Wykład 1 - Sieci komputerowe

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

Protokół komunikacyjny to zbiór zasad określających sposób wymiany danych między aplikacjami w sieci. Warstwy protokołów wprowadza się w celu modularności, ułatwienia implementacji, możliwości niezależnego rozwoju warstw i prostoty zarządzania funkcjami sieciowymi.

Warstwy internetowego modelu warstwowego i ich zadania

1. **Aplikacji** – HTTP, SMTP – protokoły użytkownika.
2. **Transportowa** – TCP, UDP – dzieli dane na pakiety, wprowadza porty, zapewnia niezawodność.
3. **Sieciowa** – IP – routuje pakiety, dostarcza globalnie.
4. **Łącza danych** – Ethernet, WiFi – przesyła ramki, zapewnia dostęp do medium.
5. **Fizyczna** – przesyła bity przez kanał.

Warstwy zaimplementowane na komputerach i routerach

- **Komputery**: wszystkie warstwy (1–5).
- **Routery**: warstwa 3 (sieciowa), 2 (łącza danych), 1 (fizyczna).

Różnice między modelem TCP/IP a OSI

- TCP/IP łączy warstwy fizyczną i łącza danych w jedną.
- OSI ma dodatkowe warstwy: sesji i prezentacji między transportową a aplikacyjną.

Co jest potrzebne do zbudowania dwukierunkowego niezawodnego kanału?

- Adresacja IP, dzielenie na pakiety, niezawodność przesyłania (np. TCP), porty aplikacji.

Wady i zalety przełączania obwodów i pakietów

Cechy	Obwody	Pakiety
Gwarancja przepustowości	✔	✘
Koszt nawiązania	wysoki	niski
Efektywność	niska	wysoka
Odporność na awarie	niska	wysoka
Skomplikowanie	wysokie	niskie

Rodzaje multipleksowania i ich zastosowanie

- **TDM (czasowe)** – każdemu przydzielany czas transmisji.
- **FDM (częstotliwościowe)** – każdemu przydzielana częstotliwość.
- **Statystyczne** – pakiety współdzielą łącze dynamicznie – najlepsze wykorzystanie medium.

Rodzaje routingu

- **Źródłowy** – trasa w nagłówku pakietu.
- **Z tablic routingu** – routery kierują pakiety wg reguł.
- **Wirtualne obwody** – ustalona trasa po wysłaniu pakietu kontrolnego.

Rodzaje komunikacji

- **Simpleksowa** – jednokierunkowa.
- **Półdupleksowa** – naprzemienna w obu kierunkach.
- **Pełnodupleksowa** – jednoczesna w obu kierunkach.

Do czego służy traceroute?

Służy do śledzenia trasy pakietu w sieci i pokazuje pośrednie routery oraz czasy przejścia.

Po co bufory w routerach? Co to przeciążenie?

Bufory przechowują pakiety przy przeładowaniu. Przeciążenie następuje przy ich przepełnieniu – prowadzi do utraty pakietów.

Przyczyny opóźnień pakietów

- Czas oczekiwania w kolejce.
- Czas transmisji (rozmiar/przepustowość).
- Czas propagacji sygnału.

BDP i czas propagacji

- **BDP (Bandwidth-Delay Product)** – ile danych można wysłać przed otrzymaniem odpowiedzi.
- **Czas propagacji** – ile trwa przesłanie sygnału między dwoma punktami.

Protokół IP – funkcje i zasada best effort

- Umożliwia przesyłanie pakietów między urządzeniami.
- Best effort – brak gwarancji dostarczenia i kolejności, ale pakiety nie są gubione celowo.

Zalety i wady zasady end-to-end

- **Zalety**: prostota sieci, elastyczność, łatwość wdrażania nowych usług.
- **Wady**: więcej odpowiedzialności po stronie urządzeń końcowych.

Po co porty?

Porty pozwalają rozróżnić różne aplikacje działające na tym samym urządzeniu.

Enkapsulacja i dekapsulacja

- **Enkapsulacja** – dodawanie nagłówków przy przechodzeniu do niższych warstw.
- **Dekapsulacja** – usuwanie nagłówków przy przechodzeniu do wyższych warstw.

Wykład 2 - Routing: adresowanie

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

Hierarchia wynika z potrzeby uproszczenia trasowania – adresy IP mają wspólne prefiksy opisujące całe sieci. Dzięki temu router nie musi znać każdej trasy osobno, tylko reguły dla większych bloków adresów. Upraszcza to tablice routingu i przyspiesza decyzje trasowania.

Notacja CIDR

CIDR (Classless Inter-Domain Routing) zapisuje zakresy adresów jako: `adres_ip/długość_prefiksu`, np. `156.17.4.32/28`. Pozwala elastycznie dzielić sieci, niezależnie od dawnych klas adresów.

Co to jest adres rozgłoszeniowy?

To ostatni adres w sieci CIDR, używany do wysyłania pakietów do wszystkich urządzeń w tej sieci. Np. w `156.17.4.32/28` adresem rozgłoszeniowym jest `156.17.4.47`.

Co to jest maska podsieci?

To długość prefiksu sieci określająca liczbę bitów opisujących sieć. Może być zapisana np. jako `/28` lub w postaci binarnej `255.255.255.240`.

Opisz sieci IP klasy A, B i C.

Podział historyczny: - Klasa A: adresy zaczynające się od `0`, maska `/8` - Klasa B: zaczynają się od `10`, maska `/16` - Klasa C: zaczynają się od `110`, maska `/24`

Co to jest pętla lokalna (loopback)?

Sieć `127.0.0.0/8`, najczęściej `127.0.0.1`, używana do połączeń z lokalnym komputerem, np. testowania aplikacji sieciowych.

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

- **TTL (Time To Live):** ogranicza liczbę przeskoków pakietu. Każdy router zmniejsza TTL o 1. Gdy osiągnie 0, pakiet jest odrzucany.
- **Protokół:** informuje, jaki protokół znajduje się w danych pakietu (np. TCP=6, UDP=17, ICMP=1).

Jakie reguły zawierają tablice routingu?

