Cisco Systems Poland

Lokalna Sieć Komputerowa

Wydajna i bezpieczna Sieć Lokalna w Jednostce Samorządu Terytorialnego

Cisco Systems Poland
Al. Jerozolimskie 146C
Warszawa, 02-305
Polska
http://www.cisco.pl

1. WSTĘP....3

2. BUDOWA SIECI LOKALNYCH LAN (*LOCAL AREA NETWORK*) 4

2.1. Zasady unikania zagrożeń w sieciach LAN 4

2.2. Rekomendacje dla sieci LAN 11

2.3. Podział funkcjonalny sieci LAN 12

2.4. Urządzenia rdzenia sieci 12

2.5. Urządzenia dostępowe w sieci 13

2.6. Uwagi eksploatacyjne i inwestycyjne 13

3. PRZYKŁADOWY PROJEKT SIECI LAN O WIELKOŚCI 300+ UŻYTKOWNIKÓW 15

4. PRZYKŁADOWY PROJEKT SIECI LAN O WIELKOŚCI 150 UŻYTKOWNIKÓW 17

5. PRZYKŁADOWY PROJEKT SIECI LAN O WIELKOŚCI 50 UŻYTKOWNIKÓW 19

6. SPECYFIKACJE PROPONOWANYCH URZĄDZEŃ 21

6.1 Rodzina Przełączników Catalyst 6500 21

6.2 Rodzina Przełączników Catalyst 4500 23

6.3 Rodzina Przełączników Catalyst 3750 25

7. PODSUMOWANIE 26

1. WSTĘP

Przemiany ostatnich lat związane z pojawieniem się Internetu i co za tym idzie nowych kanałów wymiany informacji, w coraz większym stopniu dotykają Jednostki Samorządu Terytorialnego (JST). Sieci komputerowe, traktowane 10 lat temu jako zbędny, nadmiarowy wydatek, są już praktycznie we wszystkich JST. Wyzwania stojące przed JST w najbliższych latach powodują jednak, że warto spojrzeć na tematykę budowy sieci od nowa.

Sieć komputerowa LAN w JST w najbliższym czasie będzie nie tylko siecią dla wymiany informacji wewnętrznych, ale również będzie pełnić rolę jednego z wielu elementów szerszego systemu – e-urzędu.

E-urząd determinuje nie tylko konkretne aplikacje wykorzystywane w JST, ale przede wszystkim modele wymiany informacji. Taki model to np. dostępność Centrum Przetwarzania Danych (nazywane często CPD, lub CD od angielskiej nazwy Data Center) zarówno dla użytkowników wewnętrznych jak i zewnętrznych. Pojawiają się tu, więc kwestie bezpieczeństwa sieci. W samym CPD z pewnością można wyróżnić aplikacje krytyczne dla działania JST, jak i te, które są istotne, ale pełnią rolę pomocniczą dla organizacji. Wynika to z konieczności wprowadzenia mechanizmów np. zapewnienia jakości usług. Podobnych aspektów związanych z działaniem sieci można wyróżnić jeszcze, co najmniej kilka.

Ważne jest, aby sieć komputerowa była budowana w sposób mądry i przemyślany, tak aby nie stanowiła wąskiego gardła i potrafiła sprostać wymaganiom coraz to nowych aplikacji. Dokument ten ma na celu przybliżenie zagadnień związanych z budową sieci LAN, wskazanie potencjalnych zagrożeń oraz sposobów ich unikania. Przedstawione także zostaną przykładowe implementacje sieci.

W niniejszym dokumencie została zamieszczona koncepcja budowy sieci lokalnych LAN dla Jednostek Samorządu Terytorialnego. Nowa sieć zakłada wyjście na przeciw pojawiającym się potrzebom tych jednostek, które wynikają z rozbudowy infrastruktury lub modernizacji sieci już istniejących. Przedstawione przykłady oraz założenia dotyczące budowy sieci LAN mają za zadanie posłużyć jako materiał poglądowy/edukacyjny do wstępnego projektu.

Szczegółowy projekt oraz kosztorys dla inwestycji pod strukturę Państwa sieci jest osobnym zadaniem, którego realizacją zajmuje się zwyczajowo Partner Cisco Systems.

Biuro Cisco Systems oferuje Państwu konsultacje na najważniejszym etapie czyli w fazie projektowej.

2. BUDOWA SIECI LOKALNYCH LAN (*LOCAL AREA NETWORK*)

Budowa sieci rozległej WAN bardzo często wiąże się z wdrożeniem aplikacji sieciowych bądź innych elementów funkcjonalnych wymagających zastosowania zdalnej komunikacji. Dotychczas wiele takich funkcjonalności było implementowanych w sieci WAN. Sieci rozległe oparte na urządzeniach Cisco posiadają możliwość implementacji funkcjonalności pozwalającej na zapewnienie odpowiedniego poziomu jakości transmisji dla aplikacji krytycznych z punktu widzenia działalności przedsiębiorstwa czy urzędu. Należy jednak pamiętać, że ogromny potencjał sieci rozległej w zakresie kształtowania polityki priorytetów może być łatwo zniwelowany przez brak odpowiednich mechanizmów dostępnych w urządzeniach sieci lokalnej LAN. Z tego powodu w rozwiązaniach sieciowych Cisco wprowadziło wiele funkcji również w urządzeniach sieci LAN. Krok ten ma na celu przygotowanie infrastruktury do realizacji takich zadań jak telefonia IP, wideokonferencje itp. Aplikacje te jako bardzo efektywne pod kątem ROI mogą spowodować szybszy zwrot z inwestycji.

2.1. Zasady unikania zagrożeń w sieciach LAN

Na podstawie analizy wielu sieci lokalnych określono następujące zagrożenia wynikające z wykorzystywania w sieci kampusowej koncentratorów oraz przełączników nieprzystosowanych do realizacji funkcji rdzeniowych:

- Zagrożenia związane z wydajnością i ciągłością pracy sieci:
    - Urządzenia typu hub charakteryzują się cechą współdzielenia pasma. Oznacza to, że urządzenie zdefiniowane jako 24-portowy Hub 10Mbps udostępnia pasmo 10Mbps – 24 użytkownikom. Statystycznie jeden użytkownik ma dla siebie znacznie mniej pasma. Dodatkowo metoda dostępu CSMA/CD powoduje, że realna przepustowość oferowana przez urządzenia typu hub to około 6 Mbps. Wynika z tego, że statystyczny użytkownik korzystający z takiego urządzenia otrzymuje przepustowość 250Kbps; realnie pasmo dostępne użytkownikowi rzadko jest większe niż 2Mbps. Komunikacja pomiędzy urządzeniami mającymi różną adresację IP lub IPX musi zaś odbywać się za pośrednictwem routera, który może dodatkowo spowolnić pracę sieci,
    - Gdy w strukturach występują połączenia łańcuchowe urządzeń typu hub, to urządzenie będące na końcu łańcucha otrzymuje procent pasma dostępnego dla użytkowników urządzenia poprzedniego w łańcuchu. Patrząc tylko statystycznie, można by powiedzieć, że traktując końcowy hub jako stację roboczą - otrzyma on statystycznie 250Kbps, które „rozdzieli” pomiędzy użytkowników doń przyłączonych. Jest to duże uproszczenie, bo oczywiście pasmo dostępne dla użytkowników jest większe, warto jednak zaznaczyć, że przesyłając ruch od grupy użytkowników do huba „nadrzędnego” korzystamy z

jednego portu, który w tym urządzeniu bardzo często nadaje/odbiera dane, zabierając pasmo pozostałym użytkownikom. W podobnych strukturach badanych w różnych systemach sieciowych (biurowy, produkcyjny) pasmo dla użytkownika na końcu łańcucha niejednokrotnie spadało poniżej 500Kbps,

