Rodzina protokołów TCP/IP

1. Informacje ogólne:

Rodzina protokołów TCP/IP jest obecnie dominującym standardem w transmisji w sieciach komputerowych. Głównym celem powstania TCP/IP była właśnie możliwość łączenie sieci (Internet) niezależnie od heterogenicznej struktury tych sieci w warstwach niższych. W chwili obecnej współistnieją ze sobą dwie wersje TCP/IPv4 i TCP/IPv6 przy czym z każdym rokiem wzrasta udział v6 w ruchu internetowym. W listopadzie 2018 udział procentowy użytkowników, którzy łączą się z usługami firmy Google z wykorzystaniem IPv6, osiągnął wartość 26%. Prognozuje się, że wartość ta będzie wzrastać przez następne lata o mniej więcej 4,7% na rok.

2. Standardy TCP/IP

TCP/IP zarówno w wersji 4 jak i 6 są rodzinami protokołów. Poszczególne protokoły a także niektóre zagadnienia ich współpracy są opisane odpowiednimi dokumentami RFC (Request For Comments). Te dokumenty są w praktyce standardami opisującymi działanie sieci TCP/IP. Podstawowym protokołem warstwy sieciowej jest protokół IP. W jego nagłówku zawarty jest adres przeznaczenia i adres źródłowy oraz podstawowe parametry transmisji. W ładunku użytecznym tego protokołu przenoszone (enkapsulowane) są pozostałe protokoły tej rodziny.

2.1 Adresowanie

2.1.1 IPv4

Adres składa się z 32 bitów, które są zwykle zapisywane jako cztery oktety oddzielone kropką. Oktet jest to jednostka informacji składająca się z 8 bitów. Najczęściej są one przedstawione w formacie dziesiętnym (zakres 0-255) lub w formacie binarnym jako 8 znaków (zakres 00000000-11111111). Teoretyczna przedstrzeń adresowa to 4 294 968 298 (2^{32}) adresów, w praktyce przestrzeń ta jest znacznie mniejsza ze względu na sposób adresowania (np adresowanie klasowe tab 1), sposobu podziału na podsieci (jeden adres staje się adresem sieci a drugi adresem rozgłoszeniowym), wykluczenie lub ograniczenie pewnych grup adresów (tabela 2)

Tabela 1 Wybrane zarezerwowane pule adresów IP

pula adresów	liczba adresów	obecne użycie
0.0.0.0/8	16 777 216 (2^{24})	0.0.0.0 oznacza sieć lokalną, może być używana tylko jako adres źródłowy
10.0.0.0/8	16 777 216 (2^{24})	dawna sieć DARPA, obecnie zarezerowane dla sieci prywatnych
127.0.0.0/8	16 777 216 (2^{24})	używane do adresacji interfejsów loopback
169.254.0.0/16	65 536 (2^{16})	nadawanie adresów typu link-local, np przed przypisaniem adresu przez serwer DHCP
172.16.0.0/12	1 048 576 (2^{20})	sieci prywatne
192.0.0.0/24	256 (2^{8})	blok zarezerwowany dla IANA
192.0.2.0/24	256 (2^{8})	TEST-NET-1, wykorzystywana w przykładach i dokumentacji (RFC 5737)
192.88.99.0/24	256 (2^{8})	zarezerwowane
192.168.0.0/16	65 536 (2^{16})	sieci prywatne
198.18.0.0/15	131072 (2^{17})	używane do testowania wydajności połączenia sieciowego między dwoma podsieciami
198.51.100.0/24	256 (2^{8})	TEST-NET-2, przykłady i dokumentacja (RFC 5737)
203.0.113.0/24	256 (2^{8})	TEST-NET-3, przykłady i dokumentacja (RFC 5737)
224.0.0.0/4	268 435 456 (2^{28})	używane w IP multicast
240.0.0.0/4	268 435 456 (2^{28})	zarezerwowanie dla przyszłego użycia

https://en.wikipedia.org/wiki/Reserved_IP_addresses

2.1.2 Adresacja klasowa

Pierwotnie podczas projektowania protokołu IP w wersji 4 zakładano, że adres będzie podzielony

