Sieci komputerowe

Warstwa sieci i warstwa transportowa

Ewa Burnecka / Janusz Szwabiński

ewa@ift.uni.wroc.pl / szwabin@ift.uni.wroc.pl

Model ISO/OSI

Warstwa aplikacji
Warstwa prezentacji
Warstwa sesji
Warstwa transportowa
Warstwa sieci
Warstwa łącza danych
Warstwa sprzętowa

Model TCP/IP

Warstwa aplikacji
Warstwa transportowa
Warstwa sieci
Warstwa łącza danych
Warstwa sprzętowa

Plan wykładu

1. Warstwa sieci
   - Protokół IP
   - Router i protokoły routingu
   - Protokół ICMP
   - IPv6
   - NAT
2. Warstwa transportowa
   - Porty i gniazda
   - Protokoły UDP i TCP
3. IPX/SPX

Protokół IP

Zadania

- definiuje format i znaczenie poszczególnych pól datagramu (jednostki danych)
- określa schemat adresowania używany w Internecie
- zapewnia wybór trasy poruszania się datagramu (ang. *routing*)
- w razie konieczności zapewnia podział danych na fragmenty oraz ich późniejsze połączenie

Cechy

- protokół bezpołączeniowy – nie ustanawia połączenia i nie sprawdza gotowości odległego komputera do odebrania danych
- protokół niepewny – nie zapewnia korekcji i wykrywania błędów transmisji

Budowa datagramu IP

Słowa	Bity								
	0	4	8	12	16	20	24	28	
1	Wersja	IHL	Typ usługi		Długość całkowita				Nagłówek
2	Identyfikator				Flagi	Przesunięcie fragmentacji			
3	Czas życia		Protokół		Suma kontrolna				
4	Adres źródła								
5	Adres przeznaczenia								
6	Opcje						Uzupełnienie		
	DANE								

Adresowanie IP

Przydział przestrzeni adresowej

- `http://www.ripe.net` (Europa)
- `http://www.arin.net` (Ameryka)
- `http://www.apnic.net` (Azja i obszar Pacyfiku)
- `http://www.afrinic.org` (Afryka)

Adres IP ma długość czterech bajtów

$\Rightarrow$ teoretycznie możliwe $2^{32} = 4294967296$

- w praktyce adresów do dyspozycji jest dużo mniej

Przykładowy adres

- w postaci binarnej:
  `10011100.00010001.01011000.10111001`
- w postaci dziesiętnej: `156.17.88.185`

Klasy adresów

`0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh`	-	klasa A
`10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh`	-	klasa B
`110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh`	-	klasa C
`1110xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx`	-	multicast
`1111xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx`	-	adresy zarezerwowane

`n` – bit adresu sieci w Internecie, `h` – bit adresu komputera w sieci

Klasa	Maksymalna ilość komputerów w sieci
A	$2^{24} - 2 = 16777214$
B	$2^{16} - 2 = 65534$
C	$2^{8} - 2 = 254$

Przykład Firma potrzebuje 300 adresów IP

- przestrzeń adresowa klasy C jest niewystarczająca
- dwie klasy C są niewygodne – dwie domeny w ramach firmy
- klasa B – zmarnowaniu ulegnie 65234 adresów

$\Rightarrow$ podział przestrzeni adresowej na klasy jest mało elastyczny i nieekonomiczny

Bezklasowe trasowanie międzydomenowe (CIDR)

- klasy zastępujemy maskami
- maska, podobnie jak adres IP, składa się z czterech bajtów
- do miejsca, gdzie w masce występują jedynki, w adresie IP mamy część określającą adres sieci
- bity adresu IP, którym w masce odpowiadają zera, identyfikują komputer w danej sieci

Przykład

adres IP:	156.17.88.185
maska:	255.255.255.192
adres IP:	10011100.00010001.01011000.10111001
maska:	11111111.11111111.11111111.11000000
adres sieci:	10011100.00010001.01011000.10000000
broadcast:	0011100.00010001.01011000.10111111
adres sieci:	156.17.88.128
broadcast:	156.17.88.191
adresy IP:	156.17.88.129 – 156.17.88.190

