OGÓLNOPOLSKA
SIEĆ EDUKACYJNA

KONFIGURACJA SIECI ORAZ URZĄDZEŃ DO POPRAWNEGO DZIAŁANIA

ose.gov.pl

Tytuł: Konfiguracja sieci oraz urządzeń do poprawnego działania
Autor: Jakub Niewiadomski
Redaktor merytoryczny: Piotr Chojnacki

O autorach:

Jakub Niewiadomski
Uczeń profilu technik informatyk. Pasjonat programowania i sieci komputerowych (ukończony kurs CCNA), a hobbystycznie związany również z fotografią koncertową, gitarą oraz instrumentami klawiszowymi.

Piotr Chojnacki
Nauczyciel przedmiotów zawodowych informatycznych. Wieloletni koordynator projektów informatycznych i współpracy cyfrowej z uczelniami wyższymi i instytucjami. Właściciel firmy szkoleniowej z zakresu IT. Instruktor CISCO CCNA R&S, CCNA Security, CCNP. Egzaminator i szkoleniowiec ECDL. Współrealizator projektów unijnych dotyczących zdobywania kompetencji ICT i TIK.

Ministerstwo Cyfryzacji

Program OSE powstał dzięki staraniom Ministerstwa Cyfryzacji.

NASK

Operatorem OSE jest NASK Państwowy Instytut Badawczy.

Streszczenie

W wykładzie zawarte zostały informacje dotyczące podstaw funkcjonowania sieci komputerowych oraz przykładowa konfiguracja routera.

Omówione zostały rodzaje sieci, media transmisyjne, podstawowe urządzenia sieciowe, usługi działające w sieci (DHCP, DNS), trasowanie, podstawy pracy z zaporą sieciową, technika translacji adresów. Poruszone zostało również zagadnienie QoS. W części praktycznej opisane zostało przystosowanie urządzenia firmy Mikrotik do pracy jako router brzegowy w szkolnej sieci internetowej oraz podstawy obliczania podsieci.

Zeszyt ćwiczeń został przygotowany, by w prosty sposób przyswoić oraz poszerzyć wiedzę z materiału zawartego w wykładzie, a także rozwinąć umiejętności praktyczne związane z sieciami komputerowymi.

Spis treści

Wykład

Wprowadzenie do sieci komputerowych

Czym jest sieć komputerowa?

Siecią komputerową nazywamy zbiór komputerów oraz innych urządzeń połączonych ze sobą poprzez medium transmisyjne w celu wymiany danych.

Czym jest medium transmisyjne?

Jest to nośnik używany do transmisji sygnałów w telekomunikacji i jest podstawowym elementem systemów telekomunikacyjnych. Możliwości transmisji danych zależą od parametrów użytego medium. Najczęściej wykorzystywanym medium jest wieloparowy kabel miedziany (dla sieci lokalnych), zwany potocznie skrętką oraz kabel światłowodowy (dla sieci miejskich i rozległych).

Szczegółowe informacje o „skrętce"

Siecią komputerową nazywamy zbiór komputerów oraz innych urządzeń połączonych ze sobą poprzez medium transmisyjne w celu wymiany danych.

Skrętką nazywamy medium transmisyjne składające się z kilku par przewodów. Są one skręcone ze sobą w celu wyeliminowania zakłóceń. Wyróżniamy kable nieekranowane (UTP – Unshielded Twisted Pair) oraz ekranowane (dawniej STP – Shielded Twisted Pair, obecnie FTP – Foiled Twisted Pair). Skrętkę dzielimy na kategorie, które odnoszą się do zastosowanych rodzajów złączy i pasma przenoszenia w danej kategorii, co bezpośrednio przekłada się na przepustowość kabla danej kategorii.

Opis przewodów według normy powinien wyglądać następująco: xx/yyTP. Oznaczenie xx dotyczy całego przewodu, natomiast yy dotyczy pojedynczych par przewodów. Zastosowane mogą być następujące oznaczenia:

- U – nieekranowane (ang. Unshielded)
- F – ekranowane folią (ang. Foiled)
- S – ekranowane siatką (ang. Shielded)
- SF – ekranowane folią i siatką

Najczęściej spotykanymi konstrukcjami są:

- U/UTP (dawniej UTP) – skrętka nieekranowana.
- F/UTP (dawniej FTP) – skrętka foliowana.
- S/UTP – skrętka nieekranowana dodatkowo w ekranie z siatki.
- SF/UTP (dawniej STP) – skrętka ekranowana folią i siatką.
- U/FTP – skrętka z każdą parą w osobnym ekranie z folii.

- F/FTP – skrętka z każdą parą w osobnym ekranie z folii dodatkowo w ekranie z folii.
- S/FTP (dawniej SFTP) – skrętka z każdą parą foliowaną dodatkowo w ekranie z siatki.
- SF/FTP (dawniej S-STP) – skrętka z każdą parą foliowaną dodatkowo w ekranie z folii i siatki.

Według europejskiej normy EN 50173 wyróżniamy następujące klasy skrętki:

- klasa A (kategoria 1) – realizacja usług telefonicznych z pasmem częstotliwości do 100 kHz;
- klasa B (kategoria 2) – okablowanie dla aplikacji głosowych i usług terminalowych z pasmem częstotliwości do 1 MHz;
- klasa C (kategoria 3) – używana najczęściej w sieciach telefonicznych, wykorzystuje pasmo częstotliwości do 16 MHz;
- klasa D (kategoria 5/5e) – najczęściej stosowana do budowy sieci lokalnych, obejmuje aplikacje wykorzystujące pasmo częstotliwości do 100 MHz;
- klasa E (kategoria 6) – obejmuje okablowanie, którego wymagania pasma są do częstotliwości 250 MHz (przepustowość rzędu 200 Mb/s). Przewiduje ono implementację Gigabit Ethernetu (4x 250 MHz = 1 GHz) i transmisji ATM 622 Mb/s;
- klasa EA (kategoria 6A) – wprowadzona wraz z klasą FA. Obejmuje pasmo do częstotliwości 500 MHz;
- klasa F (kategoria 7) –Możliwa jest realizacja aplikacji wykorzystujących pasmo do 600 MHz. Różni się ona od poprzednich klas stosowaniem kabli typu S/FTP (każda para w ekranie plus ekran obejmujący cztery pary) łączonych ekranowanymi złączami. Dla tej klasy okablowania jest możliwa realizacja systemów transmisji danych z prędkościami przekraczającymi 1 Gb/s;
- klasa FA (kategoria 7A) – obejmuje pasmo do częstotliwości 1000 MHz; umożliwia uzyskanie prędkości do 100 Gbit/s do 15m i 40 Gbit/s do 100m;
- klasa I (kategoria 8.1) - w trakcie rozwoju, wykorzystująca pasmo częstotliwości 1600-2000 MHz; prędkość transmisji > 40 Gbit/s;
- klasa II (kategoria 8.2) - w sprzedaży, wykorzystująca pasmo częstotliwości 1600-2000 MHz.

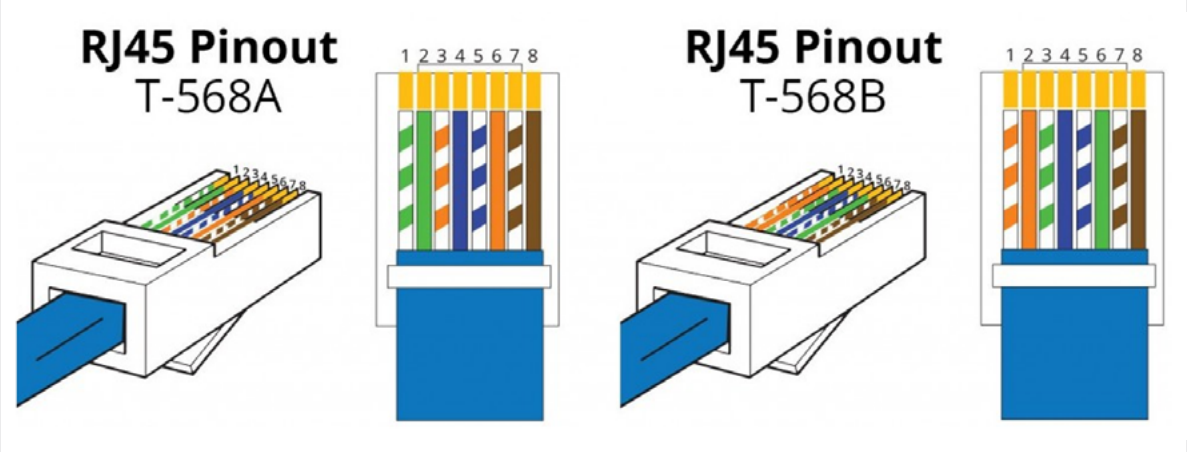
Dodatkowo norma TIA/EIA 568A definiuje:

- Kategoria 4 – dla szybkich sieci lokalnych, obejmuje aplikacje wykorzystujące pasmo częstotliwości do 20 MHz;

Najczęściej wykorzystywaną kategorią skrętki jest 5E.

