Sieci Komputerowe

Wybrane Zagadnienia

„UDP is like the adventurous intern who just sends the message and hopes for the best”

Popełnione przez

Zosia
Bajtocjanin

Kraków
Anno Domini 2024

Spis treści

1 Teoria sygnałów

1.1 Twierdzenie Fouriera

Rozsądne funkcje okresowe wyrażają się szeregiem funkcji trygonometrycznych.

$$f(x) = c_0 + \sum_{i=1}^{\infty} a_i \sin(i \cdot x) + \sum_{i=1}^{\infty} b_i \cos(i \cdot x)$$

gdzie

$$c_0 = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(x)\, dx$$

$$a_i = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \sin(i \cdot x)\, dx$$

$$b_i = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \cos(i \cdot x)\, dx$$

1.2 Twierdzenie Nyquista

Jeżeli funkcja f nie ma składowych o częstotliwościach większych niż B Hz i próbkujemy ją z częstotliwością $2B$ Hz, to możemy jednoznacznie odtworzyć f.
Maksymalna przepustowość, to $2B \log \sum$, gdzie $\sum$ to liczba bitów w każdej próbce.

1.3 Twierdzenie Shannona

Jeżeli S/N to stosunek mocy sygnału do mocy szumu, to maksymalna przepustowość, to $B \log(1 + S/N)$.

2 Model ISO-OSI i TCP/IP

2.1 Model ISO-OSI?

Open System Interconnection Reference Model - jest traktowany jako wzorzec dla większości rodzin protokołów komunikacyjnych, jego podstawowym założeniem jest podział systemów sieciowych na 7 warstw:

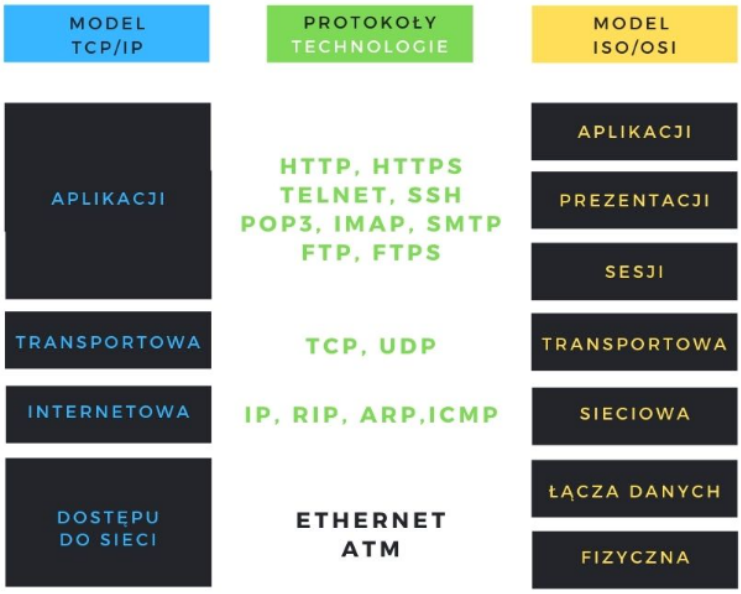
- Warstwa fizyczna
  transmisja danych pomiędzy węzłami sieci, połączenia mechaniczne, przewody elektryczne, karty sieciowe, koncentratory
- Warstwa łącza danych
  kontrola błędów podczas przesyłania, kompresja danych, mosty, przełączniki, sterowniki kart sieciowych
- Warstwa sieci
  ustanawianie, utrzymywanie i rozłączanie połączenia, wyznaczanie optymalnej trasy dla połączenia (trasowanie), rutery
- Warstwa transportowa
  dbanie o kolejność pakietów otrzymywanych przez odbiorcę, zapewnianie retransmisji w przypadku problemów
- Warstwa sesji
  nawiązywanie i zrywanie połączenia przez aplikację, realizacja zapytania o usługę (coś jak obsługa API)
- Warstwa prezentacji
  tłumaczenie danych, definiowanie formatu i odpowiedniej składni, przekształcanie danych na postać standardową, rozwiązywanie problemów z niezgodnymi reprezentacjami
- Warstwa aplikacji
  zapewnianie aplikacjom metod dostępu do środowiska OSI

2.2 Czym jest TCP/IP?

Uproszczony, 4 warstwowy model ISO-OPI

- Warstwa dostępu do sieci
  umieszczanie pakietów TCP/IP w nośniku sieciowym i ich odbiór z nośnika

- Warstwa internetu
  adresowanie, pakowanie i funkcje routowania
- Warstwa transportowa
  dostarczanie warstwie aplikacji usług sesji i data-gramowych (TCP i UDP)
- Warstwa aplikacji
  umożliwienie aplikacjom korzystania z usług innych warstw



https://ti.nstrefa.pl/wp-content/uploads/2020/11/protokoly-modelu-sieci.jpg

2.3 Nadawanie większych komunikatów

2.3.1 Sposoby synchronizacji zegara

Manchester

Zmiana sygnału w połowie każdego bitu

$1 \rightarrow 10$

$0 \rightarrow 01$

Jest odporny na zmiany szybkości transmisji i dobrze radzi sobie z długimi ciągami jednakowych bitów, wadą jest, to że trzeba używać dwukrotnie szerszego pasma przez to, że jest zmiana sygnału na początku bitu, gdy poprzedni był taki sam.

NRZI (Non-Return to Zero Invert)
Zmiana sygnału koduje 0, brak zmiany koduje 1. Nie daje sobie rady dla długich ciągów 0, bo może wtedy wystąpić desynchronizacja, dlatego zwykle używa się go łącznie z inną metodą synchronizacji, która zapewnia, że takie ciągi nie wystąpią takie jak:

- **4B/5B** Zamienia każdy 4 bitowy segment informacji w 5 bitowy segment według odpowiedniego klucza, zapewniając, że w każdym 5 bitowym segmencie znajdą się przynajmniej 2 jedynki.
- **8B/10B** Analogiczne do 4B/5B, ale dodatkowo ilość 1 i 0 jest bardziej równomierna, różnica max 1 na segment, gdzie dla 4B/5B jest to 3 na segment
- **64B/66B** Analogicznie do poprzednich, ale rośnie pokrycie łącza, używamy 97% łącza do komunikacji, zamiast 80%
- **Random Scrambling** Równoważy liczbę 0 i 1

2.4 Niwelowanie błędów komunikacji

Parity bit
Sprawdzenie parzystości, ostatni bit notuje, czy ilość jedynek w poprzednich jest parzysta

CRC (Cyclic Redundancy Check)
Obliczany poprzez dzielenie ciągu po dopisaniu do niego tylu zer, ile jest bitów w wielomianie.
$11010 \rightarrow x^4 + x^3 + x$ wielomian stopnia 4
Ponieważ pomijamy początkowe zera, to taki sam kod zostanie wygenerowany dla danych mających inną liczbę zer na początku. W Ethernecie używany był CRC32, który używa 33 bitowego dzielnika

Kody korygujące
Kody Hamminga pozwalają nie tylko sprawdzić, czy wiadomość jest poprawna, ale także ją skorygować, potrzebujemy dużo nadmiarowości, ale czasem warto.

