

Sieci komputerowe – klasa 2

Konfiguracja routera	2
Diody LED.....	2
Zmiana nazwy urządzenia	2
Przywracanie ustawień fabrycznych	2
Klucze szyfrujące	5
SSH i Telnet	5
Ustawienia bramy domyślnej.....	5
Firewall	6
Konfiguracja NAT i DHCP.....	8
Konfiguracja DNS.....	14
Konfiguracja sieci w Mikrotiku	15
Routing statyczny i dynamiczny	22
Routing statyczny	22
Tablica routingu	24
OSPF	26
RIP i RIP2.....	27
Konfiguracja przełącznika	29
Reset.....	29
VLAN i Trunk	32
Przekierowanie portów	38
Laboratoria	42

Część 1, konfiguracja routera

Diody na routerze TP LINK



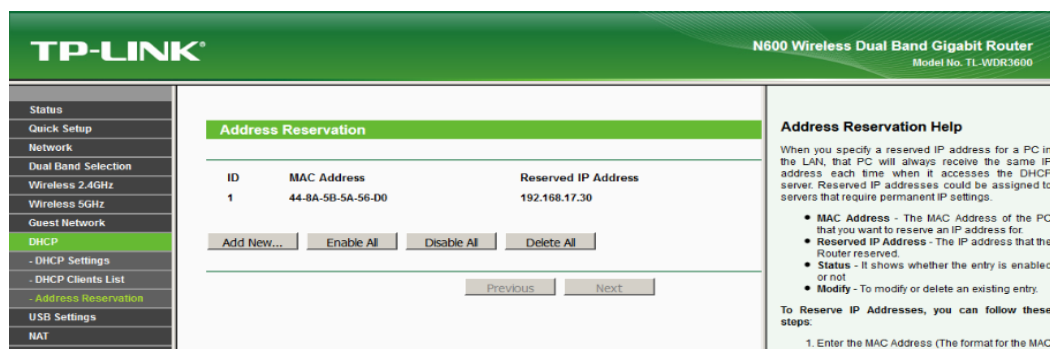
The screenshot shows the 'Easy Setup Assistant' for a TP-LINK Wireless N Router. The left sidebar contains navigation options: Witamy, Instalacja routera (highlighted), Konfiguracja routera, and Zatwierdzenie ustawień. The main content area is titled 'Opis wskazań diod LED' and includes a table with the following data:

Name	Status	Indication
⏻ (Power)	Włączona	Podłączone zasilanie.
⚙️ (System)	Pulsuje	Router działa poprawnie.
📶 (WLAN)	Pulsuje	Aktywne połączenie bezprzewodowe.
🌐 (WAN), 📺 (LAN 1-4)	Włączona	Podłączono urządzenia do portów routera, brak transmisji danych.
	Pulsuje	Transmisja danych.

Jeżeli diody urządzenia mają inny status, niż opisany powyżej, sprawdź fizyczne podłączenie routera. Następnie kliknij przycisk **DALEJ**.

Podstawową konfiguracją tego routera w GUI jest wprowadzenie odpowiedniej adresacji, zmiana hasła oraz wprowadzenie klucza zabezpieczeń WPA2.

Poniższemu komputerowi o adresie MAC 44-8A-5B-5A-56-D0 usługa DHCP routera przydzieli adres IP 192.168.17.30:



The screenshot shows the 'Address Reservation' page in the TP-LINK web interface. The left sidebar lists various settings, with 'DHCP' expanded to show 'Address Reservation'. The main content area displays a table with one reservation entry:

ID	MAC Address	Reserved IP Address
1	44-8A-5B-5A-56-D0	192.168.17.30

Buttons for 'Add New...', 'Enable All', 'Disable All', and 'Delete All' are visible below the table. A 'Help' section on the right provides instructions on how to reserve IP addresses.

Łączenie z routerem TP-LINK

Najpierw należy odłączyć nasz komputer od Internetu WAN – z powodów bezpieczeństwa. Podpinamy router kablem RJ45 używając jednego z portów LAN i wyjścia RJ45 w komputerze/laptopie. Możemy połączyć się przy pomocy przeglądarki wpisując adres 192.168.0.1/192.168.1.1 albo tplinkwifi.net gdzie najczęściej login to admin a hasło admin. Jeśli nie pojawia się okno logowania to należy w naszym komputerze zmienić ustawienia karty sieciowej w IPV4 na przydzielanie dynamiczne. Na dole routera znajdują się loginy i hasła do wifi oraz nazwa sieci SSID.

Przywracanie ustawień fabrycznych TPLINK

Jeśli zapomnieliśmy hasła przy kolejnym logowaniu reset jest idealnym rozwiązaniem. Przy włączonym zasilaniu przetrzymaj przycisk reset aż dioda zacznie migać. Można zalogować się na stronę administracyjną routera i tam przywrócić ustawienia fabryczne. Pierwszą czynnością niezbędną do zabezpieczenia routera przed dostępem do jego panelu konfiguracyjnego przez osoby niepowołane jest zmiana hasła i loginu admina.

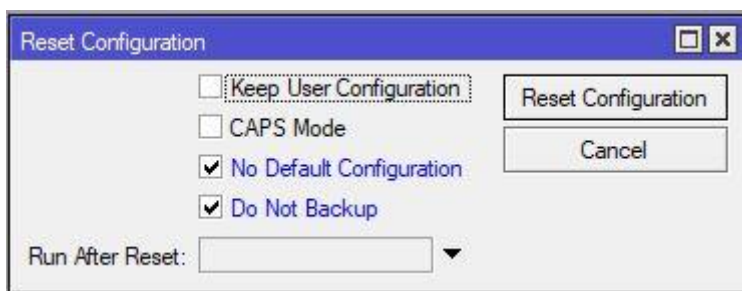
Router Mikrotik

Logujemy się po adresie Mac, bo router nie ma nadanego adresu IP (192.168.88.1/24).

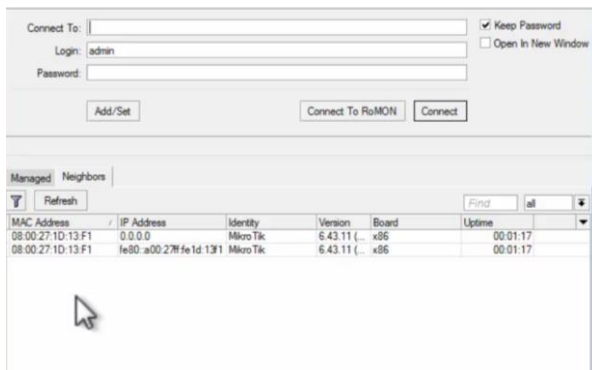
Do routera możemy logować się przez przeglądarkę lub Winboxa.

„add” – po 1 udanym zalogowaniu zapamiętuje router w Winboxie.

Większość modeli Mikrotik'ów po wyjęciu z pudełka jest tak naprawdę skonfigurowane do pracy jako prosty router. Jednak korzystanie z niego ma kilka wad m.in. fasttrack który sztucznie podkręca wydajność urządzenia. Uniemożliwia on jednak korzystanie z np. ograniczania prędkości użytkownikom (kolejki), markowania ruchu, hostspot'a i wielu innych funkcji. Jeśli ktoś chce router na zasadzie „podłączę i działa” to odsyłam do oferty np. TP-Link'a.



Reasumując gdy wyciągniemy router z pudełka włączmy go podłączmy się to jednego z portu LAN (na pudełku zwykle zawsze jest napisane które z portów domyślnie to LAN). Otwórzmy winbox'a i wyczyścimy konfigurację „na czysto”. Łączymy się zatem do IP 192.168.88.1 Robimy to wchodząc w System->”Reset Configuration” i zaznaczamy aby reset był bez domyślnej konfiguracji oraz że nie chcemy backupu. Potwierdzamy operację i czekamy.



Po resece urządzenie nie ma adresu IP więc łączymy się po adresie MAC z listy neighbors. Login to admin a hasło pozostaje puste.

Zmiana nazwy urządzenia: system -> info -> wpisujemy nazwę i klikamy ok. Hasło ustawiamy w system -> users -> password.

Router CISCO

Łączymy się poprzez terminal wykorzystując np. Putty (jeśli router nie posiada GUI). Potrzebny jest kabel konsolowy a do USB przejściówka RS232. Klikamy w Putty „serial”, prędkość 9600 i open.

Zmiana nazwy urządzenia: w odpowiednim trybie wpisujemy „hostname” -> ...

Router CISCO bez GUI resetujemy poprzez przerwanie bootowania ctrlc/ctrl break. Jeśli restart routera ctrl break lub ctrl c nie działa, mamy 2 opcje.

1 metoda:

Reset routera Cisco nie działa z tego powodu, że w systemie Rommon została wyłączona komenda przerywająca bootowanie. Rozwiązanie, w CLI:

- enable -> config -> config-reg 0x0 -> exit -> reload.

Wtedy router CISCO przejdzie w tryb Rommon:

- confreg-> disable break/abort has the effect (yes), później klikamy no, reload.

2 metoda:

In Hyper Terminal: complete these steps to simulate a break key sequence:

Connect to the router with these terminal settings: (1200 baud rate, No parity, 8 data bits, 1 stop bit, no flow control). You no longer see any output on your screen, and this is normal. Power cycle (switch off and then on) the router and press the SPACEBAR for 10-15 seconds in order to generate a signal similar to the break sequence. Disconnect your terminal, and reconnect with a 9600 baud rate. You enter the ROM Monitor mode.

<after getting into ROMMON follow below steps>

```
rommon 1 > confreg 0x2142
```

```
rommon 2 > reset
```

```
Router#copy startup-config running-config
```

```
Router(config)#enable secret < password >
```

```
Router#show ip interface brief
```

<unshut the shutdown interfaces>

```
Router(config)#config-register 0x2102
```

```
Router#copy running-config startup-config
```

<restart router>

Klucze szyfrujące

Klucze te zabezpieczają administratora i połączenie w sieci. Klucze symetryczne oznaczają, że klucz prywatny i publiczny jest niezmienny a klucze asymetryczne gdy klucz prywatny zmienia się przy każdym logowaniu i jest generowany po stronie użytkownika przy każdym logowaniu.

Komenda w CLI w urządzeniach CISCO do szyfrowania to “service password-encryption”, “crypto key generate rsa general keys 360-2048” albo „crypto key generate rsa modulus” (modulus wartość, wpisujemy tutaj długość klucza).

W Mikrotiku klucze generujemy poprzez np. Putty key generator -> generate -> w czasie generowania ruszamy cały czas kursorem -> wpisujemy “passphrase 2x -> kopiujemy wygenerowany klucz do “rsa” -> na pulpicie tworzymy dokument w notatniku zmieniając rozszerzenie na “.pub”. Teraz generujemy w putty key generator klucz prywatny klikając w “save private key” -> zapisujemy go również na pulpicie.

W menu Mikrotika klikamy files -> upload -> umieszczamy klucz z rozszerzeniem .pub z pulpitu. Później system -> userlist -> ssh keys -> import ssh keys. Teraz generujemy klucz prywatny w Putty dodając go w menu -> authenticate i łączymy się w „session” przez SSH i adres IP.

Telnet/SSH

Telnet w Windows kliencie i Windows Server są domyślnie wyłączone.

Włączenie telnetu w Windows klient to: panel sterowania -> programy -> włącz lub wyłącz funkcje -> zaznaczamy “klient telnet” -> ok. Następnie otwieramy CMD -> telnet -> open i wpisujemy adres IP routera. Powyższa ścieżka może się nieznacznie różnić w zależności od wersji system Windows.

Telnet w Windows Server -> Serwer Lokalny -> role i funkcje -> 4x klik -> zaznaczamy telnet.

W Cisco telnet zabezpieczamy wpisując “line console vty 0 4 lub 0 15” -> „password” -> „login”,

SSH łączymy się poprzez Putty wybierając opcje SSH w menu głównym i wpisując adres IP routera/przełącznika.

Brama domyślna

Brama domyślna jest “oknem na świat” tzn. wskazuje, którądy idzie sieć od dostawcy Internetu. W CISCO konfigurujemy ją poprzez wpisanie w CLI “ip default-gateway (adres IP bramy)”.

W Mikrotiku bramę domyślną wpisujemy w “IP-> “Routes” -> “+” (w tym miejscu wpisujemy z reguły adres sieci docelowej lub adres IP routera kolejnego przeskoku), -> default gateway.

W TP-LINK bramę wpisujemy w zakładce “network”:



Firewall

Zapora sieciowa jest systemem zabezpieczającym routery od zewnątrz tj. od WAN.

W routerach TP-LINK WR841N, które używamy w naszej szkole w zakładce “security”-> “basic security” stosowany jest firewall SPI (*Firewall Stateful Packet Inspection*). To architektura zapory sieciowej, która umożliwia wykrywanie bieżących połączeń na wszystkich interfejsach. W ramach Firewall SPI filtrowane są różne typy połączeń. Pakiety danych poddaje się bardzo szczegółowej analizie na podstawie ich stanu, co zapewnia wysoką ochronę przed złośliwym oprogramowaniem.

Co istotne, Firewall SPI nie wykorzystuje filtrowania statycznego. Nie sprawdza wyłącznie nagłówek – ochrona rozszerzona jest o filtrowanie ich całej zawartości. Proces odbywa się w obrębie warstwy sieciowej. Dane filtrowane przez FirewallSPI notowane są na tzw. tablicy stanów. Proces można określić mianem dynamicznego i nie jest on uzależniony od zasad ustalonych przez administratora sieci.

Filtrowanie bazuje na informacjach czerpanych z pakietów przychodzących. Firewall SPI odpowiada zatem za zwiększenie bezpieczeństwa w sieci LAN – chroni zasoby przed szkodliwym działaniem z zewnątrz. Pierwotne wersje SPI wymagały dużej mocy obliczeniowej procesora. Obecnie oparte są na filtrze pakietów, który zapewnia wysoką wydajność pracy.

Dodatkowo w tej zakładce możemy zastosować filtrowanie użytkowników sieci na podstawie adresów MAC przy jednoczesnym wyłączeniu SSID sieci. Możemy także zablokować konkretne numery portów.

Zapora w CISCO

W routerach CISCO możemy m.in. konfigurować listy kontrolne tzw. ACL, które określamy za pomocą poleceń „deny” albo „permit” lub przypisać inspekcję firewalla do interfejsu, np.

```
Router(config)# access-list 103 deny ip any any
Router(config)# access-list 103 permit host
200.1.1.1 eq isakmp any
Router(config)# interface vlan 1
Router(config-if)# ip inspect firewall in
```

W Mikrotiku dodajemy ściśle określone reguły w zakładce:

a) IP -> firewall -> filter rules/nat -> + -> chain:

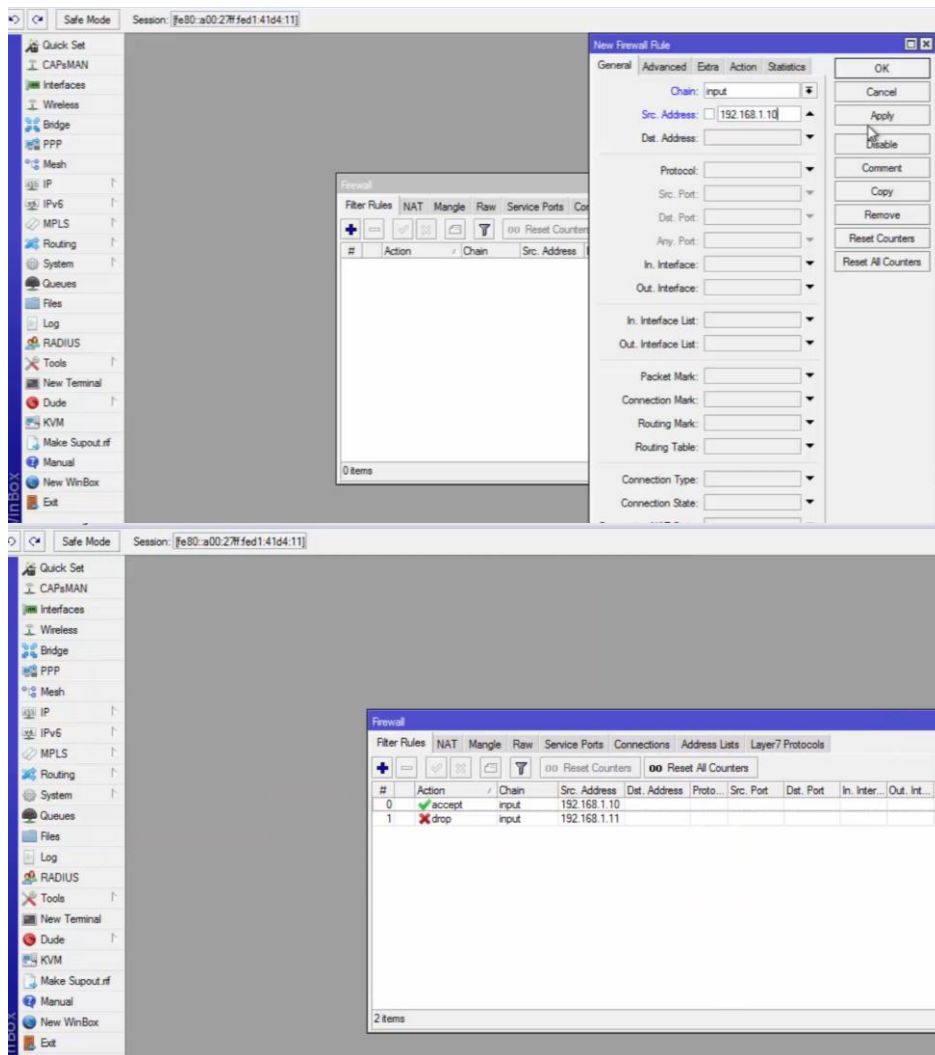
- input (pakiety kierowane do routera),
- output (pakiety generowane przez router),
- forward (pakiety przesyłane przez router).

b) IP -> firewall -> new firewall rule -> actions

- accept (zaakceptuj),
- drop (odrzuć),
- jump/return (wróć do reguły skonfigurowanej przez administratora),
- reject (odrzuć i wyślij odpowiedni komunikat ICMP).

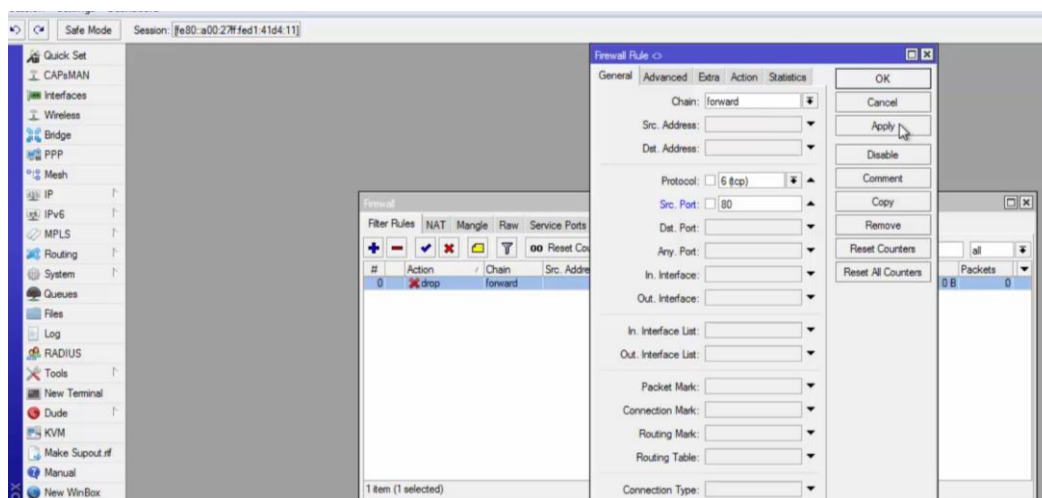
c) IP -> firewall -> address list -> możemy zablokować np. adres lub grupę adresów IP na określony czas.

