Sieci komputerowe

Tadeusz Kobus, Maciej Kokociński
Instytut Informatyki, Politechnika Poznańska

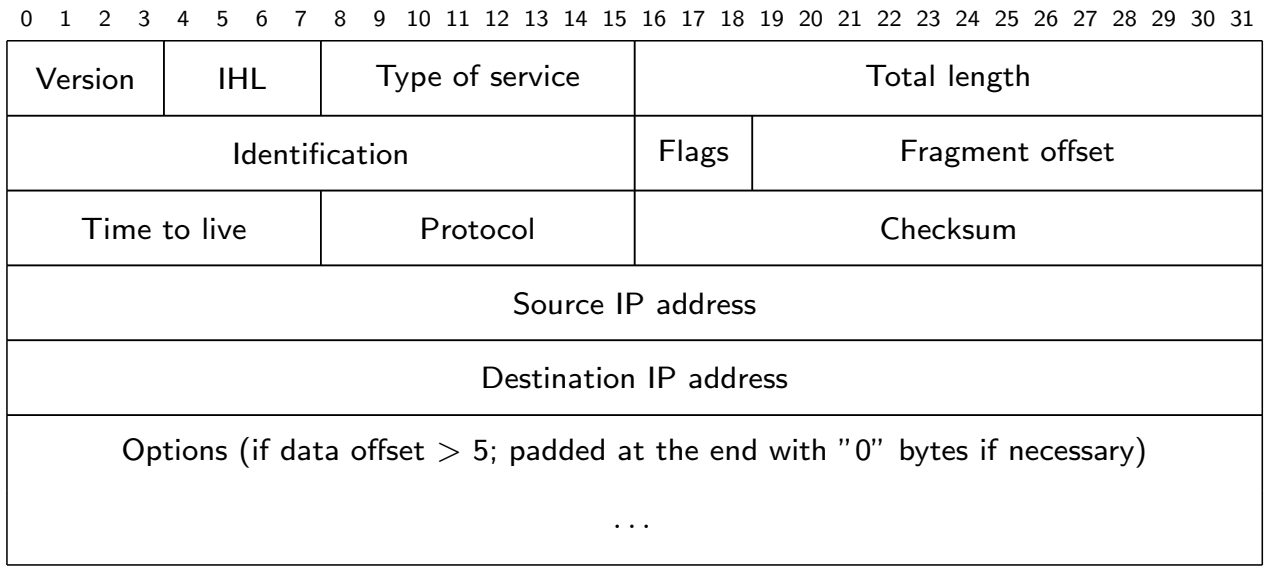
Warstwa sieciowa

Warstwa sieciowa

- Definiuje pakiety.
- Definiuje schemat adresowania używanego w Internecie.
- Ustala drogę transmisji danych między oddalonymi węzłami sieci.
- Odpowiada za fragmentacje pakietów (ze względu na Maximum Transmission Unit, MTU).
- Działa w modelu bezpołączeniowym.
- Przykładowe standardy:
  - IP
  - IPX
  - ICMP
  - ARP
  - DDP

Internet Protocol (IPv4)

- Rola – jednoznaczna adresacja urządzeń i trasowanie pakietów przez wiele sieci.
- Adres IP identyfikuje urządzenie i określa jego logiczną lokalizacje.
- Struktura nagłówka pakietu:



Flags (3b) + Fragment offset (13b) – jeśli datagram to fragment większego komunikatu

Time to live (TTL) – maksymalna liczba przeskoków (hops), którą może pokonać pakiet

Fragmentacja pakietów

- Pierwotny pakiet: 4000B (20B nagłówka + 3980B danych).
- Router przekazuje pakiet do sieci o mniejszym MTU: 1500B.

