

## 2.3 Komunikacja w sieci LAN

E. Odpowiedz na pytania:

### b) Co się dzieje po uruchomieniu polecenia **ping**? (analiza przechwyconych pakietów)

Po uruchomieniu polecenia ping , komputer inicjuje wysłanie pakietów sieciowych do przypisanego adresu IP lub nazwy domenowej. Głównym celem polecenia ping jest sprawdzenie dostępności i opóźnienia sieciowego dla danego hosta.

### c) Jakimi danymi dysponuje komputer a jakie musi zdobyć, żeby poprawnie wysłać pakiet w sieci lokalnej?

Aby poprawnie wysłać pakiet w sieci lokalnej, komputer musi dysponować pewnymi danymi i zdobyć inne informacje. Adres IP komputera: Każdy komputer w sieci lokalnej ma przypisany unikalny adres ip, dysponuje adresami IP innych urządzeń w sieci lokalnej, adres mac.

Informacje które komputer musi zdobyć:

Aby wysłać pakiet do innego urządzenia w sieci lokalnej komputer musi zdobyć adres IP docelowego urządzenia, adres mac, adres IP bramy domyślnej routera.

Poprzez posiadanie tych danych i zdobyciu wymaganych informacji, komputer będzie w stanie poprawnie wysłać pakiety w sieci lokalnej.

### e) Jakie urządzenia są potrzebne aby komputery w sieci LAN mogły się ze sobą komunikować?

Aby komputery w sieci lokalnej mogły się ze sobą komunikować, potrzebne są następujące urządzenia:

- Komputery
- przełącznik switch
- kable ethernet
- router
- modem
- serwer

Wszystkie te urządzenia współpracują, aby umożliwić komunikację między komputerami w sieci LAN.

## 2.4 Sprawdzenie dostępności serwera **helios**.

E. Odpowiedz na pytania:

### b) Co się dzieje po uruchomieniu polecenia **ping**? Dlaczego tak się dzieje? (analiza pakietów).

Po uruchomieniu polecenia ping , komputer inicjuje wysłanie pakietów sieciowych do przypisanego adresu IP lub nazwy domenowej. Głównym celem polecenia ping jest sprawdzenie dostępności i opóźnienia sieciowego dla danego hosta.

### c) Jaki jest zasięg adresów IP (OSI: W. sieci) oraz adresów MAC (OSI: W. Łączy danych)?

Zasięg adresów IP i adresów MAC różni się w kontekście warstw modelu OSI. Adresy IP są używane w warstwie sieci (warstwa 3) modelu OSI. Adresy IP mają globalny zasięg i są wykorzystywane do unikalnej identyfikacji urządzeń w sieciach IP takich jak internet.

Adresy MAC są używane w warstwie łącza danych(warstwa 2) modelu OSI. Adresy mac mają lokalny zasięg i są przypisywane do interfejsów sieciowych na fizycznym poziomie. Są one wykorzystywane do identyfikacji urządzeń w obrębie jednej sieci lokalnej (LAN).

Podsumowując:

- Adresy IP mają globalny zasięg i są używane w warstwie sieci(warstwa 3) do identyfikacji urządzeń w sieciach IP(np. Internet)
- Adresy MAC mają lokalny zasięg i są używane w warstwie łącza danych(warstwa 2) do identyfikacji urządzeń w obrębie jednej sieci lokalnej(LAN).

## **2.8 Komunikacja komputer-serwer WWW**

. Na podstawie przechwyconych pakietów odpowiedz na pytania:

### **a) Jakie operacje muszą być wykonane aby została wysłana wiadomość echo request?**

Aby została wysłana wiadomość Echo request konieczne są niestępujące operacje:

- Tworzenie pakietu ICMP
- Określenie adresu IP docelowego
- Wybór interfejsu sieciowego
- Tworzenie ramki sieciowej
- Wysłanie ramki sieciowej
- Odbiór i przetworzenie przez host docelowy

W ten sposób wiadomość Echo request jest wysyłana do hosta docelowego, a później host docelowy może odpowiedzieć wiadomością echo reply.

**Narysuj graf przepływu pakietów.**

### **b) Do czego służy protokół DNS?**

Protokół DNS służy do przekładania nazw domenowych na adresy IP i odwrotnie. Jest to system Rozwiązywania nazw używany w sieciach komputerowych, w tym w internecie. Głównym celem protokołu DNS jest ułatwienie komunikacji między urządzeniami poprzez umożliwienie identyfikacji hostów za pomocą czytelnych nazw domenowych, zamiast korzystania z trudnych do zapamiętania adresów IP.

### **c) Jaki protokół warstwy transportowej używany jest do przenoszenia wiadomości DNS?**

Protokół warstwy transportowej używany do przenoszenia wiadomości DNS to protokół UDP. UDP jest często wybierany jako preferowany protokół do przesyłania pakietów DNS ze względu na jego prostotę, niski narzut i szybkość.

