Łukasz Guziak

KONFIGURACJA USŁUG SIECIOWYCH NA URZĄDZENIACH MIKROTIK

Poziom zaawansowany

Helion

Redaktor prowadzący: Małgorzata Kulik

Projekt okładki: Studio Gravite/Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki

Grafika na okładce została wykorzystana za zgodą AdobeStock.com.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
helion.pl/user/opinie/konuza
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-289-1233-5

Printed in Poland.

Spis treści

ROZDZIAŁ 1.

Routing statyczny

Podstawy routingu statycznego są przedstawione w mojej wcześniejszej książce, ale to omówienie nie wyczerpuje tematu. Teraz poruszę bardziej zaawansowane kwestie.

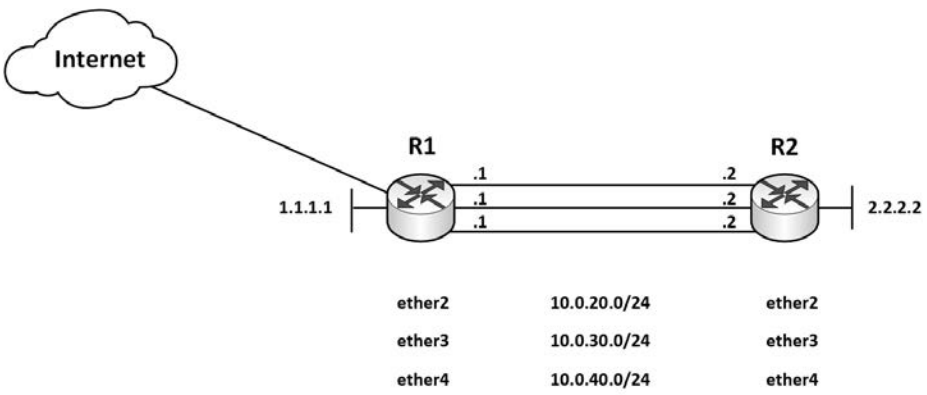
W tym rozdziale:

- Nauczysz się, jak skonfigurować dodatkowe trasy statyczne.
- Dowiesz się, za co odpowiada dystans administracyjny.
- Zmienisz wartość pola TTL.
- Zastosujesz strategie routingu.

1.1. Redundancja tras

Redundancja (nadmiarowość) zazwyczaj kojarzy się z zastosowaniem dodatkowych elementów infrastruktury (np. serwer, router, UPS), które zastępują urządzenie główne w razie jego awarii. W kontekście sieci komputerowych redundancja będzie również dotyczyć zapasowych łączy, które są aktywowane, gdy zawodzi to podstawowe.

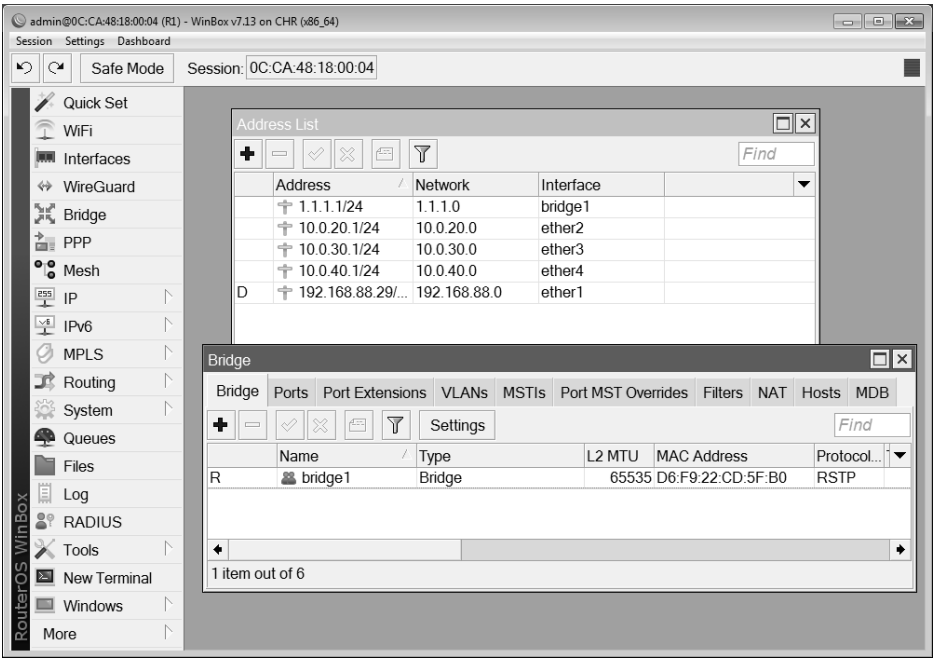
Obowiązująca w tym podrozdziale i następnym topologia sieciowa jest pokazana na rysunku 1.1.



RYSUNEK 1.1. Topologia sieciowa

Router *R1* z routerem *R2* połączono za pośrednictwem trzech niezależnych połączeń. Każde z nich tworzy odrębną sieć. Dodatkowo router *R1* ma zestawione połączenie z siecią Internet.

Test połączenia będzie przeprowadzany pomiędzy interfejsami o adresach IP *1.1.1.1* i *2.2.2.2*. Ci z Was, którzy mają (bądź mieli) styczność z urządzeniami Cisco, zapewne kojarzą interfejs typu *loopback*. Jest to wirtualny interfejs, który najczęściej stosuje się do diagnostyki oraz testów. W przypadku urządzeń MikroTik do utworzenia tego typu interfejsu można wykorzystać bridge'a. Wystarczy go utworzyć i przypisać do niego adres IP — rysunek 1.2.

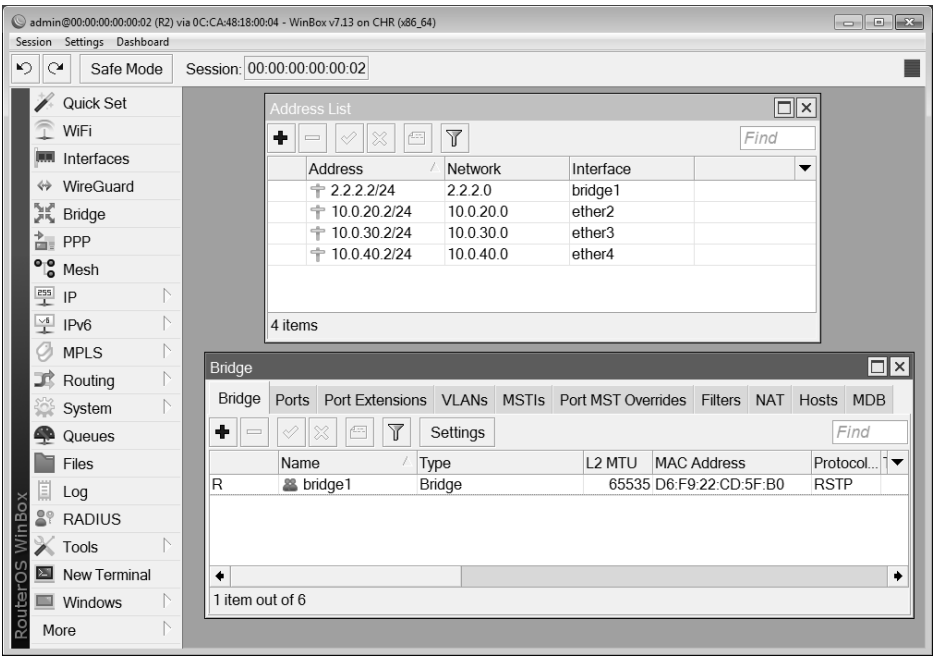


RYSUNEK 1.2. Konfiguracja routera R1, utworzenie bridge'a na potrzeby interfejsu loopback

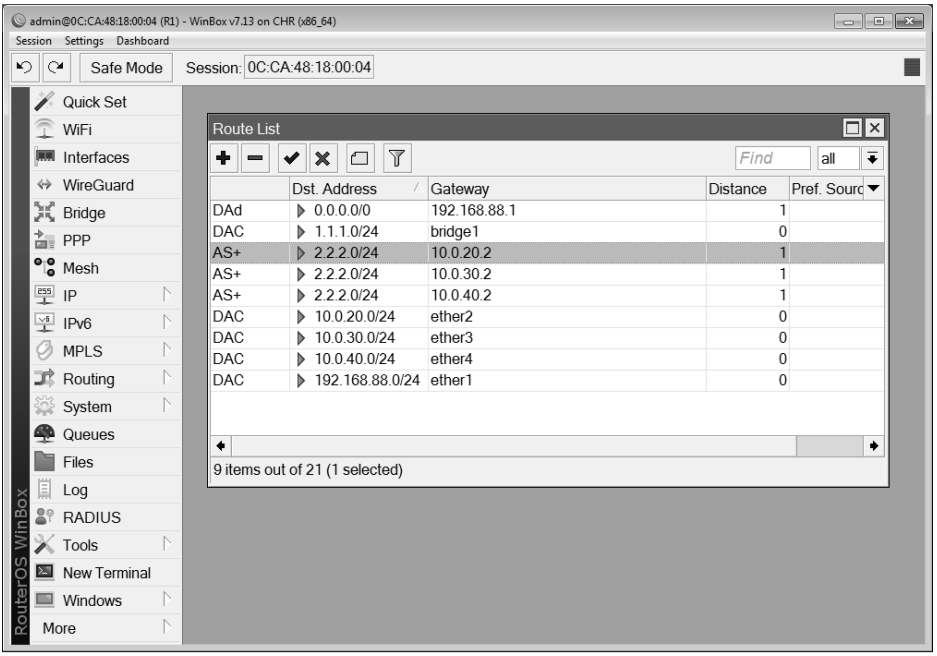
Konfiguracja routera *R2* jest pokazana na rysunku 1.3. Podobnie jak router *R1*, ma on trzy aktywne połączenia oraz interfejs *bridge* (IP *2.2.2.2/24*).

Aby możliwa była komunikacja pomiędzy sieciami *1.1.1.0/24* i *2.2.2.0/24* należy skonfigurować trasy statyczne. Na routerze *R1* zostały utworzone trzy trasy prowadzące do sieci *2.2.2.0/24* (poprzez interfejsy: *ether2*, *ether3* oraz *ether4*) — rysunek 1.4.

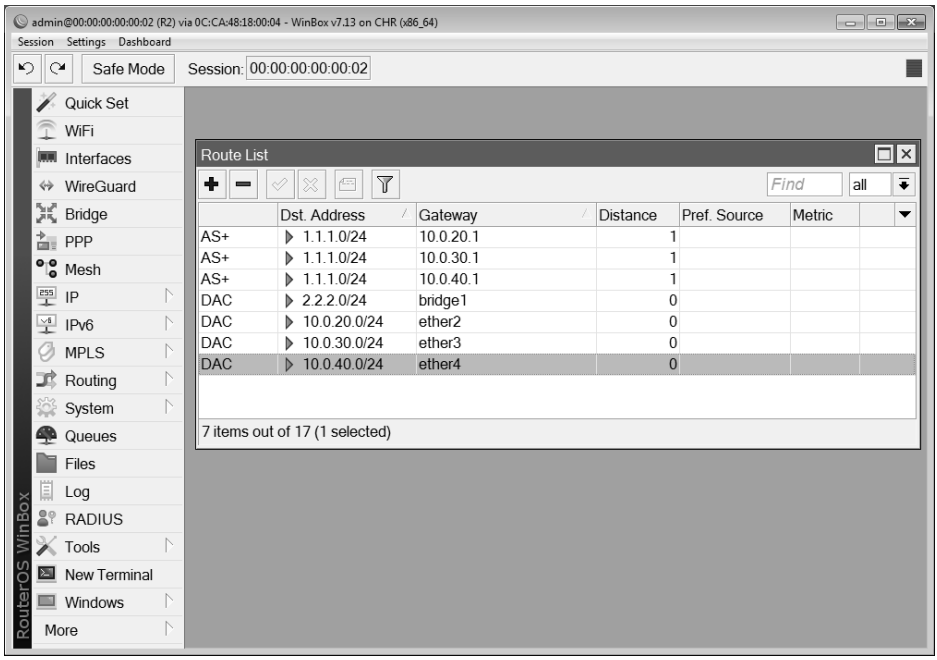
Trasy należy również utworzyć na routerze *R2*. W tablicy routingu znajdują się trzy trasy, prowadzące do sieci *1.1.1.0/24* — rysunek 1.5.



