

Adam Józefiok

GNS3

Emulowanie
sieci komputerowych **Cisco**



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 Wydawnictwo HELION 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 Wydawnictwo HELION nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

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

Copyright © Helion 2017

Printed in Poland.

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

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

Spis treści

Wstęp	5
Rozdział 1. Wprowadzenie do GNS3, pobieranie i instalacja programu oraz wstępna konfiguracja	7
Wprowadzenie do programu	7
Wymagania sprzętowe	8
Pobieranie programu ze strony projektu	9
Instalacja programu GNS3	10
Ważniejsze funkcje i opcje	16
Obszar roboczy GNS3	18
Rozdział 2. Tworzenie wirtualnych maszyn i używanie ich w GNS3	21
Program Oracle VM VirtualBox	21
Tworzenie nowej maszyny wirtualnej	22
Podstawowe ustawienia maszyny wirtualnej	27
Dodatkowe ustawienia wirtualnej maszyny	32
Program VMware Workstation	35
Tworzenie nowej maszyny wirtualnej w VMware	37
Wykorzystanie VPCS	42
Uruchomienie maszyn wirtualnych w GNS3	44
Komunikacja stacji roboczych w GNS3	48
Emulowanie urządzeń Cisco L2 i L3 za pomocą IOU VM	52
Podłączenie urządzeń IOU do rzeczywistego przełącznika	62
Projekt z urządzeniami IOU i oprogramowaniem L3	64
Rozdział 3. Tworzenie wirtualnego routera	69
Przygotowanie IOS	69
Dodawanie routerów do obszaru roboczego i zmiana ustawień	73
Wartość Idle PC	77
Podłączenie routerów i uruchomienie prostej sieci	78
Połączenie wirtualnego routera z siecią rzeczywistą za pomocą obiektu Cloud	82
Emulowanie przełącznika Cisco	88
Konfiguracja CCP na stacji roboczej i podłączenie do routera uruchomionego w programie GNS3	101
Program SuperPuTTY i podłączenie do routerów	103

Rozdział 4. Wykorzystanie programu Wireshark w GNS3	107
Wykorzystanie w GNS obiekту HUB	112
Rozdział 5. Wykorzystanie GNS do emulacji połączeń WAN	117
Ogólnie o Frame-Relay	117
Konfiguracja enkapsulacji w przykładowym modelu punkt-punkt	118
Technologia Frame Relay w GNS3	121
Konfiguracja Frame Relay (hub-and-spoke) — multipoint	121
Konfiguracja Frame Relay (hub-and-spoke) — point-to-point	125
Samodzielna konfiguracja przełącznika Frame Relay	127
Konfiguracja ATM za pomocą obiektu ATM switch w GNS3	129
Rozdział 6. Wykorzystanie GNS do emulacji urządzenia ASA	133
Rozdział 7. Wykorzystanie GNS do VOIP	143
Wprowadzenie	143
Podłączenie wirtualnego routera VOIP oraz wirtualnych telefonów VOIP w programie GNS3	143
Podłączenie rzeczywistego telefonu do wirtualnego routera VOIP	154
Rozdział 8. Emulowanie urządzeń Juniper	157
Rozdział 9. Dodatkowe funkcjonalności GNS3	165
Konfiguracja zdalnego serwera IOS w GNS3	165
Umożliwienie zdalnej konfiguracji urządzeń w GNS3 z innej stacji roboczej	171
Przenoszenie konfiguracji pomiędzy routerami w GNS3 i rzeczywistymi urządzeniami	173
Tworzenie urządzenia Access Server	177
Tworzenie snapshot-ów i zarządzanie nimi	180
Skorowidz	185

Rozdział 4.

Wykorzystanie programu Wireshark w GNS3

Podczas instalacji GNS3 instaluje się również program Wireshark. Jest to darmowy snifer, 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.

