

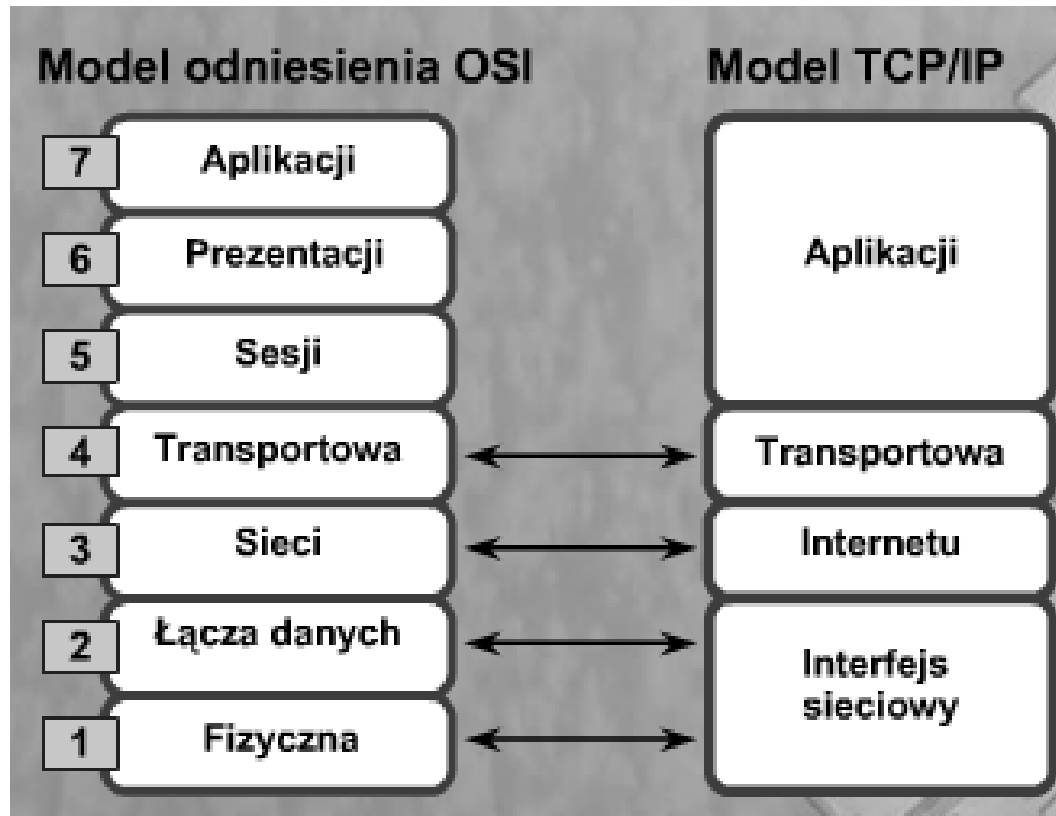


PODSTAWY SIECI KOMPUTEROWYCH

**Modele warstwowe - Model OSI
- warstwa sieci.**

Funkcje warstwy sieci

- odpowiedzialna za adresowanie logiczne i domenę routingu.



Warstwa sieci / model OSI

- Rozpoznaje, jakie drogi łączą poszczególne komputery (trasowanie).

Trasowanie - oznacza to wyznaczanie trasy i wysłanie nią pakietu danych w sieci komputerowej.

Router - urządzenie węzłowe, w którym kształtowany jest ruch sieciowy, jego rolę może pełnić np.

- komputer stacjonarny
- dedykowane urządzenie.

Warstwa sieci / model OSI

- Rozpoznaje, jakie drogi łączą poszczególne komputery (trasowanie).

Trasowanie - oznacza to wyznaczanie trasy i wysłanie nią pakietu danych w sieci komputerowej.

Router - urządzenie węzłowe, w którym kształtowany jest ruch sieciowy, jego rolę może pełnić np.

- komputer stacjonarny
- dedykowane urządzenie.

Warstwa sieci / model OSI

Protokoły trasowane (ang. routed protocols) odpowiadają za dostarczanie danych do celu, czyli przenoszą pakiety zawierające dane użytkowników sieci.

Jest to możliwe dzięki zawieraniu w swoim nagłówku warstwy sieciowej informacji (adresu nadawcy i odbiorcy), w oparciu o które router może przekazać dane do innego routera (wykonać trasowanie) w taki sposób, że po przejściu przez wiele routerów pakiety osiągną host przeznaczenia.

Protokoły routujące to protokoły używane do wymiany informacji o trasach pomiędzy sieciami komputerowymi, co pozwala na dynamiczną budowę tablic trasowania.

Warstwa Internet / modelu TCP/IP

Przerzuca pakiety z danymi od maszyny źródłowej do maszyny docelowej, bez żadnej gwarancji, że dotrą do celu.

Na warstwę Internet składają się trzy protokoły wchodzące w skład TCP/IP:

- IP (Internet Protocol),

- ICMP (Internet Control Message Protocol),

- IGMP (Internet Group Management Protocol).

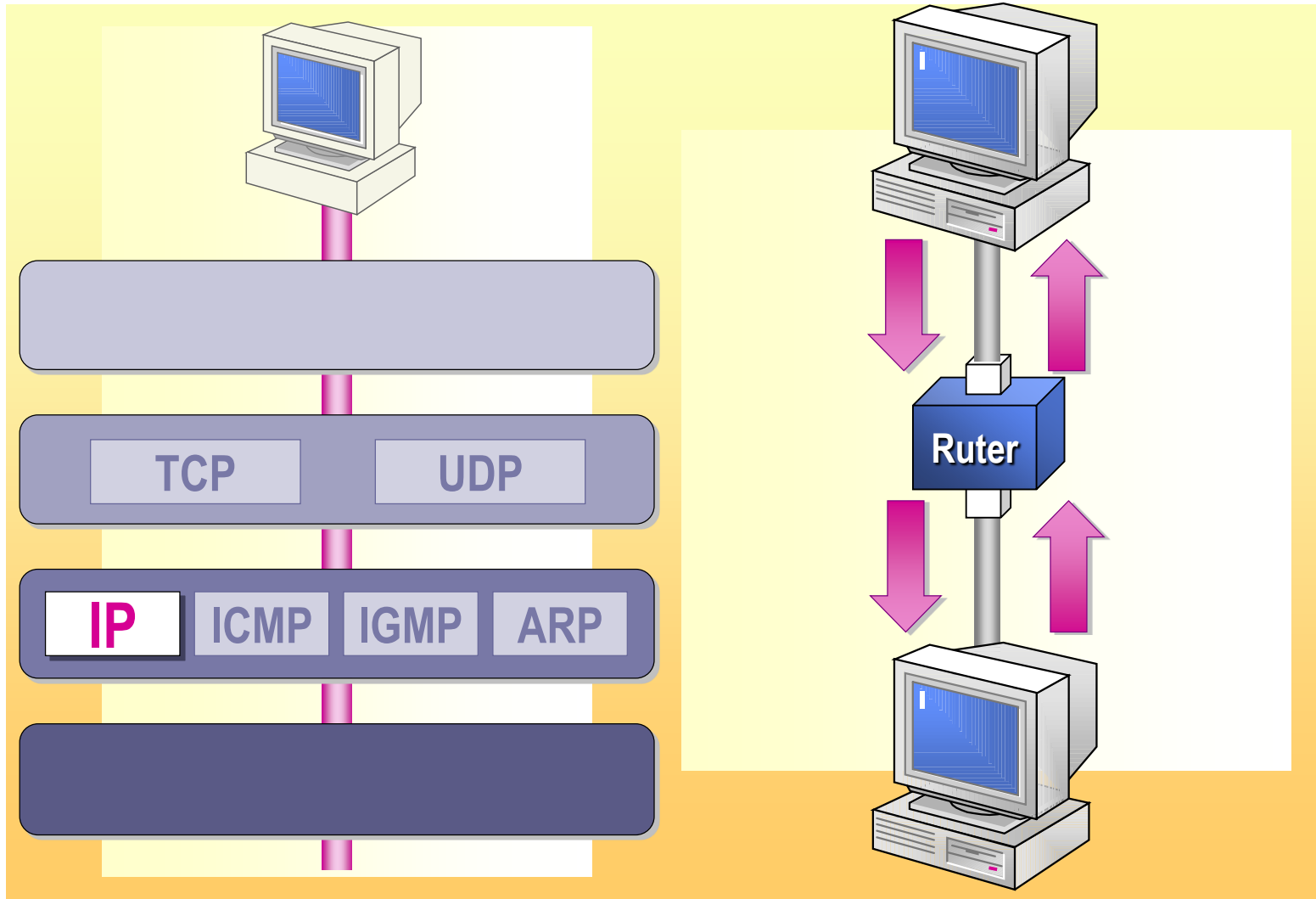
IP służy do transportu pakietów, a ICMP i IGMP - do ustalania trasy między nadawcą i odbiorcą pakietów.

Warstwa ta nie wykrywa i nie poprawia błędów.

IP (Internet Protocol)



IP (Internet Protocol)



IP (Internet Protocol)

- protokół komunikacyjny (warstwy sieciowej modelu OSI / warstwy internet w modelu TCP/IP).
- używany powszechnie w Internecie i sieciach lokalnych.

Dane w sieciach IP są wysyłane w formie bloków określanych mianem pakietów.

W przypadku protokołu IP, przed rozpoczęciem transmisji nie jest zestawiana wirtualna sesja komunikacyjna pomiędzy dwoma hostami, które nie komunikowały się ze sobą wcześniej.

Protokół IP jest protokołem zawodnym - nie gwarantuje, że pakiety dotrą do adresata, nie zostaną pofragmentowane, czy też zdublowane, a ponadto mogą dotrzeć do odbiorcy w innej kolejności niż zostały nadane.

Niezawodność transmisji danych jest zapewniana przez protokoły warstw wyższych (np. TCP), znajdujących się w hierarchii powyżej warstwy sieciowej.

IP (Internet Protocol) (IETF RFC 791)

zadania

- bezpołączeniowe dostarczanie pakietów (datagramów)
- wyznaczanie „najlepszej trasy”
- dokonywanie fragmentacji i ponownego składania datagramów stosownie do wykorzystywanego połączenia, które charakteryzuje parametr maksymalnej wielkości jednostki maximum-transmission unit (MTU).

IP (Internet Protocol)

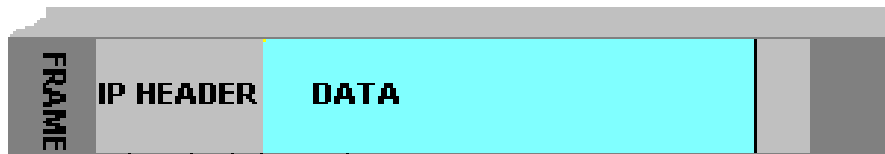
- adresuje i przesyła pakiety
- protokół bezpołączeniowy
 - nie ustala sesji
- niegwarantowany “Best Effort”
- integralność przesyłu jest sprawą protokołów wyższej warstwy (np. TCP) lub aplikacji
- dzieli, a potem łączy podzielone pakiety

IP (Internet Protocol)

opis nagłówka IPv4


1																2																3															
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1																
Wersja				IHL				Typ usługi				Długość całkowita																																			
Identyfikator								Flagi				Przemieszczenie fragmentacji																																			
TTL				Protokół				Suma kontrolna nagłówka																																							
Adres źródłowy																																															
Adres docelowy																																															
Opcje																								Dopełnienie																							

IP (Internet Protocol)

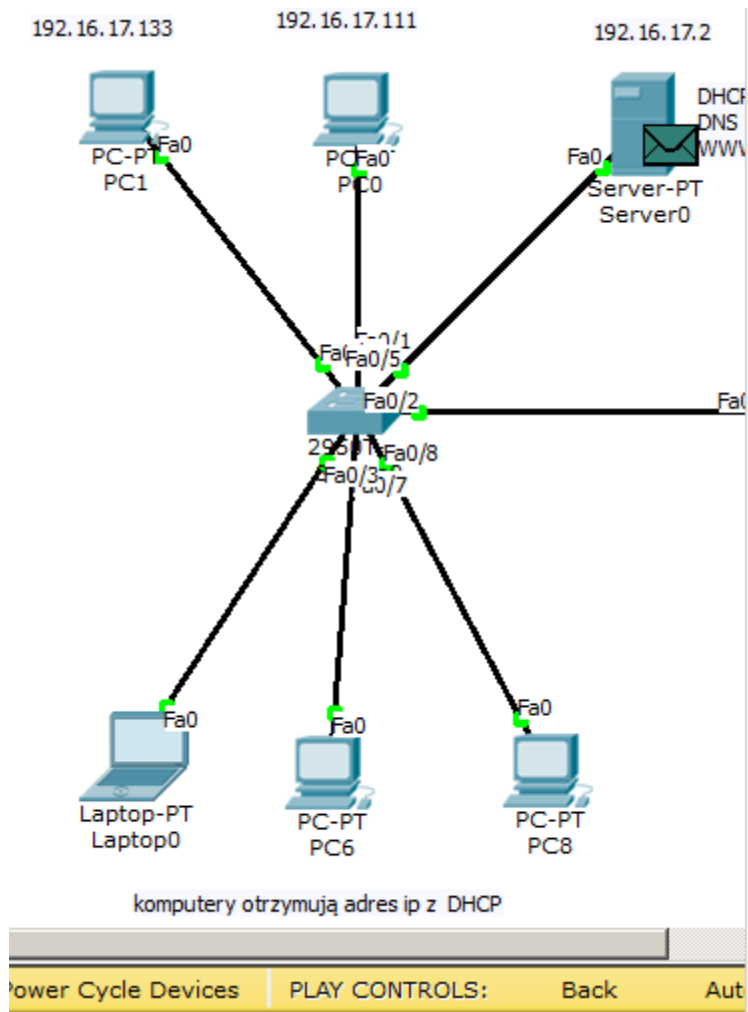


- **Protokół poziomu sieciowego (network layer protocol)** umożliwia przekazywanie pakietów TCP/IP pomiędzy podsieciami
- adres stacji jest wewnątrz pakietu IP
- niskie ryzyko utraty połączenia

```
Packet Number : 3                2:16:34 PM
Length : 322 bytes
ether: ===== Ethernet Datalink Layer =====
Station: 00-60-97-93-17-52 ----> 00-12-56-F4-DD-23
Type: 0x0800 (IP)
ip: ===== Internet Protocol =====
Station:198.112.65.10 ---->198.112.65.251
Protocol: TCP
Version: 4
Header Length (32 bit words): 5
Precedence: Routine
Normal Delay, Normal Throughput, Normal Reliability
Total length: 304
Identification: 59937
Fragmentation not allowed, Last fragment
Fragment Offset: 0
Time to Live: 32 seconds
Checksum: 0x5FC0(Valid)
```



