

# Specyfikacja zagadnień

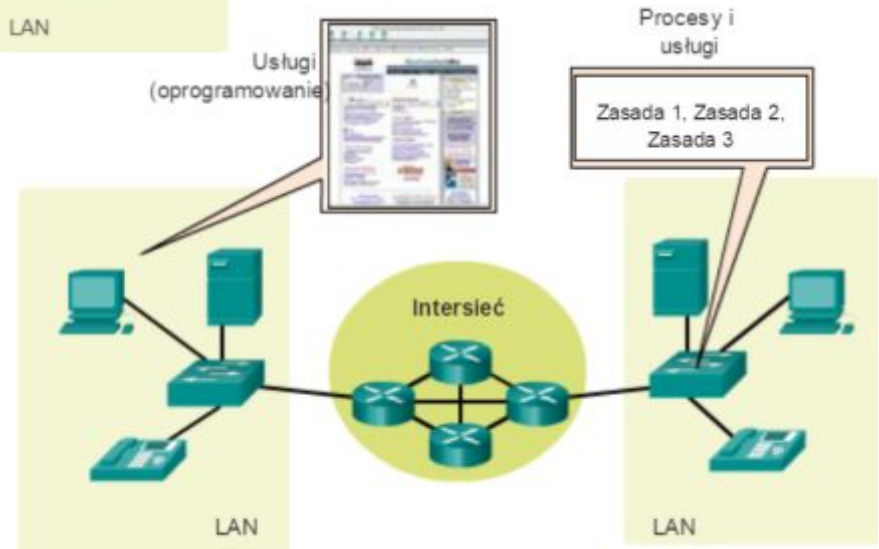
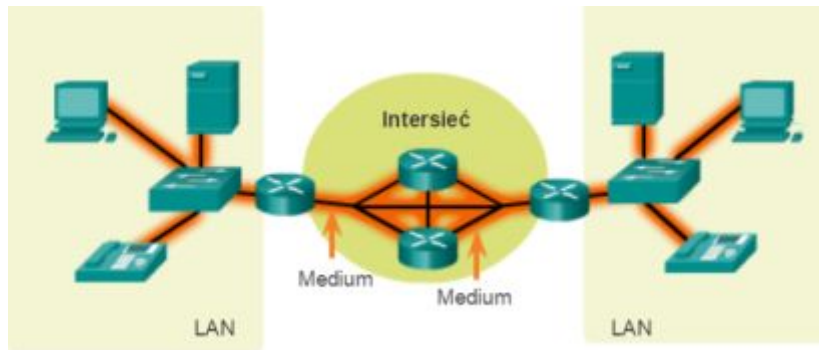
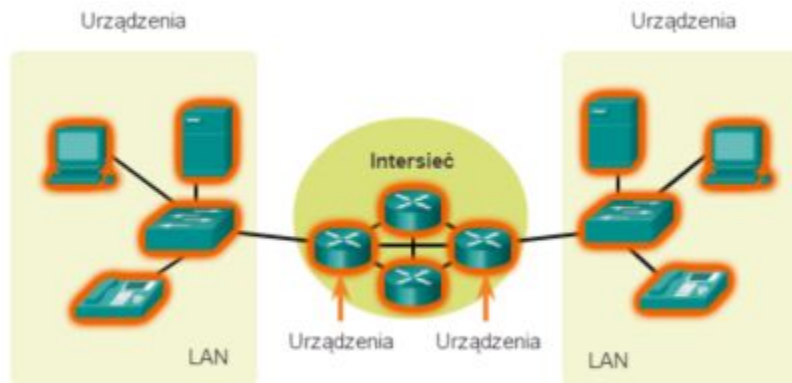
Sieci

- Co to jest sieć?
- Rozmiary sieci (dom, małe biuro, Średnia firma, globalny)
- Wspomaganie (komunikacja, praca, nauka, zabawa)
- Serwery i klienci

# Komponenty sieci

Sieci składają się z trzech elementów, do których zaliczamy:

- urządzeń
- media
- usługi



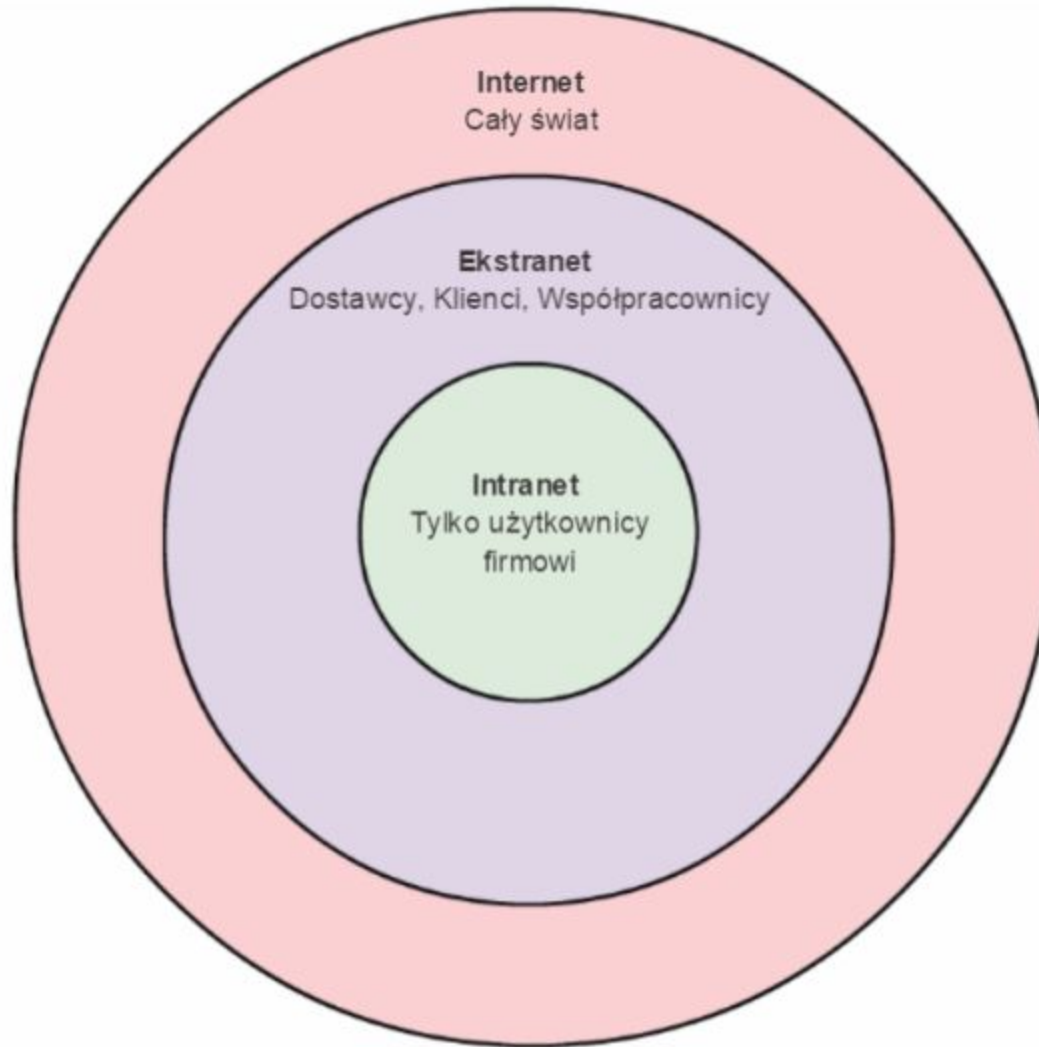
# Komponenty sieci

- Urządzenia końcowe (komputery, drukarki, ....)
- Media (bezprzewodowe i przewodowe – miedziane i światłowody)
- Urządzenia sieciowe (dostępowe – switch, koncentrator ....., łączące sieci - router, bezpieczeństwo – firewall)
- Topologie – fizyczne (peer-to-peer, gwiazda, ....) i logiczne (Ethernet, Token-ring)

- Typy sieci (WAN, LAN, MAN, SAN, Pan, WLAN)
- Opcje połączeń (dzierżawione, DSL, modem ...)
- Wspieranie architektury (skalowalność, tolerancja błędów, QoS, bezpieczeństwo....)
- Trendy w sieciach (praca grupowa, chmura obliczeniowa, komunikacja video, centra danych, PoE....)

Sieci LAN i WAN i Internet

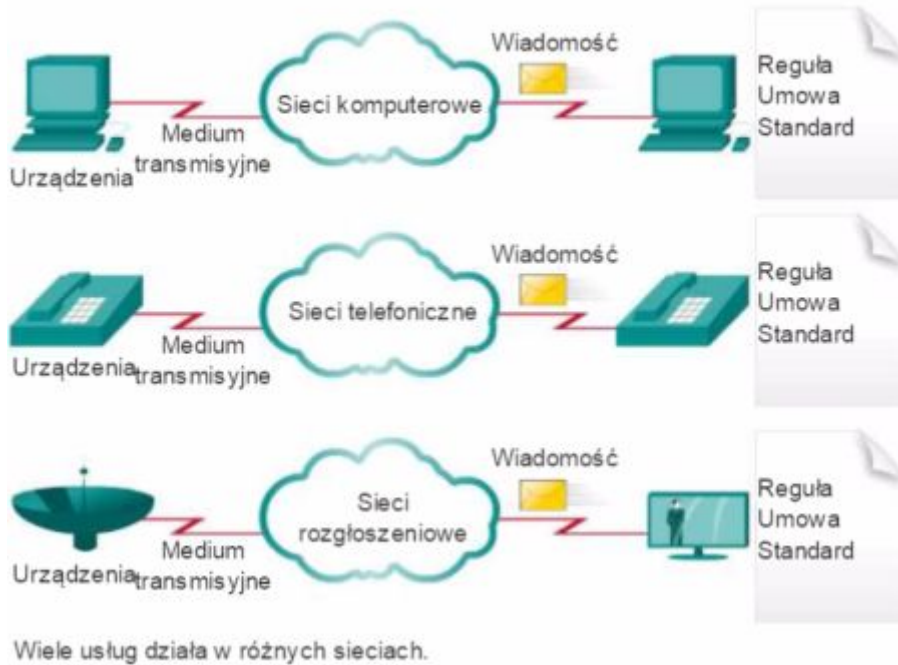
# Intranet i Extranet



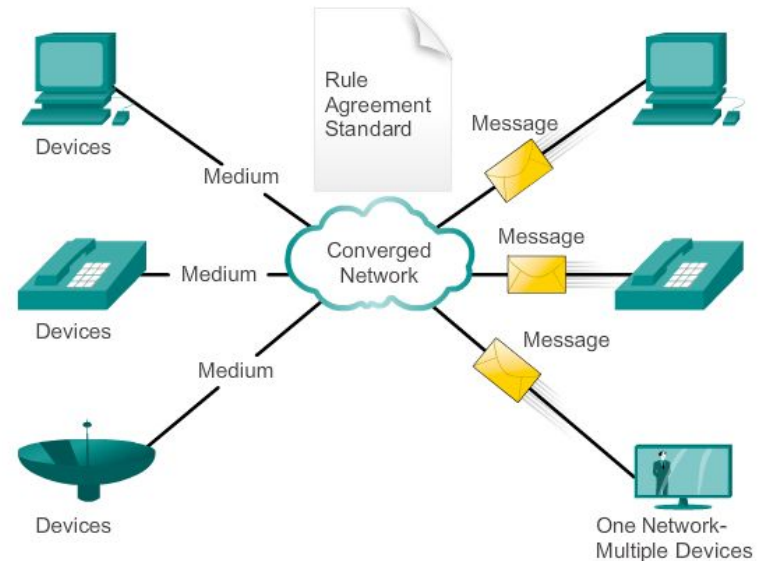
## Sieci konwergentne

# Konwergencja sieci

Wiele sieci



Converged Networks



Converged data networks carry multiple services on one network.

Niezawodność sieci

# Zapewnianie bezpieczeństwa sieci

Bezpieczeństwo sieci jest ważnym czynnikiem podczas korzystania z sieci



Transmisja poufnych, z punktu widzenia użytkownika, danych i informacji jest zabezpieczona przed dostępem niepowołanych osób.