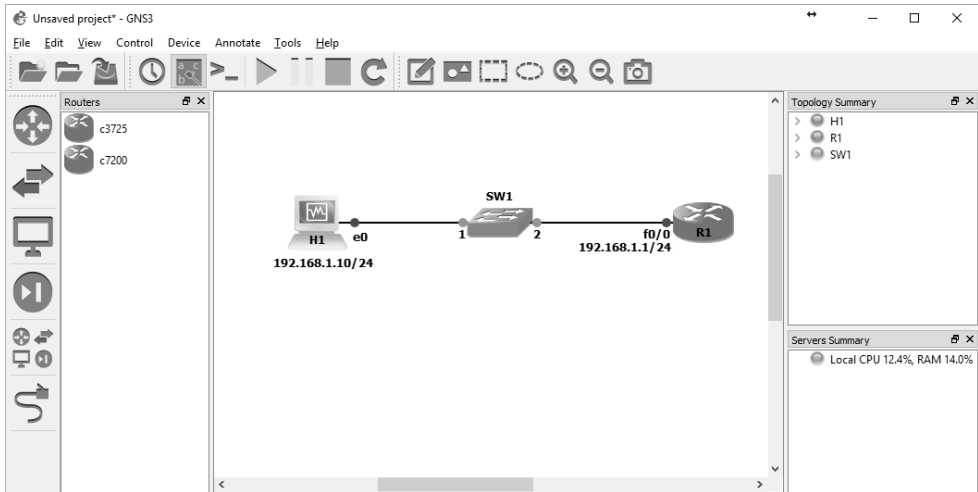
W programie GNS3 istnieje możliwość przechwycenia ruchu na dowolnym łączu, dzięki czemu użycie analizatora Wireshark jest niezwykle łatwe. W działaniu rzeczywistej sieci komputerowej przechwycenie ruchu pomiędzy np. dwoma routerami byłoby bardziej utrudnione, a w niektórych przypadkach niemożliwe. W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

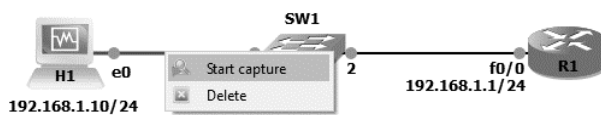
Na ekranie pojawi się okno *Packet capture* (rysunek 4.3), gdzie będziesz miał do wyboru interfejsy, na których chcesz rozpocząć przechwytywanie. W naszym przypadku jest to pozycja *SW1 port 1* należąca do przełącznika SW1 oraz pozycja *H1 port Ethernet0* należąca do stacji roboczej H1.

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.

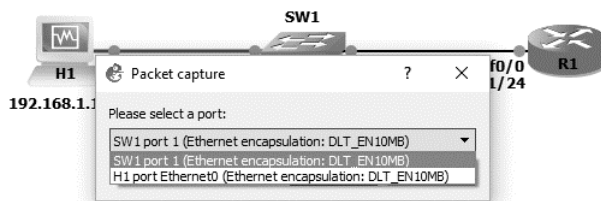


Rysunek 4.1. Projekt prostej sieci

Rysunek 4.2.
Rozpoczęcie
przechwytywania



Rysunek 4.3.
Wybór interfejsu



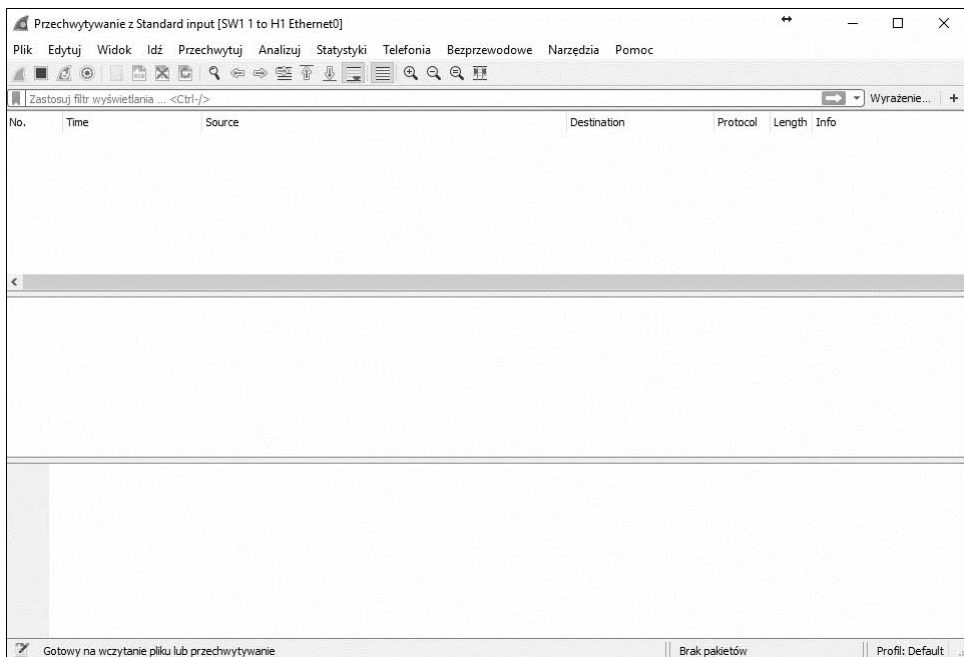
W tym przypadku wybierz pierwszą pozycję *SW1 port 1*. Następnie kliknij przycisk *OK*. Zostanie uruchomiony program Wireshark i na ekranie pojawi się jego okno główne (rysunek 4.4).

