



Łukasz Guziak

KONFIGURACJA USŁUG SIECIOWYCH NA URZĄDZENIACH

MIKROTIK

Poziom zaawansowany

Helion 

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz wydawca dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz wydawca nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

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/konuz
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-289-1233-5

Copyright © Helion S.A. 2025

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

Spis treści

Wstęp	7
ROZDZIAŁ 1. Routing statyczny	9
1.1. Redundancja tras	9
1.2. Dystans administracyjny	17
1.3. Zmiana wartości pola TTL	19
1.4. Strategie routingu	25
ROZDZIAŁ 2. Routing dynamiczny	33
2.1. Wprowadzenie do routingu dynamicznego	33
2.2. Protokół RIP.....	38
2.2.1. Wprowadzenie do protokołu RIP	38
2.2.2. Podstawowa konfiguracja protokołu RIP.....	40
2.2.3. Pętle routingu.....	49
2.2.4. Uwierzytelnianie RIP.....	52
2.2.5. Strict mode, sąsiad statyczny.....	55
2.2.6. Rozgłoszenie trasy domyślnej.....	58
2.2.7. Rozgłoszenie trasy statycznej.....	61
2.2.8. Trasy alternatywne.....	64
2.3. Protokół OSPF	66
2.3.1. Wprowadzenie do OSPF. Pakiety Hello	66
2.3.2. Konfiguracja protokołu OSPF	68
2.3.3. Passive interface	73
2.3.4. Uwierzytelnianie OSPF	75
2.3.5. Rozgłoszenie trasy domyślnej.....	79
2.3.6. Rozgłoszenie trasy statycznej i pochodzącej od innego protokołu routingu dynamicznego	83
2.3.7. Problemy z działaniem protokołu OSPF	89
2.3.8. OSPF w sieciach wielodostępnych	97
2.3.9. Multiarea OSPF	109
2.3.10. Virtual Link.....	114
ROZDZIAŁ 3. Switching	121
3.1. VLAN	121
3.1.1. Opis technologii	121
3.1.2. Konfiguracja sieci VLAN — RouterBOARD	123
3.1.3. Konfiguracja sieci VLAN — Switch Chip	133
3.1.4. Konfiguracja sieci VLAN — CRSxxx	137
3.1.5. Konfiguracja sieci VLAN — SwOS	142

3.1.6. Management VLAN	144
3.1.7. MAC-based VLAN	155
3.1.8. Q-in-Q	159
3.2. Blokowanie portów	173
3.2.1. Port isolation	175
3.2.2. Bridge Horizon	178
3.3. Rodzina protokołów Spanning Tree	179
3.3.1. Protokół Spanning Tree	181
3.3.2. Protokół RSPT	198
3.3.3. Protokół MSTP	199
3.3.4. Mechanizmy ochronne w STP	209
3.4. Bonding	214
3.5. L2 QoS	221
3.6. Port mirroring	223
3.7. Połączenie konsolowe	226
ROZDZIAŁ 4. Połączenia VPN. Tunelowanie ruchu sieciowego	231
4.1. L2TP	232
4.1.1. Połączenie lokacja-lokacja	232
4.1.2. Połączenie klient-lokacja	238
4.2. OpenVPN	246
4.2.1. Połączenie lokacja-lokacja	246
4.2.2. Połączenie klient-lokacja	254
4.3. WireGuard	263
4.3.1. Połączenie lokacja-lokacja	264
4.3.2. Połączenie klient-lokacja	269
4.4. Bridge Control Protocol (BCP)	276
4.5. Generic Routing Encapsulation (GRE)	285
4.6. IPIP (IP over IP)	293
4.7. EoIP (Ethernet over IP)	297
4.7.1. EoIP — konfiguracja tunelu	297
4.7.2. EoIP — sieci VLAN	302
4.8. ZeroTier	308
ROZDZIAŁ 5. Sieci bezprzewodowe	317
5.1. Centralne zarządzanie siecią Wi-Fi za pomocą CAPsMAN	317
5.1.1. Wprowadzenie, opis, zastosowanie	317
5.1.2. Połączenie CAP z CAPsMAN	318
5.1.3. Profil Channel	329
5.1.4. Profil Security	334
5.1.5. Rozgłoszenie sieci Wi-Fi	335
5.1.6. Profil Datapath	337
5.1.7. Kontener Configuration	342
5.1.8. Provisioning	346
5.1.9. Wirtualne interfejsy Wi-Fi	350
5.1.10. Access List	353

5.1.11. Upgrade	355
5.1.12. Zapasowy kontroler	359
5.2. Budowa sieci Hotspot	364
5.2.1. Konfiguracja podstawowa	365
5.2.2. Użytkownik	373
5.2.3. Zarządzanie dostępem (Cookies, Trial)	379
5.2.4. Profil użytkownika	383
5.2.5. IP Binding	387
5.2.6. Walled Garden	388
5.2.7. Usługa reklamy	393
Skorowidz	397

ROZDZIAŁ 1.

Routing statyczny

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

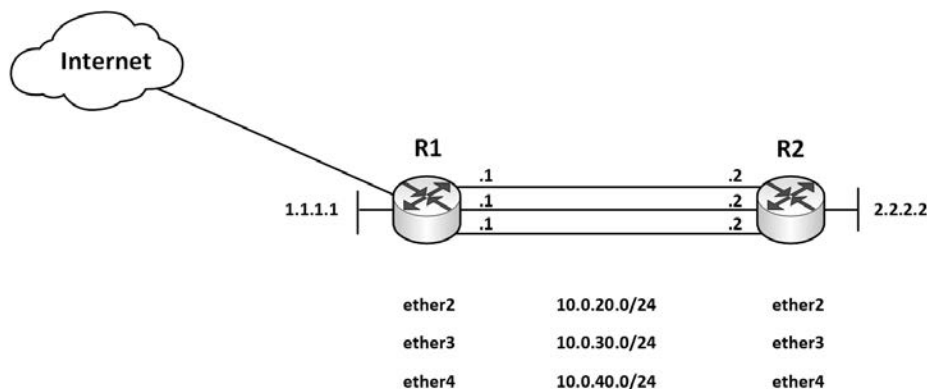
W tym rozdziale:

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

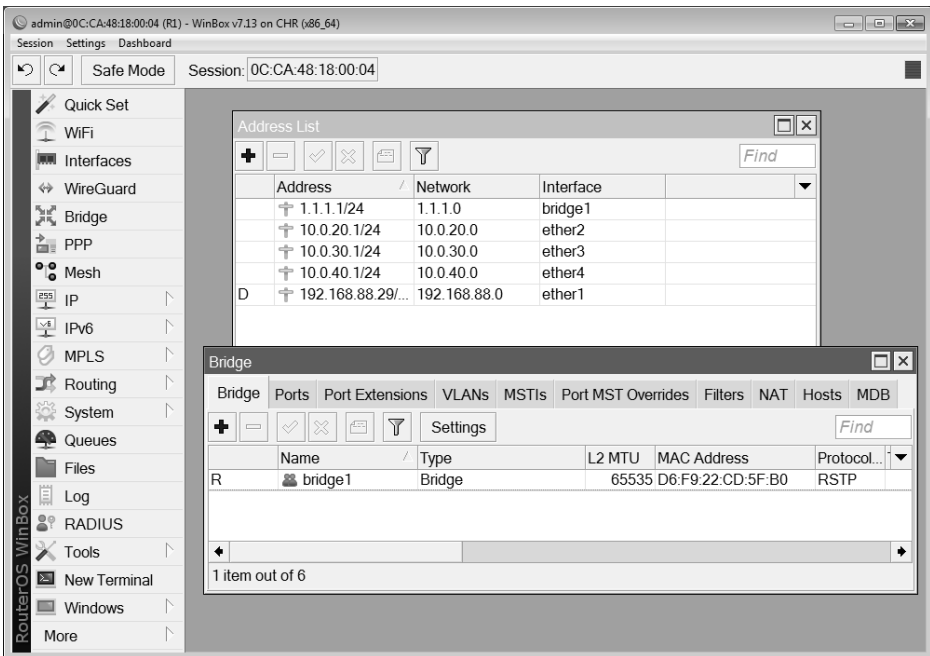
Obowiązująca w tym podrozdziale i następnym topologia sieciowa jest pokazana na rysunku 1.1.



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 interfejsy 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.

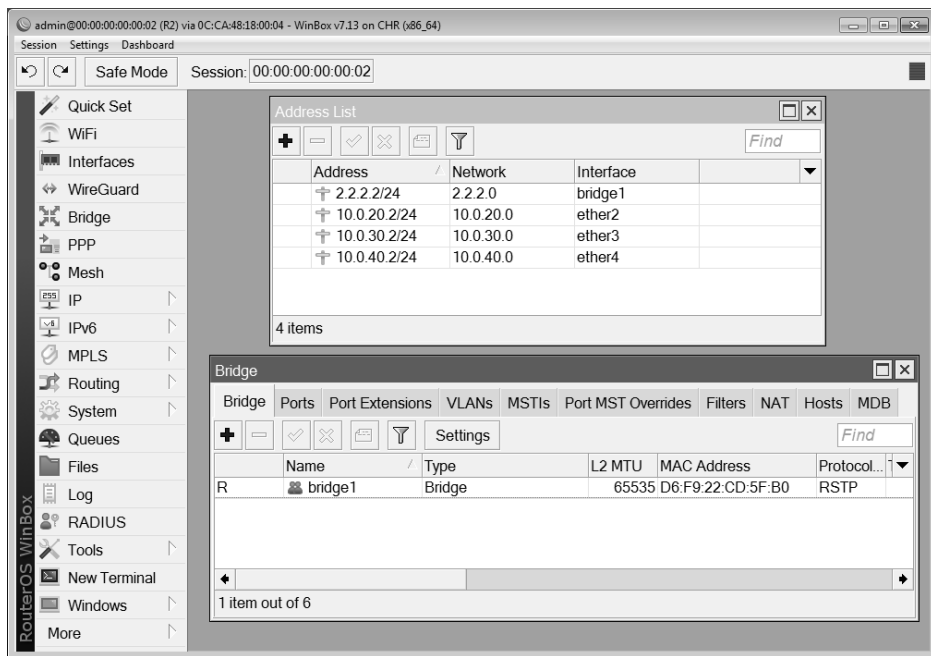


RYСУNEK 1.2. Konfiguracja routera *R1*, utworzenie bridge'a na potrzeby interfejsu loopback