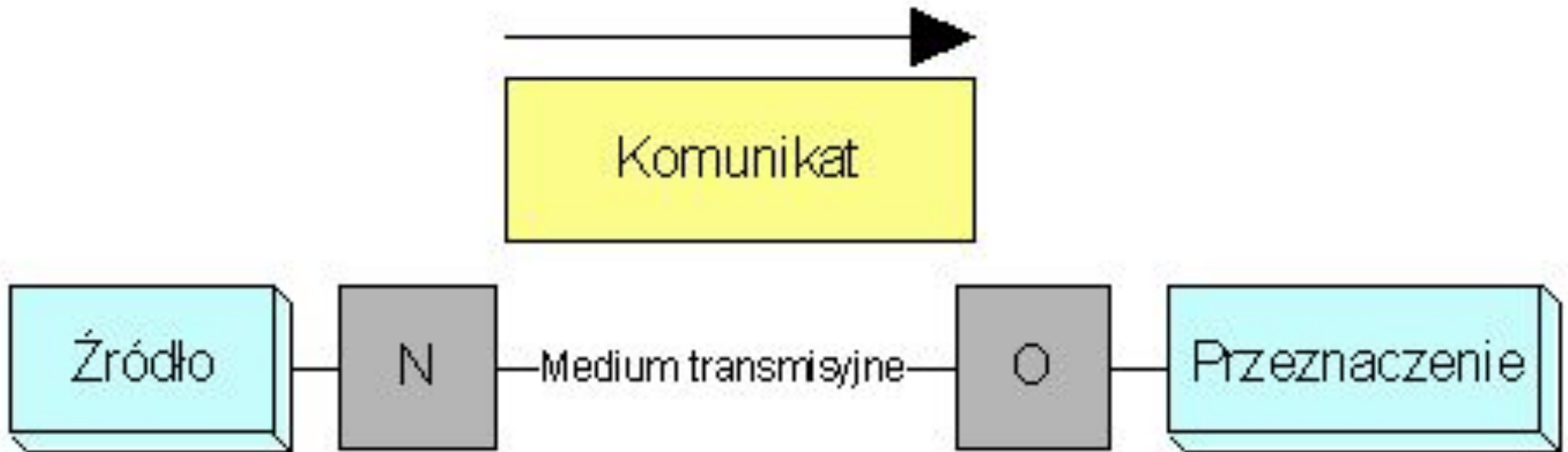


# Protokoły sieciowe i komunikacja

**Sieć** jest systemem komunikacji komputerów między sobą poprzez medium transmisyjne z użyciem określonych protokołów komunikacyjnych.

**Protokołem komunikacyjnym** określa się zespół zasad i reguł przekazywania komunikatów między komputerami – stacjami sieciowymi.

**Medium transmisyjne** jest to nośnik umożliwiający rozchodzenie się informacji w postaci prądu elektrycznego, fali elektromagnetycznej, świetlnej, akustycznej, itp.



# Reguły

- identyfikacja nadawcy i odbiorcy,
- uzgodnienie metody komunikacji (bezpośrednia, przez telefon, list, fotografia),
- wspólny język i gramatyka,
- szybkość i czas dostarczenia,
- wymagania dotyczące potwierdzenia otrzymania wiadomości

# Opcje dostarczenia wiadomości

- Unicast
- Multicast
- Broadcast

# Protokoły sieciowe

- Idea
- współdziałanie

## Zestawy protokołów

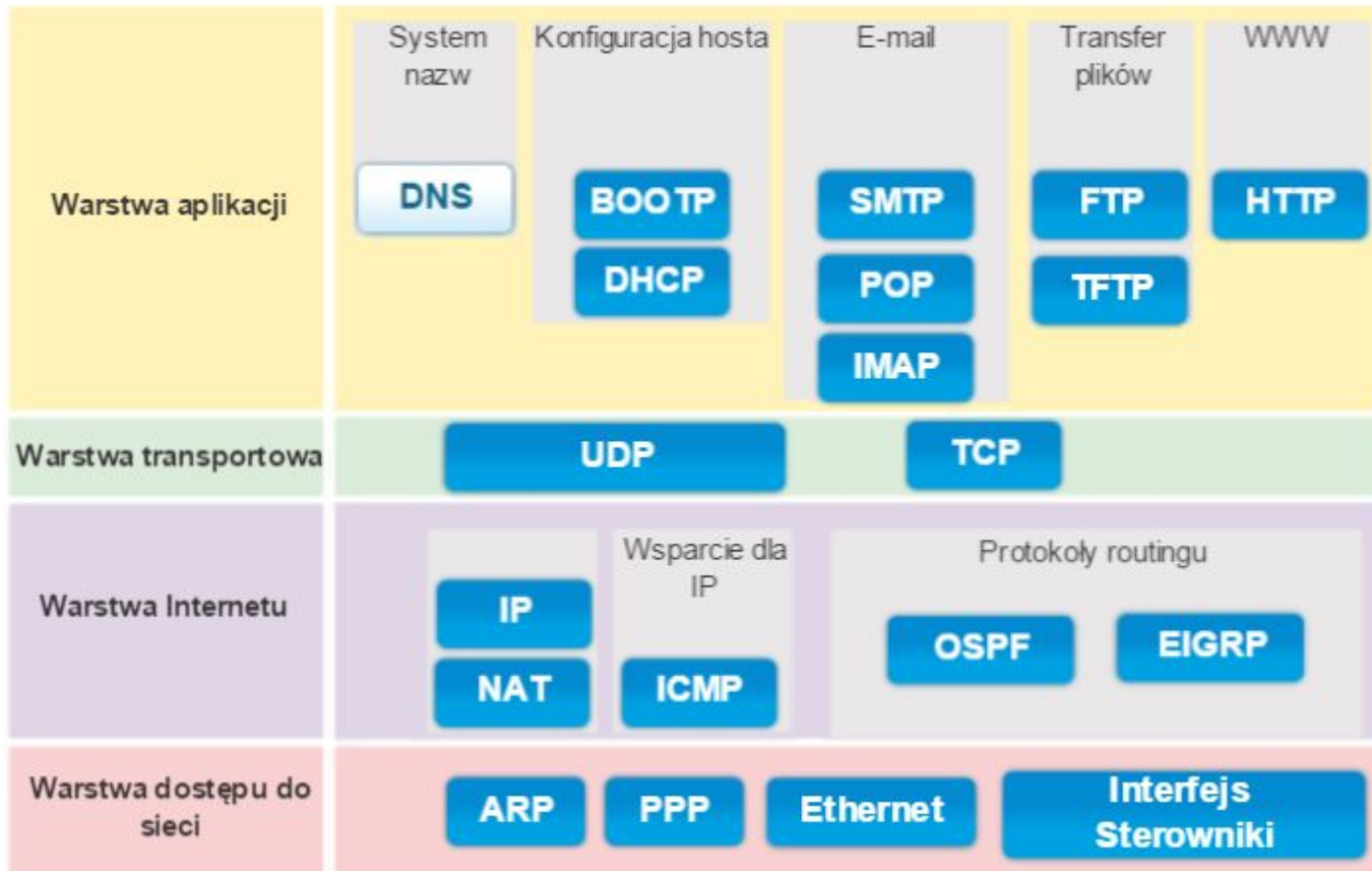
# Zestawy protokołów i standardy przemysłowe

### Zestawy protokołów i standardy przemysłowe

TCP/IP	ISO	AppleTalk	Novell NetWare
HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE	AFP	NDS
TCP UDP	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
IPv4 IPv6 ICMPv4 ICMPv6	CONP/CMNS CLNP/CLNS	AARP	IPX
Ethernet PPP Frame Relay ATM WLAN			

# Stos protokołów TCP/IP i komunikacja

Zestaw protokołów TCP/IP i proces komunikacji



# *Model warstwowy sieci*

## **1978 r. - wzorcowy model warstwowy sieci (ISO/OSI):**

- nadanie nazw;
- określenie zadań.

## **Warstwy umożliwiają:**

- przesyłanie informacji między sieciami o różnych technologiach;
- współdziałanie różnorodnego sprzętu, urządzeń i programów;
- zrozumienie działania sieci;
- dzielenie komunikacji i ułatwienie pracy;
- dokonywanie zmian w warstwie nie zmienia struktury pozostałych.



# Warstwy sieci komputerowych

## Usługi komunikacyjne:

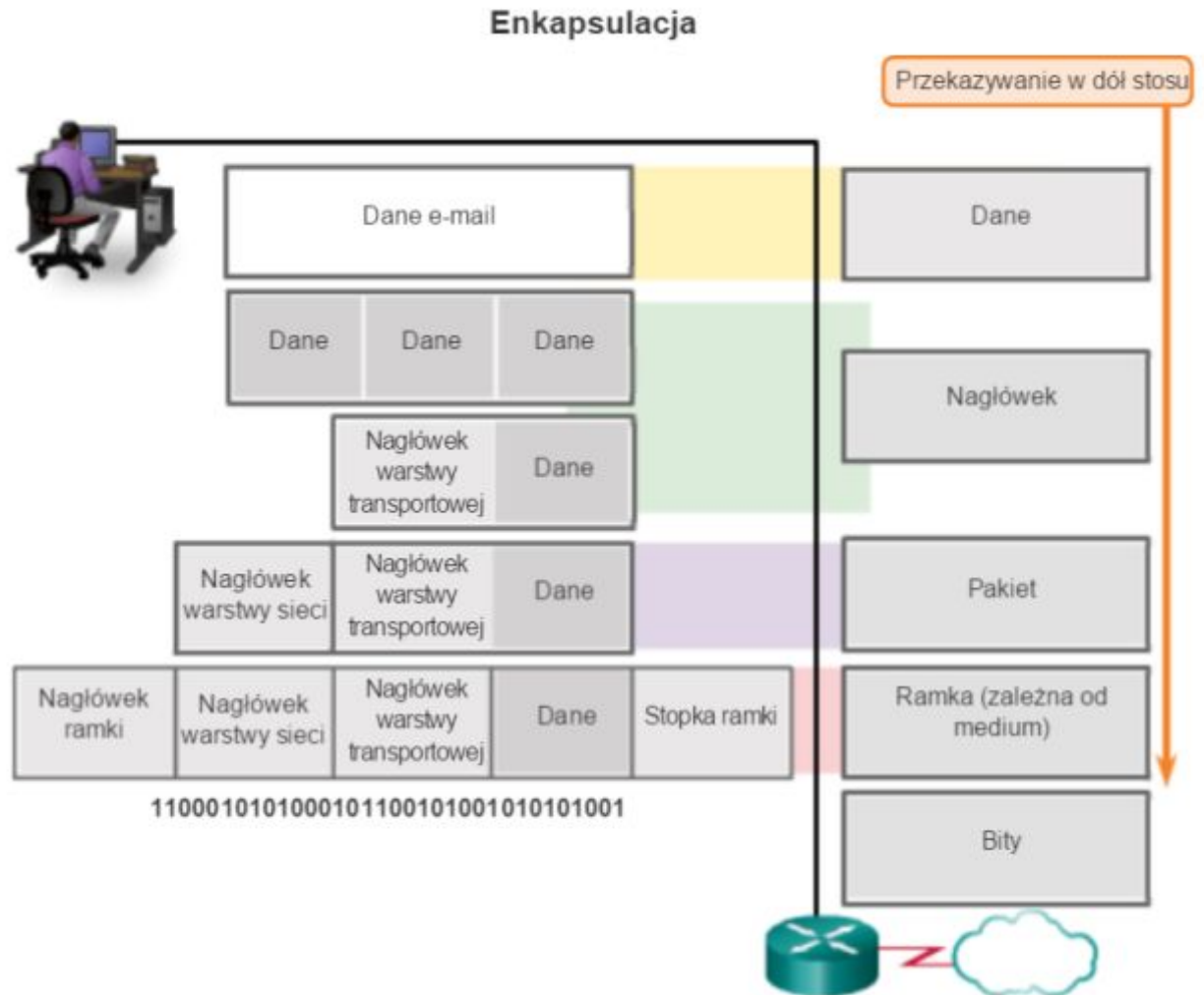
aplikacji	VII	aplikacji	• dostęp do zasobów innych użytkowników; • drukowanie w sieci;
	VI	prezentacji	
	V	sesji	
przeptywu	IV	transportu	• obsługa poczty elektronicznej; • przesyłanie i przeglądanie plików; • przyłączanie terminali.
	III	sieciowa	
	II	łączna danych	
	I	fizyczna	

OPROGRAMOWANIE W STOSIE PROTOKOŁÓW **OSI**,  
KTÓRE UDOSTĘPNIĄ PUNKT STARTOWY DLA SESJI  
KOMUNIKACJI.