Standardy zaciskania wtyków RJ45

Istnieją dwa standardy zaciskania wtyków RJ45 - T568A oraz T568B. Aby wykonać przewód prosty, należy na obu jego końcach zacisnąć wtyk według standardu A bądź B (po obu stronach jednakowe). Aby wykonać przewód krosowy należy z jednej strony zacisnąć wtyk według standardu A, natomiast z drugiej według standardu B.



Rodzaje sieci

Wyróżniamy 3 główne rodzaje sieci, a są to:

- LAN, czyli Lokalna Sieć Komputerowa, łącząca urządzenia takie jak komputery, na określonym, stosunkowo małym obszarze. Przykładem takiej sieci może być np. sieć szkolna.

- MAN, czyli Miejska Sieć Komputerowa, łącząca urządzenia takie jak komputery, na obszarach miast lub aglomeracji miejskich. W jej skład wchodzi wiele sieci LAN. Przykładem takiej sieci są sieci ośrodków akademickich, które oprócz łączenia budynków w ramach kampusu łączą również ośrodki poza głównymi zabudowaniami.

- WAN, czyli Rozległa Sieć Komputerowa, łącząca mniejsze segmenty sieciowe w ogromnych rozmiarów sieci o rozpiętości kraju czy kontynentu. Sieć ta pozwala także na komunikację rozsianych na dużych obszarach sieci LAN i MAN ze sobą. Połączenie między dwoma odległymi od siebie miejscami opiera się na łączach szkieletowych sieci rozległych, które w Polsce zapewnia m.in. NASK - Naukowa i Akademicka Sieć Komputerowa.

Urządzenia wykorzystywane przy budowie sieci

Przy tworzeniu sieci wykorzystujemy wiele urządzeń, dzięki którym jesteśmy w stanie uzyskać różnorakie opcje konfiguracyjne, łączące fragmenty sieci ze sobą. Wyróżniamy 2 podstawowe urządzenia sieciowe:

- Router, którego zadaniem jest łączyć ze sobą różne sieci na poziomie warstwy 3 (lub sieciowej). Jest on swego rodzaju pośrednikiem pomiędzy np. dwoma sieciami LAN, czy też siecią LAN i WAN (tudzież Internet)
- Przełącznik łączy segmenty w jednej sieci na poziomie warstwy 2, do każdego jego portu można podłączyć jedno urządzenie końcowe. Przełącznik umożliwia segmentację sieci na domeny rozgłoszeniowe, co przyczynia się do redukcji kolizji.

Jak łączyć urządzenia w sieci?

Połączenia między urządzeniami wykonywane są według zasady, która głosi iż przewód krosowy wykorzystujemy przy łączeniu urządzeń tego samego typu, czyli na przykład router-router, komputer-komputer. W obecnych czasach stosowany jest on jednak wyłącznie do połączenia komputer-komputer, gdyż w większości urządzeń sieciowych wbudowana jest funkcja automatycznego krosowania (Auto MDI-MDIX).

Od czego zacząć budowę sieci?

Pierwszym etapem tworzenia sieci jest wykonanie jej projektu, zarówno w warstwie fizycznej, jak i w warstwie sieci.

Przy projektowaniu każdej sieci niezbędna jest prawidłowa adresacja IP. Każdy adres IP wersji 4 jest 32-bitową liczbą składających się z czterech oktetów. Na podstawie adresu IP jesteśmy w stanie zidentyfikować nie tylko komputer, ale również podsieć do której należy. Wyróżniamy następujące klasy adresów publicznych:

Klasa	Zastosowanie	I oktet	II oktet	II oktet	IV oktet	Zakres adresów	Liczba podsieci	Liczba hostów w sieci
A	Obsługa bardzo dużych sieci	sieć	host	host	host	1.0.0.0 – 126.0.0.0	127	16777214
B	Obsługa średnich i dużych sieci	sieć	sieć	host	host	128.0.0.0 – 191.255.255.255	16382	65534
C	Obsługa dużej liczby małych sieci	sieć	sieć	sieć	host	192.0.0.0 – 223.255.255.255	2097150	254
D	Multiemisja (multicast) – kierowanie pakiety do grup adresów IP	-	-	-	-	224.0.0.0 – 239.255.255.254	Brak podziału	Brak podziału
E	Zarezerwowane przez IETF na potrzeby badawcze	-	-	-	-	240.0.0.0 – 255.255.255.255	-	-

oraz następujące klasy adresów prywatnych (mogą być one wykorzystywane tylko w sieciach lokalnych i są niewidoczne w Internecie):

Klasa	Zakres adresów prywatnych
A	10.0.0.0 – 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

Szczególnie wartym uwagi adresem jest 127.0.0.0, który jest zarezerwowany dla tak zwanej pętli zwrotnej (ang. Loopback). Urządzenia sieciowe, za pomocą tego adresu, mogą wysyłać pakiety do samych siebie. Liczby tej nie można przypisać żadnej sieci.

W części praktycznej zeszytu zostały zawarte sposoby obliczania tych adresów dla konkretnej liczby hostów wraz z przykładami.

Ze względu na ograniczoną pojemność zbioru adresacji IP wersji 4 w stosunku do obecnych potrzeb sieci Internet, od dłuższego czasu trwa ekspansja adresacji IP wersji 6. Planując adresację IP dla sieci, należy podjąć decyzję dotyczącą wersji używanej adresacji IP, tj. tylko wersja 4, tylko wersja 6 lub obydwie równocześnie. Zagadnienia dotyczące adresacji IP wykraczają poza ramy tego opracowania.

Statycznie, czy dynamicznie?

Adresy IP mogą być przydzielane i konfigurowane statycznie, co sprawdza się w komunikacji pomiędzy urządzeniami szkieletowymi. W sieciach LAN, w zakresie adresacji IP dla urządzeń końcowych, często wykorzystuje się DHCP, protokół realizujący dynamiczny przydział i zarządzanie adresami IP w sieci. DHCP ma również możliwość przydzielania bramy domyślnej oraz adresów DNS, a także innych parametrów, wymaganych przez urządzenia końcowe.

Do czego służy DNS?

DNS jest internetowym odzwierciedleniem książki telefonicznej. Odpowiada on za zamianę nazw domen internetowych na adresy IP serwerów, do których są one przypisane. Przykładem jest strona www.nask.pl, której odpowiednikiem jest adres IP 195.187.242.157.

Trasowanie, czyli nawigacja GPS dla sieci

Do prawidłowego działania sieci niezbędne jest również trasowanie (ang. Routing), czyli nadanie pakietowi odpowiedniej trasy i wysłanie go nią w celu dotarcia do odpowiedniego miejsca docelowego. Pakiety przesyłane przez sieć zawierają adresy nadawcy i odbiorcy, a zadaniem router'ów, jako urządzeń pośredniczących pomiędzy nadawcą a odbiorcą, jest przesłanie pakietów do celu najlepszą trasą.

Zapora sieciowa

Nieodzownym elementem sieci jest również Firewall, czyli zapora sieciowa, pracująca na styku z siecią publiczną. Służy on do filtrowania danych przychodzących i wychodzących w sieci. Zapora sieciowa umożliwia tworzenie polityki bezpieczeństwa i definiowania reguł, na przykład blokowanie ruchu pomiędzy dwiema podsieciami działającymi w obrębie tego samego routera, bądź zablokowanie wszelkich połączeń przychodzących z zewnątrz do naszego urządzenia końcowego. Waga reguły jest zazwyczaj zależna od numeru pozycji na którym znajduje się w ustawieniach firewall'a (im wyżej, tym ważniejsza, ma przewagę nad pozostałymi, jeśli któraś poniżej się z nią pokrywa, stosowana jest ta wyższa).

Translacja adresów i jej zastosowanie

Ważną rzeczą jest również NAT, czyli technika translacji adresów. Translacja ta jest zazwyczaj dynamiczna – jeden adres IP z sieci WAN jest tłumaczony na dowolną ilość adresów w sieci LAN. Technologia ta umożliwia podłączenie dużej ilości komputerów z sieci LAN do Internetu wykorzystując jedno IP zewnętrzne. Adresacja urządzeń końcowych jest dobierana w oparciu o klasę adresów prywatnych, dzięki czemu zapobiega się również konfliktom z adresami publicznymi.

W zastosowanym przez nas urządzeniu firmy Mikrotik opcja ta (dosłownie) kryje się pod nazwą masquerade.

QoS

Przydatną rzeczą jest również QoS (Quality of Service), czyli zapewnienie jakości usługi. Składa się na to między innymi: kształtowanie i ograniczanie przepustowości, zapewnienie sprawiedliwego dostępu do zasobów, nadawanie odpowiednich priorytetów poszczególnym pakietom wędrującym przez sieć, zarządzanie opóźnieniami w przesyłaniu danych, zarządzanie buforowaniem nadmiarowych pakietów, określenie charakterystyki gubienia pakietów, unikanie przeciążeń.

