Projekt „NEW-TECH Program rozwoju praktycznych kompetencji nauczycieli zawodów branż nowych technologii” jest współfinansowany przez Unię Europejską w ramach środków Europejskiego Funduszu Społecznego

Warsztaty NEW-TECH , branża telekomunikacyjna

„Warsztaty CISCO”

MATERIAŁY SZKOLENIOWE

Człowiek – najlepsza inwestycja

www.kapitalludzki.gov.pl

Podręcznik jest współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Podręcznik jest dystrybuowany bezpłatnie.

www.newtech.eduportal.pl

Gdynia 2013

Projekt realizowany przez COMBIDATA Poland sp. z o.o. w ramach umowy o dofinansowanie projektu w ramach Programu Operacyjnego Kapitał Ludzki 2007-2013, Priorytetu III „Wysoka jakość systemu oświaty”, Działanie 3.4 „Otwartość systemu edukacji w kontekście uczenia się przez całe życia” , Poddziałanie: 3.4.3 „Upowszechnienie uczenia się przez całe życie - projekty konkursowe”.

Spis treści

1. Podstawy sieci

Czym jest sieć? Jest to zbiór urządzeń występujących na określonym obszarze, połączonych ze sobą za pomocą różnych typów medium. W zależność od rodzaju użytego medium komunikacja ta może być realizowana na różnych dystansach. W sieci pracuje wiele urządzeń, które będą pośredniczyć w procesie tworzenie oraz dostarczania danych do odcelowego odbiorcy. Do grona takich urządzeń możemy zaliczyć: komputery, serwery, stacje terminalowe, drukarki, telefony IP, switch-e, routery.

Nadrzędna rolą sieci jest, zapewnienie możliwości przesyłania i dostępu do danych pomiędzy urządzeniami. Rozmiar sieci będzie uwarunkowany od skali firmy i jej potrzeb. Rozważmy kwestię rozmiarów sieci w oparciu o poniższe aspekty.

Centrala firmy może posiadać setki urządzeń kocowych (PC) oraz dziesiątki urządzeń aktywnych (switch-e), co ewidentnie będzie wskazywało na duży rozmiar sieci. W przypadku oddziału firmy mamy do czynienia z kilkoma pracownikami podłączonych do jednego przełącznika, poprzez router dostęp jest realizowany do Internetu (a w tym do centrali firmy). Rozmiar takiej sieci jest nie duży i stanowi namiastkę infrastruktury w centrali firmy.

W sieciach domowych mamy do czynienia z dwoma może trzema urządzeniami, które będą się ze sobą komunikowały i za pośrednictwem routera maja zapewniony dostęp do Internetu. Rozmiar takiej sieci określimy jako mały. Najmniejszą sieci, jaką możemy utworzyć to połączenie dwóch komputerów ze sobą.

Sieci zapewniają nam dostęp przede wszystkim do danych oraz aplikacji, ale pozwalają nam korzystać z innych zasobów sieciowych takich jak: drukarki, skanery, kamery IP. Dodatkowo sieci umożliwiają wykorzystania zdalnego dostępu do przestrzeni dyskowej, które oferują nam rozwiania takie jak: NAS, SUN. Kolejną wymierną korzyścią wykorzystywania sieci jest możliwość realizowania zdalnych backup-ów.

Sieci możemy scharakteryzować za pomocą kilku istotnych cech, takich jak:
Prędkość – jak szybko dane będą się przemieszczały z punktu A do punktu B w infrastrukturze.
Koszt – realny koszt utworzenia infrastruktury oraz koszty miesięczne utrzymania sieci.
Bezpieczeństwo – zapewnienie bezpieczeństwa dla danych w obrębie firmy.

Dostępność – sieć, która utrzymuje ciągłą i nieprzerwaną pracę 7/24/365

Skalowalność – odpowiednia ilość slotów, portów - zapewnia możliwość podłączania do infrastruktury kolejnych urządzeń.

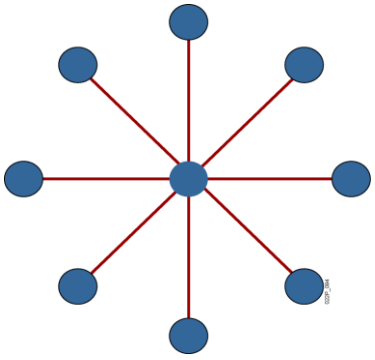
Niezawodność – odpowiedniej klasy i jakości sprzęt zapewniający małą awaryjność.

Topologia - sposób, w jaki urządzenia będą połączone ze sobą i jak realizowany będzie przesył danych.

2. Topologie sieci

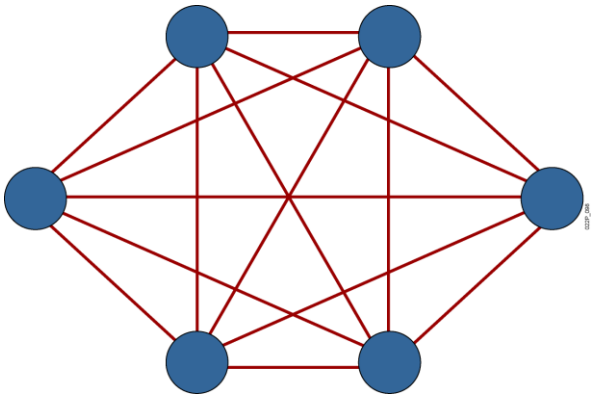
Kiedy mówimy o sieci przed oczyma mamy urządzenia oraz okablowanie strukturalne, jednak aby zrozumieć jak to wszystko funkcjonuje należy zwrócić uwagę na dwa pojęcia: topologia fizyczna i topologia logiczna.

Topologia fizyczna – opisuje, w jaki sposób dokonano fizycznego połączenia urządzeń ze sobą w serwerowni lub w szafach na piętrach w budynku. W dzisiejszych czasach wykorzystujemy klika sposobów tworzenia fizycznej topologii, najczęściej używanym jest model gwiazdy.



Cechą charakterystyczna dla tego modelu jest centralny punkt agregujący połączenia od innych urządzeń i to przez niego jest realizowany tranzyt danych. Jednak słabym punktem tego rozwiązania jest centralny punkt, w wyniku awarii tego elementu nie ma możliwość komunikowania się pomiędzy urządzeniami.

Kolejna topologia używana w sieciach to Full-Mesh, która zapewnia połączenia „każdy z każdym”, przez co zapewniamy pełną komunikację pomiędzy urządzeniami.



Ten rodzaj topologii na pewno powinien zostać zaimplementowany w sieciach opartych o technologie Wireless. Dzięki czemu użytkownik może być przepinamy pomiędzy Acccess-Pointami w momencie, kiedy siła sygnału słabnie, bez rozłączanie go z siecią.

Należy wspomnieć o dwóch topologiach: szyny oraz koła. Nie są one już dzisiaj używane w sieciach ze względu na ich charakterystykę działania.

Topologia logiczna – opisuje, w jaki sposób dane będą się przemieszczały z punktu A do punktu B w obrębie naszej infrastruktury. Logiczną topologię możemy zaplanować w oparciu o wydajność urządzeń i potrzeby administratora.

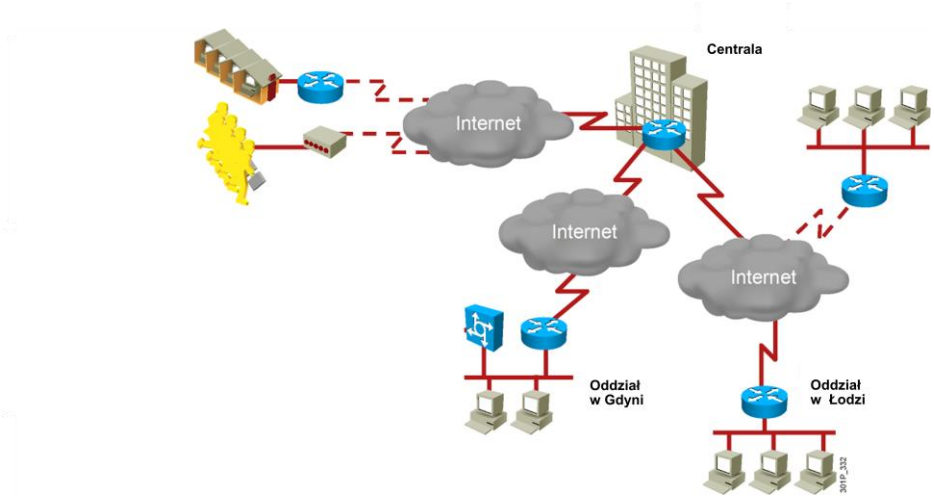
3. Zagrożenia w sieci

Zarządzanie infrastrukturą wymaga od administratora nie tylko posiadania odpowiedniego sprzętu, ale przede wszystkim umiejętności i wiedzy dotyczącej działania sieci oraz potencjalnych zagrożeni, z którymi może się spotkać.

Pojawia się tutaj pytanie, jakie to są bezpieczne sieci? Z punktu widzenia bezpieczeństwa mogą to być sieci, które zostaną odłączone od dostępu do Internetu. Jednak takie podejście w dzisiejszych czasach jest niedopuszczalne. Wynika to z faktu, iż dzisiaj biznes szeroko pojęty realizowany jest za pośrednictwem Internetu. Kolejnym argumentem, który będzie skutecznie obalał teorię pozbawienia firmy dostępu do Internetu jest fakt, iż przeszło 70% ataków na

infrastrukturę jest realizowanych do środka przez użytkowników.

Bezpieczne sieci to takie, które są otwarte i zarządzane przez uświadomionych administratorów. Zapewniają Oni dostęp do firmowej infrastruktury partnerom biznesowym jednocześnie udostępniając im fragment sieci, a z drugiej strony nie pozwolą, aby z tych wydzielonych miejsc osoby trzecie mogły mieć prawo dostępu do istotnych zasobów firmy.



W dzisiejszych czasach przeprowadzenie ataku na siec nie wymaga wysokiego poziomu wiedzy czy umiejętność. Dostępne gotowe aplikacje lub dystrybucje Linux-a pozwalają przeprowadzić atak. Aby skutecznie bronić się przed atakami musimy poznać metody ataków, grupy społeczne, które takie ataki wykonują oraz przesłanki nimi kierujące.

Atakujący – do tej grupy możemy zaliczyć: hakerów, crakerów, ludzi piszących skrypty, cyber przestępców, pracowników, uczniów.

Motywacja / powody – chęć sprawdzenia się, wyzwanie, uprzykrzenie drugiej osobie życia, kradzież informacji.

Rodzaje ataków – złożoność przeprowadzanych ataków zależy od stopnia determinacji atakującego.

Ataki możemy podzielić na klika grup:

Pasywne - to takie, kiedy atakujący zbiera ruch za pomocą aplikacji z całej infrastruktury, a zabrany materiał analizuje celem poznania haseł do określonych miejsc.

Aktywne – te ataki są wykonywane między innymi poprzez podsyłanie odnośników do odpowiednio spreparowanych stron, które wyglądem mogą przypominać strony banków, portali społecznościowych. Wszystko po to, aby osoba podała login i hasło, które będzie przechwycone przez osobę, która podesłała nam odnośnik do strony.

Bezpośrednie – ataki przeprowadzane przez osoby, które mają bezpośredni dostęp do naszej infrastruktury i mogą się do niej podłączyć. Otrzymując odpowiednie informacje jak adres IP, maska sieci są w stanie przeprowadzać wstępny rekonesans infrastruktury.

Wewnętrzne – ten rodzaj ataku posiada ma dwa oblicza. Pierwsze, kiedy administrator żyje w przekonaniu, że wszystko zostało zabezpieczone poprawnie, ale mimo to osoby niepowołane i tak maja dostęp do zasobów. Drugie - administrator może otrzymać zwrotnie informacje od pracownika, że posiada dostęp do niepowołanych zasobów, co może wyczulić administratorów na potencjalne luki w zabezpieczeniach.

Dystrybucyjne – te ataki wymierzone są w różne platformy sprzętowe oraz pracujący na nich software. Należy zadbać o to, aby dysponować najnowszymi wersjami systemów operacyjnych, co pozwoli wykluczać tego typu ataki.

Kolejnym istotnym zagadnieniem, który ma wpływ na bezpieczeństwo sieci to odpowiednie przygotowanie naszej infrastruktury. W tym miejscu należy zacząć od fizycznego zabezpieczania dostępu do sprzętu aktywnego. W tym celu musimy posiadać wydzielone pomieszczenie, w którym będzie ten sprzęt przechowywany. Serwerownia powinna być wyposażona w: podłogę techniczną, drzwi ognioodporne, system gaśniczy z wykorzystaniem mieszanek gazów. Dostęp do serwerowni powinien być ograniczony dla grupy administratorów, z wykorzystaniem czytników linii papilarnych, kart dostępowych. Kolejnym istotnym elementem zapewnienia poprawnego funkcjonowania urządzeń jest zapewnienie im odpowiedniego środowiska tj. temperatury oraz wilgotność. Należy pamiętać również o okresowych konserwacjach tego sprzętu. Zapewnienie odpowiedniego zasilania ma kluczowe znaczenie dla działania urządzeń i zalecane jest w tym miejscu wyposażenie serwerowni w dwa niezależne źródła zasilania wysokiego napięcia, dodatkowo zakup UPS-ów ewentualnie agregatu prądotwórczego. Jedną z największych bolączek administratorów jest brak odpowiedniej dokumentacji infrastruktury. Dobrze przygotowana dokumentacja i plany pozwolą w przejrzysty i klarowny sposób lokalizować miejsca usterki i ich przyczyny.

4. Warstwy sieci

Nieodłącznym elementem sieci są warstwy. Stworzenie modelu warstw wymusił fakt braku jednoznacznych standardów, brak możliwości łączenia różnych technologii, bardzo duża złożoność w zarządzaniu infrastrukturą. Takie podejście pozwoliło ustalić ramy, określające, co jest realizowane w obrębie danej warstwy oraz kto (urządzenie, protokół) w danym momencie odpowiada za określone czynności. W sieciach występuje 7 warstw modelu OSI i każda z nich zostanie przedstawiona poniżej.

Warstwa Fizyczna – jest to warstwa, w której zachodzą odpowiednie procesy fizyczne i mechaniczne, określające, w jaki sposób i na jakim dystansie będą przesyłane informacje w fizycznym linku. W tej warstwie mówimy o fizycznym medium takim jak Ethernet, światłowód, sygnał radiowy.

Warstwa Łącza danych – warstwa ta ustala, w jaki sposób dane będą sformatowane przed wysłaniem przez fizyczne medium. Jednocześnie ustala, z jakim protokołem warstwy Sieciowej ma kontakt. Dodatkowo dostarcza funkcji wykrywania błędów poprzez wyliczanie sum kontrolnych ramek FCS. **W tej warstwie pracują switch-e, które dokonują przełączania (przesyłania) ramek w oparciu o mac-adresy** .

Warstwa Sieci – warstwa odpowiedzialna za wyszukiwanie najbardziej optymalnych tras do docelowych sieci. Jednocześnie dostarcza logicznych adresów IP, którymi będą posługiwały się urządzenia w sieci. **W tej warstwie pracują routery**.

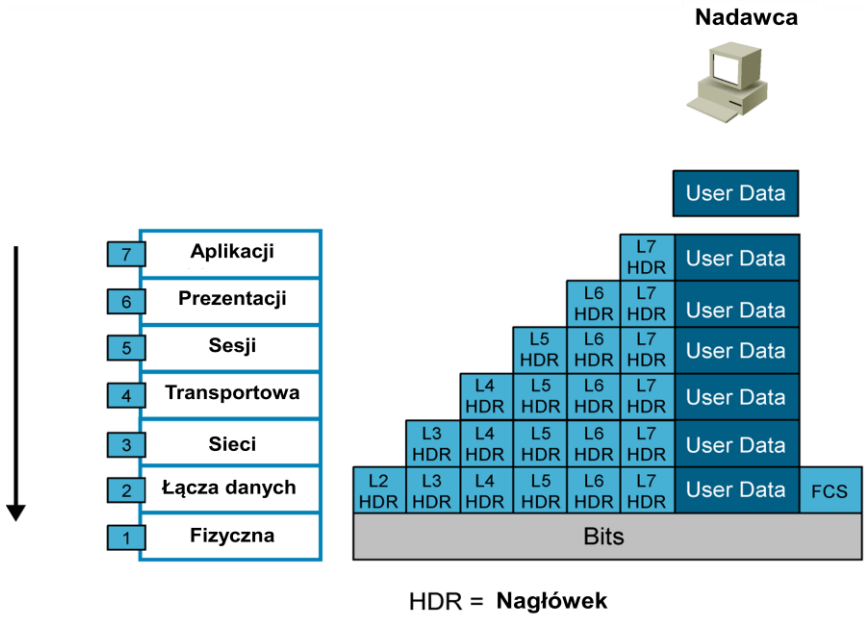
Warstwa Transportowa – jest to warstwa, która ustanawia wirtualne obwody pomiędzy hostami zanim nastąpi proces przesyłania danych. Dodatkowo wyposażona w funkcje niezawodnego dostarczania danych, funkcje odzyskiwania utraconych danych oraz w funkcje przeciwdziałająca przeciążeniu odbiorcy (**flow control**).

Warstwa Sesji – to warstwa ustanawia i utrzymuje sesje pomiędzy aplikacjami komunikującymi się ze sobą np. za utrzymanie połączeń serwera WWW z wieloma hostami będzie odpowiedzialna warstwa sesji, która kontroluje, kto nawiązał określone połączenie i czy połączenie jest nadal wymagane.

Warstwa Prezentacji – jest to warstwa, odpowiedzialna za odpowiednie sformatowanie danych tak, aby były one czytelne dla odbiorcy. Mówimy tutaj o odpowiednim kodowaniu, strukturze danych. Na poziomie tej warstwy wykonywany jest proces szyfrowania.

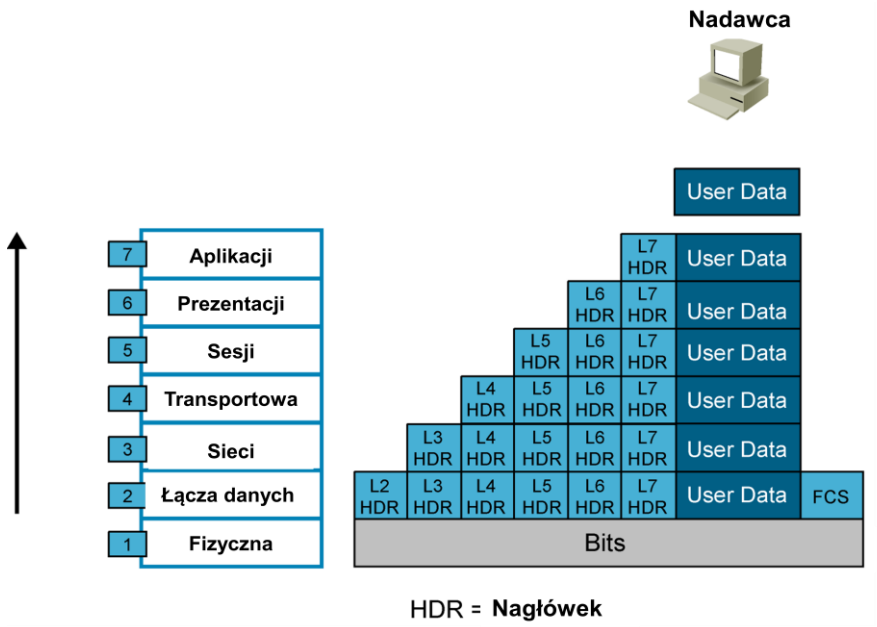
Warstwa Aplikacji – to warstwa, która pośredniczy w procesie komunikowania się z aplikacjami pracującymi na stacji, a jednocześnie dostarcza usług sieciowych dla tych aplikacji tj. poczta, ftp, itp. występujących w modelu OSI. Na poziomie tej warstwy wykonywana jest również autentykacja użytkownika.

W czasie komunikacji pomiędzy dwoma hostami dane są przesyłane poprzez wszystkie warstwy modelu OSI. Na poziomie każdej warstwy następuje utworzenie nagłówków. W nagłówku przenosi się informacja, jakie usługi świadczy dana warstwa dla wyższych warstw. Proces ten nazywany jest enkapsulacja danych.



HDR = **Nagłówek**

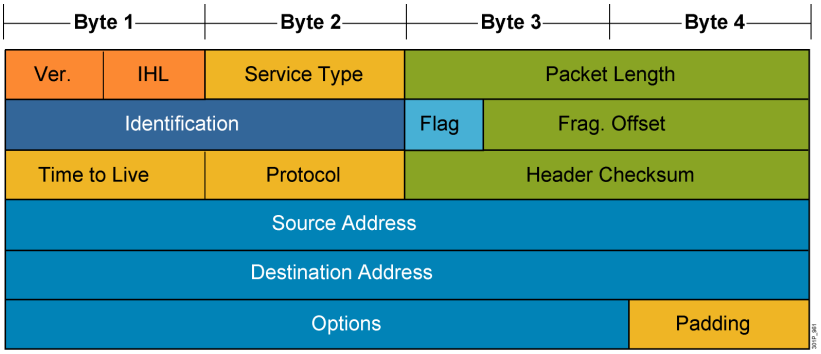
Kiedy dane zostaną zamienione w bity i poprzez fizyczny medium dotrą do odbiorcy, następuje proces odwrotny do procesu enkapsulacji nazywany de-enkapsulacją.



Cechą charakterystyką procesu de-enkapsulacji jest zrywanie nagłówków na poziomie każdej warstwy a następnie przesyłanie informacji dalej. Zawartość każdego nagłówka informuje, co należy zrobić dalej tj., do jakiego protokołu wyższej warstwy przesłać dane, tak, aby dotarły w określone miejsce.

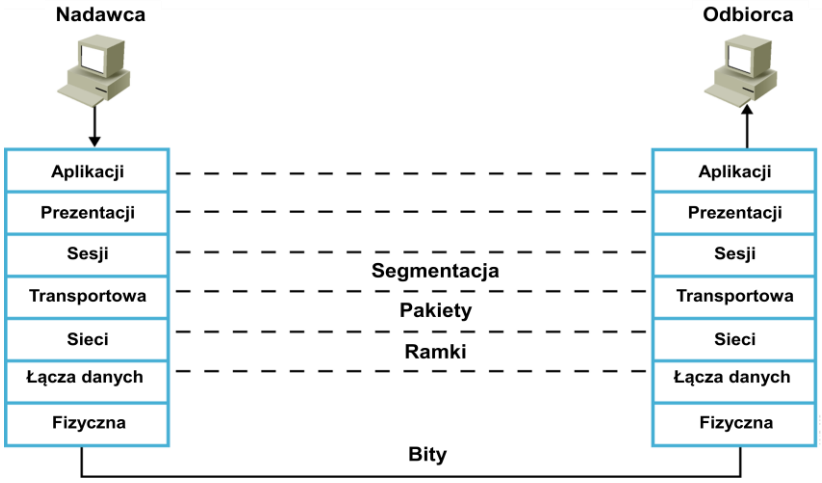
Znając zasadę działania modelu OSI należy jeszcze usystematyzować pojęcia, które będą się pojawiały w odniesieniu do określonych warstw. Kiedy dane są przesyłane przez model OSI na poziomie warstwy transportowej następuje proces zwany **segmentacją**. To nic innego jak podzielenie danych na mniejsze kawałki. Zapewnia to szybszy transport danych do odbiorcy, co więcej urządzenia posiadają pełną kontrolę, co zostało przesłane a co wymaga retransmisji. W procesie retransmisji utraconych danych jest to istotna informacja, jakie elementy nie dotarły do odbiorcy i co należy ponownie przesłać.