## Enkapsulacja danych

# Jednostka danych protokołu PDU (ang. Protocol Data Unit)

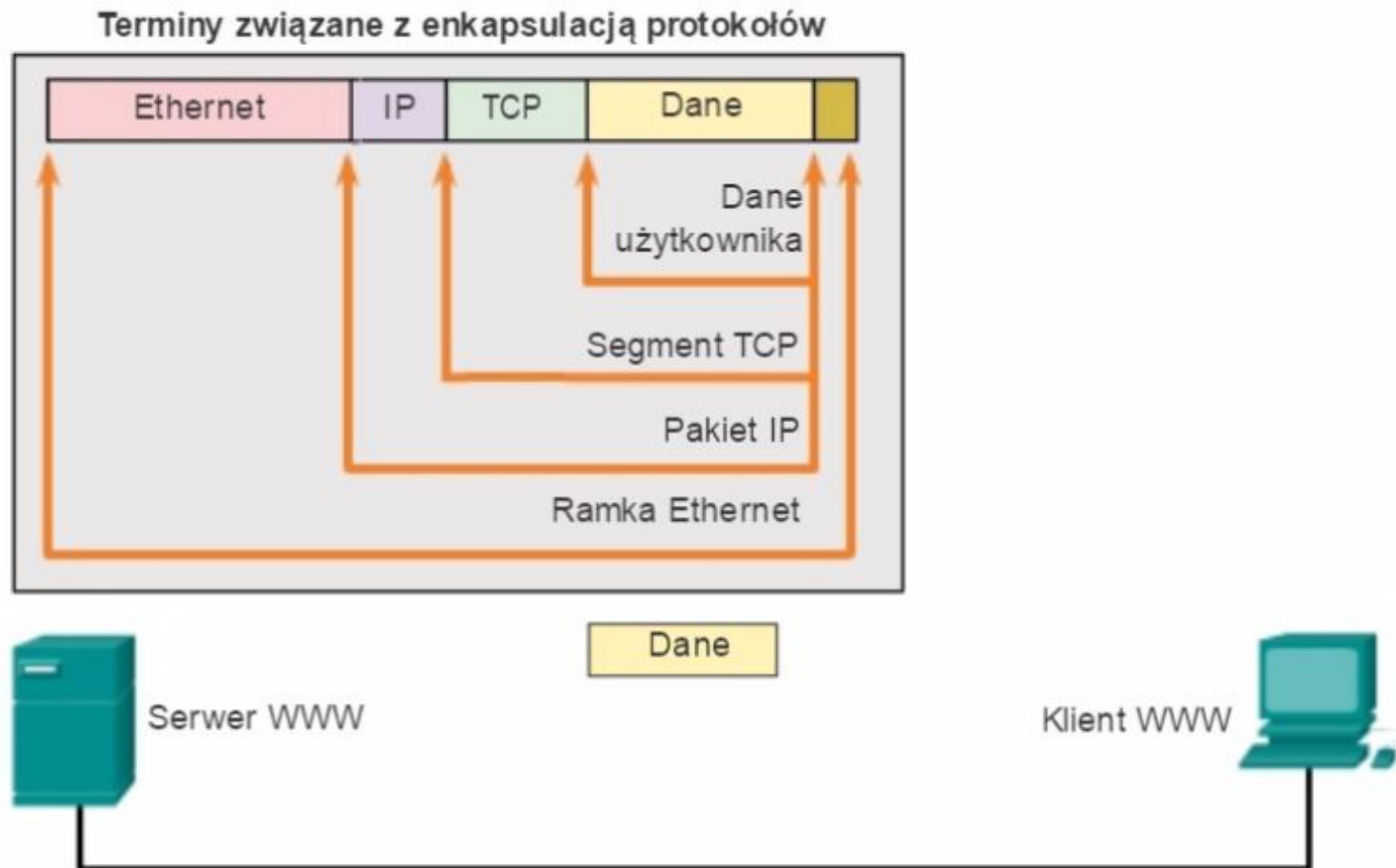
- Dane
- Segment
- Pakiet
- Ramka
- Bity



# Enkapsulacja danych

## Enkapsulacja

Działanie protokołu podczas wysyłania wiadomości

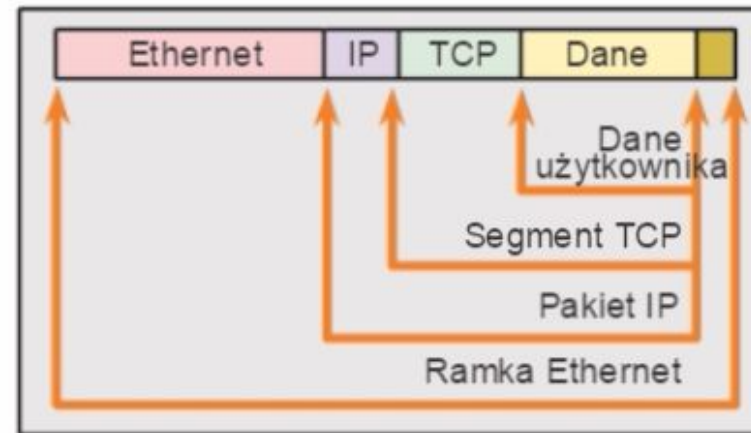


# Enkapsulacja danych

# Dekapsulacja

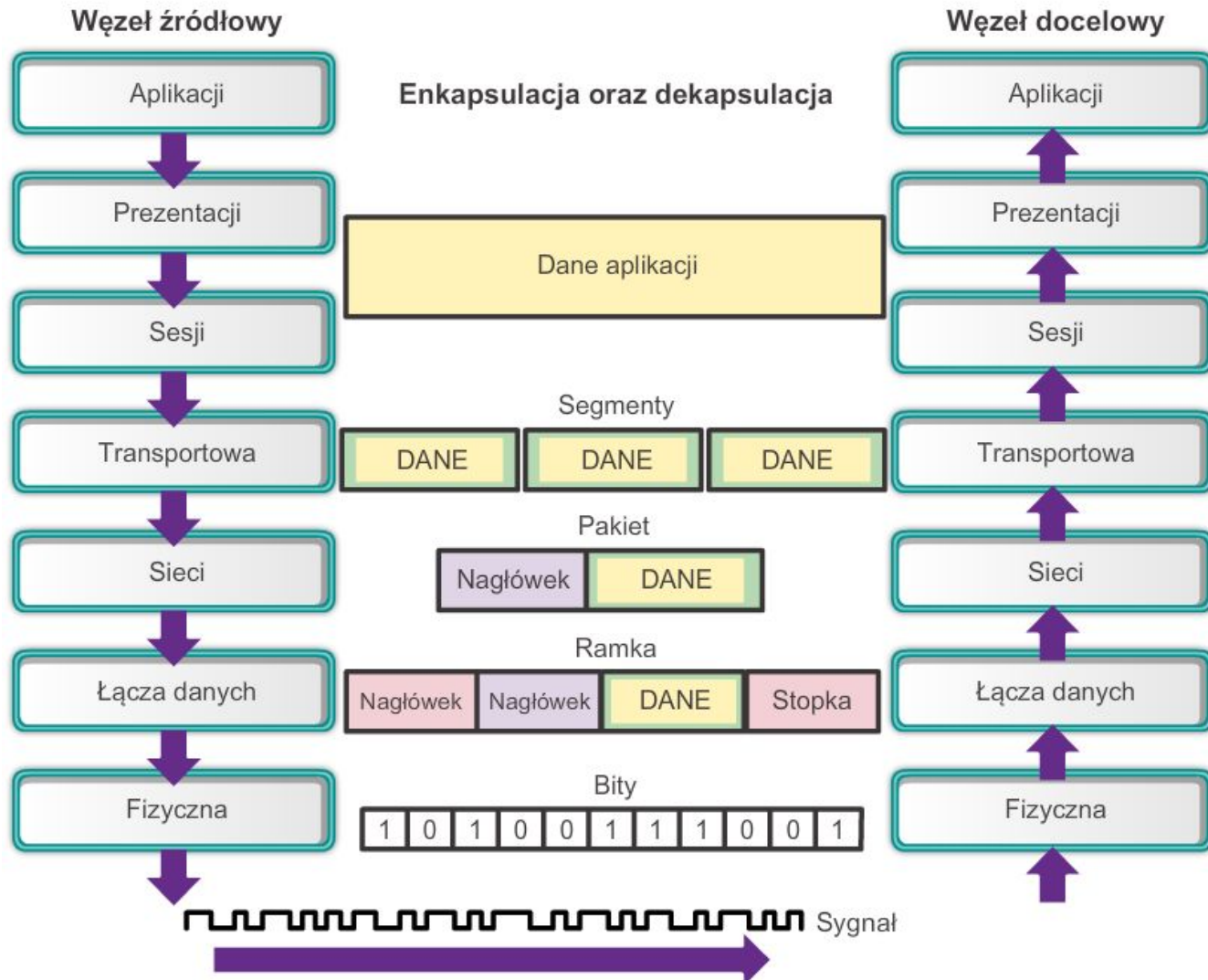
Działanie protokołu podczas odbierania wiadomości

Terminy związane z enkapsulacją  
protokołów



## Warstwa fizyczna - cele

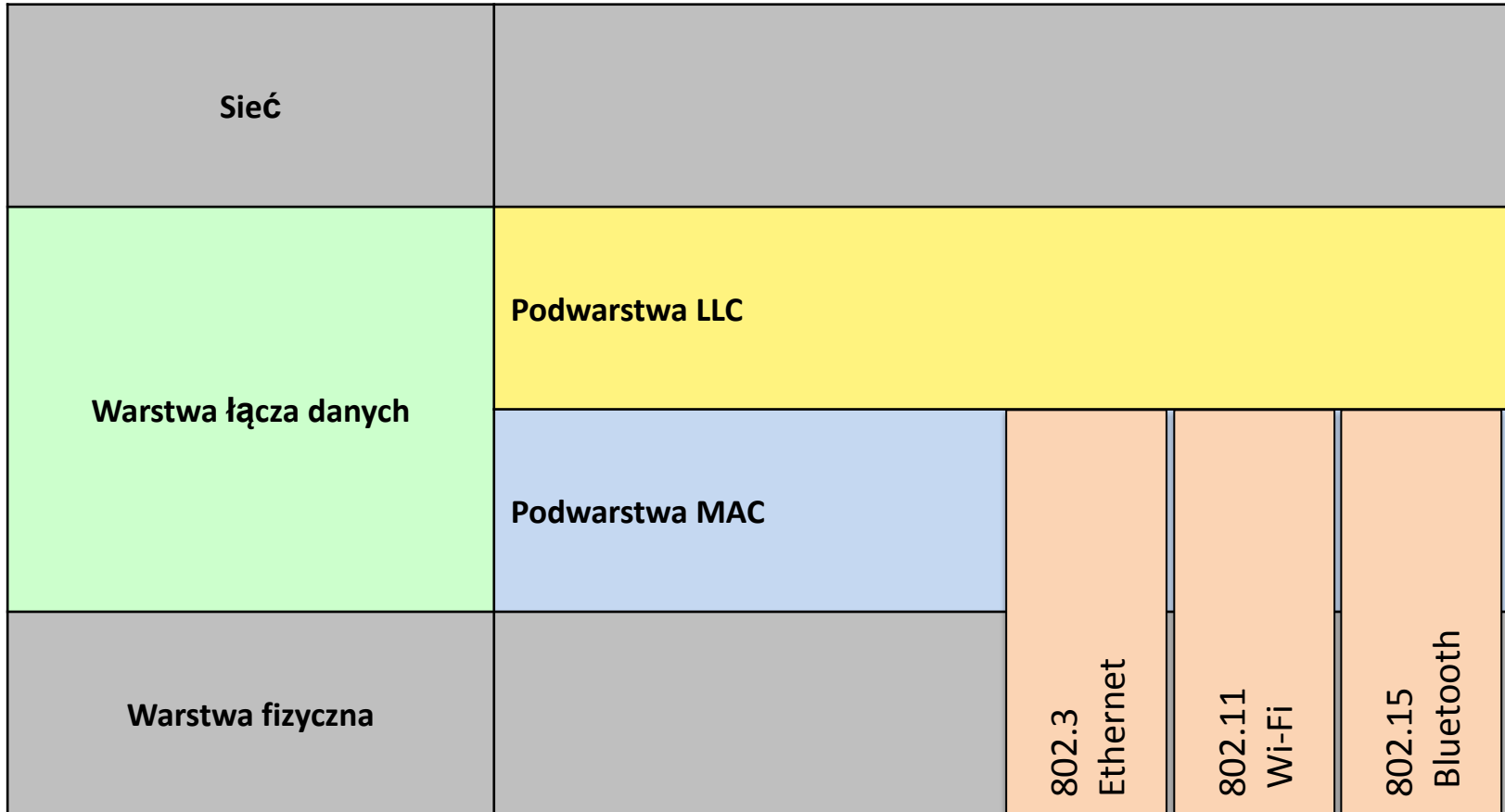
# Warstwa fizyczna



# Media sieciowe – budowa, zastosowania

- Światłowody (jedno i wielomodowe)
- Miedziane (UTP, STP, koncentryczny)
- Bezprzewodowe
- Złącza
- Właściwości

