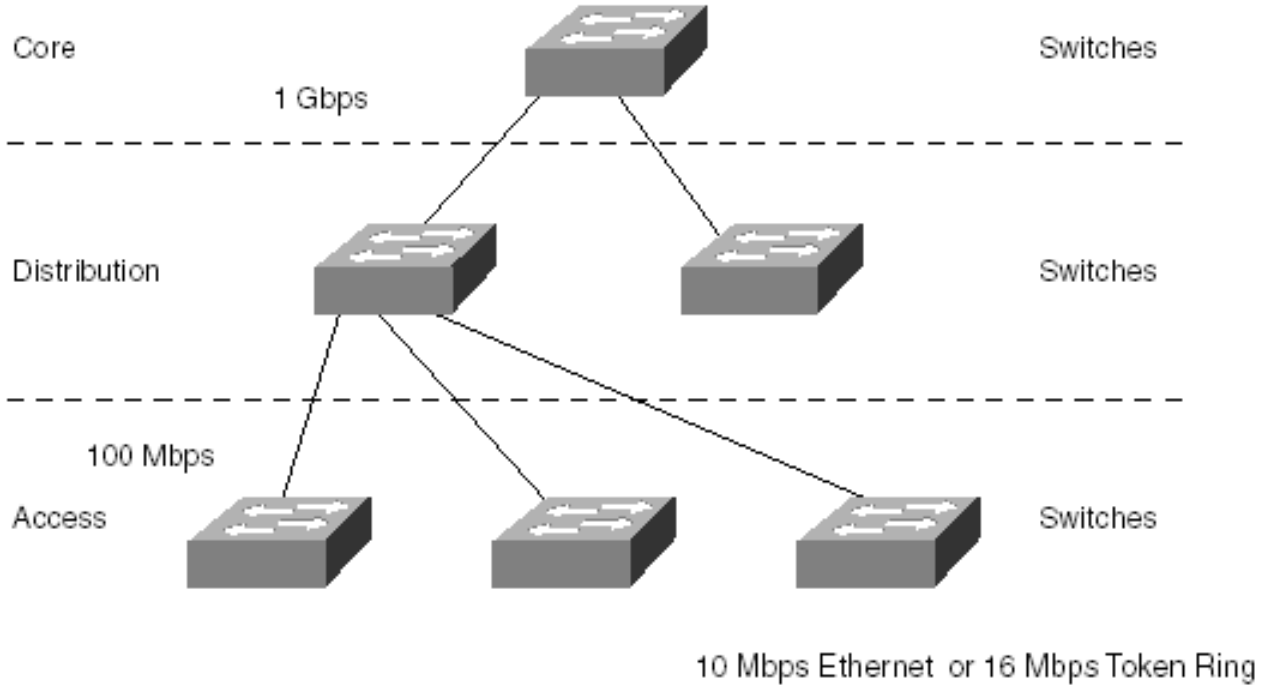
projekt hierarchiczny topologia gwiazdy

- hub-and-spoke topology



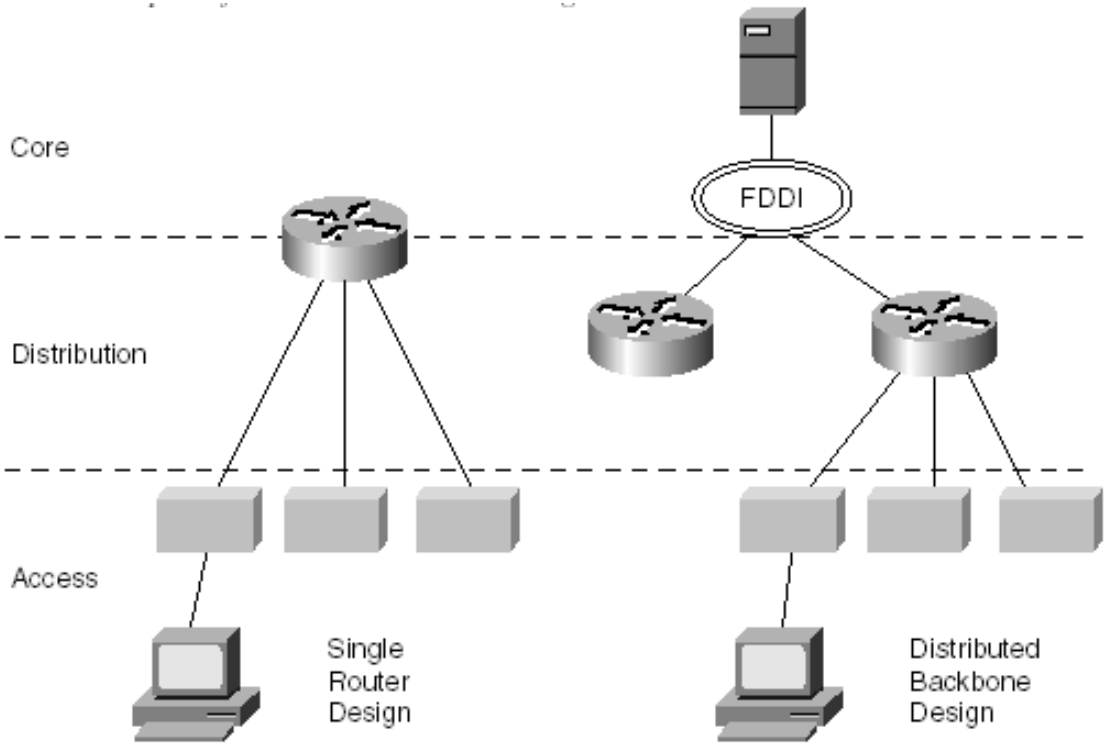
projekt hierarchiczny na komutatorach

- przykład



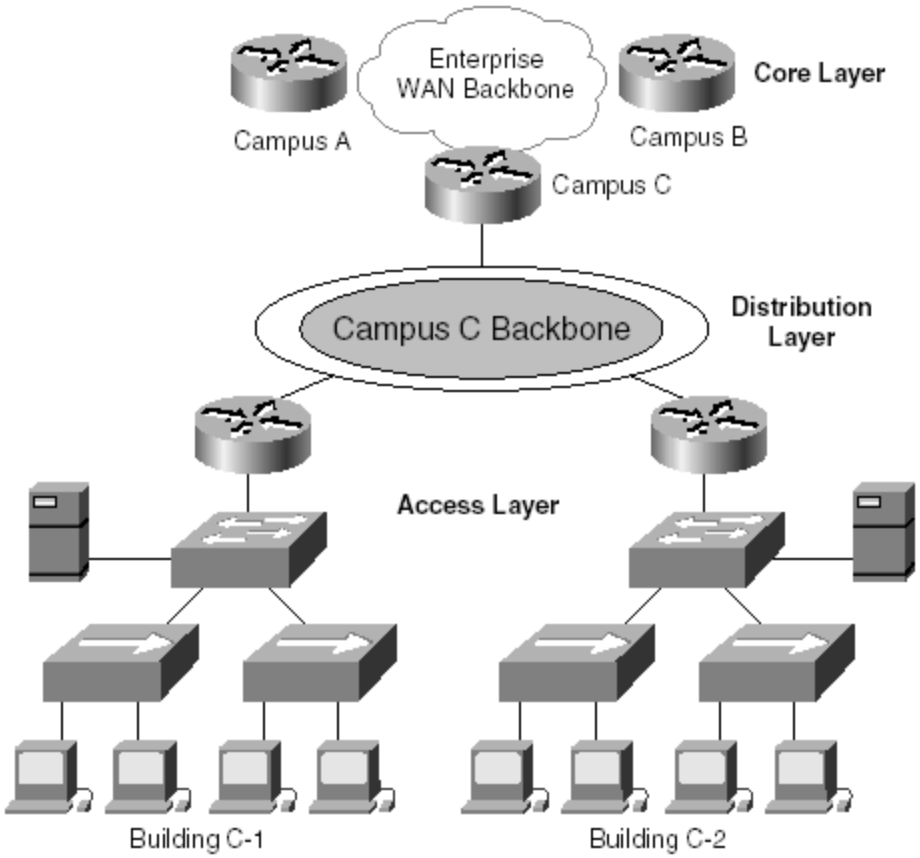
projekt hierarchiczny na ruterach

- przykład



hierarchiczny projekt sieci

- typowy



hierarchiczny projekt sieci

- szybkie rutery WAN przenoszą ruch poprzez szkielet firmy (warstwa rdzenia)
- rutery o średniej prędkości łączą budynki w każdym kampusie (warstwa dystrybucji)
- komutatory i koncentratory łączą urządzenia użytkowników i serwery wewnątrz budynków (warstwa dostępu)