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

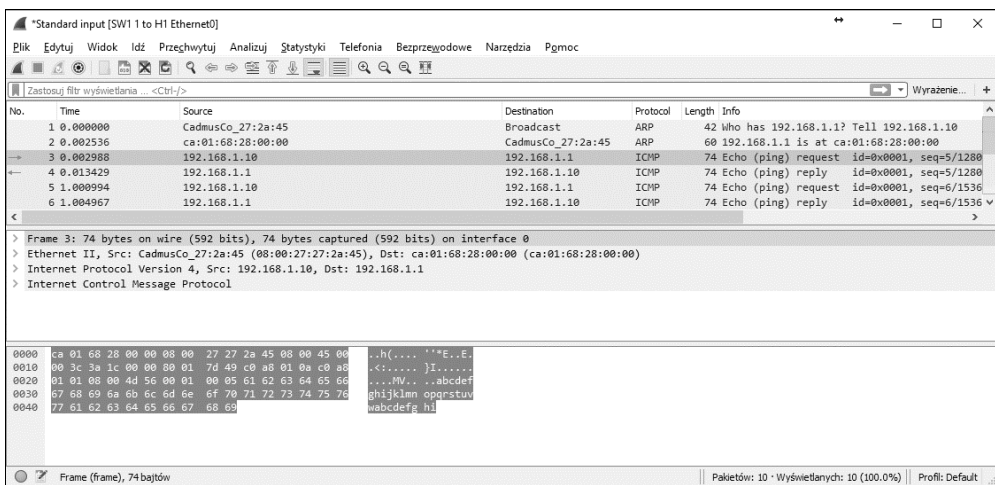
Aby zobaczyć konkretne ramki, które zostały przechwycone w programie Wireshark, należy wygenerować jakiś ruch. W związku z tym wykonaj test ping ze stacji roboczej H1 do routera.

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



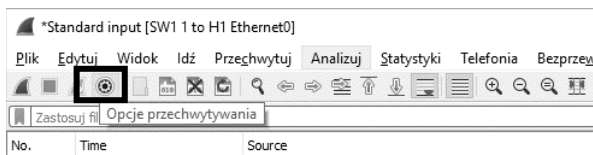
Rysunek 4.5. Przechwycone dane przesłane pomiędzy stacją H1 i routerem R1