# Podwarstwy warstwy łącza danych



# Współdzielenie medium

- Rywalizacja, dostęp kontrolowany
- Kolizje, domeny kolizyjne



# Ramka łączy danych

# Ramka Ethernet

## Protokół Ethernet

Powszechny protokół warstwy łączy danych w sieciach LAN

Ramka						
Nazwa pola	Preambuła	Cel	Źródło	Typ	Dane	Suma kontrolna ramki
Rozmiar	8 bajtów	6 bajtów	6 bajtów	2 bajty	46-1500 bajtów	4 bajty

**Preambuła** - Wykorzystana w celu synchronizacji; zawiera również znacznik pozwalający na określenie zakończenia informacji taktowania.

**Adres docelowy** - 48 bitowy adres węzła docelowego.

**Adres Źródłowy** - 48-bitowy adres węzła źródłowego.

**Typ** - Wartość wskazująca jaki protokół warstwy wyższej otrzyma dane po zakończeniu procesu przetwarzania przez protokół Ethernet.

**Dane** - jest to datagram PDU, zazwyczaj jest to pakiet IPv4, który jest przesyłany przez medium.

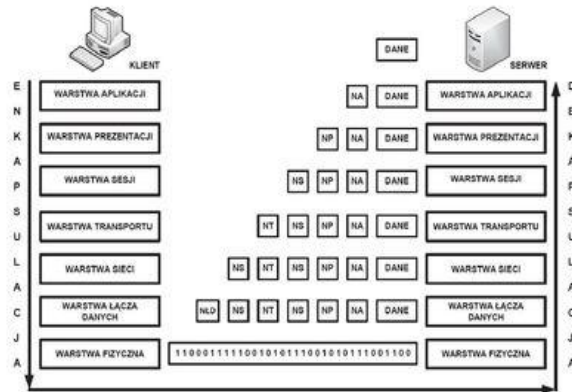
**Suma kontrolna ramki (FCS)** - Wartość wykorzystywana w celu wykrycia uszkodzonych ramek

Ethernet

# Enkapsulacja

Warstwy w modelu odniesienia ISO/OSI współpracują ze sobą zarówno w pionie jak i w poziomie. Na przykład warstwa transportu klienta współpracuje z warstwami sesji i sieci klienta a także warstwą transportu serwera.

## Enkapsulacja (dekapsulacja) danych



Rysunek 10. Proces enkapsulacji i dekapulacji danych

Enkapsulacja (dekapsulacja) danych jest procesem zachodzącym w kolejnych warstwach modelu ISO/OSI. Proces enkapsulacji oznacza dokładanie dodatkowej informacji (nagłówek) związanej z działającym protokołem danej warstwy i przekazywaniu tej informacji warstwie niższej do kolejnego procesu enkapsulacji. Proces dekapulacji polega na zdejmowaniu dodatkowej informacji w kolejnych warstwach modelu ISO/OSI.

### Dane, segmenty, pakiety, ramki, bity

W poszczególnych warstwach w modelu odniesienia ISO/OSI przechodzące dane noszą nazwę jednostek danych protokołu PDU (ang. *Protocol Data Unit*).



Rysunek 11. Jednostki informacji w poszczególnych warstwach w modelu odniesienia ISO/OSI

Jednostki te mają różne nazwy w zależności od protokołu. I tak w trzech górnych warstwach mamy do czynienia ze **strumieniem danych**, w warstwie transportu są **segmenty**, w warstwie sieci są **pakiety**, w warstwie łącza danych – **ramki**, a w warstwie fizycznej – **bity** (zera i jedyńki). Jednostki te w poszczególnych warstwach różnią się częścią nagłówkową.

### Model TCP/IP

Historycznie starszym modelem sieciowym jest **model TCP/IP** (ang. *Transmission Control Protocol/Internet Protocol*). Działanie sieci Internet opiera się właśnie na tym modelu sieciowym (patrz rys. 12). Opracowano go w połowie lat siedemdziesiątych XX wieku w amerykańskiej agencji DARPA (ang. *Defense Advanced Research Projects Agency*). Model TCP/IP składa się z czterech warstw.



# Enkapsulacja w Wireshark

The screenshot displays the Wireshark interface with a capture of network traffic. The main pane shows a list of packets with the following details:

lo.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.0.5	10.0.0.1	LDAP	MsgId=14857 Search Request, Base DN=CN=Configur
2	0.000113	10.0.0.5	10.0.0.1	ICMP	Echo (ping) request
3	0.000176	10.0.0.1	10.0.0.5	ICMP	Echo (ping) reply
4	0.000632	10.0.0.1	10.0.0.5	LDAP	MsgId=14857 search Entry, 1 result
5	0.202407	10.0.0.5	10.0.0.1	TCP	22862 > 3268 [ACK] Seq=188 Ack=169 win=63564 Le
6	0.921485	10.0.0.5	10.0.0.1	LDAP	MsgId=62548 Search Request, Base DN=CN=Configur
7	0.921993	10.0.0.1	10.0.0.5	LDAP	MsgId=62548 search Entry, 1 result
8	1.076817	10.0.0.5	10.0.0.1	TCP	22863 > 3268 [ACK] Seq=189 Ack=171 win=63214 Le
9	2.154733	10.0.0.5	10.0.0.1	ICMP	Echo (ping) request
10	2.155209	10.0.0.1	10.0.0.5	ICMP	Echo (ping) reply
11	6.813562	10.0.0.5	10.0.0.1	LDAP	Invalid LDAP message (Can't parse sequence head
12	6.813658	10.0.0.5	10.0.0.1	LDAP	Invalid LDAP message (Can't parse sequence head

The packet details pane for the selected packet (Frame 1) shows the following layers:

- Frame 1 (242 bytes on wire, 242 bytes captured)
- Ethernet II, Src: vmware\_e6:45:e6 (00:0c:29:e6:45:e6), Dst: vmware\_32:1a:5f (00:0c:29:32:1a:5f)
- Internet Protocol, Src: 10.0.0.5 (10.0.0.5), Dst: 10.0.0.1 (10.0.0.1)
- Transmission Control Protocol, Src Port: 22862 (22862), Dst Port: 3268 (3268), Seq: 0, Ack: 169, Win: 63564, Len: 14
- Lightweight Directory Access Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000  00 0c 29 32 1a 5f 00 0c 29 e6 45 e6 08 00 45 00  ..)2... ).E...E.
0010  00 e4 c4 fa 40 00 80 06 21 14 0a 00 00 05 0a 00  ....@... !.....
0020  00 01 59 4e 0c c4 8e 97 90 94 d8 83 db 2c 50 18  ..YN.... .....,P.
0030  f8 f5 63 96 00 00 00 00 00 b8 60 81 b5 06 09 2a  ..C.... ..*
0040  86 48 86 f7 12 01 02 02 02 01 11 00 ff ff ff ff  .H.....
0050  37 4a 80 7e 2d e8 19 9d 21 f7 0a ca fb 0e e8 78  7J.~... !.....x
0060  00 10 01 53 12 f0 15 40 20 04 00 00 00 00 00 00  _..._...
File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\etherXXXX4XAWBT" 3... [P: 59 D: 59 M: 0 Drops: 0
```



# Enkapsulacja w Wireshark

The screenshot displays the Wireshark network protocol analyzer interface. The title bar indicates the capture source is 'AMD PCNET Family Ethernet Adapter (Microsoft's Packet Scheduler) : Capturing - Wireshark'. The main window is divided into several sections:

- Filter:** A text box for applying filters, currently empty.
- Packet List:** A table showing captured packets. The columns are No., Time, Source, Destination, Protocol, and Info. The packets listed are all UDP traffic from 10.0.2.15 to various destinations.
- Packet Details:** A tree view showing the structure of the selected packet (Frame 1). It includes Ethernet II, Internet Protocol, User Datagram Protocol, and Data (103 bytes).
- Packet Bytes:** A hex dump of the packet data with corresponding ASCII characters.

No.	Time	Source	Destination	Protocol	Info
59	4.434148	125.224.133.118	10.0.2.15	UDP	Source port: 10309 Destination port:
60	4.497557	10.0.2.15	199.0.86.178	UDP	Source port: 21667 Destination port:
61	5.011805	10.0.2.15	98.109.10.168	UDP	Source port: 21667 Destination port:
62	5.017830	10.0.2.15	83.213.151.102	UDP	Source port: 21667 Destination port:
63	5.023041	10.0.2.15	85.85.208.247	UDP	Source port: 21667 Destination port:
64	5.026073	10.0.2.15	217.17.248.253	UDP	Source port: 21667 Destination port:
65	5.030948	10.0.2.15	221.121.246.224	UDP	Source port: 21667 Destination port:
66	5.116186	85.85.208.247	10.0.2.15	UDP	Source port: 28736 Destination port:
67	5.120513	10.0.2.15	79.18.126.151	UDP	Source port: 21667 Destination port:
68	5.148378	98.109.10.168	10.0.2.15	UDP	Source port: 54131 Destination port:
69	5.288715	217.17.248.253	10.0.2.15	UDP	Source port: 30521 Destination port:
70	5.294777	10.0.2.15	83.204.174.9	UDP	Source port: 21667 Destination port:
71	5.296733	79.18.126.151	10.0.2.15	UDP	Source port: 52308 Destination port:
72	5.301436	10.0.2.15	114.180.89.43	UDP	Source port: 21667 Destination port:
73	5.547639	221.121.246.224	10.0.2.15	UDP	Source port: 17839 Destination port:
74	5.708097	10.0.2.15	90.154.195.66	UDP	Source port: 21667 Destination port:
75	5.969007	83.213.151.102	10.0.2.15	UDP	Source port: peerwire Destination po

Packet Details for Frame 1 (145 bytes on wire, 145 bytes captured):

- Ethernet II, Src: CadmusCo\_76:0d:d9 (08:00:27:76:0d:d9), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)
- Internet Protocol, Src: 10.0.2.15 (10.0.2.15), Dst: 190.82.22.39 (190.82.22.39)
- User Datagram Protocol, Src Port: 21667 (21667), Dst Port: 26513 (26513)
- Data (103 bytes)

Packet Bytes:

```
0000 52 54 00 12 35 02 08 00 27 76 0d d9 08 00 45 00  RT..5... 'v....E.
0010 00 83 f5 e9 00 00 80 11 63 f8 0a 00 02 0f be 52  .....c.....R
0020 16 27 54 a3 67 91 00 6f 24 cb 64 31 3a 61 64 32  .T.g..o $.d1:ad2
0030 3a 67 64 32 30 3a bc e6 46 55 e4 91 4a 9d af 27  :id20:...FU..J..'
0040 6d dd 7e a9 45 7f ab c4 51 67 36 3a 74 61 72 67  m..~.E...Qg6:targ
0050 65 74 22 20 2a bc 06 7f 80 0f 40 22 04 d3 50 b0  eT20:  T  A
```

# Kontrola dostępu do medium

- Kontrola
- Adresy MAC
- Protokół ARP, tablica ARP
- Problemy ARP, eliminowanie problemów

# Przełączniki

- Full Duplex, Half Duplex, Auto MDIX
- Metody przesyłania ramek (Fast Forward, Cut-through.....)
- Przełączniki wielowarstwowe

Warstwa sieci



# Protokoły warstwy sieci

## **Podstawowe protokoły warstwy sieci to:**

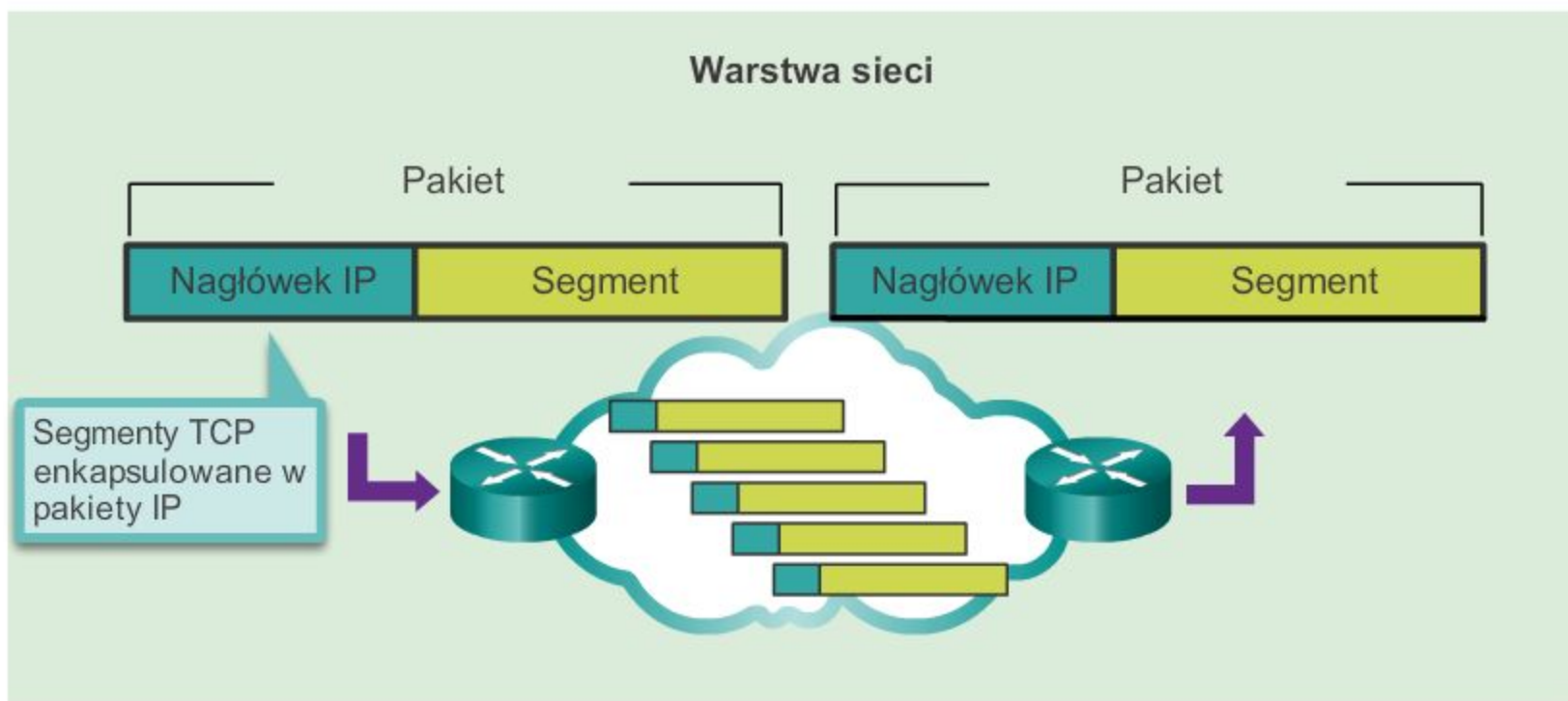
- IP w wersji 4 (IPv4)
- IP w wersji 6 (IPv6)

## **Tradycyjne protokoły warstwy sieci to:**

- Protokół Novell IPX (Internetwork Packet Exchange)
- AppleTalk
- Bezpołączeniowa usługa sieciowa (CLNS/DECNet)

# Charakterystyka IP

## Komponenty IP



Pakiety IP przepływają przez sieć komputerową.

Charakterystyka protokołu IP

# IP - Bezpołączeniowe

Komunikacja bezpołączeniowa



List został wysłany.

**Nadawca nie wie:**

- Czy odbiorca jest dostępny
- Czy przesyłka dotarła
- Czy odbiorca może przeczytać wiadomość

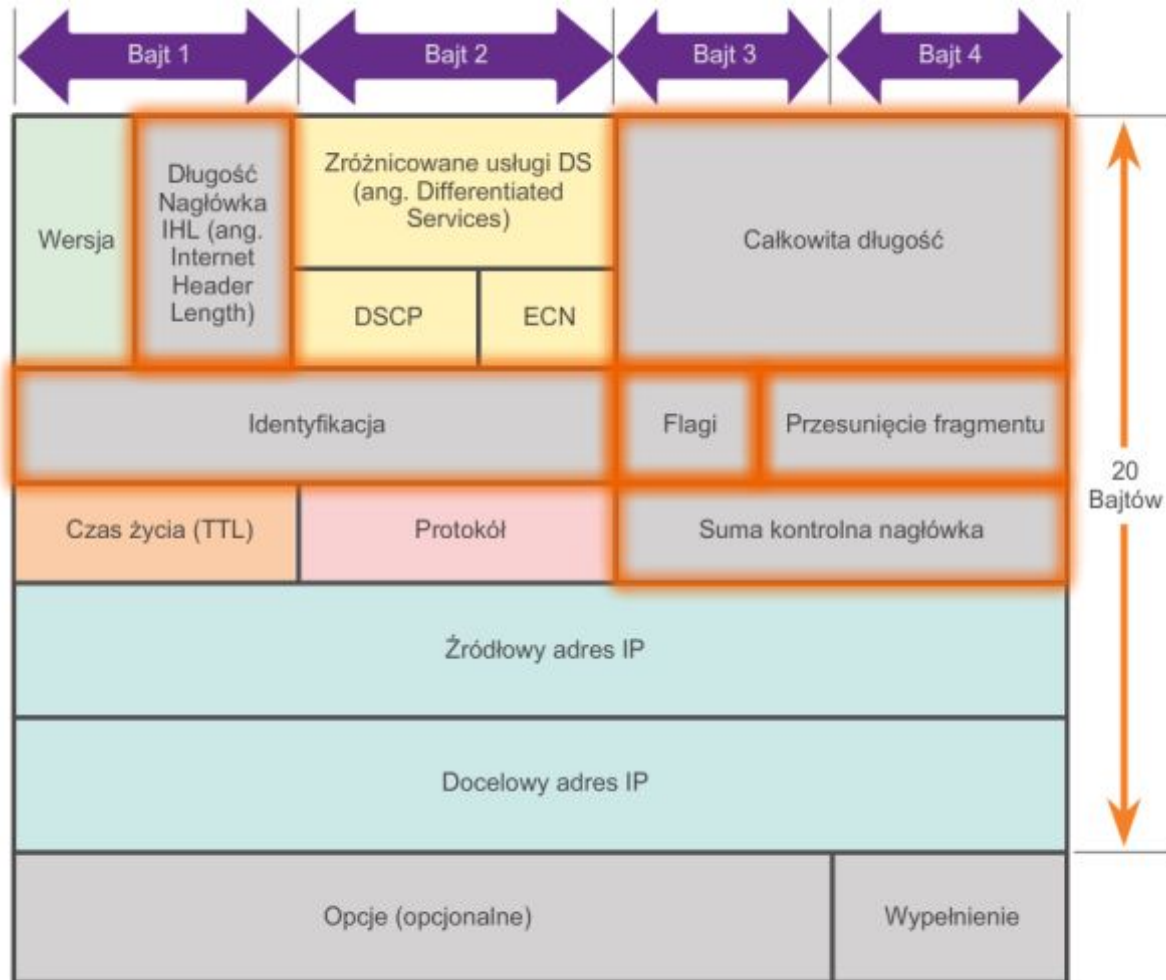
**Odbiorca nie wie:**

- Kiedy pakiet nadejdzie

# IPv4 vs IPv6

# IPv4 Nagłówek pakietu IPv4

## Zawartość nagłówka pakietu IPv4



# Wprowadzenie do IPv6

- zwiększona przestrzeń adresowa,
- udoskonalenie obsługi pakietów,
- eliminuje potrzebę wykorzystywania NAT,
- zintegrowane bezpieczeństwo,
- 4 miliardy adresów IPv4  
4 000 000 000
- 340 sekstylionów adresów IPv6  
340 000 000 000 000 000 000 000 000 000 000 000 000 000 000




## Pakiet IPv6

# Enkapsulacja IPv6

### Nagłówek IPv4

Wersja	IHL	Typ usługi	Całkowita długość	
Identyfikacja		Flagi	Przesunięcie fragmentu	
Czas życia (TTL)	Protokół	Suma kontrolna nagłówka		
Adres źródłowy				
Adres docelowy				
Opcje			Wypełnienie	



#### Opis

-  - Nazwy pól protokołu IPv4 zachowane w protokole IPv6
-  - Nazwy pól oraz miejsca w datagramie zmienione w IPv6
-  - Pola niewystępujące już w protokole IPv6

### Nagłówek IPv6

Wersja	Klasa ruchu (ang. Traffic Class)	Znacznik strumienia (ang. Flow Label) -		
Długość danych (ang. Payload Length)		Następny nagłówek (ang. Next Header)	Limit skoków (ang. Hop Limit)	
Źródłowy adres IP				
Docelowy adres IP				

#### Opis

-  - Nazwy pól protokołu IPv4 zachowane w protokole IPv6
-  - Nazwy pól oraz miejsca w datagramie zmienione w IPv6
-  - Nowe pole w IPv6

## Pakiet IPv4

# Przykładowy nagłówek IPv4

Microsoft: \Device\NPF\_{7BB3C130-30C5-4419-B79E-C0868085ABED} [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
16	3.64050300	192.168.1.109	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128
17	3.64506800	192.168.1.1	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=64
18	3.68215500	192.168.1.109	38.112.107.53	TCP	54	55502 > https [ACK] Seq=1 Ack=134 win=16661 Len=0
19	4.19945400	fe80::15ff:98d8:d28ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
20	4.60748800	fe80::15ff:98d8:d28ff02::c	fe80::b1ee:c4ae:a11	SSDP	453	HTTP/1.1 200 OK
21	4.64229900	192.168.1.109	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128
22	4.64509200	192.168.1.1	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=64
23	4.73605200	192.168.1.109	255.255.255.255	DB-LSP-	154	Droobox LAN svnc Discoverv Protocol

Frame 16: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Ethernet II, Src: IntelCor\_45:5d:c4 (24:77:03:45:5d:c4), Dst: Cisco-Li\_a0:d1:be (00:18:39:a0:d1:be)

Internet Protocol Version 4, Src: 192.168.1.109 (192.168.1.109), Dst: 192.168.1.1 (192.168.1.1)

- Version: 4
- Header length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
- Total Length: 60
- Identification: 0x3704 (14084)
- Flags: 0x00
  - Fragment offset: 0
  - Time to live: 128
  - Protocol: ICMP (1)
- Header checksum: 0x7ffe [correct]
  - Source: 192.168.1.109 (192.168.1.109)
  - Destination: 192.168.1.1 (192.168.1.1)
  - [Source GeoIP: Unknown]
  - [Destination GeoIP: Unknown]

Internet Control Message Protocol