W wykorzystanym przez nas urządzeniu do tego celu służy narzędzie Queues (kolejki). Kolejki dzielimy na:

- Simple – możemy dodać proste ograniczenia, na przykład maksymalnej prędkości, dla konkretnej podsieci lub konkretnych połączeń (możliwe jest również działanie tylko w wyznaczonych godzinach)
- Tree – możemy dodać zaawansowane, zagnieżdżone i rozbudowane parametrami drzewo kolejek, zawierające m.in priorytety danych jego elementów, przypisanie do konkretnie oznaczonych pakietów, oraz ograniczenia ich dotyczące.

Dlaczego Mikrotik?

Powodem, dla którego kurs ten został przygotowany w oparciu o urządzenie firmy Mikrotik jest budżetowość. Dla (przykładowo) szkoły, która zapewne nie dysponuje aż takimi środkami, by wdrożyć w swojej placówce sprzęt z górnej półki (np. Cisco), a tym bardziej nie dysponuje osobami, które mają wiedzę i doświadczenie w konfiguracji takowego sprzętu, naprzeciw wychodzi właśnie Mikrotik. Urządzenia tej firmy są stosunkowo tanie oraz posiadają bardzo zaawansowaną i rozbudowaną konfigurację, pozwalającą zrealizować niemalże każdy pomysły administratora sieci w stosunkowo prosty sposób.

Warsztaty

Proste obliczenia podsieci

Przykład 1

Podział sieci o adresie IP 220.110.40.0/24 na 5 podsieci.

1. Podstawą naszej maski jest maska 24 bitowa, zatem możemy ją zapisać w postaci binarnej:
   11111111.11111111.11111111._ _ _ _ _ _ _ _
   co w postaci dziesiętnej da nam:
   255.255.255._ _ _ _ _ _ _ _
2. Wiedząc, że będzie to 5 równych podsieci, musimy zapisać liczbę 5 w postaci binarnej - 101(2). Liczba ta została zapisana na 3 bitach, zatem w masce naszej podsieci będą trzy jedynki aktywne. Pozostałe miejsca maski wypełniamy zerami:
   255.255.255.11100000
   co w postaci dziesiętnej da nam:
   255.255.255.224
3. Aby obliczyć liczbę hostów musimy na początek zanegować postać binarną maski – innymi słowy zamienić 0 na 1, a 1 na 0.
   Otrzymamy zatem 00000000.00000000.00000000.00011111 Teraz podliczamy ilość jedynek i podstawiamy pod n do wzoru: 2n-2=25-2=30. Dlaczego odejmujemy 2? 1 z adresów musi być adresem podsieci, drugi natomiast adresem rozgłoszeniowym, dlatego liczba adresów dla hostów jest o 2 mniejsza.
4. Adresem pierwszej podsieci jest adres podany w zadaniu, tj. 220.110.40.0 , maską (tak jak w każdej podsieci) obliczona wcześniej 255.255.255.224, zakres hostów to adres IP podsieci + 1 (czyli 220.110.40.1) do adres IP podsieci + liczba hostów (czyli 220.110.40.30), natomiast adres rozgłoszeniowy o 1 większy od adresu ostatniego hosta, czyli 220.110.40.31
5. Adresem kolejnej sieci jest adres o 1 większy, niż rozgłoszeniowy poprzedniej. Reszta obliczeń jest analogiczna, jak w pierwszej podsieci.

Nr podsieci	Adres podsieci	Maska podsieci	Zakres hostów	Adres rozgłoszeniowy
1	220.110.40.0	255.255.255.224	220.110.40.1 - 220.110.40.30	220.110.40.31
2	220.110.40.32	255.255.255.224	220.110.40.33 – 220.110.40.62	220.110.40.63
3	220.110.40.64	255.255.255.224	220.110.40.65 – 220.110.40.94	220.110.40.95
4	220.110.40.96	255.255.255.224	220.110.40.97 – 220.110.40.126	220.110.40.127
5	220.110.40.128	255.255.255.224	220.110.40.129 – 220.110.40.158	220.110.40.159

Przykład 2

Podział sieci o adresie IP 195.130.25.0/24 na 3 podsieci.

1. Podstawą naszej maski jest maska 24 bitowa, zatem możemy ją zapisać w postaci binarnej:
   11111111.11111111.11111111._ _ _ _ _ _ _ _
   co w postaci dziesiętnej da nam:
   255.255.255._ _ _ _ _ _ _ _
2. Wiedząc, że będą to 3 równe podsieci, musimy zapisać liczbę 3 w postaci binarnej - 11(2). Liczba ta została zapisana na 2 bitach, zatem w masce naszej podsieci będą dwie jedynki aktywne. Pozostałe miejsca maski wypełniamy zerami:
   255.255.255.11000000
   co w postaci dziesiętnej da nam:
   255.255.255.192
3. Aby obliczyć liczbę hostów musimy na początek zanegować postać binarną maski – innymi słowy zamienić 0 na 1, a 1 na 0. Otrzymamy zatem 00000000.00000000.00000000.00111111
   Teraz podliczamy ilość jedynek i podstawiamy pod n do wzoru: 2n-2=26-2=62.
   Dlaczego odejmujemy 2? 1 z adresów musi być adresem podsieci, drugi natomiast adresem rozgłoszeniowym, dlatego liczba adresów dla hostów jest o 2 mniejsza.
4. Adresem pierwszej podsieci jest adres podany w zadaniu, tj. 195.130.25.0, maską (tak jak w każdej podsieci) obliczona wcześniej 255.255.255.192, zakres hostów to adres IP podsieci + 1 (czyli 195.130.25.1) do adres IP podsieci + liczba hostów (czyli 195.130.25.62), natomiast adres rozgłoszeniowy o 1 większy od adresu ostatniego hosta, czyli 195.13.25.63
5. Adresem kolejnej sieci jest adres o 1 większy, niż rozgłoszeniowy poprzedniej. Reszta obliczeń jest analogiczna, jak w pierwszej podsieci.

Nr podsieci	Adres podsieci	Maska podsieci	Zakres hostów	Adres rozgłoszeniowy
1	195.130.25.0	255.255.255.192	195.130.25.1 - 195.130.25.62	195.130.25.63
2	195.130.25.64	255.255.255.192	195.130.25.65 - 195.130.25.126	195.130.25.127
3	195.130.25.128	255.255.255.192	195.130.25.129 - 195.130.25.190	195.130.25.191

Opis przykładowej sieci szkolnej

Charakterystyka budynku

Szkoła dwupiętrowa, na każdym piętrze znajduje się 30 pracowni. W każdej z nich znajduje się komputer nauczyciela, który ma zostać podłączony. Na parterze, w pomieszczeniu 008 znajduje się również pracownia informatyczna, w której znajduje się 20 komputerów.

Łącze internetowe

Przez ISP (Internet Service Provider – dostawca usług internetowych) zostało zapewnione symetryczne łącze 100 Mb/s podłączane przez port Ethernet 1Gb/s (1000BASE-T).

Niezbędne urządzenia

Biorąc pod uwagę charakterystykę budynku niezbędne są następujące urządzenia:

- Na każde piętro jeden przełącznik z co najmniej 30 użytecznymi portami FastEthernet (100BASE-TX) [zazwyczaj są to 48 portowe przełączniki) oraz co najmniej 2 portami Ethernet 1 Gb/s (1000BASE-T) do połączenia między przełącznikiem i routerem.
  Dopuszczalne jest również użycie na każdym piętrze dwóch przełączników po 24 porty o podobnych parametrach do wcześniej opisanych.
- Router (brzegowy) powinien być wyposażony w przynajmniej 1 port WAN [Ethernet 1 Gb/s (1000BASE-T)], oraz co najmniej 3 porty LAN [Ethernet 1 Gb/s (1000BASE-T)].

Zagospodarowanie portów router'a

Koncepcja połączeniowa sieci jest następująca:

1. Do portu pierwszego podłączone będą przełączniki zapewniające łącze przewodowe na każdym z pięter, adresacja zostaje przydzielona przez DHCP z puli adresów 192.168.0.0/24 (klasa C, maksymalna ilość hostów/komputerów w tej podsieci 254, biorąc pod uwagę że przełącznik na każdym piętrze ma 48 portów, zatem 254-3*48=254-144=110 hostów zapasu).
2. Do portu drugiego podłączona będzie pracownia informatyczna, w której znajduje się 20 komputerów, adresacja zostaje przydzielona przez DHCP z puli adresów 192.168.8.0/24 (klasa C, maksymalna ilość hostów/komputerów w tej podsieci 254, biorąc pod uwagę że przełącznik ma 24 porty, zatem 254-24=230 hostów zapasu). Niezbędne będzie zatem umiejscowienie w tej pracowni przełącznika o minimalnej ilości użytecznych portów FastEthernet (100BASE-TX) 20 (zazwyczaj są to 24 portowe przełączniki) oraz co najmniej 1 portem Ethernet 1 Gb/s (1000BASE-T) do połączenia między przełącznikiem i routerem.
3. Pozostałe porty pozostają niepodłączone – przeznaczone są one na przyszłościowy rozwój istniejącej sieci np. o część bezprzewodową.

