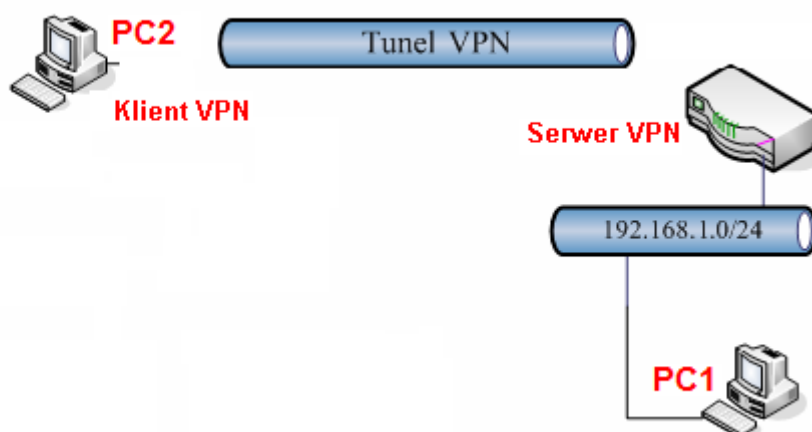


1. Ustawienia komputerów
2. Tunel VPN
3. Odnajdywanie zasobów
 - 3.1. \\adres_IP
 - 3.2. \\nazwa_hosta
4. Problemy z rozwiązywaniem nazw
 - 4.1. WINS
 - 4.2. LMHOSTS



Główne założenia:

- nazwa grupy roboczej: GRUPA_ROBOCZA
- PC1:
 - system operacyjny: WinXP
 - IP: 192.168.1.10
 - nazwa komputera: brinet001
- PC2:
 - system operacyjny: WinXP
 - IP: 99.99.99.10
 - nazwa komputera: brinet002

1. Ustawienia komputerów

PC1

Zmiany nazwy komputera [?] [X]

Możesz zmienić nazwę i członkostwo tego komputera. Zmiany mogą mieć wpływ na dostęp do zasobów sieciowych.

Nazwa komputera:
brinet001

Pełna nazwa komputera:
brinet001.

[Więcej...](#)

Członkostwo

Domena:

Grupa robocza:
GRUPA_ROBOCZA

OK Anuluj

PC2

Zmiany nazwy komputera [?] [X]

Możesz zmienić nazwę i członkostwo tego komputera. Zmiany mogą mieć wpływ na dostęp do zasobów sieciowych.

Nazwa komputera:
brinet002

Pełna nazwa komputera:
brinet002.

[Więcej...](#)

Członkostwo

Domena:

Grupa robocza:
GRUPA_ROBOCZA

OK Anuluj

2. Tunel VPN

Tunel skonfigurowany zgodnie z przykładami zamieszczonymi na stronie www.draytek.pl w zakładce POMOC -> Przykłady -> VPN i dostęp zdalny.

VPN i Dostęp Zdalny>> Kontrola połączeń

Wymuszanie inicjacji połączeń Czas odświeżania : 10 [v] [Odśwież](#)

_____ [v] [Inicjuj](#)

Stan połączenia VPN

Bieżąca strona: 1

Nr strony [] [Przejdź](#) [>>](#)

VPN	Typ	Zdalny IP	Sieć wirtualna	Tx pakietów	Tx prędk.(Bps)	Rx pakietów	Rx prędk.(Bps)	Czas akt.	
1 (test)	PPTP/MPPE	99.99.99.10 via WAN2	192.168.1.11/32	350	16040	280	2361	0:0:7	Rozłącz

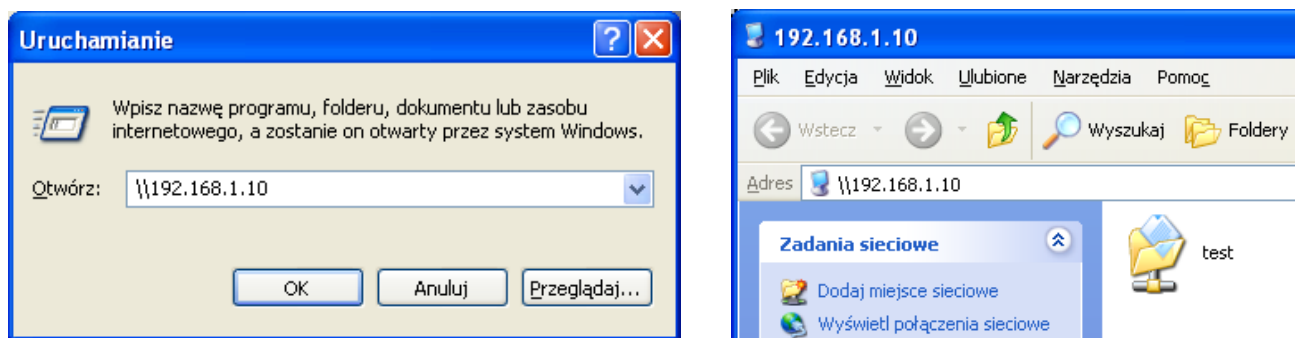
xxxxxxxx : Dane są szyfrowane.
xxxxxxxx : Dane nie są szyfrowane.

