Sieci komputerowe – konwersatorium 4

Jarosław Szkoła

Wybrane protokoły modelu ISO/OSI

Wstęp

- Agenda
  - Model ISO/OSI
  - Stos TCP/IP
  - Protokół ARP
  - Protokół IPv4
  - Protokół ICMP

Model ISO/OSI

Model ISO/OSI	
Warstwa	Znaczenie
7. Aplikacji	Pozwala korzystać z sieci użytkownikom
6. Prezentacji	Określa format danych oraz ich kodowanie
5. Sesji	Zarządza sesjami użytkowników
4. Transportowa	Odpowiada za sprawną obsługę komunikatów
3. Sieci	Określa trasę przesyłanych danych
2. Łącza danych	Kontroluje dostęp do medium transmisyjnego
1. Fizyczna	Koduje dane w postaci bitów i przekazuje do medium

Wybrane warstwy modelu ISO/OSI

- Warstwy pierwsza i druga modelu ISO/OSI odpowiadają za budowę fizycznej infrastruktury sieciowej
- Warstwa trzecia (sieci) zapewnia obsługę protokołów sieciowych, co umożliwia właściwą komunikację
- Komunikacja może być również zapewniona przez wyższe warstwy modelu ISO/OSI
- Do celów komunikacyjnych stosuje się protokół IP który wraz z innymi protokołami występującymi w stosie protokołów TCP/IP stanowi podstawę współczesnych sieci komputerowych

Stos TCP/IP

- Stos protokołów TCP/IP jest zestawem kilku protokołów sieciowych zaprojektowanych do komunikowania się komputerów w dużych, rozległych sieciach WAN
- Protokoły TCP/IP zostały po raz pierwszy zastosowane w roku 1969 w ramach projektu ARPANET

Stos TCP/IP

- Model logiczny stosu protokołów TCP/IP składa się z czterech warstw:
  - Warstwy aplikacji
  - Warstwy transportowej
  - Warstwy internetowej
  - Warstwy interfejsu sieciowego

- Protokoły TCP/IP zostały po raz pierwszy zastosowane w roku 1969 w ramach projektu ARPANET

Stos TCP/IP

Warstwy modelu ISO/OSI	Warstwy stosu TCP/IP
Warstwa aplikacji Warstwa prezentacji Warstwa sesji	Warstwa aplikacji
Warstwa transportowa	Warstwa transportowa
Warstwa sieci	Warstwa internetu
Warstwa łącza Warstwa fizyczna	Warstwa interfejsu sieciowego

Każda z warstw stosu TCP/IP odpowiada jednej lub kilku warstwom modelu ISO/OSI

Stos TCP/IP – warstwy i protokoły

Warstwy stosu TCP/IP	Protokoły stosu TCP/IP TCP	Protokoły stosu TCP/IP UDP
Warstwa aplikacji	Telnet, FTP, SMTP	DNS, RIP, SNMP
Warstwa transportowa	TCP	UDP
Warstwa internetu	ARP	ICMP, IGMP
Warstwa interfejsu sieciowego	Ethernet, Token Ring	Frame Relay, ATM

Stos TCP/IP - warstwy

- Warstwa interfejsu sieciowego
  - Odpowiada za przekazywanie i odbieranie pakietów z kanału transmisyjnego
  - Stos protokołów TCP/IP został tak zaprojektowany, aby uniezależnić się od rodzaju kanału komunikacyjnego, formatu ramki fizycznej, czy architektury sieciowej
  - Dzięki temu TCP/IP może być stosowany w sieciach wykorzystujących różne technologie tj.
    - Ethernet
    - Token Ring
    - X.25
    - Frame Relay
    - ATM

Stos TCP/IP - warstwy

- Warstwa internetowa
  - Jest odpowiedzialna za adresowanie, podział na pakiety oraz routing (trasowanie). W skład tej warstwy wchodzą następujące protokoły:
    - Protokół IP (Internet Protokol), odpowiada za prawidłowe adresowanie pakietów oraz dostarczanie ich do miejsca przeznaczenia
    - Protokół ARP (Address Resolution Protokol), odpowiada za identyfikacje sprzętowego adresu interfejsu sieciowego komputera docelowego (identyfikacja MAC)
    - Protokół ICMP (Internet Control Message Protocol) odpowiada za diagnozowanie transmisji datagramów IP oraz raportowanie o błędach, które mogą się pojawić w trakcie przesyłania pakietów IP
    - Protokół IGMP (Internet Group Management Protocol) odpowiada za rozsyłanie informacji w trybie multicast

Stos TCP/IP - warstwy

- Warstwa transportowa
  - Jest odpowiedzialna za poprawną komunikację między komputerami w sieci oraz przepływ danych między warstwą internetową a warstwa aplikacji
  - Do podstawowych protokołów warstwy transportowej należą:
    - Protokół TCP
    - Protokół UDP

Stos TCP/IP - warstwy

- Warstwa transportowa
  - Protokół TCP (Transmission Control Protocol)
    - TCP odpowiada za bezbłędne dostarczanie informacji. Charakteryzuje się następującymi cechami:
      - Jest zorientowany na połączenie: oznacza to, że program użytkowy, który chce skorzystać z protokołu TCP musi najpierw zwrócić się do odbiorcy z prośbą o uzyskanie połączenia i uzyskać jego zgodę,
      - Jest protokołem typu punkt-punkt: oznacza to, że każde połączenie TCP ma dokładnie dwa końce
      - Zapewnia niezawodność: oznacza to, że protokół TCP gwarantuje dostarczenie pakietów