Główne założenia sieci

1. Zapewnienie stabilnego łącza sieciowego w obrębie szkoły
2. Umożliwiającego dostępu do internetu na następujących zasadach:
   a. Zarezerwowanie połowy przydzielonego łącza internetowego dla nauczycieli
   b. Zarezerwowanie pozostałej części, czyli drugiej połowy przydzielonego łącza, dla pracowni informatycznej
3. Separacja ruchu pomiędzy siecią nauczycielską a siecią uczniowską
4. Zapewnienie połączenia między komputerem nauczyciela w pracowni informatycznej, a pozostałymi komputerami w pracowni informatycznej

Przykładowy kosztorys urządzeń

- Router Mikrotik RB750Gr3: 220 zł
- Po 2 przełączniki dla 3 pięter - 24 porty Mikrotik CSS326-24G-2S+RM: 2*3*500 zł = 3000 zł
- Przełącznik dla pracowni informatycznej - 24 porty Mikrotik CSS326-24G-2S+RM 500 zł

Sumaryczny koszt zakupu urządzeń to około 3720 złotych. Należy pamiętać, że niezbędny będzie również zakup przewodu sieciowego (np. Cat. 5E), listw kablowych, gniazd abonenckich RJ45, oraz wtyków RJ45. Do zrealizowania sieci potrzebne będą również podstawowe narzędzia, takie jak wiertarka, a także narzędzia specyficzne – zaciskarka oraz tester okablowania sieciowego.

Całość kosztów powinna zamknąć się w kwocie 5000 złotych.

Dlaczego warto zainwestować w taką sieć?

Cała infrastruktura opisanej sieci skonstruowana jest w taki sposób, by dawała nieograniczone możliwości zarządzania, nadzoru i dalszego rozwoju sieci bez straty wydajności. W każdej chwili można na przykład sprawdzić wykorzystanie łącza przez dowolne urządzenie w sieci, wykryć nadmierne obciążenie i za pomocą dostępnych w urządzeniach narzędzi wyeliminować problem. Znakomitym przykładem może być uruchamianie na zajęciach w pracowni informatycznej bez wiedzy nauczyciela programu typu P2P który wykorzystywałby całe łącze przydzielone dla pracowni informatycznej – w ciągu chwili można taki ruch wyciąć.

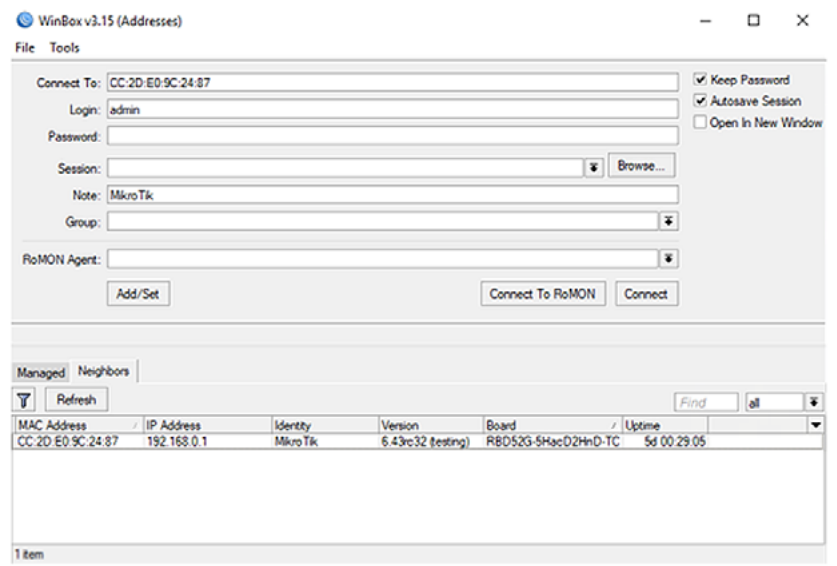
Konfiguracja routera firmy Mikrotik do obsługi podanej sieci

Pobranie oprogramowania WinBox

Jednym ze sposobów zarządzania urządzeniami firmy Mikrotik jest wykorzystanie oprogramowania Winbox, dostępnego wyłącznie dla systemu Windows. W celu pobrania go, należy udać się na stronę mikrotik.com/download , a następnie kliknąć w przycisk WinBox i pobrać najnowszą wersję. Program ten nie wymaga instalacji – po uruchomieniu jest od razu gotowy do pracy.

Podłączanie się do urządzenia

Podłączamy nasz komputer do dowolnego portu routera (zalecany port 2 – w przypadku niektórych nowych modeli może być wgrana przykładowa konfiguracja uniemożliwiająca połączenie poprzez port 1), a następnie uruchamiamy oprogramowanie WinBox. Przechodzimy do zakładki Neighbors i wyszukujemy nasze urządzenie – klikamy dwukrotnie.

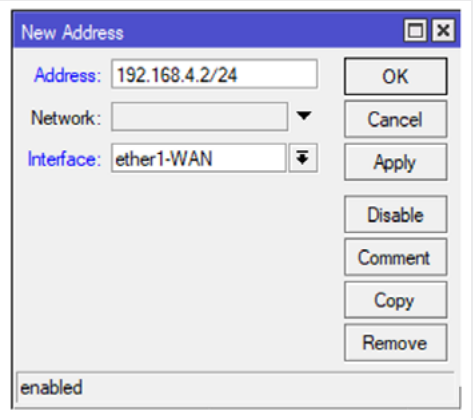


W polu Connect To: ustawi się mac address urządzenia bądź jego adres IP (jeśli był wcześniej konfigurowany). Domyślne dane logowania są następujące: Login admin, a hasła brak. Klikamy Connect.

Konfiguracja adresacji portu WAN

IP przypisywane statycznie przez dostawcę

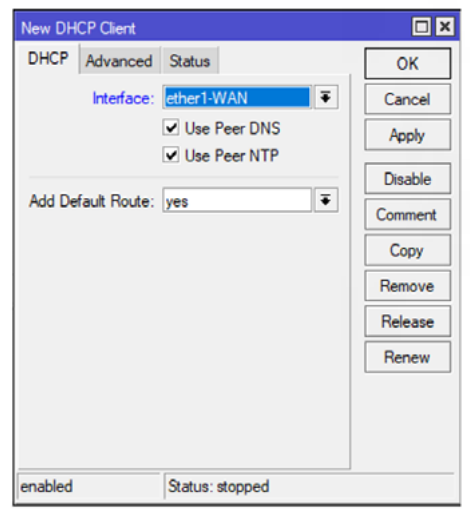
W wypadku, gdy nasz dostawca zapewnia nam statyczny adres IP należy przejść do zakładki IP -> Addresses, klikamy na +.



W otwartym oknie wpisujemy otrzymany od dostawcy adres IP, stawiamy ukośnik, a po nim wpisujemy ilu bitowa jest maska podsieci. Wybieramy odpowiedni interfejs, na którym będzie podłączony WAN (z reguły jest to port 1). Zatwierdzamy.

IP przypisywane dynamicznie przez dostawcę

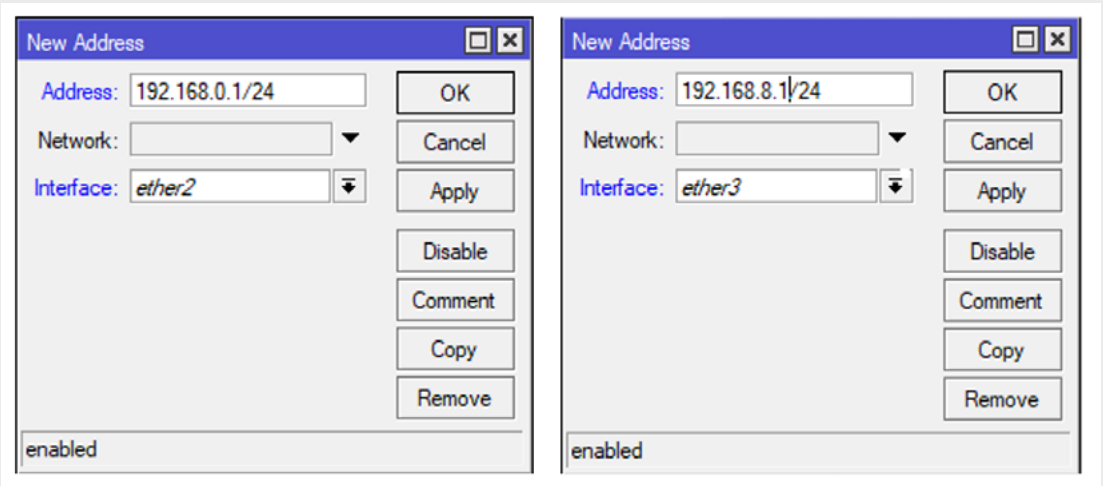
W przypadku, gdy nasz dostawca zapewnia nam dynamiczny adres IP należy przejść do zakładki IP -> DHCP Client i kliknąć +.