Na poziomie warstwy sieciowej posegmentowane dane zostają przekształcone w pakiety. W nagłówku zostają uzupełnione pola **źródłowego i docelowego adresu IP** oraz pojawia się informacja, z jakim protokołem warstwy 4 należy się kontaktować.



Warstwa łącza danych będzie odpowiedzialna za sprawdzenie poprawności otrzymanych informacji, weryfikacja obywa się w oparciu o wyliczenie sumy kontrolnej ramki. W nagłówku zostaną uzupełnione pola **źródłowego i docelowego adresu mac adresu** oraz informacja, z jakim protokołem warstwy sieciowej należy się komunikować. Dodatkowo warstwa łącza danych odpowiednio formatuje dane do przesłania ich przez medium fizyczne. W tej warstwie mówimy o ramkach.

W ostatnim kroku dane są przesyłane przez fizyczne medium w formie bitów. Poniżej schemat obrazując powyższe procesy.



5. TCP/UDP

Warstwa transportowa spełnia istotną role w procesie przesyłania danych, ponieważ: ustanawia wirtualne obwody pomiędzy hostami zanim nastąpi proces przesyłania danych. Wyposażona w funkcje niezawodnego dostarczania danych, która umożliwia przesyłanie utraconych danych. Dodatkowo wykorzystuje funkcje przeciwdziałającą przeciążeniu odbiorcy (flow control). Wspiera multiplexing, czyli możliwość komunikowania się oraz odbierania danych w tym samym czasie.

W obrębie warstwy transportowej będą pracowały dwa protokoły **TCP** oraz **UDP**. Każdy z nich posiada zupełnie inna charakterystykę działania i będzie używany do obsługi innego typu danych przesyłanych przez nadawcę.

Charakterystyka protokołu TCP:

- Jest to protokół zorientowany połączeniowo, zanim dane zostaną przesłane do odbiorcy TCP sprawdzi czy odbiorca jest zainteresowany komunikacją z nadawcą. Jeśli jest zgoda na komunikację, urządzenia wykorzystają mechanizm „trójstronnego uścisku dłoni" celem utworzenia wirtualnego obwodu. Świadczy to o możliwość przesyłania danych do odbiorcy.

- Jest to protokół, który zapewnia dostęp do usług sieciowych dla warstwy aplikacyjnej.

- Wykorzystuje full-duplex - możliwość komunikowania się oraz odbierania danych w tym samym czasie.

- Wbudowany mechanizm kontroli błędów.

- Przypisuje przesyłanym danym numery sekwencyjne, które pokazują, jaka partia danych jest przesyłana oraz w procesie retransmisji TCP używa numery sekwencyjne do ponownego przesłania utraconych danych.

- Wykorzystuje mechanizm potwierdzeń w celu upewnienia się, że określona partia informacji dotarła do odbiorcy i można przesyłać kolejną partię. Ewentualnie rozpocząć proces retransmisji - ponownego przesyłanie brakujących informacji.

Charakterystyka protokołu UDP:

- Jest to protokół niezorientowany połączeniowo, nie sprawdza czy odbiorca jest zainteresowany komunikacją z nadawcą.

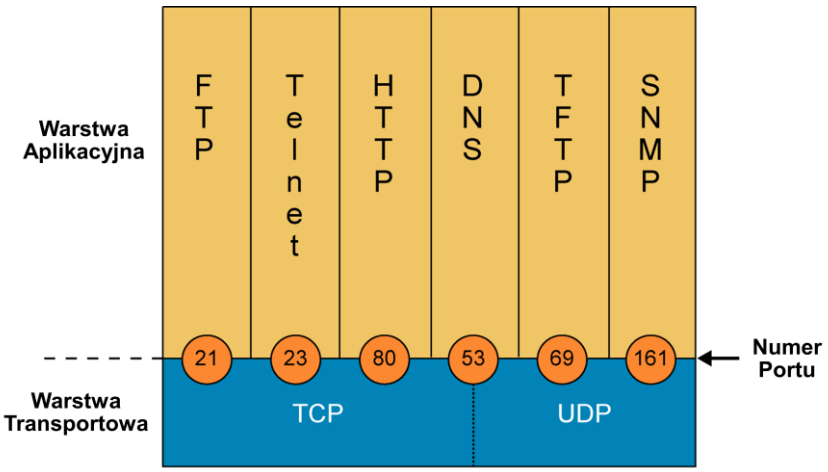
- Jest to protokół, który zapewnia warstwie aplikacyjnej dostęp do usług sieciowych bez żadnych gwarancji dostarczenia w sposób niezawodny danych.

- dostarcza usługę „**best-effort delivery**" – po otrzymaniu danych są one natychmiast przesyłane do odbiorcy.

- nie posiada funkcji odzyskiwania utraconych danych.

Na poziomie warstwy transportowej podejmowana jest decyzja, jaki protokół należy użyć do przesyłania danych z warstwy aplikacyjnej do docelowego odbiorcy. Ten proces nazywamy

„mapowaniem” i wykorzystuje on informacje o protokole TCP/UDP oraz numerze portu, który będzie wykorzystywała określona aplikacja.



Lista niektórych standardowych usług:

BOOTP – serwer 67, klient 68

DNS – 53

FTP – 20, przesyłanie danych

FTP – 21, przesyłanie poleceń

HTTP – 80, dodatkowe serwery, np. proxy, są najczęściej umieszczane na porcie 8080

HTTPS – 443 (HTTP na SSL)

IMAP – 143

IMAP3 – 220

IRC – 6661 do 6667

LDAP – 389

LDAPS – 636 (LDAP na SSL)

MySQL – 3306

NNTP – 119

POP3 – 110

POP3S – 995 (POP3 na SSL)

PostgreSQL – 5432

Rsync – 873

SMTP – 25

SSH – 22

Syslog – 514

Telnet – 23

TFTP – 69

6. Ethernet i Mac-adres

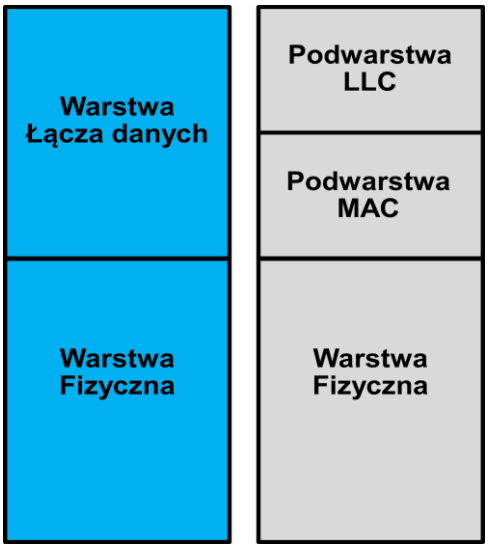
Ethernet – to technologia, która zawiera określone standardy wykorzystywane w budowie sieci lokalnych. Standardy te obejmują parametryzację przewodów (medium) oraz przesyłanych nimi sygnałów. Ethernet odnosi się również do struktury ramki oraz protokołu łącza danych modelu OSI.

W obrębie warstwy łącza danych (L2) będą operowały dwie podwarstwy: **LLC** oraz **MAC**. Zapewniają one komunikację warstwy łącza danych z warstwą sieciowa oraz warstwą fizyczną.

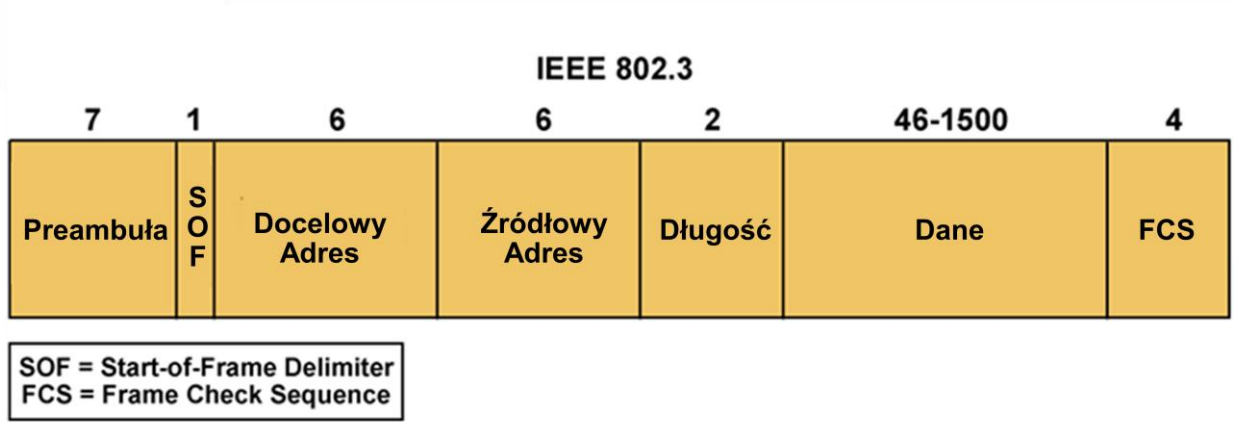
Charakterystyka podwarstw:

LLC (Logical Link Control) - to podwarstwa, która jest odpowiedzialna za komunikowanie się warstwy łącza danych z określonym protokołem warstwy sieciowej (IP, IPX, Apple Talk).

MAC (Media Access Control) - jest to podwarstwa odpowiedzialna za przechowywanie fizycznych adresów mac urządzeń oraz komunikację z warstwą fizyczną.



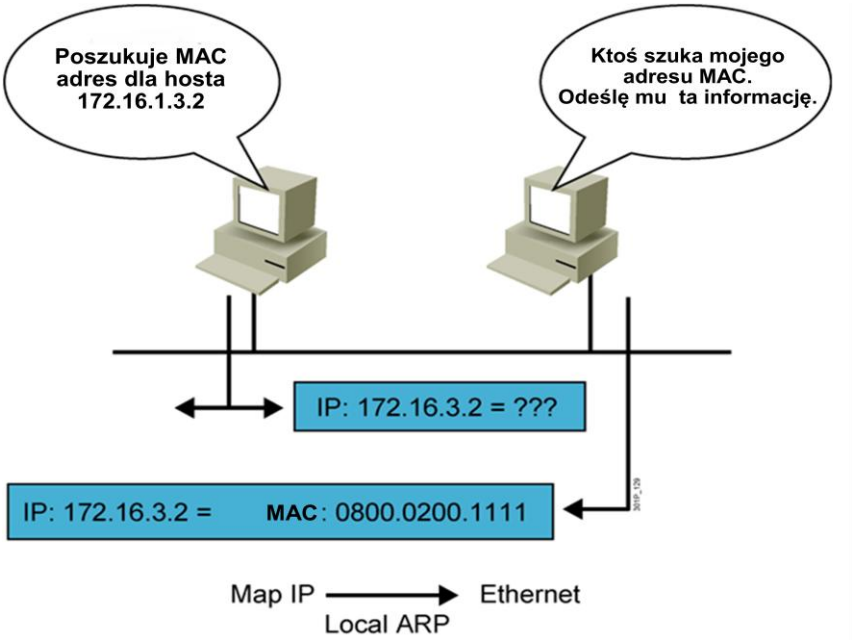
Struktura ramki Ethernetowej zawiera zbiór pól, które musza zostać uzupełnione określonymi parametrami, aby była możliwość przesyłania informacji pomiędzy urządzeniami.



Pola adres docelowy oraz źródłowy będą wymagały wprowadzenie określonych adresów MAC nadawcy oraz odbiorcy. W obrębie tych dwóch pól operuje **podwarstwa MAC**.

W polu „**Długość**” zapisywana jest informacja, jaki protokół warstwy sieciowej jest używany i z jakim należy się komunikować w procesie de-enkapsulacji. Za przechowywanie tej informacji odpowiada **podwarstwa LLC**.

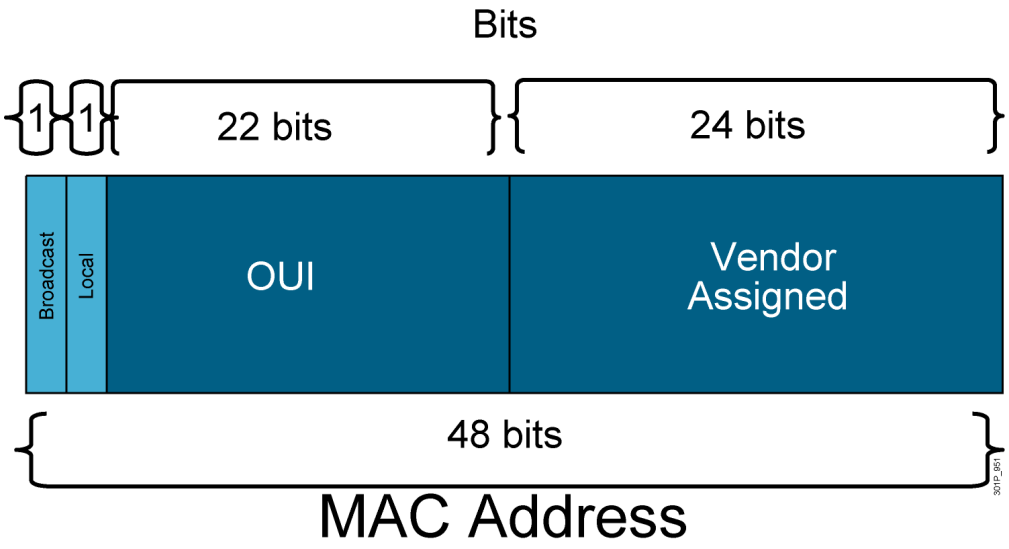
W jaki sposób urządzenia są w stanie poznać mac adres docelowego hosta? W obrębie warstwy łącza danych będzie używany protokół **ARP (Address Resolution Protocol). ARP** – jest protokołem sieciowym umożliwiający zamianę logicznych adresów IP, na fizyczne adresy warstwy łącza danych. W wyniku działania tego protokołu następuje mapowanie adresu logicznego z fizycznym.



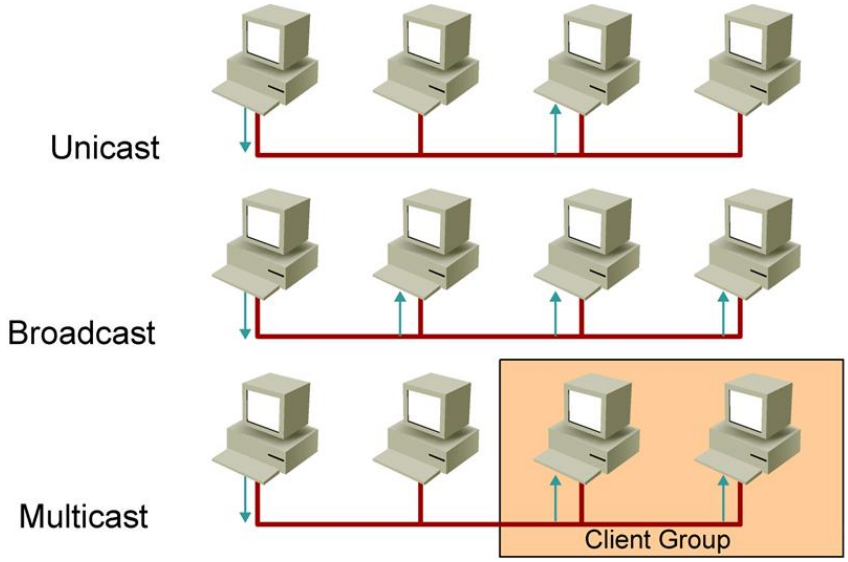
Tablica ARP jest budowana lokalnie w każdym urządzeniu, po upływnie 5 minut tablica jest czyszczona z wpisów adresów mac. Żeby wyświetlić tablicę ARP należy w linii poleceni w systemie Windows, Linux wpisać polecenie **arp –a**.

```
D:\>arp -a

Interface: 192.168.1.101 on Interface 0x1000003
  Internet Address      Physical Address      Type
  192.168.1.1           00-04-5a-22-ec-c7     dynamic
  192.168.1.40          00-02-4b-cc-d6-d9     dynamic
  192.168.1.42          00-02-fd-65-9f-82     dynamic
  192.168.1.43          00-03-6b-09-59-29     dynamic
  192.168.1.100         00-02-4b-cc-d6-d0     dynamic
  192.168.1.135         00-03-6d-1e-6a-a5     dynamic
  192.168.1.149         00-50-8b-f7-cf-59     dynamic

D:\>_
```

Adres Mac jest to 48-bitowy adres zapisywany heksadecymalnie (szesnastkowo). Pierwsze 24 bity oznaczają producenta karty sieciowej, pozostałe 24 bity są unikatowym identyfikatorem danego egzemplarza karty. Na przykład adres **00:1F:16**:**24:ED:04** oznacza, że producentem karty jest firma Intel, i została opatrzona numerem identyfikacyjnym 24:ED**:04**.



W sieciach możemy spotkać klika rodzajów typów komunikacji realizowanej pomiędzy urządzeniami. Będą to Unicast-y, Broadcast-y oraz Multicast-y.



Unicast – jest to komunikacja realizowana z określonego źródła do określonego jednego celu np. komunikacja ze stroną www.

Broadcast – jest to komunikacja realizowana z określonego źródła do wszystkich odbiorców w danym segmencie sieci, np. zapytanie ARP.

Multicast - jest to komunikacja realizowana do określonej grupy odbiorców. Odbiorcy są widziani dla nadawcy, jako pojedynczy grupowy odbiorca (host group) dostępny pod jednym adresem dla danej grupy multikastowej.

7. Adresacja IP

Adres IP to unikalny identyfikator każdego urządzenia pracującego w sieci. To inaczej pesel urządzenia, którym się posługuje urządzenie w sieci. Nie dopuszczalny jest fakt, aby adres przypisany dla określonego urządzenia powtórzył się w sieci. Struktura adresu to **cztery ośmiobitowe oktety**, które odpowiadają wartości 32 bitów. Mogą być one wypełnione na przemiennie **1** lub **0**. Każdy oktet jest od siebie oddzielony „ **.**” , dzięki czemu adres staje się bardziej czytelny i łatwy do interpretacji np. 192.168.110.67.

Ludzie używają zapisu adresu sieciowego w formacie decymalnym, tym którym się posługujemy na co dzień. W przypadku maszyn cyfrowych sytuacja jest odwrotna, używany jest zapis binarny (**11000000.10101000. 01101110.01000011)**. W wyniku „**zapalania się**" odpowiednio wartości „**1**" lub „**0**" na 32 bitach, urządzenia są w stanie poprawnie interpretować np. adresy IP czy maski sieciowe.

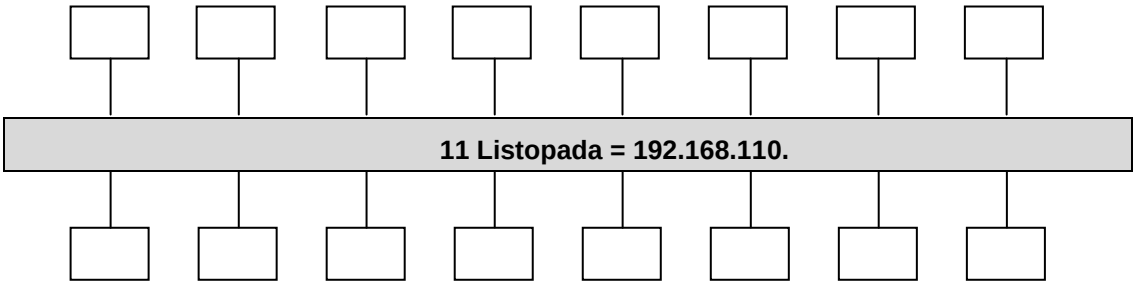
Zapis binarnym	**1 1000000**	**1 0101000**	**0 1101110**	**01 000011**
Zapis decymalny	**1 92.**	**1 68.**	**1 10.**	**67**

Co jeszcze kryje się w adresie IP? Przede wszystkim dwie istotne informacje tj.: **adres sieci** oraz **adres hosta**.

NETWORK ADRESS			**HOST ADRESS**
192	**168**	**110**	**67**

Te wartości pozwalają określić urządzeniom, w jakiej sieci się znajdują oraz jaki posiadają unikalny identyfikator sieciowy.

W codziennym życiu podobne zjawisko możemy zaobserwować na przykładzie ulicy i numerów domów. Nazwa głównej ulicy odpowiada adresowi sieciowemu natomiast numery domów będą reprezentowały adresy hostów.



Pojawia się pytanie, w jaki sposób urządzenia interpretują zapis decymalny adresów IP na zapis binarny?

Wiemy, że adres sieciowy składa się z czterech oktetów, które reprezentują zapis 32 bitowego adresu IP. Oktet składa się z ośmiu bitów, każdy z tych bitów będzie mógł przyjmować wartości „**1**” lub „**0**” . Kiedy bit zostanie ustawiony na wartość „1” zostanie mu przypisana wartość liczbowa z poniższej tabelki, która reprezentuje potęgę liczby 2. Natomiast kiedy bit przyjmie wartość „**0**”, jego decymalna wartość równa się „0”. Sumując wartości liczbowe przypisane dla każdego bitu otrzymamy liczbę decymalną reprezentującą dany oktet.

Skrajny lewy bity	7	2*2*2*2*2*2*2	**28**
	6	2*2*2*2*2*2	**4**
	5	2*2*2*2*2	**2**
	4	2*2*2*2	**6**
	3	2*2*2	
	2	2*2	
	1	2	
Skrajny prawy bit	0		

Na poniższym przykładzie dokonamy konwersji zapisu decymalnego na binarny w oparciu o liczbę 35.

Potęga	7	6	5	4	3	2	1	0
Wartość potęgi	**28**	**4**	**2**	**6**				
Binarna wartość								

Cały proces konwersji rozpoczyna się od sprawdzenia czy określona wartość potęgi liczby 2 będzie zawierała się w liczbie **35**. Pierwsze dwie liczby 128 oraz 64 nie spełniają tego warunku dlatego bity zapalają się wartością „**0**”. W przypadku liczby 32 następuje dopasowanie i bit zostanie zapalony wartością „1”. Po odjęciu od siebie dwóch cyfr 35 – 32 otrzymujemy wartość **3**,

którą należy dopasować do pozostałych wartości potęgi liczby 2.

