Wrocław
University
of Science
and Technology

Administrowanie sieciowymi systemami operacyjnymi

Wykład 3

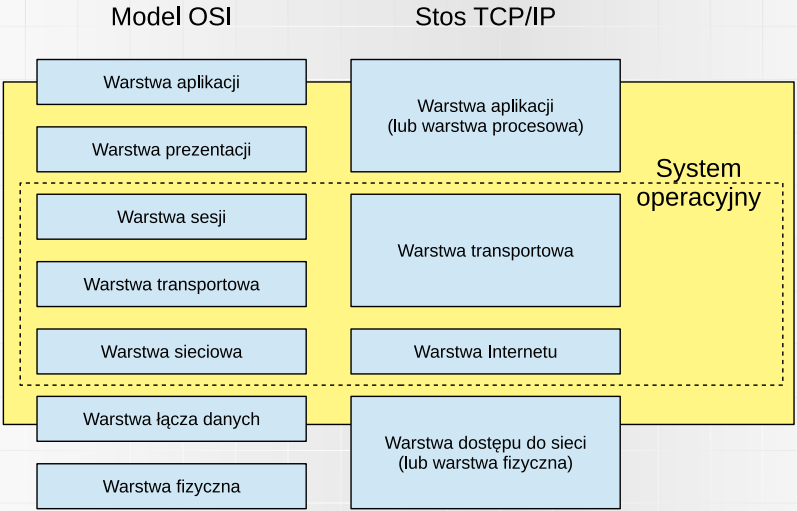
Konfiguracja warstwy sieciowej

dr inż. Jarosław Rudy

24 marca 2021

HR EXCELLENCE IN RESEARCH

Warstwy sieciowe



Warstwy sieciowe

Warstwa dostępu do sieci:

- „Niezawodny” przesył bitów i ramek pomiędzy sąsiednimi hostami (sieć lokalna).
- Adresy MAC.
- Dobór parametrów fizycznych (np. poziomy napięć).
- Korekcja, kontrola błędów, detekcja kolizji.
- Protokoły: Ethernet (IEEE 802.3), CSMA/CA, ARP itd.
- Odpowiada warstwom 1 i 2 modelu OSI.

Warstwy sieciowe

Warstwa Internetu:

- Przesył pojedynczych pakietów między odległymi hostami.
- Trasowanie.
- Nadmiarowe lub błędne pakiety są ignorowane.
- Adresy IP.
- Protokoły: IPv4, IPv6, ICMP, DNS, BOOTP, DHCP itd.
- Odpowiada warstwie 3 modelu OSI.

Warstwy sieciowe

Warstwa transportowa:

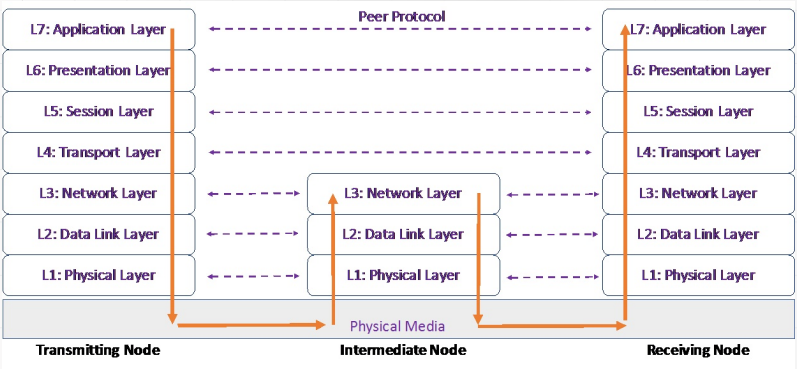
- Strumieniowanie danych w wersji połączeniowej (TCP, segmenty, handshake) lub bezpołączeniowej (UDP, datagramy).
- Kontrola kolejności dostarczania pakietów (TCP).
- Kontrola błędów, retransmisje (TCP).
- Numery portów, gniazdka (warstwa sesji).
- Protokoły: TCP, UDP itd.
- Odpowiada warstwom 4 i 5 modelu OSI.

