Notatki z kursu Sieci Komputerowe

Małgorzata Dymek

2018/19, semestr letni

1 Charakterystyka sieci LAN, WAN. Topologie połączeń. Komutacja obwodów vs. komutacja pakietów i komutacja komórek.

- **LAN** - Local Area Network
- **MAN** - Metropolitan Area Network
- **WAN** - Wide Area Network

1.1 Topologia sieci lokalnych

- hierarchiczna
- (rozszerzonej) gwiazdy
- pierścienia
- magistrali

Dwa rodzaje topologii: **fizyczne i logiczne**. Jeżeli przy fizycznej topologii gwiazdy komputer przesyła dane bezpośrednio do komputera docelowego (przełącznik), to mamy logiczną topologię gwiazdy. Jeżeli ramka jest wysyłana do wszystkich dostępnych komputerów (koncentrator), to logicznie jest to topologia magistrali.

Komutacja obwodów - technologia sidn, „wersja cyfrowa telefonii", jak się dzwoniło to się robiło logiczno/fizyczne stałe połączenie trwające tak długo jak trwa rozmowa

Komutacja pakietów - podzielone dane na pakiety, pakiety wysyłane różnymi ścieżkami

2 Model ISO OSI, model TCP/IP.

OSI (Open Systems Interconnection) utworzony przez Międzynarodową Organizację Normalizacyjną stanowi **model referencyjny**.

Nr warstwy OSI	Nazwa warstwy OSI	Nazwa warstwy TCP/IP
7	Aplikacji	Aplikacji
6	Prezentacji	
5	Sesji	
4	Transportu	Transportu
3	Sieci	Intersieci
2	Łącza danych	Interfejsu sieciowego
1	Fizyczna	

- **Warstwa fizyczna** - standard połączenia fizycznego, charakterystyki wydajnościowe nośników. Same media transmisyjne pozostają poza dziedziną jej zainteresowania (czasem określane są terminem warstwa zerowa).

- **Warstwa łącza danych** – grupowanie danych wejściowych (z warstwy fizycznej) w bloki zwane **ramkami** danych („jednostki danych usług warstwy fizycznej"), mechanizmy kontroli poprawności transmisji (FCS).
- **Warstwa sieci** - określenie trasy przesyłania danych między komputerami poza lokalnym segmentem sieci LAN, protokoły trasowane takie jak IP (ze stosu protokołów TCP/IP).
- **Warstwa transportu** - kontrola błędów i przepływu danych poza lokalnymi segmentami LAN, protokoły zapewniające komunikację procesów uruchomionych na odległych komputerach, protokoły TCP, UDP.
- **Warstwa sesji** - zarządzanie przebiegiem komunikacji podczas połączenia między komputerami.
- **Warstwa prezentacji** - kompresja, kodowanie i translacja między niezgodnymi schematami kodowania oraz szyfrowanie.
- **Warstwa aplikacji** - interfejs między aplikacjami a usługami sieci.

2.1 Zestaw (stos) protokołów TCP/IP

Protokoły z zestawu TCP/IP

- warstwa aplikacji: **TELNET, FTP, DNS**
- warstwa transportu: **TCP, UDP**
- warstwa internetowa: **IP - IPv4 i IPv6**
- **ARP** - tłumaczy adresy między warstwą internetową a warstwą interfejsu sieciowego, czasami zaliczany do tej ostatniej,
- **ICMP** - m.in. komunikaty o problemach,
- **IGMP** - komunikacja grupowa.

Dane przechodząc w dół stosu protokołów TCP/IP są opakowywane i otrzymują odpowiedni nagłówek. Porcje danych przesyłane w dół stosu mają różne nazwy:

- **Komunikat** - porcja danych utworzona w warstwie aplikacji i przesłana do warstwy transportu.
- **Segment** - porcja danych utworzona przez oprogramowanie implementujące protokół TCP w warstwie transportu. Zawiera w sobie komunikat.
- **Datagram UDP** - porcja danych utworzona przez oprogramowanie implementujące protokół UDP w warstwie transportu.
- **Datagram** - również porcja danych utworzona w warstwie internetowej przez oprogramowanie implementujące protokół IP. Datagram IP zawiera w sobie segment, bywa nazywany pakietem.
- **Ramka** - porcja danych utworzona na poziomie dostępu do sieci.

Sekwencja zdarzeń przy wysłaniu danych:

- Aplikacja przesyła dane do warstwy transportu.
- Dalszy dostęp do sieci realizowany jest przez TCP albo UDP.
- Segment lub datagram UDP przesyłany jest do warstwy IP, gdzie protokół IP dołącza między innymi informacje o adresach IP źródła i celu tworząc datagram IP (pakiet).
- Datagram z IP przechodzi do warstwy interfejsu sieciowego, gdzie tworzone są ramki. W sieci LAN ramki zawierają adres fizyczny (przypisany do karty sieciowej) otrzymany zprotokołu ARP.
- Ramka przekształcana jest w ciąg sygnałów, który zostaje przesłany przez sieć.

3 Standaryzacja w sieciach komputerowych, co to są dokumenty RFC.

Instytucje: ISO, IEEE, IANA podinstytucja ICANN, IAB.

Dokumenty RFC (Request for Comments) są produkowane przez IAB (International Standards Organization). Są standardami lub pełnią funkcję informacyjną. RFC stałe, zmiany jako kolejne RFC, numery niezmienne.

IEEE 802.3 - Ethernet, 802.11 - WiFi, 802.1q - VLAN

ISO - zrzesza narodowe instytucje standaryzujące i wypuszcza swoje standardy.

4 Ethernet: sposób dostępu do nośnika, ramki.

Preambuła	src MAC	dst MAC	Typ danych	46-1500 Dane	CRC
żeby się karty sieciowe zsynchronizowały				tu jest pakiet IP i segment TCP	suma kontrolna
warstwa 1	warstwa 2				

4.1 Dostęp do nośnika

Dla Ethernet I: Dostęp do nośnika realizowany był na zasadzie **CSMA** (Carrier Sense, Multiple Access – wielodostęp do nośnika z badaniem stanu nośnika).

Dla Ethernet II: Dostęp do nośnika realizowany był na zasadzie **CSMA/CD** (Carrier Sense, Multiple Access with Collision Detection – wielodostęp do nośnika z badaniem stanu oraz wykrywaniem kolizji). Teraz już nie ma problemu z kolizjami, bo mamy switche.

Kabel cross, jak łączymy bez switcha dwa urządzenia. Kabel prosty, jak jest switch Teraz sobie urządzenia wykrywają czy są dobrze połączone i same korygują żeby było ok.

5 Ethernet: działanie przełączników i koncentratorów (podstawy).

Koncentrator (Hub) - rozsyła dane do wszystkie połączeń które ma (więc można podsłuchiwać, są kolizje, zbędny ruch).

Przełącznik (Switch) - uczy się co jest na którym porcie i przesyła dane tam gdzie mają iść (chyba że nie wie, to wszystkie).

6 Protokół IPv4: adresacja, pola w nagłówku, fragmentacja.

Adres IP jest przypisywany do karty sieciowej, nie do komputera.

Są **trzy typy adresów IPv4**:

- **Adresy jednostkowe** (unicast) – pojedynczy interfejs sieciowy (komunikacja one-to-one).
- **Adresy rozgłoszeniowe** (broadcast) – wszystkie węzły w tym samym segmencie sieci (one-to-everyone).
- **Adresy grupowe** (multicast) – jeden lub wiele komputerów w jednej lub w różnych segmentach sieci (one-to-many).

W **adresie IP** zapisanym binarnie można wyróżnić **dwie części**:

- **Identyfikator sieci** (Network ID) - pewna liczba bitów z lewej strony adresu
- **Identyfikator hosta** (Host ID) - pozostałe bity.

Granica między identyfikatorem sieci a identyfikatorem hosta może być wyznaczona przez tzw. **maskę sieci**.

Adres IP, który zawiera **same zera** w części hosta jest traktowany jako **adres sieci**. **Adresy rozgłoszenia do sieci lub podsieci mają jedynki tylko w części hosta**.

Adres ograniczonego rozgłoszenia - 255.255.255.255- adres rozgłoszenia w danym segmencie sieci ograniczonym routerami.

6.1 Adresowanie oparte na klasach

Pierwszy bajt adresu determinuje do jakiej klasy należy sieć.

Klasa	Adres sieci	Adresy	Zakres 1-go bajtu	Najstarsze bity
A	w.0.0.0	1.0.0.0 - 126.0.0.0	1 – 126	0
B	w.x.0.0	128.0.0.0 - 191.255.0.0	128 – 191	10
C	w.x.y.0	192.0.0.0 - 223.255.255.0	192 – 223	110
D	nie dotyczy	nie dotyczy	224 – 239	1110
E	nie dotyczy	nie dotyczy	240 – 255	11110

Klasa	Ilość sieci	Komp. w sieci	ID sieci	ID hosta	"pierwszy"	"ostatni"
A	126	$2^{24} - 2$	1 bajt	3 bajty	w.0.0.1	w.255.255.254
B	$(191 - 128 + 1) * 256$	$2^{16} - 2 = 65534$	2 bajty	2 bajty	w.x.0.1	w.x.255.254
C	$(192 - 223 + 1) * 256 * 256$	$2^8 - 2 = 254$	3 bajty	1 bajt	w.x.z.1	w.x.z.254

- **Adresy klasy D** - przeznaczone są do transmisji grupowych.
- **Adresy klasy E** - zarezerwowane (nie wykorzystywane normalnie do transmisji pakietów).
- **Adresy pętli zwrotnej** (loopback) - postaci 127.x.y.z (na ogół 127.0.0.1). Cały ruch przesyłany na ten adres nie wychodzi z komputera.

