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:

- Topologie fizyczne
- Topologie 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	Nazwa warstwy Tannenbaum
7	Aplikacji	Aplikacji	Aplikacji
6	Prezentacji		
5	Sesji		
4	Transportu	Transportu	Transportu
3	Sieci	Intersieci	Sieci
2	Łącza danych	Interfejsu sieciowego	Łącza danych
1	Fizyczna		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

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

Na warstwę aplikacji składają się komponenty programowe sieci, wysyłające i odbierające informacje przez tzw. porty TCP lub UDP (z warstwy transportu). Protokoły warstwy aplikacji to między innymi:

- FTP (File Transfer Protocol),
- TELNET,
- DNS (Domain Name System) związany z usługą DNS (Domain Name Service).

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.
  - TCP realizuje tzw. niezawodne połączenia i kontroluje przepływ danych zapewniając niezawodne dostarczenie danych.
  - UDP nie zapewnia niezawodności, ale jest szybszy.
- 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). RFC stałe, zmiany jako kolejne RFC, numery niezmiennne

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				

sposób dostępu do nośnika - kiedyś przy topologii magistrali był half-duplex (albo tylko nadajesz, albo tylko odbierasz, tylko jeden komputer może nadawać żeby się nie pokrywały)

CSMA - Carrier Sense Multiple Access - komputer nasłuchuje czy ktoś inny nadaje, jak nie to dopiero sam zaczyna nadawać; żąda potwierdzenia otrzymania ramek; jak ktoś nadaje to czeka pseudolosowy czas i próbuje znowu

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

CSMA CD (Colission Detect) - nasłuchują nadając, żeby wiedzieć czy jest kolizja; jak jest kolizja to wysyłają sygnał zagłuszający, żeby powiedzieć że była kolizja i dane wysłane przed chwilą to śmieci

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.

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.
  - 224.0.0.1 – wszystkie komputery uczestniczące w transmisji grupowej (również routery) w segmencie sieci lokalnej.
  - 224.0.0.2 – wszystkie routery uczestniczące w transmisji grupowej (multicast routers) w segmencie sieci lokalnej.
  - 224.0.0.4 – routery DVMRP.
  - 224.0.0.5 – wszystkie routery OSPF.
  - 224.0.0.6 – routery DR OSPF.
  - 224.0.0.9 – routery RIPv2 (RIPv1 wykorzystuje rozgłoszenie – broadcast, nie multicast).
  - 224.0.0.0 – 239.255.255.255 - klasa D adresów IPv4
- 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 (general membership query), wysyłany jest okresowo (co kilkadziesiąt sekund) przez routery na wszystkiue komputery.
- Membership report służy do zgłoszenia się jako odbiorca pakietów wysyłanych na ten adres; membership report wysyłany jest też w odpowiedzi na membership query.

Host po otrzymaniu membership query czeka pewien pseudolosowy czas z zakresu od 0 do 10 sekund) 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. Domyślnie router zakłada, że jest routerem odpytującym, ale jak dostanie query od routera z „niższym" adresem IP, to przestanie być routerem odpytującym. Jeśli router non-querier nie słyszy komunikatów query od routera odpytującego przez pewien czas, to staje się routerem odpytującym.

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 (CAM – Content Addressable Memory) i uwzględnia adresy Ethernet multicast. To rozwiązanie wymaga jednak odpowiednio wydajnych przełączników, najlepiej z dołączonym specjalnym sprzętowym modułem (ASIC) do analizy komunikatów IGMP.

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 (jeśli w warstwie sieci wykorzystywany jest protokół IPv4), był też używany w sieciach Token Ring. W wersji IPv6 protokół ARP

nie jest w ogóle wykorzystywany, zastępują go inne mechanizmy.

Struktura ramki 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**, defending node), węzeł wysyłający „zbędny ARP" jest **węzłem konfliktowym** (offending node).
- **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), więc zgodny wysyła ARP Request ze swoim adresem po wykryciu konfliktu.