Haszowanie

2.5 Potwierdzanie komunikacji

2.6 Strategie współdzielenia kanału komunikacji

- ALOHA
  wyślij → poczekaj → jeśli nie ma potwierdzenia, wyślij jeszcze raz

- slotted ALOHA
  Kanał jest podzielony na krótkie odcinki czasu i można zacząć nadawanie tylko na początku odcinka.
- CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
  nasłuchuj → jeśli nikt nie nadaje, to wyślij dane → jeśli była kolizja, wyślij sygnał o kolizji.
- Exponential Backoff
  * kolizja * → wylosuj liczbę odcinków czasu → poczekaj → wyślij ponownie, po i kolizjach losujemy liczbę z przedziału $[0, 2^i]$
- Tokeny
  otrzymaj token → wyślij wiadomość

3 Ethernet

3.1 Historia rozwoju

Ethernet został stworzony przez Boba Metcalfe kiedy to pracował on nad rozwojem systemu ALOHA, stworzono wtedy metodę wykrywania kolizji poprzez CSMA/CD. Pierwsza wersja powstała na bazie ALOHA w 1973 roku, ale oficjalnie opublikowana została dopiero w 1980, osiągał wtedy maksymalną przepustowość 2,94Mb/s. Później przez wiele lat udoskonalany, w 2022 roku Metcalfe dostał za ten wynalazek Nagrodę Turinga.

3.2 Ramka

Nagłówek (7 x 10101010 + 10101011)
Adres odbiorcy (6)
Adres nadawcy (6)
Typ protokołu / długość komunikatu (2)
Dane (46-1500) Suma kontrolna (4)

Rozmiar pola w bajtach	7	1	6	6	2	46 - 1500	4
Nazwa pola	Preambuła	Znacznik początku ramki	Adres MAC odbiorcy	Adres MAC nadawcy	Długość/Typ	Dane i wypełnienie	Kod kontrolny ramki (FCS)

3.3 Szczegóły Ethernetu

- Adres MAC
  Unikalny adres urządzenia fizycznego zapisywany w postaci XX:XX:XX:XX:XX:XX
- Broadcast
  FF:FF:FF:FF:FF:FF szesnastkowo transmituje wiadomość do wszystkich
- Protokół ARP (Address Resolution Protocol)
  Wysyłane jest zapytanie z adresem docelowym i adresem pytającego. Odpowiada na nie tylko host o adresie podanym w zapytaniu.
- Switche Pośredniczy w komunikacji pomiędzy urządzeniami.
- Cykle
- VLAN (wirtualna sieć lokalna)
  Fizyczna sieć podzielona na logiczne segmenty na poziomie drugiej warstwy.

3.4 Switched Ethernet

Z czasem wymyślono przełączniki (switchę), które pozwalają na segmentację sieci co znacznie usprawniło działanie Ethernetu. Przełączniki mają przekazywać ramki między urządzaniami sieciowymi, analizują otrzymaną ramkę i przesyłają ją tylko do portu docelowego. Mechanizm ten pozwala na minimalizowanie liczby kolizji przy zachowaniu przy zachowaniu wszechstronnego połączenia.

3.5 Cykle

Cykle w sieci mogą powodować zatory, komunikacja może podróżować w kółko co bez odpowiednich środków zaradczych spowoduje przeciążenie, w dodatku podczas cyklenia się adresy mac mogą być nieprawidłowo aktualizowane. Lepiej unikać.

3.6 VLAN

VLAN - (z ang. Virtual Local Area Network) pozwala na segmentację sieci LAN na mniejsze, urządzenia wewnątrz danego vlanu mogą się ze sobą bezpośrednio komunikować, natomiast żeby się skomunikować z urządzeniem z poza swojego vlanu trzeba przejść przez router.

4 Sieci mobilne

4.1 Wi-Fi

Wi-FI to standard bezprzewodowej radiowej komunikacji. Buduje się w niej wirtualne sieci lokalne oparte na routerach, przez które urządzenia się komunikują. Maksymalna przepustowość to około 1000Mbit/s.

4.1.1 wykrywanie kolizji

w technologiach radiowych niemożliwe jest wykrywanie kolizji podczas przesyłu, więc WI-FI nasłuchuje tylko na początku czy coś jest wysyłane i zaczyna wysyłać dopiero jak jest wolne, nie może przerwać w trakcie, później używa potwierdzeń, aby ustalić czy transmisja się udała.

4.1.2 Podłączanie się

Chcąc podłączyć się do sieci Wi-FI urządzenie nasłuchuje wysyłanych periodycznie przez punkty dostępowe Beacon Frame'ów, które zawierają informacje o sieci. Klient informuje punkt dostępu o chęci komunikacji i następuję negocjacja zabezpieczeń (jeśli sieć jest zabezpieczona). Większość sieci jest zabezpieczona protokołami WPA lub WPA2. Wymieniają one wtedy klucze uwierzytelniające i jeśli są one poprawne ustalane są klucze, które będą używane do komunikacji między urządzeniami. W WPA używa się do tego 4 way handshake'ów. Ustalany jest adres IP podłączonego urządzenia i można zacząć komunikacje.

4.1.3 Point to Point Wi-FI

Point to Point Wi-Fi to bezprzewodowa metoda rozprzestrzeniania łączności internetowej na dużych obszarach bez konieczności stosowania rozbudowanego okablowania. Osiąga się to poprzez utworzenie pojedynczego szybkiego łącza w optymalnej lokalizacji oraz wykorzystanie anten i sprzętu radiowego PtP do skonfigurowania dodatkowych punktów połączeń. WiFi + Ethernet Połączenie Wi-Fi i internetu polega odbywa się przez punkt dostępowy. Punkt dostępowy jest podłączony kablem do sieci Ethernet i umożliwia on komunikację urządzenia do niego podłączonym.