Warstwy sieciowe

Warstwa aplikacji (procesowa):

- Interfejs dostępu do komunikacji sieciowej (gniazdka sieciowe).
- Standaryzacja kolejności bajtów (warstwa prezentacji).
- Protokoły: HTTP, HTTPS, TELNET, SSH, SSL, SMTP, IMAP, POP, FTP, NFS, ONC/RPC, NTP, PTP.
- Odpowiada warstwom 6 i 7 modelu OSI.

Warstwy sieciowe



Źródło: [1]

W praktyce stos TCP/IP nie jest ściśle warstwowy!

Konfiguracja sieci lokalnej

Sieciowe parametry konfiguracyjne:

- adres IP,
- adres domyślnego routera (bramy),
- maska podsieci (lub sufiks CIDR),
- adres serwera DNS,
- adresy innych urządzeń, serwerów i usług lokalnych:
  - drukarek sieciowych, serwera wydruku,
  - serwera proxy,
  - serwera czasu (NTP, PTP),
  - inne,
- parametry protokołów lokalnych innych niż TCP/IP.

Konfiguracja sieci lokalnej

Komenda `ifconfig`[1]:

- Listowanie interfejsów sieciowych (także nieaktywnych z użyciem flagi `-a`) wraz z ich parametrami:
  - adresy IPv4, IPv6,
  - adres MAC,
  - adres rozgłoszeniowy,
  - maska sieciowa,
  - błędy, łączny transfer itd.
- Konfiguracja podanego interfejsu.
- Wspiera różne rodziny adresów.

[1] Nie należy jej mylić z Windowsowym poleceniem `ipconfig`!

Konfiguracja sieci lokalnej

Niektóre flagi dla `ifconfig` (część wymaga praw roota):

- `up` i `down` – włącz/wyłącz interfejs.
- `arp` i `-arp` – włącz/wyłącz użycie ARP.
- `promisc` i `-promisc` – włącz/wyłącz nasłuch wszystkich pakietów.
- `mtu N` – ustawia wartość MTU (Maximum Transfer Unit) na `N`,
- `netmask addr` – ustawia maskę sieciową na `addr` (bez tego klasa maski jest wnioskowana z adresu IP).
- `broadcast addr` – ustawia adres rozgłoszeniowy na `addr`.
- Inne (multicast, zmiana MAC, tunele itd.).

Adres IP zwykle jest podawany wprost:

```
ifconfig eth0 192.168.1.2 netmask 255.255.255.0 broadcast 255.255.255.255 up
```

Konfiguracja sieci lokalnej

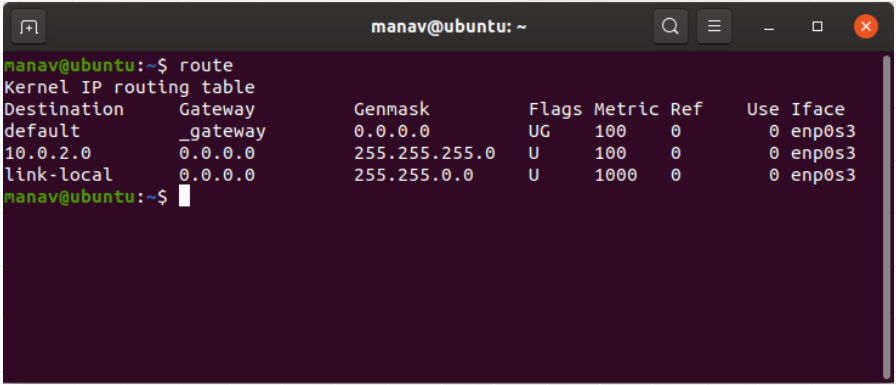
- Komenda `route` – wyświetlenie i modyfikacja tabel trasowania IP (reguły przesyłania lokalnego dla każdego interfejsu).
- Przykład dodania domyślnej bramy:

```
route add default gw 169.254.0.0
```

- Blokowanie ruchu do danego hosta lub sieci:

```
route add -host 192.168.1.51 reject
route add -net 192.168.1.0 reject
```

Konfiguracja sieci lokalnej



Źródło: [2]

Konfiguracja sieci lokalnej

Alternatywne sposoby konfiguracji sieciowej:

- Komenda `ip` (w większości obecnych dystrybucji zastępuje ifconfig):
  - Wyświetlenie informacji:

    ```
    ip addr
    ```
  - Ustawienie adresu IP i maski sieciowej:

    ```
    ip addr 156.17.42.30/8 dev eth0
    ```
  - Ustawienie adresu rozgłoszeniowego:

    ```
    ip addr add brd 156.17.42.255 dev eth0
    ```
  - Ustawienie domyślnej bramy:

    ```
    ip route add default via 192.168.1.254
    ```
  - Wyświetlenie reguł trasowania:

    ```
    ip route show
    ```

Konfiguracja sieci lokalnej

Konfiguracja poprzez plik `/etc/network/interfaces`. Przykładowa zawartość pliku:

```
auto eth0
iface eth0 inet static
     address 192.168.1.42
     network 192.168.1.0
     netmask 255.255.255.128
     broadcast 192.168.1.0
     up route add -net 192.168.1.128 netmask 255.255.255.128 gw 192.168.1.2
     up route add default gw 192.168.1.200
     down route del default gw 192.168.1.200
     down route del -net 192.168.1.128 netmask 255.255.255.128 gw 192.168.1.2
```

Podstawowa diagnostyka sieci

- Komenda `ping` – wysyłanie pakietów `ICMP` możliwość wyboru celu, odstępów, interfejsu, pola TTL. Możliwość zapisu trasy (ignorowane jednak przez wiele hostów).
- Komenda `traceroute`.

```
traceroute google.com
traceroute to google.com (172.217.10.46), 64 hops max, 52 byte packets
 1  192.168.1.1 (192.168.1.1)  1747.782 ms  1.812 ms  4.232 ms
 2  10.170.2.1 (10.170.2.1)  10.838 ms  12.883 ms  8.510 ms
 3  xx.xx.xx.xx (xx.xx.xx.xx)  10.588 ms  10.141 ms  10.652 ms
 4  xx.xx.xx.xx (xx.xx.xx.xx)  14.965 ms  16.702 ms  18.275 ms
 5  xx.xx.xx.xx (xx.xx.xx.xx)  15.092 ms  16.910 ms  17.127 ms
 6  108.170.248.97 (108.170.248.97)  13.711 ms  14.363 ms  11.698 ms
 7  216.239.62.171 (216.239.62.171)  12.802 ms
        216.239.62.169 (216.239.62.169)  12.647 ms  12.963 ms
 8  lga34s13-in-f14.1e100.net (172.217.10.46)  11.901 ms  13.666 ms  11.813 ms
```

Podstawowa diagnostyka sieci

Komenda `netstat` – pozwala wypisać otwarte połączenia sieciowe, tablice routingu, statystyki interfejsów sieciowych itd.

```
root@demo [~]# netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:imaps                     *:*                         LISTEN
tcp        0      0 *:pop3s                     *:*                         LISTEN
tcp        0      0 *:mysql                     *:*                         LISTEN
tcp        0      0 *:pop3                      *:*                         LISTEN
tcp        0      0 *:imap                      *:*                         LISTEN
tcp        0      0 *:http                      *:*                         LISTEN
tcp        0      0 *:ftp                       *:*                         LISTEN
tcp        0      0 *:smtp                      *:*                         LISTEN
tcp        0      0 *:https                     *:*                         LISTEN
tcp        0      0 localhost:mysql             localhost:45774             TIME_WAIT
tcp        0      0 192.168.1.2:https           117.237.188.240:64823       TIME_WAIT
tcp        0      0 192.168.1.2:imap            147.107.103.176:46229       ESTABLISHED
udp        0      0 demo.linuxhint.com:41687    google-public-dns-a.:domain ESTABLISHED


Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     229283964 /var/run/dovecot/imap-urlauth-worker
unix  2      [ ACC ]     STREAM     LISTENING     229283986 /var/run/dovecot/dns-client
unix  2      [ ACC ]     STREAM     LISTENING     229284018 /var/run/dovecot/auth-userdb
unix  2      [ ACC ]     STREAM     LISTENING     7312   @/com/ubuntu/upstart
unix  3      [ ]         STREAM     CONNECTED     229108430
unix  3      [ ]         STREAM     CONNECTED     229108429
unix  2      [ ]         DGRAM                    167759786
unix  3      [ ]         STREAM     CONNECTED     11814
unix  3      [ ]         STREAM     CONNECTED     10236  /var/run/dbus/system_bus_socket
unix  3      [ ]         DGRAM                    7909
```