### **d) Który port używany jest przez serwer DNS?**

Serwery DNS używają dwóch głównych portów, w zależności od rodzaju komunikacji: Port 53 jest najczęściej używanym portem przez serwery DNS do nasłuchiwania i obsługi zapytań DNS przy użyciu protokołu TCP.

### **e) Jaki numer portu używany jest przez lokalny komputer?**

243

### **f) Czy serwer DNS znajduje się w sieci lokalnej**

Serwer DNS może znajdować się w sieci lokalnej i w tym przypadku znajduje się sieci LAN pod nazwą wiii.local.

### **j) Z ilu bajtów składają się wiadomości protokołu DNS?**

Wiadomości protokołu DNS składają się z 12 bajtów.

### **k) Z ilu bajtów składają się wiadomości protokołu ARP?**

Wiadomości protokołu ARP składają się z nagłówka ARP, który ma stały rozmiar 28 bajtów.

**l) Co znajduje się w polu danych wybranej wiadomości DNS, ARP i ICMP?**

Pole danych w wiadomości DNS.

W przypadku wiadomości DNS, pole danych zawiera informacje takie jak:

- Zapytania DNS(Zawiera nazwę domeny)
- Odpowiedzi DNS(zawiera rekordy DNS).

Pole danych w wiadomości ARP

W przypadku wiadomości ARP, pole danych zawiera:

- Adres MAC nadawcy
- Adres IP nadawcy
- Adres MAC docelowego sprzętu.

Pole danych w wiadomości ICMP

W przypadku wiadomości ICMP, pole danych zawiera:

- wiadomości echo request i echo reply
- wiadomości o błędzie(typ3)
- inne typy wiadomości ICMP.

**m) Ile pakietów musi wysłać komputer zanim zacznie się łączyć z serwerem WWW?**

Aby nawiązać połączenie z serwerem www, komputer musi przeprowadzić pewną sekwencję wymiany pakietów zgodnie z protokołem HTTP. W przypadku korzystania z protokołu HTTP1.1 i protokołu transportowego TCP, zwykle zachodzi proces nazywany „Trzykrotnym uderzeniem” który obejmuje wysłanie trzech pakietów w celu nawiązania połączenia. W związku z tym, aby nawiązać połączenie z serwerem WWW przy użyciu tego protokołu, komputer musi wysłać co najmniej trzy pakiety: SYN, SYN-ACK i ACK.

## **4 ROUTERY CZ.1**

### **4.4**

**c)Jaka jest składnia polecenia ping?**

Składnia polecenia ping składa się:

ping [opcje] [adres docelowy]

Gdzie:

‘ping’ to polecenie służące do wysyłania zapytań ICMP Echo Request i oczekiwania na odpowiedzi ICMP Echo Reply.

‘[opcje]’ to opcjonalne parametry, które można podać, aby dostosować działanie polecenia ping.

**d) Wprowadź polecenie ping i wciśnij klawisz ENTER. Jakie są dodatkowe opcje polecenia?**

```

C:\Users\Mateusz>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
           [-r count] [-s count] [[-j host-list] | [-k host-list]]
           [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
           [-4] [-6] target_name

Options:
    -t                Ping the specified host until stopped.
                      To see statistics and continue - type Control-Break;
                      To stop - type Control-C.
    -a                Resolve addresses to hostnames.
    -n count          Number of echo requests to send.
    -l size           Send buffer size.
    -f                Set Don't Fragment flag in packet (IPv4-only).
    -i TTL            Time To Live.
    -v TOS            Type Of Service (IPv4-only. This setting has been deprecated
and has no effect on the type of service field in the IP
Header).
    -r count          Record route for count hops (IPv4-only).
    -s count          Timestamp for count hops (IPv4-only).
    -j host-list      Loose source route along host-list (IPv4-only).
    -k host-list      Strict source route along host-list (IPv4-only).
    -w timeout        Timeout in milliseconds to wait for each reply.
    -R                Use routing header to test reverse route also (IPv6-only).
                      Per RFC 5095 the use of this routing header has been
                      deprecated. Some systems may drop echo requests if
                      this header is used.
    -S srcaddr        Source address to use.
    -c compartment    Routing compartment identifier.
    -p                Ping a Hyper-V Network Virtualization provider address.
    -4                Force using IPv4.
    -6                Force using IPv6.

```

Dodatkowe opcje polecenia ping to:

‘-t’ - kontynuuj wysyłanie pakietów ping do momentu przerwania przez użytkownika (nieskończony ping)

‘-n count’ - określ liczbę pakietów ping do wysłania, gdzie ‘count’ to liczba pakietów

‘-l size’ - określ rozmiar pakietu ping, gdzie ‘size’ to liczba bajtów.