W przypadku wartości 16, 8, 4 nie następuje dopasowanie, dlatego też bity zostaną odpowiednio zapalone na „**0**”. Dopiero liczba 2 będzie spełniała nasz warunek i bit zostanie zapalony na „1”. Różnica pomiędzy cyframi 3 - 2 równa się 1 i do tej wartości dopasuje się ostatni bit w naszym oktecie, który przyjmie wartość 1. Wynik konwersji liczby **35** na zapis binarny otrzymuje wartość **00100011**, która będzie zrozumiała dla urządzeń cyfrowych.

Na poniższym przykładzie dokonamy konwersji zapisu binarnego [**10111001**] do zapisu decymalnego wykorzystując potęgę liczby 2.

Potęga	7	6	5	4	3	2	1	0
Wartość potęgi	**28**	**4**	**2**	**6**				
Binarna wartość								
Decymalna wartość	**28**		**2**	**6**				

W wierszu „**Binarna wartość** „zostały wprowadzone wartość **1** i **0** i na tej podstawie postaramy się ustalić jak to liczba w formacie decymalnym kryje się pod tym zapisem. Kiedy bit przyjmuje wartość „1” będzie to sugerowało nam konieczność odnalezienia wartości decymalnej potęgi liczby 2 i wpisanie jej poniżej bitu zapalonego na „1”. Kiedy mamy uzupełnione wartości decymalne dokonujemy sumowania **128**+0+**32**+**16**+**8**+0+0+**1** = **185**

Liczba 185 będzie reprezentowała jeden oktet adresu sieciowego.

W sieciach występują różne klasy adresów takie jak **A,B,C**. Każda z tych klas będzie miała inną cechę szczególną, która ją wyróżnia.

W przypadku klasy „**A**” cechą szczególną jest przede wszystkim fakt, że pierwszy oktet został zarezerwowany na **ADRES SIECI**, a pozostałe trzy oktety będą reprezentowały **ADRESY HOSTÓW**.

0XXXXXXX	HOST	HOST	HOST

Kiedy przyjrzymy się pierwszemu oktetowi zarezerwowanemu na adresy sieci, widać że pierwszy ważny bit został zapalony wartością „**0**” i jest to wartość **niezmienna**.

Pozostałe siedem bitów może przyjmować naprzemiennie wartości „**0**” lub „**1**”. Pojawiają się dwa wyjątki od tej reguły: kiedy wypełnimy wszystkie siedem bitów wartością „**0**” [**00000000**] otrzymamy w zapisie decymalnym „**0**”. Sieć o adresie „**0**” nie istnieje.

Kolejne odstępstwo od w/w reguły pojawia się kiedy wypełnimy wszystkie siedem bitów wartością „**1**” [**01111111**] otrzymujemy adres sieci 127.X.X.X – który jest zarezerwowany do celów diagnostycznych.

W przypadku klasy A dysponujemy bardzo dużą ilością adresów dla hostów natomiast ograniczoną ilością adresów sieci. Dostępna liczba adresów dla hostów to 224- 2 hosty **= 16777214** hostów. Zakres dostępny adresów siec 1 – 126. Wartości te wynikają z potęgi liczby 2.

W przypadku klasy „**B**” cechą szczególną jest przede wszystkim fakt, że pierwsze dwa oktety został zarezerwowany na **ADRES SIECI**, a pozostałe dwa oktety będą reprezentowały **ADRESY HOSTÓW**.

10XXXXXX	**NETWORK**	HOST	HOST

Kiedy przyjrzymy się pierwszemu oktetowi, widać że pierwsze dwa ważne bity zostały zapalone wartością „**10**” i jest to wartość, niezmienna. Wskazuje to na początek adresów sieciowych dla klasy „**B**”. Pozostałe bity mogą przyjmować naprzemiennie wartości „**0**” lub „**1**”.

W przypadku klasy B dysponujemy sporą ilością adresów dla hostów i znaczą ilością adresów sieci. Dostępna liczba adresów **to 2^{16}- 2 hosty = 65534** hostów, zakres dostępny adresów sieci dla klasy „B” : 128 – 191. Wartości te wynikaj w potęgi liczby 2.

W przypadku klasy „**C**” cechą szczególną jest przede wszystkim fakt, że trzy oktety zostały zarezerwowane na **ADRES SIECI**, a pozostały oktet będzie reprezentował **ADRESY HOSTÓW**.

110XXXXX	**NETWORK**	**NETWORK**	HOST

Kiedy przyjrzymy się pierwszemu oktetowi widać, że pierwsze trzy ważne bity zostały zapalone wartością „**110**” i jest to wartość, niezmienna. Wskazuje to na początek adresów

sieciowych dla klasy „**C**”. Pozostałe bity mogą przyjmować naprzemiennie wartości „**0**” lub „**1**”. W przypadku klasy **C** dysponujemy ograniczoną ilość adresów dla hostów i znaczą ilością adresów sieci. Dostępna liczba adresów to **2^8- 2 hosty = 254** hosty, zakres dostępny adresów sieci dla klasy „C” : 192 – 223. Wartości te wynikaj w potęgi liczby 2.

Część hosta wyliczamy w oparciu o poniższy wzór:

$$2^h - 2$$

gdzie h – to liczba bitów z części hosta.

7.1. Czym są maski sieciowe i po co je musimy używać?

Maski sieciowe pojawiły się w sieciach w wyniku szybko kurczących się przestrzeni adresowych adresów w wersji 4. Duży popyt na publiczne adresy wymusiło wprowadzenie podziału sieci na podsieci i wykorzystanie masek sieciowych. Maski pozwalają nam w elastyczny sposób dokonywać podziału każdej klasy adresów na mniejsze grupy tzw. podsieci.

Czym jest maska sieciowa? – to liczba służąca do wyodrębnienia w adresie IP części sieciowej od części hosta. Zapisywana podobnie jak adres IP na czterech oktetach z tą różnicą, że składa się ona z ciągu bitów o wartości „**1**”, po których następuje ciąg „0”. Maska stanowi istotną informację dla urządzeń sieciowych, ponieważ na tej podstawie urządzenia potrafią zidentyfikować, w jakiej sieci pracują.

Poniżej tabelka przedstawia domyślne wartości masek dla różnych klas adresów.

Klasa	Maska domyślna	Oktet I	Oktet II	Oktet III	Oktet IV
A	255.0.0.0	11111111	0	0	0
B	255.255.0.0	11111111	11111111	0	0
C	255.255.255.0	11111111	11111111	11111111	0

W jaki sposób routery czy komputery potrafią ustalić, w jakiej sieci pracują? – wykorzystują tutaj porównania dwóch dostępnych informacji takich jak adresu IP oraz maski sieciowej. Jeżeli urządzenie dysponuje adresem 192.168.110.56 oraz maską 255.255.255.0 to wykonywany jest logiczny AND (mnożenie Adresu IP i maski sieciowej), dzięki czemu otrzyma dwie informacje: w jakiej sieci pracuje i jaki jest identyfikator hosta.

Adres IP	192.168.110.56	11000000	10101000	01101110	0110111
Maska sieciowa	255.255.255.0	11111111	11111111	11111111	00000000
Mnożenie AND		11000000	10101000	01101110	00000000
Adres sieci		192	168	110	0
Adres hosta		-	-	-	56
Adres rozgłoszeniowy		11000000	1010100	01101110	11111111

Kiedy oktet / oktety zarezerwowane na adresy hosta zostaną wypełnione samymi „1” utworzony zostanie adres rozgłoszenia dla danej sieci. Należy pamiętać, że **adresu sieci** jak i **adresu rozgłoszeniowego** nie wolno nam używać do adresowania urządzeń w sieci.

7.2. Podział sieci na podsieci, z czego to wynika?

Chcąc uniknąć tworzenia płaskiej struktury sieci opartej na jednym adresie sieci przypisywanym wszystkim urządzeniom w infrastrukturze, należy wprowadzić podział sieci na podsieci. Płaska struktura wprowadza sporo problemów między innymi: problemy z rozgłoszeniami, problemy z zabezpieczeniem dostępu do zasobów sieciowych, problemy z multicast-ami.

Podsieci to sieci, które zostały wydzielone z głównego adresu sieci. Cały proces polega na pożyczaniu bitów. Wolno nam pożyczać jedynie bity z pól zarezerwowanych na **adresy hostów**. O ilości zapożyczonych bitów z adresu hosta decyduje maska podsieci.

Załóżmy, że posiadamy adres sieci **192.168.1.0/24** i chcemy utworzyć **8** podsieci. Zaczynamy od ustalenia ile bitów należy pożyczyć z ostatniego oktetu zarezerwowanego na adresy hostów, aby uzyskać 8 podsieci. Do tego celu będziemy korzystać z wzoru:

$$2^S$$

gdzie S – to liczba bitów, które pożyczamy z części hosta.

	Oktety I	**Oktet II**	**Oktet III**	**Oktet IV**
Domyślna maska klasy C	**255**	**255**	**255**	**0**
Zapis binarny maski klasy B	**11111111**	**11111111**	**11111111**	**00000000**

Aby utworzyć **8** podsieci musimy pożyczyć **3** bity z ostatniego oktetu **$2^3 = 8$**.

Pożyczam 3 bity na kolejne 8 subnetów	**11111111**	**11111111**	**11111111**	**11100000**

W wyniku pożyczenia 3 bitów powstanie nowa maska sieciowa. Z domyślnej **/24** bitowej została utworzona **/27** bitowa maska [**255.255.255.224**]. Teraz musimy ustalić, jakie powstaną podsieci i ile hostów w nich będzie mogło pracować. Do tego celu posłuży nam ostatni oktet. Za ostatnim trzecim bitem, który zapalił się na „1” wstawiamy pionowa kreskę, która będzie oddzielała adresy sieci od adresów hostów (bity zapalone wartością „0”). **111|00000**.

W kolejnym kroku należy rozpisać część sieciową „**111**” na wszystkie możliwe kombinacje tak jak w poniższej tabeli.

OKTET IV	Adres sieci	Adresy hostów
	111	00000
1 podsieć	000	00000
2 podsieć	001	00000
3 podsieć	010	00000
4 podsieć	011	00000
5 podsieć	100	00000
6 podsieć	101	00000
7 podsieć	110	00000
8 podsieć	111	00000

Znając już wszystkie kombinacje dla adresów sieciowych, możemy ustalać zakresy wszystkich podsieci. Do tego celu należy wykorzystać tabelkę z potęgą liczby 2 i odszukać wartości liczbowe dla określonych bitów.

Potęga	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Wartość potęgi	128	64	32	16	8	4	2	1

Poniżej w tabeli zostały przedstawione zakresy adresów dla wszystkich ośmiu podsieci

OKTET IV	Adres sieci
1 podsieć	192.168.1.0
2 podsieć	192.168.1.32
3 podsieć	192.168.1.64
4 podsieć	192.168.1.96
5 podsieć	192.168.1.128
6 podsieć	192.168.1.160
7 podsieć	192.168.1.192
8 podsieć	192.168.1.224

Ostatnią rzeczą, jaka musimy ustalić to liczba dostępnych hostów dla każdej podsieci. Wykorzystamy do tego wzór:

$$2^h - 2$$

gdzie h – to liczba bitów z części hosta.

$$2^5 - 2 = 32\text{-}2 = 30 \text{ hostów.}$$

W naszym przypadku dysponujemy 5 bitami, które możemy wykorzystać do zaadresowania hostów. Od otrzymanej wartości 32 musimy odjąć dwa adresy, których nie wolno mam używać: **adres sieci** oraz **adres rozgłoszeniowy**, dlatego realna liczba adresów przewidziana dla hostów to 30.

Tabela poniżej zawiera szczegółowe informacje dotyczące wykonanego podziału sieci na 8 podsieci w oparciu o źródłowy adres 192.168.1.0/24

	Adres sieci	**Adresy dla hostów**	**Adres rozgłoszeniowy**
1 podsieć	**192.168.1.0 /27**	**1 - 30**	**192.168.1.31**
2 podsieć	**192.168.1.32 /27**	**33 - 62**	**192.168.1.63**
3 podsieć	**192.168.1.64 /27**	**65 - 94**	**192.168.1.95**
4 podsieć	**192.168.1.96 /27**	**97 - 126**	**192.168.1.127**
5 podsieć	**192.168.1.128 /27**	**129 - 158**	**192.168.1.159**
6 podsieć	**192.168.1.160 /27**	**161 - 190**	**192.168.1.191**
7 podsieć	**192.168.1.192 /27**	**193 - 222**	**192.168.1.223**
8 podsieć	**192.168.1.224 /27**	**225 - 254**	**192.168.1.255**

Kolejny aspekt posługiwania się adresami sieciowymi będzie dotyczył umiejętności odnajdowania określonej podsieci na podstawie adresu IP hosta.

Załóżmy, że dysponujemy adresem 192.168.1.156 / 27 i chcemy poznać, w jakiej podsieci pracuje nasz host. Krok pierwszy będzie wymagał od nas rozpisania w formacie binarnym liczby .156 (reprezentuje czwarty oktet) oraz ostatni oktet maski podsieci.

Zapis binarny liczby .156	**100|11100**
Zapis binarny maski sieciowej	**111|00000**

Następnie wykonujemy mnożenie logiczne (AND) pierwszych trzech bitów, z adresu hosta oraz maski sieciowej. Czemu tylko trzy bity? Ponieważ pierwsze trzy bity w adresie maski, będą wyznaczały granicę pomiędzy adresami sieci a adresami hostów.

Zapis binarny liczby .156	**100|11100**
Zapis binarny maski sieciowej	**111|00000**
Wartość logicznego AND	**100|00000**

Otrzymana wartość iloczynu pozwala nam dokładnie określić sieć, w jakiej pracuje ten konkretny host. Do tego celu ponownie wykorzystamy tabelkę z potęgą liczby 2.

Tabela poniżej zawiera szczegółowe informacje, które możemy uzyskać wykorzystując powyższą metodę.

Adres sieci:	**192.168.1.128**
Adres pierwszego hosta:	**192.168.1.129**
Adres ostatniego hosta:	**192.168.1.162**
Adres rozgłoszeniowy:	**192.168.1.163**

8. Ćwiczenia #1 Adresacja IP

8.1. Zadanie 1: Dokonaj konwersji zapisu decymalnego na binarny.

Potęgi 2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Wartość decymalny	128	64	32	16	8	4	2	1

Zapis decymalny	Zapis binarny
48	
146	
222	
119	
135	
60	

8.2. Zadanie 2: Dokonaj konwersji zapisu binarnego na decymalnego.

Zapis binarny	Zapis decymalny
11001100	
10101010	
11100011	
10110011	
00110101	
10010111	

8.3. Zadanie 3: Konwersja Adresu IP do zapisu binarnego.

Adres IP : 145.32.59.24

Zapis decymalny	Zapis binarny
145	
32	
59	
24	
Binarny format :	

Adres IP : 200.42.129.16

Zapis decymalny	Zapis binarny
200	
42	
129	
16	
Binarny format :	

Adres IP : 14.82.19.54

Zapis decymalny	Zapis binarny
14	
82	
19	
54	
Binarny format :	

8.4. Zadanie 4: Konwersja zapisu binarnego do Adresu IP.

Zapis decymalny : 11011000.00011011.00111101.10001001

Zapis decymalny	Zapis binarny
11011000	
00011011	
00111101	
10001001	
Adres IP :	

Zapis decymalny: 11000110.00110101.10010011.00101101

Zapis decymalny	Zapis binarny
11000110	
00110101	
10010011	
00101101	
Adres IP :	

Zapis decymalny: 01111011.00101101.01000011.01011001

Zapis decymalny	Zapis binarny
01111011	
00101101	
01000011	
01011001	
Adres IP :	

8.5. Zadanie 5: Zidentyfikuj klasę adresu IP oraz liczbę hostów dostępną dla danej klasy.

Adres IP	Klasa Adresu	Ilość bitów w adresie sieci	Max ilość hostów
145.32.59.24			
200.42.129.16			
14.82.19.54			
216.27.61.137			
179.45.67.89			
198.53.147.45			

8.6. Zadanie 6: Sprawdź poprawność poniższych adresów.

Adres IP	Poprawny / Niepoprawny	Jeżeli nie poprawny to z czego to wynika.
145.32.259.24		
200.42.129.16		
14.19.54		
216.27.61.137		
0.139.25.16		
255.255.255.255		

8.7. Zadanie 7: Określ liczbę bitów potrzebnych do utworzenia podsieci w klasie C.

Libcza podsieci	Ilość pożyczanych bitów	Ilość dostępnych adresów dla hostów
2		
5		
12		
24		
40		

8.8. Zadanie 8: Określ liczbę bitów potrzebnych do utworzenia podsieci w klasie B.

Libcza podsieci	Ilość pożyczanych bitów	Ilość dostępnych adresów dla hostów
5		
8		
14		
20		
35		

8.9. Zadanie 9: Maski sieciowe oraz dostępna liczba hostów.

Maska sieciowa	Zapis decymalny maski	Zapis binarny maski	Liczba hostów dla danej podsieci.
/20			
/21			
/22			
/23			
/24			
/25			
/26			
/27			
/28			
/29			
/30			

8.10. Zadanie 10: Wykonaj podział sieci na podsieci.

Otrzymałeś adres sieci 192.168.1.0 /24 który należy:

a) podzielić na 6 podsieci .

b) określić nową maskę sieciową.

c) wypełnić poniższą tabelkę

Nr. Podsieci	Adres sieci	Zakres adresów dla hostów	Adresy rozgłoszeniowe
0			
1			
2			
3			
4			
5			

8.11. Zadanie 11: Ustal, w jakiej sieci pracuje poniższy adres.

Otrzymałeś adres ip 192.168.111.129 /28

a) zapisz maskę sieciową w formacie decymalny oraz binarnym.

b) ile podsieci możemy utworzyć używając powyższą maskę sieciową?

c) ile hostów będzie pracowało w każdej podsieci?

d) ustal, w jakiej podsieci sieci pracuje adres **192.168.111.129** oraz ustal pozostałe dostępne adresy oraz adres rozgłoszeniowy.

8.12. Zadanie 12: Ustal, w jakiej sieci pracuje poniższy adres.

Otrzymałeś adres ip 192.168.111.163 /29

a) zapisz maskę sieciową w formacie decymalny oraz binarnym.

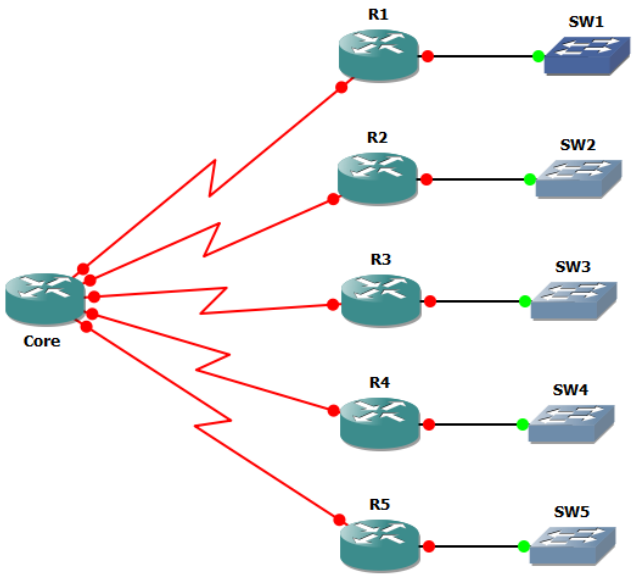
b) ile podsieci możemy utworzyć używając powyższą maskę sieciową?

c) ile hostów będzie pracowało w każdej podsieci?

d) ustal, w jakiej podsieci sieci pracuje adres **192.168.111.163** oraz ustal pozostałe dostępne adresy oraz adres rozgłoszeniowy.

8.13. Zadanie 13: Wykonaj podział sieci na podsieci.

Dysponujesz w firmie poniższą topologa. Twoim zadaniem jest zaplanowanie odpowiedniej ilości adresów na potrzeby firmy według poniższych wytycznych.



Posiadasz adres sieci 192.168.110.0 /24 i na tej podstawie:

a) Utwórz **18** podsieci w których pracują po **4** hosty.

b) Wykorzystaj **18-stą** podsieć do zaadresowanie połączeń **point-to-point /30 pomiędzy routerami**.

9. Switche – podstawy

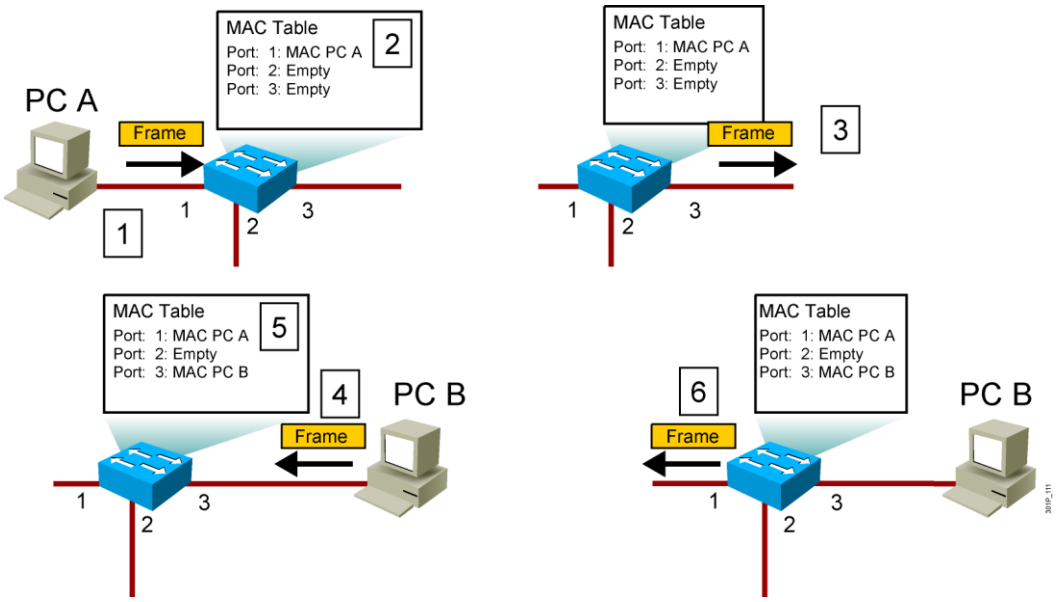
W początkach rozwoju sieci urządzeniami, które pozwalały na komunikowanie się większej grupy użytkowników między sobą były huby. Urządzenia te nie były optymalnym rozwiązaniem. Często powstające kolizje oraz towarzyszące im retransmisje danych powodowały, iż w sieci panował paraliż i ogromne opóźnienia. Ten stan narastał wraz z szybkim rozwojem komputerów klasy PC i coraz większym apetytem ich użytkowników na dostęp do zasobów.

