Adam Józefiok

GNS3

Emulowanie sieci komputerowych **Cisco**

Helion

Opieka redakcyjna: Ewelina Burska
Projekt okładki: Studio Gravite/Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki
Materiały graficzne na okładce zostały wykorzystane za zgodą Shutterstock.

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/gns3em
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-283-2664-4

Printed in Poland.

Spis treści

Rozdział 4.

Wykorzystanie programu Wireshark w GNS3

Podczas instalacji GNS3 instaluje się również program Wireshark. Jest to darmowy sniffer, którego możesz użyć do przechwytywania ruchu pomiędzy urządzeniami, co pozwoli potem go analizować.

Program umożliwia przechwytywanie ruchu sieciowego na wybranym interfejsie i jego analizę w rozbiciu na poszczególne warstwy modelu ISO/OSI. Zobaczysz na własne oczy każdą przesłaną ramkę. Program umożliwia analizę ruchu w czasie rzeczywistym oraz zapisywanie przechwytywanych informacji do pliku.

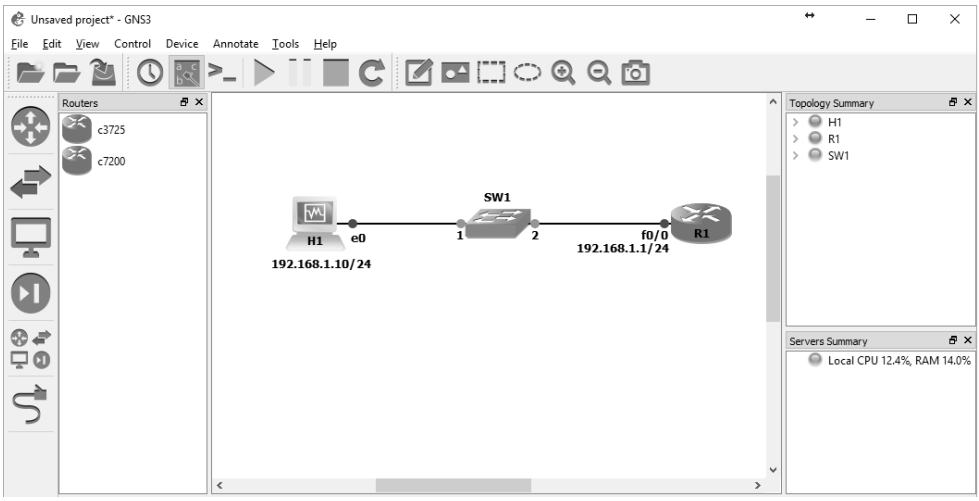
W programie GNS3 istnieje możliwość przechwycenia ruchu na dowolnym łączu, dzięki czemu użycie analizatora Wireshark jest niezwykle łatwe. W działaniu rzeczywistej sieci komputerowej przechwycenie ruchu pomiędzy np. dwoma routerami byłoby bardziej utrudnione, a w niektórych przypadkach niemożliwe. W przypadku GNS3 nie będzie z tym problemu.

Wykonaj taki sam projekt sieci jak na rysunku 4.1 i nadaj adresy IP zgodne z poniższymi.

Jeśli chcesz przechwycić ruch pomiędzy urządzeniami, kliknij prawym przyciskiem myszy np. na łączu pomiędzy stacją H1 oraz przełącznikiem SW1 i z menu podręcznego wybierz pozycję *Start capture* (rysunek 4.2).

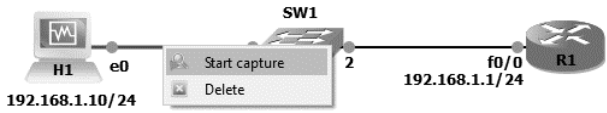
Na ekranie pojawi się okno *Packet capture* (rysunek 4.3), gdzie będziesz miał do wyboru interfejsy, na których chcesz rozpocząć przechwytywanie. W naszym przypadku jest to pozycja *SW1 port 1* należąca do przełącznika SW1 oraz pozycja *H1 port Ethernet0* należąca do stacji roboczej H1.