···	length = 4000	ID = x	fragflag = 0	offset = 0	···

- Pakiet dzielony jest na 3 fragmenty (dane: 1480B + 1480B + 1020B = 3980B).
- Offset jest podawany nie w bajtach, ale w bajtach podzielonych przez 8 $\longrightarrow$ redukcja rozmiaru nagłówka:
  - $1480/8 = 185$
  - $(1480 + 1480)/8 = 370$

···	length = 1500	ID = x	fragflag = 1	offset = 0	···

···	length = 1500	ID = x	fragflag = 1	offset = 185	···

···	length = 1040	ID = x	fragflag = 0	offset = 370	···

Zadanie 1

1. Zaloguj ruch przy pomocy programu `wireshark`. Jakie zazwyczaj są ustawione flagi w pakietach?
2. Powtórz ćwiczenie otwierając w międzyczasie jakąś stronę internetową przy użyciu protokołu `https`.
3. Powtórz ćwiczenie w międzyczasie wykonując polecenie `ping -s 4000` na wybrany adres IP.

Czas życia pakietu

W warstwie łącza danych ramki nie krążą w nieskończoność bo jest używany STP.

W warstwie sieciowej wykorzystywany jest mechanizm TTL:

- pole TTL nagłówka IP jest inicjalizowane na np. 64,
- pole TTL jest dekrementowane przez każdy router na drodze pakietu,
- router nie przekazuje dalej pakietu gdy TTL $= 0$.

Dlaczego wartość 64 jest wystarczająca?

Zadanie 2

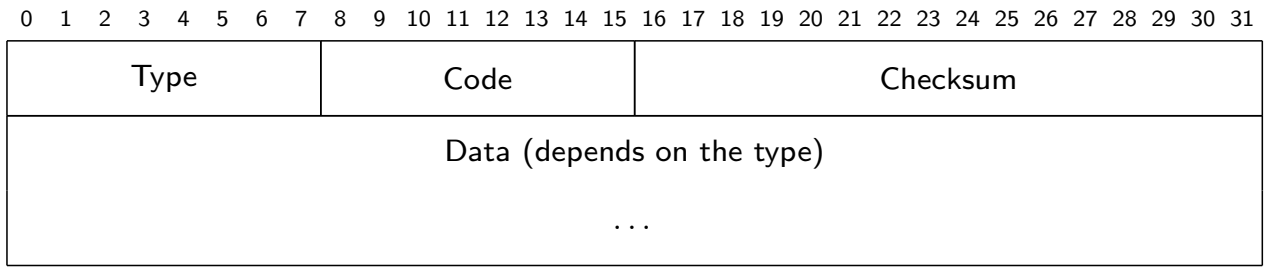
1. Jak działa program `traceroute` (ewentualnie skorzystaj z opcji `-I` lub `-T`)?
2. Zaloguj ruch przy pomocy programu `wireshark` i zbadaj nagłówki pakietów generowanych przez program `traceroute`.

Internet Control Message Protocol (ICMP)

- Protokół diagnostyczny przesyłający informacje o stanie i błędach w sieci.
- Musi być realizowany w każdej implementacji protokołu IP.
- Po co?
  - IP jest protokołem bezpołączeniowym.
  - IP nie ma wbudowanego mechanizmu informacji o sytuacjach wyjątkowych, np. o braku hosta docelowego, błędnym routowaniu, etc.
- Komunikaty ICMP mogą być generowane przez dowolne urządzenie *napotkane* na drodze pakietu (karta sieciowa, router, etc.)
- ICMP funkcjonuje na pograniczu warstw 3 i 4:
  - ICMP realizuje zadania warstwy sieciowej (3),
  - ICMP korzysta z IP do przesyłania komunikatów $\longrightarrow$ może być zaliczany do protokołów warstwy transportowej (4).