4.2 Sieci komórkowe

4.3 Problemy z komunikacją

- Słabnący sygnał
- Zakłócenia
- Auto-zakłócenia

- Problemy z obserwacją innych użytkowników
- Problem ukrytej stacji
  Do stacji nie docierają sygnały, które powstrzymałyby ją od wysłania wiadomości, a które docierają do odbiorcy i zakłócają przesył.
- Problem eksponowanej stacji
  Sygnały z innej stacji dosięgają tej, przez co powstrzymuje się ona od wysłania wiadomości, choć niesłusznie, bo nie docierają one do adresata.
- Kształtowanie wiązki
  Kierowanie sygnału Wi-Fi w określonym kierunku (nie we wszystkich kierunkach jak router).
- QAM w WiFi (Quadrature Amplitude Modulation)
  Tłumaczy cyfrowe paczki danych na sygnał analogowy.

4.4 Role punktów dostępu

- AP (Access Point) w WiFi
  Wzmacnia sygnał z rutera
- BTS w GSM (Base Transceiver Station)
  Stacja bazowa w systemie radiotelefonii Global System for Mobile Telecommunication (standard telefonii komórkowej)
- Nawiązywanie połączenia
- Sterowanie komunikacją
- Przekazywanie połączenia
- Bezpieczeństwo

4.5 Kontrola przepływu

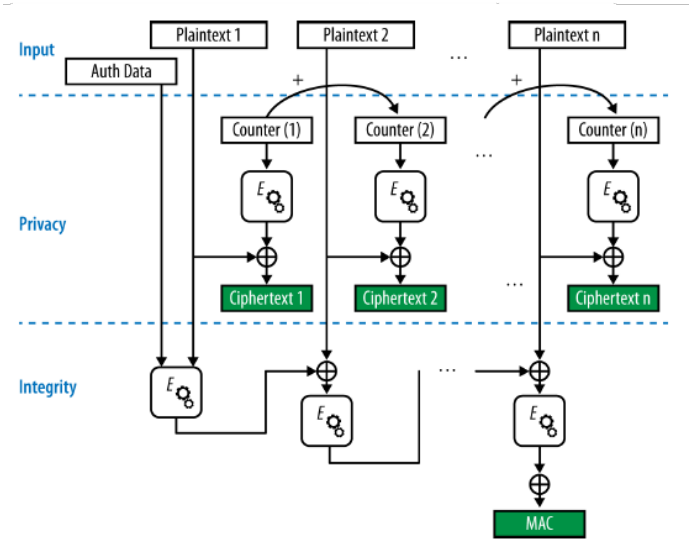
W zależności od protokołu podczas transmisji często konieczne jest wysłanie specjalnej wiadomości informującej drugą stronę o stanie transmisji np.:

- **ACK (Acknowledgement)** - wiadomość z potwierdzeniem dostarczenia poprawnej wiadomości wysyłana przez odbiorcę.
- **ARQ (Automatic Repeat Request / Query)** - retransmituje wiadomość, jeśli ACK nie przyszło przed upływem określonego czasu. Używane w przypadku zmiennej lub nieznanej przepustowości.

- **LDCP (Low-Density Parity Check)** - kody wyznaczane liniowo, które pozwalają na wykrywanie błędów w wiadomościach rzadkich
- **RTS i CTS (request to send / clear to send)** - opcjonalny mechanizm rozwiązujący problem ukrytej stacji. Działa, jeśli urządzenia z niego korzystają. Jest wykorzystywany przy przesyłaniu dużych paczek danych.

4.6 Bezpieczeństwo WiFi

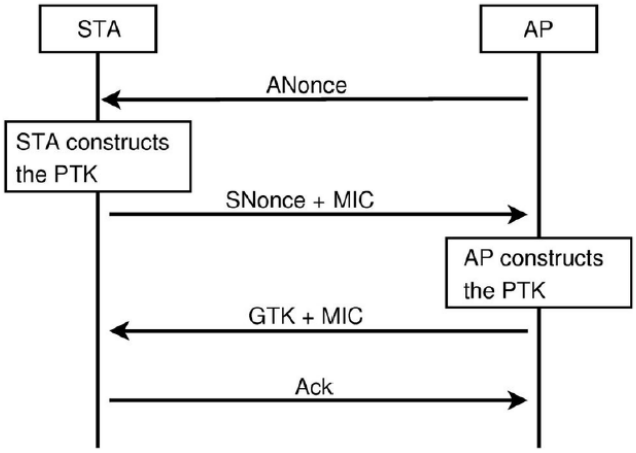
- Szyfrowanie kluczem symetrycznym AES (Advanced Encryption Standard)
  to algorytm symetrycznego szyfru blokowego o rozmiarze porcji wynoszącym 128 bitów. Konwertuje pojedyncze bloki przy użyciu kluczy o długości 128, 192 i 256 bitów. Po zaszyfrowaniu tych bloków łączy je ze sobą, tworząc zaszyfrowany tekst.
  tekst + tajny klucz → szyfr → zaszyfrowany tekst
- CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) to protokół szyfrowania stanowiący część standardu dla bezprzewodowych sieci lokalnych (WLAN). CCMP używa szyfru AES do szyfrowania wrażliwych danych. Wykorzystuje 128-bitowe klucze i 48-bitowy wektor inicjujący (CCM), do wykrywania powtórek.



CCMP = CTR + CBC-MAC
CTR (counter mode) - tryb szyfrowania **AES**, w którym wszystkie kroki można wykonywać równolegle CBC-MAC (Cipher Block Chaining Message Authentication Code) - technika

konstruowania kodu uwierzytelniającego wiadomość (MAC). Wiadomość jest szyfrowana za pomocą algorytmu szyfru blokowego w trybie łączenia bloków szyfru (CBC) w celu utworzenia łańcucha bloków w taki sposób, że każdy blok zależy od prawidłowego zaszyfrowania poprzedniego bloku. Ta współzależność gwarantuje, że zmiana dowolnego bitu tekstu jawnego spowoduje zmianę końcowego zaszyfrowanego bloku w sposób, którego nie można przewidzieć bez znajomości klucza do szyfru blokowego

- WPA-PSK (Wi-Fi Protected Access Pre-Shared Key), 4-way handshake
  WPA to protokół zabezpieczeń sieci Wi-Fi z silnym algorytmem szyfrowania oraz uwierzytelnianiem użytkownika. WPA-PSK to wersja protokołu WPA ze współdzielonym kluczem. Wszystkie podłączone stacje wykorzystują jeden wspólny klucz do autoryzacji i szyfrowania transmisji.