```
0000 00 18 39 a0 d1 be 24 77 03 45 5d c4 08 00 45 00  ..9...$w .E]...E.
0010 00 3c 37 04 00 00 80 01 7f fe c0 a8 01 6d c0 a8  <?.....m..
0020 01 01 08 00 4d 56 00 01 00 05 61 62 63 64 65 66  ..MV.. ..abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69                    wabcdefg hi
```

Internet Protocol Version 4 (ip), 20 bytes | Packets: 35 Displayed: 35 Marked: 0 Dropped: 0 | Profile: Default



## Pakiet IPv6

# Przykładowy nagłówek IPv6

Wireshark capture of an IPv6 HTTP packet. The packet list shows a SYN-ACK, an ACK, a GET request, a TCP segment, and a FIN-ACK. The packet details pane shows the IPv6 header, TCP header, and the beginning of the HTTP GET request.

No.	Time	Source	Destination	Protocol	Length	Info
47	325.030878	2001:6f8:900:7c0::2	2001:6f8:102d:0:2d0:TCP	82	http > 59201 [SYN, ACK] Seq=0 Ack=1 win=6	
48	325.031166	2001:6f8:102d:0:2d0:9ff:fee:2001:6f8:900:7c0::2	TCP	74	59201 > http [ACK] Seq=1 Ack=1 win=5760 L	
49	325.040411	2001:6f8:102d:0:2d0:9ff:fee:2001:6f8:900:7c0::2	HTTP	314	GET / HTTP/1.0	
50	325.045496	2001:6f8:900:7c0::2	2001:6f8:102d:0:2d0:TCP	1506	[TCP segment of a reassembled PDU]	
51	325.045525	2001:6f8:900:7c0::2	2001:6f8:102d:0:2d0:HTTP	901	HTTP/1.1 200 OK (text/html)	
52	325.045627	2001:6f8:900:7c0::2	2001:6f8:102d:0:2d0:TCP	74	http > 59201 [FIN, ACK] Seq=2260 Ack=241	

Frame 49: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)

- Ethernet II, Src: HsingTec\_e3:e8:de (00:d0:09:e3:e8:de), Dst: Ibm\_82:95:b5 (00:11:25:82:95:b5)
- Internet Protocol Version 6, Src: 2001:6f8:102d:0:2d0:9ff:fee3:e8de (2001:6f8:102d:0:2d0:9ff:fee3:e8de), Dst: 2001:6f8:102d:0:2d0:9ff:fee3:e8de
  - 0110 .... = Version: 6
  - .... 0000 0000 .... = Traffic class: 0x00000000
  - .... 0000 0000 0000 0000 = Flowlabel: 0x00000000
  - Payload length: 260
  - Next header: TCP (6)
  - Hop limit: 64
  - Source: 2001:6f8:102d:0:2d0:9ff:fee3:e8de (2001:6f8:102d:0:2d0:9ff:fee3:e8de)
  - [Source SA MAC: HsingTec\_e3:e8:de (00:d0:09:e3:e8:de)]
  - Destination: 2001:6f8:900:7c0::2 (2001:6f8:900:7c0::2)
  - [Source GeoIP: Unknown]
  - [Destination GeoIP: Unknown]
- Transmission Control Protocol, Src Port: 59201 (59201), Dst Port: http (80), Seq: 1, Ack: 1, Len: 240
- Hypertext Transfer Protocol