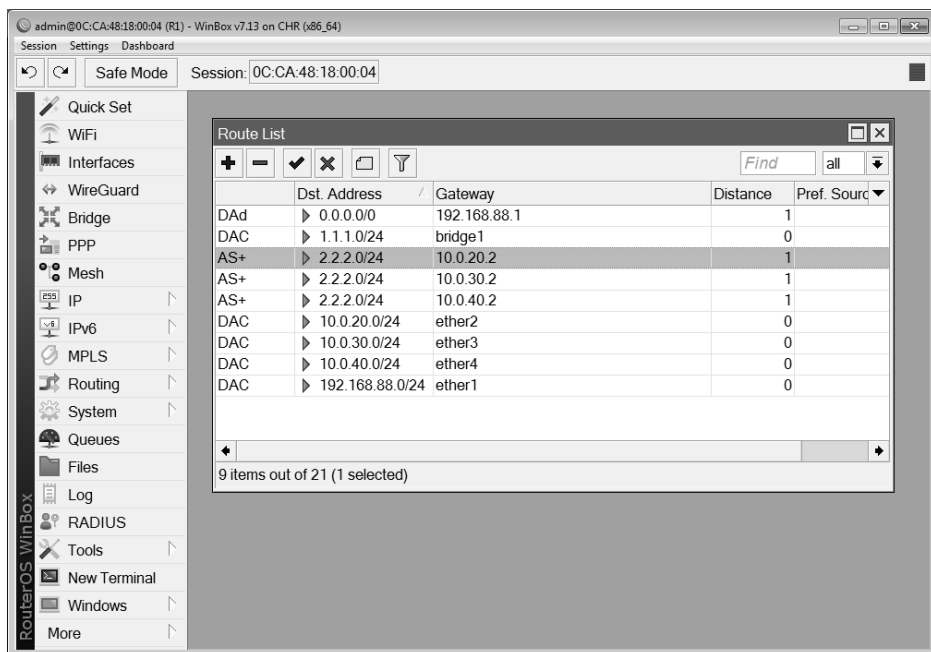
Konfiguracja routera *R2* jest pokazana na rysunku 1.3. Podobnie jak router *R1*, ma on trzy aktywne połączenia oraz interfejs *bridge* (IP *2.2.2.2/24*).

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.

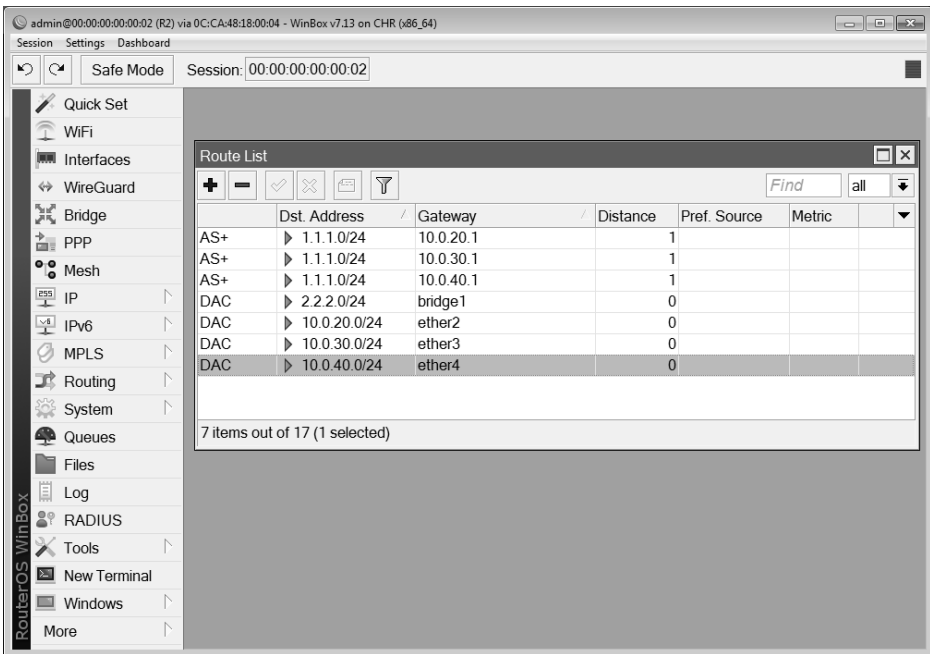
Trasy należy również utworzyć na routerze *R2*. W tablicy routingu znajdują się trzy trasy, prowadzące do sieci *1.1.1.0/24* — rysunek 1.5.



RYSUNEK 1.3. Konfiguracja routera R2



RYSUNEK 1.4. Router R1, konfiguracja tras statycznych



RYСУNEK 1.5. Router R2, konfiguracja tras statycznych

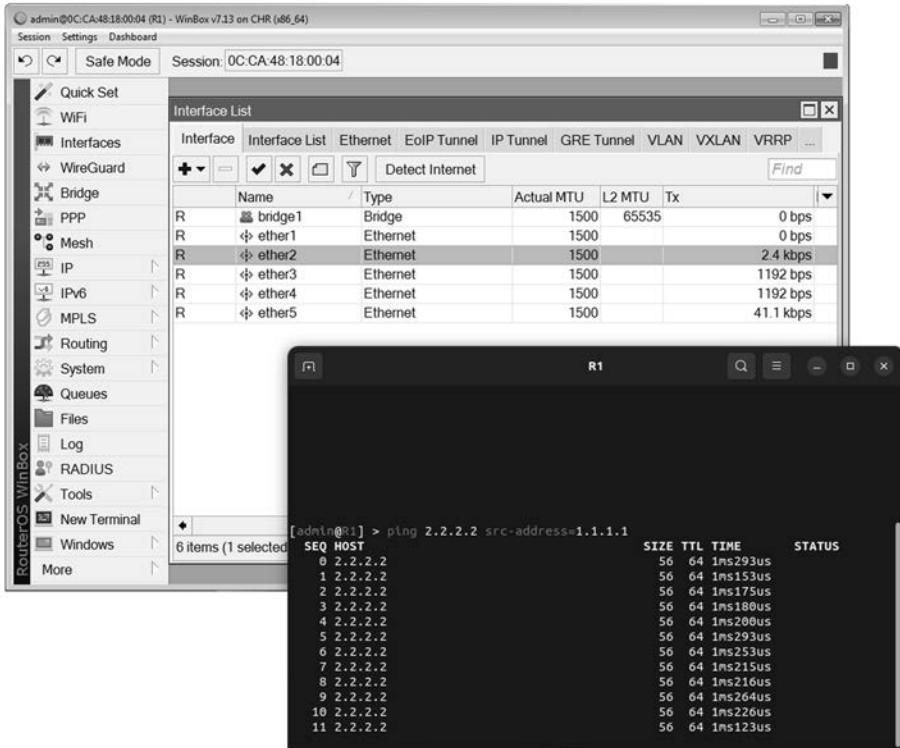
Podczas tworzenia tras z pewnością zauważyłeś, że router w miarę ich dodawania nie wyłącza ani nie zastępuje tras już istniejących. Oznacza to, że wszystkie trzy mają status aktywnych, o czym informuje duża litera *A* (od *active*) w polu statusu trasy. Dodatkowo przy każdej z nich znajduje się znak 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.

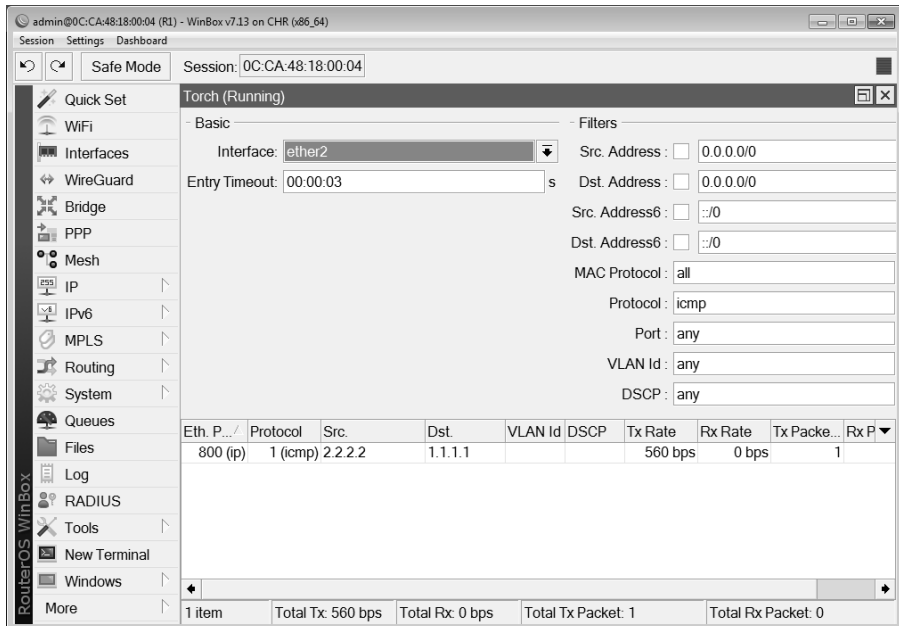
Taka nadmiarowość tras ma na celu zapewnienie ciągłości połączenia w razie wystąpienia awarii. Sprawdźmy zatem, co się stanie, gdy do niej dojdzie. Zasyemułujmy ją i wyłączmy dwa spośród trzech połączeń — interfejsy *ether3* oraz *ether4* na routerze *R1* zostają wyłączone.

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.

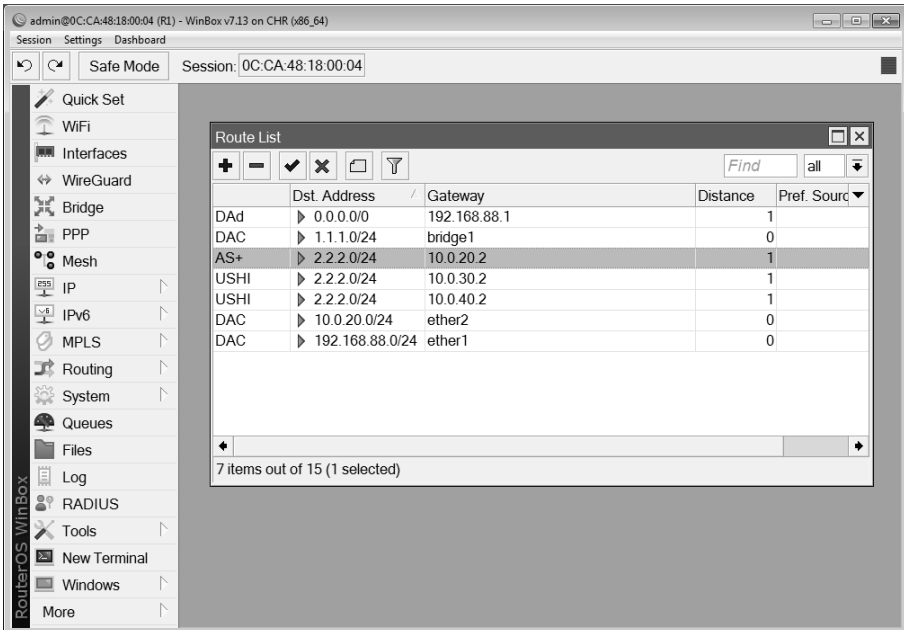
Komunikacja pomiędzy sieciami (pomimo jednej aktywnej trasy) w tym momencie nie jest możliwa. Test ping kończy się niepowodzeniem — rysunek 1.9.



