Zagadnienia z Sieci Komputerowych

Na końcu są egzaminy z poprzednich lat wraz z rozwiązaniami.

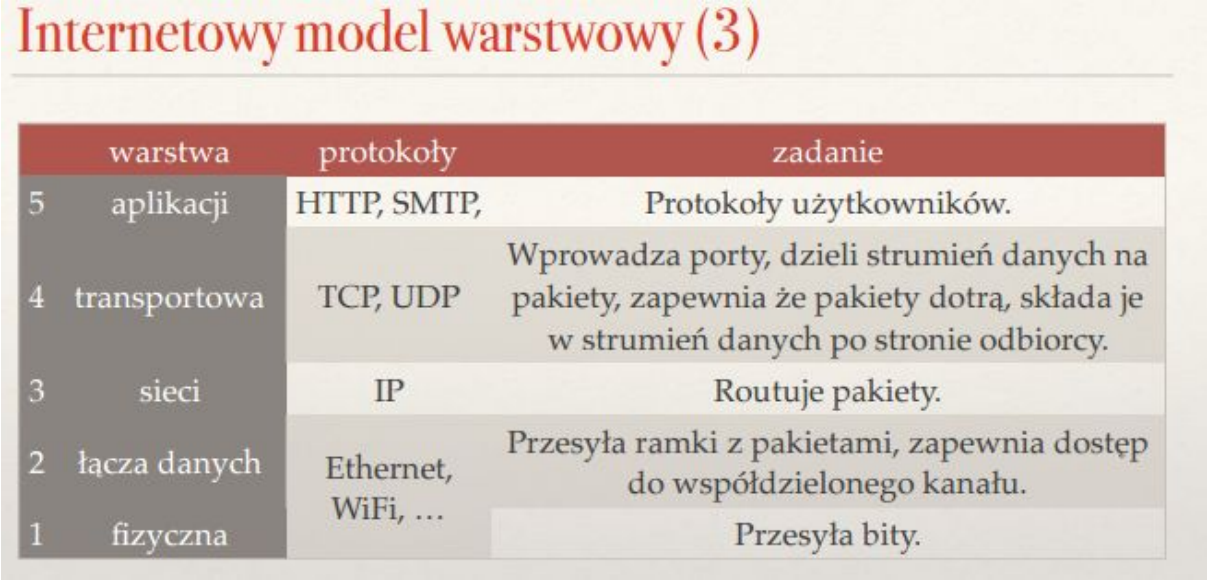
Wykład 1: Wstęp

Co to jest protokół komunikacyjny? Dlaczego wprowadza się warstwy protokołów?

Protokół komunikacyjny – zbiór ścisłych reguł i kroków postępowania, które są automatycznie wykonywane przez urządzenia **komunikacyjne** w celu nawiązania łączności i wymiany danych. **Protokół komunikacji** określa jak wygląda przesyłany **strumień danych**,

Warstwy wprowadza się w celu osiągnięcia **modularności** (łatwej wymienialności i rozwijalności).

Wymień warstwy internetowego modelu warstwowego. Jakie są zadania każdej z nich?



Jakie warstwy są zaimplementowane na komputerach a jakie na routerach?

Na komputerach są wszystkie warstwy, zaś na routerach zazwyczaj jedynie warstwy fizyczna, łącza danych oraz sieciowa. Jeśli jest to router NAT to rozumie on także warstwę transportową.

Czym różni się model warstwowy TCP/IP od OSI?

Model TCP/IP: sklejona warstwa 1 i 2.
Model ISO OSI: dodatkowe warstwy sesji i prezentacji pomiędzy warstwą 4 i 5.

Co jest potrzebne do zbudowania dwukierunkowego niezawodnego kanału?

Potok pomiędzy dwoma procesami.

Porównaj wady i zalety przełączania obwodów i przełączania pakietów.

przełączanie obwodów	przełączanie pakietów
gwarancja przepustowości	brak gwarancji
szybkie transfery danych	oczekiwanie pakietów w kolejkach
narzut czasowy na nawiązanie połączenia	narzut czasowy dla każdego pakietu (nagłówek)
marnowanie łącza jeśli są przerwy w strumieniu danych	**efektywne wykorzystanie łącza (statystyczny multipleksing)**
wolne odtwarzanie w przypadku awarii	**odporne na awarie: wybierana inna ścieżka routingu**
skomplikowane	**prostsze**

Jakie znasz rodzaje multipleksowania? Po co i kiedy się je stosuje?

Multipleksowanie to dawanie tylko fragmentu łącza dla strumienia danych. Rodzaje:

- z podziałem czasu (TDM)
- z podziałem częstotliwości (FDM)

Stosuje się je, aby efektywnie wykorzystać łącze. Dzięki temu gwarantowana jest stała szybkość, lecz łącze jest marnotrawione jeśli akurat nic nie wysyłamy.

Porównaj ze sobą rodzaje routingu.

- routing źródłowy
  Nagłówek pakietu zawiera całą trasę do celu.
- routing wykorzystujący tablice routingu
  To taki, który utrzymuje stan nazwany **tablicą routingu**.
- wirtualne przełączanie obwodów
  Polega na wysłaniu jednego pakietu (takiego zwiadowcy), który ustala ścieżkę do celu, konfiguruje routery i być może rezerwuje część łącza, cała reszta danych leci tą samą ścieżką.

Do czego służy polecenie traceroute? Co pokazuje?

Polecenie traceroute służy do podglądnięcia jaką trasą wędrują pakiety w sieci IP. Pokazuje adres IP kolejnego routera i czas dotarcia do niego.

Po co stosuje się bufory w routerach? Co to jest przeciążenie?

Bufory w routerach stosuje się, gdy możliwości łącza wychodzącego są za małe, aby przekazać wszystkie dane z łącza wejściowego, w takim wypadku pakiety trafiają do bufora (zwyczajowo kolejki) i dopiero z niego są przesyłane dalej. Przeciążenie to sytuacja, gdy bufor się zapełni i nie będzie w stanie zapamiętać kolejnego pakietu. W takiej chwili pakiety są odrzucane przez router. (Jest to podobno główna przyczyna utraty pakietów w internecie.)

Jakie są przyczyny opóźnień pakietów?

Opóźnienie pakietu na łączu = czas oczekiwania pakietu w kolejce + rozmiar pakietu / przepustowość + czas propagacji.

Co to jest BDP? Co to jest czas propagacji?

Bandwidth-Delay product - iloczyn przepustowości i RTT = „ile danych może naraz pomieścić kanał“

Wyjaśnij pojęcia: komunikacja simpleksowa, półdupleksowa, pełnodupleksowa.

Simpleksowa : Komunikacja odbywa się wyłącznie w jedną stronę od nadawcy do odbiorcy.
Półdupleksowa : Oba urządzenia mogą nadawać i odbierać jednak nie jednocześnie.
Pełnodupleksowa : j.w. tylko bez ograniczenia.

Co umożliwia protokół IP? Co to znaczy, że protokół realizuje zasadę best effort?

Umożliwia przesyłanie pakietu pomiędzy dwoma urządzeniami w sieci. Definiuje zawodną, bezpołączeniową usługę.
Best effort to znaczy, że protokół nie daje gwarancji, że pakiet dotrze do adresata, lecz nie będzie gubił pakietów celowo..

Jakie są zalety i wady zasady end-to-end?

+ łatwa ewolucja
+ niski koszt innowacyjności
– słabo z rozwijaniem gotowej architektury

Po co wprowadza się porty?

Chcemy zapewnić niezawodny kanał komunikacyjny pomiędzy aplikacjami. Porty są sposobem identyfikowania aplikacji na komputerze.

Wyjaśnij pojęcie enkapsulacji i dekapsulacji.

Enkapsulacja to dodawanie przez kolejne warstwy Internetowego modelu warstwowego swoich nagłówków do przechodzącego przez nie pakietu. Dekapsulacja to usuwanie.

Wykład 2: Routing (adresowanie)

Z czego wynika hierarchia adresów IP? Jaki ma wpływ na konstrukcję tablic routingu?

No bo są sieci i one się w sobie zawierają. I przez to wiemy że można wysyłać do mniejszych sieci, bo te większe zawierają mniejsze.

Notacja CIDR.

Classless Inter-Domain Routing - opisuje zakres adresów IP za pomocą pary (pierwszy adres sieci, długość prefiksu).

Co to jest adres rozgłoszeniowy?

Ostatni adres sieci. Pakiet wysyłany na adres rozgłoszeniowy dotrze do wszystkich adresów IP z zakresu.

Co to jest maska podsieci

Długość prefiksu notacji CIDR.

Opisz sieci IP klasy A, B i C.

IP zaczynające się od 0 należą do klasy A (prefiks /8)
IP zaczynające się od 10 należą do klasy B (prefiks /16)
IP zaczynające się od 110 należą do klasy C (prefiks /24)

Co to jest pętla lokalna (loopback)?

Jest to sieć 127.0.0.0/8, łącząc się z dowolnym adresem tej sieci łączymy się z lokalnym komputerem, pozwala to na testowanie aplikacji sieciowych bez połączenia się z siecią.

Do czego służy pole TTL w pakiecie IP? Do czego służy pole protokół?

TTL (Time To Live) określa ile jeszcze razy może być przekazany pakiet, jeśli TTL pakietu jest równe 0 wtedy router wyrzuca taki pakiet.

Pole protokół określa datagram jakiego protokołu przechowywany jest w danych pakietu (1 - ICMP, 6-TCP, 17-UDP).

Jakie reguły zawierają tablice routingu?

Prefiks - router/komputer; „jeśli adres docelowy pakietu zaczyna się od prefiksu A, to wyślij pakiet do X“. Pakiet niepasujący do żadnej reguły jest odrzucany.

Na czym polega reguła najdłuższego pasującego prefiksu?

W przypadku, gdy do adresu pasuje wiele reguł router wybiera tę, która pasuje na najdłuższym prefiksie (najbardziej konkretną regułę).

Co to jest trasa domyślna?

Jest to trasa przez którą przechodzą pakiety jeśli nie dopasowują się do żadnej z reguł. (Tak naprawdę jest to sama w sobie reguła postaci 0.0.0.0/0.)

Do czego służy protokół ICMP? Jakie znasz typy komunikatów ICMP?

Internet Control Message Protocol to pomocniczy protokół warstwy trzeciej(sieci) służący do zbierania informacji o sieci samej w sobie.
Typ 8 - echo req
Typ 0 - echo reply
Typ 11 podtyp 0 - Time exceeded

Jak działa polecenie ping?

Wysyłamy ICMP o typie 8 (echo req) odbiorca wysyła na ICMP o typie 0 (echo reply), możemy na tej podstawie obliczyć RTT (round trip time).

Jak działa polecenie traceroute?

Wysyłamy ICMP o typie 8 (echo req) o coraz większych TTL aż nie osiągniemy celu. Stąd możemy dowiedzieć się jakie są kolejne routery na trasie do naszego celu.

Dlaczego do tworzenia gniazd surowych wymagane są uprawnienia administratora?

Ponieważ omijają one warstwę transportową.

Co to jest sieciowa kolejność bajtów?

Kolejność bajtów wymagana przez protokoły (big endian) i powszechnie używana w sieci.

Co robią funkcje socket(), recvfrom() i sendto()?

socket - tworzy gniazdo służące do wysyłania i odbierania
recvfrom - odbiera kolejny pakiet z kolejki związanej z gniazdem

sendto - wysyła pakiet przez gniazdo

Jakie informacje zawiera struktura adresowa sockaddr_in?

- Rodzinę adresów. W przypadku TCP lub UDP jest nią zawsze AF_INET.
- Numer portu.
- Adres IP.

Co to jest tryb blokujący i nieblokujący?

Tryb blokujący to taki w którym nasz program się blokuje czyli czeka na otrzymanie jakiejś informacji. Tryb nieblokujący to taki który jedynie sprawdza czy jest jakaś informacja do odebrania.

Jakie jest działanie funkcji select()?

select - czekanie maksymalnie x sekund na pakiet w gnieździe sockfd. Jeśli wynik funkcji jest:

- < 0 oznacza to błąd
- = 0 oznacza to timeout
- > 0 tyle obserwowanych deskryptorów jest gotowych do odczytu

Wykład 3: Routing (tworzenie tablic)

Co to jest cykl w routingu? Co go powoduje?

Cykl w routingu to pakiet krążący w kółko. Cykle powstają zazwyczaj na skutek awarii sieci.

Czym różni się tablica routingu od tablicy przekazywania?

tablica przekazywania (forwarding table) - zawiera informacje o następnym routerze na trasie. Jest to silnie zoptymalizowana struktura danych wspomagana sprzętowo.
tablica routingu - zawiera informacje o trasach oraz dodatkowe informacje np. zapasowe trasy routingu

Dlaczego w algorytmach routingu dynamicznego obliczamy najkrótsze ścieżki?

