

DOBRA ATMOSFERA NA SIECIACH,



JEST KLUCZEM DO SUKCESU

Spis treści

1. SIECI KOMPUTEROWE – TEORIA	6
1.1 SIECI KOMPUTEROWE I INTERNET	6
1.0.1 ODPOWIEDŹ Czym jest sieć komputerowa?	6
1.0.2 ODPOWIEDŹ Podział sieci ze względu na wielkość	6
1.0.3 ODPOWIEDŹ Wymień urządzenia sieciowe	9
• ROUTERY SIECI DOMOWEJ (WAN/LAN)	10
1.1.1 ODPOWIEDŹ 1 Czym jest Internet.....	18
1.1.2 ODPOWIEDŹ 2 Co to znaczy, że Internet jest infrastrukturą zapewniającą usługi dla aplikacji?.....	19
1.1.3 ODPOWIEDŹ 3 Co to jest API?.....	19
1.1.4 ODPOWIEDŹ 5 Jaką analogię możemy zastosować, aby wyjaśnić czym jest protokół sieciowy?	19
1.1.5 ODPOWIEDŹ 6 Wyjaśnij pojęcie obrzeże sieci?	21
1.1.7 ODPOWIEDŹ 7 Wyjaśnij na czym polega komunikacja P2P?	22
1.1.8 ODPOWIEDŹ 8 Przedstaw budowę modeli OSI i TCP/IP	22
1.1.9 ODPOWIEDŹ 9 Jak pakowane są porcje danych (ładunek użyteczny) w poszczególnych warstwach modelu OSI po stronie nadawcy	23
1.1.10 ODPOWIEDŹ 10 Wyjaśnij czym jest proces enkapsulacji	24
1.2 PROTOKOŁY WARSTWY APLIKACJI	25
Porty wymagane do komunikacji AD.....	26
Porty wymagane do komunikacji PKI	27
1.2.1 ODPOWIEDŹ 1: Charakterystyka protokołu DHCP	28
1.2.2 ODPOWIEDŹ 2: Czym jest proces DORA protokołu DHCP.....	29
1.2.3 ODPOWIEDŹ 3: Omów strukturę pakietu DHCP	32
1.2.4 ODPOWIEDŹ 4: Ogólna charakterystyka protokołu HTTP.....	34
1.2.5 ODPOWIEDŹ 5: Omów nagłówki pakietu HTTP żądania GET w oparciu o poniższy screen:.....	35
1.2.6 ODPOWIEDŹ 6: Jak wygląda transmisja danych strony (obiektów) z serwera WWW do klienta?	36
1.2.8 ODPOWIEDŹ 8: Omów strukturę pakietu DNS.....	37
1.2.9 ODPOWIEDŹ 9: Jaka jest procedura pozyskiwania adresu IP strony WWW przez klienta	38
1.2.10 ODPOWIEDŹ 10: Wymień i scharakteryzuj ważne usługi systemu DNS	38
1.2.11 ODPOWIEDŹ 11: Jak jest zbudowana hierarchiczna baza danych DNS	41
1.2.12 ODPOWIEDŹ 12: Jakiego typu dane zawiera rekord z bazy danych DNS; wymień typy rekordów DNS i uzupełnij je w oparciu o wymyślone przez siebie nazwy i adresy IP	46
1.2.13 ODPOWIEDŹ 13: Czym się różnią rekurencyjne zapytania od iteracyjnych zapytań DNS?.....	47
1.3 WARSTWA TRANSPORTOWA (THE TRANSPORT LAYER).....	49
1.3.1 ODPOWIEDŹ 1: Scharakteryzuj procesy multipleksowania i demultipleksowania	50
1.3.2 ODPOWIEDŹ 2: Jak wiele gniazd TCP może obsługiwać pojedynczy host serwera?.....	52
1.3.3 ODPOWIEDŹ 3: Wyjaśnij w oparciu o Serwer WWW i protokół TCP, że między gniazdami połączeń i procesami nie zawsze występuje relacja jeden do jednego	52

1.3.4 ODPOWIEDŹ 4: Scharakteryzuj protokół UDP	53
1.3.5 ODPOWIEDŹ 5: Przedstaw jak wygląda struktura segmentu UDP.....	54
1.3.6 ODPOWIEDŹ 6: Scharakteryzuj protokół TCP	55
1.3.7 ODPOWIEDŹ 7 : Przedstaw strukturę segmentu TCP	55
1.3.8 ODPOWIEDŹ 8: Na czym polega 3 etapowy proces negocjacji protokołu TCP/IP?.....	58
1.3.9 ODPOWIEDŹ 9: Jak przebiega komunikacja na poziomie warstwy transportowej - przykładowo między klientem i serwerem - po ustanowieniu połączenia TCP?	65
1.3.10 ODPOWIEDŹ 10: Opisz jak przebiega proces kończenia połączenia protokołu TCP	66
1.3.11 ODPOWIEDŹ 11: Na czym polega retransmisja TCP spowodowana zgubieniem potwierdzenia ACK? ...	68
1.3.12 ODPOWIEDŹ 12: Na czym polega retransmisja TCP spowodowana upłynięciem czasu oczekiwania? ...	69
1.3.13 ODPOWIEDŹ 13: Na czym polega zjawisko w sieci: skumulowane potwierdzenia segmentów TCP? ...	70
1.3.14 ODPOWIEDŹ 14: Na czym polega szybka retransmisja segmentów TCP?	71
1.3.15 ODPOWIEDŹ 15: Jakie mogą być przyczyny przepełnienia bufora TCP?	72
1.3.16 ODPOWIEDŹ 16: W jaki sposób protokół TCP zapewnia kontrolę przepływu segmentów	72
1.3.17 ODPOWIEDŹ 17: Jakie mogą być przyczyny przeciążenia w sieci?	73
1.4 WARSTWA SIECI	74
1.4.1 ODPOWIEDŹ 0: Aspekt danych i aspekt sterowania	74
1.4.2 ODPOWIEDŹ 1: Charakterystyka datagramu na przykładzie protokołu IP	79
1.4.3 ODPOWIEDŹ 2: Klasy adresów IPv4	80
1.4.3 ODPOWIEDŹ 2: IPv4 – pule adresów prywatnych.....	81
1.4.4 ODPOWIEDŹ 3: IPv4 - maski podsieci.....	81
1.4.5 ODPOWIEDŹ 4 Charakterystyka protokołu ARP.....	83
1.4.6 ODPOWIEDŹ 5 W jaki sposób host A pozyskuje adres mac hosta B, z którym to chce nawiązać połączenie	85
1.4.7 ODPOWIEDŹ 6 Jak przebiega atak ARP, w którym atakujący podszywa się pod bramę domyślną routera?	85
1.4.8 ODPOWIEDŹ 7 Jak przebiega atak ARP, w którym atakujący podaje routerowi (Gateway) fałszywe adresy mac hostów?	87
1.4.9 ODPOWIEDŹ 8 Jak przebiega atak ARP, w którym atakujący podaje fałszywy adresy mac hosta A hostowi B?.....	88
1.4.10 ODPOWIEDŹ 9 Jak przebiega atak ARP typu „Człowiek w środku”?	89
1.4.11 ODPOWIEDŹ 10 Protokół ICMP	90
1.4.12 ODPOWIEDŹ 9 Protokół IGMP.....	96
1.4.13 ODPOWIEDŹ 9 IPv6	99
1.5 WARSTWA ŁĄCZA DANYCH	100
1.5.1 ODPOWIEDŹ 1 Budowa ramki Ethernet.....	100
1.5.2 ODPOWIEDŹ 2 Protokół STP – budowa ramki BPDU	101
1.5.3 ODPOWIEDŹ 3 Protokół STP –Wireshark	103
2. PRACOWNIA SIECI KOMPUTEROWYCH.....	104

2.01 Topologie sieci.....	105
2.02 Skrętka miedziana - budowa.....	114
2.03 Skrętka miedziana – standard T568 i oznaczanie par	142
2.04 Skrętka miedziana – parametry transmisyjne.....	146
2.0.4.1 NEXT (Near end crosstalk) – przesłuch zbliżny.....	146
2.0.4.2 ACR-N Attenuation (tłumienie)	148
2.0.4.4 PSNEXT (Power Sum NEXT) – suma mocy przesłuchów w bliskim końcu	152
2.0.4.5 FEXT (Far End Cross Talk) przesłuch na dalekim końcu - zdalny	153
2.0.4.7 PSFEXT (Power Sum FEXT) – Suma mocy przesłuchu FEXT	154
2.0.4.7 ANEXT (Alien crosstalk) – przesłuch obcy	155
2.04 Światłowody.....	156
Film pt. Prawa odbicia i załamania światła	158
2.1 Cisco Packet Tracert	172
2.2 Konsolowe resetowanie przełącznika	174
2.3 Wstępne czyszczenie ciasteczek w przeglądarce Firefox.....	177
2.4 Wstępna konfiguracja przełączników	180
2.5 Dlaczego nie mogę się dostać na przełącznik sieciowy.....	192
2.6 Wstępna konfiguracja routera – zmiana adresu IPv4 LAN urządzenia	193
2.7 Rezerwacja DHCP na routerze TP-LINK	200
2.8 Konfiguracja przełącznika - Access Security	216
2.8 SWITCHING.....	232
3. PRACOWNIA SIECI KOMPUTEROWYCH - VIRTUAL LAN (VLAN)	286
3.1 VLAN TEORIA.....	286
3.2 KONFIGURACJA VLAN-ÓW NA ROUTERZE - METODA KLASYCZNA.....	293
3.3 KONFIGURACJA VLAN-ÓW NA ROUTERZE – ROUTER ON THE STICK.....	306
3.4 VLAN MANAGEMENT 500.....	312
3.3 MAC VLANY	323
3.4 PROTOCOL VLAN	331
3.5 ROUTER CISCO UMBRELLA RV240W	342
3.6 ROUTER CISCO UMBRELLA RV240W + ACCESS POINT	350
3.7 Protokół drzewa rozpinającego STP.....	365
3.8 Protokół drzewa rozpinającego MSTP	376
4.ROUTING	399
4.1 Protokół routingu RIPv2 - Cisco Packet.....	399
4.2 Protokół routingu OSPF - Cisco Packet	431
4.3 Protokół routingu BGP - Cisco Packet	439
4.3 Konfiguracja protokołu OSPF na przełączniku TP-LINK T3700G-28TQ_V2	443
5.1 Access Control List – Cisco Packet.....	444

5.2 Access Control List – TP-LINK switch	444
5.2.1 MAC ACL.....	444
5.2.3 Standardowe ACL – IP	452
5.2.2 External ACL	456
6.1 Remote Access L2TP VPN Topology	476
5.2 Configuring PPTP VPN	491
5.3 LAN to LAN VPN with NAT.....	497
5.4 How to connect to Omada Router using IKEv2 VPN of Android/iOS	519
6. URZĄDZENIA PERYFERYJNE	527
6.1 Instalowanie sterowników do drukarki po domenie w sieci LAN	527
6.2 Drukowanie u sąsiada przez WAN po domenie	574
6.3 Drukowanie dwustronne na krótkiej krawędzi w sytemie Windows	592
6.4 Drukowanie dwustronne na długiej krawędzi w sytemie Linux	597
7. SERWER UBUNTU.....	612
7.1 Ubuntu Serwer – http	612
7.2 Ubuntu Serwer – konfiguracja serwera DNS.....	625
8. DIAGNOSTYKA SIECI	635
8.1 Netstat Linux	635
SKŁADNIA	635
8.2 Netstat windows	642

1. SIECI KOMPUTEROWE – TEORIA

1.1 SIECI KOMPUTEROWE I INTERNET

1.0.1 ODPOWIEDŹ Czym jest sieć komputerowa?

Sieć komputerowa łączy ze sobą komputery w celu wymiany danych.

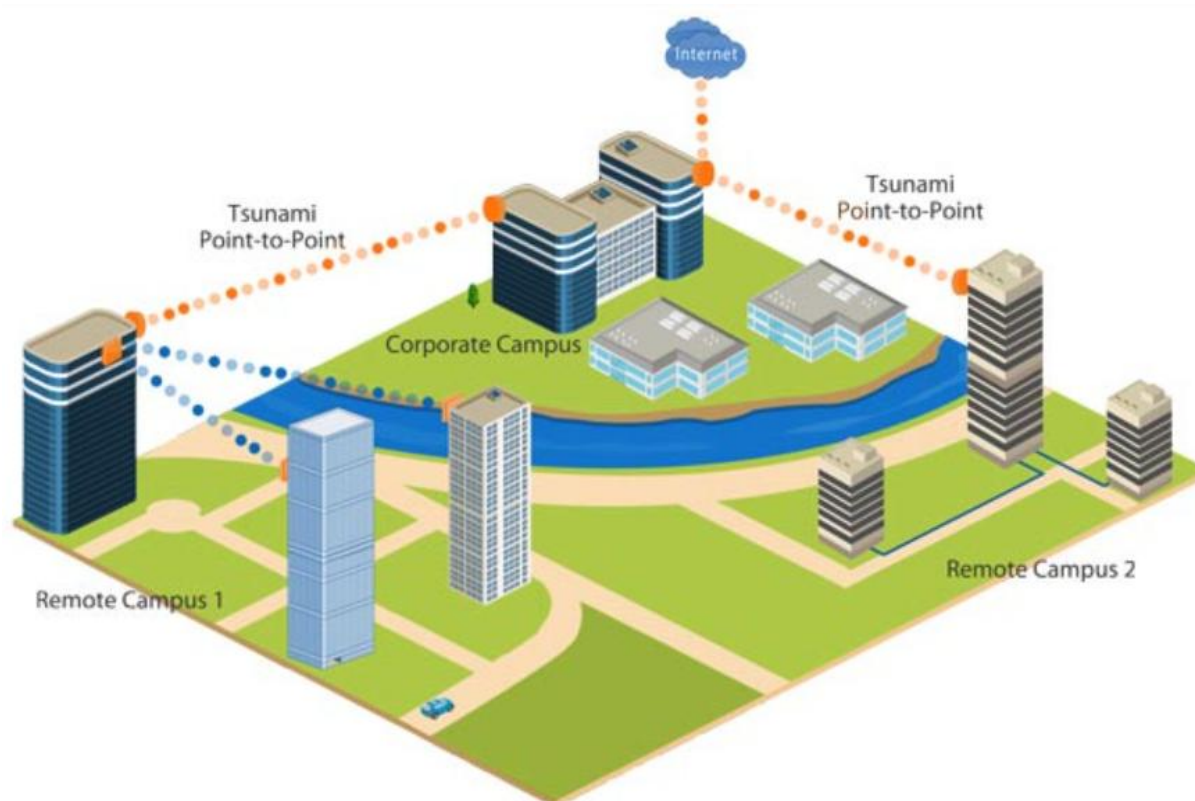
Najmniejsza sieć komputerowa składa się z dwóch komputerów połączonych ze sobą łączem komunikacyjnym.

Największą siecią jest Internet.

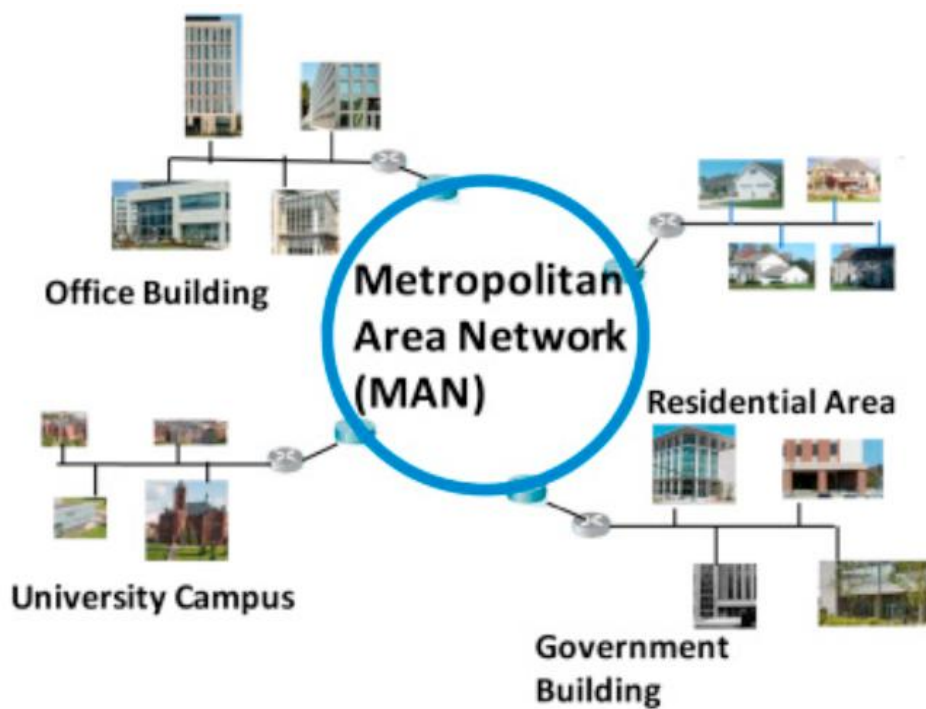
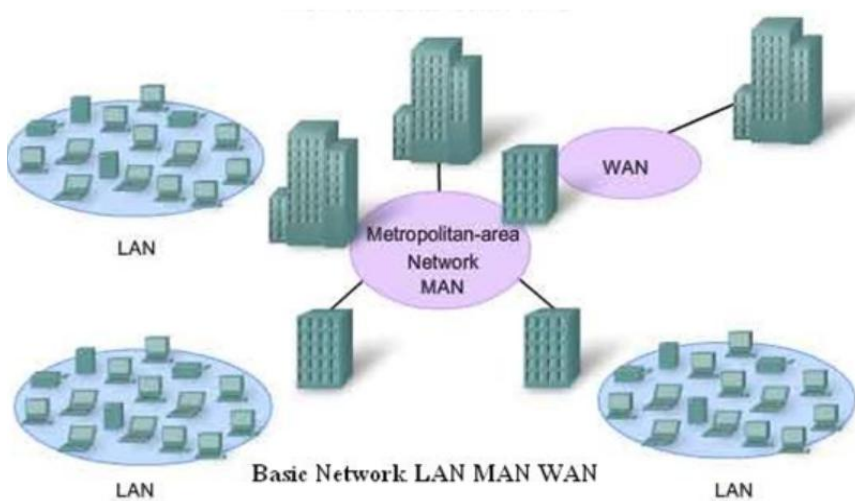
1.0.2 ODPOWIEDŹ Podział sieci ze względu na wielkość

Sieci lokalne (z ang. **LAN** – *Local Area Network*) – obejmuje komputery połączone na ograniczonym obszarze (najczęściej w jednym budynku lub kilku budynkach) zazwyczaj w ramach jednej jednostki organizacyjnej (szkoła, biuro, firma). Jeśli w sieci lokalnej połączenia zrealizowano bez użycia przewodów, mówimy o bezprzewodowej sieci lokalnej (z ang. **WLAN** – *Wireless Local Area Network*).

Sieć kampusowa (z ang. **CAN** – *Campus Area Network*) – większa sieć w obszarze administracyjnym uczelni wyższej, korporacji itd. łączy zazwyczaj wiele budynków.



Sieci miejskie (z ang. **MAN** – *Metropolitan Area Network*) – łączą sieci lokalne na terenie jednego miasta.



Miejska sieć komputerowa w Krakowie

https://www.cyfronet.pl/sieci/13152,artykul,charakterystyka_sieci.html

Sieci rozległe (z ang. **WAN** – *Wide Area Network*) – łączą ze sobą wybrane sieci lokalne na większym obszarze.

Internet – łączy ze sobą prawie wszystkie sieci na świecie.

Oceaniczna sieć szkieletowa

1	https://www.ovhcloud.com/pl/network/backbone/
2	https://networkexpert.pl/aktualnosci/mapa-podwodnych-kabli-swiatlowodowych-czy-zastanawialiscie-sie-kiedys-jak-to-wszystko-jest-podlaczone/
3	https://www.submarinecablemap.com/
4	https://youtu.be/6dkiqJ_IzGw
5	https://www.youtube.com/watch?v=DKHZKTRyze8
6	budowa kabla światłowodowego oceanicznego
7	https://www.youtube.com/watch?v=PIQhA2h1ERY
8	instalacja kabli światłowodowych na dnie morza
9	https://www.youtube.com/watch?v=eTBLIYJSzdc
10	https://www.youtube.com/watch?v=Gg1aFmsKQgk&list=PLokGt-Zs-l1Fa5GGroyEZ3cNBGa_PKZPL&index=1
11	https://www.youtube.com/watch?v=_T-wLgB1zM

Sieć szkieletowa w Polsce

1	Polski Internet Optyczny PIONIER	https://www.man.torun.pl/o-nas/siec-pionier/
2	400 Gb/s w sieci szkieletowej Orange	https://biuroprasowe.orange.pl/blog/400-gb-s-w-sieci-szkieletowej-orange/
3	Ogólnopolska światłowodowa sieć Atman	https://www.atman.pl/lacznosc/siec-swiatlowodowa/
4	Sieć szkieletowa NETIA	https://www.telko.in/co-zrobi-z-netia-cyfrowy-polsat,1
5	NASK - Ogólnopolska Sieć Edukacyjna (OSE).	https://www.telko.in/nask-oglosil-przetarg-na-siec-szkieletowa-ose
6		
7	Mapa zasięgu PLAY 3G / 4G /5G	https://www.nperf.com/pl/map/PL/-/5505.Play/signal?ll=51.020666012558124&lg=19.802856445312504&zoom=7
8	Regionalny ISP FIBERWAY	https://www.fiberway.pl/zasieg

1.0.3 ODPOWIEDŹ Wymień urządzenia sieciowe

- ROUTERY SIECI SZKIELETOWEJ I BRZEGOWEJ

Cisco ASR 9000 to rodzina routerów klasy operatorskiej przeznaczonej do pracy w szkielecie i na brzegu sieci. Urządzenia charakteryzują się wysoką wydajnością, niezawodnością oraz bogatą dostępnością funkcji operatorskich.



Figure 1.

Cisco ASR 9902 chassis



Figure 2.

Cisco ASR 9902 Route Processor

- ROUTERY SIECI DOMOWEJ (WAN/LAN)



- PRZEŁĄCZNIKI (SWITCHES)

TP-Link PoE Switch

Supply power and data to network devices over a single Ethernet cable

16× Gigabit PoE+ Ports
Up to 30 W on Each Port
Total 250 W Power Budget



TL-SG1218MPE



Surveillance
IP Camera



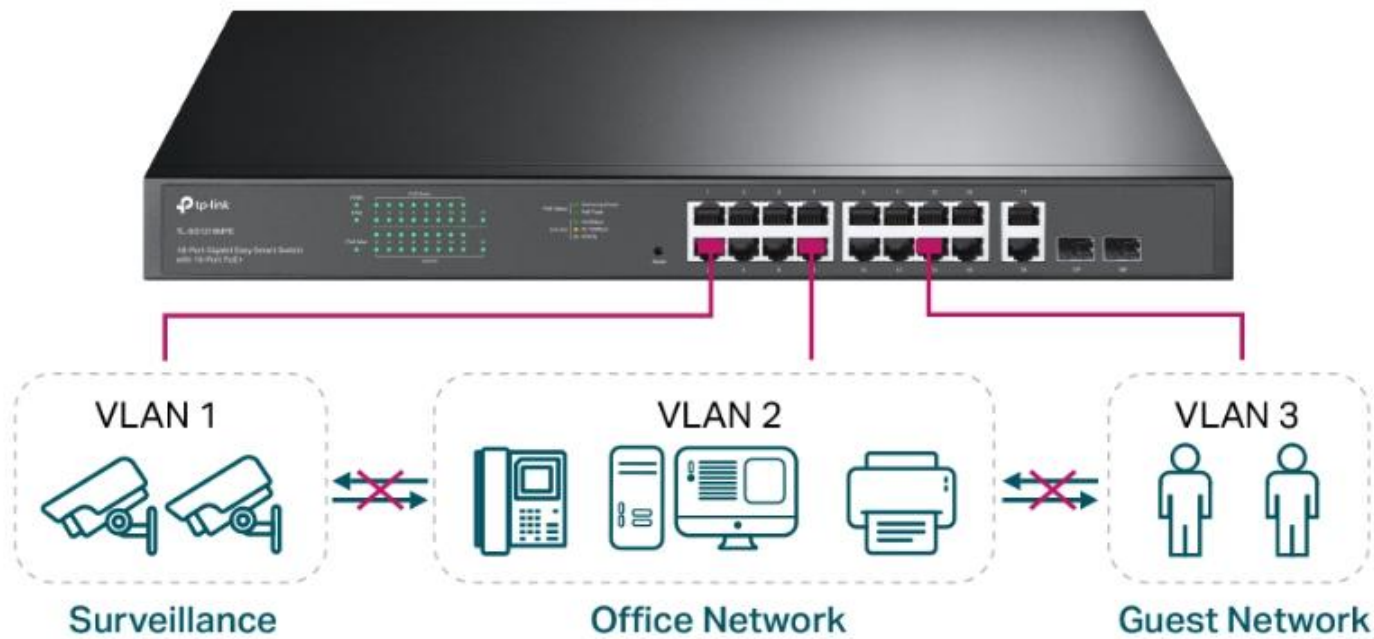
Conference Calls
IP Phone



Wi-Fi Coverage
Access Point

Advanced Network Features

VLAN for simplified management, enhanced security and better experience



Easy Management
Monitor and manage the network via Web UI or Utility



QoS
Smooth traffic for latency sensitive applications



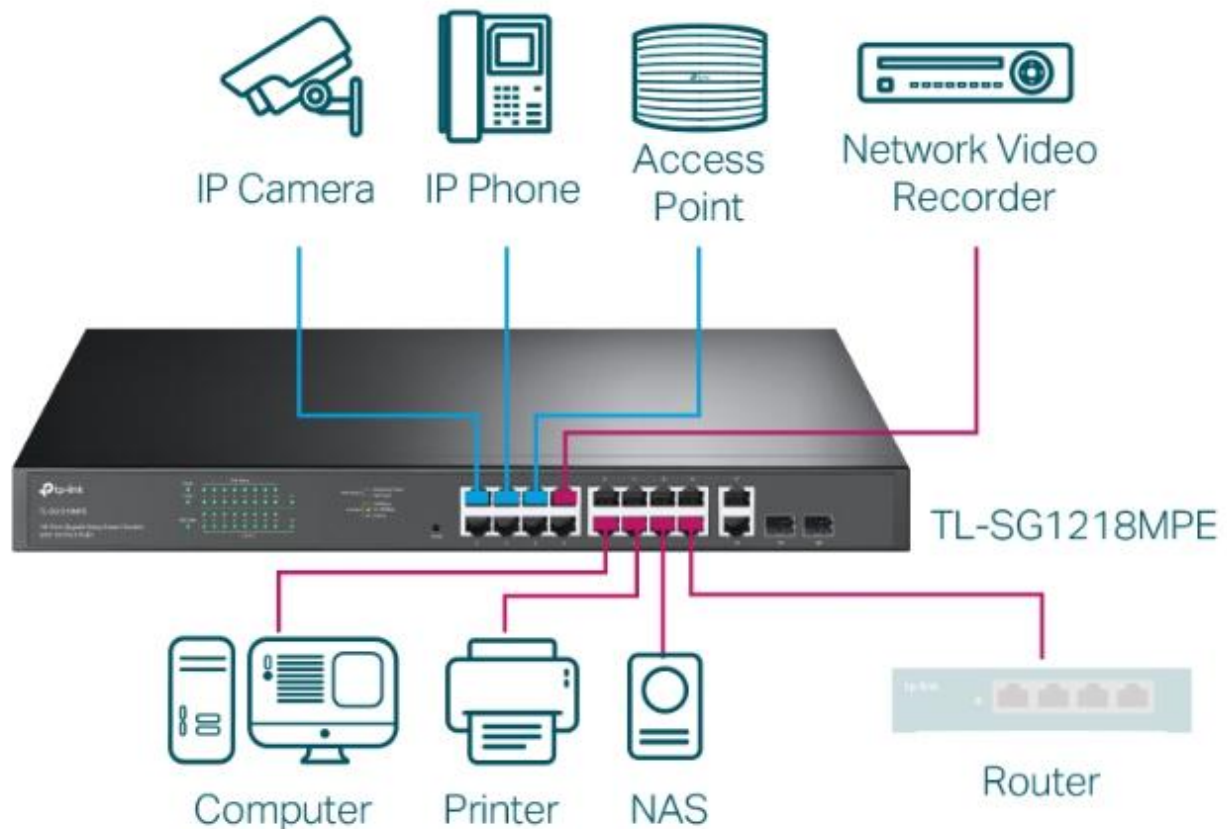
IGMP Snooping
Traffic optimization for IPTV



LAG
Higher bandwidth, reliability, and availability

TP-Link Easy Smart Switch Plug and Play

- 1 Plug In
- 2 Connect Devices



- 3 Enjoy

PUNKTY DOSTĘPWE SIECI (ACCESS POINTS)



Figure 1.

Catalyst 9166 Series access point





EAP650-Outdoor

Bezprzewodowy, wewnętrzny/zewnętrzny punkt dostępu, standard AX3000



EAP625-Outdoor HD

Bezprzewodowy, wewnętrzny/zewnętrzny punkt dostępu, standard AX1800



EAP623-Outdoor HD

Bezprzewodowy, wewnętrzny/zewnętrzny punkt dostępu Wi-Fi 6, standard AX1800

- 574 Mb/s w paśmie 2,4GHz + 1201 Mb/s w paśmie 5 GHz
- Stabilna praca w mocno obciążonych środowiskach
- Duży zasięg
- Technologia Mesh
- Anteny Smart
- Odporność na warunki atmosferyczne IP67
- Scentralizowane zarządzanie w Chmurze



EAP610-Outdoor

Bezprzewodowy, wewnętrzny/zewnętrzny punkt dostępu, standard AX1800



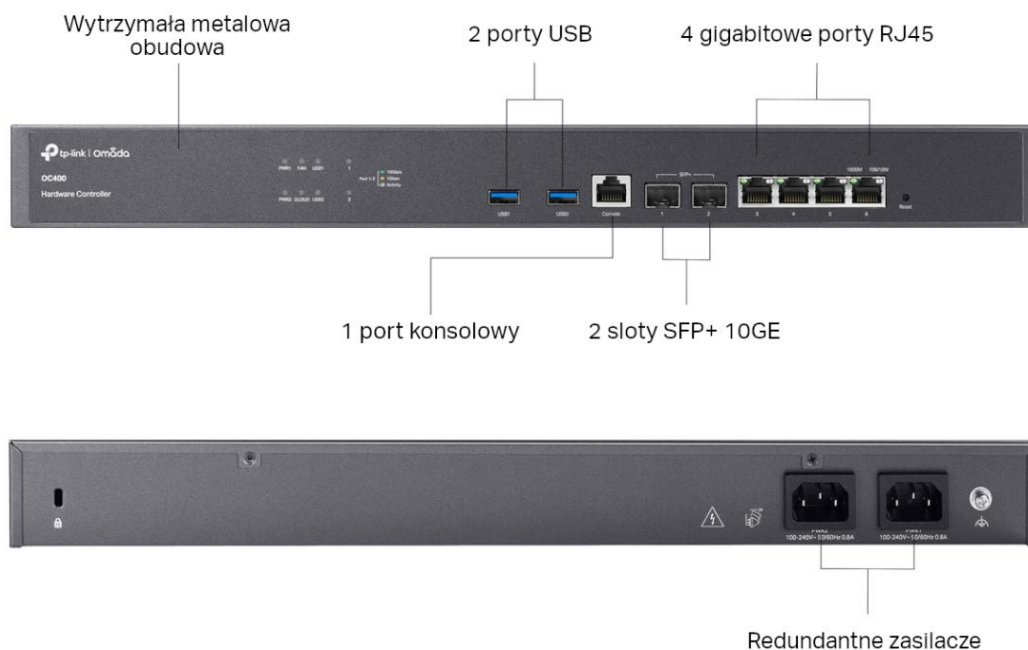
EAP211-Bridge KIT

Bezprzewodowy, wewnętrzny/zewnętrzny Most Omada, 5 GHz 867 Mb/s

EAP225-Outdoor

Bezprzewodowy, wewnętrzny/zewnętrzny punkt dostępu MU-MIMO, standard

• KONTROLERY SPRZĘTOWE

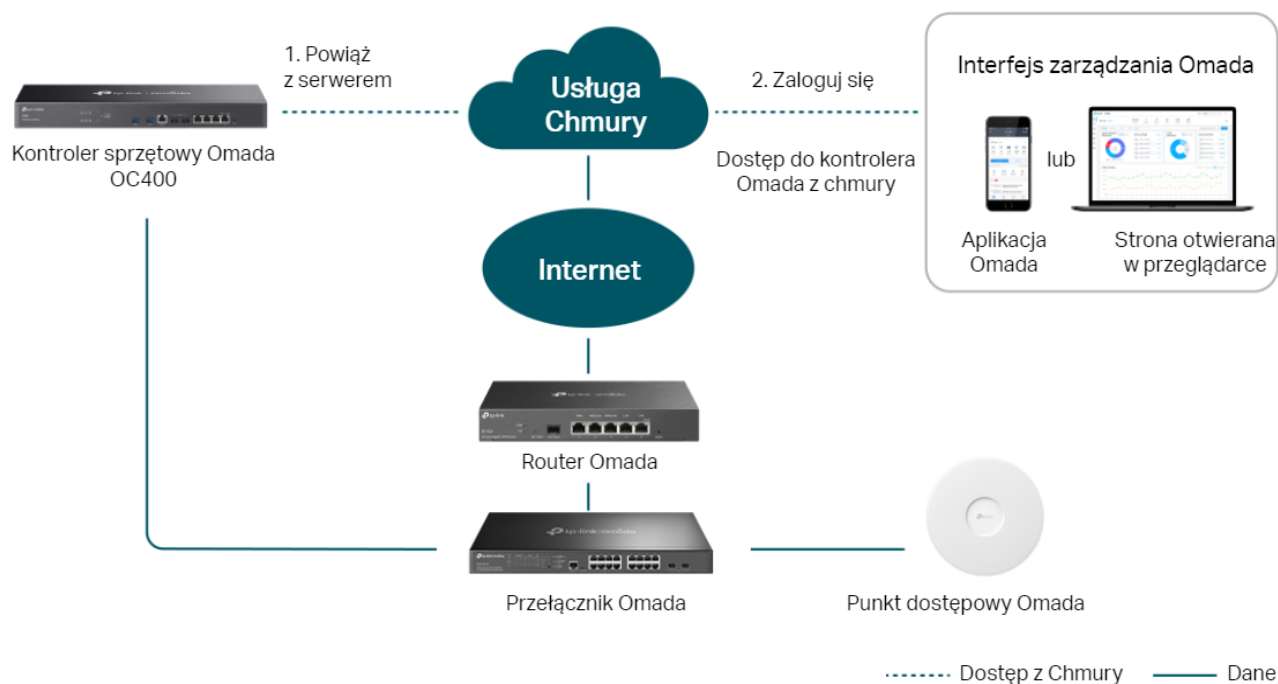


Sterowanie programowe infrastrukturą sieciową (SDN) z dostępem z chmury

Platforma do programowego sterowania infrastrukturą sieciową (SDN) Omada integruje działanie urządzeń sieciowych, w tym punktów dostępowych, przełączników i bram sieciowych, zapewniając kompleksowe zarządzanie centralne z chmury. Omada umożliwia stworzenie wysoce skalowalnej sieci — w pełni kontrolowanej za pomocą jednego interfejsu. Przekłada się to na płynne połączenia przewodowe i bezprzewodowe, które są niezbędne w hotelarstwie, edukacji, sprzedaży detalicznej, biurach i w wielu innych branżach i miejscach.



Jeszcze większa wygoda dzięki chmurze hybrydowej



- ANTENY KIERUNKOWE



CPE710

Zewnętrzne urządzenie CPE 23 dBi, 5 GHz, 867 Mb/s



CPE605

Zewnętrzne urządzenie CPE 23dBi, 5GHz, 150Mb/s

- 150 Mb/s w paśmie 5 GHz
- Antena kierunkowa 23 dBi
- Ochrona przed wyładowaniami elektrostatycznymi 15 kV i ochrona przeciwprzepięciowa 6 kV
- Klasa IP65 wodoszczelności
- Scentralizowane zarządzanie



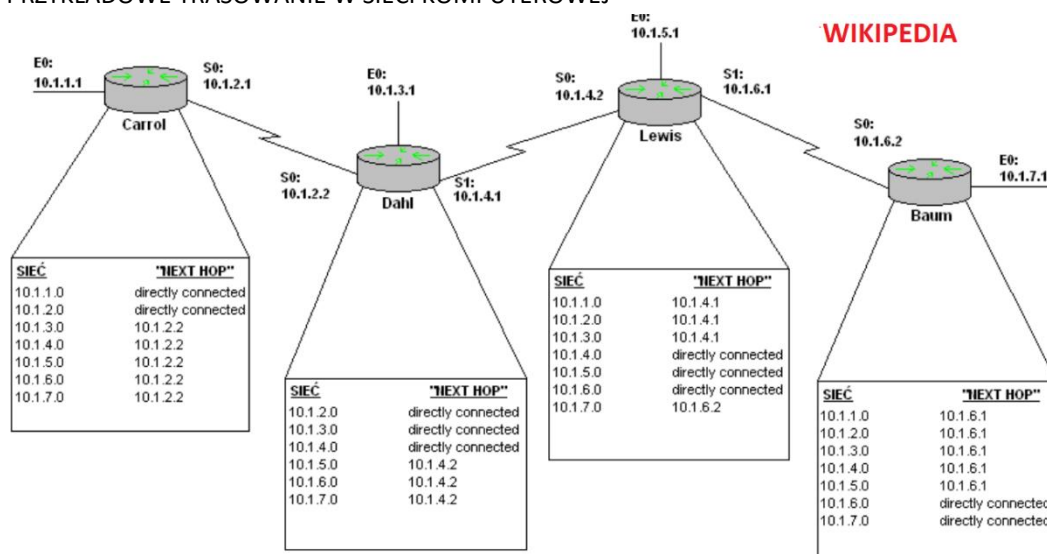
CPE210

Zewnętrzne urządzenie CPE 9dBi, 2,4GHz, 300Mb/s

1.1.1 ODPOWIEDŹ 1 Czym jest Internet

- Publiczny Internet jest siecią łączącą miliony urządzeń zwanymi **systemami końcowymi** (end systems) lub **hostami**, zlokalizowanymi w różnych częściach świata.
 - Do systemów końcowych zaliczamy wszystkie urządzenia, które mogą komunikować się ze sobą w Internecie za pomocą odpowiednich interfejsów sieciowych powszechnie zwanych kartami sieciowymi.
 - Przykładowymi systemami końcowymi są: komputery stacjonarne, komputery przenośne, telefony komórkowe, konsole gier, telewizory, kamery, samochody, czujniki środowiskowe, cyfrowe ramki do zdjęć, domowe urządzenia elektryczne i systemy zabezpieczeń.
 - Systemy końcowe są połączone za pomocą łączy **komunikacyjnych i przełączników pakietów**.
 - **Szybkość transmisji** łącza jest wyrażana w bitach na sekundę. Kiedy jeden system końcowy wysyła dane do innego takiego systemu, dzieli informacje na segmenty i dołącza do każdego z nich nagłówek. Powstają w ten sposób porcje danych, nazywane w żargonie związanym z sieciami komputerowymi **pakietami**.
 - Przesłane przez sieć pakiety w systemie końcowym są ponownie łączone w pierwotne dane (dokonuje tego aplikacja sieciowa np. przeglądarka internetowa).
 - Droga pokonywana przez pakiety w sieci nazywana jest **trasą** lub **ścieżką**.
-
- Pakiety to odpowiednik ciężarówek, łączy komunikacyjne to autostrady i drogi, przełączniki pakietów, przypominają skrzyżowania, a systemy końcowe to budynki (miejsca wysyłek, miejsca docelowe).
 - Systemy końcowe uzyskują dostęp do Internetu za pośrednictwem **dostawcy usług internetowych ISP** (Internet Service Provider).
 - Systemy końcowe, przełączniki pakietów i inne składniki Internetu wykorzystują **protokoły**, które kontrolują proces wysyłania i odbierania informacji transferowanych w internecie.
 - **TCP** (ang. *Transmission Control Protocol*) i **IP** (ang. *Internet Protocol*) to dwa najważniejsze protokoły stosowane w internecie.
 - Standardy internetowe są opracowywane przez organizację **IETF** (ang. *Internet Engineering Task Force*).
 - Dokumenty standardów IETF są nazywane **dokumentami RFC** (ang. *Requests for Comments*).

PRZYKŁADOWE TRASOWANIE W SIECI KOMPUTEROWEJ



1.1.2 ODPOWIEDŹ 2 Co to znaczy, że Internet jest infrastrukturą zapewniającą usługi dla aplikacji?

- Internet jako infrastruktura sieciowa zapewnia dostęp do usług takich jak:
 - poczta elektroniczna,
 - przeglądanie stron WWW,
 - telefonia VOIP,
 - obsługa internetowych stacji radiowych,
 - transmisja strumieniowa danych wideo,
 - wymiana plików w sieciach równorzędnych (ang. *Peer to Peer - P2P*),
 - telewizja internetowa
 - bankowość elektroniczna itd.

1.1.3 ODPOWIEDŹ 3 Co to jest API?

- **API** (ang. *Application Programing Interface*) czyli interfejs programowania aplikacji.
- Systemy końcowe podłączone do Internetu udostępniają interfejs API.
- Określa on, w jaki sposób program działający w jednym systemie końcowym ma żądać od Internetu przekazanie danych do określonej aplikacji docelowej funkcjonującej w innym systemie.
- Interfejs API Internetu obejmuje zestaw reguł, których oprogramowanie wysyłające informacje musi przestrzegać, aby Internet mógł przesłać dane do aplikacji docelowej.

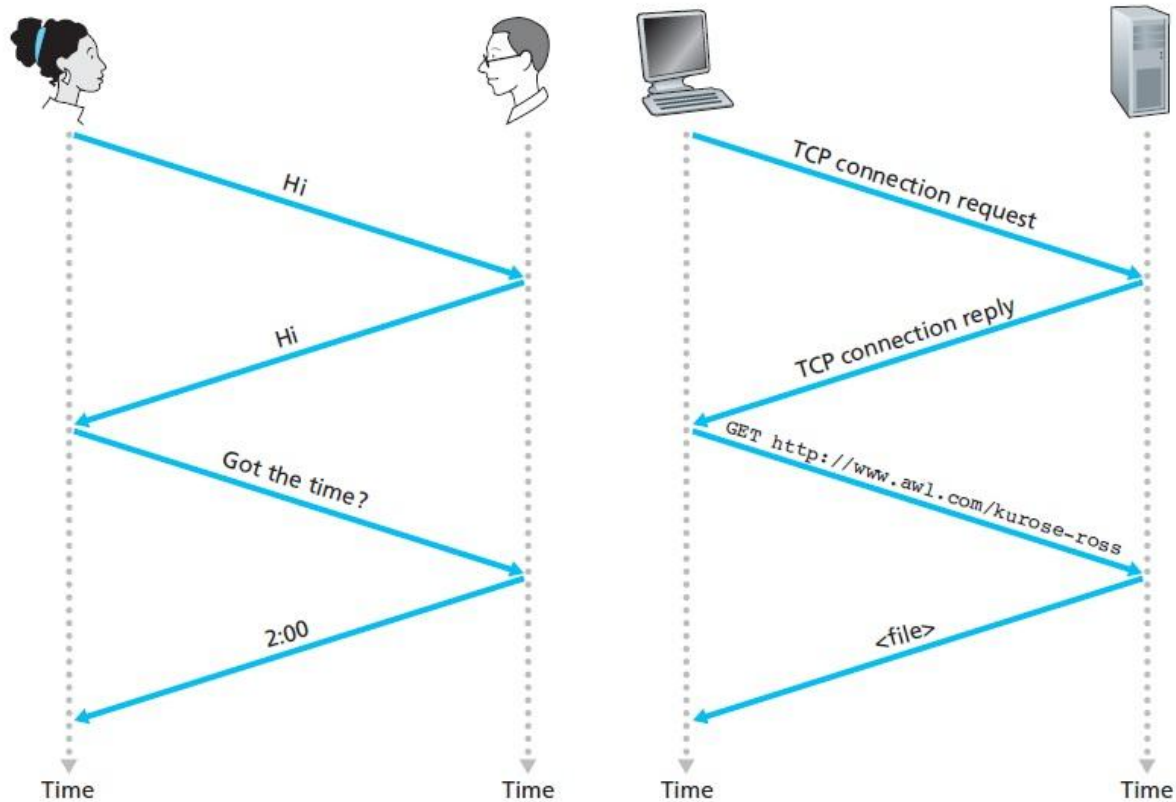
1.1.4 ODPOWIEDŹ 4 Czym jest protokół sieciowy?

- Protokół definiuje format i kolejność komunikatów wymienianych między dwoma lub większą liczbą komunikujących się jednostek, a także operacje wykonywane w momencie wysyłania i (lub) odbierania komunikatu bądź innego zdarzenia.
- Wszystkie operacje realizowane w Internecie, które angażują dwie lub więcej zdalnych jednostek komunikacyjnych, są zarządzane przez protokół.
- Przykładowo, sprzętowe protokoły kart sieciowych dwóch połączonych ze sobą komputerów kontrolują przepływ bitów w kablu znajdującym się między dwoma interfejsami sieciowymi.
- Protokoły systemów końcowych kontrolujące przeciążenie decydują, z jaką szybkością pakiety będą transmitowane między nadawcą i odbiorcą.
- Protokoły ruterów określają ścieżkę, jaką pakiet będzie podążał od miejsca źródłowego do docelowego.
- Protokoły sieciowe są stosowane w każdym miejscu Internetu.

1.1.4 ODPOWIEDŹ 5 Jaką analogię możemy zastosować, aby wyjaśnić czym jest protokół sieciowy?

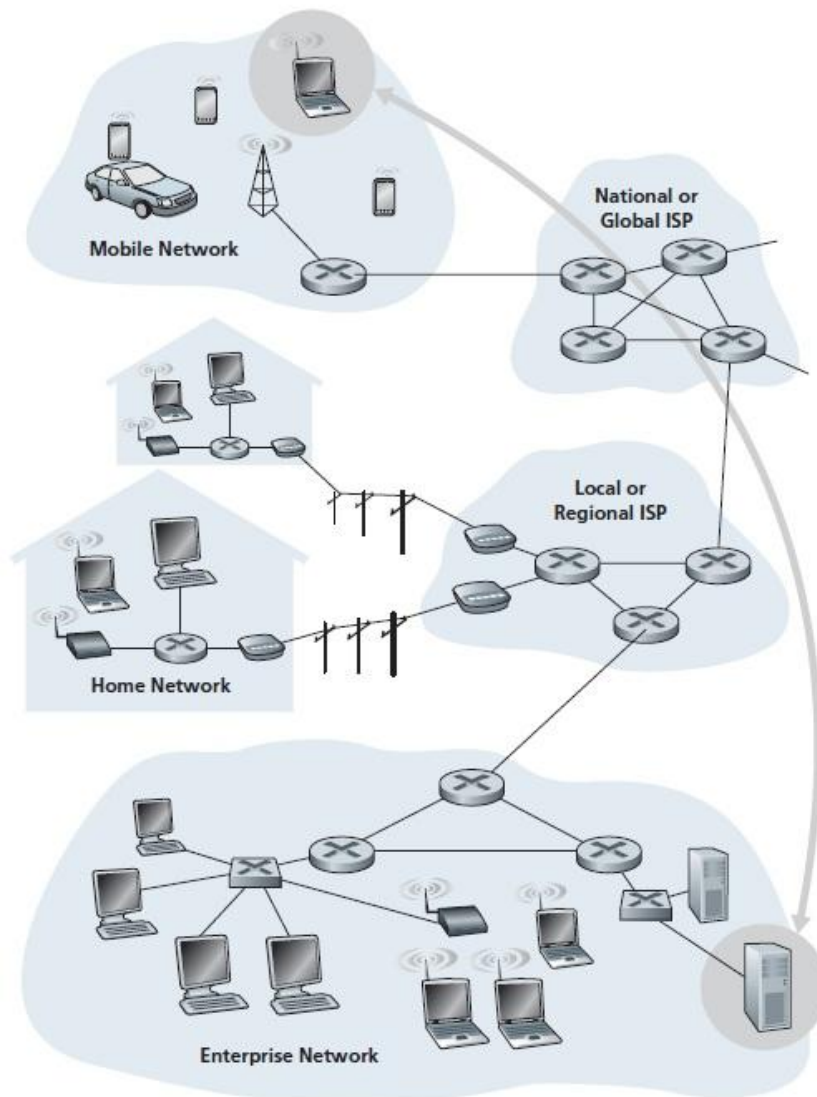
- Najprostszym sposobem pozwalającym zrozumieć protokół sieciowy jest zastosowanie analogii dotyczącej komunikacji międzyludzkiej.

Ludzie podczas komunikacji stosują się do ustalonego protokołu czyli reguł. Poniższy obrazek wyjaśnia wyżej wspomnianą analogię:



A human protocol and a computer network protocol

1.1.5 ODPOWIEDŹ 6 Wyjaśnij pojęcie obrzeże sieci?



End-system interaction

- Obrzeże sieci, to ta część sieci, która obejmuje systemy końcowe.
- Systemy końcowe określa się mianem **hosty** (ang. gospodarze), ponieważ goszczą (uruchamiają) aplikacje, takie jak przeglądarka internetowa, program serwera WWW, program pocztowy lub program serwera poczty.
- Czasami hosty są dzielone na dwie kategorie - **klienty** i **serwery**.
- Za klienty uważa się stacjonarne i przenośne PC, palmtopy, telefony komórkowe, tablety itd.
- Serwerami są bardziej wydajne komputery, które przechowują i dystrybuują strony internetowe, strumieniowe dane wideo, wiadomości pocztowe itd.

1.1.6 ODPOWIEDŹ 6 Przybliż temat: "Programy klienta i serwera"?

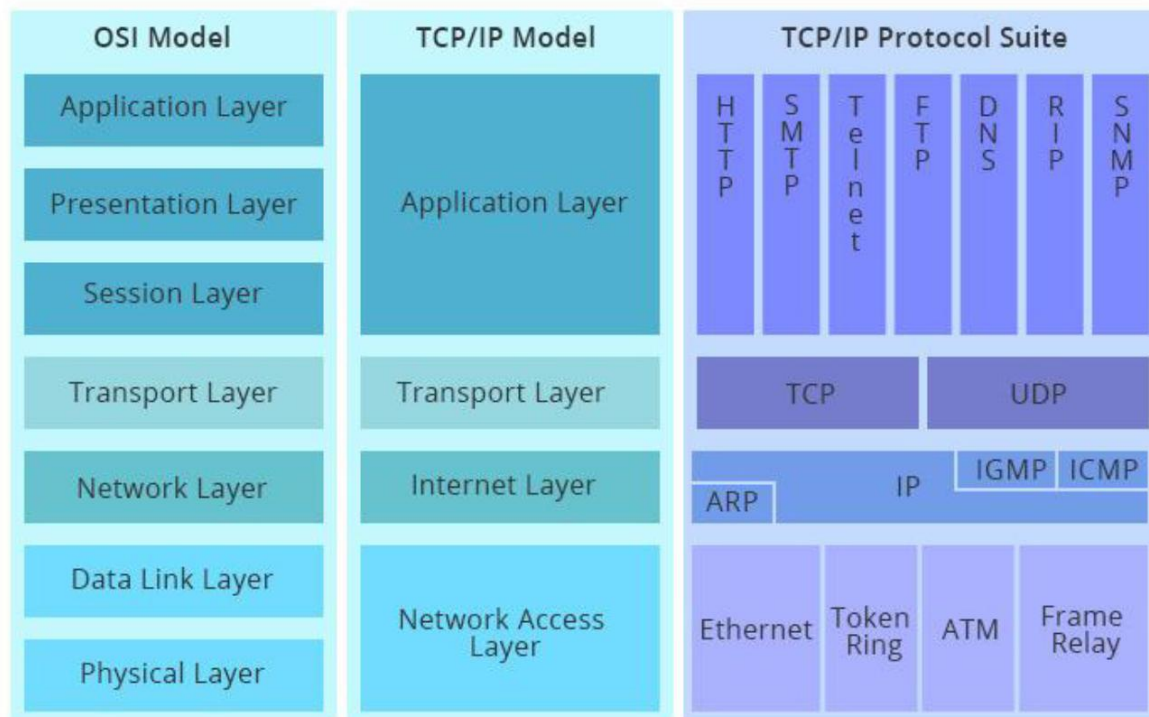
- Aplikacja klienta jest programem uruchomionym na jednym systemie końcowym, który żąda i korzysta z usługi świadczonej przez aplikację serwera uaktywnioną na drugim systemie końcowym. Modelem tego używają serwery WWW, serwery pocztowe, serwery FTP, obsługujące zdalne logowania i grupy dyskusyjne i inne aplikacje.
- Aplikacje klient - serwer nazywamy **aplikacjami rozproszonymi**, ponieważ aplikacja klienta jest uruchomiona na jednym komputerze, a aplikacja serwera na drugim, w często odległych od siebie obszarach sieci.

1.1.7 ODPOWIEDŹ 7 Wyjaśnij na czym polega komunikacja P2P?

- P2P (ang. *peer-to-peer*)
- Obecnie nie wszystkie aplikacje internetowe są złożone wyłącznie z aplikacji klienta, które komunikują się tylko z aplikacjami serwera.
- **P2P** umożliwia komunikację **programów równorzędnych**. Polega to na tym, że systemy końcowe uruchamiają aplikacje pełniące jednocześnie funkcje klienta i serwera oraz komunikują się z takimi programami.
- Przykładowe aplikacje P2P to:
 - Big Torrent - służący do wymiany plików. Np. pobieranie systemu Linux-Ubuntu
 - Skype - telefonia internetowa
- Program uaktywniony na węźle (komputer użytkownika) jest klientem, gdy żąda pliku innego węzła (np. instalacji systemu Linux-Ubuntu). Z kolei program pełni rolę serwera, gdy wysyła plik do innego węzła (np. wyżej wspomnianą instalację systemu Linux - Ubuntu).

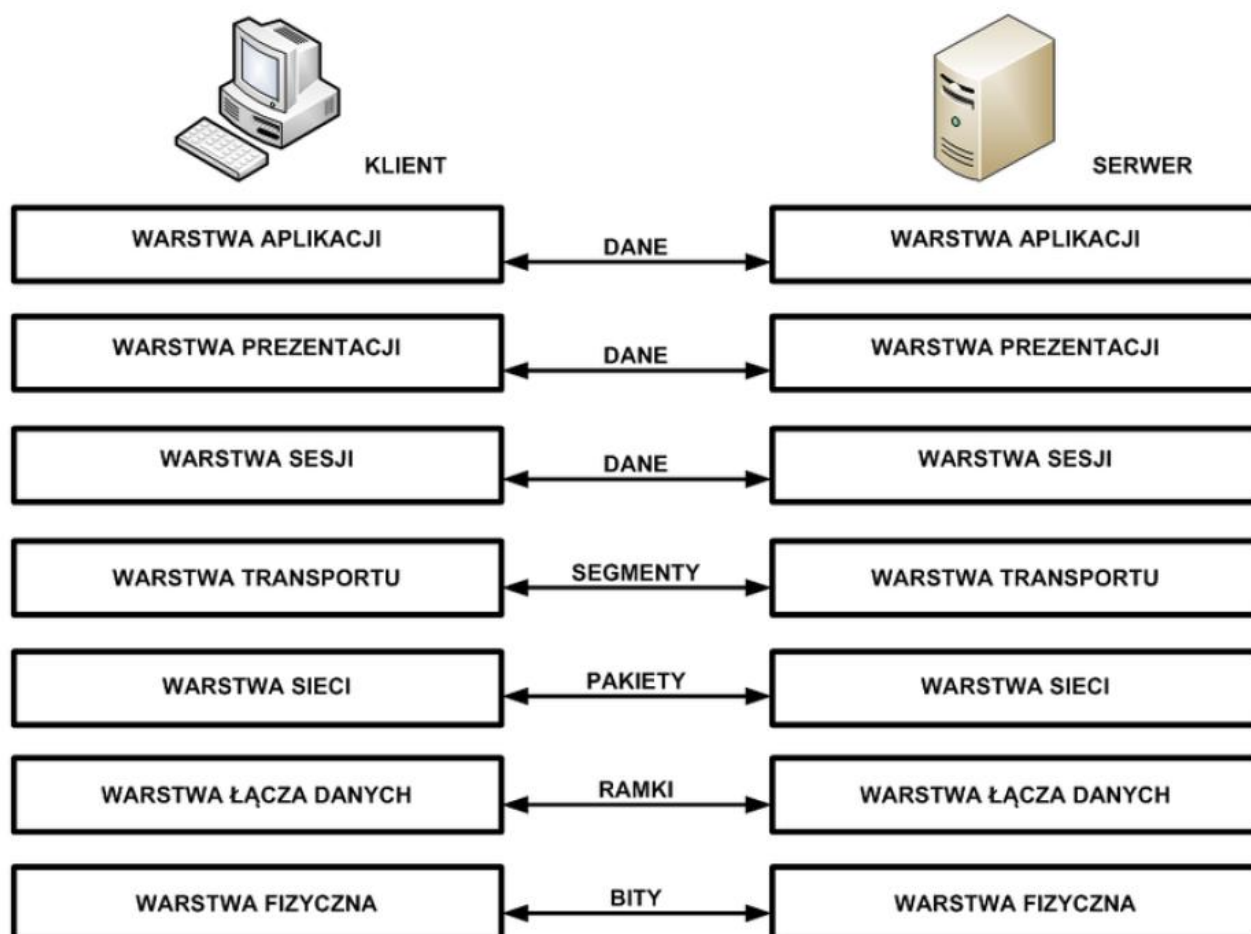
1.1.8 ODPOWIEDŹ 8 Przedstaw budowę modeli OSI i TCP/IP

ODPOWIEDŹ 8 Przedstaw budowę modeli OSI i TCP/IP

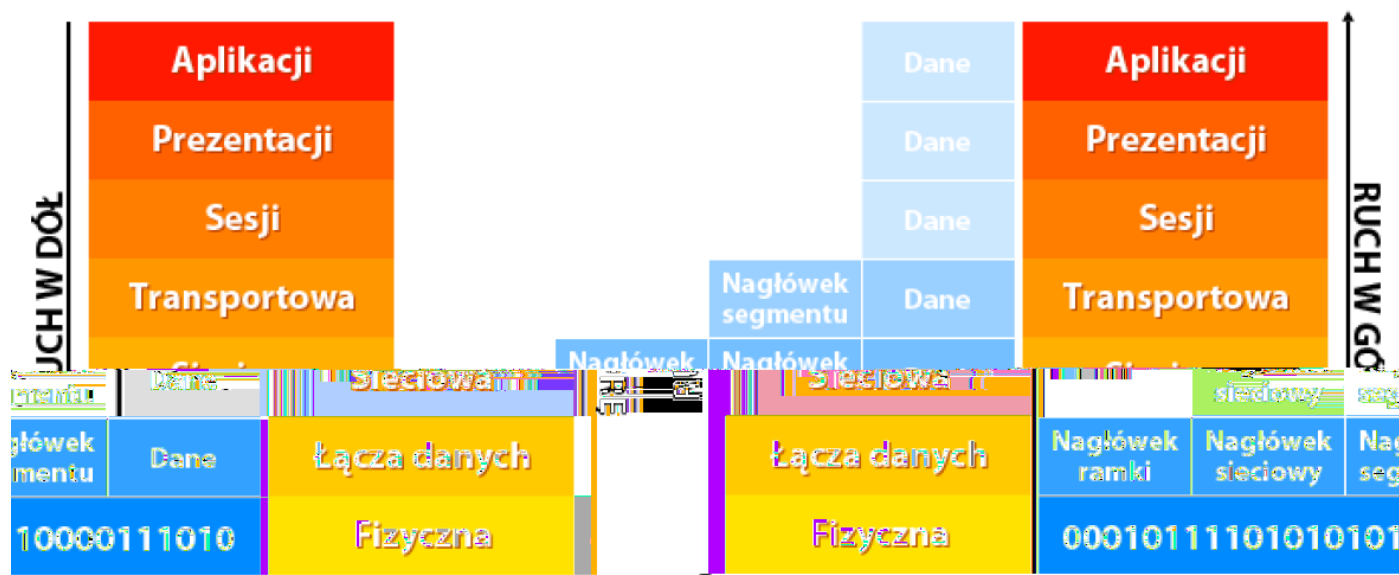


1.1.9 ODPOWIEDŹ 9 Jak pakowane są porcje danych (ładunek użyteczny) w poszczególnych warstwach modelu OSI po stronie nadawcy

- Dane przechodzące z warstwy aplikacji do warstwy transportowej są dzielone porcje danych. Do każdej takiej porcji danych dodawany jest nagłówek i w ten sposób powstaje **segment**
- **Segmenty** z warstwy transportowej przekazywane są do warstwy sieciowej. Do segmentu jako ładunku użytecznego warstwy wyższej (tu warstwy transportowej) dodawany jest nagłówek i powstaje **datagram (pakiet)**.
- **Datagramy** z warstwy sieciowej przekazywane są do warstwy łącza danych. Do datagramu jako ładunku użytecznego warstwy wyższej (tu warstwy sieciowej) dodawany jest nagłówek i powstaje **ramka**.
- **Ramki** w warstwie fizycznej w postaci bitów nadawane są z karty sieciowej do sieci.



Warstwy w modelu odniesienia OSI



1.1.10 ODPOWIEDŹ 10 Wyjaśnij czym jest proces enkapsulacji

Kapsułkowanie (lub enkapsulacja, od (ang.) encapsulation) – termin odnoszący się do struktury protokołu komunikacyjnego, np. opartego na modelu OSI lub modelu TCP/IP. Kapsułkowanie polega na upakowaniu danych z wyższej warstwy w warstwie niższej danego protokołu po stronie nadawczej, a więc przed wysłaniem pakietu telekomunikacyjnego (datagramu, ramki) w sieciach pakietowych. Po stronie odbiorczej wykonywane jest działanie odwrotne (tzw. dekapulacja), prowadzące do wyodrębnienia danych warstwy najwyższej przenoszącej dane użytkowe (zwanej warstwą aplikacji) z danych warstw niższych.

1.2 PROTOKOŁY WARSTWY APLIKACJI

Protokół	Opis	Port
HTTP	Protokół przesyłania dokumentów hipertekstowych (stron WWW)	80
HTTPS	Szyfrowany protokół HTTP wykorzystujący protokoły szyfrujące TLS lub SSL	443
POP3	Protokół odbierania poczty elektronicznej	110 (szyfrowany 995)
IMAP	Protokół odbierania poczty elektronicznej umożliwiający zarządzanie folderami znajdującymi się w skrzynce pocztowej	143 (szyfrowany 993)
SMTP	Protokół wysyłania poczty elektronicznej	25 (szyfrowany 465 lub 587)
FTP	Protokół przesyłania plików	21 (polecenia) i 20 (pliki)
FTPS	Szyfrowany protokół FTP	990
TELNET	Protokół połączenia terminalowego	23
SSH	Szyfrowany protokół połączenia terminalowego	22
DNS	Protokół zamiany nazw domenowych na adresy IP	53
DHCP	Protokół automatycznej konfiguracji hostów w sieci	67 i 68 (dla IPv6 546 i 547)
LDAP	Protokół usług katalogowych (np. Active Directory w Windows Server)	389 (szyfrowany 639)
SNMP	Protokół konfiguracji urządzeń sieciowych	161
MySQL	System zarządzania bazami danych	3306
PostgreSQL	System zarządzania bazami danych	5432

Protokół warstwy aplikacji	Numer portu	Protokół warstwy transportowej
HTTP	80	TCP
HTTPS	443	TCP
POP3	110 (szyfrowany 995)	TCP
IMAP	143 (szyfrowany 993)	TCP
SMTP	25 (szyfrowany 465 lub 587)	TCP
FTP	21 (polecenia) i 20 (pliki)	TCP
FTPS	990	TCP
TELNET	23	TCP
SSH	22	TCP
DNS	53	TCP lub UDP
DHCP	67 i 68 (dla IPv6 546 i 547)	UDP
LDAP	389 (szyfrowany 639)	TCP lub UDP
SNMP	161	UDP

Domyślny port dla pulpitu zdalnego w systemie Windows to **TCP 3389**

Porty wymagane do komunikacji AD

Do podstawowej komunikacji AD wymagane są następujące porty:

- Port UDP 53: DNS
- Port TCP/UDP 88: uwierzytelnianie Kerberos
- Port TCP/UDP 135: RPC
- Port UDP 137-138: NetBIOS
- Port TCP/UDP 389: LDAP
- Port TCP/UDP 445: SMB
- Port TCP/UDP 464: zmiana hasła Kerberos
- Port TCP/UDP 636: LDAP SSL
- Port TCP/UDP 3268-3269: Katalog globalny

Oprócz tych portów mogą być wymagane inne porty, w zależności od konkretnych komponentów i funkcji środowiska AD. Na przykład, jeśli używasz zasad grupy, wymagane będą również następujące porty:

- Port TCP 80: HTTP
- Port TCP 443: HTTPS
- Port TCP 445: SMB

Jeśli używasz usług ADFS (Active Directory Federation Services) do pojedynczego logowania, wymagane będą również następujące porty:

- Port TCP 80: HTTP
- Port TCP 443: HTTPS
- Port TCP 49443: ADFS

Porty wymagane do komunikacji PKI

Aby infrastruktura [PKI](#) działała prawidłowo, należy otworzyć pewne porty w zaporze sieciowej, aby umożliwić komunikację pomiędzy różnymi komponentami systemu PKI. Porty te obejmują:

1. Port TCP 80

Ten port jest używany do komunikacji HTTP, która jest wymagana, aby klienci mogli uzyskać dostęp do [listy odwołanych certyfikatów \(CRL\)](#) i innych informacji z serwera [urzędu certyfikacji \(CA\)](#).

2. Port TCP 389

Ten port jest używany do komunikacji LDAP, która jest wymagana, aby klienci mogli uzyskać dostęp do bazy danych certyfikatów na serwerze urzędu certyfikacji.

3. Port TCP 636

Ten port jest używany do komunikacji LDAPS, bezpiecznej wersji LDAP, która do [szyfrowania używa protokołu SSL/TLS](#). Jest to wymagane, jeśli używasz protokołu LDAP w sieci publicznej.

4. Port TCP 9389

Ten port jest używany przez protokół Web Services for Management (WS-Management), który jest wymagany, aby klienci mogli uzyskać dostęp do serwera urzędu certyfikacji za pomocą przystawki Certyfikaty w konsoli Microsoft Management Console (MMC).

Oprócz tych portów może być konieczne otwarcie innych portów, w zależności od konkretnych komponentów i konfiguracji systemu PKI. Na przykład, jeśli do sprawdzania stanu certyfikatów używasz [protokołu OCSP](#), konieczne będzie otwarcie portu TCP 2560.

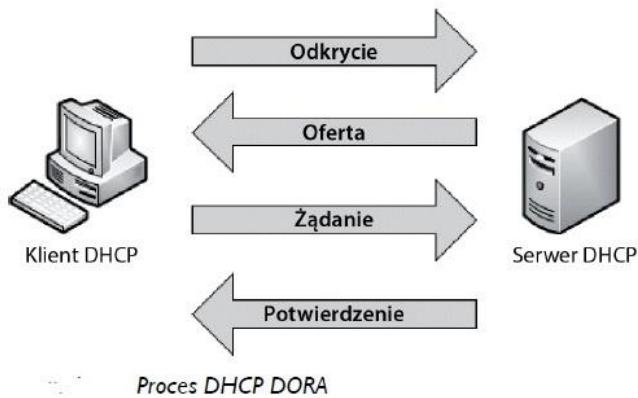
1.2.1 ODPOWIEDŹ 1: Charakterystyka protokołu DHCP

Nazwa DHCP: Dynamic Host Configuration Protocol (W Wireshark -u używana nazwa to Bootstrap Protocol) **4**

- Protokół DHCP odpowiedzialny jest za umożliwienie urządzeniu sieciowemu (węzłowi) automatycznego pobierania adresu IP z maską podsieci, adresu serwerów DNS, ruterów (bramy domyślnej) !!! Patrz pakiet DHCP Offer poniżej: **7 - 11**
- Adres docelowy nagłówka ramki to ff:ff:ff:ff:ff:ff (adres rozgłoszeniowy typu broadcast). **1**
- Klient wysyła pakiet DHCP z adresem IP 0.0.0.0 do urządzenia o adresie IP 255.255.255.255. **2**
- Klient używa adresu 0.0.0.0, ponieważ nie ma jeszcze przypisanego adresu IP. **5**
- Usługa DHCP jako protokół warstwy transportowej wykorzystuje protokół UDP. **3**
- Protokół DHCP ma wbudowane mechanizmy zapewniające niezawodność działania, więc protokół UDP może być wykorzystany ze względu na jego szybkość działania. Przypisywanie adresu IP węzłom w sieci musi się odbywać bardzo sprawnie
- Ponieważ węzeł klienta nie zna adresu serwera DHCP wysyła ramkę, która ma go odszukać. Ramka jest w sieci lokalnej kopiowana do wszystkich pozostałych węzłów. Serwer DHCP prowadzi nasłuch na ramki kierowanych do niego.

```
Wireshark · Pakiet 60 · wireshark_A1D9FE5D-FF11-4003-A704-3B890C614707_20161008041849_a05644
[+] Frame 60: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
[+] Ethernet II, Src: Tp-LinkT_0c:14:0f (ec:08:6b:0c:14:0f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  [+] Destination: Broadcast (ff:ff:ff:ff:ff:ff) 1
    Address: Broadcast (ff:ff:ff:ff:ff:ff)
    .... ..1. .... .. = LG bit: Locally administered address (this is NOT the factory default)
    .... ..1. .... .. = IG bit: Group address (multicast/broadcast)
  [+] Source: Tp-LinkT_0c:14:0f (ec:08:6b:0c:14:0f)
    Address: Tp-LinkT_0c:14:0f (ec:08:6b:0c:14:0f)
    .... ..0. .... .. = LG bit: Globally unique address (factory default)
    .... ..0. .... .. = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
  [+] Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255 2
  [+] User Datagram Protocol, Src Port: 68, Dst Port: 67 3
  [+] Bootstrap Protocol (Discover) 4
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x674f262a
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0 5
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Tp-LinkT_0c:14:0f (ec:08:6b:0c:14:0f)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  [+] Option: (53) DHCP Message Type (Discover) 6
  [+] Option: (61) Client identifier
  [+] Option: (50) Requested IP Address
  [+] Option: (12) Host Name
  [+] Option: (60) Vendor class identifier
  [+] Option: (55) Parameter Request List
  [+] Option: (255) End
```


1.2.2 ODPOWIEDŹ 2: Czym jest proces DORA protokołu DHCP



- Proces dzierżawy adresu IP zachodzi między pojedynczym klientem i serwerem DHCP
- Proces dzierżawy adresu IP jest często określany mianem procesu DORA, ponieważ zwykle opiera się na czterech pakietach:

- odkrycie (ang. *Discover*) - screen powyżej
- oferta (ang. *Offer*)
-

```
Frame 63: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Tp-LinkT_90:b5:ac (ec:08:6b:90:b5:ac), Dst: Tp-LinkT_0c:14:0f (ec:08:6b:0c:14:0f)
Internet Protocol Version 4, Src: 222.222.222.1, Dst: 222.222.222.2
User Datagram Protocol, Src Port: 67, Dst Port: 68
Bootstrap Protocol (Offer)
  Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x674f262a
  Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
    0... .... = Broadcast flag: Unicast
    .000 0000 0000 0000 = Reserved flags: 0x0000
  Client IP address: 0.0.0.0
  Your (client) IP address: 222.222.222.2 7
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: Tp-LinkT_0c:14:0f (ec:08:6b:0c:14:0f)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (53) DHCP Message Type (Offer)
    Length: 1
    DHCP: Offer (2)
  Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (7200s) 2 hours
  Option: (54) DHCP Server Identifier
    Length: 4
    DHCP Server Identifier: 222.222.222.1 8
  Option: (1) Subnet Mask
    Length: 4
    Subnet Mask: 255.255.255.240 9
  Option: (3) Router
    Length: 4
    Router: 222.222.222.1 10
  Option: (6) Domain Name Server
    Length: 8
    Domain Name Server: 222.222.222.1 11
    Domain Name Server: 0.0.0.0
  Option: (255) End
    Option End: 255
  Padding: 53465420352e30370c010f03062c2e2f1f2179f92bfff
```

➤ żądanie (ang. *Request*)

```
⊞ Frame 64: 368 bytes on wire (2944 bits), 368 bytes captured (2944 bits) on interface 0
⊞ Ethernet II, Src: Tp-LinkT_0c:14:0f (ec:08:6b:0c:14:0f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
⊞ User Datagram Protocol, Src Port: 68, Dst Port: 67
⊞ Bootstrap Protocol (Request)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x674f262a
  Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
    0... .. = Broadcast flag: Unicast
    .000 0000 0000 0000 = Reserved flags: 0x0000
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: Tp-LinkT_0c:14:0f (ec:08:6b:0c:14:0f)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (53) DHCP Message Type (Request)
    Length: 1
    DHCP: Request (3)
  Option: (61) Client identifier
    Length: 7
    Hardware type: Ethernet (0x01)
    Client MAC address: Tp-LinkT_0c:14:0f (ec:08:6b:0c:14:0f)
  Option: (50) Requested IP Address
    Length: 4
    Requested IP Address: 222.222.222.2
  Option: (54) DHCP Server Identifier
    Length: 4
    DHCP Server Identifier: 222.222.222.1
  Option: (12) Host Name
    Length: 15
    Host Name: michal-Komputer
  Option: (81) Client Fully Qualified Domain Name
    Length: 18
    ⊞ Flags: 0x00
    A-RR result: 0
    PTR-RR result: 0
    Client name: michal-Komputer
  Option: (60) Vendor class identifier
    Length: 8
    Vendor class identifier: MSFT 5.0
  Option: (55) Parameter Request List
    Length: 12
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (15) Domain Name
    Parameter Request List Item: (3) Router
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
    Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
    Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
```

➤ potwierdzenie (ang. *Acknowledgment*)

```
Wireshark · Pakiet 66 · wireshark_A1D9FE5D-FF11-4003-A704-3B890C614707_20161008041849_a05644

+ Frame 66: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
+ Ethernet II, Src: Tp-LinkT_90:b5:ac (ec:08:6b:90:b5:ac), Dst: Tp-LinkT_0c:14:0f (ec:08:6b:0c:14:0f)
+ Internet Protocol Version 4, Src: 222.222.222.1, Dst: 222.222.222.2
+ User Datagram Protocol, Src Port: 67, Dst Port: 68
+ Bootstrap Protocol (ACK)
  - Message type: Boot Reply (2)
  - Hardware type: Ethernet (0x01)
  - Hardware address length: 6
  - Hops: 0
  - Transaction ID: 0x674f262a
  - Seconds elapsed: 0
  - Bootp flags: 0x0000 (Unicast)
    - 0... .. = Broadcast flag: Unicast
    - .000 0000 0000 0000 = Reserved flags: 0x0000
  - Client IP address: 0.0.0.0
  - Your (client) IP address: 222.222.222.2
  - Next server IP address: 0.0.0.0
  - Relay agent IP address: 0.0.0.0
  - Client MAC address: Tp-LinkT_0c:14:0f (ec:08:6b:0c:14:0f)
  - Client hardware address padding: 00000000000000000000
  - Server host name not given
  - Boot file name not given
  - Magic cookie: DHCP
  - Option: (53) DHCP Message Type (ACK)
    - Length: 1
    - DHCP: ACK (5)
  - Option: (51) IP Address Lease Time
    - Length: 4
    - IP Address Lease Time: (7200s) 2 hours
  - Option: (54) DHCP Server Identifier
    - Length: 4
    - DHCP Server Identifier: 222.222.222.1
  - Option: (1) Subnet Mask
    - Length: 4
    - Subnet Mask: 255.255.255.240
  - Option: (3) Router
    - Length: 4
    - Router: 222.222.222.1
  - Option: (6) Domain Name Server
    - Length: 8
    - Domain Name Server: 222.222.222.1
    - Domain Name Server: 0.0.0.0
  - Option: (255) End
    - Option End: 255
  - Padding: 74657251120000006d696368616c2d4b6f6d70757465
```

1.2.3 ODPOWIEDŹ 3: Omów strukturę pakietu DHCP

Protokół DHCP				
Pozycja	0–15		16–31	
0	Kod operacji	Typ warstwy fizycznej	Długość adresu sprzętowego	Liczba skoków
32	Identyfikator transakcji			
64	Liczba sekund		Flagi	
96	Adres IP klienta			
128	Twój adres IP			
160	Adres IP serwera			
196	Adres IP bramy domyślnej			
228+	Sprzętowy adres klienta (16 bajtów)			
	Nazwa serwera (64 bajty)			
	Nazwa pliku startowego (128 bajtów)			
	Opcje			

Struktura pakietu DHCP

W pakiecie DHCP znajdują się następujące pola:

- **Kod operacji.** Wskazuje rodzaj pakietu: żądanie DHCP lub odpowiedź DHCP.
- **Typ warstwy fizycznej.** Rodzaj wykorzystywanej warstwy sprzętowej (10 MB Ethernet, IEEE 802, ATM itd.).
- **Długość adresu sprzętowego.** Pole zawiera długość adresu sprzętowego. Liczba skoków. Wartość używana przez agentów przekazywania do pomocy w wyszukaniu serwera DHCP.
- **Identyfikator transakcji.** Losowo wygenerowana wartość przeznaczona do powiązania żądania z odpowiedzią.
- **Liczba sekund.** Liczba sekund, które upłynęły od wysuniętego przez klienta pierwszego żądania adresu z serwera DHCP.
- **Flagi.** Rodzaje ruchu sieciowego akceptowanego przez klienta DHCP (unicast, broadcast itd.).
- **Adres IP klienta.** Adres IP klienta (pobrany z pola Twój adres IP).
- **Twój adres IP.** Adres IP zaoferowany przez serwer DHCP (ostatecznie stanie się adresem IP klienta, przechowywanym w polu Adres IP klienta).
- **Adres IP serwera.** To pole zawiera adres IP serwera DHCP.
- **Adres IP bramy.** To pole zawiera adres IP bramy domyślnej.
- **Sprzętowy adres klienta.** To adres MAC klienta.
- **Nazwa serwera.** To nazwa serwera (opcjonalna).
- **Nazwa pliku startowego.** To nazwa pliku startowego używanego przez DHCP (opcjonalna).
- **Opcje.** Pole używane do rozszerzenia struktury pakietu DHCP w celu udostępnienia mu większej liczby funkcji.

Protokół HTTP

http://brzoza5.edu.pl/pcapng

PL Edycja Widok Id Przechwyty Analiza Statystyki Telefon Bezprzewodowe Narzędzia Pomoc

ip.addr == 94.152.8.4

Wynajęcie

No.	Time	Source	Destination	Protocol	Length	Info
1537	12.069823	222.222.222.3	94.152.8.4	TCP	66	49912→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1538	12.069195	222.222.222.3	94.152.8.4	TCP	66	49913→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1539	12.089555	94.152.8.4	222.222.222.3	TCP	62	80→49912 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 WS=128
1540	12.089608	222.222.222.3	94.152.8.4	TCP	54	49912→80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
1541	12.091244	94.152.8.4	222.222.222.3	TCP	62	80→49913 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 WS=128
1542	12.091291	222.222.222.3	94.152.8.4	TCP	54	49913→80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
1543	12.112469	222.222.222.3	94.152.8.4	HTTP	454	GET / HTTP/1.1
1544	12.144499	94.152.8.4	222.222.222.3	TCP	54	80→49912 [ACK] Seq=1 Ack=401 Win=30336 Len=0
1545	12.668511	94.152.8.4	222.222.222.3	HTTP	543	HTTP/1.1 301 Moved Permanently (text/html) (text/html)
1548	12.697194	222.222.222.3	94.152.8.4	TCP	66	49914→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1549	12.697677	222.222.222.3	94.152.8.4	TCP	66	49915→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1550	12.717478	94.152.8.4	222.222.222.3	TCP	62	80→49914 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 WS=128
1551	12.717542	222.222.222.3	94.152.8.4	TCP	54	49914→80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
1552	12.717920	94.152.8.4	222.222.222.3	TCP	62	80→49915 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 WS=128
1553	12.717979	222.222.222.3	94.152.8.4	TCP	54	49915→80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
1554	12.720727	222.222.222.3	94.152.8.4	HTTP	484	GET / HTTP/1.1
1555	12.742112	94.152.8.4	222.222.222.3	TCP	54	80→49914 [ACK] Seq=1 Ack=431 Win=30336 Len=0
1558	12.876267	222.222.222.3	94.152.8.4	TCP	54	49912→80 [ACK] Seq=401 Ack=490 Win=65536 Len=0
1577	14.143899	94.152.8.4	222.222.222.3	TCP	14...	[TCP segment of a reassembled PDU]
1578	14.145499	94.152.8.4	222.222.222.3	TCP	14...	[TCP segment of a reassembled PDU]
1579	14.145501	94.152.8.4	222.222.222.3	TCP	14...	[TCP segment of a reassembled PDU]
1580	14.145549	222.222.222.3	94.152.8.4	TCP	54	49914→80 [ACK] Seq=431 Ack=4321 Win=66048 Len=0
1581	14.147968	94.152.8.4	222.222.222.3	TCP	14...	[TCP segment of a reassembled PDU]
1582	14.147970	94.152.8.4	222.222.222.3	TCP	14...	[TCP segment of a reassembled PDU]
1583	14.147971	94.152.8.4	222.222.222.3	TCP	14...	[TCP segment of a reassembled PDU]
1584	14.147975	94.152.8.4	222.222.222.3	TCP	14...	[TCP segment of a reassembled PDU]
1585	14.148030	222.222.222.3	94.152.8.4	TCP	54	49914→80 [ACK] Seq=431 Ack=10070 Win=66048 Len=0
1586	14.171427	94.152.8.4	222.222.222.3	HTTP	74	HTTP/1.1 200 OK (text/html)
1587	14.175233	222.222.222.3	94.152.8.4	TCP	66	49916→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1588	14.175475	222.222.222.3	94.152.8.4	TCP	66	49917→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1589	14.178947	222.222.222.3	94.152.8.4	HTTP	521	GET /wp-content/plugins/mtouch-quiz/style.min.css?ver=2.5.5 HTTP/1.1
1590	14.186645	222.222.222.3	94.152.8.4	TCP	66	49918→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1591	14.193644	222.222.222.3	94.152.8.4	TCP	66	49919→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1

Frame 1539: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0

Ethernet II, Src: Tp-LinkT_90:b5:ac (ec:08:6b:90:b5:ac), Dst: Tp-LinkT_0c:14:0f (ec:08:6b:0c:14:0f)

Destination: Tp-LinkT_0c:14:0f (ec:08:6b:0c:14:0f)

0000 ec 08 6b 0c 14 0f ec 08 6b 90 b5 ac 08 00 45 00 ..k.... k....E.

0010 00 30 00 00 40 00 38 06 1f 4a 5e 98 08 04 de de ..0..@.8. .J^.....

0020 de 03 00 50 c2 f8 98 45 19 66 2e 55 f2 2c 70 12 ...P...E .f.U.,p.

http://brzoza5

Pakietów: 5043 · Wyświetlonych: 2886 (57.2%) · Porzuconych: 0 (0.0%) · Czas ładowania: 0:0.95 | Profil: Default

22:54 2016-10-10

1.2.4 ODPOWIEDŹ 4: Ogólna charakterystyka protokołu HTTP

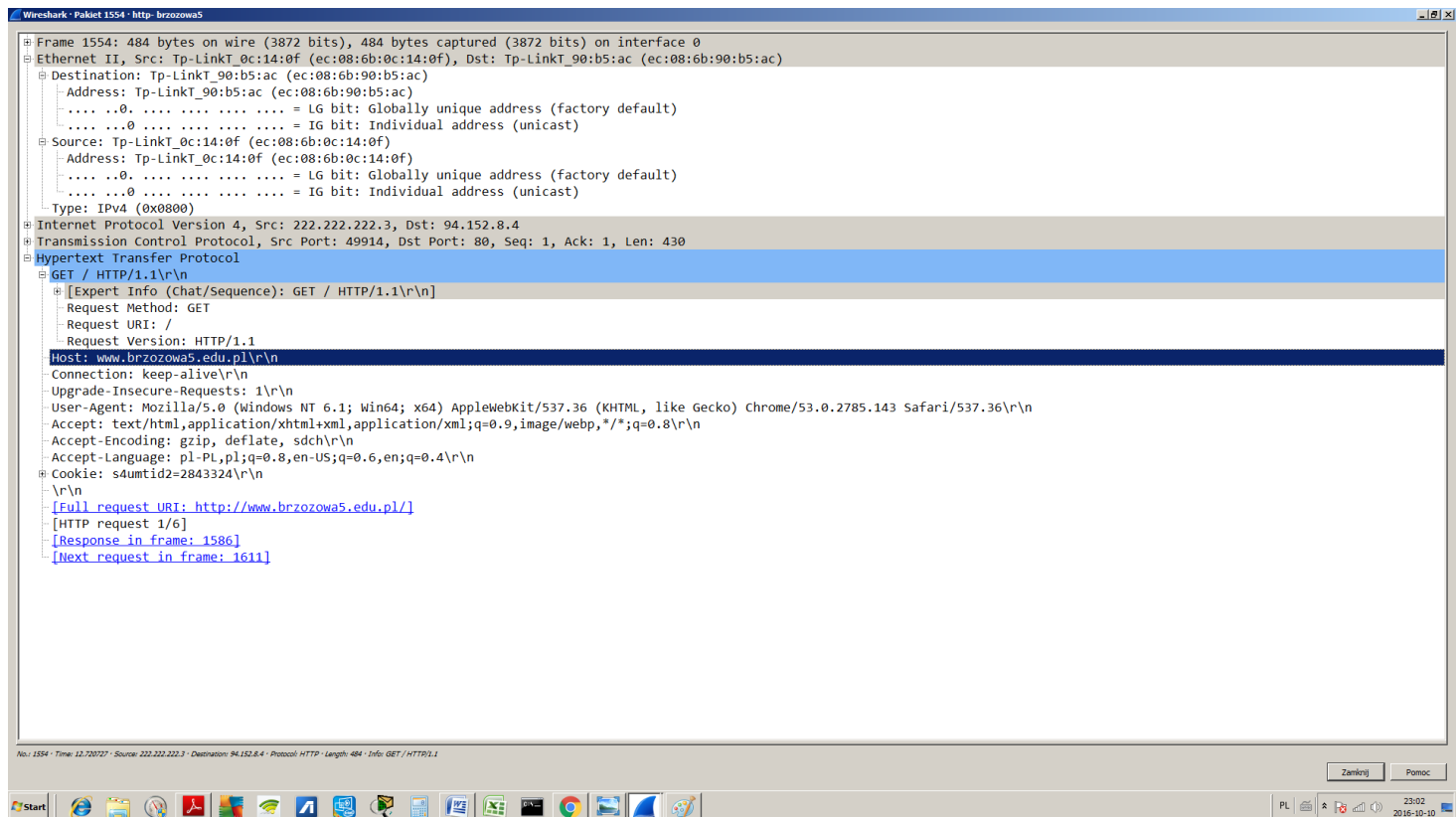
- Nazwa HTTP : Hypertext Transfer Protocol
- jest mechanizmem dostarczania stron WWW (transport hipertekstowych znaczników)
- aplikacja HTTP tworzy gniazdo warstwy transportowej TCP/IP
- jest to protokół bezstanowy warstwy aplikacji tzn. nie zbiera danych o użytkownikach (klientach)
- przypisywany port domyślny 80
- protokół używa komunikatów np. 200 - operacja zakończona powodzeniem
- używa metody: get, post, delete
- nagłówek zawiera: metodę, wersję protokołu, adres URL, User-Agenta (używana przeglądarka np. Mozilla ..., Accept-language: np. eu-us, pl, fr, Accept-Charset: ISO 8859-1, utf-8 ...

!!!patrz - poniższe obrazki

```
Frame 1586: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: Tp-LinkT_90:b5:ac (ec:08:6b:90:b5:ac), Dst: Tp-LinkT_0c:14:0f (ec:08:6b:0c:14:0f)
Internet Protocol Version 4, Src: 94.152.8.4, Dst: 222.222.222.3
Transmission Control Protocol, Src Port: 80, Dst Port: 49914, Seq: 10070, Ack: 431, Len: 20
[8 Reassembled TCP Segments (10089 bytes): #1577(1440), #1578(1440), #1579(1440), #1581(1440), #1582(1440), #1583(1440), #1584(1429), #1586(20)]
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      [HTTP/1.1 200 OK\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
    Date: Mon, 10 Oct 2016 20:17:56 GMT\r\n
    Server: Apache\r\n
    X-Pingback: http://www.brzozowa5.edu.pl/xmlrpc.php\r\n
    Link: <http://wp.me/1SylI>; rel=shortlink\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    Set-Cookie: wfv1_141919092=57fbf7756b11e; expires=Mon, 10-Oct-2016 20:47:57 GMT; path=/; httponly\r\n
    Via: 1.1 brzozowa5.edu.pl\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
    Keep-Alive: timeout=15, max=100\r\n
    Connection: Keep-Alive\r\n
    Transfer-Encoding: chunked\r\n
    \r\n
    [HTTP response 1/6]
    [Time since request: 1.450700000 seconds]
    [Request in frame: 1554]
    [Next request in frame: 1611]
    [Next response in frame: 1645]
  HTTP chunked response
    Data chunk (9596 octets)
    Data chunk (10 octets)
    End of chunked encoding
    \r\n
```


1.2.5 ODPOWIEDŹ 5: Omów nagłówek pakietu HTTP żądania GET w oparciu o poniższy screen:

- Pakiet stosuje metodę Get, czyli żąda katalogu głównego serwera sieciowego: Resource URI: /¹ używając do tego wersji protokołu HTTP/1.1
- Nazwa hosta czyli serwera to www.brzozowa5.edu.pl
- Następnie klient wysyła serwerowi WWW następujące informacje o sobie:
 - używanego agenta (przeglądarkę internetową,
 - akceptowany język przez przeglądarkę,
 - informacje o ciasteczkach (ang. *cookies*)



1.2.6 ODPOWIEDŹ 6: Jak wygląda transmisja danych strony (obiektów) z serwera WWW do klienta?

- Kiedy serwer WWW otrzymuje żądanie GET odpowiada klientowi pakietem potwierdzenia (TCP ACK) a następnie przekazuje żądane dane.
- Protokół HTTP jest używany jedynie do wykonywania poleceń warstwy aplikacji pomiędzy klientem i serwerem.
- Kiedy trzeba przekazać faktycznie dane, kontrola nie należy już do warstwy aplikacji, poza rozpoczęciem i zakończeniem strumienia.
- Kod 200 protokołu HTTP wysłanego przez serwer do klienta kończy przesyłanie żądanych danych

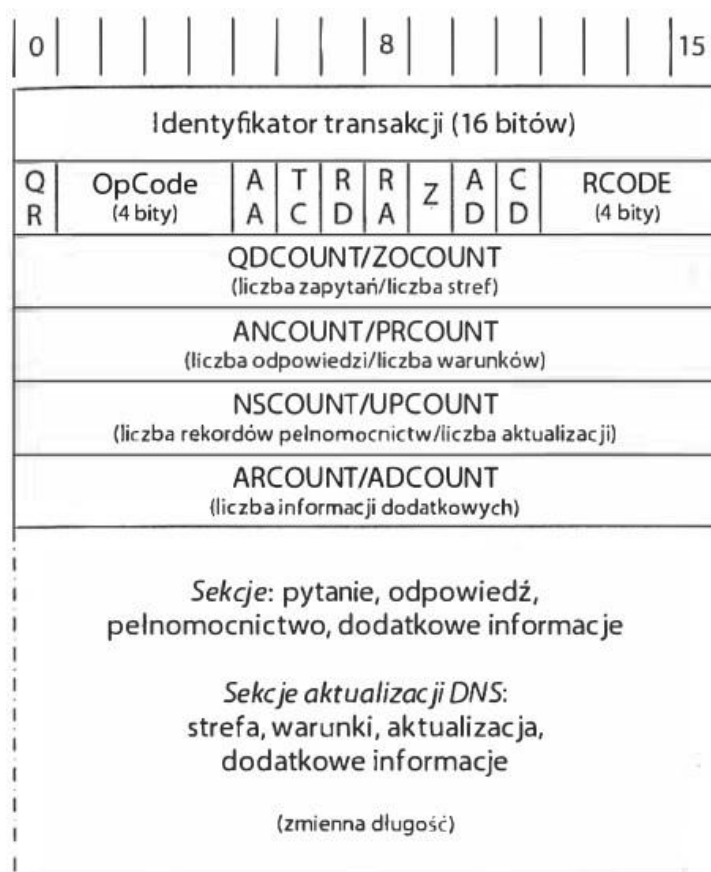
1554	12.720727	222.222.222.3	94.152.8.4	HTTP	484 GET / HTTP/1.1
1555	12.742112	94.152.8.4	222.222.222.3	TCP	54 80→49914 [ACK] Seq=1 Ack=431 Win=30336 Len=0
1558	12.876267	222.222.222.3	94.152.8.4	TCP	54 49912→80 [ACK] Seq=401 Ack=490 Win=65536 Len=0
1577	14.143899	94.152.8.4	222.222.222.3	TCP	14... [TCP segment of a reassembled PDU]
1578	14.145499	94.152.8.4	222.222.222.3	TCP	14... [TCP segment of a reassembled PDU]
1579	14.145501	94.152.8.4	222.222.222.3	TCP	14... [TCP segment of a reassembled PDU]
1580	14.145549	222.222.222.3	94.152.8.4	TCP	54 49914→80 [ACK] Seq=431 Ack=4321 Win=66048 Len=0
1581	14.147968	94.152.8.4	222.222.222.3	TCP	14... [TCP segment of a reassembled PDU]
1582	14.147970	94.152.8.4	222.222.222.3	TCP	14... [TCP segment of a reassembled PDU]
1583	14.147971	94.152.8.4	222.222.222.3	TCP	14... [TCP segment of a reassembled PDU]
1584	14.147975	94.152.8.4	222.222.222.3	TCP	14... [TCP segment of a reassembled PDU]
1585	14.148030	222.222.222.3	94.152.8.4	TCP	54 49914→80 [ACK] Seq=431 Ack=10070 Win=66048 Len=0
1586	14.171427	94.152.8.4	222.222.222.3	HTTP	74 HTTP/1.1 200 OK (text/html)

1.2.7 ODPOWIEDŹ 7: Scharakteryzuj protokół DNS

Protokół DNS

- (ang. Domain Name System)
- jest protokołem warstwy aplikacji
- pośredniczy w komunikacji systemów końcowych korzystających z architektury klient - serwer
- do transferowania komunikatów wykorzystuje znajdujący się niżej międzywzłowy protokół transportowy UDP.
- nie umożliwia użytkownikowi prowadzenia z nim bezpośredniej interakcji
- Protokół DNS powoduje powiązanie nazwy, na przykład www.google.com, z jej adresem IP, na przykład **74.125.159.99**. Kiedy zachodzi potrzeba przeprowadzenia komunikacji z urządzeniem w sieci, którego adres IP pozostaje nieznanym, dostęp do tego urządzenia można uzyskać za pomocą nazwy DNS.

1.2.8 ODPOWIEDŹ 8: Omów strukturę pakietu DNS



W pakiecie DNS można znaleźć następujące pola:

- **Identyfikator DNS.** Wartość używana do powiązania zapytania DNS z odpowiedzią na nie.
- **Żądanie/odpowiedź (QR).** Pole określa rodzaj pakietu: żądanie lub odpowiedź DNS.
- **Kod operacji.** Pole definiuje typ zapytania zawartego w pakiecie.
- **Odpowiedź autorytatywna (AA).** Jeżeli ta wartość została ustawiona w pakiecie odpowiedzi, to wskazuje, że odpowiedź pochodzi z autorytatywnego serwera nazw.
- **Obciążenie (TC).** Wartość ta określa, czy odpowiedź została skrócona, ponieważ była zbyt duża, aby zmieściła się w pakiecie.
- **Żądanie rekurencji (RD).** Jeżeli ta wartość została ustawiona w zapytaniu, to wskazuje, że klient DNS żąda wykonania zapytania rekurencyjnego, gdy serwer nazw nie będzie zawierał żądanych informacji.
- **Rekurencja jest dostępna (RA).** Jeżeli ta wartość została ustawiona w odpowiedzi, to wskazuje, że serwer nazw obsługuje zapytania rekurencyjne.
- **Zarezerwowane (Z).** W dokumencie RFC 1035 zdefiniowano, że wszystkimi wartościami tego pola powinny być zera. Jednak czasami pole to jest używane jako rozszerzenie pola RCode.
- **Kod odpowiedzi (RCode).** Pole używane w odpowiedzi DNS w celu wskazania istnienia ewentualnych błędów.
- **Liczba zapytań.** Pole określa liczbę rekordów w sekcji zapytań.
- **Liczba odpowiedzi.** Pole określa liczbę rekordów w sekcji odpowiedzi.
- **Liczba rekordów serwera.** Pole określa liczbę rekordów zasobów w sekcji autorytatywnej.
- **Liczba rekordów dodatkowych.** Pole określa liczbę rekordów innych źródeł w sekcji informacji dodatkowych.
- **Sekcja zapytań.** Sekcja o zmiennej wielkości zawierająca wysyłane do serwera DNS co najmniej jedno zapytanie o informacje.
- **Sekcja odpowiedzi.** Sekcja o zmiennej wielkości zawierająca co najmniej jeden rekord zasobów będący odpowiedzią na otrzymane przez serwer DNS zapytanie.
- **Sekcja autorytatywna.** Sekcja o zmiennej wielkości zawierająca rekordy zasobów prowadzących do autorytatywnych serwerów nazw, które to nazwy mogą być używane do dalszego prowadzenia procesu określania nazw.
- **Sekcja informacji dodatkowych.** Sekcja o zmiennej wielkości zawierająca rekordy zasobów przechowujących informacje dodatkowe związane z zapytaniami. Informacje te nie są niezbędne do udzielenia odpowiedzi na zapytania.

1.2.9 ODPOWIEDŹ 9: Jaka jest procedura pozyskiwania adresu IP strony WWW przez klienta

Aby pozyskać adres IP strony WWW np. www.brzozowa5.edu.pl wykonywane są następujące kroki:

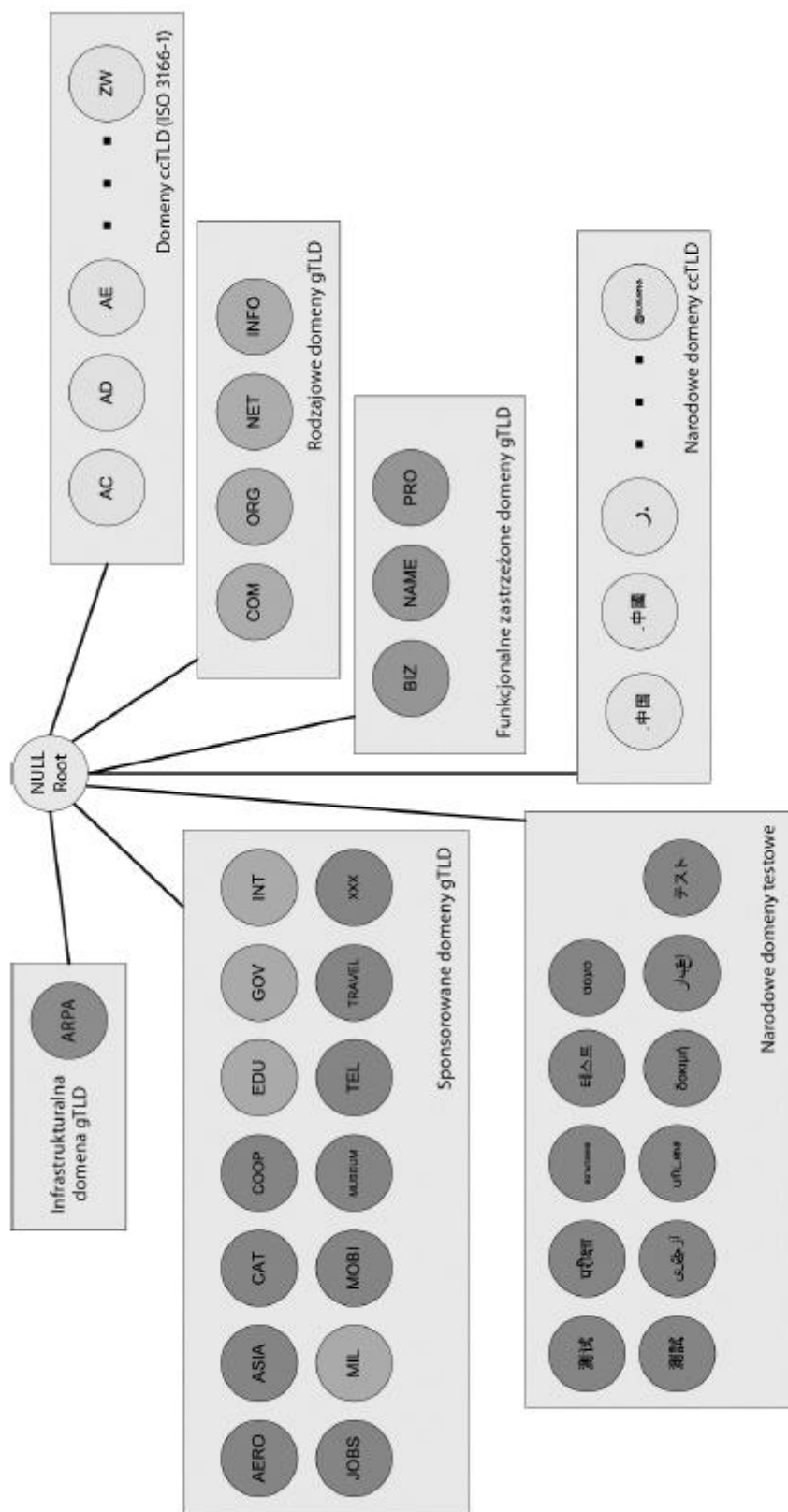
- Na komputerze użytkownika jest uaktywniany klient DNS
- Przeglądarka z adresu URL wyodrębnia nazwę hosta np. www.brzozowa5.edu.pl i przekazuje ją klientowi DNS
- Klient DNS wysyła do serwera DNS zapytanie zawierające nazwę hosta.
- Klient DNS otrzymuje odpowiedź uwzględniającą adres IP odpowiadający nazwie hosta
- Po odebraniu adresu IP od klienta DNS przeglądarka internetowa może zainicjować połączenie TCP z procesem serwera HTTP, działającym w porcie 80 pod tym adresem (w tym wypadku to adres **94.152.8.4**)

1.2.10 ODPOWIEDŹ 10: Wymień i scharakteryzuj ważne usługi systemu DNS

- **Translacja nazw hostów na ich adresy IP.** Serwery DNS przechowują bazy danych rekordów zasobów mapowań adresów IP na nazwy DNS, które następnie udostępniają klientom oraz innym serwerom DNS. Np. rekord A dla strony WWW naszej szkoły przechowuje kanoniczną nazwę hosta zsz.pgnig.brzozowa5.edu.pl i IP **94.152.8.4**².
- **Tworzenie aliasów kanonicznej nazwy hosta.** Np. Kanoniczna nazwa serwera WWW naszej szkoły to zsz.pgnig.brzozowa5.edu.pl, alias to wpisywana w przeglądarce nazwa brzozowa5.edu.pl.
- **Tworzenie aliasów nazwy serwera poczty.** Może być tak, że nazwa serwera poczty szkolnej to alias innego serwera (w naszym przypadku serwera WWW - brzozowa5.edu.pl). Aby serwer DNS nie mylił sobie serwera WWW z pocztowym, musi przechowywać rekord **MX**, w którym powiązana jest domena (alias) brzozowa5.edu.pl z kanoniczną nazwą serwera poczty poczta.zsz.pgnig.brzozowa5.edu.pl.
- **Równoważenie obciążenia.** System DNS jest też wykorzystywany do równoważenia obciążenia między serwerami. Załóżmy, że strona WWW naszej szkoły jest wyjątkowo regularnie obciążana ;-). W tym wypadku pod domenę www.brzozowa5.edu.pl może być przypisanych kilka serwerów o różnych IP. Na każdym z tych serwerów jest umieszczona strona naszej szkoły. Serwer DNS może dokonywać rotacji adresami tych serwerów. Podsumowując moja przeglądarka chcąc pobrać stronę www.brzozowa5.edu.pl może od serwera DNS otrzymać adres serwera **94.152.8.4** a pięć godzin później adres serwera **94.152.8.5** itd³.

² nazwy kanoniczne podanych serwerów WWW i poczty są zmyślane na potrzeby edukacyjne :-)

³ faktycznie strona naszej szkoły jest umieszczona na jednym serwerze

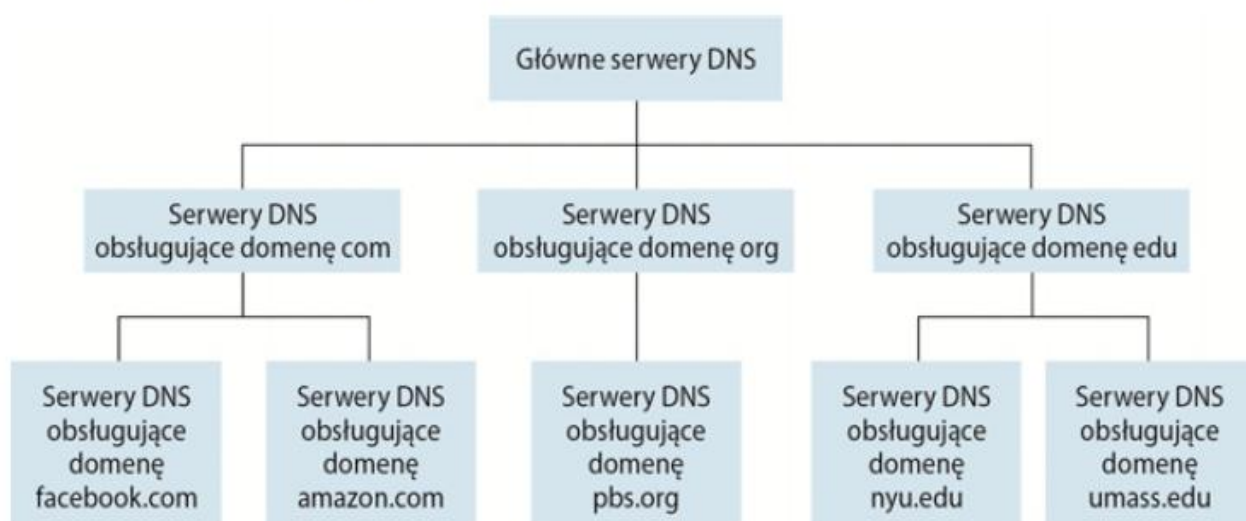
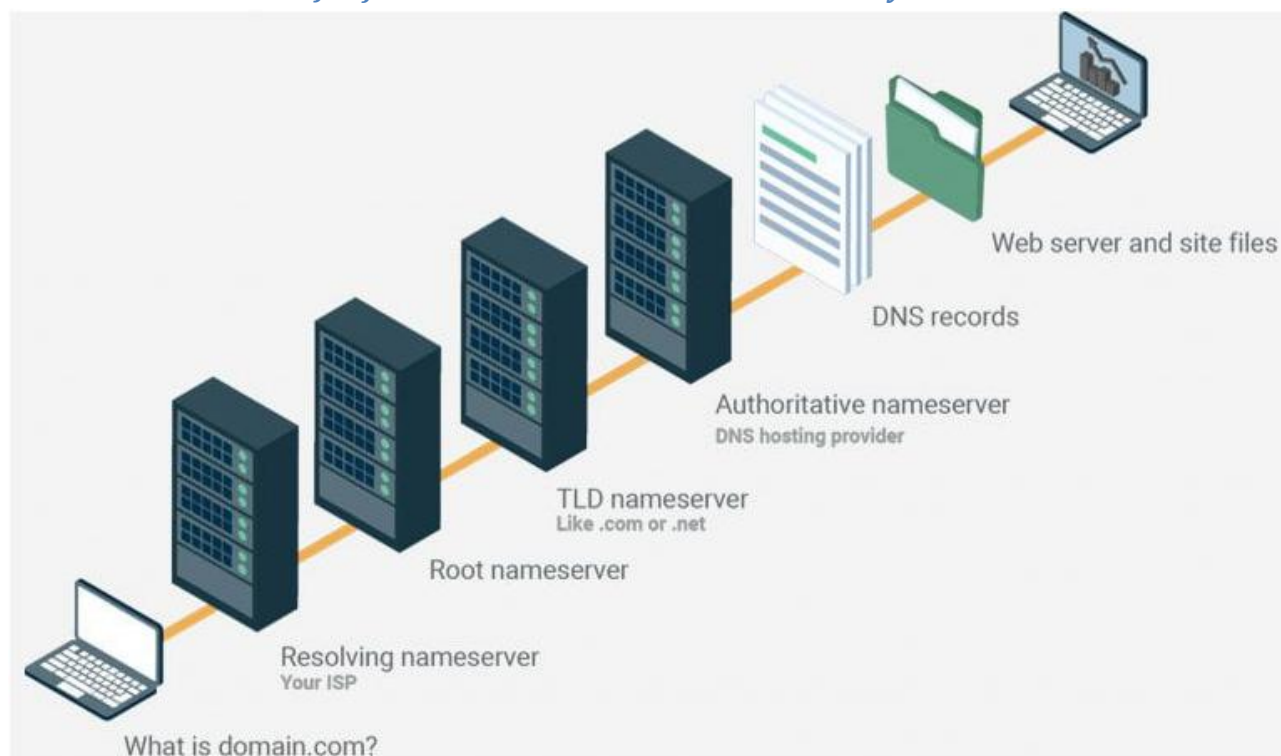


Rysunek 11.1. Przestrzeń nazw domenowych rozchodzi się od nienazwanego węzła głównego (oznaczanego też jako root), pod którym znajdują się domeny najwyższego poziomu (TLD) z domenami rodzajowymi (gTLD), domenami krajowymi (ccTLD), domenami krajowymi w zapisie narodowym (IDN ccTLD) oraz specjalnymi infrastrukturalnymi domenami ARPA

Tabela 11.1. Rodzajowe domeny najwyższego poziomu (gTLD)

TLD	Pierwsze użycie (szacunkowo)	Przeznaczenie	Przykład
AERO	21 grudnia 2001	Przemysł lotniczy	<i>www.bzg.aero</i>
ARPA	1 stycznia 1985	Infrastruktura Internetu	<i>18.in-addr.arpa</i>
ASIA	2 maja 2007	Azja i azjatycki obszar Pacyfiku	<i>www.seo.asia</i>
BIZ	26 czerwca 2001	Wykorzystanie w biznesie	<i>neustar.biz</i>
CAT	19 grudnia 2005	Katalońska społeczność językowa (kulturowa)	<i>www.domini.cat</i>
COM	1 stycznia 1985	Ogólne przeznaczenie	<i>icanhascheezburger.com</i>
COOP	15 grudnia 2001	Stowarzyszenia współpracujących firm	<i>www.ems.coop</i>
EDU	1 stycznia 1985	Policealne instytucje edukacyjne w Stanach Zjednoczonych	<i>hpu.edu</i>
GOV	1 stycznia 1985	Organizacje rządowe w Stanach Zjednoczonych	<i>whitehouse.gov</i>
INFO	25 czerwca 2001	Ogólne przeznaczenie	<i>germany.info</i>
INT	3 listopada 1988	Organizacje międzynarodowe	<i>nato.int</i>
JOBS	8 września 2005	Zarządzanie zasobami ludzkimi	<i>intel.jobs</i>
MIL	1 stycznia 1985	Organizacje militarne w Stanach Zjednoczonych	<i>dtic.mil</i>
MOBI	30 października 2005	Klienci i producenci urządzeń i usług mobilnych	<i>jestem.mobi</i>
MUSEUM	30 października 2001	Muzea	<i>chopin.museum</i>
NAME	16 sierpnia 2001	Osoby prywatne	<i>www.poznan.name</i>
NET	1 stycznia 1985	Ogólne przeznaczenie	<i>mikrofale.net</i>
ORG	9 grudnia 2002	Ogólne przeznaczenie	<i>www.joemonster.org</i>
PRO	6 maja 2002	Certyfikowani specjaliści i firmy	<i>nic.pro</i>
TEL	1 marca 2007	Dane kontaktowe dla firm i osób prywatnych	<i>telnic.tel</i>
TRAVEL	27 lipca 2005	Przemysł turystyczny	<i>cancun.travel</i>

1.2.11 ODPOWIEDŹ 11: Jak jest zbudowana hierarchiczna baza danych DNS



Rysunek 2.17. Fragment hierarchii serwerów DNS

- Baza danych DNS to system połączonych ze sobą hierarchicznie uporządkowanych serwerów, rozproszonych po całym świecie
- Żaden pojedynczy serwer DNS nie przechowuje mapowań nazw - adres IP dla wszystkich hostów znajdujących się i internecie. Mapowania są rozmieszczone między wieloma serwerami DNS.
- W przybliżeniu można wyróżnić trzy klasy serwerów DNS - główne, najwyższego poziomu (ang. Top-LevelDomain - TLD) i autorytatywne
- Każdy z głównych serwerów to w rzeczywistości klaster serwerów uczestniczących w replikacji (ze względu na bezpieczeństwo i niezawodność)
- Serwery TLD są odpowiedzialne za domeny najwyższego poziomu, takie jak com, org, net, edu i gov, a także za wszystkie domeny najwyższego poziomu państw np. pl, ru, uk, fr itd. Serwerami tymi zarządzają firmy
- Autorytatywne serwery DNS obowiązkowo przechowują mapowania nazw i IP hostów im podlegających. Autorytatywny serwer może posiadać organizacja, instytucja, korporacja. Większość dużych uczelni i firm we własnym zakresie wdraża i

zarządza podstawowymi i dodatkowymi (zapasowymi) autorytatywnymi serwerami DNS. Można również zapłacić wybranemu dostawcy usług za magazynowanie rekordów DNS na jego autorytatywnym serwerze.

- Lokalne serwery DNS nie przynależą ściśle do hierarchii serwerów DNS, choć stanowi centralny element architektury systemu DNS.
- Każdy dostawca ISP, uczelnia lub duża firma posiada lokalny serwer DNS. Dostawcy ISP najczęściej dysponują kilkoma lokalnymi serwerami DNS (sprawdź DNS na swoim routerze).
- Lokalne serwery DNS zwykle znajdują się w pobliżu naszego routera brzegowego (max odległość kilku ruterów)

Przykładowy główny(root) serwer DNS



Root Servers

The authoritative name servers that serve the DNS root zone, commonly known as the “root servers”, are a network of hundreds of servers in many countries around the world. They are configured in the DNS root zone as 13 named authorities, as follows.

List of Root Servers

HOSTNAME	IP ADDRESSES	OPERATOR
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	Verisign, Inc.
b.root-servers.net	170.247.170.2, 2801:1b8:10::b	University of Southern California, Information Sciences Institute
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	Verisign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

Mapa rozmieszczenia serwerów głównych (Root) na świecie.

Google

root dns map

X

Wszystko

Grafika

Miejsca

Wideo

Wiadomości

Sieć

Książki

Więcej

Root-Servers.org

<https://root-servers.org> · [Tłumaczenie strony](#) · [...](#)

Root Server Technical Operations Association

The 13 root name servers are operated by 12 independent organisations. You can find more information about each of these organisations by visiting their ...

[M-Root DNS Server](#) · [Verisign](#) · [USC/ISI's DNS Root Server](#) · [E.root-servers.net](#)

root-servers.org

[FAQ](#) [RSSAC001](#) [RSSAC002](#)

angie

Google Trans

Verisign USC-ISI Cogent UMD NASA OCIO ISC DISA DoD NIC ARL Netnod RIPE NCC ICANN WIDE

News and publications [show all](#)

2024-04-15 [Root Server System Operational Information](#)

2022-08-02 [Statement on adding ZONEMD to the root zone](#)

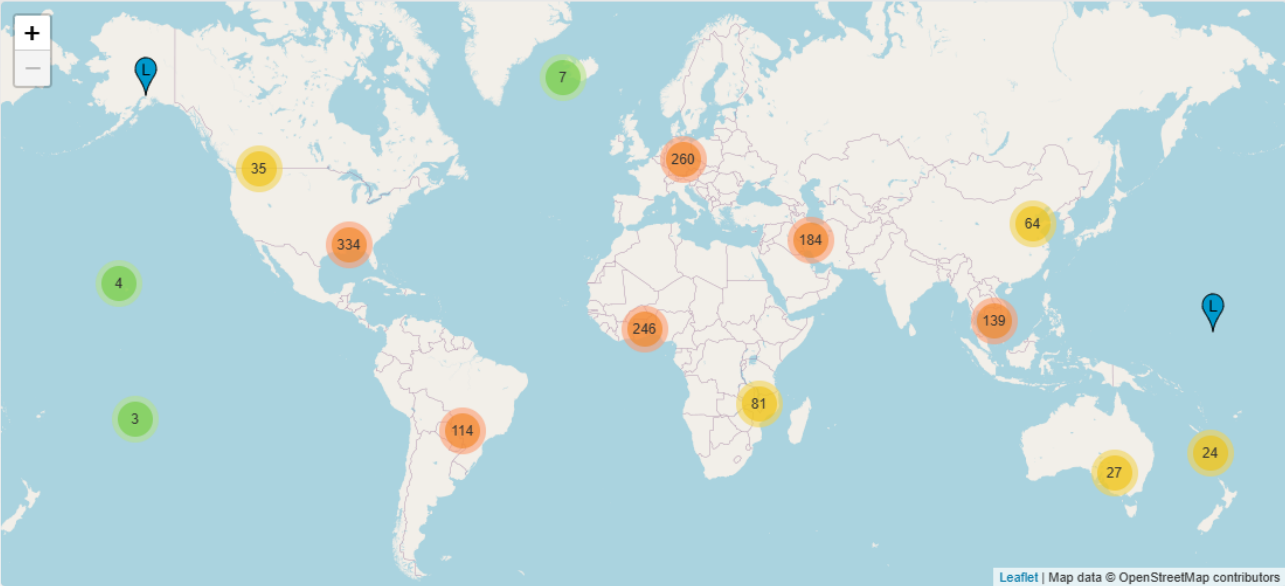
2021-03-30 [Statement on DNS Encryption](#)

Meeting agendas [show all](#)

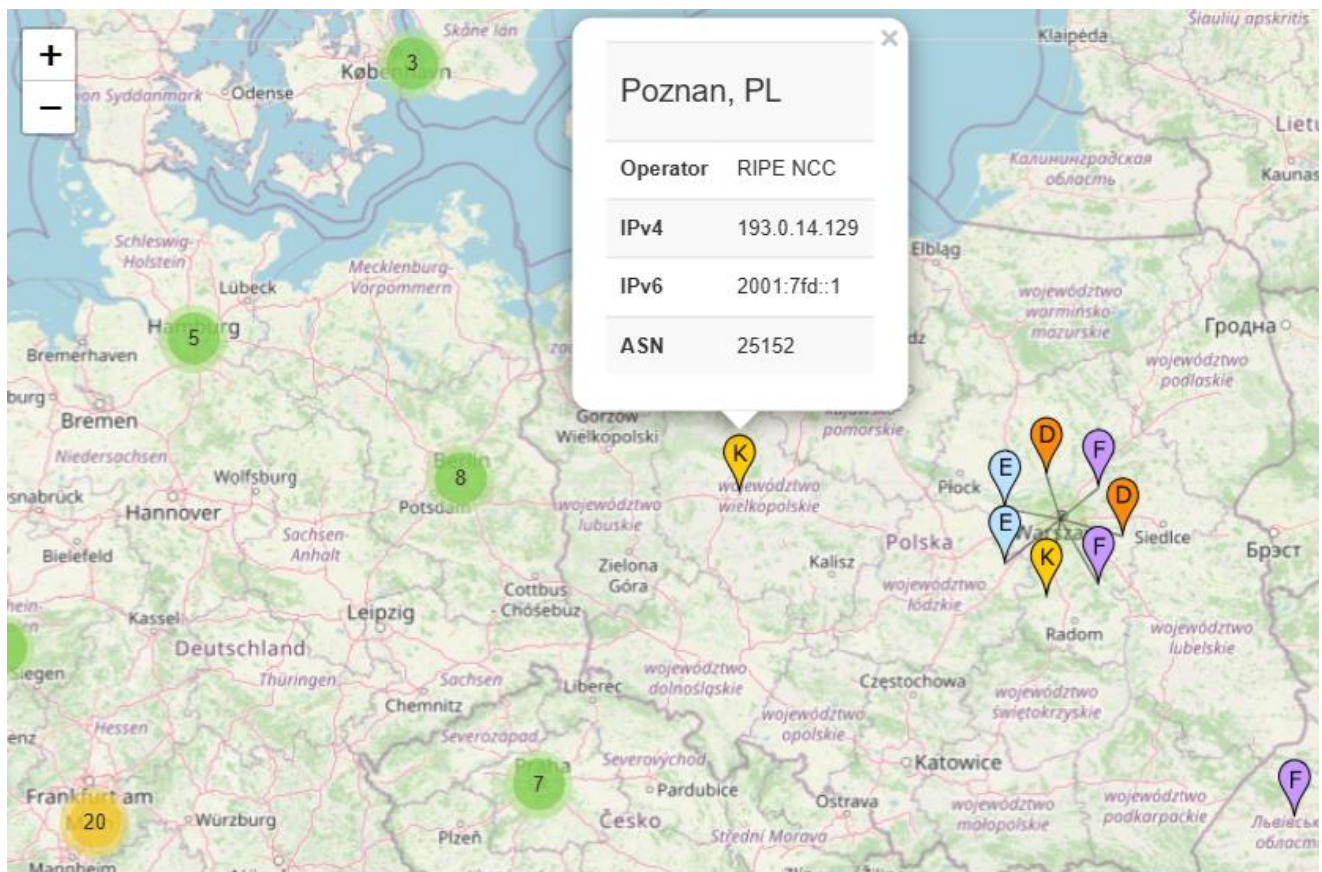
2024-11-03 [IETF 121/Dublin/Virtual \(PDF\)](#)

2024-07-21 [IETF 120/Vancouver/Virtual \(PDF\)](#)

2024-03-17 [IETF 119/Brisbane/Virtual \(PDF\)](#)



As of 2025-01-09T13:03:20Z, the root server system consists of 1921 instances operated by the 12 independent root server operators.



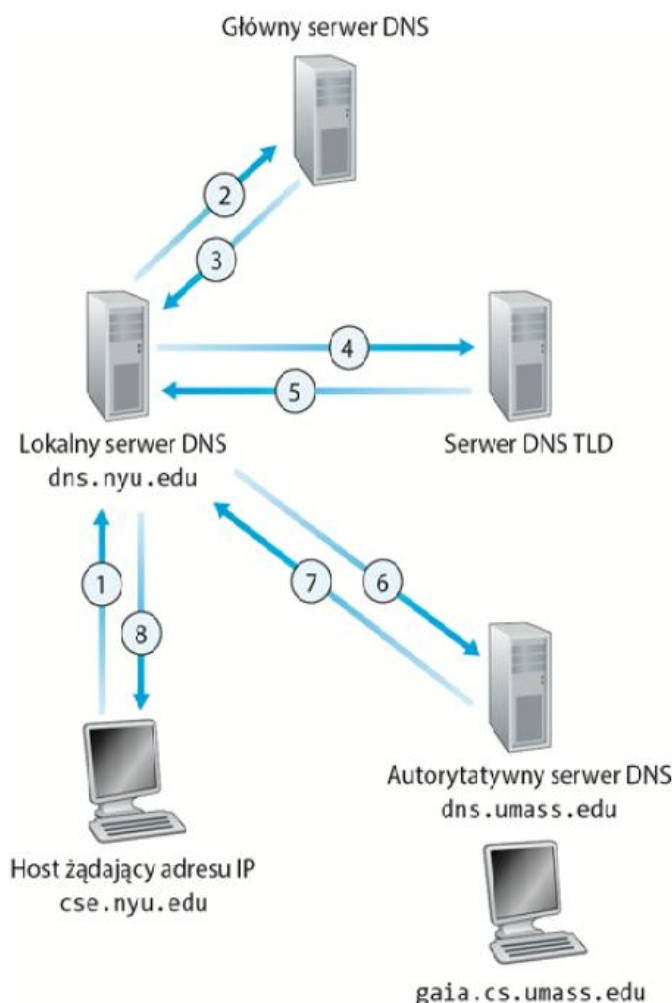
1454 Country: PL
1455 Created: '2000-01-01T01:00:00Z'
1456 ID: '1032'
1457 IPv4: true
1458 IPv6: true
1459 Identifiers:
1460 - ns1.pl-poz.k.ripe.net
1461 Instances: 1
1462 Latitude: 52.4006632
1463 Longitude: 16.91973259178088
1464 Status: operational
1465 Town: Poznan
1466 Type: Global
1467 Updated: '2024-02-19T13:23:42Z'

1.2.12 ODPOWIEDŹ 12: Jakiego typu dane zawiera rekord z bazy danych DNS; wymień typy rekordów DNS i uzupełnij je w oparciu o wymyślone przez siebie nazwy i adresy IP

WYBRANE PODSTAWOWE REKORDY DNS

Nazwa	Wartość	TYPE	TTL
Kanoniczna nazwa serwera	IPv4		Czas buforowania rekordu na serwerach podany w sekundach
web.hostcztery.kei.pl	94.152.8.4	A	3600
domena	Kanoniczna nazwa serwera albo domena strefy		
www.brzozowa5.edu.pl	web.hostcztery.kei.pl	CNAME	3600
Obsługiwana domena na serwerze dns	Kanoniczna nazwa serwera dns	NS	3600
brzozowa5.edu.pl	ns1.kei.pl		
domena poczty	Kanoniczna nazwa serwera poczty	MX	3600
poczta.brzozowa5.edu.pl	smtp.hostcztery.kei.pl		
domena strefy	Informacje o strefie domenowej	SOA	3600
brzozowa5.edu.pl	primary name server = ns1.kei.pl responsible mail addr = admin.kei.pl serial = 2020022000 refresh = 10800 (3 hours) retry = 2100 (35 mins) expire = 604800 (7 days) default TTL = 86400 (1 day) brzozowa5.edu.pl nameserver = ns1.kei.pl brzozowa5.edu.pl nameserver = ns2.kei.pl		
Kanoniczna nazwa serwera	IPv6	AAAA	
youtube-ui.l.google.com	2a00:1450:401b:806::200e		
IPv4	Domena powiązana z IPv4	PTR	
128.232.132.8	132.232.128.in-addr.arpa domain name (DNAME) = 132.232.128.in-addr.arpa.cam.ac.uk 8.132.232.128.in-addr.arpa canonical name = 8.132.232.128.in-addr.arpa.cam.ac.uk 8.132.232.128.in-addr.arpa.cam.ac.uk name = tm-128-232-132-8.tm.uis.cam.ac.uk		
IPv6	Domena powiązana z IPv6	PTR	
2001:630:212:8::d:a0	0.a.0.0.d.0.0.0.0.0.0.0.0.0.0.8.0.0.0.2.1.2.0.0.3.6.0.1.0.0.2.ip6.arpa a name = auth0.dns.cam.ac.uk		

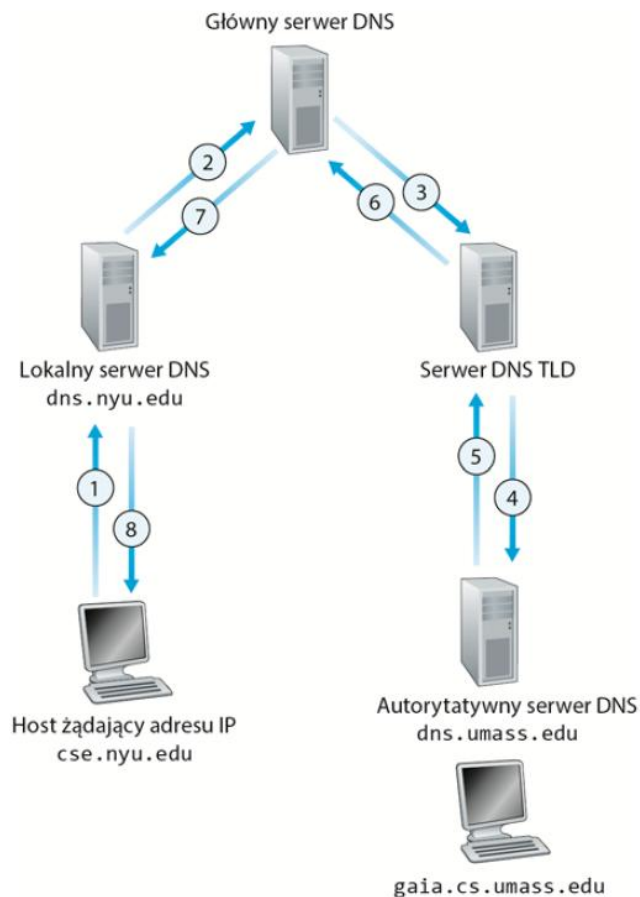
1.2.13 ODPOWIEDŹ 13: Czym się różnią rekurencyjne zapytania od iteracyjnych zapytań DNS?



Rysunek 2.19. Współpraca różnych serwerów DNS

Iteracyjne zapytania DNS charakteryzują się tym, że:

- wszystkie odpowiedzi na zapytania są zwracane na ten sam serwer DNS najczęściej lokalny. Może to wyglądać tak, że w pierwszej kolejności lokalny serwer DNS wyśle zapytanie o adres nazwy hosta np. www.brzozowa5.edu.pl do głównego serwera DNS.
- Ten nie posiadając rekordu A mapowania nazwy www.brzozowa5.edu.pl z IP wyśle rekord A mapujący nazwę serwera TLD DNS .edu.pl z jego adresem IP.
- Lokalny serwer DNS ponownie wyśle zapytanie o adres IP hosta www.brzozowa5.edu.pl, tym razem do serwera TLD DNS. Ten jeśli nie posiada w swojej bazie danych mapowania domeny oczekiwanej domeny i IP prześle rekord A mapujący nazwę autorytatywnego serwera i jego IP powiązanego z domeną www.brzozowa5.edu.pl (rekord NS).
- Lokalny serwer znowu prześle zapytanie do autorytatywnego serwera .edu.pl i uzyska adres IP serwera naszej szkoły.
- Kiedy lokalny serwer uzyska odpowiednie rekordy, rekurencyjnie prześle je do klienta DNS uruchomionego w komputerze klienta (np. ucznia ZSZ PGNiG).

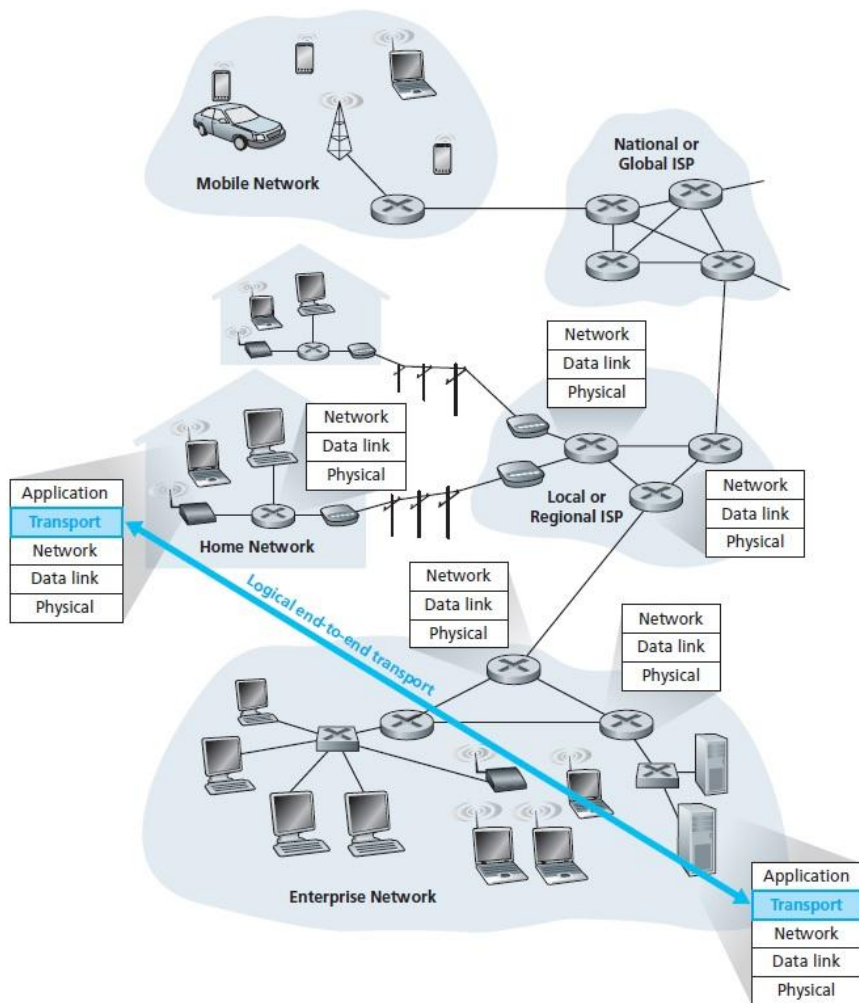


Rysunek 2.20. Rekurencyjne zapytania systemu DNS

Rekurencyjne zapytania DNS charakteryzują się tym, że:

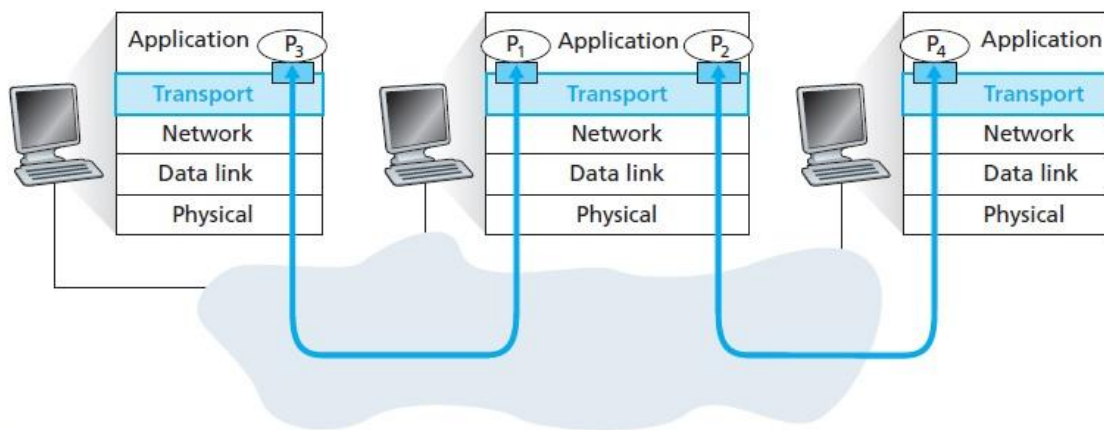
- klient DNS przesyła zapytanie o adres IP hosta np. www.brzozowa5.edu.pl do lokalnego serwera DNS. Ten może przestać zapytanie do głównego serwera DNS. Główny serwer z kolei prześle zapytanie w imieniu serwera lokalnego do serwera TLD powiązanego z domenami .edu.pl. Serwer TLD DNS jeśli nie posiada w tym momencie rekordu A mapującego nazwę www.brzozowa5.edu.pl z jego IP, to w imieniu serwera głównego prześle zapytanie o IP strony szkoły do autorytatywnego serwera powiązanego z domeną www.brzozowa5.edu.pl.
- W przypadku pozytywnej odpowiedzi ze strony autorytatywnego serwera .edu.pl, serwer TLD DNS przesyła ją do serwera głównego, a ten do serwera lokalnego, który powiązany jest z klienckim DNS inicjalizującym żądanie IP strony szkoły www.brzozowa5.edu.pl.

1.3 WARSTWA TRANSPORTOWA (THE TRANSPORT LAYER)



The transport layer provides logical rather than physical communication between application processes

1.3.1 ODPOWIEDŹ 1: Scharakteryzuj procesy multipleksowania i demultipleksowania

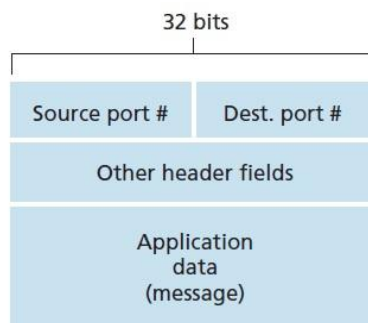


Key:

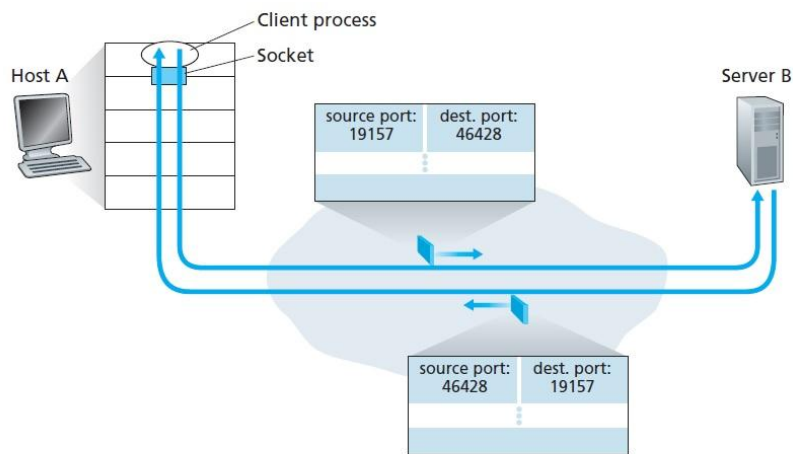
○ Process ■ Socket

Transport-layer multiplexing and demultiplexing

- Proces (jako składnik aplikacji sieciowej) może dysponować jednym lub kilkoma **gniazdami** (drzwiami), za pośrednictwem których dane są przesyłane między siecią i procesem.
- Warstwa transportowa hosta odbiorczego właściwie nie dostarcza danych bezpośrednio procesowi, lecz pośredniczemu gniazdu. Ponieważ w dowolnej chwili host odbiorczy może posiadać więcej niż jedno gniazdo każdemu zostanie przypisany unikatowy identyfikator (numer portu)
- Format identyfikatora zależy od tego czy gniazdo jest gniazdem protokołu TCP, czy UDP
- Aby każdy segment trafił do odpowiedniego gniazda, warstwa transportowa odbiorczego systemu końcowego sprawdza odpowiednie pole nagłówka segmentu (nr portu docelowego - ang. destination port number)



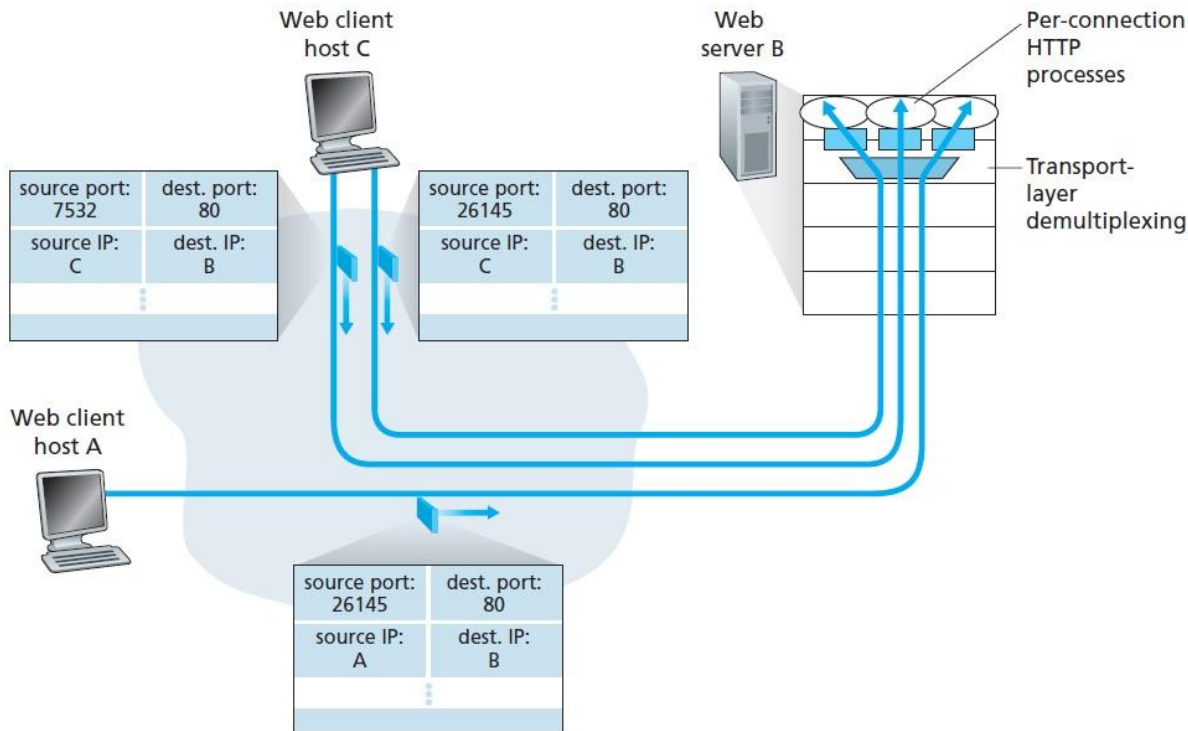
Source and destination port-number fields in a transport-layer segment



The inversion of source and destination port numbers

- Operacja polegająca na dostarczeniu danych znajdujących się w segmencie warstwy transportowej do właściwego gniazda jest nazywana **demultipleksowaniem**.
- Proces złożony z zebrania przez źródłowy host porcji danych od różnych gniazd, kapsułkowania każdej porcji danych wraz z dołączonym nagłówkiem (który jest potem wykorzystywany podczas demultipleksowania) w celu utworzenia segmentów i przekazania ich warstwie sieci jest określany mianem **multipleksowania**.

1.3.2 ODPOWIEDŹ 2: Jak wiele gniazd TCP może obsługiwać pojedynczy host serwera?



Two clients, using the same destination port number (80) to communicate with the same Web server application

- Host serwera może jednocześnie obsługiwać wiele gniazd TCP, z których każde jest powiązane z procesem.
- Ponadto każde gniazdo jest identyfikowane przez własne cztery wartości (źródłowy adres IP, docelowy adres IP i port docelowy) zostaną użyte do przekazania (zdemultipleksowania) segmentu do właściwego gniazda.
- (Analiza powyższego rysunku) Klient A i Klient C rozpoczynają sesje HTTP z hostem B (serwerem). Wszystkie hosty A,B,C mają unikatowe adresy IP oznaczone kolejno literami A,B,C. Host C przydziela swoim dwóm połączeniom HTTP różne numery portów źródłowych 7532 i 26145. Ponieważ host A określił numery portów źródłowych niezależnie od hosta C, własnemu połączeniu HTTP też może przypisać port źródłowy o numerze 26145. Serwer (host B) nadal będzie w stanie dokonać poprawnej demultipleksacji dwóch połączeń używających portu źródłowego o identycznym numerze. Wynika to stąd, że oba połączenia posiadają różne źródłowe adresy IP.

1.3.3 ODPOWIEDŹ 3: Wyjaśnij w oparciu o Serwer WWW i protokół TCP, że między gniazdami połączeń i procesami nie zawsze występuje relacja jeden do jednego

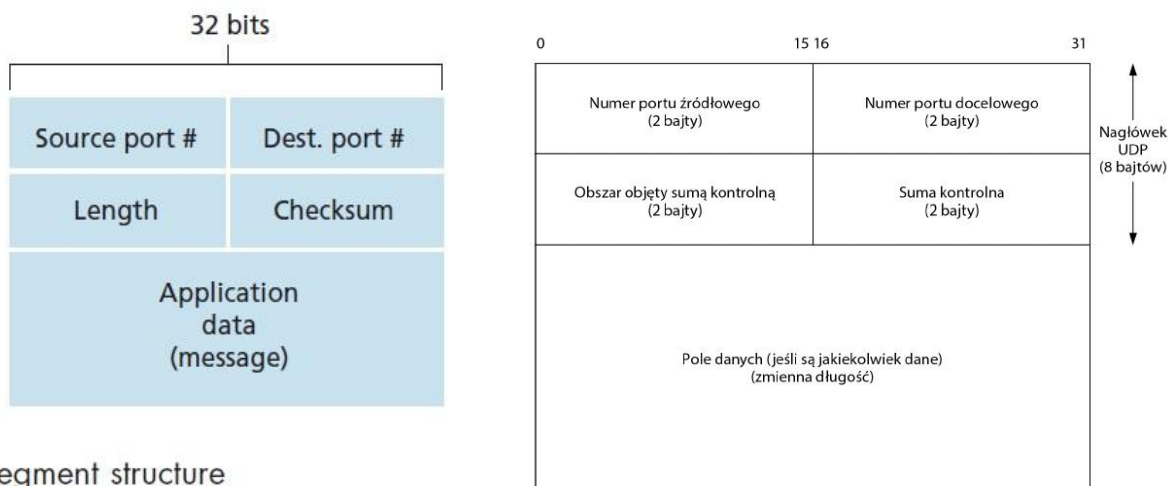
- Obecnie stosowane bardzo wydajne serwery WWW często korzystają tylko z jednego procesu, ale za to dla każdego nowego połączenia klienta tworzą nowy wątek i gniazdo połączenia (wątek można potraktować jak uproszczony proces podrzędny).
- W przypadku wielowątkowego serwera WWW w dowolnej chwili z tym samym procesem może być powiązanych wiele gniazd połączeń posiadających różne identyfikatory.
- Jeśli klient i serwer korzystają z trwałego połączenia HTTP, w czasie jego trwania będą wymieniały się komunikatami HTTP za pośrednictwem tego samego gniazda serwerowego.
- Jeśli jednak klient i serwer używają nietrwałego połączenia HTTP, dla każdego żądania i odpowiedzi zostanie utworzone nowe połączenie TCP, a następnie zostanie ono przerwane.

1.3.4 ODPOWIEDŹ 4: Scharakteryzuj protokół UDP

Protokół UDP

- ang User Datagram Protocol - protokół pakietów użytkownika
- jest uproszczonym protokołem transportowym oferującym ograniczony model usług
- jest protokołem protokołem bezpołączeniowym, co oznacza, że zanim dwa procesy rozpoczną komunikację, nie trzeba przeprowadzić procesu negocjowania.
- zapewnia usługę zawodnego transferu danych. Oznacza to, że po umieszczeniu przez proces komunikatu w gnieździe protokół UDP nie da żadnej gwarancji, że komunikat w ogóle dotrze do procesu odbiorczego.
- komunikaty mogą docierać do procesu odbiorczego w niewłaściwej kolejności.
- nie korzysta z mechanizmu kontroli przeciążenia, co powoduje, że proces nadawczy może przekazywać dane do niższej warstwy (warstwy sieciowej) z dowolną szybkością.
- jest wykorzystywany przez następujące protokoły warstwy aplikacji: SNMP (zarządzanie siecią), RIP (protokół routingu), DNS, NFS (zdalny serwer plików); z UDP korzystają także: telefonia internetowa (zwykle protokół zastrzeżony), strumieniowa transmisja danych multimedialnych (zwykle protokoły zastrzeżone)

1.3.5 ODPOWIEDŹ 5: Przedstaw jak wygląda struktura segmentu UDP



UDP segment structure

- **Port źródłowy.** Port, z którego są wysyłane dane.
- **Port docelowy.** Port, do którego są dostarczane dane.
- **Obszar objęty sumą kontrolną.** Wyrażona w bajtach wielkość pakietu.
- **Suma kontrolna.** Pole używane w celu zagwarantowania, że dostarczone dane i nagłówek UDP nie zostały zmodyfikowane podczas transmisji.

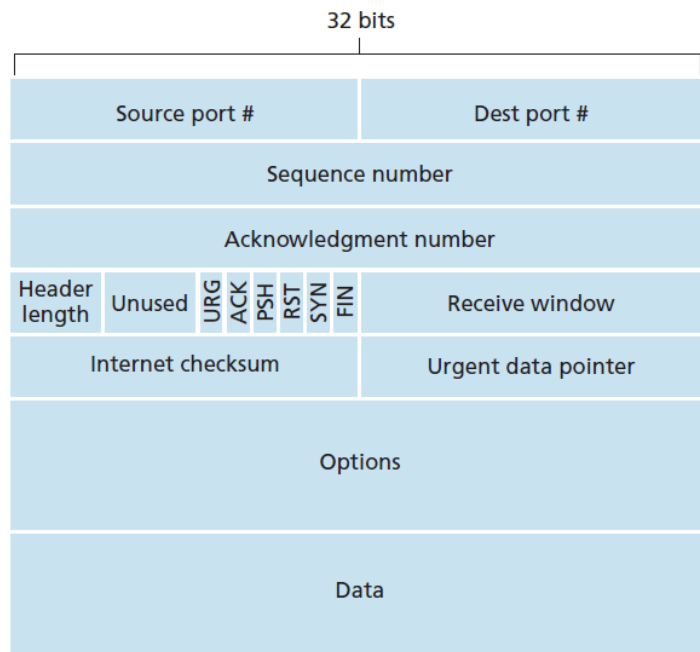
```
354 6.392620000 128.222.222.101 128.222.222.1 DNS 80 Standard query 0x6703 A www.brzozowa5.edu.pl
Frame 354: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
Ethernet II, Src: QuantaCo_57:33:67 (08:9e:01:57:33:67), Dst: Tp-LinkT_46:e1:a6 (f8:1a:67:46:e1:a6)
Internet Protocol Version 4, Src: 128.222.222.101 (128.222.222.101), Dst: 128.222.222.1 (128.222.222.1)
User Datagram Protocol, Src Port: 56362 (56362), Dst Port: 53 (53)
  Source Port: 56362 (56362)
  Destination Port: 53 (53)
  Length: 46
  Checksum: 0xefca [validation disabled]
    [Good checksum: False]
    [Bad checksum: False]
    [Stream index: 15]
  Domain Name System (query)
    [Response In: 362]
    Transaction ID: 0x6703
    Flags: 0x0100 Standard query
      0... .. = Response: Message is a query
      .000 0... .. = opcode: Standard query (0)
      ....0. .... = Truncated: Message is not truncated
      ....1. .... = Recursion desired: Do query recursively
      ....0.. .... = Z: reserved (0)
      ....0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    www.brzozowa5.edu.pl: type A, class IN

0000 f8 1a 67 46 e1 a6 08 9e 01 57 33 67 08 00 45 00 ..gF.... .w3g..E.
0010 00 42 21 67 00 00 80 11 5b 20 80 de de 65 80 de .B!g.... [ ...e..
0020 de 01 dc 2a 00 35 00 2e ef ca 67 03 01 00 00 01 ..*.5.. .g.....
0030 00 00 00 00 00 00 03 77 77 77 09 62 72 7a 6f 7a .....w ww.brzoz
0040 6f 77 61 35 03 65 64 75 02 70 6c 00 00 01 00 01 owa5.edu .pl.....
```

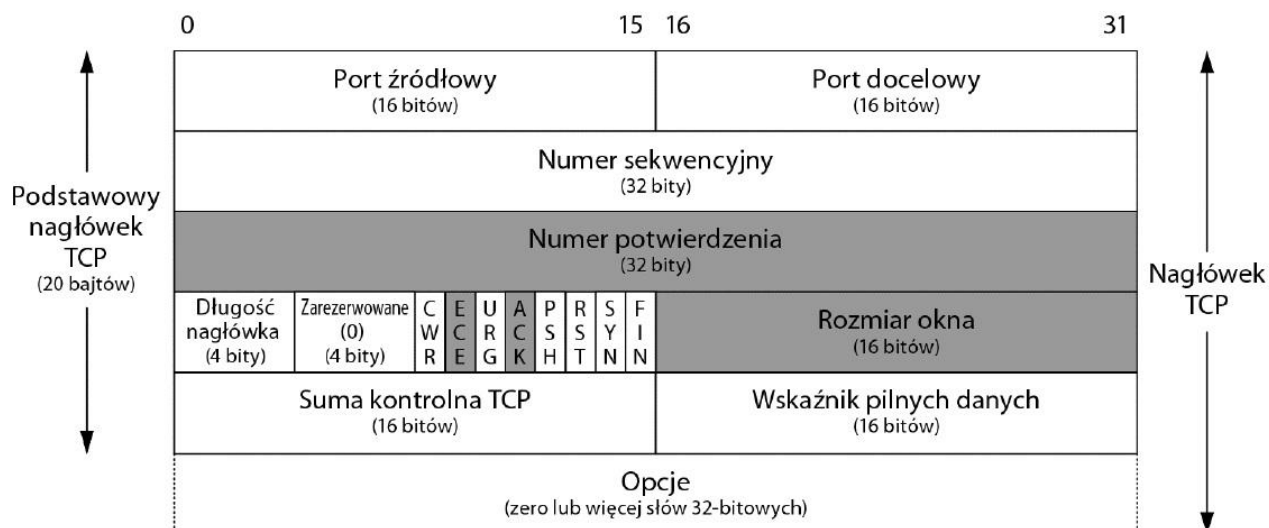
1.3.6 ODPOWIEDŹ 6: Scharakteryzuj protokół TCP

- TCP (Transmission Control Protocol) - Protokół Kontroli Transmisji
- protokół TCP jest protokołem warstwy transportowej modelu OSI i TCP/IP
- protokół TCP jest nazywany protokołem zorientowanym na połączenie, ponieważ zanim jeden proces aplikacji może zacząć wysyłać dane do drugiego, oba procesy muszą przeprowadzić między sobą proces negocjacji.
- połączenie TCP zapewnia usługę pełnego duplexu
- połączenie TCP jest zawsze połączeniem punkt - punkt, czyli między jednym nadawcą i jednym odbiorcą

1.3.7 ODPOWIEDŹ 7 : Przedstaw strukturę segmentu TCP



TCP segment structure



- **Numer portu źródłowego i docelowego** są wykorzystywane na potrzeby multipleksowania i demultipleksowania danych do lub z wyżej położonej warstwy aplikacji.

```

Transmission Control Protocol, Src Port: 49200, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 49200
  Destination Port: 80

```

- 32-bitowe **pole numeru sekwencyjnego** i 32-bitowe pole numeru potwierdzenia - są używane przez stronę nadawczą i odbiorczą protokołu TCP w celu zapewnienia usługi niezawodnego transferu danych

```

Sequence number: 0      (relative sequence number)
Acknowledgment number: 0

```

- 16 bitowe **pole okna odbiorczego** używanego na potrzeby kontroli przepływu. Wkrótce okaże się, że pole to określa liczbę bajtów, które przyjmie odbiorca.

```

Window size value: 8192
[Calculated window size: 8192]

```

- 4-bitowe **pole długości nagłówka** określa długość nagłówka segmentu TCP wyrażoną za pomocą 32-bitowych słów. Ze względu na pole opcji nagłówek może mieć zmienną długość (zwykle pole opcji jest puste, dlatego zazwyczaj nagłówek segmentu TCP ma długość wynoszącą 20 bajtów.
- **pole opcji** - opcjonalne - o zmiennej długości jest stosowane, gdy nadawca i odbiorca negocjują maksymalny rozmiar segmentu (parametr MSS). Za jego pomocą można skalować wielkość okna w przypadku sieci o dużej szybkości itd.

```

Options: (12 bytes), Maximum segment size, No-Operation (NOP),
  Maximum segment size: 1460 bytes
    Kind: Maximum Segment Size (2)
    Length: 4
    MSS Value: 1460
  No-Operation (NOP)
    Type: 1
    0... .... = Copy on fragmentation: No
    .00. .... = Class: Control (0)
    ...0 0001 = Number: No-Operation (NOP) (1)
  Window scale: 8 (multiply by 256)
    Kind: Window Scale (3)
    Length: 3
    Shift count: 8
    [Multiplier: 256]
  No-Operation (NOP)
    Type: 1
    0... .... = Copy on fragmentation: No
    .00. .... = Class: Control (0)
    ...0 0001 = Number: No-Operation (NOP) (1)
  No-Operation (NOP)
    Type: 1
    0... .... = Copy on fragmentation: No
    .00. .... = Class: Control (0)
    ...0 0001 = Number: No-Operation (NOP) (1)
  TCP SACK Permitted Option: True
    Kind: SACK Permitted (4)
    Length: 2

```

- pole znaczników (flagi):
 - CWR (Congestion Window Reduced) — nadawca zmniejszył swoją szybkość transmisji
 - ECE (ECN Echo) — nadawca otrzymał wcześniej powiadomienie o przeciążeniu
 - URG (*Urgent*) — *pole Wskaźnik pilnych danych jest istotne — rzadko używane*
 - ACK (Acknowledgement) — pole Numer potwierdzenia jest istotne — zawsze włączone po ustanowieniu połączenia
 - PSH (Push) — odbiorca powinien przekazać te dane aplikacji tak szybko, jak to możliwe — niezaimplementowane w niezawodny sposób i nieużywane
 - RST (Reset) — zresetowanie połączenia, zwykle z powodu błędu
 - SYN (Synchronize) — synchronizacja numerów sekwencyjnych w celu zainicjowania połączenia
 - FIN (Finished) — nadawca segmentu skończył wysyłanie danych do swojego odbiorcy;

```

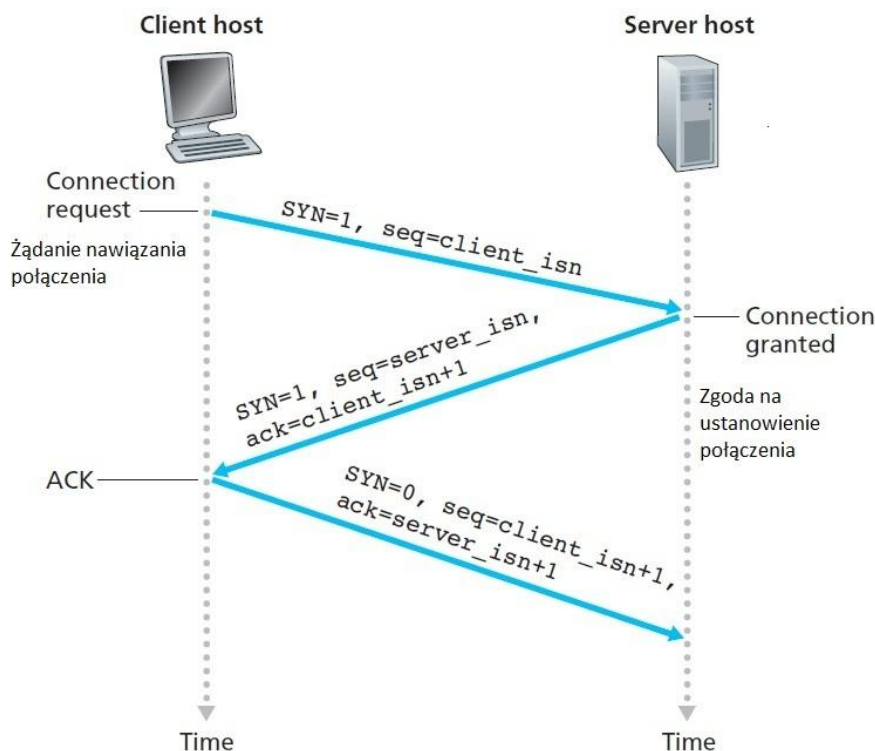
Flags: 0x002 (SYN)
 000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...0 = Acknowledgment: Not set
.... .... 0... = Push: Not set
.... .... .0.. = Reset: Not set
.... .... ..1. = Syn: Set
  [Expert Info (Chat/Sequence): Connection establish request (SYN): server port 80]
    [Connection establish request (SYN): server port 80]
    [Severity level: Chat]
    [Group: Sequence]
.... .... ...0 = Fin: Not set
[TCP Flags: .....S.]

```

- **pole sumy kontrolnej** TCP obejmuje nagłówek TCP i dane oraz niektóre pola z nagłówka IP; Suma kontrolna jest obowiązkowo obliczana i zapisywana przez nadawcę, a potem weryfikowana przez odbiorcę. Sumę kontrolną TCP obliczamy przy użyciu tego algorytmu, co sumy kontrolne używane w protokołach IP, ICMP i UDP.

1.3.8 ODPOWIEDŹ 8: Na czym polega 3 etapowy proces negocjacji protokołu TCP/IP?

- Proces negocjacji protokołu TCP polega na przesłaniu wstępnych segmentów wymaganych do ustalenia parametrów związanych z transferem danych, który ma nastąpić.
- Protokół TCP klienta wysyła protokołowi TCP po stronie serwera specjalny segment nazywany **SYN**. Segment SYN nie zawiera żadnych danych warstwy aplikacji, ma za to przypisany losowo numer sekwencyjny np SYN=1.
- Segment jest kapsułkowany w datagram IP i przesyłany do serwera.
- Serwer wyodrębnia segment SYN z datagramu IP, przydzieli bufor połączenia i zmienne protokołu TCP, a następnie prześle klientowi TCP segment zgody na ustanowienie połączenia zwany **SYNACK**.
- Po odebraniu segmentu SYNACK klient również przydziela połączeniu bufory i zmienne. Host klienta wysyła serwerowi kolejny segment zwany ACK. Ten ostatni segment potwierdza otrzymanie zgody na połączenie wysłanego przez serwer



TCP three-way handshake: segment exchange

3 etapowy proces negocjowania stosowany przez protokół TCP - wymiana segmentów

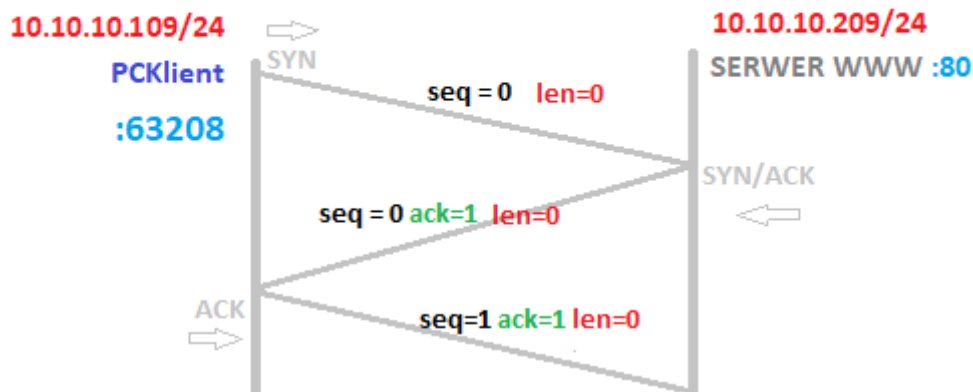


SERWER
10.10.10.209/24

PCKlient
10.10.10.109/24

19	6.313763	10.10.10.109	10.10.10.209	TCP	66	63208 → 80	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	WS=256	SACK_PERM
20	6.313884	10.10.10.109	10.10.10.209	DNS	69	Standard query 0xcc83 A www.local							
21	6.314068	10.10.10.209	10.10.10.109	TCP	66	80 → 63208	[SYN, ACK]	Seq=0	Ack=1	Win=65535	Len=0	MSS=1460	WS=256
22	6.314096	10.10.10.109	10.10.10.209	TCP	54	63208 → 80	[ACK]	Seq=1	Ack=1	Win=2102272	Len=0		

strona IIS serwera WIN2022



```

> Frame 19: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface
> Ethernet II, Src: ASUSTekCOMPU_10:2b:5f (e8:9c:25:10:2b:5f), Dst: ASUSTekCOMPU_
> Internet Protocol Version 4, Src: 10.10.10.109, Dst: 10.10.10.209
✓ Transmission Control Protocol, Src Port: 63208, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 63208
  Destination Port: 80
  [Stream index: 0]
  > [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 2402347716
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
✓ Flags: 0x002 (SYN)
  000. .... = Reserved: Not set
  ...0 .... = Accurate ECN: Not set
  .... 0... = Congestion Window Reduced: Not set
  .... .0.. = ECN-Echo: Not set
  .... ..0. = Urgent: Not set
  .... ...0 = Acknowledgment: Not set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
  > .... .... ..1. = Syn: Set
  .... .... ...0 = Fin: Not set
  [TCP Flags: .....S.]
  Window: 64240
  [Calculated window size: 64240]
  Checksum: 0x2978 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale,
  > [Timestamps]

```

```

> Frame 21: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on
> Ethernet II, Src: ASUSTekCOMPU_68:3e:af (f0:79:59:68:3e:af), Dst: ASUST
> Internet Protocol Version 4, Src: 10.10.10.209, Dst: 10.10.10.109
v Transmission Control Protocol, Src Port: 80, Dst Port: 63208, Seq: 0, A
  Source Port: 80
  Destination Port: 63208
  [Stream index: 0]
> [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 961314645
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 2402347717
  1000 .... = Header Length: 32 bytes (8)
v Flags: 0x012 (SYN, ACK)
  000. .... = Reserved: Not set
  ...0 .... = Accurate ECN: Not set
  .... 0... = Congestion Window Reduced: Not set
  .... .0.. = ECN-Echo: Not set
  .... ..0. = Urgent: Not set
  .... ...1 .... = Acknowledgment: Set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
> .... .... ..1. = Syn: Set
  .... .... ...0 = Fin: Not set
  [TCP Flags: .....A..S.]
Window: 65535
[Calculated window size: 65535]
Checksum: 0x1bde [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window
> [Timestamps]

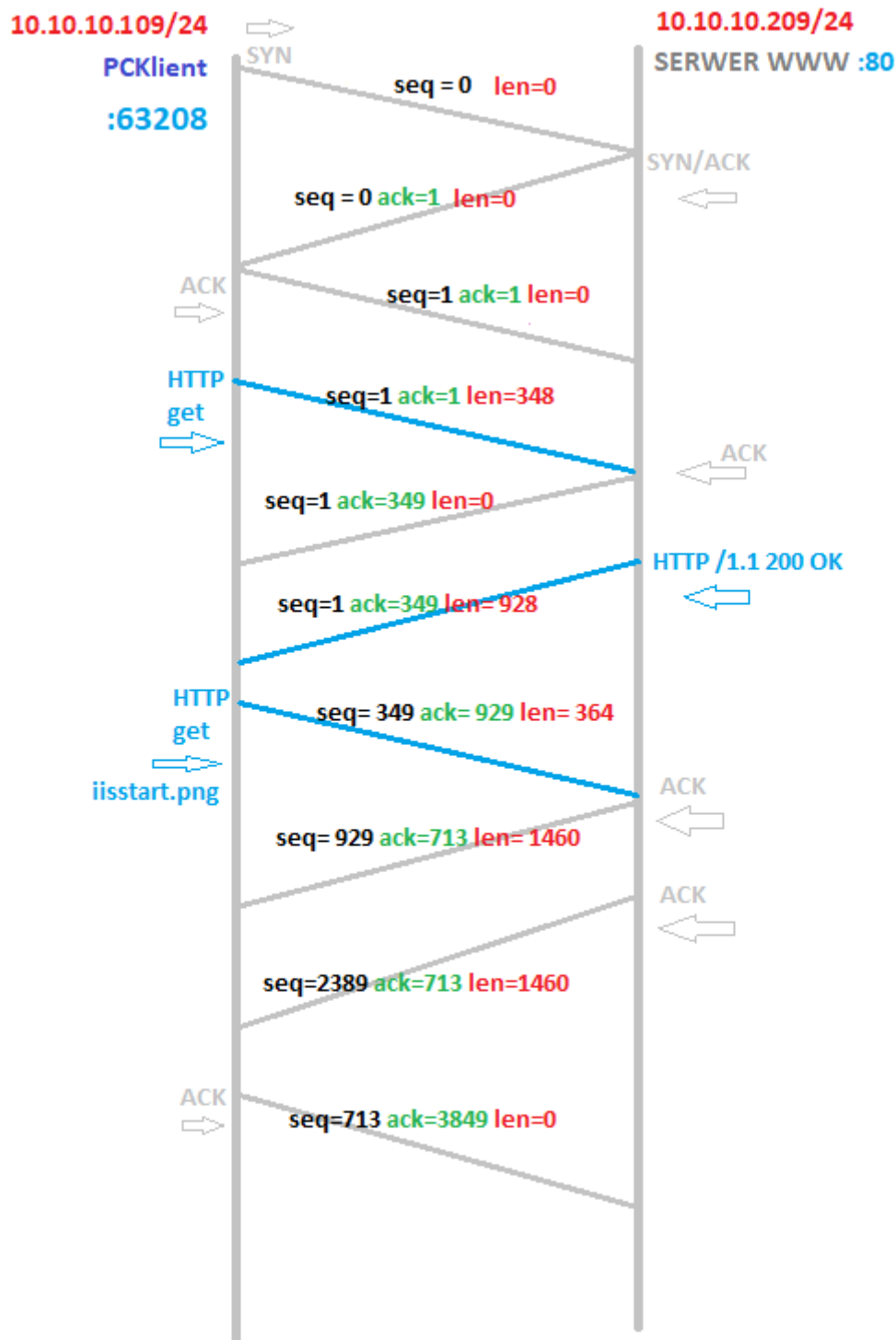
```

```

> Frame 22: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
> Ethernet II, Src: ASUSTekCOMPU 10:2b:5f (e8:9c:25:10:2b:5f), Dst: A
> Internet Protocol Version 4, Src: 10.10.10.109, Dst: 10.10.10.209
v Transmission Control Protocol, Src Port: 63208, Dst Port: 80, Seq:
  Source Port: 63208
  Destination Port: 80
  [Stream index: 0]
> [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 2402347717
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 961314646
  0101 .... = Header Length: 20 bytes (5)
v Flags: 0x010 (ACK)
  000. .... = Reserved: Not set
  ...0 .... = Accurate ECN: Not set
  .... 0... = Congestion Window Reduced: Not set
  .... .0.. = ECN-Echo: Not set
  .... ..0. = Urgent: Not set
  .... ...1 = Acknowledgment: Set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
  .... .... ..0. = Syn: Not set
  .... .... ...0 = Fin: Not set
  [TCP Flags: .....A....]
Window: 8212
[Calculated window size: 2102272]
[Window size scaling factor: 256]
Checksum: 0x296c [unverified]
[Checksum Status: Unverified]

```

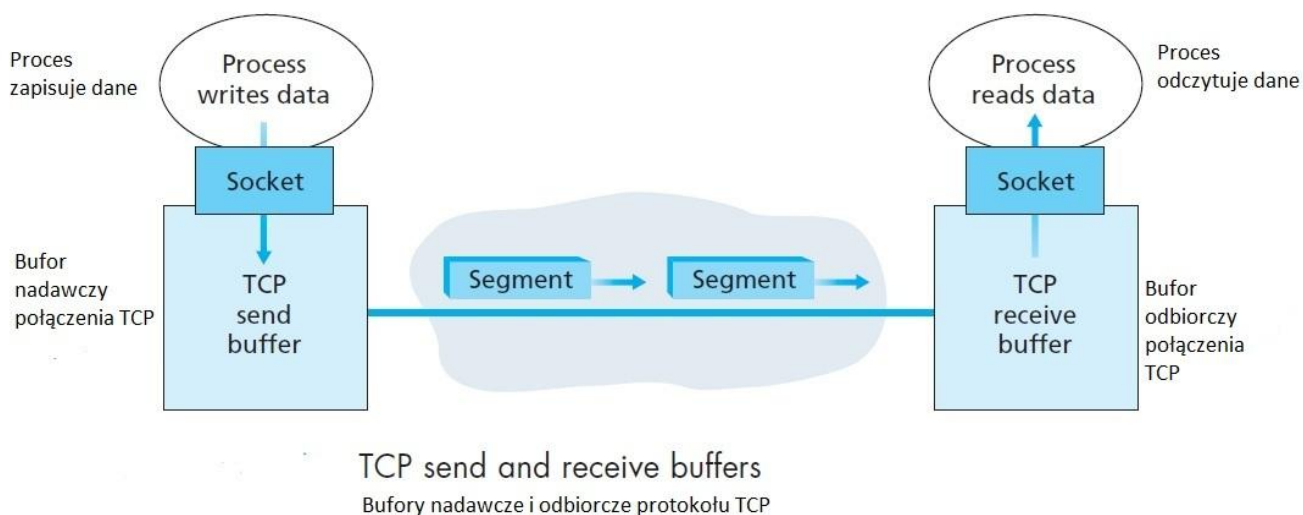
strona IIS sewera WIN2022



6.313763	10.10.10.109	10.10.10.209	TCP	66 63208 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_	
6.313884	10.10.10.109	10.10.10.209	DNS	69 Standard query 0xcc83 A www.local	
6.314068	10.10.10.209	10.10.10.109	TCP	66 80 → 63208 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 W	
6.314096	10.10.10.109	10.10.10.209	TCP	54 63208 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0	
6.314197	10.10.10.109	10.10.10.209	HTTP	402 GET / HTTP/1.1	
6.314515	10.10.10.209	10.10.10.109	DNS	85 Standard query response 0xcc83 A www.local A 10.10.10.209	
6.314768	10.10.10.109	10.10.10.209	DNS	69 Standard query 0xa0d AAAA www.local	
6.315163	10.10.10.209	10.10.10.109	DNS	121 Standard query response 0xa0d AAAA www.local SOA serwer	
6.324482	10.10.10.209	10.10.10.109	TCP	60 80 → 63208 [ACK] Seq=1 Ack=349 Win=2097664 Len=0	
6.427061	10.10.10.209	10.10.10.109	HTTP	982 HTTP/1.1 200 OK (text/html)	
6.447824	10.10.10.109	10.10.10.209	DNS	90 Standard query 0x23e0 A incoming.telemetry.mozilla.org	
6.449373	10.10.10.109	10.10.10.209	HTTP	418 GET /iisstart.png HTTP/1.1	
6.457507	10.10.10.209	10.10.10.109	TCP	1514 80 → 63208 [ACK] Seq=929 Ack=713 Win=2097152 Len=1460	TCP s
6.457509	10.10.10.209	10.10.10.109	TCP	1514 80 → 63208 [ACK] Seq=2389 Ack=713 Win=2097152 Len=1460	[TCP
6.457594	10.10.10.109	10.10.10.209	TCP	54 63208 → 80 [ACK] Seq=713 Ack=3849 Win=2102272 Len=0	

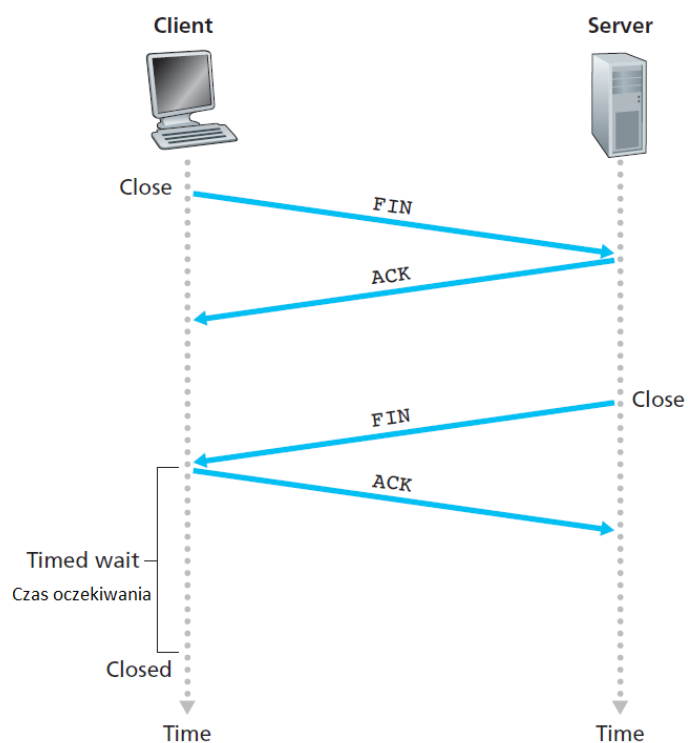
1.3.9 ODPOWIEDŹ 9: Jak przebiega komunikacja na poziomie warstwy transportowej - przykładowo między klientem i serwerem - po ustanowieniu połączenia TCP?

- po ustanowieniu połączenia TCP dwa procesy aplikacji mogą wysyłać do siebie dane.
- proces klienta przekazuje strumień danych za pośrednictwem gniazda (drzwi).
- gdy dane przejdą przez gniazdo, zajmie się nimi protokół TCP klienta, kierując dane do **bufora nadawczego** połączenia, będącego jednym z buforów definiowanych podczas 3 etapowego procesu negocjacji.
- od czasu do czasu protokół TCP pobierze porcję danych znajdujących się w buforze nadawczym.
- maksymalna ilość danych, które mogą zostać pobrane z bufora i umieszczone w segmencie, jest ograniczona przez **maksymalny rozmiar segmentu** (ang. Maximum Segment Size - MSS).
- MSS uściślając określa maksymalną liczbę bajtów danych w segmencie, nie licząc rozmiaru nagłówka segmentu
- każdą porcję danych klienta protokół TCP łączy z nagłówkiem tworząc segmenty TCP
- segmenty są przekazywane warstwie sieciowej, która kapsułkuje je w datagramach IP.
- po odebraniu segmentu przez host docelowy, ten umieszcza dane w buforze odbiorczym protokołu TCP
- na koniec aplikacja pobiera strumień danych zlokalizowanych w buforze



1.3.10 ODPOWIEDŹ 10: Opisz jak przebiega proces kończenia połączenia protokołu TCP

- proces aplikacji klienta generuje polecenie zakończenia połączenia
- klient TCP wysyła do procesu serwera specjalny segment TCP zwany **FIN**
- gdy serwer otrzyma segment, odeśle klientowi potwierdzenie dostarczenia.
- w dalszej kolejności serwer wyśle własny segment przerwania połączenia **FIN**
- na końcu klient potwierdzi otrzymanie tego segmentu



1.3.10.10 Closing a TCP connection
Kończenie połączenia TCP

```

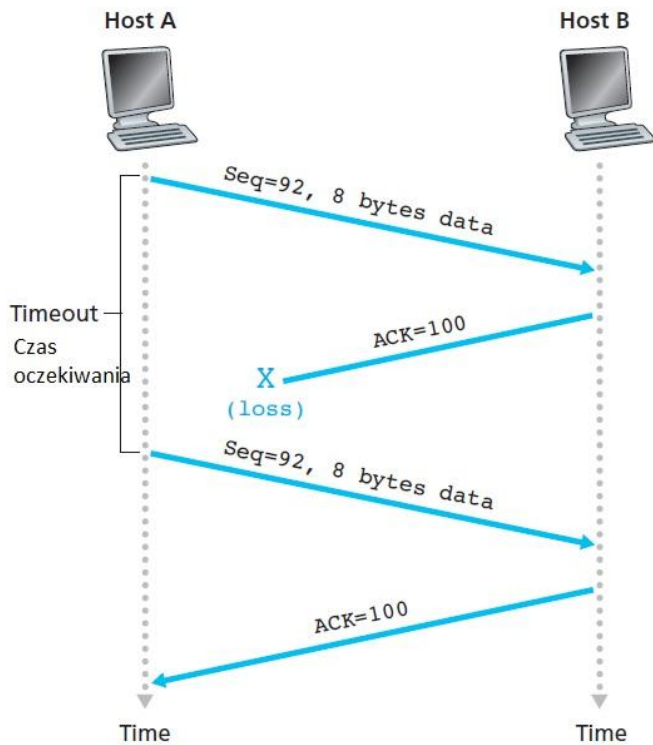
+ Frame 888: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
+ Ethernet II, Src: Tp-LinkT_0c:14:0f (ec:08:6b:0c:14:0f), Dst: Tp-LinkT_90:b5:ac (ec:08:6b:90:b5:ac)
+ Internet Protocol Version 4, Src: 222.222.222.2, Dst: 46.134.193.59
- Transmission Control Protocol, Src Port: 49174, Dst Port: 443, Seq: 466, Ack: 4638, Len: 0
  Source Port: 49174
  Destination Port: 443
  [Stream index: 8]
  [TCP Segment Len: 0]
  Sequence number: 466 (relative sequence number)
  Acknowledgment number: 4638 (relative ack number)
  Header Length: 20 bytes
- Flags: 0x011 (FIN, ACK)
  000. .... = Reserved: Not set
  ...0 .... = Nonce: Not set
  .... 0... = Congestion Window Reduced (CWR): Not set
  .... .0.. = ECN-Echo: Not set
  .... ..0. = Urgent: Not set
  .... ...1 = Acknowledgment: Set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
  .... .... ..0. = Syn: Not set
  .... .... ...1 = Fin: Set
  + [Expert Info (Chat/Sequence): Connection finish (FIN)]
  [TCP Flags: .....A...F]
  Window size value: 257
  [Calculated window size: 65792]
  [Window size scaling factor: 256]
  Checksum: 0x7290 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0

+ Frame 923: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
+ Ethernet II, Src: Tp-LinkT_90:b5:ac (ec:08:6b:90:b5:ac), Dst: Tp-LinkT_0c:14:0f (ec:08:6b:0c:14:0f)
+ Internet Protocol Version 4, Src: 46.134.193.88, Dst: 222.222.222.2
- Transmission Control Protocol, Src Port: 443, Dst Port: 49168, Seq: 4638, Ack: 471, Len: 0
  Source Port: 443
  Destination Port: 49168
  [Stream index: 2]
  [TCP Segment Len: 0]
  Sequence number: 4638 (relative sequence number)
  Acknowledgment number: 471 (relative ack number)
  Header Length: 20 bytes
- Flags: 0x011 (FIN, ACK)
  000. .... = Reserved: Not set
  ...0 .... = Nonce: Not set
  .... 0... = Congestion Window Reduced (CWR): Not set
  .... .0.. = ECN-Echo: Not set
  .... ..0. = Urgent: Not set
  .... ...1 = Acknowledgment: Set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
  .... .... ..0. = Syn: Not set
  .... .... ...1 = Fin: Set
  + [Expert Info (Chat/Sequence): Connection finish (FIN)]
  [TCP Flags: .....A...F]
  Window size value: 245
  [Calculated window size: 31360]
  [Window size scaling factor: 128]
  Checksum: 0xc897 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
+ [SEQ/ACK analysis]

```

1.3.11 ODPOWIEDŹ 11: Na czym polega retransmisja TCP spowodowana zgubieniem potwierdzenia ACK?

- Przykładowo host A wysyła do hosta B jeden segment z wymyślonym numerem sekwencyjnym 92 i z 8 bajtami danych.
- Po wysłaniu segmentu Seq=92 host A czeka na segment potwierdzenia z numerem 100 (ACK=100), odesłany przez host B.
- Host B otrzymuje segment Seq=92 wysłany przez host A i odsyła segment potwierdzenia ACK=100, który jednak ginie gdzieś w sieci
- W tym przypadku wystąpi zdarzenie upływu czasu oczekiwania i host A dokona retransmisji tego samego segmentu.
- Gdy host B ponownie otrzyma segment, na podstawie jego numeru sekwencyjnego stwierdzi, że w segmencie znajdują się dane, które już odebrał.
- Protokół hosta B odrzuci bajty jeszcze raz przesłanego segmentu Seq=92 i ponownie wyśle do hosta A segment potwierdzenia ACK=100, który wcześniej w sieci przepadł.

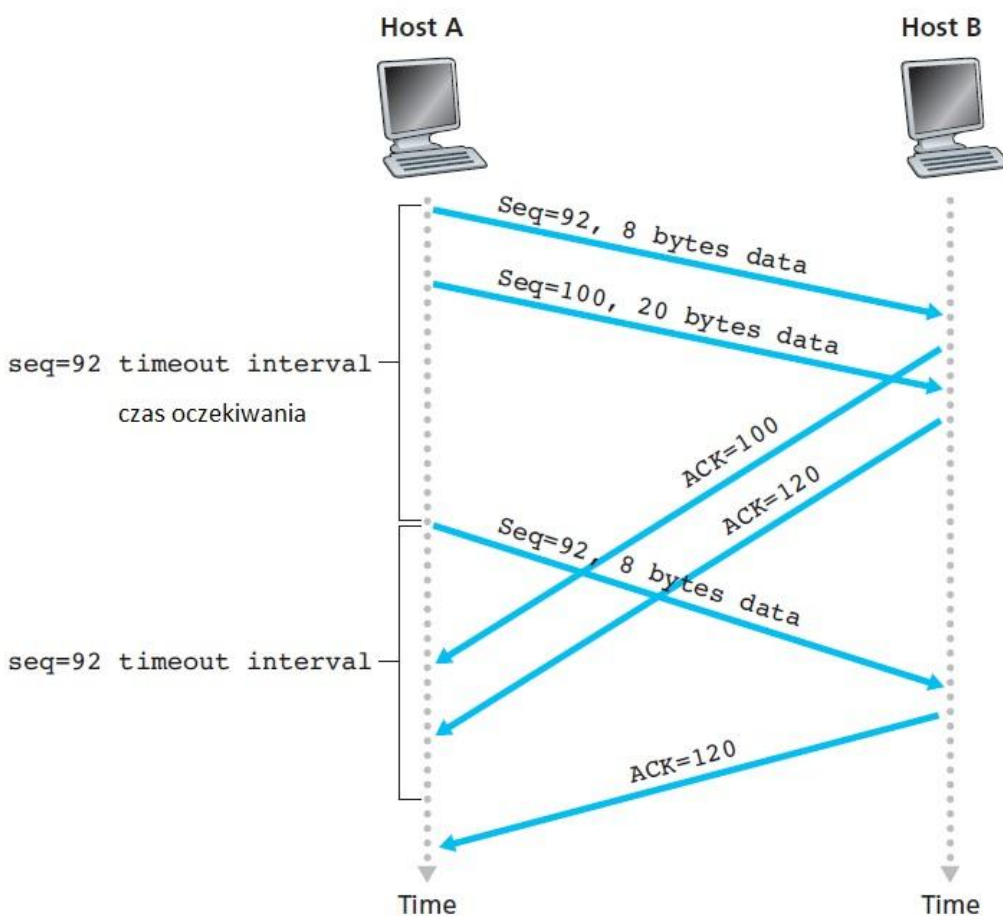


Retransmission due to a lost acknowledgment

Retransmisja spowodowana zgubieniem potwierdzenia

1.3.12 ODPOWIEDŹ 12: Na czym polega retransmisja TCP spowodowana upłynięciem czasu oczekiwania?

- Przykładowo host A wysyła dwa segmenty. Pierwszy posiada numer sekwencyjny Seq=92 i 8 bajtów danych, natomiast drugi segment na numer Seq=100 i 20 bajtów danych.
- Załóżmy, że oba segmenty nienaruszone docierają do hosta B, który dla każdego z nich odsyła niezależne potwierdzenie. Pierwsze potwierdzenie ma numer ACK=100, natomiast drugie numer ACK=120
- Z jakiegoś tam powodu potwierdzenia ACK=100 i potwierdzenia ACK=120 nie docierają do hosta A przed upływem czasu oczekiwania.
- Gdy czas oczekiwania dla hosta A upłynął ten dokonuje retransmisji pierwszego segmentu z numerem Seq=92 i ponownie uruchamia zegar czasu oczekiwania na potwierdzenie.
- Jeśli potwierdzenie ACK dla drugiego segmentu Seq=100 pojawi się przed rozpoczęciem odmierzania nowego czasu oczekiwania, segment ten nie będzie ponownie retransmitowany
- Host B po odbiorze zdublowanego segmentu Seq=92 wyśle potwierdzenie ACK z numerem ACK=120, a nie ACK=100 jak za pierwszym razem, ponieważ wszystkie segmenty Seq=92 i Seq=100 zostały już wcześniej przez niego odebrane. Skoro został już odebrany Seq=100 nie ma sensu potwierdzać odebrania segmentu Seq=92. Segment ACK=100 nie zostaje ponownie wysłany przez hosta B

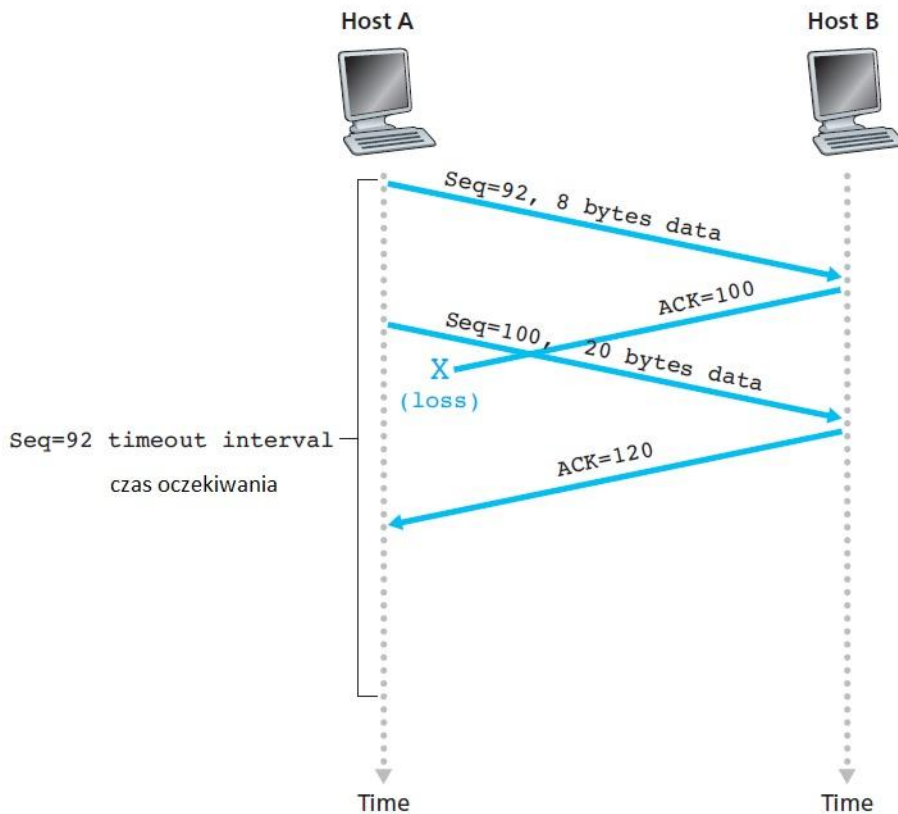


Segment 100 not retransmitted

Segment Seq=100 nie jest retransmitowany

1.3.13 ODPOWIEDŹ 13: Na czym polega zjawisko w sieci: skumulowane potwierdzenia segmentów TCP?

- Kumulowanie potwierdzenia ACK TCP pozwala uniknąć niepotrzebną retransmisję segmentów Seq=[nr] .
- Załóżmy, że host A wysyła dwa segmenty z numerami sekwencyjnymi w kolejności Seq=91 (8 bajtów danych) i Seq=100 (20 bajtów danych).
- Potwierdzenie pierwszego segmentu ACK=100 jest gubione w sieci. Jednak jeszcze przed wystąpieniem zdarzenia upływu czasu oczekiwania host A otrzymuje potwierdzenie z numerem ACK=120.
- Dzięki temu host A "wie", że host B odebrał wszystkie bajty aż do bajta z numerem 119.
- W związku z tym host A nie wysyła ponownie żadnego z tych dwóch segmentów (Seq=92 i Seq=100).

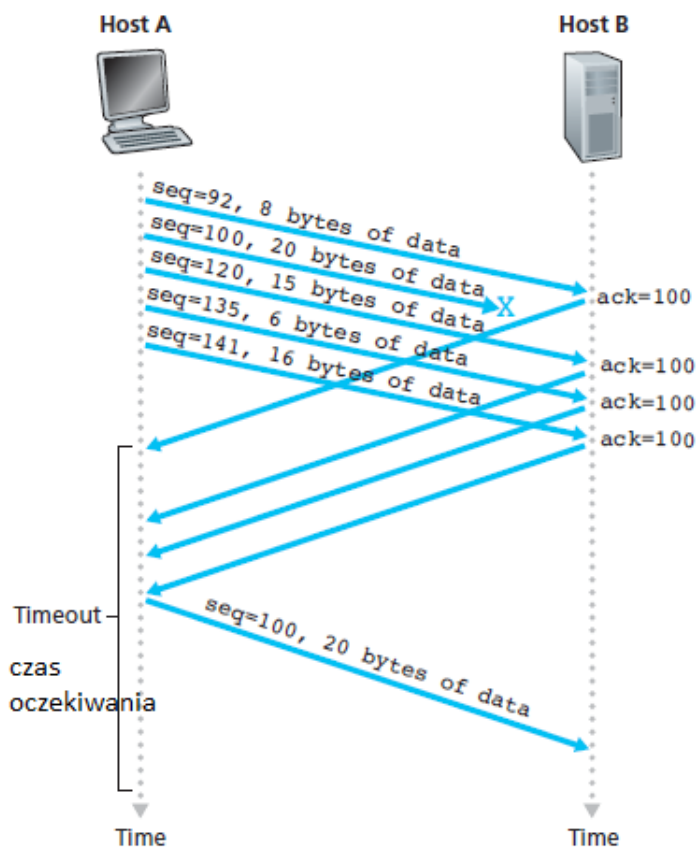


A cumulative acknowledgment avoids retransmission of the first segment

Skumulowane potwierdzenie pozwala uniknąć retransmisji pierwszego segmentu Seq=92

1.3.14 ODPOWIEDŹ 14: Na czym polega szybka retransmisja segmentów TCP?

- Jednym z problemów związanych z retransmisjami sterowanymi przez czas oczekiwania jest to, że okres oczekiwania może być stosunkowo długi.
- Gdy przepadnie segment, długi okres oczekiwania zmusza nadawcę do opóźnienia ponownego przesłania segmentu. W efekcie wzrasta opóźnienie łączne.
- Na szczęście nadawca może często stwierdzić fakt utraty segmentu na długo przed upływem czasu oczekiwania. Polega to wykryciu tak zwanych zduplikowanych potwierdzeń ACK.
- **Zduplikowane potwierdzenie ACK** jeszcze raz potwierdza odebranie segmentu, dla którego nadawca otrzymał już potwierdzenie.
- Gdy odbiorca otrzyma segment z numerem sekwencyjnym większym od numeru następnego oczekiwanego segmentu (zgodnie z kolejnością wysłania), stwierdzi fakt wystąpienia luki w strumieniu danych. Oznacza to brak segmentu.
- Luka może być wynikiem zgubienia segmentów w sieci lub zmiany ich kolejności
- Ponieważ protokół TCP nie stosuje negatywnych potwierdzeń, odbiorca nie może go odesłać nadawcy. Zamiast tego odbiorca po prostu ponownie potwierdza (generuje duplikat potwierdzenia ACK) otrzymanie ostatniego bajta danych zgodnie z kolejnością wysłania
- Jeżeli nadawca TCP dla tych samych danych otrzyma trzy zduplikowane potwierdzenia ACK, uzna, że został zgubiony segment wysłany po segmencie, który trzykrotnie potwierdzono
- W przypadku gdy odebrano trzy zduplikowane potwierdzenia ACK, nadawca protokołu TCP przeprowadzi **szybką retransmisję**



Fast retransmit: retransmitting the missing segment before the segment's timer expires

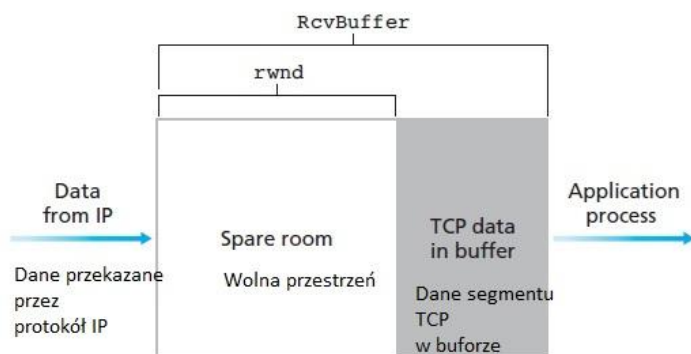
Szybka retransmisja - ponowne przesłanie zabudowanego segm.

1.3.15 ODPOWIEDŹ 15: Jakie mogą być przyczyny przepełnienia bufora TCP?

- Hosty znajdujące się z obu stron połączenia TCP definiują dla niego bufor odbiorczy.
- Gdy połączenie TCP odbierze bajty, które są poprawne i zachowują kolejność wysłania, umieści je w buforze odbiorczym.
- Odpowiedni proces aplikacji wczyta dane z tego bufora. W rzeczywistości aplikacja może być zajęta realizowaniem innego zadania, a nawet może nie próbować odczytać danych długo po ich odebraniu.
- Jeśli aplikacja dość wolno wczytuje dane, nadawca może bardzo łatwo zapewnić bufor odbiorczy połączenia przez wysłanie zbyt wielu danych w krótkim czasie.
- W celu wyeliminowania możliwości przepełnienia przez nadawcę bufora odbiorczego protokołu TCP zapewnia swoim aplikacjom **usługę kontroli przepływu**. Wynika z tego, że jest to usługa zajmująca się dostosowaniem szybkości, z jaką nadawca wysyła dane, do szybkości, z jaką aplikacja je wczytuje.

1.3.16 ODPOWIEDŹ 16: W jaki sposób protokół TCP zapewnia kontrolę przepływu segmentów

- Protokół TCP zapewnia kontrolę przepływu przez nadanie nadawcy utrzymania zmiennej nazywanej oknem odbiorczym. Okno odbiorcze umożliwia nadawcy zorientowanie się, jaka część bufora po stronie odbiorcy jest wolna.
- Ponieważ protokół TCP oferuje pełny duplex, nadawca po każdej stronie połączenia utrzymuje inne okno odbiorcze.
- Załóżmy, że za pośrednictwem połączenia TCP host A przesyła duży plik do hosta B. Host B przydziela połączeniu bufor odbiorczy o pojemności wyrażonej przez `RcvBuffer`. Od czasu do czasu proces aplikacji hosta B odczytuje bufor
- Okno odbiorcze oznaczone jako `rwnd` zawiera informacje o wolnej przestrzeni bufora.
- Ponieważ wolna przestrzeń bufora zmienia się z upływem czasu, wielkość okna `rwnd` jest dynamiczna.
- Kontrola przepływu polega na tym, że host B informuje host A o ilości wolnej przestrzeni w buforze połączenia.
- Jeśli dojdzie do przeciążenia w buforze hosta B ten opróżnia go i zajdzie konieczność retransmisji usuniętych segmentów.

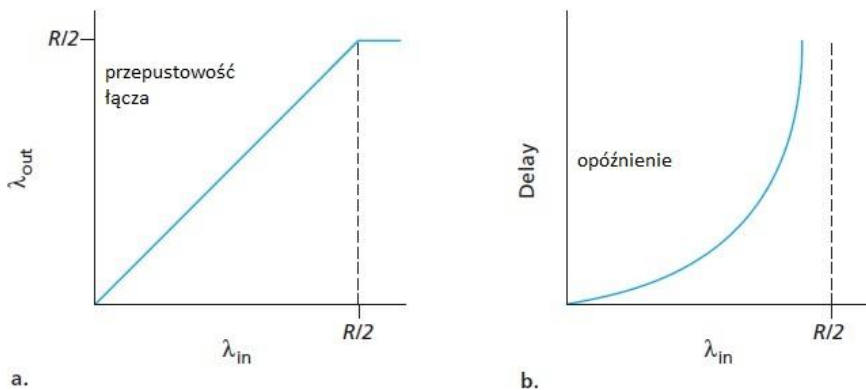


The receive window (`rwnd`) and the receive buffer (`RcvBuffer`)

Okno odbiorcze (`rwnd`) i bufor odbiorczy (`RcvBuffer`)

1.3.17 ODPOWIEDŹ 17: Jakie mogą być przyczyny przeciążenia w sieci?

- Jeśli łącze jest dzielone przez N hostów, przepustowość tego łącza dla każdego hosta wynosi R/N (R – przepustowość łącza). Im więcej hostów w sieci tym mniejszy limit przepustowości przypada na każdy z nich.
- Szybkość wysyłania danych nie może przekroczyć R/N .
- Jeśli szybkość wysyłania danych zbliża się do maksymalnych możliwości łącza, średnie opóźnienie staje się coraz większe
- Wzrost opóźnienia w sieci może wymusić konieczność retransmisji segmentów. Retransmitowane segmenty zajmują część przepustowości łącza co powoduje wydłużenie czasu przesłania wszystkich żądanych danych.
- Im większa liczba urządzeń w sieci, tym większa szansa, że pakiet zostanie odrzucony (np. w wyniku przepełnienia bufora wejściowego rutera) na dowolnym etapie podróży segmentu.