dlaczego stosuje się hierarchiczny projekt sieci ?

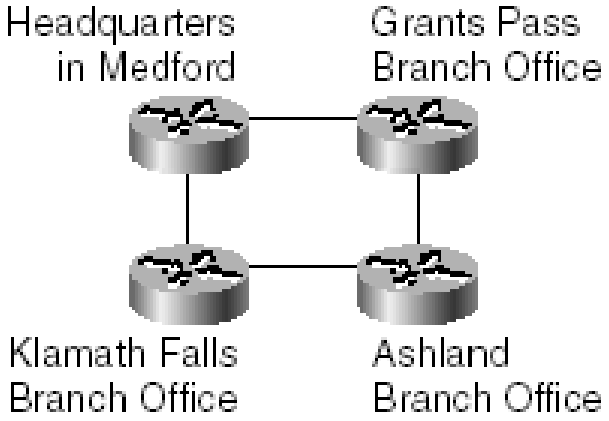
- sieci bez planu – *fur-ball networks („futrzaste” kule)*
- *sieci płaskie* - zwiększenie obciążenia procesorów przez obsługę rozgłaszań, i aktualizacje wyboru trasy
- hierarchia minimalizuje koszty, ułatwia planowanie pojemności, ułatwia zarządzanie, lokalizację błędów, i ćwiczenie personelu, ułatwia aktualizację i skalowanie
- hierarchia pozwala na sumowanie tras i ułatwia stosowanie protokołów wyboru trasy

płaska topologia

- płaska topologia odpowiednia dla małych sieci
- każde urządzenie sieciowe ma praktycznie te same zadania