Datagramy IP wysłane na w ramkach z niepoprawnym adresem MAC odbiorcy przepadają. Protokół IP nie zapewnia niezawodnej dostawy datagramów i nie spowoduje powtórnego przesłania datagramu w nowej ramce. Za niezawodność odpowiedzialne są protokoły warstwy transportu.

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 (domyślna brama, default gateway). 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

Założenia:

- Komputer źródłowy - Komputer 1: IP1, MAC1
- Komputer docelowy - Komputer 2: IP2, MAC2

Połączone switchem. Na komputerze docelowym jest serwer strony WWW2.

Jeżeli na komputerze 1 ktoś spróbuje otworzyć WWW2, to:

- Zadziała system DNS: komputer 1 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 komputera 1.

- 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. **Komputer 1 nie zna adresu MAC komputera 2**. Zna tylko jego adres IP. Wykorzystywany jest **protokół ARP** – Address Resolution Protocol.
  - Komputer 1 wysyła specjalną ramkę **ARP Request** (ta NIE zawiera pakietu IP), która ma adres rozgłoszeniowy jako adres docelowy (same jedynki).
  - 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 to specjalna ramka **ARP Reply**. Odpowiedź ARP jest wysyłana na adres MAC komputera 1.
- Po tym, jak komputer 1 pozna adres MAC komputera 2, może już zbudować ramkę przeznaczoną do komputera 2. Ramka jest wysyłana do przełącznika, a przełącznik dostarcza ją tylko do komputera 2.
  - Przełącznik uczy się adresów MAC przyłączonych komputerów i routerów i zapamiętuje w tablicy przypisanie adresu MAC do konkretnego swojego portu.
- Komputer 2 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 komputera 1. Mechanizm jest analogiczny jak poprzednio.

W rzeczywistości zanim może zostać przesłany segment TCP, komputery wykorzystujące ten protokół do komunikacji, muszą zbudować tzw. połączenie TCP.

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

- Wszystko do skonstruowania pakietu IP włącznie działa tak samo. Komputer tworzący ramkę musi więc wykorzystując ARP Request poznać MAC adres routera, czyli swojej **bramy domyślnej**.
- Ramka jest wysyłana do routera.
- Router (brama) po otrzymaniu ramki „wyjmuje" z niej pakiet IP, zagląda do nagłówka i sprawdza jaki jest adres docelowy IP. Na podstawie tego adresu i tablicy routowania wyznacza router następnego skoku i konstruuje i wysyła do niego nową ramkę, w której umieszcza przesyłany pakiet IP. Analogicznie aż pakiet dotrze w kolejnych ramkach do docelowej sieci i do docelowego komputera.

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.

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 20 bajtów	nagłówek UDP 8 bajtów	dane UDP ...

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)
- 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. Zero oznacza, że nadawca musi zaczekać, aż program użytkowy odbierze dane z bufora.
- 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 (Maximum Transmission Unit) 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. Jeden ze sposobów atakowania serwisów (np. WWW) polegał na otwieraniu bardzo dużej liczby połączeń półotwartych. Obecnie implementacje TCP są odporne na tego typu ataki. Dopuszczalne jest, by oprogramowanie realizujące TCP mogło sprawdzać stan połączenia przez okresowe przesyłanie segmentów sprawdzających aktywność. Segment taki to zawiera ustawioną na 1 flagę ACK i nie zawiera żadnych danych. Dodatkowo ma on ustawiony numer sekwencyjny na o 1 mniejszy od tego, którego normalnie spodziewa się strona wysyłająca ACK. Partner odpowiada też segmentem z ustawioną na 1 flagą ACK ze standardowo ustawionymi prawidłowymi wartościami numerów sekwencyjnych.

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 (ruchomych) 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**
  „Dopasowuje się" do sieci, w której przesyłane są segmenty.
  - 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".

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**.
- **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**.

12.2 Protokół RIP

- Metryką w RIP jest liczba skoków (hops) do celu. Metryka 16 oznacza umownie 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** (standardowo 30 sekund) – po przesłaniu wektora odległości (routing update) zegar jest zerowany. Po osiągnięciu 30 s. wysyłany jest następny wektor.
  - **Invalid timer** (standardowo 180 sekund) – 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** (standardowo 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** (standardowo 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.