Stos TCP/IP - warstwy

- Warstwa transportowa
  - Protokół TCP (Transmission Control Protocol)
    - TCP odpowiada za bezbłędne dostarczanie informacji. Charakteryzuje się następującymi cechami:
      - Zapewnia dwukierunkową komunikację: oznacza to, że komunikacja w połączeniu TCP odbywa się w dwóch kierunkach, od nadawcy do odbiorcy i na odwrót,
      - Zapewnia strumieniowy interfejs: oznacza to, że program może wysyłać połączeniem całą sekwencję bajtów, w konsekwencji prowadzi to do tego, że dane nie muszą być dostarczane do odbiorcy w kawałkach tych samych wielkości, w których zostały wysłane,
      - Zapewnia łagodne kończenie połączenia: oznacza to, że protokół gwarantuje niezawodne dostarczenie pakietów przez zamknięciem połączenia

Stos TCP/IP - warstwy

- Warstwa transportowa
  - Protokół TCP
    - Retransmisja
      - Jednym z mechanizmów zapewnienia niezawodności transportu danych jest retransmisja
      - Mechanizm polega na tym, że odbiorca po odebraniu danych zobowiązany jest do przesłania do nadawcy potwierdzenia odebrania danych
      - Jeśli potwierdzenie nie nadejdzie w określonym czasie, to nadawca wysyła dane ponownie
      - Czas na wysłanie potwierdzenia jest dobierany dynamicznie w zależności od przepustowości sieci

Stos TCP/IP - warstwy

- Warstwa transportowa
  - Protokół TCP
    - Okna: Inny mechanizm pozwalający na kontrolę przepływu danych
      - Każdy z komputerów uczestniczący w połączeniu TCP dysponuje swoim własnym buforem danych
      - Dane oczekują w buforze na przyjęcie ich przez odpowiednią aplikację
      - Bufor ma ograniczony rozmiar
      - Komputer odbiorcy wraz z potwierdzeniem otrzymania danych wysyła dodatkowo informację o wolnym rozmiarze bufora czyli o oknie
      - Jeśli odbiorca nie jest w stanie czytać nadchodzących danych tak szybko jak nadchodzą, to za którymś razem wyśle do nadawcy informację o zerowym rozmiarze okna. Jest to sygnał dla nadawcy, że ma przerwać nadawanie. Przerwa trwa aż do momentu, gdy odbiorca ponownie prześle niezerowy rozmiar okna

Stos TCP/IP - warstwy

- Warstwa transportowa
  - Protokół UDP (User Datagram Protocol)
    - UDP odpowiada za za dostarczenie danych, ale nie gwarantuje jednak niezawodności ich dostarczenia
    - W przeciwieństwie do protokołu TCP, UDP nie potrzebuje zestawiać połączenia między nadawcą a odbiorcą – protokół bezpołączeniowy
    - Istnieją aplikacje, które do pracy nie potrzebują odporności na błędy transmisji i stabilności protokołu TCP
    - Koszt transmisji dla protokołu TCP jest wyższy niż dla protokołu UDP
    - UDP zapewnia zawodne usługi połączeniowe na protokołem IP

Stos TCP/IP - warstwy

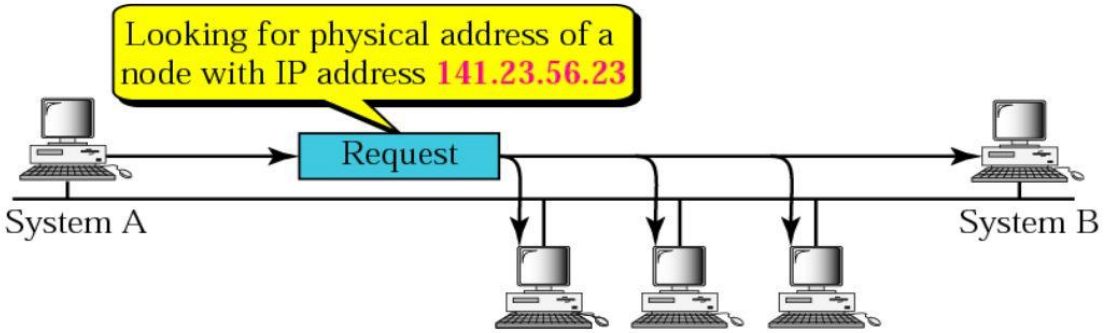
- Warstwa internetu
  - Protokół ARP
    - ARP jest protokołem odwzorowywania adresów
      - Protokół ARP definiuje dwa rodzaje komunikatów:
        - » Pytanie o adres MAC
        - » Odpowiedź
    - Komunikat ARP transmitowany jest wewnątrz ramki sprzętowej (pole danych)
    - Informacja o tym, że przesyłany jest komunikat ARP zawarta jest w nagłówku ramki w polu określającym typ ramki (wartość 0x806)