Alternatywą dla hub-ów miały być mosty. To nic innego jak komputer PC wyposażony w większą ilość kart sieciowych. W efekcie dokonano pierwszej segmentacji sieci. Segmentacja polega na podzieleniu jednej wielkiej sieci na mniejsze kawałki, w efekcie czego potencjalne problemy występujące w jednym segmencie sieci nie przenoszą się do kolejnych segmentów sieci. Proces segmentacji pozwolił również ograniczyć rozmiary domeny rozgłoszeniowej, z jednej wielkiej do kliku mniejszych. Mosty dokonywały przełączania ramek, budowały tablice CAM, w której przechowywały nauczone mac-adresy. Jednak wadą tego rozwiązania była prędkość, z jaką były przełączane ramki, ponieważ za ten proces odpowiadał software.

Rozwiązaniem wszystkich problemów, które trapiły sieci oparte o huby lub mosty było wprowadzanie do sieci Switch-y (przełączników). Urządzenia wyposażone w dużą ilość portów 24 i 48, dodatkowo porty pracujące z prędkością 10Mb/s, 100Mb/s, 1000Mb/s zapewniały i zapewniają kompatybilność wstecz, pozwalając podłączyć różne urządzenia do jednego przełącznika, który zapewniał im komunikację. Siłą Switch-y jest szybkość przełączania ramek, która jest realizowana w hardwarerze, dzięki czemu można uzyskać prędkość nawet 130 Gb/s. Tak szybka matryca przełączania pozwala uzyskiwać wydajną komunikację pomiędzy urządzeniami.

Dzisiaj na rynku mamy do czynienia z Switch-ami 1U, takie jak 2960, 3560, 3750X zapewniającymi wysoką wydajność w przełączaniu, jednak istnieją przełączniki znacznie wydajniejsze nazywane modularnymi. Wyposażone w klika slotów 3,6,13 na różne karty rozszerzeń. Używane do agregowania ruchu z wielu przełączników dystrybucyjnych. Takimi urządzeniami są przełączniki z serii 4500, 6500 zapewniające wysoką wydajność. Są to urządzenia operujące w powyżej warstwy 3 modelu OSI.

Switch-e dokonują przełączania w oparciu o tablicę CAM, w której przechowują wpisy dotyczące nauczonych mac adresów. Przełącznik wprowadza kolejne wpisy w tablice CAM, kiedy na porcie pojawia się ramka z nowym adres mac urządzenia. Następuje połączenie dwóch informacji ze sobą: numeru portu oraz adresu mac. Każdorazowo przełącznik zanim prześle ramkę do celu, sprawdzi na jakim porcie znajduje się odbiorca. Poniżej został przedstawiony proces budowy tablicy CAM na przełączniku.



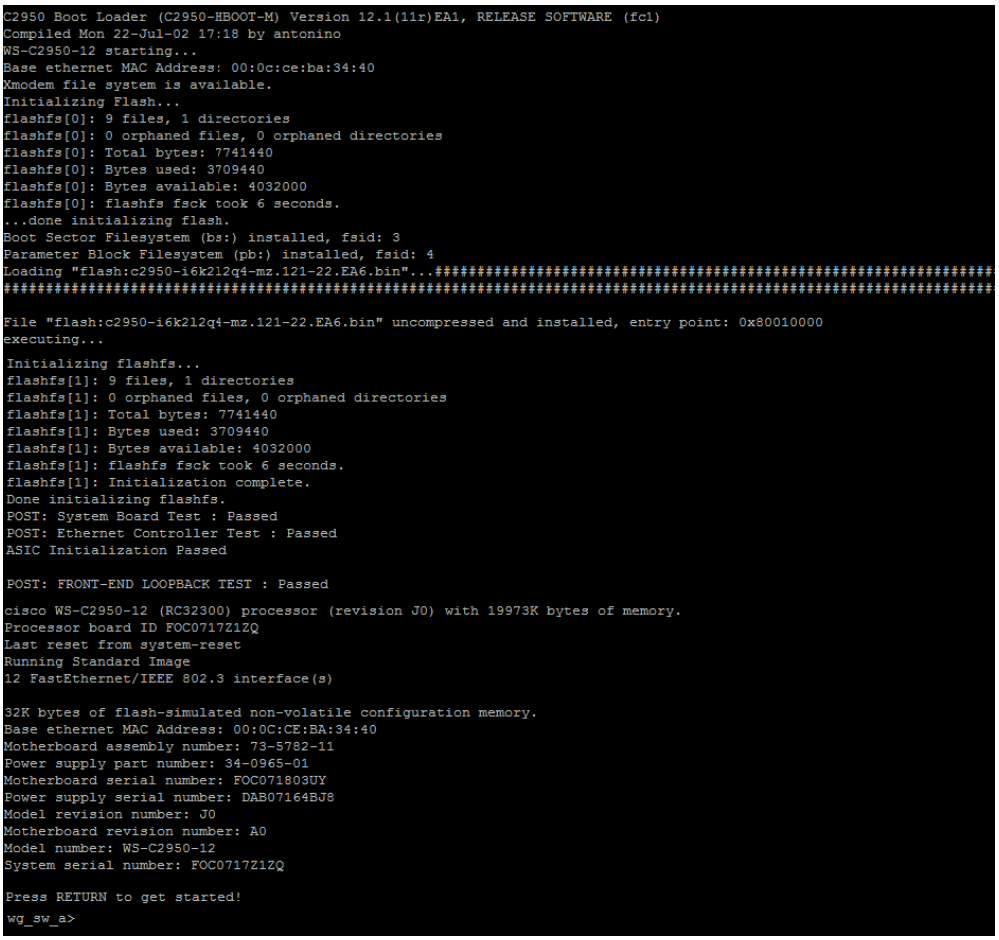
W tym przypadku Host A wysyła zapytanie ARP, które dociera do przełącznika na porcie 1. Switch w swojej tablicy CAM wprowadza mac adres Hosta A i przypisuje mu port 1. Zapytanie ARP jest przenoszone, jako broadcast w sieci. Kiedy przełącznik otrzymuje broadcast rozpoczyna zalewanie wszystkich portów otrzymanym broadcast-em oprócz portu, na którym to rozgłoszenie się pojawiło. Informacja ta dociera do Hosta B, który odpowiada zwrotnie na ARP. Ramka dociera do przełącznika, ponieważ do tej porty nie było żadnej komunikacji pomiędzy nimi, Switch wprowadza do swojej tablicy CAM mac adres Hosta B i przypisuje mu port 2.

W kolejnym kroku przełącznik analizuje w ramce pola docelowego mac adresu. W tym miejscu pojawia się mac adres Hosta A, dlatego Switch zagląda do swojej tablicy CAM, aby ustalić, na którym porcie ten mac adres już figuruje. W efekcie poprzez port 1 Switch prześlę ramkę do Hosta A.

10. Switche – uruchomienie

Zanim uruchomimy przełącznik musimy podłączyć kabel konsolowy do gniazda konsolowego, które jest umieszone na tylni panelu urządzenia. Dodatkowo wymagane jest uruchomienie aplikację hyperterminal lub putty, za pomocą której będzie realizowana komunikacja znakowa z Switchem. Kabel konsolowy jest z jednej strony za terminowany złączem RJ-45, a z drugiej RS232. Po zasileniu urządzenia prądem w oknie konsoli możemy zaobserwować jak przebiega procedura startu urządzenia.

Proces uruchomienia się przełącznika jest bardzo zbliżony do tego, jaki towarzyszy uruchomieniu każdego komputera. W pierwsze fazie jest realizowany POST w czasie, którego sprawdzane jest hardware. Kiedy testy zakończą się pomyślnie urządzane zaczyna wyszukiwać miejsc przechowywania system IOS, na ogół będzie to pamięć FLASH odpowiednik HDD w PC. System jest rozpakowywany do pamięci RAM, ostatnią czynnością, która jest wykonywana to próba zlokalizowania i załadowania pliku konfiguracyjnego. Domyślnie jest on przechowywany w pamięci NVRAM. Po wykonaniu powyższych kroków przełącznik jest gotowy do pracy.



Urządzenia Cisco wyposażone są w system operacyjny nazywany IOS-em. Służy on do zarządzania procesami, które są wykonywane na przełącznikach czy routerach. Jest to system używający linii poleceń (CLI) za pomocą, której możemy wprowadzać odpowiednie komendy. Wszystkie wprowadzane polecenia należy zatwierdzać przy użyciu klawisza **ENTER**. Użytkownicy mogą przeklejać gotową konfigurację z plików tekstowych bezpośrednio w okno konsoli.

Jak każdy system operacyjny tak i IOS posiada dwa tryby pracy tzw. (EXEC MODE), **użytkownika podstawowego** oraz **użytkownika uprzywilejowanego**.

W trybie **użytkownika podstawowego**, urządzenie w linii wiersza poleceń wyświetli nazwę urządzenia (tj. hostname), za którą pojawi się znak większości „**>**" np. **Switch>**. W tym trybie nie mamy prawa wykonywać konfiguracji przełącznika, dysponujemy ograniczoną ilością dostępnych komend.

W trybie **użytkownika uprzywilejowanego,** urządzenie w linii wiersza poleceń wyświetli nazwą urządzenia (tj. hostname), za którą pojawi się znak większości „**#**" np. **Switch#.** Chcąc pracować w trybie uprzywilejowanym na urządzeniu, w trybie zwykłego użytkownika należy wydać polecenie „**enable**" i zatwierdzić klawiszem ENTER.

Switch>enable

Switch#

W tym trybie pracy posiadamy pełną kontrolę nad urządzeniem, dysponując wszystkimi dostępnymi poleceniami.

System IOS dysponuje rozbudowanym system pomocy, dzięki któremu możemy poprawnie wprowadzać komendy. Mamy możliwość korzystania z dwóch trybów pomocy: **Word help** - wprowadzamy jedynie pierwsza literę po czym wprowadzamy znak zapytania, system wyszukuje jedynie dostępne komendy zaczynające się od określonej litery.

wg_sw_a>s?

*s=show set show ssh systat

Syntax help – ten rodzaj pomocy pozwala poznawać dostępne podkomendy występujące w obrębie głównego polecenia. W tym celu należy wprowadzić określoną komendę następnie użyć

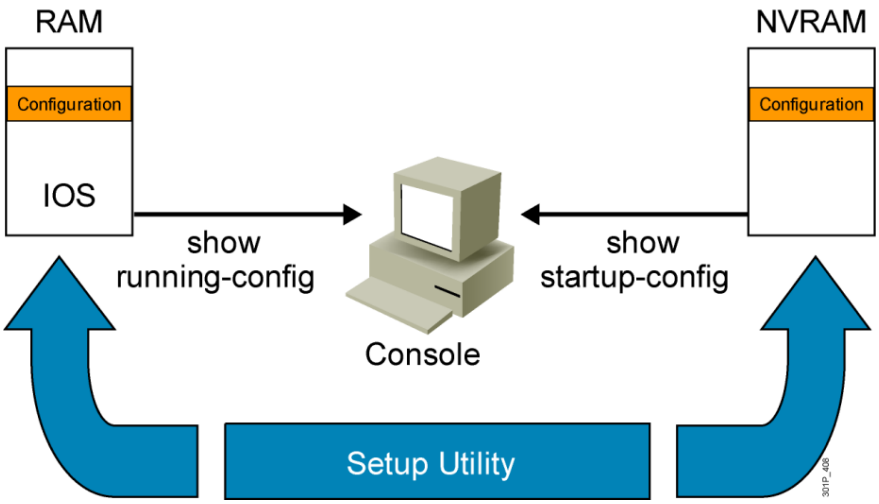
klawisza **SPACE** i ponownie wprowadzić znak zapytania. Na ekranie listuje się lista dostępnych podkomend.

```
wg_sw_a>show ?
  clock          Display the system clock
  version        System hardware and software status
  flash:         Display information about flash: file system
  flowcontrol    Show flow control information
  users          Display information about terminal lines
```

Dodatkowo urządzenie posiada wbudowany bufor ostatnio wprowadzonych poleceń chcąc wyświetlić wprowadzone komendy należy wydać polecenie **show history**.

Chcąc wyświetlić konfigurację przełącznika musimy zrozumieć, w jaki sposób urządzenie zarządza swoimi pamięciami (NVRAM, RAM). Przy starcie przełącznik wyszukuje plik konfiguracyjny, który domyślnie przechowywany jest w pamięci NVRAM. Jeżeli w NVRAM-ie została zapisana konfiguracja urządzenia, to nastąpi skopiowanie jej do pamięci RAM i w oparci o tą konfiguracje urządzenie będzie wykonywało określone procesy.

Kiedy przełącznik nie znajdzie w pamięci NVRAM pliku konfiguracyjnego, uruchomi się w trybie dialogu konfiguracyjnego. Gdzie za pomocą kliku pytań wykonujemy wstępną konfigurację urządzenia. Pamięć RAM nie tylko służy do składowania bieżącego pliku konfiguracyjnego, dodatkowo urządzenie rozpakowuje ISO do tej pamięci, przechowuje tablicę CAM, to w tej pamięci będą wykonywane złożone operacje.



Chcąc wyświetlić bieżącą używaną konfigurację na urządzeniu należy wydać polecenie **show runnig-config**, w tym przypadku zostanie wyświetlona konfiguracja przechowywana w pamięci RAM.

Natomiast chcąc sprawdzić z jakiej wyjściowej konfiguracji urządzenie się uruchomiło należy wydać polecenie **show startup-config**. Urządzenie sięga wtedy do pamięci NVRAM i wyświetla konfigurację.

Domyślnym miejscem składowania systemu operacyjnego w przełącznikach jest pamięć FLASH. Aby wyświetlić zawartość w/w pamięci należy użyć polecenia **show flash:**

```
DSW#sh flash

Directory of flash:/

    2  -rwx        1756   Mar 1 1993 01:02:27 +01:00  vlan.dat
    4  -rwx    10713279   Mar 1 1993 01:30:41 +01:00  c3560-advipservicesk9-mz.122-46.SE.bin

32514048 bytes total (21767680 bytes free)
```

11. Switche – konfiguracja

Konfigurację przełącznika należy rozpocząć od wprowadzenia polecenia **enable** w trybie użytkownika podstawowego. Zostaniemy przeniesieni w tryb globalnej konfiguracji i jest to punkt wyjściowy do dalszych prac. W tym miejscu należy wydać polecenie **configure terminal**, który informuje przełącznik, że chcemy pracować w trybie globalnej konfiguracji. Z tego poziomu możemy rozpocząć konfigurację określonych elementów naszego urządzenia np. adres IP, użytkowników, zdalny dostęp, interfejsy itp.

DSW#configure terminal

DSW(config)#

Kolejnym krokiem, który musimy wykonać to określić, co dokładnie będzie przez nas konfigurowane. Chcąc skonfigurować określony interfejs przełącznika należy wydać następujące polecenia:

DSW(config)#interface fa0/1

DSW(config-if)#

interface fa0/1 wskazuje, że chcemy skonfigurować pierwszy port przełącznika. W wyniku wpisania powyższego polecenia, zostaniemy przeniesieni w tryb konfiguracji określonego portu. Konfigurację urządzenia można odnieść do czynności rozpakowywania prezentu: gdzie otwieramy pierwsze pudełko i trafiamy na kolejny, które po rozpakowaniu ujawnia kolejne i tak aż dotrzemy do fizycznego przedmiotu.

Każde urządzenie po uruchomieniu się pierwszy raz, domyślnie przedstawi się nazwą np. Switch, aby mieć kontrolę, jakie urządzenie konfigurujemy należy nadać mu określoną nazwę. W tym celu w trybie konfiguracji wydajemy polecenie **hostname** i wprowadzamy nazwę identyfikującą urządzenie.

Switch(config)#

Switch(config)#hostname DSW

DSW(config)#

Na przełączniku istnieje możliwość skonfigurowania bramy domyślnej. Będzie ona używana przez Switch, kiedy dane zmierzają poza sieć, w której pracuje przełącznik. W tym celu należy wydać poniższe polecenie:

DSW(config)#ip default-gateway [IP address of default gateway]

DSW(config)#ip default-gateway 10.1.1.1

Przełączniki to urządzenia, które pracują w warstwie łącza danych modelu OSI. W tej warstwie posługujemy się fizycznymi adresami mac urządzeń. Jednak chcąc mieć możliwość zdalnego logowania się na przełącznik wymagany jest adres IP (L3).

Adresy nie są przypisywane bezpośrednio na fizycznym interfejsie przełącznika, lecz na wirtualny interfejs nazywany **interface vlan1**. Nadanie adresu IP wykonujemy w trybie globalnej konfiguracji od wydania poniższych poleceń:

DSW(config)#interface vlan 1

DSW(config-if)#ip address 10.5.5.11 255.255.255.0

DSW(config-if)#no shutdown

Polecenie **no shutdown** zostało wydane celowo, ponieważ wszystkie interfejsy na urządzeniach, które pracują w warstwie trzeciej, a na których możemy nadać adres IP są domyślnie wyłączone. Aby interfejs stał się aktywny należy wydać powyższe polecenie.

Po zakończeniu konfiguracji należy ją zapisać, w tym celu wydajemy poniższe polecenia określając źródło skąd będzie kopiowana konfiguracja (wszelkie zmiany przechowywane są w pamięci RAM) oraz cel gdzie będzie ona zapisana (pamięć NVRAM).

DSW#copy running-config startup-config

Destination filename [startup-config]?

Building configuration…

DSW#

Chcąc wyświetlić informacje na temat konfiguracji urządzenia, stanu interfejsów, platform sprzętowej i wielu innych parametrów należy posługiwać się poleceniem **show** dopełniając go odpowiednią pod komendą.

show version – wyświetla informacje dotyczące platformy sprzętowej, wersji oprogramowania, liczby interfejsów, czasu pracy urządzenia.

show running-config – wyświetla informacje na temat bieżącej konfiguracji (RAM).

show interfaces – wyświetla stan i statystki wszystkich interfejsów dostępnych w urządzeniu

show clock – wyświetla informację na temat czasu skonfigurowanego na urządzeniu.

show users – wyświetla listę zalogowanych na danym urządzeniu użytkowników.

show cdp neighnors – wyświetla listę urządzeń bezpośrednio podłączonych do naszego urządzenia.

Przejście na tryb uprzywilejowany wymaga podania polecenia **enable**, aby ograniczyć dostęp do tego trybu należy go zabezpieczyć tworząc hasło. W tym celu w trybie konfiguracji wydajemy polecenie:

DSW(config)#enable secret { hasło które będziemy używać }

Polecenie **enable secret** powoduje że w prowadzone hasło podlega procesowi szyfrowania. W efekcie hasło nie jest wyświetlane jawnym tekstem, a dodatkowo użyta funkcja szyfrująca ma uniemożliwić odszyfrowanie hasła.

Każda próba przejścia w tryb uprzywilejowany od tego momentu będzie wymagała podania hasła.

DSW>enable

Password: { w tym miejscu podaje hasło będzie ono nie widoczne }

DSW#

Chcąc usunąć całkowicie konfigurację z urządzenia należy posłużyć się poleceniem **erase startup-config,** w wyniku użycia tego polecenia zostanie skasowana zawartość pamięci NVRAM. Po ponownym uruchomieniu się, urządzenia przejdzie w tryb konfiguracji dialogowej. Ponowne uruchomienie się urządzenia możemy wykonać używając polecenia **reload**.

12. Ćwiczenia #2 Switche

Przegląd poleceń wymaganych do zrealizowania zadań:

Polecenia	Opis
enable	Przejście w tryb uprzywilejowany
configure-terminal	Przejście w tryb konfiguracji
enable secret	Szyfrowanie hasła..
exit lub Ctrl + Z	Wyjście z określonego trybu pracy
end	Przejście do trybu uprzywilejowanego w czasie konfiguracji.
Hostname ***nazwa urządzenia***	Nadanie nazwy urządzeniu
interface vlan1	Przejście do trybu konfiguracji interfejsu vlan1
ip address	Nadanie adresu IP na interfejsie vlan1
ip default-gateway *ip adres*	Skonfigurowanie adresu bramy domyślnej dla przełącznika
show interface vlan 1	Wyświetla szczegółowe informacje o statusie interfejsu vlan1
copy running-config startup-config	Kopiowanie konfiguracji
show version	Wyświetla informacje na temat platformy sprzętowej

12.1. Zadanie 1: Wstępna konfiguracja przełącznika

1) Utwórz nazwę dla przełącznika **wg_sw_X** – gdzie X odpowiada grupie, w której pracujesz.
2) Zabezpiecz dostęp do trybu uprzywilejowanego używając hasła **cisco.** Hasło ma być szyfrowane.
3) Skonfiguruj adres IP na **interfejsie vlan 1** używając adresu **10.1.1.X /24** – gdzie **X** dopowiada poniższej tabelce.

Grupa	Adres IP
A	10.1.1.10 /24
B	10.1.1.20 /24
C	10.1.1.30 /24
D	10.1.1.40 /24
E	10.1.1.50 /24
F	10.1.1.60 /24

Skonfiguruj adres bramy domyślnej – 10.1.1.3

4) Sprawdź komunikację z grupowego przełącznika z bramą domyślną.
5) Sprawdź komunikację z grupowego przełącznika do pozostałych Switchy w laboratorium.
6) Sprawdź, z jakiej platformy sprzętowej korzystasz i jaki używany jest IOS i zapisz poniżej w tabelce:

Platforma sprzętowa	System Operacyjny

7) Wyświetl konfigurację urządzenia
8) Zapisz konfiguracje w pamięci NVRAM.

13. Switche – zdalny dostęp

Zdalny dostęp to wygodna forma komunikowania się z urządzeniami rozproszonymi w infrastrukturze, realizowana poprzez dwa protokoły Telnet oraz SSH.

Telnet – jest to protokół komunikacyjny używany w sieciach komputerowych. Jednak ten protokół przesyła dane otwarty tekstem, co dyskryminuje go w dzisiejszych czas ze względu na stosowane polityki bezpieczeństwa.

SSH – (secure Shell) – jest to następca protokołu telnet wykorzystywany do komunikacji zdalnej z urządzeniami. SSH różni się od Telnetu tym, że transfer wszelkich danych jest zaszyfrowany. Najczęściej stosowany sposób szyfrowania to AES chodź wspiera również i DES

Chcąc uruchomić na przełączniku możliwość zdalnego logowania musimy zrealizować poniższe korki:

1) Zdefiniowanie użytkownika

DSW(config)#username admin password cisco

2) Stworzenie nazwy domeny.

DSW(config)#ip domain-name dsw.local

3) Wygenerowanie klucza RSA i jego rozmiar.

DSW(config)#crypto key generate rsa

The name for the keys will be: DSW.dsw.local

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes

How many bits in the modulus [512]: **1024**

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

4) Określenia, na jakich linia vty będzie realizowana zdalna komunikacja telnet / ssh

DSW(config)#line vty 0 4

5) Skonfigurować logowanie w oparciu o lokalnego użytkownika.