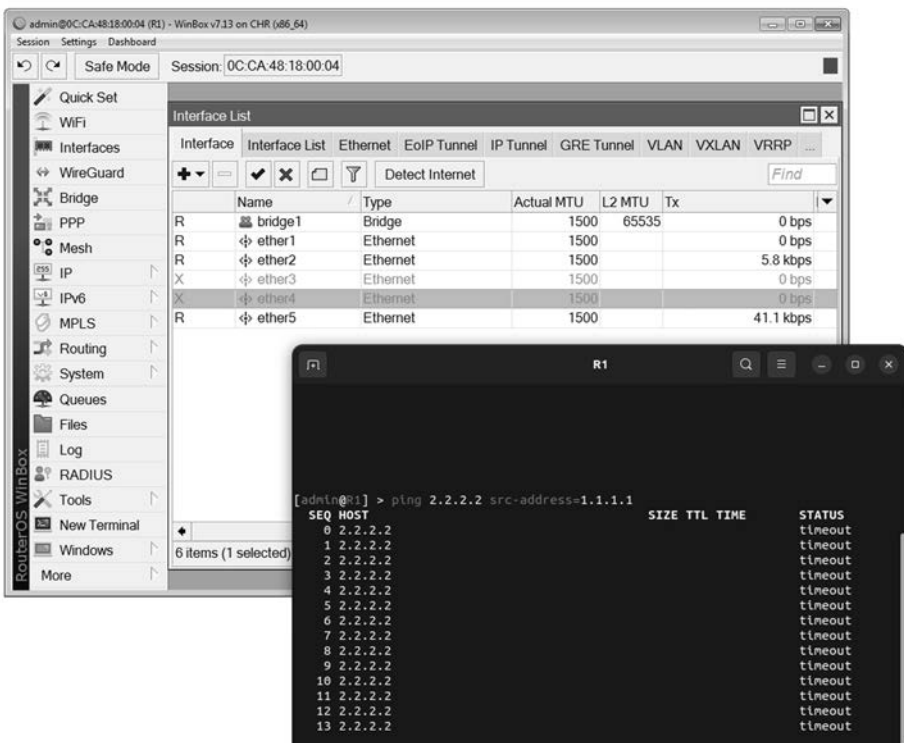
RYSUNEK 1.6. Router R1, test ping



RYSUNEK 1.7. Router R1, użycie narzędzia Torch

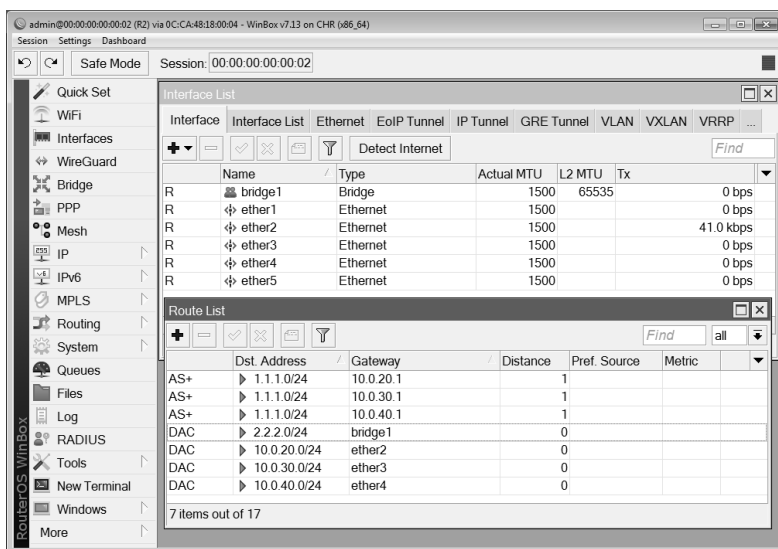


RYSUNEK 1.8. Router R1, status tras prowadzących do sieci 2.2.2.0/24



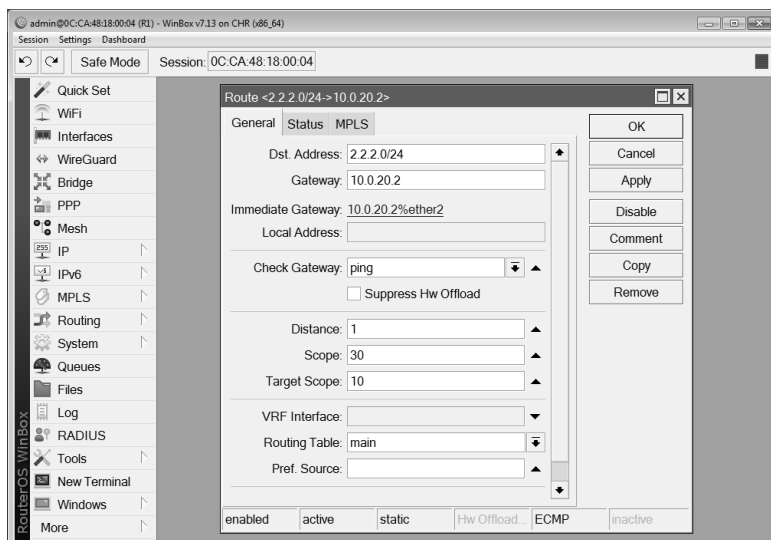
RYSUNEK 1.9. Router R1, test ping

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.



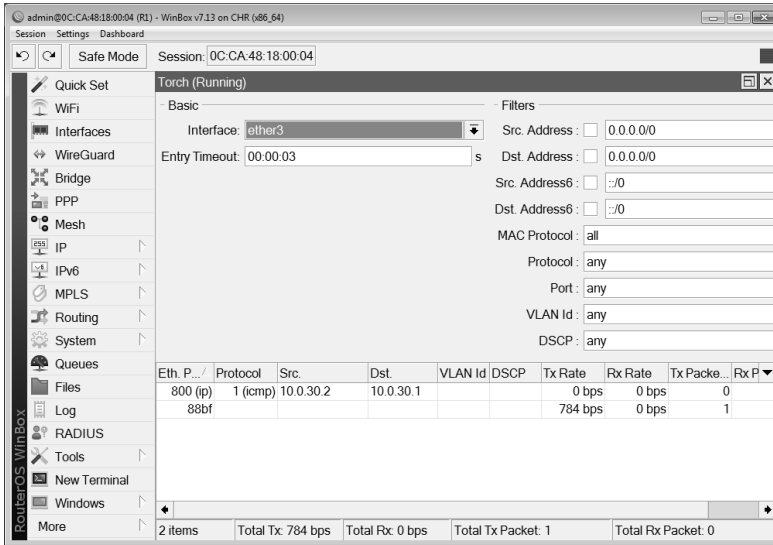
RYSUNEK 1.10. Router R2, status tras prowadzących do sieci 1.112.0/24

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.



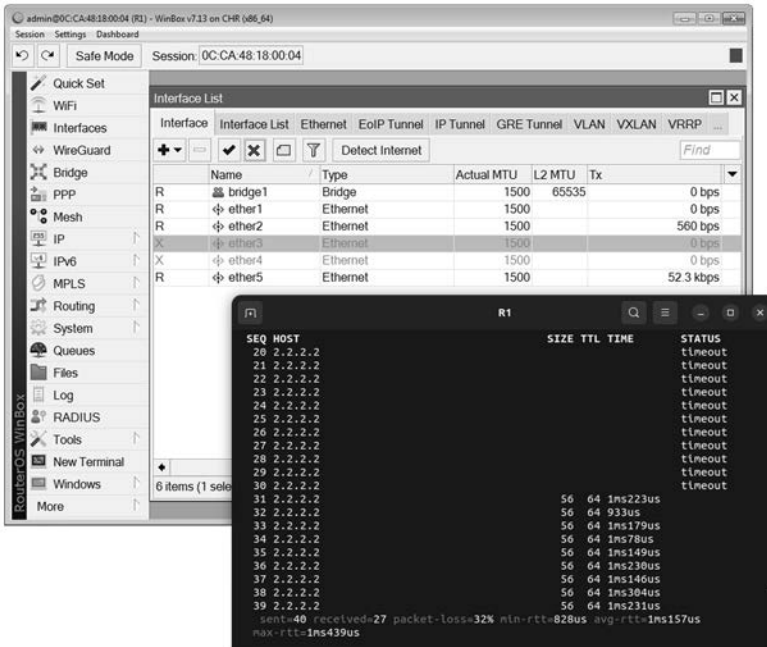
RYSUNEK 1.11. Ustawienie Check Gateway

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



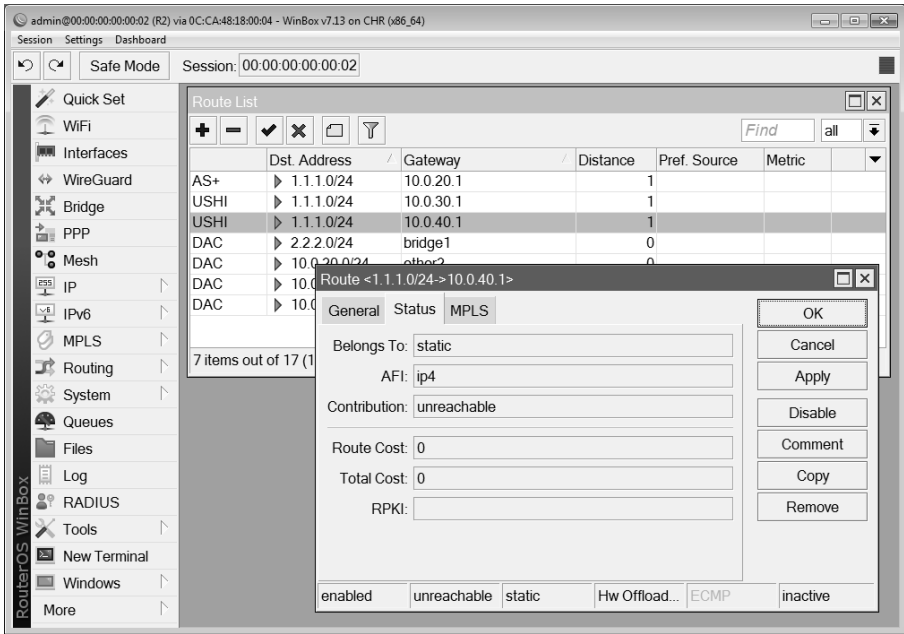
RYSUNEK 1.12. Router R1, test dostępności bramy IP 10.0.30.1, interfejs ether3

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.