Internet Control Message Protocol (ICMP)

- Struktura komunikatu:

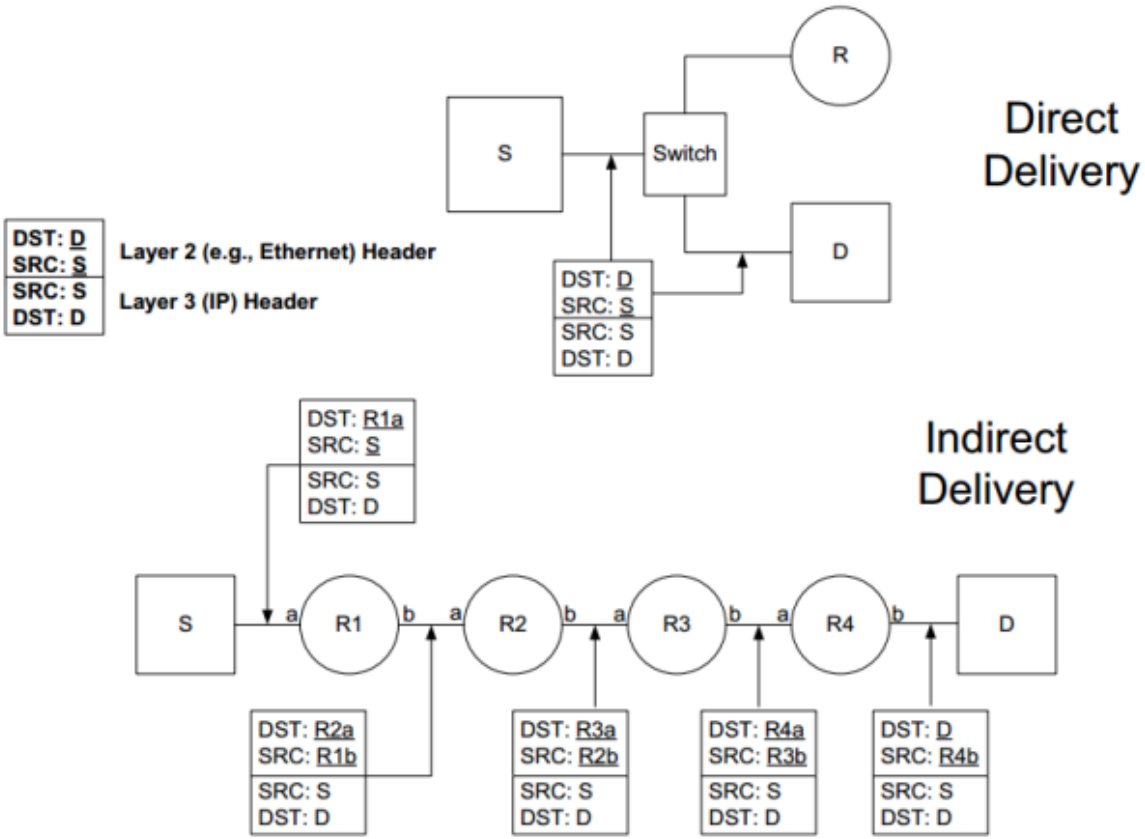


- Typy komunikatów ICMP (link).
- `ping`:
  - Echo Reply (0),
  - Destination Unreachable (3),
  - Echo Request (8).
- `traceroute` $\longrightarrow$ sprawdzanie TTL:
  - Echo Request (8),
  - Time Exceeded (11).

Internet Group Management Protocol (IGMP)

- Zarządzanie grupami multicastowymi w danej sieci:
  - dołączanie/odłączanie od grupy,
  - badanie stanu grupy.
- Komunikaty podobne do komunikatów ICMP.

Komunikacja w sieci globalnej



- Pakiet IP przechodzi przez sieć w (prawie) niezmienionej formie.
- Czas życia ramki to czas transmisji przez sieć lokalną.

Address Resolution Protocol (ARP) (1)

Problem:

- W sieciach IP komputery identyfikowane są przez adresy IP (warstwa 3).
- W sieciach Ethernetowych komputery identyfikowane są poprzez adresy MAC (warstwa 2).
- Skąd wiadomo jak skojarzyć adres MAC z adresem IP danego komputera?

Trywialne rozwiązanie:

- statyczna konfiguracja mapowania MAC–IP,
- nieskalowalne i problematyczne.

Address Resolution Protocol (ARP) (2)

Dynamiczne odwzorowanie adresów IP w adresy MAC
(protokół warstwy 2.5).