6.2 Adresowanie bezklasowe

Dzielenie na podsieci z **użyciem dowolnej liczby jedynek**. Do określenia sieci należy podać adres sieci oraz maskę. Obecnie w Internecie powszechnie jest wykorzystywane adresowanie bezklasowe.

- Protokół **warstwy trzeciej** modelu ISO OSI.
- Oprogramowanie implementujące protokół IP jest odpowiedzialne za:
  - **adresowanie** IP,
  - **tworzenie datagramów** IP (pakietów)
  - uczestniczenie w **kierowaniu ich** w sieci z punktu początkowego do punktu docelowego.
- Realizuje usługę **zawodną**. Jeśli komunikacja powinna zawierać mechanizmy niezawodności, to muszą one być dostarczone przez protokoły warstwy wyższej.
- Datagram IP składa się z nagłówka (header) i bloku danych (payload).
  - **Nagłówek** dzięki informacjom w nim zawartym umożliwia obsługę routowania, identyfikację bloku danych, określenie rozmiaru nagłówka i datagramu oraz obsługę fragmentacji. W nagłówku mogą się znaleźć również tzw. opcje rozszerzające.
  - **Blok danych**.

6.3 Nagłówek IPv4

- **Wersja** (4 bity) (=0100)
- **Długość nagłówka IP** (IHL – Internet Header Length)
- **Typ usługi**: TOS (Type of Service) lub DS. (Differentiaded Services)
  Flagi:
  - małe opóźnienie
  - duża przepustowość
  - niezawodność
  - Bits 0-5: DCSP (priorytet + flagi)
  - Bits 6-7: ECN

  ECN jest rozszerzeniem protokołów IP oraz TCP. Umożliwia powiadamianie punktów końcowych IP/TCP o nadchodzącym zatorze bez usuwania pakietów, poprzez ustawienie warość 11 na bitach ECN. Jest opcjonalny.
- **Długość całkowita** - na podstawie tego pola oraz pola Długość nagłówka można określić wielkość bloku danych oraz początek tego bloku.
- **Identyfikator** kolejnych datagramów. Wartość jest wpisywana przez host nadający i dla kolejnych datagramów jest zwiększana.
- **Flagi** - 3 bity tworzące dwie flagi używane przy fragmentacji datagramów.
- **Przesunięcie fragmentu**
- **Czas życia** (TTL)
- **Protokół** - ICMP, UDP, TCP.
- **Suma kontrolna nagłówka**
- **Adres IP źródła**
- **Adres IP docelowy**
- **Dodatkowe opcje i wypełnienie** Opcje mogą zająć maksymalnie 40 bajtów i mogą zawierać m.in.:
  - zapis trasy przez którą przeszedł datagram
  - zapis czasu – timestamp - trasa, czas przejścia.
  - routowanie źrodłowe
    Normalnie to routery wybierają dynamicznie trasę datagramów. Można jednak określić trasę datagramu w opcjach nagłówka IP.
    * dokładne – wysyłający komputer określa dokładną trasę, jaką musi przejść datagram. Jeśli kolejne routery na tej trasie są przedzielone jakimś innym routerem, to wysyła komunikat ICMP „source route failed" i datagram jest odrzucany.
    * swobodne – wysyłający określa listę adresów IP, przez jakie musi przejść datagram, ale datagram może przechodzić również przez inne routery.

Za nagłówkiem IP w datagramie znajdują się dane (segment TCP, datagram UDP, komunikat ICMP).

6.4 Fragmentacja datagramów IPv4

MTU (Maximum Transmission Unit) to największa porcja danych, jaka może być przesłana w ramce przez pewną sieć przy wykorzystaniu konkretnej technologii. Jeśli datagram IP jest większy niż wynika to z MTU dla warstwy łącza, to IP dokonuje **fragmentacji**. Najmniejsze MTU po drodze przejścia

datagramu nazywa się **ścieżką MTU**. Fragmenty też mogą być dalej dzielone, stają się samodzielnymi pakietami.

Pole identyfikator w nagłówku IP zawiera numer wysłanego pakietu. Pole powinno być inicjowane przez protokół warstwy wyższej. Warstwa IP zwiększa identyfikator o 1 dla kolejnych pakietów.

Jeśli flaga jest ustawiona na Don't Fragment to znaczy, że pakiet nie może być dzielony. W przypadku konieczności dzielenia jest odrzucany i do nadawcy wysyłany jest komunikat ICMP (typ 3 z polem kod = 4).

Jeśli zgubiony zostanie chociaż jeden fragment, wówczas cały wyjściowy pakiet jest odrzucony, więc fragmentacja jest niekorzystna. Do tego może ona bardzo obciążać routery.

7 Multiemisja (multicast) w IPv4 (IGMP, IGMP-snooping, współpraca technologii Ethernet z multiemisją – adresy MAC multiemisji).

Multicast – transmisja grupowa, multiemisja.

- Wysłanie jednego pakietu ze źródła **do wielu miejsc docelowych**. Pakiety są kopiowane w routerach i przełącznikach warstwy drugiej.
- Mniejsze obciążenie sieci, większa **skalowalność** w stosunku do unicastu.
- Schematy jeden-do-wielu, wiele-do-wielu.
- Komunikaty w większości protokołów routowania mają zarezerwowane adresy multiemisji.
- Aby uczestniczyć w transmisji grupowej, komputer musi sprawdzać określone adresy w przychodzących pakietach (IP) i generalnie w ramkach (MAC).
- Transmisja grupowa odbywa się z wykorzystaniem różnych mechanizmów i protokołów.

7.1 IGMP - Internet Group Management Protocol

- wykorzystywany do **dynamicznego** rejestrowania/wyrejestrowania odbiornika w routerze
- komunikaty IGMP są przesyłane w pakietach IP z adresem docelowym typu multicast i ustawioną wartością TTL na 1.

7.1.1 IGMPv1

Są **dwa** typy komunikatów:

- **Membership query**, wysyłany okresowo (co kilkadziesiąt sekund) przez routery na wszystkiue komputery.
- **Membership report** służy do zgłoszenia się jako odbiorca pakietów wysyłanych na ten adres; wysyłany jest też w odpowiedzi na membership query.

Host po otrzymaniu membership query czeka pewien pseudolosowy czas i wysyła membership report. Jeśli w tym pseudolosowym czasie host usłyszy membership report od innego hosta, to nie wysyła swojego raportu.

W IGMPv1 **host „po cichu" opuszcza grupę**. Jeśli router nie dostanie raportu w odpowiedzi na **trzy kolejne** membership query, router usuwa grupę z tablicy multicastu i przestaje przesyłać pakiety kierowane do tej grupy.

7.1.2 IGMPv2

W IGMPv2 są **cztery** typy komunikatów:

- **Membership query**
- **Version 1 membership report**
- **Version 2 membership report**
- **Leave group**

Ważne zmiany w porównaniu do wersji pierwszej:

- Membership query może być typu **group-specific query**.
- Leave group message – **komunikat o opuszczeniu grupy**, wysyłany jest na adres 224.0.0.2 (wszystkie routery multicast na łączu).
- Dodano do zapytań IGMP określenie czasu **query-interval response time**, jaki mają uczestnicy na wysłanie raportu, czas ten jest określany przez wysyłającego zapytanie.
- Dodano mechanizm wyboru routera odpytującego (**querier**) w segmencie sieci wykorzystującej wielodostęp. Zostaje nim router, którego adres IP jest najmniejszą liczbą.

7.1.3 IGMPv3

Dodano możliwość zgłaszania się do grup z **wyspecyfikowaniem adresu jednostkowego** IPv4 pewnego nadawcy.

7.2 Transmisje grupowe a technologie sieci lokalnych

Ethernet daje możliwość adresowania **MAC typu multicast**. Wykorzystywane są adresy z zakresu 01:00:5e:00:00:00 do 01:00:5e:7f:ff:ff. **23 bity adresu IPv4 są wprost wykorzystane w adresie MAC**.

Zatem każdy adres Ethernet multicast jest związany z 32 adresami IPv4 z klasy D (różniącymi się na 5 bitach).

Przykłady 239.20.20.20 odpowiada adresowi MAC: $01-00-5e-14-14-14$.
239.10.10.10 odpowiada adresowi MAC: $01-00-5e-0a-0a-0a$.

IGMP Snooping
IGMP snooping polega na tym, że **przełącznik warstwy drugiej „słucha"** konwersacji między hostami a routerami i analizuje pakiety z komunikatami IGMP (raporty członkostwa w grupie membership reports oraz zgłoszenia opuszczenia grupy – membership leaves). Na podstawie śledzonych komunikatów IGMP przełącznik **aktualizuje swoją tablicę** przypisania adresów MAC do portów i uwzględnia adresy Ethernet multicast. To rozwiązanie wymaga jednak odpowiednio wydajnych przełączników.

Protokół CGMP
Switch "słucha" konwersacji między hostami a routerami i analizuje pakiety z IGMP, na tej podstawie aktualizuje tablicę MAC portów i wysyła do komputerów to co chcą słuchać

8 Protokół ARP.

ARP (Address Resolution Protocol) stosowany jest w sieciach Ethernet z IPv4, był też używany w sieciach Token Ring. W wersji IPv6 protokół ARP nie jest w ogóle wykorzystywany, zastępują go inne mechanizmy.