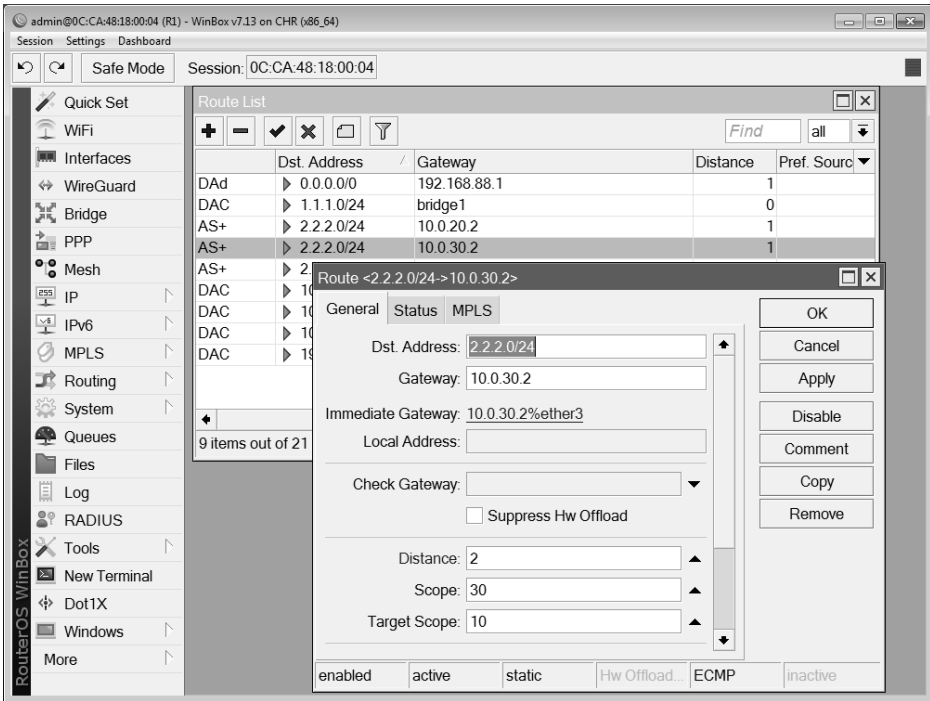
RYСУNEK 1.14. Router *R2*, wyłączenie tras routingu

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

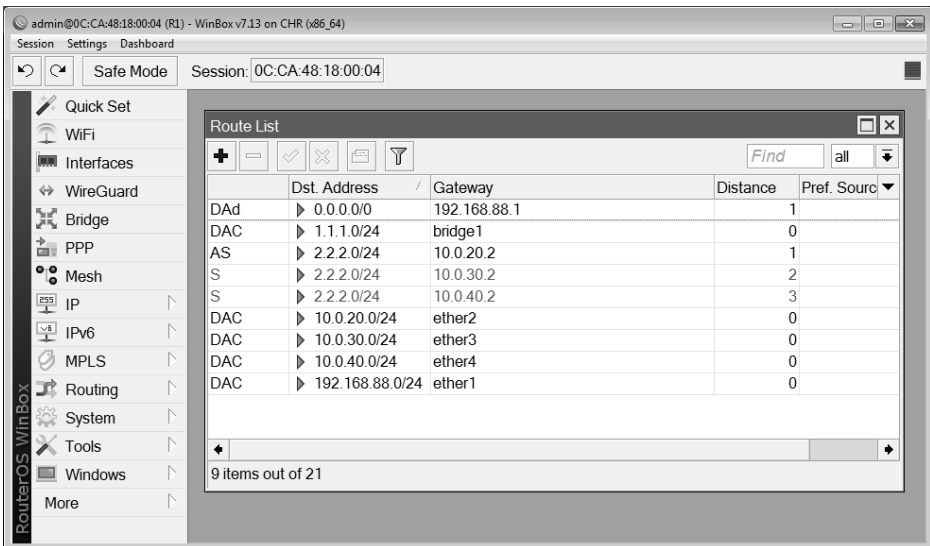
Zdarzają się sytuacje, w których nie chcemy, aby ruch sieciowy był jednocześnie przekazywany poprzez różne interfejsy routera. Chcemy, aby pakiety podróżowały stale określoną trasą, a alternatywna była używana dopiero wtedy, gdy zawiedzie główna. Cel osiągniemy przez zmianę dystansu administracyjnego. 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.



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

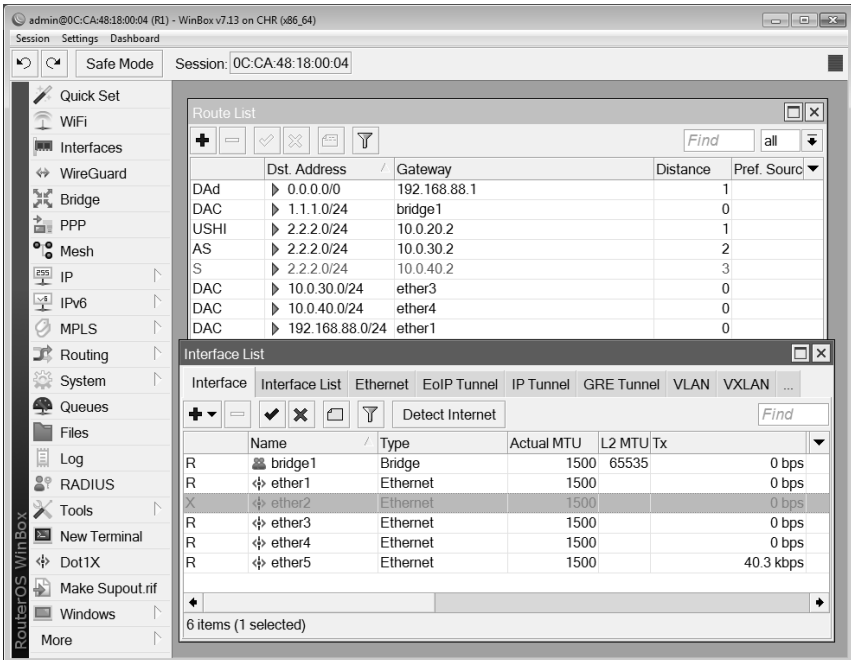
Dystans administracyjny został również zmieniony dla trasy skojarzonej z interfejsem *ether4* (adres IP bramy *10.0.40.2*) i wynosi on *3* — rysunek 1.16.



RYСУNEK 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 zastępuje ją tą, która ma przypisaną niższą wartość dystansu administracyjnego — zostaje użyta trasa prowadząca poprzez interfejs *ether3* — rysunek 1.17.



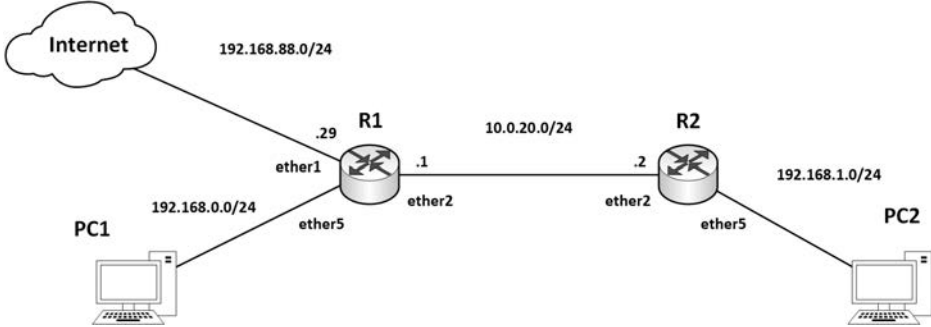
RYSunEK 1.17. Router R1, wyłączenie interfejsu ether2

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

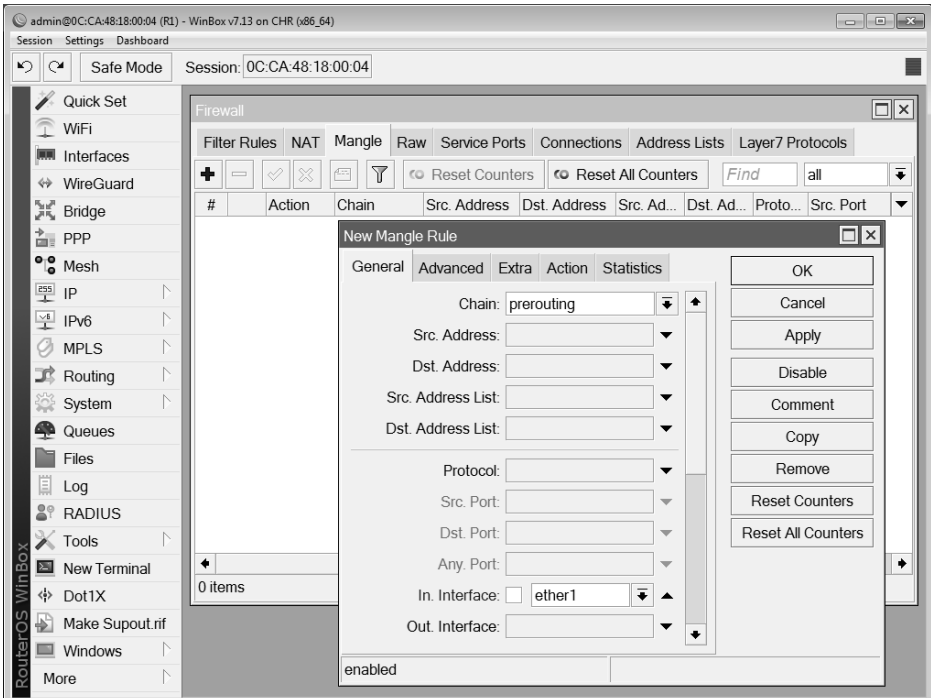
Pole TTL zarządza czasem życia pakietów. Oznacza to, że gdy router otrzyma pakiet, którego wartość pola TTL wynosi 1, nie przekaże go dalej. Wartość pola TTL jest zmniejszana o jeden za każdym razem, gdy jest on przekazywany przez router. Zapobiega to sytuacji, w której pakiety byłyby przekazywane pomiędzy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