‘-f’ - ustaw flagę „Nie fragmentuj” w pakietach ping.

‘-4’ - użyj protokołu IPv4.

‘-6’ - użyj protokołu IPv6.

‘-a’ - wyświetl nazwę komputera docelowego dla podanego adresu IP.

‘-w timeout’ - określ czas oczekiwania na odpowiedź w milisekundach.

#### e) Jaka jest składnia polecenia **tracert**?

Dla systemów opartych na systemie Windows składnia występuje następująco:

Tracert [opcje] [adres docelowy]

Np. ‘tracert www.wp.pl

#### g) Jaka jest składnia polecenia **ipconfig**?

Dla systemów opartych na systemie Windows składnia wygląda następująco:

Ipconfig [opcje].

Gdzie:

‘ipconfig’ to polecenie służące do wyświetlania informacji o konfiguracji interfejsów sieciowych.

‘[opcje]’ to opcjonalne parametry, które można podać, aby dostosować wyświetlane informacje.

#### 4.5

Sprawdzić, jakie są dostępne opcje polecenia **show**.

```
C:\Users\Mateusz>ipconfig show

Error: unrecognized or incomplete command line.

USAGE:
    ipconfig [/allcompartments] [/? | /all |
        /renew [adapter] | /release [adapter] |
        /renew6 [adapter] | /release6 [adapter] |
        /flushdns | /displaydns | /registerdns |
        /showclassid adapter |
        /setclassid adapter [classid] |
        /showclassid6 adapter |
        /setclassid6 adapter [classid] ]

where
    adapter          Connection name
                     (wildcard characters * and ? allowed, see examples)

Options:
    /?              Display this help message
    /all            Display full configuration information.
    /release        Release the IPv4 address for the specified adapter.
    /release6       Release the IPv6 address for the specified adapter.
    /renew          Renew the IPv4 address for the specified adapter.
    /renew6         Renew the IPv6 address for the specified adapter.
    /flushdns       Purges the DNS Resolver cache.
    /registerdns     Refreshes all DHCP leases and re-registers DNS names
    /displaydns     Display the contents of the DNS Resolver Cache.
    /showclassid    Displays all the dhcp class IDs allowed for adapter.
    /setclassid     Modifies the dhcp class id.
    /showclassid6   Displays all the IPv6 DHCP class IDs allowed for adapter.
    /setclassid6    Modifies the IPv6 DHCP class id.

The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.
```

For Release and Renew, if no adapter name is specified, then the IP address leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.

Examples:

> ipconfig	... Show information
> ipconfig /all	... Show detailed information
> ipconfig /renew	... renew all adapters
> ipconfig /renew EL*	... renew any connection that has its name starting with EL
> ipconfig /release *Con*	... release all matching connections, eg. "Wired Ethernet Connection 1" or "Wired Ethernet Connection 2"
> ipconfig /allcompartments	... Show information about all compartments
> ipconfig /allcompartments /all	... Show detailed information about all compartments

#### 4.6

Korzystając z systemu pomocy wyjaśnij do czego służą polecenia:

a.)**show version;**

Polecenie „show version” w routerze Cisco IOS jest używane do wyświetlania informacji dotyczących wersji oprogramowania, konfiguracji urządzenia, sprzętu oraz innych szczegółowych informacji dotyczących routera.

b.)**show IP route;**

Wyświetla tablicę routingu IP, która zawiera informacje o dostępnych trasach dla pakietów IP w routerze. Pokazuje, jakie sieci są dostępne i przez które interfejsy można nimi dotrzeć.

c.)**show running-config;**

Wyświetla bieżącą konfigurację urządzenia. Pokazuje wszystkie bieżące ustawienia i konfigurację, które są obecnie w użyciu na routerze.

d.)**show startup-config;**

Wyświetla zawartość pliku konfiguracyjnego startup-config. Plik ten zawiera konfigurację, która jest ładowana przy uruchomieniu routera.

e.)**show flash;**

Wyświetla zawartość pamięci flash w routerze. Pamięć ta służy do przechowywania różnych danych, takich jak obraz systemu operacyjnego, pliki konfiguracyjne, pliki firmware, obrazy IOS.

f.)**show interfaces.**

Służy do wyświetlania informacji o wszystkich interfejsach routera, takich jak status, typ, prędkość, adresy IP. Pozwala to monitorować i diagnozować stan interfejsów sieciowych w routerze.

#### 4.12

##### D) Odpowiedz na pytania

a) Co ile sekund router wysyła wiadomość cdp i po jakim czasie informacja o urządzeniu sąsiednim zostanie usunięta? (polecenie **show cdp**);

Router Cisco IOS wysyła domyślnie komunikaty CDP co 60 sekund na wszystkich aktywnych interfejsach. Jeśli chodzi o czas przechowywania informacji o sąsiednich urządzeniach, to domyślnie informacje są przechowywane przez 180 sekund. Po tym czasie informacje o urządzeniu sąsiednim zostaną usunięte z tablicy CDP.