Stos TCP/IP - warstwy

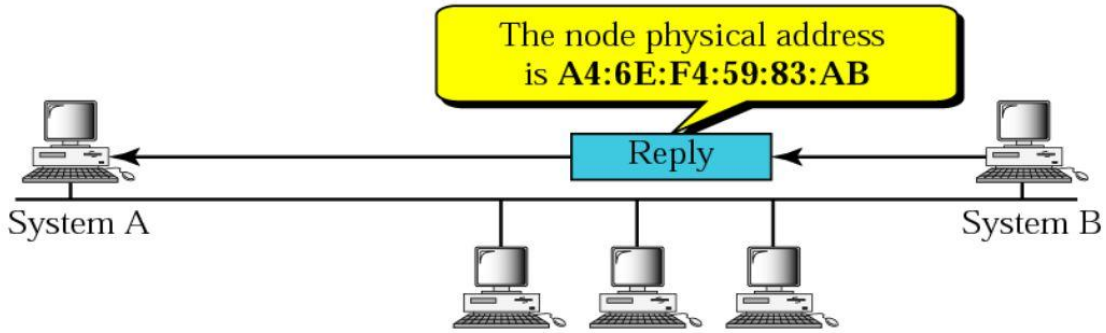
- Warstwa internetu
  - Protokół ARP
    - W celu wysłania pakietu z danymi musi być ustalony adres MAC odpowiadający adresowi IP
    - Protokół ARP działa w ten sposób, że odpytuje kolejno wszystkie komputery w sieci, czy mają potrzebny mu adres IP, i prosi o przesłanie odpowiedniego adresu MAC
    - Aby ograniczyć ruch w sieci budowana jest dynamiczna tablica ARP, w które są zapisywane pary adresów IP oraz MAC komputerów, z którymi udało się nawiązać kontakt
    - Tablica taka ma jednak ograniczony rozmiar
    - Jeśli tablica ARP się przepełni, to jest z niej usuwany najstarszy wpis

Stos TCP/IP - warstwy

- Protokół ARP – przykładowa sesja



a. ARP request is broadcast



b. ARP reply is unicast

Stos TCP/IP - warstwy

- Protokół ARP – przykładowa sesja
  - System A sprawdza, czy posiada wpis w tablicy dla adresu IP: 141.23.56.23
  - Jeśli posiada wpis, to algorytm kończy działanie
  - Jeśli nie posiada odpowiedniego wpisu, to wysyła zapytanie do sieci
  - Każdy z komputerów sprawdza swój adres IP
  - Komputer, którego adres IP pasuje do adresu 141.23.56.23 odsyła odpowiedź w postaci swojego adresu MAC - A4:6E:F4:59:83:AB
  - Do tablicy ARP zostaje dodany nowy wpis łączący adres IP z adresem MAC: [141.23.56.23 -> A4:6E:F4:59:83:AB]
  - Jeśli nastąpi ponowne zapytanie o ten sam adres IP, i odpowiedni wpis będzie dostępny w tablicy ARP, to zostanie zwrócona wartości z tablicy tymczasowej

Protokół IP

- Protokół IP nie posiada mechanizmów sygnalizujących błędy oraz mechanizmów umożliwiających kontrolowanie przepływu pakietów.
- Z tego względu zgłaszaniem problemów z przesyłaniem datagramów oraz sterowaniem zajmuje się protokół ICMP
- Innym protokołem, który umożliwia bardziej efektywne rozsyłanie pakietów jest protokół IGMP. Protokół ten działa w oparciu o adresy rozsyłania grupowego.
- Powszechnie stosowaną wersją protokołu IP jest wersja 4. Jednak ze względu na ograniczenia dotyczące adresowania logicznego spowodowane niedostateczną, w stosunku do potrzeb, liczbą bitów przeznaczonych na adres IP protokół ten będzie zastąpiony nowszą wersją IPv6.