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

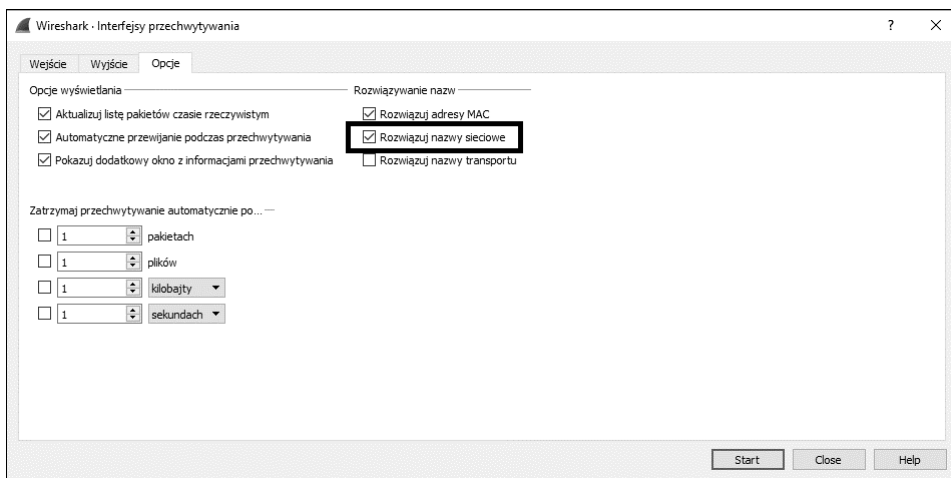
- ♦ *No.* — zawiera kolejny numer przechwyconej informacji.
- ♦ *Time* — pokazuje czas całego procesu przechwytywania.

- ◆ *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 *Rozwiąż 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.

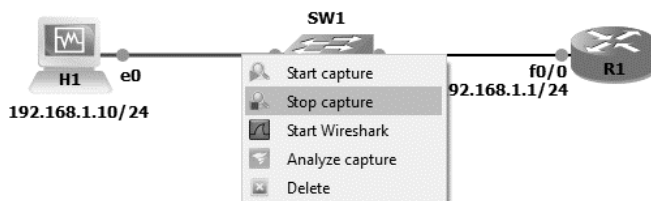
Podczas kolejnego przechwytywania w polu *Source* zamiast adresu IP zobaczysz nazwę serwera, który jest źródłem przechwyconej informacji. Oczywiście, jeśli przechwycona komunikacja nie dotyczy DNS, wówczas standardowo pojawi się adres IP.

- ◆ *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*

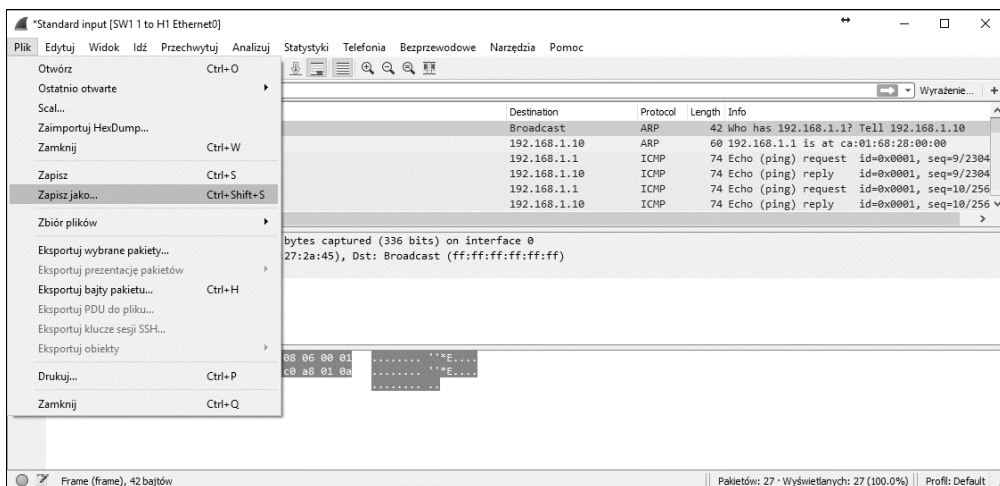


Jeśli po przechwyceniu informacji będziesz chciał przeanalizować je dokładniej, możesz, klikając na połączeniu prawym przyciskiem myszy, z menu podręcznego wybrać pozycję *Analyze capture*. Następnie w programie SolarWinds (rysunek 4.9), który również instalowany jest wraz z programem GNS3, będziesz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

Rysunek 4.9.
*Analiza
przechwyconych
danych
w programie
SolarWinds*

Application	Network Response Time	Application Response Time	Data Volume	Transaction
CIFS	0 ms	0 ms	2,2 KB	0
UDP	0 ms	0 ms	21,6 KB	0
NetBIOS Name Servic	0 ms	0 ms	46,6 KB	0
SSDP	0 ms	0 ms	16,8 KB	0