RYSUNEK 1.3. Konfiguracja routera R2



RYSUNEK 1.4. Router R1, konfiguracja tras statycznych



RYSUNEK 1.5. Router R2, konfiguracja tras statycznych

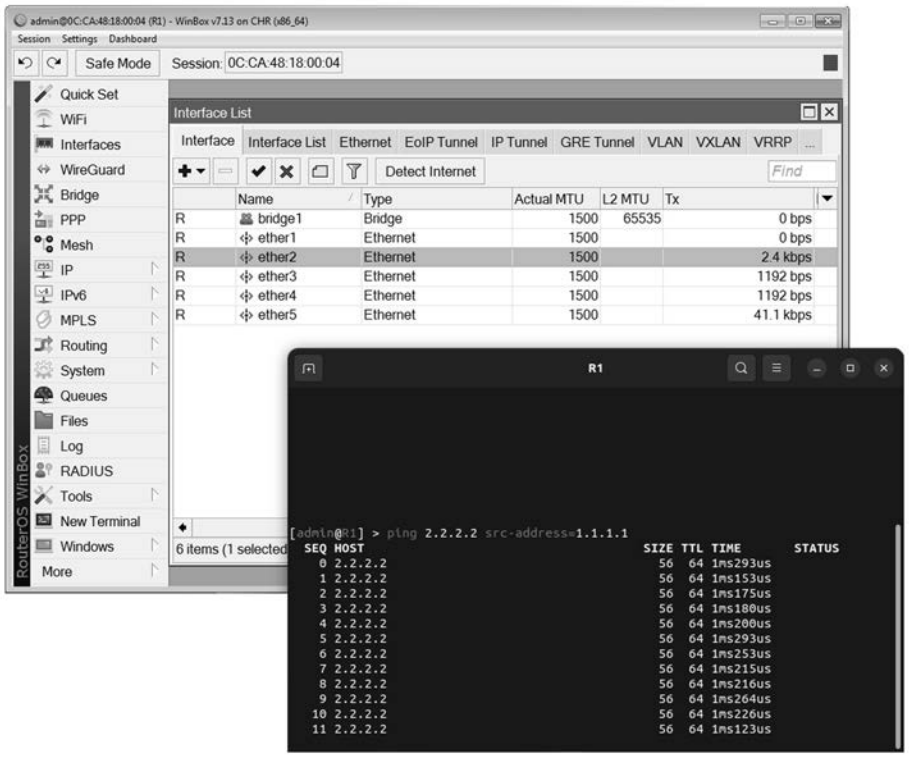
Podczas tworzenia tras z pewnością zauważyłeś, że router w miarę ich dodawania nie wyłącza ani nie zastępuje tras już istniejących. Oznacza to, że wszystkie trzy mają status aktywnych, o czym informuje duża litera *A* (od *active*) w polu statusu trasy. Dodatkowo przy każdej z nich znajduje się znak plusa (*+*), który oznacza włączony mechanizm ECMP (ang. *Equal Cost Multi-Path*). **ECMP pozwala przekazywać pakiety z tym samym docelowym i źródłowym adresem IP różnymi trasami.** Ponieważ koszt dotarcia do sieci dla wszystkich tras jest jednakowy, router będzie równoważył ruch sieciowy (ang. *load balancing*) przez podzielenie go na dostępne ścieżki. Po uruchomieniu testu poleceniem `ping 2.2.2.2 src-address=1.1.1.1` w oknie *Interface List* można śledzić, który interfejs jest obecnie w użyciu — rysunek 1.6.

Do tego celu można również wykorzystać narzędzie *Torch* — rysunek 1.7.

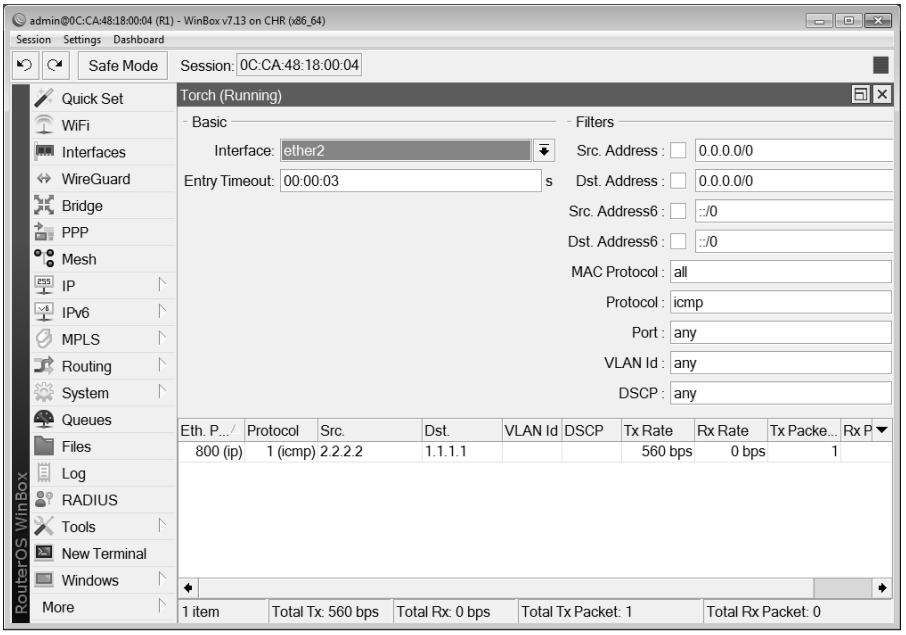
Taka nadmiarowość tras ma na celu zapewnienie ciągłości połączenia w razie wystąpienia awarii. Sprawdźmy zatem, co się stanie, gdy do niej dojdzie. Zasymulujmy ją i wyłączmy dwa spośród trzech połączeń — interfejs *ether3* oraz *ether4* na routerze *R1* zostają wyłączone.

Po wyłączeniu interfejsów wyłączone zostają dwie trasy. Ich status to: *unreachable* oraz *inactive* (litery *U* oraz *I* w polu statusu). Nadal aktywna jest ta wykorzystująca interfejs *ether2* (*2.2.2.0/24* via *10.0.20.2*) — rysunek 1.8.

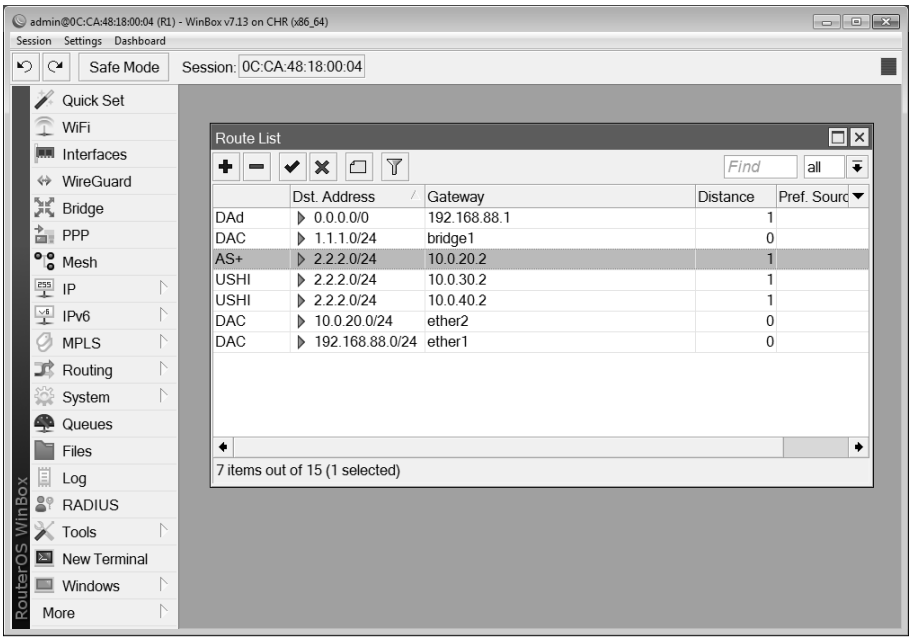
Komunikacja pomiędzy sieciami (pomimo jednej aktywnej trasy) w tym momencie nie jest możliwa. Test ping kończy się niepowodzeniem — rysunek 1.9.