3. Odnajdywanie zasobów

3.1. \\adres_IP

Użyj *Internet Explorer*, *Eksplorator Windows* lub *Uruchom...* w Menu Start. Wpisz adres zasobu w formacie \\adres_IP. W przykładzie \\192.168.1.10.

Poniżej wykorzystanie *Uruchom...*:



3.2. \\nazwa_hosta

Przejdź do profilu VPN LAN-LAN i włącz przepuszczanie nazw NetBIOS.

<p>Konto użytkownika</p> <p><input checked="" type="checkbox"/> Włącz konto</p> <p>Czas nieaktywności <input type="text" value="300"/> sek</p> <hr/> <p>Akceptowane protokoły</p> <p><input checked="" type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> Tunel IPSec</p> <p><input checked="" type="checkbox"/> L2TP z polisą IPSec <input type="text" value="Brak"/></p> <p><input type="checkbox"/> Określ węzeł zdalny</p> <p>Adres IP/nr ISDN klienta zdalnego <input type="text"/></p> <p>lub ID <input type="text"/></p> <p>Nazwy NetBIOS <input checked="" type="radio"/> Przepuść <input type="radio"/> Blokuj</p> <p>Multicast przez VPN <input type="radio"/> Przepuść <input checked="" type="radio"/> Blokuj (IGMP, Kamery IP, DHCP Relay..itd.)</p>	<p>Użytkownik <input type="text" value="test"/></p> <p>Hasło <input type="password" value="••••"/></p> <p><input type="checkbox"/> Włącz mOTP (Mobile One-Time Passwords)</p> <p>Kod PIN <input type="text"/></p> <p>Klucz Secret <input type="text"/></p> <hr/> <p>Metoda uwierzytelniania IKE</p> <p><input checked="" type="checkbox"/> Klucz PSK</p> <p>IKE PSK <input type="text"/></p> <p><input type="checkbox"/> Podpis cyfrowy (X.509)</p> <p>Brak <input type="text"/></p> <hr/> <p>Poziom zabezpieczeń IPSec</p> <p><input checked="" type="checkbox"/> Średni (AH)</p> <p>Wysoki (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p> <p>Lokalny ID (opcja) <input type="text"/></p>
---	--

Uwaga!!!

Opcja przepuszczania nazw NetBIOS nie działa dla standardowego tunelu IPSec ze względu na polityki Windows.

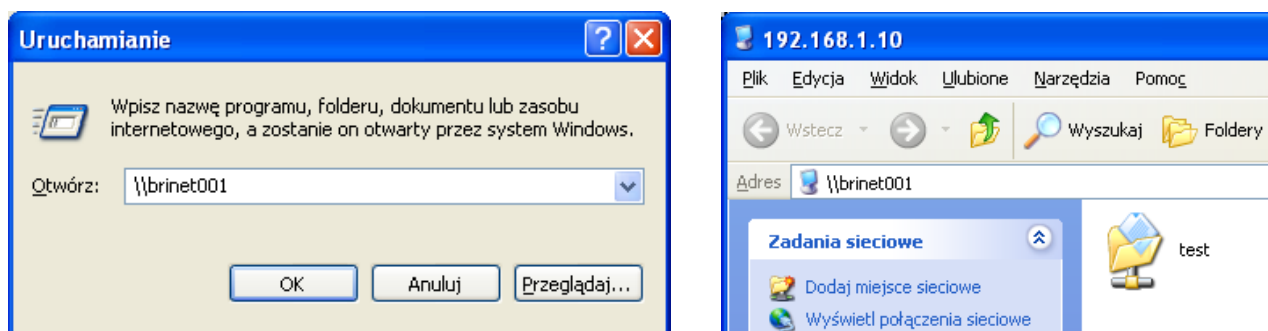
Po włączeniu powyższej opcji routery Vigor przekazują nazwy NetBIOS przez tunel VPN z użyciem 192.168.1.255.

Poniżej przechwycone dane przez PC2 z użyciem WireShark.

