Fundusze Europejskie dla Rozwoju Społecznego
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Politechnika Świętokrzyska
Wydział Zarządzania i Modelowania Komputerowego

Kierunek studiów:
Inżynieria danych

Mirosław Płaza

Materiały dydaktyczne do przedmiotu

AKADEMIA SIECI CISCO

opracowane w ramach realizacji Projektu
„Dostosowanie kształcenia w Politechnice Świętokrzyskiej do potrzeb współczesnej gospodarki”
FERS.01.05-IP.08-0234/23

Kielce, 2025

Spis treści

1. Wprowadzenie

Przedmiot Akademia Sieci Cisco realizowany jest we współpracy z jednym z liderów technologii teleinformatycznych na świecie – firmą Cisco. Cisco Networking Academy jest globalnym programem edukacyjnym, który od ponad 25 lat przygotowuje kursantów/studentów do kariery w bardzo dynamicznie rozwijającej się branży IT. Program ten, oferuje szeroki zakres profesjonalnych i certyfikowanych kursów, które łączą wiedzę teoretyczną z praktycznymi umiejętnościami, odpowiadając stale na aktualne zapotrzebowanie rynku pracy. Program realizowany jest we współpracy z uczelniami, szkołami i organizacjami na całym świecie, zapewniając dostęp do wysokiej jakości materiałów szkoleniowych.

Jednym z najważniejszych kursów udostępnianych w ramach Cisco Networking Academy jest CCNA (Cisco Certified Network Associate). CCNA to jeden z najbardziej rozpoznawalnych i cenionych certyfikatów w branży IT, potwierdzający fundamentalną wiedzę i praktyczne umiejętności w zakresie zarządzania sieciami komputerowymi. Jest to pierwszy i najważniejszy krok dla każdego, kto chce rozpocząć karierę jako inżynier sieci, administrator systemów czy specjalista IT. Kurs obejmuje trzy główne moduły: Introduction to Networks (ITN), Switching, Routing, and Wireless Essentials (SRWE) oraz Enterprise Networking, Security, and Automation (ENSA). Pierwszy z nich (ITN) stanowi wprowadzenie do zagadnień sieci komputerowych. Uczestnicy uczą się budowy i działania sieci, poznają modele OSI i TCP/IP, adresowanie IPv4 i IPv6 oraz konfigurację podstawowych urządzeń, takich jak przełączniki i routery. Moduł koncentruje się na poszczególnych warstwach OSI, stanowiąc solidny fundament do dalszej nauki. Druga część kursu CCNA – moduł SRWE obejmuje głównie konfigurację przełączników, routingu oraz sieci bezprzewodowych. Wyjaśnia szczegółowe zagadnienia, takie jak wirtualne sieci LAN (VLAN), protokoły drzewa rozpinającego (STP) oraz routing statyczny i dynamiczny. Dodatkowo, kursanci poznają zasady działania i konfigurację podstawowych sieci WLAN. Ostatnia część to moduł ENSA, gdzie poznawana jest wiedza o zaawansowanych technikach routingu, bezpieczeństwie i automatyzacji sieci. W tej części kursu uczestnicy uczą się konfiguracji protokołów routingu dynamicznego, takich jak OSPF, implementacji list kontroli dostępu (ACL) i tłumaczenia adresów (NAT). Kluczowe jest również wprowadzenie do koncepcji automatyzacji sieci, w tym programowalności urządzeń.
W ramach przedmiotu Akademia Sieci Cisco realizowany jest pierwszy moduł kursu CCNA. Zajęcia oparte są o profesjonalne materiały udostępniane przez Cisco w ramach współpracy z Politechniką Świętokrzyską, natomiast niemniejsze opracowanie stanowi rozwinięcie wybranych zagadnień.

2. Zakres przedmiotu Akademia Sieci Cisco

2.1. Wykłady

Zakres wykładów obejmuje następujące zagadnienia: Wprowadzenie do zagadnień sieci komputerowych. Modele odniesienia. Komponenty sieci: urządzenia, media, usługi. Topologie fizyczne i logiczne. Aktualne trendy rozwoju małych i średnich sieci komputerowych. Funkcje i konfiguracja sieciowych systemów operacyjnych. Metody dostępu. Wybrane zagadnienia konfiguracji aktywnych urządzeń sieciowych. Schematy adresowania. Wybrane protokoły i sposoby komunikacji w sieciach komputerowych, stos protokołów TCP/IP. Kodowanie/dekodowanie informacji. Pojęcia enkapsulacji, dekapsulacji, segmentacji oraz multipleksacji. Standaryzacja w sieciach komputerowych. Dostęp do sieci, warstwa fizyczna oraz warstwa łącza danych. Protokoły warstwy fizycznej. Media transmisyjne. Wybrane typy interfejsów i portów. Protokoły warstwy łącza danych. Podwarstwy LLC i MAC. Metody kontroli dostępu do medium transmisyjnego. Ethernet – standardy. Procesy CSMA/CD oraz CSMA/CA. Identyfikacja w sieci Ethernet – typy adresów MAC. Ramka Ethernet. Protokół ARP; funkcje i operacje. Przełączniki LAN warstwy 2. Warstwa sieci, podstawy routingu. Brama domyślna. Tablice routingu. Adres następnego przeskoku. Metryka. Routery. Protokół IPv4. Nagłówek pakietu IPv4. Enkapsulacja w IPv4. Ograniczenia protokołu IPv4. Publiczne i prywatne adresy IPv4. Protokół IPv6. Budowa nagłówka pakietu IPv6. Enkapsulacja IPv6. Zalety protokołu IPv6. Publiczne i prywatne adresy IPv6. Warstwa transportowa – jej rola w sieciach komputerowych. Charakterystyka protokołów TCP oraz UDP – porównanie, wady i zalety. Adresacja IPv4 oraz IPv6. Prefiks, rodzaje adresów (sieci, hosta, rozgłoszeniowy). Adresacja statyczna i dynamiczna. Komunikacja unicast, broadcast, multicast. Współistnienie IPv4 i IPv6 (podwójny stos, tunelowanie, translacja). Zasady podziału sieci na podsieci. Czynniki, jakie należy wziąć pod uwagę projektując sieć. Grupowanie urządzeń. Komunikacja pomiędzy podsieciami. Przygotowanie planu adresacji. Maska podsieci. Podstawowy podział na podsieci – stała długości maski. Mechanizm zmiennej długość maski podsieci (VLSM). Podział sieci na podsieci z wykorzystaniem VLSM. Rozważania projektowe dla IPv6. Warstwy: sesji, prezentacji i aplikacji. Usługi i protokoły (DNS, Telnet, Boostrap, DHCP, HTTP, FTP, TFTP, SMTP, POP, IMAP). Projektowanie sieci komputerowych. Uwarunkowania. Wybór urządzeń do małej sieci. Nadmiarowość. Skalowalność. Aplikacje czasu rzeczywistego. Dokumentacja. Zagrożenia w sieciach komputerowych. Wprowadzenie do zagadnień cyberbezpieczeństwa.

2.2. Laboratorium

Zakres laboratorium obejmuje następujące zagadnienia: Zapoznanie z pakietem Cisco Packet Tracer – budowa prostych topologii sieciowych. Konfiguracja podstawowych elementów w routerze i przełączniku sieciowym. Analiza ruchu w sieci komputerowej za pomocą programu Wireshark. Praktyczne wykonanie okablowania sieciowego. Budowa ramek – analiza danych przesyłanych przez sieć. Badanie protokołu ARP. Badanie fizycznych cech routera. Budowa sieci z przełącznikami i routerami. Badanie mechanizmu uzgadniania trójetapowego TCP. Badanie protokołów DNS, FTP i TFTP. Badanie protokołów IPv4 oraz IPv6. Konfiguracja protokołów IPv4 oraz IPv6 na urządzeniach sieciowych. Testowanie połączeń sieciowych. Projektowanie i wdrażanie schematów adresowania podsieci IPv4. Budowa sieci komputerowych z uwzględnieniem mechanizmu zmiennej długości maski. Badanie współdzielenia plików w sieci peer-to-peer. Badanie zagrożeń bezpieczeństwa sieci komputerowych. Zabezpieczanie urządzeń sieciowych. Zarządzanie plikami konfiguracji przełącznika i routera za pomocą oprogramowania emulacji terminali oraz przy użyciu TFTP, pamięci Flash i USB. Technologie IoT – projektowanie.