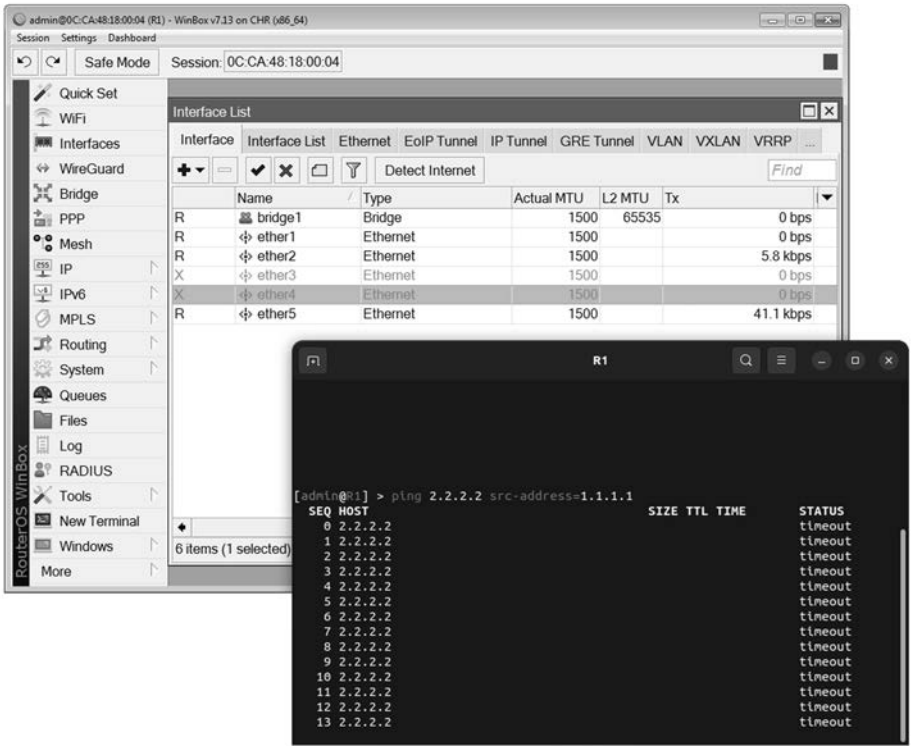
RYSUNEK 1.6. Router R1, test ping



RYSUNEK 1.7. Router R1, użycie narzędzia Torch

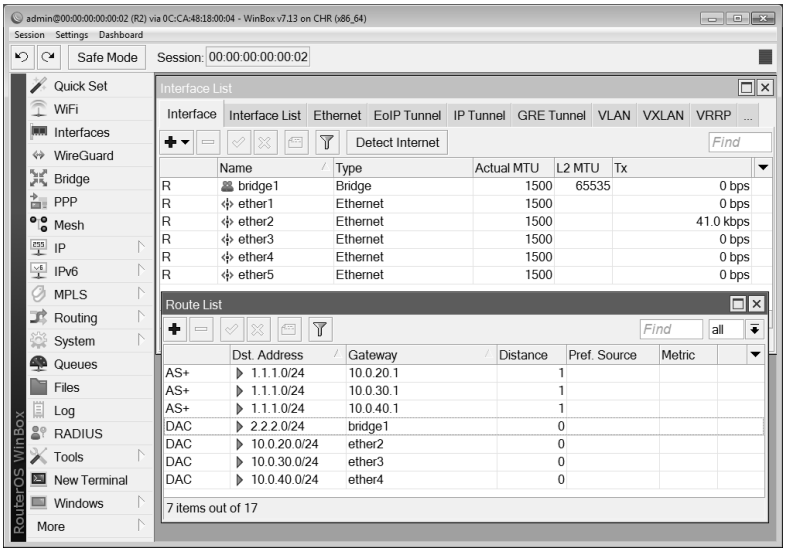


RYSUNEK 1.8. Router R1, status tras prowadzących do sieci 2.2.2.0/24



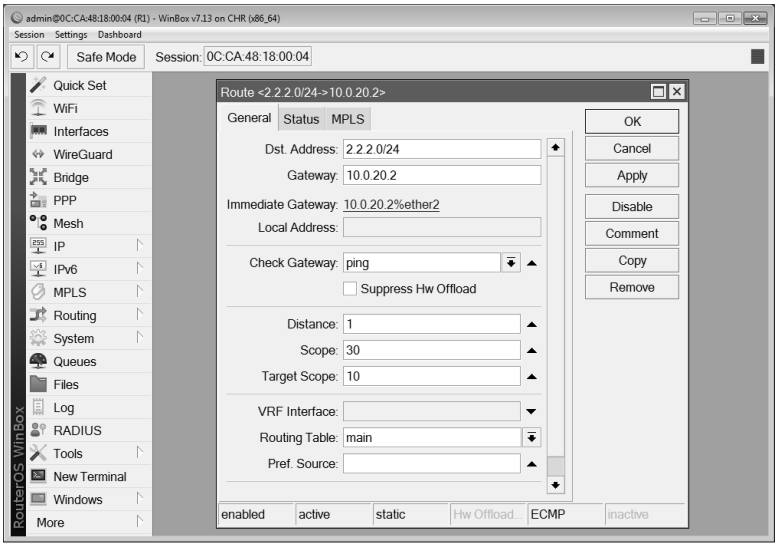
RYSUNEK 1.9. Router R1, test ping

Winnym sytuacji jest router *R2*, gdyż w jego tablicy routingu nadal znajdują się trasy wykorzystujące interfejsy *ether3* oraz *ether4*. Router *R2* nie wie, że oba interfejsy zostały wyłączone, i nadal wykorzystuje skojarzone z nimi trasy — rysunek 1.10.



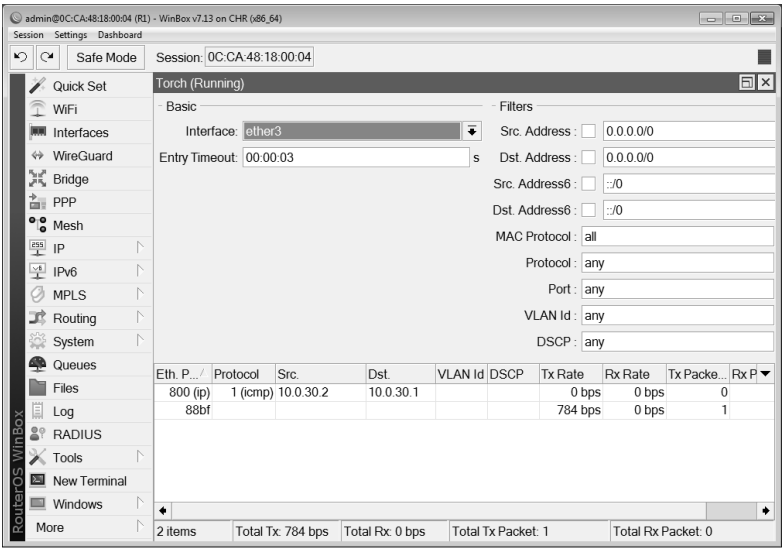
RYSUNEK 1.10. Router R2, status tras prowadzących do sieci 1.112.0/24

Aby uniknąć tego typu zdarzenia, należy wykorzystać ustawienie *Check Gateway*, które znajduje się w oknie konfiguracji trasy. Wybranie opcji *arp* (użycie komunikatu *ARP request*) lub *ping* (wykorzystanie komunikatu *ICMP echo request*) spowoduje włączenie testu dostępności bramy. **Router co 10 sekund wykorzysta wybrany protokół, aby zweryfikować, czy adres IP następnego skoku jest aktywny.** Zakończenie testu niepowodzeniem spowoduje wyłączenie trasy — rysunek 1.11.



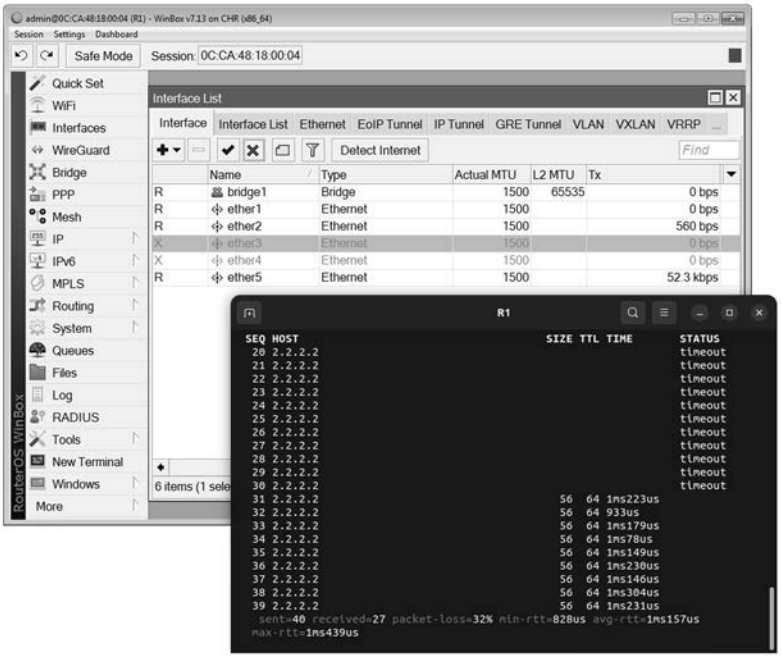
RYSUNEK 1.11. Ustawienie Check Gateway

Po włączeniu ustawienia router okresowo będzie wykonywał test. Można go śledzić za pomocą narzędzia *Torch* — rysunek 1.12.



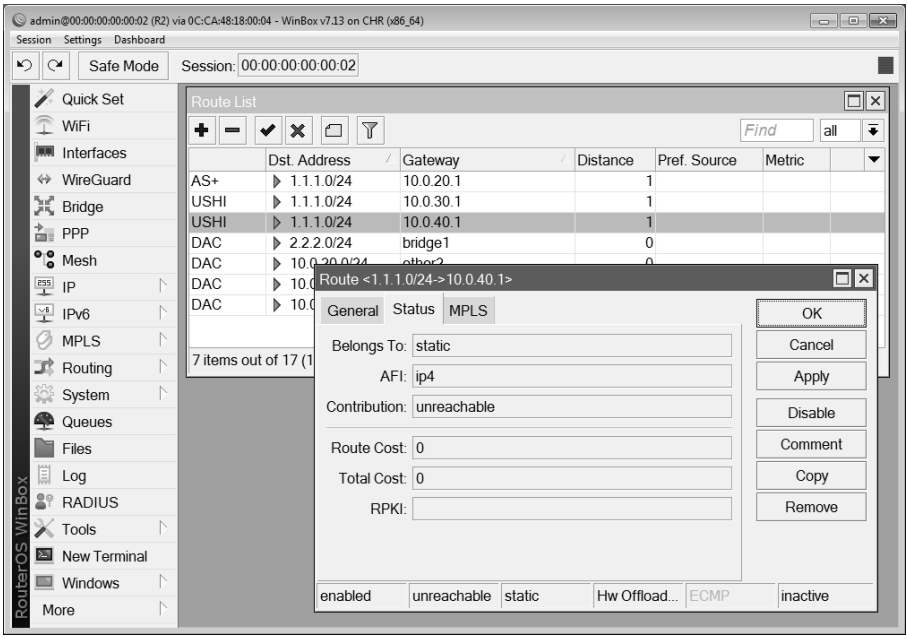
RYSUNEK 1.12. Router R1, test dostępności bramy IP 10.0.30.1, interfejs ether3

Po korekcie ustawień wszystkich sześciu tras ponownie zostaje zasymulowana awaria. Po chwilowej przerwie w komunikacji łączność zostaje wznowiona — rysunek 1.13.



RYSUNEK 1.13. Router R1, test działania funkcji testu bramy

Router *R2* oznacza trasy wykorzystujące interfejsy *ether3* (router *R1*, IP *10.0.30.1*) oraz *ether4* (router R1, *IP 10.0.40.1*) jako nieosiągalne. Test bramy kończy się niepowodzeniem — rysunek 1.14.



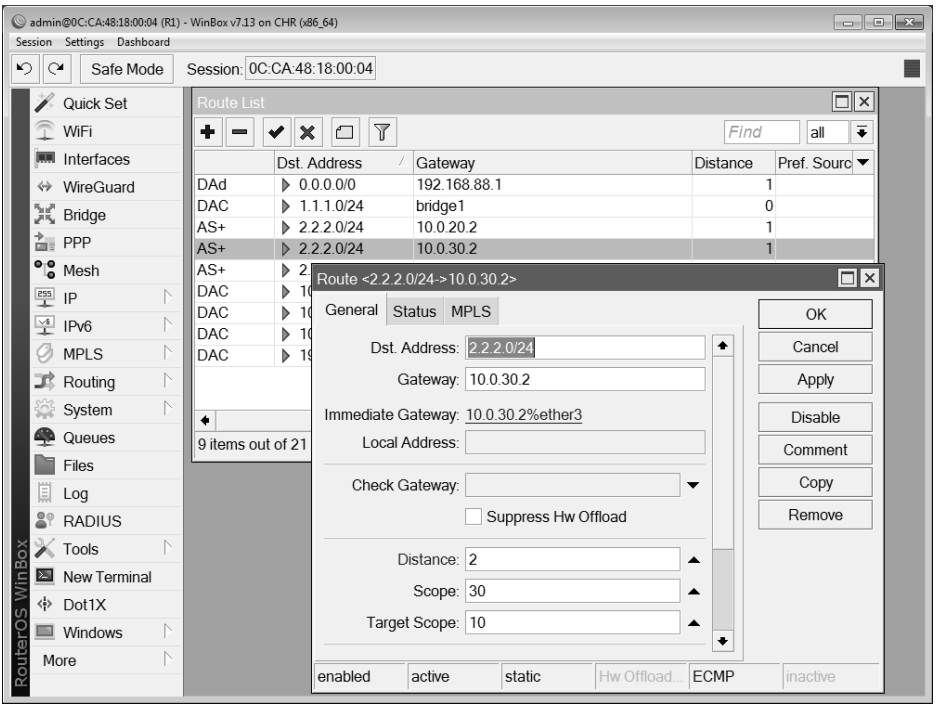
RYSUNEK 1.14. Router R2, wyłączenie tras routingu

Użycie polecenia `ip route set check-gateway=<sposób_sprawdzenia> numbers=<numer_trasy>`, np. `ip route set check-gateway=arp numbers=0`, uruchomi test bramy.