W otwartym oknie wybieramy interfejs WAN (z reguły port 1), upewniamy się że mamy zaznaczone Use Peer DNS oraz NTP (pobierze nam z serwera DHCP automatycznie adresy serwera DNS oraz NTP – czasu). Upewniamy się również, że mamy wybrane Add Default Route: yes (dzięki tej opcji, automatycznie zostanie wykonane odpowiednie trasowanie). Zatwierdzamy.

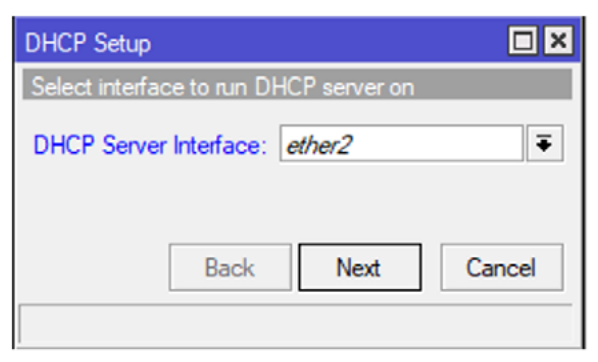
Konfiguracja adresacji pozostałych portów

Teraz konfigurujemy pozostałe porty, identycznie jak konfiguruje się statyczny adres IP (opisane powyżej). Port 2 o adresie IP 192.168.0.1/24 (sieć nauczycieli), a port 3 o adresie IP 192.168.8.1/24.

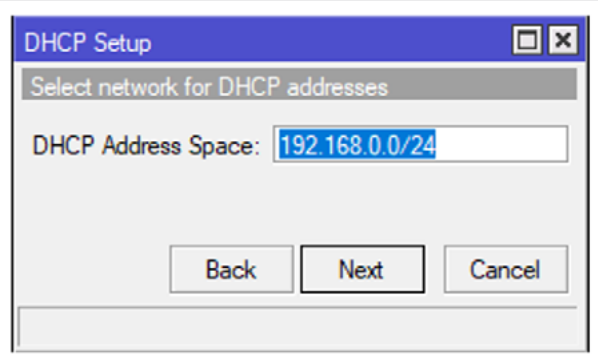


Konfiguracja serwera DHCP

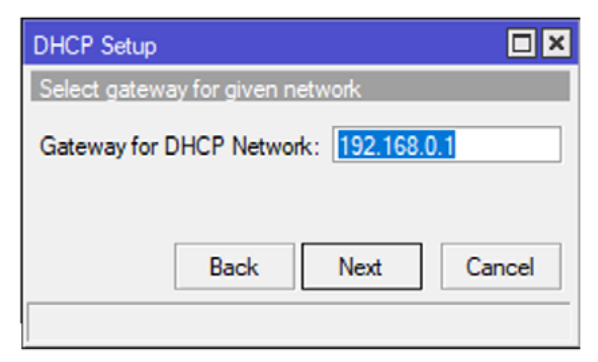
Przechodzimy do zakładki IP -> DHCP Server. Klikamy na przycisk DHCP Setup.



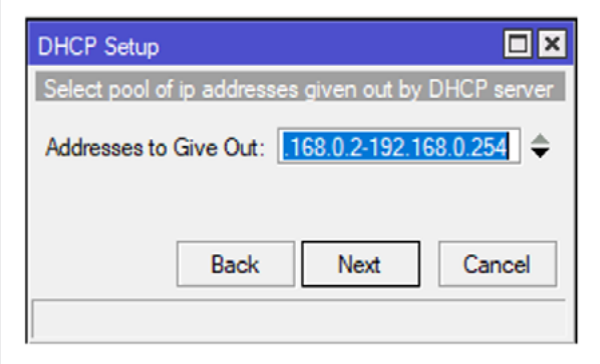
Wybieramy interfejs, dla którego chcemy skonfigurować serwer DHCP, klikamy dalej.



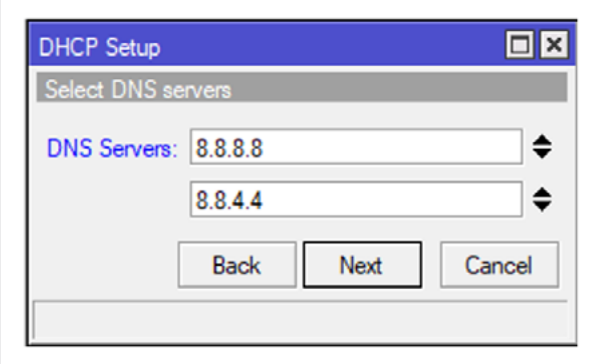
Teraz należy wpisać przestrzeń adresową do zagospodarowania – ze względu na to, iż wcześniej ustawiliśmy adresację portu, pole to jest już wypełnione prawidłowo. Klikamy dalej.



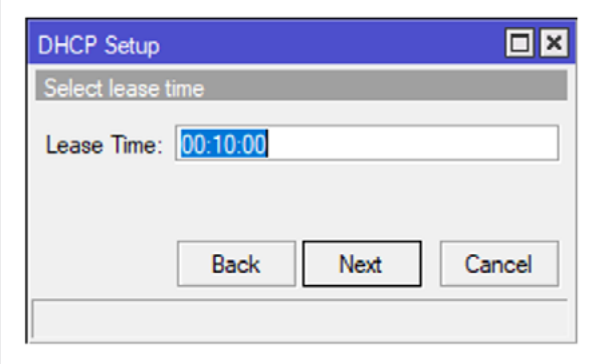
Brama domyślna jest również prawidłowo ustawiona, ze względu na wcześniejszą adresację IP portu. Innymi słowy powinien być tu podany adres IP naszego routera, który będzie bramą do innych podsieci. Klikamy dalej.



W tym oknie należy wybrać zakres adresów, które serwer będzie nadawał – polecam pozostawić domyślne.



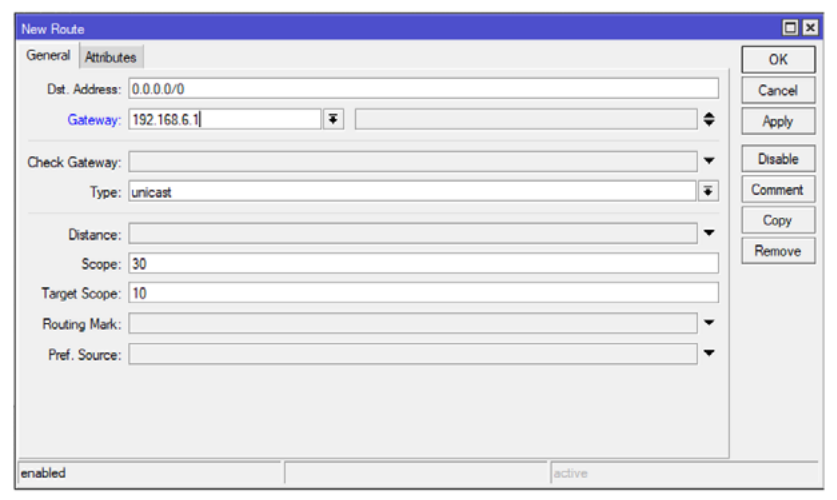
Teraz należy wprowadzić adresy serwerów DNS, które będzie przydzielał serwer DHCP – zalecam użycie darmowej usługi DNS Google (adresy: 8.8.8.8, 8.8.4.4).



W następnym oknie wpisujemy czas, przez jaki chcemy, by przypisany przez serwer DHCP adres powiązany był z adresem MAC komputera. Po upłynięciu tego czasu, adres IP będzie nadawany ponownie – można pozostawić domyślne 10 minut. Kończymy konfigurację DHCP dla portu 2. Identycznym schematem postępujemy z serwerem DHCP dla portu 3.