Protokół:

- zapytanie: nadawca rozgłasza w sieci fizycznej pytanie o adres MAC urządzenia o adresie IP `X.X.X.X`; pytanie zawiera adres MAC `aa:aa:aa:aa:aa:aa` nadawcy,
- odpowiedź: urządzenie, które dostało zapytanie i którego adres IP to `X.X.X.X` wysyła na `aa:aa:aa:aa:aa:aa` swój adres MAC `bb:bb:bb:bb:bb:bb`,
- (optymalizacja) nadawca zapisuje w prywatnej tablicy ARP-cache odzworowanie `X.X.X.X` do `bb:bb:bb:bb:bb:bb`. Wpisy w ARP-cache są tymczasowe.

Address Resolution Protocol (ARP) (3)

Reverse ARP:

- tłumaczenie MAC na IP,
- obecnie nieużywane.

Proxy ARP:

- używany, gdy niektóre komputery w sieci nie mają zdefiniowanej bramy,
- gdy komputer próbuje wysłać komunikat do komputera spoza sieci, router może odpowiedzieć na zapytanie ARP swoim adresem MAC (adresem MAC interfejsu znajdującego się w tej sieci, z której pochodzi zapytanie),
- router działa jako brama, choć komputer o tym nie wie.

ARP – narzędzia (1)

```
# ip neigh show
192.168.1.1 dev eth0 lladdr 98:fc:11:bc:f1:a0 REACHABLE
# ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=83.1 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=128 ms
^C
--- 192.168.1.100 ping statistics ---
# ip neigh show
192.168.1.100 dev eth0 lladdr 90:72:40:67:24:c7 REACHABLE
192.168.1.1 dev eth0 lladdr 98:fc:11:bc:f1:a0 REACHABLE

(minute pozniej)

# ip neigh show
192.168.1.100 dev eth0 lladdr 90:72:40:67:24:c7 STALE
192.168.1.1 dev eth0 lladdr 98:fc:11:bc:f1:a0 REACHABLE
```

ARP – narzędzia (2)

```
# ip neigh add 192.168.1.101 lladdr aa:bb:cc:dd:ee:ff dev eth0
# ip neigh show
192.168.1.100 dev eth0 lladdr 90:72:40:67:24:c7 REACHABLE
192.168.1.101 dev eth0 lladdr aa:bb:cc:dd:ee:ff PERMANENT
192.168.1.1 dev eth0 lladdr 98:fc:11:bc:f1:a0 DELAY
# ip neigh del 192.168.1.101 dev eth0
# ip neigh show
192.168.1.100 dev eth0 lladdr 90:72:40:67:24:c7 REACHABLE
192.168.1.101 dev eth0  FAILED
192.168.1.1 dev eth0 lladdr 98:fc:11:bc:f1:a0 REACHABLE

# ip neigh flush dev eth0
# ip link set arp off dev eth0
# ip link set arp on dev eth0
```

ARP – narzędzia (3)

```
# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
ap11                     ether   98:fc:11:bc:f1:a0   C                     eth0

# arp -i eth0 -s 192.168.1.101 aa:bb:cc:dd:ee:ff
# arp -i eth0 -d 192.168.1.101

# cat /proc/sys/net/ipv4/neigh/eth0/gc_stale_time
60

# arping -I eth0 192.168.1.100
ARPING 192.168.1.100 from 192.168.1.103 eth0
Unicast reply from 192.168.1.100 [90:72:40:67:24:C7]  106.945ms
Unicast reply from 192.168.1.100 [90:72:40:67:24:C7]  51.238ms
Unicast reply from 192.168.1.100 [90:72:40:67:24:C7]  74.105ms
^CSent 4 probes (1 broadcast(s))
Received 3 response(s)
```

Zadanie 3

1. Podłącz swój komputer (poprzez port `p4p1`) do koncentratora (na zapleczu).
2. Skonfiguruj interfejs `p4p1`, tak by wszystkie komputery w rzędzie działały w jednej sieci (unikalne sieci między rzędami).
3. Zbadaj jak zmienia się tablica ARP, gdy uruchamiasz program `ping` z argumentami będącymi adresami IP komputerów z Twojej sieci i adresami komputerów w innych rzędach (należących do innych sieci).