- Sytuacja opisana w poprzednim punkcie może wpływać na urządzenia rdzenia sieci. Wynika to z faktu występowania tzw. burz (sztormów) kolizyjnych. Sytuacja taka ma miejsce w systemach z dostępem do medium zgodnym z CSMA/CD (współdzielony Ethernet) w chwili, gdy wielu użytkowników żąda dostępu do medium w krótkim odstępie czasu. Sztorm kolizyjny powoduje zablokowanie transmisji w danym segmencie sieci. Przełącznik, który jest przyłączony do takiego segmentu (switch sam w sobie rozdziela domeny kolizyjne) nie może przesłać danych do niego skierowanych, napływających z innych segmentów sieci. Dane te są buforowane w buforach portów przełącznika. Jeżeli przełączniki rdzeniowe są urządzeniami nieprzygotowanymi do realizacji takich funkcji bądź też przełączniki takie obsługują wiele portów z przyłączonymi hubami (potencjalne miejsce występowania sztormów kolizyjnych) to może bardzo łatwo dojść do wysycenia tychże buforów oraz obciążenia przełącznika uniemożliwiając efektywną pracę,

- W systemach sieciowych zazwyczaj dostępne jest okablowanie pionowe (rdzeniowe połączenia światłowodowe), które ułożone jest nadmiarowo. Te drogi połączeniowe mogą być wykorzystane bądź na żądanie – z ingerencją administratora bądź automatycznie. Pierwsza opcja jest konieczna do zastosowania w przypadku, gdy w systemie sieciowym stosowane są huby. Huby nie dopuszczają dostępności hosta przez dwie drogi połączeniowe. Drugi przypadek jest z powodzeniem stosowany w sieciach przełączanych. Przełączniki sieciowe umożliwiają zestawienie dwóch (lub więcej) alternatywnych dróg połączeniowych, przy czym aktywna w danej chwili jest tylko jedna droga (802.1D, 802.1s/w). W szczególnym przypadku, gdy dwie alternatywne drogi kablowe łączą dwa przełączniki (nie tworzymy „trójkąta" czy „kwadratu" połączeń, lecz budujemy połączenie punkt-punkt wykorzystując dwie drogi i kablowe), możliwe jest zastosowanie tzw. grupowania portów (LACP 802.3ad), które pozwala na utrzymanie obu tych dróg w stanie aktywnym, co powoduje zwiększenie przepustowości pomiędzy zaangażowanymi węzłami. W przypadku awarii jednego z połączeń następuje bądź rekonfiguracja sieci (802.1D, 802.1s/w), która może potrwać od kilku sekund do kilkunastu minut w zależności od złożoności sieci, bądź zmniejszenie przepustowości połączenia o przepustowość uszkodzonego łącza (802.3ad),

- Brak możliwości realizacji połączenia poprzez dwie drogi kablowe (STP) powoduje brak możliwości realizacji węzła centralnego z wykorzystaniem redundantnych urządzeń (przełączników), lub też

redundantnych modułów przełączających w urządzeniach modularnych,

- Broadcasty – wysyłane przez wszystkie stacje, a wykorzystywane przez wiele protokołów sieciowych (np. ARP), mogą być przyczyną natłoków w sieci i utylizacji pasma przewidzianego dla użytkowników. W sytuacjach ekstremalnych broadcasty mogą konsumować nawet ponad 50% pasma przewidzianego dla użytkowników. W nowo projektowanych urządzeniach sieciowych stosuje się metody tzw. broadcast supression – ograniczania ilości pakietów broadcast w poszczególnych segmentach sieciowych. Pozwala to na znacznie efektywniejsze wykorzystanie zasobów sieciowych,

- Niepożądany ruch w sieci może spowodować blokowanie działania pewnych usług. Jednym z przykładów ruchu, który może spowodować takie niedogodności jest ruch broadcast, opisany powyżej. Wygenerowanie dużego ruchu broadcast w sieci jest zadaniem banalnie prostym (Smurf attack). Inne typy tego rodzaju ruchu to ICMP Flooding, UDP Flooding, SYN Flooding. Wszystkie powyższe są znanymi atakami sieciowymi DoS – na pasmo dostępne w sieci. Ruch taki jest stosunkowo łatwo definiowalny – co powoduje, że można stosunkowo łatwo utworzyć odpowiednie filtry blokujące taki ruch. Szkopuł w tym, że ruchu TCP z flagą SYN nie można zablokować w 100%. Podobnie blokowanie ruchu ICMP może spowodować utrudnienia w diagnostyce sieci. Konieczne jest, zatem nie tyle filtrowanie, co ograniczanie pasma dostępnego dla określonego gatunku ruchu. Realizowane jest to zazwyczaj poprzez mechanizm CAR (Comitted Access Rate) gwarantujący przesłanie pakietów spełniających wymagania „filtra" tylko do pewnego poziomu przepustowości np. „przepuszczamy ruch ICMP z maksymalną przepustowością 200Kbps", co jest zupełnie wystarczające dla potrzeb diagnostyki, a uniemożliwia przeprowadzenie ataku ICMP Flooding. Mechanizm ten może być również wykorzystywany do ograniczania pasma dla aplikacji, do internetu, dla użytkownika etc.

- Zagrożenia związane z zarządzaniem:

  - Obecne badania kosztów utrzymania sieci wskazują, że struktury homogeniczne (z urządzeniami pochodzącymi od jednego producenta) są zdecydowanie tańsze w utrzymaniu (nawet do 30% całościowego kosztu posiadania sieci w okresie 3 lat – wliczając m.in. koszt zakupu i utrzymania urządzeń). Duża część tych oszczędności wiąże się z łatwością zarządzania strukturami homogenicznymi – jedna platforma zarządzająca, jeden rodzaj interfejsu administratora, jeden sposób zbierania i analizy logów etc.,

  - Postawą działań strategicznych i rozwojowych w strukturach sieciowych jest dokładna analiza statystyk otrzymywanych z poszczególnych urządzeń. Również wprowadzenie dodatkowych połączeń, wymiana urządzeń itp. jest determinowane otrzymywanymi statystykami per port, per VLAN, per użytkownik. Przydatne są także

narzędzia śledzenia użytkownika (user tracking), analizy ruchu kopiowanego z portu lub całej sieci VLAN (funkcje SPAN i RSPAN). Jeszcze innym – najbardziej widocznym – narzędziem jest możliwość wizualizacji połączeń (mapa) z aktualizacją w czasie rzeczywistym,

- W większości dużych systemów sieciowych administracją zajmuje się grupa osób. Wynika to z konieczności zabezpieczenia ciągłości pracy i monitoringu sieci. Zazwyczaj jednak podstawową obsługą sieci zajmują się np. dwie osoby. Pozostałe mają możliwość monitoringu urządzeń. W takich przypadkach wymagane jest zastosowanie wielopoziomowego systemu dostępu administracyjnego tak, aby uprawnienia administratorów zajmujących się siecią, na co dzień, były wyższe aniżeli pozostałych użytkowników.