  PTK = Hash(Key, ANonce, SNonce, APMAC, STAMAC)

- WPA-Enterprise
  system zabezpieczeń oparty na uwierzytelnianiu klucza za pomocą serwera RADIUS, co często wiąże się z koniecznością posiadania odpowiedniego certyfikatu. W przeciwieństwie do WPA-PSK każdy użytkownik dostaje oddzielny klucz.

- SAE (Diffie-Hellman) w WPA3 (Simultaneous Authentication of Equals)
  mechanizm równoczesnego uwierzytelniania równych stron, pozwalający zapobiegać ujawnieniu komunikacji klienta, kiedy hasło zostanie odgadnięte (np. brute forcem).

4.7 Inne sieci bezprzewodowe

- LTE (Long Term Evolution)
  standard przesyłu danych w sieci 4g
- Ad-hoc
  struktura sieci bezprzewodowej bez centralnego punktu dostępu
- Sensor networks sieć czujników komunikujących się między sobą i / lub przesyłających dane do wspólnego punktu
- Bluetooth
  standard bezprzewodowej komunikacji krótkiego zasięgu
- Zigbee
  protokół transmisji danych w sieci bezprzewodowej (np. mesh, cluster tree). Podobny do Wi-Fi, ale zużywa mniej energii. Ma zasięg do 100 km.

5 Warstwa sieci (warstwa internetu)

- Adresowanie
  obliczanie adresów
  MAC → druga warstwa OSI
  IP → trzecia warstwa OSI
- Trasowanie
  wyznaczanie trasy
  Jaki powinien być algorytm trasowania?
  Jakie cele optymalizować?
  Jak zainicjalizować algorytm?
  Czy i jak go dostosowywać do sytuacji? AS -
  IGP (Interior Gateway Protocol)
  - RIP (Routing Information Protocol) (Distance Vector)
  - OSPF (Open Shortest Path First) (Link State)
  EGP (Exterior Gateway Protocol)
  - BGP (Border Gateway Protocol)
- Połączenia
  Inicjalizacja trasy
  Adresowanie

Stan trasy
Alokacja przepustowości
Transmisja pakietowa

- Łączenie różnych sieci
  Tłumaczenie adresów
  ARP (Address Resolution Protocol) - wykorzystywany, kiedy znany jest adres IP adresata, a potrzebny adres MAC (np. W sieciach lokalnych). Nadawca broadcastuje IP adresata z zapytaniem, czyj jest ten adres, a adresat odsyła w odpowiedzi swój adres MAC (translacja).
  Tłumaczenie wiadomości

- Wielu adresatów
  unicast, czyli one-to-one (karty Ethernet)
  multicast, czyli one-to-many (jeden grupowy odbiorca - host group)
  broadcast, czyli one-to-all
  anycast, czyli one-to-nearest-one

- Panowanie nad buforami
  Nadawca i odbiorca mają bufory. Nadawca może opróżnić swój dopiero po otrzymaniu potwierdzenia odbioru. Przy każdym potwierdzeniu dostaje też informacje o rozmiarze okna odbiorcy.
  Router z nieograniczonym buforem $\implies$ nieograniczone opóźnienia (dlaczego?)
  Router z dużym buforem i mechanizm TTL $\implies$ zerowa przepustowość
  Mechanizm TTL -
  Kiedy bufor zbliża się do zapełnienia, lepiej sprawdza się usunięcie losowego bufora niż najstarszego. Wtedy bardziej narażony na straty jest ten, który wysyła najwięcej pakietów Prealokacja zasobów
  Współpraca z wyższymi warstwami
  ECN (Explicit Congestion Notification) informuje nadawcę o zatorze, żeby podjąć odpowiednie działania. Oznacza pakiety poprzez odwrócenia bitu nagłówków. Hipotetyczna sytuacja:
  → X wysyła kopertę do Z dwa domy od niego.
  → X przekazuje kopertę pośrednikowi Y.
  → Jeśli Y jest zatłoczony, to stawia krzyżyk w rogu koperty i przekazuje ją dalej.
  → Kiedy Z otrzymuje kopertę i odnotowuje krzyżyk, to wie, że u któregoś z pośredników jest tłoczno.
  → Z wysyła ACK do X, również oznaczając je krzyżykiem i w ten sposób X też wie o zatorze.

QoS (Quality of Service) - charakterystyka usługi komunikacyjnej obejmująca następujące mechanizmy kształtowanie i ograniczanie przepustowości:

- Zapewnianie sprawiedliwego dostępu do zasobów
- Nadawanie odpowiednich priorytetów pakietom wędrującym przez sieć
- Zarządzanie opóźnieniami w przesyle danych
- Zarządzanie buforowaniem nadmiarowych pakietów (DRR, WFQ, WRR)
  DDR (Deficit Round Robin) - mechanizm zarządzania pamięcią
  WRR (Weighted Round Robin) - mechanizm zarządzania pakietami
  WFQ (Weighted Fair Queuing) - mechanizm zarządzania przepływami w oparciu o przpisane im wagi
- Określenie charakterystyki gubienia pakietów
- Unikanie przeciążeń (CAC, UPC)
  CAC - Connection Admission Control
  UPC - Usage Parameter Control

RED (Random Early Detection) - algorytm kolejkowania oraz unikania zakleszczeń. W tradycyjnym algorytmie router lub inne urządzenie sieciowe buforuje tyle pakietów, ile tylko może, a resztę po prostu odrzuca.

5.1 Adresy IP

0.0.0.0/8 Current network
127.0.0.0/8 Loopback
10.0.0.0/8 Private network
172.16.0.0/12 Private network
192.168.0.0/16 Private network
192.88.99.0/24 IPv6 to IPv4 relay
224.0.0.0/4 IP Multiticast
255.255.255.255 Broadcast

Maska określa, które bity muszą się zgadzać.
Multicasty są realizowane poprzez zakładanie wirtualnego adresu IP dla całej grupy odbiorców.
Zasięg adresów zaczynających się od 10 jest ograniczony do sieci prywatnej. Dlatego można nadać taki sam numer wielu urządzeniom, jeśli tylko są w różnych sieciach prywatnych.
Adresy są globalnie zarządzane przez IANA. Organizacja sprzedaje paczki adresów organizacjom na dany region świata.