```
0000 00 11 25 82 95 b5 00 d0 09 e3 e8 de 86 dd 60 00  ..%.
0010 00 00 01 04 06 40 20 01 06 f8 10 2d 00 00 02 d0  @
0020 09 ff fe e3 e8 de 20 01 06 f8 09 00 07 c0 00 00  .
0030 00 00 00 00 00 02 e7 41 00 50 ab dc d6 61 01 4a  .A.P...a.J
0040 73 9f 50 18 16 80 f4 48 00 00 47 45 54 20 2f 20  s.P...H ..GET /
0050 48 54 54 50 2f 31 2e 30 0d 0a 48 6f 73 74 3a 20  HTTP/1.0 ..Host:
0060 63 6c 2d 31 39 38 35 2e 68 61 6d 2d 30 31 2e 64  cl-1985. ham-01.d
0070 65 2e 73 69 78 78 73 2e 6e 65 74 0d 0a 41 63 63  e.sixxs. net..Acc
```

Internet Protocol Version 6 (ipv6), 40 bytes | Packets: 55 Displayed: 55 Mark... | Profile: Default

# Routing

- Brama domyślna, tablice routingu

# Wnętrze routera

1. Moduł zasilacza
2. Gniazdo dla modułu WIC
3. Wentylator
4. SDRAM
5. NVRAM
6. Procesor
7. Advanced Integration Module (AIM)



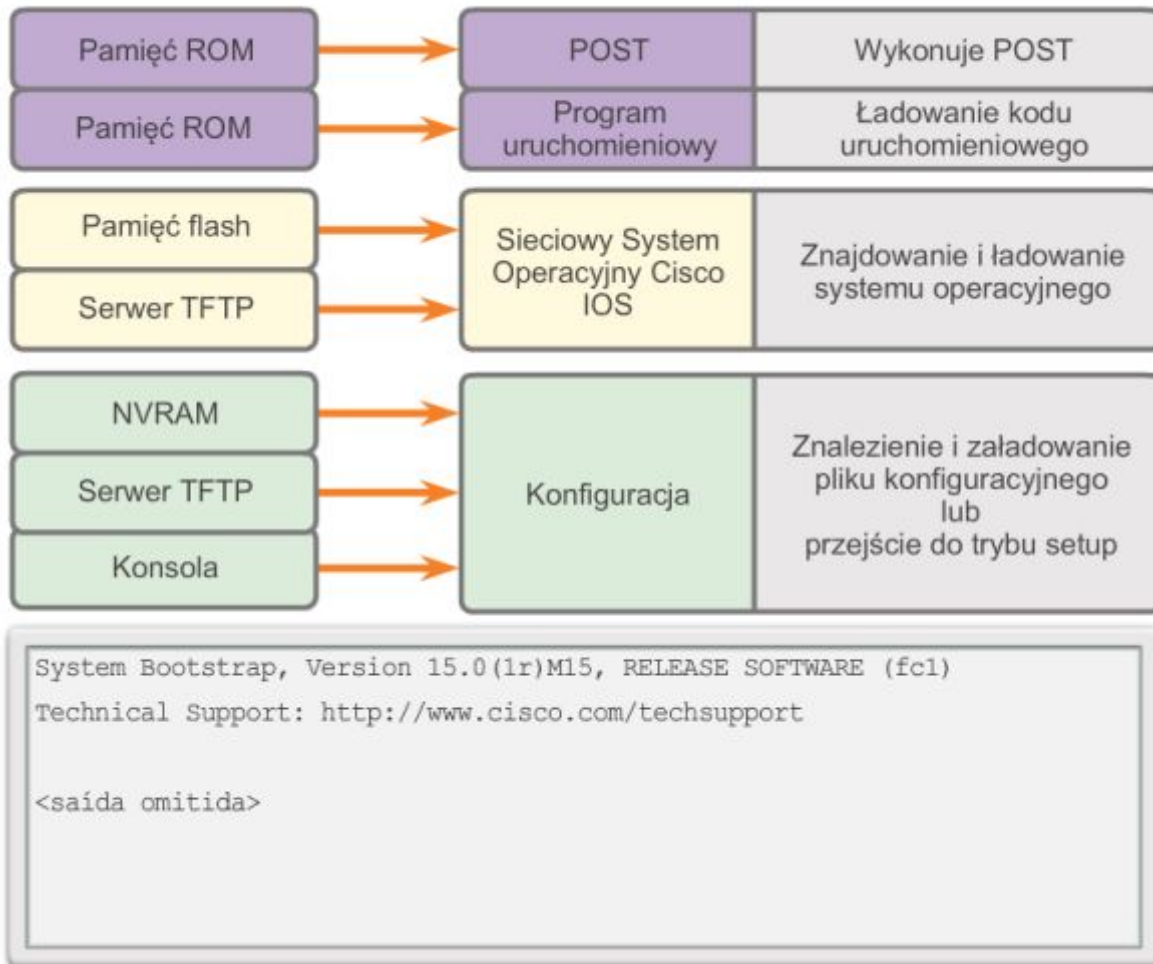
# Pamięć routera

Pamięć	Ulotna / Nieulotna	Przechowuje
RAM	Ulotna	<ul style="list-style-type: none"><li>• Uruchomiony IOS</li><li>• Plik konfiguracji bieżącej (running-config)</li><li>• Tablice routingu i tablice ARP</li><li>• Bufor pakietów</li></ul>
ROM	Nieulotna	<ul style="list-style-type: none"><li>• Rozkazy procesu rozruchowego</li><li>• Podstawowe oprogramowanie diagnostyczne</li><li>• Ograniczony funkcjonalnie IOS</li></ul>
NVRAM	Nieulotna	<ul style="list-style-type: none"><li>• Plik konfiguracji startowej</li></ul>
Pamięć flash	Nieulotna	<ul style="list-style-type: none"><li>• IOS</li><li>• Pozostałe pliki systemowe</li></ul>

## Rozruch routera

# Proces rozruchu routera

W jaki sposób uruchamia się router



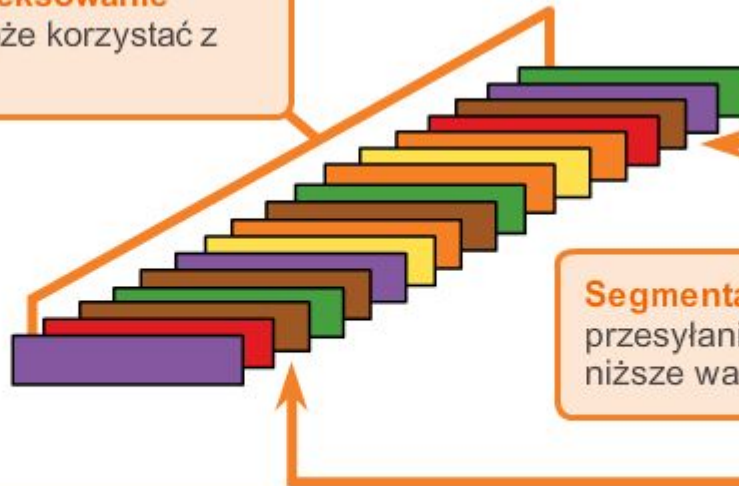
# Warstwa transportowa

TCP i UDP



# Multipleksowanie konwersacji (cd.)

Segmentacja umożliwia **multipleksowanie** konwersacji - wiele aplikacji może korzystać z sieci w tym samym czasie.



**Segmentacja** umożliwia przesyłanie danych przez niższe warstwy sieciowe.

**Kontrola błędów** może zostać przeprowadzona na danych w segmencie w celu sprawdzenia, czy zawartość segmentu zmieniła się podczas jego transmisji.

# Niezawodność warstwy transportowej

Różne aplikacje mogą wymagać różnych mechanizmów niezawodności.

TCP/IP zapewnia dwa protokoły warstwy transportowej, **TCP i UDP**.

## **TCP**

- Zapewnia niezawodność dostarczenia upewniając się że wszystkie dane dotarły do celu.
- Wykorzystuje potwierdzenie dostarczenia i inne procesy w celu zapewnienia dostarczenia.
- Ma większe wymagania sieciowe- większe narzuty.

## **UDP**

- Zapewnia tylko podstawowe funkcje dostawy - bez zapewnienia niezawodności.
- Mniejszy narzut

## **TCP czy UDP**

- Jest to kompromis pomiędzy wartością niezawodności i obciążeniem wprowadzanym przez nią do sieci.
- Twórcy aplikacji wybierają protokół transportowy w oparciu o wymagania ich aplikacji.

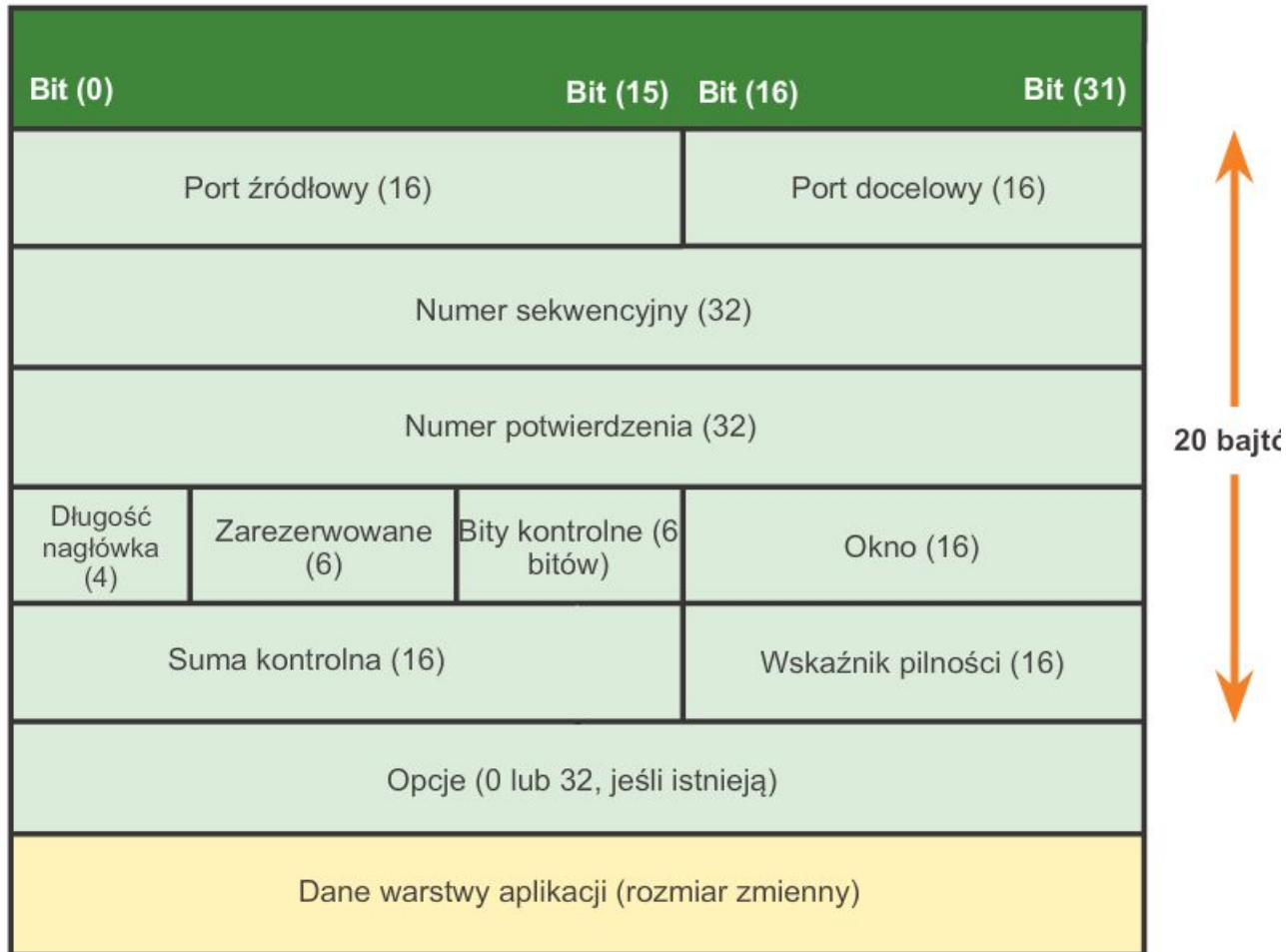


# Wprowadzenie do TCP

- Zdefiniowany w RFC 793
- Połączeniowy - tworzy sesję pomiędzy źródłem a odbiorcą.
- Niezawodna dostawa - retransmituje utracone lub uszkodzone dane.
- Uporządkowana rekonstrukcja danych - rekonstruuje numerację i sekwencjonowanie segmentów.
- Kontrola przepływu - reguluje ilość przesyłanych danych.
- Protokół stanowy - śledzenie sesji.

# Wprowadzenie do TCP

## Segment TCP

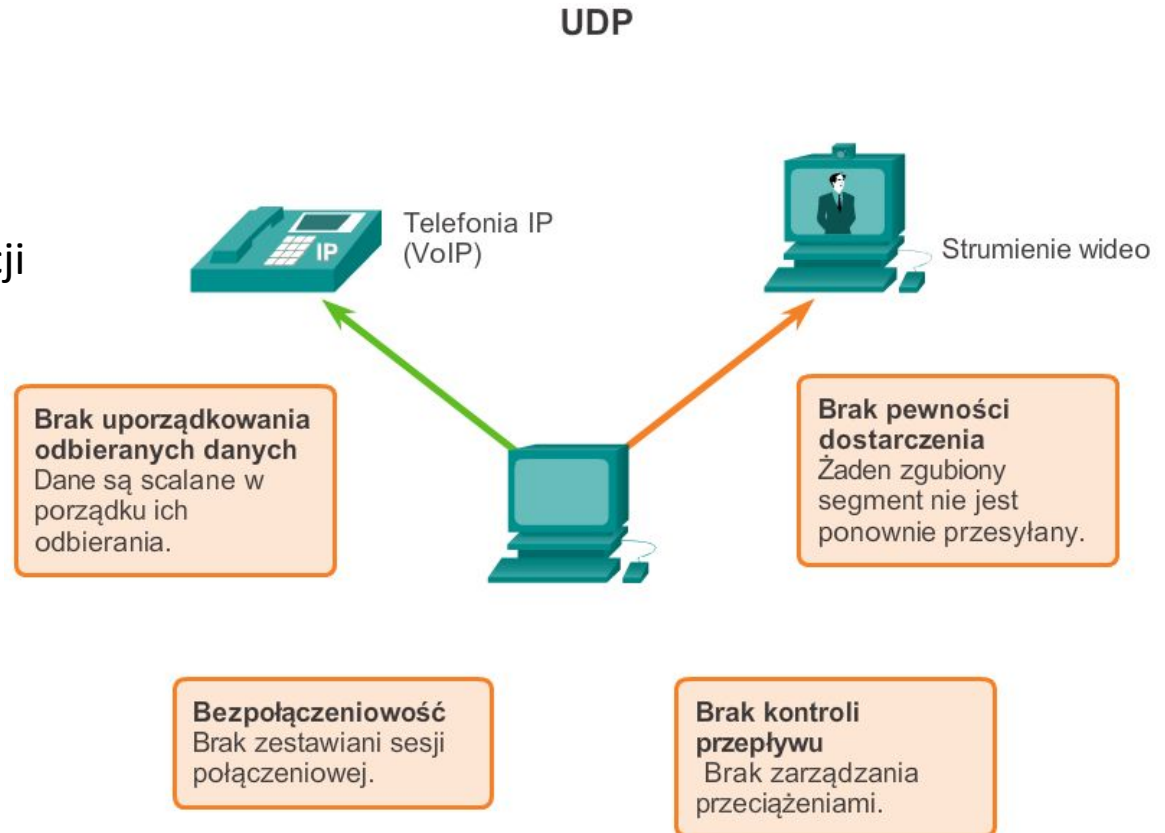


# Wprowadzenie do UDP

- RFC 768.
- Beipołączeniowy.
- Brak gwarancji dostarczania danych.
- Brak możliwości rekonstrukcji danych we właściwej kolejności.
- Brak kontroli przepływu.
- Protokół bezstanowy.

## Aplikacje wykorzystujące UDP:

- Protokół DNS (ang. Domain Name System), system nazw domenowych)
- aplikacje przesyłające strumienie Video,
- VoIP



# TCP, UDP, adresacja portów

- Porty dobrze znane,
  - Zarejestrowane
  - prywatne i/lub dynamiczne
- 
- Niezawodność TCP
  - Szybkość UDP

# Porty programów w TCP

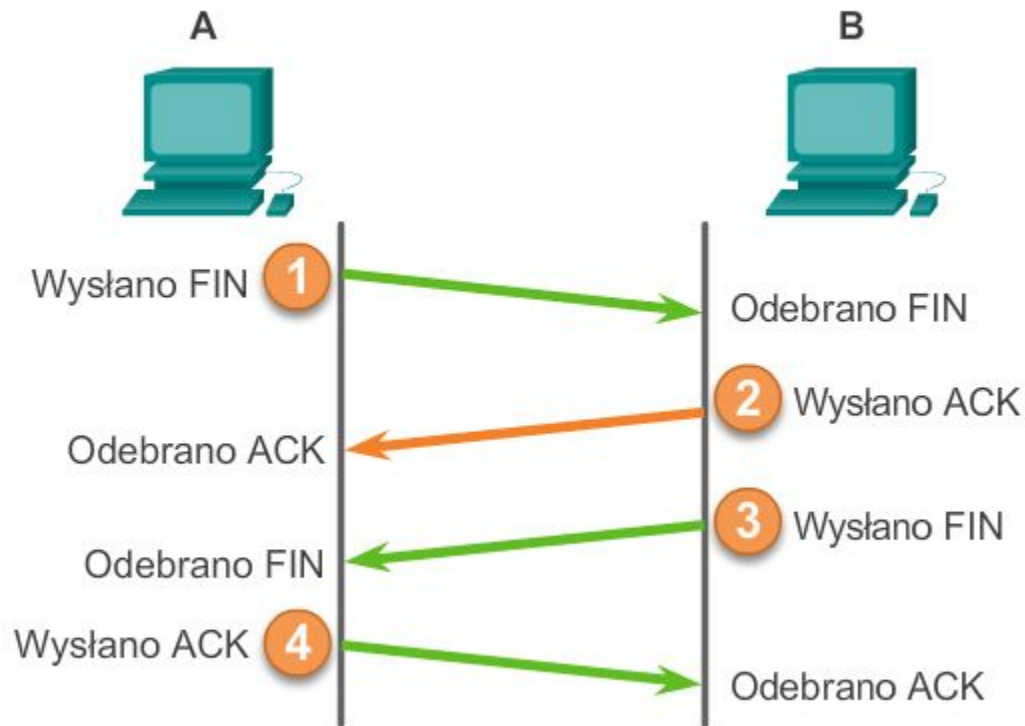
<b>Numer portu TCP</b>	<b>Opis</b>
20	Serwer FTP (kanał danych)
21	Serwer FTP (kanał kontrolny)
23	Serwer Telnet
53	Transfery stref DNS
80	Serwer sieci Web (HTTP)
139	Usługa sesji NetBIOS

# Porty UDP

<b>Numer portu UDP</b>	<b>Opis</b>
53	Kwerendy nazw DNS
69	Protokół TFTP (Trivial File Transfer Protocol)
137	Usługa nazw NetBIOS
138	Usługa datagramów NetBIOS
161	Protokół SNMP (Simple Network Management Protocol)
520	Protokół RIP (Routing Information Protocol)

# Kończenie sesji TCP (i nawiązywanie sesji)

## Nawiązywanie i finalizowanie połączenia TCP



A wysłała odpowiedź ACK do B.

# Porównanie UDP i TCP

## UDP

Usługa bez ustanowionego połączenia; między hostami nie jest ustanawiana sesja.

Protokół UDP nie gwarantuje dostarczenia przesyłki, a także potwierdzania i szeregowania danych.

Programy wykorzystujące protokół UDP odpowiadają za prawidłowe transportowanie danych.

Protokół UDP jest szybki, ma niskie wymagania organizacyjne i obsługuje połączenia bezpośrednie i połączenia jednego punktu z wieloma punktami.

## TCP

Usługa zorientowana na połączenie; między hostami jest ustanawiana sesja.

Protokół TCP gwarantuje dostarczenie przesyłki dzięki użyciu potwierdzania i szeregowania dostarczania danych.

Programy wykorzystujące protokół TCP mają zapewniony niezawodny transport danych.

Protokół TCP jest wolniejszy, ma wyższe wymagania organizacyjne i obsługuje tylko połączenia bezpośrednie.



# Adresacja IP i podsieci


# ADRESY INTERNETOWE



ADRES IP  identyfikacja docelowej maszyny

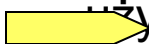
ADRES IP  identyfikuje interfejs sieciowy komputera

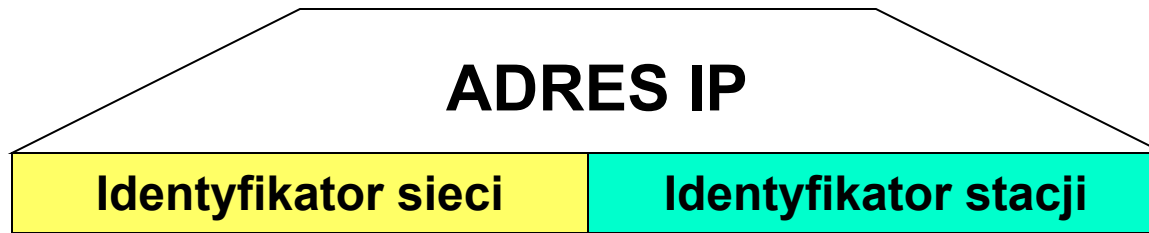


jeżeli komputer posiada wiele interfejsów sieciowych (np. do różnych sieci) - będzie też posiadał wiele adresów IP

 Tak jak w przypadku telefonów, wszystkie sieci pewnego dnia będą połączone ze sobą.

IP musi być  unikalny w sensie globalnym  
przyznawane  e IP musi być koordynowane globalnie

Obecnie ( **IP v.4** )  używane są adresy **32 bitowe**  
co pozwala nadać adresy  $2^{32}$  stacjom  
czyli 4 294 967 296 stacjom



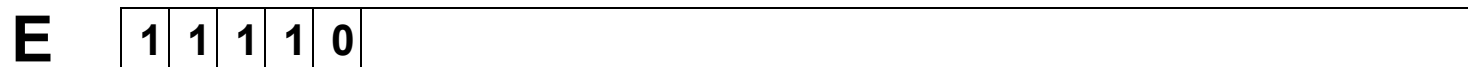
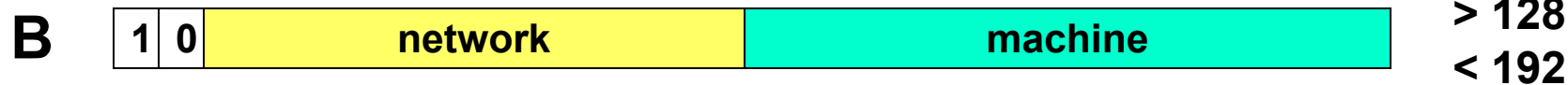
- Routowanie w sensie globalnym** „nie przejmuję się” identyfikowaniem stacji - uwzględniany jest jedynie identyfikator sieci
  
- Routowanie lokalne** (tzn. takie w którym  $id\_sieci = IP\_sieci$  w adresie) używa jedynie identyfikatora stacji.
  
