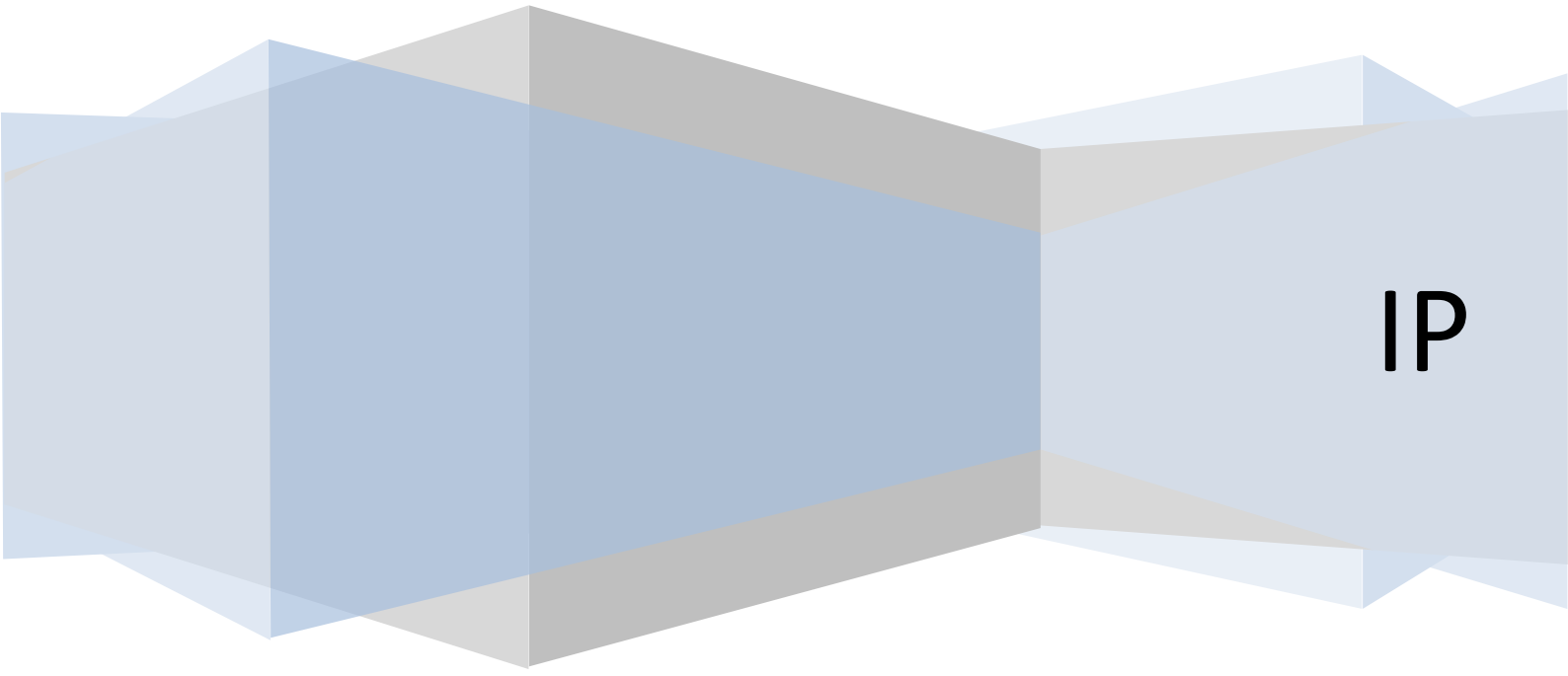
Politechnika Krakowska

Katedra Automatyki i Technik Informacyjnych

Laboratorium Sieci Komputerowych

2012/2013



1. Wprowadzenie

1.1. Protokół internetowy

Protokół internetowy (ang. Internet Protocul, IP) jest to protokół komunikacyjny wykorzystywany w celu nawiązania łączności i wymiany danych między sieciami. Protokoły IP umożliwiają komunikację wielu różnych sieci fizycznych w jednym systemie komunikacji.

Istnieje analogia pomiędzy sieciami fizycznymi, a intersieciami, w sieci fizycznej podstawową jednostką przesyłanych danych jest ramka zbudowana z nagłówka (z adresem fizycznym) oraz przenoszonych danych. W intersieci podstawą jednostką przesyłania informacji jest pakiet (czasami zwany datagramem IP), który również zawiera nagłówek (z adresem logicznym) oraz przenoszone dane.