Tabela 2 Podział na klasy

Sposób wyróżnienia	Klasa	Zakres adresów	Bity maski/uwagi
Najstarszy bit 0	A	1.0.0.0 – 127.255.255.255	8
Najstarsze bity 10	B	128.0.0.0 – 191.255.255.255	16
Najstarsze bity 110	C	192.0.0.0 – 223.255.255.255	24
Najstarsze bity 1110	D	224.0.0.0 – 239.255.255.255	specjalne przeznaczenie
Najstarsze bity 11110	E	240.0.0.0 – 254.255.255.255	zarezerwowane

2.1.3 Maska podsieci

Szybko okazało się, że stworzenie sieci klasowych nie jest wystarczającym rozwiązaniem przy ciągle rosnącej liczbie urządzeń pracujących w sieci Internet. Z tego powodu w 1987 roku wprowadzono VLSM (ang. Variable-Length Subnet Mask), czyli mechanizm maski o zmiennej długości (RFC 1109). Umożliwiał on na definiowanie dowolnego rozmiaru identyfikatora sieci w adresie IP. Kolejnym etapem było wprowadzenie w 1993 roku mechanizmu CIDR (ang. Classless Inter-Domain Routing), opisanego w RFC 1517. Jedną z głównych koncepcji było wprowadzenie nowego formatu zapisu adresu IP, który jest powszechnie stosowany do dzisiaj. Sprowadza się on do przedstawienia maski podsieci jako liczby po ukośniku, która odpowiada liczbie bitów oznaczających identyfikator podsieci (przykład: /24).

Maska podsieci jest liczbą służącą do wydzielenia z adresu IP części będacej adresem podsieci oraz części będacej adresem hosta. Maska ma taką samą długosć jak adres, czyli 32 bity dla IPv4 i 128 bitów dla IPv6. Maska zawsze zaczyna się od ciągu bitów o wartości 1, po którym następuje ciąg bitów o wartości 0.
Na podstawie adresu IP oraz maski podsieci możliwe jest obliczenie adresu podsieci, adresu rozgłoszeniowego, a także liczby hostów, które mogą być zaadresowane w danej podsieci.

Tabela 3 Metody zapisu maski podsieci

Zapis binarny	`11111111 11111111 11110000 00000000`
Zapis dziesiętny z kropką (dot-decimal notation)	`255.255.240.0`
Zapis w notacji CIDR (ang CIDR notation)	`/20`

3. Protokoły TCP i UDP

TCP

Protokół kontroli transmisji (ang. Transmission Control Protocol), jest to połączeniowy i niezawodny protokół komunikacyjny warstwy transportowej modelu OSI. Stanowi część powszechnie stosowanego stosu TCP/IP.

Nagłówek TCP składa się conajmniej z pięciu 32 bitowych słów, co łącznie daje 160 bitów. Dodatkowo zawierać może pole Opcje o zmiennej długości będącej wielokrotnością 8 bitów.

0-3	4-9	10-15	16-31
Port źródłowy			Port docelowy
Numer sekwencji			
Numer potwierdzenia (jeśli flaga ACK jest ustawiona)			
Długość nagłówka	Zarezerwowane	Flagi	Szerokość okna
Suma kontrolna			Wskaźnik priorytetu (jeśli URG jest ustawiona)
Opcje			

Budowa nagłówka TCP

Najważniejsze cechy protokołu:

- działa w trybie klient-serwer
- wykorzystuje procedury do nawiązania i zakończenia połączenia
- połączenie sterowane jest przy pomocy flag
- gwarantuje dostarczenie wszystkich pakietów z zachowaniem kolejności, bez duplikatów