12.4 Protokół IGRP

- wymaga podania numeru AS przy konfiguracji, musi być 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 (patrz też objaśnienia w oddzielnym pliku).
  - Opóźnienie (delay) – czas wędrówki pakietu od źródła do celu; wartości od 1 do 224, przy czym 1 oznacza 10 mikrosekund.
  - Obciążenie (load); wartość od 1 do 255. 1 oznacza sieć najmniej obciążoną, 255 najbardziej obciążoną.
  - Niezawodność (reliability); wartość od 1 do 255. Wartość liczona jest jako swoisty „procent" pakietów, które dotarły do następnego routera, przy czym liczba 255 oznacza 100%.

  $metric = (K_1 * bandwidth + \frac{(K_2 * bandwidth)}{(256 - load)} + K_3 * delay) * \frac{K_5}{(reliability + K_4)}$ Standardowo $K_1 == K_3 == 1, K_2 == K_4 == K_5 == 0$.
- przesyłane są również wartości MTU (Maximum Transfer Unit) – 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,
- konfiguracja EIGRP wymaga określenia numeru 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.
- Wysyłanie aktualizacji tylko po wykryciu nowego sąsiada i w przypadku wystąpienia zmiany, dotyczące tylko zmiany.

- Komunikaty HELLO.
- Wyznaczają 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 (handshake).
- 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 tzw. wykonalnych sukcesorów określających trasy zapasowe. W przypadku utraty pewnej trasy (uszkodzenia) router może natychmiast wyznaczyć niezapętloną trasę zastępczą (jeśli jest wyznaczony FS). Gdyby się zdarzyło, że nie ma informacji o trasie zastępczej, to router prosi sąsiadów o odnalezienie takiej trasy, jeśli sąsiedzi nie znajdują, to odpytują dalej. Zapytanie rozchodzi się (dyfunduje) coraz dalej, stąd nazwa DUAL (Diffusion Algorithm).
- 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.

Wewnątrz obszaru:

- routery zgłaszają wszystkie połączenia które mają do sąsiadów i tak kaskadowo rozsyłają info o wszystkich
- updaty o zmianach
- każdy ma swój własny obraz sieci, użycie Dijkstry

Na brzegach są border routery. Wszystkie area 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.

Gateway of last resort - router do którego idziemy kiedy nie mamy trasy.

14 DNS.

Oprócz adresu IP komputer ma przyporządkowaną **nazwę**. Konwencje nazywania komputerów:

- **nazwy hosta**
- **nazwy DNS**
- **nazwy NetBIOS**

Istnieją mechanizmy tłumaczące nazwy na numery IP i odwrotnie. Ciałem odpowiedzialnym za koordynację nazw domen górnego poziomu a także odpowiedzialnym za przypisywanie adresów IP jest IANA Internet Assigned Numbers Authority. Ciałem nadzorującym od strony technicznej różne działania związane z uzyskiwaniem (rejestrowaniem) nazw domen, numerów Ip, numerów portów jest ICANN - Internet Corporation for Assigned Names and Numbers.

Domeny górnego poziomu

- arpa - specjalna, wykorzystywana do odwzorowania adresów IP w nazwy.
- Domeny podstawowe (generic, gTLD), np: com, edu, gov.
- Domeny geograficzne (krajowe, country-code ccTLD), np: pl, uk, de.

Domeny drugiego poziomu - w wielu krajach domeny drugiego poziomu odzwierciedlają domeny organizacyjne pierwszego poziomu, ale ujmowane na swoim terytorium. Przykłady: edu.pl, com.pl, co.uk, ac.uk.