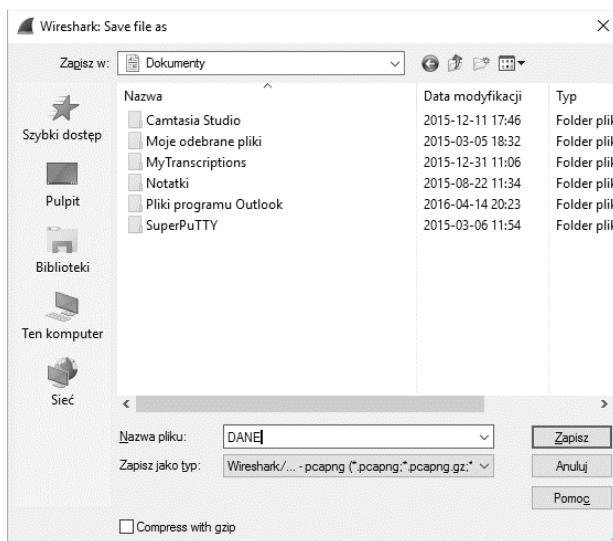
Jeśli chcesz zapisać wyniki oraz przechwycone dane w programie Wireshark, zatrzymaj przechwytywanie, kliknij menu *Plik* (rysunek 4.10) i wybierz pozycję *Zapisz jako....*



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 GNS3 obiektu HUB

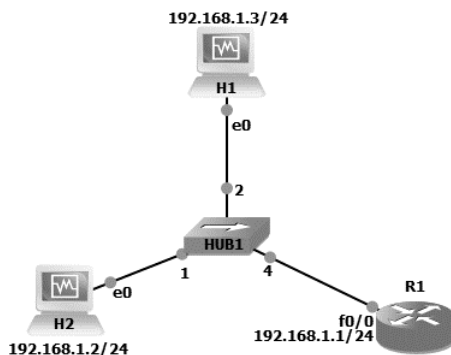
W GNS3 jednym z urządzeń, które również możesz wykorzystać, jest HUB, czyli tzw. koncentrator. Jest to urządzenie, które jeszcze kilkanaście lat temu było bardzo popularne niemalże w każdej sieci komputerowej. Obecnie zastąpił je przełącznik i HUB nie powinien być już używany. W GNS3 możesz go jednak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

The screenshot shows the Wireshark interface with the following details:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	CadmusCo_27:2a:45	Broadcast	ARP	60	who has 192.168.1.1? Tell 192.168.1.3
2	0.02177300	ca:01:27:68:00:00	CadmusCo_27:2a:45	ARP	60	192.168.1.1 is at ca:01:27:68:00:00
3	0.02200100	192.168.1.3	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=1/256
4	0.04176900	192.168.1.1	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256
5	0.099451200	192.168.1.3	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=2/512
6	0.09968400	192.168.1.1	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512
7	1.99658500	192.168.1.3	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=3/768
8	2.00061300	192.168.1.1	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768
9	2.99739300	192.168.1.3	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024
10	3.00085600	192.168.1.1	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024
11	4.69353000	ca:01:27:68:00:00	ca:01:27:68:00:00	LOOP	60	Reply
12	5.97752500	fe80::157a:1bbc:f27ff02::1:2		DHCPv6	147	Solicit XID: 0x830fde CID: 000100011563c6f

Selected packet details:

- Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
- Ethernet II, Src: cadmusco_27:2a:45 (08:00:27:27:2a:45), Dst: ca:01:27:68:00:00 (ca:01:27:68:00:00)
- Internet Protocol Version 4, Src: 192.168.1.3 (192.168.1.3), Dst: 192.168.1.1 (192.168.1.1)
- Internet Control Message Protocol