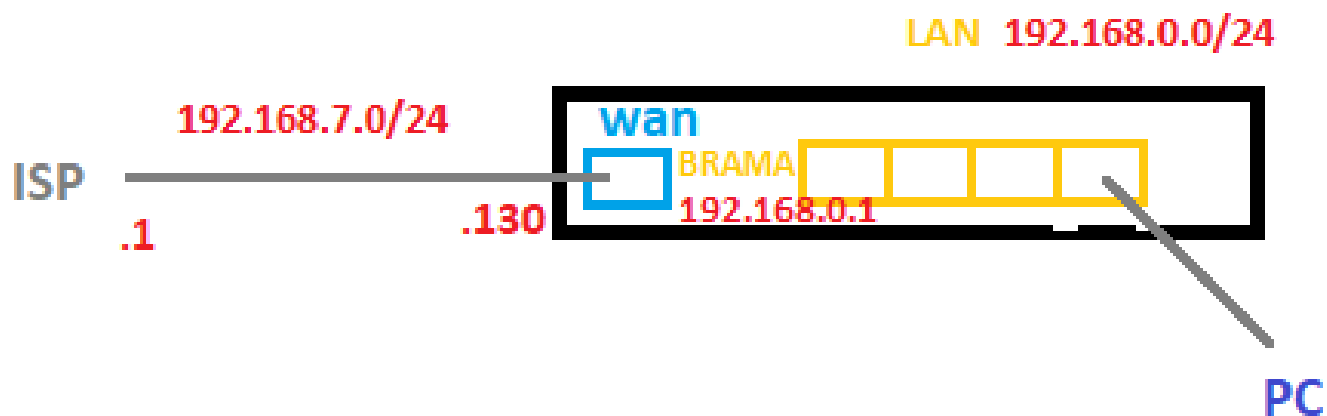
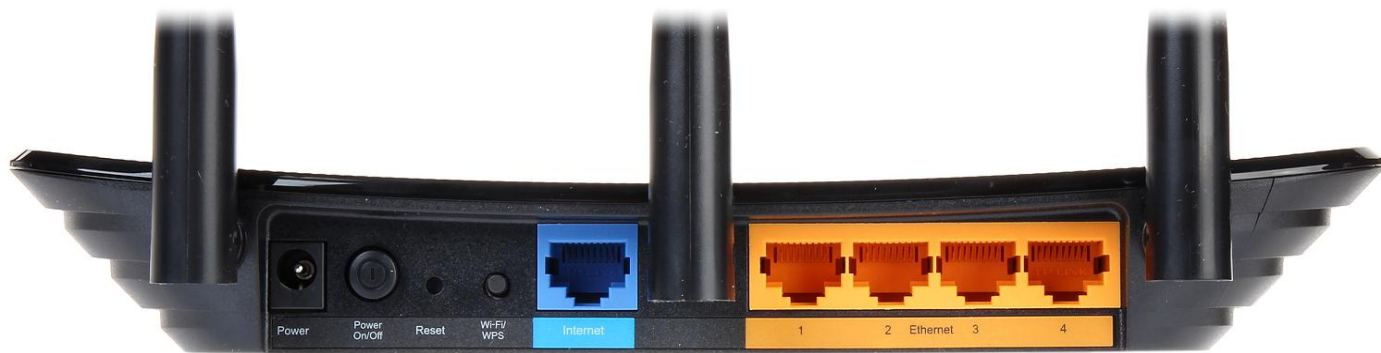
Congestion scenario 1: Throughput and delay as a function of host sending rate

W wariancie dla dwóch hostów lewy wykres pokazuje dzielenie przepustowości łącza, drugi wzrost opóźnienia.

1.4 WARSTWA SIECI

1.4.1 ODPOWIEDŹ 0: Aspekt danych i aspekt sterowania

Router TL-940dn



450M Wireless N Router

Model No. TL-WR940N

LAN

MAC Address:

D8-0D-17-FF-11-E2

IP Address:

192.168.0.1

Subnet Mask:

255.255.255.0 ▾

Save

450M Wireless N Router

Model No. TL-WR940N

WAN

WAN Connection Type:

Dynamic IP ▾

Detect

IP Address:

192.168.7.130

Subnet Mask:

255.255.255.0

Default Gateway:

192.168.7.1

Renew

Release

MTU Size (in bytes):

1500

(The default is 1500, do not change)

☒ Use These DNS Servers

Primary DNS:

8.8.8.8

Secondary DNS:

8.8.4.4

(Optional)

Tabela routingu



450M Wireless N Router

Model No. TL-WR940N

- Status
- Quick Setup
- WPS
- Working Mode
- Network
- Wireless
- Guest Network
- DHCP
- Forwarding
- Security
- Parental Control
- Access Control
- Advanced Routing
 - Static Routing List
 - System Routing Table

System Routing Table

ID	Destination Network	Subnet Mask	Gateway	Interface
1	192.168.7.0	255.255.255.0	0.0.0.0	WAN
2	192.168.0.0	255.255.255.0	0.0.0.0	LAN & WLAN
3	239.0.0.0	255.0.0.0	0.0.0.0	LAN & WLAN
4	0.0.0.0	0.0.0.0	192.168.7.1	WAN

Refresh

**dostęp do Internetu**

CISCO RV34W-router35f0B2





☐	VLAN ID ↕	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask	IPv6 Address/Prefix Length
☐	1	VLAN1	☒	☒ ⓘ	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.11-192.168.1.100	fec0:1::1/64 DHCP Disabled
☐	2	VLAN2	☒	☐ ⓘ	192.168.2.1/24 255.255.255.0 DHCP Server: 192.168.2.2-192.168.2.254	fec0:2::1/64 DHCP Disabled
☐	3	VLAN3	☒	☐ ⓘ	192.168.3.1/24 255.255.255.0 DHCP Server: 192.168.3.2-192.168.3.254	fec0:3::1/64 DHCP Disabled
☐	4	VLAN4	☒	☐ ⓘ	192.168.4.1/24 255.255.255.0 DHCP Server: 192.168.4.2-192.168.4.254	fec0:4::1/64 DHCP Disabled
☐	5	VLAN5	☒	☐ ⓘ	192.168.5.1/24 255.255.255.0 DHCP Server: 192.168.5.2-192.168.5.90	fec0:5::1/64 DHCP Disabled
☐	6	VLAN6	☒	☐ ⓘ	192.168.6.1/24 255.255.255.0 DHCP Server: 192.168.6.100-192.168.6.149	fec0:6::1/64 DHCP Disabled
☐	7	VLAN7	☒	☐ ⓘ	192.168.7.1/24 255.255.255.0 DHCP Server: 192.168.7.100-192.168.7.149	fec0:7::1/64 DHCP Disabled

VLANs to Port Table



VLAN ID LAN1 LAN2 LAN3 LAN4

1	U	U	U	U
2	E	T	E	E
3	E	E	T	E
4	E	E	E	T
5	T	T	T	T
6	T	E	E	E
7	T	E	E	E

U : Untagged, T : Tagged, E : Excluded

IPv4

IPv6

Interface	WAN1	WAN2	USB1	USB2
IP Address	10.10.81.237	--	--	--
Default Gateway	10.10.87.250	--	--	--
DNS	192.166.202.136 192.166.202.10	--	--	--
Dynamic DNS	Disabled	Disabled	Disabled	Disabled
Multi-WAN Status	Detection Disabled	Offline	Offline	Offline
	Disconnect	Renew	(Not Attached)	(Not Attached)

Tabela routingu

IPv4 Routes

Destination ↕	Next Hop ↕	Metric ↕	Interface ↕	Source ↕
0.0.0.0/0	10.10.87.250	6	WAN1	Static
10.10.87.250/32	-	0	WAN1	Connected
192.168.1.0/24	-	0	VLAN1	Connected
192.168.2.0/24	-	0	VLAN2	Connected
192.168.3.0/24	-	0	VLAN3	Connected
192.168.4.0/24	-	0	VLAN4	Connected
192.168.5.0/24	-	0	VLAN5	Connected
192.168.6.0/24	-	0	VLAN6	Connected
192.168.7.0/24	-	0	VLAN7	Connected

1.4.2 ODPOWIEDŹ 1: Charakterystyka datagramu na przykładzie protokołu IP

Protokół IP					
Pozycja	0–3	4–7	8–15	16–18	19–31
0	Wersja	Długość nagłówka	Typ usługi	Długość całkowita	
32	Identyfikator			Flagi	Pozycja fragmentu
64	Wartość Time to Live		Protokół	Suma kontrolna nagłówka	
96	Adres IP nadawcy				
128	Adres IP odbiorcy				
160	Opcje				
160 or 192+	Dane				

Struktura pakietu IP

Wersja. Wersja używanego protokołu .

Długość nagłówka. Wielkość nagłówka .

Typ usługi. Opcje wyznaczające pierwszeństwo oraz typ usługi są używane przez routery podczas przydzielania priorytetów dla ruchu sieciowego.

Długość całkowita. Wielkość całkowita nagłówka IP oraz danych znajdujących się w pakiecie.

Identyfikator. Unikalny identyfikator używany w celu identyfikacji pakietu i sekwencji pofragmentowanych pakietów.

Flagi. Flagi określające, czy pakiet należy, czy nie należy do sekwencji pofragmentowanych pakietów.

Przesunięcie fragmentu. Jeżeli pakiet jest fragmentem, to ta wartość jest używana podczas łączenia pakietów w odpowiedniej kolejności.

Wartość Time to Live. Długość życia pakietu wyrażona w sekundach lub „skokach”, które może wykonać pakiet.

Protokół. Identyfikuje typ pakietu, który jest kolejnym pakietem w sekwencji pakietów.

Suma kontrolna nagłówka. Mechanizm wykrywania błędów używany do sprawdzenia, czy zawartość nagłówka IP nie została uszkodzona bądź zniszczona.

Adres IP nadawcy. Adres IP urządzenia, które wysłało pakiet.

Adres IP odbiorcy. Adres IP urządzenia, dla którego jest przeznaczony pakiet.

Opcje. Pole zarezerwowane dla opcji dodatkowych protokołu. Można tutaj podać opcje dotyczące routingu nadawcy oraz znaczników czasu.

Dane. Pole zawiera rzeczywiste dane przekazywane przez ten pakiet IP.

1.4.3 ODPOWIEDŹ 2: Klasy adresów IPv4

Klasa adresu IP	przeznaczenie	Adres sieci	Adres hosta	Pierwszy oktet binarnie	Zakres adresów	Max. liczba stacji
A	Do obsługi dużych sieci	Oktet pierwszy	Oktety 2-4	0xxxxxxx	1.0.0.0 - 127.255.255.255	16 777 214
B	Do obsługi sieci dużych i małych	Oktety: 1-2	Oktety 3-4	10xxxxxx	128.0.0.0.0 - 191-255.255.255	65 534
C	Do obsługi dużej ilości małych sieci	Oktety: 1-3	Oktet 4	110xxxxx	192.0.0.0 - 223.255.255.255	Każda sieć może obsługiwać 254 stacje.
D	Służą do multipleksacji (multicast) w sieciach IP	Adres sieci jest niepowtarzalnym adresem sieci, kierującym pakiety do zdefiniowanych z góry grup adresów IP		1110xxxx	224.0.0.0 - 239.255.255.255	Jedna stacja może przysyłać strumień danych do wielu odbiorców jednocześnie.
E	Zarezerwowana do badań dla zespołu IANA	Z adresów tych nie można korzystać w Internecie		1111xxxx	240.0.0.0 - 255.255.255.255	-

W każdej z klas adresów dwa spośród nich były zarezerwowane do celów specjalnych. Adres , w którym w części przeznaczonej dla hosta znajdują się same zera (dwójkowo), jest **adresem sieci** np. 192.168.0.0. Adres, w którym w części przeznaczonej dla hosta znajdują się same jedynki jest adresem **rozgłoszeniowym** (broadcast). Adresów tych nie można przypisać hostom.

Ponadto istnieją jeszcze inne specjalne adresy opisane w poniższej tabeli.

Adres	Funkcja	Zastosowanie
0.0.0.0	Adres domyślny trasy	Użycie w tablicach routingu
127.0.0.0	Adres pierwszej pętli zwrotnej	Komunikacja sieciowa hosta z samym sobą
255.255.255.255	Adres rozgłoszeniowy w sieci lokalnej	Komunikacja hosta ze wszystkimi hostami w ramach jednej sieci fizycznej

1.4.3 ODPOWIEDŹ 2: IPv4 – pule adresów prywatnych

Adres sieci	Maska sieci	Dostępne adresy	Liczba adresów IP	Adres rozgłoszeniowy
10.0.0.0	255.0.0.0 (8 bitów)	10.0.0.1 – 10.255.255.254	$256^3 - 2$	10.255.255.255
172.16.0.0	255.240.0.0 (12 bitów)	172.16.0.1 – 172.31.255.254	$16 * 256^2 - 2$	172.31.255.255
192.168.0.0	255.255.0.0 (16 bitów)	192.168.0.1 – 192.168.255.254	$256^2 - 2$	192.168.255.255

1.4.4 ODPOWIEDŹ 3: IPv4 - maski podsieci

Numer **CIDR** oznacza ile bitów odpowiada za określenie adresu podsieci. Innymi słowy, informuje ile bitów ustawionych na 1 znajduje się w masce podsieci:

Maska sieci zwykła	Maska sieci skrócona	Klasa maski	Ilość szt. IP dla sieci z daną maską.
255.0.0.0	/8	A	16777216 szt.
255.128.0.0	/9	A	8388608 szt.
255.192.0.0	/10	A	4194304 szt.
255.224.0.0	/11	A	2097152 szt.
255.240.0.0	/12	A	1048576 szt.
255.248.0.0	/13	A	524288 szt.
255.252.0.0	/14	A	262144 szt.
255.254.0.0	/15	A	131072 szt.
255.255.0.0	/16	B	65536 szt.
255.255.128.0	/17	B	32768 szt.
255.255.192.0	/18	B	16384 szt.
255.255.224.0	/19	B	8192 szt.

255.255.240.0	/20	B	4096 szt.
255.255.248.0	/21	B	2048 szt.
255.255.252.0	/22	B	1024 szt.
255.255.254.0	/23	B	512 szt.
255.255.255.0 lub wersja skrócona: [0]	/24	C	256 szt. IP
255.255.255.128 lub [128]	/25	C	128 szt. IP
255.255.255.192 lub [192]	/26	C	64 szt. IP
255.255.255.224 lub [224]	/27	C	32 szt. IP
255.255.255.240 lub [240]	/28	C	16 szt. IP
255.255.255.248 lub [248]	/29	C	8 szt. IP
255.255.255.252 lub [252]	/30	C	4 szt. IP (najmniejsza możliwa podsieć zawierająca 2 szt. hostów)
255.255.255.254 lub [254]	/31	C	2 szt. IP Nie można utworzyć podsieci.
255.255.255.255 lub [255]	/32	C	1 szt. IP ADRES HOSTA.

Pamiętaj, że ilość hostów jest o 2 szt mniejsza od ilości adresów IP przydzielonej dla danej podsieci (odejmujemy IP adresu sieci oraz Broadcast).

1.4.5 ODPOWIEDŹ 4 Charakterystyka protokołu ARP

- Nazwa ARP: Address Resolution Protocol
- pracuje w warstwie łącza danych i sieciowej
- określa adres docelowy używany przez sieci TCP/IP (wraz z IPv4) w celu przełożenia adresu IP na adres MAC
- tworzy tabele, w której łączy adres IP z adresem MAC interfejsu sieciowego (węzła)
- dokonuje translacji adresów tylko w tej samej podsieci
- węzeł przechowuje tabelę ARP w pamięci RAM
- tabela zawiera wartość TTL. Tabela usuwa wpisy których żywotność TTL się zakończyła
- protokół używa komunikatów żądania i odpowiedzi
- ramka ARP kierowana jest do wszystkich węzłów w sieci lokalnej (broadcast), adresów rozgłoszeniowych: MAC ff:ff:ff:ff:ff:ff, IP 255.255.255.255

Prawidłowy ruch sieciowy ARP – widok ruchu sieciowego

Time	Source	Destination	Protocol	Length	Info
30...	151.286614	192.168.255....	104.237.191.1	TLSv...	100 Application Data
30...	151.356367	104.237.191.1	192.168.255....	TCP	60 443 → 49197 [ACK] Seq=3729 Ack=1061 Win=32512 Len=6
30...	152.049474	192.168.255....	172.217.16.46	UDP	714 52486 → 443 Len=672
30...	152.049556	192.168.255....	172.217.16.46	UDP	66 52486 → 443 Len=24
30...	152.057879	172.217.16.46	192.168.255....	UDP	77 443 → 52486 Len=35
30...	152.077292	172.217.16.46	192.168.255....	UDP	107 443 → 52486 Len=65
30...	152.078547	172.217.16.46	192.168.255....	UDP	60 443 → 52486 Len=17
30...	152.078899	192.168.255....	172.217.16.46	UDP	83 52486 → 443 Len=41
30...	153.151228	192.168.255....	192.168.255.1	DNS	86 Standard query 0xd0f7 A hp_p1606dn.wojtusiak.local
30...	156.136772	TpLinkTechno...	ASUSTekCOMPU...	ARP	60 Who has 192.168.255.100? Tell 192.168.255.1
30...	156.136795	ASUSTekCOMPU...	TpLinkTechno...	ARP	42 192.168.255.100 is at d0:17:c2:d4:99:85
30...	157.151456	fe80::a462:a...	ff02::1:3	LLMNR	90 Standard query 0x94bf A hp_p1606dn
30...	157.151642	192.168.255....	224.0.0.252	LLMNR	70 Standard query 0x94bf A hp_p1606dn
30...	157.251140	fe80::a462:a...	ff02::1:3	LLMNR	90 Standard query 0x94bf A hp_p1606dn
30...	157.251163	192.168.255....	224.0.0.252	LLMNR	70 Standard query 0x94bf A hp_p1606dn
30...	157.451672	192.168.255....	192.168.255....	NBNS	92 Name query NB HP_P1606DN<00>
30...	158.201103	192.168.255....	192.168.255....	NBNS	92 Name query NB HP_P1606DN<00>
30...	158.951064	192.168.255....	192.168.255....	NBNS	92 Name query NB HP_P1606DN<00>
30...	159.703126	192.168.255....	192.168.255.1	DNS	86 Standard query 0x7872 A hp_p1606dn.wojtusiak.local
30...	160.358096	192.168.255....	172.217.16.10	TCP	55 [TCP Keep-Alive] 49183 → 443 [ACK] Seq=1 Ack=1 Win=
30...	160.358119	192.168.255....	172.217.16.3	TCP	55 [TCP Keep-Alive] 49184 → 443 [ACK] Seq=1 Ack=1 Win=
30...	160.364903	172.217.16.10	192.168.255....	TCP	66 [TCP Keep-Alive ACK] 443 → 49183 [ACK] Seq=1 Ack=2
30...	160.365680	172.217.16.3	192.168.255....	TCP	66 [TCP Keep-Alive ACK] 443 → 49184 [ACK] Seq=1 Ack=2

Prawidłowy ruch sieciowy ARP – nagłówki pakietu

7 0.077018	192.168.255....	192.168.255....	NBNS	92 Name query NB PVLUMZUAETOQ<00>
8 0.206943	192.168.255....	192.168.255.1	DNS	82 Standard query 0x7acb A SERWER.wojtusiak.local
9 0.305879	TpLinkTechno...	Broadcast	ARP	60 Who has 192.168.255.200? Tell 192.168.255.1
10 0.45	Wireshark - Pakiet 9 - arp_prawidlowy_ruch_sieciowy.pcapng			
11 0.64	Frame 9: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{56			
12 0.64	Ethernet II, Src: TpLinkTechno_28:a0:7e (18:d6:c7:28:a0:7e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)			
13 0.64	Address Resolution Protocol (request)			
14 0.65	Hardware type: Ethernet (1)			
15 0.65	Protocol type: IPv4 (0x0800) prawidłowe adresy MAC			
16 0.65	Hardware size: 6			
17 0.65	Protocol size: 4			
18 0.65	Opcode: request (1)			
19 0.65	Sender MAC address: TpLinkTechno_28:a0:7e (18:d6:c7:28:a0:7e)			
20 0.65	Sender IP address: 192.168.255.1			
21 0.65	Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)			
22 0.65	Target IP address: 192.168.255.200			
23 0.65				
24 0.65				
25 0.65				
26 0.65				

Burza sieciowa (sztorm sieciowy) ARP

29...	28.440692	TpLinkTechno...	Broadcast	ARP	60 Who has 192.168.255.1? Tell 192.168.255.253
29...	28.440692	TpLinkTechno...	Broadcast	ARP	60 Who has 192.168.255.1? Tell 192.168.255.253
29...	28.440692	TpLinkTechno...	Broadcast	ARP	60 Who has 192.168.255.197? Tell 192.168.255.1
29...	28.440692	192.168.255....	255.255.255....	UDP	717 53874 → 29810 Len=675
29...	28.440693	192.168.255....	224.0.0.251	MDNS	291 Standard query response 0x0000 PTR, cache fl
29...	28.440693	fe80::aa9c:e...	ff02::fb	MDNS	311 Standard query response 0x0000 PTR, cache fl
29...	28.440693	TpLinkTechno...	Broadcast	ARP	60 Who has 192.168.255.1? Tell 192.168.255.253
29...	28.440693	TpLinkTechno...	Broadcast	ARP	60 Who has 192.168.255.1? Tell 192.168.255.253
29...	28.440694	TpLinkTechno...	Broadcast	ARP	60 Who has 192.168.255.197? Tell 192.168.255.1
29...	28.440694	192.168.255....	255.255.255....	UDP	717 53874 → 29810 Len=675
29...	28.440694	192.168.255....	224.0.0.251	MDNS	291 Standard query response 0x0000 PTR, cache fl
29...	28.440694	192.168.255....	255.255.255....	UDP	715 53874 → 29810 Len=673
29...	28.440695	192.168.255....	255.255.255....	UDP	715 53874 → 29810 Len=673
29...	28.440695	192.168.255....	224.0.0.251	MDNS	291 Standard query response 0x0000 PTR, cache fl
29...	28.440695	fe80::aa9c:e...	ff02::fb	MDNS	311 Standard query response 0x0000 PTR, cache fl
29...	28.440696	192.168.255....	255.255.255....	UDP	717 53874 → 29810 Len=675
29...	28.440696	TpLinkTechno...	Broadcast	ARP	60 Who has 192.168.255.1? Tell 192.168.255.253
29...	28.440696	TpLinkTechno...	Broadcast	ARP	60 Who has 192.168.255.1? Tell 192.168.255.253
29...	28.440696	TpLinkTechno...	Broadcast	ARP	60 Who has 192.168.255.197? Tell 192.168.255.1
29...	28.440696	192.168.255....	224.0.0.251	MDNS	291 Standard query response 0x0000 PTR, cache fl
29...	28.440697	fe80::aa9c:e...	ff02::fb	MDNS	311 Standard query response 0x0000 PTR, cache fl
29...	28.440697	TpLinkTechno...	Broadcast	ARP	60 Who has 192.168.255.1? Tell 192.168.255.253
29...	28.440697	TpLinkTechno...	Broadcast	ARP	60 Who has 192.168.255.1? Tell 192.168.255.253

1.4.6 ODPOWIEDŹ 5 W jaki sposób host A pozyskuje adres mac hosta B, z którym to chce nawiązać połączenie

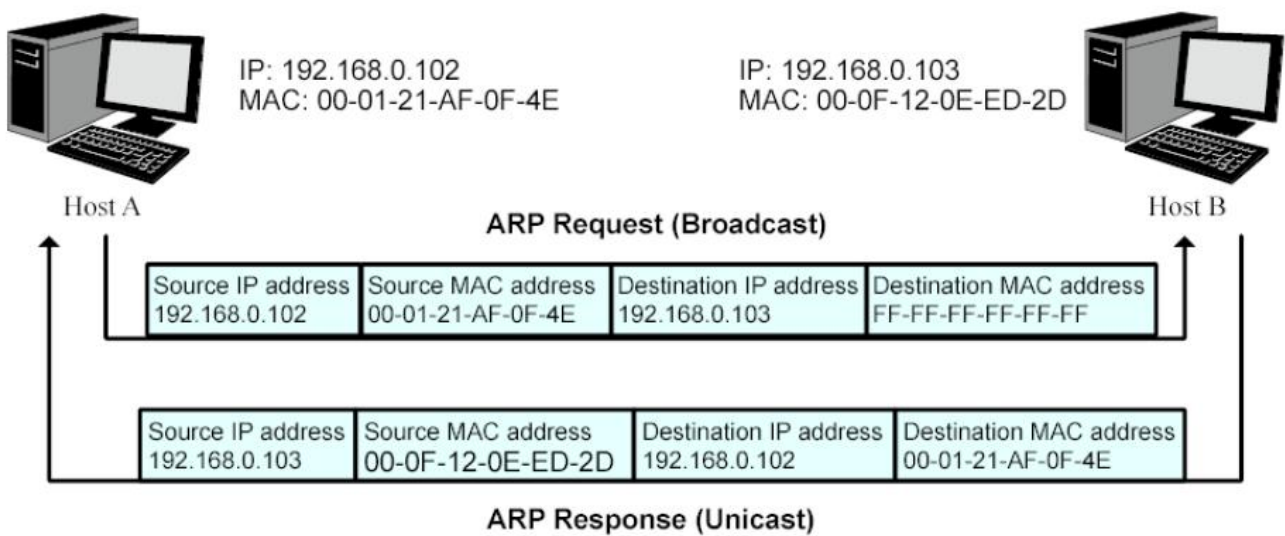


Figure 12-3 ARP Implementation Procedure

1.4.7 ODPOWIEDŹ 6 Jak przebiega atak ARP, w którym atakujący podszywa się pod bramę domyślną routera?

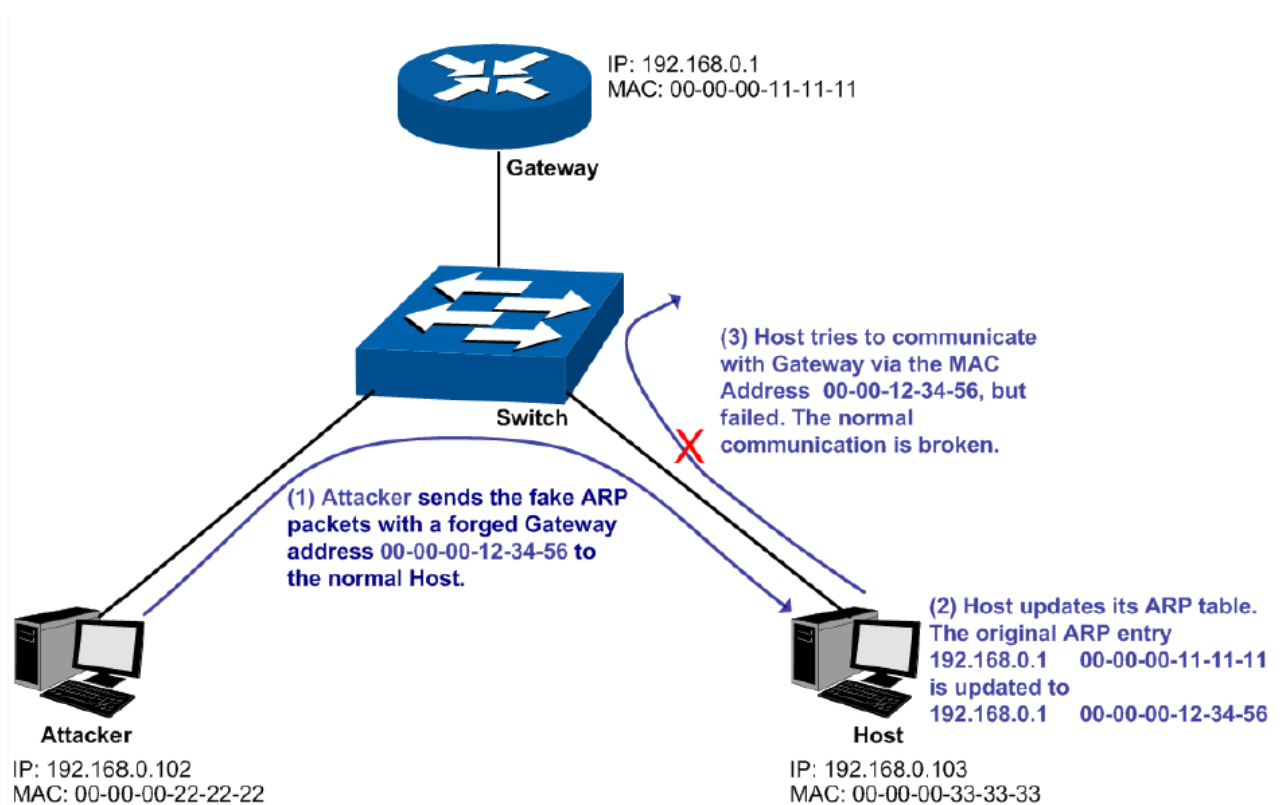


Figure 12-9 ARP Attack - Imitating Gateway

ATAK ARP – Imitating Gateway (imitacja bramy) – widok ruchu sieciowego

Time	Source	Destination	Protocol	Length	Info
1 0.000000	ASUSTekCOMPU...	MotorolaMobi...	ARP	60	Who has 192.168.3.48? Tell 192.168.3.1
2 0.000358	ASUSTekCOMPU...	ASUSTekCOMPU...	ARP	60	Who has 192.168.3.45? Tell 192.168.3.1
3 0.000734	ASUSTekCOMPU...	ASUSTekCOMPU...	ARP	60	Who has 192.168.3.2? Tell 192.168.3.1
4 0.000766	ASUSTekCOMPU...	3b:75:55:64:...	ARP	42	192.168.3.2 is at 78:24:af:3b:ae:dd
5 0.001184	ASUSTekCOMPU...	SamsungElect...	ARP	60	Who has 192.168.3.78? Tell 192.168.3.1
6 0.001457	ASUSTekCOMPU...	SamsungElect...	ARP	60	Who has 192.168.3.9? Tell 192.168.3.1
7 0.003281	ASUSTekCOMPU...	XiaomiCommun...	ARP	60	Who has 192.168.3.132? Tell 192.168.3.1
8 0.003663	Dell_21:16:9f	3b:75:55:64:...	ARP	60	192.168.3.68 is at b8:ac:6f:21:16:9f
9 0.004732	ASUSTekCOMPU...	HuaweiTechno...	ARP	60	Who has 192.168.3.24? Tell 192.168.3.1
10 0.005201	TpLinkTechno...	3b:75:55:64:...	ARP	60	192.168.3.246 is at e8:de:27:c1:91:88
11 0.005445	ASUSTekCOMPU...	SamsungElect...	ARP	60	Who has 192.168.3.41? Tell 192.168.3.1
12 0.005857	ASUSTekCOMPU...	3b:75:55:64:...	ARP	60	192.168.3.127 is at f8:32:e4:8d:ce:07
13 0.006220	ASUSTekCOMPU...	3b:75:55:64:...	ARP	60	192.168.3.82 is at f8:32:e4:8d:d8:e2
14 0.015650	MicroStarInt...	3b:75:55:64:...	ARP	60	192.168.3.113 is at 00:19:db:71:86:df
15 0.015986	MicroStarInt...	3b:75:55:64:...	ARP	60	192.168.3.89 is at 00:19:db:71:87:e3
16 0.016334	ASUSTekCOMPU...	HuaweiTechno...	ARP	60	Who has 192.168.3.92? Tell 192.168.3.1
17 0.017508	ASUSTekCOMPU...	3b:75:55:64:...	ARP	60	192.168.3.138 is at 2c:4d:54:e4:2a:2b
18 0.017902	ASUSTekCOMPU...	3b:75:55:64:...	ARP	60	192.168.3.58 is at 2c:4d:54:e4:2a:8f
19 0.018291	ASUSTekCOMPU...	3b:75:55:64:...	ARP	60	192.168.3.27 is at 2c:4d:54:e4:2d:4f
20 0.018718	ASUSTekCOMPU...	3b:75:55:64:...	ARP	60	192.168.3.25 is at 2c:4d:54:e4:2f:83
21 0.018998	ASUSTekCOMPU...	3b:75:55:64:...	ARP	60	192.168.3.29 is at 2c:4d:54:e4:2f:8e
22 0.019382	ASUSTekCOMPU...	3b:75:55:64:...	ARP	60	192.168.3.117 is at 2c:4d:54:e4:2f:ba

ATAK ARP – Imitating Gateway (imitacja bramy) – analiza nagłówków pakietu

1 0.000000 ASUSTekCOMPU... MotorolaMobi... ARP 60 Who has 192.168.3.48? Tell 192.168.3.1

Wireshark · Pakiet 1 · atak arp.pcapng

- > Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{FEFCEDDE-45B2}
- > Ethernet II, Src: ASUSTekCOMPU_3b:7a:20 (2c:56:dc:3b:7a:20), Dst: MotorolaMobi_b2:56:b9 (64:db:43:b2:56:b9)
- Address Resolution Protocol (request)
 - Hardware type: Ethernet (1)
 - Protocol type: IPv4 (0x0800)
 - Hardware size: 6
 - Protocol size: 4
 - Opcode: request (1)
 - Sender MAC address: 3b:75:55:64:60:0d (3b:75:55:64:60:0d)
 - Sender IP address: 192.168.3.1
 - Target MAC address: Xerox_00:00:00 (00:00:00:00:00:00)
 - Target IP address: 192.168.3.48

prawdziwy adres mac
karty sieciowej
komputera (sprzętowy)

falszywy adres mac generowany przez atakujące oprogramowanie

1.4.8 ODPOWIEDŹ 7 Jak przebiega atak ARP, w którym atakujący podaje routerowi (Gateway) fałszywe adresy mac hostów?

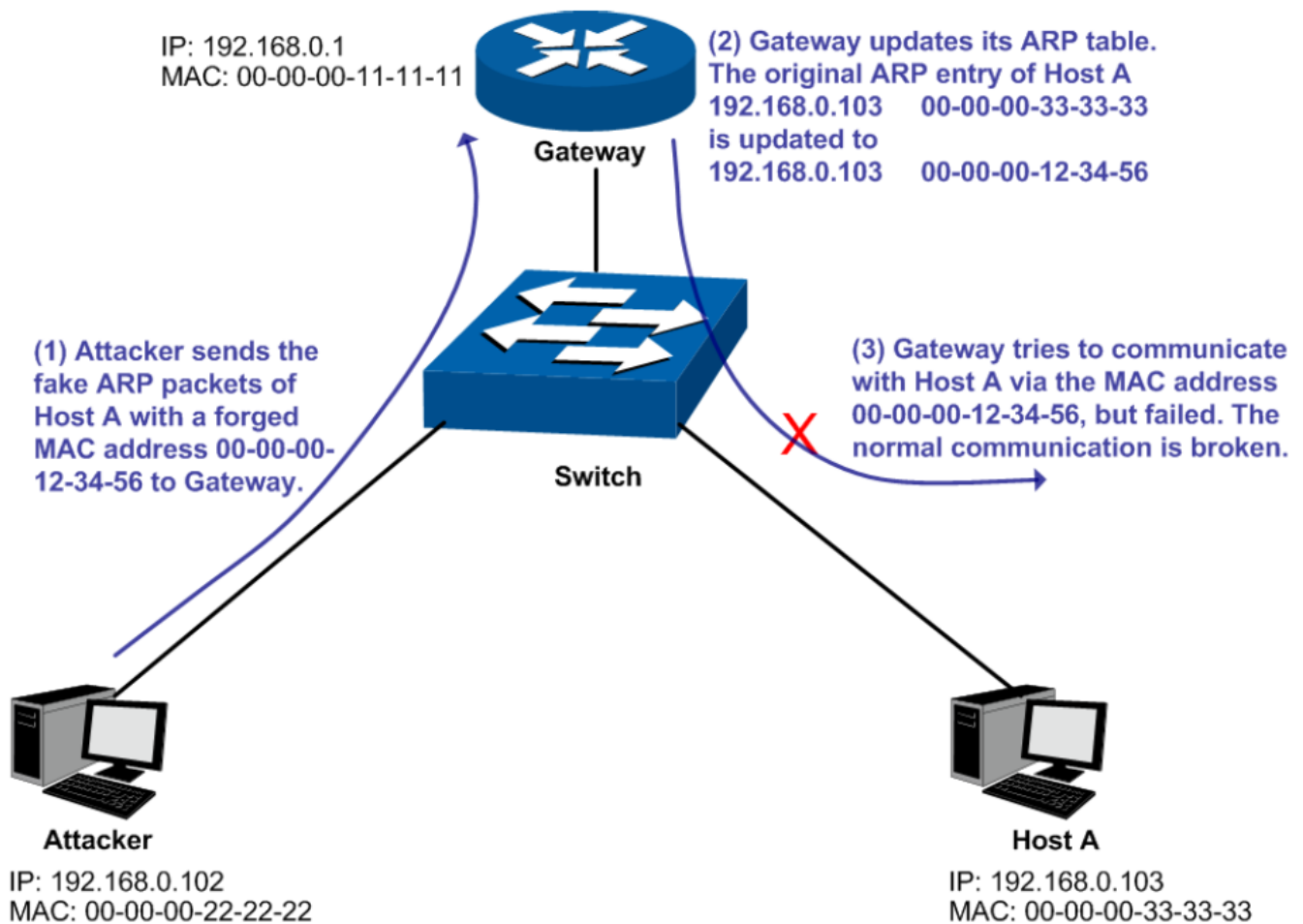


Figure 12-10 ARP Attack – Cheating Gateway

1.4.9 ODPOWIEDŹ 8 Jak przebiega atak ARP, w którym atakujący podaje fałszywy adresy mac hosta A hostowi B?

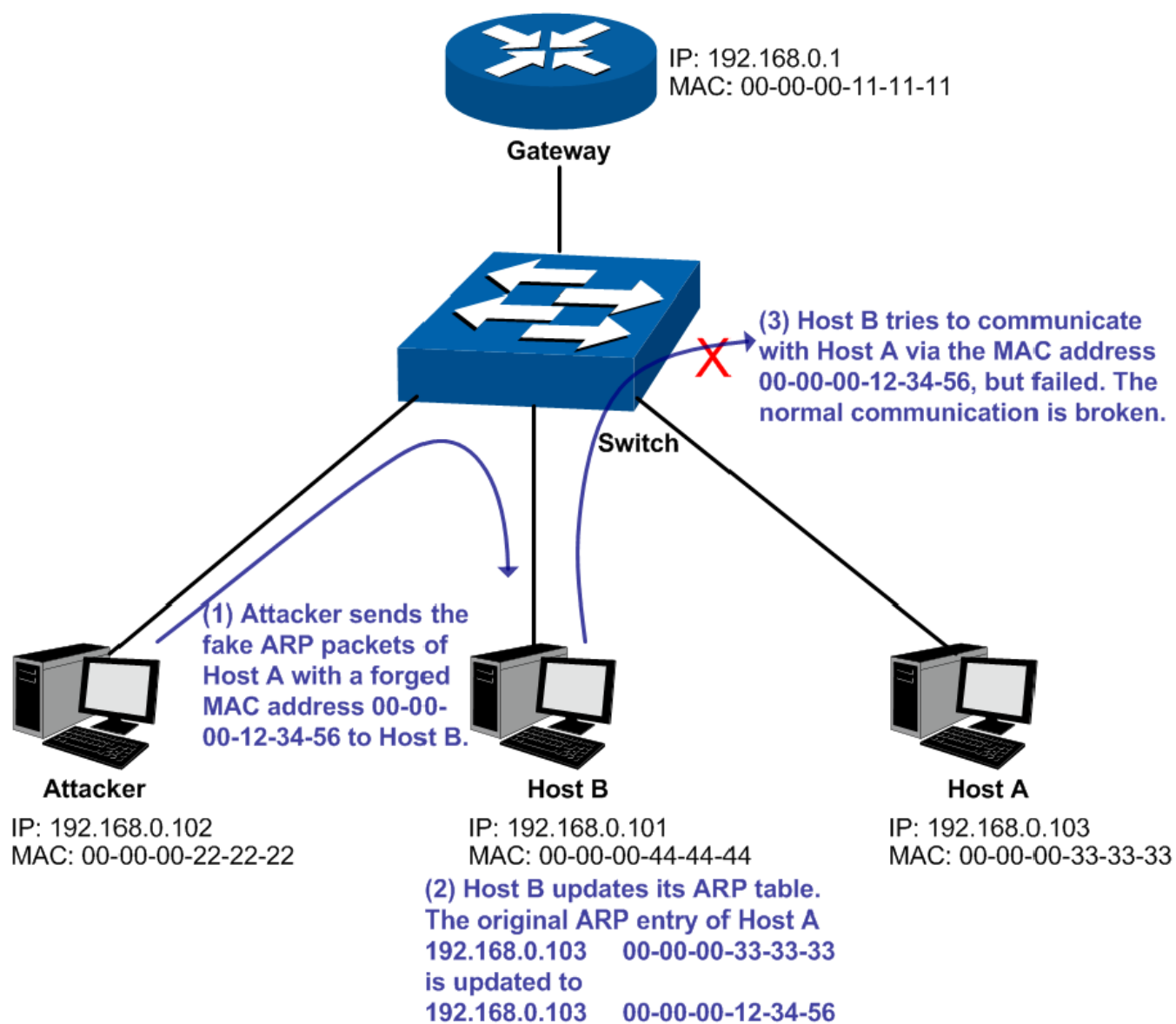


Figure 12-11 ARP Attack – Cheating Terminal Hosts

1.4.10 ODPOWIEDŹ 9 Jak przebiega atak ARP typu „Człowiek w środku”?

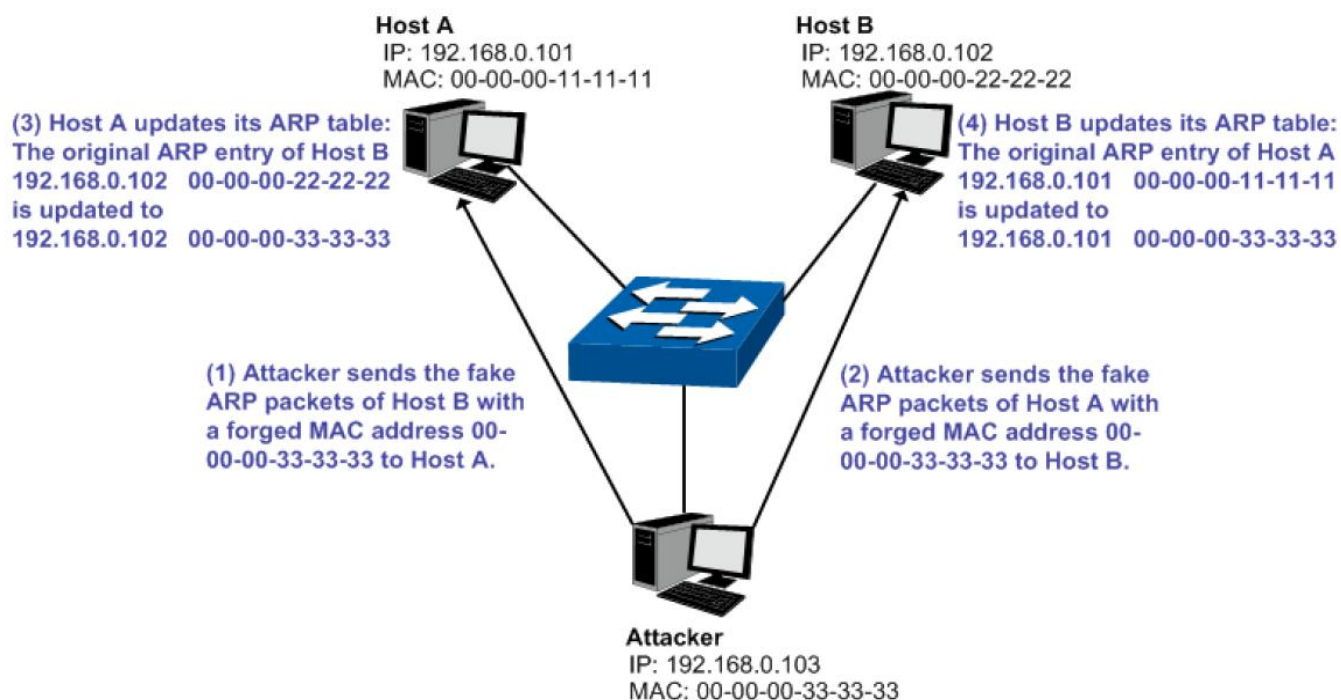


Figure 12-12 Man-In-The-Middle Attack

1.4.11 ODPOWIEDŹ 10 Protokół ICMP

Po co protokół ICMP, jeżeli mamy protokół IP

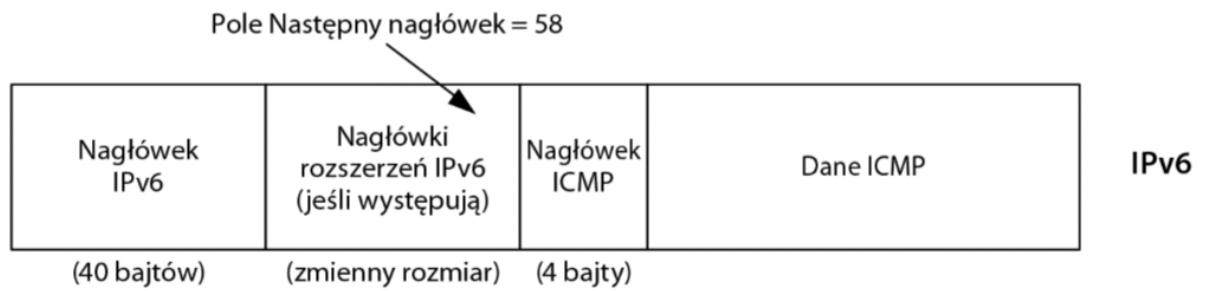
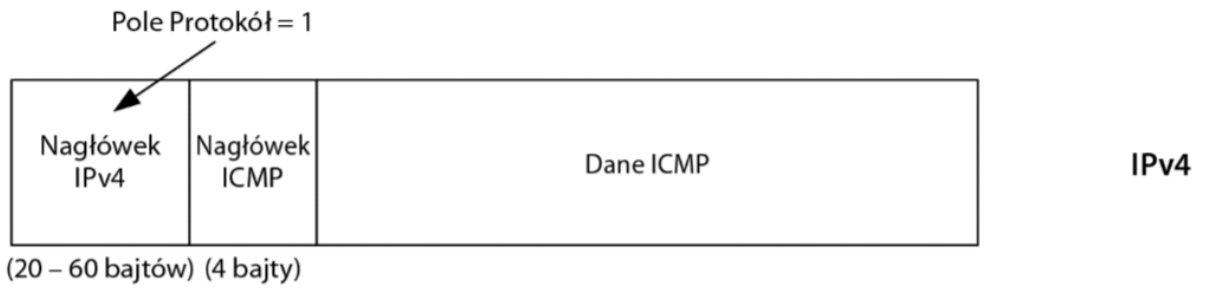
- Protokół IP nie udostępnia sam z siebie mechanizmów umożliwiających śledzenie losu datagramów, które — z różnych przyczyn — nie docierają do miejsc swego przeznaczenia.
- Nie udostępnia on także żadnych narzędzi do uzyskiwania informacji diagnostycznych, np. listy routerów na trasie datagramu czy też szacowanego czasu jego wędrówki.
- Z zamiarem uzupełnienia tych niedostatków opracowano specjalny protokół o nazwie Internet Control Message Protocol — „internetowy protokół komunikatów kontrolnych” — powszechnie oznaczany akronimem ICMP

Charakterystyka ogólna protokołu ICMP:

- protokół narzędziowy TCP/IP odpowiedzialny za dostarczanie informacji dotyczących dostępności urządzeń, usług lub routerów w sieci TCP/IP,
- jest częścią IP i wykorzystuje IP do przesyłania wiadomości,
- nagłówek protokołu ICMP jest dość mały i zmienia się w zależności od potrzeb,
- nagłówek ICMP zawiera następujące pola:
 - ❖ **Typ.** Typ klasyfikacyjny wiadomości ICMP oparty na specyfikacji RFC.
 - ❖ **Kod.** Kod wiadomości ICMP oparty na specyfikacji RFC.
 - ❖ **Suma kontrolna.** Pole używane w celu zagwarantowania, że dostarczone dane i nagłówek ICMP nie zostały zmodyfikowane podczas transmisji.
 - ❖ **Zmienna.** Zawartość tego pola zależy od wartości pól Typ i Kod.

Protokół ICMP					
Pozycja	Oktet	0	1	2	3
Oktet	Bit	0 – 7	8 – 15	16 – 23	24 – 31
0	0	Typ	Kod	Suma kontrolna	
4+	32+	Zmienna			

Nagłówek ICMP



Enkapsulacja komunikatów ICMP w datagramach IPv4 i IPv6.

Komunikaty ICMP

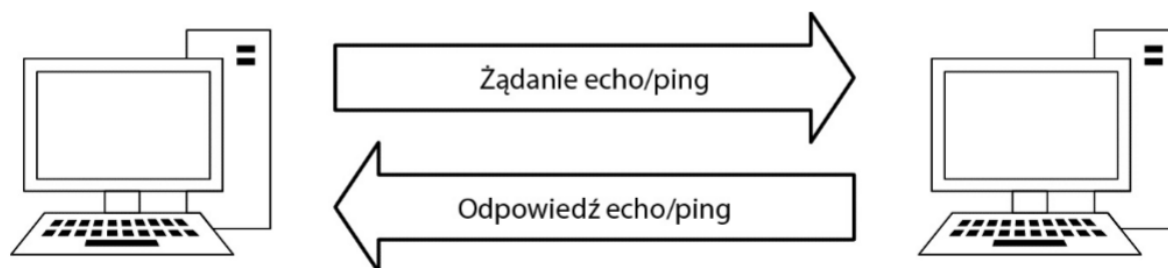
Przyjrzymy się teraz bliżej komunikatom ICMP, poświęcając szczególną uwagę wykorzystywanym najczęściej. Generalnie komunikaty ICMP dzielą się na dwie grupy: do pierwszej należą **komunikaty oznajmiające problemy z dostarczaniem datagramów IP**, zwane popularnie komunikatami o błędach (error messages), druga grupa to **komunikaty zwane popularnie informacyjnymi**, wymieniane w ramach dialogów żądanie-odpowiedź, związanych z uzyskiwaniem różnorodnych informacji konfiguracyjnych.

Standardowe typy komunikatów ICMPv4. Typy najczęściej występujące wyróżniono gwiazdką, znakiem + opatrzone natomiast typy komunikatów mogących zawierać obiekty rozszerzeń. W kolumnie Rodzaj wskazano rodzaju komunikatu — I oznacza komunikat informacyjny, zaś E komunikat o błędzie

Typ	Nazwa oficjalna	Dokument	Rodzaj	Znaczenie
0 (*)	<i>Echo Reply</i>	[RFC0792]	I	Odpowiedź na żądanie <i>Echo</i> (ping), zwraca dane
3 (*) (+)	<i>Destination Unreachable</i>	[RFC0792]	E	Nieosiągalny host lub protokół
4	<i>Source Quench</i>	[RFC0792]	E	Wystąpiło przeciążenie (nieużywany)
5 (*)	<i>Redirect</i>	[RFC0792]	E	Konieczność użycia alternatywnego routera
8 (*)	<i>Echo Request</i>	[RFC0792]	I	Żądanie <i>Echo</i> (ping) (opcjonalnie może zawierać dane)
9	<i>Router Advertisement</i>	[RFC1256]	I	Wskazanie adresu lub preferencji routera
10	<i>Router Solicitation</i>	[RFC1256]	I	Żądanie wysłania komunikatu <i>Router Advertisement</i>
11 (*) (+)	<i>Time Exceeded</i>	[RFC0792]	E	Wyczerpanie zasobów lub wyzerowanie pola <i>Czas życia</i> (TTL)
12 (*) (+)	<i>Parameter Problem</i>	[RFC0792]	E	Niepoprawny format pakietu lub jego nagłówek

Komunikaty ICMPv4 występujące w kilku odmianach (podtypach) dla danej wartości pola Typ; poszczególne podtypy rozróżniane są na podstawie pola Kod. Najczęściej występujące kombinacje Typ/Kod wyróżniliśmy gwiazdką w kolumnie Typ

Typ	Kod	Nazwa oficjalna	Znaczenie
3	0	<i>Net Unreachable</i>	Nie istnieje żadna trasa do miejsca przeznaczenia
3 (*)	1	<i>Host Unreachable</i>	Istniejący, lecz nieosiągalny host
3	2	<i>Protocol Unreachable</i>	Nierozpoznany protokół transportowy
3 (*)	3	<i>Port Unreachable</i>	Nierozpoznany (nieużywany) port transportowy
3 (*)	4	<i>Fragmentation Needed and Don't Fragment Was Set</i> (komunikat PTB)	Wymagana jest fragmentacja pakietu, lecz zabrania jej ustawiony bit DF; komunikat generowany w ramach PMTUD (patrz [RFC1191])
3	5	<i>Source Route Failed</i>	Nieosiągalny router pośredni
3	6	<i>Destination Network Unknown</i>	Komunikat wycofany przez [RFC1812]
3	7	<i>Destination Host Unknown</i>	Docelowy host nie istnieje



Polecenie ping to jedynie dwa kroki

```
C:\Users\user>ping 192.168.7.1

Pinging 192.168.7.1 with 32 bytes of data:
Reply from 192.168.7.1: bytes=32 time<1ms TTL=64
Reply from 192.168.7.1: bytes=32 time=1ms TTL=64
Reply from 192.168.7.1: bytes=32 time<1ms TTL=64
Reply from 192.168.7.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

No.	Time	Source	Destination	Protoc	Length	Info
28	3.648934	192.168.7.129	192.168.7.1	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (reply in 29)
29	3.649790	192.168.7.1	192.168.7.129	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=64 (request in 28)
40	4.651894	192.168.7.129	192.168.7.1	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128 (reply in 41)
41	4.653497	192.168.7.1	192.168.7.129	ICMP	74	Echo (ping) reply id=0x0001, seq=27/6912, ttl=64 (request in 40)
51	5.655162	192.168.7.129	192.168.7.1	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=128 (reply in 52)
52	5.655991	192.168.7.1	192.168.7.129	ICMP	74	Echo (ping) reply id=0x0001, seq=28/7168, ttl=64 (request in 51)
63	6.658543	192.168.7.129	192.168.7.1	ICMP	74	Echo (ping) request id=0x0001, seq=29/7424, ttl=128 (reply in 64)
64	6.659346	192.168.7.1	192.168.7.129	ICMP	74	Echo (ping) reply id=0x0001, seq=29/7424, ttl=64 (request in 63)

Przy pingowaniu na bramę domyślną stacja robocza zna adres mac celu.

```
Interface: 192.168.7.129 --- 0xf
Internet Address      Physical Address      Type
192.168.7.1          04-eb-40-35-f0-b2    dynamic
```

- > Frame 27: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{D66E431}
- > Ethernet II, Src: ASUSTekCOMPU_68:3e:af (f0:79:59:68:3e:af), Dst: Cisco_35:f0:b2 (04:eb:40:35:f0:b2)
- > Internet Protocol Version 4, Src: 192.168.7.129, Dst: 192.168.7.1
- > Internet Control Message Protocol

Wireshark - Pakiet 28 - NIC1

Internet Protocol Version 4, Src: 192.168.7.129, Dst: 192.168.7.1 **IPv4**

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 60
- Identification: 0x2b79 (11129)
- > 000. = Flags: 0x0
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 128
- Protocol: ICMP (1)
- Header Checksum: 0x7f75 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.7.129
- Destination Address: 192.168.7.1
- [Stream index: 0]

Internet Control Message Protocol **ICMP**

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0x4d41 [correct]
- [Checksum Status: Good]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence Number (BE): 26 (0x001a)
- Sequence Number (LE): 6656 (0x1a00)
- [\[Response frame: 29\]](#)

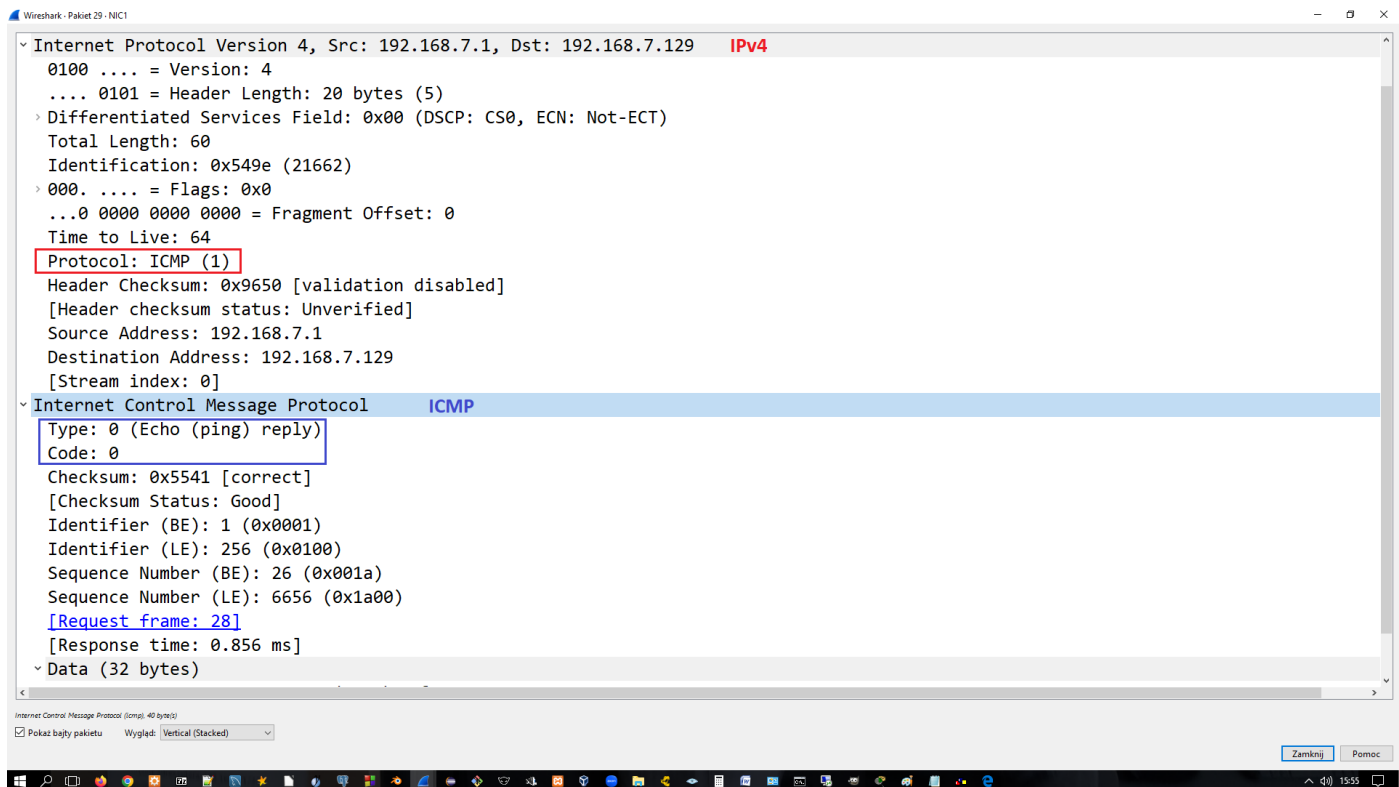
Data (32 bytes)

Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

No. 28 - Time: 3.648934 - Source: 192.168.7.129 - Destination: 192.168.7.1 - Protocol: ICMP - Length: 74 - Info: Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (reply in 29)

☒ Pokaż bajty pakietu Wygląd: Vertical (Stacked)

Zamknij Pomoc



Pingowanie na nieosiągalny host **192.168.7.248** . Stacja robocza nie zna adresu mac celu.

```
Interface: 192.168.7.129 --- 0xf
Internet Address      Physical Address      Type
192.168.7.1          04-eb-40-35-f0-b2     dynamic
192.168.7.126        f8-32-e4-a4-5a-b5     dynamic
192.168.7.255        ff-ff-ff-ff-ff-ff     static
224.0.0.22           01-00-5e-00-00-16     static
224.0.0.251          01-00-5e-00-00-fb     static
224.0.0.252          01-00-5e-00-00-fc     static
239.255.255.250      01-00-5e-7f-ff-fa     static
255.255.255.255      ff-ff-ff-ff-ff-ff     static
```


Poniżej widać, że nie został wysłany pakiet ICMP Typ:8 Code:0 echo (ping) request).

icmp					
No.	Time	Source	Destination	Protoc	Lengt Info
50	38.814025	192.166.202.1	192.168.7.129	ICMP	148 Destination unreachable (Network unreachable)
78	48.917208	192.166.202.1	192.168.7.129	ICMP	148 Destination unreachable (Network unreachable)
98	58.918966	192.166.202.1	192.168.7.129	ICMP	148 Destination unreachable (Network unreachable)

Wireshark · Pakiet 50 · NIC1

> Frame 50: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface \Device\NPF_{D66E431E...}

> Ethernet II, Src: Cisco_35:f0:b2 (04:eb:40:35:f0:b2), Dst: ASUSTekCOMPU_68:3e:af (f0:79:59:68:3e:af)

> Internet Protocol Version 4, Src: 192.166.202.1, Dst: 192.168.7.129 **IPv4**

> Internet Control Message Protocol **ICMP**

Type: 3 (Destination unreachable)

Code: 0 (Network unreachable)

Checksum: 0x9131 [correct]

[Checksum Status: Good]

Unused: 00000000

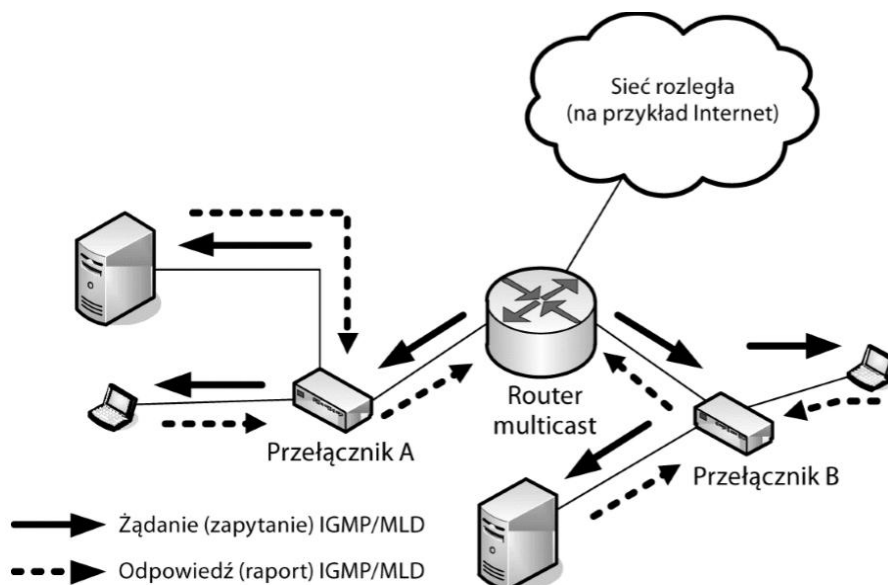
> Internet Protocol Version 4, Src: 192.168.7.129, Dst: 192.168.10.248

> User Datagram Protocol, Src Port: 53988, Dst Port: 161

> Simple Network Management Protocol

1.4.12 ODPOWIEDŹ 9 Protokół IGMP

IGMP (Internet Group Management Protocol — internetowy protokół zarządzania grupami), w IPv6 natomiast funkcje tę pełni protokół MLD (Multicast Listener Discovery — odnajdywanie obserwatorów multicastingu).



Rysunek . Routery multicast periodycznie wysyłają żądania IGMP (MLD) do każdej przyłączonej podsieci w celu uzyskania informacji na temat istniejących grup multicast. W odpowiedzi na takie żądanie każdy host należący do którejkolwiek grupy (grup) odsyła raport wskazujący tę grupę (grupy) wraz z informacjami o potencjalnych nadawcach, od których życzy sobie otrzymywać komunikaty multicast. Hosty mogą także wysyłać raporty z własnej inicjatywy, w sytuacjach gdy zmienia się ich status uczestnictwa w grupach multicast

Protokół IGMP rozsyła swe żądania na adres grupowy wszystkich hostów (All Hosts — 224.0.0.1), protokół MLD — na lokalny dla łącza adres grupowy wszystkich węzłów (link-local All Nodes — ff02::1). Komunikaty te przetwarzane są przez wszystkie hosty

implementujące multicasting IP (z wyjątkiem opisanym w punkcie 9.4.2), które to hosty odsyłają w odpowiedzi raporty dotyczące swego członkostwa w grupach multicast.

Raporty takie „spontaniczne” raporty wysyłane są na adres IP reprezentujący wszystkie routery multicast, w IGMPv3 jest to adres **224.0.0.22**, a w MLDv2 — adres **ff02::16**. Zauważmy przy okazji, że routery multicast, oprócz realizacji opisanego przetwarzania, także mogą uzyskiwać członkostwo w grupach multicast.

W wersjach IGMPv1 i IGMPv2 host po otrzymaniu żądania nie udziela odpowiedzi natychmiast, lecz odczekuje losowy interwał czasu w nadziei, iż w międzyczasie wyręczy go w tym inny host tej samej grupy. Jak wcześniej wyjaśnialiśmy, dla pytającego routera obojętna jest informacja na temat liczebności grupy — jemu chodzi tylko o związki istniejących grup z jego poszczególnymi interfejsami i dla każdej grupy multicast rozstrzygnięcie dokonuje się na zasadzie dylematu „jest odpowiedź” albo „brak odpowiedzi”. Ten użyteczny mechanizm, notabene przyczyniający się do redukcji natężenia ruchu w sieci, został jednak zarzucony w wersji IGMPv3, z powodów wyjaśnionych w szczegółowo w punkcie 2. dodatku A do dokumentu [RFC3376]. Ujmując rzecz skrótowo, chodzi tu m.in. o  zapewnienie routerowi możliwości szczegółowego (na poziomie konkretnych hostów) śledzenia statusu członkostwa w grupach związanych z poszczególnymi interfejsami, co może być pomocne w implementacji szybkiego opuszczania grupy przez host (fast leave) oraz jest niezbędne dla zbierania informacji statystycznych, np. na potrzeby rozliczeń;  komplikację implementacji „podsluchiwania” IGMP (o którym piszemy w punkcie 9.4.7), wynikającą z konieczności zatrzymania forwardowania raportów IGMP między segmentami sieci LAN;  uproszczenie maszyny stanowej hosta — jeżeli jest on członkiem przynajmniej jednej grupy multicast, otrzymanie żądania IGMP skutkuje wysłaniem stosownego raportu, bez względu na kontekst innych hostów w grupie;  małą użyteczność całego mechanizmu w sytuacji, gdy wysyłany raport dotyczy członkostwa w wielu grupach multicast.

helion kopia dla: Michal Wojtusiak mwojtusiakbrzozowa5@gmail.com

7b7bd53ba5107cf5fb2c2a51dd887c95

7b7bd53ba5107cf5fb2c2a51dd887c95

9.4. Protokoły IGMP i MLD 485

Specyfikacje IGMPv3 oraz MLDv2 wymagają jednocześnie zgodności ze swymi poprzednimi wersjami w celu zapewnienia współpracy ze starszymi hostami i routerami rezydującymi w tej samej podsieci.

Przykłady

Na rysunku 9.12 widzimy efekt śledzenia pakietów związanych z protokołami IGMPv2, IGMPv3, MLDv1 i MLDv2 działającymi w tej samej podsieci. Śledzenie obejmuje 16 pakietów (na rysunku widoczne jest 10), z których pierwszy jest żądaniem pochodzącym z węzła (routera) identyfikowanego lokalnym dla łącza adresem fe80::204:5aff:fe9f:9e80 (w obu wersjach MLD format żądania jest identyczny). Ten sam węzeł formułuje jednocześnie żądania protokołu IGMP i identyfikuje się adresem IPv4 10.0.0.1.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	fe80::204:5aff:fe9f:9e80	ff02::1	ICMPv6	Multicast listener query (Unknown (0x00))
2	1.163826	fe80::fd26:de93:5ab7:405a	ff02::16	ICMPv6	Multicast Listener Report Message v2
3	1.549130	fe80::217:f2ff:fee7:6d91	ff02::2:7408:ff55	ICMPv6	Multicast listener report
4	3.149993	fe80::217:f2ff:fee7:6d91	ff02::1:ffe7:6d91	ICMPv6	Multicast listener report
5	4.150466	fe80::217:f2ff:fee7:6d91	ff02::fb	ICMPv6	Multicast listener report
6	5.059168	fe80::204:5aff:fe9f:9e80	ff02::16	ICMPv6	Multicast Listener Report Message v2
7	5.163634	fe80::fd26:de93:5ab7:405a	ff02::16	ICMPv6	Multicast Listener Report Message v2
8	6.108808	10.0.0.1	224.0.0.1	IGMP	V3 Membership Query, general
9	7.163508	fe80::fd26:de93:5ab7:405a	ff02::16	ICMPv6	Multicast Listener Report Message v2
10	7.653561	10.0.0.14	224.0.1.60	IGMP	V2 Membership Report / Join group 224.0.1.60

Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)

Ethernet II, Src: 00:04:5a:9f:9e:80 (00:04:5a:9f:9e:80), Dst: 33:33:00:00:00:01 (33:33:00:00:00:01)

Internet Protocol Version 6, Src: fe80::204:5aff:fe9f:9e80 (fe80::204:5aff:fe9f:9e80), Dst: ff02::1 (ff02::1)

0110 = Version: 6

.... 0000 0000 = Traffic class: 0x00000000

.... 0000 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000

Payload length: 36

Next header: IPv6 hop-by-hop option (0x00)

Hop limit: 1

Source: fe80::204:5aff:fe9f:9e80 (fe80::204:5aff:fe9f:9e80)

[Source SA MAC: 00:04:5a:9f:9e:80 (00:04:5a:9f:9e:80)]

Destination: ff02::1 (ff02::1)

Hop-by-Hop Option

Next header: ICMPv6 (0x3a)

Length: 0 (8 bytes)

Router alert: MLD (4 bytes)

PadN: 2 bytes

Internet Control Message Protocol v6

Type: 130 (Multicast listener query)

Code: 0 (Unknown)

Checksum: 0x5c73 [correct]

Maximum response delay[ms]: 10000

Multicast Address: ::

Rysunek 9.12. Pakiety protokołów IGMPv2, IGMPv3, MLDv1 i MLDv2 działających w tej samej podsieci. Wyróżniony pakiet jest żądaniem MLD

Wspomniane żądanie MLD (pakiet 1.) wysyłane jest na adres grupowy wszystkich węzłów (ff02::1); źródłowym adresem MAC jest 00:04:5a:9f:9e:80, docelowym 33:33:00:00:00:01 — to ilustracja opisanej wcześniej zasady konwersji adresów IP na adresy MAC (dla przypomnienia — w IPv6 prefiks 33:33 rozpoczyna sprzętowe adresy multicast, tak jak na rysunku 9.3). W polu Limit przeskoków znajduje się wartość 1, bo komunikaty MLD nie powinny być forwardowane poza lokalną sieć. Rozmiar ładunku użytecznego wynosi 36 bajtów — składają się nań: 8-bitowa opcja Router Alert, 4-bajtowy nagłówek ICMPv6 i 24 bajty „właściwych” danych MLD. Pola Typ, Kod, Suma kontrolna i Maksymalne opóźnienie odpowiedzi zajmują łącznie 8 bajtów ze wspomnianych 24, na 16 kolejnych znajduje się przedmiotowy adres IPv6 multicast, w tym przypadku 0 (mamy do czynienia z żądaniem generalnym).

1.4.13 ODPOWIEDŹ 9 IPv6

fec0:1::1 ->

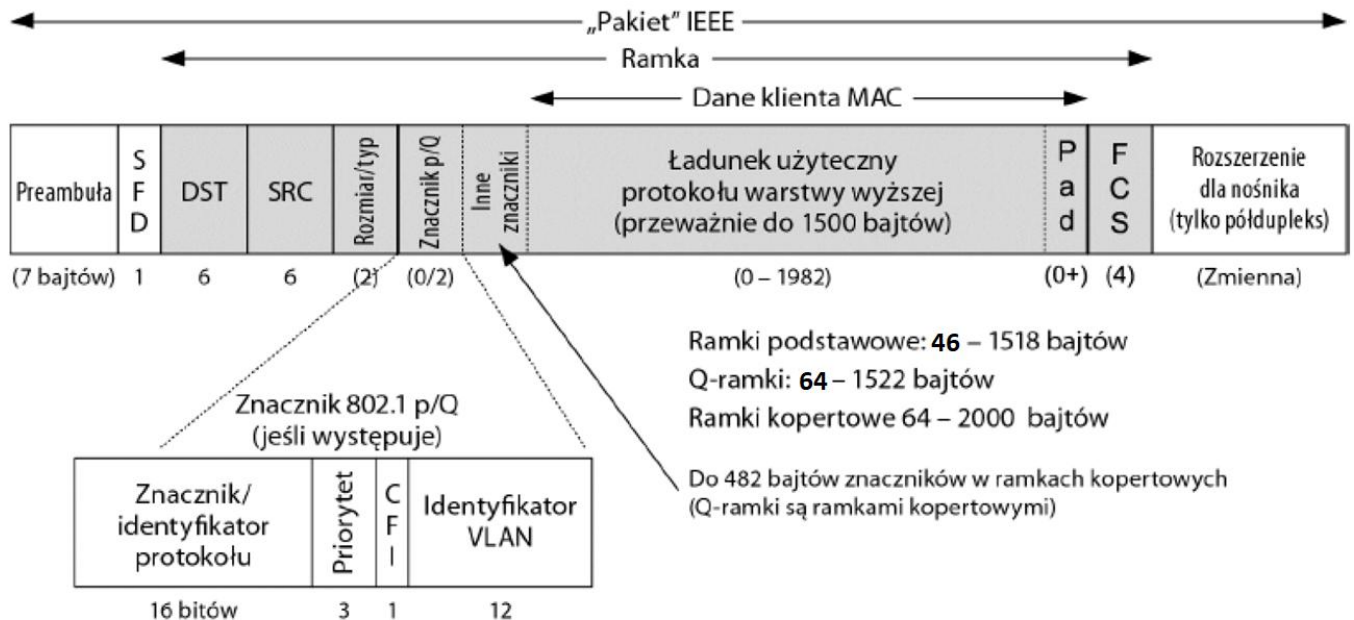
fec0:0001:0000:0000:0000:0000:0000:0001

fec0:1::fe ->

fec0:0001:0000:0000:0000:0000:0000:00fe

1.5 WARSTWA ŁĄCZA DANYCH

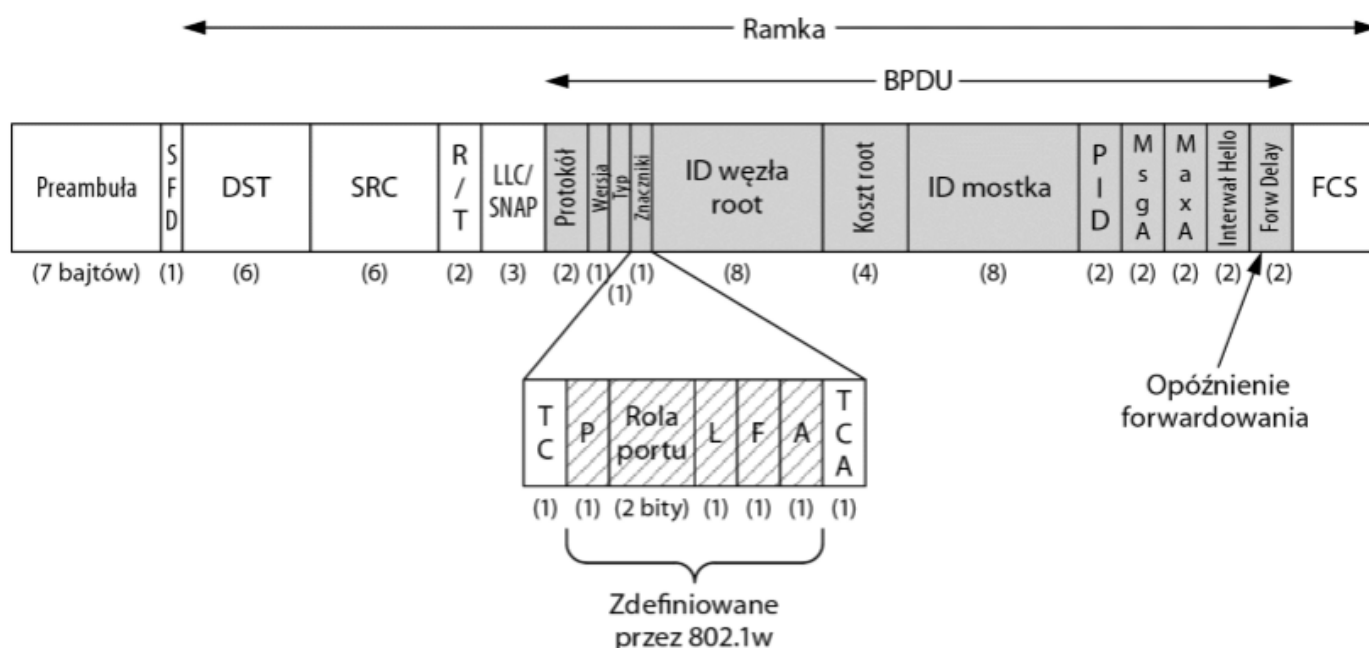
1.5.1 ODPOWIEDŹ 1 Budowa ramki Ethernet



- **Preambuła** - składa się z 7 bajtów złożonych z naprzemiennych jedynek i zer.
- **SFD** (ang. start frame delimiter), czyli znacznik początkowy ramki w postaci sekwencji 8 bitów (1 bajt).
- **Adres MAC odbiorcy** (6 bajtów).
- **Adres MAC nadawcy** (6 bajtów).
- **Rozmiar/Typ ramki** (2 bajty).
 - Jeżeli wartość tych dwóch bajtów jest mniejsza od wartości 1536 to pole "Typ ramki" informuje o wielkości ramki ethernetowej.
 - Jeżeli zaś wartość tych dwóch bajtów jest większa od wartości 1536 to pole "Typ ramki" informuje o ładunku użytecznym ramki
 - wartość 0x0800 identyfikuje protokół IPv4 jako ładunek użyteczny
 - wartość 0x86DD identyfikuje protokół IPv6 jako ładunek użyteczny
 - wartość 0x0806 identyfikuje protokół ARP jako ładunek użyteczny
- **Znacznik p/Q**
 - **Znacznik/identyfikator protokołu**: 16 bitowe pole wskazujące, że ta ramka danych jest tagowana. Domyślna wartość tagowanej ramki to liczba szesnastkowa 0x8100.
 - **Priorytet**: Złożony z 3 bitów pozwala utworzyć priorytety przesyłu dla pakietów w zakresie dziesiętnym od 0 - 7. Wartość 0 oznacza najniższy priorytet, a wartość 7 najwyższy.
 - **CFI** - (Canonical Format Indicator) - używany w celu zapewnienia kompatybilności sieci Ethernet z sieciami Token Ring
 - **Identyfikator VLAN** - określa przynależność do grypy VLAN
- **Inne znaczniki** - pole przyjmuje inne znaczniki do 482 bajtów w ramach kopertowych
- **Ładunek użyteczny** - bity danych protokołów warstwy wyższej (Network Layer) od 46 - 1500 bajtów. Jeżeli dane są mniejsze niż 46 bajtów, to są uzupełniane zerami (pole **Pad**)

- **FCS** (ang. Frame Check Sequence) - ciąg kontrolny ramki - zadaniem tego pola jest kontrola integralności informacji zawartej w ramce. Pole to zawiera 32-bitową sumę kontrolną, obliczaną dla całej zawartości ramki jako cykliczny kod nadmiarowy (CRC- Cyclic Redundancy Check)

1.5.2 ODPOWIEDŹ 2 Protokół STP – budowa ramki BPDU



Na powyższym obrazku przedstawiono format ramek BPDU, wymienianych między mostkami w ramach budowania drzewa rozpinającego przez protokół STP; jest to format wspólny dla obu wersji protokołów: klasycznej (STP) i ulepszonej (RSTP).

Ramki BPDU wysyłane są na adres grupowy 01:80:C2:00:00:00, a przejście ramki przez mostek zawsze wiąże się z jej modyfikacją.

Znaczenie pól DST, SRC i R/T jest takie samo jak w klasycznym formacie ramki ethernetowej 802.3 — pole R/T zawiera wartość 38 (dziesiętnie), czyli rozmiar ładunku użytecznego (rozpoczynającego się od pola LLC/SNAP).

W 3-bajtowym polu LLC/SNAP znajduje się stała 0x424203, zdefiniowana dla ramek BPDU przez standard 802.1 (niektóre ramki BPDU nie wykorzystują tego pola).

Pole Protokół ma wartość 0, pole Wersja zawiera 0 albo 2, zależnie od wersji protokołu (odpowiednio STP albo RSTP), na podobnej zasadzie ustalana jest wartość pola Typ.

W polu znaczników obecne są bity związane ze zmianą topologii sieci (zgodnie ze standardem 802.1d):

- TC — Topology Change i TCA — Topology Change Acknowledgment)
- propozycją (P — Proposal)
- rolą portu (00 — nieznana, 01 — alternatywny, 10 — główny, 11 — wyznaczony), uczeniem mostka (L — Learning), forwardowaniem ramek (F — Forwarding) i negocjowaniem (A — Agreement);
- ID węzła root to identyfikator domniemywany przez nadawcę ramki, zaś analogiczny identyfikator nadawcy znajduje się w polu ID mostka root; oba identyfikatory stanowią konkatencję 2-bajowego priorytetu i adresu MAC.

- Wartość w polu Koszt root wyliczana jest jako koszt drogi prowadzącej od mostka nadawcy do mostka root (koszt rozumiany jako suma kosztu łączy leżących na tej drodze).
- Identyfikator mostka ma kluczowe znaczenie w procesie wyboru mostka root, manipulowanie wspomnianym priorytetem (stanowiącym bardziej znaczącą część identyfikatora) jest podstawowym sposobem preferowania konkretnych mostków w tej roli przez oprogramowanie zarządzające
- W polu PID znajduje się identyfikator (numer) portu, przez który mostek nadawca wysłał ramkę, skonkatenowany z 1-bajtowym polem priorytetu (o domyślnej wartości 0x80).

Następne pola związane są z czasowymi uwarunkowaniami transmisji ramek:

- Pole **MsgA** zawiera wartość odzwierciedlającą upływ „czasu życia” ramki
- W polu **MaxA** definiowany jest interwał przeterminowania (domyślnie 20 sekund)
- Wartość pola **Interwał Hello** określa interwał czasowy ponawiania okresowej transmisji ramek konfiguracyjnych
- Wartość pola **Opóźnienie forwardowania (Forw Delay)** określa długość pozostawiania portu w stanie „uczący się” lub „nasłuchujący”.

Wszystkie wartości czasowe wyrażane są w jednostkach równych $1/256$ sekundy.

Pole **MsgA**, w odróżnieniu od innych pól czasowych, nie ma ustalonej wartości. W ramce BPDU wysyłanej przez mostek root pole ma to wartość 0; przy przejściu ramki przez każdy kolejny mostek wartość tego pola jest zwiększana o 1 (z wyjątkiem przypadku, gdy jej wysłanie następuje przez port uważany za prowadzący do mostka root). W rzeczywistości zatem pole to jest licznikiem przeskoków, czyli mostków pośrednich, przez które przeszła dotychczas ramka od momentu wygenerowania jej przez mostek root.

Gdy ramka BPDU odbierana jest przez mostek, zawarta w niej informacja gromadzona jest na potrzeby algorytmu STP i usuwana po okresie przeterminowania równym $\text{MaxA} - \text{MsgA}$ — jeżeli w tym czasie nie nadejdzie do mostka ramka przez port główny, dotychczasowy mostek root potraktowany zostaje jako „martwy” i ponownie uruchamiany jest proces jego elekcji.

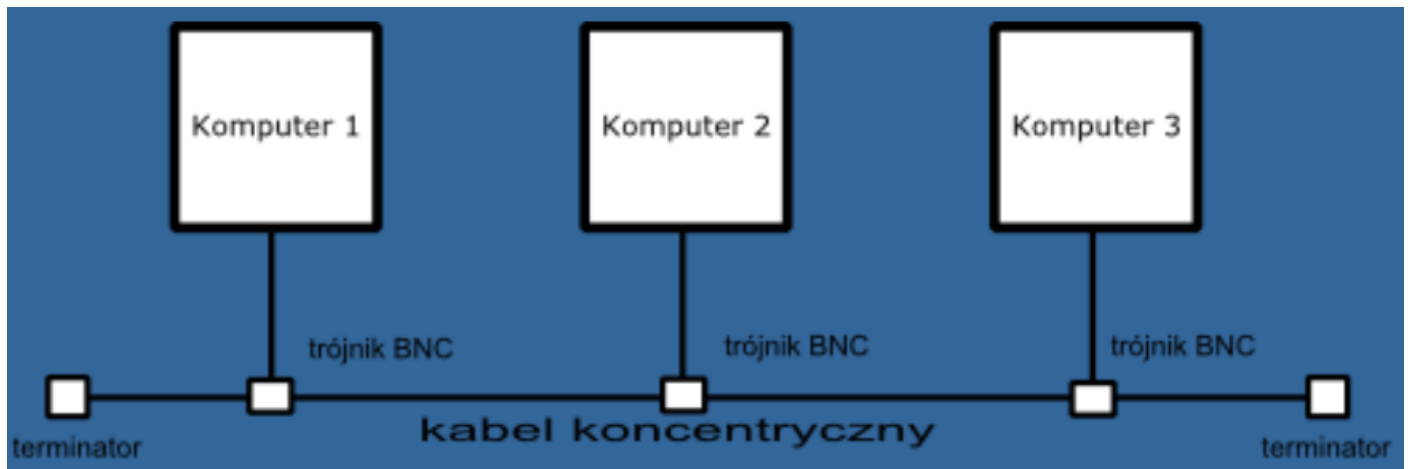
1.5.3 ODPOWIEDŹ 3 Protokół STP –Wireshark

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{D66E431E-47D0-4846-A72B-9051B6D9079D}, id 0
▼ IEEE 802.3 Ethernet
  ▼ Destination: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
    Address: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..1. .... = IG bit: Group address (multicast/broadcast)
  ▼ Source: HuaweiTe_64:11:80 (9c:74:1a:64:11:80)
    Address: HuaweiTe_64:11:80 (9c:74:1a:64:11:80)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
    Length: 39
    Padding: 0000000000000000
▼ Logical-Link Control
  ▼ DSAP: Spanning Tree BPDU (0x42)
    0100 001. = SAP: Spanning Tree BPDU
    .... ..0 = IG Bit: Individual
  ▼ SSAP: Spanning Tree BPDU (0x42)
    0100 001. = SAP: Spanning Tree BPDU
    .... ..0 = CR Bit: Command
  ▼ Control field: U, func=UI (0x03)
    000. 00.. = Command: Unnumbered Information (0x00)
    .... ..11 = Frame type: Unnumbered frame (0x3)
```

```
▼ Spanning Tree Protocol
  Protocol Identifier: Spanning Tree Protocol (0x0000)
  Protocol Version Identifier: Rapid Spanning Tree (2)
  BPDU Type: Rapid/Multiple Spanning Tree (0x02)
  ▼ BPDU flags: 0x7c, Agreement, Forwarding, Learning, Port Role: Designated
    0... .... = Topology Change Acknowledgment: No
    .1.. .... = Agreement: Yes
    ..1. .... = Forwarding: Yes
    ...1 .... = Learning: Yes
    .... 11.. = Port Role: Designated (3)
    .... ..0. = Proposal: No
    .... ...0 = Topology Change: No
  ▼ Root Identifier: 32768 / 0 / 9c:74:1a:64:11:80
    Root Bridge Priority: 32768
    Root Bridge System ID Extension: 0
    Root Bridge System ID: HuaweiTe_64:11:80 (9c:74:1a:64:11:80)
    Root Path Cost: 0
  ▼ Bridge Identifier: 32768 / 0 / 9c:74:1a:64:11:80
    Bridge Priority: 32768
    Bridge System ID Extension: 0
    Bridge System ID: HuaweiTe_64:11:80 (9c:74:1a:64:11:80)
    Port identifier: 0x8002
    Message Age: 0
    Max Age: 20
    Hello Time: 2
    Forward Delay: 15
    Version 1 Length: 0
```


2.01 Topologie sieci

Topologia magistrali (bus). Urządzenia końcowe podłączone są jednego medium transmisyjnego, którym kabel koncentryczny.



Kabel koncentryczny



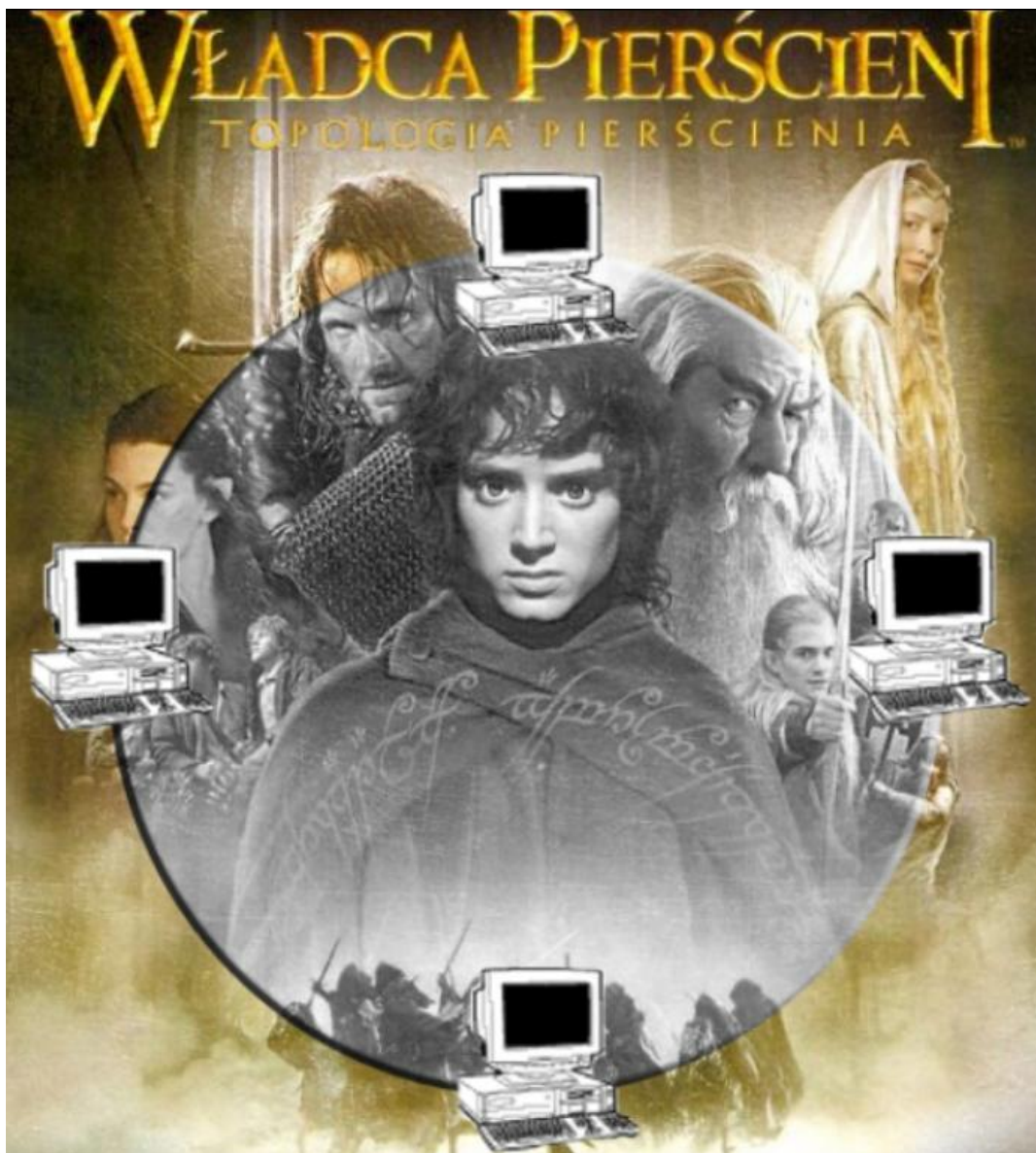
Trójnik do kabla koncentrycznego



Terminator BNC do kabla koncentrycznego

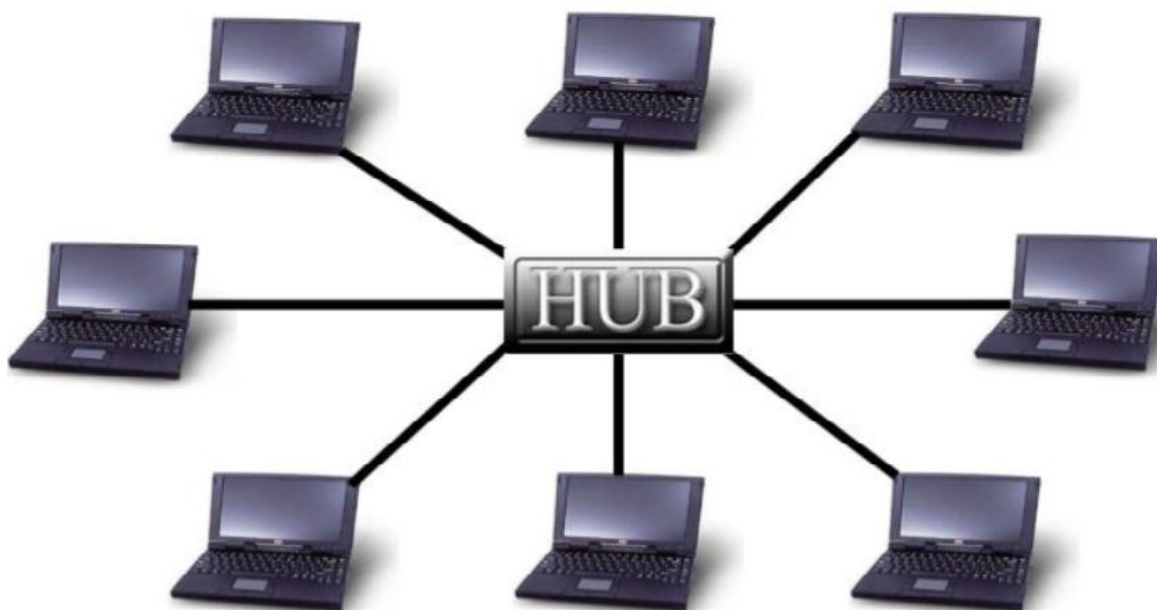


Topologia pierścienia

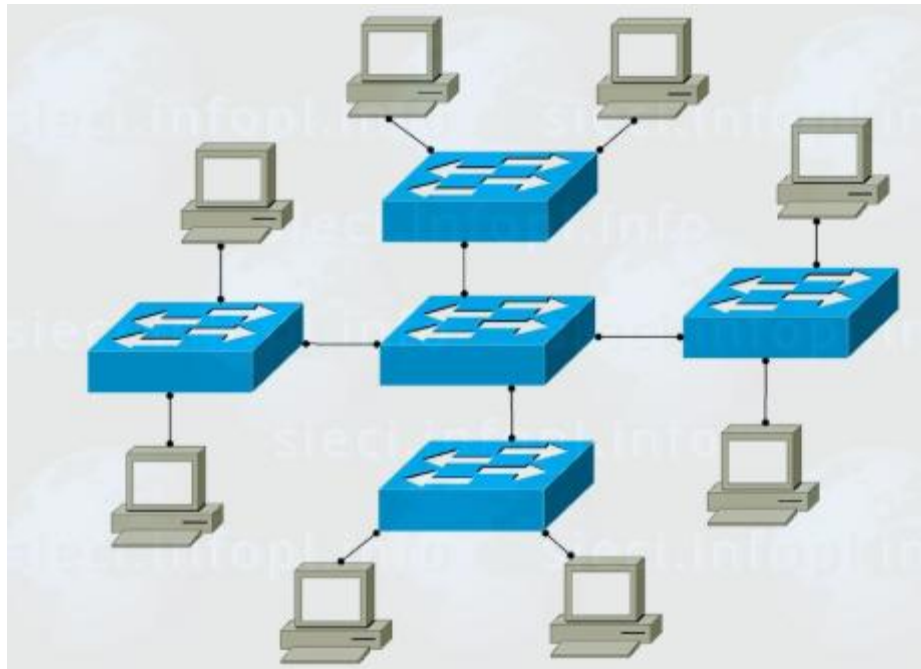


Topologia gwiazdy

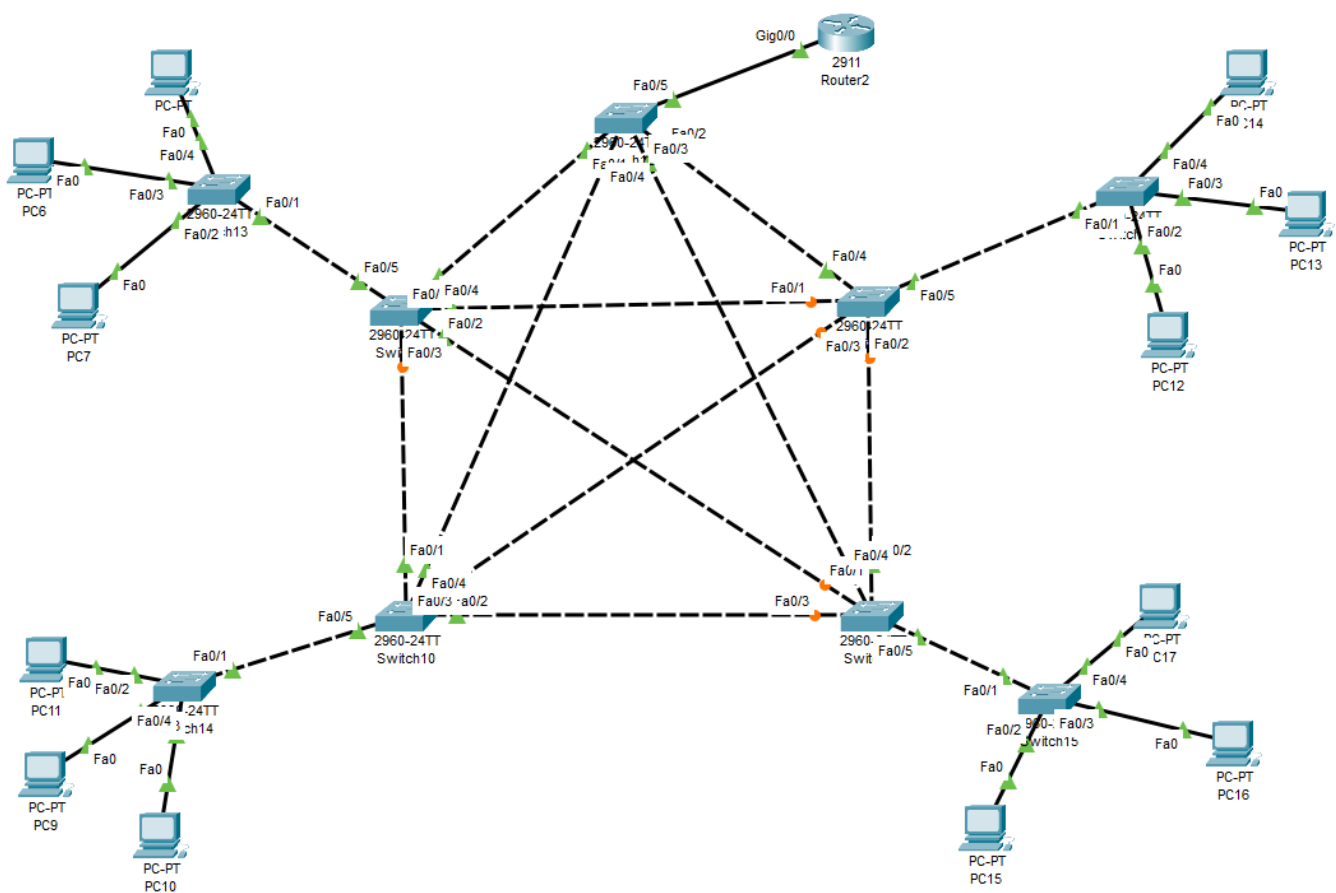
Topologia gwiazdy



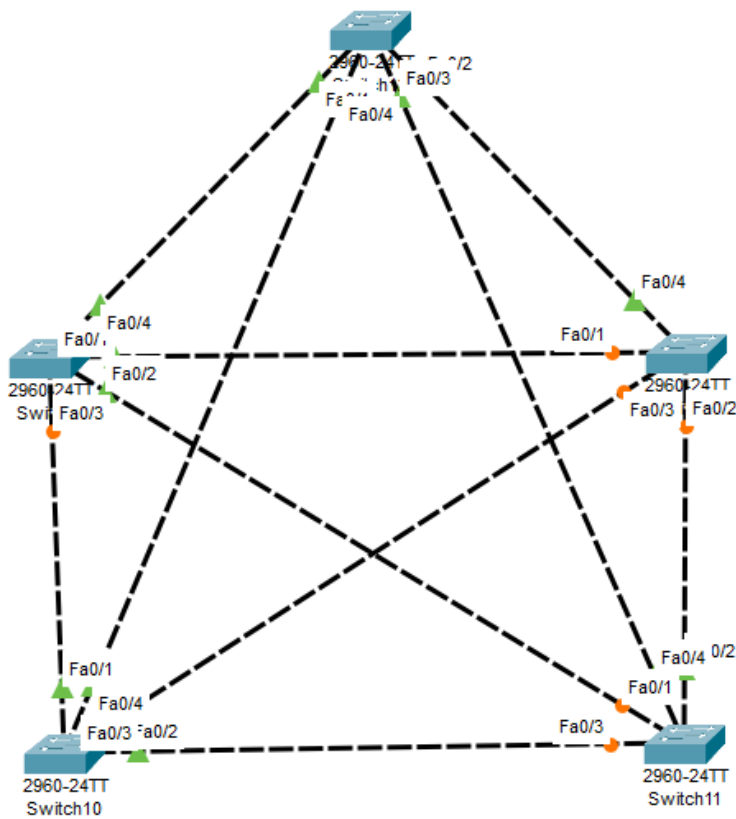
Topologia rozszerzonej gwiazdy



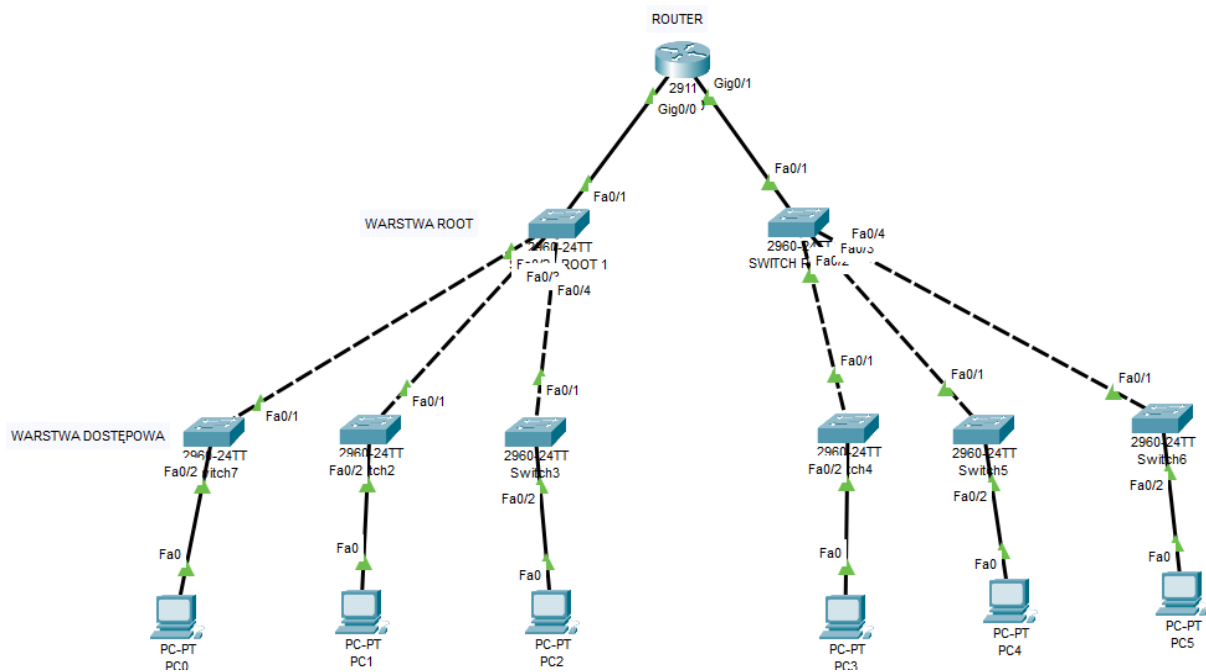
Topologia częściowej siatki



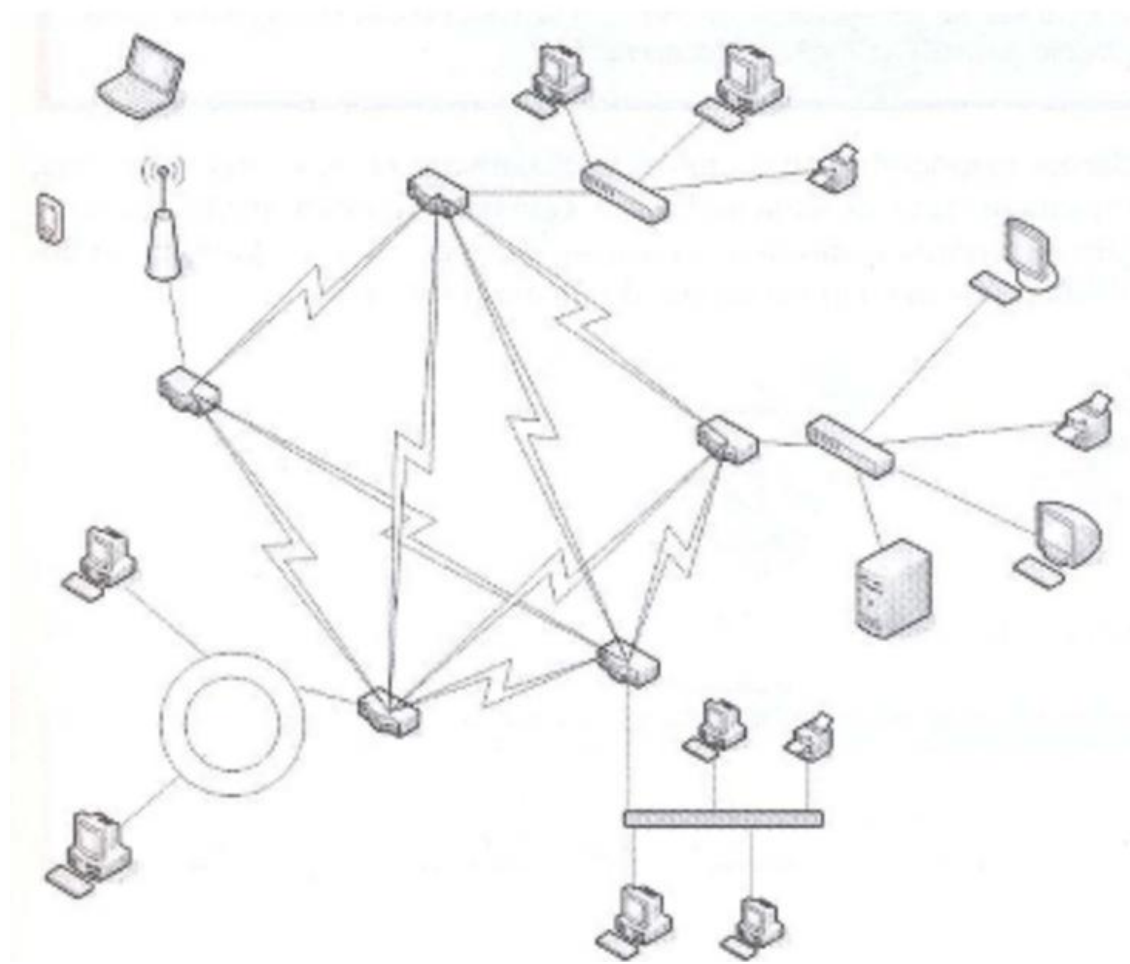
Topologia pełnej siatki



Topologia hierarchiczna



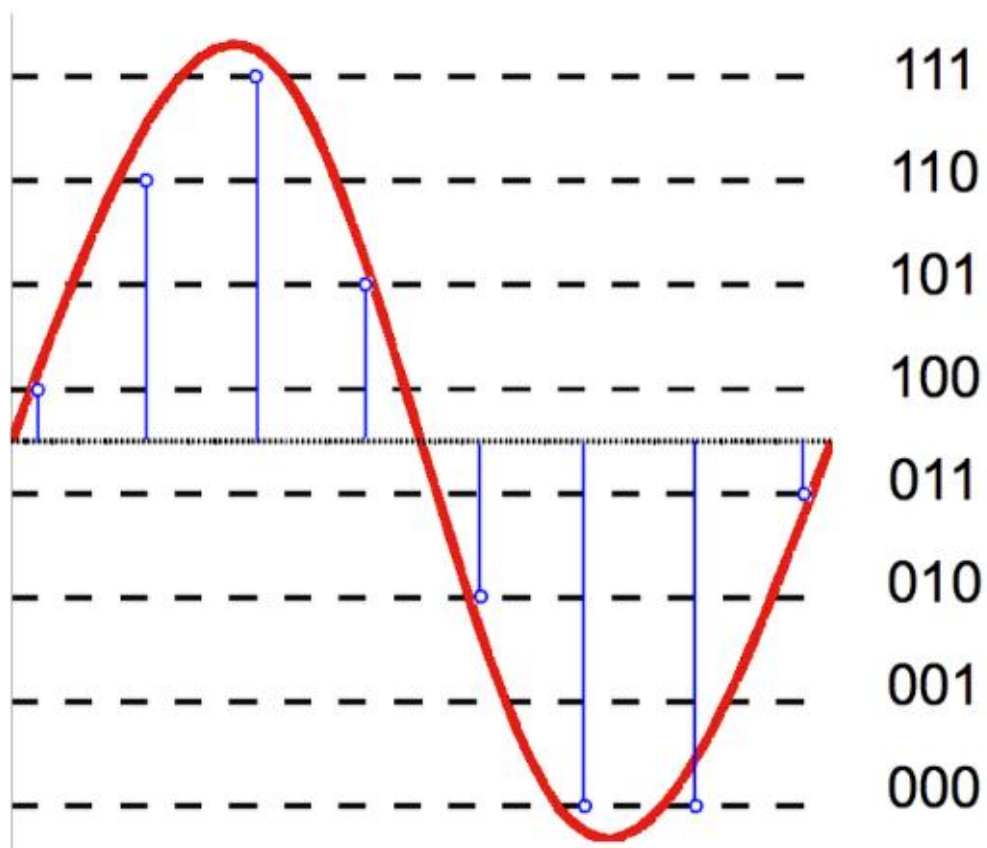
Topologia mieszana

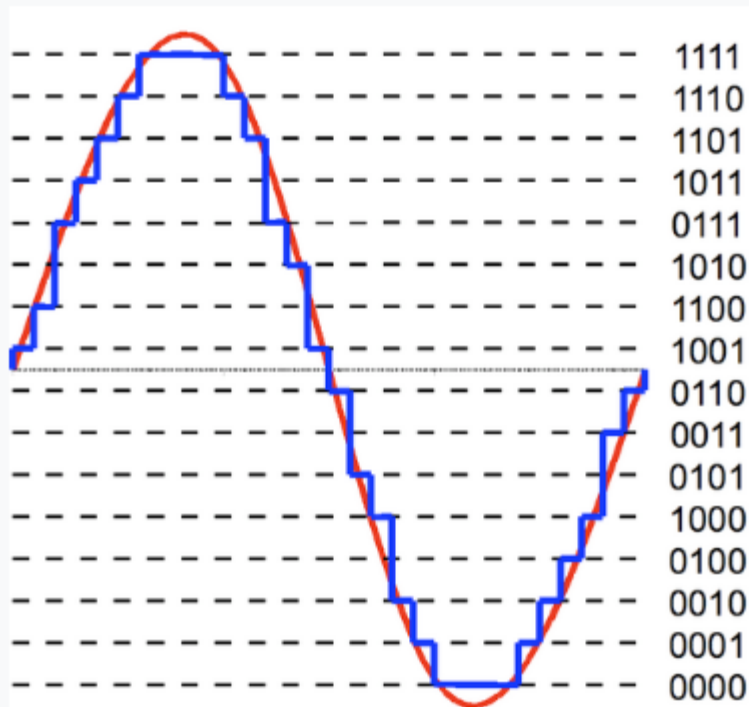
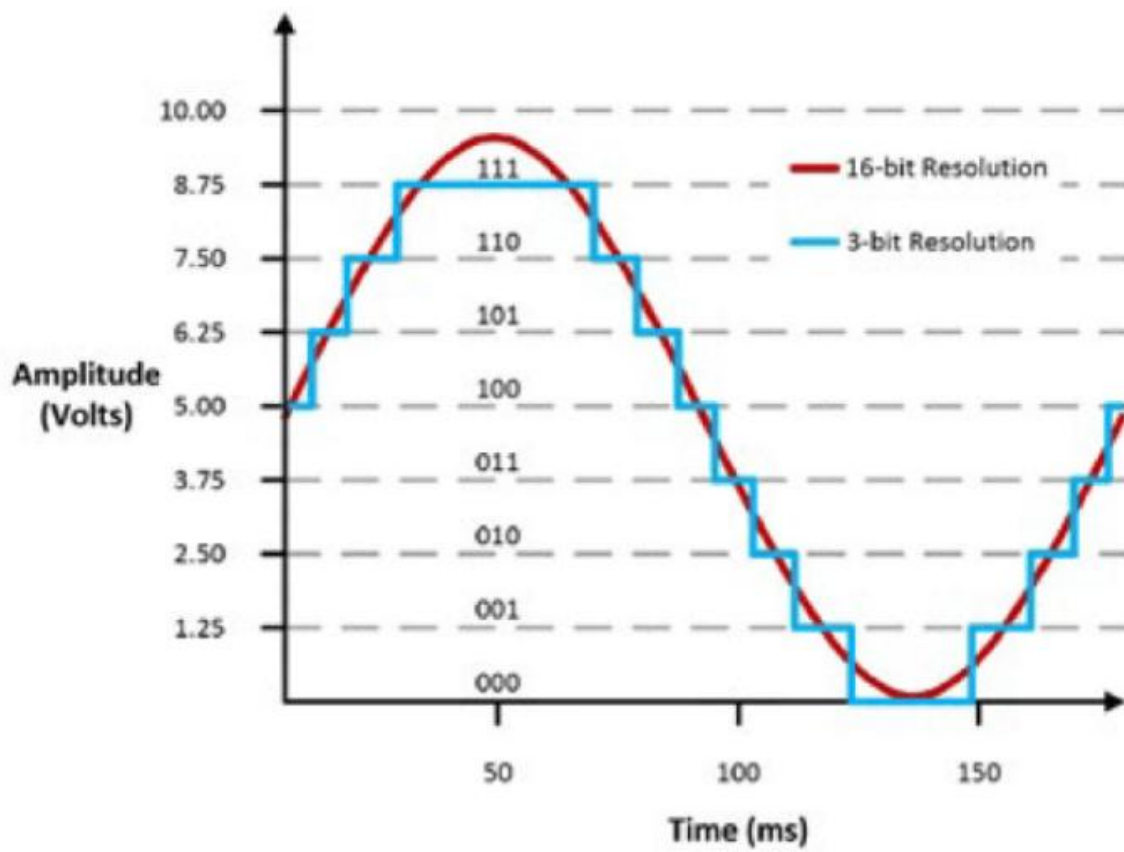


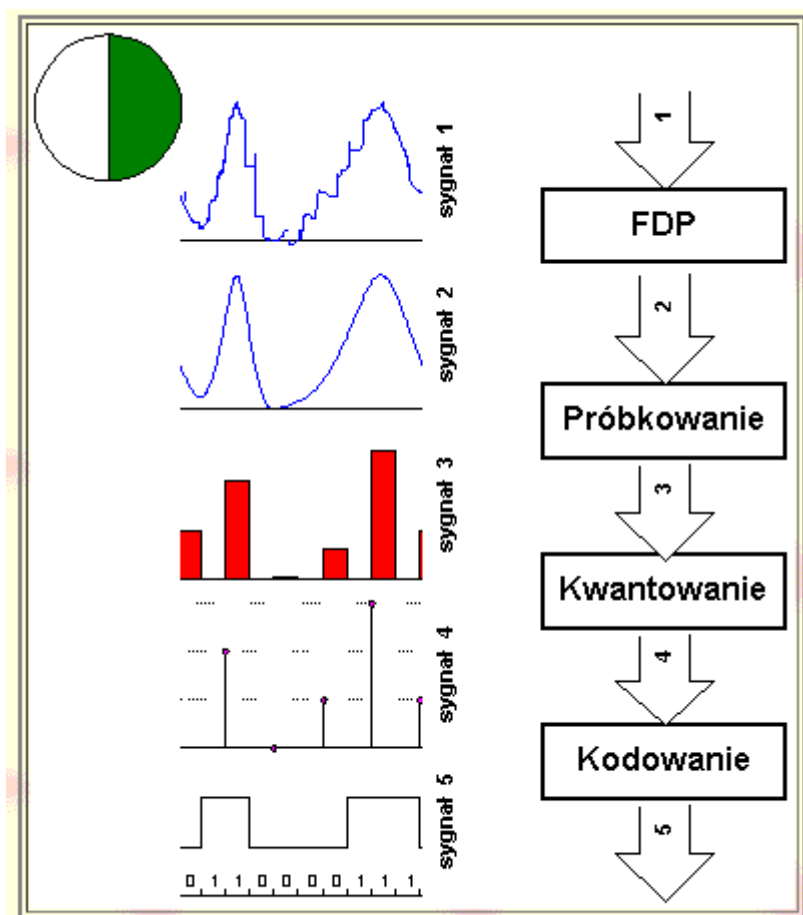
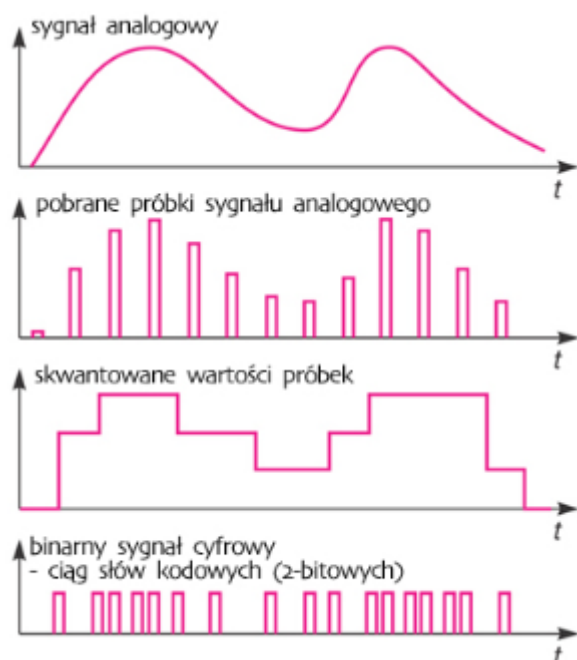
Przewodowe media transmisyjne

Typy sygnałów

Konwersja sygnału analogowego na cyfrowy

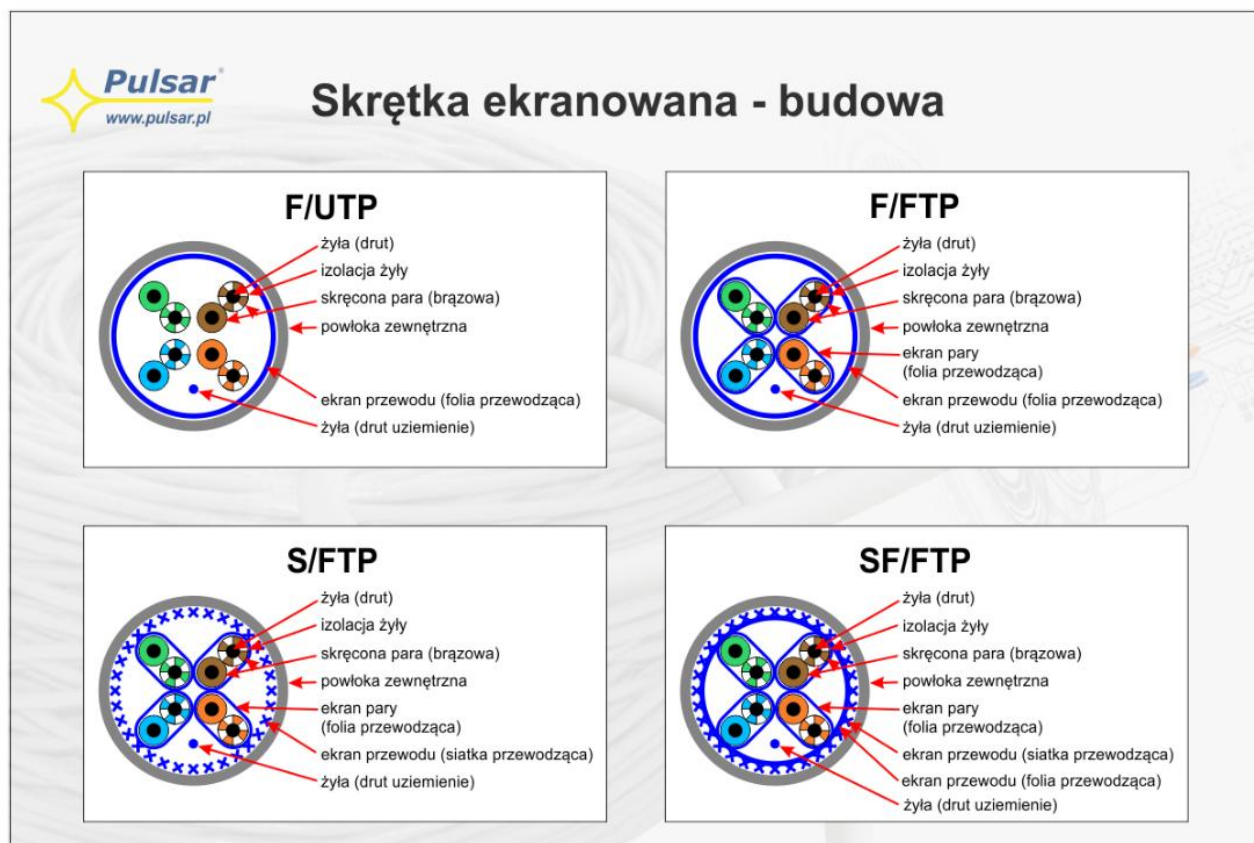
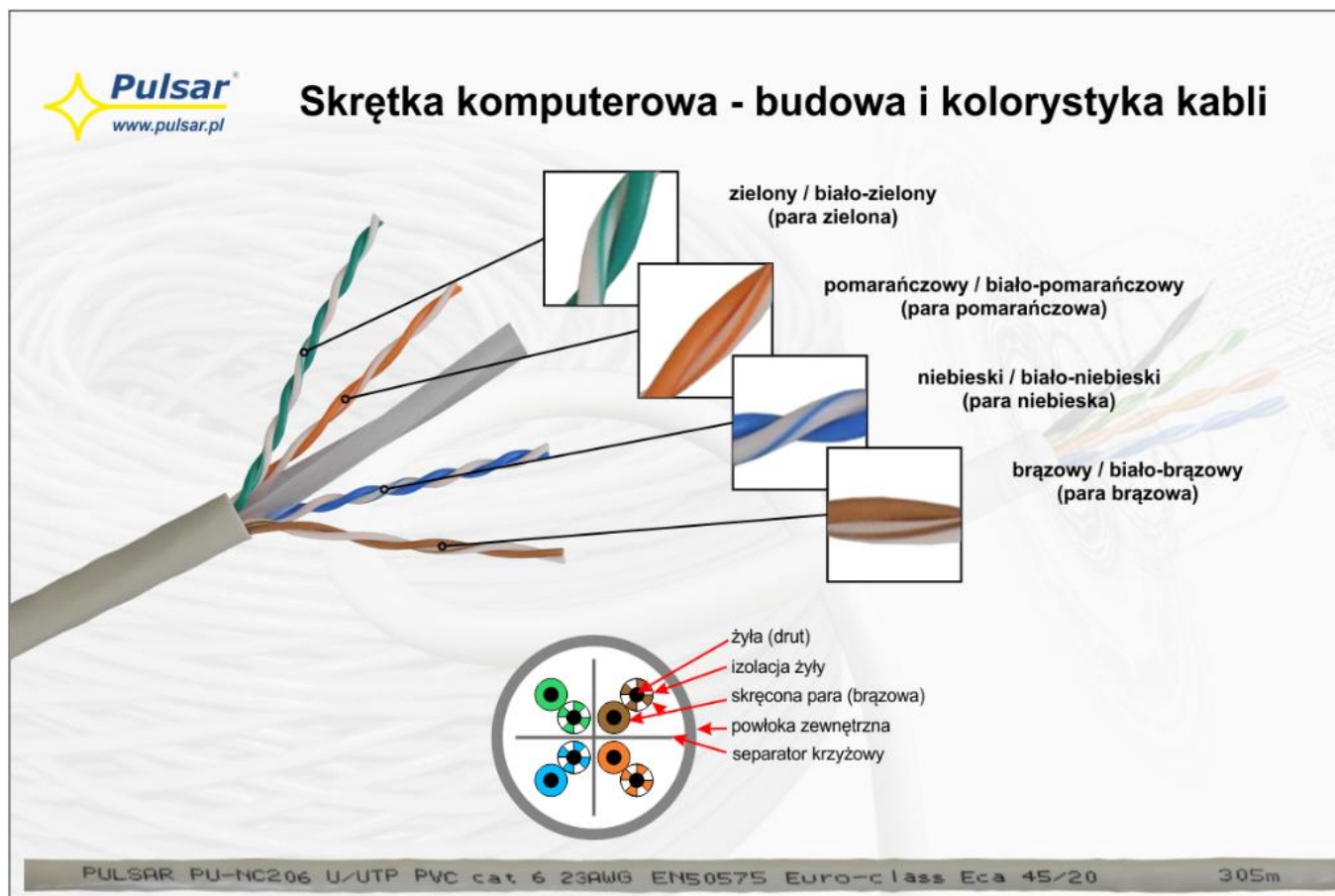




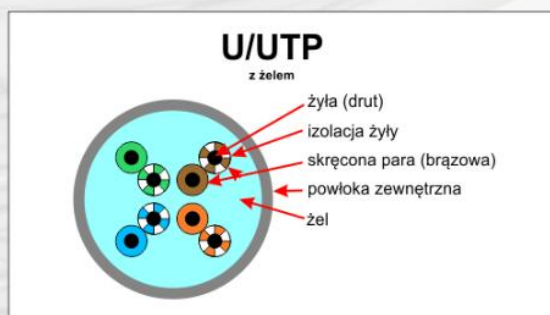
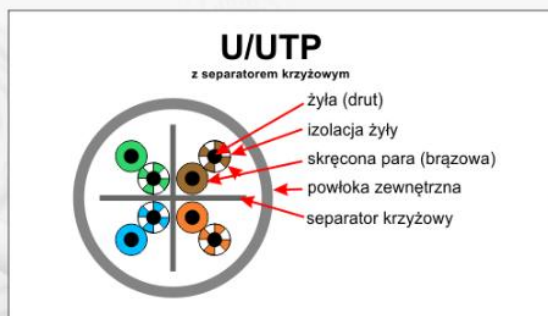
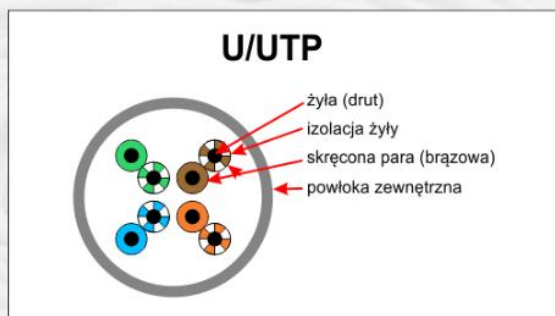


Modulacja kodowo impulsowa.

2.02 Skrętka miedziana - budowa



Skrętka nieekranowana - budowa



KATEGORIA			OPIS				PRZYKŁADOWY STANDARD
ISO	EIA/TIA	Częstotliwość	Minimalna przepustowość		Maksymalna przepustowość		
D	5	do 100 MHz	100 Mb/s	do 100m	100 Mb/s	do 100m	100Base-TX
D+	5e	do 100 MHz	1000 Mb/s	do 100m	1000 Mb/s	do 100m	1000Base-T
E	6	do 250 MHz	1000 Mb/s	do 100m	10Gb/s	do 55m	1000Base-T
EA	6A	do 500 MHz	1000 Mb/s	do 100m	10Gb/s	do 100m	10GBase-T
F	7	do 600 MHz	10Gb/s	do 100m	10Gb/s	do 100m	10GBase-T
FA	7A	do 1000 MHz	10Gb/s	do 100m	40Gb/s	do 100m	10GBase-T
Klasa1	8.1	1600-2000MHz	25Gb/s	do 30m	40Gb/s	do 30m	25GBase-T 40GBase-T
Klasa 2	8.2	1600-2000MHz	25Gb/s	do 30m	40Gb/s	do 30m	25GBase-T 40GBase-T

Oznaczanie kabli skrętki miedzianej



Skrętka miedziana i wymagania ochrony przeciwpożarowej

WYKONANIE: 1. KABEL LAN U/FTP kat.6a Solarix SXKD-6A-STP-LSOH-B2ca (500m)

SOLARIX



Kabel LAN U/FTP kat.6a Solarix SXKD-6A-STP-LSOH-B2ca (500m)

Kod produktu: 7075/5

2 172,18 zł

1 766,00 zł netto

Ilość

- 1 opak. +



NAPAWA
SLAM-Tech SYSTEMY Zabezpieczeń

Standaryzowana klasa palności B2ca w wariancie s1 d1 a1, a także osłona LSOH dodatkowo ograniczają powstawanie i rozprzestrzenianie się ognia i dymu w instalacji. Alumiowy ekran każdej z par przewodów oraz solidne uziemienie zapewniają niezakłóconą transmisję danych i umożliwiają zabezpieczenie toru transmisji przed wyładowaniami. Ponadprzeciętne wartości użytkowe przewodu SXKD 6A STP LSOH B2ca gwarantują efektywną i bezpieczną komunikację w ramach wspólnej sieci wymiany danych.

Standaryzowana jakość, której możesz zaufać

Przewód wyprodukowany został zgodnie z najwyższymi standardami produkcji oraz w oparciu o obowiązujące normy jakości i bezpieczeństwa użytkowania produktu. Zgodność z szeregiem regulacji gwarantuje wysoką efektywność oraz niezawodność pracy w docelowym środowisku instalacji.

ISO/IEC 11801

Uniwersalna specyfikacja systemów okablowania strukturalnego dla szerokiego zakresu aplikacji użytkowych.

IEC 61156-5

Ujednolicona specyfikacja przewodów posiadających zastosowanie w cyfrowej komunikacji systemów horyzontalnych dla transmisji do 1000 Mhz.

EN 13501

Przepisy klasyfikujące stopień reakcji na ogień dla przewodów elektrycznych wykorzystywanych w obiektach budowlanych.

EN 50173

Regulacje z zakresu techniki informatycznej kształtujące generalne wymogi przewidziane dla systemów okablowania strukturalnego.

EN 50288

Grupowe wymagania ekranowanych kabli telekomunikacyjnych do częstotliwości 500 Mhz, stosowanych w instalacjach wewnątrz obiektu.

EN 50575

Wytyczne dla przewodów elektrotechnicznych mających zastosowanie w obiektach budowlanych o określonej klasie odporności pożarowej.

EN 60332-1

Zalecenia regulujące standard oceny ogniowej związanej z odpornością kabli i przewodów elektrycznych oraz światłowodowych.

EN 60754

Standaryzowane wytyczne toksyczności dla kabli lokowanych w ramach instalacji o zwiększonym poziomie ochrony przeciwpożarowej.

EN 61034

Zestawienie optymalnych wartości dla przewodów ograniczających gęstość dymów wydzielanych w trakcie procesu spalania.

ANSI/TIA 568.2-D

Zestaw norm kształtujących struktury okablowania w obiektach komercyjnych wraz z parametrami komponentów transmisyjnych dla kategorii 5e.

EN 13501 – KLASYFIKACJA MATERIAŁU POD WZGLĘDEM REAKCJI NA OGIEŃ

Kabel skrętka miedziana cat. 5e U/UT



Dane techniczne:

- Producent: **NEKU**
- Symbol: **01.0203**
- Kategoria: **5e**
- Klasa: **D**
- Konstrukcja (ekranowanie): **U/UTP**
- Typ kabla: **wewnętrzny**
- Przekrój AWG: **4x2x24AWG**
- Przepustowość binarna (max): **1 Gb/s**
- Pasmo częstotliwości (max): **100 MHz** (rozszerzona charakterystyka do **155 MHz**)
- Klasyfikacja ogniowa CPR (Euroklasa): **Eca**
- Średnica zewnętrzna: **4,6 mm**
- Promień zgięcia : **4 x średnica kabla**
- Zakres temp. podczas użycia: **-30°C do +70°C**
- Zakres temp. podczas instalacji: **-10°C do +50°C**
- Waga nominalna: **26 kg/km**
- Indeks miedziowy: **14 kg/km**

Budowa:

- **Żyły:** jednodrutowe z miedzi elektrolitycznej o średnicy 0,5mm (24AWG)
- **Izolacja żył:** specjalna mieszanka poliolefinowa
- **Ośrodek:** 4 pary skręcone
- **Powłoka zewnętrzna:** polwinil oponowy PVC
- **Przegroda par:** nie
- **Kolor powłoki:** szary (RAL 7035)

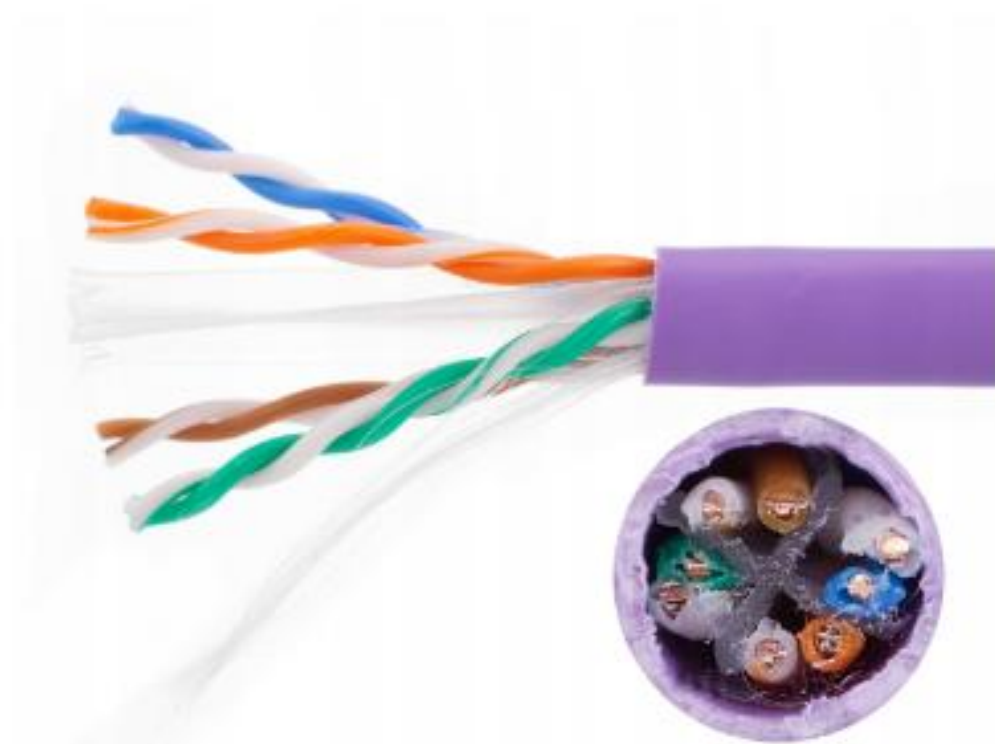


Właściwości elektryczne:

- Rezystancja pętli żyły/pary w temp. 20°C (max): **190 Ω /km**
- Rezystancja izolacji (min): **5 $G\Omega$ /km**
- Asymetria rezystancji żył w parze: **$\leq 2\%$**
- Pojemność skuteczna dowolnej pary przy 1kHz: **50 ± 5 nF/km**
- Asymetria pojemności torów transmisyjnych względem ziemi przy 1 kHz (max): **1600 pF/km**
- Napięcie pracy: **150 V**
- Próba napięciowa (AC): **700 VAC**
- Próba napięciowa (DC): **1000 VDC**
- Impedancja falowa: **100 ± 5 Ω**
- Prędkość propagacji NVP: **69%**
- Tłumienność odbiciowa (częst. 4-10MHz): **20+5•lg(f) dB**
- Tłumienność odbiciowa (częst. 10-20MHz): **25 dB**
- Tłumienność odbiciowa (częst. 20-155MHz): **25-7•lg(f/20) dB**

Kabel skrętka miedziana cat. 6 U/UTP





Na tej aukcji przewód sprzedawany jest na metry.

(Np. kupując 45 sztuk - otrzymasz 45 metrów bieżących w jednym odcinku)

Na innych naszych aukcjach kabel dostępny także w gotowych odcinkach 50, 100 , 305 i 500m

Kable instalacyjne U-UTP kategorii 6 firmy DIGITUS® są produkowane i testowane zgodnie ze specyfikacją norm ISO/IEC 11801, DIN EN 50173 i DIN EN 50288-5-1 kategorii 6. Każdy kabel składa się z 8 żył izolowanych polietylenem z kodem kolorów AWG 23. Informacje nadrukowane na zewnętrznym płaszczu kabla zawierają nazwę marki, kod przedmiotu i długość kabla.

- NVP: 69%
- Kategoria: CAT 6
- Kolor: fioletowy
- CPR: Eca
- Ekranowanie: U-UTP, nieekranowany
- AWG: 23



Właściwości fizyczne:

- Przewód: **AWG 23/1**, goły drut miedziany, **średnica 0,57 mm** nom.
- Izolacja: HD-PE
- Liczba wszystkich izolowanych przewodów: **8, skrócone w 4 parach**
- Grubość płaszczu zewnętrznego: 0,50 mm nominalnie
- Kolor: **fioletowy (RAL 4005)**

Właściwości mechaniczne:

- Obciążenie rozciągające: 150 N maks.
- Promień gięcia dynamicznego: 8x AD mm min.
- Statyczny promień gięcia: 4x AD mm min.
- Zakres temperatur podczas transportu i składowania: -20 do +60 °C
- Zakres temperatury roboczej: -20 °C do +75 °C
- Zakres temperatur przy instalacji: 0°C do +50 °C
- Średnica zewnętrzna pasa: 6,0 mm nominalnie



Przewód musi mieć promień gięcia o długości co najmniej 8-krotnej średnicy przewodu. Im większy promień, tym mniejszy nacisk wywierany jest na przewody, co zapewnia dłuższą żywotność.

Molex kabel przewód skrętka Cu UTP kat.6 drut LSOH 500m

Kabel najwyższej jakości, z solidną **powłoką nierozprzestrzeniającą płomienia LSOH / LSZH**, grubymi żyłami w 100% miedzianymi i bardzo dobrymi parametrami transmisyjnymi.

Produkt oryginalny, znanego światowego koncernu. Symbol producenta: CAA-00325

Parametry mechaniczne:

- Średnica przewodnika [mm]: **23 AWG (0.57 mm)**
- Średnica przewodnika w izolacji [mm]: ≤ 1.0
- Ekran wokół pojedynczej pary: brak
- Liczba par: 4
- Ekran wokół kabla: brak
- Element centralny: **Separator krzyżowy rozdzielający pary**
- Zewnętrzna średnica kabla [mm]: ≤ 6.3



Temperatura pracy: -20 do +60 °C; w czasie pracy: -20 do +60 °C
Wytrzymałość na rozciąganie: 8 razy średnica kabla; w czasie pracy:
Średnica kabla
Materiał powłoki: **LSOH (IEC332.3C)**
Kolor powłoki: **fioletowy (RAL 4005)**
Ciężar z opakowaniem szpula 500m [kg]: 22.5
Ciężar maks.[N]: 100

Średnica kabla
Długość
Instalacja
4 razy
Materiał
Kolor
Waga
Napięcie

ZASTOSOWANIE:

Kabel U/UTP PowerCat 6 jest częścią kompletnej oferty PowerCat 6 spełniającej a nawet **przewyższającej wymagania kategorii 6** (TIA/EIA 568B.2-1) oraz klasy E (ISO 11801:2002 ; EN50173-1:2007).

Kabel posiada specjalny **separator krzyżowy** rozdzielający poszczególne pary między sobą co pozwala poprawić parametr **NEXT i ELFEXT** jak również zapewnia dużą odporność na błędy instalacyjne (dzięki dużemu odstępowi parametrów faktycznych od parametrów nominalnych wymaganych przez normę). Produkt jest przeznaczony do instalowania w okablowaniu poziomym oraz pionowym przeznaczonym do przesyłu danych.

Powłoka kabla wykonana jest z niepalnego, samogasnącego tworzywa o statusie LSZH (Low Smoke Zero Halogen) – materiał podczas spalania wydziela nieznaczłą ilość dymu który dodatkowo nie zawiera tzw. halogenków.

Mała średnica zewnętrzna kabla, wysoka elastyczności i doskonałe parametry transmisyjne należą do głównych zalet produktu. Kabel dostarczany jest w 500m odcinkach nawijanych na drewniane szpule, które ułatwiają prace instalacyjne oraz minimalizują zgięcia/naprężenia w kablu. Szpule mogą być bezpiecznie utylizowane w procesie recyklingu.



Parametry elektryczne:

- Impedancja charakterystyczna [Ω]: 100 ± 6 @ 1-250 MHz 100 ± 15 @ 250-300 MHz
- Rezystancja [Ω/Km]: 72 max.
- Tolerancja rezystancji [%]: 2 max.
- Pojemność [pF/m]: 45 nom. @ 1 KHz
- Niezrównoważeni pojemności (przewodnik względem ziemi) [pF/Km]: 1500 max. @ 1 KHz.
- Max. napięcie [Vdc]: 72 max.
- Wytrzymałość dielektryczna: 1500 Volt/1 minute min rms
- NVP: 68%
- Delay Skew [$\text{nS}/100\text{m}$]: 45 max. @ 1-250 MHz
- Rezystancja izolacji [$\text{M}\Omega \cdot \text{Km}$] 5000 min. @ 500 Vdc
- Tłumienność: 45 dB min @ 30-100 MHz $40 - 20\text{Log}(f/100)$ @ 100-250 MHz



Parametry transmisyjne:

- Insertion Loss[1-250Hz] $\leq 1.808 \cdot \sqrt{f} + 0.017 \cdot (f) + 0.2/\sqrt{f}$ dB/100m
- NEXT[1-250MHz] $\geq 44.3 - 15 \cdot \log(f/100)$ dB
- PS NEXT [1-250MHz] $\geq 42.3 - 15 \cdot \log(f/100)$ dB
- EEXT [1-250MHz] $\geq 27.8 - 20 \cdot \log(f/100)$ dB
- PS EEXT [1-250MHz] $\geq 24.8 - 20 \cdot \log(f/100)$ dB
- RL [$1 \leq f < 10\text{MHz}$] $20 + 5 \cdot \log(f)$ dB
- RL [$10 \leq f < 20\text{MHz}$] 25 dB
- RL [$20 \leq f \leq 250\text{MHz}$] $\geq 25 - 7 \cdot \log(f/20)$ dB
- Propagation Delay[1-250MHz] $\leq 534 + 36/\sqrt{f}$ ns/100
- Delay Skew[1-250MHz] ≤ 45 ns/100
- LCL[1-250MHz] $\geq 30 - 10 \cdot \log(f/100)$ dB

Standardy branżowe:

- TIA/EIA 568B.2-1
- ANSI/TIA-568-C.2
- ISO 11801:2002
- EN50173:2007
- IEC 61156-5
- IEC 60332-1-2 (332.1)
- EN50288-5

Firma **Molex** od ponad 30 lat dostarcza firmom z całego świata wysokiej jakości rozwiązania z dziedziny przesyłania sygnału głosu, danych i obrazu wideo przez przewody miedziane, światłowodowe oraz bezprzewodowo, a marka Molex Premise Networks (obecnie Molex Connected Enterprise Solutions) stała się synonimem wysokiej jakości, innowacyjności i trwałości.

Rozbudowane portfolio produktów oraz podejście koncentrujące się na usługach doradczych odegrały zasadniczą rolę w odniesieniu przez firmę sukcesu na skalę globalną – dzięki temu takie rozwiązania stosuje coraz więcej liczących się firm z całego świata.

The Molex logo is displayed in a bold, red, sans-serif font. The word "molex" is in lowercase, and a registered trademark symbol (®) is located at the top right of the letter "x".

Kabel skrętka miedziana cat. 6A F/UTP



Kabel skrętka F/UTP kat.6 4x2x0,56 (23AWG) wewnętrzny drut Dca LSOH szary NEKU

Ekranowany przewód **F/UTP** marki NEKU przeznaczony do budowy sieci komputerowych spełniających wymogi **kategorii 6** oraz pracujących w częstotliwości do **250MHz**.

Kabel charakteryzuje się najwyższą jakością oraz doskonałymi parametrami. Pozwala na transmisję danych, dźwięku i obrazu telewizyjnego o przepustowości binarnej **powyżej 1Gb/s** (w zależności od długości nawet 10Gb/s). Posiada bezhalogenową powłokę **LSOH** oraz żyły wykonane w **100% z miedzi** o średnicy **23AWG**. Został sklasyfikowany zgodnie z euroklasą **Dca**.

Przeznaczony do wykonywania instalacji **wewnętrznych poziomych i pionowych** w sieciach teleinformatycznych **narażonych** na oddziaływanie zakłóceń elektromagnetycznych. Najczęściej wykorzystywany w instalacjach komputerowych, telefonicznych, alarmowych oraz CCTV.



Charakterystyka:

- Producent: **NEKU**
- Symbol: **01.0250**
- Kategoria: **6**
- Klasa: **E**
- Konstrukcja: **F/UTP**
- Typ kabla: **wewnętrzny**
- Przekrój AWG: **4x2x23AWG**
- Przepustowość binarna: **1-10 Gb/s** (w zależności od długości)
- Pasma częstotliwości (max): **250 MHz**
- Klasyfikacja ogniowa CPR (Euroklasa): **Dca**
- Normy: **EN 50173, ISO/IEC 11801, ANSI/TIA 568.2-D**
- Temperatura instalacji: **0°C do +50°C**
- Temperatura pracy: **-20°C do +60°C**
- Średnica zewnętrzna (przybliżona): **7,6 mm**
- Waga: **56 kg/km**

Budowa:

- **Żyły:** miedziane jednodrutowe Cu Ø 0,56 mm (23AWG)
- **Izolacja:** polietylen o wysokiej gęstości HDPE Ø 1,06 mm
- **Powłoka:** tworzywo bezhalogenowe nierozprzestrzeniające płomienia, o ograniczonym wydzielaniu dymu oraz gazów korozyjnych (LSOH/FRNC) Ø 7,6 mm
- **Ośrodek:** 4 pary skręcone na wkładce rdzeniowej w kształcie krzyża, owinięte folią PET oraz folią aluminiową
- **Ekran:** folia aluminiowa, pod ekranem żyła uziemiająca z drutu miedzianego ocynowanego o średnicy min. 0,4 mm (26AWG)
- **Warstwa rozdzielająca:** folia PET
- **Rip cord:** tak
- **Kolor powłoki:** szary



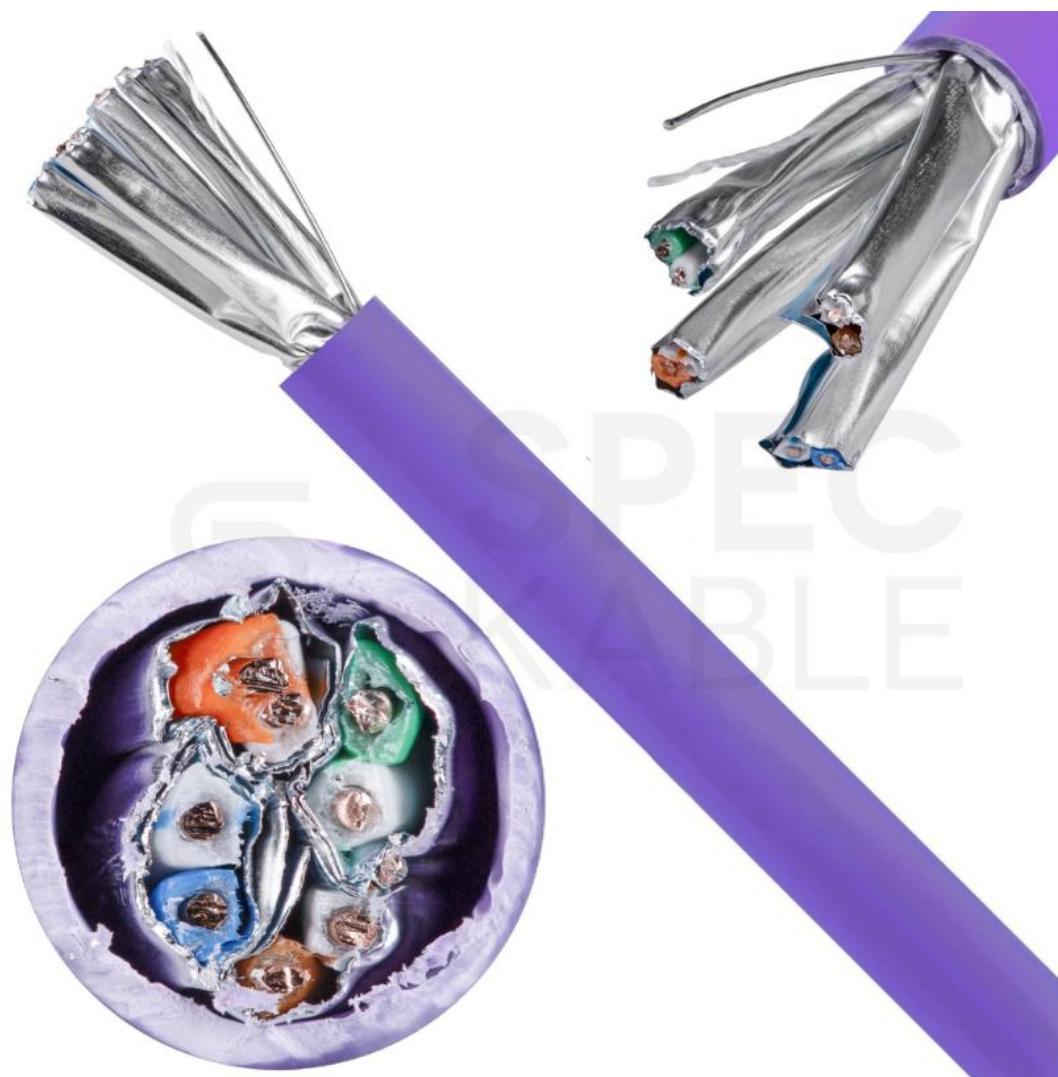
Właściwości mechaniczne:

- Maksymalna siła naciągu: **≤100 N**
- Wydłużenie przewodnika: **≥15%**
- Wytrzymałość na rozciąganie (powłoka przed starzeniem): **≥8,3 MPa**
- Wydłużenie (powłoka przed starzeniem): **≥100%**
- Wytrzymałość na rozciąganie (powłoka po starzeniu 100°C, 24×2h): **≥75% × wytrzymałość przed starzeniem**
- Wydłużenie (powłoka po starzeniu 100°C, 24×2h): **≥75% × wydłużenie przed starzeniem**

Właściwości elektryczne:

- Impedancja w zakresie 4-250 MHz: **100 ± 15 Ω**
- Asymetria rezystancji (DC): **max. 5%**
- Rezystancja przewodnika przy 20°C (DC): **≤73,2 Ω/km**
- Asymetria pojemności pary względem ziemi: **≤330 pF/100m**
- Rezystancja izolacji: **>5000 MΩxkm**
- Wytrzymałość dielektryczna: **DC 2500V przez 2 sekundy**

Kabel skrętka miedziana cat. 6A U/FTP



Kabel skrętka U/FTP kat.6A 4x2x0,56 (23AWG) wewnętrzny drut Dca LSOH fioletowy NEKU

Ekranowany przewód **U/FTP** marki NEKU przeznaczony do budowy sieci komputerowych spełniających wymogi **kategorii 6A** oraz pracujących w częstotliwości do **500MHz**.

Kabel charakteryzuje się najwyższą jakością oraz doskonałymi parametrami. Pozwala na transmisję danych, dźwięku i obrazu telewizyjnego o przepustowości binarnej **do 10Gb/s** (na odległości do 100m). Posiada bezhalogenową powłokę **LSOH** oraz żyły wykonane w **100% z miedzi** o średnicy **23AWG**. Został sklasyfikowany zgodnie z euroklasą **Dca**.

Przeznaczony do wykonywania instalacji **wewnętrznych poziomych i pionowych** w sieciach teleinformatycznych **narażonych** na oddziaływanie zakłóceń elektromagnetycznych. Najczęściej wykorzystywany w instalacjach komputerowych, telefonicznych, alarmowych oraz CCTV.

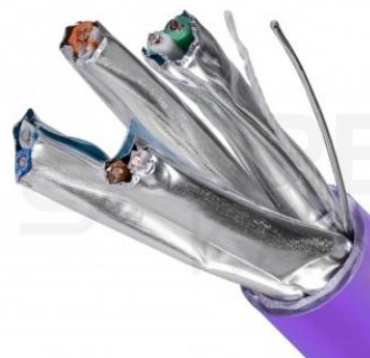


Charakterystyka:

- Producent: **NEKU**
- Symbol: **01.0249**
- Kategoria: **6A**
- Klasa: **EA**
- Konstrukcja: **U/FTP**
- Typ kabla: **wewnętrzny**
- Przekrój AWG: **4x2x23AWG**
- Przepustowość binarna: **10 Gb/s** (odległość do 100m)
- Pasmo częstotliwości (max): **500 MHz**
- Klasyfikacja ogniowa CPR (Euroklasa): **Dca**
- Normy: **EN 50173, ISO/IEC 11801, ANSI/TIA 568.2-D**
- Temperatura instalacji: **0°C do +50°C**
- Temperatura pracy: **-20°C do +60°C**
- Średnica zewnętrzna (przybliżona): **7,4 mm**
- Waga: **58 kg/km**

Budowa:

- **Żyły:** miedziane jednodrutowe Cu Ø 0,56 mm (23AWG)
- **Izolacja:** polietylen o trzywarstwowej konstrukcji PE (Skin-Foam-Skin) Ø 1,32 mm
- **Powłoka:** tworzywo bezhalogenowe nierozprzestrzeniające płomienia, o ograniczonym wydzielaniu dymu oraz gazów korozyjnych (LSOH/FRNC) Ø 7,4 mm
- **Ośrodek:** 4 pary skręcone, każda para owinięta folią aluminiową
- **Ekran:** folia aluminiowa, pod powłoką żyła uziemiająca z drutu miedzianego ocynowanego o średnicy min. 0,4 mm (26AWG)
- **Rip cord:** tak
- **Kolor powłoki:** fioletowy



Właściwości elektryczne:

- Impedancja w zakresie 4-100 MHz: **$100 \pm 15 \Omega$**
- Impedancja w zakresie 100-200 MHz: **$100 \pm 22 \Omega$**
- Impedancja w zakresie 200-500 MHz: **$100 \pm 32 \Omega$**
- Asymetria rezystancji (DC): **max. 5%**
- Rezystancja przewodnika przy 20°C (DC): **$\leq 73,2 \Omega/\text{km}$**
- Asymetria pojemności pary względem ziemi: **$\leq 330 \text{ pF}/100\text{m}$**
- Rezystancja izolacji: **$> 5000 \text{ M}\Omega \times \text{km}$**
- Wytrzymałość dielektryczna: **DC 2500V przez 2 sekundy**



Właściwości mechaniczne:

- Maksymalna siła naciągu: $\leq 100 \text{ N}$
- Wydłużenie przewodnika: $\geq 15\%$
- Wytrzymałość na rozciąganie (powłoka przed starzeniem): $\geq 8,3 \text{ MPa}$
- Wydłużenie (powłoka przed starzeniem): $\geq 100\%$
- Wytrzymałość na rozciąganie (powłoka po starzeniu 100°C , $24 \times 2\text{h}$): $\geq 75\% \times$ **wytrzymałość przed starzeniem**
- Wydłużenie (powłoka po starzeniu 100°C , $24 \times 2\text{h}$): $\geq 75\% \times$ **wydłużenie przed starzeniem**

Kabel skrętka miedziana cat. 6A F/FTP



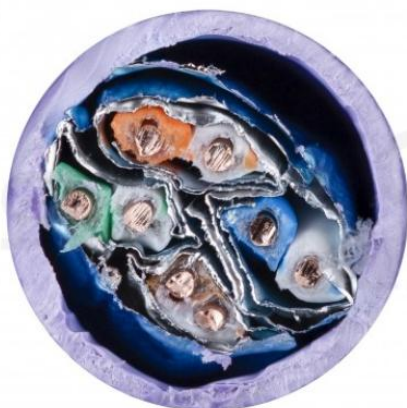


Charakterystyka:

- Producent: **NEKU**
- Symbol: **01.0248**
- Kategoria: **6A**
- Klasa: **EA**
- Konstrukcja: **F/FTP**
- Typ kabla: **wewnętrzny**
- Przekrój AWG: **4x2x23AWG**
- Przepustowość binarna: **10 Gb/s** (odległość do 100m)
- Pasmo częstotliwości (max): **500 MHz**
- Klasyfikacja ogniowa CPR (Euroklasa): **Dca**
- Normy: **EN 50173, ISO/IEC 11801, ANSI/TIA 568.2-D**
- Temperatura instalacji: **0°C do +50°C**
- Temperatura pracy: **-20°C do +60°C**
- Średnica zewnętrzna (przybliżona): **7,6 mm**
- Waga: **56 kg/km**

Budowa:

- **Żyły:** miedziane jednodrutowe Cu Ø 0,56 mm (23AWG)
- **Izolacja:** polietylen o trzywarstwowej konstrukcji PE (Skin-Foam-Skin) Ø 1,32 mm
- **Powłoka:** tworzywo bezhalogenowe nierozprzestrzeniające płomienia, o ograniczonym wydzielaniu dymu oraz gazów korozyjnych (LSOH/FRNC) Ø 7,6 mm
- **Ośrodek:** 4 pary skręcone, każda para owinięta folią aluminiową, dodatkowo całość ekranowana folią aluminiową
- **Ekran:** folia aluminiowa (całość i pary), pod wspólnym ekranem żyła uziemiająca z drutu miedzianego ocynowanego o średnicy min. 0,4 mm (26AWG)
- **Rip cord:** tak
- **Kolor powłoki:** fioletowy



Właściwości mechaniczne:

- Maksymalna siła naciągu: **≤100 N**
- Wydłużenie przewodnika: **≥15%**
- Wytrzymałość na rozciąganie (powłoka przed starzeniem): **≥8,3 MPa**
- Wydłużenie (powłoka przed starzeniem): **≥100%**
- Wytrzymałość na rozciąganie (powłoka po starzeniu 100°C, 24×2h): **≥75% × wytrzymałość przed starzeniem**
- Wydłużenie (powłoka po starzeniu 100°C, 24×2h): **≥75% × wydłużenie przed starzeniem**

Właściwości elektryczne:

- Impedancja w zakresie 4-100 MHz: **$100 \pm 15 \Omega$**
- Impedancja w zakresie 100-200 MHz: **$100 \pm 22 \Omega$**
- Impedancja w zakresie 200-500 MHz: **$100 \pm 32 \Omega$**
- Asymetria rezystancji (DC): **max. 5%**
- Rezystancja przewodnika przy 20°C (DC): **$\leq 73,2 \Omega/\text{km}$**
- Asymetria pojemności pary względem ziemi: **$\leq 330 \text{ pF}/100\text{m}$**
- Rezystancja izolacji: **$> 5000 \text{ M}\Omega \times \text{km}$**
- Wytrzymałość dielektryczna: **DC 2500V przez 2 sekundy**

Kabel skrętka miedziana cat. 7 S/FTP



OPIS PRODUKTU

Ekranowany przewód **S/FTP** marki NEKU przeznaczony do budowy zaawansowanych sieci komputerowych spełniających wymogi **kategorii 7** oraz pracujących w częstotliwości do **600MHz (rozszerzona do 1000MHz)**. Kabel charakteryzuje się najwyższą jakością oraz doskonałymi parametrami **przewyższającymi standardy**. Pozwala na transmisję danych, dźwięku i obrazu telewizyjnego o przepustowości binarnej **do 10Gb/s** (na długości do 100m). Posiada solidną powłokę bezhalogenową **LSOH** oraz żyły wykonane w **100% z miedzi** o średnicy **23AWG**.

Przeznaczony do wykonywania instalacji **wewnętrznych poziomych i pionowych** w sieciach teleinformatycznych **narażonych** na oddziaływanie zakłóceń elektromagnetycznych o dużym natężeniu. Najczęściej wykorzystywany w dużych serwerowniach, przemyśle oraz wszędzie tam gdzie wymagana jest **bardzo szybka transmisja danych** połączona z odpornością na niekorzystne warunki.

Nadaje się do stosowania w obiektach objętych uregulowaniami odnośnie reakcji wyrobów budowlanych na oddziaływanie ognia (**klasyfikacja ogniowa Eca, powłoka bezhalogenowa**).

Parametry techniczne:

- Producent: **NEKU**
- Symbol: **01.4015**
- Kategoria: **7**
- Klasa: **F**
- Konstrukcja: **S/FTP**
- Typ kabla: **wewnętrzny**
- Przekrój AWG: **4x2x23AWG**
- Przepustowość binarna (max): **10 Gb/s** (do 100m)
- Pasma częstotliwości (max): **600MHz** (rozszerzona charakterystyka do **1000MHz**)
- Klasyfikacja ogniowa CPR (Euroklasa): **Dca**
- Średnica zewnętrzna: **7,3 mm**
- Promień zgięcia : **4 x średnica kabla**
- Zakres temp. podczas użycia: **-20°C do +60°C**
- Zakres temp. podczas instalacji: **0°C do +50°C**
- Waga nominalna: **51 kg/km**

Budowa:

- **Żyły:** jednodrutowe z miedzi elektrolitycznej o średnicy 0,57mm (23AWG)
- **Izolacja:** specjalna mieszanka poliolefinowa
- **Ośrodek:** 4 pary skręcone, każda para owinięta folią, całość ekranowana opłotem
- **Ekran:** pary indywidualnie ekranowane folią poliestrową pokrytą warstwą aluminium, pod ekranem żyła uziemiająca z drutu miedzianego ocynowanego, ośrodek dodatkowo ekranowany opłotem z ocynowanych drutów Cu
- **Powłoka:** tworzywo bezhalogenowe nierozprzestrzeniające płomienia, o ograniczonym wydzielaniu dymu oraz gazów korozyjnych (LSOH/FRNC)
- **Kolor powłoki:** pomarańczowy (RAL 2003)

Właściwości elektryczne:

- Impedancja w zakresie 4-100Mhz: **100±15Ω**
- Impedancja w zakresie 100-200Mhz: **100±22Ω**
- Impedancja w zakresie 200-600Mhz: **100±32Ω**
- Max. oporność przewodnika w 20°C: **8,4Ω/100m**
- Asymetria rezystancji żył w parze: **≤2,5%**
- Pojemność wzajemna: **45 pF/m**
- Asymetria pojemności torów transmisyjnych względem ziemi: **330pF/100m**
- Impedancja sprzężeniowa ekranu w zakresie częstotliwości 100MHz (max): **10mΩ/m**
- Tłumienność sprzężeniowa: **≥ 80 dB**
- Tłumienność odbiciowa dla częst. 4MHz (min): **23dB**
- Tłumienność odbiciowa dla częst. 20MHz (min): **25dB**
- Tłumienność odbiciowa dla częst. 100MHz (min): **20,1dB**
- Tłumienność odbiciowa dla częst. 200MHz (min): **18dB**
- Tłumienność odbiciowa dla częst. 600MHz (min): **17,3dB**
- Prędkość propagacji NVP: **79%**
- Opóźnienie propagacji przy częst. 4MHz: **552ns/100m**
- Opóźnienie propagacji przy częst. 20MHz: **542ns/100m**
- Opóźnienie propagacji przy częst. 100MHz: **538ns/100m**
- Opóźnienie propagacji przy częst. 600MHz: **535ns/100m**
- Kąt opóźnienia (max): **25ns/100m**

Normy i badania:

- PN-EN 50173
- ISO/IEC 11801
- Przewody NEKU są **zgodne z dyrektywą CPR** (norma PN-EN 50575) dotyczącą klasyfikacji wyrobów budowlanych pod względem odporności na działanie ognia oraz definiujące metody badań dla przewodów przeznaczonych do instalowania w budynkach
- Produkt został objęty **5 letnią** gwarancją produktową

O producencie:

Marka NEKU obejmuje okablowanie strukturalne oraz wszelkie komponenty służące do budowy sieci teleinformatycznych i telekomunikacyjnych. Jej wieloletnie doświadczenie, duża różnorodność oraz najwyższa jakość oferowanych produktów i urządzeń przekładają się na ciągły rozwój marki bezpośrednio związany z dużym zaufaniem Klientów. Oferta produktów marki NEKU to szeroki wybór komponentów o atrakcyjnym zróżnicowaniu cenowym m.in. patchpanele, listwy zasilające, szafy RACK 10" i 19" wraz z osprzętem, patchcordsy, gniazda i keystony, narzędzia elektroinstalacyjne, testery, osprzęt LSA, kable i przewody oraz wszelkiego rodzaju wtyki i łączniki.

Kabel skrętka miedziana cat. 8.2 S/FTP



OPIS PRODUKTU

Przyszłościowy standard i najwyższa możliwa jakość dla Twojej sieci!

Najwyższej jakości, podwójnie ekranowany (S/FTP) przewód instalacyjny spełniający wymogi standardu **kategorii 8.2** i osiągający bardzo wysoką częstotliwość przesyłu - **do 2000 MHz**.

Kabel charakteryzuje się doskonałymi parametrami elektrycznymi, pozwala na transmisję danych, dźwięku i obrazu telewizyjnego o przepustowości binarnej do **40 Gb/s**. Posiada solidną, bezhalogenową powłokę nierozprzestrzeniającą płomienia (**LSOH / LSZH, klasa Dca**) oraz żyły wykonane w **100% z miedzi** o średnicy **AWG 22/1**.

Przeznaczony do wykonywania **instalacji wewnętrznych poziomych i pionowych** w sieciach teleinformatycznych szczególnie zagrożonych oddziaływaniem zakłóceń elektromagnetycznych oraz wymagającym wysokich częstotliwości pracy. Idealny wybór do **najbardziej wymagających** aplikacji teleinformatycznych.

Specyfikacja:

- Producent: **Digitus**
- Symbol: **DK-1843-VH**
- Kategoria: **8.2**
- Typ ekranowania: **S/FTP**
- Typ kabla: **wewnętrzny**
- Konstrukcja: **8 przewodów, skręconych w 4 pary**
- Przepustowość binarna (max): **40 Gb/s**
- Pasma częstotliwości (max): **2000 MHz**
- Średnica zewnętrzna (nom.): **7,9 mm**
- Średnica powłoki zewnętrznej (nom.): **0,55 mm**
- Klasa CPR: **Dca**
- Obciążenie rozciągające (max.): **150 N**
- Obciążenie ogniowe: **620 MJ/km**
- Dynamiczny promień gięcia (min.): **8x $\varnothing$**
- Statyczny promień gięcia (min.): **4x $\varnothing$**
- Temperatura przechowywania: **-20°C do +75°C**
- Temperatury pracy: **-20°C do +60°C**
- Temperatura instalacji: **0°C do +50°C**
- Waga: **60 kg/km**

Właściwości elektryczne:

- Średnia impedancja: $100 \pm 15 \text{ Ohm @ } 1\text{-}2000 \text{ MHz}$
- Pojemność: 43 pF/m nominalna przy 1 KHz
- Asymetria pojemności (para - uziemienie): 99 pF/30 m max. przy 1 KHz
- Rezystancja izolacji (min.): 5 GOhm x km
- Rezystancja stałoprądowa (max.): 2.4 Ohm/30m (4% max. niezrównoważenie rezystancji)
- Rezystancja stałoprądowa pętli (max.): 5.6 Ohm/24m (3% max. niewyważenie rezystancji)
- Napięcie pracy (max.): 72 VDC
- Tłumienie sprzężenia: 85 dB Typ 1
- Opóźnienie fazowe (max.): 171 nS/30 m
- Opóźnienie propagacji sygnału (max.): 13.5 nS/30 m
- Klasyfikacja rozdzielania: „d” (zgodnie z EN 50174-2)
- Nominalna prędkość propagacji (NVP): 79%

Budowa:

- **Przewodnik:** drut miedziany AWG 22/1 (0,60mm nominalnie), czysta wyżarzona miedź
- **Izolacja:** polietylen spieniony SFS-PE (Foam-Skin)
- **Indywidualne ekranowanie par:** folia aluminiowa zapewniająca 100% pokrycie
- **Ekran całościowy:** opłot miedziany ocynowany zapewniający 50% pokrycie
- **Powłoka zewnętrzna:** LSZH, Dca
- **Kodowanie kolorem:** niebiesko-biały, pomarańczowo-biały, zielono-biały, brązowo-biały
- **Kolor powłoki:** zielony

Normy:

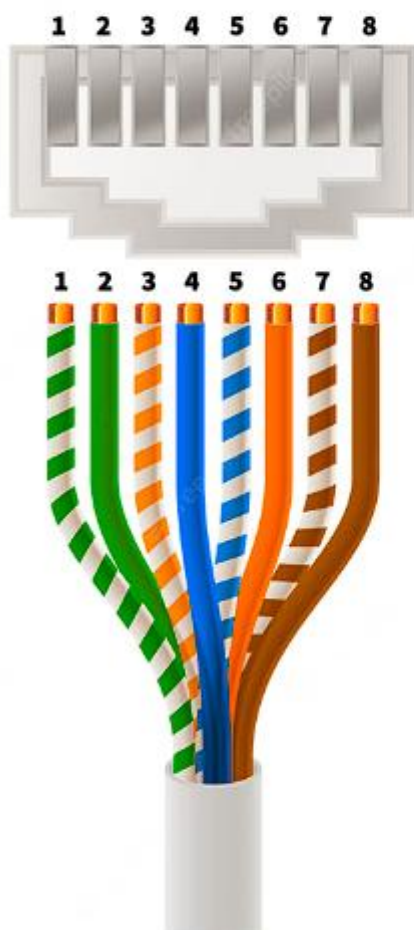
- Certyfikacja: połączenie kanału siłowego klasy I (kategoria 8) (2019-792)
- Standardy ISO/IEC 11801 3rd Ed.; IEC 61156-5
- Standardy DIN EN 50173-1/4; DIN EN 50288-9-1
- Bezhalogenowa powłoka kabla zgodna z normami IEC 60332-3-24, FRNC-C, LSZH-3 oraz CPR Euroclass Dca

Obszary zastosowań:

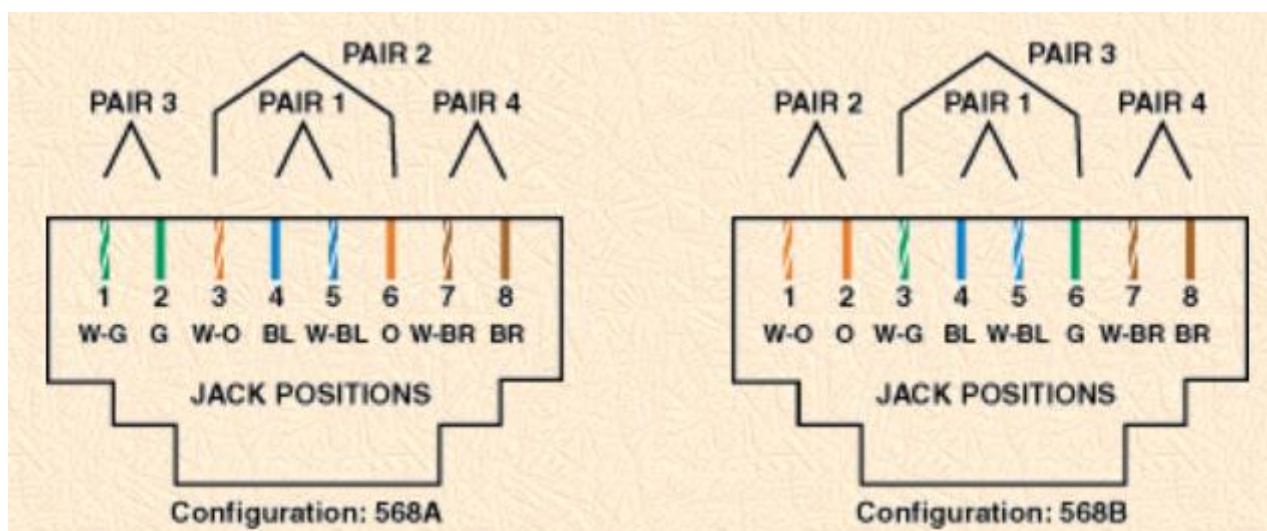
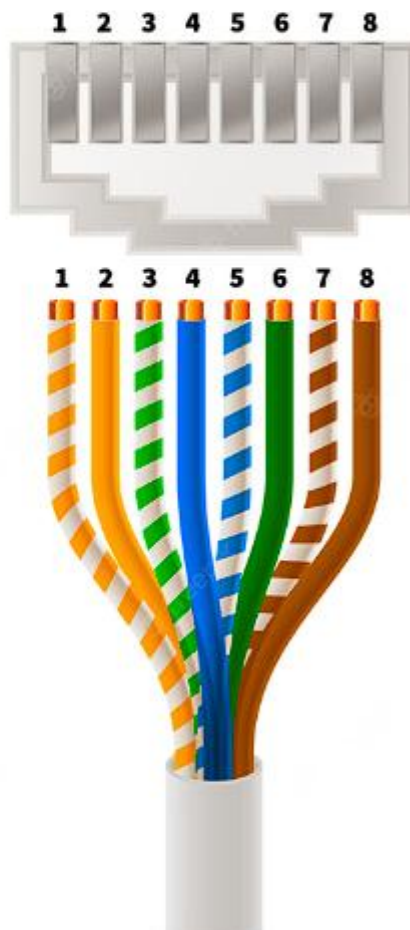
- Okablowanie podstawowe (kampus), drugorzędne (pionowe), trzeciorzędne (poziome)
- IEEE 802.3: 10Base-T, 100Base-T, 1000Base-T, 2.5GBase-T, 5GBase-T, 10GBase-T, 25GBase-T, 40GBase-T
- IEEE 802.5 16 MB; ISDN; FDDI; ATM; CATV
- Power over Ethernet Typ 1-4 (PoE / PoE+ / 4PPoE)

2.03 Skrętka miedziana – standard T568 i oznaczanie par

T568A



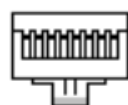
T568B



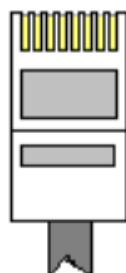
RJ-45 WTYK
MĘSKI



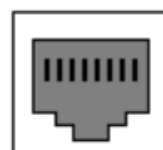
8 7 6 5 4 3 2 1



1 2 3 4 5 6 7 8



1 2 3 4 5 6 7 8



RJ-45 GNIAZDO
ŻEŃSKIE

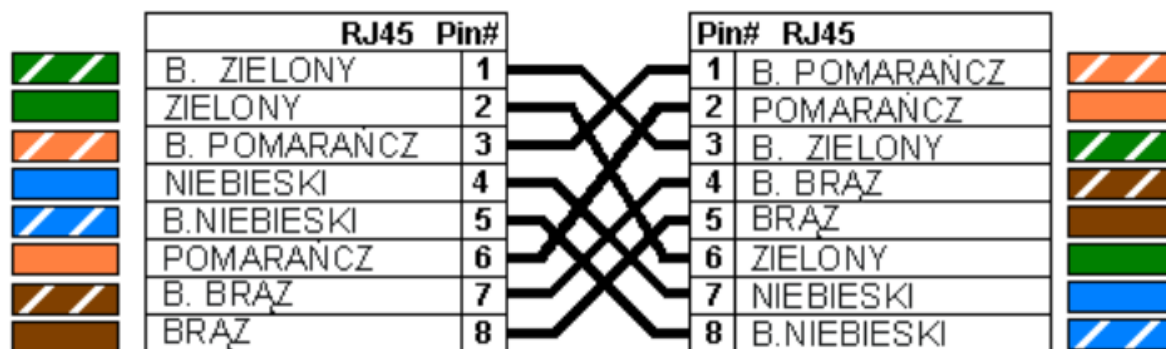
EIA/TIA T568A

KABEL PROSTY



EIA/TIA T568A

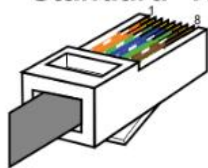
KABEL KRZYŻOWY



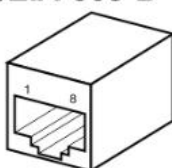
Standard TIA/EIA-568-B / A

różnice w rozszyciu, kabel prosty

Standard TIA/EIA-568-B

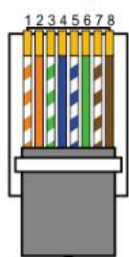


Złącze RJ45 męskie
wtyk

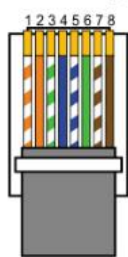


Złącze RJ45 żeńskie
gniazdo

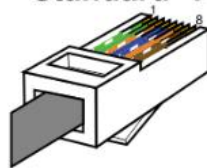
Kabel prosty (np. komputer - switch)



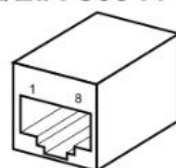
1. Biało-pomarańczowy
2. Pomarańczowy
3. Biało-zielony
4. Niebieski
5. Biało-niebieski
6. Zielony
7. Biało-brązowy
8. Brązowy



Standard TIA/EIA-568-A

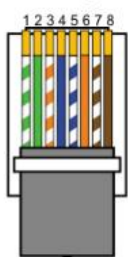


Złącze RJ45 męskie
wtyk

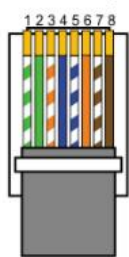


Złącze RJ45 żeńskie
gniazdo

Kabel prosty (np. komputer - switch)



1. Biało-zielony
2. Zielony
3. Biało-pomarańczowy
4. Niebieski
5. Biało-niebieski
6. Pomarańczowy
7. Biało-brązowy
8. Brązowy

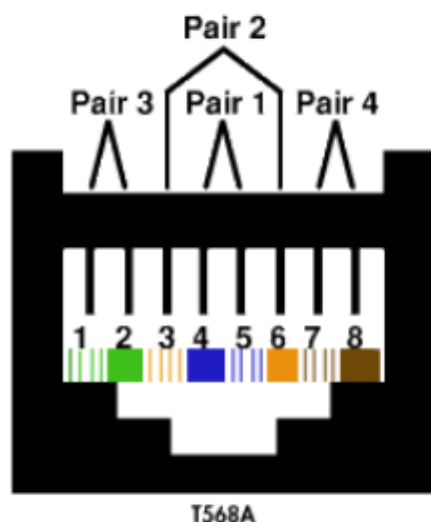
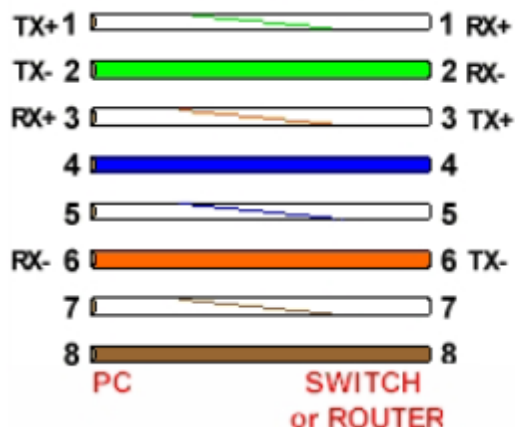


STRAIGHT-THROUGH

Wiring Standards Used

T568A

T568A

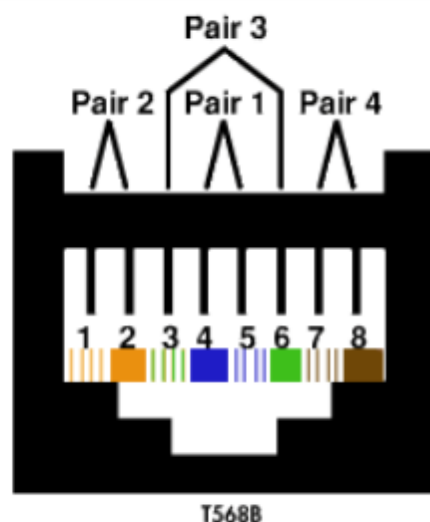
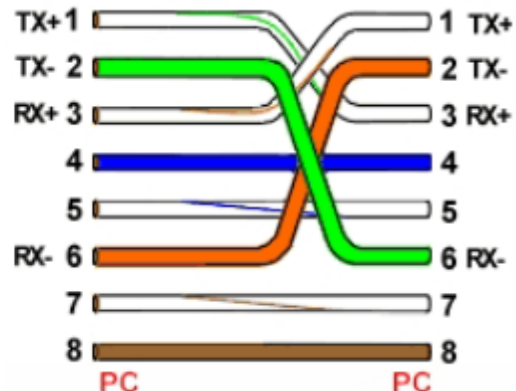


CROSS-OVER

Wiring Standards Used

T568A

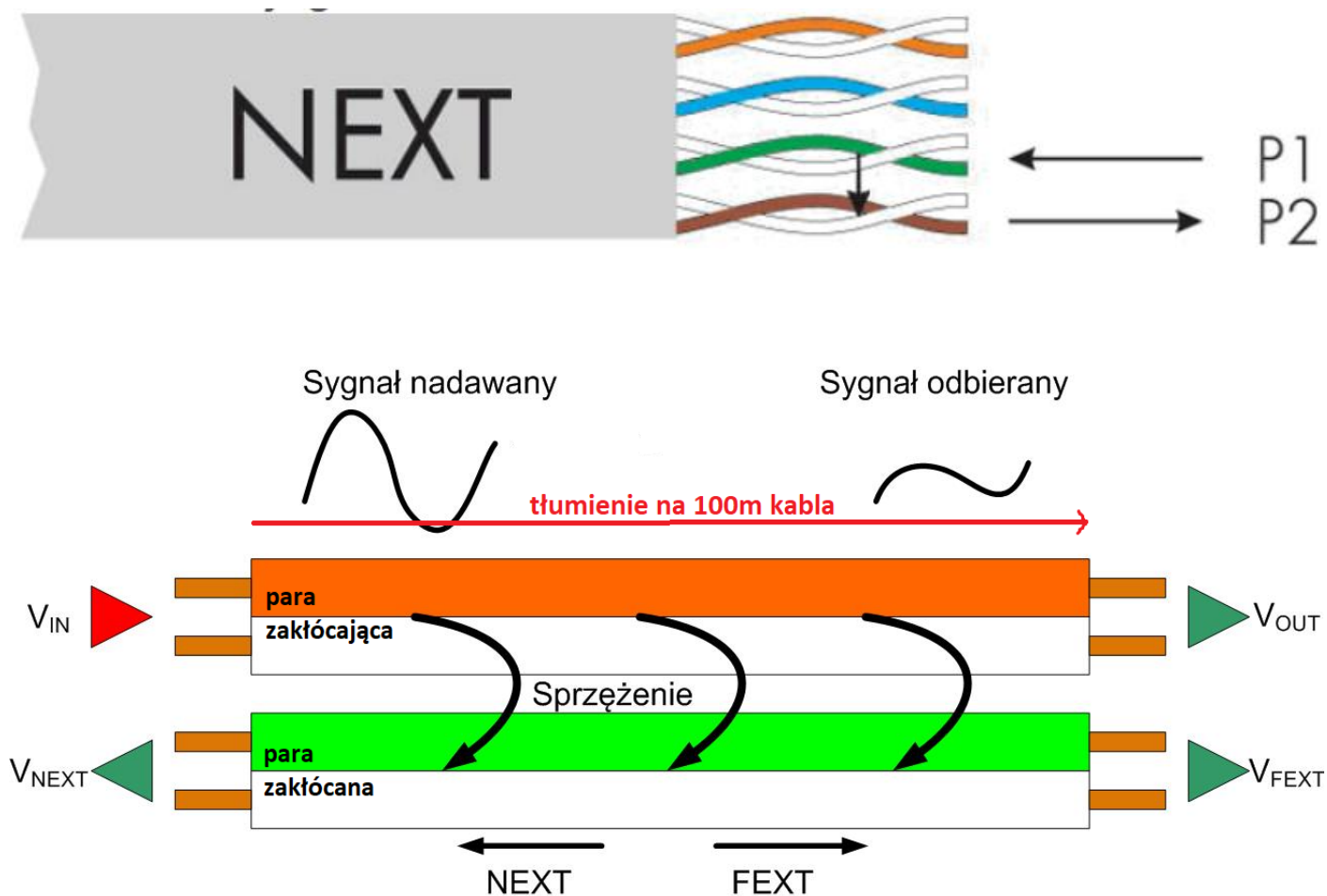
T568B



2.04 Skrętka miedziana – parametry transmisyjne

2.0.4.1 NEXT (Near end crosstalk) – przesłuch zbliżny

- powstaje w sytuacji gdy we wspólnej wiązce nieekranowanych przewodów UTP znajdują się skręcone pary wykorzystywane w danym momencie do transmisji w przeciwnych kierunkach.



- parametr NEXT określa wartość sprzężenia między przyległymi parami żył. Jest to stosunek mocy podawanej w jednej parze kabla UTP do mocy mierzonej w innej parze tego samego kabla. Pomiary dokonuje się po tej samej stronie po której nadawano sygnał.

Stopień przenikania sygnału z jednej pary sygnałowej do drugiej



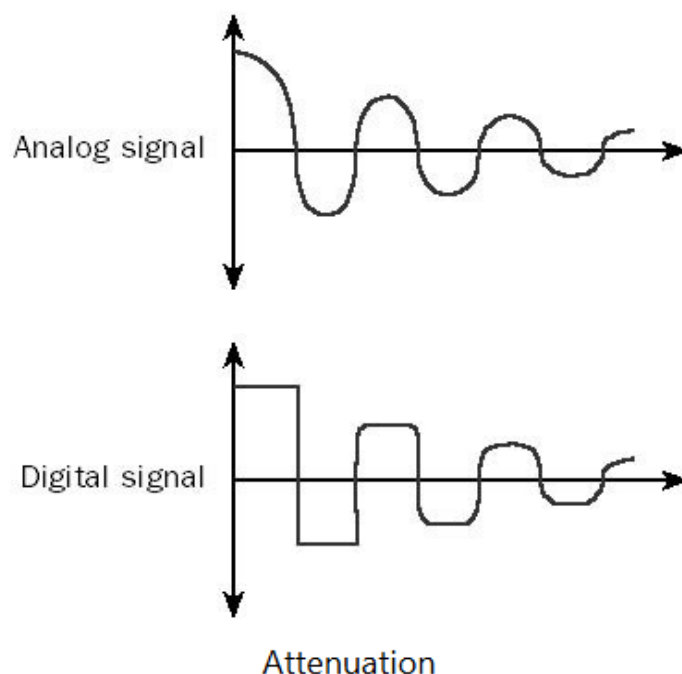
$$\text{NEXT}(f) = -20 \cdot \log_{10} \left(\frac{V_{\text{NEXT}}}{V_{\text{in}}} \right) [dB]$$

- Takie oddziaływanie zawsze występuje w trakcie transmisji dwukierunkowej, gdy pokrywają się pasma nadawanych i odbieranych sygnałów.
- W wyniku sprzężenia elektromagnetycznego między parami tych przewodów część energii sygnału generowanego po stronie lokalnej jednej pary transmisyjnej przenika do innej i w tłumionej postaci oraz z niejednorodnym opóźnieniem powraca torem odbiorczym do urządzenia po tej samej stronie linii komunikacyjnej.
- Poziom przenik zbliżony zależy w dużej mierze od ułożenia par, długości linii, częstotliwości pracy i szerokości przenoszonego pasma, przyjmując najczęściej postać kolorowego szumu gaussowskiego.
- W sieciach strukturalnych LAN parametr NEXT jest najważniejszym parametrem. Zależy od rodzaju kabla tłumienności toru. Jego wynik jest podawany w dB.
- NEXT jest parametrem wydajności łącza mierzonym w danym łączy lub kanale. Mierzy sprzężony sygnał z jednej pary do drugiej. Para powodująca zakłócenia jest nazywana „parą zakłócającą”, podczas gdy para, na którą oddziałuje zakłócenie „parą zakłócaną”.

- NEXT mocno zależy od częstotliwości transmisji, ponieważ wyższe częstotliwości powodują większe zakłócenia. Im wyższa wartość NEXT w dB tym mniej zakłóceń jest odbieranych przez zakłócany link/kanal.
- Parametr jest nazywany „przesłuchem zbliżnym”, ponieważ jest mierzony na tym samym końcu linku/kanalu, co jest nadawany sygnał zakłócający.
- Jeżeli kiedykolwiek zastanawiałeś się, dlaczego pary w „skrętce” są skręcone to właśnie po to, aby pomagać minimalizować przesłuchy. Różne stopnie skrętu sąsiadujących par uniemożliwiają im odbieranie sygnałów z innych par. Dlatego bardzo istotne jest to, aby utrzymywać skręt par jak najbliżej każdego zakończenia kabla.
- Pomiar NEXT polega na tym, że mierzy się różne kombinacje par w ramach jednego kabla– tj. 12-36, 12-45, 12-78, 36-45, 36-78, 45-78 –i to na obu jego końcach.

2.0.4.2 ACR-N Attenuation (tłumienie)

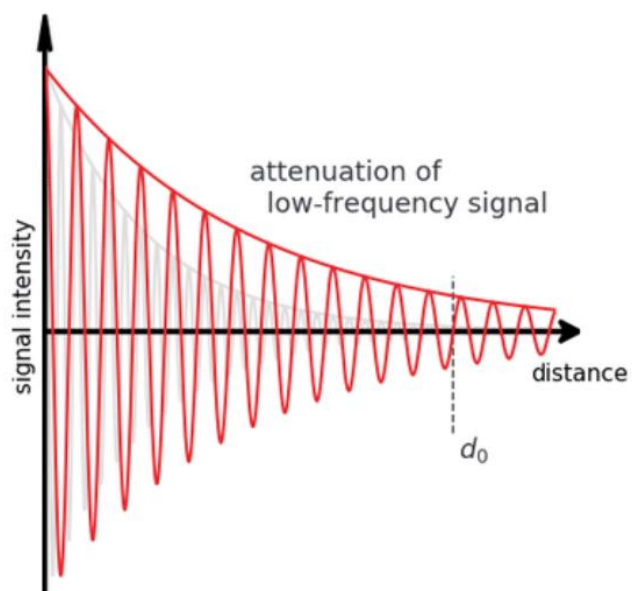
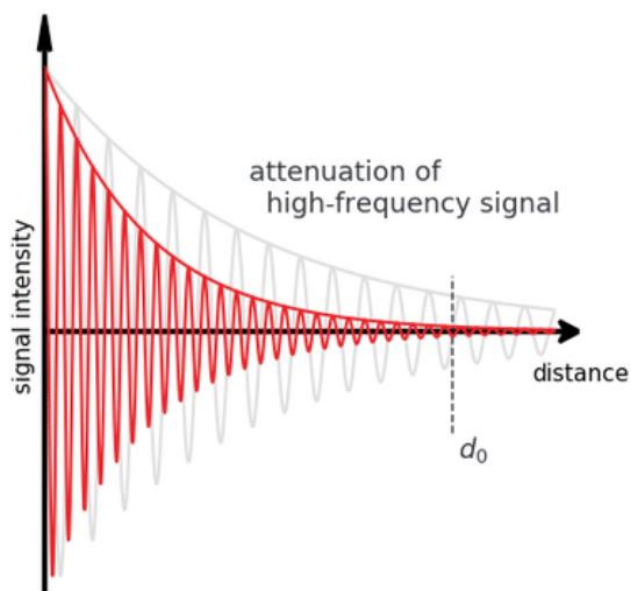
Attenuation by signal absorption



Tłumienie pokazuje różnicę pomiędzy wielkością sygnału wejściowego oraz sygnału na końcu przewodu.



Głównie ze względu na opór, który stawia przewód i zwykle jest większy dla większych częstotliwości.

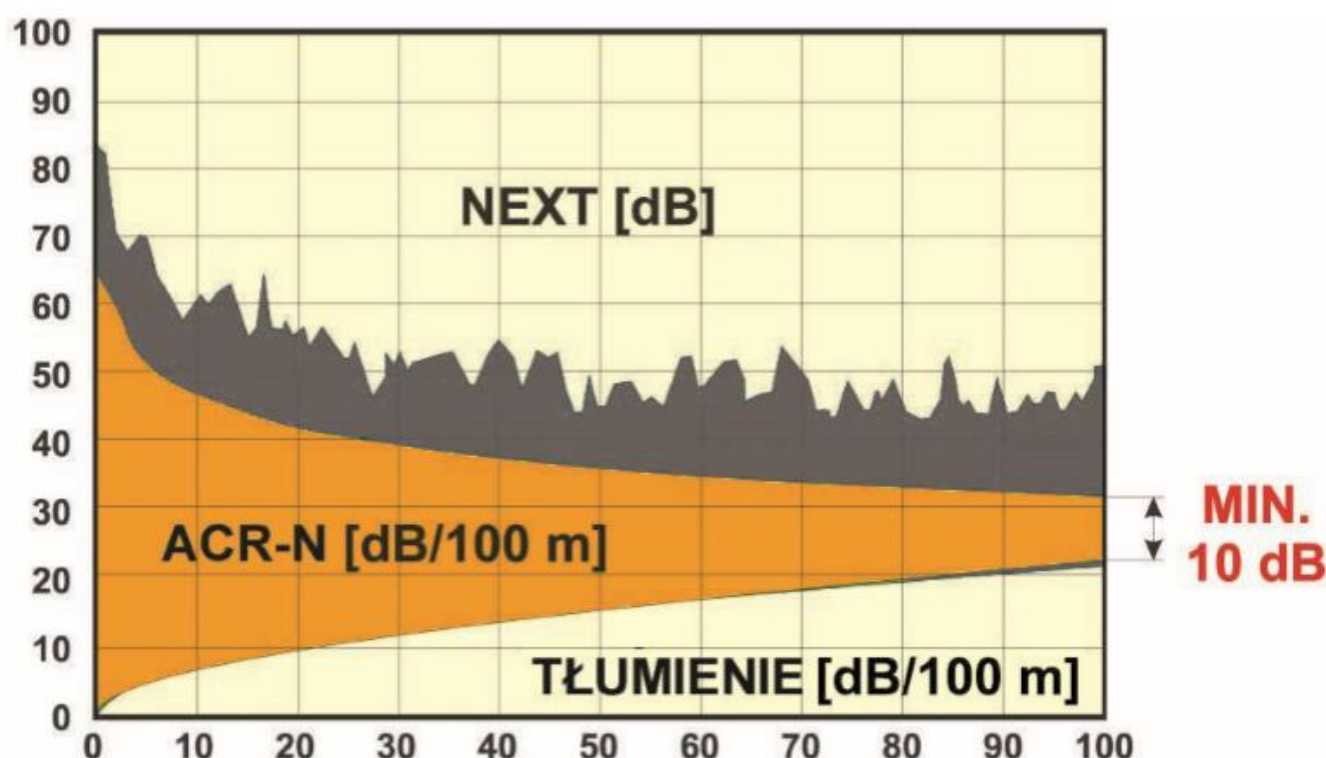


Tłumienie zwiększa się wraz ze zmniejszaniem się średnicy przewodów - tzn. Wielkość kabla AWG 24 ma nieco większe tłumienie niż grubszy przewód z AWG 23

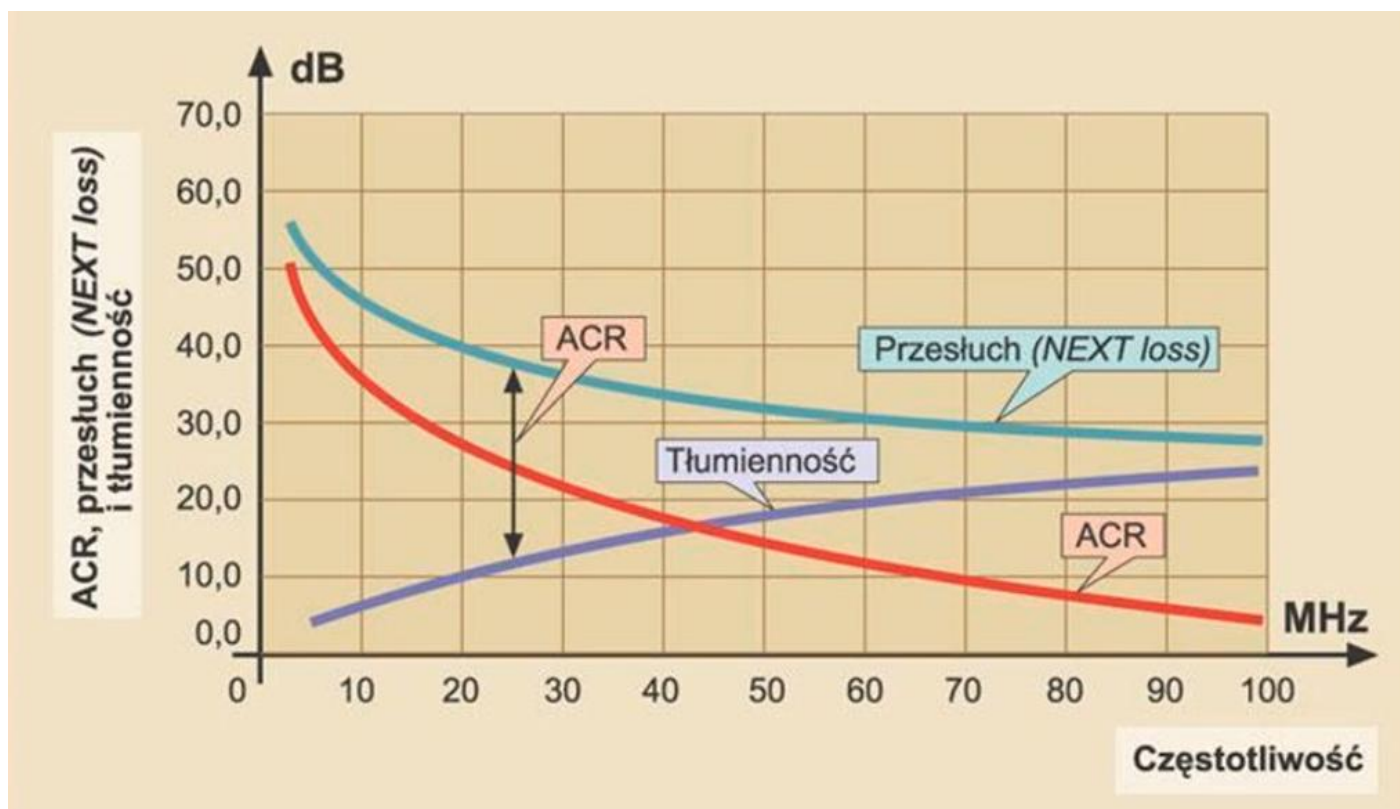
American Wire Gauge w skrócie **AWG** – to przyjęty i stosowany w USA system miary średnicy przekroju przewodu elektrycznego. Im wyższa liczba AWG, tym mniejsza średnica przewodu.