3. Zadania uzupełniające

Niniejsza sekcja zawiera zbiór zadań wraz z rozwiązaniami stanowiący materiały uzupełniające do przedstawianych wyżej treści w zakresie wykładów oraz laboratorium. Zadania dobrano w taki sposób, aby poruszały najbardziej istotne zagadnienia z zakresu prezentowanych wyżej treści programowych.

3.1. Analiza procesu routingu i fragmentacji

Zadanie 1: Firma X wysyła plik o rozmiarze 2000 bajtów z komputera A (10.1.1.10) do serwera B (200.2.2.50) za pomocą protokołu HTTP przez sieć, która ma dwa routery.

- Maksymalna jednostka transmisji (MTU) dla pierwszej sieci wynosi 1500 bajtów.
- MTU dla drugiej sieci (pomiędzy routerami) wynosi 1000 bajtów.
- MTU dla trzeciej sieci wynosi 1500 bajtów. Zakładamy, że nagłówek TCP ma 20 bajtów oraz nagłówek IP również 20 bajtów.

Należy opisać proces, jak pakiet HTTP zostanie podzielony (sfragmentowany) w trakcie podróży. Ile pakietów IP dotrze do serwera B? Jaki będzie rozmiar nagłówka i danych w każdym z pakietów IP? W której warstwie stosu TCP/IP odbywa się proces fragmentacji i defragmentacji?

Odpowiedź:
Główny pakiet danych ma rozmiar 2000 bajtów (czystych danych HTTP).

Pierwszy etap: Wysyłanie pakietu z komputera A (MTU = 1500). Enkapsulacja: Do danych HTTP (2000 B) dodawane są nagłówki TCP (20 B) i IP (20 B). Całkowity rozmiar pakietu to 2040 B (2000 + 20 + 20). Analiza MTU: Komputer A musi wysłać pakiet o rozmiarze 2040 B, ale MTU (Maximum Transmission Unit) w jego sieci wynosi 1500 B. Oznacza to, że pakiet musi podlegać procesowi fragmentacji.

Fragmentacja: Pakiet 1 – Nagłówek IP: 20 B, Dane: 1480 B (1500 - 20), Całkowity rozmiar: 1500 B; Pakiet 2 – Nagłówek IP: 20 B, Dane: 520 B (2000 - 1480), Całkowity rozmiar: 540 B. Zatem, dwa pakiety IP, o rozmiarach 1500 B i 540 B, są wysyłane do pierwszego routera.

Drugi etap: Router 1 (MTU = 1000).
Analiza pakietu 1 (1500 B): Router odbiera pakiet o rozmiarze 1500 B, ale MTU następnego łącza wynosi tylko 1000 B. Pakiet musi ponownie podlegać procesowi fragmentacji.

Fragmentacja: Pakiet 1a - Nagłówek IP: 20 B, Dane: 980 B (1000 - 20), Całkowity rozmiar: 1000 B; Pakiet 1b - Nagłówek IP: 20 B, Dane: 500 B (1480 - 980), Całkowity rozmiar: 520 B.

Analiza pakietu 2 (540 B): Rozmiar tego pakietu (540 B) jest mniejszy niż MTU 1000 B, więc nie jest on fragmentowany. Zatem, trzy pakiety IP, o rozmiarach 1000 B, 520 B i 540 B, są wysyłane do drugiego routera.

Trzeci etap: Router 2 (MTU = 1500)
Analiza pakietów: Wszystkie trzy pakiety, o rozmiarach 1000 B, 520 B i 540 B, są mniejsze niż MTU 1500 B. Żadna dalsza fragmentacja nie jest konieczna. Docelowo, do serwera B dotrą trzy pakiety IP.

Odpowiedzi na zadane pytania:
Opis procesu: Pakiet o rozmiarze 2040 B jest najpierw fragmentowany na 2 pakiety przez komputer A (ze względu na wielkość MTU 1500 B). Następnie, pierwszy z tych

pakietów (1500 B) jest ponownie fragmentowany przez Router 1 na 2 mniejsze pakiety (ze względu na MTU 1000 B). Drugi pakiet (540 B) przechodzi bez zmian. W sumie, jeden oryginalny pakiet generuje trzy mniejsze fragmenty. Zatem, do serwera B dotrą trzy pakiety IP.
Rozmiar nagłówka i danych w każdym docelowych pakietach wynoszą odpowiednio: Pakiet 1 (oryginalny fragment 1a) – Nagłówek IP: 20 B, Dane: 980 B; Pakiet 2 (oryginalny fragment 1b) – Nagłówek IP: 20 B, Dane: 500 B; Pakiet 3 (oryginalny fragment 2) – Nagłówek IP: 20 B, Dane: 520 B.

Proces fragmentacji odbywa się w warstwie warstwa 3. Defragmentacja następuje natomiast po dotarciu wszystkich fragmentów do hosta docelowego (serwera B), również w tej samej warstwie.

Zadanie 2: Sieć ma topologię składającą się z 4 routerów (R1, R2, R3, R4) oraz 4 podsieci (A, B, C, D).

Router	Adres IP interfejsu	Podłączona podsieć
R1	10.10.10.1	Podsieć A (10.10.10.0/24)
	172.16.1.1	Łącze do R2 (172.16.1.0/30)
R2	172.16.1.2	Łącze do R1 (172.16.1.0/30)
	172.16.2.1	Łącze do R3 (172.16.2.0/30)
R3	172.16.2.2	Łącze do R2 (172.16.2.0/30)
	172.16.3.1	Łącze do R4 (172.16.3.0/30)
	192.168.1.1	Podsieć B (192.168.1.0/24)
R4	172.16.3.2	Łącze do R3 (172.16.3.0/30)
	192.168.2.1	Podsieć C (192.168.2.0/24)
	10.10.20.1	Podsieć D (10.10.20.0/24)

Tabele routingu dla routerów 1-4:

Router	Docelowa sieć	Maska	Następny skok (next hop)	Interfejs wyjściowy
R1	10.10.10.0	255.255.255.0	-	Ethernet0
	172.16.1.0	255.255.255.252	-	Serial0
	192.168.1.0	255.255.255.0	172.16.1.2	Serial0
	192.168.2.0	255.255.255.0	172.16.1.2	Serial0
	10.10.20.0	255.255.255.0	172.16.1.2	Serial0
Router	**Docelowa sieć**	**Maska**	**Następny skok (next hop)**	**Interfejs wyjściowy**
R2	172.16.1.0	255.255.255.252	-	Serial0
	172.16.2.0	255.255.255.252	-	Serial1
	10.10.10.0	255.255.255.0	172.16.1.1	Serial0

	192.168.1.0	255.255.255.0	172.16.2.2	Serial1
	192.168.2.0	255.255.255.0	172.16.2.2	Serial1
	10.10.20.0	255.255.255.0	172.16.2.2	Serial1

Router	Docelowa sieć	Maska	Następny skok (next hop)	Interfejs wyjściowy
R3	172.16.2.0	255.255.255.252	-	Serial0
	172.16.3.0	255.255.255.252	-	Serial1
	192.168.1.0	255.255.255.0	-	Ethernet0
	10.10.10.0	255.255.255.0	172.16.2.1	Serial0
	192.168.2.0	255.255.255.0	172.16.3.2	Serial1
	10.10.20.0	255.255.255.0	172.16.3.2	Serial1

Router	Celowa sieć	Maska	Następny skok (next hop)	Interfejs wyjściowy
R4	172.16.3.0	255.255.255.252	-	Serial0
	192.168.2.0	255.255.255.0	-	Ethernet0
	10.10.20.0	255.255.255.0	-	Ethernet1
	10.10.10.0	255.255.255.0	172.16.3.1	Serial0
	192.168.1.0	255.255.255.0	172.16.3.1	Serial0

Opisz krok po kroku, w jaki sposób pakiet z hosta 10.10.10.5 w Podsieci A dociera do hosta 192.168.2.5 w Podsieci C. W opisie uwzględnij, przez które routery przechodzi pakiet i na podstawie jakich wpisów w tabeli routingu jest podejmowana decyzja.

