Warstwa sieciowa

mgr inż. Krzysztof Szałajko

Modele odniesienia

OSI		TCP/IP
7	Aplikacji	Aplikacji
6	Prezentacji	
5	Sesji	
4	Transportowa	Transportowa
3	Sieciowa	Internetowa
2	Łącza danych	Dostępu do sieci
1	Fizyczna	

Komunikacja

Warstwa sieciowa wykonuje 4 podstawowe zadania:

- Enkapsulacja / dekapsulacja
- Adresowanie
- Routing

Komunikacja

- Routing
  Wybranie odpowiedniej trasy przesyłu danych.

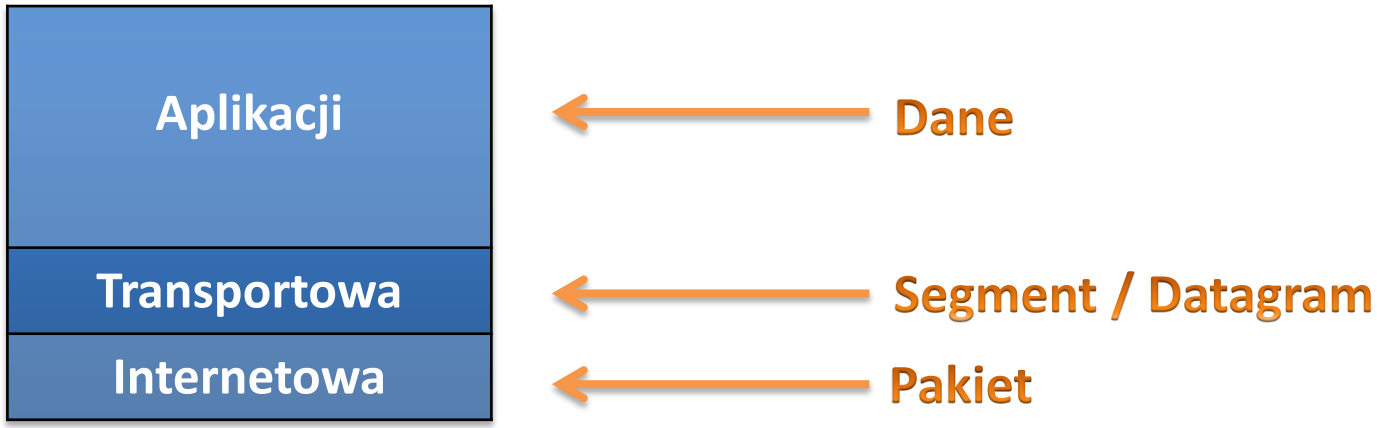
- Dekapsulacja
  Proces odwrotny do enkapsulacji. Odczytanie nagłówka, sprawdzenie adresu docelowego, usunięcie nagłówka, przekazanie PDU do warstwy 4.

Komunikacja

- Adresowanie
  Zapewniony mechanizm adresowania urządzeń końcowych – adresacja IP.

- Enkapsulacja
  Doklejenie do otrzymanej z warstwy 4 jednostki PDU nagłówka bądź etykiety.

Nazewnictwo



Przykładowe protokoły warstwy sieci

- IPv4
- IPv6
- Novell IPX
- AppleTalk

Internet Protocol

- IPv4
  - Jeszcze najczęściej wykorzystywany
  - Bezpołączeniowy
  - Best Effort
  - Niezależny od medium
- IPv6
  - Używany równolegle z IPv4, następnie wyprze „starszego brata”