Źródło: [3]

Trasowanie lokalne i ARP

- Określamy czy adres docelowy jest w sieci lokalnej, poprzez porównanie jego podsieci z naszą:

$$\text{adres\_odbiorcy} \wedge \text{maska} \stackrel{?}{=} \text{adres\_lokalny} \wedge \text{maska}$$

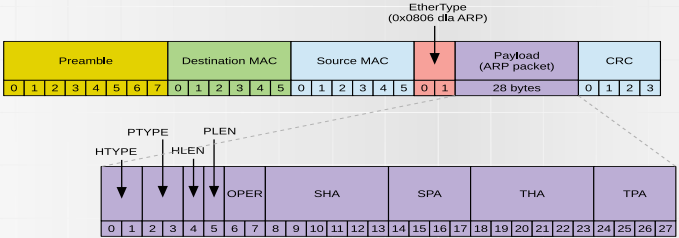
- Jeśli adres jest w tej samej sieci to wykorzystujemy jego adres IP wprost (cel bezpośredni).
- Jeśli adres jest w innej sieci to zamiast niego korzystamy z IP bramy (cel pośredni).
- W obu przypadkach pakiet wysyłamy do celu po przetłumaczeniu jego adresu IP na adres MAC.

Trasowanie lokalne i ARP

- Metody odwzorowania adresów IP na adresy MAC:
  - aktywne (np. ARP, NDP),
  - pasywne (np. nasłuch ARP),
  - statyczne (konfiguracja hosta),
  - centralna baza w Internecie (historyczne).
- Address Resolution Protocol (ARP, RFC826):
  - Protokół warstwy dostępu do sieci.
  - Hosty przechowują dynamiczną tablicę mapowań IP-MAC (ARP cache).
  - W przypadku nieznanego adresu MAC rozgłaszane jest żądanie ARP (ARP request).
  - Komputer z danym adresem odpowiada swoim adresem MAC (ARP response).
  - Komputery muszą znać własne adresy IP oraz MAC.

Trasowanie lokalne i ARP

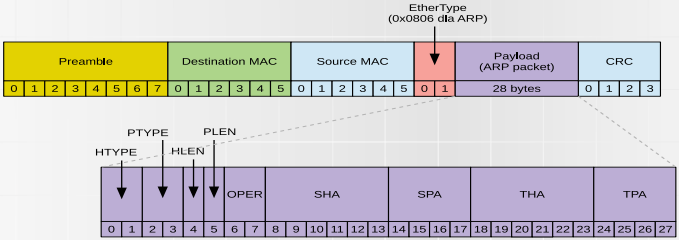
Struktura pakietu ARP (dla wersji IP over Ethernet): 28 bajtów plus 26 bajtów nagłówka Ethernet.



- `HTYPE` – typ adresu fizycznego (warstwy łącza danych) np. 1 dla Ethernetu.
- `PTYPE` – typ adresu międzysieciowego (warstwy sieciowej) np. 0x0800 dla IPv4.
- `HLEN` i `PLEN` – długości adresów fizycznych i sieciowych w bajtach (np. 6 dla Ethernetu, 4 dla IPv4).
- `OPER` – typ operacji (1 dla żądania, 2 dla odpowiedzi).

Trasowanie lokalne i ARP

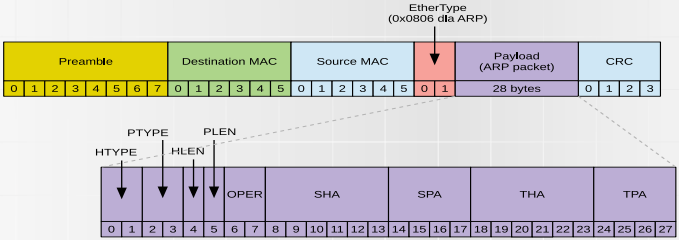
Struktura pakietu ARP (dla wersji IP over Ethernet): 28 bajtów plus 26 bajtów nagłówka Ethernet.



- `SHA` – adres fizyczny nadawcy. W żądaniu określa adres zwrotny, w odpowiedzi określa właściwą odpowiedź.
- `SPA` – adres sieciowy („protokołowy") nadawcy.