1.2. Dystans administracyjny

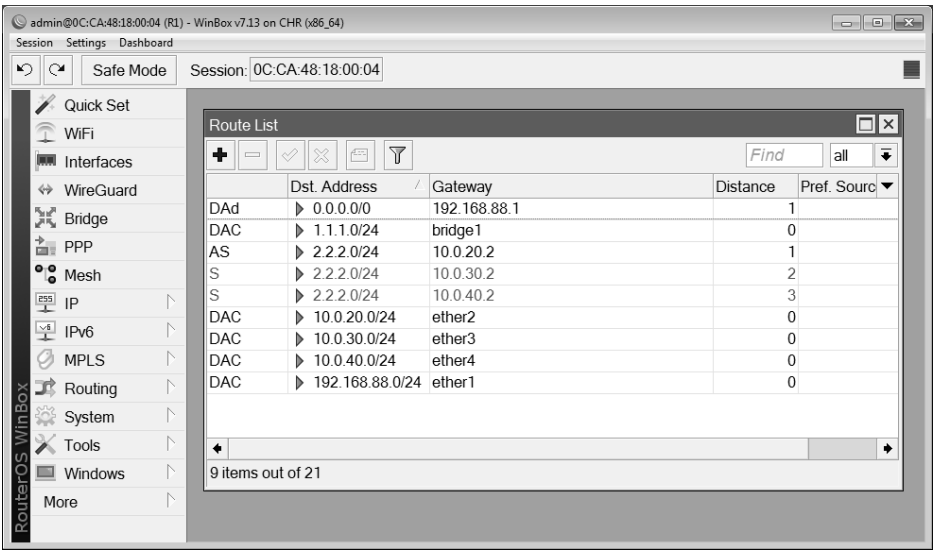
Zdarzają się sytuacje, w których nie chcemy, aby ruch sieciowy był jednocześnie przekazywany poprzez różne interfejsy routera. Chcemy, aby pakiety podróżowały stale określoną trasą, a alternatywna była używana dopiero wtedy, gdy zawiedzie główna. Cel osiągniemy przez zmianę dystansu administracyjnego. Tu wybiegnę trochę do przodu, bo to zagadnienie dokładnie omawiam w następnym rozdziale, który dotyczy routingu dynamicznego. Teraz pokażę, jak zmienić wartość tego parametru, a jego obszerniejszy opis znajdziesz kilka stron dalej. Na tym etapie ważne jest, abyś wiedział, **że im dystans administracyjny niższy, tym trasa ważniejsza**. Przez zmianę domyślnej wartości dystansu administracyjnego (wynosi ona 1) wskażemy trasę, której ma użyć router.

Router *R1* zna trzy równorzędne trasy prowadzące do sieci *2.2.2.0/24* i każdą z nich wykorzystuje. Aby to zmienić, należy wyświetlić opcje trasy i zmodyfikować wartość umieszczoną w polu *Distance*. Domyślna wartość dystansu administracyjnego dla trasy wykorzystującej interfejs *ether3* i adres IP bramy *10.0.30.2* została zmieniona na *2* — rysunek 1.15.



RYSUNEK 1.15. Router R1, zmiana wartości dystansu administracyjnego dla trasy wykorzystującej interfejs ether3

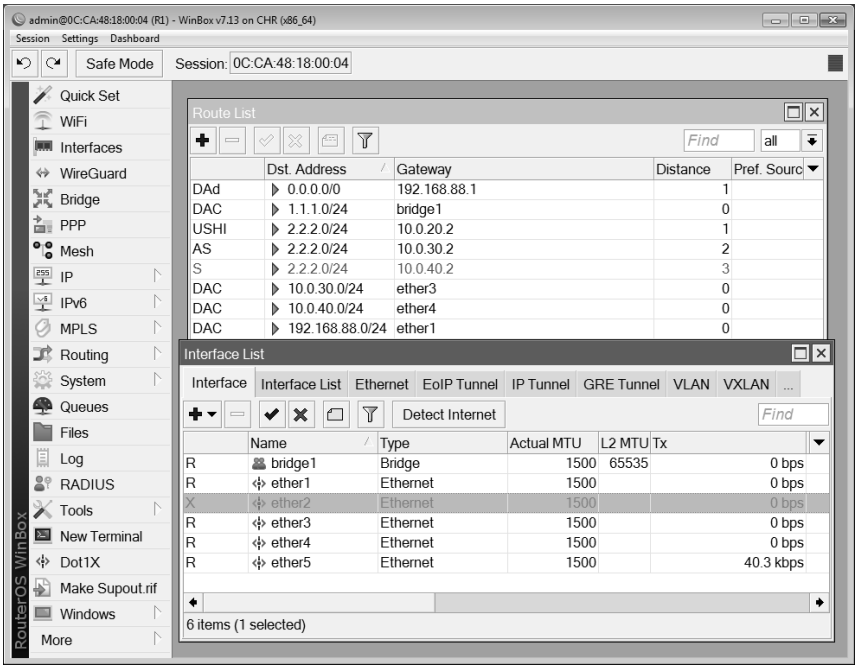
Dystans administracyjny został również zmieniony dla trasy skojarzonej z interfejsem *ether4* (adres IP bramy *10.0.40.2*) i wynosi on *3* — rysunek 1.16.



RYSUNEK 1.16. Router R1, zmiana wartości dystansu administracyjnego dla trasy wykorzystującej interfejs ether4

Przeprowadzona konfiguracja sprawiła, że obie trasy „wypadają" z tablicy routingu routera, a ich status zostaje zmieniony na *static* (znika *active*). Ponieważ spośród trzech tras ta pierwsza ma najniższy dystans administracyjny (o domyślnej wartości wynoszącej 1), router jako tę preferowaną wybierze właśnie ją.

Kiedy router użyje pozostałych tras? Wtedy, gdy bieżącą ulegnie awarii. Po wyłączeniu interfejsu *ether2* wykorzystująca go trasa jest niedostępna. Router automatycznie zastępują ją tą, która ma przypisaną niższą wartość dystansu administracyjnego — zostaje użyta trasa prowadząca poprzez interfejs *ether3* — rysunek 1.17.



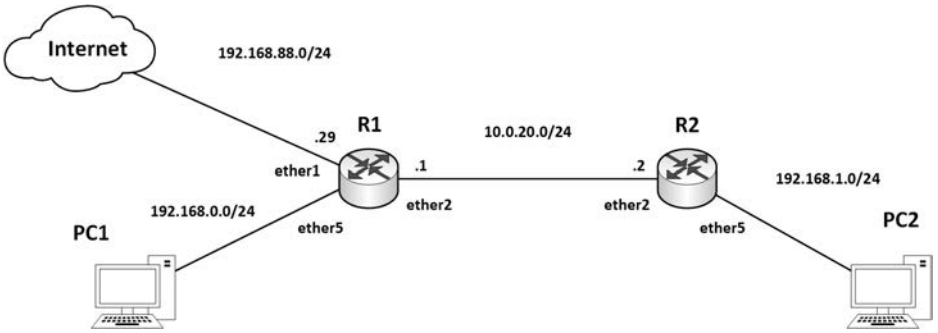
RYSUNEK 1.17. Router R1, wyłączenie interfejsu ether2

Z użyciem terminala wartość dystansu administracyjnego możemy ustalić na etapie tworzenia trasy (np. polecenie `ip route add disabled=no distance=4 dst-address=` `↪2.2.2.0/24 gateway=10.0.30.2` utworzy trasę do sieci *2.2.2.0/24* i ustali wartość dystansu na *4*) lub przez zmianę ustawień już istniejącej trasy (np. polecenie `ip route set distance=3 numbers=0` zmienia dystans administracyjny trasy o numerze *0* na *3*).

1.3. Zmiana wartości pola TTL

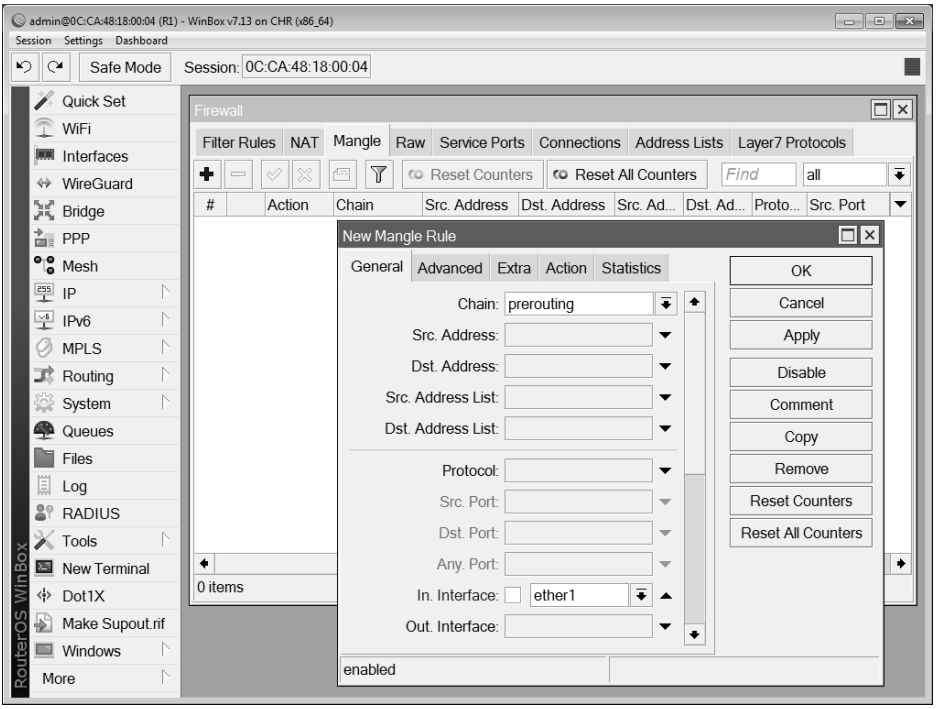
Pole TTL zarządza czasem życia pakietów. Oznacza to, że gdy router otrzyma pakiet, którego wartość pola TTL wynosi *1*, nie przekaże go dalej. Wartość pola TTL jest zmniejszana o jeden za każdym razem, gdy jest on przekazywany przez router. Zapobiega to sytuacji, w której pakiety byłyby przekazywane pomiędzy routerami w nieskończoność. Wartość *0* w polu TTL oznacza skasowanie pakietu.

System routera MikroTik pozwala na modyfikację pola TTL, dzięki czemu administrator może określić, jak „głęboko" pakiet może wniknąć do zarządzanej sieci (ile routerów może pokonać, zanim zostanie skasowany). W omówieniu tego zagadnienia pomoże topologia przedstawiona na rysunku 1.18. Sprawimy, że po zmianie wartości pola TTL router *R2* straci połączenie z siecią Internet.