Poniżej reguła firewalla, która akceptuje hosta o adresie 192.168.1.10 (w zakładce “action” jest accept) a adres 192.168.1.11 jako drop tzn. odrzuć:



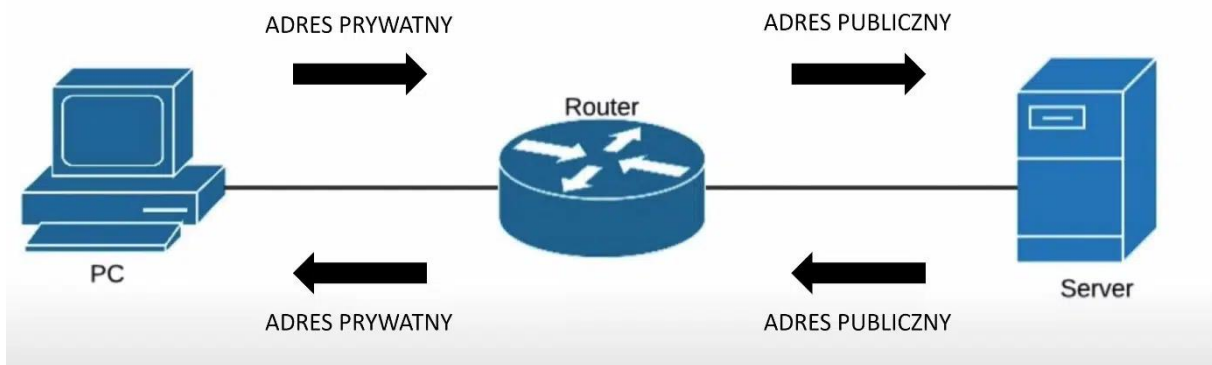
By sprawdzić czy działa powyższa reguła wystarczy z CMD lub terminala Mikrotika spingować urządzenia.

Poniżej blokada http przez firewall Mikrotika:



NAT i DHCP

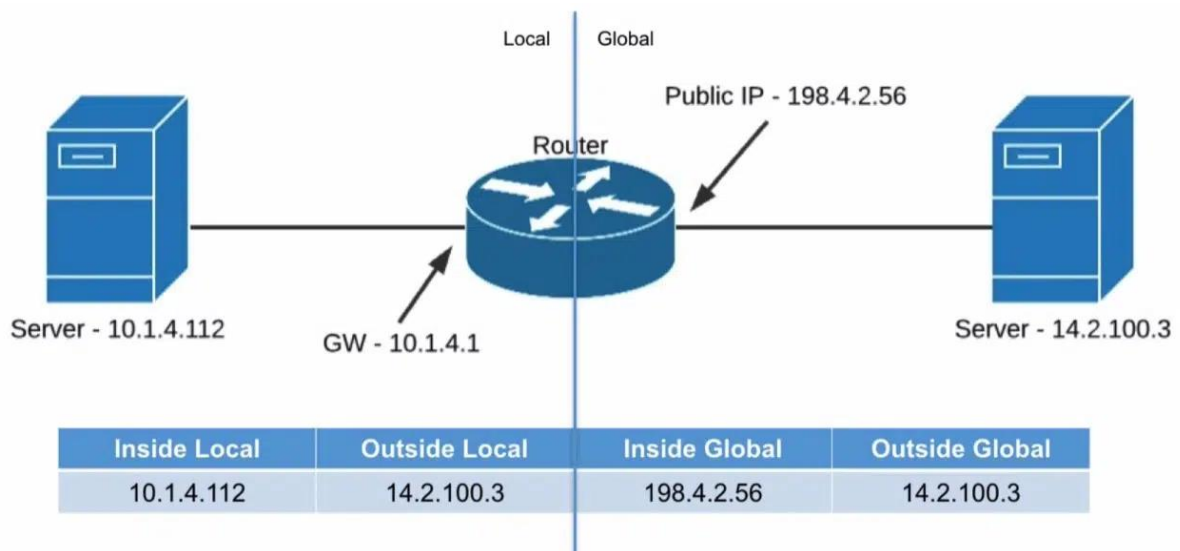
Translacja adresów sieciowych umożliwia używanie prywatnych adresów IP (czyli adresów, które są przeznaczone do używania wyłącznie w sieciach wewnętrznych i nie mogą być rozgłaszane globalnie w Internecie – są to adresy o prefixach 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) i jednocześnie komunikowanie się ze wszystkimi urządzeniami w Internecie. Jest to możliwe dzięki zamianie prywatnych adresów IP na publiczne zarejestrowane adresy, zarówno jeden do jednego, jak i jeden do wielu, co będzie bardziej szczegółowo omówione w dalszej części artykułu. Router mapuje prywatny adres wewnętrzny oraz adres publiczny i dokonuje zamiany adresu IP zarówno, gdy pakiet wychodzi z sieci jak również gdy do niej wraca. Dzięki temu na przykład posiadając nawet jeden publiczny adres IP firma może zapewnić komunikację z Internetem wielu hostom znajdującym się w sieci firmowej.



Router TP-LINK WR841N nie posiada funkcji kontroli NAT. Jednakże, posiada on mechanizmy, które go wspierają np. port triggering. W port triggering możemy konfigurować lokalnego hosta z połączeniem wychodzącym do zewnętrznego hosta przy wykorzystaniu numeru portu.

W NAT wyróżniamy 4 główne pojęcia:

- Inside local – rzeczywisty adres IP przydzielony hostowi znajdującemu się w sieci wewnętrznej
- Outside local – adres IP zewnętrznego hosta widziany z perspektywy sieci wewnętrznej
- Inside global – jest to adres hosta znajdującego się w sieci wewnętrznej, ale widziany z poziomu Internetu
- Outside global – rzeczywisty adres hosta znajdującego się poza siecią wewnętrzną



Pierwszym krokiem w konfiguracji w CISCO jest stworzenie mapowania adresu prywatnego na publiczny.

```
R1(config)#ip nat inside source static 10.1.4.112 198.4.2.56
```

Następnie określamy, który port będzie interfacem wewnętrznym.

```
R1(config)#interface GigabitEthernet 0/0
```

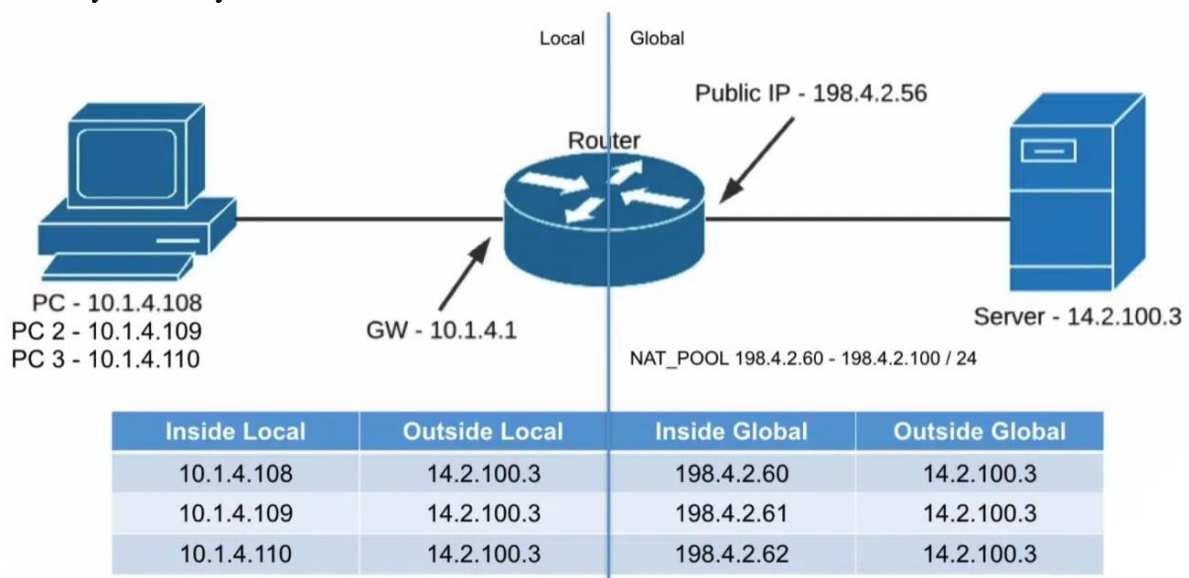
```
R1(config-if)#ip nat inside
```

Określamy port zewnętrzny.

```
R1(config-if)#interface GigabitEthernet 0/1
```

```
R1(config-if)#ip nat outside
```

NAT dynamiczny



Poprzez access listę określamy listę adresów wewnętrznych, dla których ma być wykonana translacja NAT.

```
R1(config)#access-list 1 permit 10.1.4.0 0.0.0.255
```

Definiujemy pulę adresów publicznych, które będą służyły do translacji.

```
R1(config)#ip nat pool NAT_POOL 198.4.2.60 198.4.2.100 netmask 255.255.255.0
```

Kolejnym poleceniem włączamy Dynamic NAT, gdzie odwołujemy się do puli adresów i access listy utworzonych w poprzednich krokach.

```
R1(config)#ip nat inside source list 1 pool NAT_POOL
```

Następnie określamy, który port będzie interfacem wewnętrznym.

```
R1(config)#interface GigabitEthernet 0/0
```

```
R1(config-if)#ip nat inside
```

Oraz analogicznie określamy port zewnętrzny.

```
R1(config-if)#interface GigabitEthernet 0/1
```

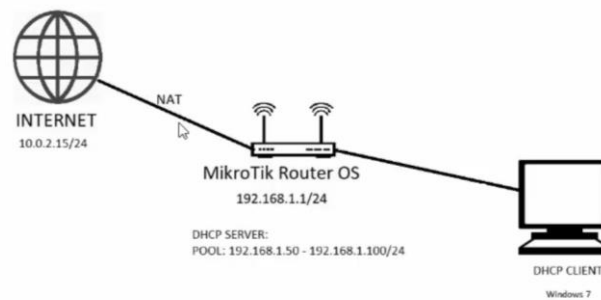
```
R1(config-if)#ip nat outside
```

W Mikrotiku lub CISCO należy najpierw sprawdzić, które interfejsy są LAN a które WAN. Dobrą praktyką jest ich opisanie. W Mikrotiku w zakładce “bridge” można zmostkować porty:

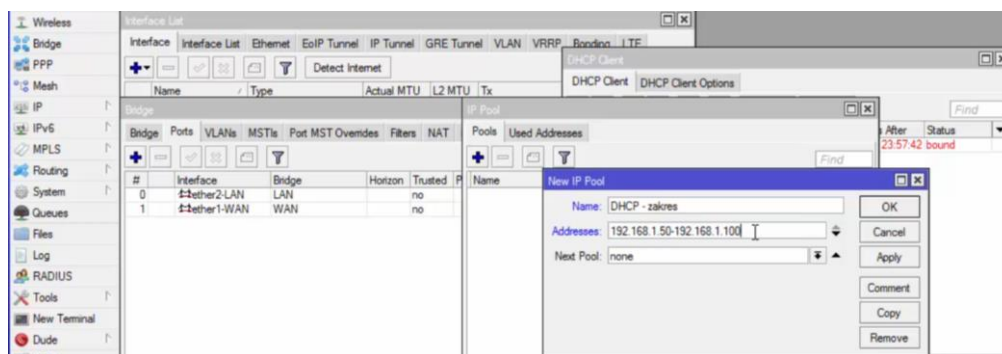
➔ bridge -> + -> nazwa -> ok

➔ ports -> + -> interface (wybieramy LAN lub WAN) i bridge (wybieramy właściwy).

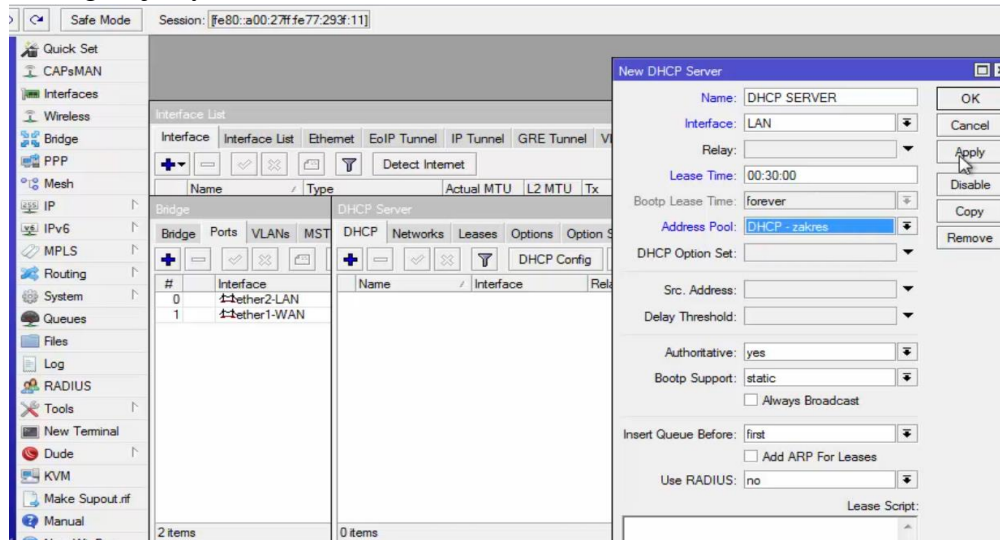
Konfigurujemy DHCP dynamicznie by lokalny host mógł pobrać IP przez NAT: IP-> DHCP client -> + -> apply -> ok. Bazujemy na poniższej sieci:



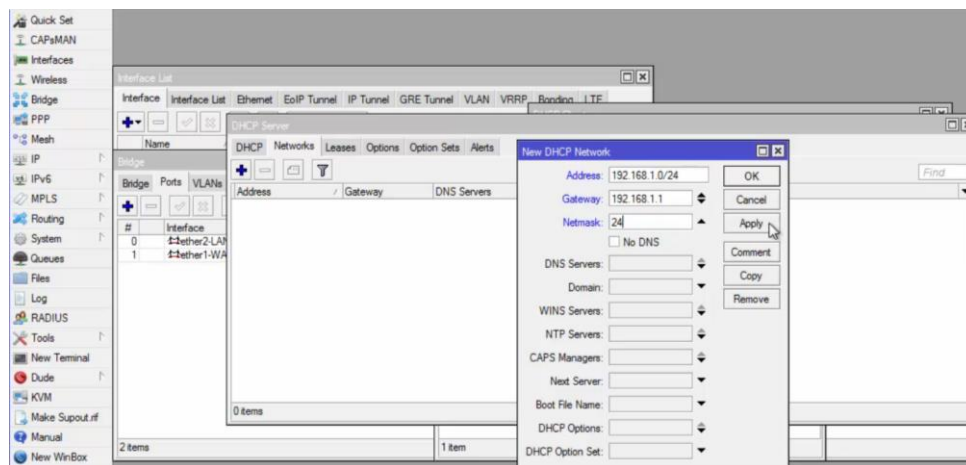
Konfigurujemy IP-> pool by określić zakres adresów IP naszej sieci, np.



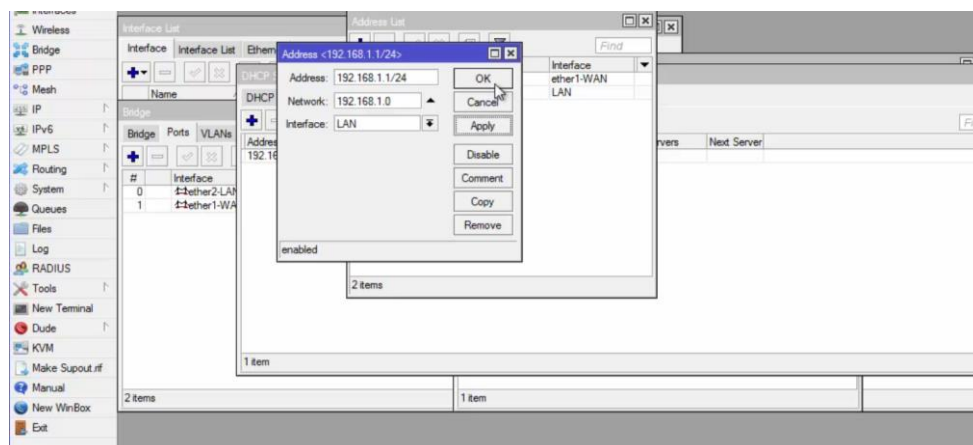
Konfigurujemy serwer DHCP:



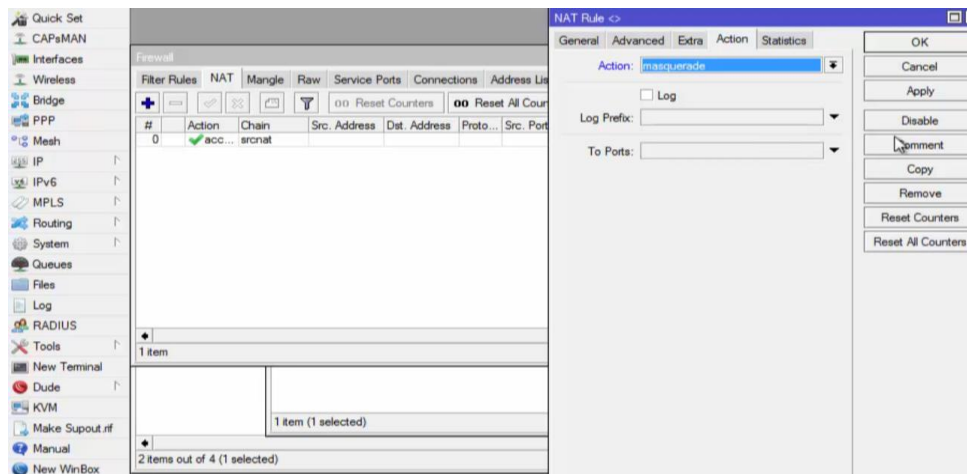
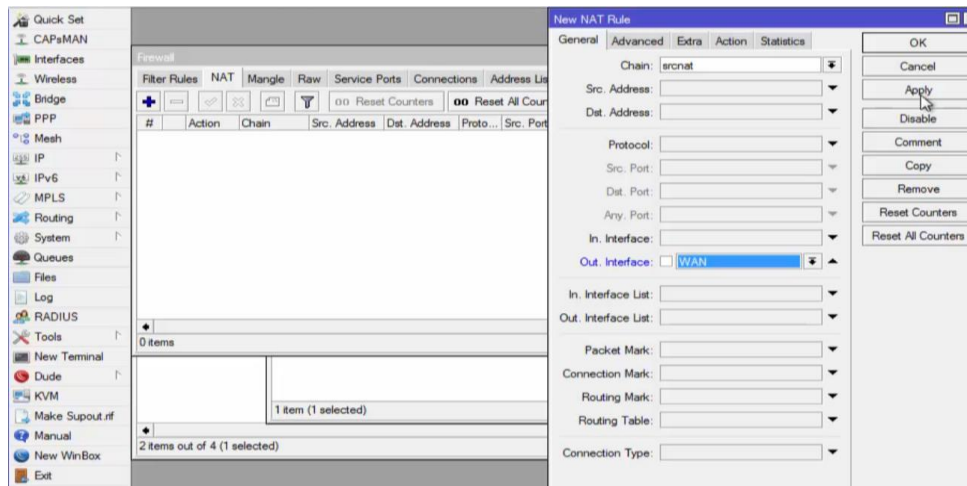
Dodajemy adres sieci i bramy domyślnej w zakładce “IP” -> “dhcp server” ->“networks”, np.:



Ustawiamy adres wyjściowy interfejsu lokalnego po to, by stacja robocza mogła się komunikować z routerem:

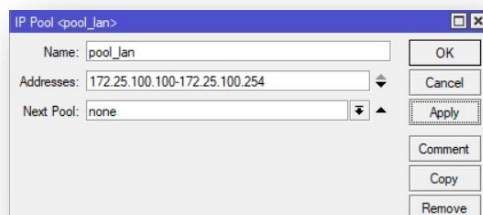


W zakładce IP-> firewall -> NAT:

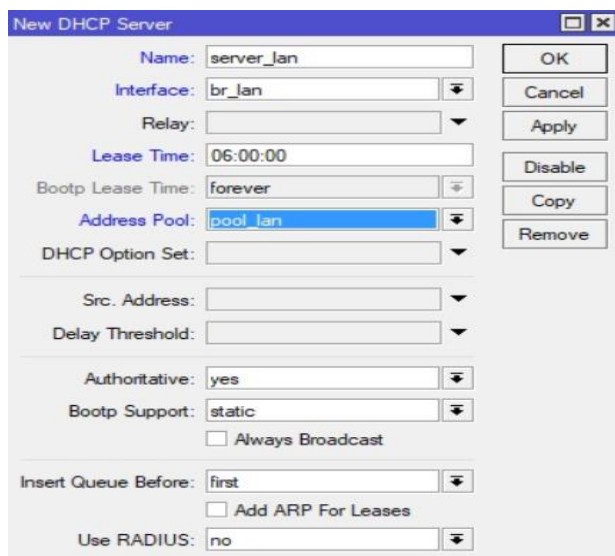


Na koniec można zresetować kartę sieciową stacji roboczej i spingować.