AWG	Średnica żyły [mm]	Przekrój [mm ²]	Rezystancja [Ohm/km]	Waga [g/m]
24	Ø 0,511	0,2050	84,22	2,190
	Ø 0,560	0,2463		
23	Ø 0,573	0,2580	66,79	2,771
	Ø 0,630	0,3117		

2.0.4.3 ACR-N (Attenuation to Crosstalk Ratio – Near End) odstęp przesłuchu na bliskim końcu



ACR-N jest parametrem teoretycznym (nie mierzony ale wynika z dwóch wcześniej zmierzonych wartości.), który pokazuje różnicę między wartościami NEXT oraz tłumienia: $ACR-N [dB] = NEXT [dB] - [dB]$. Jeśli poziom tłumienia zbliża się do poziomu przesłuchów, sygnał zanika. Odstęp między NEXT i tłumieniem musi wynosić co najmniej 10 dB. W starszych wersjach norm, parametr ten był znany jako ACR (Attenuation to Crosstalk Ratio).



Co dalej gdy ACR-N jest poza zakresem?

Jako że ACR-N wyliczamy z NEXTu i tłumienia, poprawa tych parametrów wpłynie na zmianę ACR-N.

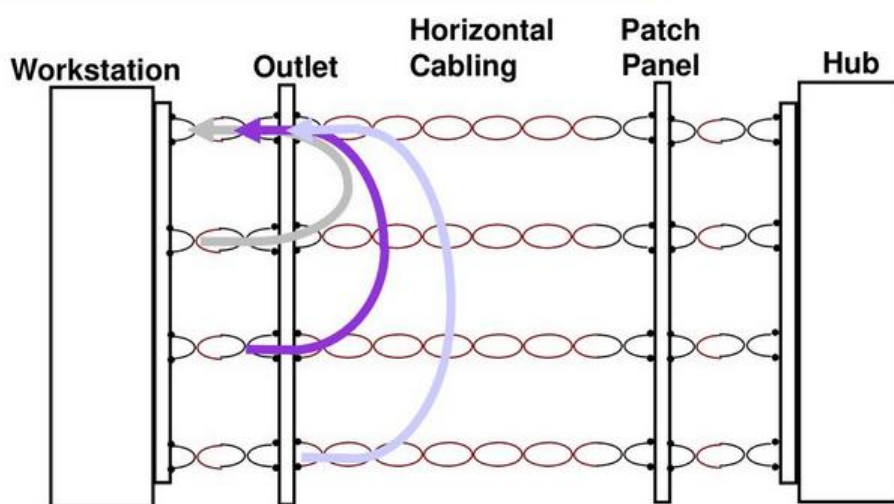
2.0.4.4 PSNEXT (Power Sum NEXT) – suma mocy przesłuchów w bliskim końcu



Viditec

FLUKE
networks

Power Sum NEXT

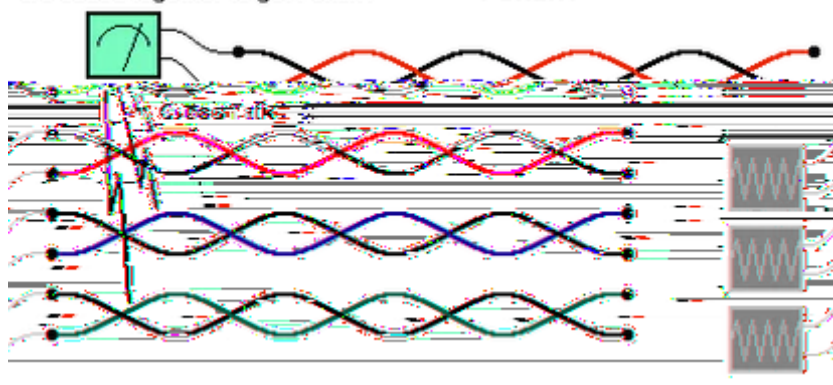


PSNEXT (Power Sum NEXT) to wartość teoretyczna obliczana z wcześniej zmierzonych. Parametr PSNEXT jest szczególnie ważny dla protokołów, które używają do przesyłania sygnału wszystkich czterech par (np Gigabit Ethernet).

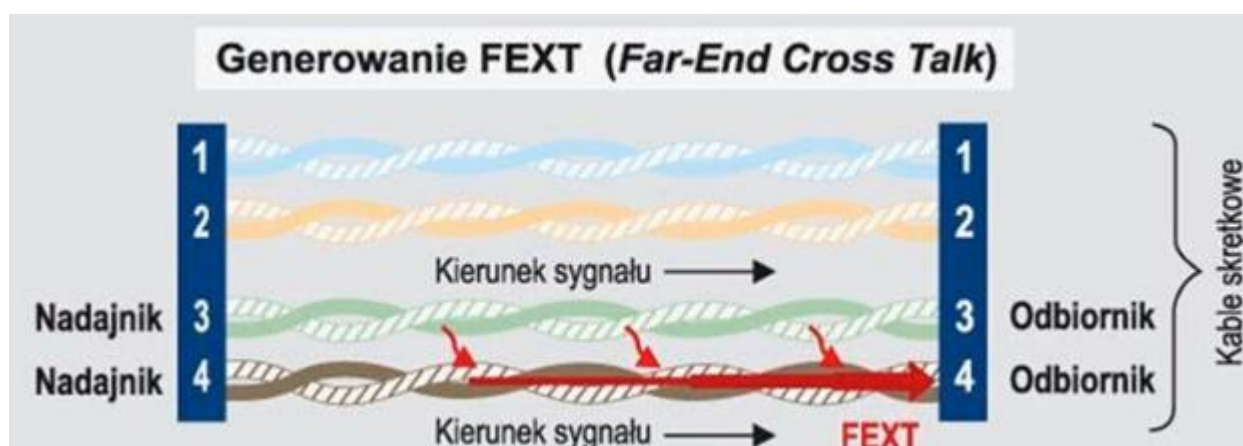
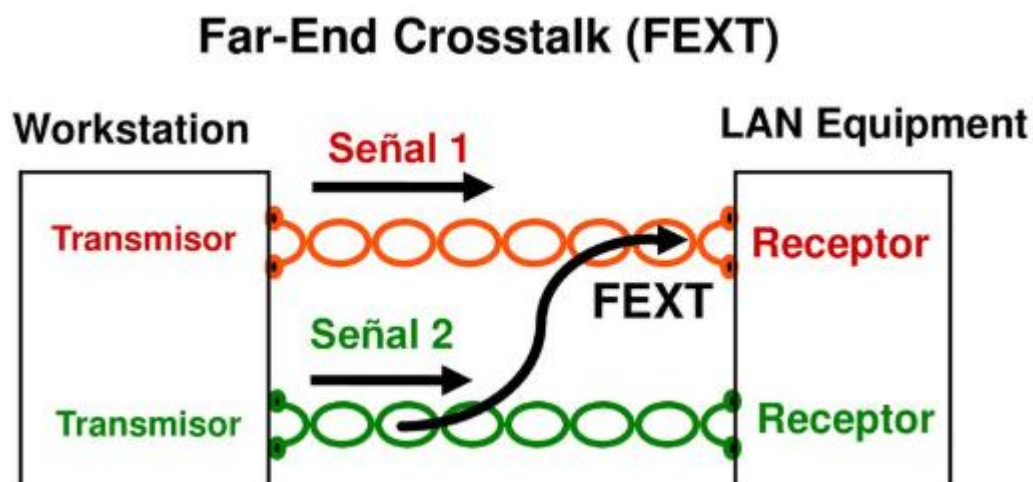
Suma mocy przesłuchów w bliskim końcu pokazuje jak dużo sygnału w jednym kablu dostaje się od trzech par do pozostałej czwartej pary. Indexowanie i źródło sygnału odbywa się na tym samym końcu.

The results from all three NEXT tests are added together to get PSNEXT

PSNEXT

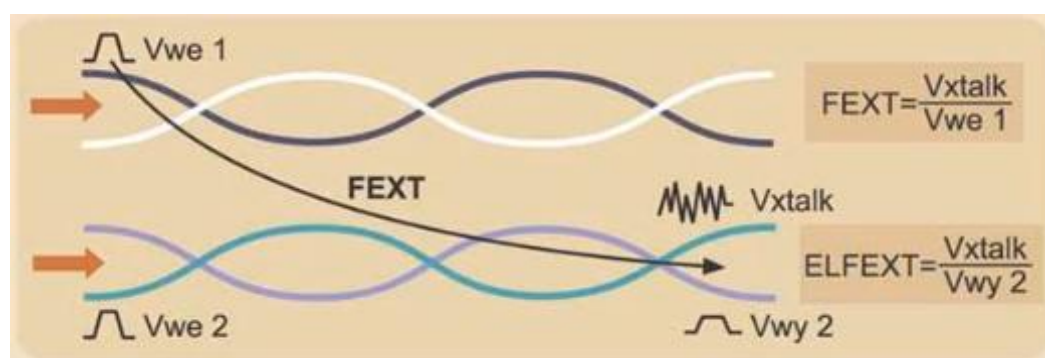


2.0.4.5 FEXT (Far End Cross Talk) przesłuch na dalekim końcu - zdalny



Przesłuch zdalny zwany FEXT również jest mierzony w kanale. Jest bardzo podobny do NEXT, ale jak sama nazwa wskazuje pomiar odbywa się na drugim końcu kanału. Sam FEXT nie za wiele nam mówi gdyż sygnały zakłócające są wytłumiane wraz z przebytą odległością.

Mierzone są wszystkie kombinacje par w obrębie jednego kabla tj. 12-36, 12-45, 12-78, 36-45, 36-78, 45-78.



Aby zapewnić bardziej miarodajny pomiar, usunięto z pomiaru FEXT tłumienie (IL) i stworzono parametr ELFEXT (Equal level far end crosstalk). TIA zmieniło nazwę tego parametru na ACRF (Attenuation to crosstalk ratio far end).

2.0.4.6 ACR-F (Attenuation to Crosstalk Ratio - Far End) odstęp przesłuchu na zdalnym końcu

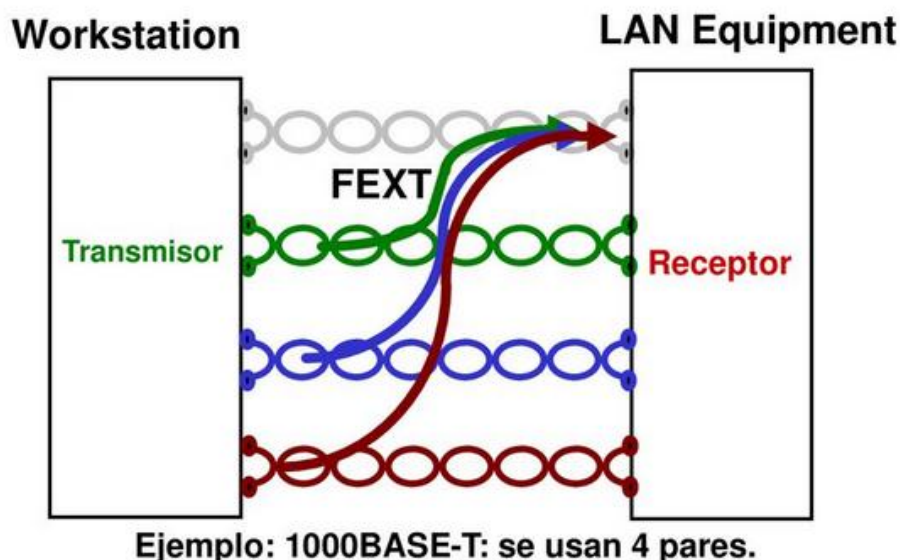
Znacznie lepiej oddaje aktualną sytuację transmisji danych niż PSFEXT. Przesłuch wewnątrz kabla maleje ze wzrostem tłumienia. Podobnie jak ACR-N jest parametrem teoretycznym (czyli nie jest mierzony, ale liczony od innych wartości zmierzonych wcześniej): $ACR-F [dB] = FEXT [dB] - A [dB]$. Odstęp przesłuchu na zdalnym końcu to FEXT pomniejszony o tłumienność.

Podobnie jak w NEXT, pomiar ACRF są sumowane dla każdej z trzech par zakłócających, co daje nam sumę mocy ACRF (PSACRF). Ten parametr był nazywany PSELFEXT zanim TIA zmieniło go na PSACRF.

2.0.4.7 PSFEXT (Power Sum FEXT) – Suma mocy przesłuchu FEXT

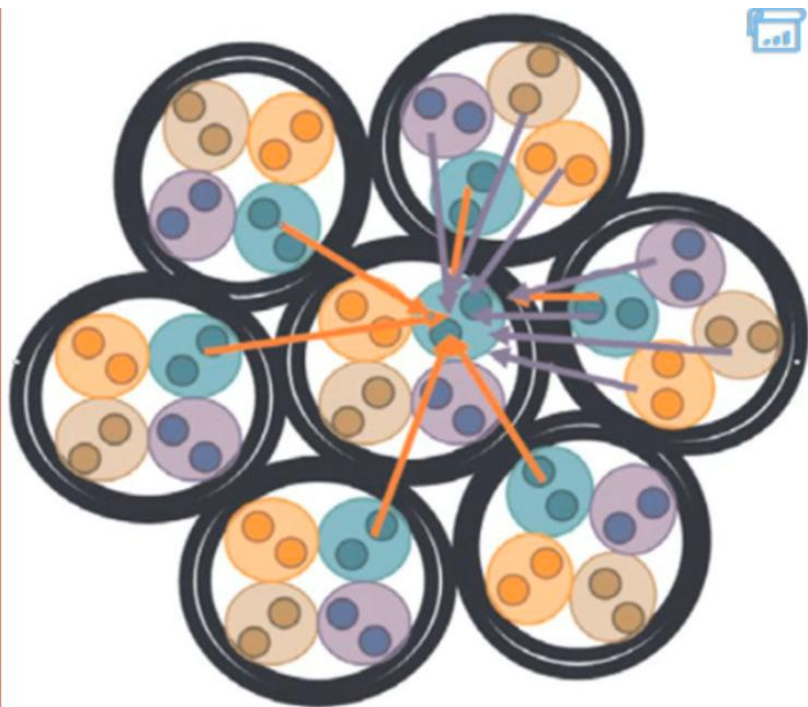


Power Sum FEXT



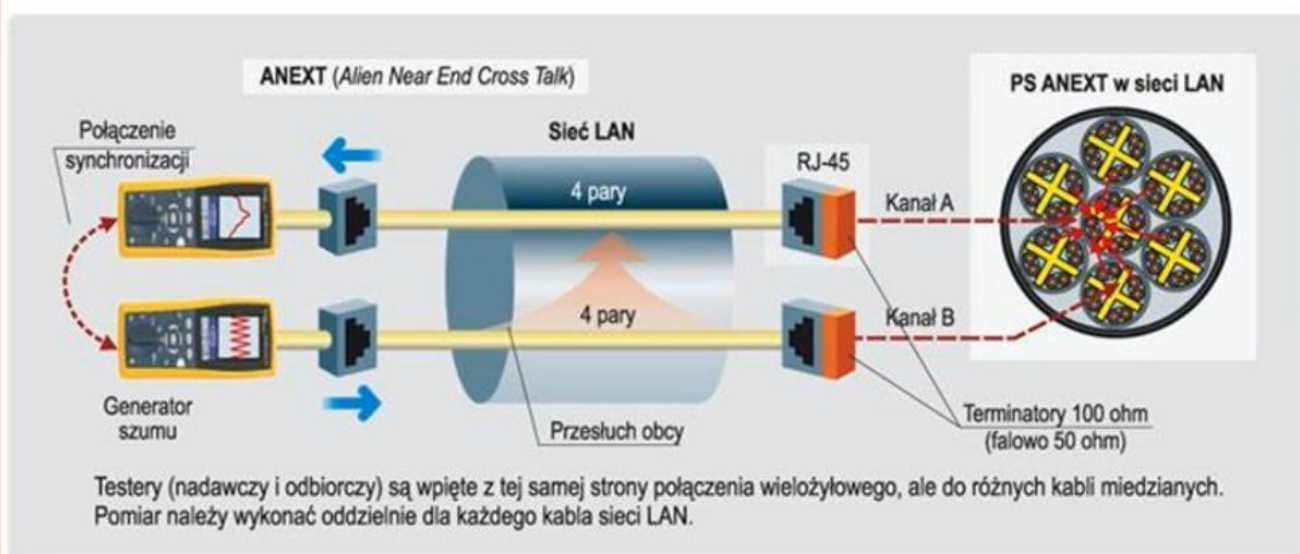
2.0.4.7 ANEXT (Alien crosstalk) – przesłuch obcy

Przechodząc do wyższych częstotliwości przy kategorii 6A oraz szybszych aplikacji rzędu 2,5/5/10 GBase-T będziemy się martwić o przesłuchy obce (ANEXT – Alien crosstalk).



Rys. 1 Przesłuch zbliżny (NEXT) oraz zdalny (ANEXT), pochodzący z par sąsiednich w wiązce. Najwyższe wartości osiąga pomiędzy parami o tych samych kolorach, ponieważ mają podobne skręty i długości żył

POMIAR PARAMETRU ANEXT



2.04 Światłowody

Zalety stosowanie:

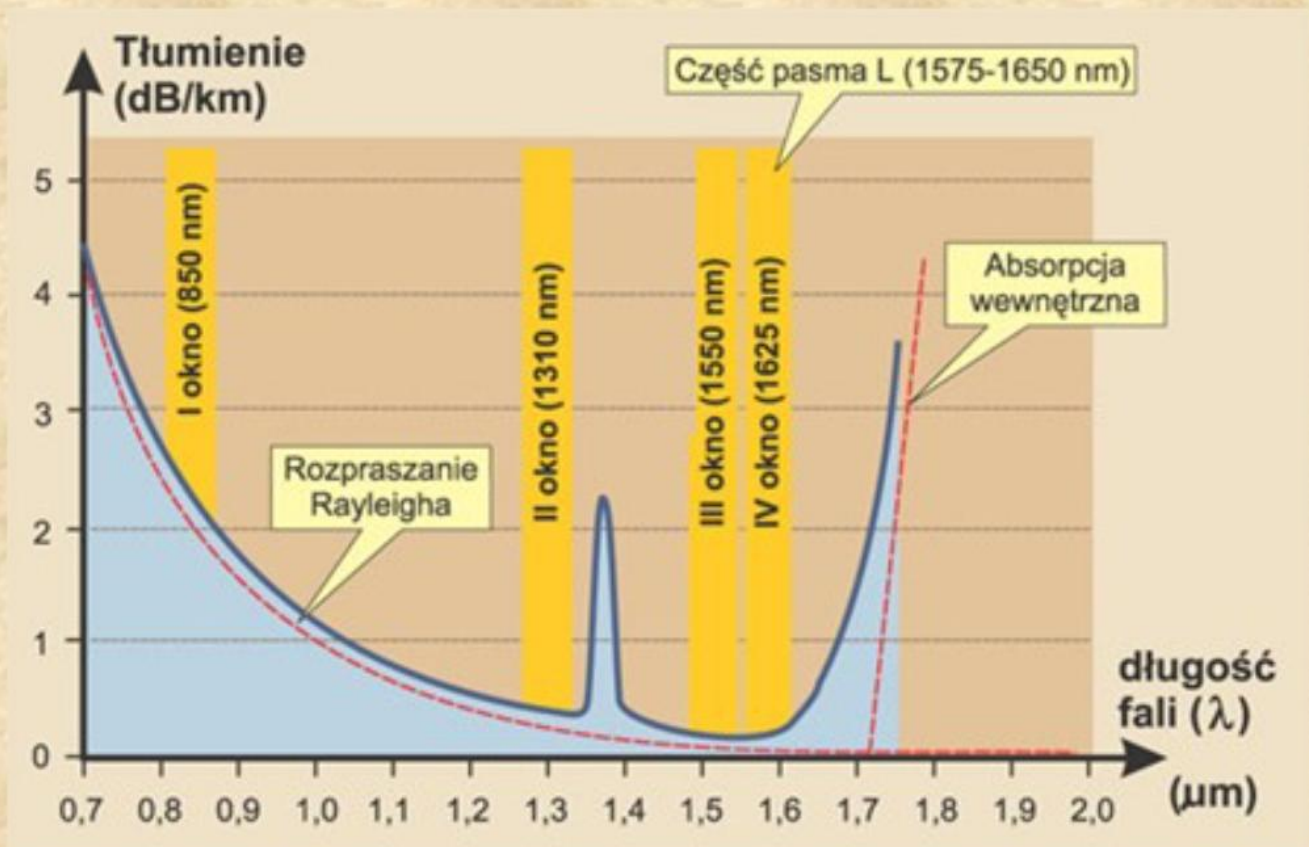
- dużą przepustowość;
- odporność na zakłócenia (elektromagnetyczne);
- bezpieczeństwo sygnału (stosunkowo trudno „podслуchać” dane przesyłane światłowodem);
- większą długość segmentów sieci (lub odległość między wzmacniaczami); jest to wynikiem dużo niższego poziomu tłumienia w porównaniu z kablami UTP;
- bezpieczeństwo przyszłego rozwoju sieci;
- obsługę wielu technologii transmisji;
- brak iskrzeń i zwarć;
- niezawodność;
- relatywnie małe wymiary i masę;
- skalowalność.

Odległości między wzmacniaczami

Medium	Odległość bez wzmacniania sygnału
Przewód miedziany	1,1 km
Kabel światłowodowy MM (850 nm)	12 – 15 km
Kabel światłowodowy MM (1300 nm)	25 – 35 km
Kabel światłowodowy SM (1310 nm)	50 – 80 km
Kabel światłowodowy SM (1550 nm)	150 – 2500 km

Okna transmisyjne

Zależność tłumienia światłowodu od długości fali



I okno transmisyjne na fali 850 nm

II okno transmisyjne na fali 1310 nm

III okno transmisyjne na fali 1550 nm

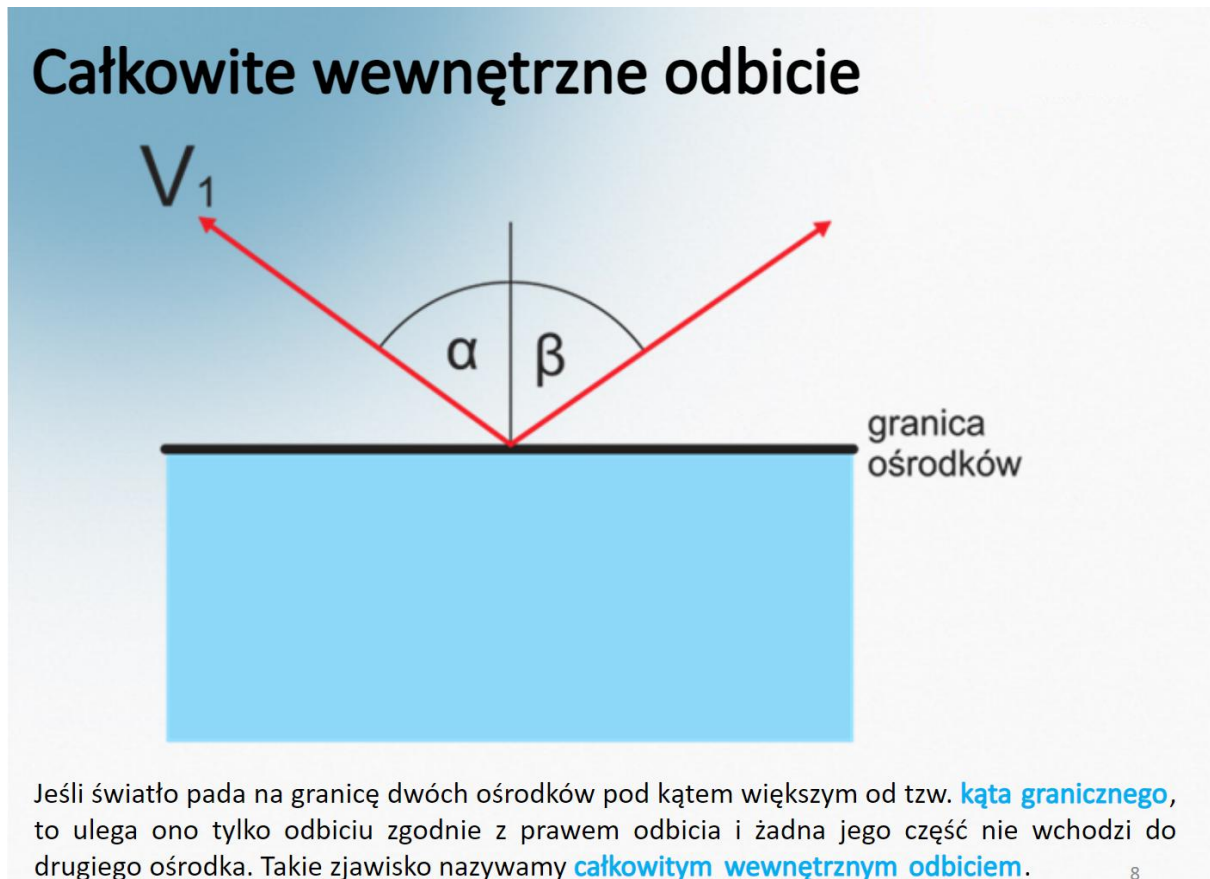
IV okno transmisyjne na fali 1625 nm

Propagacja:

Film pt. Prawa odbicia i załamania światła

<https://www.youtube.com/watch?v=G5SUB82b6Zk>

- Propagacja sygnału (rozchodzenie się) oparta jest na prawie załamania (odbicia).



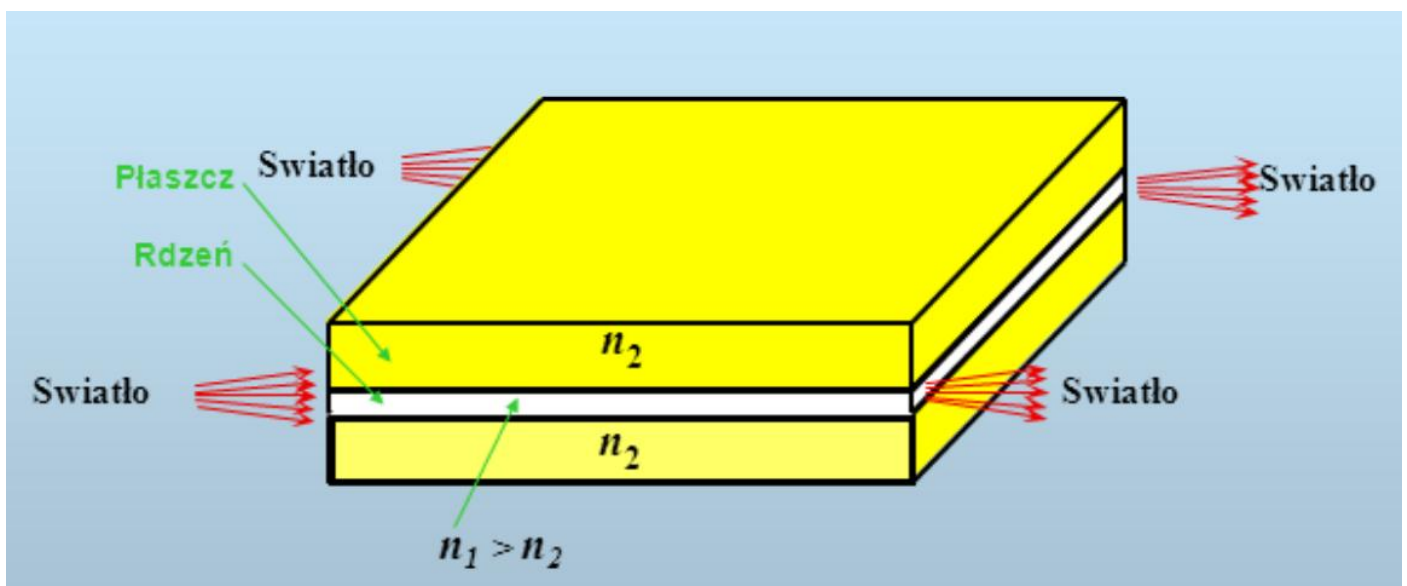
- Zjawisko całkowitego odbicia wewnętrznego stanowi klucz do zrozumienia zasady działania światłowodu.
- Polega ono na całkowitym (wewnętrznym dla włókna) odbiciu promienia świetlnego. Jest to możliwe przy zastosowaniu odpowiedniego kąta α „wejścia” impulsu do włókna.
- Zjawisko odbicia zachodzi na granicy dwóch środowisk o różnym współczynniku załamania n

Geometria światłowodu

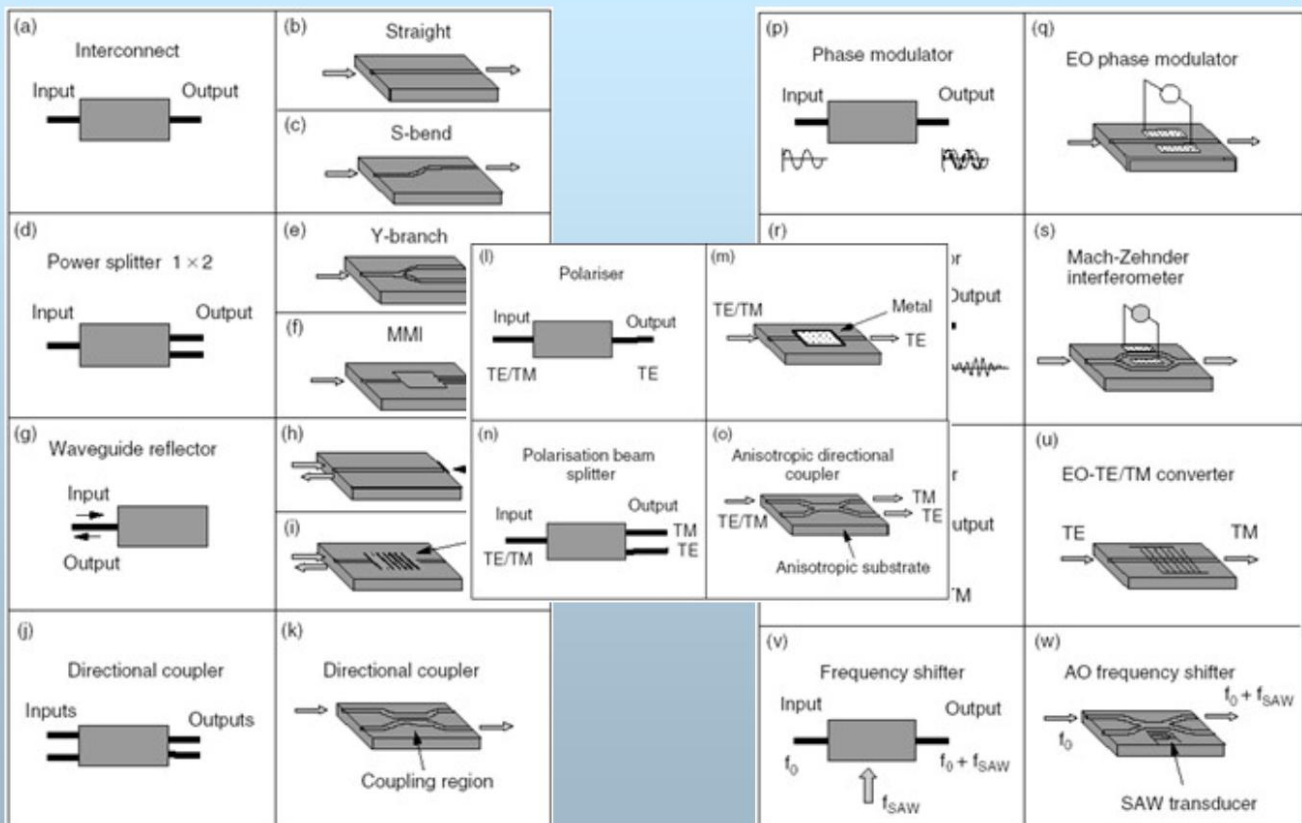
Światłowody telekomunikacyjne dzielimy na **planarne**, **paskowe** i **włókniste**. Pod względem budowy różnią się one przede wszystkim grubością szklanego rdzenia (grubość pozostałych warstw jest taka sama), co wpływa na sposób przesyłania informacji.

Światłowody planarne

Najprostszy światłowód planarny składa się z trzech warstw, z których środkowa ma większy współczynnik załamania, niż warstwy zewnętrzne. Światło jest uwięzione w tej warstwie na skutek całkowitego wewnętrznego odbicia, o ile kierunki rozchodzenia się promieni tworzą z normalną kąty większe od kąta granicznego.

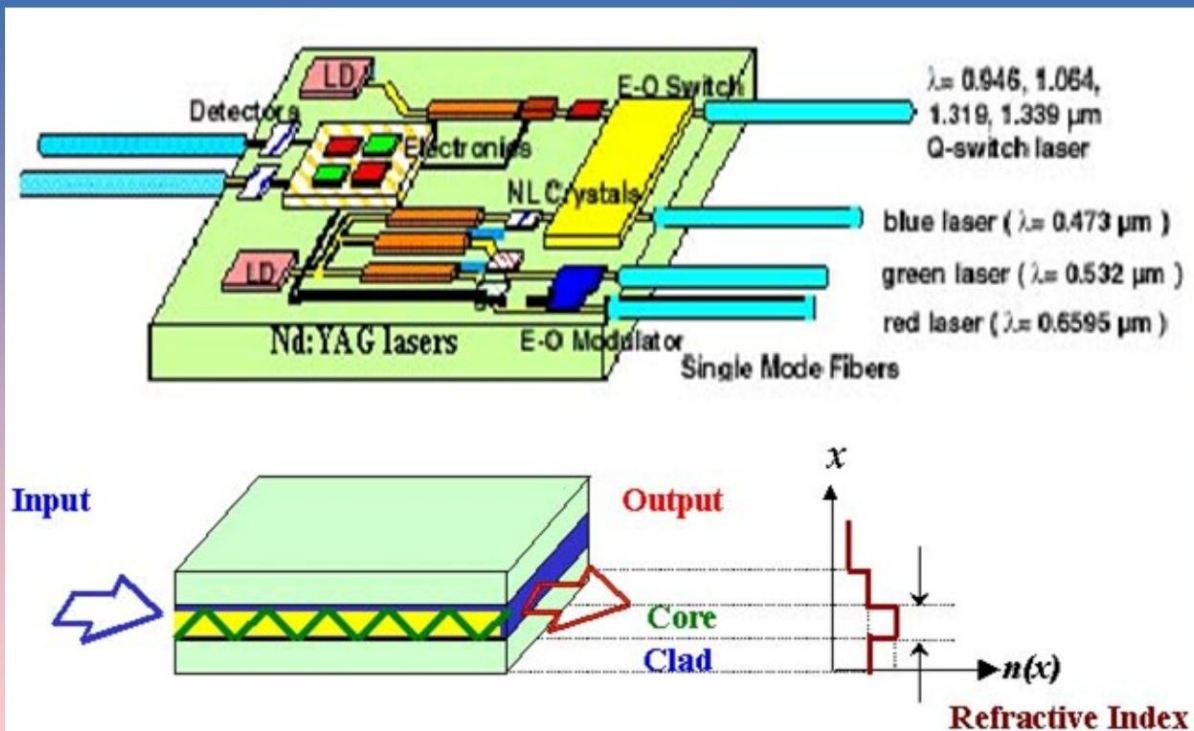


Elementy i układy planarne

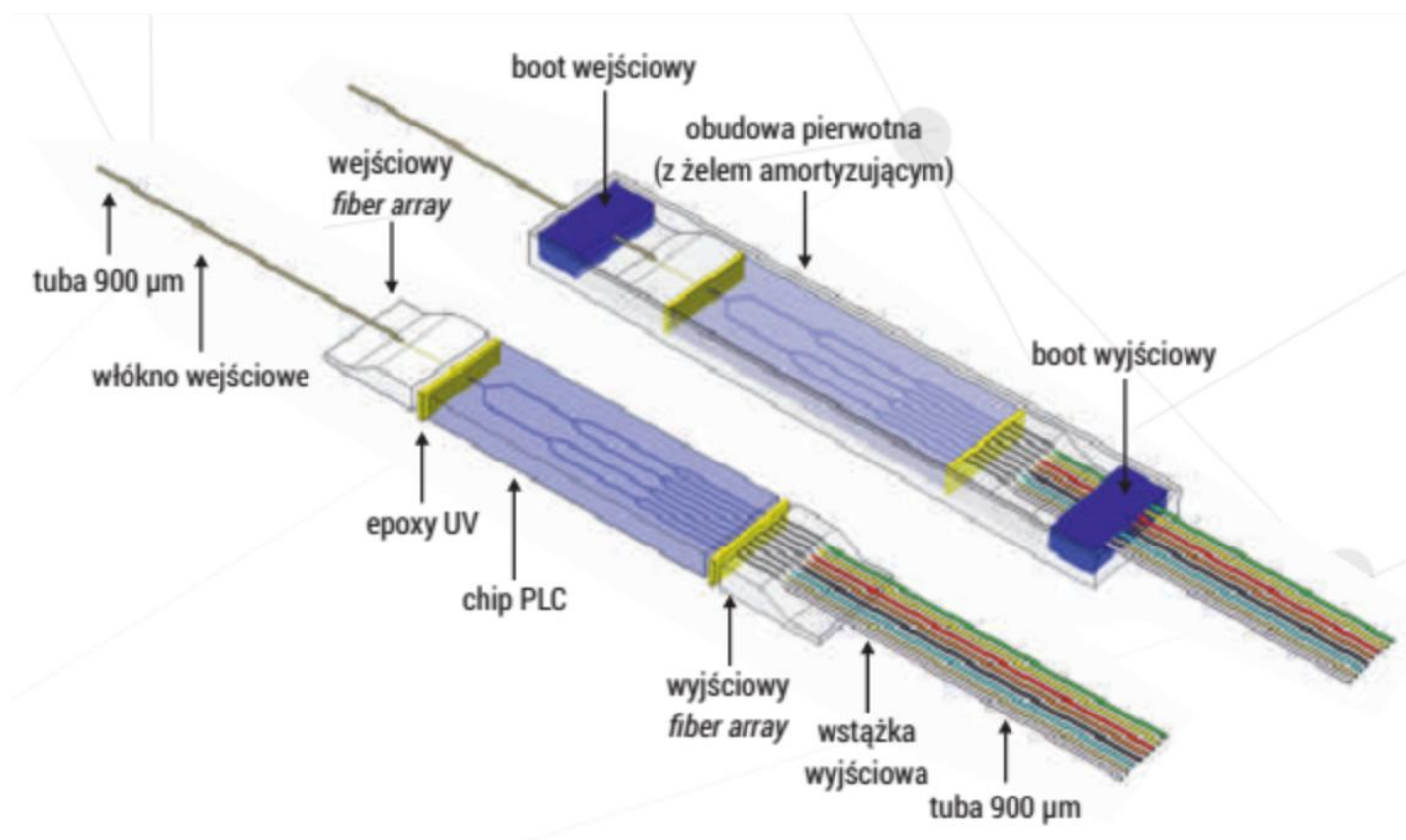


Zintegrowane układy planarne

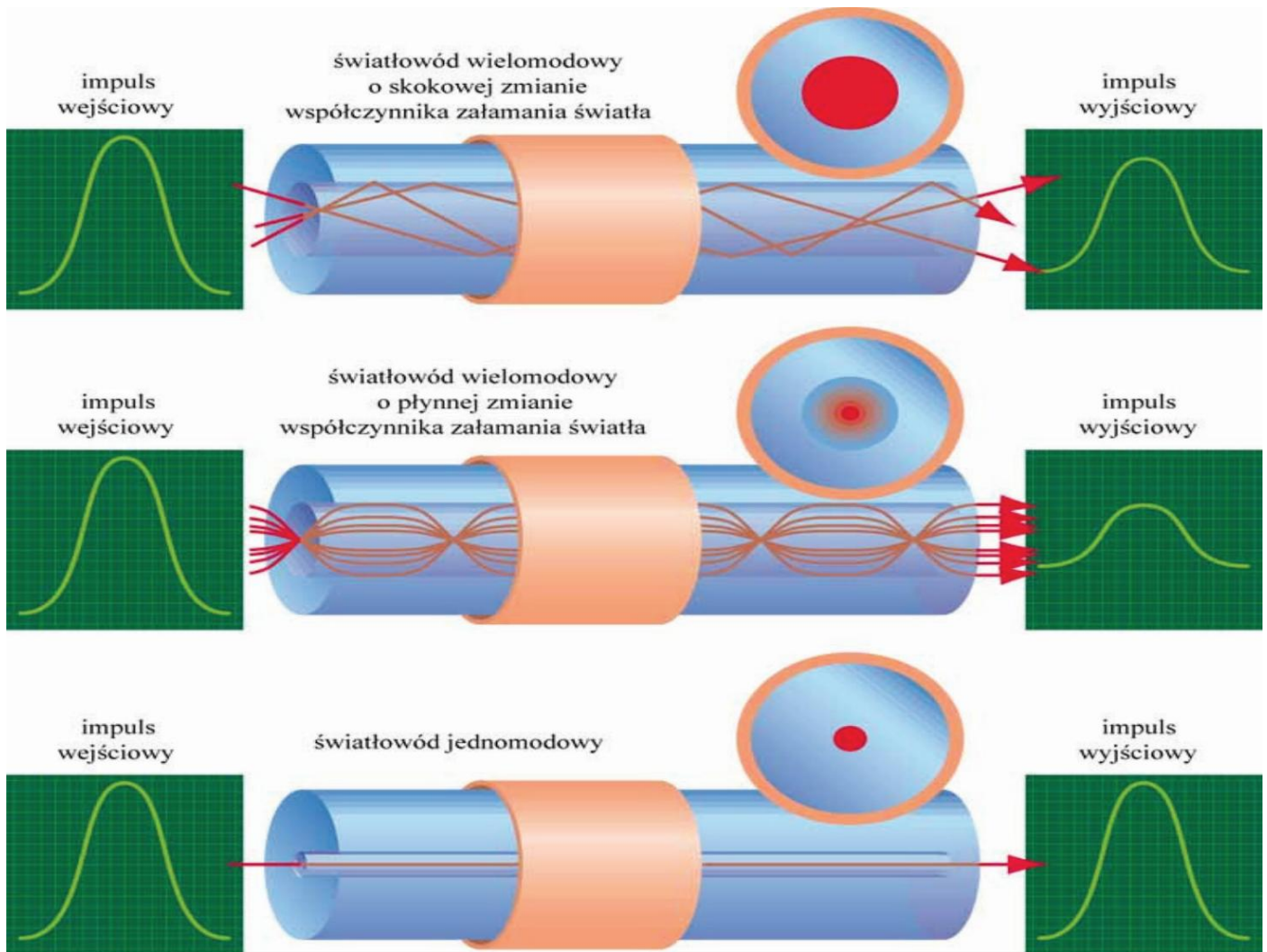
optoelectronics



Światłowody planarne są wykorzystywane w soliterach optycznych



Światłowody włókniste

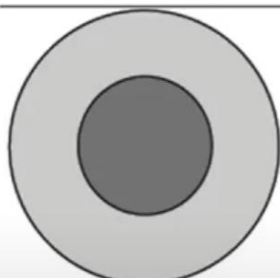


Basic Optical Fiber Types

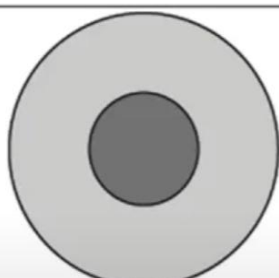
1. Multimode

62.5 micron

50 micron



OM1

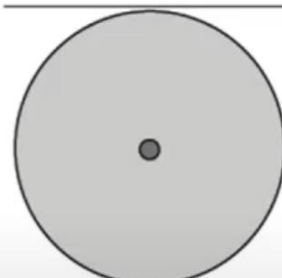


OM2, OM3, OM4

850 nm
& 1300 nm

2. Single-mode

~8 micron



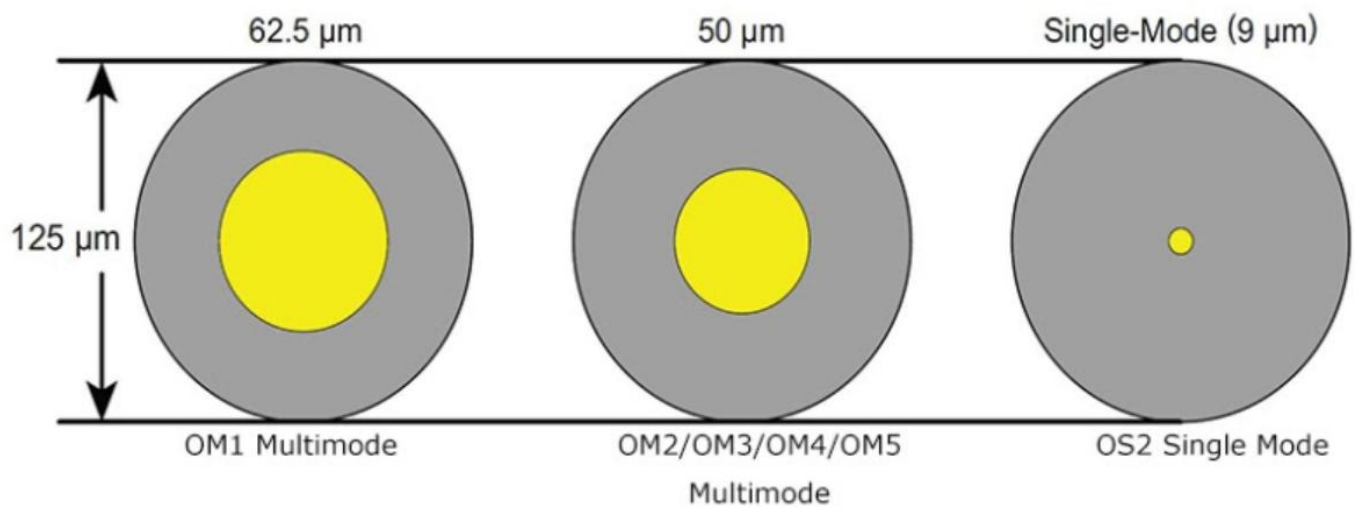
125 micron

OS1

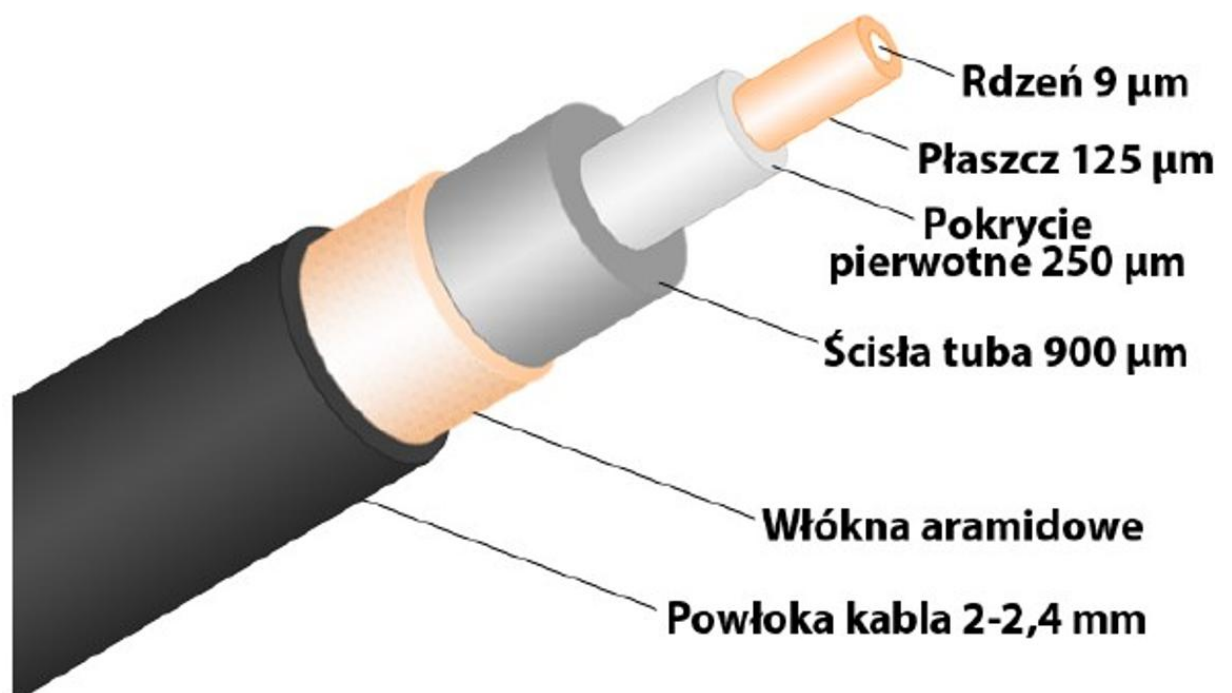
1310 - 1625 nm

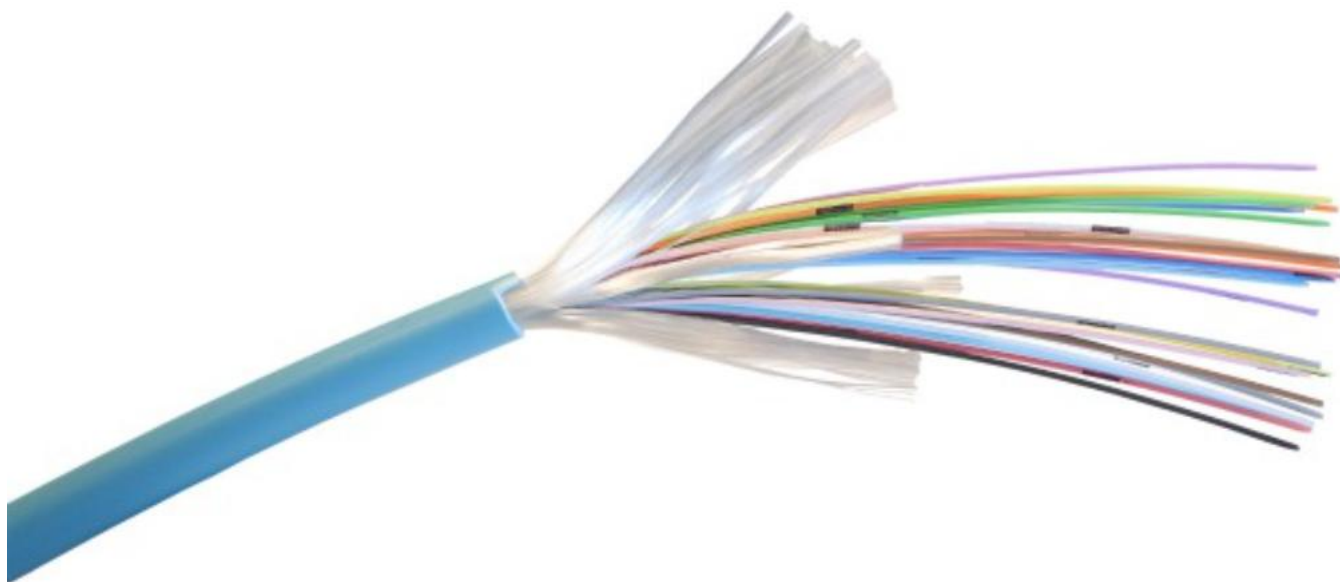
Operating
Wavelengths

Optical Fiber Core Diameters



Budowa Światłowodu jednomodowego - Ścisła tuba



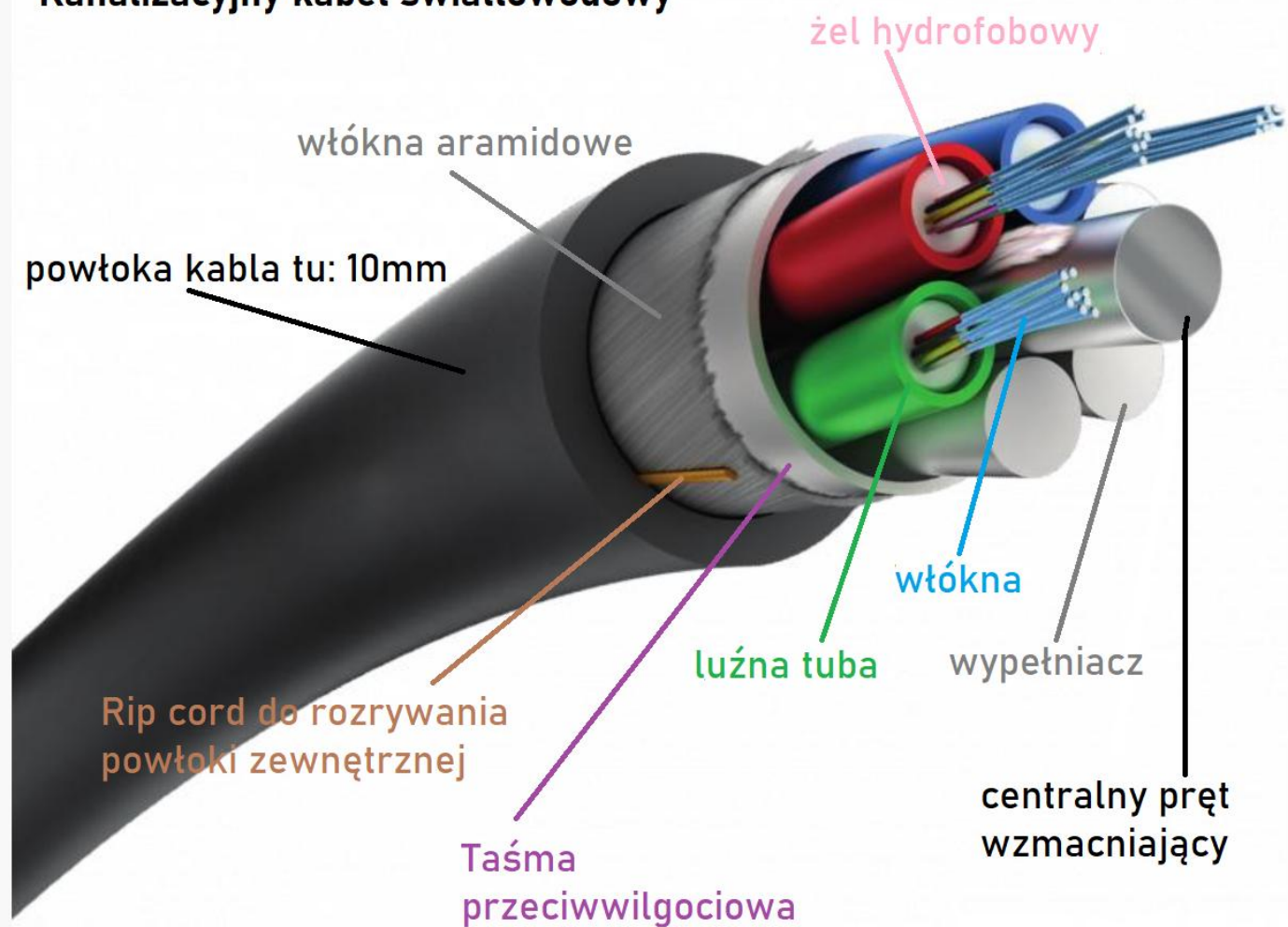


Uniwersalny kabel światłowodowy 24xOM3 ścista tuba



Uniwersalny kabel światłowodowy 6xOM2 ścista tuba

Kanalizacyjny kabel światłowodowy



Kabel światłowodowy Z-XOTKtsdD 48J 4T12F ITU-T G.652D 3kN

Multimode Fiber Jacket Color Codes



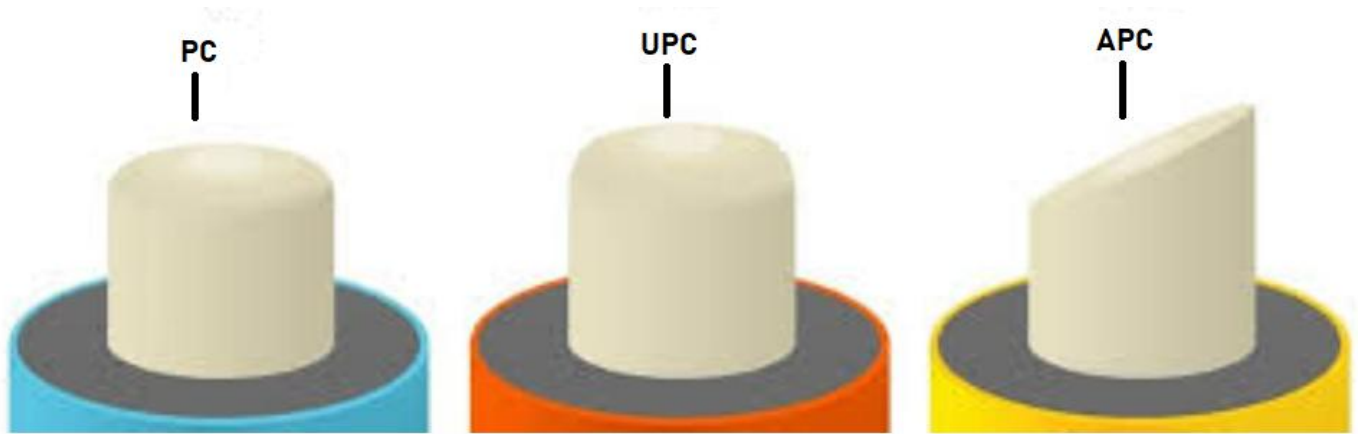
Złącza światłowodowe



Budowa złączki światłowodowej

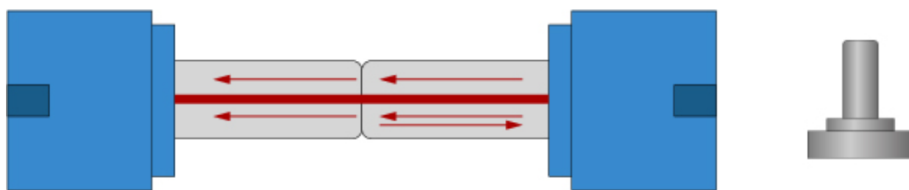
Złącza katowe ze szczeliną powietrzną WAN CATV <table><tr><td></td><td>Tłumienie złącza</td><td>Tłumienie wsteczne</td></tr><tr><td>Szczelina powietrzna</td><td>od 0,4 do 0,8 dB</td><td>> 60 dB</td></tr></table>		Tłumienie złącza	Tłumienie wsteczne	Szczelina powietrzna	od 0,4 do 0,8 dB	> 60 dB	Złącza stykowe PC (Physical Contact) LAN WAN <table><tr><td></td><td>Tłumienie złącza</td><td>Tłumienie wsteczne</td></tr><tr><td>PC (Physical Contact)</td><td>< 0,5 dB</td><td>> 30 dB</td></tr><tr><td>Super</td><td>< 0,5 dB</td><td>> 40 dB</td></tr><tr><td>Ultra</td><td>< 0,5 dB</td><td>> 50 dB</td></tr></table>		Tłumienie złącza	Tłumienie wsteczne	PC (Physical Contact)	< 0,5 dB	> 30 dB	Super	< 0,5 dB	> 40 dB	Ultra	< 0,5 dB	> 50 dB	Złącza katowo-stykowe APC (Angled Physical Contact) WAN CATV <table><tr><td></td><td>Tłumienie złącza</td><td>Tłumienie wsteczne</td></tr><tr><td>Kątowe (8° APC)</td><td>< 0,5 dB</td><td>> 60 dB</td></tr></table>		Tłumienie złącza	Tłumienie wsteczne	Kątowe (8° APC)	< 0,5 dB	> 60 dB
	Tłumienie złącza	Tłumienie wsteczne																								
Szczelina powietrzna	od 0,4 do 0,8 dB	> 60 dB																								
	Tłumienie złącza	Tłumienie wsteczne																								
PC (Physical Contact)	< 0,5 dB	> 30 dB																								
Super	< 0,5 dB	> 40 dB																								
Ultra	< 0,5 dB	> 50 dB																								
	Tłumienie złącza	Tłumienie wsteczne																								
Kątowe (8° APC)	< 0,5 dB	> 60 dB																								
SIMPLEX		DUPLEX																								
VFO																										

PC UPC APC są różnymi stykami tulejek światłowodowych (ferruli), które określają jakość transmisji światłowodowej fali świetlnej, wykonywanej głównie przy stratach powrotu optycznego i stratach wtrąceniowych.

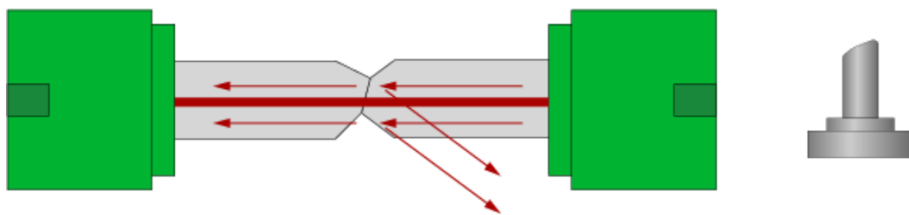


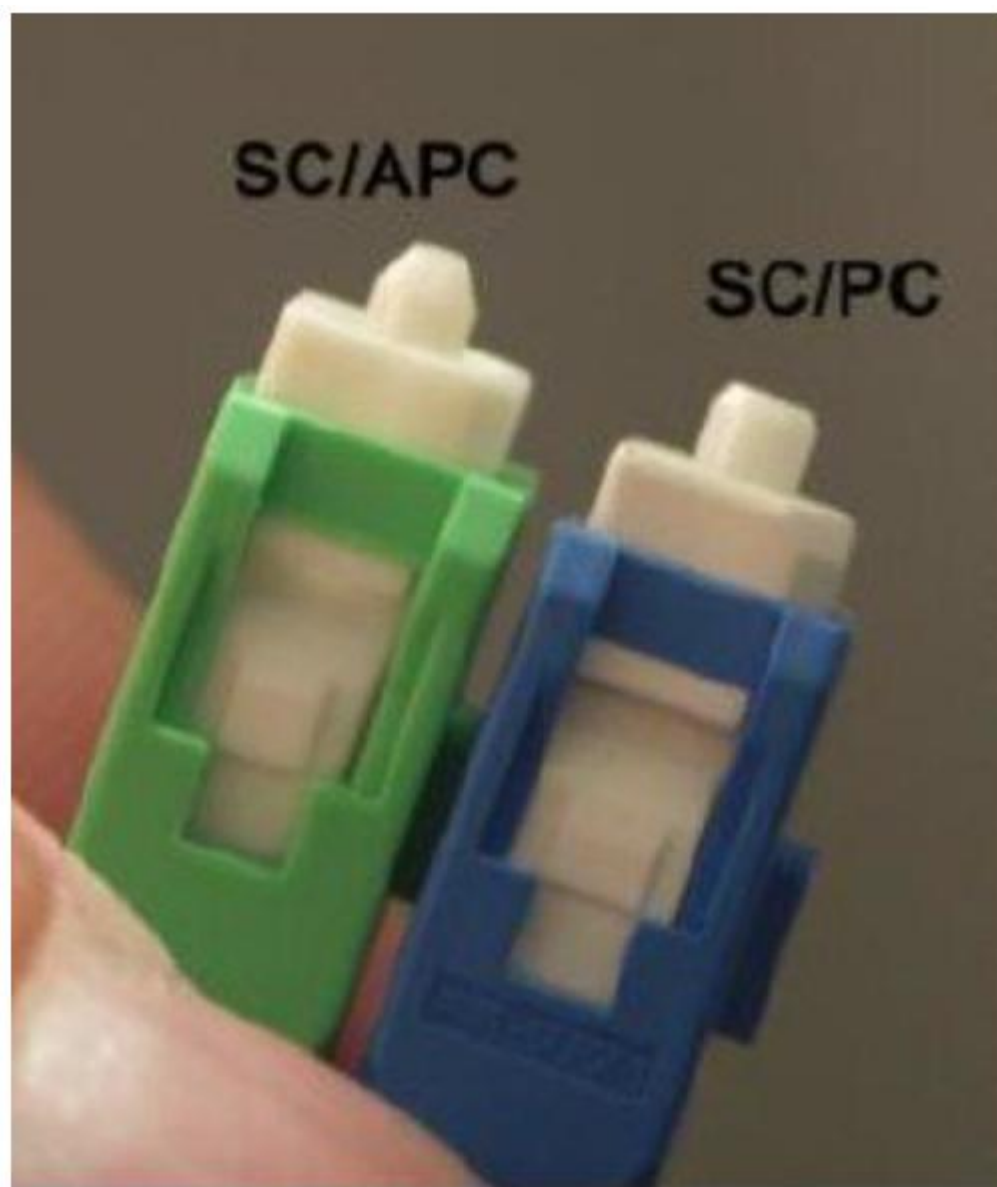
Zdjęcie złączy APC, UPC, PC.

Adapter UPC



Adapter APC

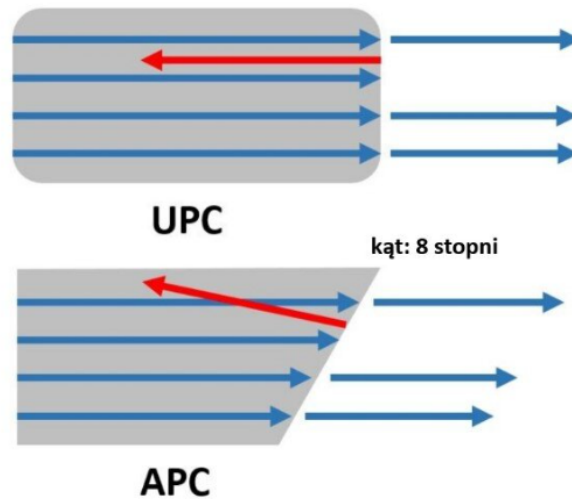




Zdjęcie złączki SC/APC oraz SC/PC

Jak różnica polerowania wpływa na wydajność?

W złączkach UPC światło odbijane jest prosto w kierunku źródła światła, a ustawiona pod kątem 8 stopni końcówka złącza APC odbija światło do okładziny. Powoduje to pewne różnice w stracie powrotnej, która jest pomiarem światła odbitego wyrażonego jako ujemna wartość dB (im wyższa wartość, tym lepiej). Standardy zalecają, aby tłumienie zwrotne złącza UPC wynosiło -50 dB lub więcej (co odpowiada nominalnemu współczynnikowi odbicia 0,001%), a tłumienie zwrotne złącza APC wynosiło -60 dB lub więcej (co odpowiada nominalnemu współczynnikowi odbicia 0,0001%).



Rozpoznawanie elementów światłowodowych – odpowiedź ustna 2

1. Patchcord simplex lub duplex

2. Pigtail

3. Jednomodowy (OS) lub wielomodowy (OM)

4. OM1(62,5), OM2(50),OM3(50),OM4(50),OM5(50),OS1(8),OS2(9)

5. Kolor złączki: zielony – APC

niebieski – PC lub UPC

szary – PC lub UPC

czarny - PC lub UPC

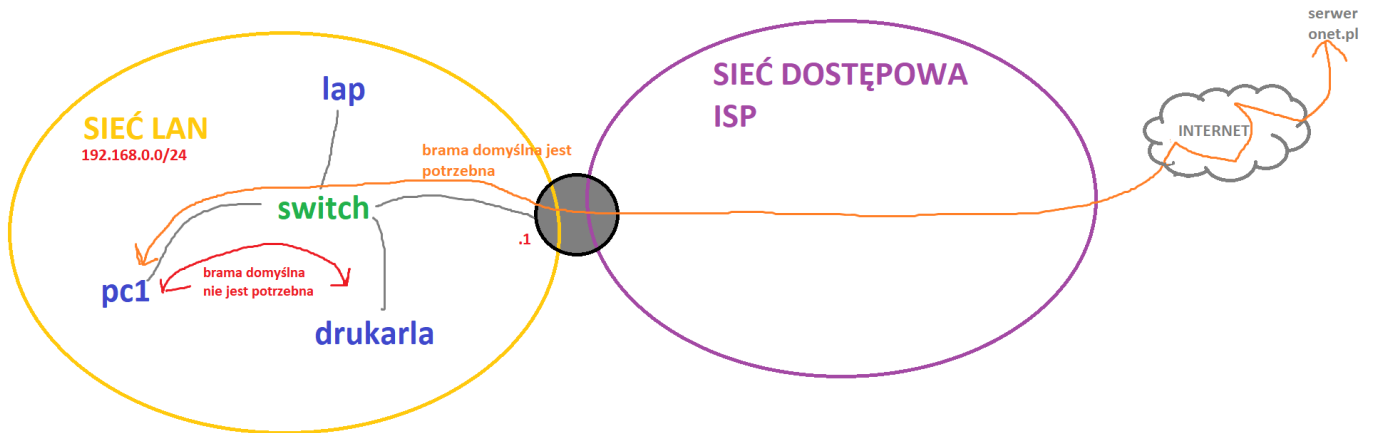
6. Typy złączy: SC, LC, ST, FC, E2000, MPO, MTRJ

7. Adaptery: np. wielomodowy, SC/UPC

2.1 Cisco Packet Tracert

Router to brama domyślna!!!!!!

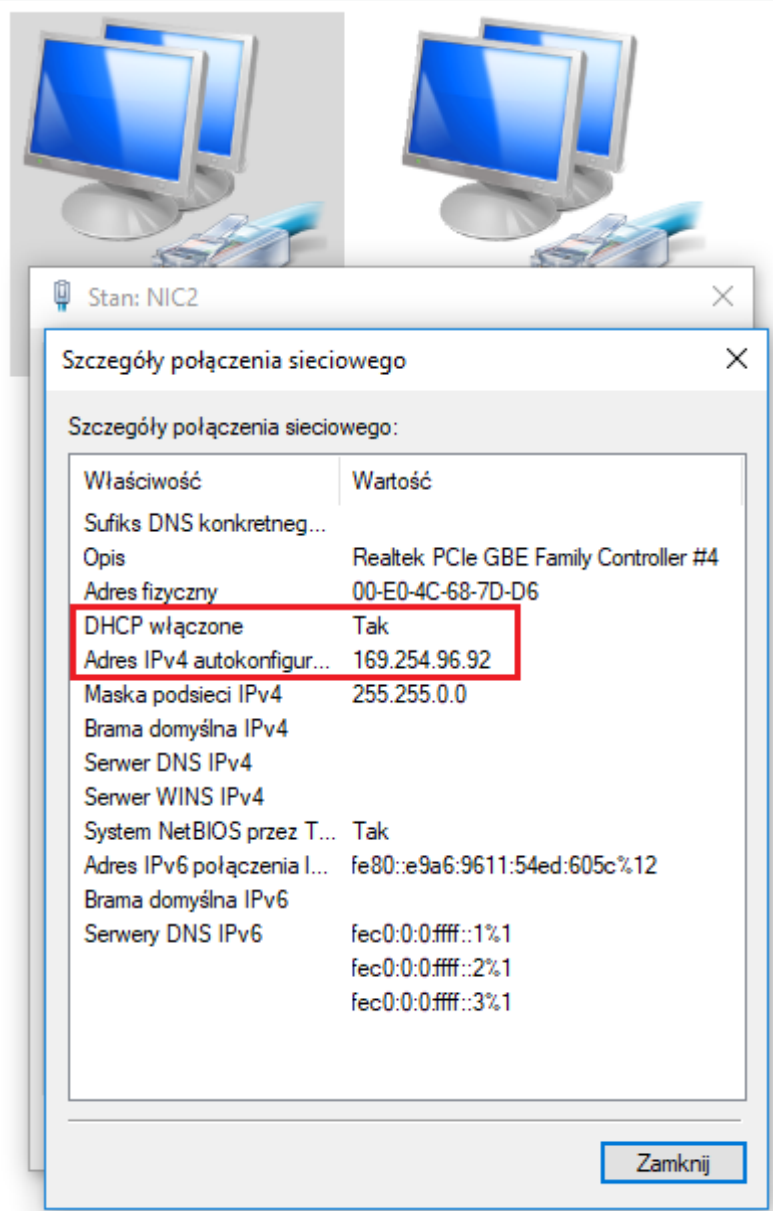
Brama domyślna to urządzenie, które wyprowadza dane z jednej sieci do innej sieci.



Urządzenia, które komunikują się ze sobą w tej samej sieci, nie potrzebują w tej komunikacji bramy domyślnej!!!

Brak połączenia z serwerem DHCP

Kiedy interfejs sieciowy hosta ustawiony na pozyskiwanie adresu automatycznie z serwera DHCP, jest podłączony do sieci, ale nie może się skontaktować z serwerem DHCP otrzymuje adres z puli 169.254.x.x.

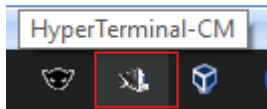


Proces diagnozowania braku połączenia z serwerem DHCP:

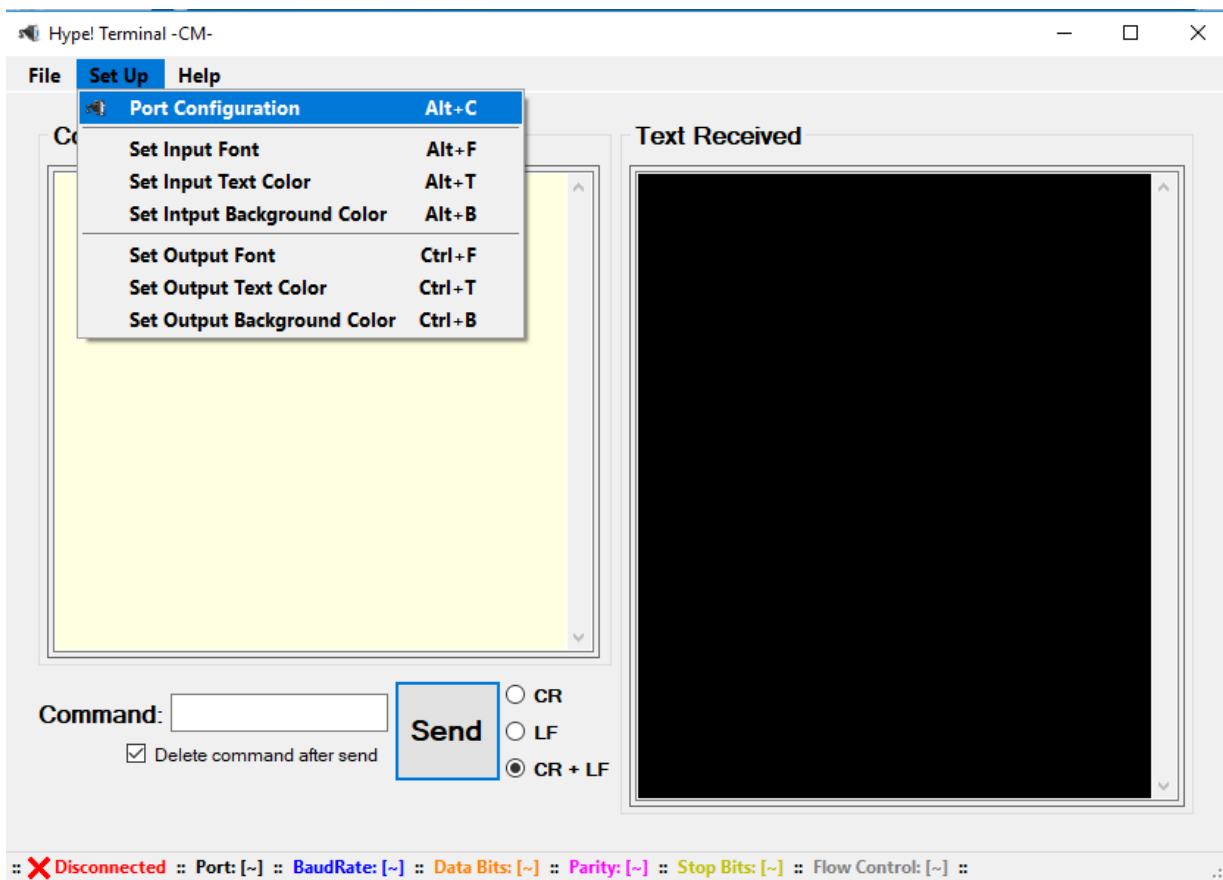
1. Sprawdź, czy kable sieciowe są należycie podłączone (może któryś jest niedociśnięty). Na przełącznikach sprawdź, czy się świecą diody sys i diody używanych portów.
2. Sprawdź, czy urządzenie L3 (Layer 3) z usługą DHCP jest włączone.
3. Sprawdź, czy usługa DHCP jest włączona i poprawnie skonfigurowana na urządzeniu L3.
4. Podłącz hosta bezpośrednio do urządzenia L3 i obserwuj reakcję interfejsu sieciowego. Sprawdź jego adres IPv4.
5. Zresetuj urządzenia sieciowe
6. Zrestartuj hosta
7. W ostateczności wymień urządzenie sieciowe L3, lub interfejs sieciowy hosta.

2.2 Konsolowe resetowanie przełącznika

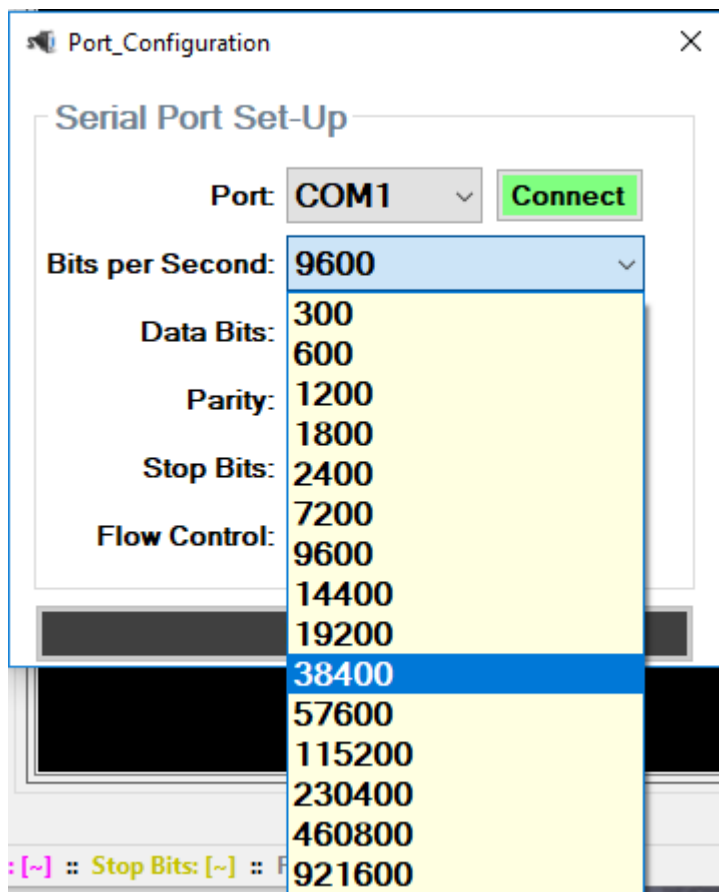
1. Uruchom program Hype Terminal-CM



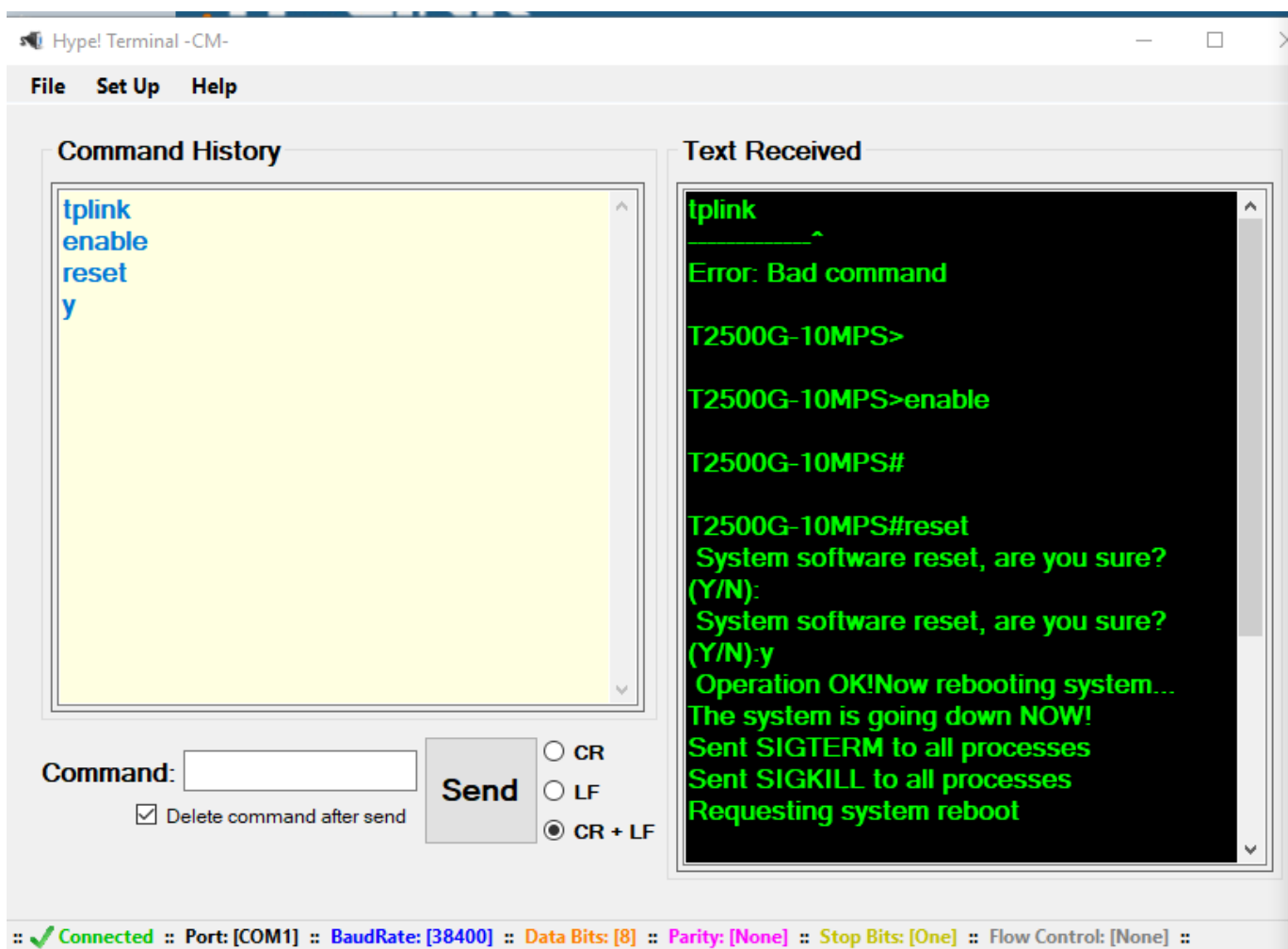
2. Wejdź na zakładkę Port Configuration



3. Wybierz **38400** z listy dla Bits per Second i kliknij **Connect**.

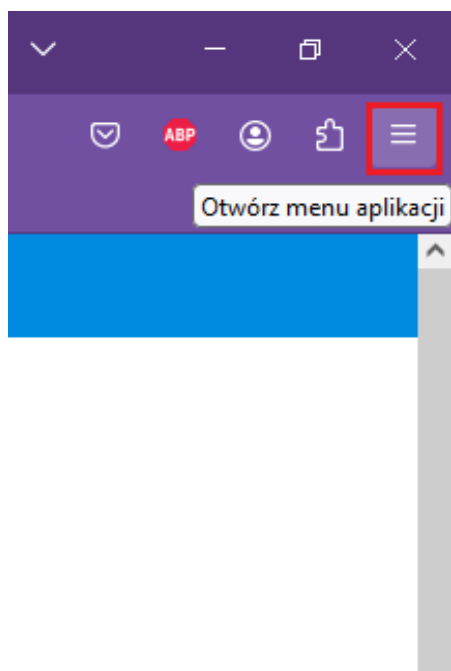


4. W polu Command: wprowadź komendy jak widać poniżej

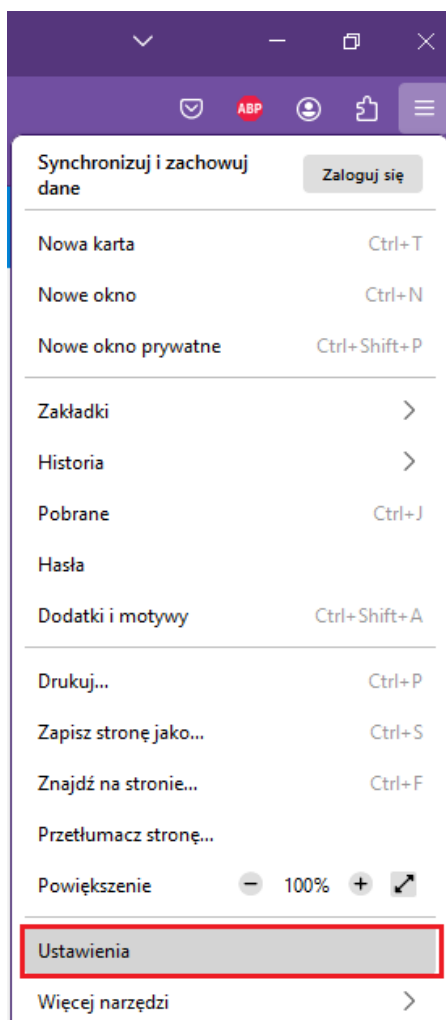


2.3 Wstępne czyszczenie ciasteczek w przeglądarce Firefox

- Otwórz [menu aplikacji](#) przeglądarki Firefox (prawy górny róg ekranu okna przeglądarki)



- Z menu wybierz [Ustawienia](#)



- Wybierz **Prywatność i bezpieczeństwo**

 **Ogólne**

 Uruchamianie

 Wyszukiwanie

 **Prywatność
i bezpieczeństwo**

 Synchronizacja

 Więcej od Mozilli

Ogólne

Uruchamianie

- ☐ Otwieranie poprzednich okien i kart
- ☐ Automatyczne otwieranie Firefoksa po włączeniu komputera
- ☒ Sprawdzanie, czy Firefox jest domyślną przeglądarką

 Firefox jest obecnie domyślną przeglądarką

Importowanie danych z innych przeglądarek

Importuj zakładki, hasła, historię i dane automatyczne Firefoksa.

- Przewiń kółkiem myszki w dół, aż do sekcji **Ciasteczka i dane witryn** i wyczyść dane przeglądarki

Ciasteczka i dane witryn

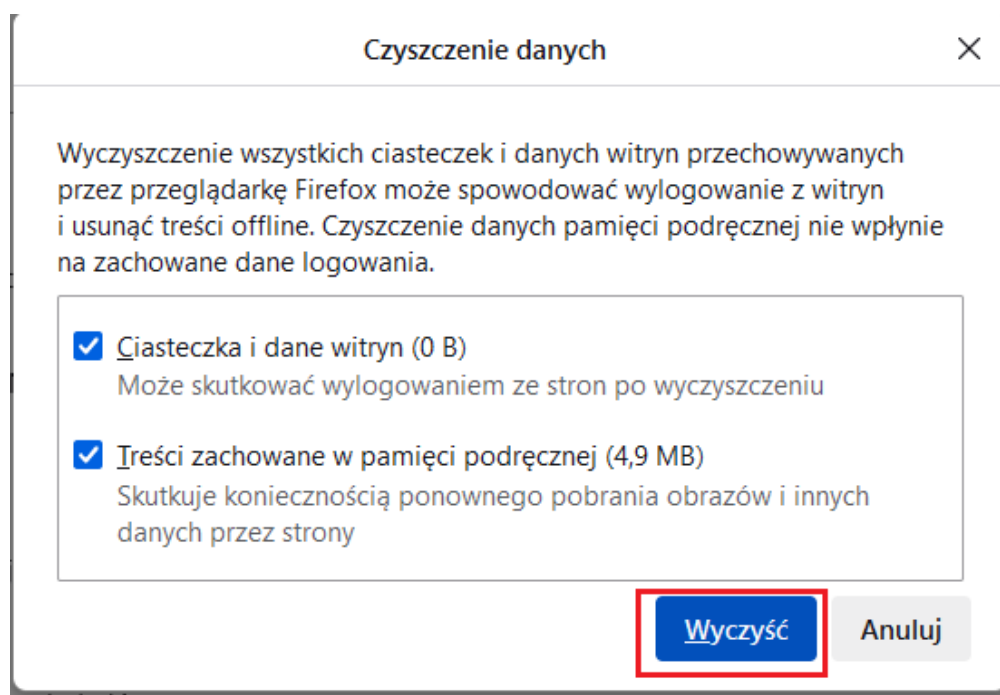
Przechowywane ciasteczka, dane i pamięć podręczna witryn zajmują 4,9 MB na dysku. [Więcej informacji](#)

- ☒ **Usuwanie ciasteczek i danych witryn podczas zamykania przeglądarki Firefox**

Wyczyść dane...

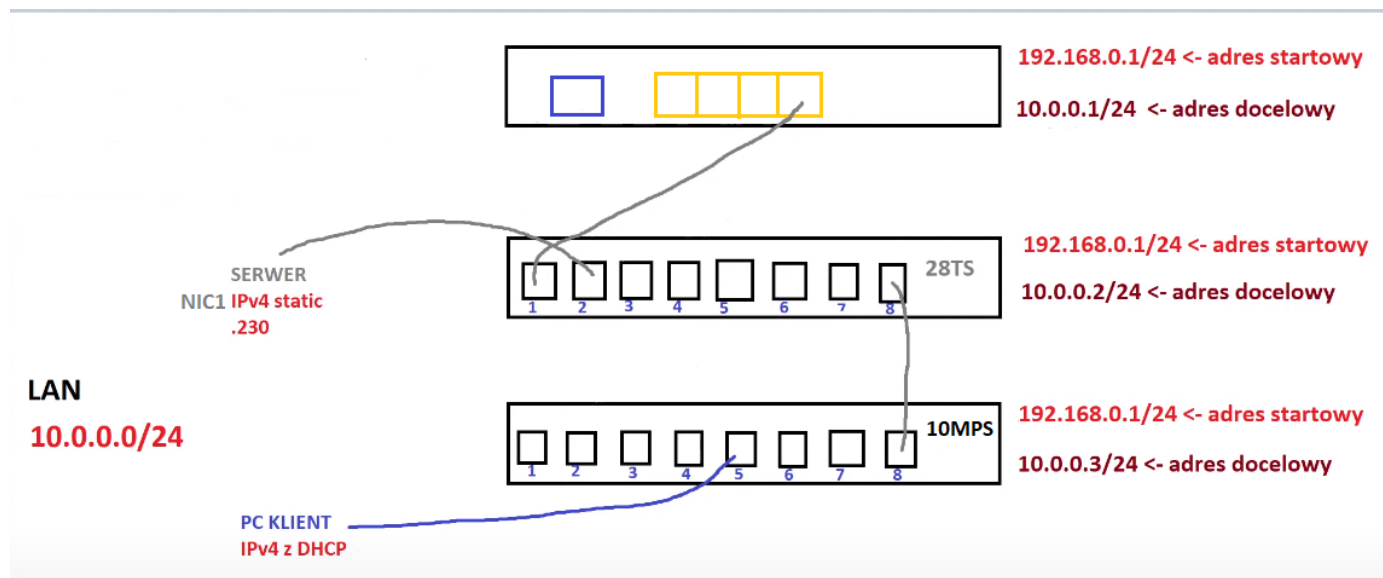
Zachowane dane...

Wyjątki...



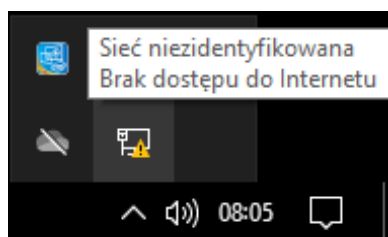
2.4 Wstępna konfiguracja przełączników

1. Zresetuj urządzenia sieciowe do fabrycznych ustawień b
2. Połącz ze sobą urządzenia sieciowe oraz urządzenia końcowe jak na poniższym obrazku

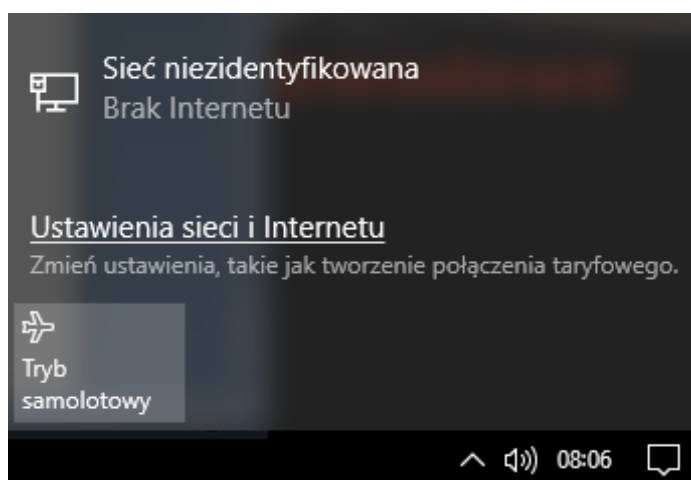


3. Sprawdź ustawienia karty sieciowej **SERWERA**

Lpm kliknij na ikonę dostępu do Internetu



Następnie wejdź w [Ustawienia sieci i Internetu](#)



Kliknij na zakładkę [Ethernet](#)

Ustawienia

Strona główna

Znajdź ustawienie

Sieć i Internet

Stan

Ethernet

Telefoniczne

VPN

Zużycie danych

Serwer proxy

Stan

Stan sieci



Brak dostępu do Internetu

Twoje urządzenie jest połączone, ale może nie być możliwy dostęp do wszystkich elementów w sieci. Jeśli masz ograniczony plan taryfowy, możesz ustawić tę sieć jako połączenie taryfowe lub zmienić inne właściwości.

Rozwiąż problemy

[Zmień właściwości połączenia](#)

[Pokaż dostępne sieci](#)

Wybierz [Zmień opcje karty](#)

Ustawienia

Strona główna

Znajdź ustawienie

Sieć i Internet

Stan

Ethernet

Telefoniczne

VPN

Zużycie danych

Serwer proxy

Ethernet

Ethernet

 Sieć niezidentyfikowana
Brak Internetu

 Sieć niezidentyfikowana
Brak Internetu

Pokrewne ustawienia

Zmień opcje karty

[Zmień opcje zaawansowane udostępniania](#)

[Centrum sieci i udostępniania](#)

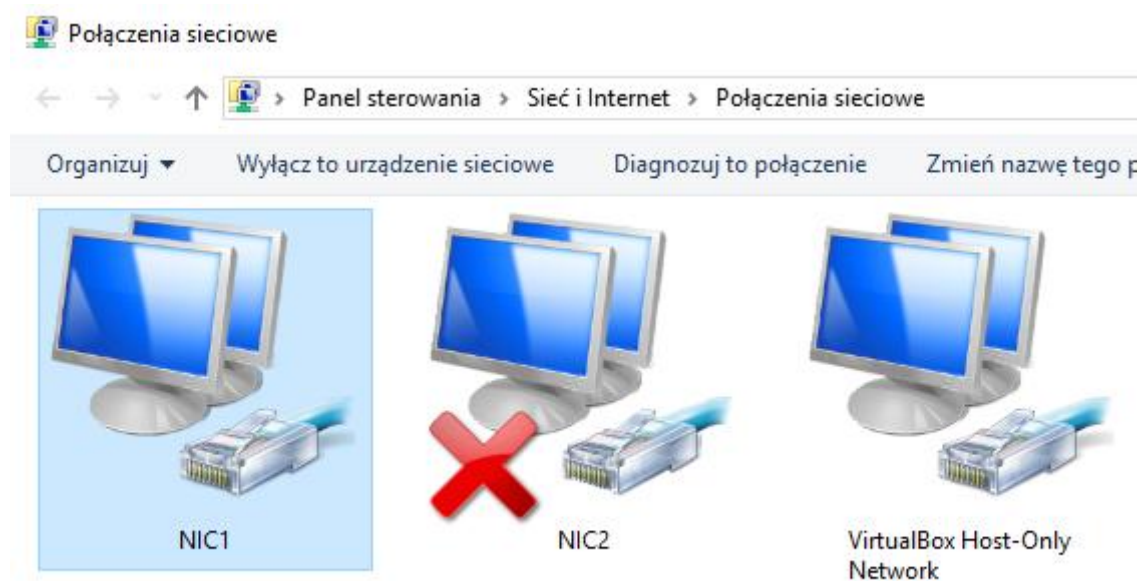
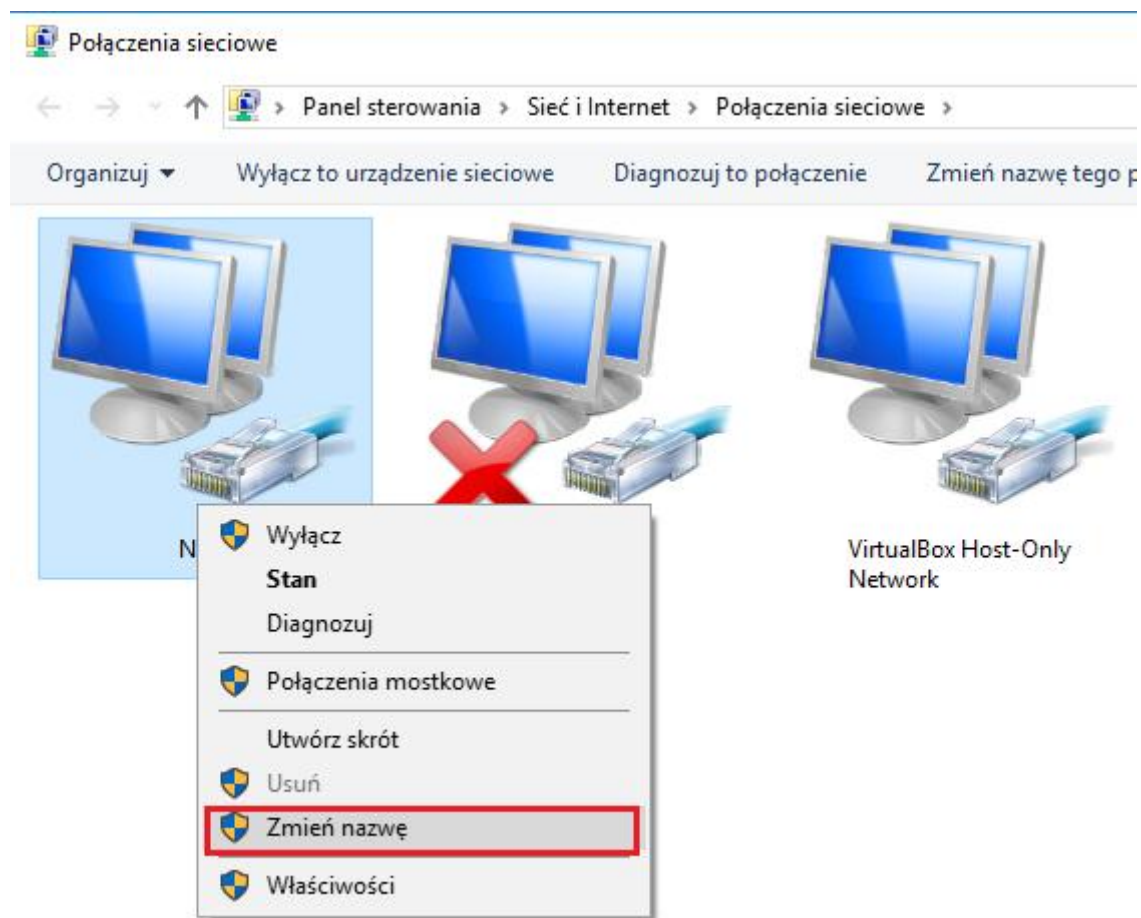
[Grupa domowa](#)

[Zapora systemu Windows](#)

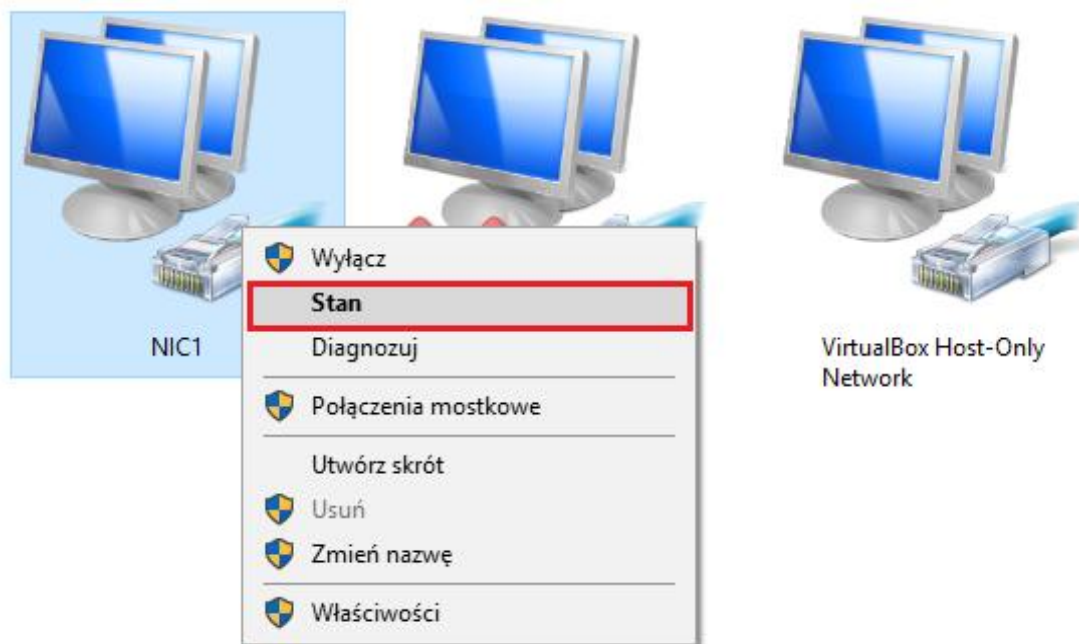
Zmień nazwy interfejsów sieciowych na **NIC1** i **NIC2**

NIC1 to interfejs, który jest podłączony kablem do przełącznika **28TS**

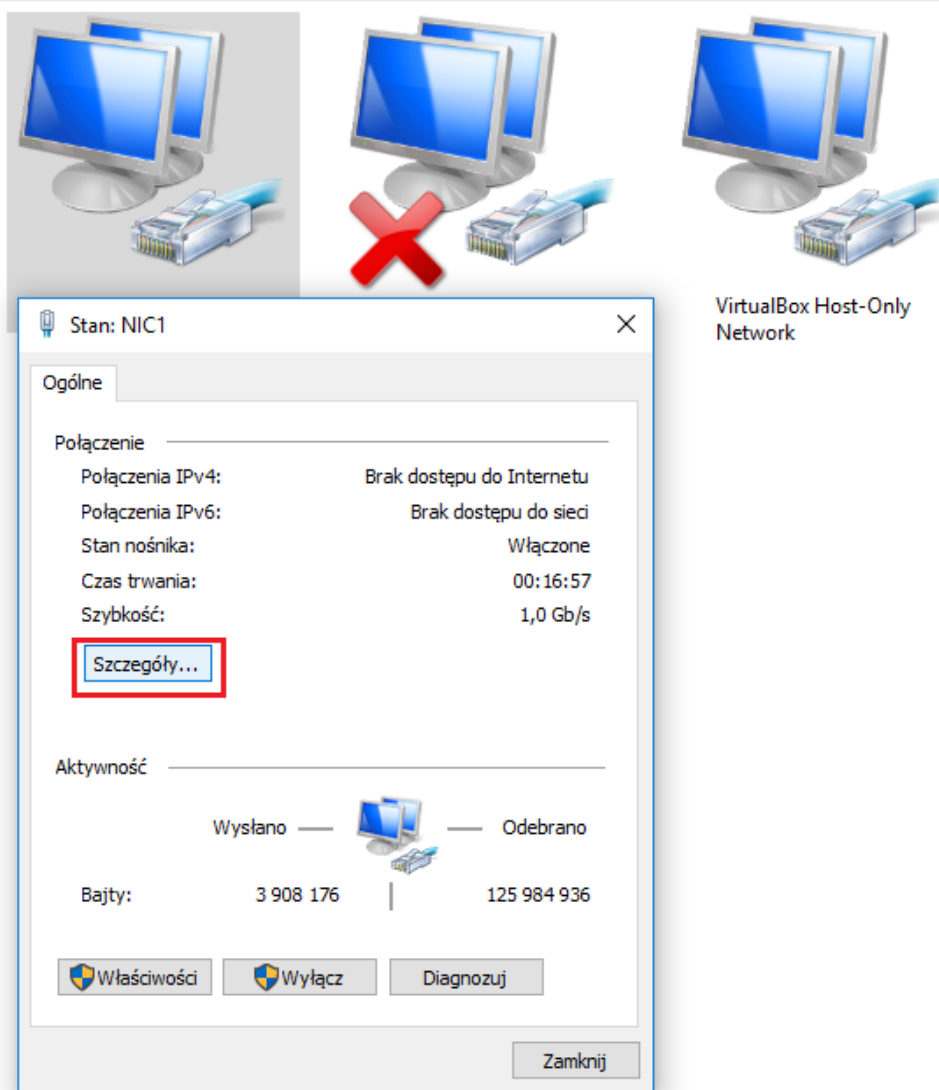
NIC2 nie jest podłączony, dlatego widnieje na nim czerwony X.



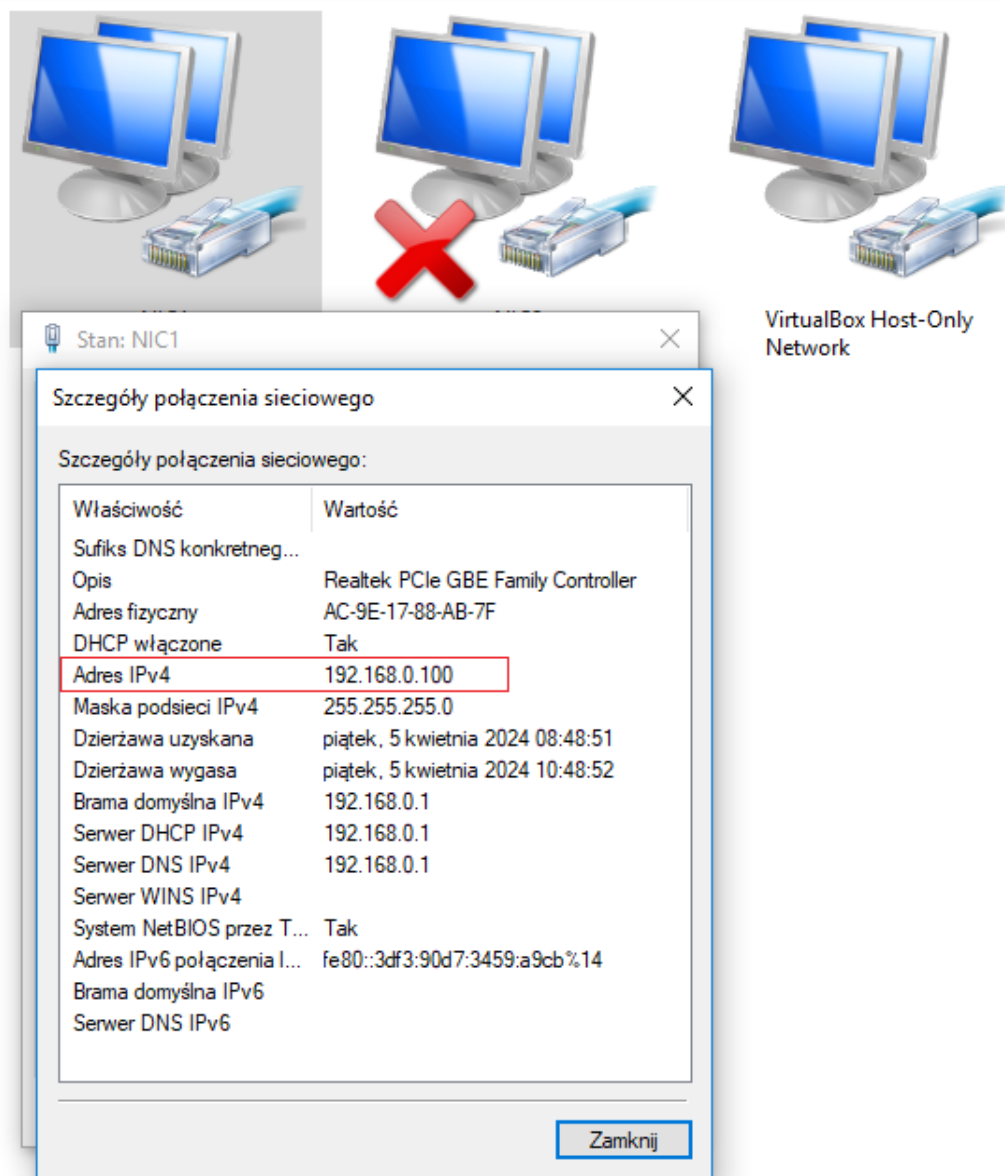
Sprawdź stan karty sieciowej **NIC1**. W tym celu kliknij **ppm** na ikonie interfejsu sieciowego i wybierz opcję **Stan**.



Następnie kliknij **lpm** na [Szczegóły...](#)

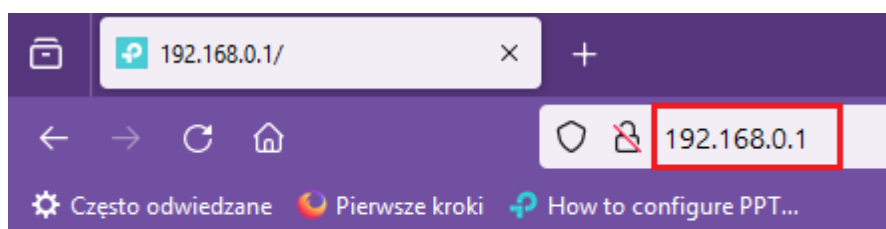


Teraz możesz zobaczyć jaki adres sieciowy IPv4 został przypisany dla interfejsu **NIC1**. Jest to w tym przypadku adres **192.168.0.100**. Adres ten umożliwi Ci teraz wejście na zresetowane do ustawień fabrycznych przełączniki.



3. Logowanie się na przełączniki

Wpisz w pasku przeglądarki adres domyślny przełącznika **192.168.0.1**



UWAGA! Jeżeli wyświetlił Ci się panel routera, to na chwilę odepnij kabel łączący router z przełącznikiem 28TS. Sprawdź czy Adres IPv4 jest podtrzymywany na karcie sieciowej SERWERA (Patrz obrazek z punktu drugiego). Może bowiem być tak, że SERWER utraci otrzymany Adres IPv4 na skutek utraty połączenia z routerem. Jeśli Adres IPv4 zostanie faktycznie utracony, podłącz router z przełącznikiem 28TS ponownie i zacznij procedurę jeszcze raz od punktu drugiego zadania. Jak sobie z tym nie poradzisz poproś Administratora o pomoc 😊.

Jeżeli Adres IPv4 na karcie SERWERA jest podtrzymywany, to w nowym oknie przeglądarki wpisz ponownie adres IPv4 **192.168.0.1**.

Pojawi się okno logowania do systemu.

Fabryczne dane do logowania:

login: admin

hasło: admin



User
Name:

Password:

Login

Clear

Wybierz zakładkę **ROUTING**

T2600G-28TS

- System
- System Info**
- User Management
- System Tools
- Access Security
- SDM Template
- Switching
- VLAN
- Spanning Tree
- Ethernet OAM
- Multicast
- Routing**
- QoS

System Summary

Device Description

System Time

Daylight S

Port Status

UNIT: 1

System Info

UNIT: 1

System Description:	JetStream 24-Port Gigabit L2 Ma
Device Name:	T2600G-28TS
Device Location:	SHENZHEN
Contact Information:	www.tp-link.com
Hardware Version:	T2600G-28TS 2.0

Edytuj Vlan1

Interface Config

Creating Interface

Interface ID: VLAN (1-4094)

IP Address Mode: ☒ None ☐ Static ☐ DHCP ☐ BOOTP

IP Address: (Format: 192.168.0.1)

Subnet Mask: (Format: 255.255.255.0)

Admin Status: Enable

Interface Name: (Optional. 1-16 characters)

Create

Interface List

Select	ID	Mode	IP Address	Subnet Mask	Interface Name	Status	Operation
☐	Vlan1	Static	192.168.0.1	255.255.255.0		Up	Edit Edit IPv6 Detail

All
Delete
Help

Wprowadź adres docelowy przełącznika **10.0.0.2/24**

Modify Interface

Interface ID: Vlan1

IP Address Mode: ☐ None ☒ Static ☐ DHCP ☐ BOOTP

IP Address: 10.0.0.2 (Format: 192.168.0.1)

Subnet Mask: 255.255.255.0 (Format: 255.255.255.0)

Admin Status: Enable

Interface Name: (Optional. 1-16 characters)

Apply

Back

Teraz powinieneś utracić połączenie z przełącznikiem.



Przerwane połączenie

Połączenie z serwerem zostało zresetowane podczas wczytywania strony.

Wpisz w przeglądarce docelowy adres przełącznika 28TS **10.0.0.2**. Połączenie z nim nie będzie możliwe, ponieważ przełącznik **28TS** ma adres **10.0.0.2/24**, a **NIC1** ma **192.168.0.100/24**.



Przekroczono limit czasu połączenia

Serwer 10.0.0.2 zbyt długo nie odpowiada.

- Witryna może być tymczasowo niedostępna lub przeciążona. Spróbuj ponowi

Ponownie wpisz w pasku przeglądarki adres fabryczny **192.168.0.1** w celu połączenia się z przełącznikiem **T2500G-10MPS**. Pojawi się okno logowania do systemu.

UWAGA! Jeżeli wyświetlił Ci się panel routera, to na chwilę odepnij kabel łączący router z przełącznikiem 28TS. Sprawdź czy Adres IPv4 jest podtrzymany na karcie sieciowej SERWERA (Patrz obrazek z punktu drugiego). Może bowiem być tak, że SERWER utraci otrzymany Adres IPv4 na skutek utraty połączenia z routerem. Jeśli Adres IPv4 zostanie faktycznie utracony, podłącz router z przełącznikiem 28TS ponownie i zacznij procedurę jeszcze raz od punktu drugiego zadania. Jak sobie z tym nie poradzisz poproś Administratora o pomoc ☺.

Jeżeli Adres IPv4 na karcie SERWERA jest podtrzymany, to w nowym oknie przeglądarki wpisz ponownie adres IPv4 **192.168.0.1**.

Fabryczne dane do logowania:

login: admin

hasło: admin

Wybierz zakładkę System Info/System IP

T2500G-10MPS

System Summary | Device Description | System Time | Daylight Saving Time | Serial Port Setting | **System IP**

System

- System Info**
- User Management
- System Tools
- Access Security

Switching

VLAN

Spanning Tree

Multicast

DHCP

QoS

PoE

IP Config

MAC Address: AC-84-C6-4A-9C-2C

IP Address Mode: ☒ Static IP ☐ DHCP ☐ BOOTP

Management VLAN: 1 (VLAN ID: 1-4094)

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Note:
Changing IP address to a different IP segment will interrupt the network communication, so please keep the new IP address in the same IP segment with the local network.

Apply

Help

Ustaw docelowy adres IPv4 **10.0.0.3/24** z bramą domyślną (router) **10.0.0.1**. Zatwierdź ustawienie klikając przycisk **Apply**.

tp-link

T2500G-10MPS

System Summary | Device Description | System Time | Daylight Saving Time | Serial Port Setting | **System IP**

System

- System Info**
- User Management
- System Tools
- Access Security

Switching

VLAN

Spanning Tree

Multicast

DHCP

QoS

IP Config

MAC Address: AC-84-C6-4A-9C-2C

IP Address Mode: ☒ Static IP ☐ DHCP ☐ BOOTP

Management VLAN: 1 (VLAN ID: 1-4094)

IP Address: 10.0.0.3

Subnet Mask: 255.255.255.0

Default Gateway: 10.0.0.1

Note:
Changing IP address to a different IP segment will interrupt the network communication, so please keep the new IP address in the same IP segment with the local network.

Apply

Help

Ponownie utracisz połączenie z przełącznikiem **10MPS**. Połączenie z nim nie będzie możliwe, ponieważ przełącznik **10MPS** ma adres **10.0.0.3/24**, a **NIC1** ma **192.168.0.100/24**.

Przekroczono limit czasu połączenia

Serwer 10.0.0.3 zbyt długo nie odpowiada.

- Witryna może być tymczasowo niedostępna lub przeciążona. Spróbuj ponownie za pewien czas.
- Jeśli nie możesz otworzyć żadnej strony, sprawdź swoje połączenie sieciowe.
- Jeśli ten komputer jest chroniony przez zaporę sieciową lub serwer proxy, należy sprawdzić, czy Firefox jest uprawniony do łączenia się z Internetem.

Spróbuj ponownie

2.5 Dlaczego nie mogę się dostać na przełącznik sieciowy.

Oto kilka potencjalnych przyczyn i sposobów ich rozwiązania:

1. **Niepoprawne połączenie fizyczne:** Upewnij się, że przewody sieciowe są poprawnie podłączone zarówno do twojego urządzenia, jak i do przełącznika. Sprawdź, czy światła na przełączniku migają, co wskazuje na poprawne połączenie.
2. **Ustawienia sieciowe:** Sprawdź, czy twoje urządzenie ma poprawnie skonfigurowane ustawienia sieciowe. Upewnij się, że używasz odpowiedniego protokołu, adresu IP, maski podsieci i bramy domyślnej.
3. **Adresacja IP:** Sprawdź, czy twoje urządzenie ma unikatowy adres IP w sieci. Jeśli korzystasz z adresacji dynamicznej (DHCP), upewnij się, że serwer DHCP jest aktywny i prawidłowo działa.
4. **Karta sieciowa:** Sprawdź, czy karta sieciowa w twoim urządzeniu działa poprawnie. Możesz to zrobić, sprawdzając menedżer urządzeń w systemie operacyjnym.
5. **Ograniczenia dostępu:** Upewnij się, że nie ma żadnych reguł blokujących dostęp do przełącznika na poziomie sieci lub urządzenia (np. firewall, lista kontroli dostępu itp.).
6. **Ustawienia przełącznika:** Jeśli masz dostęp do panelu administracyjnego przełącznika, sprawdź jego ustawienia, aby upewnić się, że nie ma żadnych blokad lub filtrów, które mogą uniemożliwiać dostęp do twojego urządzenia.

Jeśli mimo podejmowania tych kroków nadal masz problemy, **najlepiej** skonsultować się **z administratorem sieci** lub osobą odpowiedzialną za zarządzanie sprzętem sieciowym, aby uzyskać dalszą pomoc.

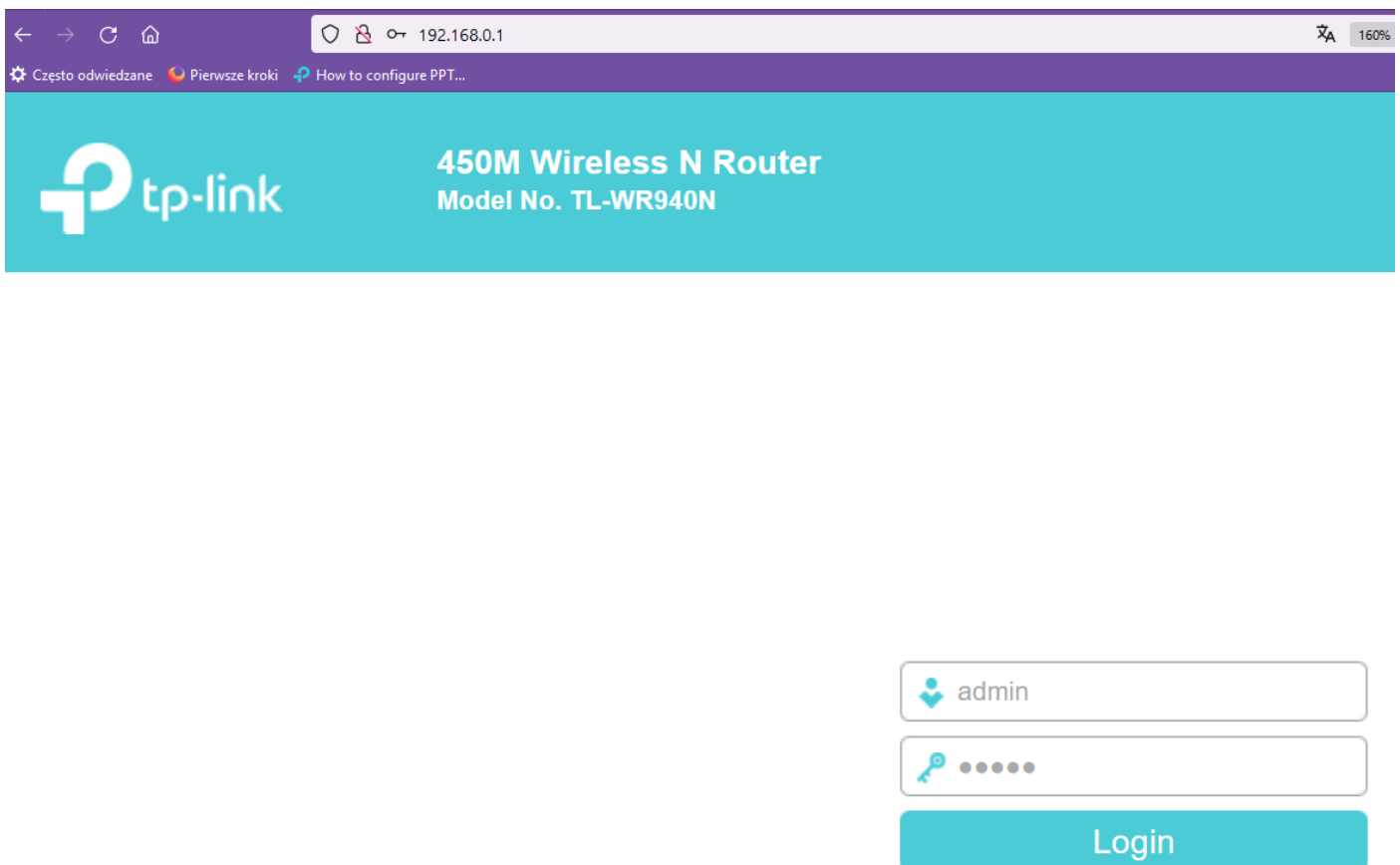
2.6 Wstępna konfiguracja routera – zmiana adresu IPv4 LAN urządzenia

1. Wpisz w pasku przeglądarki adres IPv4 **192.168.0.1** routera przywróconego wcześniej do fabrycznych ustawień.

Fabryczne dane do logowania:

login: admin

hasło: admin



← → ↻ 🏠 192.168.0.1 160%

⚙️ Często odwiedzane 🍷 Pierwsze kroki 🗑️ How to configure PPT...

 **450M Wireless N Router**
Model No. TL-WR940N

 admin

 •••••

Login

2. Wejdź w zakładkę Network/LAN, żeby edytować adres IPv4 routera

Status	
Quick Setup	
WPS	
Working Mode	
Network	
- WAN	
- MAC Clone	
- LAN	
- IPTV	
Wireless	
Guest Network	
DHCP	

LAN

MAC Address:

98-DA-C4-64-61-86

IP Address:

192.168.0.1

Subnet Mask:

255.255.255.0 ▾

Save

Status	
Quick Setup	
WPS	
Working Mode	
Network	
- WAN	
- MAC Clone	
- LAN	
- IPTV	
Wireless	

LAN

MAC Address:

98-DA-C4-64-61-86

IP Address:

10.0.0.1

Subnet Mask:

255.255.255.0 ▾

Save

LAN

MAC Address: 98-DA-C4-64-61-86

IP Address: 10.0.0.1

Subnet Mask: 255.255.255.0

Save

192.168.0.1

Modification of LAN Settings will result in the rebooting of this device, OK?

OK

Anuluj

Status

Quick Setup

WPS

Working Mode

Network

- WAN

- MAC Clone

- LAN

- IPTV

Wireless

Guest Network

Restart

Configuration Completed Successfully.

Restarting...

23%





Ta witryna jest nieosiągalna

Serwer **10.0.0.1** potrzebował zbyt wiele czasu na odpowiedź.

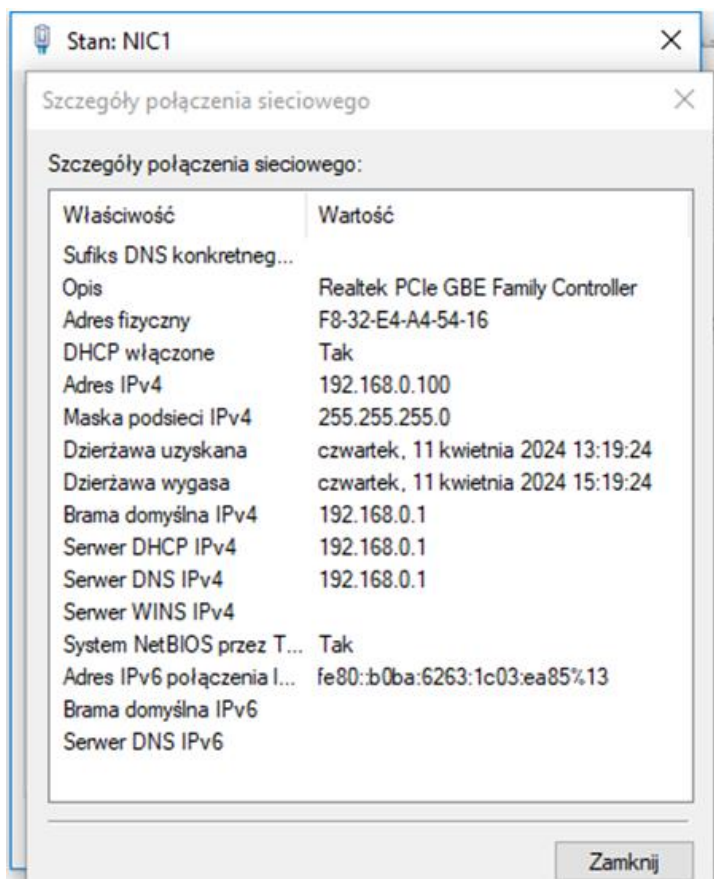
Wypróbuj te rozwiązania:

- Sprawdź połączenie
- Sprawdź serwer proxy i zaporę sieciową
- Uruchom Diagnostykę sieci systemu Windows

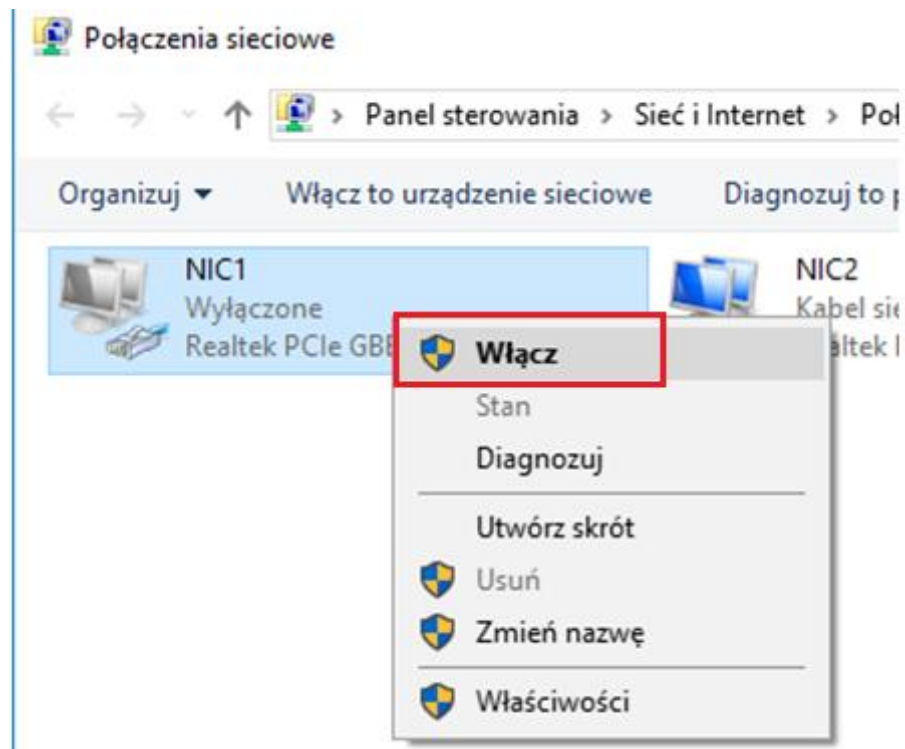
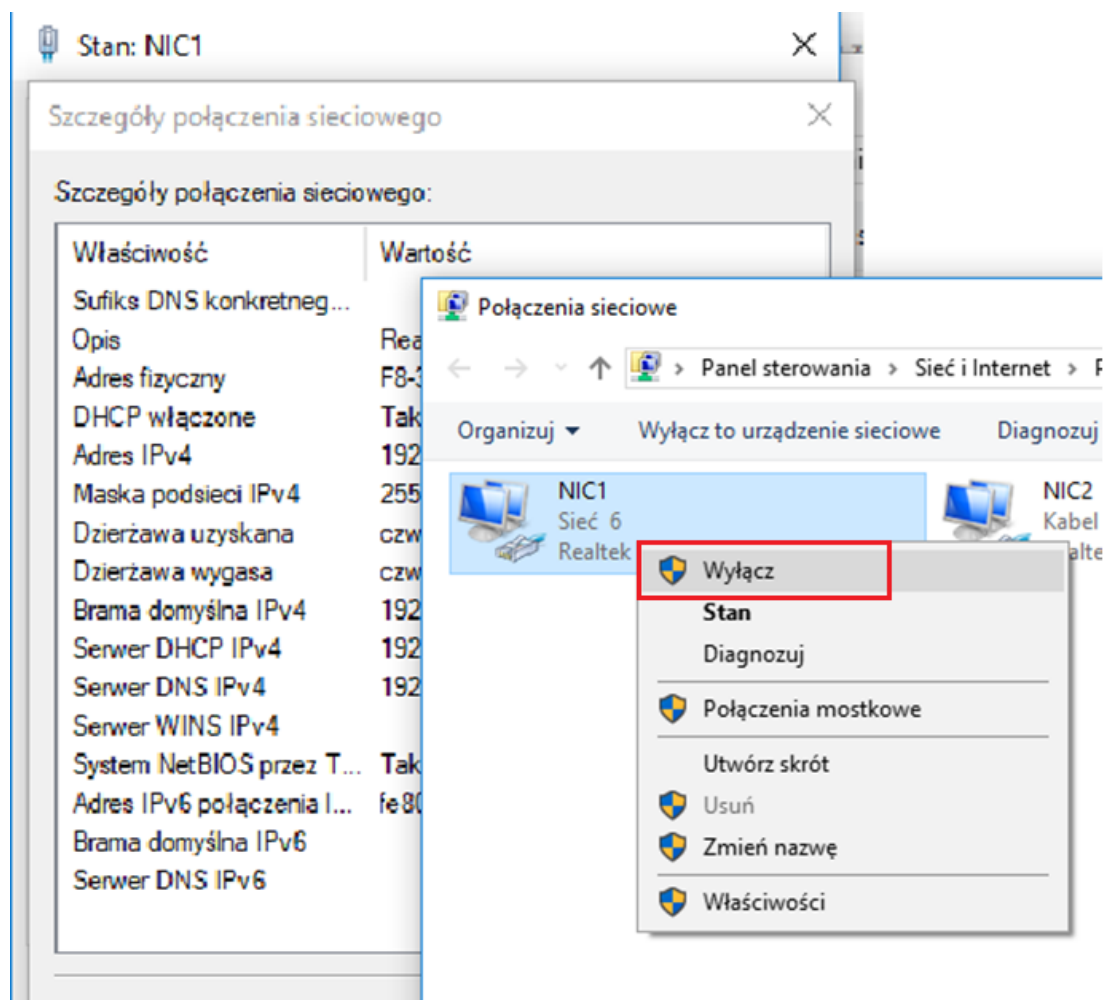
ERR_CONNECTION_TIMED_OUT

Odśwież

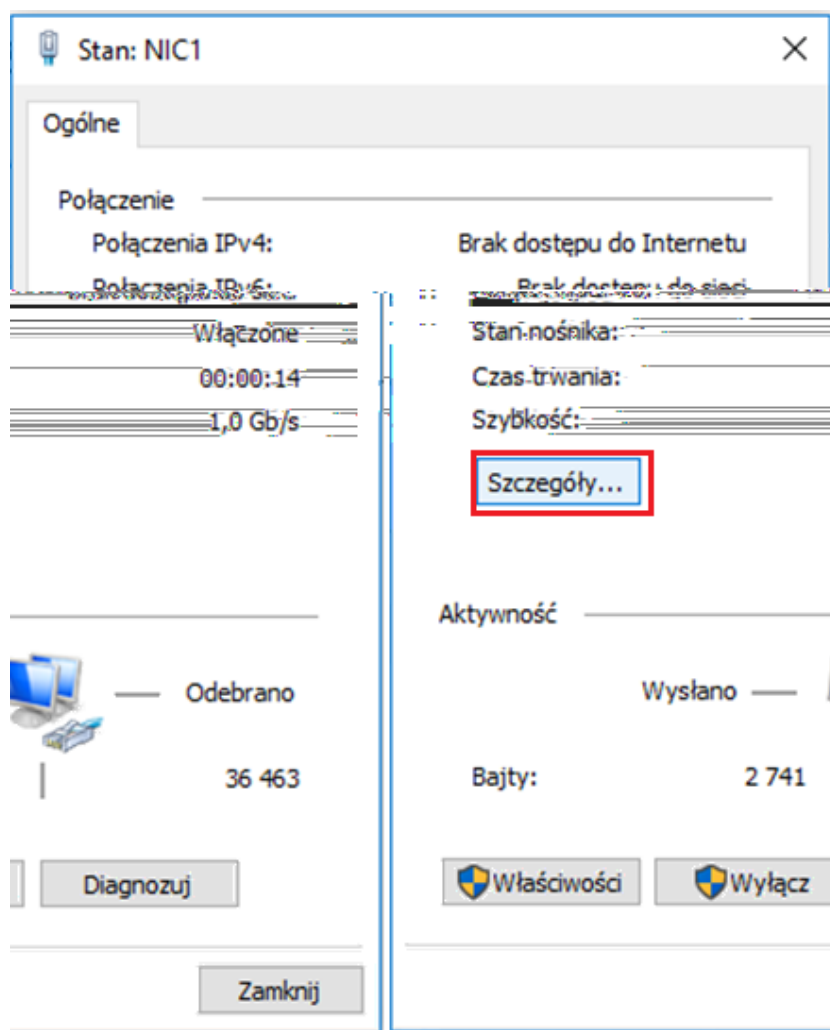
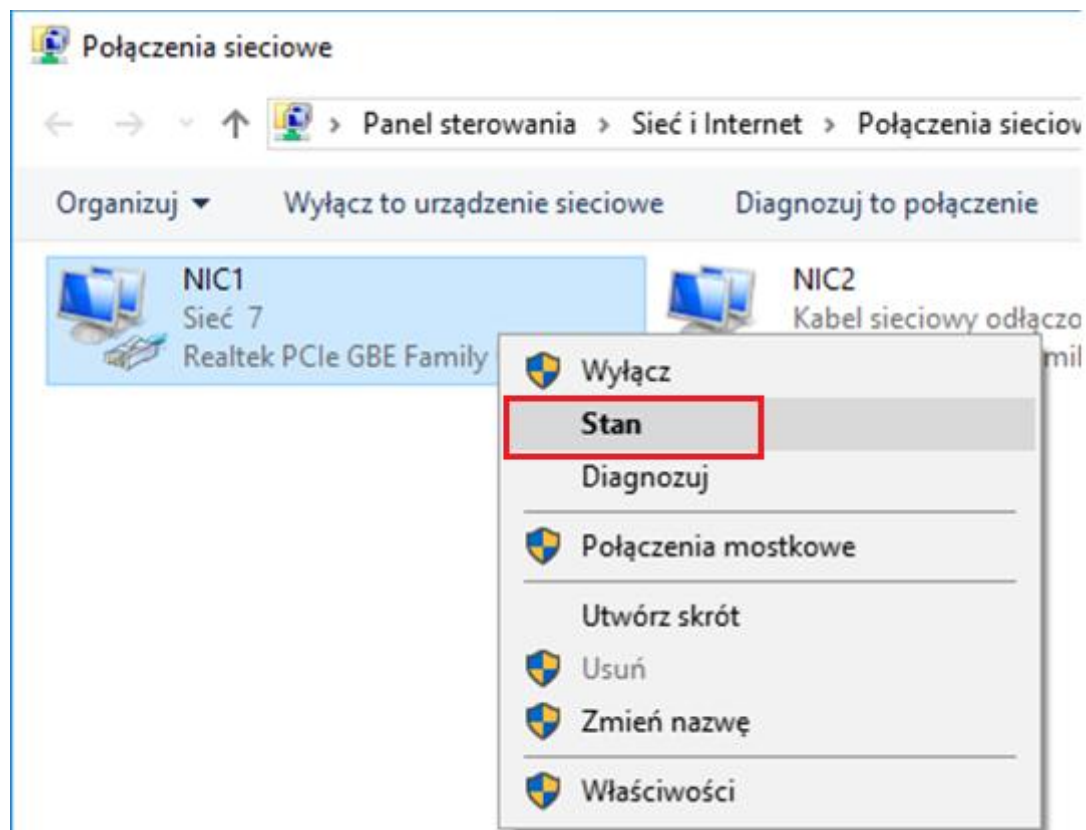
Teraz nie możesz się dostać na router, ponieważ adres karty sieciowej jest nadal 192.168.0.100/24



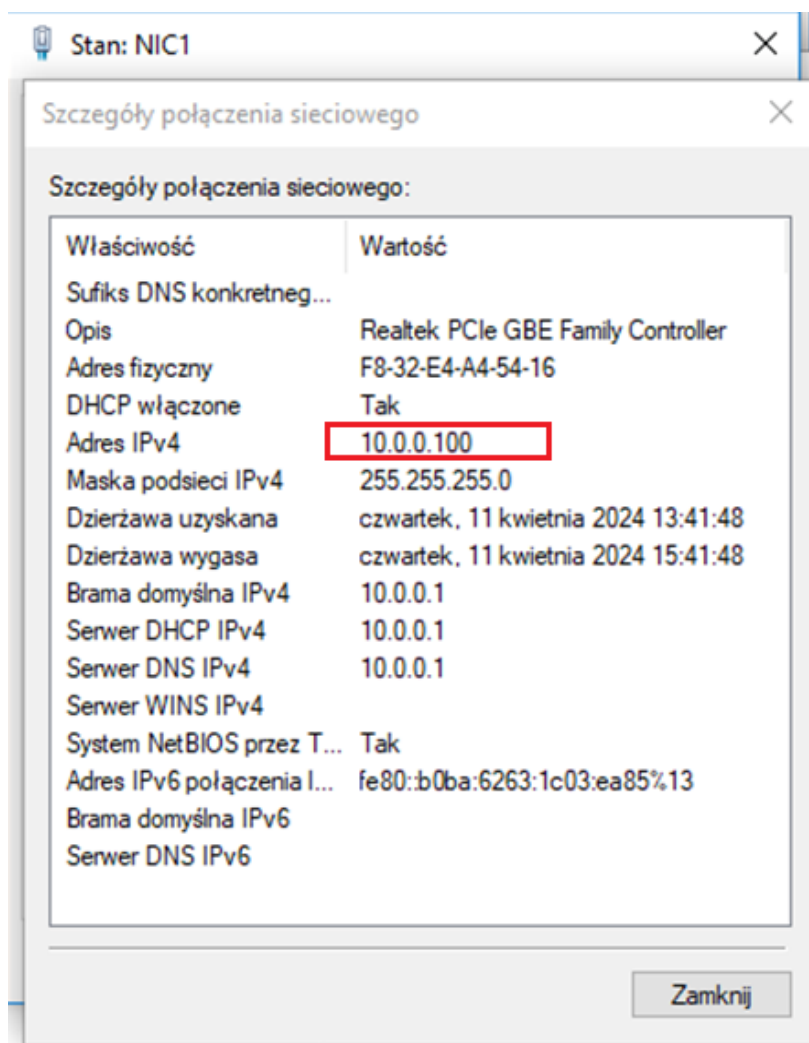
Wyłącz NIC1 i włącz z powrotem, a karta sieciowa NIC1 pozyska adres z puli DHCP sieci LAN 10.0.0.0/24



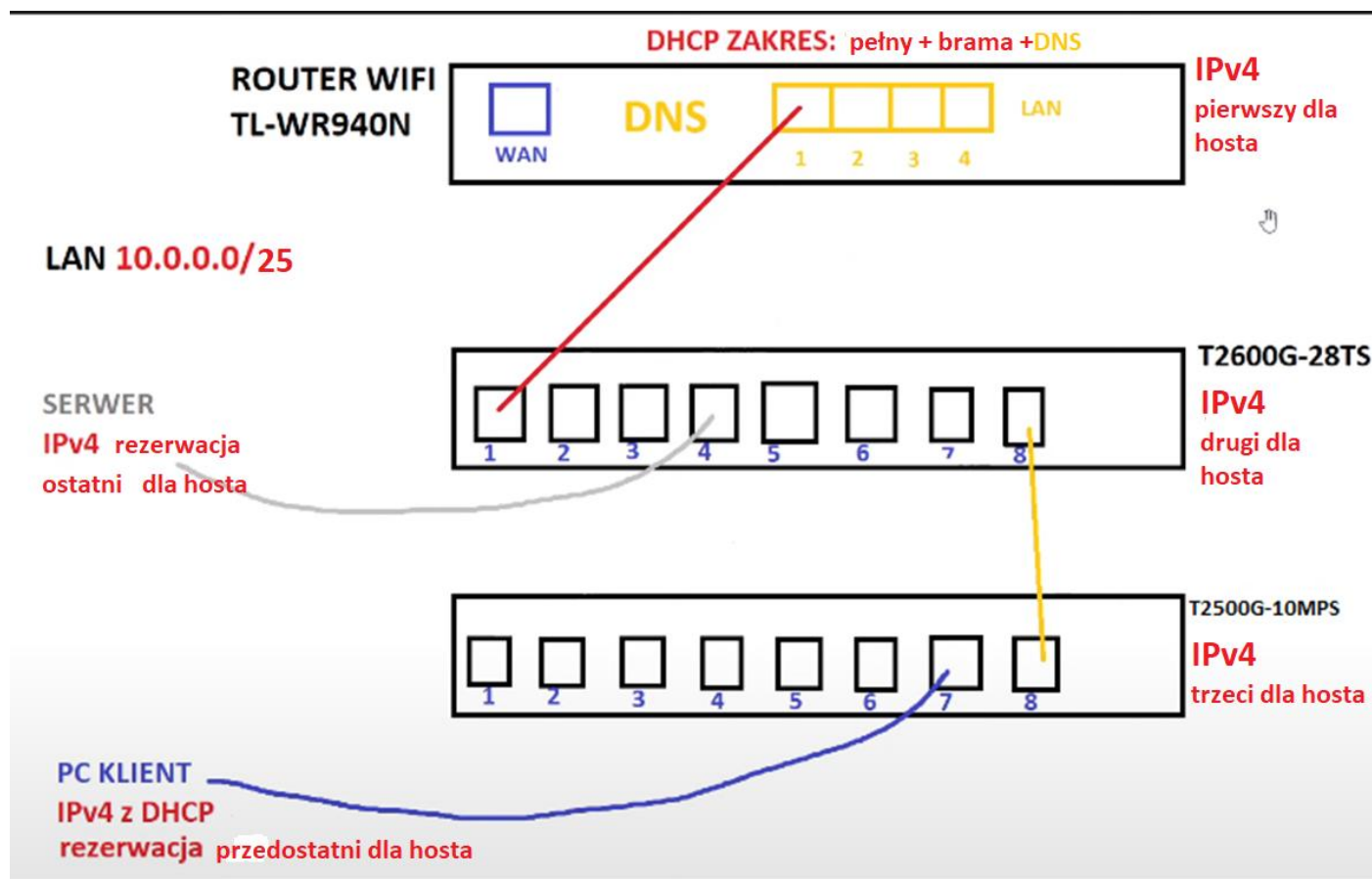
Sprawdź stan karty sieciowej NIC1



Teraz NIC1 ma adres 10.0.0.100/24



2.7 Rezerwacja DHCP na routerze TP-LINK



Maska sieci zwykła	Maska sieci skrócona	Klasa maski	Ilość szt. IP dla sieci z daną maską.
255.0.0.0	/8	A	16777216 szt.
255.128.0.0	/9	A	8388608 szt.
255.192.0.0	/10	A	4194304 szt.
255.224.0.0	/11	A	2097152 szt.
255.240.0.0	/12	A	1048576 szt.
255.248.0.0	/13	A	524288 szt.
255.252.0.0	/14	A	262144 szt.
255.254.0.0	/15	A	131072 szt.
255.255.0.0	/16	B	65536 szt.

255.255.128.0	/17	B	32768 szt.
255.255.192.0	/18	B	16384 szt.
255.255.224.0	/19	B	8192 szt.
255.255.240.0	/20	B	4096 szt.
255.255.248.0	/21	B	2048 szt.
255.255.252.0	/22	B	1024 szt.
255.255.254.0	/23	B	512 szt.
255.255.255.0 lub wersja skrócona: [0]	/24	C	256 szt. IP
255.255.255.128 lub [128]	/25	C	128 szt. IP
255.255.255.192 lub [192]	/26	C	64 szt. IP
255.255.255.224 lub [224]	/27	C	32 szt. IP
255.255.255.240 lub [240]	/28	C	16 szt. IP
255.255.255.248 lub [248]	/29	C	8 szt. IP
255.255.255.252 lub [252]	/30	C	4 szt. IP (najmniejsza możliwa podsieć zawierająca 2 szt. hostów)
255.255.255.254 lub [254]	/31	C	2 szt. IP Nie można utworzyć podsieci.
255.255.255.255 lub [255]	/32	C	1 szt. IP ADRES HOSTA.

część sieci (prefix) część hosta

/25 -> 11111111.11111111.11111111.1 | 0000000

255 . 255 .255 .128

Mamy 7 zer.

2 do potęgi liczby zer -> 2 do 7 -> 128 adresów IPv4

adres sieci 10.0.0.0/25

adres rozgłoszeniowy 10.0.0.0 + 128 = ?

Przesunięcie 128 -1 = 127 (ostatni adres w puli adresów).

adres rozgłoszeniowy 10.0.0.127/25

PODSUMOWANIE

adres sieci 10.0.0.0/25

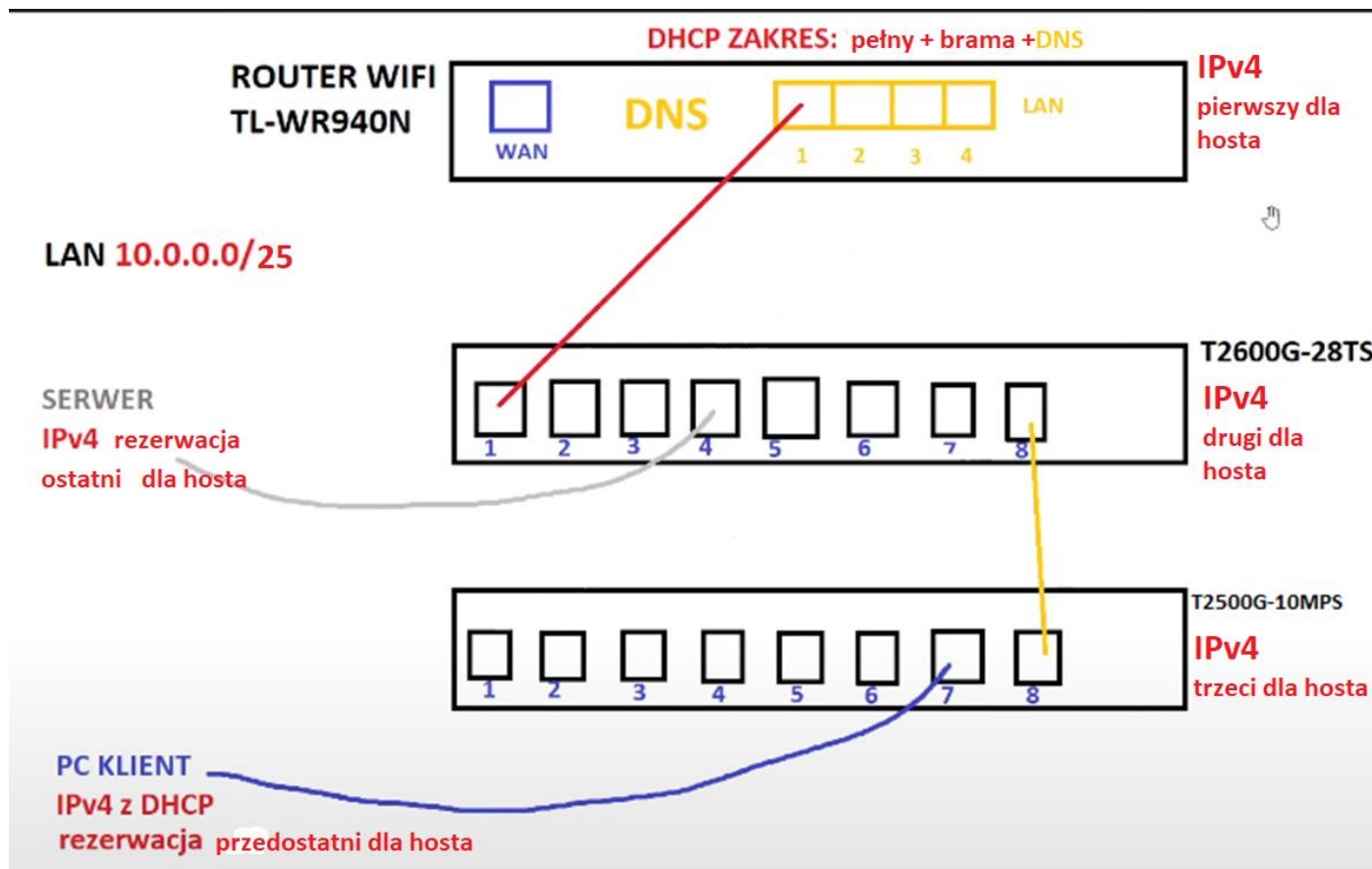
adresy dla hostów 10.0.0.1 ... 10.0.0.126

adres rozgłoszeniowy 10.0.0.127/25

WZÓR TABELI ADRESÓW DO ZADANIA

router	10.0.0.1/25	
switch 28ts/28tq	10.0.0.2/25	AC-84-C6-46-24-B9
switch 10mps	10.0.0.3/25	a2-bb-cc-dd-ee-ff
KLIENT	10.0.0.125/25	a3-bb-cc-dd-ee-ff
SERWER	10.0.0.126/25	a4-bb-cc-dd-ee-ff

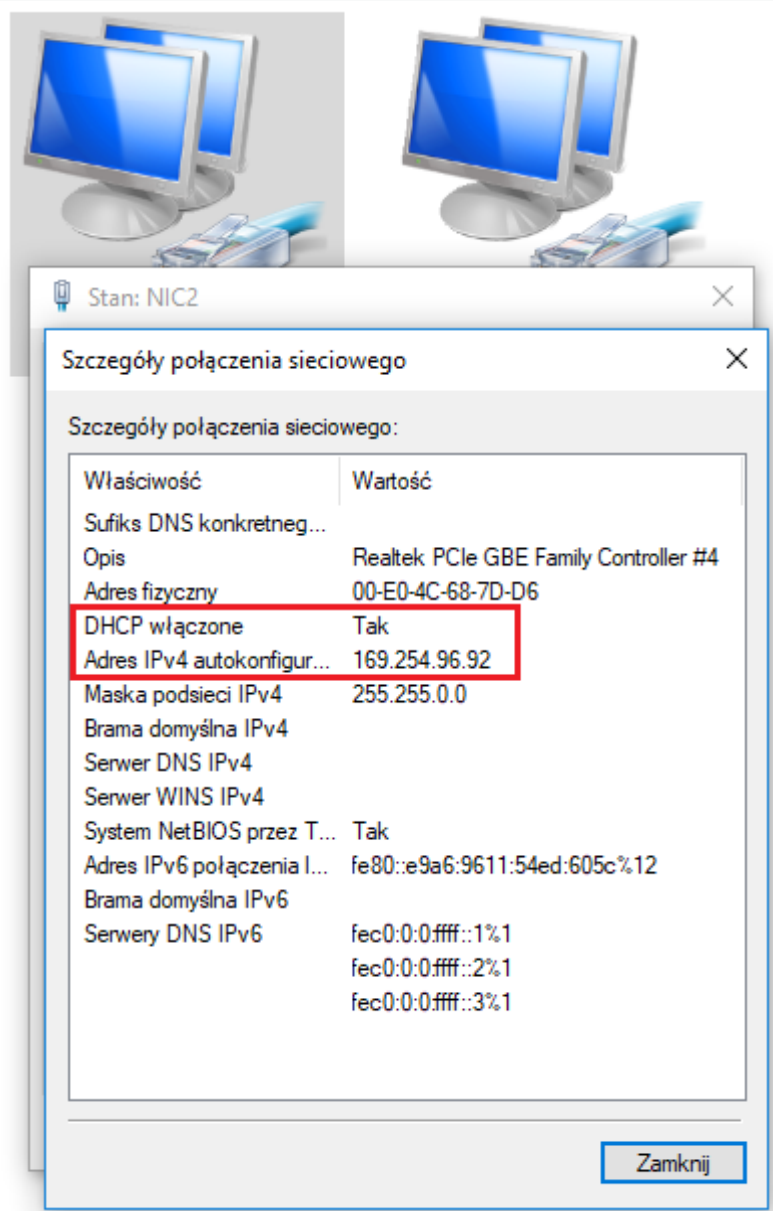
1. Połącz urządzenia sieciowe według schematu



2. Sprawdź, czy SERWER otrzymał adres z puli **192.168.0.0/24**.

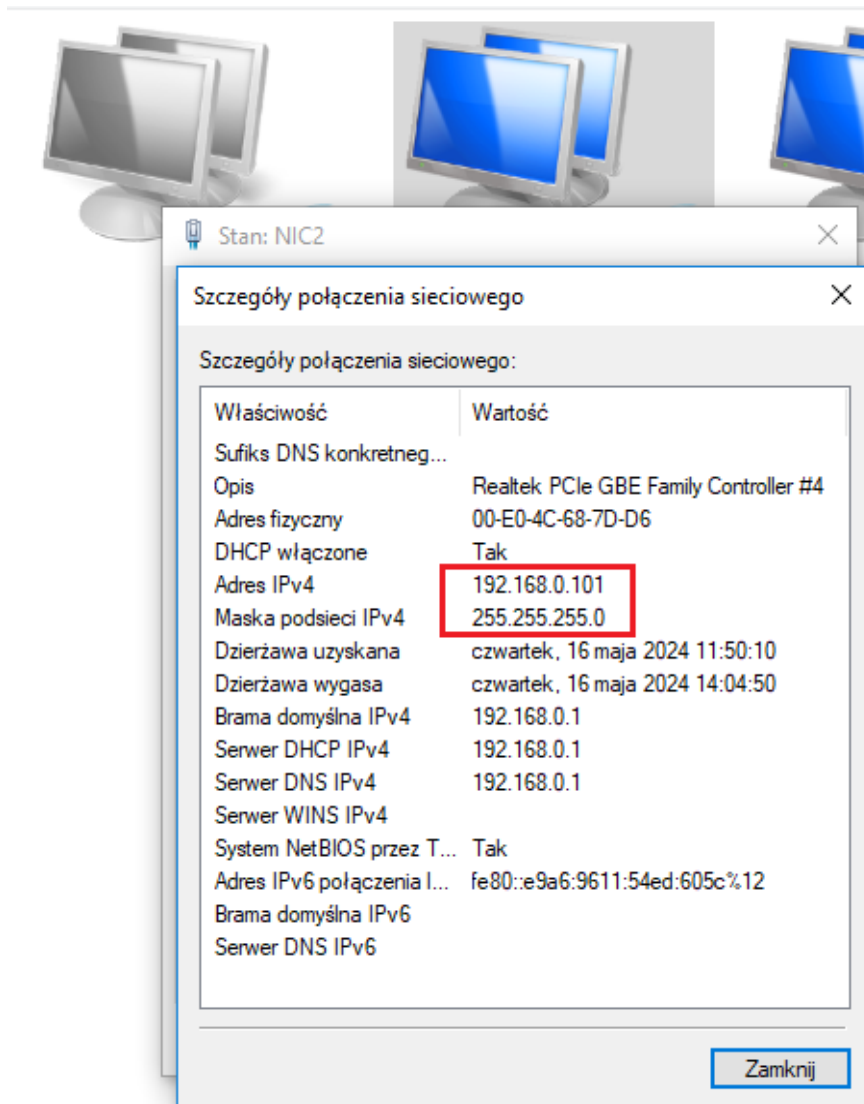
Brak połączenia z serwerem DHCP

Kiedy interfejs sieciowy hosta ustawiony na pozyskiwanie adresu automatycznie z serwera DHCP, jest podłączony do sieci, ale nie może się skontaktować z serwerem DHCP otrzymuje adres z puli 169.254.x.x.



Proces diagnozowania braku połączenia z serwerem DHCP:

1. Sprawdź, czy kable sieciowe są należycie podłączone (może któryś jest niedociśnięty). Na przełącznikach sprawdź, czy się świecą diody sys i diody używanych portów.
2. Sprawdź, czy urządzenie L3 (Layer 3) z usługą DHCP jest włączone.
3. Sprawdź, czy usługa DHCP jest włączona i poprawnie skonfigurowana na urządzeniu L3.
4. Podłącz hosta bezpośrednio do urządzenia L3 i obserwuj reakcję interfejsu sieciowego. Sprawdź jego adres IPv4.
5. Zresetuj urządzenia sieciowe
6. Zrestartuj hosta
7. W ostateczności wymień urządzenie sieciowe L3, lub interfejs sieciowy hosta.



3. Wpisz w pasku przeglądarki adres IPv4 **192.168.0.1**, aby połączyć się z przełącznikiem 28TS.

Fabryczne dane do logowania:

login: admin

pass: admin

UWAGA! Jeżeli wyświetlił Ci się panel routera, to na chwilę odepnij kabel łączący router z przełącznikiem 28TS. Sprawdź czy Adres IPv4 jest podtrzymany na karcie sieciowej SERWERA (Patrz obrazek z punktu drugiego). Może bowiem być tak, że SERWER utraci otrzymany Adres IPv4 na skutek utraty połączenia z routerem. Jeśli Adres IPv4 zostanie faktycznie utracony, podłącz router z przełącznikiem 28TS ponownie i zacznij procedurę jeszcze raz od punktu drugiego zadania. Jak sobie z tym nie poradzisz poproś Administratora o pomoc 😊.

Jeżeli Adres IPv4 na karcie SERWERA jest podtrzymany, to w nowym oknie przeglądarki wpisz ponownie adres IPv4 **192.168.0.1**.

4. Ustaw static IPv4 na przełączniku 28TS

T2600G-28TS

Interface Config

Modify Interface

Interface ID: Vlan1

IP Address Mode: ☐ None ☒ Static ☐ DHCP ☐ BOOTP

IP Address: 10.0.0.2 (Format: 192.168.0.1)

Subnet Mask: 255.255.255.128 (Format: 255.255.255.0)

Admin Status: Enable

Interface Name: (Optional. 1-16 characters)

Apply Back

5. Ustaw static IPv4 na przełączniku 10MTS

UWAGA! Jeżeli wyświetlił Ci się panel routera, to na chwilę odepnij kabel łączący router z przełącznikiem 28TS. Sprawdź czy Adres IPv4 jest podtrzymany na karcie sieciowej SERWERA (Patrz obrazek z punktu drugiego). Może bowiem być tak, że SERWER utraci otrzymany Adres IPv4 na skutek utraty połączenia z routerem. Jeśli Adres IPv4 zostanie faktycznie utracony, podłącz router z przełącznikiem 28TS ponownie i zacznij procedurę jeszcze raz od punktu drugiego zadania. Jak sobie z tym nie poradzisz poproś Administratora o pomoc 😊.

Jeżeli Adres IPv4 na karcie SERWERA jest podtrzymany, to w nowym oknie przeglądarki wpisz ponownie adres IPv4 **192.168.0.1**.

T2500G-10MPS

System Summary Device Description System Time Daylight Saving Time Serial Port Setting **System IP**

IP Config

MAC Address: AC-84-C6-4A-9C-2C

IP Address Mode: ☒ Static IP ☐ DHCP ☐ BOOTP

Management VLAN: 1 (VLAN ID: 1-4094)

IP Address: 10.0.0.3

Subnet Mask: 255.255.255.128

Default Gateway: 10.0.0.1

Apply Help

6. W nowej zakładce wpisz ponownie adres IPv4 **192.168.0.1**, żeby zalogować się na router

 admin

 ●●●●●

Login

7. Ustaw docelowy adres IPv4 routera **10.0.0.1/25**

Status	
Quick Setup	
WPS	
Working Mode	
Network	LAN
- WAN	
- MAC Clone	
- LAN	
- IPTV	
Wireless	

MAC Address: 98-DA-C4-64-61-86

IP Address:

Subnet Mask:

Other Mask ▾

Save

8. Wyłącz i włącz kartę sieciową SERWERA. Sprawdź, czy karta otrzymała adres IPv4 z nowej puli adresowej **10.0.0.0/25**.

Szczegóły połączenia sieciowego

Szczegóły połączenia sieciowego:

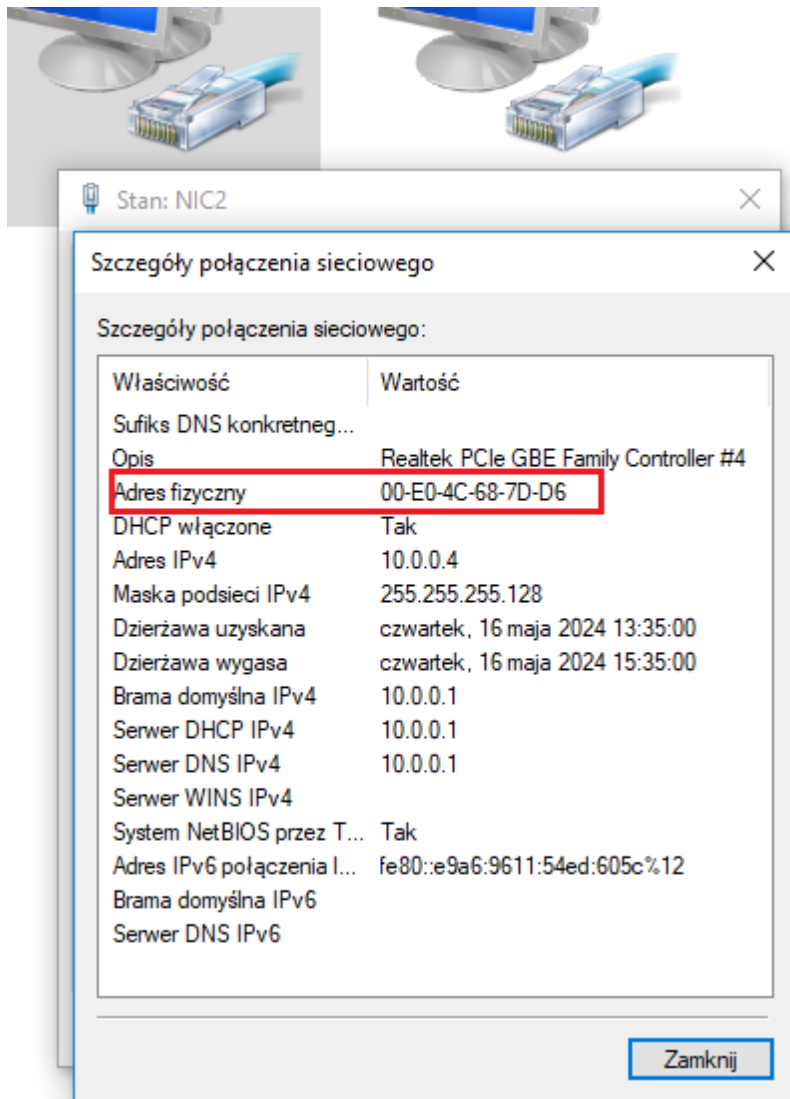
Właściwość	Wartość
Sufiks DNS konkretneg...	
Opis	Realtek PCIe GBE Family Controller #4
Adres fizyczny	00-E0-4C-68-7D-D6
DHCP włączone	Tak
Adres IPv4	10.0.0.4
Maska podsieci IPv4	255.255.255.128
Dzierżawa uzyskana	czwartek, 16 maja 2024 13:35:00
Dzierżawa wygasa	czwartek, 16 maja 2024 15:35:00
Brama domyślna IPv4	10.0.0.1
Serwer DHCP IPv4	10.0.0.1
Serwer DNS IPv4	10.0.0.1
Serwer WINS IPv4	
System NetBIOS przez T...	Tak
Adres IPv6 połączenia l...	fe80::e9a6:9611:54ed:605c%12
Brama domyślna IPv6	
Serwer DNS IPv6	

9. W notatniku wykonaj tabelkę według poniższego wzoru:

WZÓR TABELI ADRESÓW DO ZADANIA

switch 28ts/28tq	10.0.0.2/25	AC-84-C6-46-24-B9
switch 10mps	10.0.0.3/25	AC-84-C6-4A-9C-2C
KLIENT	10.0.0.125/25	AC-9E-17-88-AB-7D
SERWER	10.0.0.126/25	00-E0-4C-68-7D-76

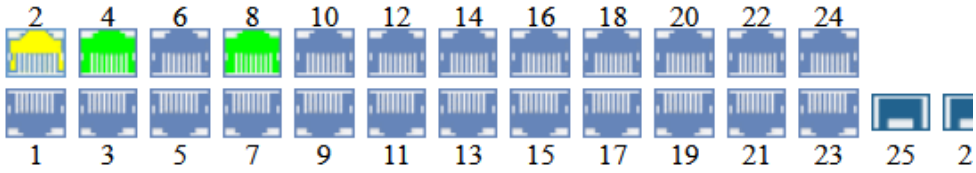
Pozyskaj adresy mac SERWERA i PCKlietna wyświetlając stany kart sieciowych hostów.



Pozyskaj adresy mac przełączników

Port Status

UNIT: 1



System Info

UNIT: 1

System Description:	JetStream 24-Port Gigabit L2 Managed S
Device Name:	T2600G-28TS
Device Location:	SHENZHEN
Contact Information:	www.tp-link.com
Hardware Version:	T2600G-28TS 2.0
Firmware Version:	2.0.0 Build 20170928 Rel.34921(s)
Bootloader Version	TP-LINK BOOTUTIL(v1.0.0)
Mac Address:	AC-84-C6-46-24-B9
Serial Number:	2183262000170
System Time:	2006-01-01 09:57:18
Running Time:	0 day - 1 hour - 58 min - 3 sec

RefreshHelp

Pozyskiwanie adresu mac przełącznika za pomocą połączenia konsolowego

File Set Up Help

Command History

```
tplink  
enable  
show system-info
```

Command:

☒ Delete command after send

Send

☐ CR☐ LF☒ CR + LF

Text Received

```
T2600G-28TS#
```

```
T2600G-28TS#show system-info
```

```
System Description - JetStream 24-Port  
Gigabit L2 Managed Switch with 4 SFP  
Slots
```

```
System Name - T2600G-28TS
```

```
System Location - SHENZHEN
```

```
Contact Information - www.tp-link.com
```

```
Hardware Version - T2600G-28TS 2.0
```

```
Software Version - 2.0.0 Build
```

```
20170928 Rel.34921(s)
```

```
Bootloader Version - TP-LINK
```

```
BOOTUTIL(v1.0.0)
```

```
Mac Address - AC-84-C6-46-24-B9
```

```
Serial Number - 2183262000170
```

```
System Time - 2006-01-01 10:35:41
```

```
Running Time - 0 day - 2 hour - 36
```

```
min - 15 sec
```

```
:: ✓ Connected :: Port: [COM1] :: BaudRate: [38400] :: Data Bits: [8] :: Parity: [None] :: Stop Bits: [One] :: Flow Control: [None] ::
```

Dokonaj rezerwacji adresów IPv4 dla SERWERA , PCKlienta oraz urządzeń sieciowych.

Status

Quick Setup

WPS

Working Mode

Network

Wireless

Guest Network

DHCP

- DHCP Settings
- DHCP Client List
- Address Reservation

Address Reservation

ID	MAC Address	Rese
----	-------------	------

Add New...

Enable All

Previous

Przykładowa rezerwacja adresu IPv4 dla PCKlienta

Add or Modify an Address Reservation Entry

MAC Address: AC-9E-17-88-AB-7D

Reserved IP Address: 10.0.0.125

Status: Enabled ▾

Save

Back

Po zakończeniu rezerwacji adresów IPv4 na routerze, jego panel konfiguracyjny powinien przedstawiać się następująco.

Address Reservation

ID	MAC Address	Reserved IP Address	Status	Modify
1	AC-9E-17-88-AB-7D	10.0.0.125	Enabled	Modify Delete
2	00-E0-4C-68-7D-76	10.0.0.126	Enabled	Modify Delete
3	AC-84-C6-46-24-B9	10.0.0.2	Enabled	Modify Delete
4	AC-84-C6-4A-9C-2C	10.0.0.3	Enabled	Modify Delete

Add New...

Enable All

Disable All

Delete All

Na przełączniku 28TS w zakładce **ROUTING** edytuj **Interface**

IP Address	Subnet Mask	Interface Name	Status	
10.0.0.2	255.255.255.128		Up	Edit

i zaznacz opcję DHCP

T2600G-28TS

Interface Config

System

Switching

VLAN

Spanning Tree

Ethernet OAM

Multicast

Routing

• Interface

Modify Interface

Interface ID: Vlan1

IP Address Mode: ☐ None ☒ Static ☒ DHCP ☐ BOOTP

IP Address: 10.0.0.2 (Format: 192.168.0.1)

Subnet Mask: 255.255.255.128 (Format: 255.255.255.0)

Admin Status: Enable

Interface Name: (Optional. 1-16 characters)

Modify Interface

Interface ID: Vlan1

IP Address Mode: ☐ None ☐ Static ☒ DHCP ☐ BOOTP

IP Address: (Format: 192.168.0.1)

Subnet Mask: (Format: 255.255.255.0)

Admin Status:

Interface Name: (Optional. 1-16 characters)

Apply

Back

Klawiszem F5 odśwież stronę. Sprawdź wpisy w zakładce **ROUTING/ Interface**

Interface List

Select	ID	Mode	IP Address	Subnet Mask	Int
☐	Vlan1	DHCP	10.0.0.2	255.255.255.128	

All

Delete

Help

Na przełączniku 10MPS w zakładce **SystemIP/IP Address Mode** wybierz opcję DHCP.

T2500G-10MPS

System Summary

Device Description

System Time

Daylight Saving Time

Serial Port Setting

System IP

System

• System Info

• User Management

• System Tools

• Access Security

Switching

VLAN

Spanning Tree

Multicast

DHCP

QoS

IP Config

MAC Address: AC-84-C6-4A-9C-2C

IP Address Mode: ☐ Static IP ☒ DHCP ☐ BOOTP

Management VLAN: (VLAN ID: 1-4094)

IP Address:

Subnet Mask:

Default Gateway:

Apply

Help

Note:

Changing IP address to a different IP segment will interrupt the network communication, so please keep the new IP address in the same IP segment with the local network.

Klawiszem F5 odśwież stronę. Sprawdź, czy właściwe adresy IPv4 zostały przydzielone urządzeniu 10MPS.

AC-84-C6-4A-9C-2C

le: ☐ Static IP ☒ DHCP ☐ BOOTP

VLAN: (VLAN ID: 1-4094)

y:

System

- System Info
- User Management
- System Tools
- Access Security

Switching

VLAN

Spanning Tree

Multicast

DHCP

IP Config

MAC Address:

IP Address Mod

Management VI

IP Address:

Subnet Mask:

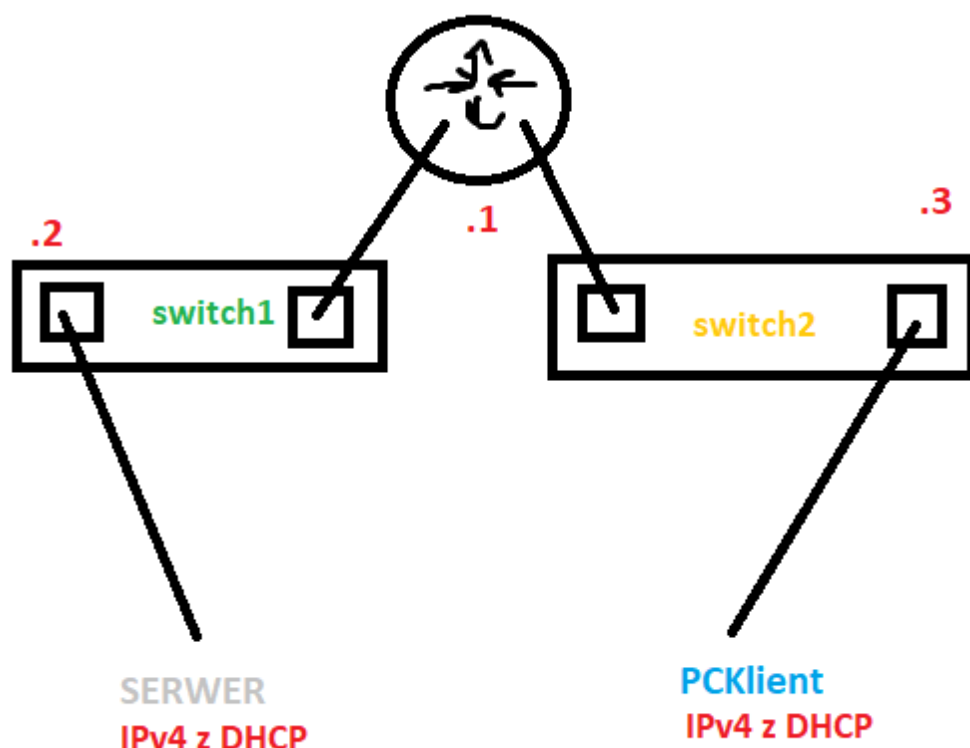
Default Gateway:

Note:

Changing IP address

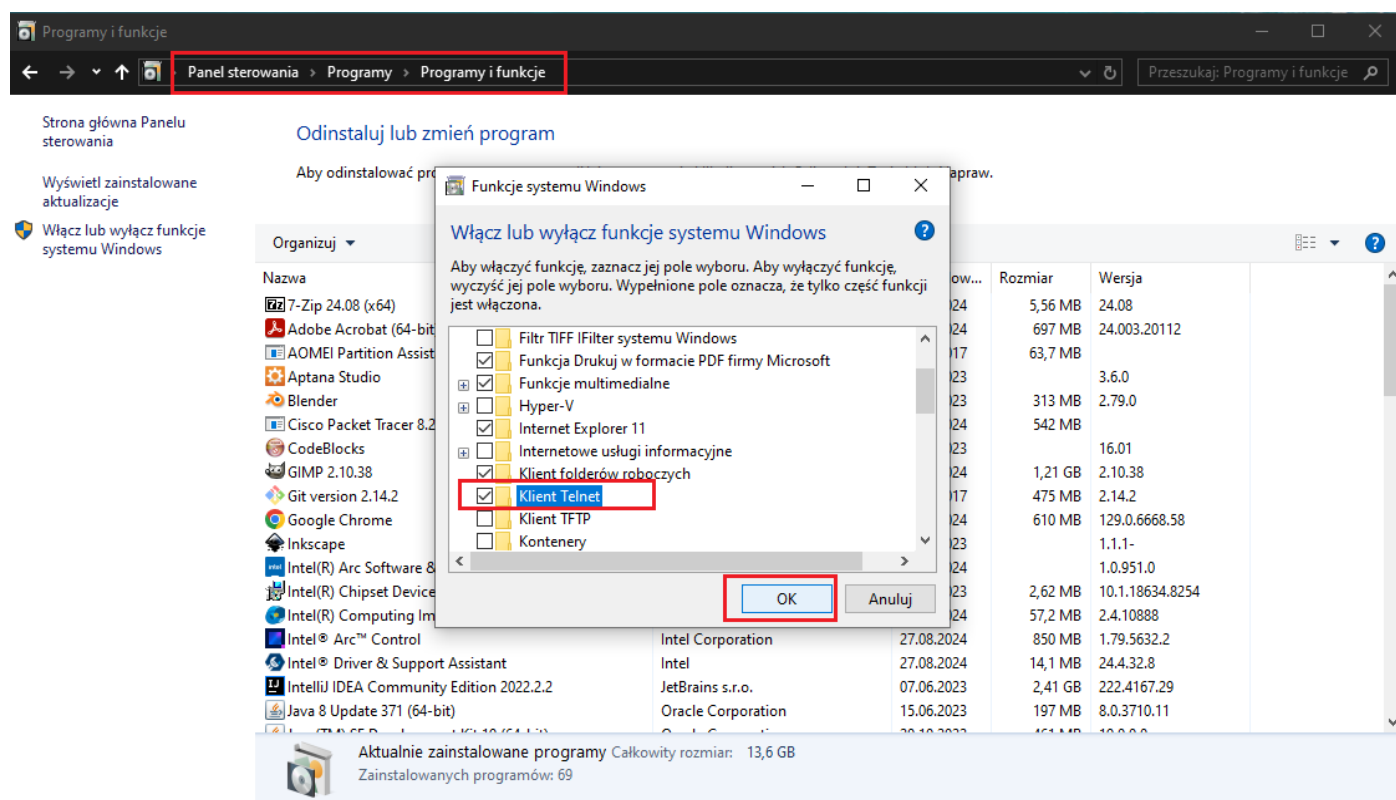
new IP address in the

2.8 Konfiguracja przełącznika - Access Security



Podłącz kable sieciowe do zresetowanych urządzeń według powyższego schematu

Zainstaluj telnet w systemie Windows



Ustaw adres IPv4 przełącznika i włącz usługę ssh w panelu graficznym, albo konsolowo

The image shows the web management interface of a TP-Link T2600G-28TS switch. The left sidebar contains a menu with 'Access Security' highlighted. The main content area is the 'SSH Config' tab, which is also highlighted with a red box. Under 'Global Config', the 'SSH' option is set to 'Enable' (indicated by a red box). The 'Protocol V1' and 'Protocol V2' are also set to 'Enable'. The 'Idle Timeout' is set to 120 seconds and 'Max Connect' is set to 5. The 'Encryption Algorithm' section shows several algorithms checked, including AES128-CBC, AES192-CBC, AES256-CBC, Blowfish-CBC, Cast128-CBC, and 3DES-CBC. The 'Data Integrity Algorithm' section shows HMAC-SHA1 and HMAC-MD5 checked. The 'Key Download' section shows 'SSH-2 RSA/DSA' selected as the key type. The 'Apply' button in the top right is also highlighted with a red box.

Enable SSH

```
Telnet 192.168.0.1

***** User Access Login *****

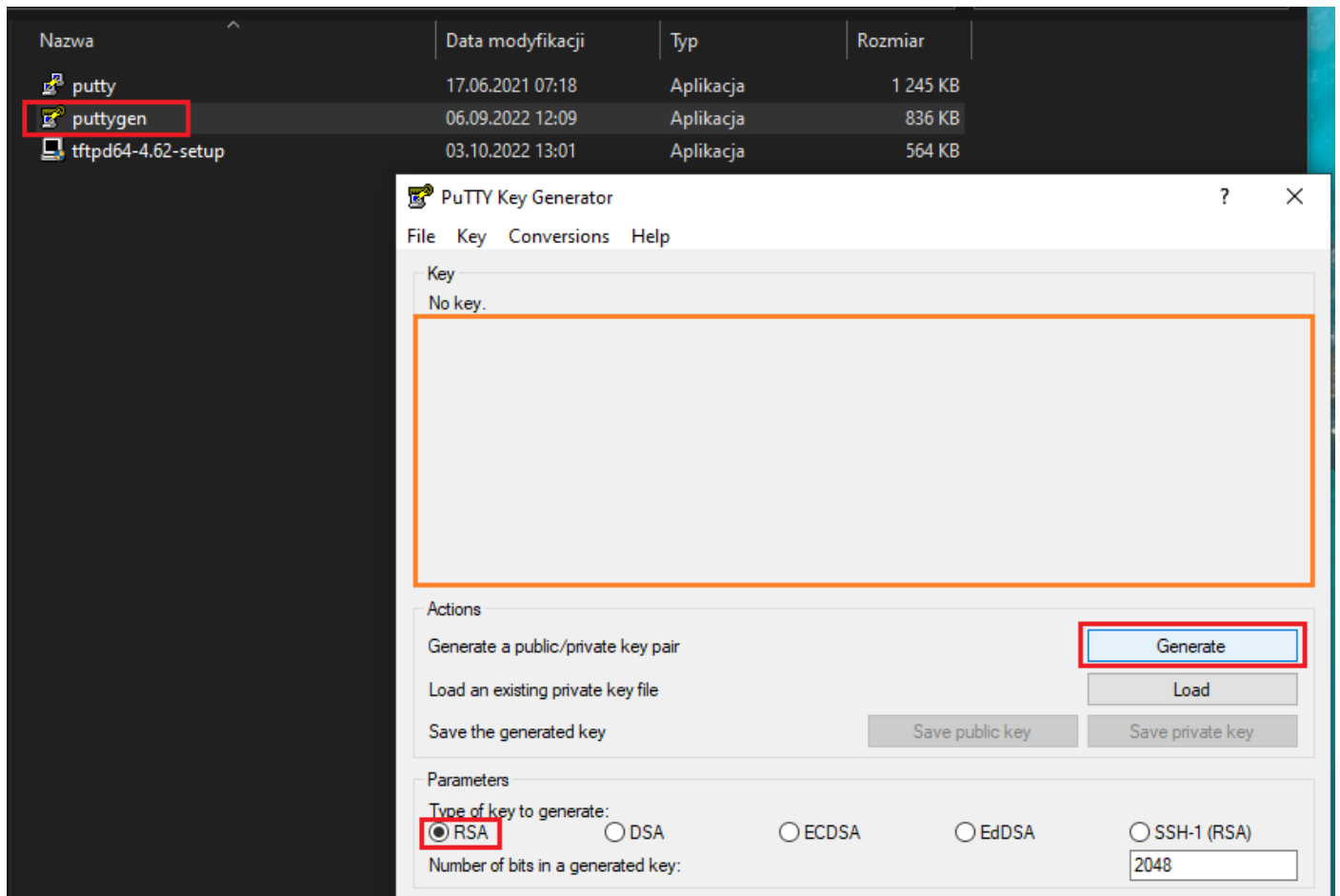
User:admin
Password:

Switch>#2006-01-01 08:10:29,[User1/3/Login the CLI by admin on vty0 <192.168.0.200>.

Switch>enable
Switch#config
Switch(config)#ip ssh server ← Enable SSH function
Switch(config)#_
```

Wygeneruj klucze ssh w programie puttygen. Ustaw dla nich hasło dostępu

Podczas generowania pary kluczy poruszaj kursorem myszy w obszarze zaznaczonym na pomarańczowo



 PuTTY Key Generator ? ×

File Key Conversions Help

Key

Please generate some randomness by moving the mouse over the blank area.