IP (Internet Protocol)



OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

PREAMBLE: 101010...1011	DEST MAC: 0003.E40C.4D30	SRC MAC: 0090.2184.170D
TYPE: 0x800	DATA (VARIABLE LENGTH)	FCS: 0x0

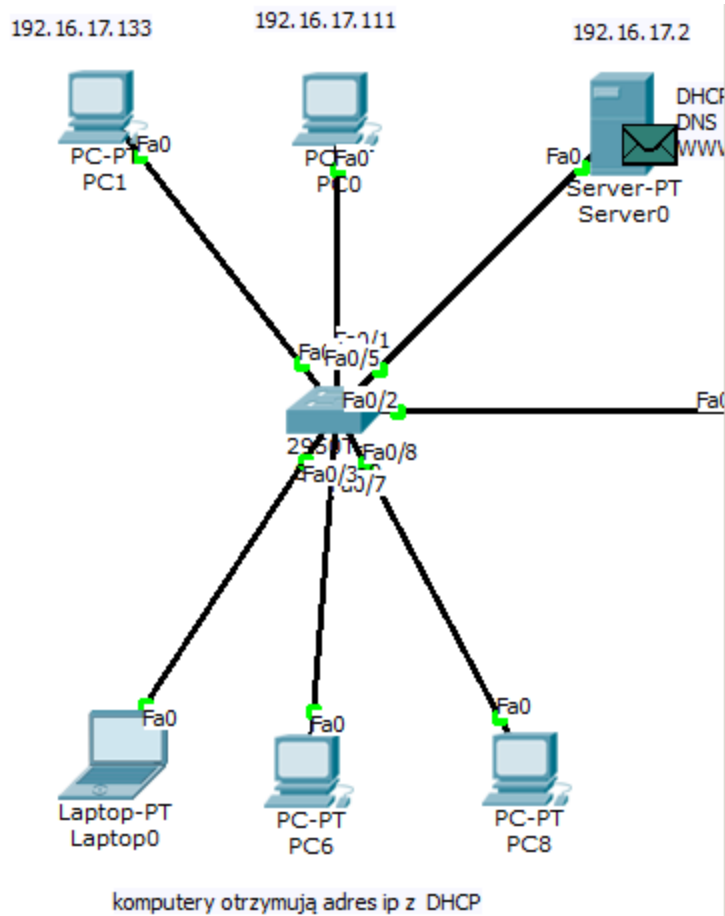
IP

4	4	8	16	19	31 Bits
IHL	DSCP: 0x0	TL: 28			
ID: 0x4		0x0	0x0		
TTL: 255	PRO: 0x1	CHKSUM			
SRC IP: 192.16.17.12					
DST IP: 192.16.17.2					
OPT: 0x0				0x0	
DATA (VARIABLE LENGTH)					

ICMP

0	8	16	31 Bits
TYPE: 0x8	CODE: 0x0	CHECKSUM	
ID: 0x4		SEQ NUMBER: 3	

IP (Internet Protocol)



PDU Information at Device: Server0

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19	Byt
PREAMBLE: 101010...1011		DEST MAC: 0090.2184.170D		SRC MAC: 0003.E40C.4D30	
TYPE: 0x800		DATA (VARIABLE LENGTH)		FCS: 0x0	

IP

0	4	8	16	19	31	Bits
4		IHL	DSCP: 0x0		TL: 28	
ID: 0xd			0x0		0x0	
TTL: 128		PRO: 0x1		CHKSUM		
SRC IP: 192.16.17.2						
DST IP: 192.16.17.12						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

ICMP

0	8	16	31	Bits	
TYPE: 0x0		CODE: 0x0		CHECKSUM	

IP (Internet Protocol)

No.	Time	Source	Destination	Protocol	Length	Info
2571	38.854491	66.189.0.100	192.168.1.220	DNS	506	Standard query response CNAME fbcdn-profile-a.akamaihd.net
2599	39.726471	192.168.1.220	50.21.182.176	HTTP	1838	POST /wp-admin/admin-ajax.php HTTP/1.1 (application/x-www-form-urlencoded)
2607	40.076925	50.21.182.176	192.168.1.220	HTTP/XML	60	HTTP/1.1 200 OK
839	7.993622	192.168.1.220	173.194.73.104	ICMP	70	Echo (ping) request id=0x0001, seq=1203/45828, ttl=1
840	7.995085	173.194.73.104	192.168.1.220	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Frame 839: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)

Ethernet II, Src: AsustekC_b9:09:04 (e0:cb:4e:b9:09:04), Dst: Cisco-Li_ee:91:3a (00:14:bf:ee:91:3a)

Internet Protocol Version 4, Src: 192.168.1.220 (192.168.1.220), Dst: 173.194.73.104 (173.194.73.104)

- Version: 4
- Header length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-capable Transport))
- Total Length: 56
- Identification: 0x3377 (13175)
- Flags: 0x00
- Fragment offset: 0
- Time to live: 1
- Protocol: ICMP (1)
- Header checksum: 0x0000 [incorrect, should be 0xcc9f (maybe caused by "IP checksum offload"?)]
- Source: 192.168.1.220 (192.168.1.220)
- Destination: 173.194.73.104 (173.194.73.104)

Internet Control Message Protocol

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0x265b [correct]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence number (BE): 1203 (0x04b3)
- Sequence number (LE): 45828 (0xb304)

IP (Internet Protocol) na routerze



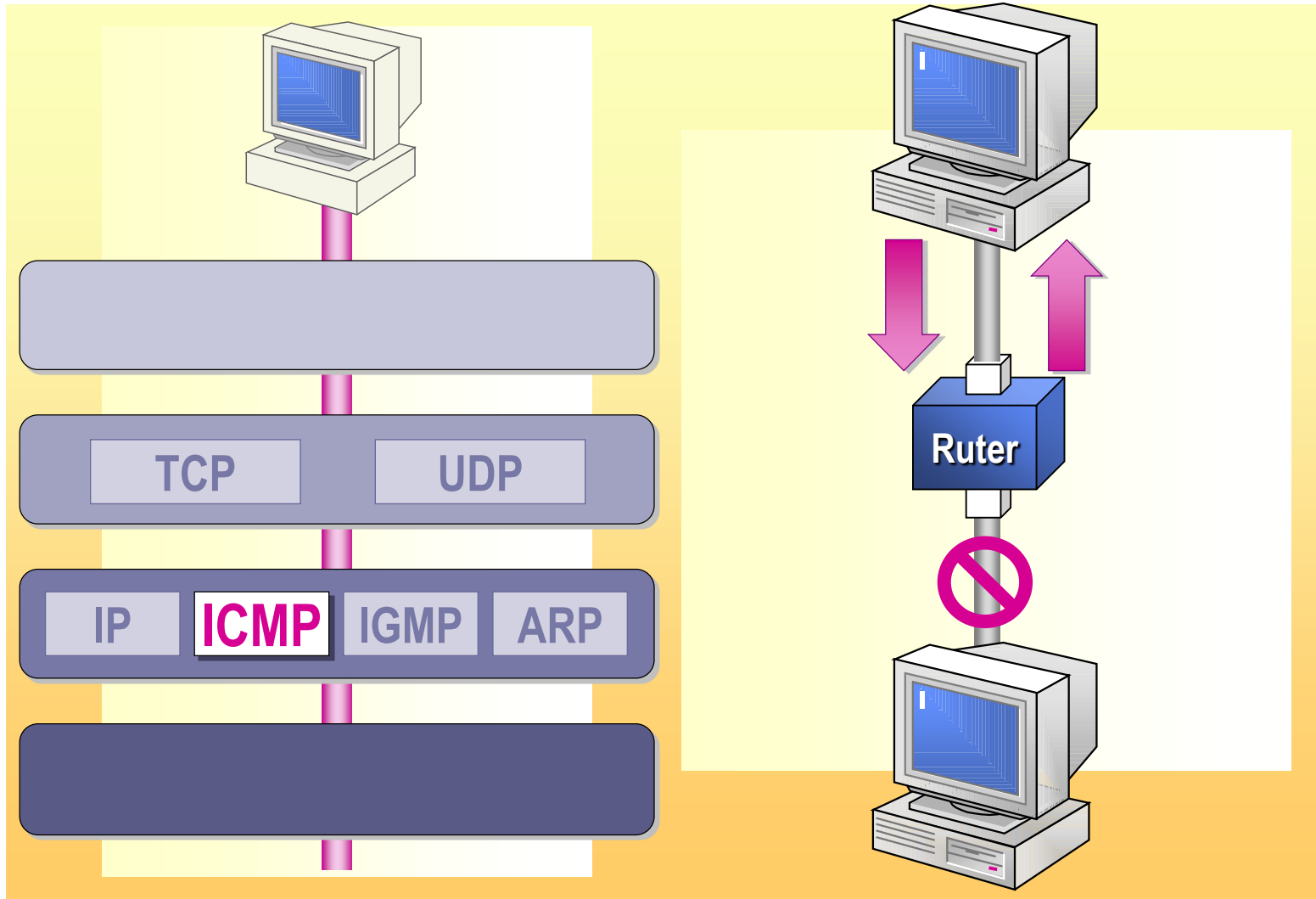
IP (Internet Protocol) na routerze

- dekrementuje TTL
- dzieli duże pakiety
- dla podzielonych pakietów tworzy nowe nagłówki
 - flagi
 - identyfikator
 - przesunięcie fragmentu
- oblicza nowe sumy kontrolne
- zdobywa adres MAC następnego routera
- przesyła pakiet

Internet Control Message Protocol



Internet Control Message Protocol



Internet Control Message Protocol

Internetowy protokół komunikatów kontrolnych.

ICMP jest ściśle związany z protokołem IP, dostarczając nieobecnej w nim funkcji informowania o błędach.

Protokół pozwala wysyłać pakiety kontrolne służące do ustalenia bieżącego stanu hosta, w tym:

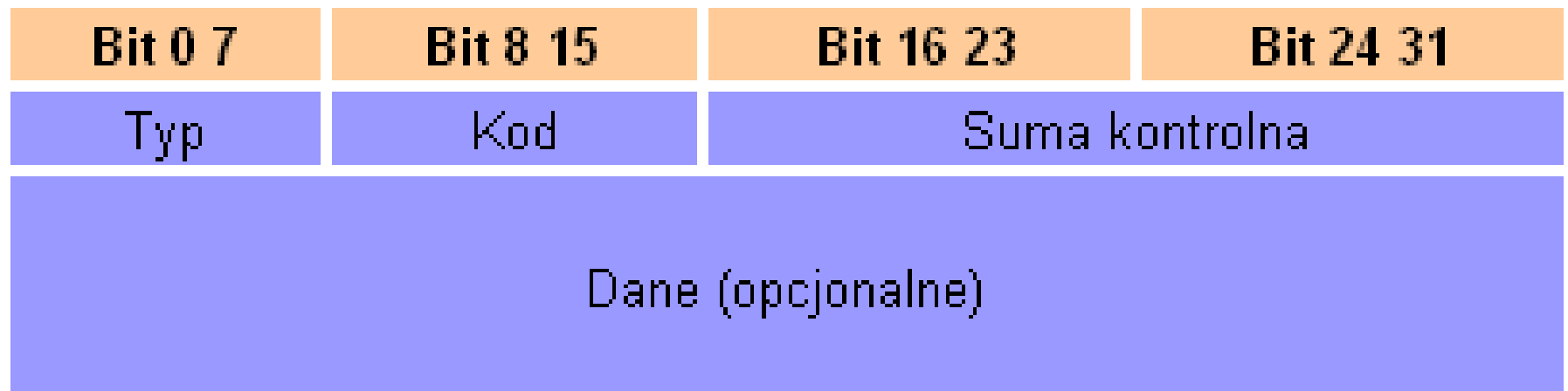
- braku możliwości dostarczenia pakietu do miejsca przeznaczenia,
- określenia opóźnienia pakietów przesyłanych przez sieć,
- zmiana wcześniej wyznaczonej trasy przez jeden z routerów pośredniczących,
- brak wolnej pamięci buforowej dla zapamiętania pakietu i związane z tym chwilowe wstrzymania nadawania,
- przekroczenie czasu życia (TTL) pakietu.