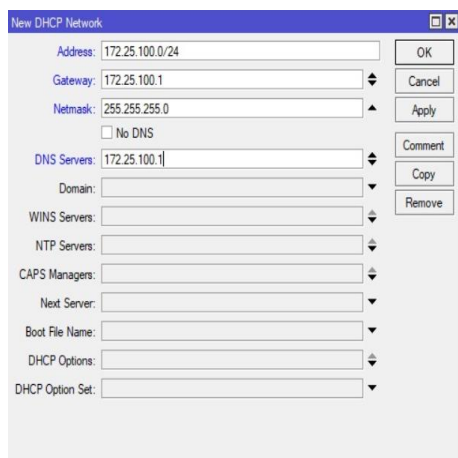
Serwer DHCP



Konfigurację serwera DHCP zaczynamy od konfiguracji puli adresów IP które ma on przydzielać. Robimy to w menu IP->Pool. Klikając dodaj w nowym oknie wpisujemy wybraną nazwę puli oraz zakres adresów. Proponuję założyć że w sieci mogą pojawić się urządzenia na statycznych adresach IP (np. drukarka lub access point). Dlatego wpisujemy adresy 172.25.100.100-172.25.100.254 które będą przydzielane przez DHCP. Natomiast adresy 172.25.100.2-172.25.100.99 mogą być użyte statycznie.



Kolejnym krokiem jest utworzenie instancji samego serwera. W tym celu wchodzimy w menu IP->"DHCP Server" i klikamy dodaj. Uzupełniamy nazwę oraz interfejs na którym ma on działać. W polu „Lease Time” wpisujemy czas na jaki będzie przydzielany adres IP, myślę że przykładowy czas 6 godzin jest odpowiedni. Musimy też wybrać wcześniej utworzoną pulę adresów w polu „Address Pool”.



Następnie w oknie „DHCP Server” przechodzimy do zakładki Networks gdzie podajemy konfigurację naszej sieci lokalnej. W polu Address wpisujemy adres naszej sieci z maską (adres sieci to nie jest adres routera!). W polu Gateway wpisujemy adres który będzie bramą dla hostów w sieci LAN czyli adres routera od strony LAN. Pole Netmask to maska naszej sieci lokalnej czyli 255.255.255.0 lub w skrócie 24. Założyłem również że serwerem DNS dla naszej sieci będzie nasz router – czyli w polu „DNS Server” również wpisałem jego adres IP.

Przykładowa konfiguracja DHCP w CISCO:

```
Router (config) # ip dhcp pool mypool
```

```
Router (dhcp-config) #network 10.1.1.0 255.255.255.0
```

```
Router (dhcp-config) # default-router 10.1.1.1
```

Router (dhcp-config) # exit

Router (config) # ip dhcp excluded-address 10.1.1.1 10.1.1.9

DNS

Serwer DNS może przetłumaczyć nazwę URL wpisaną w przeglądarce na adres IP, dzięki czemu urządzenie może połączyć się ze stroną internetową (działa jak dawna książka telefoniczna). Jeśli chcesz zmienić internetowy serwer DNS, możesz zmienić adres IP internetowego serwera DNS w routerze, aby połączyć się z innym serwerem DNS. Na przykład serwery DNS Google mają adresy 8.8.8.8 i 8.8.4.4.

The screenshot shows the WAN configuration page of a TP-Link 300M Wireless N Router. The WAN Connection Type is set to Dynamic IP. The IP Address, Subnet Mask, and Default Gateway are all 0.0.0.0. The MTU Size is 1500. The Primary and Secondary DNS fields are empty. The Host Name is TL-WR841N. There are buttons for Renew, Release, and Save. A warning message indicates that the WAN port is unplugged.

CISCO:

Router (config) #ip dns server

Router (config) #ip domain-lookup

Router (config) #ip name-server 4.2.2.2

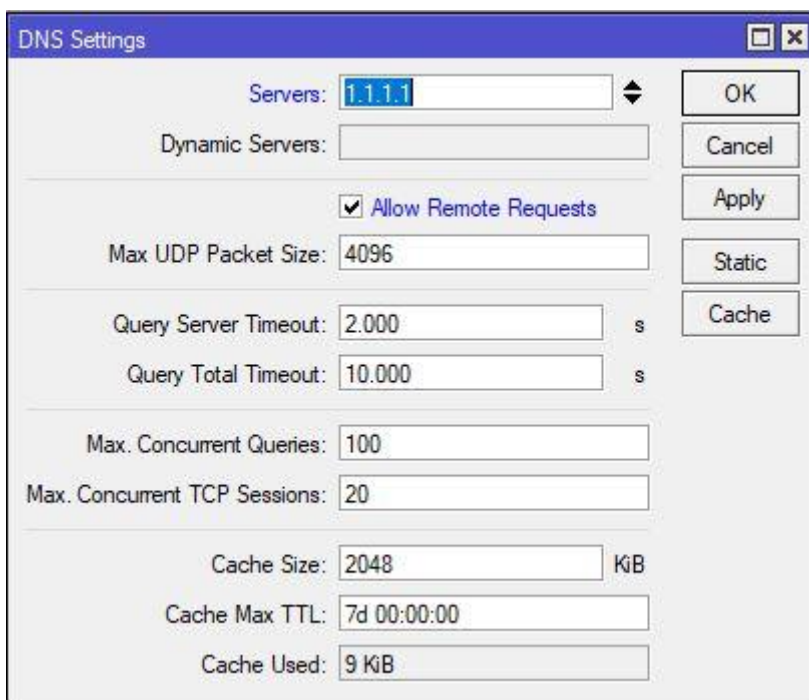
Później konfigurujemy DNS z lokalnymi hostami w lokalnej sieci np. ip host (nazwa), (adres IP).

Konfiguracja DNS Google dla Mikrotika: IP->DNS -> Servers:

The screenshot shows the DNS Settings window in Mikrotika. The Servers field contains 9.9.9.9 and 149.112.112.112. The Dynamic Servers field contains 1.1.1.1. The Use DoH Server checkbox is unchecked. The Allow Remote Requests checkbox is checked. The Max UDP Packet Size is 4096. The Query Server Timeout is 2.000 s. The Query Total Timeout is 10.000 s. The Max. Concurrent Queries is 100. The Max. Concurrent TCP Sessions is 20. The Cache Size is 2048 KiB. The Cache Max TTL is 7d 00:00:00. The Cache Used is 27 KiB.

Temat serwera DNS można rozwiązać na dwa sposoby. Albo nasze urządzenia w sieci LAN będą korzystały bezpośrednio z zewnętrznego serwera DNS. Wtedy w konfiguracji sieci serwera DHCP w polu DNS Server wpisujemy jego adres np. 8.8.8.8. Natomiast bardziej optymalnym pomysłem jest wykorzystanie naszego routera jako serwera DNS dla naszej sieci lokalnej. Będzie to klasyczny cache DNS który gdy otrzyma zapytanie z LAN'u sprawdzi czy nie ma już takiej domeny w pamięci. Gdy jej nie ma wyśle zapytanie do zewnętrznego serwera i zapamięta odpowiedź przez określony czas. Zapamiętany rekord będzie dostępny dla innych hostów korzystających z tego serwera. Taka konfiguracja skraca czas oczekiwania na odpowiedź DNS.

My zastosujemy wariant z lokalnym DNS. Aby to zrobić wchodzimy w menu IP->DNS. W polu Servers wpisujemy adres serwera DNS z którego ma korzystać nasz MikroTik (polecam tutaj darmowy publiczny DNS Cloudflare dostępny pod adresem 1.1.1.1) oraz zaznaczamy opcję „Allow Remote Requests”.



Puła adresowa – Mikrotik

IP pool – add new -> podajemy adres od do np. 192.168.2.2-192.168.2.12 -> ok. UWAGA, nie może być adres IP LAN routera

IP DHCP server -> networks +, wpisujemy adres sieci + Gateway dla interfejsu. DNS=Gateway

DHCP + wybrać nazwę bridge'a (w tym przypadku „pracownia219”, potem adres pool – „pracownia219”).

W DHCP leases sprawdzamy czy karta sieciowa PC połączyła się z pulą adresową (na PC też włączone DHCP). Jeśli nie ma komunikacji to w PC możemy w CMD wpisać: ipconfig /release a potem ipconfig /renew

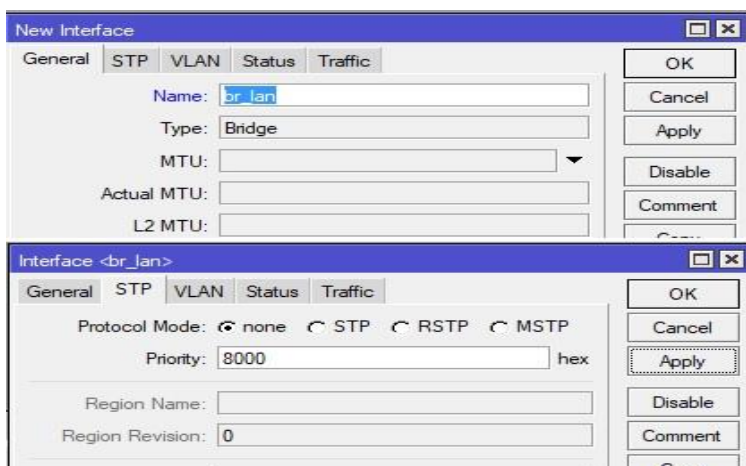
W DHCP leases prawym klikasz -> make static by na stałe rezerwować adres IP do karty sieciowej

DNS serwery jeśli chcemy mieć informacje z jakiego PC leci komunikacja.

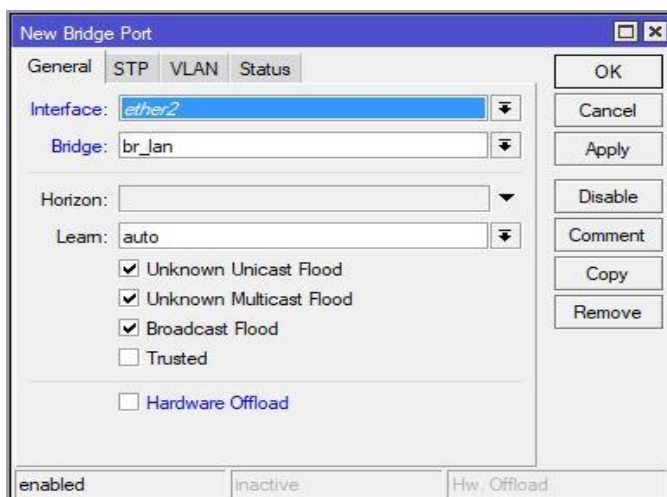
Bridge LAN

Po zalogowaniu pierwszą rzeczą jaką robimy to utworzenie bridge'a na którym stworzymy sieć LAN. Jest to wirtualny interfejs do którego połączą się inne interfejsy (ethernet, wifi, vlan, sfp) tak aby utworzyły jedną całość.

Aby to zrobić wchodzimy w zakładkę bridge w menu po lewej stronie i klikamy dodaj. W nowym oknie uzupełniamy tylko nazwę następnie przychodzimy do zakładki STP i zaznaczamy „Protocol Mode” na none.



Kolejnym krokiem jest przypisanie portów/interfejsów to utworzonego bridge'a. Zatem w otwartym wcześniej oknie bridge przechodzimy do zakładki Ports i klikamy dodaj. Wybieramy bridge oraz interfejs który chcemy do niego dodać. Należy zwrócić uwagę na pole „Hardware Offload”. Jest to funkcjonalność która pozwala na odciążenie użycia CPU poprzez obsługę części ruchu w ramach bridge'a przez switch chip. Działa ona wyłącznie w ramach jednego bridge na raz (czyli jeżeli mamy kilka interfejsów bridge tylko jeden z nich może korzystać z „Hardware Offload”). Włączenie opcji jest dobrym pomysłem przy prostych konfiguracjach. Opcja ta powinna się sama wyłączyć jeśli w konfiguracji inna opcja nie pozwala na obsługę ruchu przez switch chip. Jednak należy mieć na uwadze że w razie problemów dobrze jest ją wyłączyć na wybranych portach.



Bridge Mikrotik (bridgowanie portów routera tj. łączenie np. 2 interfejsów w 1)

Bridge -> dodajemy most (bridge)

Bridge -> ports

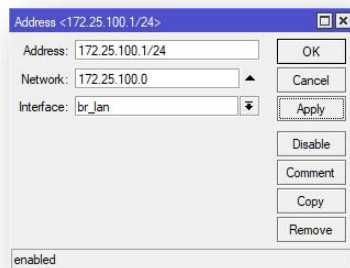
Bridge polega na spinaniu adresacji 2,3,4 interfejsów w 1.

Zakładka "interfaces" Czcionka prosta (nie kursywa) oznacza aktywny interfejs, R - oznacza running. Status portu możemy sprawdzić najeżdżając kursorem. Jak będziemy dodawać interfejs w bridgu to będzie nas wyrzucać – ucięta gałąź.

Przydzielamy adres IP (IP->addresses) do bridge'a np. 192.168.2.1/24 o nazwie pracownia219 (nazwa Bridge'a). Można wejść w ustawienia karty sieciowej PC i ustawić adres statyczny np. 192.168.2.1 z maską ale bez bramy. Można potem zalogować się do routera z przeglądarki – tam też jest możliwość konfigurowania.

Adresacja IP

Kolejnym krokiem jest skonfigurowanie adresacji w sieci LAN oraz utworzenie serwera DHCP który automatycznie skonfiguruje urządzenia działające w sieci lokalnej.



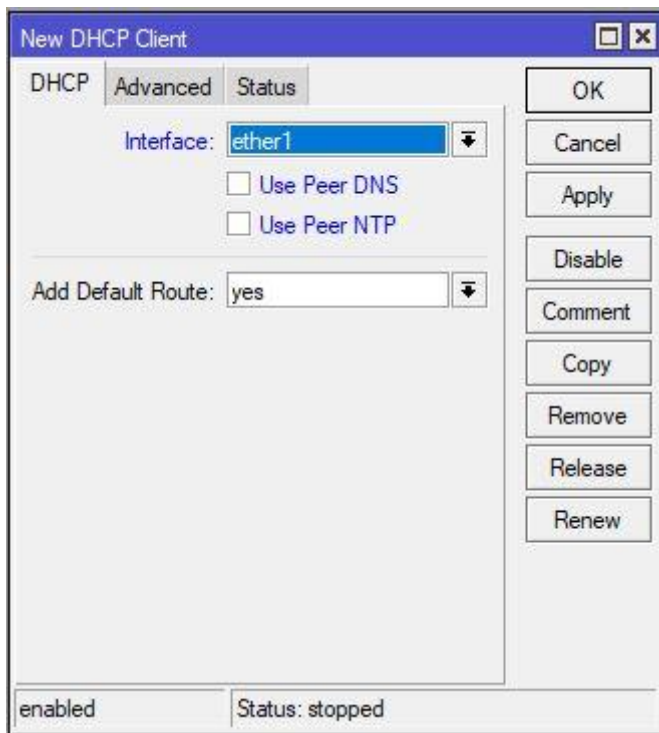
Na początku wchodzimy w zakładkę IP w menu po lewej stronie winbox'a, wybieramy Addresses i klikamy dodaj. A polu Address wpisujemy adres IP który nasz router będzie miał po stronie LAN. Proponuję zastosować jakiś bardziej ambitny niż 192.168.1.1 ze względu że może tak być że taki adres dostaniemy na WAN naszego routera (np. przy założeniu że to będzie nasz drugi router w domu a router dostawcy nie ma możliwości zmiany puli adresacji czy ustawienia go „przezroczyście”). Przykładowo użyjmy adresacji 172.25.100.0/24 umownie adres routera będzie pierwszym adresem w sieci czyli 172.25.100.1 interfejsem jest bridge lan czyli br_lan. Pole Network uzupełnia się automatycznie.

Bardzo ważne jest aby pamiętać że gdy jakiś interfejs jest dodany do bridge'a staje się jego częścią. Nie może być on już postrzegany jako osobny interfejs. Nie możemy wykorzystać go w firewallu, wskazać jako interfejs dla serwera dhcp itd. To wszystko robimy już na bridge'u do którego jest on dodany.

Konfiguracja interfejsu WAN

Na interfejsie WAN Mikrotik będzie działał po prostu klient DHCP. Pobierze on adres i podstawowe dane od naszego dostawcy. Aby to zrobić wchodzimy w menu IP->”DHCP

Client” i dodajemy nowego klienta. W nowym oknie wybieramy interfejs na którym ma działać klient. I to by w sumie wystarczyło jednak proponuję wyłączenie opcji „Use Peer DNS” i „Use Peer NTP” i już pisze dlaczego.

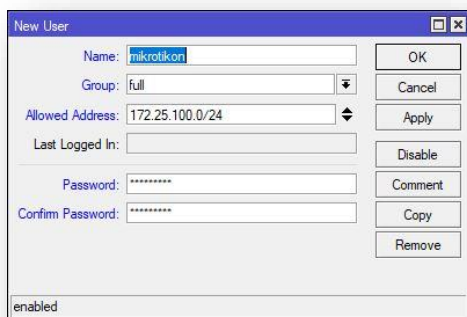


„Use Peer DNS” – ta opcja powoduje że lokalny DNS routera będzie korzystał z serwerów które poda dostawca. Jednak takie serwery często mają swoje mankamenty, i statystycznie istnieje większe ryzyko awarii niż w firmach taki jak Google czy Cloudflare. Także polecam wpisanie DNS takich jak: 1.1.1.1, 8.8.8.8 lub skorzystanie z systemu OpenDNS.

„Use Peer NTP” – ta opcja powoduje że MikroTik będzie korzystał z serwera czasu podanego przez dostawcę (o ile ISP go poda). W mojej opinii nie ma sensu ponieważ systemy RouterOS korzystają z chmury MikroTik do synchronizacji czasu. W terminalu możemy wpisać /ip route print detail lub /ip dns print by sprawdzić adresację i tablicę routingu.

Zabezpieczenie routera

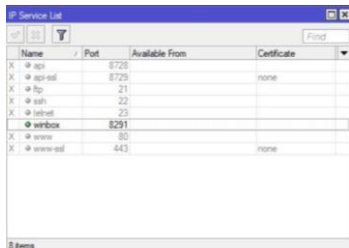
Zmiana domyślnego użytkownika i ustawienie hasła.



Podstawową sprawą jest ustawienie hasła logowania do naszego MikroTik'a. Proponuję również przy okazji otworzyć użytkownika o loginie innym niż admin. Aby to zrobić przechodzimy do menu System->Users i dodajemy nowego użytkownika. Uzupełniamy nazwę użytkownika a jako grupę wybieramy full. Warto również w polu „Allowed Address” wpisać adresy z których będzie można się zalogować jako ten użytkownik. Tutaj dla przykładu będą to wszystkie adresy z naszego LAN'u. Następnie wymyślamy silne hasło i zatwierdzamy.

Należy teraz się wylogować z urządzenia i zalogować jako nowo utworzony user. Następnie ponownie wejść to zarządzania użytkownikami i koniecznie usunąć użytkownika admin.