Główną różnicą pomiędzy sieciami fizycznymi a intersieciami jest fakt, że intersieci są pewnym abstrakcyjnym systemem wytworzonym i obsługiwanym przez oprogramowanie intersieciowe.

Protokołu internetowe są protokołami zawodnymi (ang. unreliable), nie gwarantują dostarczenia pakietów, nie gwarantują dostarczenia pakietu do odbiorcy w kolejności w jakiej były wysyłane, a co więcej każdy pakiet może być dostarczony do odbiorcy inną ścieżką.

W kontekście modelu OSI, protokół IP znajduje się w warstwie 3. Jest on kapsułowany w ramkach warstwy łącza danych, a sam enkapsuluje w sobie protokoły warstwy wyższej – transportowe. Jak chociaż protokół TCP (zapewniający niezawodność dostarczania danych)

1.2. Kapsułowanie datagramu

Cały datagram IP jest umieszczany w części ramki sieciowej przeznaczonej na dane, przedstawia to rysunek 1.

Rys 1. Kapsułowanie protokołu IP w ramce ethernetowej

Ramka ethernetowa	Nagłówek ramki	dane		CRC
Protokół IP		Nagłówek protokołu	Dane przenoszone przez protokół IP	

1.3. Fragmentacja datagramu IP

Datagramy IP mogą być przenoszone w różnych sieciach fizycznych np: FDDI, ethernetowych. Każda z sieci występujących pomiędzy hostem źródłowym a docelowym może posiadać inny maksymalny rozmiar przenoszonych danych (MTU) w ramce. Sztywne ustawienie MTU na mniejszą wartość występującą w którejś ze sieci było by bardzo nieopłacalne (w innych sieciach datagramy przenoszone były by przez ramki w których można by zawrzeć dużo więcej informacji), a z kolei ustawienie na maksymalną wartość MTU powodowało by niemieszczenia się datagramów w ramkach w sieciach z mniejszym MTU. Oprogramowanie intersieci rozwiązuje ten problem poprzez możliwość dzielenia datagramu na fragmenty, a sam proces fragmentacji i (defragmentacji) realizowany jest przez rutery.

1.4. Format datagramu IP

Format datagramu IP przedstawia rys 2.

Rys 2. Format datagramu IP

<table>
<tr><td>0</td><td>4</td><td>8</td><td></td><td>16</td><td></td><td></td><td>31</td></tr>
<tr><td>Wersja</td><td>Długość nagłówka</td><td colspan="2">Typ obsługi</td><td colspan="4">Długość całkowita</td></tr>
<tr><td colspan="4">Identyfikacja</td><td>Znacznik</td><td colspan="3">Przesunięcie fragmentu</td></tr>
<tr><td colspan="2">Czas życia</td><td colspan="2">Protokół</td><td colspan="4">Suma kontrolna nagłówka</td></tr>
<tr><td colspan="8">Adres IP nadawcy</td></tr>
<tr><td colspan="8">Adres IP odbiorcy</td></tr>
<tr><td colspan="5">Opcje IP</td><td colspan="3">Uzupełnienie</td></tr>
<tr><td colspan="8">Dane</td></tr>
<tr><td colspan="8">...</td></tr>
</table>

Wersja, zawiera informacje o wersji protokołu

Długość nagłówka, długość nagłówka datagramu mierzona w 32 bitowych słowach

Długość całkowita, mierzona w bajtach długość datagramu. Zawiera bajty nagłówka oraz danych. Minimalny rozmiar datagramu to 576 bajtów, maksymalna długość datagramu IP to 65535 bajtów.

Typ obsługi, określa sposób w jaki datagram powinien zostać obsłużony przez ruter, pierwsze 3 bity oznaczają pierwszeństwo , bity od 3 do 5 (włącznie) oznaczają odpowiednio prośbę o krótki czas oczekiwania, prośbę przesłanie szybkim łączem, prośbę o przesłanie łączem o dużej pewności przesłania danych.

Identyfikacja, numer identyfikujący fragment do określonego datagramu

Znacznik, wykorzystywany w fragmentacji, zawiera informację czy pakiet może być fragmentowany oraz czy za danym fragmentem znajduje się kolejny

Przesunięcie fragmentu, pole określa przesunięcie z pierwotnego fragmentu dla danych przenoszonych w danym fragmencie

Czas życia, określa jak długo pakiet może istnieć na sieci, wartość ta jest wyrażona w sekundach

Protokół, zawiera informacje o rodzaju protokołu zawartym w polu dane

Suma kontrolna nagłówka, służy do sprawdzenia zawartości nagłówka. Odnosi się tylko do nagłówka, nie do danych.