Sposoby zapisu

- `156.17.88.185/255.255.255.192`
- `156.17.88.185/26`

Uwaga praktyczna

- chcąc podzielić naszą sieć na 2^n podsieci, wydłużamy maskę o n bitów

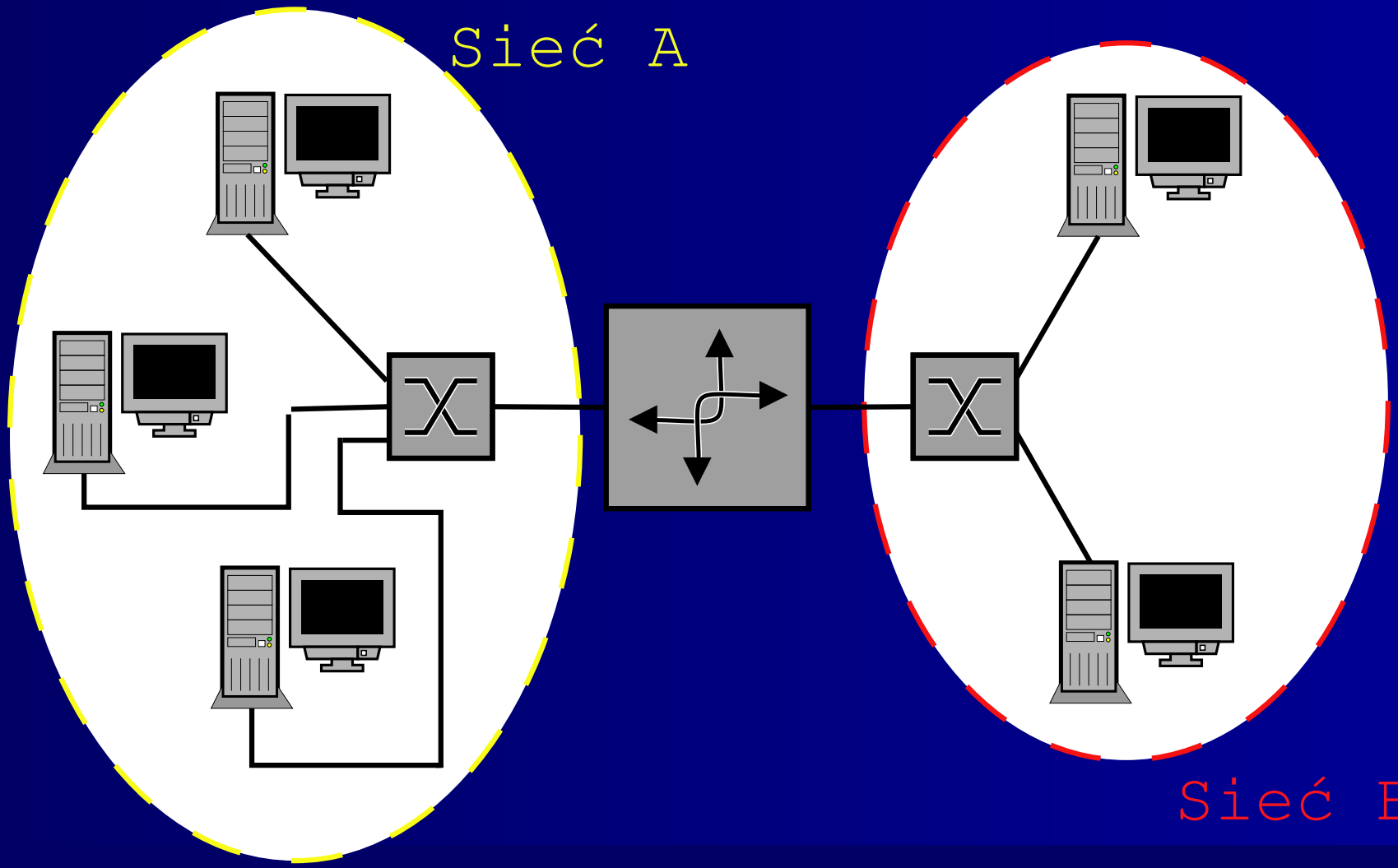
Adresy specjalne

- adres sieci dla Internetu: `0.0.0.0`
- adres rozgłoszeniowy dla Internetu (teoretycznie): `255.255.255.255`
- adres pętli (loopback address): `127.0.0.1/8`
- multicast
- adresy zarezerwowane