Konfiguracja IP Services



Name	Port	Available From	Certificate
X <input type="checkbox"/> ssh	22		
X <input type="checkbox"/> sftp	22		
X <input type="checkbox"/> telnet	23		
X <input type="checkbox"/> winbox	8291		
X <input type="checkbox"/> www	80		
X <input type="checkbox"/> www-ssl	443		

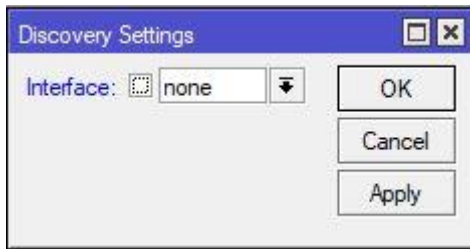
Kolejnym ważnym tematem jest konfiguracja tzw. serwisów czyli usług przez które można uzyskać dostęp do naszego MikroTik'a. Konfigurujemy je w menu IP->Services. W założeniu że nasz MikroTik ma być po prostu routerem domowym w zupełności wystarczy wyłączenie wszystkich z wyjątkiem winbox'a. Opcjonalnie możemy również dla każdego serwisu dopisać sieć z której ma być on dostępny.

Dostęp przez adres MAC

MikroTik domyślnie ma włączony tzw. mac server czyli funkcjonalność pozwalającą na logowanie się przez adres MAC z urządzenia w tej samej domenie rozgłoszeniowej. Jest to dobre rozwiązanie w przypadku sieci bardziej rozbudowanych jednak w przypadku sieci domowej jest ono niepotrzebne. Wyłączyć je możemy w menu Tools -> „MAC Server”.



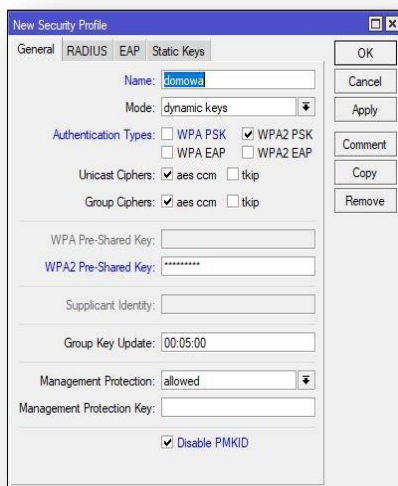
Wchodzimy po kolei w każdy z 3 rodzajów MAC server'a.



Dodatkowo proponuję wyłączyć tzw. „MikroTik Neighbor Discovery protocol” czyli protokół dzięki któremu urządzenia MikroTik badają swoje otoczenie i mogą zobaczyć sąsiednie urządzenia MikroTik. Jego włączenie powoduje też widoczność routera w programie winbox w liście Neighbors. Jednak w sieci domowej jest on niepotrzebny tym bardziej że wiemy jaki jest jego lokalny adres IP aby się z nim połączyć. W celu jego wyłączenia wchodzimy w menu IP->Neighbors następnie w „Discovery Settings” i wybieramy z listy none, checkbox obok listy rozwijalnej też musi być niezaznaczony.

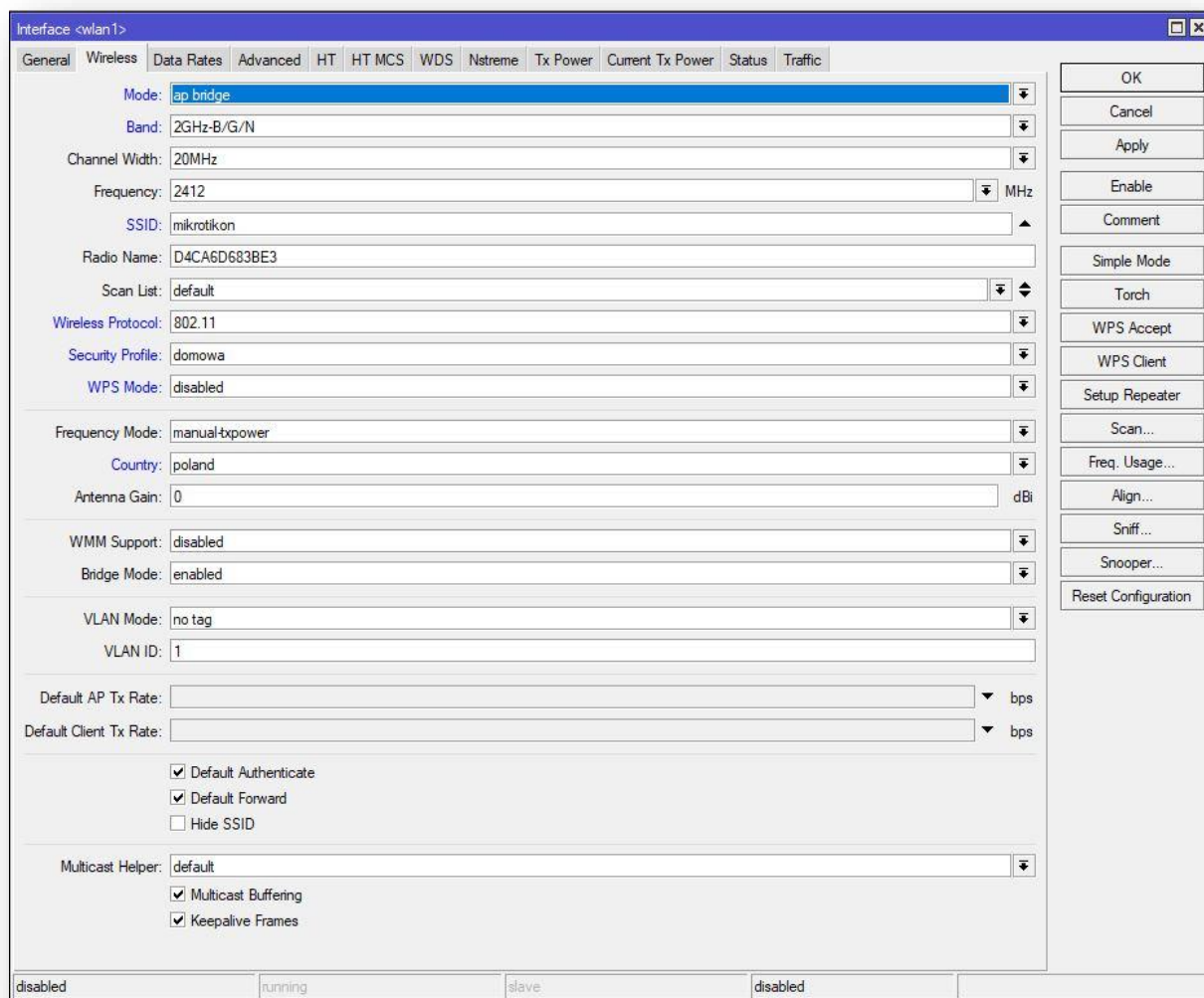
Konfiguracja sieci bezprzewodowej

Konfiguracja sieci bezprzewodowej to temat na osobny artykuł. Jednak aby nasz router mógł być pełnoprawnym urządzeniem domowym musi też rozgłaszać sieć WiFi.



Konfigurację zaczynamy wchodząc w menu Wireless i przechodzimy do zakładki „Security Profiles” gdzie dodajemy nową politykę. Wpisujemy nazwę profilu następnie w „Authentication Types” zostawiamy zaznaczoną tylko opcję „WPA2-PSK” i wpisujemy klucz zabezpieczeń sieciowych. Proponuję też zaznaczyć opcję „Disable PMKID”. Rozwiąże ona podatność na atak dla protokołu WPA2-PSK.

Jeżeli w naszej sieci mamy też starsze urządzenia może być konieczne włączenie starszego szyfrowania WPA-PSK i/lub włączenie PMKID.

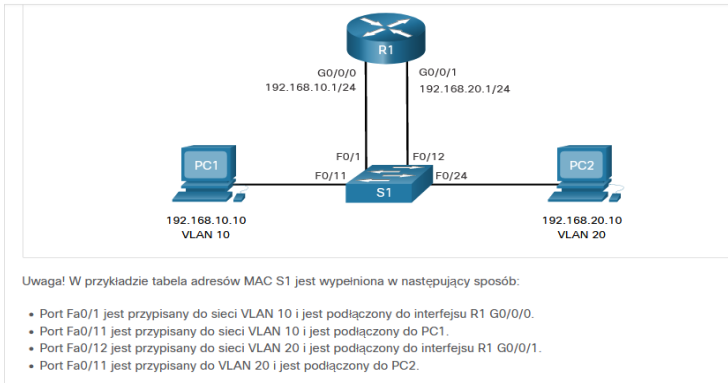


Następnie w oknie „Wireless Tables” przechodzimy do zakładki „WiFi Interfaces” i wchodzimy w interfejs Wi-Fi. W nowym oknie w zakładce Wireless zmieniamy Mode na „ap bridge” polecam też kliknąć w „Advanced Mode” po prawej stronie okna aby zobaczyć więcej opcji konfiguracji. Band ustawiamy na 2GHz-B/G/N. Szerokość kanału proponuję ustawić najpierw na 20MHz aby uzyskać teoretycznie lepszy zasięg do testów WiFi. Częstotliwość proponuję ustawić na kanał 1 lub 6 lub 11. Protokół ustawiamy jako 802.11. SSID to nazwa sieci naszej sieci WiFi. Jeżeli nie potrzebujemy funkcji WPS dobrze jest ją wyłączyć. Ostatnim elementem jest ustawienie kraju.

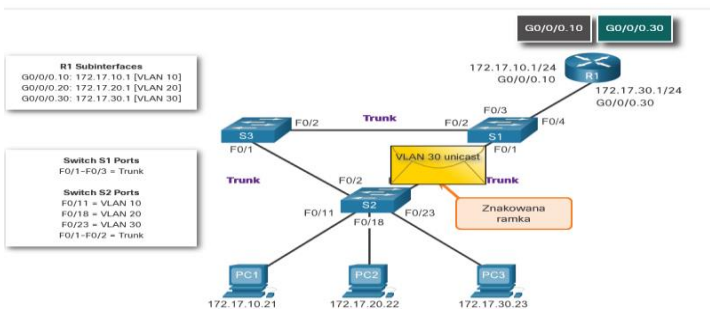
Routing

Metody routingu:

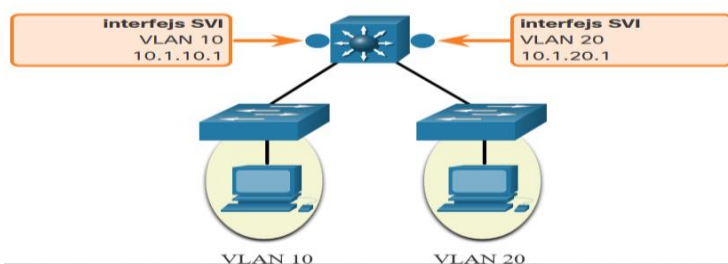
Tradycyjna metoda routingu - użycie routera z wieloma interfejsami Ethernet, niestosowana obecnie:



Routing na patyku - wymaga tylko 1 interfejsu do kierowania ruchu między VLAN, router nie jest w centrum topologii, wymagane jest utworzenie podinterfejsów dla każdej sieci VLAN, która ma być routowana, rozwiązanie dla małych/średnich organizacji, nie skaluje się łatwo:



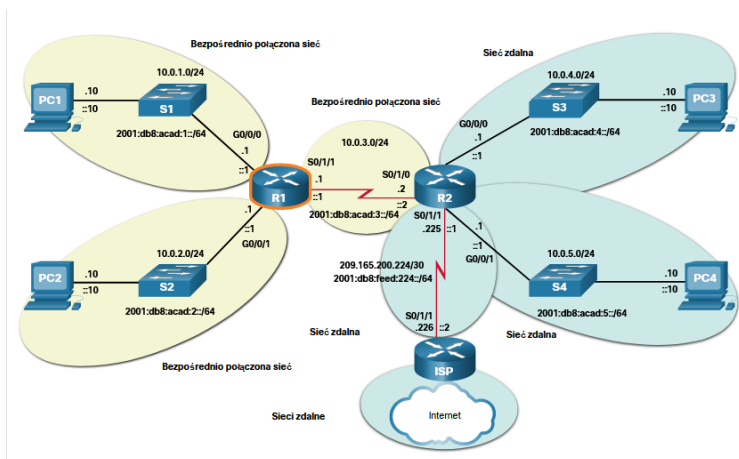
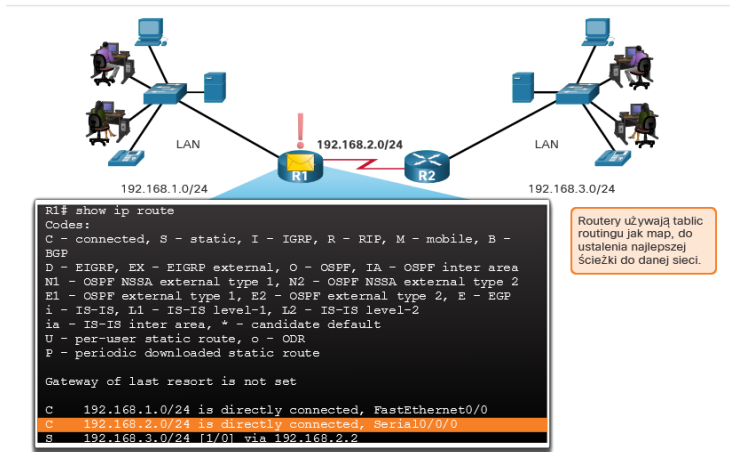
Routing z przełącznikiem warstwy 3 (korzystamy z wirtualnych interfejsów (SVI) i przełączników pracujących na warstwie 3, szybszy niż routing na patyku):



Zadaniem routingu jest określenie najlepszej ścieżki na podstawie tabeli routingu. Sieci zdalne to sieci, które nie są bezpośrednio połączone z routerem. Routery uczą się o sieciach na dwa sposoby:

- **Trasy statyczne** - dodane do tabeli routingu, gdy trasa jest ręcznie skonfigurowana.

- **Dynamiczne protokoły routingu** - gdy protokoły routingu dynamicznie dowiadują się o sieci zdalnej. Dynamiczne protokoły routingu obejmują Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF).



Trasa domyślna

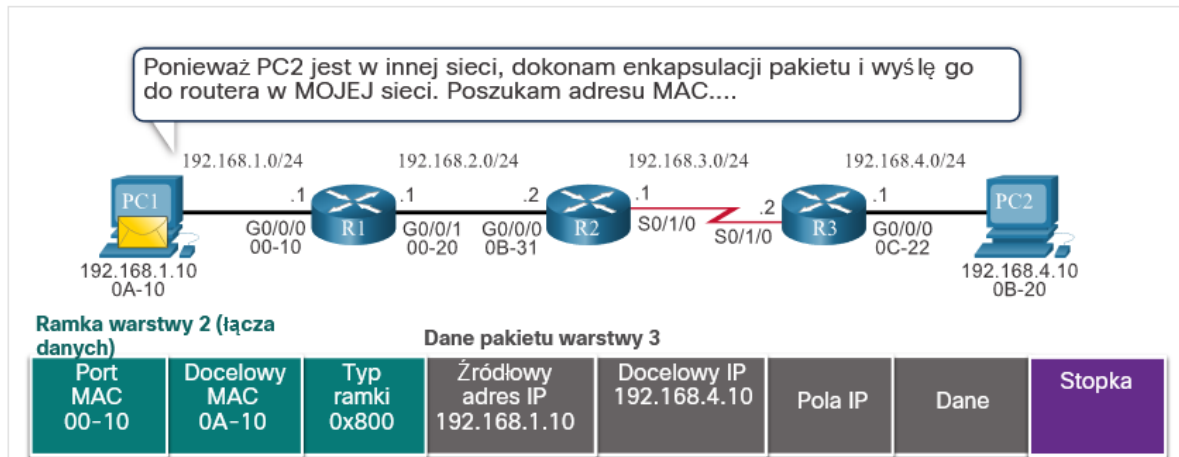
Trasa domyślna określa router następnego przeskoku, który ma być używany, gdy tabela routingu nie zawiera określonej trasy zgodnej z docelowym adresem IP. Trasa domyślna może zostać wprowadzona ręcznie jako trasa statyczna lub wyuczona automatycznie na podstawie protokołu routingu dynamicznego. Trasa domyślna ma wpis trasy IPv4 0.0.0.0/0 lub wpis trasy IPv6::/0.

Tablica ARP w routerze

- **Pakiet IPv4** - Router sprawdza tabelę ARP pod kątem docelowego adresu IPv4 i powiązanego adresu MAC Ethernet. Jeśli nie ma dopasowania, router wysyła żądanie ARP. Urządzenie docelowe zwróci odpowiedź ARP z adresem MAC. Router może teraz przesyłać pakiet IPv4 w ramce Ethernet z odpowiednim docelowym adresem MAC.
- **Pakiet IPv6** - Router sprawdza swoją pamięć podręczną sąsiada dla docelowego adresu IPv6 i powiązanego adresu MAC Ethernet. Jeśli nie ma dopasowania, router wysyła komunikat ICMPv6 Neighbor Solicitation (NS). Urządzenie docelowe zwróci

komunikat ICMPv6 Neighbor Advertisement (NA) z adresem MAC. Router może teraz przesyłać pakiet IPv6 w ramce Ethernet z odpowiednim docelowym adresem MAC.

W pierwszej animacji PC1 wysłał pakiet do PC2. Należy zauważyć, że jeśli wpis ARP nie istnieje w tabeli ARP dla bramy domyślnej 192.168.1.1, PC1 wysłał żądanie ARP. Router R1 zwrócił odpowiedź ARP.



Tablica routingu - zawiera listę tras do znanych sieci (prefiksy i długości prefiksów). Źródłem tych informacji są sieci połączone bezpośrednio, trasy statyczne oraz protokoły routingu dynamicznego:

```
R2# 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
       I - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       a - application route
       * - replicated route, % - next hop override, p - overrides from PBR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 209.165.200.226
  10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O 10.0.1.0/24 [110/65] via 10.0.3.1, 00:31:38, Serial0/1/0
O 10.0.2.0/24 [110/65] via 10.0.3.1, 00:31:38, Serial0/1/0
C 10.0.3.0/24 is directly connected, Serial0/1/0
L 10.0.3.2/32 is directly connected, Serial0/1/0
C 10.0.4.0/24 is directly connected, GigabitEthernet0/0/0
L 10.0.4.1/32 is directly connected, GigabitEthernet0/0/0
C 10.0.5.0/24 is directly connected, GigabitEthernet0/0/1
L 10.0.5.1/32 is directly connected, GigabitEthernet0/0/1
  209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.165.200.224/30 is directly connected, Serial0/1/1
L 209.165.200.225/32 is directly connected, Serial0/1/1
R2#
```

- **L** \ - Identyfikuje adres przypisany do interfejsu routera. Pozwala to routerowi na wydajne określenie, kiedy otrzymuje pakiet skierowany do interfejsu, zamiast przekazywać go dalej.
- **C** - Identyfikuje bezpośrednio połączoną sieć.
- **S** - Identyfikuje trasę statyczną utworzoną w celu dotarcia do określonej sieci.
- **O** - Identyfikuje dynamicznie wyuczoną sieć z innego routera przy użyciu protokołu routingu OSPF.
- ***** - Ta trasa jest kandydatem dla trasy domyślnej.

Głównym poleceniem służącym do zmieniania tablicy routingu jest **route**. Wyświetla ono tablicę – warto dołożyć **-n**.