Reguły postaci: „jeśli adres zaczyna się od prefiksu X, wyślij pakiet do Y (interfejs/router)”.

Na czym polega reguła najdłuższego pasującego prefiksu?

Gdy więcej niż jedna reguła pasuje do adresu, wybierana jest ta z najdłuższym (najbardziej szczegółowym) prefiksem.

Co to jest trasa domyślna?

Reguła `0.0.0.0/0` – pasuje do każdego adresu. Używana, gdy brak innej, bardziej szczegółowej reguły.

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

ICMP to pomocniczy protokół IP używany do diagnostyki (np. błędy, ping). Typy: - 0 – Echo reply - 3 – Destination unreachable - 8 – Echo request - 11 – Time exceeded

Jak działa polecenie ping?

Wysyła ICMP echo request (typ 8). Odbiorca odsyła echo reply (typ 0), co pozwala zmierzyć czas odpowiedzi.

Jak działa polecenie traceroute?

Wysyła pakiety z rosnącym TTL. Każdy router odsyła „Time Exceeded” (typ 11). Pozwala ustalić trasę do celu.

Dlaczego do tworzenia gniazd surowych wymagane są uprawnienia administratora?

Gniazda surowe dają dostęp do niskopoziomowych pakietów (np. ICMP), co może być wykorzystywane do ataków sieciowych – dlatego wymagane są uprawnienia roota.

Co to jest sieciowa kolejność bajtów?

To „big endian” – najpierw najbardziej znaczący bajt. Wszystkie liczby w nagłówkach IP muszą być w tej kolejności. Do konwersji służą `htons`, `htonl`, `ntohs`, `ntohl`.

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

- `socket()` – tworzy gniazdo
- `recvfrom()` – odbiera pakiet z gniazda
- `sendto()` – wysyła pakiet przez gniazdo

Jakie informacje zawiera struktura adresowa sockaddr_in?

- Typ rodziny adresowej (`AF_INET`)
- Port (`sin_port`)
- Adres IP (`sin_addr`)
- Pole na zera

Co to jest tryb blokujący i nieblokujący? Co to jest aktywne czekanie?

- **Blokujący:** `recvfrom()` czeka na pakiet.
- **Nieblokujący:** `recvfrom()` zwraca od razu, nawet jeśli nie ma pakietu.
- **Aktywne czekanie:** ciągłe wywoływanie `recvfrom()` w pętli – zużywa 100% CPU.

Jakie jest działanie funkcji select()?

Funkcja `select()` (lub `poll()`) pozwala monitorować wiele deskryptorów (np. gniazd) i czekać na gotowość do odczytu bez aktywnego czekania.

Wykład 3 - Routing: tworzenie tablic

Co to jest cykl w routingu? Co go powoduje?

Cykl w routingu to sytuacja, gdy pakiet krąży w sieci bez końca między routerami. Powodowany jest przez niespójne lub błędne tablice routingu – np. gdy routery nie wiedzą o awarii łącza i aktualizują się wzajemnie, tworząc błędne trasy.

Czym różni się tablica routingu od tablicy przekazywania?

- **Tablica routingu** zawiera wszystkie znane trasy, także zapasowe.
- **Tablica przekazywania (forwarding table)** zawiera tylko informacje potrzebne do podjęcia decyzji o przesłaniu pakietu – zawiera najdłużej pasujący prefiks i wskazanie następnego hopu.

Dlaczego w algorytmach routingu dynamicznego obliczamy najkrótsze ścieżki?

Aby zminimalizować opóźnienie, koszt lub liczbę przeskoków – zależnie od wybranej metryki. Unika to cykli i pozwala efektywnie wykorzystywać sieć.

Co to jest metryka? Jakie metryki mają sens?

Metryka to wartość przypisana krawędziom sieci używana do wyznaczania najkrótszych ścieżek. Przykłady: - czas propagacji, - koszt finansowy, - liczba przeskoków (hops).

Czym różnią się algorytmy wektora odległości od algorytmów stanów łączy?

- **Stanów łączy**: każdy router informuje wszystkich o swoich sąsiadach i sam oblicza ścieżki.
- **Wektora odległości**: routery wymieniają się informacjami tylko z sąsiadami, aktualizując tablice na podstawie ich wektorów.

Jak router może stwierdzić, że bezpośrednio podłączona sieć jest nieosiągalna?

Poprzez brak odpowiedzi lub brak komunikatów od sąsiada przez określony czas (np. brak Hello przez 30s). Wtedy ustawia odległość do tej sieci na ∞.

Co to znaczy, że stan tablic routingu jest stabilny?

Oznacza, że kolejne wymiany informacji nie powodują już zmian w tablicach – sieć zbiega się do stanu spójnego.

Jak zalewać sieć informacją? Co to są komunikaty LSA?

- **Zalewanie**: router wysyła informację do wszystkich sąsiadów, którzy przesyłają ją dalej (z pominięciem źródła).
- **LSA (Link State Advertisement)**: komunikat opisujący stan łącza – zawiera źródło, numer sekwencyjny i jest podstawą działania OSPF.

Co wchodzi w skład wektora odległości?

Wektor odległości zawiera: - odległość do znanych sieci, - informację o następnym routerze (hopie) do celu.

W jaki sposób może powstać cykl w routingu?

Gdy routery aktualizują się nawzajem na podstawie błędnych informacji (np. po awarii łącza) – powstaje błędne przekonanie, że ścieżka istnieje przez sąsiada, który używa nas jako trasy.

Co to jest problem zliczania do nieskończoności? Kiedy występuje?

Występuje w wektorze odległości, gdy routery błędnie zwiększają wartość odległości do nieosiągalnej sieci w każdej turze – powoduje to opóźnione wykrycie problemu.

Na czym polega technika zatruwania ścieżki zwrotnej (poison reverse)?

Router, który używa danego sąsiada jako trasy do celu, wysyła temu sąsiadowi informację, że ma do celu odległość ∞, aby zapobiec błędnej aktualizacji.

Po co w algorytmach wektora odległości definiuje się największą odległość (np. 16 w RIP)?