- Zagrożenia związane z bezpieczeństwem:

  - Wymiana informacji pomiędzy grupami roboczymi/działami powinna być kontrolowana. Oznacza to, konieczność wykreowania wirtualnych sieci dla grup roboczych, serwerów etc. Dla stworzonych sieci wirtualnych możemy skonfigurować i przypisać filtry określające rodzaj ruchu (Access List), akceptowanego. Przynależność do sieci VLAN może być ustalana statycznie, bądź dynamicznie – w szczególności z wykorzystaniem protokołu 802.1x. Logowanie odbywa się wtedy z podaniem parametrów użytkownik/hasło,

  - Dostęp zarządzający do urządzeń zazwyczaj jest specjalnie autoryzowany, czasem (coraz częściej) jest on również szyfrowany. Utrata kontroli nad urządzeniami sieciowymi może być przyczyną straty danych przechowywanych na serwerach, stacjach roboczych itp. Z tego powodu dostęp do urządzeń na poziomie administracyjnym jest w szczególny sposób chroniony. Mechanizmy ochrony zawierają najczęściej ograniczenie dostępu do interfejsu zarządzającego z ograniczonej grupy hostów, dostęp ten jest możliwy tylko z jednego VLAN (Management VLAN), który jest dodatkowo chroniony listami dostępowymi działającymi na poziomie warstwy trzeciej. Jeszcze innym mechanizmem jest szyfracja całości transmisji (SSH) oraz szyfrowanie haseł, jeżeli są one przechowywane w pamięci samego urządzenia. Zalecane jest jednak zarządzanie urządzeniami sieciowymi w wykorzystaniem centralnego serwera autoryzacji, który komunikuje się z urządzeniami sieciowymi z użyciem protokołów RADIUS lub TACACS+. Taka architektura pozwala na skorzystanie z serwerów tokenowych dla uwierzytelnienia i autoryzacji administratorów z wykorzystaniem haseł jednorazowych,

  - Serwery pracujące na potrzeby organizacji zazwyczaj przechowują większość informacji krytycznych dla jej działania. Wiedząc, że część ataków sieciowych (np. Man-in-the-Middle) powiązana jest z protokołem ARP oraz mechanizmami przekierowania (Redirect), konieczne jest zabezpieczenie serwerów przed takimi działaniami. Coraz częściej w segmentach serwerowych stosuje się

zabezpieczenia pozwalające na komunikację do serwerów umieszczonych w jednej sieci VLAN przy jednoczesnym blokowaniu komunikacji pomiędzy urządzeniami w tymże VLANanie za wyjątkiem połączenia do tzw. portu uplinkowego. Pozwala to nie tylko na zabezpieczenie się przed atakami opisanymi powyżej (z dodatkową listą dostępową na urządzeniu routującym), ale również w przypadku ataku na jeden z serwerów – ochronę pozostałych (szczególnie, że w konfiguracji systemów aplikacyjnych może wystąpić błąd: nie wynikający z architektury rozwiązania, ani złej woli pracownika).

- Zagrożenia związane z jakością usług aplikacji krytycznych:

    - Jednym z największych problemów w systemach sieciowych rozwiązywanym na przestrzeni ostatnich paru lat jest kwestia zabezpieczenia ciągłości transmisji dla aplikacji krytycznych. W systemach sieci LAN pozornie nie jest to problem jednakże warto zwrócić uwagę na następujące aspekty zagadnienia:
        - Procesowanie pakietów FIFO czyli w przypadku obsługi jednej kolejki na port, pakiety pochodzące z aplikacji krytycznej mogą być blokowane przez duży wolumen ruchu innej aplikacji sieciowej,
        - Ograniczona głębokość buforów wejściowych na portach urządzeń sieciowych – w przypadku dużego wolumenu ruchu np. FTP bufory mogą być dość szybko zapełnione, co będzie skutkowało odrzucaniem kolejnych pakietów (np. aplikacji krytycznej),
        - Konieczność dynamicznej alokacji pasma dla aplikacji krytycznej – po zaniku ruchu pochodzącego z tej aplikacji pasmo powinno być „zwrócone" dla potrzeb pozostałych aplikacji (brak statycznego przypisania pasma do aplikacji),
        - Konieczność zapewnienia (lub odrzucenia) parametrów klasyfikacji pakietu proponowanego przez np. serwer sieciowy oraz możliwość zmiany priorytetu pakietu w przypadku, gdy polityka przypisania priorytetów realizowana jest na urządzeniach sieciowych.

      Obecnie większość nowych sieci przejmuje na siebie zapewnienie parametrów transmisyjnych dla aplikacji przez wykorzystanie mechanizmów strict priority dla aplikacji krytycznych, dedykowanie dla nich pamięci buforów itp.

- Zagrożenia związane z serwisowaniem sieci:

    - Jednym z wyjątkowo istotnych parametrów determinujących poprawność funkcjonowania sieci w rzeczywistości biznesowej jest konieczność zapewnienia wsparcia producenta oraz integratora dla zastosowanego rozwiązania sieciowego. Wiąże się to między innymi z możliwością serwisowania sprzętu jak i oprogramowania na nim pracującego. Wsparcie producenta oraz integratora jest związane najczęściej z czasem życia produktu poszerzonym najczęściej o okres 3-5 lat po zakończeniu produkcji urządzenia. W przypadku braku takiego wsparcia użytkownik zmuszony jest radzić sobie samodzielnie, co wymaga zazwyczaj posiadania własnego magazynu serwisowanego dla całej sieci oraz zatrudnienia dodatkowych administratorów. To rozwiązanie jest stosowane bardzo rzadko ze względu na bardzo wysokie koszty, jak również ze względu na fakt, że to producent posiada większą wiedzę o urządzeniach.

PODSUMOWANIE

Sieci budowane wg kryteriów projektowania sprzed około 6 lat mają ograniczone możliwości skalowania. W wielu przypadkach praktycznie oznacza to konieczność wprowadzenia do sieci nowych urządzeń zwiększających przepustowość pomiędzy sieciami VLAN (lub bezpośrednio pomiędzy urządzeniami sieciowymi). W przypadku mniejszych sieci zazwyczaj antidotum jest wprowadzenie wydajnych przełączników sieciowych z możliwością płynnej rozbudowy do przełączników warstwy trzeciej.