Aby pakiety docierały najszybciej do celu jak to możliwe. Zależnie od metryki może to pozwolić nam oszczędzić różne zasoby takie jak czas czy też pieniądze. Dodatkowo zapobiega to powstawaniu cykli.

Co to jest metryka? Jakie metryki mają sens?

Metryka to funkcja pozwalająca na określanie odległości pomiędzy obiektami. W sieciach mają sens metryki, które optymalizują jakiś zasób. Takimi metrykami mogą być koszt pieniężny, czy też czas propagacji.

Czym różnią się algorytmy wektora odległości od algorytmów stanów łączy?

Algorytm stanu łączy powiadamia wszystkich o swoim bezpośrednim sąsiedztwie, na podstawie sąsiedztw buduje graf sieci i lokalnie oblicza najkrótsze ścieżki.
Algorytm wektora odległości okresowo powiadamia sąsiadów o całej swojej tablicy przekazywania i aktualizuje tablice routing na tej podstawie.

Jak router może stwierdzić, że sąsiadujący z nim router jest nieosiągalny?

Sąsiadujące routery co chwilę wysyłają sobie pakiety kontrolne, lub dzięki zliczaniu do nieskończoności. Możemy też nie otrzymać od sieci żadnej informacji przez jakiś okres czasu.

Co to znaczy, że stan tablic routingu jest stabilny?

Stan tablic routingu jest stabilny jeśli kolejne informacje nie zmieniają wektora odległości.

Jak zalewać sieć informacją? Co to są komunikaty LSA?

Zalewamy sieć informacją gdy te same pakiety są wysyłane przez ten sam router. LSA (Link - State Advertisement) to stan pojedynczego łącza (wykorzystywany w protokole OSPF) zawiera informacje o źródle pakietu i numer sekwencyjny. Jest to informacja o jednej krawędzi w grafie sieci.

Co wchodzi w skład wektora odległości?

Wektor odległości zawiera odległości do znanych mu routerów i sieci.

W jaki sposób podczas działania algorytmu routingu dynamicznego może powstać cykl w routingu?

Jak coś się zepsuje i informacja o awarii nie rozejdzie się dość szybko.

Co to jest problem zliczania do nieskończoności? Kiedy występuje?

Kiedy następuje awaria sieci (np. w algorytmie wektorów odległości) a informacja o awarii nie dojdzie do sąsiedniego routera wystarczająco szybko, a nasz router uaktualni sobie informacji na podstawie wektora odległości swojego kolegi (którego trasa przebiegała przez ten router), to w następnej rundzie ten kolega sobie powiększy o 1 odległość w następnej my i tak w nieskończoność.

Na czym polega technika zatruwania ścieżek?

Jeżeli X jest wpisany jako następny router na ścieżce do Y to wysyłamy do X info “mam do Y ścieżkę nieskończoną”

Po co w algorytmach wektora odległości definiuje się największą odległość w sieci (16 w protokole RIPv1)?

Bo czasem zatruwanie ścieżek i inne tricki zawodzą, więc nieskończoność nie może być zbyt wielka podczas zliczania do nieskończoności.

Po co stosuje się przyspieszone uaktualnienia?

Pomaga to przy unikaniu cykli. Szybciej informujemy o awarii. Możemy dzięki temu uniknąć zliczania do nieskończoności.

Co to jest system autonomiczny (AS)? Jakie znasz typy AS?

Jest to spójny kawałek sieci w posiadaniu jakiegoś ISP. AS może być:

- Tranzytowy
- Nie tranzytowy z wieloma wyjściami
- Z jednym wyjściem

Czym różnią się połączenia dostawca-klient pomiędzy systemami autonomicznymi od łącz partnerskich (peering)?

Za te pierwsze się płaci. Te drugie to współpraca pomiędzy ISP.

Dlaczego w routingu pomiędzy systemami autonomicznymi nie stosuje się najkrótszych ścieżek?

Bo światem rządzi pieniądz (ze względów polityczno-ekonomicznych).

Które trasy w BGP warto rozgłaszać i komu? A które wybierać?

Zawartość naszego AS trzeba rozgłosić wszystkim, bo inaczej nikt do nas nie trafi.
Trasy do naszych klientów należy rozgłaszać wszystkim, bo za to nam oni płacą.
Szczególnie należy je rozgłaszać naszym partnerom, bo za to nie płacimy. Trasy do naszych dostawców należy rozgłaszać jedynie naszym klientom. Trasy do naszych partnerów rozgłaszamy zazwyczaj tylko klientom.
Innymi słowy rozgłaszamy:

- Zawartość naszego AS (prefiksy CIDR):
    - Inaczej nikt do nas nie trafi.
- Trasy do naszych klientów:
    - Tak, bo klienci nam płacą, za przesyłane dane.
    - Szczególnie warto rozgłaszać je naszym partnerom, bo to jest ruch za który nie płacimy.
- Trasy do naszych dostawców:
    - Naszym klientom tak.
    - Poza tym nie: nie chcemy, żeby inni przesyłali przez nasz AS ruch do naszego dostawcy (my płacimy, nam nie płacą).
- Trasy do naszych partnerów:

    - Naszym klientom tak.
    - Poza tym zazwyczaj nie.

Wybór polega na:
Wiele możliwości dotarcia do jakiejś sieci (prefiksu CIDR)

- Zazwyczaj wybór najkrótszej trasy (najmniejsza liczba AS).
- Ale można zmienić taki wybór. Częsta polityka:
    - wybierz najpierw trasę przez swojego klienta,
    - potem przez partnera,
    - a na końcu trasę przez dostawcę.

Jak BGP współpracuje z algorytmami routingu wewnątrz AS?

- Routery brzegowe danego AS (via BGP):
    - rozgłoś prefiksy CIDR tego AS;
    - dowiedz się o trasach do innych AS.
- Opcje:
    - AS z jednym wyjściem X:
        - Ustal routing wewnątrz AS (OSPF lub RIP lub IS-IS lub …)
        - Dodaj X na wszystkich routerach jako bramę domyślną.
    - AS z wieloma wyjściami X1,X2,X3,…, opcja 1 (hot-potato routing)
        - Ustal routing wewnątrz AS (bez udziału zewnętrznych tras).
        - Każdy router wybiera najbliższy Xi jako bramę domyślną.
        - Informacja o dostępnych trasach musi być synchronizowana między routerami Xi (protokołem iBGP).
    - AS z wieloma wyjściami X1,X2,X3,…, opcja 2:
        - Routery Xi biorą udział w protokole routingu wewnątrz AS udostępniając trasy, których nauczyły się przez BGP jako swoje „sąsiedztwo“ (z odpowiednimi odległościami).
        - Lepsze trasy ale każdy router musi przechowywać informacje o wielu sieciach.

Jeśli AS ma tylko jedno wyjście to na każdym routerze ustawiamy je jako bramę domyślną.
AS z wieloma wyjściami synchronizuje routery ustawiając im bramę domyślną na najbliższy router wyjściowy. (hot-potato routing) Informacja pomiędzy routerami wyjściowymi musi być w takim wypadku synchronizowana na przykład za pomocą protokołu iBGP.
Można też zastosować drugą opcję mianowicie użyć protokołu na całej znanej sieci włączając w to to co wiedzą routery wyjściowe.

Wykład 4: Routing (wewnątrz routera)

Co to są prywatne adresy IP? Jakie pule adresów są zarezerwowane na takie adresy?

Adresy prywatne to adresy przeznaczone do sieci lokalnych. Pula adresów to:
* 10.0.0.0/8 (1 adres klasy A),
* 172.16.0.0/12 (16 adresów klasy B)
* 192.168.0.0/16 (256 adresów klasy C)

Co robi funkcja bind()?

Funkcja bind() związuje serwer z danym portem.

Czym różnią się porty o numerach mniejszych niż 1024 od innych? Co to są porty efemeryczne?

Port od numerach <= 1024 wymagają uprawnień administratora do dostępu. Porty efemeryczne to porty przydzielane usługom automatycznie (tymczasowe zazwyczaj >= 32768).

Jakie są zadania procesora routingu, portu wejściowego, portu wyjściowego, struktury przełączającej?

Procesor routingu tworzy tablicę przekazywania i wysyła je do portów wejściowych oraz dba o strukturę przekazującą jeśli taka istnieje.
Port wejściowy odbiera pakiety z łącza, uaktualnia nagłówek i sprawdza do którego portu wyjściowego go przesłać.
Port wyjściowy to miejsce do którego zapisywane są pakiety.
Struktura przełączająca to struktura wiążąca porty wejściowe z wyjściowymi w odpowiedni sposób.

Na czym polega przełączanie pakietów za pomocą RAM w routerze od przełączania za pomocą sieci?

W pierwszym z tych podejść procesor wykonuje całą pracę. Od rozpoznania pakietów przez przypisanie go do odpowiednich portów wyjściowych oraz skopiowanie go z portu wejściowego do RAM, a następnie z RAM do portu wyjściwego.
W drugim podejściu struktura przełączników zajmuje się bezpośrednim przesyłaniem danych, a procesor ustala jedynie strukturę przełączników.

Jakie są pożądane cechy struktury przełączającej w routerze?

Przekazywać pakiety z prędkością zbliżoną do szybkości łącza.

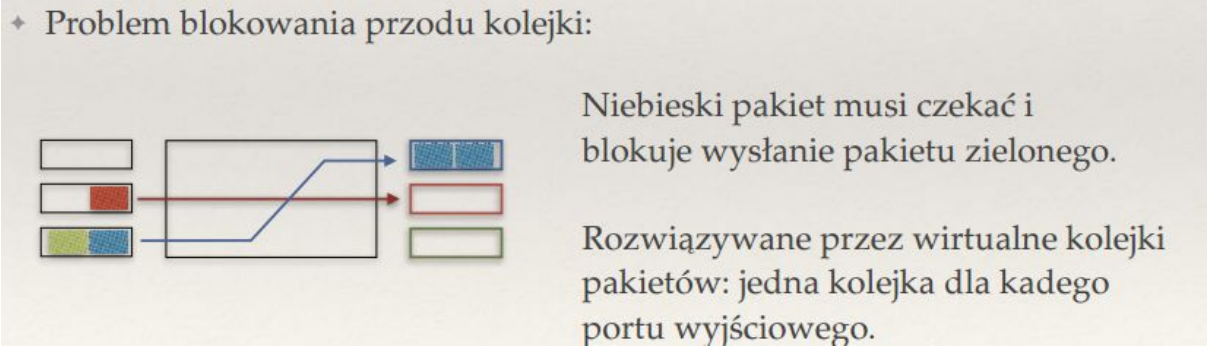
Gdzie w routerze stosuje się buforowanie? Po co?

Na wyjściu FIFO jest (było już wyżej).
Na wejściu jak przepustowość struktury przełączającej jest za mała, pakiety kierowane do zajętych portów są blokowane.

Po co w portach wyjściowych klasyfikuje się pakiety?

Ponieważ niektóre mogą mieć większy priorytet.

Co to jest blokowanie początku kolejki? Gdzie występuje? Jak się go rozwiązuje?



Rozwiń skrót LPM.

Longest Prefix Match.

Jakie znasz struktury danych implementujące LPM? Porównaj je.

	pamięć	lookup	insert	delete
List prefiksów	O(n)	O(n)	O(1)	O(n)
Tablice haszujące	O(n)	O(w) oczekiwany	O(1) oczekiwany	O(1) oczekiwany
Drzewa trie	O(n*w)	O(w)	O(w)	O(w)
Trie ze skrótami	O(n) ?	O(log w) ?	O(n) ?	O(n) ?

Lista prefiksów - Pamięć O(n), Lookup O(n), Insert O(1), Delete O (n).
Tablice haszujące - Pamięć O(n), Lookup O(w), Insert O(1), Delete O (1).
Drzewa Trie - Pamięć O(n*w), Lookup O(w), Insert O(w), Delete O (w).
Trie z dodatkowymi krawędziami skracającymi - Pamięć O(), Lookup O(log w), Insert O(n), Delete O (n).
Sprzętowe TCAM - odp niżej.

w - rozmiar adresu

Co to jest pamięć TCAM? Jak można ją zastosować do implementacji LPM?

Ternary content addressable memory - przechowuje pary (p,m), dla adresu w można równolegle znaleźć wszystkie pary takie że w&m = p &m (wszystkie pasujace prefiksy) a następnie wybrać najdłuzszy pasujący prefiks.

Na czym polega fragmentacja IP? Gdzie się ją stosuje i dlaczego? Gdzie łączy się fragmenty?

Jak pakiet jest większy niż MTU łącza wyjściowego to dzielimy go na fragmenty. Dzielenie odbywa się na dowolnym routerze na trasie po to, aby możliwe było przesłanie pakieciku. Fragmenty łączone są dopiero na komputerze docelowym.