Trasowanie lokalne i ARP

Struktura pakietu ARP (dla wersji IP over Ethernet): 28 bajtów plus 26 bajtów nagłówka Ethernet.



- `THA` – adres fizyczny odbiorcy. W żądaniu ignorowany, w odpowiedzi jest adresem hosta, króry nadał ARP request.
- `TPA` – adres sieciowy („protokołowy") odbiorcy.

Trasowanie lokalne i ARP

Konfiguracja i badanie stanu mapowania IP-MAC:

- Komenda `arp`:
  - wyświetlanie aktualnego stanu tablicy,
  - modyfikacja wpisów (`arp -s` oraz `arp -d`),
  - Ma wpływ na żądania ARP kierowanie do hosta!
- Komenda `ip`:
  - wylistowanie „sąsiedztwa”

    ```
    ip neigh show
    ```

  - dodanie statycznej reguły

    ```
    ip neigh add 192.168.1.1 lladdr 46:9c:f0:3c:17:10 dev eth0 nud perm
    ```

  - czyszczenie tablicy

    ```
    ip neighbour flush
    ```

Nazwy domenowe

Domain Name System (DNS):

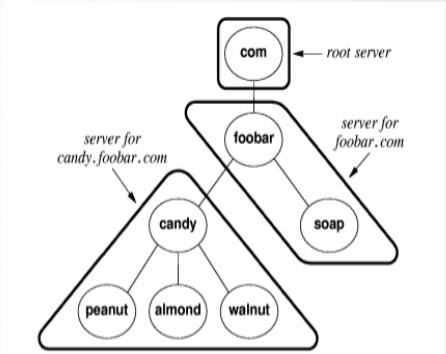
- alfanumeryczne segmenty połączone znakiem . (kropka),
- segmenty ułożone od najbardziej znaczącego (nadrzędnego) po prawej,
- niejednoznaczność – kropka nie musi odznaczać poddomeny, istnienie domen względnych, fully qualified domain name (FQDN),
- struktura hierarchiczna (drzewiasta): poddomeny rejestrowane w ramach domen nadrzędnych

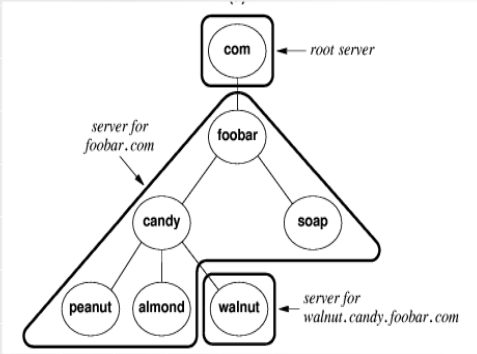
  `weka.pwr.edu.pl`

- tłumaczenie nazw domenowych na adresy IP realizowane jest przez zapytania wysyłane do serwerów DNS.
- serwery DNS zorganizowane są jako rozproszona, hierarchiczna baza danych:
  - każda domena ma główny serwer DNS (autorytatywny),
  - dla każdej domeny zdefiniowany serwer alternatywny,
  - serwery buforują fragmenty tablic tłumaczących (cache).

Nazwy domenowe

Przykład struktury serwerów DNS





Nazwy domenowe

Algorytm zamiany nazw:

- Jako protokół DNS operuje w warstwie sieciowej (dyskusyjne).
- Klient wysyła zapytanie do lokalnego serwera DNS.
- Serwer lokalny odpowiada, jeżeli zna odpowiedź (cache).
- Jeśli serwer lokalny nie zna odpowiedzi, to odpytuje dalsze serwery, zaczynając od serwera domeny głównej i dalej w dół hierarchii.
- Po uzyskaniu odpowiedzi serwer lokalny przesyła ją do klienta i zapamiętuje (cache).

Nazwy domenowe

Konfiguracja DNS:

- poprzez plik `/etc/resolv.conf` – zawiera adresy serwerów, nazwę domeny lokalnej, sufiksy itp. Prosty przykład:

  ```
  nameserver 12.34.56.78
  nameserver 12.34.56.79
  ```

- poprzez program `resolvconf` (nie mylić z powyższym plikiem!) – przydatny gdy wiele programów może modyfikować plik `/etc/resolv.conf` . Program `resolvconf` nadpisuje ten plik automatycznie (nie należy edytować go ręcznie jest `resolvconf` jest zainstalowany).
- serwery DNS można też dodać w pliku `/etc/network/interfaces` po podaniu bramy np.

  ```
  dns-nameservers 12.34.56.78 12.34.56.79
  ```

- poprzez plik `/etc/route.conf` – konfiguracja pracy resolvera: czy korzysta z tablicy `/etc/hosts`, czy i jak przetwarza odpowiedzi serwera.