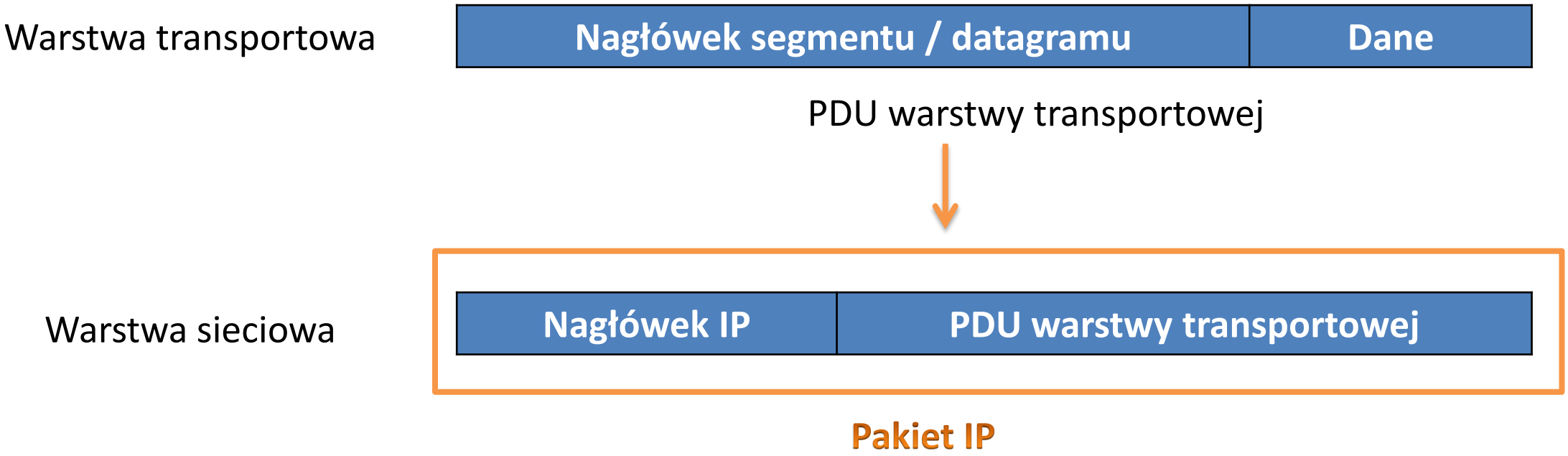
Bezpołączeniowość IP

- Pakiety wysyłane bez uprzedniego informowania o tym odbiorcy
- Brak dodatkowego nakładu – na utworzenie i podtrzymanie sesji
- Pakiety mogą dojść w zmienionej kolejności, ale to już „problem” warstwy aplikacji

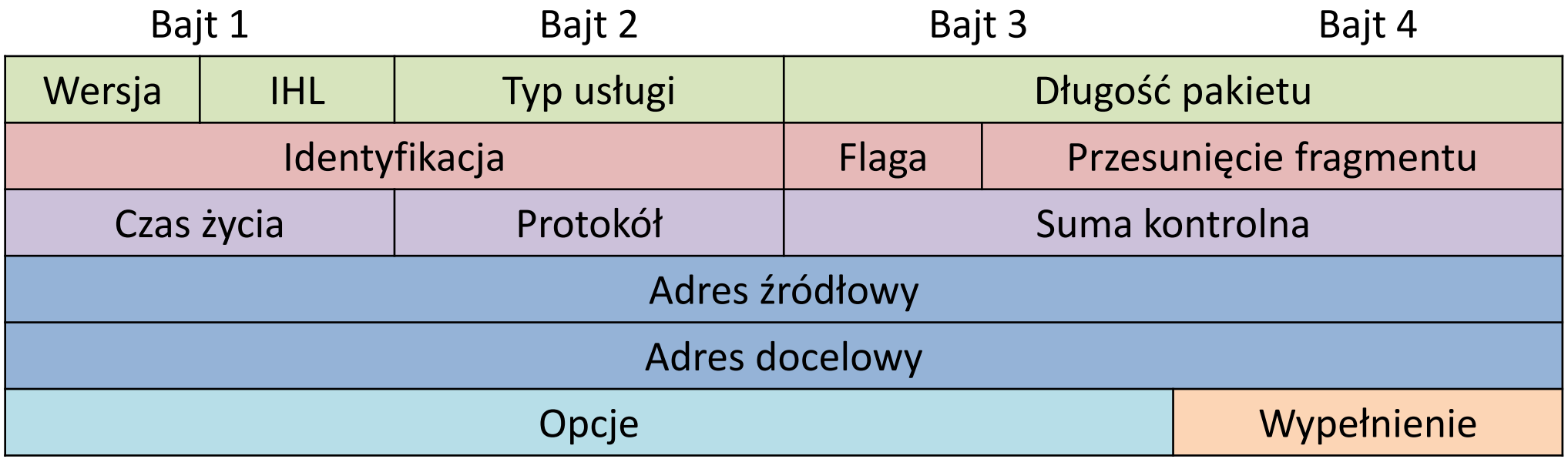
Best Effort Service

- Brak wymagania niezawodności
- Mniejsze obciążenie sieci
- Lepsza wydajność
- Brak zdolności zarządzania zagubionymi bądź uszkodzonymi pakietami oraz ich odzyskiwania