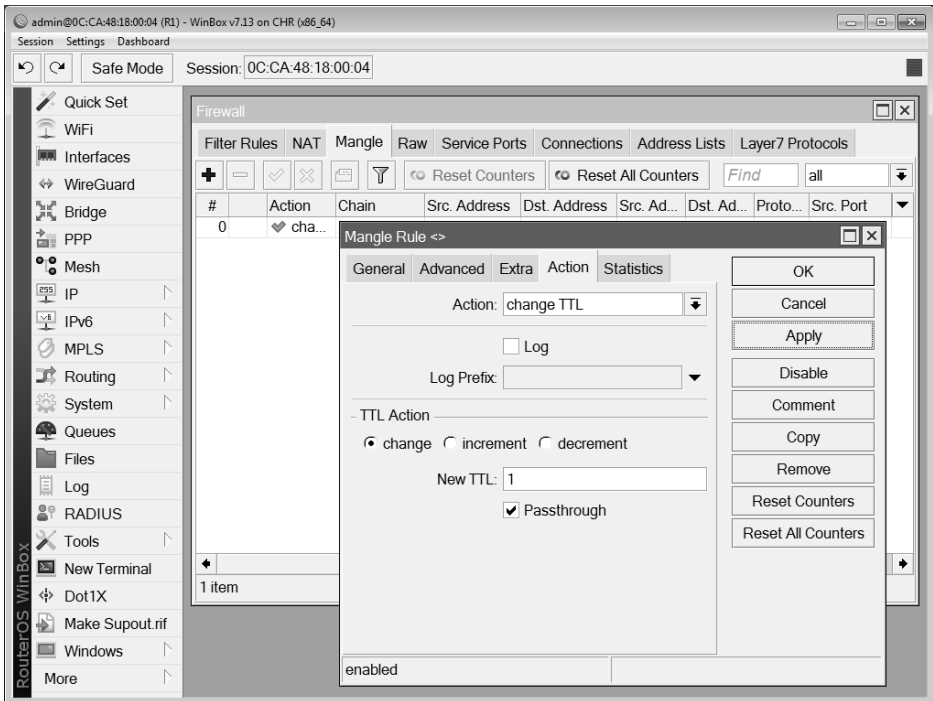
RYSUNEK 1.18. Topologia sieciowa

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.



RYСУNEK 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. Miejsmem 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 (otrzymane i przesłane dalej) łączą wartość pola *Sequence Number* — rysunek 1.24 (2).

Route List

	Dst. Address	Gateway	Distance	Pref. Source	Metric
AS	0.0.0.0/0	10.0.20.1	1		
AS	1.1.1.0/24	10.0.20.1	1		
USHI	1.1.1.0/24	10.0.30.1	2		

Terminal <1>

```
[admin@R2] > ping 8.8.8.8
```

SEQ	HOST	SIZE	TTL	TIME	ST
0	8.8.8.8	56	1	20ms964us	
1	8.8.8.8	56	1	17ms100us	
2	8.8.8.8	56	1	17ms138us	
3	8.8.8.8	56	1	16ms834us	
4	8.8.8.8	56	1	16ms768us	
5	8.8.8.8	56	1	16ms995us	
6	8.8.8.8	56	1	16ms658us	
7	8.8.8.8				ti
8	8.8.8.8				ti
9	8.8.8.8				ti
10	8.8.8.8				ti
11	8.8.8.8				ti
12	8.8.8.8				ti
13	8.8.8.8				ti
14	8.8.8.8				ti
15	8.8.8.8				ti

RYSUNEK 1.21. Router R2, brak połączenia z siecią Internet

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

Mangle Rule <>

General Advanced Extra Action Statistics

Action: change TTL

Log

Log Prefix: []

TTL Action

change increment decrement

New TTL: 2

Passthrough

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

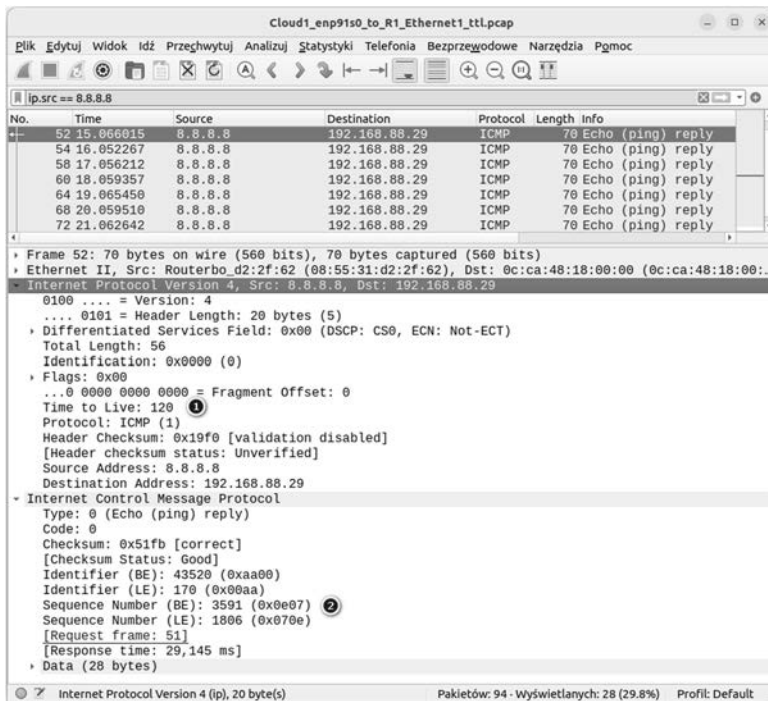
Terminal <1>

```
R2
```

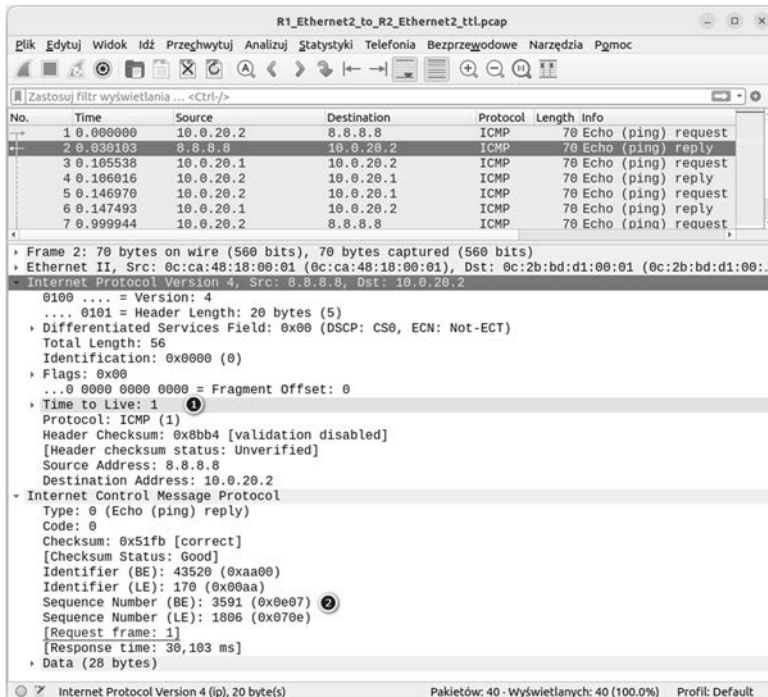
127	8.8.8.8				timeout
128	8.8.8.8				timeout
129	8.8.8.8				timeout
130	8.8.8.8				timeout
131	8.8.8.8				timeout
132	8.8.8.8				timeout
133	8.8.8.8				timeout
134	8.8.8.8				timeout
135	8.8.8.8	56	1	16ms323us	
136	8.8.8.8	56	1	16ms758us	
137	8.8.8.8	56	1	16ms774us	
138	8.8.8.8	56	1	17ms10us	
139	8.8.8.8	56	1	17ms41us	
140	8.8.8.8	56	1	17ms72us	

sent=140 received=22 packet-loss=84% min-rtt=16ms323us avg-rtt=16ms915us max-rtt=17ms430us

RYSUNEK 1.22. Router R2, odzyskanie połączenia z siecią Internet

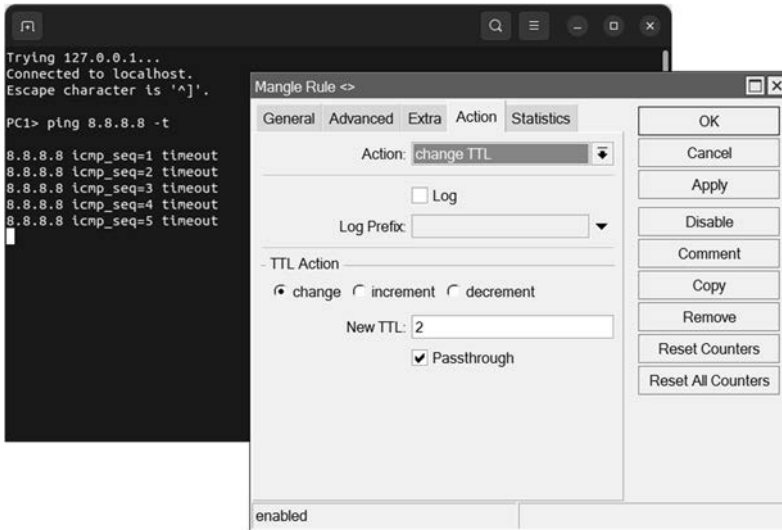


RYSUNEK 1.23. Router R1, interfejs ether1, przechwycony pakiet ICMP



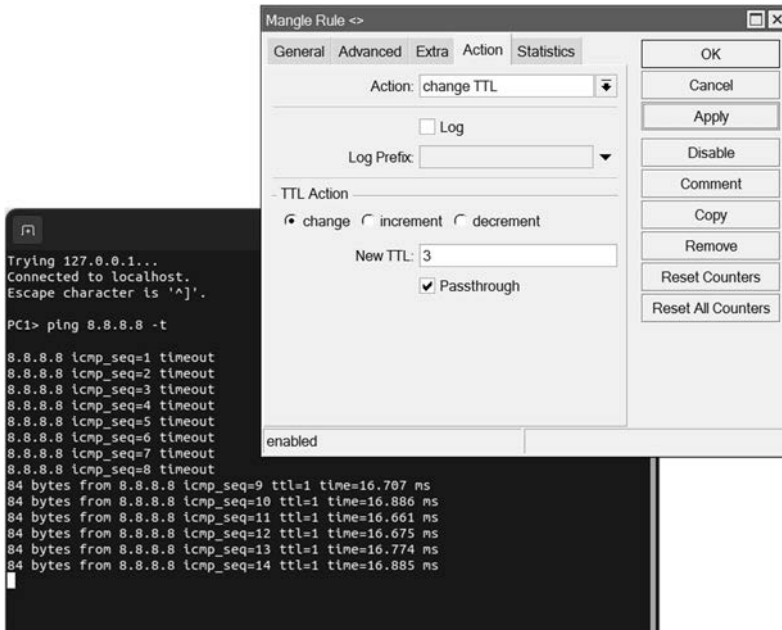
RYSUNEK 1.24. Router R1, interfejs ether2, przechwycony pakiet ICMP

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.