Dla uzyskania pożądanego poziomu wydajności oraz gwarancji dotyczących odpowiedniego traktowania ruchu krytycznego w dużych sieciach, konieczne jest zastosowanie przełączników sieciowych przełączających w warstwie trzeciej. Wymagać to może zmiany szeregu elementów w topologii obecnej sieci LAN. Ważnym aspektem budowy i użytkowania dużych sieci kampusowych jest zapewnienie funkcjonalności oraz wsparcia technicznego integratora i producenta dla urządzeń stanowiących o sprawności działania sieci – urządzeń rdzenia.

2.2. Rekomendacje dla sieci LAN

Struktura rdzeniowa sieci LAN powinna być budowana w celu uzyskania nowej funkcjonalności i pozbycia się (o ile istnieją w zależności od węzła) opisanych powyżej potencjalnych zagrożeń dla transferu danych. Proponowane zmiany w obrębie głównych węzłów sieciowych powinny obejmować:

- Migrację do sieci w pełni przełączanej;
- Wprowadzenie modularnych przełączników warstwy trzeciej, pozwalających na stworzenie sieci zdolnej do szybkiej rekonfiguracji na wypadek awarii, oraz ograniczenie domen rozgłoszeniowych,
- Podział grup roboczych, przypisanie użytkowników do sieci VLAN oraz konfigurację reguł wymiany informacji pomiędzy nimi,
- Wdrożenie mechanizmów zapewnienia jakości usług dla krytycznych aplikacji sieciowych oraz dla ochrony przed atakami typu Flood,
- Wprowadzenie narzędzi zarządzania siecią pozwalających na monitorowanie parametrów sieci w czasie rzeczywistym. Konfigurację sieci w celu ograniczenia dostępu do interfejsu administracyjnego urządzeń z ściśle kontrolowanej grupy hostów,
- Wprowadzenie dodatkowych mechanizmów pozwalających na skuteczne zapobieganie niepożądanym sytuacjom w segmentach krytycznych np. serwerowym,
- Usprawnienie polityki monitorowania urządzeń sieciowych celem unikania sytuacji użytkowania urządzeń niewspieranych przez producenta lub/i integratora.

Przykładowy scenariusz realizacji powyższych zadań został zamieszczony w kolejnych punktach tego opracowania.

2.3. Podział funkcjonalny sieci LAN

Wymagania użytkowników w poszczególnych węzłach sieci LAN różnią się. Wynika to chociażby z ich ilości, rozmieszczenia serwerów etc. Wymagania dotyczące podstawowej funkcjonalności są takie same we wszystkich węzłach. Wzrost wymagań zwiększa się oczywiście wraz ze wzrostem gęstości portów urządzenia, a to przekłada się na podniesienie krytyczności zasobu, jakim jest przełącznik. Przyjęto, iż wszystkie węzły sieciowe mogą zostać podzielone na dwie grupy:

- Węzeł duży (rdzeniowy) - węzeł ten agreguje ruch od użytkowników korzystających z piętrowych węzłów agregujących. Wymagane jest zastosowanie urządzenia modularnego o wysokiej gęstości portów GigaEthernet, z możliwością instalacji zapasowego zasilacza. W tej lokalizacji zalecane jest zapewnienie redundancji,
- Węzły dostępowe - węzły te agregują ruch bezpośrednio od użytkowników. Zalecane jest zastosowanie urządzenia z możliwością tworzenia stosu. Węzły dostępowe to wszystkie pozostałe węzły sieci.

2.4. Urządzenia rdzenia sieci

Urządzenia rdzeniowe poza kryterium gęstości portów, które determinuje zastosowanie określonych grup urządzeń, muszą charakteryzować się pewnymi właściwościami:

- Urządzenia centralne muszą posiadać wystarczającą wydajność, aby obsłużyć połączenia FastEthernet i Gigabit Ethernet:
    - Oczekiwana wydajność przełącznika rdzeniowego nie może być mniejsza aniżeli sumaryczna prędkość transmisji ze wszystkich węzłów dostępowych oraz wszystkich komputerów sieciowych,
    - Ze względu na fakt, że szybkość pracy uplinku urządzeń dostępowych jest niższa aniżeli sumaryczna prędkość wszystkich portów tego urządzenia przewiduje się, że łącza te mogą mieć chwilowe obciążenia do 100%,
    - W przypadku połączeń do serwerów (do Data Center), z wykorzystaniem portów Gigabit Ethernet należy założyć nadsubskrypcję ruchu w relacji 4:1 w kierunku do węzła agregującego.
- Urządzenia centralne muszą posiadać odpowiednią ilość pamięci w buforach pozwalającą na realną implementację mechanizmów Quality of Service,
- Urządzenia centralne powinny być przełącznikami warstwy 3 wraz z zaimplementowanymi funkcjami filtracji ruchu,
- Powinny w znaczący sposób zmniejszać czas konwergencji (odbudowy połączeń logicznych) w przypadku przerwy w transmisji. Może się to odbywać przez:
    - Wsparcie protokołów agregacji połączeń pomiędzy urządzeniami włączając w to warstwę dostępową LACP),
    - Wsparcie dla funkcjonalności PVST (Per VLAN Spanning Tree),

    - Wsparcie dla poza standardowych mechanizmów skrócenia procesu uczenia się sieci zgodnego ze specyfikacją STP np. PortFast, UplinkFast, BackboneFast.
- Urządzenia centralne muszą pozwalać na zapewnienie redundancji co najmniej zasilaczy oraz możliwość wprowadzenia redundancji na poziomie głównych modułów przełączających,
- Urządzenia powinny mieć możliwość korzystania z mechanizmów podniesienia poziomu redundancji „per chassis" – wsparcie protokołów HSRP lub VRRP,
- Powinny mieć możliwość konfiguracji off-line (edycja pliku konfiguracyjnego) celem skrócenia przerw w sieci w wypadku wykonywania czynności serwisowych,
- Powinny być łatwo zarządzane:
    - Jeden adres IP dostępny tylko z VLANu zarządzania dla zapewnienia niezbędnego poziomu bezpieczeństwa,
    - Możliwość autoryzacji użytkownika/administratora na kilku poziomach dostępu,
    - Możliwość analizy zarówno ruchu sieciowego jak i parametrów mechanicznych urządzenia.

2.5. Urządzenia dostępowe w sieci

Dla urządzeń węzłów dostępowych przyjęto następujące wymagania:

- Urządzenia dostępowe małych węzłów muszą posiadać wystarczającą wydajność, aby obsłużyć połączenia FastEthernet i uplinki GigaEthernet; dodatkowy uplink stosowany jest dla zwiększenia przepustowości oraz podniesienia poziomu niezawodności,
- Powinny w znaczący sposób zmniejszać czas konwergencji (odbudowy połączeń logicznych) w przypadku przerwy w transmisji. Może się to odbywać przez:
    - Wsparcie dla protokołów routingu IP (RIP, OSPF, EIGRP etc.), zapewniając tym samym najszybszy możliwy czas konwergencji w przypadku awarii przy jednoczesnej możliwości wykorzystania wielu tras w czasie normalnej pracy sieci,
    - Wsparcie protokołów agregacji połączeń pomiędzy urządzeniami włączając w to warstwę dostępową,
    - Wsparcie dla funkcjonalności PVST (Per VLAN Spenning Tree),
    - Wsparcie dla poza standardowych mechanizmów skrócenia procesu uczenia się sieci zgodnego ze specyfikacją STP.
- Powinny być zarządzane.