Tworzenie pakietu IP



Nagłówek pakietu IPv4



Nagłówek pakietu IPv4

- Adres źródłowy / adres docelowy

  Adresy IP hosta wysyłającego i odbierającego przesyłane pakiety. Adresy te pozostają niezmienione w czasie swojej podróży przez sieć. Adres źródłowy wykorzystany będzie przy ewentualnej odpowiedzi, docelowy natomiast przy przesyłaniu pakietu przez kolejne routery.

Nagłówek pakietu IPv4

- Czas życia – TTL – Time to live
  - 8 bitowa wartość binarna

  Liczba skoków, jakie wykona pakiet zanim zostanie odrzucony. Jest ona pomniejszana przy każdym skoku. Jest to mechanizm zapobiegający zapętlaniu się krążącego w sieci pakietu.

Nagłówek pakietu IPv4

- Protokół

  Informacja o tym, do jakiego protokołu przekazać dane warstwie wyższej po odebraniu pakietu przez hosta docelowego, np.:

  - 01 ICMP
  - 06 TCP
  - 17 UDP

Nagłówek pakietu IPv4

- Typ usługi – ToS – Type of Service

  Priorytet danych QoS. Umożliwia określanie przez router ważności przesyłanych danych, np. strumień danych głosowych będzie miał wyższy priorytet od statycznej strony internetowej.

Typy usługi ToS

Aplikacja	Minimalizacja opóźnień	Maksymalizacja szybkości przesyłania	Maksymalizacja poprawności	Minimalizacja kosztów	Wartość szesnast-k owa
Telnet/Rlogin	1	0	0	0	0x10
FTP					
kontrola	1	0	0	0	0x10
dane	0	1	0	0	0x08
dowolne dane masowe	0	1	0	0	0x08
TFTP	1	0	0	0	0x10
SMTP					
faza koment	1	0	0	0	0x10
faza danych	0	1	0	0	0x08
DNS					
zapytanie UDP	1	0	0	0	0x10
zapytanie TCP	0	0	0	0	0x00
transmisja obszaru	0	1	0	0	0x08
ICMP					
błąd	0	0	0	0	0x00
zapytanie	0	0	0	0	0x00
dowolne IGP	0	0	1	0	0x04
SNMP	0	0	1	0	0x04
BOOTP	0	0	0	0	0x00
NNTP	0	0	0	1	0x02

Nagłówek pakietu IPv4

- Przesunięcie fragmentu

  Określa porządek, w jakim należy poskładać pakiety w całość po dotarciu do hosta docelowego.

Nagłówek pakietu IPv4

- Flagi

  Znaczniki kontrolne:
  MF (more fragment) – 0 ostatni fragment, 1 więcej fragmentów
  DF (don`t fragment) – znacznik dozwoloności dzielenia pakietu

Nagłówek pakietu IPv4

- Wersja – wersja protokołu IP – 4
- IHL – długość nagłówka
- Długość pakietu – całkowita długość pakietu
- Identyfikacja – jednoznaczne identyfikowanie kolejnych fragmentów podzielonego pakietu
- Suma kontrolna – sprawdzenie błędów
- Opcje – miejsce dla innych usług

Dzielenie sieci

Bardziej praktycznym od łączenia hostów w jedną wielką sieć jest ich podział na wiele sieci.

W momencie coraz większego rozrastania się sieci zaczęto je dzielić na jeszcze mniejsze części – podsieci.