Oczywiście w naszym przypadku nie ma znaczenia, na którym interfejsie będziesz chciał przechwycić dane, ponieważ połączenie jest tylko pomiędzy dwoma urządzeniami. Lista ma znaczenie w momencie, gdy do interfejsu podłączonych jest więcej urządzeń.

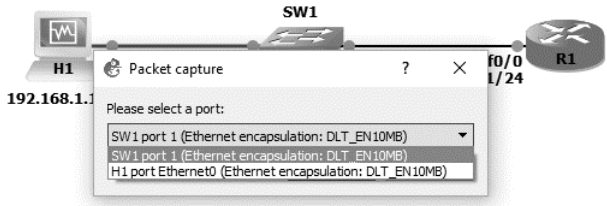


Rysunek 4.1. *Projekt prostej sieci*

Rysunek 4.2. *Rozpoczęcie przechwytywania*



Rysunek 4.3. *Wybór interfejsu*



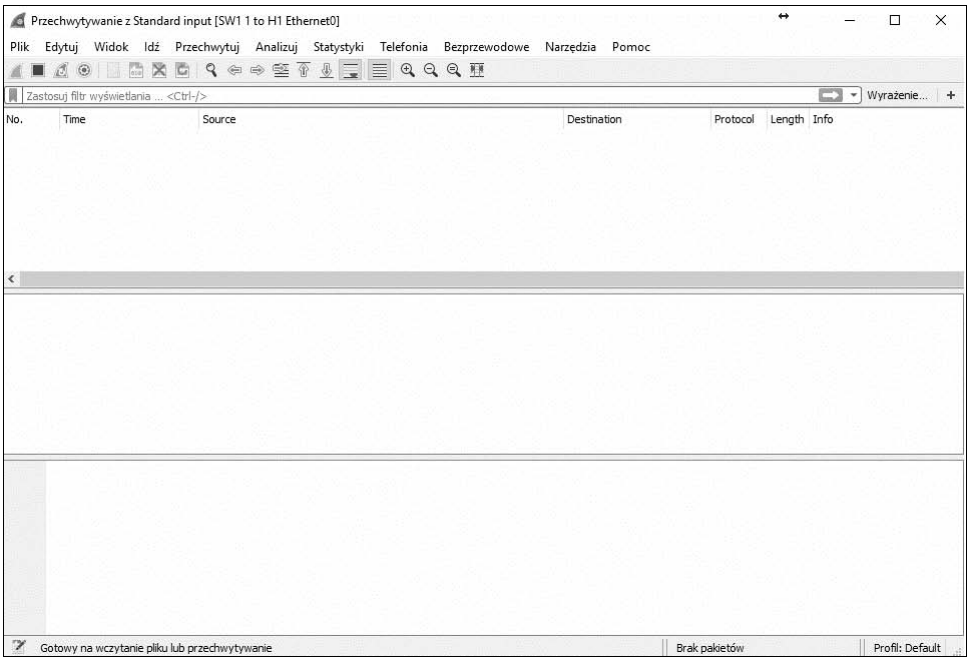
W tym przypadku wybierz pierwszą pozycję *SW1 port 1*. Następnie kliknij przycisk *OK*. Zostanie uruchomiony program Wireshark i na ekranie pojawi się jego okno główne (rysunek 4.4).

Przechwycone ramki pojawią się w oknie prawdopodobnie dopiero po kilku sekundach.

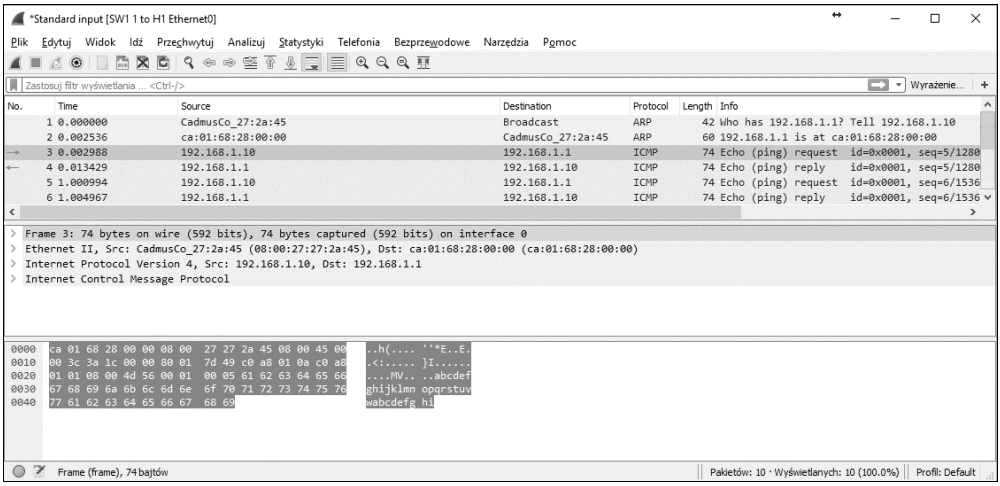
Aby zobaczyć konkretne ramki, które zostały przechwycone w programie Wireshark, należy wygenerować jakiś ruch. W związku z tym wykonaj test `ping` ze stacji roboczej H1 do routera.