Konfiguracja trasowania (tylko w przypadku statycznego IP portu WAN)

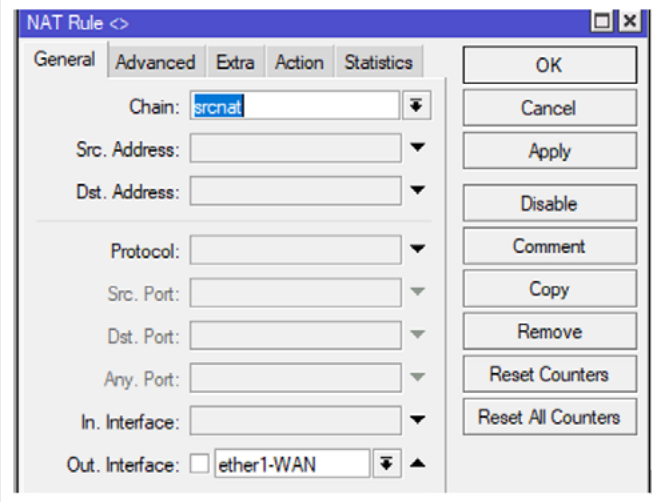
Przejdźmy do konfiguracji trasowania (tylko w wypadku, gdy WAN podawany był statycznie) – wchodzimy w zakładkę IP -> Routes, klikamy +.



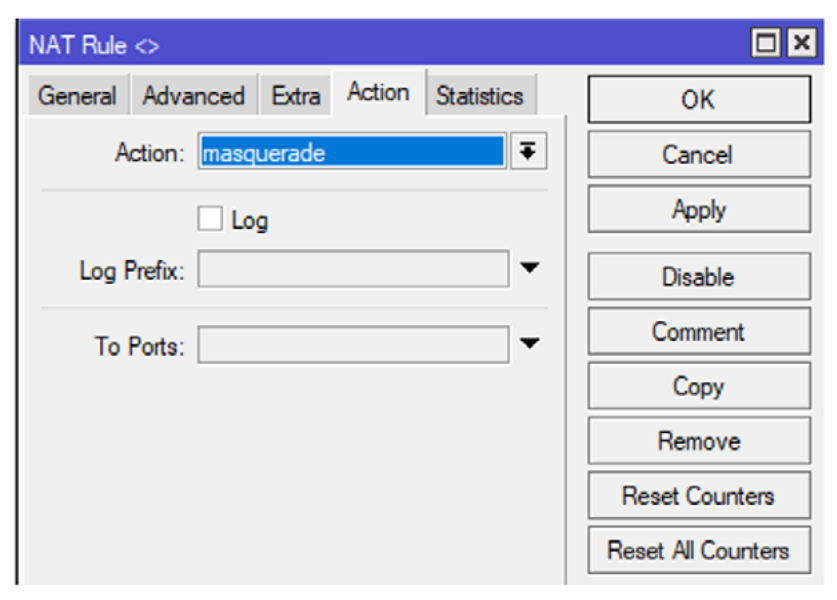
Otwieramy sobie pole Gateway, w którym podajemy bramę domyślną podaną przez naszego dostawcę i zatwierdzamy.

Konfiguracja NAT

Teraz ustawimy NAT dynamiczny, zwany masquerade. W tym celu przechodzimy do zakładki IP –> Firewall, następnie podzakładka NAT – klikamy +.



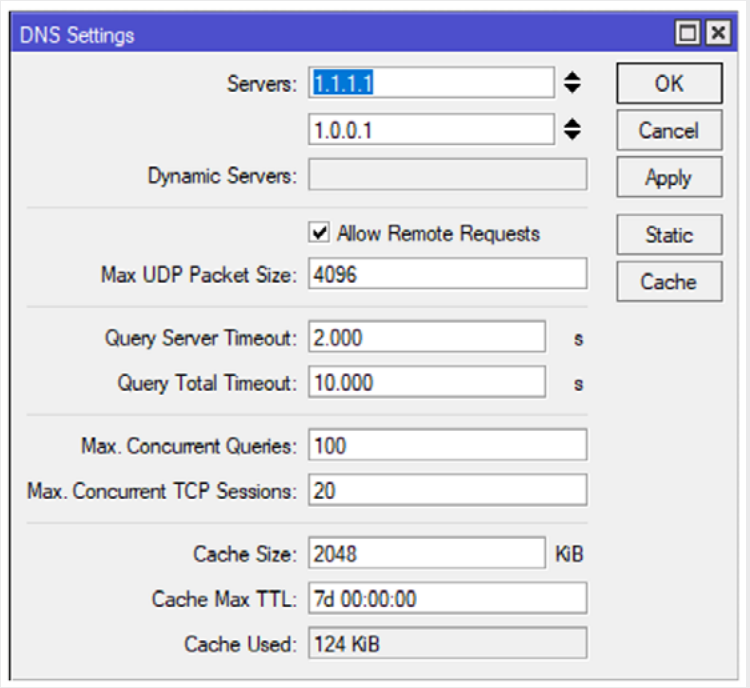
W otwartym oknie w zakładce general wybieramy Chain: srcnat oraz Out. Interface naszInterfejsWAN.



W zakładce Action wybieramy Action: masquerade.

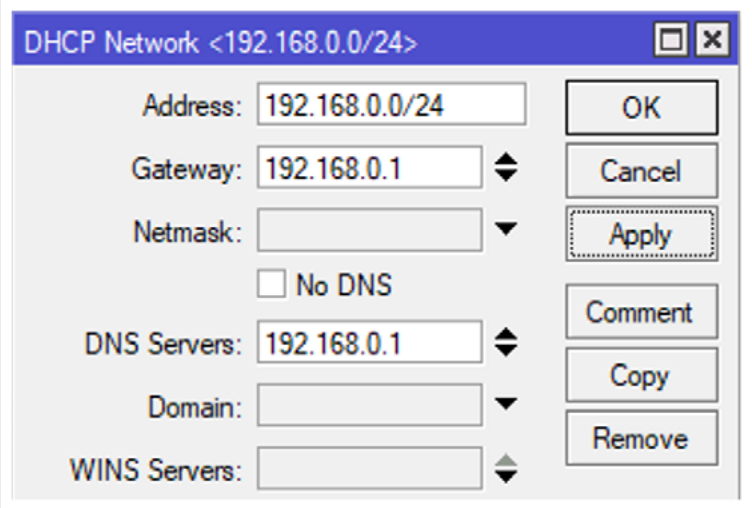
Uruchomienie i konfiguracja serwera DNS w sieci lokalnej

Aby umożliwić użytkownikom jak najszybszy dostęp do serwera rozpoznawania nazw, można uruchomić usługę serwera DNS na routerze. Będzie on pobierał do pamięci podręcznej informacje DNS z publicznej usługi DNS, takiej jak np. google (8.8.8.8, 8.8.4.4) czy cloudflare (1.0.0.1, 1.1.1.1). W tym celu przechodzimy do zakładki IP -> DNS.



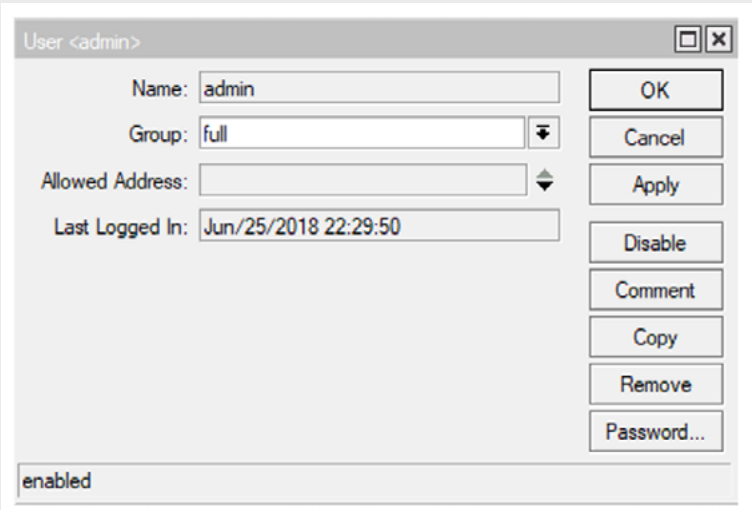
W polach servers wpisujemy adresy DNS jednej z wcześniej wymienionych usług, upewniamy się że zaznaczona jest opcja Allow Remote Requests, zatwierdzamy.

Należy pamiętać, by zmienić w ustawieniach serwera DHCP, przypisywany automatycznie serwer DNS na adres portu naszego routera przypisanego do danego serwera DHCP. W tym celu przechodzimy do zakładki IP -> DHCP Server, następnie do podzakładki networks, klikamy dwukrotnie na każdą z naszych podsieci DHCP i ustawiamy przypisywanie tylko jednego serwera DNS – o IP takim, jak brama domyślna, czyli serwer DNS naszego routera.