Odpowiedź:

Analiza ścieżki pakietu (10.10.10.5 do 192.168.2.5). Start: Host 10.10.10.5 w Podsieci A chce wysłać pakiet do 192.168.2.5. Ponieważ cel jest w innej podsieci, pakiet zostaje wysłany do domyślnej bramy (10.10.10.1), czyli routera R1. Krok 1 (Router R1): R1 odbiera pakiet i analizuje docelowy adres IP (192.168.2.5). Na podstawie swojej tabeli routingu, wyszukuje sieć docelową 192.168.2.0. Odpowiedni wpis wskazuje, że następny skok (next hop) to 172.16.1.2 (adres R2), a pakiet ma być wysłany przez interfejs Serial0. Krok 2 (Router R2): R2 odbiera pakiet od R1. Na podstawie docelowego adresu 192.168.2.5, wyszukuje w swojej tabeli wpis dla sieci 192.168.2.0. Wpis wskazuje, że następny skok to 172.16.2.2 (adres R3), a pakiet ma być wysłany przez interfejs Serial1. Krok 3 (Router R3): R3 odbiera pakiet. Analizuje docelowy adres 192.168.2.5. W swojej tabeli routingu znajduje wpis dla sieci 192.168.2.0. Wpis ten wskazuje, że następny skok to 172.16.3.2 (adres R4), a pakiet

ma być wysłany przez interfejs Serial1. Krok 4 (Router R4): R4 odbiera pakiet. Analizuje adres 192.168.2.5. Ten adres należy bezpośrednio do jednej z jego podsieci (192.168.2.0/24). Router R4 wie, że host znajduje się w podsieci C, do której jest bezpośrednio podłączony, więc dostarcza pakiet bezpośrednio do hosta.

3.2. Protokół ARP

Zadanie 1: Administrator musi zdiagnozować problem z komunikacją w małej sieci biurowej. Do dyspozycji ma komputer (PC1) z adresem IP 192.168.1.100 i adresem MAC 00:1A:2B:3C:4D:5E. W tej samej sieci znajduje się serwer (SERWER) z adresem IP 192.168.1.50 i adresem MAC AA:BB:CC:DD:EE:FF. Brama domyślna (ROUTER) ma adres IP 192.168.1.1 i adres MAC 11:22:33:44:55:66. Należy przeanalizować ruch sieciowy w programie **Wireshark** i odpowiedzieć na poniższe pytania, obserwując proces, w którym PC1 próbuje nawiązać połączenie z SERWEREM. Aby wykonać zadanie należy:

- Upewnić się, że na komputerze PC1 jest wyczyszczona tablica ARP. Można to zrobić w wierszu poleceń za pomocą komendy arp -d.
- Uruchomić program Wireshark na komputerze PC1 i rozpocząć przechwytywanie pakietów na interfejsie sieciowym.
- Z wiersza poleceń na PC1 należy wysłać polecenie ping do serwera, wpisując komendę ping 192.168.1.50.
- Zatrzymać przechwytywanie pakietów w Wireshark oraz przefiltrować pakiety w Wireshark, wpisując arp w pasku filtra.

Pytania:

- Ile pakietów ARP zostało przechwyconych i jakiego są typu (request/reply)?
- Przeanalizuj pakiet ARP request oraz określ jaki jest adres MAC nadawcy (Source MAC) i odbiorcy (Destination MAC) oraz jaki jest adres IP nadawcy (Sender IP) i docelowy adres IP (Target IP)?
- Przeanalizuj pakiet ARP reply i określ jaki jest adres MAC nadawcy i odbiorcy oraz adres IP nadawcy i docelowy adres IP?
- W jaki sposób tablica ARP na PC1 została zaktualizowana po tym procesie?

Odpowiedź:

Po wykonaniu kroków opisanych w treści zadania oraz przeprowadzeniu analizy ruchu w programie Wireshark, powinny pojawić się dwa pakiety ARP.

Zostaną przechwycone dwa pakiety ARP: ARP request (żądanie ARP), ARP reply (odpowiedź ARP). Z analizy pakietu ARP request wynika, że: Source MAC:

00:1A:2B:3C:4D:5E (adres MAC komputera PC1); Destination MAC: ff:ff:ff:ff:ff:ff (adres rozgłoszeniowy, broadcast). Żądanie jest wysyłane do wszystkich urządzeń w sieci, ponieważ PC1 nie wie, który adres MAC należy do serwera; Sender IP: 192.168.1.100 (adres IP komputera PC1); Target IP: 192.168.1.50 (adres IP serwera, którego adres MAC jest poszukiwany). Z analizy pakietu ARP reply wynika, że: Source MAC: AA:BB:CC:DD:EE:FF (adres MAC serwera, który odpowiada na żądanie); Destination MAC: 00:1A:2B:3C:4D:5E (adres MAC komputera PC1); Sender IP: 192.168.1.50 (adres IP serwera); Target IP: 192.168.1.100 (adres IP komputera PC1).

Po otrzymaniu odpowiedzi ARP reply, komputer PC1 zapisuje w swojej tablicy ARP parę adresów: 192.168.1.50 jest powiązany z adresem MAC AA:BB:CC:DD:EE:FF. Dzięki temu, kolejne pakiety przeznaczone dla serwera będą mogły być wysyłane bezpośrednio, bez konieczności ponownego wysyłania żądań ARP. Można to sprawdzić, wpisując w wierszu poleceń arp -a.

Proces ten pokazuje, jak protokół ARP pozwala na dynamiczne mapowanie adresów, co jest fundamentalne dla komunikacji w sieciach lokalnych. Brak protokołu ARP uniemożliwiłby jakąkolwiek komunikację między urządzeniami w tej samej podsieci.

Zadanie 2: Użytkownik (PC1) ma problem z połączeniem się z drukarką sieciową (DRUKARKA). Obydwa urządzenia znajdują się w tej samej podsieci. PC1: Adres IP: 192.168.1.100; Adres MAC: 00:1A:2B:3C:4D:5E. DRUKARKA: Adres IP: 192.168.1.200; Adres MAC: AA:BB:CC:DD:EE:FF. Użytkownik twierdzi, że wielokrotnie próbował nawiązać połączenie z drukarką, ale bezskutecznie. Tablica ARP dla PC1 zawiera następujący, niepoprawny wpis:

Interface: 192.168.1.100

Internet Address	Physical Address	Type
192.168.1.200	CC:CC:CC:CC:CC:CC	dynamic

Pytania:

- Dlaczego użytkownik nie może połączyć się z drukarką, pomimo że jego komputer zna jej adres IP?
- Co spowodowało, że tablica ARP zawiera błędny adres MAC? Jaka jest jedna z najczęstszych przyczyn?
- Jakie działanie powinien podjąć technik, aby rozwiązać problem tymczasowo?
- Jaki jest prawidłowy wpis w tablicy ARP dla drukarki?