Dynamic Host Conf. Protocol (DHCP) (1)

Protokół pozwalający urządzeniu na otrzymanie od serwera w (lokalnej) sieci danych do konfiguracji, np.:

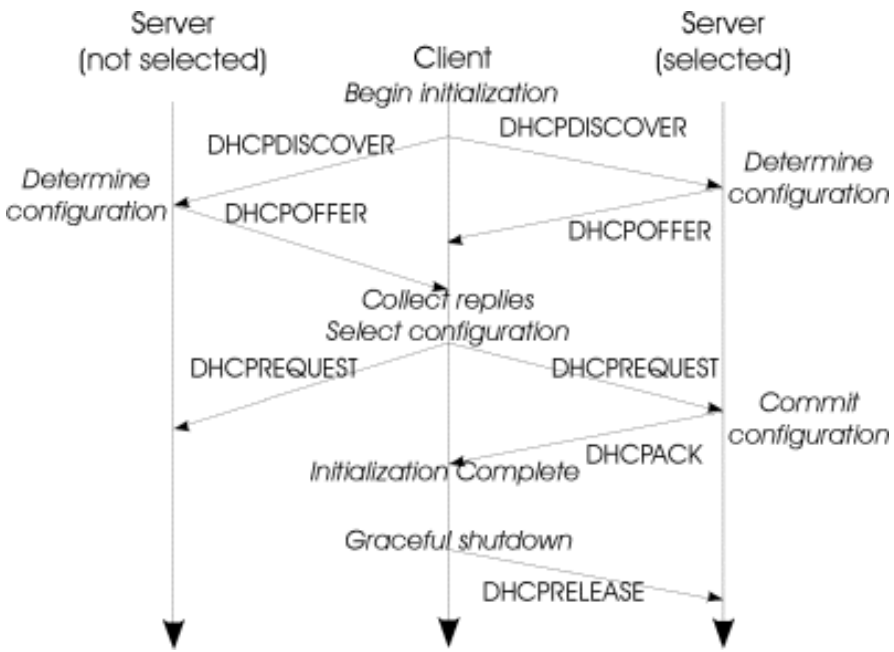
- adres IP, maska,
- adres IP bramy sieciowej,
- wartość MTU,
- nazwa DNS (Domain Name Server),
- adresy serwerów DNS,
- inne: adresy IP serwera SMTP, serwera TFTP, ...

Dynamic Host Conf. Protocol (DHCP) (2)

Sposoby przydzielania adresu z DHCP (możliwe konfiguracje serwera):

- przypisanie na stałe adresu IP do konkretnego urządzenia (po adresie MAC),
- przydział automatyczny z wcześniej zdefiniowanej puli adresów,
- przydział dynamiczny pozwalający urządzeniom na ponowne wykorzystanie poprzednio przydzielonych adresów:
  - pula adresów zdefiniowana jak w przydziale automatycznym,
  - każdy adres jest przydzielany (dzierżawiony) na określony czas,
  - urządzenia starają się *odświeżać* dzierżawę.

Dynamic Host Conf. Protocol (DHCP) (3)



Inne komunikaty:

- `DHCPNAK` – odmowa przydziału parametrów konfiguracji,
- `DHCPDECLINE` – informacja, że adres sieciowy jest już używany,
- `DHCPINFORM` – żądanie przydziału parametrów konfiguracji bez przydziału adresu IP.