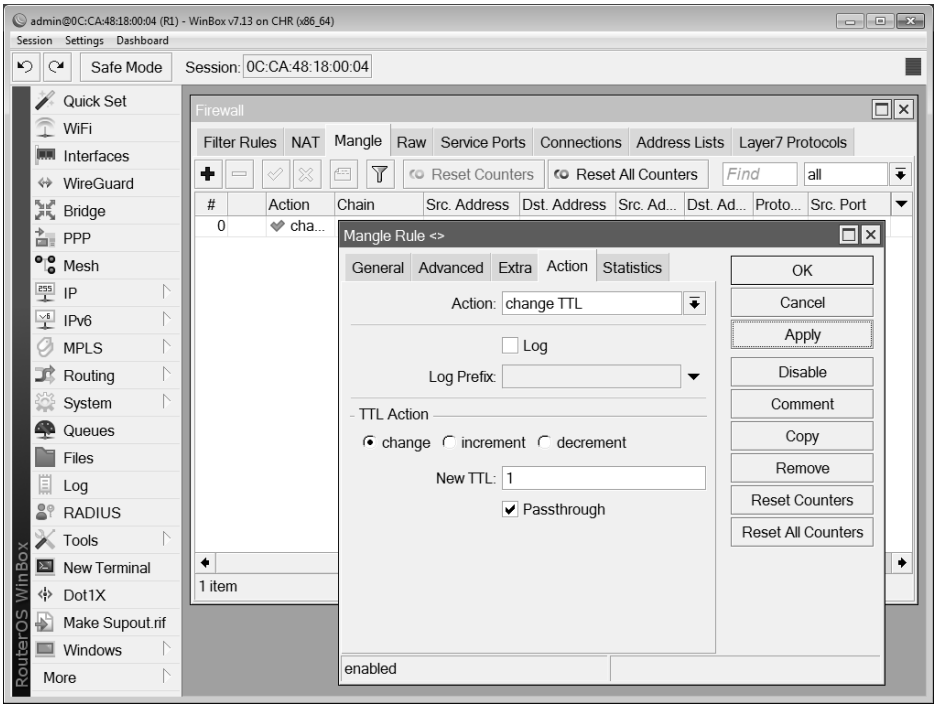
RYSUNEK 1.18. Topologia sieciowa

Zmianę wartości pola TTL wykonamy na routerze *R1*. Ustawienie zaszyte jest w opcjach firewalla. Po wyświetleniu okna ustawień należy przejść na zakładkę *Mangle* i wybrać ikonę plusa. W nowo otwartym oknie (karta *General*) w polu *Chain* należy wybrać opcję *prerouting*, a w polu *In. Interface* wskazać interfejs *ether1* — rysunek 1.19.



RYSUNEK 1.19. Router R1, zakładka General, zmiana wartości pola TTL

Następnie po wybraniu karty *Action* należy w polu *Action* odszukać opcję *change TTL*. W polu *New TTL* umieszczamy *1* — rysunek 1.20.



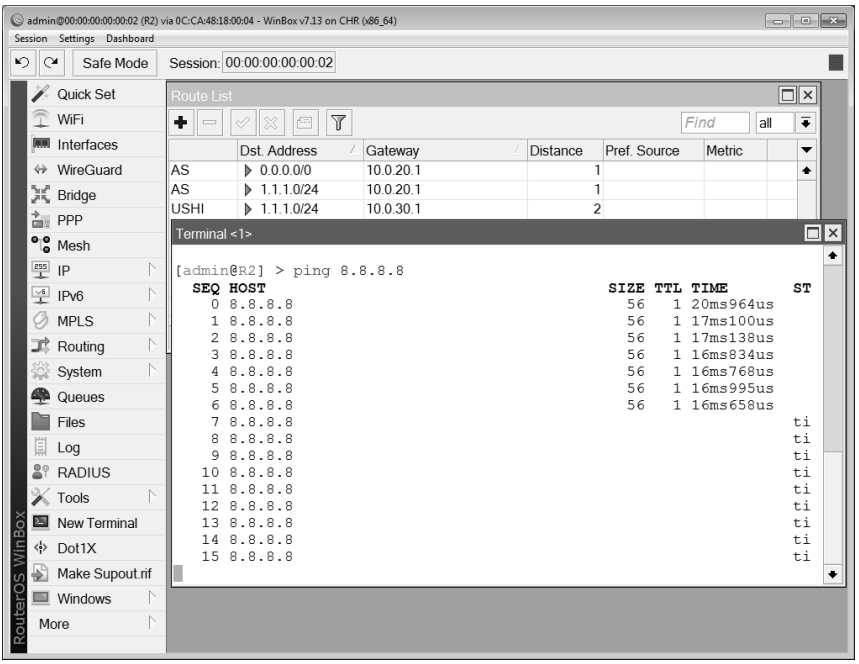
RYSUNEK 1.20. Router R1, karta Action, zmiana wartości pola TTL

Przeprowadzona konfiguracja sprawi, że gdy router *R1* otrzyma pakiet na interfejsie *ether1* (który ma połączenie z siecią Internet), zmodyfikuje wartość pola TTL na *1*. Zmiana ta następuje przed wykonaniem routowania, tak więc gdy przychodzi do podjęcia decyzji o przekazaniu pakietu dalej, jest on odrzucany, gdyż wartość pola TTL wynosi *1*. Dzięki temu zabiegowi router *R2* traci połączenie z siecią Internet — rysunek 1.21.

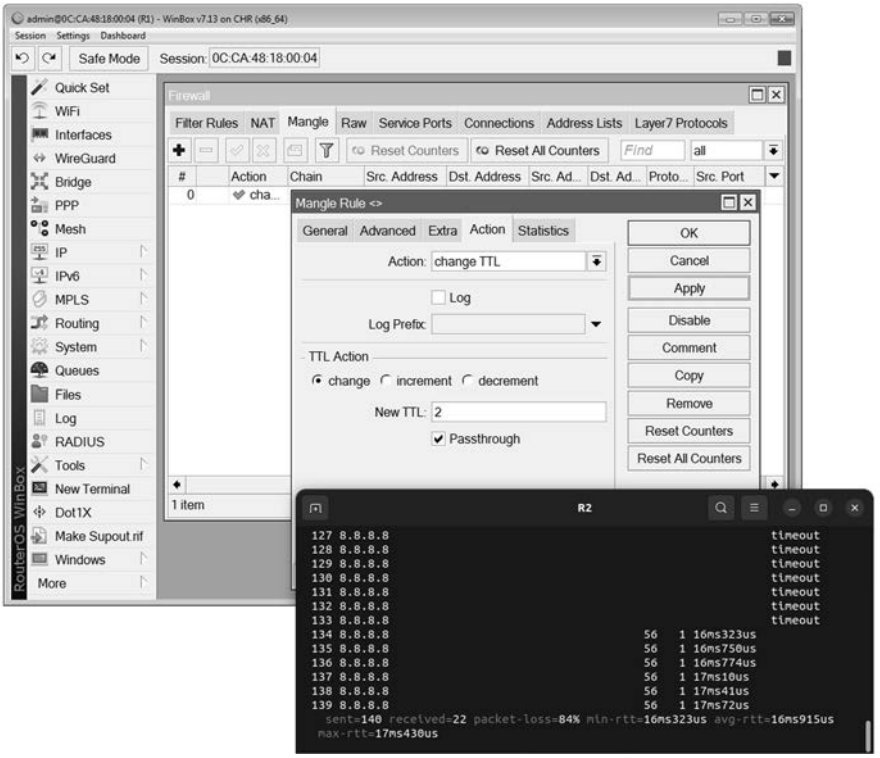
Gdy w polu *New TTL* umieścimy wartość *2*, router *R2* odzyska połączenie z siecią Internet — rysunek 1.22.

Zmianę wartości pola TTL można obserwować po przechwyceniu pakietów. Na rysunku jest pokazany pakiet będący odpowiedzią serwera na test ping. Miejscem przechwycenia pakietu jest interfejs *ether1* routera *R1*, a wartość ustawiona w polu *TTL* wynosi *120* — rysunek 1.23 (1).

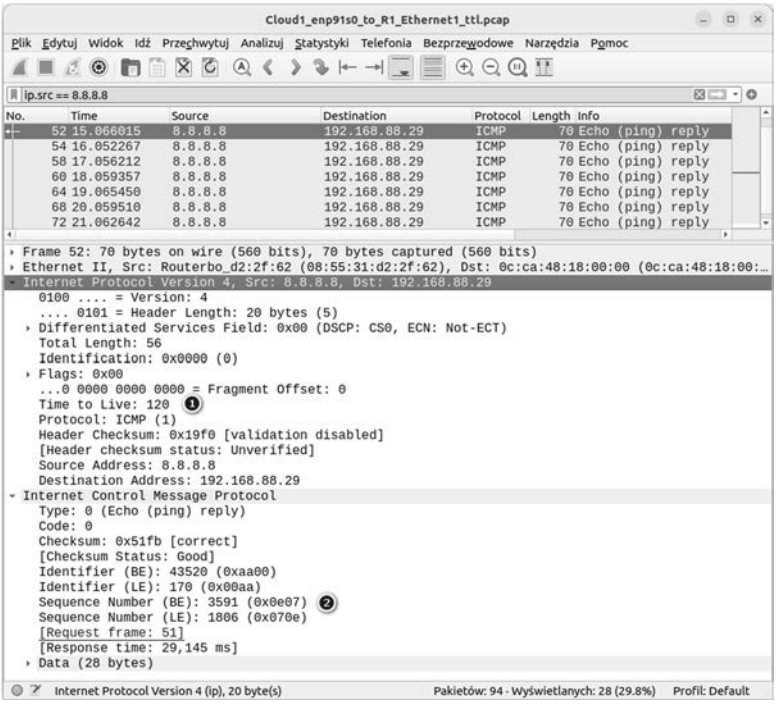
Gdyby zmiana wartości pola TTL nie została skonfigurowana w momencie przekazania pakietu przez router *R1*, jego wartość wyniosłaby *119*. Router *R1* modyfikuje wartość pola TTL pakietu na *2* i przekazuje go w kierunku routera *R2* (poprzez interfejs *ether2*), a nowa wartość pola TTL wynosi *1*. Oba pakiety (otrzymany i przesłany dalej) łączy wartość pola *Sequence Number* — rysunek 1.24 (2).