Internet Control Message Protocol

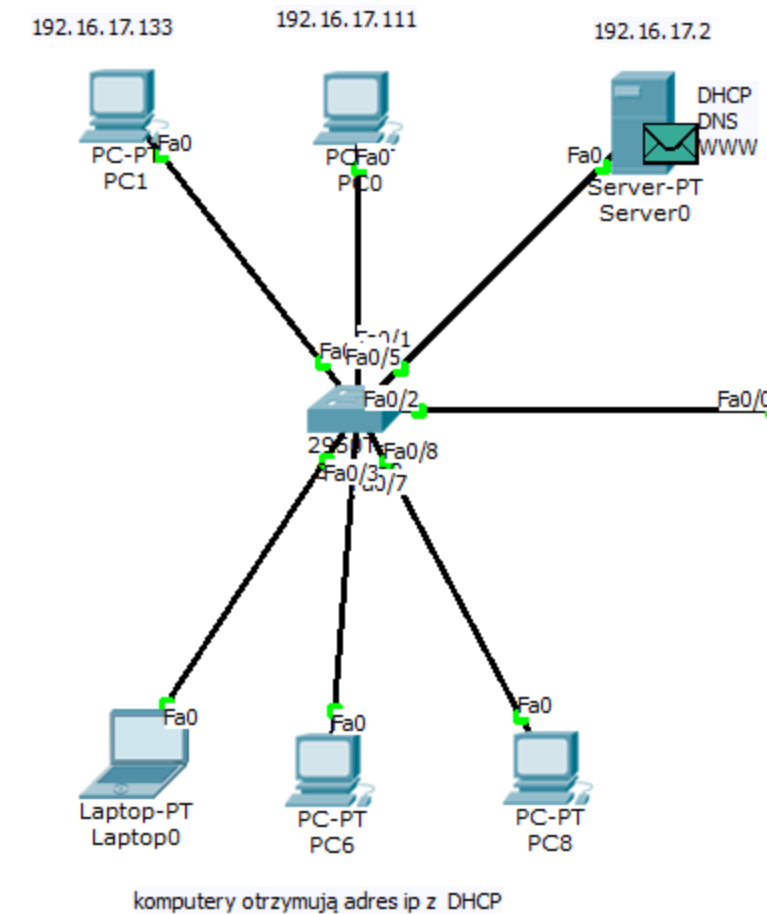
- Datagram IP wędruje od nadawcy do odbiorcy, jeśli nie może być dostarczony w przewidzianym czasie (uszkodzenie, przeciążenie sieci, wyłączenie odbiorcy ...) wówczas do nadawcy zwrótnie dostarczany jest komunikat ICMP-Internet Control Message Protocol (zawiera echo)
- Komunikat ICMP jest przenoszony w polu danych pakietu IP

Internet Control Message Protocol

ramka ICMP



Internet Control Message Protocol



PDU Information at Device: Server0

OSI Model | Inbound PDU Details | Outbound PDU Details

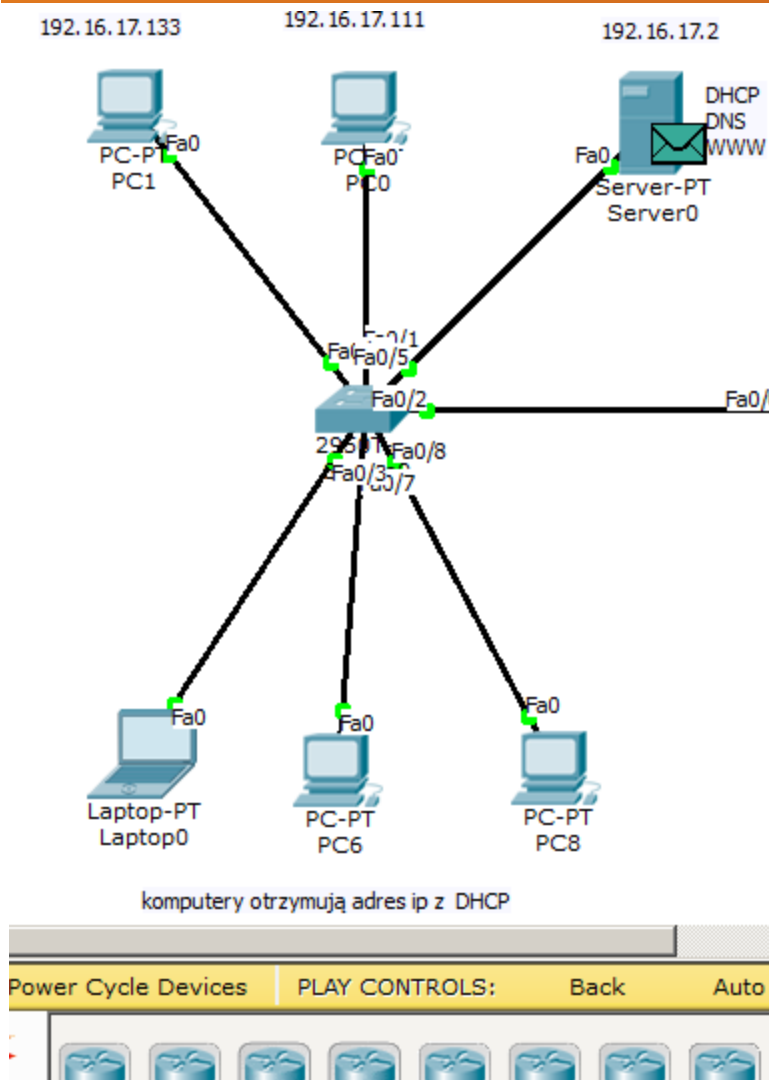
At Device: Server0
Source: Laptop0
Destination: Server0

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 192.16.17.11, Dest. IP: 192.16.17.2 ICMP Message Type: 8	Layer 3: IP Header Src. IP: 192.16.17.2, Dest. IP: 192.16.17.11 ICMP Message Type: 0
Layer 2: Ethernet II Header 0090.2184.170D >> 0003.E40C.4D30	Layer 2: Ethernet II Header 0003.E40C.4D30 >> 0090.2184.170D
Layer 1: Port FastEthernet0	Layer 1: Port(s): FastEthernet0

1. The packet's destination IP address matches the device's IP address or the broadcast address. The device de-encapsulates the packet.
2. The packet is an ICMP packet. The ICMP process processes it.
3. The ICMP process received an Echo Request message.

Challenge Me << Previous Layer Next Layer >>

Internet Control Message Protocol



PDU Information at Device: Server0

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

PREAMBLE: 101010...1011	DEST MAC: 0003.E40C.4D30	SRC MAC: 0090.2184.170D
TYPE: 0x800	DATA (VARIABLE LENGTH)	FCS: 0x0

IP

0	4	8	16	19	31 Bits
4	IHL	DSCP: 0x0	TL: 28		
ID: 0x4		0x0	0x0		
TTL: 255	PRO: 0x1	CHKSUM			
SRC IP: 192.16.17.11					
DST IP: 192.16.17.2					
OPT: 0x0				0x0	
DATA (VARIABLE LENGTH)					

ICMP

0	8	16	31 Bits
TYPE: 0x8	CODE: 0x0	CHECKSUM	
ID: 0x5		SEQ NUMBER: 4	

Internet Control Message Protocol

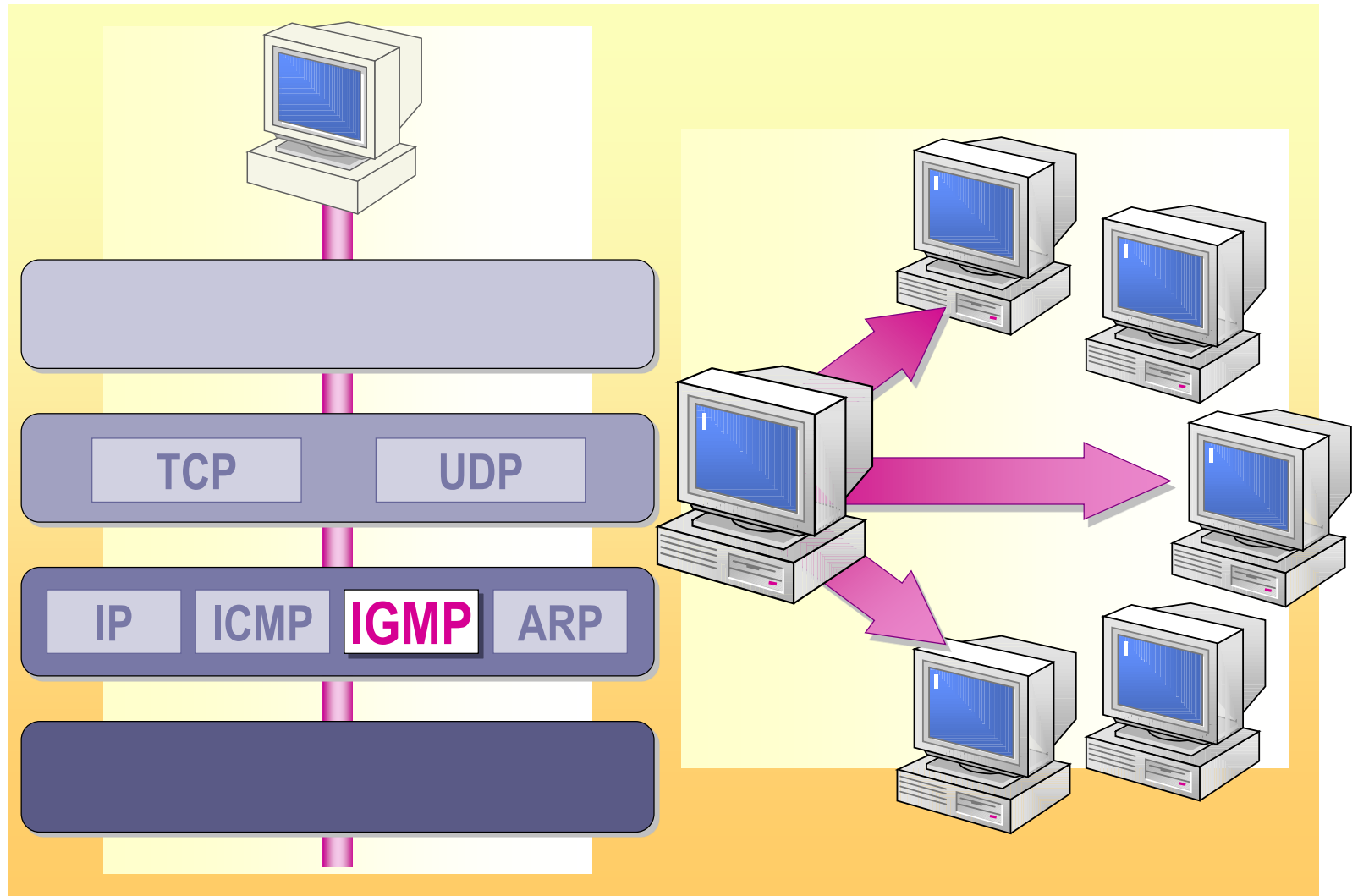
The image shows a Wireshark network traffic capture. The main pane displays a list of packets. Packet 4 is highlighted in blue, representing an ICMP Echo (ping) request. The details pane below shows the structure of this packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.0.103	239.255.255.250	SSDP	389	NOTIFY * HTTP/1.1
2	4.98599100	192.168.0.103	239.255.255.250	SSDP	390	NOTIFY * HTTP/1.1
3	5.07642200	192.168.0.103	239.255.255.250	SSDP	390	NOTIFY * HTTP/1.1
4	5.15855800	192.168.0.106	50.87.146.111	ICMP	42	Echo (ping) request id=0x6358, seq=0/0, ttl=49
5	5.16712100	192.168.0.106	50.87.146.111	TCP	58	33400 > https [SYN] Seq=0 win=3072 Len=0 MSS=1460
6	5.16735900	192.168.0.106	50.87.146.111	TCP	54	33400 > http [ACK] Seq=1 Ack=1 win=3072 Len=0
7	5.16756300	192.168.0.106	50.87.146.111	ICMP	54	Timestamp request id=0x3b37, seq=0/0, ttl=39
8	5.36250500	50.87.146.111	192.168.0.106	ICMP	42	Echo (ping) reply id=0x6358, seq=0/0, ttl=48
9	5.36805500	192.168.0.106	200.13.152.3	DNS	86	Standard query 0x183e PTR 111.146.87.50.in-addr.arpa
10	5.37135900	50.87.146.111	192.168.0.106	TCP	58	https > 33400 [SYN, ACK] Seq=0 Ack=1 win=14600 Len=0 MSS=1440
11	5.40967700	200.13.152.3	192.168.0.106	DNS	198	Standard query response 0x183e PTR 50-87-146-111.unifiedlayer.com
12	5.41360500	192.168.0.106	50.87.146.111	TCP	58	33400 > microsoft-ds [SYN] Seq=0 win=4096 Len=0 MSS=1460
13	5.41386700	192.168.0.106	50.87.146.111	TCP	58	33400 > rfb [SYN] Seq=0 win=2048 Len=0 MSS=1460
14	5.41409700	192.168.0.106	50.87.146.111	TCP	58	33400 > netbios-ssn [SYN] Seq=0 win=1024 Len=0 MSS=1460
15	5.41433600	192.168.0.106	50.87.146.111	TCP	58	33400 > imap [SYN] Seq=0 win=4096 Len=0 MSS=1460

Frame 4: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

- Ethernet II, Src: HonHaiPR_45:55:80 (00:1f:3a:45:55:80), Dst: Tp-LinkT_e1:6c:e8 (a0:f3:c1:e1:6c:e8)
- Internet Protocol version 4, Src: 192.168.0.106 (192.168.0.106), Dst: 50.87.146.111 (50.87.146.111)
- Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Code: 0
 - Checksum: 0x94a7 [correct]
 - Identifier (BE): 25432 (0x6358)
 - Identifier (LE): 22627 (0x5863)
 - Sequence number (BE): 0 (0x0000)
 - Sequence number (LE): 0 (0x0000)
 - [Response In: 8]

Internet Group Management Protocol

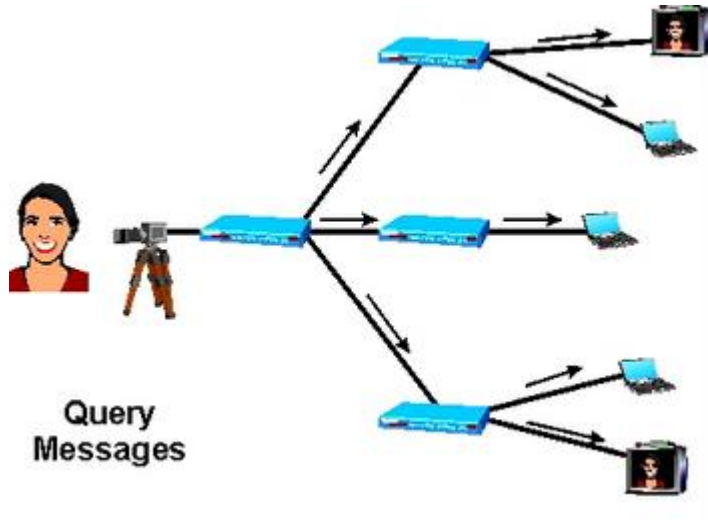


Internet Group Management Protocol

IGMP - jeden z rodziny protokołów TCP/IP.

Służy do zarządzania grupami multicastowymi w sieciach opartych na protokole IP.

Węzły wykorzystują komunikaty IGMP do powiadamiania routerów w swojej sieci o chęci przyłączenia się do lub odejścia z określonej grupy multicastowej.