DHCP jest protokołem wykorzystującym transakcje!

dhclient – klient DHCP (1)

```
# dhclient -r -v eth0
Killed old client process
Internet Systems Consortium DHCP Client 4.3.4
...
Listening on LPF/eth0/1c:6f:65:82:11:8e
Sending on   LPF/eth0/1c:6f:65:82:11:8e
Sending on   Socket/fallback
DHCPRELEASE on eth0 to 150.254.31.62 port 67 (xid=0xb4d0356)

# dhclient -v eth0
Internet Systems Consortium DHCP Client 4.3.4
...
Listening on LPF/eth0/1c:6f:65:82:11:8e
Sending on   LPF/eth0/1c:6f:65:82:11:8e
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 7 (xid=0x1b07331)
DHCPOFFER from 150.254.31.62
DHCPREQUEST on eth0 to 255.255.255.255 port 67 (xid=0x1b07331)
DHCPACK from 150.254.31.62 (xid=0x1b07331)
bound to 150.254.31.4 -- renewal in 1781 seconds.
```

dhclient – klient DHCP (2)

```
# dhclient eth0
(rownolegle: journalctl [-e][-f] lub tail [-f] /var/log/messages)
# journalctl -f
...
Mar 24 14:44:45 tux dhclient[6363]: Created duid
                          "\000\004q\212W6$\374A\275\237W)\265\375\0138U".
Mar 24 14:44:45 tux dhclient[6363]: DHCPDISCOVER on eth0 to \
                       255.255.255.255 port 67 interval 8 (xid=0x8519f52c)
Mar 24 14:44:45 tux dhclient[6363]: DHCPREQUEST on eth0 to \
                                  255.255.255.255 port 67 (xid=0x8519f52c)
Mar 24 14:44:45 tux dhclient[6363]: DHCPOFFER from 150.254.31.62
Mar 24 14:44:45 tux dhclient[6363]: DHCPACK from 150.254.31.62 (xid=0x8519f52c)
Mar 24 14:44:45 tux NET[6391]: /usr/sbin/dhclient-script : \
                                                  updated /etc/resolv.conf
Mar 24 14:44:47 tux dnsmasq[1272]: reading /etc/resolv.conf
Mar 24 14:44:47 tux dnsmasq[1272]: using nameserver 150.254.30.30#53
Mar 24 14:47:47 tux dnsmasq[1272]: using nameserver 150.254.5.4#53
Mar 24 14:44:47 tux dhclient[6363]: bound to 150.254.31.4 -- \
                                                    renewal in 1577 seconds.
# ip addr show eth0
...
    inet 150.254.31.4/25 brd 150.254.31.127 scope global dynamic eth0
       valid_lft 2898sec preferred_lft 2898sec
```

dhclient – klient DHCP (3)

```
(czasami inna sciezka dostepu, np. /var/lib/dhcp/dhclient.leases)
$ more /var/lib/dhclient/dhclient.leases
default-duid "\000\004q\212W6$\374A\275\237W)\265\375\0138U";
lease {
  interface "eth0";
  fixed-address 150.254.31.4;
  option subnet-mask 255.255.255.128;
  option routers 150.254.31.1;
  option dhcp-lease-time 3600;
  option dhcp-message-type 5;
  option domain-name-servers 150.254.30.30,150.254.5.4;
  option dhcp-server-identifier 150.254.31.62;
  option broadcast-address 150.254.31.127;
  option domain-name "cs.put.poznan.pl";
  renew 5 2017/03/24 14:40:12;
  rebind 5 2017/03/24 15:02:59;
  expire 5 2017/03/24 15:10:29;
}
```

Zadanie 4

1. Przy pomocy programu `wireshark` loguj ruch na interfejsie `p4p1`.
2. Wymuś ponowne przydzielenie adresu z DHCP.
3. Porównaj dane z zalogowanego ruchu z zawartością logów systemowych.
4. Porównaj zawartość plików `/etc/resolv.conf` oraz `/var/lib/dhclient/dhclient.leases` (w innych dystrybucjach ścieżka może się różnić, np. `/var/lib/dhcp/dhclient.leases`).

Zeroconf

Protokół automatycznej konfiguracji urządzeń do pracy w sieci TCP/IP – Zero Configuration Networking:

- tworzenie adresów IP dla urządzeń $\longrightarrow$ `169.254.0.0/16`,
- przypisywanie nazw domenowych,
- wykrywanie urządzeń i usług w sieci, m.in., drukarek, serwerów FTP.

Popularne implementacje:

- Avahi – Linux, BSD,
- Apple Bonjour.