Aby przerwać zliczanie do nieskończoności – po osiągnięciu tej wartości sieć jest uznawana za nieosiągalną.

Po co stosuje się przyspieszone uaktualnienia?

Aby szybciej propagować informacje o zmianach w sieci (np. awariach), bez czekania na standardowy interwał aktualizacji.

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

AS to zbiór routerów zarządzanych przez jednego operatora z jednolitą polityką routingu. Typy: - z jednym wyjściem, - nietranzytowy (wiele wyjść, nie przekazuje ruchu), - tranzytowy (przekazuje ruch innych AS).

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

- **Dostawca-klient**: klient płaci, dostawca rozgłasza jego trasy.
- **Peering**: wzajemna wymiana danych bez opłat; nie rozgłasza się tras do swoich dostawców.

Dlaczego w routingu między AS nie stosuje się najkrótszych ścieżek?

Bo decyzje routingowe wynikają z polityki (koszty, prywatność, autonomia), a nie z długości trasy.

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

- **Rozgłaszać**: trasy do siebie, swoich klientów (bo płacą).
- **Nie rozgłaszać**: tras do dostawców i partnerów (chyba że klientowi).
- **Wybierać**: najpierw przez klienta, potem partnera, na końcu dostawcę.

Jak BGP może współpracować z algorytmami routingu wewnątrz AS?

Routery brzegowe używają BGP do poznania tras między AS-ami, a następnie udostępniają te informacje do wewnętrznego protokołu (np. OSPF, RIP), który rozprowadza je wewnątrz AS.

Wykład 4 - Routing wewnątrz routera

Prywatne adresy IP i zarezerwowane pule

Prywatne adresy IP są przeznaczone do użytku w sieciach lokalnych i nie są routowalne w Internecie. Zarezerwowane pule: - 10.0.0.0/8 - 172.16.0.0/12 - 192.168.0.0/16 - IPv6: fd00::/8

Funkcja `bind()`

Służy do powiązania gniazda z konkretnym adresem IP i portem. Wymagana dla serwera. Klienci często korzystają z automatycznie przydzielanego portu.

Porty < 1024

Porty o numerach mniejszych niż 1024 są tzw. portami uprzywilejowanymi. Aby się z nimi związać, wymagane są uprawnienia administratora.

Zadania elementów routera

- **Procesor routingu** – tworzy tablice przekazywania.
- **Port wejściowy** – odbiera pakiety, modyfikuje TTL i sumy kontrolne.
- **Port wyjściowy** – wysyła pakiety.
- **Struktura przełączająca** – przekazuje pakiety między portami z dużą prędkością.

Przełączanie przez RAM vs strukturę przełączającą

- RAM: wszystkie operacje przez CPU, wolniejsze.
- Struktura przełączająca: dedykowana sieć połączeń, szybsze i skalowalne przekazywanie.

Pożądane cechy struktury przełączającej

- Przepustowość zbliżona do $N \times R$ (N – liczba portów, R – prędkość portu).
- Niska złożoność połączeń (np. $O(N \log N)$ – sieci Benesa).

Buforowanie w routerze

Stosowane przy portach wejściowych i wyjściowych: - **Wyjściowe** – zapobiegają utracie przy nagłych skokach ruchu. - **Wejściowe** – konieczne, gdy struktura przełączająca jest zbyt wolna.

Klasyfikacja pakietów w portach wyjściowych

Służy do przypisania pakietów do strumieni i umożliwia szeregowanie wg priorytetów lub round-robin.

Blokowanie początku kolejki

Zjawisko, gdy pakiet czekający na zajęty port blokuje inne. Występuje przy buforowaniu na wejściu. Rozwiązanie: wirtualne kolejki (dla każdego portu wyjściowego osobna kolejka).

LPM – Longest Prefix Match

Mechanizm wyboru reguły w tablicy przekazywania z najdłuższym pasującym prefiksem.

Struktury danych dla LPM

1. **Lista prefiksów** – pamięć O(n), lookup O(n)
2. **Tablice haszujące** – O(w) lookup, O(1) insert/delete
3. **Trie (drzewo prefiksów)** – O(w) wszystkie operacje, możliwość kompresji
4. **Trie z krawędziami skracającymi** – lookup O(log w), insert/delete nawet O(n)
5. **TCAM** – sprzętowa, szybkie wyszukiwanie pasujących prefiksów równolegle

TCAM

Ternary CAM – pamięć sprzętowa do szybkiego wyszukiwania. Zawiera pary (prefiks, maska) i pozwala na równoległe dopasowanie wszystkich reguł.

Fragmentacja IP

Dzieli pakiet na mniejsze fragmenty, jeśli przekracza MTU. Może zachodzić na dowolnym routerze, a łączenie fragmentów następuje dopiero u odbiorcy.

MTU i jego wykrywanie

MTU = maksymalna wielkość pakietu dla łącza. Wykrywanie przez ustawienie bitu DF – router zwraca ICMP, jeśli konieczna fragmentacja, z informacją o MTU.

Szeregowanie pakietów

- FIFO – wg kolejności przyjścia.
- Priorytetowe – wg ważności strumienia.
- Round-robin – naprzemiennie z każdego strumienia.

IPv4 vs IPv6

- IPv6: 128-bitowe adresy, brak fragmentacji i sumy kontrolnej, nagłówek o stałej długości.
- IPv4: 32-bitowe adresy, możliwość fragmentacji, suma kontrolna.

Skrócony adres IPv6

0321:0000:0000:0123:0000:0000:0000:0001 → `321:0:0:123::1`

Tunelowanie 6in4

Pakiety IPv6 osadzane jako dane w pakietach IPv4. Umożliwia przesył IPv6 przez infrastrukturę IPv4.

NAT – Network Address Translation

Mechanizm zamiany prywatnych adresów IP na publiczne. Zalety: - Oszczędność adresów IP. - Niezależność od ISP. Wady: - Trudność w inicjowaniu połączeń z Internetu. - Łamanie modelu warstwowego.

Stan w NAT

Router NAT musi przechowywać tabelę mapującą (adres źródłowy, port, adres docelowy, port) → port translacji. Przypisanie tymczasowe, używane do powrotu pakietów.