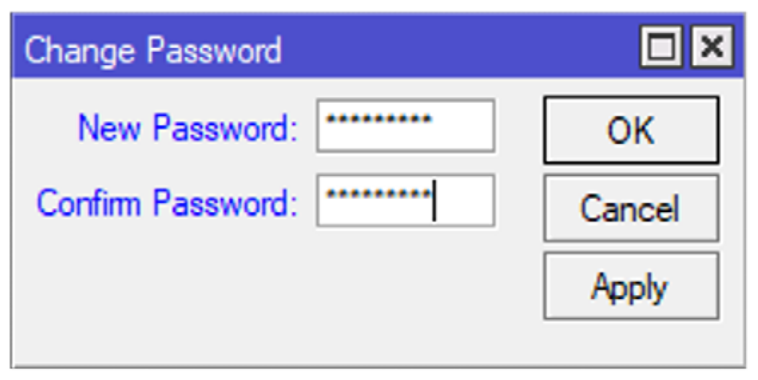


Zmiana domyślnego hasła administratora

Aby zapobiec nieuprawionemu dostępowi, należy najpierw zmienić hasło. W tym celu wchodzimy do zakładki System -> Users, klikamy dwukrotnie na użytkownika admin.

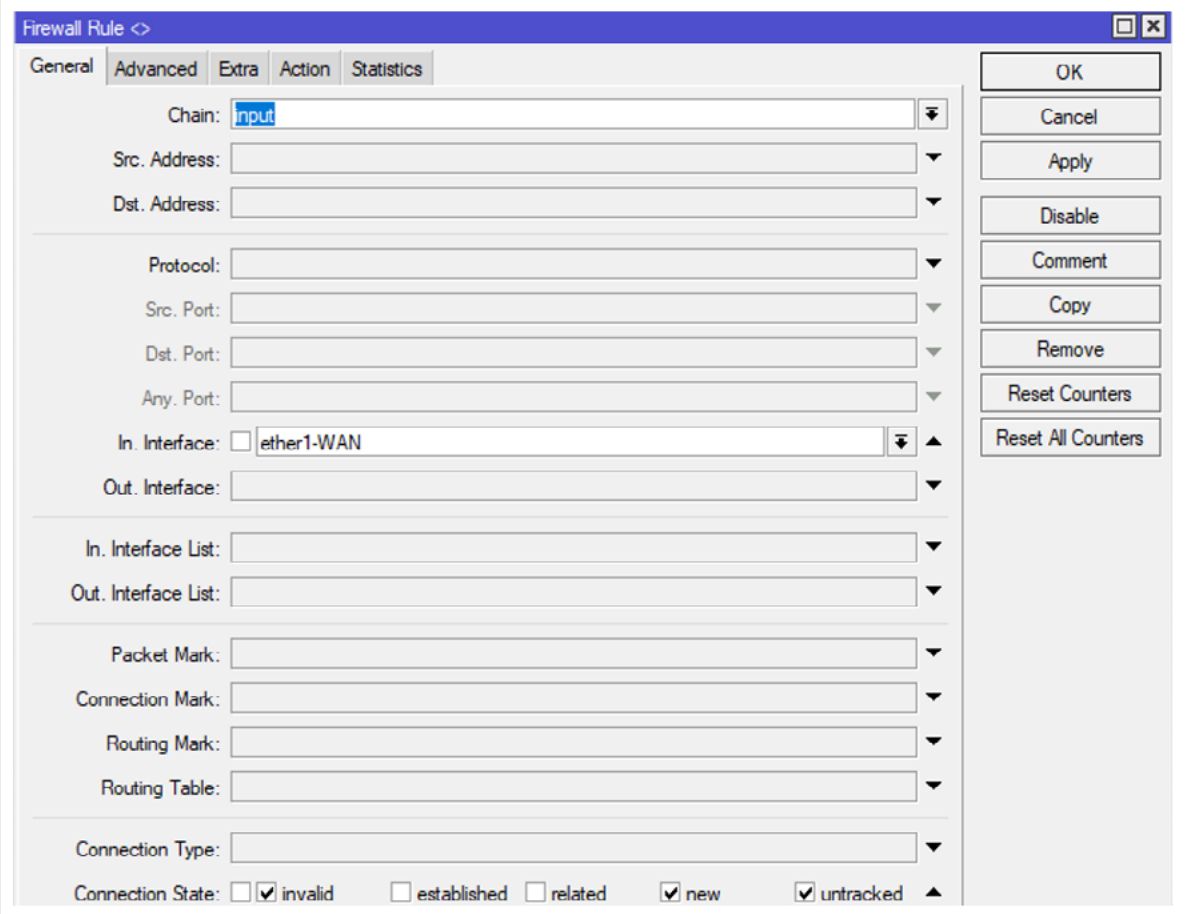


W otwartym oknie klikamy na przycisk password.

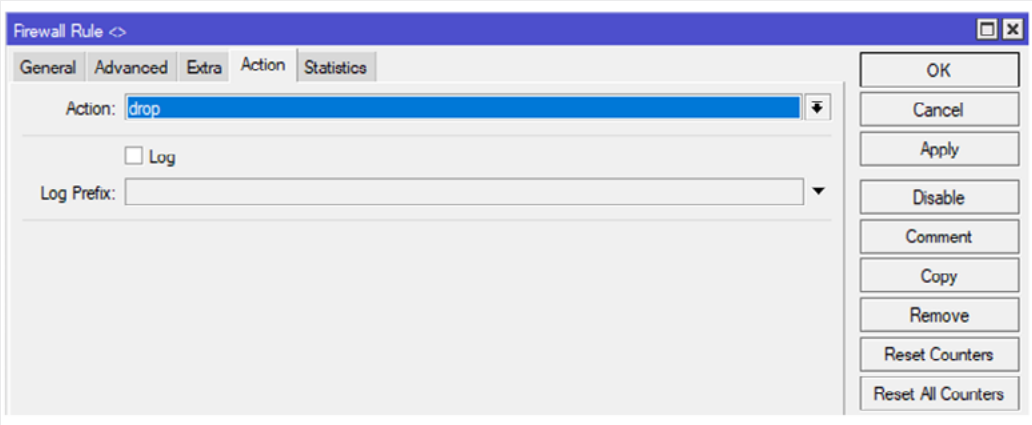


Zablokowanie ruchu przychodzącego

Aby zablokować wszystkie połączenia przychodzące do naszego routera, przechodzimy do zakładki IP -> Firewall i klikamy +.



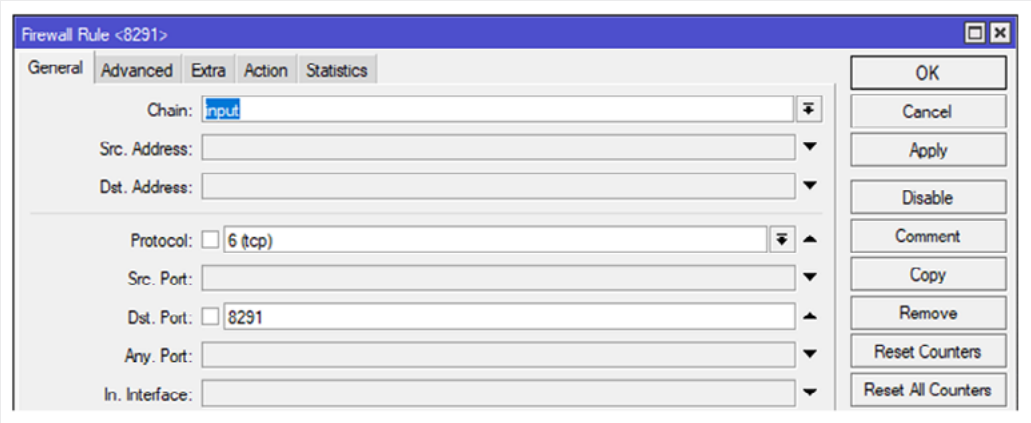
Zakładka General, wybieramy Chain: input, In. Interface: naszInterfejsWAN, Connection State: zaznaczmy invalid, new, untracked.



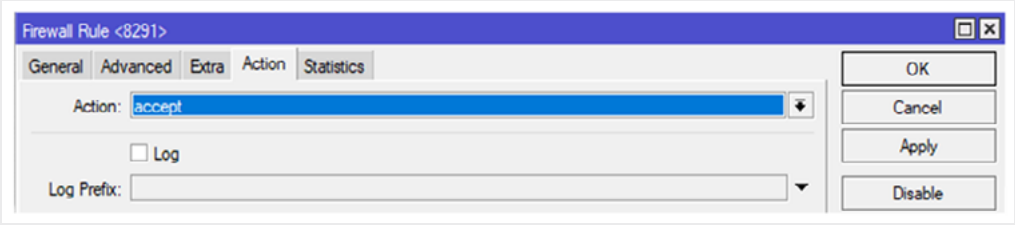
Zakładka Action wybieramy Action: drop. Zapisujemy. Teraz wszystkie połączenia na wejściu są zablokowane.

Umożliwienie zdalnego dostępu Winbox

Aby umożliwić dostęp zdalny do naszego routera poprzez winbox, musimy utworzyć nową regułę Firewall.