2.6. Uwagi eksploatacyjne i inwestycyjne

Ponadto przy doborze urządzeń kierowano się następującymi wskazówkami techniczno-inwestycyjnymi:

- Unifikacja urządzeń:

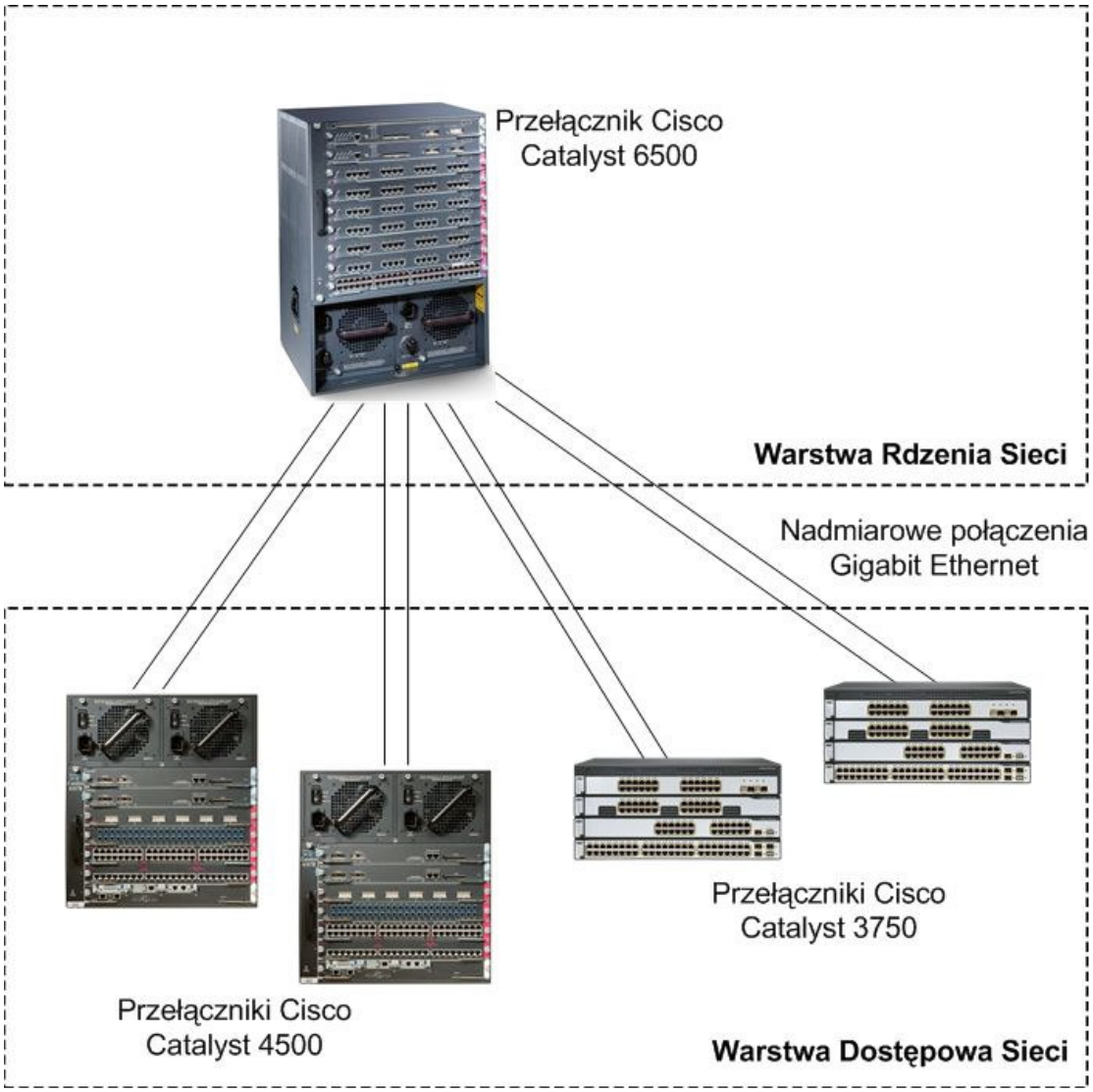
    - Stosowanie jednej rodziny produktów w węzłach centralnych sieci,
    - Stosowanie jednej rodziny produktów w węzłach dostępowych sieci.

- Skalowanie urządzeń:
    - Po określeniu maksymalnego obciążenia urządzeń przy uwzględnieniu przyłączania wszystkich obecnie użytkowanych stacji roboczych i drukarek, należy przewidzieć pewną ilość portów nadmiarowych na bieżącą rozbudowę,
    - Stosowanie urządzeń umożliwiających skalowanie o 7-10% rocznie,
    - W urządzeniach rdzeniowych powinny być wolne sloty na rozbudowę natomiast urządzenia dostępowe powinny mieć możliwość budowy stosów,
    - Zaleca się, aby urządzenia zapewniały zasilanie in-line 802.3af dla telefonii IP na wszystkich portach przeznaczonych dla użytkowników. Dopuszcza się, aby porty przeznaczone dla serwerów sieciowych, w tym aplikacyjnych i bazodanowych nie wspierały zasilania in-line. Zalecenie to jest opcjonalne – ma na celu zabezpieczenie inwestycji w przypadku migracji do telefonii IP.

Kierowanie się powyższymi zaleceniami pozwala na uzyskanie znaczących oszczędności w eksploatacji sieci (niższe koszty serwisowania, rekonfiguracji etc.). Należy zaznaczyć, że koszty eksploatacji (koszt sprzętu to około 25-30% ogólnego kosztu sieci przez okres 3 lat (w ogólny koszt sieci wliczone są koszt nabycia sieci, koszty związane z serwisowaniem, administracją oraz koszty łącz operatorskich).

3. PRZYKŁADOWY PROJEKT SIECI LAN O WIELKOŚCI 300+ UŻYTKOWNIKÓW

Zgodnie z powyższymi założeniami przyjęto, że rodzina produktów spełniające powyższe wymagania to Cisco Catalyst 6500 jako urządzenia rdzeniowe oraz Cisco Catalyst 4500 jako urządzenia dostępowe (lub w przypadku mniejszych aplikacji Cisco Catalyst 3750). Urządzenia są przewidywane w różnych wariantach wyposażenia.