Wykład 5 - Niższe warstwy sieci komputerowych

Zadania warstw

- **Warstwa łącza danych**: komunikacja między sąsiadującymi urządzeniami, wykrywanie błędów transmisji, zawodna usługa ramek.
- **Warstwa fizyczna**: przesyłanie bitów przez medium fizyczne (np. fale radiowe, światłowód, skrętka).

Koncentrator vs przełącznik

- **Koncentrator (hub)**: przekazuje każdą ramkę do wszystkich portów, brak inteligencji.
- **Przełącznik (switch)**: uczy się adresów MAC i kieruje ramki tylko do odpowiedniego portu.

Algorytmy ALOHA

- **Rundowy ALOHA**: czas podzielony na rundy, nadawanie z prawdopodobieństwem `p`.
- **Bezrundowy ALOHA**: brak synchronizacji, mniejsze wykorzystanie łącza.

Algorytm odczekiwania wykładniczego

Po kolizji zwiększamy zakres odczekiwania: losowanie z przedziału `0..2^m - 1`, stosowane w Ethernet i WiFi.

CSMA/CD vs CSMA/CA

- **CSMA/CD** (Ethernet): wykrywanie kolizji i przerywanie transmisji.
- **CSMA/CA** (WiFi): unikanie kolizji, brak możliwości ich wykrycia.

Budowa ramki Ethernetowej

- Adres docelowy i źródłowy MAC, typ, dane (46-1500 B), suma kontrolna CRC.
- Minimalna długość ramki: 64 bajty (dla wykrywania kolizji).

Adres MAC

- 6 bajtów, unikatowy identyfikator karty sieciowej, możliwy do zmiany.

Tryb nasłuchu (promiscuous mode)

- Karta sieciowa przekazuje wszystkie ramki do systemu operacyjnego.

Minimalna długość ramki w Ethernecie

- Zapewnia wykrycie kolizji zanim nadawanie zostanie zakończone.

Protokół ARP i DHCP

- **ARP**: zamiana adresów IP na MAC.
- **DHCP**: dynamiczne przydzielanie adresu IP i innych parametrów sieci.

Most vs router

- **Most**: działa na warstwie łącza danych, szybszy, nie obsługuje fragmentacji IP.
- **Router**: działa na warstwie sieci, obsługuje IP i routing.

Rozgłaszanie w warstwie łącza danych

- Ramki wysyłane na MAC `FF:FF:FF:FF:FF:FF` trafiają do wszystkich urządzeń w domenie rozgłoszeniowej.

Tryb uczenia się przełącznika

- Przełącznik zapamiętuje adresy MAC i porty, aby kierować ruch bez rozgłaszania.

Algorytm drzewa spinającego (STP)

- Zapobiega cyklom w sieci poprzez tworzenie drzewa spinającego, używa go Ethernet.

VLAN

- Logiczny podział sieci niezależnie od fizycznego połączenia. Ramki zawierają identyfikator VLAN.

Zjawisko ukrytej stacji

- Komputer nie wykrywa transmisji innego komputera i powoduje kolizję w punkcie dostępowym.

RTS i CTS

- **RTS (Request To Send)** i **CTS (Clear To Send)**: rezerwacja kanału w WiFi przed wysłaniem danych.

Wykład 6 - Transport (podstawy)

Co może stać się z przesyłanym ciągiem pakietów IP?

W przypadku zawodnego transportu (UDP) pakiety mogą zostać: uszkodzone, zgubione, opóźnione, przyjść w złej kolejności lub zostać zduplikowane. Niezawodny transport (TCP) wykrywa i naprawia te błędy.

Co to jest kontrola przepływu?

Mechanizm zapobiegający zalewaniu odbiorcy danymi, na które nie ma miejsca w buforze. Odbiorca wysyła tzw. okno oferowane (wolne miejsce), a nadawca dostosowuje szybkość transmisji.

UDP vs TCP + zastosowania

UDP: szybki, zawodny – np. DNS, DHCP, gry.
TCP: wolniejszy, niezawodny – np. HTTP(S), transmisje danych.

Co to segmentacja i MSS?

Segmentacja to dzielenie danych na mniejsze jednostki.
MSS (Maximum Segment Size) = MTU - nagłówki IP i TCP.
Segmenty mają ograniczoną wielkość z powodu ryzyka błędów i ograniczeń sieci.

Jednostki danych w warstwach:

- Aplikacji: dane
- Transportowej: segmenty (TCP) / datagramy (UDP)
- Sieciowej: pakiety
- Łącza danych: ramki

Jak małe pakiety zmniejszają opóźnienie?

Małe pakiety szybciej przechodzą przez routery i są łatwiejsze do umieszczenia w kolejce.

RTT i RTO

RTT – czas przelotu tam i z powrotem.
RTO – czas oczekiwania na ACK, po którym następuje retransmisja.
RTO = 2×avgRTT + 4×varRTT

Jak wykrywane są duplikaty?

Za pomocą numerów sekwencyjnych. Duplikaty są ignorowane lub potwierdzane ponownie.

Stop-and-Wait – opis

Nadawca czeka na ACK po każdym segmencie.
Zalety: prostota.
Wady: niska wydajność na dużych opóźnieniach (niewykorzystane łącze).

Numery sekwencyjne – do czego służą?

Numerują segmenty/bajty, umożliwiają wykrycie brakujących lub duplikatów i ich uporządkowanie.

Algorytm okna przesuwnego

Nadawca może wysłać kilka segmentów bez oczekiwania na ACK. Po odebraniu ACK okno przesuwa się dalej.

Rozmiar okna a BDP

BDP (bandwidth-delay product) = przepustowość × opóźnienie. Okno powinno być co najmniej tej wielkości, aby w pełni wykorzystać łącze.

Porównanie mechanizmów potwierdzania:

- **Go-Back-N:** ACK tylko dla ostatniego poprawnego segmentu, brak bufora, retransmisje wielu segmentów.
- **Selektywne:** ACK dla każdego segmentu, buforowanie, retransmisja tylko brakujących.
- **Skumulowane:** ACK dla największego ciągłego segmentu, możliwość opóźniania ACK.