Po chwili w oknie głównym programu Wireshark pojawią się pierwsze ramki (rysunek 4.5).

W programie zostały przechwycone ramki związane nie tylko z testem `ping` (komunikacja za pośrednictwem protokołu ICMP). Zauważ, że ramki z numerami 1 i 2 to ramki związane z ARP. Czyli w pierwszej kolejności stacja robocza przesyła zapytanie do sieci, aby uzyskać adres MAC urządzenia z adresem IP `192.168.1.1`. W ramce z numerem 2 urządzenie odpowiada i przesyła swój adres MAC. Dopiero po tym za pomocą ramki z numerem 3 rozpoczyna się komunikacja ICMP.



Rysunek 4.4. *Okno główne programu Wireshark*



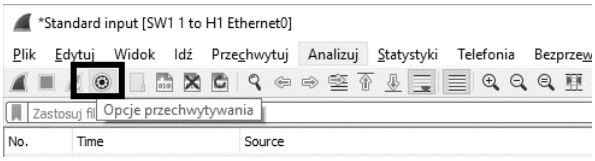
Rysunek 4.5. *Przechwycone dane przesłane pomiędzy stacją H1 i routerem R1*

Zauważ, że w oknie głównym znajduje się 7 kolumn. Patrząc od lewej strony, są to:

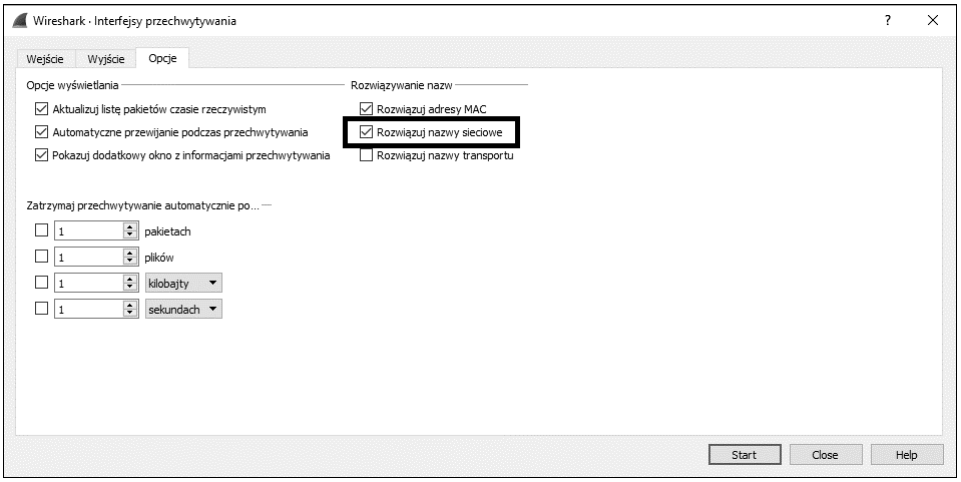
- *No.* — zawiera kolejny numer przechwyconej informacji.
- *Time* — pokazuje czas całego procesu przechwytywania.

- *Source* — pokazuje adres IP źródła informacji, która została przechwycona. W tym przypadku, jeśli analizujesz ruch dotyczący np. transmisji pochodzącej z serwera WWW, możesz nieco zmodyfikować wyświetlane informacje i sprawić, aby zamiast źródłowego adresu IP pojawiała się np. nazwa DNS. Znacznie ułatwi Ci to sprawdzanie i analizowanie otrzymanych informacji. W tym celu kliknij ikonę *Opcje przechwytywania* (rysunek 4.6).