Nazwy domenowe

Typy rekordów DNS:

- `A` (address) – podstawowy typ rekordu, przypisuje nazwom domenowym adresy IPv4,
- `AAAA` (IPv6 address) – przypisuje nazwom domenowym adresy IPv6,
- `NS` (name server) – mapuje nazwę domenową na listę serwerów DNS, które ją obsługują.
- `MX` (mail exchange) – przypisuje nazwom domenowym adresy IP serwerów obsługujące pocztę (plus ich priorytet),
- `CNAME` (canonical name) – definiuje nazwy alternatywne komputerów (aliasy). Powszechnie używane do definiowania stron `www`,
- `PTR` (pointer) – odwrotna translacja (adresy IP na nazwy domenowe). Korzysta z domen `in-addr.arpa` (dla IPv4) lub `ip6.arpa` (dla IPv6).

Nazwy domenowe

Komenda `host`

```
user@debian-laptop:~$ host pwr.edu.pl
pwr.edu.pl has address 156.17.16.240
pwr.edu.pl mail is handled by 10 alt4.aspmx.l.google.com.
pwr.edu.pl mail is handled by 0 aspmx.l.google.com.
pwr.edu.pl mail is handled by 5 alt1.aspmx.l.google.com.
pwr.edu.pl mail is handled by 5 alt2.aspmx.l.google.com.
pwr.edu.pl mail is handled by 10 alt3.aspmx.l.google.com.
```

```
user@debian-laptop:~$ host 127.0.0.1
1.0.0.127.in-addr.arpa domain name pointer localhost.
```

Dokładniejsze dane można uzyskać dodając flagę `-v` (verbose).

Nazwy domenowe

Komenda `dig`

```
user@debian-laptop:~$ dig pwr.edu.pl

; <<>> DiG 9.11.3-1ubuntu1.14-Ubuntu <<>> pwr.edu.pl
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53727
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;pwr.edu.pl. IN A

;; ANSWER SECTION:
pwr.edu.pl. 103 IN A 156.17.16.240

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Mar 19 16:26:06 CET 2021
;; MSG SIZE  rcvd: 55
```

Uproszczone wyjście można uzyskać z dopiskiem `+short`.

Nazwy domenowe

Komenda nslookup

```
user@debian-laptop:~$ nslookup pwr.edu.pl
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: pwr.edu.pl
Address: 156.17.16.240


user@debian-laptop:~$ nslookup 127.0.0.1
1.0.0.127.in-addr.arpa name = localhost.

Authoritative answers can be found from:
```

Bootstrap Protocol

Boostrap Protocol (BOOTP)

- Protokół pozwalający na uzyskanie adresu IP od zdalnego hosta.
- Poprzednik DHCP.
- Pozwala też na wskazanie pliku obrazu do bootowania.
- Dotyczy warstwy sieciowej (dyskusyjne).
- Zastosowanie:
  - konfiguracja stacji bezdyskowych (oprogramowanie stacji ściągane z serwera przez sieć),
  - konfigurowanie sprzętu przenośnego (notebooki),
  - konfigurowanie systemów wbudowanych.

Bootstrap Protocol

Zasada działania:

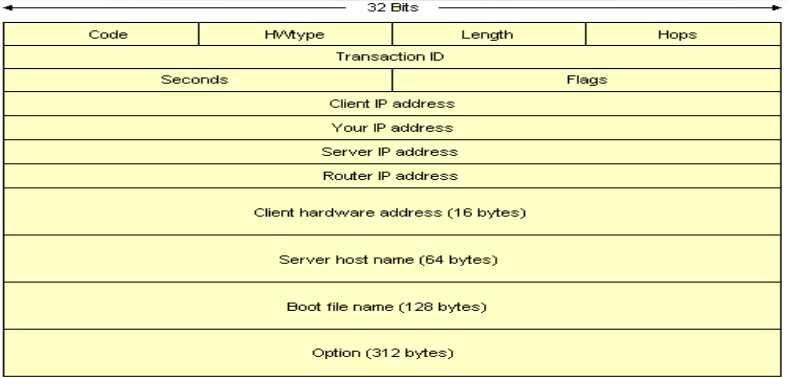
- Klient rozgłasza zapytanie BOOTREQUEST (port docelowy 67, źródłowy 68).
- Serwer sprawdza czy ma konfigurację dla danego klienta:
  - jeśli tak to ją przesyła klientowi (BOOTREPLY),
  - jeśli nie to serwer sprawdza czy ma informacje o innym serwerze BOOTP do którego należy przesłać zapytanie.
- Podczas każdego przesyłu wzrasta czas i liczba skoków.
- Pakiet jest odrzucany gdy serwer nie ma konfiguracji dla klienta i zachodzi któryś z poniższych warunków:
  - nie ma dalszego serwera do przesyłu,
  - przekroczono limit czasu lub liczby skoków.

Bootstrap Protocol

- Klient ustawia swój adres IP w zapytaniu na 0.
- Cała konfiguracja przychodzi w jednym pakiecie.
- Jeśli otrzymano dane (adres IP, nazwa pliku) do pobrania obrazu do bootowania, to klient pobiera go z wykorzystaniem TFTP (Trivial FTP).
- w przypadku gdy docelowy serwer BOOTP jest za bramą (w innej podsieci), w sieci lokalnej musi być serwer BOOTP, który przekieruje żądanie.

Bootstrap Protocol

Format pakietu BOOTP



Źródło: [4]

Bootstrap Protocol

Konfiguracja servera BOOTP na Linuksie – demon `bootpd` z pakietu `bootp`

- Odpowiedni wpis w pliku `/etc/inetd.conf`

  ```
  bootps dgram udp wait root /usr/sbin/bootpd bootpd -i -t 120
  ```

  Na Debianie można w tym celu wykonać `update-inetd --enable bootps` oraz `/etc/init.d/inetd reload`

- Utworzenie pliku `/etc/bootptab`. Przykładowo:

  ```
  client:\
    hd=/tftpboot:\
    bf=tftpboot.img:\
    ip=192.168.1.90:\
    sm=255.255.255.0:\
    sa=192.168.1.1:\
    ha=0123456789AB:
  ```

- BOOTP można też ustawić poprzez demona `dhcpd`.

Dynamic Host Configuration Protocol

- Rozszerzenie protokołu BOOTP – używa tych samych portów i bardzo zbliżonego formatu pakietów.
- Zdefiniowany w RFC 2131 (oraz w RFC 3315 dla DHCPv6).
- Pozwala na automatyczne przypisanie adresu IP, szczególnie wygodne dla stacji przenośnych.
- Dotyczy warstwy sieciowej (dyskusyjne).
- Metody przydziału adresu IP:
  - ręczna – na podstawie tabeli mapowań MAC-IP stworzonej przez administratora serwera,
  - automatyczna – adresy IP z danego zakresu przydzielane klientom zgodnie z kolejnością zgłoszeń,
  - dynamiczna – podobne do automatycznej, ale adresy są wypożyczane (dzierżawa) na określony czas.
- Dzierżawę można przedłużać (serwer może się nie zgodzić).

Dynamic Host Configuration Protocol

Dodatkowe opcje konfiguracji poza adresem IP klienta mogą obejmować:

- adres serwera DNS,
- domena,
- dane podsieci (maska, brama domyślna, adres rozgłoszeniowy),
- limit czasu oczekiwania dla ARP,
- wartość MTU,
- adresy serwerów i domena NIS (yellow pages),
- adres serwera SMTP,
- adres serwera TFTP,
- adres serwera NetBIOS,
- adres serwera WINS.