Klasy nieroutowalne

Klasa	Zakres
A	10.0.0.0 – 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

Router



- łączy ze sobą różne sieci
- oddziela domeny kolizji i domeny rozgłoszeniowe w sieciach Ethernet
- potrafi przekazywać dane między sieciami opartymi na różnych technologiach
- przesyła dane jak najlepszą i najszybszą drogą (na podstawie tablic routingu)
- może służyć jako „zapora ogniowa”

Tablica routingu

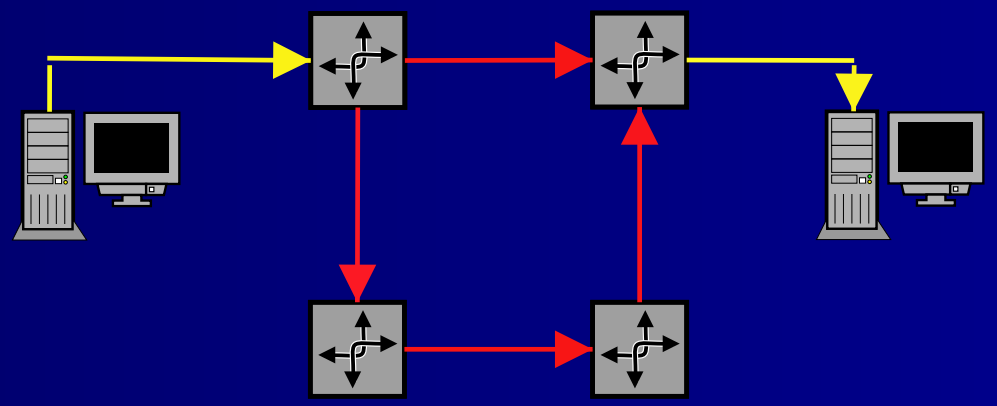
Przykład Tablica routingu komputera w sieci A

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
0.0.0.0	192.168.1.1	0.0.0.0	UG	0	0	0	eth0

Przykład Tablica routingu routera

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
10.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	eth1
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
0.0.0.0	10.0.0.1	0.0.0.0	UG	0	0	0	eth1

Protokoły routingu



Zadania

- wyszukiwanie nowych tras
- przekazywanie do innych routerów informacji o znalezionych trasach
- tworzenie tablic routingu

System autonomiczny

- grupa połączonych routerów, wykorzystujących ten sam protokół
- routery te są utrzymywane i zarządzane przez jedną organizację
- każda para routerów jest połączona ze sobą ścieżką (z wyjątkiem awarii)

Podział protokołów

- protokoły dla sieci o nieskomplikowanej budowie (*ad hoc network routing protocols*)
- wewnętrzne protokoły routingu (w pojedynczym systemie autonomicznym)
  - IGRP/EIGRP (*Interior Gateway Routing Protocol / Enhanced IGRP*)
  - OSPF (*Open Shortest Path First*)
  - RIP (*Routing Information Protocol*)
  - IS-IS (*Intermediate System to Intermediate System*)

- zewnętrzne protokoły routingu
  - EGP (*Exterior Gateway Protocol*)
  - BGP (*Border Gateway Protocol*)

RIP (RFC 1058 / RFC 1723)

- protokół oparty na algorytmie wektora odległości (algorytmie Bellmana-Forda)
- metryka odległości mierzona liczbą skoków (*hop count*)
- maksymalna dopuszczalna ilość skoków od źródła do celu wynosi 15

Budowa pakietu RIP

0	1	2	3
Polecenie	Wersja	Zero	
Rodzina adresów		Zero	
Adres IP			
Zero			
Zero			
Metryka			

Protokół ICMP

Internet Control Message Protocol (RFC 792)

Zadania

- sterowanie przepływem danych
- raportowanie o braku możliwości dostarczenia danych
- przekierowywanie tras
- testowanie osiągalności zdalnego komputera
- powiadamianie komputera źródłowego o usunięciu datagramu po przekroczenia czasu życia