Odpowiedź:

Użytkownik nie może połączyć się z drukarką, ponieważ jego komputer (PC1) ma w swojej tablicy ARP błędne mapowanie adresu IP drukarki na adres MAC. Zgodnie z tablicą, komputer próbuje wysłać pakiety do adresu MAC CC:CC:CC:CC:CC:CC, który nie należy do drukarki, zamiast do poprawnego adresu AA:BB:CC:DD:EE:FF. W efekcie, pakiety nie docierają do celu. Najczęstszą przyczyną pojawienia się nieprawidłowego wpisu w tablicy ARP jest atak typu ARP spoofing (ARP poisoning). W takim ataku, złośliwe urządzenie w sieci wysyła fałszywe odpowiedzi ARP, podając swój własny adres MAC jako adres MAC innego urządzenia (w tym przypadku drukarki). Komputer ofiary (PC1) aktualizuje swoją tablicę ARP z nieprawidłowymi danymi, co powoduje przekierowanie całego ruchu na adres atakującego.

Aby tymczasowo rozwiązać problem, technik powinien wyczyścić tablicę ARP na komputerze użytkownika. W systemach Windows można to zrobić za pomocą komendy w wierszu poleceń: arp -d 192.168.1.200. Po wyczyszczeniu wpisu, gdy użytkownik spróbuje ponownie połączyć się z drukarką, jego komputer wyśle nowe żądanie ARP (ARP request), a drukarka odpowie poprawnym adresem MAC. Wtedy w tablicy ARP pojawi się prawidłowy wpis.

Po prawidłowym rozwiązaniu, tablica ARP na PC1 powinna wyglądać następująco:

Interface: 192.168.1.100

Internet Address	Physical Address	Type
192.168.1.200	AA:BB:CC:DD:EE:FF	dynamic

3.3. Ramka Ethernet

Zadanie 1: Administrator sieci przechwytuje ruch sieciowy za pomocą programu Wireshark. Jego zadaniem jest przeanalizowanie struktury ramki Ethernet i obliczenie jej całkowitego rozmiaru po dodaniu narzutu protokołu. Przechwycona ramka danych ma następujące parametry: Adres MAC docelowy: 00:0A:95:9D:68:16; Adres MAC źródłowy: 00:1B:77:E5:2C:9A; Typ protokołu: 0x0800 (IP); Rozmiar danych (Payload): 1000 bajtów.

Pytania:

- Wymień nazwy i rozmiary w bajtach dla wszystkich pól ramki Ethernet, które są wymagane do poprawnego przesłania pakietu.
- Jaki jest całkowity rozmiar całej ramki w bajtach, włączając w to dane i wszystkie pola?
- Jaka jest minimalna i maksymalna wielkość ramki Ethernet (bez preambuły i Start of Frame Delimiter)?
- Jaki jest cel pola CRC (Cyclic Redundancy Check)?

Odpowiedź:

Pola ramki Ethernet mają następujące rozmiary: Adres docelowy (Destination MAC): 6 bajtów; Adres źródłowy (Source MAC): 6 bajtów; Typ/Długość (Type/Length): 2 bajty; Dane (Payload): od 46 do 1500 bajtów; Suma kontrolna (FCS - Frame Check Sequence): 4 bajty. Przed ramką występują jeszcze Preamble (7 bajtów) i Start of Frame Delimiter (SFD) (1 bajt), które służą do synchronizacji odbiornika, ale nie są uwzględniane w ogólnym rozmiarze ramki.

Aby obliczyć całkowity rozmiar ramki, należy zsumować rozmiary wszystkich pól, włącznie z danymi (payload).

Rozmiar ramki = (Adres docelowy) + (Adres źródłowy) + (Typ/Długość) + (Dane) + (FCS), zatem Rozmiar ramki = 6 B+6 B+2 B+1000 B+4 B = 1018 B

Minimalna wielkość ramki: 64 bajty. Jest to suma wszystkich stałych pól (18 bajtów) plus minimalna wielkość danych (46 bajtów). Jeśli dane mają mniej niż 46 bajtów, są uzupełniane (padded) do tej minimalnej wartości. Maksymalna wielkość ramki: 1518 bajtów. Jest to suma stałych pól (18 bajtów) plus maksymalna wielkość danych (1500 bajtów). Ramki o większym rozmiarze nazywane są jumbo frames.

Pole CRC (Cyclic Redundancy Check), ma na celu wykrycie błędów w transmisji danych. Nadawca oblicza wartość CRC na podstawie wszystkich pól ramki i umieszcza ją w tym polu. Odbiornik po otrzymaniu ramki ponownie oblicza tę wartość. Jeśli obliczona wartość nie zgadza się z wartością w polu CRC, oznacza to, że ramka została uszkodzona podczas transmisji i zostanie odrzucona. Jest to prosty, ale skuteczny mechanizm zapewniający integralność danych.

3.4. Protokoły TCP i UDP

Zadanie 1: Programista pracuje nad aplikacją klient-serwer. Jego zadaniem jest przeanalizowanie procesu nawiązywania połączenia TCP. W tym celu używa programu Wireshark, aby przechwycić ruch sieciowy między klientem a serwerem.
KLIENT: Adres IP: 192.168.1.100; Numer portu: 51234 (port efemeryczny),
SERWER: Adres IP: 192.168.1.50, Numer portu: 80 (usługa HTTP).

Pytania:

- Należy wymienić i opisać, jakie pakiety są wysyłane w procesie trzykrotnego uzgadniania połączenia TCP, wraz z flagami TCP, które są w nich ustawione.
- Jaki jest cel tego procesu?
- Załóżmy, że klient wysyła pakiet SYN z numerem sekwencyjnym 1000. Jaki numer sekwencyjny i potwierdzenia (ACK) znajdzie się w odpowiedzi serwera (SYN-ACK)?
- W jaki sposób TCP zapewnia niezawodność, jeśli któryś z tych pakietów zaginie?

Odpowiedź:

Proces nawiązywania połączenia TCP składa się z trzech etapów:

- SYN (Synchronize): Klient wysyła pakiet do serwera, aby zainicjować połączenie. W tym pakiecie ustawiona jest flaga SYN. Klient proponuje początkowy numer sekwencyjny, który ma być używany do śledzenia przesyłanych bajtów.
- SYN-ACK (Synchronize-Acknowledge): Serwer odbiera pakiet SYN, ustawia flagę SYN oraz flagę ACK (potwierdzenie), aby potwierdzić otrzymanie pakietu klienta. Jednocześnie wysyła swój własny początkowy numer sekwencyjny i potwierdza numer sekwencyjny klienta.
- ACK (Acknowledge): Klient odbiera pakiet SYN-ACK, ustawia flagę ACK i wysyła potwierdzenie do serwera. Po tym etapie połączenie jest w pełni nawiązane i gotowe do wymiany danych.

Głównym celem trzykrotnego uzgadniania połączenia jest wzajemna synchronizacja numerów sekwencyjnych między klientem a serwerem. Bez tej synchronizacji, obydwa urządzenia nie wiedziałyby, które bajty danych zostały już wysłane i odebrane. Proces ten pozwala na ustalenie początkowych numerów sekwencyjnych, które będą używane do śledzenia przepływu danych i zapewnienia, że wszystkie pakiety zostaną dostarczone w prawidłowej kolejności.

Pakiet SYN (od klienta): Numer sekwencyjny (Seq): 1000;
Pakiet SYN-ACK (od serwera): Numer sekwencyjny (Seq): Serwer wybiera swój własny, losowy początkowy numer sekwencyjny, np. 5000; Numer potwierdzenia (Ack): Serwer ustawia numer potwierdzenia na 1001 (numer sekwencyjny klienta + 1), aby potwierdzić, że otrzymał bajt danych od klienta i oczekuje następnego.

Jeśli jeden z pakietów (SYN, SYN-ACK lub ACK) zaginie w trakcie transmisji, protokół TCP włącza mechanizm retransmisji. Każdy wysłany segment ma przypisany licznik czasu (timeout). Jeśli nadawca nie otrzyma potwierdzenia w określonym czasie, zakłada, że pakiet zaginął i wysyła go ponownie. Dzięki temu, nawet w przypadku błędów w sieci, połączenie zostanie nawiązane i dane zostaną przesłane niezawodnie.