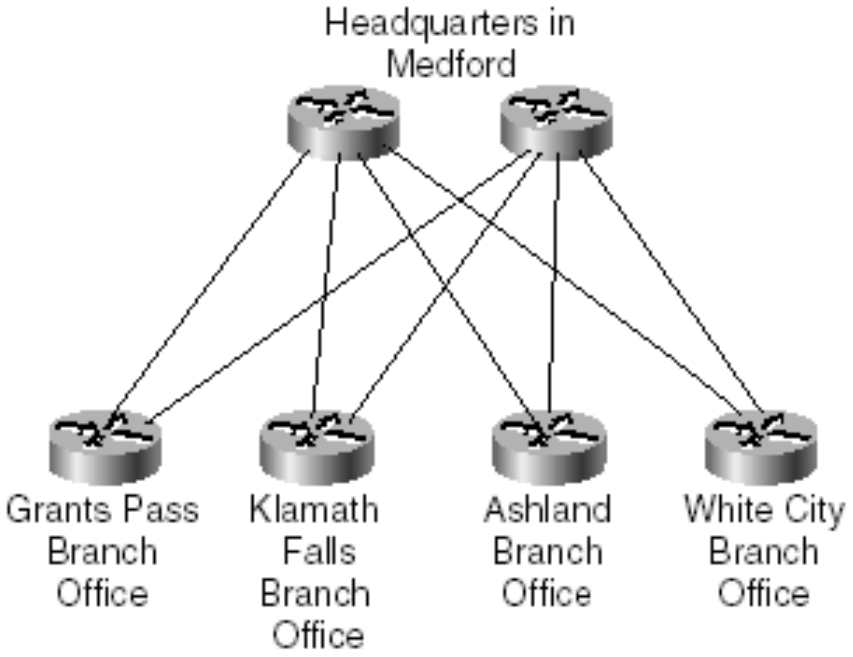
płaska topologia w sieci WAN

- sieć WAN dla małej firmy może składać się z kilku lokalizacji połączonych w pętlę
- każda lokalizacja ma ruter WAN łączący się z sąsiednią lokalizacją łączem dwupunktowym
- płaska topologia nie jest zalecana dla sieci WAN o wielu lokalizacjach



hierarchiczna nadmiarowa topologia w sieci WAN

- skalowalność, wysoka dostępność, małe opóźnienie



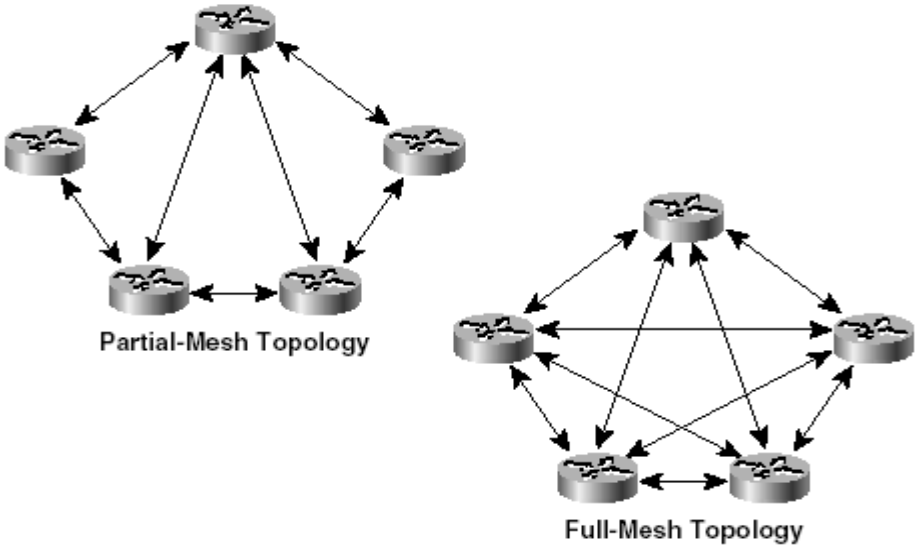
płaska topologia w sieci LAN

- typowa dla małej sieci LAN, gdzie komputery i serwery dołączone są do jednego lub kilku koncentratorów, a metodą dostępu jest przekazywanie znacznika albo CSMA/CS
- dla sieci o dużych wymaganiach co do szerokości pasma, poleca się dołączanie komputerów i serwerów do komutatorów (=urządzeń w warstwie 2), zamiast do koncentratorów, wtedy sieć jest dzielona na małe domeny szerokości pasma, tak więc mała liczba urządzeń konkuruje o szerokość pasma w danej chwili

płaska topologia w sieci LAN

- komutatory pozwalają przeznaczyć określoną szerokość pasma dla określonego portu
- komutatory nie dzielą domeny rozgłaszania, robią to dopiero rutery

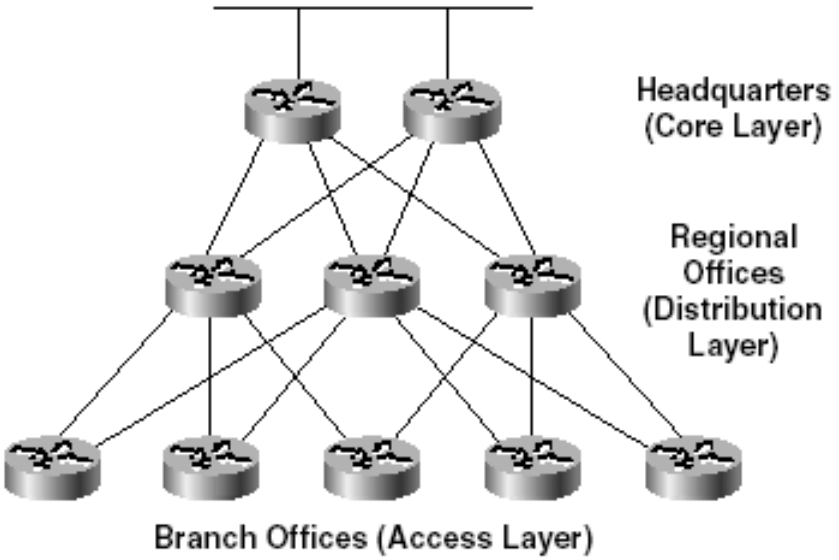
topologia częściowej i pełnej kraty



- liczba łączy w topologii pełnej kraty = ($N(N-1)$)/2
- większa dostępność, drogie rozwiązanie, trudne do optymalizacji, wyszukiwania błędów i aktualizacji