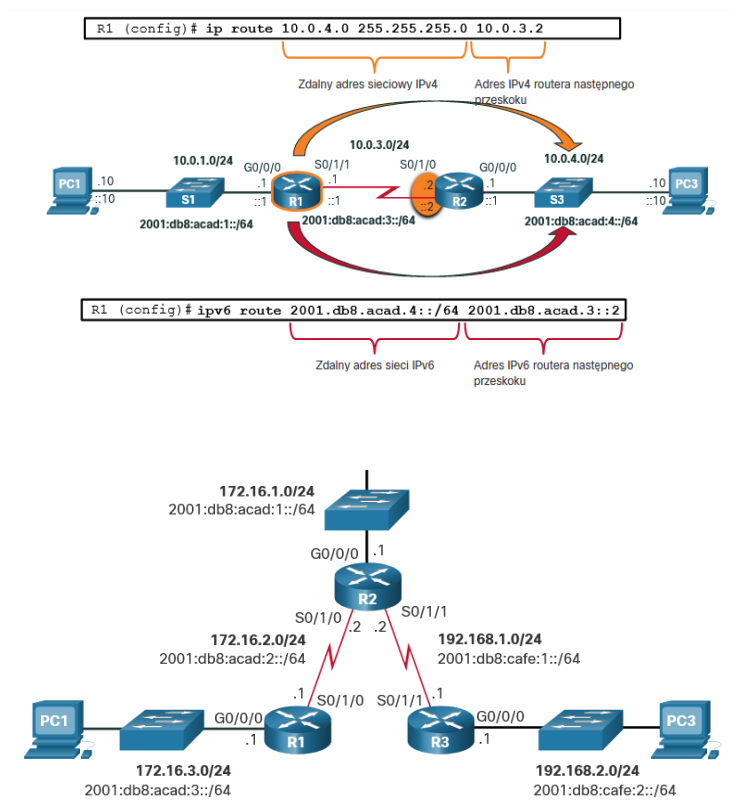
Konfiguracja tablicy routingu w routerze z interfejsem lo:

```
# route add -net 127.0.0.0 netmask 255.0.0.0 lo
# route add -net 192.168.1.0 netmask 255.255.255.0 eth0 (dodajemy kartę eth routera),
# route add -net 10.0.0.0 netmask 255.0.0.0 eth1 (dodajemy kartę eth1),
# route add default gw 10.0.0.1 (definiujemy trasę domyślną dla routera).
```

Trasy statyczne.

Trasy statyczne są konfigurowane ręcznie. Definiują one jawnie ścieżkę pomiędzy dwoma urządzeniami sieciowymi. W przeciwieństwie do protokołu routingu dynamicznego, trasy statyczne nie są aktualizowane automatycznie i muszą zostać zrekonfigurowane ręcznie po każdej zmianie topologii. Zaletą stosowania tras statycznych jest zwiększone bezpieczeństwo oraz wydajność zużycia zasobów. Trasy statyczne zużywają mniej pasma niż dynamiczne protokoły routingu i nie obciążają CPU do obliczania i informowania o trasach. Routing statyczny ma trzy podstawowe zastosowania:

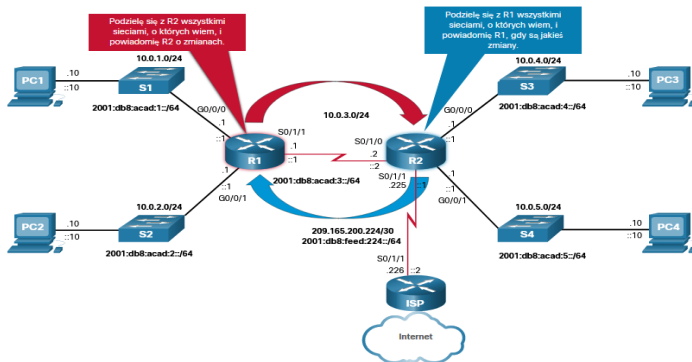
- Zapewnia łatwość obsługi tablic routingu w mniejszych sieciach, w przypadku których nie oczekuje się znacznego wzrostu.
- Używa pojedynczej trasy domyślnej do reprezentowania ścieżki do dowolnej sieci, która nie ma dokładniejszego dopasowania z inną trasą w tablicy routingu. Trasy domyślne są używane wtedy, gdy router nie znajduje dla danej sieci docelowej, pasującej pozycji w tablicy routingu.
- Kieruje do i z sieci pośredniczących.



rzy bezpośrednio połączone trasy statyczne IPv4 są konfigurowane na routerze R1 przy użyciu interfejsu wyjściowego.

```
R1 (config)# ip route 172.16.1.0 255.255.255.0 s0/1/0
R1 (config)# ip route 192.168.1.0 255.255.255.0 s0/1/0
R1 (config)# ip route 192.168.2.0 255.255.255.0 s0/1/0
```

Routing dynamiczny



Przykład routingu (spaja 2 sieci tj. 2 routery)

OSPF (*Open Shortest Path First*), w wolnym tłumaczeniu: „pierwszeństwo ma najkrótsza ścieżka” – protokół trasowania oparty na analizie stanu łącza (ang. *link-state*), kontroluje przepływ pakietów wewnątrz systemu autonomicznego (*Autonomous System, AS*).

Cechami protokołu OSPF są: trasowanie wielościeżkowe, trasowanie najmniejszym kosztem.

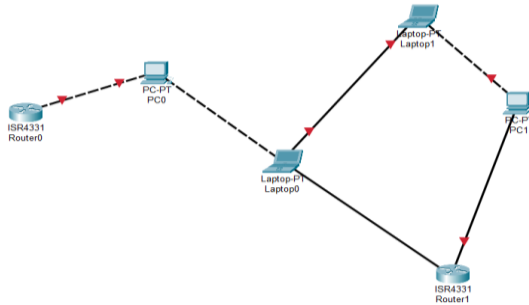
Jest zalecanym protokołem wśród protokołów niezależnych, do których należy także RIP. W przeciwieństwie do protokołu RIP, charakteryzuje się dobrą skalowalnością, wyborem optymalnych ścieżek, przyspieszoną zbieżnością i brakiem ograniczenia skoków powyżej 15. Protokół OSPF używa hierarchicznej struktury sieci z podziałem na obszary, z centralnie umieszczonym obszarem zerowym (*area 0*), który pośredniczy w wymianie tras między wszystkimi obszarami w domenie OSPF. Przeznaczony jest dla sieci posiadających do 500 routerów w wyznaczonym obszarze trasowania. Routery korzystające z tego protokołu porozumiewają się ze sobą za pomocą pięciu komunikatów:

- *hello* – nawiązywanie i utrzymywanie relacji sąsiedzkich,
- *database descriptions* – opis przechowywanych baz danych,
- *requests link-state* – żądanie informacji na temat stanów połączeń,
- *updates link-state* – aktualizacja stanów połączeń,
- *acknowledgments links-state* – potwierdzenia stanów połączeń.

OSPF jest protokołem typu *link-state* jedynie wewnątrz obszaru. Oznacza to, że w ramach pojedynczego obszaru wszystkie routery znają całą jego topologię i wymieniają się między sobą informacjami o stanie łącza, a każdy z nich przelicza trasy samodzielnie (zob. algorytm Dijkstry). Między obszarami OSPF działa jak protokół typu *distance-vector*, co oznacza, że routery brzegowe obszarów wymieniają się między sobą gotowymi trasami. Istnienie obszaru zerowego umożliwia trasowanie pakietów pomiędzy obszarami bez powstawania pętli.

Aby zmniejszyć liczbę pakietów rozsyłanych w sieci, OSPF wybiera router desygnowany DR (ang. *designated router*) oraz zapasowy BDR (*backup designated router*), które służą do wymiany informacji o stanie łącza z pozostałymi routerami OSPF. Komunikat *hello* służy tutaj do wyboru DR i BDR oraz do wykrywania nieaktywnych sąsiednich routerów OSPF.

Popatrzmy na przykład poniżej. Załóżmy, że wszystkie interfejsy są Fastethernet poza laptopem 0 do laptopa 1 i od laptopa 1 do PC1 i do Routera na dole (te są Gigabitowe). Protokół RIP wybrałby najkrótszą ścieżkę czyli R0->PC0->Laptop0-> R1 (na podstawie ilości przeskoków tj. urządzeń). Tylko ta trasa byłaby dużo wolniejsza niż ta, którą wybrałby OSPF: R0->PC0->L0->L1->PC1->R1 ponieważ tam od Laptopa zero jest dużo szybsza prędkość interfejsu.



Przykładowo, aby ustawić routing statyczny do sieci 192.168.10.0, należy wydać polecenie:
 route ADD 192.168.10.0 MASK 255.255.255.0 192.168.10.1 5

RIP vs RIP 2

Najprostszy sposób routingu z tym, że RIP1 może trasować tylko w sieciach z maskami /8, /16, /24 a RIP2 jest protokołem bezklasowym i obsługuje podsieci z maskami o dowolnej długości. Konfiguracja RIP2 (przykładowa):

```
configure terminal -> router rip -> version 2 -> network 10.0.0.0 -> network 192.168.1.0 -> end
(analogicznie należy skonfigurować 2 router).
```

Konfiguracja RIP w Mikrotiku hAP:

By skonfigurować interfejs np. Ethernet1 należy z menu bocznego wybrać ip/addresses, w oknie address list kliknąć + i wprowadzić dane interfejsu (adres ip i sieci oraz maska) a potem apply i ok (np. 10.0.0.1/30 -> 10.0.0.0 -> ether1). By skonfigurować port Ethernet 2, wybieramy z menu bocznego ip/addresses. W oknie address list kliknąć +, wprowadzić dane konfiguracyjne interfejsu, kliknąć apply i ok (np. 192.168.1.1/24 -> 192.168.1.0 -> ether2).

Teraz konfigurujemy RIP. Z menu bocznego wybieramy routing/rip, rip->networks, +, wpisać 10.0.0.0 i 192.168.1.0. (łącznie 2 wiersze). Kliknąć apply i ok.

Skonfigurować 2 router. Dla interfejsu Eth1 przydzielić adres 10.0.0.2/30, a Eth2 192.168.2.1/24. Skonfigurować protokół routingu tj. dodać sieci 10.0.0.0 i 192.168.2.0. Do portów Eth2 w obu routerach podłączyć hosty z odpowiednią adresacją IP i spingować.

Bridgowanie a routing w hAP

Teraz skonfigurujemy sieć szkolną 10.0.0.8 z siecią lokalną 192.168.10.0/24.

Konfigurujemy port WAN, z reguły jest to Eth1 od dostawcy sieci. Jeśli nie chcemy DHCP, możemy samodzielnie wprowadzić dane dostawcy w zakładce: ip/addresses -> address list +, wprowadzamy dane konfiguracyjne WAN: 10.1.51.101, network: 255.0.0.0, eth1.

Teraz konfigurujemy LAN: porty ethernet są połączone mostem. Teraz przypiszemy adres IP do mostu bridge. Wybieramy: bridge -> ports -> + wskazać porty należące do mostu. By wprowadzić adres IP do mostu należy z menu wybrać ip/addresses-> address list -> + wprowadzić dane konfiguracyjne mostu (192.168.10.1/24, network: 192.168.10.0, interface: bridge) i kliknąć apply i ok.

Z menu bocznego klikamy quick set a w nim ustawiamy:

adres bramy 10.1.1.1, DNS 8.8.8.8 i 8.8.4.4, włączenie DHCP i zakres np. od 192.168.10.100 do 192.168.10.110, usługę NAT a potem apply i ok.

Ustawienie interfejsu wewnętrznego o adresie 10.0.0.1/24 dla technologii NAT:

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip address 10.0.0.1 255.255.255.0
Router(config-if)#ip nat inside
```

Część 2 - konfiguracja przełącznika

CISCO

Przełączniki eliminują domeny kolizyjne, zmniejszają przeciążanie sieci.

Przełączniki CISCO posiadają 5 etapową sekwencję rozruchu. Procedura POST zapisana w pamięci ROM, po POST uruchamia się program boot loader, który inicjuje pracę CPU oraz system plików pamięci Flash na płycie głównej i na końcu wyszukuje lokalizuje i ładuje system IOS.

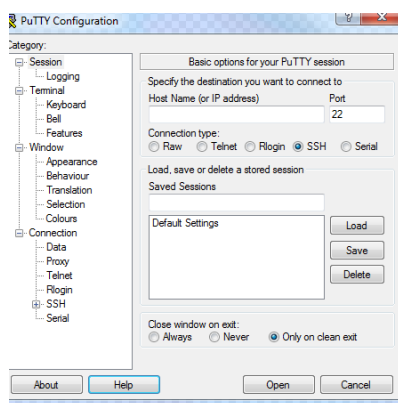
Jeśli przełącznik ma być zarządzany zdalnie (SVI) to musi mieć skonfigurowaną bramę domyślną. Komunikacja w przełącznikach odbywa się na zasadzie full duplex (jednoczesne wysyłanie i odbieranie, działa w domenie rozgłoszeniowej) oraz half duplex (wysyłanie lub odbieranie, działa w domenie kolizji). Karty sieciowe Gigabit Ethernet i 10Gb wymagają full duplex. Autonegociacja jest przydatna, gdy ustawienia prędkości i duplexu urządzenia podłączonego do portu są nieznane lub mogą ulec zmianie.

Rodzaje ramek w przełącznikach to ingress (wchodzą do przełącznika) i egress (wychodzą z przełącznika). Ramka Ethernet nigdy nie zostanie przekazana do tego samego portu, którym została odebrana. Im ramki są mniejsze tym więcej można ich przesłać w danym przedziale czasowym. Jednakże większe natężenie ruchu ramek to większe prawdopodobieństwo kolizji.

Resetowanie hasła switcha TPLINK i innych ustawień

1 część wykonujemy na wyłączonym switchu. Należy wpiąć kabel RS232 do właściwego portu o nazwie „console” (kabel konsolowy i przejściówkę). Potem sprawdzamy numer portu „com” w menadżerze urządzeń w PC.

W putty lub terra term łączymy za pomocą „serial”, prędkość zmieniamy na 38400. Wpisujemy właściwy numer portu np. „Com3”. Następnie na dole menu po lewej w zakładce „SSH”-> Serial musi być 2x „none”. Teraz włączamy switcha.



Klikamy w dowolny przycisk by przerwać bootowanie systemu. By zresetować hasło wpisujemy „6” – password recovery. Pamiętamy o reboocie i resecie.

Auto MDIX (automated medium dependent interface crossover) to funkcja, która upraszcza połączenie 2 przełączników ze sobą lub przełącznika z routerem. Gdy jest włączona – automatycznie wykrywa rodzaj kabla i konfiguruje połączenie.

Rodzaje błędów w komunikacji przełącznika:

```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0025.83e6.9092 (bia 0025.83e6.9092)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    2295197 packets input, 305539992 bytes, 0 no buffer
      Received 1925500 broadcasts (74 multicasts)
        0 runts, 0 giants, 0 throttles
        3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored
        0 watchdog, 74 multicast, 0 pause input
        0 input packets with dribble condition detected
    3594664 packets output, 436549843 bytes, 0 underruns
      8 output errors, 1790 collisions, 10 interface resets
```

Input errors – runt, no buffer CRC, błędy ramek

Runt – pakiety są pomijane bo są mniejsze niż minimalny rozmiar pakietu

Giant – plakiety są pomijane bo są większe niż rozmiar pakietu,

CRS – błąd sumy kontrolnej (obliczona nie jest taka sama jak otrzymana), błąd mediów/kabla.

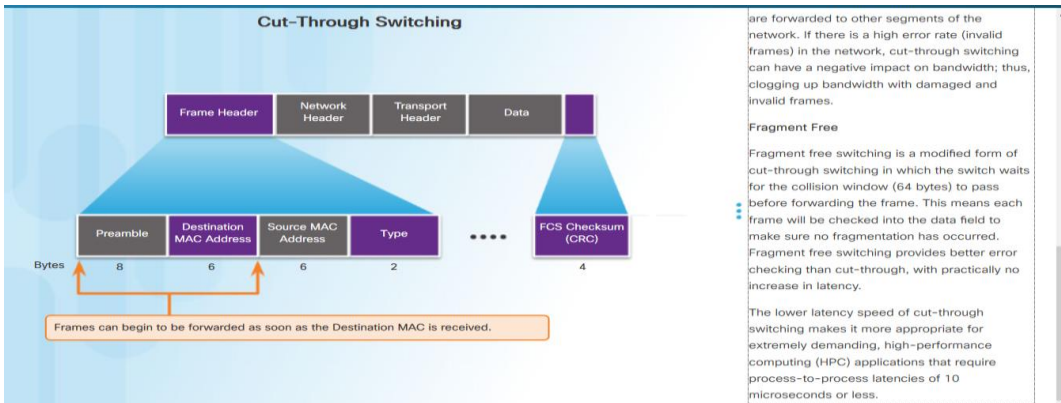
Kolizje – kolizje ramek, np. gdy kabel jest zbyt długi.

Dostęp zdalny do przełącznika

Telnet – niezabezpieczony dostęp do switcha, komunikacja i uwierzytelnianie idzie otwartym tekstem.

SSH – zabezpieczony/zaszyfrowany sposób komunikacji ze switchem.

Sieci, które bazują na przełącznikach zapewniają zarządzanie ruchem sieciowym, jakość usług (QoS) tj. ustalenie priorytetu dla portu lub np. audio kosztem video, wsparcie bezpieczeństwa, obsługę telefonów z IP. Switche przekazują ramki na warstwie 2 (łącza danych) oraz posiadają tabelę adresów MAC. Główne decyzje, które podejmują switche to decyzja jakim portem zostaną wprowadzone dane oraz jaki jest adres docelowy ramki. Aby przełącznik wysłał ramkę w odpowiednie miejsce musi najpierw nauczyć się jakie urządzenia są do niego wpięte (na podstawie adresów fizycznych MAC). Ramka ma w swojej pamięci adres MAC urządzenia wysyłającego oraz numer portu switcha. Jeśli adres MAC nie znajduje się w tablicy tj. on dodawany. Metody przesyłania ramek przez switch to store-and-forward (po otrzymaniu całej ramki, switch podejmuje decyzję o wysłaniu jej do urządzenia docelowego, sprawdzane są również błędy za pomocą mechanizmu CRC – Cyclic Redundancy Check, ta metoda ma elastyczność w automatycznym buforowaniu, np. przesłanie 100Mb/s przez port 1Gigabitowy) oraz cut-through, gdzie ramka jest forwardowana zanim otrzyma informacje o porcie wychodzącym (dzieli ją na części) i adresie docelowym MAC ramki wchodzącej. Cut through prześle ramkę zawierającą błędy/nie odrzuci jej a switch and forward nie prześle i odrzuci ją.



W rozwiązaniach biznesowych istnieją np. switche modułarne np. spięte 9 switchów razem:

Chapter 4 Switched Networks > 4.1 LAN Design > 4.1.2 Switched Networks > 4.1.2.2 Form Factors

Stackable Configuration Switches

Stackable switches, connected by a special cable, effectively operate as one large switch.

line card could have an additional 24-port line card installed to bring the total number of ports up to 48.

Stackable Configuration Switches

Stackable configuration switches can be interconnected using a special cable that provides high-bandwidth throughput between the switches (Figure 4). Cisco StackWise technology allows the interconnection of up to nine switches. Switches can be stacked one on top of the other with cables connecting the switches in a daisy chain fashion. The stacked switches effectively operate as a single larger switch. Stackable switches are desirable where fault tolerance and bandwidth availability are critical and a modular switch is too costly to implement. By cross-connecting these stacked switches, the network can recover quickly if a single switch fails. Stackable switches use a special port for interconnections. Many Cisco stackable switches also support StackPower technology, which enables power sharing among stack members.

Chapter 4 Switched Networks > 4.1 LAN Design > 4.1.2 Switched Networks > Activity - Identify Switch Hardware

Activity - Selecting Switch Hardware

Instructions

Read the switch selection criteria and locate the switch category names which best represent them. Drag the category name representing the criteria to the appropriate field.

Category Name

Stackable

Power

Reliability

Scalability

Port Density

Switch Selection Criteria

Affected by the number of network devices to support

Redundancy through PoE

How fast the interfaces will process network data

Continuous access to the network

Affected by the number of interfaces, features, and expandability

The capacity to store frames in the cache

Ability to adjust to growth of network users

Switches with adjustable switching line/port cards

Switches with pre-set features or options

Daisy-chain switches with high-bandwidth throughput

Check Reset

Activity - Switch It!

Instructions

Determine how the switch forwards a frame based on the Source MAC and Destination MAC addresses and information in the switch MAC table. Answer the questions below using the information provided.

Frame

Preamble	Destination MAC	Source MAC	Length	Type	Encapsulated Data	End of Frame
0E	0E	0D				

MAC Table

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
0A	0B	0C	0D	0E	0F						

Question 1 - Where will the switch forward the frame?

Fa1 Fa2 Fa3 Fa4 Fa5 Fa6 Fa7 Fa8 Fa9 Fa10 Fa11 Fa12

Question 2 - When the switch forwards the frame, which statement(s) are true?

Switch adds the source MAC address to the MAC table.

Frame is a broadcast frame and will be forwarded to all ports.

Frame is a unicast frame and will be sent to specific port only.

Frame is a unicast frame and will be flooded to all ports.

Frame is a unicast frame but it will be dropped at the switch.

Catalyst 2950 Series

Fa1 Fa2 Fa3 Fa4 Fa5 Fa6 Fa7 Fa8 Fa9 Fa10 Fa11 Fa12

Fa0E Fa0F

Check Help New Problem

Przypisywanie adresów MAC na stałe do portów

Jest to potrzebne by określony MAC nie uległ przedawnieniu (max. 300s) lub by zapewnić większe bezpieczeństwo. Konfiguracja w CISCO:

```
mac-address-table static <adres mac hosta> interface fastethernet <identyfikatorEthernet> vlan <nazwa sieci vlan>
```

usuwanie konfiguracji:

```
no mac-address-table static <adres mac hosta> interface fastethernet <identyfikatorEthernet> vlan <nazwa sieci vlan>
```

Można też skorzystać z komendy: clear mac-address-table.

Agregacja portów

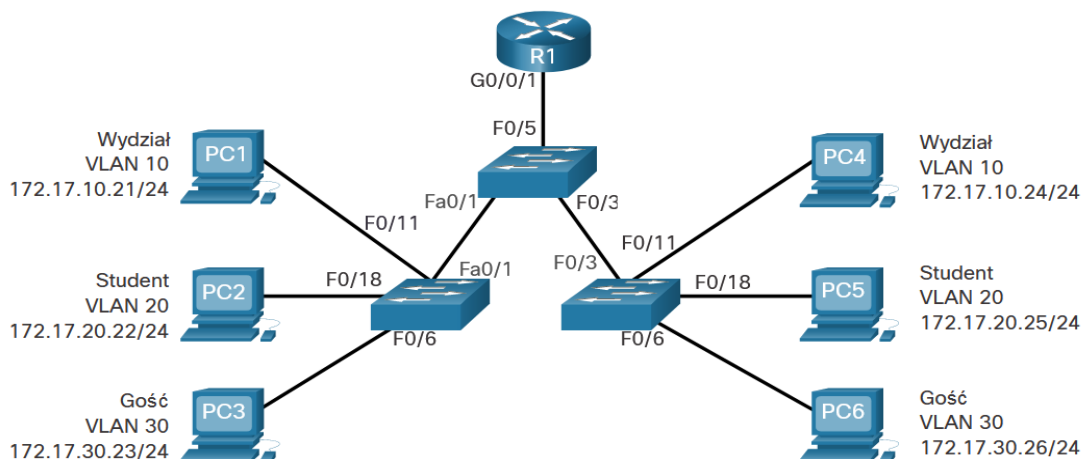
Łączenie kilku portów w 1 logiczny port to agregacja. Zagregowanie kilku portów w 1 zwiększa przepustowość łącza. Do agregacji wykorzystywany jest protokół PagP (CISCO) oraz LACP:

```
Enable-> configure terminal -> interface range fastethernet 0/1-4 (agregujemy 4 porty),  
channel-group 1 mode active -> end
```

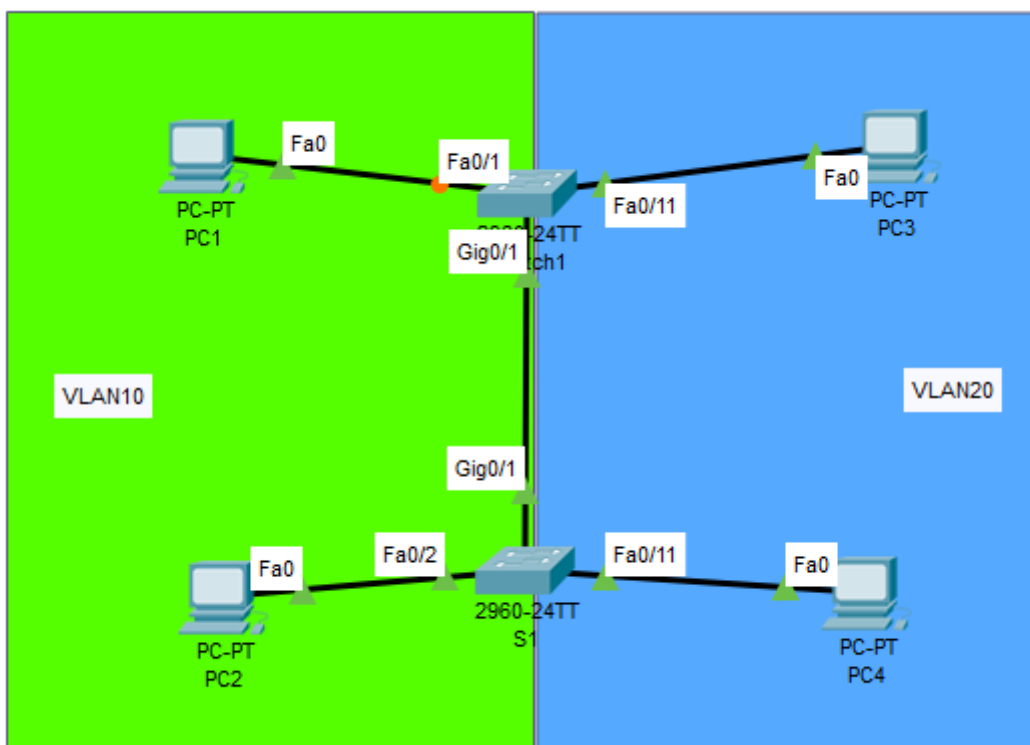
Weryfikacja: show etherchannel port-channel

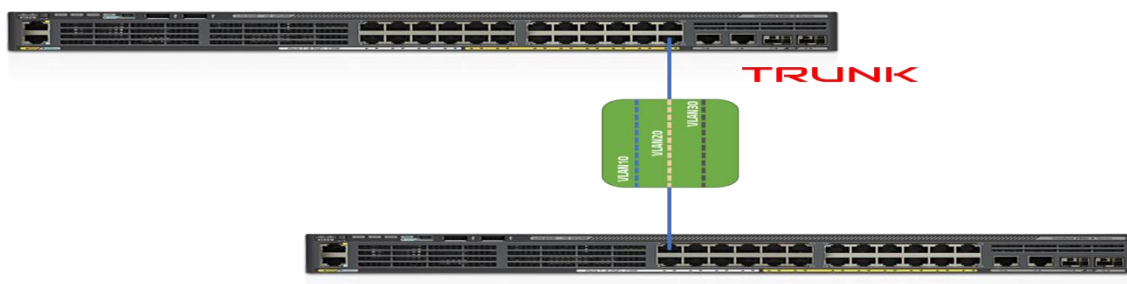
VLANy

Tworzenie wirtualnych sieci, oprócz separacji portów (urządzeń), pozwala logicznie łączyć urządzenia w sieci, bez względu na ich fizyczne położenie oraz tworzyć domenę rozgłoszeniową. Na poniższym schemacie mamy 3 domeny rozgłoszeniowe (wydział, student, gość):



Oczywistym jest, że komputery uczniów czy nauczycieli nie muszą znajdować się w tym samym pomieszczeniu. Pracownie komputerowe uczniów znajdują się również często na różnych kondygnacjach, tak samo jak komputery nauczycieli. Za pomocą technologii VLAN możemy bez ingerencji w fizyczną sieć, spowodować, że będą one pracowały w ramach logicznych sieci, bez zmiany ich fizycznego położenia. I tutaj uwaga, jeśli przełącznik nie wspiera w pełni technologii VLAN ze standardem 802.1Q, a obsługuje tylko Port Based, to takiej konfiguracji nie uda się przeprowadzić. Będzie ona możliwa tylko na urządzeniach, które w pełni obsługują standard 802.1Q czyli standard opisujący działanie sieci VLAN oraz tak zwane ramkowanie (ang. tagging). Weźmy dla przykładu taką topologię:





U innych producentów możemy nie spotkać pojęcia TRUNK, a VLAN tagowany. Tak czy inaczej oba oznaczają to samo, a chodzi w nich o oznaczanie (tagowywanie) ramek, które jako oznaczone transportowane są łączem pomiędzy przełącznikami. Ramka poniżej, to zwyczajna ramka Ethernetowa:

Preambuła	Znacznik początku ramki	Adres MAC docelowy (odbiorcy)	Adres MAC źródłowy (nadawcy)	Długość/Typ	Dane i wypełnienie	Kod kontrolny ramki (FCS)
-----------	-------------------------	-------------------------------	------------------------------	-------------	--------------------	---------------------------

W takiej ramce nie ma wzmianki o sieciach VLAN i taka ramka przekazywana jest do komputera z przełącznika (ang. untag vlan). Ramki transportowane pomiędzy przełącznikami, na których zaimplementowano sieci VLAN są odpowiednio oznaczone (otagowane) i wyglądają tak:

Preambuła	Znacznik początku ramki	Adres MAC docelowy (odbiorcy)	Adres MAC źródłowy (nadawcy)	TPID	TCI	Długość/Typ	Dane i wypełnienie	Kod kontrolny ramki (FCS)
-----------	-------------------------	-------------------------------	------------------------------	------	-----	-------------	--------------------	---------------------------

Widać w takiej ramce dwa dodatkowe pola umieszczone pomiędzy sekcją źródłowy adres MAC, a polem określającym długość ramki. Te dwa dodatkowe pola są właśnie wspomnianym tagiem, czyli informacją że ramka została poprzez przełącznik zmodyfikowana i odpowiednio oznaczona. Pole TPID zawsze zawiera tę samą wartość 0x8100. Jest to informacja że ramka została otagowana zgodnie ze standardem opisującym działanie sieci VLAN czyli wspomnianym już 802.1Q.

To drugie pole, pole TCI zawiera przede wszystkim identyfikator sieci VLAN, ten numer który nadaje się podczas tworzenia sieci, a także znacznik priorytetu oraz oznaczenie rodzaju standardu sieci LAN, najczęściej jest to 0 oznaczające sieć ETHERNET. Taka właśnie ramka transportowana jest pomiędzy przełącznikami, kiedy porty je łączące pracują w trybie TRUNK lub TAG VLAN.

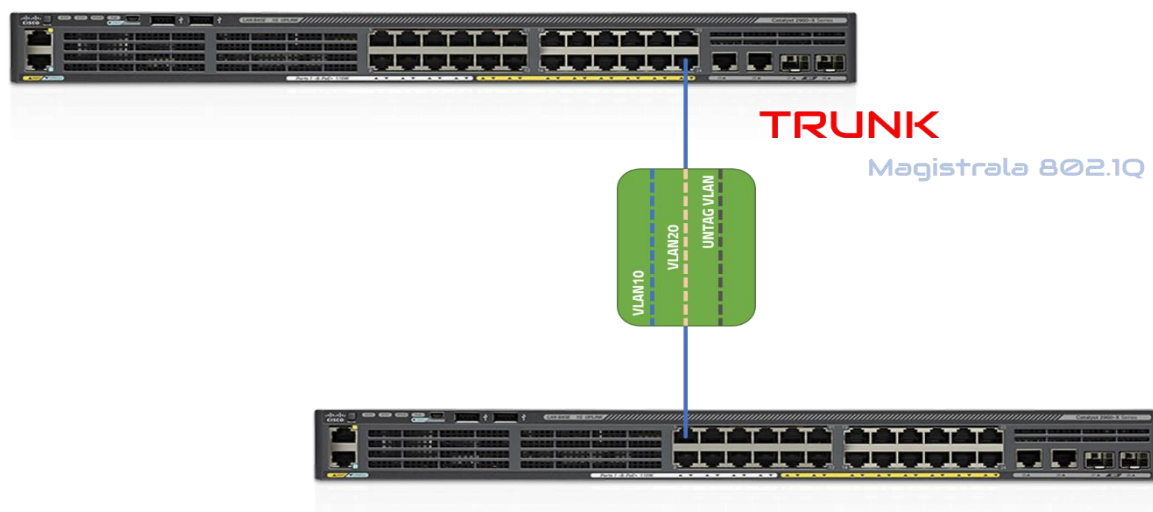
Wracamy do konfiguracji przełącznika. W trybie uprzywilejowanym, na pierwszym urządzeniu, wydajemy następujące polecenia:

- Switch(config)# interface gigabitEthernet 0/1
- Switch(config-if)# switchport mode trunk
- Switch(config-if)# switchport trunk allowed vlan 10, 20

Pierwsze polecenie to przejście do trybu konfiguracji portu, na którym przełącznik na parterze spięty jest z tym na 1 piętrze. Dalej mamy polecenie uruchamiające tryb TRUNK, no i na koniec polecenie, które pozwala transportować ramki VLANów o numerze 10 i 20.

Dokładnie te same czynności należy wykonać na drugim urządzeniu!!!

VLAN natywny (ang. native VLAN), zwany czasem VLANem pierwotnym jest to rodzaj sieci wirtualnej, która obsługuje tak zwany ruch nieoznakowany, czyli przesyła ramki, które nie mają identyfikatora VLAN. Łącza trunkowe, czasami nazywane **magistralami 802.1Q**, potrafią obsługiwać ruch pochodzący właśnie z różnych sieci VLAN, ruch oznakowany, otagowany, ale również ruch z poza sieci VLAN.



Jeśli do łącza trunk trafi taka nieoznakowana ramka to zostaje przekazana właśnie do pierwotnej, czyli natywnej sieci VLAN. Ten Native VLAN został zdefiniowany w standardzie 802.1Q po to, aby zapewnić kompatybilność wsteczną w sieciach, gdzie czasem stosuje się jeszcze koncentratory, ale może być czasem wykorzystywany do transportu danych sterujących różnych protokołów sieciowych. Domyślnym natywnym VLANem w przełącznikach CISCO jest VLAN 1, ten do którego należą wszystkie porty przełącznika przed implementacją sieci wirtualnych.

Dobłą praktyką związaną z bezpieczeństwem sieci jest przeniesienie natywnego VLANu do innej sieci niż domyślna, najlepiej do takiej, która odseparowana jest od innych sieci VLAN, oczywiście tylko wtedy kiedy ten natywny vlan nie przenosi jakiegoś faktycznego ruchu, który w sieci jest pożądanym. W większości opracowań dotyczących bezpieczeństwa sieci CISCO znajdziemy informacje, że jako VLAN natywny ustawić powinniśmy VLAN o numerze 99, ale to tak naprawdę nie ma znaczenia jaki numer zostanie wybrany. Aby zmienić ustawienie dotyczące natywnej sieci VLAN, należy w trybie konfiguracji portu, który jest TRUNKiem (w przypadku naszej sieci to port GigabitEthernet 0/1) wydać następujące polecenie:

- Switch(config-if)# switchport trunk native vlan 99

Wykonanie tego polecenia spowoduje, że ruch nieoznakowany trafiać będzie do sieci VLAN o numerze 99. Warto zaznaczyć, że tej sieci nie znajdziecie w pliku VLAN.DAT, gdyż tak naprawdę nie została ona stworzona. Takie polecenie kieruje tylko ruch nieoznakowany, ale nie

tworzy nam sieci VLAN o numerze 99. Jeśli w realnej sieci VLAN natywny będzie potrzebny, no to zanim wykonane zostanie takie polecenie, to należy utworzyć ręcznie sieć o odpowiednim identyfikatorze. Pamiętać należy o tym, że taką modyfikację, czyli zmianę natywnej sieci VLAN na inną niż domyślna, wykonać należy na wszystkich przełącznikach w sieci. Aby sprawdzić czy VLAN natywny został zmieniony, należy wykonać polecenie, w trybie uprzywilejowanym show interface trunk:

```
Switch>en
Switch#show interface trunk
Port      Mode          Encapsulation  Status        Native vlan
Gig0/1    on            802.1q         trunking      99

Port      Vlans allowed on trunk
Gig0/1    10,20

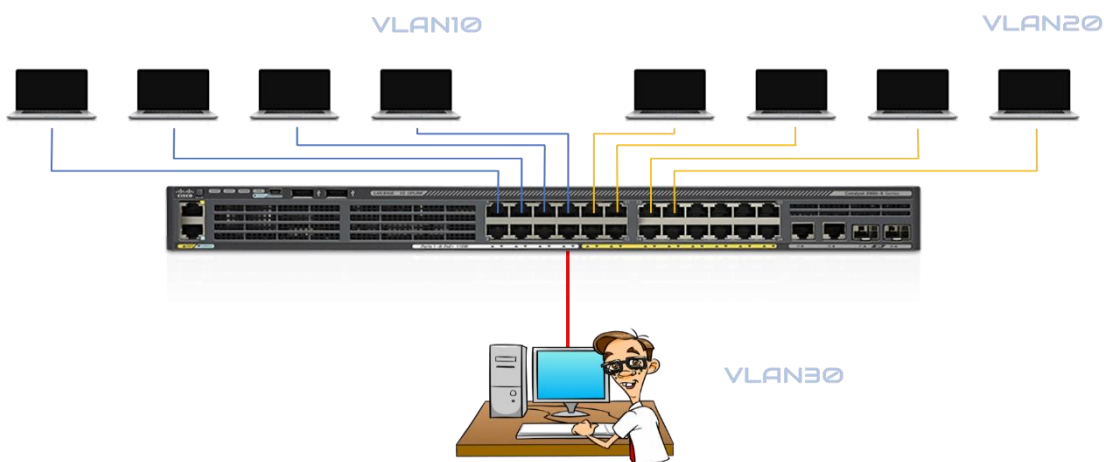
Port      Vlans allowed and active in management domain
Gig0/1    10,20