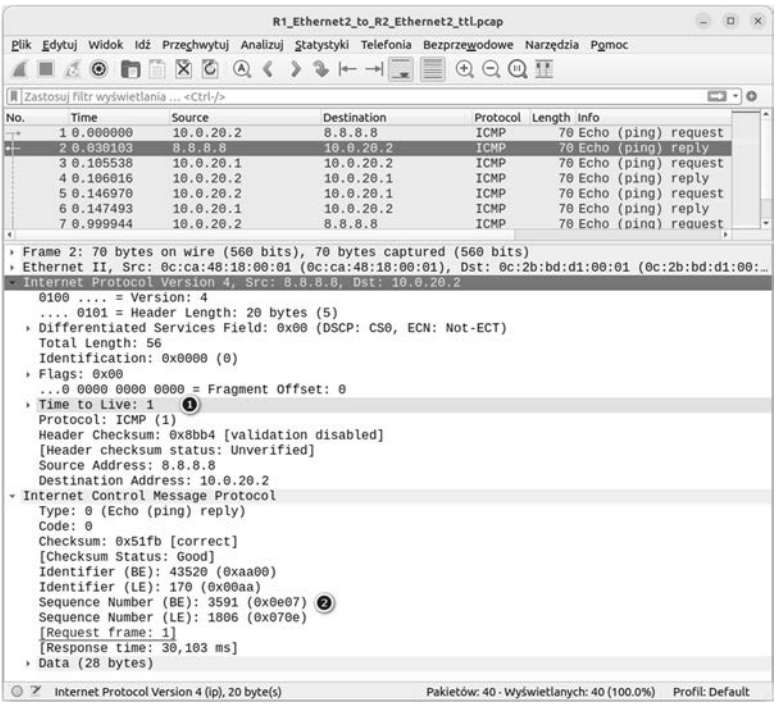
RYSUNEK 1.21. Router R2, brak połączenia z siecią Internet



RYSUNEK 1.22. Router R2, odzyskanie połączenia z siecią Internet

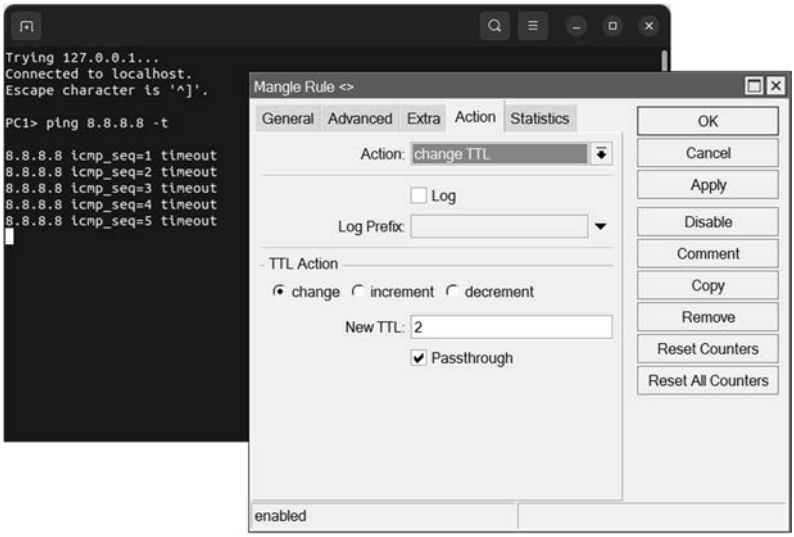


RYSUNEK 1.23. Router R1, interfejs ether1, przechwycony pakiet ICMP



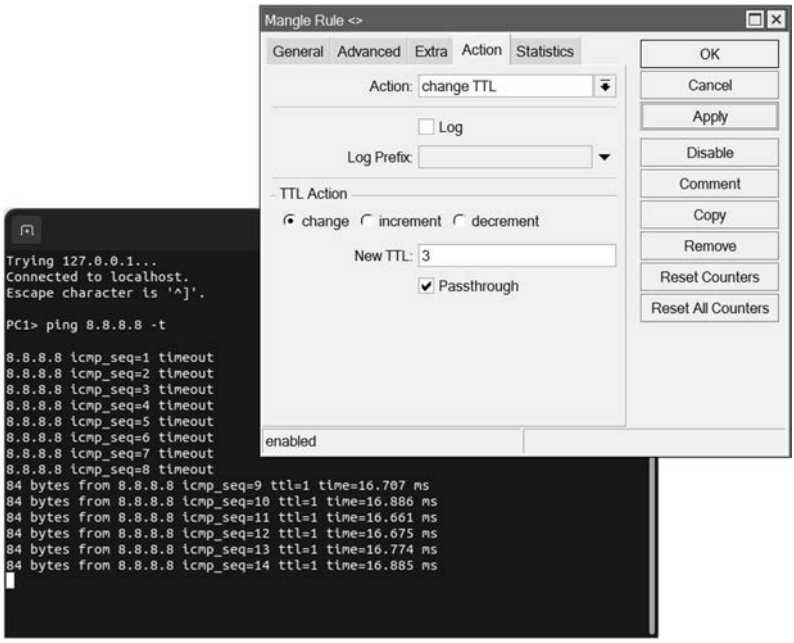
RYSUNEK 1.24. Router R1, interfejs ether2, przechwycony pakiet ICMP

Wartość pola *New TTL*, która wynosi *2*, jest niewystarczająca, aby komputer *PC2* mógł połączyć się z siecią Internet — router *R1* wartość pola *TTL* zmniejsza z *2* na *1*, a to za mało, aby router *R2* mógł pakiet przekazać dalej — rysunek 1.25.



RYSUNEK 1.25. Modyfikacja pola TTL, komputer PC2 nie ma dostępu do sieci Internet

Aby komputer *PC2* mógł połączyć się z serwerami internetowymi, minimalna wartość pola *New TTL* musi wynosić *3*. Po korekcie ustawień komunikacja jest możliwa — rysunek 1.26.



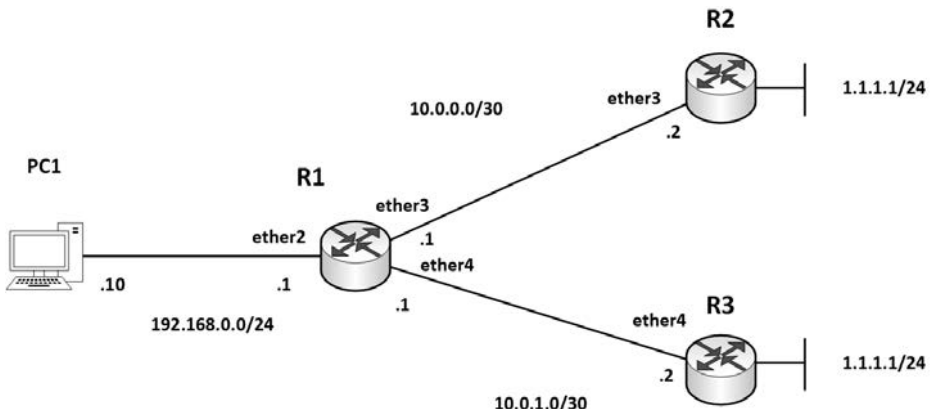
RYSUNEK 1.26. Modyfikacja pola TTL, komputer PC2 uzyskuje połączenie z siecią Internet

Zmianę wartości pola TTL można również wykonać z poziomu terminala. Pozwala na to polecenie `ip firewall mangle add action=change-ttl chain=prerouting in-interface=<identyfikator_interfejsu> new-ttl=set:<nowa_wartość> passthrough=yes`, np. `ip firewall mangle add action=change-ttl chain=prerouting in-interface=ether1 new-ttl=set:2 passthrough=yes`.

Pokazane ustawienia chronią sieć przed nieautoryzowanym routerem, który udostępniałby połączenie internetowe podłączonym do niego hostom. Gdy komputer *PC2* zastąpimy routerem, ten z siecią Internet będzie mógł się komunikować, ale podłączone do niego urządzenia już nie — podstawiony router otrzyma pakiety, których wartość pola *TTL* wynosi *1*.

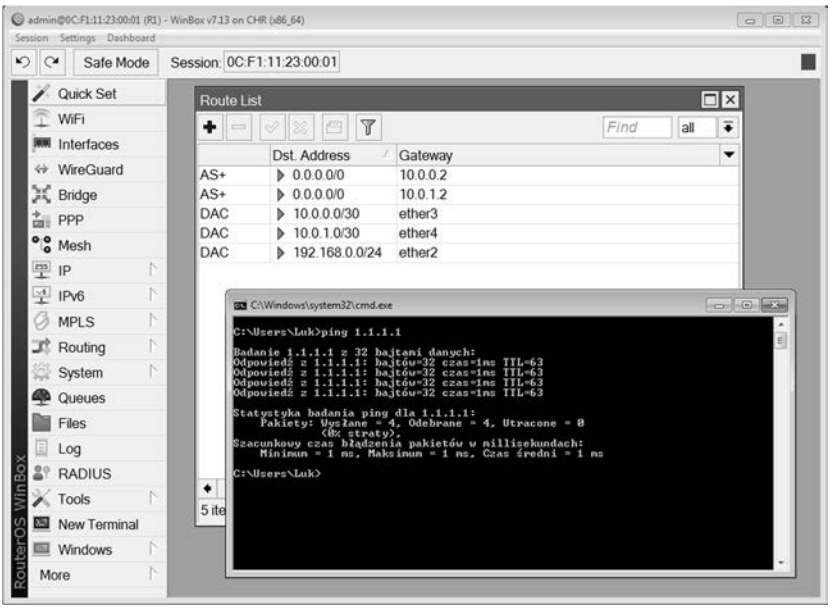
1.4. Strategie routingu

Prędzej czy później staniesz przed wyzwaniem przekierowania określonego ruchu sieciowego. Spójrz na rysunek 1.27 i wyobraź sobie następującą sytuację. Routery *R2* oraz *R3* są urządzeniami należącymi do różnych ISP i oba łączą Twoją sieć z siecią Internet. Naszym zadaniem jest przekierowanie ruchu sieciowego tak, aby jego część została wysłana za pośrednictwem routera *R2*, pozostała zaś z użyciem routera *R3*. Zasymulujemy sytuację przekazania ruchu ICMP (charakter tego ruchu oczywiście może być dowolny, kryteria dopasowania ustalasz Ty), pakiety protokołu zostaną przekazane routerowi *R2*, a wszystkie pozostałe docelową sieć *1.1.1.0/24* osiągną za pośrednictwem routera *R3* — rysunek 1.27.



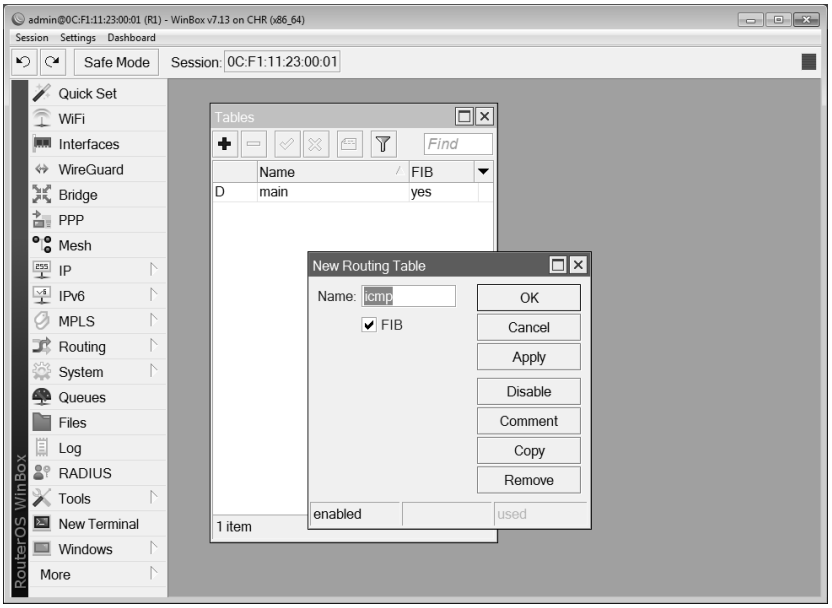
RYSUNEK 1.27. Topologia sieciowa

Sieć *1.1.1.0/24* jest osiągalna poprzez router *R2*, jak i *R3* — w tablicy routingu routera *R1* znajdują się dwie trasy domyślne, powiązane z oboma routerami. Ponieważ koszt dotarcia do sieci w przypadku obu tras jest jednakowy, router *R1* wykorzystuje *ECMP* — rysunek 1.28.



RYSUNEK 1.28. Tablica routingu routera R1

Konfigurację przekierowania ruchu ICMP (przez interfejs *ether3*) należy rozpocząć od utworzenia nowej tablicy routingu, która będzie przechować trasę skojarzoną z przekierowywanym ruchem sieciowym. Tablicę utworzymy po wywołaniu okna *Tables* — z menu po lewej należy wybrać *Routing*, a następnie *Table*. Klikamy ikonę plusa i w polu *Name* wpisujemy nazwę tworzonej tablicy (tablicę nazwano *icmp*), a następnie zaznaczamy pole *FIB* — rysunek 1.29.

