

# Wojskowa Akademia Techniczna



Prowadzący: mgr inż. Kamil Renczewski

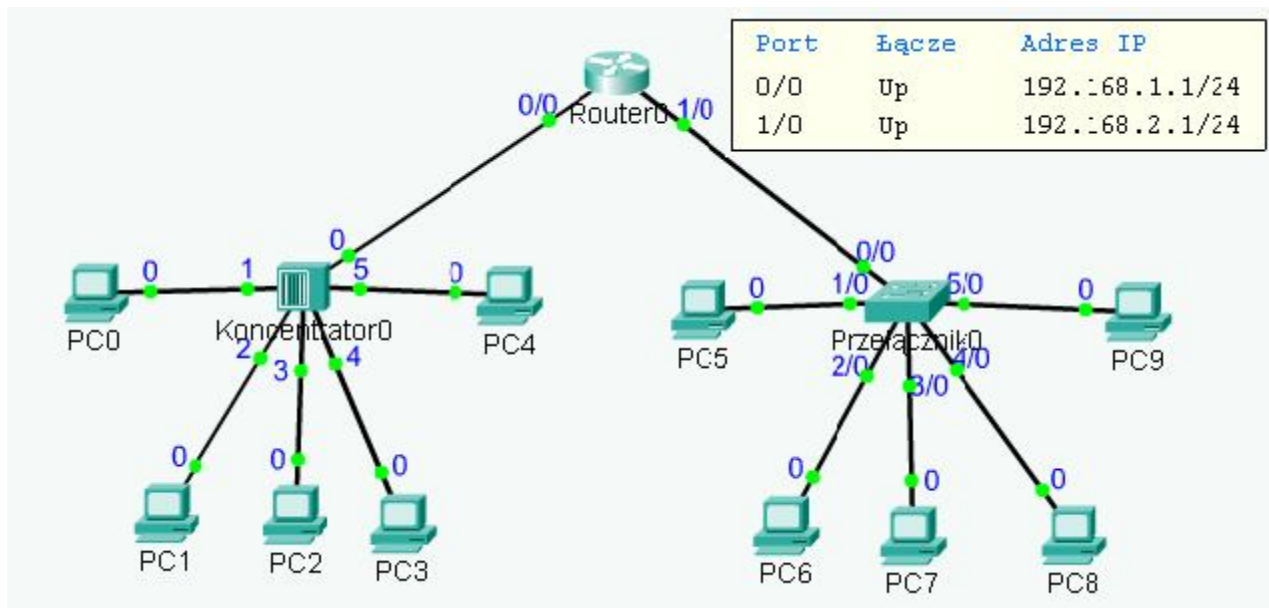
Grupa szkoleniowa: I7G2S1

Autorzy: Darnikowski Przemysław  
Oknińska Elżbieta  
Piersa Kamil  
Piotrowski Krzysztof  
Pol Grzegorz  
Złamański Tomasz

Data wykonania: 12.01.2010r.

Temat: Konfigurowanie sieci komputerowej przy wykorzystaniu koncentratora

Tworzymy wycinek sieci komputerowej pokazanej na poniższym rysunku obejmującej koncentrator. Interfejsy routera Router0 są skonfigurowane zgodnie z danymi podanymi w ramce na rysunku.



```

C:\WINDOWS\system32\cmd.exe
Konfiguracja IP systemu Windows

Karta Ethernet Połączenie lokalne 2:
Sufiks DNS konkretnego połączenia :
Adres IP. . . . . : 192.168.1.38
Maska podsieci. . . . . : 255.255.255.0
Brama domyślna. . . . . : 192.168.1.1

C:\Documents and Settings\Administrator>ping 192.168.1.36
Badanie 192.168.1.36 z 32 bajtami danych:

Odpowiedź z 192.168.1.36: bajtów=32 czas=4ms TTL=128
Odpowiedź z 192.168.1.36: bajtów=32 czas=1ms TTL=128
Odpowiedź z 192.168.1.36: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 192.168.1.36: bajtów=32 czas<1 ms TTL=128

Statystyka badania ping dla 192.168.1.36:
Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
Szacunkowy czas błędzenia pakietów w milisekundach:
Minimum = 0 ms, Maksimum = 4 ms, Czas średni = 1 ms

C:\Documents and Settings\Administrator>ping 192.168.1.44
Badanie 192.168.1.44 z 32 bajtami danych:

Odpowiedź z 192.168.1.44: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 192.168.1.44: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 192.168.1.44: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 192.168.1.44: bajtów=32 czas<1 ms TTL=128

Statystyka badania ping dla 192.168.1.44:
Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
Szacunkowy czas błędzenia pakietów w milisekundach:
Minimum = 0 ms, Maksimum = 0 ms, Czas średni = 0 ms

C:\Documents and Settings\Administrator>ping 192.168.1.42
Badanie 192.168.1.42 z 32 bajtami danych:

Odpowiedź z 192.168.1.42: bajtów=32 czas=2ms TTL=128
Odpowiedź z 192.168.1.42: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 192.168.1.42: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 192.168.1.42: bajtów=32 czas=6ms TTL=128

Statystyka badania ping dla 192.168.1.42:
Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
Szacunkowy czas błędzenia pakietów w milisekundach:
Minimum = 0 ms, Maksimum = 6 ms, Czas średni = 2 ms
    
```