Adres IP nadawcy i **Adres IP odbiorcy**, pola zawierają 32 bitowe adresy IP

Opcje IP, opcjonalne pole umożliwiające określenie zachowania się datagramu. Na przykład poprzez wyznaczenie trasy pakiety w zależności od nadawcy

Dane, informacje (protokoły warstwy wyższej) przenoszone przez datagram

1.5. Adresy IP

Adres logiczny internetu (adres IP) składa się z 32 bitów, najczęściej jest przedstawiany w formie czterech grup bajtów przedstawionych w systemie dziesiętnym przedzielonych kropkami, poniżej przedstawiono dwa przykłady adresów IP:

a) 192.168.0.1

b) 10.0.0.1

Adres IP można podzielić na dwie części, część odpowiedzialną za adres sieci (zwaną prefiksem) oraz część odpowiedzialna za adres hosta w sieci (zwana sufiksem). Pierwotny system adresowania w sieciach IP zakładał podział ze względu na wielkość sieci i wprowadzał trzy główne klasy adresów: A, B, C oraz na dwie klasy dodatkowe: D, E. Klasa A zawiera 127 podsieci, a w każdej z nich można przydzielić 16 777 214 adresów, klasa B zawiera możliwość adresacji 16 384 sieci, a w każdej z nich 65 534 adresów, klasa C zawiera możliwość adresacji 2 097 152 sieci, a każdej z nich 254 hostów. Klasa D wykorzystywana jest do transmisji pakietów do pewnych grup hostów, a klasa E stosowana jest do

celów badawczych. Klasy rozróżniały się na podstawie pierwszych czterech bitów adresu (przedstawionego w postaci binarnej)

1.6. Bezklasowa adresacja w sieciach IP i maski podsieci

Rozwój sieci i internetu doprowadził do wyczerpania się koncepcji adresowania klasowego, zamiast niego zaproponowano możliwość wskazania dowolnego bitu, który będzie stanowił podział adresu IP na prefiks i sufiks. System adresowania bezklasowego wymaga od komputerów przetwarzających adresy przechowywanie dodatkowej struktury, która wyznacza rzeczoną granicę, w specyfikacji IP przewidziano do tego użycie 32 bitowej maski – zwanej maską podsieci. Występujące w masce jedynki (w notacji binarnej) wyznaczają część prefiks, a zera sufiks adresu. Formalna nazwa adresowanie bezklasowe to CIDR (ang. Classless Interdomain Routing).

Adresacja bezklasowa wprowadza też modyfikację zapisu adres IP w formie dziesiętnej z kropką, rozszerzając zapis o postać maski podsieci (wartość po ukośniku), np: adres 192.168.0.1/24 znaczy, że maska składa się z ciągu 24 bitów o wartości „1”. Tabela 1 zawiera zestawienie kilku typowych masek podsieci w notacji CIDR oraz ich forma w zapisie dziesiętnym.

Tabela 1. Maski podsieci w postaci CIDR oraz w zapisie dziesiętnym

CIDR	Maska w postaci dziesiętnej	Uwagi
/8	255.0.0.0	Maska klasy A
/13	255.248.0.0	
/16	255.255.0.0	Maska Klasy B
/20	255.255.240.0	
/24	255.255.255.0	Maska klasy C
/30	255.255.255.252	

1.7. Prywatne i publiczne adresu IP

Adresy IP można również podzielić ze względu na ich zasięg na dwie grupy adresów publicznych i prywatnych. Adresy publiczne są bezpośrednio dostępne w intersieci, natomiast adresy prywatne są przeważnie ukryte za ruterem. Klasa A zezwala na wykorzystanie adresów od 10.0.0.0 do 10.255.255.255, klasa B zezwala na wykorzystanie adresów od 172.16.0.0 do 172.31.255.255, natomiast klasa C pozwala na wykorzystanie adresów od 192.168.0.0 do 192.168.255.255.

1.8. Specjalne adresy IP

Istnieją adresy IP, które mają specjalne przeznaczenie i nie mogą być przypisane do żadnego urządzenia sieciowego. Zestawienie specjalnych adresów przedstawia tabela 2.