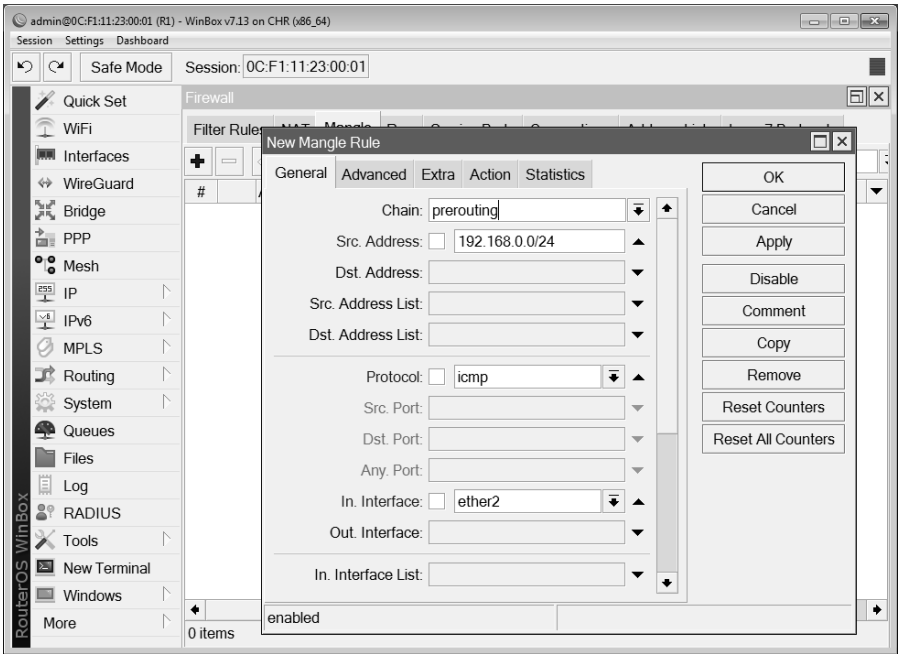


RYSUNEK 1.29. Router R1, utworzenie nowej tablicy routingu

FIB (ang. *Forwarding Information Base*) zawiera kopię informacji, które są niezbędne to tego, aby router mógł przekazać pakiety. Domyślnie (gdy nie jest stosowane oznaczanie ruchu sieciowego) wszystkie aktywne trasy znajdują się w tabeli głównej (*main*) i to ona decyduje o drodze, którą zostanie przesłany pakiet. Po oznaczeniu pakietów o miejscu ich przeznaczenia decyduje *FIB*. Do tego celu wykorzystuje on: adres źródłowy, adres docelowy, interfejs i oznaczenie pakietów.

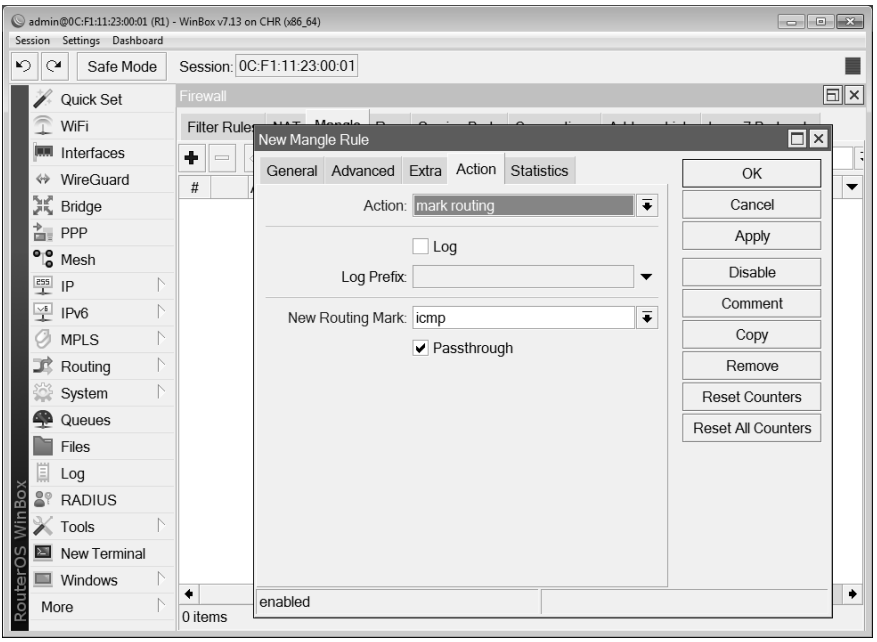
Kolejnym krokiem jest oznaczenie ruchu sieciowego, który ma zostać przez router przekierowany. Kryterium oznaczenia określa się na zakładce *Mangle*, znajdującej się w ustawieniach zapory sieciowej (*Firewall*). Po kliknięciu ikony plusa w oknie *New Mangle Rule* (karta *General*) określa się kryteria dopasowania. Ponieważ ma zostać przekierowany ruch *ICMP* pochodzący z sieci *192.168.0.0/24*, na karcie skonfigurowano następujące pola (rysunek 1.30):

- *Chain* — ruch sieciowy, który trafia do routera przed podjęciem decyzji o routowaniu (wybrano *prerouting*),
- *Src. Address* — określa adres źródłowy przekierowywanych pakietów (wpisano *192.168.0.0/24*),
- *Protocol* — protokół, którego dotyczy przekierowanie (wybrano *ICMP*),
- *In. Interface* — interfejs, na którym ma zostać zarejestrowany pakiet (wybrano *ether2*).



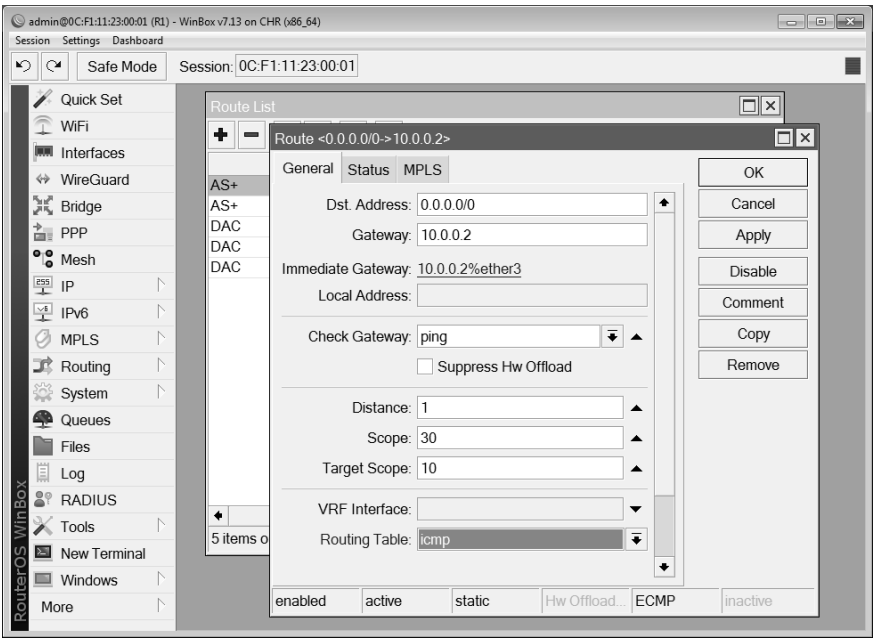
RYSUNEK 1.30. Router R1, zakładka General, oznaczenie ruchu sieciowego

Po określeniu cech pakietu należy na karcie *Action* w polu *Action* wskazać czynność, jaka ma zostać wykonana — z dostępnych opcji wybieramy *mark routing*. Pole *New Routing Mark* określa nazwę tablicy routingu (wybrano *icmp*) zawierającej trasę, której router ma użyć, aby przesłać oznaczony ruch sieciowy — rysunek 1.31.



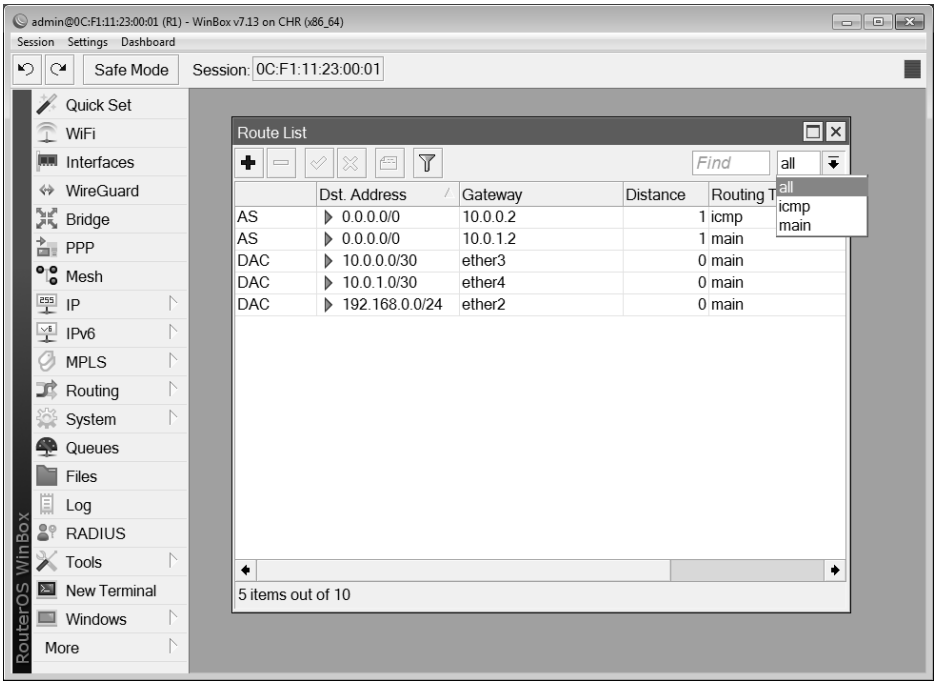
RYSUNEK 1.31. Router R1, karta Action, oznaczenie ruchu sieciowego

Ostatnią czynnością jest powiązanie trasy z tablicą routingu. Ponieważ ruch ICMP ma zostać przekazany w kierunku routera *R2* (poprzez interfejs *ether3*), należy we właściwościach trasy domyślnej zastąpić w polu *Routing Table* domyślną wartość *main* wartością *icmp* — rysunek 1.32.



RYSUNEK 1.32. Router R1, zmiana tablicy routingu

Wykonana zmiana ma odzwierciedlenie w oknie routingu — trasa *0.0.0.0/0* via *10.0.0.2* znajduje się w tablicy *icmp*. Zauważ, że przestał działać mechanizm *ECMP* (brak znaku *+* w polu statusu trasy) — trasy domyślne znajdują się w oddzielnych tablicach. Rozwinąwszy pole znajdujące się w prawym górnym rogu okna, można filtrować trasy zależnie od ich przynależności do określonych tablic — rysunek 1.33.