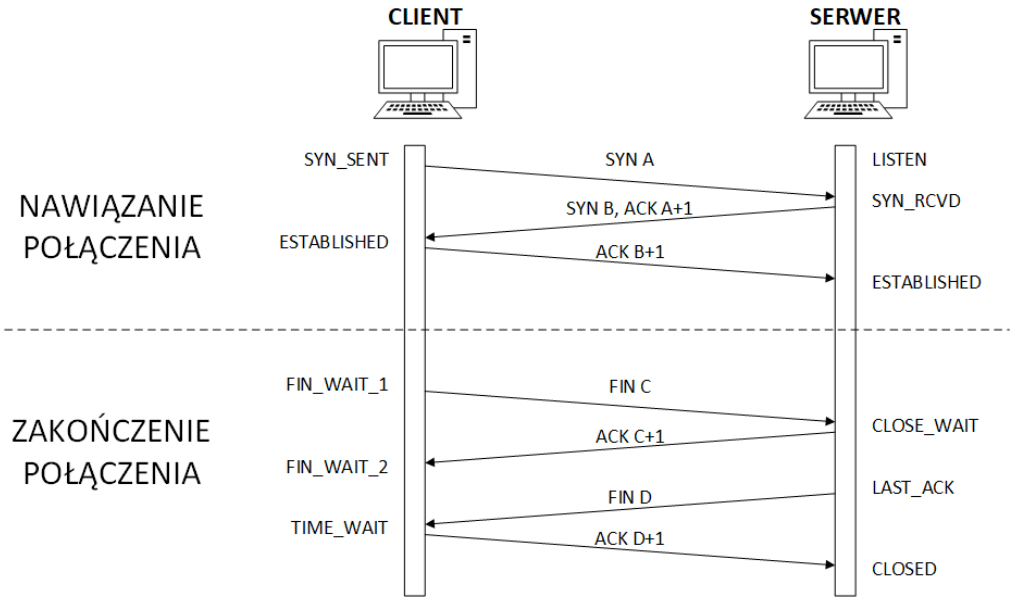
Flagi:

- NS – (ang. Nonce Sum) jednobitowa suma wartości flag ECN (ECN Echo, Congestion Window Reduced, Nonce Sum) weryfikująca ich integralność
- CWR – (ang. Congestion Window Reduced) flaga potwierdzająca odebranie powiadomienia przez nadawcę, umożliwia odbiorcy zaprzestanie wysyłania echa.
- ECE – (ang. ECN-Echo) flaga ustawiana przez odbiorcę w momencie otrzymania pakietu z ustawioną flagą CE
- URG – informuje o istotności pola "Priorytet"
- ACK – informuje o istotności pola "Numer potwierdzenia"
- PSH – wymusza przesłanie pakietu
- RST – resetuje połączenie (wymagane ponowne uzgodnienie sekwencji)
- SYN – synchronizuje kolejne numery sekwencyjne
- FIN – oznacza zakończenie przekazu danych

Mechanizm nawiązania połączenia

Jedną z najważniejszych cech protokołu sterowania transmisją jest obecność mechanizmów nawiązania i zakończenia połączenia. Nawiązanie połączenia jest opartę o procedurę zwaną *three-way handshake*. Ustanowienia połączenia wygląda następująco:

1. Klient wysyła segment SYN wraz z inicjującym numerem sekwencji np. liczbą 100 (symbol A)
2. Serwer odpowiada wysyłając segment SYN ze swoim numerem sekwencji (symbol B), a także potwierdza otrzymanie segmentu od klienta wysyłając ACK z numerem A+1.
3. Klient wysyła potwierdzenie ACK z numerem B+1 odebrania segmentu SYN od serwera.



Procedury nawiązania i zakończenia połączenia

UDP

Protokół pakietów użytkownika (ang. User Datagram Protocol) jest bezpołączeniowym protokołem komunikacyjnym warstwy transportowej modelu OSI. W przeciwieństwie do protokołu TCP nie gwarantuje dostarczenia wszystkich pakietów, ani zachowania kolejności. W zamian za to oferuje szybszą transmisję oraz mniejszy narzut danych. Nagłówek UDP składa się z 4 pól po 16 bitów.

0-15	16-31
Port źródłowy	Port docelowy
Długość datagramu	Suma kontrolna

Budowa nagłówka UDP

4. Port

Port jest to mechanizm działający na poziomie oprogramowania, który służy do identyfikacji procesów i usług sieciowych działających na danym urządzeniu. Port razem z adresem IP tworzą adres gniazda internetowego (ang. Internet socket address) w protokole TCP/IP, który jest wykorzystywany do transmisji danych między procesami na różnych urządzeniach sieciowych.
Port jest reprezentowany przez 16-bitową liczbę naturalną z zakresu 0-65535 (2^{16}). Ze względu na ograniczoną liczbę portów IANA (The Internet Assigned Numbers Authority) stworzyła rejestr portów z przypisanymi do nich usług. Cały zakres został podzielony na trzy przedziały:

- dobrze znane porty (ang. well-known ports) – numery portów z przedziału 1-1023. Nazywane są one również portami systemowymi, gdyż korzysta z nich wiele usług systemowych. Są one wykorzystywane przez najpopularniejsze usługi internetowe takie, jak FTP (20, 21), HTTP (80), czy DNS (53).
- zarejestrowane porty (ang. registered ports) – porty o numerach z przedziału 1024-49151. IANA rezerwuje dany numer portu po otrzymaniu żądania od zainteresowanej instytucji lub firmy.
- porty przydzielane dynamiczne (ang. dynamically allocated ports) – porty o numerach z przedziału 49152-65536. Porte z tej grupy przydzielane są dynamicznie do użytku tymczasowego, do wykorzystania przez prywatne usługi wewnątrz danej firmy/instytucji, czy do wykorzystania przez mechanizmy automatycznego przydzielania portów. Numery portów z tej grupy nie mogą być zarezerwowane przez IANA.

Tabela 4 Wybrane dobrze znane porty

Numer portu	opis
20	FTP (File Transfer Protocol) – przesył danych
21	FTP (File Transfer Protocol) – sterowanie
22	SSH (Secure Shell) – szyfrowane połączenie, bezpieczne logowanie, transfer plików, port forwarding
23	Telnet – nieszyftowana komunikacja tesktowa
25	SMTP (Simple Mail Transfer Protocol) – transfer poczty email między serwerami pocztowymi
53	DNS (Domain Name System) – serwer systemu nazw domenowych
80	HTTP (Hypertext Transfer Protocol) – protokół przesyłania dokumentów hipertekstowych będący podstawą sieci WWW, obecnie coraz częściej wypierany przez protokół HTTPS
110	POP3 (Post Office Protocol, version 3) – protokół wykorzystywany przez klienty pocztowe do pobierania wiadomości z serwerów pocztowych, obecnie wypierany przez protokół IMAP
143	IMAP (Internet Message Access Protocol) – protokół wykorzystywany przez klienty pocztowe do pobierania wiadomości z serwerów pocztowych, główną przewagą nad POP3 jest możliwość zarządzania skrzynką przez wiele klientów ponieważ poczta nawet po pobraniu zostaje na serwerze do momentu jawnego usunięcia jej
443	HTTPS (Hypertext Transfer Protocol over TLS/SSL) – rozwinięcie protokołu HTTP umożliwiające szyfrowany i bezpieczny transfer treści

Tabela 5 Wybrane zarejestrowane porty

Numer portu	opis
1119	Protokół Battle.net wykorzystywany do obslugi trybu multiplayer oraz chatu w grach firmy Blizzard
1194	OpenVPN – otwarty pakiet oprogramowania wykorzystujący biblioteki OpenSSL i umożliwiający tworzenie bezpiecznych połączeń VPN
1234	Domyślny port do strumieniowania UDP/RTP w programie VLC media player
1293	IPSec (Internet Protocol Security)
1581	MIL STD 2045-47001 VMF – Variable Message Format, protokół komunikacyjny służący do przesyłania informacji wojskowych
3306	System bazodanowy MySQL
3479, 3480	PlayStation Network
5004	RTP (Real-time Transport Protocol) – transfer danych
5005	RTCP (Real-time Tranport Protocol control protocol) – sterowanie
5432	System bazowanowy PostgreSQL

4. Instrukcje do użytego oprogramowania

4.1 Ping

```
ping <opcje> adres
```

gdzie <opcje> to np:
-c liczba wysłanie określonej liczny pakietów (w Windows -t)

4.3 nmap

Program nmap jest typowym skanerem portów (sprawdza otwarte porty TCP i UDP) umożliwia identyfikację usług oraz identyfikację systemu operacyjnego skanowanego hosta (na podstawie charakterystycznych cech pakietu jak TTL czy numery sekwencji:

```
nmap <typ skanowania> <opcje> adres lub zakres adresów
```

gdzie <typ skanowania>:

-sL lista hostów do skanowania (z odwrotnym DNS'em sprawdzającym nazwy hostów)
-sP tylko ping (sprawdza czy host odpowiada na echo_request)
-sT skanowanie TCP
-sU skanowanie UDP (powolne)
-sS niewidzialne skanowanie SYN
-sO skanowanie IP
-sV rozpoznawanie usług
-O rozpoznawanie systemu operacyjnego
-A rozpoznawanie systemu operacyjnego wraz z wersją usług