Ramka ARP

- **Typ sprzętu** (2 oktety)

- **Typ protokołu** (2 oktety)
- **Długość adresu sprzętu** (1 oktet)
- **Długość adresu protokołu** (1 oktet)
- **Kod operacji** (2 oktety)
- **Adres sprzętu nadawcy** (dla Ethernet 6 oktetów)
- **Adres protokołu nadawcy** (dla IPv4 4 oktety)

8.0.1 Wykrywanie zduplikowanych adresów IP

Tzw **"zbędny ARP"**

- Węzeł wysyła ARP Request z **zapytaniem o swój własny adres**.
  - Jeśli ARP Reply **nie nadejdzie** to znaczy, że w lokalnym segmencie **nie ma konfliktu** adresów.
  - Jeśli odpowiedź nadejdzie, oznacza to konflikt.
- Węzeł już skonfigurowany traktowany jest jako węzeł z poprawnym adresem (**węzeł zgodny**), węzeł wysyłający „zbędny ARP" jest **węzłem konfliktowym**.
- **Węzeł konfliktowy wprowadza błąd** w pamięci podręcznej ARP komputerów w **całym segmencie** sieci. ARP Reply z węzła zgodnego nie naprawia sytuacji (ramka ARP Reply nie jest ramką rozgłoszeniową).

8.0.2 Proxy ARP

Router ze skonfigurowanym mechanizmem Proxy ARP **odpowiada na ramki ARP Request w imieniu wszystkich** węzłów – komputerów spoza segmentu sieci lokalnej. Może być używany jest np. w sytuacji, gdy komputery w sieci nie mają ustawionego domyślnego routera. Routery mogą mieć włączoną standardowo opcję Proxy ARP, wówczas jeśli jakiś komputer wyśle ARP Request z adresem spoza danej sieci lokalnej (zwykle to nie następuje), to router odpowie „w imieniu" komputera zewnętrznego.

8.0.3 Komunikacja między komputerami

Komputer źródłowy K1 (IP1, MAC1), docelowy K2 (IP2, MAC2, WW2).

Jeżeli na K1 ktoś spróbuje otworzyć WWW2, to:

- Zadziała system DNS: K1 skontaktuje się ze swoim serwerem DNS i zapyta jaki jest adres IP komputera związanego z nazwą domenową WW2. Serwer DNS znajdzie odpowiedni adres w swoich zasobach i odeśle informację do K1.
- Przeglądarka utworzy komunikat (wg protokołu HTTP). Do komunikatu zostanie dodany nagłówek (wg protokołu TCP), który zawiera m.in. port docelowy (standardowo 80) oraz port źródłowy. Komunikat razem z dołączonym nagłówkiem TCP nazywa się **segmentem TCP**.
- Do segmentu TCP zostanie dodany nagłówek IP – w ten sposób powstanie **pakiet IP**.
- Pakiet musi być przesłany w ramce. Do pakietu musi zostać dodany nagłówek ramki, zawierający źródłowy i docelowy adres MAC. **K1 nie zna adresu MAC2**. Zna tylko IP2. Wykorzystywany jest **protokół ARP**.
  - K1 wysyła **ARP Request** (ta NIE zawiera pakietu IP), która ma adres rozgłoszeniowy jako adres docelowy.
  - Każdy komputer przyłączony do przełącznika ma obowiązek odebrać ramkę wysłaną na adres rozgłoszeniowy MAC. Jednak tylko komputer o zadanym IP odpowie na ARP Request.
  - Odpowiedź **ARP Reply** jest wysyłana na adres MAC komputera 1.

- Po tym, jak K1 pozna adres MAC2 może już zbudować ramkę przeznaczoną do K2. Ramka jest wysyłana do przełącznika, a przełącznik dostarcza ją tylko do K2.
- K2 odbiera ramkę, sprawdza adres MAC docelowy i sumę kontrolną, po czym „wyjmuje" z ramki pakiet IP. Sprawdza adres docelowy IP i „wyjmuje" z pakietu segment TCP. Sprawdza do którego portu należy przekazać zawartość (komunikat HTTP) i ostatecznie „wyjmuje" komunikat http z segmentu i przekazuje do portu 80, na którym nasłuchuje serwer WWW.
- Serwer WWW konstruuje odpowiedź – stronę WWW. Strona ta zostanie umieszczona w komunikacie http, który następnie musi być przesłany do K1. Mechanizm jest analogiczny jak poprzednio.

Nagłówek ramki (numery MAC)	**Nagłówek IP** (numery IP) 20 bajtów	**Nagłówek TCP** (numery portów) 20 bajtów	**Komunikat HTTP**	**Suma kontrolna** 4 bajty

W przypadku komunikacji między komputerami rozdzielonymi przynajmniej jednym routerem ramka wysyłana jest do bramy domyślnej (ARP na bramę), gdzie jest niszczona i nowa jest przekazywana dalej wg tego co w nagłówku pakietu IP.

9 Protokół ICMP.

ICMP (Internet Control Message Protocol)

- **raportowanie routingu**,
- dostarczanie informacji o **błędach** podczas przesyłania ze źródła do komputera docelowego,
- dostarczanie funkcji sprawdzających możliwość komunikacji komputerów wykorzystaniem protokołu IP,
- pomoc w automatycznej konfiguracji hostów.

Komunikaty ICMP wysyłane są **w pakietach IP**. W efekcie w ramce znajduje się nagłówek IP, nagłówek ICMP oraz dane komunikatu ICMP.

Struktura komunikatu ICMP

- **Typ** (1 oktet)
- **Kod** (1 oktet)
- **Suma kontrolna** (2 oktety)
- **Dane charakterystyczne dla typu** (różna długość)

Typy komunikatów ICMP

0	Odpowiedź echa (echo reply)
3	Miejsce docelowe nieosiągalne (destination unreachable)
4	Tłumienie źródła (source quench)
5	Przekierowanie (redirect)
8	Żądanie echa (echo request)
9	Ogłoszenie routera (router advertisement)
10	Wybór routera (router selection)
11	Przekroczenie czasu (time exceeded)
12	Problem parametru (parameter problem)

Żądanie i odpowiedź echa
Cel – wysłanie prostego komunikatu do węzła IP i odebranie echa tego komunikatu. Bardzo użyteczne przy usuwaniu problemów i naprawianiu sieci. Narzędzia takie jak ping oraz tracert i traceroute używają tych komunikatów ICMP do uzyskania informacji o dostępności węzła docelowego.

9.1 Komunikaty ICMP o przekierowaniu

Komunikaty ICMP o przekierowaniu pozwalają hostom TCP/IP na konfigurację tylko jednego routera – bramy domyślnej nawet w sytuacji, gdy w sieci lokalnej są dwa lub więcej routerów, które są odpowiedzialne za pewne miejsca docelowe. Hosty mogą zacząć pracę z jedną domyślną trasą i uczyć się topologii sieci (w szczególności informacji o routowaniu) poprzez otrzymywanie komunikatów ICMP.

Komunikaty ICMP o przekierowaniu powinny być generowane przez routery, ale korzystać z nich mogą tylko hosty. Jeśli datagram IP zostanie celowo usuwanięty przez router, to może być wysłany odpowiedni komunikat protokołu ICMP do nadawcy.

10 Protokół UDP: charakterystyka, nagłówek.

UDP – User Datagram Protocol

- Prosty protokół bezpołączeniowy warstwy transportu.
- Umożliwia przesyłanie danych między procesami dzięki określeniu **adresów IP** komputerów oraz 16 bitowych **numerów portów**.
- Porcja danych zgodna z protokołem UDP nazywana jest **datagramem/pakietem UDP**.
- **Nie zapewnia niezawodności**. Ewentualne zapewnienie niezawodności musi być realizowane przez protokoły warstwy aplikacji.
- Niewielki nagłówek (8 bajtów), nie zawiera mechanizmów ustanawiania połączenia ani sterowania przepływem datagramów, zatem jest szybszy od TCP.
- Datagramy UDP mogą być przesyłane w pakietach IP z adresem docelowym przesyłania grupowego.
- Przykłady zastosowań: strumieniowanie audio/wideo, **wideokonferencje, transmisje głosu; RIP** (port 520).

Aplikacja jest odpowiedzialna za rozmiar wysyłanego datagramu. Jeśli wielkość przekroczy MTU sieci, wówczas datagram IP (zawierający w sobie datagram UDP) jest dzielony (następuje fragmentacja IP).

10.0.1 Enkapsulacja datagramu UDP

nagłówek IP	nagłówek UDP	dane UDP
20 bajtów	8 bajtów	...

Nagłówek UDP

- **Numer portu źródłowego** (16 bitów)
- **Numer portu docelowego** (16 bitów)
- **Długość UDP (nagłówek + dane) – wypełniana opcjonalnie** (16 bitów)
- **Suma kontrolna UDP** (16 bitów) - jedyny mechanizm sprawdzenia nieuszkodzenia datagramu. Opcjonalna w IPv4, obowiązkowa w IPv6.
- **Dane, jeśli są.**

11 Protokół TCP: charakterystyka, mechanizmy, nagłówek.

11.1 TCP – Transmission Control Protocol

Ilość bajtów danych przesyłanych w jednym segmencie nie powinna być większa niż ustalony MSS (**Maximum Segment Size**).