CIDR -
AS -

5.2 Protokoły towarzyszące IP

- ARP (Address Resolution Protocol)
  protokół do mapowania logicznych adresów warstwy sieciowej na fizyczne adresy warstwy łącza danych
- DHCP (Dynamic Host Configuration Protocol)
  protokół komunikacyjny umożliwiający hostom uzyskanie od serwera danych konfiguracyjnych, np. adresu IP hosta
- ICMP (Internet Control Message Protocol) protokół do diagnostyki sieci i trasowania. Kontroluję transmisje danych.
- IGMP (Internet Group Management Protocol)
  protokół do zarządzania grupami multicatowymi

Gdzie to można zobaczyć?
https://www.iana.org/numbers
whois
https://stat.ripe.net

6 TCP

Połączeniowy, niezawodny, strumieniowy protokół do przesyłania sieciowego, operuje w warstwie transportowej OSI.

6.1 Nagłówek

Offset Oktet		0								1								2								3							
Oktet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Port nadawcy																Port odbiorcy															
4	32	Numer sekwencyjny																															
8	64	Numer potwierdzenia (jeżeli flaga ACK jest ustawiona)																															
12	96	Długość nagłówka				Zarezerwowane				NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Szerokość okna														
16	128	Suma kontrolna																Wskaźnik priorytetu (jeżeli flaga URG jest ustawiona)															
20 …	160 …	Opcje (jeżeli długość nagłówka > 5, to pole jest uzupełniane „0”) …																															

6.2 Sposoby na niezawodny transport

6.2.1 Niezawodne łączę

6.2.2 Łącze z błędami, ale bez traconych pakietów

- Potwierdzenia transmisji
- Retransmisje
- Błędy w potwierdzeniach

6.2.3 Łącze z błędami i traconymi pakietami

6.3 Cechy TCP

- Podczas transmisji między hostami utrzymywane jest wirtualne trwałe połączenie
- Zapewnia niezawodny transfer danych, dzięki potwierdzaniu dostarczenia i retransmisji zgubionych pakietów
- Transmisja jest dwustronna (w jedną stronę dane, w drugą potwierdzenia)
- Radzi sobie z niepoprawną kolejnością
- Steruje przepływem, zapewniając, że nie przeciąży odbiorcy dzięki mechanizmowi *sliding window*. TCP wysyła tylko tyle pakietów ile zmieści się w tym momencie w buforze użytkownika, kiedy wiadomość jest przetworzona to wysyłany jest ACK tej wiadomości wraz z aktualnym rozmiarem bufora.
- Ma uzgadnianie tożsamości poprzez handshake 6.5
- W celu weryfikacji wysyłki i poprawności datagramu używa sum kontrolnych
- Zakończenie połączenia może być zainicjowane przez dowolną stronę, wysyłany jest pakiet z flagą FIN. Operacja ta wymaga potwierdzenia pakietem z flagą FIN-ACK, w awaryjnych przypadkach można też zakończyć połączenie flagą RST (reset), co nie wymaga potwierdzenia.

6.4 Stany połączenia

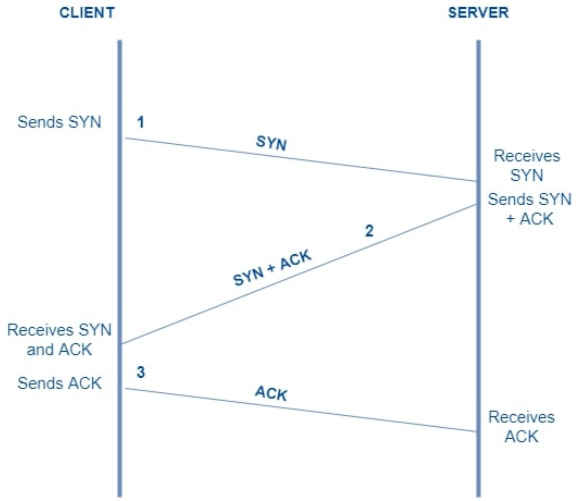
Połączenie może znajdować się w jednym z 11 stanów.

- **LISTEN**
- **SYN-RECEIVED**
- **SYN-SENT**
- **ESTABLISHED**

- **FIN-WAIT-1**
- **FIN-WAIT-2**
- **CLOSE-WAIT**
- **CLOSING**
- **LAST-ACK**
- **TIME-WAIT**
- **CLOSED**,

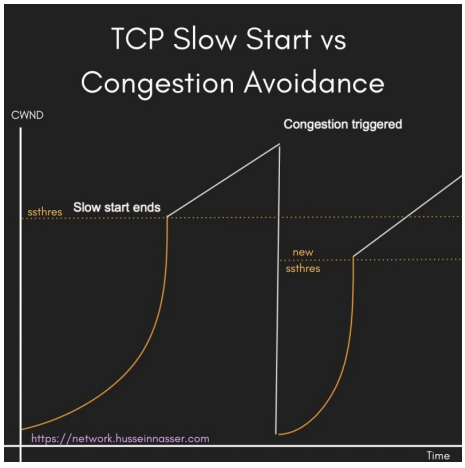
6.5 Potrójny uścisk dłoni (three-way handshake)

- Pierwsze urządzenie wysyła drugiemu wiadomość SYN (synchronize), z własnym numerem x
- Drugie urządzenie odpowiada wiadomością SYN-ACK, z własnym numerem y i potwierdzającym $x + 1$
- Pierwsze urządzenie odpowiada wiadomością ACK, z numerem potwierdzającym $y + 1$
- Drugie już nie odpowiada, synchronizacja zakończona



6.6 Slow Start

Slow start to algorytm na kontrole szybkości transmisji, gdy nie znamy prędkości łącza. Zaczynamy od bardzo powolnego przesyłu i zwiększamy jego prędkość, póki dostajemy poprawne potwierdzenie jej otrzymania. Kiedy jej nie dostaniemy to zmniejszamy prędkość. Najczęściej implementowane poprzez bin-search. Nie jest idealne, ale działa bar-



dzo dobrze kiedy wszyscy użytkownicy sieci się do tego stosują, gdyż dzieli wtedy łącze po równo.