Port      Vlans in spanning tree forwarding state and not pruned
Gig0/1    10,20

Switch#
```

VLAN zarządzający (ang. management VLAN), to rodzaj sieci wirtualnej, która utworzona jest na przełącznikach sieciowych po to aby odseparować ruch, tak zwany zarządzający (ang. management traffic), od faktycznego ruchu sieciowego, który generują komputery użytkowników. W pierwszym odcinku pokazałem jak konfigurować urządzenia za pomocą fizycznego połączenia z wykorzystaniem kabla konsolowego. To oczywiście jest dobra, skuteczna i zarazem bezpieczna metoda konfiguracji urządzeń sieciowych, ale oczywiście nie jedyna.

Urządzenia sieciowe można również konfigurować za pomocą protokołów zdalnego dostępu takich jak Telnet czy też SSH. Jeśli chcemy konfigurować nasze urządzenia z poziomu własnego protokołu zdalnego dostępu no to jasne jest, że komputer administratora musi być podłączony do jednego z portów takiego przełącznika. W takiej sytuacji dobrą praktyką jest utworzenie osobnego VLANu, do którego podłączone są tylko urządzenia administratorów.



Ostatnim typem "specjalnych" rodzajów sieci VLAN jest VLAN typu czarna dziura (ang. black hole VLAN). Biorąc pod uwagę fakt, że w sieciach komputerowych jako cel nadrzędny

powinniśmy obierać siebie bezpieczeństwo, coś musimy teraz zrobić z naszymi nieużywanymi portami. Te nieaktywne, nieużywane porty możemy dodać do jakiegoś fałszywego VLANu, w którym nie pracują żadne maszyny. Dzięki temu nawet jeśli jakiś intruz się do niego dostał, nie będzie mógł za wiele namieszać.

Sieci VLAN mogą być oznaczane identyfikatorami z zakresu normalnego od 1 do 1005 lub rozszerzonego od 1006 do 4094. Identyfikatory od 1002 do 1005 są zarezerwowane dla sieci Token Ring i FDDI. Sieci VLAN1 i te od 1002-1005 są tworzone automatycznie i nie mogą być skasowane.

Tworzenie VLANów: np. vlan 10, name vlan10, interface range fa0/1-8, switchport mode access (by porty działały w trybie dostępowym), switchport access vlan10 (przydzielamy porty do VLAN), exit.

Sprawdzanie VLANów: show vlan lub show vlan brief.

Tworzenie trunków (switch-switch): np. interface fa0/1-24, switchport mode trunk, switchport trunk allowed vlan add 10 (dodajemy VLAN10 do obsługiwanych sieci), end -> show interfaces trunk.

Konfiguracja VLAN – TPLINK

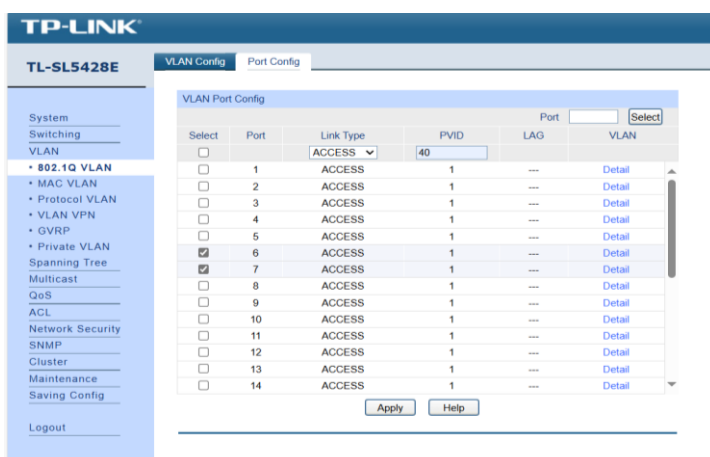
Choose the menu **VLAN** → **802.1Q VLAN** → **VLAN Config** to load the following page.

Select	VLAN ID	Name	Members	Operation
<input type="checkbox"/>	1	Default VLAN	1-24	Edit Detail
<input type="checkbox"/>	2	...		Edit Detail

Total VLAN: 2

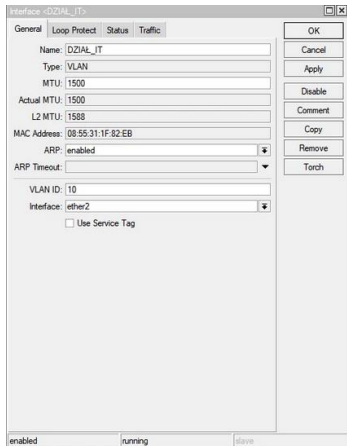
Figure 6-3 VLAN Table

Po utworzeniu VLAN-u (tutaj VLAN40) musimy przypisać go do portu wchodząc w zakładkę Port Config i klikamy apply:

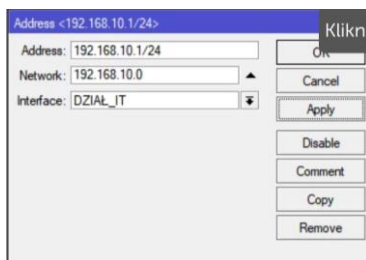


W tych samych zakładkach tworzymy TRUNK (switch<->switch) zmieniając Link Type.

Tworzenie VLAN w Mikrotik o nazwie DZIAŁ_IT w ether2:



Przypisanie interfejsów do VLAN:



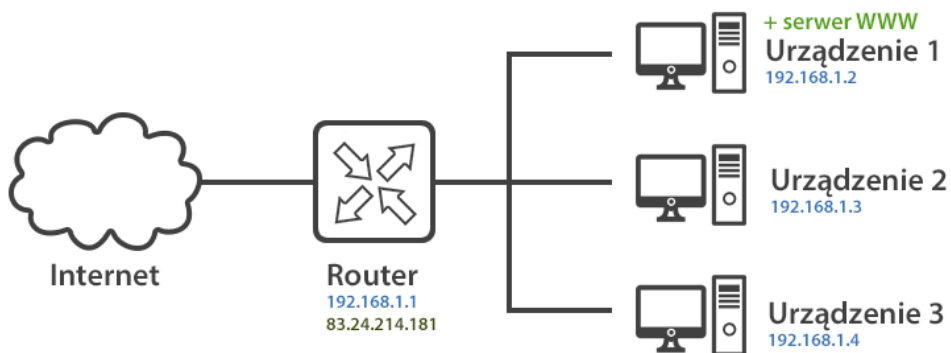
Czym jest Przekierowanie portu?

Przekierowanie portów to technika konieczna do dostępu do serwerów bądź usług znajdujących się w sieciach wewnętrznych normalnie niedostępnych „od strony” Internetu.

Różne usługi wykorzystują różne porty: przeglądarka internetowa domyślnie łączy się z serwerem WWW na porcie o numerze 80, połączenia z MySQL używa portu 3306, a protokół do synchronizacji czasu – 123. Załóżmy, że w sieci wewnętrznej jest kilka urządzeń (niezależnie czy jest to tablet, telefon, komputer czy laptop) i na jednym z nich, o adresie 192.168.1.2 jest zainstalowany serwer WWW który nasłuchuje na porcie 80.

Przyjmijmy też, że router ma w sieci wewnętrznej adres IP: 192.168.1.1, zaś na zewnątrz jego adres to 83.24.214.181. Ten ostatni został przyznany przez usługodawcę Internetu – w tym wypadku jest to Neostroda od Orange. Czym jest router? To po prostu pośrednik między siecią wewnętrzną a Internetem (który logicznie jest taką samą siecią jak ta wewnętrzna, tylko o dużo większej skali). Sytuację logiczną prezentuje poniższy obrazek. W aktualnej konfiguracji wspomniany serwer WWW będzie dostępny z każdego urządzenia w sieci. Po wpisaniu adresu 192.168.1.2 w przeglądarce na dowolnym z urządzeń zostanie wyświetlona strona umieszczona na serwerze.

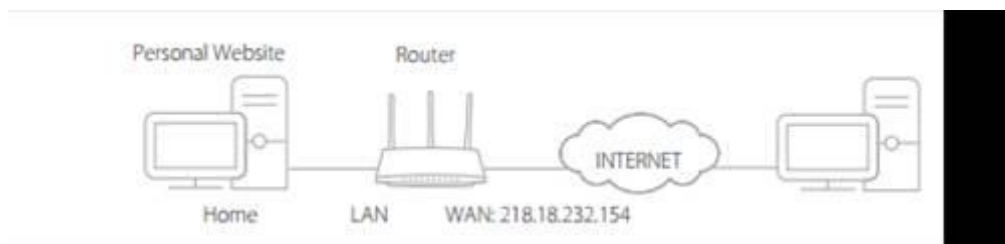
Co jednak gdyby ktoś chciał pochwalić się stroną w internecie? U innych użytkowników podanie adresu serwera w sieci wewnętrznej (czyli 192.168.1.2) nie zadziała, podobnie jak wpisanie 83.24.214.181. Choć jest to dobrym tropem, to router (który pośredniczy między internetem a siecią wewnętrzną) nie wie do którego z urządzeń przekierować komunikację.



Przypadek 1: Dla TL-WR840N, TL-WR940N, Archer C20, Archer C50, itp.

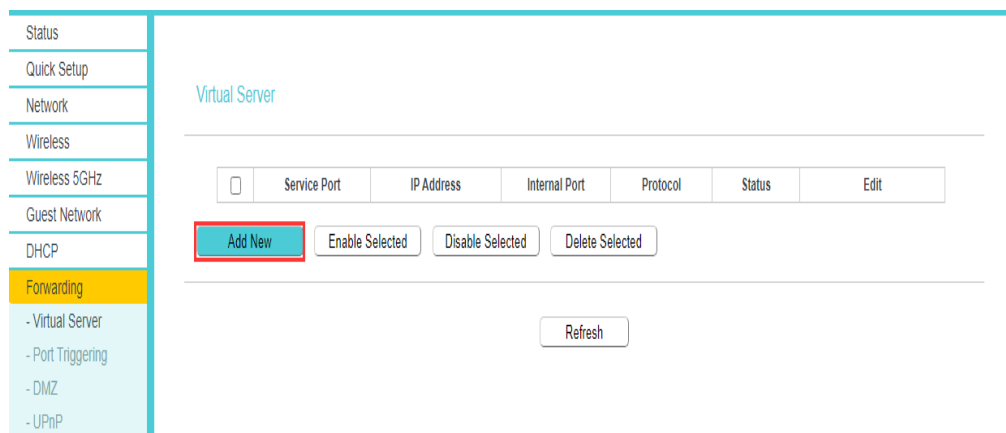
Przykład: Udostępnianie własnej strony internetowej stworzonej w sieci LAN, aby znajomi mieli do niej dostęp przez Internet.

Strona internetowa jest stworzona na komputerze z adresem IP 192.168.0.106, działa na porcie 90, a komputer podłączony jest do routera z adresem WAN 218.18.232.154.



Krok 1. Zaloguj się na stronę konfiguracyjną routera:

Krok 2. Otwórz zakładkę Forwarding->Virtual Servers / Przekierowanie->Serwery wirtualne w menu po lewej stronie i kliknij przycisk Add New / Dodaj.



Krok 3. W sekcji usługi wpisz dokładne informacje. Przykładowo, jeśli chcesz przekierować port 90 dla urządzenia z adresem 192.168.0.106, wprowadź poniższe dane:

Status
Quick Setup
Network
Wireless
Wireless 5GHz
Guest Network
DHCP
Forwarding
- Virtual Server
- Port Triggering
- DMZ
- UPnP
Security

Virtual Server

Service Port:	90	(XX-XX or XX)
IP Address:	192.168.0.106	
Internal Port:	90	(XX or keep empty. If it's empty, Internal port equals to Service port)
Protocol:	ALL	
Status:	Enabled	
Common Service Port:	---Please Select---	

Service Port / Port usługi: Wybierz usługę z listy Typ usługi / Common Service Port. Jeśli na tej liście nie ma usługi którą chcesz dodać, możesz jej nie wybierać, tylko wpisać port ręcznie.

Service Port / Port usługi i Internal Port / Port wewnętrzny: Jeśli wybierzesz Typ usługi z listy, wtedy, Port usługi i Port wewnętrzny zostaną wpisane automatycznie. W przeciwnym razie wpisz Port usługi i Port wewnętrzny ręcznie. Upewnij się, że wprowadzasz poprawne numery portów.

Jeśli chcesz wprowadzić zakres portów (xx-xx), wpisz je w Porcie usługi i Port wewnętrzny pozostaw pusty. Portu usługi i Portu wewnętrznego zazwyczaj używa się tego samego.

Adres IP: Określ adres IP urządzenia dla którego otwierasz port.

Protokół: Wybierz protokół z którego korzysta aplikacja. Jeśli nie jesteś pewny/a, wybierz ALL/Wszystkie.

Status: Wybierz opcję Enabled/Włączony.

Krok 4 Kliknij przycisk Save/Zapisz, aby zachować ustawienia.

Uwaga: Aby zapewnić ciągłe działanie Przekierowania portu, zalecamy przypisać statyczny adres IP do Twojego urządzenia, ponieważ jego adres IP może zostać zmieniony poprzez funkcję serwera DHCP.

Krok 5 Przejdź do zakładki Status i sprawdź Adres IP WAN swojego routera. W tym momencie możesz sprawdzić przekierowanie portu wpisując adres http:// WAN IP: numer portu (w tym przypadku: http:// 218.18.232.154:90), aby odwiedzić swoją stronę.

Status
Quick Setup
Operation Mode
Network
Dual Band Selection
Wireless 2.4GHz
Wireless 5GHz
Guest Network
DHCP
Forwarding
Security
Parental Controls
Access Control
Advanced Routing
Bandwidth Control
IP & MAC Binding
Dynamic DNS
IPv6
System Tools
Logout

Wireless 5GHz

Operation Mode:	Router
Wireless Radio:	Enabled
Name(SSID):	TP-Link_0909_5G
Mode:	11a/n/ac mixed
Channel:	Auto(Channel 36)
Channel Width:	Auto
MAC Address:	00:0A:EB:13:09:68

WAN

MAC Address:	30 B5 C2 E8 A0 91
IP Address:	218.18.232.154 (PPPoE)
Subnet Mask:	255.255.255.255
Default Gateway:	218.18.232.154
DNS Server:	192.168.137.124 172.31.1.1
Online Time:	0 day(s) 00:00:00

Jeśli Adres IP WAN routera nie jest publiczny, tylko prywatny, oznacza to, że przed Twoim routerem TP-Link znajduje się inny router, na którym również trzeba przekierować port.

A) Jeśli chcesz otworzyć port 80 dla lokalnego urządzenia, zmień port zarządzania zdalnego routera, ponieważ jego domyślny port to 80. Port wewnętrzny to również 80, ale nie można go zmienić, pomimo zmiany portu zdalnego. Port lokalnego zarządzania routerem nie wpływa na przekierowanie portu.

Przejdź do Security->Remote Management / Bezpieczeństwo->Zarządzanie zdalne i zmień Web Management Port / Port zarządzania WEB na inny, na przykład 8080 i kliknij Save/Zapisz.

The screenshot shows the 'Remote Management' configuration page. On the left sidebar, 'Security' is selected, and 'Remote Management' is highlighted. The main configuration area has the following fields:

- Web Management Port: 8080
- Remote Management IP Address: 255.255.255.255 (Enter 255.255.255.255 for all)

A 'Save' button is located at the bottom center of the configuration area.

B) Niektóre modele routerów umożliwiają ustawienie różnych Portów usługi i Portów wewnętrznych. Przykładowo, jeśli chcesz otworzyć port 90 tylko dla jednego urządzenia z adresem 192.168.0.106, wystarczy że wykonasz konfigurację jak powyżej. W przypadku, jeżeli masz dwa lub więcej urządzeń (w tym przypadku 192.168.0.106 i 192.168.0.103) działające na tym samym porcie, wtedy możesz użyć innych Portów usługi. W Porcie wewnętrznym wpisz faktyczny port (w tym przypadku 90) oraz inny w Porcie usługi (przykładowo 9000 i 9001).

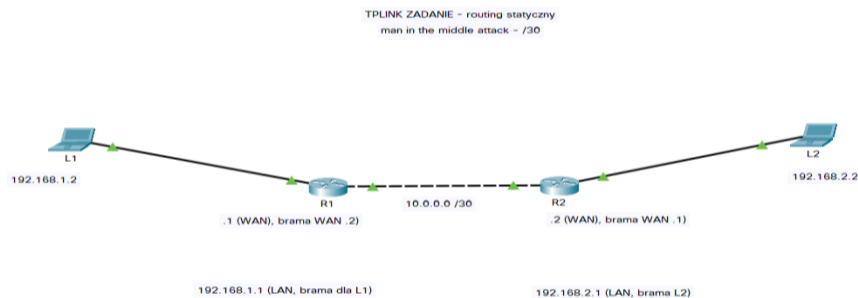
The screenshot shows the 'Virtual Server' configuration page. On the left sidebar, 'Forwarding' is selected, and 'Virtual Server' is highlighted. The main configuration area has the following fields:

- Service Port: 9000 (XXX-XX or XX)
- IP Address: 192.168.0.106
- Internal Port: 90 (XX or keep empty. If it's empty, Internal port equals to Service port)
- Protocol: ALL
- Status: Enabled
- Common Service Port: ---Please Select---

'Save' and 'Back' buttons are located at the bottom center of the configuration area.

Część 3 - laboratoria

Zadanie 1 - routing statyczny w TPLINK:



Na podstawie powyższej topologii skonfiguruj 3 sieci tak, by była komunikacja pomiędzy urządzeniami końcowymi, stosując routing statyczny. Na Laptopie 1 i laptopie 2 ustaw adresację tak by były w oddzielnych sieciach, ale się komunikowały. Routery są dla siebie nawzajem bramami WAN. Maskę /30 jest po to by tylko 2 hosty mogły być wpięte do sieci więc zapobiegamy atakom „man in the middle”.

Skonfiguruj sieci LAN.

TPLINK: W zakładce „network”-> WAN2 wpisz adres WAN routera 1 i routera 2 i maskę.

Wepnij kabel cross to 1 portu WAN routera 1 i routera 2.

W zakładce „transmission” -> „routing” wpisz nazwę sieci i ustaw na dwóch routerach „Net”.

W zakładce „transmission” -> „routing” wpisz w R1, destination IP: 192.168.2.0, maskę i next hop czyli adres WAN 2 routera, wybierz interfejs WAN2.

W zakładce „transmission” -> „routing” wpisz w R2, destination IP: 192.168.1.0, maskę i next hop czyli adres WAN 1 routera, wybierz interfejs WAN2.

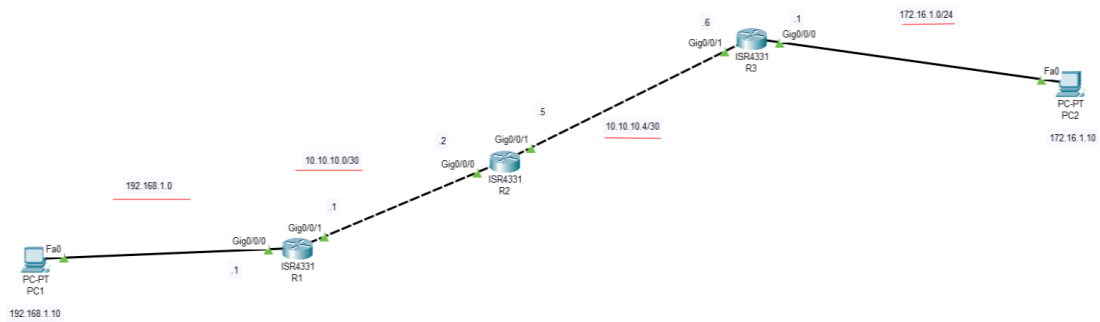
Spinguj urządzenia końcowe.

Mikrotik: ip addresses:

LAN1: 192.168.1.1/24 eth 2, 10.0.0.1/24 eth3, ip routes: wpisać 0.0.0.0/0, gateway: 10.0.0.2,

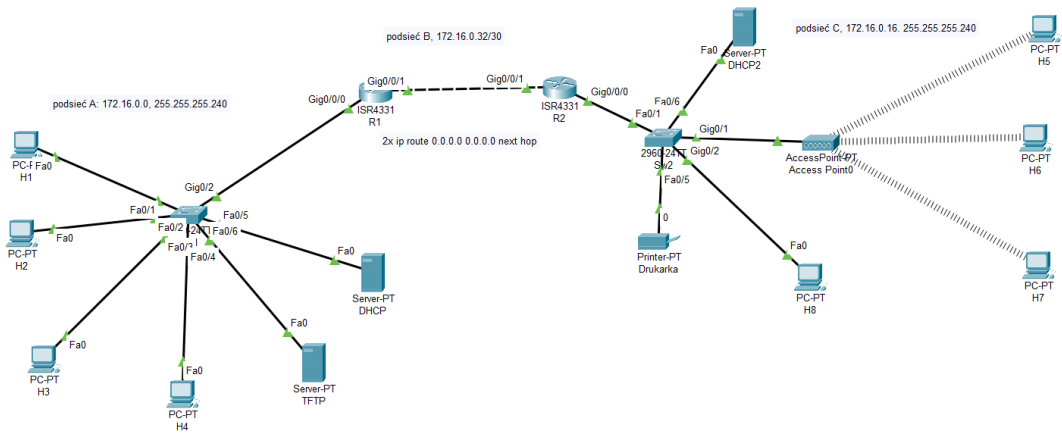
LAN2: 192.168.2.1/24 eth2, 10.0.0.2/24 eth3, ip routes 0.0.0.0/0, gateway 10.0.0.1.

Zadanie 2 – routing statyczny na 3 routerach



Zadanie 3 – trasa domyślna, DHCP

Podziel sieć 172.16.0.0 na 3 podsieci.



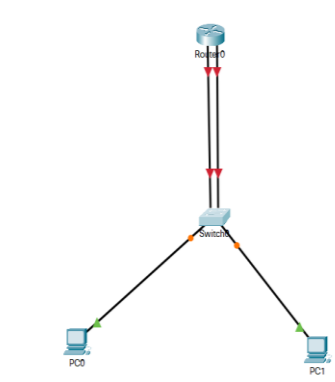
02:56:01

Cooper Straight-Through

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	H8	H2	ICMP	Yellow	0.000	N	0	(edit)	
●	Successful	Druka...	H5	ICMP	Green	0.000	N	1	(edit)	
●	Successful	H1	H5	ICMP	Blue	0.000	N	2	(edit)	

Toggle PDU List Window

Zadanie 4 - routing między VLANami:

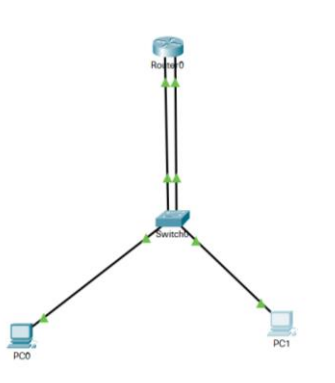


```

Switch0
-----
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/20, changed
state to up
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/13, changed
state to up

Switch>
Switch#enable
Switch#conf ter
Switch#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name uczniowie
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name nauczyciele
Switch(config-vlan)#exit
Switch(config-if-range)#interface range fa0/1-13
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range fa0/13-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
Switch(config)#
Switch(config)#
    
```



```

Router0
-----
IOS Command Line Interface

Router#enable
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface g0/0/0
Router(config-if)#ip address 192.168.10.0.1 255.255.255.0
% Invalid input detected at '' marker.