Packet bytes:

```

0000 ca 01 27 68 00 00 08 00 27 27 2a 45 08 00 45 00 ..h....''*E..E.
0010 00 3c 01 43 00 00 80 01 b6 29 c0 a8 01 03 c0 a8 <.C....).).....
0020 01 01 08 00 4d 5a 00 01 00 01 61 62 63 64 65 66 ...MZ...abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmnpqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcedfg hi

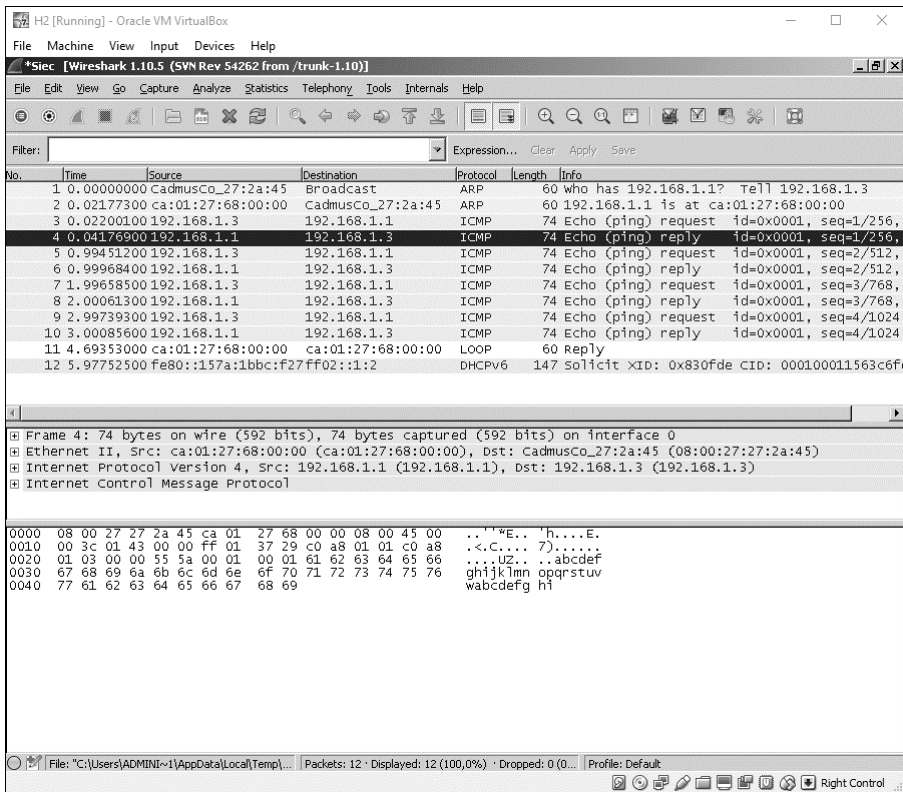
```

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.

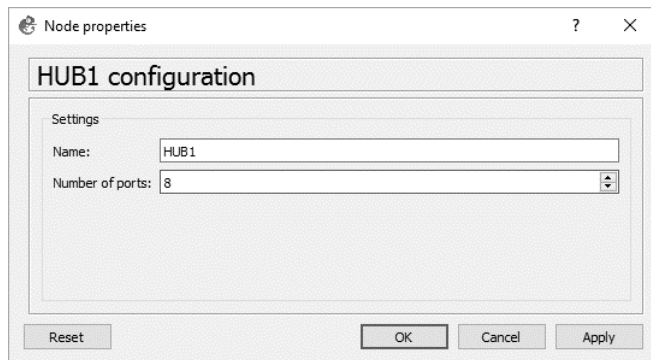
Jeśli w projektach w programie GNS3 zechcesz używać tego obiektu, możesz, klikając go prawym przyciskiem myszy i wybierając pozycję *Properties*, przejść do konfiguracji tego urządzenia (rysunek 4.15).

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

A

Access Server, 177
Adaptive Security Appliance, *Patrz:* ASA
adres

- DLCI, *Patrz:* DLCI
- domyślnej bramy, 90
- IP, 90, 108, 110, 125
 - publiczny, 94
 - wykluczanie, 145
- MAC, 108, 121

ARP, 108
ASA, 133

- emulacja, 133
- podłączanie do rzeczywistej sieci, 139, 140, 141

ASDM, 140
ATM, 118
ATM Switch, 129

B

biblioteka WinPCAP, 11

C

CCP, 101

- konfiguracja, 103

CCP Express, 97, 99
Challenge Handshake Authentication Protocol,
Patrz: uwierzytelnienie CHAP
circuit switched, *Patrz:* przełączanie obwodów
Cpulimit, 13