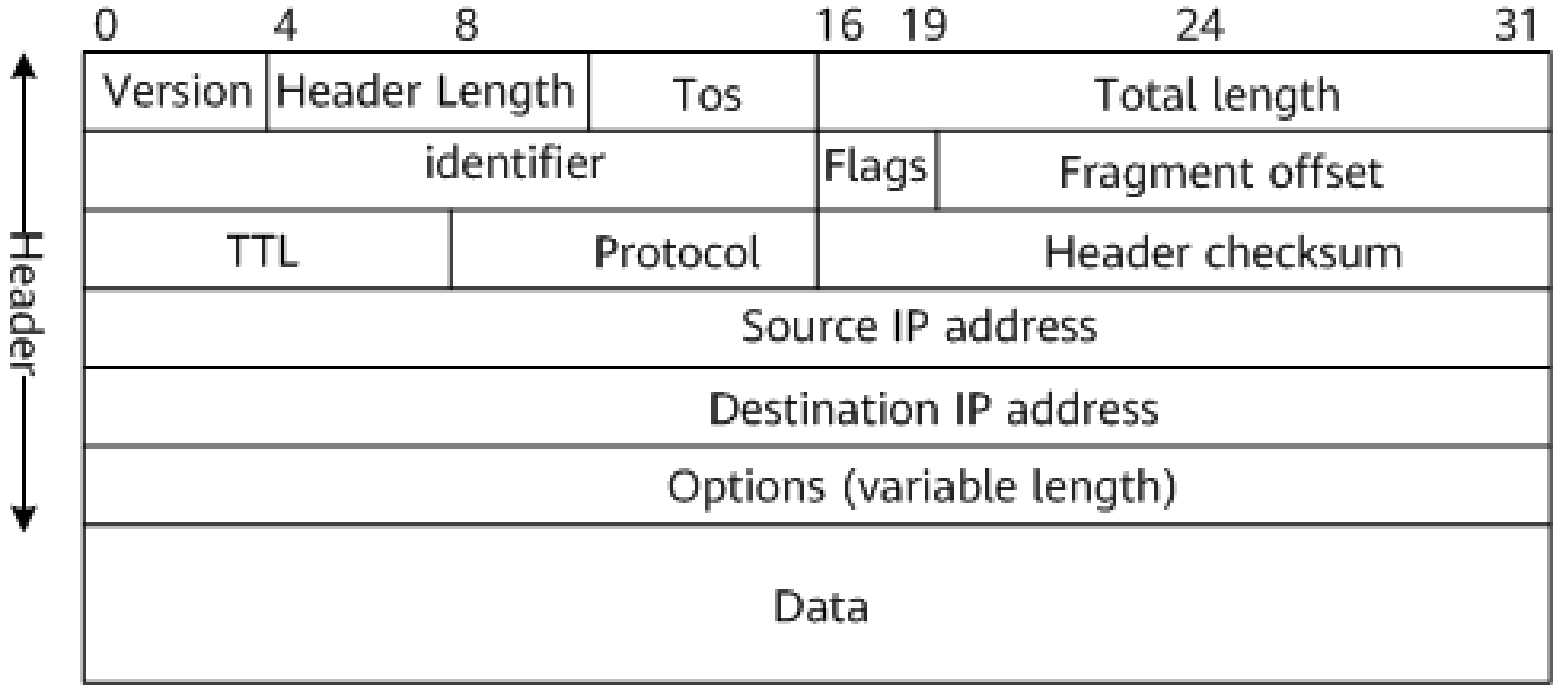
Protokół IPv4

- Protokół IPv4 został szczegółowo opisany w dokumencie RFC 791.
- Sam protokół IP został opracowany jak odporny na błędy i potrafiący pracować w trudnych warunkach
- W normalnych warunkach jego funkcja sprowadza się do wyboru optymalnej trasy i przesyłania nią pakietów
- W przypadku wystąpienia awarii, na którymś z połączeń protokół będzie próbował dostarczyć pakiety trasami alternatywnymi (nie zawsze optymalnymi)
- Protokół IP jest podstawowym protokołem przesyłania pakietów w Internecie
- Protokół IP jest protokołem bezpołączeniowym. Oznacza to, że w celu przesłania pakietów nie jest nawiązywane połączenie z hostem docelowym

Protokół IPv4

- Pakiety mogą być przesyłane różnymi trasami do miejsca przeznaczenia, gdzie są następnie składane w całość. Podobna zasada działa przy przesyłaniu listów tradycyjnym systemem pocztowym. Tutaj również w momencie wysyłania listu adresat nie musi potwierdzać, że przesyłkę odbierze
- Do przesyłania danych protokół IP używa specjalnego formatu pakietu
- Pakiet ten składa się z nagłówka pakietu oraz danych do przesłania
- Zgodnie z zasadą przesyłania strumieniowego dane protokołu IP są danymi pochodzącymi z wyższych warstw modelu ISO/OSI
- Dane te są następnie enkapsulowane do postaci pakietu IP
- Przy przejściu do warstwy łącza danych pakiet IP jest enkapsulowany do postaci ramki Ethernetowej.

Pakiet IPv4


0
4
8
16
19
24
31
Version
Header Length
Tos
Total length
identifier
Flags
Fragment offset
TTL
Protocol
Header checksum
Source IP address
Destination IP address
Options (variable length)
Data
Header

Pakiet IPv4

Cechy pakietu IPV4:

- Pakiet IP składa się z nagłówka oraz danych.
- Ze względów technicznych pakiet ten został przedstawiony w formie tabeli, po 32 bity (4 bajty) w rzędzie, w rzeczywistości należy go sobie wyobrazić jako jednolity strumień bitów przedstawionych w sposób ciągły.

Poszczególne pola pakietu mają następujące znaczenie:

- wersja (Version) - pole 4-bitowe określające typ protokołu IP. Jeśli jest tam wpisana wartość 4 oznacza to wersję czwartą protokołu. Jeśli jest tam wartość 6 oznacza to IPv6. Rozróżnianie pomiędzy pakietami wersji 4 i 6 jest przeprowadzane już przy analizowaniu ramki warstwy drugiej poprzez badanie pola typu protokołu.

- długość nagłówka (Header Length) - pole 4 bitowe określające długość datagramu wyrażoną jako wielokrotność słów 32 bitowych.