Dlaczego istotne są ACK duplikatów?

Pozwala nadawcy odróżnić brak ACK od jego utraty i uniknąć niepotrzebnych retransmisji.

Okno oferowane

Okno oznacza ile miejsca ma odbiorca. Wysyłane nadawcy, który dostosowuje transmisję.

TCP – mechanizmy niezawodności i kontroli:

- retransmisje, timeouty, numery sekwencyjne, potwierdzenia (ACK),
- kontrola przepływu za pomocą okna oferowanego.

Opóźnione ACK w TCP

ACK nie jest wysyłane natychmiast – czeka się chwilę lub do wysłania danych w drugą stronę.

Mechanizm Nagle’a

Zbiera małe dane i wysyła większy pakiet – ogranicza liczbę małych pakietów. Nie stosować w aplikacjach interaktywnych.

Pola w nagłówku TCP:

- **Numer sekwencyjny** – numer pierwszego bajtu.
- **Numer potwierdzenia (ACK)** – numer kolejnego oczekiwanego bajtu.

Czy warstwa transportowa jest na routerach?

Nie. Transport działa tylko na końcach (hostach), routery operują na warstwie sieciowej.

Zasada end-to-end:

- **Słaba wersja:** niższe warstwy mogą pomagać.
- **Silna wersja:** niezawodność zapewniana tylko na końcach – routery nie ingerują.

Wykład 7 - TCP

Co to jest gniazdo?

Gniazdo (ang. socket) to interfejs komunikacyjny pomiędzy aplikacją a warstwą transportową, identyfikowany przez adres IP i numer portu. Pozwala na odbieranie i wysyłanie danych przez sieć.

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

- **Gniazdo nasłuchujące (serwera)** – służy tylko do przyjmowania połączeń, nie do przesyłania danych.
- **Gniazdo połączone** – tworzone po zestawieniu połączenia, służy do komunikacji.
- W UDP **nie ma gniazd połączonych**, każde gniazdo działa niezależnie i nie utrzymuje stanu połączenia.

Co robią funkcje jądra:

- `bind()` – przypisuje gniazdu lokalny adres IP i port.
- `listen()` – przygotowuje gniazdo do nasłuchiwania połączeń (tworzy kolejkę).
- `accept()` – przyjmuje połączenie przychodzące z kolejki, tworząc gniazdo połączone.
- `connect()` – klient nawiązuje połączenie z serwerem.

Czym różni się komunikacja bezpołączeniowa od połączeniowej?

- **Bezpołączeniowa (UDP)** – brak utrzymywanego stanu, każda wiadomość jest niezależna.
- **Połączeniowa (TCP)** – wymagane nawiązanie i zakończenie połączenia, przesył danych jest bardziej uporządkowany i niezawodny.

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

- **Otwarcie bierne** – `listen()`, serwer oczekuje na połączenie.
- **Otwarcie aktywne** – `connect()`, klient inicjuje połączenie.
- Serwer **zwykle nie wykonuje otwarcia aktywnego**, ale technicznie jest to możliwe.

Do czego służą flagi TCP: SYN, ACK, FIN, RST?

- **SYN** – synchronizacja, inicjuje połączenie.
- **ACK** – potwierdzenie odebrania danych.
- **FIN** – zakończenie połączenia.
- **RST** – reset połączenia w przypadku błędu.

Trójstopniowe nawiązywanie połączenia TCP:

1. Klient wysyła `SYN`.
2. Serwer odpowiada `SYN-ACK`.
3. Klient wysyła `ACK`. Każda strona ustala początkowy numer sekwencyjny (losowy).

Dlaczego numeracja bajtów nie zaczyna się od zera?

Ponieważ początkowy numer sekwencyjny jest losowy – zwiększa bezpieczeństwo i zapobiega podszywaniu się.

Jakie segmenty są wymieniane podczas zamykania połączenia w TCP?

1. Jedna strona wysyła `FIN`.
2. Druga odpowiada `ACK`.
3. Druga strona wysyła `FIN`.
4. Pierwsza odpowiada `ACK`.

Co zwraca funkcja `recv()`?

- W trybie **blokującym**: czeka aż pojawią się dane, zwraca liczbę bajtów.
- W trybie **nieblokującym**: zwraca od razu, może zwrócić 0 (brak danych) lub -1 (błąd).

Po co jest stan TIME_WAIT?

Pozwala upewnić się, że ostatni `ACK` dotarł oraz zapobiega pomyłkom przy szybkim otwarciu nowego połączenia z tymi samymi parametrami (IP + porty).

Diagram stanów TCP – scenariusze:

- **Nawiązanie połączenia**: `CLOSED` → `SYN_SENT` (klient), `CLOSED` → `LISTEN` → `SYN_RECEIVED` (serwer) → `ESTABLISHED`.
- **Zamknięcie połączenia**: `ESTABLISHED` → `FIN_WAIT_1` → `FIN_WAIT_2` → `TIME_WAIT` → `CLOSED` (klient), `ESTABLISHED` → `CLOSE_WAIT` → `LAST_ACK` → `CLOSED` (serwer).

Wykład 8 - HTTP (Warstwa aplikacji)

Budowa adresu URL (http)

Adres URL (Uniform Resource Locator) ma postać: `schemat://nazwa_serwera[:port]/ścieżka`

Dla `http`: - schemat: `http` lub `https` - `//`: separator - nazwa serwera (np. `example.com`) - opcjonalnie `:port` - identyfikator zasobu (np. `/strona/index.html`)

MIME – typ zawartości

Serwer ustawia typ MIME, aby przeglądarka wiedziała jak obsłużyć plik. **Przykłady typów MIME:** - `text/html` – strony internetowe - `image/jpeg` – obrazki JPG - `application/pdf` – pliki PDF - `application/octet-stream` – surowe dane binarne

Pole `Host` w HTTP/1.1

Wskazuje, do jakiej domeny kierowane jest żądanie. Umożliwia hostowanie wielu stron na jednym adresie IP.