Cechy TCP

- Partnerzy (procesy) tworzą połączenie z wykorzystaniem **mechanizmu trójfazowego uzgodnienia**.
- **Zamknięcie** połączenia odbywa się z wykorzystaniem **mechanizmu uzgodnienia** (zgoda na zamknięcie).
- TCP zapewnia **sterowanie przepływem**. Informuje partnera o tym ile bajtów danych ze strumienia danych może od niego przyjąć (**okno oferowane**). Rozmiar okna zmienia się **dynamicznie** i jest równy rozmiarowi wolnego miejsca w buforze odbiorcy.
- Dane ze strumienia danych dzielone są na fragmenty, które według TCP mają najlepszy do przesłania rozmiar. Jednostka przesyłania danych nazywa się **segmentem**.
- TCP zapewnia **niezawodność** połączenia.

Mechanizmy niezawodności

- **Potwierdzanie otrzymania segmentów z mechanizmem zegara.**
  Odebrany segment musi być potwierdzony przez odbiorcę przez wysłanie segmentu potwierdzającego. Jeśli potwierdzenie nie nadejdzie w odpowiednim czasie, segment zostanie przesłany powtórnie.
- **Sumy kontrolne.**
  Jeśli segment zostanie nadesłany z niepoprawna sumą kontrolną, to jest odrzucany. Nadawca po odczekaniu odpowiedniego czasu prześle segment jeszcze raz.
- **Przywracanie kolejności nadchodzących segmentów.**
  Segmenty mogą nadchodzić w kolejności innej niż zostały wysłane, oprogramowanie TCP przywraca prawidłową kolejność przed przekazaniem do aplikacji.
- **Odrzucanie zdublowanych danych.**

11.1.1 Nagłówek TCP

- **Numer sekwencji.**
- **Długość nagłówka** (przesunięcie danych).
- **Jednobitowe znaczniki** (flagi):
- **Rozmiar okna** - liczba bajtów, które odbiorca może zaakceptować.
- **Suma kontrolna.**
- **Wskaźnik ważności.**
- **Opcje** - rodzaj opcji (bajt), długość opcji (bajt), opcja. Najważniejsza opcja to **MSS**. Może być uzyskana jako **MTU minus rozmiar nagłówka IP oraz TCP**.

Specyfika stanu TIME WAIT
Spóźnione segmenty są w czasie 2 MSL odrzucane. Para punktów końcowych definiujących połączenie nie może być powtórnie użyta przed upływem 2MSL. Eliminuje to ewentualne kłopoty związane z odbieraniem z sieci segmentów jeszcze ze starego połączenia.

Półzamknięcie TCP
Strona, która zakończyła połączenie i nie nadaje danych, może dane odbierać od partnera TCP. Takie połączenie nazywane jest połączeniem półzamkniętym (half-closed).

Segmenty RST
Segment RST wysyłany jest przez oprogramowanie implementujące TCP, kiedy nadchodzi segment niepoprawny z punktu widzenia dowolnego połączenia. Segment RST nie jest potwierdzany. W protokole UDP generowany jest komunikat ICMP o tym, że port jest nieosiągalny. Segment RST jest wysyłany również wtedy, gdy przekroczona jest maksymalna dopuszczalna liczba połączeń TCP.

Połączenia półotwarte (połowicznie otwarte)
Jest to połączenie nie poprawnie nawiązane. Występuje, jeśli jedna ze stron przerwała połączenie bez

informowania drugiej. Segment z ustawioną na 1 flagą SYN został przesłany od klienta do serwera, serwer odpowiedział segmentem z ustawionymi na 1 flagami SYN i ACK, ale klient nie odpowiedział segmentem z ustawioną na 1 flagą ACK.

11.1.2 Przepływ danych w TCP

Potwierdzenia

- **Skumulowane potwierdzanie** - wysyłamy dużo segmentów, oczekujemy jednego skumulowanego potwierdzenia.
- **Opóźnione potwierdzenia** - serwer może wysłać potwierdzenie z opóźnieniem.
- **Selektywne potwierdzenia** - selektywnie potwierdzamy co dostaliśmy [przedziały], więc jeśli zginęło tylko kilka datagramów, to można retransmitować tylko je a nie całość.

Ruchome okna TCP (sliding windows)
Połączenie TCP obejmuje dwa strumienie danych. W każdym strumieniu określony jest nadawca i odbiorca. Kontrolę przesyłania oktetów w strumieniu umożliwiają mechanizmy tzw. **przesuwnych okien**, które można sobie wyobrazić jako nałożone na strumień. Dla strumienia określone jest **okno nadawcy** oraz **okno odbiorcy**. Nadawca może wysyłać tylko te dane, które są w tej chwili w jego oknie nadawczym, przy czym może to zrobić tylko za zgodą odbiorcy. Okno nadawcze jest przesuwane nad wyjściowym strumieniem bajtów, okno odbiorcze nad strumieniem wejściowym.

11.1.3 Przesyłanie małych segmentów

Tak określa się segmenty o rozmiarze mniejszym od MSS.

- **Algorytm Nagle'a**
  Małe niepotwierdzone segmenty są gromadzone w buforze, wysyłane razem. Algorytm Nagle'a może być wyłączany przez oprogramowanie TCP.
- **Syndrom głupiego okna** (SWS)
  - Jeśli odbiorca ma **zerowy rozmiar okna** (i nadawca też) oraz warstwa aplikacji pobierze 1 bajt, to okno odbiorcze otwiera się o jeden bajt.
  - Nadawca unika SWS **wstrzymując się** z wysyłaniem danych dopóki rozmiar okna proponowanego przez odbiorcę nie jest równy **co najmniej MSS**.

Dodatkowa kontrola przepływu po stronie nadawcy

- **Algorytm powolnego startu**
  Po otwarciu połączenia lub dłuższym czasie nie przesyłania danych wielkość okna przeciążeniowego ustawiana jest na 2*MSS. Każde przychodzące potwierdzenie (ACK) powoduje zwiększenie okna przeciążeniowego o jeden MSS. Może to prowadzić do wykładniczego wzrostu wielkości tego okna.
- **Algortym unikania zatoru**
  Tu stosuje się wolniejszy wzrost wielkości okna przeciążeniowego, np. o jeden segment na kilka przychodzących ACK. Algorytm ten działa zwykle od pewnego progu (najpierw działa powolny start).

11.1.4 Retransmisje segmentów w TCP

W każdym połączeniu definiowana jest zmienna **RTO (Retransmission Time-out)**. Jeśli TCP nie odbierze ACK w czasie RTO dla pewnego nadanego segmentu, to segment musi być retransmitowany.

12 Protokoły routowania typu wektor odległości: sposób działania, wady i zalety, podstawowe parametry protokołów RIP, RIP2, IGRP, EIGRP. (M.in. pętle routowania, zliczanie do nieskończoności, dzielony horyzont, zegary).

Protokoły routowania wektora odległości - oparte na **algorytmie Bellmana Forda** obliczania najkrótszych ścieżek w grafie, "odległości od sieci".

System autonomiczny - to zbiór prefiksów (adresów sieci IP) pod **wspólną administracyjną kontrolą**, w którym utrzymywany jest spójny schemat trasowania

12.1 Niekorzystne zjawiska związane z routowaniem wg protokołów wektora odległości

- **Pętle routowania.**
- **Efekt odbijania.**
- **Zliczanie do nieskończoności.**

Taktyki rozwiązania:

- **Dzielony horyzont (split horizon)**
  - **Do łącza nie zostanie przekazana informacja o trasach wiodących przez to łącze**.
  - Dzielony horyzont nie zawsze, ale zazwyczaj likwiduje **pętle routowania**.
- **Split horizon with poison reverse**
  Informacja odwrotna(reverse) jest przekazywana, jednak z metryką nieskończoną.
- **Natychmiastowe/wymuszane aktualizacje (triggered updates)**
  - W przypadku zmiany metryki trasy **musi nastąpić rozgłoszenie bez względu na okres rozgłoszeń** charakterystyczny dla danego protokołu.
  - Powoduje to **szybszą zbieżność** i częściowo zapobiega **pętlom routowania**.
- **Zegary hold-down (hold-down timers)**
  - Router po otrzymaniu od sąsiada informacji o dezaktualizacji trasy włącza **specjalny zegar** (hold-down timer).
  - Jeśli przed upływem czasu progowego nastąpi:
    * **aktualizacja od tego samego sąsiada** na trasę aktywną, to **trasa** jest zaznaczana jako **aktywna**.
    * router dostanie **od innego routera informację** o trasie do rozważanego miejsca docelowego z **metryką mniejszą bądź równą** tej zdezaktualizowanej, wówczas następuje **wpis zgłoszonej trasy**.
    * router dostanie **od innego routera informację** o trasie do rozważanego miejsca docelowego z **metryką większą** od tej zdezaktualizowanej, taka trasa **nie jest brana pod uwagę**.
- **Zatruwanie tras**
  Przekazywanie informacji o trasach niedostępnych, przyspiesza uzyskanie zbieżności.