Actions

Generate a public/private key pair Generate

Load an existing private key file Load

Save the generated key Save public key Save private key

Parameters

Type of key to generate:

☒ RSA ☐ DSA ☐ ECDSA ☐ EdDSA ☐ SSH-1 (RSA)

Number of bits in a generated key:

 PuTTY Key Generator ? ×

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACQurswGo9pJBtVx0Pk4WltwsH3+7ldBTkVSF1cDNvyDk7wKtilHgK0BhSwkeM898kpCfNfPyccrA/u7YscZFnx6SaBHY3phsnYRie/OCcLU96J05ihXAz7ZZSpuc6usi3mgefx6LOFh682cA20trUaTQYIzns/NmcEKqb4BaCv520HkwBGvMxtfbbZhGQ3JQaHznXckRM1/1glvmScqomCuVOlkN4RoK5efmVwPKC2NhIPiza7dMuslcpj46D67Yh322wQI3+ENy5Rk3jGlymQMFNimbeL88Vwi97dqWyzSnGofanXSd4pqu5
```

Key fingerprint:

Key comment:

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair Generate

Load an existing private key file Load

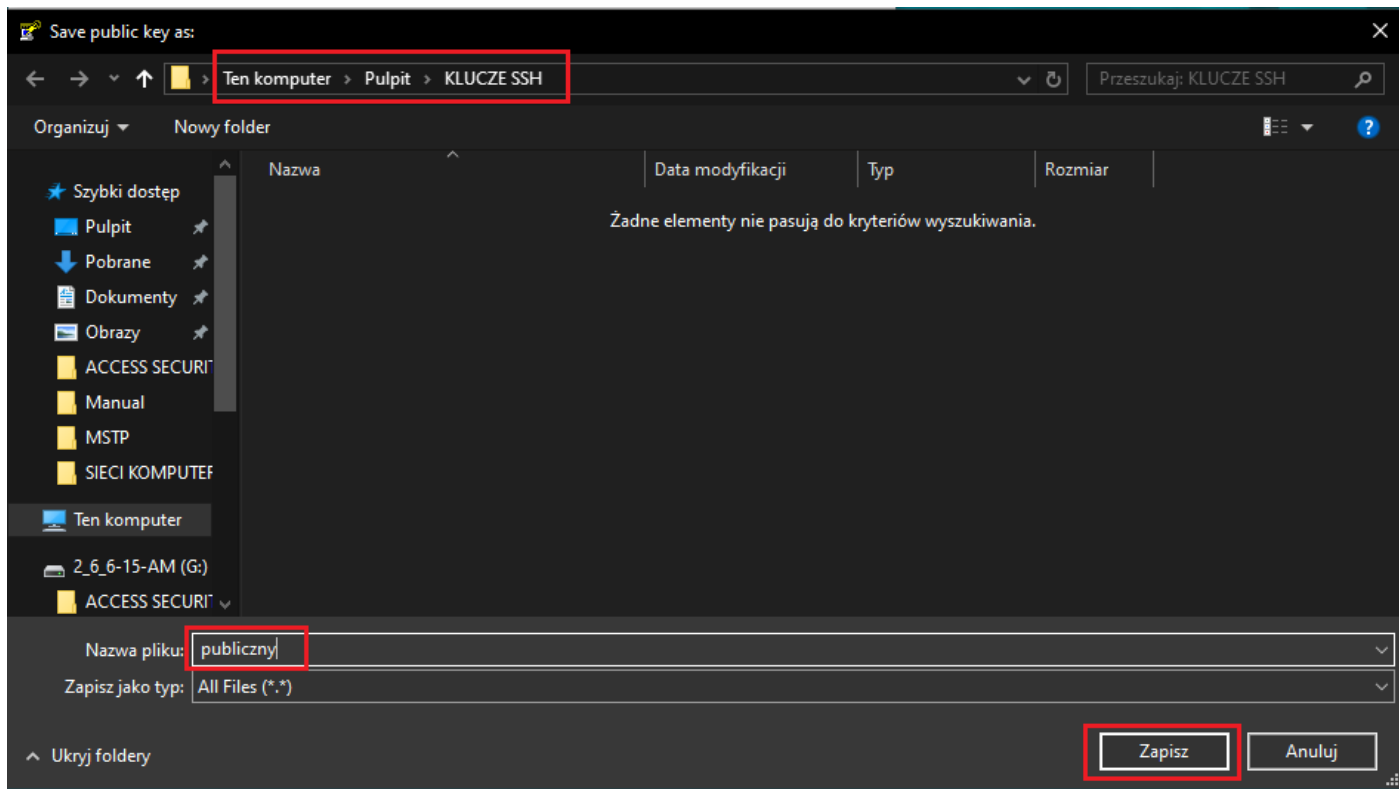
Save the generated key Save public key Save private key

Parameters

Type of key to generate:

☒ RSA ☐ DSA ☐ ECDSA ☐ EdDSA ☐ SSH-1 (RSA)

Number of bits in a generated key:



Key comment: switch1

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair Generate

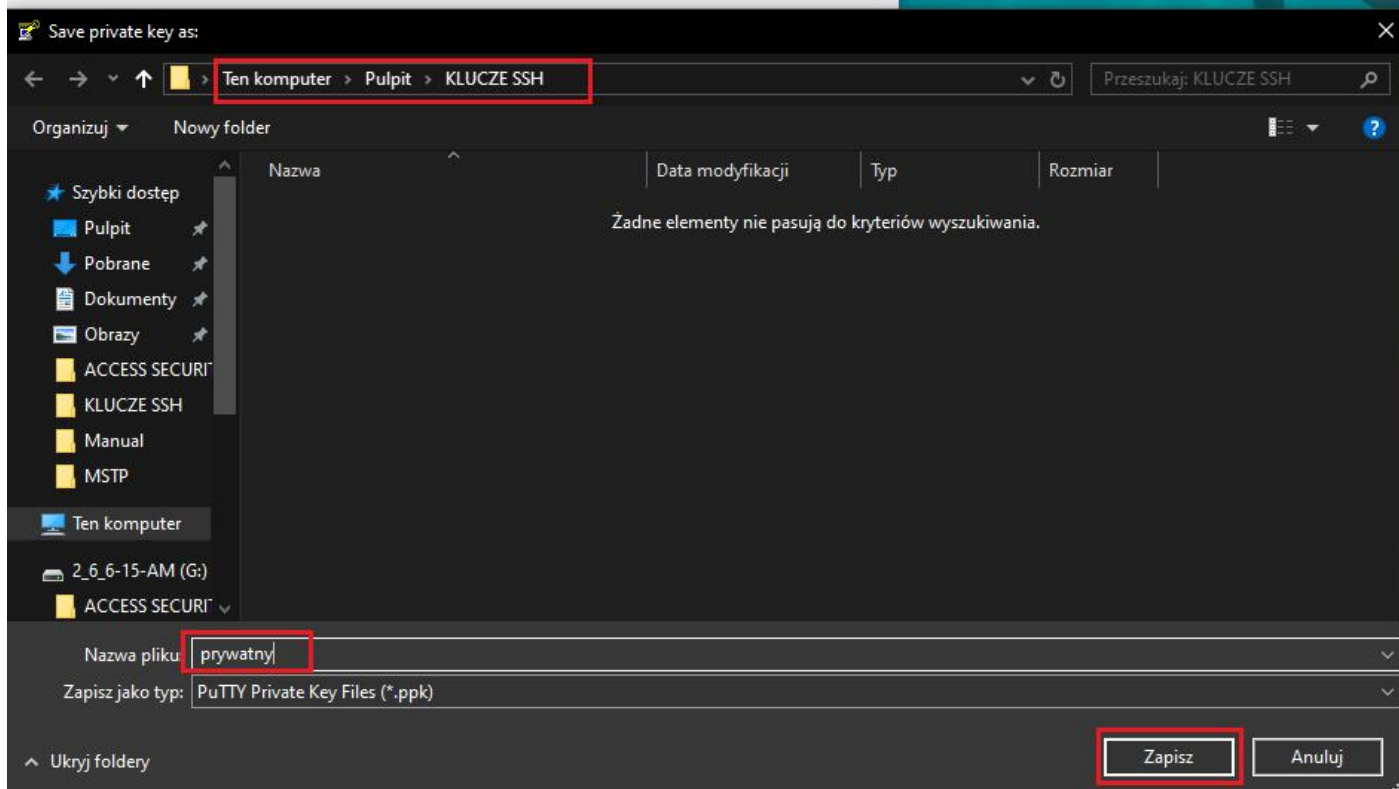
Load an existing private key file Load

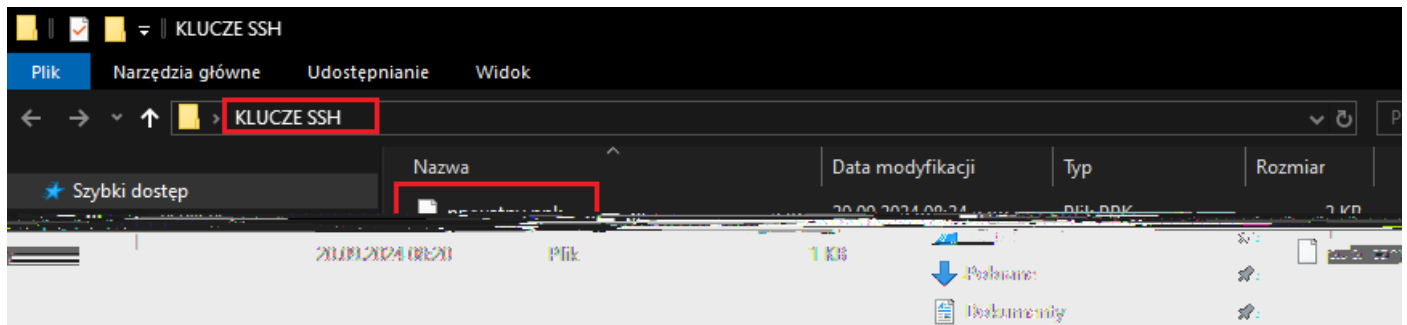
Save the generated key Save public key Save private key

Parameters

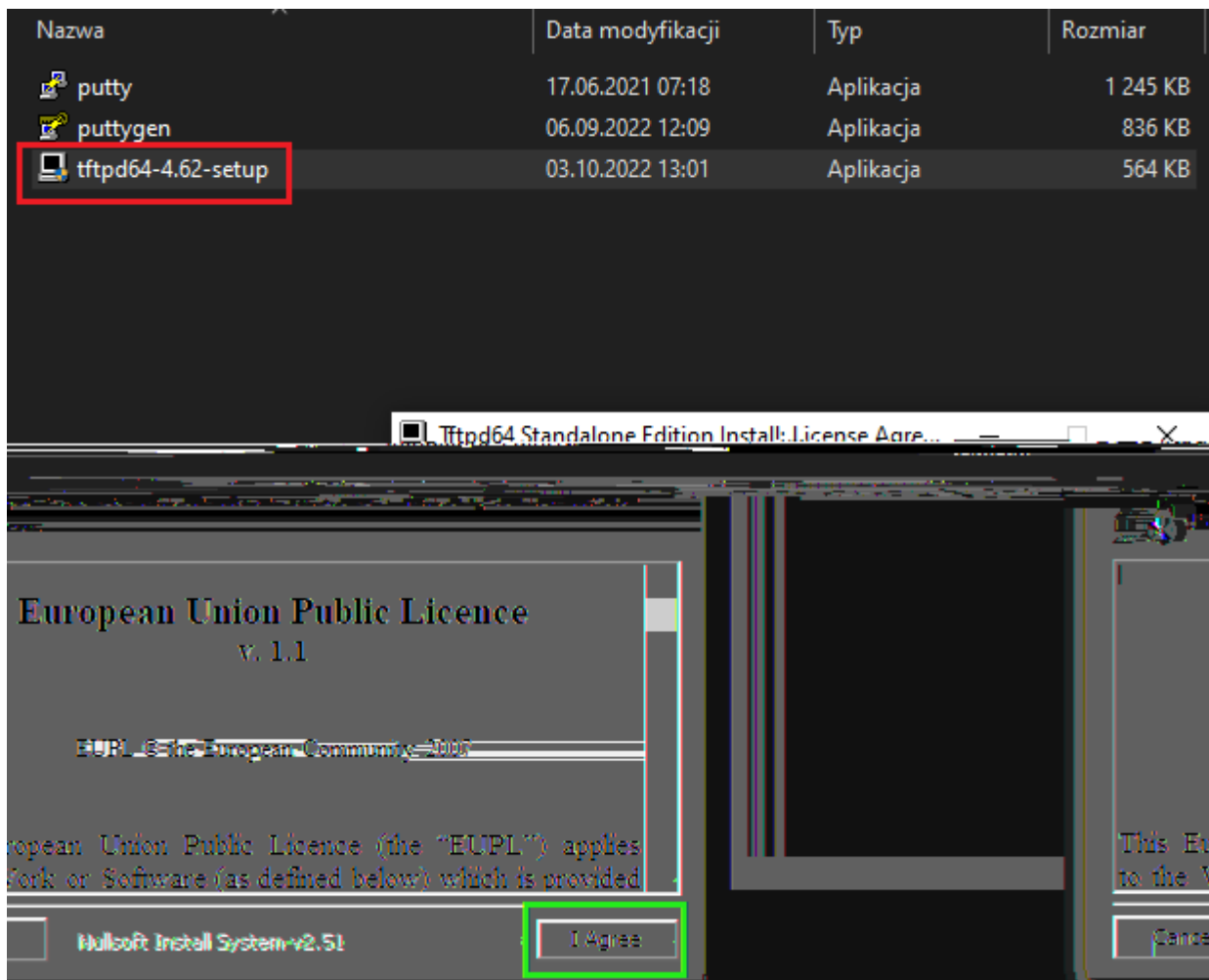
Type of key to generate: ☒ RSA ☐ DSA ☐ ECDSA ☐ EdDSA ☐ SSH-1 (RSA)

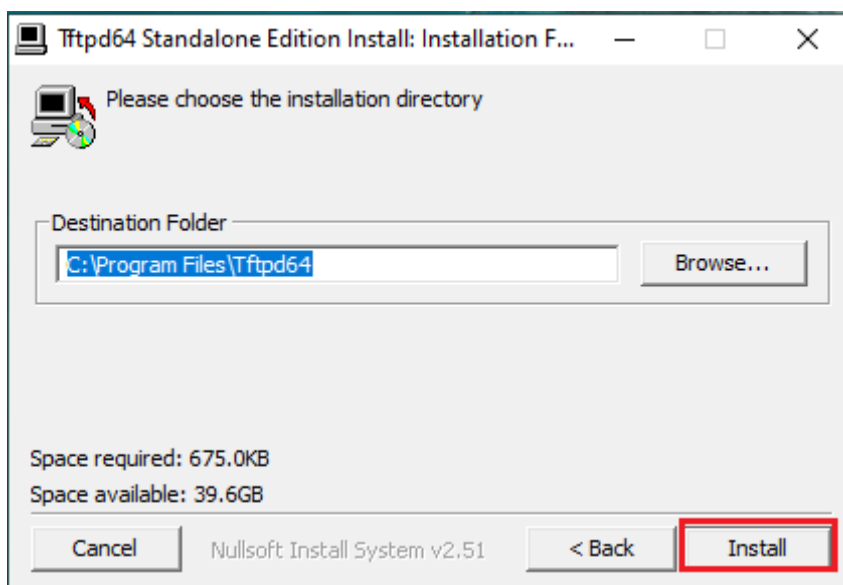
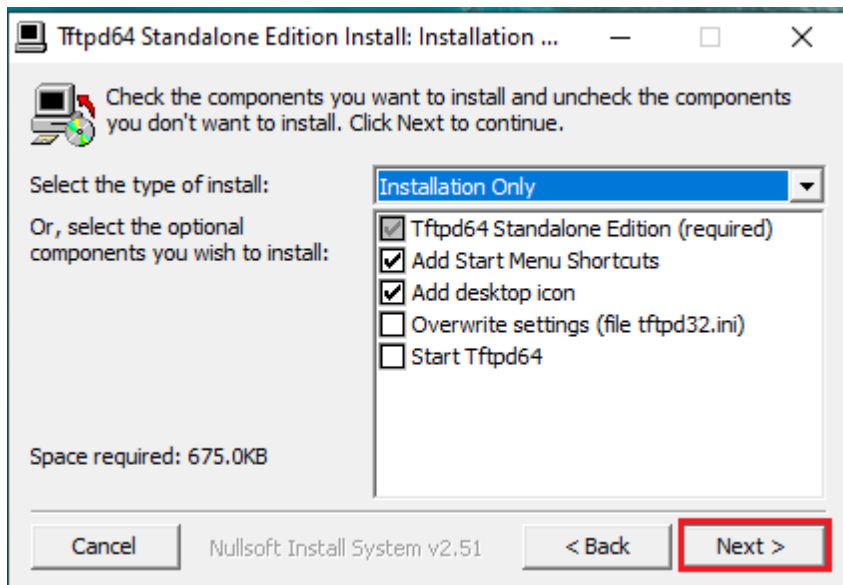
Number of bits in a generated key: 2048

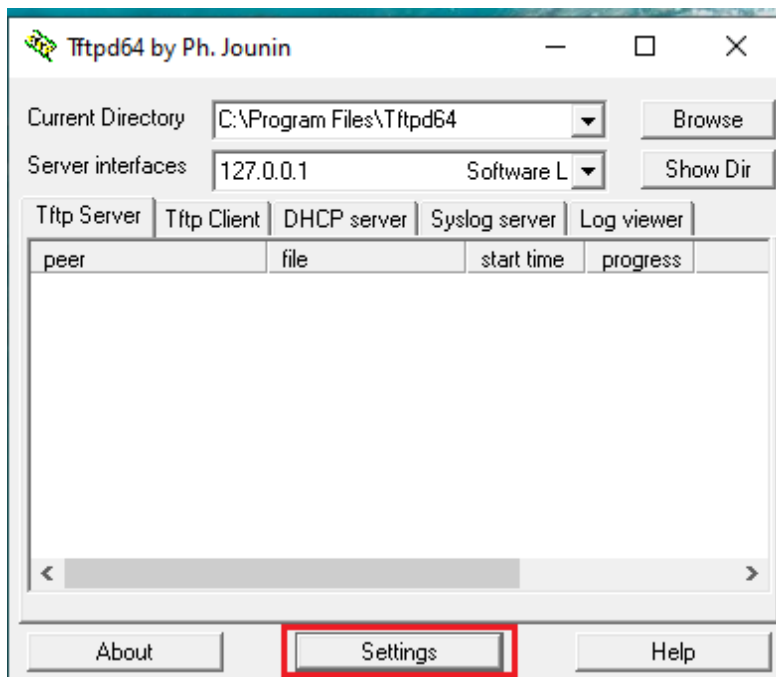
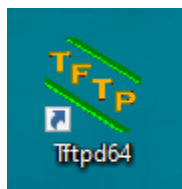
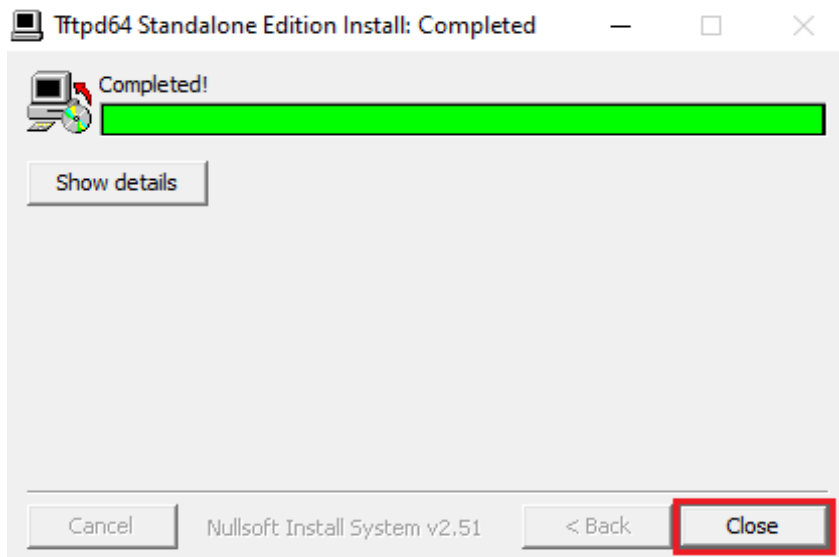


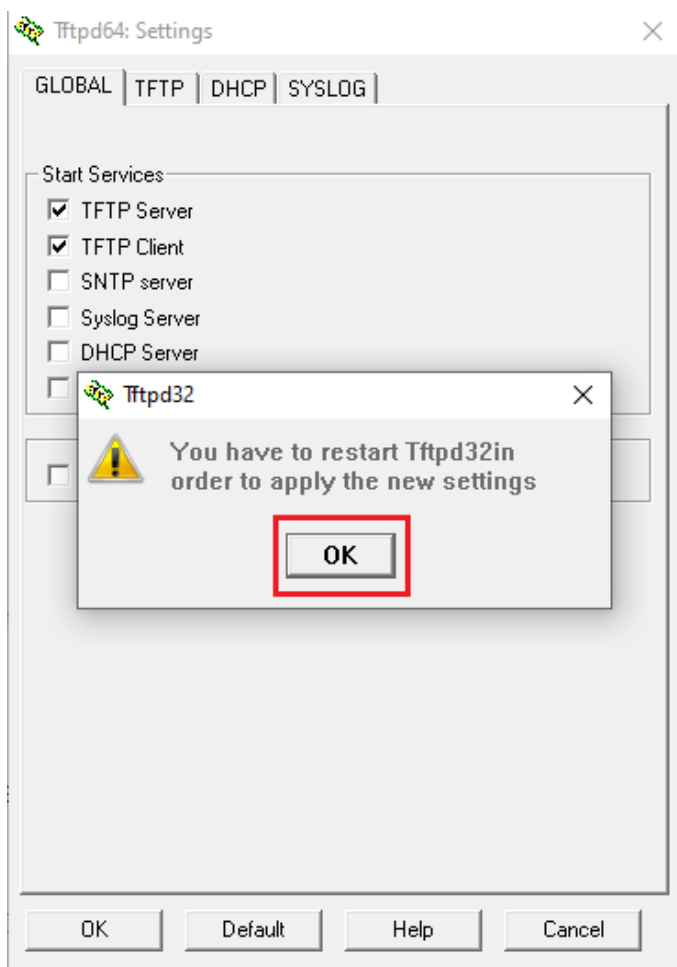
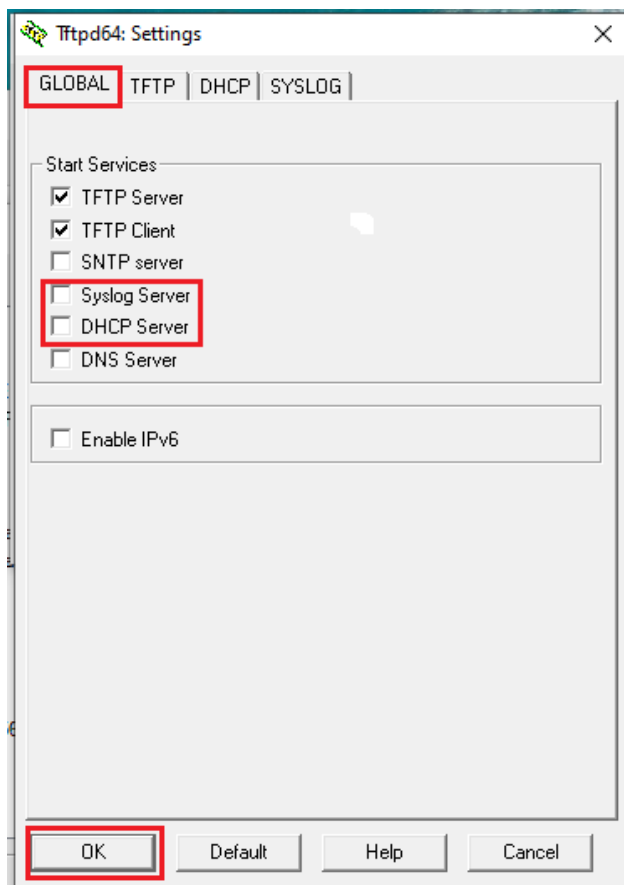


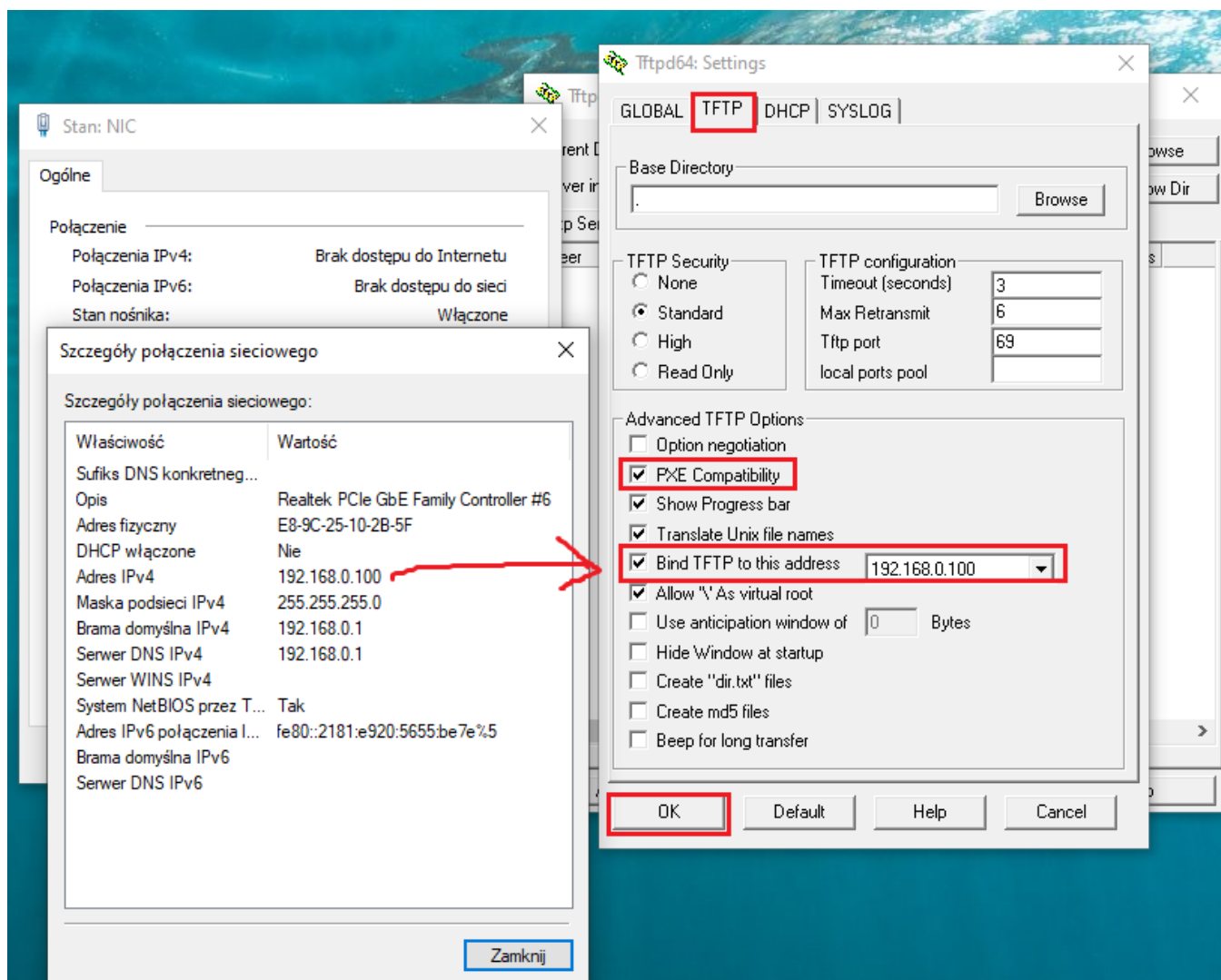
Zainstaluj serwer tftp i skonfiguruj

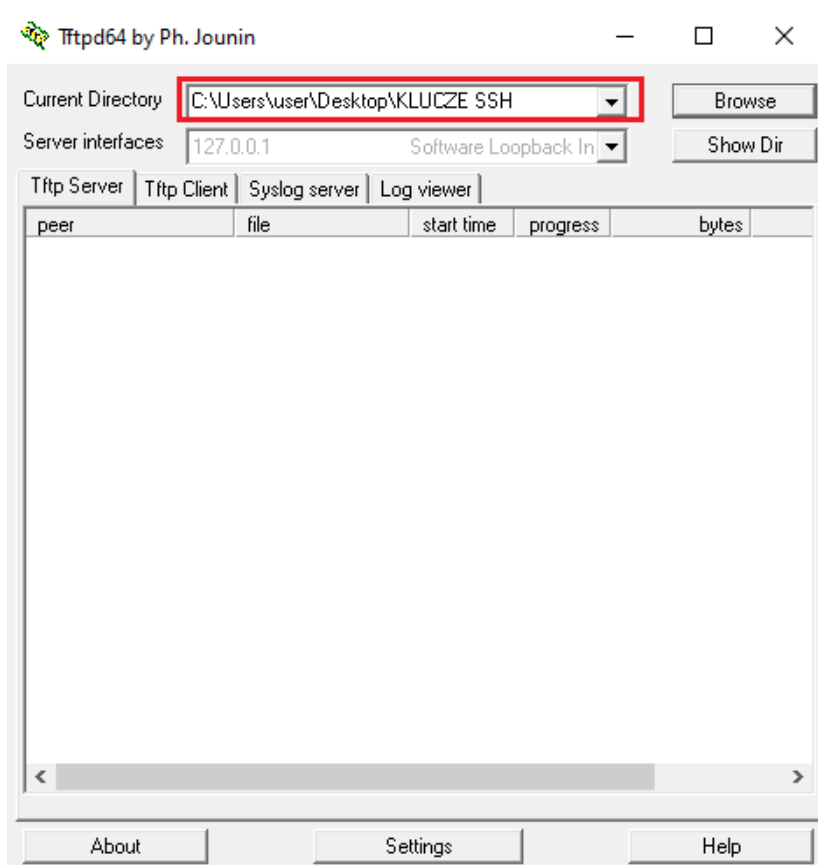
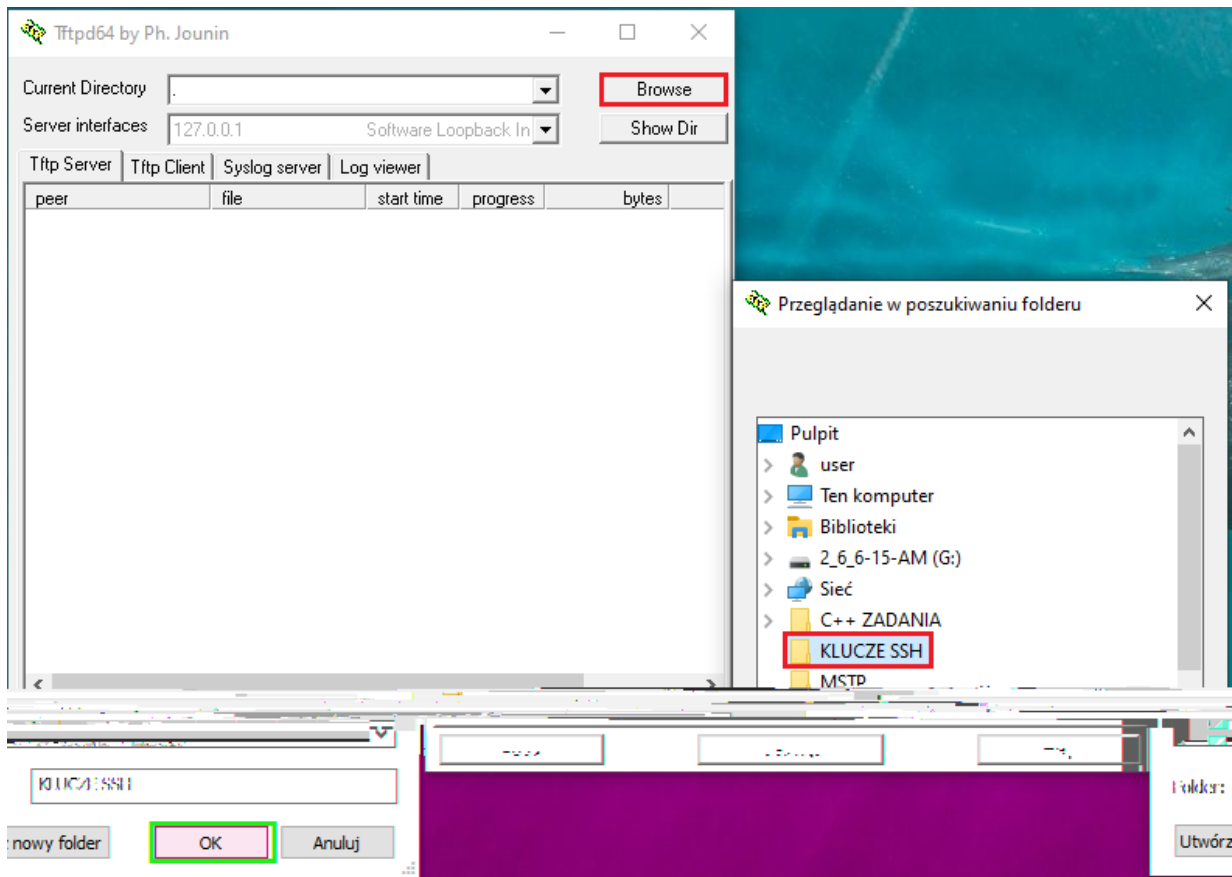












W konsoli cmd połącz się z przełącznikiem i prześlij mu klucz publiczny z serwera ftp

```
Wiersz polecenia
Microsoft Windows [Version 10.0.19045.4780]
(c) Microsoft Corporation. Wszelkie prawa zastrzeżone.
C:\Users\user>telnet 192.168.0.2
```

```
Telnet 192.168.0.2
***** User Access Login *****
User:admin
Password: admin

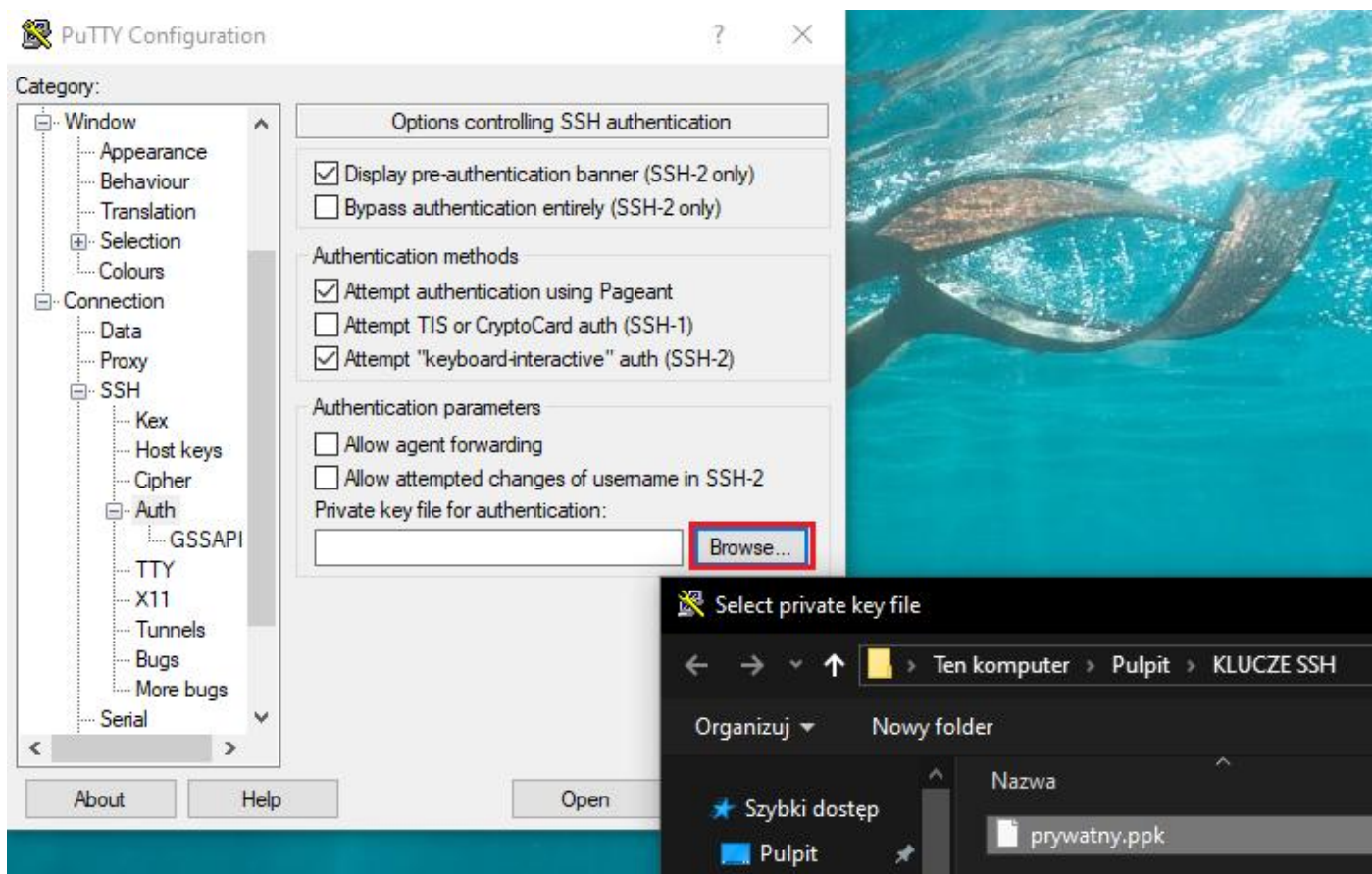
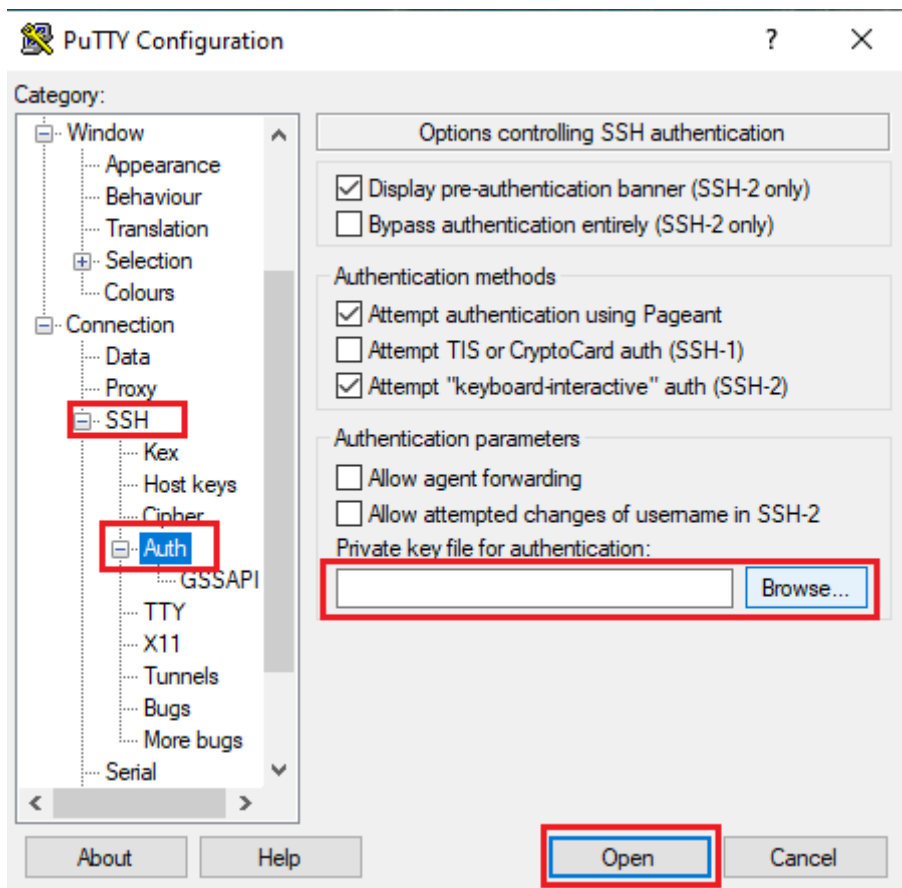
T2500G-10MPS>enable

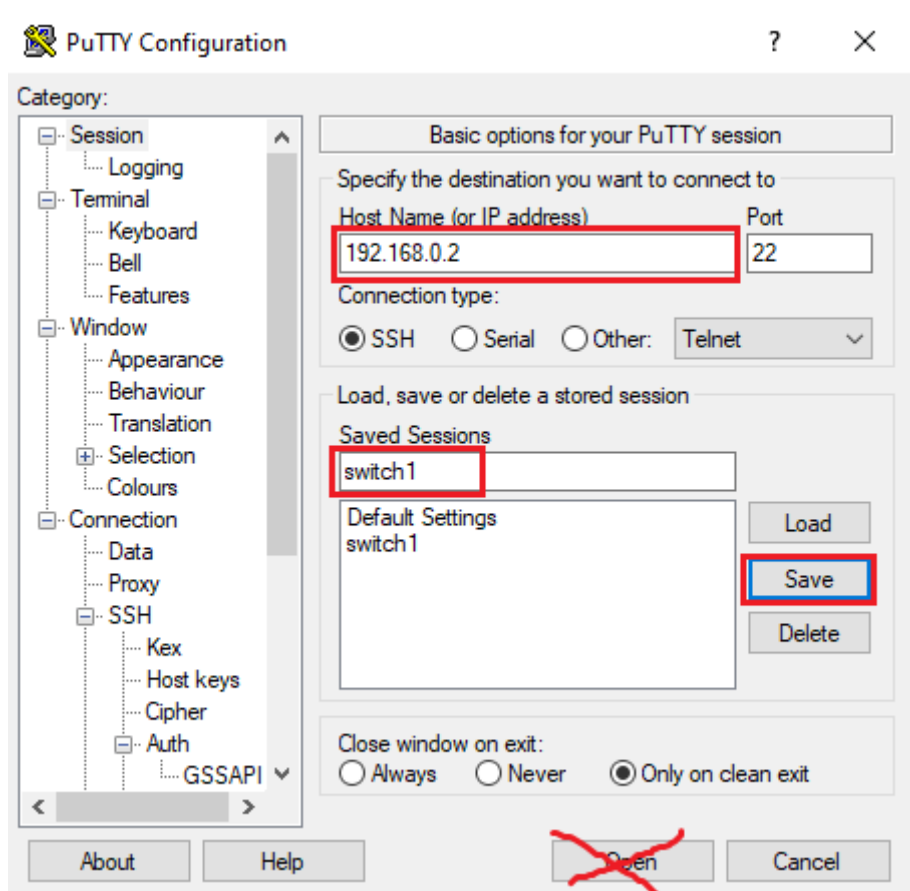
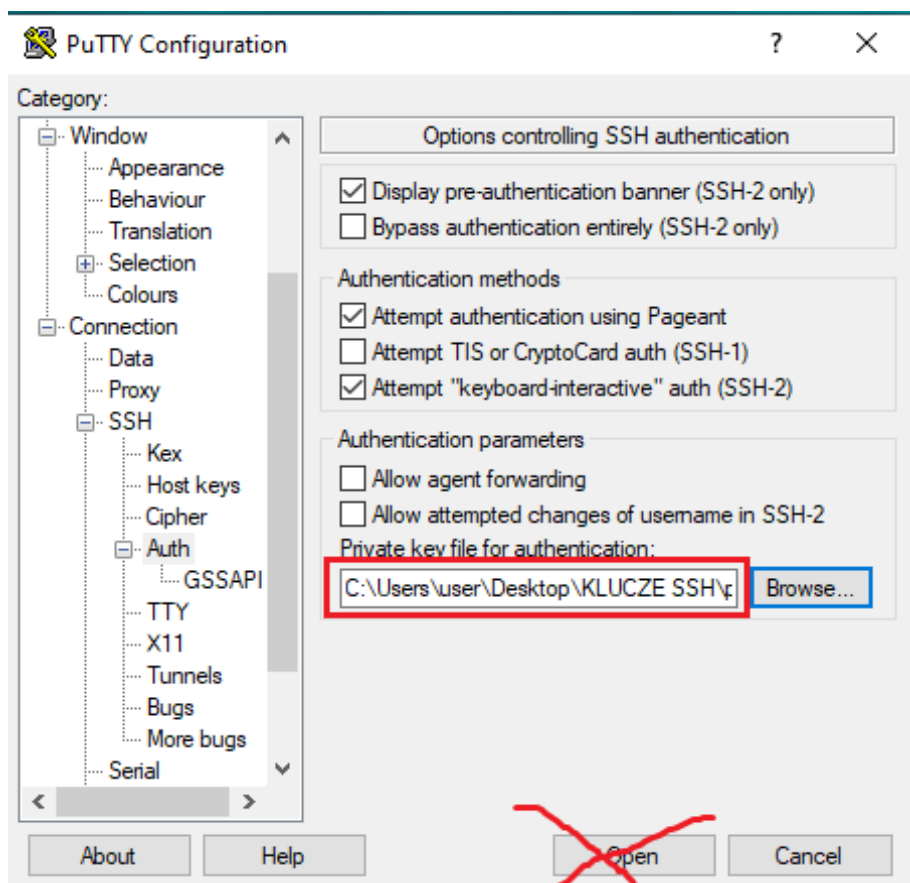
T2500G-10MPS#configure
configure

T2500G-10MPS#configure

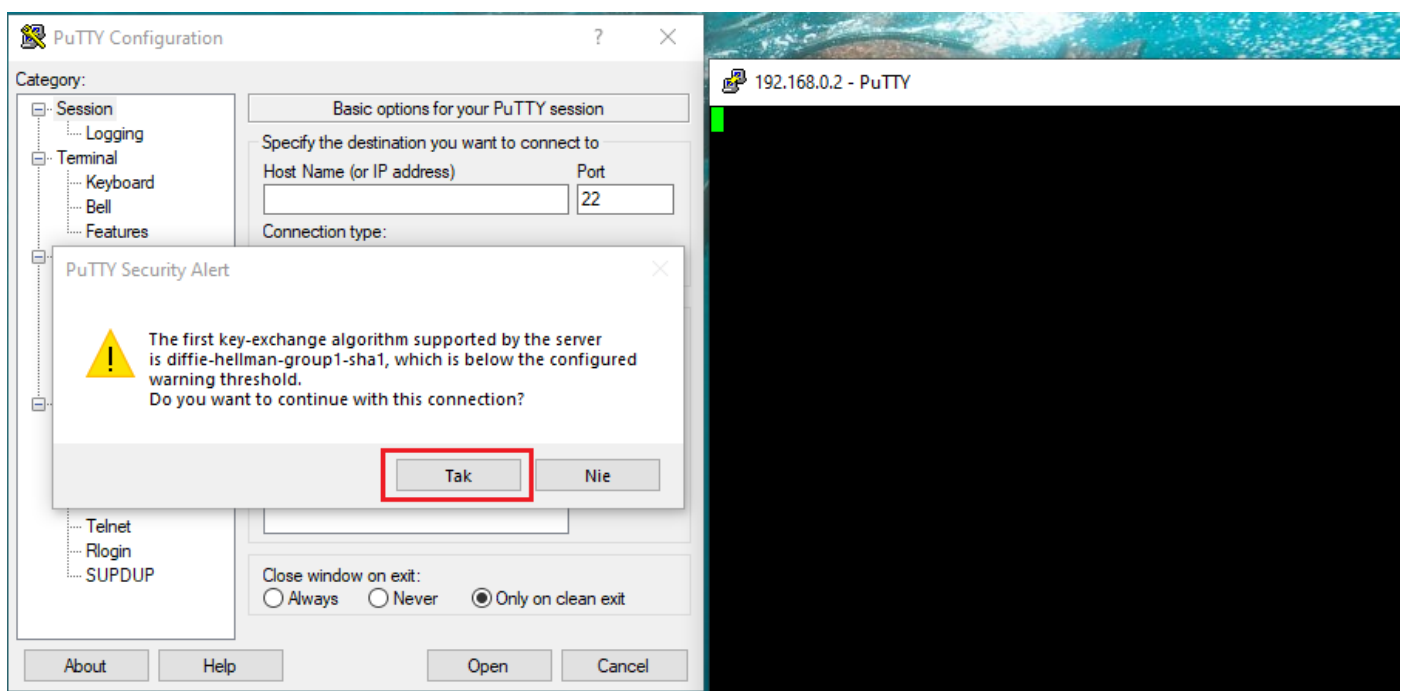
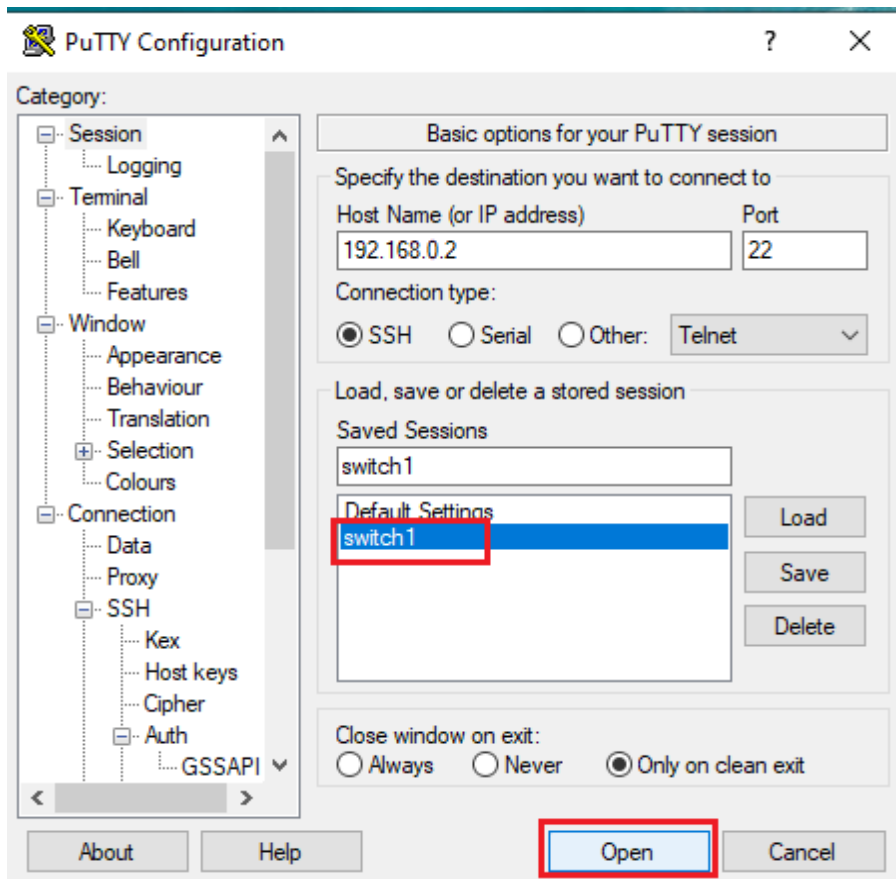
T2500G-10MPS(config)#$publiczny ip-address 192.168.0.100
Start to download SSH key file.....
Download SSH key file OK.
                                     nazwa klucza publicznego
                                     ↓
T2500G-10MPS(config)#ip ssh download v2 publiczny ip-address 192.168.0.100
Start to download SSH key file.....
Download SSH key file OK.
                                     IPv4 serwera tftp
                                     ↓
T2500G-10MPS(config)#
```

W programie putty zdefiniuj połączenie z przełącznikiem z kluczem prywatnym





Połącz się z przełącznikiem w procesie uwierzytelniania hasłem klucza prywatnego.



PuTTY Security Alert



The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.

The server's dss key fingerprint is:

ssh-rsa 512 SHA256:h1nD8T017X119NkY3wD9Voh81iHYUJubf2M23KLU70U1

[Help](#)[More info...](#)[Accept](#)[Connect Once](#)[Cancel](#)

```
login as: admin
Further authentication required
Authenticating with public key "switch1"
Passphrase for key "switch1":
```

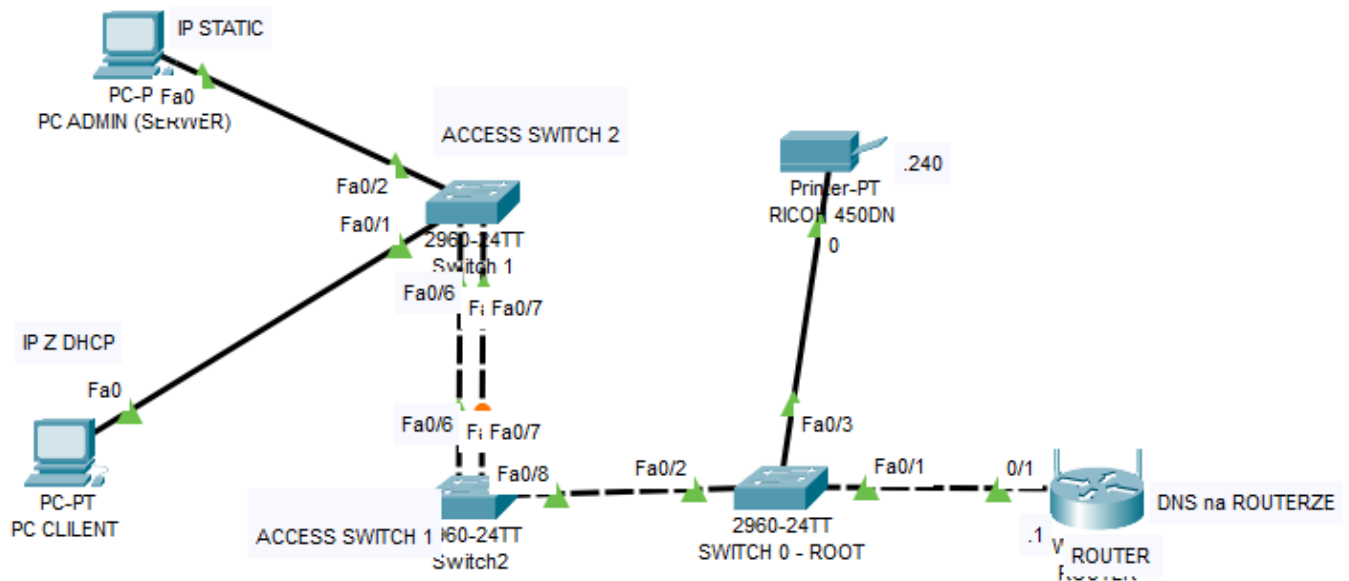
```
T2500G-10MPS>
```

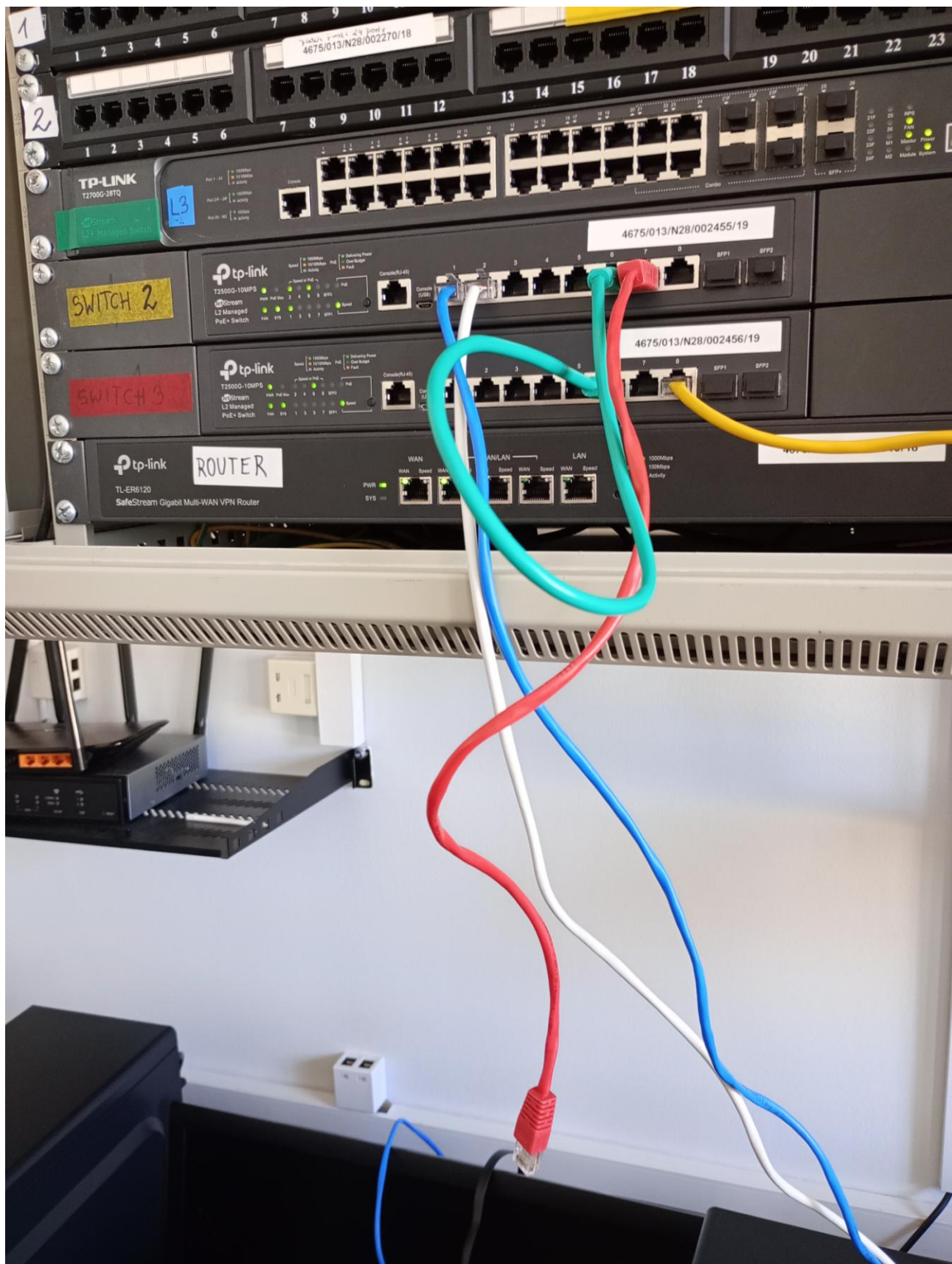
2.8 SWITCHING

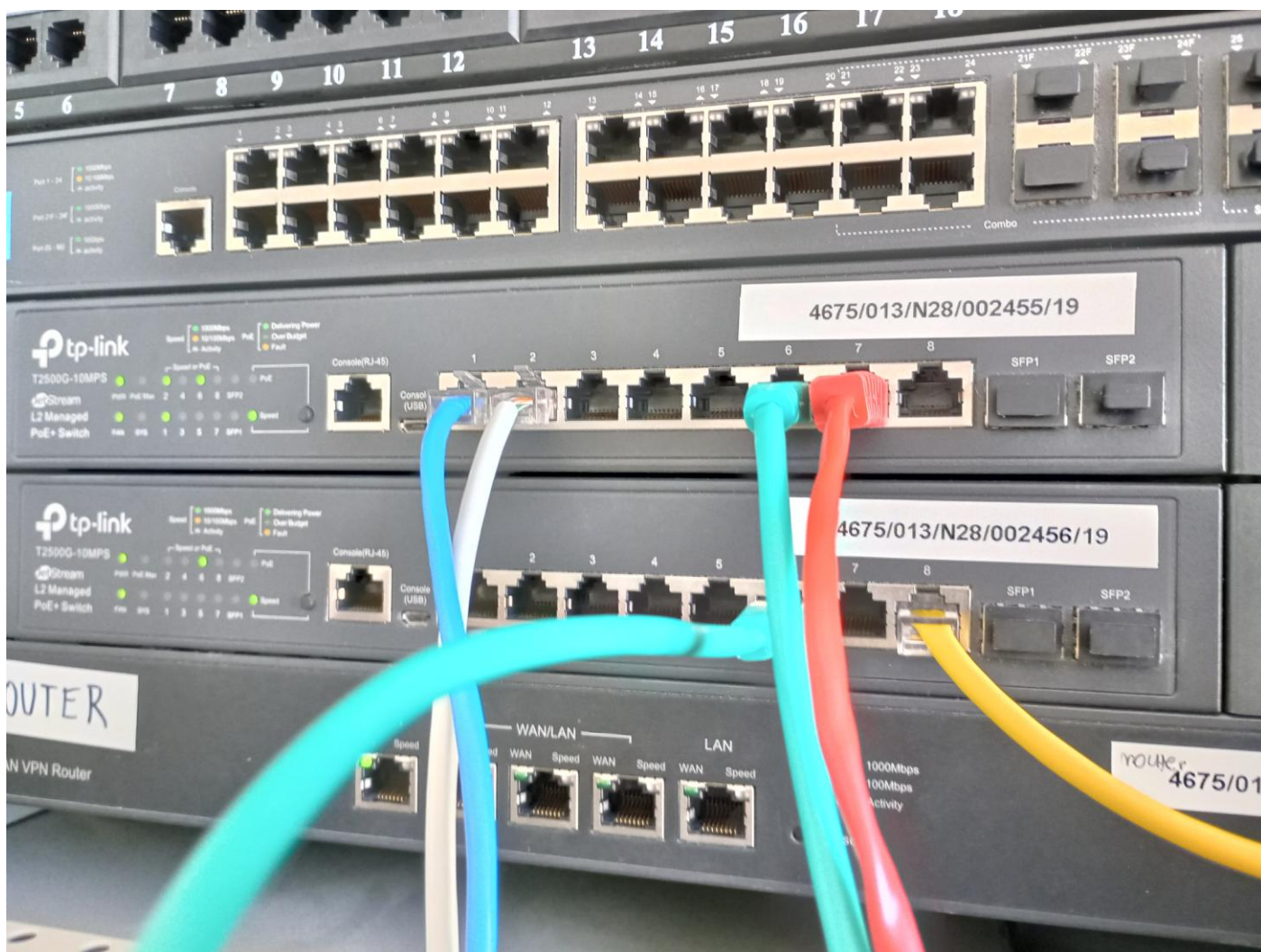
1. Podłącz kable według schematu z Cisco Packet

Fizyczna konfiguracja sieci LAN 192.168.10.0/24

Statyczna Konfiguracja interfejsów sieciowych na PC ADMIN i przełączniku (ACCESS SWITCH 2) wg poniższej tabeli:

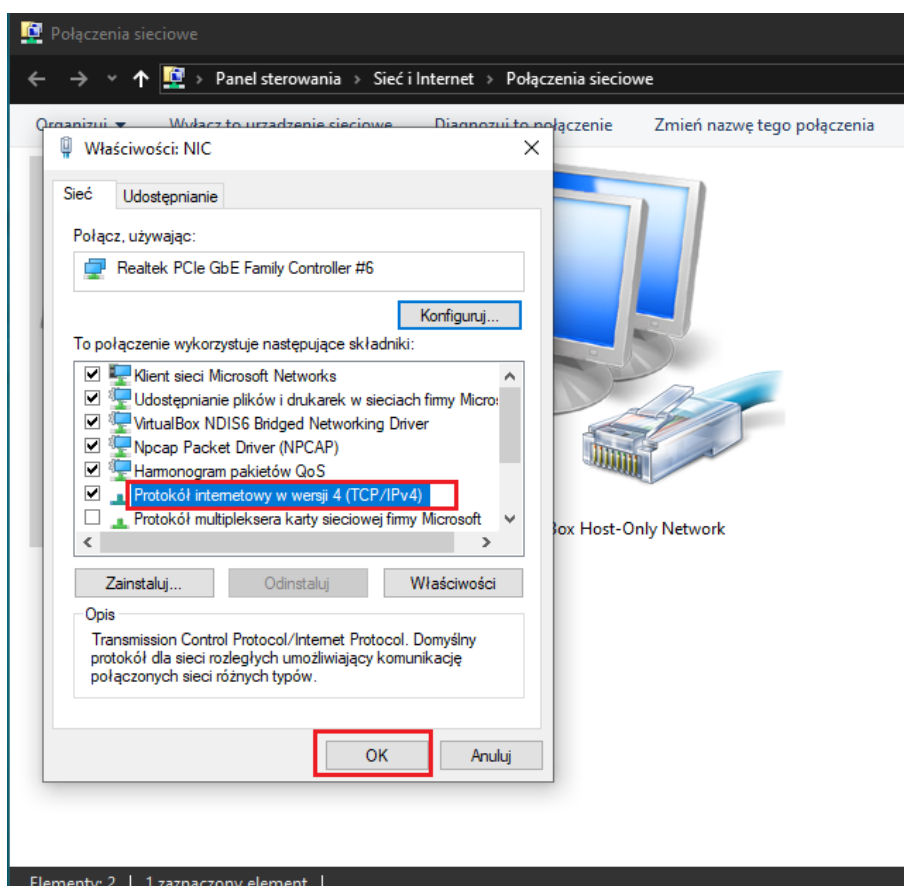
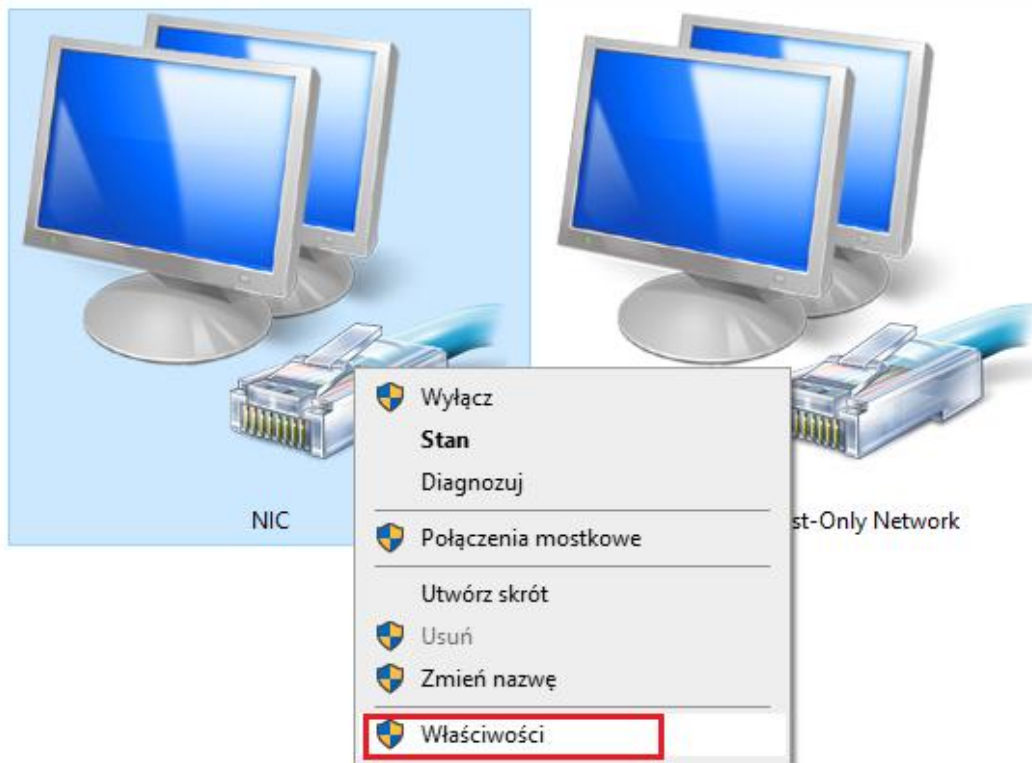


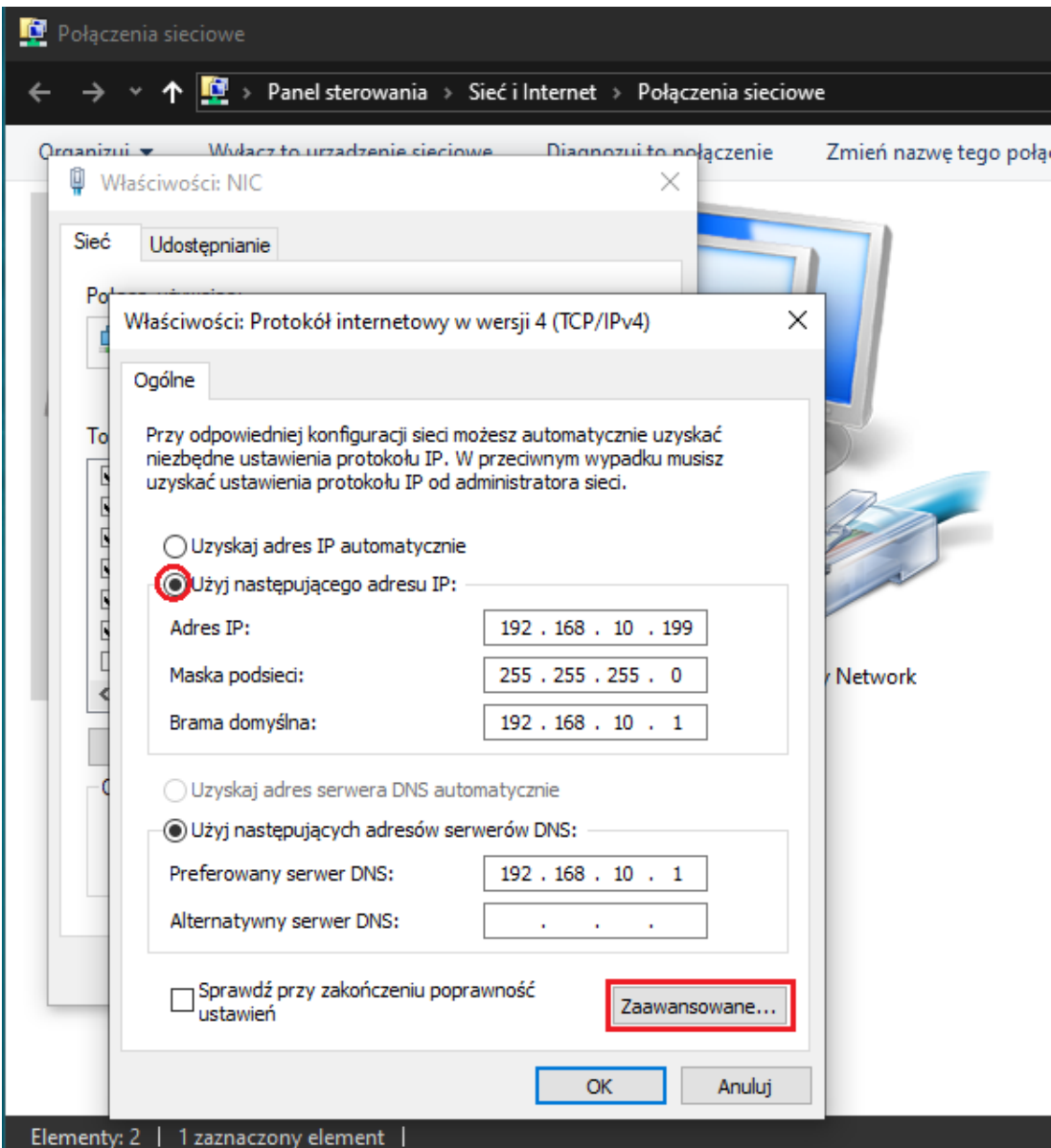


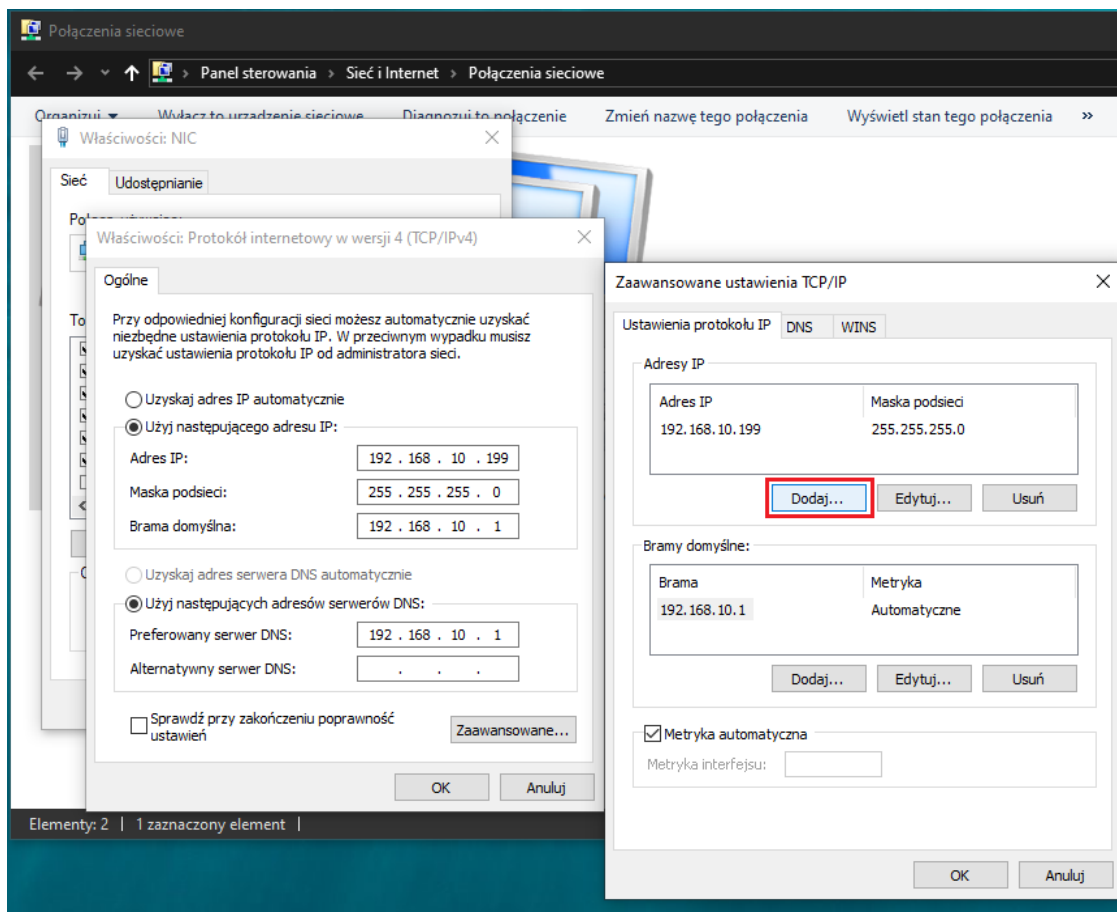


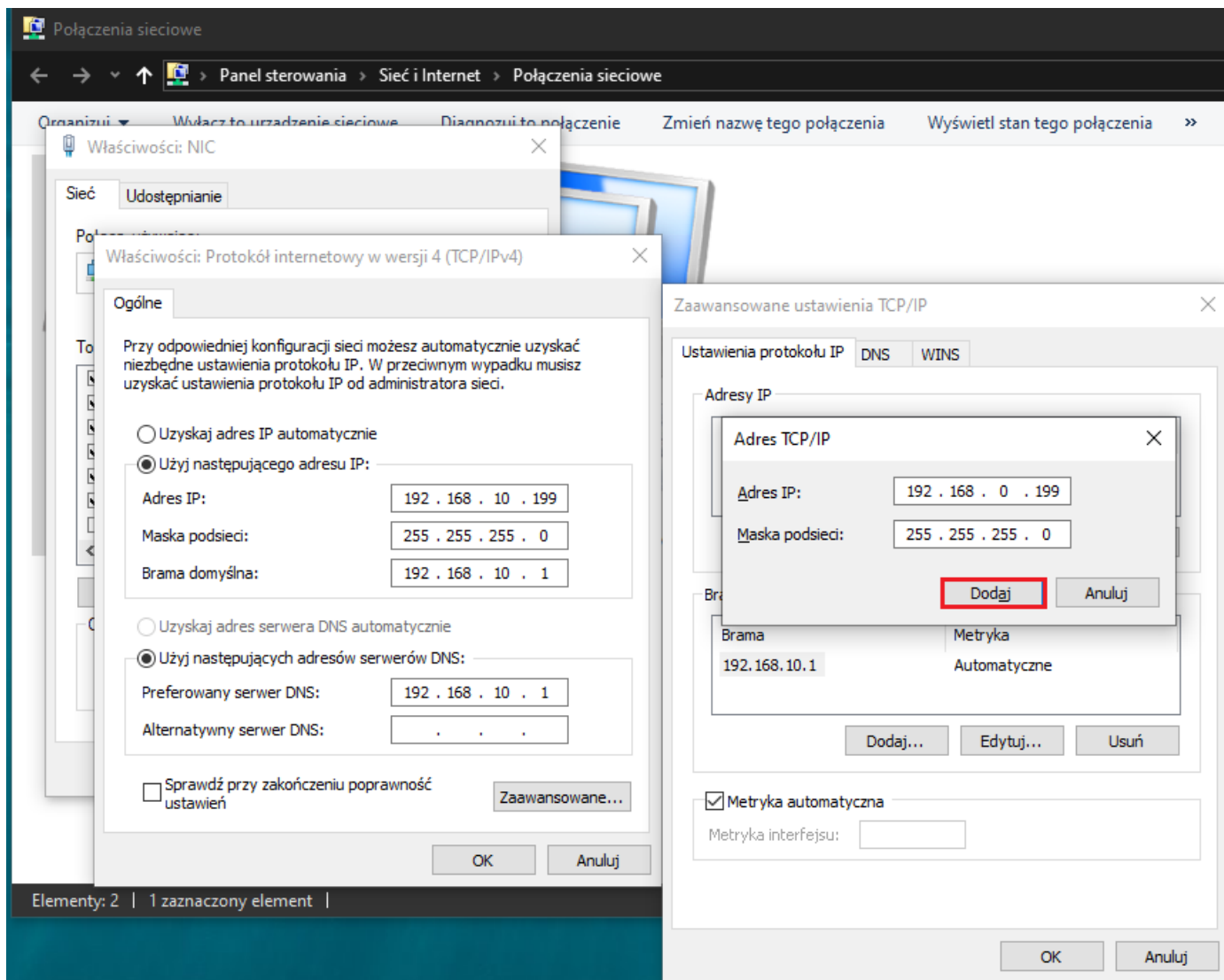
2. Ustaw kartę sieciową na PC Adminie według tabelki. Każda grupa ma swój wiersz. W tej instrukcja zostały zastosowane adresy z grupy dziewiętej.

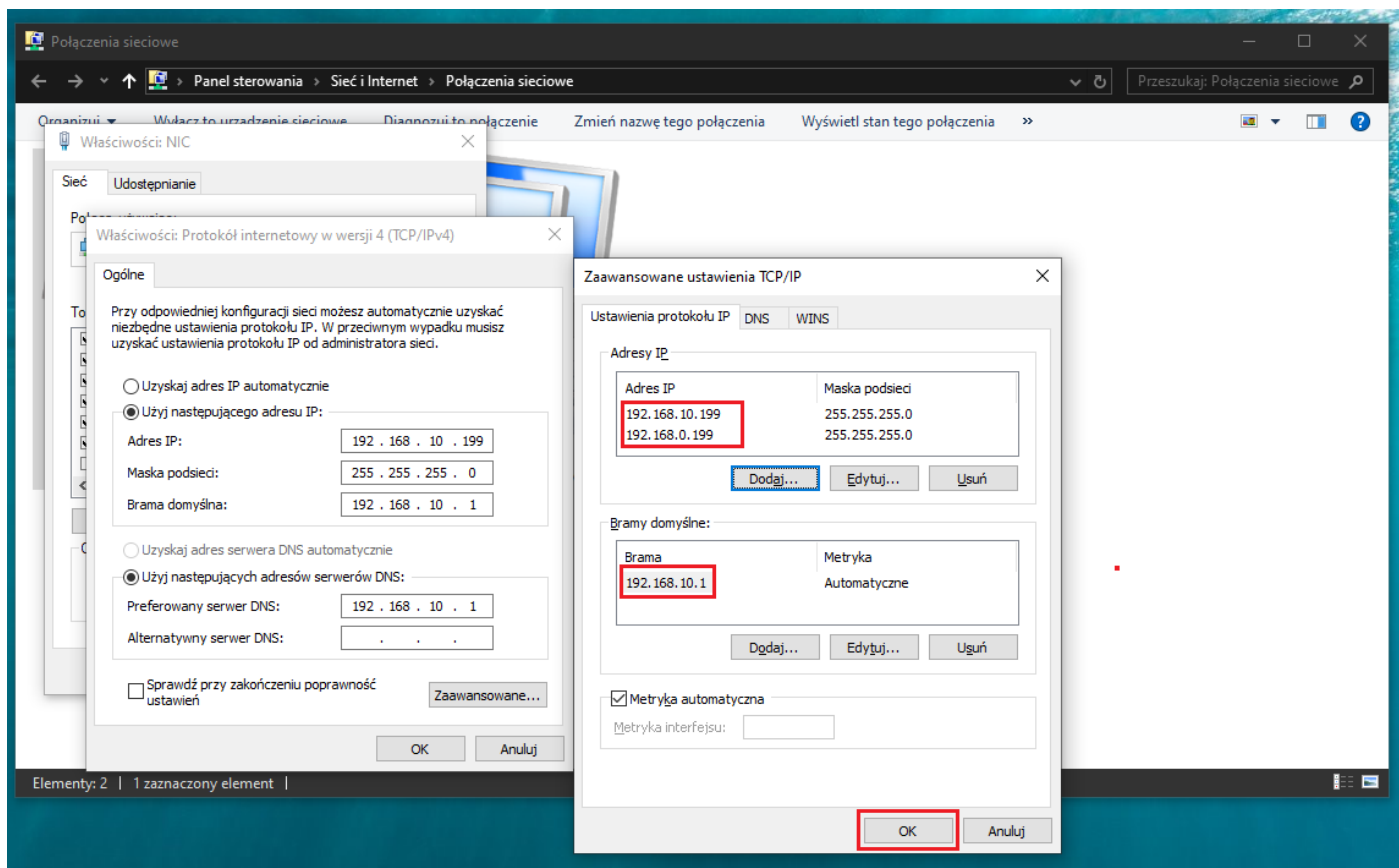
GRUPA1	IPv4 PC ADMIN (SERWER) 192.168.0.0/24	IPv4 PC ADMIN (SERWER) 192.168.10.0/24	IPv4 ACCESS SWITCH 1	IPv4 ACCESS SWITCH 2
1	192.168.0.191	192.168.10.191	192.168.10.221	192.168.10.231
2	192.168.0.192	192.168.10.192	192.168.10.222	192.168.10.232
3	192.168.0.193	192.168.10.193	192.168.10.223	192.168.10.233
4	192.168.0.194	192.168.10.194	192.168.10.224	192.168.10.234
5	192.168.0.195	192.168.10.195	192.168.10.225	192.168.10.235
6	192.168.0.196	192.168.10.196	192.168.10.226	192.168.10.236
7	192.168.0.197	192.168.10.197	192.168.10.227	192.168.10.237
8	192.168.0.198	192.168.10.198	192.168.10.228	192.168.10.238
9	192.168.0.199	192.168.10.199	192.168.10.229	192.168.10.239

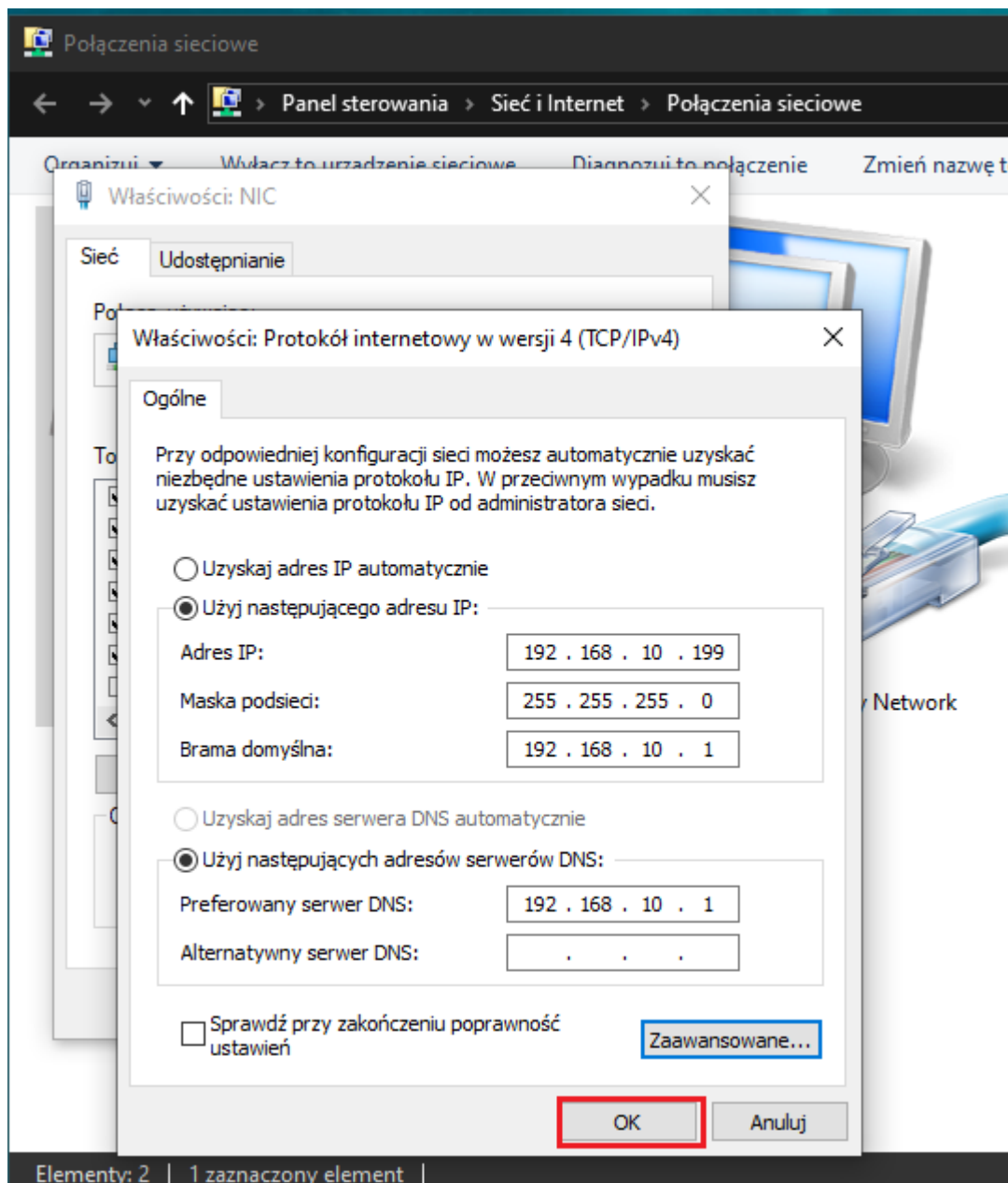


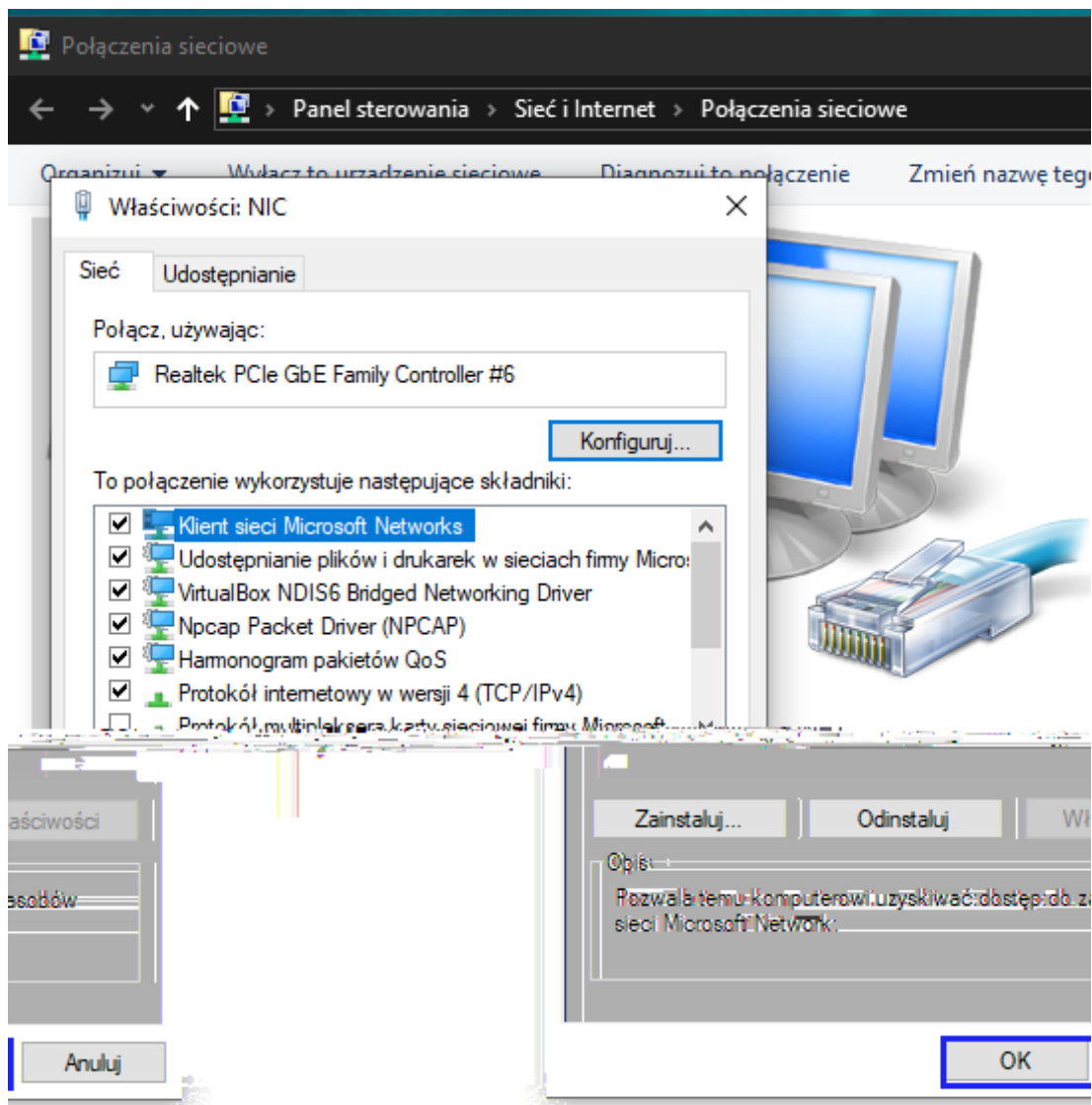


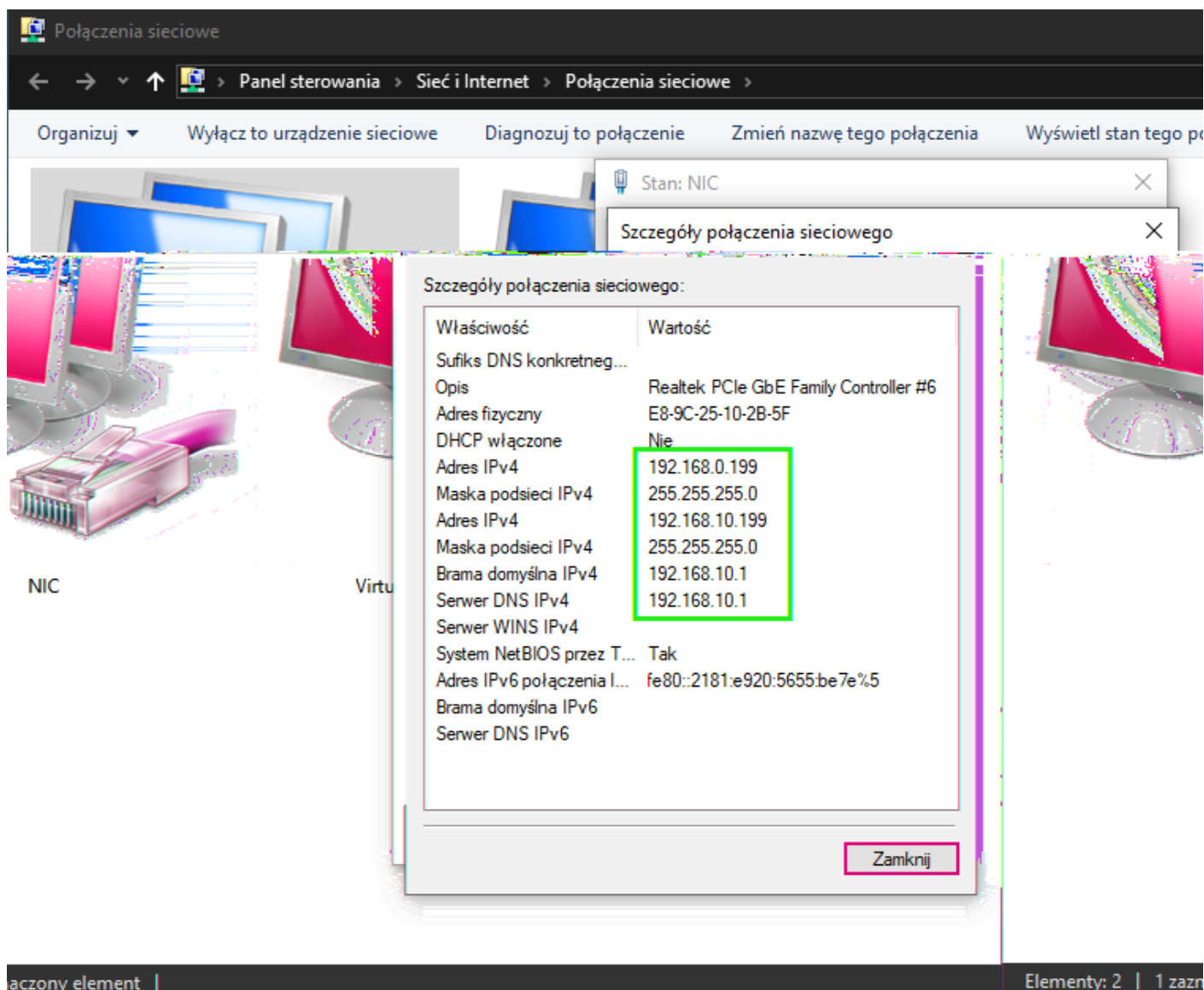












3. Ustaw nowe adresy IPv4 przełączników w sieci **192.168.10.0/24**.

GRUPA1	IPv4 PC ADMIN (SERWER) 192.168.0.0/24	IPv4 PC ADMIN (SERWER) 192.168.10.0/24	IPv4 ACCESS SWITCH 1	IPv4 ACCESS SWITCH 2
1	192.168.0.191	192.168.10.191	192.168.10.221	192.168.10.231
2	192.168.0.192	192.168.10.192	192.168.10.222	192.168.10.232
3	192.168.0.193	192.168.10.193	192.168.10.223	192.168.10.233
4	192.168.0.194	192.168.10.194	192.168.10.224	192.168.10.234
5	192.168.0.195	192.168.10.195	192.168.10.225	192.168.10.235
6	192.168.0.196	192.168.10.196	192.168.10.226	192.168.10.236
7	192.168.0.197	192.168.10.197	192.168.10.227	192.168.10.237
8	192.168.0.198	192.168.10.198	192.168.10.228	192.168.10.238
9	192.168.0.199	192.168.10.199	192.168.10.229	192.168.10.239

Poniżej zaprezentowany **ACCESS SWITCH 2**

LIBRUS Synergia x T2500G-10MPS x +

192.168.0.1 170%

tp-link

T2500G-10MPS System Summary Device Description System Time Daylight Saving Time Serial Port Setting System IP System IPv6

System

- **System Info**
- User Management
- System Tools
- Access Security

Switching

VLAN

Spanning Tree

Multicast

DHCP

QoS

PoE

ACL

Network Security

SNMP

LLDP

Maintenance

Save Config

Index

IP Config

MAC Address: B0-BE-76-81-35-5D

IP Address Mode: ☒ Static IP ☐ DHCP ☐ BOOTP

Management VLAN: 1 (VLAN ID: 1-4094)

IP Address: 192.168.10.239

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.1

Apply

Help

Note:
Changing IP address to a different IP segment will interrupt the network communication, so please keep the new IP address in the same IP segment with the local network.

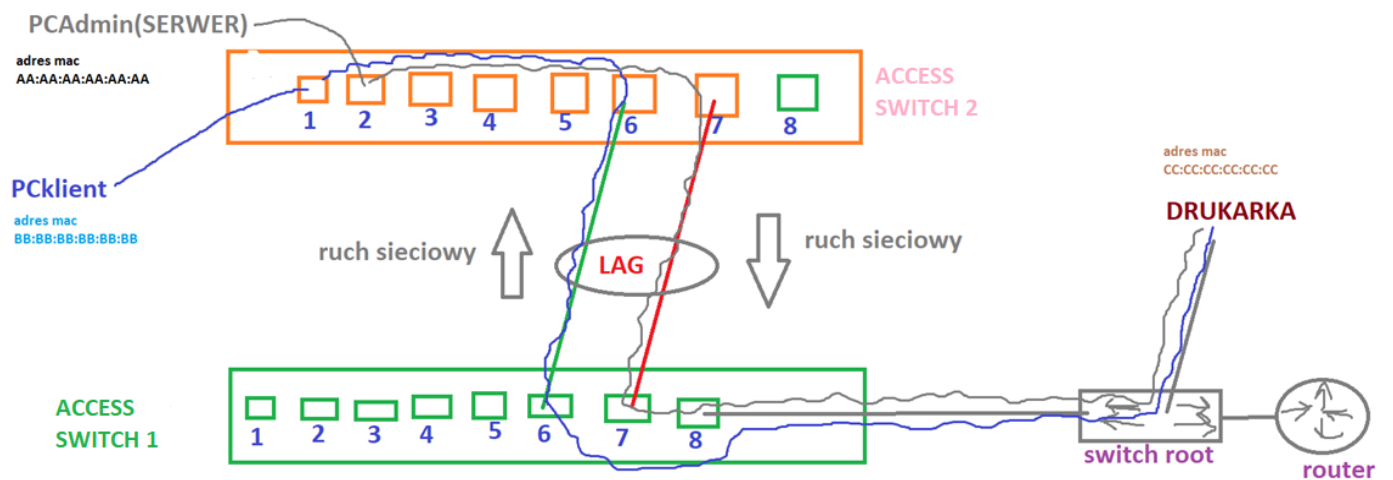
Tak samo ustaw adres IPv4 na **ACCESS SWITCH-u 1**

4. LAG – TEORIA

NETWORKING KUNG FU



Sztuka LAG - owania



5. USTAW LAG na przełącznikach

SWITCHING

1. LAN STATIC. Agregowanie łączy ustaw na portach 6 i 7 na przełącznikach access switch 1 i 2.

UWAGA! **Access switch 1** podłączony jest do Internetu z portu 8.

ACCESS SWITCH 2

T2500G-10MPS

System

Switching

• Port

• **LAG**

• Traffic Monitor

• MAC Address

• DDM

• L2PT

LAG TableStatic LAGLACP Config

Global Config

Hash Algorithm:SRC MAC+DST MAC

Apply

LAG Table

Select	Group Number	Description	Member	Operation
No entry in the table.				

AllDeleteHelp

T2500G-10MPS

System

Switching

• Port

• **LAG**

• Traffic Monitor

• MAC Address

• DDM

• L2PT

VLAN

Spanning Tree

Multicast

DHCP

QoS

PoE

LAG TableStatic LAGLACP Config

LAG Config

Group Number:LAG6

DescriptionStatic LAG

Member Port

UNIT:1

12345678910

ClearApplyHelp

Unselected Port(s)

Selected Port(s)

Not A

Note:
1. LAG* denotes the Link Aggregation Group which the port belongs to.

T2500G-10MPS

Port Config

Port Mirror

Port Security

Port Isolation

Loopback Detection

System

Switching

Port

LAG

Traffic Monitor

MAC Address

DDM

L2PT

VLAN

Spanning Tree

Multicast

DHCP

QoS

PoE

ACL

Network Security

SNMP

LLDP

Global Config

Jumbo:

1518

(1518-9216, default: 1518)

Apply

Port Config

UNIT: 1 LAGS

Select	Port	Type	Description	Status	Speed	Duplex	Flow Control	LAG
☐								
☐	1/0/1	Copper		Enable	Auto	Auto	Disable	---
☐	1/0/2	Copper		Enable	Auto	Auto	Disable	---
☐	1/0/3	Copper		Enable	Auto	Auto	Disable	---
☐	1/0/4	Copper		Enable	Auto	Auto	Disable	---
☐	1/0/5	Copper		Enable	Auto	Auto	Disable	---
☐	1/0/6	Copper		Enable	Auto	Auto	Disable	LAG 6
☐	1/0/7	Copper		Enable	Auto	Auto	Disable	LAG 6
☐	1/0/8	Copper		Enable	Auto	Auto	Disable	---
☐	1/0/9	Sfp		Enable	1000M	Full	Disable	---
☐	1/0/10	Sfp		Enable	1000M	Full	Disable	---

All

Apply

Help

Tak samo ustaw na ACCESS SWITCH 1

LAG Table

Static LAG

LACP Config

Global Config

Hash Algorithm:

SRC MAC+DST MAC

Apply

LAG Table

Select	Group Number	Description	Member	Operation
No entry in the table.				

All

Delete

Help

T2600G-28TS

LAG Table

Static LAG

LACP Config

System

Switching

Port

LAG

Traffic Monitor

MAC Address

DDM

L2PT

VLAN

Spanning Tree

Ethernet OAM

Multicast

Routing

QoS

ACL

LAG Config

Group Number:

LAG1

Description

Static LAG

Member Port

UNIT: 1

2	4	6	8	10	12	14	16	18	20	22	24	26	28
1	3	5	7	9	11	13	15	17	19	21	23	25	27

Clear

Apply

Help

Unselected Port(s)

Selected Port(s)

Not Available for Selection

Note:

1. LAG* denotes the Link Aggregation Group which the port belongs to.

Port Config									
Port Mirror									
Port Security									
Port Isolation									
Loopback Detection									
Port Config									
UNIT:		1 LAGS							
Select	Port	Type	Description	Status	Speed	Duplex	Flow Control	Jumbo	LAG
☐				v	v	v	v	v	
☐	1/0/1	Copper		Enable	Auto	Auto	Disable	Disable	---
☐	1/0/2	Copper		Enable	Auto	Auto	Disable	Disable	---
☐	1/0/3	Copper		Enable	Auto	Auto	Disable	Disable	---
☐	1/0/4	Copper		Enable	Auto	Auto	Disable	Disable	---
☐	1/0/5	Copper		Enable	Auto	Auto	Disable	Disable	---
☐	1/0/6	Copper		Enable	Auto	Auto	Disable	Disable	LAG 1
☐	1/0/7	Copper		Enable	Auto	Auto	Disable	Disable	LAG 1
☐	1/0/8	Copper		Enable	Auto	Auto	Disable	Disable	---
☐	1/0/9	Copper		Enable	Auto	Auto	Disable	Disable	---
☐	1/0/10	Copper		Enable	Auto	Auto	Disable	Disable	---
☐	1/0/11	Copper		Enable	Auto	Auto	Disable	Disable	---

Podłącz kabel czerwony do portu 7.

Odśwież strony z panelami konfiguracyjnymi przełącznika (Klawisz F5).

Jeżeli strony panelów konfiguracyjnych przełączników nie wyświetlają się, to najprawdopodobniej wystąpił FLASHING (szybkie mruganie diod na przełącznikach). Wypnij jeden koniec czerwonego kabla z portu 7 i popraw konfigurację.

Połącz **access switch 1** (**port 8**) z routerem i drukarką.

Odśwież kartę sieciową PCKlienta. Powinien on dostać adres IPv4 w sieci 192.168.10.0/24.

Wykonaj pingowanie na router i drukarkę


```
C:\Users\user>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time<1ms TTL=64
Reply from 192.168.10.1: bytes=32 time<1ms TTL=64
Reply from 192.168.10.1: bytes=32 time<1ms TTL=64
Reply from 192.168.10.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\user>ping 192.168.10.240

Pinging 192.168.10.240 with 32 bytes of data:
Reply from 192.168.10.240: bytes=32 time<1ms TTL=255
Reply from 192.168.10.240: bytes=32 time<1ms TTL=255
Reply from 192.168.10.240: bytes=32 time<1ms TTL=255
Reply from 192.168.10.240: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.240:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. Na access switch-u 1 ustaw flow control dla portów 6,7 i 8.

Po co flow control ?

Instrukcja T2500G-10MPS str. 76 -77

With this option enabled, the switch synchronizes the data transmission speed with the peer device, thus avoiding the packet loss caused by congestion. By default, it is disabled.



179 / 5 000

Po włączeniu tej opcji przełącznik synchronizuje prędkość transmisji danych z urządzeniem równorzędnym, unikając w ten sposób utraty pakietów spowodowanej przeciążeniem. Domyślnie opcja ta jest wyłączona.



Prześlij opinię

Port Config

Port Mirror

Port Security

Port Isolation

Loopback Detection

Global Config

Jumbo:

1518

(1518-9216, default: 1518)

Port Config

UNIT: 1 LAGS

Select	Port	Type	Description	Status	Speed	Duplex	Flow Control
☐							
☒	1/0/1	Copper	PCKlient	Enable	100M	Auto	
☒	1/0/2	Copper	PCAdmin	Enable	100M	Auto	Disable
☐	1/0/3	Copper		Enable	Auto	Auto	Enable
☐	1/0/4	Copper		Enable	Auto	Auto	Disable
☐	1/0/5	Copper		Enable	Auto	Auto	Disable
☒	1/0/6	Copper	28ts_router_druk	Enable	Auto	Auto	Disable
☒	1/0/7	Copper	28ts_router_druk	Enable	Auto	Auto	Disable
☐	1/0/8	Copper		Enable	Auto	Auto	Disable
☐	1/0/9	Sfp		Enable	1000M	Full	Disable
☐	1/0/10	Sfp		Enable	1000M	Full	Disable

All

Apply

Help

3. Na przełączniku 2 ustaw przepustowość 100Mb/s na portach 1 i 2.

Jeżeli prawidłowo podłączyłeś kable,

do portu 2 podłączony jest PC-admin(serwer),

do portu 1 podłączony jest PC-client.

Ustaw flow control dla portów 1,2,6,7.

Speed

Select the appropriate speed mode for the port.

When Auto is selected, the port autonegotiates speed mode with the connected device.

The default setting is Auto.

This value is recommended if both ends of the line support autonegotiation.

Prędkość

Wybierz odpowiedni tryb prędkości dla portu.

Gdy wybrano opcję Auto, port automatycznie negocjuje tryb prędkości z podłączonym urządzeniem.

Domyślnym ustawieniem jest Auto.

Ta wartość jest zalecana, jeśli oba końce linii obsługują autonegotiację.

Prześlij opinię

Opisz porty, do których podłączone są kable sieciowe

Port Config
Port Mirror
Port Security
Port Isolation
Loopback Det

Global Config

Jumbo:
(1518-9216, default: 1518)

Port Config

UNIT: 1 LAGS

Select	Port	Type	Description	Status	Speed
☐			PCAdmin	v	
☐	1/0/1	Copper	PCKlient	Enable	Auto
☒	1/0/2	Copper		Enable	Auto
☐	1/0/3	Copper		Enable	Auto
☐	1/0/4	Copper		Enable	Auto
☐	1/0/5	Copper		Enable	Auto
☐	1/0/6	Copper		Enable	Auto
☐	1/0/7	Copper		Enable	Auto
☐	1/0/8	Copper		Enable	Auto
☐	1/0/9	Sfp		Enable	10G
☐	1/0/10	Sfp		Enable	10G

All
Apply

Global Config

Jumbo:

(1518-9216, default: 1518)

Port Config

UNIT: LAGS

Select	Port	Type	Description	Status	Speed
☐			28ts_router_druk	v	
☐	1/0/1	Copper	PCKlient	Enable	Auto
☐	1/0/2	Copper	PCAdmin	Enable	Auto
☐	1/0/3	Copper		Enable	Auto
☐	1/0/4	Copper		Enable	Auto
☐	1/0/5	Copper		Enable	Auto
☒	1/0/6	Copper		Enable	Auto
☒	1/0/7	Copper		Enable	Auto
☐	1/0/8	Copper		Enable	Auto
☐	1/0/9	Sfp		Enable	1000
☐	1/0/10	Sfp		Enable	1000

Ustaw przepustowość 100M dla portów 1 i 2

Port Config

Port Mirror

Port Security

Port Isolation

Loopback Detection

Global Config

Jumbo: (1518-9216, default: 1518)

Port Config

UNIT:

1

 LAGS

Select	Port	Type	Description	Status	Speed	Dup
☐				▼	▼	
☒	1/0/1	Copper	PCKlient	Enable		Au
☒	1/0/2	Copper	PCAdmin	Enable	10M	Au
☐	1/0/3	Copper		Enable	100M	Au
☐	1/0/4	Copper		Enable	1000M	Au
☐	1/0/5	Copper		Enable	Auto	Au
☐	1/0/6	Copper	28ts_router_druk	Enable	Auto	Au
☐	1/0/7	Copper	28ts_router_druk	Enable	Auto	Au
☐	1/0/8	Copper		Enable	Auto	Au
☐	1/0/9	Sfp		Enable	1000M	Fu
☐	1/0/10	Sfp		Enable	1000M	Fu

All

Apply

Help

Ustaw flow control dla portów 1,2,6,7

Port Config

Port Mirror

Port Security

Port Isolation

Loopback Detection

Global Config

Jumbo:1518(1518-9216, default: 1518)

Port Config

UNIT:1LAGS

Select	Port	Type	Description	Status	Speed	Duplex	Flow Control
☐							
☒	1/0/1	Copper	PCKlient	Enable	100M	Auto	
☒	1/0/2	Copper	PCAdmin	Enable	100M	Auto	Disable
☐	1/0/3	Copper		Enable	Auto	Auto	Enable
☐	1/0/4	Copper		Enable	Auto	Auto	Disable
☐	1/0/5	Copper		Enable	Auto	Auto	Disable
☒	1/0/6	Copper	28ts_router_druk	Enable	Auto	Auto	Disable
☒	1/0/7	Copper	28ts_router_druk	Enable	Auto	Auto	Disable
☐	1/0/8	Copper		Enable	Auto	Auto	Disable
☐	1/0/9	Sfp		Enable	1000M	Full	Disable
☐	1/0/10	Sfp		Enable	1000M	Full	Disable

All

Apply

Help

Port Config

Port Mirror

Port Security

Port Isolation

Loopback Detection

Global Config

Jumbo:1518(1518-9216, default: 1518)

Port Config

UNIT:1LAGS

Select	Port	Type	Description	Status	Speed	Duplex	Flow Control
☐							
☐	1/0/1	Copper	PCKlient	Enable	100M	Auto	Enable
☐	1/0/2	Copper	PCAdmin	Enable	100M	Auto	Enable
☐	1/0/3	Copper		Enable	Auto	Auto	Disable
☐	1/0/4	Copper		Enable	Auto	Auto	Disable
☐	1/0/5	Copper		Enable	Auto	Auto	Disable
☐	1/0/6	Copper	28ts_router_druk	Enable	Auto	Auto	Enable
☐	1/0/7	Copper	28ts_router_druk	Enable	Auto	Auto	Enable
☐	1/0/8	Copper		Enable	Auto	Auto	Disable
☐	1/0/9	Sfp		Enable	1000M	Full	Disable
☐	1/0/10	Sfp		Enable	1000M	Full	Disable

All

Apply

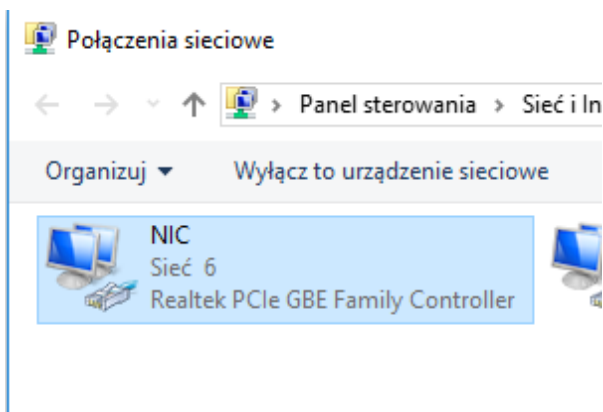
Help

4. Na przełączniku 2 ustaw śledzenie ruchu sieciowego na PCadmin.

Zadaniem twoim jest przechwycić ruch sieciowy Pc-clienta: wchodzący i wychodzący, za pomocą programu Wireshark.

Odszukaj za pomocą programu Wireshark pakiety powiązane z PC-client po adresie IP.

Na **PCKliencie** zmień nazwę interfejsu sieciowego na NIC



W oknie konsolowym wpisz polecenie *ipconfig*, w celu uzyskania informacji o stanie karty sieciowej NIC.

W tym przypadku interfejs otrzymał adres **IPv4 192.168.10.117**. Zapamiętaj adres swojego interfejsu!!!

```
C:\Users\user>ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter VirtualBox Host-Only Network:
```

```
Connection-specific DNS Suffix  . :  
Link-local IPv6 Address . . . . . : fe80::b14f:29bb:a731:5bf4%6  
IPv4 Address. . . . . : 192.168.56.1  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . :
```

```
Wireless LAN adapter Wi-Fi:
```

```
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix  . :
```

```
Wireless LAN adapter Połączenie lokalne* 9:
```

```
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix  . :
```

```
Ethernet adapter NIC:
```

```
Connection-specific DNS Suffix  . :  
Link-local IPv6 Address . . . . . : fe80::a4df:ecc5:d4e6:ffd8%13  
IPv4 Address. . . . . : 192.168.10.117  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.10.1
```

```
Tunnel adapter Teredo Tunneling Pseudo-Interface:
```


Ustaw przekierowanie portów w zakładce **Port Mirror**

Port Config

Port Mirror

Port Security

Port Isolation

Loopback Detection

Mirror Session List

Session	Destination	Mode	Source	Operation
1	---	Ingress Only		Edit Clear
		Egress Only		
		Both		

Help

Destination Port

Destination Port: (Format: 1/0/1)UNIT:

☐ 1 ☒ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8

☐ 9 ☐ 10



Unselected Port(s)



Selected Port(s)



Not Available for Selection

Source Port

UNIT: LAGS

Select	Port	Ingress	Egress	LAG
☐		Enable	v	
☒	1/0/1	Disable		---
☐	1/0/2	Disable	Disable	---
☐	1/0/3	Disable	Enable	---
☐	1/0/4	Disable	Disable	---
☐	1/0/5	Disable	Disable	---
☐	1/0/6	Disable	Disable	---
☐	1/0/7	Disable	Disable	---
☐	1/0/8	Disable	Disable	---
☐	1/0/9	Disable	Disable	---
☐	1/0/10	Disable	Disable	---

Operation succeeded.

Destination Port

Destination Port: 1/0/2 (Format: 1/0/1) Apply

UNIT: 1

1 2 3 4 5 6 7 8 9 10

Unselected Port(s) Selected Port(s) Not Available for Selection

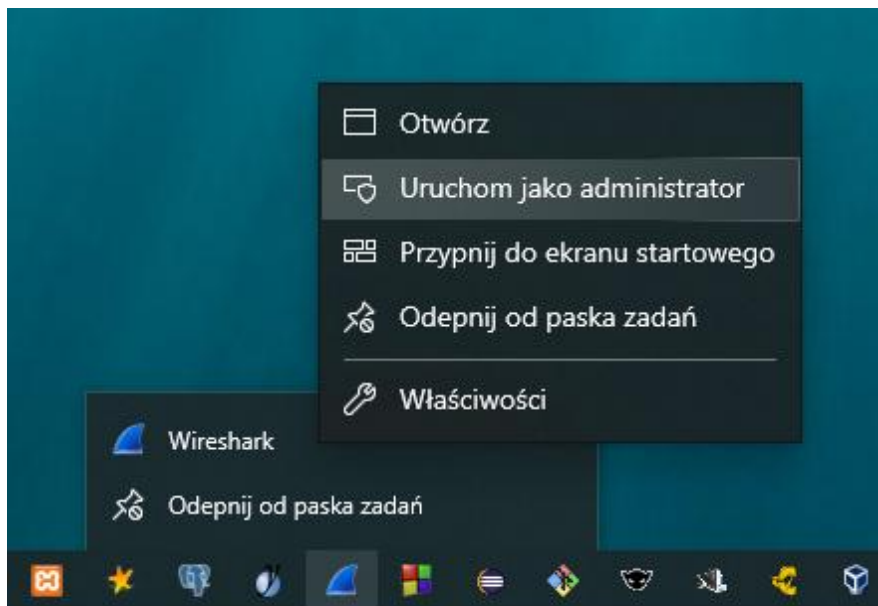
Source Port

UNIT: 1 LAGS

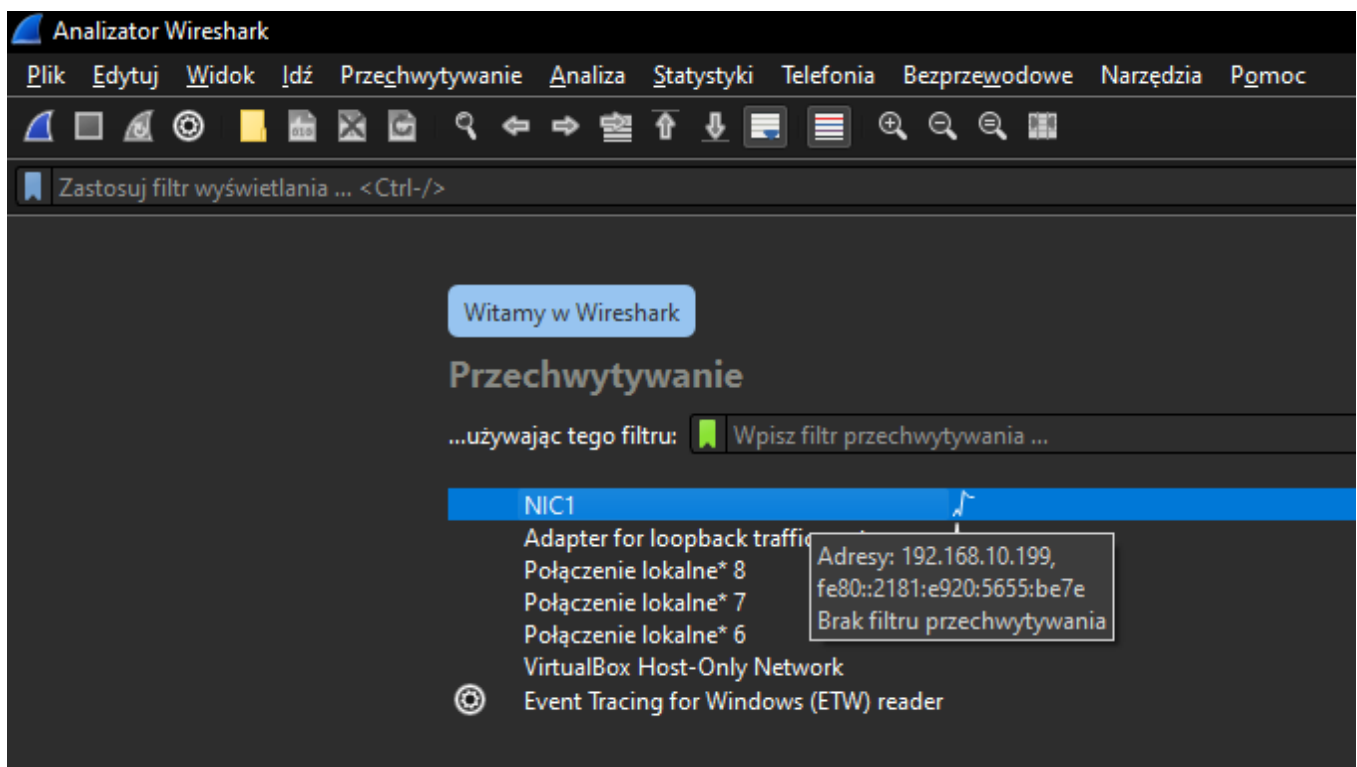
Select	Port	Ingress	Egress	LAG
☐				
☐	1/0/1	Enable	Enable	---
☐	1/0/2	Disable	Disable	---
☐	1/0/3	Disable	Disable	---
☐	1/0/4	Disable	Disable	---
☐	1/0/5	Disable	Disable	---
☐	1/0/6	Disable	Disable	---
☐	1/0/7	Disable	Disable	---
☐	1/0/8	Disable	Disable	---
☐	1/0/9	Disable	Disable	---
☐	1/0/10	Disable	Disable	---

All Apply Back Help

Uruchom program Wireshark



Włącz odpowiedni interfejs tutaj **NIC1**



Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\user>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=64

Reply from 192.168.10.1: bytes=32 time<1ms TTL=64

Reply from 192.168.10.1: bytes=32 time<1ms TTL=64

Reply from 192.168.10.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.10.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\user>ping 192.168.10.240

Pinging 192.168.10.240 with 32 bytes of data:

Reply from 192.168.10.240: bytes=32 time<1ms TTL=255

Reply from 192.168.10.240: bytes=32 time<1ms TTL=255

Reply from 192.168.10.240: bytes=32 time<1ms TTL=255

Reply from 192.168.10.240: bytes=32 time<1ms TTL=255

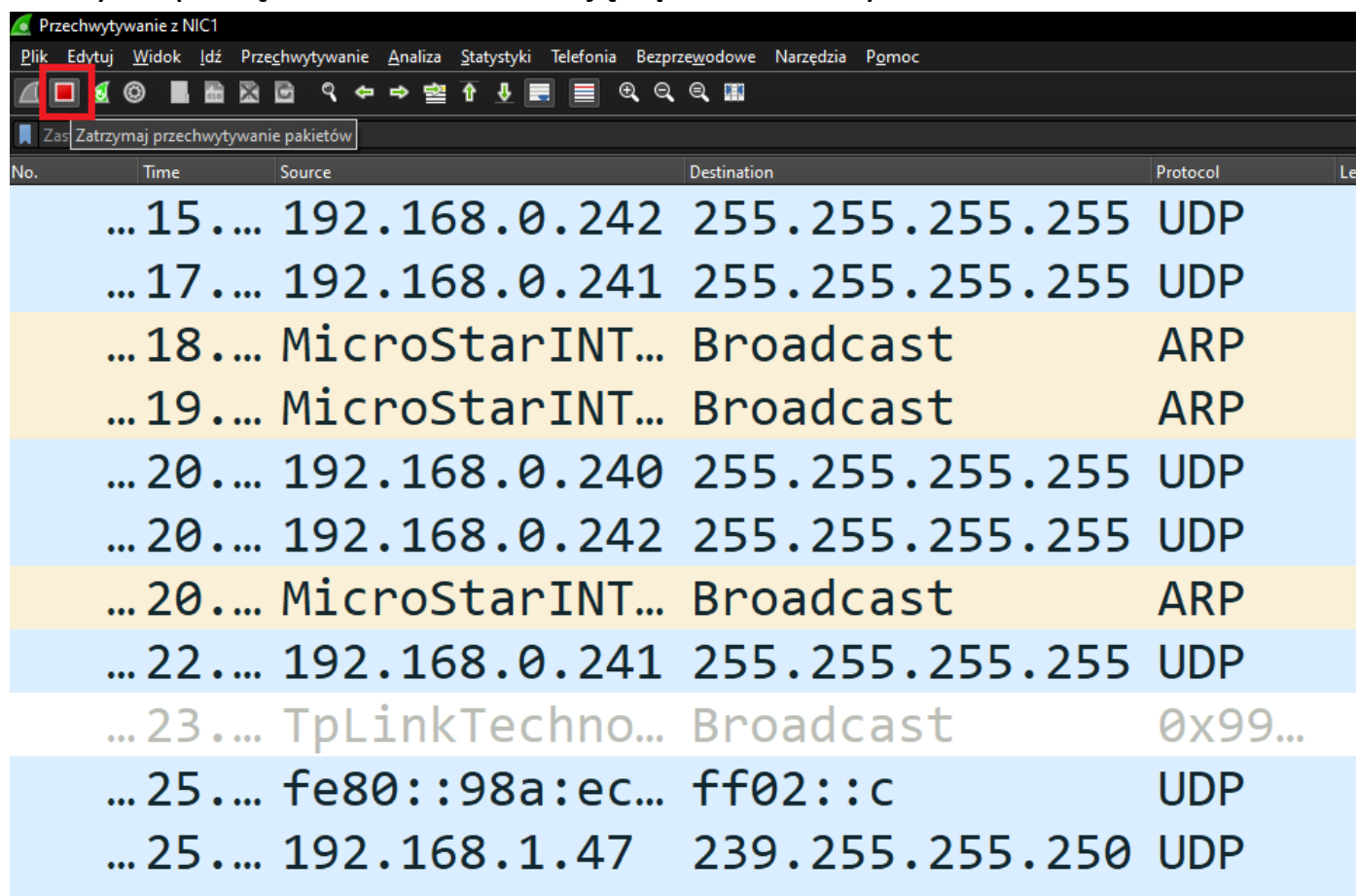
Ping statistics for 192.168.10.240:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

Zatrzyma pracę Wireshark –a klikając **lpm** czerwony kwadrat

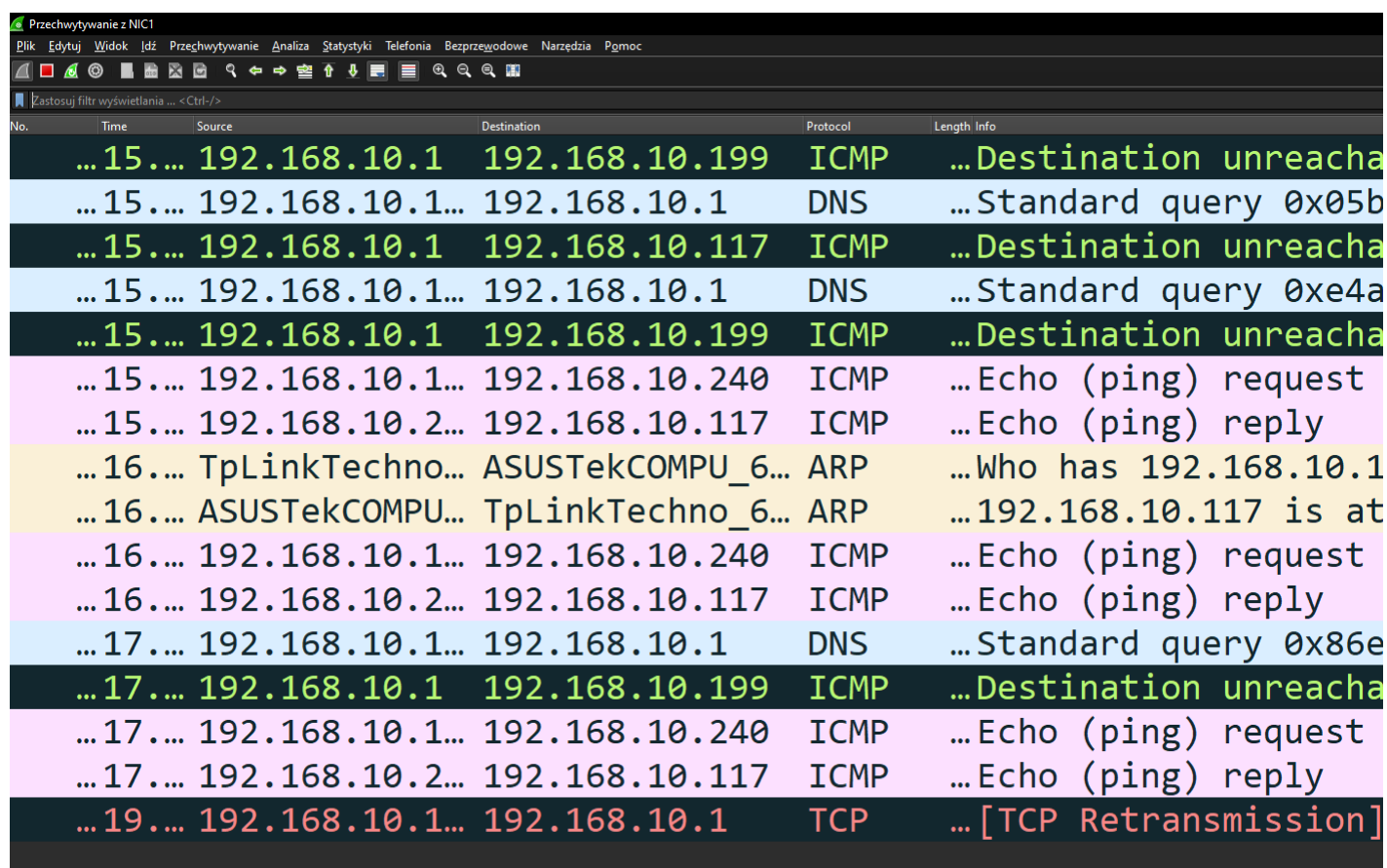


Przechwytywanie z NIC1

Plik Edytuj Widok Idź Przechwytywanie Analiza Statystyki Telefonii Bezprzewodowe Narzędzia Pomoc

Zatrzymaj przechwytywanie pakietów

No.	Time	Source	Destination	Protocol	Length	Info
...15...		192.168.0.242	255.255.255.255	UDP		
...17...		192.168.0.241	255.255.255.255	UDP		
...18...		MicroStarINT...	Broadcast	ARP		
...19...		MicroStarINT...	Broadcast	ARP		
...20...		192.168.0.240	255.255.255.255	UDP		
...20...		192.168.0.242	255.255.255.255	UDP		
...20...		MicroStarINT...	Broadcast	ARP		
...22...		192.168.0.241	255.255.255.255	UDP		
...23...		TpLinkTechno...	Broadcast	0x99...		
...25...		fe80::98a:ec...	ff02::c	UDP		
...25...		192.168.1.47	239.255.255.250	UDP		



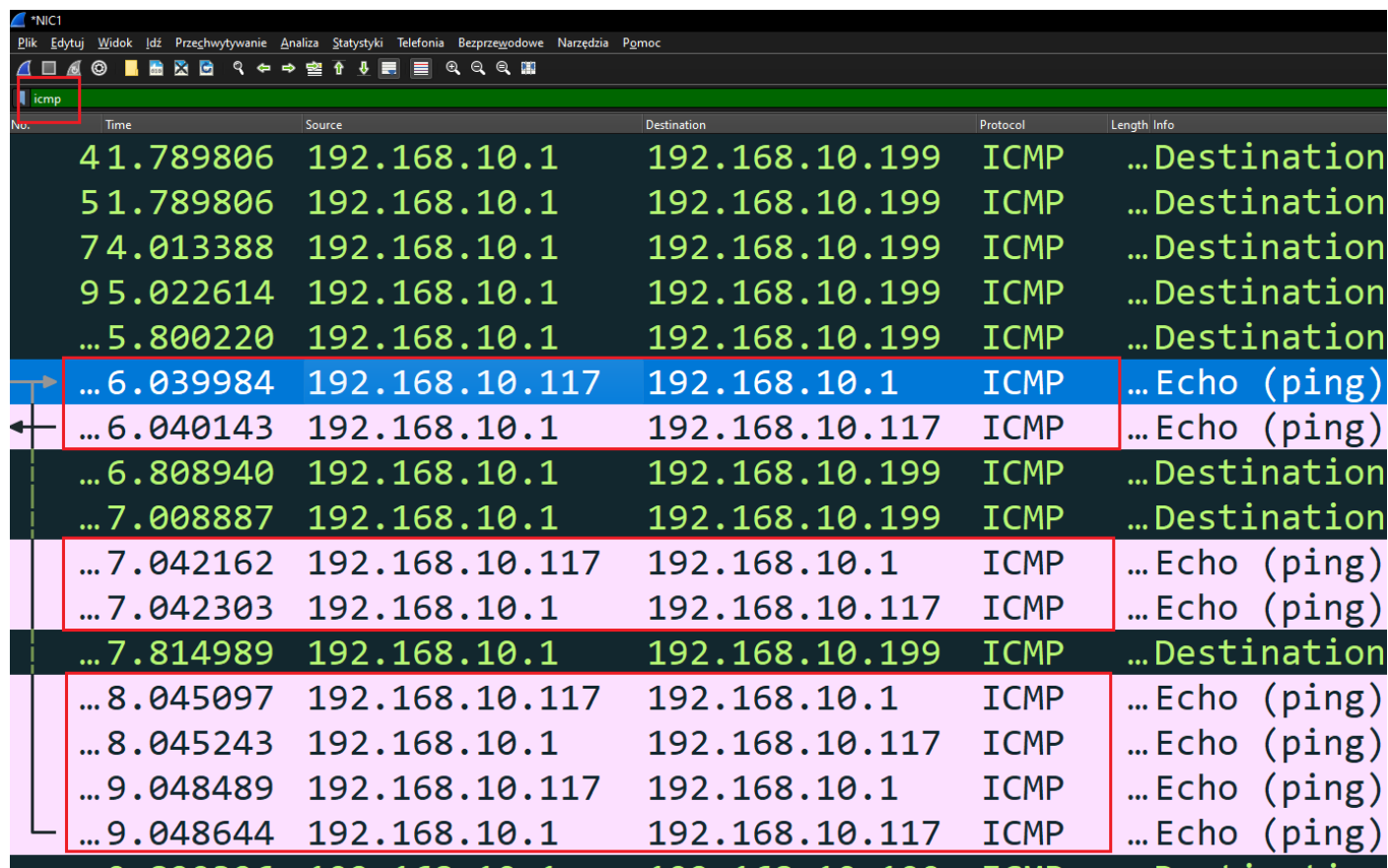
Przechwytywanie z NIC1

Plik Edytuj Widok Idź Przechwytywanie Analiza Statystyki Telefonii Bezprzewodowe Narzędzia Pomoc

Zastosuj filtr wyświetlania ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
...15...		192.168.10.1	192.168.10.199	ICMP		...Destination unreachable
...15...		192.168.10.1...	192.168.10.1	DNS		...Standard query 0x05b
...15...		192.168.10.1	192.168.10.117	ICMP		...Destination unreachable
...15...		192.168.10.1...	192.168.10.1	DNS		...Standard query 0xe4a
...15...		192.168.10.1	192.168.10.199	ICMP		...Destination unreachable
...15...		192.168.10.1...	192.168.10.240	ICMP		...Echo (ping) request
...15...		192.168.10.2...	192.168.10.117	ICMP		...Echo (ping) reply
...16...		TpLinkTechno...	ASUSTekCOMPU_6...	ARP		...Who has 192.168.10.1
...16...		ASUSTekCOMPU...	TpLinkTechno_6...	ARP		...192.168.10.117 is at
...16...		192.168.10.1...	192.168.10.240	ICMP		...Echo (ping) request
...16...		192.168.10.2...	192.168.10.117	ICMP		...Echo (ping) reply
...17...		192.168.10.1...	192.168.10.1	DNS		...Standard query 0x86e
...17...		192.168.10.1	192.168.10.199	ICMP		...Destination unreachable
...17...		192.168.10.1...	192.168.10.240	ICMP		...Echo (ping) request
...17...		192.168.10.2...	192.168.10.117	ICMP		...Echo (ping) reply
...19...		192.168.10.1...	192.168.10.1	TCP		...[TCP Retransmission]

W pasku wpisz nazwę protokołu diagnozującego: **icmp**



No.	Time	Source	Destination	Protocol	Length Info
41	789806	192.168.10.1	192.168.10.199	ICMP	...Destination
51	789806	192.168.10.1	192.168.10.199	ICMP	...Destination
74	013388	192.168.10.1	192.168.10.199	ICMP	...Destination
95	022614	192.168.10.1	192.168.10.199	ICMP	...Destination
...	5.800220	192.168.10.1	192.168.10.199	ICMP	...Destination
...	6.039984	192.168.10.117	192.168.10.1	ICMP	...Echo (ping)
...	6.040143	192.168.10.1	192.168.10.117	ICMP	...Echo (ping)
...	6.808940	192.168.10.1	192.168.10.199	ICMP	...Destination
...	7.008887	192.168.10.1	192.168.10.199	ICMP	...Destination
...	7.042162	192.168.10.117	192.168.10.1	ICMP	...Echo (ping)
...	7.042303	192.168.10.1	192.168.10.117	ICMP	...Echo (ping)
...	7.814989	192.168.10.1	192.168.10.199	ICMP	...Destination
...	8.045097	192.168.10.117	192.168.10.1	ICMP	...Echo (ping)
...	8.045243	192.168.10.1	192.168.10.117	ICMP	...Echo (ping)
...	9.048489	192.168.10.117	192.168.10.1	ICMP	...Echo (ping)
...	9.048644	192.168.10.1	192.168.10.117	ICMP	...Echo (ping)

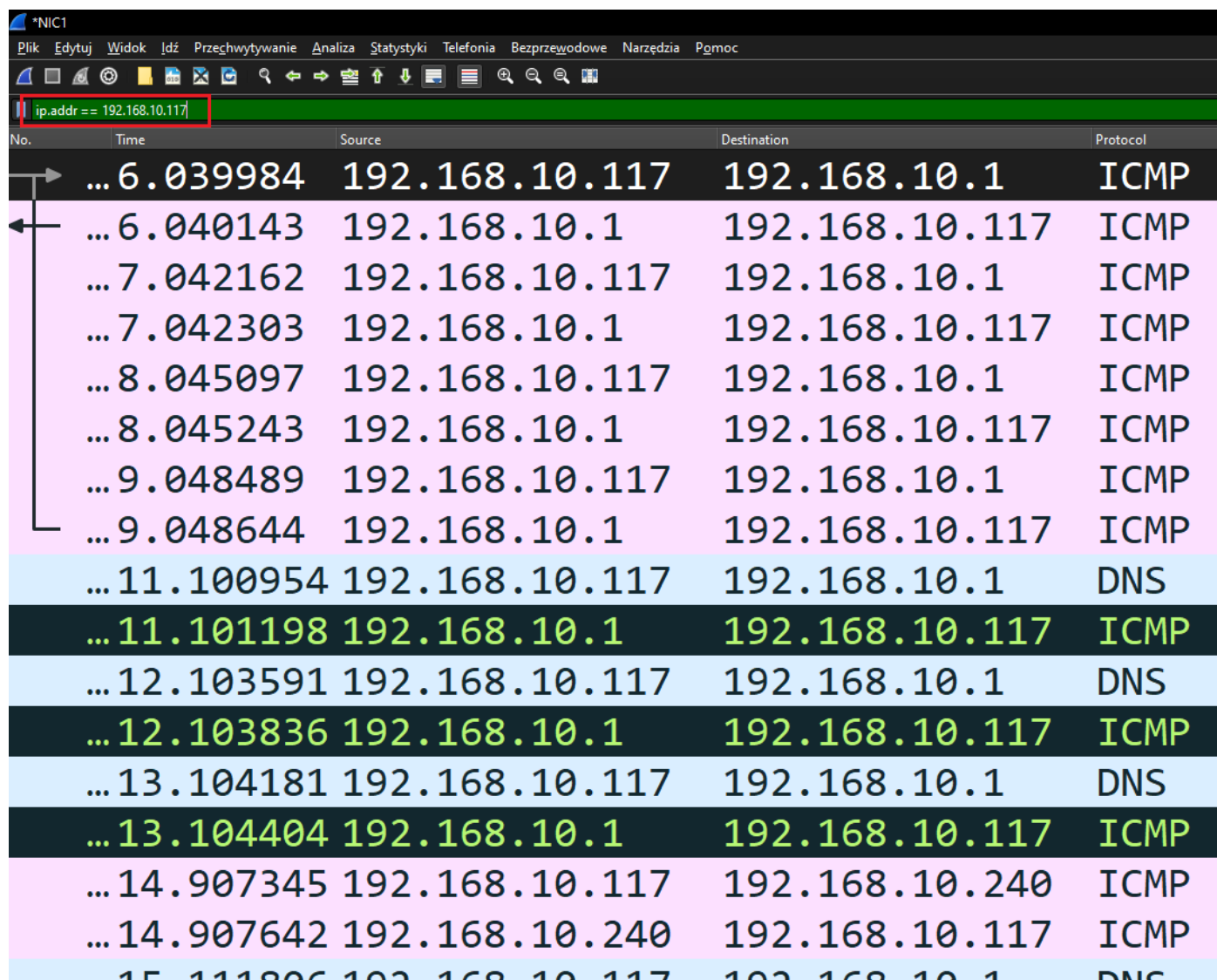
Z powyższego obrazka wynika, że ruch sieciowy z **PCKlienta** został przechwycony, o czym świadczy adres **IPv4 192.168.10.117**.

Filtrowanie pakietów po adresie IPv4. Kliknij na niebieską flagę znajdującą się pod płetwą rekina w lewym górnym rogu.

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes 'Plik', 'Edytuj', 'Widok', 'Idź', 'Przechwytywanie', 'Analiza', 'Statystyki', 'Telefonia', 'Bezprzewodowe', 'Narzędzia', and 'Pomoc'. Below the menu is a toolbar with various icons. A red rectangle highlights a blue flag icon in the toolbar, which is used to apply filters. A context menu is open, displaying various filter options. The option 'IPv4 address 192.0.2.1: ip.addr == 192.0.2.1' is highlighted with a blue background and a red border. The background of the interface shows a list of network packets with columns for time, length, protocol, and IP addresses.

Time	Length	Protocol	Source	Destination
...	6.808561	192.168.10.199	192.168.10.1	192.168.10.1
...	6.808940	192.168.10.1	192.168.10.1	192.168.10.1
...	7.008596	192.168.10.199	192.168.10.199	104.154.0.0
...	7.008887	192.168.10.1	192.168.10.1	192.168.10.1

Wpisz adres IPv4 **PCKlienta** w zielonym pasku



The image shows a Wireshark packet capture window for interface *NIC1. The filter bar at the top contains the expression `ip.addr == 192.168.10.117`. The packet list below shows a series of ICMP Echo (ping) requests and responses, as well as DNS queries. A bracket on the left side of the packet list groups packets 6 through 9, which are all ICMP Echo requests from 192.168.10.117 to 192.168.10.1.

No.	Time	Source	Destination	Protocol
...	6.039984	192.168.10.117	192.168.10.1	ICMP
...	6.040143	192.168.10.1	192.168.10.117	ICMP
...	7.042162	192.168.10.117	192.168.10.1	ICMP
...	7.042303	192.168.10.1	192.168.10.117	ICMP
...	8.045097	192.168.10.117	192.168.10.1	ICMP
...	8.045243	192.168.10.1	192.168.10.117	ICMP
...	9.048489	192.168.10.117	192.168.10.1	ICMP
...	9.048644	192.168.10.1	192.168.10.117	ICMP
...	11.100954	192.168.10.117	192.168.10.1	DNS
...	11.101198	192.168.10.1	192.168.10.117	ICMP
...	12.103591	192.168.10.117	192.168.10.1	DNS
...	12.103836	192.168.10.1	192.168.10.117	ICMP
...	13.104181	192.168.10.117	192.168.10.1	DNS
...	13.104404	192.168.10.1	192.168.10.117	ICMP
...	14.907345	192.168.10.117	192.168.10.240	ICMP
...	14.907642	192.168.10.240	192.168.10.117	ICMP
...	15.111806	192.168.10.117	192.168.10.1	DNS

5. Za pomocą narzędzia administratorskiego cmd zwolnij IP na karcie sieciowej PC-client. Następnie używając odpowiedniego polecenia, niech serwer DHCP ponownie przypisze adres IP dla karty sieciowej PC-clienta. Przechwyć za pomocą programu Wireshark powyższy cztero etapowy proces przypisania adresu IP z DHCP dla karty sieciowej PC-clienta.

Włącz program Wireshark na **PCAdminie**

Zwolnij IPv4 na interfejsie **NIC PCKlienta**

```
C:\Users\user>ipconfig /release NIC
```

Windows IP Configuration

Ethernet adapter NIC:

brak IPv4

Connection-specific DNS Suffix . :

Link-local IPv6 Address : fe80::a4df:ecc5:d4e6:ffd8%13

Default Gateway :

Ethernet adapter VirtualBox Host-Only Network:

Connection-specific DNS Suffix . :

Link-local IPv6 Address : fe80::b14f:29bb:a731:5bf4%6

IPv4 Address. : 192.168.56.1

Subnet Mask : 255.255.255.0

Default Gateway :

Wireless LAN adapter Wi-Fi:

Media State : Media disconnected

Connection-specific DNS Suffix . :

Wireless LAN adapter Połączenie lokalne* 9:

Media State : Media disconnected

Connection-specific DNS Suffix . :

Teraz wpisz polecenie przypisania adresu IPv4 z DHCP dla **PCklienta**

```
C:\Users\user>ipconfig /renew NIC

Windows IP Configuration

Ethernet adapter NIC:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::a4df:ecc5:d4e6:ffd8%13
    IPv4 Address. . . . . : 192.168.10.117
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::b14f:29bb:a731:5bf4%6
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Wi-Fi:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Połączenie lokalne* 9:
```

*NIC1					
Plik Edytuj Widok Idź Przechwytywanie Analiza Statystyki Telefonia Bezprzewodowe Narzędzia Pomoc					
dhcpl					
No.	Time	Source	Destination	Protocol	Length Info
31	3.498181	0.0.0.0	255.255.255.255	DHCP	3... DHCP Discover
32	3.498181	0.0.0.0	255.255.255.255	DHCP	3... DHCP Discover
37	4.500444	192.168.10.1	192.168.10.117	DHCP	5... DHCP Offer
38	4.500771	0.0.0.0	255.255.255.255	DHCP	3... DHCP Request
39	4.500771	0.0.0.0	255.255.255.255	DHCP	3... DHCP Request
40	4.501326	192.168.10.1	192.168.10.117	DHCP	5... DHCP ACK

6. Dla portu 4 ustaw max liczbę zapamiętywanych adresów mac na wartość 19.

Ustaw w tabeli tryb dynamicznego zapamiętywania adresów mac. Status: drop.

Z instrukcji przełącznika

Port Config

Port Mirror

Port Security

Port Isolation

Loopback Detection

Port Security

Select	Port	Max Learned MAC	Learned Num	Learn Mode	Status
☐				Dynamic ▾	Disable ▾
☐	1	64	0	Dynamic	Disable
☐	2	64	0	Dynamic	Disable
☐	3	64	0	Static	Disable
☐	4	64	0	Permanent	Disable
☐	5	64	0	Dynamic	Disable
☐	6	64	0	Dynamic	Disable
☐	7	64	0	Dynamic	Disable
☐	8	64	0	Dynamic	Disable
☐	9	64	0	Dynamic	Disable
☐	10	64	0	Dynamic	Disable
☐	11	64	0	Dynamic	Disable
☐	12	64	0	Dynamic	Disable

Apply

Help

Learn Mode

Select the learn mode of the MAC addresses on the port. Three modes are provided:

Dynamic: The switch will delete the MAC addresses that are not used or updated within the aging time. It is the default setting.

Static: The learned MAC addresses are out of the influence of the aging time and can only be deleted manually. The learned entries will be cleared after the switch is rebooted.

Permanent: The learned MAC addresses are out of the influence of the aging time and can only be deleted manually. The learned entries will be saved even the switch is rebooted.

Tryb nauki

Wybierz tryb nauki adresów MAC na porcie. Dostępne są trzy tryby:

Dynamiczny: Przełącznik usunie adresy MAC, które nie są używane lub aktualizowane w czasie starzenia. Jest to ustawienie domyślne.

Statyczny: Wyuczone adresy MAC nie podlegają wpływowi czasu starzenia i można je usunąć tylko ręcznie. Wyuczone wpisy zostaną wyczyszczone po ponownym uruchomieniu przełącznika.

Stały: Wyuczone adresy MAC nie podlegają wpływowi czasu starzenia i można je usunąć tylko ręcznie. Wyuczone wpisy zostaną zapisane nawet po ponownym uruchomieniu przełącznika.

Port Security

UNIT: 1

Select	Port	Max Learned MAC	Learned Num	Learn Mode	Status
☐				v	v
☐	1/0/1	64	0	Dynamic	
☐	1/0/2	64	0	Dynamic	
☐	1/0/3	64	0	Dynamic	
☐	1/0/4	64	0	Dynamic	
☐	1/0/5	64	0	Dynamic	
☐	1/0/6	64	0	Dynamic	Disable
☐	1/0/7	64	0	Dynamic	Disable
☐	1/0/8	64	0	Dynamic	Disable
☐	1/0/9	64	0	Dynamic	Disable
☐	1/0/10	64	0	Dynamic	Disable
☐	1/0/11	64	0	Dynamic	Disable
☐	1/0/12	64	0	Dynamic	Disable
☐	1/0/13	64	0	Dynamic	Disable
☐	1/0/14	64	0	Dynamic	Disable
☐	1/0/15	64	0	Dynamic	Disable

Apply

Help

Note:

The maximum number of MAC addresses learned from individual port can be set to 64.

Status

Select the status of Port Security. Three kinds of status can be selected:

Drop: When the number of learned MAC addresses reaches the limit, the port will stop learning and discard the packets with the MAC addresses that have not been learned.

Forward: When the number of learned MAC addresses reaches the limit, the port will stop learning but send the packets with the MAC addresses that have not been learned.

Disable: The number limit on the port is not effective, and the switch follows the original forwarding rules. It is the default setting.



557 / 5 000



Status

Wybierz status Port Security. Można wybrać trzy rodzaje statusu:

Odrzuć: Gdy liczba nauczonych adresów MAC osiągnie limit, port przestanie się uczyć i odrzuci pakiety z adresami MAC, których nie nauczono.

Przełącz: Gdy liczba nauczonych adresów MAC osiągnie limit, port przestanie się uczyć, ale wyśle pakiety z adresami MAC, których nie nauczono.

Wyłącz: Limit liczby na porcie nie obowiązuje, a przełącznik stosuje się do oryginalnych reguł przekazywania. Jest to ustawienie domyślne.



Port Config

Port Mirror

Port Security

Port Isolation

Loopback Detection

Port Security

UNIT: 1

Select	Port	Max Learned MAC	Learned Num	Learn Mode	Status
☐		19			Drop
☐	1/0/1	64	0	Dynamic	Disable
☐	1/0/2	64	0	Dynamic	Disable
☐	1/0/3	64	0	Dynamic	Disable
☒	1/0/4	64	0	Dynamic	Disable
☐	1/0/5	64	0	Dynamic	Disable
☐	1/0/6	64	0	Dynamic	Disable
☐	1/0/7	64	0	Dynamic	Disable
☐	1/0/8	64	0	Dynamic	Disable
☐	1/0/9	64	0	Dynamic	Disable
☐	1/0/10	64	0	Dynamic	Disable

Apply

Help

Port Config

Port Mirror

Port Security

Port Isolation

Loopback Detection

Operation succeeded.

Port Security

UNIT: 1

Select	Port	Max Learned MAC	Learned Num	Learn Mode	Status
☐					
☐	1/0/1	64	0	Dynamic	Disable
☐	1/0/2	64	0	Dynamic	Disable
☐	1/0/3	64	0	Dynamic	Disable
☐	1/0/4	19	0	Dynamic	Drop
☐	1/0/5	64	0	Dynamic	Disable
☐	1/0/6	64	0	Dynamic	Disable
☐	1/0/7	64	0	Dynamic	Disable
☐	1/0/8	64	0	Dynamic	Disable
☐	1/0/9	64	0	Dynamic	Disable
☐	1/0/10	64	0	Dynamic	Disable

Apply

Help

6. Odizoluj PC-clienta od Internetu.

Port Config

Port Mirror

Port Security

Port Isolation

Loopback Detection

Port Isolation List

UNIT: 1 LAGS

Port	LAG	Forward Portlist
1/0/1	---	1/0/1-10,LAG1-14
1/0/2	---	1/0/1-10,LAG1-14
1/0/3	---	1/0/1-10,LAG1-14
1/0/4	---	1/0/1-10,LAG1-14
1/0/5	---	1/0/1-10,LAG1-14
1/0/6	---	1/0/1-10,LAG1-14
1/0/7	---	1/0/1-10,LAG1-14
1/0/8	---	1/0/1-10,LAG1-14
1/0/9	---	1/0/1-10,LAG1-14
1/0/10	---	1/0/1-10,LAG1-14

Edit

Help

Port Config

Port Mirror

Port Security

Port Isolation

Loopback Detection

Port Isolation Config

Port:

UNIT: 1 LAGS

1

2

3

4

5

6

7

8

9

10

PClient

All

Clear

Help

Forward Portlist: lista przepuszczania ruchu sieciowego

UNIT: 1 LAGS

1

2

3

4

5

6

7

8

9

10

PCAdmin(server)

All

Clear

Apply

Back

Unselected Port(s)

Selected Port(s)

Not Available for Selection

Efekt po izolacji na porcie 1

Port Config Port Mirror Port Security Port Isolation Loopback Detection

Operation succeeded.

Port Isolation List

UNIT: 1 LAGS

Port	LAG	Forward Portlist
1/0/1	---	1/0/2
1/0/2	---	1/0/1-10,LAG1-14
1/0/3	---	1/0/1-10,LAG1-14
1/0/4	---	1/0/1-10,LAG1-14
1/0/5	---	1/0/1-10,LAG1-14
1/0/6	---	1/0/1-10,LAG1-14
1/0/7	---	1/0/1-10,LAG1-14
1/0/8	---	1/0/1-10,LAG1-14
1/0/9	---	1/0/1-10,LAG1-14
1/0/10	---	1/0/1-10,LAG1-14

Edit Help

Zdejmnowanie izolacji dla portu 1

Port Config Port Mirror Port Security Port Isolation Loopback Detection

Port Isolation Config

Port:

UNIT: 1 LAGS

1 2 3 4 5 6 7 8 9 10

All Clear Help

Forward Portlist:

UNIT: 1 LAGS

1 2 3 4 5 6 7 8 9 10

All Clear Apply Back

 Unselected Port(s)  Selected Port(s)  Not Available for Selection

Port Config

Port Mirror

Port Security

Port Isolation

Loopback Detection

Operation succeeded.

Port Isolation List

UNIT: 1 LAGS

Port	LAG	Forward Portlist
1/0/1	---	1/0/1-10,LAG1-14
1/0/2	---	1/0/1-10,LAG1-14
1/0/3	---	1/0/1-10,LAG1-14

8. Ustaw wykrywanie sprzężenia zwrotnego (loopback detection)

na wszystkich portach przełączników 1 i 2.

Interwał detekcji ustaw na 35,

a automatyczne przywracanie pracy portu na 4

lub wartość minimalną dla przełącznika 28TS.

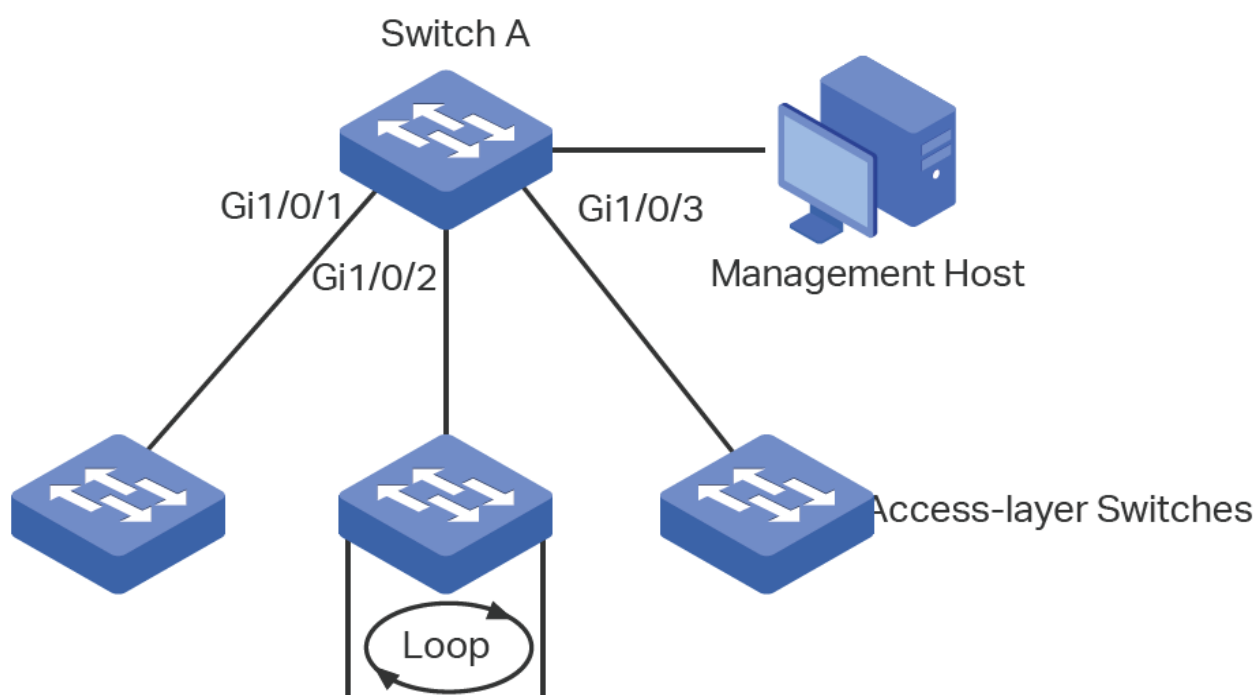
W tabeli Port config w opcji Operation Mode tryb Port based.

W opcji Recovery Mode ustaw tryb auto.

Z dokumentacji przełącznika – objaśnienie

Loopback Detection chroni przełącznik przed krążeniem danych w zapętleniu na urządzeniu.

Jak pokazuje poniższy obrazek problem z zapętleniem powstaje, gdy wepnie się dwa końce kabla do portów tego samego przełącznika.



Global config

Loopback Detection Status:
 ☐ Enable
 ☒ Disable

Detection Interval:

 seconds(1-1000)

Automatic Recovery Time:

 detection times(1-100)

Web Refresh Status:
 ☐ Enable
 ☒ Disable

Web Refresh Interval:

 seconds(3-100)

Apply

Port Config

UNIT: 1 LAGS

Select	Port	Status	Operation mode	Recovery mode	Loop status	Block status	LAG
☐		v	v	v			
☐	1/0/1	Disable	Alert	Auto	---	---	---
☐	1/0/2	Disable	Alert	Auto	---	---	---
☐	1/0/3	Disable	Alert	Auto	---	---	---
☐	1/0/4	Disable	Alert	Auto	---	---	---
☐	1/0/5	Disable	Alert	Auto	---	---	---
☐	1/0/6	Disable	Alert	Auto	---	---	---
☐	1/0/7	Disable	Alert	Auto	---	---	---
☐	1/0/8	Disable	Alert	Auto	---	---	---
☐	1/0/9	Disable	Alert	Auto	---	---	---
☐	1/0/10	Disable	Alert	Auto	---	---	---

All

Apply

Recover

Help

Detection Interval

Set the interval of sending loopback detection packets.

The valid values are from 1 to 1000 seconds and the default value is 30 seconds.



Interwał wykrywania

Ustaw interwał wysyłania pakietów wykrywania pętli zwrotnej.

Dopuszczalne wartości to od 1 do 1000 sekund, a wartość domyślna to 30 sekund.

Automatic Recovery Time

Set the recovery time globally, after which the blocked port in Auto Recovery mode can automatically recover to normal status.

It should be integral times of detection interval.
The valid values are from 1 to 100, and the default value is 3.

Web Refresh Status

With this option enabled, the switch refreshes the web timely. By default, it is disabled.

Web Refresh Interval

If you enabled web refresh, set the refresh interval between 3 and 100 seconds.
The default value is 6 seconds.

In the Port Config section, select one or multiple ports for configuration. Then set the parameters and click Apply.

Status Enable loopback detection for the port.

Operation Mode

Select the operation mode when a loopback is detected on the port:

Alert: The switch will display alerts. It is the default setting.

Port Based: In addition to displaying alerts, the switch will block the port on which the loop is detected.

×

Czas automatycznego odzyskiwania

Ustaw czas odzyskiwania globalnie, po którym zablokowany port w trybie automatycznego odzyskiwania może automatycznie powrócić do normalnego stanu.

Powinien to być całkowity czas interwału wykrywania. Dopuszczalne wartości to od 1 do 100, a wartość domyślna to 3.

×

Status odświeżania sieci

Po włączeniu tej opcji przełącznik odświeża sieć na bieżąco. Domyślnie jest wyłączona.

×

Interwał odświeżania sieci

Jeśli włączono odświeżanie sieci, ustaw interwał odświeżania między 3 a 100 sekundami.
Wartość domyślna to 6 sekund.

×

W sekcji Port Config wybierz jeden lub wiele portów do konfiguracji. Następnie ustaw parametry i kliknij Zastosuj.

Status Włącz wykrywanie pętli zwrotnej dla portu.

Tryb działania

Wybierz tryb działania, gdy pętla zwrotna zostanie wykryta na porcie:

Alert: Przełącznik będzie wyświetlał alerty. Jest to ustawienie domyślne.

Port Based: Oprócz wyświetlania alertów, przełącznik zablokuje port, na którym wykryto pętlę.

×

Tryb odzyskiwania

Jeśli wybierzesz Port Based jako tryb działania, musisz również skonfigurować tryb odzyskiwania dla zablokowanego portu:

Auto: Zablokowany port automatycznie powróci do normalnego stanu po upływie czasu automatycznego odzyskiwania. Jest to ustawienie domyślne.

Manual: Musisz ręcznie zwolnić zablokowany port. Kliknij przycisk Recovery, aby zwolnić wybrany port.

Recovery Mode

If you select Port Based as the operation mode, you also need to configure the recovery mode for the blocked port:

Auto: The blocked port will automatically recover to normal status after the automatic recovery time. It is the default setting.

Manual: You need to manually release the blocked port. Click the Recovery button to release the selected port.

Na przełączniku 2 dokonaj właściwych ustawień w sekcji **Global config** i **Port Config**

Port Config

Port Mirror

Port Security

Port Isolation

Loopback Detection

Global config

Loopback Detection Status:

☒

Enable

☐

Disable

Detection Interval:

35

seconds(1-1000)

Automatic Recovery Time:

4

detection times(1-100)

Web Refresh Status:

☐

Enable

☒

Disable

Web Refresh Interval:

6

seconds(3-100)

Apply

Port Config

UNIT: 1 LAGS

Select	Port	Status	Operation mode	Recovery mode	Loop status	Block status	LAG
☒		Enable					
☒	1/0/1	Disable	Alert	Auto	---	---	---
☒	1/0/2	Disable	Alert	Auto	---	---	---
☒	1/0/3	Enable	Alert	Auto	---	---	---
☒	1/0/4	Disable	Alert	Auto	---	---	---
☒	1/0/5	Disable	Alert	Auto	---	---	---
☒	1/0/6	Disable	Alert	Auto	---	---	---
☒	1/0/7	Disable	Alert	Auto	---	---	---
☒	1/0/8	Disable	Alert	Auto	---	---	---
☒	1/0/9	Disable	Alert	Auto	---	---	---
☒	1/0/10	Disable	Alert	Auto	---	---	---

All

Apply

Recover

Help

Port Config

UNIT: 1 LAGS

Select	Port	Status	Operation mode	Recovery mode	Loop status
☒		▼	▼	▼	
☒	1/0/1	Enable	Alert	Auto	---
☒	1/0/2	Enable	Alert	Auto	---
☒	1/0/3	Enable	Port based	Auto	---
☒	1/0/4	Enable	Alert	Auto	---
☒	1/0/5	Enable	Alert	Auto	---
☒	1/0/6	Enable	Alert	Auto	---
☒	1/0/7	Enable	Alert	Auto	---
☒	1/0/8	Enable	Alert	Auto	---
☒	1/0/9	Enable	Alert	Auto	---
☒	1/0/10	Enable	Alert	Auto	---

All

Apply

Recover

Help

Port Config

UNIT: 1 LAGS

Select	Port	Status	Operation mode	Recovery mode	Loop status
☐		▼	▼	▼	
☐	1/0/1	Enable	Port based	Auto	---
☐	1/0/2	Enable	Port based	Auto	---
☐	1/0/3	Enable	Port based	Auto	---
☐	1/0/4	Enable	Port based	Auto	---
☐	1/0/5	Enable	Port based	Auto	---
☐	1/0/6	Enable	Port based	Auto	---
☐	1/0/7	Enable	Port based	Auto	---
☐	1/0/8	Enable	Port based	Auto	---
☐	1/0/9	Enable	Port based	Auto	---
☐	1/0/10	Enable	Port based	Auto	---

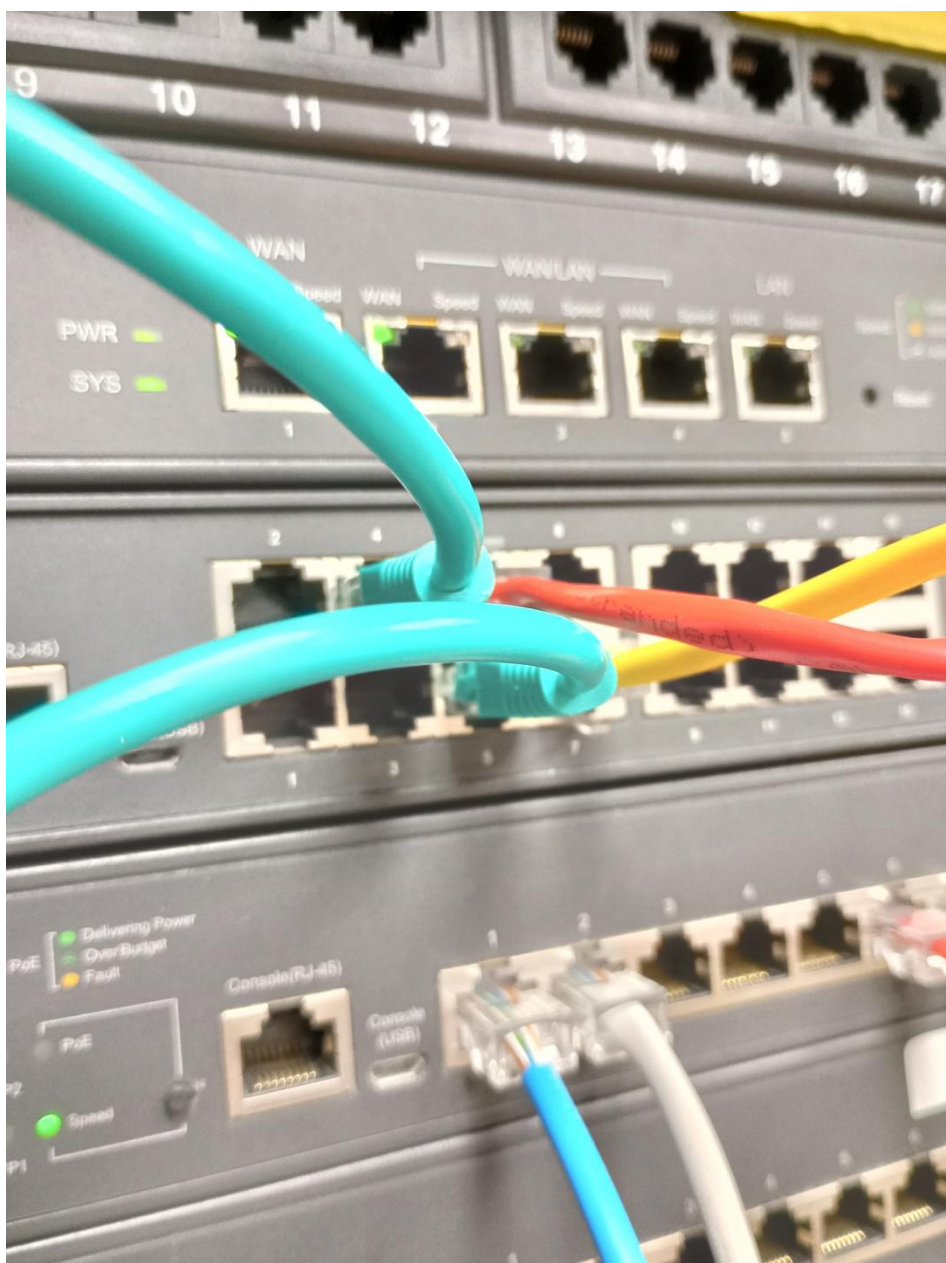
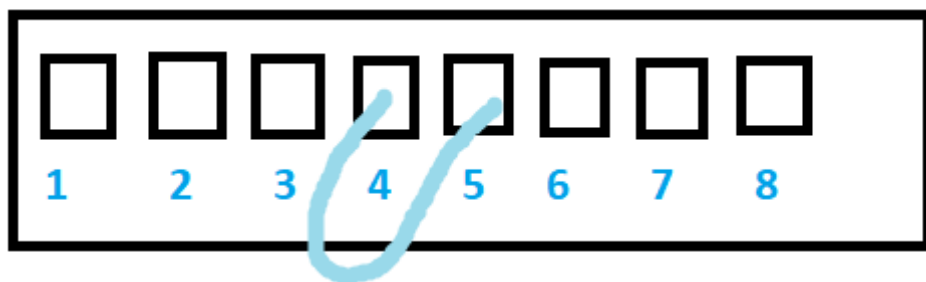
All

Apply

Recover

Help

Na przełączniku 1 dokonaj podobnej konfiguracji, a następnie wepnij nowy kabel do wolnych portów np. 4,5. Przełącznik powinien wyłączyć te porty na krótki czas, broniąc sieć przed flashingiem.



9.Odszukaj drukarkę w sieci.

W tabeli arp **PCAdmin** odszukaj adres mac drukarki.

Następnie odszukaj adres mac drukarki za pomocą tabeli filtrującej adresy mac w przełączniku.

Na **PCAdmin** w CMD wpisz poniższe polecenia

```
C:\Users\user>ping 192.168.10.240

Pinging 192.168.10.240 with 32 bytes of data:
Reply from 192.168.10.240: bytes=32 time<1ms TTL=255
Reply from 192.168.10.240: bytes=32 time<1ms TTL=255
Reply from 192.168.10.240: bytes=32 time<1ms TTL=255
Reply from 192.168.10.240: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.240:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\Users\user>arp -a
```

```
Interface: 192.168.0.199 --- 0x5
```

Internet Address	Physical Address	Type
192.168.0.255	ff-ff-ff-ff-ff-ff	static
192.168.10.1	98-da-c4-64-61-86	dynamic
192.168.10.221	ac-84-c6-46-24-50	dynamic
192.168.10.226	ac-84-c6-46-24-b9	dynamic
192.168.10.228	ac-84-c6-46-24-47	dynamic
192.168.10.240	00-26-73-db-ed-f7	dynamic
224.0.0.2	01-00-5e-00-00-02	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

```
Interface: 192.168.56.1 --- 0x6
```

Internet Address	Physical Address	Type
192.168.56.255	ff-ff-ff-ff-ff-ff	static
224.0.0.2	01-00-5e-00-00-02	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static

Odszukanie adres mac drukarki za pomocą tabeli filtrującej adresy mac w przełączniku

Address Table

Static Address

Dynamic Address

Filtering Address

Mac Notification

Mac Vlan Security

Search Option

☒ MAC Address:

00-26-73-db-ed-f7

(Format: 00-00-00-00-00-01)

☐ VLAN ID:

(1-4094)

☐ Type:

☒ All

☐ Static

☐ Dynamic

☐ Filter

Search

Help

Port:

UNIT: 1 LAGS

12345678

910

Address Table

Static Address

Dynamic Address

Filtering Address

Mac Notification

Mac Vlan Security

Search Option

☒ MAC Address:

00-26-73-db-ed-f7

(Format: 00-00-00-00-00-01)

☐ VLAN ID:

(1-4094)

☐ Type:

☒ All

☐ Static

☐ Dynamic

☐ Filter

Search

Help

Port:

UNIT: 1 LAGS

12345678

910

Unselected Port(s)

Selected Port(s)

Not Available for Selection

Address Table				
UNIT: 1				
MAC Address	VLAN ID	Port	Type	Aging Status
00-26-73-DB-ED-F7	1	1/0/6	Dynamic	Aging

10. Ustaw statyczne zapamiętanie adresu mac drukarki na **Access Switch 1**.

Address Table

Static Address

Dynamic Address

Filtering Address

Mac Notification

Mac Vlan Security

Create Static Address

MAC Address:

00-26-73-db-ed-f7

(Format: 00-00-00-00-00-01)

VLAN ID:

1

(1-4094)

Port:

UNIT: 1

1

2

3

4

5

6

7

8

9

10

Access Switch 1

 Unselected Port(s)

 Selected Port(s)

 Not Available for Selection

Search Option

Search Option:

All

Search

Static Address Table

UNIT: 1

Select	MAC Address	VLAN ID	Port	Type	Aging Status
☐					
☐	00-26-73-DB-ED-F7	1	1/0/8	Config static	no-Aging

All

Apply

Delete

Help

11. W cmd sprawdź połączenie z drukarką za pomocą polecenia ping.

Przechwyć pingowanie na drukarę za pomocą programu Wireshark z PC-admina

12. Za pomocą tabeli Filtering Address zabronić pakietom z adresem mac drukarki na forwordowanie w sieci.

Funkcja nie zadziała, gdy izolowany adres mac jest ustawiony statycznie.

Usuń statyczne ustawienie adresu mac drukarki

Address Table

Static Address

Dynamic Address

Filtering Address

Mac Notification

Mac Vlan Security

MAC Address:

(Format: 00-00-00-00-00-01)

VLAN ID:

(1-4094)

Create

Port:

UNIT:

1

1

2

3

4

5

6

7

8

9

10

Unselected Port(s)

Selected Port(s)

Not Available for Selection

Search Option

Search Option:

All

Search

Static Address Table

UNIT:

1

Select	MAC Address	VLAN ID	Port	Type	Aging Status
☐					
☒	00-26-73-DB-ED-F7	1	1/0/8	Config static	no-Aging

All

Apply

Delete

Help

Wpisz adres mac drukarki w polu **MAC Address** i zatwierdź.

Address Table

Static Address

Dynamic Address

Filtering Address

Mac Notification

Mac Vlan Security

Create Filtering Address

MAC Address:

00-26-73-db-ed-f7

(Format: 00-00-00-00-00-01)

VLAN ID:

1

(1-4094)

Create

Search Option

Search Option:

All

Search

Filtering Address Table

Select	MAC Address	VLAN ID	Port	Type	Aging Status
No entry in the table.					

Address Table Static Address Dynamic Address **Filtering Address** Mac Notification Mac Vlan Security

Operation succeeded.

Create Filtering Address

MAC Address: (Format: 00-00-00-00-00-01)

VLAN ID: (1-4094) Create

Search Option

Search Option: All Search

Filtering Address Table

Select	MAC Address	VLAN ID	Port	Type	Aging Status
☐	00-26-73-DB-ED-F7	1	--	Filter	no-Aging

All Delete Help

Sprawdź połączenie z drukarką

```
C:\Users\user>ping 192.168.10.240
```

```
Pinging 192.168.10.240 with 32 bytes of data:  
Reply from 192.168.10.199: Destination host unreachable.  
Reply from 192.168.10.199: Destination host unreachable.  
Reply from 192.168.10.199: Destination host unreachable.  
Reply from 192.168.10.199: Destination host unreachable.  
  
Ping statistics for 192.168.10.240:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Po sprawdzeniu skuteczności działania izolacji adresu mac drukarki, usuń jego wpis w sekcji **Filtering Address Table**.

Address Table

Static Address

Dynamic Address

Filtering Address

Mac Notification

Mac Vlan Security

Create Filtering Address

MAC Address: (Format: 00-00-00-00-00-01)

VLAN ID: (1-4094)

Create

Search Option

Search Option:

All

Search

Filtering Address Table

Select	MAC Address	VLAN ID	Port	Type	Aging Status
☒	00-26-73-DB-ED-F7	1	--	Filter	no-Aging

All

Delete

Help

13. Sprawdź połączenie z drukarką za pomocą polecenia ping w cmd

```
C:\Users\user>ping 192.168.10.240

Pinging 192.168.10.240 with 32 bytes of data:
Reply from 192.168.10.240: bytes=32 time<1ms TTL=255
Reply from 192.168.10.240: bytes=32 time<1ms TTL=255
Reply from 192.168.10.240: bytes=32 time<1ms TTL=255
Reply from 192.168.10.240: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.240:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

3. PRACOWNIA SIECI

KOMPUTEROWYCH - VIRTUAL LAN (VLAN)

3.1 VLAN TEORIA

Ramka tagowana – ramka, która w polu NACZNIK p/Q zawiera wpis dotyczący identyfikatora VLAN np. vlan 10 (patrz budowa ramki ETHERNET) - ruch wyjściowy z portu switch-a lub routera.

```
> Frame 14: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF
v Ethernet II, Src: ASUSTekC_88:ab:7f (ac:9e:17:88:ab:7f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: ASUSTekC_88:ab:7f (ac:9e:17:88:ab:7f)
    Type: QinQ: old non-standard 802.1ad (0x9100)
v 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1
  000. .... = Priority: Best Effort (default) (0)
  ...0 .... = DEI: Ineligible
  .... 0000 0000 0001 = ID: 1
  Type: ARP (0x0806)
  Padding: 00000000000000000000000000000000
  Trailer: 00000000
> Address Resolution Protocol (request)
```

Ramka nie tagowana - ramka, która w polu ZNACZNIK p/Q nie ma wpisu identyfikatora VLAN - ruch wyjściowy z portu switch-a lub routera

```
> Frame 11: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF
v Ethernet II, Src: Tp-LinkT_7f:52:47 (ac:84:c6:7f:52:47), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: Tp-LinkT_7f:52:47 (ac:84:c6:7f:52:47)
    Type: ARP (0x0806)
    Padding: 00000000000000000000000000000000
> Address Resolution Protocol (request)
```

Warunki używania ramek tagowanych i nietagowanych

W normalnym trybie pracy karty sieciowej urządzenia końcowego **nie tagujemy** portu przełącznika, do którego ta stacja jest podłączona.

Stacja – pcklient, serwer, drukarka ...

W niektórych warunkach możemy także nie tagować na portach łączących przełączniki lub router z przełącznikiem.

Jest to zawsze opcja domyślna na zresetowanych urządzeniach sieciowych. Wówczas porty przełącznika lub routera ustawione są w trybie **ACCESS – UNTAG**.

VLAN Members

Port

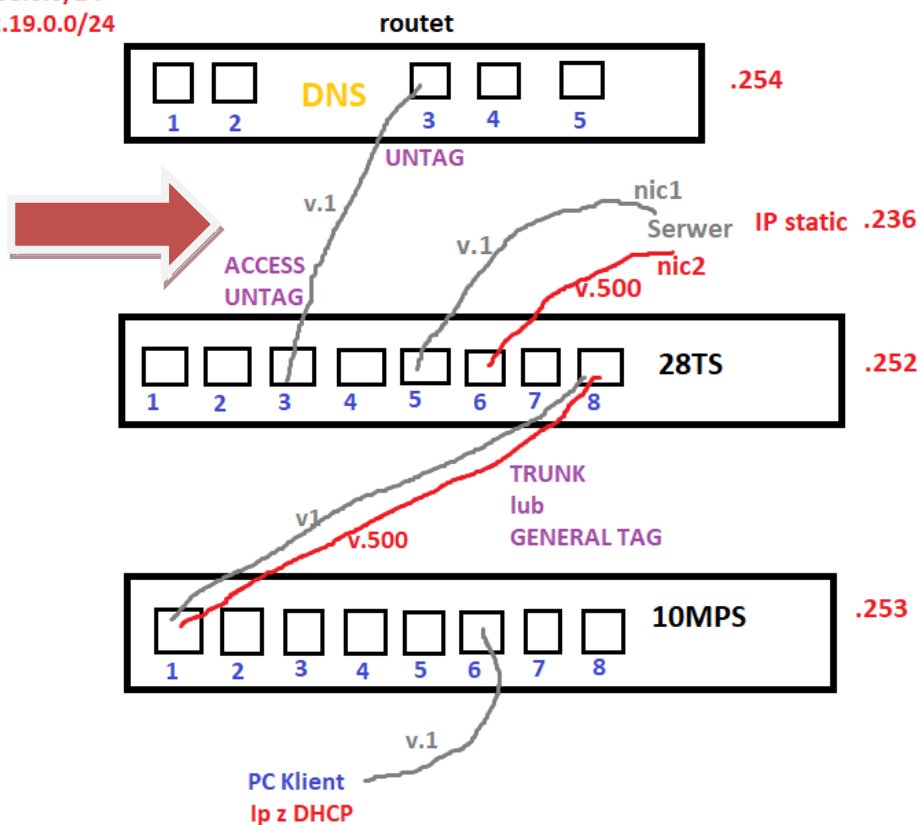
Select	Port	Link Type	Egress Rule	LAG
☐	1	ACCESS	UNTAG	---
☐	2	ACCESS	UNTAG	---
☐	3	ACCESS	UNTAG	---
☐	4	ACCESS	UNTAG	---
☐	5	ACCESS	UNTAG	---
☐	6	ACCESS	UNTAG	---
☐	7	ACCESS	UNTAG	---
☐	8	ACCESS	UNTAG	---
☐	9	ACCESS	UNTAG	---
☐	10	ACCESS	UNTAG	---
☐	11	ACCESS	UNTAG	---
☐	12	ACCESS	UNTAG	---
☐	13	ACCESS	UNTAG	---
☐	14	ACCESS	UNTAG	---

Skrzynka sieciowa zadania: VLAN 500 Management

GR.A

vlan1 -> 192.168.0.0/24

vlan500 -> 172.19.0.0/24



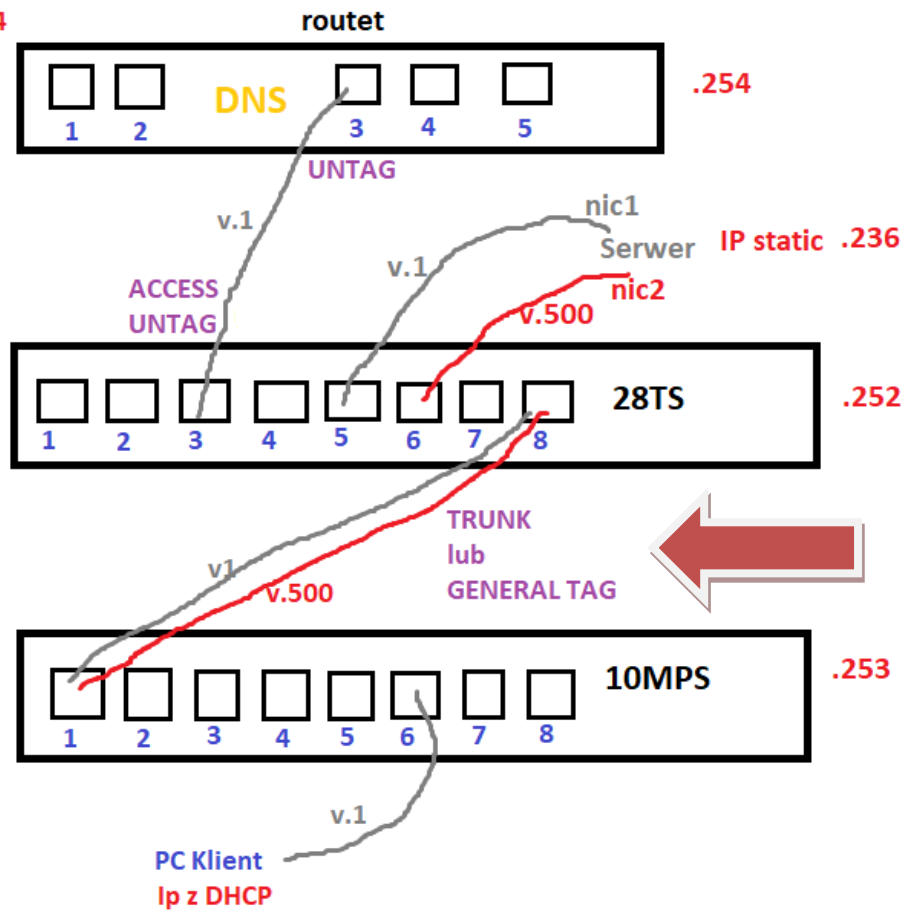
Tagujemy pomiędzy urządzeniami sieciowymi na portach obsługujących wiele vlanów (**TRUNK – TAG, GENERAL –TAG**).

Skrzynka sieciowa zadania: VLAN 500 Management

GR.A

vlan1 -> 192.168.0.0/24

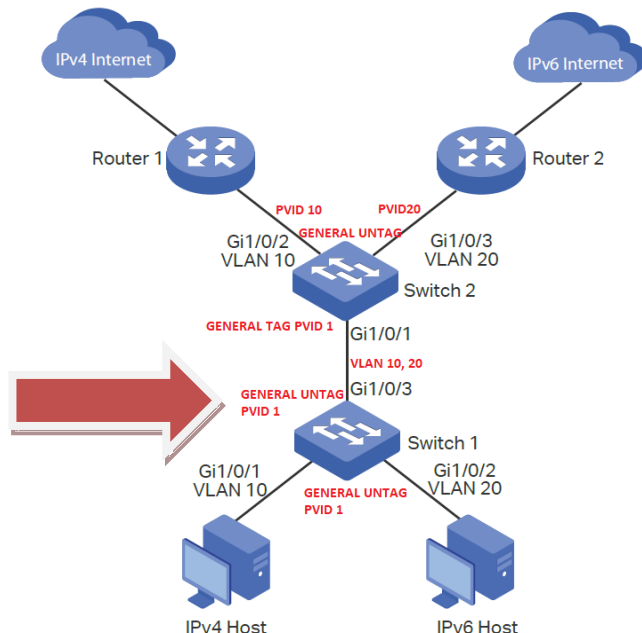
vlan500 -> 172.19.0.0/24



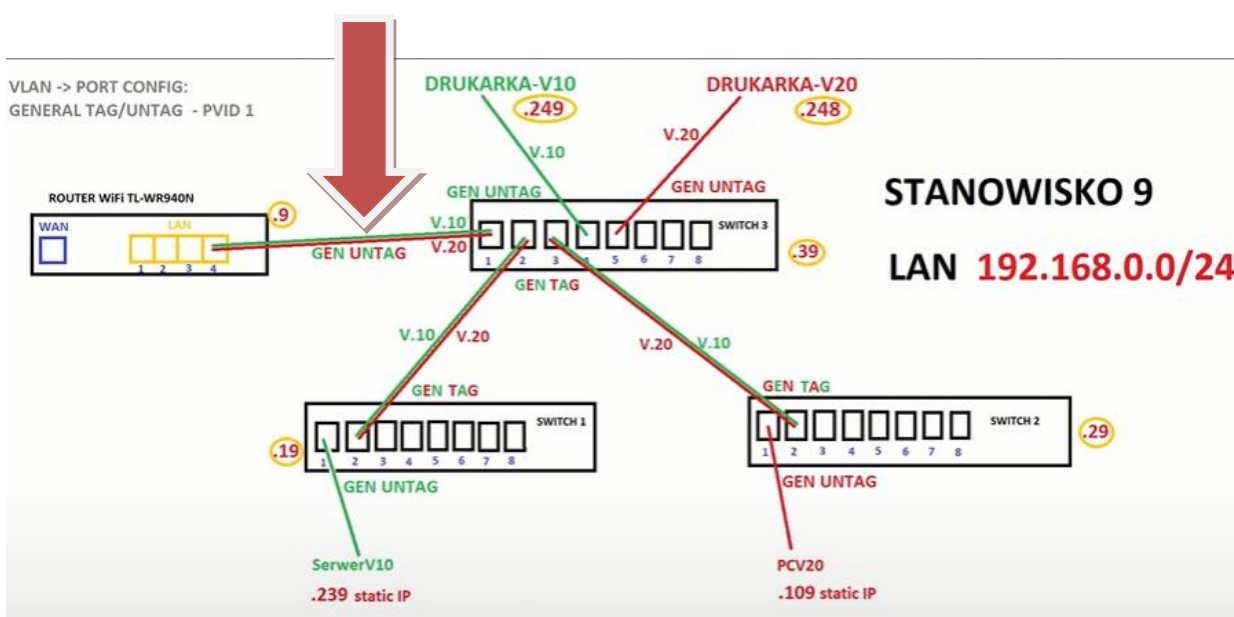
Wyjątek min stanowić może:

- użycie w sieci komputerowej urządzeń sieciowych z ustawioną opcją **Protocol VLAN**.

Figure 3-1 Network Topology



- użycie w sieci routera nie obsługującego vlany, podłączonego do przełącznika na porcie (router on the stick) lub portach (metoda klasyczna) w trybie **GEN-UNTAG**.



Port config :

Access – untag | jeden vlan

Trunk – Tag | wiele vlanów

General – Tag / untag | wiele vlanów

VLAN Config

Port Config

VLAN Port Config

Port

Select

Select	Port	Link Type	PVID	LAG	VLAN
☐		ACCESS ▾			
☐	1	ACCESS	1	---	Detail
☐	2	ACCESS	1	---	Detail
☐	3	ACCESS	1	---	Detail
☐	4	ACCESS	1	---	Detail
☐	5	ACCESS	1	---	Detail
☐	6	ACCESS	1	---	Detail
☐	7	ACCESS	1	---	Detail
☐	8	ACCESS	1	---	Detail
☐	9	ACCESS	1	---	Detail
☐	10	ACCESS	1	---	Detail
☐	11	ACCESS	1	---	Detail
☐	12	ACCESS	1	---	Detail
☐	13	ACCESS	1	---	Detail
☐	14	ACCESS	1	---	Detail

Apply

Help

PVID – dotyczy ruchu wejściowego do portu przełącznika dla ramek nietagowanych.

Jeżeli do portu dotrze ramka nietagowana, to przełącznik wrzuci do pola **Identyfikator VLAN** numer, zgodny z opisem **PVID** dla danego portu zdefiniowanego w zakładce **Port Config**.

VLAN Config

Port Config

VLAN Port Config					
UNIT: 1 LAGS					
Select	Port	Link Type	PVID	LAG	VLAN
☐		▼			
☐	1/0/1	GENERAL	1	---	Detail
☐	1/0/2	TRUNK	1	---	Detail
☐	1/0/3	ACCESS	1	---	Detail
☐	1/0/4	ACCESS	1	---	Detail
☐	1/0/5	ACCESS	1	---	Detail
☐	1/0/6	ACCESS	1	---	Detail
☐	1/0/7	ACCESS	1	---	Detail
☐	1/0/8	ACCESS	1	---	Detail
☐	1/0/9	ACCESS	1	---	Detail
☐	1/0/10	ACCESS	1	---	Detail

All

Apply

Help

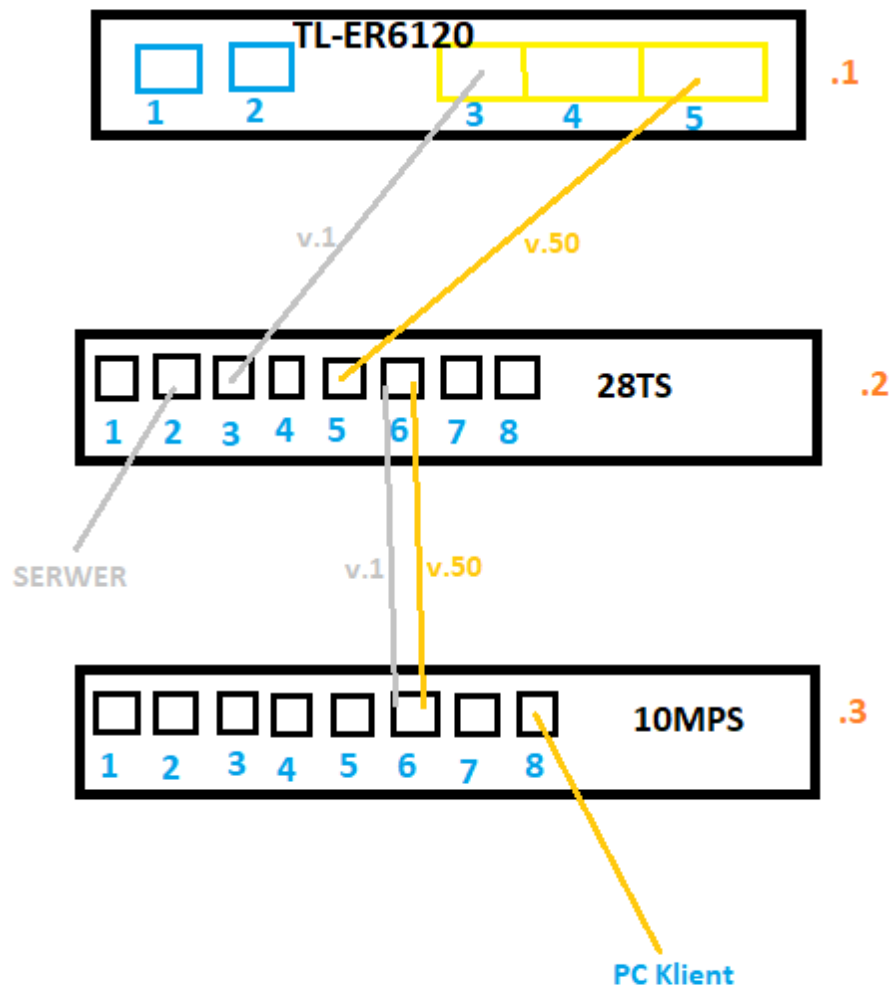
3.2 KONFIGURACJA VLAN-ÓW NA ROUTERZE - METODA KLASYCZNA

1. Połącz urządzenia według poniższego schematu.

UWAGA! Kabel żółty (VLAN50) z routera ma wstępnie luźno wisieć.

LAN

192.168.0.0/24



2. Ustaw VLANY na routerze TL-ER6120

tp-link

Status

VLAN

Ports

Network

WAN

LAN

IPTV

MAC

Switch

VLAN

IPv6

Preferences

Transmission

VLAN List

+ Add

- Delete

☐	ID	VLAN ID	Name	Ports	Description	Operation
☐	1	1	vlan1	3(UNTAG) 4(UNTAG) 5(UNTAG)	Default Vlan For LAN	☐
☐	2	10	vlan10	1(UNTAG)	Default Vlan For WAN1	☐
☐	3	20	vlan20	2(UNTAG)	Default Vlan For WAN2	☐

Status

VLAN

Ports

Network

WAN

LAN

IPTV

MAC

Switch

VLAN

IPv6

Preferences

Transmission

VLAN List

+ Add

- Delete

☐	ID	VLAN ID	Name	Ports	Description	Operation
☒	1	1	vlan1	3(UNTAG) 4(UNTAG) 5(UNTAG)	Default Vlan For LAN	☒
☐	2	10	vlan10	1(UNTAG)	Default Vlan For WAN1	☐
☐	3	20	vlan20	2(UNTAG)	Default Vlan For WAN2	☐

3. Odznacz port 5 dla VLAN-u pierwszego.

VLAN List

+ Add - Delete

☐	ID	VLAN ID	Name	Ports	Description	Operation
☐	1	1	vlan1	3(UNTAG) 4(UNTAG) 5(UNTAG)	Default Vlan For LAN	

VLAN ID: (1-4094)

Name: (1-50 characters)

Ports:

☐ 1

TAG

☐ 2

TAG

☒ 3

UNTAG

☒ 4

UNTAG

☐ 5

UNTAG

Description: (1-50 characters, optional)

VLAN Ports

VLAN List

+ Add - Delete

☐	ID	VLAN ID	Name	Ports	Description	Operation
☐	1	1	vlan1	3(UNTAG) 4(UNTAG)	Default Vlan For LAN	
☐	2	10	vlan10	1(UNTAG)	Default Vlan For WAN1	
☐	3	20	vlan20	2(UNTAG)	Default Vlan For WAN2	

4. Dodaj VLAN 50

Status

Network

- WAN
- LAN
- IPTV
- MAC
- Switch
- VLAN
- IPv6

Preferences

Transmission

Firewall

VLAN Ports

VLAN List

+ Add - Delete

☐	ID	VLAN ID	Name	Ports	Description	Operation
☐	1	1	vlan1	3(UNTAG) 4(UNTAG)	Default Vlan For LAN	
☐	2	10	vlan10	1(UNTAG)	Default Vlan For WAN1	
☐	3	20	vlan20	2(UNTAG)	Default Vlan For WAN2	

☐	ID	VLAN ID	Name	Ports
--	--	--	--	--

VLAN ID: (1-4094)

Name: (1-50 characters)

Ports:

☐ 1	TAG
☐ 2	TAG
☐ 3	TAG ▼
☐ 4	TAG ▼
☒ 5	TAG ▼

Description: (1-50 characters, optional)

OK Cancel

VLAN List

[+ Add](#) [- Delete](#)

☐	ID	VLAN ID	Name	Ports	Description	Operation
☐	1	1	vlan1	3(UNTAG) 4(UNTAG)	Default Vlan For LAN	
☐	2	10	vlan10	1(UNTAG)	Default Vlan For WAN1	
☐	3	20	vlan20	2(UNTAG)	Default Vlan For WAN2	
☐	4	50	vlan50	5(TAG)		

5. Dodaj VLAN 50 na przełączniku 28ts lub 28tq

System

Switching

VLAN

• 802.1Q VLAN

• MAC VLAN

• Protocol VLAN

• VLAN VPN

• GVRP

• Private VLAN

Spanning Tree

Ethernet OAM

Multicast

Routing

QoS

ACL

Network Security

VLAN Port Config

UNIT: 1 LAGS

Select	Port	Link Type	PVID
☐			
☐	1/0/1	ACCESS	1
☐	1/0/2	ACCESS	1
☐	1/0/3	ACCESS	1
☐	1/0/4	ACCESS	1
☐	1/0/5	TRUNK	1
☐	1/0/6	TRUNK	1
☐	1/0/7	ACCESS	1
☐	1/0/8	ACCESS	1
☐	1/0/9	ACCESS	1
☐	1/0/10	ACCESS	1
☐	1/0/11	ACCESS	1
☐	1/0/12	ACCESS	1
☐	1/0/13	ACCESS	1

T2600G-28TS

VLAN Config

Port Config

System

Switching

VLAN

• 802.1Q VLAN

• MAC VLAN

• Protocol VLAN

• VLAN VPN

• GVRP

• Private VLAN

Spanning Tree

Ethernet OAM

Multicast

Routing

QoS

ACL

Network Security

SNMP

LLDP

Maintenance

Save Config

VLAN Info

VLAN ID: (2 - 4094)Name : (16 characters maximum)

Untagged port

UNIT: LAGS

☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

All

Clear

Tagged port

UNIT: LAGS

☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

All

Clear

Apply

Help



Unselected Port(s)



Selected Port(s)



Not Available for

T2600G-28TS

VLAN Config

Port Config

System

Switching

VLAN

• 802.1Q VLAN

• MAC VLAN

• Protocol VLAN

• VLAN VPN

• GVRP

Vlan Table

Select	VLAN_ID	Name	Members	Operation
☐	1	System-VLAN	1/0/1-28	Edit Detail
☐	50	vlan50	1/0/5-6	Edit Detail

All

Create

Delete

Help

Total VLAN: 2

6. Dodaj VLAN 50 na przełączniku 10mps

UWAGA! NA przełączniku 28TQ używaj GENERAL zamiast TRUNK. Na TRUNK-u oprogramowanie urządzenia nie pozwala ustawić VLANÓW w sekcji Tagged port w zakładce VLAN Config.

T2500G-10MPS

System

Switching

VLAN

• 802.1Q VLAN

• MAC VLAN

• Protocol VLAN

• VLAN VPN

• GVRP

Spanning Tree

Multicast

DHCP

QoS

PoE

ACL

Network Security

SNMP

LLDP

VLAN Config

Port Config

VLAN Port Config

UNIT: 1 LAGS

Select	Port	Link Type	PVID	LAG
☐				
☐	1/0/1	ACCESS	1	---
☐	1/0/2	ACCESS	1	---
☐	1/0/3	ACCESS	1	---
☐	1/0/4	ACCESS	1	---
☐	1/0/5	ACCESS	1	---
☐	1/0/6	TRUNK	1	---
☐	1/0/7	ACCESS	1	---
☐	1/0/8	ACCESS	1	---
☐	1/0/9	ACCESS	1	---
☐	1/0/10	ACCESS	1	---

All

Apply

Help

T2500G-10MPS

System

Switching

VLAN

• 802.1Q VLAN

• MAC VLAN

• Protocol VLAN

• VLAN VPN

• GVRP

Spanning Tree

Multicast

DHCP

QoS

PoE

ACL

Network Security

SNMP

LLDP

Maintenance

Save Config

Index

VLAN Config

Port Config

VLAN Info

VLAN ID:

50

 (2 - 4094)

Name :

vlan50

 (16 characters maximum)

Untagged port

UNIT: 1 LAGS

1

2

3

4

5

6

7

8

9

10

All

Clear

Tagged port

UNIT: 1 LAGS

1

2

3

4

5

6

7

8

9

10

All

Clear

Apply

Help

Unselected Port(s)

Selected Port(s)

Not Available for Selection

T2500G-10MPS

VLAN Config
Port Config

System
Switching
VLAN

- 802.1Q VLAN
- MAC VLAN
- Protocol VLAN
- VLAN VPN
- GVRP

Vlan Table

Select	VLAN_ID	Name	Members	Operation
☐	1	System-VLAN	1/0/1-7, 1/0/9-10	Edit Detail
☐	50	vlan50	1/0/6, 1/0/8	Edit Detail

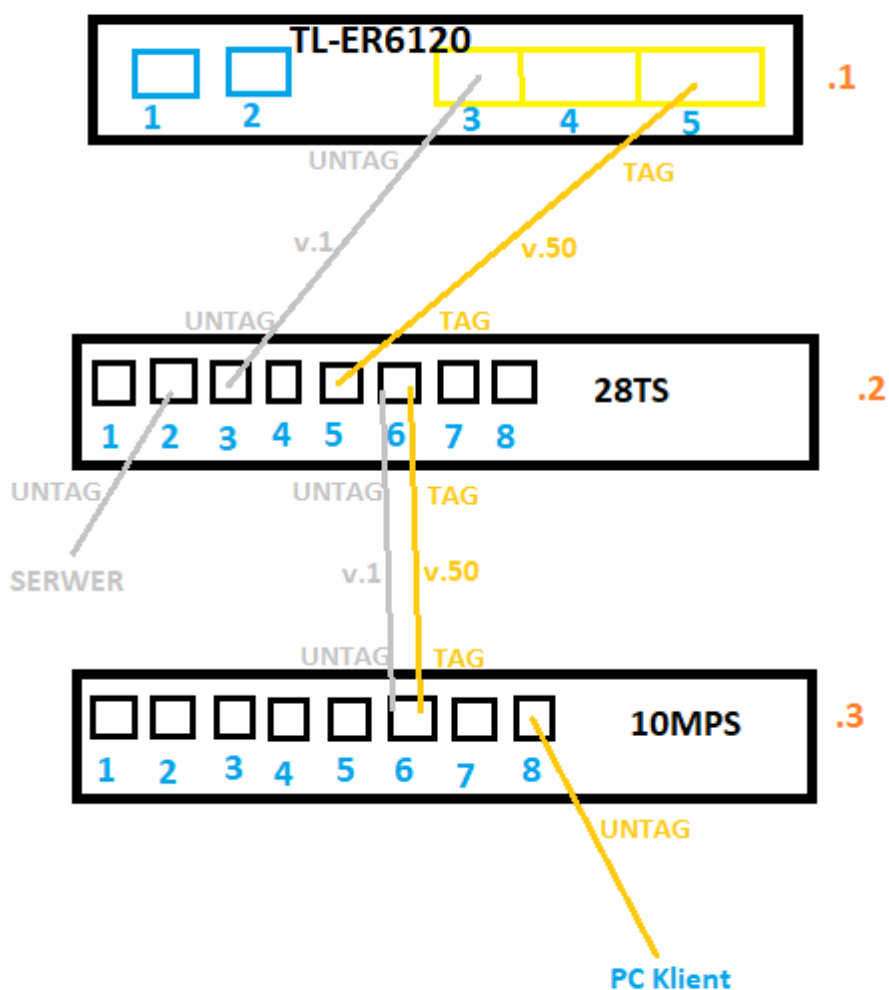
All
Create
Delete
Help

Total VLAN: 2

7. Poniższy obrazek pokazuje TAG i UNTAG dla poszczególnych VLANÓW na używanych portach.

LAN

192.168.0.0/24



8. Sprawdź numery VLAN-ów w kolumnie **PVID** w zakładce **VLAN Config**.

T2500G-10MPS

System

Switching

VLAN

• 802.1Q VLAN

• MAC VLAN

• Protocol VLAN

• VLAN VPN

• GVRP

Spanning Tree

Multicast

DHCP

QoS

PoE

ACL

Network Security

SNMP

LLDP

VLAN Config

Port Config

VLAN Port Config

UNIT: 1 LAGS

Select	Port	Link Type	PVID	LAG	VLAN
☐					
☐	1/0/1	ACCESS	1	---	Detail
☐	1/0/2	ACCESS	1	---	Detail
☐	1/0/3	ACCESS	1	---	Detail
☐	1/0/4	ACCESS	1	---	Detail
☐	1/0/5	ACCESS	1	---	Detail
☐	1/0/6	TRUNK	1	---	Detail
☐	1/0/7	ACCESS	1	---	Detail
☐	1/0/8	ACCESS	50	---	Detail
☐	1/0/9	ACCESS	1	---	Detail
☐	1/0/10	ACCESS	1	---	Detail

All

Apply

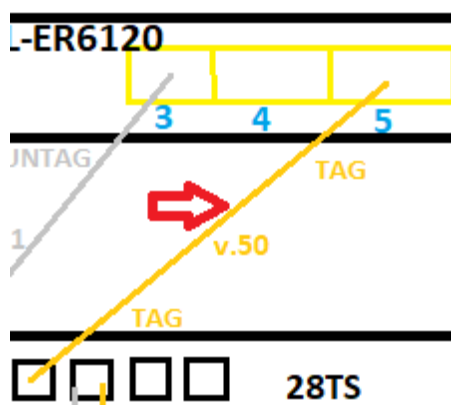
Help

9. Z pozycji **SERWERA** zaloguj się na switch 2. Sprawdź w zakładce **System info/System IP** wiersz **Management VLAN**. Zarządzanie przełącznikiem w tym momencie jest możliwe tylko po VLAN- ie pierwszym.

T2500G-10MPS		System Summary	Device Description	System Time	Daylight Saving Time	Serial Port Setting	System
System		IP Config					
• System Info		MAC Address: AC-84-C6-4A-9D-FC					
• User Management		IP Address Mode: ☒ Static IP ☐ DHCP ☐ BOOTP					
• System Tools		Management VLAN: 1 (VLAN ID: 1-4094)					Apply
• Access Security		IP Address: 192.168.0.3					Help
Switching		Subnet Mask: 255.255.255.0					
VLAN		Default Gateway: 192.168.0.1					
Spanning Tree							
Multicast							
DHCP							
QoS							

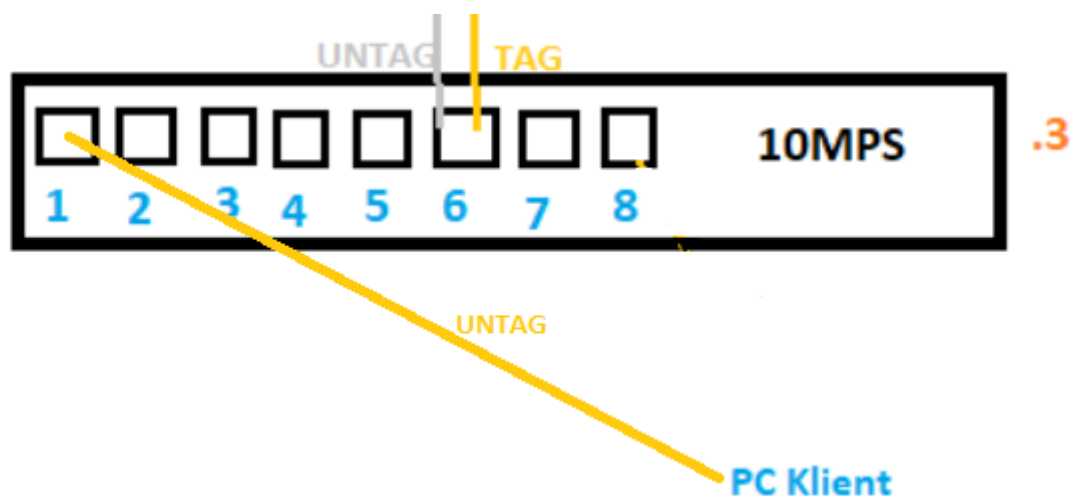
Note:
Changing IP address to a different IP segment will interrupt the network communication, so please keep the new IP address in the same IP segment with the local network.

10. Podłącz router z przełącznikiem 28ts lub 28tq na porcie 5. Teraz router połączony jest z przełącznikiem dwoma kablami.



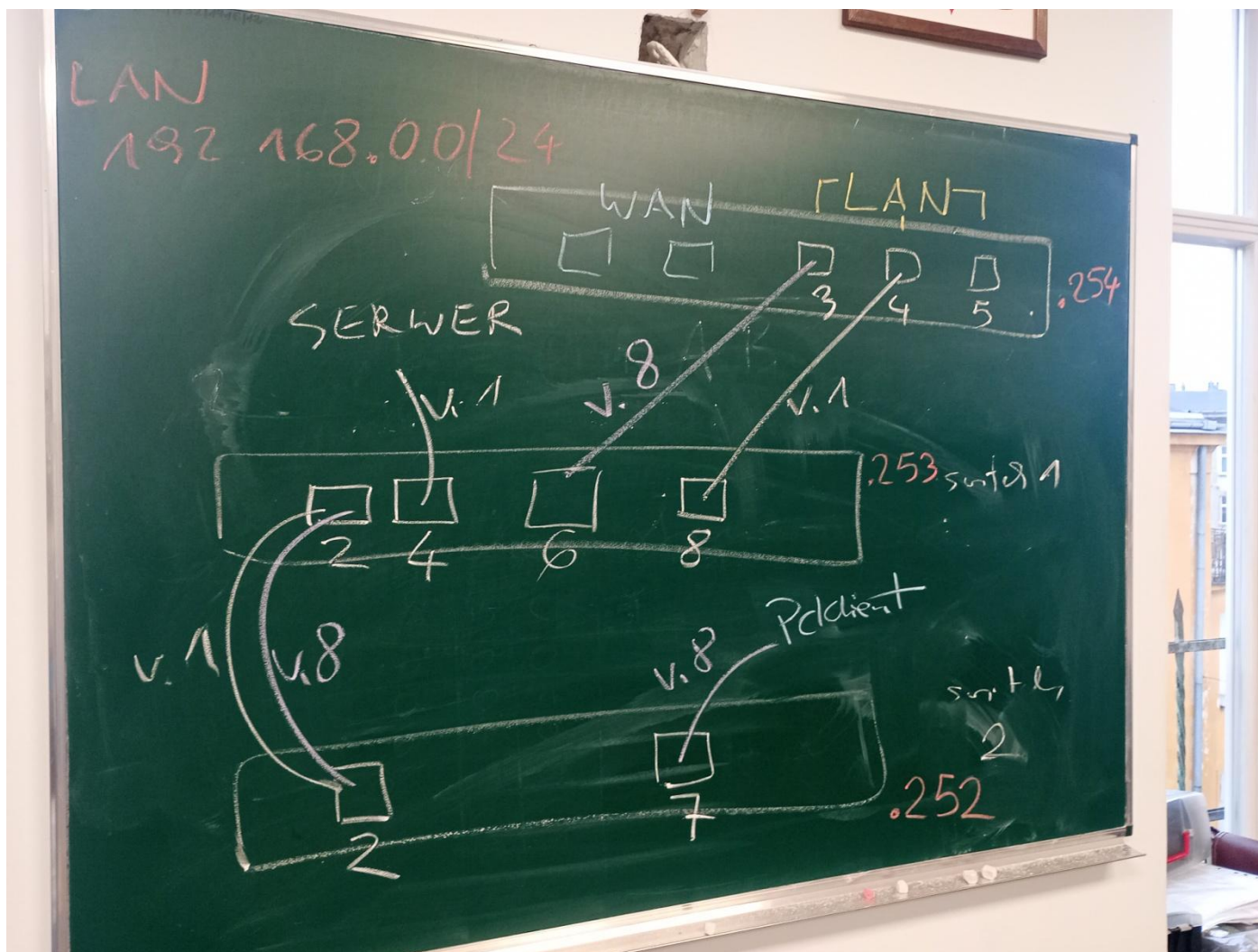
11. Ponieważ PCKlient połączony jest do portu 8, który należy do VLAN – u 50, to zarządzanie urządzeniami sieciowymi z tej stacji jest niemożliwe. Sprawdź czy możesz wyświetlić w przeglądarce panel konfiguracyjny przełącznika 10MPS.
12. Wykonaj pingowanie ze stacji roboczej na serwer. Urządzenia nie powinny się widzieć, ponieważ serwer należy do VLAN –u 1, a PCKlient do VLAN –u 50.

13. Przełącz kabel sieciowy PCKlienta z **portu 8** na port należący domyślnie do VLAN-u pierwszego np. **port 1**. Teraz w przeglądarce powinien dać się wyświetlić panel konfiguracyjny przełącznika 10MPS.

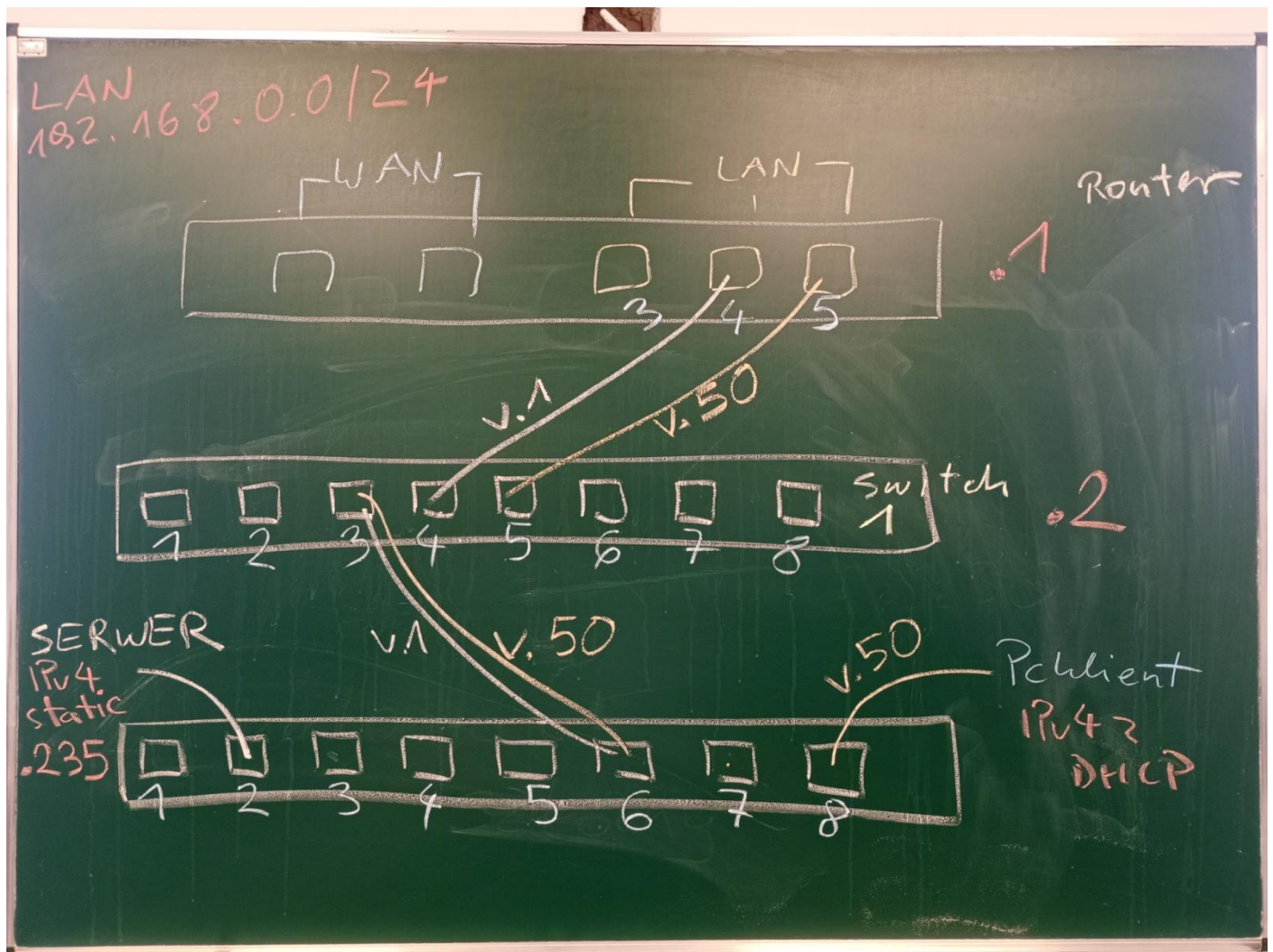


14. Na przełączniku 2 w zakładce **System info/System IP** ustaw Management **50**. Następnie wepnij kabel od PCKlienta ponownie do portu 8. Naciśnij klawisz F5. W przeglądarce powinien Ci się wyświetlić panel konfiguracyjny przełącznika 2.