RYСУNEK 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.



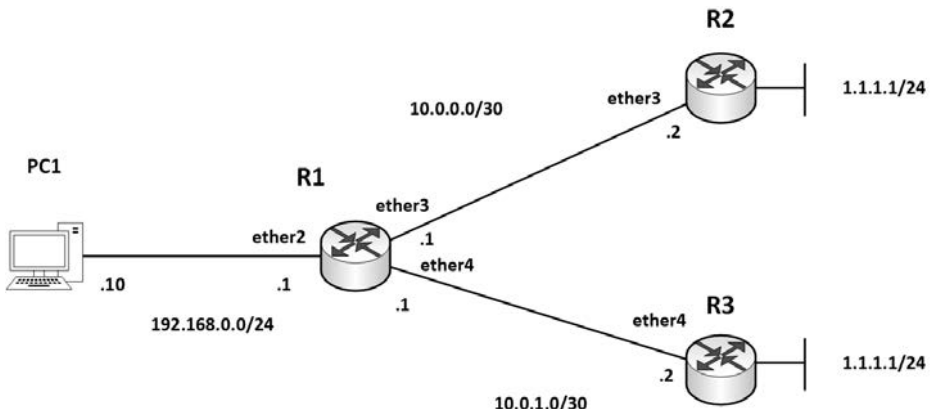
RYСУNEK 1.26. Modyfikacja pola TTL, komputer PC2 uzyskuje połączenie z siecią Internet

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 udostępniłby 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.

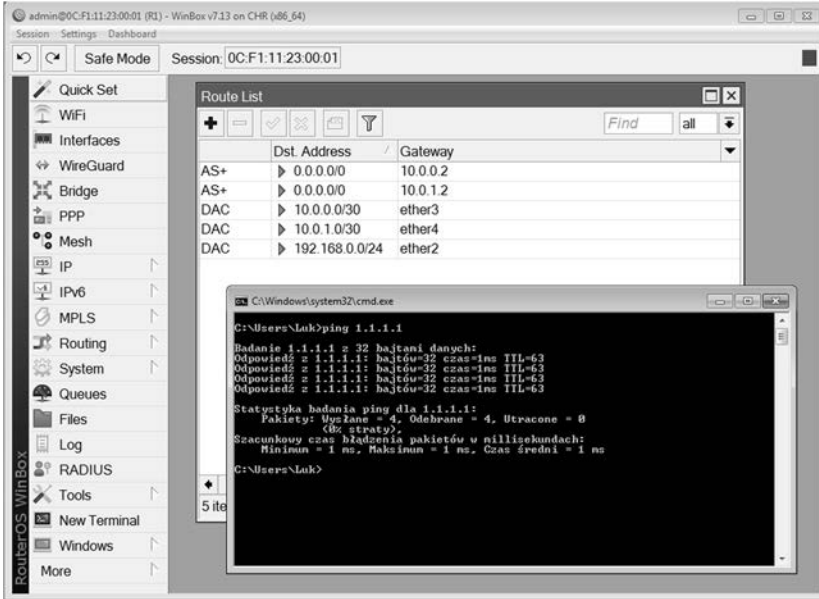
1.4. Strategie routingu

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*. Zasymlujemy 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.



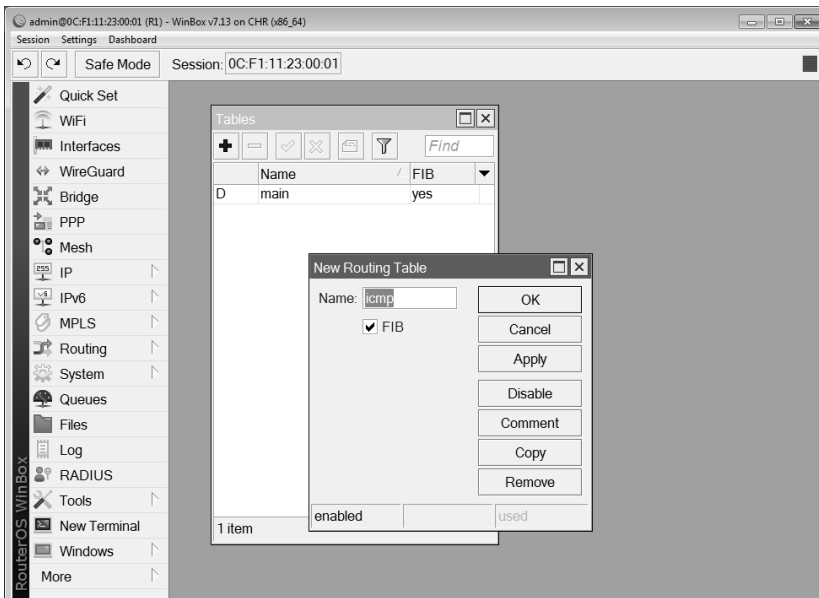
RYSUNEK 1.27. Topologia sieciowa

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 przechowywać 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.

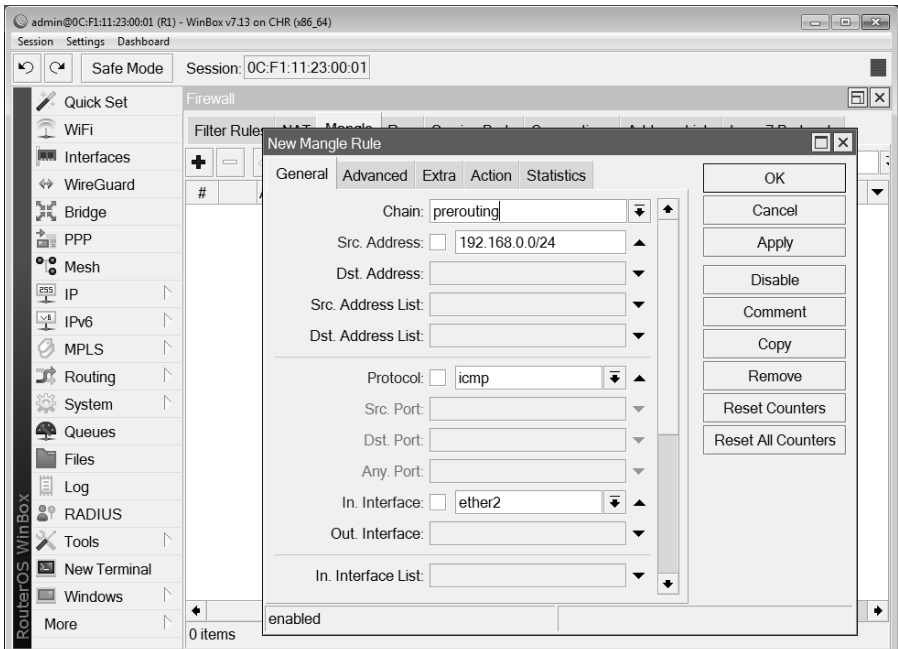


RYSUNEK 1.29. Router R1, utworzenie nowej tablicy routingu

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.

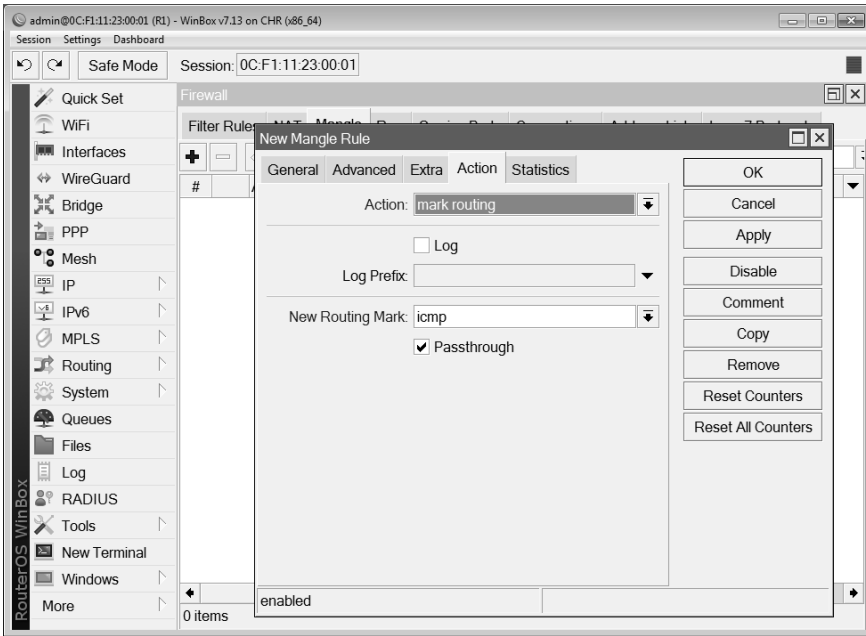
Kolejnym krokiem jest oznaczenie ruchu sieciowego, który ma zostać przez router przekierowany. Kryterium oznaczenia określa się na zakładce *Mangle*, znajdującej się w ustawieniach zapory sieciowej (*Firewall*). Po kliknięciu ikony plusa w oknie *New Mangle Rule* (karta *General*) określa się kryteria 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*).



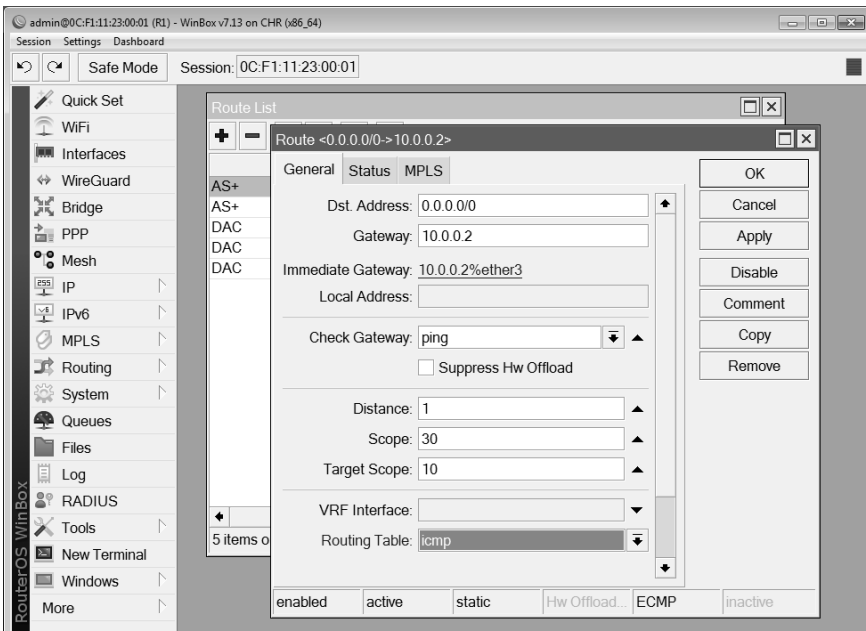
RYСУNEK 1.30. Router R1, zakładka *General*, oznaczenie ruchu sieciowego

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.