Pakiet IPv4

- typ usługi (Tos ang. Type-of-Service): 8-bitowe pole określające poziom ważności jaki został nadany przez protokół wyższej warstwy. Znaczenie poszczególnych bitów tego pola jest następujące:
  - Bity: 0 - 2:
    - 000: Routine
    - 001: Priority
    - 010: Immediate
    - 011: Flash
    - 100: Flash Override
    - 101: CRITIC/ECP
    - 110: Internetwork Control
    - 111: Network Control
  - Bit 3 – opóźnienie
    - 0 – Normal,
    - 1 – Minimise

Pakiet IPv4

- Bit 4- prośba o przesyłanie danych szybkimi łączami
  - 0 – Normal,
  - 1 – Maximise
- Bit 5 - prośba o dużą pewność przesyłania danych
  - 0 – Normal,
  - 1 – Maximise
- Bit 6 – koszt transmisji
  - 0 – Normal,
  - 1 – Minimise
- Bit 7 – zarezerwowany, zawsze 0

Pakiet IPv4

- całkowita długość (Total length) - pole 16-bitowe.

  W celu uzyskania długości pola danych należy odjąć od długości całkowitej długość nagłówka. Wartość minimalna wynosi 576 oktetów zaś maksymalna 65535 oktetów, tzn. 64 kB
- Identyfikacja (identifier) - 16 bitowe pole używane do określania numeru sekwencyjnego bieżącego datagramu.
- Znaczniki (Flags) - 3 bitowe pole.
  - Bit 0: zawsze 0
  - Bit 1: 0 – fragmentacja, 1 – bez fragmentacji
  - Bit 2: 0 – pakiet pochodzi ze środka, 1 – pakiet powstał w wyniku podzielenia
- Przesunięcie fragmentu (Fragment Offset) - 13-bitowe pole służące do składania fragmentów datagramu

Protokół IPv4

- Czas życia (TTL, ang. Time To Live) - 8-bitowe pole określające liczbę routerów (przeskoków), przez które może być przesłany pakiet. Wartość tego pola jest zmniejszana przy przejście przez każdy router na ścieżce. Gdy wartość tego pola wynosi 0, wtedy pakiet taki jest odrzucany. Zasada ta pozwala na stosowanie mechanizmów zapobiegających zapętlaniu się tras routingu.
- Protokół (Protocol) - 8-bitowe pole określające, który z protokołów warstwy wyższej odpowiada za przetworzenie pola Dane.

Protokół IPv4

- Suma kontrolna nagłówka (Header checksum) - 16-bitowe pole z sumą kontrolną nagłówka pozwalającą stwierdzić, czy nie nastąpiło, naruszenie integralności nagłówka. Ze względu na fakt, że każdy router dokonuje zmian w nagłówku musi ona być przeliczona na każdym z routerów.
- Adres IP nadawcy (Source IP address) - 32-bitowe pole z adresem IP nadawcy pakietu
- Adres IP odbiorcy (Destination IP address) - 32-bitowe pole z adresem IP odbiorcy pakietu
- Opcje (Options – variable length) - pole to nie występuje we wszystkich pakietach. Pole to może być wypełnione zerami jeśli jest potrzebna, aby długość nagłówka była wielokrotnością 32 bitów
- Dane - pole o długości do 64kB zawierające dane pochodzące z wyższych warstw.

Protokół ICMP

- W ramach warstwy sieciowej sprawdzaniem dostępności sieci docelowej zajmuje się protokół ICMP (ang. Internet Control Message Protocol).
- Jego zadaniem nie jest rozwiązywanie problemów z zawodnością IP, ale zgłaszanie braku łączności. Protokół ten został zdefiniowany w dokumencie RFC 792.
- Komunikaty ICMP wysyłają zwykle bramy lub hosty.
- Najczęstsze powody wysyłania tych komunikatów to:
  - zbytnie obciążenie routera lub hosta - wysyłany jest komunikat ICMP,
  - należy zwolnić prędkość przesyłania komunikatów, bo host nie nadąża z ich przetwarzaniem
  - router lub host znajduje lepszą trasę - może wtedy wysłać do źródła komunikat o lepszej trasie
  - host docelowy jest nieosiągalny - wtedy ostatnia brama wysyła komunikat ICMP o niedostępności adresata i przesyła go do hosta źródłowego
  - pole TTL pakietu jest równe 0 - wtedy router może wysłać komunikat ICMP do źródła i odrzuca pakiet

Protokół ICMP

- Przy przesyłaniu komunikaty ICMP są poddawane enkapsulacji do postaci pakietów IP, a następnie do postaci ramki warstwy drugiej
- Pod tym względem stanowią one integralną część danych pakietu IP
- Komunikat ICMP jest przesyłany w datagramie IP
- Komunikat ICMP składa się z nagłówka ICMP oraz danych ICMP. Warto przy tym zauważyć, że ze względu na zawodny charakter protokołu IP w momencie zaginięcia datagramu przenoszącego komunikat ICMP, nie zostanie to zdiagnozowane
- Wysyłanie komunikatów o błędach powodowałoby występowanie znacznego ruchu w sieci
- Struktura datagramu ICMP jest odmienna od struktury datagramu IP. Wspólny jest tylko sposób adresacji

Format komunikatu ICMP

Typ – 8 bitów	Kod – 8 bitów	Suma kontrolna – 16 bitów
Identyfikacja		Numer sekwencji
Dane (opcjonalne)		

- Najważniejsze dane przesyłane w komunikacie ICMP zawarte są w polach Typ i Kod. Zatem wszystkie wersje komunikatów ICMP musza zawierać pola:
  - Typ
  - Kod
  - Suma kontrolna

Format komunikatu ICMP

Znaczenie poszczególnych bajtów jest następujące:

- Pole Typ:
  - 0 - odpowiedź z echem (ang. Echo Reply)
  - 3 - odbiorca nieosiągalny (ang. Destination Unreachable).
  - 4 - zmniejszenie szybkości nadawania - tłumienie źródła (ang. source quench)
  - 5 - zmiana trasowania - przekierowanie (ang. redirect).
  - 8 - prośba o echo (ang. echo request)
  - 9 - rozgłaszanie routera (ang. router advertisement)
  - 10 - wywołanie routera (ang. router solicitation)
  - 11 - przekroczenie TTL (ang. Time Exceeded)
  - 12 - kłopot z parametrami datagramu
  - 13 - prośba / żądanie o wysłanie znacznika czasu (ang. timestamp request)
  - 14 - odpowiedź na prośbę / żądanie o wysłanie znacznika czasu (ang. timestamp reply)
  - 15 - prośba o informację

Format komunikatu ICMP

Znaczenie poszczególnych bajtów jest następujące:

- Pole Typ:
  - 16 - odpowiedź z informacją
  - 17 - prośba o maskę adresu
  - 18 - odpowiedź z maską adresu
  - 30 - Traceroute
  - 31 - błąd konwersji datagramu (ang. Datagram Conversion Error)
  - 32 - przekierowanie hosta mobilnego (ang. Mobile Host Redirect)
  - 33 - IPv6 Where-Are-You
  - 34 - IPv6 Here-I-Am
  - 35 - prośba o zarejestrowanie urządzenia mobilnego (ang. Mobile Registration Request)
  - 36 - odpowiedź na prośbę o zarejestrowanie urządzenia mobilnego (ang. Mobile Registration Reply)
  - 37 - żądanie nazw domeny (ang. Domain Name Request)
  - 38 - zwrot nazwy domeny (ang. Domain Name Reply)
  - 39 - SKIP Algorithm Discovery Protocol
  - 40 - Photuris, Security Failures

Format komunikatu ICMP

- Następujące wartości pola Typ są zarezerwowane :
  - 1,2,7,19 (zarezerwowane dla bezpieczeństwa)
  - 20-29
  - 41-255

Format komunikatu ICMP

- W przypadku komunikatu ICMP typu żądanie „echo request” i „echo reply” wartości pola typ wynoszą odpowiednio 8 albo 0
- Wartość pola Kod w obu przypadkach wynosi 0.
- Dodatkowo w celu połączenia zapytań i odpowiedzi pola Identyfikator i Numer sekwencji muszą mieć wartości unikalne. W polu danych mogą być przenoszone dodatkowe informacje potrzebne do zapytania i/lub odpowiedzi. Tego typu komunikaty ICMP są wykorzystywane przez podstawowe programy testujące, takie jak ping czy traceroute.

Format komunikatu echo request lub echo reply

Typ	Kod	Suma kontrolna
Typ (0 lub 8)	Kod (0)	Suma kontrolna
Identyfikator		Numer sekwencji
Dane opcjonalne		

Błędne komunikaty ICMP

- Przy próbach wysyłania pakietów do miejsca przeznaczenia może wystąpić szereg błędów związanych z np. z uszkodzeniem łącza, błędnym adresem docelowym, nieznaną lokalizacją, itd.

- W takich przypadkach router, który wykryje problem wysyła komunikat o niedostępnym adresacie (ang. destination unreachable)

- W zależności od przyczyny błędu w polu „Kod” pojawiają się wartości liczbowe powiązane z następującymi usterkami:

  - 0 - sieć niedostępna
  - 1 - host niedostępny
  - 2 - protokół niedostępny
  - 3 - port niedostępny
  - 4 - niezbędna fragmentacja, ustawiona wartość DF
  - 5 - nie powiodło się określenie trasy przez nadawcę (ang. source route)

Błędne komunikaty ICMP

- W zależności od przyczyny błędu w polu „Kod” pojawiają się wartości liczbowe powiązane z następującymi usterkami:
  - 6 - nieznana sieć docelowa
  - 7 - nieznany host docelowy
  - 8 - host źródłowy odizolowany
  - 9 - komunikacja z siecią docelową zablokowana przez administratora
  - 10 - komunikacja z hostem docelowym zablokowana przez administratora
  - 11 - sieć niedostępna dla tego typu usługi
  - 12 - host niedostępny dla tego typu usługi