DSW(config-line)#login local

DSW(config-line)#transport input ssh telnet

14. Switche – bezpieczeństwo

W życiu codziennym właściciele posesji umieszczają tabliczkę z informacją, że teren posesji pilnuje pies i wchodzimy tam na własne ryzyko. Taki napis nie koniecznie zabezpieczy dom przed włamaniem jednak, może odstraszyć potencjalnych intruzów. W przypadku urządzeń sieciowych istnieje możliwość stworzenia podobnej tabliczki informacyjnej nazywanej **banner login**.

Ma ona na celu jedynie informować osobę próbującą się zalogować na urządzenie, do kogo należy ten sprzęt i jakie są konsekwencje logowania osób nieautoryzowanych. Aby utworzyć banner login należy w trybie globalnej konfiguracji wprowadzić polecenie banner login, a następnie wprowadzić znak specjalny, który wskazuje na początek wprowadzanej informacji. Kiedy tekst został wprowadzony należy użyć znaku specjalnego.

DSW(config)#banner login #

```
++++++++++++++++++++++++++++++++++++++++++++++++++
+                                                +
+                        !!! Uwaga !!!           +
+                                                +
+ Dostep do urzadzenia tylko dla autoryzowanych uzytkownikow   +
+                                                +
++++++++++++++++++++++++++++++++++++++++++++++++++

#
```

Jednym ze sposobów zabezpieczenia przełączników w infrastrukturze przed podłączeniem się osób niepowołanych jest użycie mechanizmu **port-security.** Port, na którym będzie używany port-security musi być portem dostępowym (**switchport mode access)**

Idea tego rozwiązania jest następująca: administrator definiuje, jaka ilość maksymalna mac adresów jest dozwolona na określonym interfejsie. Dodatkowo możemy zdefiniować, jakie to mogą być adresy urządzeń, którym zezwalamy, aby mogły komunikować się z naszą infrastrukturą.

Istotnym elementem port-security jest zachowanie się portu po naruszeniu restrykcji. Port-security posiada trzy możliwe warianty zachowań:

protect – po osiągnięciu limitu źródłowych adresów MAC, pozostałe ramki (z innymi adresami źródłowymi) są odrzucane

restrict – tak samo jak protect, ale wysyłany jest trap SNMP

shutdown – po osiągnięciu limitu źródłowych adresów MAC, port zostaje zamknięty (wymaga shut/no shut, aby ponownie został aktywowany)

Domyślnym zachowaniem port-security jest **shutdown** – takie zachowanie pozwala administratorowi ustalić, co było przyczyną wyłączenia portu i dodatkowo jak mac adres dokonał powyższego naruszenia.

Konfigurację należy rozpocząć od wydania w trybie konfiguracji interfejsu polecenia **port-security**, co skutkuje uruchomieniem tego procesu w obrębie interfejsu. W kolejnych krokach definiujemy liczbę mac adresów (domyślnie jest 1), następnie zdefiniować zachowanie port-security po naruszeniu restrykcji.

Dodatkowo istnieje możliwość skonfigurowania opcji „**sticky”.** Kiedy przełącznik uczy się określonych mac adresów możemy wymusić aby zostały one zapamiętane na stałe na określonym porcie. Należy pamiętać, że te wszystkie informacje są przechowywane w pamięci RAM. Dlatego jeśli mac adresy mają zostać na stałe przypisane do portu, należy zapisać konfigurację do pamięci NVRAM. Przykładowa konfiguracja portu fa0/10

DSW (config)#interface fa0/10

DSW (config-if)#switchport mode access

DSW (config-if)#switchport port-security

DSW (config-if)#switchport port-security maximum 1

DSW (config-if)#switchport port-security mac-address sticky

DSW (config-if)#switchport port-security violation shutdown

Chcąc weryfikować działanie port-security możemy posłużyć się poleceniami :

show port-security interface fa0/10

show port-security address

show port-security

DSW#show port-security interface fa0/10

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 20 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 1

Total MAC Addresses : 1

Configured MAC Addresses : 0

Sticky MAC Addresses : 0

Last Source Address : 001F.AD02.14C0

Security Violation Count : 0

DSW#sh port-security address

Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	001F.AD02.14C0	SecureConfigured	Fa0/10	-

Total Addresses in System (excluding one mac per port) : 0

Max Addresses limit in System (excluding one mac per port) : 1024

DSW#sh port-security

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Fa0/5	1	1	0	Shutdown

Total Addresses in System (excluding one mac per port) : 0

Max Addresses limit in System (excluding one mac per port) : 1024

Kolejną dobrą praktyką jaką należy stosować w przypadku zabezpieczania urządzeń sieciowych jest zakładanie haseł w obrębie wszystkich dostępnych metod logowania do urządzeń.

Zabezpieczenie portu konsoli:

DSW(config)#line console 0

DSW(config-line)#password cisco

DSW(config-line)#login

Zabezpieczenie linii vty:

DSW(config)#line vty 0 4

DSW(config-line)#login

DSW(config-line)#password cisco

Zabezpieczenie trybu enable:

DSW(config)#enable secret cisco

15. Ćwiczenie #3 Switche

Przegląd poleceń wymaganych do zrealizowania zadań:

Polecenia	Opis
banner login	Konfiguracja baneru informacyjnego na urządzeniu.
username [ ] password [ ]	Tworzenie lokalnego użytkownika oraz hasła.
enable secret	Szyfrowanie hasła.
crypto key generale rsa	Generowanie klucza RSA
ip domain-name	Tworzenie nazwy domeny na potrzeby generowania kluczy rsa
line console 0	Konfiguracja portu konsoli
ip ssh version	Konfiguracja ssh w określonej wersji 1 / 2
line vty 0 4	Konfiguracja liny terminalowych do sesje zdalnych
login / login local	Wymusza logowania / wymusza logowanie z użyciem użytkownika lokalnego
password	Polecenie do utworzenia hasła w obrębie linii konsoli / vty
show mac-address-table	Wyświetla adresy mac powiązane z określonymi poratami.
switchport mode access	Port staje się portem dostępowym
spannig-tree portfast	Wyłączenie protokołu STP na porcie.
switchport port-security	Uruchamia port-security na interfejsie
switchport port-security maximum [liczba]	Określenie dozwoloną ilości mac adresów na porcie.
switchport port-security violation [shutdown]	Definiuje zachowanie kiedy zostanie naruszona restrykcja dotycząca ilości adresów mac.
transport input telnet ssh	Określa jakie protokoły będę używane do komunikacji zdalnej
show interface	Wyświetla szczegółowe informacje o statusie oraz parametrach interfejsu
exit lub Ctrl + Z	Wyjście z określonego trybu pracy oraz rozłączenie sesji zdalnej

15.1. Zadanie 1: Zabezpieczenie dostępu do urządzenia.

1) Na przełączniku utwórz użytkownika **admin** z hasłem **cisco**
2) Zabezpiecz dostęp do linii konsoli hasłem **cisco,** wymagane jest logowanie**.**
3) Na przełączniku zabezpiecz dostęp do linii vty 0 4 hasłem **cisco.**
4) W obrębie linii vty 0 4 wymagaj logowania lokalnego.

15.2. Zadanie 2: Konfiguracja zdalnego dostępu.

1) Utwórz następującą nazwę domeny **wg_sw_X.local** – gdzie X oznacza numer grupy laboratoryjnej.
2) Wygeneruj klucze **RSA** o długość 1024 bitów.
3) Zezwól na używanie następujących protokołów zdalnego dostępu : **telnet / ssh**
4) Zapisz konfigurację**.**

15.3. Zadanie 3: Weryfikacja połączeń telnet / ssh.

1) Zaloguj się na urządzenie **wg_ro_X** – gdzie X oznacza numer grupy laboratoryjnej.
2) Nadaj adres IP, na interfejsie **fa0/0** według poniższej tabelki

Grupa	Adres IP
A	10.1.1.11 /24
B	10.1.1.21 /24
C	10.1.1.31 /24
D	10.1.1.41 /24
E	10.1.1.51 /24
F	10.1.1.61 /24

3) Sprawdź komunikację warstwie trzeciej pomiędzy urządzeniami.
4) Wykonaj test połączenia: telnet
5) Wykonaj test połączenia: ssh
6) Zapisz konfigurację na przełączniku.

15.4. Zadanie 4: Konfiguracja port-security.

1) Zaloguj się na urządzenie **wg_ro_X** – gdzie X oznacza numer grupy laboratoryjnej.
2) Sprawdź jaki mac adres został przypisany do interfejsu f**a0/0**
3) Zaloguj się na urządzenie **wg_sw_X** – gdzie X oznacza numer grupy laboratoryjnej
4) Port Fa0/12 skonfiguruj jako port dostępowy (**switchport mode access)** oraz wydaj dodatkowe polecenie: **spannig-tree portfast**
5) Uruchom **port-security** na porcie **Fa0/12** według poniższych wytycznych
   a) Akceptowalna ilość mac adresów to 1.
   b) Adres mac ma być „przyklejony" do portu.
   c) Po naruszeniu restrykcji port ma być automatycznie wyłączony.
6) Użyj polecenia ping pomiędzy urządzeniami, a następnie sprawdź jakiego mac adresu nauczył się przełącznik.
7) Na routerze **wg_ro_X** – gdzie **X** oznacza numer grupy laboratoryjnej dokonaj modyfikacji mac adresu na porcie **Fa0/0**, zmieniając ostatnie dwie wartość w adresie. W tym celu w trybie konfiguracji portu F0/0 wydaj polecenie: **mac-address** i wprowadź nowy adres mac.
8) Ponownie użyj polecenia ping z routera do przełącznika.
9) Sprawdź zachowanie port-security na przełączniku
10) Na routerze przywróci pierwotny mac adres.
11) Na przełączniku w obrębie konfiguracji interfejsu fa0/2 wydaj polecenie **shoutdown** a następnie **no shutdown**.
12) Ponownie użyj polecenia ping z routera do przełącznika sprawdzając komunikację pomiędzy nimi.
13) Zapisz konfigurację na przełączniku.

16. Switche – VLANy

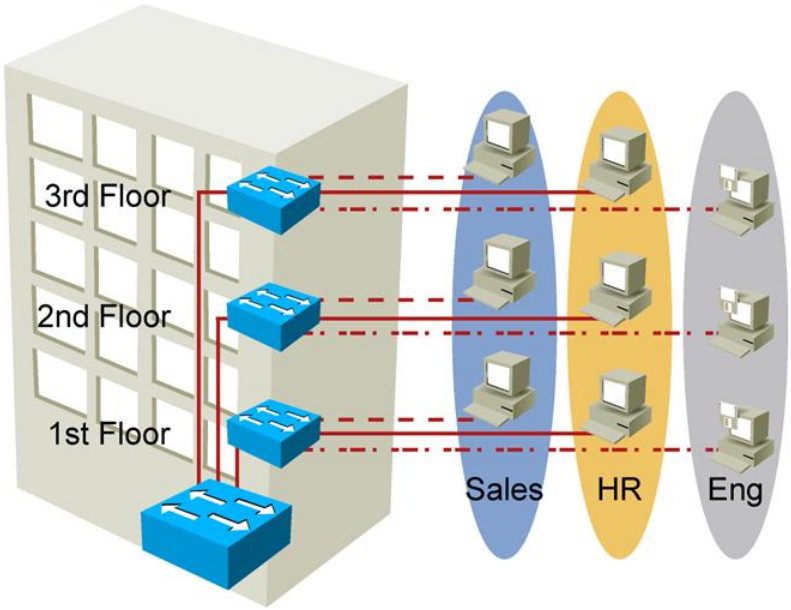
Sieci, w których używamy tylko jednego adresu sieci dla wszystkich urządzeń nazywam sieciami płaskimi. Tak budowana sieć nastręcza sporej ilości problemów w zarządzaniu nią, a wynika to z następujących faktów:

Rozgłoszenia – ten typ ruchu zalewa cała infrastrukturę sieciowa i jest przenoszony natychmiast pomiędzy przełącznikami. W sieciach gdzie mamy duże ilości urządzeń ten typ ruchu będzie powodował spore zamieszanie i zmniejszy znacznie wydajność sieci.

Multicast-y - ten typ ruchu podobnie jak rozgłoszenia może powodować sporą ilość problemów w płaskiej topologii.

Brak polityk bezpieczeństwa – kiedy urządzenia pracują w tej samej sieci zabezpieczenie dostępu do określonych jest praktycznie niemożliwe. Ponieważ komunikacja jest realizowana na poziomie warstwy drugiej, czyli w oparciu o adresy mac.

Jedynym optymalnym rozwiązaniem tego problemu, jest implementowanie vlan-ów. To nic innego jak podzielenie dużej infrastruktury na klika mniejszych sieci (podsieci), w celu łatwiejszego zarządzania środowiskiem. Dodatkowo VLAN-y niwelują wymienione wcześniej problemy. Dla każdego VLAN-u wymagane jest nadanie unikatowego i niepowtarzalnego adresu sieci.



Zaletami implementowania VLAN-ów w sieciach jest:

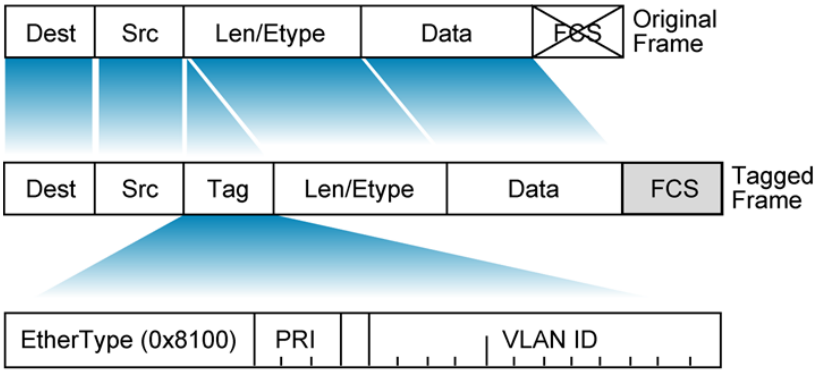
Segmentacja – podzielenie dużej infrastruktury na mniejsze części.

Elastyczność – tworzone VLAN-y grupują użytkowników w obrębie określonego piętra, działów, funkcji którą pełnią w firmie.

Bezpieczeństwo - implementując VLAN-y w infrastrukturze administrator posiada pełną kontrolę nad komunikacją pomiędzy urządzeniami. Administrator ma możliwość selektywnego określenia, jakie urządzenia mogą się między sobą komunikować i za pośrednictwem jakich protokołów.

Ograniczenie rozgłoszeni – VLANy dzielą jedna wielką domenę rozgłoszeniową, (która występuje w płaskiej topologii) na wiele mniejszych. W efekcie rozgłoszenia pomiędzy VLAN-nami nie będą się przenosiły

Kiedy w sieciach pojawiają się VLAN-y następuje zmiana struktury ramki Ethernetowej. Zostaje dodane dodatkowe pole nazywane TAG, w którym zostaje zapisana informacja, z jakiego VLAN-u pochodzi określona ramka.



Chcąc utworzyć VLAN-y na przełącznikach należy rozważyć poniższe kwestie:

1) Ustalić ilość VLAN-ów i określić unikatowe identyfikatory dla każdego z VLAN-ów
2) Przypisać nazwy dla każdego VLAN-u
3) Określić, które porty będą przypisane do wcześniej utworzonych VLAN-ów.
4) Sprawdzić konfigurację.

Tworzenie VLAN-ów wykonujemy używając poniższych komend:

DSW# configure terminal

DSW(config)# vlan 10

DSW(config-vlan)# name Marketing
DSW(config-vlan)# vlan 20

DSW(config-vlan)# name Handlowy

Weryfikację utworzonych VLAN-ów wykonujemy używając polecenia **show vlan [brief | id *vlan-id* || name *vlan-name*]**

SwitchX# show vlan id 10

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

10 Marketing active Fa0/21, Fa0/22

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2

---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

10 enet 100002 1500 - - - - - 0 0

Przypisanie określonego portu lub grupy portów wykonujemy używając poniższych poleceń:

DSW# configure terminal

DSW(config)# interface fastethernet 0/21

DSW(config-if)# switchport access vlan *10*

Jeżeli pojawia się potrzeba przypisania większej ilości portów do określonego VLAN-u należy użyć polecenia **range** , określić typ interfejsu, a następnie podać zakres portów.

DSW(config)# interface range fastethernet fa0/20 – 23

DSW# show vlan

VLAN Name Status Ports

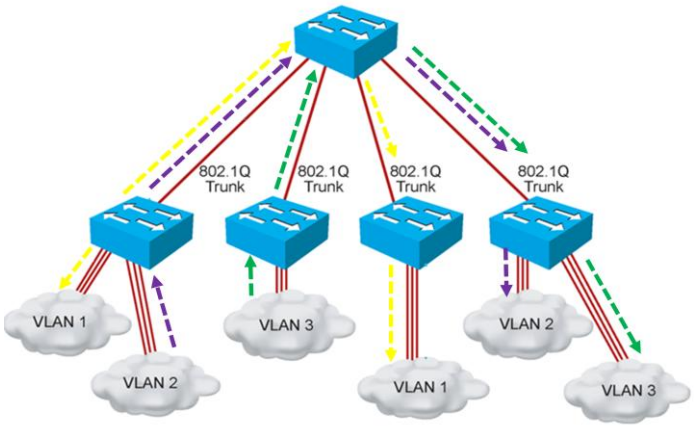
---- -------------------------------- --------- -------------------

1 default active Fa0/1

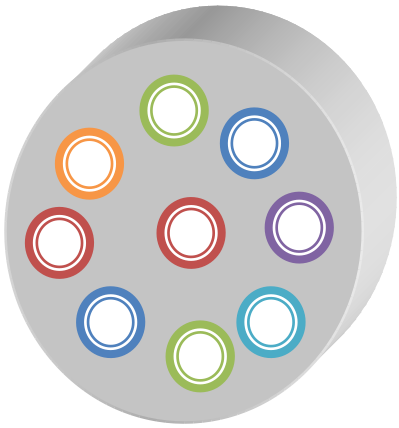
2 Marketing active Fa0/20, Fa0/21, Fa0/23

17. Switche – Trunk

Kiedy na przełącznikach zostały skonfigurowane VLAN-y trzeba utworzyć specjalne połączenie między nimi. Za pomocą tego linku przełączniki będą przesyłać między sobą informacje pochodzące z różnych VLAN-ów. Do tego celu używa się linki tranzytowe nazywane **TRUNK**-iem. TRUNK odpowiada za przesyłanie znakowanych ramek pochodzących z różnych VLAN-ów.



Rysunek poniżej obrazuje przekrój linku TRUNK zawierający ramki znakowane pochodzące z różnych VLAN-ów.



Jeśli trzeba skonfigurować port tak, aby pracował jako TRUNK, należy przejść do trybu konfiguracji określonego portu, a następnie wydać poniższe polecenie.

DSW(config-if)#switchport mode trunk

Wyświetlenie informacji na temat portów pracujących jako TRUNK, wydaje polecenie:

DSW#show interfaces trunk

18. Ćwiczenia #4 Switche

Przegląd poleceń wymaganych do zrealizowania zadań:

Polecenia	Opis
switchport mode trunk	Port przechodzi w tryb TRUNK.
switchport access vlan[ID]	Przypisanie portu do określonego VLAN-u.
vlan [ID VLAN]	Tworzenie VLANU o określonym identyfikatorze
name [vlan-name]	Przypisanie nazywy dla VLAN-u
vtp mode transparent	Przełącznik pracuje w trybie transparent i nie aktualizuje się ogłoszeniami z protokołu VTP
show vlan brief	Wyświetla informacje na temat utworzonych VLAN-ów, oraz przypisanych portów do określonych VLAN-ów.
show interfaces trunk	Wyświetla informacje o portach pracujących jako TRUNK.

18.1. Zadanie 1: Konfiguracja linków TRUNK .

1) Zaloguj się na urządzenie **wg_sw_X** – gdzie X oznacza numer grupy laboratoryjnej.
2) Skonfiguruj interfejs **Fa0/1 – 2** aby pracowały jako **TRUNK**
3) Sprawdź informacje o portach TRUNK.
4) Sprawdź poleceniem ping kontakt z urządzeniem **core_ro** używając adresu 10.1.1.3.
5) Zapisz konfigurację na przełączniku.

18.2. Zadanie 2: Konfiguracja VLAN-ów .

Grupa	Numer VLAN-u	Core Router	Adres dla Fa0/0 na wg_ro_X
A	**20**	**10.2.2.3**	**10.2.2.10 /24**
B	**30**	**10.3.3.3**	**10.3.3.10 /24**
C	**40**	**10.4.4.3**	**10.4.4.10 /24**
D	**50**	**10.5.5.3**	**10.5.5.10 /24**
E	**60**	**10.6.6.3**	**10.6.6.10 /24**

F	**70**	**10.7.7.3**	**10.7.7.10 /24**

1) Zaloguj się na urządzenie **wg_sw_X** – gdzie **X** oznacza numer grupy laboratoryjnej.
2) W trybie globalnej konfiguracji wydaj polecenie **vtp mode transparent**
3) Utwórz odpowiedni VLAN dla swojej grupy, korzystając z powyżej tabelki.
4) Zweryfikuj czy VLAN został utworzony w obrębie przełącznika
5) Przypisz port **Fa0/12** do VLAN, który został utworzony na przełączniku.
6) Zweryfikuj czy port został przypisany do odpowiedniego VLAN-u.
7) Zaloguj się na urządzenie **wg_ro_X** – gdzie X oznacza numer grupy laboratoryjnej.
8) Na routerze, skonfiguruj adres IP na interfejs **Fa0/0** posługując się tabelą.
9) Użyj polecenie ping na wg_ro_X , w celu sprawdzenia czy posiadasz kontakt routerem core_ro.
   (wykorzystaj odpowiedni adres z powyżej tabeli).
10) Na przełączniku wg_sw_X sprawdź adres IP nadany na interfejsie VLAN1
11) Na routerze wg_ro_X , użyj polecenia ping wykorzystując adres IP przełącznika.
    Ping powinien nie zakończyć się powodzeniem. Czemu ?
12) Rozwiąż problem braku komunikacji.
13) Zapisz konfigurację.

19. Routery – podstawy

Routery to urządzenia, które operują w warstwie sieciowej modelu OSI. Wyposażone są one w takie same komponenty, jak każdy komputer klasy PC (płyta główna, pamięć RAM, pamięć flash – (odpowiednik HDD w PC), procesor.) Routery dysponują przynajmniej dwoma złączami Ethernet-owymi, dodatkowo mogą posiadać klika slotów na karty umożliwiające używanie różnych technologii. Do zarządzania routerami będziemy używali portu konsoli, tak jak w przypadku przełączników.

Nadrzędną rolą jaką pełnią routery w sieciach jest przesyłanie pakietów do docelowych sieci. Proces ten jest realizowany w oparciu o tablicę routingu. Na podstawie wpisów w tablicy routingu, router wie jak osiągać docelowe sieci (za pomocą jakiego fizycznego interfejsu). Kiedy w sieci zostanie wykryta zmiana tj. dodanie nowej podsieci lub brak możliwości osiągnięcia podsieci, taka informacja zostanie odnotowana przez router i opatrzona odpowiednim wpisem w tablicy routingu.