IGMP Configuration

IGMP Configuration

IGMP Proxy Enable

Upstream Interface WAN
 LAN

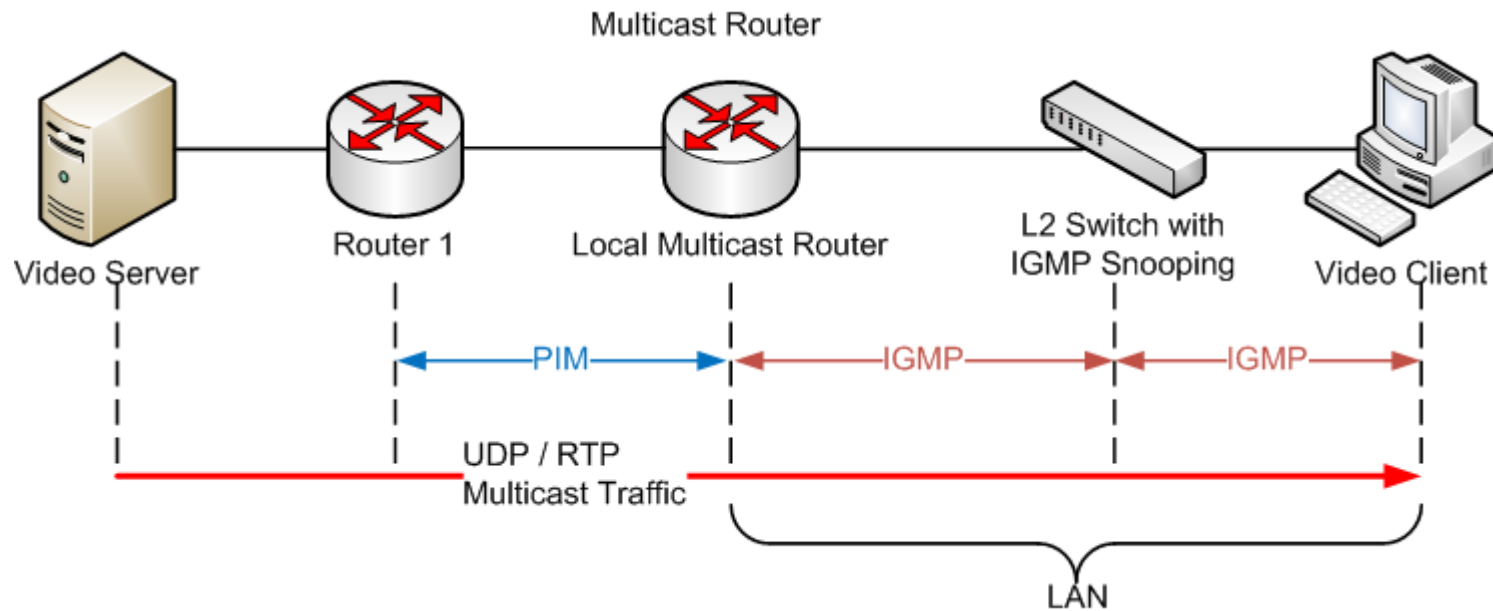
Save Cancel

Allowed Networks Table

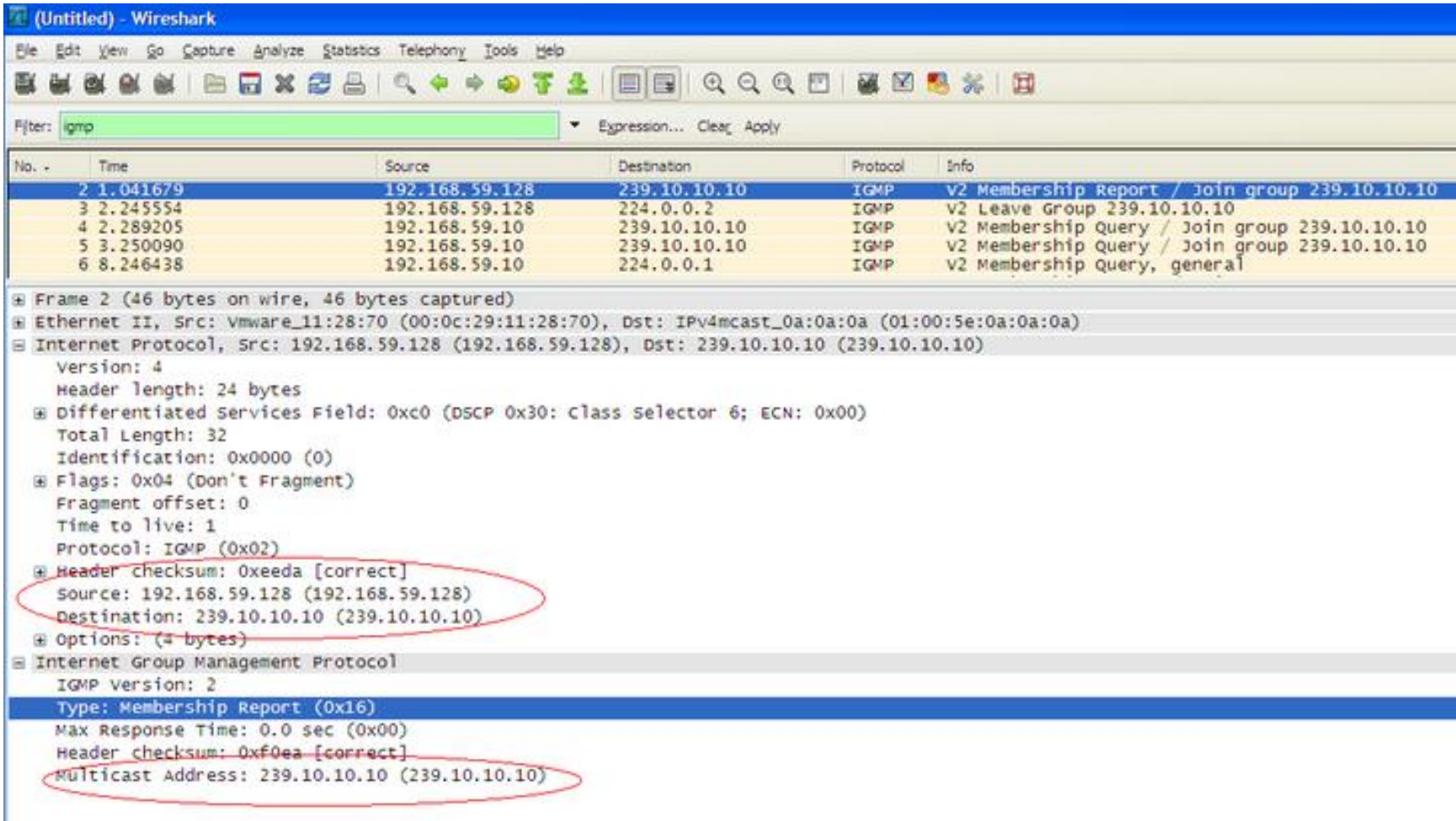
<input type="checkbox"/>	Network Address	Mask Length
<input type="checkbox"/>	0 results found	

Add Edit Delete

Internet Group Management Protocol



Internet Group Management Protocol



The image shows a Wireshark capture of Internet Group Management Protocol (IGMP) traffic. The packet list pane displays six packets, with packet 2 selected. The packet details pane shows the structure of the selected packet, including the IP header and the IGMP membership report.

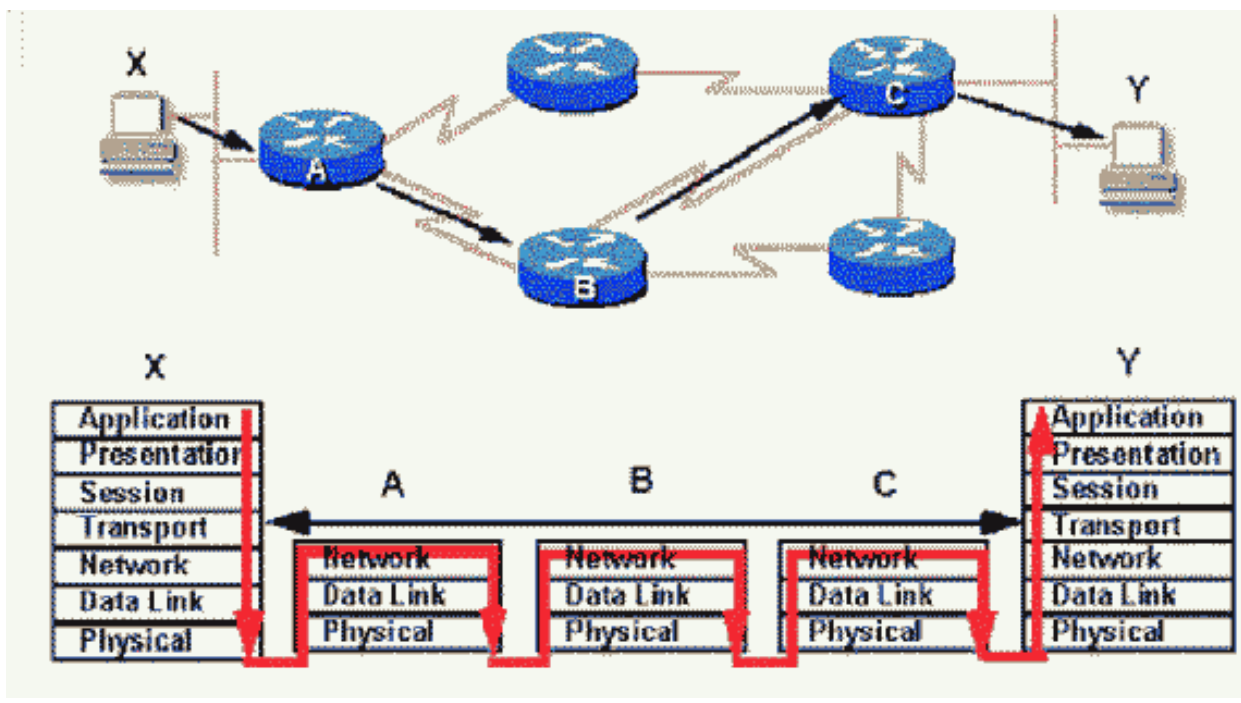
No.	Time	Source	Destination	Protocol	Info
2	1.041679	192.168.59.128	239.10.10.10	IGMP	V2 Membership Report / Join group 239.10.10.10
3	2.245554	192.168.59.128	224.0.0.2	IGMP	V2 Leave Group 239.10.10.10
4	2.289205	192.168.59.10	239.10.10.10	IGMP	V2 Membership Query / Join group 239.10.10.10
5	3.250090	192.168.59.10	239.10.10.10	IGMP	V2 Membership Query / Join group 239.10.10.10
6	8.246438	192.168.59.10	224.0.0.1	IGMP	V2 Membership Query, general

Frame 2 (46 bytes on wire, 46 bytes captured)

- Ethernet II, Src: Vmware_11:28:70 (00:0c:29:11:28:70), Dst: IPv4mcast_0a:0a:0a (01:00:5e:0a:0a:0a)
- Internet Protocol, Src: 192.168.59.128 (192.168.59.128), Dst: 239.10.10.10 (239.10.10.10)
 - Version: 4
 - Header length: 24 bytes
 - Differentiated services Field: 0xc0 (DSCP 0x30: class selector 6; ECN: 0x00)
 - Total Length: 32
 - Identification: 0x0000 (0)
 - Flags: 0x04 (Don't Fragment)
 - Fragment offset: 0
 - Time to live: 1
 - Protocol: IGMP (0x02)
 - Header checksum: 0xeeda [correct]
 - Source: 192.168.59.128 (192.168.59.128)
 - Destination: 239.10.10.10 (239.10.10.10)
 - Options: (4 bytes)
- Internet Group Management Protocol
 - IGMP Version: 2
 - Type: Membership Report (0x16)
 - Max Response Time: 0.0 sec (0x00)
 - Header checksum: 0xf0ea [correct]
 - Multicast Address: 239.10.10.10 (239.10.10.10)

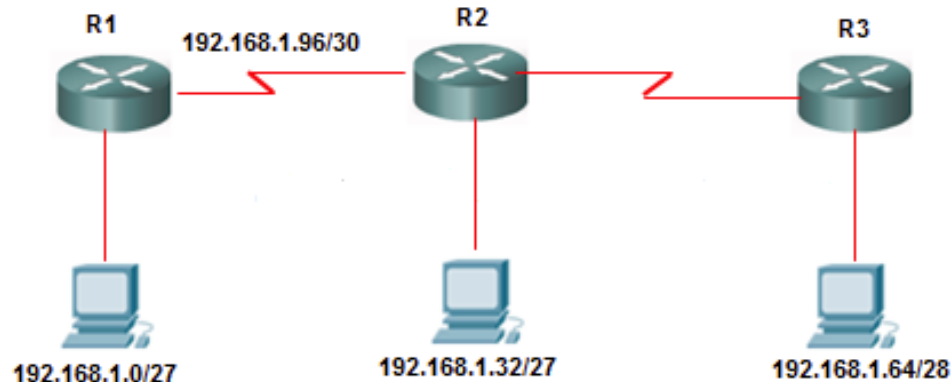
RIP (Routing Information Protocol)

jest protokołem routingu z wykorzystaniem wektora odległości, w którym stosuje się liczbę przeskoków jako metrykę służącą do określenia kierunku i odległości do dowolnego łącza w intersieci. Jeżeli do punktu docelowego prowadzi więcej niż jedna ścieżka, protokół RIP wybierze tę, która zawiera najmniejszą liczbę przeskoków.

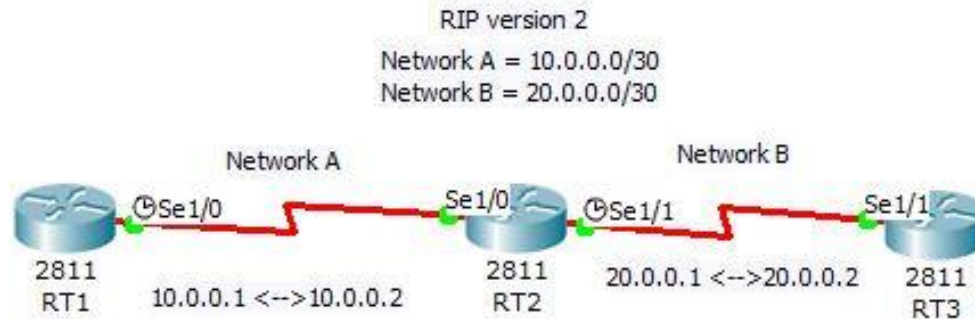


RIP (Routing Information Protocol)

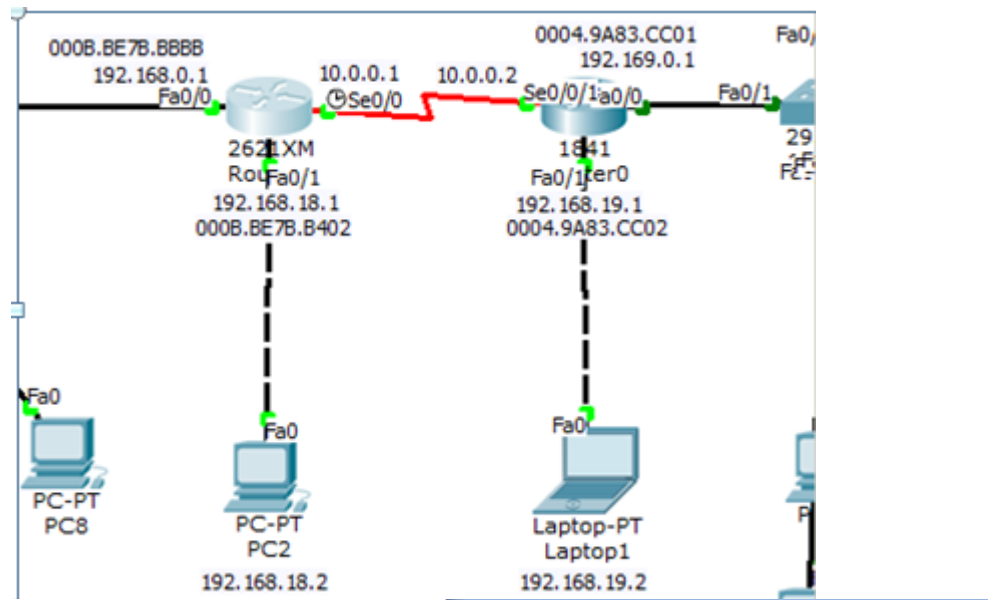
RIP v1 Configuration



Protokół RIPv2 (RIP wersja 2) wysyła w ramach aktualizacji tras informacje dotyczące masek podsieci. Określane jest to mianem routingu bezklasowego.