12.2 Protokół RIP

- Metryką w RIP jest **liczba skoków** do celu. Metryka 16 oznacza nieskończoność.
- Wysyła **cały wektor** odległości.
- Można ustawić trasę domyślną (adres 0.0.0.0).
- **Autosumaryzacja, system klasowy** adresacji ip.
- **Cztery zegary, liczniki** (timers, counters):
  - **Update timer** (30s.) – po przesłaniu wektora odległości zegar jest zerowany. Po osiągnięciu 30 s. wysyłany jest następny wektor.
  - **Invalid timer** (180s.) – za każdym razem jak router dostaje uaktualnienie pewnej trasy zegar ten dla trasy jest zerowany. Po osiągnięciu wartości progowej trasa jest zaznaczana jako niepoprawna, ale pakiety jeszcze są kierowane tą trasą.
  - **Hold-down timer** (180s.) – po przekroczeniu wartości progowej przez invalid timer trasa jest ustawiana w stan hold-down. Trasa jest ustawiana w stan holddown również gdy router dostanie informację o tym, że sieć jest nieosiągalna (i nie ma innej, osiągalnej trasy).
  - **Flush-timer** (240s.) – zegar dla trasy jest zerowany po otrzymaniu informacji o trasie. Po osiągnięciu czasu progowego trasa jest usuwana nawet, jeśli trasa jest jeszcze w stanie hold-down.
- **Zalety RIP**
  - **prostota** - procesor nie jest nadmiernie obciążony aktualizacją tablicy routowania i innymi działaniami,
  - **łatwość** konfiguracji.
- **Wady RIP**
  - **wolne** rozprzestrzenianie się informacji o zmianach w topologii sieci (wolna zbieżność),
  - stosunkowo częste (co 30s.) przesyłanie dużych porcji informacji w komunikatach RIP, co **obciąża** sieć.
  - Wadą RIPv1 jest to, że nie daje możliwości przesyłania masek.

12.3 RIPv2

- RIPv2 przekazuje maski podsieci, można stosować sieci **bezklasowe** i podsieci o zmiennym rozmiarze.
- Umożliwia prostą **autentykację** (przez hasła).
- Przekazuje adresy następnego skoku w komunikatach.
- Część wad RIP pozostała: 16 jako metryka oznaczająca nieskończoność, brak alternatywnych tras.
- Rozgłaszanie przez **multicast**.

12.4 Protokół IGRP

- **numer AS** taki sam we wszystkich routerach na danym obszarze z komunikacją IGRP
- obsługuje **adresy klasowe**,
- metryka 24-bitowa w IGRP jest tworzona na podstawie wartości metryk cząstkowych oraz zmiennych określających wagę każdej użytej metryki.
  - **Szerokość pasma** (bandwidth); oznacza liczbę bitów, jakie może transmitować w jednostce czasu dana technologia.

- **Opóźnienie** (delay) – czas wędrówki pakietu od źródła do celu.
- **Obciążenie** (load).
- **Niezawodność** (reliability); wartość liczona jest jako swoisty „procent" pakietów, które dotarły do następnego routera.

$metric = (K_1 * bandwidth + \frac{(K_2 * bandwidth)}{(256 - load)} + K_3 * delay) * \frac{K_5}{(reliability + K_4)}$ Standardowo $K_1 == K_3 == 1, K_2 == K_4 == K_5 == 0$.

- przesyłane są również wartości **MTU** – najmniejsze MTU na trasie do sieci oraz liczba skoków
- przechowywanych jest **kilka optymalnych tras** do pewnego miejsca docelowego, mogą być przechowywane informacje o trasach nieoptymalnych
- **NIE ma trasy domyślnej 0.0.0.0**. Są trasy zewnętrzne, przez tzw. '**router of last resort**' wybierane jeśli nie znaleziono żadnej innej.

12.5 Protokół EIGRP

- obsługuje **adresowanie bezklasowe**,
- **numer AS**, taki sam w komunikujących się routerach
- **IGRP i EIGRP mogą ze sobą współpracować**, jeśli mają ten sam numer; nastąpi przeliczenie metryki; trasa z IGRP jest traktowana jak trasa zewnętrzna
- metryka 32 bitowa; aktualizacje zawierają liczbę skoków dla trasy, jednak liczba skoków nie jest brana pod uwagę przy wyliczaniu metryki

Kluczowe technologie i idee wykorzystane w EIGRP

- Wykrywanie **sąsiadów**.
- Diffusing Update Algorithm **DUAL**.
- **Tigger updates** po wykryciu zmiany lub nowego sąsiada.
- Komunikaty **HELLO**.
- Wyznaczają **succesorów, feasible succesorów**.

Wybrane zalety EIGRP

- **Minimalne zużycie szerokości pasma** gdy sieć jest stabilna. W czasie normalnego stabilnego działania sieci jedynymi wymienianymi pakietami pomiędzy węzłami EIGRP są pakiety HELLO.
- Wydajne wykorzystanie szerokości pasma w czasie uzyskiwania zbieżności. Po zmianie propagowane są jedynie zmiany, nie całe wektory odległości. Po wykryciu sąsiada uaktualnienie wysyłane jest tylko do niego (unicast).
- **Szybka zbieżność** po wykryciu zmiany w sieci.

EIGRP wykorzystuje specjalny **niezawodny protokół** w warstwie transportu – **Reliable Transport Protocol**.

- Aktualizacje są przesyłane niezawodnie na adres grupowy 224.0.0.10. Potwierdzenia są przesyłane na adres jednostkowy (unicast). Jeśli potwierdzenie z określonym numerem sekwencji nie nadejdzie w czasie RTO (Retransmission TimeOut), pakiet z aktualizacją jest retransmitowany, tym razem na adres jednostkowy.
- Zwykłe pakiety HELLO oraz potwierdzenia nie są potwierdzane.
- DUAL jest używany do wyznaczenia sukcesorów i wykonalnych sukcesorów określających **trasy zapasowe**.
- Mechanizm wyznaczania tras zapasowych zapewnia, że **nie ma w nich pętli routowania**.

13 Protokoły routowania stanu łącza: sposób działania, charakterystyka protokołu OSPF, rodzaje obszarów.

Metryką jest szybkość łącza.

- informacje rozsyłane **do wszystkich** węzłów
- rozsyłana tylko część tablicy routingu o **bezpośrednio połączonych** sieciach
- każdy router buduje **pełną mapę topologii**, wylicza najlepsze ścieżki (Dijkstra)

OSPF

- protokół **bezklasowy**
- umożliwia **uwierzytelnienie**
- **szybko uzyskuje zbieżność**, trigger updates
- **flooding** do utworzenia map topologii

Nagłówek OSPF: typ pakietu, id routera, id obszaru.

Pakiety OSPF

- **Hello** - nawiązywanie sąsiedztwa.
- **DBD** - skrócona lista bazy danych łącze stan
- **LSR** - żądanie dodatkowych informacji o wpisie z DBD
- **LSU** - aktualizacja będąca odpowiedzą na LSR
- **LSA** - potiwerdzenie odebrania LSU

Rodzaje routerów

- **Router desygnowany** - hosty mają z nim relację przyległości, z pozostałymi sąsiadami nie (on reaguje na zmiany, hosty na niego).
- Routery wewnętrzne, brzegowe, szkieletowe, brzegowe AS.
- **Gateway of last resort** - router do którego idziemy kiedy nie mamy trasy.

Wszystkie obszary połączone do Area 0. **Rodzaje obszarów**:

- "normalne" - bez stuba
- **Stub Area** – do takiego obszaru NIE są wprowadzane trasy zewnętrzne, natomiast sumy tras z innych obszarów są wprowadzane.
- **Totally Stubby Area** – do takiego obszaru nie są wprowadzane ani trasy zewnętrzne, ani sumy tras z innych obszarów OSPF. Wyjście z takiego obszaru jest tylko przez trasę domyślną
- **Not So Stubby Area (NSSA)** – obszar Stub, do którego wprowadzane są pewne (na ogół nieliczne) trasy zewnętrzne, które następnie przekazywane są do innych obszarów tak jak sumy tras.
- **Not So Stubby Totally Stubby Area** – obszar połączenie NSSA i Totally Stabby Area. Routery ABR na granicach różnych obszarów powinny być odpowiednio skonfigurowane, co stanowi dodatkową trudność w konfigurowaniu OSPF.

Trasy zewnętrzne - z innych protokołów routingu.

14 DNS.

Hierarchiczny rozproszony system przechowującym informacje o **nazwach komputerów** i ich numerach IP, który odpowiada na zapytania o nazwy domen.

Za koordynację nazw domen i przypisywanie adresów IP jest **IANA** (Internet Assigned Numbers Authority) działająca pod ICANNem (Internet Corporation for Assigned Names and Numbers).

Domeny górnego poziomu

- **Arpa** - specjalna, wykorzystywana do odwzorowania adresów IP w nazwy.
- **Domeny podstawowe**, np: com, edu, gov.
- **Domeny geograficzne**), np: pl, uk, de.

Domeny drugiego poziomu - np: edu.pl, com.pl, co.uk, ac.uk.

Obszar, inaczej **strefa** jest częścią systemu DNS, która jest **oddzielnie administrowana**.

Poszukiwania w DNS

- **Proste**, „do przodu"– klient zna nazwę domenową, a chce uzyskać numer IP.
- **Odwrotne** – klient zna adres IP i chce uzyskać nazwę domenową; wykorzystuje domenę arpa.in-addr.

14.1 Typy serwerów DNS

W każdej strefie musi być uruchomiony podstawowy serwer DNS oraz pewna liczba serwerów drugoplanowych, zapewniających usługi w razie awarii serwera podstawowego.

- **Serwer podstawowy** pobiera dane z pliku konfiguracyjnego, natomiast serwery drugoplanowe uzyskują dane od serwera podstawowego na drodze tzw. transferu strefy.
- **Serwery drugoplanowe** odpytują serwer podstawowy o dane w sposób regularny.
- **Serwery podręczne** (lokalne), których zadaniem jest zapamiętanie na pewien czas w pamięci podręcznej danych uzyskanych od innych serwerów tak, aby kolejne zapytania klientów mogły być obsłużone lokalnie.