Wpisy w tablicy routingu mogą pojawić się w oparciu o poniższe informacje:

1) Urządzenie rozpoznaje, określony swój interfejs, jego stan (operatywny) i nadany adres IP. Na podstawie tych informacji pojawia się wpis w tablicy routingu opatrzony literą **„C" – connected**.
2) Wpisy statyczne tworzone przez administratora, gdzie została z góry narzucona trasa dostarczania pakietów do docelowej sieci. W tablicy routingu takie trasy opatrywane są literą **„S" – static**.
3) Routery za pomocą dynamicznych protokołów routingu wymieniają się informacjami o dostępnych sieciach. Spośród wszystkich proponowanych tras wiodących do celu router wybiera tylko jedną, która jest najbardziej optymalna. W tablicy routingu takie trasy opatrywane są litera **„R" – RIP, „E" – EIGRP, „O" – OSPF, „B" - BGP**.
4) Trasy domyślne, pełnią rolę „koła ratunkowego", kiedy router nie posiada informacji jak osiągnąć docelowe sieci, wysyła zapytanie do routera znajdującego się np. u operatora (czyli wyżej w hierarchii). Dzięki takiemu podejściu routery szukają kolejnych urządzeń, które mogą pomóc znaleźć trasę do docelowej sieci.

20. Routery – Routing statyczny / dynamiczny

Routing to proces wyznaczania tras, prowadzących do docelowych sieci. Za pomocą tras mogą być przesyłane dane. Cały ten proces jest realizowany w oparciu o warstwę sieciową, gdzie wykorzystywana jest informacja o źródłowym i docelowym adresie IP. Routery mogą wykorzystywać dwie dostępne metody, w celu przesyłania pakietów w sieci:

a) **Routing statyczny**.

b) **Routing dynamiczny**.

Routing statyczny – jest tworzony przez administratora, który sam decyduje w jaki sposób pakiety będą docierały do docelowej sieci. Administrator definiuje kolejne skoki na drodze pakietu. Takie rozwiązanie nie nadaje się do dużych infrastruktur, ponieważ jeżeli w sieci pojawi się awaria jednego z urządzeń pośredniczących w przesyle danych, administrator musi przekonfigurować pozostałe urządzenia tak aby pakiety trafiały w odpowiednie miejsce.

Routing dynamiczny – możemy przyjąć, że jest to „**język**" w jakim rozmawiają ze sobą routery. Za jego pośrednictwem potrafią się wymieniać informacjami o sieciach. Jest to zalecane rozwiązanie w przypadku dużych sieci. W przypadku awarii routery informują się że dana siec jest nieosiągalna i starają się wyszukać zapasowe trasy do określonej sieci. W przypadku kiedy taka trasa jest dostępna pojawia się ona w tablicy routing routera.

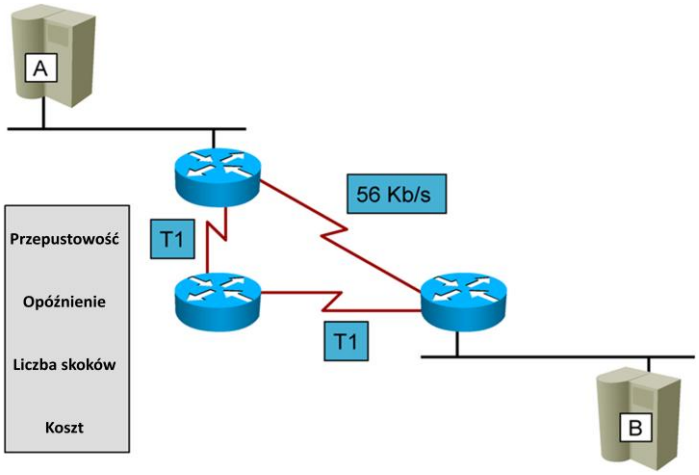
Żeby protokoły routing mogły się ze sobą komunikować, wymagany jest odpowiedni protokół warstwy sieciowej. W dzisiejszych sieciach takim protokołem jest IP.

21. Routery – Metryka

W sieciach może pracować klika dynamicznych protokołów routingu, takie jak RIP, EIGRP, OSPF, IS-IS. Pomiędzy routerami następuje wymiana informacji o dostępnych sieciach. Każdy router może otrzymać klika propozycji prowadzących do docelowej sieci. Jednak musi podjąć decyzję, która z tych ofert będzie najlepsza. Router zanim podejmie ostateczną decyzję, którą trasę umieścić w tablicy routingu, do każdej oferty przypisze odpowiednią wartość liczbową nazywana metryką. Metryka jest to wartość liczbowa od 0 – 255, i jest ona tworzona w oparciu o inne parametry przez każdy protokół. Takimi czynnikami decydującymi o metryce mogą być: przepustowość linków , opóźnienie pojawiające się na wszystkich linkach wiodących do docelowej sieci, liczba skoków oraz koszt. W przypadku kosztu nie mówimy tu o aspektach finansowych, a

jedynie wartości liczbowej, która wynika ze wzoru **Koszt = 100Mb/s / przepustowość fizycznego linku**.

Metryka wyliczana w oparciu o **liczbę skoków** jest nie optymalna ponieważ nie bada przepustowości czy opóźnień linku / linków, które wiodą do docelowej sieci, a jedynie liczbę skoków. Poniższy przykład pokazuje słabą stronę tego rozwiązania.



Metryka wyliczana w oparciu o **koszt**, skupia się na przepustowości każdego linku prowadzącego do docelowej sieci i przypisaniu mu odpowiedniej wartości liczbowej. Znając przepustowość każdego odcinka do docelowej sieci, wyliczany jest koszt dla pojedynczego linku na podstawie wzoru : **Koszt = 100Mb/s / przepustowość fizycznego linku** . Sumując te wartości router poznaje całkowity koszt do docelowej sieci.

Metryka wyliczana w oparciu o **przepustowość i opóźnienie** jest najbardziej optymalną metodą. Wynika to z faktu, iż analizowana jest przepustowość, która jest istotna z punktu widzenia transferu danych, ale badany jest drugi parametr: **opóźnienie.** Może ono znacząco wpływać na dostarczanie danych. Suma wszystkich opóźnień oraz aspekt przepustowość na wszystkich odcinkach do docelowej sieci pozwala routerowi wybrać najbardziej optymalna trasę. I umieścić ją w tablicy routingu.

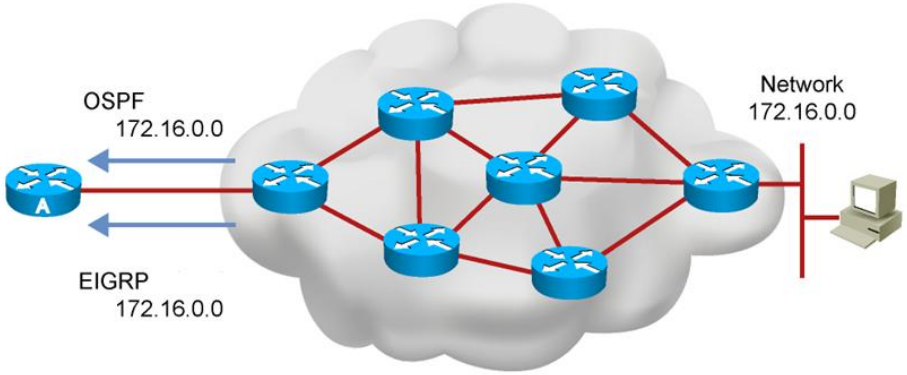
22. Routery – Dystans Administracyjny

Na routerach Cisco możemy uruchomic klika prokołów rotuingu jednocześnie np. RIP, EIGRP, OSPF, IS-IS, BGP, MPLS. W czasie ich pracy routery będą się wymieniały informacjami o sieciach, wykorzystując odpowiedni algorytm ustalą najniższa metrykę, a trasa z najmniejszą wartością metryki trafi do tablicy routingu. Jednak routery muszą wiedzieć, który z protokołów (**źródło informacji**) jest najbardziej godnym zaufania aby go używać.

W tym celu stworzono pojęcie dystansu administracyjnego (**AD** - **Administrative Distance**). Jest to wartość liczbowa od 0 do 255, która wskazuje czy źródło z którego pochodzi informacja jest godne zaufania. Im niższa wartość dystansu administracyjnego tym źródło jest traktowane jako zaufane.

Dystans administracyjny dla określonych typów tras:	
sieci bezpośrednio podłączone	**0**
trasa statyczna, wprowadzona przez administratora	**1**
trasa dynamiczna, protokół eBGP	**20**
trasa dynamiczna, protokół EIGRP	**90**
trasa dynamiczna, protokół OSPF	**110**
trasa dynamiczna, protokół IS-IS	**115**
trasa dynamiczna, protokół RIP	**120**
trasa dynamiczna, zewnętrzna trasa protokół EIGRP	**170**

Poniższy rysunek przedstawia sytuację kiedy do Routera A docierają ogłoszenia z dwóch różnych protokołów routingu OSPF i EIGRP (źródeł). W oparciu o wartość dystansu administracyjnego router może podjąć decyzję jaki protokół jest bardziej zaufanym źródłem informacji.

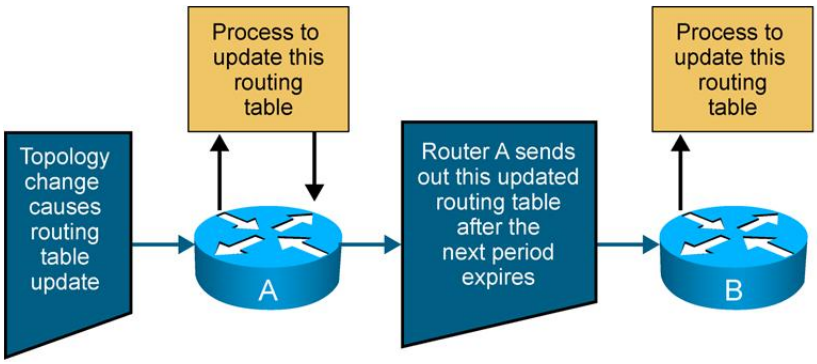


23. Routery – Tablica routingu

Routery podejmują decyzje w jaki sposób przesyłać pakiety do docelowych sieci, w oparciu o wpisy w tablicy routingu. Tablice routingu możemy potraktować jako rozkład odlotów na lotnisku, gdzie zawarte są informacje jak dotrzeć do określonego miejsca na świecie. Co jakiś czas taka tablica jest uzupełniana kolejnymi nowymi informacja. W przypadku routerów występuje identyczne zjawisko.

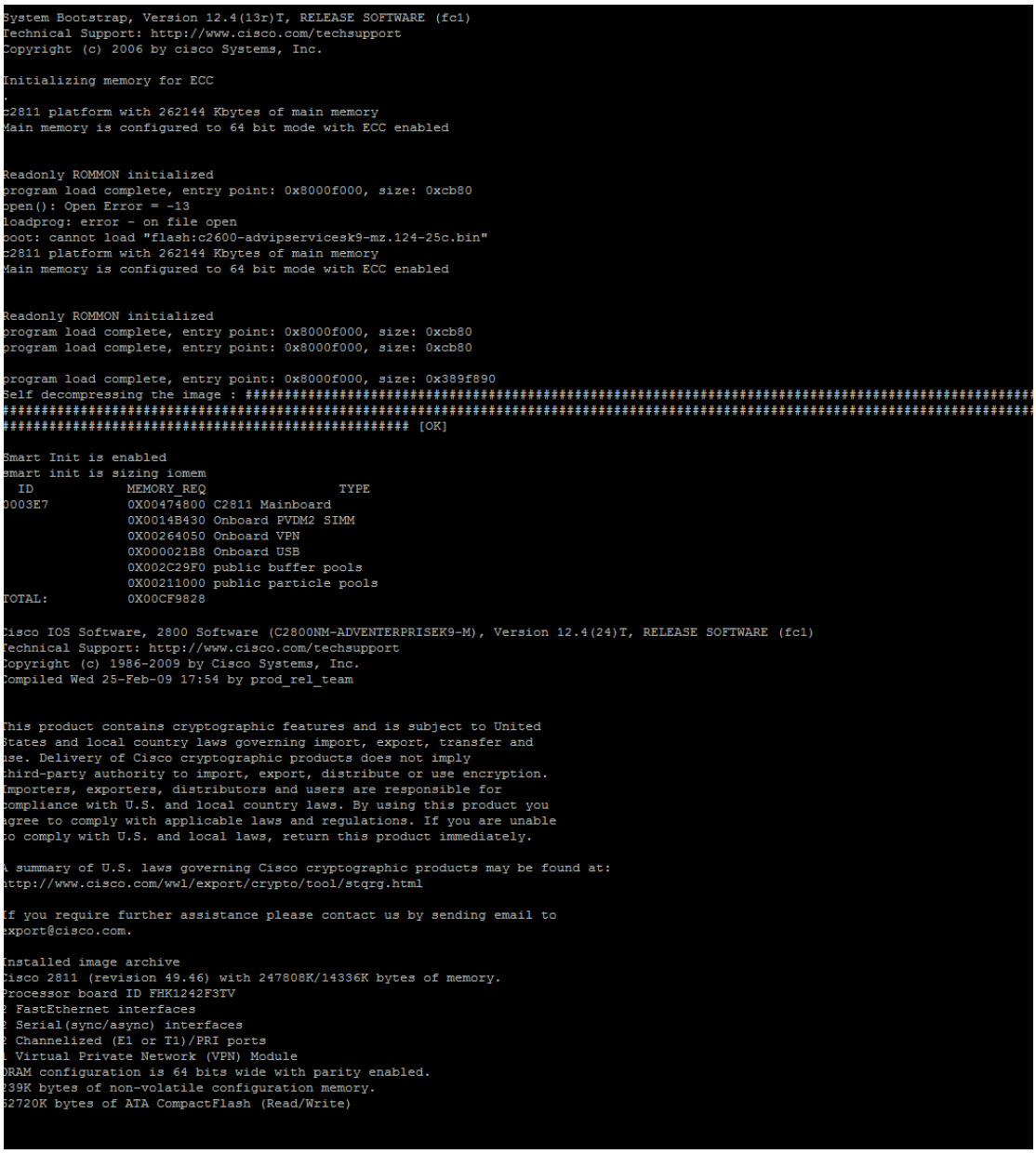
Kiedy używamy dynamicznych protokołów routingu, urządzenia wysyłają między sobą ogłoszenia. W ogłoszeniu przenosi się informacja o sieciach, o których wiedzą routery. Ten proces jest bardzo istotny z punktu widzenia przesyłania pakietów do docelowych sieci, pozwala ustalić optymalne trasy do określonych sieci.

Urządzenie po otrzymaniu ogłoszenia, rozpoczyna jego analizę. Routery porównują lokalną tablicę routingu z otrzymanym ogłoszeniem. Jeżeli ogłoszenie przenosi informacje o sieciach, o których już wie router, a metryki do tych sieci są niższe, router aktualizuje swoją tablicę routingu. Kiedy w ogłoszeniu trasy posiadają taką samą metrykę lub wyższą niż tą którą router posiada w tablicy routingu, nie następuje zaktualizowanie tablicy routing.



24. Routery – Uruchomienie

Zanim uruchomimy router musimy podłączyć kabel konsolowy do gniazda konsolowego, które jest umieszone w zależności albo na frontowym bądź tylnim panelu urządzenia. Dodatkowo wymagane jest uruchomienie aplikacji hyperterminal lub putty, za pomocą której będzie realizowana komunikacja znakowa z routerem. Kabel konsolowy jest z jednej strony zaterminowany złączem RJ-45, a z drugiej RS232. Po zasileniu urządzenia prądem należy uruchomić urządzenia za pomocą przycisku na zasilaczu. Następnie w oknie konsoli możemy zaobserwować jak przebiega procedura startu urządzenia.



Proces uruchomienia się routerów jest bardzo zbliżony do tego jaki towarzyszy uruchomieniu każdego komputera. W pierwsze fazie jest realizowany POST w czasie którego sprawdzane jest hardware. Kiedy testy zakończą się pomyślnie urządzane zaczyna wyszukiwać miejsc przechowywania system IOS, na ogół będzie to pamięć FLASH odpowiednik HDD w PC. System jest rozpakowywany do pamięci RAM, ostatnią czynnością która jest wykonywana to próba zlokalizowania i załadowania pliku konfiguracyjnego. Domyślnie jest on przechowywany w pamięci NVRAM. Po wykonaniu powyższych kroków router jest gotowy do pracy.

Urządzenia Cisco wyposażone są w system operacyjny nazywany IOS-em. Służy on do zarządzania procesami, które są wykonywane na przełącznikach czy routerach. Jest to system używający linii poleceń (CLI) za pomocą, której możemy wprowadzać odpowiednie komendy. Wszystkie wprowadzane polecenia należy zatwierdzać przy użyciu klawisza **ENTER**. Użytkownicy mogą przeklejać gotową konfigurację z plików tekstowych bezpośrednio w okno konsoli.

Jak każdy system operacyjny tak i IOS posiada dwa tryby pracy tzw. (EXEC MODE), **użytkownika podstawowego** oraz **użytkownika uprzywilejowanego**.

W trybie **użytkownika podstawowego**, urządzenie w linii wiersza poleceń wyświetli nazwe urządzenia (tj. hostname), za którą pojawi się znak większości „**>**” np. **Router>**. W tym trybie nie mamy prawa wykonywać konfiguracji routera, dysponujemy ograniczoną ilością dostępnych komend.

W trybie **użytkownika uprzywilejowanego,** urządzenie w linii wiersza poleceń wyświetli nazwę urządzenia (tj. hostname), za którą pojawi się znak większości „**#**” np. **Router#.** Chcąc pracować w trybie uprzywilejowanym na urządzeniu, w trybie zwykłego użytkownika należy wydać polecenie „**enable**” i zatwierdzić klawiszem ENTER.

Router>enable

Router#

W tym trybie pracy posiadamy pełną kontrolę nad urządzeniem, dysponując wszystkimi dostępnymi poleceniami.

System IOS dysponuje rozbudowanym system pomoc, dzięki któremu możemy poprawnie wprowadzać komendy. Mamy możliwość korzystania z dwóch trybów pomocy: **Word help** - wprowadzamy jedynie pierwszą literę po czym wprowadzamy znak zapytania, system wyszukuje

jedynie dostępne komendy zaczynające się od określonej litery.

```
wg_ro_a>s?
*s=show  set  show  ssh  systat
```

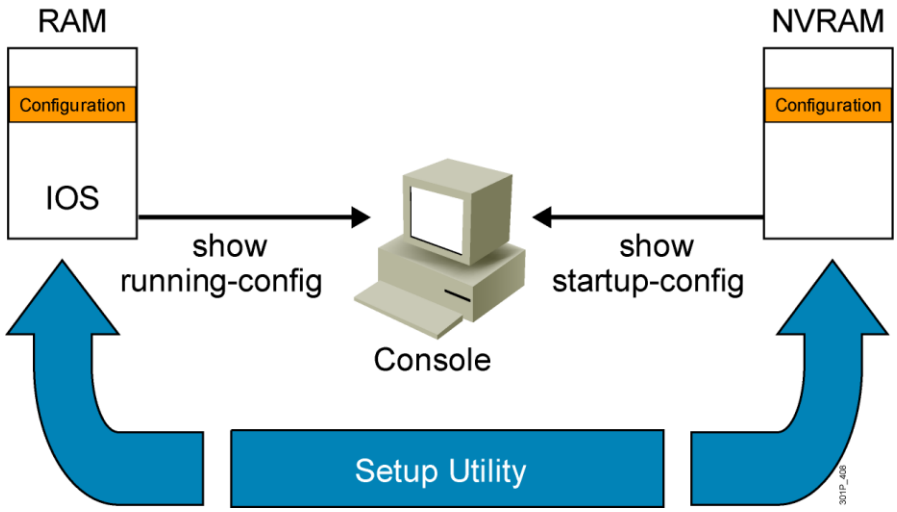
Syntax help – ten rodzaj pomocy pozwala poznawać dostępne pod komendy występujące w obrębie głównego polecenia. W tym celu należy wprowadzić określoną komendę następnie użyć klawisza **SPACE** i ponownie wprowadzić znak zapytania. Na ekranie listuje się lista dostępnych pod komend.

```
wg_ro_a>show ?
  clock          Display the system clock
  version        System hardware and software status
  flash:         Display information about flash: file system
  flowcontrol    Show flow control information
  users          Display information about terminal lines
```

Dodatkowo urządzenie posiada wbudowany bufor ostatnio wprowadzonych poleceń. Należy wydać polecenie **show history** i wyświetlimy ostatnio wprowadzone komendy.

Chcą wyświetlić konfigurację routera należy zrozumieć w jaki sposób urządzenie zarządza swoimi pamięciami (NVRAM, RAM). Przy starcie router wyszukuje plik konfiguracyjny, który domyślnie przechowywany jest w pamięci NVRAM. Jeżeli w NVRAM-ie została zapisana konfiguracja urządzenia, to nastąpi skopiowanie jej do pamięci RAM i w oparciu o tą konfigurację urządzenie będzie wykonywało określone procesy.

Kiedy router nie znajdzie w pamięci NVRAM pliku konfiguracyjnego, uruchomi się w trybie dialogu konfiguracyjnego. Pamięć RAM nie tylko służy do składowania pliku konfiguracyjnego dodatkowo urządzenie rozpakowuje ISO do tej pamięci, przechowuje tablicę TCAM, Tablicę routing, Tablicę translacji NAT. To w tej pamięci będą wykonywane złożone operacje.



Chcąc wyświetlić bieżącą używaną konfigurację na urządzeniu należy wydać polecenie **show runnig-config**, w tym przypadku zostanie wyświetlona konfiguracja przechowywana w pamięci RAM.

Natomiast chcąc sprawdzić z jakiej wyjściowej konfiguracji urządzenie się uruchomiło należy wydać polecenie **show startup-config**. Urządzenie sięga w tedy do pamięci NVRAM i wyświetla konfigurację.

Domyślnym miejscem składowania systemu operacyjnego w routerze jest pamięć FLASH. Aby wyświetlić zawartość w/w pamięci należy użyć polecenia **show flash:**

```
wg_ro_a#sh flash:
-#- --length-- -----date/time------ path
1      59374168 Mar 17 2009 15:39:42 c2800nm-adventerprisek9-mz.124-24.T.bin
2          1410 Nov 09 2010 13:55:04 G1Client2.txt

4632576 bytes available (59379712 bytes used)

wg_ro_a#
```

25. Routery – Konfiguracja

Konfigurację routera należy rozpocząć od wprowadzenia polecenia **enable** w tryby użytkownika podstawowego. Zostaniemy przeniesieni w tryb globalnej konfiguracji i jest to punkt wyjściowy do dalszych prac. W tym miejscu należy wydać polecenie **configure terminal**, który informuje router, że chcemy pracować w trybie globalnej konfiguracji. Z tego poziomu możemy rozpocząć konfigurację kreślonych elementów naszego urządzenia np. adres IP, użytkowników , zdalny dostęp, interfejsy itp.