6.7 Kontrola rozmiaru buforów

Warianty TCP:

- TCP Tahoe
- TCP Reno
- TCP Vegas

6.8 Egzaminogenne ciekawostki

- Lepiej wysyłać duże segmenty. Nagle.
- Według standardu można wysyłać priorytetowe segmenty, jednak jest to archaizm, i większość implementacji nie traktuje ich inaczej.

6.9 warianty

- **TCP Tahoe** = Slow Start + AIMD + Fast Retrasmit

7 UDP

Protokół stosowany w warstwie transportowej OSI, nie gwarantuje dostarczenia datagramu.

7.1 Nagłówek

Nagłówki są bardzo proste. Port nadawcy i suma kontrolna są opcjonalne, ale bez sumy kontrolnej nie możemy sprawdzić poprawności.

+	Bity 0 – 15	16 – 31
0	Port nadawcy	Port odbiorcy
32	Długość	Suma kontrolna
64	Dane	

7.2 Zastosowania

- DHCP - Protokół umożliwiający hostom uzyskania od serwera danych konfiguracyjnych. Musi używać UDP bo w momencie gdy prosimy serwer o te dane nie mamy jeszcze nadanego adresu IP, a TCP wymaga posiadania stałego adresu IP.
- DNS - używa UDP po komunikacje są małe i muszą być wysłane jak najszybciej to możliwe

8 Różnice między TCP a UDP

Są używane w różnych scenariuszach, TCP znacznie popularniejszy

1. **Prędkość** UDP znacznie szybszy od TCP.
2. **Połączenie**
   - TCP jest zorientowany na połączenie, podczas wysyłania danych trwa ciągła komunikacja
   - UDP wysyła wszystko jak leci, bez zastanowienia
3. **Gwarancje i kolejność pakietów**
   - TCP gwarantuje pełność i odpowiednią kolejność pakietów
   - W UDP dane mogą przyjść w złej kolejności, albo nawet wcale
4. **Zastosowania**
   - TCP używane wszędzie, gdzie potrzebne jest niezawodne połączenie i gwarancja poprawności danych
   - UDP jest używane, gdy zależy nam na przesyle o jak najmniejszym opóźnieniu, używany przede wszystkim w streamingu wideo i grach online, dla których utrata pojedynczego pakietu nie jest istotna
5. Większość implementacji faworyzuje transfer TCP nad UDP

9 HTTP

HTTP - (z ang. Hypertext Transfer Protocol) - protokół do komunikacji w sieci WWW, służy do komukacji między użytkownikiem a serwerem, oparty na TCP. Domyślnie działa na porcie 80 (HTTPS na 443).

9.1 Metody HTTP

- **GET**
- **HEAD**
- **PUT**
- **POST**
- **DELETE**
- **OPTIONS**
- **TRACE**
- **PATCH**

9.2 Nagłówki

W nagłówkach zawieramy dodatkowe informacje, takie jak data, język, typ danych czy informacje o hoście, aktualnie typów nagłówków jest bardzo dużo, w HTTP/1.0 tylko 14.
Nagłówki w HTTP/1.0

- **Date**
- **Pragma** - zależne od implementacji
- **Authorization** - hasło uwierzytelniające
- **From** - adres email proszącego o dane (archaizm)
- **If-Modified-Since** - prosi o przesłanie dokumenty tylko jeśli był zmodyfikowany od podanej daty, używany do cache'owania
- **Referer** - adres strony, z której było przekierowanie
- **Server** - identyfikuje serwer i użyte w nim oprogramowanie
- **WWW-Authenticate** - określa sposób w jaki ma zostać przeprowadzone uwierzytelnienie użytkownika
- **Allow** - określa metody http obsługiwane przez serwer
- **Content-Encoding** - podaje format kompresji treści
- **Content-Length** - długość w bajtach przesyłanej wiadomości, dla danych przesyłanych z serwera obowiązkowy
- **Content-Type** - w jakim formacie jest dokument (html, pdf i.t.d.)
- **Expires** - data, po której dokument jest nieaktualny, używany do cache'owania
- **Last-Modified** - data ostatniej modyfikacji, używany do cache'owania

9.3 Statusy

Na zapytanie dostajemy od serwera odpowiedź z kodem statusu i opcjonalnie z jakimś plikiem (jeśli się wszystko powiodło)
1xx oznaczają, że serwer otrzymał poprawny request, i jeszcze go nie prze-procesował
2xx Sukces, robię to co mi kazano
3xx Przekierowania
4xx Błąd po stronie klienta
5xx Błąd po stronie serwera
Przykładowe, i najczęściej używane statusy

- 200 OK
- 201 Created
- 202 Accepted
- 204 No Content
- 301 Moved Permanently
- 302 Moved Temporarily
- 304 Not Modified
- 400 Bad Request
- 401 Unauthorized
- 403 Forbidden
- 404 Not Found
- 418 I am a teapot
- 500 Internal Server Error
- 501 Not implemented
- 502 Bad Gateway
- 503 Service Unavailable

9.4 Porównanie protokołów

UDP jest szybszy niż TCP
TFTP(UDP) i HTTP(TCP) - różnie bywa, ponieważ TFTP zyskuje na tym, że UDP jest szybszy, ale same TFTP i HTTP są protokołami wyższej warstwy i zależą od warunków w sieci (przeciążenia, ilość danych do przesłania, itp.)
Potencjalne czynniki spowalniające

- UDP
  Pakiety mogą się gubić.
- TCP
  Wykorzystuje mechanizm sliding widow, co może ograniczać maksymalny rozmiar przesyłanych na raz danych.

Wymaga mechanizmu potrójnego uścisku dłoni do nawiązania połączenia.

- HTTP
  Nagłówki do przesyłanych danych mogą być całkiem spore (informacje o cookies, itp.).
  Wymaga dodatkowego nakładu czasu (pewnie niewielkiego) przy nawiązywaniu połączenia związanego z wymogami protokołu TCP.

- TFTP
  Maksymalny rozmiar pakietu do wysłania na raz to 512B.
  Po każdym pakiecie trzeba poczekać na ACK, zanim zostanie wysłany kolejny.