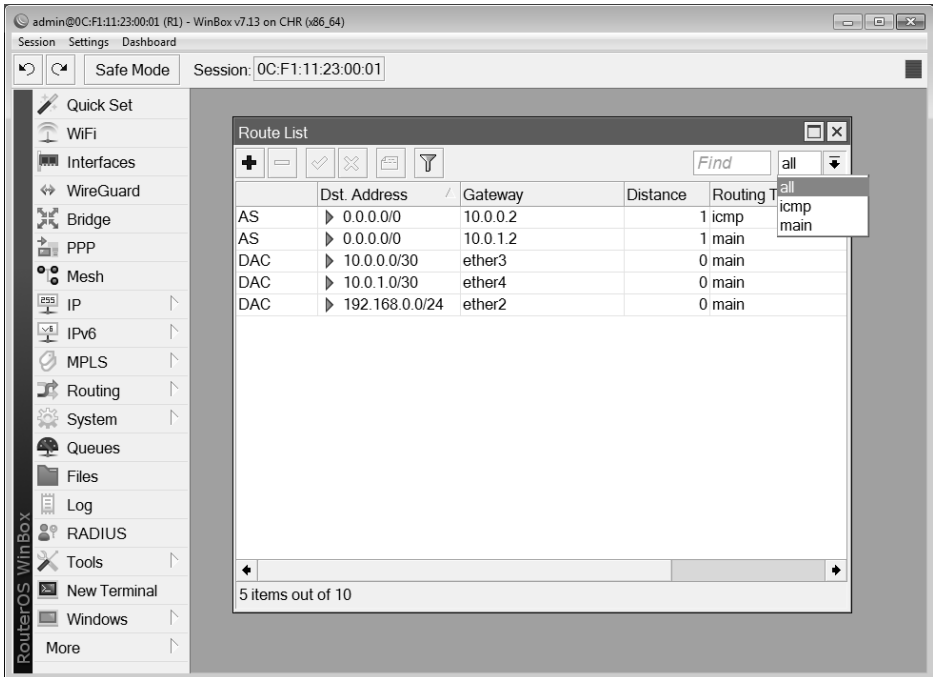
RYSUNEK 1.31. Router R1, karta Action, oznaczenie ruchu sieciowego

Ostatnią czynnością jest powiązanie trasy z tabelą 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.



RYСУNEK 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.

admin@0C:F1:11:23:00:01 (R1) - WinBox v7.13 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 0C:F1:11:23:00:01

Quick Set

WiFi

Interfaces

WireGuard

Bridge

PPP

Mesh

IP

IPv6

MPLS

Routing

System

Queues

Files

Log

RADIUS

Tools

New Terminal

Windows

More

Torch (Running)

- Basic

Interface: ether3

Entry Timeout: 00:00:03 s

- Filters

Src. Address: 0.0.0.0

Dst. Address: 0.0.0.0

Src. Address6: ::0

Dst. Address6: ::0

MAC Protocol: all

Protocol: any

Port: any

VLAN Id: any

DSCP: any

Eth. P.../	Protocol	Src.	Dst.	VLAN Id	DSCP
800 (ip)	1 (icmp)	1.1.1.1	192.168.0.10		
800 (ip)	1 (icmp)	10.0.0.2	10.0.0.1		
88bf					

3 items Total Tx: 1824 b... Total Rx: 1152 b... Total Tx Packet: 3 Total Rx Packet: 2

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

admin@0C:F1:11:23:00:01 (R1) - WinBox v7.13 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 0C:F1:11:23:00:01

Quick Set

WiFi

Interfaces

WireGuard

Bridge

PPP

Mesh

IP

IPv6

MPLS

Routing

System

Queues

Files

Log

RADIUS

Tools

New Terminal

Windows

More

Torch (Running)

- Basic

Interface: ether4

Entry Timeout: 00:00:03 s

- Filters

Src. Address: 0.0.0.0

Dst. Address: 0.0.0.0

Src. Address6: ::0

Dst. Address6: ::0

MAC Protocol: all

Protocol: any

Port: any

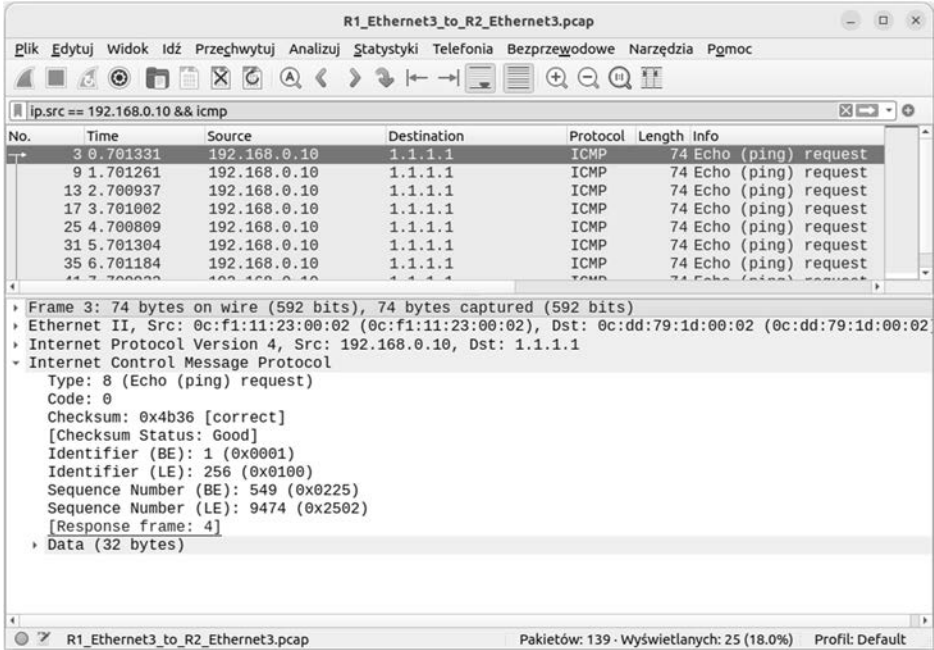
VLAN Id: any

DSCP: any

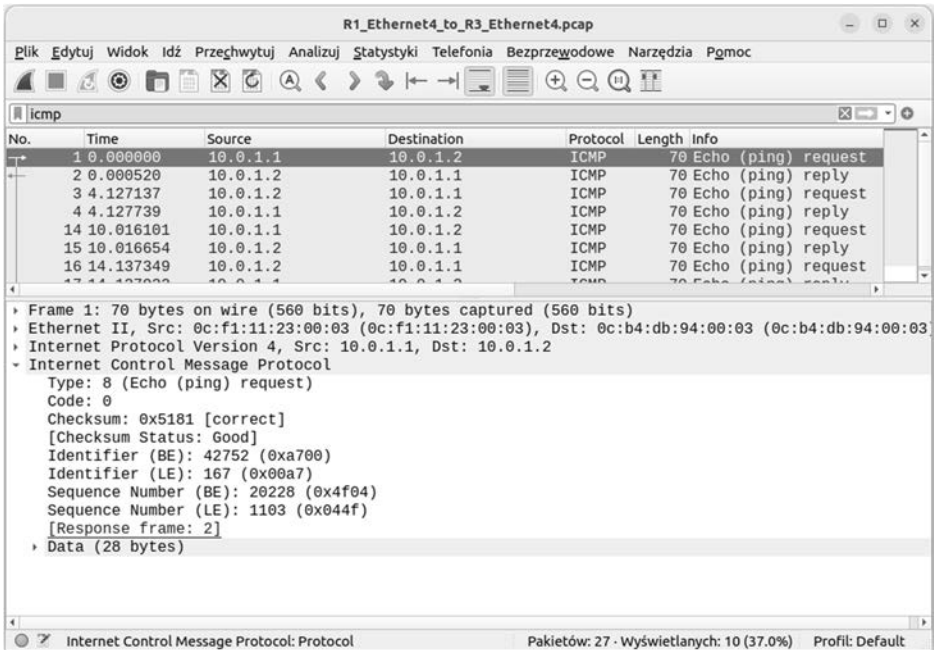
Eth. P.../	Protocol	Src.	Dst.	VLAN Id	DSCP
800 (ip)	1 (icmp)	10.0.1.2	10.0.1.1		
806 (arp)					
88bf					

3 items Total Tx: 0 bps Total Rx: 0 bps Total Tx Packet: 0 Total Rx Packet: 0

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

A

ABR, Area Border Router, 110
Access List, 353
adres MAC, 155, 183
algorytm
 cbc, 235
 drzewa rozpinającego, 181
 HMAC, 235
ASBR, Autonomous System
 Boundary Router, 110

B

BCP, Bridge Control Protocol,
 276
 działanie protokołu, 276
BDR, Backup Designated
 Router, 98
blokowanie portów, 173
bonding, 214
BPDU Guard, 212
bridge horizon, 178
burza rozgłoszeniowa,
 broadcast storm, 179

C

CAP, 317
CAPsMAN, 317
 Access List, 353
 aktualizacja jednostek CAP,
 355
 kontener Configuration, 342
 połączenie z CAP, 318
 profil
 Channel, 329
 Datapath, 337
 Security, 334
 provisioning, 346
 rozgłoszenie sieci Wi-Fi, 335
 wirtualne interfejsy Wi-Fi,
 350
 zapasowy kontroler, 359
 zarządzanie siecią Wi-Fi,
 317

certyfiakat

 CA, 361
 CAP, 323
 hotspot, 372
Check Gateway, 15
CRS, Cloud Router Switch, 137
CSS, Cloud Smart Switch, 142
czarna dziura, black hole
 VLAN, 155
czas życia pakietów, 19

D

DHCP, 58, 123
 konfiguracja serwera, 126
 stan serwera, 129
 uruchomienie serwera, 147
DR, Designated Router, 98
drother, 98
dystans administracyjny, 17, 36
 wartości, 37