Router#configure terminal

Router(config)#

Kolejnym krokiem, który musimy wykonać to określić co dokładnie będzie przez nas konfigurowane. Chcąc skonfigurować określony interfejs urządzenia należy wydać następujące polecenia :

Router(config)#interface fa0/0

Rouer(config-if)#

Gdzie **interface fa0/0** wskazuje, że chcemy skonfigurować pierwszy port routera. W wyniku wpisania powyższego polecenia, zostaniemy przeniesieni w tryb konfiguracji określonego portu. Konfigurację urządzenia można odnieść do czynności rozpakowywania prezentu: gdzie otwieramy pierwsze pudełko i trafiamy na kolejny które po rozpakowaniu ujawnia kolejne i tak aż dotrzemy do fizycznego przedmiotu.

Każde urządzenie po uruchomieniu się pierwszy raz, domyślnie przedstawi się nazwę np. Router, aby mieć kontrolę jakie urządzenie konfigurujemy należy nadać mu określoną charakterystyczna nazwę. W tym celu w trybie konfiguracji wydajemy polecenie **hostname** i wprowadzamy nazwę identyfikującą urządzenie.

Router(config)#

Router(config)#hostname wg_ro_a

wg_ro_a(config)#

Po zakończeniu konfiguracji należy ją zapisać, w tym celu wydajemy poniższe polecenia określając źródło skąd będzie kopiowana konfiguracja (wszelkie zmiany przechowywane są w pamięci RAM) oraz cel gdzie będzie ona zapisana (pamięć NVRAM).

wg_ro_a #copy running-config startup-config

Destination filename [startup-config]?

Building configuration…

wg_ro_a #

Chcąc wyświetlić informacje na temat konfiguracji urządzenia, stanu interfejsów, platformy sprzętowej i wielu innych parametrów należy posługiwać się poleceniem **show** dopełniając go odpowiednią pod komendą.

show version – wyświetla informacje dotyczące platform sprzętowej, wersji oprogramowania, liczby interfejsów, czasu pracy urządzenia.

show running-config – wyświetla informacje na temat bieżącej konfiguracji (RAM). **show interfaces** – wyświetla stan i statystki wszystkich interfejsów dostępnych w urządzeniu **show clock** – wyświetla informację na temat czasu skonfigurowanego na urządzeniu. **show users** – wyświetla listę zalogowany na danym urządzeniu użytkowników. **show cdp neighnors** – wyświetla listę urządzeń bezpośrednio podłączonych do naszego urządzenia.

Przejście w tryb uprzywilejowany wymaga podania polecenia **enable**, aby ograniczyć dostęp do tego trybu należy go zabezpieczyć tworząc hasło. W tym celu w trybie konfiguracji wydajemy polecenie :

wg_ro_a (config)#enable secret { hasło które będziemy używać }

Polecenie **enable secret** powoduje ze wprowadzone hasło podlega procesowi szyfrowania. W efekcie czego hasło nie jest wyświetlane jawnym tekstem a dodatkowo użyta funkcja szyfrująca ma uniemożliwić odszyfrowanie hasła.

Każda próba przejścia w tryb uprzywilejowany od tego momentu będzie wymagała podania hasła.

wg_ro_a >enable

Password: { w tym miejscu podaje hasło będzie ono nie widoczne }

wg_ro_a #

Chcąc usunąć całkowicie konfigurację z urządzenia należy posłużyć się poleceniem **erase startup-config.** W wynik użycia tego polecenia zostanie skasowana zawartość pamięci NVRAM. Po ponownym uruchomieniu się, urządzenia przejdzie w tryb konfiguracji dialogowej. Ponowne uruchomienie się urządzenia możemy wykonać używając polecenia **reload** .

26. Ćwiczenia #5 Routery

Przegląd poleceń wymaganych do zrealizowania zadań:

Polecenia	Opis
enable	Przejście w tryb uprzywilejowany
configure-terminal	Przejście w tryb konfiguracji
enable secret	Szyfrowanie hasła..
exit	Wyjście z określonego trybu pracy
end	Przejście do trybu uprzywilejowanego w czasie konfiguracji.
hostname ***nazwa urządzenia***	Nadanie nazwy urządzeniu
iInterface { *type* **}**	Przejście do trybu konfiguracji interfejsu vlan1
ip address	Nadanie adresu IP na interfejsie vlan1
show ip interface brief	Wyświetla informacje o statusie interfejsów
copy running-config startup-config	Kopiowanie konfiguracji
show version	Wyświetla informacje na temat platformy sprzętowej

26.1. Zadanie 1: Wstępna konfiguracja routera.

1) Utwórz nazwę dla przełącznika **wg_ro_X** – gdzie X odpowiada grupie w której pracujesz.
2) Zabezpiecz dostęp do trybu uprzywilejowanego używając hasła **cisco.** Hasło ma być szyfrowane.
3) Skonfiguruj adres IP na **interfejsie fa0/0** używając adresu **10.X.X.3 /24** – gdzie **X** dopowiada poniższej tabelce.

Grupa	Adres IP
A	10.2.2.3 /24
B	10.3.3.3 /24
C	10.4.4.3 /24
D	10.5.5.3 /24
E	10.6.6.3 /24
F	10.7.7.3 /24

4) Na przełączniku **wg_sw_X**, skonfiguruj adres IP na **interfejsie vlan1** używając adresu **10.X.X.11 /24** – gdzie **X** dopowiada poniższej tabelce.

Grupa	Adres IP
A	10.2.2.11 /24
B	10.3.3.11 /24
C	10.4.4.11 /24
D	10.5.5.11 /24
E	10.6.6.11 /24
F	10.7.7.11 /24

5) Na przełączniku **wg_sw_X**, skonfiguruj adres bramy domyślnej – 10.X.X.3 – gdzie **X** dopowiada poniższej tabelce.

Grupa	Adres IP
A	10.2.2.3 /24
B	10.3.3.3 /24
C	10.4.4.3 /24
D	10.5.5.3 /24
E	10.6.6.3 /24
F	10.7.7.3 /24

6) Sprawdź komunikacje z grupowego przełącznika z routerem **wg_ro_X**.

7) Sprawdź z jakiej platformy sprzętowej korzystasz i jaki używany jest IOS i zapisz poniżej w tabelce :

Platforma sprzętowa	System Operacyjny

8) Wyświetl konfigurację urządzenia.

9) Zapisz konfiguracje w pamięci NVRAM.

27. Ćwiczenia #6 Routery

Przegląd poleceń wymaganych do zrealizowania zadań:

Polecenia	Opis
banner login	Konfiguracja baneru informacyjnego na urządzeniu.
username [ ] password [ ]	Tworzenie lokalnego użytkownika oraz hasła.
enable secret	Szyfrowanie hasła.
crypto key generale rsa	Generowanie klucza RSA
ip domain-name	Tworzenie nazwy domeny na potrzeby generowania kluczy rsa
line console 0	Konfiguracja portu konsoli
ip ssh version	Konfiguracja ssh w określonej wersji 1 / 2
line vty 0 4	Konfiguracja liny terminalowych do sesje zdalnych
login / login local	Wymusza logowania / wymusza logowanie z użyciem użytkownika lokalnego
password	Polecenie do utworzenia hasła w obrębie linii konsoli / vty
transport input telnet ssh	Określa, jakie protokoły będą używane do komunikacji zdalnej
show interface	Wyświetla szczegółowe informacje o statusie oraz parametrach interfejsu
exit	Wyjście z określonego trybu pracy oraz rozłączenie sesji zdalnej

27.1. Zadanie 1: Zabezpieczenie dostępu do urządzenia.

1) Na routerze utwórz użytkownika **admin** z hasłem **cisco**
2) Zabezpiecz dostęp do linii konsoli hasłem **cisco,** wymagane jest logowanie**.**
3) Na routerze zabezpiecz dostęp do linii vty 0 4 hasłem **cisco.**
4) W obrębie linii vty 0 4 wymagaj logowania lokalnego.
5) Skonfiguruj baner login.

27.2. Zadanie 2: Konfiguracja zdalnego dostępu.

1) Utwórz następującą nazwę domeny **wg_ro_X.local** – X nr grupy.
2) Wygeneruj klucze **RSA** o długość 1024 bitów.
3) Zezwól na używanie następujących protokołów zdalnego dostępu : **telnet / ssh**
4) Zapisz konfigurację**.**

27.3. Zadanie 3: Weryfikacja połączeń telnet / ssh.

1) Zaloguj się na urządzenie **wg_sw_X** – gdzie X oznacza numer grupy laboratoryjnej.
2) Sprawdź komunikację warstwie trzeciej pomiędzy urządzeniami.
3) Wykonaj test połączenia: telnet
4) Wykonaj test połączenia: ssh
5) Zapisz konfigurację na routerze.

28. Routery - OSPF

OSPF to protokół routingu dynamicznego implementowany w sieciach. Cechą charakterystyczną tego protokołu jest fakt, iż traktuje on interfejsy routera jako linki. Poprzez stany, które występują na linkach urządzenia, OSPF pozyskują określone informacje tj.: adresy IP, maskę sieciową, w jakim typie sieci pracują. Zbiór tych informacji przechowywany jest w lokalnej bazie nazywanej **LSDB – link-state database**.

Pomiędzy routerami co 10 sekund rozsyłane są pakiety **HELLO**, w których przenoszone są szczegółowe informacje o nadawcy tj. identyfikator routera, obszar w którym pracuje, informacje o sąsiednich routerach, z którymi dane urządzenie ma kontakt, interwały czasowe dla pakietów HELLO, dodatkowo może być przenoszone hasło wymagane w procesie autentykacji pomiędzy urządzeniami.

W oparciu o informacje zawarte w pakietach HELLO następuje weryfikacja nadawcy. Odbiorca zagląda do pakietu HELLO i sprawdza szczegółowe informacje na temat: adresu sieciowego nadawcy (muszą pracować w tej samej sieci), obszaru w którym nadawca pracuje (wymagana zgodność tych samych obszarów). Jeżeli powyższe dane są poprawne odbiorca do swojej listy sąsiadów doda router, od którego otrzymał pakiet HELLO. W kolejnym kroku router który był odbiorcą, wyśle pakiet HELLO do nadawcy (wymiana pakietów HELLO). Proces weryfikacji będzie przebiegał identycznie po otrzymaniu pakietu. Kiedy router analizujący HELLO i wymagane parametry są prawidłowo (obszar, adres ip), dodatkowo w tablicy sąsiadów routera, który wysłał pakiet zobaczy swój router ID, podejmuje decyzję o nawiązanie relacji sąsiedzkiej z drugim urządzeniem? Ten stan nazywamy (**tow-way** lub **bidirectional**), ponieważ mamy pełną komunikację z drugim urządzeniem znajdującym się na końcu określonego linku (interfejsu).

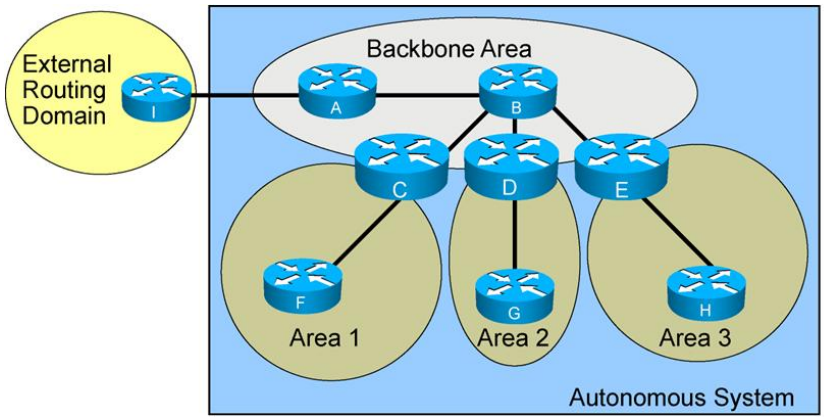
Od tego momentu routery zaczynają przesyłać między sobą informacje o stanie swoich linków (**LSA – link-state advertisement**), używanych metryk. W oparciu o te informacje budowana jest tablica topologiczna w obrębie każdego routera. Tablica topologiczna daje pełen obraz topologii sieci każdemu urządzeniu, dzięki czemu wie jakie trasy prowadzą do docelowych sieci. W życiu codziennym taką tablicą topologiczną może być np.: mapa miasta, na której naniesione są wszystkie ulice. Dzięki czemu mamy możliwość zaplanowania jak dotrzemy do docelowego punktu. Kiedy tablica topologiczna jest taka sama na każdym urządzeniu, następuje proces ustalenia, która z tras jest najbardziej optymalna. Każdy router podejmuje decyzję, że od

samego siebie będzie wyszukiwał trasy do docelowej sieci. Do tego celu używany jest algorytm drzewa rozpinającego SPF. Każda trasa opatrywana jest odpowiednią wartością liczbową tj. metryką. Najniższa wartość metryki decyduje o wprowadzeniu takie trasy do tablicy routingu i używaniu jej. Routery co 30 minut wysyłają między sobą (**LSA – link-state advertisement)**, lub wysyłają ogłoszenia natychmiastowe, kiedy wykrywają zmiany w sieci.

OSPF wykorzystuje hierarchiczny dwuwarstwowy model, w którym można rozróżnić charakterystyczne elementy takie jak:

Autonomiczny system – możemy traktować jako „wyspę", na której operują urządzenia będące pod wspólną administracją. Aby zapewnić większą wydajność w procesie routingu autonomiczne systemy zostały podzielone na mniejsze obszary.

Obszary – dokonują logicznego podziału autonomicznego obszaru, grupując określoną liczbę urządzeń mających kontakt ze sobą. W obrębie obszaru powinno pracować do 50 urządzeń (routerów), dzięki czemu uzyskujemy optymalną zbieżność infrastruktury.



Istotna zaletą używania obszarów jest fakt, iż problemy, które występują w obrębie jednego obszaru nie są przenoszone do pozostałych. Ułatwia to przede wszystkim administratorowi rozwiązywanie problemów.

W OSPF-ie istnieje podział obszarów ze względu na specyfikę:

Obszar 0 (babione) – jest obszarem tranzytowym, za pośrednictwem którego przesyłane są pakiety pomiędzy obszarami. Do obszaru 0 podłączone są pozostałe regularne obszary jak na powyższym rysunku.

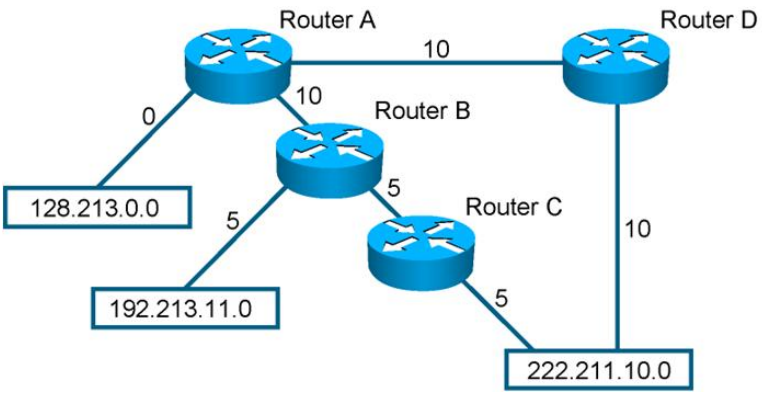
Obszar Regularny (non babione) – to obszar, który zapewnia komunikację użytkownikom i zapewnia im dostęp do zasobów. Obszary regularne tworzone są na określonym obszarze geograficznym. Do zapewnienie komunikacji pomiędzy obszarami regularnym wymagany jest obszar 0. Odnoszą się do powyższego rysunku routery będziemy dzielili na:

Babione Router – (**B**) - routery operujące w obszarze 0

Area Border Router - (**C, D, E**) - to routery, które występują na styku obszaru regularnego a obszaru 0. Za ich pośrednictwem przenoszone są pakiety to routerów w obszarze 0. **Internal routery** – (**F, G, H**) - to routery pracujące w regularnych obszarach to za ich pośrednictwem użytkownicy mają dostęp do określonych zasobów.

Autonomous System Boundary Router – (**B**) – to router, który pracuje na styku obszaru 0 i zapewnia kontakt z urządzeniami pracującymi w innych domenach routingu tj. z urządzeniami, które mogą wykorzystywać inne protokołu routing.

OSPF wykorzystuje tablicę topologiczną oraz algorytm SFP do wyszukania najbardziej optymalnej trasy do docelowej sieci. Kiedy router w swojej tablicy topologicznej posiada więcej propozycji prowadzących do określonej sieci musi podjąć decyzję, której trasy używać.



Do rozstrzygnięcia tej kwestii, router przypisze do każdej trasy odpowiednią wartość liczbową nazywana metryką (kosztem). Sumując wszystkie koszty linków prowadzących do docelowej sieci, uzyskuje realny koszt do określonej sieci. Najniższy koszt wskazuje na najbardziej optymalną trasę, która zostanie umieszczona w tablicy routingu.

W przypadku protokołu OSPF metryka (koszt) wyliczana jest w oparciu o wzór:

KOSZT = 10^8 / przepustowość na określonym interfejsie (b/s)

gdzie 10^8 = 100 000 000 (100Mb/s).

Dobrą praktyką administratora jest nawyk wprowadzania w obrębie każdego interfejsu operującego w procesie OSPF, odpowiedniej przepustowość w kilobitach na sekundę. Użycie polecenia **bandwitch** i podanie określonej wartości nie przekłamuje kalkulacji kosztów. Kiedy na interfejsie nie zostanie wpisana realna przepustowość, OSPF będzie używał domyślnych wartość dla określonych typów interfejsów, co może negatywnie wpłynąć na wybór optymalnej trasy do docelowej sieci.

Router(config)# interface serial 0/0

Router(config-if)# bandwitch <1-10000000> Bandwidth w kilobits

Kiedy na routerach zostanie uruchomiony proces OSPF, router wyszukuje najwyższy adres IP przypisany na fizycznym interfejsie i używa go w sieci, jako swój identyfikator tj. **Router ID**. Router ID jest przenoszony w pakiecie HELLO. Nie jest to jednak optymalna rozwiązanie, ponieważ przy większej ilości routerów w sieci tak wybierany router ID nie jednoznacznie wskazuje na określone urządzenie. Dlatego też istnieje możliwość utworzenia logiczny interfejsów w obrębie routera nazywanych **loopback**.

Ten interfejs pozwala administratorowi przypisać określony adres IP, który będzie jednoznacznie identyfikował router w sieci. Dodatkową zaletą logicznego interfejsu jest fakt, iż nie można go fizycznie uszkodzić, wyłączyć, dzięki czemu nie jesteśmy uzależnieni od stanu fizycznego interfejsu.

Konfiguracja interfejsu loopback:

Router(config)# interface loopback < numer interfejsu>

Router(config)# interface loopback1

Router(config-if)# ip address 1.1.1.1 255.255.255.255

W przypadku, kiedy nie chcemy używać interfejsów loopback w obrębie naszego urządzenia możemy skonfigurować router ID w czasie konfiguracji procesu OSPF używając poniższego polecenia.

Router(config)#router ospf 1

Router(config-router)#router-id 1.1.1.1

29. Routery – OSPF konfiguracja

Uruchomienie procesu OSPF na routerze rozpoczynamy od wydania poniższych poleceń w trybie konfiguracji routera.

Router(config)#router ospf { process-id } - gdzie { process-id } to wartość liczbowa identyfikująca proces OSPF lokalnie na routerze.

W kolejnym kroku wymagane jest opublikowanie określonych adresów sieci podłączonych do naszego urządzenia. Administrator sam decyduje, jakie prefixy sieciowe będzie ogłaszał do innych routerów pracujących w tym obszarze. W tym celu wydajemy poniższe polecenie:

RouterX(config-router)#network address wildcard-mask area area-id – gdzie: **adres sieci** to prefix który ogłaszamy np **10.1.1.0**

wildcard-mask jest to odwrócona maska sieciowa w której na początku występuje ciąg logicznych "**0**" a następnie ciąg logicznych "**1**".

Np. maska sieciowa /24 bitowa jest zapisywana w takiej formie 255.255.255.0 - gdzie pierwsze trzy oktety są wypełniona logicznymi „**1**, co jednoznacznie wskazuje iż w pierwszych trzech oktetach adresu IP wartości nie mogą ulec zmianie 10.1.1.0. W przypadku ostatniego oktetu może on zostać wypełniony dowolnymi wartościami „0" lub „1".

W przypadku wildcard-mask zapis tej samej maski wygląda w następujący sposób 0.0.0.255 gdzie logiczne „0" wskazują na pola z adresu IP, które nie mogą ulec zmianie. W przypadku ostatniego oktetu wpis „255" pozwala naprzemiennie wypełniać oktet dowolnymi wartościami „0" i „1".

area area-id – po słowie area należy wpisać wartość liczbową, która odpowiada obszarowi w którym ten prefix pracuje np. area 0

Dodatkowo należy pamiętać o poleceniu **router-id 1.1.1.1**, którym możemy skonfigurować identyfikator urządzenia w sieci.

Router(config)#router ospf 1

Router(config-router)#router-id 1.1.1.1

Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router(config-router)#network 192.168.3.0 0.0.0.7 area 0

30. Ćwiczenia #7 Routery

Przegląd poleceń wymaganych do zrealizowania zadań:

Polecenia	Opis
show controllers { type } {slot}	Weryfikacja typu kabla DTE / DCE
bandwidth	Konfiguracja przepustowości linku. Na interfejsie DTE.
clock rate	Konfiguracji prędkości taktowania zegara.
interface loopback {numer}	Tworzenie interfejsu loopback.
router ospf { process-id }	Uruchomienie protokołu OSPF.
router-id { IP adres }	Konfiguracja identyfikatora routera w procesie OSPF.
network {*network nr***}** **wildcard-mask area { area-id }**	Publikowanie określonego prefixu sieci w procesie OSPF
show ip protocols	Sprawdzenie, jakie protokoły są uruchomione na routerze.
show ip ospf neighbor	Wyświetla listę sąsiadów.
show ip route	Wyświetla zawartość tablicy routingu.

Adresacja IP wymagana do wykonania poniższych ćwiczeń.