Rysunek 4.6. *Ikona Opcje przechwytywania*



Pojawi się okno *Wireshark — Interfejsy przechwytywania* (rysunek 4.7). Przejdź do zakładki *Opcje* i zaznacz pozycję *Rozwiązuj nazwy sieciowe*, a następnie kliknij przycisk *Start*.



Rysunek 4.7. *Zakładka Opcje*

Aktualne okno zostanie zamknięte. Aby rozpocząć ponowne przechwytywanie, konieczne będzie zatrzymanie przechwytywania i ponowne jego uruchomienie.

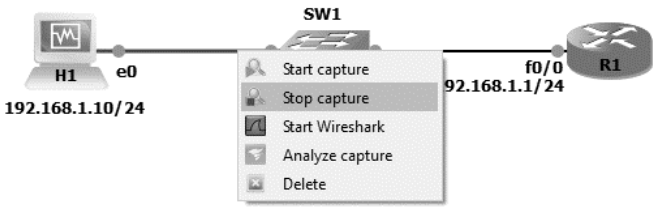
Podczas kolejnego przechwytywania w polu *Source* zamiast adresu IP zobaczysz nazwę serwera, który jest źródłem przechwyconej informacji. Oczywiście, jeśli przechwycona komunikacja nie dotyczy DNS, wówczas standardowo pojawi się adres IP.

- *Destination* — w tym polu znajduje się docelowy adres IP przesyłanej informacji. Podobnie jak w przypadku pola *Source*, tutaj pojawi się nazwa DNS (jeśli wykonałeś powyższe czynności).
- *Protocol* — w tym polu znajduje się informacja na temat wykorzystywanego protokołu.
- *Length* — ta kolumna zawiera informacje dotyczące długości przesyłanej ramki.

- *Info* — informuje, czego dotyczy przesyłana ramka. Mogą tutaj pojawić się informacje na temat numeru portu oraz inne charakteryzujące przesyłany rodzaj ruchu.

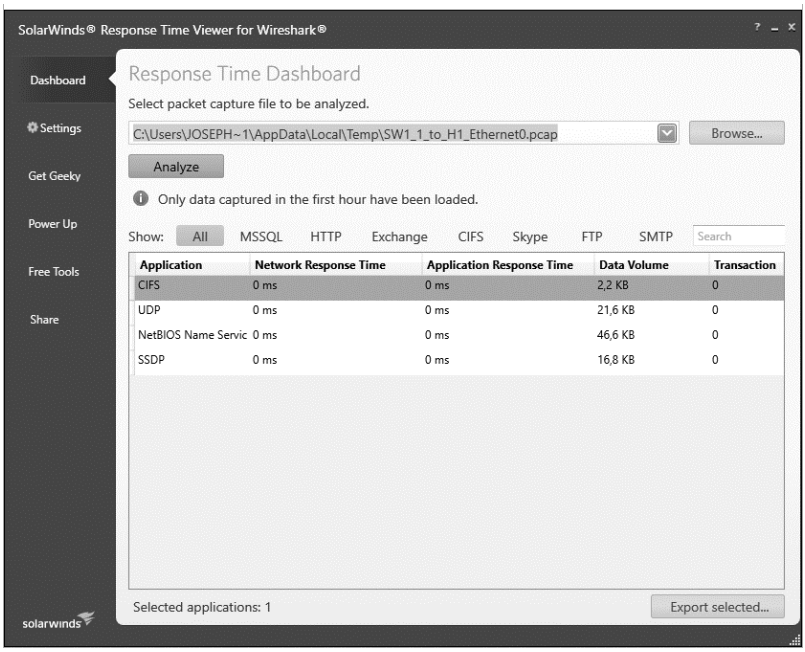
Aby zatrzymać przechwytywanie, należy kliknąć łącze prawym przyciskiem myszy i z menu podręcznego wybrać pozycję *Stop capture* (rysunek 4.8).