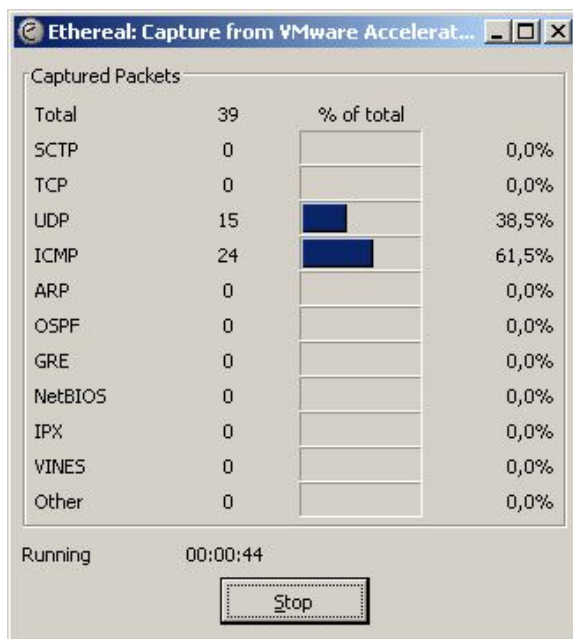
Skonfigurowaliśmy komputery PC1-PC4. Adresy IP podajemy poniżej.

Numer Komputera	IP
PC1	192.168.1.36
PC2	192.168.1.38
PC3	192.168.1.42
PC4	192.168.1.44

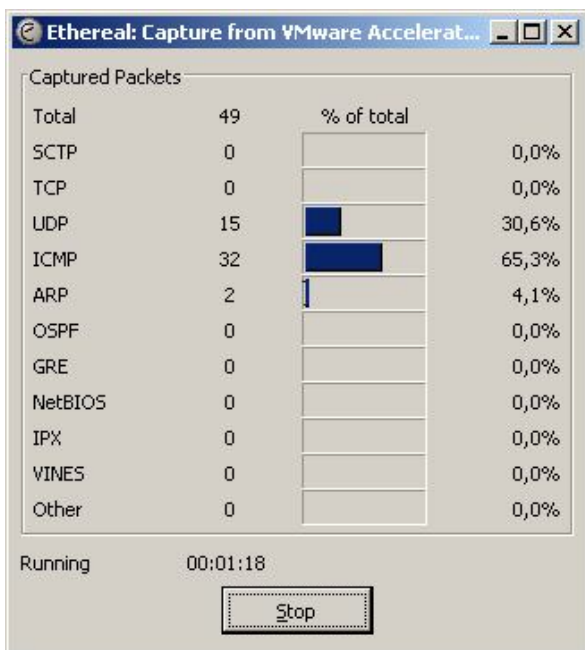
Następnie sprawdziliśmy wzajemną osiągalność. Obraz konsoli po pingowaniu znajduje się po lewej stronie

Na węzłach PC1-PC4 uruchomiliśmy program do przechwytywania ramek Ethereal. Sprawdziliśmy wzajemną osiągalność wszystkich komputerów PC1-PC4. Następnie pingowaliśmy komputer PC2 i w w/w programie sprawdzaliśmy przechwytywanie ramek. Udało się przechwycić ramki ICMP i ARP. Jednocześnie na innych komputerach w sieci, które nie pingowały ani nie były pingowane został zaobserwowany ruch sieciowy, ponieważ koncentrator w odróżnieniu od switcha wysyła pakiety na wszystkie swoje porty, a nie tylko na porty do których są podłączone odbiorcy pakietów. Poniższe statystyki pokazują, że protokół ARP służy do sprawdzania kto chce nas zpingować a protokół ICMP to pojedynczy pakiet – pytanie – odpowiedź.