9.5 Serwery wirtualne

Można hostować więcej niż jedną domenę na jednym serwerze. Trzeba wtedy dla każdej wiadomości przychodzącej/wychodzącej z serwera ustawić stosowny nagłówek **HOST**, jest on tak czy siak wymagany od HTTP/1.1.

9.6 Ciasteczka (cookies)

Pliki cookie są zapisywane na maszynie klienta i przy niektórych requestach wysyłane z powrotem do hosta aby dostać jakieś spersonalizowane dane. Używane często do implementacji systemu logowania i utrzymywania sesji. Żeby je zapisać, serwer wysyła request z nagłówkiem **Set-Cookie**, a żeby je wysłać z powrotem, do requesta dołączamy odpowiedni nagłówek **Cookie**

9.7 Utrzymywanie połączenia

W wersjach HTTP/1.1 i nowszych może być utrzymywane stałe połączenie TCP, które zamykane jest kiedy, któraś ze stron wyśle request z nagłówkiem 'Connection: close', włączamy tą opcję dodając do wiadomości nagłówek 'Connection: keep-alive', przydatne jeśli planujemy robić dużo requestów w krótkim czasie.

9.8 Wysyłanie tylko części pliku

9.8.1 range

Przy pomocy nagłówka **range** możemy poprosić serwer o dosłanie tylko części pliku, przydatne kiedy plik jest duży i chcemy usprawnić ładowanie, można poprosić o wiele części na raz. Serwer odsyła nam częściowy plik wraz ze statusem 206 - Partial Content, jeśli wyszliśmy poza zakres dostaniemy status 416 - Range not satisfiable.

9.8.2 chunk

Możemy także przy pomocy nagłówka **Transfer-Encoding: chunked** wysłać plik w chunkach, przydatne jeśli plik jest generowany dynamicznie. Pomijamy wtedy nagłówek 'Content-Length'

9.9 Negocjacja zawartości

9.10 Trzeba trzymać standardy

Metoda **options** to prośba o przesłanie informacji na temat dostępnych metod komunikacji.

10 Bezpieczeństwo i poufność

10.1 Rodzaje zagrożeń

- Podglądanie
- Modyfikacja, usuwanie komunikatów
- Blokowanie komunikacji

10.2 Hasze kryptograficzne

- **MD4** - została złamana i można wygenerować kolizję w czasie rzędu sekund, przez to wyparta przez MD5, która jest jej następnikiem.
- **MD5** - z ciągu danych o dowolnej długości generuje 128 bitowy hasz, znaleziono sposób na generowanie kolizji, jednak i tak jest użyteczna w niektórych zastosowaniach.
- **SHA1** tworzy 160 bitowy hasz z wiadomości o rozmiarze maksymalnym 2^64 bitów, ciężki do złamani, jednak powoli się nad tym pracuje więc w nowych aplikacjach lepiej używać SHA2.
- **SHA2** - Następnik SHA1 składa się z zestawu czterech funkcji generujących odpowiednio 224, 256, 384 lub nawet 512 bitowe hasze, ma podobną implementacje co SHA1.
- **SHA3** - wyłoniony w 2012 w konkursie następnik SHA2, działa na bazie algorytmu Keccak. Ma zupełnie inną budowę niż SHA2 dzięki czemu jest znacznie wydajnieszy zachowując zbliżone parametry bezpieczeństwa.

10.3 Szyfrowanie symetryczne

Algorytmy symetryczne do szyfrowania i deszyfrowania informacji używają tego samego klucza, lub takich dwu kluczy, z których mając jeden można jednoznacznie wyznaczyć drugi. Szyfrując wiadomość wynikowy szyfr jest równy na długość wiadomości. Dzielą się na **szyfry strumieniowe**, gdzie przetwarzamy informacje bit po bicie i **blokowe** gdzie szyfrujemy naraz bloki danych i potem je sklejamy.

- **XOR** - xorujemy z kluczem. Często używany w połączeniu z innych szyfrem. Jest ekstra bo jest idealnie zbalansowany, każdy bit ma statystycznie równe szanse stać się 0 jak i 1.
- **AES** - Szyfr blokowy, o rozmiarze bloku 128 bitów, bardzo bezpieczny, zoptymalizowany pod szybkość działania i niskie zużycie pamięci, standard do szyfrowania tajnych informacji przez agencje wywiadowcze.
- **CBC** - (z ang. Cipher Block Chaining) tryb pracy szyfrów blokowych, gdzie każdy blok jest przez zaszyfrowaniem jest xorwany z szyfrem poprzedniego bloku.
- **CTR**
- **Diffie-Hellman**
- **Needham-Schroeder**
- **Needham-Schroeder (Kerberos style)**

10.4 Szyfrowanie kluczem publicznym - RSA

RSA to najpopularniejszy asymetryczny algorytm kryptograficzny. Może być stosowany zarówno do szyfrowania jak i do podpisów cyfrowych. Jego bezpieczeństwo opiera się na trudności faktoryzacji dużych liczb. Na terenie USA opatentowany więc można go tam używać tylko do celów niekomercyjnych *(america at its finest xdd)*

10.4.1 Generowanie kluczy

1. Wybieramy losowo dwie duże liczby p i q
2. obliczamy $n = p * q$
3. obliczamy $\lambda = NWW(p-1, q-1)$
4. wybieramy liczbę e względnie pierwszą z λ, z przedziału $(1, \lambda)$

5. znajdujemy liczbę d, dla której $d * e \equiv 1(mod\lambda)$

Szyfrowanie i deszyfrowanie Dzielimy wiadomość na bloki a następnie szyfrujemy i deszyfrujemy każdy blok używając wzorów.

$$c \equiv m^e \pmod{n}$$
(szyfrowanie)

$$m \equiv c^d \pmod{n}$$
(deszyfrowanie)

10.4.2 Bezpieczeństwo

Im większe liczby wybierzemy tym trudniejszy jest do złamania. W 2020r. największy złamany klucz miał 829 bitów. Potencjalnym zagrożeniem dla RSA jest skonstruowanie stabilnego komputera kwantowego, gdyż w teorii mogą one z łatwością poradzić sobie z problemem faktoryzacji, jednak na razie ze względu na niestabilność największa zfaktoryzowana przez nie liczba ma zaledwie 72 bity.