Zadanie do samodzielnego rozwiązania 1

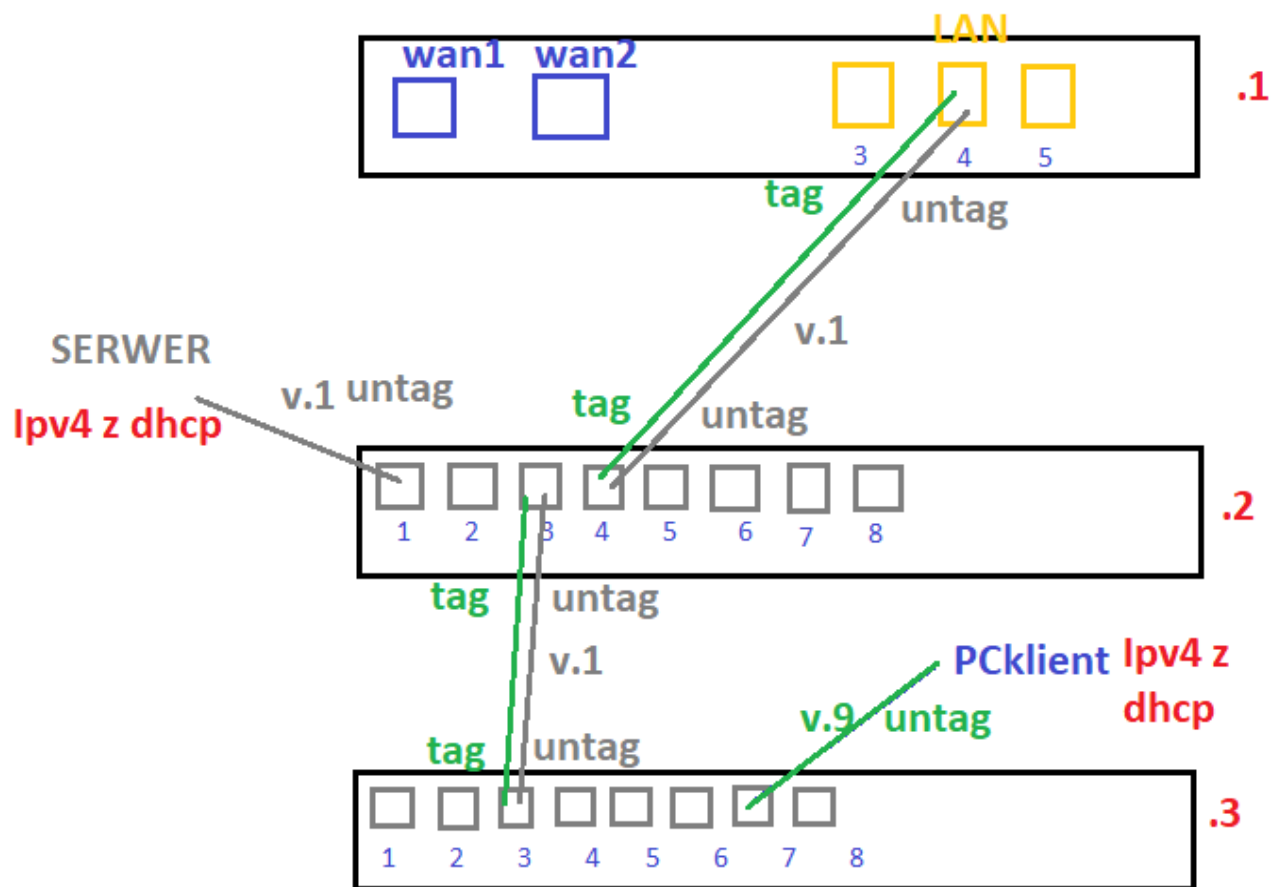


Zadanie do samodzielnego rozwiązania 2



3.3 KONFIGURACJA VLAN-ÓW NA ROUTERZE – ROUTER ON THE STICK

192.168.0.0/24



Konfiguracja vlan-ów na routerze

Status

Network

- WAN
- LAN
- IPTV
- MAC
- Switch
- VLAN
- IPv6

Preferences

Transmission

Firewall

Behavior Control

VPN

Authentication

Services

System Tools

Logout

Copyright © 2018
TP-Link Technologies Co., Ltd.
All rights reserved.

VLAN

Ports

VLAN List

+ Add

- Delete

	ID	VLAN ID	Name	Ports	Description	Operation
☐	--	--	--	--	--	--
VLAN ID: 9 (1-4094) Name: vlan9 (1-50 characters) Ports: ☐ 1 TAG ☐ 2 TAG ☐ 3 TAG ☒ 4 TAG ☐ 5 TAG						

Description:(1-50 characters, optional)

OK

Cancel

Status

Network

- WAN
- LAN
- IPTV
- MAC
- Switch
- VLAN
- IPv6

Preferences

Transmission

Firewall

Behavior Control

VLAN

Ports

VLAN List

+ Add

- Delete

	ID	VLAN ID	Name	Ports	Description	Operation
☐	1	1	vlan1	3(UNTAG) 4(UNTAG) 5(UNTAG)	Default Vlan For LAN	
☐	2	9	vlan9	4(TAG)		
☐	3	10	vlan10	1(UNTAG)	Default Vlan For WAN1	
☐	4	20	vlan20	2(UNTAG)	Default Vlan For WAN2	

Konfiguracja vlan-ów na przełączniku 28ts

T2600G-28TS

VLAN Config **Port Config**

Operation succeeded.

VLAN Port Config

UNIT: 1 LAGS

Select	Port	Link Type	PVID	LAG	VLAN
☐					
☐	1/0/1	ACCESS	1	---	Detail
☐	1/0/2	ACCESS	1	---	Detail
☐	1/0/3	TRUNK	1	---	Detail
☐	1/0/4	TRUNK	1	---	Detail
☐	1/0/5	ACCESS	1	---	Detail
☐	1/0/6	ACCESS	1	---	Detail
☐	1/0/7	ACCESS	1	---	Detail
☐	1/0/8	ACCESS	1	---	Detail
☐	1/0/9	ACCESS	1	---	Detail
☐	1/0/10	ACCESS	1	---	Detail
☐	1/0/11	ACCESS	1	---	Detail
☐	1/0/12	ACCESS	1	---	Detail
☐	1/0/13	ACCESS	1	---	Detail
☐	1/0/14	ACCESS	1	---	Detail
☐	1/0/15	ACCESS	1	---	Detail

All

Apply

Help

T2600G-28TS

VLAN Config **Port Config**

VLAN Info

VLAN ID:

9

 (2 - 4094)

Name :

vlan9

 (16 characters maximum)

Untagged port

UNIT: 1 LAGS

2

4

6

8

10

12

14

16

18

20

22

24

26

28

1

3

5

7

9

11

13

15

17

19

21

23

25

27

All

Clear

Tagged port

UNIT: 1 LAGS

2

4

6

8

10

12

14

16

18

20

22

24

26

28

1

3

5

7

9

11

13

15

17

19

21

23

25

27

All

Clear

Apply

Help

Unselected Port(s) Selected Port(s) Not Available for Selection

Konfiguracja vlan-ów na przełączniku 10mps

T2500G-10MPS

VLAN Config **Port Config**

Operation succeeded.

VLAN Port Config

UNIT: 1 LAGS

Select	Port	Link Type	PVID	LAG	VLAN
☐					
☐	1/0/1	ACCESS	1	---	Detail
☐	1/0/2	ACCESS	1	---	Detail
☐	1/0/3	TRUNK	1	---	Detail
☐	1/0/4	ACCESS	1	---	Detail
☐	1/0/5	ACCESS	1	---	Detail
☐	1/0/6	ACCESS	1	---	Detail
☐	1/0/7	ACCESS	1	---	Detail
☐	1/0/8	ACCESS	1	---	Detail
☐	1/0/9	ACCESS	1	---	Detail
☐	1/0/10	ACCESS	1	---	Detail

All

Apply

Help

T2500G-10MPS

VLAN Config **Port Config**

VLAN Info

VLAN ID:

9

 (2 - 4094)

Name :

vlan9

 (16 characters maximum)

Untagged port

UNIT: 1 LAGS

1

2

3

4

5

6

7

8

9

10

All

Clear

Tagged port

UNIT: 1 LAGS

1

2

3

4

5

6

7

8

9

10

All

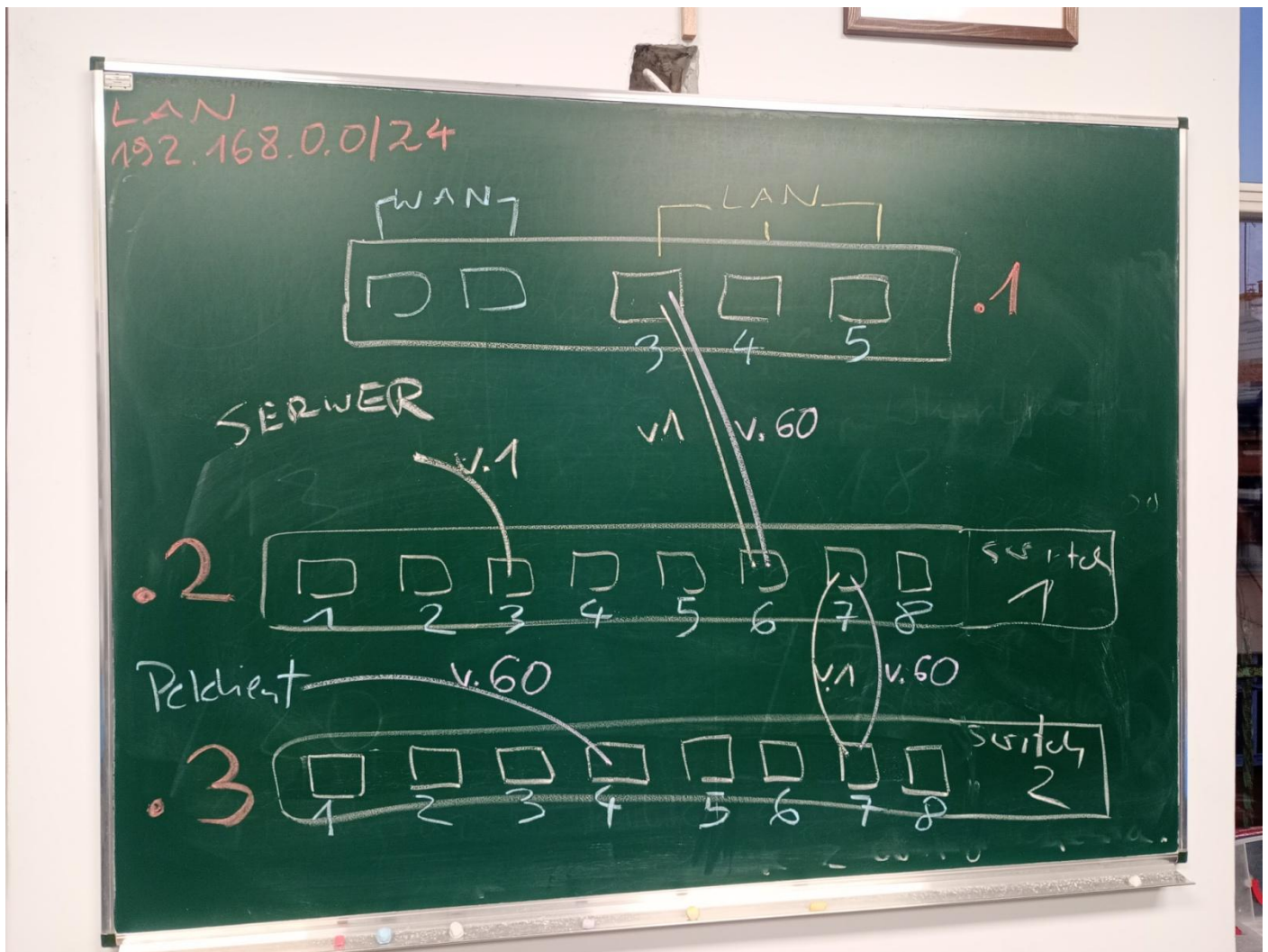
Clear

Apply

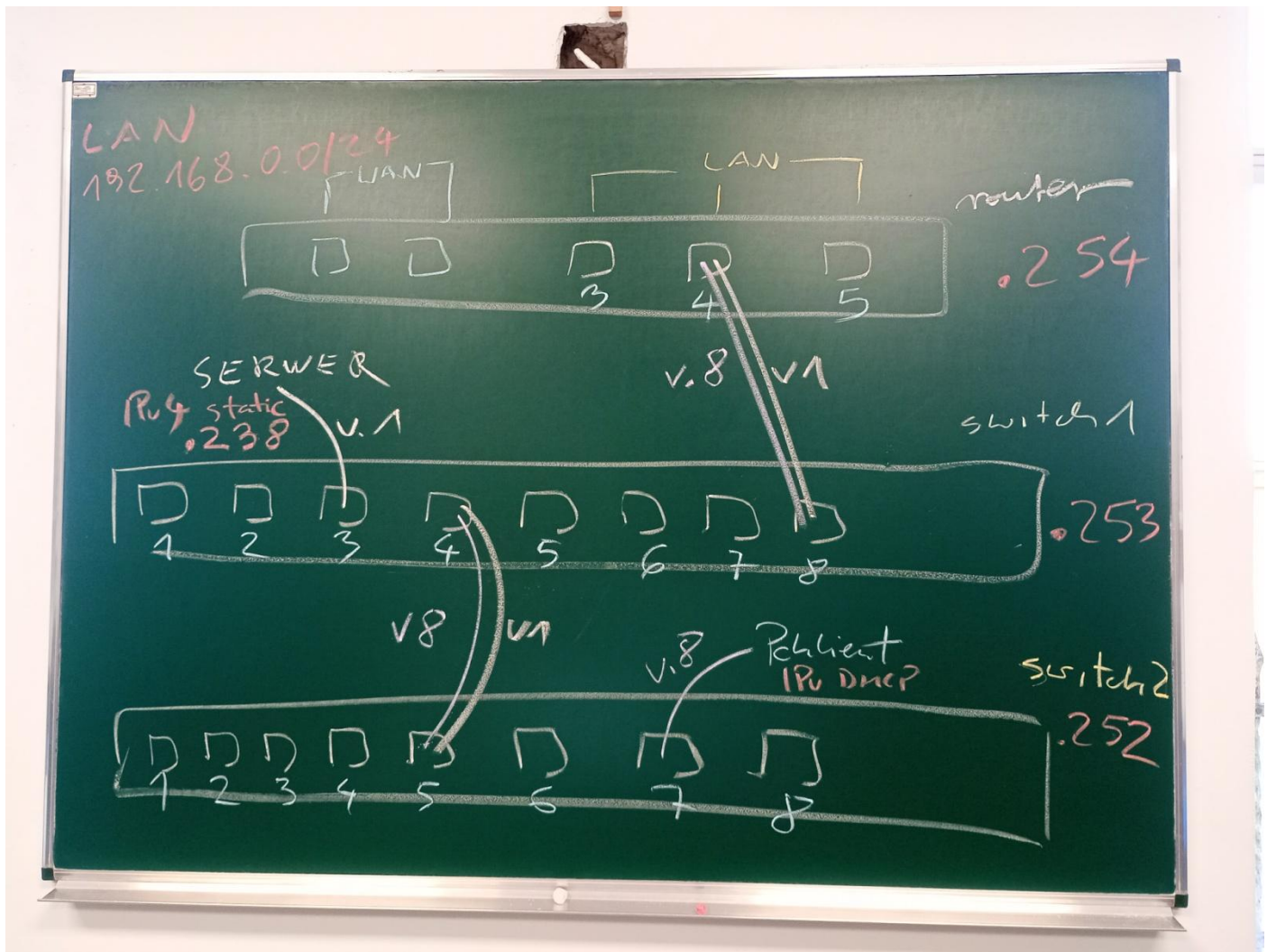
Help

Unselected Port(s) Selected Port(s) Not Available for Selection

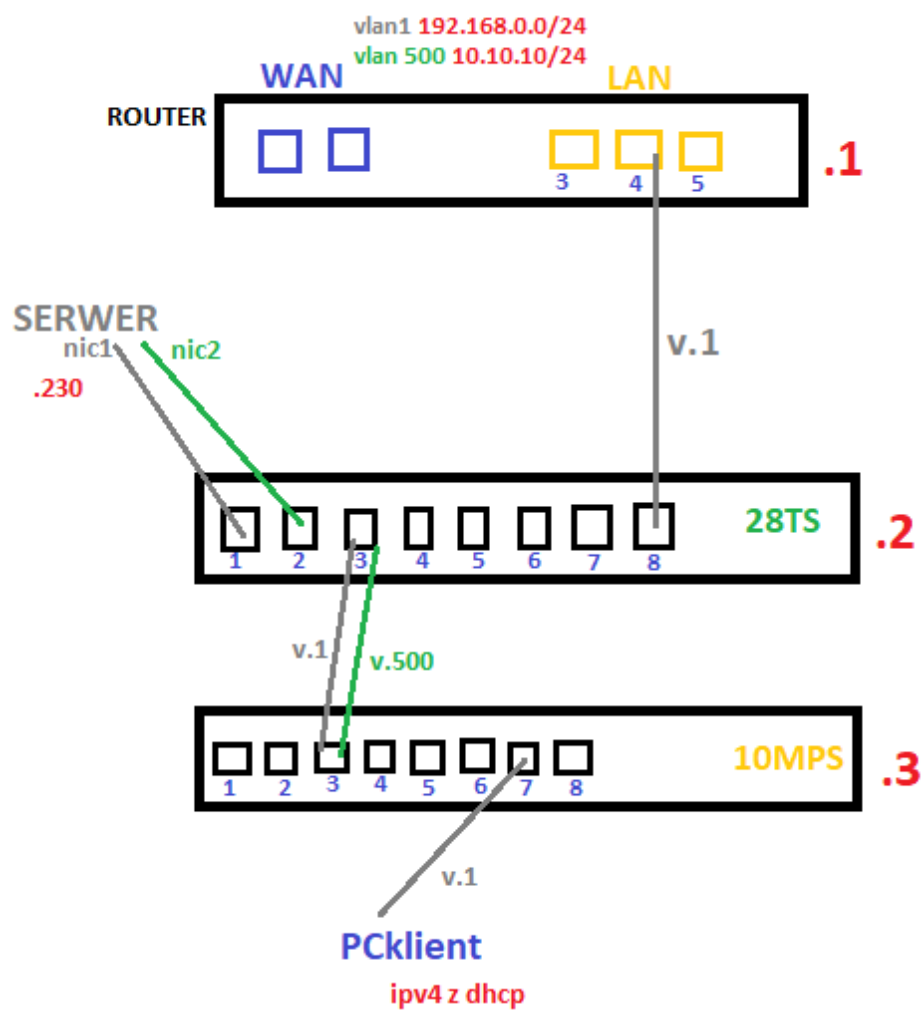
Zadanie do samodzielnego rozwiązania 1



Zadanie do samodzielnego rozwiązania 2

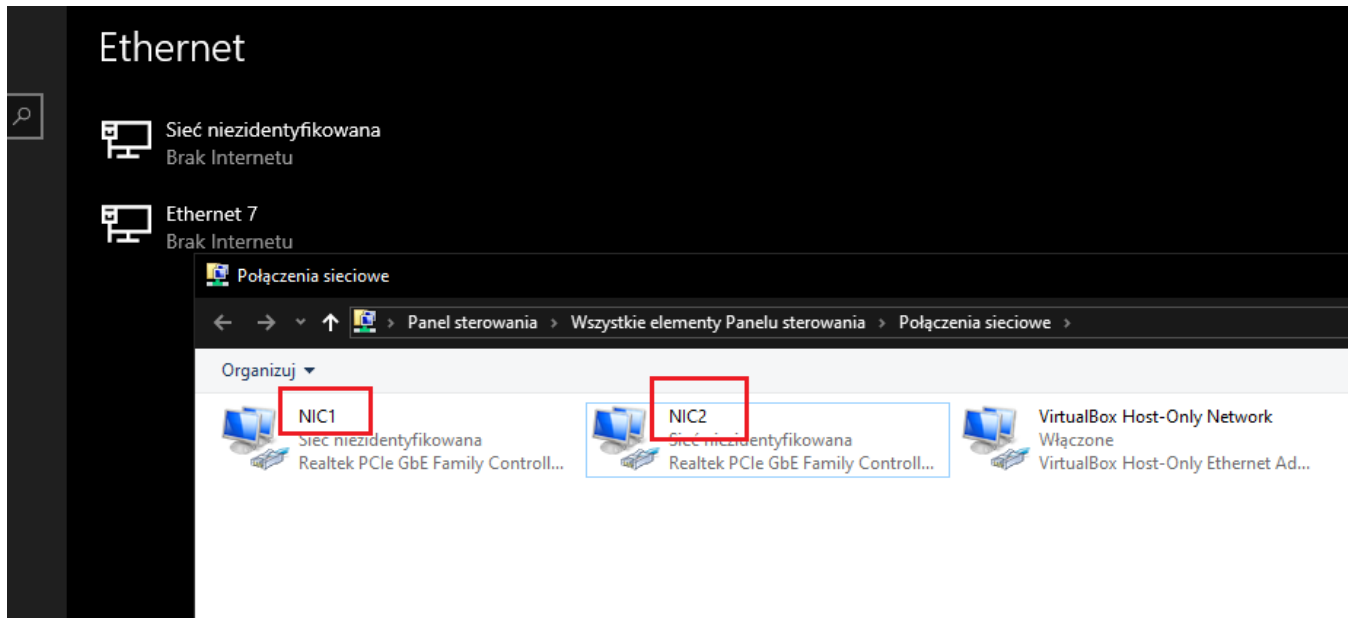


3.4 VLAN MANAGEMENT 500

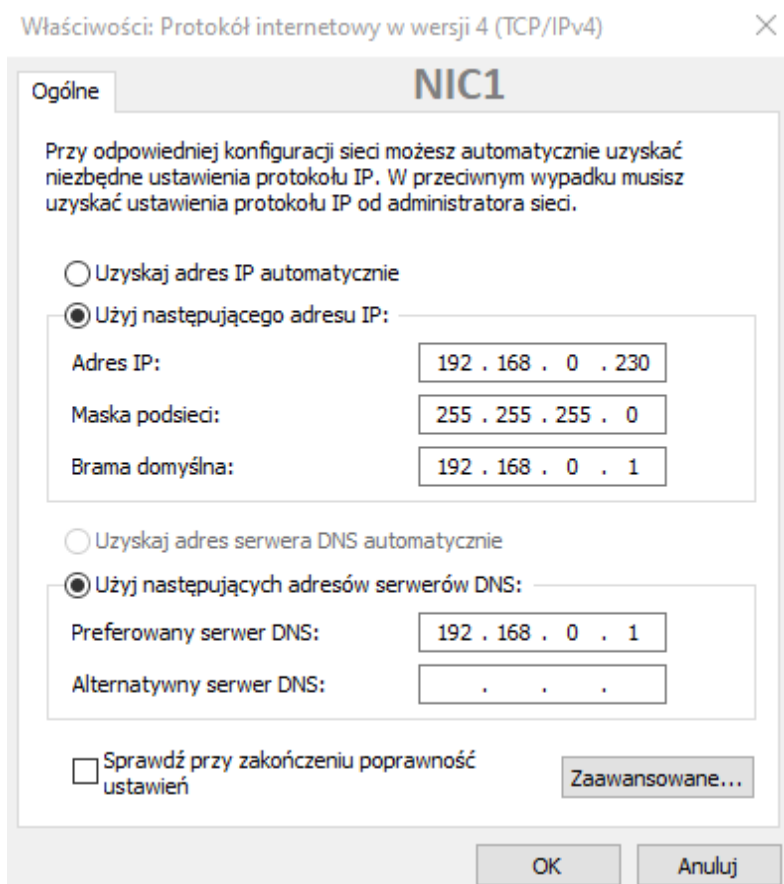


SWITCH 28TS lub 28TQ

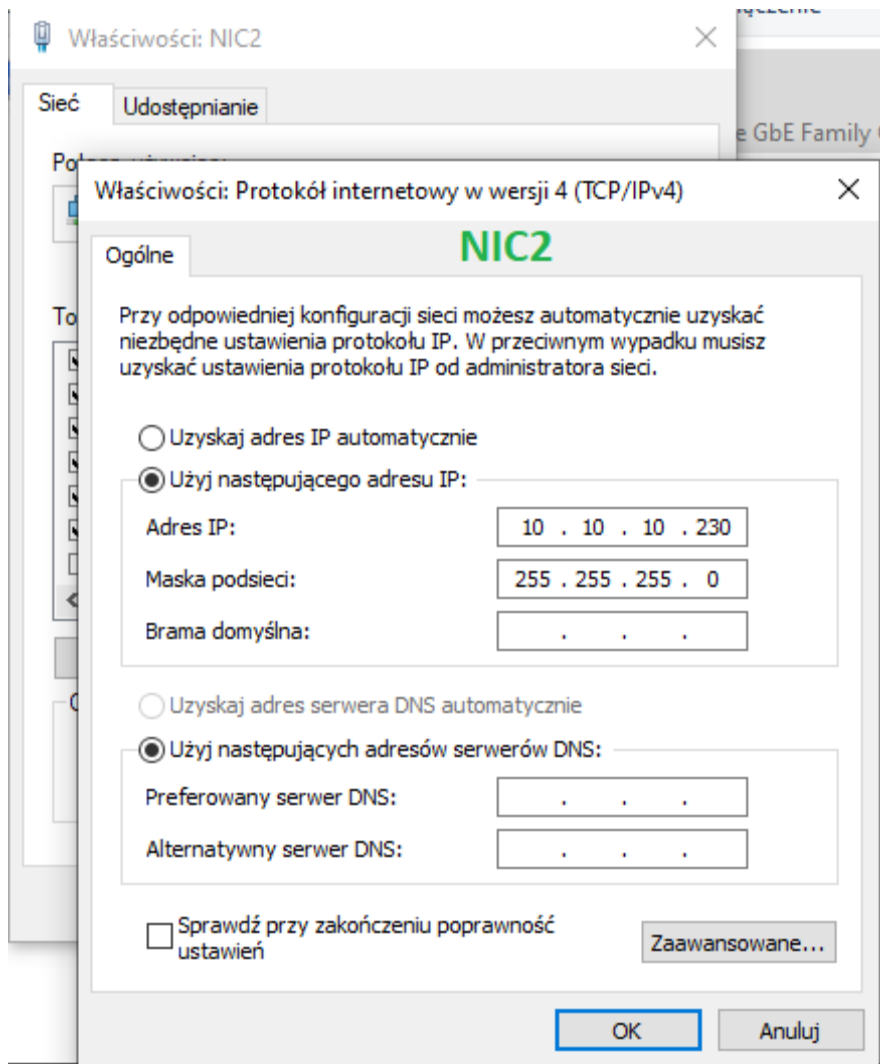
1. Wyświetl interfejsy sieciowe na SERWERZE. Podłącz kabel biały do przełącznika na **PORCIE 1** i obserwuj reakcję kart sieciowych. Ta, na której zniknął czerwony X niech otrzyma nazwę **NIC1**.
2. Teraz połącz zielonym kablem drugą kartę sieciową SERWERA z portem przełącznika (**PORT 2**). Nadaj nazwę drugiemu interfejsowi sieciowemu **NIC2**.



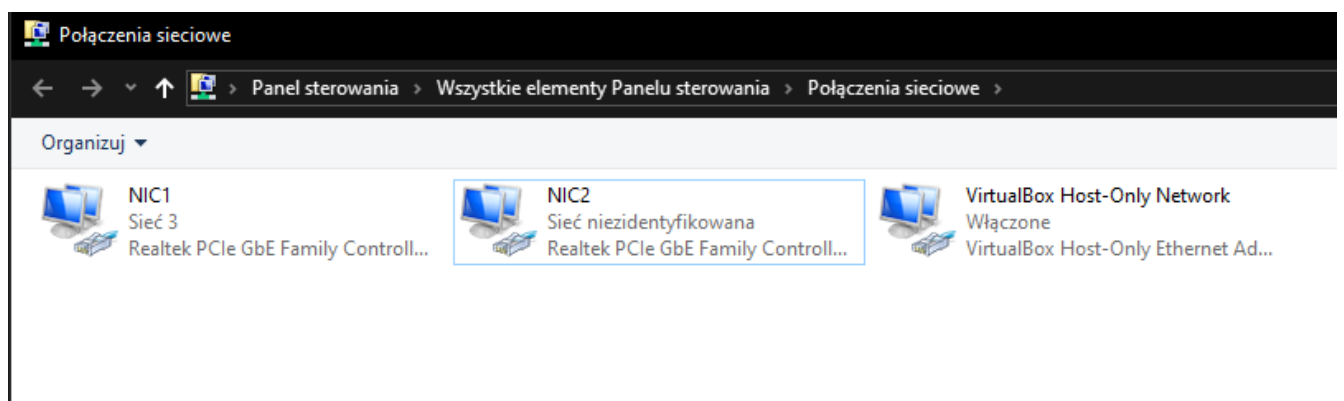
3. Ustaw IPv4 statycznie na interfejsie **NIC1** dla VLAN-u 1



4. Ustaw IPv4 statycznie na interfejsie NIC2 dla VLAN-u 500



5. Zwróć uwagę, że **NIC1** obsługujący VLAN 1 kontaktuje się z routerem, ponieważ otrzymała wpis Sieć 3.



SWITCH 28TS

6. Ustaw statyczny adres przełącznika na **192.168.0.2/24**.

T2600G-28TS

Interface Config

Creating Interface

Interface ID: VLAN (1-4094)

IP Address Mode: ☒ None ☐ Static ☐ DHCP ☐ BOOTP

IP Address: (Format: 192.168.0.1)

Subnet Mask: (Format: 255.255.255.0)

Admin Status: Enable

Interface Name: (Optional. 1-16 characters)

Create

Interface List

Select	ID	Mode	IP Address	Subnet Mask	Interface Name	Status	Operation
☐	Vlan1	Static	192.168.0.2	255.255.255.0		Up	Edit Edit IPv6 Detail

All Delete Help

Interface Count: 1

Note:

The addresses of different interfaces can't be the same.

7. Teraz ustaw nowy adres przełącznika **10.10.10.2/24** dla **VLAN-u 500**.

T2600G-28TS

Interface Config

Creating Interface

Interface ID: VLAN (1-4094)

IP Address Mode: ☐ None ☒ Static ☐ DHCP ☐ BOOTP

IP Address: (Format: 192.168.0.1)

Subnet Mask: (Format: 255.255.255.0)

Admin Status: Enable

Interface Name: (Optional. 1-16 characters)

Create

Interface List

Select	ID	Mode	IP Address	Subnet Mask	Interface Name	Status	Operation
☐	Vlan1	Static	192.168.0.2	255.255.255.0		Up	Edit Edit IPv6 Detail

All Delete Help

Interface Count: 1

Note:

The addresses of different interfaces can't be the same.

8. Ponieważ nie utworzyliśmy **VLAN-u 500** w zakładce VLAN status ID Vlan500 jest **Down**.

T2600G-28TS

Interface Config

Creating Interface

Interface ID: VLAN (1-4094)

IP Address Mode: ☒ None ☐ Static ☐ DHCP ☐ BOOTP

IP Address: (Format: 192.168.0.1)

Subnet Mask: (Format: 255.255.255.0)

Admin Status: Enable

Interface Name: (Optional. 1-16 characters)

Create

Interface List

Select	ID	Mode	IP Address	Subnet Mask	Interface Name	Status	Operation
☐	Vlan500	Static	10.10.10.2	255.255.255.0		Down	Edit Edit IPv6 Detail
☐	Vlan1	Static	192.168.0.2	255.255.255.0		Up	Edit Edit IPv6 Detail

AllDeleteHelp

Interface Count: 2

9. Utwórz VLAN 500

T2600G-28TS

VLAN ConfigPort Config

Operation succeeded.

VLAN Port Config

UNIT: 1 LAGS

Select	Port	Link Type	PVID	LAG	VLAN
☐					
☐	1/0/1	ACCESS	1	---	Detail
☐	1/0/2	ACCESS	1	---	Detail
☐	1/0/3	TRUNK	1	---	Detail
☐	1/0/4	ACCESS	1	---	Detail
☐	1/0/5	ACCESS	1	---	Detail
☐	1/0/6	ACCESS	1	---	Detail
☐	1/0/7	ACCESS	1	---	Detail
☐	1/0/8	ACCESS	1	---	Detail
☐	1/0/9	ACCESS	1	---	Detail
☐	1/0/10	ACCESS	1	---	Detail
☐	1/0/11	ACCESS	1	---	Detail
☐	1/0/12	ACCESS	1	---	Detail
☐	1/0/13	ACCESS	1	---	Detail
☐	1/0/14	ACCESS	1	---	Detail
☐	1/0/15	ACCESS	1	---	Detail

AllApplyHelp

T2600G-28TS

VLAN Config

Port Config

System

Switching

VLAN

• 802.1Q VLAN

• MAC VLAN

• Protocol VLAN

• VLAN VPN

• GVRP

• Private VLAN

Spanning Tree

Ethernet OAM

Multicast

Routing

QoS

ACL

Network Security

SNMP

LLDP

Maintenance

Save Config

VLAN Info

VLAN ID:

500

(2 - 4094)

Name :

Management

(16 characters maximum)

Untagged port

UNIT: 1 LAGS

2

4

6

8

10

12

14

16

18

20

22

24

26

28

1

3

5

7

9

11

13

15

17

19

21

23

25

27

All

Clear

Tagged port

UNIT: 1 LAGS

2

4

6

8

10

12

14

16

18

20

22

24

26

28

1

3

5

7

9

11

13

15

17

19

21

23

25

27

All

Clear

Apply

Help

Unselected Port(s)

Selected Port(s)

Not Available for Selection

T2600G-28TS

VLAN Config

Port Config

System

Switching

VLAN

• 802.1Q VLAN

• MAC VLAN

• Protocol VLAN

• VLAN VPN

• GVRP

Vlan Table

Select	VLAN_ID	Name	Members	Operation
☐	1	System-VLAN	1/0/1,1/0/3-28	Edit Detail
☐	500	Management	1/0/2-3	Edit Detail

All

Create

Delete

Help

Total VLAN: 2

10. Usuń Vlan1 z Interface List.

T2600G-28TS

Interface Config

System

Switching

VLAN

Spanning Tree

Ethernet OAM

Multicast

Routing

• Interface

• Routing Table

• Static Routing

• DHCP Server

• DHCP Relay

• DHCP L2 Relay

• ARP

QoS

ACL

Network Security

Creating Interface

Interface ID:

VLAN

(1-4094)

IP Address Mode:

None

Static

DHCP

BOOTP

IP Address:

(Format: 192.168.0.1)

Subnet Mask:

(Format: 255.255.255.0)

Admin Status:

Enable

Interface Name:

(Optional. 1-16 characters)

Create

Interface List

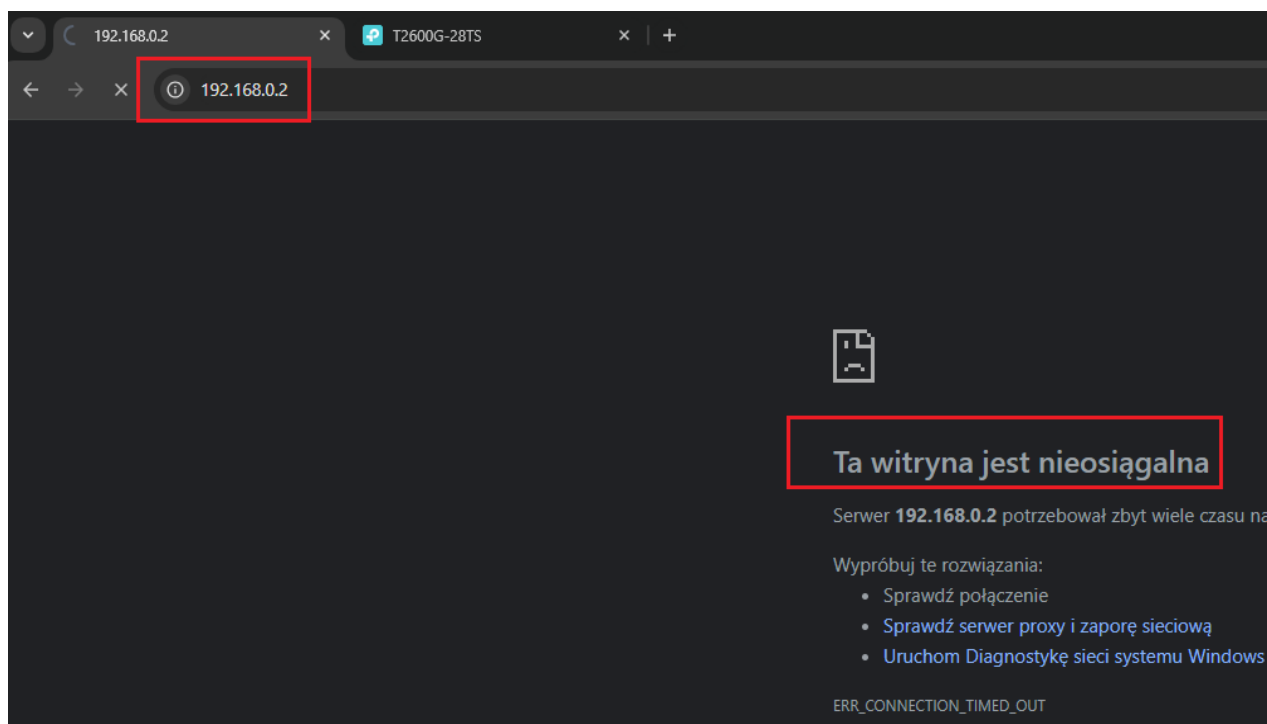
Select	ID	Mode	IP Address	Subnet Mask	Interface Name	Status	Operation
☐	Vlan500	Static	10.10.10.2	255.255.255.0		Down	Edit Edit IPv6 Detail
☒	Vlan1	Static	192.168.0.2	255.255.255.0		Up	Edit Edit IPv6 Detail

All

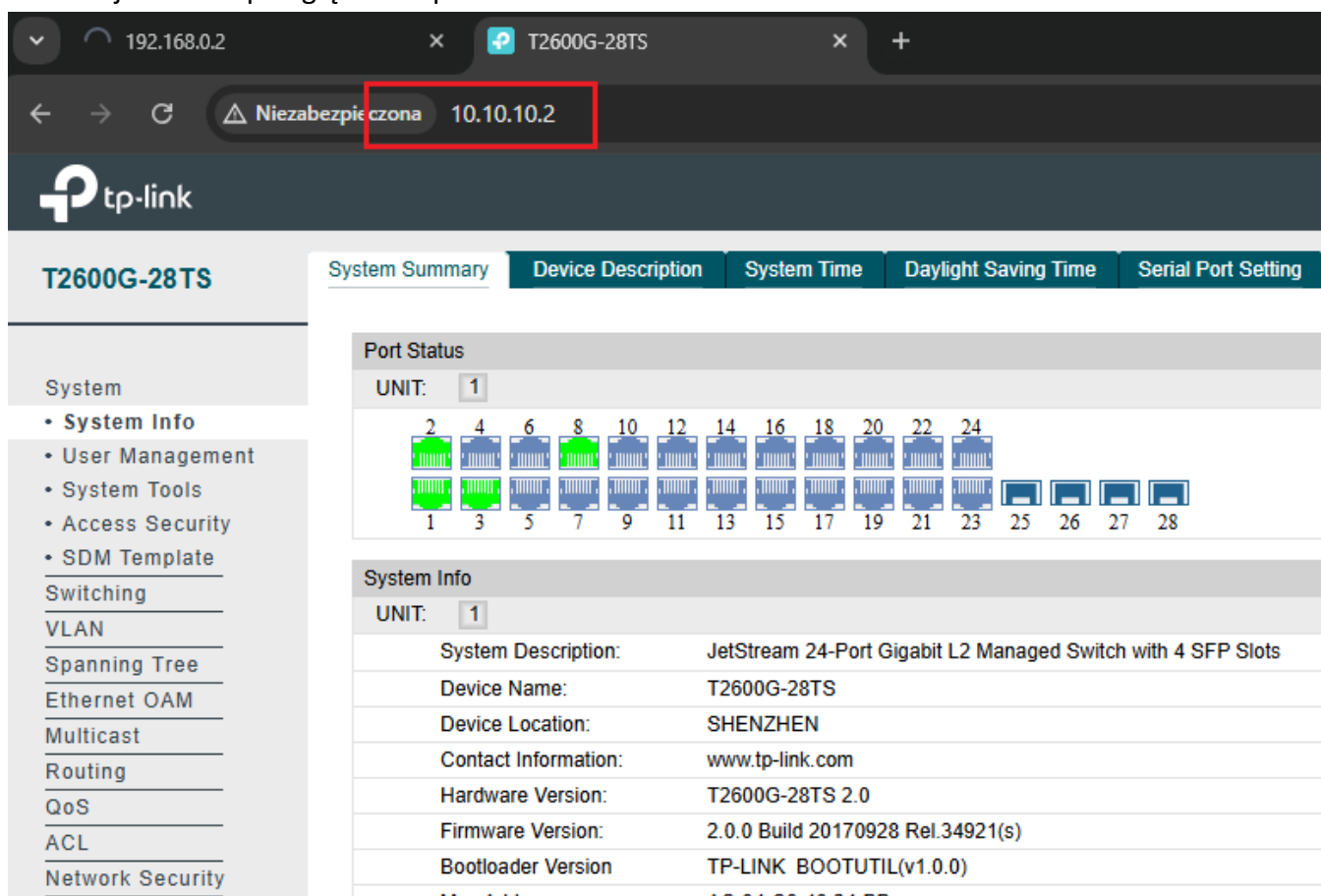
Delete

Help

11. Teraz nie można wyświetlić panelu konfiguracyjnego przełącznika po adresie **192.168.0.2**.



12. W nowej zakładce przeglądarki wpisz **10.10.10.2**.



SWITCH 10MPS

13. Ustaw nowy adres IPv4 urządzenia sieciowego **192.168.0.3/24**; brama domyślna **0.0.0.0**
14. Zakładka VLANY -> Utwórz VLAN 500
15. Zakładka System -> System IP -> W polu **Management VLAN** wpisz 500
 - > W polach **IP Address/Subnet Mask** wpisz 10.10.10.3/2
 - > **Default Gateway**: 0.0.0.0

Pojawi się komunikat na żółtym tle jak pokazuje poniższy obrazek

System Summary	Device Description	System Time	Daylight Saving Time	Serial Port Setting	System IP
At least one port's PVID must be set as the management VLAN ID.					
IP Config					
MAC Address:	AC-84-C6-4A-9C-2C				
IP Address Mode:	☒ Static IP ☐ DHCP ☐ BOOTP				
Management VLAN:	1 (VLAN ID: 1-4094)				
IP Address:	192.168.0.3				Apply Help
Subnet Mask:	255.255.255.0				
Default Gateway:	0.0.0.0				

16. Zaznacz kafelek w sekcji untag w vlanie 500 jako port tymczasowy, żeby ustawił się choć jeden PVID 500

VLAN Config

Port Config

VLAN Port Config

UNIT: 1 LAGS

Select	Port	Link Type	PVID	LAG	VLAN
☐		▼			
☐	1/0/1	ACCESS	1	---	Detail
☐	1/0/2	ACCESS	1	---	Detail
☐	1/0/3	TRUNK	1	---	Detail
☐	1/0/4	ACCESS	1	---	Detail
☐	1/0/5	ACCESS	1	---	Detail
☐	1/0/6	ACCESS	1	---	Detail
☐	1/0/7	ACCESS	1	---	Detail
☐	1/0/8	ACCESS	1	---	Detail
☐	1/0/9	ACCESS	1	---	Detail
☐	1/0/10	ACCESS	1	---	Detail

All

Apply

Help

VLAN Config

Port Config

VLAN Info

VLAN ID:

500

 (1 - 4094)

Name :

vlan500

 (16 characters maximum)

Untagged port

UNIT: 1 LAGS

1

2

3

4

5

6

7

8

9

10

tymczasowy port

All

Clear

Tagged port

UNIT: 1 LAGS

1

2

3

4

5

6

7

8

9

10

All

Clear

Apply

Help



Unselected Port(s)



Selected Port(s)



Not Available for Selection

VLAN Port Config

UNIT: 1 LAGS

Select	Port	Link Type	PVID	LAG	VLAN
☐					
☐	1/0/1	ACCESS	500	---	Detail
☐	1/0/2	ACCESS	1	---	Detail
☐	1/0/3	TRUNK	1	---	Detail
☐	1/0/4	ACCESS	1	---	Detail
☐	1/0/5	ACCESS	1	---	Detail
☐	1/0/6	ACCESS	1	---	Detail
☐	1/0/7	ACCESS	1	---	Detail
☐	1/0/8	ACCESS	1	---	Detail
☐	1/0/9	ACCESS	1	---	Detail
☐	1/0/10	ACCESS	1	---	Detail

All

Apply

Help

IP Config

MAC Address: AC-84-C6-4A-9C-2C

IP Address Mode: ☒ Static IP ☐ DHCP ☐ BOOTP

Management VLAN: 500 (VLAN ID: 1-4094)

IP Address: 10.10.10.3

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Apply

Help

bezpieczona 10.10.10.3

ta! LIBRUS Szkoła Logowanie - System... Platforma edukacyjna D Jak w PuTTY połącz... #! Jak wyg

VLAN Config

Port Config

VLAN Info

VLAN ID: 500 (1 - 4094)

Name : vlan500 (16 characters maximum)

Untagged port

UNIT: 1 LAGS

1 2 3 4 5 6 7 8 9 10

odznacz port

All

Clear

Tagged port

UNIT: 1 LAGS

1 2 3 4 5 6 7 8 9 10

All

Clear

Apply

Help



Unselected Port(s)



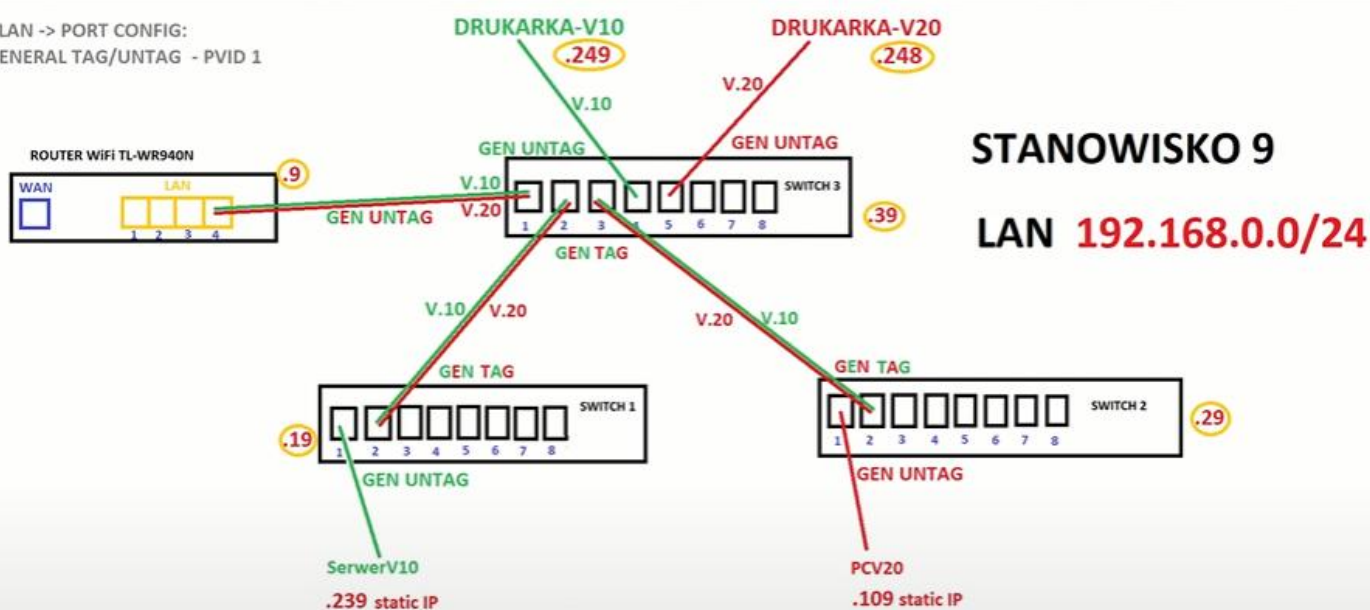
Selected Port(s)



Not Available for Selection

3.3 MAC VLANY

VLAN -> PORT CONFIG:
GENERAL TAG/UNTAG - PVID 1



1. Podłącz kable według powyższego schematu, ale bez podłączania drukarek
2. Zaloguj się na przełączniki, oraz router i ustaw adresy docelowe IPv4 urządzeń sieciowych uwzględniając numer swojego stanowiska.
3. Ustaw IPv4 static na kartach sieciowych **SERWERA** i **Pcklienta** uwzględniając numer swojego stanowiska.
4. Zaloguj się na **switch1** ustaw **GENERAL** na portach używanych: **port1** i **port2**
Zaloguj się na **switch2** ustaw **GENERAL** na portach używanych: **port1** i **port2**

T2600G-28TS

System

Switching

VLAN

- 802.1Q VLAN
- MAC VLAN
- Protocol VLAN
- VLAN VPN
- GVRP
- Private VLAN

Spanning Tree

Ethernet OAM

Multicast

Routing

QoS

ACL

Network Security

SNMP

LLDP

Maintenance

Save Config

VLAN Config

Port Config

Operation succeeded.

VLAN Port Config

UNIT: 1 LAGS

Select	Port	Link Type	PVID	LAG
☐	1/0/1	GENERAL	1	---
☐	1/0/2	GENERAL	1	---
☐	1/0/3	ACCESS	1	---
☐	1/0/4	ACCESS	1	---
☐	1/0/5	ACCESS	1	---
☐	1/0/6	ACCESS	1	---
☐	1/0/7	ACCESS	1	---
☐	1/0/8	ACCESS	1	---
☐	1/0/9	ACCESS	1	---
☐	1/0/10	ACCESS	1	---
☐	1/0/11	ACCESS	1	---
☐	1/0/12	ACCESS	1	---
☐	1/0/13	ACCESS	1	---
☐	1/0/14	ACCESS	1	---
☐	1/0/15	ACCESS	1	---

All Apply Help

5. Ustaw **vlan10** i **vlan20** na przełącznikach 1 i 2.

T2600G-28TS

VLAN ConfigPort Config

VLAN Info

VLAN ID:10(2 - 4094)

Name :vlan10(16 characters maximum)

Untagged port

UNIT:1LAGS

2	4	6	8	10	12	14	16	18	20	22	24	26	28
1	3	5	7	9	11	13	15	17	19	21	23	25	27

AllClear

Tagged port

UNIT:1LAGS

2	4	6	8	10	12	14	16	18	20	22	24	26	28
1	3	5	7	9	11	13	15	17	19	21	23	25	27

AllClearApplyHelp

☐ Unselected Port(s)☒ Selected Port(s)☐ Not Available for Selection

T2600G-28TS

VLAN ConfigPort Config

VLAN Info

VLAN ID:20(2 - 4094)

Name :vlan20(16 characters maximum)

Untagged port

UNIT:1LAGS

2	4	6	8	10	12	14	16	18	20	22	24	26	28
1	3	5	7	9	11	13	15	17	19	21	23	25	27

AllClear

Tagged port

UNIT:1LAGS

2	4	6	8	10	12	14	16	18	20	22	24	26	28
1	3	5	7	9	11	13	15	17	19	21	23	25	27

AllClearApplyHelp

☐ Unselected Port(s)☒ Selected Port(s)☐ Not Available for Selection

6. W notatniku zapisz adresy mac **SERWERA** i **Pcklienta**.
Pozyskaj adres mac **SERWERA** poleceniem **ipconfig /all**

```
Wykonanie polecenia
C:\Users\dom>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-IA95RGS
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter NIC2:

Connection-specific DNS Suffix . . :
Description . . . . . : Realtek PCIe GBE Family Controller
Physical Address. . . . . : 18-D6-C7-05-15-BB
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::e053:3af7:6be3:b1e%10(Preferred)
IPv4 Address. . . . . : 192.168.0.239(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.9
DNS Servers . . . . . : 192.168.0.9
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\dom>
```

```
ipconfig /all

nfiguration
. . . . . 18-D6-C7-05-15-BB serwer
s Suffix
```

- Z pozycji **SERWERA** pozyskaj mac adres **Pcklienta** za pomocą polecenia **arp - a**.
Najpierw wykonaj pingowanie na **Pcklienta**

```
C:\Users\dom>ping 192.168.0.109

Pinging 192.168.0.109 with 32 bytes of data:
Reply from 192.168.0.109: bytes=32 time=1ms TTL=128
Reply from 192.168.0.109: bytes=32 time<1ms TTL=128
Reply from 192.168.0.109: bytes=32 time=2ms TTL=128
Reply from 192.168.0.109: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.0.109:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

Następnie wyświetl zawartość bufora ARP **Pcklienta**


```
C:\Users\dom>arp -a

Interface: 192.168.0.239 --- 0xa
Internet Address      Physical Address      Type
192.168.0.1           ac-84-c6-46-24-4f    dynamic
192.168.0.9           98-da-c4-64-61-86    dynamic
192.168.0.19          ac-84-c6-46-24-48    dynamic
192.168.0.29          ac-84-c6-46-24-4f    dynamic
192.168.0.39          30-b5-c2-3a-e4-ae    dynamic
192.168.0.109         98-ee-cb-9b-32-ec    dynamic
192.168.0.248         30-05-5c-42-47-82    dynamic
192.168.0.249         ac-16-2d-cd-08-f5    dynamic
192.168.0.255         ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-5e-00-00-02    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250      01-00-5e-7f-ff-fa    static
```

```
for 192.168.0.109:
t = 4, Received = 4, Lost = 0 (0% loss),
d trip times in milli-seconds:
s, Max
-a
18-D6-C7-05-15-BB serwer
98-ee-cb-9b-32-ec klient
68.0.2
ss
```

7. Na **przełącznikach 1 i 2**, w zakładce **MAC VLAN** przypisz adresy mac do odpowiednich vlanów

T2600G-28TS

- System
- Switching
- VLAN
 - 802.1Q VLAN
 - MAC VLAN**
 - Protocol VLAN
 - VLAN VPN
 - GVRP
 - Private VLAN
- Spanning Tree
- Ethernet OAM
- Multicast

MAC VLAN

Port Enable

Create MAC VLAN

MAC Address: 18-D6-C7-05-15-BB (Format: 00-00-00-00-00-01)
Description: serwer (8 characters maximum)
VLAN ID: 10 (1-4094)

Create

Clear

MAC VLAN Table

Select	MAC Address	Description	VLAN ID	Operation
No entry in the table.				

All

Delete

Help

Total MAC VLAN:0

T2600G-28TS

MAC VLAN
Port Enable

System
Switching
VLAN

- 802.1Q VLAN
- MAC VLAN**
- Protocol VLAN
- VLAN VPN
- GVRP
- Private VLAN

Spanning Tree
Ethernet OAM

Create MAC VLAN

MAC Address: 98-ee-cb-9b-32-ec (Format: 00-00-00-00-00-01)
Description: pcklient (8 characters maximum)
VLAN ID: 20 (1-4094)

Create

Clear

MAC VLAN Table

Select	MAC Address	Description	VLAN ID	Operation
☐	18-d6-c7-05-15-bb	server	10	Edit

All

Delete

Help

Total MAC VLAN:1

8. Na **switch** – u **2** wejdź na zakładkę PORT Enable i zaznacz port 1.
To samo wykonaj na switch-u 1.

UWAGA! Jeżeli dobrze masz podłączone kable i poprawnie ustawiony vlan to **SERWER** powinien utracić dostęp do panelu konfiguracyjnego przełącznika.

Przepnij kabel **SERWERA** na port różny od **portów 1 i 2**.

9. Zaloguj się na **przełącznik 3**.

Ustaw opcję **GENERAL** na używane **porty** od **1** do **5**.

10. Połącz kablem **przełącznik 3** z drukarką po **vlanie 10**.

11. Pozyska adresy mac drukarek i zapisz w notatniku

W tym celu na **SERWERZE** wykonaj pingowanie na drukarki, a następnie wyświetl zawartość bufora ARP

```

C:\Users\dom>arp -a

Interface: 192.168.0.239 --- 0xa
Internet Address      Physical Address      Type
192.168.0.1           ac-84-c6-46-24-4f     dynamic
192.168.0.9           98-da-c4-64-61-86     dynamic
192.168.0.19          ac-84-c6-46-24-48     dynamic
192.168.0.29          ac-84-c6-46-24-4f     dynamic
192.168.0.39          30-b5-c2-3a-e4-ae     dynamic
192.168.0.109         98-ee-cb-9b-32-ec     dynamic
192.168.0.248         30-05-5c-42-47-82     dynamic
192.168.0.249         ac-16-2d-cd-08-f5     dynamic
192.168.0.255         ff-ff-ff-ff-ff-ff     static
224.0.0.2             01-00-5e-00-00-02     static
224.0.0.22           01-00-5e-00-00-16     static
224.0.0.251          01-00-5e-00-00-fb     static
224.0.0.252          01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static

```

192.168.0.9	98-da-c4-64-61-86	dynamic
192.168.0.19	ac-84-c6-46-24-48	
192.168.0.29	ac-84-c6-46-24-4f	
192.168.0.39	30-b5-c2-3a-e4-ae	
192.168.0.109	98-ee-cb-9b-32-ec	
192.168.0.248	30-05-5c-42-47-82	druk248
192.168.0.249	ac-16-2d-cd-08-f5	druk249

12. Ustaw **vlan10** i **vlan20** na przełączniku 3

TL-SG3210

- System
- Switching
- VLAN
- 802.1Q VLAN
- MAC VLAN
- Protocol VLAN
- GVRP
- Spanning Tree
- Multicast
- QoS
- ACL
- Network Security
- SNMP
- Cluster
- Maintenance
- Save Config
- Logout

VLAN Config
Port Config

VLAN Create

VLAN ID: 10 (2-4094)
Description: vlan10 (16 characters maximum)

VLAN Members

Select	Port	Link Type	Egress Rule	LAG
☒	1	GENERAL	UNTAG	---
☒	2	GENERAL	TAG	---
☒	3	GENERAL	TAG	---
☒	4	GENERAL	UNTAG	---
☐	5	GENERAL	UNTAG	---
☐	6	ACCESS	UNTAG	---
☐	7	ACCESS	UNTAG	---
☐	8	ACCESS	UNTAG	---
☐	9	ACCESS	UNTAG	---
☐	10	ACCESS	UNTAG	---

Apply
All
Back
Help

TL-SG3210

- System
- Switching
- VLAN
- 802.1Q VLAN
- MAC VLAN
- Protocol VLAN
- GVRP
- Spanning Tree
- Multicast
- QoS
- ACL
- Network Security
- SNMP
- Cluster
- Maintenance
- Save Config
- Logout

VLAN Config
Port Config

VLAN Create

VLAN ID: 20 (2-4094)
Description: vlan20 (16 characters maximum)

VLAN Members

Select	Port	Link Type	Egress Rule	LAG
☒	1	GENERAL	UNTAG	---
☒	2	GENERAL	TAG	---
☒	3	GENERAL	TAG	---
☐	4	GENERAL	UNTAG	---
☒	5	GENERAL	UNTAG	---
☐	6	ACCESS	UNTAG	---
☐	7	ACCESS	UNTAG	---
☐	8	ACCESS	UNTAG	---
☐	9	ACCESS	UNTAG	---
☐	10	ACCESS	UNTAG	---

Apply
All
Back
Help

13. Na **przełącznikach 3** , w zakładce **MAC VLAN** przypisz adresy mac drukarek do odpowiednich vlanów

TL-SG3210 MAC VLAN

Create MAC VLAN

MAC Address: 30-05-5c-42-47-82 (Format: 00-00-00-00-00-01)

Description: druk20 (8 characters maximum)

VLAN ID: 20 (1-4094)

Create Clear

MAC VLAN Table

Select	MAC Address	Description	VLAN ID	Operation
No entry in the MAC VLAN table.				

All Delete Help

TL-SG3210 MAC VLAN

Create MAC VLAN

MAC Address: ac-16-2d-cd-08-f5 (Format: 00-00-00-00-00-01)

Description: druk10 (8 characters maximum)

VLAN ID: 10 (1-4094)

Create Clear

MAC VLAN Table

Select	MAC Address	Description	VLAN ID	Operation
☒	30-05-5c-42-47-82	druk20	20	Edit

All Delete Help

Total MAC Based VLAN: 1

14. Jeżeli jako **przełącznik3** używasz modelu **28ts** lub **10mps**, to dodatkowo w zakładce **Port Enable** musisz zaznaczyć porty dla których usługa **MAC VLAN** ma działać.

T2500G-10MPS MAC VLAN Port Enable

Port Enable

UNIT: 1 LAGS

1 2 3 4 5 6 7 8 9 10

All Clear Apply Help

Unselected Port(s) Selected Port(s) Not Available

15. Połącz kablem **przełącznik 3** z drukarką po **vlanie 20**.
16. Z pozycji **SERWERA** wykonaj pingowanie na **DRUKARKA-V10**, a następnie na **DRUKARKA-V20**. **SERWER** nie powinien łączyć się z **DRUKARKA-V20**.

```
C:\Users\dom>ping 192.168.0.249

Pinging 192.168.0.249 with 32 bytes of data:
Reply from 192.168.0.249: bytes=32 time<1ms TTL=255
Reply from 192.168.0.249: bytes=32 time=2ms TTL=255
Reply from 192.168.0.249: bytes=32 time<1ms TTL=255
Reply from 192.168.0.249: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.249:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\dom>ping 192.168.0.248

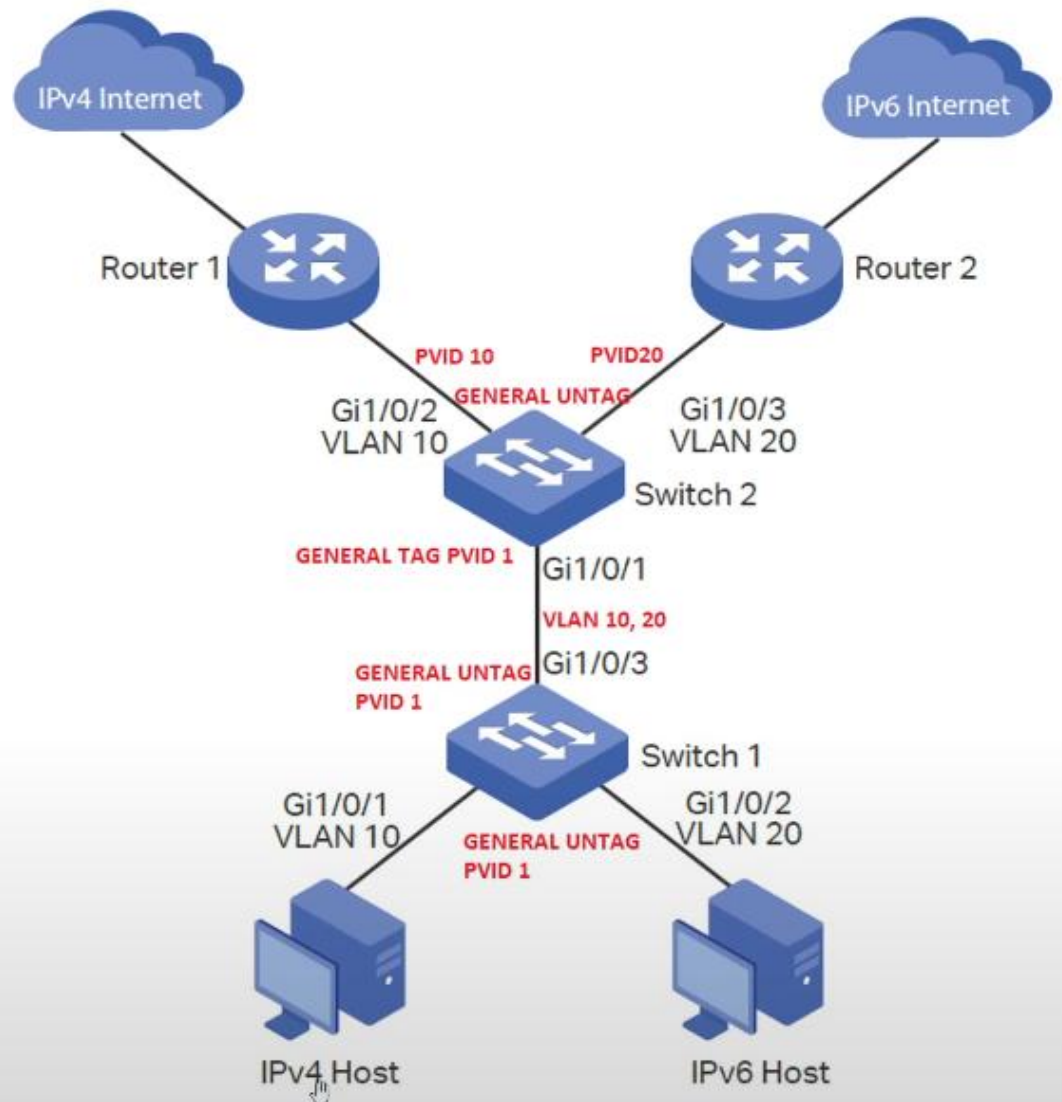
Pinging 192.168.0.248 with 32 bytes of data:
Reply from 192.168.0.239: Destination host unreachable.
```

17. Z pozycji **PCKlienta** wykonaj pingowanie na **DRUKARKA-V20**, a następnie na **DRUKARKA-V10**. **PCKlient** nie powinien łączyć się z **DRUKARKA-V10**.

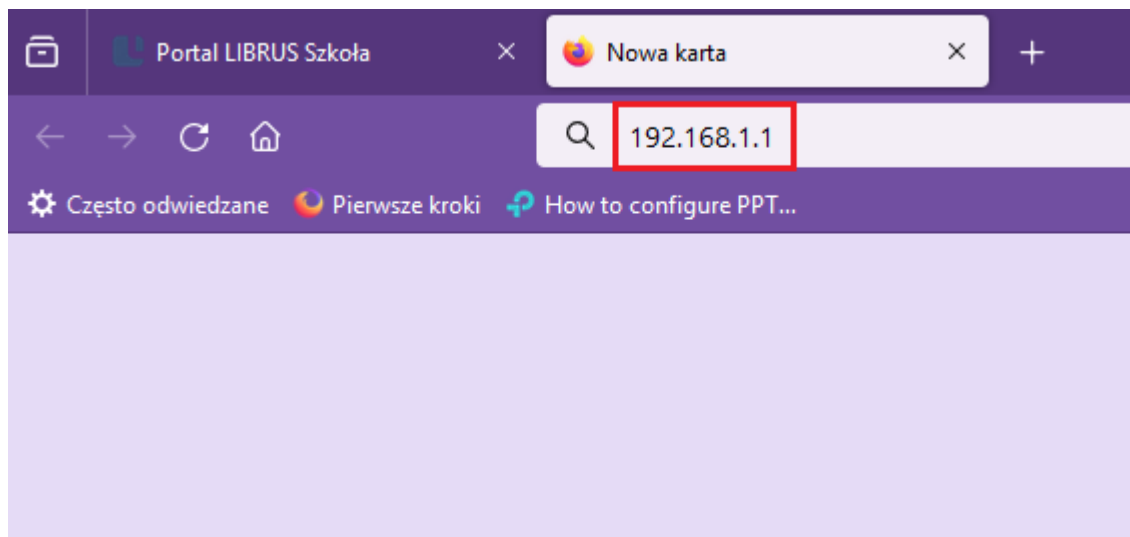
3.4 PROTOCOL VLAN

1. Wyłącz router czarny TL-WR940N. Ma być off.
2. Podłącz kable według poniższego schematu.

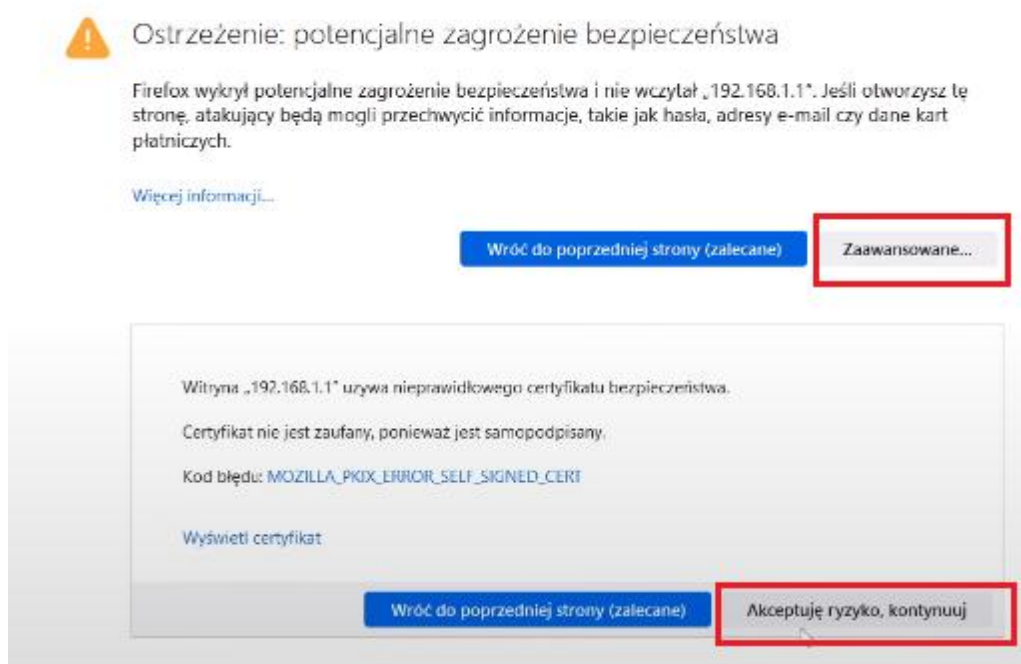
Figure 3-1 Network Topology



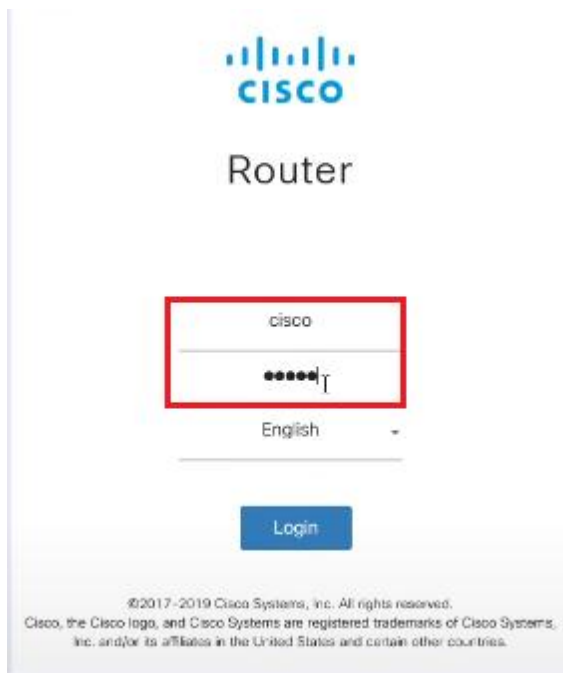
3. W pasku przeglądarki wpisz adres routera Cisco **192.168.1.1**.



4. Wyświetli się komunikat o ryzyku z powodu braku prawidłowego certyfikatu. Zaakceptuj ryzyko jak widać poniżej.



5. Zaloguj się na router:
Login: **cisco**
Hasło: **cisco**



6. Na routerze Cisco wejdź w zakładkę **VLAN** -> **VLAN SETTINGS** i edytuj **vlan1**.

RV340W-router6B2442

Getting Started
Status and Statistics
Administration
System Configuration
WAN
LAN
Port Settings
VLAN Settings
LAN/DHCP Settings
Static DHCP
802.1X Configuration
DNS Local Database
Router Advertisement
Wireless
Routing

VLAN Settings

+
Edit

VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask	IPv6 Address/Prefix Length
☒ 1	VLAN1	☒	☒	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149	fec0:1::1/64 DHCP Disabled

VLANs to Port Table

VLAN ID	LAN1	LAN2	LAN3	LAN4
1	U	U	U	U

U : Untagged, T : Tagged, E : Excluded

7. Wyłącz DHCP dla **IPv4** i włącz DHCP dla **IPv6**.

Getting Started
Status and Statistics
Administration
System Configuration
WAN
LAN
Port Settings
VLAN Settings
LAN/DHCP Settings
Static DHCP
802.1X Configuration
DNS Local Database
Router Advertisement
Wireless
Routing
Firewall
VPN

cisco (admin) English ? i ↻

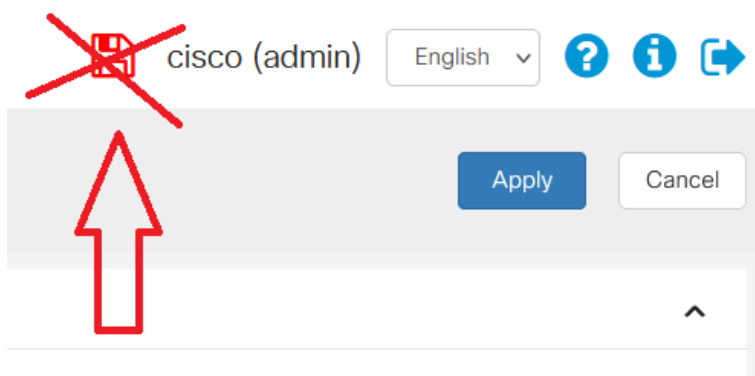
VLAN Settings

Apply **Cancel**

VLAN Table

VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask	IPv6 Address/Prefix Length
1	VLAN1	☒	☒	IPv4 Address: 192.168.1.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: ☒ Disabled ☐ Server ☐ Relay	Prefix: ☐ fec0:1:: ☐ Prefix from DHCP-PD Prefix Length: 64 Preview: [fec0:1:0:0:0:0:1] Interface Identifier: ☒ EUI-64 ☐ 1 DHCP Type: ☐ Disabled ☒ Server Lease Time: 1440 Range Start: fec0:1:: 2 Range End: fec0:1:: fe DNS Server: Use DNS Proxy

8. **Nie naciskaj czerwonej dyskiетки**, bo zapiszesz ustawienia na trwałe i trzeba będzie potem resetować router, a jest to trudne zadanie.



9. Włącz router czarny **TL-WR940N**. Odśwież kartę sieciową na **SERWERZE**. Interfejs sieciowy serwera powinien otrzymać adres z puli sieci **192.168.0.0/24**.
10. Zaloguj się na przełącznik 1, który zapewne jest już zresetowany.
11. Ustaw go na adres **192.168.0.11/24**
12. Ustaw opcję GENERAL na **portach 1,2,3** na **przełączniku 1**.

VLAN Config Port Config

VLAN Port Config

UNIT: 1 LAGS

Select	Port	Link Type	PVID	LAG	VLAN
☐		v			
☐	1/0/1	GENERAL	1	---	Detail
☐	1/0/2	GENERAL	1	---	Detail
☐	1/0/3	GENERAL	1	---	Detail
☐	1/0/4	ACCESS	1	---	Detail
☐	1/0/5	ACCESS	1	---	Detail
☐	1/0/6	ACCESS	1	---	Detail
☐	1/0/7	ACCESS	1	---	Detail
☐	1/0/8	ACCESS	1	---	Detail
☐	1/0/9	ACCESS	1	---	Detail
☐	1/0/10	ACCESS	1	---	Detail

All
Apply
Help

13. Ustaw **vlan 10** na **porty 1 i 3** w sekcji portów nietagowanych

VLAN Config Port Config

VLAN Info

VLAN ID: (2 - 4094)

Name : (16 characters maximum)

Untagged port

UNIT: 1 LAGS

☒ 1
☐ 2
☒ 3
☐ 4
☐ 5
☐ 6
☐ 7
☐ 8
☐ 9
☐ 10

All
Clear

Tagged port

UNIT: 1 LAGS

☐ 1
☐ 2
☐ 3
☐ 4
☐ 5
☐ 6
☐ 7
☐ 8
☐ 9
☐ 10

All
Clear
Apply
Help

☐ Unselected Port(s)
☒ Selected Port(s)
☐ Not Available for Selection

14. Teraz **vlan 20** na **porty 2 i 3** w sekcji portów nietagowanych

VLAN Info

VLAN ID: (2 - 4094)

Name : (16 characters maximum)

Untagged port

UNIT: LAGS☐ 1 ☒ 2 ☒ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10

All

Clear

Tagged port

UNIT: LAGS☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10

All

Clear

Apply

Help



Unselected Port(s)

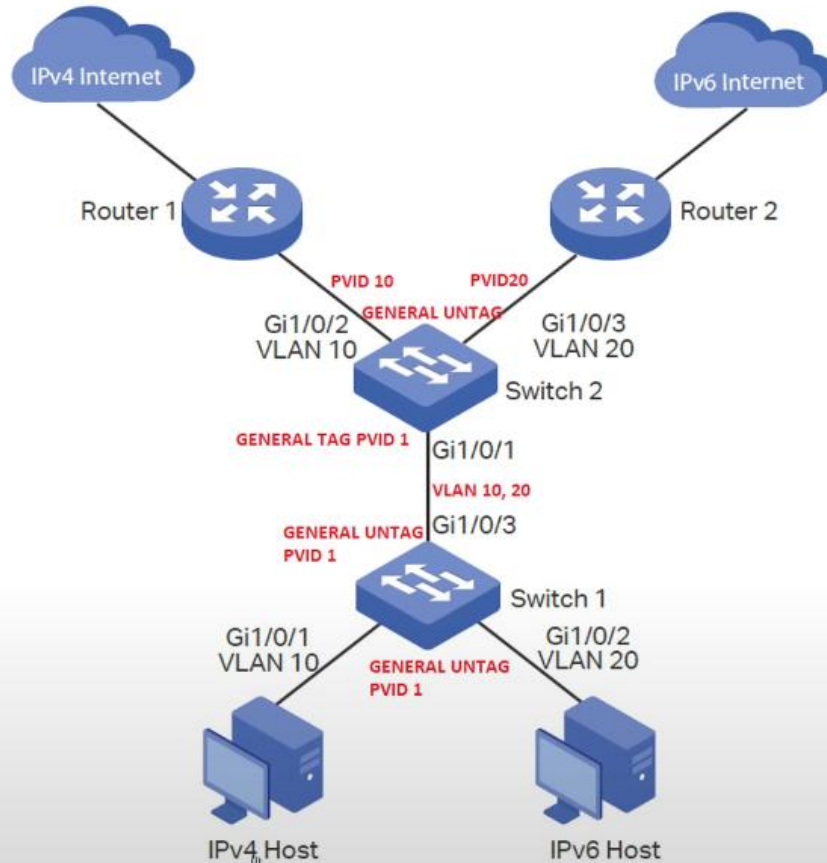


Selected Port(s)



Not Available for Selection

Figure 3-1 Network Topology



15. Zaloguj się na **przełącznik 2** i ustaw jego adres docelowy **192.168.0.12/24**
16. W zakładce **Port Config** ustaw opcję **GENERAL** na używane porty przełącznika 2 oraz ustaw **PVID 10** dla **portu 2** i **PVID 20** dla **portu 3**.

VLAN Config

Port Config

VLAN Port Config

UNIT: 1 LAGS

Select	Port	Link Type	PVID	LAG	VLAN
☐		▼			
☐	1/0/1	GENERAL	1	---	Detail
☐	1/0/2	GENERAL	10	---	Detail
☐	1/0/3	GENERAL	20	---	Detail
☐	1/0/4	ACCESS	1	---	Detail
☐	1/0/5	ACCESS	1	---	Detail
☐	1/0/6	ACCESS	1	---	Detail
☐	1/0/7	ACCESS	1	---	Detail
☐	1/0/8	ACCESS	1	---	Detail
☐	1/0/9	ACCESS	1	---	Detail
☐	1/0/10	ACCESS	1	---	Detail

All

Apply

Help

17. Ustaw **vlan 10** na **port 1** w sekcji portów tagowanych oraz **port 2** w sekcji portów nietagowanych.

VLAN Config Port Config

VLAN Info

VLAN ID: (2 - 4094)

Name : (16 characters maximum)

Untagged port

UNIT: LAGS

☐ 1 ☒ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10

Tagged port

UNIT: LAGS

☒ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10

☐ Unselected Port(s) ☒ Selected Port(s) ☐ Not Available for Selection

18.f

VLAN Config Port Config

VLAN Info

VLAN ID: (2 - 4094)

Name : (16 characters maximum)

Untagged port

UNIT: LAGS

☐ 1 ☐ 2 ☒ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10

Tagged port

UNIT: LAGS

☒ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10

☐ Unselected Port(s) ☒ Selected Port(s) ☐ Not Available for Selection

19. Wejdź w zakładkę **Protocol VLAN** i z menu poziomego wybierz zakładkę **Protocol Template**. Wprowadź brakujący w tabeli typ **86DD** protokołu **IPv6**. Zatwierdź konfigurację przyciskiem **Create**.

T2500G-10MPS

Protocol Group Table Protocol Group Protocol Template

Create Protocol Template

Protocol Name: (8 characters maximum)

Ether Type: (4 Hex integers, 0600-FFFF)

Create

Protocol Template Table

Select	ID	Protocol Name	Protocol type
☐	1	IP	0800
☐	2	ARP	0806
☐	3	RARP	8035
☐	4	IPX	8137
☐	5	AT	809B

All **Delete** **Help**

Protocol Group Table Protocol Group Protocol Template

Operation succeeded.

Create Protocol Template

Protocol Name: (8 characters maximum)

Ether Type: (4 Hex integers, 0600-FFFF)

Create

Protocol Template Table

Select	ID	Protocol Name	Protocol type
☐	1	IP	0800
☐	2	ARP	0806
☐	3	RARP	8035
☐	4	IPX	8137
☐	5	AT	809B
☐	6	IPv6	86DD

All **Delete** **Help**

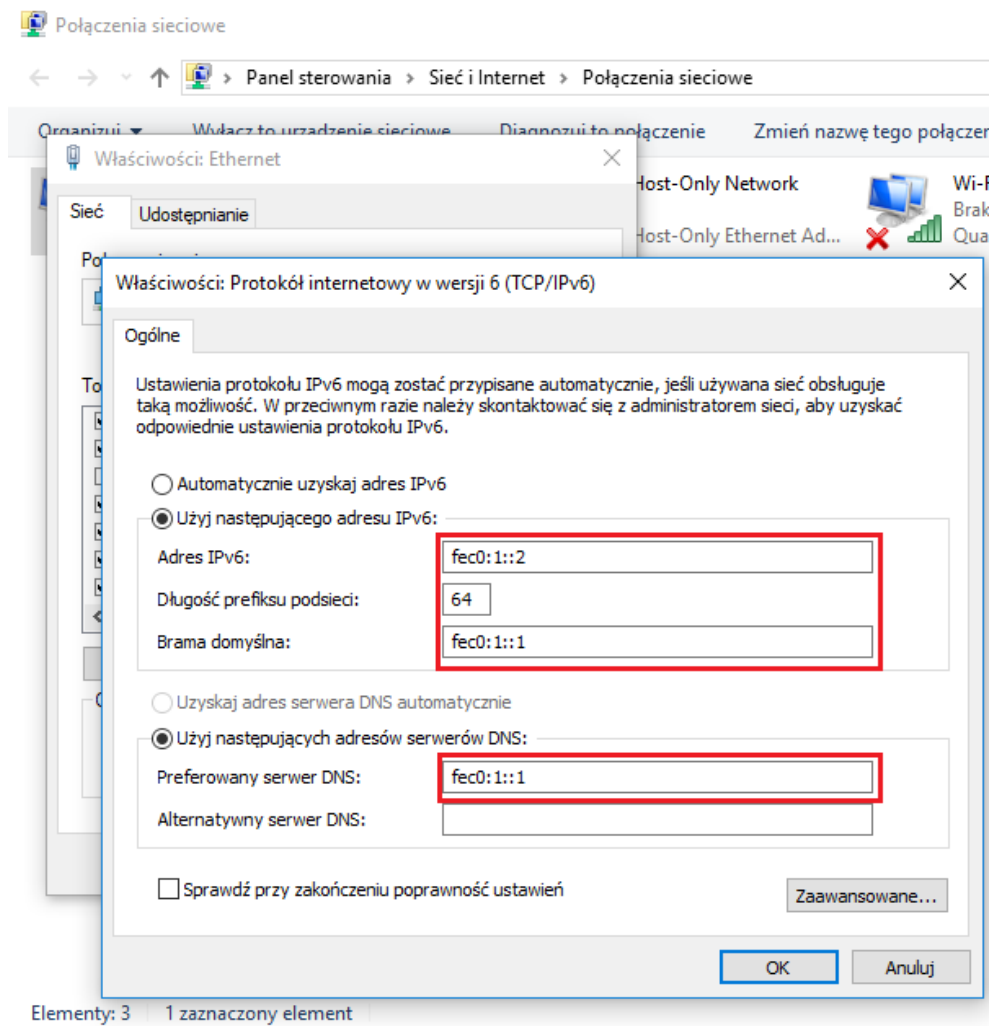
20. W zakładce Protocol Group powiąż protokół warstwy 3-ciej (Network Layer) z odpowiednim VLAN – Em.

The screenshot shows the 'Protocol Group' configuration page. At the top, there are three tabs: 'Protocol Group Table', 'Protocol Group', and 'Protocol Template'. The 'Protocol Group' tab is active. Below the tabs is a section titled 'Protocol Group Config'. It contains two fields: 'Protocol Name:' with a dropdown menu set to 'IP', and 'VLAN ID:' with a text input set to '10' and a range '(1-4094)' to its right. Below this is a section titled 'Protocol Group Member'. It contains a 'UNIT:' field set to '1' and 'LAGS'. Below the unit field is a row of 10 port selection buttons, numbered 1 to 10. Port 1 is highlighted with a blue icon. Below the port selection buttons are four buttons: 'All', 'Clear', 'Apply', and 'Help'. The 'Apply' button is highlighted with a red box. Below the buttons are three icons with labels: 'Unselected Port(s)' (light blue icon), 'Selected Port(s)' (dark blue icon), and 'Not Available for Selection' (grey icon).

The screenshot shows the 'Protocol Group' configuration page for IPv6. At the top, there are three tabs: 'Protocol Group Table', 'Protocol Group', and 'Protocol Template'. The 'Protocol Group' tab is active. Below the tabs is a section titled 'Protocol Group Config'. It contains two fields: 'Protocol Name:' with a dropdown menu set to 'IPv6', and 'VLAN ID:' with a text input set to '20' and a range '(1-4094)' to its right. Below this is a section titled 'Protocol Group Member'. It contains a 'UNIT:' field set to '1' and 'LAGS'. Below the unit field is a row of 10 port selection buttons, numbered 1 to 10. Port 1 is highlighted with a blue icon. Below the port selection buttons are four buttons: 'All', 'Clear', 'Apply', and 'Help'. The 'Apply' button is highlighted with a red box. Below the buttons are three icons with labels: 'Unselected Port(s)' (light blue icon), 'Selected Port(s)' (dark blue icon), and 'Not Available for Selection' (grey icon).

21. Na **SERWERZE** wyłącz i włącz kartę sieciową NIC1. Sprawdź czy karta otrzymała adres IPv4 z puli adresów routera czarnego **TL-WR940N** w sieci lokalnej **192.168.0.0/24** z bramą domyślną **192.168.0.1**.

22. Na PCKliencie ustaw statycznie IPv6 jak przedstawiono poniżej, a następnie wykonaj pingowanie na bramę domyślną (router Cisco) z adresem **fec0:1::1**.



```
Wiersz polecenia
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\user>ping -6
IP address must be specified.

C:\Users\user>ping -6 fec0:1::1

Pinging fec0:1::1 with 32 bytes of data:
Reply from fec0:1::1: time<1ms
Reply from fec0:1::1: time<1ms
Reply from fec0:1::1: time<1ms
Reply from fec0:1::1: time<1ms

Ping statistics for fec0:1::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

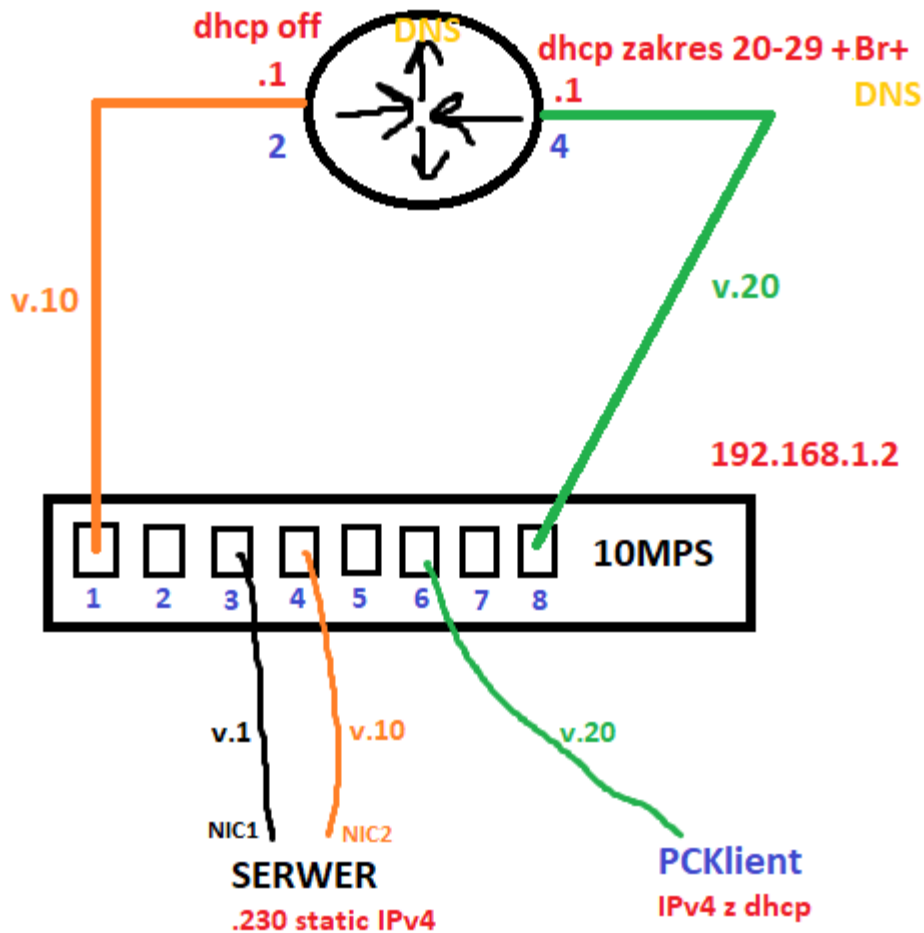
C:\Users\user>
```

3.5 ROUTER CISCO UMBRELLA RV240W

V.1 192.168.1.0/24

V.10 192.168.10.0/24

V.20 192.168.20.0/24



1. Podłącz kabel do portu **NIC1** SERWERA
2. Ustaw tymczasowy adres IPv4 na karcie **NIC1** np. **192.168.0.2/24** bez bramy domyślnej
3. Zaloguj się na przełącznik i ustaw adres docelowy **192.168.1.2/24**
4. Teraz ustaw na karcie **NIC1** adres IP v4 **192.168.1.230/24**
5. Podłącz router CISCO do przełącznika. Na routerze jest to **port 2**, na przełączniku **port 1**.
6. Zaloguj się na router.

Login: cisco

Pass.:cisco lub cisco1

7. Na SERWERZE ustaw **IPv4** na **NIC2**

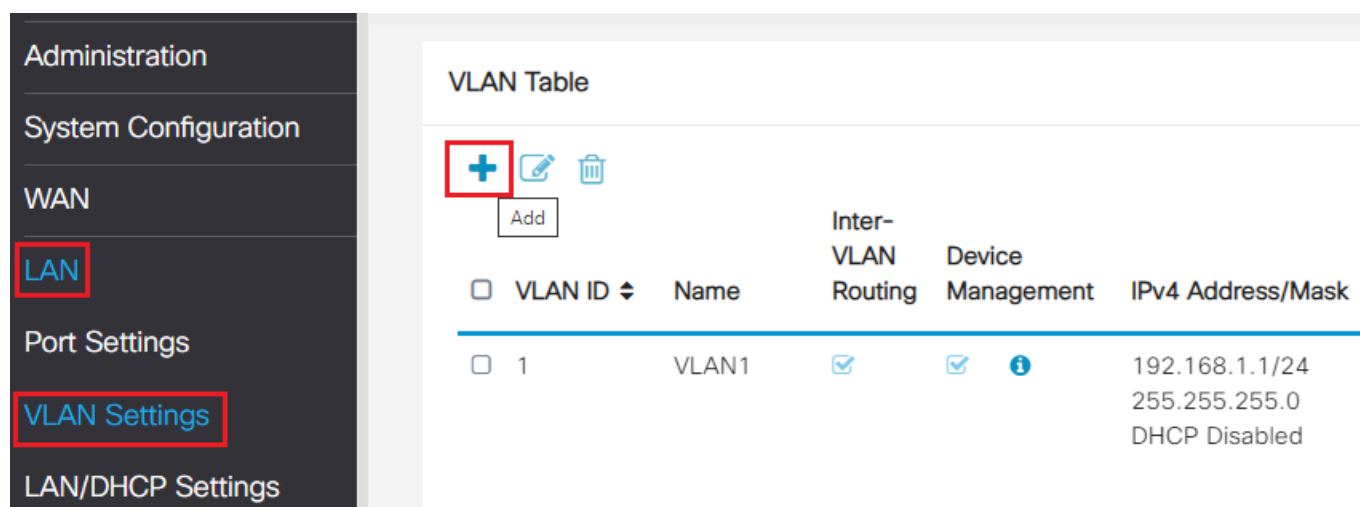
IPv4 192.168.10.230/24

Brama 192.168.10.1

DNS 192.168.10.1

8. Na routerze w zakładce **LAN** -> **VLAN Settings** utwórz vlany **10** i **20**

Aby utworzyć vlany w sekcji **VLAN Table** naciśnij plusik (+)



The screenshot shows the Mikrotik WinBox interface. On the left is a dark sidebar menu with the following items: Administration, System Configuration, WAN, LAN (highlighted with a red box), Port Settings, VLAN Settings (highlighted with a red box), and LAN/DHCP Settings. The main area on the right is titled 'VLAN Table'. At the top of this area are three icons: a plus sign (+) in a red box, a pencil icon, and a trash can icon. Below these icons is a table with the following columns: ☐ VLAN ID, Name, Inter-VLAN Routing, Device Management, and IPv4 Address/Mask. The table contains one entry: ☐ 1, VLAN1, a checked box for Inter-VLAN Routing, a checked box for Device Management, and an information icon (i). The IPv4 Address/Mask for this entry is 192.168.1.1/24, 255.255.255.0, and DHCP Disabled.

Następnie dodaj vlany

Status and Statistics

Administration

System Configuration

WAN

LAN

Port Settings

VLAN Settings

LAN/DHCP Settings

Static DHCP

802.1X Configuration

DNS Local Database

Router Advertisement

Wireless

Routing

Firewall

VPN

Security

QoS

VLAN Settings

☐ VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
☒ 10	VLAN10	☒	☐	IPv4 Address: 192.168.10.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: ☒ Disabled ☐ Server ☐ Relay
☒ 20	VLAN20	☒	☐	IPv4 Address: 192.168.20.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: ☐ Disabled ☒ Server ☐ Relay Lease Time: 1440 min. Range Start: 192.168.20.20 Range End: 192.168.20.29 DNS Server: Use DNS Proxy WINS Server: DHCP Options

WAN

LAN

Port Settings

VLAN Settings

LAN/DHCP Settings

Static DHCP

802.1X Configuration

DNS Local Database

Router Advertisement

Wireless

☐ VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask	IPv6 Address/Prefix Length
☐ 1	VLAN1	☒	☒	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149	fec0:1::1/64 DHCP Disabled
☐ 10	VLAN10	☒	☐	192.168.10.1/24 255.255.255.0 DHCP Disabled	fec0:2::1/64 DHCP Disabled
☐ 20	VLAN20	☒	☐	192.168.20.1/24 255.255.255.0 DHCP Server: 192.168.20.20-192.168.20.29	fec0:3::1/64 DHCP Disabled
☐ 2222	VLAN2222	☒	☐	192.168.2.1/24 255.255.255.0 DHCP Disabled	fec0:4::1/64 DHCP Disabled

VLAN SŁUP - dla przyjęcia trybu Untagged dla wybranego portu LAN routera

Zatwierdź konfigurację w prawym górnym rogu panelu konfiguracyjnego routera

cisco (admin) English ? i ↗

Apply

Cancel

Edytuj sekcję **VLANs to Port Table**

VLANs to Port Table

 Edit

VLAN	LAN1	LAN2	LAN3	LAN4
1	U	U	U	U

U : Untagged, T : Tagged, E : Excluded

Wszystkie porty routera w ramach vlanów **10** i **20** są tagowane (T) lub wyłączone (Excluded) niepotrzebne dla danego vlanu. Tryb Untagged ustaw dla VLAN-ów 1 i 2222 jak widać poniżej.

VLANs to Port Table



VLAN ID	LAN1	LAN2	LAN3	LAN4
1	U	U	U	E
10	E	T	E	E
20	E	E	E	T
2222	T	E	T	U

U : Untagged, T : Tagged, E : Excluded

jeden vlan zawsze musi być Untagged dla danego portu routera

Efekt po zatwierdzeniu konfiguracji

Wireless

Routing

Firewall

VPN

Security

QoS

Configuration Wizards

License

VLANs to Port Table

VLAN ID	LAN1	LAN2	LAN3	LAN4
1	U	U	U	U
10	E	T	E	E
20	E	E	E	T
2222	T	T	T	T

U : Untagged, T : Tagged, E : Excluded

9. Utwórz vlany 10 i 20 na przełączniku.

VLAN Config

Port Config

VLAN Info

VLAN ID: (2 - 4094)

Name : (16 characters maximum)

Untagged port

UNIT: LAGS

☒ 1 ☐ 2 ☐ 3 ☒ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10

All

Clear

Tagged port

UNIT: LAGS

☒ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10

All

Clear

Apply

Help



Unselected Port(s)



Selected Port(s)



Not Available for Selection

VLAN Info

VLAN ID: (2 - 4094)Name : (16 characters maximum)

Untagged port

UNIT: LAGS☒ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☒ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10

Tagged port

UNIT: LAGS☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☒ 8 ☐ 9 ☐ 10

Unselected Port(s)



Selected Port(s)



Not Available for Selection

VLAN Port Config

UNIT: LAGS

Select	Port	Link Type	PVID	LAG	VLAN
☐					
☐	1/0/1	TRUNK	1	---	Detail
☐	1/0/2	ACCESS	1	---	Detail
☐	1/0/3	ACCESS	1	---	Detail
☐	1/0/4	ACCESS	10	---	Detail
☐	1/0/5	ACCESS	1	---	Detail
☐	1/0/6	ACCESS	20	---	Detail
☐	1/0/7	ACCESS	1	---	Detail
☐	1/0/8	TRUNK	1	---	Detail
☐	1/0/9	ACCESS	1	---	Detail
☐	1/0/10	ACCESS	1	---	Detail

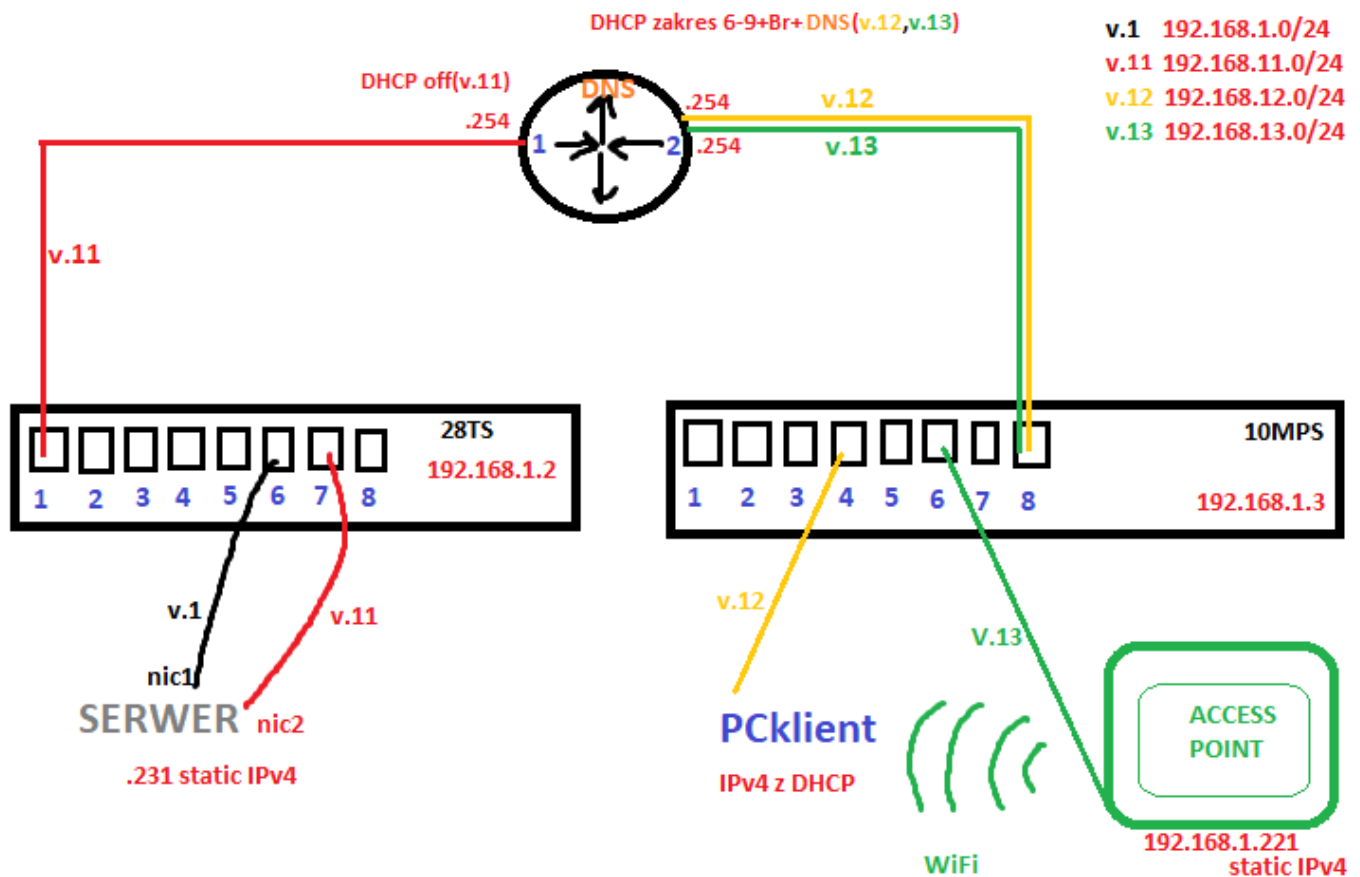
10.Sprawdź ustawienia karty sieciowej PCKlienta poleceniem **ipconfig**

11.Wykonaj pingowanie z SERWERA na PCKlienta z ustawioną flagą adresu źródłowego **[-S]**.

ping [-S srcaddr]

ping -S 192.168.10.230 192.168.20.X

3.6 ROUTER CISCO UMBRELLA RV240W + ACCESS POINT



1. Podłącz kabel do portu **NIC1** SERWERA
2. Ustaw tymczasowy adres IPv4 na karcie **NIC1** np. **192.168.0.2/24** bez bramy domyślnej
3. Zaloguj się na przełącznik **28TS** i ustaw adres docelowy **192.168.1.2/24**
4. Zaloguj się na przełącznik **10MPS** i ustaw adres docelowy **192.168.1.3/24**
5. Teraz ustaw na karcie **NIC1** adres IP v4 **192.168.1.230/24**
6. Podłącz router CISCO do przełącznika **28TS** . Na routerze jest to **port 1**, na przełączniku **port 1**.
7. Podłącz router CISCO do przełącznika **10MPS** . Na routerze jest to **port 2**, na przełączniku **port 8**.

8. Zaloguj się na router.

Login: cisco

Pass.:cisco lub cisco1

9. Na SERWERZE ustaw **IPv4** na **NIC2**

IPv4 192.168.11.231/24

Brama 192.168.11.254

DNS 192.168.11.254

10. Na routerze w zakładce **LAN** -> **VLAN Settings** utwórz vlany **11, 12, 13**

Aby utworzyć vlany w sekcji **VLAN Table** naciśnij plusik (+)

VLAN Table

☐	VLAN ID ↕	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask	IPv6 Address/Prefix Length
☐	1	VLAN1	☒	☒ ⓘ	192.168.1.1/24 255.255.255.0 DHCP Disabled	fec0:1::1/64 DHCP Disabled
☐	11	VLAN11	☒	☐ ⓘ	192.168.11.254/24 255.255.255.0 DHCP Disabled	fec0:2::1/64 DHCP Disabled
☐	12	VLAN12	☒	☐ ⓘ	192.168.12.254/24 255.255.255.0 DHCP Server: 192.168.12.6-192.168.12.9	fec0:3::1/64 DHCP Disabled
☐	13	VLAN13	☒	☐ ⓘ	192.168.13.254/24 255.255.255.0 DHCP Server: 192.168.13.6-192.168.13.9	fec0:4::1/64 DHCP Disabled

UWAGA!!!

Zalecane jest wykonać rezerwację DHCP dla Access Pointa w zakładce **LAN** -> **Static DHCP**, następnie wyłączyć i włączyć AP poprzez odpięcie od urządzenia kabla UTP i ponowne podpięcie. Access Point uzyskuje zasilanie na czterech żyłach kabla UTP w usłudze PoE.

Wszystkie porty routera w ramach vlanów **11**, **12**, **13** są tagowane (T), wyłącz (Excluded) niepotrzebne dla danego vlanu.

VLANs to Port Table

VLAN ID	LAN1	LAN2	LAN3	LAN4
1	U	U	U	U
11	T	E	E	E
12	E	T	E	E
13	E	T	E	E

U : Untagged, T : Tagged, E : Excluded

11. Utwórz vlan **11** na przełączniku **28TS**.

T2600G-28TS

System

Switching

VLAN

• 802.1Q VLAN

• MAC VLAN

• Protocol VLAN

• VLAN VPN

• GVRP

• Private VLAN

Spanning Tree

Ethernet OAM

Multicast

Routing

QoS

ACL

Network Security

SNMP

LLDP

Maintenance

VLAN Config

Port Config

VLAN Info

VLAN ID:11(1 - 4094)

Name :vlan11(16 characters maximum)

Untagged port

UNIT:1LAGS

246810121416182022242628

13579111315171921232527

AllClear

Tagged port

UNIT:1LAGS

246810121416182022242628

13579111315171921232527

AllClearApplyHelp

Unselected Port(s)

Selected Port(s)

Not Available for Selection

T2600G-28TS

VLAN Config Port Config

System

Switching

VLAN

• 802.1Q VLAN

• MAC VLAN

• Protocol VLAN

• VLAN VPN

• GVRP

• Private VLAN

Spanning Tree

Ethernet OAM

Multicast

Routing

QoS

ACL

Network Security

SNMP

LLDP

Maintenance

Save Config

VLAN Port Config

UNIT: 1 LAGS

Select	Port	Link Type	PVID	LAG	VLAN
☐		▼			
☐	1/0/1	TRUNK	1	---	Detail
☐	1/0/2	ACCESS	1	---	Detail
☐	1/0/3	ACCESS	1	---	Detail
☐	1/0/4	ACCESS	1	---	Detail
☐	1/0/5	ACCESS	1	---	Detail
☐	1/0/6	ACCESS	1	---	Detail
☐	1/0/7	ACCESS	11	---	Detail
☐	1/0/8	ACCESS	1	---	Detail
☐	1/0/9	ACCESS	1	---	Detail
☐	1/0/10	ACCESS	1	---	Detail
☐	1/0/11	ACCESS	1	---	Detail
☐	1/0/12	ACCESS	1	---	Detail
☐	1/0/13	ACCESS	1	---	Detail
☐	1/0/14	ACCESS	1	---	Detail
☐	1/0/15	ACCESS	1	---	Detail

All

Apply

Help

12. Utwórz vlany **12**, **13** na przełączniku **10MPS**.

T2500G-10MPS

VLAN Config Port Config

System

Switching

VLAN

• 802.1Q VLAN

• MAC VLAN

• Protocol VLAN

• VLAN VPN

• GVRP

Spanning Tree

Multicast

DHCP

QoS

PoE

ACL

Network Security

SNMP

LLDP

Maintenance

Save Config

Index

VLAN Info

VLAN ID: 12 (1 - 4094)

Name : vlan12 (16 characters maximum)

Untagged port

UNIT: 1 LAGS

1 2 3 4 5 6 7 8 9 10

All

Clear

Tagged port

UNIT: 1 LAGS

1 2 3 4 5 6 7 8 9 10

All

Clear

Apply

Help



Unselected Port(s)



Selected Port(s)



Not Available for Selection

T2500G-10MPS

System
Switching
VLAN

• 802.1Q VLAN

- MAC VLAN
- Protocol VLAN
- VLAN VPN
- GVRP

Spanning Tree

Multicast

DHCP

QoS

PoE

ACL

Network Security

SNMP

LLDP

Maintenance

VLAN Config

Port Config

VLAN Info

VLAN ID: (1 - 4094)

Name: (16 characters maximum)

Untagged port

UNIT: LAGS

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10

All

Clear

Tagged port

UNIT: LAGS

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10

All

Clear

Apply

Help



Unselected Port(s)



Selected Port(s)



Not Available for Selection

T2500G-10MPS

System

Switching

VLAN

• 802.1Q VLAN

- MAC VLAN
- Protocol VLAN
- VLAN VPN
- GVRP

Spanning Tree

Multicast

DHCP

QoS

PoE

ACL

Network Security

VLAN Config

Port Config

VLAN Port Config

UNIT: LAGS

Select	Port	Link Type	PVID	LAG
☐				
☐	1/0/1	ACCESS	1	---
☐	1/0/2	ACCESS	1	---
☐	1/0/3	ACCESS	1	---
☐	1/0/4	ACCESS	12	---
☐	1/0/5	ACCESS	1	---
☐	1/0/6	TRUNK	1	---
☐	1/0/7	ACCESS	1	---
☐	1/0/8	TRUNK	1	---
☐	1/0/9	ACCESS	1	---
☐	1/0/10	ACCESS	1	---

All

Apply

Help

13. Zaloguj się na router i edytuj **VLAN ID 1**

Administration

System Configuration

WAN

LAN

Port Settings

VLAN Settings

VLAN Table

+ [Edit] -

☐	VLAN ID ↕	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
☒	1	VLAN1	☒	☒	192.168.1.1/24 255.255.255.0 DHCP Disabled

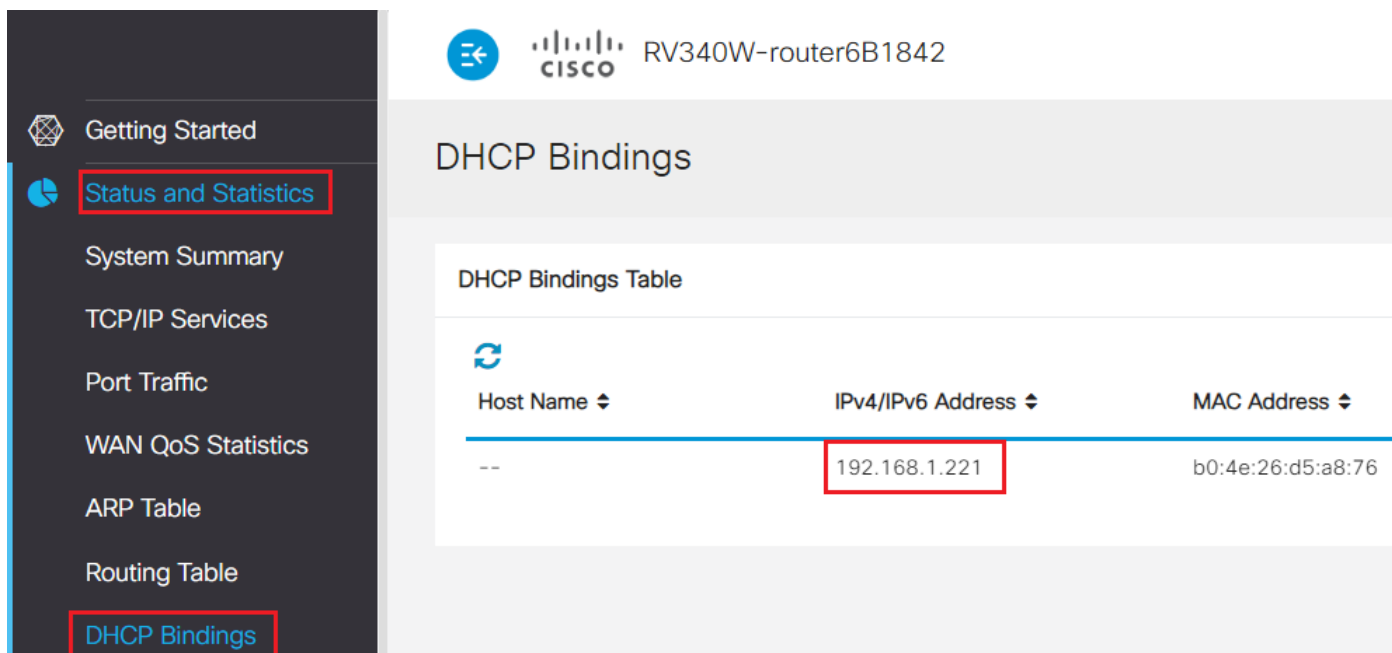
14. Tymczasowo włącz DHCP dla VLAN-u 1 i ustaw zakres jak na poniższym obrazku

VLAN Table

+ [Edit] -

☐	VLAN ID ↕	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
☒	1	VLAN1	☒	☒	IPv4 Address: 192.168.1.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: ☒ Server ☐ Disabled ☐ Relay Lease Time: 1440 min. Range Start: 192.168.1.221 Range End: 192.168.1.221 DNS Server: Use DNS Proxy

15. W zakładce **Status and Statistics/DHCP Binding** sprawdź przypisany adres 192.168.1.221 dla **EAP245**



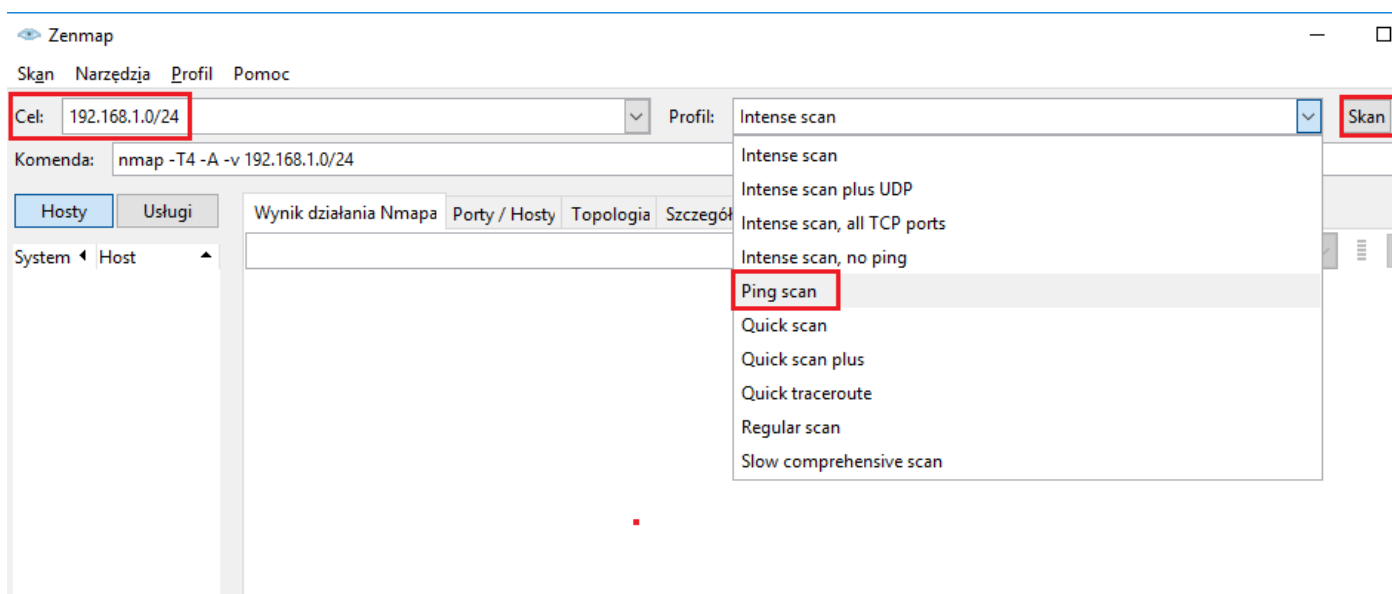
RV340W-router6B1842

DHCP Bindings

DHCP Bindings Table

Host Name	IPv4/IPv6 Address	MAC Address
--	192.168.1.221	b0:4e:26:d5:a8:76

16. Za pomocą programu **Zenmap** przeskanuj sieć 192.168.1.0/24 w poszukiwaniu **EAP245**.



Zenmap

Skonfiguruj Narzędzia Profil Pomoc

Cel: 192.168.1.0/24 Profil: Intense scan [Skan]

Komenda: nmap -T4 -A -v 192.168.1.0/24

Hosty Usługi Wynik działania Nmapa Porty / Hosty Topologia Szczegóły

System Host

- Intense scan
- Intense scan plus UDP
- Intense scan, all TCP ports
- Intense scan, no ping
- Ping scan
- Quick scan
- Quick scan plus
- Quick traceroute
- Regular scan
- Slow comprehensive scan

Zenmap

Skon Narzędzia Profil Pomoc

Cel: 192.168.1.0/24 Profil: Ping scan [Skon] [Anuluj]

Komenda: nmap -sn 192.168.1.0/24

Hosty Usługi

System Host

- router6B1842 (192.168.1.1)
- 192.168.1.2
- 192.168.1.3
- 192.168.1.199
- EAP245-B0-4E-26-D5-A8-76 (192.168.1.221)**

Wynik działania Nmapa Porty / Hosty Topologia Szczegóły hosta Skany

nmap -sn 192.168.1.0/24

Starting Nmap 7.80 (<https://nmap.org>) at 2024-03-06 16:22 ?rodkowoeuropejski czas stand.
Nmap scan report for router6B1842 (192.168.1.1)
Host is up (0.0020s latency).
MAC Address: BC:4A:56:6B:18:42 (Unknown)
Nmap scan report for 192.168.1.2
Host is up (0.0040s latency).
MAC Address: AC:84:C6:46:24:B9 (Tp-link Technologies)
Nmap scan report for 192.168.1.3
Host is up (0.0055s latency).
MAC Address: AC:84:C6:4A:9C:2C (Tp-link Technologies)
Nmap scan report for EAP245-B0-4E-26-D5-A8-76 (192.168.1.221)
Host is up (0.0050s latency).
MAC Address: B0:4E:26:D5:A8:76 (Tp-link Technologies)
Nmap scan report for 192.168.1.199
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.04 seconds

17. Zaloguje się na **ACCESS POINT** – a.

Login: **admin**

Pass: **admin**

192.168.1.221

Logowanie - System... Platforma edukacyjna Jak w PuTTY połącz... Jak wygenerować kl... Słownik łaciński - p... YouTube

tp-link | EAP245

Username

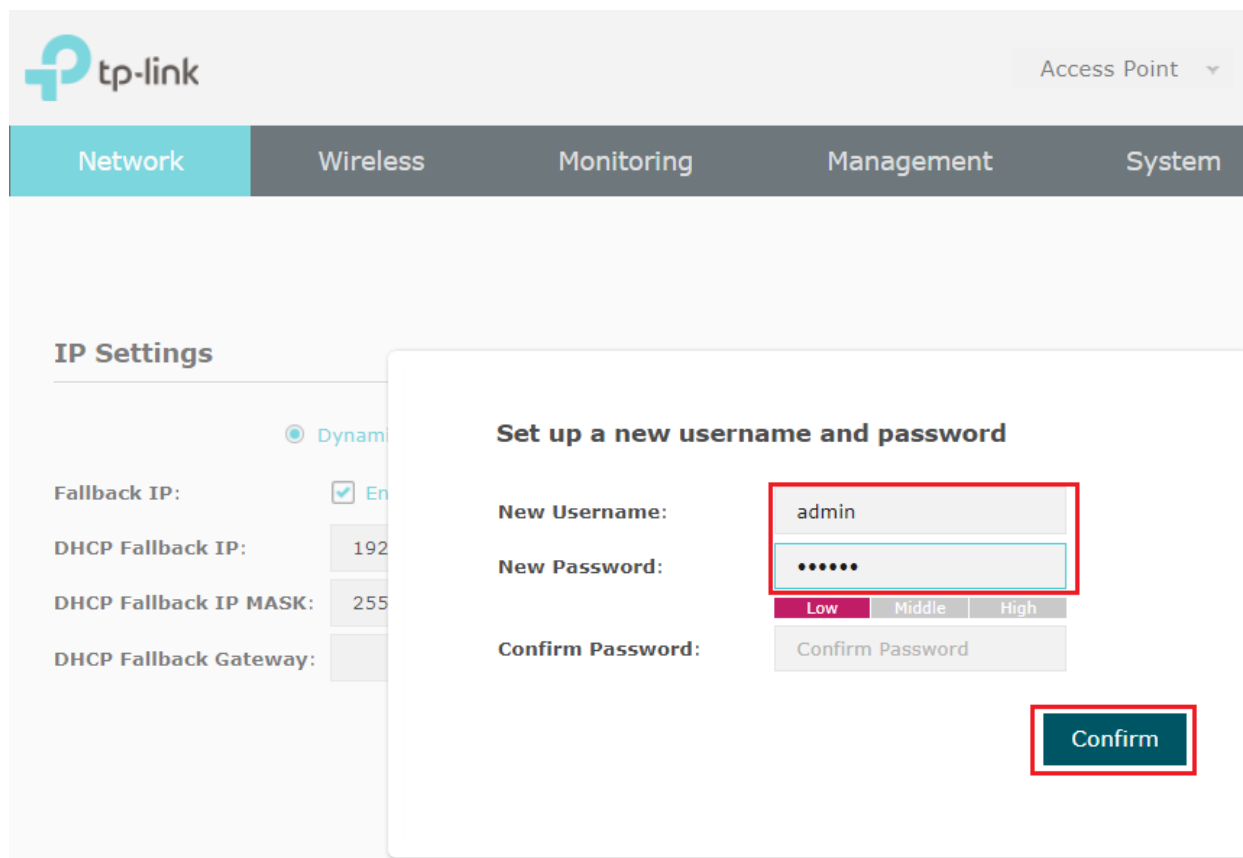
Password

LOGIN

18. Ustaw nowe hasło dostępu.

Login: **admin**

Pass: **admin1**



The image shows the TP-Link web interface. At the top, there is a header with the TP-Link logo and a dropdown menu labeled "Access Point". Below the header is a navigation bar with tabs: "Network", "Wireless", "Monitoring", "Management", and "System". The "Network" tab is selected. On the left side, under "IP Settings", there is a section for "Dynamic IP" with a radio button selected. Below this, there are fields for "Fallback IP:", "DHCP Fallback IP:", "DHCP Fallback IP MASK:", and "DHCP Fallback Gateway:". A modal window titled "Set up a new username and password" is open in the center. It contains three input fields: "New Username:" with the value "admin", "New Password:" with masked characters "•••••", and "Confirm Password:" with the placeholder "Confirm Password". Below the "New Password:" field, there are three buttons: "Low", "Middle", and "High". The "Confirm" button is located at the bottom right of the modal.

tp-link Access Point

Network Wireless Monitoring Management System

IP Settings

Dynamic IP

Fallback IP: ☒ Enable

DHCP Fallback IP: 192.168.1.1

DHCP Fallback IP MASK: 255.255.255.0

DHCP Fallback Gateway: 192.168.1.1

Set up a new username and password

New Username: admin

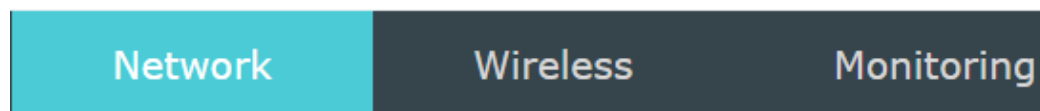
New Password: •••••

Low Middle High

Confirm Password: Confirm Password

Confirm

19. Ustaw IPv4 static EAP w zakładce **Network** -> **IP Settings**



IP Settings

☐ Dynamic ☒ Static

IP Address:

192.168.1.221

IP Mask:

255.255.255.0

Gateway:

192.168.1.1

Primary DNS:

192.168.1.1

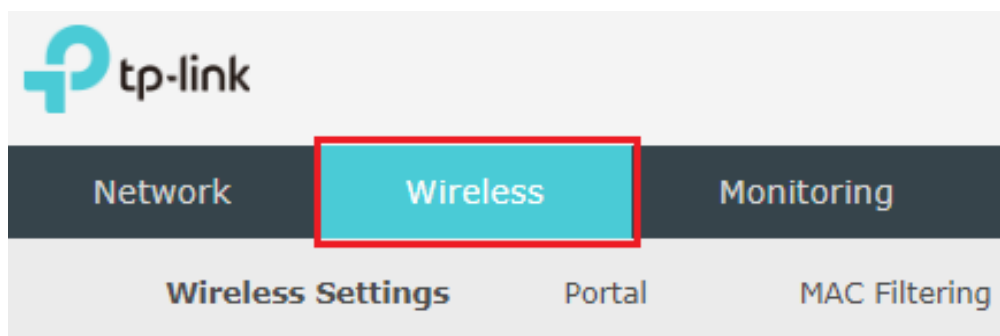
Secondary DNS:

0.0.0.0

(optional)

20. Wejdź w zakładkę **Wireless**. W sekcji **Wireless Basic Settings** dla **2.4GHz Wireless Ratio** ustaw:

- 802.11n Orly
- 40MHz
- Numer kanału zgodnie z numerem twojego stanowiska



Wireless Basic Settings

2.4GHz Wireless Radio: ☒ Enable

Wireless Mode: 802.11n only ▼

Channel Width: 40MHz ▼

Channel: 9 / 2452MHz ▼

Tx Power(EIRP): 19 dBm(10-19)

Note:

The EIRP transmit power includes the antenna gain.

21. W zakładce **Wireless**, w sekcji **SSIDs** edytuj dotychczasowy TP-Link_2.4GHz i ustaw:

- nową nazwę sieci bezprzewodowej na STANOWISKOX_2.4GHz
- vlan 13
- WPA-PSK -> WPA2-PSK
- Hasło: stanowiskoX

SSIDs

+ Add							
ID	SSID	Wireless VLAN ID	SSID Broadcast	Security Mode	Portal	SSID Isolation	Modify
1	TP-Link_2.4GHz_D5A876	0	Enable	None	Disable	Disable	Edit

Network

Wireless

Monitoring

Management

System

Wireless Settings

Portal

MAC Filtering

Scheduler

QoS

Rogue AP Detection

+ Add

ID	SSID	Wireless VLAN ID	SSID Broadcast	Security Mode	Portal	SSID Isolation	Modify
1	TP-Link_2.4GHz_D5A876	0	Enable	None	Disable	Disable	

SSID:

STANOWISK09_2.4GHz

Wireless VLAN ID:

13

(1-4094)

SSID Broadcast:

☒ Enable

Security Mode:

WPA-PSK

Version:

☐ Auto

☐ WPA-PSK

☒ WPA2-PSK

Encryption:

☒ Auto

☐ TKIP

☐ AES

Wireless Password:

stanowisko9

Group Key Update Period:

0

seconds (30-8640000. 0 means no update.)

Portal:

☐ Enable

SSID Isolation:

☐ Enable

Cancel

OK

SSIDs

+ Add

ID	SSID	Wireless VLAN ID	SSID Broadcast	Security Mode	Portal	SSID Isolation	Modify
1	STANOWISKO9_2.4GHz	13	Enable	WPA-PSK	Disable	Disable	 

22. W sekcji **Wireless Basic Settings** dla **5GHz Wireless Ratio** ustaw:

- 802.11ac only
- 80MHz
- Kanał 48 / 5240MHz



Network

Wireless

Monitoring

Wireless Settings

Portal

MAC Filtering

2.4GHz

5GHz

Wireless Basic Settings

5GHz Wireless Radio:	☒ Enable
Wireless Mode:	802.11ac only ▼
Channel Width:	80MHz ▼
Channel:	48 / 5240MHz ▼
Tx Power(EIRP):	23 dBm(11-23)

23. W zakładce **Wireless**, w sekcji **SSIDs** edytuj dotychczasowy TP-Link_5GHz i ustaw:

- nową nazwę sieci bezprzewodowej na STANOWISKOX_5GHz
- vlan 13
- WPA-PSK -> WPA2-PSK
- Hasło: stanowiskoX

Network	Wireless	Monitoring	Management	System
Wireless Settings	Portal	MAC Filtering	Scheduler	QoS
				Rogue AP Detection
Save				

SSIDs

+ Add

ID	SSID	Wireless VLAN ID	SSID Broadcast	Security Mode	Portal	SSID Isolation	Modify
1	STANOWISK09_5GHz	13	Enable	WPA-PSK	Disable	Disable	 

SSID: STANOWISK09_5GHz

Wireless VLAN ID: 13 (1-4094)

SSID Broadcast: ☒ Enable

Security Mode: WPA-PSK

Version: ☐ Auto ☐ WPA-PSK ☒ WPA2-PSK

Encryption: ☒ Auto ☐ TKIP ☐ AES

Wireless Password: stanowisko9

Group Key Update Period: 0 seconds (30-8640000. 0 means no update.)

Portal: ☐ Enable

SSID Isolation: ☐ Enable

Cancel OK

SSIDs

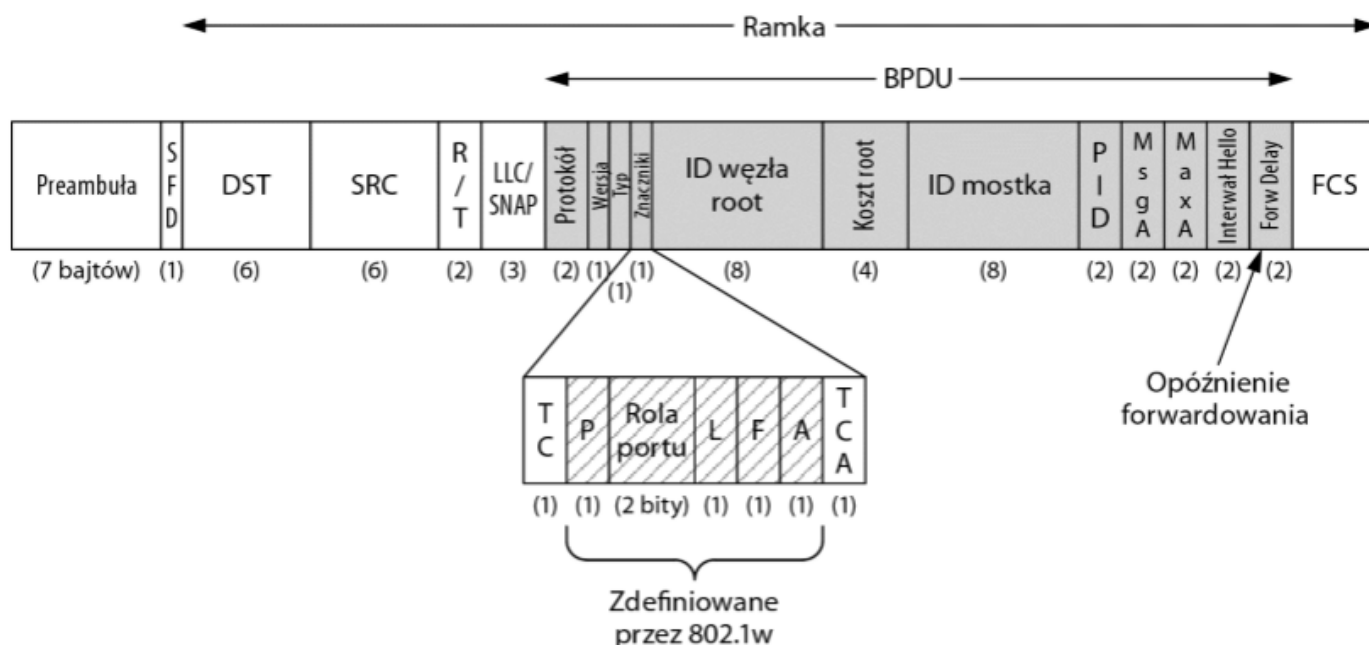
+ Add

ID	SSID	Wireless VLAN ID	SSID Broadcast	Security Mode	Portal	SSID Isolation	Modify
1	STANOWISK09_5GHz	13	Enable	WPA-PSK	Disable	Disable	 

24. Podłącz **PCKlienta** do sieci bezprzewodowej STANOWISKOX_2.4GHz
25. Sprawdź poleceniem **ping** połączenie bezprzewodowej karty sieciowej **PCKlienta** z bramą domyślną routera w ramach segmentu sieci należącego do vlanu 13.
26. Sprawdź poleceniem **ping** połączenie **SERWERA** z **PCKlientem**.

3.7 Protokół drzewa rozpinającego STP

Budowa ramki BPDU



Na powyższym obrazku przedstawiono format ramek BPDU, wymienianych między mostkami w ramach budowania drzewa rozpinającego przez protokół STP; jest to format wspólny dla obu wersji protokołów: klasycznej (STP) i ulepszonej (RSTP).

Ramki BPDU wysyłane są na adres grupowy 01:80:C2:00:00:00, a przejście ramki przez mostek zawsze wiąże się z jej modyfikacją.

Znaczenie pól DST, SRC i R/T jest takie samo jak w klasycznym formacie ramki ethernetowej 802.3 — pole R/T zawiera wartość 38 (dziesiętnie), czyli rozmiar ładunku użytecznego (rozpoczynającego się od pola LLC/SNAP).

W 3-bajtowym polu LLC/SNAP znajduje się stała 0x424203, zdefiniowana dla ramek BPDU przez standard 802.1 (niektóre ramki BPDU nie wykorzystują tego pola).

Pole Protokół ma wartość 0, pole Wersja zawiera 0 albo 2, zależnie od wersji protokołu (odpowiednio STP albo RSTP), na podobnej zasadzie ustalana jest wartość pola Typ.

W polu znaczników obecne są bity związane ze zmianą topologii sieci (zgodnie ze standardem 802.1d:

TC — Topology Change i TCA — Topology Change Acknowledgment)

propozycją (P — Proposal)

- rolą portu (00 — nieznana, 01 — alternatywny, 10 — główny, 11 — wyznaczony), uczeniem mostka (L — Learning), forwardowaniem ramek (F — Forwarding) i negocjowaniem (A — Agreement);
- ID węzła root to identyfikator domniemywany przez nadawcę ramki, zaś analogiczny identyfikator nadawcy znajduje się w polu ID mostka root; oba identyfikatory stanowią konkatenację 2-bajtowego priorytetu i adresu MAC.
- Wartość w polu Koszt root wyliczana jest jako koszt drogi prowadzącej od mostka nadawcy do mostka root (koszt rozumiany jako suma kosztu łączy leżących na tej drodze).
- Identyfikator mostka ma kluczowe znaczenie w procesie wyboru mostka root, manipulowanie wspomnianym priorytetem (stanowiącym bardziej znaczącą część identyfikatora) jest podstawowym sposobem preferowania konkretnych mostków w tej roli przez oprogramowanie zarządzające
- W polu PID znajduje się identyfikator (numer) portu, przez który mostek nadawca wysłał ramkę, skonkatenowany z 1-bajtowym polem priorytetu (o domyślnej wartości 0x80).

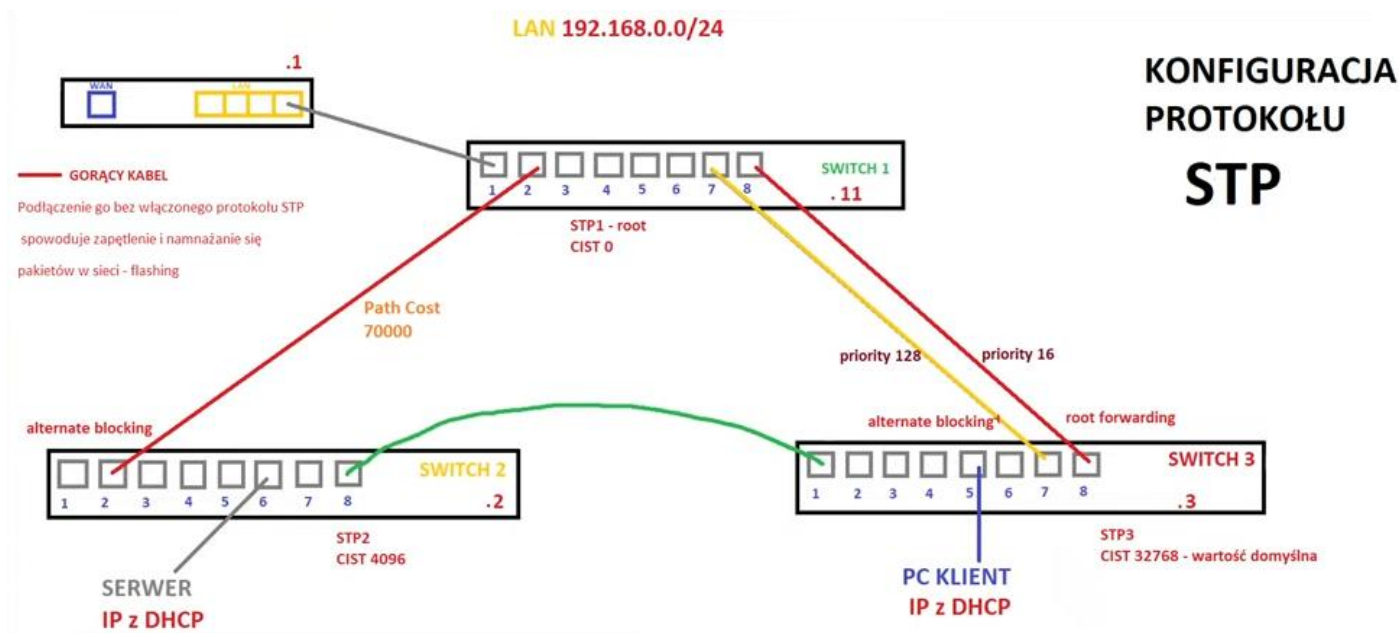
Następne pola związane są z czasowymi uwarunkowaniami transmisji ramek:

- Pole MsgA zawiera wartość odzwierciedlającą upływ „czasu życia” ramki
- W polu MaxA definiowany jest interwał przeterminowania (domyślnie 20 sekund)
- Wartość pola Interwał Hello określa interwał czasowy ponawiania okresowej transmisji ramek konfiguracyjnych
- Wartość pola Opóźnienie forwardowania (Forw Delay) określa długość pozostawiania portu w stanie „uczący się” lub „nasłuchujący”.

Wszystkie wartości czasowe wyrażane są w jednostkach równych 1/256 sekundy.

Pole MsgA, w odróżnieniu od innych pól czasowych, nie ma ustalonej wartości. W ramce BPDU wysyłanej przez mostek root pole ma to wartość 0; przy przejściu ramki przez każdy kolejny mostek wartość tego pola jest zwiększana o 1 (z wyjątkiem przypadku, gdy jej wysłanie następuje przez port uważany za prowadzący do mostka root). W rzeczywistości zatem pole to jest licznikiem przeskoków, czyli mostków pośrednich, przez które przeszła dotychczas ramka od momentu wygenerowania jej przez mostek root.

Gdy ramka BPDU odbierana jest przez mostek, zawarta w niej informacja gromadzona jest na potrzeby algorytmu STP i usuwana po okresie przeterminowania równym $\text{MaxA} - \text{MsgA}$ — jeżeli w tym czasie nie nadejdzie do mostka ramka przez port główny, dotychczasowy mostek root potraktowany zostaje jako „martwy” i ponownie uruchamiany jest proces jego elekcji.



1. Podłącz kable według powyższego schematu, przy czym kable czerwone powinny wisieć.
2. Ustaw adresy IPv4 przełączników sieciowych. Router powinien pracować na fabrycznych ustawieniach.
3. Na **SWITCH1** wejdź w zakładkę **Spanning Tree**.



17. Ustaw **CIST Priority** na 0.

TP-LINK®

TL-SG3210

System

Switching

VLAN

Spanning Tree

• STP Config

• Port Config

• MSTP Instance

• STP Security

Multicast

QoS

ACL

Network Security

SNMP

Cluster

Maintenance

Save Config

STP Config

STP Summary

Global Config

STP:

☐ Enable
 ☒ Disable

Version:

STP

Apply

Parameters Config

CIST Priority:

0

(0-61440)

Hello Time:

2

sec (1-10)

Max Age:

20

sec (6-40)

Forward Delay:

15

sec (4-30)

TxHoldCount:

5

pps (1-20)

Max Hops:

20

hop (1-40)

Apply

Help

18.Na SWITCH2 ustaw CIST Priority na 4096.

tp-link

T2600G-28TS

System

Switching

VLAN

Spanning Tree

• STP Config

• Port Config

• MSTP Instance

• STP Security

Ethernet OAM

Multicast

Routing

QoS

ACL

Network Security

SNMP

STP Config

STP Summary

Global Config

Spanning-Tree :

☐ Enable
 ☒ Disable

Mode :

STP

Apply

Parameters Config

CIST Priority :

4096

(0-61440, in increments of 4096)

Hello Time :

2

sec (1-10)

Max Age :

20

sec (6-40)

Forward Delay :

15

sec (4-30)

TxHoldCount :

5

pps (1-20)

Max Hops :

20

hop (1-40)

Apply

Help

19.Na SWITCH3 pozostaw CIST Priority na 32768.

T2600G-28TS

STP Config

STP Summary

Operation succeeded.

Global Config

Spanning-Tree :

☐ Enable
☒ Disable

Apply

Mode :

STP

Parameters Config

CIST Priority :

32768

(0-61440, in increments of 4096)

Hello Time :

2

sec (1-10)

Max Age :

20

sec (6-40)

Forward Delay :

15

sec (4-30)

TxHoldCount :

5

pps (1-20)

Max Hops :

20

hop (1-40)

Apply

Help

System

Switching

VLAN

Spanning Tree

• STP Config

• Port Config

• MSTP Instance

• STP Security

Ethernet OAM

Multicast

Routing

QoS

ACL

Network Security

SNMP

20.Na **SWITCH1** wejdź w zakładkę **Spanning Tree/Port Config**.

TL-SG3210

Port Config

Port Config

Select	Port	Status	Priority
☐		Disable ▾	
☐	1	Disable	128
☐	2	Disable	128
☐	3	Disable	128
☐	4	Disable	128
☐	5	Disable	128
☐	6	Disable	128
☐	7	Disable	128
☐	8	Disable	128
☐	9	Disable	128
☐	10	Disable	128

System

Switching

VLAN

Spanning Tree

• STP Config

• Port Config

• MSTP Instance

• STP Security

Multicast

QoS

ACL

Network Security

SNMP

Cluster

Maintenance

21. Zaznacz porty, do których podłączone są kable i wybierz z listy rozwijanej status **Enable**.

TL-SG3210

Port Config

Port Config

Select	Port	Status	Priority	ExtPath Cost	IntPath Cost	Edge Port	P2P Lin
☐		▼				▼	
☒	1	▼	128	Auto	Auto	Disable	Auto
☒	2	Disable	128	Auto	Auto	Disable	Auto
☐	3	Enable	128	Auto	Auto	Disable	Auto
☐	4	Disable	128	Auto	Auto	Disable	Auto
☐	5	Disable	128	Auto	Auto	Disable	Auto
☐	6	Disable	128	Auto	Auto	Disable	Auto
☒	7	Disable	128	Auto	Auto	Disable	Auto
☒	8	Disable	128	Auto	Auto	Disable	Auto
☐	9	Disable	128	Auto	Auto	Disable	Auto
☐	10	Disable	128	Auto	Auto	Disable	Auto

Apply **Refresh**

22. Ustaw status **Enable** w kolumnie **Edge Port** dla **portu 1**, do którego podłączony jest router.

TL-SG3210

Port Config

Port Config

Select	Port	Status	Priority	ExtPath Cost	IntPath Cost	Edge Port	P2P Lin
☐	1	Enable ▼	128	Auto	Auto	Disable ▼	Auto
☒	1	Enable	128	Auto	Auto	▼	Auto
☐	2	Enable	128	Auto	Auto	Disable	Auto
☐	3	Disable	128	Auto	Auto	Enable	Auto
☐	4	Disable	128	Auto	Auto	Disable	Auto
☐	5	Disable	128	Auto	Auto	Disable	Auto
☐	6	Disable	128	Auto	Auto	Disable	Auto
☐	7	Enable	128	Auto	Auto	Disable	Auto
☐	8	Enable	128	Auto	Auto	Disable	Auto
☐	9	Disable	128	Auto	Auto	Disable	Auto
☐	10	Disable	128	Auto	Auto	Disable	Auto

Apply **Refresh**

10.Ustaw **Priority** dla **portu 8** z wartością **16**.

TL-SG3210

System

Switching

VLAN

Spanning Tree

• STP Config

• **Port Config**

• MSTP Instance

• STP Security

Multicast

QoS

ACL

Network Security

SNMP

Cluster

Maintenance

Port Config

Port Config

Select	Port	Status	Priority	ExtPath Cost	IntPath Cost	Edge Port	P2P Lin
☐	8	Enable ▾	16	Auto	Auto	Disable ▾	Auto
☐	1	Enable	128	Auto	Auto	Enable	Auto
☐	2	Enable	128	Auto	Auto	Disable	Auto
☐	3	Disable	128	Auto	Auto	Disable	Auto
☐	4	Disable	128	Auto	Auto	Disable	Auto
☐	5	Disable	128	Auto	Auto	Disable	Auto
☐	6	Disable	128	Auto	Auto	Disable	Auto
☐	7	Enable	128	Auto	Auto	Disable	Auto
☒	8	Enable	128	Auto	Auto	Disable	Auto
☐	9	Disable	128	Auto	Auto	Disable	Auto
☐	10	Disable	128	Auto	Auto	Disable	Auto

Apply

Refresh

Port Config

Select	Port	Status	Priority
☐		Disable ▾	
☐	1	Enable	128
☐	2	Enable	128
☐	3	Disable	128
☐	4	Disable	128
☐	5	Disable	128
☐	6	Disable	128
☐	7	Enable	128
☐	8	Enable	16
☐	9	Disable	128
☐	10	Disable	128

11. Ustaw koszt połączenia na **70000** dla **portu 2**.

TL-SG3210

System

Switching

VLAN

Spanning Tree

• STP Config

• **Port Config**

• MSTP Instance

• STP Security

Multicast

QoS

ACL

Network Security

SNMP

Cluster

Maintenance

Port Config

Port Config

Select	Port	Status	Priority	ExtPath Cost	IntPath Cost	Edge Port	P2P Link
☐	2	Enable ▾	128	70000	70000	Disable ▾	Auto
☐	1	Enable	128	Auto	Auto	Enable	Auto
☒	2	Enable	128	Auto	Auto	Disable	Auto
☐	3	Disable	128	Auto	Auto	Disable	Auto
☐	4	Disable	128	Auto	Auto	Disable	Auto
☐	5	Disable	128	Auto	Auto	Disable	Auto
☐	6	Disable	128	Auto	Auto	Disable	Auto
☐	7	Enable	128	Auto	Auto	Disable	Auto
☐	8	Enable	16	Auto	Auto	Disable	Auto
☐	9	Disable	128	Auto	Auto	Disable	Auto
☐	10	Disable	128	Auto	Auto	Disable	Auto

Apply

Refresh

Operation successful.

Port Config

Select	Port	Status	Priority	ExtPath Cost	IntPath Cost	Edge Port	P2P Link
☐		Disable ▾				Disable ▾	Auto
☐	1	Enable	128	Auto	Auto	Enable	Auto
☐	2	Enable	128	70000	70000	Disable	Auto
☐	3	Disable	128	Auto	Auto	Disable	Auto
☐	4	Disable	128	Auto	Auto	Disable	Auto
☐	5	Disable	128	Auto	Auto	Disable	Auto
☐	6	Disable	128	Auto	Auto	Disable	Auto
☐	7	Enable	128	Auto	Auto	Disable	Auto
☐	8	Enable	16	Auto	Auto	Disable	Auto
☐	9	Disable	128	Auto	Auto	Disable	Auto
☐	10	Disable	128	Auto	Auto	Disable	Auto

Apply

Refresh

12. Na **SWITCH 2** wejdź w zakładkę **Spanning Tree/Port Config**.
13. Zaznacz porty, do których podłączone są kable i wybierz z listy rozwijanej status **Enable**.
14. Ustaw status **Enable** w kolumnie **Edge Port** dla **portu 6**, do którego podłączony jest **SERWER**.
15. Ustaw koszt połączenia na **70000** dla **portu 2**.
16. Na **SWITCH 3** wejdź w zakładkę **Spanning Tree/Port Config**.
17. Zaznacz porty, do których podłączone są kable i wybierz z listy rozwijanej status **Enable**.
18. Ustaw status **Enable** w kolumnie **Edge Port** dla **portu 5**, do którego podłączony jest **PCKLIENT**.
19. Ustaw **Priority** dla **portu 8** z wartością **16**.
20. Teraz na każdym przełączniku włącz protokół STP w głównym panelu sterowania pod nazwą **Global Config**.



21. Podłącz wszystkie kable i poczekaj 50 sekund. Jeżeli przełączniki nie flaszują, znaczy to, że w konfiguracji STP nie dochodzi do zapętleń.
22. Na każdym przełączniku, w zakładce **Spanning Tree/Port Config** sprawdź stan połączeń.

SWITCH 1

TL-SG3210

- System
- Switching
- VLAN
- Spanning Tree
 - STP Config
 - **Port Config**
 - MSTP Instance
 - STP Security
- Multicast
- QoS
- ACL
- Network Security
- SNMP
- Cluster
- Maintenance
- Save Config

Port Config

Port Config

Port

Select	Port	Status	Priority	ExtPath Cost	IntPath Cost	Edge Port	P2P Link	MCheck	STP Version	Port Role	Port Status
☐		Disable				Disable	Auto	Unchange			
☐	1	Enable	128	20000(Auto)	20000(Auto)	Enable	Enable(Auto)	---	STP	Designated	Forwarding
☐	2	Enable	128	70000	70000	Disable	Enable(Auto)	---	STP	Designated	Forwarding
☐	3	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---
☐	4	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---
☐	5	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---
☐	6	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---
☐	7	Enable	128	20000(Auto)	20000(Auto)	Disable	Enable(Auto)	---	STP	Designated	Forwarding
☐	8	Enable	16	20000(Auto)	20000(Auto)	Disable	Enable(Auto)	---	STP	Designated	Forwarding
☐	9	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---
☐	10	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---

Apply
Refresh
Help

SWITCH 2

T2600G-28TS

- System
- Switching
- VLAN
- Spanning Tree
 - STP Config
 - **Port Config**
 - MSTP Instance
 - STP Security
- Ethernet OAM
- Multicast
- Routing
- QoS
- ACL
- Network Security
- SNMP
- LLDP
- Maintenance
- Save Config
- Index

Port Config

Port Config

UNIT: 1 LAGS

Select	Port	Status	Priority	Ext-Path Cost	Int-Path Cost	Edge Port	P2P Link	MCheck	Port Mode	Port Role	Port Status	LAG
☐												
☐	1/0/1	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
☐	1/0/2	Enable	128	70000	70000	Disable	Open(Auto)	---	STP	Alternate	Blocking	---
☐	1/0/3	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
☐	1/0/4	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
☐	1/0/5	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
☐	1/0/6	Enable	128	20000(Auto)	20000(Auto)	Enable	Open(Auto)	---	STP	Designated	Forwarding	---
☐	1/0/7	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
☐	1/0/8	Enable	128	20000(Auto)	20000(Auto)	Disable	Open(Auto)	---	STP	Root	Forwarding	---
☐	1/0/9	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
☐	1/0/10	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
☐	1/0/11	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
☐	1/0/12	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
☐	1/0/13	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
☐	1/0/14	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
☐	1/0/15	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---

All
Apply
Refresh
Help

SWITCH 3

T2600G-28TS

- System
- Switching
- VLAN
- Spanning Tree
 - STP Config
 - **Port Config**
 - MSTP Instance
 - STP Security
- Ethernet OAM
- Multicast
- Routing
- QoS
- ACL
- Network Security
- SNMP
- LLDP
- Maintenance
- Save Config
- Index

Port Config

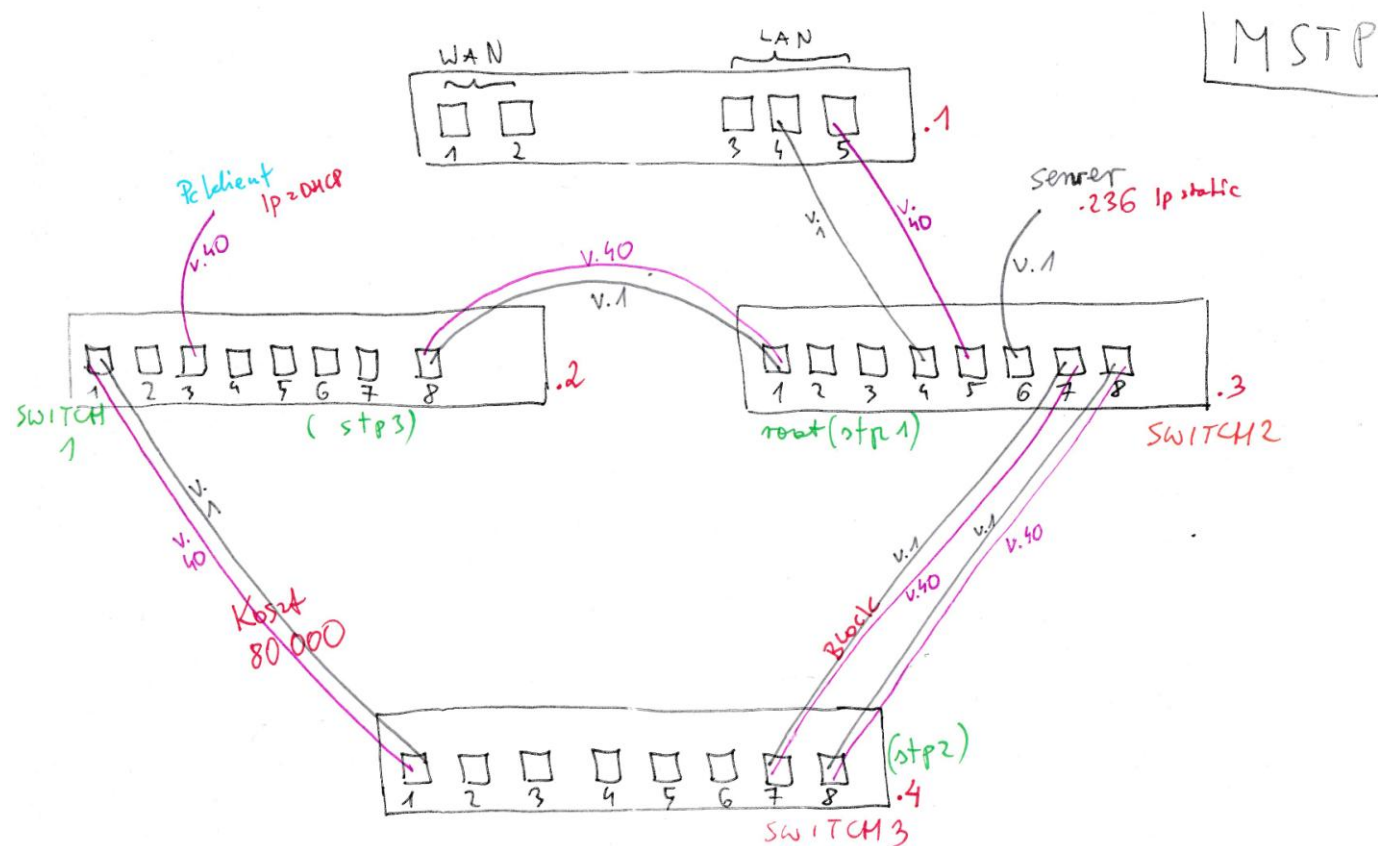
Port Config

1 LAGS

rt	Status	Priority	Ext-Path Cost	Int-Path Cost	Edge Port	P2P Link	MCheck	Port Mode	Port Role	Port S
/1	Enable	128	20000(Auto)	20000(Auto)	Disable	Open(Auto)	---	STP	Designated	Forwa
/2	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---
/3	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---
/4	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---
/5	Enable	128	200000(Auto)	200000(Auto)	Enable	Open(Auto)	---	STP	Designated	Forwa
/6	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---
/7	Enable	128	20000(Auto)	20000(Auto)	Disable	Open(Auto)	---	STP	Alternate	Bloc
/8	Enable	16	20000(Auto)	20000(Auto)	Disable	Open(Auto)	---	STP	Root	Forwa
/9	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---
10	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---
11	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---
12	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---
13	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---
14	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---
15	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---

All
Apply
Refresh
Help

3.8 Protokół drzewa rozpinającego MSTP



Krok1

Network

- WAN
- LAN
- IPTV
- MAC
- Switch
- VLAN**
- IPv6

Preferences

Transmission

Firewall

Behavior Control

VPN

Authentication

Services

System Tools

Logout

Copyright © 2018

TP-Link Technologies Co., Ltd.

All rights reserved.

+

 Add

-

 Delete

ID	VLAN ID	Name	Ports	Description	Operation
1	1	vlan1	3(UNTAG) 4(UNTAG) 5(UNTAG)	Default Vlan For LAN	

VLAN ID:

1

(1-4094)

Name:

vlan1

(1-50 characters)

Ports:

1

TAG

2

TAG

3

UNTAG

4

UNTAG

5

UNTAG

Description:

Default Vlan For LAN

(1-50 characters, optional)

OK

Cancel

2	10	vlan10	1(UNTAG)	Default Vlan For WAN1	
3	20	vlan20	2(UNTAG)	Default Vlan For WAN2	

Krok2

Status

Network

- WAN
- LAN
- IPTV
- MAC
- Switch
- VLAN
- IPV6

Preferences

Transmission

VLAN

Ports

VLAN List

+

 Add

-

 Delete

☐	ID	VLAN ID	Name	Ports	Description	Operation
☐	1	1	vlan1	3(UNTAG) 4(UNTAG)	Default Vlan For LAN	
☐	2	10	vlan10	1(UNTAG)	Default Vlan For WAN1	
☐	3	20	vlan20	2(UNTAG)	Default Vlan For WAN2	

Krok3

Status

Network

- WAN
- LAN
- IPTV
- MAC
- Switch
- VLAN
- IPV6

Preferences

Transmission

Firewall

Behavior Control

VPN

Authentication

Services

System Tools

VLAN

Ports

☐	ID	VLAN ID	Name	Ports
☐	--	--	--	--

VLAN ID:

40

(1-4094)

Name:

vlan40

(1-50 characters)

Ports:

☐ 1 TAG

☐ 2 TAG

☐ 3 TAG

☐ 4 TAG

☒ 5 TAG

Description:

(1-50 characters, optional)

OK

Cancel

Krok4

VLAN

Ports

VLAN List

+

 Add

-

 Delete

☐	ID	VLAN ID	Name	Ports	Description	Operation
☐	1	1	vlan1	3(UNTAG) 4(UNTAG)	Default Vlan For LAN	
☐	2	10	vlan10	1(UNTAG)	Default Vlan For WAN1	
☐	3	20	vlan20	2(UNTAG)	Default Vlan For WAN2	
☐	4	40	vlan40	5(TAG)		

Krok5

← → ↻ Niezabezpieczona 192.168.0.2

tp-link

T2500G-10MPS

VLAN Config Port Config

System
Switching
VLAN
• 802.1Q VLAN
• MAC VLAN
• Protocol VLAN
• VLAN VPN
• GVRP
Spanning Tree
Multicast
DHCP
QoS
PoE
ACL
Network Security

VLAN Port Config

UNIT: 1 LAGS

Select	Port	Link Type	PVID	LAG
☐		v		
☐	1/0/1	TRUNK	1	---
☐	1/0/2	ACCESS	1	---
☐	1/0/3	ACCESS	1	---
☐	1/0/4	ACCESS	1	---
☐	1/0/5	ACCESS	1	---
☐	1/0/6	ACCESS	1	---
☐	1/0/7	ACCESS	1	---
☐	1/0/8	TRUNK	1	---
☐	1/0/9	ACCESS	1	---
☐	1/0/10	ACCESS	1	---

All Apply Help

Krok6

VLAN Info

VLAN ID:

40

(2 - 4094)

Name :

vlan40

(16 characters maximum)

Untagged port

UNIT: 1 LAGS



All

Clear

Tagged port

UNIT: 1 LAGS



All

Clear

Apply

Help

Krok7

TL-ER6120

T2500G-10MPS

T2500G-10MPS

T2500G-10MPS

← → ↻ Niebezpieczona 192.168.0.2



T2500G-10MPS

VLAN Config

Port Config

System

Switching

VLAN

• 802.1Q VLAN

• MAC VLAN

• Protocol VLAN

• VLAN VPN

• GVRP

Spanning Tree

Multicast

DHCP

QoS

PoE

ACL

Network Security

VLAN Port Config

UNIT: 1 LAGS

Select	Port	Link Type	PVID	LAG	VLAN
☐					
☐	1/0/1	TRUNK	1	---	Detail
☐	1/0/2	ACCESS	1	---	Detail
☐	1/0/3	ACCESS	40	---	Detail
☐	1/0/4	ACCESS	1	---	Detail
☐	1/0/5	ACCESS	1	---	Detail
☐	1/0/6	ACCESS	1	---	Detail
☐	1/0/7	ACCESS	1	---	Detail
☐	1/0/8	TRUNK	1	---	Detail
☐	1/0/9	ACCESS	1	---	Detail
☐	1/0/10	ACCESS	1	---	Detail

All

Apply

Help

Krok8

← → ↻ Niezabezpieczona 192.168.0.3

 tp-link

T2500G-10MPS

VLAN Config Port Config

System
Switching
VLAN

- 802.1Q VLAN
- MAC VLAN
- Protocol VLAN
- VLAN VPN
- GVRP

Spanning Tree
Multicast
DHCP
QoS
PoE
ACL
Network Security

VLAN Port Config

UNIT: 1 LAGS

Select	Port	Link Type	PVID	LAC
☐				
☐	1/0/1	TRUNK	1	---
☐	1/0/2	ACCESS	1	---
☐	1/0/3	ACCESS	1	---
☐	1/0/4	ACCESS	1	---
☐	1/0/5	TRUNK	1	---
☐	1/0/6	ACCESS	1	---
☐	1/0/7	TRUNK	1	---
☐	1/0/8	TRUNK	1	---
☐	1/0/9	ACCESS	1	---
☐	1/0/10	ACCESS	1	---

All Apply Help

Krok9

VLAN Info

VLAN ID:

40

(2 - 4094)

Name :

vlan40

(16 characters maximum)

Untagged port

UNIT: 1 LAGS

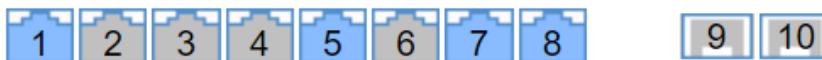


All

Clear

Tagged port

UNIT: 1 LAGS



All

Clear

Apply

Help



Unselected Port(s)



Selected Port(s)



Not Availab

VLAN Port Config

UNIT: 1 LAGS

Select	Port	Link Type	PVID	LAG
☐				
☐	1/0/1	TRUNK	1	---
☐	1/0/2	ACCESS	1	---
☐	1/0/3	ACCESS	1	---
☐	1/0/4	ACCESS	1	---
☐	1/0/5	TRUNK	1	---
☐	1/0/6	ACCESS	1	---
☐	1/0/7	TRUNK	1	---
☐	1/0/8	TRUNK	1	---
☐	1/0/9	ACCESS	1	---
☐	1/0/10	ACCESS	1	---

←→↻

Niezabezpieczona192.168.0.4

tp-link

T2500G-10MPS

System

Switching

VLAN

• 802.1Q VLAN

• MAC VLAN

• Protocol VLAN

• VLAN VPN

• GVRP

Spanning Tree

Multicast

DHCP

QoS

PoE

ACL

Network Security

VLAN Config

Port Config

Operation succeeded.

VLAN Port Config

UNIT:1LAGS

Select	Port	Link Type	PVID	LAC
☐				
☐	1/0/1	TRUNK	1	---
☐	1/0/2	ACCESS	1	---
☐	1/0/3	ACCESS	1	---
☐	1/0/4	ACCESS	1	---
☐	1/0/5	ACCESS	1	---
☐	1/0/6	ACCESS	1	---
☐	1/0/7	TRUNK	1	---
☐	1/0/8	TRUNK	1	---
☐	1/0/9	ACCESS	1	---
☐	1/0/10	ACCESS	1	---

All

Apply

Help

Krok12

VLAN Info

VLAN ID:

(2 - 4094)

Name :

(16 charac

Untagged port

UNIT: LAGS

Tagged port

UNIT: LAGS

← → ↻ Niezabezpieczona 192.168.0.2

tp-link

T2500G-10MPS

System
Switching
VLAN
Spanning Tree
• **STP Config**
• Port Config
• MSTP Instance
• STP Security
Multicast
DHCP
QoS
PoE
ACL
Network Security

STP Config STP Summary

Global Config

Spanning-Tree : ☐ Enable ☒ Disable

Mode : **MSTP**

Parameters Config

CIST Priority : **8192** (0-61440, in increments of 4096)

Hello Time : **2** sec (1-10)

Max Age : **20** sec (6-40)

Forward Delay : **15** sec (4-30)

TxHoldCount : **5** pps (1-20)

Max Hops : **20** hop (1-40)

Apply

Apply Help

Krok14

← → ↻ Niezabezpieczona 192.168.0.2

tp-link

T2500G-10MPS

System
Switching
VLAN
Spanning Tree
• STP Config
• **Port Config**
• MSTP Instance
• STP Security
Multicast
DHCP
QoS
PoE
ACL
Network Security
SNMP
LLDP
Maintenance
Save Config
Index

Port Config

UNIT: **1** LAGS

Select	Port	Status	Priority	Ext-Path Cost	Int-Path Cost	Edge Port	P2P Link	MCheck	Port Mode	Port Role	Port S
☐	1/0/1	Enable	128	80000	80000	Disable	Auto	---	---	---	---
☐	1/0/2	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---
☐	1/0/3	Enable	128	Auto	Auto	Enable	Auto	---	---	---	---
☐	1/0/4	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---
☐	1/0/5	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---
☐	1/0/6	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---
☐	1/0/7	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---
☐	1/0/8	Enable	128	Auto	Auto	Disable	Auto	---	---	---	---
☐	1/0/9	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---
☐	1/0/10	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---

All Apply Refresh Help

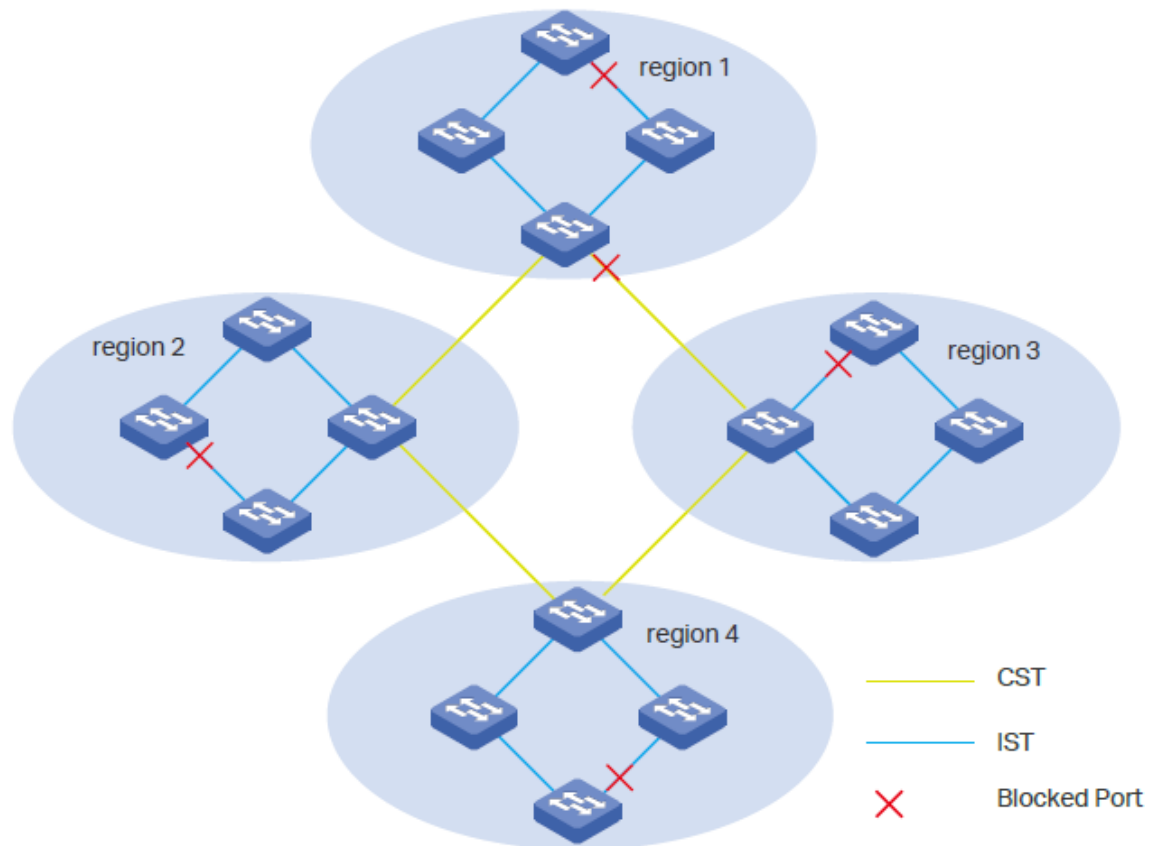
Note :
If the Path Cost of a port is set to 0, it will alter automatically according to the port's link speed.

Krok15 Trochę teorii

1.2.2 MSTP Concepts

MSTP, compatible with STP and RSTP, has the same basic elements used in STP and RSTP. Based on the networking topology, this section will introduce some concepts only exist in MSTP.

Figure 1-3 MSTP Topology

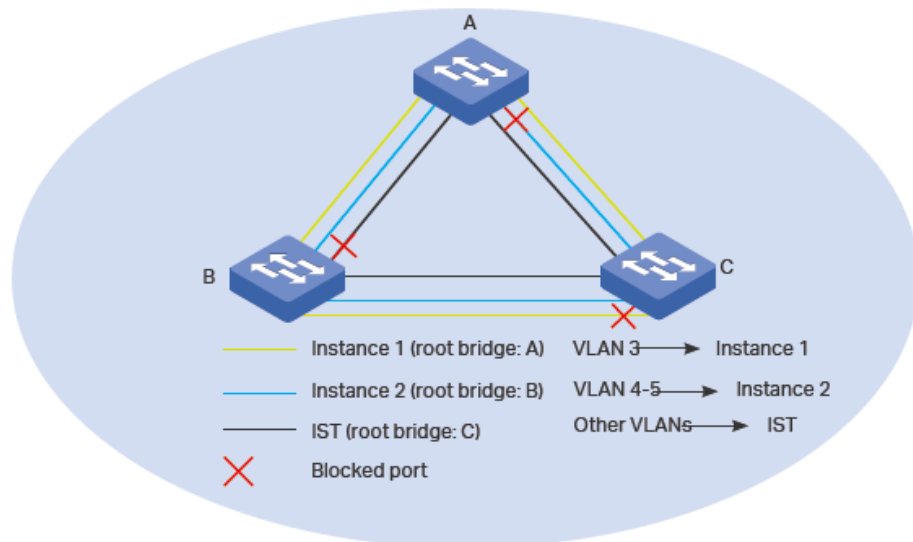


MST Region

An MST region consists of multiple interconnected switches. The switches that have the following characteristics are considered as in the same region:

- Same region name
- Same revision level
- Same VLAN-Instance mapping

Figure 1-4 MST Region



VLAN-Instance Mapping

VLAN-Instance Mapping describes the mapping relationship between VLANs and instances. Multiple VLANs can be mapped to a same instance, but one VLAN can be mapped to only one instance. As Figure 1-4 shows, VLAN 3 is mapped to instance 1, VLAN 4 and VLAN 5 are mapped to instance 2, the other VLANs are mapped to the IST.

IST

The Internal Spanning Tree, which is a special MST instance with an instance ID of 0. By default, all the VLANs are mapped to IST.

CST

The Common Spanning Tree, which is the spanning tree connects all MST regions. As is shown in Figure 1-3, region1-region 4 are connected by the CST.

CIST

The Common and Internal Spanning Tree, comprising IST and CST, is the spanning tree that connects all the switches in the network.

Krok16

T2500G-10MPS

Region Config

Instance Config

Instance Port Config

System

Switching

VLAN

Spanning Tree

- STP Config
- Port Config
- **MSTP Instance**
- STP Security

Region Config

Region Name :

40

Revision :

40

(0-65535)

Apply

Help

Krok17

Region Config

Instance Config

Instance Port Config

VLAN-Instance Mapping

Instance ID :

4

(0-8, 0 stand for CIST)

VLAN ID :

40

(1-4094, format: 1,3,4-7,11-30)

Add

Delete

Instance Config

Select	Instance ID	Status	Priority	VLAN ID	
☐					
☐	CIST	Disable	8192	1-4094,	Show All Clear All
☐	1	Disable	32768		Show All Clear All
☐	2	Disable	32768		Show All Clear All
☐	3	Disable	32768		Show All Clear All
☐	4	Disable	32768		Show All Clear All
☐	5	Disable	32768		Show All Clear All
☐	6	Disable	32768		Show All Clear All
☐	7	Disable	32768		Show All Clear All
☐	8	Disable	32768		Show All Clear All

Apply

Help

Krok18

Instance ID :

(0-8, 0 stand for CIST)

Add

VLAN ID :

(1-4094, format: 1,3,4-7,11-30)

Delete

Instance Config					
Select	Instance ID	Status	Priority	VLAN ID	
☐			8192		
☐	CIST	Disable	8192	1-39,41-4094,	Show All Clear All
☐	1	Disable	32768		Show All Clear All
☐	2	Disable	32768		Show All Clear All
☐	3	Disable	32768		Show All Clear All
☒	4	Enable	32768	40,	Show All Clear All
☐	5	Disable	32768		Show All Clear All
☐	6	Disable	32768		Show All Clear All
☐	7	Disable	32768		Show All Clear All
☐	8	Disable	32768		Show All Clear All

Apply

Help

Krok19

Instance Config					
Select	Instance ID	Status	Priority	VLAN ID	
☐					
☐	CIST	Disable	8192	1-39,41-4094,	
☐	1	Disable	32768		
☐	2	Disable	32768		
☐	3	Disable	32768		
☐	4	Enable	8192	40,	
☐	5	Disable	32768		
☐	6	Disable	32768		
☐	7	Disable	32768		
☐	8	Disable	32768		

Apply

Help

Krok20

Region Config

Instance Config

Instance Port Config

Instance ID :

1

▼

1

2

3

4

5

6

7

8

Instance Port Config

UNIT:

1

 LAG:

3

Select	Port	P	Path Cost	Port Role	Port Stat
☐		☐			
☐	1/0/1		Auto	---	---
☐	1/0/2		Auto	---	---
☐	1/0/3	128	Auto	---	---
☐	1/0/4	128	Auto	---	---
☐	1/0/5	128	Auto	---	---
☐	1/0/6	128	Auto	---	---
☐	1/0/7	128	Auto	---	---
☐	1/0/8	128	Auto	---	---
☐	1/0/9	128	Auto	---	---
☐	1/0/10	128	Auto	---	---

All

Apply

Refresh

Help

Instance ID Select

Instance ID :

4 ▾

Instance Port Config

UNIT: 1 LAGS

Select	Port	Priority	Path Cost	Port Role	Port Sta
☐			80000		
☒	1/0/1	128	Auto	---	---
☐	1/0/2	128	Auto	---	---
☐	1/0/3	128	Auto	---	---
☐	1/0/4	128	Auto	---	---
☐	1/0/5	128	Auto	---	---
☐	1/0/6	128	Auto	---	---
☐	1/0/7	128	Auto	---	---
☐	1/0/8	128	Auto	---	---
☐	1/0/9	128	Auto	---	---
☐	1/0/10	128	Auto	---	---

All

Apply

Refresh

Help

Operation succeeded.

Instance ID Select

Instance ID :

4 ▾

switch1 192.168.0.2

Instance Port Config

UNIT: 1 LAGS

Select	Port	Priority	Path Cost	Port Role	Port S
☐					
☐	1/0/1	128	80000	---	--
☐	1/0/2	128	Auto	---	--
☐	1/0/3	128	Auto	---	--
☐	1/0/4	128	Auto	---	--
☐	1/0/5	128	Auto	---	--
☐	1/0/6	128	Auto	---	--
☐	1/0/7	128	Auto	---	--
☐	1/0/8	128	Auto	---	--
☐	1/0/9	128	Auto	---	--
☐	1/0/10	128	Auto	---	--

All

Apply

Refresh

Help

Operation succeeded.

Instance ID Select

Instance ID :

4 ▼

switch2 192.168.0.3

Instance Port Config

UNIT: 1 LAGS

Select	Port	Priority	Path Cost	Port Role	Port Status
☐					
☐	1/0/1	128	Auto	---	---
☐	1/0/2	128	Auto	---	---
☐	1/0/3	128	Auto	---	---
☐	1/0/4	128	Auto	---	---
☐	1/0/5	128	Auto	---	---
☐	1/0/6	128	Auto	---	---
☐	1/0/7	128	Auto	---	---
☐	1/0/8	0	Auto	---	---
☐	1/0/9	128	Auto	---	---
☐	1/0/10	128	Auto	---	---

All

Apply

Refresh

Help

Instance ID :

4 ▾

switch3 192.168.0.4

Instance Port Config

UNIT: 1 LAGS

Select	Port	Priority	Path Cost	Port Role	Port
☐					
☐	1/0/1	128	80000	---	
☐	1/0/2	128	Auto	---	
☐	1/0/3	128	Auto	---	
☐	1/0/4	128	Auto	---	
☐	1/0/5	128	Auto	---	
☐	1/0/6	128	Auto	---	
☐	1/0/7	128	Auto	---	
☐	1/0/8	0	Auto	---	
☐	1/0/9	128	Auto	---	
☐	1/0/10	128	Auto	---	

All

Apply

Refresh

Help

Sprawdzanie stanów portów STP

Region Config

Instance Config

Instance Port Config

Instance ID Select

switch1 192.168.0.2

Instance ID :

4 ▼

(stp3)

Instance Port Config

UNIT: 1 LAGS

Select	Port	Priority	Path Cost	Port Role	Port Status	LAG
☐						
☐	1/0/1	128	80000	Alternate	Blocking	---
☐	1/0/2	128	Auto	---	---	---
☐	1/0/3	128	20000(Auto)	Designated	Forwarding	---
☐	1/0/4	128	Auto	---	---	---
☐	1/0/5	128	Auto	---	---	---
☐	1/0/6	128	Auto	---	---	---
☐	1/0/7	128	Auto	---	---	---
☐	1/0/8	128	20000(Auto)	Root	Forwarding	---
☐	1/0/9	128	Auto	---	---	---
☐	1/0/10	128	Auto	---	---	---

All

Apply

Refresh

Help

Port Config

switch2 192.168.0.3 (stp1)

Port Config

UNIT: 1 LAGS

Select	Port	Status	Priority	Ext-Path Cost	Int-Path Cost	Edge Port	P2P Link	MCheck	Port Mode	Port Role	Port Status	LAG
☐		▼				▼	▼	▼				
☐	1/0/1	Enable	128	20000(Auto)	20000(Auto)	Disable	Open(Auto)	---	MSTP	Designated	Forwarding	---
☐	1/0/2	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
☐	1/0/3	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
☐	1/0/4	Enable	128	20000(Auto)	20000(Auto)	Enable	Open(Auto)	---	MSTP	Designated	Forwarding	---
☐	1/0/5	Enable	128	20000(Auto)	20000(Auto)	Enable	Open(Auto)	---	MSTP	Designated	Forwarding	---
☐	1/0/6	Enable	128	20000(Auto)	20000(Auto)	Enable	Open(Auto)	---	MSTP	Designated	Forwarding	---
☐	1/0/7	Enable	128	20000(Auto)	20000(Auto)	Disable	Open(Auto)	---	MSTP	Designated	Forwarding	---
☐	1/0/8	Enable	0	20000(Auto)	20000(Auto)	Disable	Open(Auto)	---	MSTP	Designated	Forwarding	---
☐	1/0/9	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
☐	1/0/10	Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---

All

Apply

Refresh

Help

Instance ID Select

switch2 192.168.0.3 (stp1)

Instance ID :

4 ▼

Instance Port Config

UNIT: 1 LAGS

Select	Port	Priority	Path Cost	Port Role	Port Status	LAG
☐						
☐	1/0/1	128	20000(Auto)	Designated	Forwarding	---
☐	1/0/2	128	Auto	---	---	---
☐	1/0/3	128	Auto	---	---	---
☐	1/0/4	128	20000(Auto)	Designated	Forwarding	---
☐	1/0/5	128	20000(Auto)	Designated	Forwarding	---
☐	1/0/6	128	20000(Auto)	Designated	Forwarding	---
☐	1/0/7	128	20000(Auto)	Designated	Forwarding	---
☐	1/0/8	0	20000(Auto)	Designated	Forwarding	---
☐	1/0/9	128	Auto	---	---	---
☐	1/0/10	128	Auto	---	---	---

All

Apply

Refresh

Help

Port Config

switch3 192.168.0.4 (stp2)

LAGS

Status	Priority	Ext-Path Cost	Int-Path Cost	Edge Port	P2P Link	MCheck	Port Mode	Port Role	Port Status	LAG
▼				▼	▼	▼				
Enable	128	80000	80000	Disable	Open(Auto)	---	MSTP	Designated	Forwarding	---
Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
Enable	128	20000(Auto)	20000(Auto)	Disable	Open(Auto)	---	MSTP	Alternate	Blocking	---
Enable	0	20000(Auto)	20000(Auto)	Disable	Open(Auto)	---	MSTP	Root	Forwarding	---
Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---
Disable	128	Auto	Auto	Disable	Auto	---	---	---	---	---

All

Apply

Refresh

Help

switch3 192.168.0.4 (stp2)

Instance ID Select

Instance ID :

4 ▼

Instance Port Config

UNIT: 1 LAGS

Select	Port	Priority	Path Cost	Port Role	Port Status	LAG
☐						
☐	1/0/1	128	80000	Designated	Forwarding	---
☐	1/0/2	128	Auto	---	---	---
☐	1/0/3	128	Auto	---	---	---
☐	1/0/4	128	Auto	---	---	---
☐	1/0/5	128	Auto	---	---	---
☐	1/0/6	128	Auto	---	---	---
☐	1/0/7	128	20000(Auto)	Alternate	Blocking	---
☐	1/0/8	0	20000(Auto)	Root	Forwarding	---
☐	1/0/9	128	Auto	---	---	---
☐	1/0/10	128	Auto	---	---	---

All

Apply

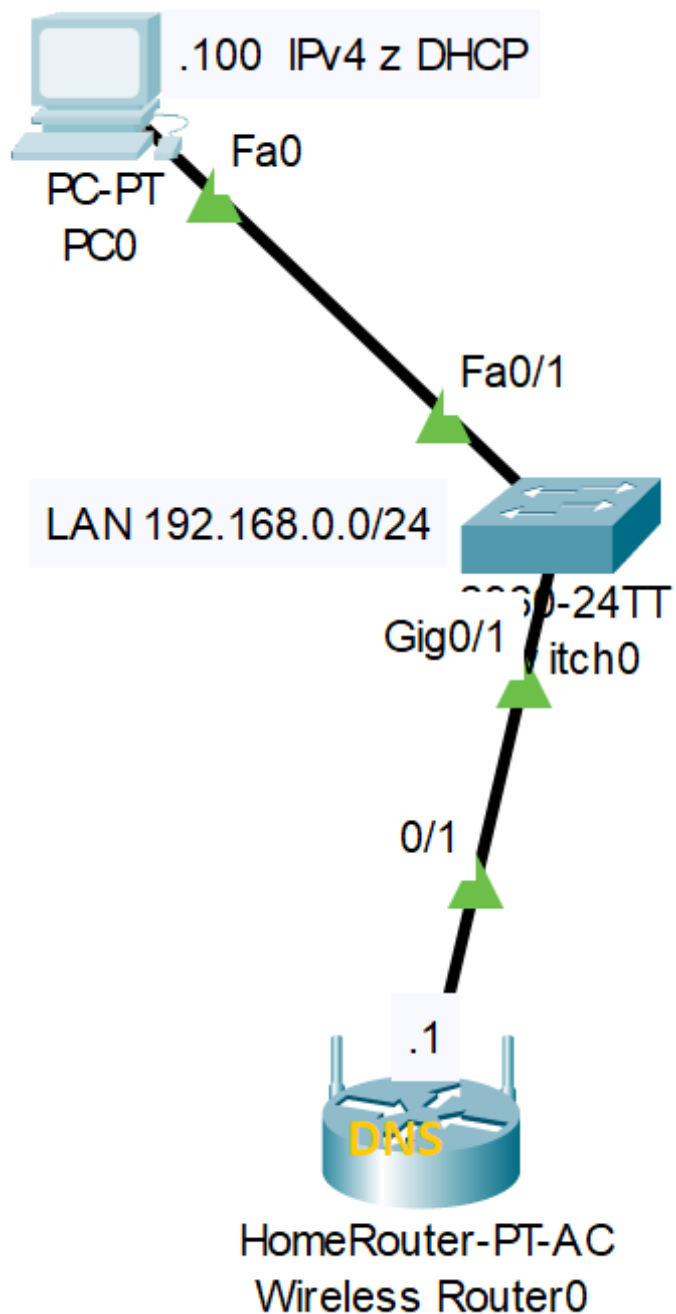
Refresh

Help

4.ROUTING

4.1 Protokół routingu RIPv2 - Cisco Packet

1. Podłącz urządzenia w sieci LAN jak widać poniżej.



2. Wejdź na router HomeRouter i ustaw DNS w sekcji DHCP. DNS zainstalowany jest na routerze.

Wireless Router0

Physical Config **GUI** Attributes

Internet Setup

Internet Connection type: Automatic Configuration - DHCP

Optional Settings (required by some internet service providers)

Host Name:

Domain Name:

MTU: Size: 1500

Network Setup

Router IP

IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255.255.255.0

DHCP Server Settings

DHCP Server: ☒ Enabled ☐ Disabled DHCP Reservation

Start IP Address: 192.168.0. 100

Maximum number of Users: 50

IP Address Range: 192.168.0. 100 - 149

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 192 . 168 . 0 . 1

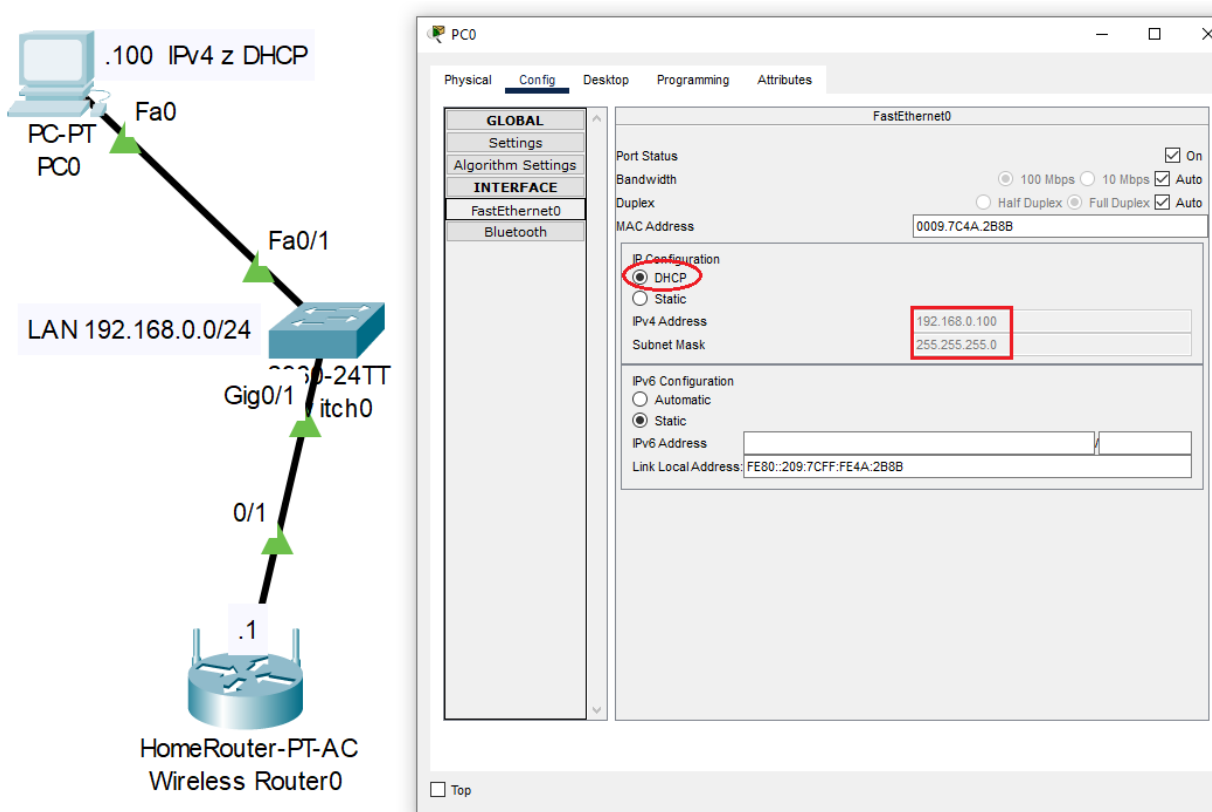
Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

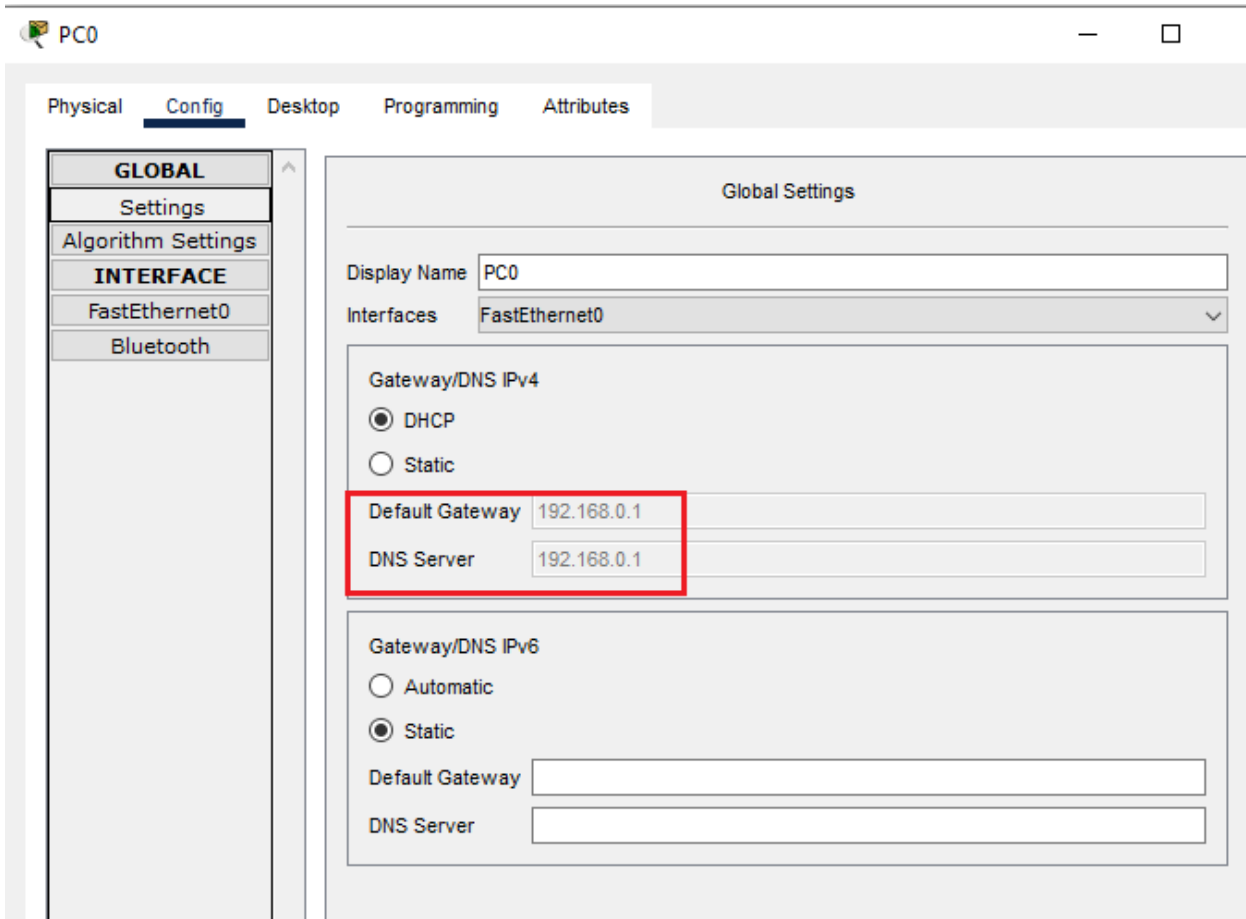
WINS: 0 . 0 . 0 . 0

☐ Top

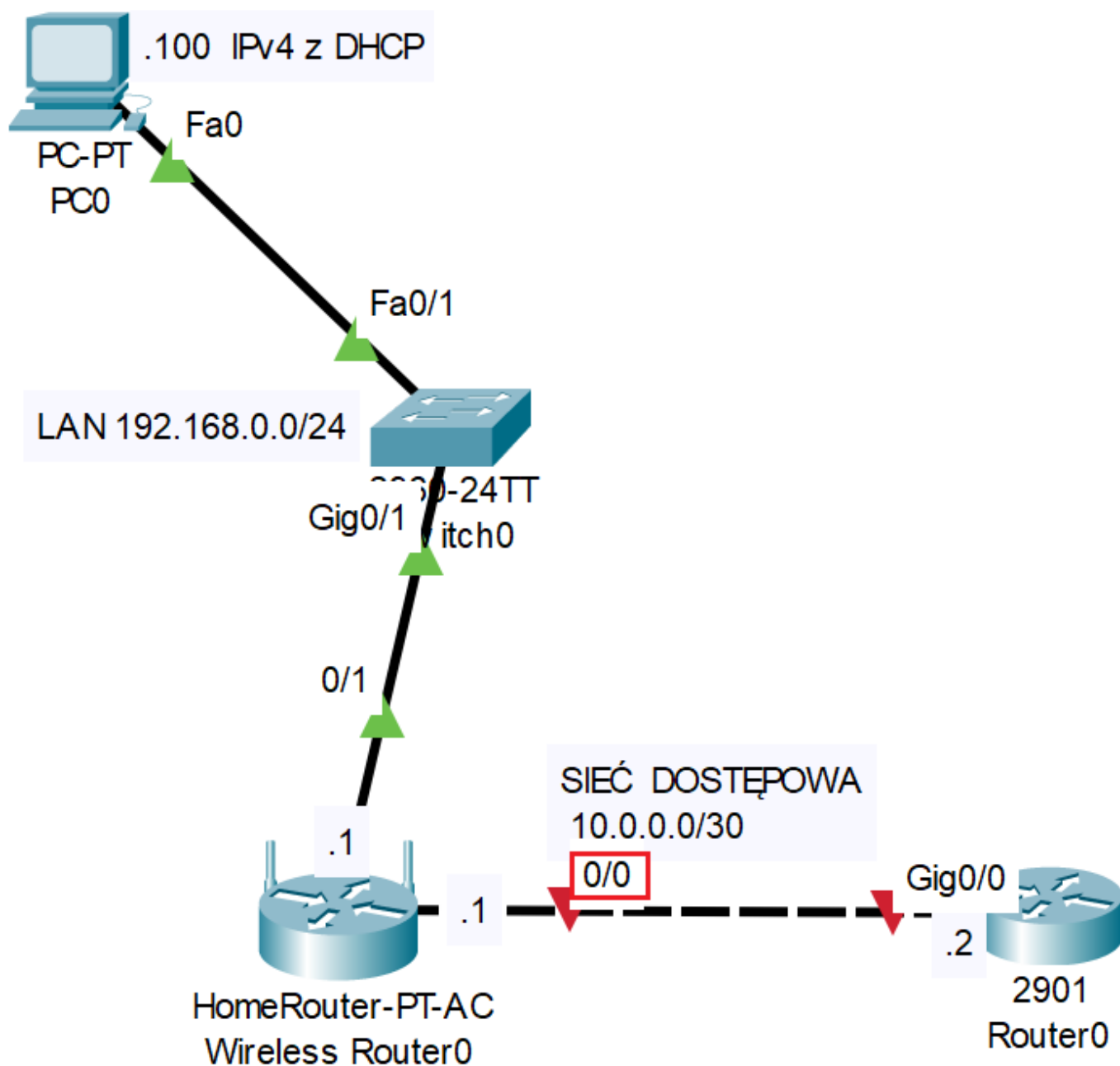
3. Na PC0 w sekcji **IP Configuration** karty sieciowej **FastEthernet0** włącz **DHCP**.



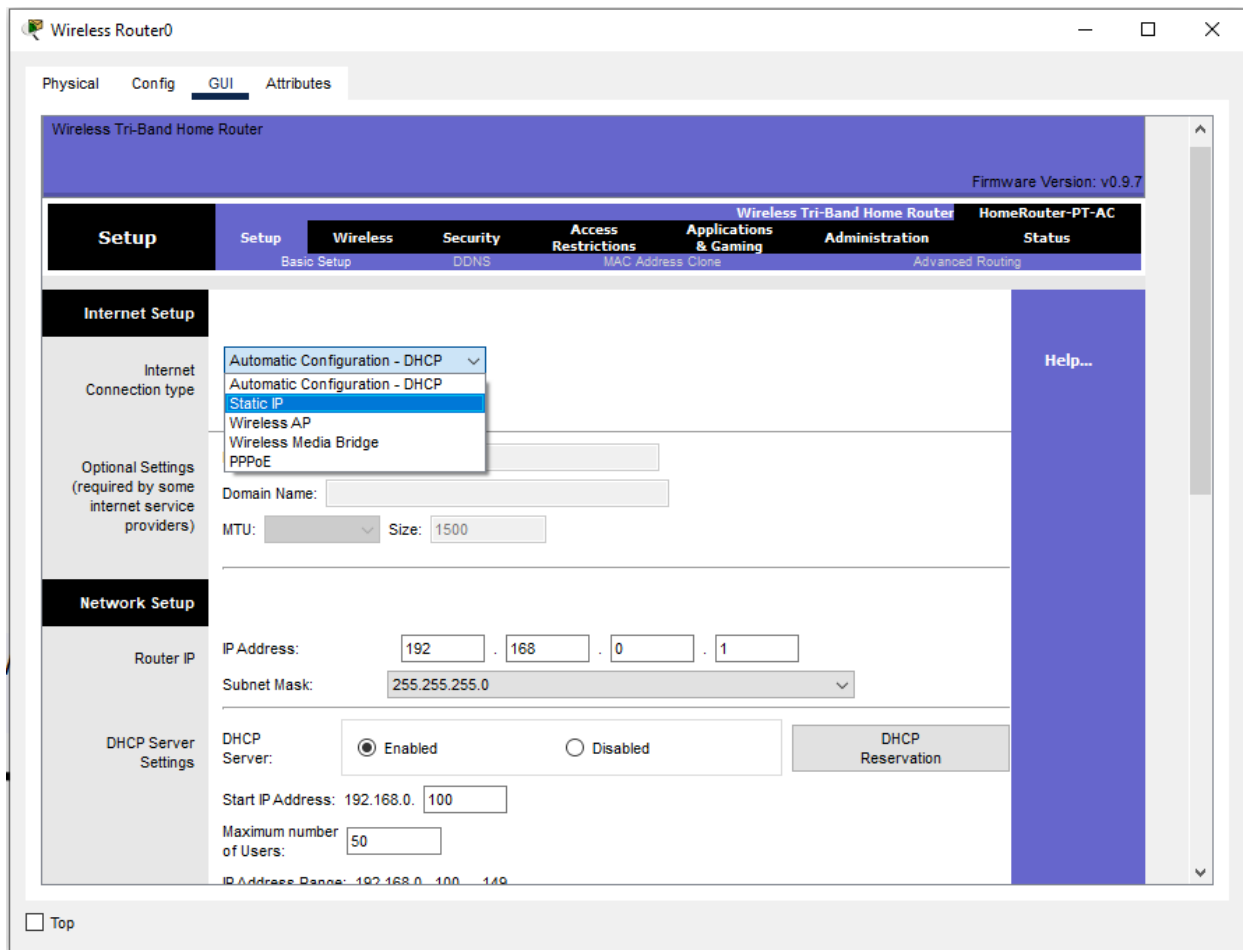
4. W zakładce **Settings/Gateway/DNS IPv4** powinieneś uzyskać poniższy rezultat.



5. Tworzenie sieci dostępowej. Podłącz **router 2091** do routera **HomeRouter**.



6. Na HomeRouterze wejdź w zakładkę **GUI** i sekcji **Internet Setup** wybierz z listy **Static IP**.



Wireless Router0

Physical Config **GUI** Attributes

Wireless Tri-Band Home Router Firmware Version: v0.9.7

Setup Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Basic Setup DDNS MAC Address Clone Advanced Routing

Internet Setup

Internet Connection type: Automatic Configuration - DHCP (selected)

Optional Settings (required by some internet service providers):

Domain Name: []

MTU: [] Size: 1500

Network Setup

Router IP: IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255.255.255.0

DHCP Server: ☒ Enabled ☐ Disabled

DHCP Reservation

Start IP Address: 192.168.0. 100

Maximum number of Users: 50

IP Address Range: 192.168.0. 100 - 149

☐ Top

7. Wpisz właściwe adresy dla połączenia z dostawcą internetowym ISP.

Wireless Router0

Physical Config **GUI** Attributes

Wireless Tri-Band Home Router

Firmware Version: v

Setup Setup **Wireless** Security Access Restrictions Applications & Gaming Administration Status

Basic Setup DDNS MAC Address Clone Advanced Routing

Internet Setup

Internet Connection type: Static IP

Internet IP Address: 10 . 0 . 0 . 1

Subnet Mask: 255 . 255 . 255 . 252

Default Gateway: 10 . 0 . 0 . 2

DNS 1: 8 . 8 . 8 . 8

DNS 2 (Optional): 0 . 0 . 0 . 0

DNS 3 (Optional): 0 . 0 . 0 . 0

Optional Settings (required by some internet service providers)

Host Name:

Domain Name:

MTU: Size: 1500

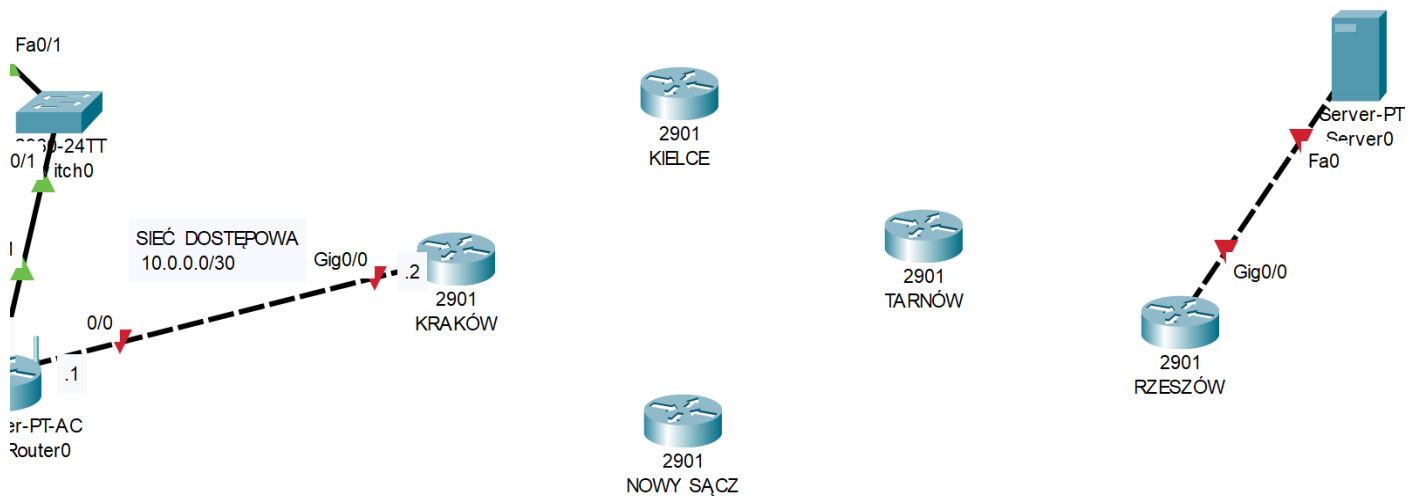
Network Setup

Top

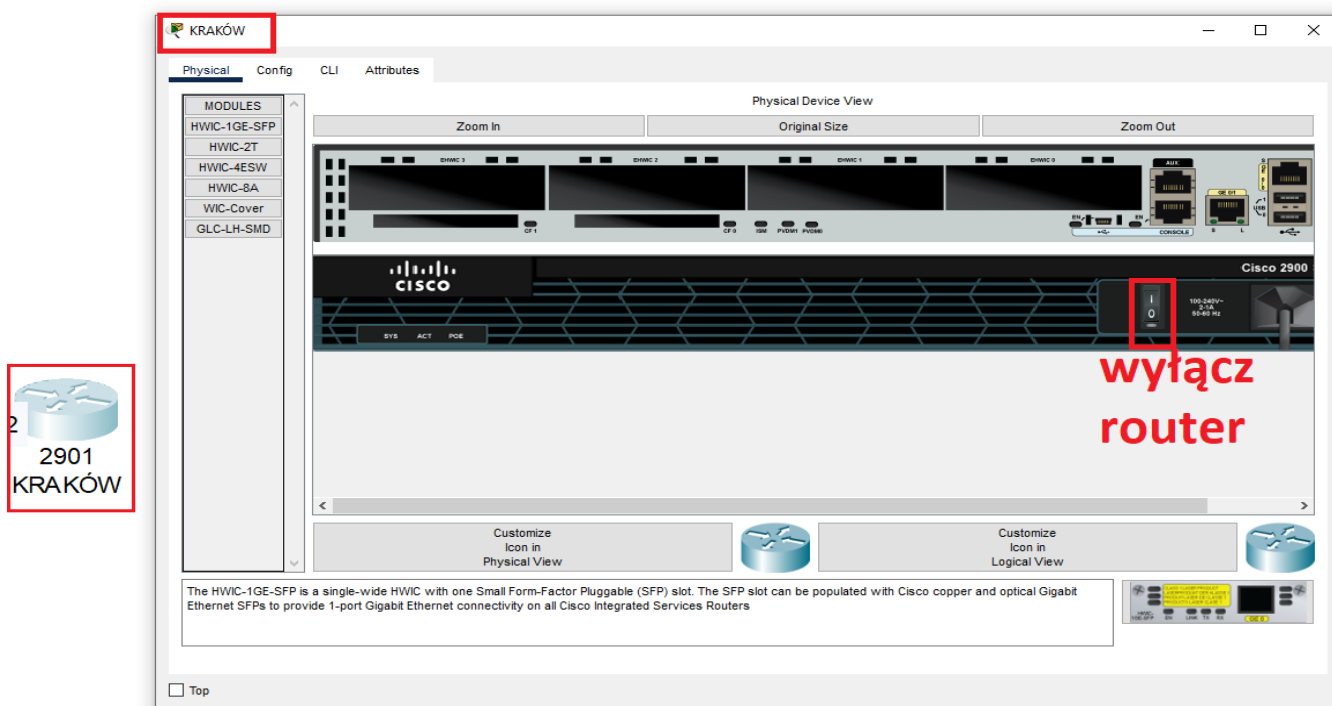
8. Przesuń pasek przewijania w dół i zatwierdź konfigurację połączenia internetowego WAN

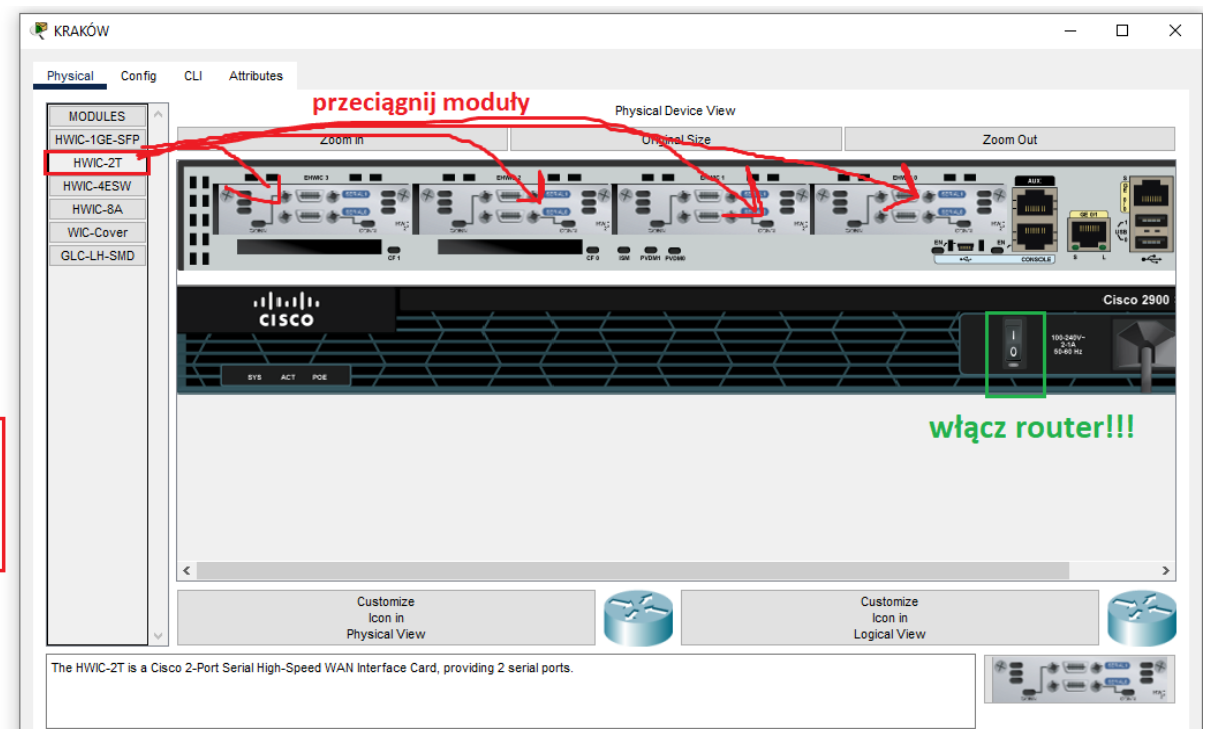
Save Settings Cancel Changes

9. Tworzymy sieć szkieletową. Dodaj nowe routery 2901 i podpisz je jak widać poniżej.



10. Wyłącz każdy z routerów 2901 i dodaj moduły HWIC-2T. Potem włącz zasilanie na urządzeniach.





11. Wejdź na router KRAKÓW w zakładkę Config. Widać Seriale, które będziemy włączać i adresować.



KRAKÓW

Physical **Config** CLI Attributes

Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
Serial0/2/0
Serial0/2/1
Serial0/3/0
Serial0/3/1

Global Settings

Display Name: KRAKÓW
Hostname: Router
NVRAM: Erase Save
Startup Config: Load... Export...
Running Config: Export... Merge...

Equivalent IOS Commands