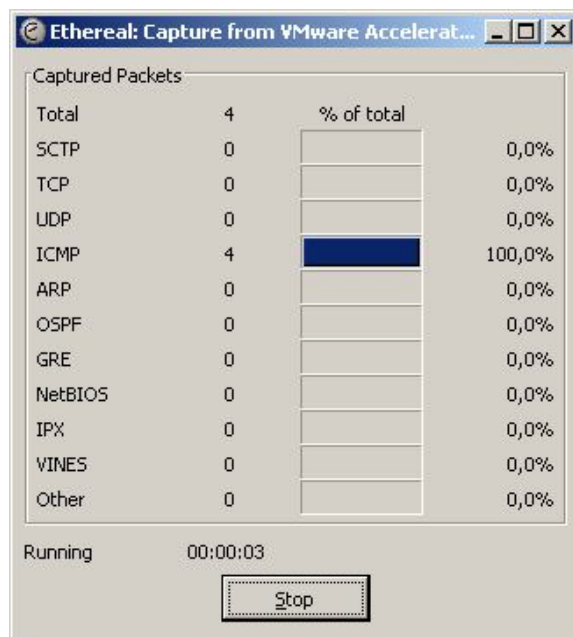
Pingowanie z adresu 192.168.1.42



Pingowanie z adresu 192.168.1.36



Pingowanie z adresu 192.168.1.44



Poniżej prezentujemy statystyki z programu Ethereal. Zamiast protokołu UDP program wskazuje serwer NetBios NBNS. Powodem tego jest to, że metoda rozpoznawania nazw węzła-p do komunikowania się z serwerem NBNS używa kierowanych datagramów UDP (User Datagram Protocol). ARP jest to metoda znajdowania adresu sprzętowego hosta, gdy dany jest adres warstwy sieciowej. ICMP to pojedynczy pakiet pytanie – odpowiedź.

(Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

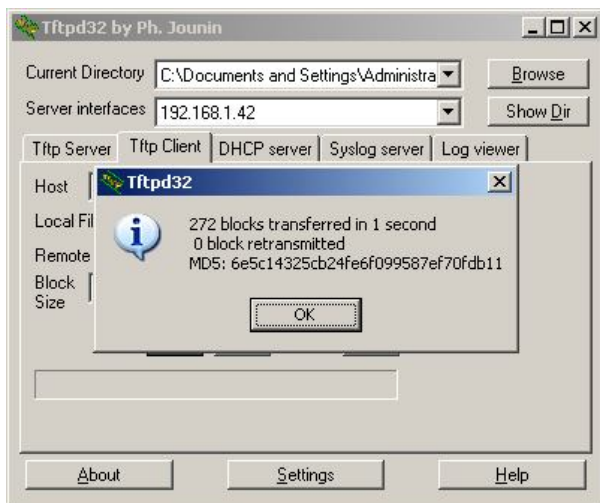
Filter: Expression... Clear Apply

No. ↓	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.42	192.168.1.38	ICMP	Echo (ping) request
2	0.000050	192.168.1.38	192.168.1.42	ICMP	Echo (ping) reply
3	0.989701	192.168.1.42	192.168.1.38	ICMP	Echo (ping) request
4	0.989737	192.168.1.38	192.168.1.42	ICMP	Echo (ping) reply
5	1.975768	192.168.1.42	192.168.1.38	ICMP	Echo (ping) request
6	1.975804	192.168.1.38	192.168.1.42	ICMP	Echo (ping) reply
7	2.993835	192.168.1.42	192.168.1.38	ICMP	Echo (ping) request
8	2.993889	192.168.1.38	192.168.1.42	ICMP	Echo (ping) reply
9	6.565119	192.168.1.44	192.168.1.38	ICMP	Echo (ping) request
10	6.565170	192.168.1.38	192.168.1.44	ICMP	Echo (ping) reply
11	7.527888	192.168.1.44	192.168.1.38	ICMP	Echo (ping) request
12	7.527917	192.168.1.38	192.168.1.44	ICMP	Echo (ping) reply
13	8.537919	192.168.1.44	192.168.1.38	ICMP	Echo (ping) request
14	8.538039	192.168.1.38	192.168.1.44	ICMP	Echo (ping) reply
15	9.544260	192.168.1.44	192.168.1.38	ICMP	Echo (ping) request
16	9.544297	192.168.1.38	192.168.1.44	ICMP	Echo (ping) reply
17	25.246646	192.168.1.44	192.168.1.255	BROWSE	Get Backup List Request
18	25.246939	192.168.1.44	192.168.1.255	NBNS	Name query NB GRUPA_ROBOCZA<1b>
19	26.018893	192.168.1.44	192.168.1.255	NBNS	Name query NB GRUPA_ROBOCZA<1b>
20	26.772816	192.168.1.44	192.168.1.255	NBNS	Name query NB GRUPA_ROBOCZA<1b>
21	29.537595	192.168.1.44	192.168.1.255	BROWSE	Get Backup List Request
22	29.537712	192.168.1.44	192.168.1.255	NBNS	Name query NB GRUPA_ROBOCZA<1b>
23	30.276673	192.168.1.44	192.168.1.255	NBNS	Name query NB GRUPA_ROBOCZA<1b>
24	30.996518	192.168.1.44	192.168.1.255	NBNS	Name query NB GRUPA_ROBOCZA<1b>
25	33.771405	192.168.1.44	192.168.1.255	BROWSE	Get Backup List Request
26	33.771425	192.168.1.44	192.168.1.255	NBNS	Name query NB GRUPA_ROBOCZA<1b>
27	34.483035	192.168.1.44	192.168.1.255	NBNS	Name query NB GRUPA_ROBOCZA<1b>
28	35.305154	192.168.1.44	192.168.1.255	NBNS	Name query NB GRUPA_ROBOCZA<1b>
29	37.985994	192.168.1.44	192.168.1.255	NBNS	Name query NB GRUPA_ROBOCZA<1e>
30	38.073918	192.168.1.44	192.168.1.38	ICMP	Echo (ping) request
31	38.074602	192.168.1.38	192.168.1.44	ICMP	Echo (ping) reply
32	38.737979	192.168.1.44	192.168.1.255	NBNS	Name query NB GRUPA_ROBOCZA<1e>
33	39.079750	192.168.1.44	192.168.1.38	ICMP	Echo (ping) request
34	39.079782	192.168.1.38	192.168.1.44	ICMP	Echo (ping) reply
35	39.549686	192.168.1.44	192.168.1.255	NBNS	Name query NB GRUPA_ROBOCZA<1e>
36	40.073860	192.168.1.44	192.168.1.38	ICMP	Echo (ping) request
37	40.073886	192.168.1.38	192.168.1.44	ICMP	Echo (ping) reply
38	41.075693	192.168.1.44	192.168.1.38	ICMP	Echo (ping) request
39	41.075724	192.168.1.38	192.168.1.44	ICMP	Echo (ping) reply
40	62.289406	192.168.1.36	192.168.1.38	ICMP	Echo (ping) request
41	62.289455	192.168.1.38	Broadcast	ARP	who has 192.168.1.36? Tell 192.168.1.38
42	62.289779	192.168.1.36	192.168.1.38	ARP	192.168.1.36 is at 00:0c:29:6c:d1:66
43	62.289791	192.168.1.38	192.168.1.36	ICMP	Echo (ping) reply
44	65.910394	192.168.1.36	192.168.1.38	ICMP	Echo (ping) request
45	65.910442	192.168.1.38	192.168.1.36	ICMP	Echo (ping) reply
46	69.569077	192.168.1.36	192.168.1.38	ICMP	Echo (ping) request
47	69.569138	192.168.1.38	192.168.1.36	ICMP	Echo (ping) reply
48	73.092788	192.168.1.36	192.168.1.38	ICMP	Echo (ping) request
49	73.092838	192.168.1.38	192.168.1.36	ICMP	Echo (ping) reply
50	77.106798	192.168.1.42	192.168.1.255	BROWSE	Get Backup List Request
51	77.106931	192.168.1.42	192.168.1.255	NBNS	Name query NB GRUPA_ROBOCZA<1b>
52	77.835765	192.168.1.42	192.168.1.255	NBNS	Name query NB GRUPA_ROBOCZA<1b>
53	78.640526	192.168.1.42	192.168.1.255	NBNS	Name query NB GRUPA_ROBOCZA<1b>
54	81.391937	192.168.1.42	192.168.1.255	BROWSE	Get Backup List Request
55	81.391967	192.168.1.42	192.168.1.255	NBNS	Name query NB GRUPA_ROBOCZA<1b>
56	82.084247	192.168.1.42	192.168.1.255	NBNS	Name query NB GRUPA_ROBOCZA<1b>
57	82.842248	192.168.1.42	192.168.1.255	NBNS	Name query NB GRUPA_ROBOCZA<1b>
58	85.577870	192.168.1.42	192.168.1.255	BROWSE	Get Backup List Request