10.5 Autoryzacja

- **hasłem**
- **kluczem**
- **podpisanym kluczem**

10.6 Podpis cyfrowy

Cyfrowy podpis służy do stwierdzenia czy wiadomość pochodzi od właściwego nadawcy i nie została zmieniona podczas transmisji. Sprawdzamy czy szyfr wiadomości jest równy oczekiwanemu.

10.6.1 PGP

PGP (z ang. Preety Good Privacy) ~~ma najlepszy skrót~~ jest jednym z najczęściej używanych programów do elektronicznego podpisywania, i szyfrowania plików. Używa RSA oraz DSA.

10.7 SSL

Protokół, który umożliwia bezpieczną komunikację w Internecie w ramach HTTPS, chroni dane w warstwie transportowej poprzez ich zaszyfrowanie, pozwala na weryfikacje tożsamości i zapewnia integralność danych. zapobiega atakom man in the middle. Używa do tego podpisów cyfrowych i haszowania za pomocą SHA2.

10.7.1 Wystawianie certyfikatów

Certyfikaty SSL strony uzyskują od urzędów certyfikacji na pewien okres czasu, po tym jak sprawdzą one w jakiś sposób (np. przez to, że uruchomimy jakiś skrypt je pingujący z serwera, do którego jest podpięta domena), naszą tożsamość. Wystawiają także specjalne certyfikaty prywatnym instytucją, które umożliwiają im podpisywanie kolejnych domen, tworzy się w ten sposób łańcuch certyfikatów, gdyż każdy certyfikat, aby móc potwierdzić jego autentyczność musi także podać certyfikat wystawiającego.

10.7.2 Inicjacja połączenia

1. W trakcie handshake'u, serwer wysyła swój certyfikat SSL, albo ich łańcuch i użytkownik decyduje czy im ufać czy nie. Wysyła także informacje o metodzie szyfrowania, czasem też prosi klienta o jego certyfikat.

2. Klien generuje klucz sesji, wysyła go serwerowi szyfrując go kluczem publicznym serwera, dzięki temu tylko serwer z jego unikalnym kluczem prywatnym może odszyfrować klucz sesji.

3. Wysyłane są komunikaty potwierdzające pomyślne wymianę kluczami od teraz całość interakcji jest szyfrowana tajnym kluczem sesji.

11 Bezpieczne Sieci

Uwaga!!! Niedokończona sekcja, bo autor uznał, że musi się wyspać, tego i tak raczej nie będzie na egzaminie

11.1 IPsec

Zbiór protokołów służących do implementacji bezpiecznych połączeń obrazy wymiany kluczy szyfrowania. Polega na szyfrowaniu całego ruchu IP. Może być wykorzystany do tworzenia VPNów. IKE **IKE** (z ang. Internet Key exchange) polega na:

- Uwierzytelnieniu obu stron, przez hasło, RSA, lub certyfikaty
- nawiązaniu bezpiecznego kanału IKE
- uzgodnienie bezpiecznych kluczy kryptograficznych oraz kanału do komunikacji.

Główną zaletą jest fakt, że nie trzeba ręcznie ustawia kluczy tylko ustalić wspólne hasło i samo się zrobi

11.2 VPN

11.2.1 OpenVPN

12 Sieci P2P

Uwaga!!! Niedokończona sekcja, bo autor uznał, że musi się wyspać, tego i tak raczej nie będzie na egzaminie

12.1 BitTorrent

protokół wymiany i dystrybucji plików przez Internet, którego celem jest odciążenie łączy serwera udostępniającego pliki. Jego największą zaletą w porównaniu do protokołu HTTP jest podział pasma pomiędzy osoby, które w tym samym czasie pobierają dany plik. Oznacza to, że użytkownik w czasie pobierania wysyła fragmenty pliku innym użytkownikom.

12.2 Torrentowe Pojęcia

Peer - użytkownik, który w danym momencie pobiera i udostępnia dany plik.
Seeder - użytkownik, który posiada kompletny plik i udostępnia go innym osobom.
Tracker - serwer przekazujący informacje (adresy IP) o innych użytkownikach pobierających dany plik.
Plik .torrent - metaplik zawierający niezbędne informacje (między innymi zawartość archiwum i adres trackera, sumy kontrolne plików) do rozpoczęcia pobierania pliku.
Magnet - typ linku URI używany w torrentach, który prowadzi do jakiegoś pliku, plik jest identyfikowany poprzez jego hasz, a nie lokalizacje czy nazwę

12.2.1 DHT

Rozproszona tablica mieszająca (z ang. distributed hash table) służą w sieciach P2P do odszukania komputerów, na których znajduje się plik. Działa jak zwykła hasz mapa, ale przestrzeń adresowa jest rozrzucona po różnych komputerach, dobrze zaimplementowana jest jednak odporna na awarie urządzeń składowych.

Chord protokół do implementacji DHT w sieci P2P. Przypisujemy każdemu wierzchołkowi (urzadzeniu) zestaw kluczy, który ma zapamiętać. Robimy cykl haszy, do którego wpinają się komputery

losując hasz i przechodzimy po nim. Pamiętamy jump-pointery do kolejnych potęg dwójki, żeby było szybciej. Oczywiście część miejsc w naszym kółku będzie niezapełniona przez żadne urządzenie.

12.3 TOR

Tor to sieć, która dzięki P2P zapewnia użytkownikom prawie anonimowy dostęp do zasobów, który nie podlega analizie ruchu sieciowego. Wielowarstwowo szyfruje komunikaty (stąd ta cebula w logo). Bazuje na protokole SOCKS, który polega na wymianę pakietów przy pośrednictwie serwera proxy. Użytkownik musi mieć uruchomiony program, który łączy się z serwerem pośredniczącym (węzłem). Zwykle komunikacja przechodzi przez wiele węzłów przez co trudne jest ustalenie jej trasy.

13 Przydasie

To są ostatnie laby, które autor pominął bo uczył się na probabila

13.1 Openvpn

Uruchamianie seerwera OpenVPN:
`sudo openvpn server.ovpn`
Uruchamianie klienta OpenVPN:
`sudo openvpn client.ovpn`
Sprawdzanie połączenia:
`ping <server_ip>`
`ping <client_ip>`
Sprawdzanie przypisanego numeru IP:
`route -n`
Tu można sprawdzić nazwy urządzeń i potem wywołać
`ip addr show name`

13.2 DNS

Żeby sprawdzić adres IP domeny można wykorzystać jedno z poleceń:
`nslookup <domain_name>`
`dig <domain_name>`