```
DRAM configuration is 64 bits wide with parity disabled.  
255K bytes of non-volatile configuration memory.  
249856K bytes of ATA System CompactFlash 0 (Read/Write)  
  
--- System Configuration Dialog ---  
  
Would you like to enter the initial configuration dialog? [yes/no]:  
  
Press RETURN to get started!
```

12. Połącz routery sieci szkieletowej kablami DCE (Serial DCE)



Ciscoland.net
3 FT. Serial Cable WIC-2T / HWIC-2T car...



YouTube
DCE V/s DTE Devices Explained by T...



eBay · Brak w magaz...
Smart Serial DTE DC...



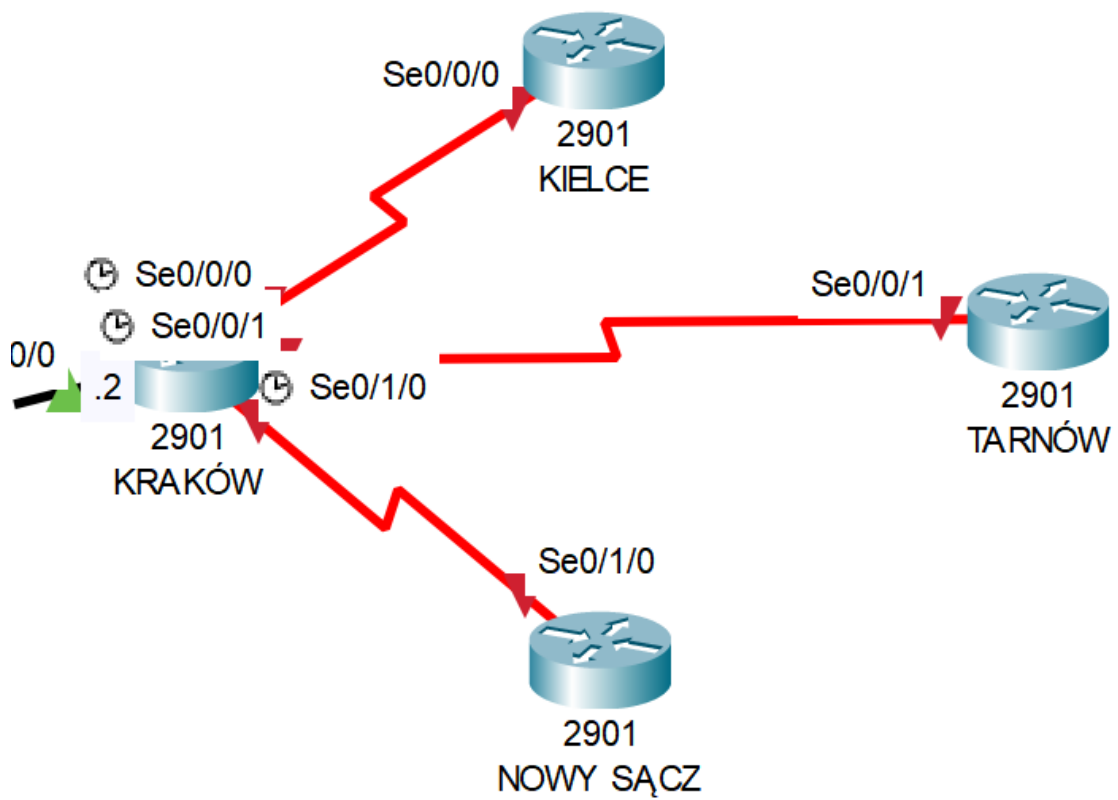
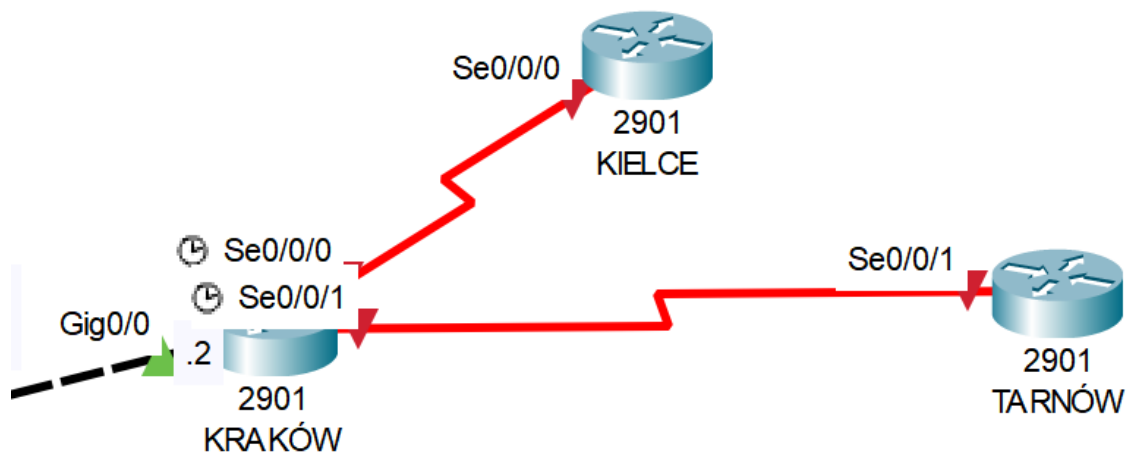
comel-it
CAB-SS-6026X-3FT - Smart Serial 2...

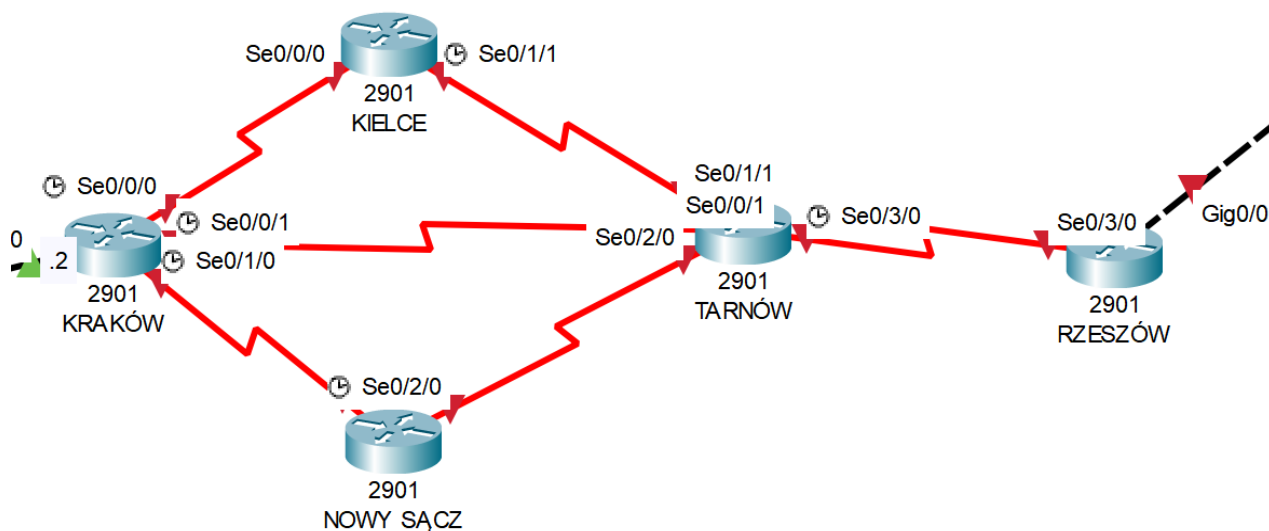


ZOOstock.com
Cable Cisco Smart Ser...

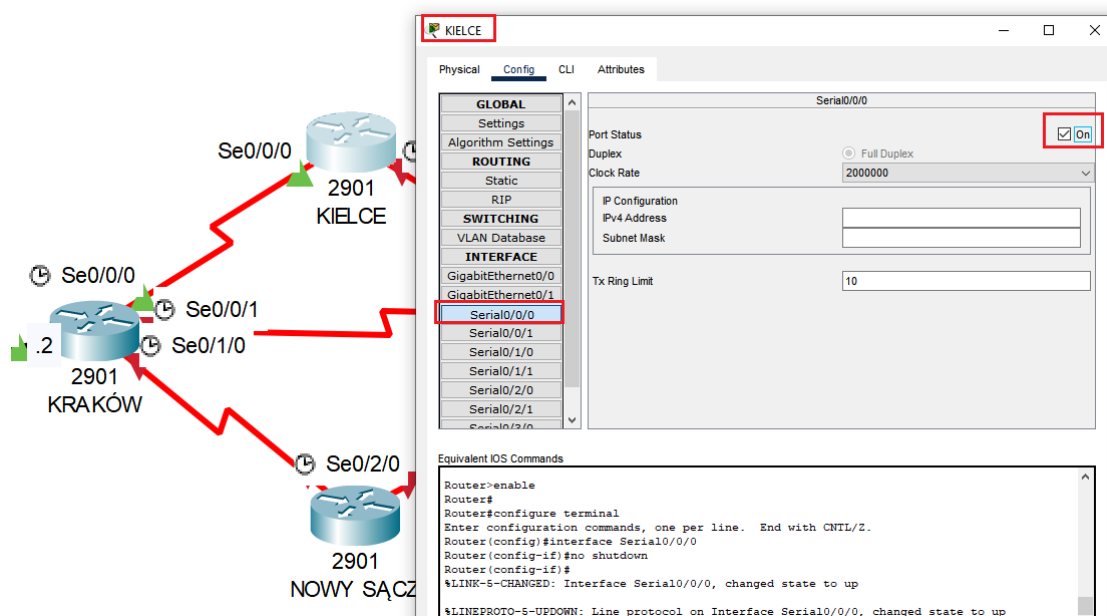
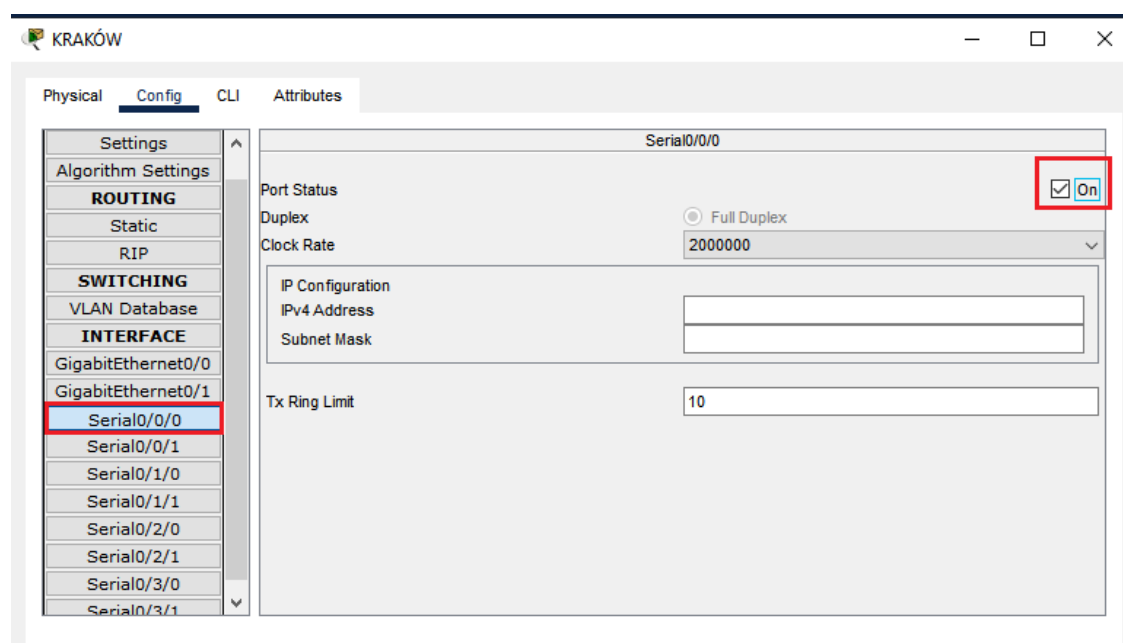
Time: 00:07:32

Serial DCE



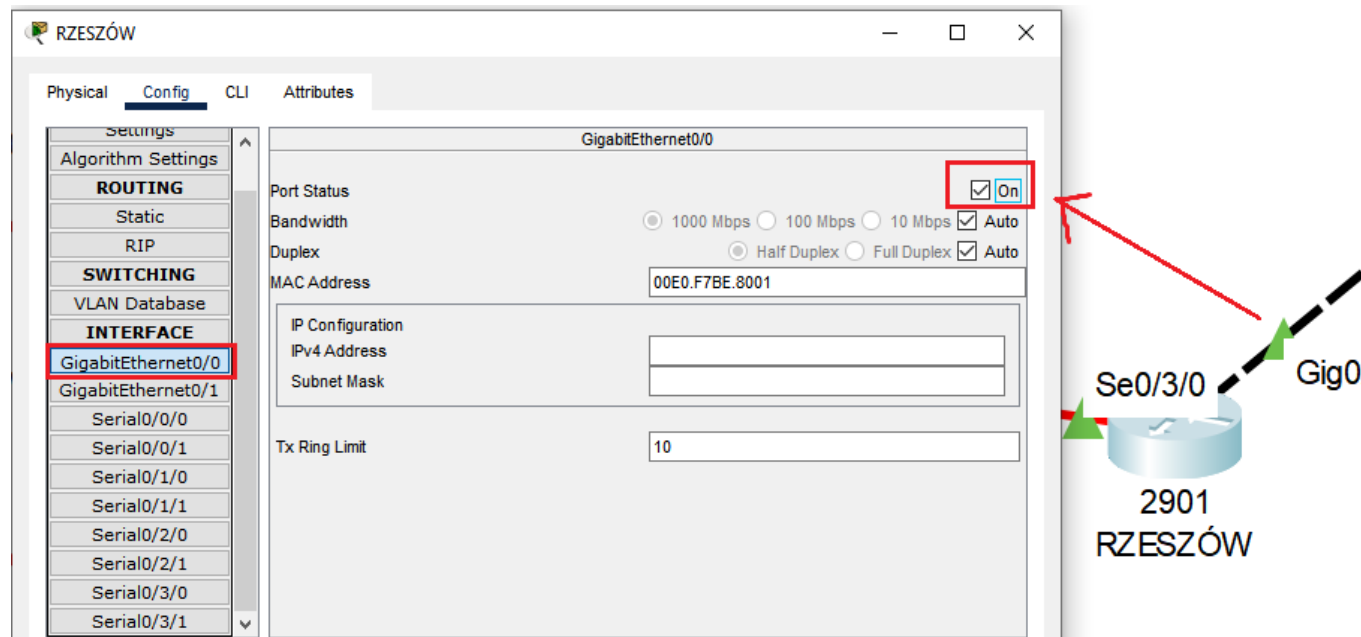


13. Na routerach sieci szkieletowej ustaw **Port Status ON** dla używanych portów

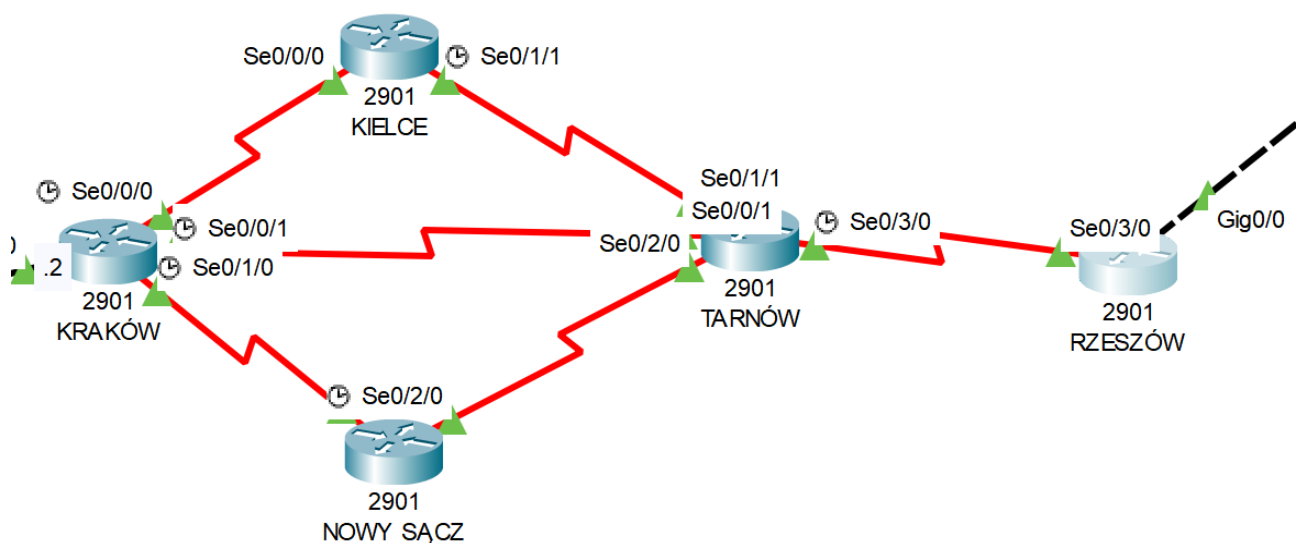


Na połączeniu międzymiastowym KRAKÓW – KIELCE trójgąty czerwone zmieniły kolor na zielony

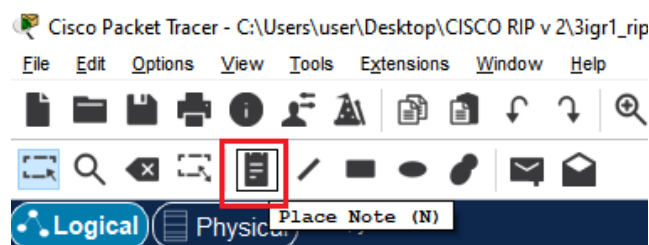
Dokończ włączanie portów na pozostałych routerach kończąc na wybranym porcie GigabitEthernet na routerze RZESZÓW



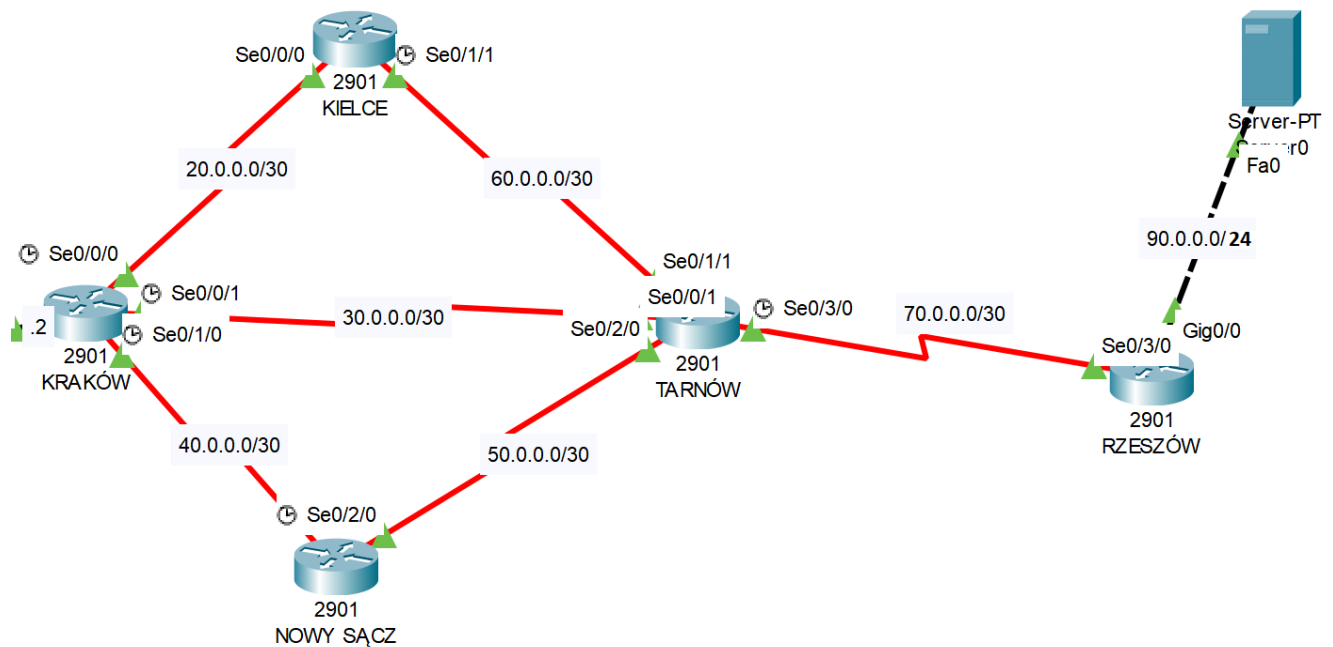
Teraz wszystkie porty są gotowe do konfiguracji



14. Wyznacz pule adresów dla poszczególnych podsieci za pomocą łatek (Ctrl+Alt+N)



20.0.0.



15. Ustaw łatki dla poszczególnych interfejsów sieciowych routerów sieci szkieletowej

/30 -> 255.255.255.252

255.255.255.11111100

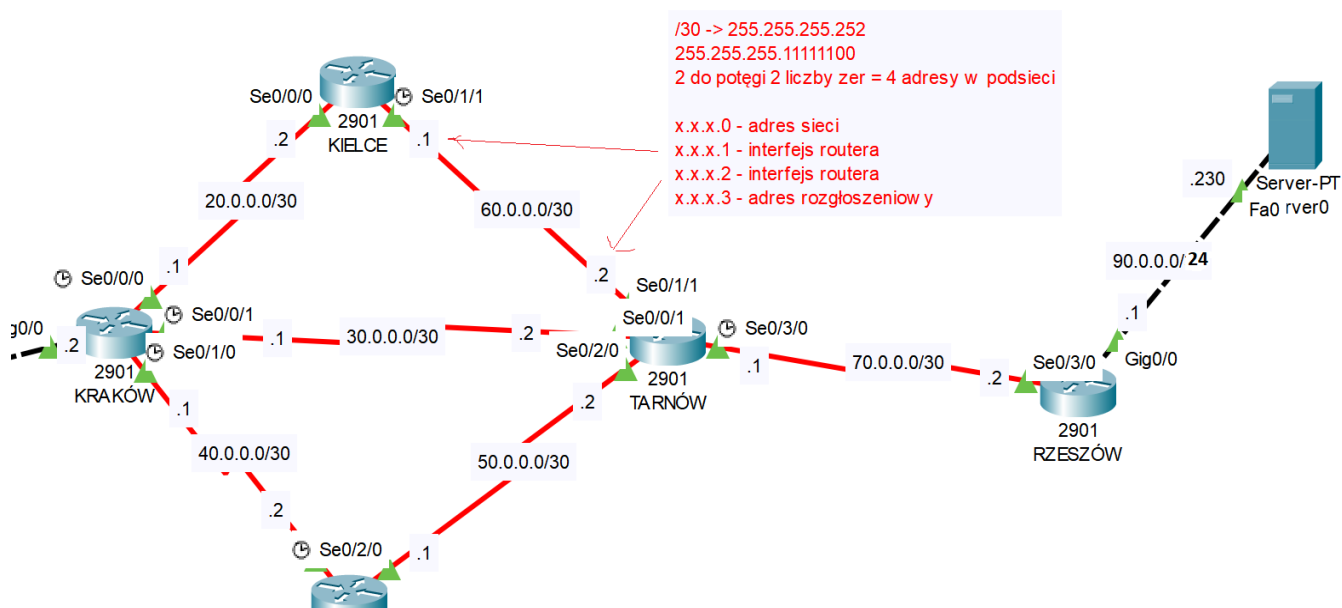
2 do potęgi 2 liczby zer = 4 adresy w podsieci

x.x.x.0 - adres sieci

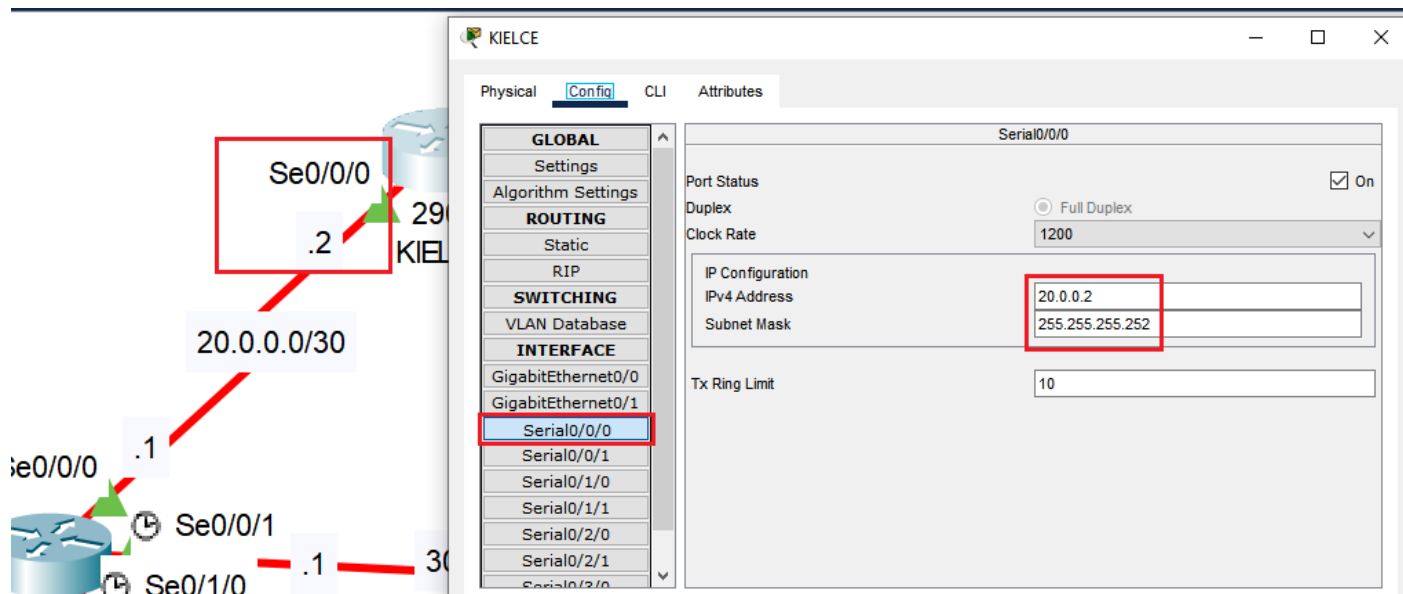
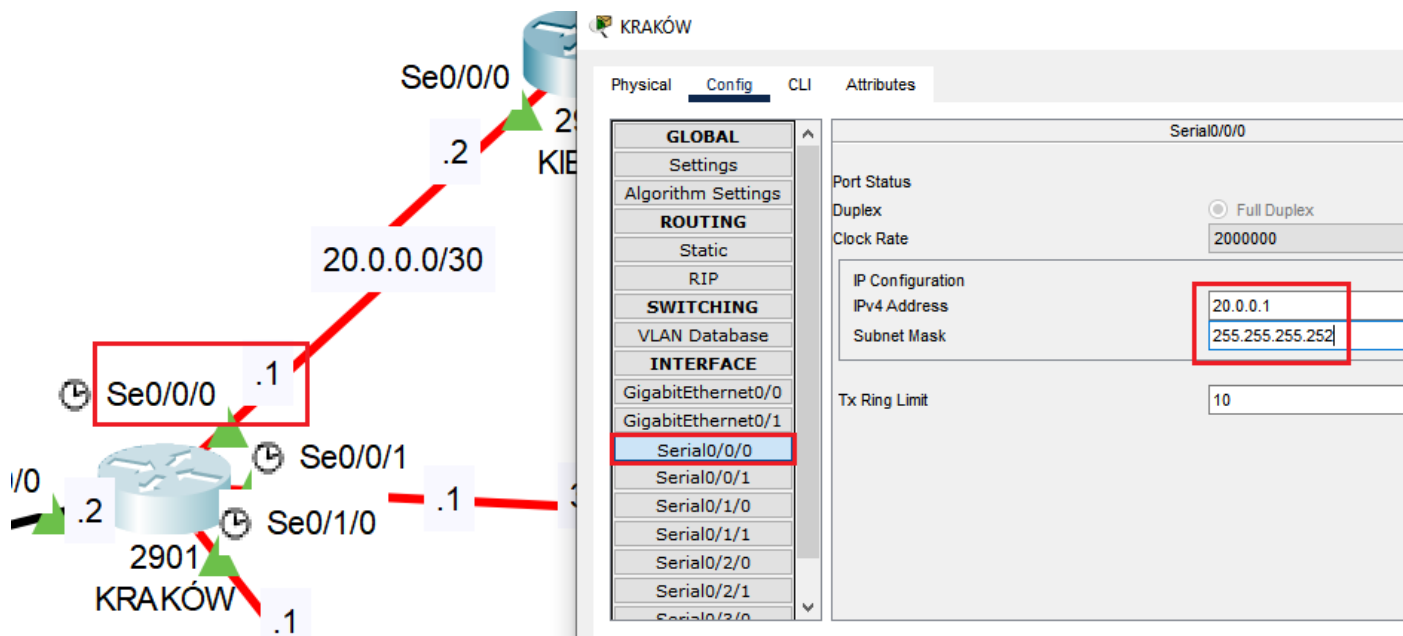
x.x.x.1 - interfejs routera

x.x.x.2 - interfejs routera

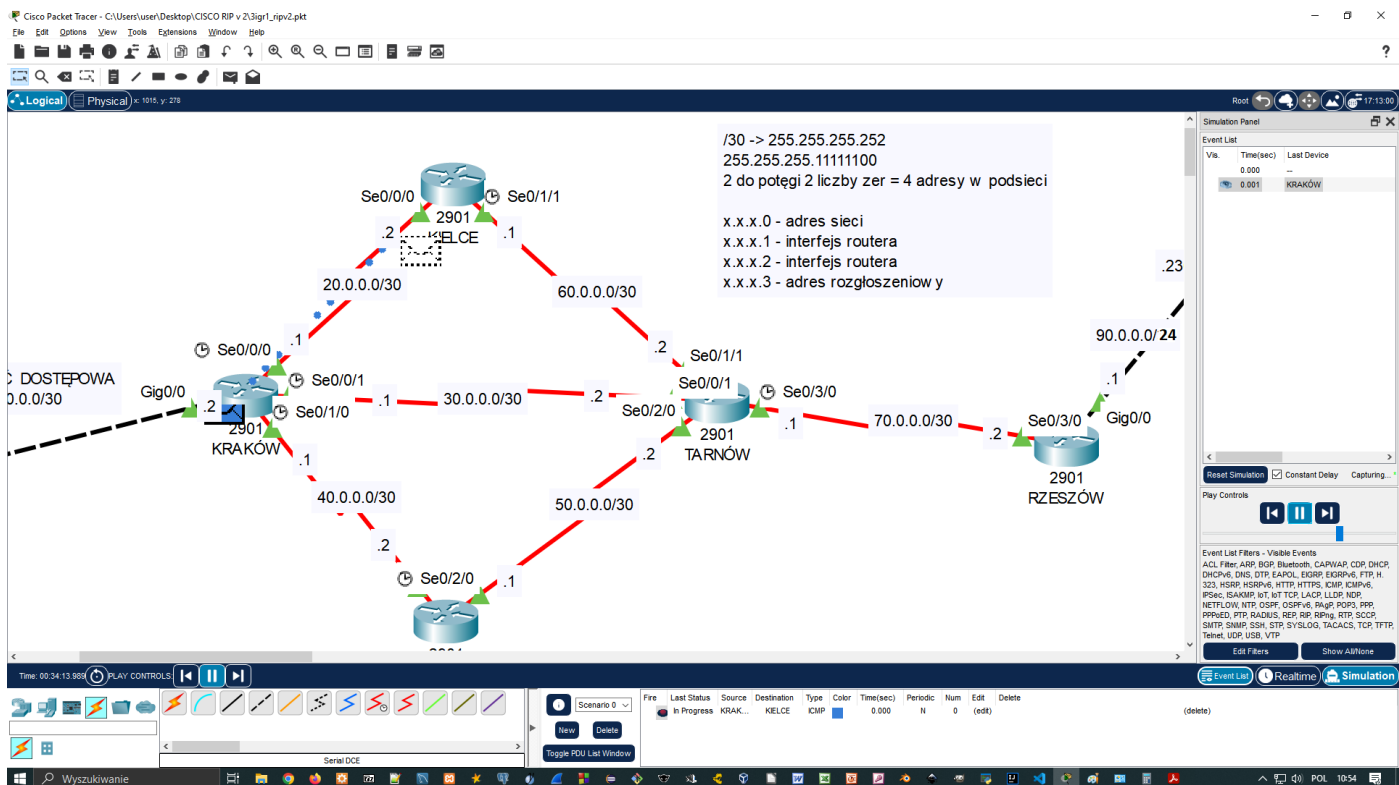
x.x.x.3 - adres rozgłoszeniowy



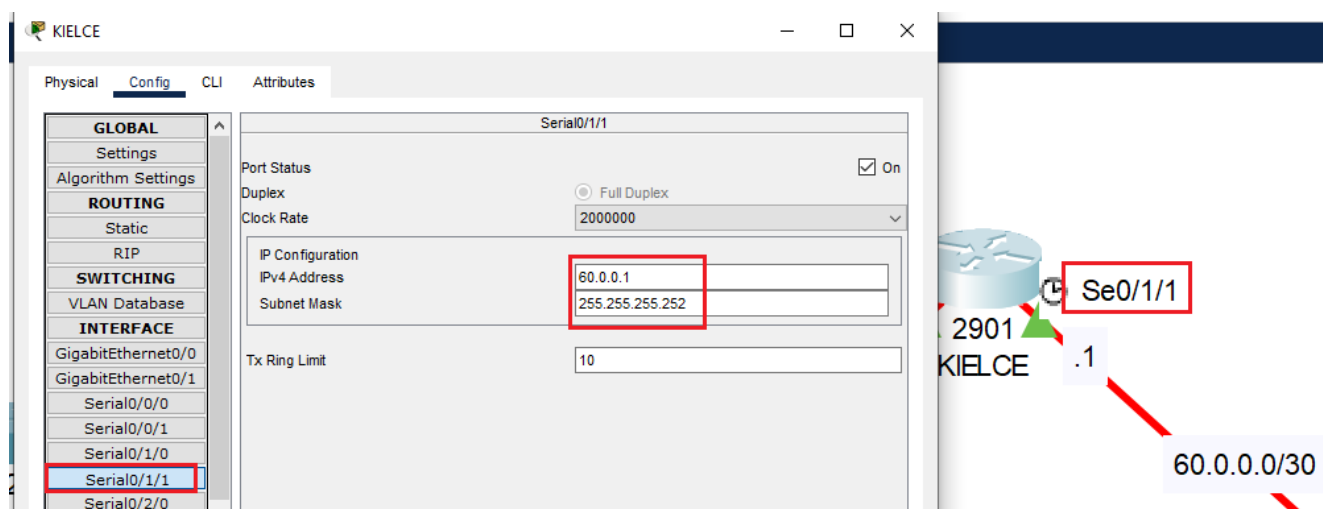
16. Ustaw adresy IPv4 dla poszczególnych interfejsów sieciowych routerów sieci szkieletowej. Poniżej przykład konfiguracji interfejsów Se0/0/0 dla połączenia KRAKÓW - KIELECE



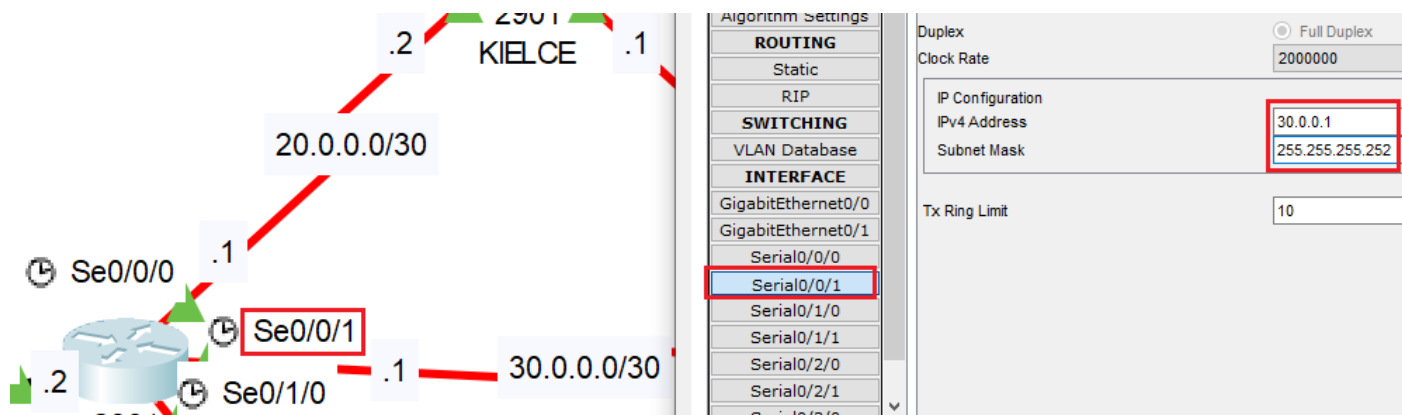
17. Sprawdź połączenie KRAKÓW – KIELCE poleceniem ping (koperta plus)



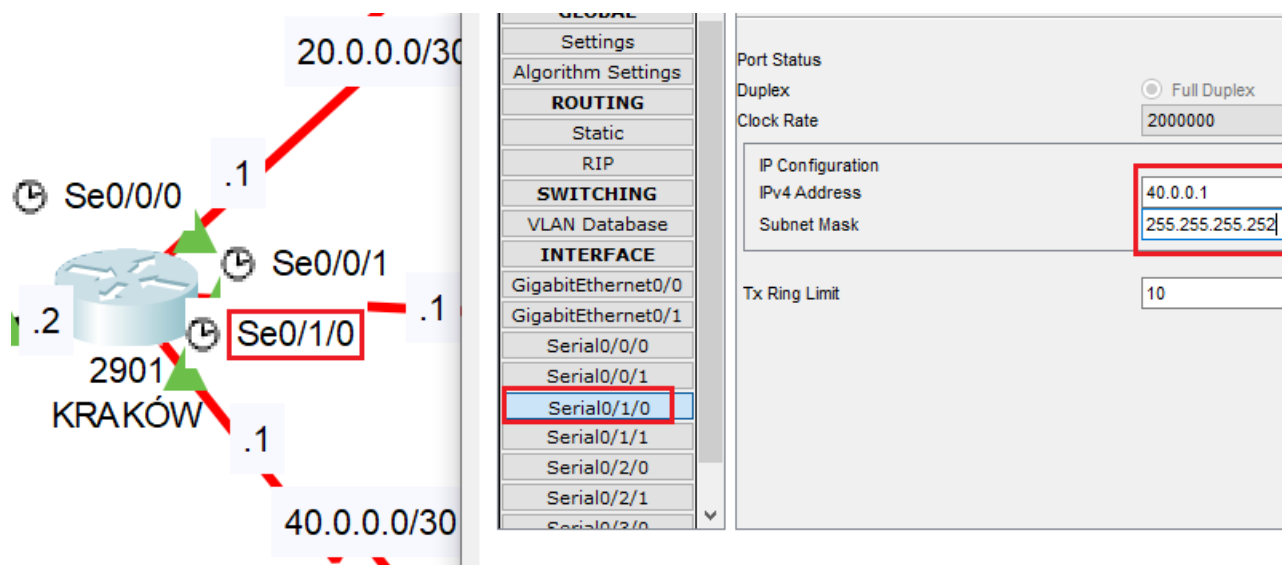
18. Na routerze KIELCE ustaw IPv4 dla połączenia KIELCE - TARNÓW



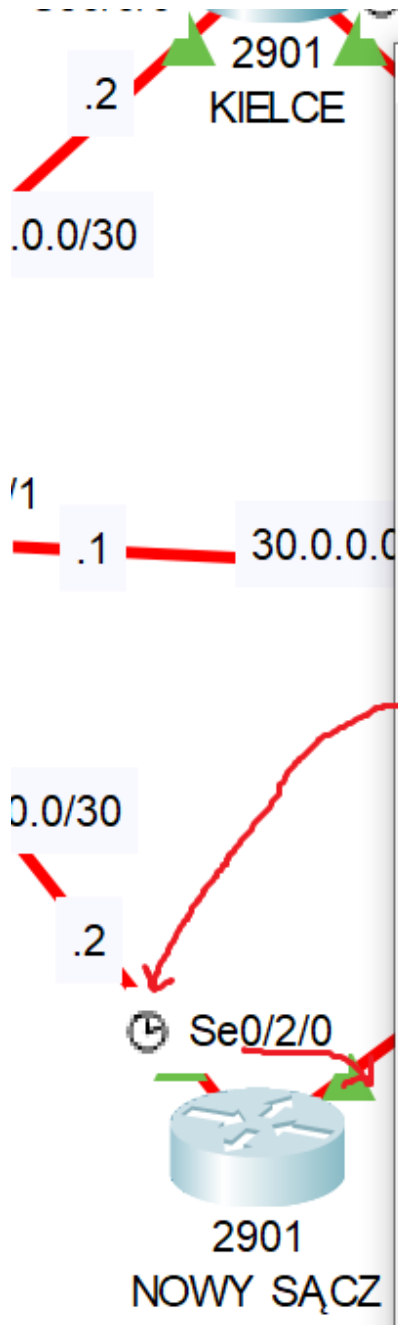
19. Na routerze KRAKÓW ustaw IPv4 dla połączenia KRAKÓW – TARNÓW



20. Na routerze KRAKÓW ustaw IPv4 dla połączenia KRAKÓW – NOWY SĄCZ



21. Na routerze NOWY SĄCZ ustaw IPv4 dla połączenia NOWY SĄCZ – KRAKÓW



NOWY SĄCZ

Physical Config CLI Attributes

GLOBAL	
Settings	
Algorithm Settings	
ROUTING	
Static	
RIP	
SWITCHING	
VLAN Database	
INTERFACE	
GigabitEthernet0/0	
GigabitEthernet0/1	
Serial0/0/0	
Serial0/0/1	
Serial0/1/0	
Serial0/1/1	
Serial0/2/0	
Serial0/2/1	
Serial0/2/2	

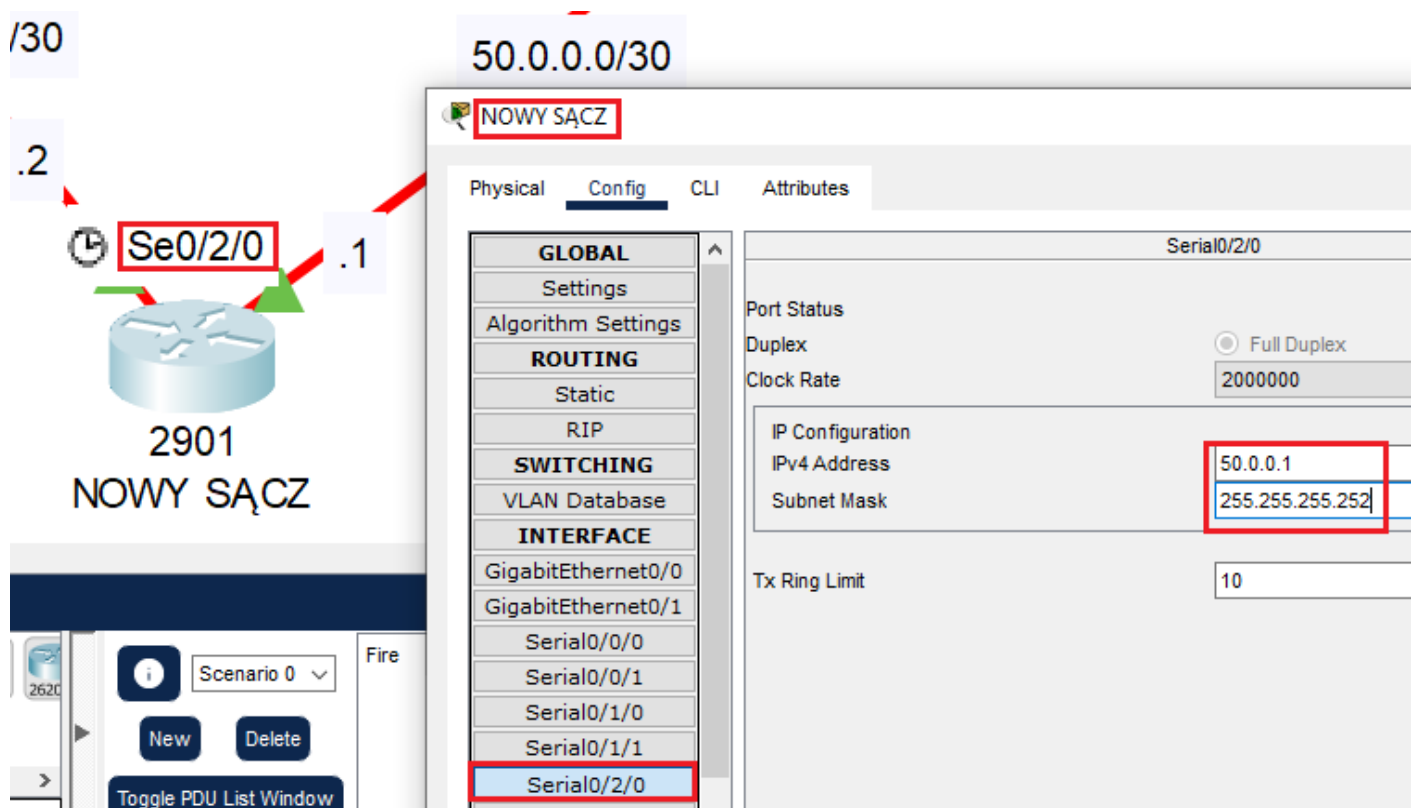
Serial0/1/0	
Port Status	
Duplex	☐ Full Duplex
Clock Rate	2000000
IP Configuration	
IPv4 Address	40.0.0.2
Subnet Mask	255.255.255.252
Tx Ring Limit	10

Equivalent IOS Commands

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed s
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed s

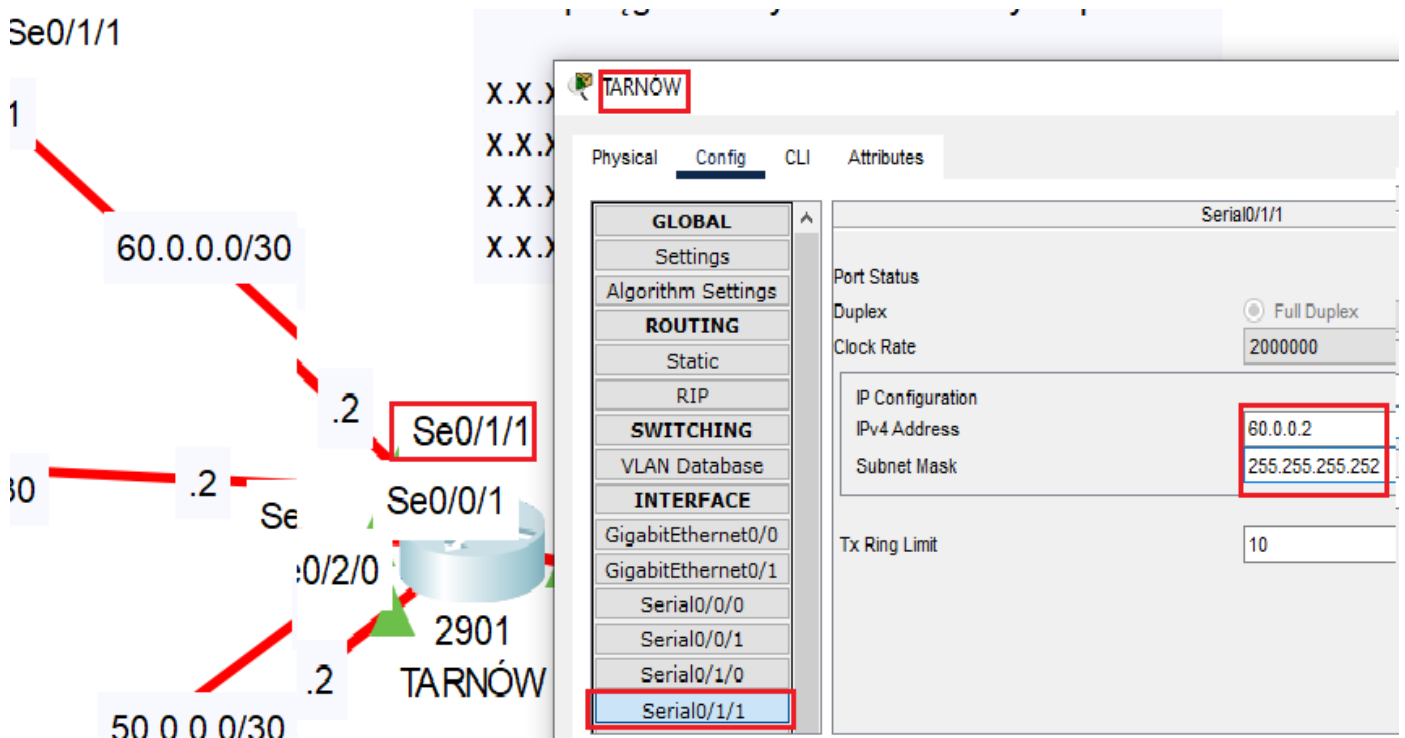
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Serial0/1/0
Router(config-if)#ip address 40.0.0.1 255.0.0.0
Router(config-if)#
```


22. Na routerze NOWY SĄCZ ustaw IPv4 dla połączenia NOWY SĄCZ – TARNÓW



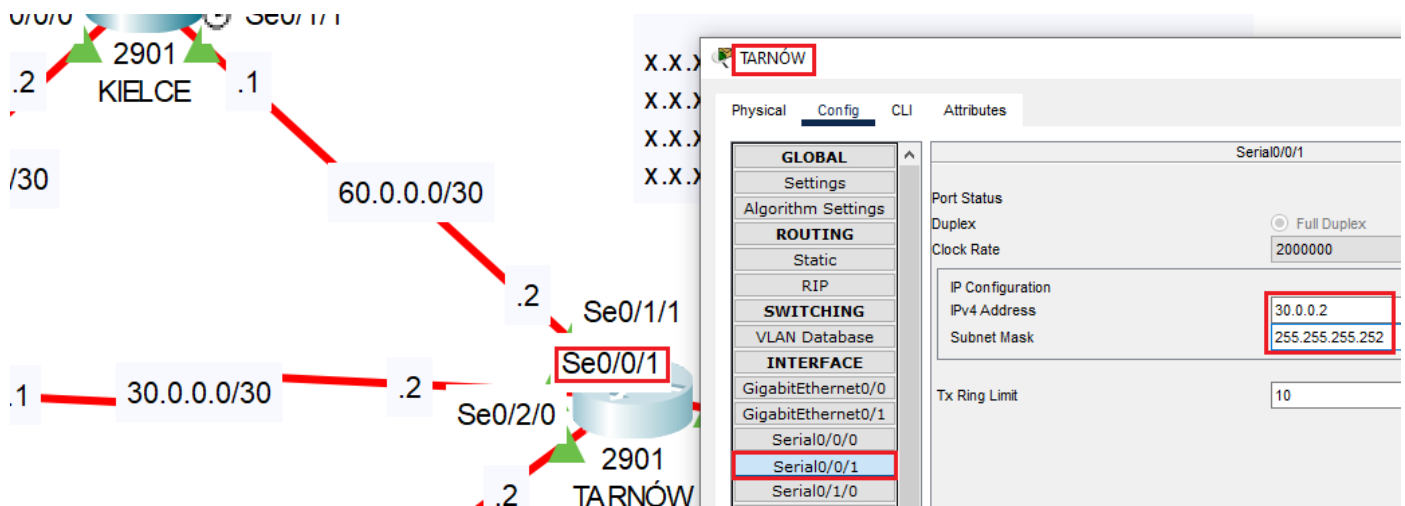
The image shows a network diagram and the configuration interface for Router NOWY SĄCZ. In the diagram, a router labeled '2901 NOWY SĄCZ' has a red arrow pointing to its 'Se0/2/0' interface, which is connected to a network with IP address '50.0.0.0/30'. The configuration window for 'NOWY SĄCZ' is open, showing the 'Config' tab. The 'Serial0/2/0' interface is selected in the 'INTERFACE' list. The 'IP Configuration' section shows the 'IPv4 Address' set to '50.0.0.1' and the 'Subnet Mask' set to '255.255.255.252'. The 'Port Status' section shows 'Duplex' set to 'Full Duplex' and 'Clock Rate' set to '2000000'. The 'Tx Ring Limit' is set to '10'.

23. Na routerze TARNÓW ustaw IPv4 dla połączenia TARNÓW – KIELCE

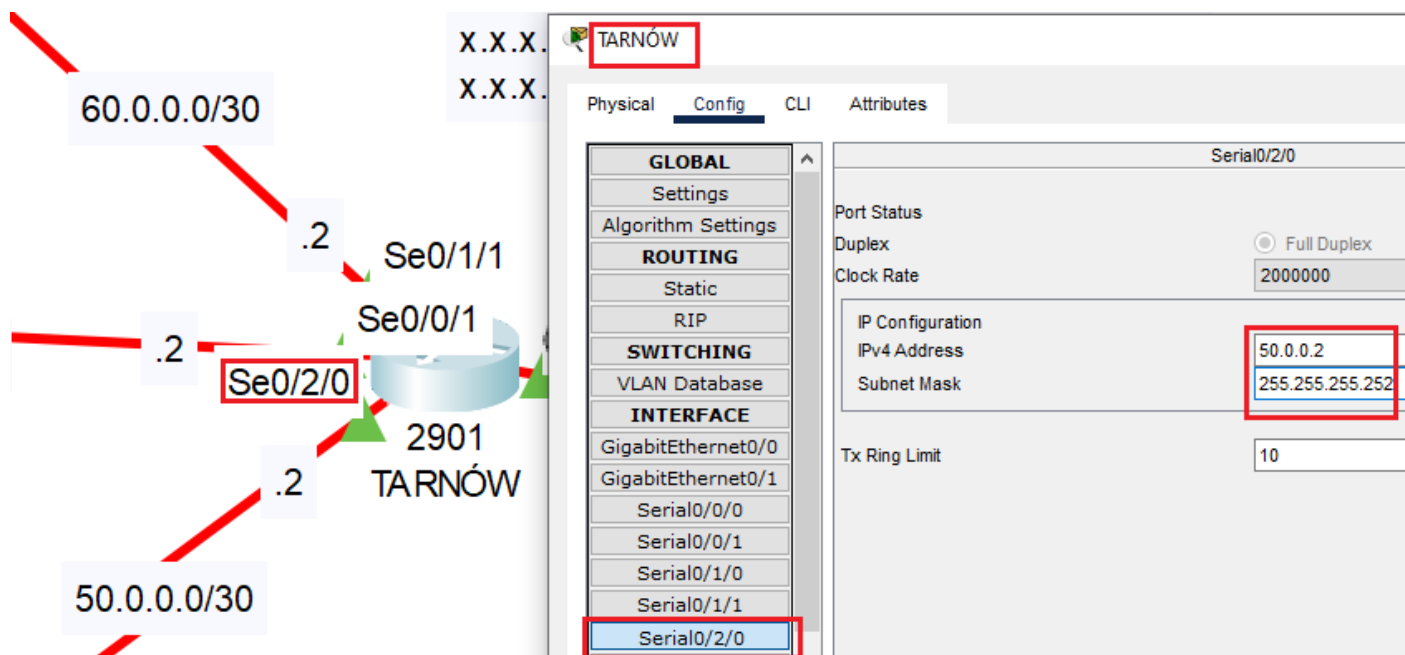


The image shows a network diagram and the configuration interface for Router TARNÓW. In the diagram, a router labeled '2901 TARNÓW' has a red arrow pointing to its 'Se0/1/1' interface, which is connected to a network with IP address '60.0.0.0/30'. The configuration window for 'TARNÓW' is open, showing the 'Config' tab. The 'Serial0/1/1' interface is selected in the 'INTERFACE' list. The 'IP Configuration' section shows the 'IPv4 Address' set to '60.0.0.2' and the 'Subnet Mask' set to '255.255.255.252'. The 'Port Status' section shows 'Duplex' set to 'Full Duplex' and 'Clock Rate' set to '2000000'. The 'Tx Ring Limit' is set to '10'.

24. Na routerze TARNÓW ustaw IPv4 dla połączenia TARNÓW – KRAKÓW



25. Na routerze TARNÓW ustaw IPv4 dla połączenia TARNÓW – NOWY SĄCZ



26. Na routerze TARNÓW ustaw IPv4 dla połączenia TARNÓW – RZESZÓW

TARNÓW

Physical Config CLI Attributes

Serial0/3/0

Port Status ☒ On

Duplex ☐ Full Duplex

Clock Rate 2000000

IP Configuration

IPv4 Address 70.0.0.1

Subnet Mask 255.255.255.252

Tx Ring Limit 10

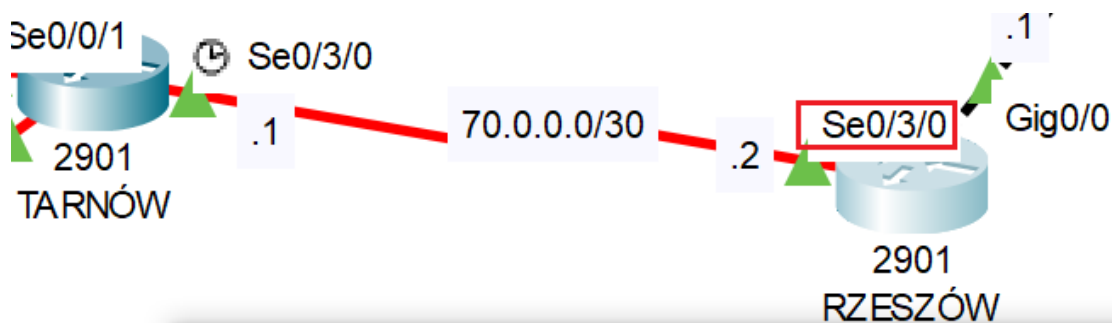
Serial0/3/0

2 do potęgi 2 liczby zer = 4 adresy

x.x.x.0 - adres sieci
x.x.x.1 - interfejs routera
x.x.x.2 - interfejs routera
x.x.x.3 - adres rozgłoszeniowy

Se0/1/1
Se0/0/1
Se0/3/0
2901 TARNÓW
70.0.0.0/30
.1

27. Na routerze RZESZÓW ustaw IPv4 dla połączenia TARNÓW – RZESZÓW



RZESZÓW

Physical Config CLI Attributes

Serial0/3/0

Port Status ☒ On

Duplex ☐ Full Duplex

Clock Rate 2000000

IP Configuration

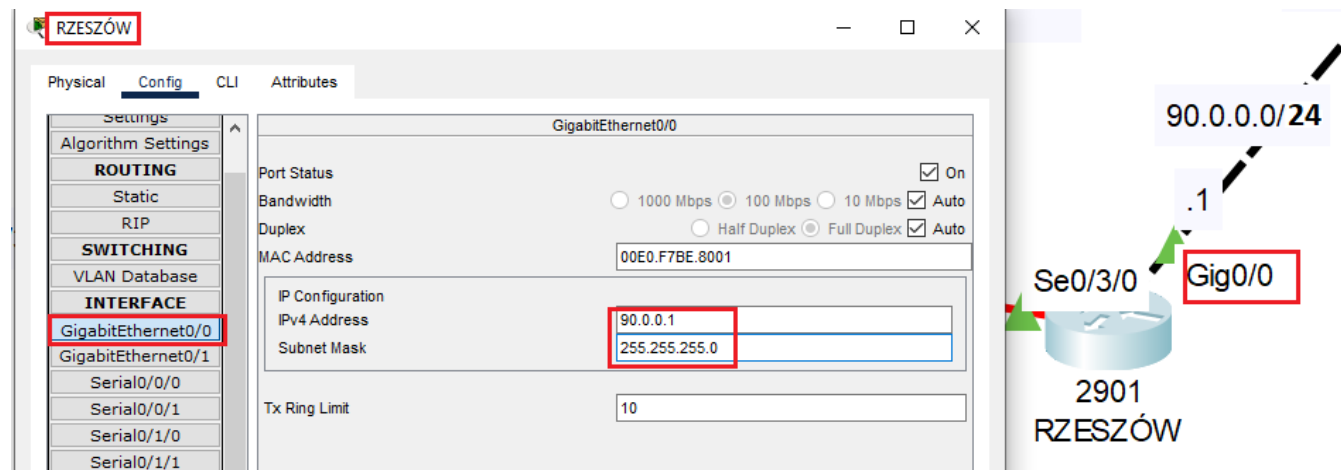
IPv4 Address 70.0.0.2

Subnet Mask 255.255.255.252

Tx Ring Limit 10

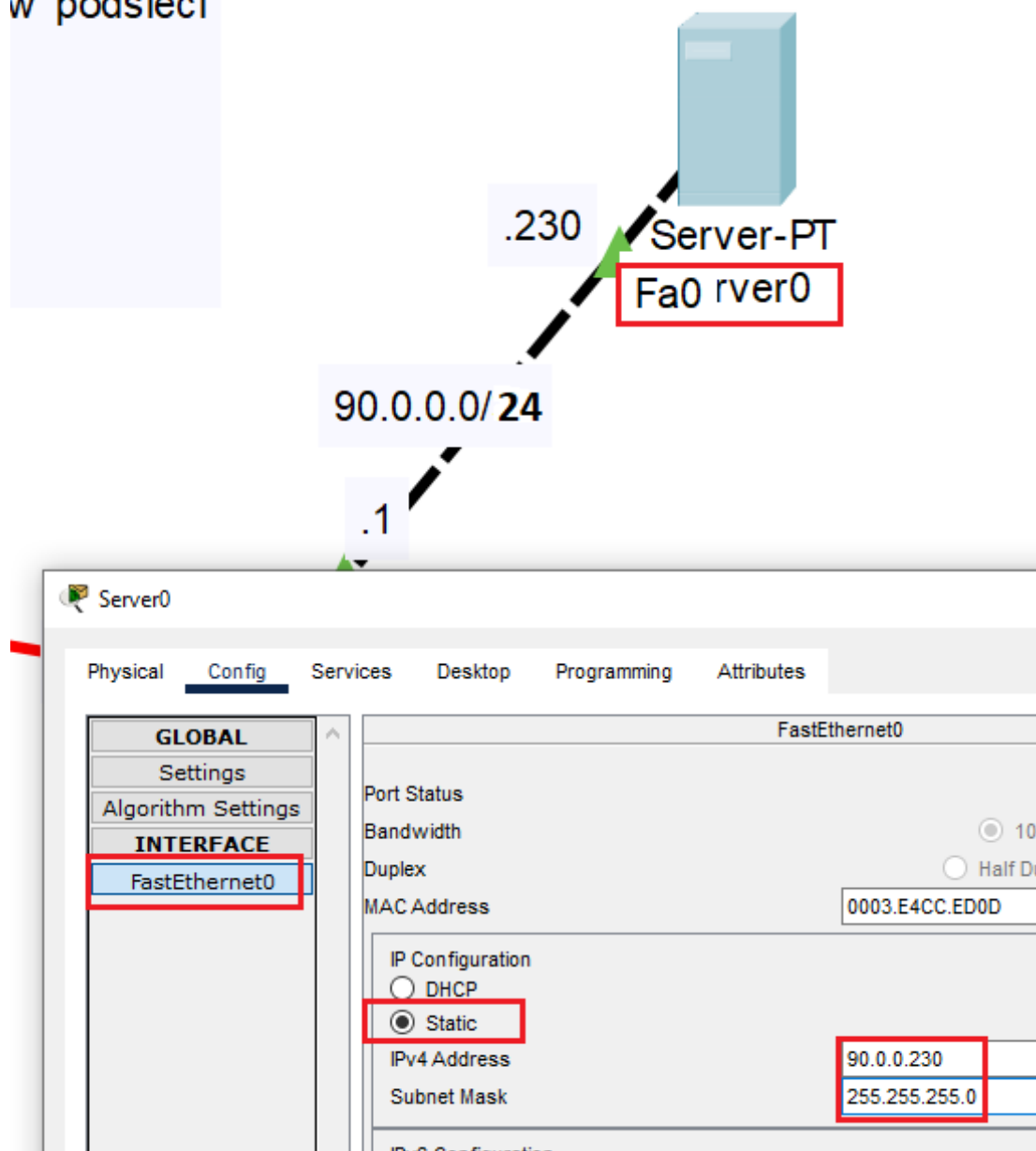
Serial0/3/0

28. Na routerze RZESZÓW ustaw IPv4 dla połączenia z SERWEREM 90.0.0.230



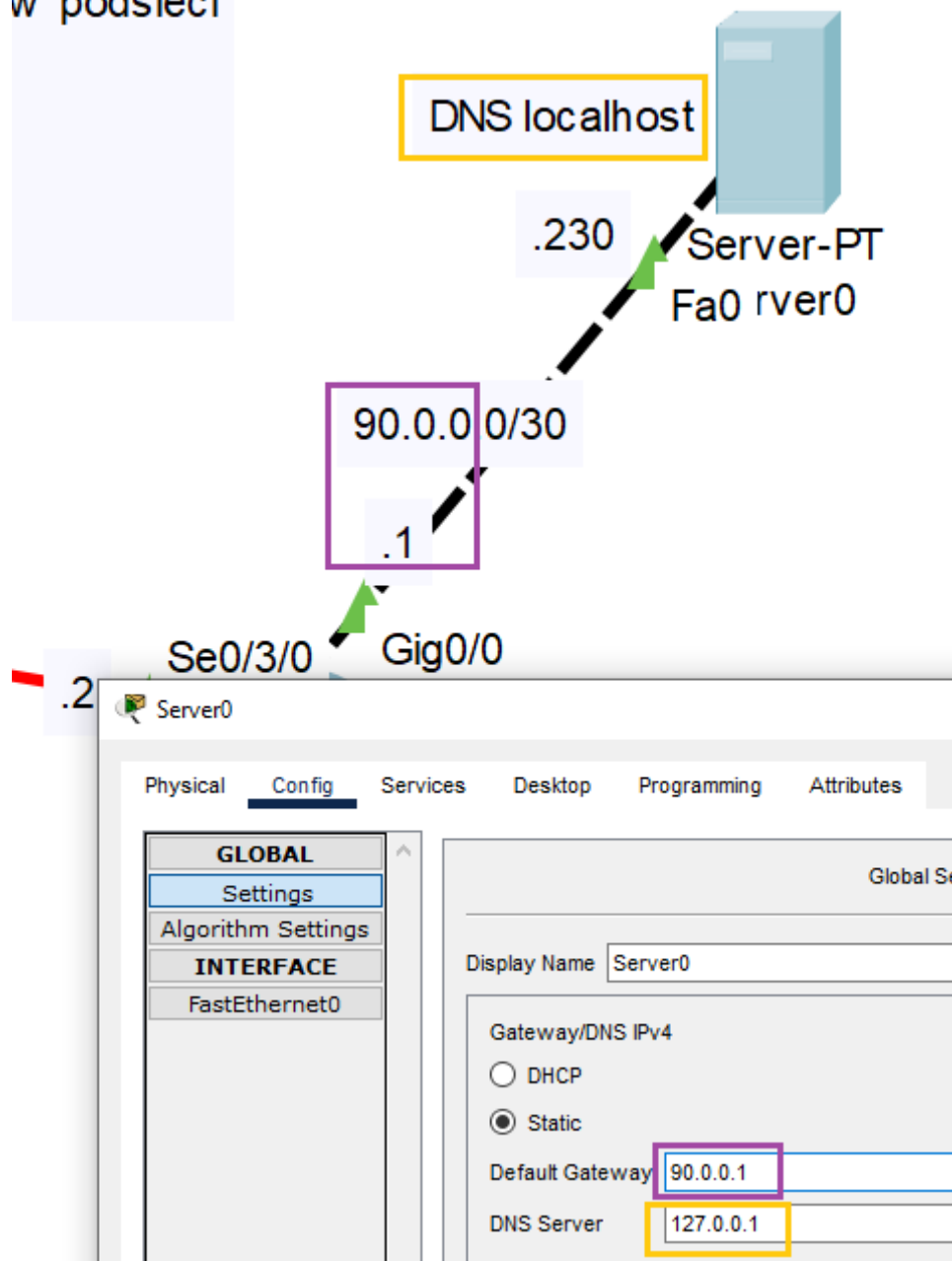
29. Ustaw na Serwerze ustaw IPv4 dla interfejsu sieciowego FastEthernet0

w pod sieci



30. Ustaw brame domyślną i DNS na SERWERZE

w pod sieci



31. Na routrze KRAKÓW ustaw trasę dla sieci docelowej 90.0.0.0/24 prowadzącej przez router KIELCE

2 do potęgi 2 liczby zer = 4 a

Se0/0/0 .2
20.0.0.0/30
.1
Se0/0/1
Se0/1/0 .1
.1
40.0.0.0/30

KRAKÓW

Physical Config CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/0/0

Serial0/0/1

Serial0/1/0

Serial0/1/1

Serial0/2/0

Serial0/2/1

Serial0/3/0

Serial0/3/1

Static Routes

Network 90.0.0.0 docelowa sieć

Mask 255.255.255.0

Next Hop 20.0.0.2 brama na routerze KIELCE

Add

Network Address

90.0.0.0/24 via 20.0.0.2

90.0.0.0/24 dostępna drogą prowadzącą przez bramę 20.0.0.2 na routerze w KIELCE

Remove

32. Na routrze KRAKÓW ustaw trasę dla sieci docelowej 90.0.0.0/24 prowadzącej przez router TARNÓW

2901 KIELCE

20.0.0.0/30
.2
20.0.0.0/30
.1
60.0.0.0/30
.2
30.0.0.0/30
.1
40.0.0.0/30
.1
50.0.0.0/30
.2

KRAKÓW

Physical Config CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/0/0

Serial0/0/1

Serial0/1/0

Serial0/1/1

Serial0/2/0

Serial0/2/1

Serial0/3/0

Serial0/3/1

Static Routes

Network 90.0.0.0

Mask 255.255.255.0

Next Hop 30.0.0.2

Add

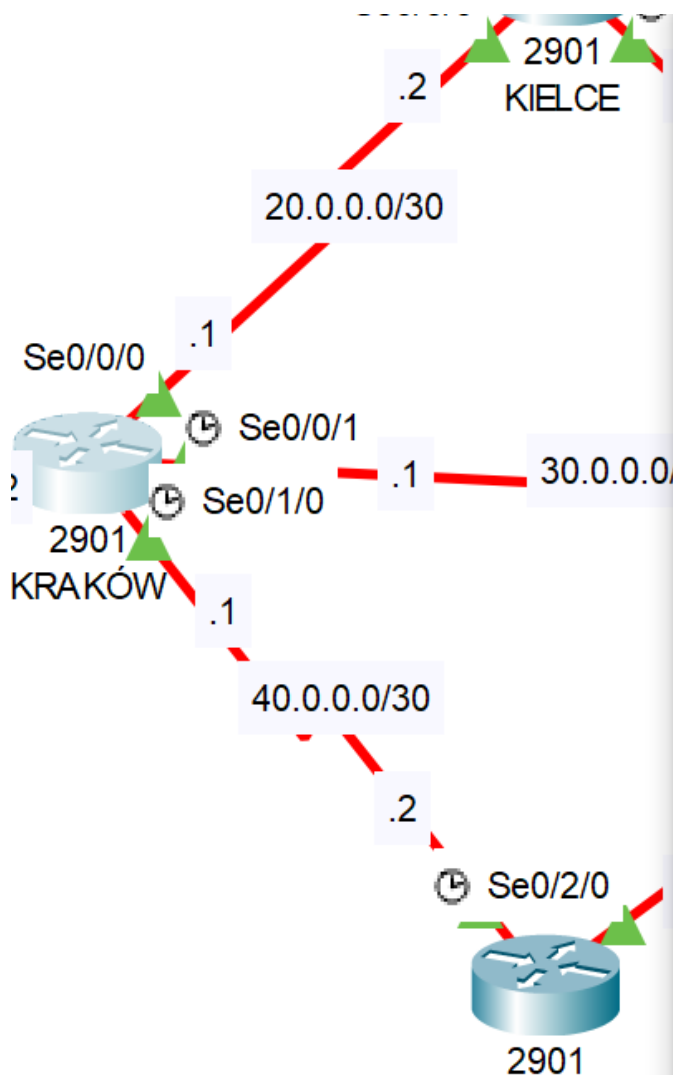
Network Address

90.0.0.0/24 via 20.0.0.2

90.0.0.0/24 via 30.0.0.2

Remove

33. Na routerze KRAKÓW ustaw trasę dla sieci docelowo 90.0.0.0/24 prowadzącą przez router NOWY SĄCZ



KRAKÓW

Physical Config CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/0/0

Serial0/0/1

Serial0/1/0

Serial0/1/1

Serial0/2/0

Serial0/2/1

Serial0/3/0

Serial0/3/1

Static Route

Network 90.0.0.0

Mask 255.255.255.0

Next Hop 40.0.0.2

Network Address

90.0.0.0/24 via 20.0.0.2

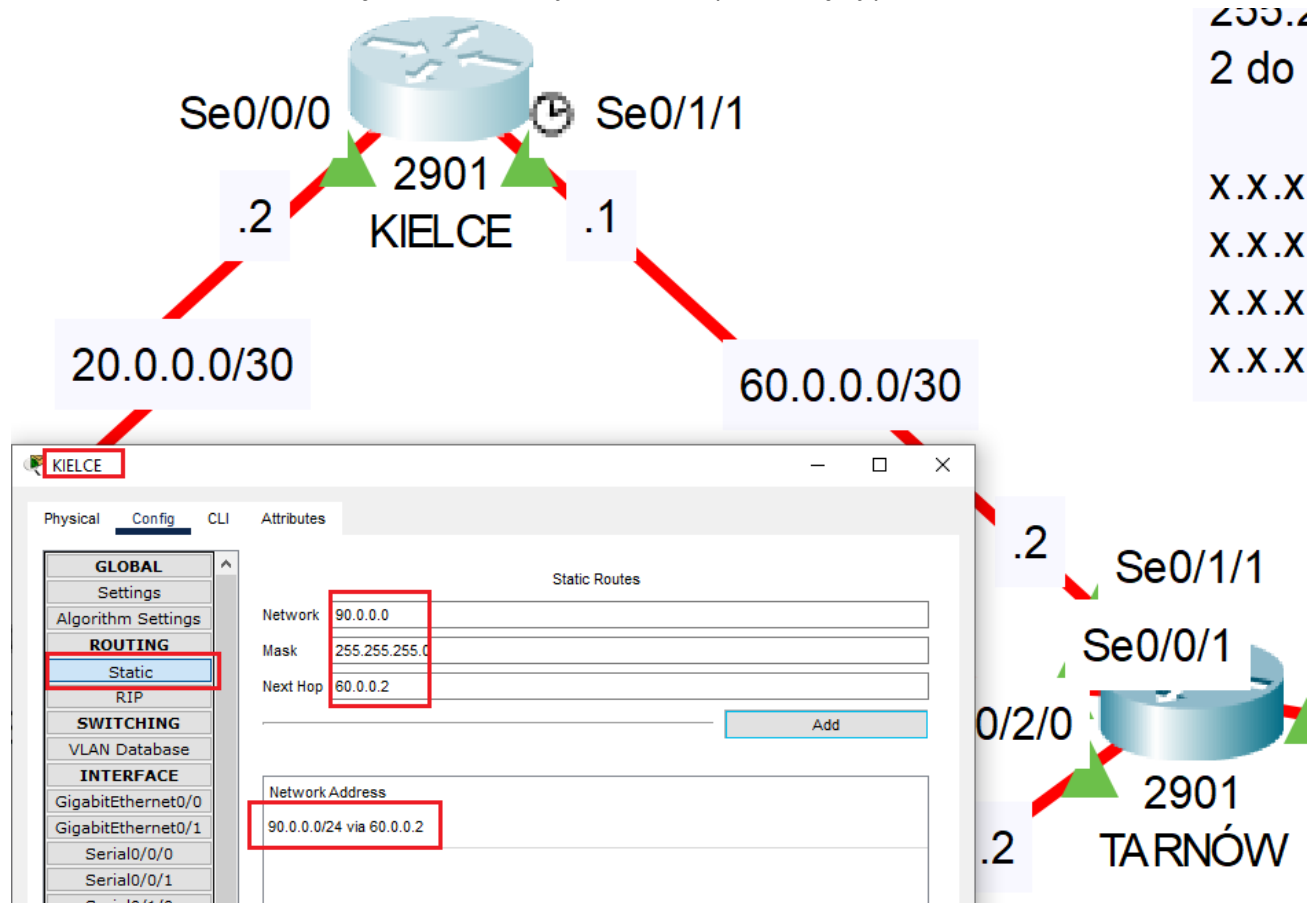
90.0.0.0/24 via 30.0.0.2

90.0.0.0/24 via 40.0.0.2

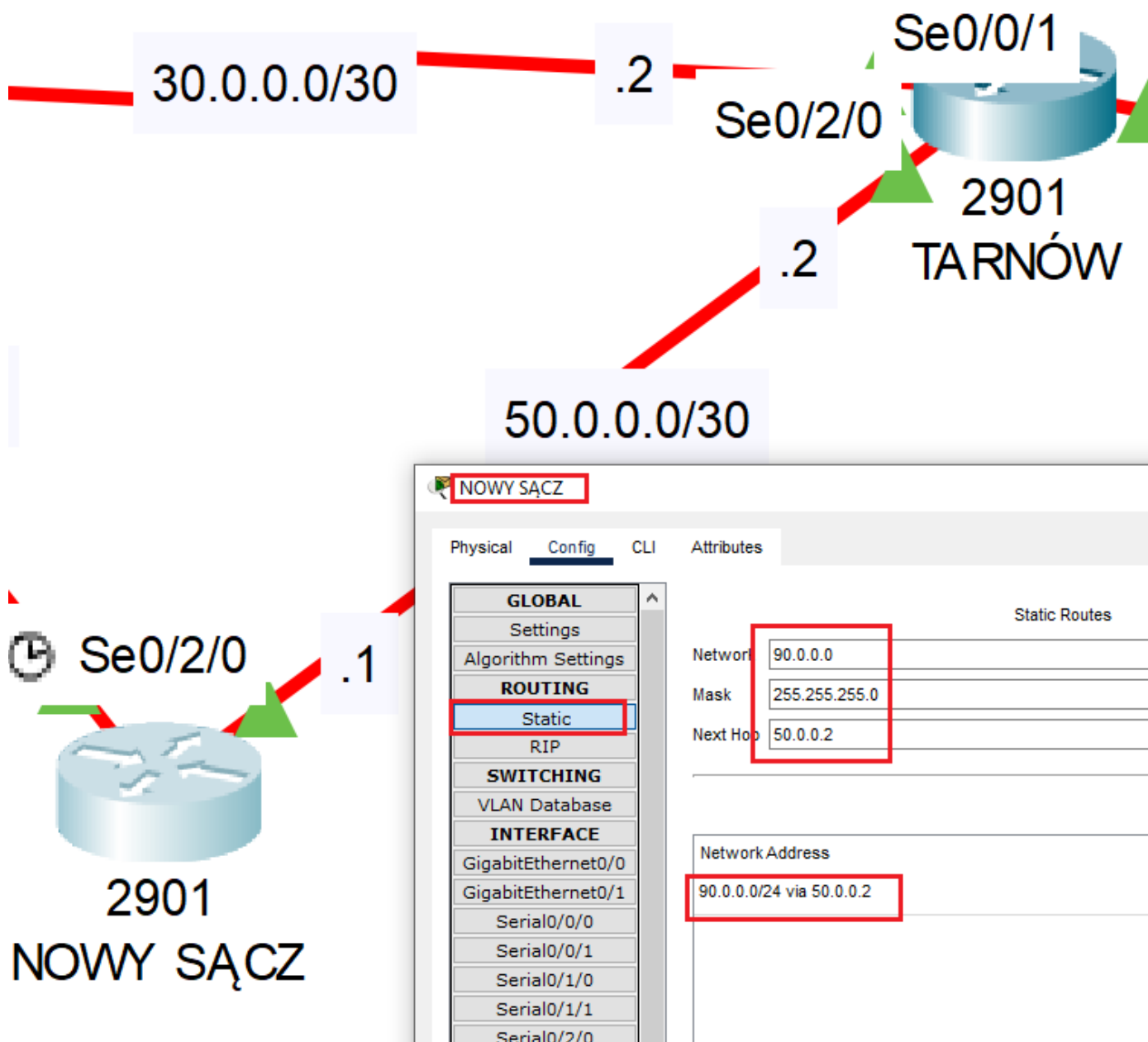
Equivalent IOS Commands

```
Router#enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL
Router(config)#
Router(config)#ip route 90.0.0.0 255.255.255.0 20.0.0.1
%Invalid next hop address (it's this router)
Router(config)#ip route 90.0.0.0 255.255.255.0 20.0.0.2
Router(config)#ip route 90.0.0.0 255.255.255.0 30.0.0.2
Router(config)#ip route 90.0.0.0 255.255.255.0 40.0.0.2
Router(config)#
```

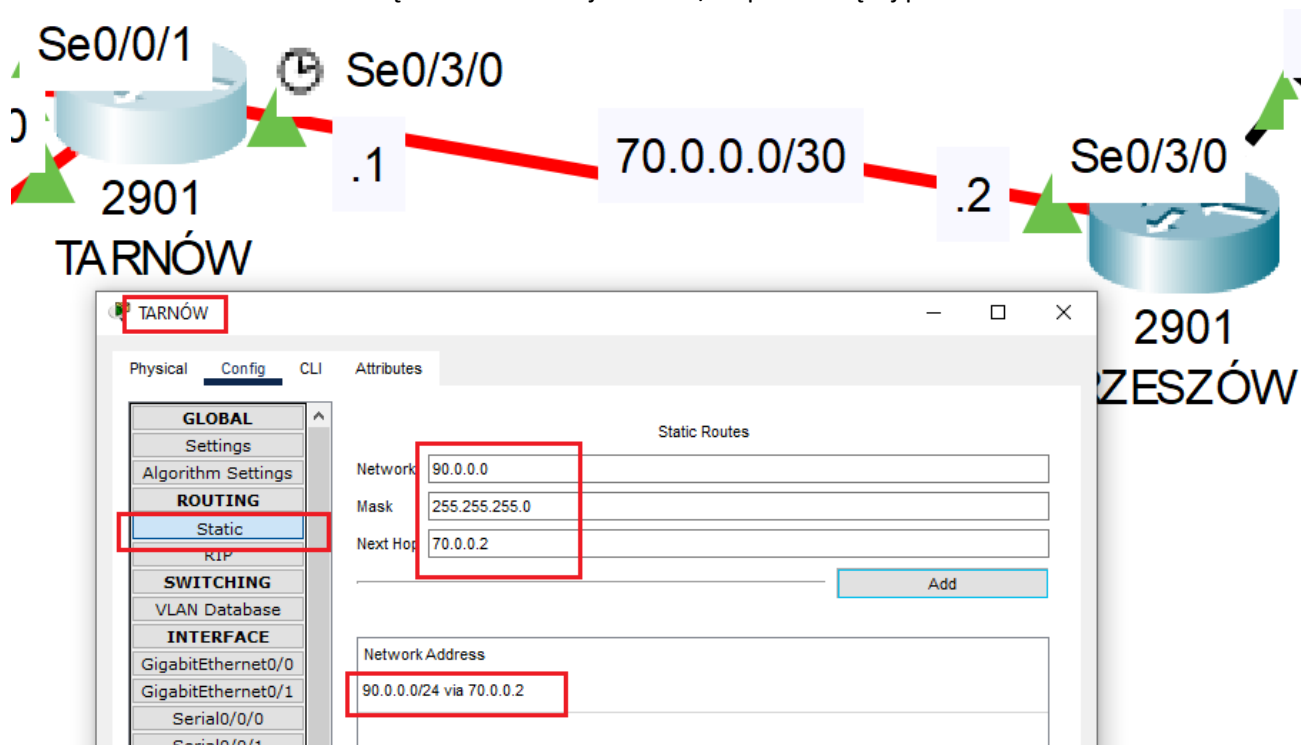

34. Na routrze KIELCE ustaw trasę dla sieci docelowo 90.0.0.0/24 prowadzącą przez router TARNÓW



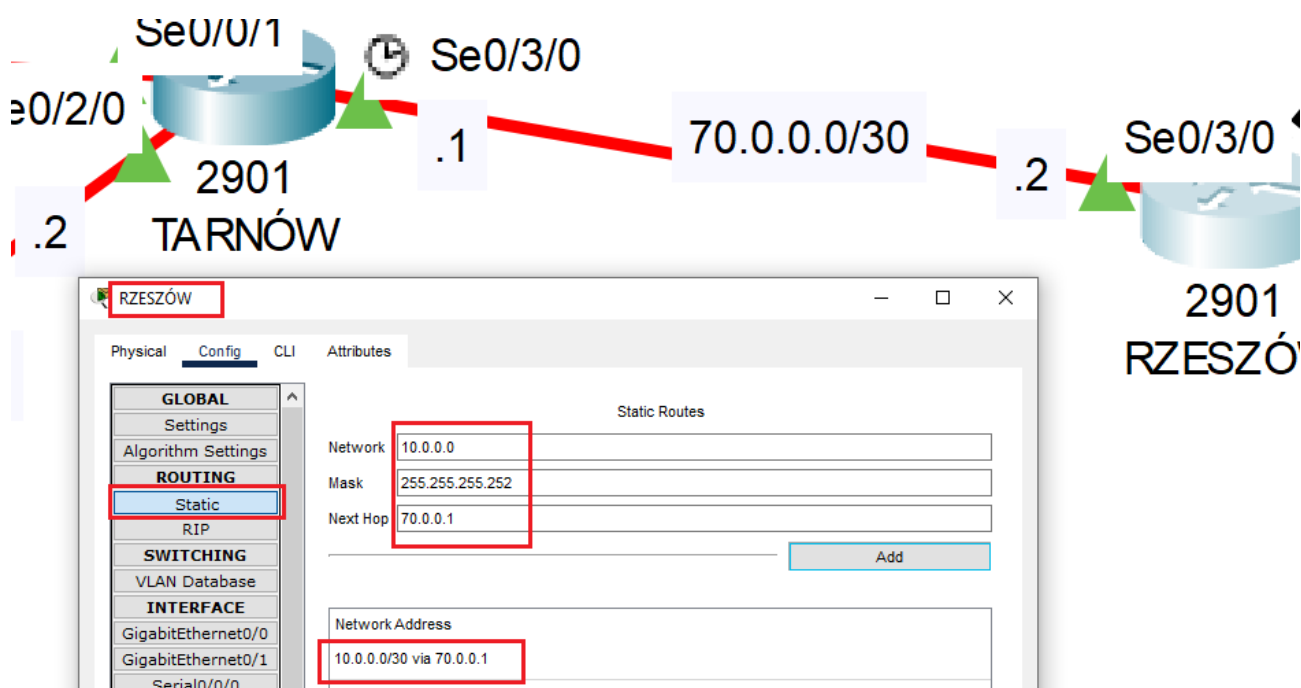
35. Na routerze NOWY SĄCZ ustaw trasę dla sieci docelowej 90.0.0.0/24 prowadzącą przez router TARNÓW



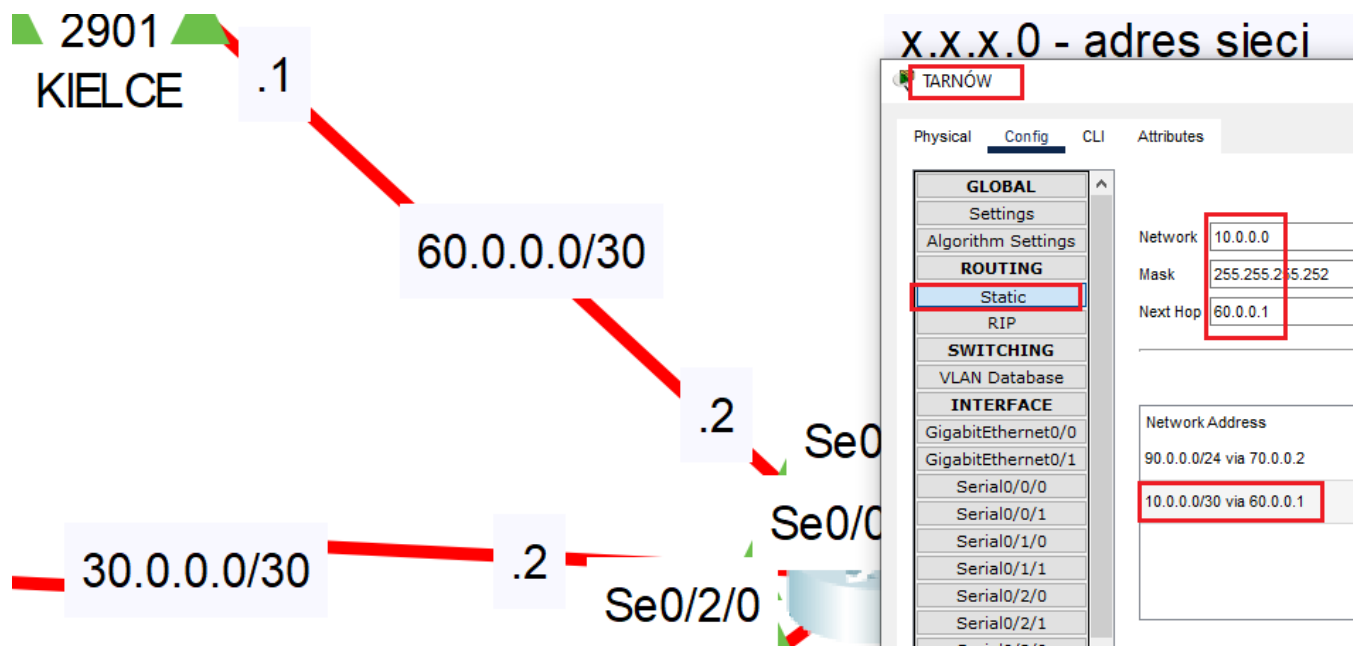
36. Na routerze TARNÓW ustaw trasę dla sieci docelowej 90.0.0.0/24 prowadzącej przez router RZESZÓW



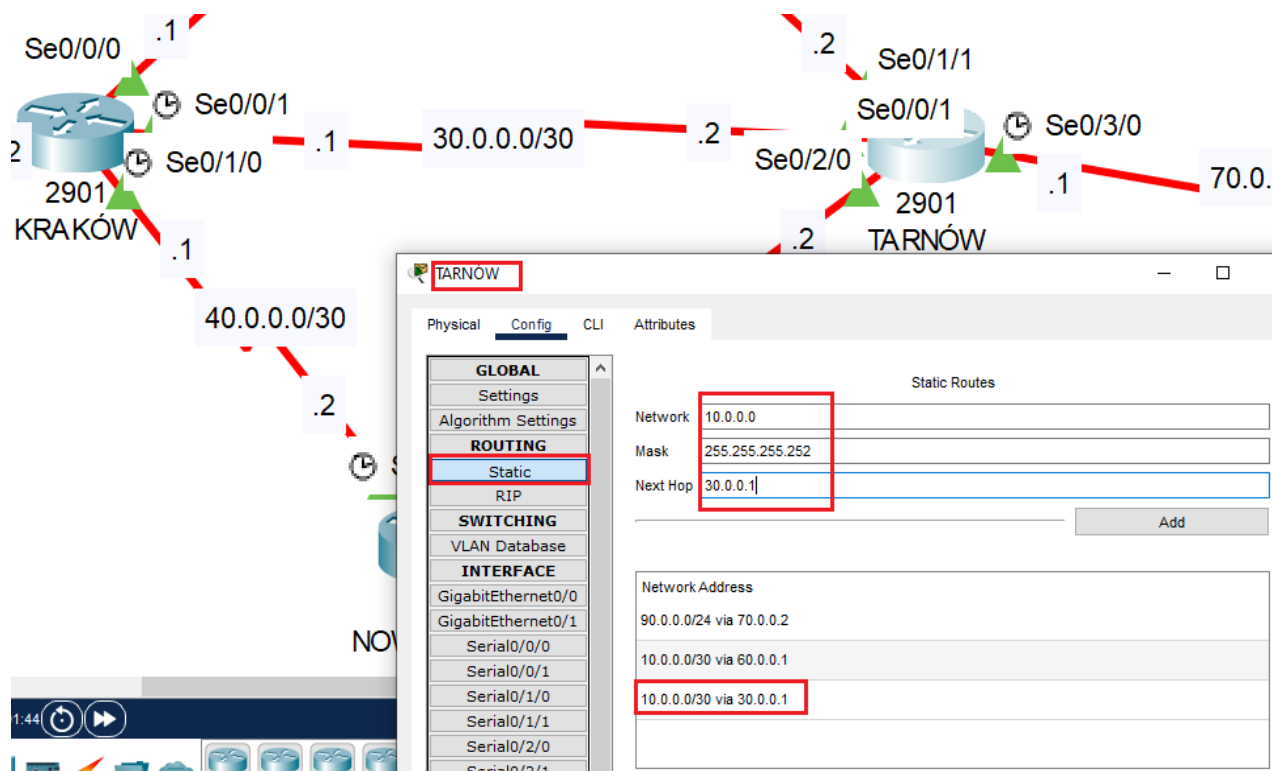
37. Na routerze RZESZÓW ustaw trasę dla sieci docelowej 10.0.0.0/30 prowadzącej przez router TARNÓW



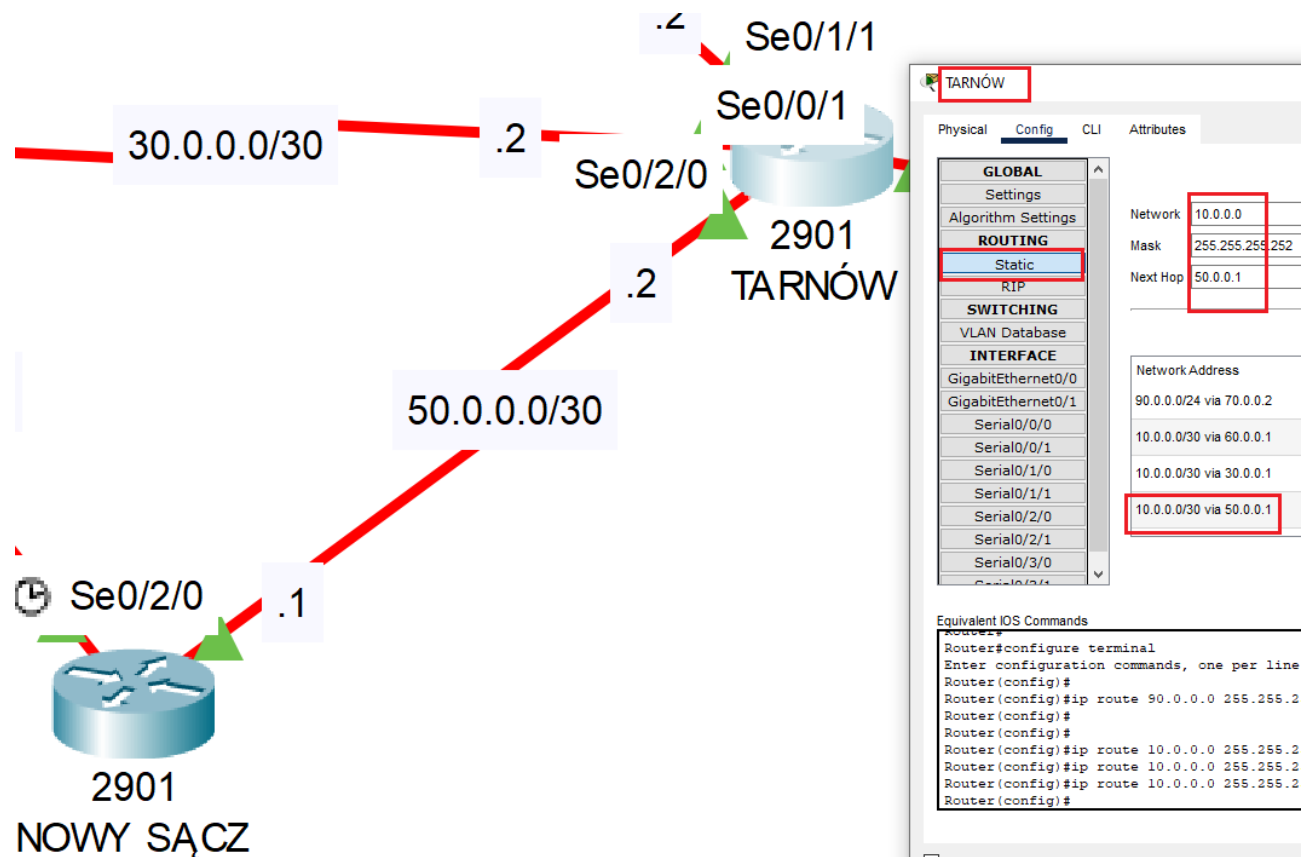
38. Na routerze TARNÓW ustaw trasę dla sieci docelowej 10.0.0.0/30 prowadzącą przez router KIELCE



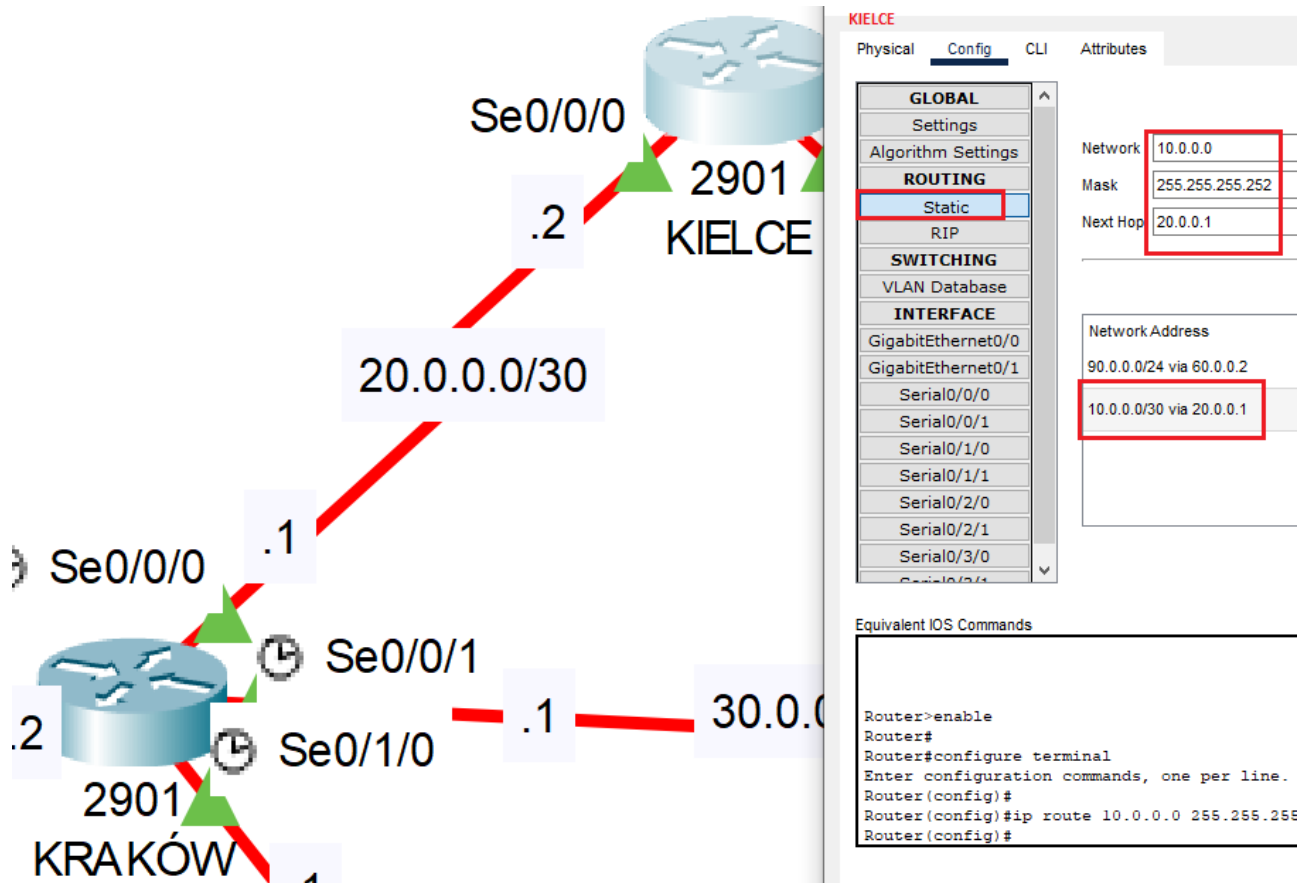
39. Na routerze TARNÓW ustaw trasę dla sieci docelowej 10.0.0.0/30 prowadzącą przez router KRAKÓW



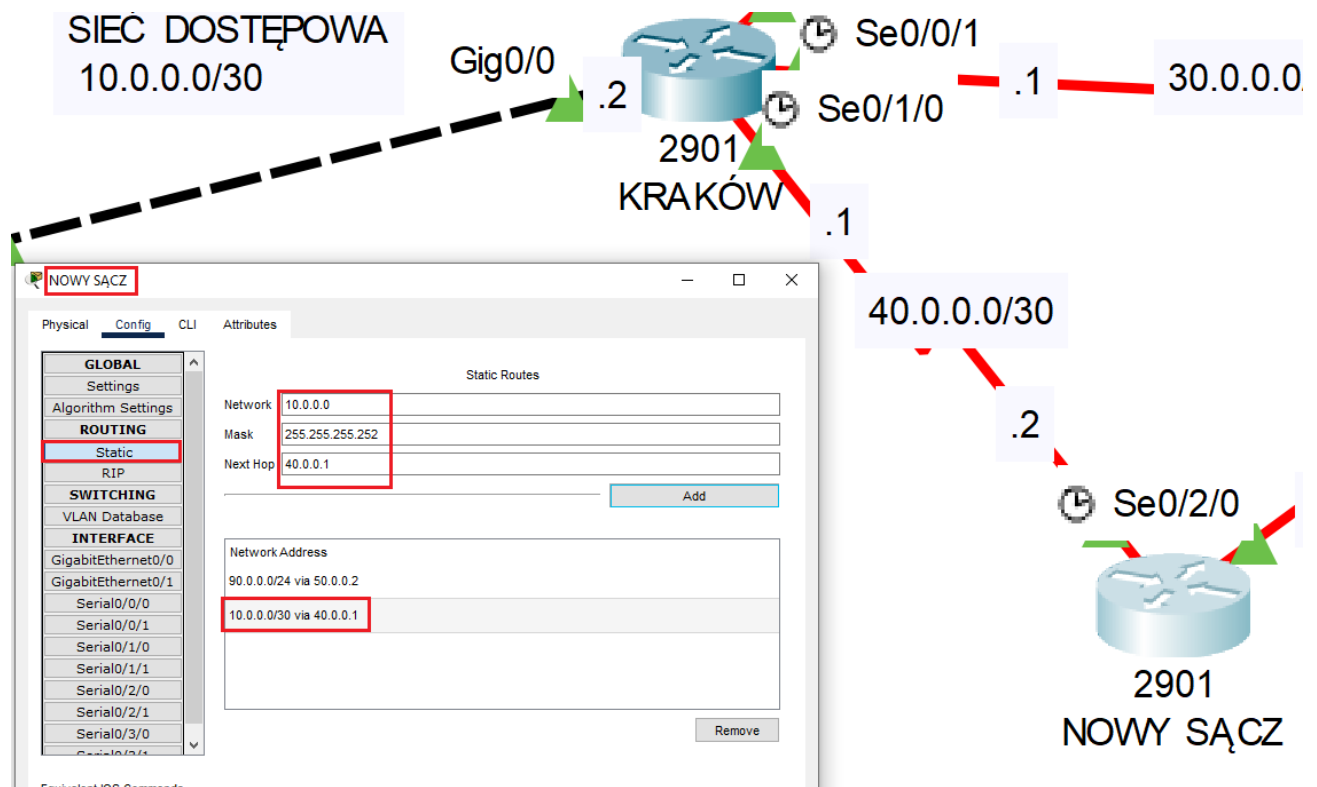
40. Na routerze TARNÓW ustaw trasę dla sieci docelowej 10.0.0.0/30 prowadzącą przez router NOWY SĄCZ



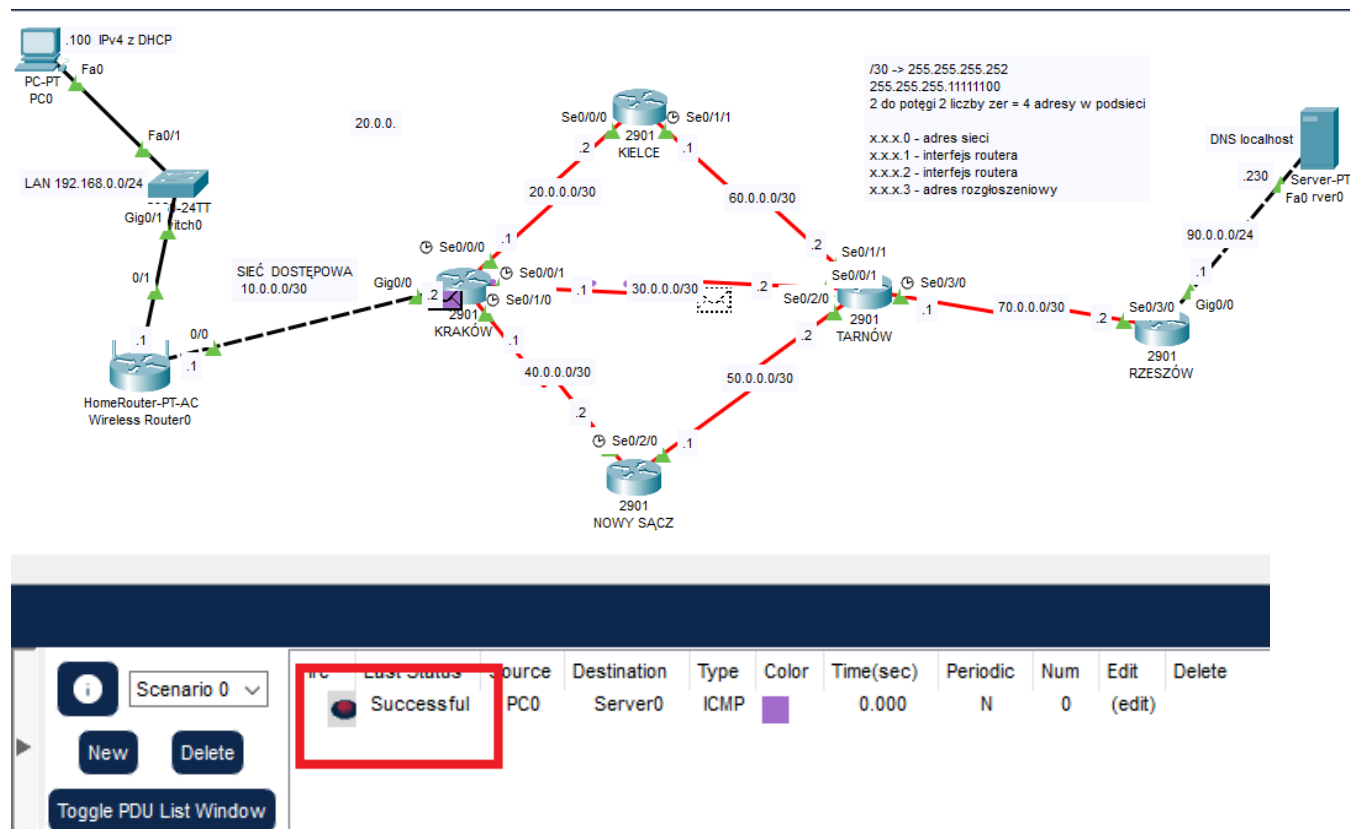
41. Na routrze KIELCE ustaw trasę dla sieci docelowo 10.0.0.0/30 prowadzącą przez router KRAKÓW



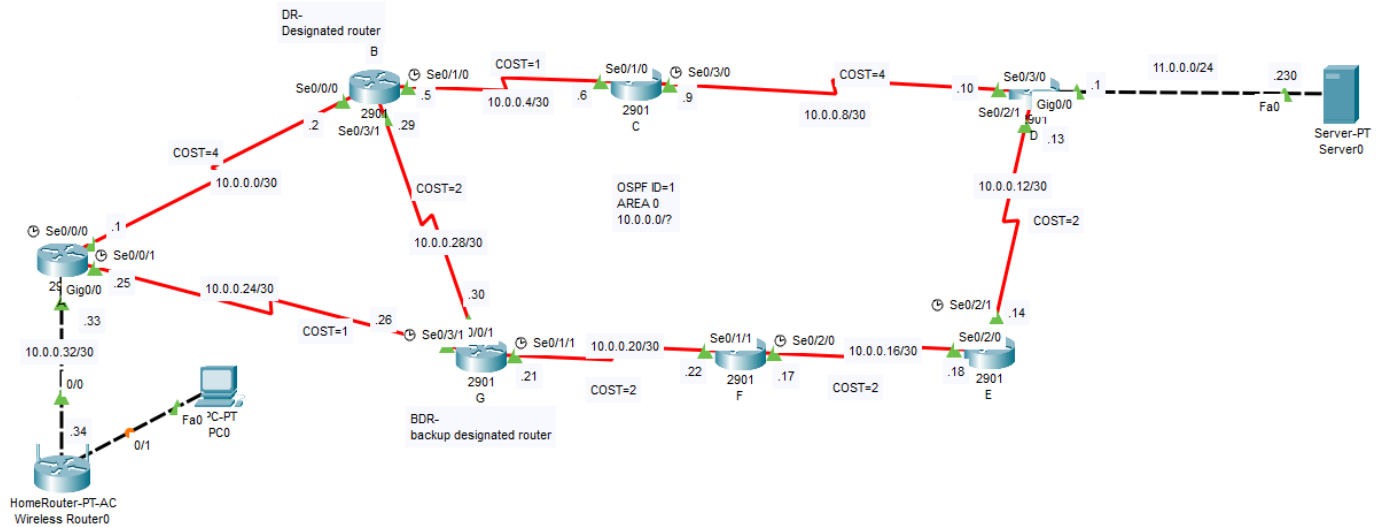
42. Na routerze NOWY SĄCZ ustaw trasę dla sieci docelowej 10.0.0.0/30 prowadzącą przez router KRAKÓW



43. Wykonaj pingowanie ze stacji roboczej (tutaj PC0) na SERWER



4.2 Protokół routingu OSPF - Cisco Packet



RouterA

Zmiana nazwy

Router>enable

Router#conf terminal

Router(config)#hostname RA

RA(config)#exit

RA#show ip route

Codes: L - local, C - connected, S - static, 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

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

C 10.0.0.0/30 is directly connected, Serial0/0/0
L 10.0.0.1/32 is directly connected, Serial0/0/0
C 10.0.0.24/30 is directly connected, Serial0/0/1
L 10.0.0.25/32 is directly connected, Serial0/0/1

USTAWIANIE KOSZTU TRAS

RA>enable

RA#conf t

RA(config)#interface s0/0/0

RA(config-if)#ip ospf cost 4

RA(config-if)#exit

RA(config)#interface s0/0/1

RA(config-if)#ip ospf cost 1

RA(config-if)#exit

RA(config)#exit

RA#

RB>enable

RB#conf t

RB(config)#interface s0/0/0

RB(config-if)#ip ospf cost 4

RB(config-if)#exit

RB(config)#interface s0/1/0

RB(config-if)#ip ospf cost 1

RB(config-if)#exit

RB(config)#interface s0/3/1

RB(config-if)#ip ospf cost 2

i tak na każdym routerze

```
RC(config)#interface s0/3/0
```

```
RC(config-if)#ip ospf cost 4
```

DODAWANIE PODSIECI DO OSPF

maska podsieci	maska blankietowa
255.255.255.252	0.0.0.3
11111111.11111111.	00000000.00000000
11111111.11111100	00000000.00000011 == 3
255.255.255.0	0.0.0.255
11111111.11111111.	00000000.00000000
11111111.11111100	00000000.11111111 == 255

```
RA>enable
```

```
RA#conf t
```

```
RA(config)#router ospf 1
```

```
RA(config-router)#network 10.0.0.0 0.0.0.3 area 0
```

```
RA(config-router)#network 10.0.0.24 0.0.0.3 area 0
```

```
RB>enable
```

```
RB#conf t
```

```
RB(config)#router ospf 1
```

```
RB(config-router)#network 10.0.0.0 0.0.0.3 area 0
```

```
RB(config-router)#network 10.0.0.4 0.0.0.3 area 0
```

```
RB(config-router)#network 10.0.0.28 0.0.0.3 area 0
```

```
RC#conf t
```

```
RC(config)#router ospf 1
```

```
RC(config-router)#network 10.0.0.4 0.0.0.3 area 0
```

```
RC(config-router)#network 10.0.0.8 0.0.0.3 area 0
```

i tak na wszystkich pozostałych routerach

```
RA#show ip route ospf
```

```
10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
```

- O 10.0.0.4 [110/4] via 10.0.0.26, 00:52:39, Serial0/0/1
- O 10.0.0.8 [110/8] via 10.0.0.26, 00:52:39, Serial0/0/1
- O 10.0.0.12 [110/7] via 10.0.0.26, 00:52:39, Serial0/0/1
- O 10.0.0.16 [110/5] via 10.0.0.26, 00:52:39, Serial0/0/1
- O 10.0.0.20 [110/3] via 10.0.0.26, 00:52:39, Serial0/0/1
- O 10.0.0.28 [110/3] via 10.0.0.26, 00:52:39, Serial0/0/1

ZMIANA IDENTYFIKATORA ROUTERA

RB TO DESIGNATED ROUTER (DR)

RB>enable

RB#conf t

RB(config)#router ospf 1

RB(config-router)#router-id 1.1.1.1

RB(config-router)#exit

RB(config)#exit

RB#clear ip ospf process

Reset ALL OSPF processes? [no]: y

RB#show ip protocols

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 1.1.1.1

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

10.0.0.0 0.0.0.3 area 0

10.0.0.4 0.0.0.3 area 0

10.0.0.28 0.0.0.3 area 0

Routing Information Sources:

Gateway	Distance	Last Update
1.1.1.1	110	00:01:45
10.0.0.9	110	00:01:45
10.0.0.13	110	00:26:16
10.0.0.18	110	00:26:17

10.0.0.22	110	00:26:17
10.0.0.25	110	00:01:55
10.0.0.29	110	00:26:17
10.0.0.30	110	00:01:54

Distance: (default is 110)

RG>enable

RG#conf t

RG(config)#router ospf 1

RG(config-router)#router-id 2.2.2.2

RG(config-router)#exit

RG(config)#exit

RG#clear ip ospf process

Reset ALL OSPF processes? [no]: y

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 2.2.2.2

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

10.0.0.20 0.0.0.3 area 0

10.0.0.28 0.0.0.3 area 0

10.0.0.24 0.0.0.3 area 0

Routing Information Sources:

Gateway	Distance	Last Update
1.1.1.1	110	00:00:17
2.2.2.2	110	00:00:17

10.0.0.9	110	00:17:41
10.0.0.13	110	00:12:10
10.0.0.18	110	00:12:10
10.0.0.22	110	00:00:22
10.0.0.25	110	00:00:34
10.0.0.29	110	00:42:12
10.0.0.30	110	00:17:50

DODANIE SERWERA DO SIECI 11.0.0.0/24

NA ROUTERZE RD WŁĄCZ SIEĆ 11.0.0.0/24 DO OSPF 1

```
RD#conf t
```

```
RD(config)#router ospf 1
```

```
RD(config-router)#network 11.0.0.0 0.0.0.255 area 0
```

DODANIE HOME ROUTERA DO SIECI 10.0.0.32/24

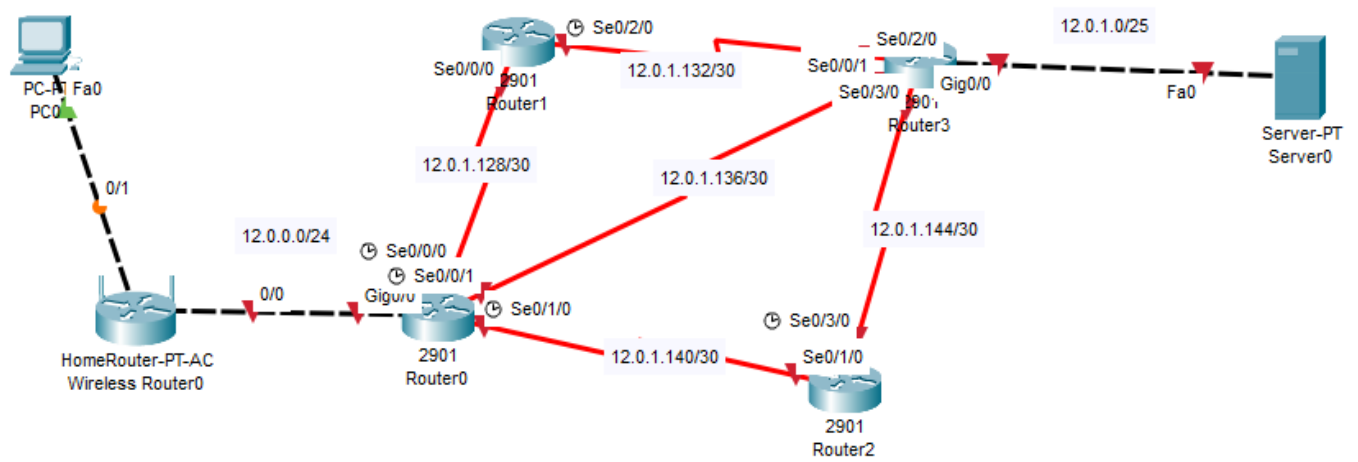
NA ROUTERZE RA WŁĄCZ SIEĆ 10.0.0.32/30 DO OSPF 1

```
RA#conf t
```

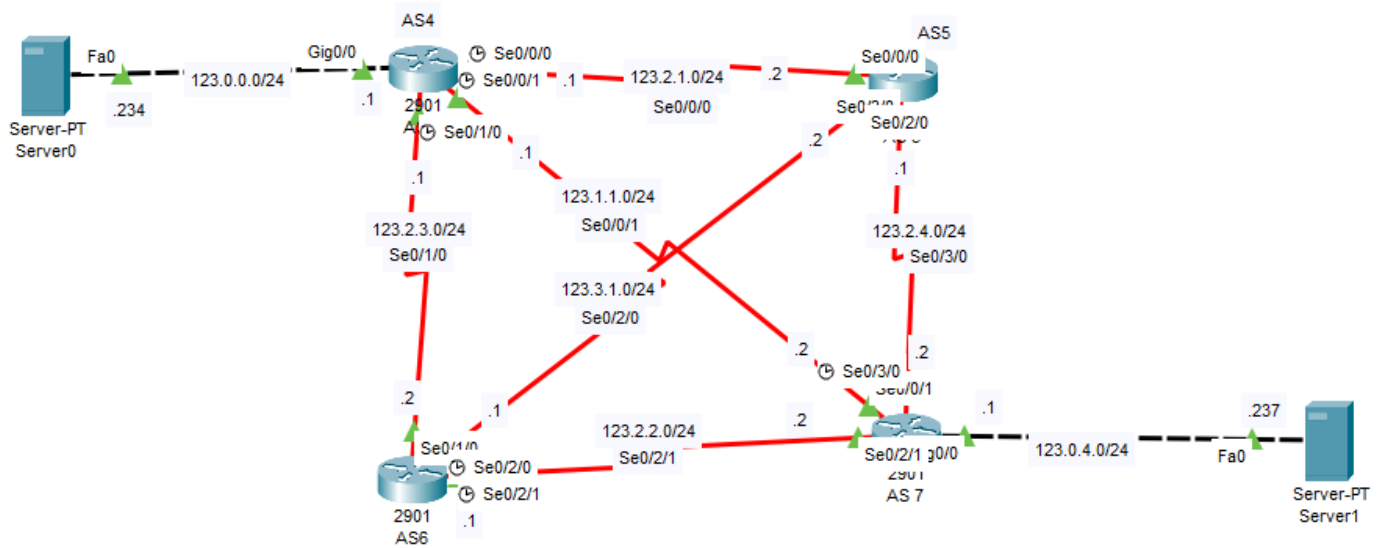
```
RA(config)#router ospf 1
```

```
RA(config-router)#network 10.0.0.32 0.0.0.3 area 0
```

OSPF ĆWICZENIA



4.3 Protokół routingu BGP - Cisco Packet



PROTOKÓŁ ROUTINGU BRAM ZEWNĘTRZNYCH STREF AUTONOMICZNYCH

ang. Border Gateway Protocol - BGP

```
Router>enable
```

```
Router#conf t
```

```
Router(config)#hostname AS4
```

```
AS4(config)#interface Loopback4
```

```
AS4(config-if)#ip address 4.4.4.4 255.255.255.0
```

```
AS4(config-if)#exit
```

```
AS4(config)#router bgp 4
```

```
AS4(config-router)#neighbor 123.2.1.2 remote-as 5
```

```
AS4(config-router)#neighbor 123.2.3.2 remote-as 6
```

```
AS4(config-router)#neighbor 123.1.1.2 remote-as 7
```

```
AS4(config-router)#network 4.4.4.4 mask 255.255.255.0
```

```
AS4(config-router)#network 123.0.0.0 mask 255.255.255.0
```

```
AS4(config-router)#network 123.2.1.0 mask 255.255.255.0
```

```
AS4(config-router)#network 123.1.1.0 mask 255.255.255.0
```

```
AS4(config-router)#network 123.2.3.0 mask 255.255.255.0
```


Router>enable

Router#conf t

Router(config)#hostname AS5

AS5(config)#interface Loopback5

AS5(config-if)#ip address 5.5.5.5 255.255.255.0

AS5(config-if)#exit

AS5(config)#router bgp 5

AS5(config-router)#neighbor 123.2.1.1 remote-as 4

AS5(config-router)#neighbor 123.3.1.1 remote-as 6

AS5(config-router)#neighbor 123.2.4.2 remote-as 7

AS5(config-router)#network 5.5.5.5 mask 255.255.255.0

AS5(config-router)#network 123.2.1.0 mask 255.255.255.0

AS5(config-router)#network 123.3.1.0 mask 255.255.255.0

AS5(config-router)#network 123.2.4.0 mask 255.255.255.0

Router>enable

Router#conf t

Router(config)#hostname AS6

AS6(config)#interface Loopback6

AS6(config-if)#ip address 6.6.6.6 255.255.255.0

AS6(config-if)#exit

AS6(config)#router bgp 6

AS6(config-router)#neighbor 123.2.3.1 remote-as 4

AS6(config-router)#neighbor 123.3.1.2 remote-as 5

AS6(config-router)#neighbor 123.2.2.2 remote-as 7

AS6(config-router)#network 6.6.6.6 mask 255.255.255.0

AS6(config-router)#network 123.2.3.0 mask 255.255.255.0

AS6(config-router)#network 123.3.1.0 mask 255.255.255.0

AS6(config-router)#network 123.2.2.0 mask 255.255.255.0

Router#conf t

Router(config)#hostname AS7

AS7(config)#interface Loopback7

AS7(config-if)#ip address 7.7.7.7 255.255.255.0

AS7(config-if)#exit

AS7(config)#router bgp 7

AS7(config-router)#neighbor 123.1.1.1 remote-as 4

AS7(config-router)#neighbor 123.2.4.1 remote-as 5

AS7(config-router)#neighbor 123.2.2.1 remote-as 6

AS7(config-router)#network 7.7.7.7 mask 255.255.255.0

AS7(config-router)#network 123.1.1.0 mask 255.255.255.0

AS7(config-router)#network 123.2.4.0 mask 255.255.255.0

AS7(config-router)#network 123.2.2.0 mask 255.255.255.0

AS7(config-router)#network 123.0.4.0 mask 255.255.255.0

AS4#show ip route bgp

B 6.6.6.0 [20/0] via 123.2.3.2, 00:00:00

B 7.7.7.0 [20/0] via 123.1.1.2, 00:00:00

B 123.0.4.0/24 [20/0] via 123.1.1.2, 00:00:00

B 123.2.2.0/24 [20/0] via 123.1.1.2, 00:00:00

B 123.2.4.0/24 [20/0] via 123.1.1.2, 00:00:00

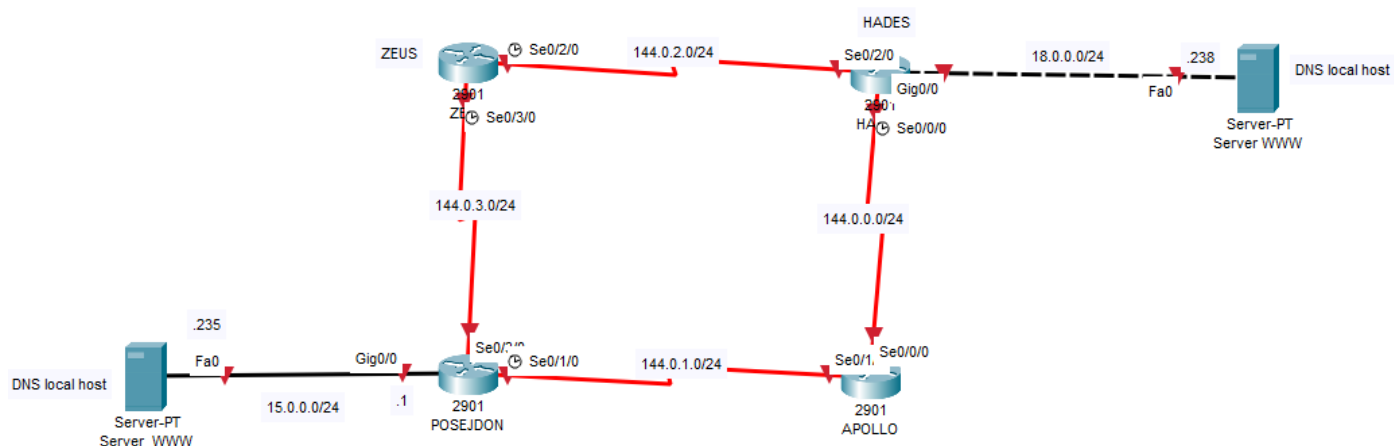
B 123.3.1.0/24 [20/0] via 123.2.3.2, 00:00:00

AS5#show ip route bgp

B 4.4.4.0 [20/0] via 123.2.1.1, 00:00:00
B 6.6.6.0 [20/0] via 123.3.1.1, 00:00:00
B 7.7.7.0 [20/0] via 123.2.4.2, 00:00:00
B 123.0.0.0/24 [20/0] via 123.2.1.1, 00:00:00
B 123.0.4.0/24 [20/0] via 123.2.4.2, 00:00:00
B 123.1.1.0/24 [20/0] via 123.2.4.2, 00:00:00
B 123.2.2.0/24 [20/0] via 123.2.4.2, 00:00:00
B 123.2.3.0/24 [20/0] via 123.3.1.1, 00:00:00

AS6#show ip route bgp

B 4.4.4.0 [20/0] via 123.2.3.1, 00:00:00
B 7.7.7.0 [20/0] via 123.2.2.2, 00:00:00
B 123.0.0.0/24 [20/0] via 123.2.3.1, 00:00:00
B 123.0.4.0/24 [20/0] via 123.2.2.2, 00:00:00
B 123.1.1.0/24 [20/0] via 123.2.3.1, 00:00:00
B 123.2.1.0/24 [20/0] via 123.2.3.1, 00:00:00
B 123.2.4.0/24 [20/0] via 123.3.1.2, 00:00:00



4.3 Konfiguracja protokołu OSPF na przełączniku TP-LINK T3700G-28TQ_V2

1. Zaloguj się na przełącznik 28TQ
2. W oknie **Routing**→**Interface**→**Interface Config**, utwórz **VLAN1120** na adres IPv4 static **1.1.2.10/24** oraz **VLAN 1110** na adres IPv4 static **1.1.1.7/24**.
3. W oknie **VLAN** -> **VLAN Config** zaznacz port **1/0/10** w **VLAN1120** oraz port **1/0/7** w **VLAN1110**

UWAGA! Nie dokonywać zmian w VLAN -> Port Config

4. Na karcie **Routing**→**OSPF**→**Process**, stwórz **OSPF process 1** i skonfiguruj **Router ID** as **1.1.1.1**.
5. Na karcie **Routing**→**OSPF**→**Network**, skonfiguruj sieć **1.1.2.0/24** w obszarze **area 0** oraz sieć **1.1.1.0/24** w obszarze **area 0**.

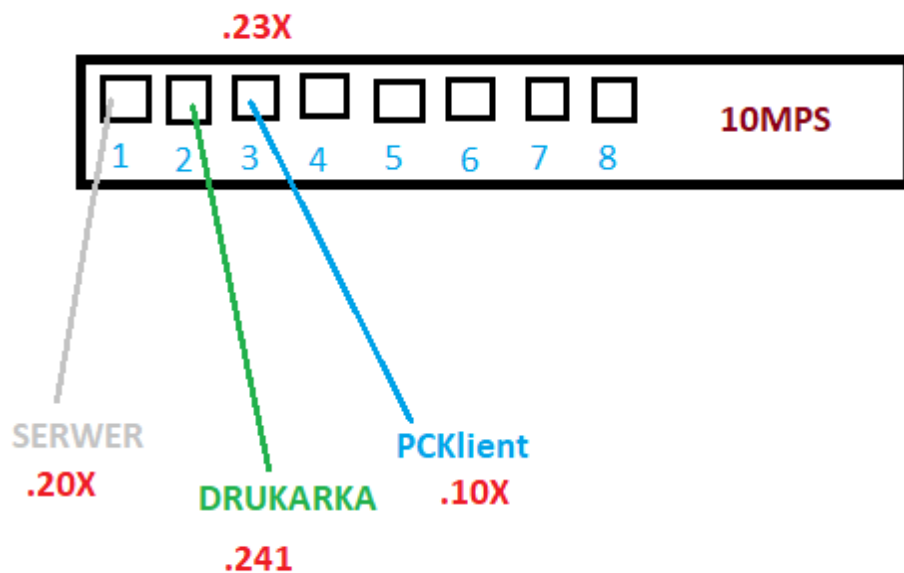
5. Access Control List – Cisco Packet

5.1 Access Control List – Cisco Packet

5.2 Access Control List – TP-LINK switch

5.2.1 MAC ACL

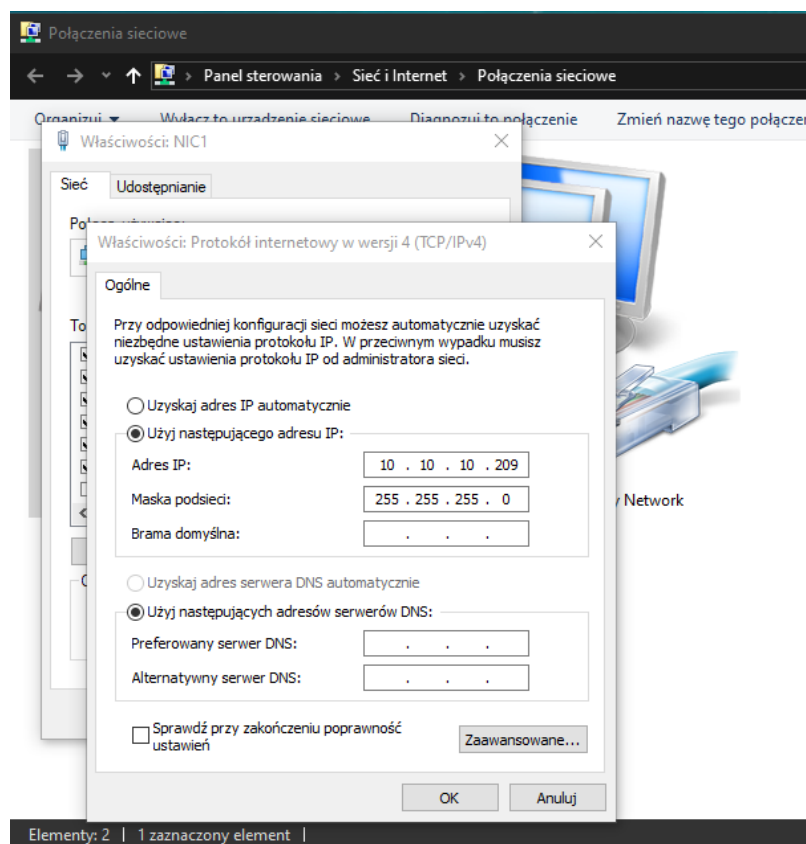
Podłącz urządzenia końcowe do przełącznika **T2500G-10MPS**.



Zaloguje się na przełącznik i ustaw jego adres docelowy **10.10.10.23x/24** z bramą domyślną **0.0.0.0**.

Pamiętaj, że nie jesteś podłączony do routera i karta sieciowa SERWERA czy PCKlienta nie otrzyma adres IPv4 z puli 192.168.0.0/24.

Ustaw docelowy adres IPv4 karty sieciowej SERWERA **10.10.10.20x/24**, i **PKlienta 10.10.10.10x/24**.



Ustaw czas systemowy przełącznika

T2500G-10MPS	System Summary	Device Description	System Time	Daylight Saving Time	Serial Port Setting	System IP
System • System Info • User Management • System Tools • Access Security Switching - VLAN - Spanning Tree - Multicast - DHCP - QoS - PoE - ACL - Network Security - SNMP - LLDP						
Time Info Current System Time: 2006-01-01 08:17:05 Sunday Current Time Source: Manual						
Time Config ☐ Manual Date: 2006 01 01 Time: 08 17 05 ☐ Get Time from NTP Server Time Zone: (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Singapore Primary Sever: 133.100.9.2 Secondary Sever: 139.78.100.163 Update Rate: 12 hour(s) ☒ Synchronize with PC's Clock Apply Refresh Help						

T2500G-10MPS

System Summary

Device Description

System Time

Daylight Saving Time

Serial Port Setting

System IP

Getting time from management PC successfully.

Time Info

Current System Time: 2025-03-10 13:55:24 Monday

Current Time Source: PC's Clock

Time Config

☐ Manual

Date:

2025

03

10

Time:

13

55

24

☐ Get Time from NTP Server

Time Zone:

(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi, Singapore

Primary Sever:

133.100.9.2

Secondary Sever:

139.78.100.163

Update Rate:

12

hour(s)

☒ Synchronize with PC's Clock

Apply

Refresh

Help

T2500G-10MPS

Time-Range Summary

Time-Range Create

Holiday Config

Create Time-Range

Name:

DRUKARKA_RICOH

☐ Holiday

☐ Absolute

Start Date:

2000

01

01

End Date:

2000

01

01

☒ Week

☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat ☒ Sun

Create Time-Slice

Start Time:

09

:

00

End Time:

10

:

00

Create

Time-Slice Table

Index	Start Time	End Time	Delete
-------	------------	----------	--------

Apply

Help

Operation succeeded.

Create Time-Range

Name:

☐ Holiday

☐ Absolute Start Date: / / End Date: / /

☒ Week ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat ☒ Sun

Create Time-Slice

Start Time: :

End Time: :

Time-Slice Table

Index	Start Time	End Time	Delete
1	09:00	10:00	Delete

Time-Range Table

Select	Index	Time-Range Name	Slice 1	Slice 2	Slice 3	Slice 4	Mode	Operation
☐	1	DRUKARKA_RICOH	09:00-10:00	---	---	---	Week	Edit Detail

Sprawdź połączenie z drukarką

```
C:\Users\user>ping 10.10.10.241

Pinging 10.10.10.241 with 32 bytes of data:
Reply from 10.10.10.241: bytes=32 time<1ms TTL=255
Reply from 10.10.10.241: bytes=32 time<1ms TTL=255
Reply from 10.10.10.241: bytes=32 time<1ms TTL=255
Reply from 10.10.10.241: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.10.241:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\user>arp -a

Interface: 192.168.56.1 --- 0x6
    Internet Address      Physical Address          Type
    192.168.56.255        ff-ff-ff-ff-ff-ff        static
    224.0.0.22            01-00-5e-00-00-16        static
    224.0.0.251          01-00-5e-00-00-fb        static
    224.0.0.252          01-00-5e-00-00-fc        static
    239.255.255.250      01-00-5e-7f-ff-fa        static

Interface: 10.10.10.209 --- 0xf
    Internet Address      Physical Address          Type
    10.10.10.241          00-26-73-db-ed-f7        dynamic
    10.10.10.255          ff-ff-ff-ff-ff-ff        static
    224.0.0.22            01-00-5e-00-00-16        static
    224.0.0.251          01-00-5e-00-00-fb        static
    239.255.255.250      01-00-5e-7f-ff-fa        static
```

Za pomocą polecenia **ipconfig /all** wyświetl informacje o karcie sieciowej SERWERA. Zapisz adres MAC karty w notatniku.

Ethernet adapter NIC1:

```
Connection-specific DNS Suffix . :  
Description . . . . . : Realtek PCIe GBE Family Controller  
Physical Address. . . . . : F0-79-59-68-3E-AF  
DHCP Enabled. . . . . : No  
Autoconfiguration Enabled . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::a4df:ecc5:d4e6:ffd8%15(Preferred)  
IPv4 Address. . . . . : 10.10.10.209(Preferred)  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . :  
DHCPv6 IAID . . . . . : 44867095  
DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-7D-5C-08-F0-79-59-68-3E-AF  
DNS Servers . . . . . : fec0:0:0:ffff::1%1  
                        fec0:0:0:ffff::2%1  
                        fec0:0:0:ffff::3%1  
NetBIOS over Tcpi. . . . . : Enabled
```

Wejdź w zakładkę **ACL/ACL Create**.

T2500G-10MPS

System
Switching
VLAN
Spanning Tree
Multicast
DHCP
QoS
PoF

ACL Summary | **ACL Create** | MAC ACL | Standard-IP ACL | Extend-IP ACL

ACL Create

ACL ID: 0-499 MAC ACL
500-1499 Standard-IP ACL
1500-2499 Extend-IP ACL

Rule Order: User Config

Następnie w zakładce **ACL/ACL Config/MAC ACL** utwórz regułę jak widać poniżej na obrazku.

CEL: Zablokuj **SERWEROVI** dostęp do **DRUKARKI_RICOH**

S-MAC adres SERWERA tutaj F0-79-59-68-3E-AF

D-MAC adres DRUKARKI tutaj 00-26-73-db-ed-f7

T2500G-10MPS

ACL Summary

ACL Create

MAC ACL

Standard-IP ACL

Extend-IP ACL

System

Switching

VLAN

Spanning Tree

Multicast

DHCP

QoS

PoE

ACL

• Time-Range

• **ACL Config**

• Policy Config

• ACL Binding

• Policy Binding

Network Security

SNMP

MAC-Rule

ACL ID:

ACL 100

Rule ID:

10

Index:

1

Operation:

Deny

☒ S-MAC:

F0-79-59-68-3E-AF

Mask:

FF-FF-FF-FF-FF-FF

(Format: 00-00-00-00-00-01)

☒ D-MAC:

00-26-73-DB-ED-F7

Mask:

FF-FF-FF-FF-FF-FF

☐ VLAN ID:

☐ EtherType:

(4-hex number)

User Priority:

No Limit

Time-Range:

No Limit

Apply

Back

Help

Przypisz ustawioną wyżej regułę do portu przełącznika obsługującego DRUKARKĘ.

Binding Table

Port Binding

VLAN Binding

Port-Bind Config

ACL ID:

Select ACL

Apply

Help

Port:

Select ACL

UNIT:

1

1

2

3

4

5

6

7

100

Unselected Port(s)

Selected Port(s)

Not Available for Selection

Port-Bind Table

UNIT:

1

Index	ACL ID	Port	Direction
No entry in the table.			

T2500G-10MPS

- System
- Switching
- VLAN
- Spanning Tree
- Multicast
- DHCP
- QoS
- PoE
- ACL
 - Time-Range
 - ACL Config
 - Policy Config
 - **ACL Binding**
 - Policy Binding

Binding Table

Port Binding

VLAN Binding

Port-Bind Config

ACL ID:

100

Apply

Port:

Help

UNIT: 1

1 2 3 4 5 6 7 8 9 10



Unselected Port(s)



Selected Port(s)



Not Available for Selection

Port-Bind Table

UNIT: 1

Index	ACL ID	Port	Direction
No entry in the table.			

T2500G-10MPS

- System
- Switching
- VLAN
- Spanning Tree
- Multicast
- DHCP
- QoS
- PoE
- ACL
 - Time-Range
 - ACL Config
 - Policy Config
 - **ACL Binding**
 - Policy Binding

Binding Table

Port Binding

VLAN Binding

Operation succeeded.

Port-Bind Config

ACL ID:

Select ACL

Apply

Port:

Help

UNIT: 1

1 2 3 4 5 6 7 8 9 10



Unselected Port(s)



Selected Port(s)



Not Available for Selection

Port-Bind Table

UNIT: 1

Index	ACL ID	Port	Direction
1	100	1/0/1	Ingress

Sprawdź połączenie SERWERA z DRUKARKĄ

```
C:\Users\user>ping 10.10.10.241
```

```
Pinging 10.10.10.241 with 32 bytes of data:
```

```
Reply from 10.10.10.209: Destination host unreachable.
```

```
Reply from 10.10.10.209: Destination host unreachable.
```

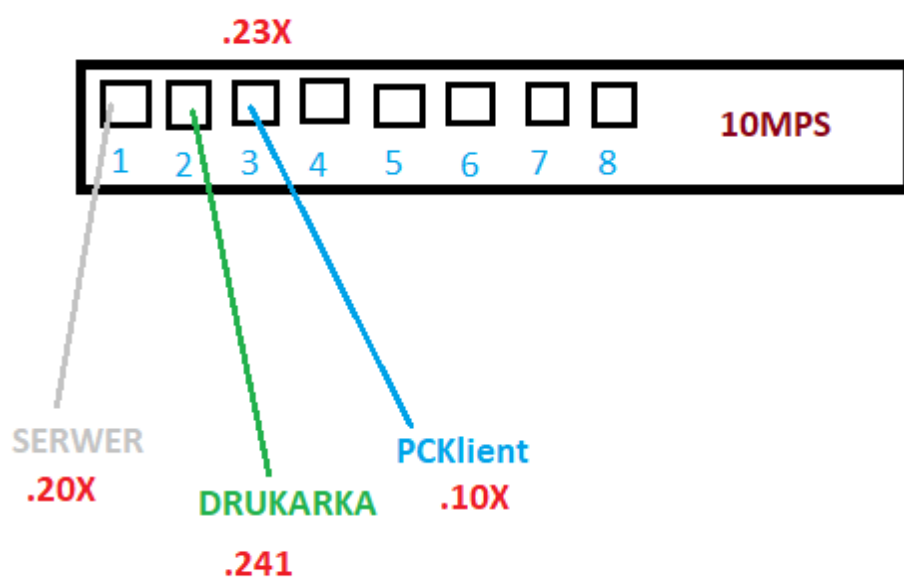
```
Reply from 10.10.10.209: Destination host unreachable.
```

```
Reply from 10.10.10.209: Destination host unreachable.
```

```
Ping statistics for 10.10.10.241:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

5.2.3 Standardowe ACL – IP



Sprawdź połączenie z **DRUKARKĄ** i **Pcklientem**.

```

C:\Users\user>ping 10.10.10.109

Pinging 10.10.10.109 with 32 bytes of data:
Reply from 10.10.10.109: bytes=32 time=1ms TTL=128
Reply from 10.10.10.109: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.109:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
^C
C:\Users\user>ping 10.10.10.241

Pinging 10.10.10.241 with 32 bytes of data:
Reply from 10.10.10.241: bytes=32 time<1ms TTL=255
Reply from 10.10.10.241: bytes=32 time<1ms TTL=255
Reply from 10.10.10.241: bytes=32 time<1ms TTL=255
Reply from 10.10.10.241: bytes=32 time<1ms TTL=255

```

Ustaw **ACL/Time-Range/Time-Range Create** na 7 dni w tygodniu od 14.00 – 15.00

T2500G-10MPS

System

Switching

VLAN

Spanning Tree

Multicast

DHCP

QoS

PoE

ACL

• Time-Range

• ACL Config

• Policy Config

• ACL Binding

Time-Range Summary

Time-Range Create

Holiday Config

Create Time-Range

Name:

blokowanie_druk

☐ Holiday

☐ Absolute

☒ Week

Start Date:

2000

 /

01

 /

01

End Date:

2000

 /

01

 /

01

☒ Mon

☐ Tue

☐ Wed

☐ Thu

☐ Fri

☐ Sat

☐ Sun

Create Time-Slice

Start Time:

14

 :

00

End Time:

15

 :

00

Create

Time-Slice Table

Index	Start Time	End Time	Delete

Apply

Help

T2500G-10MPS

ACL Summary

ACL Create

MAC ACL

Standard-IP ACL

Extend-IP ACL

System

Switching

VLAN

Spanning Tree

Multicast

DHCP

QoS

PoE

ACL

• Time-Range

• ACL Config

ACL Create

ACL ID: 500

0-499 MAC ACL

500-1499 Standard-IP ACL

1500-2499 Extend-IP ACL

Rule Order: User Config

Apply

Help

T2500G-10MPS

ACL Summary

ACL Create

MAC ACL

Standard-IP ACL

Extend-IP ACL

System

Switching

VLAN

Spanning Tree

Multicast

DHCP

QoS

PoE

ACL

• Time-Range

• ACL Config

• Policy Config

Standard-IP Rule

ACL ID: ACL 500

Rule ID: 10

Index: 1

Operation: Deny

☒ S-IP: 10.10.10.109 Mask: 255.255.255.255 (Format: 192.168.0.1)

☒ D-IP: 10.10.10.241 Mask: 255.255.255.255

Time-Range: blokowanie_druk

Apply

Back

Help

System

Switching

VLAN

Spanning Tree

Multicast

DHCP

QoS

PoE

ACL

• Time-Range

• ACL Config

• Policy Config

• ACL Binding

• Policy Binding

Network Security

Port-Bind Config

ACL ID: 500

Port: Select ACL

500

Apply

Help

UNIT: 1

1 2 3 4 5 6 7 8 9 10

Unselected Port(s)

Selected Port(s)

Not Available for Selection

Port-Bind Table

UNIT: 1

Index	ACL ID	Port	Direction
No entry in the table.			

T2500G-10MPS

- System
- Switching
- VLAN
- Spanning Tree
- Multicast
- DHCP
- QoS
- PoE
- ACL
 - Time-Range
 - ACL Config
 - Policy Config
 - **ACL Binding**
 - Policy Binding

Binding Table

Port Binding

VLAN Binding

Port-Bind Config

ACL ID:

Apply

Port:

Help

UNIT:

☐ 1
 ☐ 2
 ☒ 3
 ☐ 4
 ☐ 5
 ☐ 6
 ☐ 7
 ☐ 8
 ☐ 9
 ☐ 10



Unselected Port(s)



Selected Port(s)



Not Available for Selection

Port-Bind Table

UNIT:

Index	ACL ID	Port	Direction
No entry in the table.			

T2500G-10MPS

- System
- Switching
- VLAN
- Spanning Tree
- Multicast
- DHCP
- QoS
- PoE
- ACL
 - Time-Range
 - ACL Config
 - Policy Config
 - **ACL Binding**
 - Policy Binding

Binding Table

Port Binding

VLAN Binding

Operation succeeded.

Port-Bind Config

ACL ID:

Apply

Port:

Help

UNIT:

☐ 1
 ☐ 2
 ☒ 3
 ☐ 4
 ☐ 5
 ☐ 6
 ☐ 7
 ☐ 8
 ☐ 9
 ☐ 10



Unselected Port(s)



Selected Port(s)



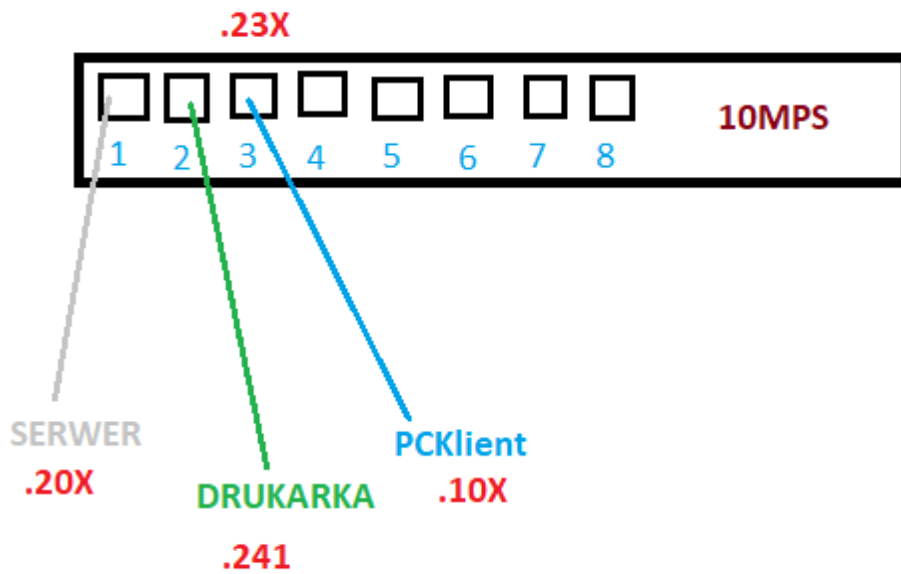
Not Available for Selection

Port-Bind Table

UNIT:

Index	ACL ID	Port	Direction
1	500	1/0/3	Ingress

5.2.2 External ACL



Sprawdź połączenie SERWERA z DRUKARKĄ i PCKlientem.

```
Wiersz polecenia
C:\Users\user>ping 10.10.10.109

Pinging 10.10.10.109 with 32 bytes of data:
Reply from 10.10.10.109: bytes=32 time=1ms TTL=128
Reply from 10.10.10.109: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.109:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
^C
C:\Users\user>ping 10.10.10.241

Pinging 10.10.10.241 with 32 bytes of data:
Reply from 10.10.10.241: bytes=32 time<1ms TTL=255
Reply from 10.10.10.241: bytes=32 time<1ms TTL=255
Reply from 10.10.10.241: bytes=32 time<1ms TTL=255
Reply from 10.10.10.241: bytes=32 time<1ms TTL=255
```

T2500G-10MPS

- System
- Switching
- VLAN
- Spanning Tree
- Multicast
- DHCP
- QoS
- PoE
- ACL
- Time-Range**
- ACL Config
- Policy Config
- ACL Binding

Time-Range Summary

Time-Range Create

Holiday Config

Create Time-Range

Name:

☐ Holiday
☐ Absolute

Start Date: / /
End Date: / /

☒ Week

☒ Mon
☐ Tue
☐ Wed
☐ Thu
☐ Fri
☐ Sat
☐ Sun

Create Time-Slice

Start Time: :
End Time: :

Create

Time-Slice Table

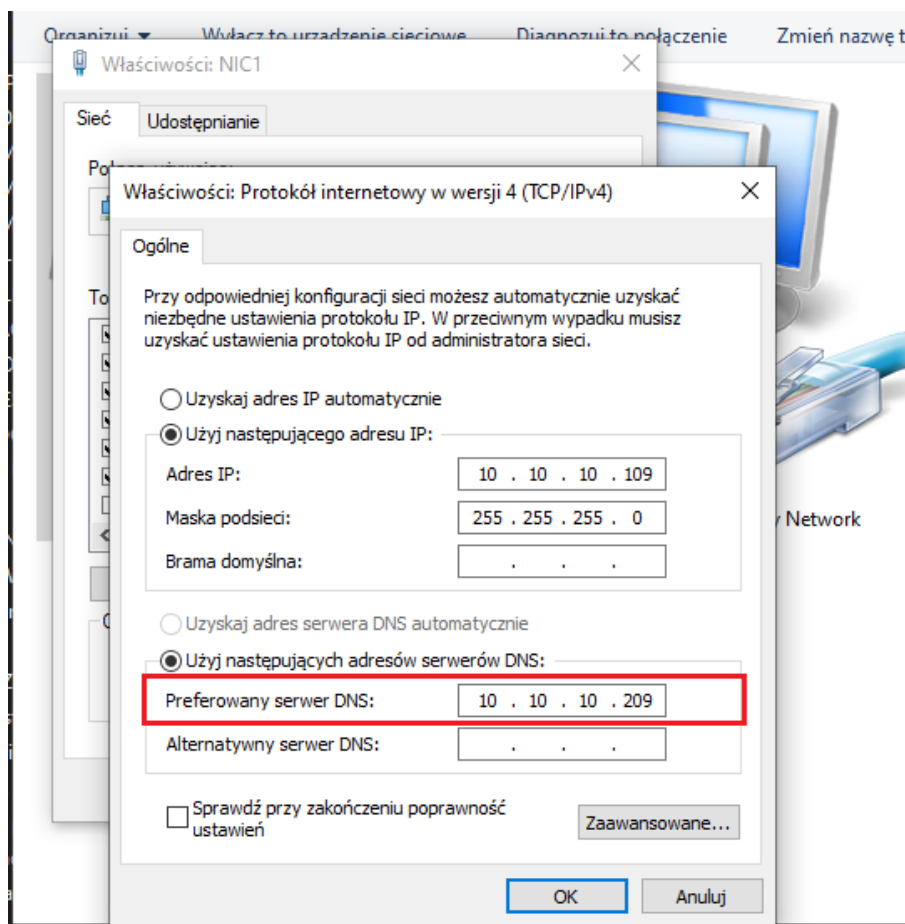
Index	Start Time	End Time	Delete

Apply

Help

CEL1: Zablokuj dostęp PCKlientowi do usługi serwera DNS

- Zainstaluj usługę IIS i DNS na **SERWERZE WINDOWS 2022**
- Zaadresuj pierwszy interfejs **SERWERA: IPv4 10.10.10.20X/24**
- Utwórz rekord A www.local na adres **10.10.10.20X** w strefie domenowej local.
- Na **PCKliencie** w panelu konfiguracyjnym interfejsu sieciowego ustaw DNS **10.10.10.20X**.



- Na **PCKliencie** w programie **nslookup** sprawdź połączenie z serwerem DNS.

```
C:\Users\user>nslookup
Default Server:  www.local
Address:  10.10.10.209

> set type=a
> www.local
Server:  www.local
Address:  10.10.10.209

Name:    www.local
Address:  10.10.10.209
```

- Wireshark Pobranie rekordu DNS

17	6.311480	10.10.10.109	10.10.10.209	DNS	69 Standard query 0x2b5f A www.local
18	6.311932	10.10.10.209	10.10.10.109	DNS	85 Standard query response 0x2b5f A www.local A 10.10.10.209
23	6.314197	10.10.10.109	10.10.10.209	HTTP	402 GET / HTTP/1.1
24	6.314515	10.10.10.209	10.10.10.109	DNS	85 Standard query response 0xcc83 A www.local A 10.10.10.209
25	6.314768	10.10.10.109	10.10.10.209	DNS	69 Standard query 0x0a0d AAAA www.local
26	6.315163	10.10.10.209	10.10.10.109	DNS	121 Standard query response 0x0a0d AAAA www.local SOA server
27	6.324482	10.10.10.209	10.10.10.109	TCP	60 80 → 63208 [ACK] Seq=1 Ack=349 Win=2097664 Len=0
28	6.427061	10.10.10.209	10.10.10.109	HTTP	982 HTTP/1.1 200 OK (text/html)
29	6.447824	10.10.10.109	10.10.10.209	DNS	90 Standard query 0x23e0 A incoming.telemetry.mozilla.org
30	6.449373	10.10.10.109	10.10.10.209	HTTP	418 GET /iisstart.png HTTP/1.1
31	6.457507	10.10.10.209	10.10.10.109	TCP	1... 80 → 63208 [ACK] Seq=929 Ack=713 Win=2097152 Len=1460 [TCF
32	6.457509	10.10.10.209	10.10.10.109	TCP	1... 80 → 63208 [ACK] Seq=2389 Ack=713 Win=2097152 Len=1460 [TC
33	6.457594	10.10.10.109	10.10.10.209	TCP	54 63208 → 80 [ACK] Seq=713 Ack=3849 Win=2102272 Len=0
34	6.457833	10.10.10.209	10.10.10.109	TCP	1... 80 → 63208 [ACK] Seq=3849 Ack=713 Win=2097152 Len=1460 [TC
35	6.457834	10.10.10.209	10.10.10.109	TCP	1... 80 → 63208 [ACK] Seq=5309 Ack=713 Win=2097152 Len=1460 [TC
36	6.457835	10.10.10.209	10.10.10.109	TCP	1... 80 → 63208 [ACK] Seq=6769 Ack=713 Win=2097152 Len=1460 [TC

T2500G-10MPS

- System
- Switching
- VLAN
- Spanning Tree
- Multicast
- DHCP
- QoS
- PoE

ACL Summary

ACL Create

MAC ACL

Standard-IP ACL

Extend-IP ACL

ACL Create

ACL ID: 0-499 MAC ACL
500-1499 Standard-IP ACL
1500-2499 Extend-IP ACL

Rule Order: User Config

Apply

Help

T2500G-10MPS

- System
- Switching
- VLAN
- Spanning Tree
- Multicast
- DHCP
- QoS
- PoE
- ACL
 - Time-Range
 - ACL Config
 - Policy Config
 - ACL Binding
 - Policy Binding
- Network Security
- SNMP
- LLDP
- Maintenance

ACL Summary

ACL Create

MAC ACL

Standard-IP ACL

Extend-IP ACL

Create Extend-IP Rule

ACL ID: (0-1999)
Rule ID: (0-1999)
Operation:

☐ S-IP: Mask: (Format: 192.168.0.1)
☐ D-IP: Mask:

IP Protocol:

TCP Flag: URG ACK PSH RST SYN FIN

☐ S-Port:
☐ D-Port:

DSCP:

IP ToS: IP Pre:

Time-Range:

Apply

Help

ACL ID: ACL 1500

Rule ID: 10

Index: 1

Operation: Deny

☒ S-IP: 10.10.10.109 Mask: 255.255.255.255 (Format: 192.168.0.1)

☒ D-IP: 10.10.10.209 Mask: 255.255.255.255

IP Protocol: 17 UDP

TCP Flag: URG * ACK * PSH * RST * SYN * FIN *

☐ S-Port:☒ D-Port: 53

DSCP: No Limit

IP ToS: No Limit

IP Pre: No Limit

Time-Range: Drukarka_ricoh

Apply

Back

Help

T2500G-10MPS

System

Switching

VLAN

Spanning Tree

Multicast

DHCP

QoS

PoE

ACL

• Time-Range

Search Options

Select an ACL: ACL 1500

ACL Type: Extend-IP ACL

Rule Order: User Config

Rule Table

Select	Index	Rule ID	S-IP Address	D-IP Address	L3 Information	Time-Range Name	Operation
☐	1	10	10.10.10.109	10.10.10.209	UDP	blokowanie_druk	Edit Detail Up Down

All

Delete

Help

T2500G-10MPS

- System
- Switching
- VLAN
- Spanning Tree
- Multicast
- DHCP
- QoS
- PoE
- ACL
 - Time-Range
 - ACL Config
 - Policy Config
 - **ACL Binding**
 - Policy Binding

Binding Table

Port Binding

VLAN Binding

Port-Bind Config

ACL ID:

Apply

Port:

Help

UNIT:

☐ 1
 ☐ 2
 ☒ 3
 ☐ 4
 ☐ 5
 ☐ 6
 ☐ 7
 ☐ 8
 ☐ 9
 ☐ 10



Unselected Port(s)



Selected Port(s)



Not Available for Selection

Port-Bind Table

UNIT:

Index	ACL ID	Port	Direction
No entry in the table.			

Binding Table

Port Binding

VLAN Binding

Operation succeeded.

Port-Bind Config

ACL ID:

Apply

Port:

Help

UNIT:

☐ 1
 ☐ 2
 ☐ 3
 ☐ 4
 ☐ 5
 ☐ 6
 ☐ 7
 ☐ 8
 ☐ 9
 ☐ 10



Unselected Port(s)



Selected Port(s)



Not Available for Selection

Port-Bind Table

UNIT:

Index	ACL ID	Port	Direction
1	1501	1/0/3	Ingress

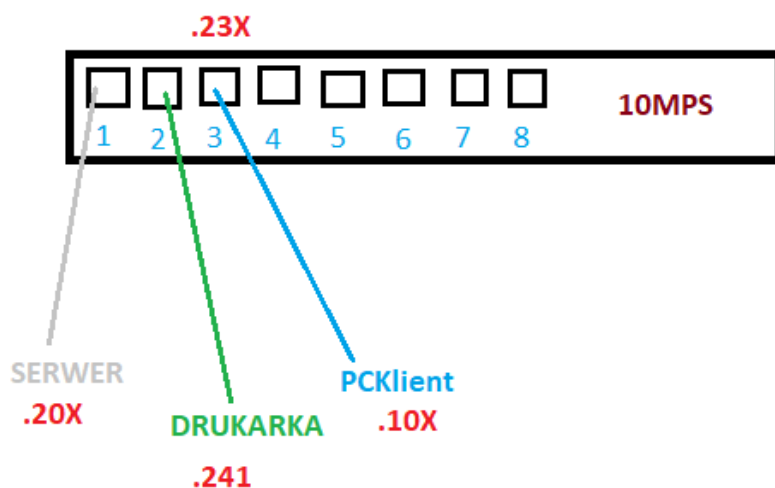
Na **PCKliencie** sprawdź teraz dostępność rekordów dns **SERWERA**.