Obszar, inaczej **strefa** (zone) jest częścią systemu DNS, która jest oddzielnie administrowana. Domeny drugiego poziomu dzielone są na mniejsze strefy. Z kolei te strefy mogą być dalej dzielone. Występuje tu delegowanie zarządzania w dół struktury drzewa. Jednostka odpowiedzialna za zarządzanie daną strefą decyduje ile będzie serwerów DNS w strefie, rejestruje i udostępnia nazwy i numery IP nowych komputerów zainstalowanych w strefie. W tej chwili jest na świecie 13 (typów) serwerów głównych (najwyższego poziomu) zwanych po angielsku root-servers, posiadającymi nazwy od a.root-servers.net do m.root-servers.net.

Poszukiwania w DNS

- Proste, „do przodu”– klient zna nazwę domenową, a chce uzyskać numer IP.
- Odwrotne (reverse) – klient zna adres IP i chce uzyskać nazwę domenową. Przeszukiwanie odwrotne wykorzystuje domenę arpa.in-addr. Jeśli chcemy poznać nazwę domenową komputera, to w systemie DNS adres ten jest reprezentowany jako specyficzna nazwa w domenie 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 (zone transfer). Serwery drugoplanowe odpytują serwer podstawowy o dane w sposób regularny, zwykle co kilka godzin. Oprócz dwóch wymienionych rodzajów serwerów są jeszcze 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. Serwery DNS działają na portach 53 UDP oraz 53 TCP. Na ogół w warstwie transportu używany jest UDP. Wyjątkiem jest m.in. transmisja danych z serwera podstawowego do drugoplanowego (większe

porcje danych) oraz komunikaty w sieciach WAN. Również kiedy w odpowiedzi od serwera (przez UDP) ustawiony jest bit TC (patrz niżej) ponawiane jest zapytanie z wykorzystaniem TCP.

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 (odpowiedzialnych za daną domenę).

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).

Standardowy sposób poszukiwania
Klient pyta swój domyślny serwer DNS wysyłając zapytanie rekurencyjne. Odpytany serwer realizuje zapytania iteracyjne, zaczynając od serwerów głównych, które odsyłają do serwerów niższego poziomu. Mechanizm ten może się wydawać nieefektywny, ale w rzeczywistości dzięki temu, że serwery DNS zapamiętują na pewien czas informacje uzyskane z innych serwerów DNS (cache), często odpowiedź na zapytanie programu-klienta zostaje znaleziona bardzo szybko.

Dynamiczny DNS (DDNS)
Chyba najważniejsze wpisy w DNS dotyczą serwisów, np. www. Standardowo DNS obsługuje odwzorowanie nazw do statycznych adresów IP. Można jednak skonfigurować odwzorowanie dla adresów zmieniających się dynamicznie. W tym celu należy skorzystać z odpowiednich usługodawców w Internecie, 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. Oddzielnym problemem, który należy rozwiązać, jest wykorzystanie serwera NAT i przypisywanie adresów prywatnych do serwisu w sieci. Na ogół wystarczy odpowiednie działanie klienta DDNS oraz odpowiednie skonfigurowanie serwera NAT.

14.2 Rekordy zasobów

Każdy serwer DNS przechowuje informacje o tej części obszaru nazw DNS, dla której jest autorytatywny (administratorzy są odpowiedzialni za poprawność informacji). Informacje zapisywane są w postaci tzw. rekordów zasobów. Dla zwiększenia wydajności serwer DNS może przechowywać również rekordy zasobów domen z innej części drzewa domen. **Istnieje szereg typów rekordów zasobów:**
SOA (Start of Authority) Rekord uwierzytelnienia – pierwszy rekord w pliku strefy, określa podmiot odpowiedzialny od tego punktu hierarchii „w dół”.

- Serial – pole zawierające numer wersji pliku strefy, zwykle w polu tym odzwierciedlona jest data oraz numer wersji pliku w danym dniu.
- Refresh – określa jak często serwer pomocniczy ma sprawdzać na serwerze podstawowym, czy nie zachodzi potrzeba uaktualnienia plików.
- Retry – czas, po którym serwer pomocniczy będzie ponownie próbował odtworzyć dane po nieudanej próbie odświeżenia.
- Expire – maksymalny limit czasu, przez który serwer pomocniczy może utrzymywać dane w pamięci cache bez ich uaktualnienia. Minimum (Default TTL) – domyślny czas, jaki ma być użyty dla rekordów, które nie mają określonego TTL.