E

ECMP, Equal Cost Multi-Path,
 12, 25, 29
edge port, 209
EGP, Exterior Gateway
 Protocols, 35
elekcja DR i BDR
 identyfikator Router ID,
 103
 najwyższy adres IP, 99
 priorytet interfejsu, 106
EoIP, Ethernet over IP, 297
 konfigurowanie tunelu, 297
 sieć VLAN, 302
 tworzenie tunelu, 301
ESP, Encapsulating Security
 Payload, 292

F

FIB, Forwarding Information
 Base, 27

G

GRE, Generic Routing
 Encapsulation, 285
 konfiguracja tunelu, 285

H

Hardware Offload, 168
Hotspot, 364
 konfiguracja
 IP Binding, 389
 reklamy, 393
 Walled Garden, 390
lista
 cookies, 384
 reguł qos, 387
 urządzeń, 376
logowanie użytkownika, 375
połączenie z panelem
 usługi, 370
status użytkownika, 371
statystyki użytkownika, 377
sterowanie dostępem, 387
tworzenie, 365, 369
tworzenie konta
 użytkownika, 374
ustawienie
 cookie, 382
 profilu, 376, 385
 trial, 380
użytkownik trial, 381

I

ICMP, 25
IGP, Interior Gateway
 Protocols, 35
interfejs wirtualny, 350, 351
IP Binding, 387
IPIP, IP over IP, 293
 konfigurowanie tunelu,
 294
 tworzenie tunelu, 296
IPsec, 235, 289
IR, internal router, 110

K

konfiguracja
 bridge'a, 279
 certyfikatów, 325, 363
 interfejsu wirtualnego, 352
 mechanizmu Q-in-Q, 159, 167
 NAT, 126
 połączenia
 L2TP, 243–245
 OVPN, 248
 protokołu
 MSTP, 202
 OSPF, 68, 92
 RIP, 40, 49
 STP, 197
 przełącznika, 151, 154
 reguły QoS, 222
 routera, 10, 11
 serwera
 DHCP, 126
 SSTP, 281
 sieci VLAN
 CRSxxx, 137
 RouterBOARD, 123
 Switch Chip, 133
 SwOS, 142
 sieci VLAN over EoIP, 307
 tras statycznych, 11, 12
 tunelu
 EoIP, 297
 GRE, 285
 IPIP, 294
 WireGuard, 264
 usługi ZeroTier, 308
 wieloobszarowego OSPF, 110
 zapory, 131
 kontener Configuration, 342

L

L2TP, Layer 2 Tunneling Protocol, 232
 konfiguracja połączenia, 240, 243, 244
 połączenie klient-lokacja, 238
 połączenie lokacja-lokacja, 232
 tworzenie tunelu, 237

ł

łącze
 typu access, 122, 127, 163
 typu trunk, 122, 124
 wirtualne, link aggregation, 214

M

management VLAN, 144
 metryka, 36
 maksymalna, 49
 MSTP, Multiple Spanning Tree, 199
 działanie protokołu, 201
 konfiguracja, 202
 multicast, 39

N

narzędzie
 PuTTY, 227
 Torch, 13, 16, 29, 130, 166
 Wireshark, 198
 NAT, 59, 126

O

OpenVPN, 246
 konfigurowanie
 połączenia, 248
 połączenie klient-lokacja, 254
 połączenie lokacja-lokacja, 246
 tworzenie tunelu, 250, 251
 OSPF, 66
 błędna konfiguracja interfejsu, 90
 czas Dead Interval, 95
 czas Hello Interval, 93
 definicja obszaru, 69
 konfiguracja interfejsu, 74
 konfiguracja protokołu, 68, 92
 pakiety Hello, 66
 passive interface, 73, 91
 połączenie Virtual Link, 114
 problemy z działaniem, 89
 przechwytywanie pakietów, 67
 trasa domyślna, 79
 trasa statyczna, 83
 trasy protokołu RIP, 87
 uruchomienie instancji, 69
 ustawienie hasła, 76
 uwierzytelnianie, 66, 75, 93
 w sieciach
 wielodostępowych, 97
 wieloobszarowy, 109
 konfiguracja, 110

P

pakiet
 Hello, 66
 ICMP, 23
 passive interface, 73
 pętle routingu, 49
 podzielony horyzont, split horizon, 49
 z zatruciem wstecz, 50
 pole
 Authentication, 94
 BPDU Guard, 212
 Bridge, 280
 Certificate, 361
 Horizon, 178
 IPsec Password, 289
 Local Address, 238
 MAC Address, 185
 MRRU, 282
 Originate Default, 59
 Password, 238
 Priority, 188
 Remote Address, 238
 rip, 46
 Router ID, 103
 SSID, 343
 TTL, 19
 Use IPsec, 235
 połączenie konsolowe, 226
 port
 isolation, 175
 mirroring, 223
 profil
 Channel, 329
 Datapath, 337
 Security, 334
 protokoły routingu, 34
 bezklasowe, 34
 bramy wewnętrznej, 35
 bramy zewnętrznej, 35
 klasowe, 34
 path-vector, 35
 stanu łącza, 35
 wektora odległości, 35
 protokoł
 BCP, 276
 EGP, 35
 EoIP, 297
 ESP, 292
 GRE, 285
 HTTPS, 371
 IGP, 35
 IPIP, 293
 IPsec, 235
 MSTP, 199
 OpenVPN, 246

OSPF, 66
 RIP, 38
 RSPT, 198
 STP, 179
 WireGuard, 263
 provisioning, 346
 przechwytywanie pakietów, 50, 67
 przełącznik, switch, 51, 121
 adres MAC urządzenia, 155
 agregacja interfejsów, 214
 blokowanie portów, 173
 bridge horizon, 178
 port isolation, 175
 edge port, 209
 konfiguracja, 151
 mechanizm
 BPDU Guard, 212
 Q-in-Q, 159, 167
 QoS, 221
 root guard, 211
 port mirroring, 223
 tryb
 active backup, 220, 221
 balance-rr, 219
 typu CRS, 137
 typu CSS, 142
 układ switch chip, 133
 punkt dostępowy, AP, 317

Q

Q-in-Q, 159
 konfiguracja, 159, 166–169, 173
 weryfikacja działania, 172
 włączenie mechanizmu, 171
 QoS, 221, 387
 konfiguracja, 222

R

ramka BPDU, 182
 redundancja tras, 9
 reguła
 IP Binding, 389
 provisioning, 349, 352
 Walled Garden, 390
 rejestrowanie ruchu sieciowego, 30
 relacja sąsiedzka, 52
 RIP, 38
 informacje o sieciach, 46
 konfiguracja protokołu, 40, 49
 przechwytywanie pakietów, 50

status protokołu, 48
 strict mode, 55
 trasa domyślna, 58
 trasa statyczna, 61
 tworzenie instancji, 42
 ustalenie hasła, 52
 uwierzytelnianie, 52
 weryfikacja działania, 44
 włączenie protokołu, 43

Root Guard, 211

router

ASBR, 110
 Branch, 311
 desygnowany, DR, 98
 desygnowany zapasowy, BDR, 98
 HQ, 233, 314
 na patyku, router on a stick, 132

RouterBOARD, 123, 142

RouterOS, 137

zmiana systemu, 142

routerzy

brzegowe, ABR, 110
 wewnętrzne, IR, 110

routing

dynamiczny, 33
 pętle, 49
 protokoły, 34
 statyczny, 9
 strategię, 25

rozgłaszanie

sieci Wi-Fi, 335

trasy

domyślnej, 58, 79
 pochodzącej od RIP, 87
 statycznej, 61, 83

RSTP, Rapid Spanning Tree Protocol, 198

S

sąsiad statyczny, 55

sieci

bezczelne, 317
 wielodostępowe, 97

stan protokołu

RSTP, 198
 STP, 197

STP, Spanning Tree Protocol, 179

algorytm STA, 181
 działanie protokołu, 181, 182, 200

konfigurowanie protokołu, 197

stany portu, 197

wyznaczanie trasy, 191, 195
 zabezpieczenia, 209
 strategię routingu, 25
 strict mode, 55
 switch, *Patrz* przełącznik
 Switch Chip, 133
 SwitchOS, 138
 SwOS, 142
 ustawienia systemu, 143

T

tablica

routingu, 26, 45
 tworzenie, 26
 zmienianie, 28
 sąsiadów, 71

tagowanie, 135, 136, 140, 144, 152

test bramy, 16

trasy

alternatywne, 64
 dynamiczne, 33
 statyczne, 9

TTL, Time to Live, 180

zmienianie wartości pola, 19

tunel, *Patrz także* VPN

EoIP, 297
 GRE, 285
 IPIP, 293
 L2TP, 232
 OVPN, 246
 WireGuard, 263

tworzenie

bridge'y, 128, 134, 138, 148, 151

certyfikatów, 247

hotspota, 366, 369

interfejsu wirtualnego, 350

kontenera Configuration, 344

łącza access, 163

łącza virtual link, 118

połączenia WireGuard, 269
 profilu

Channel, 330, 334
 Datapath, 339
 Security, 334

sieci VLAN, 124, 135, 144, 150–153, 160, 171

tablicy routingu, 26

tras statycznych, 85

tunelu

EoIP, 301
 IPIP, 296
 L2TP, 237
 OVPN, 250, 251

U

urządzenia
 CRS, 137
 CSS, 142
 usługa
 Walled Garden, 388
 ZeroTier, 308
 uwierzytelnianie
 OSPF, 75
 RIP, 52

V

Virtual Link, 114
 VLAN, Virtual LAN, 121
 czarna dziura, 155
 konfiguracja sieci
 CRSxxx, 137
 RouterBoard, 123
 Switch Chip, 133
 SwOS, 142
 powiązanie adresu MAC,
 155
 tunel EoIP, 302
 zarządzające, management
 VLAN, 144

VPN, 231–316

protokoły
 BCP, 276
 EoIP, 297
 GRE, 285
 IPIP, 293
 L2TP, 232
 OpenVPN, 246
 WireGuard, 263
 ZeroTier, 308

W

Walled Garden, 388
 Wi-Fi, 317
 WireGuard, 263
 konfigurowanie tunelu, 264
 połączenie klient-lokacja,
 269
 połączenie lokacja-lokacja,
 264
 tworzenie połączenia, 269
 wirtualne interfejsy Wi-Fi,
 350

Z

zapasowy router
 desygnowany, BDR, 98
 zapora, 131, 391
 ZeroTier, 308
 autoryzacja routera, 312
 konfiguracja usługi, 308

PROGRAM PARTNERSKI

— GRUPY HELION —

- 
1. ZAREJESTRUJ SIĘ
 2. PREZENTUJ KSIĄŻKI
 3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

GRUPA
Helion

KONFIGURACJA USŁUG SIECIOWYCH NA URZĄDZENIACH

MIKROTİK

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