```
C:\Users\user>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server:  UnKnown
Address:  10.10.10.209

> set type=a
> www.local
Server:  UnKnown
Address:  10.10.10.209

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
```

CEL2: Blokowanie **PCKlientowi 10.10.10.10X/24** dostępu zdalnego do **SERWERZE 10.10.10.20X/24**.



- Uruchom dostęp zdalny na **SERWERZE**.
- Sprawdź dostęp połączenia zdalnego w programie Wireshar uruchomionego na **PCKliencie**.

35	2.474231	10.10.10.109	10.10.10.209	TCP	66 59327 → 3389 [SYN]	Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
36	2.474471	10.10.10.209	10.10.10.109	TCP	66 3389 → 59327 [SYN, ACK]	Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SAC
37	2.474514	10.10.10.109	10.10.10.209	TCP	54 59327 → 3389 [ACK]	Seq=1 Ack=1 Win=2102272 Len=0
38	2.474838	10.10.10.109	10.10.10.209	TLS...	101 Ignored Unknown Record	
39	2.485257	10.10.10.209	10.10.10.109	TCP	60 3389 → 59327 [ACK]	Seq=1 Ack=48 Win=63953 Len=0
40	2.491318	10.10.10.209	10.10.10.109	TLS...	73 Ignored Unknown Record	
41	2.492220	10.10.10.109	10.10.10.209	TLS...	237 Client Hello	
42	2.492886	10.10.10.209	10.10.10.109	TLS...	882 Server Hello, Certificate, Server Hello Done	
43	2.493127	10.10.10.109	10.10.10.209	TLS...	372 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
44	2.497581	10.10.10.209	10.10.10.109	TLS...	105 Change Cipher Spec, Encrypted Handshake Message	
45	2.498040	10.10.10.109	10.10.10.209	TLS...	140 Application Data	
46	2.498322	10.10.10.209	10.10.10.109	TLS...	254 Application Data	
47	2.498823	10.10.10.109	10.10.10.209	TLS...	634 Application Data	
48	2.499429	10.10.10.209	10.10.10.109	TLS...	142 Application Data	
49	2.499642	10.10.10.109	10.10.10.209	TLS...	191 Application Data	
50	2.499943	10.10.10.209	10.10.10.109	TLS...	87 Application Data	
51	2.500055	10.10.10.109	10.10.10.209	TLS...	545 Application Data	
52	2.500722	10.10.10.209	10.10.10.109	TLS...	209 Application Data	

- Ustaw czas blokady zdalnego pulpitu w zakładce ACL/Time-Range/Time-Range Create

T2500G-10MPS

Time-Range Summary

Time-Range Create

Holiday Config

System

Switching

VLAN

Spanning Tree

Multicast

DHCP

QoS

PoE

ACL

• Time-Range

• ACL Config

• Policy Config

• ACL Binding

• Policy Binding

Create Time-Range

Name: zdalny_dostep

☐ Holiday
☐ Absolute
☒ Week

Start Date: 2000 / 01 / 01

End Date: 2000 / 01 / 01

☐ Mon
☐ Tue
☐ Wed
☐ Thu
☒ Fri
☐ Sat
☐ Sun

Create Time-Slice

Start Time: 09 : 00

End Time: 10 : 00

Create

Time-Slice Table

Index	Start Time	End Time	Delete

Apply

Help

Time-Range Summary

Time-Range Create

Holiday Config

Time-Range Table						
Select	Index	Time-Range Name	Slice 1	Slice 2	Slice 3	Slice 4
☐	1	Drukarka_ricoh	09:00-10:00	---	---	---
☐	2	zdalny_dostep	09:00-10:00	---	---	---

All

Delete

Help

- Zablokuj dostęp zdalny **PCKlientowi** na **SERWER**.

ACL Summary

ACL Create

MAC ACL

Standard-IP ACL

Extend-IP ACL

Create Extend-IP Rule

ACL ID:

ACL 1501

▼

Rule ID:

20

(0-1999)

Operation:

Deny

▼

☒ S-IP:

10.10.10.109

Mask: 255.255.255.255

☒ D-IP:

10.10.10.209

Mask: 255.255.255.255

IP Protocol:

6 TCP

▼

TCP Flag:

URG * ▼

ACK * ▼

PSH * ▼

RST * ▼

SYN 1 ▼

FIN * ▼

☐ S-Port:

☒ D-Port:

3389

DSCP:

No Limit

▼

IP ToS:

No Limit

▼

IP Pre: No Limit

▼

Time-Range:

zdalny_dostep

▼

Apply

Help

ACL Summary

ACL Create

MAC ACL

Standard-IP ACL

Extend-IP ACL

Search Options

Select an ACL:

ACL 1501

▼

ACL Type:

Extend-IP ACL

Rule Order:

User Config

Rule Table

Select	Index	Rule ID	S-IP Address	D-IP Address	L3 Information	Time-Range Name
☐	1	20	10.10.10.109	10.10.10.209	TCP	Drukarka_ricoh

All

Delete

Help

T2500G-10MPS

Binding Table

Port Binding

VLAN Binding

System

Switching

VLAN

Spanning Tree

Multicast

DHCP

QoS

PoE

ACL

• Time-Range

• ACL Config

• Policy Config

• **ACL Binding**

• Policy Binding

Port-Bind Config

ACL ID:

1501

Apply

Port:

Help

UNIT:

1

1

2

3

4

5

6

7

8

9

10

Unselected Port(s)

Selected Port(s)

Not Available for Selection

Port-Bind Table

UNIT:

1

Index	ACL ID	Port	Direction
No entry in the table.			

Binding Table

Port Binding

VLAN Binding

Operation succeeded.

Port-Bind Config

ACL ID:

Select ACL

Apply

Port:

Help

UNIT:

1

1

2

3

4

5

6

7

8

9

10

Unselected Port(s)

Selected Port(s)

Not Available for Selection

Port-Bind Table

UNIT:

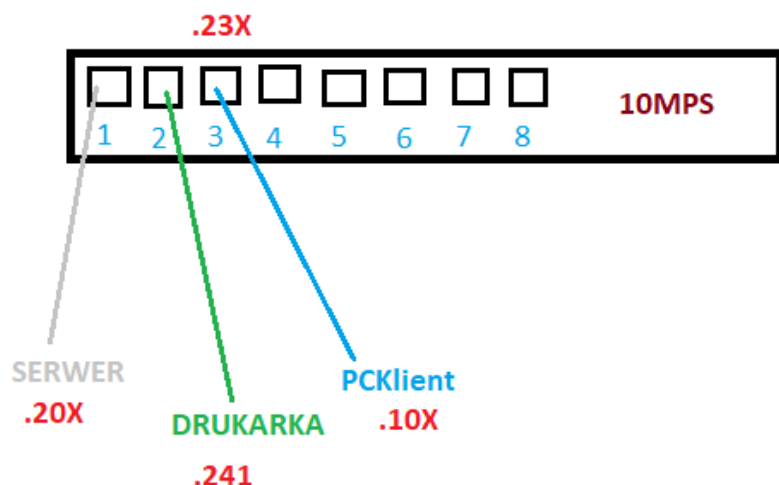
1

Index	ACL ID	Port	Direction
1	1501	1/0/3	Ingress

- Za pomocą programu Wireshar udowodnij, że blokada procesu synchronizacyjnego zdalnego połączenia SYN/SYN ACK/ ACK się powiodła.

15	2.012312	10.10.10.109	10.10.10.209	TCP	66 59839 → 3389 [SYN] Seq=0 Win=64240 Len=0
16	2.019957	Cisco_35:f0:b2	Broadcast	ARP	60 Who has 192.168.7.116? Tell 192.168.7.1
17	2.119967	Cisco_35:f0:b2	Broadcast	ARP	60 Who has 192.168.7.115? Tell 192.168.7.1
18	2.199993	Cisco_35:f0:b2	Broadcast	ARP	60 Who has 192.168.7.121? Tell 192.168.7.1
19	2.365456	Cisco_35:f0:b2	Broadcast	ARP	60 Who has 192.168.7.133? Tell 192.168.7.1
20	2.670049	Cisco_35:f0:b2	Broadcast	ARP	60 Who has 192.168.7.122? Tell 192.168.7.1
21	2.708868	Cisco_35:f0:b2	Broadcast	ARP	60 Who has 192.168.7.119? Tell 192.168.7.1
22	2.937524	Cisco_35:f0:b2	Broadcast	ARP	60 Who has 192.168.7.117? Tell 192.168.7.1
23	3.014062	10.10.10.109	10.10.10.209	TCP	66 [TCP Retransmission] 59839 → 3389 [SYN] S
24	3.029820	Cisco_35:f0:b2	Broadcast	ARP	60 Who has 192.168.7.116? Tell 192.168.7.1
25	3.049032	Cisco_35:f0:b2	Broadcast	ARP	60 Who has 192.168.7.114? Tell 192.168.7.1

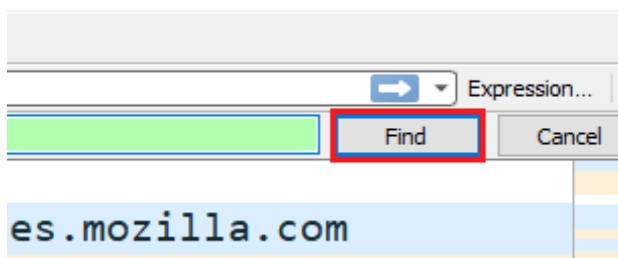
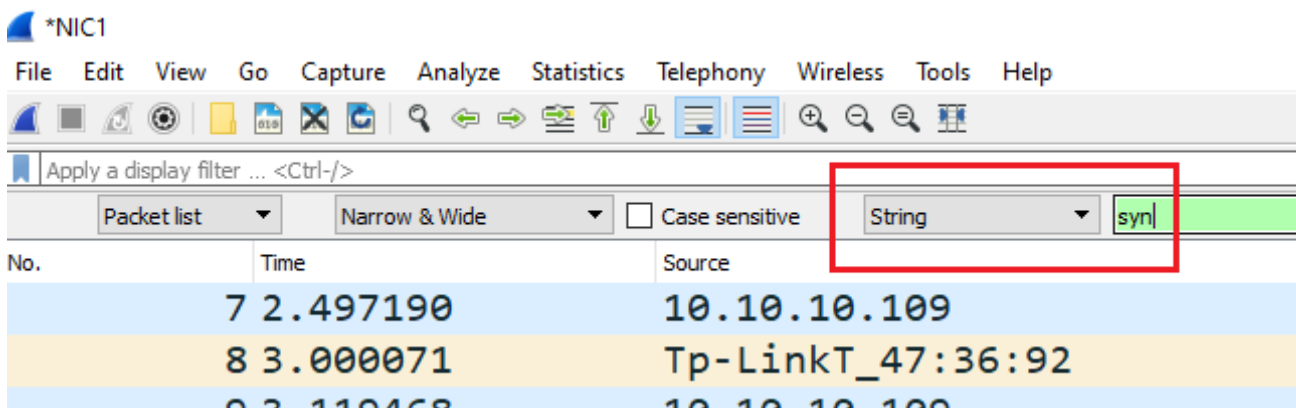
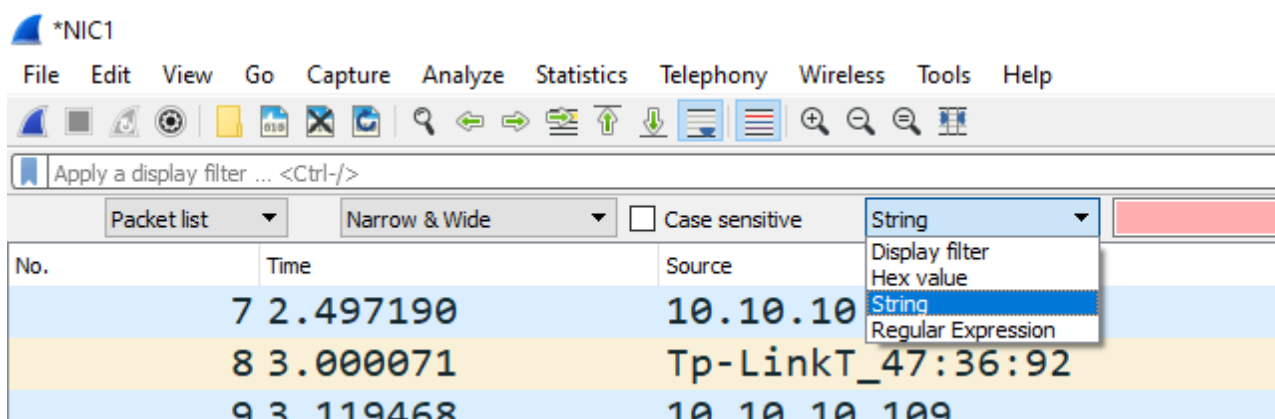
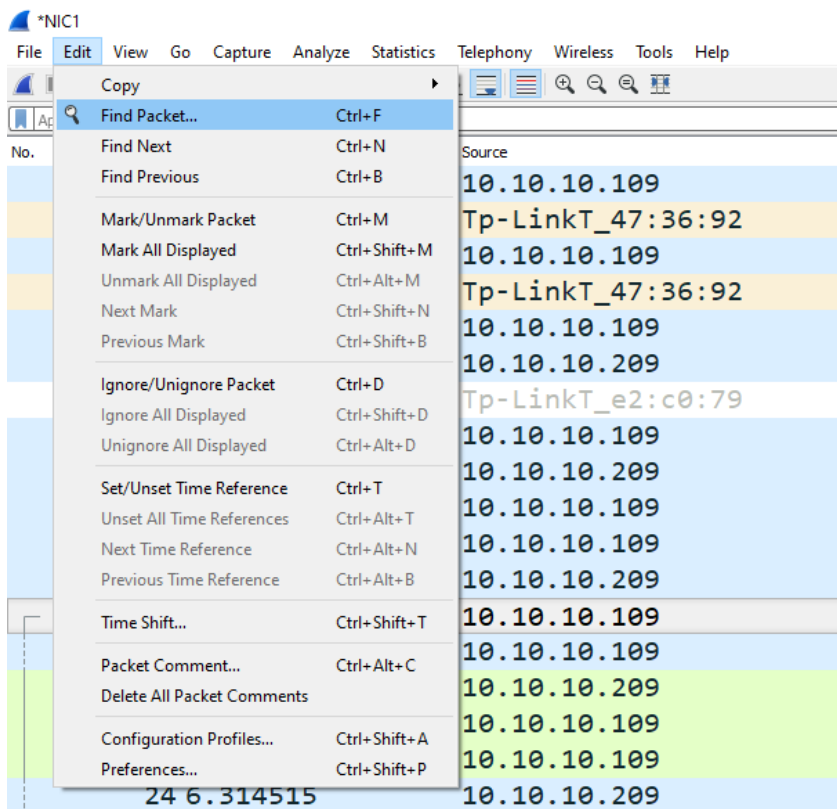
CEL3: Blokowanie **PCKlientowi 10.10.10.10X/24** dostępu do WWW na **SERWERZE 10.10.10.20X/24**.



- Na **PCKliencie** , za pomocą programu Wireshark przechwycić proces pobierania strony www.local z **SERWERA**.

23	6.314197	10.10.10.109	10.10.10.209	HTTP	402	GET / HTTP/1.1
24	6.314515	10.10.10.209	10.10.10.109	DNS	85	Standard query response 0xcc83 A www.local A 10.10.10.209
25	6.314768	10.10.10.109	10.10.10.209	DNS	69	Standard query 0xa0d AAAA www.local
26	6.315163	10.10.10.209	10.10.10.109	DNS	121	Standard query response 0xa0d AAAA www.local SOA serwer
27	6.324482	10.10.10.209	10.10.10.109	TCP	60	80 → 63208 [ACK] Seq=1 Ack=349 Win=2097664 Len=0
28	6.427061	10.10.10.209	10.10.10.109	HTTP	982	HTTP/1.1 200 OK (text/html)
29	6.447824	10.10.10.109	10.10.10.209	DNS	90	Standard query 0x23e0 A incoming.telemetry.mozilla.org
30	6.449373	10.10.10.109	10.10.10.209	HTTP	418	GET /iisstart.png HTTP/1.1
31	6.457507	10.10.10.209	10.10.10.109	TCP	1...	80 → 63208 [ACK] Seq=929 Ack=713 Win=2097152 Len=1460 [TCP
32	6.457509	10.10.10.209	10.10.10.109	TCP	1...	80 → 63208 [ACK] Seq=2389 Ack=713 Win=2097152 Len=1460 [TC
33	6.457594	10.10.10.109	10.10.10.209	TCP	54	63208 → 80 [ACK] Seq=713 Ack=3849 Win=2102272 Len=0
34	6.457833	10.10.10.209	10.10.10.109	TCP	1...	80 → 63208 [ACK] Seq=3849 Ack=713 Win=2097152 Len=1460 [TC
35	6.457834	10.10.10.209	10.10.10.109	TCP	1...	80 → 63208 [ACK] Seq=5309 Ack=713 Win=2097152 Len=1460 [TC
36	6.457835	10.10.10.209	10.10.10.109	TCP	1...	80 → 63208 [ACK] Seq=6769 Ack=713 Win=2097152 Len=1460 [TC

- Za pomocą narzędzi wyszukiwania znaleźć pakiet synchronizacyjny **PCKlienta** z **SERWERM**.



17	6.311480	10.10.10.109	10.10.10.209	DNS	69	Standard query 0x2b5f A www.local
18	6.311932	10.10.10.209	10.10.10.109	DNS	85	Standard query response 0x2b5f A www.local A 10.
19	6.313763	10.10.10.109	10.10.10.209	TCP	66	63208 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
20	6.313884	10.10.10.109	10.10.10.209	DNS	69	Standard query 0xcc83 A www.local
21	6.314068	10.10.10.209	10.10.10.109	TCP	66	80 → 63208 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=
22	6.314096	10.10.10.109	10.10.10.209	TCP	54	63208 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
23	6.314197	10.10.10.109	10.10.10.209	HTTP	402	GET / HTTP/1.1

19 6.313763 10.10.10.109 10.10.10.209 TCP 66 63208 → 80 [SYN]

Wireshark · Packet 19 · strona IIS sewera WIN2022.pcapng

> Frame 19: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

> Ethernet II, Src: e8:9c:25:10:2b:5f (e8:9c:25:10:2b:5f), Dst: Asus

> Internet Protocol Version 4, Src: 10.10.10.109, Dst: 10.10.10.209

> Transmission Control Protocol, Src Port: 63208, Dst Port: 80, Seq:

Source Port: 63208

Destination Port: 80

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

[Next sequence number: 0 (relative sequence number)]

Acknowledgment number: 0

1000 = Header Length: 32 bytes (8)

> Flags: 0x002 (SYN)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion Window Reduced (CWR): Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...0 = Acknowledgment: Not set

.... 0... = Push: Not set

....0.. = Reset: Not set

>1. = Syn: Set

....0 = Fin: Not set

[TCP Flags:S.]

Window size value: 64240

[Calculated window size: 64240]

Checksum: 0x2978 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

- Ustaw czas blokady strony **www.local** w zakładce ACL/Time-Range/Time-Range Create

T2500G-10MPS

Time-Range Summary

Time-Range Create

Holiday Config

System

Switching

VLAN

Spanning Tree

Multicast

DHCP

QoS

PoE

ACL

• Time-Range

• ACL Config

• Policy Config

• ACL Binding

• Policy Binding

Create Time-Range

Name: deny_www.local

☐ Holiday
☐ Absolute
☒ Week

Start Date: 2000 / 01 / 01

End Date: 2000 / 01 / 01

☐ Mon
☐ Tue
☐ Wed
☐ Thu
☒ Fri
☐ Sat
☐ Sun

Create Time-Slice

Start Time: 08 : 00

End Time: 10 : 00

Create

Time-Slice Table

Index	Start Time	End Time	Delete

Apply

Help

Time-Range Table							
Select	Index	Time-Range Name	Slice 1	Slice 2	Slice 3	Slice 4	Mode
☐	1	Drukarka_ricoh	09:00-10:00	---	---	---	Week
☐	2	zdalny_dostep	09:00-10:00	---	---	---	Week
☐	3	deny_www.local	08:00-10:00	---	---	---	Week

All

Delete

Help

- Zablokuj dostęp **PCKlienta** do strony www.local.

T2500G-10MPS

System

Switching

VLAN

Spanning Tree

Multicast

DHCP

QoS

PoE

ACL

• Time-Range

• **ACL Config**

• Policy Config

• ACL Binding

ACL Summary

ACL Create

MAC ACL

Standard-IP ACL

Extend-IP ACL

ACL Create

ACL ID:

1502

0-499 MAC ACL

500-1499 Standard-IP ACL

1500-2499 Extend-IP ACL

Rule Order:

User Config

Apply

Help

Extend-IP Rule

ACL ID: ACL 1502

Rule ID: 10

Index: 1

Operation: Deny

☒ S-IP: 10.10.10.109 Mask: 255.255.255.255 (F 19☒ D-IP: 10.10.10.209 Mask: 255.255.255.255

IP Protocol: 6 TCP

TCP Flag: URG * ACK * PSH * RST * SYN 1 FIN *

☐ S-Port:☒ D-Port: 80

DSCP: No Limit

IP ToS: No Limit

IP Pre: No Limit

Time-Range: deny_www.local

Apply

Back

Help

Port-Bind Config

ACL ID: 1502

Apply

Port:

Help

UNIT: 1

1 2 3 4 5 6 7 8 9 10



Unselected Port(s)



Selected Port(s)



Not Available for Selection

Port-Bind Table

UNIT: 1

Index	ACL ID	Port	Direction
No entry in the table.			

Search Options

Show Mode:

Show All



ACL Vlan-Bind Table

Select	Index	ACL ID	Interface	Direction
No entry in the table.				

All

Delete

ACL Port-Bind Table

UNIT:

1

Select	Index	ACL ID	Interface	Direction
☐				
☐	1	1502	Port 1/0/3	Ingress

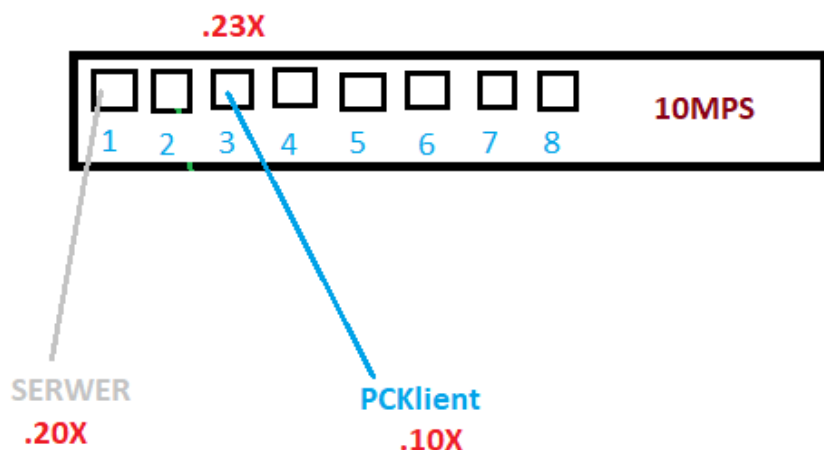
All

Delete

Help

- Za pomocą programu Wireshar udowodnij, że blokada procesu synchronizacyjnego PCKlienta z SERWEREM SYN/SYN ACK/ ACK się powiodła.

CEL3: Blokowanie **PCKlientowi** dostępu do usługi DHCP na **SERWERZE 10.10.10.20X/24**.



- Zainstaluj usługę DNS i DHCP na **SERWERZE**.
- Skonfiguruj usługę DHCP następująco:
 - X- numer stanowiska
 - PULA STANOWISKO_X
 - Zakres: 10.10.10.X1 - X9/24
 - Dzierżawa: 600 minut
 - Brama domyślna: 10.10.10.1
 - DNS: 10.10.10.20X
 - Wykluczenia: ?
- Na **PCKliencie** uruchom program Wireshark i przechwyc czterech etapowy proces pozyskiwania adresu IPv4 protokołu DHCP. Powinnes przechwycić cztery pakiety DHCP: Discover/Offer/Request/ACK

No.	Time	Source	Destination	Protocol	Length	Info
30	3.523381	10.10.10.91	10.10.10.209	DHCP	342	DHCP Release - Transaction ID 0xda1a124f
104	12.5191...	0.0.0.0	255.255.255...	DHCP	342	DHCP Discover - Transaction ID 0xab1d86bb
105	12.5198...	10.10.10.209	255.255.255...	DHCP	342	DHCP Offer - Transaction ID 0xab1d86bb
106	12.5201...	0.0.0.0	255.255.255...	DHCP	354	DHCP Request - Transaction ID 0xab1d86bb
108	12.5211...	10.10.10.209	255.255.255...	DHCP	342	DHCP ACK - Transaction ID 0xab1d86bb
173	16.4837...	192.168.7.1	255.255.255...	DHCP	342	DHCP Offer - Transaction ID 0xab1d86bb
174	16.4857...	192.168.7.1	255.255.255...	DHCP	342	DHCP NAK - Transaction ID 0xab1d86bb

Wireshark - Packet 104 - NIC1

> Frame 104: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0

> Ethernet II, Src: e8:9c:25:10:2b:5f (e8:9c:25:10:2b:5f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

> User Datagram Protocol, Src Port: 68, Dst Port: 67

> Bootstrap Protocol (Discover)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0xab1d86bb

Seconds elapsed: 0

> Bootp flags: 0x8000, Broadcast flag (Broadcast)

Client IP address: 0.0.0.0

Your (client) IP address: 0.0.0.0

Next server IP address: 0.0.0.0

Relay agent IP address: 0.0.0.0

Client MAC address: e8:9c:25:10:2b:5f (e8:9c:25:10:2b:5f)

Client hardware address padding: 00000000000000000000

Server host name not given

- Na przełączniku 10MPS zablokuj **PCKlientowi** dostęp do usługi DHCP na **SERWERZE**.

T2500G-10MPS

System
Switching
VLAN
Spanning Tree
Multicast
DHCP
QoS
PoE
ACL
Time-Range
• ACL Config
• Policy Config
• ACL Binding
• Policy Binding
Network Security

Time-Range SummaryTime-Range CreateHoliday Config

Create Time-Range

Name:deny_dhcp

☐ Holiday

☐ Absolute

☒ Week

Start Date:2000 / 01 / 01End Date:2000 / 01 / 01

☐ Mon☐ Tue☐ Wed☐ Thu☒ Fri☐ Sat☐ Sun

Create Time-Slice

Start Time:15 : 00End Time:16 : 00

Create

Time-Slice Table

Index	Start Time	End Time	Delete
			ApplyHelp

Time-Range SummaryTime-Range CreateHoliday Config

Time-Range Table						
Select	Index	Time-Range Name	Slice 1	Slice 2	Slice 3	Slice 4
☐	1	Drukarka_ricoh	09:00-10:00	---	---	---
☐	2	zdalny_dostep	09:00-10:00	---	---	---
☐	3	deny_www.local	08:00-10:00	---	---	---
☐	4	deny_dhcp	15:00-16:00	---	---	---

AllDeleteHelp

T2500G-10MPS

System
Switching
VLAN
Spanning Tree
Multicast
DHCP
QoS
PoE
ACL
• Time-Range
ACL Config

ACL SummaryACL CreateMAC ACLStandard-IP ACLExtend-IP ACL

ACL Create

ACL ID:1503

0-499 MAC ACL
500-1499 Standard-IP ACL
1500-2499 Extend-IP ACL

Rule Order:User Config

ApplyHelp

T2500G-10MPS

ACL Summary

ACL Create

MAC ACL

Standard-IP ACL

Extend-IP ACL

System

Switching

VLAN

Spanning Tree

Multicast

DHCP

QoS

PoE

ACL

• Time-Range

• ACL Config

• Policy Config

• ACL Binding

• Policy Binding

Network Security

SNMP

LLDP

Maintenance

Create Extend-IP Rule

ACL ID:

ACL 1503

Rule ID:

10

(0-1999)

Operation:

Deny

☒ S-IP:

0.0.0.0

Mask:

255.255.255.255

(Format: 192.168.0.1)

☒ D-IP:

255.255.255.255

Mask:

255.255.255.255

IP Protocol:

17 UDP

TCP Flag:

URG

*

ACK

*

PSH

*

RST

*

SYN

*

FIN

*

☒ S-Port:

68

☒ D-Port:

67

DSCP:

No Limit

IP ToS:

No Limit

IP Pre:

No Limit

Time-Range:

deny_dhcp

Apply

Help

ACL Summary

ACL Create

MAC ACL

Standard-IP ACL

Extend-IP ACL

Search Options

Select an ACL: ACL 1503

ACL Type: Extend-IP ACL

Rule Order: User Config

Rule Table

Select	Index	Rule ID	S-IP Address	D-IP Address	L3 Information	Time-Range Name
☐	1	10	0.0.0.0	255.255.255.255	UDP	deny_dhcp

AllDeleteHelp

T2500G-10MPS

Binding Table

Port Binding

VLAN Binding

Port-Bind Config

ACL ID: 1503

Port:

UNIT: 1

12345678910

Unselected Port(s) Selected Port(s) Not Available for Selection

Port-Bind Table

UNIT: 1

Index	ACL ID	Port	Direction
No entry in the table.			

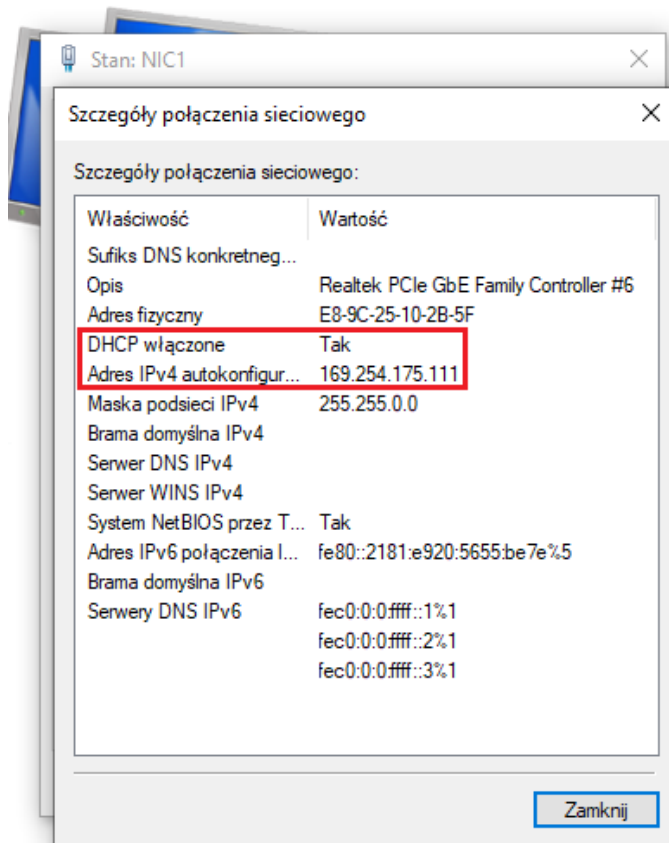
- Na **PCKliencie** uruchom program Wireshark i przechwyc cztero etapowy proces pozyskiwania adresu IPv4 protokołu DHCP. Powiniśś przechwycić tylko pakiety DHCP Discover, a klient powinien otrzymać adres IPv4 wygenerowany przez system operacyjny komputera **169.254.x.x**.

*NIC1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

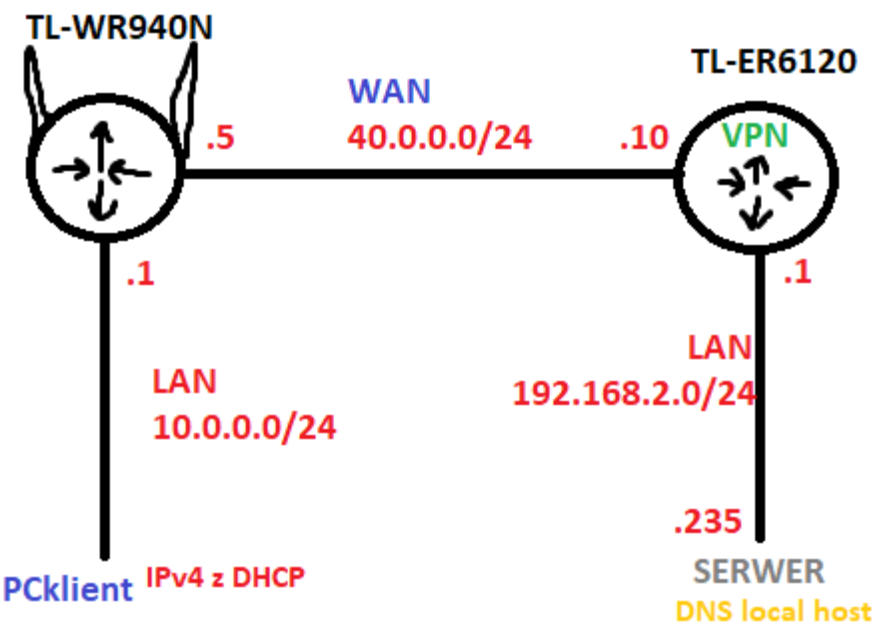
bootp lub dhcp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255...	DHCP	342	DHCP Discover - Transaction ID 0x9d9be9d4
2	3.727844	0.0.0.0	255.255.255...	DHCP	342	DHCP Discover - Transaction ID 0x9d9be9d4
3	6.921492	0.0.0.0	255.255.255...	DHCP	342	DHCP Discover - Transaction ID 0x9d9be9d4
4	15.9056...	0.0.0.0	255.255.255...	DHCP	342	DHCP Discover - Transaction ID 0x9d9be9d4
5	31.4000...	0.0.0.0	255.255.255...	DHCP	342	DHCP Discover - Transaction ID 0x9d9be9d4



•

6.1 Remote Access L2TP VPN Topology



Configuration Procedure

Follow the steps below to configure L2TP VPN on the router and PC:

- Configuring the router

1) Choose the menu **Preferences > VPN IP Pool > VPN IP Pool** to load the configuration page, and click **Add**. Specify the pool name as VPN_Pool, and enter the starting/ending IP address.

▼ Preferences

• IP Group

• Time Range

• VPN IP Pool

• Service Type

▶ Transmission

▶ Firewall

▶ Behavior Control

▶ VPN

▶ Authentication

▶ Services

▶ System Tools

VPN IP Pool List

+ Add

- Delete

☒	ID	IP Pool Name	Starting IP Address	Ending IP Address	Operation
--	1	brzozowa5	10.0.0.100	10.0.0.199	---

IP Pool Name:

brzozowa5

Starting IP Address:

10.0.0.100

Ending IP Address:

10.0.0.199

OK

Cancel

2) Choose the menu **VPN> L2TP > Global Config** to load the following page. You can keep the L2TP/PPP hello interval as the default value.

3) Choose the menu **VPN> L2TP > L2TP Server** to load the configuration page, and click **Add**. Specify WAN1 as the outgoing interface of L2TP VPN tunnel, enable IPsec encryption and specify the pre-shared key as 123456.

4) Choose the menu **VPN> Users > Users** to load the configuration page, and click **Add**. Specify the account name as tplink, and enter the password 123456. Select the protocol as L2TP, specify the LAN IP (192.168.2.1) as the local IP address of the gateway router, select VPN_Pool as the IP address pool to assign an IP address for the L2TP client, enter the DNS address (for example, 8.8.8.8), select the network mode as Client-to-LAN as the VPN gateway is connected to a host, specify the max connections as 10, then click **OK**.

User Account List

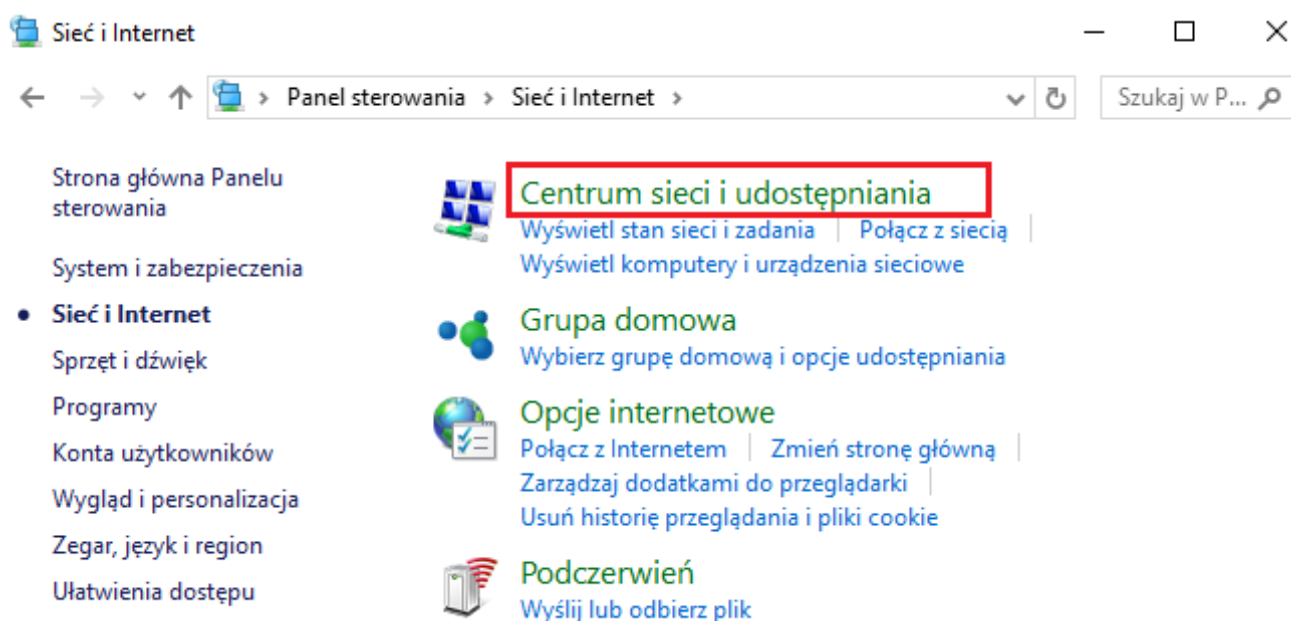
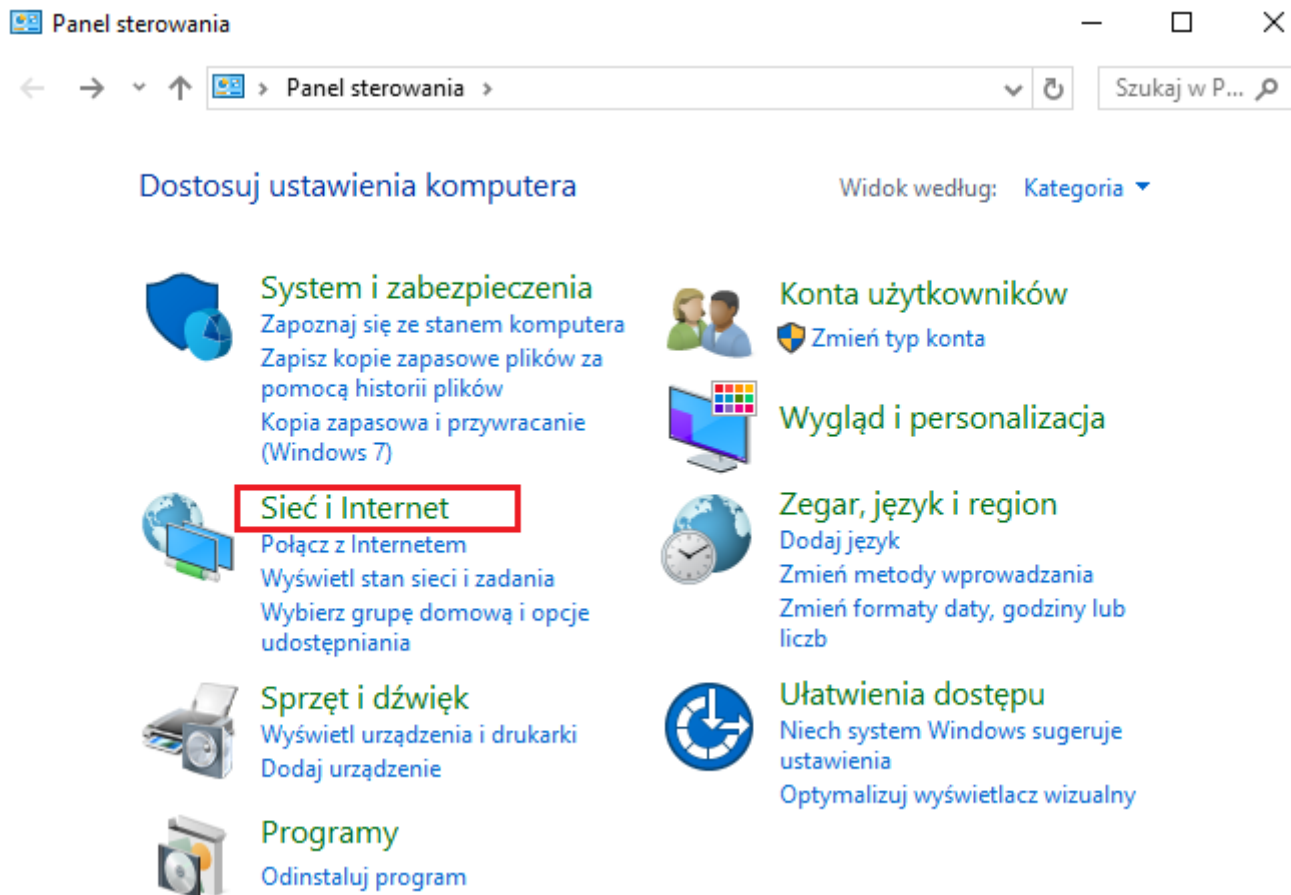
 Add Delete

☐	ID	Account Name	Protocol	Local IP Address	IP Address Pool	Network Mode	Remote Subnet	Operation
--	1	michal	L2TP	192.168.2.1	brzozowa5	Client-to-LAN	--	---

Account Name:	michal		
Password:	••••••		
	Low	Middle	High
Protocol:	L2TP ▼		
Local IP Address:	192.168.2.1		
IP Address Pool:	brzozowa5 ▼		
DNS Address:	8.8.8.8		
Network Mode:	Client-to-LAN ▼		
Max Connections:	10 (1-100)		

Configuring the Remote PC (PCKlient)

For remote PC, use Windows built-in L2TP software or third-party L2TP software to connect to L2TP server.



Strona główna Panelu sterowania

Zmień ustawienia karty sieciowej

Zmień zaawansowane ustawienia udostępniania

Wyświetl podstawowe informacje o sieci i skonfiguruj połączenia

Wyświetl aktywne sieci

Połączenie sieci VPN
Sieć publiczna

Typ dostępu: Brak dostępu do Internetu
Połączenia: [Połączenie sieci VPN](#)

Sieć 5
Sieć publiczna

Typ dostępu: Brak dostępu do Internetu
Połączenia: [NIC2](#)

Zmień ustawienia sieci



Skonfiguruj nowe połączenie lub nową sieć

Skonfiguruj połączenie szerokopasmowe, telefoniczne lub VPN albo skonfiguruj router lub punkt dostępu.



Rozwiąż problemy

Zdiagnozuj i rozwiąż problemy z siecią lub uzyskaj informacje na temat rozwiązywania problemów.

← Skonfiguruj połączenie lub sieć

Wybierz opcję połączenia.



Połącz z Internetem

Skonfiguruj połączenie szerokopasmowe lub telefoniczne z Internetem.



Skonfiguruj nową sieć

Skonfiguruj nowy router lub punkt dostępu.



Połącz z miejscem pracy

Skonfiguruj połączenie telefoniczne lub połączenie VPN z miejscem pracy.

Dalej

Anuluj

←  Połącz z miejscem pracy

Jak chcesz się łączyć?

- Użyj mojego połączenia internetowego (VPN)
Połącz przy użyciu połączenia wirtualnej sieci prywatnej (VPN) za pośrednictwem Internetu.



- Wybierz numer bezpośrednio
Połącz bezpośrednio z numerem telefonu bez pośrednictwa Internetu.



Anuluj

←  Połącz z miejscem pracy

Czy chcesz skonfigurować połączenie internetowe przed kontynuowaniem?

Do używania połączenia sieci VPN niezbędne jest połączenie internetowe.

- Konfiguruj połączenie internetowe
- Skonfiguruję połączenie internetowe później

Anuluj

Wpisz adres internetowy, z którym chcesz się połączyć

Ten adres można uzyskać od administratora sieci.

Adres internetowy:	40.0.0.10
Nazwa miejsca docelowego:	Brzozowa5

- ☐ Użyj karty inteligentnej
- ☒ Zapamiętaj moje poświadczenia
-  ☐ Zezwalaj innym osobom na korzystanie z tego połączenia
Ta opcja zezwala dowolnej osobie z dostępem do tego komputera na używanie tego połączenia.

Utwórz

Anuluj

Połączenia sieciowe

← → ▾ ▴  > Panel sterowania > Sieć i Internet > Połączenia sieciowe

Organizuj ▾ Uruchom to połączenie Zmień nazwę tego połączenia Usuń to połączenie Zmień ustawienia tego połączenia



Połącz/Rozłącz

Stan

Ustaw jako połączenie domyślne

Utwórz kopię

Utwórz skrót



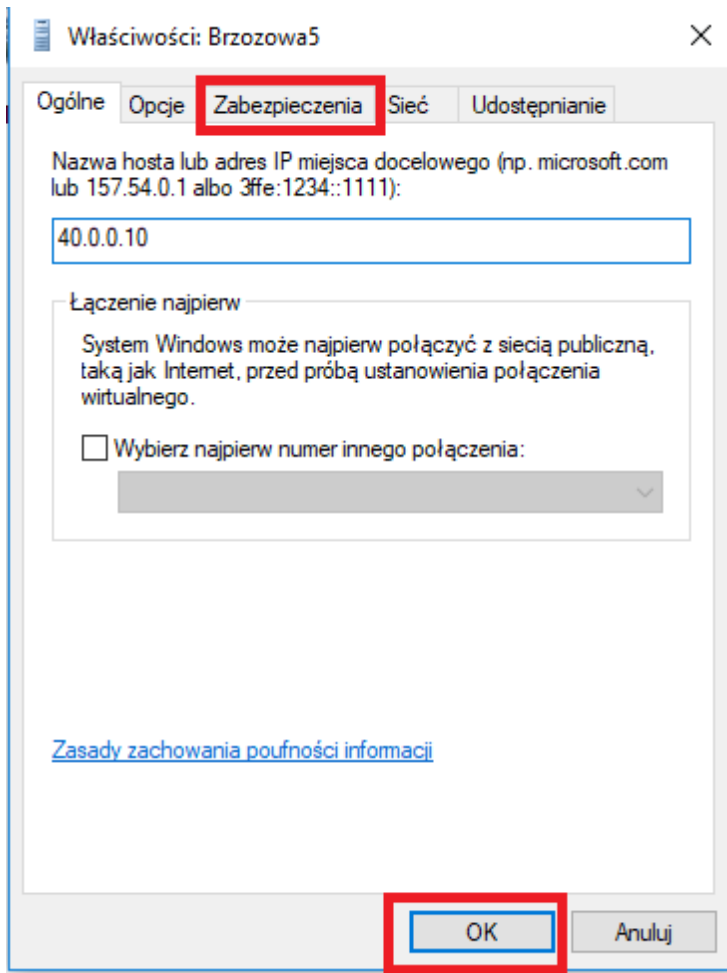
Usuń

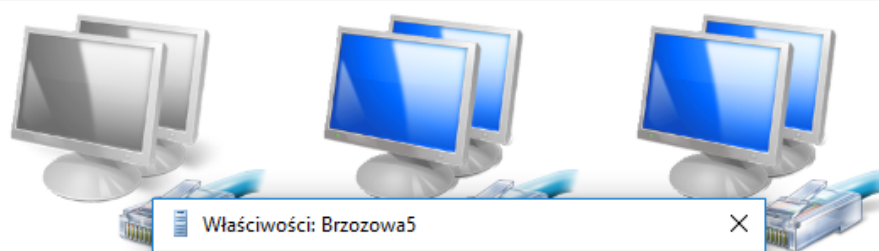
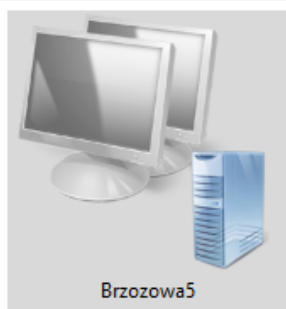


Zmień nazwę



Właściwości





INTER

Host-Only

Właściwości: Brzozowa5

Ogólne Opcje Zabezpieczenia Sieć Udostępnianie

Typ wirtualnej sieci prywatnej (VPN):

Automatyczny

Automatyczny
Protokół PPTP (Point to Point Tunneling Protocol)
Protokół L2TP/IPSec (Layer 2 Tunneling Protocol with IPsec)
Protokół SSTP (Secure Socket Tunneling Protocol)
IKEv2

Uwierzelnianie

☐ Użyj protokołu uwierzelniania rozszerzonego (EAP)

Właściwości

☐ Zezwalaj na użycie tych protokołów

Protokół EAP-MSCHAPv2 zostanie użyty dla sieci VPN typu IKEv2. Wybierz dowolny z podanych protokołów dla innych typów sieci VPN.

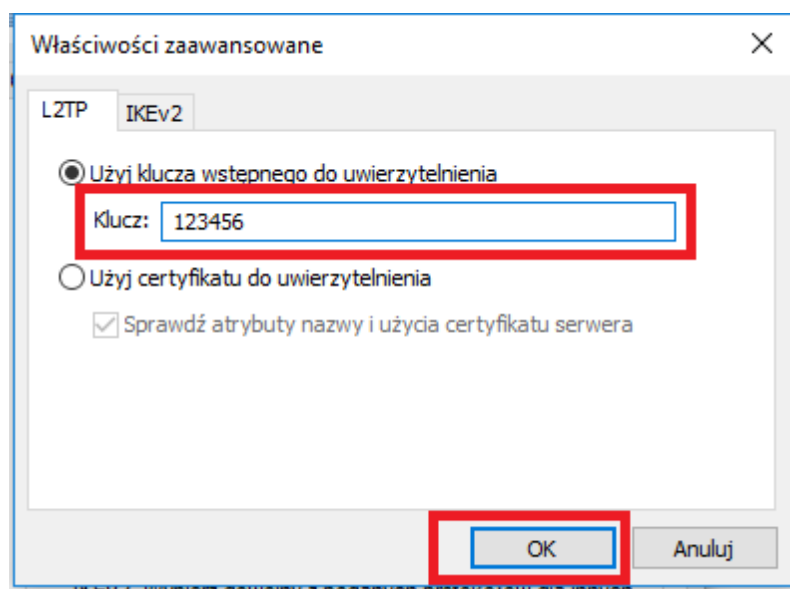
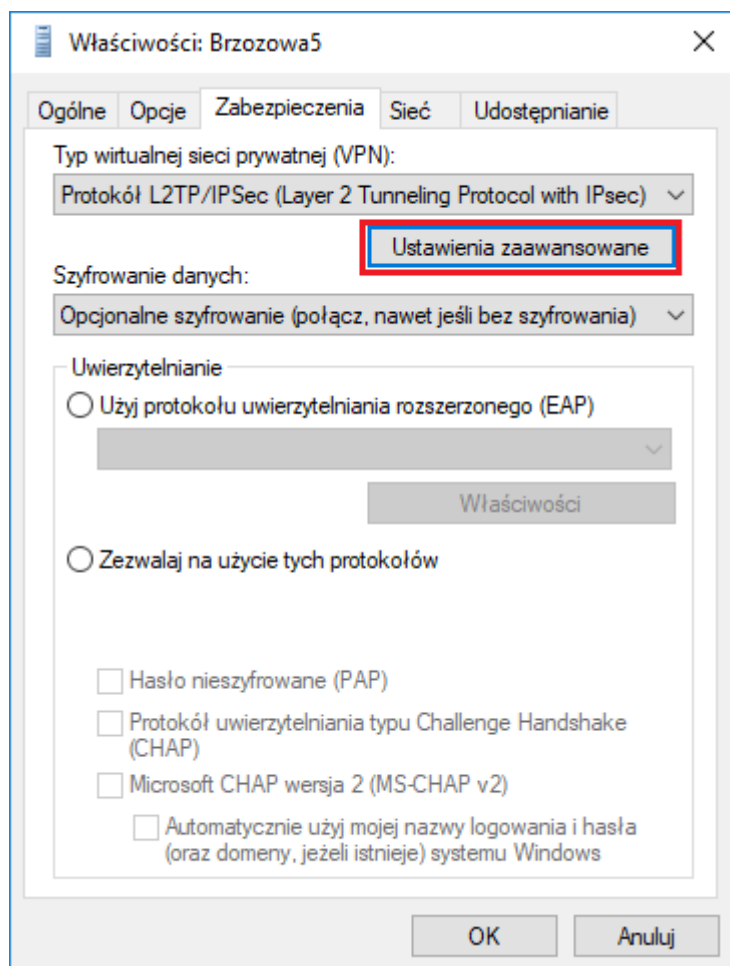
☐ Hasło nieszyfrowane (PAP)

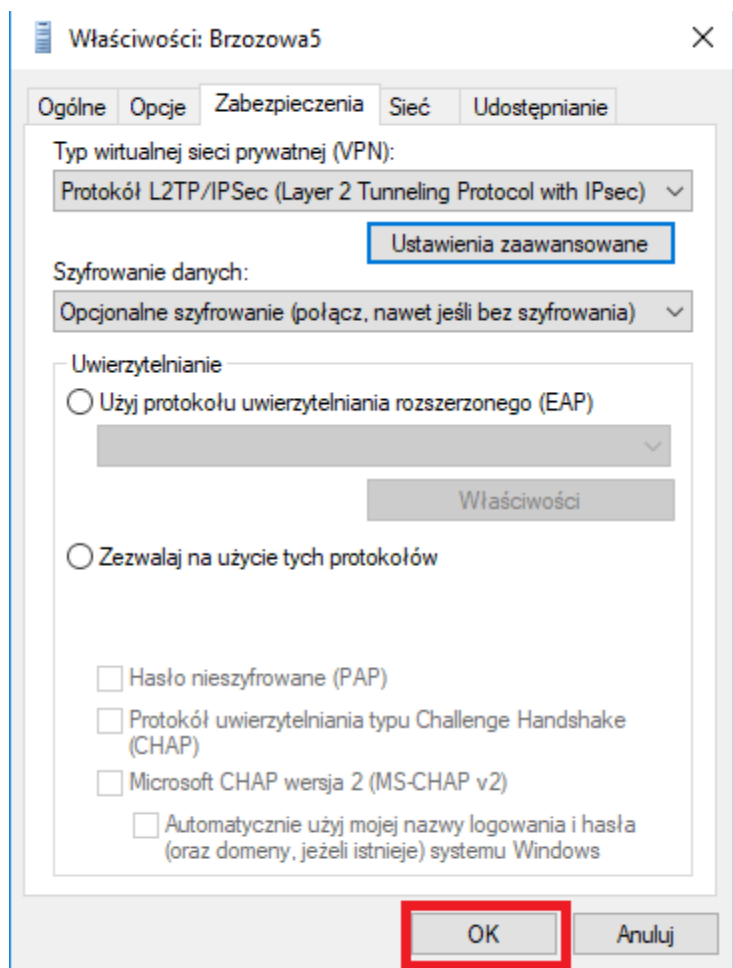
☐ Protokół uwierzelniania typu Challenge Handshake (CHAP)

☐ Microsoft CHAP wersja 2 (MS-CHAP v2)

☐ Automatycznie użyj mojej nazwy logowania i hasła (oraz domeny, jeżeli istnieje) systemu Windows

OK Anuluj





Łączymy się do sieci

Panel sterowania > Sieć i Internet > Połączenia sieciowe

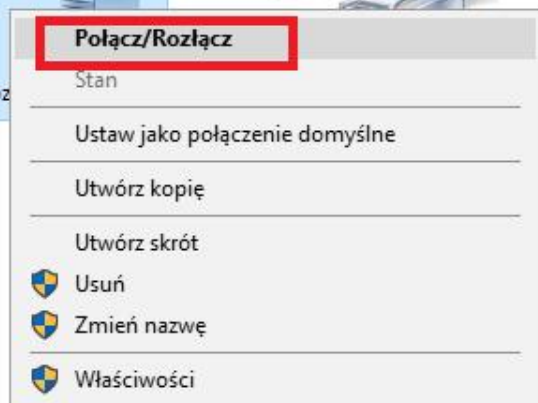
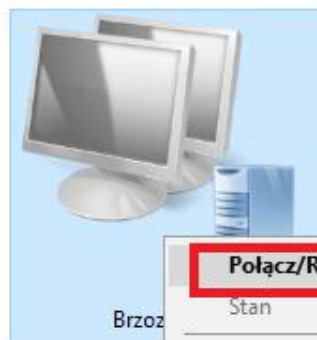
Organizuj

Uruchom to połączenie

Zmień nazwę tego połączenia

Usuń to połączenie

Zmień ustawienia tego połączenia



Ustawienia

Strona główna

Znajdź ustawienie

Sieć i Internet

Stan

Ethernet

Telefoniczne

VPN

Zużycie danych

Serwer proxy

VPN

VPN



Dodaj połączenie VPN



Brzoza5

Opcje zaawansowane

Zezwalaj na połączenia VPN w sieciach taryfowych



Włączone

Zezwalaj na połączenia VPN podczas korzystania z roamingu



Włączone

 Strona główna

Znajdź ustawienie



Sieć i Internet

 Stan Ethernet Telefoniczne VPN Zużycie danych Serwer proxy

VPN

VPN



Dodaj połączenie VPN



Brzozowa5

Połącz

Opcje zaawansowane

Usuń

Opcje zaawansowane

Zezwalaj na połączenia VPN w sieciach taryfowych



Włączone

Zezwalaj na połączenia VPN podczas korzystania z roamingu



Włączone

 Strona główna

Znajdź ustawienie



Sieć i Internet

 Stan Ethernet Telefoniczne VPN Zużycie danych Serwer proxy

VPN

VPN



Dodaj połączenie VPN



Brzozowa5

Połączono

Opcje zaawansowane

Rozłącz

Opcje zaawansowane

Zezwalaj na połączenia VPN w sieciach taryfowych



Włączone

Zezwalaj na połączenia VPN podczas korzystania z roamingu



Włączone

Zezwalaj na znajdowanie tego komputera

Zezwalaj innym komputerom i urządzeniom w tej sieci na znajdowanie Twojego komputera. Ze względów bezpieczeństwa zalecamy włączenie tego ustawienia w prywatnej sieci domowej lub służbowej, ale nie w sieci publicznej.

☐ Wyłączone

Właściwości połączenia

Nazwa połączenia	Brzozowa5
Nazwa serwera lub adres IP	40.0.0.10
Typ informacji logowania	Nazwa użytkownika i hasło
Nazwa użytkownika (opcjonalnie)	michal
Hasło (opcjonalnie)	

Edytuj

Wyczyść informacje logowania

←

Ustawienia

—

□

×

Edytowanie połączenia sieci VPN

Te zmiany zostaną wprowadzone po następnym nawiązaniu połączenia.

Nazwa połączenia

Brzozowa5

×

Nazwa lub adres serwera

40.0.0.10

Typ sieci VPN

L2TP/IPsec z kluczem wstępnym

▼

Klucz wstępny

.....

Typ informacji logowania

Nazwa użytkownika i hasło

▼

Nazwa użytkownika (opcjonalnie)

Zapisz

Anuluj

```
C:\Users\user>ping 192.168.2.235
```

```
Pinging 192.168.2.235 with 32 bytes of data:
```

```
Reply from 192.168.2.235: bytes=32 time=1ms TTL=126
```

```
Reply from 192.168.2.235: bytes=32 time<1ms TTL=126
```

```
Reply from 192.168.2.235: bytes=32 time<1ms TTL=126
```

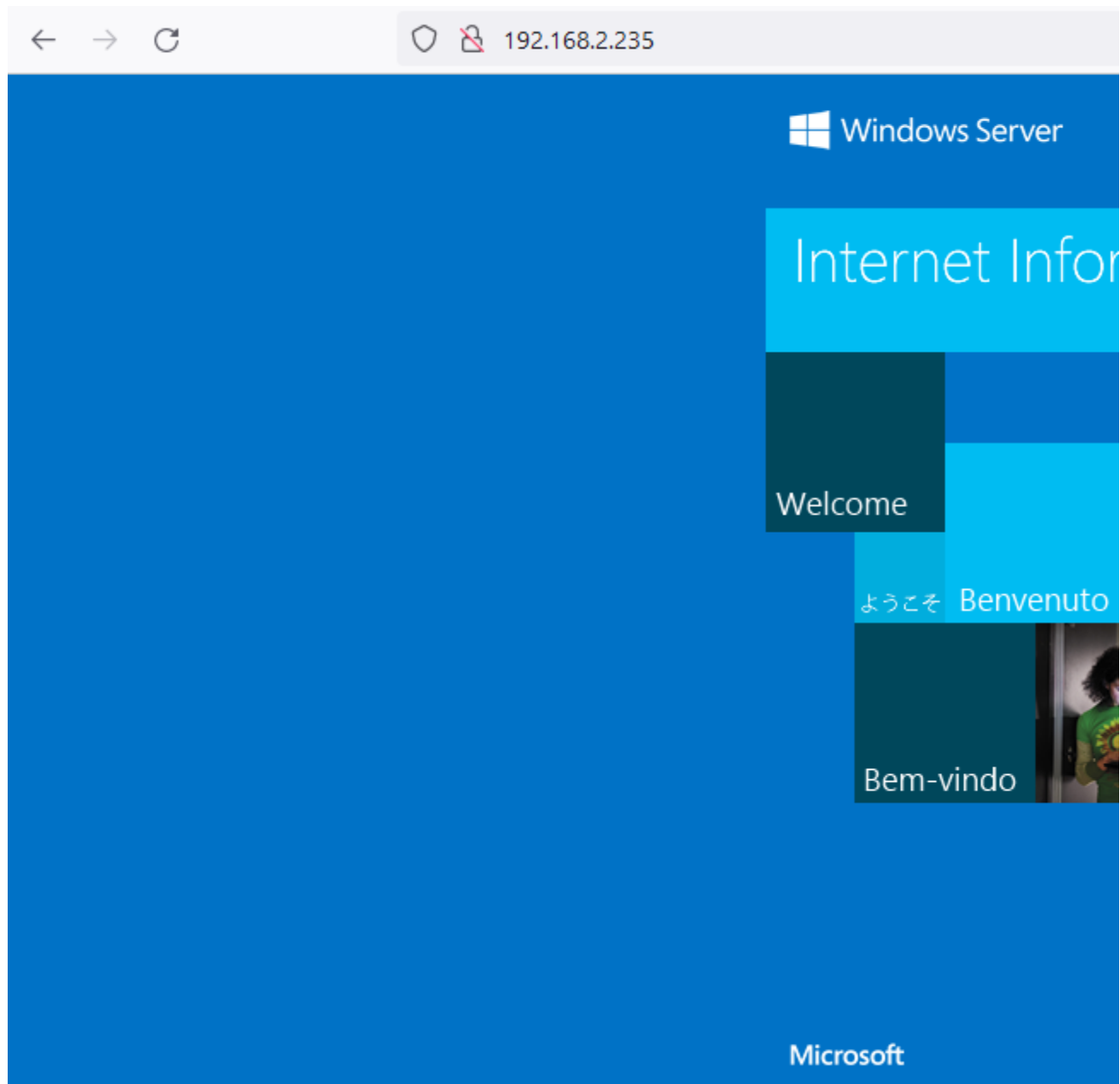
```
Reply from 192.168.2.235: bytes=32 time<1ms TTL=126
```

```
Ping statistics for 192.168.2.235:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Round-trip times: Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```



2) Choose the menu **VPN> PPTP > Global Config** to load the following page. You can keep the PPTP/PPP hello interval as the default value.

► Status

► Network

► Preferences

► Transmission

► Firewall

► Behavior Control

▼ VPN

- IPsec
- L2TP
- PPTP
- Users

► Authentication

► Services

► System Tools

Logout

PPTP Server PPTP Client Global Config Tunnel List

General

PPTP Hello Interval: 60 seconds (60-1000)

PPP Hello Interval: 20 seconds (0-120, 0 means not send)

NetBIOS Passthrough: ☐ Enable

Save

3) Choose the menu **VPN> PPTP > PPTP Server** to load the configuration page, and click **Add**. Specify WAN1 as the outgoing interface of PPTP VPN tunnel, enable MPPE encryption.

► Status

► Network

► Preferences

► Transmission

► Firewall

► Behavior Control

▼ VPN

- IPsec
- L2TP
- PPTP
- Users

► Authentication

► Services

► System Tools

Logout

PPTP Server PPTP Client Global Config Tunnel List

Server List

+ Add - Delete

☐	ID	WAN	MPPE Encryption	Status	Operation
--	1	WAN	Encrypted	Enabled	---

WAN: WAN

MPPE Encryption: Encrypted

Status: ☒ Enable

OK Cancel

4) Choose the menu **VPN> Users > Users** to load the configuration page, and click

Add. Specify the account name as `tplink`, and enter the password `123456`. Select the protocol as `PPTP`, specify the LAN IP (`192.168.2.1`) as the local IP address of the gateway router, select `VPN_Pool` as the IP address pool to assign an IP address for the PPTP client, enter the DNS address (for example, `8.8.8.8`), select the network mode **LAN-to-LAN** as the network is connected to the other network, specify the max connections as `10`, then click **OK**.

▶ Status

▶ Network

▶ Preferences

▶ Transmission

▶ Firewall

▶ Behavior Control

▼ VPN

- IPsec
- L2TP
- PPTP
- Users

▶ Authentication

▶ Services

▶ System Tools

Logout

Users

User Account List

+

Add

●

Delete

☐	ID	Account Name	Protocol	Local IP Address	IP Address Pool	Network Mode	Remote Subnet	Operation
☐	--	--	--	--	--	--	--	--

Account Name:

Account Name:

Password:

•••••

Low

Middle

High

Protocol:

Protocol:

PPTP

Local IP Address:

Local IP Address:

IP Address Pool:

IP Address Pool:

brzozowa5

DNS Address:

DNS Address:

Network Mode:

Network Mode:

Client-to-LAN

Max Connections:

Max Connections: (1-100)

OK

Cancel

Strona główna

Znajdź ustawienie

Sieć i Internet

Stan

Ethernet

Telefoniczne

VPN

Zużycie danych

Serwer proxy

VPN

VPN

+ Dodaj połączenie VPN



brzozowa5

Połącz

Opcje zaawansowane

Usuń

Opcje zaawansowane

Zezwalaj na połączenia VPN w sieciach taryfowych

☒ Włączone

Zezwalaj na połączenia VPN podczas korzystania z roamingu

☒ Włączone

Strona główna

Znajdź ustawienie

Sieć i Internet

Stan

Ethernet

Telefoniczne

VPN

Zużycie danych

Serwer proxy

VPN

VPN

+ Dodaj połączenie VPN



brzozowa5

Łączenie z brzozowa5

Anuluj

Zabezpieczenia systemu Windows

Zaloguj

michal

123456



OK

Anuluj

Pokrewne ustawienia

[Zmień opcje karty](#)[Zmień opcje zaawansowane udostępniania](#)

VPN

VPN



Dodaj połączenie VPN



brzozowa5
Połączono

Opcje zaawansowane

Rozłącz

```
C:\Users\user>ping 192.168.2.235
```

```
Pinging 192.168.2.235 with 32 bytes of data:
```

```
Reply from 192.168.2.235: bytes=32 time=1ms TTL=126
```

```
Reply from 192.168.2.235: bytes=32 time<1ms TTL=126
```

```
Reply from 192.168.2.235: bytes=32 time<1ms TTL=126
```

```
Reply from 192.168.2.235: bytes=32 time<1ms TTL=126
```

```
Ping statistics for 192.168.2.235:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

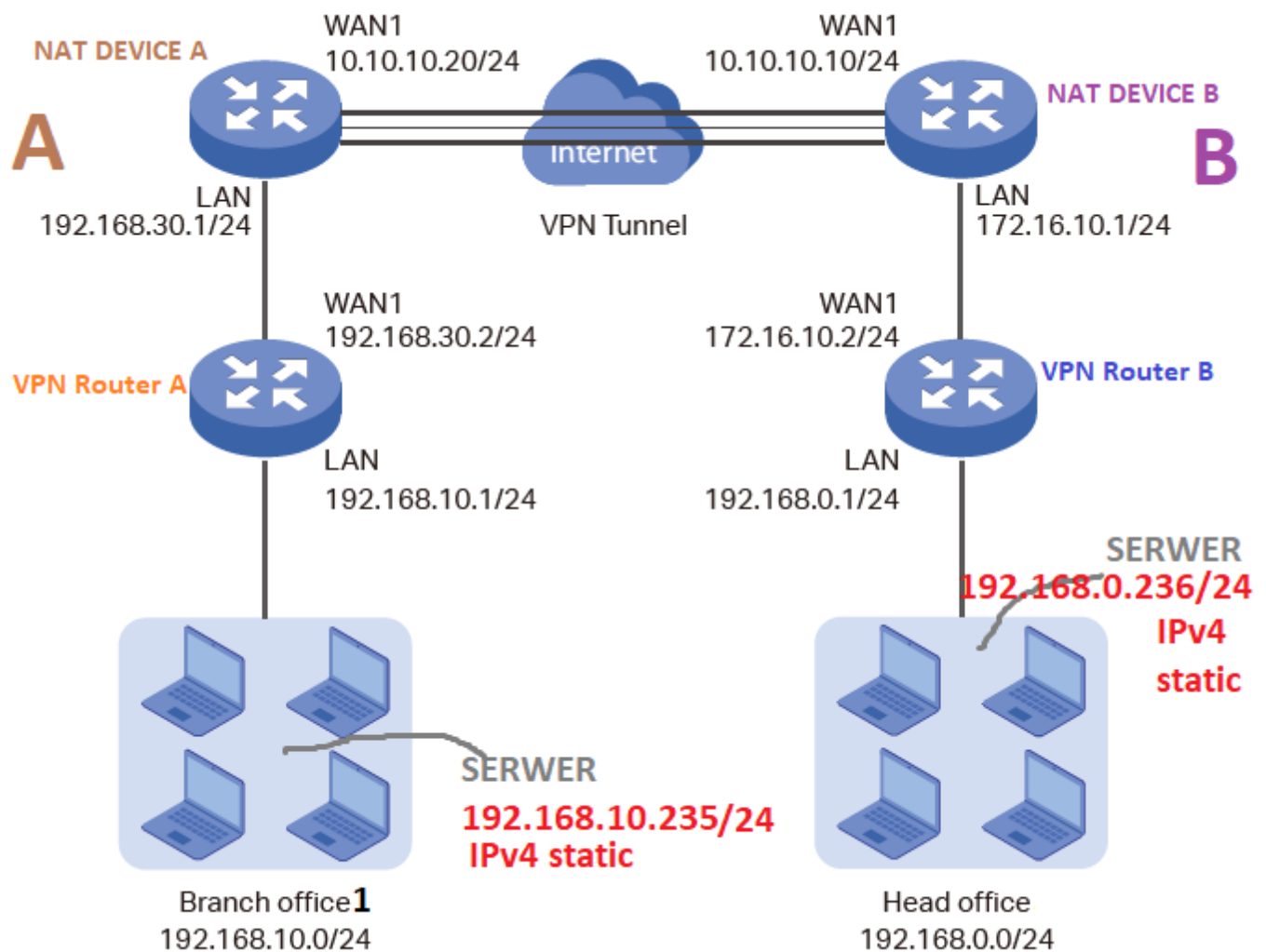
```
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Min

5.3 LAN to LAN VPN with NAT

GRUPA A

Network Topology



1. Połącz urządzenia ze sobą i dokonaj wstępnej konfiguracji urządzeń według powyższego schematu.

2. Na routerze **VPN Router A**, w zakładce **Transmission -> Routing** wypełnij pola jak na poniższym obrazku

The screenshot shows the Mikrotik WinBox interface. On the left, the 'Transmission' menu is expanded, and 'Routing' is selected. The main window displays a table of existing routes and a form for adding a new route.

ID	Name	Destination IP	Subnet Mask	Next Hop	Interface	Metric	Status	Operation
1	Branch_office1	192.168.10.0	255.255.255.0	192.168.30.2	LAN1	1	Enabled	---

The form for adding a new route contains the following fields:

- Name: Branch_office1
- Destination IP: 192.168.10.0
- Subnet Mask: 255.255.255.0
- Next Hop: 192.168.30.2
- Interface: LAN1
- Metric: 1 (0-15)
- Description: (Optional)
- Status: ☒ Enable

Buttons: OK, Cancel

3. Sprawdzenie wpisów w tabeli routingu

4. Na SERWERZE z adresem 192.168.10.235 sprawdź połączenia z portami WAN routerów:

192.168.30.1

10.10.10.20

Administrator: Wiersz polecenia

```
Pinging 10.10.10.20 with 32 bytes of data:
```

```
Control-C
```

```
^C
```

```
C:\Users\Administrator>ping 192.168.30.1
```

```
Pinging 192.168.30.1 with 32 bytes of data:
```

```
Reply from 192.168.30.1: bytes=32 time<1ms TTL=61
```

```
Reply from 192.168.30.1: bytes=32 time<1ms TTL=61
```

```
Reply from 192.168.30.1: bytes=32 time<1ms TTL=61
```

```
Reply from 192.168.30.1: bytes=32 time<1ms TTL=61
```

```
Ping statistics for 192.168.30.1:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\Users\Administrator>ping 10.10.10.20
```

```
Pinging 10.10.10.20 with 32 bytes of data:
```

```
Reply from 10.10.10.20: bytes=32 time=2ms TTL=64
```

```
Reply from 10.10.10.20: bytes=32 time=2ms TTL=64
```

```
Reply from 10.10.10.20: bytes=32 time=2ms TTL=64
```

```
Reply from 10.10.10.20: bytes=32 time=2ms TTL=64
```

```
Ping statistics for 10.10.10.20:
```

```
    Packets: Sent = 4, Received = 4,
```

```
Approximate round trip times in milli-
```

```
seconds: Minimum = 2ms, Maximum = 2ms, Ave
```

```
C:\Users\Administrator>
```

5. IPsec LAN-to-LAN VPN Configuration

LAN-to-LAN VPN can be established via three methods, including IPsec LAN-to-LAN VPN, PPTP LAN-to-LAN VPN, and L2TP LAN-to-LAN VPN. The topology shown in Figure is used as an example, with TL-ER6120 used as the VPN router for demonstration purposes. Configuration instructions for the three methods are given below.

5.1 IPsec LAN-to-LAN VPN Configuration

To configure the IPsec LAN-to-LAN VPN, follow these steps:

- 1) Configure the IPsec policy for the responder.
- 2) Configure the IPsec policy for the initiator.
- 3) (Optional) Implement configuration for NAT devices.
- 4) Verify the connectivity of the IPsec VPN tunnel.

5.1.1 Configuring the IPsec Policy for the Initiator

Select the other VPN Router as the Initiator of IPsec negotiation. Here we select **VPN Router A** as the Initiator. Follow these steps to configure IPsec Policy for the initiator.

- 1) Choose the menu **VPN > IPsec > IPsec Policy** and click **Add** to load the following page. Configure the basic parameters for the IPsec policy.

▶ Network

▶ Preferences

▶ Transmission

▶ Firewall

▶ Behavior Control

▼ VPN

- IPsec
- L2TP
- PPTP
- Users

▶ Authentication

▶ Services

▶ System Tools

Logout

IPsec Policy List

☐	ID	Policy Name	Mode	Remote Gateway	Local Subnet	Re
--	1	VPN	LAN-to-LAN	10.10.10.10	192.168.10.0/24	15

Policy Name:

VPN(1-32 characters)

Mode:

LAN-to-LAN▼

Remote Gateway:

10.10.10.10(IP Address/Domain Name)

WAN:

WAN▼

Local Subnet:

192.168.10.0 / 24

Remote Subnet:

192.168.0.0 / 24

Pre-shared Key:

123456(1-128 characters)

Status:

☒ Enable

⌵ Advanced Settings

OK

Cancel

Policy Name	Specify the name of IPsec Policy. Here we enter VPN .
Mode	Specify the mode as LAN-to-LAN .
Remote Gateway	Specify the remote gateway as 10.10.10.10 . This should be the IP address of the other end of the VPN tunnel.
WAN	Specify WAN as WAN1 . This should be the WAN port which the VPN tunnel is established on.
Local Subnet	Specify the local subnet as 192.168.10.0/24 . This should be the subnet address of the local network.
Remote Subnet	Specify the remote subnet as 192.168.0.0/24 . This should be the subnet address of the remote network.
Pre-shared key	Specify the pre-shared key as you like. Here we enter 123456 .
Status	Enable the IPsec policy list entry.

2) Click **Advanced Settings** to load the following page. In the **Phase-1 Settings** section, configure the IKE phase-1 parameters for the IPsec policy.

Proposal

Select the proposal from the drop-down list. Here we select **md5-des-dh1**.

Exchange Mode

Specify the exchange mode according to your needs. Here we specify the exchange mode as **Main Mode**.

Negotiation Mode

Specify the negotiation mode as **Responder Mode**.

Local ID Type/

Remote ID Type

Specify the local ID type and remote ID type as you like. Here we specify the local ID type and remote ID type as **NAME**.

Local ID/ Remote ID

Specify the local ID and remote ID as you like. Here we specify the local ID as **321** and remote ID as **123**.

SA Lifetime

Specify the SA lifetime as your like. Here we keep the default setting.

DPD

Enable or disable DPD (Dead Peer Detection) according to your needs. Here we disable DPD.

3) In the **Phase-2 Settings** section, configure the IKE chase-2 parameters for the IPsec policy. Click **OK**.

VPN

- IPsec
- L2TP
- PPTP
- Users

Authentication

Services

System Tools

Logout

Phase-2 Settings

Encapsulation Mode: ☒ Tunnel Mode ☐ Transport Mode

Proposal: esp-md5-des

Proposal: ---

Proposal: ---

Proposal: ---

PFS: none

SA Lifetime: 28800 seconds (120-604800)

OK Cancel

Encapsulation Mode

Specify the encapsulation mode as **Tunnel Mode**.

Proposal

Select **esp-md5-des** as the proposal. This should be kept the same as that of the responder configuration.

PFS

Select **none** as the PFS. This should be kept the same as that of the responder configuration.

SA Lifetime

Specify the SA Lifetime according to your needs. Here we keep the default setting.

6. (Optional) Implementing configuration for NAT Devices

- 1) For **NAT Device A**, choose the menu **Transmission > NAT > Virtual Servers** and click **Add** to load the following page. Configure the parameters for the virtual server. Click **OK**.

The screenshot shows the configuration interface for NAT Device A. The left sidebar has a menu with 'Transmission' selected, which includes 'NAT' and 'Virtual Servers'. The main area shows the 'Virtual Server List' table with one entry 'IPsec1'. Below the table, the configuration fields for 'IPsec1' are shown: Name (IPsec1), Interface (SFP WAN), External Port (500), Internal Port (500), Internal Server IP (192.168.30.2), Protocol (UDP), and Status (checked 'Enable'). The 'OK' button is highlighted with a red box.

ID	Name	Interface	External Port	Internal Port	Internal Server IP	Protocol	Status
--	--	--	--	--	--	--	--

Name: IPsec1

Interface: SFP WAN

External Port: 500 (XX or XX-XX ,1-65535)

Internal Port: 500 (XX or XX-XX ,1-65535)

Internal Server IP: 192.168.30.2

Protocol: UDP

Status: ☒ Enable

OK Cancel

Name	Specify a name for the virtual server list entry. Here we enter IPsec1 .
Interface	Specify WAN as This should be the WAN port which the VPN tunnel is established on.
External Port/	Specify the external port and the internal port as 500 .
Internal Port	
Internal Server IP	Specify the internal server IP as 192.168.30.2 . This should be the WAN IP address of the responder.
Protocol	Specify the protocol as UDP .
Status	Enable the virtual server list entry.

- 2) Similarly, add another virtual server list entry, with the name IPsec2, and set the external and internal port as 4500.

The screenshot shows the Mikrotik WinBox interface. On the left is a sidebar menu with categories: Status, Network, Preferences, and Transmission (expanded). Under Transmission, there are sub-items: NAT, Bandwidth Control, Session Limit, Load Balancing, and Routing. Below these are Firewall, Behavior Control, VPN, Authentication, Services, and System Tools. At the bottom of the sidebar is a Logout button. The main panel has tabs: One-to-One NAT, Virtual Servers (selected), Port Triggering, NAT-DMZ, and ALG. Below the tabs is a 'Virtual Server List' section with a table. The table has columns: ID, Name, Interface, External Port, Internal Port, and Int. The first row shows a virtual server named 'IPsec2' with Interface 'SFP WAN', External Port '4500', and Internal Port '4500'. Below the table is a configuration form for the selected virtual server. The form fields are: Name (IPsec2), Interface (SFP WAN), External Port (4500), Internal Port (4500), Internal Server IP (192.168.30.2), Protocol (UDP), and Status (checked 'Enable'). The 'OK' button is highlighted with a red box.

ID	Name	Interface	External Port	Internal Port	Int
--	--	--	--	--	--

Virtual Server Configuration:

Name: IPsec2

Interface: SFP WAN

External Port: 4500 (XX or XX-XX ,1-65535)

Internal Port: 4500 (XX or XX-XX ,1-65535)

Internal Server IP: 192.168.30.2

Protocol: UDP

Status: ☒ Enable

OK Cancel

- 3) For NAT Device A, choose the menu **Transmission > NAT > ALG** to load the following page. Enable the IPsec ALG, and click **Save**.

Status

Network

Preferences

Transmission

NAT

Bandwidth Control

Session Limit

Load Balancing

Routing

Firewall

Behavior Control

VPN

Authentication

Services

System Tools

Logout

One-to-One NATVirtual ServersPort TriggeringNAT-DMZALG

ALG

☒ FTP ALG

☒ H.323 ALG

☒ PPTP ALG

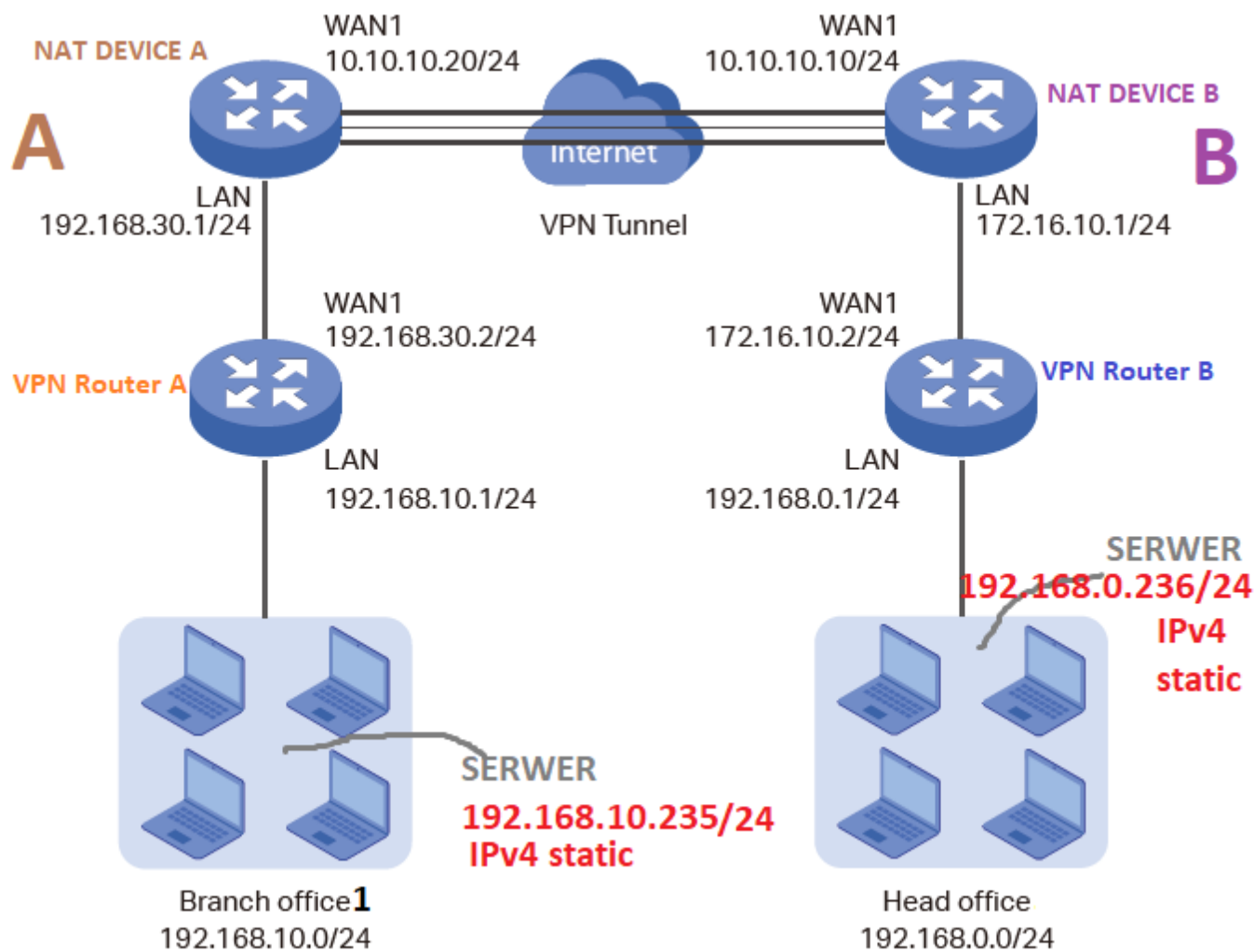
☒ SIP ALG

☒ IPsec ALG

Save

GRUPA B

Network Topology



1. Połącz urządzenia ze sobą i dokonaj wstępnej konfiguracji urządzeń według powyższego schematu.
2. Na routerze **VPN Router B**, w zakładce **Transmission -> Routing** wypełnij pola jak na poniższym obrazku

The screenshot shows the MikroTik WinBox interface. On the left, the 'Transmission' menu is expanded, and 'Routing' is selected. The main window displays the 'Static Route' configuration window. The window has tabs for 'Static Route', 'Policy Routing', and 'Routing Table'. Below the tabs, there is a table listing existing static routes. Below the table, there is a configuration form for a new static route. The form includes fields for Name, Destination IP, Subnet Mask, Next Hop, Interface, Metric, Description, and Status. A red box highlights the configuration fields, and another red box highlights the 'OK' button.

☐	ID	Name	Destination IP	Subnet Mask
--	--	--	--	--

Name: Head_office

Destination IP: 192.168.0.0

Subnet Mask: 255.255.255.0

Next Hop: 172.16.10.2

Interface: SFP WAN

Metric: 1 (0-15)

Description: Head_office (Optional)

Status: ☒ Enable

OK Cancel

3. Sprawdzenie wpisów w tabeli routingu

► Status	Static Route	Policy Routing	Routing Table
► Network			
► Preferences			
▼ Transmission			
• NAT			
• Bandwidth Control			
• Session Limit			
• Load Balancing			
• Routing			
► Firewall			
► Behavior Control			
► VPN			
► Authentication			
► Services			
► System Tools			
Logout			

Routing Table					
Entry Count: 7					
ID	Destination IP	Subnet Mask	Next Hop	Interface	Metric
1	192.168.0.0	255.255.255.0	172.16.10.2	SFP WAN	1
2	0.0.0.0	0.0.0.0	10.10.10.20	SFP WAN	0
3	8.8.4.4	255.255.255.255	10.10.10.20	SFP WAN	0
4	8.8.8.8	255.255.255.255	10.10.10.20	SFP WAN	0
5	10.10.10.0	255.255.255.0	0.0.0.0	SFP WAN	0
6	127.0.0.0	255.0.0.0	0.0.0.0	lo	0
7	172.16.10.0	255.255.255.0	0.0.0.0	LAN1	0

4. Na SERWERZE z adresem **192.168.0.235** sprawdź połączenia z portami **WAN** routerów:

172.16.10.1/24

10.10.10.10

```
C:\Users\user>ping 172.16.10.1

Pinging 172.16.10.1 with 32 bytes of data:
Reply from 172.16.10.1: bytes=32 time<1ms TTL=62
Reply from 172.16.10.1: bytes=32 time<1ms TTL=62
Reply from 172.16.10.1: bytes=32 time<1ms TTL=62
Reply from 172.16.10.1: bytes=32 time<1ms TTL=62

Ping statistics for 172.16.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\user>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.10: bytes=32 time<1ms TTL=62
Reply from 10.10.10.10: bytes=32 time<1ms TTL=62
Reply from 10.10.10.10: bytes=32 time<1ms TTL=62
Reply from 10.10.10.10: bytes=32 time<1ms TTL=62
```

5. IPsec LAN-to-LAN VPN Configuration

LAN-to-LAN VPN can be established via three methods, including IPsec LAN-to-LAN VPN, PPTP LAN-to-LAN VPN, and L2TP LAN-to-LAN VPN. The topology shown in Figure is used as an example, with TL-ER6120 used as the VPN router for demonstration purposes. Configuration instructions for the three methods are given below.

5.1 IPsec LAN-to-LAN VPN Configuration

To configure the IPsec LAN-to-LAN VPN, follow these steps:

- 1) Configure the IPsec policy for the responder.
- 2) Configure the IPsec policy for the initiator.
- 3) (Optional) Implement configuration for NAT devices.
- 4) Verify the connectivity of the IPsec VPN tunnel.

5.1.1 Configuring the IPsec Policy for the Responder

Select any one of the VPN routers as the responder. Here we select VPN Router B as the responder. Follow these steps to configure IPsec policy for the responder.

- 1) Choose the menu **VPN > IPsec > IPsec Policy** and click **Add** to load the following page. Configure the basic parameters for the IPsec Policy.

► Status

► Network

► Preferences

► Transmission

► Firewall

► Behavior Control

▼ VPN

- IPsec
- L2TP
- PPTP
- Users

► Authentication

► Services

► System Tools

Logout

IPsec Policy

IPsec SA

IPsec Policy List

☐	ID	Policy Name	Mode	Remote Gateway	Local Subnet	R
--	1	VPN	LAN-to-LAN	10.10.10.20	192.168.0.0/24	15

Policy Name:

VPN

(1-32 characters)

Mode:

LAN-to-LAN

Remote Gateway:

10.10.10.20

(IP Address/Domain Name)

WAN:

WAN

Local Subnet:

192.168.0.0

/

24

Remote Subnet:

192.168.10.0

/

24

Pre-shared Key:

123456

(1-128 characters)

Status:

☒ Enable

⚙ Advanced Settings

Policy Name	Specify the name of IPsec Policy. Here we enter VPN .
Mode	Specify the mode as LAN-to-LAN .
Remote Gateway	Specify the remote gateway as 10.10.10.20 . This should be the IP address of the other end of the VPN tunnel.
WAN	Specify WAN as WAN1 . This should be the WAN port which the VPN tunnel is established on.
Local Subnet	Specify the local subnet as 192.168.0.0/24 . This should be the subnet address of the local network.
Remote Subnet	Specify the remote subnet as 192.168.10.0/24 . This should be the subnet address of the remote network.
Pre-shared key	Specify the pre-shared key as you like. Here we enter 123456 .
Status	Enable the IPsec policy list entry.

Click **Advanced Settings** to load the following page. In the **Phase-1 Settings** section, configure the IKE phase-1 parameters for the IPsec policy.

Phase-1 Settings

Proposal:

md5-des-dh1

Proposal:

Proposal:

Exchange Mode:

☐ Initiator Mode

☒ Responder Mode

Local ID Type:

☐ IP Address

☒ NAME

Local ID:

123

(1-28 non-blank characters)

Remote ID Type:

☐ IP Address

☒ NAME

Remote ID:

321

(1-28 non-blank characters)

SA Lifetime:

28800

seconds (60-604800)

☐ Enable

DPD:

DPD Interval:

0

seconds (1-300)

Proposal Select the proposal from the drop-down list. Here we select **md5-des-dh1**.

Exchange Mode Specify the exchange mode according to your needs. Here we specify the exchange mode as **Main Mode**.

Negotiation Mode Specify the negotiation mode as **Responder Mode**.

Local ID Type/ Remote ID Type Specify the local ID type and remote ID type as you like. Here we specify the local ID type and remote ID type as **NAME**.

Local ID/ Remote ID Specify the local ID and remote ID as you like. Here we specify the local ID as **123** and remote ID as **321**.

SA Lifetime

Specify the SA lifetime as your like. Here we keep the default setting.

DPD

Enable or disable DPD (Dead Peer Detection) according to your needs. Here we disable DPD.

In the **Phase-2 Settings** section, configure the IKE chase-2 parameters for the IPsec policy. Click **OK**.

Phase-2 Settings

Encapsulation Mode:

☒ Tunnel Mode

☐ Transport Mode

Proposal:

esp-md5-des

Proposal:

Proposal:

Proposal:

PFS:

none

SA Lifetime:

28800

seconds (120-604800)

OK

Cancel

- Encapsulation Mode

Specify the encapsulation mode as **Tunnel Mode**.
- Proposal

Select **esp-md5-des** as the proposal. This should be kept the same as that of the responder configuration.
- PFS

Select **none** as the PFS. This should be kept the same as that of the responder configuration.
- SA Lifetime

Specify the SA Lifetime according to your needs. Here we keep the default setting.

6. (Optional) Implementing configuration for NAT Devices

- 1) For **NAT Device B**, choose the menu **Transmission > NAT > Virtual Servers** and click **Add** to load the following page. Configure the parameters for the virtual server. Click **OK**

The screenshot shows the 'Virtual Servers' configuration page. The left sidebar has a menu with 'Transmission' expanded, showing sub-items like 'NAT', 'Bandwidth Control', 'Session Limit', 'Load Balancing', and 'Routing'. The 'Virtual Servers' tab is selected. The main area displays a 'Virtual Server List' table with columns: ID, Name, Interface, External Port, and Internal Port. Below the table is a configuration form for the selected entry. The form fields are: Name (IPsec1), Interface (SFP WAN), External Port (500), Internal Port (500), Internal Server IP (172.16.10.2), Protocol (UDP), and Status (checked 'Enable'). The 'OK' button is highlighted with a red box.

ID	Name	Interface	External Port	Internal Port
--	--	--	--	--

Virtual Server List

Name: IPsec1

Interface: SFP WAN

External Port: 500 (XX or XX-XX ,1-65535)

Internal Port: 500 (XX or XX-XX ,1-65535)

Internal Server IP: 172.16.10.2

Protocol: UDP

Status: ☒ Enable

OK Cancel

Name

Specify a name for the virtual server list entry. Here we enter **IPsec1**.

Interface

Specify WAN as This should be the WAN port which the VPN tunnel is established on.

External Port/

Specify the external port and the internal port as **500**.

Internal Port

Internal Server IP

Specify the internal server IP as **172.16.10.2** This should be the WAN IP address of the responder.

Protocol

Specify the protocol as **UDP**.

Status

Enable the virtual server list entry.

- 2) Similarly, add another virtual server list entry, with the name IPsec2, and set the external and internal port as 4500.

The screenshot shows the firewall configuration interface. On the left is a sidebar menu with the following items: Status, Network, Preferences, Transmission (expanded), NAT, Bandwidth Control, Session Limit, Load Balancing, Routing, Firewall, Behavior Control, VPN, Authentication, Services, System Tools, and Logout. The main area has tabs for One-to-One NAT, Virtual Servers, Port Triggering, NAT-DMZ, and ALG. The 'Virtual Servers' tab is active, displaying a 'Virtual Server List' table.

☐	ID	Name	Interface	External Port	Internal Port
☐	1	IPsec1	SFP WAN	500	500
--	2	IPsec2	SFP WAN	4500	4500

Below the table is a configuration form for the selected entry (IPsec2). The form fields are: Name (IPsec2), Interface (SFP WAN), External Port (4500), Internal Port (4500), Internal Server IP (172.16.10.2), Protocol (UDP), and Status (checked 'Enable'). The 'OK' button is highlighted with a red box.

- 3) For NAT Device B, choose the menu **Transmission > NAT > ALG** to load the following page. Enable the IPsec ALG, and click **Save**.

Status

Network

Preferences

Transmission

NAT

Bandwidth Control

Session Limit

Load Balancing

Routing

Firewall

Behavior Control

VPN

Authentication

Services

System Tools

Logout

One-to-One NATVirtual ServersPort TriggeringNAT-DMZALG

ALG

☒ FTP ALG

☒ H.323 ALG

☒ PPTP ALG

☒ SIP ALG

☒ IPsec ALG

Save

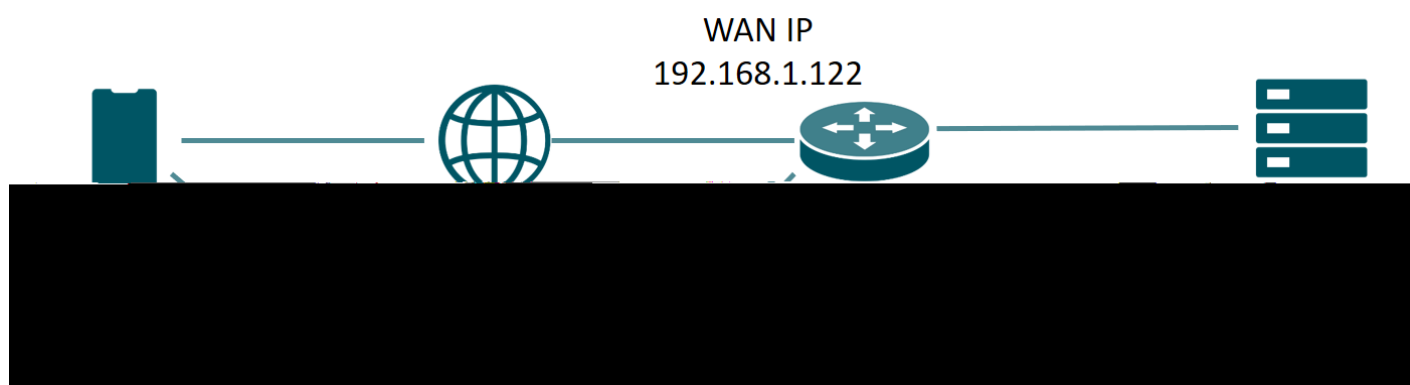
5.4 How to connect to Omada Router using IKEv2 VPN of Android/iOS

Configuration Guide

Zaktualizowano w dniu 08-25-2023

Most cell phones now support IKEv2 VPN connections. Especially since Android has removed L2TP VPN. When you are out of home without a computer around and want to access some resources from your home network, establishing a VPN connection with the router through your phone is an easy and secure way.

Next, we take the ER605 v2 as an example to show you how to configure IKEv2 VPN on Omada Router.



Configuration for IKEv2 VPN and Android/iOS

Step 1. Configure IKEv2 VPN setting on Router

(1) Choose the menu **VPN > IPsec > IPsec Policy** and click Add to load the following page on the VPN router. Configure the basic parameters for the IPsec policy.

- Specify the mode as **Client-to-LAN**.
- Specify the Remote Host as **0.0.0.0**.
- Specify the WAN as **WAN**.
- Specify the Local Network as **LAN**. Or you can customize the Local IP address.
- Specify the Pre-shared Key as you like. Here we enter **123456**.
- Specify the IP Address Pool as **10.10.10.1/24**.

Policy Name:	test	(1-32 characters)
Mode:	Client-to-LAN	
Remote Host:	0.0.0.0	(IP Address/Domain Name)
WAN:	WAN	
Local Network Type:	☒ Network ☐ Custom IP	
Local Networks:	LAN	
Pre-shared Key:		(1-128 characters)
IP Address Pool:	10.10.10.1 / 24	
Primary DNS:		(Optional)
Secondary DNS:		(Optional)
Status:	☒ Enable	

 Advanced Settings

Step 2. Configure the IKEv2 Advanced Settings – Phase 1

Click **Advanced Settings** to load the following page. In the **Phase-1 Settings** section, configure the IKE phase-1 parameters.

- Select IKE Protocol Version as **IKEv2**.
- Select **sha256-aes256-dh16/sha256-aes256-dh14/sha1-aes256-dh14/sha1-aes256-dh5** as the proposal.
- Specify Negotiation Mode as **Responder Mode**.
- Specify Local ID Type as **IP Address**.
- Specify the Remote ID Type as **NAME** and specify the remote ID as **123**.

Note:

1) Since each phone supports different proposals, we only list some common proposal combinations here. If the above four combinations cannot be successfully connected, please contact [TP-Link technical support](#).

2) Since IKEv2 for Android cannot edit Local ID Type, only IP address can be used. So it is required that there must be no NAT device on the front of Omada router, which means the WAN IP address of Omada router must be a public IP address for the client to be able to connect successfully.

Phase-1 Settings

IKE Protocol Version:	☐ IKEv1	☒ IKEv2	
Proposal:	sha256 ▼	aes256 ▼	dh16 ▼
Proposal:	sha256 ▼	aes256 ▼	dh14 ▼
Proposal:	sha1 ▼	aes256 ▼	dh14 ▼
Proposal:	sha1 ▼	aes256 ▼	dh5 ▼
Negotiation Mode:	☐ Initiator Mode	☒ Responder Mode	
Local ID Type:	☒ IP Address	☐ NAME	
Local ID:	(1-28 non-blank characters)		
Remote ID Type:	☐ IP Address	☒ NAME	
Remote ID:	(1-28 non-blank characters)		
SA Lifetime:			seconds (60-604800)
DPD:	☒ Enable		
DPD Interval:			seconds (1-300)

Step 3. Configure the IKEv2 Advanced Settings – Phase 2

In the Phase-2 Settings section, configure the IKE phase-2 parameters. Click **OK**.

- Specify Encapsulation Mode as **Tunnel Mode**.
- Select **esp-sha256-aes256/esp-sha1-aes256** as the proposal.

Phase-2 Settings

Encapsulation Mode:	☒ Tunnel Mode	☐ Transport Mode	
Proposal:	esp ▼	sha256 ▼	aes256 ▼
Proposal:	esp ▼	sha1 ▼	aes256 ▼
Proposal:	--- ▼	--- ▼	aes256 ▼
Proposal:	--- ▼	--- ▼	3des ▼
PFS:	none ▼		
SA Lifetime:	28800		seconds (120-604800)
OK Cancel			

Configure the IKEv2 VPN settings on Android

Here we use a phone with Android 12 as an example. Configure the IKEv2 VPN with the following parameters. Click **Save** and connect to the VPN server.

- Specify Name as **test**.
- Specify VPN type as **IKEv2/IPsec PSK**.
- Specify Server address as **192.168.1.122**.
- Specify IP Identifier as **123**.
- Specify IPsec Pre-shared Key as **123456**.
- Specify Proxy as **None**.

Edit VPN profile

Name

test



VPN type

IKEv2/IPSec PSK

Server address

192.168.1.122

IPSec Identifier

123

IPSec Pre-shared Key

.....



Proxy

None

Always-on VPN



Cancel

Remove

Save

Verification process

Go to **VPN > IPSec > IPSec SA**, the information about VPN Tunnel will be displayed above.

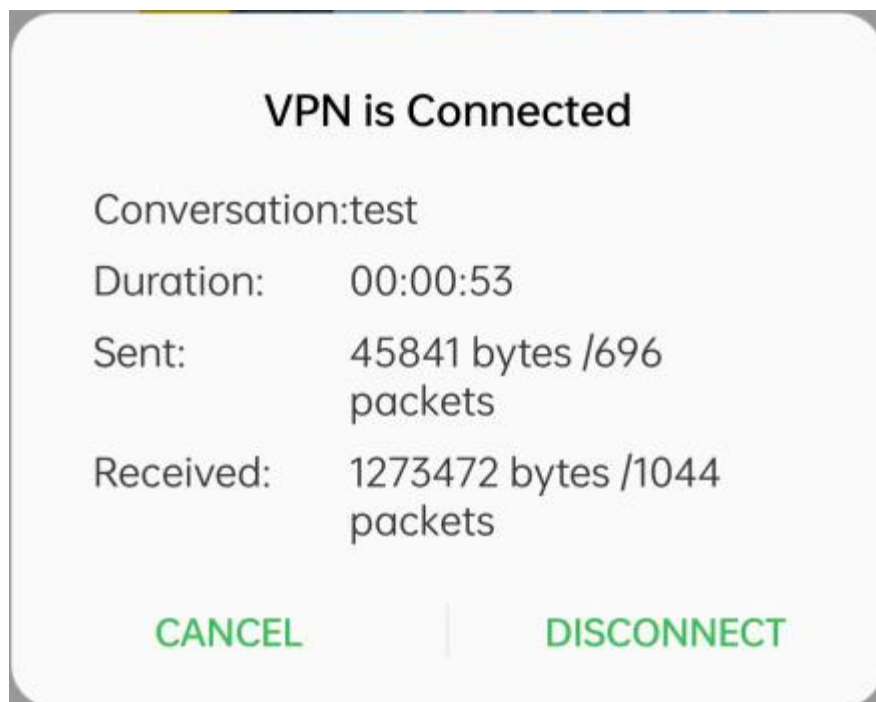
IPsec SA List

Entry Count: 2

 Refresh

☐	ID	Name	SPI	Direction	Tunnel ID	Data Flow	Protocol	AH Authentication	ESP Authentication	ESP Encryption
☐	1	test	3422662849	in	192.168.1.122<- -192.168.1.151	192.168.2.0/24 <- - 10.10.10.1/32	ESP	--	HMAC_SHA2_256_128	AES-256
☐	2	test	1792891049	out	192.168.1.122-- >192.168.1.151	192.168.2.0/24 -- > 10.10.10.1/32	ESP	--	HMAC_SHA2_256_128	AES-256

It will also show a successful VPN connection on the phone



Configure the IKEv2 VPN settings on iOS Devices

Step 1. Configure IKEv2 VPN setting on Router

Since iOS supports changing Local ID Type, we select Local ID Type as **NAME** in the phase-1 setting and specify Local ID as **321**. The other settings are exactly the same as above, so we will not show them here.

Phase-1 Settings

IKE Protocol Version:	☐ IKEv1	☒ IKEv2	
Proposal:	sha256 ▼	aes256 ▼	dh16 ▼
Proposal:	sha256 ▼	aes256 ▼	dh14 ▼
Proposal:	sha1 ▼	aes256 ▼	dh14 ▼
Proposal:	sha1 ▼	aes256 ▼	dh5 ▼
Negotiation Mode:	☐ Initiator Mode	☒ Responder Mode	
Local ID Type:	☐ IP Address	☒ NAME	
Local ID:	321	(1-28 non-blank characters)	
Remote ID Type:	☐ IP Address	☒ NAME	
Remote ID:	123	(1-28 non-blank characters)	
SA Lifetime:	28800	seconds (60-604800)	
DPD:	☒ Enable		
DPD Interval:	10	seconds (1-300)	

Step 2. Configure IKEv2 VPN setting on Phone.

Here we use iOS 15.5 as an example for IKEv2 VPN connection. Configure the IKEv2 VPN parameters. Click Done and connect to the VPN server.

- Specify Type as **IKEv2**.
- Specify Description as **Test**.
- Specify Server as **192.168.1.122**.
- Specify Remote ID as **321**.
- Specify Local ID as **123**.
- Specify User Authentication as **None**.
- Disable the Use Certificate.
- Specify Secret as **123456**.
- Specify PROXY as **Off**.

Cancel

Add Configuration

Done

Type

IKEv2 >

Description

Test

Server

192.168.1.122

Remote ID

321

Local ID

123

AUTHENTICATION

User Authentication

None >

Use Certificate

☐

Secret

PROXY

Off

Manual

Auto

Step 3. Verification process

The figure below shows that the iPhone successfully connected to the VPN Server and obtained the VPN IP address of 10.10.10.1.

< VPN

Test

Edit

Type

IKEv2

Server

192.168.1.122

Address

10.10.10.1

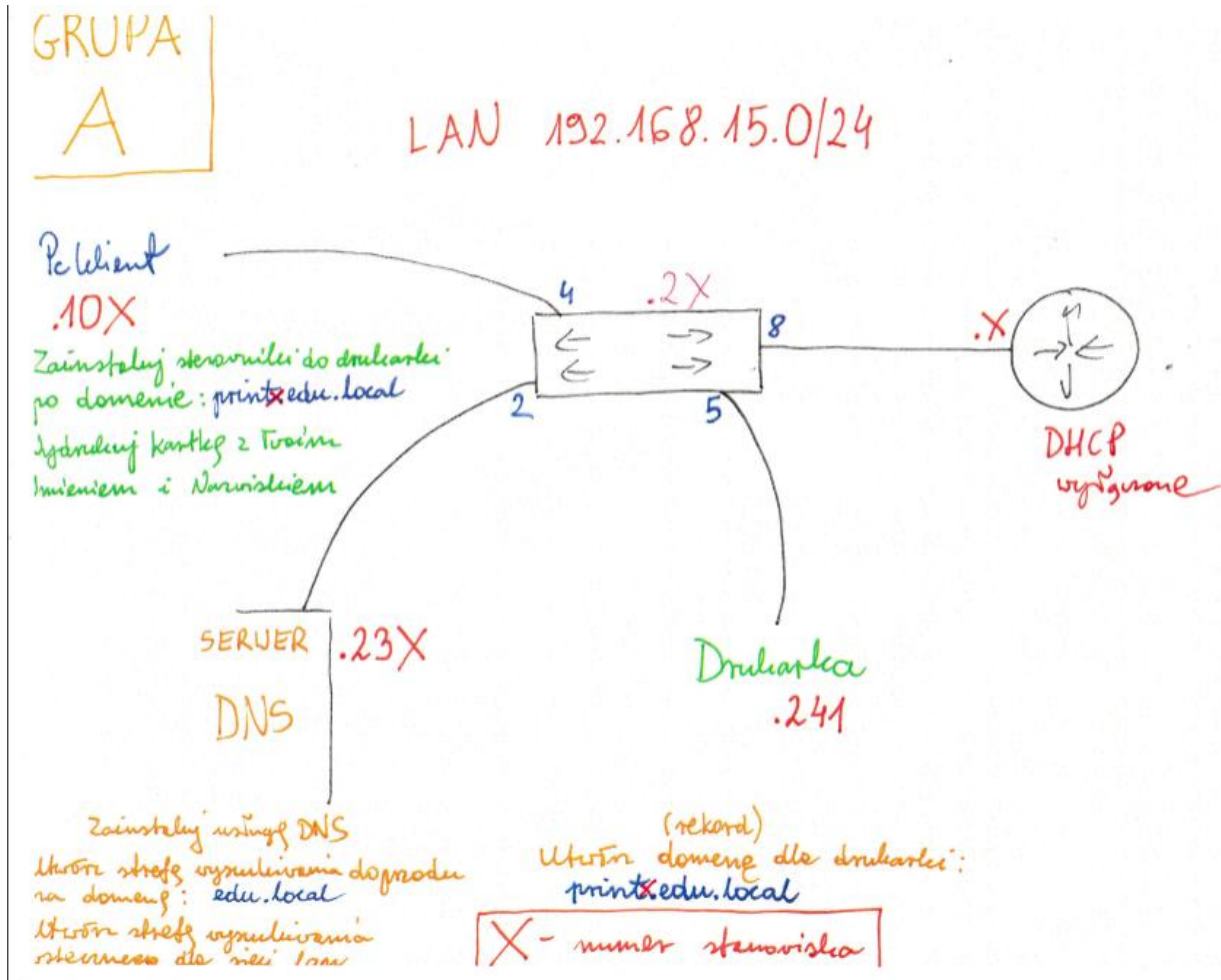
Connect Time

0:32

Delete VPN

6. URZĄDZENIA PERYFERYJNE

6.1 Instalowanie sterowników do drukarki po domenie w sieci LAN



Ustawienia na routerze

Na routerze ustaw LAN routera i wyłącz DHCP

DHCP Settings

DHCP Server:	☒ Disable ☐ Enable
Start IP Address:	192.168.15.100
End IP Address:	192.168.15.199
Address Lease Time:	120 minutes (1~2880 minutes, tr
Default Gateway:	192.168.15.9 (Optional)
Default Domain:	(Optional)
Primary DNS:	0.0.0.0 (Optional)
Secondary DNS:	0.0.0.0 (Optional)

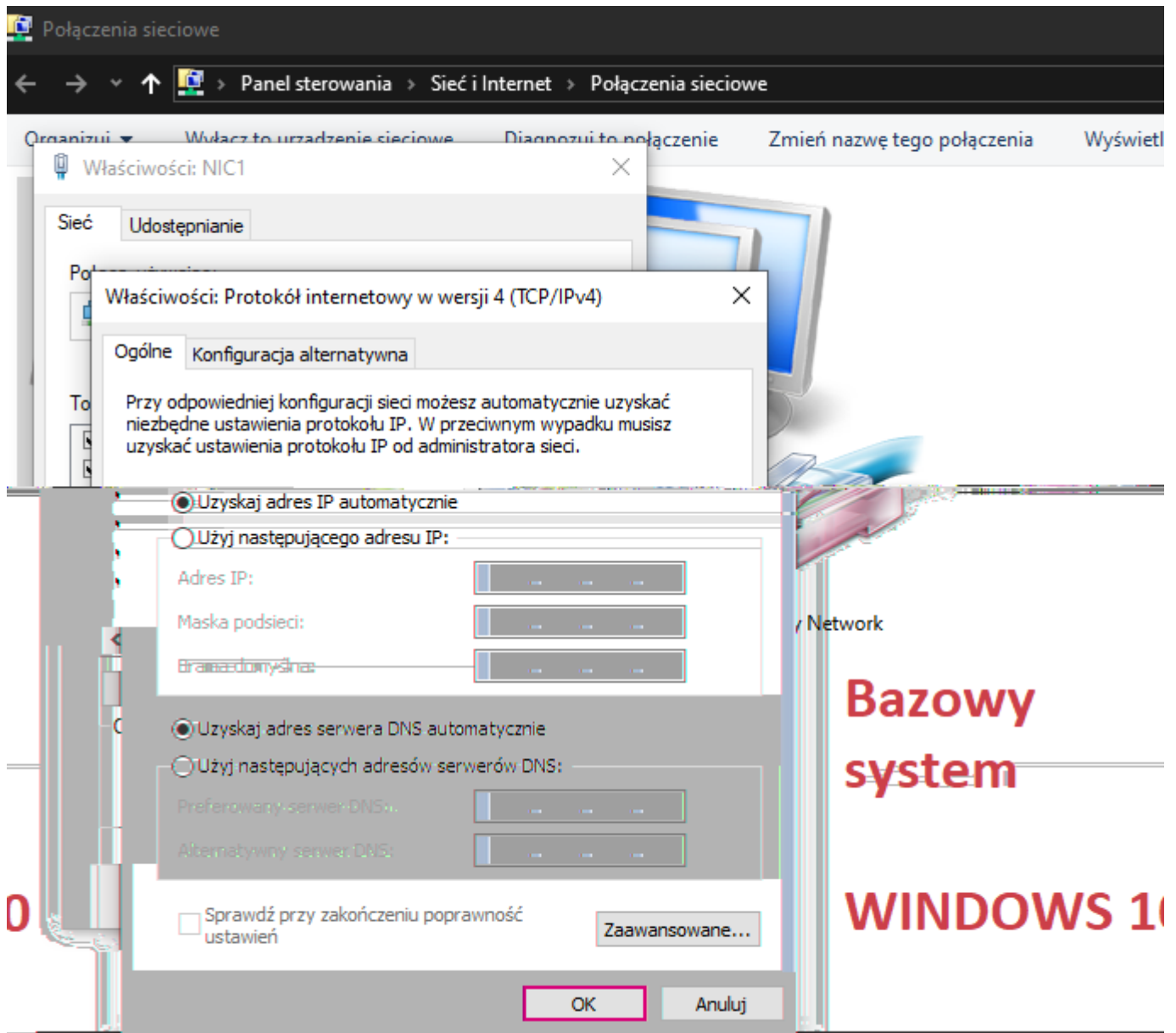
Save

Przygotowanie Virtual Box

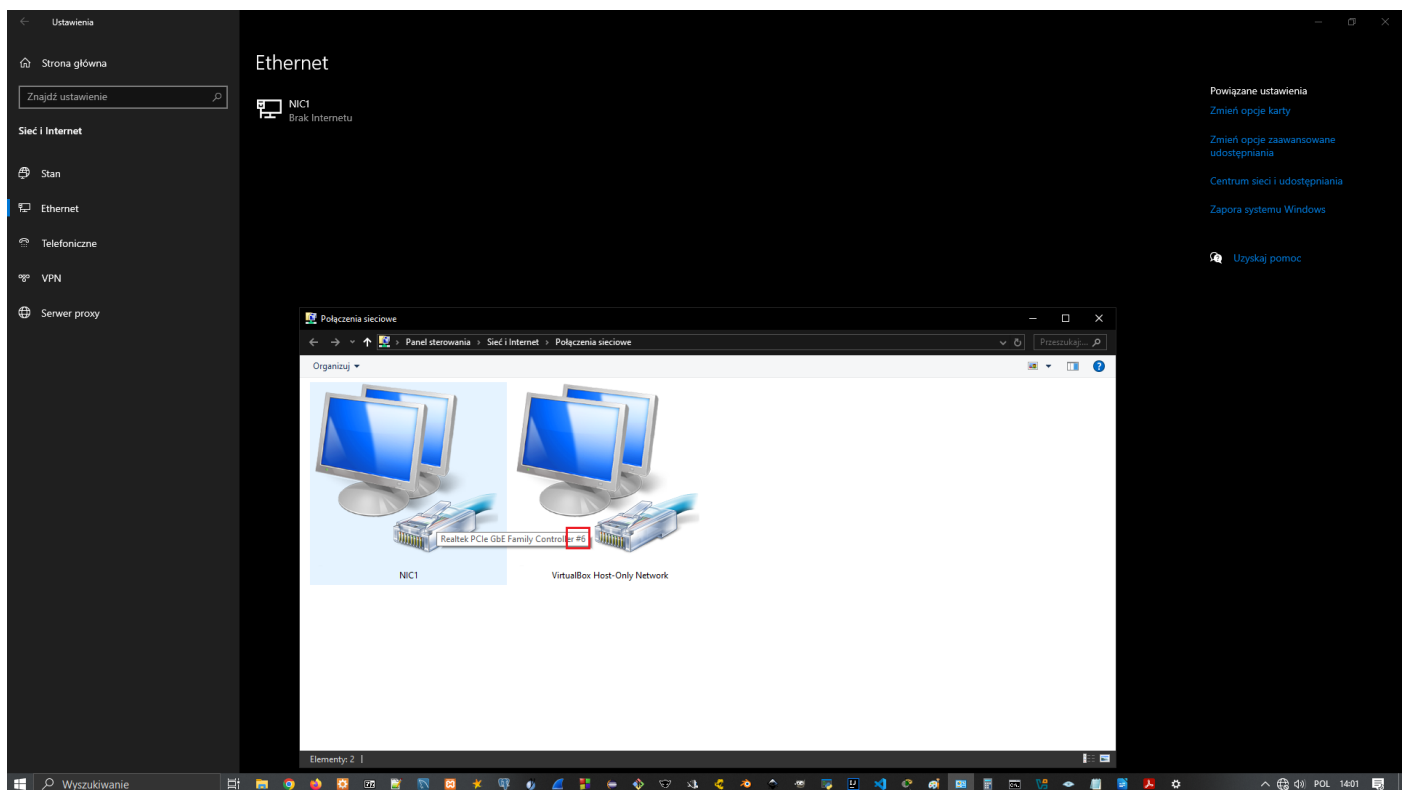
Na bazowym systemie WINDOWS 10 ustaw nazwę używanej karty sieciowej NIC1.

Druga karta sieciowa ma być wyłączona.

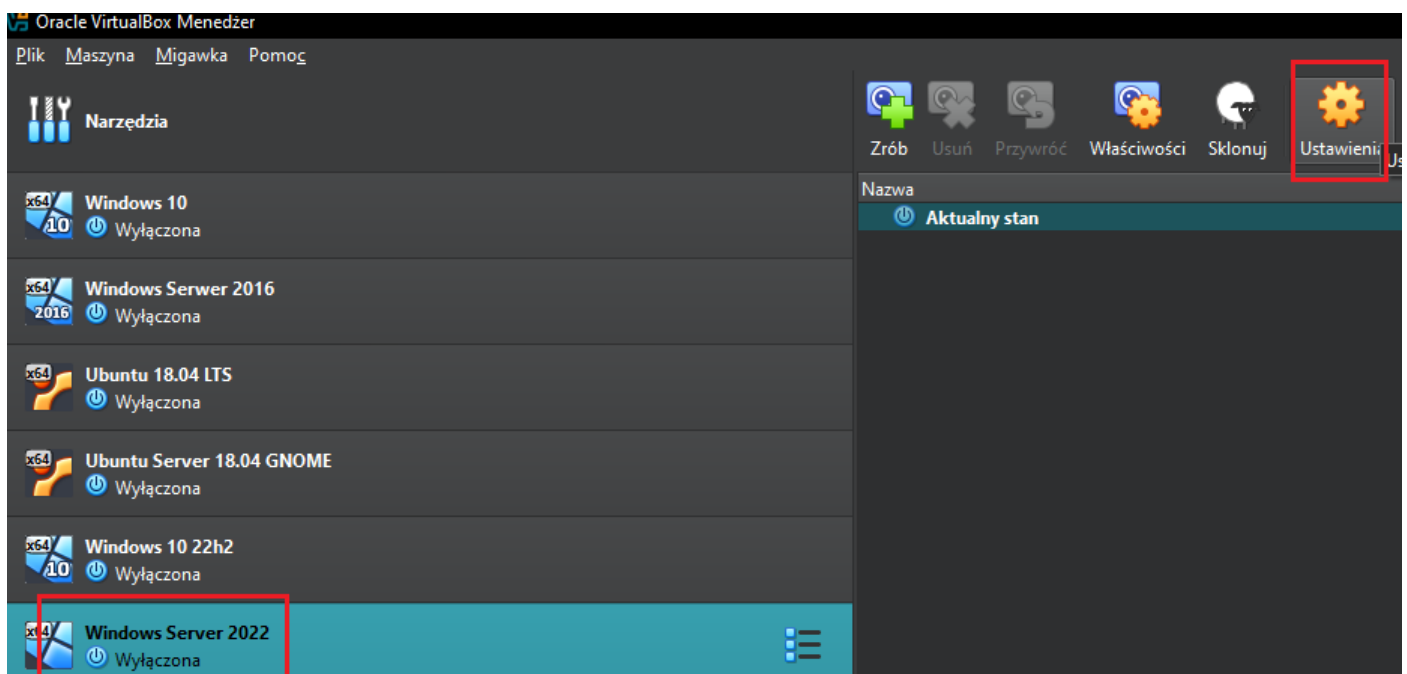
NIC1 ma pozyskiwać IPv4 automatycznie.

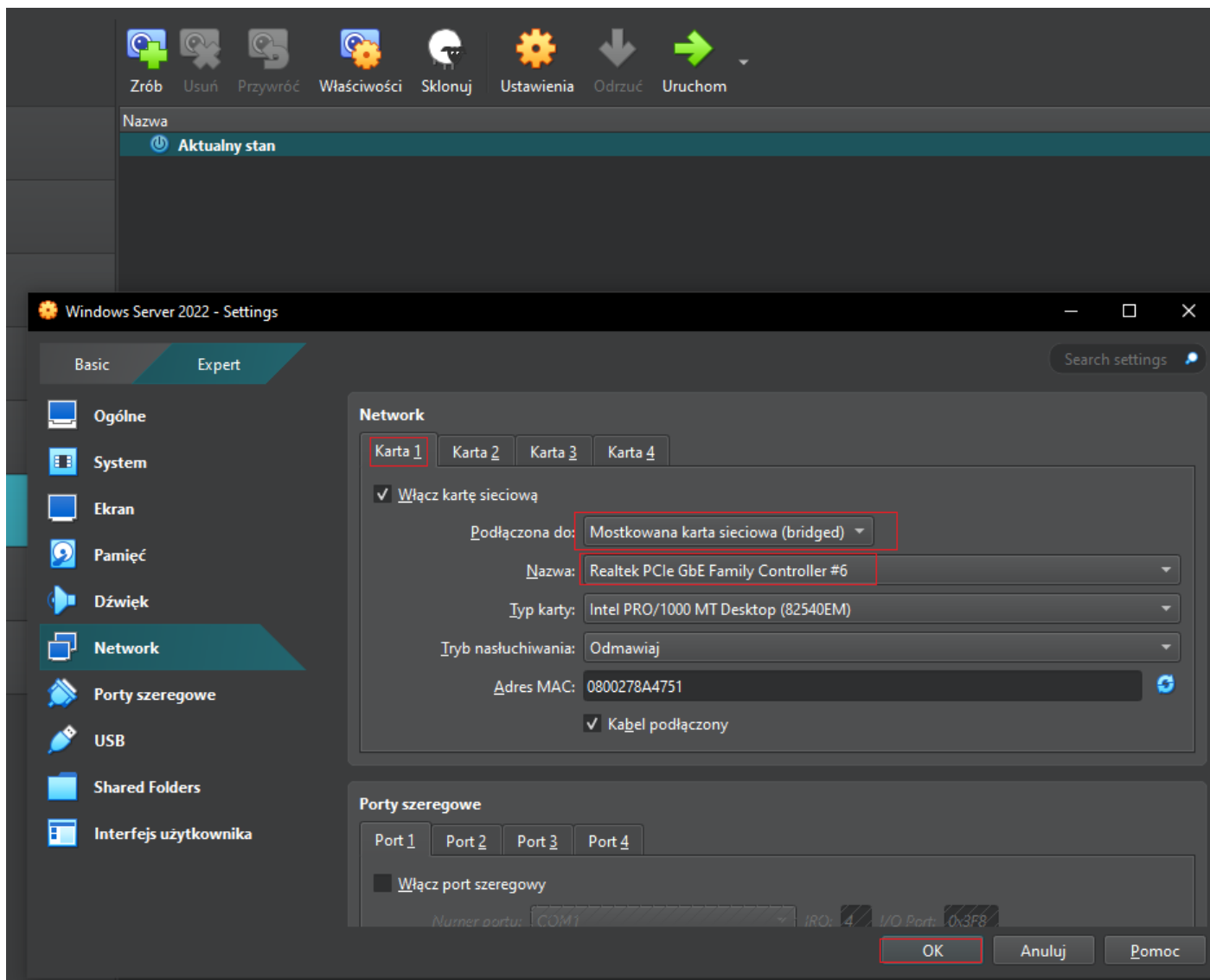


Sprawdź # karty sieciowej najeżdżając kursorem myszy na interfejs sieciowy NIC1

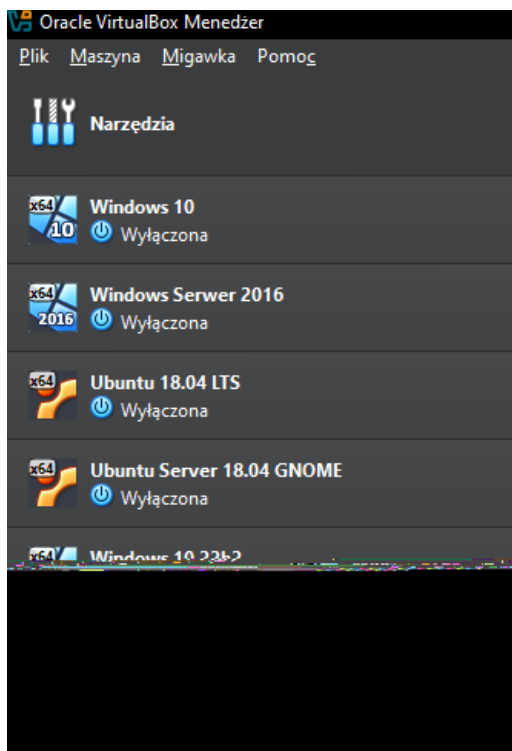


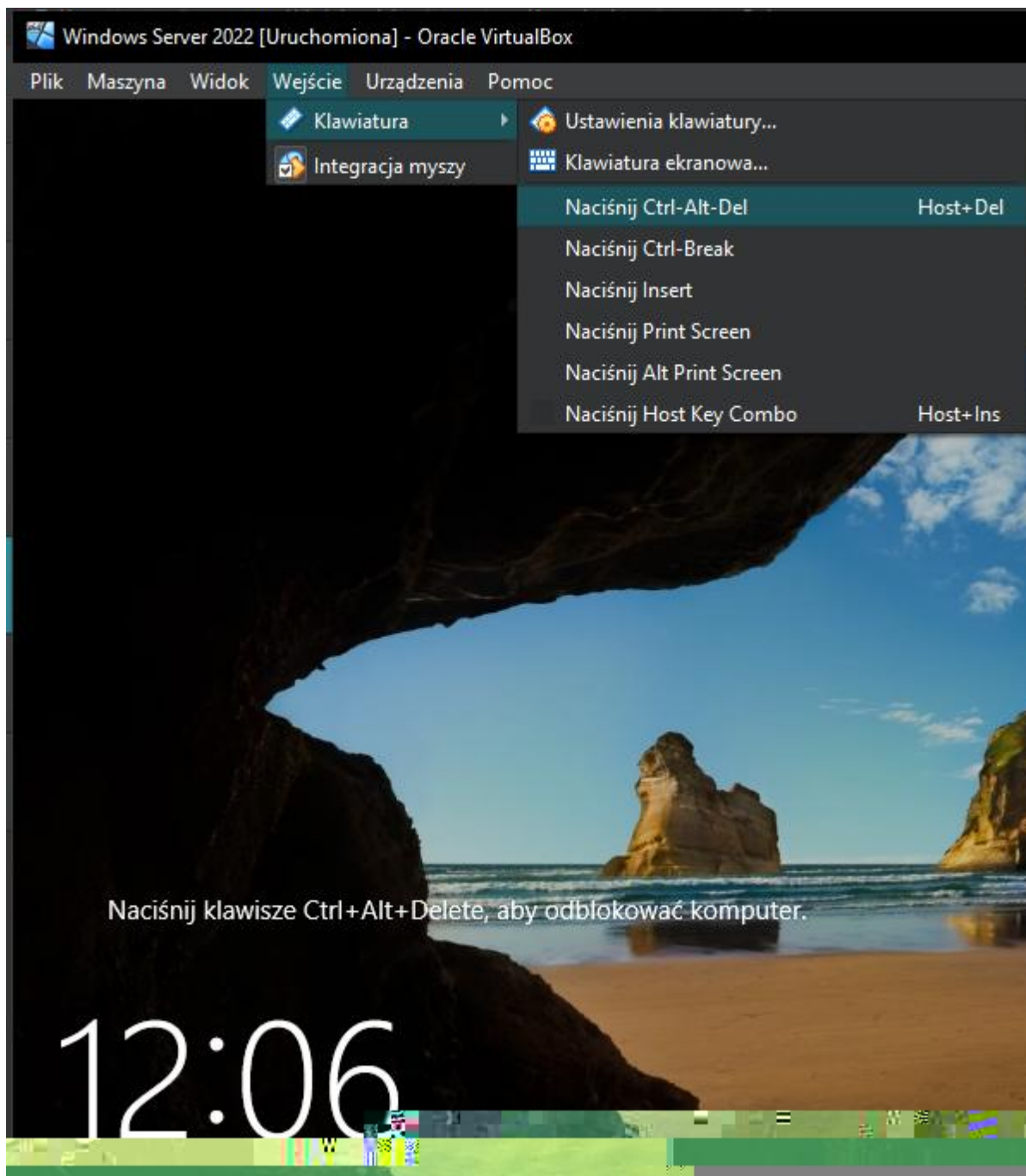
Uruchom Oracle Virtual Box i dokonaj mostkowania karty sieciowej na interfejs sieciowy sytemu bazowego WINDOWS 10.





Uruchom SERWER WINDOWS 2022





Wyłącz na SERWERZE WINDOWS 2022 i PCKliencie zapory sieciowe

Strona główna Panelu sterowania

Zezwalaj aplikacji lub funkcji na dostęp przez Zaporę Windows Defender

- Zmień ustawienia powiadomień
- Włącz lub wyłącz Zaporę Windows Defender
- Przywróć domyślne
- Ustawienia zaawansowane
- Rozwiązywanie problemów z siecią

Chroń swój komputer za pomocą Zapory Windows Defender

Zapora Windows Defender utrudnia hakerom lub złośliwemu oprogramowaniu uzyskanie dostępu do tego komputera za pośrednictwem Internetu lub sieci.

Aktualizuj ustawienia zapory

Zapora Windows Defender nie używa zalecanych ustawień w celu ochrony komputera.

[Jakie są zalecane ustawienia?](#)

[Użyj ustawień zalecanych](#)

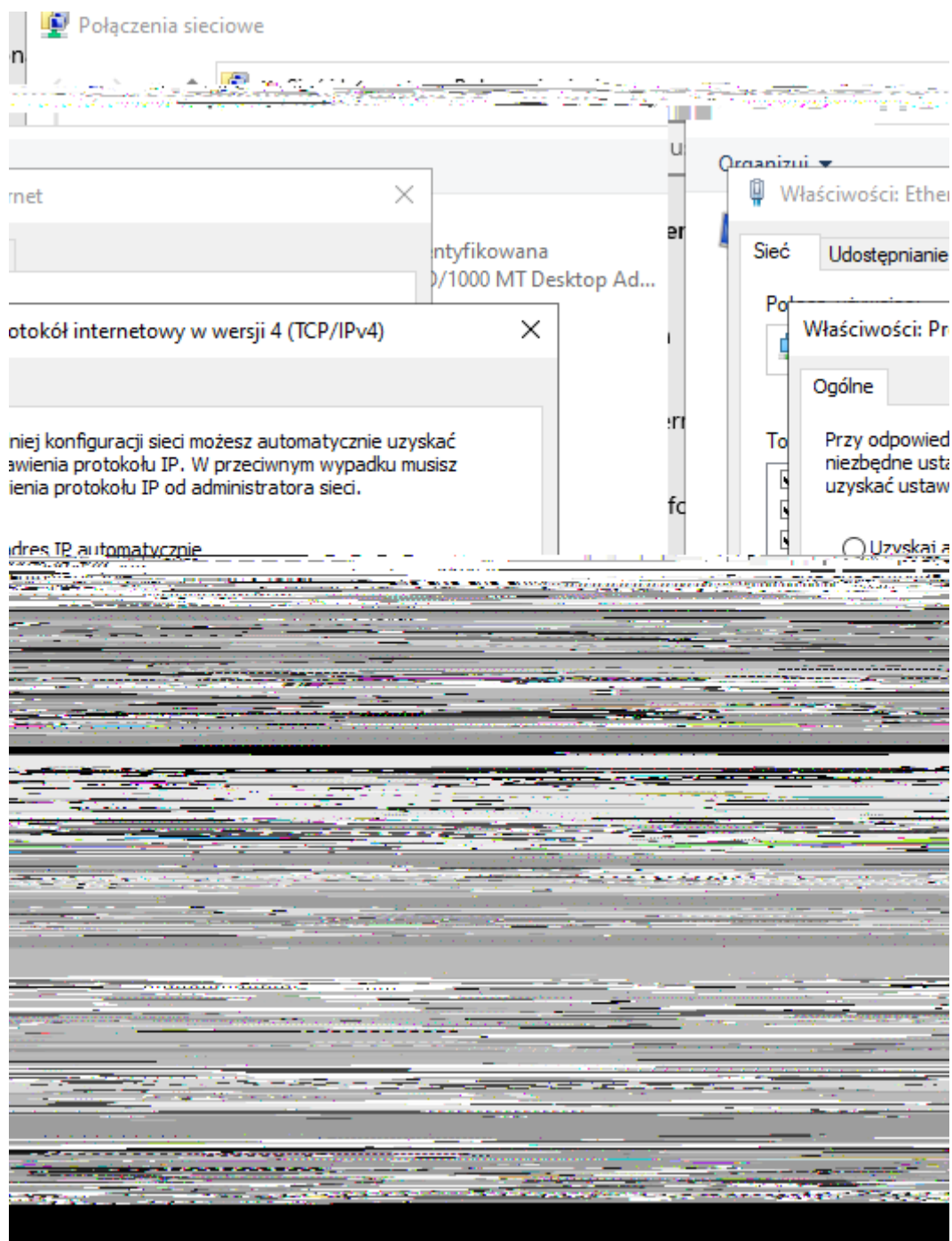
Sieci prywatne Brak połączenia

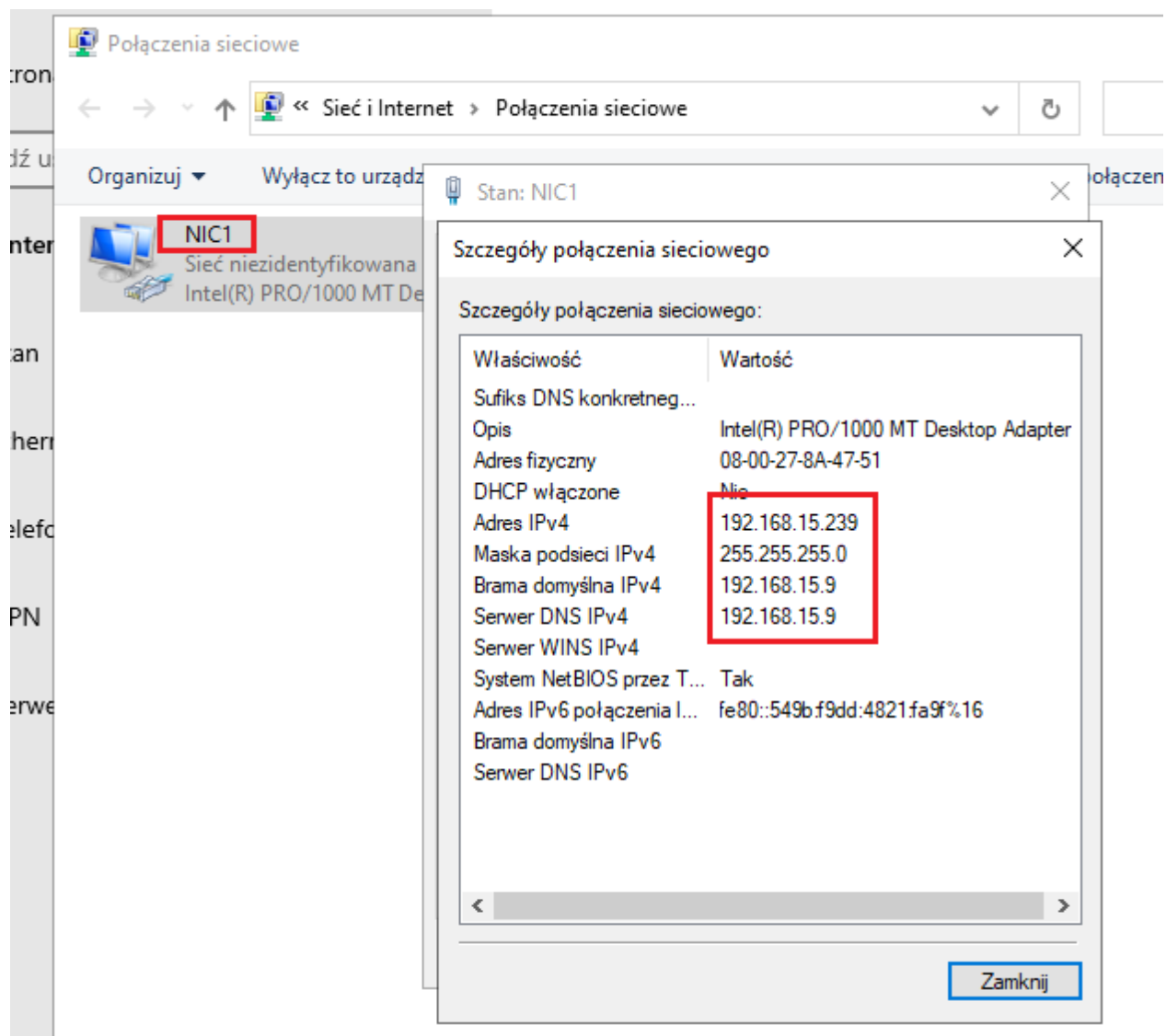
Sieci publiczne Połączono

Sieci w miejscach publicznych, takich jak porty lotnicze czy kawiarnie

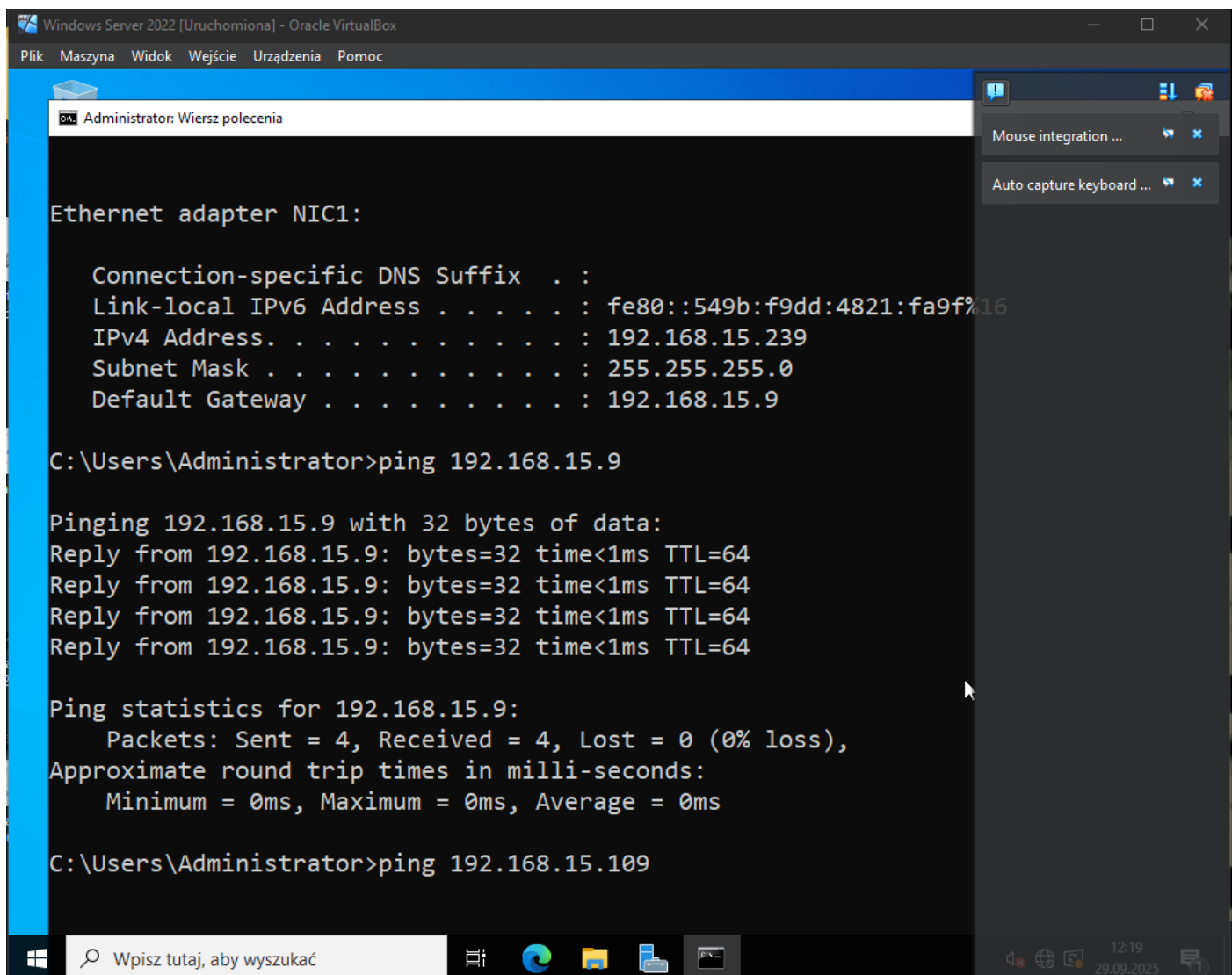
Stan Zapory Windows Defender:	Wył.
Połączenia przychodzące:	Blokuj wszystkie połączenia z aplikacjami, których nie ma na liście dozwolonych aplikacji
Aktywne sieci publiczne:	Sieć 11
Stan powiadamiania:	Powiadamiam mnie, gdy Zapora Windows Defender zablokuje nową aplikację

Opisz karty na SERWERZE WINDOWS 2022





Sprawdź połączenie SERWER WINDOWS –a 2022 z PCKlientem



```
Administrator: Wiersz poleceń

Ethernet adapter NIC1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::549b:f9dd:4821:fa9f%16
    IPv4 Address. . . . . : 192.168.15.239
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.15.9

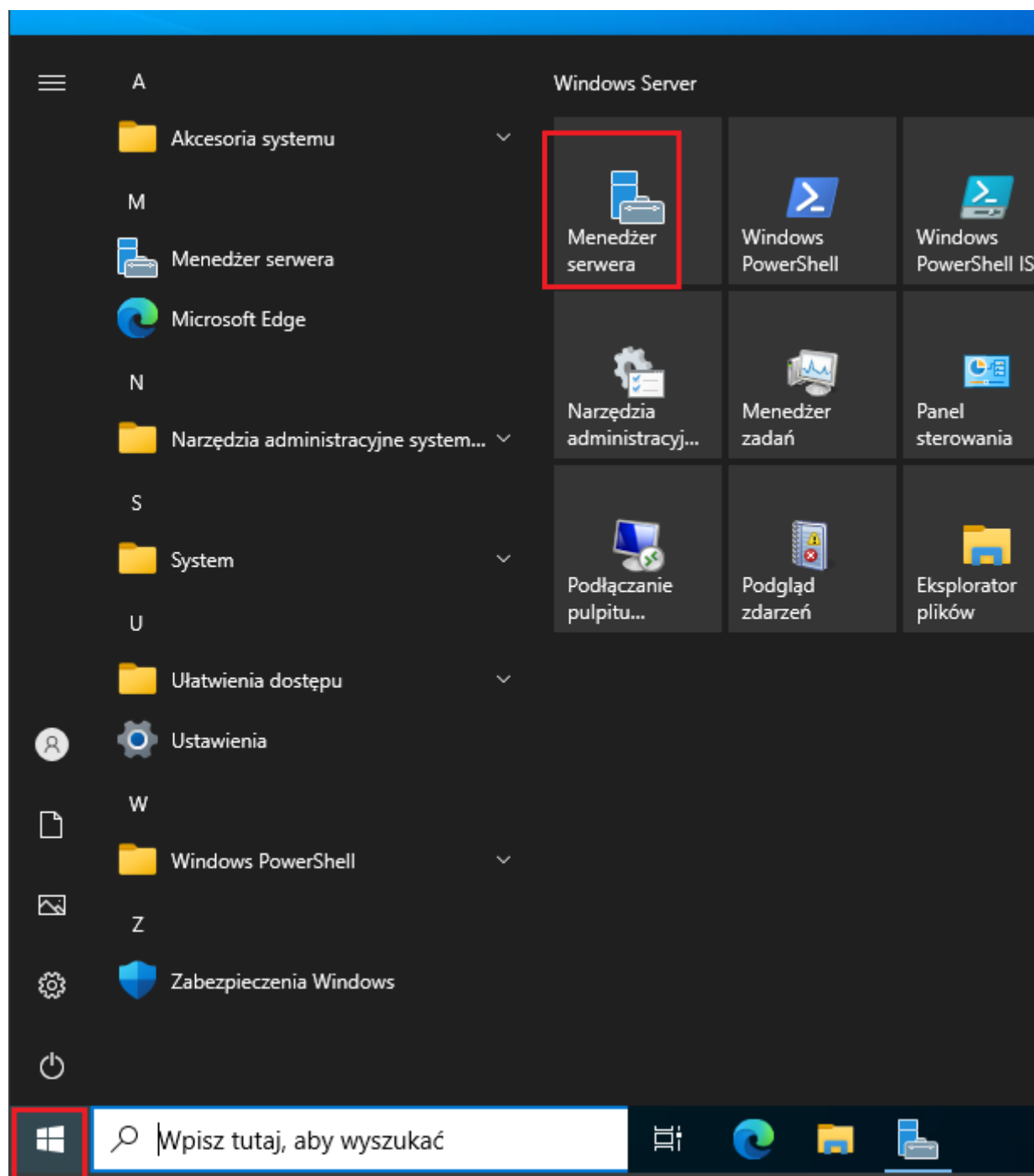
C:\Users\Administrator>ping 192.168.15.9

Pinging 192.168.15.9 with 32 bytes of data:
Reply from 192.168.15.9: bytes=32 time<1ms TTL=64
Reply from 192.168.15.9: bytes=32 time<1ms TTL=64
Reply from 192.168.15.9: bytes=32 time<1ms TTL=64
Reply from 192.168.15.9: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.15.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping 192.168.15.109
```


Instalacja i konfiguracja usługi DNS na SERWERZE WINDOWS 2022





Pulpit nawigacyjny

Serwer lokalny

Wszystkie serwery

Usługi plików i magazyny... ▸

MENEDŻER SERWERA — ZAPRASZAMY!

TART

TEGO

Z SIĘ

1

Konfiguruj ten serwer lokalny

2

Dodaj role i funkcje

3

Dodaj inne serwery do zarządzania

4

Utwórz grupę serwerów

5

Połącz ten serwer z usługami w chmurze

Ukryj

ROLE I GRUPY SERWERÓW

Role: 1 | Grupy serwerów: 1 | Łączna liczba serwerów: 1

← → ▾ « Pulpit nawigacyjny ▾ ⓘ | 🚩 Zarządzaj Narzędzia Widok Pomoc

MENEDŻER SERWERA — ZAPRASZAMY!

1 Konfiguruj ten serwer lokalny

2 Dodaj role i funkcje

3 Dodaj inne serwery do zarządzania

4 Utwórz grupę serwerów

5 Połącz ten serwer z usługami w chmurze

ROLE I GRUPY SERWERÓW
Role: 1 | Grupy serwerów: 1 | łączna liczba serwerów: 1

Pulpit nawigacyjny

- Server lokalny
- Wszystkie serwery
- Usługi plików i magazyny...

SZYBKI START

CO NOWEGO

DOWIEDZ SIĘ WIĘCEJ

Kreator dodawania ról i funkcji

Zanim rozpoczniesz

SERWER DOCELOWY
WIN-ADLL63PI067

Ten kreator pomaga zainstalować role, usługi ról lub funkcje. Użytkownik określa role, usługi ról lub funkcje do zainstalowania w zależności od potrzeb organizacji w zakresie przetwarzania danych, takich jak udostępnianie dokumentów lub hostowanie witryny sieci Web.

Aby usunąć role, usługi ról lub funkcje:
[Uruchom Kreatora usuwania ról i funkcji](#)

Przed kontynuowaniem sprawdź, czy ukończono wykonywanie następujących zadań:

- Konto administratora ma silne hasło
- Ustawienia sieciowe (np. statyczny adres IP) są skonfigurowane
- Zainstalowane są najnowsze aktualizacje zabezpieczeń z witryny Windows Update

Jeśli musisz sprawdzić, czy dowolne z poprzednich wymagań wstępnych zostało spełnione, zamknij

kontynuować, kliknij przycisk Dalej.

Zanim rozpoczniesz

- Typ instalacji
- Wybieranie serwera
- Role serwera
- Funkcje
- Potwierdzenie
- Wyniki

< Wstecz **Dalej >** Zainstaluj Anuluj

Wybieranie typu instalacji

SERWER DOCELOWY
WIN-ADLL63PI067

Zanim rozpoczniesz

Typ instalacji

Wybieranie serwera

Role serwera

Funkcje

Potwierdzenie

Wyniki

Wybierz typ instalacji. Role i funkcje mogą zostać zainstalowane na działającym komputerze fizycznym, na maszynie wirtualnej lub na wirtualnym dysku twardym (VHD) w trybie offline.

☒ Instalacja oparta na rolach lub oparta na funkcjach

Skonfiguruj pojedynczy serwer, dodając do niego role, usługi ról i funkcje.

☐ Instalacja usług pulpitu zdalnego

Zainstaluj wymagane usługi roli Infrastruktura pulpitu wirtualnego, aby utworzyć wdrożenie pulpitów oparte na maszynach wirtualnych lub sesjach.

< Wstecz

Dalej >

Zainstaluj

Anuluj

Wybieranie serwera docelowego

SERWER DOCELOWY
WIN-ADLL63PI067

Zanim rozpoczniesz

Typ instalacji

Wybieranie serwera

Role serwera

Funkcje

Potwierdzenie

Wyniki

Wybierz serwer lub wirtualny dysk twardy, na którym mają zostać zainstalowane role i funkcje.

☒ Wybierz serwer z puli serwerów☐ Wybierz wirtualny dysk twardy

Pula serwerów

Filtr:		
Nazwa	Adres IP	System operacyjny
WIN-ADLL63PI067	192.168.15.239	Microsoft Windows Server 2022 Standard

Liczba znalezionych komputerów: 1

Na tej stronie są wyświetlane serwery z systemem Windows Server 2012 lub nowszą wersją systemu Windows Server, które zostały dodane przy użyciu polecenia Dodaj serwery w Menedżerze serwera. Obiekty wirtualne klastra, serwery w trybie offline i nowo dodane serwery, dla których zbieranie danych nie zostało jeszcze ukończonych, nie są wyświetlane.

< Wstecz

Dalej >

Zainstaluj

Anuluj

Wybieranie ról serwera

SERWER DOCELOWY
WIN-ADLL63PI067

Zanim rozpocznesz

Typ instalacji

Wybieranie serwera

Role serwera

Funkcje

Potwierdzenie

Wyniki

Wybierz jedną lub więcej ról do zainstalowania na wybranym serwerze.

Role	Opis
☐ Dostęp zdalny	
☐ Hyper-V	
☐ Serwer DHCP	
☒ Serwer DNS	Serwer DNS (Domain Name System) umożliwia rozpoznawanie nazw w sieciach TCP/IP. Zarządzanie serwerem DNS będzie łatwiejsze, jeśli zostanie zainstalowany na tym samym serwerze co Usługi domenowe Active Directory. W przypadku wybrania roli Usługi domenowe Active Directory można zainstalować i skonfigurować serwer DNS i Usługi domenowe Active Directory w taki sposób, aby współpracowały ze sobą.
☐ Serwer faksów	
☐ Serwer sieci Web (IIS)	
☐ Usługa Ochrona hosta	
☐ Usługi aktywacji zbiorczej	
☐ Usługi certyfikatów Active Directory	
☐ Usługi domenowe Active Directory	
☐ Usługi drukowania i zarządzania dokumentami	
☐ Usługi federacyjne Active Directory (AD FS)	
☐ Usługi LDS w usłudze Active Directory	
☒ Usługi plików i magazynowania (Zainstalowano 1 z 2)	
☐ Usługi pulpitu zdalnego	
☐ Usługi zarządzania prawami dostępu w usłudze Active Directory	
☐ Usługi zasad sieciowych i dostępu sieciowego	
☐ Windows Deployment Services	
☐ Windows Server Update Services	

< Wstecz Dalej > Zainstaluj Anuluj

Kreator dodawania ról i funkcji

Wybieranie ról serwera

Zanim rozpocznesz

Typ instalacji

Wybieranie serwera

Role serwera

Funkcje

Potwierdzenie

Wyniki

Kreator dodawania ról i funkcji

Czy dodać funkcje wymagane przez funkcję Serwer DNS?

Do zarządzania tą funkcją są potrzebne poniżej wymienione narzędzia, które nie są zainstalowane na tym samym serwerze.

- Narzędzia administracji zdalnej serwera
 - Narzędzia do administrowania rolami
 - [Narzędzia] Narzędzia serwera DNS

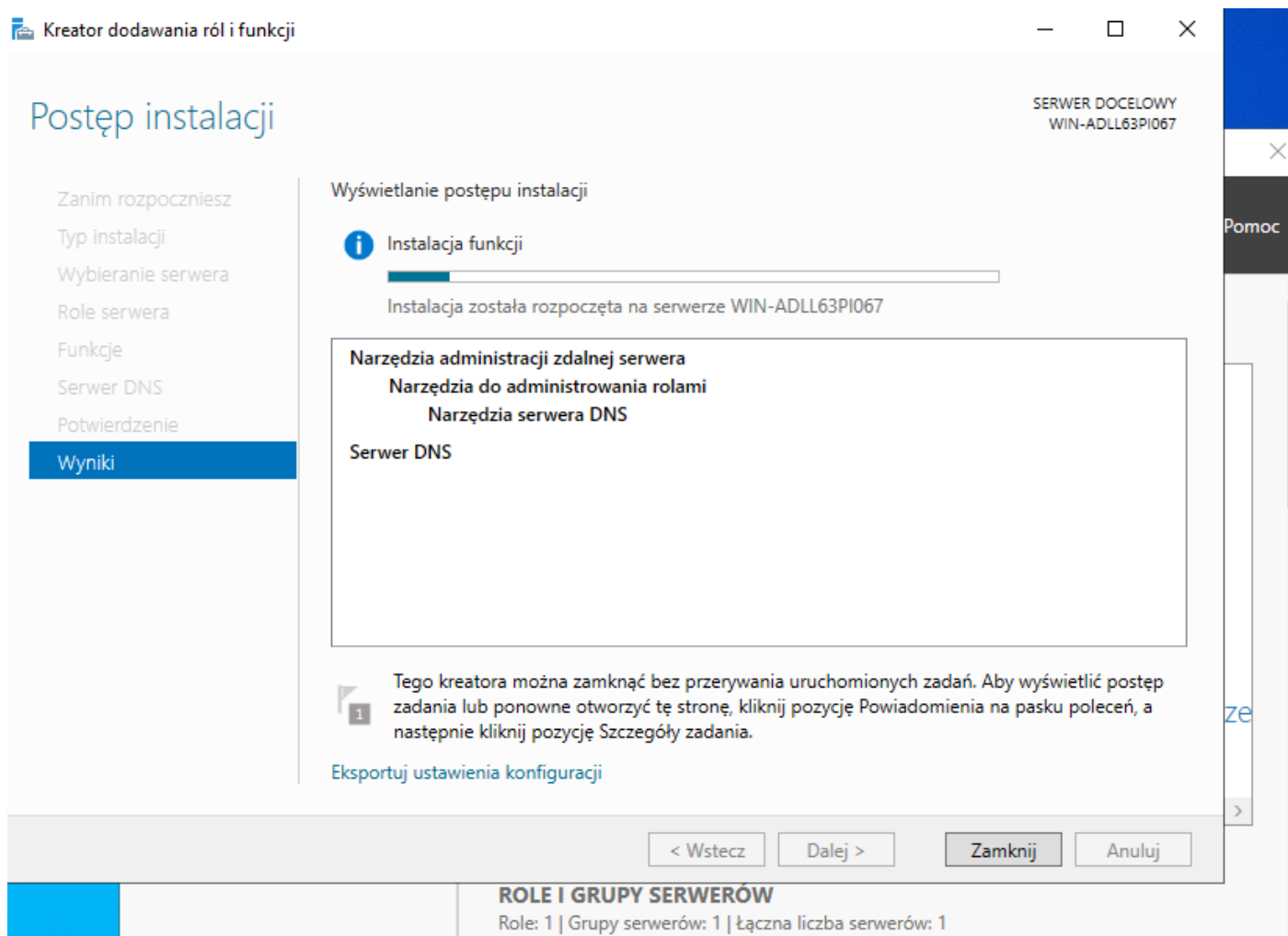
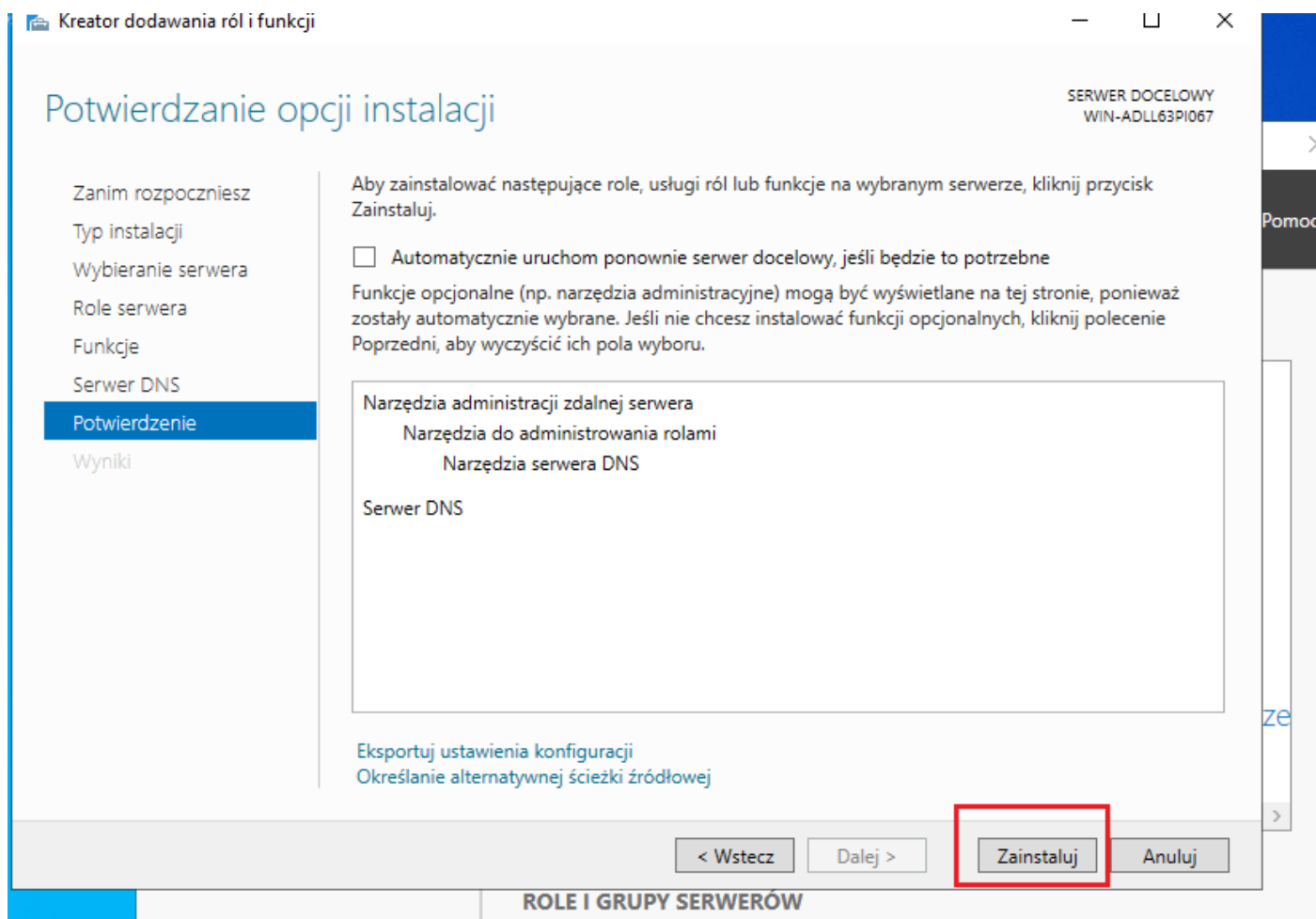
☒ Dołącz narzędzia do zarządzania (jeśli dotyczy)

Dodaj funkcje Anuluj

< Wstecz Dalej > Zainstaluj

ROLE I GRUPY SERWERÓW

Role: 1 | Grupy serwerów: 1 | łączna liczba serwerów: 1



Postęp instalacji

SERWER DOCELOWY
WIN-ADLL63PI067

Zanim rozpocznesz

Typ instalacji

Wybieranie serwera

Role serwera

Funkcje

Serwer DNS

Potwierdzenie

Wyniki

Wyświetlanie postępu instalacji

 Instalacja funkcji

Instalacja na serwerze WIN-ADLL63PI067 powiodła się.

Narzędzia administracji zdalnej serwera

Narzędzia do administrowania rolami

Narzędzia serwera DNS

Serwer DNS



Tego kreatora można zamknąć bez przerywania uruchomionych zadań. Aby wyświetlić postęp zadania lub ponownie otworzyć tę stronę, kliknij pozycję Powiadomienia na pasku poleceń, a następnie kliknij pozycję Szczegóły zadania.

Eksportuj ustawienia konfiguracji

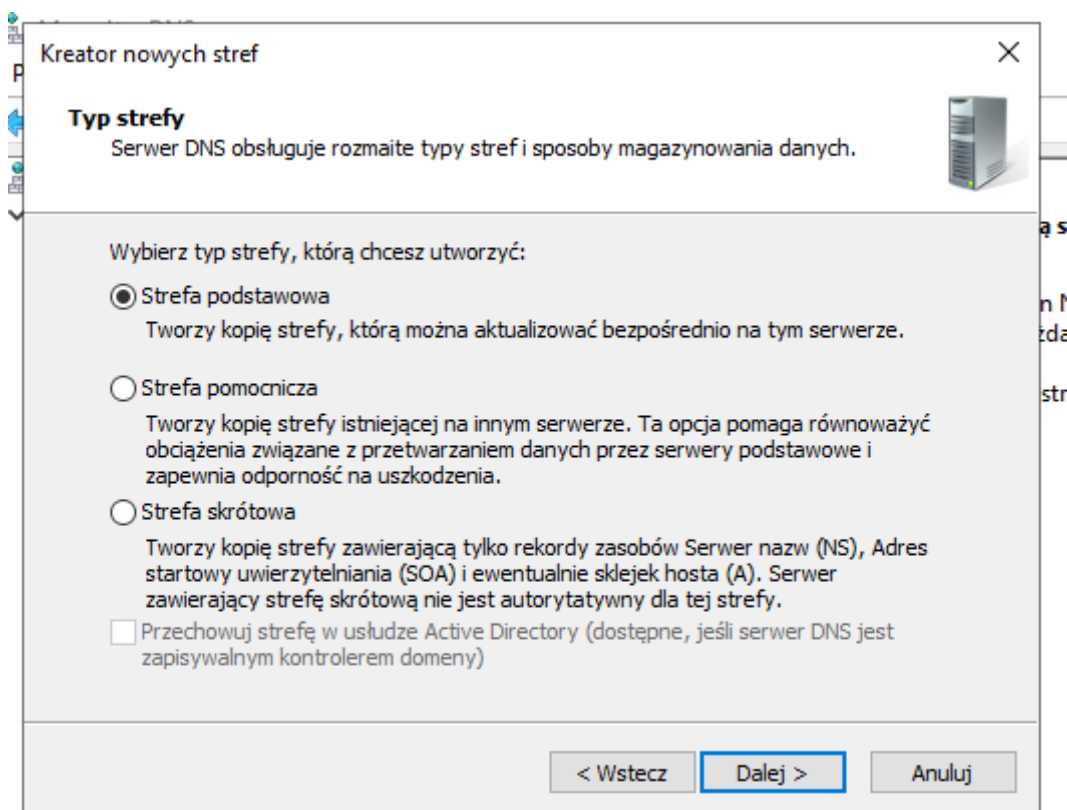
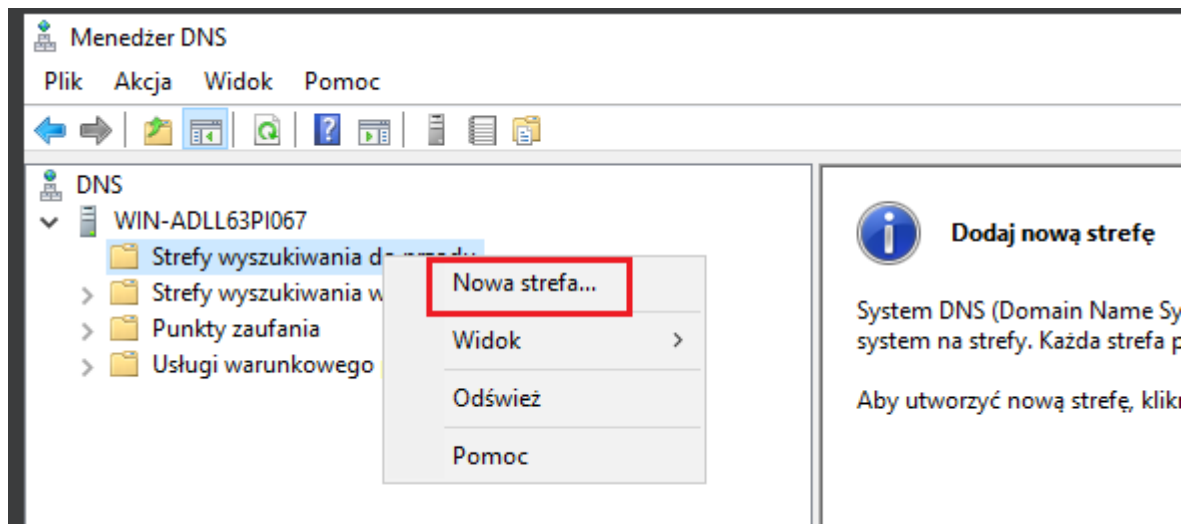
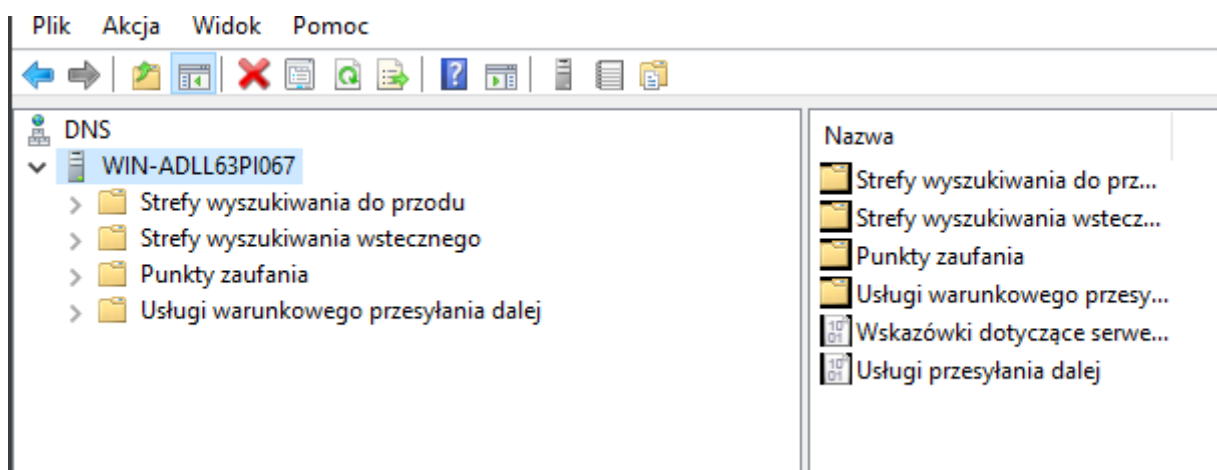
< Wstecz

Dalej >

Zamknij

Anuluj

ROLE I GRUPY SERWERÓW



Kreator nowych stref

Nazwa strefy
Jaka jest nazwa nowej strefy?

Nazwa strefy określa część obszaru nazw DNS, dla którego ten serwer jest autorytatywny. Może to być nazwa domeny organizacji (np. microsoft.com) lub część nazwy domeny (np. nowastrefa.microsoft.com). Nazwa strefy nie jest nazwą serwera DNS.

Nazwa strefy:
edu.local

< Wstecz Dalej > Anuluj

Kreator nowych stref

Plik strefy
Możesz utworzyć nowy plik strefy lub użyć pliku skopiowanego z innego serwera DNS.

Czy chcesz utworzyć nowy plik strefy czy też użyć istniejącego pliku skopiowanego z innego serwera DNS?

☒ Utwórz nowy plik o tej nazwie:
edu.local.dns

☐ Użyj istniejącego pliku:

Aby użyć tego istniejącego pliku, upewnij się, że został on skopiowany do folderu %SystemRoot%\system32\dns na tym serwerze, a następnie kliknij przycisk Dalej.

< Wstecz Dalej > Anuluj

Menedżer DNS

Plik Akcja Widok Pomoc

DNS

- WIN-ADLL63PI067
 - Strefy wyszukiwania do przodu
 - edu.local
 - Strefy wyszukiwania wstecznego
 - Punkty zaufania
 - Usługi warunkowego przesyłania dalej

Nazwa	Typ	Dane
(identyczny jak folder nadrz...	Adres startowy uwierzyt...	[1], win-adll63pi067., host...
(identyczny jak folder nadrz...	Serwer nazw (NS)	win-adll63pi067.



Kreator nowych stref

Aktualizacja dynamiczna

Można określić, że ta strefa DNS akceptuje dynamiczne aktualizacje zabezpieczone lub niezabezpieczone albo nie akceptuje dynamicznych aktualizacji.

Aktualizacje dynamiczne pozwalają komputerom klienckim usługi DNS na rejestrowanie i dynamiczne aktualizowanie ich rekordów zasobów przy użyciu serwera DNS za każdym razem, kiedy nastąpią jakieś zmiany.

Wybierz typ aktualizacji dynamicznych, na które chcesz zezwalać:

- ☐ Zezwalaj tylko na zabezpieczone aktualizacje dynamiczne (zalecane dla Active Directory)
Ta opcja jest dostępna tylko dla stref zintegrowanych z usługą Active Directory.
- ☐ Zezwalaj na zabezpieczone oraz niezabezpieczone aktualizacje dynamiczne
Aktualizacje dynamiczne rekordów zasobów są akceptowane od dowolnego klienta.
 Ta opcja stanowi poważne zagrożenie zabezpieczeń, ponieważ aktualizacje mogą być akceptowane z niezaufanych źródeł.
- ☒ Nie zezwalaj na aktualizacje dynamiczne
Aktualizacje dynamiczne rekordów zasobów nie są akceptowane przez tę strefę. Musisz ręcznie zaktualizować te rekordy.

< Wstecz Dalej > Anuluj

Nazwa	Typ	Dane
(identyczny jak folder nadrz...	Adres startowy uwierzyt...	[1], win-adll63pi067., h
(identyczny jak folder nadrz...	Serwer nazw (NS)	win-adll63pi067.

Właściwości: edu.local ? X

Ogólne	Adres startowy uwierzytelniania (SOA)	
Serwery nazw	WINS	Transfery stref

Aby dodać serwery nazw do poniższej listy, kliknij przycisk Dodaj.

W pełni kwalifikowana nazwa domeny (FQDN)...	Adres IP
win-adll63pi067.	Nieznane

* odpowiada adresowi IP pobranemu jako wynik zapytania DNS i może nie odpowiadać rzeczywistym rekordom przechowywanym na tym serwerze.

Nazwa	Typ	Dane
 (identyczny jak folder nadrz...	Adres startowy uwierzyt...	[1], win-adll63pi067., host...
 (identyczny jak folder nadrz...	Serwer nazw (NS)	win-adll63pi067.

Właściwości: edu.local

?

×

Edytuj rekord serwera nazw

×

Wprowadź nazwę serwera i co najmniej jeden adres IP. Obie te wartości są potrzebne do zidentyfikowania serwera nazw.

W pełni kwalifikowana nazwa domeny (FQDN) serwera:

win-adll63pi067.

Rozpoznaj

Adresy IP tego rekordu serwera nazw:

Adres IP	Sprawdzono poprawność
<Kliknij tutaj, aby dodać adres IP>	
 192.168.15.239	OK

Usuń

W górę

W dół

OK

Anuluj

OK

Anuluj

Zastosuj

Pomoc

Nazwa	Typ	Dane
(identyczny jak folder nadrz...	Adres startowy uwierzyt...	[1], win-adll63pi067., hos
(identyczny jak folder nadrz...	Serwer nazw (NS)	win-adll63pi067.

Właściwości: edu.local

Ogólne Adres startowy uwierzytelniania (SOA)

Serwery nazw WINS Transfery stref

Aby dodać serwery nazw do poniższej listy, kliknij przycisk Dodaj.

W pełni kwalifikowana nazwa domeny (FQDN)...	Adres IP
win-adll63pi067.	[192.168.15.239]

Dodaj... Edytuj... Usuń

* odpowiada adresowi IP pobranemu jako wynik zapytania DNS i może nie odpowiadać rzeczywistym rekordom przechowywanym na tym serwerze.

OK Anuluj Zastosuj Pomoc

Menedżer DNS

Plik Akcja Widok Pomoc

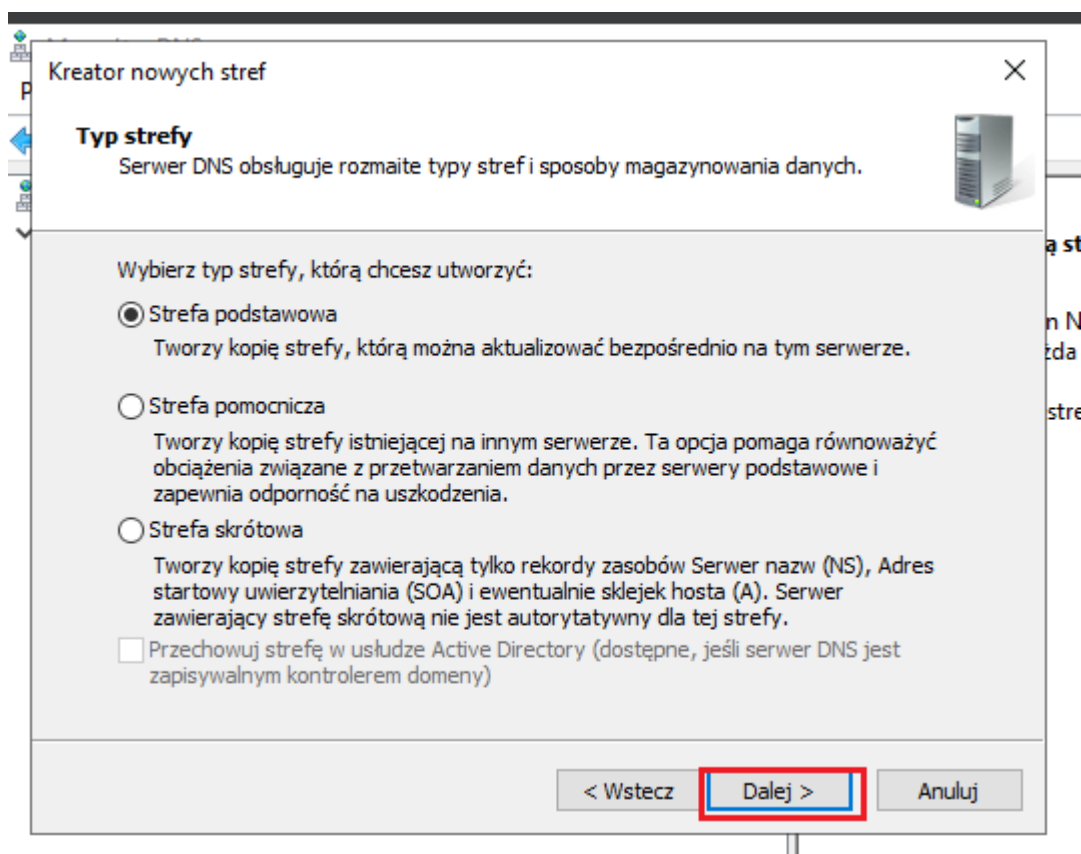
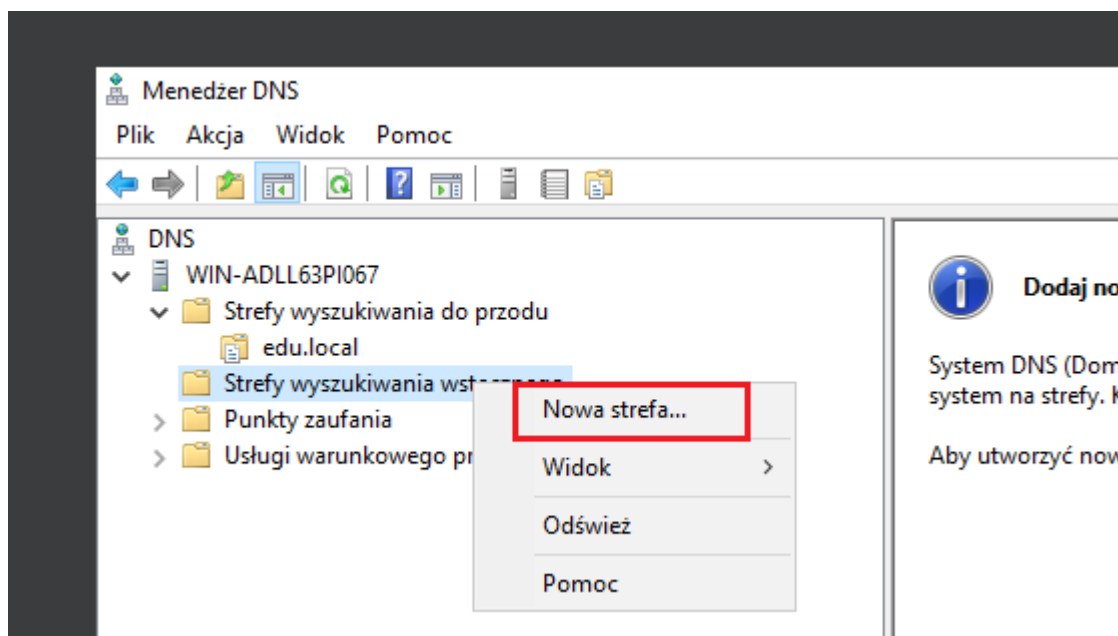
DNS

- WIN-ADLL63PI067
 - Strefy wyszukiwania do przodu
 - edu.local
 - Strefy wyszukiwania wstecznego**
 - Punkty zaufania
 - Usługi warunkowego przesyłania dalej

Dodaj nową strefę

System DNS (Domain Name System) używa stref. Każda strefa zawiera informacje o komputerach i usługach w sieci.

Aby utworzyć nową strefę, kliknij przycisk Dodaj nową strefę.



Kreator nowych stref

Nazwa strefy wyszukiwania wstecznego
Strefa wyszukiwania wstecznego tłumaczy adresy IP na nazwy DNS.

Określ, czy chcesz utworzyć strefę wyszukiwania wstecznego dla adresów IPv4, czy dla adresów IPv6.

☒ Strefa wyszukiwania wstecznego IPv4

☐ Strefa wyszukiwania wstecznego IPv6

< Wstecz Dalej > Anuluj

Kreator nowych stref

Nazwa strefy wyszukiwania wstecznego
Strefa wyszukiwania wstecznego tłumaczy adresy IP na nazwy DNS.

Aby zidentyfikować strefę wyszukiwania wstecznego, wpisz identyfikator sieci lub nazwę strefy.

☒ Identyfikator sieci:

192 .168 .15

Identyfikator sieci jest częścią adresu IP należącego do tej strefy. Wprowadź identyfikator sieci w zwykłej kolejności (nieodwrócony).

Jeśli w identyfikatorze sieci zostanie użyte zero, pojawi się ono w nazwie strefy. Na przykład identyfikator sieci 10 utworzy strefę 10.in-addr.arpa, a identyfikator sieci 10.0 utworzy strefę 0.10.in-addr.arpa.

☐ Nazwa strefy wyszukiwania wstecznego:

15.168.192.in-addr.arpa

< Wstecz Dalej > Anuluj

Kreator nowych stref

Plik strefy

Możesz utworzyć nowy plik strefy lub użyć pliku skopiowanego z innego serwera DNS.

Czy chcesz utworzyć nowy plik strefy czy też użyć istniejącego pliku skopiowanego z innego serwera DNS?

☒ Utwórz nowy plik o tej nazwie:

15.168.192.in-addr.arpa.dns

☐ Użyj istniejącego pliku:

Aby użyć tego istniejącego pliku, upewnij się, że został on skopiowany do folderu %SystemRoot%\system32\dns na tym serwerze, a następnie kliknij przycisk Dalej.

< Wstecz Dalej > Anuluj

Kreator nowych stref

Aktualizacja dynamiczna

Można określić, że ta strefa DNS akceptuje dynamiczne aktualizacje zabezpieczone lub niezabezpieczone albo nie akceptuje dynamicznych aktualizacji.

Aktualizacje dynamiczne pozwalają komputerom klienckim usługi DNS na rejestrowanie i dynamiczne aktualizowanie ich rekordów zasobów przy użyciu serwera DNS za każdym razem, kiedy nastąpią jakieś zmiany.

Wybierz typ aktualizacji dynamicznych, na które chcesz zezwalać:

☐ Zezwalaj tylko na zabezpieczone aktualizacje dynamiczne (zalecane dla Active Directory)

Ta opcja jest dostępna tylko dla stref zintegrowanych z usługą Active Directory.

☐ Zezwalaj na zabezpieczone oraz niezabezpieczone aktualizacje dynamiczne

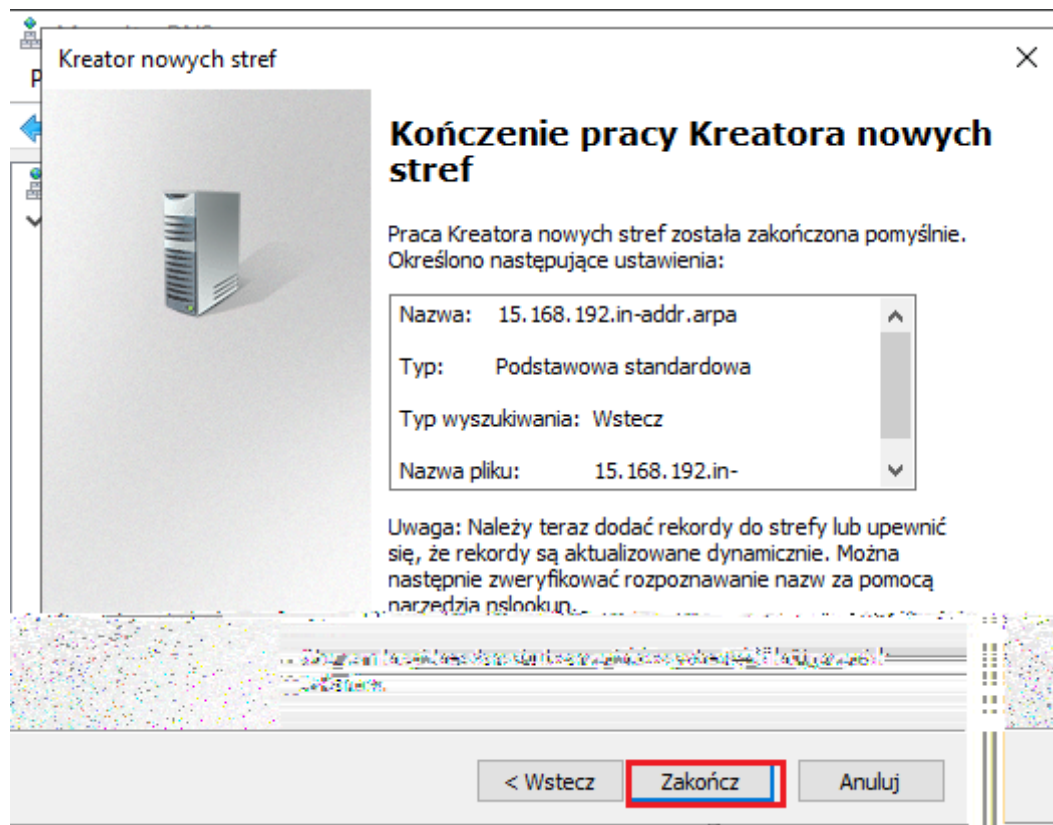
Aktualizacje dynamiczne rekordów zasobów są akceptowane od dowolnego klienta.

⚠ Ta opcja stanowi poważne zagrożenie zabezpieczeń, ponieważ aktualizacje mogą być akceptowane z niezaufanych źródeł.

☒ Nie zezwalaj na aktualizacje dynamiczne

Aktualizacje dynamiczne rekordów zasobów nie są akceptowane przez tę strefę. Musisz ręcznie zaktualizować te rekordy.

< Wstecz Dalej > Anuluj



Menedżer DNS

⌵ Akcja Widok Pomoc



DNS

WIN-ADLL63PI067

- ▼ Strefy wyszukiwania do przodu
 - edu.local
- > Strefy wyszukiwania wstecznego
- > Punkty zaufania
- > Usługi warunkowego przesyłania dalej

Nazwa	Typ
15.168.192.in-addr.arpa	Podstawowa s

DNS

WIN-ADLL63PI067

Strefy wyszukiwania do przodu

edu.local

Strefy wyszukiwania wstecznego

15.168.192.in-addr.arpa

Punkty zaufania

Usługi warunkowego przesyłania dalej

Nazwa	Typ	Dane
(identyczny jak folder nadrz...	Adres startowy uwierzyt...	[1], win-adll63pi067., host...
(identyczny jak folder nadrz...	Serwer nazw (NS)	win-adll63pi067.

Właściwości: 15.168.192.in-addr.arpa

Ogólne

Adres startowy uwierzytelniania (SOA)

Serwery nazw

WINS-R

Transfery stref

Aby dodać serwery nazw do poniższej listy, kliknij przycisk Dodaj.

W pełni kwalifikowana nazwa domeny (FQDN)...	Adres IP
win-adll63pi067.	Nieznane

Dodaj...

Edytuj...

Usuń

* odpowiada adresowi IP pobranemu jako wynik zapytania DNS i może nie odpowiadać rzeczywistym rekordom przechowywanym na tym serwerze.

OK

Anuluj

Zastosuj

Pomoc

DNS

WIN-ADLL63PI067

▼ Strefy wyszukiwania do przodu

edu.local

▼ Strefy wyszukiwania wstecznego

15.168.192.in-addr.arpa

> Punkty zaufania

> Usługi warunkowego przesyłania dalej

Nazwa	Typ	Dane
(identyczny jak folder nadrz...	Adres startowy uwierzyt...	[1], win-adll63pi067., host...
(identyczny jak folder nadrz...	Serwer nazw (NS)	win-adll63pi067.

Właściwości: 15.168.192.in-addr.arpa

Ogólne

Adres startowy uwierzytelniania (SOA)

Serwery nazw

WINS-R

Transfery stref

Aby dodać serwery nazw do poniższej listy, kliknij przycisk Dodaj.

W pełni kwalifikowana nazwa domeny (FQDN)...

Adres IP

win-adll63pi067.

[192.168.15.239]

Dodaj...

Edytuj...

Usuń

* odpowiada adresowi IP pobranemu jako wynik zapytania DNS i może nie odpowiadać rzeczywistym rekordom przechowywanym na tym serwerze.

OK

Anuluj

Zastosuj

Pomoc

DNS

WIN-ADLL63PI067

Strefy wyszukiwania do przodu

edu.local

Strefy wyszukiwania wstecznego

15.168.192.in-addr.arpa

Punkty zaufania

Usługi warunkowego przesyłania dalej

Nazwa	Typ	Dane
(identyczny jak folder nadrz...	Adres startowy uwierzyt...	[1], win-adll63pi067, host...
(identyczny jak folder nadrz...	Serwer nazw (NS)	win-adll63pi067.

Właściwości: 15.168.192.in-addr.arpa

Edytuj rekord serwera nazw

Wprowadź nazwę serwera i co najmniej jeden adres IP. Obie te wartości są potrzebne do zidentyfikowania serwera nazw.
W pełni kwalifikowana nazwa domeny (FQDN) serwera

Wprowadź nazwę serwera i co najmniej jeden adres IP. Obie te wartości są potrzebne do zidentyfikowania serwera nazw.
W pełni kwalifikowana nazwa domeny (FQDN) serwera

Nazwa	Typ	Dane
(identyczny jak folder nadrz...	Adres startowy uwierzyt...	[1], win-adll63pi067, host...
(identyczny jak folder nadrz...	Serwer nazw (NS)	win-adll63pi067.

Usun

W gore

W dol

OK

Anuluj

Menedżer DNS

Plik Akcja Widok Pomoc

DNS

WIN-ADLL63PI067

Strefy wyszukiwania do przodu

edu.local

Strefy wyszukiwania wstecznego

Punkty zaufania

Usługi warunkowego przesyłania dalej

Nazwa

edu.local

Typ

Punkt

Nazwa	Typ	Dane
 (identyczny jak folder nadrz...	Adres startowy uwierzyt...	[1], win-adll63pi067., host...
 (identyczny jak folder nadrz...	Serwer nazw (NS)	win-adll63pi067.

Aktualizuj plik danych serwera

Załaduj ponownie

Nowy host (A lub AAAA)...

Nowy alias (CNAME)...

Nowa usługa wymiany poczty (MX)...

Nowa domena...

Nowe delegowanie...

Inne nowe rekordy...

DNSSEC >

Wszystkie zadania >

Odśwież

Eksportuj listę...

Widok >

Rozmieść ikony >

Szereguj ikony

Właściwości

Pomoc



DNS

- WIN-ADLL63PI067
 - Strefy wyszukiwania do przodu
 - edu.local
 - Strefy wyszukiwania wstecznego
 - 15.168.192.in-addr.arpa
 - Punkty zaufania
 - Usługi warunkowego przesyłania dalej

Nazwa	Typ	Dane
(identyczny jak folder nadrz...	Adres startowy uwierzyt...	[1], wir
(identyczny jak folder nadrz...	Serwer nazw (NS)	win-ac

Nowy host

Nazwa (jeżeli pole pozostanie puste, użyta zostanie nazwa domeny nadrzędnej):

print9

W pełni kwalifikowana nazwa domeny (FQDN):

print9.edu.local.

Adres IP:

192.168.15.241

☒
 Utwórz skojarzony rekord wskaźnika (PTR)

Dodaj hosta

Anuluj



WIN-ADLL63PI067

Strefy wyszukiwania do przodu

edu.local

Strefy wyszukiwania wstecznego

15.168.192.in-addr.arpa

Punkty zaufania

Usługi warunkowego przesyłania dalej

Nazwa	Typ	Dane
(identyczny jak folder nadrz...	Adres startowy uwierzyt...	[1], win-
(identyczny jak folder nadrz...	Serwer nazw (NS)	win-
print9	Host (A)	192.

Nowy host

Nazwa (jeżeli pole pozostanie puste, użyta zostanie nazwa domeny nadrzędnej):

W pełni kwalifikowana nazwa domeny (FQDN):

edu.local.

DNS



Utworzono pomyślnie rekord hosta print9.edu.local.

OK

Dodaj hosta

Anuluj

Menedżer DNS

Plik Akcja Widok Pomoc



DNS

WIN-ADLL63PI067

Strefy wyszukiwania do przodu

edu.local

Strefy wyszukiwania wstecznego

15.168.192.in-addr.arpa

Punkty zaufania

Usługi warunkowego przesyłania dalej

Nazwa	Typ	Dane
(identyczny jak folder nadrz...	Adres startowy uwierzyt...	[1], win-adll63pi067., host...
(identyczny jak folder nadrz...	Serwer nazw (NS)	win-adll63pi067.
print9	Host (A)	192.168.15.241

Menedżer DNS

Plik Akcja Widok Pomoc

DNS

- WIN-ADLL63PI067
 - Strefy wyszukiwania do przodu
 - edu.local
 - Strefy wyszukiwania wstecznego
 - 15.168.192.in-addr.arpa
 - Punkty zaufania
 - Usługi warunkowego przesyłania dalej

Nazwa	Typ	Dane
(identyczny jak folder nadrz...	Adres startowy uwierzyt...	[1], win-adll63pi067, host...
(identyczny jak folder nadrz...	Serwer nazw (NS)	win-adll63pi067.

- Aktualizuj plik danych serwera
- Załaduj ponownie
- Nowy wskaźnik (PTR)...
- Nowy alias (CNAME)...
- Nowe delegowanie...
- Inne nowe rekordy...
- DNSSEC >
- Wszystkie zadania >
- Odśwież**
- Eksportuj listę...
- Widok >
- Rozmieść ikony >
- Szereguj ikony
- Właściwości
- Pomoc

Menedżer DNS

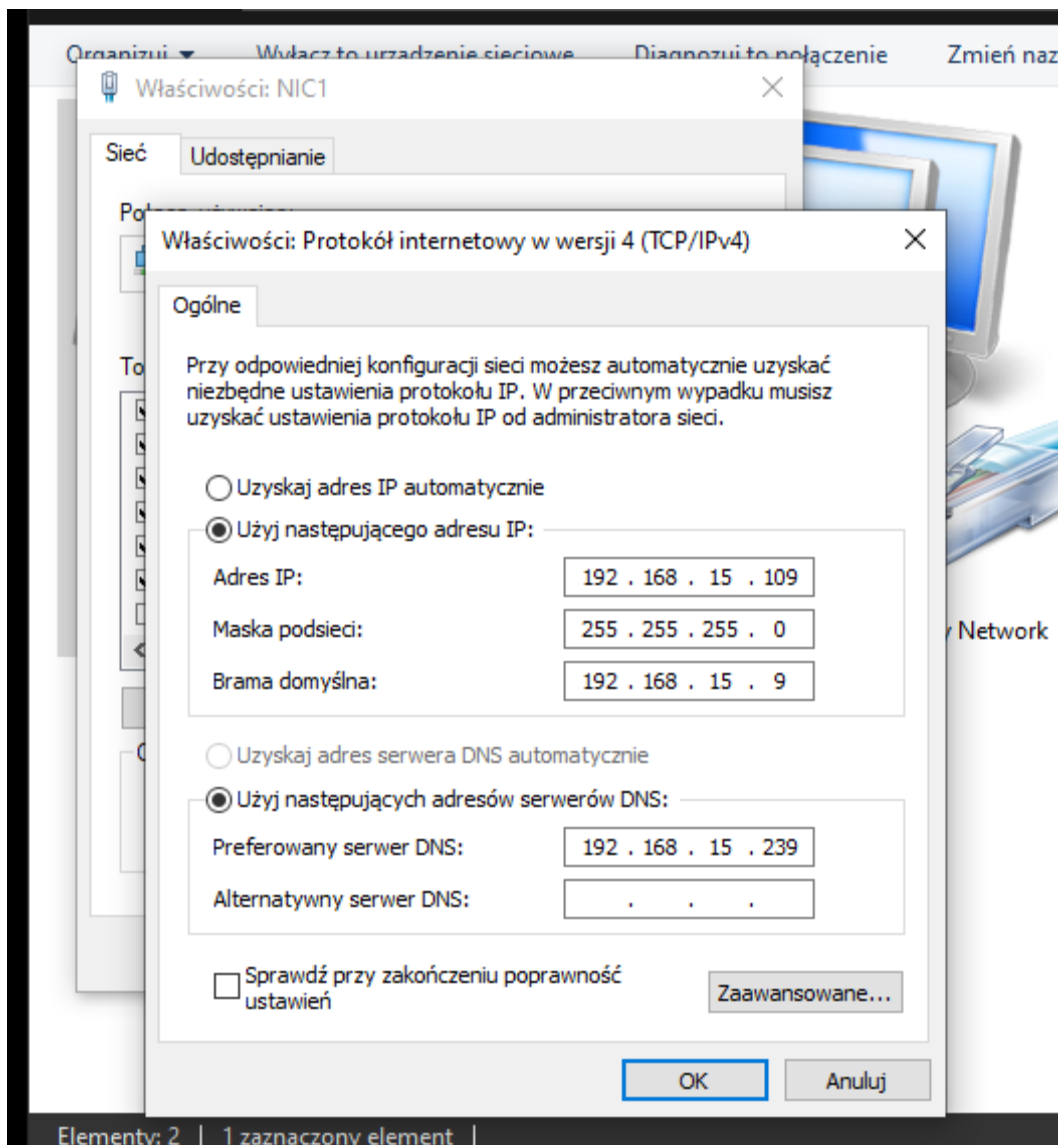
Plik Akcja Widok Pomoc

DNS

- WIN-ADLL63PI067
 - Strefy wyszukiwania do przodu
 - edu.local
 - Strefy wyszukiwania wstecznego
 - 15.168.192.in-addr.arpa
 - Punkty zaufania
 - Usługi warunkowego przesyłania dalej

Nazwa	Typ	Dane
(identyczny jak folder nadrz...	Adres startowy uwierzyt...	[3], win-adll63pi067, host...
(identyczny jak folder nadrz...	Serwer nazw (NS)	win-adll63pi067.
192.168.15.2 41	Wskaźnik (PTR)	print9.edu.local.

Na PCKliencie powinienes mieć ustawiony preferowany DNS na adres SERWERA WINDOWS 2022



W cmd uruchom program nslookup i sprawdź rekord A domeny drukarki

```
C:\Users\user>nslookup  
Default Server:  UnKnown  
Address:  192.168.15.239
```

```
> set type=a  
> print9.edu.pl  
Server:  UnKnown  
Address:  192.168.15.241
```

```
DNS request timed out.  
    timeout was 2 seconds.
```

```
DNS request timed out.  
    timeout was 2 seconds.
```

```
*** Request to UnKnown timed-out
```

```
> _
```

Inne polecenia diagnozujące

```
C:\Users\user>ipconfig /displaydns
```

Windows IP Configuration

```
print9.edu.local
```

```
-----  
Record Name . . . . . : print9.edu.local  
Record Type . . . . . : 1  
Time To Live . . . . . : 3429  
Data Length . . . . . : 4  
Section . . . . . : Answer  
A (Host) Record . . . : 192.168.15.241
```

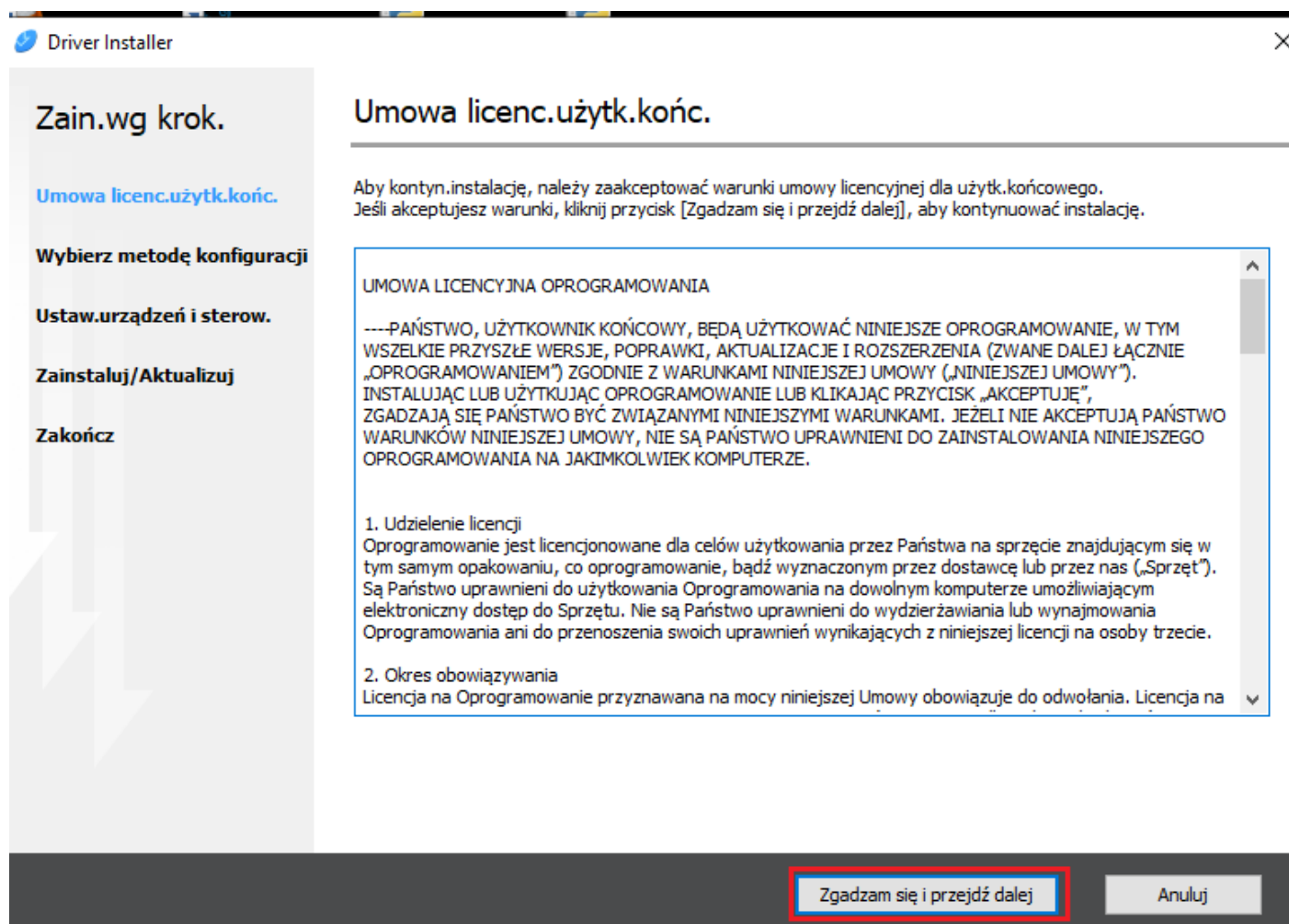
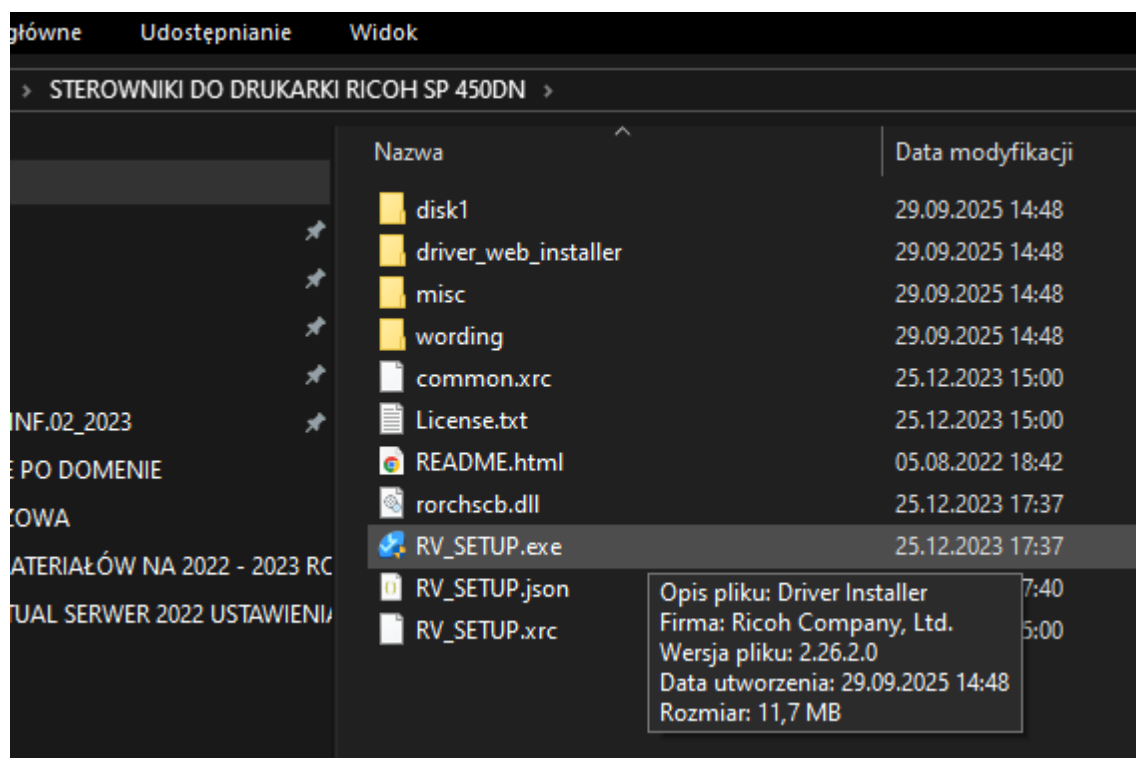
```
C:\Users\user>ping print9.edu.local
```

```
Pinging print9.edu.local [192.168.15.241] with 32 bytes of data:  
Reply from 192.168.15.241: bytes=32 time<1ms TTL=255  
Reply from 192.168.15.241: bytes=32 time<1ms TTL=255  
Reply from 192.168.15.241: bytes=32 time<1ms TTL=255  
Reply from 192.168.15.241: bytes=32 time<1ms TTL=255
```

```
Ping statistics for 192.168.15.241:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Instalacja sterowników do drukarki RICOH 450 DN



Zain.wg krok.

Umowa licenc.użytk.końc.

Wybierz metodę konfiguracji

Ustaw.urządzeń i sterow.

Zainstaluj/Aktualizuj

Zakończ

Wybierz metodę konfiguracji

Wybierz interfejs urządzenia i kliknij [Dalej].

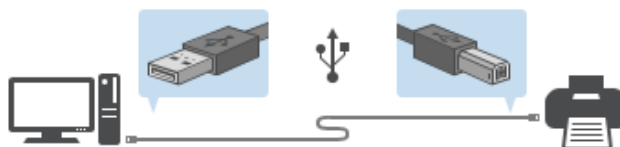
Jeśli chcesz aktualizować sterownik w swoim komputerze, kliknij [Aktualizuj sterownik].

☒ Sieć

Dokonaj wyboru, gdy komputer i urządzenie są połączone przez sieć.

☐ USB

Dokonaj wyboru, gdy komputer i urządzenie są bezp.podłączone za pomocą kabla USB.



Aktualizuj sterownik

Aktual.sterownika, który jest zainst.w komputerze.

Wstecz

Dalej

Anuluj

Zain.wg krok.

Umowa licenc.użytk.końc.

Wybierz metodę konfiguracji

Ustaw.urządzeń i sterow.

Wybierz urządzenie

Wybierz sterow.urządź.

Właściwości drukarki

Zainstaluj/Aktualizuj

Zakończ

Wybierz urządzenie

Wybierz drukarkę z listy i kliknij [Dalej].

Kliknij [Kliknij jeśli nie możesz znaleźć urządzenia] podczas określania adresu IP urządzenia.

Zakończono wyszukiwanie.

Wyszukaj ponownie

Nazwa urządzenia	Adres IP	Komentarz
SP 450DN	192.168.15.241	

Kliknij jeśli nie możesz znaleźć urządzenia

☐ Ręczne wpisywanie ustawień ⓘ

Wstecz

Dalej

Anuluj

Zain.wg krok.

Umowa licenc.użytk.końc.

Wybierz metodę konfiguracji

Ustaw.urządzeń i sterow.

Wybierz urządzenie**Wybierz sterow.urządz.****Właściwości drukarki****Zainstaluj/Aktualizuj****Zakończ**

Wybierz metodę wyszukiwania

Wybierz metodę wyszukiwania i kliknij [Dalej].

☐ Określ adres IP urządzenia☒ Określ adres urządzenia

Wstecz

Dalej

Anuluj

Zain.wg krok.

Umowa licenc.użytk.końc.

Wybierz metodę konfiguracji

Ustaw.urządzeń i sterow.

Wybierz urządzenie**Wybierz sterow.urządz.****Właściwości drukarki****Zainstaluj/Aktualizuj****Zakończ**

Wybierz urządzenie

Wybierz drukarkę, którą chcesz używać i kliknij [Dalej].

Nazwa urządzenia:

MP C2503Z

DSm1025
DSm1020
MP 3353
MP 3053
MP 2553
MP 401SPF
Pro C5110S
Pro C5100S
Pro 8120S
Pro 8110S
Pro 8100S
Pro 8120
Pro 8110
Aficio SP C730DN
SP C730DN
Aficio SP C831DN
Aficio SP C830DN
SP C831DN
SP C830DN
SP 400DN
SP 3600DN
SP 3610SF
SP 3600SF
SP 4520DN
SP 4510DN
SP 450DN
SP 4510SF
SP 6430DN
Aficio SP 8300DN
SP 8300DN

Anuluj

Zain.wg krok.

Umowa licenc.użytk.końc.

Wybierz metodę konfiguracji

Ustaw.urządzeń i sterow.

Wybierz urządzenie

Wybierz sterow.urządź.

Właściwości drukarki

Zainstaluj/Aktualizuj

Zakończ

Właś.drukarki

Ustawienia drukarki mogą być zmienione.

Nazwa sterownika: RICOH SP 450DN PCL 6 ⓘ

* Nazwa drukarki: RICOH SP 450DN PCL 6 ⓘ

Komentarz: PCL6 Driver (For Windows) ⓘ

* Nazwa portu: ⓘ

Dodaj port

☒ Ustaw jako domyślną drukarkę ⓘ

Zaawansowane ustawienia

☐ Udostępnij druk. ⓘ

Współdzielona nazwa: RICOH SP 450DN PCL 6 ⓘ

Kod użytkownika: ⓘ

* : wymagane pole.

Przyw.ustaw.domyś.

Wstecz

Dalej

Anuluj

Zain.wg krok.

Umowa licenc.użytk.końc.

Wybierz metodę konfiguracji

Ustaw.urządzeń i sterow.

Wybierz urządzenie

Wybierz sterow.urządź.

Właściwości drukarki

Zainstaluj/Aktualizuj

Zakończ

Właś.drukarki

Dodaj port

Wybierz rodzaj portu, aby dodać.

Dostępne rodzaje portów:

Appmon
Local Port
Standard TCP/IP Port
Drukarka sieciowa
Port IPP

OK

Anuluj

* : wymagane pole.

Przyw.ustaw.domyś.

Wstecz

Dalej

Anuluj

ain.wg krok.

owa licenc.użytk.końc.

bierz metodę konfiguracji

aw.urządzeń i sterow.

Wybierz urządzenie

Wybierz sterow.urządź.

Właściwości drukarki

instaluj/Aktualizuj

kończ

Właś.drukarki

Dodaj port

Kreator dodawania standardowego portu TCP/IP drukarki

**Kreator dodawania standardowego portu TCP/IP drukarki — Zapraszamy!**

Ten kreator pomaga dodać port dla drukarki sieciowej.

Zanim zaczniesz kontynuować, upewnij się, że:

1. Urządzenie jest włączone.
2. Sieć jest podpięta i skonfigurowana.

Aby kontynuować, kliknij przycisk Dalej.

< Wstecz

Dalej >

Anuluj

in.wg krok.

wa licenc.użytk.końc.

bierz metodę konfiguracji

w.urządzeń i sterow.

Wybierz urządzenie

Wybierz sterow.urządź.

Właściwości drukarki

instaluj/Aktualizuj

ończ

Właś.drukarki

Dodaj port

Kreator dodawania standardowego portu TCP/IP drukarki

Dodaj port

Dla jakiego urządzenia chcesz dodać port?



Podaj nazwę drukarki lub adres IP oraz nazwę portu dla żadanego urządzenia.

Nazwa drukarki lub adres IP:

print9.edu.local

Nazwa portu:

print9.edu.local

< Wstecz

Dalej >

Anuluj

rok.

Właśc. drukarki

ytł.końc.

konfiguracji

i sterow.

gdzenie

ow.urządz.

ci drukarki

ualizuj

Dodaj port

Kreator dodawania standardowego portu TCP/IP drukarki

Kończenie pracy Kreatora dodawania standardowego portu TCP/IP drukarki

Został wybrany port o następujących charakterystykach.

Protokół SNMP:	Tak
Protokół:	RAW, Port 9100
Urządzenie:	print9.edu.local
Nazwa portu:	print9.edu.local
Typ karty:	SP 450DN

Aby ukończyć pracę kreatora, kliknij przycisk Zakończ.

< Wstecz Zakończ Anuluj

Driver Installer

×

Zain.wg krok.

Umowa licenc. użytł.końc.

Wybierz metodę konfiguracji

Ustaw.urządzeń i sterow.

Wybierz urządzenie

Wybierz sterow.urządz.

Właściwości drukarki

Zainstaluj/Aktualizuj

Zakończ

Właśc. drukarki

Ustawienia drukarki mogą być zmienione.

Nazwa sterownika: RICOH SP 450DN PCL 6 ⓘ

* Nazwa drukarki: RICOH SP 450DN PCL 6 ⓘ

Komentarz: PCL6 Driver (For Windows) ⓘ

* Nazwa portu: print9.edu.local ⓘ

Dodaj port ⓘ

☒ Ustaw jako domyślną drukarkę ⓘ

Zaawansowane ustawienia

☐ Udostępnij druk. ⓘ

Współdzielona nazwa: RICOH SP 450DN PCL 6 ⓘ

Kod użytkownika: ⓘ

* : wymagane pole.

Przyw.ustaw.domyś.

Wstecz

Dalej

Anuluj

Zain.wg krok.

Umowa licenc.użytk.końc.

Wybierz metodę konfiguracji

Ustaw.urządzeń i sterow.

Zainstaluj/Aktualizuj

Zainstaluj

Zakończ

Zainstaluj

Instalowanie sterownika...
RICOH SP 450DN PCL 6

Anuluj

Zain.wg krok.

Umowa licenc.użytk.końc.

Wybierz metodę konfiguracji

Ustaw.urządzeń i sterow.

Zainstaluj/Aktualizuj

Zakończ

Zakończ

Powiodło się dodanie urządzenia.

Raport:

[Wynik instalacji]
RICOH SP 450DN PCL 6: Pomyślnie
Powiodło się dodanie urządzenia.

[Powiodło się dodanie urządzenia]
RICOH SP 450DN PCL 6
-Domyślna drukarka:Włączone
-Sterownik:RICOH SP 450DN PCL 6
-Wersja:3.0.0.0
-Nazwa portu:print9.edu.local
-Comentarz:PCL6 Driver (For Windows)
-Kod użytkownika:
-Współdzielona drukarka:Wyłączone
-Dodany sterownik:Nie zainstalowano

Pomyślnie zainstalowane urządzenia :

RICOH SP 450DN PCL 6

Wydrukuj stronę testową

Sprawdź/Zmień ust. druku

Zakończ

Zain.wg krok.

Umowa licenc. użyt.k. końc.

Wybierz metodę konfiguracji

Ustaw urządzeń i sterow.

Zainstaluj/Aktualizuj

Zakończ

Zainstaluj Device Software Manager

Łatwa instalacja i aktualizacja najnowszych sterowników do MFP i drukarek Ricoh.
Device Software Manager automatycznie wykrywa odpowiednie urządzenia wielofunkcyjne i drukarki w twojej sieci lub podłączone do komputera przez USB.

Device Software Manager zostanie zainstalowany po zakończeniu instalowania sterownika.
Pliki w pakiecie sterowników służą do instalacji.
Nie usuwaj plików w pakiecie sterowników.

☐ Zainstaluj Device Software Manager**Dalej**

Wyszukaj

Aplikacje

Dokumenty

Sieć

Więcej ▾

Najlepszy wynik

**Panel sterowania**
System

Aplikacje



XAMPP Control Panel



Paint



Paint 3D



Wyszukaj w sieci Web

**Panel sterowania**
System

Otwórz





System i zabezpieczenia

Zapoznaj się ze stanem komputera

Zapisz kopie zapasowe plików za pomocą historii plików

Kopia zapasowa i przywracanie (Windows 7)



Sieć i Internet

Połącz z Internetem

Wyświetl stan sieci i zadania



Sprzęt i dźwięk

Wyświetl urządzenia i drukarki

Dodaj urządzenie



Programy

Odinstaluj program



Sprzęt i dźwięk
Dodaj lub usuń drukarki i inny sprzęt, zmień dźwięki systemowe, odtwarzaj automatycznie dyski CD, oszczędzaj energię elektryczną, zaktualizuj sterowniki urządzeń i wykonaj inne działania.

Sprzęt i dźwięk

Panel sterowania > Sprzęt i dźwięk

Strona główna Panelu sterowania

System i zabezpieczenia

Sieć i Internet

• Sprzęt i dźwięk

Programy

Konta użytkowników

Wygląd i personalizacja

Zegar i region

Ułatwienia dostępu



Urządzenia i drukarki

Dodaj urządzenie

Zmień ustawienia urządzeń

Zaawansowane ustawienia drukarki

Mysz



Menedżer urządzeń

Urządzenia i drukarki
Wyświetl urządzenia, drukarki oraz zadania drukowania i zarządzaj nimi



Autoodtwarzanie

Zmień domyślne ustawienia nośników lub urządzeń

Automatycznie odtwarzaj dyski CD lub inne nośniki



Dźwięk

Dopasuj głośność systemu

Zmień dźwięki systemu

Zarządzaj urządzeniami audio



Opcje zasilania

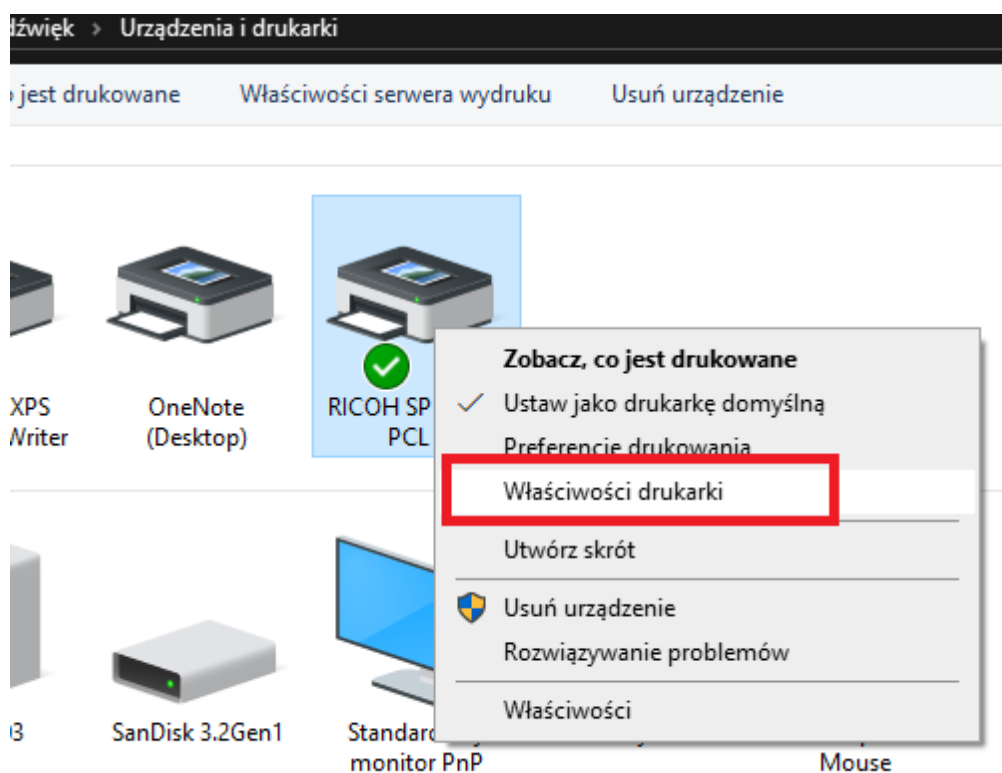
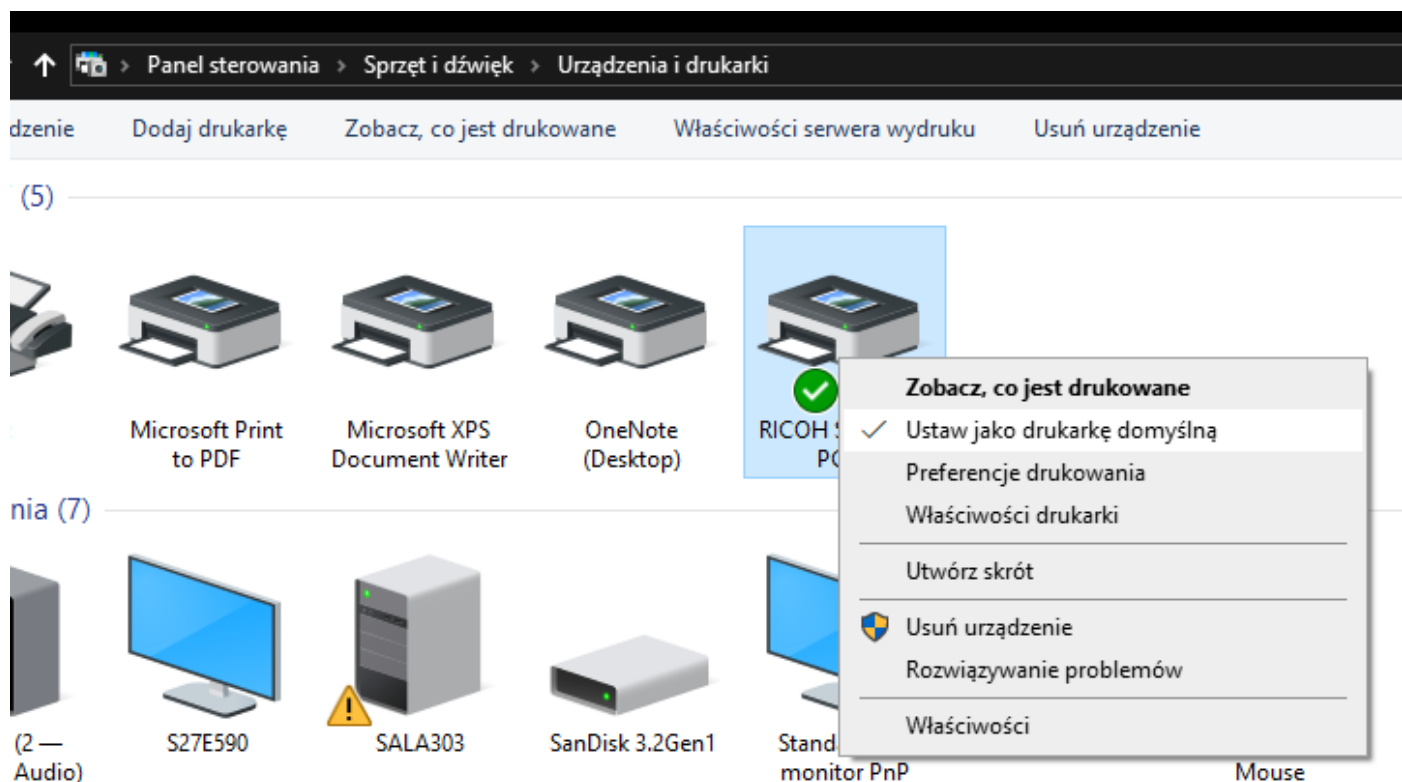
Zmień ustawienia oszczędzania energii

Zmień działanie przycisków zasilania

Zmień moment przejścia komputera w tryb uśpienia

Wybierz plan zasilania

Edytuj plan zasilania



Ogólne Udziałowanie Porty Zaawansowane Zarządzanie kolorami Zabezpieczenia Akcesoria Opcje zaawansowane

 RICOH SP 450DN PCL 6

Drukuj do następujących portów. Dokumenty będą drukowane w pierwszym wolnym wśród wybranych portów.

Port	Opis	Drukarka
☐ COM2:	Port szeregowy	
☐ COM3:	Port szeregowy	
☐ COM4:	Port szeregowy	
☐ FILE:	Drukuj do pliku	
☐ IP_10.1...	Standardowy port TC...	
☐ IP_192....	Standardowy port TC...	
☒ print9....	Standardowy port TC...	RICOH SP 450DN PCL 6

☒ Włącz obsługę dwukierunkową
☐ Włącz buforowanie drukarek

Konfiguruj monitor standardowego portu TCP/IP

Ustawienia portu

Nazwa portu:

Nazwa drukarki lub adres IP:

Protokół

☒ Raw
 ☐ LPR

Ustawienia Raw

Numer portu:

Ustawienia LPR

Nazwa kolejki:

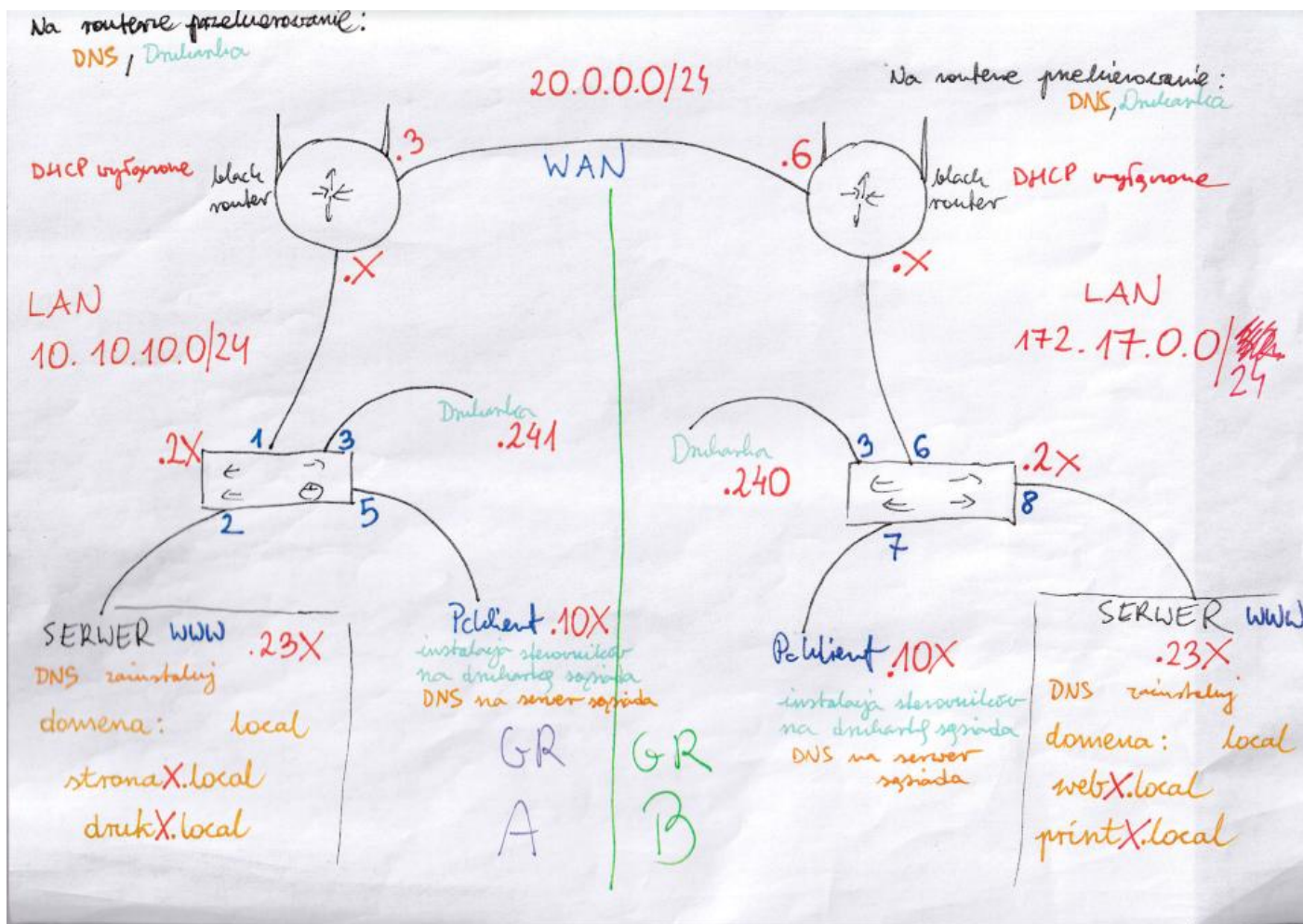
☐ Włączone zliczanie bajtów LPR

☒ Włączony stan protokołu SNMP

Nazwa społeczności:

Indeks urządzenia SNMP:

6.2 Drukowanie u sąsiada przez WAN po domenie



KONFIGURACJA DLA GRUPY 8

Ustawienia na routerze

► Status

▼ Network

- WAN
- LAN
- IPTV
- MAC
- Switch
- VLAN
- IPV6

► Preferences

► Transmission

LAN

DHCP Server

DHCP Client List

Address Reserve

IP Address: 172.17.0.8

Subnet Mask: 255.255.255.0

Management Vlan: ---

Save

Status

Network

- WAN
- LAN
- IPTV
- MAC
- Switch
- VLAN
- IPv6

Preferences

Transmission

Firewall

Behavior Control

VPN

Authentication

Services

WAN Mode

WAN1

WAN2

Connection Configuration

Connection Type:

Dynamic IP

Host Name:

Static IP

(Optional)

Upstream Bandwidth:

Dynamic IP

Kbps (100-1000000)

Downstream Bandwidth:

PPPoE

Kbps (100-1000000)

L2TP

(576-1500)

PPTP

(Optional)

BigPond Cable

(Optional)

MTU:

Primary DNS:

Secondary DNS:

Vlan:

10

☐ Get IP using Unicast DHCP

Save

Connect

Disconnect

Status

Network

- WAN
- LAN
- IPTV
- MAC
- Switch
- VLAN
- IPv6

Preferences

Transmission

Firewall

Behavior Control

VPN

Authentication

Services

System Tools

WAN Mode

WAN1

WAN2

Connection Configuration

Connection Type:

Static IP

IP Address:

20.0.0.6

Subnet Mask:

255.255.255.0

Default Gateway:

20.0.0.3

Upstream Bandwidth:

1000000

Downstream Bandwidth:

1000000

MTU:

1500

Primary DNS:

Secondary DNS:

Vlan:

10

Save

Wyłącz blokowanie pingowania WAN

▶ **Status**

▶ **Network**

▶ **Preferences**

▶ **Transmission**

▼ **Firewall**

- Anti ARP Spoofing
- **Attack Defense**
- MAC Filtering
- Access Control

▶ **Behavior Control**

▶ **VPN**

▶ **Authentication**

▶ **Services**

▶ **System Tools**

Logout

Copyright © 2018
TP-Link Technologies Co., Ltd.
All rights reserved.

Attack Defense

Packet Anomaly Defense

☒ Block Fragment Traffic

☒ Block TCP Scan (Stealth FIN/Xmas/Null)

☒ Block Ping of Death

☒ Block Large Ping

☐ Block Ping from WAN

☒ Block WinNuke attack

☒ Block TCP packets with SYN and FIN Bits set

☒ Block TCP packets with FIN Bit set but no ACK Bit set

☒ Block packets with specified IP options

☒ Security Option ☒ Loose Source Route Option

☒ Strict Source Route Option ☒ Record Route Option

☒ Stream Option ☒ Timestamp Option

☒ No Operation Option

Save

Sprawdź połączenie na WAN sąsiada **20.0.0.3**, a także sprawdź połączenie z drukarką w twojej sieci **172.17.0.240**.