14.3 DHCP - Dynamic Host Configuration Protocol

Wadą BOOTP jest statyczny sposób przydzielania numerów IP. Przydział dynamiczny umożliwia pracę (ale nie jednoczesną) wielu komputerów z przydzielonym jednym numerem IP. Serwer DHCP przydziela adresy IP dynamicznie. Obecnie w bardzo wielu sieciach lokalnych komputery nie mają na stałe wpisanych IP, ale pobierają IP od serwera DHCP w momencie startu systemu. 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

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

STP - drzewo rozpinające switchy, switche mogą sobie dezaktywować porty na krawędziach których nie ma w drzewie; jak coś się zepsuje to porty włączane i nowe drzewo rozpinające wybór switcha od którego rozpoczynane jest budowanie drzewa przez 1) priorytet 2) MAC

tryby działa switchy: cut-through (puszcza ramki jak leci), store-and-forward (analiza czy ramka jest ok, przesyła dalej tak żeby nie było kolizji)

VLAN - odseparowanie w warstwie drugiej - ramki między vlanami nie mogą bezpośrednio przechodzić

łącza trunkingowe - do trunka są pchane wszystkie ramki z vlanów do niego przypisanych (domyślnie wszystkie ze switchu), tak samo do trunkiem można łączyć switche z komputerami z tymi samymi vlanami

przełączniki warstwy 3 - mają odciążyć router przy vlanach (ramka do vlanu w tym samym switchu musi być wysłana przez wszystkie switche do routera i z powrotem [bez sensu], więc switch może to obsłużyć) - czyli "switch, który może odpowiadac za routing między vlanami".

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
- teoretycznie możliwy do złamania brute forcem (w praktyce niezbyt)
- różne algorytmy szyfrowania
  - Szyfrowanie z kluczem symetrycznym
    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 lub co określoną liczbę bajtów, z użyciem specjalnych protokołów.

    * Data Encryption Standard DES, 3DES
    * RC - szyfr strumieniowy wykorzystywany w szyfrowaniu ramek w sieciach bezprzewodowych WiFi/WPA
    * Advanced Encryption Standard AES - szyfr blokowy, np WPA2
  - Szyfrowanie z kluczem asymetrycznym
    * Szyfrowanie i odszyfrowanie jest tu realizowane przy pomocy pary kluczy - prywatnym (tajnym) i publiczny (znany). Jeden szyfruje, drugi odszyfrowywuje.
    * Odgadnięcię 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 szyfrowany jest 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.
- Po podpisaniu dodatkowo możemy wiadomość zaszyfrować, ale to nie należy już do samego podpisu.

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 powinny zapewniać:

- Poufność przesyłanych danych (osoby niepowołane nie powinny móc odczytać danych).
- Autentyczność (dane pochodzą rzeczywiście od określonego źródła).
- Integralność (nikt danych nie zmienił).

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.

Protokoły szyfrujące przesyłane dane

- SSL (warstwa aplikacji) – Używany do zabezpieczania innych protokołów, wykorzystuje połączenie szyfrowania asymetrycznego z kluczem publicznym i symetrycznego. Często wykorzystywany z HTTP w sieci WWW (HTTPS).
- TLS (warstwa aplikacji) – Podobny do SSL.
- SMB - Server Message Block Signing, znany też jako Common Internet File System CIFS) – do transferu plików, umieszcza cyfrowe podpisy w każdym bloku danych.
- S/MIME – Secure Multpurpose Internet Mail Extensions – szyfruje i umieszcza podpisy cyfrowe w wiadomościach pocztowych e-mail. Jest rozszerzeniem MIME, standardu włączania danych binarnych do listów elektronicznych.
- IPSec (warstwa IP)

17.1 Protokół IPSec

- warstwa IP
- może szyfrować dane pochodzące z dowolnej aplikacji, proces szyfrowania i deszyfrowania jest niewidoczny dla użytkownika
- framework umożliwiający wykorzystanie pewnych protokołów (Authentication Headers AH i Encapsulating Security Payloads ESP)i metod według określonych zasad.