Co to jest MTU? Na czym polega technika wykrywania wartości MTU dla ścieżki?

Max Transmission Unit - maksymalna wielkość pakietu która może przejść przez łącze. Wysyłamy pakiet z flagą DF (dont fragment) i jak ktoś nam odrzuci pakiet to przyśle info jakie ma MTU i my sobie wtedy dzielimy na mniejsze pakieciki (wykrywamy wartość MTU dla ścieżki).

Jak działa szeregowanie pakietów w buforze wyjściowym routera?

Szeregujemy pakiety na strumienie o różnych priorytetach. Wtedy wysyłamy najpierw te o najwyższym itd.
Możemy też szeregować cyklicznie i stosować round-robin.

Jakie są różnice w nagłówkach IPv4 i IPv6?

Nagłówki IPv6 są stałej długości. W IPv6 nie używamy fragmentacji. Nie mamy też sumy kontrolnej. Trzymamy za to dodatkowo etykietę strumienia tak by nie trzeba było patrzeć na porty. Jedna mają 32 bity, a drugie 128 bitów.

Zapisz adres IPv6 0321:0000:0000:0123:0000:0000:0000:0001 w najkrótszej możliwej postaci.

321:0:0:123::1 Jak niby z tego odzyskać oryginalny adres?

Co to jest tunelowanie 6in4?

Pakiety IPv6 przesyłane jako dane pakietów IPv4. Mamy broker tunelu, który usuwa nagłówek IPv4 i wtedy mamy same IPv6.

Na czym polega NAT i po co się go stosuje? Jakie są jego zalety i wady?

Network Address Translation to tłumaczenie adresu i portu z sieci lokalnej na adres i port routera widoczny z Internetu. Działa tak że dostajemy pakiet, którego adres i port to (A,P_a) a cel ma (C,P_c) to wybieramy port P_b, a adres źródłowy podmieniamy na (B,P_b), przypisanie jest przechowywane w tablicy NAT przez pewien czas.

+ rozwiązanie problemu braku adresów IP
+ można zmienić adresy IP wewnętrznej sieci bez informowania całego świata
+ można zmienić ISP bez zmiany adresów IP wewnątrz sieci
- nieosiągalność komputerów z Internetu (P2P)
- psucie modelu warstwowego (bo router modyfikuje treść pakietu)

Jaki stan musi przechowywać router z funkcją NAT?

Tablicę NAT przypisań (A,P_a,C,P_c) -> P_b.

Wykład 5: Niższe warstwy

Jakie są zadania warstwy łącza danych a jakie warstwy fizycznej?

Warstwa łącza danych zapewnia usługę wysyłania ramek (między dwoma połączonymi urządzeniami) oraz musi sobie radzić z błędami transmisji.
Warstwa fizyczna określa szczegóły przesyłania pojedynczych bitów.

Rozwiń pojęcia LAN i WAN.

Local Area Network - sieć lokalna (Ethernet, WLAN)
Wide Area Network - sieć rozległa (Frame Relay,PPP)

Czym różni się koncentrator od przełącznika sieciowego?

Przełącznik rozumie protokoły warstwy drugiej, uczy się które adresy MAC podłączone są do których portów.

Co to jest komunikacja pełnodupleksowa, półdupleksowa i simpleksowa?

To samo co wcześniej. Ale tutaj odnosi się do komunikacji a nie do rodzaju do kabla.

Jak działa algorytm rundowy i bezrundowy ALOHA?

Rundowy ALOHA - czas podzielony na rundy, jedna runda wystarcza do nadania jednej ramki, sukces to sytuacja w której tylko jeden komputer nadaje, jeżeli komputer nadaje to może ją wysłać z ppb p. Potrzeba tutaj globalnego zegara na rundki.

Bezrundowy Aloha działa jak wyżej tylko każdy ma własne rundy, zostaje wyeliminowana potrzeba globalnego zegara.

Jak działa algorytm odczekiwania wykładniczego?

Dopasowuj dynamicznie wartość p w sposób wykładniczy, czyli na początku p = 1, a za po każdej kolizji p = p / 2.

Wyjaśnij skróty CSMA/CD i CSMA/CA, opisz te algorytmy

Carrier Sense Multiple Access with Collision Detection

- m ← 1
- Poczekaj aż kanał będzie pusty i zacznij nadawać.
- Podczas nadawania, nasłuchuj. Jeśli usłyszysz kolizję:
    - skończ nadawać,
    - wylosuj k ze zbioru { 0, …, 2m - 1 } i odczekaj k rund,
    - m ← m + 1,
    - wróć do kroku 2.

Można stosować jedynie jeśli umiemy jednocześnie nadawać i odbierać tak żeby wiedzieć czy są kolizje.
Trzeba tylko dobrze dobrać długość rundy. Najlepiej ustawić R = czas wysyłania 64 bajtów.

Carrier Sense Multiple Access with Collision Avoidance
Taki sam jak ten poprzedni algorytm, tylko stosujemy potwierdzanie ramek. Ramki są zawsze nadawane do końca. Odczekujemy pewien czas, nawet jeśli kanał właśnie się zwolnił.

Opisz budowę ramki ethernetowej.

Ramka ethernetowa zawiera:

- adres docelowy MAC
- adres źródłowy MAC
- typ (0x0800 = IP)
- dane
- sumę kontrolną

Co to jest adres MAC?

MAC to 6 bajtowy unikatowy ciąg teorytycznie przypisany do karty sieciowej, w praktyce łatwo go zmienić. Pierwsze 3 bajty przyznaje IEEE producentowi kart sieciowych, 3 kolejne nadaje producent.

Do czego służy tryb nasłuchu (promiscuous mode)?

Przekazywania do systemu wszystkich widzialnych ramek.

Dlaczego w Ethernecie definiuje się minimalną długość ramki?

Aby łatwo odróżnić ramkę od śmieci oraz czas wysyłania trwało conajmniej 2*czas propagacji,

Jak dobierać długość rundy odczekiwania w protokokole CSMA/CD?

Czas wysyłania 64 bajtów (R>= 2* tau). Musimy umieć dowiedzieć się czy nam się udało wysłać czy nie.

Do czego służą protokoły ARP, RARP, DHCP i APIPA?

ARP = Address Resolution Protocol
Służy do dowiedzenia się “kto ma dany adres IP”. Jest zawarty w ramkach wysyła na adres rozgłoszeniowy. (FF:FF:FF:FF:FF:FF), pole type w takiej ramce to 0x0806.
Jeden komputer odpowiada.
Wszyscy słyszą odpowiedź i zapisują ją w lokalnej tablicy ARP na jakiś czas.
RARP = Reverse ARP
Służy do dowiadywania się kto ma dany adres MAC.
DHCP = Dynamic Host Configuration Protocol
Przydziela automatycznie adresy IP.

Czym różni się łączenie dwóch sieci za pomocą mostu od łączenia ich za pomocą routera?

Most to przełącznik z dwoma portami, który łączy 2 sieci. Łączenie za pomocą mostu jest szybsze, bo podmiane podlega jedynie nagłówki oraz suma kontrolna, ale most nie rozumie IP, więc nie dokona fragmentacji.

Jak warstwa łącza danych realizuje rozgłaszanie?

Każdy otrzymuje informacje jeśli nadana ona jest na adres rozgłoszeniowy MAC.

Na czym polega tryb uczenia się w przełączniku sieciowym?

Przełącznik uczy się które adresy MAC są podłączone do których portów.

Po co w przełączanym Ethernecie stosuje się algorytm drzewa spinającego?

Chcemy osiągnąć topologię bez cykli (a przy okazji mieć krótkie ścieżki) (STP)

Wyjaśnij zjawisko ukrytej stacji.

Ukryta stacja jest wtedy gdy dwa urządzenia są w zasięgu AP, a nie widzą siebie nawzajem, wtedy myślą że są same i mogą coś nadawać do AP.

Na czym polega rezerwowanie łącza za pomocą RTS i CTS?

Rozwiązuje to problem ukrytej stacji. RTS (Real Time Strategy/Request to Send) - urządzenie pytana o pozowolenie na nadawanie AP i wtedy ono mu odpowiada CTS (Clear to Send) - co oznacza że nie ma konkurentów do nadawania i może lecieć.

Jakie znasz problemy z warstwą fizyczną w sieciach przewodowych i bezprzewodowych?

- malejąca siła sygnału
- interferencja

Jakie znasz standardy szyfrowania w sieciach bezprzewodowych?

- WEP (Wired Equivalent Privacy)
- WPA (WIFI Protected Access)
- WPA2 = 802.11i

Wymień popularne standardy Ethernetu i sieci WLAN

Ethernet:

- Fast Ethernet
- Gigabit Ethernet

WLAN

- 802.11g
- 802.11n

Wykład 6: Transport (niezawodny transport)

Co może stać sie z przesyłanym ciągiem pakietów IP podczas zawodnego i niezawodnego transportu?

Podczas zawodnego pakiety mogą być: uszkodzone, zgubione, opóźnione, zamienione, zduplikowane.
Podczas niezawodnego pakiety mogą być dostarczone do odbiorcy

Co to jest kontrola przepływu?

Nadawca powinien dostosowywać prędkość transmisji do szybkości odbierania odbiorcy.

Czym różnią się protokoły UDP i TCP? Podaj zastosowania każdego z nich.

UDP to możliwie najprostszy protokół warstwy transportowej. Nie daje żadnych gwarancji, jedynie zasadę best effort. Wymagana jest kontrola przepływu = nadawca powinien dostosowywać prędkość transmisji do szybkości odbiorcy. Używane gdy przesyłane są małe ilości danych, lub wymagana jest szybka reakcja.

Co to jest segmentacja? Dlaczego segmenty mają ograniczoną wielkość?

Segmentacja to dzielenie bajtów na segmenty. Segmenty mają ograniczoną wielkość ze względu na MTU. Nie zwiększamy MTU bo byłaby wtedy większa szansa na zakłócenia, mogłyby wystąpić problemy podczas szeregowania(opóźnienia małych pakiecików), a przede wszystkim ze względu mniejsze opóźnienia przy dłuższych ścieżkach.

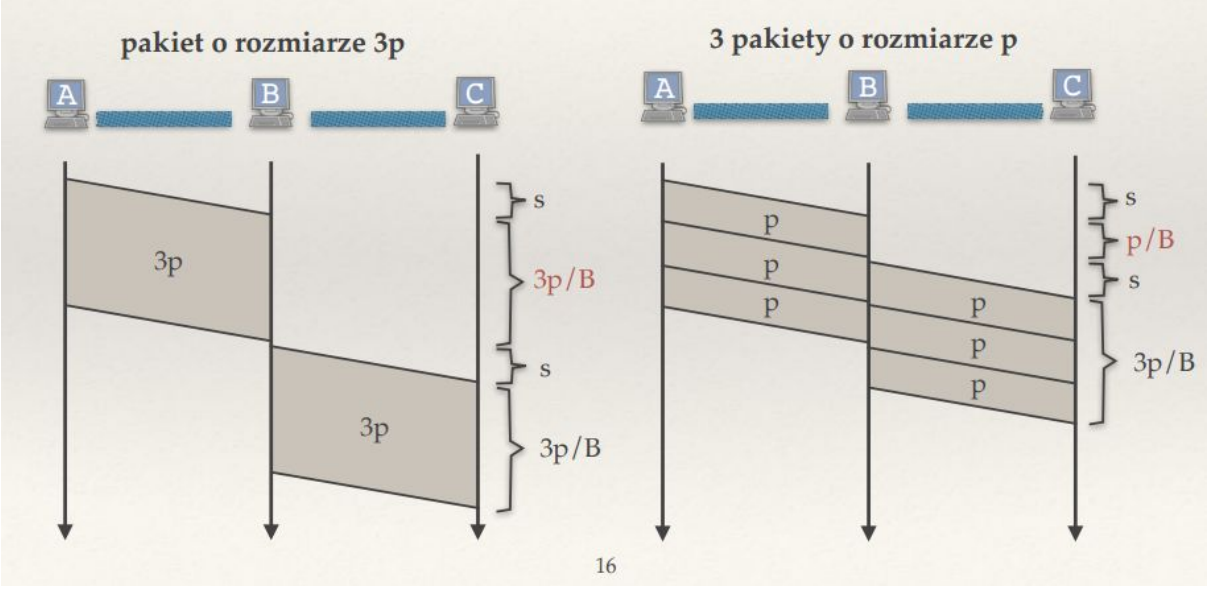
Jak nazywają się jednostki danych przesyłane w kolejnych warstwach?

warstwa transportowa - datagramy (gdy użytkownik sam dzieli na części np.UDP),segmenty (gdy warstwa dzieli np.TCP)
warstwa sieciowa - pakiety
warstwa łącza danych - ramki

Rozwiń i wytłumacz skrót MSS.

Maximum Segment Size = MTU - rozmiar nagłowka IP - rozmiar nagłówka TCP. Maksymkowa wielkość przesyłanego segmentu.