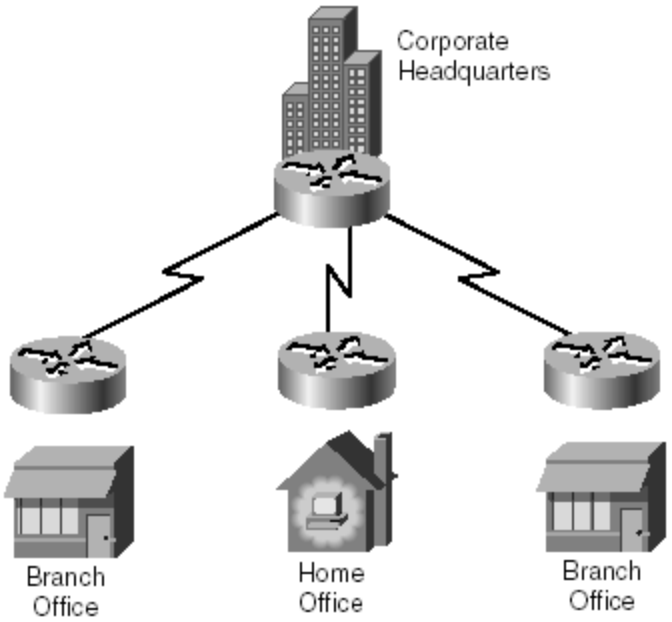
hierarchiczna topologia częściowej kraty

- klasyczne rozwiązanie dla firmy



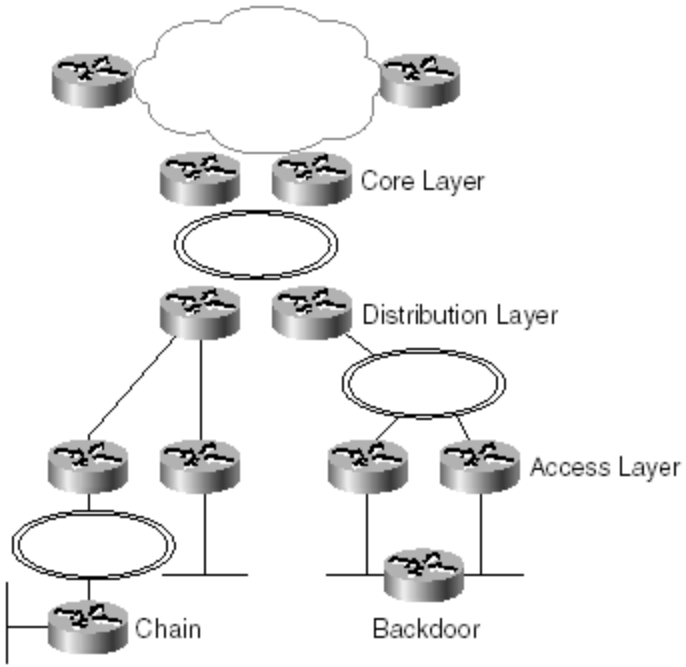
hierachiczna topologia „piasta i szprychy” (gwiazda)

- *hub-and-spoke*
- *dla średnich firm*



błędy projektowania

- *dodanie łańcucha* (=czwarta warstwa)
- *tylne drzwi* (problemy z wyborem trasy, z dokumentacją sieci i wyszukiwaniem błędów)



kolejność projektowania warstw

- wpierw warstwa dostępu, dokładniej planujesz pojemności w warstwie dystrybucji i rdzenia
- potem warstwa dystrybucji
- na końcu warstwa rdzenia
- każdą warstwę projektujesz stosując moduły i hierarchię, a następnie planujesz ich połączenie analizując wielkość ruchu, przepływy i zachowanie

topologie nadmiarowe

- przy projektowaniu topologii dla inwestora, który ma systemy, usługi albo ścieżki w sieci, o znaczeniu krytycznym, musisz oszacować prawdopodobieństwo że elementy te zawiodą i zaprojektować nadmiarowość, tam gdzie to konieczne
- rozważ wprowadzenie do projektu nadmiarowości dotyczących:
  - znalezienia adresu rutera przez stację
  - serwera
  - tras
  - łączy

znalezienie adresu rutera przez stację

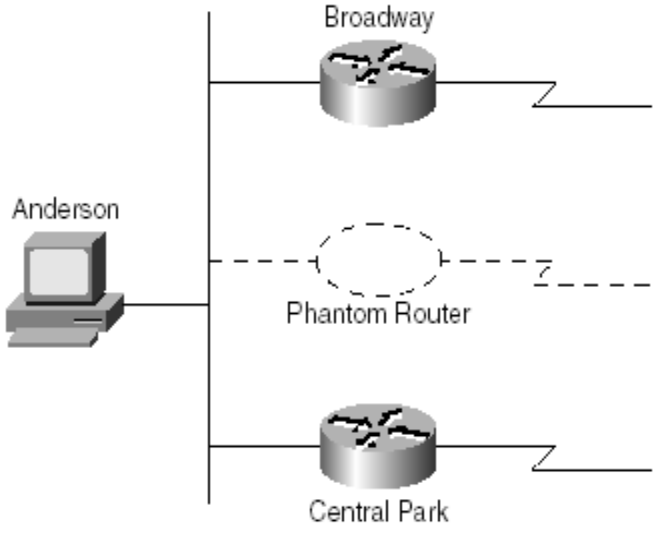
- protokół odwzorowania adresu - ARP (*Address Resolution Protocol*) – stacja nadaje ramkę ARP z adresem IP poszukiwanej stacji, poszukiwana stacja albo ruter pośredniczący (proxy) odpowiada adresem fizycznym
- jawna konfiguracja – stacja ma podany adres IP bramki domyślnej
- protokół znalezienia rutera - RDP (*Router Discovery Protocol*) – rozszerzenie ICMP pozwalające stacji i ruterowi uruchomić protokół RDP umożliwiający poznanie stacji adresu IP rutera
- protokół wyboru trasy (np. RIP albo OSPF)