Polecenia wykorzystujące ICMP

- `ping`
- `traceroute/tracert`

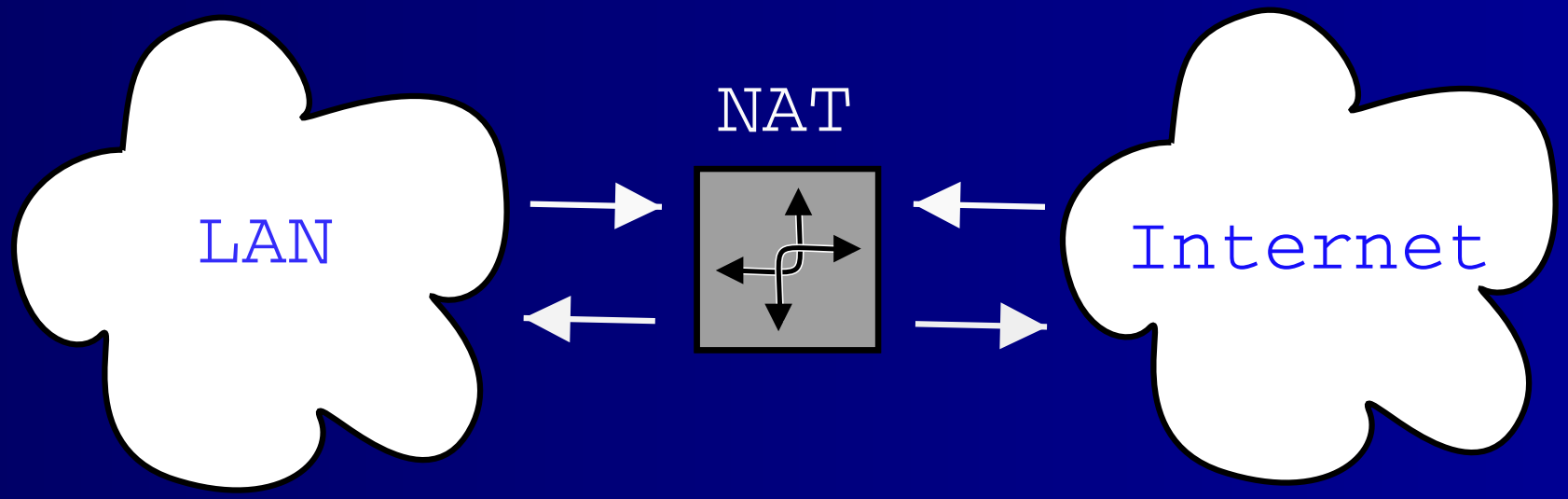
IPv6 – wersja szósta protokołu IP

- 128 bitowa długość adresu

  $\Rightarrow$ 2^{128} możliwych adresów

  $\Rightarrow$ 665 570 793 348 866 943 898 599 adresów na metr kwadratowy Ziemi
- nowy typ adresów: anycast
- prostszy nagłówek
- lepsze wsparcie dla sterowania przepływem danych w czasie rzeczywistym
- mechanizmy uwierzytelniania i szyfrowania
- konfiguracja nowych węzłów sieci na podstawie adresu MAC

NAT



Rodzaje

- statyczny NAT – adresy sieci lokalnej (na ogół nieroutowalne) są tłumaczone na adresy sieci zewnętrznej na zasadzie 1 do 1, tzn. komputer sieci lokalnej będzie miał zawsze ten sam adres zewnętrzny
- dynamiczny NAT – komputerowi z sieci lokalnej przyporządkowany jest jeden (pierwszy dostępny) z puli adresów zewnętrznych

- overloading – sieć lokalna odwzorowana jest na tylko jeden adres zewnętrzny. Router identyfikuje poszczególne komputery za pomocą portów

Komputer źródłowy	Adres IP	Port komp. źródłowego	Adres routera NAT	Port routera NAT
A	192.168.32.10	400	215.37.32.203	1
B	192.168.32.13	50	215.37.32.203	2
C	192.168.32.15	3750	215.37.32.203	3
D	192.168.32.18	206	215.37.32.203	4

- overlapping – kiedy adresy sieci lokalnej są również routowalne

Zalety

- oszczędność (nie tylko dostępnych adresów IP)
- bezpieczeństwo – sieć lokalna nie jest widoczna na zewnątrz; ataki na tą sieć są w rzeczywistości atakami na router, który jest na ogół dobrze zabezpieczony