Jak małe pakiety zmniejszają opóźnienie przesyłania danych?



Wytłumacz znaczenie skrótów RTT i RTO. Na jakiej podstawie ustalana jest wartość RTO?

RTT - round trip time - było 2 * czas propagacji
RTO - retransmission timeout = 2*avg_RTT + 4*var_RTT - po jakim czasie nadać ponownie segment.

Jak protokoły niezawodnego transportu wykrywają duplikaty pakietów i potwierdzeń?

Pamiętają sobie co już miały.

Opisz algorytm Stop-and-Wait. Jakie są jego wady i zalety?

Wysyłamy segment czekamy na ACK i wysyłamy następny.

- \+ łatwe w implementacji
- \- dużo marnowanego czasu mało wysyłanych danych

Do czego służa numery sekwencyjne w niezawodnym protokole transportowym?

Do tego żebyśmy zczaili się czy coś już wysłaliśmy/dostaliśmy czy nie.

Opisz algorytm okna przesuwnego.

Wysyłamy segmenty z okna(SWS).(sender window size) Dostajemy na nie ACK. Jak przyjdzie ACK dla LAR+1 to przesuwamy okno w prawo, dość intuicyjna sprawa.

Jaki jest związek między rozmiarem okna a BDP (bandwidth-delay product)?

Chcielibyśmy nadawać co najmniej BDP danych, aby wykorzystac całe łącze.

Opisz i porównaj następujące mechanizmy potwierdzania: Go-Back-N, potwierdzanie selektywne, potwierdzanie skumulowane.

Go Back N - ACK wysyłamy tylko dla S <= P+1, gdzie P to ostatni potwierdzony pakiet, S segment.
Potwierdzanie Selektywne - mamy bufor odbiorcy (okno) dla S <= LFRcvd + RWS wysyłamy ACK. Dla okna = 1 jest to Go Back N. Wiemy tutaj dokładnie jakie pakiety do nas dotarły.
Potwierdzanie Skumulowane - Poza wysyłaniem ACK podobnie jak w Selektywnym. Po dostaniu S ACK wysyłamy dla segmentu po którym jest dziura. Można dzięki temu wnioskować jakie pakiety się zgubiły.

Dlaczego istotne jest potwierdzanie odbioru duplikatów segmentów?

Bo ACK mógł się zgubić.

Co to jest okno oferowane? Jak pomaga w kontroli przepływu?

Odbiorca mówi jak dużo segmentów może pomieścić. Wtedy nadawca może sobie adjustnąć prędkość wysyłania.

Jakie mechanizmy niezawodnego transportu i kontroli przepływu implementowane są w protokole TCP?

Używa okna przesuwanego z potwierdzaniem skumulowanym. Umie też oferować okno.Nag

Na czym polega opóźnione wysyłanie ACK w protokole TCP?

Jeśli czasami nie mamy danych do odesłania to opóźniamy wysyłanie ACK.

Na czym polega mechanizm Nagle'a? Kiedy nie należy go stosować?

Czekam z wysyłanie aż wszystkie poprzednie dane zostaną potwierdzone. (Jeśli aplikacja generuje dane mniejsze niż MSS)
Problem jest jak aplikacja jest interaktywna. Wtedy mogłaby się zaciąć.

Co oznaczają pola ,,numer sekwencyjny" i ,,numer potwierdzenia" w nagłówku TCP?

numer sekwencyjny (numer pierwszego bajtu w segmencie)
numer ostatniego potwierdzanego bajtu + 1

Czy warstwa transportowa implementowana jest na routerach? Dlaczego?

Raczej nie, bo zasada end-to-end i one mają tylko przekazywać pakiety dalej.

Sfomułuj słabą i silną zasadę end-to-end.

Silna - niezawodne przesyłanie danych musi być implementowane na urządzeniach końcowych a warstwy niższe nie powinny wgl się tym zajmować.
Słaba - niezawodne przesyłanie danych musi być implementowane na urządzeniach końcowych a warstwy niższe mogą w tym pomagać.

Wykład 7: Transport (protokół TCP)

Co to jest gniazdo?

Deskryptor pozwalający na komunikację sieciową. Z góry jest bardzo podobny do deskryptorów pliku.

Czym różni się gniazdo nasłuchujące od gniazda połączonego? Czy w protokole UDP mamy gniazda połączone?

W UDP nie ma gniazd połączonych. Gniazdo nassłuchujący są tylko tylko dla serwera i tylko do nawiązywania połączenia. Gniazdo połączone są dla serwera i klienta tworzone po połączeniu, do wymiany właściwych danych.

Co robią funkcję jądra bind(), listen(), accept(), connect()?

bind() - łączy gniazdo z portem
listen() - oznacza gniazdo jako nasłuchujące. Na takim gnieździe będzie można wykonać accept.
connect() - zwraca gniazdo połączone po stronie klienta
accept() - zwraca gniazdo połączone (po 3fazowej operacji nawiązania połączenia). Blokuje aż do połączenia z klientem

Czym różni się komunikacja bezpołączeniowa od połączeniowej?

Bezpołączeniowa - strony nie utrzymują stanu.
Połączeniowa - na początku strony wymieniają komunikaty nawiązujące połączenie dzięki czemu późniejsza komunikacja jest wygodniejsza, na koniec trzeba tu kończyć połączenie.

Czym różni się otwarcie bierne od otwarcia aktywnego? Czy serwer może wykonać otwarcie aktywne?

Otwarcie aktywna oznacza, że wywoływany jest connect, który blokuje się aż do uzyskania połączenia.
Otwarcie bierne oznacza, że wywoływany jest accept, który się blokuje aż ktoś się do niego nie połączy.
No chyba serwer to czeka aż ktoś do niego się połączy, ale według diagramu dalej chyba może wysłać SYN'a.

Do czego służą flagi SYN, ACK, FIN i RST stosowane w protokole TCP?

SYN oznacza chęć sparowania. (Synchronizuje kolejne numery sekwencyjne)
ACK oznacza potwierdzenie otrzymania pakietu. (Zawiera numer potwierdzenia)
FIN chęć zakończenia połączenia. (Zakończenie przekazu danych)
RST resetuje połączenie.

Opisz trójstopniowe nawiązywanie połączenia w TCP. Jakie informacje są przesyłane w trakcie takiego połączenia?

1) Klient wysyła SYN J
2) Server wysyła SYN K i Potw J+1
3) Klient wysyłą POtw K+1

Dlaczego przesyłanych bajtów nie numeruje się od zera?

Jakie segmenty są wymieniane podczas zamykania połączenia w protokole TCP?

1) Klient FIN M
2) Server Potw M+1
3) Server FIN N
4) Klient Potw N+1

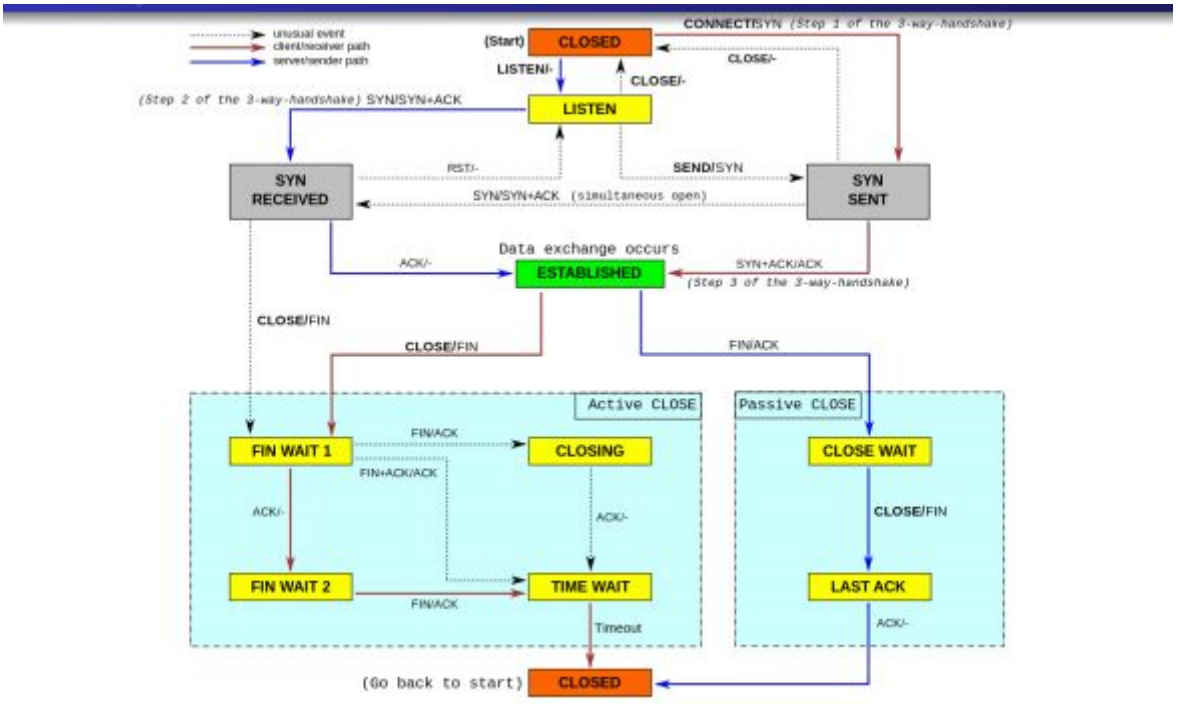
Co zwraca funkcja recv() wywołana na gnieździe w blokującym i nieblokującym trybie?

Jeśli w trybie blokującym to zawsze zwraca liczbę bajtów odebranych. W trybie nieblokującym zwraca -1 jeśli nie było co odebrać i odpowiednio ustawia errno. Jeśli udało się coś odebrać to zwraca liczbę odebranych bajtów.

Czy do stanu TIME_WAIT przechodzi strona, która wykonuje zamknięcie aktywne czy bierne? Po co wprowadzono taki stan?

Do stanu tego przechodzi strona wykonująca zamykanie aktywne bo nie wie czy druga strona dostała jej ACK. Utrzymuje się go 1-4 min (2*max czas życia segmentu) aby prawidłowo zakończyć połączenie TCP (jeśli ACK nie dotarło to druga strona wyśle znowu FIN które chcemy poprawnie obsłużyć), aby usunąć stare duplikaty segmentów z sieci.

Na podstawie diagramu stanów TCP opisz możliwe scenariusze nawiązywania i kończenia połączenia.



Wykład 8: Transport (kontrola przeciążenia)

Czym różni się kontrola przepływu od kontroli przeciążenia?

Kontrola przepływu - nie chcemy zalać odbiorcy pakietami
Kontrola przeciążenia - nie chcemy zalać sieci pakietami.

Co to jest przeciążenie?

Przypadek kiedy przepełnia się bufor na pakiety.

Na czym polega mechanizm opóźnionych potwierdzeń?

Chyba było wyżej.

Jaka jest zależność między rozmiarem okna nadawcy a prędkością transmisji?

Im większe ma okno tym więcej wysyła.

Czy nieskończone bufory rozwiązałyby problem przeciążenia?

Przeciążeń w rozumieniu pełnych kolejek by nie było, ale opóźnienia byłyby ogromne i krążyłyby duplikaty po sieci.

Jak zależy średni rozmiar kolejki od średniej prędkości nadchodzenia pakietów?

Pełne kolejki to większe opóźnienia.
Puste kolejki oznaczają że możemy nadawać szybciej.

Jakie są cele kontroli przeciążenia?

wysokie wykorzystanie łączy
sprawiedliwy podział
Rozproszony algorytm.
działa w rozproszonym środowisku i szybko reaguje na zmiany

Jak można definiować sprawiedliwy podział łącza? Co to jest max-min fairness?

Maxymek-minymek fairness - jeżeli nie można zwiększyć szybkości żadnego ze strumieni bez spowolnienia innego strumienia, który ma szybkość <= naszej szybkości.
Sprawiedliwy podział łącza to taki w którym każdy dostaje po równo (?)

Na jakiej podstawie zmienia się rozmiar okna przeciążenia?

Na podstawie oferowanego okna oraz congestion window obliczanego przez nadawcę.

Kiedy TCP wnioskuje, że pakiet zaginął?

Nie dostało ACK po RTO, albo otrzymaliśmy podwójne potwierdzenie porpzedniego segmentu. (ACK 1, ACK 2, ACK 3, ACK 3, ACK 3)

Opisz algorytm ustalania rozmiaru okna przeciążenia

Jeśli otrzymujemy ACK pakietu to zwiększamy cwnd o MSS * MSS / cwnd.
Jeśli pakiet zaginął (przekroczony timeout albo podwójne potwierdzenie) zmniejszamy cwnd dwukrotnie.

Rozwiń skrót AIMD. Czego dotyczy?