- Jeżeli komputer zostanie przeniesiony do innej sieci jego adres musi ulec zmianie.



KLAS  
A

# 5 KLAS ADRESÓW IP

NUMER  
SIECI



## NOTACJA ADRESÓW IP - „kropkowana” dziesiętna

przykład

**130.104.29.10**

**128<130<192**  
**klasa B**

**Stacja nr 29.10**

## ADRESY SPECJALNE

0 oznacza „this” - określenie aktualnej sieci

wszystkie bity = 1      wszystkie maszyny w danej sieci  
(*Broadcast address*)

**127.0.0.1**      lokalna pętla umożliwiająca TCP/IP  
komunikację pomiędzy procesami na  
lokalnej maszynie

# PROBLEMY Z ADRESAMI IP

- ⚡ Adresy dla sieci klasy B są już prawie wyczerpane
- ⚡ Nie stworzono klas dla średnich wielkości sieci (pomiędzy 256 a 5000 stacji)

⚡ Rozmiary tablic routingu wymykają się spod kontroli

nie ma związku z numerem sieci i jej lokalizacją

w backbone routerach w tablicach routingu znajduje się po jednej linii dla każdego adresu IP na świecie !

## ➔ ROZWIĄZANIE: CIDR (Classless Inter-Domain Routing)

generalizacja idei maskowania

fuzyja klas A, B i C

sieć identyfikowana przez parę <prefix maska>

# Maski

- Daną klasę adresów można podzielić na logiczne podsieci za pomocą Maski
- Jeśli bit w masce ma wartość 1, to odpowiadający mu bit w adresie IP jest bitem części sieciowej
- Jeśli bit w masce jest równy 0, to bit adresu należy do części określającej komputer

# Przykład maski

adres dziesiętnie	62	121	77	1
adres bitowo	00111110	01111001	01001101	00000001
maska dziesiętnie	255	255	252	0
maska bitowo	11111111	11111111	11111100	00000000

Operacja AND na odpowiadających sobie bitach adresu IP i Maski pozwala ustalić adres sieci



# Maski podsieci dla klas adresów

<b>Klasa adresu</b>	<b>Bity maski podsieci</b>	<b>Maska podsieci</b>
Klasa A	11111111 00000000 00000000 00000000	255.0.0.0
Klasa B	11111111 11111111 00000000 00000000	255.255.0.0
Klasa C	11111111 11111111 11111111 00000000	255.255.255.0

# Poziomy hierarchii w adresacji IP

- Tradycyjna adresacja (dwupoziomowa): sieć i host (router przekazuje pakiet do właściwej sieci, korzystając z części sieciowej adresu a po osiągnięciu sieci identyfikuje urządzenie końcowe korzystając z części hostowej adresu IP
- Współcześnie (trzydziomowa): sieć, podsieć, host. Efektem jest przyśpieszenie dostarczenia pakietu i minimalizacja ruchu lokalnego.

# Po co podział na podsieci?

Łatwiej zapanować nad kilkoma mniejszymi częściami niż nad dużą całością

Minimalizowanie ruchu wewnętrznego (np. transmisje rozgłoszeniowe)

# Kryteria podziału na podsieci

- Lokalizacja geograficzna (np. piętra w budynku)
- Jednostki organizacyjne (sprzedaż, księgowość, projektanci)
- Typy urządzeń (serwery, drukarki)
- Inne – logiczny i ważny

# Adresy prywatne - zakresy

- 10.0.0.0 z maską podsieci 255.0.0.0
- 172.16.0.0 z maską podsieci 255.240.0.0
- 192.168.0.0 z maską podsieci 255.255.0.0

Zadanie: dla każdej z sieci ustal: minimalny i maksymalny adres hosta oraz liczbę hostów, które w niej zaadresujemy.

# Stwórz standardy nadawania adresacji IP w zakresie poszczególnych sieci

- Drukarki oraz serwery będą miały przypisane statyczne adresy IP
- Użytkownicy otrzymają adresy IP z serwera DHCP wykorzystując podsieci z maską /24
- Routerom przypisano pierwszy dostępny adres hosta z puli adresów

# A gdy już będziesz umiał(a)....

- [www.ipcalc.org](http://www.ipcalc.org) – może nie działać
- [www.subnetmask.info](http://www.subnetmask.info)
- [www.42.pl](http://www.42.pl)

# Projektowanie sieci

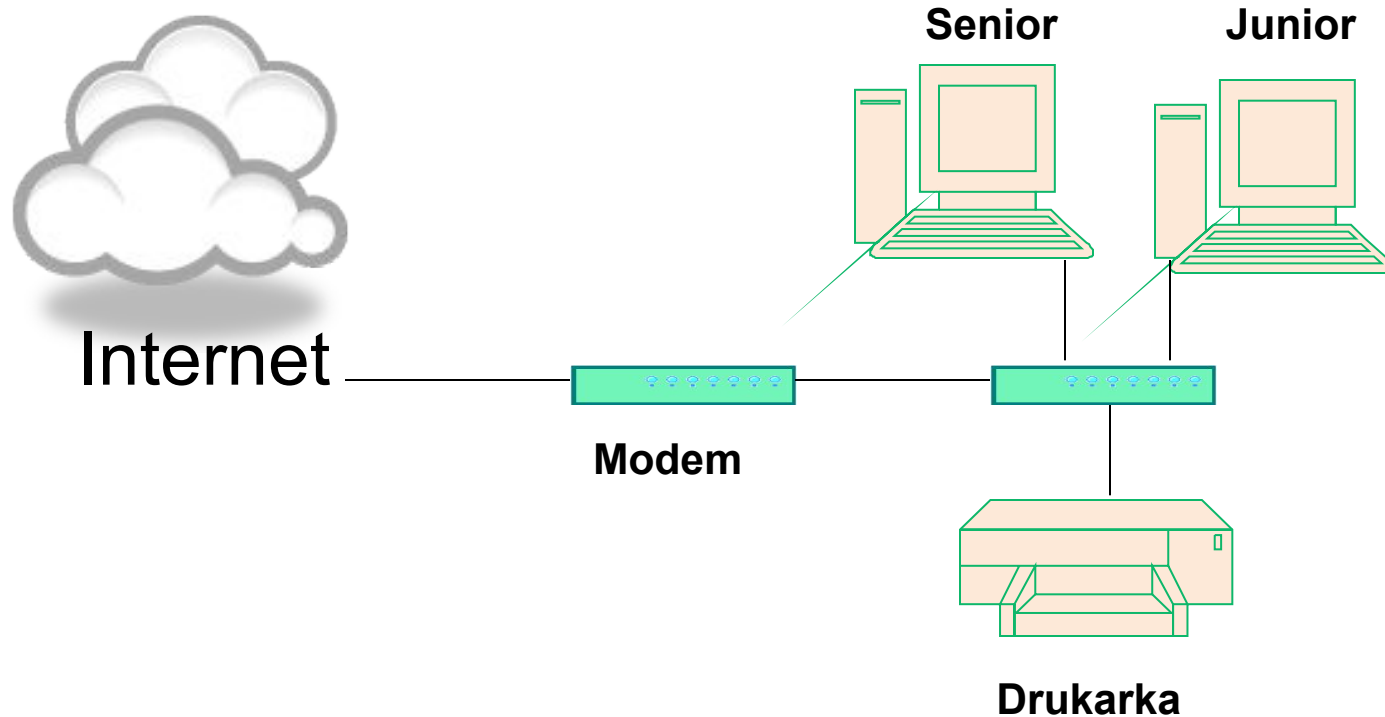


# Co to jest niezbędne do budowy sieci?

Aby zbudować sieć komputerową, musimy:

- Zaopatrzyć komputery w karty sieciowe,
- Wybrać odpowiednią topologię sieci,
- Ułożyć okablowanie,
- Zainstalować oprogramowanie klienta sieci,
- Wybrać usługi, z których chcemy korzystać,
- Przydzielić i skonfigurować odpowiednie protokoły komunikacyjne.

Ze względu na rodzaj okablowania aktualnie najpopularniejsze są sieci wykonane przy użyciu skrętki ekranowanej lub nieekranowanej



Nawet najmniejsza sieć komputerowa umożliwia korzystanie ze wspólnych zasobów, urządzeń, Internetu oraz realizację projektów zespołowych. Umożliwia również komunikację (dźwięk, obraz, tekst).

# Konfiguracja komputerów sieciowych

Kiedy już przygotujemy połączenie sieciowe, można przystąpić do uruchomienia i konfiguracji sieci.

Każdy komputer sieciowy musi posiadać:

- kartę sieciową zgodną ze standardem sieci – najczęściej Fast Ethernet,
- oprogramowanie nazywane klientem sieci i zgodnie z SO,
- protokół sieciowy – sugerujemy wybór protokołu TCP/IP jako najbardziej uniwersalnego i niezbędnego przy połączeniu z Internetem.

# Brama

Brama (ang. Gateway) – urządzenie posiadające własny adres IP. Umożliwia ono dostęp do Internetu. Bramą może być router, jak też komputer z dołączonym terminalem SDI. Brama znajduje się w obrębie sieci lokalnej.

# Serwer DHCP

Serwer DHCP – program przydzielający automatycznie adresy IP kolejno przyłączanym do sieci komputerom. W sieci lokalnej serwer DHCP może być związany z urządzeniem pełniącym funkcję bramy, a więc np. z routerem. Lokalny serwer DHCP może przydzielać adresy z puli przeznaczonej dla sieci lokalnej. Dynamicznie przydzielone adresy tracą ważność z chwilą odłączenia komputera od sieci. Przy następnym przyłączeniu otrzymany adres może być inny. Na serwerze dostawcy Internetu również działa serwer DHCP. Przydziela on chwilowe adresy IP zgłaszającym się do niego sieciom lokalnym. Numer ten przekazany jest urządzeniu dostępowemu (modem, terminal ISDN, karta sieciowa).

# Serwer DNS

Serwer DNS (z ang. Domain Name Server) – serwer nazw domenowych tłumaczący literowe nazwy serwerów przyjazne dla ludzi na ich odpowiedniki liczbowe zrozumiałe dla maszyn. Dzięki wykorzystaniu DNS nazwa mnemoniczna, może zostać zamieniona na odpowiadający jej adres IP, czyli *145.97.39.155*.

Adresy DNS składają się z domen internetowych rozdzielonych kropkami. W ten sposób możliwe jest budowanie hierarchii nazw, które porządkują Internet. DNS to złożony system komputerowy oraz prawny. Zapewnia z jednej strony rejestrację nazw domen internetowych i ich powiązanie z numerami IP. Z drugiej strony realizuje bieżącą obsługę komputerów odnajdujących adresy IP odpowiadające poszczególnym nazwom.