Pola nagłówka HTTP

- `Accept`: typy MIME akceptowane przez klienta
- `Accept-Language`: preferencje językowe
- `User-Agent`: informacje o przeglądarce/kliencie
- `Server`: dane o oprogramowaniu serwera
- `Content-Length`: długość treści odpowiedzi
- `Content-Type`: typ MIME zawartości odpowiedzi

Przechowywanie stanu w HTTP

HTTP jest bezstanowe. Stan przechowuje aplikacja, np. poprzez `Set-Cookie` z identyfikatorem sesji (`sID=...`), który klient potem odsyła w `Cookie`.

Warunkowe zapytanie GET

Używa nagłówka `If-Modified-Since`. Odpowiedź: - `200 OK` – zmodyfikowano - `304 Not Modified` – brak zmian

Kody odpowiedzi HTTP

- `1xx`: informacyjne
- `2xx`: sukces (`200 OK`)
- `3xx`: przekierowania (`301`, `302`)
- `4xx`: błąd klienta (`404 Not Found`)
- `5xx`: błąd serwera (`500 Internal Server Error`)

Połączenia trwałe w HTTP/1.1

Wiele żądań i odpowiedzi może być przesyłanych jednym połączeniem TCP. `Connection: close` – zamyka połączenie po odpowiedzi.

Cel metody POST

Umożliwia przesyłanie danych w treści żądania – np. formularzy i plików. Bezpieczniejsze niż GET (nie widać w URL).

REST (Representational State Transfer)

Styl tworzenia usług webowych wykorzystujący HTTP (metody GET, POST, PUT, DELETE). Umożliwia prostą, czytelną i zautomatyzowaną komunikację.

Serwery proxy – zastosowanie

Pośredniczą w żądaniach HTTP: - mogą przechowywać dane w cache, - zmniejszają obciążenie łącza, - filtrują lub kontrolują dostęp.

Odwrotne proxy i CDN

- **Odwrotne proxy**: przed serwerem WWW, rozdzielają ruch.
- **CDN**: sieć serwerów blisko klientów, serwuje statyczne zasoby szybciej.

Skierowanie klienta do proxy

- Ustawienia przeglądarki lub sieci
- ISP może wymusić użycie proxy
- DNS może kierować na adres proxy

Nagłówki dodawane przez proxy

- `X-Forwarded-For`: IP klienta
- `Via`: IP proxy

Anonimowe serwery proxy

Nie dodają identyfikujących nagłówków. Zwykle płatne – zwiększają prywatność.

QUIC – nowy protokół

Zastępuje TCP + TLS dla HTTP/3: - Bazuje na UDP - Zawiera szyfrowanie (TLS 1.3) - Mniejsza latencja (1 RTT) - Odporny na opóźnienia jednego strumienia (multiplexing)

Wykład 9 - Warstwa aplikacji cz. 2

Cel systemu DNS

Umożliwia tłumaczenie nazw domenowych (łatwych do zapamiętania dla ludzi) na adresy IP, niezależnie od zmian tych adresów.

Plik /etc/hosts

Historyczny plik lokalny zawierający mapowanie nazw domen na adresy IP, używany zanim powstał DNS. Nadal obecny w systemach operacyjnych.

TLD (Top Level Domains)

Domeny najwyższego poziomu, np. `.pl`, `.com`, `.edu`, `.uk`.

Strefy i delegacje DNS

- Strefa: fragment drzewa domen, zarządzany przez określony serwer nazw.
- Delegacja: wpis w nadrzędnej strefie wskazujący, który serwer obsługuje daną strefę.

Iteracyjne vs rekurencyjne odpytywanie DNS

- Iteracyjne: klient sam odpytuje kolejne serwery.
- Rekurencyjne: resolver DNS odpytuje kolejne serwery w imieniu klienta.

Odwrotny DNS

Zamiana adresu IP na nazwę domeny, używa rekordu `PTR` oraz specjalnej domeny `in-addr.arpa`.

Typy rekordów DNS

- `A` – IPv4
- `AAAA` – IPv6
- `NS` – wskazuje serwer nazw
- `MX` – wskazuje serwer poczty
- `CNAME` – alias innej domeny (kanoniczna nazwa)

SMTP vs IMAP

- SMTP – protokół do wysyłania maili (port 25/587).
- IMAP – protokół do pobierania i zarządzania mailami na serwerze.

Przekaźniki SMTP (relays)

Serwery pośredniczące w przekazywaniu wiadomości między serwerami nadawcy i odbiorcy.

Rekord DNS sprawdzany przed wysłaniem poczty

`MX` – wskazuje serwer odpowiedzialny za przyjmowanie poczty dla danej domeny.

Popularne pola nagłówka maila

- `Received` – ślad trasy wiadomości przez serwery
- `Bcc` – ukryta kopia wiadomości

Standard MIME

Pozwala przesyłać różne typy danych (tekst, HTML, załączniki), definiuje m.in. `Content-Type`.

Spam i metody walki

Uczenie maszynowe, blokowanie IP, spowalnianie połączeń, SPF, podpisy cyfrowe

SPF

Rekord TXT w DNS określający, które adresy IP mają prawo wysyłać pocztę w imieniu danej domeny.

Rola trackera w BitTorrent

Utrzymuje listę użytkowników i udostępnia listę peerów chcących pobrać dany plik.

Funkcje skrótu w .torrent

Pozwalają na weryfikację poprawności fragmentów pliku.

Seeder vs leecher

- Seeder – posiada cały plik i udostępnia go innym.
- Leecher – pobiera fragmenty, udostępniając przy tym innym te, które już ma.

Połączenia odwrócone

Gdy klient za NAT nie może odebrać połączenia, zewnętrzny serwer pośredniczy i klient inicjuje połączenie.

FTP i NAT

- Tryb aktywny FTP nie działa za NAT.
- Tryb pasywny FTP pozwala serwerowi inicjować połączenie odbioru danych, co działa za NAT.