Podział ze względu na sposób uzyskania odpowiedzi poszukiwania

- **Przeszukiwanie rekurencyjne** – klient oczekuje od serwera żądanej informacji. W przypadku, gdy serwer nie przechowuje żądanej informacji, sam znajduje ją na drodze wymiany komunikatów z innymi serwerami.
- **Przeszukiwanie iteracyjne** – występuje między lokalnym serwerem DNS a innymi serwerami DNS. Jeśli odpytywany serwer nie zna szukanego adresu IP, odsyła pytającego do innych serwerów.

Komunikacja klienta z serwerem DNS
Przy odwołaniu do nazwy domenowej system zwykle najpierw sprawdza, czy nie jest to nazwa hosta lokalnego, następnie sprawdza plik hosts - o ile istnieje. Jeśli nie znajdzie odpowiedniego wpisu, to wysyłane jest zapytanie do pierwszego serwera DNS (adres w pliku konfiguracyjnym).

Dynamiczny DNS (DDNS)
Chyba najważniejsze wpisy w DNS dotyczą serwisów, np. www. Standardowo DNS obsługuje odwzorowanie nazw do statycznych adresów IP, można skonfigurować dynamiczne przez usługodawców, którzy przypisują nazwę do swojego IP i pewnego numeru portu, następnie zapytanie przekierowują do komputera ze zmiennym IP z ewentualną zmianą portu. Na komputerze ze zmiennym IP należy zainstalować odpowiedni program (klient DDNS), który będzie powiadamiał serwer DDNS o zmianach adresu IP.

14.2 Rekordy zasobów

Każdy serwer DNS przechowuje **informacje o tej części obszaru nazw DNS, dla której jest autorytatywny**. Informacje zapisywane są w postaci tzw. rekordów zasobów. Są to np: określenie adresu IPv4/6 dla hosta; nazwę kanoniczną jako nazwę domeny, rekord wymiany poczty. Dla zwiększenia wydajności serwer DNS może przechowywać również rekordy zasobów domen z innej części drzewa domen.

14.3 DHCP - Dynamic Host Configuration Protocol

Serwer DHCP **przydziela adresy IP dynamicznie**. Przydział dynamiczny numerów IP umożliwia pracę (ale nie jednoczesną) wielu komputerów z przydzielonym jednym numerem IP.

Serwer DHCP może wykorzystywać różne sposoby przypisywania adresów:

- **przydział statyczny** IP do danego komputera (ustawienie „ręczne", danemu adresowi MAC jest przypisywany stale jeden na stałe wybrany IP),
- **automatyczny przydział statyczny** przy pierwszym starcie komputera i kontakcie z serwerem,
- **przydział dynamiczny**, w którym serwer **wynajmuje** adres IP na określony czas.

DHCP umożliwia budowanie systemów konfigurujących się automatycznie. Oprócz przydzielenia adresu IP serwer DHCP przesyła do komputera klienta również inne dane konfiguracyjne, np. adres sieci, maskę sieci, adres domyślnego rutera (bramy).

15 Działanie przełączników Ethernet: tryby działania, protokół STP, sieci VLAN, łącza trunkingowe, przełączniki warstwy 3.

Koncentratory - huby, dostają info na jeden port i **wzmacniają go i wysyłają na wszystkie inne**. Nie analizuje ramek, fizyczna budowa gwiazdy a logicznie magistrali, **1 warstwa** ISO OSI.

Mosty - analizują ramki, **2 warstwa** ISO OSI, ma **filtrować ruch** tak by niektóre ramki pozostawić w jednym segmencie(jeśli MAC jest w tym segmencie), uczy się MAC.

Przełącznik - analizuje ramki, **2 warstwa**, ma kilka portów też uczy sie MAC-ów (jak zna to tam wysyła a jak nie zna to wysyła wszędzie oprócz tego co dostało). **Tryby działania**:

- **Store and Forward** - pobiera całą ramkę, sprawdza czy błędna i dopiero potem dalej
- **Cut-through**
  - **Fast Forward Switching** - po otrzymaniu MAC od razu ją nadaje, nie sprawdza błędów, albo czy nie nastąpiła kolizja
  - **Fragment-Free Switching** - ramka jest przesyłana dopiero jak dojdzie 64 bajty

Burza broadcastów - cały czas są robione broadcasty i zapychają sieć(jak mamy 3 przełączniki w trójkąt połączone i A wyśle broadcast to odbiorą go B i C, nie wyślą go do A(bo stamtąd przyszło), ale wyślą do siebie, co z powrotem wyśle do A i tak w kółko).

STP - SpanningTree Protocol - jak łączymy przełączniki to chcemy redundancje między nimi i to jest fajne, ale przez to są pętle (burza broadcastów, double packety, złe MAC) i już nie jest, na ratunek STP - będzie redundancja, ale w danej chwili tylko jedno ze zduplikowanych jest aktywne.
Działanie:

- **Wybór korzenia** - na podstawie najniższego priorytetu przełącznika
- **Wybór root-portów** (komunikacja z korzeniem) - jak jest połączony z rootem to jest automatycznie, inne wybierane na podstawie szerokości pasma
- **Wybór portów wyznaczonych** - wszystkie inne połączenia muszą "zdecydować" w którą stronę będą działać i porównują sobie BID i wybierają niższy, a ten drugi port jest robiony na disabled

Stany portów:

- **Blocking** - nie przekazuje normalnych, czyta BPDU
- **Listening** - zwykłe ramki nie przekazywane, BPDU czytane i wysyłane
- **Learning** - zwykłe ramki nie przekazywane, BPDU czytane i wysyłane, uczy się MAC
- **Forwarding** - wszystko przekazywane, czytane
- **Disabled** - przez admina

EtherChannel - połączenie kilku ethernetowych łącz fizycznych w jedno logiczne. Przełączniki mogą wówczas równomiernie rozkładać obciążenie na łączu.

Shortest Path Bridging - rozwinięcie STP, wiele redundantnych ścieżek jest wykorzystywanych jednocześnie, link-state do wyznaczenia najkrótszych ścieżek w warstwie drugiej.

Przełącznik 3 warstwy - to urządzenie sieciowe podobne w działaniu do routera. Decyzje routingowe podejmowane są na podstawie danych z trzeciej warstwy modelu OSI. Do wyznaczania trasy używany jest pierwszy pakiet z danego przepływu a reszta pakietów z danego przepływu przełączana jest już w warstwie 2. W związku z tym przełącznik warstwy trzeciej nie ma pełnej funkcjonalności routera. Ograniczenia dotyczą m.in. translacji adresów (NAT), implementacji mechanizmów bezpieczeństwa czy niestandardowych protokołów. Przełącznik warstwy trzeciej jest zazwyczaj droższy i szybszy w działaniu niż router. **Wykonują routowanie między VLANAMI.**

VLAN - wirtualne sieci LAN tworzone są przy pomocy przełączników. Są konfigurowane programowo, zatem ewentualne zmiany konfiguracji nie wymagają zmian w okablowaniu. Komputery z każdej utworzonej sieci wirtualnej nie muszą być dołączone bezpośrednio do jednego przełącznika. Urządzenia należące do jednej sieci wirtualnej mogą się ze sobą komunikować tak jakby były w jednym segmencie sieci LAN, działa np. ARP.

Trunk - połączenia między przełącznikami. Połączenie typu trunk umożliwia przekazywanie ramek należących do różnych sieci VLAN po jednym fizycznym nośniku. Za kontrolę połączenia trunk odpowiada **protokół VTP** (VLAN Trunking Protocol). Łączenie danych w jeden wspólny kanał, w którym przesyłane są dane.

VTP - Virtual Trunking Protocol - umożliwia zautomatyzowaną konfigurację wielu przełączników z jednego miejsca na drodze wymiany odpowiednich ramek z sąsiadującymi przełącznikami.

16 Podstawy kryptografii: szyfrowanie z kluczem symetrycznym, szyfrowanie z kluczem publicznym i prywatnym, funkcje skrótu, podpis cyfrowy, certyfikaty.

16.1 Szyfrowanie z kluczem

- liczba lub kilka liczb, składająca się z kilkudziesięciu do kilku tysięcy bitów
- służy do szyfrowania i odszyfrowywania rzeczy
- różne algorytmy szyfrowania
  - **Szyfrowanie z kluczem symetrycznym**
    - **Teoretycznie możliwy do złamania** brute forcem (w praktyce niezbyt).
    - Szyfrowanie dużych porcji danych przy użyciu jednego klucza ułatwia złamanie szyfru, dlatego klucz symetryczny **powinien być zmieniany**.
    - Może być przesłany zaszyfrowany przy pomocy techniki z kluczem publicznym i prywatnym.
    - Można generować oddzielne klucze sesji i szyfrować je wcześniej uzgodnionym tajnym kluczem symetrycznym. Klucze symetryczne mogą być też zmieniane co określony czas.

    * Algorytmy szyfrujące używające klucza symetrycznego: DES, 3DES, RC (WiFi/WPA), AES (WPA2)
  - **Szyfrowanie z kluczem asymetrycznym**
    * Szyfrowanie i odszyfrowanie jest tu realizowane przy pomocy pary kluczy - **prywatnego i publicznego**. Jeden szyfruje, drugi odszyfrowywuje.
    * **Odgadnięcie** jednego z kluczy **praktycznie niemożliwe** nawet przy znajomości drugiego.
    * Szyfrujemy coś czyimś kluczem publicznym, by tylko ten ktoś mógł to odszyfrować (swoim kluczem prywatnym).
    * Wielokrotnie **kosztowniejsze czasowo** od szyfrowania z kluczem symetrycznym.
    * Używane do uzgodnienia kluczy symetrycznych.
    * Algorytm RSA.