Problemy związane z dużymi sieciami:

- Spadek wydajności
- Bezpieczeństwo
- Zarządzanie adresami

Zwiększenie wydajności

- Duża liczba hostów w sieci generuje bardzo duży ruch – zarówno związany z danymi użytkowników, jak i dodatkowy, np. transmisja rozgłoszeniowa (informacja wysyłana do wszystkich komputerów w sieci)

Bezpieczeństwo

- Sieć może być zabezpieczona zarówno przed dostępem z zewnątrz jak i z wewnątrz, poprzez podział na odpowiednie podsieci ze względu na dostęp użytkownika

Adresowanie

- Przykład pocztowy:
  List wysłany z zagranicy do Jana Kowalskiego na ulicy TechnikInformatyk.pl 80 w Warszawie.
  W zagranicznym urzędzie pocztowym sprawdzą tylko, że list adresowany jest do Polski, reszta informacji ich nie interesuje. Po dotarciu do naszego kraju kierowany jest do Warszawy, tam dopiero pod odpowiedni adres…

Jest to przykład adresowania hierarchicznego.

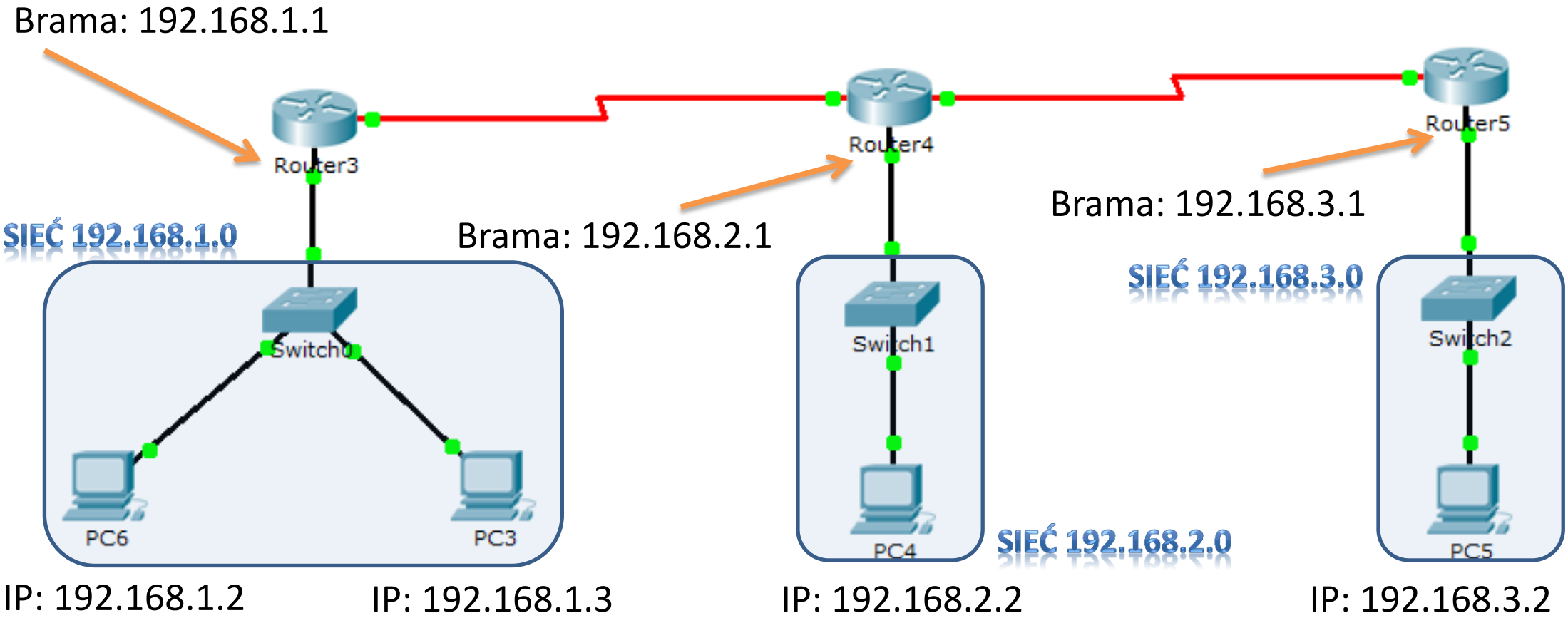
Adresowanie

32 bitowy adres IPv4 jest adresem hierarchicznym. Składa się z 2 części:

- Identyfikującej sieć
- Identyfikującej hosta

```
Adres IPv4. . . . . . . . . . . . : 192.168.0.102
```