```
C:\Users\Administrator>ping 20.0.0.3

Pinging 20.0.0.3 with 32 bytes of data:
Reply from 20.0.0.3: bytes=32 time<1ms TTL=63
Reply from 20.0.0.3: bytes=32 time<1ms TTL=63
Reply from 20.0.0.3: bytes=32 time<1ms TTL=63
Reply from 20.0.0.3: bytes=32 time<1ms TTL=63

Ping statistics for 20.0.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping 172.17.0.240

Pinging 172.17.0.240 with 32 bytes of data:
Reply from 172.17.0.240: bytes=32 time<1ms TTL=255
Reply from 172.17.0.240: bytes=32 time<1ms TTL=255
Reply from 172.17.0.240: bytes=32 time<1ms TTL=255
Reply from 172.17.0.240: bytes=32 time<1ms TTL=255

Ping statistics for 172.17.0.240:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Konfiguracja przekierowania na routerze

Status

Network

Preferences

Transmission

NAT

Bandwidth Control

Session Limit

Load Balancing

Routing

Multi-Nets NAT

One-to-One NAT

Virtual Servers

Port Triggering

NAT-DMZ

ALG

Virtual Server List

+ Add

☐	ID	Name	Interface	External Port	Internal Port	Internal Server IP	Protocol	Status	Operation
☐	--	--	--	--	--	--	--	--	

Status

Network

Preferences

Transmission

NAT

Bandwidth Control

Session Limit

Load Balancing

Routing

Firewall

Behavior Control

VPN

Authentication

Services

System Tools

Multi-Nets NAT

One-to-One NAT

Virtual Servers

Port Triggering

NAT-DMZ

ALG

☐	ID	Name	Interface	External Port	Internal Port	Internal Server IP
☐	--	--	--	--	--	--

Name:

Interface:

External Port:

Internal Port:

Internal Server IP:

Protocol:

Status:

www

WAN1

80

80

172.17.0.238

ALL

☒ Enable

OK

Cancel

Multi-Nets NAT

One-to-One NAT

Virtual Servers

Port Triggering

NAT-DMZ

ALG

Virtual Server List

+ Add

- Delete

☐	ID	Name	Interface	External Port	Internal Port	Internal Server IP	Protocol	Status	Operation
☐	1	www	WAN1	80	80	172.17.0.238	ALL	Enabled	

Status

Network

Preferences

Transmission

Firewall

Behavior Control

Multi-Nets NAT

One-to-One NAT

Virtual Servers

Port Triggering

NAT-DMZ

ALG

Virtual Server List

NAT

Bandwidth Control

Session Limit

Load Balancing

Routing

+

 Add

-

 Delete

☐	ID	Name	Interface	External Port	Internal Port	Internal Server IP	Protocol	Status	Operation
☐	1	www	WAN1	80	80	172.17.0.238	ALL	Enabled ✖	
☐	2	dns	WAN1	53	53	172.17.0.238	ALL	Enabled ✖	
☐	3	druk	WAN1	9100	9100	172.17.0.240	ALL	Enabled ✖	

Zainstaluj i skonfiguruj usługę DNS na SERWERZE WINDOWS 2022.

The screenshot displays the Windows Server 2012 R2 interface. On the left, the 'Pulpit nawigacyjny' (Navigation pane) shows the hierarchy: 'Serwer lokalny' (Local server) > 'Wszystkie serwery' (All servers) > 'DNS' > 'IIS' > 'Usługi plików i magazyny...' (File and storage services). The main window is titled 'SERWERY' (Servers) and shows 'Wszystkie serwery | Razem: 1' (All servers | Total: 1). Below this, a table lists the servers:

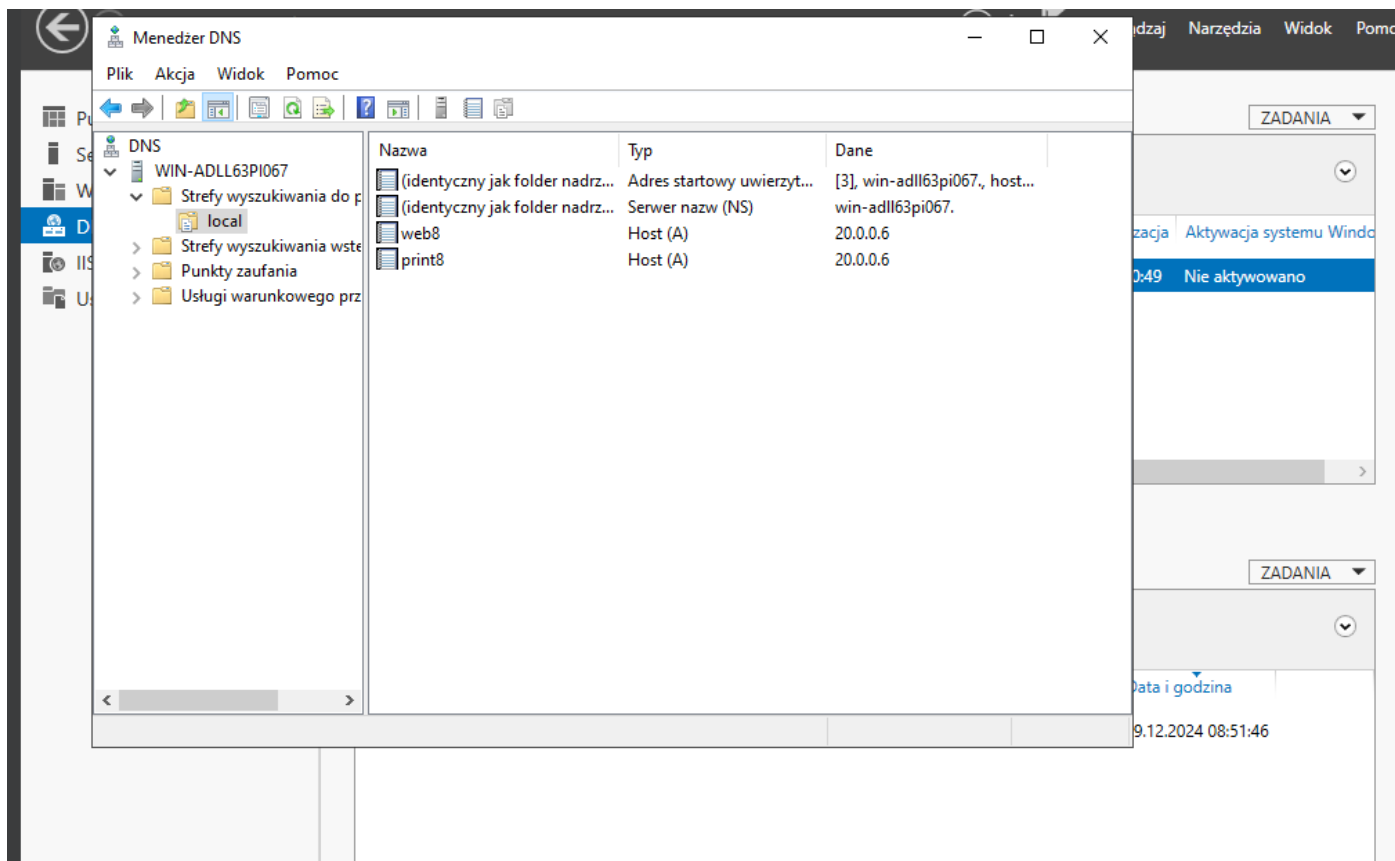
Nazwa serwera	Adres IPv4	Łatwość zarządzania	Ostatnia aktualizacja	Aktywacja systemu Windows
WIN-ADLL63PI067	172.17.0.238	Tryb online — nie uruchomiono liczników wydajności	19.12.2024 09:50:49	Nie aktywowano

The 'Menedżer internetowych usług informacyjnych (IIS)' (Internet Information Services (IIS) Manager) window is open, showing the 'Witryny' (Sites) feature. The left pane shows the tree structure: 'Strona początkowa' (Home page) > 'WIN-ADLL63PI067 (WIN-ADLL63PI067)' > 'Pule aplikacji' (Application pools) > 'Witryny' (Sites). The main pane displays the 'Witryny' (Sites) table:

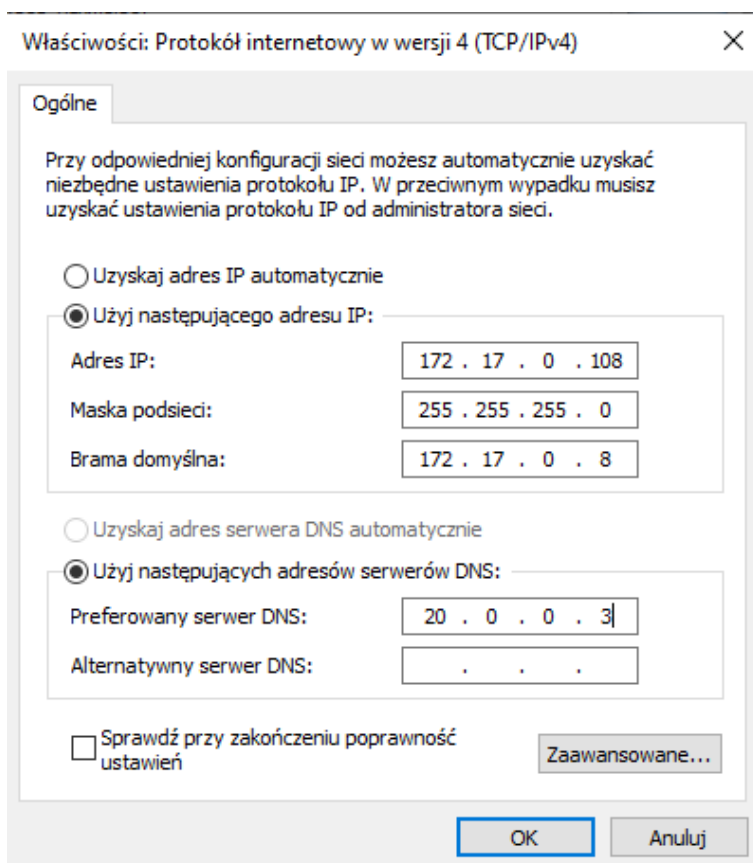
Nazwa	Identyfikator	Stan	Pow
Default Web Site	1	Uruchomi...	*:80

The right pane shows the 'Akcje' (Actions) menu with options: 'Dodaj witrynę sieci Web...' (Add Web site...), 'Określ ustawienia domyślne witryny sieci Web...' (Set default Web site settings...), and 'Pomoc' (Help).

Zainstaluj i skonfiguruj usługę DNS na SERWERZE WINDOWS 2022.



Na karcie sieciowej **PCKLIEN-a** ustaw DNS na adres **20.0.0.3** (WAN sąsiada).



U sąsiada na **PCKLIEN – cie** (tutaj na stanowisku nr 7) sprawdzić dostępność rekordów A **print8.local** i **web8.local**.

```
C:\Windows\system32>nslookup
Default Server:  web8.local
Address:  20.0.0.6

> set type=a
> print8.local
Server:  web8.local
Address:  20.0.0.6

Name:    print8.local
Address:  20.0.0.6
```

ping **web8.local**

Xezx545555

```
> set type=a
> web8.local
Server:  print8.local
Address:  20.0.0.6

Name:    web8.local
Address:  20.0.0.6
```

U sąsiada na **PCKLIEN – cie** (tutaj na stanowisku nr 7) wykonaj pingowanie na SERWER i drukarkę po domenie

ping **web8.local**

ping **print8.local**

Następnie wyświetl pobrane rekordy DNS za pomocą polecenia **ipconfig /displaydns**

```
C:\Windows\system32>ipconfig /displaydns

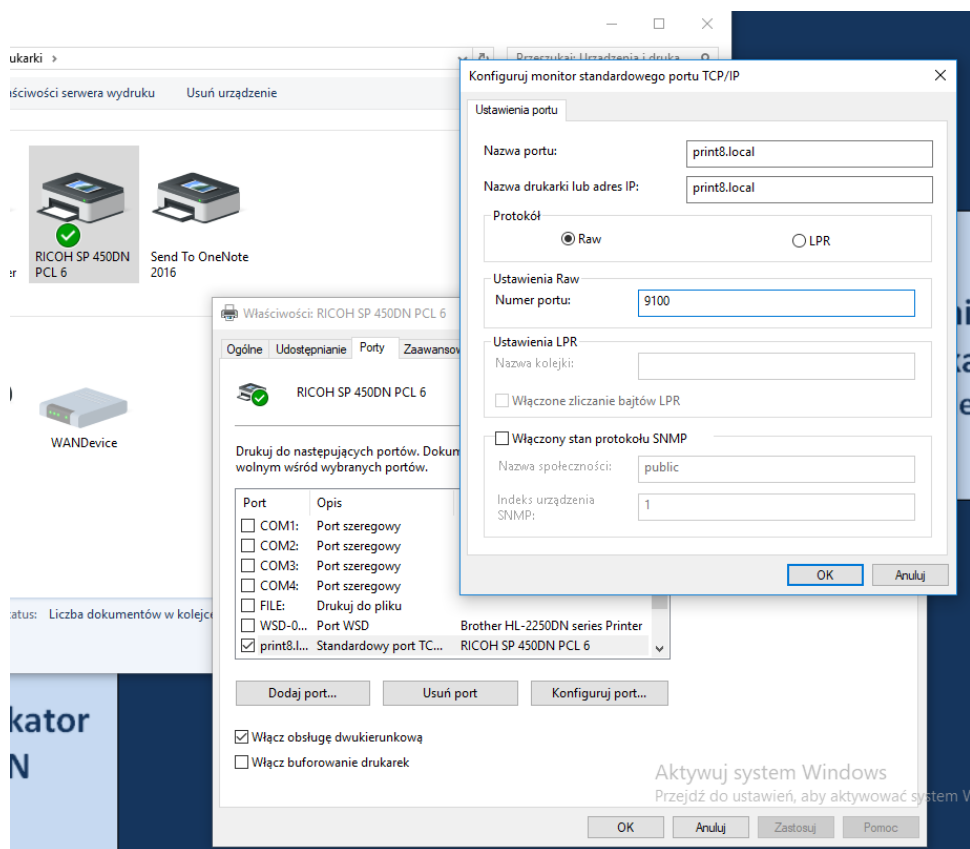
Windows IP Configuration

web8.local
-----
Record Name . . . . . : web8.local
Record Type . . . . . : 1
Time To Live . . . . . : 1753
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 20.0.0.6

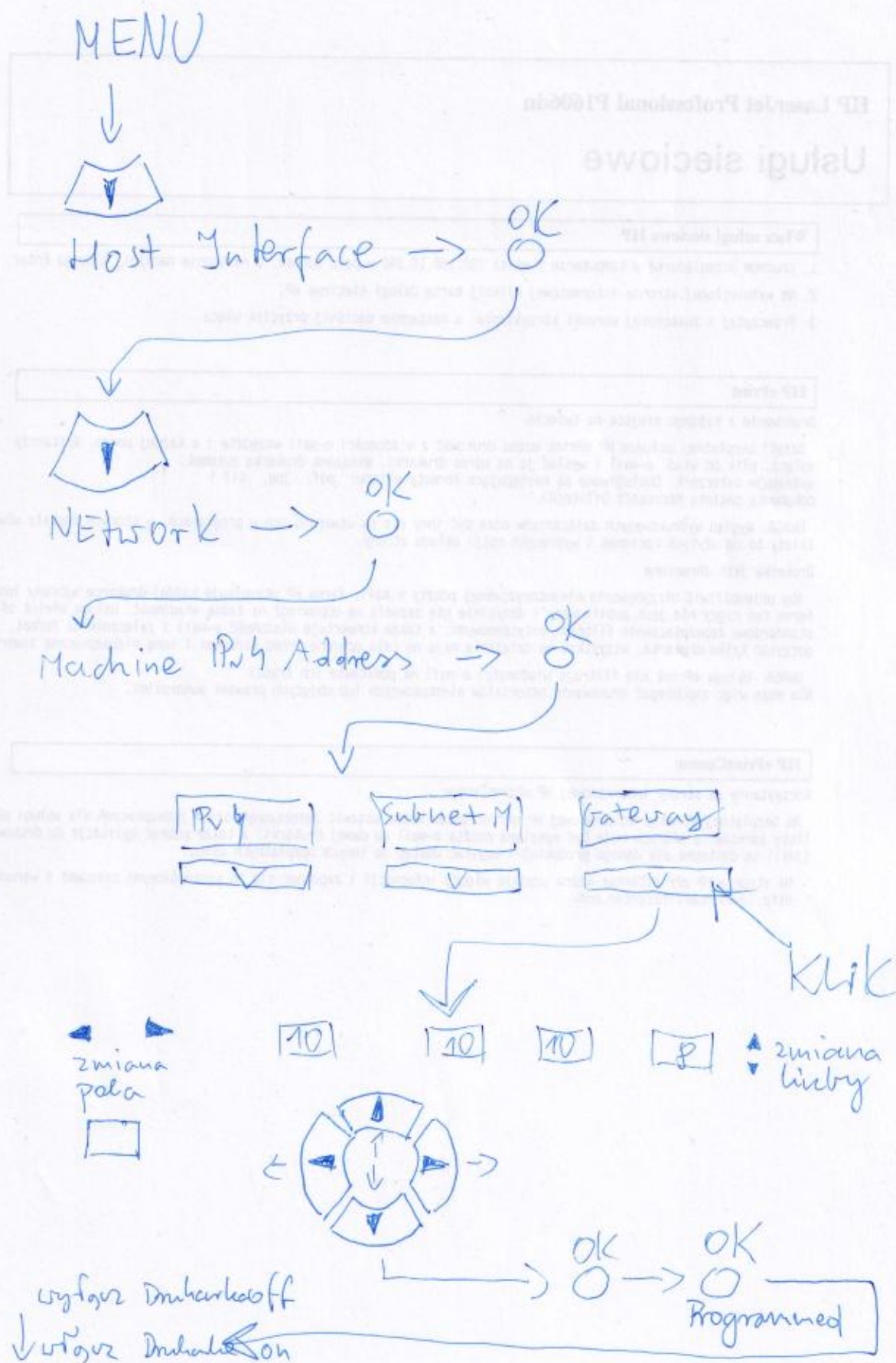

print8.local
-----
Record Name . . . . . : print8.local
Record Type . . . . . : 1
Time To Live . . . . . : 3297
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 20.0.0.6
```

Zainstaluj na **PCKLIEN – cie** (tutaj stanowisko 7) sterowniki do drukarki po domenie **print8.local**.

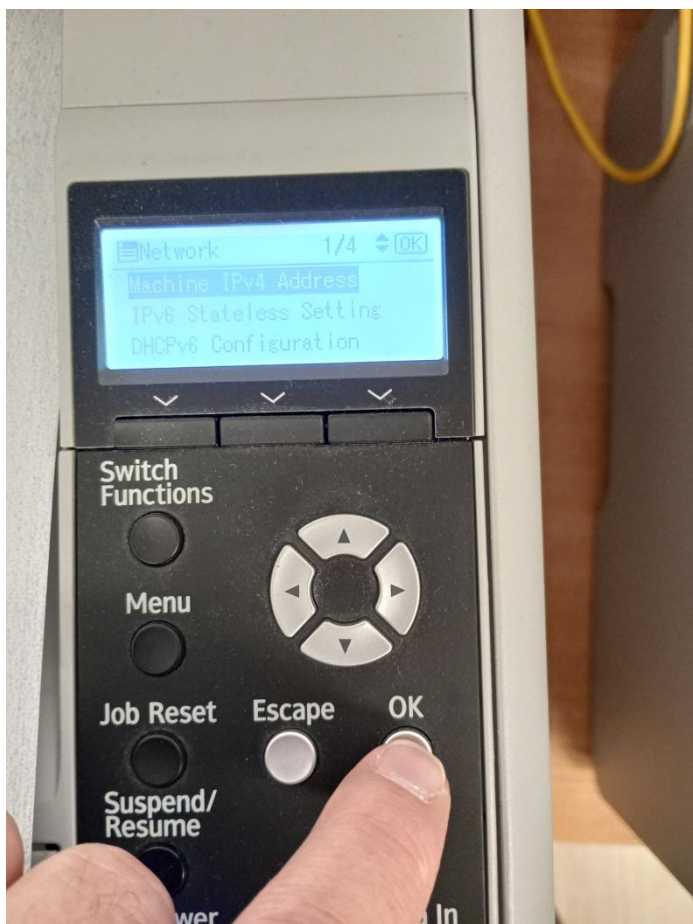
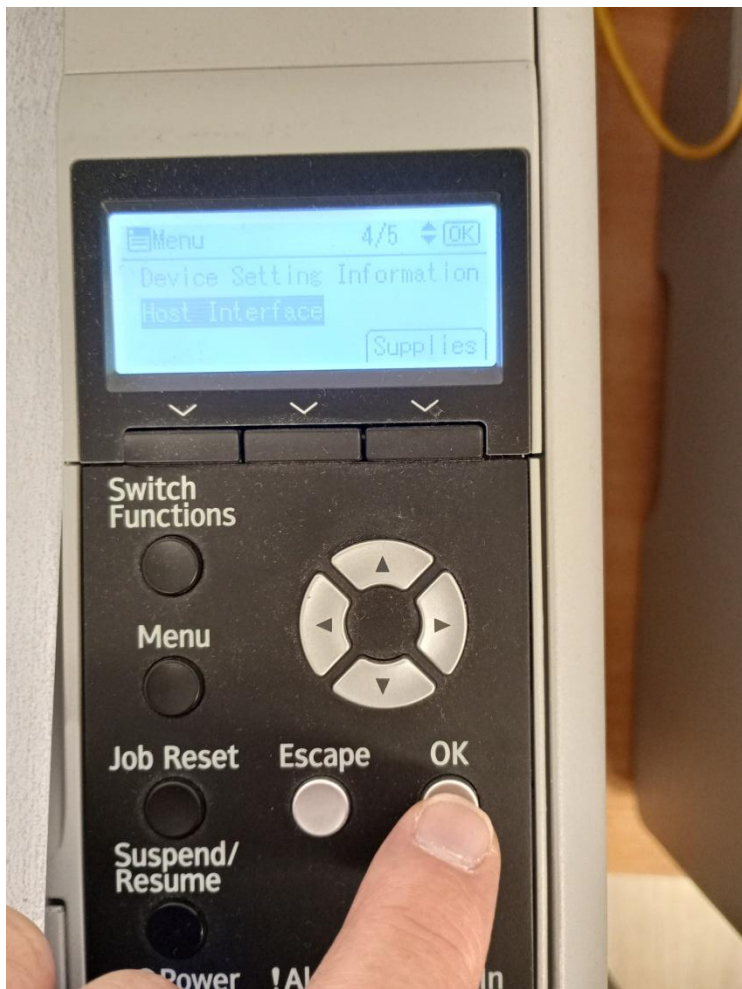
Efekt instalacji widziany poniżej:

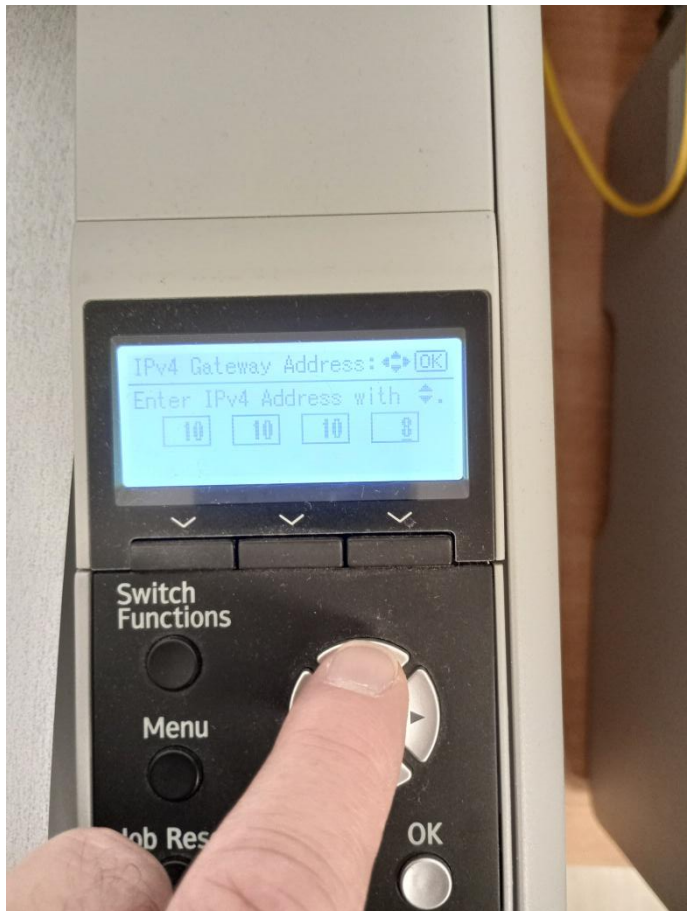
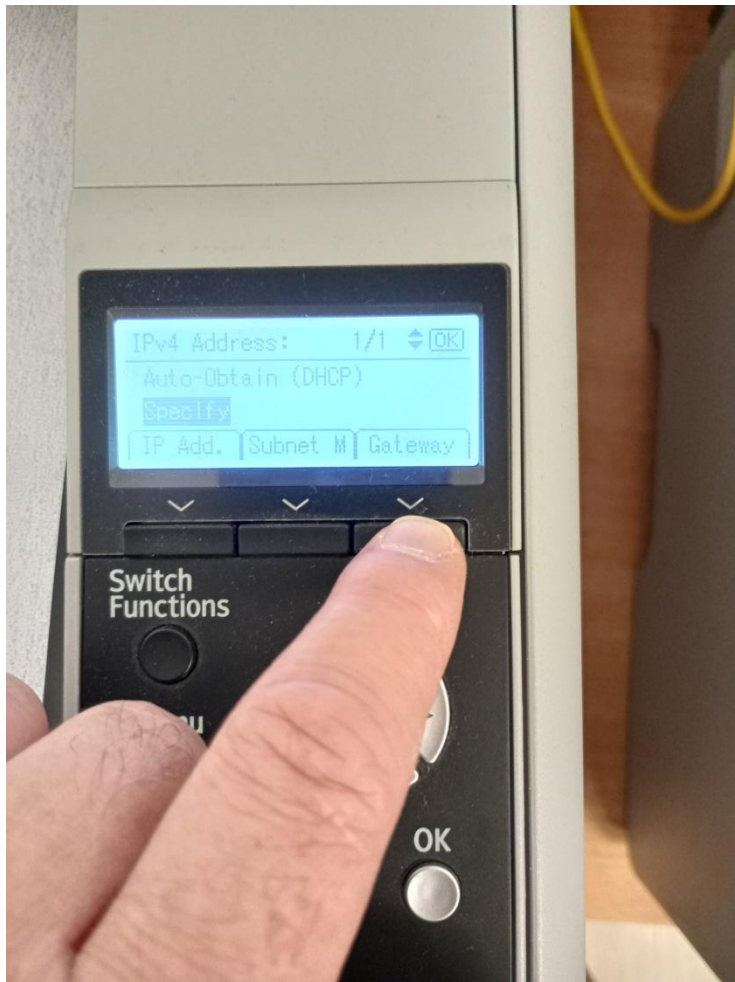


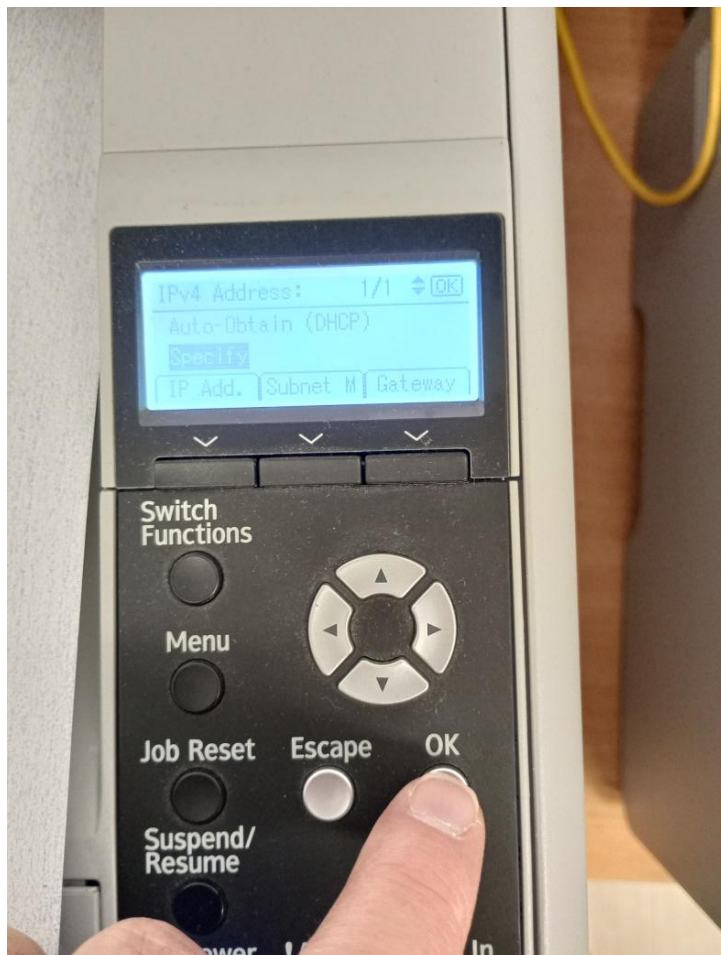
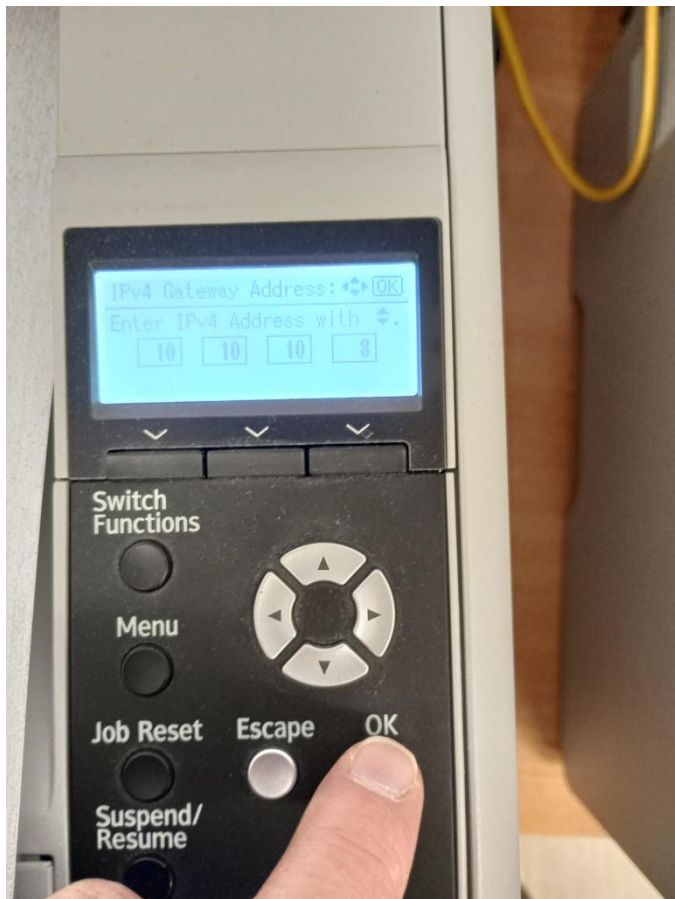
USTAWIENIE BRAMY DOMYŚLNEJ NA DRUKARCE RICOH450DN

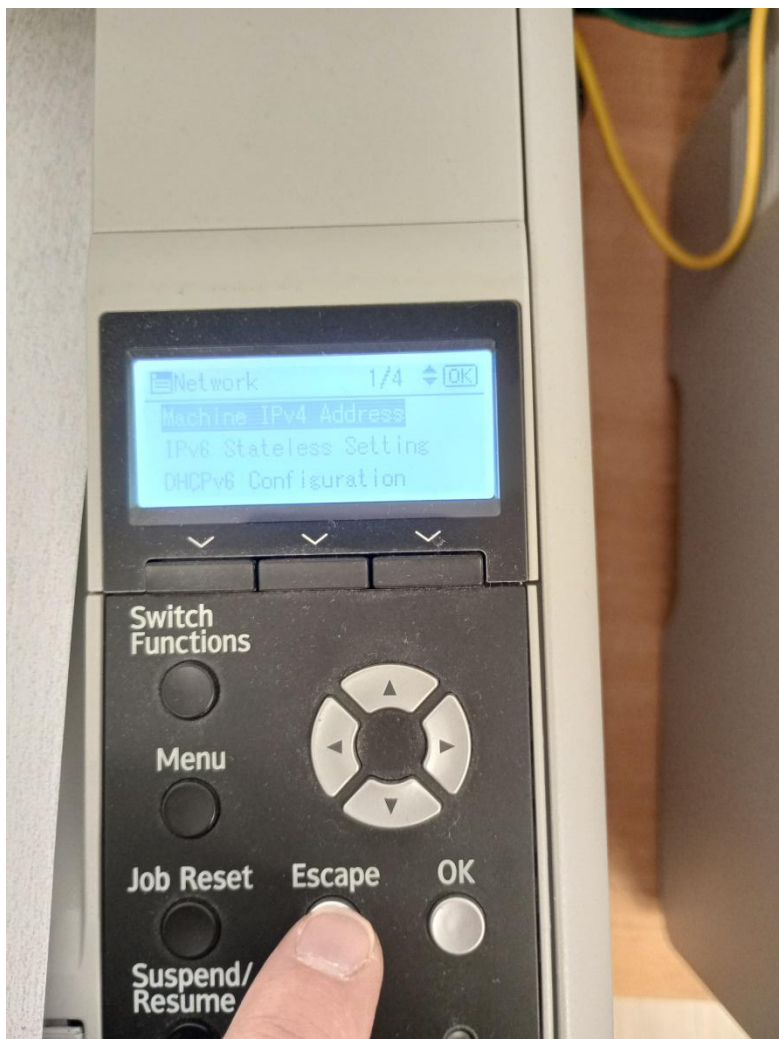












Wyłącz i włącz drukarkę ponownie



Poniżej możesz zobaczyć proces synchronizacji i przekazywania pliku do druku w programie Wireshark

Wireshark interface showing network traffic analysis. The main pane displays a list of captured packets with columns: No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 48) is a TCP packet from 10.10.10.107 to 20.0.0.6, Seq=2651, Ack=9100, Win=65536, Len=0, labeled as [ACK].

The packet details pane shows the structure of the selected packet:

- Frame 0000: ac 84 c6 31 bb cf 18 24 a1 3b ae dc 08 00 45 00 ... 1..k5;...E-
- Ethernet II, Src: Intel(R) Ethernet Controller (3:0:1), Dst: Intel(R) Ethernet Controller (3:0:1)
- Internet Protocol Version 4, Src: 10.10.10.107, Dst: 20.0.0.6
- TCP, Seq=2651, Ack=9100, Win=65536, Len=0, Window Scale=0
- 6: microsecond offset from capture time

The packet bytes pane shows the raw data of the selected packet:

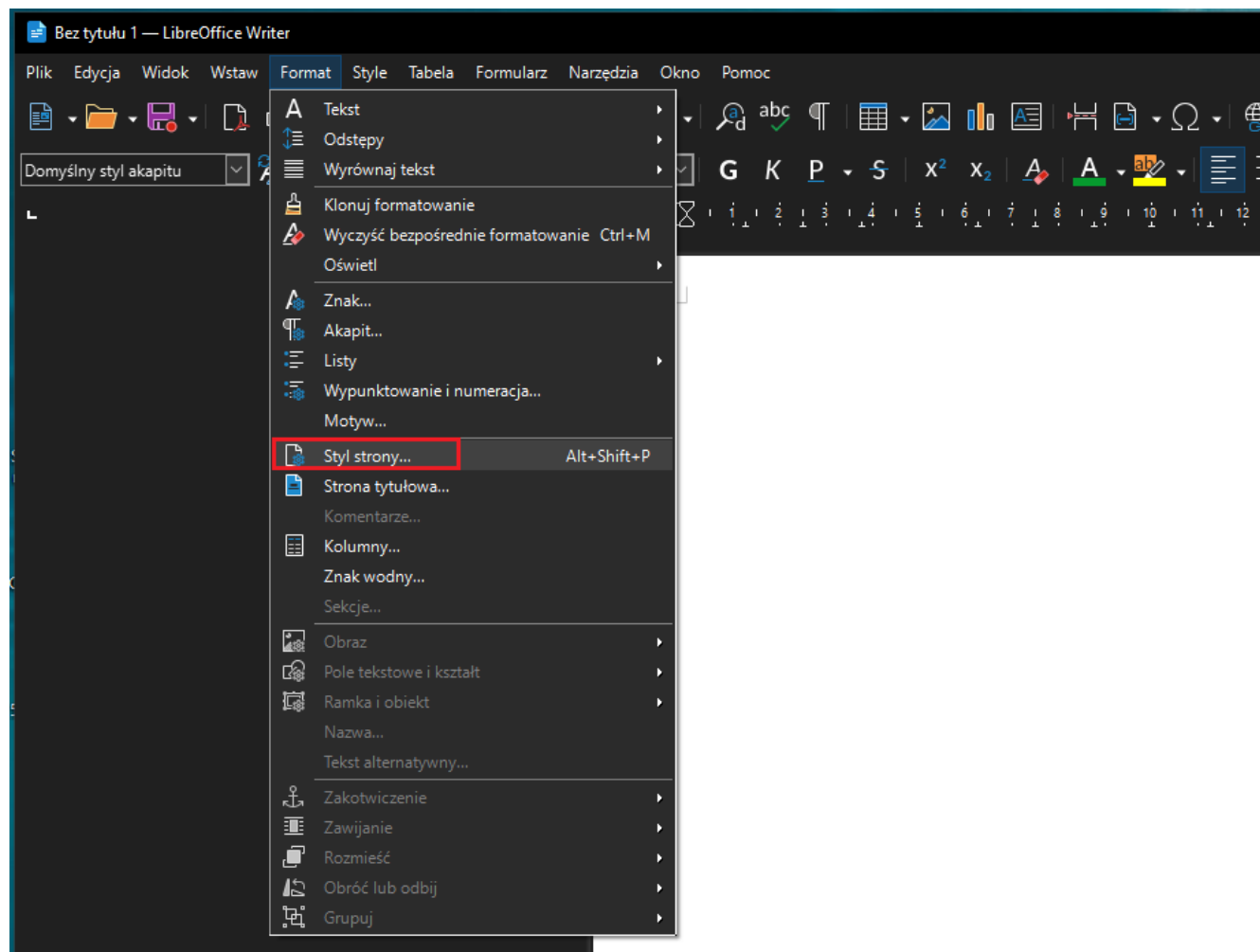
```
0000  ac 84 c6 31 bb cf 18 24 a1 3b ae dc 08 00 45 00  ... 1..k5;...E-
0010  00 46 77 a7 00 00 80 11 9a 85 0a 0a 0a 6b 14 00  -FW-----k--
0020  00 06 cb 56 00 35 00 32 d8 b7 f2 a1 01 00 00 01  -V-5:2 .....
0030  00 00 00 00 00 00 05 77 69 6e 31 30 04 69 70 76  -.....w in10-ipv
0040  36 09 6d 69 63 72 6f 73 6f 66 74 03 63 6f 6d 00  6-micros oft-com
0050  00 01 00 01
```

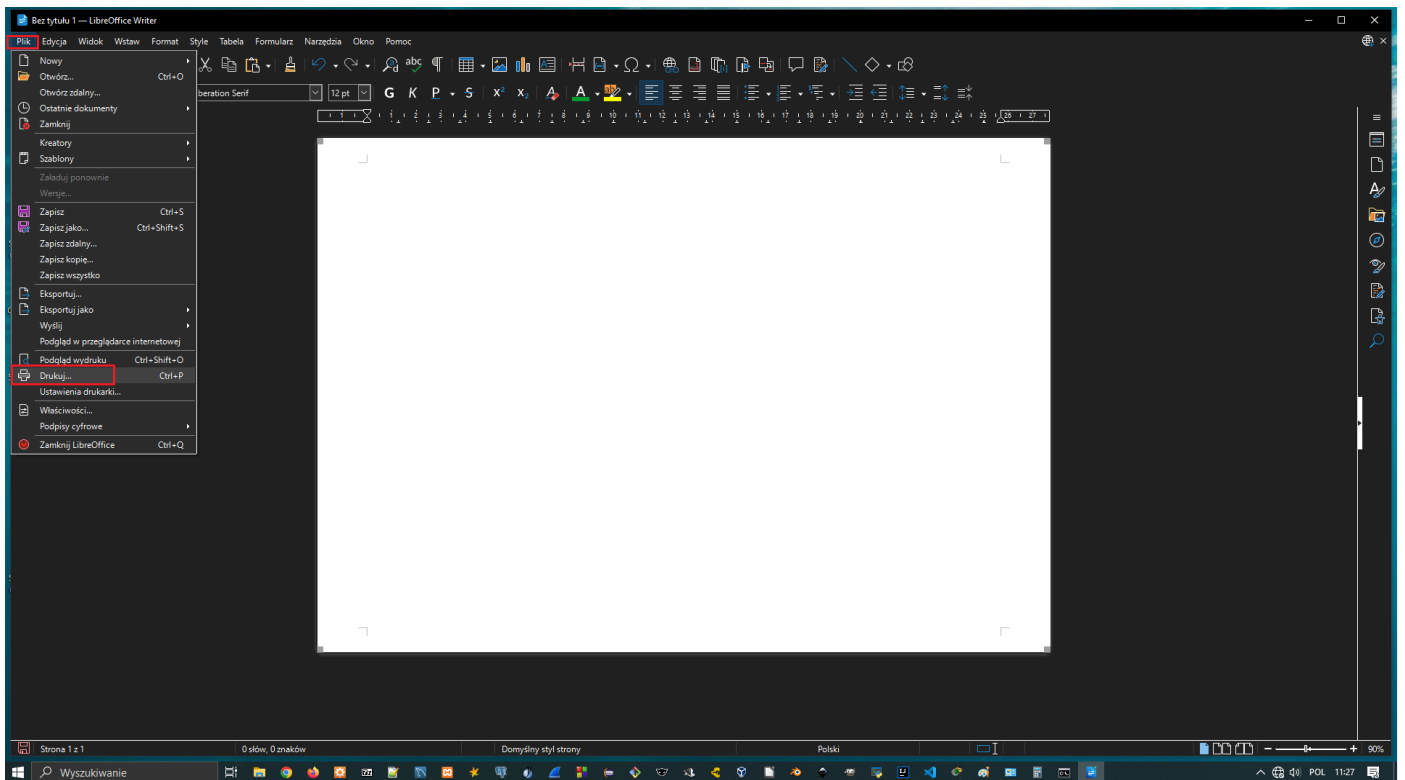
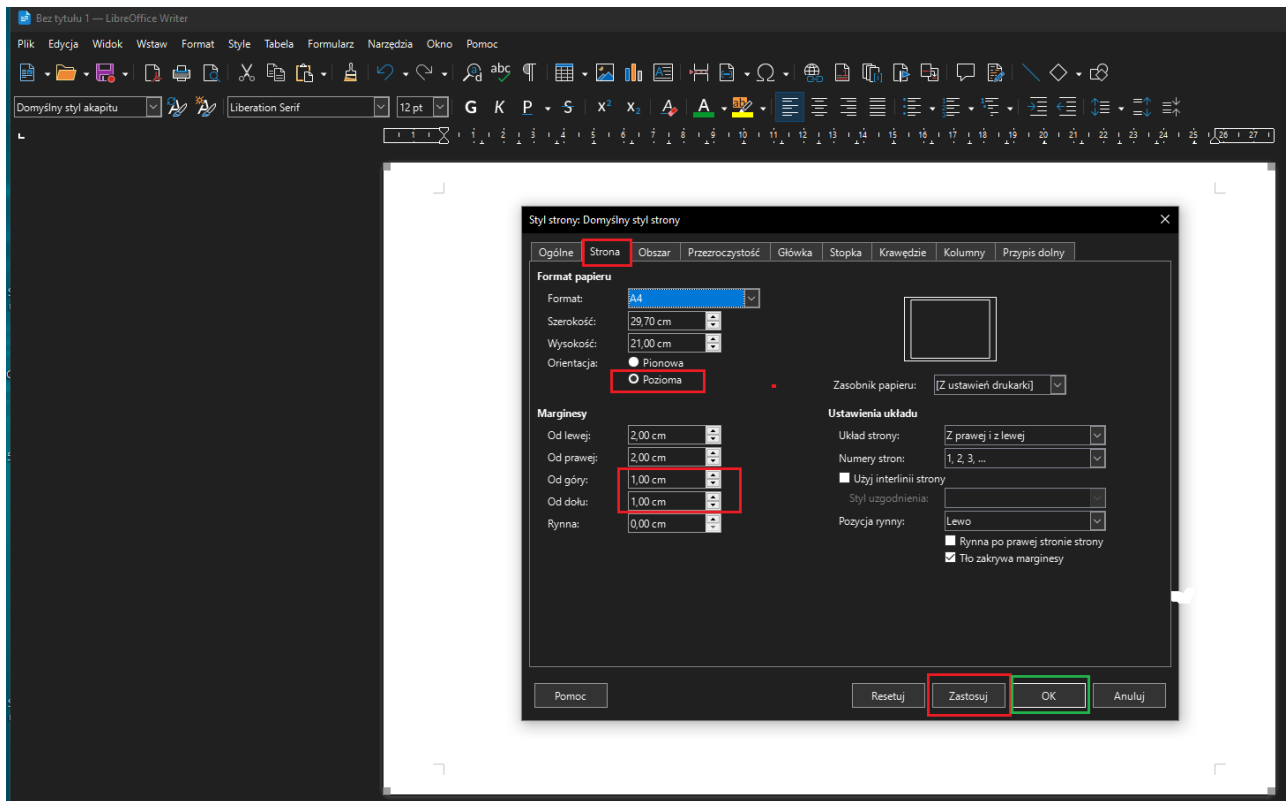
The status bar at the bottom indicates: Pakietów: 77 - Wyświetlonych: 77 (100.0%) - Porzuconych: 0 (0.0%)

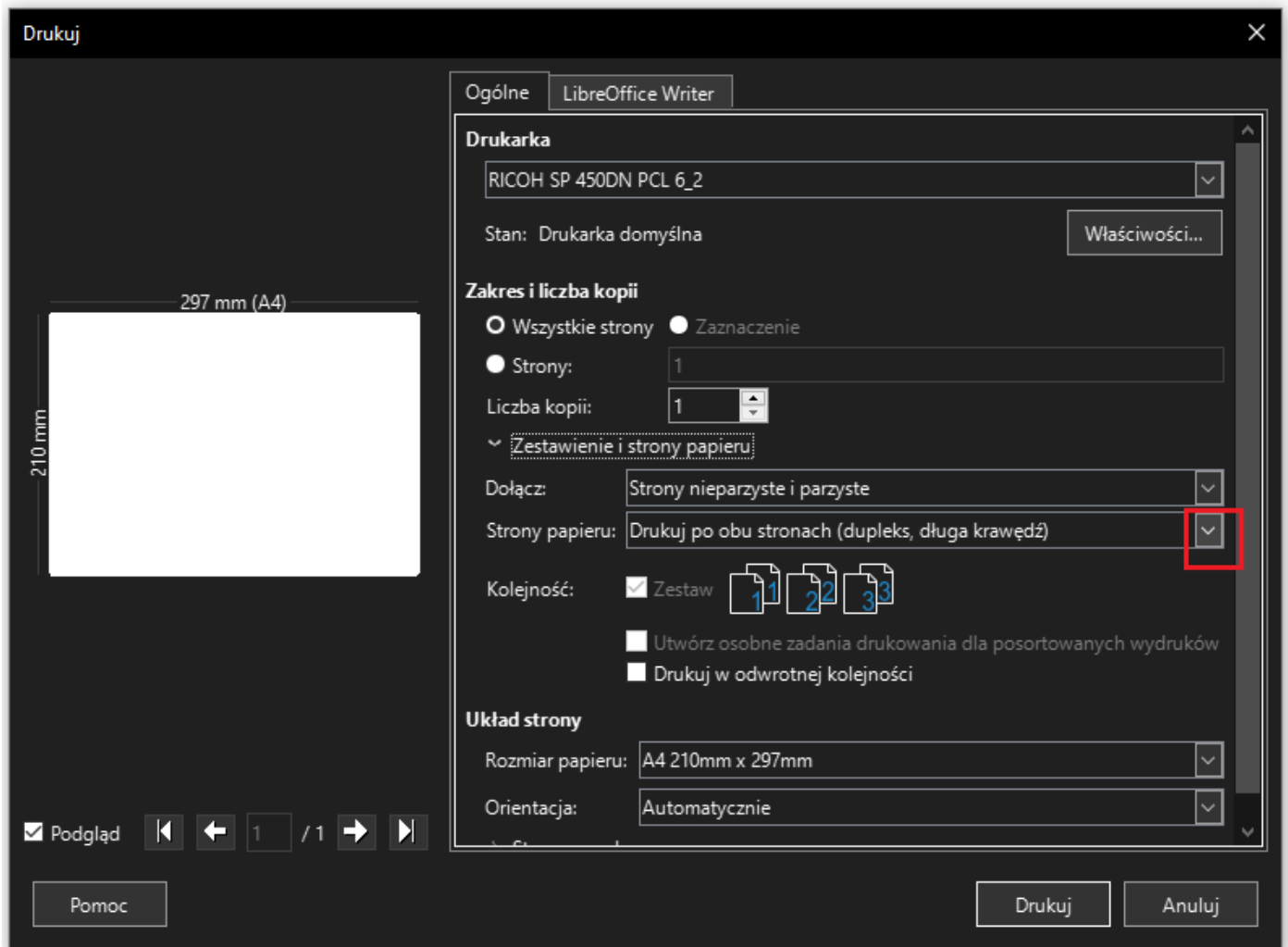
6.3 Drukowanie dwustronne na krótkiej krawędzi w sytemie Windows

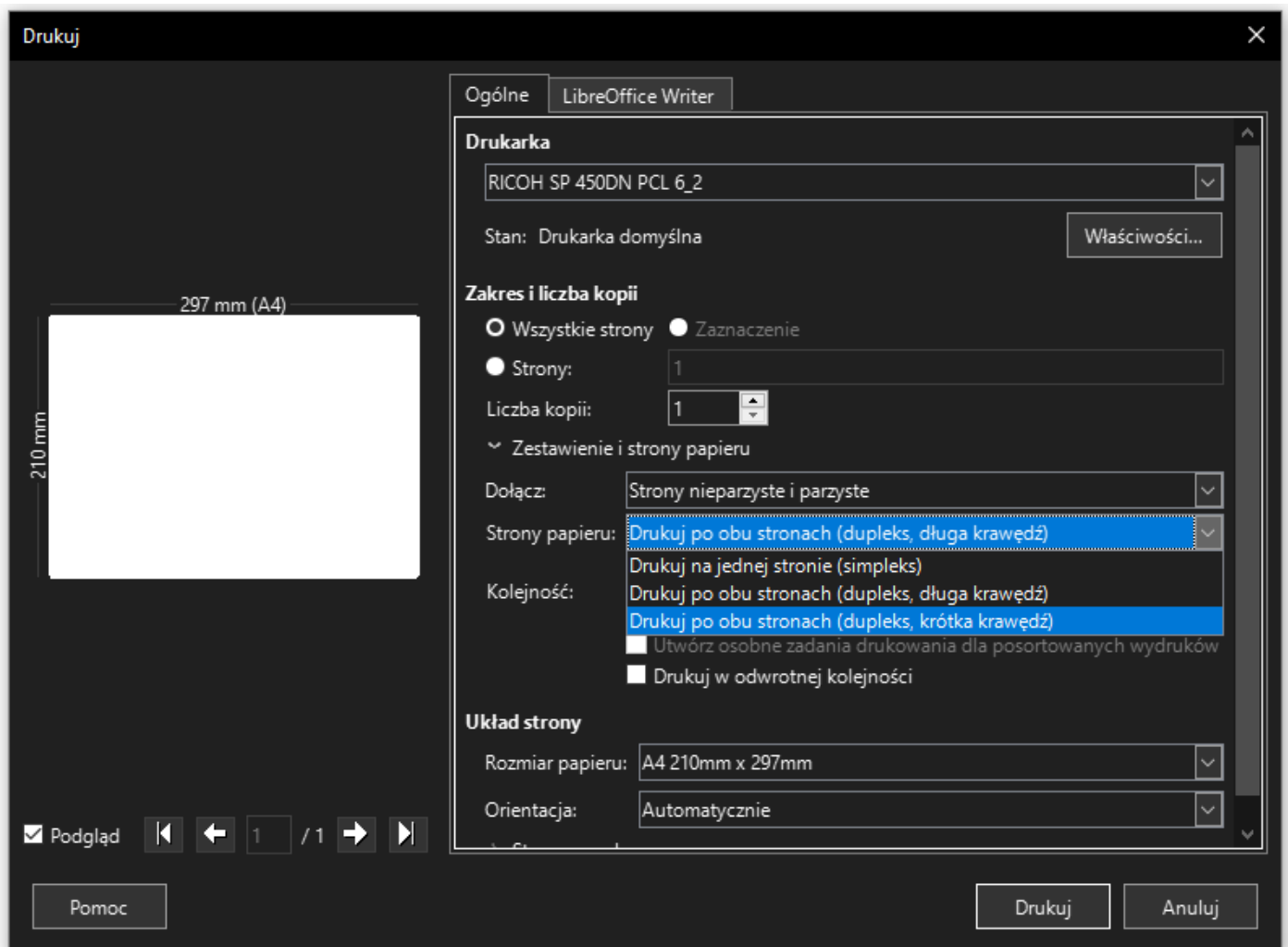
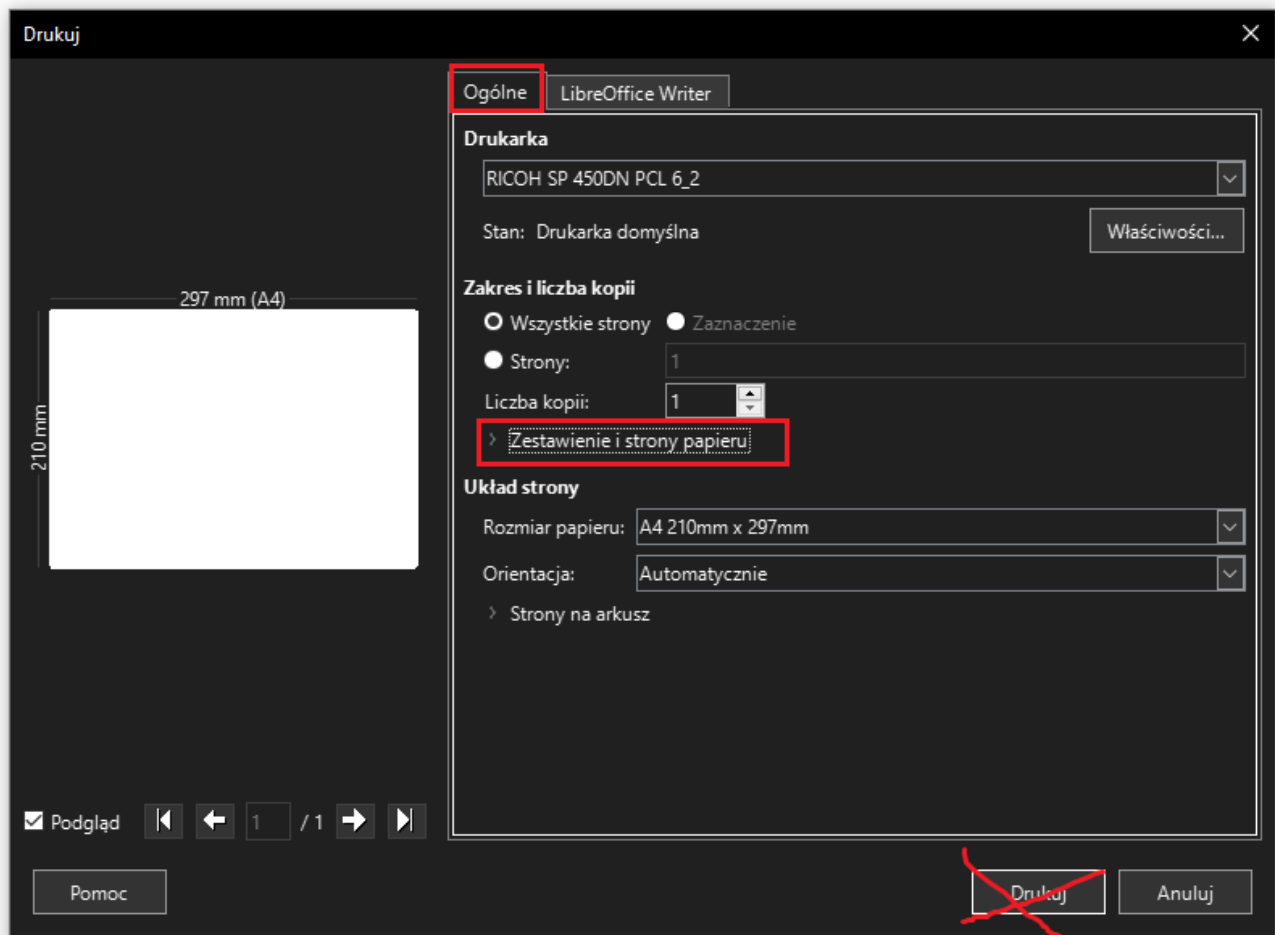
1. Zainstaluj sterownik drukarki.

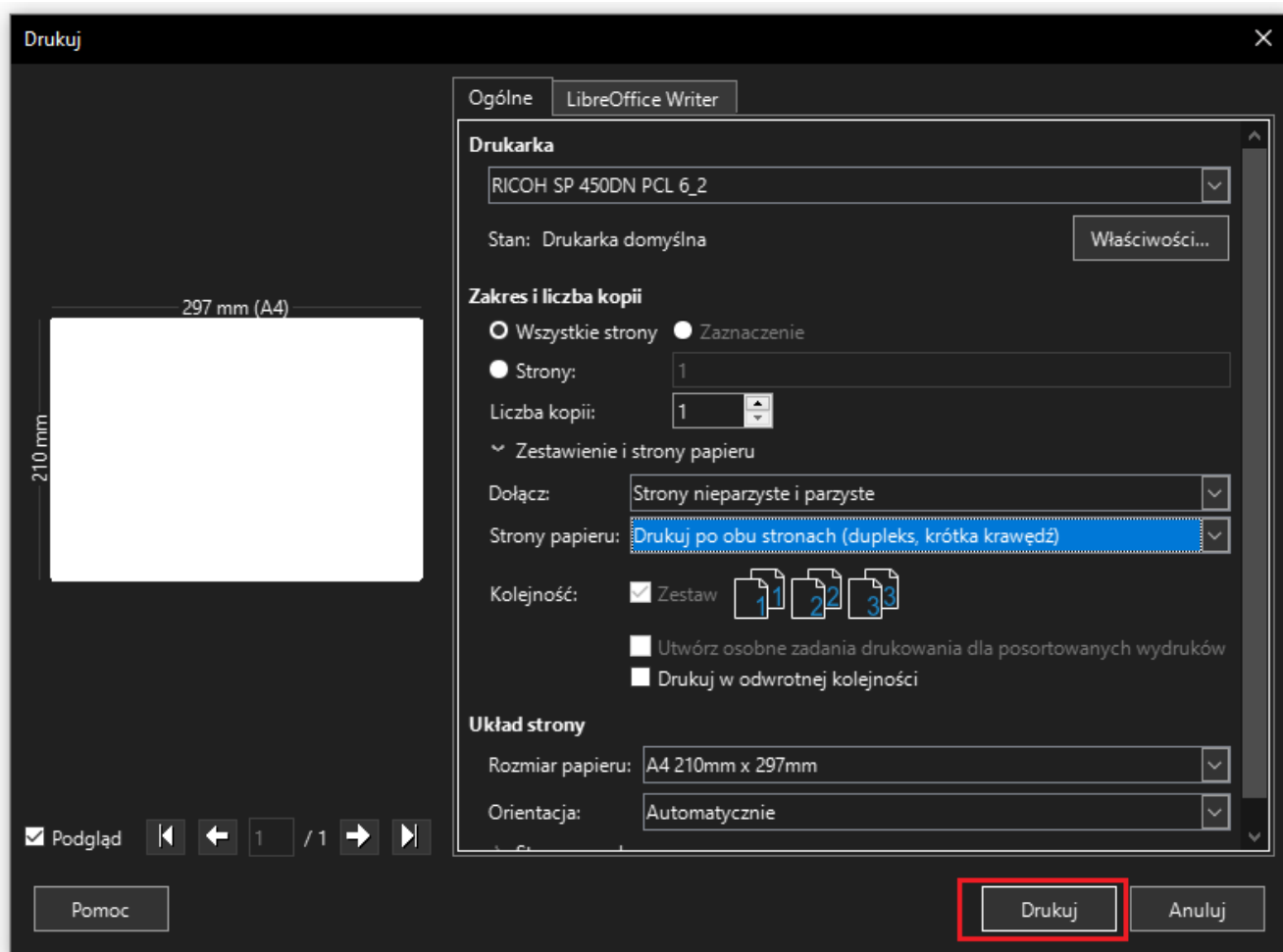
2. Konfiguracja w LibreOffice



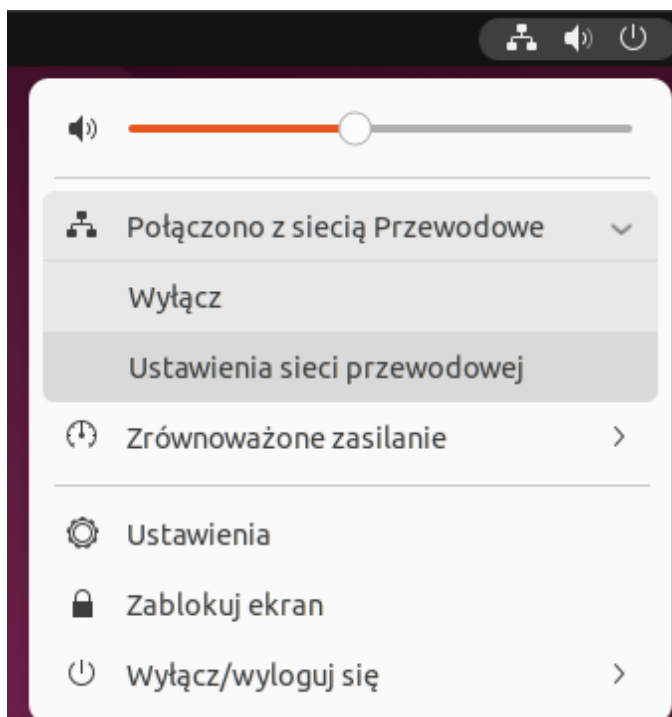
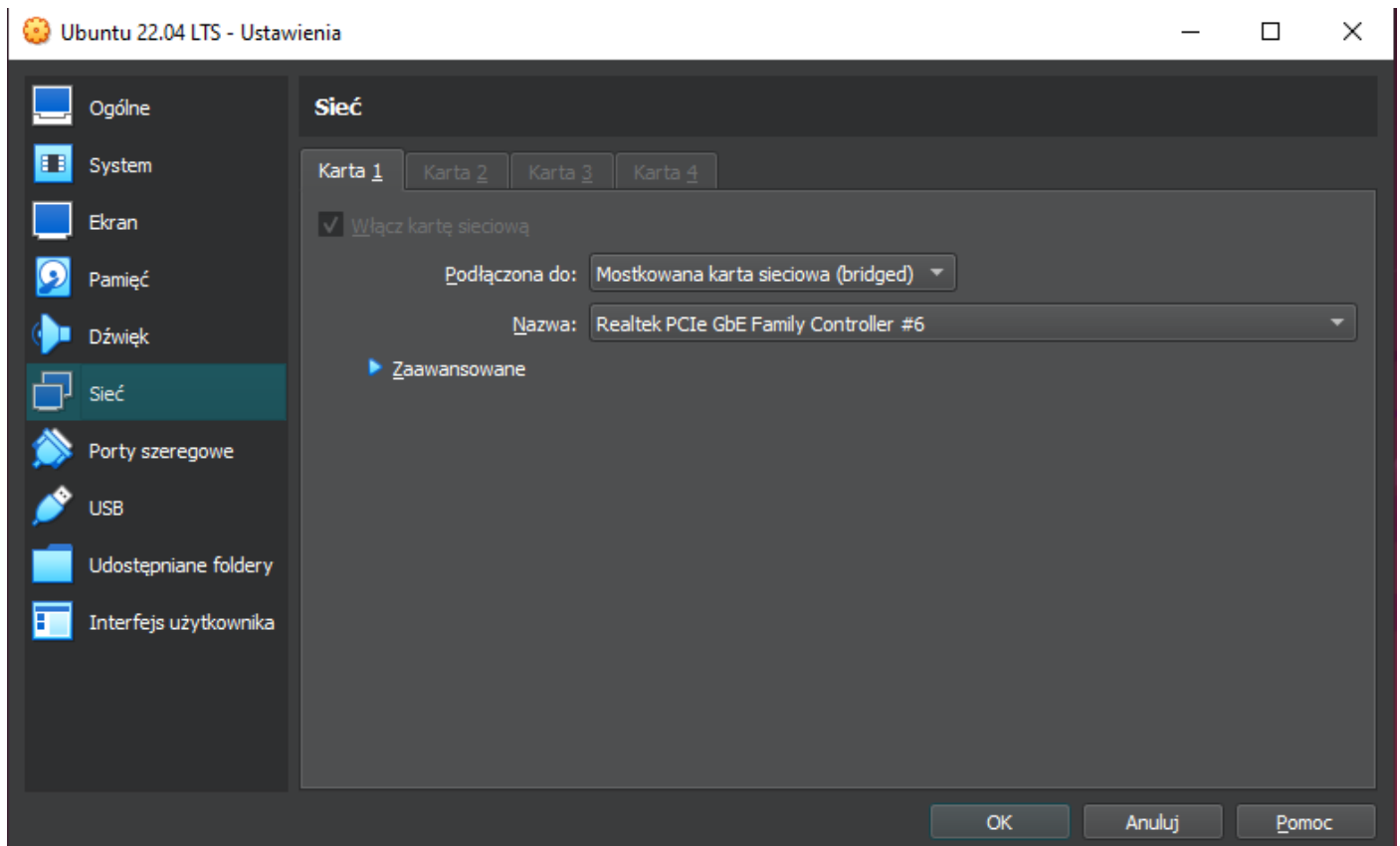


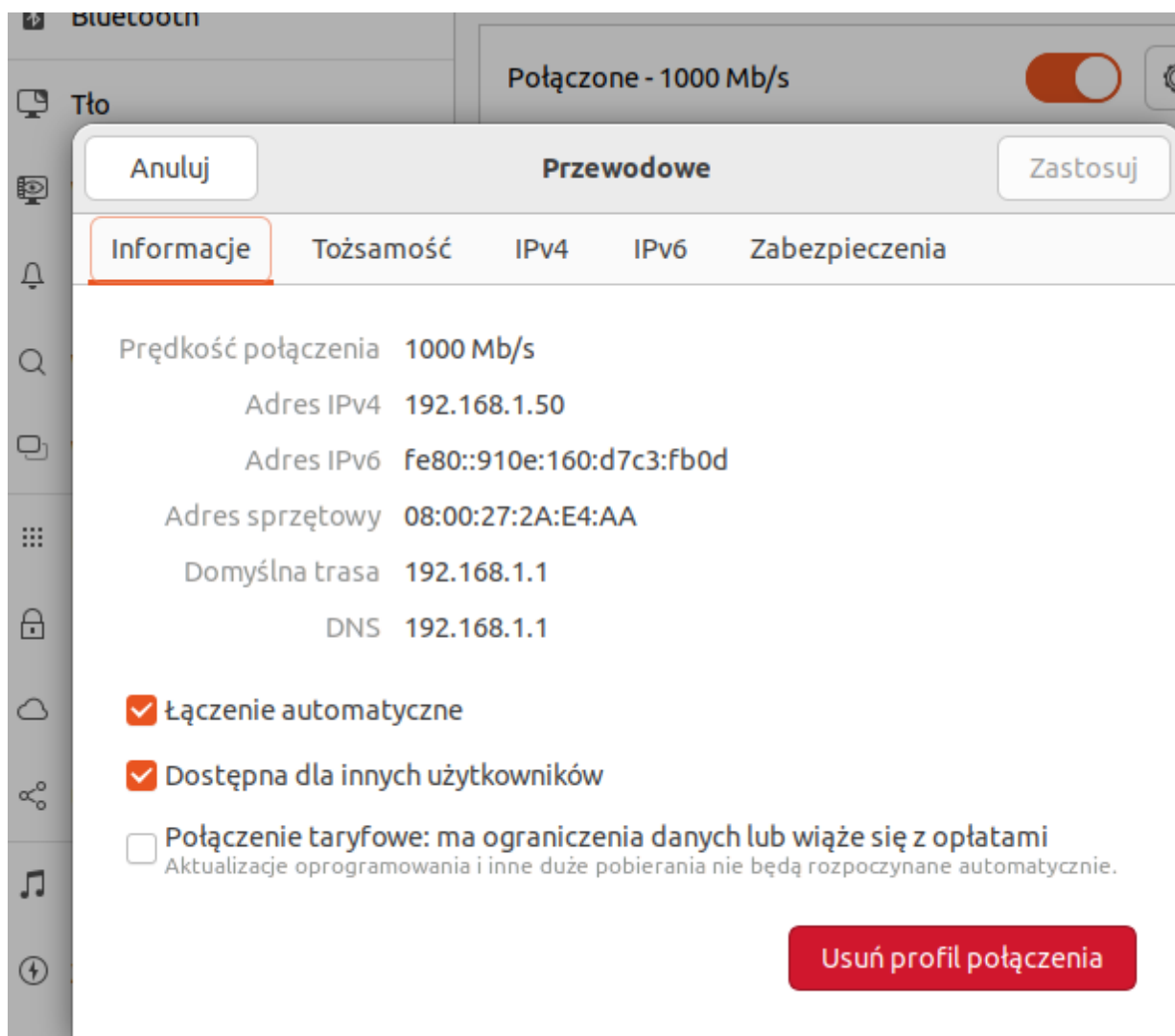
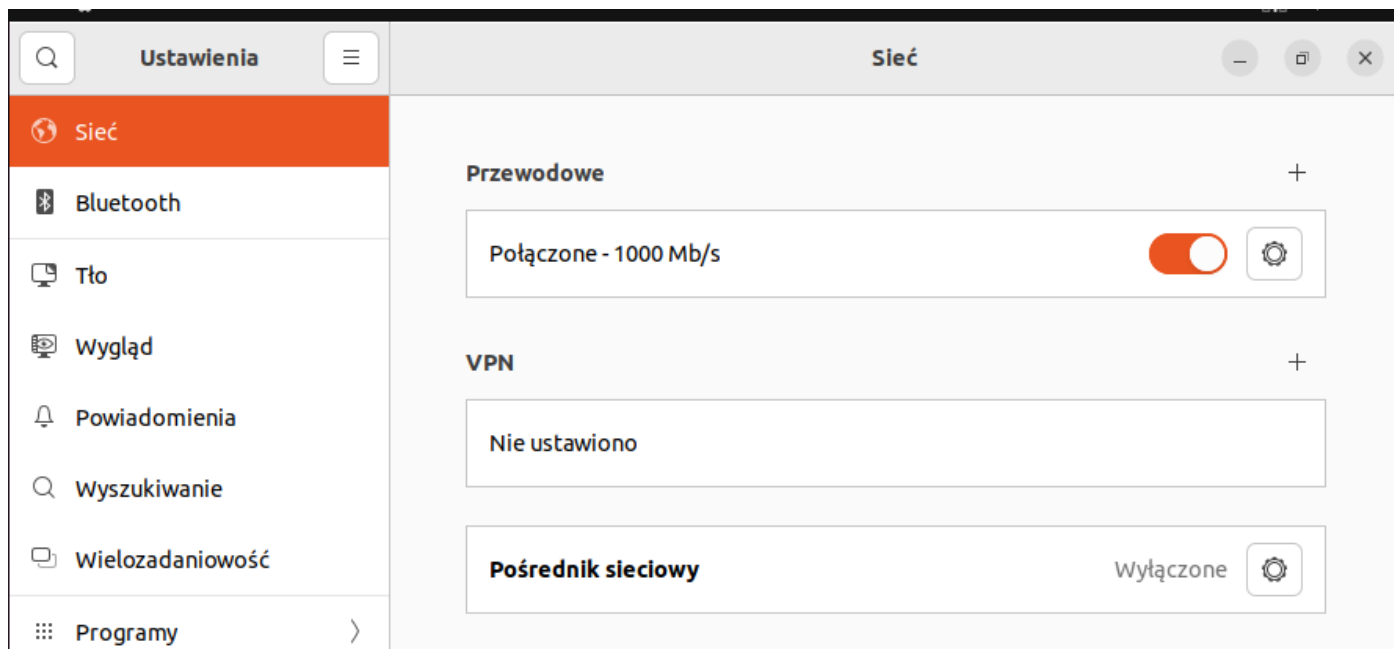


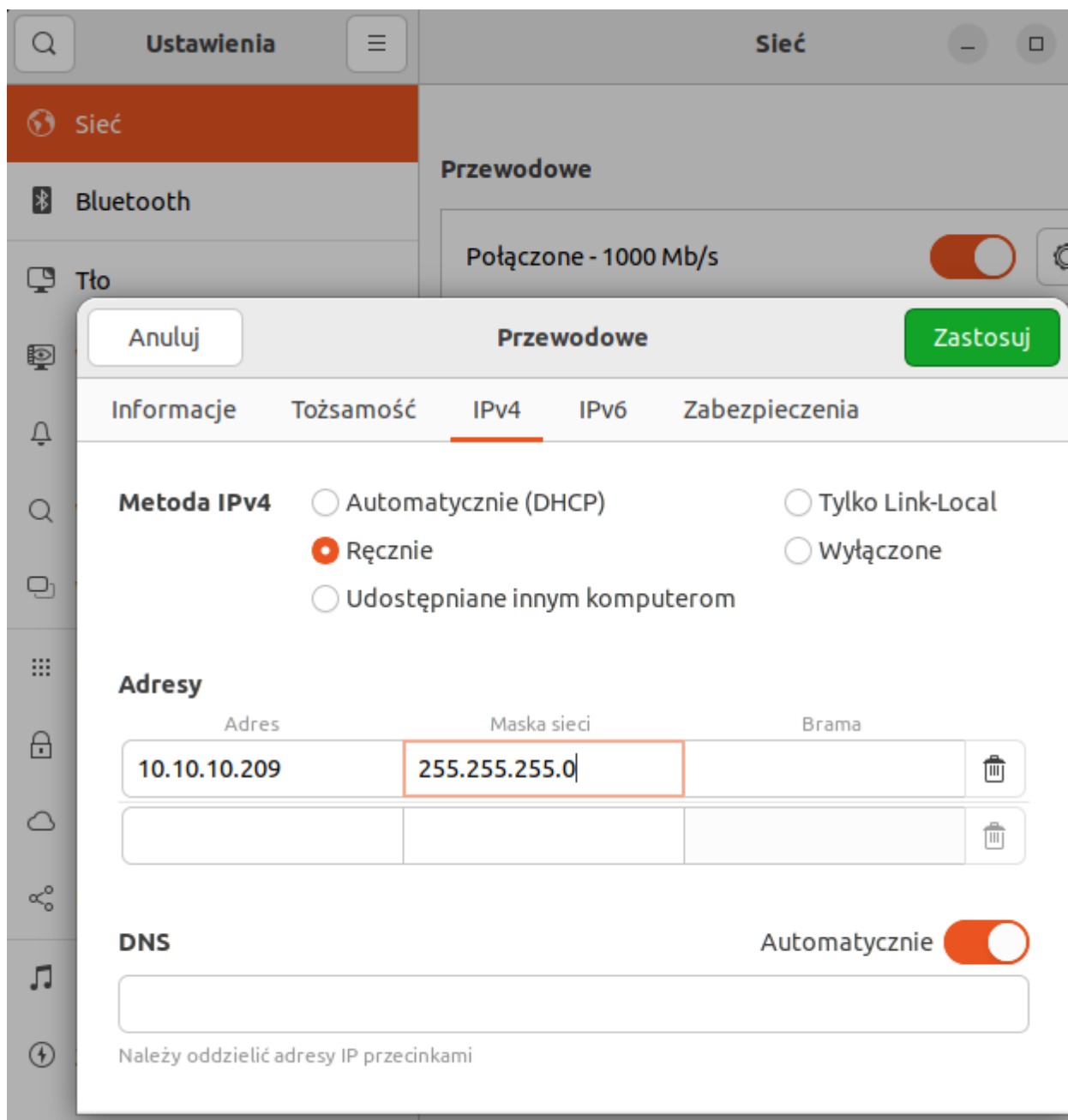




6.4 Drukowanie dwustronne na długiej krawędzi w sytemie Linux

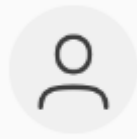






Wymagane jest uwierzytelnienie

Ustawienia systemu uniemożliwiają modyfikację ustawień sieciowych dla wszystkich użytkowników

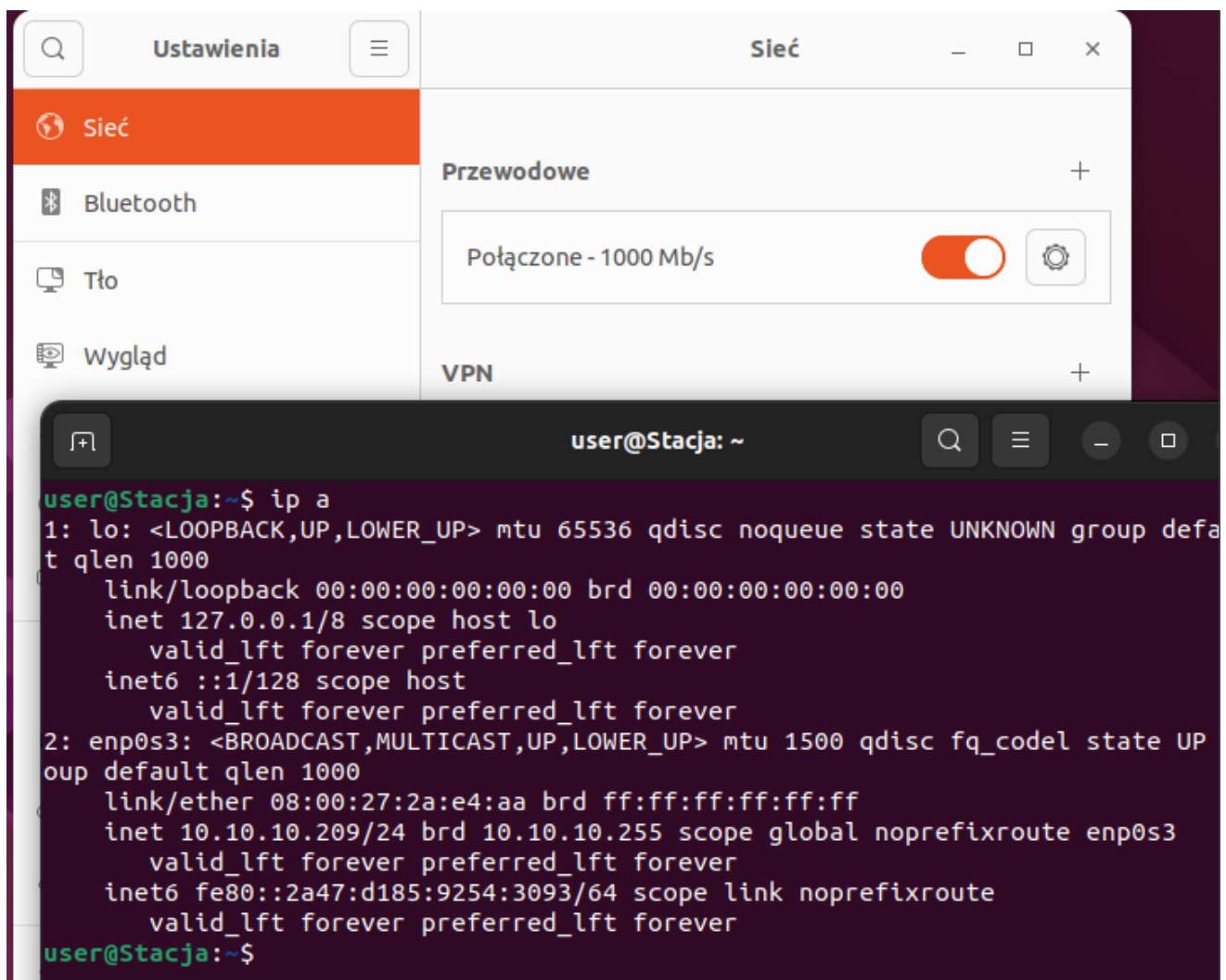
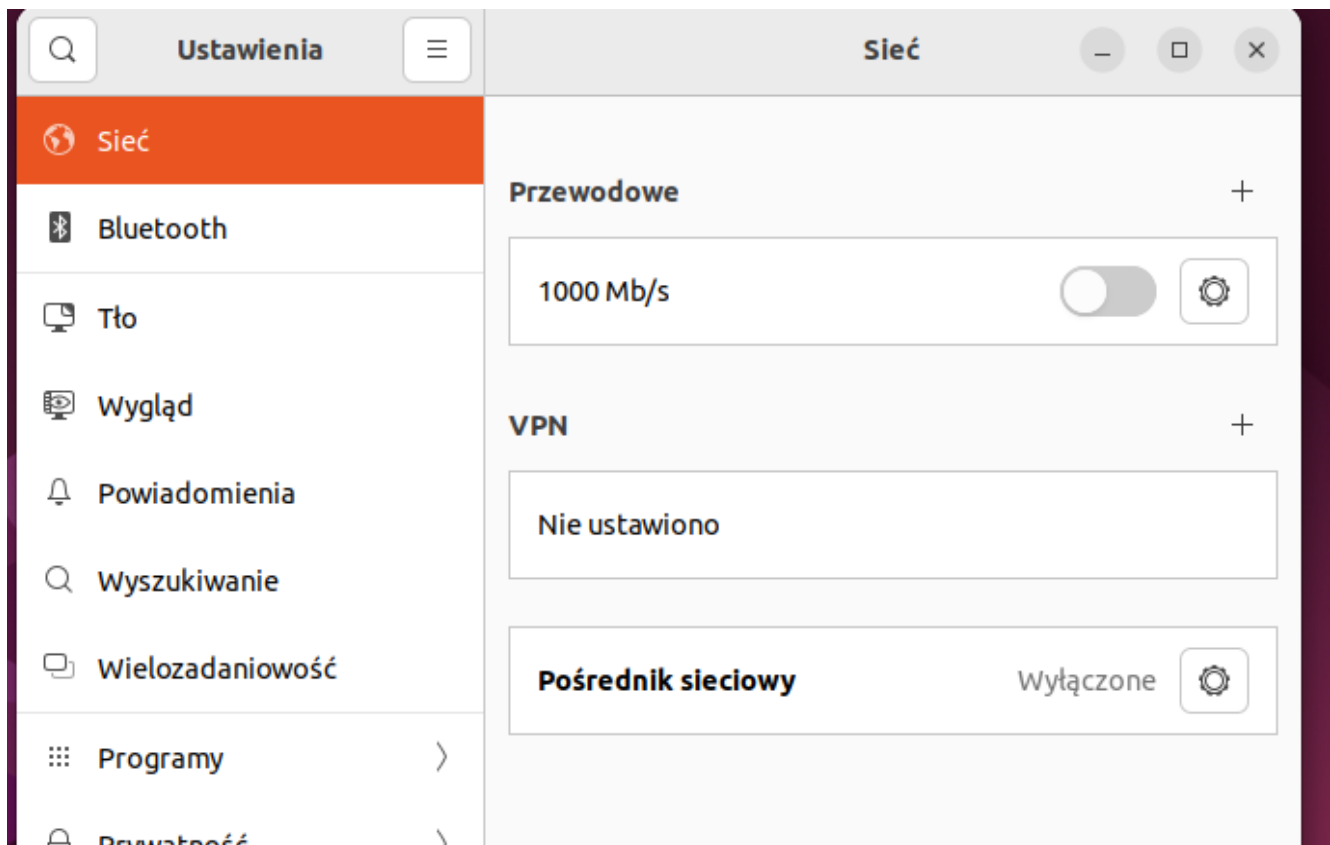


Administrator

Anuluj

Uwierzytelnij

```
Podgląd Terminal 7 mar 08:38
user@Stacja: ~
user@Stacja:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:2a:e4:aa brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.50/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
        valid_lft 35483sec preferred_lft 35483sec
    inet6 fe80::910e:160:d7c3:fb0d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
user@Stacja:~$
```

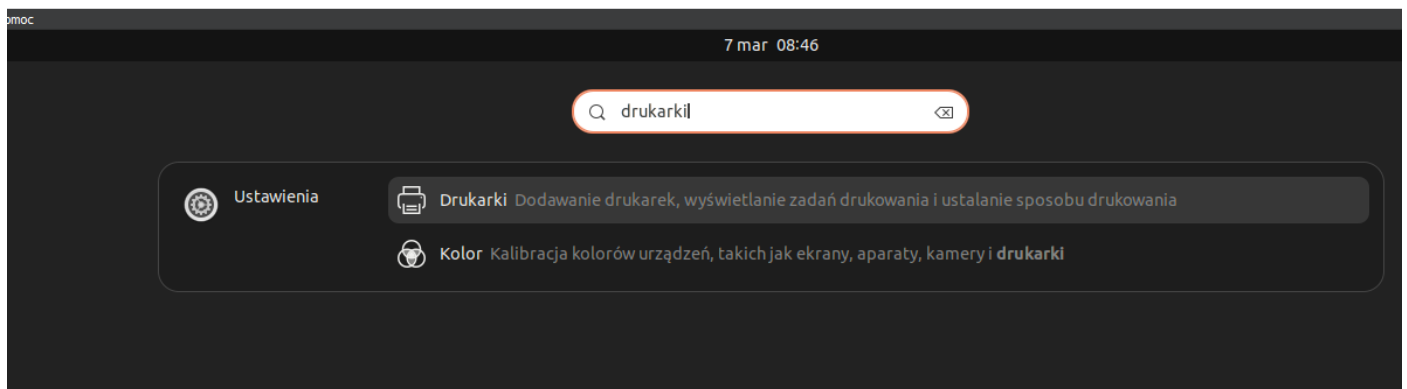


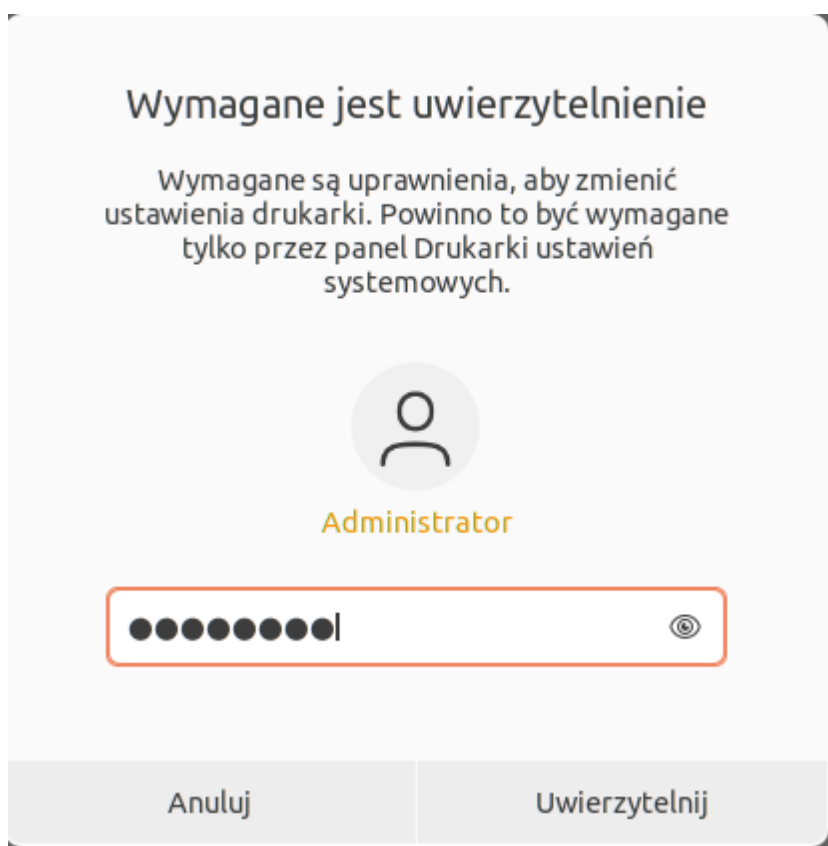
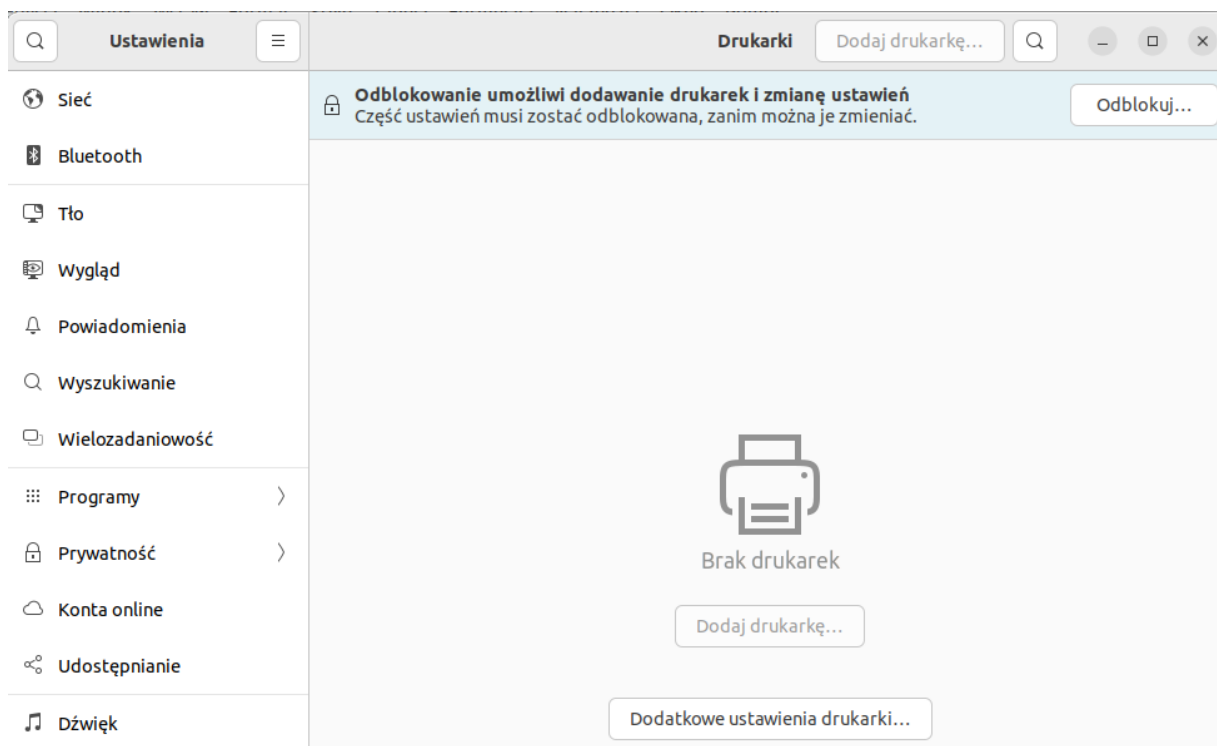
drukowanie dwustronne
na długiej krawędzi.

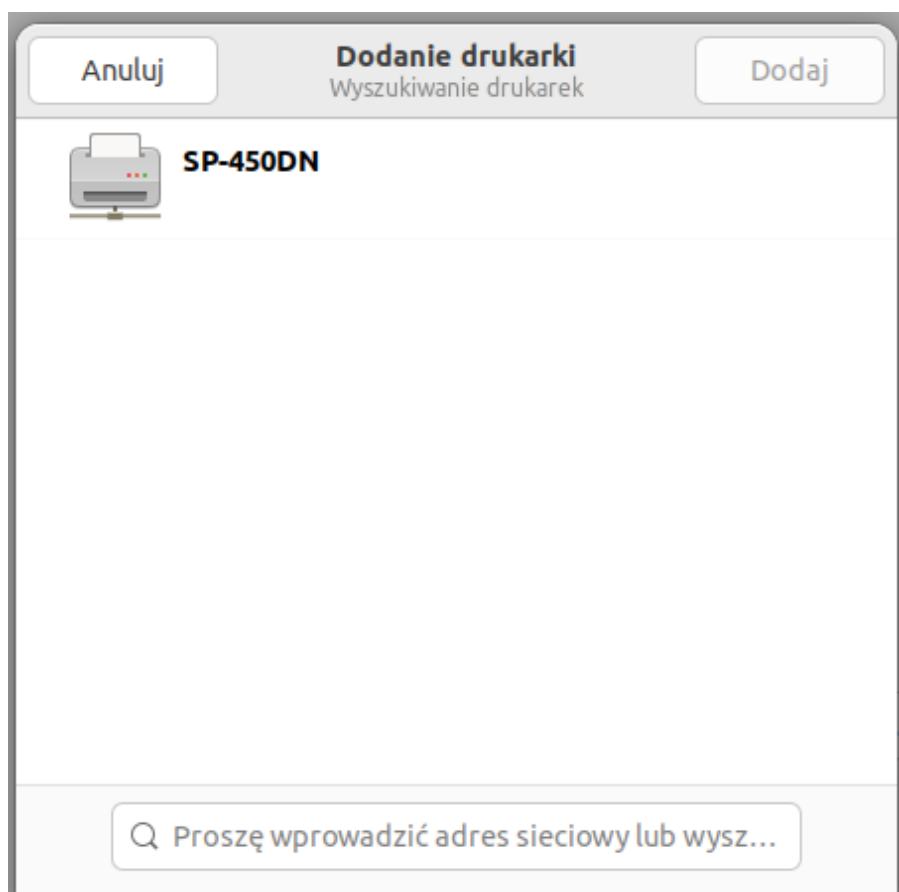
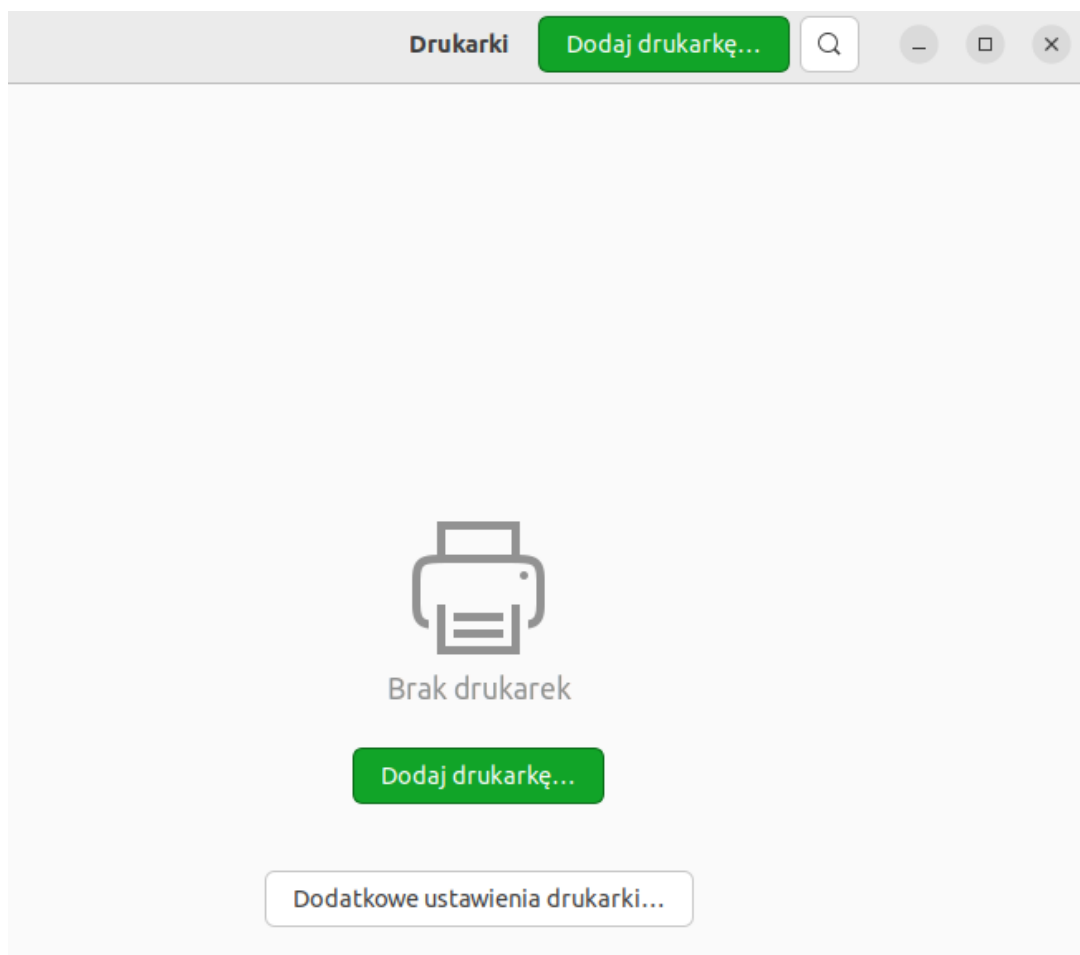
Margines górny i dolny 1,5 cm

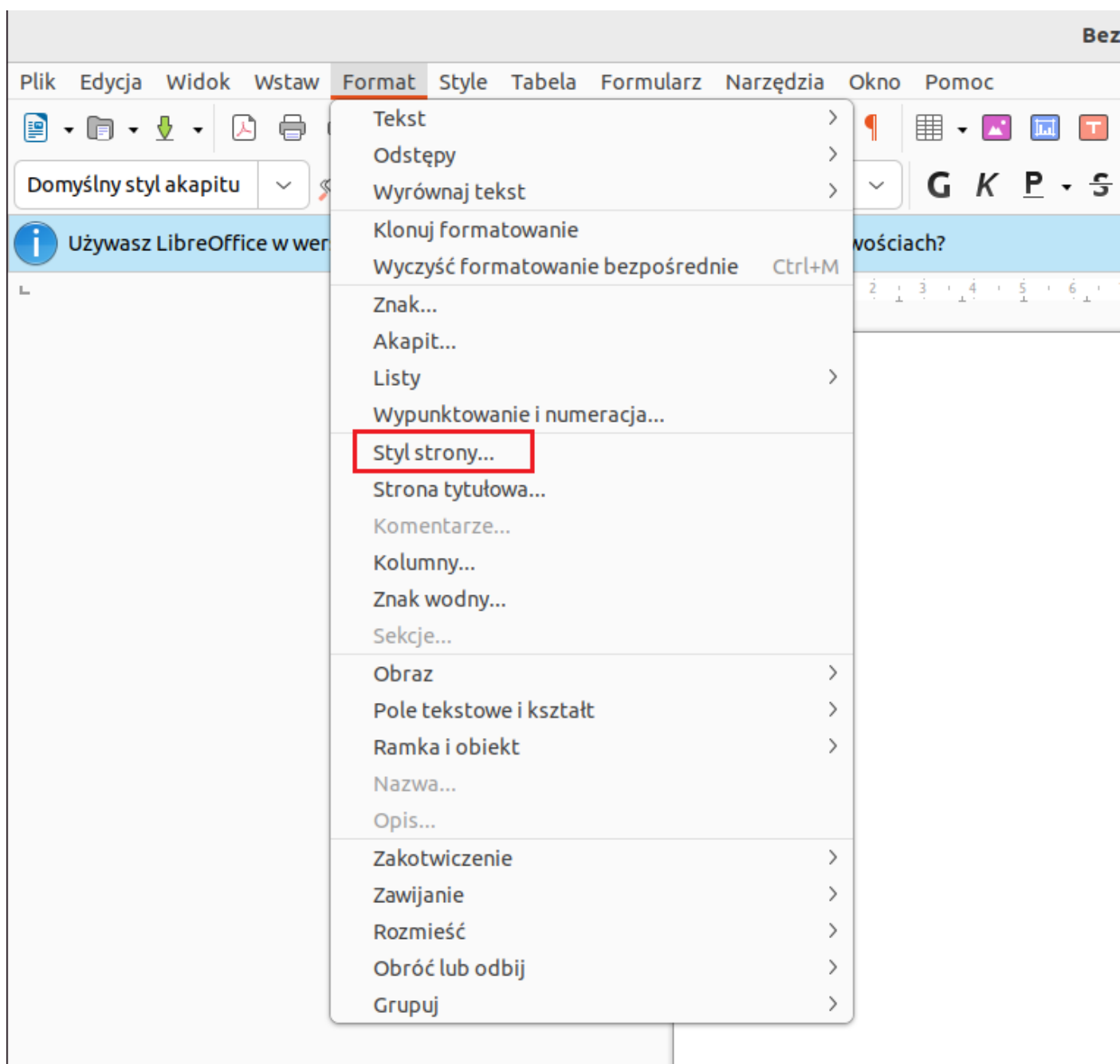
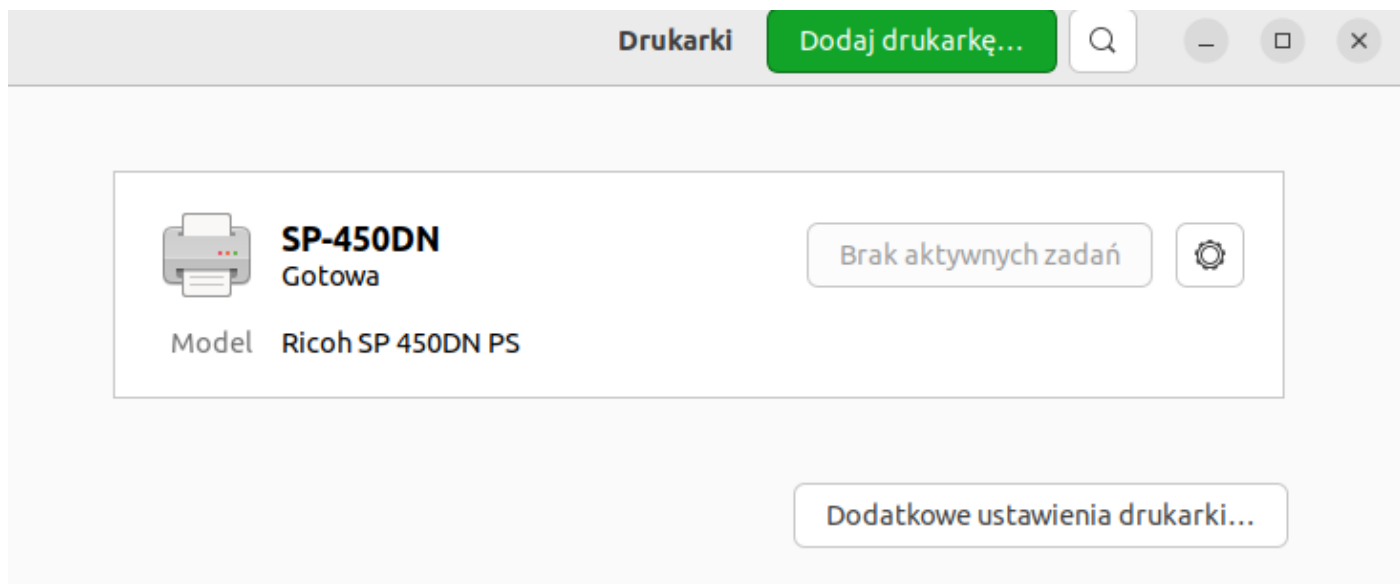
```
user@Stacja: ~  
user@Stacja:~$ ping 10.10.10.241  
PING 10.10.10.241 (10.10.10.241) 56(84) bytes of data.  
64 bytes from 10.10.10.241: icmp_seq=1 ttl=255 time=0.501 ms  
64 bytes from 10.10.10.241: icmp_seq=2 ttl=255 time=0.512 ms  
64 bytes from 10.10.10.241: icmp_seq=3 ttl=255 time=0.546 ms  
64 bytes from 10.10.10.241: icmp_seq=4 ttl=255 time=0.588 ms  
64 bytes from 10.10.10.241: icmp_seq=5 ttl=255 time=0.486 ms  
64 bytes from 10.10.10.241: icmp_seq=6 ttl=255 time=0.565 ms  
^C  
--- 10.10.10.241 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5103ms  
rtt min/avg/max/mdev = 0.486/0.533/0.588/0.036 ms  
user@Stacja:~$
```

Oracle VM VirtualBox









Styl strony: Domyślny styl strony

Organizator

Strona

Obszar

Przezroczystość

Główka

Stopka

Krawędzie

Kolumny

Przypis dolny

Styl

Nazwa:

Domyślny styl strony

Następny styl:

Domyślny styl strony

Edytuj syl

Dziedziczenie po:

Edytuj styl

Kategoria:

Style niestandardowe

Zawiera

29,7 cm + Od góry 2,0 cm, Od dołu 2,0 cm + Kierunek tekstu od lewej do prawej (poziomo) + Opis strony: Arabski, Orientacja pionowa, Wszystko + Domyślny styl strony + Z wyjątkiem odstępów między wierszami na stronie

Styl strony: Domyślny styl strony

Organizator

Strona

Obszar

Przezroczystość

Główka

Stopka

Krawędzie

Kolumny

Przypis dolny

Format papieru

Format:

A4

Szerokość:

29,70 cm

–

+

Wysokość:

21,00 cm

–

+

Orientacja:

☐ Pionowa

☒ Pozioma

Zasobnik papieru:

[Z ustawień drukarki]

Ustawienia układu

Układ strony:

Z prawej i z lewej

Numery stron:

1, 2, 3, ...

Styl uzgodnienia:

Pozycja rynny:

Lewo

☐ Użyj odstępów między wierszami na stronie

☐ Rynna po prawej stronie strony

☒ Tło zakrywa marginesy

Marginesy

Od lewej:

2,00 cm

–

+

Od prawej:

2,00 cm

–

+

Od góry:

1,50 cm

–

+

Od dołu:

1,50 cm

–

+

Rynna:

0,00 cm

–

+

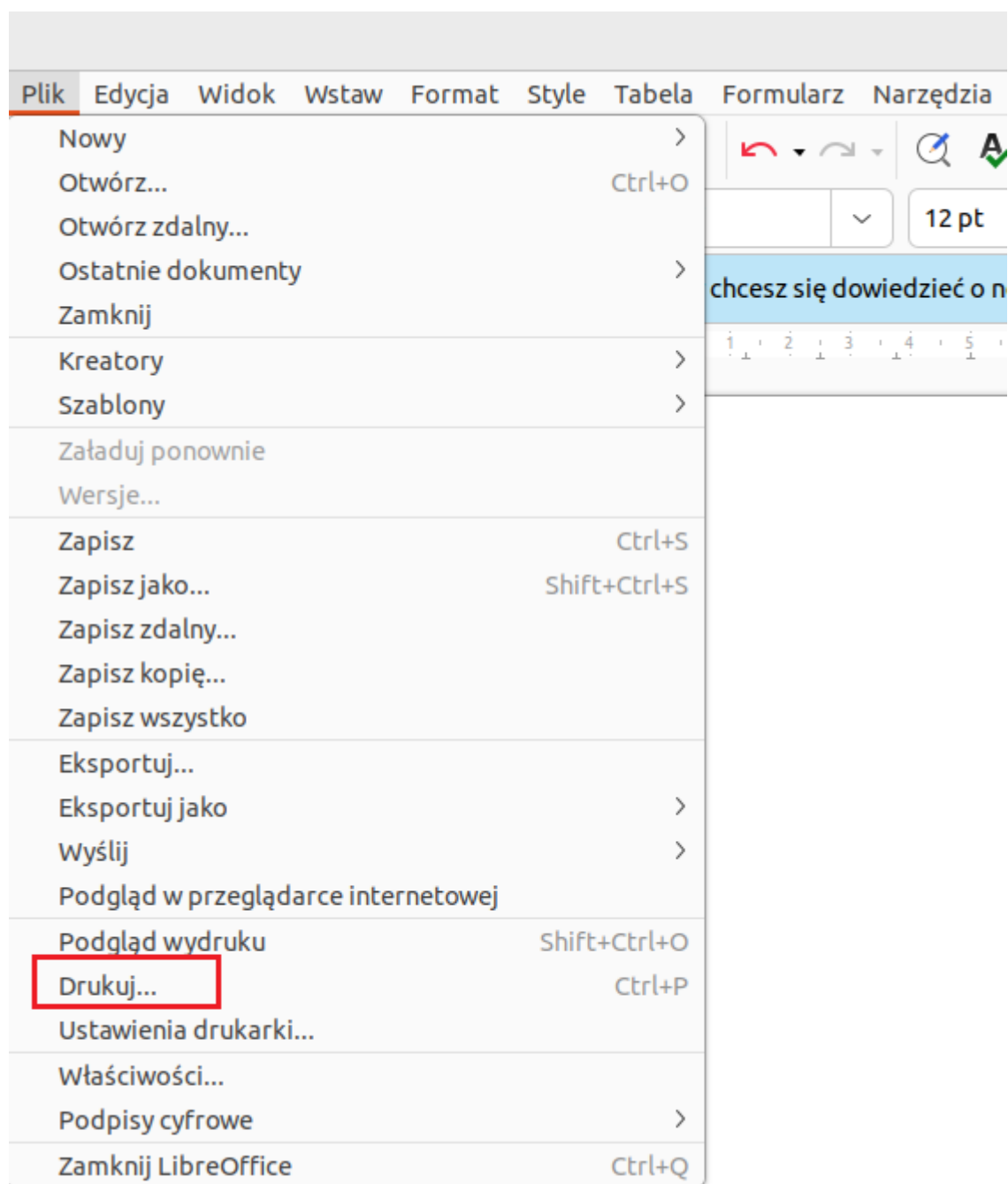
Pomoc

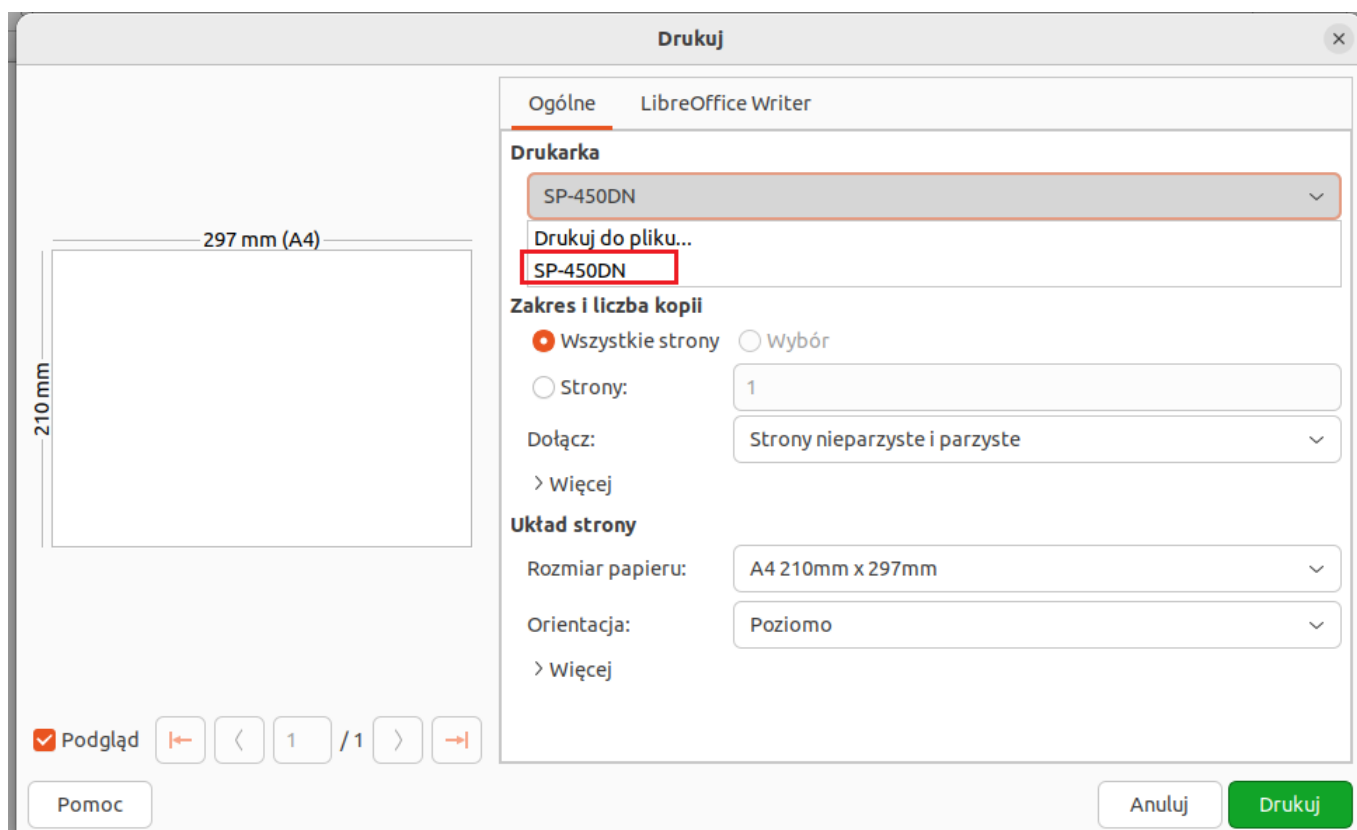
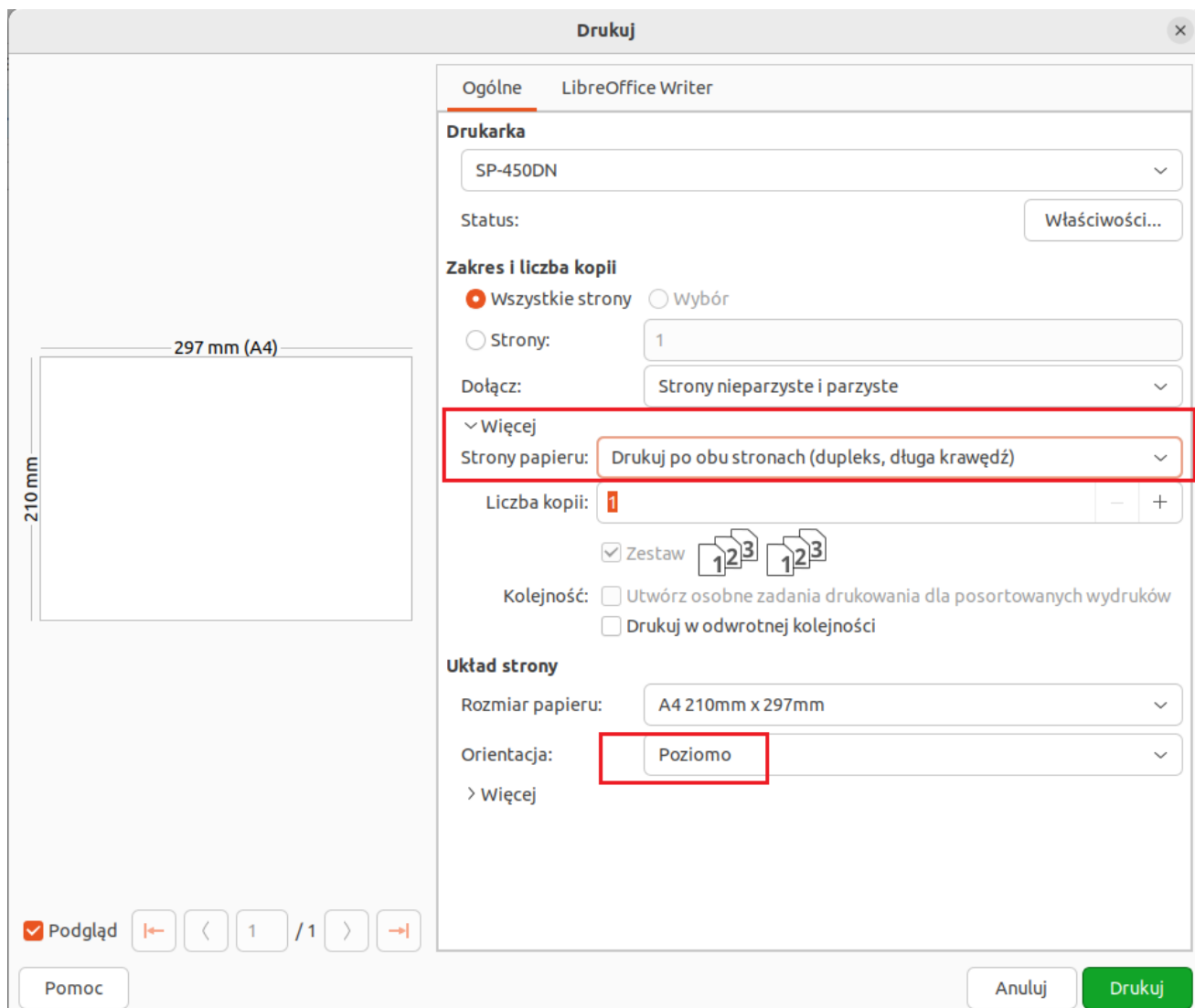
Resetuj

Zastosuj

Anuluj

OK





7. SERWER UBUNTU

7.1 Ubuntu Serwer – http

Ubuntu Server – HTTP

!!! Skonfiguruj najpierw DNS – strefę domenową z odpowiednimi domenami dla stron www. Pamiętaj o konfiguracji wyszukiwania wstecznego dla rekordów PTR.

Instalacja i konfiguracja podstawowa

Przejdźcie na konto root

sudo su

Instalacja serwera Apache2 i modułu PHP5:

sudo apt-get install apache2 php5

Po instalacji wyżej wymieniony serwer i moduł zostaną automatycznie uruchomione.

Pliki konfiguracyjne:

/etc/apache2/apache2.conf

Trzeba pamiętać, że **apache2.conf** jest głównym plikiem konfiguracyjnym, ale nie jedynym. Kolejny to **/etc/apache2/ports.conf**. Pozostałe pliki konfiguracyjne związane są z modułami, konfiguracjami i witrynami.

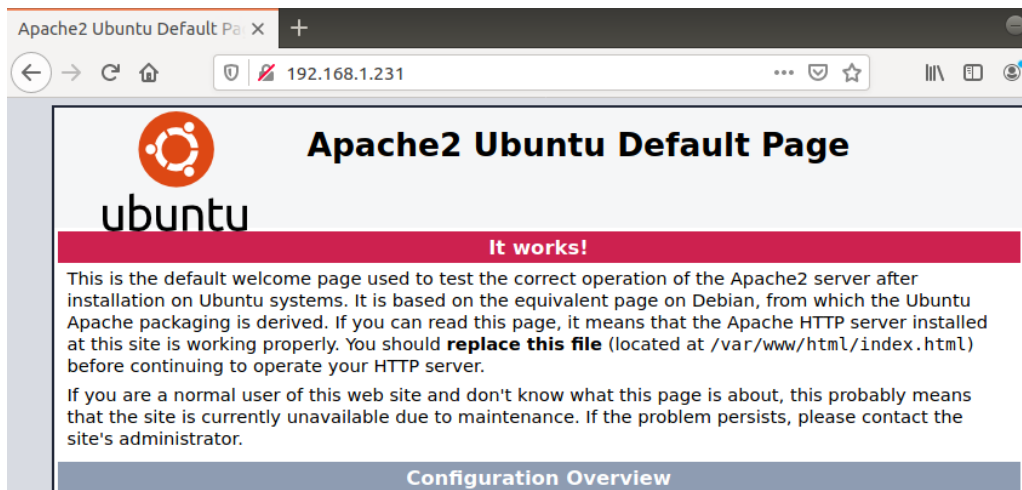
Uruchamianie, zatrzymywanie i reloadowanie usługi serwera http:

service apache2 start

service apache2 stop

service apache2 reload

Sprawdzamy czy serwer http działa. Wpisuję w pasku przeglądarki adres IPv4 serwera www. Po naciśnięciu klawisza ENTER, powinna się wyświetlić domyślna strona Apache2 Ubuntu.



Wyświetlona powyższa strona dostępna jest w katalogu **/var/www/html**.

Otwórzmy plik **index.html** w powyższym katalogu:

```
michal@serwer: /var/www/html
Plik Edycja Widok Wyszukiwanie Terminal Pomoc
/var/www/html/index.html [----] 0 L: [ 1+ 0 1/376] *(0 /10918b) 0010
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www
<html xmlns="http://www.w3.org/1999/xhtml">
  <!--
    Modified from the Debian original for Ubuntu
    Last updated: 2016-11-16
    See: https://launchpad.net/bugs/1288690
  -->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Ubuntu Default Page: It works</title>
    <style type="text/css" media="screen">
      * {
        margin: 0px 0px 0px 0px;
        padding: 0px 0px 0px 0px;
      }

      body, html {
        padding: 3px 3px 3px 3px;

        background-color: #D8DBE2;

        font-family: Verdana, sans-serif;
        font-size: 11pt;
        text-align: center;
      }
    </style>
  </head>
  <div style="text-align: center;">
    <div style="display: inline-block; width: 45%; vertical-align: top;">
      <h1>Apache2 Ubuntu Default Page: It works</h1>
    </div>
  </div>
</html>
```

Plik można modyfikować według uznania. Gdyby ktoś chciał zakończyć konfigurację serwera na tym poziomie to może, ponieważ strona www jest dostępna pod adresem IPv4 serwera Apache2.

Jeżeli chcemy udostępnić stronę www na domenę, to należy odpowiednio skonfigurować serwer DNS, dodatkowo jeśli chcemy mieć więcej dostępnych witryn obsługiwanych przez jeden serwer http, musimy odpowiednio skonfigurować nasz Apache2.

Stworzymy dodatkową witrynę www, a do tego potrzebne nam będą dodatkowe polecenia (skrypty):

1. Aktywacja i deaktywacja witryn
 - **a2ensite**
 - **a2dissite**
2. Aktywacja i deaktywacja modułów
 - **a2enmod**
 - **a2dismod**
3. Aktywacja i deaktywacja konfiguracji
 - **a2enconf**
 - **a2disconf**

wstawka w poleceniach **-en** – pochodzi od słowa **enable**

wstawka w poleceniach **-dis** – pochodzi od słowa **disable**

Kopiowanie oryginalnego katalogu **apache2.conf**

cp /etc/apache2/apache2.conf /etc/apache2/apache2.conf.org

Edytujemy plik **apache2.conf** i dołączamy do niego dodatkowe pliki konfiguracyjne. Proces ten nazywamy includowaniem od słowa **include** z języka programowania

Po usunięciu wszystkich komentarzy i pogrupowaniu wpisów plik prezentuje się następująco:

```
GNU nano 2.9.3                                apache2.conf

#-----dodatkowe pliki konfiguracyjne-----
IncludeOptional mods-enabled/*.load
IncludeOptional mods-enabled/*.conf

Include ports.conf

IncludeOptional conf-enabled/*.conf
IncludeOptional sites-enabled/*.conf

#-----konfiguracja katalogów-----
<Directory />
    Options FollowSymLinks
    AllowOverride None
    Require all denied
</Directory>

<Directory /usr/share>
    AllowOverride None
    Require all granted
</Directory>

<Directory /var/www/>
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>

#-----pliki .ht*-----
AccessFileName .htaccess

<FilesMatch ".ht">
    Require all denied
</FilesMatch>
```

<Directory /> Pierwsze wystąpienie dyrektywy blokuje dostęp do katalogu głównego naszego serwera http. Serwer www nie będzie mógł przeglądać katalogu głównego.

Poniższe katalogi są dostępne dla serwera www.

<Directory /usr/share>

<Directory /var/www>

Pliki **.ht*** , są to specjalne pliki, które powodują że serwer będzie działał inaczej w danej lokalizacji, w danym katalogu, który przegląda niż w całej witrynie. Pierwszy parametr **AccessFileName** określa nazwę takich plików i jest to **.htaccess** i nie ma sensu tego zmieniać.

Druga dyrektywa **<FileMatch "\.ht"> Require All deny** określa zabezpieczenie przed żądaniami dotyczącymi plików **.ht***. Zapytania te będą odrzucane, żeby nie można było zobaczyć zawartości plików zaczynających się od **.ht***.

```
#-----pozostałe-----

DefaultRuntimeDir ${APACHE_RUN_DIR}

Timeout 300
KeepAlive On
MaxKeepAliveRequests 100
KeepAliveTimeout 5

ServerName localhost

User ${APACHE_RUN_USER}
Group ${APACHE_RUN_GROUP}

HostnameLookups Off

PidFile ${APACHE_PID_FILE}
ErrorLog ${APACHE_LOG_DIR}/error.log
LogLevel warn

LogFormat "%v:%p %h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" vhost_combined
LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %O" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent
```

Wprowadzony został dodatkowo wpis **ServerName localhost**. Brak tego parametru generuje ostrzeżenie (warning), kiedy za każdym razem restartujemy serwer Apache2. Chodzi o to, że serwer próbuje rozwiązać nazwę lokalną, nazwę po adresie IP, której jednak nie potrafi rozwiązać, bo nie miał na przykład umieszczonej jej w definicjach stref wyszukiwania wstecznego.

Poniżej z kolei prezentuje się zawartość pliku **ports.conf**, do którego dodany został wpis **Listen 8080**, zezwalający na nasłuch serwera http na porcie 8080

```
GNU nano 2.9.3 ports.conf

# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80
Listen 8080

<IfModule ssl_module>
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Obecnie serwer Apache2 nasłuchuje na portach 80 i 8080. Jeżeli uruchomione zostaną moduły **ssl_module** i **mod_gnutls.c**, to serwer dodatkowo będzie nasłuchiwał na porcie 443, na którym działa protokół szyfrowany https.

Możemy teraz zrestartować serwer www poleceniem

service apache2 restart

Wypada teraz sprawdzić, czy usługa jest uruchomiona na określonych portach wpisując:

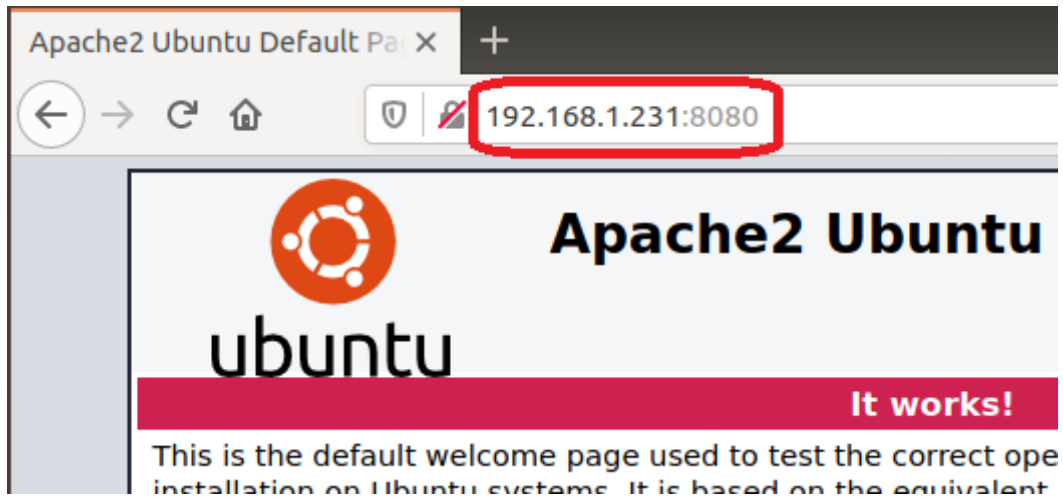
nmap localhost

```
root@serwer:/home/michał# nmap localhost

Starting Nmap 7.60 ( https://nmap.org ) at 2021-03-16 19:58 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 986 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
631/tcp   open  ipp
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql
5432/tcp  open  postgresql
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds
root@serwer:/home/michał#
```

Uruchomić przeglądarkę internetową i sprawdzić, czy strona się wyświetla. W pasku przeglądarki wpisać IPv4 serwera http z dodatkowo wprowadzonym numerem portu.



Dodatkowe witryny www

Jeden serwer http może przechowywać wiele odrębnych odseparowanych od siebie witryn internetowych. Mogą te witryny być powiązane konkretnymi adresami IP lub nazwami mnemonicznymi bądź numerami portów. Wszystko zależy od tego jak chcemy konfigurować nasze witryny.

Na początku wyłączymy domyślną witrynę **index.html** zlokalizowaną w katalogu **/var/www/html/**, i zobaczymy jak działa w tej sytuacji serwer Apache2.

Przechodzimy do katalogu **/etc/apache2/sites-enabled**,

```
root@serwer:/etc/apache2# cd sites-enabled/
root@serwer:/etc/apache2/sites-enabled# ls -l
razem 0
lrwxrwxrwx 1 root root 35 sty 25 22:13 000-default.conf -> ../sites-available/000-default.conf
root@serwer:/etc/apache2/sites-enabled#
```

gdzie znajduje się link **000-default.conf -> ../ sites ...** odnoszący się do oryginalnego pliku domyślnej witryny serwera

```
root@serwer:/etc/apache2/sites-available# ls -l
razem 12
-rw-r--r-- 1 root root 1332 lip 16 2019 000-default.conf
-rw-r--r-- 1 root root 6338 lip 16 2019 default-ssl.conf
```

Wyłączamy witrynę poleceniem **a2dissite**. Link w katalogu **site-enabled** znika. Serwer informuje, że należy zrestartować apache2 i czynimy to.

```
root@serwer:/etc/apache2/sites-enabled# a2dissite 000-default.conf
Site 000-default disabled.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@serwer:/etc/apache2/sites-enabled# ls
root@serwer:/etc/apache2/sites-enabled# service apache2 reload
root@serwer:/etc/apache2/sites-enabled#
```

Teraz tworzymy nowy katalog **moje** z plikiem **index.html** dla naszej nowej witryny w uznanej przez siebie lokalizacji. Możemy to zrobić w katalogu **/var/www**, gdzie znajduje się domyślny katalog witryny serwera apache2.

```
root@serwer:/var/www# mkdir moje
root@serwer:/var/www# ls -l
razem 8
drwxr-xr-x 2 root root 4096 mar 14 23:48 html
drwxr-xr-x 2 root root 4096 mar 16 21:56 moje
```

W celach wyłącznie testowych kopiuję plik **index.html** z katalogu **html** do katalogu **moje** i odrobinę przerabiam.

```
cp /var/www/html/index.html /var/www/moje/index.html
```

Utworzę jeszcze dodatkowy katalog **moje2** z plikiem **index.html**. w katalogu **/var/www**

```
root@serwer:/var/www# ls -l
razem 12
drwxr-xr-x 2 root root 4096 mar 16 21:59 html
drwxr-xr-x 2 root root 4096 mar 16 22:12 moje
drwxr-xr-x 2 root root 4096 mar 16 22:48 moje2
```

Przechodzimy do katalogu **/etc/apache2/sites-available**, gdzie znajdują się wszystkie nasze witryny, które chcemy mieć do dyspozycji i będą włączone.

Konfigurując witryny, należy określić, gdzie znajduje się najwyższy poziom struktury katalogów danej witryny internetowej, czyli ten, gdzie znajduje się plik domyślnie ładowany, bądź inne pliki domyślnie ładowane np. **index.html**, **index.htm**, **index.php**, jakiegokolwiek sobie sami określimy. ----> opcja **DocumentRoot**. Należy pamiętać, że wyżej niż **DocumentRoot** nasza witrynie nie może sięgnąć, czyli nie będzie można załadować pliki CSS, Java Script itp. będące poza katalogiem najwyższego poziomu. Można tworzyć podkatalogi, ale będą one zaczynały się od lokalizacji określonej jako parametr **DocumentRoot**.

DirectoryIndex – drugi istotny parametr konfiguracyjny. Domyślnie serwer Apache2 ma swoją konfigurację, w jakiej kolejności powinien szukać plików i je ładować, jeżeli je znajdzie. Domyślnym plikiem, który jest zawsze wysyłany przez Apache2 do przeglądarki internetowej swojego klienta jest **index.html**. Można oczywiście zmienić domyślnie ładowany plik np. na **index.htm** lub **index.php**, **strona.html** lub inny z wymyśloną przez siebie nazwą. Konfiguracja tutaj może mieć charakter globalny i dotyczyć całego serwera http, albo lokalny dla konkretnej witryny czyli tzw. wirtualnego hosta.

Włączenie witryny za pomocą polecenia **a2ensite** powoduje utworzenie linku do pliku konfiguracyjnego w lokalizacji **/etc/apache2/sites-enabled**.

Tworzymy witryny w katalogu `/etc/apache2/sites-available`, poprzez skopiowanie pliku `000-default.conf`, którego zawartość prezentuje się następująco:

```
root@serwer: /etc/apache2/sites-available
Plik Edycja Widok Wyszukiwanie Terminal Pomoc
GNU nano 2.9.3 000-default.conf

<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

```
root@serwer:/etc/apache2/sites-available# cp 000-default.conf moje.conf
root@serwer:/etc/apache2/sites-available# cp 000-default.conf moje2.conf
```

Otwieramy plik **moje.conf** i konfigurujemy witrynę internetową. Można na wstępie usunąć komentarze.

```
root@serwer: /etc/apache2/sites-available
Plik Edycja Widok Wyszukiwanie Terminal Pomoc
GNU nano 2.9.3 moje.conf

<VirtualHost *:80>

    ServerName moje.local
    ServerAlias www.moje.local

    ServerAdmin webmaster@moje.local
    DocumentRoot /var/www/moje
    DirectoryIndex index.html

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>
```

W parametrze **DirectoryIndex** możemy podać więcej niż jeden plik domyślnie ładowany, jeśli takie stworzyliśmy. Prezentować się to będzie następująco:

DirectoryIndex index.html index.htm index.php start.html

Należy pamiętać, że dla powyższej witryny jej lokalne ustawienia są ważniejsze od ustawień globalnych serwera Apache2.

Konfiguracja drugiej witryny **moje2.conf**. Tutaj nie ma ustawionego parametru **DirectoryIndex**, tak więc w stosunku do niego zostaną zastosowane zasady globalne serwera Apache2.

```
root@serwer: /etc/apache2/sites-available
Plik Edycja Widok Wyszukiwanie Terminal Pomoc
GNU nano 2.9.3 moje2.conf

<VirtualHost *:80>

    ServerName moje.local
    ServerAlias web.moje.local

    ServerAdmin webmaster@moje.local
    DocumentRoot /var/www/moje2

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>
```

Włączamy witryny i reloadujemy serwer http.

```
root@serwer:/etc/apache2/sites-available# a2ensite moje.conf
Enabling site moje.
To activate the new configuration, you need to run:
    systemctl reload apache2
root@serwer:/etc/apache2/sites-available# a2ensite moje2.conf
Enabling site moje2.
To activate the new configuration, you need to run:
    systemctl reload apache2
root@serwer:/etc/apache2/sites-available# service apache2 reload
root@serwer:/etc/apache2/sites-available#
```


Wyświetlanie stron na domenach poniżej określonych w strefie domenowej **moje.local**

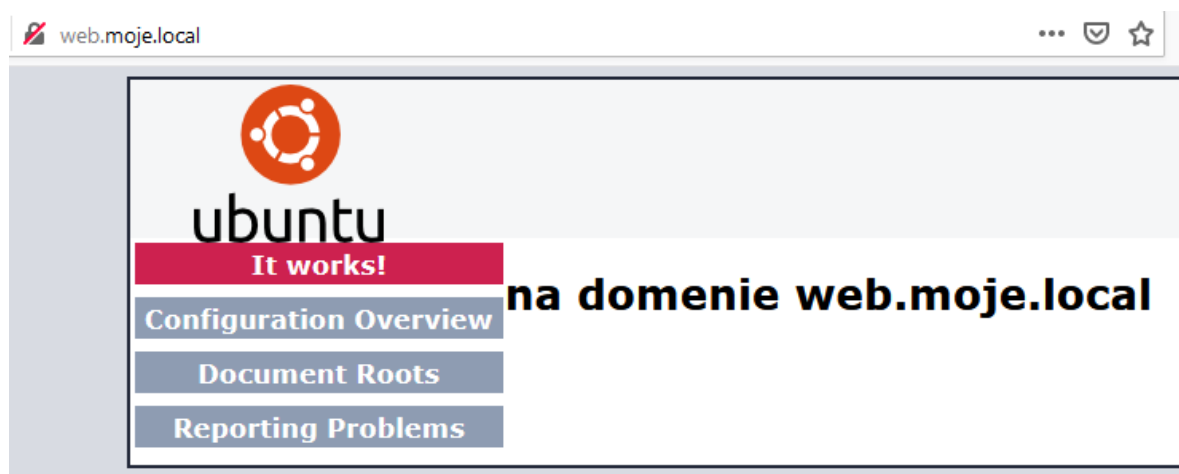
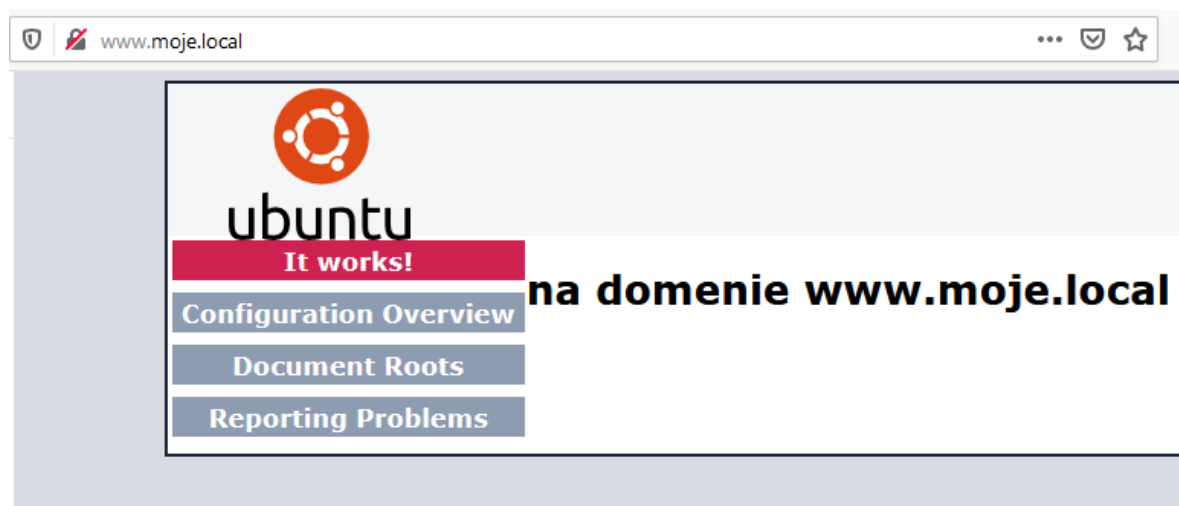
Menedżer DNS

Plik Akcja Widok Pomoc

DNS

- WINDOWS2016
 - Strefy wyszukiwania do przodu
 - moje.local**
 - Strefy wyszukiwania wstecznego
 - Punkty zaufania
 - Usługi warunkowego przesyłania dalej

Nazwa	Typ	Dane
(identyczny jak folder nadrz...	Adres startowy uwierzyt...	[25], windows2016., host...
(identyczny jak folder nadrz...	Serwer nazw (NS)	ns1.moje.local.
(identyczny jak folder nadrz...	Serwer nazw (NS)	windows2016.
(identyczny jak folder nadrz...	Host (A)	192.168.1.232
ns1	Host (A)	192.168.1.230
userver	Alias (CNAME)	moje.local.
www	Alias (CNAME)	moje.local.
web	Alias (CNAME)	moje.local



7.2 Ubuntu Serwer – konfiguracja serwera DNS

Ubuntu Server – konfiguracja serwera DNS

!!! W razie problemów kontaktować się z Administratorem 😊

Instalacja serwera DNS:

`sudo apt install bind9`

Pliki konfiguracyjne DNS są w katalogu: `/etc/bind/`

Podstawowe opcje konfiguracji dokonujemy w plikach:

`named.conf`

`named.conf.options`

`named.conf.local`

Konfiguracja pliku `named.conf.options`

`sudo nano named.conf.options`

// **forwarders** – serwery dns, do których wysyłane są zapytania dns np. o IPv4 domeny wp.pl

```
forwarders { 208.67.222.222;  
             208.67.220.220;  
};
```

// **forward only** – wysyłanie zapytań o rekordy do swoich forwarderów

```
forward only;
```

// **forward first** – wysyłanie zapytań o rekordy tylko raz do swoich forwarderów, kiedy te nie odpowiedzą,
// zapytanie skierowane zostanie do serwerów tld i root określonych w pliku: `/etc/bind/db.root`

// **listen-on** - parametr, który decyduje, na których adresach IPv4 będzie nasłuchiwał niniejszy serwer dns.
// Nasłuchiwanie może odbywać się zarówno na adresach wewnętrznych jak i zewnętrznych.
// Można zapisać adres IPv4 z maską podsieci lub bez.

```
listen-on { 192.168.255.231/32;  
};
```

// **allow-query** – parametr określa skąd mają przychodzić zapytania dns. Można więc podać całą sieć
// np. `192.168.1.0/24`; albo podać hosta `192.168.1.200/32`; oraz serwer jako `localhost`;

```
allow-query { 192.168.1.0/24;  
             192.168.10.0/24;  
             192.168.20.0/24;  
             localhost;  
};
```

Tworzenie stref lokalnych

Strefy lokalne tworzymy w pliku **named.conf.local**

Strefy lokalne są to takie strefy, które sam, jako administrator obsługuję. Czyli mój serwer będzie pełnił rolę serwera autorytatywnego dla tych stref.

Jeżeli mój serwer działa w sieci lokalnej z dostępem do Internetu, to nie powinienem tworzyć stref dla domen już wcześniej zarezerwowanych. Przykładowo jeśli w sieci jest aktywna domena moje.pl, to nie mam prawa stworzyć strefy domenowej o tej nazwie, wystawionej w Internecie. Za to mogę więc spokojnie stworzyć strefy: serwer.local, moje.local itd.

Otwieramy plik

sudo nano named.conf.local

i dokonujemy wpisu

```
zone "serwer.local" {  
    type master;      //serwer główny
```

// jeśli chcemy dodać serwer pomocniczy dodajemy wpis **type slave;**

```
    file "/etc/bind/db.serwer.local";  
};
```

```
zone "moje.local" {  
    type master;  
    file "/etc/bind/db.moje.local";  
};
```

// strefa wyszukiwania wstecznego dla sieci 192.168.1.0 /24

```
zone "1.168.192.in-addr.arpa" {  
    type master;  
    file "/etc/bind/db.1.168.192";  
};
```

Zapisać plik i sprawdzić konfigurację poleceniem

named-checkconf -p

Przeładowanie stref poleceniem **service bind9 reload**. Serwer DNS nie jest wyłączany i włączany jak to się dzieje po wpisaniu polecenia **restart**.

sudo service bind9 reload

Sprawdzić ponownie logi poleceniem

less /var/log/syslog

lub za pomocą frazy

grep zone -a /var/log/syslog

W logach wystąpią błędy ponieważ nie mamy jeszcze utworzonych plików:

db.serwer.local

db.moje.local

db.1.168.192

w katalogu **/etc/bind**.

Tworzymy pliki w katalogu **/etc/bind**.

touch db.serwer.local

touch db.moje.local

touch db. 1.168.192

Ponownie przeładować strefy dns i sprawdzić logi.

System informuje, że dalej są błędy, ale nie z powodu braku utworzonych wyżej katalogów. System informuje, że w każdym z katalogów powinny znajdować się rekordy SOA i NS .

Trzeba je będzie utworzyć.

Tworzenie stref dns w utworzonych katalogach

```
sudo nano db.serwer.local
```

Uwaga!

Uważać na wprowadzanie znaków białych i wszelkiego rodzaju innych znaków. Mogą one mieć znaczenie zwłaszcza na początku linii.

Tutaj w pliku średnik ";" jest komentarzem

```
; Tworzymy rekord SOA.
; Time to live. Określamy domyślną wartość dla wszystkich rekordów. Domyślnie podany w sekundach.
; można podać parametr s (sekunda),
;                               m (minuta),
;                               h (godzina), i w (tydzień)
```

```
$TTL 3600
```

; Tworzymy rekord SOA.

;Poszczególne parametry oddzielamy spacją lub tabulatorem. Tutaj będzie używany tabulator.

```
; @tabulator604800tabulatorINtabulatorSOAtabulator ...
```

```
; pierwszy parametr to @, która określa nazwę strefy, w tym przypadku to serwer.local
; drugi parametr za @ to parametr TTL. Jeżeli nie zostanie podany, wtedy będzie stosowany
; parametr $TTL 3600 określony na początku pliku.
; trzeci parametr IN oznaczający, że strefa będzie działać w sekcji Internet
; czwarty parametr to typ rekordu dns, tutaj rekord SOA .
; Rekord SOA wymaga następujących wartości:
;         - nazwa głównego serwera dns, który przechowuje tą strefę, tutaj ns1.serwer.local.
;         Kropka za etykietą local. oznacz, że mamy do czynienia z pełną nazwą domenową
;         serwera dns. Za kropką nie ma już żadnych etykiet.
;         - adres maila osoby odpowiedzialnej za domenę strefy. root.serwer.local.
;         Jak bym chciał napisać do administratora to użyłbym adresu root@serwer.local.
;         W zapisie rekordu SOA znak kropki zastępuje znak @ w adresie mailowym,
;         ponieważ znak @ zarezerwowany jest jako skrót domeny utworzonej strefy dns.
```

```
@      IN      SOA      ns1.serwer.local. root.serwer.local. (
```

```
20210224 ; Serial
```

```
3600      ; Refresh
```

```
2h        ; Retry Nie używać spacji!
```

```
10h       ;Expire
```

```
6h        ; Negative Case TTL
```

```
)
```

; Tworzymy rekord NS, który określa nazwę głównego serwera dns. Wymagany przynajmniej jeden, choć ; powinno być ich więcej.

```
@      IN      NS      ns1.serwer.local.
```

;Można napisać **ns1** (bez kropki na końcu) zamiast **ns1.serwer.local.** (z kropką na końcu), ponieważ po ; prawej stronie etykiety zostanie doklejona domena strefy:

```
ns1.@ == ns1.serwer.local
```

; Tworzymy rekord A dla domeny **ns1.serwer.local**

```
ns1     IN      A       192.168.1.231
```

PREZENTACJA ZAWARTOŚCI PLIKU **db.serwer.local** W CAŁOŚCI

\$TTL 3600

```
@      IN      SOA    ns1.serwer.local. root.serwer.local. (
                                20210224 ; Serial
                                3600      ; Refresh
                                2h        ; Retry Nie używać spacji!
                                10h       ; Expire
                                6h        ; Negative Case TTL
                                )

@      IN      NS     ns1.serwer.local.
ns1     IN      A      192.168.1.231
serwer.local. IN    A      192.168.1.231 ; pozwoli na zdalne logowanie się na serwer
                                           ; po domenę za pomocą ssh lub telnet
                                           ; np. ssh stefan@serwer.local
```

PREZENTACJA ZAWARTOŚCI PLIKU **db.moje.local** W CAŁOŚCI

\$TTL 3600

```
@      IN      SOA    ns1.serwer.local. root.serwer.local. ( 20210224 3600 2h 10h 6h)

@      IN      NS     ns1.serwer.local.
```

; nie tworzymy rekordu A dla ns1.serwer.local. Został bowiem już stworzony w pliku **db.serwer.local**

```
moje.local.  IN      A      192.168.1.231
```

```
www.moje.local.  IN      CNAME    moje.local. ; inny zapis to www  IN CNAME    @
web.moje.local.  IN      CNAME    moje.local.
```

; Przeładowanie stref poleceniem

sudo service bind9 reload.

; Sprawdzić ponownie logi poleceniem

less /var/log/syslog

;lub za pomocą frazy

grep zone -a /var/log/syslog

; Sprawdzenie działania strefy za pomoc narzędzia nslookup

nslookup -192.168.1.231

> ns1.serwer.local

; Ustawienie w konfiguracji interfejsów sieciowych, żeby niniejszy lokalny serwer obsługiwał wszystkie zapytania dns. Jeżeli w pliku konfiguracyjnym interfejsu sieciowego (**/etc/netplan/01-netcfg.yaml**) mamy ustawiony pożądany adres serwera dns, to poniższe kroki można pominąć.

W przeciwnym wypadku wyłączyć odpowiednie interfejsy sieciowe. U mnie jest to interfejs pod nazwą **enp0s3**. Jeżeli nie pamiętasz nazw swoich interfejsów sieciowych użyj polecenia **ifconfig** , aby to sprawdzić.

ifconfig enp0s3 down

Sprawdzamy plik **/etc/resolv.conf**

cat /etc/resolv.conf

Powinien prezentować poniższą zawartość. I niech tak zostanie.

```
root@serwer:/etc/bind# cat /etc/resolv.conf
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "systemd-resolve --status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0
```

Można jeszcze dodatkowo sprawdzić czy interfejs, który faktycznie wyłączyliśmy (tutaj **enp0s3**) jest wyłączony używając polecenia **ifconfig**. Jeśli system go wyłączył to nie powinien być widoczny.

Teraz otwieramy plik:

```
sudo nano /etc/netplan/01-netcfg.yaml
```

i zmieniamy adres serwera dns na pożądany **dns-nameservers 192.168.1.231** lub **127.0.0.1**

Są tacy co konfiguruja ustawienia karty sieciowej w pliku **/etc/network/interfaces**.

Podnoszenie interfejsów sieciowych

```
ifconfig enp0s3 up
```

Sprawdzenie konfiguracji poleceniem **ifconfig**

Sprawdzamy ponownie plik **/etc/resolv.conf**

```
cat /etc/resolv.conf
```

Otwieramy plik **named.conf.options**

```
sudo nano named.conf.options
```

Dodajemy wpis **127.0.0.1/32;** lub **localhost;**

```
listen-on { 192.168.255.231/32;
```

```
localhost;
```

```
};
```

Restartowanie serwera:

```
sudo service bind9 restart
```

; Sprawdzenie ponownie działania strefy za pomoc narzędzia nslookup

```
nslookup
```

```
> ns1.serwer.local
```

```
> set type=SOA
```

```
> serwer.local
```

```
> moje.local
```

```
> set type=a
```

```
> www.moje.local
```

```
>exit
```

; Konfiguracja strefy wyszukiwania wstecznego w stworzonym uprzednio pliku **db.1.168.192** .

PREZENTACJA ZAWARTOŚCI PLIKU **db.1.168.192** W CAŁOŚCI

\$TTL 3600

@ IN SOA ns1.serwer.local. root.serwer.local. (20210312 3600 2h 10h 6h)

@ IN NS ns1.serwer.local.

1.168.192 IN PTR serwer.local.

1.168.192 IN PTR moje.local.

; Przeładowanie stref poleceniem

sudo service bind9 reload.

; Sprawdzić ponownie logi poleceniem

less /var/log/syslog

;lub za pomocą frazy

grep zone -a /var/log/syslog

nslookup

> 192.168.1.231

8. DIAGNOSTYKA SIECI

8.1 Netstat Linux

NAZWA

```
9      netstat - wyświetla połączenia sieciowe, tablice trasowania,  
10      statystyki interfejsu,  
11      połączenia maskaradowe i udziale w połączeniach multicast
```

SKŁADNIA

```
12      netstat [opcje-rodziny-adresów] [--tcp|-t] [--udp|-u] [--raw|-w]  
13      [--listening|-l]  
14      [--all|-a] [--numeric|-n] [--numeric-hosts] [--numeric-ports] [-  
15      -numeric-users]  
16      [--symbolic|-N] [--extend|-e[--extend|-e]] [--timers|-o] [--program|-p]  
17      [--verbose|-v]  
18      [--continuous|-c]  
19      netstat {--route|-r} [opcje-rodziny-adresów] [--extend|-e[--extend|-e]]  
20      [--verbose|-v]  
21      [--numeric|-n] [--numeric-hosts] [--numeric-ports] [--numeric-users] [--  
22      continuous|-c]  
23      netstat {--interfaces|-i} [--all|-a] [--extend|-e[--extend|-e]]  
24      [--verbose|-v]  
25      [--program|-p] [--numeric|-n] [--numeric-hosts] [--numeric-ports] [-  
26      -numeric-users]  
27      [--continuous|-c]  
28      netstat {--groups|-g} [--numeric|-n] [--numeric-hosts] [--numeric-ports] [-  
29      -numeric-users]  
30      [--continuous|-c]  
31      netstat {--masquerade|-M} [--extend|-e] [--numeric|-n] [--numeric-hosts] [-  
32      -numeric-ports]  
33      [--numeric-users] [--continuous|-c]  
34      netstat {--statistics|-s} [--tcp|-t] [--udp|-u] [--raw|-w]  
35      netstat {--version|-V}  
36      netstat {--help|-h}  
37      opcje-rodziny-adresów:  
38      [-4] [-6] [--protocol={inet,unix,ipx,ax25,netrom,ddp}[...]] [--unix|-x]  
39      [--inet|--ip]  
40      [--ax25] [--ipx] [--netrom] [--ddp]
```

```
40      Netstat wyświetla dane o podsystemie sieciowym Linuksa. Typ wyświetlanej
informacji jest
41      kontrolowany przez pierwszy argument, jak poniżej:
42
43      (bez opcji)
44      Domyślnie netstat wyświetla listę otwartych gniazd. Jeśli nie poda się
rodzin adresów, to
45      wypisane zostaną aktywne gniazda wszystkich skonfigurowanych rodzin
adresów.
46
47      --route , -r
48      Wyświetla tabele trasowania. Więcej informacji znajduje się w
podręczniku route(8).
49      netstat -r i route -e wyświetlają to samo.
50
51      --groups , -g
52      Wyświetla informacje o członkostwie w połączeniach multicast w przypadku
IPv4 i IPv6.
53
54      --interfaces, -i
55      Wyświetla tabelę wszystkich interfejsów sieciowych.
56
57      --masquerade , -M
58      Wyświetla listę połączeń maskaradowych.
59
60      --statistics , -s
61      Wyświetla związane statystyki każdego protokołu.
```

OPCJE

```
62  --verbose , -v
63      Mówi użytkownikowi co się dzieje, wyświetlając więcej informacji. Co
    ważne, wypisuje
64      niektóre interesujące informacje o nieskonfigurowanych rodzinach adresów.
65
66  --wide , -W
67      Nie skraca adresów IP, używając tak szerokiego wyjścia, jakie jest
    potrzebne. Jest to
68      obecnie opcjonalne, aby nie zepsuć istniejących skryptów.
69
70  --numeric , -n
71      Pokazuje adresy numeryczne; nie próbuje zdeterminować symbolicznego hosta,
    portu czy nazwy
72      użytkownika.
73
74  --numeric-hosts
75      pokazuje adresy numeryczne; ale nie wpływa na określenie portu lub nazwy
    użytkownika.
76
77  --numeric-ports
78      pokazuje porty numeryczne, ale nie wpływa na określenie komputera czy nazwy
    użytkownika.
79
80  --numeric-users
81      pokazuje numeryczne identyfikatory użytkowników, ale nie wpływa na
    określenie komputera
82      czy nazw portów.
83
84  --protocol=rodzina , -A
85      Określa rodzinę adresów (prawdopodobnie lepsze określenie to protokoły
    niskiego poziomu)
86      do pokazywanych połączeń. rodzina jest listą oddzielonych przecinkami
    słów kluczowych,
87      takich jak inet, unix, ipx, ax25, netrom i ddp. To ma taki sam efekt, jak
    długie opcje
88      --inet, --unix (-x), --ipx, --ax25, --netrom i --ddp.
89
90      Rodzina adresów inet obejmuje gniazda protokołów raw, udp i tcp.
91
92  -c, --continuous
93      To powoduje, że netstat będzie wypisywał wybraną informację w trybie
    ciągłym, co sekundę.
94
95  -e, --extend
96      Wyświetla dodatkowe informacje. Dwukrotne użycie tej opcji da
    maksymalny poziom
97      szczegółowości.
98
99  -o, --timers
100     Obejmuje informacje związane z sieciowymi licznikami czasu.
101
102  -p, --program
103     Pokazuje PID-y oraz nazwy programów, do których należą poszczególne
    gniazda.
104
105  -l, --listening
106     Pokazuje jedynie nasłuchujące gniazda (są one domyślnie pomijane).
107
108  -a, --all
109     Pokazuje zarówno nasłuchujące jak i nienasłuchujące gniazda. Z opcją --
interfaces pokazuje
110     nieaktywne interfejsy.
111
112  -F
113     Wypisuje informacje trasowania z FIB (domyślnie).
```

```
114
115     -C
116     Wypisuje informacje trasowania z buforu trasowania.
```

WEJŚCIE

```
117     Aktywne połączenia internetowe (TCP, UDP, RAW)
118     Proto
119         Protokół (tcp, udp, raw) używany przez gniazdo.
120
121     Recv-Q
122         Liczba bajtów nieskopiowanych przez program użytkownika podłączonego do
123         tego gniazda.
124
125     Send-Q
126         Liczba bajtów, których odbiór nie został potwierdzony przez zdalny host.
127
128     Local Address
129         Adres lokalny (lokalna nazwa hosta) i numer portu gniazda. O ile
130         nie podano opcji
131         --numeric (-n), adres gniazda jest rozwiązywany do jego postaci
132         kanonicznej (FQDN), a
133         numer portu jest tłumaczony na odpowiadającą mu nazwę usługi.
134
135     Foreign Address
136         Adres zdanego komputera i numer portu jego gniazda. Analogiczne do "Local
137         Address".
138
139     State
140         Stan gniazda. Ponieważ w RAW to nie działa, a zazwyczaj w UDP też nie, to
141         pole pozostaje
142         czasem puste. Normalnie może być to jedna z kilku wartości:
143
144         ESTABLISHED
145             Gniazdo zestawilo połączenie.
146
147         SYN SENT
148             Gniazdo aktywnie próbuje zestawit połączenie.
149
150         SYN RECV
151             Żądanie połączenia zostało otrzymane z sieci.
152
153         FIN WAIT1
154             Gniazdo jest zamknięte, a połączenie się zamyka.
155
156         FIN WAIT2
157             Połączenie jest zamknięte, a gniazdo czeka na zamknięcie na drugim
158             końcu.
159
160         TIME WAIT
161             Po zamknięciu, gniazdo czeka na obsługę pakietów wciąż będących w
162             sieci.
163
164         CLOSE
165             Gniazdo nie jest używane.
166
167         CLOSE WAIT
168             Zdalny koniec zamknął i oczekuje aż gniazdo się zamknie.
169
170         LAST ACK
171             Zdalny koniec zamknął, a gniazdo jest zamknięte. Oczekiwanie
172             potwierdzenia.
173
174         LISTEN
175             Gniazdo nasłuchuje nadchodzących połączeń. Te gniazda są
176             wyświetlane tylko jeśli
177             ustawiono opcję --listening (-l) lub --all (-a).
```

```

168      CLOSING
169      Obydwa gniazda są zamknięte, lecz wciąż nie mamy wysłanych
wszystkich danych.
170
171      UNKNOWN
172      Stan gniazda jest nieznany.
173
174      User
175      Nazwa lub identyfikator użytkownika (UID) właściciela gniazda.
176
177      PID/Program name
178      Identyfikator procesu i oddzielona ukośnikiem nazwa procesu, który
jest właścicielem
179      gniazda. Opcja --program powoduje, że kolumna ta jest brana pod uwagę.
Potrzebne są
180      również uprawnienia superużytkownika, aby zobaczyć tę informację w
przypadku gniazd,
181      których nie jest się właścicielem. Ta informacja identyfikacyjna nie jest
wciąż dostępna
182      dla gniazd IPX.
183
184      Timer
185      (musi to być napisane)
186
187      Gniazda aktywne dziedziny UNIX-owej
188      Proto
189      Protokół (zwykle unix) używany przez gniazdo.
190
191      RefCnt
192      Liczba referencji (np. załączonych przez to gniazdo procesów).
193
194      Flags
195      Wyświetlane flagi to SO_ACCEPTON (wyświetlane jako ACC), SO_WAITDATA (W)
lub SO_NOSPACE
196      (N). SO_ACCEPTON jest używane na niepodłączonych gniazdach jeśli
odpowiadające im
197      procesy oczekują na żądanie połączenia. Pozostałe flagi zwykle nie są
interesujące.
198
199      Type
200      Istnieje wiele rodzajów dostępu do gniazd:
201
202      SOCK_DGRAM
203      Gniazdo jest używane w trybie datagramowym (beipołączeniowym).
204
205      SOCK_STREAM
206      Gniazdo jest strumieniowe (połączeniowe).
207
208      SOCK_RAW
209      Gniazdo jest gniazdem typu raw.
210
211      SOCK_RDM
212      Gniazdo serwuje rdm (reliably-delivered messages).
213
214      SOCK_SEQPACKET
215      Gniazdo jest gniazdem typu sequential packet.
216
217      SOCK_PACKET
218      Gniazdo dostępu interfejsu RAW.
219
220      UNKNOWN
221      Któż wie, co przyszłość może nam przynieść - wypełnij :-)
222
223      State
224      To pole będzie zawierać jedno z następujących słów kluczowych:
225
226      FREE      Gniazdo nie jest zaalokowane

```



```

227
228     LISTENING
229         Gniazdo nasłuchuje żądań połączeń. Te gniazda są wyświetlane tylko
jeśli ustawiono
230         opcję --listening (-l) lub --all (-a).
231
232     CONNECTING
233         Gniazdo ma zamiar zestawić połączenie.
234
235     CONNECTED
236         Gniazdo jest połączone.
237
238     DISCONNECTING
239         Gniazdo się rozłącza.
240
241     (empty)
242         Gniazdo nie jest podłączone do innego.
243
244     UNKNOWN
245         Ten stan nie powinien nigdy wystąpić.
246
247     PID/Program name
248         Identyfikator procesu (PID) i nazwa procesu, który posiada otwarte dane
gniazdo. Więcej
249         informacji znajduje się w rozdziale Aktywne połączenia internetowe,
znajdującym się wyżej.
250
251     Path
252         Wyświetla ścieżkę do procesów przywiązanych do gniazda.
253
254     Aktywne gniazda IPX
255         (powinno to być zrobione przez kogoś, kto je zna)
256
257     Aktywne gniazda NET/ROM
258         (powinno to być zrobione przez kogoś, kto je zna)
259
260     Aktywne gniazda AX.25
261         (powinno to być zrobione przez kogoś, kto je zna)

```

UWAGI

```

262     Od Linuksa 2.2, netstat -i nie wyświetla statystyk interfejsu, w
przypadku aliasu
263     interfejsu. Aby uzyskać liczniki aliasu interfejsu należy skonfigurować
odpowiednie reguły
264     za pomocą polecenia ipchains\(8\).
265     /etc/services -- Plik translacji usług
266
267     /proc -- Punkt montowania systemu plików proc, który daje dostęp do
informacji statusu
268     jądra za pomocą następujących plików:
269
270     /proc/net/dev -- informacja o urządzeniach
271
272     /proc/net/raw -- informacja o gniazdach RAW
273
274     /proc/net/tcp -- informacja o gniazdach TCP
275
276     /proc/net/udp -- informacja o gniazdach UDP
277
278     /proc/net/igmp -- informacja o multicast IGMP.
279
280     /proc/net/unix -- informacja o gniazdach dziedziny UNIX-owej
281
282     /proc/net/ipx -- informacja o gniazdach IPX

```

```
283
284     /proc/net/ax25 -- informacja o gniazdach AX25
285
286     /proc/net/appletalk -- informacja o gniazdach DDP (appletalk)
287
288     /proc/net/nr -- informacja o gniazdach NET/ROM
289
290     /proc/net/route -- informacje o trasowaniu IP
291
292     /proc/net/ax25 route -- informacje o trasowaniu AX25
293
294     /proc/net/ipx route -- informacje o trasowaniu IPX
295
296     /proc/net/nr nodes -- lista węzłów NET/ROM
297
298     /proc/net/nr neigh -- jądrowi sąsiedzi NET/ROM
299
300     /proc/net/ip masquerade -- połączenia maskaradowe
301
302     /proc/net/snmp -- statystyki
```

8.2 Netstat windows

Polecenie netstat w systemie Windows służy do wyświetlania informacji o połączeniach sieciowych, portach sieciowych i protokołach sieciowych. Może być używane do diagnostyki problemów z siecią lub do monitorowania aktywnych połączeń.

Składnia polecenia:

```
netstat [-a] [-b] [-e] [-f] [-n] [-o] [-p protocol] [-q] [-r] [-s] [-t] [-v]  
[interval]
```

Netstat -n wyświetla adresy i numery portów w postaci liczbowej.

W pierwszej kolumnie mamy wyświetlony używany protokół, w tym przypadku "TCP". Następnie nasz adres wraz z nr portu używanym do komunikacji. Następnie zdalny adres wraz z nr portu. Na końcu mamy stan połączenia.

```
C:\Users\user>netstat
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:1566	S302-17:11300	ESTABLISHED
TCP	127.0.0.1:11300	S302-17:1566	ESTABLISHED
TCP	192.168.1.199:1562	a23-64-12-26:https	CLOSE_WAIT
TCP	192.168.1.199:1675	199.232.189.91:https	ESTABLISHED
TCP	192.168.1.199:1693	mil04s41-in-f3:https	TIME_WAIT
TCP	192.168.1.199:1694	mil04s41-in-f3:https	TIME_WAIT
TCP	192.168.1.199:1696	46-248-183-10:https	ESTABLISHED
TCP	192.168.1.199:1697	waw07s06-in-f8:https	ESTABLISHED
TCP	192.168.1.199:1698	46-248-183-10:https	ESTABLISHED
TCP	192.168.1.199:1699	46-248-183-11:https	ESTABLISHED

```
C:\Users\user>netstat -n
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:1566	127.0.0.1:11300	ESTABLISHED
TCP	127.0.0.1:11300	127.0.0.1:1566	ESTABLISHED
TCP	192.168.1.199:1562	23.64.12.26:443	CLOSE_WAIT
TCP	192.168.1.199:1675	199.232.189.91:443	ESTABLISHED
TCP	192.168.1.199:1696	46.248.183.10:443	ESTABLISHED
TCP	192.168.1.199:1697	142.250.203.136:443	ESTABLISHED
TCP	192.168.1.199:1698	46.248.183.10:443	ESTABLISHED
TCP	192.168.1.199:1699	46.248.183.11:443	ESTABLISHED

Netstat -a wyświetla aktualne połączenia sieciowe, a także nasłuch na portach TCP i UDP

Adresy IPv4 **0.0.0.0:port** oznaczają nasz komputer. Zapis ten oznacza, że port nie nasłuchuje na określonym adresie IPv4, tylko na wszystkich interfejsach sieciowych komputera. Ponieważ lokalny adres IPv4 to same zera, to drugi koniec połączenia to nasz komputer S302-17 w kolumnie zdalnego adresu (docelowego).

```
C:\Users\user>netstat -a
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	S302-17:0	LISTENING
TCP	0.0.0.0:445	S302-17:0	LISTENING
TCP	0.0.0.0:1536	S302-17:0	LISTENING
TCP	0.0.0.0:1537	S302-17:0	LISTENING
TCP	0.0.0.0:1538	S302-17:0	LISTENING
TCP	0.0.0.0:1539	S302-17:0	LISTENING
TCP	0.0.0.0:1540	S302-17:0	LISTENING
TCP	0.0.0.0:1557	S302-17:0	LISTENING
TCP	0.0.0.0:11100	S302-17:0	LISTENING
TCP	127.0.0.1:1566	S302-17:11300	ESTABLISHED
TCP	127.0.0.1:11200	S302-17:0	LISTENING
TCP	127.0.0.1:11300	S302-17:0	LISTENING
TCP	127.0.0.1:11300	S302-17:1566	ESTABLISHED
TCP	192.168.0.199:139	S302-17:0	LISTENING
TCP	192.168.1.199:1562	a23-64-12-26:https	CLOSE_WAIT
TCP	192.168.1.199:1822	server-18-172-242-76:https	TIME_WAIT
TCP	192.168.1.199:1823	server-3-160-150-61:https	TIME_WAIT
TCP	192.168.1.199:1825	104.22.75.216:https	ESTABLISHED
TCP	192.168.1.199:1828	server-3-160-150-61:https	TIME_WAIT
TCP	192.168.1.199:1829	172.67.69.19:https	ESTABLISHED
TCP	192.168.1.199:1832	104.18.187.31:https	ESTABLISHED
TCP	192.168.1.199:1836	104.22.75.216:https	ESTABLISHED
TCP	192.168.1.199:1841	104.22.75.216:https	ESTABLISHED
TCP	192.168.1.199:1844	server-13-32-121-65:https	TIME_WAIT
TCP	192.168.1.199:1848	104.26.8.169:https	ESTABLISHED
TCP	192.168.1.199:1849	server-18-172-244-239:https	ESTABLISHED
TCP	192.168.1.199:1851	waw07s05-in-f1:https	TIME_WAIT
TCP	192.168.1.199:1866	a23-52-185-64:https	ESTABLISHED
TCP	192.168.1.199:1868	104.18.38.76:https	ESTABLISHED
TCP	192.168.1.199:1869	a2-17-240-177:https	ESTABLISHED
TCP	192.168.1.199:1873	52.46.151.131:https	ESTABLISHED
TCP	192.168.1.199:1878	168:https	ESTABLISHED
TCP	192.168.1.199:1879	64:https	ESTABLISHED
TCP	192.168.1.199:1887	ip-185-184-8-90:https	ESTABLISHED
TCP	192.168.1.199:1888	a0f671730127a0812:https	ESTABLISHED
TCP	192.168.1.199:1889	198.47.127.18:https	ESTABLISHED

TCP	192.168.1.199:1994	a104-81-211-161:https	ESTABLISHED
TCP	192.168.1.199:1995	216.239.32.36:https	ESTABLISHED
TCP	192.168.56.1:139	S302-17:0	LISTENING
TCP	:::135	S302-17:0	LISTENING
TCP	:::445	S302-17:0	LISTENING
TCP	:::1536	S302-17:0	LISTENING
TCP	:::1537	S302-17:0	LISTENING
TCP	:::1538	S302-17:0	LISTENING
TCP	:::1539	S302-17:0	LISTENING
TCP	:::1540	S302-17:0	LISTENING
TCP	:::1557	S302-17:0	LISTENING
TCP	:::11100	S302-17:0	LISTENING
UDP	0.0.0.0:5050	*:*	
UDP	0.0.0.0:5353	*:*	
UDP	0.0.0.0:5353	*:*	
UDP	0.0.0.0:5353	*:*	
UDP	0.0.0.0:5353	*:*	
UDP	0.0.0.0:5353	*:*	
UDP	0.0.0.0:5353	*:*	
UDP	0.0.0.0:5355	*:*	
UDP	0.0.0.0:64930	*:*	
UDP	127.0.0.1:1900	*:*	
UDP	127.0.0.1:60701	*:*	
UDP	192.168.0.199:137	*:*	
UDP	192.168.0.199:138	*:*	
UDP	192.168.0.199:1900	*:*	
UDP	192.168.0.199:60699	*:*	
UDP	192.168.56.1:137	*:*	
UDP	192.168.56.1:138	*:*	
UDP	192.168.56.1:1900	*:*	
UDP	192.168.56.1:60700	*:*	
UDP	:::5353	*:*	
UDP	:::5353	*:*	
UDP	:::5353	*:*	
UDP	:::5353	*:*	
UDP	:::5355	*:*	
UDP	:::1:1900	*:*	
UDP	:::1:60698	*:*	
UDP	[fe80::3409:2d20:3f57:fe38%7]:546	*:*	
UDP	[fe80::3df3:90d7:3459:a9cb%14]:1900	*:*	
UDP	[fe80::3df3:90d7:3459:a9cb%14]:60696	*:*	
UDP	[fe80::b14f:29bb:a731:5bf4%6]:1900	*:*	

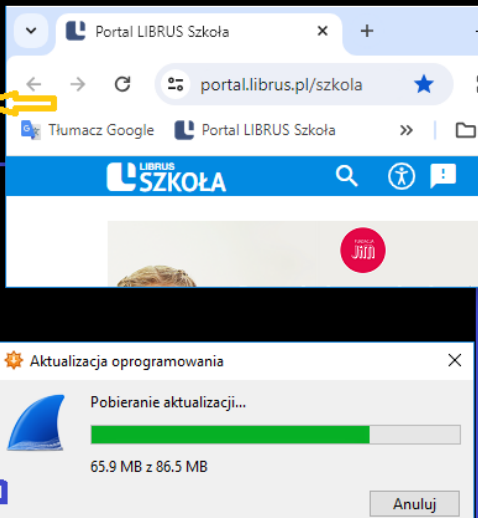
Netstat -a wyświetla nazwę pliku wykonywalnego dla każdego procesu, który korzysta z połączenia.

```
C:\Windows\system32>netstat -b
```

Active Connections

Proto	Local Address	Foreign Address	State	
TCP	127.0.0.1:1566	S302-17:11300	ESTABLISHED	
[veyon-worker.exe]	TCP	127.0.0.1:11300	S302-17:1566	ESTABLISHED
[veyon-service.exe]	TCP	192.168.1.199:1562	a23-64-12-26:https	CLOSE_WAIT
[SearchUI.exe]	TCP	192.168.1.199:1992	199.232.189.91:https	CLOSE_WAIT
[chrome.exe]	TCP	192.168.1.199:1996	a2-18-121-14:https	CLOSE_WAIT
[chrome.exe]	TCP	192.168.1.199:1998	104.26.11.240:https	ESTABLISHED
[Wireshark.exe]	TCP	192.168.1.199:1999	waw02s22-in-f3:http	ESTABLISHED
[Wireshark.exe]	TCP	192.168.1.199:2000	13.107.42.16:https	ESTABLISHED
[msedgeview2.exe]	TCP	192.168.1.199:2001	172.67.75.39:https	ESTABLISHED
[msedgeview2.exe]	TCP	192.168.1.199:2003	20.56.187.20:https	ESTABLISHED
[msedgeview2.exe]	TCP	192.168.1.199:2004	static:https	ESTABLISHED
[Wireshark.exe]				

C:\Windows\system32>_



Netstat -f polecenie wyświetla pełną nazwę DNS hosta dla każdego adresu IP.

Możemy na pierwszym rzucie zobaczyć kanoniczną nazwę serwera Web naszej szkoły: smtp.host4.kei.pl

```
C:\Users\user>netstat -f
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:1569	S302-17:11300	ESTABLISHED
TCP	127.0.0.1:11300	S302-17:1569	ESTABLISHED
TCP	192.168.1.199:1547	a23-64-12-25.deploy.static.akamaitechnologies.com:https	CLOSE_WAIT
TCP	192.168.1.199:2253	104.26.10.240:https	ESTABLISHED
TCP	192.168.1.199:2254	waw02s22-in-f3.1e100.net:http	ESTABLISHED
TCP	192.168.1.199:2255	13.107.42.16:https	ESTABLISHED
TCP	192.168.1.199:2256	104.26.11.240:https	ESTABLISHED
TCP	192.168.1.199:2258	192.229.221.95:http	ESTABLISHED
TCP	192.168.1.199:2259	20.191.45.158:https	ESTABLISHED
TCP	192.168.1.199:2260	static.21.100.78.5.clients.your-server.de:https	ESTABLISHED
TCP	192.168.1.199:2261	smtp.hostcztery.kei.pl:https	ESTABLISHED
TCP	192.168.1.199:2262	199.232.189.91:https	ESTABLISHED
TCP	192.168.1.199:2263	waw02s22-in-f10.1e100.net:https	ESTABLISHED
TCP	192.168.1.199:2264	smtp.hostcztery.kei.pl:https	ESTABLISHED
TCP	192.168.1.199:2265	a104-94-100-169.deploy.static.akamaitechnologies.com:https	ESTABLISHED
TCP	192.168.1.199:2266	104.18.40.68:https	ESTABLISHED
TCP	192.168.1.199:2267	104.18.186.31:https	ESTABLISHED
TCP	192.168.1.199:2268	waw07s06-in-f3.1e100.net:https	ESTABLISHED
TCP	192.168.1.199:2269	waw07s06-in-f3.1e100.net:https	ESTABLISHED
TCP	192.168.1.199:2270	waw07s06-in-f8.1e100.net:https	ESTABLISHED
TCP	192.168.1.199:2272	waw02s17-in-f10.1e100.net:https	ESTABLISHED
TCP	192.168.1.199:2273	a104-81-211-161.deploy.static.akamaitechnologies.com:https	ESTABLISHED
TCP	192.168.1.199:2274	216.239.34.36:https	ESTABLISHED
TCP	192.168.1.199:2275	a104-81-211-161.deploy.static.akamaitechnologies.com:https	ESTABLISHED

C:\Users\user>_

Na tym zrzucie z kolei widoczne jest połączenie lokalnego hosta z serwerem www.wp.pl.

```
C:\Users\user>netstat -f
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:1569	S302-17:11300	ESTABLISHED
TCP	127.0.0.1:11300	S302-17:1569	ESTABLISHED
TCP	192.168.1.199:1547	a23-64-12-25.deploy.static.akamaitechnologie	
TCP	192.168.1.199:2295	199.232.190.172:http	ESTABLISHED
TCP	192.168.1.199:2296	www.wp.pl:https	ESTABLISHED
TCP	192.168.1.199:2297	www.wp.pl:https	ESTABLISHED
TCP	192.168.1.199:2298	www.wp.pl:https	ESTABLISHED
TCP	192.168.1.199:2299	wpcdn.pl:https	ESTABLISHED
TCP	192.168.1.199:2300	edge-917.bunnyinfra.net:https	ESTABLISHED
TCP	192.168.1.199:2301	v.wpimg.pl:https	ESTABLISHED
TCP	192.168.1.199:2303	wp.hit.gemius.pl:https	ESTABLISHED
TCP	192.168.1.199:2304	178.250.7.2:https	ESTABLISHED
TCP	192.168.1.199:2305	rt.inistrack.net:https	ESTABLISHED

Netstat -o wyświetla identyfikator procesu będącego właścicielem powiązany z każdym połączeniem.

```
C:\Users\user>netstat -o
```

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	127.0.0.1:1569	S302-17:11300	ESTABLISHED	4944
TCP	127.0.0.1:11300	S302-17:1569	ESTABLISHED	4960
TCP	192.168.1.199:3286	199.232.189.91:https	CLOSE_WAIT	7156
TCP	192.168.1.199:3299	46-248-183-42:https	CLOSE_WAIT	7156
TCP	192.168.1.199:3301	smtp:https	ESTABLISHED	7156
TCP	192.168.1.199:3302	a104-94-100-176:https	ESTABLISHED	7156
TCP	192.168.1.199:3303	172.64.147.188:https	ESTABLISHED	7156
TCP	192.168.1.199:3304	waw07s06-in-f3:https	ESTABLISHED	7156

```
C:\Users\user>
```

Menedżer zadań

Plik Opcje Widok

Procesy Wydajność Historia aplikacji Uruchamianie Użytkownicy Szczegóły Usługi

Nazwa	Identyfikator PID	Stan	Nazwa uży...	Uży...	Pamięć (pr...	Opis
ApplicationFrameHo...	5192	Uruchomiony	user	00	3 800 K	Application Fr...
armsvc.exe	3528	Uruchomiony	SYSTEM	00	872 K	Acrobat Updat
atkexComSvc.exe	3520	Uruchomiony	SYSTEM	00	5 496 K	atkexComSvc
audiodg.exe	8444	Uruchomiony	USŁUGA L...	00	4 900 K	Izolacja wykres
chrome.exe	1832	Uruchomiony	user	00	130 920 K	Google Chrom
chrome.exe	7936	Uruchomiony	user	00	15 016 K	Google Chrom
chrome.exe	3012	Uruchomiony	user	00	6 176 K	Google Chrom
chrome.exe	4840	Uruchomiony	user	00	50 956 K	Google Chrom
chrome.exe	6612	Uruchomiony	user	00	131 232 K	Google Chrom
chrome.exe	2060	Uruchomiony	user	00	1 296 K	Google Chrom
chrome.exe	4304	Uruchomiony	user	00	121 012 K	Google Chrom
chrome.exe	7156	Uruchomiony	user	00	14 104 K	Google Chrom
chrome.exe	2504	Uruchomiony	user	00	4 984 K	Google Chrom
chrome.exe	9624	Uruchomiony	user	00	50 224 K	Google Chrom
chrome.exe	2708	Uruchomiony	user	00	212 032 K	Google Chrom
chrome.exe	2108	Uruchomiony	user	00	10 264 K	Google Chrom
chrome.exe	8732	Uruchomiony	user	00	3 380 K	Google Chrom
chrome.exe	7672	Uruchomiony	user	00	46 372 K	Google Chrom
chrome.exe	1184	Uruchomiony	user	00	56 820 K	Google Chrom
cmd.exe	8724	Uruchomiony	user	00	608 K	Windows Com
conhost.exe	2508	Uruchomiony	user	00	5 716 K	Console Wind
csrss.exe	548	Uruchomionv	SYSTEM	00	1 052 K	Proces wykona

Mniej szczegółów

Zakończ zadanie

Netstat -oa dddd

C:\Users\user>netstat -oa

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	S302-17:0	LISTENING	452
TCP	0.0.0.0:445	S302-17:0	LISTENING	4
TCP	0.0.0.0:1536	S302-17:0	LISTENING	656
TCP	0.0.0.0:1537	S302-17:0	LISTENING	1316
TCP	0.0.0.0:1538	S302-17:0	LISTENING	1432
TCP	0.0.0.0:1539	S302-17:0	LISTENING	3308
TCP	0.0.0.0:1540	S302-17:0	LISTENING	732
TCP	0.0.0.0:1555	S302-17:0	LISTENING	744
TCP	0.0.0.0:11100	S302-17:0	LISTENING	4960
TCP	127.0.0.1:1569	S302-17:11300	ESTABLISHED	4944
TCP	127.0.0.1:11200	S302-17:0	LISTENING	4960
TCP	127.0.0.1:11300	S302-17:0	LISTENING	4960
TCP	127.0.0.1:11300	S302-17:1569	ESTABLISHED	4960
TCP	192.168.0.199:139	S302-17:0	LISTENING	4
TCP	192.168.1.199:3337	a23-64-12-34:https	CLOSE_WAIT	5756
TCP	192.168.1.199:3339	204.79.197.237:https	ESTABLISHED	7156
TCP	192.168.10.199:139	S302-17:0	LISTENING	4
TCP	192.168.56.1:139	S302-17:0	LISTENING	4
TCP	:::135	S302-17:0	LISTENING	452
TCP	:::445	S302-17:0	LISTENING	4
TCP	:::1536	S302-17:0	LISTENING	656
TCP	:::1537	S302-17:0	LISTENING	1316
TCP	:::1538	S302-17:0	LISTENING	1432
TCP	:::1539	S302-17:0	LISTENING	3308
TCP	:::1540	S302-17:0	LISTENING	732
TCP	:::1555	S302-17:0	LISTENING	744
TCP	:::11100	S302-17:0	LISTENING	4960
UDP	0.0.0.0:5050	*.*		6748
UDP	0.0.0.0:5353	*.*		6612
UDP	0.0.0.0:5353	*.*		868
UDP	0.0.0.0:5353	*.*		6612
UDP	0.0.0.0:5353	*.*		6612
UDP	0.0.0.0:5353	*.*		6612
UDP	0.0.0.0:5353	*.*		6612
UDP	0.0.0.0:5353	*.*		6612
UDP	0.0.0.0:5355	*.*		868
UDP	0.0.0.0:53330	*.*		7156
UDP	0.0.0.0:57208	*.*		3308
UDP	127.0.0.1:1900	*.*		4524
UDP	127.0.0.1:49435	*.*		4524

UDP	192.168.0.199:137	*.*	4
UDP	192.168.0.199:138	*.*	4
UDP	192.168.0.199:1900	*.*	4524
UDP	192.168.0.199:49432	*.*	4524
UDP	192.168.10.199:137	*.*	4
UDP	192.168.10.199:138	*.*	4
UDP	192.168.10.199:1900	*.*	4524
UDP	192.168.10.199:49434	*.*	4524
UDP	192.168.56.1:137	*.*	4
UDP	192.168.56.1:138	*.*	4
UDP	192.168.56.1:1900	*.*	4524
UDP	192.168.56.1:49433	*.*	4524
UDP	[::]:5353	*.*	6612
UDP	[::]:5353	*.*	6612
UDP	[::]:5353	*.*	868
UDP	[::]:5353	*.*	6612
UDP	[::]:5355	*.*	868
UDP	[::1]:1900	*.*	4524
UDP	[::1]:49431	*.*	4524
UDP	[fe80::3df3:90d7:3459:a9cb%14]:1900	*.*	
UDP	[fe80::3df3:90d7:3459:a9cb%14]:49428	*.*	
UDP	[fe80::b14f:29bb:a731:5bf4%6]:1900	*.*	
UDP	[fe80::b14f:29bb:a731:5bf4%6]:49429	*.*	
UDP	[fe80::e9a6:9611:54ed:605c%12]:1900	*.*	
UDP	[fe80::e9a6:9611:54ed:605c%12]:49430	*.*	

C:\Users\user>_

Netstat -e wyświetla statystyki Ethernet. Można to połączyć z -s opcja.

```
C:\Users\user>netstat -e
Interface Statistics

                Received                Sent
Bytes          4087472100             237547716
Unicast packets    3052206             1716384
Non-unicast packets  413232             24186
Discards           0                   0
Errors             0                   0
Unknown protocols  0

C:\Users\user>_
```

Netstat -r wyświetla tabelę routingu

```
C:\Users\user>netstat -r
=====
Interface List
14...ac 9e 17 88 ab 7f .....Realtek PCIe GBE Family Controller
 6...0a 00 27 00 00 06 .....VirtualBox Host-Only Ethernet Adapter
12...00 e0 4c 68 7d d6 .....Realtek PCIe GBE Family Controller #4
 1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.1.1      192.168.0.199    281
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        331
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        331
127.255.255.255            255.255.255.255  On-link          127.0.0.1        331
192.168.0.0                255.255.255.0    On-link          192.168.0.199    281
192.168.0.199              255.255.255.255  On-link          192.168.0.199    281
192.168.0.255              255.255.255.255  On-link          192.168.0.199    281
192.168.1.0                255.255.255.0    On-link          192.168.0.199    281
192.168.1.199              255.255.255.255  On-link          192.168.0.199    281
192.168.1.255              255.255.255.255  On-link          192.168.0.199    281
192.168.10.0               255.255.255.0    On-link          192.168.10.199   281
192.168.10.199             255.255.255.255  On-link          192.168.10.199   281
192.168.10.255             255.255.255.255  On-link          192.168.10.199   281
192.168.56.0               255.255.255.0    On-link          192.168.56.1     281
192.168.56.1               255.255.255.255  On-link          192.168.56.1     281
192.168.56.255             255.255.255.255  On-link          192.168.56.1     281
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        331
224.0.0.0                  240.0.0.0        On-link          192.168.56.1     281
224.0.0.0                  240.0.0.0        On-link          192.168.10.199   281
224.0.0.0                  240.0.0.0        On-link          192.168.0.199    281
255.255.255.255            255.255.255.255  On-link          127.0.0.1        331
255.255.255.255            255.255.255.255  On-link          192.168.56.1     281
255.255.255.255            255.255.255.255  On-link          192.168.10.199   281
255.255.255.255            255.255.255.255  On-link          192.168.0.199    281
=====
Persistent Routes:
Network Address            Netmask  Gateway Address  Metric
0.0.0.0                    0.0.0.0    192.168.1.1     Default
=====
```

IPv6 Route Table

Active Routes:

If	Metric	Network Destination	Gateway
1	331	::1/128	On-link
6	281	fe80::/64	On-link
12	281	fe80::/64	On-link
14	281	fe80::/64	On-link
14	281	fe80::3df3:90d7:3459:a9cb/128	On-link
6	281	fe80::b14f:29bb:a731:5bf4/128	On-link
12	281	fe80::e9a6:9611:54ed:605c/128	On-link
1	331	ff00::/8	On-link
6	281	ff00::/8	On-link
12	281	ff00::/8	On-link
14	281	ff00::/8	On-link

Persistent Routes:

None

C:\Users\user>

Netstat -s wyświetla statystyki dla poszczególnych protokołów. Domyślnie statystyki to pokazano dla IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP i UDPv6; Opcja -p może być użyta do określenia podzbioru wartości domyślnej.

```
C:\Users\user>netstat -s
```

IPv4 Statistics

Packets Received	= 558821
Received Header Errors	= 0
Received Address Errors	= 1599
Datagrams Forwarded	= 0
Unknown Protocols Received	= 0
Received Packets Discarded	= 38763
Received Packets Delivered	= 521897
Output Requests	= 288729
Routing Discards	= 0
Discarded Output Packets	= 27
Output Packet No Route	= 25
Reassembly Required	= 0
Reassembly Successful	= 0
Reassembly Failures	= 0
Datagrams Successfully Fragmented	= 0
Datagrams Failing Fragmentation	= 0
Fragments Created	= 0

IPv6 Statistics

Packets Received	= 3144
Received Header Errors	= 0
Received Address Errors	= 17
Datagrams Forwarded	= 0
Unknown Protocols Received	= 0
Received Packets Discarded	= 1504
Received Packets Delivered	= 2219
Output Requests	= 956
Routing Discards	= 0
Discarded Output Packets	= 0
Output Packet No Route	= 0
Reassembly Required	= 0
Reassembly Successful	= 0
Reassembly Failures	= 0
Datagrams Successfully Fragmented	= 0
Datagrams Failing Fragmentation	= 0
Fragments Created	= 0

ICMPv4 Statistics

ICMPv4 Statistics

	Received	Sent
Messages	2861	188
Errors	0	0
Destination Unreachable	2861	188
Time Exceeded	0	0
Parameter Problems	0	0
Source Quenches	0	0
Redirects	0	0
Echo Replies	0	0
Echos	0	0
Timestamps	0	0
Timestamp Replies	0	0
Address Masks	0	0
Address Mask Replies	0	0
Router Solicitations	0	0
Router Advertisements	0	0

ICMPv6 Statistics

	Received	Sent
Messages	57	36
Errors	0	0
Destination Unreachable	1	3
Packet Too Big	0	0
Time Exceeded	0	0
Parameter Problems	0	0
Echos	0	0
Echo Replies	0	0
MLD Queries	0	0
MLD Reports	0	0
MLD Dones	0	0
Router Solicitations	0	9
Router Advertisements	0	0
Neighbor Solicitations	10	11
Neighbor Advertisements	46	13
Redirects	0	0
Router Renumberings	0	0

TCP Statistics for IPv4

TCP Statistics for IPv4

Active Opens	= 1830
Passive Opens	= 25
Failed Connection Attempts	= 16
Reset Connections	= 265
Current Connections	= 9
Segments Received	= 342455
Segments Sent	= 250543
Segments Retransmitted	= 3567

TCP Statistics for IPv6

Active Opens	= 22
Passive Opens	= 0
Failed Connection Attempts	= 2
Reset Connections	= 0
Current Connections	= 0
Segments Received	= 112
Segments Sent	= 148
Segments Retransmitted	= 4

UDP Statistics for IPv4

Datagrams Received	= 199162
No Ports	= 38767
Receive Errors	= 0
Datagrams Sent	= 61036

UDP Statistics for IPv6

Datagrams Received	= 1388
No Ports	= 1504
Receive Errors	= 0
Datagrams Sent	= 616

Netstat -arp widoczne jest połączenie wyświetla informacje o protokole ARP

```
C:\Users\user>netstat -arp
```

Active Connections

Proto	Local Address	Foreign Address	State
-------	---------------	-----------------	-------

Interface List

14...ac 9e 17 88 ab 7f	Realtek PCIe GBE Family Controller
6...0a 00 27 00 00 06	VirtualBox Host-Only Ethernet Adapter
12...00 e0 4c 68 7d d6	Realtek PCIe GBE Family Controller #4
1.....	Software Loopback Interface 1

IPv4 Route Table

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.1.1	192.168.0.199	281
	127.0.0.0	255.0.0.0	On-link	127.0.0.1	331
	127.0.0.1	255.255.255.255	On-link	127.0.0.1	331
127.255.255.255	255.255.255.255		On-link	127.0.0.1	331
	192.168.0.0	255.255.255.0	On-link	192.168.0.199	281
	192.168.0.199	255.255.255.255	On-link	192.168.0.199	281
	192.168.0.255	255.255.255.255	On-link	192.168.0.199	281
	192.168.1.0	255.255.255.0	On-link	192.168.0.199	281
	192.168.1.199	255.255.255.255	On-link	192.168.0.199	281
	192.168.1.255	255.255.255.255	On-link	192.168.0.199	281
	192.168.10.0	255.255.255.0	On-link	192.168.10.199	281
	192.168.10.199	255.255.255.255	On-link	192.168.10.199	281
	192.168.10.255	255.255.255.255	On-link	192.168.10.199	281
	192.168.56.0	255.255.255.0	On-link	192.168.56.1	281
	192.168.56.1	255.255.255.255	On-link	192.168.56.1	281
	192.168.56.255	255.255.255.255	On-link	192.168.56.1	281
	224.0.0.0	240.0.0.0	On-link	127.0.0.1	331
	224.0.0.0	240.0.0.0	On-link	192.168.56.1	281
	224.0.0.0	240.0.0.0	On-link	192.168.10.199	281
	224.0.0.0	240.0.0.0	On-link	192.168.0.199	281
255.255.255.255	255.255.255.255		On-link	127.0.0.1	331
255.255.255.255	255.255.255.255		On-link	192.168.56.1	281
255.255.255.255	255.255.255.255		On-link	192.168.10.199	281
255.255.255.255	255.255.255.255		On-link	192.168.0.199	281

Persistent Routes:

Network	Address	Netmask	Gateway Address	Metric
	0.0.0.0	0.0.0.0	192.168.1.1	Default

Ciąg dalszy **Netstat -arp**

IPv6 Route Table

Active Routes:

If	Metric	Network	Destination	Gateway
1	331	::1/128		On-link
6	281	fe80::/64		On-link
12	281	fe80::/64		On-link
14	281	fe80::/64		On-link
14	281	fe80::3df3:90d7:3459:a9cb/128		On-link
6	281	fe80::b14f:29bb:a731:5bf4/128		On-link
12	281	fe80::e9a6:9611:54ed:605c/128		On-link
1	331	ff00::/8		On-link
6	281	ff00::/8		On-link
12	281	ff00::/8		On-link
14	281	ff00::/8		On-link

Persistent Routes:

None

C:\Users\user>