16.1.1 Skrót (hash)

- **Skrót wiadomości** w podpisach cyfrowych, tworzony za pomocą funkcji haszujacej.
- 128 bitów (MD5), 160 bitów(SHA-1), 224-512 bitów (rodzina SHA-2)
- Jeśli w oryginalnej wiadomości (pliku) zmieniony **zostanie chociaż jeden bit, to skrót będzie zupełnie inny** niż ten, który został utworzony przed zmianą.
- **Algorytmy haszujące są deterministyczne**.
- **Odtworzenie** oryginalnej wiadomości ze skrótu jest **prawie niemożliwe**.

16.1.2 Podpis cyfrowy

- Zaszyfrowanie kluczem prywatnym daje **gwarancję**, że zaszyfrowana wiadomość **pochodzi z odpowiedniego źródła**.
- Samej podpisywanej wiadomości nie musi się szyfrować. Generowany jest jej skrót i ten **skrót jest szyfrowany** z wykorzystaniem klucza **prywatnego** osoby **podpisującej**. Zaszyfrowany skrót stanowi podpis cyfrowy. Niezaszyfrowana wiadomość może być przesłana jawnie razem z zaszyfrowanym skrótem (czyli podpisem cyfrowym).
- Odbiorca **odszyfrowuje** skrót używając klucza **publicznego nadawcy**. Potem tworzy skrót wiadomości używając tej samej funkcji haszującej. Jeśli wyniki obu operacji są identyczne, to znaczy, że wiadomość na pewno podpisał określony nadawca, a ponadto nikt po tej wiadomości nie zmienił już po podpisaniu.

16.1.3 Klucze publiczne i prywatne, infrastruktura kluczy publicznych

- Klucze mogą być generowane na komputerze lokalnym przy pomocy odpowiedniego oprogramowania i powinny być podpisane przez jakieś centrum certyfikacyjne.
- Centrum certyfikacyjne (CA) wydaje tzw. certyfikaty cyfrowe zawierające m.in:
  - Identyfikator osoby/firmy/obiektu
  - Identyfikator CA, który wydał certyfikat
  - Numer identyfikacyjny certyfikatu
  - Cel stosowania (np. podpisywanie bezpiecznych stron WWW albo podpisywanie listów elektronicznych)
  - Wartość klucza publicznego
  - Okres ważności

  - Podpis cyfrowy wydawcy
- Jeśli ufamy danemu CA, to ufamy, że zawarty w certyfikacie klucz publiczny jest rzeczywiście prawdziwy. W systemach operacyjnych oraz różnych programach jest wpisana lista zaufanych CA. Zarządzanie centrum certyfikacyjnym jest realizowane na przez konsolę MMC.
- Niezależnym standardem opisującym tworzenie kluczy, rejestrowanie i wykorzystywanie certyfikatów jest PGP (Pretty Good Privacy). Powstał standard Open PGP.

17 Bezpieczne protokoły: SSL, TLS, IPSec (ze szczególnym naciskiem na protokół IPSec).

Bezpieczne protokoły mogą być wykorzystywane:

- **w warstwie aplikacji**- szyfrowanie komunikatów HTTPS, protokoły SSL, TLS,
- **między warstwą sieci a transportu** - szyfrowanie pakietów IP – protokół IPSec,
- **w warstwie łącza danych** - szyfrowanie ramek, np. WEP, WPA, WPA2 w sieciach bezprzewodowych.

17.1 Protokół IPSec

- **warstwa IP**
- może szyfrować dane pochodzące z dowolnej aplikacji, proces szyfrowania i deszyfrowania jest **niewidoczny** dla użytkownika
- **Authentication Headers** (AH) - sprawdzenie **autentyczności i integralności** danych.
- **Encapsulating Security Payloads** (ESP) - **szyfrowanie** danych, oraz autentyczność i integralność danych. ESP może być używany samodzielnie lub z AH.

Przed przesyłaniem danych strony komunikujące się uzgadniają szczegóły takie jak sposób uwierzytelniania, wymiana kluczy, algorytmy szyfrowania.

Tryby działania IPSec (zarówno AH jak i ESP):

- **Tryb transportu** (w sieci lokalnej) między dwoma punktami końcowymi transmisji.
- **Tryb tunelowania** – szyfrowanie w niezabezpieczonej części sieci (np. dane między biurami przesyłane przez Internet).

Metody uwierzytelniania w IPSec:

- **Kerberos**
- **Oparty o certyfikaty cyfrowe**
- **Klucz dzielony** - przechowywany we właściwościach napis jednakowy dla obu komunikujących się stron.

Polityki stosowania IPSec

- **Client** (respond only) - transmisje bez IPSec, chyba że druga strona zażąda IPSec
- **Server** (request security) - żądanie transmisji IPSec, ale jeśli druga strona nie implementuje IPSec, to komunikacja bez IPSec
- **Secure server** (require security) - żądanie transmisji IPSec, jeśli druga strona nie implementuje IPSec, to komunikacja nie jest kontynuowana.

Filtry IPSec
Filtr IPSec pozwala na automatyczne przepuszczenie datagramów IP, blokowanie lub użycie negocjacji (i

w konsekwencji użycie IPSec) w zależności od źródła i miejsca docelowego IP, protokołu transportowego, portów źródłowych i docelowych.

17.2 SSL - Secure Socket Layer

- **warstwa aplikacji** TCP/IP (prezentacji w ISO/OSI)
- jego zadaniem jest **zabezpieczanie informacji** przesyłanych siecią.
- zapewnia autoryzację serwerów internetowych i (opcjonalnie) klientów (utrudnia podszywanie pod autoryzowanych usługodawców i użytkowników)
- często prezentowany jako protokół, który leży powyżej warstwy transportu (TCP, UDP) i sieci (IP) a poniżej warstwy aplikacji (np. HTTP, FTP, SMTP, TELNET)
- jest protokołem **otwartym**
- wykorzystuje **szyfrowanie symetryczne** z kluczem **publicznym**
- protokoły zabezpieczone SSL oznaczane są jako HTTPS (dla HTTP), FTPS (dla FTP) itd.
- stosuje **sumy kontrolne** dla zapewnienia **integralności**.

Po nawiązaniu połączenia następuje wymiana informacji (certyfikatów CA i kluczy publicznych) uwierzytelniających serwera i (opcjonalnie) klienta. Serwer i klient uzgadniają również algorytmy szyfrowania – najsilniejsze dostępne jednocześnie obu stronom. Następnie serwer i klient generują klucze sesji (symetryczne), które są szyfrowane kluczem publicznym drugiej strony. Klucze sesji są odszyfrowywane przy pomocy klucza prywatnego i następnie służą do szyfrowania danych.

17.3 TLS - Transport Layer Security

- **warstwa aplikacji**
- strony dogadują się co do klucza symetrycznego szyfrowaniem niesymetrycznym
- symetryczne szyfrowanie danych

18 Protokół IPv6: adresacja, nagłówki, mechanizmy, ICMPv6 (m.in. jak odnaleźć adres MAC na podstawie adresu IPv6), mechanizmy przejścia między IPv4 i IPv6, mobilny IP.

- **dłuższy adres** - 128 bitów
- **złożona hierarchia adresów**.
- nowa forma nagłówka
  - **podstawowy nagłówek** jest uproszczony - zawiera 40 oktetów
  - dodatkowe informację przekazywane są za pomocą **dodatkowych nagłówków**, które są opcjonalne
  - dzięki temu router szybciej jest w stanie przetworzyć pakiet
  - takie rozwiązanie daje więcej możliwości rozszerzenia protokołu
- **fragmentacja** jest **realizowana przez nadwacę**, nie przez routery pośrednie (jak w IPv4)
- zawiera rozwinięte mechanizmy **autokonfiguracji**
- zawiera ulepszone mechanizmy obsługi rozgłaszania grupowego (**multicast**) oraz nowy rodzaj adresowania – adresy pobliskie **anycast** (przesłanie do jednego – na ogół najbliższego – routera skonfigurowanego do odbierania określonego adresu typu anycast)

- włączone są **mechanizmy bezpieczeństwa** (włączony standard **IPSec**).
- Wsparcie dla **QoS** (Quality of Service) – mechanizm rezerwacji zasobów na potrzeby komunikujących się programów

18.1 Nagłówek IPv6.

Version	wersja protokółu (6)
Traffic Class	używana do określenia priorytetu pakietu
Flow Label	etykietowanie pakietów wymagających takiego samego traktowania przez routery
Payload Length	wielkość danych za nagłówkiem, obejmuje też nagłówki dodatkowe
Next Header	identyfikuje typ następnego nagłówka, np. TCP, UDP lub nagłówka dodatkowego IPv6
Hop Limit	TTL (Czas życia pakietu)
Source Address	adres źródłowy
Destination Address	adres docelowy (puste jeśli został załączony dodatkowy nagłówek typu Routing)

18.1.1 Dodatkowe nagłówki.

- **typ** nagłówka dodatkowego jest określony w polu **Next Header** w nagłówku poprzedzającym
- nagłówki dodatkowe są sprawdzane i **przetwarzane przez węzeł** (router, host) o adresie zawartym w polu **Destination Address** w nagłówku podstawowym
- nagłówki dodatkowe muszą być **sprawdzane i przetwarzane dokładnie w kolejności występowania**
- jeśli węzeł musi przetworzyć nagłówek dodatkowy, ale nie może rozpoznać poprawnej liczby w polu Next Header, powinien odrzucić datagram i wysłać komunikat ICMPv6 Parameter Problem