Zadanie 2: Technik, który analizuje ruch sieciowy z gry online przechwycił segment UDP: Komputer gracza (KLIENT): Adres IP: 192.168.1.100, Numer portu: 60000 (port efemeryczny); Serwer gry (SERWER): Adres IP: 123.45.67.89, Numer portu: 27015 (standardowy port serwera gry); Segment UDP (Payload): 500 bajtów danych.

Pytania:

- Wymień i opisz, z jakich pól składa się nagłówek UDP i jaki jest rozmiar każdego z nich w bajtach.
- Oblicz całkowity rozmiar segmentu UDP (nagłówek + dane) w bajtach dla podanych danych.
- Wyjaśnij, dlaczego protokół UDP jest preferowany w przypadku gier online, a TCP nie.
- W jakich innych aplikacjach, oprócz gier, UDP jest często wykorzystywany i dlaczego?

Odpowiedź:

Nagłówek protokołu UDP jest bardzo prosty i składa się zaledwie z czterech pól, z których każde ma stały rozmiar: Port źródłowy (Source Port): 2 bajty. Identyfikuje port aplikacji, która wysłała segment UDP. Port docelowy (Destination Port): 2 bajty. Identyfikuje port aplikacji, do której przeznaczony jest segment. Długość (Length): 2 bajty. Określa całkowitą długość nagłówka UDP i danych (payload) w bajtach. Suma kontrolna (Checksum): 2 bajty. Opcjonalne pole, które służy do wykrywania błędów w nagłówku i danych. Zazwyczaj używane do zapewnienia integralności danych, chociaż nie gwarantuje retransmisji.

Aby obliczyć całkowity rozmiar segmentu UDP, należy zsumować rozmiar nagłówka i rozmiar danych (payload). Rozmiar nagłówka UDP = 2 B + 2 B + 2 B + 2 B = 8 bajtów; Rozmiar danych (Payload) = 500 bajtów; Całkowity rozmiar segmentu = Rozmiar nagłówka + Rozmiar danych; Całkowity rozmiar segmentu = 8 B+500 B=508 bajtów

W grach online kluczowym czynnikiem jest niski czas opóźnienia. Nawet milisekundy mają znaczenie. UDP jest idealny do tego celu, ponieważ jest bezpołączeniowy, tzn. nie wymaga trójstopniowego uzgadniania połączenia, co eliminuje dodatkowe opóźnienia na początku komunikacji. Ponadto, nie ma mechanizmów kontroli niezawodności, czyli nie wysyła potwierdzeń (ACK) ani nie ponawia transmisji utraconych pakietów. W przypadku, gdy gracz porusza się, a pakiet z informacją o jego starej pozycji zostanie utracony, bardziej efektywne jest przesłanie nowego pakietu z jego aktualną pozycją niż retransmisja starego. Nowsza informacja jest po prostu bardziej wartościowa. Użycie TCP spowodowałoby opóźnienia, ponieważ protokół ten wstrzymywałby grę w oczekiwaniu na potwierdzenie lub retransmisję zagubionych pakietów.

UDP jest często wykorzystywany w aplikacjach, gdzie szybkość jest ważniejsza niż pewność dostarczenia i gdzie utrata danych jest akceptowalna, np.: Transmisja głosu i wideo (VoIP, streaming): Utrata kilku pakietów w strumieniu audio lub wideo jest często niezauważalna dla użytkownika, a opóźnienie spowodowane retransmisją byłoby znacznie gorsze. DNS (Domain Name System): Zapytania DNS są proste i składają się z pojedynczych pakietów. UDP jest używany, aby szybko uzyskać odpowiedź; w przypadku jej braku, klient może po prostu ponowić zapytanie. DHCP (Dynamic Host Configuration Protocol): Służy do automatycznego przydzielania adresów IP. Protokół ten musi działać szybko i sprawnie w sieciach lokalnych, a prostota UDP doskonale się do tego nadaje.

3.5. Protokół IP v 4

Zadanie 1: Przedstaw w postaci binarnej następujące adresy IPv4.

A. 10.150.25.1
B. 172.30.200.5
C. 195.8.12.254
D. 1.1.1.1 (adres powszechnie używany jako jeden z publicznych serwerów DNS)
E. 127.0.0.1 (lokalny adres pętli zwrotnej – localhost)
F. 255.255.255.255 (adres rozgłoszeniowy dla sieci lokalnej – broadcast)

Odpowiedź:

A. 00001010.10010110.00011001.00000001
B. 10101100.00011110.11001000.00000101
C. 11000011.00001000.00001100.11111110
D. 00000001.00000001.00000001.00000001
E. 01111111.00000000.00000000.00000001
F. 11111111.11111111.11111111.11111111

Zadanie 2: Mając podany adres IP 192.168.10.50 z maską podsieci /28 oblicz:

A. Oblicz adres sieci
B. Oblicz adres rozgłoszeniowy (broadcast)
C. Podaj zakres adresów IP, które mogą być przypisane do hostów
D. Jaka jest całkowita liczba adresów w tej podsieci?

Odpowiedź:

Maska /28 oznacza, że 28 bitów jest przypisanych do części sieciowej adresu IP v 4, co w notacji dziesiętnej zapiszemy jako 255.255.255.240. Zatem adres IP v 4 w postaci binarnej zapiszemy jako 11000000.10101000.00001010.00110010, natomiast maskę podsieci jako 11111111.11111111.11111111.11110000.

A. Wykonujemy operację logiczną AND na adresie IP i masce podsieci, co prowadzi do wyznaczenia adresu sieci w postaci: 192.168.10.48
B. Mając adres sieci, w części hosta zmieniamy wszystkie bity (w tym przypadku ostatnie 4 bity) na wartość 1. Adres rozgłoszeniowy to 192.168.10.63.
C. Zakres adresów IP, które mogą być przypisane do hostów obejmuje obszar pomiędzy adresem sieci, a adresem rozgłoszeniowym, czyli od 192.168.10.49 do 192.168.10.62.
D. Całkowita liczba adresów w sieci obliczana jest jako 2^4, czyli 16 (gdzie 4, oznacza liczbę bitów w części hosta).

3.6. Podział sieci na podsieci

Zadanie 1: Firma posiada adres sieciowy 192.168.50.0/24. Dział IT chce podzielić sieć na 4 równe podsieci, aby oddzielić ruch sieciowy pomiędzy poszczególnymi wydziałami.

A. Określ, ile bitów z części hosta adresu IP v 4 należy pożyczyć, aby wydzielić 4 wymagane w treści zadania podsieci?
B. Jaka będzie nowa maska podsieci w notacji CIDR oraz dziesiętnej?
C. Podaj adresy sieciowe dla każdej z 4 nowych podsieci.

Odpowiedź:

A. Aby stworzyć 4 podsieci, musimy pożyczyć 2 bity z części hosta, ponieważ $2^2=4$
B. Nowa maska podsieci: Oryginalna maska to /24. Dodajemy 2 pożyczone bity: /24 + 2 = /26. Notacja dziesiętna: /26 oznacza 26 bitów jedynek. Oktety 1-3: 255.255.255. Oktet 4: Ostatnie 2 bity to bity sieciowe, a 6 to bity hosta. Binarne: 11000000. Dziesiętnie: 128+64=192. Nowa maska to 255.255.255.192 lub /26.
C. Adresy sieciowe nowych podsieci to:
   - Podsieć 1: 192.168.50.0 /26
   - Podsieć 2: 192.168.50.64 /26
   - Podsieć 3: 192.168.50.128 /26
   - Podsieć 4: 192.168.50.192 /26

Zadanie 2: Firma posiada dostęp do publicznego adresu sieciowego 203.0.113.0/24 i potrzebuje podzielić go na kilka podsieci, aby obsłużyć różne działy, z których każdy ma inne zapotrzebowanie na liczbę hostów. Dział sprzedaży (Sales): 100 hostów, dział marketingu (Marketing): 50 hostów, dział HR (Human Resources): 20 hostów oraz wymagane są połączenia między routerami w postaci 2 osobnych podsieci. Zaplanuj podział sieci, stosując VLSM (Variable Length Subnet Masking), aby zminimalizować pulę niewykorzystanych adresów IP. Dla każdej podsieci podaj: adres sieci (w notacji CIDR), maskę podsieci, zakres użytecznych adresów hostów oraz Adres rozgłoszeniowy (broadcast).