NAT cone vs symetryczny

- Full cone NAT: przekazuje pakiety z dowolnego źródła.
- Restricted cone NAT: przekazuje tylko jeśli wcześniej nastąpiła komunikacja.
- Symetryczny NAT: przypisania zależą od pary nadawca-odbiorca, przez co trudny do przejścia.

Hole punching

Technika obejścia NAT polegająca na inicjacji połączenia do znanego portu z pomocą serwera pośredniczącego, pozwalająca na bezpośrednią komunikację.

Wykład 10 - Kodowanie i szyfrowanie

Typy kodów detekcyjnych

- **Bit parzystości** – wykrywa błędy z nieparzystą liczbą przekłamań.
- **Prosta suma kontrolna** – sumowanie słów, wykrywa niektóre błędy; nie wykrywa zamiany słów.
- **CRC (Cyclic Redundancy Check)** – oparty na wielomianach, skuteczny i powszechnie stosowany (np. w Ethernecie).

Rodzaje błędów transmisji

- Przekłamania bitów (pojedynczych lub ciągów),
- Zgubione lub wstawione bity,
- Błędy sprzętowe (RAM, oprogramowanie).

Algorytm CRC – jak działa

1. Zamieniamy wiadomość m na wielomian M(x),
2. Obliczamy $x^r \cdot M(x)$ i dzielimy przez G(x),
3. Reszta z dzielenia to suma kontrolna S(x),
4. Wysyłamy $B(x) = x^r \cdot M(x) + S(x)$,
5. Odbiorca sprawdza, czy G(x) dzieli B'(x).

Wykrywanie błędów CRC

- $G(x) \nmid B'(x) \Rightarrow$ błąd transmisji,
- Wiele typów błędów jest wykrywanych, np. pięć kolejnych przekłamań.

Metody korekcji błędów

- **Kody korekcyjne** – pozwalają również na poprawę błędów,
- **Kod Hamminga (np. (7,4))** – wykrywa 2 błędy, koryguje 1,
- **(3,1)-kod** – powtarzanie każdego bitu 3 razy (mało efektywne).

(a,b)-kod – definicja i przykład

- Kodowanie wiadomości długości b na długość $a \geq b$,
- Przykład: bit parzystości dla 7 bitów to (8,7)-kod,
- Narzut = a/b.

Odległość Hamminga

- Minimalna liczba bitów, jakie trzeba zmienić między dwoma kodami,
- Kod o odległości $\geq k$:
    - wykrywa do k-1 błędów,
    - koryguje do (k-1)/2 błędów.

Kody MAC i HMAC

- **MAC** – wykrywa celowe modyfikacje wiadomości,
- **HMAC** – bezpieczna wersja MAC: h(s#h(s#m)),
- Wykorzystywany w TLS, OpenVPN itp.

Cechy funkcji skrótu

- Jednokierunkowość,
- Trudność znalezienia kolizji,
- Szybkość działania,
- Deterministyczność.

Poufność vs integralność

- **Poufność** – ochrona treści (szyfrowanie),
- **Integralność** – wykrywanie modyfikacji (np. CRC, MAC).

Szyfry monoalfabetyczne

- Proste podstawienie liter (np. Cezara, ROT13),
- Łatwe do złamania analizą częstotliwości.

Typy ataków kryptograficznych

- **Wybrany tekst jawny** – atakujący wybiera tekst,
- **Znany tekst jawny** – zna pary (tekst, szyfrogram),
- **Znany szyfrogram** – zna tylko szyfrogram.

Szyfrowanie one-time pad

- m XOR K, klucz tak długi jak wiadomość,
- Teoretycznie idealne, praktycznie trudne (zarządzanie kluczem).

Szyfrowanie blokowe – ECB vs CBC

- **ECB** – każdy blok szyfrowany niezależnie, identyczne bloki = identyczny szyfrogram,
- **CBC** – każdy blok zależy od poprzedniego, używa IV, bezpieczniejsze.

Wykład 11 - Podstawy kryptografii: Szyfrowanie i Uwierzytelnianie

Różnica między szyfrowaniem symetrycznym a asymetrycznym

- **Symetryczne**: ten sam klucz do szyfrowania i deszyfrowania, efektywne obliczeniowo, ale trudne w dystrybucji klucza.
- **Asymetryczne**: dwa różne klucze – publiczny do szyfrowania, prywatny do deszyfrowania; łatwiejsza dystrybucja kluczy.

Bezpieczeństwo szyfrowania asymetrycznego

- Opiera się na problemach trudnych obliczeniowo (np. rozkład liczby na czynniki).
- Znajomość klucza publicznego nie umożliwia odczytania wiadomości.

Algorytm RSA

1. Wybór dwóch dużych liczb pierwszych `p` i `q`.
2. Obliczenie `n = p * q` i `φ(n) = (p - 1) * (q - 1)`.
3. Wybór `e` względnie pierwszego z `φ(n)`.
4. Obliczenie `d` takiego, że `d * e ≡ 1 (mod φ(n))`.
5. Klucz publiczny: `(e, n)`, prywatny: `(d, p, q)`.
6. Szyfrowanie: `c = m^e mod n`, deszyfrowanie: `m = c^d mod n`.

Różnica: szyfrowanie vs uwierzytelnianie

- **Szyfrowanie** zapewnia poufność.
- **Uwierzytelnianie** zapewnia, że wiadomość pochodzi od deklarowanego nadawcy.

Atak powtórzeniowy

- Adwersarz przechwytuje podpisaną wiadomość i odtwarza ją później.
- Obroną jest użycie losowego wyzwania (nonce).

Klucze w szyfrowaniu asymetrycznym

- **Szyfrowanie**: klucz publiczny odbiorcy.
- **Deszyfrowanie**: klucz prywatny odbiorcy.

Podpisywanie wiadomości

- Tworzy się podpis: `Ea(h(m))`, czyli szyfrowana funkcja skrótu.
- Podpis wykonuje się kluczem **prywatnym**, a weryfikuje kluczem **publicznym**.

Podpisy cyfrowe a uwierzytelnianie

- Podpis potwierdza tożsamość nadawcy (tylko on zna klucz prywatny).
- Weryfikacja podpisu potwierdza autentyczność.