Additive Increase Multiplicative Decrease - służy obliczeniu przeciążenia okna (cwnd). To jest w sumie idea matematyczna, która pozwala zbiegać, ale ok.

W jaki sposób AIMD gwarantuje sprawiedliwy podział łącza?

Po pewnym czasie rozmiary okien zbiegają do R/n, gdzie R = BDP + rozmiar kolejki, n liczba urzadzeń.

Opisz fazy unikania przeciążenia i wolnego startu w TCP.

Unikanie przeciążenia:

- pakiet dostarczono - cwnd = cwnd + MSS*MSS/cwnd (w RTT zmiana cwnd od MSS)
- pakiet zgubiono - cwnd = cwnd/2

Wolny start:

- na początku cwnd = 1
- pakiet dostarczono - cwnd += MSS (co RTT zmiana cwnd = 2cwnd)
- do utraty pierwszego pakietu trwa

Ustawiamy sobie też jakiś threshold poniżej którego używamy wolnego startu. Jeśli cwnd > ssthresh i straciliśmy pakiet to koniec tej fazy.

Opisz mechanizm szybkiej retransmisji i szybkiego przywracania.

Szybka retransmisja to wysyłanie segmentu bez oczekiwania na timeout.
Szybkie przywracanie (pomijanie fazy wolnego startu) ustawiamy ssthresh = cwnd/2, a cwnd = ssthresh.

Na czym polega mechanizm RED?

Random Early Detection: router wyrzuca losowe pakiety (ppb wyrzucenia jako rosnąca funkcja średniej długości kolejki), dzięki temu mamy krótsze kolejki.

Opisz działanie mechanizmu ECN (explicit congestion notification).

ECN gdy następuje ppb przeciążenia to router ustawia bity ECN w nagłówku IP, wtedy odbiorca ustawia ECN w TCP ACK i nadawca reaguje na to jak na utratę pakietu.

Jaka jest relacja w AIMD między przepustowością a traconymi pakietami?

Dwie transmisje korzystającego z tego samego łącza o małej przepustowości: ich okna przeciążenia i frakcja traconych pakietów taka sama

Jakie modyfikacje wprowadza FastTCP do AIMD? Dlaczego?

Powyżej pewnej wartości cwnd zwiększamy szybciej i zmniejszamy wolniej.
Modyfikacje wprowadzamy, bo to nie możliwe, żeby tylko tracić jeden segmant na 2 * 10^10.

Wykład 9: Zastosowania (część 1)

Jaki jest cel systemu nazw DNS?

Zamiana nazwy symbolicznych na adresy IP i z powrotem

Do czego służy plik /etc/hosts?

Zapisane są w nim lokalne odwzorowania IP nazwa domeny

Rozwiń skrót TLD (kontekst: DNS), podaj parę przykładów.

Top Level Domains. Przykłady .uk .pl .com

Czym są strefy i delegacje DNS?

Strefy to najmniejsze jednostki administracyjne w DNS (takie gminiki hehhe). Delegacja DNS zachodzi wtedy jak dana strefa jest za ogólna aby resolvnąć adres ale zna zioma co jest bardziej szczegółowy i deleguje nas do niego.

Czym różni się rekurencyjne odpytywanie serwerów DNS od iteracyjnego?

Iteracyjne to takie ręczne po kolei od głównych serwerów pytamy o adres.
Rekurencyjnie to pytamy resolver DNS o addres a on sam w naszym imieniu dokonuje kolejnych zapytań.

Jak działa odwrotny DNS? Jaki typ rekordów i jaką domenę wykorzystuje?

Odwrotny DNS to zamiana IP na adres domeny. Wykorzystują typ rekordów PTR oraz sztuczną domenę in-addr.arp, której poddomenami są klasy lub adresy IP (np. strefa 33.22.11.in-addr.arpa ma info na temat sieci 11.22.33.0/24)

Jakie znasz typy rekordów DNS? Co to jest rekord CNAME?

Typy: A,AAA,NS,CNAME,MX. Rekord Cname(canonical name) nazwa to nazwa domeny, a wartość to główna nazwa domeny.

Po co są wpisy sklejające w opisie delegacji DNS?

Co robi funkcja getaddrinfo()

Wykonuje za nas zapytania dns.

Opisz budowę adresu URL. Opisz budowę adresu URL w przypadku schematu http.

URL (Uniform Resource Locator) składa się z 2 częśći oddzielonych dwukropkiem

- schemat
- część zależna od schematu.

W przypadku schematu http mamy po dwukropku // nazwa serwera to www, opcjonalnie można zrobić : port, / definiuje hierarchię.

W jakim celu serwer WWW ustawia typ MIME dla wysyłanej zawartości? Podaj kilka przykładów typów MIME.

Aby przeglądarka wiedziała jaką akcje podjąć (jaką wtyczkę odpalić) przykłady: text/html, text/xml, application/pdf, application/octet-stream,image/jpeg

Wymień parę możliwych odpowiedzi HTTP wraz z ich znaczeniem.

200 OK - sukces
404 NOT FOUND
403 Forbidden
500 Internal Server Error

Po co w nagłówku żądania HTTP/1.1 podaje się pole Host?

Żeby było wiadomo z kim się łączy.

Do czego służą pola Accept, Accept-Language, User-Agent, Server, Content-Length, Content-Type w nagłówku HTTP?

Accept: lista akceptowanych typów MIME
Accept-Language: Jakie języki znamy
User-Agent: Identyfikuje przeglądarke
Server: Identyfikuje serwer i użyte w nim oprogramowanie
Content-Length: Długość danych
Content-Type: Format danych

Jak wygląda warunkowe zapytanie GET protokołu HTTP?

No może mięc na przykład If-Modified-Since.

Jakie znasz kody odpowiedzi protokołu HTTP?

- 1xx: informacyjne
- 2xx: sukces (200 = OK)
- 3xx: przekierowania
- 4xx: błąd po stronie klienta (błędne żądanie, brak autoryzacji,
- zabroniony dostęp, 404 = Not Found)

- 5xx: błąd po stronie serwera (500 = Internal Server Error)

Na czym polegają połączenia trwałe w HTTP/1.1? Do czego służy opcja Connection: close w nagłówku HTTP?

Na tym że połączenie nie zostaje zamykane po obsłużeniu jedenego requesta. Opcja ta służy aby zamknąć połączenie (domyślnie jest otwarte).

Do czego służą arkusze stylów CSS?

Do modelowania wyglądu strony HTML.

Wymień parę możliwości uzyskiwania dynamicznych stron WWW.

Po stronie klienta:
- Javascript

Po stronie serwera:
- CGI
- PHP
- JSP

Co to jest CGI?

Common GateWay Interface - standard umożliwiający wykonanie dowolnego zewnętrznego programu

Po co stosuje się metodę POST?

Można dzięki temu przekazać także treść żądania. W ten sposób można także wysyłać pliki do serwera.

Co to jest technologia REST?

REST (Representational State Transfer) - filozofia tworzenia usług sieciowych wykorzystujących metody protokołu HTTP.

Jaka jest rola trackera w sieci Bittorrent?

Niżej powinno być.
Łączymy się z nim na początku zna on adresy członków sieci i udostępnia je nam.

Po co w plikach .torrent stosuje się funkcje skrótu?

Niżej powinno być
Aby sprawdzić czy pobraliśmy dobry kawałek pliku

Jakie są różnice w postępowaniu seedera i leechera w sieci BitTorrent?

Niżej powinno być
Seeder to ziomek co ma juz cały pliczek i wybiera sobie Q chętnych od tych co chcą od niego pobierać.
Leecher to ziomek co jeszcze pobiera i ma zasady ulicy: Jak Ty mi coś dałeś to ja też Ci coś mogę dać, najlepiej to dawać tym co najszybciej mi wysyłają, czasem jednak lubię zagrać losem i wysłać coś losowemu ziomowi a nóż będzie moim friendem. Jak jesteś nowy na ulicy to dam Ci szansę w postaci fragmetnu pliczku lepiej się spłać kurwiu.

Wykład 10: Zastosowania (część 2)

Na czym polegają połączenia odwrócone? Jak stosuje się je w protokole FTP?

No bo NAT blokuje nam życie. Chcemy jakoś się przez niego przebić żeby on mógł się z nami połączyć i nam wysyać dane.

Opisz podobieństwa i różnice asymetrycznych (cone) NAT (pełnego, ograniczonego i ograniczonego portowo) i symetrycznych NAT.

NAT symetryczny wybiera port P_b na podstawie adresu i portu zarówno nadawcy jak i obiorcy.
NAT asymetryczny wybiera port P-b na podstawie tylko adresu i portu nadawcy.
Pełny asymetryczny NAT jest wtedy kiedy przekazujemy wszystkie pakiety dalej
Ograniczony asymetrycznie NAT jest wtedy gdy przekazujemy tylko pakiety od adresów IP z listy odbiorców
Ograniczony portowo asymetryczny NAT jest wtedy gdy przekazuje tylko pakiety od par (adres,port) z listy odbiorców.

Opisz technikę wybijania dziur (hole punching) w NAT. Po co konieczny jest serwer pośredniczący?

Serwer pośredniczący jest potrzebny żeby powiedział kolesiom do kogo chcą się dobić.
Działa to tak że próbują komunikować się ze sobą ale nie są na liście odbiorców swojej, więc wysyłają sobie komunikaty i już są. Działo to niestety tylko w przypadku NAT asymetrycznego.

Do czego służą serwery proxy?

Mogą cachować zapytanka HTTP. Proxy tylko w razie potrzeby się połączy z serwerem HTTP. Optymalizują ilość przesyłanych danych.
Zazwyczaj proxy dodaje do żądania HTTP dodatkowe pola.

X-Forwarded-For: adres IP
Via: adres IP proxy
Anonimowe serwery proxy tego nie dodają i są zwykle płatne.

Co to jest odwrotne proxy? Co to jest CDN?

To takie proxy, ale bliżej serwera WWW. Zmniejszają obciążenie serwera. Zazwyczaj korzystają z DNS żeby balansować obiciążeniem. CDN - Content Distribution Networks to serwery proxy osobnych organizacji, które zazwyczaj obsługują wiele serwerów WWW i są ładnie rozłożone po świecie.

Jak skłonić klienta, żeby łączył się z serwerem proxy a nie bezpośrednio ze stroną WWW?

Wbić mu na dns.

Jakie informacje dołączane są przez serwer proxy do zapytania?

X-Forward-For : adres IP
via : adres IP proxy

Co to są anonimowe serwery proxy?

To takie co nie dodają dodatkowych info w nagłówkach. Zwykle płatne.

Do czego służy protokół SMTP a do czego POP3?

SMTP - przekazywanie poczty, protokół tekstowy nasłuchuje na 25.
POP3 - dostarczanie poczty.

Co to jest przekazywanie poczty (relaying)? Co to jest smarthost?

No mamy jakiś pośredników którym wysyłamy pocztę i oni za nas przekazują ją dalej czy coś.

Jaki rekord DNS jest sprawdzany przed wysłaniem poczty do danej domeny?

MX

Wymień parę popularnych pól w nagłówku maila. Do czego służą pola Received i Bcc?

From To Subject CC Bcc (ślepa kopia, tajniacka kopia ktorej nie widzi odbiorca glowny)
Received (by/from what)

Jakie pola w nagłówku są używane do tworzenia wątków z wiadomościami?

Co umożliwia standard MIME?

Jakie dane przesyłamy.

Co to jest spam? Jakie znasz metody walki ze spamem?

Spam to niechciana wiadomość pocztowa. Walczymy :

- reczne blokowanie
- metody statystyyczne, uczenie massznowe
- graylisting
- SPF

Na czym polega greylisting?

Koncepcja jest taka że nie opyla się wolno spamu wysyłać, więc mówimy kolesiowi sry nie można wysłać wyślij za ileś tam czasu i jak wyśle to wtedy dopiero przerzucamy dod nas.

Na czym polega mechanizm SPF?

Sender Policy Framewrok definiuje jakie komputery są uprawnione do wysyłania poczty z polem From równym coś tam. Rekordy SPF są sprawdzane przez odbiorcę.

Wykład 11: Kodowanie i szyfrowanie + notatki

Jakie znasz typy kodów detekcyjnych? Do czego służą i jakie są między nimi różnice?

sumy kontrolne - jakaś sumka
kody CRC - wielomianki
kody MAC - kody uwerzytelniające (trudno jest uzyskac po zmianie ten sam kod MAC)

Jakie rodzaje błędów mają wykrywać kody detekcyjne? Z czego biorą się błędy przy przesyłaniu danych?

Przekłamania parzystości bitów, przekłamania na kolejnych k bitach,błędy oddalone o ileś tam. Zazwyczaj z zakłóceń w warstwie fizycznej.

Jak działa algorytm obliczania sum kontrolnych CRC?