Rysunek 4.8. *Zatrzymanie przechwytywania*

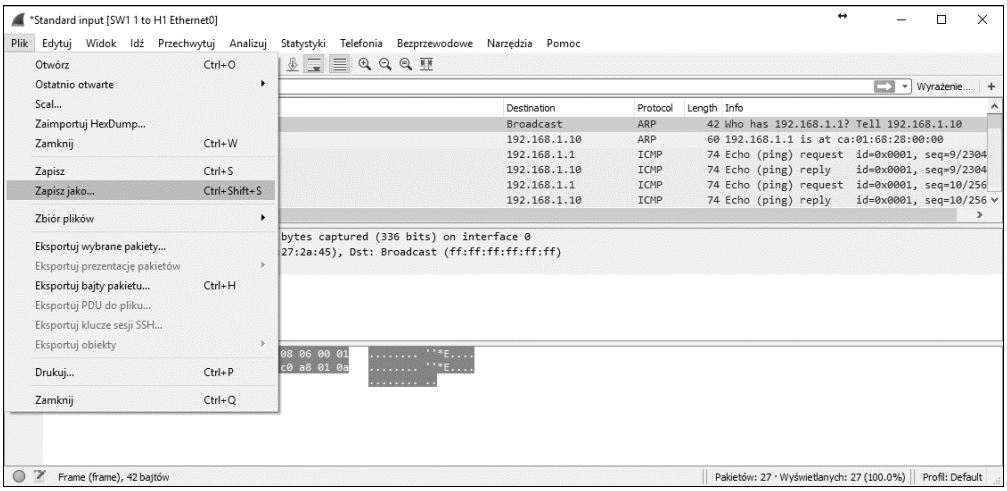


Jeśli po przechwyceniu informacji będziesz chciał przeanalizować je dokładniej, możesz, klikając na połączeniu prawym przyciskiem myszy, z menu podręcznego wybrać pozycję *Analyze capture*. Następnie w programie SolarWinds (rysunek 4.9), który również instalowany jest wraz z programem GNS3, będziesz mógł dokonać stosownych analiz.

Rysunek 4.9. *Analiza przechwyconych danych w programie SolarWinds*



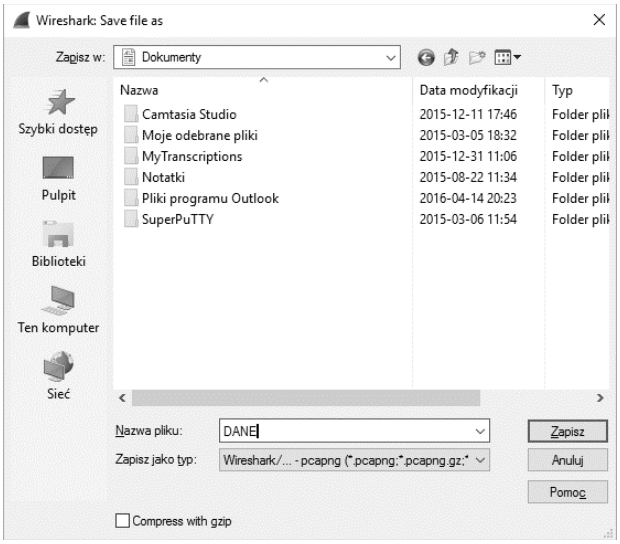
Jeśli chcesz zapisać wyniki oraz przechwycone dane w programie Wireshark, zatrzymaj przechwytywanie, kliknij menu *Plik* (rysunek 4.10) i wybierz pozycję *Zapisz jako*….



Rysunek 4.10. *Zapisywanie wyników*

W oknie *Wireshark: Save file as* (rysunek 4.11) podaj dowolną nazwę pliku oraz kliknij przycisk *Zapisz*. Po zapisaniu pliku z wynikami będziesz mógł w dowolnym czasie wrócić do przechwyconych danych oraz informacji na ich temat.

