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 ta druga wersja nie jest do dzisiaj w powszechnym użytkowaniu.

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 4 liczby oddzielone znakiem „.”. Liczny mogą być zapisywane w reprezentacji dziesiętnej (0-255 - najpopularniejszy sposób), szesnastkowej lub binarnej. Przestrzeń adresowa to teoretycznie 232=4 294 968 298 w praktyce 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 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 1111	E	240.0.0.0 – 254.255.255.255	zarezerwowane

Tabela 2 Wykorzystanie adresów IP

adresy	Obecne użycie
0.0.0.0/8	0.0.0.0 oznacza całą sieć poza lokalną
10.0.0.0/8	dawna sieć DARPA obecnie tylko dla sieci wewnętrznych
14.0.0.0/8	publiczne sieci danych
24.0.0.0/8	Telewizje kablowe
39.0.0.0/8	Zarezerwowane ale w trakcie podziału
127.0.0.0/8	localnet
128.0.0.0/16	Zarezerwowane ale w trakcie podziału
169.254.0.0/16	lokalne łącze
172.16.0.0/16	dla sieci wewnętrznych
191.255.0.0/16	Zarezerwowane ale w trakcie podziału
192.0.0.0/24	Zarezerwowane ale w trakcie podziału
192.0.2.0/24 192.88.99.0/24	Test-Net – Łączenie sieci IPv4 i IPv6
192.18.0.0/15	Połączenia międzysieciowe testowanie urządzeń
192.168.0.0-192.168.255.255	dla sieci wewnętrznych
223.255.255.0/24	Zarezerwowane ale w trakcie podziału
224.0.0.0/4	Multicast
240.0.0.0/4	Zarezerwowane dla przyszłego użycia

Do działania sieci TCP/IP wymagany jest adres IP oraz maska, adres rozgłoszeniowy (informacja przeznaczona dla wszystkich hostów w podsieci) może być wyliczony z adresu i maski podobnie jak numer sieci.

Adres bramy (gateway) jest konieczny tylko w wypadku połączeń międzysieciowych.

2.1.1 IPv6

Opracowano aby wyeliminować pewne niedostatki poprzedniej wersji głównie:

a) Mała jak na obecne potrzeby liczba adresów (co prawda stosowanie sieci wewnętrznych ograniczyło te potrzeby)
b) Brak zabezpieczeń transmisji przed zmianą czy przechwyceniem

3. Protokoły

3.1 TCP/IPv4

Protokół ARP[RFC826] i RARP

Te dwa protokoły działają na styku warstwy łącza danych niektórych sieci i warstwy sieciowej ale formalnie przypisane są do warstwy sieciowej TCP/IP. Zadaniem ARP (protokół rozwiązywania adresów) jest tłumaczenie adresów sprzętowych urządzeń na adresy IP im przypisane. Protokół RARP działa odwrotnie. ARP/RARP jest konieczny do działania TCP/IP z sieciami standardów IEEE802.x, które używają adresowania MAC. Pewna odmiana

ARP została także zaimplementowana w sieciach ATM. Tam gdzie używany jest protokóły bezpośredniego połącznia np PPP (point-to-point protocol) ARP/RARP nie jest konieczy.

Typ sprzętu (Ethernet=1)
Typ protokołu wyższego rzędu, który wysłał żądanie (IP = 0x0800)
HLEN – długość adresu sprzętowego
PLEN - długość adresu protokołu, który wysłał żądanie

Działanie - określa protokół (ARP/RARP) oraz kierunek (żądanie/odpowiedź):

1 – żądanie ARP
2 – odpowiedź ARP
3 – żądanie RARP
4 – odpowiedź RAR

Protokół IP[RFC791]

Podstawowy protokół internetu pracujący w warstwie sieci tzn podlega regułom trasowania (routowania). Oprócz adresowania jego głównym celem jest przenoszenie ładunku użytecznego w postaci protokołów warstwy transportowej oraz zapewnienie przenoszenia informacji kontrolnych o sieci (np protokół ICMP czy IGMP). Dzięki TTL internet jest automatycznie odśmiecany ze zgubionych pakietów.