Komunikacja na zewnątrz sieci



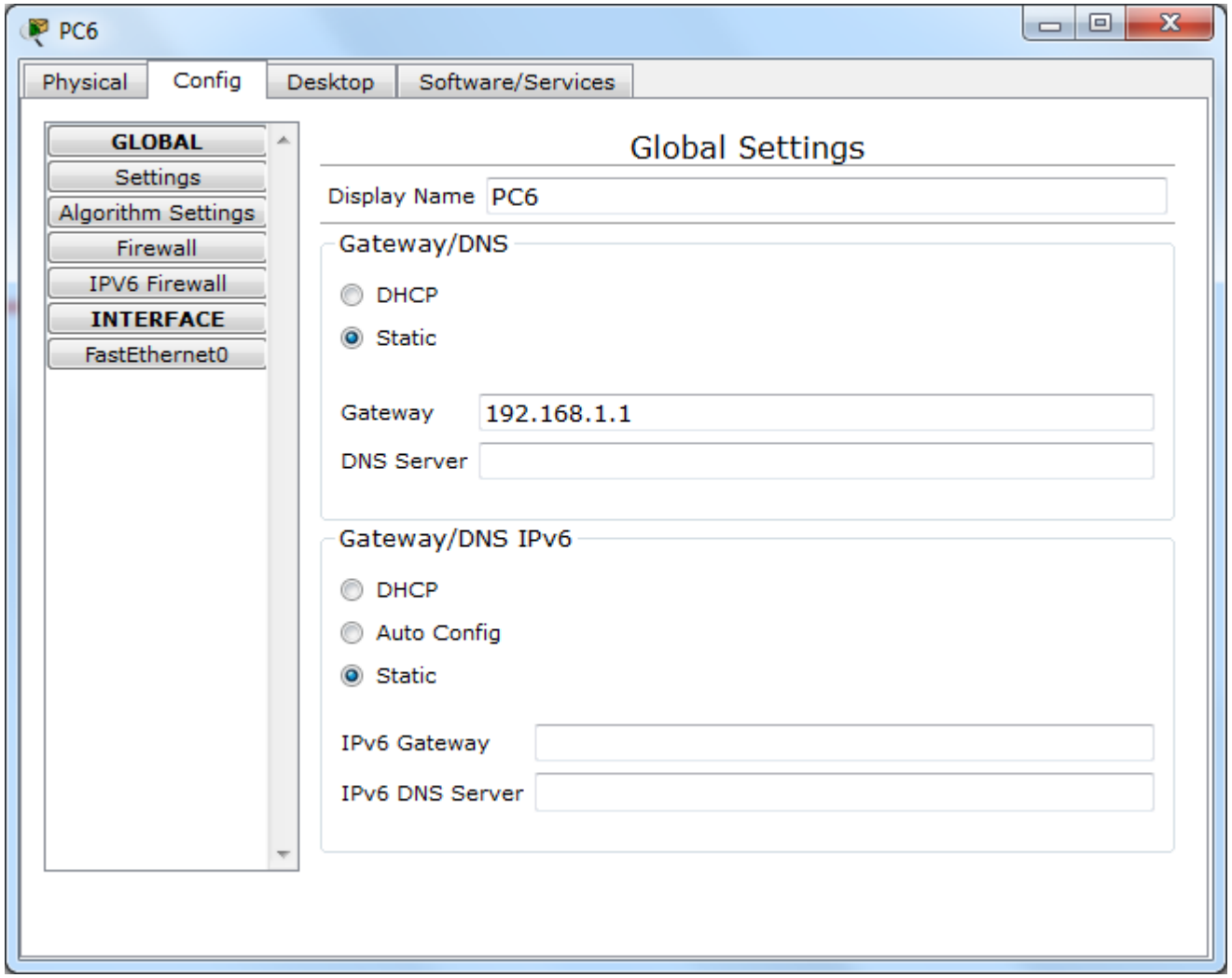
Komunikacja na zewnątrz sieci

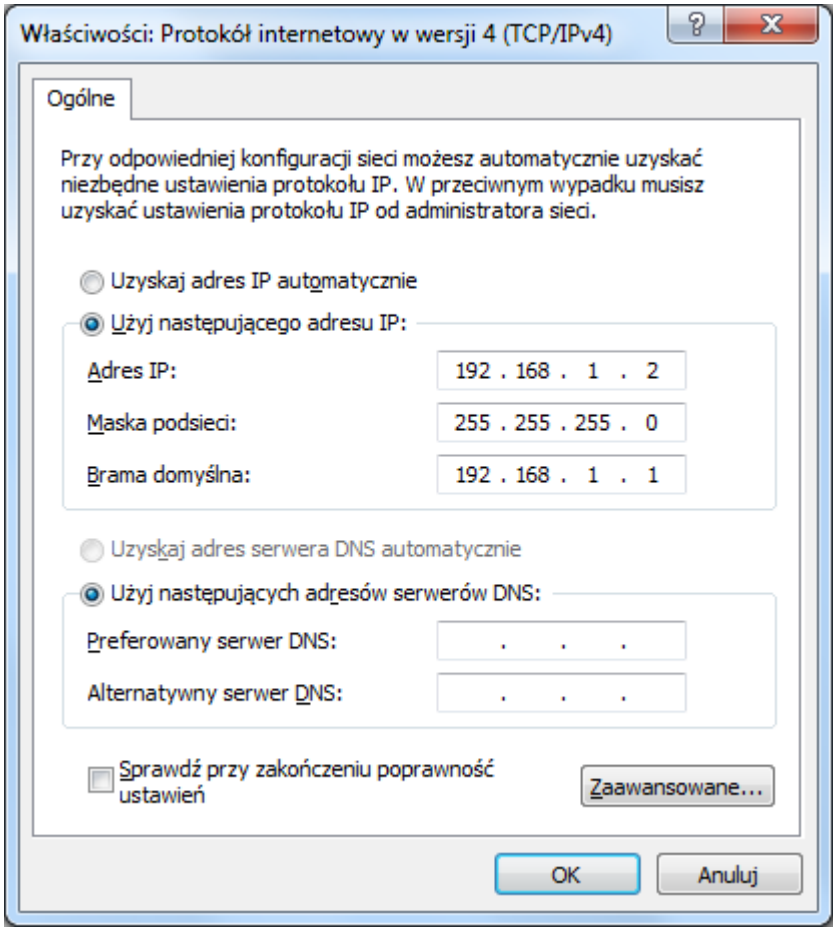
- W obszarze jednej sieci urządzenia komunikują się między sobą bez pośrednictwa urządzeń warstwy sieci
- Przy konieczności komunikacji z inną siecią router pełni rolę bramy
- Jeżeli router zna trasę, przekaże pakiet do następnego routera na ścieżce prowadzącej do urządzenia docelowego – next-hop

Brama domyślna

- Potrzebna do wysłania pakietu poza sieć lokalną
- Jeśli część sieciowa docelowego adresu IP jest inna od sieci, z której jest wysyłany, pakiet będzie przekazany poza sieć źródłową
- Każdy z hostów danej sieci ma ten sam adres bramy domyślnej

Brama domyślna





Routing

- Sieć docelowa może się znajdować o wiele przeskoków od sieci źródłowej
- Każdy router wskazuje tylko przeskok do kolejnego
- Proces routingu polega na znalezieniu trasy poprzez ustalenie kolejnego przeskoku na podstawie adresu docelowego oraz przekazanie tam pakietu

Tablica routingu

- Zawiera informacje o przyłączonych i odległych sieciach
  - Sieci przyłączone – połączone bezpośrednio
  - Sieci odległe – znajdujące się minimum 1 przeskok dalej od sieci przyłączonej
- Trasy do sieci mogą być skonfigurowane ręcznie bądź uzyskane automatycznie dzięki protokołom routingu

Tablica routingu hostów

- Hosty automatycznie dodają adresy sieci przyłączonych
- Skonfigurowana brama domyślna staje się lokalną trasą domyślną
- Zawiera trasy do sieci bezpośrednio przyłączonych do hosta
  - netstat –r
  - route PRINT

Routing

- Każdy pojedynczy pakiet jest traktowany indywidualnie na całej trasie przeskoków
- Sprawdzany jest adres docelowy, wybierana trasa
- Pakiet może zostać:
  - Przesłany do routera kolejnego przeskoku
  - Przesłany do hosta docelowego
  - Odrzucony