Dynamic Host Configuration Protocol

Komunikaty DHCP:

- DHCPDISCOVER – pierwszy komunikat w trybie rozgłoszeniowym,
- DHCPOFFER – oferta od serwerów DHCP,
- DHCPREQUEST – żądanie udzielenia adresu (wybierane z ofert, zwykle pierwsza otrzymana oferta),
- DHCPACK – zgoda na udzielenie adresu (ACKnowledgement), kończy proces,
- DHCPNAK – brak zgody (No AcKnowledgement), klient musi zacząć proces komunikacji od nowa,
- DHCPDECLINE – klienta uznaje konfigurację za błędną, klient musi zacząć proces komunikacji od nowa,
- DHCPRELEASE – odrzucenie adresu IP lub zakończenie dzierżawy,
- DHCPINFORM – używany w celu uzyskania pewnych dodatkowych parametrów konfiguracyjnych (zdefiniowany w RFC-2131).

Dynamic Host Configuration Protocol

Klient DHCP – program `dhclient`

- normalnie wykonuje się jako demon,
- jedna instancja obsługuje wszystkie interfejsy sieciowe,
- Konfiguracja w pliku `/etc/dhcp/dhclient.conf`,
- wywołuje skrypt `/sbin/dhclient-script`,
- lista dzierżaw w pliku

  `/var/lib/dhclient/dhclient.leases`
- można też podglądnąć syslog z pomocą

  `sudo grep dhclient /var/log/syslog`

Dynamic Host Configuration Protocol

Klient DHCP – program `dhclient`

- wywoływany w skryptach startowych systemu,
- przykładowy wpis w pliku `/etc/network/interfaces`:

  ```
  iface eth0 inet dhcp
  ```

- łagodne zakończenie pracy `dhclient`:
  - `dhclient -r` – kończy proces daemona i zwalnia wypożyczony adres,
  - `dhclient -x` – jak wyżej, ale bez zwalniania adresu.

Dynamic Host Configuration Protocol

- Server DHCP – program `dhcpd` z pakietu `isc-dhcp-server`.
- Stan przydziału adresów w pliku `/var/lib/dhcp/dhcpd.leases`
- Przykładowa konfiguracja:

```
subnet 239.252.197.0 netmask 255.255.255.0 {
range 239.252.197.10 239.252.197.250;
default-lease-time 600 max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 239.252.197.255;
option routers 239.252.197.1;
option domain-name-servers 239.252.197.2, 239.252.197.3;
option domain-name "isc.org";
}
host haagen {
  hardware ethernet 08:00:2b:4c:59:23;
 fixed-address 239.252.197.9;
}
```

Serwer czasu

Network Time Protocol (NTP)

- Synchronizacja czasu pomiędzy urządzeniami rozproszonymi w sieci o zmiennym opóźnieniu.
- Jest jednym z najstarszych protokołów Internetu wciąż w użyciu.
- Prezycja rzędu dziesiątek milisekund w rozległym Internecie i poniżej milisekundy w sieciach lokalnych.
- Alternatywą jest Precision Time Protocol (PTP) z zwiększonym wsparciem kontrolerów sieciowych (zwiększa precyzję do rzędu mikrosekund).

Serwer czasu

Konfiguracja serwera – demon `ntpd` z pakietu `ntp`

- Serwer posiada domyślną konfigurację (plik `/etc/ntp.conf`), zawierającą m.in. nazwy dalszych serwerów NTP do odpytania:

```
pool 0.debian.pool.ntp.org iburst
pool 1.debian.pool.ntp.org iburst
pool 2.debian.pool.ntp.org iburst
pool 3.debian.pool.ntp.org iburst
```

- Możliwość zmiany na serwery bliższe lub krajowe:

```
pool 0.pl.pool.ntp.org iburst
```

- Ograniczenie serwera do podsieci:

```
restrict 10.0.0.0 mask 255.0.0.0 nomodify notrap
```

- `systemctl restart ntp` – restart serwera.
- `systemctl enable ntp` – restart serwera po reboocie.

Serwer czasu

Konfiguracja klienta – program `ntpdate` z pakietu `ntpdate`

- `ntpdate nazwa_serwera` – ręczna synchronizacja z serwerem.
- W celu automatycznej synchronizacji należy dodać nazwę serwera do pliku `/etc/default/ntpdate`.

Bibliografia

- https://oracle-patches.com/en/cloud-net/4058-the-osi-model-and-the-tcp-ip-stack
- https://www.geeksforgeeks.org/route-command-in-linux-with-examples/
- https://linuxhint.com/netstat-a/
- https://www.technologyuk.net/computing/computer-networks/internet/application-layer-protocols.shtml