Bierzemy sobie wielomian jakiego używamy mnożymy wiadomość przez jego stopień następnie otrzymaną liczbę dzielimy przez nasz wielomian i dodajemy na koniec wiadomości.(suma kontrolna ma tyle bitow jaki stopien mial wileomian kontrolny)

Do czego służą kody MAC? Co to jest HMAC?

MessageAuthenticationCode - kody uwierzytelniające służące do zapenienia że wiadomość nie uległa przekłamaniu podczas procesu dostarczania do odbiorcy(uwierzytelnianie nadawcy). HMAC to standard wysyłania wysyłamy parę m,h(s||h(s||m))).

Jakie własności powinna mieć kryptograficzna funkcja skrótu?

normalnie szybko obliczalna, odwrotnośc wolno obliczalna, znalezienie takiego x != y ze h(x) = h(y) niemal impossible,

Jakie znasz metody korygowania błędów w transmisji?

Hamiing 7,4, arq, kody korekcyjne

Co to jest (a,b)-kod? Podaj przykład.

(α, β)-kod: zamienia wiadomość długości β na kod o długości α ≥ β. Przykładowo: bit parzystosci dla ciagów 7-bitowych to (8, 7)-kod.

Co to jest odległość Hamminga? Jak wpływa na możliwość detekcji i korekcji błędów?

Odległość Hamminga to liczba różnych bitów w 2 liczbach bitowych. Hamming (7,4)

Czym różni się poufność od integralności?

Poufność to że tylko Alicja i Bob wiedzą o czym piszą,a integralność to wykrywanie złośliwych zmiana w wiadomościach.

Co to są szyfry monoalfabetyczne? Dlaczego łatwo je złamać?

Szyfry monoalfabetyczne (podstawieniowe) zamieniaja pewne literki na jakieś inne. Łatwo jest łamać bo wystaczy podsłuchiwać albo zmusić do wysłania pewnej wiadomości aby ogarnąć o co chodzi.

Na czym polegają ataki z wybranym tekstem jawnym, znanym tekstem jawnym i znanym szyfrogramem?

Z wybranym tesktem jawnym zmuszenie wysłania wiadomości co ma wszystkie literki
Znanym szyfrogramem podglądanie par (test jawny, szyfrogram)
znanym tekstem jawnym intruz widzi szyfrogramy może je poddać analizie statystycznej.

Czym szyfrowanie symetryczne różni się od asymetrycznego?

W symetrycznym szyfruje i deszyfruje się tym samym kluczem.
W asymetrycznym ma się klucz pulbiczny i prywatny.

Co to jest szyfrowanie one-time pad?

Szyfrowanie symetryczne polegające na xorze wiadomości z kluczem. Zazwyczaj strony mają taką samą książeczkę z kluczami i stosują po jednym a później wyrzucają zużyte klucze.

Na czym polega szyfrowanie blokowe? Czym różni się tryb ECB od CBC?

Szyfrowanie blokowe to podział tekstu na bloki odpowiedniej wielkości i szyfrowanie po bloczku potem. ECB losuje tylko r_i ile jest bloczkow i robi E_k(m_i xor r_i)
CBC losuej tylko r_1 robi c_1 = E_k(m_1 xor r1) a potem c_i = E_k(m_i xor c_(i-1))

Wykład 12: Podstawy kryptografii + notatki

Czym szyfrowanie symetryczne różni się od asymetrycznego?

Było.

Na czym polega bezpieczeństwo przy szyfrowaniu asymetrycznym?

Mamy klucz prywatny który znamy tylko my i klucz publiczny znany całemu światu. Wiadomości szyfrują do nas kluczem publicznym a odszyfrować je możemy tlyko przy użyciu klucza prywantego.

Opisz algorytm RSA.

12.1 Algorytm szyfrowania RSA

Na początku generujemy dla siebię kluczy (publiczny i prywatny) w następujący sposób.

1. Wybieramy $p \neq q$: duże liczby pierwsze.
2. Obliczamy $n = p \cdot q$.
3. Znajdujemy dużą liczbę d względnie pierwszą z $(p-1)\cdot(q-1)$.
4. Znajdujemy takie e, że $d \cdot e \mod (p-1)\cdot(q-1) = 1$ (za pomocą rozszerzonego algorytmu Euklidesa).
5. Para (e, n) to nasz klucz publiczny, a (d, n) to nasz klucz prywatny.

Jak teraz szyfrujemy daną wiadomość? Zapisujemy ją bitowo i dzielimy na kawałki, których długość jest nie większa od $\log n$. Dzięki temu, każdy z kawałków jest liczbą z zakresu $[0, n)$. Każdą z liczb będziemy szyfrować osobno.[1]

Załóżmy zatem, że chcemy zaszyfrować liczbę $m \in [0, n)$. Obliczamy liczbę

$$E(m) = m^e \mod n \ ,$$

i wysyłamy ją jako szyfrogram s odbiorcy. Odbiorca otrzymuje szyfrogram s i odszyfrowuje go obliczając

$$D(s) = s^d \mod n \ .$$

Czy różni się szyfrowanie od uwierzytelniania?

Szyfrowanie to utajnianie wiadomości. Uwierzytelnianie to potwierdzenie kto co wysyła.

Co to jest atak powtórzeniowy?

Można nagrać transmisje i ją powtórzyć

Czy w szyfrowaniu asymetrycznym szyfrujemy kluczem publicznym czy prywatnym?

publicznym wiadomości, podpisy prywatnym

Na czym polega podpisywanie wiadomości? Jakim kluczem to robimy?

Prywatnym.

Jak można wykorzystać podpisy cyfrowe do uwierzytelniania?

Czy HMAC można wykorzystać do uwierzytelniania? Czy HMAC jest podpisem cyfrowym?

Można, nie jest.

Dlaczego lepiej podpisywać funkcję skrótu wiadomości niż samą wiadomość? Z jakim ryzykiem się to wiąże?

Bo jest krócej.
Że ktoś nas oszuka.

Co to są certyfikaty? Co to jest ścieżka certyfikacji?

Dostajemy od kogoś kogo ufamy wiadomość: klucz publiczny zioma to x podpisaną jego kluczem. Taka wiadomość to certyfikat, bo skoro wierzymy temu człowiekowi to uwierzymy też ziomowi.
Scieżki to podpisy kolejnych osób, które się nazwajem potwierdzały.

Co to jest urząd certyfikacji (CA)?

Urząd wydający certyfikaty (podpisujący klucze publiczne)

Jak SSL/TLS zapewnia bezpieczeństwo połączenia?

Dodatkowa warstwa między warstwą transportową i warstwą aplikacji odpowiadająca za szyfrowania. Większość popularnych usług ma swoje warianty wykorzystująca SSL np. HTTPS = HTTP over SSL

W jaki sposób w SSL następuje uwierzytelnienie serwera, z którym się łączymy?

Serwer WWW wysyła certyfikat podpisany przez pewne CA
Przeglądarka sprawdza czy posiada klucz publiczny tego CA i sprawdza prawdziwość podpisu CA oraz czy dane o stronie opisują tę stronę, z którą zamierzamy się łączyć
Mamy uwierzytelniony serwer i możemy sobie szyfrować jego kluczem publicznym

Czym różnią się certyfikaty zwykłe od rozszerzonych?

Zwykłe: zaświadczenie, że łączymy się z konkretną stroną
Rozszerzone: zaświadczenie, że łączymy się ze stroną danej instytucji

Co to są klucze sesji? Po co się je stosuje?

Klucze sesji stosuje się gdy chcemy szyfrować wymianę informacji zarówno między nami a serwerem, a serwerem do nas. Ustala go przeglądarka na początku kontaktu w sposób asymetryczny.

Co to są kolizje kryptograficznej funkcji skrótu?

Jeśli znajdujemy takie x i y, że x != y oraz h(x) = h(y)

Na czym polega atak urodzinowy?

Próbujemy aż do skutku. Żeby znaleźć dwie osoby, które mają urodziny tego samego dnia wystarczy spytać około 23 osób (wtedy ppb > 1/2)

Na jaki atak narażone jest podejście, w którym wiadomość najpierw szyfrujemy a potem podpisujemy?

Atak powtórzeniowy.

Na jaki atak narażone jest podejście, w którym wiadomość najpierw podpisujemy a potem szyfrujemy?

Bo osoba do której wysyłamy może przesłać go dalej i podpisać swoim podpisem.

Wykład 13: Bezpieczeństwo sieci

Co to jest pamięć CAM i jak stosuje się ją w przełącznikach? Jak można ją przepełnić?

content addressable memory - zawiera wpisy adres MAC - port.
Można go przepełnić zmieniając często adres Mac.

Opisz atak typu ARP spoofing; jak można go wykorzystać do podsłuchiwania komunikacji między dwoma komputerami podłączonymi do przełącznika sieciowego?

Rozgłaszamy nasz MAC jako bramę domyślną i hulamy.

Co oznacza termin IP spoofing? Na czym polega metoda weryfikacji tak zmodyfikowanych pakietów (ingress filtering)?

Można zrobić swoje dhcp i rozgłaszać swoje ip jako bramę domyślną. Fałszować własne IP.
ingress filtering to przepuszczanie tylko jeśli adresy się zgadzają

Na czym polega atak RIP spoofing?

Rozgłaszamy trasę do różnych sieci o małym koszcie i nagle nam wszystkie wysyłają.

Opisz, jak wygląda uwierzytelnianie serwera SSH.

On podaje jakiś fingerprint i trzeba zadzwonić. Zapisuje sobie też znane serwery.

Na czym polega uwierzytelnianie użytkownika przez SSH z wykorzystaniem kluczy RSA?

Można zapisać swój klucz publiczny na serwerze.

Przedstaw przykładowe ataki wykorzystujące brak sprawdzania poprawności wprowadzanych danych.

buffer overflow
sql injection

Wyjaśnij pojęcia: robak internetowy, exploit, botnet

robak to zły program
exploit to luki dobra do wykorzystania
botnet to zbiór komputerów zombie

Na czym polega phishing?

Podajemy się za kogoś innego

Co to jest skanowanie portów? Po co się je wykonuje?

Można szukać otwartych portów

Co to są ataki DoS i DDoS?

Zalewamy kanały. Wysyłamy szybciej niż są w stanie odebrać.

Na czym polega atak typu odbity (reflected) DoS?

wysyłamy do pośrednika

Jak działa i do czego jest wykorzystywany ICMP Traceback?

Czasami wysyłamy do obiorcy komunikat ICMP, który daje informacje o routerze.

Podaj przykłady tunelowania.

IPv6 w IPv4

Rozwiń skrót VPN. Do czego służy?

Wirtualna prywatna sieć. Bierzemy dwie sieci i łączymy je wirtualnie przez internet. Jak się pracuje z domu to się przydaje.

Porównaj wady i zalety filtrów pakietów: prostych, stanowych i działających w warstwie aplikacji.

proste

- analizują nagłówki ip
- szybkie

stanowe

- analizują ip i tcp
- śledzą nawiązywanie połaczenia

działające w warstwie aplikacji

- analizują segmenty i datagramy

Do czego służą moduły (chains) INPUT OUTPUT i FORWARD w zaporze Linuksa?

INPUT przy wejściu pakietu możemy coś z nim zrobić
OUTPUT możemy przy wyjściu coś zrobić
FORWARD przy przekazywaniu można coś zrobić

W jakich łańcuchach zapory Linuksa wykonywany jest źródłowy a w jakich docelowy NAT?

źródłowy w POSTROUTING
docelowy w PREROUTING

Komendy

ip link

Wypisuje dostępne interfejsy. Aktywne interfejsy oznaczone są napisem Up, nieaktywne - DOWN.

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: wlp3s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DORMANT group default qlen 1000
    link/ether c4:85:08:83:73:a9 brd ff:ff:ff:ff:ff:ff
```

ip addr

Wyświetla podobną informację co ip link, lecz wyświetla dodatkowo przypisane do interfejsów adresy IP.

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: wlp3s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether c4:85:08:83:73:a9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.16/24 brd 192.168.1.255 scope global dynamic wlp3s0
       valid_lft 85044sec preferred_lft 85044sec
    inet6 fe80::1838:9fd7:d3bc:bffa/64 scope link
       valid_lft forever preferred_lft forever
```

ifconfig -a

Podobne informacje do tych zwracanych przez ip addr.