Routing

- Router otrzymuje dane w postaci ramki warstwy 2 modelu OSI. Dekapsuluje on ramkę do postaci pakietu warstwy 3.
- Wydobywa adres docelowy IP
- Przeszukuje tablicę routingu
- Ponownie enkapsuluje pakiet
- Wysyła pakiet zgodnie z wpisem w tablicy routingu

Trasa domyślna

- Jeśli router nie odnajdzie w tablicy routingu adresu kolejnego przeskoku zgodnego dla danego docelowego adres IP, a ma skonfigurowaną trasę domyślną, to na nią wyśle ponownie zenkapsulowany pakiet.
- Jeśli w tej sytuacji nie ma trasy domyślnej, pakiet jest odrzucany.

Routing statyczny

- Ręcznie skonfigurowane trasy do sieci odległych wraz z adresem kolejnego przeskoku

Routing dynamiczny

- Routery dzielą się dynamicznie informacjami o trasach za pomocą protokołów routingu
- Jeśli dany router wykryje zmiany w sieciach dla których pełni rolę bramy, bądź w połączeniach z innymi routerami – przekazuje tą informację do innych routerów

Routing dynamiczny

Protokoły routingu:

- **RIP** (Routing Information Protocol)
- **EIGRP** (Enhanced Interior Gateway Routing Protocol)
- **OSPF** (Open Shortest Path First)

Routing statyczny / dynamiczny

- Routing statyczny
  - Brak dodatkowego nakładu – zmniejszenia przepustowości sieci
  - Kłopotliwa konfiguracja
- Routing dynamiczny
  - Dodatkowy nakład – wymiana informacji pomiędzy routerami

Protokół ICMP

Internet Control Message Protocol

Protokół sieciowy wykorzystywany w diagnostyce i trasowaniu. Pełni funkcję kontroli transmisji w sieci.

Przykłady wykorzystania: ping, traceroute.

Protokół ICMP - ramka

Typ	Kod	Suma kontrolna
Dane (opcjonalnie)		

0	Echo Reply (zwrot echa – "odpowiedź na ping")
1 - 2	Zarezerwowane
3	Destination Unreachable (nieosiągalność miejsca przeznaczenia)
4	Source Quench (tłumienie nadawcy)
5	Redirect Message (zmień trasowanie)
6	Alternate Host Address (alternatywny adres hosta)
7	Zarezerwowane
8	Echo Request (żądanie echa)
9	Router Advertisement (ogłoszenie routera)
10	Router Solicitation (wybór routera)
11	Time Exceeded (przekroczenie limitu czasu)
12	Parameter Problem (Problem z parametrem)
13	Timestamp (żądanie sygnatury czasowej)
14	Timestamp Reply (zwrot sygnatury czasowej)
15	Information Request (żądanie informacji)
16	Information Reply (zwrot informacji)
17	Address Mask Request (żądanie maski adresowej)
18	Address Mask Reply (zwrot maski adresowej)
19	Zarezerwowane dla bezpieczeństwa
20-29	Zarezerwowane
30	Traceroute (śledzenie trasy)
31	Datagram Conversion Error (błąd konwersji datagramu)
32	Mobile Host Redirect (zmiana adresu ruchomego węzła)
33	IPv6 Where-Are-You (Pytanie IPv6 "gdzie jesteś")
34	IPv6 Here-I-Am (Odpowiedź IPv6 "tu jestem")
35	Mobile Registration Request (prośba o rejestrację węzła ruchomego)
36	Mobile Registration Reply (odpowiedź na prośbę o rejestrację węzła ruchomego
37	Domain Name Request (żądanie nazwy domeny)
38	Domain Name Reply (zwrot nazwy domeny)
39	SKIP Algorithm Discovery Protocol
40	Photuris, Security failures
41-255	Zarezerwowane

Typy wiadomości ICMP

Protokół ICMP

Przykłady wykorzystania:

- Zbytnie obciążenie routera, zwolnienie szybkości napływania pakietów
- Zmiana trasy routingu
- Host nieosiągalny – wysyłany przez ostatnią bramę
- Komunikat o odrzuceniu pakietu z powodu przekroczenia liczby hopów TTL

TechnikInformatyk.pl

Wszelkie Uwagi i Spostrzeżenia:

kontakt@technikinformatyk.pl