Rysunek 4.11. *Wybór lokalizacji do zapisania pliku*



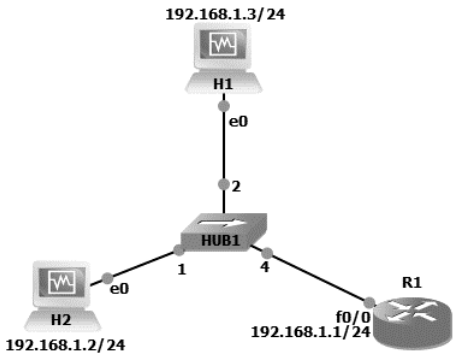
Wykorzystanie w GNS obiektu HUB

W GNS3 jednym z urządzeń, które również możesz wykorzystać, jest HUB, czyli tzw. koncentrator. Jest to urządzenie, które jeszcze kilkanaście lat temu było bardzo popularne niemalże w każdej sieci komputerowej. Obecnie zastąpił je przełącznik i HUB nie powinien być już używany. W GNS3 możesz go jednak wykorzystać chociażby do celów testowych

czy zaprezentowania sposobu jego działania, które polega na tym, że HUB za każdym razem po otrzymaniu ramki kopiuje ją na wszystkie swoje interfejsy. Dzięki temu każde urządzenie podłączone do HUB-a otrzymuje pełne dane związane z określoną transmisją.

Aby się o tym przekonać, wykonaj w programie GNS3poniższy prosty projekt. Wykorzystując obiekt HUB, najpierw uruchom wszystkie urządzenia i przydziel im adresy IP (rysunek 4.12).

Rysunek 4.12. *Projekt sieci komputerowej z obiektem HUB*



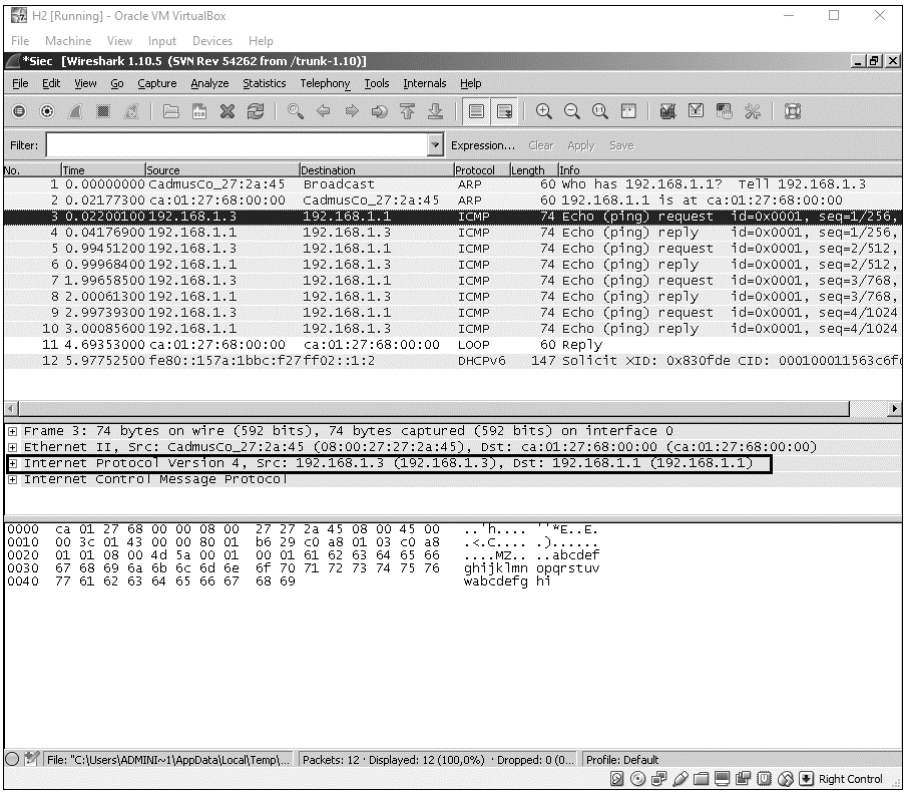
Następnie na stacji H1 uruchom program Wireshark, ewentualnie rozpocznij przechwytywanie ramek na łączu pomiędzy obiektem HUB i stacją roboczą H1. Potem ze stacji roboczej H2 wykonaj `ping` na adres interfejsu f0/0 routera R1, czyli w naszym przypadku na adres IP `192.168.1.1`.