RIP (Routing Information Protocol)



```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial0/0
C    192.168.0.0/24 is directly connected, FastEthernet0/0
C    192.168.18.0/24 is directly connected, FastEthernet0/1
R    192.168.19.0/24 [120/1] via 10.0.0.2, 00:00:00, Serial0/0
R    192.169.0.0/24 [120/1] via 10.0.0.2, 00:00:00, Serial0/0
Router#
```

OSPF i EIGRP

Open Shortest Path First jest protokołem routingu z wykorzystaniem stanu łącza zaprojektowanym przez organizację IETF (Internet Engineering Task Force) w 1988 roku. Został on opracowany na potrzeby dużych skalowanych intersieci, dla których protokół RIP nie był już wystarczający.

Protokół EIGRP jest własnością firmy Cisco. Protokół EIGRP jest zaawansowaną wersją protokołu IGRP. W szczególności, protokół EIGRP cechuje doskonała wydajność działania, w tym szybka zbieżność i niski narzut na szerokość pasma.

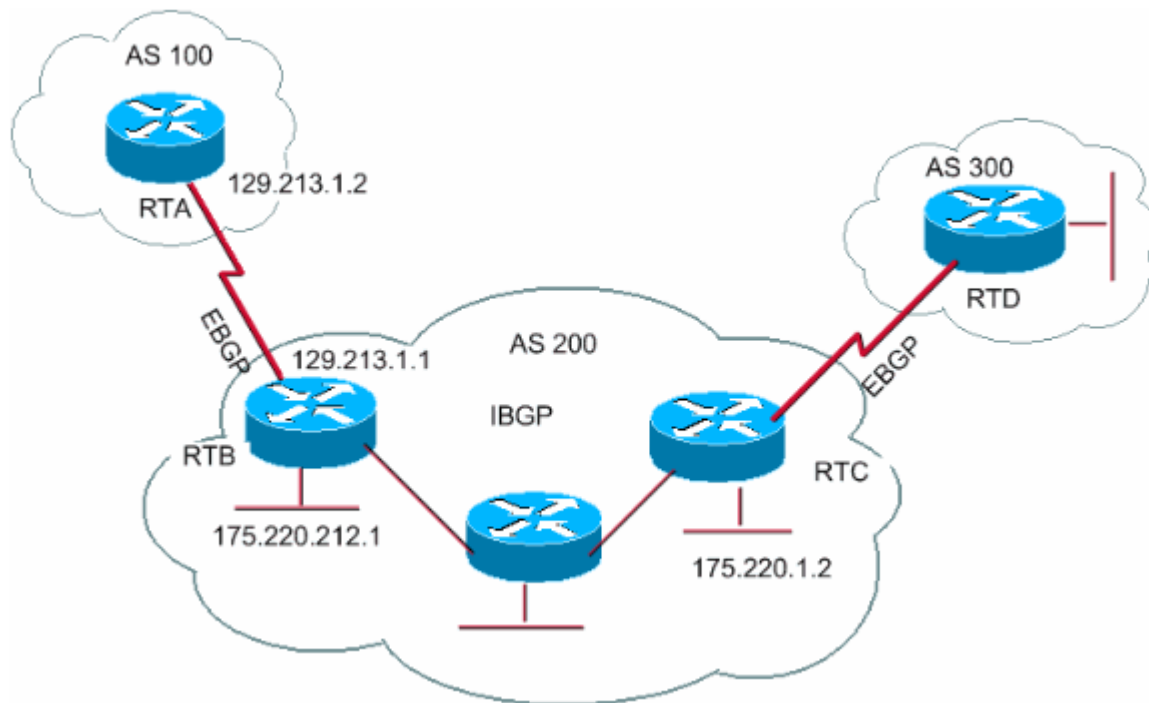
Protokół EIGRP jest zaawansowanym protokołem wektora odległości wykorzystującym także pewne funkcje protokołu stanu łącza. Z tego powodu protokół EIGRP jest czasami określany mianem hybrydowego protokołu routingu.

EGP

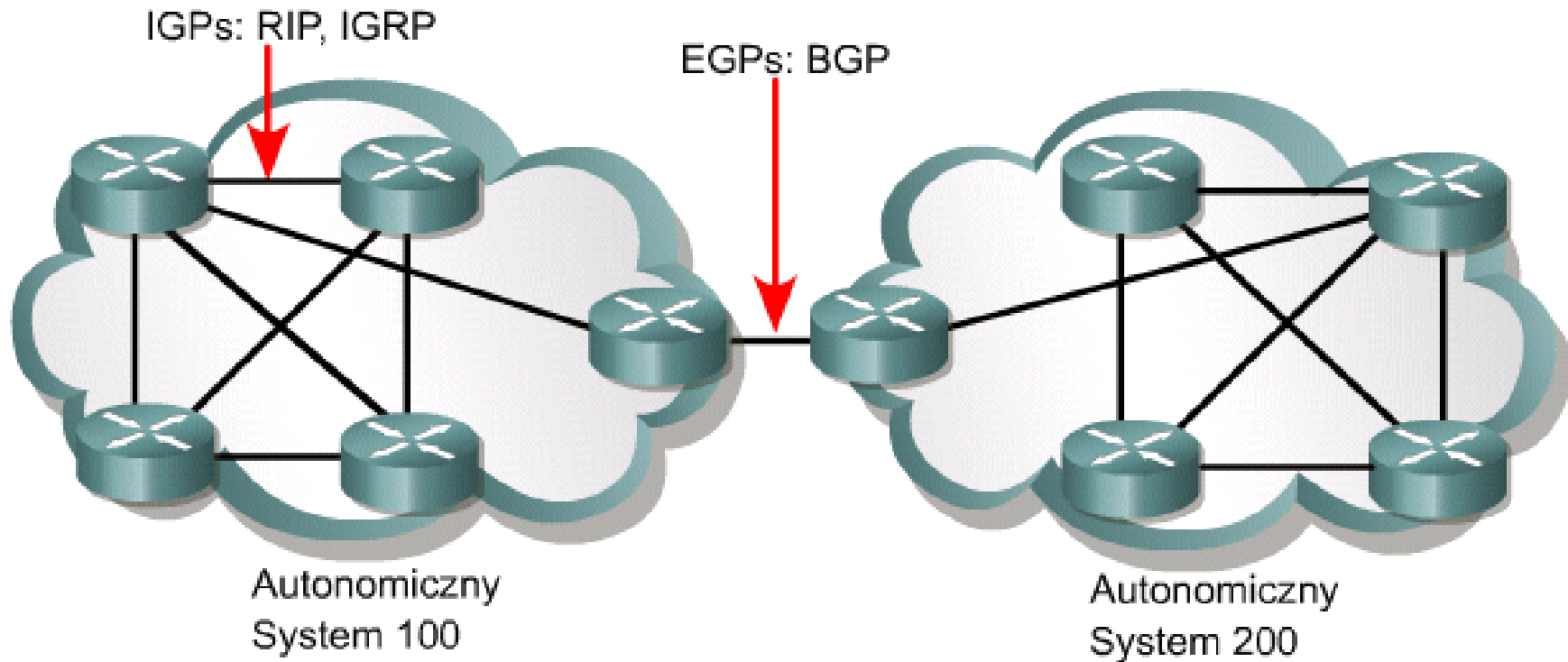
Exterior Gateway Protocol

Protokoły EGP prowadzą routing danych między systemami autonomicznymi.

Przykładem protokołu z rodziny EGP jest protokół BGP (ang. Border Gateway Protocol).

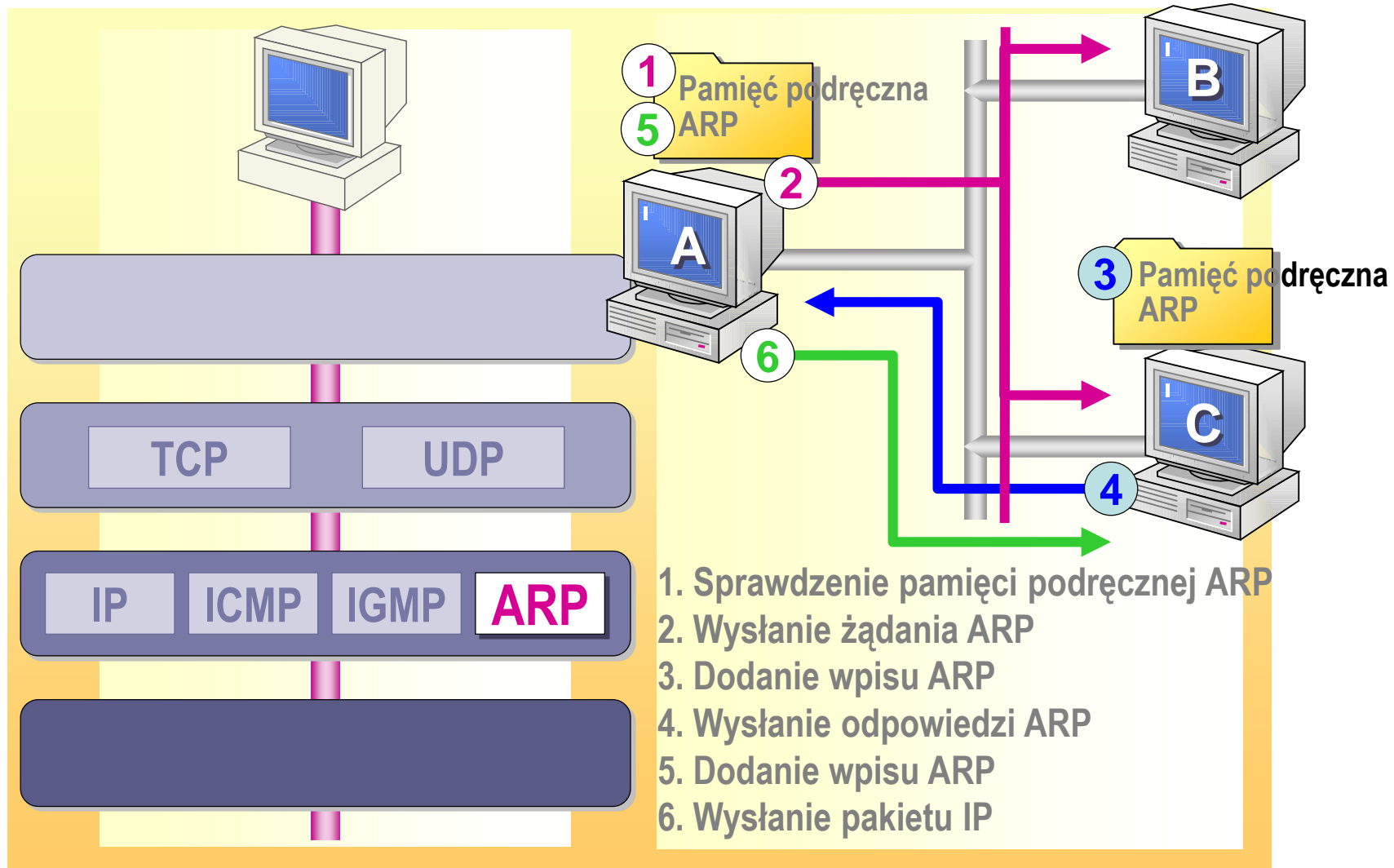


Protokoły routingu, systemy autonomiczne



Protokoły **IGP** (ang. *Interior Gateway Protocols*) i **EGP** (ang. *Exterior Gateway Protocols*) stanowią dwie rodziny protokołów routingu.

Address Resolution Protocol



Address Resolution Protocol

Protokół komunikacyjny przekształcania adresów IP (ustalanych autorytarnie przez użytkownika/administratora) na fizyczne, 48-bitowe adresy MAC (przypisane fizycznie m.in. do kart sieciowych) w komputerowych sieciach lokalnych typu Ethernet.

Każdy komputer w sieci powinien posiadać tzw. tablicę ARP. Znajduje się w niej adres IP i przypisany do niego adres MAC. Dzięki temu komputery mogą się ze sobą komunikować za pośrednictwem adresu MAC, ale tylko w obrębie danej sieci LAN. Jeśli jakieś informacje mają być przesłane do innej sieci (lub podsieci w sieci złożonej, sieci oddzielonej routerem, itp.), to adres MAC musi być zastąpiony adresem IP.

ARP jest protokołem pracującym na drugiej warstwie modelu ISO/OSI, czyli warstwie łącza danych, pracuje ona na ramkach i może je analizować tzn. np. sprawdzać ich poprawność.

Protokół ARP jest zdefiniowany w dyrektywie RFC 826.