znalezienie adresu rutera przez stację

- protokół IPX (*Internetwork Packet Exchange*) – rozgłasza komunikat „znajdź numer sieci”, ruter odpowiada
- *Apple Talk* – pamięta adres rutera, który jako ostatni nadał pakiet RTMP (Routing Table Maintenance Protocol)
- protokół HRSP *(Hot Standby Router Protocol)* firmy Cisco – stacja stosuje ruter fantom, kiedy ruter domyślny nie jest dostępny

protokół HRSP – ruter fantom reprezentuje prawdziwe rutery

- stacja Anderson stosuje ruter *fantom* jako ruter domyślny
- po uruchomieniu, rutery wybierają *Broadway* jako ruter aktywny. Ruter ten pracuje na rzecz rutera *fantom*. *Central Park* jest ruterem zapasowym
- kiedy stacja wysyła ramkę ARP aby znaleźć ruter domyślny, Broadway odpowiada adresem MAC rutera fantom
- kiedy Broadway zawodzi, Central Park staje się aktywny, zmiana ta jest transparentna dla stacji



nadmiarowość w serwerze

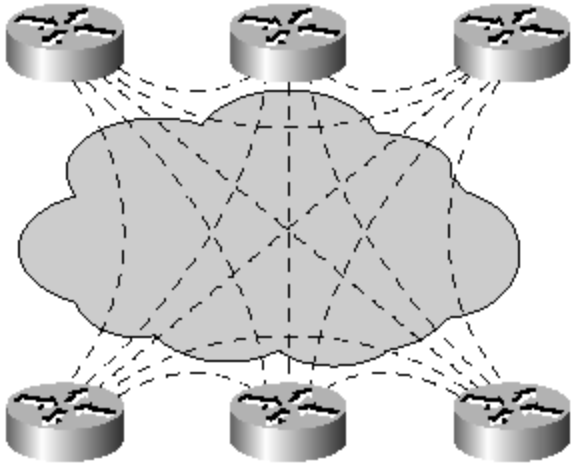
- serwery powielone (np. serwery na giełdzie)
- w oddzielnych sieciach i z oddzielnym zasilaniem
- wersja tańsza: powielenie dysków twardych:
  - *mirroring*: synchronizacja dwóch dysków
  - *duplexing*: dyski sterowane przez oddzielne kontrolery

nadmiarowość tras

- dwa cele: zrównoważenie obciążenia i minimalizacja czasu przestoju
- zrównoważenie obciążenia
  - rutery AppleTalk i IPX pamiętają z założenia tylko jedną trasę do zdalnej sieci, można to zmienić poleceniem **appletalk maximum-paths** albo **ipx maximum-paths** na ruterze Cisco
  - wszystkie ścieżki powinny mieć ten sam koszt
- minimalizacja czasu przestoju
  - protokoły wyboru trasy powracają do stanu ustalonego szybciej, gdy istnieje wiele ścieżek o tym samym koszcie do odbiorcy

minimalizacja czasu przestoju

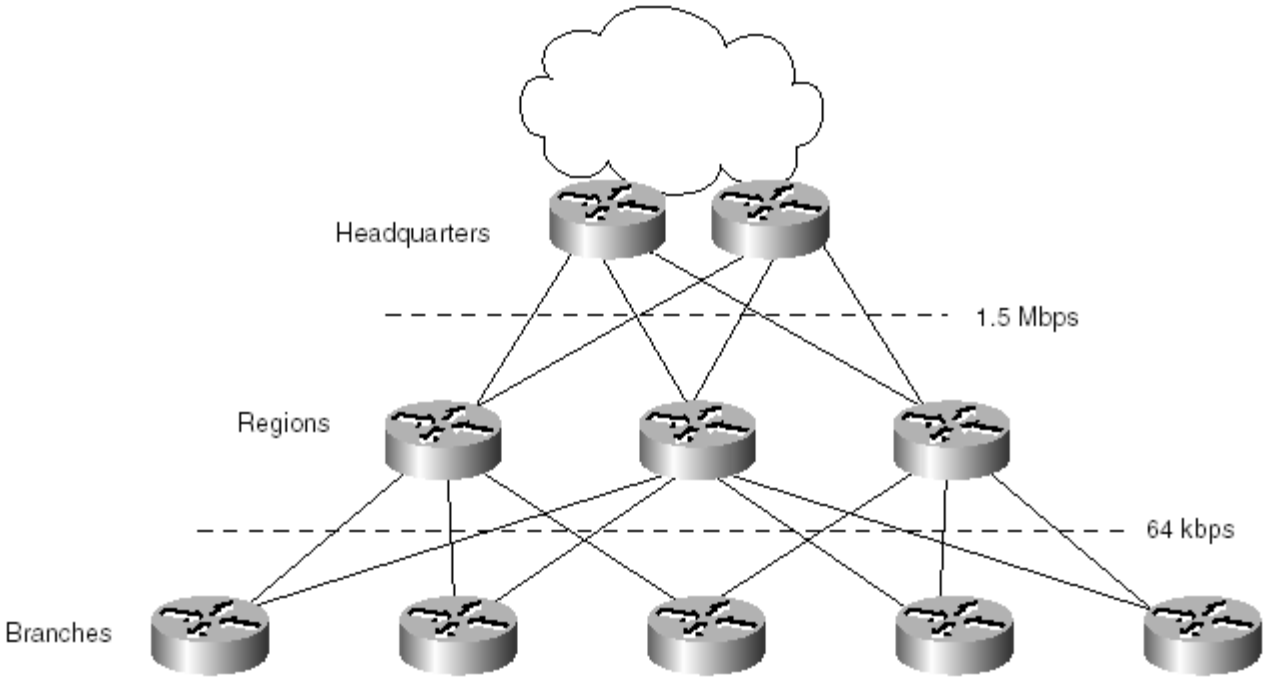
- przy stosowaniu topologii kraty awaria jednego łącza nie jest groźna
- topologia pełnej kraty: każdy ruter ma łącze z każdym ruterem
- zwiększa liczbę rozgłaszań w sieci (powinna być mniejsza niż 20% całego ruchu)