Błędne komunikaty ICMP

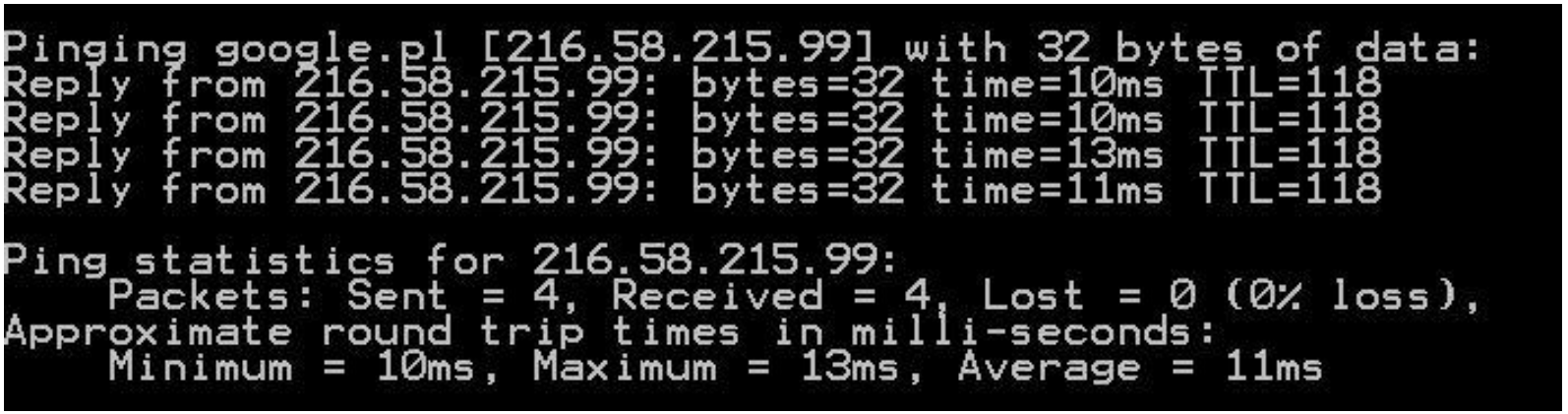
- Komunikat o niedostępnym adresie wysyłany jest również w przypadku, gdy przesyłany pakiet musi zostać podzielony na mniejsze datagramy, np. przy przesyłaniu z sieci typu Token Ring do sieci Ethernet, a znacznik w nagłówku pakietu nie pozwala na taką fragmentację. Wysyłany jest wtedy kod błędu o wartości 4.
- W przypadku zablokowania przez administratora określonych usług sieciowych, takich jak np. www, również nie można przesłać pakietów z żądaniem wyświetlenia strony. Generowany jest wtedy komunikat o niedostępnym adresacie ze stosowną wartością kodu błędu.

Typ (3)	Kod (0 – 12)	Suma kontrolna
Nieużywane (musi mieć wartość 0)		
Nagłówek internetowy + pierwsze 64 bity datagramu		

Ramka komunikatu destination unreachable

Narzędzia diagnostyczne ICMP

- Komunikaty ICMP są wykorzystywane przez program narzędziowy ping. Program ten wysyła komunikat ICMP z wartością pola Typ ustawioną na wartość równą 8 prośba o wysłanie komunikatu echo (ang. echo request).
- W odpowiedzi na ten komunikat host, do którego jest adresowany ten komunikat może odpowiedzieć komunikatem ICMP o wartości pola Typ równą 0.



Komunikaty sterujące ICMP

- Oprócz komunikatów o błędach, protokół ICMP służy również do przesyłania komunikatów sterujących (stąd część nazwy protokołu: control).
- Komunikaty te są wysyłane, m.in. w celu efektywniejszego przesyłania pakietów przez IP.
- Wybrane komunikaty sterujące:
  - Zmiana trasowania / przekierowanie
  - Synchronizacja zegarów i oszacowanie czasu tranzytu
  - Żądanie przesłania informacji
  - Żądanie maski adresowej
  - Wykrywanie routera

ICMP - przekierowanie

- W przypadku wykrycia lepszej trasy dla pakietów wysyłany jest komunikat o wartości pola Typ równej 5. Oznacza on zmianę trasowania / przekierowanie (ang. redirect).
- Za wysłanie takiego komunikatu odpowiada host będący domyślną bramą, aby komunikat taki został wysłany muszą być jednak spełnione następujące warunki:
  - pakiet przesyłany do routera na jego interfejs jest następnie zawracany i kierowany przez ten sam interfejs do innego routera - adres sieci IP nadawcy jest taki sam jak routera następnego przeskoku routowanego pakietu
  - trasa pakietu nie jest określona przez nadawcę - trasa określona po przekierowaniu nie jest trasą domyślną lub kolejnym przekierowaniem ICMP
  - router jest skonfigurowany do wysyłania żądań przekierowania pakietów

- Żądanie przekierowania pakietów w zależności od wartości pola Kod może dotyczyć zarówno sieci jak i hostów:
  - 0 - datagramy przekierowania dla sieci
  - 1 - datagramy przekierowania dla hosta
  - 2 - datagramy przekierowania dla typu usługi i sieci
  - 3 - datagramy przekierowania dla typu usługi i hosta

ICMP – żądanie znacznika czasu

- Przy komunikacji poprzez sieci rozległe może istnieć potrzeba synchronizacji zegarów w odległych od siebie lokalizacjach. Ma to istotne znaczenie w przypadku użytkowania aplikacji wymagających zgodności znaczników czasowych.
- W celu synchronizacji zegarów na danym hoście (serwerze) z innym hostem (serwerem) wysyłany jest stosowny komunikat ICMP żądanie / prośba wysłania znacznika czasowego (ang. timestamp request) o wartości pola Typ równej 13.
- W odpowiedzi na taką prośbę wysyłany jest komunikat odpowiedzi o wartości pola Typ równej 14.
- Pola kodu w przypadku obu typów komunikatów są równe 0.
- Pola, w których będą umieszczane znaczniki czasu są wypełniane czasem podanym w milisekundach liczonych od północy czasu uniwersalnego (UTC).