Grupa	Interfejs Vlan 1 IP adres	Router Fa0/0 IP adres	Interfejs Loopback 0 IP adres	Interfejs S0/0 IP adres	Interfejs S0/1 IP adres	Core_router Serial int. IP adres
A	**10.2.2.10 /24**	**10.2.2.3 /24**	**2.2.2.2**	**10.140.1.2/24**	**192.168.1.1/24**	**10.140.1.1/24**
B	**10.3.3.10 /24**	**10.3.3.3 /24**	**3.3.3.3**	**10.140.2.2/24**	**192.168.1.2/24**	**10.140.2.1/24**
C	**10.4.4.10 /24**	**10.4.4.3 /24**	**4.4.4.4**	**10.140.3.2/24**	**192.168.2.1/24**	**10.140.3.1/24**
D	**10.5.5.10 /24**	**10.5.5.3 /24**	**5.5.5.5**	**10.140.4.2/24**	**192.168.2.2/24**	**10.140.4.1/24**
E	**10.6.6.10 /24**	**10.6.6.3 /24**	**6.6.6.6**	**10.140.5.2/24**	**192.168.3.1/24**	**10.140.5.1/24**
F	**10.7.7.10 /24**	**10.7.7.3 /24**	**7.7.7.7**	**10.140.6.2/24**	**192.168.3.2/24**	**10.140.6.1/24**

30.1. Zadanie 1: Konfiguracja przełącznika.

1) Korzystając z tabeli powyżej przypisz odpowiednie adres IP do interfejsu vlan1.
2) Skonfiguruj na przełączniku bramę domyślną **.**
3) Wyświetl konfigurację przełącznika**.**
4) Zapisz konfigurację.

30.2. Zadanie 2:Konfiguracja wg_ro_X.

1) Zaloguj się na urządzenie **wg_ro_X** – X nr grupy laboratoryjnej.
2) Utwórz interfejs **loopback0** i przypisz mi odpowiedni adres IP z tabeli.
3) Przypisz adres IP do interfejsu Fastethernet0/0 korzystając z tabeli.
4) Sprawdź, który interfejs Serial pracuje jako DCE a który DTE
5) Przypisz adres IP na interfejsie S0/0 korzystając z tabeli.
6) Przepustowość dla interfejsu S0/0 powinna mieć wartość **128**.
7) Przypisz adres IP na interfejsie S0/1 korzystając z tabeli.
8) Skonfiguruj **clock rate** podając wartość 64000.
9) Przepustowość dla interfejsu S0/1 powinna mieć wartość **64**.
10) Dokonaj weryfikacji czy posiadasz kontakt z wszystkim urządzeniami. W tym celu przeprowadź test poleceniem PING.
11) Zapisz konfigurację.

30.3. Zadanie 2: Konfiguracja OSPF-a.

1) Na urządzeniu **wg_ro_X** – X nr grupy laboratoryjnej, uruchom proces „10” protokołu routingu OSPF.
2) Opublikuj wszystkie podłączone do wg_ro_X sieci. Routery w laboratorium pracują w **AREA 0.**
3) Sprawdź, czy nawiązały się relacje sąsiedzkie.
4) Uzupełnij poniższa tabelkę.

ID Sąsiada	Adres IP Sąsiada	Interfejs lokalny którym osiągamy sąsiada.

5) Sprawdź, czy w tablicy routingu pojawiają się wpisy o innych sieciach.
6) Użyj polecenia PING celem sprawdzenia czy posiadasz kontakt z innymi urządzeniami w laboratorium.
7) Zapisz konfigurację routera.

31. Routery - EIGRP

EIGRP to zaawansowany protokół routingu dynamicznego, który jest hybrydą ponieważ wykorzystuje cechy dwóch innych protokołów: dystans wektor oraz stanu łącza.

Cechami charakterystycznymi dla tego protokołu są :

1) **Bardzo szybka zbieżność** – wynika ona z wykorzystywania algorytmu **DUAL** (**Diffusing Update Algorithm**). Router, który używa EIGRP przechowuje wszystkie zapasowe trasy do docelowej sieci i w przypadku awarii natychmiast wykorzystuje alternatywna trasę.
2) **Ograniczone utylizowanie przepustowości linku** – EIGRP nie wysyła okresowych ogłoszeń, a częściowe. Takie ogłoszenia pojawiają się, kiedy router wykryje zmianę metryki lub zmianę stanu linku. Natychmiast taka informacja jest przesyłana.
3) **Wsparcie dla wielu protokołów L3** – EIGRP wspiera IPv4 , IPv6, ale posiada wsteczną kompatybilność dla IPX.
4) **Bezklasowy protokół** – umożliwia to przesyłanie zmiennej długości masek dla każdej sieci.
5) **Rozłożenie obciążenia –** load balancing realizowany na linka o nie równych metrykach. Umożliwia to administratorowi efektywniejsze wykorzystywanie kliku dostępnych tras do docelowej sieci.
6) **Prosta sumaryzacja –** administrator może dokonywać sumaryzację tras do klasowej maski w dowolnym punkcie sieci. Dzięki czemu redukujemy ilość wpisów do tablicy routingu.
7) **EIGRP –** jest protokołem firmy Cisco i możemy go implementować w produktach firmy Cisco.

Protokół EIGRP wykorzystuje trzy tabele w oparciu o które wykonuje procesy routingu.

Tabela sąsiadów – jest to tabela, która zawiera listę wszystkich bezpośrednio podłączonych routerów używających EIGRP, z którymi została nawiązana relacja sąsiedzka.

Tabela topologiczna – zawiera ona wpisy o wszystkich trasach prowadzących do docelowej sieci, które router otrzymał od swoich sąsiadów. Najlepsza trasa z tablicy topologicznej zostaje wybrana i trafia do tablicy routingu.

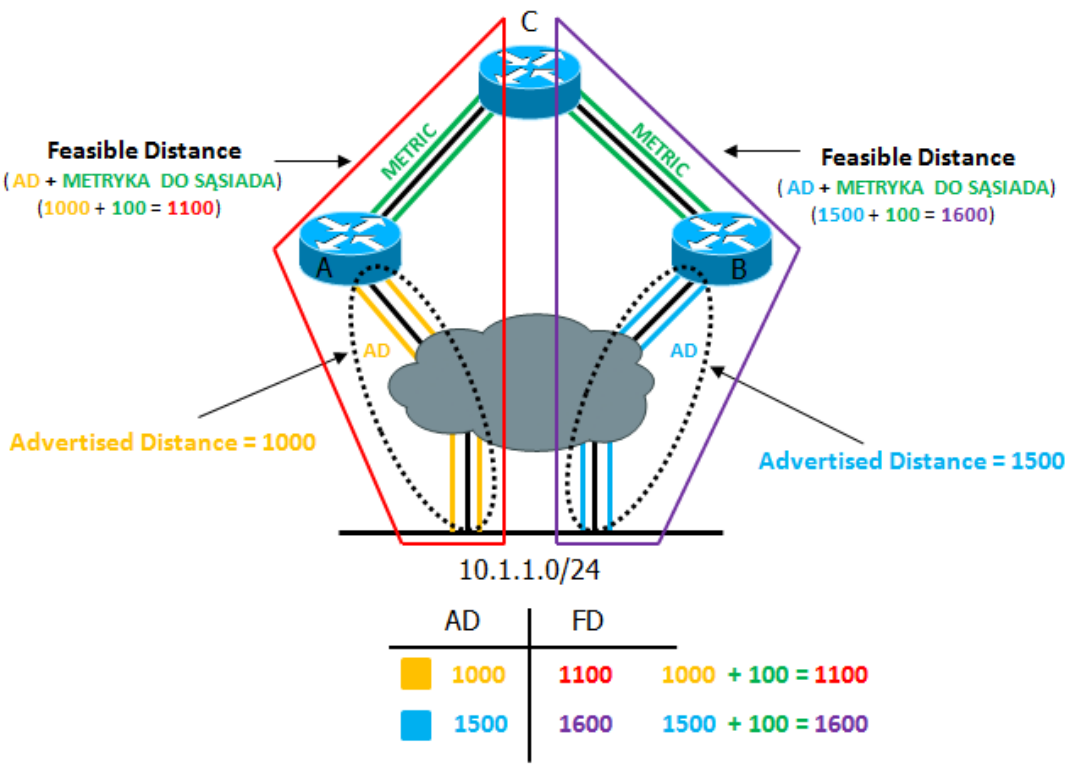
Tablica routingu – w tym miejscu router przechowuje najlepszą trasę do docelowej sieci. W przypadku, kiedy trasa ta przestaje być dostępna router skorzysta z kolejnej trasy,

którą przechowuje w swojej tablicy topologicznej. Dzięki czemu router nie będzie wyszukiwał innej trasy w sieci. Takie podejście gwarantuje szybką zbieżność w sieci.

W przypadku protokołu EIGRP najlepsza trasa nazywana jest **sukcesorem**, natomiast zapasowa trasa prowadząca do tego samego celu jest nazywana **fizybilnym sukcesorem (potencjalny sukcesor)**. Do ustalenia sukcesora i fizybilnego sukcesora EIGPR wykorzystuje dwie składowe :

Advertised distance – to metryka, która jest ogłaszana przez sąsiada i wskazuje na koszt osiągnięcia docelowej sieci przez tego określonego sąsiada. („ Ile kosztuje przejście do docelowej sieci po przez tego sąsiada”).

Feasible distance – jest to całkowity „koszt” osiągnięcia docelowej sieci, na który składa się **AD** (**Advertised distance**) + metryka do sąsiada.

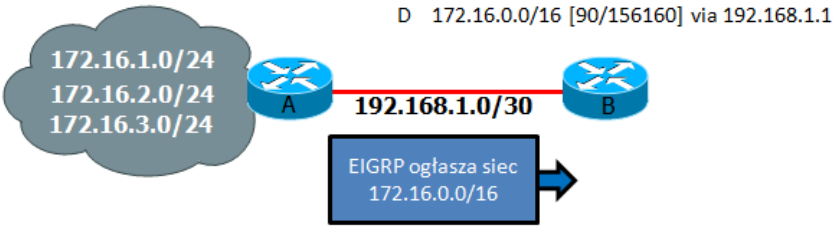


Tablica routingu Routera C

Network	Metric (FD)	Next Hop
10.1.1.0/24	1100	Router A

32. Routery – EIGRP Sumaryzacja

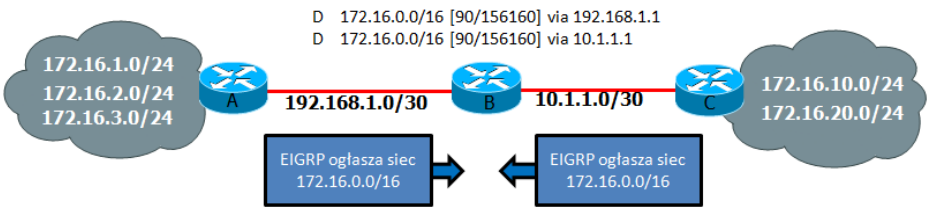
Sumaryzacja to proces, który jest wykonywany na routerach na granicy stref sieci. Tymi strefami są miejsca zmian prefixów sieciowych pomiędzy urządzeniami. Np. router A posiada informacje o sieci 172.16.1.0/24, 172.16.2.0/24 172.16.3.0/24, a za pomocą innego interfejsu komunikuje się z drugim routerem używając adresu 192.168.1.0/30.



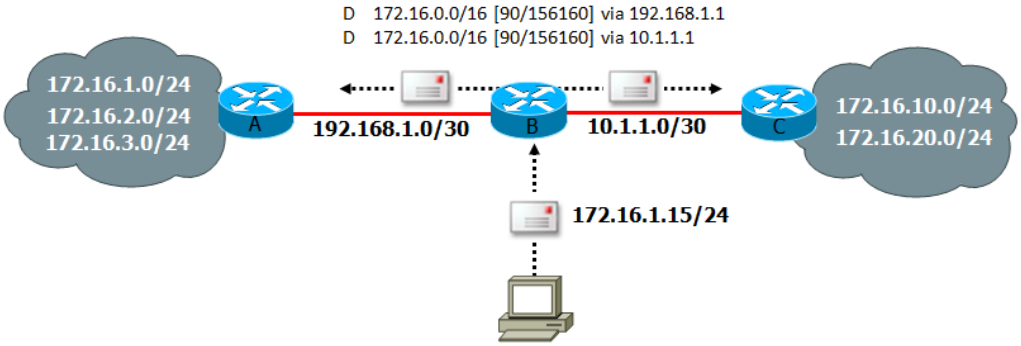
W przypadku automatycznej sumaryzacji router używa klasowej maski dla ogłaszanych sieci. W efekcie czego **router A** informuje **router B** o tym, iż on posiada pełną informację o sieci 172.16.0.0/16 i wszystkie pakiety zmierzające do sieci 172.16.0.0/16 powinny trafiać do niego.

Problem, z jakim może zetknąć się administrator, to sytuacja kiedy np. fragment sieć 172.16.0.0/16 występuje w obrębie innego routera i jest ogłaszana w protokole EIGRP.

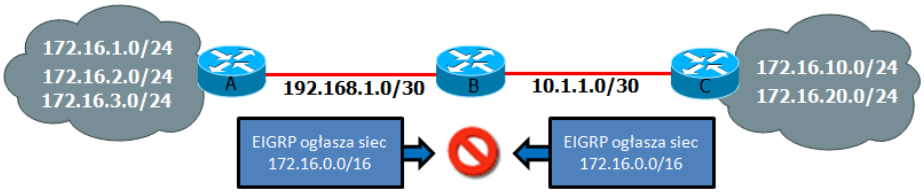
Router C ogłasza do routera B informacje o sieci 172.16.10.0/24 i 172.16.20.0/24. Domyślnie na routerze C używana jest autosumaryzacja, w efekcie czego następuje przesłanie jednego prefixu sieć 172.16.0.0/16. W tablicy routingu routera B pojawiają się dwa wpisy mówiące jak osiągnąć sieci 172.16.0.0.



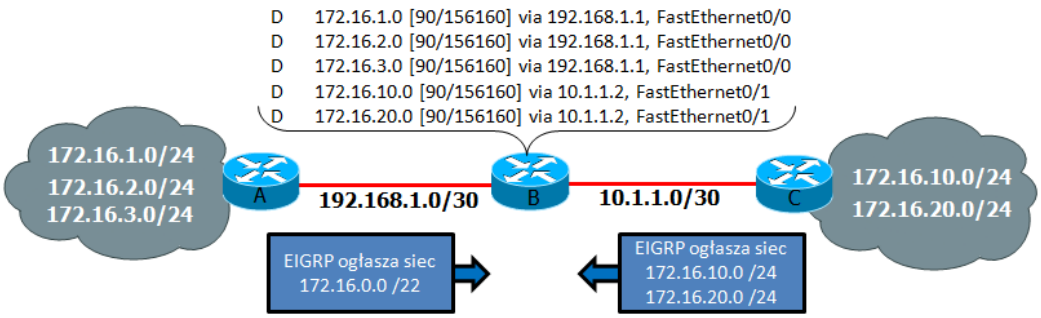
Stosowanie domyślnej autosumaryzacji doprowadza do błędnych wpisów w tablicy routingu routera B. Konsekwencja takiego działania jest load balancing. Kiedy router B otrzyma pakiet zmierzający do sieci 172.16.1.0/24 będzie przesyłał pakiety naprzemiennie do routera A oraz C. Wynika to z faktu, iż oba routery ogłosiły że posiadają dostęp do sieci 172.16.0.0/16.



Auto sumaryzacji nie wolno nam używać na routerach, *kiedy nie jesteśmy pewni czy w zdalnych lokalizacjach nie występuje fragment określonego prefixu sieciowego.*. Dlatego dobra praktyka jest używanie w każdej lokalizacji innej adresacji sieciowej.



Administratorzy wykonują celowo ręczną sumaryzację, aby ograniczyć ilość wpisów w tablicy routingu routera, a przez to zwiększyć jego efektywność w procesie routingu. Kiedy nie mam pewności, czy określony prefix sieci nie występuje w innym miejscu należy wyłączyć auto sumaryzację w obrębie protokołu EIGRP i dokonać ręcznej sumaryzacji. Ogłaszając określony prefix z odpowiednią maską sieciową.



33. Routery – EIGRP Konfiguracja

Uruchomienie procesu EIGRP na routerze rozpoczynamy od wydania poniższych poleceń w trybie konfiguracji routera.

Router(config)# router eigrp { <1-65535> Autonomous system number } - gdzie { **Autonomous system number** } to wartość liczbowa musi być taka sama na wszystkich routerach pracujących w sieci i używających EIGRP.

W kolejnym kroku wymagana jest opublikowanie określonych adresów sieci podłączonych do naszego urządzenia. Administrator sam decyduje jakie prefixy sieciowe będzie ogłaszał do innych routerów. W tym celu wydajemy poniższe polecenie :

RouterX(config-router)#network address wildcard-mask – gdzie:

adres sieci to prefix który ogłaszamy w EIGRP np 10.2.2.0

wildcard-mask jest to odwrócona maska sieciowa w której na początku występuje ciąg logicznych “0” a następnie ciąg logicznych “1”.

Np. maska sieciowa /24 bitowa jest zapisywana w takiej formie 255.255.255.0 - gdzie pierwsze trzy oktety są wypełniona logicznymi „1, co jednoznacznie wskazuje, iż w pierwszych trzech oktetach adresu IP wartości nie mogą ulec zmianie 10.1.1.0. W przypadku ostatniego oktetu może on zostać wypełniony dowolnymi wartościami „0” lub „1”.

W przypadku wildcard-mask zapis tej samej maski wygląda w następujący sposób 0.0.0.255 gdzie logiczne „0” wskazują na pola z adresu IP które nie mogą ulec zmianie. W przypadku ostatniego oktetu wpis „255” pozwala naprzemiennie wypełniać oktet dowolnymi wartościami „0” i „1”. Przykładowa konfiguracja EIGRP :

Router(config)#router eigrp 100

Router(config-router)#no auto-summary

Router(config-router)#network 192.168.1.0 0.0.0.255

Router(config-router)#network 192.168.2.0 0.0.0.255

Router(config-router)#network 172.16.0.0 0.0.3.255

34. Ćwiczenia #8 Routery

Przegląd poleceń wymaganych do zrealizowania zadań:

Polecenia	Opis
show controllers { type } {slot}	Weryfikacja typu kabla DTE / DCE
bandwidth	Konfiguracja przepustowości linku. Na interfejsie DTE.
clock rate	Konfiguracji prędkości taktowania zegara.
interface loopback {numer}	Tworzenie interfejsu loopback.
router eigrp { AS-id }	Uruchomienie protokołu OSPF.
no auto-summary	Wyłącza automatyczna sumaryzację do klasy sieci.
network {*network nr***} wildcard-mask**	Publikowanie określonego prefixu sieci w procesie EIGRP
show ip protocols	Sprawdzenie, jakie protokoły są uruchomione na routerze.
show ip eigrp neighbor	Wyświetla listę sąsiadów.
show ip route	Wyświetla zawartość tablicy routingu.

Adresacja IP wymagana do wykonania poniższych ćwiczeń.

Grupa	Interfejs Vlan 1 IP adres	Router Fa0/0 IP adres	Interfejs Loopback 0 IP adres	Interfejs S0/0 IP adres	Interfejs S0/1 IP adres	Core_router Serial int. IP adres
A	10.2.2.10 /24	10.2.2.3 /24	2.2.2.2	10.140.1.2/24	192.168.1.1/24	10.140.1.1/24
B	10.3.3.10 /24	10.3.3.3 /24	3.3.3.3	10.140.2.2/24	192.168.1.2/24	10.140.2.1/24
C	10.4.4.10 /24	10.4.4.3 /24	4.4.4.4	10.140.3.2/24	192.168.2.1/24	10.140.3.1/24
D	10.5.5.10 /24	10.5.5.3 /24	5.5.5.5	10.140.4.2/24	192.168.2.2/24	10.140.4.1/24
E	10.6.6.10 /24	10.6.6.3 /24	6.6.6.6	10.140.5.2/24	192.168.3.1/24	10.140.5.1/24
F	10.7.7.10 /24	10.7.7.3 /24	7.7.7.7	10.140.6.2/24	192.168.3.2/24	10.140.6.1/24

34.1. Zadanie 1: Konfiguracja EIGRP.

1) Na urządzeniu **wg_ro_X** – X nr grupy laboratoryjnej, uruchom protokołu routingu EIGRP używając numeru autonomicznego „**100**”.
2) Opublikuj wszystkie podłączone do **wg_ro_X** sieci wyłączając auto sumaryzację.
3) Sprawdź, czy nawiązały się relacje sąsiedzkie.
4) Uzupełnij poniższa tabelkę.

Adres IP Sąsiada	Interfejs lokalny którym osiągamy sąsiada.

5) Sprawdź wpisy w tablicy topologicznej.
6) Sprawdź, czy w tablicy routingu pojawiają się wpisy o innych sieciach.
7) Użyj polecenia PING celem sprawdzenia czy posiadasz kontakt z innymi urządzeniami w laboratorium.
8) Zapisz konfigurację routera.

35. Routery – Praktyczne zaostosowania konifugiracji ACCESS-LIST (filtowanie ruchu oraz NAT) .

Zadanie jakie zostało postawione przed Wami to rozwiązanie przykładowego case study (CS), pracując w grupie, w tym celu stosujemy pracę zespołową oraz zbiór pytań i odpowiedzi wg. schematu:

a) Omówienie istoty problemu,

b) Analiza problemu,

c) Wykonujecie zadane polecenia,

d) Prezentujecie efekty pracy.

35.1. Case Study: Zaplanowanie i wdrożenie ACCESS-LIST-y w celu filtrowania określonego typu ruchu w sieci.

Zadanie do zrealizowania:

a) Wykonanie testu komunikacyjnego pomiędzy urządzeniami (nawiązanie sesji: telnet, ssh oraz wykorzystania polecenia ping).

b) Zaplanuj ACL, która zabroni wysłania pakietów „ping-a" do routera grupowego oraz pozostałych routerów w innych zespołach z Twojego przełącznika. Zdarzenia powinny być logowane na konsoli. Pozostały ruch IP powinien być nadal dostępny (np. telnet oraz ssh).

c) Zastanów się, w którym miejscu w/w ACL powinna być umieszczona.

d) Na routerze grupowym skonfiguruj ACL oraz umieść ją w określonym miejscu.

e) Wykonaj test komunikacyjny jak w punkcie „a", w celu sprawdzenia poprawności działania ACL.

f) Zaplanuj ACL, która zabroni ruchu ssh oraz telnet do Twojego grupowego routera. Zdarzenie powinny być logowane na konsoli.

g) Zastanów się, w którym miejscu w/w ACL powinna być umieszczona.

h) Na routerze grupowy skonfiguruj ACL oraz umieść ją w określonym miejscu.

35.2. Case Study: Zaplanowanie i wdrożenie translacji adresów w sposób dynamiczny.

Zadanie do zrealizowania:

a) Usunięcie wszystkich ACL z routera grupowego.

b) Zaplanuj ACL, która zezwoli na translację adresów z Twojej lokalnej sieci.

c) Zastanów się, który interfejs urządzenia będzie używany jako wejściowy, a który jako wyjściowy.

d) Na routerze grupowym skonfiguruj ACL oraz translację NAT w sposób dynamiczny z wykorzystaniem portów.

e) Wykonaj test komunikacyjny pomiędzy routerami, w celu sprawdzenia poprawności działania ACL.