D

danych kompresowanie, 119
Data Communications Equipment,
Patrz: urządzenie DCE

Data Terminal Equipment, *Patrz:* urządzenie DTE
Data-Link Connection Identifier, *Patrz:* DLCI
DLCI, 118, 121
DNS, 110
Dynamips, 8

E

emulator QEMU, *Patrz:* QEMU
enkapsulacja, 92, 120, 155

- frame-relay, 122, 123, 126
- HDLC, 118, 119
- PPP, 118, 119, 120

F

firewall, 133
Frame Relay, 118, 121

- identyfikator, *Patrz:* DLCI

G

gniazdo compact flash, 69
GNS3

- instalacja, 10
- konfiguracja, 17, 18
- obszar roboczy, 18, 19, 73, 74
- portal, 9
- serwer, 165
- uruchamianie, 16

Guest Additions, 34

H

hasło, 120
High-level Data Link Control, *Patrz:* enkapsulacja
HDLC
HUB, 112, 114

I

IDLEPC, 13, 77
interfejs
 A-8E, 8
 ATM, 129
 AUI, 76
 FastEthernet, 76
 graficzny, 97
 identyfikator, 78
 konfiguracja, 121
 punkt-punkt, 121, 125
 wielopunkt, 121
 loopback, 85, 97, 139
 PA-2FE-TX, 8
 PA-4E, 8
 PA-4T+, 8
 PA-8T, 8
 PA-A1, 8
 PA-FE-TX, 8
 PA-GE, 8
 PA-POS-OC3, 8
 przechwytywanie ruchu sieciowego, 107, 110,
 111, 112, 113
 szeregowy, 76, 118
 trunkowy, 93, 155
 VLAN1, 154
IOS, 69
 konfiguracja, 70
 obraz, 70, 72
 wersja, 70
IOU VM, 52

J

Juniper, 157
Juniper Olive, 157

K

karta
 loopback, 86
 NM-16ESW, 8, 76
 NM-1E, 8, 76
 NM-1FE-TX, 8, 76
 NM-4E, 8, 76
 NM-4T, 8, 76
 sieciowa wirtualna, 30
 WIC, 71
 WIC-1ENET, 8
 WIC-1T, 8
 WIC-2T, 8
 z portem

Ethernet, 8
 szeregowym, 8, *Patrz też:* karta WIC-1T,
 karta WIC-2T

klient DHCP, 84
komenda
 broadcast, 124
 clock rate, 119, 128
 encapsulation frame-relay, 122, 126, 127
 ephone, 152
 format flash, 98, 145
 frame-relay interface-dlci, 126
 frame-relay map, 124, 125
 frame-relay switching, 127
 interface, 126
 ip default-gateway, 90
 ip dhcp excluded-address, 145
 ip http server, 99
 ip nat inside, 95
 ip nat outside, 95
 ip source-address, 147
 login local, 99
 mac-address, 152
 ping, 90
 show ephone, 152
 show frame-relay map, 124
 show interface, 119
 show ip nat transpation, 96
 switchport mode trunk, 92, 155
 switchport trunk encapsulation, 92
 telephony-service, 147
koncentrator, *Patrz:* HUB
kopia migawkowa, 181

L

leased line, *Patrz:* linia dzierżawiona
linia
 dzierżawiona, 117
 wirtualna, 99

Link Control Protocol, *Patrz:* protokół LCP
login, 120

M

mapowanie statyczne, 124
maszyna wirtualna, 21
 dysk twardy, 23, 24, 25
 IOU VM, 52
 komunikacja, 51
 sterowniki, 34
 tworzenie, 22, 37
 ustawienia, 27, 28, 30, 31, 32
 VPCS, *Patrz:* VPCS