18.1.2 Rodzaje nagłówków.

- **IPv6 header** - nagłówek podstawowy.
- **Hop-by-hop Options header** - np. w protokole RVSP, w protokole MLD – Multicast Listener Discovery.
- **Destination Options header** - jeśli użyty jest nagłówek dodatkowy Routing. Służy do przekazania opcji, które będą przetwarzane przez węzeł o adresie zawartym w polu Destination Address w nagłówku podstawowym oraz przez węzły o adresach wymienionych w nagłówku dodatkowym typu Routing.
- **Routing header**
  - **typ 0**: odpowiednik routowania źródłowego z IPv4
  - **typ 2**: wykorzystywany do obsługi mobilności do przekazania Home Address mobilnego węzła docelowego).
  - jest używany do określenia **listy routerów**, przez które **powinien przejść** pakiet na drodze do miejsca przeznaczenia.
  - pierwszy węzeł, który przetwarza nagłówek Routing to węzeł (router), którego adres znajduje się w polu Destination Address nagłówka podstawowego. Węzeł ten zmniejsza o jeden liczbę zawartą w polu Segments Left i przepisuje następny adres z nagłówka Routing do pola Destination nagłówka podstawowego. Ostateczne miejsce docelowe datagramu jest określone przez ostatni adres w nagłówku Routing.
  - w odróżnieniu od IPv4, w IPv6 **adres docelowy może się zmieniać** na drodze datagramu – jeśli wykorzystywany jest nagłówek dodatkowy Routing
- **Fragment header**.
  - Fragmentacja występuje **tylko w węźle źródłowym**.

  - Pakiet ma część, która nie podlega fragmentacji – jest to podstawowy nagłówek i wszystkie nagłówki dodatkowe, które muszą być przetwarzane na drodze datagramu.
  - Część, która podlega fragmentacji składa się z pozostałych nagłówków dodatkowych, nagłówka warstwy wyższej i danych.
  - Część niepodlegająca fragmentacji jest na początku każdego fragmentu, potem jest nagłówek Fragment, potem część pofragmentowana.
- **Authentication header**.
- **Encapsulating Security Payload header**.
- **Destination Options header** (wykorzystywany dla opcji, które będą przetwarzane tylko przez ostatecznego odbiorcę pakietu, wykorzystywany w mobilnym IP do przekazania źródłowego adresu home).
- **Mobility header** (wykorzystywany do obsługi mobilności, przy zgłaszaniu).
- **Upper-Layer header** (np. TCP, UDP) <- nagłówek dotyczący danych

18.2 Adresacja IPv6.

- **osiem 16 bitowych sekcji w zapisie szesnastkowym**, oddzielonych dwukropkami,

  np.: fe80:0000:0000:0000:0202:b3ff:fe1e:8329
- długi ciąg zer może być **raz** połączony i przedstawiony jako dwa dwukropki "::"
- w środowisku z węzłami IPv4 oraz IPv6 często **w adresie IPv6 umieszcza się również IPv4**. Są dwa typy takich adresów:
  - **Typ 1: IPv4-Compatible IPv6 Address** - 96 bitów zero + adres IPv4
  - **Typ 2: IPv4-Mapped IPv6 Address** (zalecany) - 0000.....0000 ffff + IPv4 address
- Zamiast identyfikatora sieci (jak było w IPv4), w IPv6 używa się tzw. **prefiksu**. Prefiks to **pewna liczba bitów** adresu licząc z lewej strony. Prefiks **określa** zatem **sieć**. Prefiks podaje się standardowo jako pewną liczbę sekcji adresu.

18.2.1 Typy adresów

- **Adres niewyspecyfikowany** - ::/128
- **Pętla zwrotna** (Loopback) - ::1/128
- **Multicast** - ff00::/8 (1111 1111)
- **Link-local unicast** - fe80::/10 (1111 1110 10)
- **Global unicast**

18.2.2 Skąd wziąć adres MAC?

- Unicastowy adres IP na multicastowy (Solicited Node Multicast address) - ff02:0:0:0:0:1:ff_:_ _, z trzema najmłodszymi bajtami adresu IP
- Multicastowy MAC - 33:33:_:_:_:_ z czterema najmłodszymi bajtami adresu multicastowego
- Ramka skonstruowana z adresem MAC, z pakietem IP z multicastowym IP w środku, z unicastowym w komunikacie ICMP
- Switche się znają na tyle, że ramka w miarę dochodzi tylko tam gdzie trzeba
- Komputer otrzymujący ramkę sprawdza czy o niego chodzi w komunikacie ICMP, i unicastowo odpowiada

18.3 ICMPv6

Mechanizmy:

- **Wykrywanie sąsiada** - jak wyżej
- **Multicast Listener Discovery** (MLD) - jest odpowiednikiem **Internet Group Management Protocol** (IGMP) w IPv4
- **Wykrywanie ścieżki MTU** (Path MTU Discovery) - nie musi być implementowane w pełni w każdym węźle. Host zaczyna wysyłać pakiety o wielkości MTU dla wykorzystywanego łącza. Jeśli dostanie komunikat ICMPv6 Packet Too Big, to zmniejsza rozmiar pakietu. Może to wystąpić wielokrotnie w czasie komunikacji do miejsca docelowego. Po ewentualnym zmniejszeniu rozmiaru pakietu od czasu do czasu host próbuje wysłać większy datagram, aby wykryć możliwość przesłania większego datagramu.
- **IPSec w IPv6**

Mechanizmy przejścia

- **6to4**
  - polega na pakowaniu pakietów IPv6 w pakiety IPv4. Pole protokołu w nagłówku otrzymuje wartość 41. Tak utworzone pakiety wysyłane są do komputera stanowiącego bramę pomiędzy siecią opartą na IPv4 a „prawdziwą" siecią IPv6.
  - łączenie sieci 6to4 z innymi sieciami 6to4 i innymi IPv6 poprzez sieć IPv4 w okresie przejściowym
- **6over4**
- **ISATAP**

19 Charakterystyka protokołu BGP (w zakresie omówionym na wykładzie).

- **Border Gatewqat Protocol** - protokół routingu **między systemami autonomicznymi** AS
- główną funkcją **routera BGP** jest wymiana informacji o **osiągalności sieci** w Internecie z sąsiednimi routerami BGP w innym AS
- działa na **niezawodnym** protokole transportowym jakim jest **TCP**
- dwa routery z BGP zestawiają między sobą **połączenie TCP**. Wymieniają między sobą **wiadomości dla otwarcia i potwierdzenia** parametrów **połączenia**.
- na początku wymiana cały tabel routingu, potem trigger updates
- routery BGP okresowo wysyłają między sobą wiadomości **KeepAlive**, by upewnić się o **żywotności połączenia**
- Wysyłane są też wiadomości **Notification** w odpowiedzi na wszelkie **błędy** i wyjątkowe sytuacje w routerach BGP. Po wysłaniu Notification o błedzie i połączenie między dwoma peerami BGP jest **zamykane**.

Typy wiadomości BGP

- **OPEN** - rozpoczęcie sesji
- **UPDATE** - informacje o routingu
- **NOTIFICATION** - wiadomość o błędzie
- **KEEPALIVE** - sprawdzenie żywotności połączenia
- **ROUTE-REFRESH** - dynamiczne żądania odświeżenia tras

Zestawienie sesji BGP

- **IDLE** - router oczekuje na zdarzenie Start - chęć parowania
- **CONNECT** - próba nawiązania nowej sesji TCP; OPENSENT jeśli sukces, ACTIVE wpp
- **ACTIVE** - routery nadal próbują nawiązać sesję TCP; OPENSENT jeśli sukces, IDLE wpp
- **OPENSENT** - parowanie routerów; OPENCONFIRM jeśli ok
- **OPENCONFIRM** - potwierdzenie parowania
- **ESTABLISHED** - parowanie zakończone

20 Podstawy programowania w interfejsie gniazd (w zakresie omówionym na wykładzie).

Gniazda - to **abstrakcyjne** mechanizmy umożliwiające wykonywanie systemowych **funkcji wejścia–wyjścia** w odniesieniu do sieci. Umożliwiają między innymi **przesyłanie danych między procesami** działającymi na komputerach w sieci z wykorzystaniem połączeń TCP lub protokołu UDP, przy czym same operacje wysyłania i odbierania danych przypominają zwykłe operacje zapisywania i odczytu z pliku.

- **Iteracyjne** - takie które kolejkują klientów.
- **Współbieżne** - starają się od razu wszystko równolegle obsłużyć.

Programowanie w skrócie:

- Struktura **socaddr_in**
  - **długość** struktury,
  - **typ adresu** (AF_INET),
  - **nr portu**,
  - struktura z **adresem** urządzenia.
- Klient uzupełnia socaddr_in danymi serwera.
- Wywołuje funkcję **socket** podając jej:
  - **typ adresu** (AF_INET),
  - **typ gniazda** - datagramowe (UDP) lub streamowe (TCP)
- **(przy TCP)** Przekazuje to co zwrócił socket (**deskryptor gniazda**) i strukturę socaddr_in do funkcji **connect** i tworzy połączenie
- Używa socketa jak **pliku** - zwykłe pisanie i czytanie.