**b) Czy router wysyła wiadomości CDP do sieci LAN? Jak można to sprawdzić? Jak zbudowana**

**jest wiadomość protokołu CDP?**

Tak, router Cisco IOS wysyła wiadomości CDP do sieci LAN. Aby sprawdzić czy router wysyła te wiadomości, można skorzystać z polecenia „show cdp neighbors” lub „show cdp neighbors detail”. Te polecenia wyświetlają informacje o sąsiednich urządzeniach, z którymi router nawiązał połączenie za pomocą CDP.

Wiadomość protokołu CDP jest strukturą binarną składającą się z tych pól informacyjnych.

Każde pole ma ustalony format i długość, co umożliwia interpretację i analizę wiadomości przez urządzenia sieciowe obsługujące CDP.

#### 4.13

##### Tablica routingu

Aby wyświetlić tablicę routingu należy użyć polecenia **show IP route**. Odpowiedz na pytania:

**a) Jakie informacje można znaleźć w tablicy routingu?**

W tablicy routingu można znaleźć informacje takie jak:

- Sieć docelowa
- Maska podsieci
- Adres bramy
- Interfejs wyjściowy
- Metryka
- Protokół routingu
- Typ trasy

W tablicy routingu mogą być również zawarte dodatkowe informacje, takie jak czas ostatniej aktualizacji trasy, status trasy (aktywna, wygasła itp), metryka szczegółowa (dla niektórych protokołów routingu )

**b) Które informacje są niezbędne do podjęcia decyzji o routingu?**

Podjęcie decyzji o routingu opiera się na kilku kluczowych informacjach takich jak:

- Adres docelowy ( W opraciu o ten adres router podejmuje decyzję, do której sieci należy przekierować pakiet)
- Informacje zawarte w tablicy routingu ( zawierają informacje o dostępnych trasach sieciowych)
- Protokoły routingu(router musi mieć informację o dostępnych trasach w sieci, aby móc podjąć decyzję o wyborze najlepszej trasy)
- Metryki ( są używane do określenia kosztu trasy i wyboru najlepszej trasy).
- Interfejsy sieciowe (router musi wiedzieć które interfejsy sieciowe są dostępne i w jakich sieciach się znajdują).

**e) Czy na podstawie tablicy routingu można narysować mapę sieci?**

Na podstawie tablicy routingu nie można narysować mapy sieci ponieważ tablica routingu nie zawiera wystarczających informacji do bezpośredniego narysowania dokładnej mapy sieci.

Tablica routingu dostarcza informacji o dostępnych trasach i interfejsach ale nie zawiera szczegółowych danych topologicznych ani fizycznych rozmieszczenia urządzeń sieciowych.

## ROUTERY CZ.2

### 4.3 Aktualna konfiguracja

#### a) Jakie informacje dotyczące interfejsów znajdują się w pliku konfiguracyjnym?

W pliku konfiguracyjnym routera Cisco IOS mogą znajdować się informacje dotyczące interfejsów takie jak:

- Nazwa interfejsu
- Adres IP
- Maska podsieci
- Stan interfejsu
- Tryb interfejsu
- Prędkość
- Protokoły i usługi
- VLANy
- ACL
- Parametry dodatkowe ( dodatkowe parametry konfiguracyjne).

### 4.6 Konfiguracja interfejsów szeregowych

#### d) Czy możliwe jest sprawdzenie dostępności interfejsu Fast Ethernet sąsiedniego routera?

Dlaczego?

Tak, możliwe jest sprawdzenie dostępności interfejsu Fast Ethernet sąsiedniego routera. Można to zrobić za pomocą narzędzi diagnostycznych, takich jak polecenie ping lub polecenie show interface. Polecenie ping pozwala na wysłanie pakietów ICMP echo request do adresu IP sąsiedniego routera na konkretnym interfejsie. Jeśli odpowiedź jest otrzymywana, oznacza to , że interfejs Fast Ethernet sąsiedniego routera jest dostępny i odpowiada na pakiety ICMP.

### 4.7 Konfiguracja protokołu routingu

#### a) Informacje o jakich sieciach znajdują się w tablicy routingu (**show ip route**)?

W poleceniu ‘show ip route’ w routerze możemy znaleźć informacje o różnych rodzajach sieci takie jak:

- Sieć docelowa
- Maska podsieci
- Interfejs wyjściowy
- Nex Hop (kolejny skok)
- Metric(Metryka)
- Typ ścieżki
- Czas życia (Liczba skoków )
- Flags (flagi)
- Adresy sąsiadów.

Tablica routingu (show ip route) zawiera informacje o różnych sieciach i trasach, które są dostępne w routerze.