Tabela 2. Zestawienie specjalnych adresów IP

Prefiks	Sufiks	Rodzaj adresu	Przeznaczenie
Sam zera	Same zera	Host	Wykorzystywany podczas uruchomienia komputera
Adres sieci	Same zera	Adres sieci	Identyfikuje sieć
Adres sieci	Same jedynki (w postaci binarnej)	Rozgłoszenia skierowane	Rozgłoszenie pakietu w wybranej sieci
Same jedynki (w postaci binarnej)	Same jedynki (w postaci binarnej)	Rozgłoszenie lokalne	Rozgłoszenie pakietu w sieci lokalnej
127/8	Dowolny	Pętla zwrotna	Testowanie

1.9. Ustawienie statycznego i dynamicznego adresy IP w systemie Linux

W celu konfiguracji karty sieciowej ethernetowej w systemach należących do rodziny systemów Linuxowych należy wykorzystać polecenie „ifconfig” w przypadku konfiguracji statycznej adresu IP lub „dhclient” dla konfiguracji dynamicznie przydzielanego adresu IP.

Przykład 1. Ustawienie statycznego adresu IP 192.168.0.2 z maską sieci 255.255.255.0 oraz bramy domyślnej 192.168.0.1 na karcie ethernetowej eth0

Ustawienie statycznego adresu IP na interfejsie „eth0” realizuje się z wykorzystaniem komend:

```
# ifconfig eth0 192.168.0.1 netmask 255.255.255.0 up

# route add default gw 192.168.0.1 eth0
```

W przypadku statycznej konfiguracji adresów IP należy pamiętać aby dodać adres serwera DNS.

Służy do tego plik „/etc/resolv.conf”, przykładowy listing wraz z komentarzem zaprezentowany jest poniżej:

```
# cat /etc/resolv.conf

nameserver 192.168.0.1                    <- adres serwera DNS
```

search localdomain <- wskazanie w jakiej domenie się znajduje

Przykład 2. Ustawienie dynamicznego przydzielania adresu IP

W celu ustawienia dynamicznego przydzielania adresu IP w systemach linuxowych wystarczy z pozycji terminalu wykonać komendę:

```
# dhclient
```

Tą samom komendę można wykorzystać w celu odnowienia adresu IP.

W celu zwolnienia adresu IP należy wykorzystać z komendy:

```
# dhclient –r
```

Konfiguracja klienta DHCP znajduje się w pliku „etc/dhclient.conf".

2. Cel ćwiczenia

Celem ćwiczenia jest zapoznanie się z podstawowymi aspektami pracy protokołu IP

3. Ćwiczenia

1. Zidentyfikuj klase adresu IP przydzielonego Twojej hosta
2. Wykorzystaj polecenie „traceroute" do stwierdzenia trasy do serwera www.onet.pl. Przeanalizuj wygenerowany ruch sieciowy
3. Wykorzystaj polecenie „traceroute" do stwierdzenia trasy do dowolnego serwera poza granicami Polski
4. Korzystając z polecenia ping odkryj MTU oraz ilość ruterów na ścieżce do serwera www.google.pl
5. Zmniejsz rozmiar MTU dla swojej stacji korzystając z komendy

   ```
   # ifconfig eth0 mtu xxx up
   ```

   gdzie „xxx" jest ustawioną przez Ciebie wartością (<200) i zaobserwuj fragmentację datagramów w programie Wireshark. Jakie pola pozwalają jednoznacznie poskładać datagram po stronie odbiorcy?
6. Proszę wysłać echo-request na adres rozgłoszeniowy sieci i przeanalizuj powstały ruch w sieci. Jaka jest alternatywa w przypadku gdy ICMP echo-request jest zablokowany?

Czy komputer może być przyłączony do wielu sieci jednocześnie?

Czym różni się wywołanie komendy „ping" z adresem IP własnego komputera a wywołanie komendy „ping" z adresem 127.0.0.1?

Dodatkowo proszę zawrzeć we sprawozdaniu opis przekazywania datagramu IP między sieciami oraz procedurę fragmentacji i odtworzenie pakietu IP.

4. Bibliografia

- „Sieci komputerowe i intersieci” D. E. Comer
- „Sieci komputerowe TCP/IP. Zasady, protokoły i architektura” D. E. Comer
- „Wprowadzenie do CCNA” A. Józefiok

Instrukcja opracowana przez:

mgr inż. Kazimierz Kiełkowicz