File: "C:\DOCUME~1\ADMINI~1\USTAWI~1\T | P: 64 D: 64 M: 0 Drops: 0

Na każdym komputerze uruchomiliśmy serwer TFTP. Nie sprawdziliśmy możliwości kopiowania plików za pomocą komendy tftp ze względu na to, że korzystaliśmy z programu Tftpd32 posiadającego własny interfejs graficzny. Poniżej prezentujemy screeny z programu podczas wysyłania z komputer PC3 na komputer PC2 pliku wraz z informacją o udanym transferze.

Wysyłanie pliku z PC3.

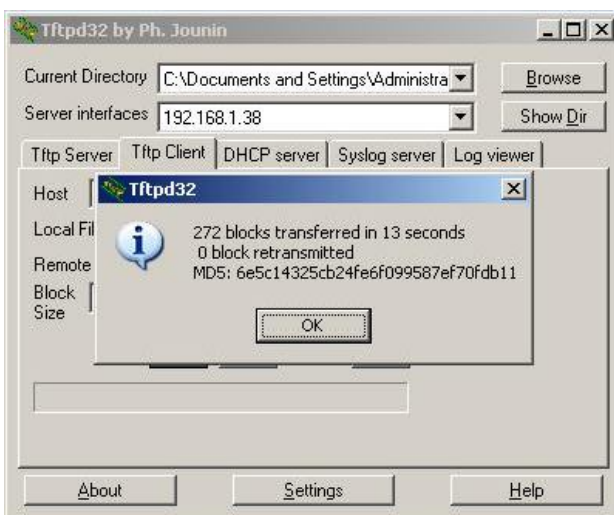


Odbieranie na komputerze PC2 pliku z komputera PC3

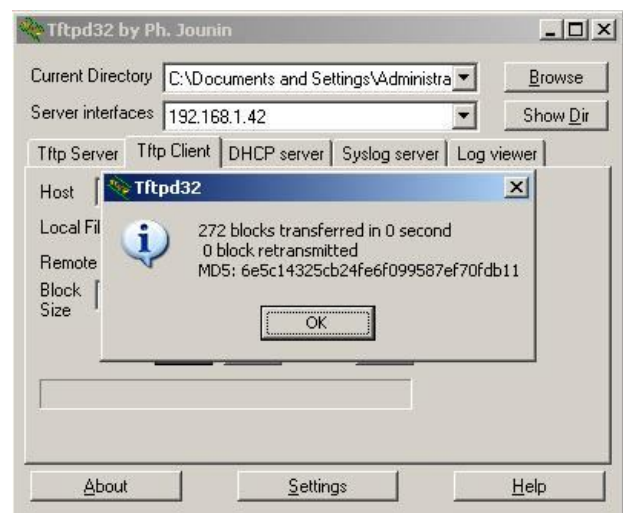


Następnie kopiowaliśmy plik z PC4 na PC3 jednocześnie kopiując plik z PC3 na PC2.

Obiór pliku wysłanego z PC3 na PC2



Odbiór pliku wysłanego z PC4 na PC3



## Wnioski

Wykonane ćwiczenie pokazało istotę działania koncentratora. Podczas pingowania dwóch stacji roboczych pakiety ICMP docierały do wszystkich komputerów podłączonych do koncentratora. Zostały one jednak odrzucone na komputerach, dla których nie były przeznaczone.

Wysyłanie plików między stacjami roboczymi odbywało się szybko, pomimo, że koncentrator rozsyłał pakiety na wszystkie swoje porty i zajmowało przy pliku zajmującym kilkadziesiąt kilobajtów 1-2 sekundy. Natomiast gdy jednocześnie wysyłano pliki między kilkoma stacjami roboczymi czasy wysyłki tego samego pliku znacznie wzrosły, gdyż koncentrator rozsyłał jeszcze więcej pakietów na wszystkie swoje porty, znacznie zwiększając ruch w sieci.