VER 4b
    Wersja protokołu – 4
IHL 4b
Długość nagłówka mierzona w 32b słowach
    Długość całkowita 4b
    Długość nagłówka i danych w oktetach (576 - 65535)
Identyfikator 8b
    Identyfikator unikalny pakietu
Flagi 3b

Sterują fragmentacją

Przesunięcia fragmentu

Mierzony w jednostkach 64b – określa położenie fragmentu

TTL

Mierzony w hopach lub sekundach czas życia pakietu

Protokół

Wskazuje rodzaj protokołu warstwy wyższej TCP/IP np:

1 – ICMP 6 – TCP 17 - UDP

2 – IGMP 8 – EGP

Suma kontrolna nagłówka

Przeliczana na każdym routerze

Opcje

Pozwalają zawrzeć dodatkowe informacje np. o trasie routowania

Wypełnienie

Uzupełnia nagłówek do długości równej wielokrotności słowa 32b

Protokół ICMP[RFC792]

Typ	Kod	Suma kontrolna

Typ (8b)

Identyfikacja typu komunikatu

0 – Echo Reply

3 – Destination Unreachable

4 – Source Quench

5 – Redirect

8 – Echo Request

11 – Time Exceeded

30 - Traceroute

Kod (8b) - pole zawiera dodatkowe informacje o typie komunikatu

0 – sieć nieosiągalna

1 – host nieosiągalny

2 – protokół nieosiągalny

3 – Nieosiągalny port

4 – konieczna fragm. ale brak zezw.

5 – informacje o trasie niepoprawne

6 – nieznana sieć

7 – nieznany host

(Packet InterNet Group utility)

Wysyła pakiet ICMP z kodem Echo Request – 8 „żądanie echa”

Odbiera pakiet z kodem 0 – Echo Replay „odpowiedź echa”

Wyświetla statystki czasów odpowiedzi i ew. Kody odpowiedzi np.

Host nieosiągalny, sieć nieosiągalna ...

(tracert w Win32)

Wykorzystuje pakiet z typ 11 do rozpoznania trasy

Następnie wysyła pakiety typ 8 (opcja -I) z TTL od 1 w górę lub pakiety UDP

Wyświetla statystki czasów odpowiedzi i ew. kody odpowiedzi np. od poszczególnych routerów

Protokół UDP[RFC768]

Protokół bezpołączeniowy

- Nie trzeba nawiązywać połączenia
  - krótszy czas
- Nie obsługuje stanów połączenia
  - prostsza implementacja
  - mniej zasobów serwera
  - Można obsłużyć więcej klientów
- Mniejsze rozmiary nagłówka
  - Wydajniej wykorzystuje sieć

Niektóre aplikacje używają domyślnie protokołu UDP (DNS, RIP...)

Protokół TCP[RFC793]

Numer sekwencji

- Pozwala kontrolować przesyłanie dużych porcji danych w segmentach

Numer potwierdzenia

- Oznacza następny bajt, którego oczekuje serwer od klienta

Długość nagłówka

- Długość nagłówka mierzona w 32b słowach

Flagi 6b

- Bity znacznikowe
  - URG – pilne dane
  - ACK – oznacza konieczność potwierdzenia
  - PSH – natychmiast przesłać dane do warstwy wyższej
  - RST – zerowanie połączenia
  - SYN – nawiązywanie połączenia
  - FIN – zamykanie połączenia