(6*5)/2=15 Circuits

klasyczne rozwiązanie

- topologia częściowej kraty z nadmiarowością
- projekt hierarchiczny

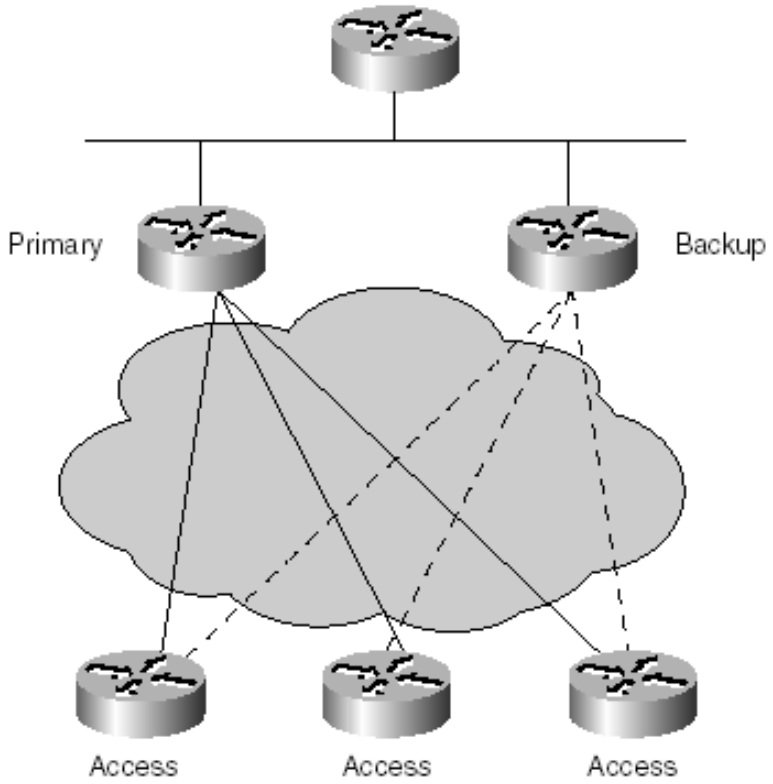


nadmiarowość łączy

- w aplikacjach o znaczeniu krytycznym
- w sieciach komutowanych zapasowe łącza
  - zmniejszają czas niedostępności sieci
  - pętle powodują burzę rozgłaszań (broadcast storm)
  - algorytm drzewa rozpinającego (IEEE 802d1) do unikania pętli, jest tylko jedna aktywna ścieżka między parą stacji, nadmiarowa ścieżka staje się aktywna, gdy dotychczasowa aktywna ścieżka nie działa
  - zapasowe łącza w powiązaniu ze zrównoważeniem obciążenia i agregacją kanału (wiele kanałów na ruterze, n.p. kanałów B w ISDN) - protokół MPPP (Multilink Point-to-Point Protocol) w Cisco