Jak widzisz na poniższym listingu, test się powiódł.

```
Microsoft Windows [Wersja 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Wszelkie prawa zastrzeżone.
C:\Users\Administrator>ping 192.168.1.1
Badanie 192.168.1.1 z 32 bajtami danych:
Odpowiedź z 192.168.1.1: bajtów=32 czas=41ms TTL=255
Odpowiedź z 192.168.1.1: bajtów=32 czas=5ms TTL=255
Odpowiedź z 192.168.1.1: bajtów=32 czas=4ms TTL=255
Odpowiedź z 192.168.1.1: bajtów=32 czas=4ms TTL=255
Statystyka badania ping dla 192.168.1.1:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0
             (0% straty),
Szacunkowy czas błądzenia pakietów w milisekundach:
    Minimum = 4 ms, Maksimum = 41 ms, Czas średni = 13 ms
C:\Users\Administrator>
```

Następnie wróć do urządzenia H1, aby sprawdzić, jakie dane przechwycił Wireshark. Przypominam, że dane, które przed chwilą wygenerowałeś, były przeznaczone nie dla stacji H1, tylko dla routera.

Zauważ, że ramka oznaczona numerem 3 (rysunek 4.13) to nic innego jak ramka, w której adresem źródłowym IP jest adres stacji H2, natomiast docelowym adresem IP jest adres routera R1. Pomimo tego dane zostały przechwycone na stacji H1. Oznacza to, że HUB rzeczywiście kopiuje całą komunikację na wszystkie swoje interfejsy.

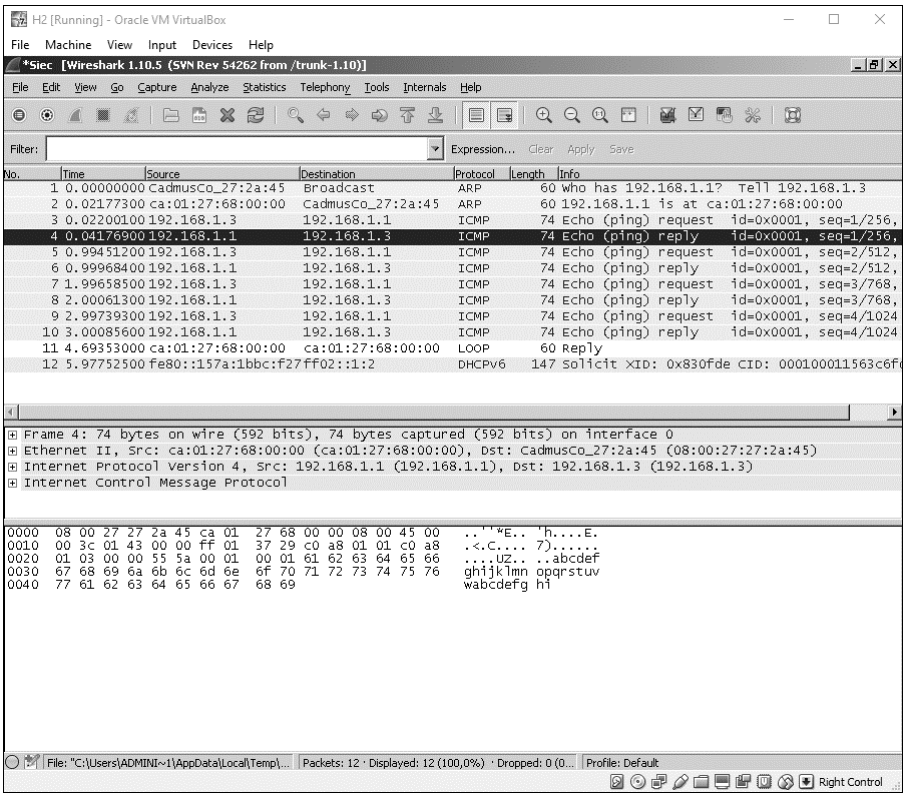


Rysunek 4.13. *Przechwycona komunikacja ze stacji H2 do routera*

Podobnie ma się sprawa z danymi przekazanymi w odpowiedzi, którą generuje router R1 do stacji H2. Jak widać, ramka z numerem 4 (rysunek 4.14) również została przechwycona, podobnie jak cała komunikacja występująca w tej sieci. Wiesz już więc, dlaczego urządzenia typu HUB nie powinno się wykorzystywać w sieciach komputerowych — po pierwsze, ze względów bezpieczeństwa, a po drugie, HUB-y generują bardzo wiele niepotrzebnego ruchu sieciowego.