Address Resolution Protocol

- mapowanie adresów MAC do adresów IP
- rozwiązywanie adresów IP na adresy MAC
- ARP używa BROADCAST'u aby rozwiązać adres IP lokalnego hosta
- rozwiązywane adresy przechowywane są w cache'u

Address Resolution Protocol

struktura ramki

+	Bity 0 - 7	8 - 15	16 - 31
0	Typ warstwy fizycznej (HTYPE)		Typ protokołu wyższej warstwy (PTYPE)
32	Długość adresu sprzętowego (HLEN)	Długość protokołu wyższej warstwy (PLEN)	Operacja (OPER)
64	Adres sprzętowy źródła (SHA)		
?	Adres protokołu wyższej warstwy źródła (SPA)		
?	Adres sprzętowy przeznaczenia (THA)		
?	Adres protokołu wyższej warstwy przeznaczenia (TPA)		

Address Resolution Protocol

Zasada działania

ARP działa w następujący sposób:

1. Utworzenie pakietu z szukanym adresem IP.
2. Wysłanie pakietu w obrębie danej sieci.
3. Wysłany pakiet odbierają wszystkie hosty podłączone do sieci.
Jako jedyny odpowiada host o szukanym IP
- przesyła pakiet z odpowiedzią zawierającą adres MAC.
4. Host szukający po odebraniu pakietu z szukanym adresem MAC zapisuje go w pamięci podręcznej, dzięki czemu nie musi później szukać jeszcze raz tego samego adresu.

Address Resolution Protocol

Działanie protokołu ARP

- kiedy urządzenie Ethernet chce wysłać pakiet IP **potrzebuje adresu MAC** urządzenia docelowego, dla którego zna adres IP
- w tym celu wysyłana jest na adres **rozgłoszeniowy** ramka z zapytaniem **ARP Request**
- urządzenie, które rozpoznaje swój adres IP, wysyła w odpowiedzi ramkę **ARP Response** skierowaną do stacji, która wysłała zapytanie

Address Resolution Protocol

Zasada działania ARP



Gdy komputer A chce odwzorować adres IP_C komputera C - rozgłasza specjalny pakiet, w którym prosi komputer o adresie IP_C , aby dał odpowiedź zawierającą jego adres fizyczny F_C . Wszystkie komputery - w tym C - otrzymują tę prośbę ale ...

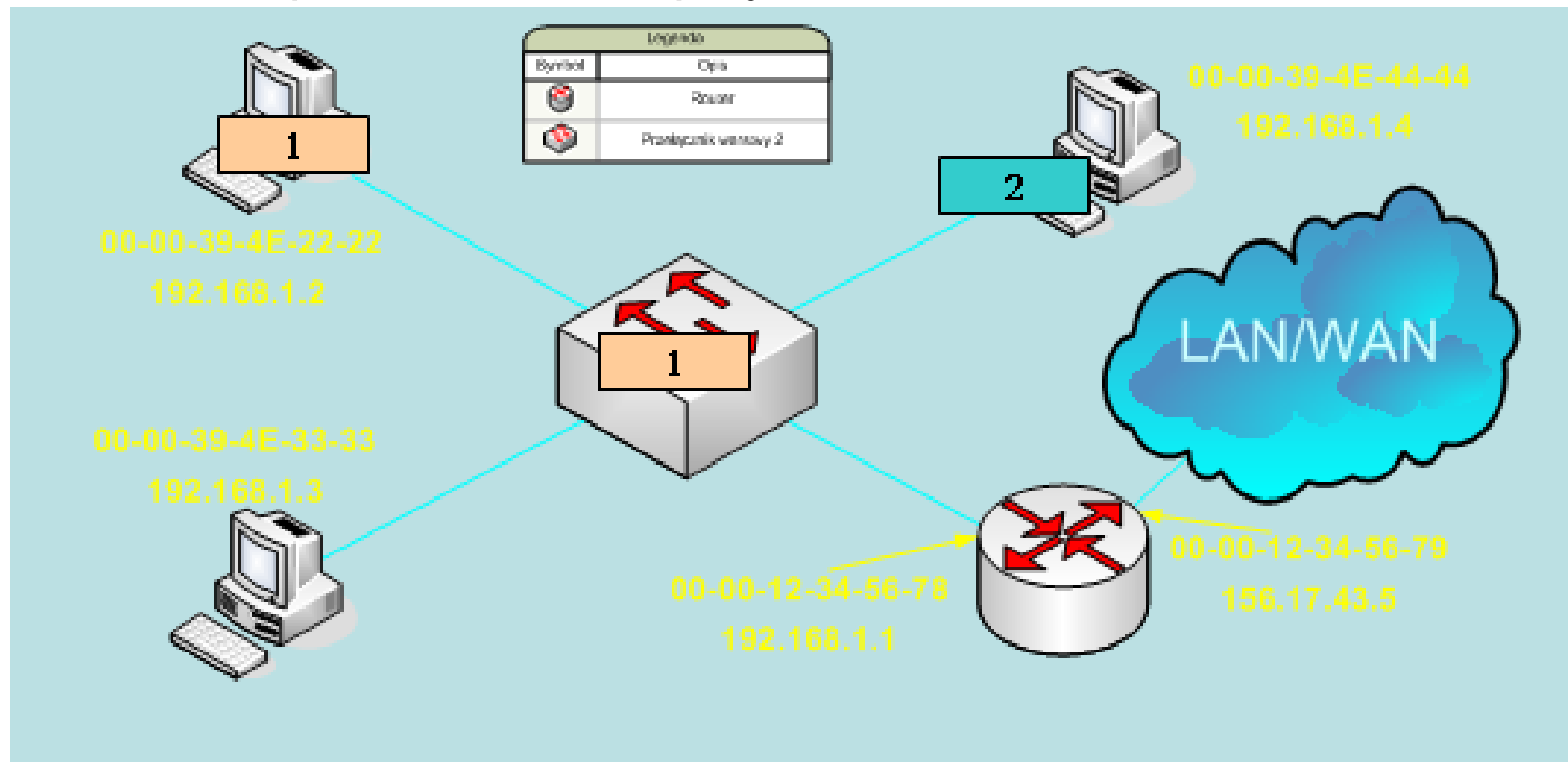


... tylko komputer C rozpoznając swój adres IP_C wysyła odpowiedź, która zawiera jego adres fizyczny F_C . Gdy A otrzyma odpowiedź, przy użyciu otrzymanego adresu fizycznego przesyła pakiet bezpośrednio do C.

Protokół ARP umożliwia komputerowi odnajdywanie fizycznego adresu maszyny docelowej z tej samej sieci fizycznej przy użyciu jedynie adresu IP.

Address Resolution Protocol

- Działanie protokołu ARP – przykład 1

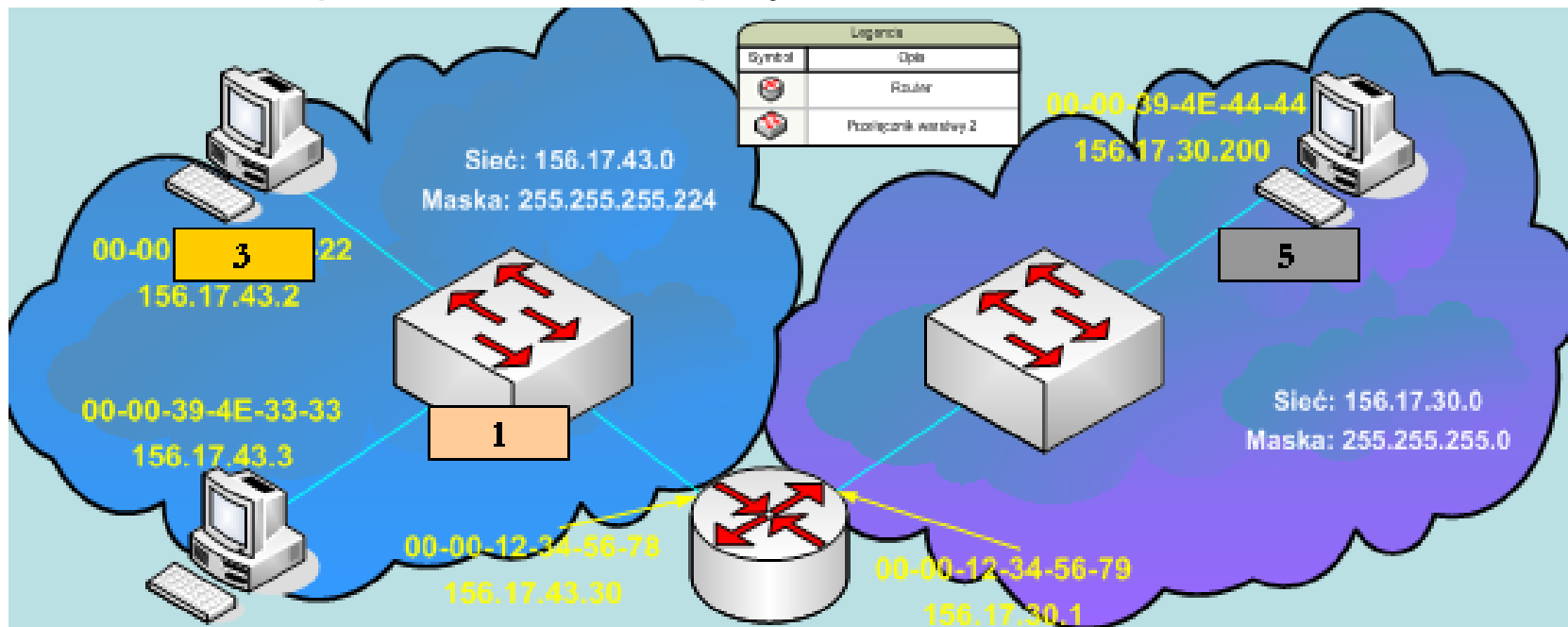


Ramka nr. 2 ARP Response

Nagłówek ramki Ethernet		Pole danych ramki - wybrane pola ARP		
MAC docelowy	MAC nadawcy	Op.	MAC docelowy	IP docelowy
00-00-39-4E-22-22	00-00-39-4E-44-44	2	00-00-39-4E-44-44	192.168.1.4

Address Resolution Protocol

- Działanie protokołu ARP – przykład 2



Stacja 156.17.43.2 ma do wysłania pakiet IP do stacji 156.17.30.200.
Tablice ARP urządzeń są puste.

Ramka nr. 6 Pakiet IP

Nagłówek ramki Ethernet		Pole danych ramki – wybrane pola pakietu IP		
MAC docelowy	MAC nadawcy	IP docelowy	IP źródłowy	Dane
00-00-39-4E-44-44	00-00-12-34-56-79	156.17.30.200	156.17.43.2	E46A

Address Resolution Protocol

Tablica pamięci ARP

- W celu usprawnienia działania protokołu ARP, urządzenia przechowują w **pamięci tablicy ARP** (ang. ARP Cache) zawierające poznane skojarzenia adresów MAC i IP
- Wpisy w tablicy pamięci ARP mają **określony czas trwania**
- Jeżeli w tym czasie zostanie odebrany przez urządzenie pakiet **potwierdzający** wpis w pamięci, to czas trwania jest **wydłużany**
- Jeżeli w tablicy pamięci ARP **nie ma wpisu** dotyczącego danego adresu IP, to urządzenie **wysyła zapytanie ARP**

Address Resolution Protocol

Podsumowanie ARP

- ARP **nie jest** częścią protokołu **IP**
- Zapytania ARP używają transmisji typu **broadcast**, nigdy **nie opuszczają logicznej podsieci** (domeny rozgłoszeniowej)
- Zapytania i odpowiedzi ARP używają ramek warstwy łącza danych, więc **nie mogą być rutowane** do innych podsieci
- Wpisy w tablicy **cache ARP** powinny mieć **ograniczony czas trwania**

Address Resolution Protocol

The screenshot displays a Packet Tracer simulation environment. On the left, a network diagram shows a central switch connected to several devices: PC1 (192.16.17.133), PC0 (192.16.17.111), Server0 (192.16.17.2), Laptop0, and PC6. The switch has multiple interfaces labeled Fa0/1 through Fa0/8. Below the diagram is a toolbar with icons for Routers, PCs, Laptops, and Servers.

In the center, two Command Prompt windows are open. The top window is for PC0, showing the output of the 'arp -a' command:

```
Packet Tracer PC Command Line 1.0
PC>arp -a
No ARP Entries Found
PC>arp -a
No ARP Entries Found
PC>arp -a
No ARP Entries Found
PC>arp -a
No ARP Entries Found
PC>arp -a
No ARP Entries Found
PC>arp -a
No ARP Entries Found
PC>arp -a
Internet Address      Physical Address      Type
192.16.17.2           0003.e40c.4d30       dynamic
PC>
```

The bottom window is for Server0, showing the output of the 'arp -a' command:

```
Packet Tracer SERVER Command Line 1.0
SERVER>arp -a
Internet Address      Physical Address      Type
192.16.17.11         0090.2184.170d       dynamic
SERVER>arp -a
Internet Address      Physical Address      Type
192.16.17.11         0090.2184.170d       dynamic
SERVER>
```

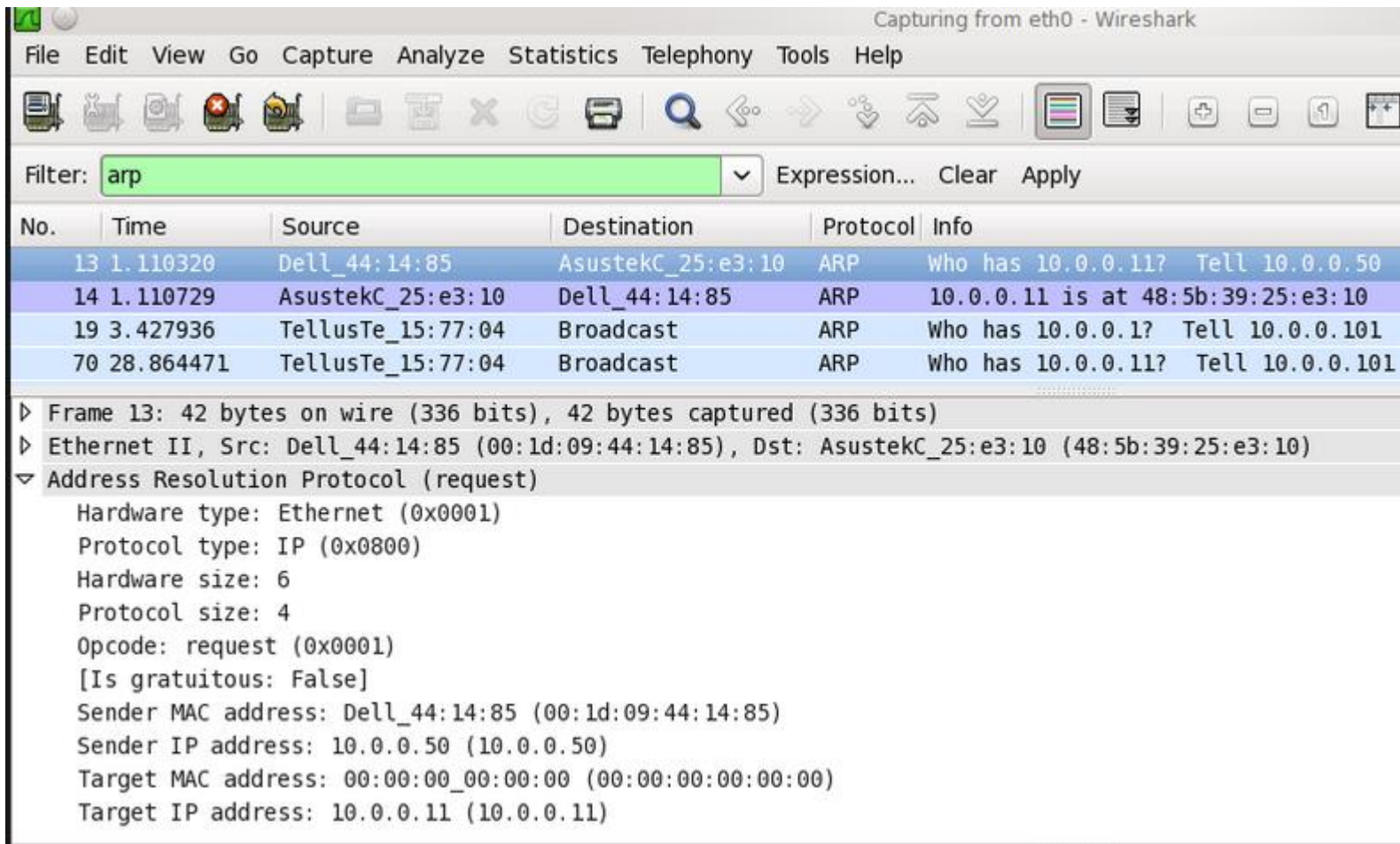
On the right side, the Simulation Panel is visible, showing an Event List table:

Time(sec)	Last Device	At Device	Type
0.001	Laptop0	Switch0	ARP
0.002	Switch0	PC0	ARP
0.002	Switch0	Router1	ARP
0.002	Switch0	Server0	ARP
0.002	Switch0	PC6	ARP
0.002	Switch0	PC1	ARP
0.003	Server0	Switch0	ARP
0.004	Switch0	Laptop0	ARP

Below the Event List, there is a table for the Simulation:

Destination	Type	Color	Time (sec)	Periodic	Num
Server0	ICMP	Red	0.000	N	0

Address Resolution Protocol



Capturing from eth0 - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: arp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
13	1.110320	Dell_44:14:85	AsustekC_25:e3:10	ARP	Who has 10.0.0.11? Tell 10.0.0.50
14	1.110729	AsustekC_25:e3:10	Dell_44:14:85	ARP	10.0.0.11 is at 48:5b:39:25:e3:10
19	3.427936	TellusTe_15:77:04	Broadcast	ARP	Who has 10.0.0.1? Tell 10.0.0.101
70	28.864471	TellusTe_15:77:04	Broadcast	ARP	Who has 10.0.0.11? Tell 10.0.0.101

▶ Frame 13: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)

▶ Ethernet II, Src: Dell_44:14:85 (00:1d:09:44:14:85), Dst: AsustekC_25:e3:10 (48:5b:39:25:e3:10)

▼ Address Resolution Protocol (request)

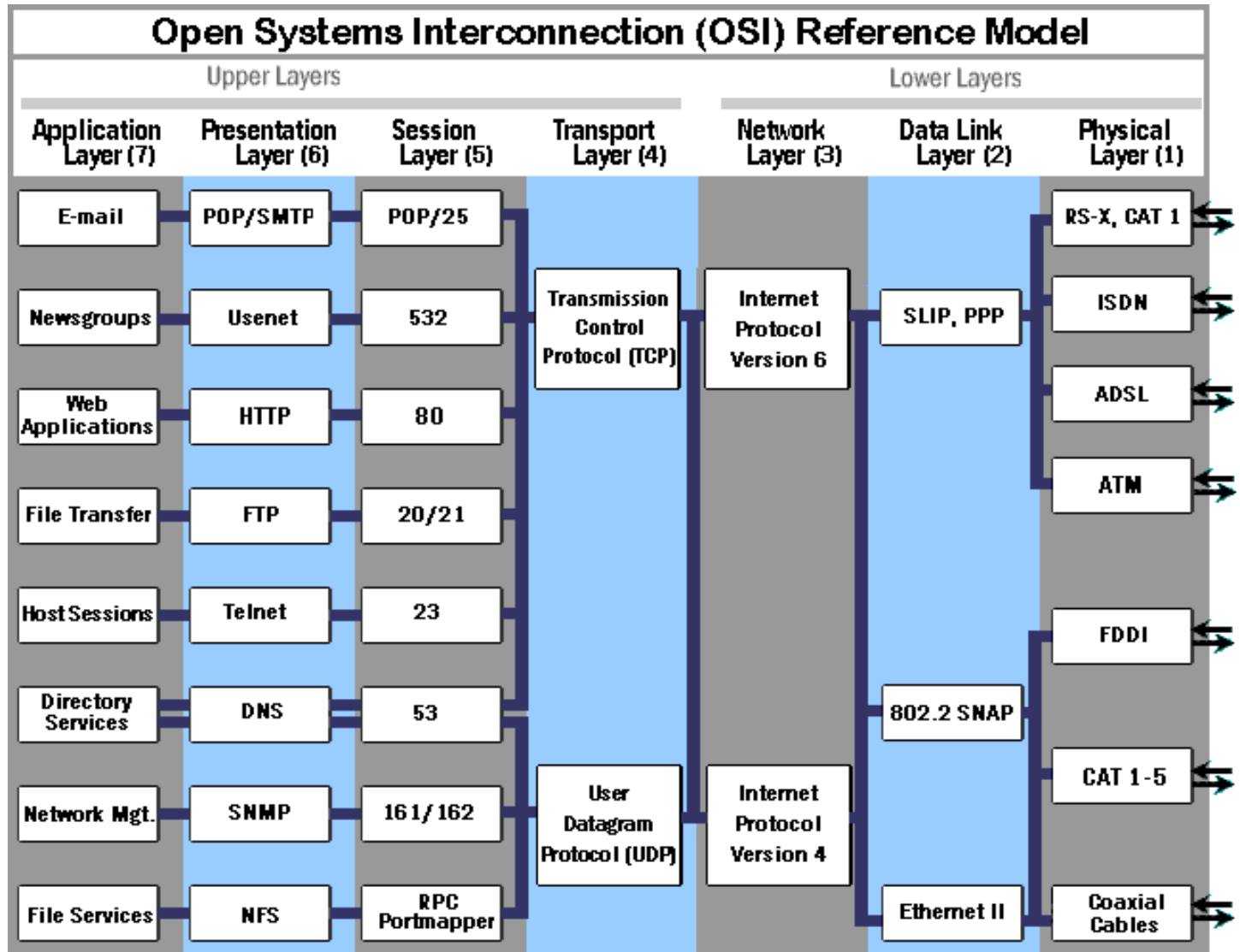
- Hardware type: Ethernet (0x0001)
- Protocol type: IP (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (0x0001)
- [Is gratuitous: False]
- Sender MAC address: Dell_44:14:85 (00:1d:09:44:14:85)
- Sender IP address: 10.0.0.50 (10.0.0.50)
- Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
- Target IP address: 10.0.0.11 (10.0.0.11)

Reverse Address Resolution Protocol

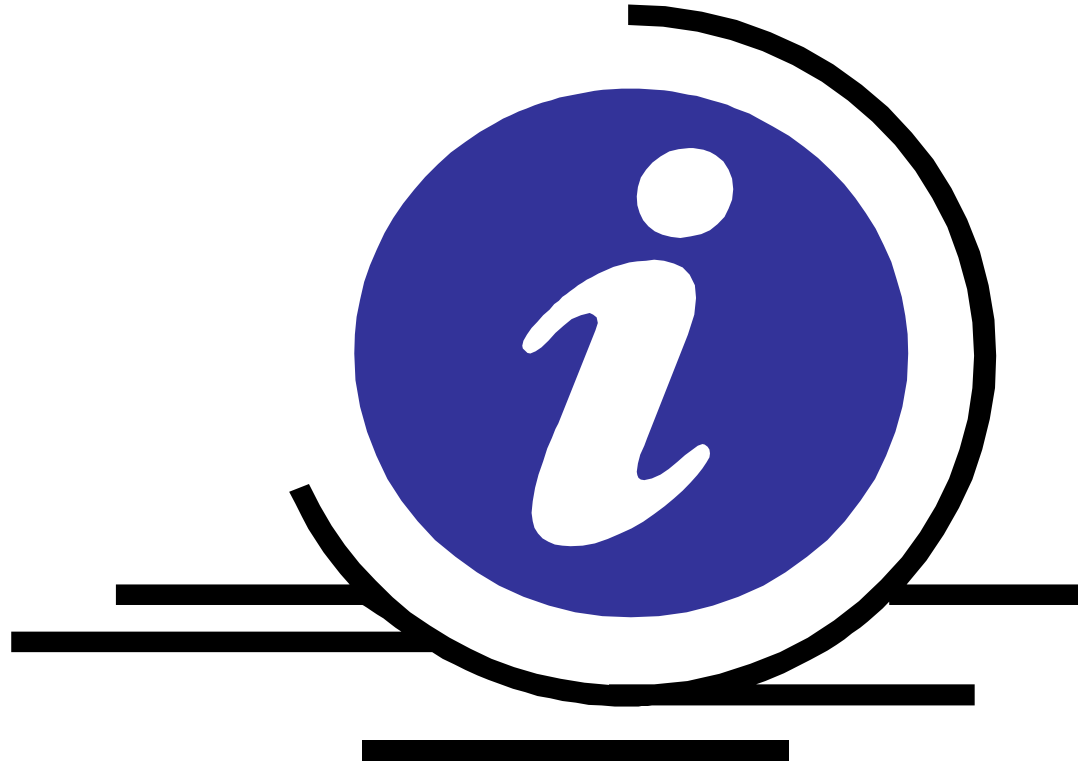
RARP

protokół komunikacyjny przekształcania 48-bitowych fizycznych adresów MAC na 32-bitowe adresy IP w komputerowych sieciach typu Ethernet.

Warstwa sieci / OSI

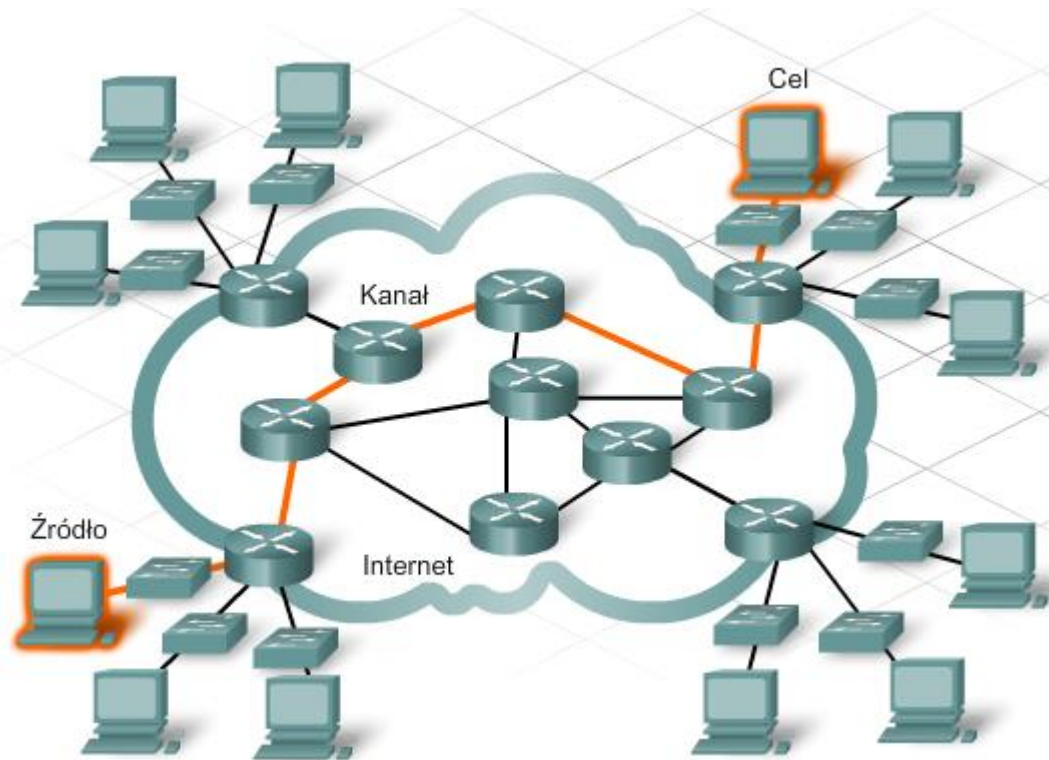


Pytania



Przesyłanie danych w sieci

- Tryb połączeniowy - przed rozpoczęciem komunikacji następuje nawiązanie logicznego połączenia pomiędzy oboma urządzeniami.
- Tryb bezpołączeniowy - komunikaty wysyłane są niezależnie.



Tryb połączeniowy

Po wybraniu najkrótszej trasy z węzła A do węzła Y, która przebiega przez węzły C i D wysyłane jest żądanie zestawienia połączenia od węzła początkowego A do węzła kolejnego C.

Po otrzymaniu potwierdzenia żądanie przekazywane jest dalej od C do D i następnie do Y.

Po zestawieniu całej trasy od węzła ostatniego wysyłane jest potwierdzenie do węzła początkowego.

Po zestawianiu trasa następuje przesyłanie danych.

Po zakończeniu przesyłania następuje rozłączanie trasy - od węzła początkowego do końcowego, z potwierdzeniem w kierunku odwrotnym.

Tryb połączeniowy

- posiada mechanizmy kontroli błędów:
 - potwierdzenie zestawienia połączenia,
 - gdy zostanie przekroczony limit czasu (brak potwierdzenia odbioru ramki od stacji docelowej) - retransmisja danych,
 - suma kontrolna sprawdzana w węźle docelowym.

Tryb bezpołączeniowy

Nie ma tu potwierdzeń zestawienia połączenia.

Zaraz po znalezieniu drogi rozpoczyna się transmisja.

Podobnie jak w trybie połączeniowym - gdy pakiet dotrze do węzła docelowego wysyłane jest potwierdzenie.