Odpowiedź:

Projektowanie zaczynamy od największej podsieci, aby zminimalizować niewykorzystane adresy IP.

- Dział Sprzedaży (100 hostów): wymagana liczba adresów: 102 (100 hostów + adres sieci + adres rozgłoszeniowy). Najbliższa potęga dwójki to 2^7=128. Potrzebujemy 7 bitów hosta. Maska podsieci: 32−7=25. Maska /25, czyli maska w zapisie dziesiętnym to: 255.255.255.128, natomiast Adres sieci to: 203.0.113.0/25. Zakres hostów: 203.0.113.1 do 203.0.113.126. Adres rozgłoszeniowy: 203.0.113.127

Kolejne podsieci obejmują działy marketingu oraz HR

- Dział Marketingu (50 hostów). Wymagana liczba adresów: 52 (50 hostów + 2). Najbliższa potęga dwójki to 2^6=64. Potrzebujemy 6 bitów hosta. Maska podsieci: 32−6=26. Maska /26 czyli 255.255.255.192. Adres sieci: 203.0.113.128/26 (po adresie broadcast 203.0.113.127). Zakres hostów: 203.0.113.129 do 203.0.113.190. Adres rozgłoszeniowy: 203.0.113.191
- Dział HR (20 hostów). Wymagana liczba adresów: 22 (20 hostów + 2). Najbliższa potęga dwójki to 2^5=32. Potrzebujemy 5 bitów hosta. Maska podsieci: 32−5=27. Maska /27 czyli 255.255.255.224. Adres sieci: 203.0.113.192/27 (po adresie broadcast 203.0.113.191). Zakres hostów: 203.0.113.193 do 203.0.113.222. Adres rozgłoszeniowy: 203.0.113.223.

Ostatnim etapem jest przypisanie adresacji na potrzeby połączeń pomiędzy routerami.

- Połączenia między routerami (2x po 2 hosty). Wymagana liczba adresów dla każdej z podsieci: 4 (2 hosty + 2). Najbliższa potęga dwójki to 2^2=4. Potrzebujemy 2 bity hosta. Maska podsieci: 32−2=30. Maska /30 czyli 255.255.255.252.
  - Podsieć 1: Adres sieci: 203.0.113.224/30. Zakres hostów: 203.0.113.225 do 203.0.113.226. Adres rozgłoszeniowy: 203.0.113.227
  - Podsieć 2: Adres sieci: 203.0.113.228/30. Zakres hostów: 203.0.113.229 do 203.0.113.230. Adres rozgłoszeniowy: 203.0.113.231.

Zadanie 3: Administrator sieci przygotował następujący plan adresacji dla sieci 172.20.0.0/16, ale popełnił błędy.

A. Podsieć A: 172.20.10.0/25
B. Podsieć B: 172.20.10.128/25
C. Podsieć C: 172.20.10.200/26
D. Podsieć D: 172.20.10.230/27

Wskaż, które z podsieci nakładają się na siebie, wyjaśnij, dlaczego ten plan adresacji jest błędny oraz zaproponuj poprawiony, poprawny plan adresacji, który wykorzysta te same maski podsieci, ale bez nakładania się adresów.

Odpowiedź:

Nakładające się podsieci to:

- Adres sieci Podsieci B to 172.20.10.128/25. Zakres hostów to 172.20.10.129 do 172.20.10.254, a adres rozgłoszeniowy to 172.20.10.255.
- Adres sieci Podsieci C to 172.20.10.200/26. Zakres hostów to 172.20.10.193 do 172.20.10.254, a adres rozgłoszeniowy to 172.20.10.255.
- Podsieć C zaczyna się od 172.20.10.192, który znajduje się w zakresie Podsieci B. Adres sieci 172.20.10.200 nie jest prawidłowym adresem sieciowym dla maski /26 (zakresy to 0, 64, 128, 192).

Błąd: Adresy Podsieci B, C i D nakładają się na siebie. Adresy sieci podane dla Podsieci C i D nie są prawidłowe dla tych masek. Adres sieci musi być pierwszą wartością w bloku adresów, a jego część hosta musi składać się z samych zer. Poprawiony plan adresacji przedstawiał będzie się następująco:

- Podsieć A (/25): Adres sieci: 172.20.10.0/25, zakres hostów: 172.20.10.1 - 172.20.10.126.
- Podsieć B (/25): Adres sieci: 172.20.10.128/25, zakres hostów: 172.20.10.129 - 172.20.10.254.
- Podsieć C (/26): Nowa, prawidłowa adresacja po Podsieci B. Adres sieci: 172.20.11.0/26.
- Podsieć D (/27): Nowa, prawidłowa adresacja po Podsieci C. Adres sieci: 172.20.11.64/27.

Zadanie 4: Masz adres sieciowy 192.168.1.0/24 należy podzielić go na 4 podsieci o następującej liczbie hostów:

- Podsieć 1: 50 hostów.
- Podsieć 2: 25 hostów.
- Podsieć 3: 10 hostów.
- Podsieć 4: 5 hostów.

Należy, używając mechanizmu VLSM przyporządkować odpowiednią maskę podsieci do każdego z przypadków oraz wypełnić tabelę z danymi dla każdej podsieci, zawierającą: wymaganą liczbę hostów, minimalną maskę podsieci, nowy adres sieci w notacji CIDR oraz zakres adresów hostów i adres rozgłoszeniowy.

Wskazówka: Aby zminimalizować pulę niewykorzystanych adresów, należy zacząć od przydzielania adresów dla największych podsieci.

Odpowiedź:

Podsieć	Liczba hostów	Obliczona maska podsieci	Adres sieci (CIDR)	Zakres adresów hostów	Adres rozgłoszeniowy (broadcast)
1	50	/26 (255.255.255.192)	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
2	25	/27 (255.255.255.224)	192.168.1.64/27	192.168.1.65 - 192.168.1.94	192.168.1.95
3	10	/28 (255.255.255.240)	192.168.1.96/28	192.168.1.97 - 192.168.1.110	192.168.1.111
4	5	/29 (255.255.255.248)	192.168.1.112/29	192.168.1.113 - 192.168.1.118	192.168.1.119

Uzasadnienie:

- Podsieć 1 (50 hostów): Aby pomieścić 50 hostów, potrzebujemy co najmniej 2^6=64 adresów. Odejmujemy dwa adresy specjalne (sieci i broadcast) i otrzymujemy 62 adresy dla hostów. Wymaga to 6 bitów hosta, co daje maskę /26 (32−6=26).
- Podsieć 2 (25 hostów): Potrzebujemy co najmniej 2^5=32 adresów. Po odjęciu dwóch adresów specjalnych, pozostaje 30 adresów dla hostów. Wymaga to 5 bitów hosta, co daje maskę /27 (32−5=27).
- Podsieć 3 (10 hostów): Potrzebujemy co najmniej 2^4=16 adresów. Po odjęciu dwóch adresów specjalnych, pozostaje 14 adresów dla hostów. Wymaga to 4 bitów hosta, co daje maskę /28 (32−4=28).
- Podsieć 4 (5 hostów): Potrzebujemy co najmniej 2^3=8 adresów. Po odjęciu dwóch adresów specjalnych, pozostaje 6 adresów dla hostów. Wymaga to 3 bitów hosta, co daje maskę /29 (32−3=29).