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:2736 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2736 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:246507 (246.5 KB)  TX bytes:246507 (246.5 KB)

wlp3s0    Link encap:Ethernet  HWaddr c4:85:08:83:73:a9
          inet addr:192.168.1.16  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::1838:9fd7:d3bc:bffa/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:700974 errors:0 dropped:0 overruns:0 frame:0
          TX packets:369205 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:984634408 (984.6 MB)  TX bytes:45642122 (45.6 MB)
```

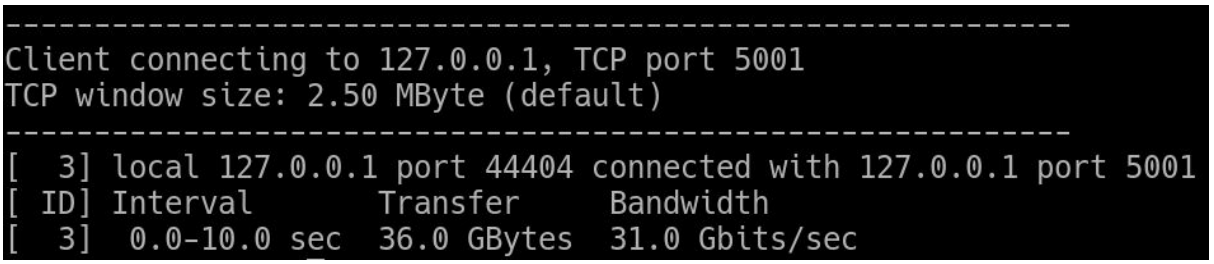
ethtool *nazwa_interfejsu*

Sprawdza status warstwy fizycznej poszczególnej karty. Pole **Link detected** określa czy danym łączem można przesyłać dane (w szczególności, czy z drugiej strony kabla jest

aktywna karta sieciowa). Dodatkowo mogą się tu znaleźć pola **Speed** oraz **Duplex** oznaczające przepustowość łącza jak i jego typ.

iperf

Służy do mierzenia wydajności połączenia. Z jednej strony na komputerze należy wydać polecenie: iperf -s, zaś na drugim iperf -c *adres_ip.*



ip link set up dev *nazwa_interfejsu*

Uaktywnia interfejs.

ip addr add *adres_ip*/*maska* dev *nazwa_interfejsu*

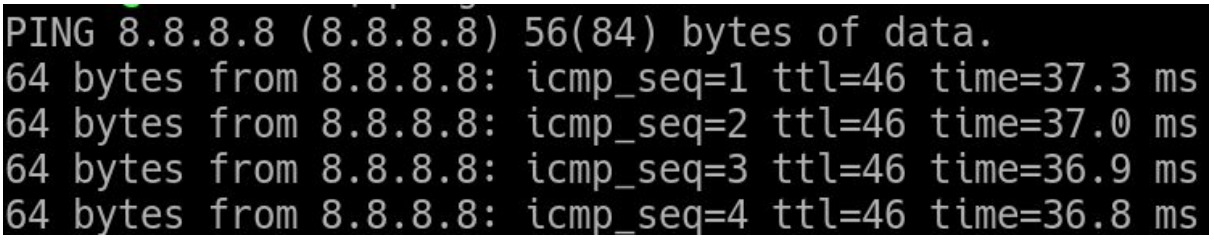
Nadaje interfejsowi adres IP.

ethtool -s *nazwa_interfejsu* speed *prędkość* duplex *rodzaj_duplexu*

Pozwala zmieniać niektóre ustawienia interfejsu. Forma powyżej pozwala zmieniać prędkość łącza jak i rodzaj duplexu.

ping *adres_ip*

Służy do testowania warstwy sieciowej poprzez wysyłanie specjalnych komunikatów protokołu ICMP.



plik hosts w /etc/hosts

Pozwala nadać nazwy znanym adresom IP.

```
127.0.1.1   boletus

192.168.2.1 moj_sasiad_kradnacy_mi_internet
8.8.8.8 serwer_dns_google


# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

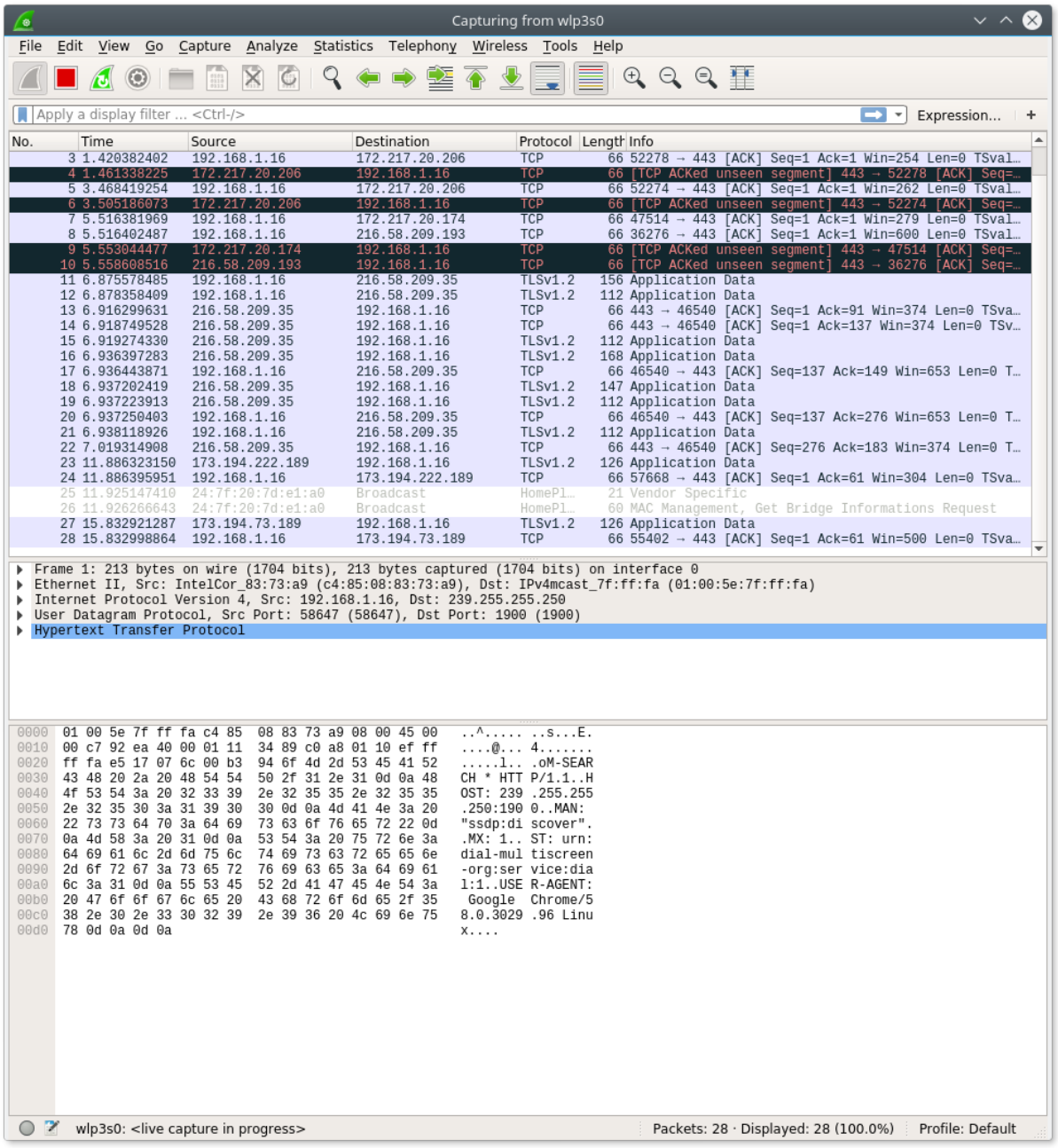
host -t a *adres_internetowy*

Sprawdza jaki jest adres IP związany z podanym adresem.

```
www.google.com has address 172.217.20.196
```

wireshark

Pozwala podglądać wysyłane oraz odbierane pakiety.



nc

Służy do zabawy z pakietami TCP oraz UDP.

telnet *adres_internetowy port*

Otwiera strumień danych do serwera WWW na komputerze pod podanym adresem.

```
Trying 156.17.4.11...
Connected to www.ii.uni.wroc.pl.
Escape character is '^]'.
GET / mbi/dyd/sieci_17s/ HTTP1.1
```

netstat -4tlp

Wyświetla uruchomione na Twoim komputerze usługi “przypięte” do konkretnych portów warstwy transportowej.

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address
  State       PID/Program name
tcp        0      0 boletus:domain          *:*
  LISTEN      1603/dnsmasq
```

ip route

Wyświetla tablice routingu.