Rozmiar okna odbioru

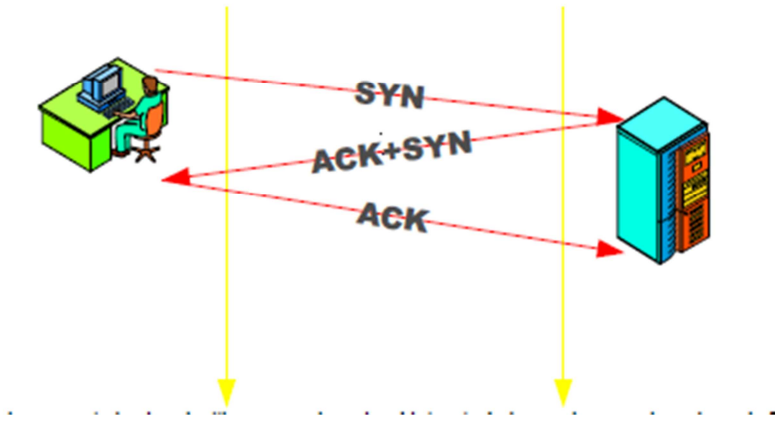
Sterowanie przepływem umożliwia zwalnianie lub przyspieszanie transmisji w zależności od wielkości i zapełnienia okna bufora u obu stron

Wskaźnik pilnych danych

Położenie ostatniego bajta pilnych danych (jeżeli ustawiono flagę URG)

Stany połączenia TCP

klient	serwer
closed	closed
sync_sent	listen
established	sync_rsvd
fine_wait1	established
fine_wait2	close_wait
time_wait	last_ack



Schemat trójdrożnego potwierdzenia (three-way hanshackin) w trakcie nawiązywania połącznie TCP.

4. Instrukcje do użytego oprogramowania

4.1 Ping

ping <opcje> adres

<opcje>

-c liczba wysłanie określonej liczny pakietów (w Windows -t)

4.2 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

<typ skanowania>

-sP tylko ping (sprawdza czy host odpowiada na echo_request), możliwe dla zwykłego użytkownika
-sT skanowanie TCP
-sU skanowanie UDP (powolne)
-sS niewidzialne skanowanie SYN
-sO skanowanie IP
-sV rozpoznawanie usług
-O rozpoznawanie systemu operacyjnego (-A działa analogicznie)

<opcja>

-v więcej informacji o wykonywanych operacjach

przykład użycia

nmap -v -sP 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)

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.

Scenariusz nr 1

Sprzęt:
Komputer PC
Procesor Intel Crore i7
RAM 8GB
SO CentOS
użytkownik student

Oprogramowanie:
Nmap

Wykonanie ćwiczenia:

Przygotowanie:

1. zalogować się jako student na konsoli graficznej bądź tekstowej

Wykonanie ćwiczenia:

1. Prowadzący ustala zakresy i typy skanowania wg podanych opcji:

◦ zakres skanowanych hostów lub podsieci

a) 10.0.2.0/24
b) 149.156.111.0/24
c) 149.156.112.0/24
d) 149.156.0.0/16
e) 149.156._._ - 149.156._._

◦ typy skanowania, wraz z uwagami

▪ **TCP** - wykryć otwarte porty TCP - we wnioskach podać statystyki na podstawie usług wywnioskować jaki to system operacyjny
▪ **UDP**- wykryć otwarte porty UDP - we wnioskach podać statystyki na podstawie usług wywnioskować jaki to system operacyjny
▪ **SYN** - wykonać niewidzialne skanowanie - we wnioskach podać statystyki na podstawie usług wywnioskować jaki to system operacyjny

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 <opcje> >/tmp/plik

3. Pierwsze skanowania (dla każdej konfiguracji) wykonać z opcją "--host_timeout 5m", kolejne bez tej opcji

4. W trakcie skanowania monitorować jego proces w drugim terminalu za pomocą polecenia ***#less /tmp/plik***

seria testów	podsieć lub hosty	typ skanowania	Uwagi
1			
2			
3			
4			

Wyniki pomiarów:

a. opis i charakterystyka poszczególnych typów skanowań
b. opracować statystycznie uzyskane dane
c. zrobić wykresy popularności usług, systemów operacyjnych, oszacować ile hostów używa filtrowania
d. wyciągnąć wnioski w oparciu o uzyskane dane