Dzięki zastosowaniu VLSM i rozpoczynaniu podziału od największej podsieci, minimalizujemy liczbę niewykorzystanych adresów IP, co jest kluczową zaletą tego podejścia.

Zadanie 5: Firma technologiczna ma cztery oddziały w różnych miastach, połączone ze sobą za pomocą routerów. Otrzymali od dostawcy usług internetowych (ISP) adres sieciowy 198.51.100.0/22 do zarządzania całą infrastrukturą. W ramach tego adresu, każdy oddział oraz połączenia między nimi muszą mieć swoje podsieci. Administrator zdefiniował następujące wymagania minimalne dla poszczególnych oddziałów: Oddział A: 250 hostów, Oddział B: 100 hostów, Oddział C: 50 hostów, Oddział D: 20 hostów. Wymagania dla połączeń WAN (router-router) określił jako: Połączenie 1: Między Oddziałem A oraz Oddziałem B (2 hosty), Połączenie 2: Między Oddziałem B oraz Oddziałem C (2 hosty), Połączenie 3: Między Oddziałem C oraz Oddziałem D (2 hosty).
Należy zaplanować adresację dla wszystkich oddziałów i połączeń WAN, używając techniki VLSM, aby w pełni wykorzystać dostępną przestrzeń adresową i nie dopuścić do zbędnego niewykorzystywania adresów IP. Dla każdej podsieci należy obliczyć i podać:

- Adres sieci (w notacji CIDR).
- Maskę podsieci (w notacji dziesiętnej z kropkami).
- Pierwszy i ostatni użyteczny adres hosta.
- Adres rozgłoszeniowy (broadcast).
- Ile niewykorzystanych adresów IP pozostało w głównej puli po zakończeniu podziału.

Wskazówka: Główny adres sieciowy 198.51.100.0/22 oznacza, że można wykorzystać adresy z zakresu od 198.51.100.0 do 198.51.103.255.

Odpowiedź:

Główna pula adresów to 198.51.100.0/22, co odpowiada masce 255.255.252.0. Daje nam to 10 bitów w części hosta, czyli 210=1024 adresy IP do podziału. Podział należy zacząć od największych podsieci.

Oddział A (250 hostów)

- Wymagana liczba adresów: 252 (250+2).
- Najbliższa potęga dwójki: 2^8=256. Potrzeba 8 bitów hosta.
- Maska: 32−8=24. Maska /24 (255.255.255.0).

- Adres sieci: 198.51.100.0/24
- Pierwszy host: 198.51.100.1
- Ostatni host: 198.51.100.254
- Adres rozgłoszeniowy: 198.51.100.255

Oddział B (100 hostów)

- Wymagana liczba adresów: 102 (100+2).
- Najbliższa potęga dwójki: 2^7=128. Potrzeba 7 bitów hosta.
- Maska: 32−7=25. Maska /25 (255.255.255.128).
- Adres sieci: 198.51.101.0/25 (następny wolny blok po 198.51.100.255)
- Pierwszy host: 198.51.101.1
- Ostatni host: 198.51.101.126
- Adres rozgłoszeniowy: 198.51.101.127

Oddział C (50 hostów)

- Wymagana liczba adresów: 52 (50+2).
- Najbliższa potęga dwójki: 2^6=64. Potrzeba 6 bitów hosta.
- Maska: 32−6=26. Maska /26 (255.255.255.192).
- Adres sieci: 198.51.101.128/26 (po 198.51.101.127)
- Pierwszy host: 198.51.101.129
- Ostatni host: 198.51.101.190
- Adres rozgłoszeniowy: 198.51.101.191

Oddział D (20 hostów)

- Wymagana liczba adresów: 22 (20+2).
- Najbliższa potęga dwójki: 2^5=32. Potrzeba 5 bitów hosta.
- Maska: 32−5=27. Maska /27 (255.255.255.224).
- Adres sieci: 198.51.101.192/27 (po 198.51.101.191)
- Pierwszy host: 198.51.101.193
- Ostatni host: 198.51.101.222
- Adres rozgłoszeniowy: 198.51.101.223

Połączenia WAN (3x po 2 hosty)

- Wymagana liczba adresów dla każdego połączenia: 4 (2+2).
- Najbliższa potęga dwójki: 2^2=4. Potrzeba 2 bity hosta.
- Maska: 32−2=30. Maska /30 (255.255.255.252).

Połączenie 1 (A-B):

- Adres sieci: 198.51.101.224/30
- Pierwszy host: 198.51.101.225

- Ostatni host: 198.51.101.226
- Adres rozgłoszeniowy: 198.51.101.227

Połączenie 2 (B-C):

- Adres sieci: 198.51.101.228/30
- Pierwszy host: 198.51.101.229
- Ostatni host: 198.51.101.230
- Adres rozgłoszeniowy: 198.51.101.231

Połączenie 3 (C-D):

- Adres sieci: 198.51.101.232/30
- Pierwszy host: 198.51.101.233
- Ostatni host: 198.51.101.234
- Adres rozgłoszeniowy: 198.51.101.235

Niewykorzystane adresy IP

- Całkowita liczba adresów w puli /22 to 2^{10}=1024.
- Liczba wykorzystanych adresów w zakresie poszczególnych oddziałów i połączeń to:
  - Oddział A: 256
  - Oddział B: 128
  - Oddział C: 64
  - Oddział D: 32
  - Połączenia WAN: 3×4=12
- Suma wykorzystanych: 256+128+64+32+12=492.
- Pozostałe niewykorzystane adresy: 1024−492=532.

W wyniku podziału, firma posiada jeszcze 532 wolne adresy IP w swojej puli, które może wykorzystać na przyszły rozwój.

3.7. Protokół IP v 6

Zadanie 1: Proszę zoptymalizować zapis następujących adresów IPv6:

A. 2001:0db8:0000:0000:0000:0000:1428:57ab
B. fe80:0000:0000:0000:2000:0000:0000:0001
C. 2001:0db8:0000:0000:a123:0000:0000:0001
D. 2001:00db:0000:000a:001a:0000:0000:0001
E. 001:0db8:234a:0001:0010:0001:0123:0001
F. fe80:0000:0000:0000:0000:0000:0000:0001 (link-loca

G. 0000:0000:0000:0000:0000:0000:0000:0001 (loopback)
H. 0000:0000:0000:0000:0000:0000:0000:0000 (unspecified)
I. 2001:0db8:a0b1:0000:1234:0000:0000:0001

Wyjaśnij, które reguły zostały zastosowane.

Odpowiedź:

A. Adres można skrócić, usuwając wiodące zera z każdej sekcji (hektetu). Można także użyć podwójnego dwukropka :: do reprezentacji jednej lub więcej kolejnych sekcji złożonych z samych zer. W tym przypadku adres ma cztery kolejne sekcje zer. Rozwiązanie: 2001:db8::1428:57ab.
B. Adres zawiera ciąg kolejnych hekstetów zerowych. Zgodnie z zasadami kompresji, można użyć :: do zastąpienia najdłuższej grupy zerowych hekstetów. W tym przypadku jest to sekcja 0000:0000:0000 na początku adresu. Po usunięciu wiodących zer i zastosowaniu kompresji otrzymujemy: fe80::2000:0:0:1.
C. Adres zawiera dwie grupy po dwa hekstety zerowe. Standard RFC 5952 rekomenduje, aby w przypadku równych grup zer, użyć podwójnego dwukropka :: do skompresowania pierwszej z nich. Ostateczny zapis będzie następujący: 2001:db8::a123:0:0:1. Alternatywnie, poprawnym rozwiązaniem będzie także 2001:db8:0:0:a123::1, choć zazwyczaj preferuje się kompresję pierwszej grupy.
D. Należy usunąć wiodące zera z każdego hekstetu (np. 00db staje się db, a 000a staje się a). Następnie, skompresuj najdłuższą grupę kolejnych hekstetów zerowych, w tym przypadku są to dwie sekcje 0000:0000. Ostateczny zapis to: 2001:db:0:a:1a::1.
E. W podanym adresie nie występują żadne kolejne hekstety zerowe, więc użycie podwójnego dwukropka :: jest niemożliwe. Jedyną formą kompresji jest usunięcie wiodących zer z poszczególnych hekstetów. Po tym zabiegu adres przyjmuje postać: 2001:db8:234a:1:10:1:123:1.
F. Adresy link-local często zawierają długie sekwencje zer. Zgodnie z zasadami kompresji, najdłuższy ciąg zer może zostać zastąpiony przez ::. Jest to jeden z najczęstszych przypadków skracania adresów. Skrócona forma to fe80::1.
G. Adres pętli zwrotnej (loopback) to jeden z najprostszych do skrócenia adresów, ponieważ składa się głównie z zer. Cały adres, z wyjątkiem ostatniego hekstetu, to same zera, więc można go skompresować do ::1.