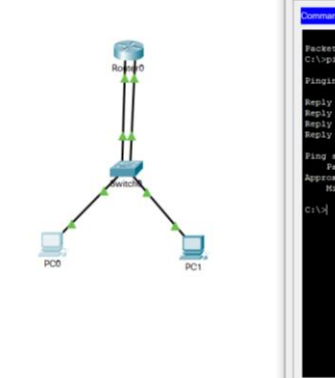
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed
state to up

Router(config-if)#exit
Router(config)#interface g0/0/1
Router(config-if)#ip address 192.168.30.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed
state to up

Router(config-if)#
    
```



```

PC0
-----
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.101

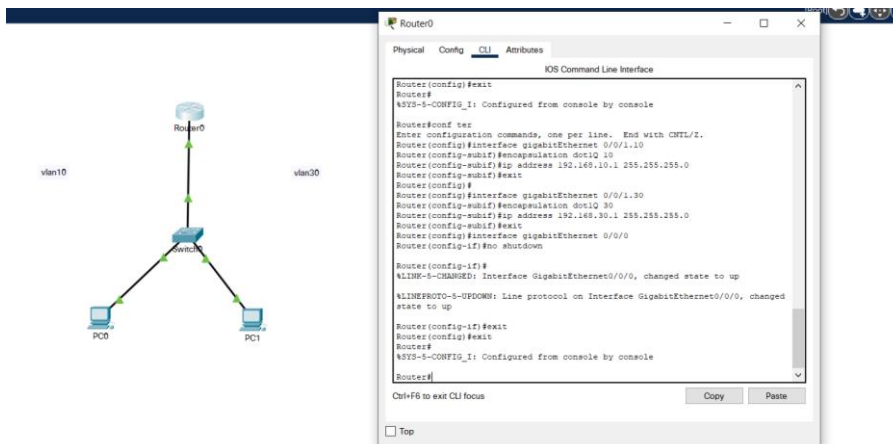
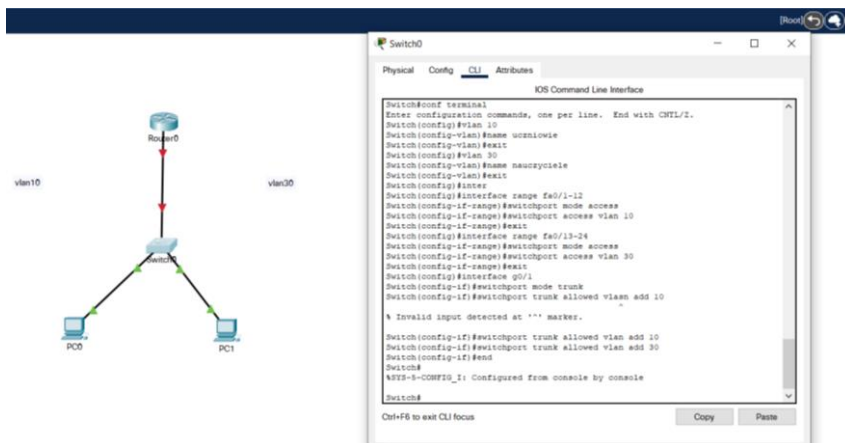
Pinging 192.168.30.101 with 32 bytes of data:

Reply from 192.168.30.101: bytes=32 time=1ms TTL=127
Reply from 192.168.30.101: bytes=32 time=1ms TTL=127
Reply from 192.168.30.101: bytes=32 time=1ms TTL=127
Reply from 192.168.30.101: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.30.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
    
```

Zadanie 5 - routing pomiędzy VLANami przy wykorzystaniu TRUNKa.

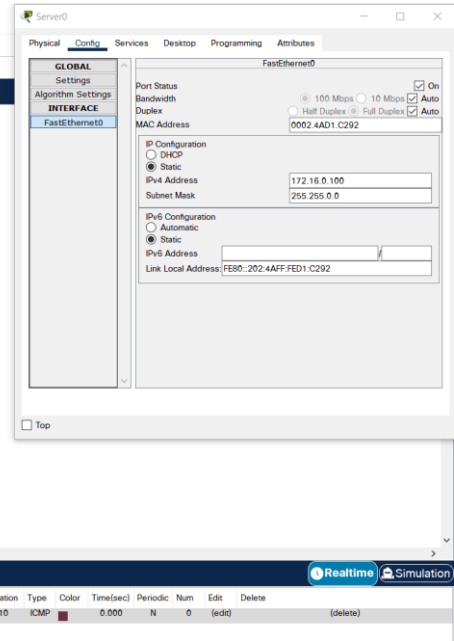
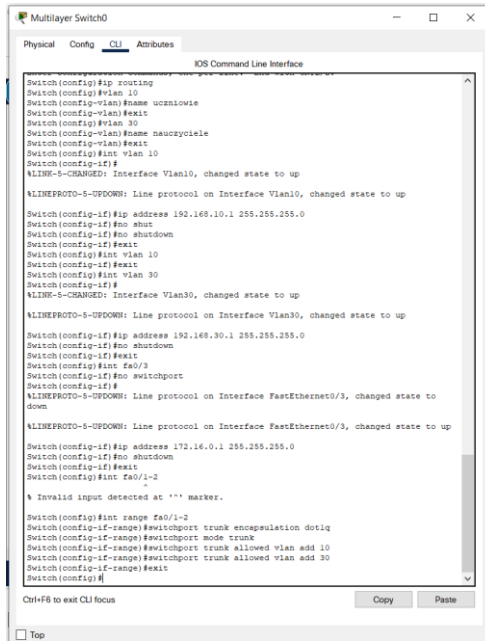
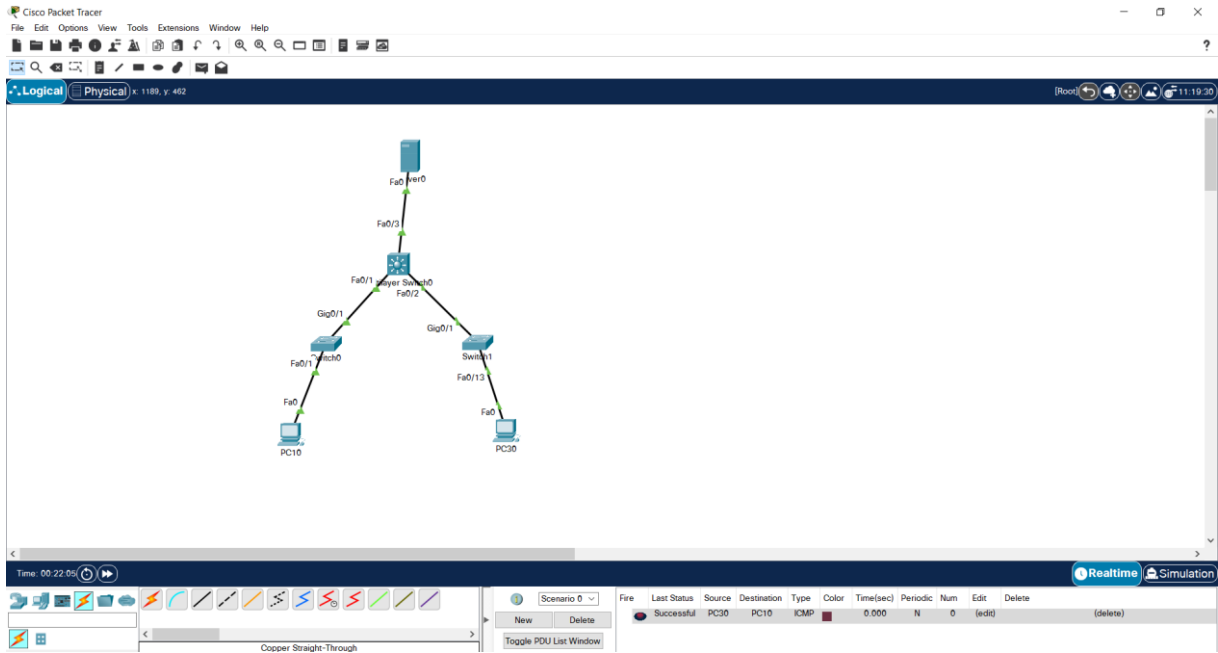


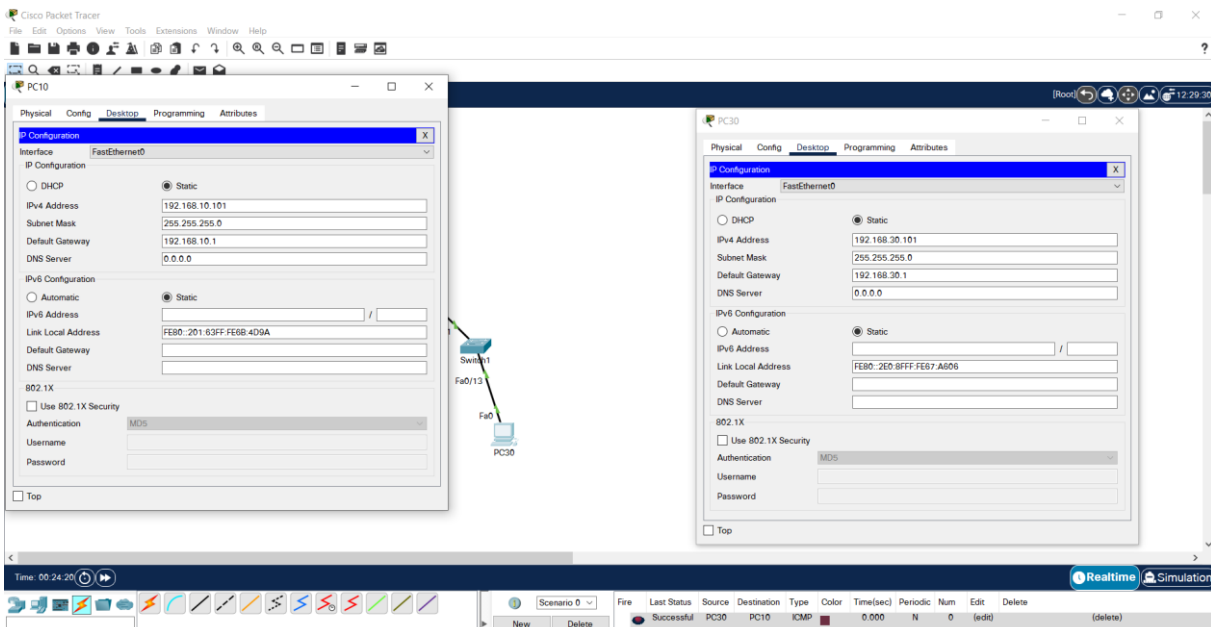
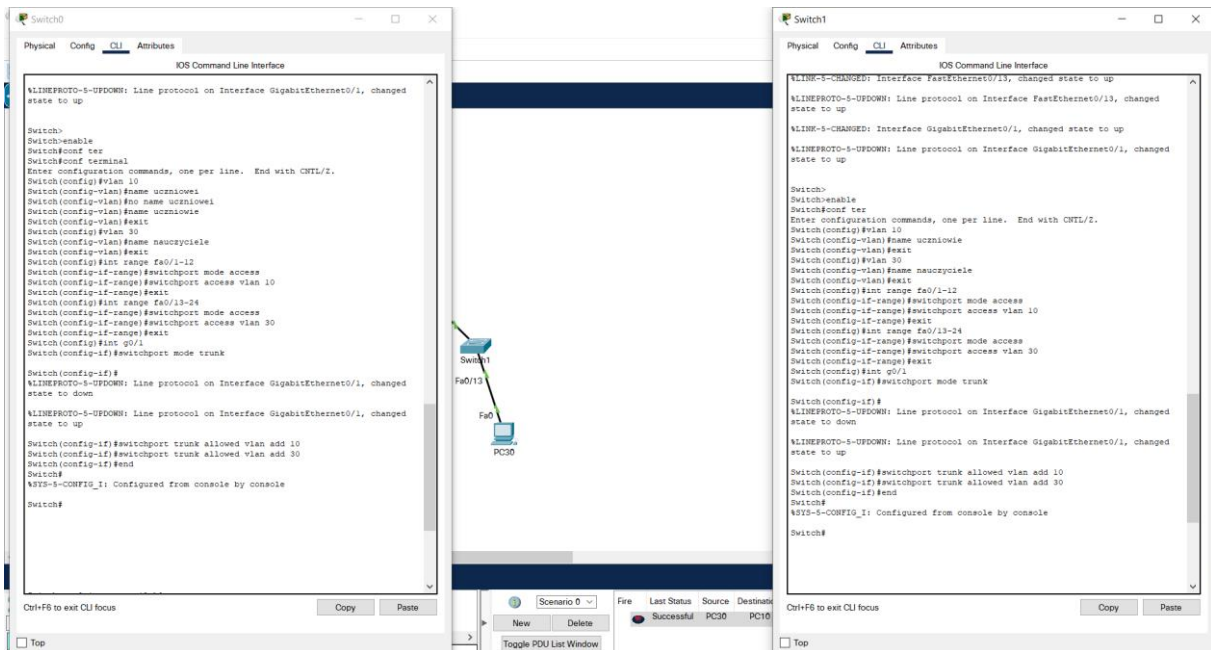
Zadanie 6 - routing między sieciami vlan ze switchem na 3 warstwie

Adres bramy domyślnej serwera 172.16.0.1.

Komenda „ip routing” na switchu 3 warstwy włącza routing.

Komenda „no switchport” przełącza port switcha do pracy w warstwie 3.





Zadanie 7 - routing pomiędzy VLANami w Mikrotik:

Z lewego panelu w routerze wybrać quick set-> apply i ok. Skonfigurować sieci VLAN i przypisać je do portu 5. Wybrać interfaces -> VLAN, +, apply i ok. Potem przypisać adresy IP i apply i ok.

Zadanie 8 - TP-Link T2500G-10TS (TL-SG3210 v3), konfiguracja VLANów nieoznakowanych:

1. Podłącz kabel Ethernet w dowolny port przełącznika i do PC
2. Ustaw kartę sieciową komputera statycznie:
IP: 192.168.0.2, Maska: 255.255.255.0, Brama: 192.168.0.1
3. Wpisz w przeglądarce adres przełącznika: 192.168.0.1,
4. Zaloguj się używając loginu i hasła z naklejki (admin/admin),

5. Utwórz nowe hasło admin1.
6. W L2 features: utwórz nietagowany VLAN 10 o ID VLANu 10 na portach 7,8 (nie wpinaj tam na razie kabla),
7. Usuń porty 7,8 z VLANu 1,
8. Ustaw PVID na portach 7,8 na VLAN 10 (port config)
9. Wejdź w zakładkę L3 Features interface → dodaj statycznie VLAN 10 o IP: 192.168.1.1 oraz maskę oraz ustaw na nim zarządzanie (możliwe, że przełącznik rozłączy się w tym momencie, bo jesteś w VLANie 1.
10. Skonfiguruj swoją kartę sieciową 2 komputera statycznie:
IP: 192.168.1.2, Maska: 255.255.255.0 Brama: 192.168.1.1
11. Wepnij kabel z komputera 2 do portu 7 lub 8.
12. Spróbuj spingować przełącznik na IP: 192.168.1.1. Jeśli pingi odpowiadają, spróbuj się zalogować do przełącznika. Jeśli chcesz spingować komputery ustaw adresację na 1 z komputerów by była w tej samej sieci.

VLANy 801.Q pomiędzy 2 przełącznikami:

Wszystkie punkty oprócz 6,7,8, 9 i 10 wykonaj tak samo na obu przełącznikach.

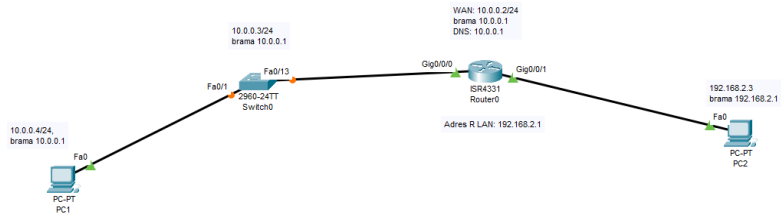
6. Utwórz nietagowany VLAN 10 o ID VLANu 10 na portach 7,8 (nie wpinaj tam na razie kabla), oraz tagowany na porcie 6.
Utwórz nietagowany VLAN 20 o ID VLANu 20 na portach 1,2 (nie wpinaj tam na razie kabla), oraz tagowany na porcie 6.
7. Usuń porty 1,2,7 i 8 z VLANu 1,
8. Ustaw PVID na portach 7,8 na VLAN 10, ustaw PVID na portach 1,2 na VLAN 20,
9. Wejdź w zakładkę L3 features → VLAN i dodaj VLAN 10 o IP: 192.168.1.1 oraz ustaw na nim zarządzanie (możliwe, że przełącznik rozłączy się w tym momencie, bo jesteś w VLANie 1); dodaj VLAN 20 o IP: 192.168.2.1
10. Skonfiguruj swoją kartę sieciową komputera statycznie:
IP: 192.168.2.2, Maska: 255.255.255.0 Brama: 192.168.2.1
11. Wepnij kabel z komputera do portu 1 lub 2.

Intencją tego zadania jest komunikacja między komputerami w VLAN 10 na obu przełącznikach, a także między komputerami wpiętymi w VLAN 20 na obu przełącznikach. Komputery należące do dwóch różnych VLANów nie będą miały ze sobą komunikacji. Ruch pomiędzy przełącznikami odbywa się dzięki przesyłaniu otagowanych ramek przez port 6 obu przełączników.

Zadanie 9 - TP-LINK, router, Switch i 2 hosty

Zaczynając od PC2, skonfiguruj router poprzez LAN (LAN 192.168.2.1, PC 192.168.2.3), wyloguj się z routera, przejdź do PC1 i tam wepnij się do LAN routera i skonfiguruj ustawienia WAN. Ustaw kartę PC1 na adres 10.0.0.4, brama 10.0.0.1 a router to 10.0.0.2.

Potem na switchu ustaw adres IP 10.0.0.3 z bramą 10.0.0.1. PC2 do PC1 powinny się pingować. Jeśli nie, to wyłącz zaporę na w Windows oraz Routerze.



Jeśli ping nie działa można na R kliknąć w:
 a) security -> advanced security -> zaznaczyć "ignore ping packet..."
 b) system tools -> administration -> ip address 255.255.255.255

Sprzęt:
 Router TP-LINK WR940N
 Switch TP-LINK SG3210

Zadanie 10 - TP-LINK trunk