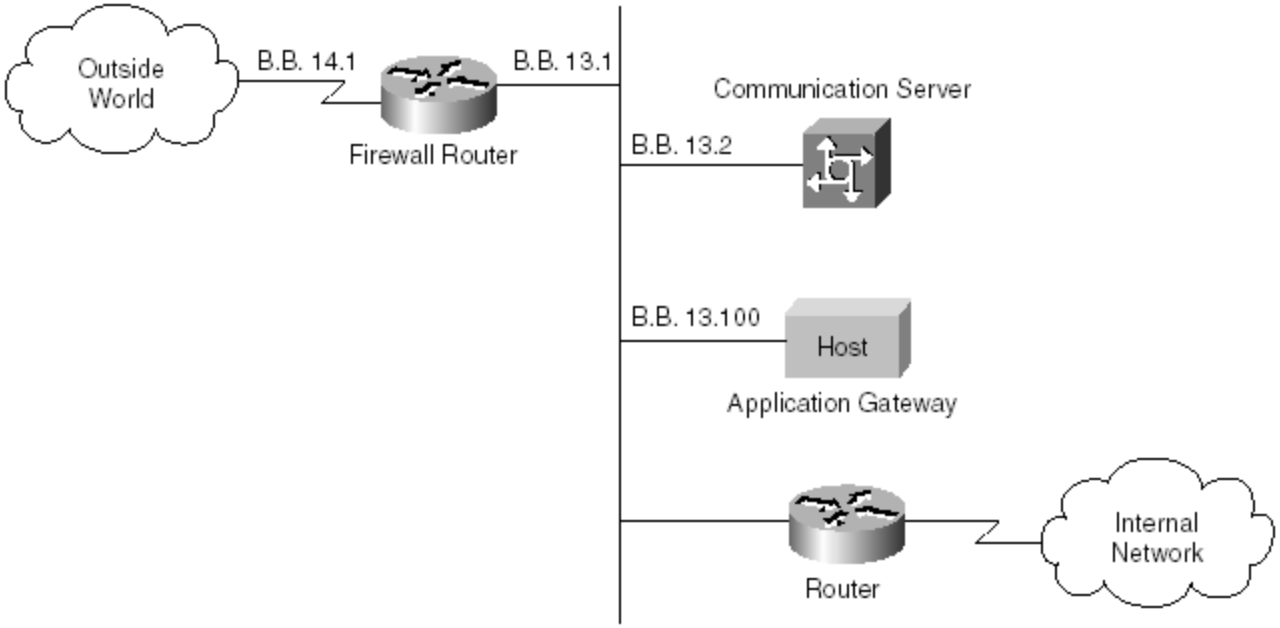
łącza zapasowe w sieci WAN

- zapewniają nadmiarowość dla łączy WAN o znaczeniu krytycznym, stosują ścieżki statyczne, ścieżka zapasowa (ISDN albo łącze komutowane) używana jedynie przy awarii ścieżki pierwotnej (łącza dzierżawionego)



topologia bezpieczna

- inne aspekty: szyfrowanie i listy dostępu później
- ściana ogniowa (*firewall*) - chroni sieć przed inną, niewiarygodną siecią, za pomocą pary mechanizmów: blokowania i zezwalania, realizowana n.p. na ruterze, albo na tak zwanym komputerze bastionie



topologie w nadmiarowym projekcie sieci

- nadmiarowy projekt sieci pozwala spełnić wymagania co do dostępności sieci, poprzez duplikację łączy i urządzeń sieciowych
- nadmiarowość eliminuje możliwość spowodowania awarii przez jeden element sieci, szczególnie w odniesieniu do aplikacji krytycznych
- elementem tym mógłby być ruter w rdzeniu, jednostka obsługi kanału, zasilacz, łącze WAN, sieć dostawcy usług, itd.
- nadmiarowość może być implementowana w sieci kampusowej (wzrost dostępności) i w sieci korporacyjnej (wzrost wydajności)
- nadmiarowość stosuj z umiarem, odnieś się do analizy celów ekonomicznych i technicznych inwestora

ścieżka zapasowa

- składa się z ruterów, komutatorów i łączy zapasowych miedzy nimi, które duplikują urządzenia i łącza ze ścieżki pierwotnej
- rozważ:
  - jak dużą pojemność powinna mieć ścieżka zapasowa?
  - jak szybko sieć powinna przełączyć się na ścieżkę zapasową, gdy ścieżka pierwotna zawiedzie?
- pojemność ścieżki zapasowej zazwyczaj mniejsza od pojemności ścieżki pierwotnej (czasem równa)
- dla aplikacji krytycznych automatyczne przełączenie ścieżek
- przetestuj działanie ścieżki zapasowej!!

zrównoważenie obciążenia

- pierwszym celem wprowadzania nadmiarowości jest spełnienie wymagań dostępności
- celem wtórnym jest poprawienie wydajności za pomocą zrównoważenia obciążenia między równoległymi łączami
- zrównoważenie obciążenia musi być zaplanowane i skonfigurowane
- pamiętanie ścieżki do zdalnego odbiorcy w pamięci podręcznej rutera – zrównoważenie obciążenia dla przepływów do różnych odbiorców
- zrównoważenie obciążenia z pakietu na pakiet

zaprojektowanie topologii sieci kampusowej

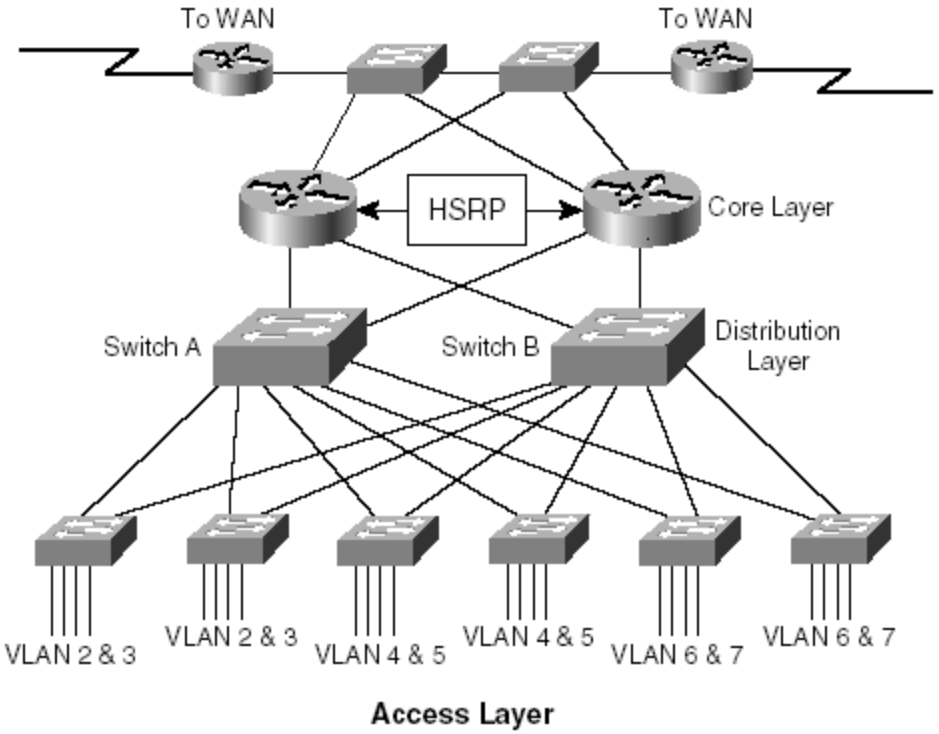
- topologia ta powinna spełniać wymagania inwestora dotyczące dostępności dając małe domeny rozgłaszania, nadmiarowe segmenty w warstwie dystrybucji, powielane serwery, i wiele dróg ze stacji do rutera pozwalających programować ten ruter
- powinna to być topologia hierarchiczna, oferująca dobrą wydajność, konserwację i skalowalność