HMAC a podpisy cyfrowe

- HMAC = `h(s # h(s # m))`, używa sekretu znanego obu stronom.
- HMAC nie jest podpisem cyfrowym – nie zapewnia niezaprzeczalności.

Podpisywanie funkcji skrótu vs całej wiadomości

- Lepsze: podpisywać `h(m)` – krótsze, szybsze.
- Ryzyko: kolizje funkcji skrótu → możliwość ataków (np. atak urodzinowy).

Certyfikaty i ścieżka certyfikacji

- **Certyfikat** = powiązanie klucza publicznego z tożsamością, podpisane przez zaufany podmiot.
- **Ścieżka certyfikacji** = ciąg zaufanych podpisów prowadzących do danego certyfikatu.

Urząd certyfikacji (CA)

- Wydaje certyfikaty, jego klucze publiczne są znane i zaufane (wbudowane w przeglądarki).

Bezpieczeństwo TLS

- TLS szyfruje dane i uwierzytelnia strony.
- Używa asymetrycznego szyfrowania do ustanowienia sesji, potem symetrycznego.

Uwierzytelnienie serwera w TLS

- Sprawdzenie certyfikatu podpisanego przez CA.
- Przeglądarka ufa CA, weryfikuje klucz serwera.

Klucze sesji

- Symetryczne klucze generowane przez klienta.
- Wysyłane zaszyfrowane kluczem publicznym serwera.

Kolizje funkcji skrótu

- Dwie różne wiadomości mają ten sam hash.
- Prowadzi do potencjalnych ataków (np. podmiana treści).

Atak urodzinowy

- Łatwiej znaleźć dwie różne wiadomości o tym samym skrócie niż jedną konkretną.
- Wymaga około `2^(n/2)` prób dla n-bitowego skrótu.

Wykład 12 - Bezpieczeństwo sieci

CAM i przepełnienie pamięci CAM

CAM (Content Addressable Memory) to pamięć przełącznika służąca do mapowania adresów MAC na porty. Przepełnienie CAM polega na wysyłaniu wielu ramek z losowymi adresami MAC, co powoduje, że przełącznik przechodzi w tryb „nasłuchu” (jak hub) i przesyła wszystkie ramki do wszystkich portów – umożliwia to podsłuchiwanie.

Atak ARP Spoofing

Atakujący zatruwa pamięć ARP, wysyłając fałszywe odpowiedzi ARP z własnym adresem MAC przypisanym do IP innego hosta. W efekcie ruch sieciowy trafia do atakującego.

IP Spoofing i Ingress Filtering

IP Spoofing polega na fałszowaniu adresu źródłowego IP. Ingress filtering to metoda weryfikacji poprawności pakietów – routery odrzucają pakiety przychodzące z niedozwolonymi adresami źródłowymi (spoza danego zakresu).

RIP Spoofing

Atak polega na rozgłaszaniu fałszywych tras w protokole RIP, który w wersji 1 nie ma uwierzytelniania. Pozwala to przejąć ruch sieciowy.

Zatruwanie cache DNS

Polega na wprowadzeniu fałszywych wpisów do pamięci cache resolvera DNS. Nowoczesne ataki wykorzystują wysyłanie wielu odpowiedzi UDP z różnymi ID, by trafić na prawidłowy identyfikator zapytania.

Uwierzytelnianie serwera SSH

Klient przy pierwszym połączeniu otrzymuje klucz publiczny serwera i może zaakceptować jego odcisk palca (fingerprint). Klucz jest potem zapisywany lokalnie.

Uwierzytelnianie użytkownika w SSH za pomocą RSA

Serwer zna klucz publiczny użytkownika. Użytkownik podpisuje dane kluczem prywatnym, a serwer weryfikuje podpis przy użyciu klucza publicznego.

Tunelowanie – przykłady

- IPv6 przez IPv4
- OpenVPN/WireGuard: pakiety IP przez UDP
- SSH: przekierowanie portów (np. `ssh -L`)

VPN

VPN (Virtual Private Network) to technologia łącząca zaufane sieci przez niezaufany Internet, zapewniająca tunelowanie i szyfrowanie transmisji.

Porównanie filtrów pakietów

- **Proste** – szybkie, tylko nagłówki IP, mało precyzyjne.
- **Stanowe** – uwzględniają stan połączenia TCP.
- **Aplikacyjne** – analizują zawartość pakietów (np. FTP), wolniejsze, dokładniejsze.

Moduły Netfilter/nftables

- **INPUT** – pakiety do lokalnego hosta.
- **OUTPUT** – pakiety wychodzące z lokalnego hosta.
- **FORWARD** – pakiety przechodzące przez host.

NAT – łańcuchy

- **SNAT (źródłowy)** – w `POSTROUTING`.
- **DNAT (docelowy)** – w `PREROUTING`.

Ataki przez brak weryfikacji danych

- **Przepełnienie bufora** – np. `scanf()` do zbyt małej tablicy.
- **Atak ../** – odczyt plików poza katalogiem WWW.
- **SQL injection** – np. `x' OR '1'='1`.
- **Heartbleed** – przesyłanie fragmentów RAM.

Robak internetowy, botnet

- **Robak** – samopowielający się złośliwy kod.
- **Botnet** – sieć komputerów zainfekowanych przez robaka, sterowanych zdalnie.

Phishing

Podszywanie się pod zaufaną stronę, by wyłudzić dane. Może mieć prawidłowy certyfikat HTTPS, ale domenę podobną do oryginału.

Skanowanie portów

Technika wykrywania otwartych portów (np. `nmap`). Pozwala ocenić, jakie usługi są dostępne.

Ataki DoS i DDoS

- **DoS** – blokowanie dostępu do usług (np. zalewanie pakietami ICMP).
- **DDoS** – atak z wielu komputerów (botnetu), trudniejszy do zablokowania.

Atak odbity DoS (reflected)

Fałszowane zapytania do serwerów (np. DNS) z adresem ofiary jako źródłowym. Serwery odpowiadają na adres ofiary, co może ją przeciążyć. Wariantem jest **smurf attack** (ICMP na broadcast).