```
default via 192.168.200.254 dev wlp3s0  proto static  metric 600
169.254.0.0/16 dev wlp3s0  scope link  metric 1000
192.168.200.0/24 dev wlp3s0  proto kernel  scope link  src 192.168.200.172  metric 600
```

Pytania z poprzednich egzaminów

Wykorzystujące adresy IP sieci S1 i S2 są połączone za pomocą routera. Komputer w sieci S1 wysyła pakiet IP do komputera w sieci S2, wkładając go uprzednio w ramkę. Co zrobi router? Zaznacz prawdziwe zdania.

- ❏ Zmodyfikuje adres docelowy ramki T
- ❏ Zmodyfikuje adres docelowy pakietu IP N
- ❏ Podzieli pakiet na fragmenty, jeśli MTU sieci S2 jest mniejsze niż rozmiar pakietu T
- ❏ Przekaże otrzymaną ramkę bez zmian do sieci S2 N

Protokół SSH:

- ❏ umożliwia pracę zdalną T
- ❏ wykorzystuje uwierzytelnianie za pomocą kryptografii asymetrycznej T
- ❏ wykorzystuje szyfrowanie za pomocą kryptografii asymetrycznej T
- ❏ wykorzystuje szyfrowanie za pomocą kryptografii symetrycznej T

Zaznacz prawdziwe zdania o routingu hierarchicznym

- ❏ Stosowany jest wyłącznie wewnątrz systemów autonomicznych N

- ❏ Stosowany jest w Internecie T
- ❏ Pozwala zredukować rozmiar tablicy routingu T
- ❏ Jego istotą jest przesyłanie segmentów TCP w pakietach IP N

Tylko jedna poprawna odpowiedź. Przy zastosowaniu sumy kontrolnej CRC opartej o wielomian x^2 + 1 do wiadomości 100001 (jedynka, cztery zera, jedynka) zostanie dołączona suma kontrolna:

- ❏ 11 T
- ❏ 01 N
- ❏ 10 N
- ❏ 1 N

Zakres adresów 123.0.0.0/18 ma zostać podzielony na 6 rozłącznych sieci, tak żeby każdy adres był w dokładnie jednej z nich. Co można powiedzieć o wielkości tych podsieci?

- ❏ Możliwe jest stworzenie podsieci o masce /22 T
- ❏ Możliwe jest stworzenie podsieci o masce /24 N
- ❏ Możliwe jest stworzenie podsieci o masce /19 T
- ❏ Możliwe jest stworzenie podsieci o masce /23 T

W jakich warstwach używane są poniższe mechanizmy?

- ❏ Nawiązywanie połączenia stosowane jest w warstwie transportowej T
- ❏ Typ MIME stosowany jest w warstwie transportowej N
- ❏ Routing stosowany jest w warstwie aplikacji N
- ❏ Sumy CRC wykorzystywana jest w warstwie łącza danych T

Protokół ICMP

- ❏ Umożliwia działanie programowi ping T
- ❏ Umożliwia kontrolę przeciążeń N
- ❏ Wykorzystuje port 23 do komunikacji N
- ❏ Wykorzystuje port 63 do komunikacji N

Tylko jedna poprawna odpowiedź. Klient DNS pyta serwer DNS o nazwę domeny skojarzoną z adresem 10.20.30.40

- ❏ Klient wyśle zapytanie o rekord A związany z domeną 10.20.30.40.ip.addr.arpa N
- ❏ Klient wyśle zapytanie o rekord A związany z domeną 40.30.20.10.ip.addr.arpa N
- ❏ Klient wyśle zapytanie o rekord PTR związany z domeną 40.30.20.10.tld N
- ❏ Klient wyśle zapytanie o rekord PTR związany z domeną 40.30.20.10.ip.addr.arpa T

Które z poniższych zdań są prawdziwe w przypadku protokołu TCP?

- ❏ Otrzymuje strumień danych z warstwy sieciowej i dzieli go na segmenty N
- ❏ Wszystkie gniazda są gniazdami nasłuchującymi N
- ❏ Potrafi dokonywać konwersji pomiędzy różnymi formatami plików N
- ❏ Wysyłane dane są potwierdzane T

Które z poniższych informacji opisują gniazdo połączone

- ❏ Zdalny port T

- ❏ MTU N
- ❏ Lokalny port T
- ❏ Zdalny adres IP T

Które z poniższych zdań są prawdziwe w przypadku Ethernetu?

- ❏ Podczas transmisji mogą występować kolizje T
- ❏ Dostęp do kanału jest deterministyczny N
- ❏ Komputery przekazują sobie token, by uzyskać dostęp do kanału T
- ❏ Wykorzystuje protokół CSMA/CA (CA = collision avoidance, unikanie kolizji) N

Komputer z prywatnym adresem IP 192.168.0.10 wysłał segment TCP do serwera DNS pod adres 22.22.22.22 i segment TCP do serwera WWW pod adres 33.33.33.33. W obu przypadkach źródłowy numer portu był równy 12345. Pośredniczący router z funkcją NAT zamienił w obu przypadkach adres źródłowy na 11.11.11.11:34567.

- ❏ Router może być symetrycznym NAT. N
- ❏ Router może być ograniczonym asymetrycznym (restricted cone) NAT. T
- ❏ Router może być asymetrycznym ograniczonym portowo (port restricted cone) NAT. T
- ❏ Router może być pełnym asymetrycznym (full cone) NAT. T

Zaznacz prawdziwe zdania:

- ❏ Kanał simpleksowy umożliwia transmisję danych w obu kierunkach, ale tylko w jednym kierunku naraz. N
- ❏ Ethernet oparty na koncentratorach umożliwia uzyskanie pełnego dupleksu. T
- ❏ Kanał półdupleksowy umożliwia transmisję danych tylko w jednym kierunku. N
- ❏ Kanał pełnodupleksowy umożliwia transmisję danych w obu kierunkach naraz. T

Zaznacz prawdziwe zdania.

- ❏ Protokół FTP służy do przesyłania poczty elektronicznej. N
- ❏ Protokół DNS służy do przesyłania plików. N
- ❏ Protokół SMTP służy do pobierania poczty elektronicznej z serwera. N
- ❏ Protokół POP3 służy do wysyłania poczty elektronicznej do serwera.N

Jakie informacje są zawarte w nagłówku UDP?

- ❏ suma kontrolna T
- ❏ numer sekwencyjny N
- ❏ rozmiar okna N
- ❏ długość T

Jeśli maską podsieci jest /28, to następujący adres można przypisać komputerowi

- ❏ 172.13.160.1 T
- ❏ 10.3.1.160 N
- ❏ 10.23.1.250 T
- ❏ 192.23.1.191 N

Podczas modelowego kończenia połączenia w protokole TCP:

- ❏ Przesyłane są dwa segmenty FIN T
- ❏ Strona wykonująca zamknięcie bierne będzie później w stanie TIME WAIT N
- ❏ Strona, która wysłała pierwszy segment FIN, może jeszcze potem nadawać dane N
- ❏ Strona, która wysłała pierwszy segment FIN, może jeszcze potem odbierać dane T

Które zdania dotyczące sieci bezprzewodowych 802.11 są prawdziwe?

- ❏ Protokół wykorzystuje przeskakiwanie częstotliwości (frequency hopping) N
- ❏ Urządzenia nadające na takiej samej częstotliwości wzajemnie się zakłócają. T
- ❏ Urządzenie pracujące w paśmie 2.4 Ghz mogą być od siebie bardziej oddalone niż urządzenia pracujące w paśmie 5 Ghz T
- ❏ Dostęp do kanału opiera się na wykrywaniu kolizji tak jak w Ethernecie N

Po wpisaniu linuksowego polecenia ifconfig eth0 10.1.1.15 następujące ustawienia zostaną skonfigurowane dla sieci podłączonej do interfejsu eth0.

- ❏ Adres rozgłoszeniowy zostanie ustawiony na 10.1.1.255 T
- ❏ Brama domyślna zostanie ustawiona na 10.0.0.1 N
- ❏ Polecenie zostanie odrzucone, gdyż nie podano maski podsieci N
- ❏ Brama domyślna zostanie ustawiona na 10.1.1.1 N

Które zdania dotyczące protokołu TCP są prawdziwe?

- ❏ RTO oznacza czas, po upływie którego niepotwierdzony segment zostanie wysłany ponownie T
- ❏ Wartość RTO jest ustalana na podstawie zmierzonego czasu RTT T
- ❏ Wartość RTO jest ustalana za pomocą protokołu ICMP N
- ❏ Wartość RTO jest stała dla wszystkich segmentów i niezmienna przez cały czas trwania połączenia. N

Zaznacz prawdziwe zdanie o atakach typu DoS (demand of service)

- ❏ Odbity atak DoS może być wykonany tylko jeśli atakujący posiada wiele komputerów N
- ❏ Rozproszony atak DoS oznacza, że wiele komputerów jest atakowanych jednocześnie N
- ❏ Atak DoS wymaga fabrykowania adresów IP N
- ❏ Do wyświetlenia źródła ataku można wykorzystywać protokół ICMP traceback T

Zaznacz prawdziwe zdania

- ❏ Protokół BOOTP zamienia adresy MAC na adresy IP T
- ❏ Protokół DNS zamienia nazwy domen na adresy IP T
- ❏ Protokół ARP zamienia adresy IP na adresy MAC T
- ❏ Protokół DHCP zamienia adresy IP na adresy MAC N

Sieć 192.168.17.0/26 została podzielona na 3 rozłączne podsieci, tak żeby każdy adres był w dokładnie jednej z nich. Jaki adres na pewno nie może być adresem rozgłoszeniowym w żadnej z tych podsieci?

- ❏ 192.168.17.31 Ten może być
- ❏ 192.168.17.63 Ten może być

- ❏ 192.168.17.255 Nie może być
- ❏ 192.168.17.15 Ten może być

Przeglądarka WWW nawiązuje połączenie z serwerem WWW. Pakiet zawierający całe żądanie HTTP gubi się. Co się stanie?

- ❏ Po pewnym czasie przeglądarka WWW wyśle zapytanie ARP N
- ❏ Po pewnym czasie serwer WWW wyśle żądanie o ponowne przesłanie zagubionego pakietu N
- ❏ Po pewnym czasie przeglądarka WWW ponownie wyśle pakiet. N
- ❏ Po pewnym czasie warstwa transportowa ponownie wyśle pakiet. T

Załóżmy, że routery A i B są bezpośrednio połączone i wykorzystują algorytm RIP. Tablica routingu A zawiera wpis określający, że istnieje ścieżka długości 5 do routera X, na której pierwszym krokiem jest router B. Router B wysyła do routera A informację, że jego odległość od X wynosi 10. Co zrobi router A?

- ❏ Zignoruje tę informację, gdyż jego obecna trasa jest lepsza N
- ❏ Powyższa informacja w ogóle nie dotrze do A ze względu na technikę dzielenia horyzontu N
- ❏ Zaktualizuje swój wpis, zmieniając odległość do routera X na 9 N
- ❏ Zaktualizuje swój wpis, zmieniając odległość do routera X na 11 T

Tylko jedna poprawna odpowiedź. W pewnym typie Ethernetu wysłanie pojedynczego bitu zajmuje 1/10 mikrosekundy (1 mikrosekunda = 10^-6 sekundy), wszystkie ramki mają po 20 bajtów. Zakładamy, że sygnał w kablu rozchodzi się z prędkością 100 000 km/s. Jaka jest maksymalna odległość między dwoma komputerami umożliwiająca działanie protokołowi CSMA/CD?

- ❏ 320 m N
- ❏ 800 m T
- ❏ 1600 m N
- ❏ 32 m N

Kryptograficzna funkcja skrótu (fingerprint) określona jest funkcją h. Jakie są pożądane właściwości takiej funkcji?

- ❏ Funkcja h powinna być efektywnie obliczalna T
- ❏ Funkcja h powinna być bijekcją N
- ❏ Dla dowolnego x znalezienie y != x spełniającego h(x) = h(y) jest obliczeniowo trudne N
- ❏ Funkcje h^-1 powinna być efektywnie obliczalna T

Komputer (nadawca) wysyła wiadomość do komputera (odbiorcy) leżącego w innej sieci. Co znajdzie się w ramce x wiadomością w momencie jej wysyłania przez komputer?

- ❏ Adres MAC karty sieciowej odbiorcy N
- ❏ Adres MAC karty sieciowej nadawcy T
- ❏ Adres MAC karty sieciowej bramy domyślnej T
- ❏ Adres MAC karty przełącznika sieciowego N

Jakie techniki pomagają w walce ze spamem?

- ❏ phishing N
- ❏ ICMP traceback N
- ❏ greylisting T
- ❏ filtry bayesowskie T

Komputerowi został przypisany adres IP równy 10.20.30.255/23, a brama domyślna została wybrana jako 10.20.32.200. Zaznacz prawdziwe zdania:

- ❏ Komputer nie będzie mógł się komunikować, gdyż ma przypisany adres rozgłoszeniowy. N
- ❏ Komputer będzie mógł komunikować się tylko z komputerami leżącymi w jego podsieci. T
- ❏ Komputer nie będzie mógł się komunikować, gdyż ma przypisany adres sieci N
- ❏ Komputer będzie mógł komunikować się bezpośrednio z komputerami leżącymi w jego (ciężko odczytać ze zdjęć)podsieci, a z innymi komputerami za pośrednictwem bramy domyślnej … N

Który z poniższych protokołów działa w warstwie transportowej?

- ❏ DNS N
- ❏ TCP T
- ❏ ICMP N
- ❏ FTP N

Tylko jedna poprawna odpowiedź. Karta sieciowa komputera ma przypisany adres 172.16.2.100/25, a jego brama domyślna ma adres 172.16.2.1. Pamięć podręczna ARP jest pusta. Co nastąpi jako pierwsze, jeśli komputer chce wysłać ramkę do adresu 172.16.2.200/25?

- ❏ Komputer roześle (na adres rozgłoszeniowy) zapytanie ARP o adres 172.16.2.1 T
- ❏ Komputer roześle (na adres rozgłoszeniowy) zapytanie ARP o adres 172.16.2.200 N
- ❏ Ramka nie zostania wysłana, a wysyłająca aplikacja otrzyma komunikat ICMP redirect. N
- ❏ Komputer wyślę ramkę do przełącznika, a przełącznik wyśle ją do odpowiedniego adresu. N

Tylko jedna poprawna odpowiedź. Załóżmy, że jedna czwarta listów to spam. Słowo zaliczyć występuje w 25% maili, które nie są spamem i w 50% maili, które są spamem. Załóżmy, że dostajemy losowy mail z puli wszystkich maili i okazuje się, że występuje w nim słowo zaliczyć. Jakie jest prawdopodobieństwo, że ten mail to spam?

- ❏ ¼ N
- ❏ 4/7 N
- ❏ ⅔ T
- ❏ ½ N

Które zdania dotycząca szyfrowania są prawdziwe?

- ❏ Algorytmy szyfrowania asymetrycznego są zazwyczaj wolniejsze niż algorytmy szyfrowania symetrycznego T

- ❏ W algorytmach szyfrowania symetrycznego wiadomość szyfrujemy i deszyfrujemy za pomocą tego samego klucza. T
- ❏ RSA jest szyfrem monoalfabetycznym N
- ❏ One-time pad jest szyfrem monoalfabetycznym N

Efektem wywołania na gnieździe TCP funkcji bind() jest:

- ❏ wysłanie segmentu z ustawioną flagą SYN N
- ❏ wysłanie segmentu z ustawiona flagą RST N
- ❏ wywołania funkcji bind() jest dozwolone tylko w przypadku gniazd UDP N
- ❏ wysłanie segmentu z ustawioną flagą ACK N

Algorytm Nagle'a:

- ❏ Jest wyłączany w przypadku niektórych usług internetowych(interaktywnych kappa) T
- ❏ Stosowany jest w protokole ARP. N
- ❏ Jest wyłączany w przypadku połączeń SMTP N
- ❏ Stosowany jest w protokole UDP N

Które z poniższych adresów są dopuszczalnymi formami zapisu adresu IPv6
0fed:0000:0000:0000:f000:0000:0000:0001

- ❏ 0fed::f000::0001 N
- ❏ fed:0:0:0:f:0:0:1 N
- ❏ fed:0:0:0:f000:0:0:1 T
- ❏ 0fed:0000:0000:0000:f000::1 T

Adres 203.0.1.191 jest adresem rozgłoszeniowym przy masce podsieci:

- ❏ /28 T
- ❏ /25 N
- ❏ /26 T
- ❏ /24 N

Zaznacz prawdziwe zdania

- ❏ Jeśli łączymy mostem dwie sieci o różnych MTU, to most będzie w razie potrzeby dzielił ramki na mniejsze części. N
- ❏ Przełącznik sieciowy pozwala na redukowanie domen kolizji. T
- ❏ Przełączenie karty sieciowej w tryb nasłuchu (promiscuous mode) umożliwia podsłuchiwanie całego ruchu sieciowego w sieci lokalnej, nawet jeśli sieć wykorzystuje przełączniki N
- ❏ Koncentrator pozwala na redukowanie domen kolizji N

Wynoszące 15 ograniczenie algorytmy RIP na maksymalną odległość między dwoma routerami:

- ❏ Umożliwia usunięcie duplikatów pakietów z sieci N
- ❏ Powoduje, że algorytmu tego nie można stosować w sieciach o średnicy równej 20 T
- ❏ W niektórych przypadkach pomaga pozbyć się pętli w routingu T
- ❏ Zabezpiecza przed otrzymywaniem spamu N