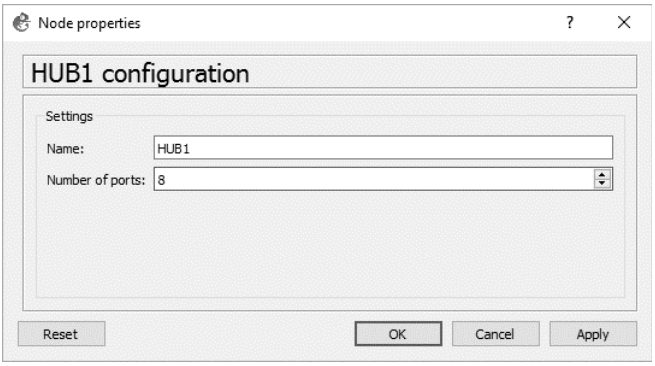
Jeśli w projektach w programie GNS3 zechcesz używać tego obiektu, możesz, klikając go prawym przyciskiem myszy i wybierając pozycję *Properties*, przejść do konfiguracji tego urządzenia (rysunek 4.15).

W konfiguracji w polu *Number of ports* możesz zwiększyć lub zmniejszyć ilość dostępnych interfejsów. Poza tym niczego zmienić nie możesz.



Rysunek 4.14. *Przechwycona komunikacja z routera przeznaczona dla stacji H2*

Rysunek 4.15. *Zmiana parametrów obiektu HUB*



Skorowidz

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z

GNS3

Sieci komputerowe już dawno oplotły świat, lecz wciąż okazuje się, że potrzeba ich więcej i więcej. W każdej firmie, domu, warsztacie i kawiarni musi działać sieć — i to taka, która zaspokoi potrzeby konkretnych użytkowników. Aby nauczyć się tworzyć takie sieci i łatwo testować ich przyszłe działanie, niezbędne jest dobre środowisko testowe, czyli GNS3. W tym programie możesz zbudować najróżniejsze sieci i przyjrzeć się ich działaniu bez konieczności zaplątywania się w kable. Dzięki temu możesz zabrać się do fizycznej budowy sieci dopiero wtedy, kiedy jej wirtualny odpowiednik spełni Twoje oczekiwania.

Jeśli chcesz nauczyć się obsługi programu GNS3 i zrozumieć, jak wygląda przepływ danych przez sieci komputerowe, a także rozpocząć przygotowania do egzaminu Cisco, sięgnij po tę książkę. Dowiesz się z niej, jak skonfigurować program, tworzyć wirtualne maszyny i routery oraz uruchamiać routing między nimi. Zobaczysz, do czego służy Wireshark i jak podglądać ruch między kluczowymi urządzeniami. Zadbasz także o bezpieczeństwo Twoich sieci oraz odkryjesz, jak emulować środowisko technologii VoIP oraz urządzenia Juniper. Wreszcie sprawdzisz, jak Twoja wirtualna sieć działa po podłączeniu jej do rzeczywistej sieci! Siadaj i projektuj!

- Wprowadzenie do GNS3, pobieranie i instalacja programu oraz wstępna konfiguracja
- Tworzenie wirtualnych maszyn i używanie ich w GNS3
- Tworzenie wirtualnego routera
- Wykorzystanie programu Wireshark w GNS3
- Zastosowanie GNS do emulacji urządzenia ASA
- Wykorzystanie GNS do VoIP
- Emulowanie urządzeń Juniper
- Dodatkowe funkcje GNS3

Śledź tę sieć i sam ją pleć!

sięgnij po WIĘCEJ

KOD KORZYŚCI

Helion

księgarnia internetowa

http://helion.pl

zamówienia telefoniczne

0 801 339900

0 601 339900

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
http://helion.pl

Sprawdź najnowsze promocje:
http://helion.pl/promocje
Książki najchętniej czytane:
http://helion.pl/bestsellery
Zamów informacje o nowościach:
http://helion.pl/nowosci

ISBN 978-83-283-2664-4

Informatyka w najlepszym wydaniu

cena: 49,00 zł