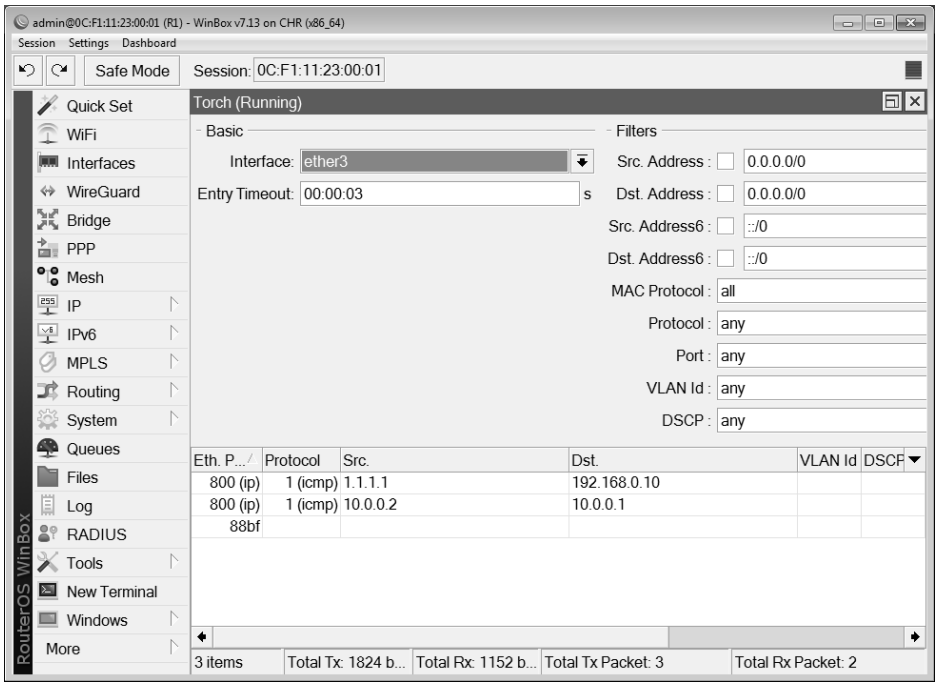
RYSUNEK 1.33. Router R1, tablica routingu

Ostatnią czynnością jest weryfikacja przeprowadzonych ustawień. Na komputerze *PC1* poleceniem `ping 1.1.1.1 -t` zostaje uruchomiony test ping. Narzędzie *Torch* na interfejsie *ether3* rejestruje ruch ICMP dotyczący skanowanego adresu IP — rysunek 1.34.

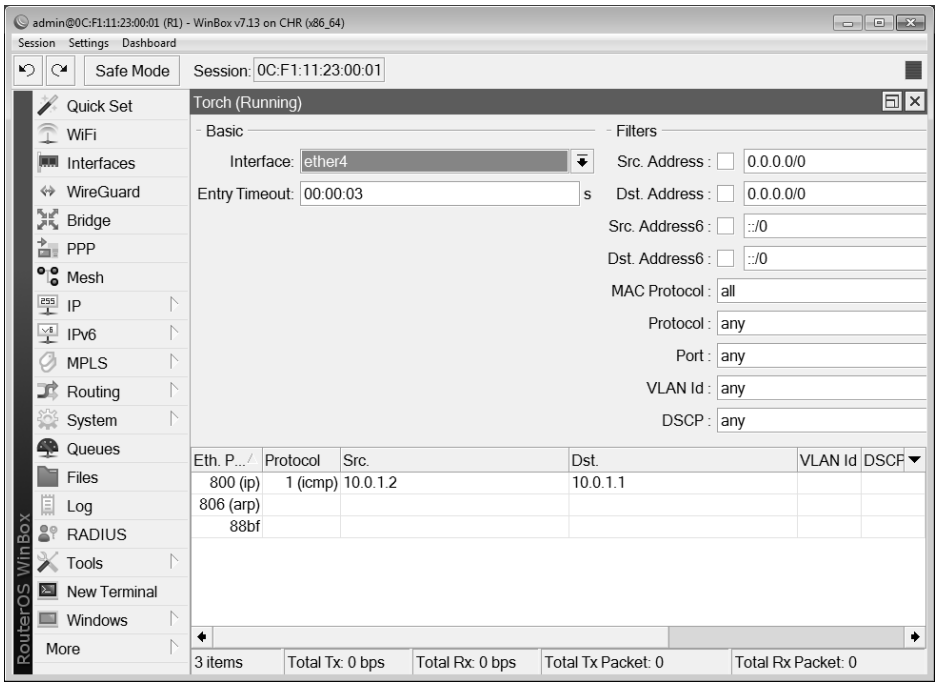
Uruchomione narzędzie *Torch* na interfejsie *ether4* również rejestruje ruch ICMP, ale pojawiające się pakiety to efekt włączenia funkcji sprawdzenia dostępności bramy (funkcję tę konfigurowaliśmy w podrozdziale 1.1) — rysunek 1.35.

Zachowanie routera jeszcze lepiej widać, gdy na obu interfejsach routera *R1* zostaną przechwycone pakiety. Mamy pewność, że jedynie interfejs *ether3* jest wykorzystywany do przekazania oznaczonych pakietów — rysunek 1.36.

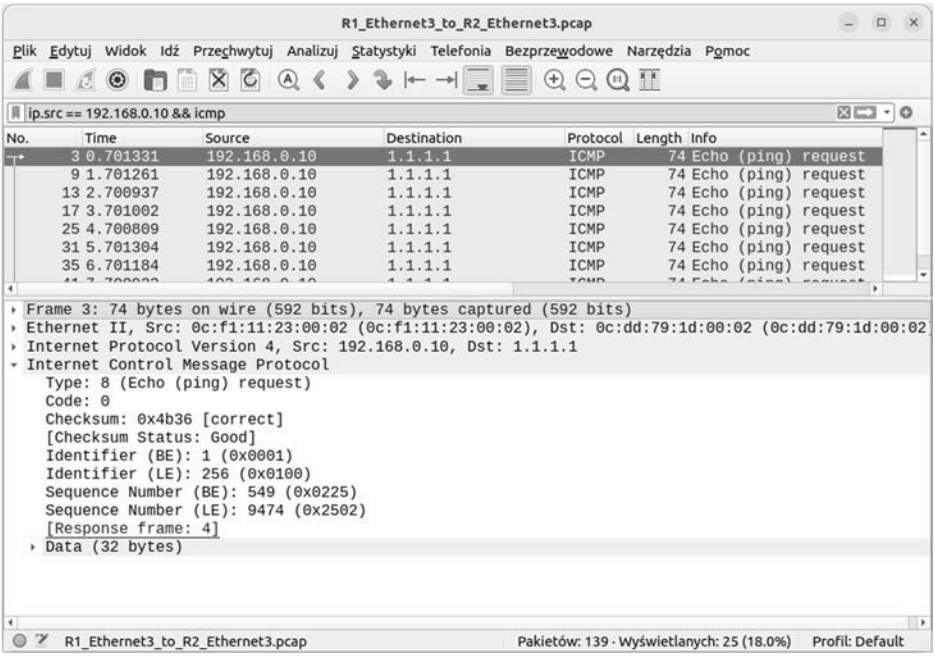
Interfejs *ether4* jest z tego procesu całkowicie wyłączony. Podobnie jak po użyciu narzędzia *Torch*, można zaobserwować jedynie ruch ICMP, który jest wynikiem włączenia funkcji sprawdzania bramy — rysunek 1.37.



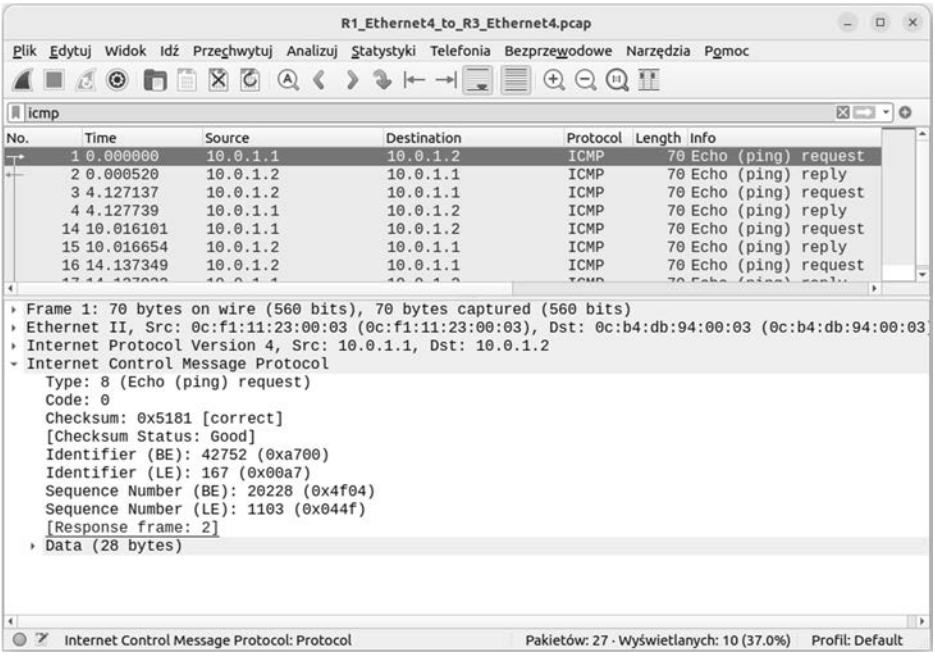
RYSUNEK 1.34. Router R1, interfejs ether3, rejestrowanie ruchu sieciowego



RYSUNEK 1.35. Router R1, interfejs ether4, rejestrowanie ruchu sieciowego



RYSUNEK 1.36. Router R1, interfejs ether3, przechwycony ruch sieciowy



RYSUNEK 1.37. Router R1, interfejs ether4, przechwycony ruch sieciowy

Całość pokazanych ustawień można wykonać za pomocą terminala:

- utworzenie nowej tablicy routingu — `routing table add disabled=no fib name=<nazwa_tablicy>`, np. `routing table add disabled=no fib name=icmp`,
- oznaczenie ruchu sieciowego — `ip firewall mangle add action=mark-routing chain=prerouting in-interface=<identyfikator_interfejsu> new-routing-mark=<nazwa_oznaczenia> passthrough=yes protocol=<protokół> src-address=<adres_źródłowy_sieci>`, np. `ip firewall mangle add action=mark-routing chain=prerouting in-interface=ether2 new-routing-mark=icmp passthrough=yes protocol=icmp src-address=192.168.0.0/24`,
- utworzenie trasy domyślnej — `ip route add check-gateway=ping disabled=no dst-address=0.0.0.0/0 gateway=<adres_bramy> routing-table=<tablica_routingu>`, np. `ip route add check-gateway=ping disabled=no dst-address=0.0.0.0/0 gateway=10.0.0.2 routing-table=icmp`.

Skorowidz

U

V

W

Z

KONFIGURACJA USŁUG SIECIOWYCH NA URZĄDZENIACH MIKROTIK

Poziom zaawansowany

Urządzenia MikroTik w sieciach firmowych

Skoro sięgasz po tę książkę, nazwa MikroTik jest Ci pewnie dobrze znana – być może z pierwszego poradnika Łukasza Guziaka *Konfiguracja usług sieciowych na urządzeniach MikroTik*. Tamta pozycja miała za zadanie wprowadzić Cię do świata urządzeń sieciowych stanowiących realną alternatywę dla sprzętu marki Cisco. Ta pozwala pogłębić wiedzę i poznać kolejne technologie, które przydadzą Ci się w trakcie pracy ze sprzętem łotewskiego producenta.

Ta książka jest skierowana przede wszystkim do osób, które zarządzają sieciami firmowymi.

Duża sieć stawia przed administratorem spore i często nowe wyzwania. Rozmiar sieci, liczba urządzeń i użyte rozwiązania sprawiają, że administrowanie nią wymaga wiedzy i umiejętności, które wykraczają daleko poza obszar sieci domowych. Ta książka pomoże Ci te kompetencje zdobyć.

W książce znajdziesz szczegółowe omówienie takich tematów jak:

- **Routing statyczny i dynamiczny**
- **Switching**
- **Połączenia VPN**
- **Sieci bezprzewodowe**

Helion

helion.pl

HELION S.A.
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej!

ISBN 978-83-289-1233-5

9 788328 912335

Cena: 99,00 zł