Przedstawiona koncepcja projektu zakłada wielkość sieci od 300 portów ethernet w górę. W projekcie wyraźnie wyszczególniony został rdzeń sieci oparty o przełącznik sieciowy z rodziny Cisco Catalyst 6500. Urządzenie to spełnia wszystkie założenia koncepcyjne wymienione wcześniej w powyższym opracowaniu. Przełączniki z rodziny Cisco Catalyst 6500 to urządzenie modularne oferujące pełną nadmiarowość, jeżeli chodzi o moduły zarządzające (funkcja natychmiastowego przełączenia – statefull failover) oraz

nadmiarowe zasilacze. Jest to wysoce skalowalny przełącznik warstwy trzeciej – do 720 Gbps przepustowości, maksymalnie do 576 portów ethernet 10/100/1000 lub do 1152 portów ethernet 10/100. Oferowane modele posiadają chassis od 3 do 13 slotów.

W przypadku powyższej sieci został on wykorzystany jako punkt agregujący ruch przychodzący od przełączników dostępowych, do których wpięci zostaną użytkownicy końcowi. Do połączenia pomiędzy przełącznikiem agregującym a przełącznikami dostępowymi wykorzystujemy podwójne łącza Gigabit Ethernet w postaci światłowodu lub skrętki miedzianej. Zastosowane medium zależy od odległości pomiędzy przełącznikami. Podwójny charakter uplinku gwarantuje nadmiarowość łącza w przypadku awarii. System przełączania lub agregacji obydwu z uplinków będzie zależał od zastosowanych mechanizmów Layer 2 (Spanning Tree, EtherChannel) lub Layer 3 (protokoły routing OSPF, EIGRP, RIP lub inne).

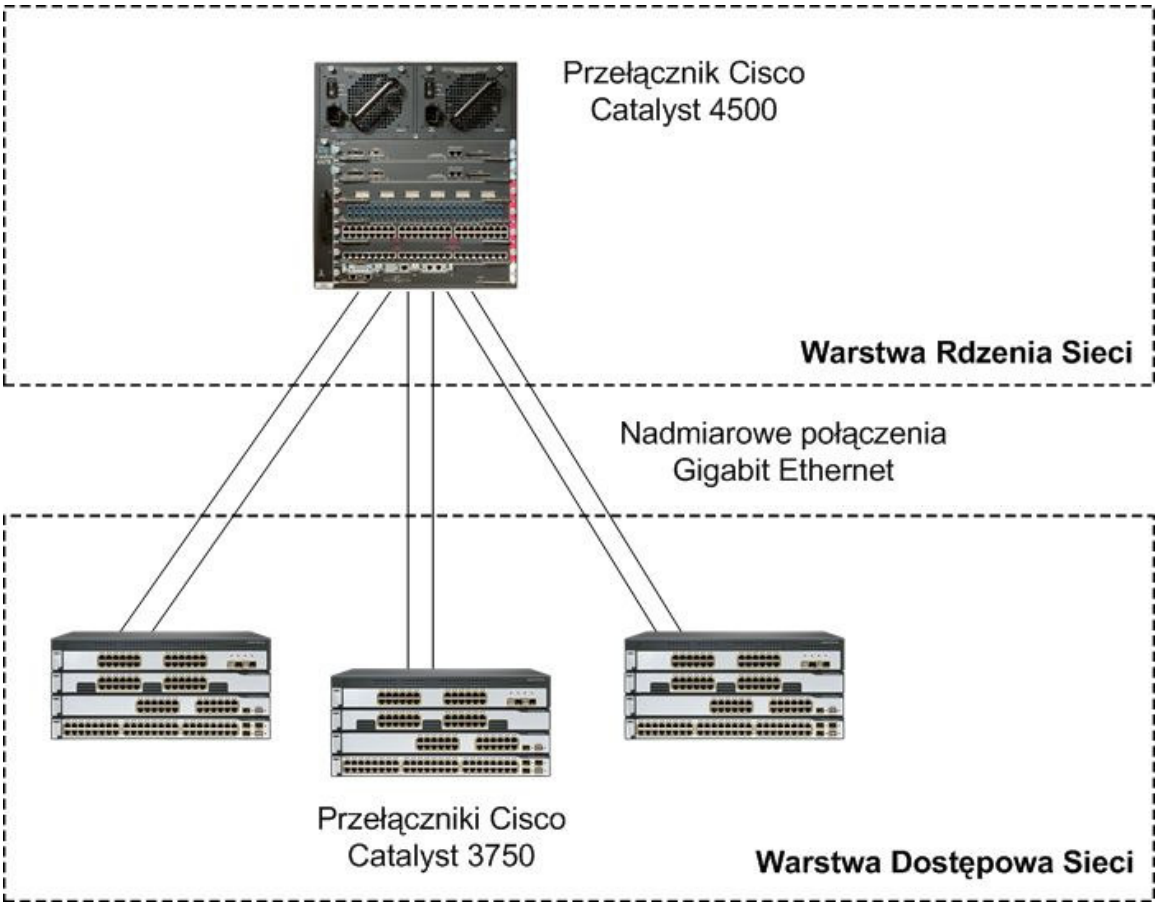
Przełączniki warstwy dostępowej zastosowane przy tej wielkości sieci to Cisco Catalyst 4500 lub w przypadku mniejszych węzłów Catalyst 3750. Przełączniki 4500 charakteryzują się modularną budową oraz nadmiarowością modułów zarządzających jak i samych zasilaczy. Oferowane chassis występują w wielkościach od 3 do 10 slotów i potrafią pomieścić karty interfejsu do 384 portów ethernet 10/100/1000 z przepustowością 96 Gbps. Są to oczywiście przełączniki warstwy trzeciej potrafiące lokalnie terminować podsieci IP należące do danego VLANu, z jednoczesną możliwością wstępnej filtracji lub ograniczania pasma ruchu użytkowników końcowych. Dla węzłów dostępowych niewymagających tak dużej ilości portów ethernet dla użytkowników końcowych, wybór padł na Cisco Catalyst 3750. Są to nie modularne przełączniki warstwy trzeciej oferujące od 24 do 48 portów ethernet 10/100. Przełączniki Catalyst 3750 oferują możliwość stakowania (połączenia wieżowego) do 9 urządzeń przy użyciu zewnętrznej magistrali o przepustowości 32 Gbps. W przeciwieństwie do urządzeń łączonych wieżowo z użyciem portów Gigabit, Catalyst 3750 pozwala na dużo szybsze przesyłanie pakietów pomiędzy przełącznikami, wspólny punkt zarządzania i konfiguracji dla wieży urządzeń, dedykowany port tylko do połączeń pomiędzy urządzeniami.

Funkcje obejmujące filtracje ruchu użytkowników powinny być zaimplementowane w centralnym punkcie sieci tj. przełączniku agregującym Catalyst 6500. Funkcje związane z ograniczaniem ruchu użytkowników powinny być zlokalizowane na przełącznikach warstwy dostępowej.