Cechy IPSec:

- Autentyczność i integralność danych.
  AH umożliwia sprawdzenie autentyczności komputerów uczestniczących w transmisji, umożliwia też sprawdzenie integralności danych. Nagłówek IP oraz dane są zabezpieczone przed modyfikacją.
- Szyfrowanie danych.
  ESP zapewnia 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. Polityki stosowania IPSec – w systemach Microsoft Windows ustala się politykę (zasadę, policy) kiedy IPSec ma być automatycznie zastosowany. W wersji Windows XP były trzy predefiniowane polityki:

- 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.

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).

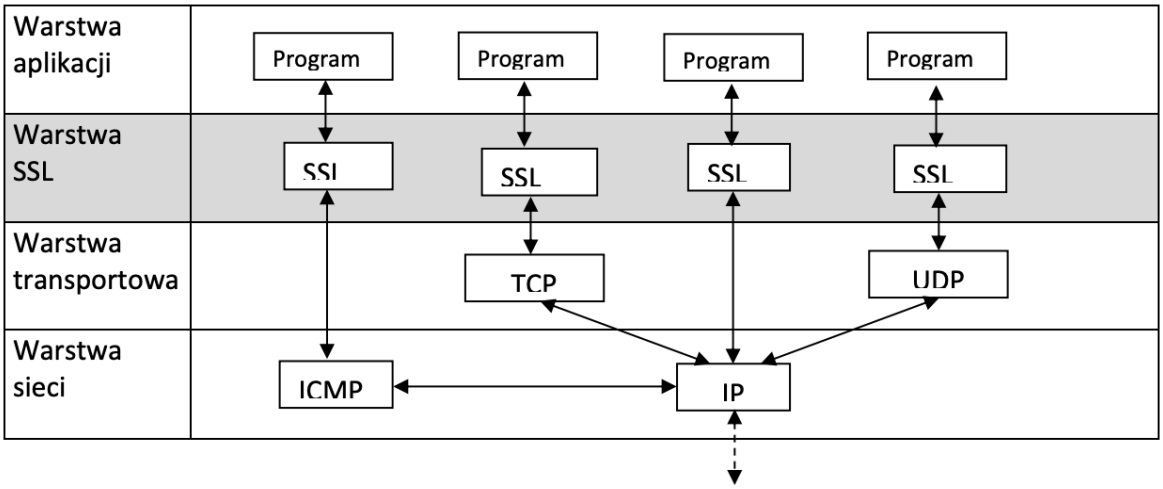
Metody uwierzytelniania w IPSec:

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

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.

17.1.1 SSL - Secure Socket Layer

- jego zadaniem jest zabezpieczanie informacji przesyłanych siecią.
- wykorzystywany przy przesyłaniu np. danych osobistych, numerów kart kredytowych.
- często prezentowany jako protokół, który leży powyżej warstwy transportu (TCP, UDP) i sieci (IP) a poniżej warstwy aplikacji (np. HTTP, FTP, SMTP, TELNET)
- W modelu ISO OSI jest przypisany do warstwy prezentacji (zatem do warstwy aplikacji w modelu TCP/IP)
- jest protokołem otwartym
- wykorzystuje szyfrowanie symetryczne z kluczem publicznym
- protokoły zabezpieczone SSL oznaczane są jako HTTPS (dla HTTP), FTPS (dla FTP) itd.



Podstawowe cechy protokołu SSL:

- Zapewnia autoryzację serwerów internetowych i (opcjonalnie) klientów (utrudnia podszywanie pod autoryzowanych usługodawców i użytkowników)
- Zapewnia szyfrowanie - poufność przesyłanych informacji.
- Stosuje sumy kontrolne dla zapewnienia integralności danych.

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.

Numery portów przy włączeniu SSL:

Protokół	Port standardowy	Port SSL
HTTP	80	443
IMAP4	143	993
POP3	110	995

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.

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

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