wirtualna sieć lokalna VLAN

- *virtual LAN* – emulacja klasycznej sieci LAN, która pozwala na przesyłanie danych bez tradycyjnych ograniczeń fizycznych
- administrator sieci grupuje użytkowników, tak że mogą się porozumiewać, jakby byli podłączeni do tego samego łącza, chociaż są przyłączeni do różnych segmentów LAN
- firmy przecież nie mogą zagwarantować, że ludzie pracujący nad tym samym projektem będą razem, VLAN to zapewniają - połączenia logiczne są elastyczne
- przydział do VLAN na podstawie aplikacji, protokołów, wymagań wydajności i bezpieczeństwa, i wielkości ruchu
- VLAN pozwala podzielić dużą płaską sieć na podsieci, i realizuje podział domeny rozgłaszania

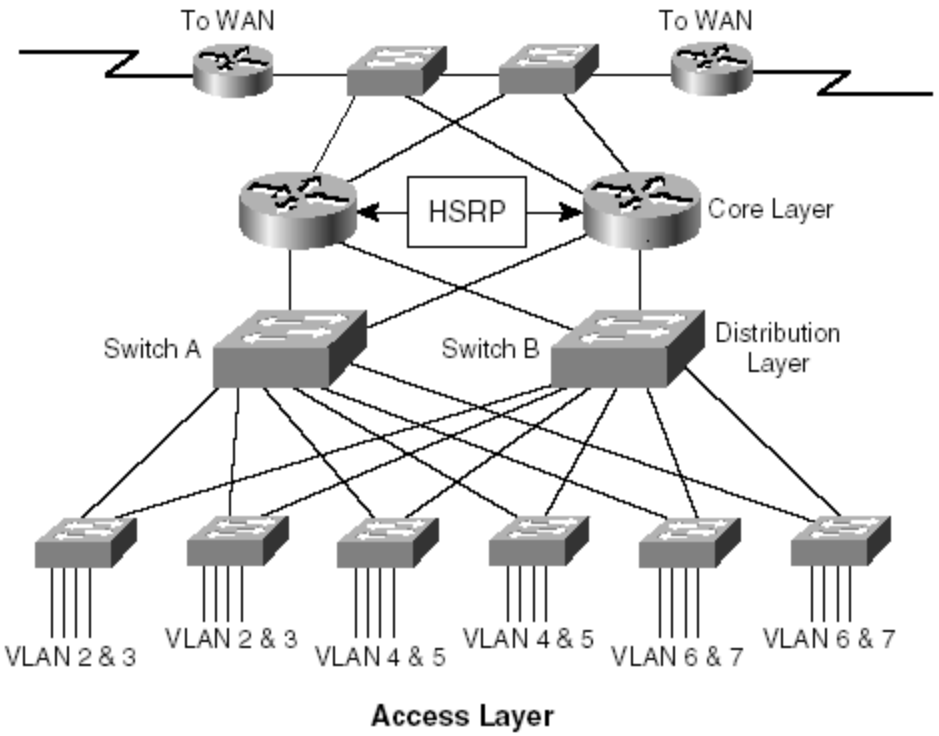
nadmiarowa sieć kampusowa

- nadmiarowe łącza między komutatorami – tolerancja na błędy i zrównoważenie obciążenia, bez pętli, z jedną ścieżką aktywną między stacjami (alg. STP).



nadmiarowa sieć kampusowa

- komutator A jako root bridge dla VLAN 2, 4 i 6
- komutator B jako root bridge dla VLAN 3, 5 i 7
- jeżeli któryś zawodzi, drugi go zastępuje



nadmiarowość w serwerze

- kandydaci do nadmiarowości: serwery plików, www, DHCP, nazw, baz danych, konfiguracji i rozgłaszania
- krytyczne są serwery DHCP – kopie DHCP (mirror) w warstwie dostępu (duże sieci) i dystrybucji (małe sieci) – unika się dużego ruchu
- w dużych sieciach serwer DHCP w innym segmencie sieci niż komputery korzystające z niego
- serwery nazw mniej krytyczne, implementują DNS (Domain Name Service), WINS (Windows Internet Naming Service), NBNS (NetBios Name Service), są w warstwie dostępu lub dystrybucji
- przy dużym koszcie, w zastępstwie powielenie dysków (mirroring lub duplexing)

nadmiarowość komunikacji stacji z ruterem

- stacje w sieci kampusowej muszą mieć dostęp do rutera, aby osiągnąć zdalne usługi, stąd komunikacja między nimi ma znaczenie krytyczne
- sposoby na wykrycie rutera przez stację Novell Netware, stację AppleTalk i stację IP
- stacja Novell Netware, gdy ma pakiet do nadania, nadaje *find-network-number-request* aby znaleźć trasę do celu i stosuje pierwszy ruter, który się odezwał

nadmiarowość komunikacji stacji z ruterem

- stacja AppleTalk pamięta adres rutera, który przesłał ostatni pakiet RTMP, ponieważ stacja może pamiętać tylko jeden taki adres, może się zdarzyć, że stacja wybierze ścieżkę, która zawiera dodatkowy etap (problem dodatkowego etapu):