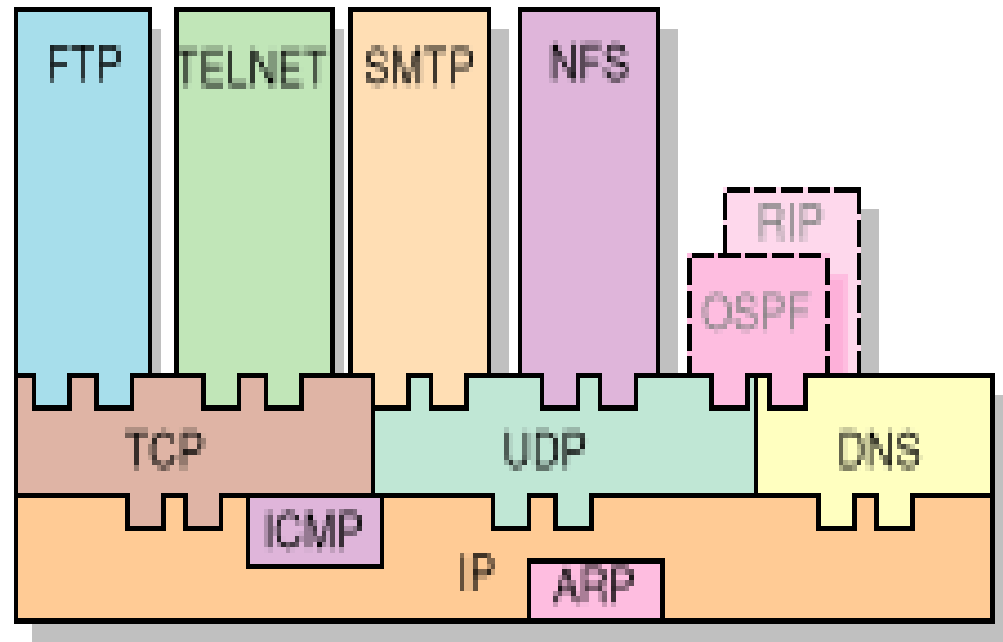
Pakiety wysyłane są niezależnie od siebie, może się zatem zdarzyć taka sytuacja, iż pójdą one różnymi trasami i dotrą do celu w innej kolejności. Stąd też potrzeba ich numerowania oraz układania w odpowiednim porządku w stacji docelowej.

ISO/OSI i stos protokołów TCP/IP

ISO/OSI



TCP/IP



znane porty 0-1023

<http://www.iana.org/assignments/port-numbers>

...

ftp 21/tcp File Transfer [Control]

ftp 21/udp File Transfer [Control] # Jon Postel postel@isi.edu

ssh 22/tcp SSH Remote Login Protocol

ssh 22/udp SSH Remote Login Protocol # Tatu Ylonen ylo@cs.hut.fi

telnet 23/tcp Telnet telnet 23/udp Telnet # Jon Postel postel@isi.edu

24/tcp any private mail system

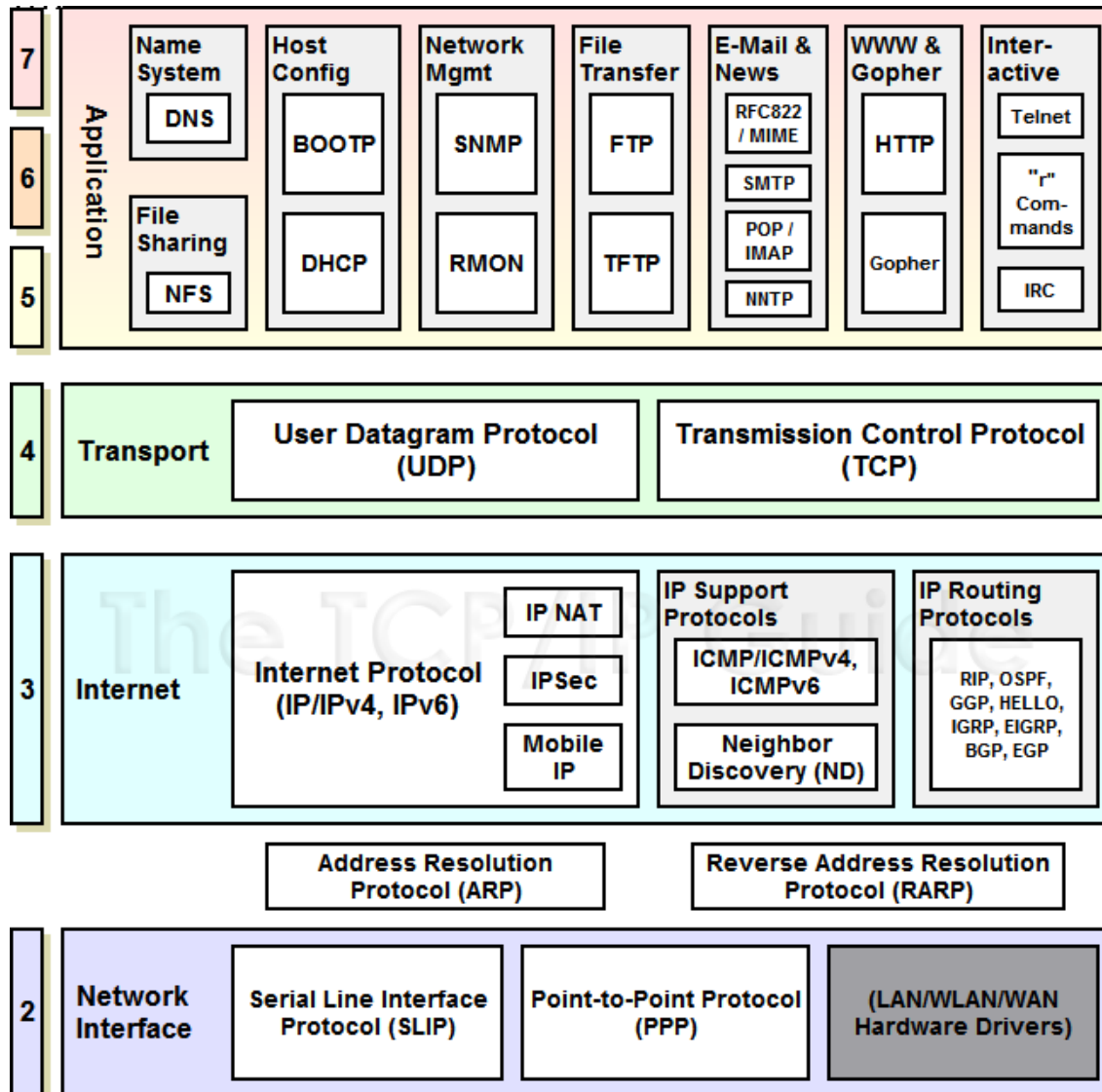
24/udp any private mail system # Rick Adams <rick@UUNET.UU.NET>

smtp 25/tcp Simple Mail Transfer

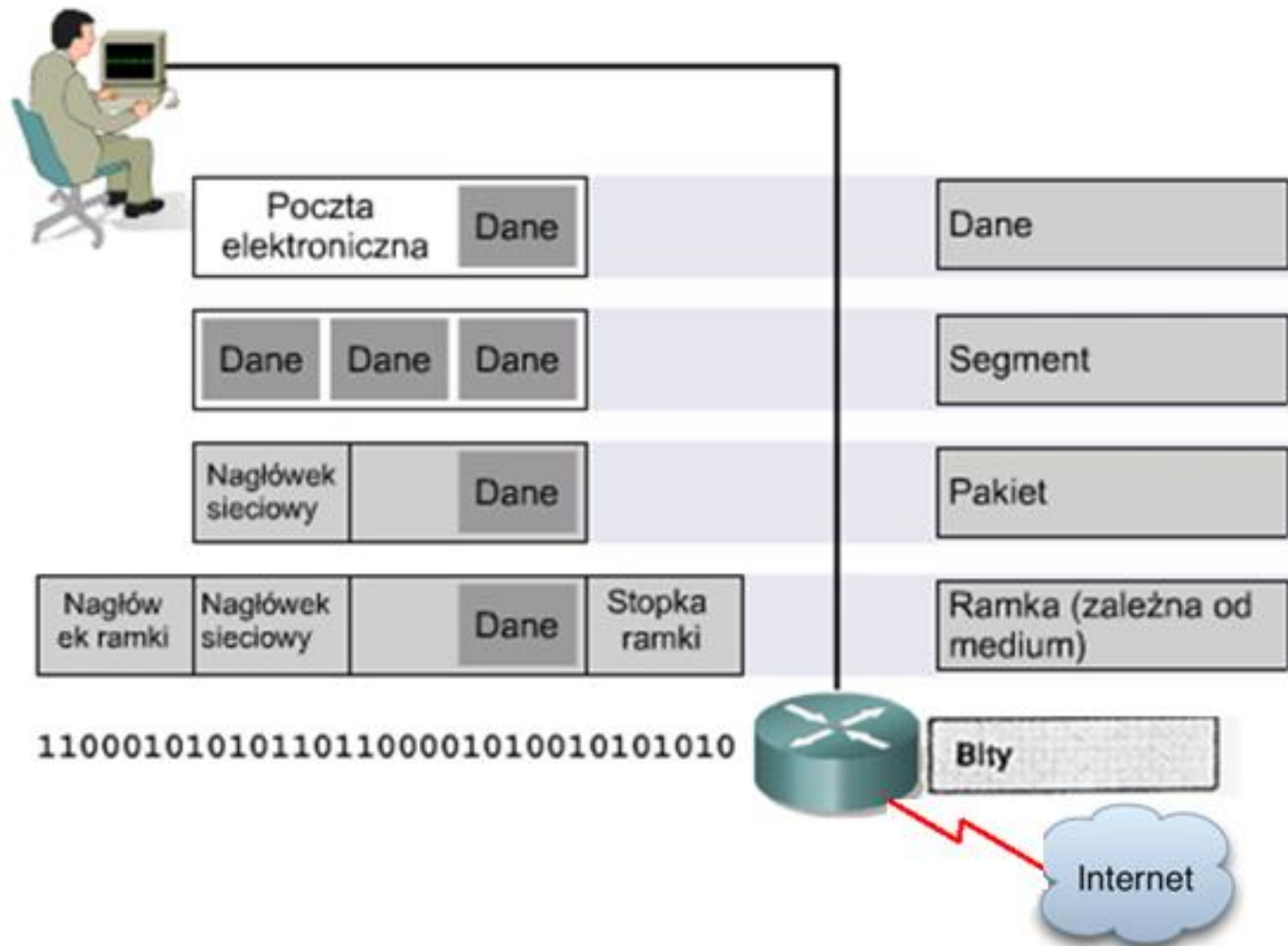
smtp 25/udp Simple Mail Transfer

...

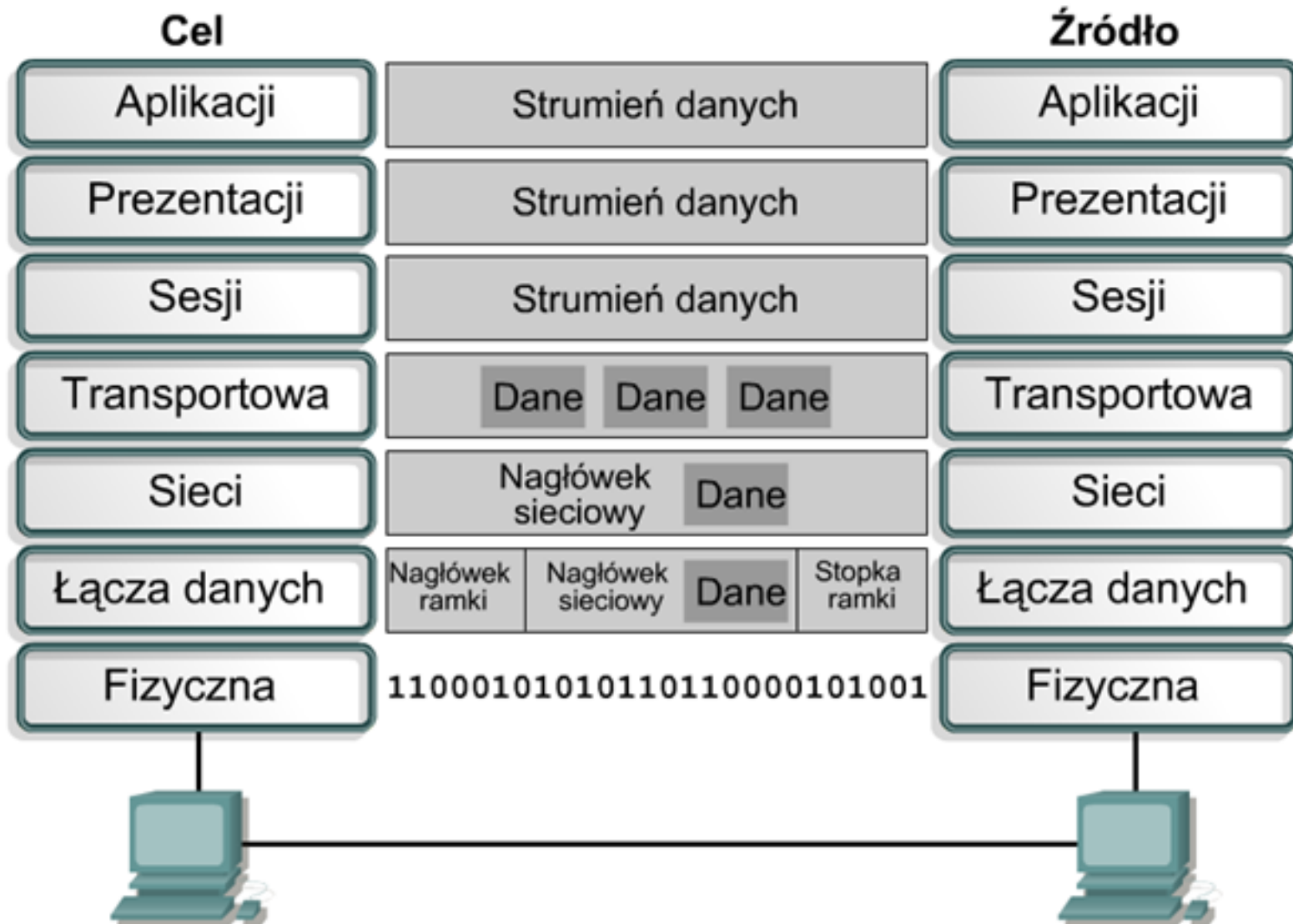
Stos protokołów TCP/IP / protokoły dostępu



Mechanizm enkapsulacji



Mechanizm enkapsulacji



Mechanizm enkapsulacji