Wszystkie z wymienionych przełączników oferują karty Ethernet obsługujące standard 802.3af Power over Ethernet co w przyszłości pozwoli na bezproblemową migrację obecnego systemu telefonicznego do Telefonii IP lub też zasilanie z portów ethernetowych innych urządzeń typu bezprzewodowy koncentrator sieciowy – Access Point.

4. PRZYKŁADOWY PROJEKT SIECI LAN O WIELKOŚCI 150 UŻYTKOWNIKÓW

Zgodnie z założeniami przyjęto, iż do budowy sieci LAN o zakładanych rozmiarach należy wykorzystać Cisco Catalyst 4500 w rdzeniu sieci oraz przełączniki rodziny Cisco Catalyst 3750 jako urządzenia dostępowe, do których podłączone zostaną komputery użytkowników, drukarki sieciowe jak i serwery. Należy wykorzystać różne warianty przełączników w zależności od indywidualnych cech projektowanej sieci.



Podobnie jak i w poprzednim przypadku (sieci o rozmiarach 300+ użytkowników) wykorzystany został tzw. model budowy sieci - colapsed backbone. Model ten zakłada odstępstwo od powszechnie znanego schematu podziału sieci LAN na warstwy rdzenia, dystrybucji i dostępu. W modelu colapsed backbone funkcje, jak i urządzenia rdzenia i dystrybucji zostały połączone w jednym urządzeniu.

Proponowany projekt zakłada zastosowanie przełącznika warstwy trzeciej - Cisco Catalyst 4500, jako przełącznika rdzeniowego agregującego połączenia od warstwy dystrybucyjnej zbudowanej z wykorzystaniem przełączników Catalyst 3750 połączonych wieżowo. Rozwiązanie takie zapewnia redundancje rdzenia z wykorzystaniem modelu 4507R lub 4510R, które to modele pozwalają na zastosowanie podwójnych modułów zarządzających oraz podwójnych zasilaczy. Warstwa dostępowa zrealizowana z wykorzystaniem przełączników stakowalnych - Catalyst 3750 pozwala na dynamiczny

wzrost wielkości węzłów dostępowych bez ograniczenia dostępnego pasma. Dzieje się tak dzięki zastosowanej w przełącznikach Catalyst 3750 dedykowanej magistrali stakującej o przepustowości 32 Gbps.

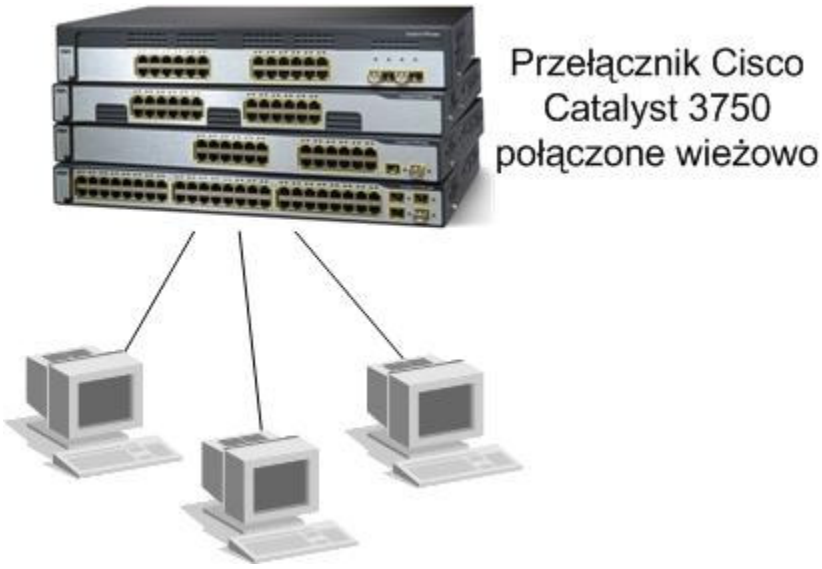
Połączenie przełączników dostępowych z przełącznikiem agregującym w rdzeniu sieci zrealizowane zostało przy pomocy redundantnych uplinków Gigabit Ethernetowych. Połączenia te mogą być wykonane w technice światłowodowej, jaki i skrętki miedzianej. Sposób przełączania w przypadku awarii lub agregacji pasma uplinków zależy od zastosowanej techniki realizacji połączenia (Spanning Tree, EtherChannel lub dynamiczne protokoły routingu).

Projekt ten różni się od poprzedniego nadmiarowością oraz wydajnością zastosowanych urządzeń. Jednak zarówno w tym jak i poprzednim przypadku umożliwia dynamiczny rozwój sieci, a w końcowym stadium migrację do projektu sieci o wielkości 300+ użytkowników.

Ponadto, podobnie jak w poprzednim przypadku zastosowane przełączniki pozwalają na zasilanie urządzeń z wykorzystaniem techniki Power over Ethernet.

5. PRZYKŁADOWY PROJEKT SIECI LAN O WIELKOŚCI 50 UŻYTKOWNIKÓW

Do najmniejszego z opisywanych projektów proponujemy wykorzystać przełączniki Cisco Catalyst 3750 połączone wieżowo. Urządzenia te spełniają wszystkie cechy wymagane w obecnie projektowanych sieciach LAN, wymienione również w niniejszym opracowaniu. Ponadto ich architektura pozwala na łatwe powiększenie ilości portów ethernet w danej lokalizacji bez utraty skalowalności rozwiązania.



Widok (z tyłu) przedstawiający system połączenia kilku przełączników Cisco Catalyst 3750 w jedną logiczną całość.

Przełączniki Cisco Catalyst 3750 pozwalają na szybką rozbudowę sieci lokalnej poprzez łączenie ich zewnętrzną magistralą stakującą. Zbudowana w ten sposób wieża urządzeń pozwala na obsłużenie do 432 portów ethernet 10/100 (do 9 przełączników 48 portowych połączonych ze sobą).

Są to przełączniki warstwy trzeciej. Pozwala to na zastosowanie technik filtracji pakietów, ograniczania pasma oraz dostępu a także zastosowanie sposobów obrony przed zagrożeniami wymienianymi w niniejszym opracowaniu.