ICMP – żądanie znacznika czasu

- Przed wysłaniem komunikatu wypełniane jest pole „Początkowy znacznik czasu” wartością daty i godziny czasu dla hosta źródłowego.
- W polu „Znacznik czasu odbioru” wstawiany jest czas odbioru przez host docelowy komunikatu z żądaniem wysłania znacznika czasu.
- Następnie, przed wysłaniem komunikatu z odpowiedzią, wypełniany jest aktualny czas do pola „Znacznik czasu wysłania”.
- Analiza trzech pól przesłanych w odpowiedzi na prośbę o znacznik czasu umożliwia oszacowanie czasu przesyłania pakietu przez sieć zarówno w jedną jak i drugą stronę.
- W praktyce zamiast tego typu pomiarów stosuje się protokoły wyższych warstw stosu protokołów TCP/IP, np. protokół NTP (ang. Network Time Protocol).

ICMP – żądanie znacznika czasu

Typ (13 lub 14)	Kod (0)	Suma kontrolna
Identyfikator		Numer sekwencji
Początkowy znacznik czasowy		
Znacznik czasowy odbioru		
Znacznik czasowy wysłania		

ICMP – żądanie przesłania informacji

- Komunikaty żądanie / prośba o przesłanie informacji (ang. information request) oraz odpowiedź na żądanie przesłania informacji (ang. information reply) zostały zaprojektowane z myślą o przesyłaniu numerów IP.
- W zależności od tego czy jest to prośba o informację, czy też odpowiedź na tę prośbę pole Typ ma wartości: 15 lub 16.
- W przypadku obu typów komunikatów wartości pola „Kod” wynoszą 0.
- W praktyce obecnie nie są wykorzystywane, gdyż informacje takie są przesyłane w sposób bardziej dogodny przez protokoły takie jak BOOTP, RARP czy też DHCP.

ICMP – żądanie przesłania informacji

Typ (15 lub 16)	Kod (0)	Suma kontrolna
Identyfikator		Numer sekwencji

ICMP – żądanie przesłania maski adresowej

- Komunikat ICMP typu żądanie maski adresowej oraz odpowiedź na żądanie maski adresowej mają odpowiednio wartości pól Typ wypełnione liczbami 17 i 18.
- Komunikaty te służą określeniu przez hosta jego maski adresowej.
- W przypadku, gdy host zna adres routera w danej podsieci, komunikat żądanie maski adresowej wysyłany jest na adres tego komputera. W przeciwnym razie komunikat ten wysyłany jest na adres rozgłoszeniowy.
- W odpowiedzi router wysyła na adres hosta, który wysłał żadanie, netmaskę w odpowiednim polu komunikatu zwrotnego.
- Pola „Identyfikator” jak i „Numer sekwencyjny” służą do skojarzenia zapytań i odpowiedzi. Mogą mieć wartość 0.

ICMP – żądanie przesłania maski adresowej

Typ (17 lub 18)	Kod (0)	Suma kontrolna
Identyfikator		Numer sekwencji
Maska adresowa		

ICMP – żądanie wykrycia routera

- Komunikaty służące do wykrywania routera (ang. router discovery messages) są pomocne w momencie podłączania do sieci hosta, który nie ma wpisanego w sposób statyczny adresu routera.
- Komunikaty takie są wykorzystywane przez protokół IRDP (ang. ICMP Router Discovery Protocol), który działa w oparciu o protokół ICMP
- Pozyskanie takiego adresu, przy pomocy protokołu IRDP, poprzez nowo podłączony host może odbyć się w dwojaki sposób
- Jednym z nich jest cykliczne wysyłanie przez router komunikatów rozgłaszania routera (ang. router advertisement), które mogą zostać odebrane przez hosty w sieci lokalnej
- Komunikat taki ma w polu Typ wpisaną wartość 9
- Komunikaty rozgłaszania routera nie służą do wyboru najlepszego routera do przesyłania pakietów do określonej lokalizacji. Gdy host wybierze router, który nie jest optymalny do przesyłania pakietów do określonej lokalizacji, to powinien zostać o tym poinformowany poprzez komunikat ICMP o przekierowaniu
- Drugim sposobem jest wysłanie przez nowo podłączony do sieci host komunikatu wywołania routera (ang. router solicitation). Taki komunikat ma w polu Typ wpisaną wartość 10
- Ze względu na własności protokołu DHCP znaczenie protokołu IRDP jest obecnie niewielkie

ICMP – żądanie wykrycia routera

Typ (9)	Kod (0)	Suma kontrolna
Liczba adresów	Rozmiar adresu	Czas życia
Adres routera 1		
Poziom preferencji 1		
Adres routera 2		
Poziom preferencji 2		

ICMP – żądanie wykrycia routera

- Poszczególne pola mają następujące znaczenie:
  - Liczba adresów - liczba adresów przesyłana w tym komunikacie
  - Rozmiar adresu - liczba 32 bitowych słów przeznaczonych na pole adresu routera(ów).
  - Czas życia - czas w sekundach, przez który adresy routerów przesłane w komunikacie są aktualne. Domyślna wartość wynosi 30 min.
  - Adres routera - adres routera
  - Poziom preferencji - pole umożliwiające oznaczenie przez administratora danego routera ważność do określonych funkcji. Wartość tego pola waha się w granicach 1 do „Liczby adresów. Czym wyższa wartość tego pola tym wybór tego routera jest bardziej pożądany.

Dziękuję za uwagę