<opcja>:
-v więcej informacji o wykonywanych operacjach
-T[0-5] – czasowe ograniczenie procesu skanowania (0–najdłużej, 3-standardowo, 5-najszybciej)

przykład użycia

```
nmap -v -sP –T4 10.0.2.0/24 149.156.112.0/24
```

skanuje przy pomocy echo_request dwie podsieci (informacje są w postaci host up lub down)
Dodatkowo przyspieszony szablon skanowania (-T4) oraz dodatkowe informacje o skanowaniu (-v)

```
nmap -v -sV 10.0.2.1-22
```

wykrywa usługi na hostach od adresu 10.0.2.1 do 10.0.2.22

Literatura:

Hunt, Craig; TCP/IP : administracja sieci. Warszawa : Oficyna Wydaw. READ ME, 1996.
Blank, Andrew G, Podstawy TCP/IP / Andrew G. Blank ; przekł. z jęz. ang. Grzegorz Kowalski, Warszawa : Mikom, 2005.
Chappell, Laura, Wireshark Network Analysis, The Officiajl Wireshark Cerified Network Analyst Study Guide, Second Edition, 2012

Scenariusz nr 1: NMAP

Sprzęt: Komputer PC (System operacyjny CentOS 7.3)

Oprogramowanie: Nmap

Wykonanie ćwiczenia:

1. Uruchomić natywny system Linux CentOS (z menu grub)
2. Zalogować się jako na konto podane przez prowadzącego
3. Prowadzący ustala zakresy i typy skanowania wg podanych opcji:
   - **zakres** skanowanych hostów lub podsieci
     a) 10.0.2.0/24
     b) 192.168.102.0/24
     c) 149.156.111.0/24
     d) 149.156.112.0/24
     e) 149.156._._ - 149.156._._
   - **typy skanowania**, wraz z uwagami
     a) **TCP** - wykryć otwarte porty TCP - we wnioskach podać statystyki na podstawie usług wywnioskować jaki to system operacyjny
     b) **UDP**- (ograniczyć liczbę hostów lub ustawić timeout) wykryć otwarte porty UDP - we wnioskach podać statystyki na podstawie usług wywnioskować jaki to system operacyjny
     c) **SYN** - wykonać niewidzialne skanowanie - we wnioskach podać statystyki na podstawie usług wywnioskować jaki to system operacyjny
     d) Cykl skanowań dla danej sieci:
        a. Sprawdzić jakie hosty są aktywne (odpowiadają na ping, -sP)
        b. Sprawdzić mapowanie odwrotne DNS dla hostów aktywnych i nieaktywnych (–sL)
        c. Wybrać zakres obejmujący 10 hostów (zakres skonsultować z prowadzącym i uzupełnić w tabeli) i przeskanować od kątem sprawdzenia systemu operacyjnego (-O) oraz protokołów i usług IP (-sO)
     e) dla hosta …… z maską …… (podane przez prowadzącego), sprawdzić jakie hosty są aktywne w jego podsieci i przeskanować danego hosta oraz trzy inne hosty pod kątem sprawdzenia systemu operacyjnego (-O) i dostępnych usług (-sO)

Seria testów	Podsieć lub hosty	Typ skanowania	Uwagi

2. Uruchomić program nmap z odpowiednimi parametrami skanowania wg wersji podanych przez prowadzącego. (dodatkowo użyć opcji "-v")
   Standardowe wyjście najlepiej przekierować do pliku poleceniem:

   ```
   nmap typ_skanowania <opcje> zakres_adresow >/tmp/plik
   ```

3. Jeśli któreś ze skanowań trwa więcej niż 10 minut, to należy je przerwać i uruchomić z opcją (–T4). Jeśli problem się powtarza to należy użyć opcji (–T5).
4. W trakcie skanowania należy monitorować jego proces w drugim terminalu obserwując zawartość pliku za pomocą polecenia **`tail -f /tmp/plik`**

   Z zajęć należy zachować w formie elektronicznej:
   - zrzuty ekranu dla każdego skanowania na których widać uruchomioną w konsoli komendę
   - wyniki każdego skanowania w plikach tekstowych.

Wyniki pomiarów:

a) opis i charakterystyka poszczególnych typów skanowań
b) opracować statystycznie uzyskane dane (lista aktywnych hostów w danej sieci oraz ich charakterystyki, wykresy popularności usług, systemów operacyjnych, oszacować ile hostów używa filtrowania)
c) wyciągnąć wnioski w oparciu o uzyskane dane