model ISO/OSI, 107, 118

moduł

NPE-225, 8

NPE-400, 8

NPE-G2, 8

MPLS, 118

multipoint, *Patrz:* interfejs konfiguracja wielopunkt

N

Network Control Protocol, *Patrz:* protokół NCP

Npcap, 12

O

obiekt

ATM Switch, 129

Cloud, 82, 83, 87, 91, 94, 139

obwód, 118

P

packet switched, *Patrz:* przełączanie pakietów

pakiet, 12

pamięć

flash, 69

formatowanie, 98

powiększanie, 97

nieulotna, 70

RAM, 23, 30, 70

ulotna, 70

Password Authentication Protocol, *Patrz:*

uwierzytelnienie PAP

PAT, 94, 96

pętla zwrotna, 85

plik

.bin, 70

asa842-initrd.gz, 133

asa842-vmlinuz, 133

point-to-point, *Patrz:* interfejs konfiguracja punkt-punkt

Point-to-Point Protocol, *Patrz:* enkapsulacja PPP

polecenie, *Patrz:* komenda

połączenie trunk, 89

port

ATM, 8

Ethernet, 8

Fast Ethernet, 8

Gigabit Ethernet, 8

szeregowy, 8

światłowodowy, 8

Port Channel, 89

procesor sterowanie obciążeniem, 13

program

GNS3, *Patrz:* GNS3

snifujący, 11

Wireshark, *Patrz:* Wireshark

protokół, 110

ICMP, 108

LCP, 119

NCP, 119

routingu, 79

RIP, 80

uwierzytelnienie, *Patrz:* uwierzytelnienie

przełączanie

obwodów, 117

pakietów, 117

przełącznik, 8, 49, 112, 157

ATM, 129

emulowanie w UNIX, 52

Frame Relay, 118, 121

konfiguracja, 127, 128

symulowanie, 121, 122

rzeczywisty, 61, 91

konfiguracja, 92

sieciowy, 76

wirtualny, 88

Q

QEMU, 13

QoS, 89

R

ramka, 107

enkapsulacja, *Patrz:* enkapsulacja

przechwytywanie, 108, 113, 114

przełącznik, 128

router, 8, 69, 72, 157

Access Server, *Patrz:* Access Server

emulowanie w UNIX, 52

komunikacja, 79

konfiguracja, 161, 162

przenoszenie na urządzenie rzeczywiste, 173

łączenie, 118

podłączenie do sieci rzeczywistej, 82, 83, 84, 85

przechwytywanie ruchu sieciowego, 113, 114

ustawienia, 73, 74, 75, 81, 82

VOIP, 154

S

serwer
 CUCM, 143
 DHCP, 84, 85, 93, 145
 HTTP, 99
 TFTP, 98, 146
 zdalny, 165, 171

sieć
 ATM, 129
 Ethernet, 121
 LAN, 95, 117
 VLAN, 88
 WAN, 117, 118

snapshot, 181

snifer, 107

Solar Winds Response, 13

Spanning-Tree, 89

stacja robocza, 13, 95
 komunikacja, 48
 wirtualna, 13, 88

SuperPuTTY, 13, 103

system
 operacyjny, 69
 aktualizacja, 69
 IOS, *Patrz:* IOS
 JunOS, 157
 wirtualizacja, 22, 36
 UNIX, 52

T

telefon
 rzeczywisty, 154
 VOIP, 145, 152
 plik konfiguracyjny, 146
 wirtualny, 143

test ping, 108, 124

TightVNC Viewer, 13

transmisji szyfrowanie, 118

trasa statyczna, 79, 95, 163

U

urządzenie
 Access Server, *Patrz:* Access Server
 DCE, 118, 121, 128
 DTE, 118
 Juniper, 157
 sieciowe, 7
 emulacja, 7
 wirtualizacja, 7

usługa PAT, *Patrz:* PAT

uwierzytelnienie
 CHAP, 119, 120
 PAP, 119, 120

V

VirtualBox, 21, 48

VMware, 35, 36, 48

Voice Port, 89

VOIP, 143

VPCS, 13, 42, 48
 uruchamianie, 44

W

wartość IDLEPC, 13, 77

WinPCAP, 11

Wireshark, 8, 12, 107

wirtualizacja, 21, 36

Z

zapora sieciowa, 157

PROGRAM PARTNERSKI

GRUPY WYDAWNICZEJ 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>

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!

Helion

księgarnia internetowa



<http://helion.pl>

zamówienia telefoniczne



0 801 339900



0 601 339900

Informatyka w najlepszym wydaniu

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>

sięgnij po **WIĘCEJ**



KOD KORZYŚCI

ISBN 978-83-283-2664-4



9 788328 326644

cena: 49,00 zł