Wartswa transportowa

Zadania protokołów warstwy transportowej

- rozdzielenie informacji nadchodzących z warstwy sieciowej
- dostarczenie tych informacji do odpowiednich procesów w warstwie aplikacji

Porty i gniazda

Port

- 16-bitowa liczba związana z procesem komunikującym się w sieci
- pozwala na identyfikację przynależności danej transmisji do konkretnego procesu

Gniazdo (*socket*)

- połączenie numeru IP komputera i numeru portu, na którym odbywa się komunikacja
- dwa gniazda jednoznacznie definiują transmisję w Internecie, np.:

  `62.211.243.226.80:216.239.33.101.6001`

Zasady przyznawania numerów portów

- liczba z zakresu od 0 do 65535
- zakres od 0 do 1024 to tzw. dobrze znane porty, zdefiniowane przez organizację IANA (`http://www.iana.org`)
- w systemie Linux porty poniżej 1024 to tzw. porty niskie, przeznaczone dla użytkownika `root`

Protokół UDP (*User Datagram Protocol*)

- bezpołączeniowy
- niepewny (ale za to efektywny)
- podstawową jednostką jest pakiet

Bity	
0	16 31
Port źródłowy	Port przeznaczenia
Długość	Suma kontrolna
Dane	

Protokół TCP (*Transmission Control Protocol*)

- połączeniowy
- niezawodny (potwierdzenie z retransmisją)
- protokół działa na strumieniach bajtów
- jednostką danych jest segment

<table>
<tr><td rowspan="2">Słowa</td><td colspan="8">Bity</td><td rowspan="2"></td></tr>
<tr><td>0</td><td>4</td><td>8</td><td>12</td><td>16</td><td>20</td><td>24</td><td>28</td></tr>
<tr><td>1</td><td colspan="4">Port źródłowy</td><td colspan="4">Port przeznaczenia</td><td rowspan="7">Nagłówek TCP</td></tr>
<tr><td>2</td><td colspan="8">Numer kolejny</td></tr>
<tr><td>3</td><td colspan="8">Numer potwierdzenia</td></tr>
<tr><td>4</td><td>Przes.</td><td colspan="3">Zarezerw. i Flagi</td><td colspan="4">Okno</td></tr>
<tr><td>5</td><td colspan="4">Suma kontrolna</td><td colspan="4">Wskaźnik pilności</td></tr>
<tr><td>6</td><td colspan="6">Opcje</td><td colspan="2">Uzupełnienie</td></tr>
<tr><td>7</td><td colspan="8">Dane</td><td></td></tr>
</table>

Nawiązanie połączenia

1. Host A wysyła segment z ustawioną flagą SYN. W segmencie podany jest inicjujący numer kolejny (ISN) danych
2. Host B odpowiada segmentem z flagami ACK (potwierdzenie odbioru) i SYN. W polu *numer kolejny* podaje własny ISN. *Numer potwierdzenia* jest równy numerowi kolejnemu otrzymanemu od hosta A
3. Host A wysyła segment potwierdzający odbiór (flaga ACK). W polu *numer potwierdzenia* znajduje się numer kolejny otrzymany od hosta B w poprzednim segmencie danych

- na zakończenie transmisji wymieniane są segmenty z flagą FIN

IPX/SPX, czyli protokoły Novella

IPX (*Internetwork Packet Exchange*)

- trasowalny
- zapewnia automatyczną konfigurację stacji po podłączeniu do sieci
- bezpołączeniowy i niepewny
- bardzo wydajny

SPX (*Sequence Packet Exchange*)

- połączeniowy i niezawodny
- przenoszony wewnątrz IPX

Budowa pakietu IPX

1 bajt	1 bajt	1 bajt	1 bajt
Suma kontrolna		Długość pakietu	
Kontrola transp.	Typ	Sieć docelowa	
Sieć docelowa		Węzeł docelowy	
Węzeł docelowy			
Gniazdo docelowe		Sieć źródłowa	
Sieć źródłowa		Węzeł źródłowy	
Węzeł źródłowy			
Gniazdo źródłowe		Dane	

Adresy IPX

4 bajty	6 bajtów	2 bajty
numer sieci	numer węzła	numer gniazda

Protokoły routowania

- RIP
- NLSP (*NetWare Link State Protocol*)