H. Adres niezdefiniowany w IPv6 składa się wyłącznie z samych zer, co umożliwia maksymalną kompresję. Skrócona forma to ::.
I. Ten przykład pokazuje sytuację, w której mamy dwie grupy zer, ale jedna jest dłuższa od drugiej. Zgodnie z zasadą, należy skompresować dłuższą grupę, co prowadzi do zastąpienia dwóch ostatnich hekstetów zerowych przez ::. Skrócona forma to 2001:db8:a0b1:0:1234::1.

Zadanie 2: Określ typ adresu IPv6:

A. 2001:0db8:85a3::8a2e:0370:7334
B. fe80::203:ff:fe58:1234
C. ff02::1
D. ::
E. ::1

Odpowiedź:

A. global unicast
B. link-local
C. multicast
D. unspecified
E. loopback

Zadanie 3: Znając adres MAC 00-25-96-ff-fe-12-34-56, utwórz adres link-local IPv6, stosując format EUI-64.

Odpowiedź:

Aby utworzyć adres IPv6 link-local z adresu MAC, należy zastosować metodę EUI-64 (Extended Unique Identifier-64), określoną w RFC 4291. Jest to proces dwuetapowy. W kroku 1 następuje podział i wstawienie identyfikatora w oparciu o 48 bitowy adres MAC. Aby przekształcić adres MAC w 64-bitowy identyfikator interfejsu (Interface ID), należy podzielić go na dwie równe części i wstawić w środek 16-bitową wartość szesnastkową FFFE. W kroku 2 należy odwrócić (zmienić na przeciwną) wartość siódmego bitu wiodącego oktetu (pierwszego bajtu) adresu MAC. Ten bit określa, czy adres jest unikalny globalnie, czy też lokalnie administrowany. Jest to standardową operacją.

Zatem, dla zadanego przykładu:

- W kroku 1 następuje konwersja MAC do EUI-64: W adresie MAC 00-25-96-ff-fe-12-34-56 wstawiamy FFFE w środku i odwracamy 7 bit wiodącego oktetu (00 staje się 02). Wynik to 0225:96ff:fe12:3456.
- W kroku 2 tworzymy adres typu link-local: Prefix fe80::/64 + EUI-64. Pełny adres: fe80::225:96ff:fe12:3456.

Zadanie 4: Utwórz adres global unicast korzystając z danych zadania 3 oraz zakładając, że adres sieci to 2001:db8:a0b1:1::/64.

Odpowiedź:

Tworząc adres typu global unicast: do prefixu sieci 2001:db8:a0b1:1::/64 dodajemy EUI-64 otrzymując pełny adres IPv6 w postaci 2001:db8:a0b1:1:225:96ff:fe12:3456.

Zadanie 5: Administrator sieci ma za zadanie skonfigurować prostą sieć opartą na protokole IPv6. Jego firma otrzymała globalny prefiks 2001:db8:a0b:12f0::/64. Należy przydzielić adresy do dwóch sieci lokalnych i skonfigurować routing. Założenia: Prefiks globalny: 2001:db8:a0b:12f0::/64; Sieć A (LAN1): Adresy hostów z tej sieci będą miały prefiks 2001:db8:a0b:12f0::/64; Sieć B (LAN2): Adresy hostów z tej sieci będą miały prefiks 2001:db8:a0b:12f1::/64.

Pytania:

- Czym różni się adresacja IPv6 od IPv4. Podaj przykład adresu IPv6 i wyjaśnij, jak można go skrócić.
- Wyznacz adresy interfejsów routera (R1), który łączy Sieć A i Sieć B. Przyjmij, że do połączenia między routerami używane są osobne podsieci o prefiksie 2001:db8:a0b:12f2::/64.
- Jak działa proces konfiguracji adresu IPv6 w sieci lokalnej w dwóch przypadkach: DHCPv6 i SLAAC.

Odpowiedź:

Główna różnica polega na długości adresu: IPv4: 32-bitowy, zapisywany w postaci dziesiętnej (np. 192.168.1.1); IPv6: 128-bitowy, zapisywany w postaci heksadecymalnej, podzielony na 8 grup po 16 bitów (np.

2001:0db8:0a0b:12f0:0000:0000:0000:0001). Skracanie adresu IPv6: Adresy IPv6 można skracać, eliminując zera wiodące i kompresując ciągi zer.

W sieciach IPv6, routery pełnią rolę bramy domyślnej, a ich interfejsy otrzymują adresy z przydzielonego prefiksu. Często przyjmuje się, że adres interfejsu bramy jest pierwszym lub ostatnim adresem hosta w podsieci. Interfejs R1 (połączony z Siecią A): Adres: 2001:db8:a0b:12f0::1 (użycie ::1 jest częstą praktyką dla bram domyślnych). Interfejs R1 (połączony z Siecią B): Adres: 2001:db8:a0b:12f1::1. Interfejs R1 (połączony z siecią routingu): Adres: 2001:db8:a0b:12f2::1

DHCPv6: W tym modelu, adresy IPv6 są centralnie zarządzane przez serwer DHCPv6. Klient wysyła zapytanie do serwera DHCPv6, a serwer przydziela mu pełny adres IPv6, maskę podsieci, adresy serwerów DNS oraz inne parametry. Jest to podobne do działania protokołu DHCP w IPv4 i zapewnia pełną kontrolę administratora nad pulą adresów.

SLAAC: SLAAC pozwala hostom na automatyczną konfigurację adresów bez potrzeby serwera. Proces działa w dwóch krokach: W pierwszym, router wysyła wiadomość Router Advertisement (RA), która zawiera prefiks sieci (np. 2001:db8:a0b:12f0::/64). W drugim hosty generują część interfejsową adresu (ostatnie 64 bity) na podstawie swojego adresu MAC (przy użyciu formatu EUI-64) lub losowo. Hosty łączą prefiks z routera z częścią interfejsową, tworząc swój unikalny adres globalny. SLAAC jest prostszy i bardziej skalowalny niż DHCPv6.

4. Literatura

[1] Wendell Odom, David Hucaby, Jason Gooley, CCNA 200-301 Official Cert Guide Library, 2nd Edition, Cisco Press, 2024.
[2] Wendell Odom, CCNA 200-301 Official Cert Guide, Volume 1, Cisco Press, 2024
[3] Allan Johnson, 31 Days Before your CCNA Exam: A Day-By-Day Review Guide for the CCNA 200-301 Certification Exam, Cisco Press, 2024
[4] Andrea, Harris, CCNA 200-301 Lab Guide Book with Packet Tracer, 2022 Downloadable Labs: Step-by-Step Practical Labs for CCNA Practise
[5] Adam Józefiok, CCNA 200-301. Zostań administratorem sieci komputerowych Cisco. Wydanie II, Helion, 2025.
[6] Materiały Akademii Sieci Cisco zawarte na platformie NetaCad udostępniane studentom na czas trwania zajęć.