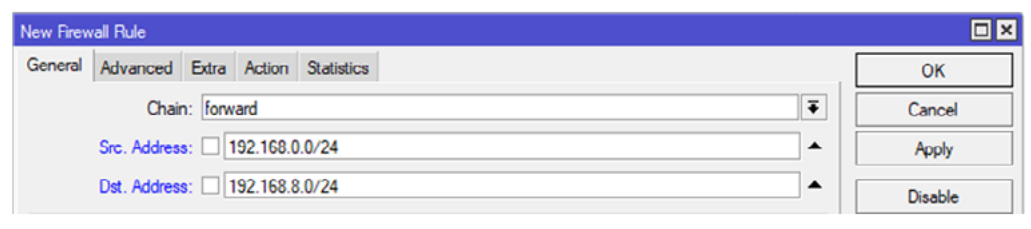
W zakładce General wybieramy: Chain: input, Protocol: 6 (tcp), Dst.Port 8291 [domyślny port winbox].



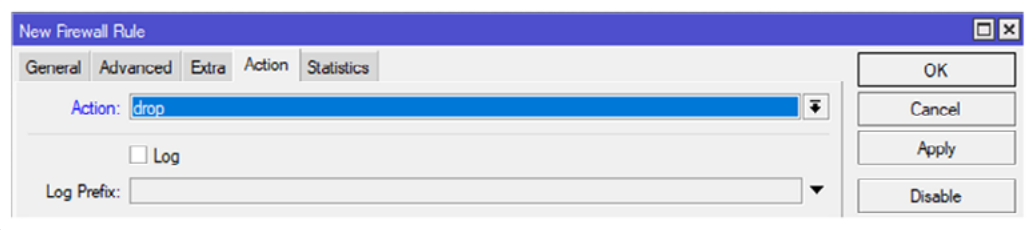
W zakładce Action wybieramy Action: accept. Zatwierdzamy.

Zablokowanie ruchu pomiędzy podsiecią nauczycieli, a uczniów

Aby zablokować ruch między podsieciami, dodamy nową regułę w Firewall'u.



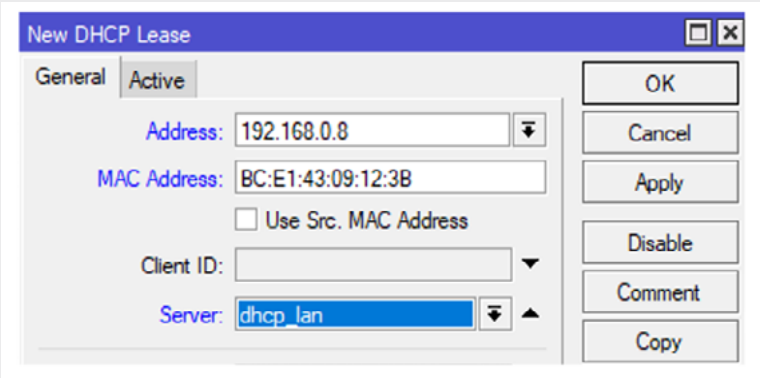
Wybieramy: Chain: forward, następnie Src. Address: 192.168.0.0/24, Dst. Address: 192.168.8.0/24.



W zakładce Action wybieramy Action: drop. Zapisujemy regułę, a następnie dodajemy kolejną, wykonując te same czynności, jednakże zamieniając miejscami Src. Address z Dst. Address.

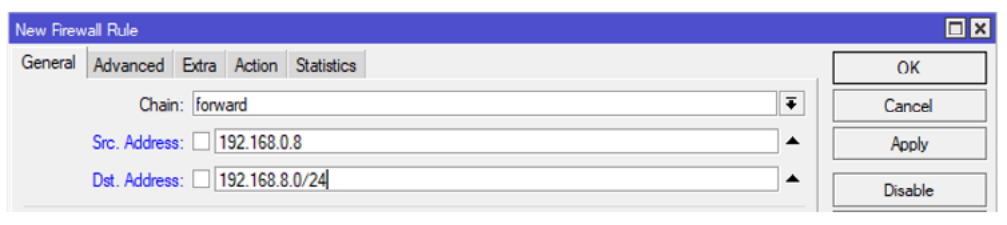
Umożliwienie nauczycielowi w pracowni informatycznej łączenia się z podsiecią uczniów

Na początek musimy przydzielić statyczne IP nauczycielowi, a następnie dodać kolejne reguły, nadrzędne nad blokadą między podsieciami, które umożliwią mu komunikację z siecią pracowni. W tym celu: przechodzimy do IP -> DHCP Server, zakładka Leases, klikamy +.

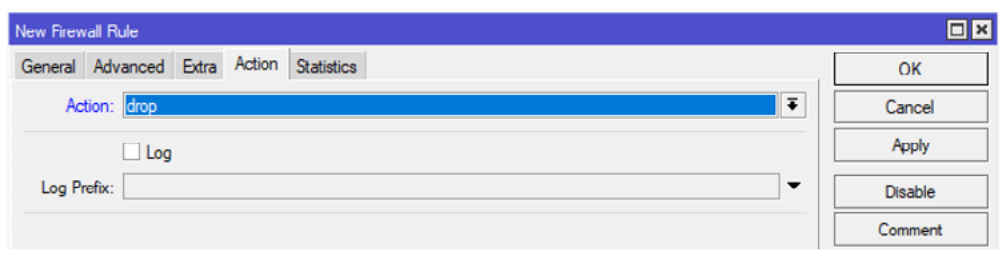


W polu Address wprowadzamy 192.168.0.8 (komputer w pracowni 8, podsieć nauczycieli 192.168.0.0/24), następnie podajemy MAC Address karty sieciowej tego komputera, wybieramy serwer dhcp nauczycieli i zapisujemy. Teraz w firewall należy utworzyć reguły nadrzędne,

które umożliwią komunikację IP 192.168.0.8 z podsiecią 192.168.8.0/24 i odwrotnie. W tym celu otwieramy IP -> Firewall, dodajemy nową regułę.



Chain: forward, Src. Address: 192.168.0.8, Dst. Address: 192.168.8.0/24.



W zakładce Action Action: accept. Powtarzamy czynność, z tym że zamieniamy kolejność Src oraz Dst.

Słownik

PING

polecenie umożliwiające sprawdzenie, czy istnieje połączenie między hostem testującym i testowanym za pomocą pakietów ICMP. Umożliwia ono mierzenie liczby zgubionych pakietów oraz opóźnienia w ich transmisji. Podstawowa składnia polecenia jest następująca:

ping <adres_ip_hosta>
lub
ping <adres_www>

W przypadku systemów z rodziny UNIX (Linux, Mac OS) polecenie to trwa, dopóki nie przerwiemy go za pomocą kombinacji klawiszy CTRL/CMD+C. W systemie Windows wysyłane są wyłącznie cztery pakiety. Aby uzyskać podobny efekt, czyli nieskończone działanie polecenia ping w systemie Windows należy dodać parametr –t do polecenia, a będzie to wyglądało następująco:

ping <adres_ip_hosta> -t
lub
ping <adres_www> -t

Rezultatami polecenia są wyniki, czy została otrzymana odpowiedź, wielkość pakietu, czas odpowiedzi oraz czas życia pakietu. Po zatrzymaniu działania polecenia wyświetlane jest krótkie podsumowanie wraz ze statystykami.

Dzięki temu narzędziu jesteśmy w stanie określić jakie opóźnienie występuje pomiędzy dwoma hostami, bądź po prostu sprawdzić między nimi połączenie.

Należy również pamiętać, iż pakiety ICMP wykorzystywane przez ping mogą być blokowane przez zapory sieciowe, dlatego należy je wyłączyć na czas testów, bądź dodać/zmodyfikować odpowiednie reguły.

TRACEROUTE

polecenie umożliwiające sprawdzenie trasy wysyłanych pakietów do wybranego hosta przez sieć.

W systemach z rodziny UNIX (Linux, Mac OS) składnia polecenia jest następująca:

traceroute <adres_ip_hosta>
lub
traceroute <adres_www>

Natomiast w systemach Windows nazwa samego polecenia jest nieco odmienna:

tracert <adres_ip_hosta>
lub
tracert <adres_www>

Polecenie trwa do momentu dotarcia do hosta docelowego, bądź (domyślnie w wielu systemach) do 30 przeskoków.

Dzięki temu narzędziu, jesteśmy w stanie określić w którym miejscu występuje problem z komunikacją – jest to niezwykle przydatne przy zgłaszaniu jakiejkolwiek awarii sieci.

Źródła:
https://pl.wikipedia.org/wiki/Skrętka

OGÓLNOPOLSKA
SIEĆ EDUKACYJNA

T: +48 22 182 55 55
E: ose@nask.pl

A: ul. Kolska 12
01-045 Warszawa

W: ose.gov.pl

NIP 5210417157
REGON 010464542

Ministerstwo
Cyfryzacji

MINISTERSTWO
EDUKACJI
NARODOWEJ

NASK