6. SPECYFIKACJE PROPONOWANYCH URZĄDZEŃ

6.1 Rodzina Przełączników Catalyst 6500

Cechy Charakterystyczne:

Wielkość Chassis

3, 6, 9, 9 w układzie wertykalnym (NEBS), lub13 slotów

Przepustowość Backplane

W zależności od zastosowanych modułów: 32 Gbps shared bus, 256 Gbps lub 720 Gbps switching fabric

Wydajność przełączania w warstwie trzeciej

W zależności od zastosowanych modułów: Supervisor 1 MSFC – 15 Mpps, Supervisor 2 MSFC – 210 Mpps, Supervisor 720 – 400 Mpps

Elementy Nadmiarowe

Moduły zarządzające – w trybie natychmiastowego, bezstratnego przełączania (stateful failover)
Zasilacze - w trybie 1+1
Zespół przełączający (Switching Fabric) - w trybie 1+1
Wymienne moduly chłodzące (Fan Tray) oraz Zegara Taktującego Backplane

Tryby przełączania i agregacji połączeń nadmiarowych

Gateway Load Balancing Protocol , Hot Standby Router Protocol , Multimodule EtherChannel , Rapid Spanning Tree, Multiple Spanning Tree, Per VLAN Rapid Spanning Tree oraz Protokoły Routingu L3

Maksymalne Ilości portów LAN

10/100/1000 Ethernet
576 portów, wszystkie ze wsparciem Inline Power
10/100 Fast Ethernet
1152 portów, wszystkie ze wsparciem Inline Power
100-Base-FX
288 portów

Gigabit Ethernet (GBIC)
194 porty (w tym 2 porty na module zarządzającym)
10 Gigabit Ethernet (XENPAK)
32 porty

Maksymalne Ilości portów WAN

OC-3 POS - 192 porty
OC-12 POS - 48 portów
OC-12 ATM - 24 porty
OC-48 POS/DPT - 24 porty

Maksymalne Ilości portów PSTN (telefonicznych)

Cyfrowe Trunki T1/E1 - 216 portów
Analogowe Interfejsy FXS - 864 portów

Zaawansowane Moduły Serwisowe

Gigabit Firewall
Gigabit VPN
High Performance Intrusion Detection
Gigabit Content Switching Module
High Performance SSL Termination
Wireless LAN Services Module
Gigabit Content Services Gateway

6.2 Rodzina Przełączników Catalyst 4500

<u>Cechy Charakterystyczne:</u>

Wielkość Chassis

3, 6, 7 lub 10 slotów

Przepustowość Backplane

W zależności od Chassis: 4503 – 28 Gbps, 4506 i 4507R – 64 Gbps, 4510R – 96 Gbps

Wydajność przełączania w warstwie trzeciej

W zależności od zastosowanych modułów:

Feature	Supervisor Engine II-Plus (WS-X4013+)	Supervisor Engine IV (WS-X4515)	Supervisor Engine V (WS-X4516)
Cisco Catalyst 4503 Chassis	Supported 28 Gbps, 21 Mpps	Supported 28 Gbps, 21 Mpps	Supported 28 Gbps, 21 Mpps
Cisco Catalyst 4506 Chassis	Supported 64 Gbps, 48 Mpps	Supported 64 Gbps, 48 Mpps	Supported 64 Gbps, 48 Mpps
Cisco Catalyst 4507R Chassis	Supported 64 Gbps, 48 Mpps	Supported 64 Gbps, 48 Mpps	Supported 68 Gbps, 51Mpps
Cisco Catalyst 4510R Chassis	Not supported	Not supported	Supported 96 Gbps 72 Mpps

Elementy Nadmiarowe

- Moduły zarządzające – tylko w Chassis 4507R (Supervisor Engine II-Plus, IV, V) oraz Chassis 4510R (tylko Supervisor Engine V)
- Zasilacze - w trybie 1+1
- Wymienne moduły chłodzące (Fan Tray) oraz Zegara Taktującego Backplane oraz Pasywny Zespół Przełączający (Fabric Redundancy Module)

Tryby przełączania i agregacji połączeń nadmiarowych

Hot Standby Router Protocol, EtherChannel , Rapid Spanning Tree, Multiple Spanning Tree, Per VLAN Rapid Spanning Tree oraz Protokoły Routingu L3

Maksymalne Ilości portów LAN

10/100/1000 Ethernet

336 portów, wszystkie ze wsparciem Inline Power

10/100 Fast Ethernet

336 portów, wszystkie ze wsparciem Inline Power

100-Base-FX

336 portów

Gigabit Ethernet (GBIC)

130 porty (w tym 4 porty na modułach zarządzających)

Maksymalne Ilości portów WAN

20 porty serial (synchroniczny lub asynchroniczny)

30 portów PRI/E1

30 portów BRI

Maksymalne Ilości portów PSTN (telefonicznych)

Cyfrowe Trunki T1/E1 - 30 portów

Analogowe Interfejsy FXS - 110 portów

6.3 Rodzina Przełączników Catalyst 3750

Cechy Charakterystyczne:

Wielkość Wieży

Do 9 urządzeń

Przepustowość Backplane

Zewnętrzna Magistrala o przepustowości 32 Gbps

Wydajność przełączania w warstwie trzeciej

Wydajność dla urządzeń połączonych wieżowo – 38,7 Mpps

Elementy Nadmiarowe

Przełącznik zarządzający stosem urządzeń (1+N)
Zewnętrzny zasilacz nadmiarowy

Tryby przełączania i agregacji połączeń nadmiarowych

Hot Standby Router Protocol, Per Chassis EtherChannel , Rapid Spanning Tree, Multiple Spanning Tree, Per VLAN Rapid Spanning Tree oraz Protokoły Routingu L3

Maksymalne Ilości portów LAN

Dla stosu 9 urządzeń
10/100/1000 Ethernet
252 portów
10/100 Fast Ethernet
432 portów, wszystkie ze wsparciem Inline Power
10Gigabit Ethernet XENPAK
9 portów

7. PODSUMOWANIE

Budowa lokalnej sieci komputerowej może okazać się zadaniem trywialnie prostym albo też bardzo skomplikowanym. Jeżeli budowa sieci zostanie sprowadzona do najniższego z możliwych poziomów – zapewnienia jakiejkolwiek komunikacji pomiędzy użytkownikami – to z pewnością można nie przejmować się opisanymi zaleceniami. Z drugiej strony budując sieć „idealną" można bardzo łatwo wpaść pułapkę nadmiernych komplikacji. W poszukiwaniu rozwiązań najbardziej wyważonych należy pamiętać, aby nie rezygnować z funkcjonalności ważnych z perspektywy bezpieczeństwa, zapewnienia jakości transmisji czy otwartości na przyszłe systemy np. telefonię IP. Niezmiernie ważne jest też zachowanie otwartości na aplikacje i rozwiązania, które mogą być implementowane w niedalekiej przyszłości; brak takiego spojrzenia może powodować, że funkcjonalność zaprojektowanej sieci jest wystarczająca w krótkim czasie, ale nie sprosta wymaganiom w perspektywie np. 2 lat.

Ponieważ sieć LAN stanowi podstawę dla funkcjonowania wszystkich aplikacji sieciowych łatwo poddać ją krytyce. W wielu przypadkach brak odpowiedniej infrastruktury połączeniowej może być przyczynkiem do usprawiedliwiania niedziałającej aplikacji czy systemu.

Sprawna sieć komputerowa pozwala także na odpowiedni monitoring zdarzeń, izolowanie problemów, a także określanie słabych punktów w sieci.

Podsumowując zagadnienia budowy wydajnych sieci komputerowych, warto przytoczyć częste porównanie do infrastruktury drogowej. Drogi zawsze determinują powstanie nowych miast, osiedli, fabryk, sklepów etc. Warto pamiętać, że sieć będąca infrastrukturą transmisyjną może stanowić o sukcesie wdrożenia aplikacji, a nie odwrotnie. Silna infrastruktura jest fundamentem budowy innych systemów w JST.