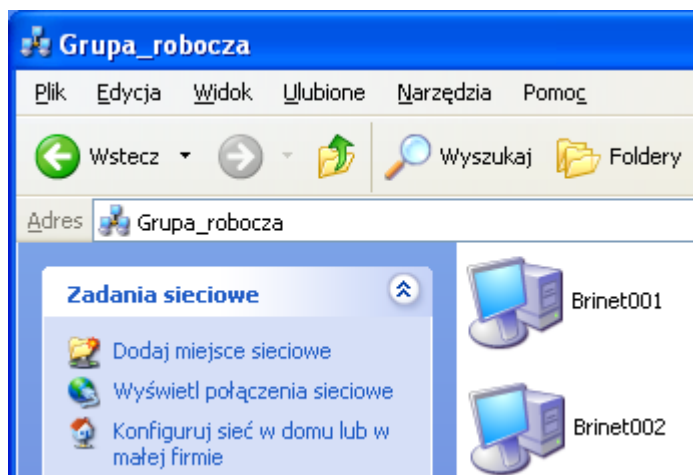
No.	Time	Source	Destination	Protocol	Info
474	219.125000	192.168.1.11	255.255.255.255	BROWSER	Request Announcement BRINET002
475	220.625000	192.168.1.11	255.255.255.255	BROWSER	Request Announcement BRINET002
476	222.125000	192.168.1.11	255.255.255.255	BROWSER	Request Announcement BRINET002
477	226.250000	192.168.1.11	255.255.255.255	NBNS	Name query NB ISATAP<00>
478	227.000000	192.168.1.11	255.255.255.255	NBNS	Name query NB ISATAP<00>
479	227.750000	192.168.1.11	255.255.255.255	NBNS	Name query NB ISATAP<00>
480	231.359375	192.168.1.10	192.168.1.255	NBNS	Registration NB BRINET001<00>
481	232.109375	192.168.1.10	192.168.1.255	NBNS	Registration NB BRINET001<00>
482	232.859375	192.168.1.10	192.168.1.255	NBNS	Registration NB BRINET001<00>
483	233.625000	192.168.1.10	192.168.1.255	NBNS	Registration NB BRINET001<00>

Użyj *Internet Explorer*, *Eksplorator Windows* lub *Uruchom...* w Menu Start. Wpisz adres zasobu w formacie \\nazwa_hosta. W przykładzie \\brinet001.

Poniżej wykorzystanie *Uruchom...*:



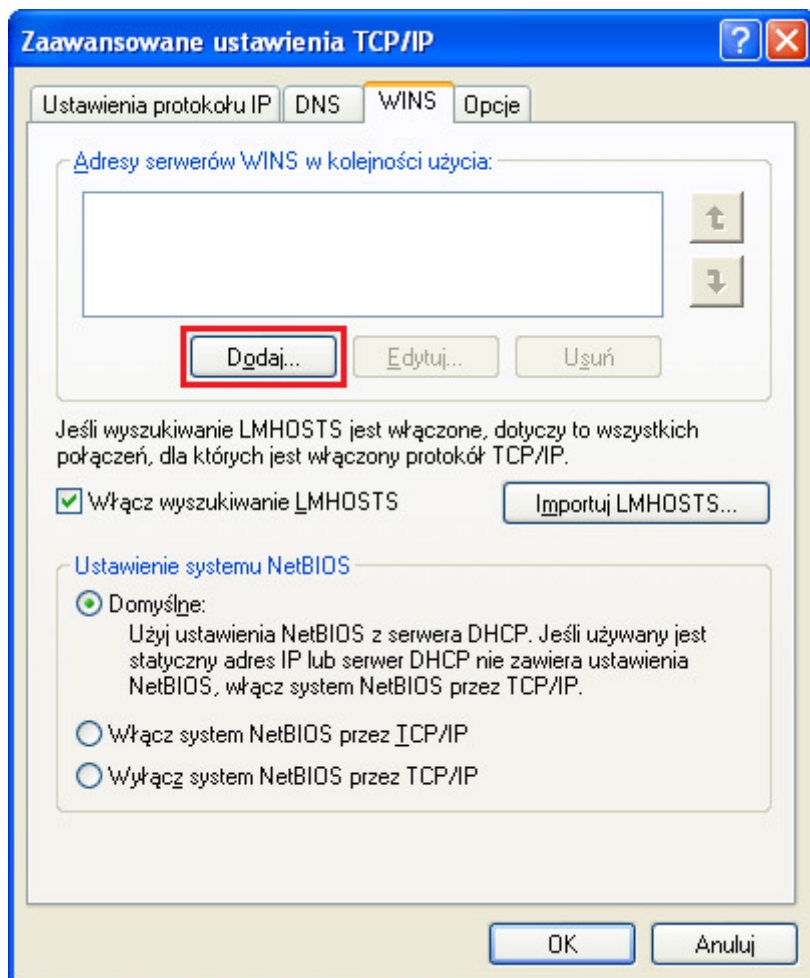
Przejdź do *Moje miejsce sieciowe*. Następnie *Wyświetl* komputery grupy roboczej.



4. Problemy z rozwiązywaniem nazw

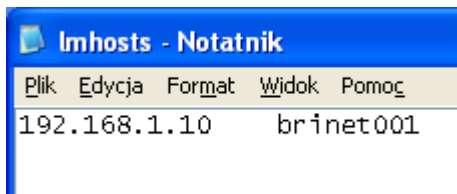
4.1. WINS

Stwórz serwer WINS oraz dodaj jego adres IP we właściwościach zaawansowanych TCP/IP karty sieciowej:

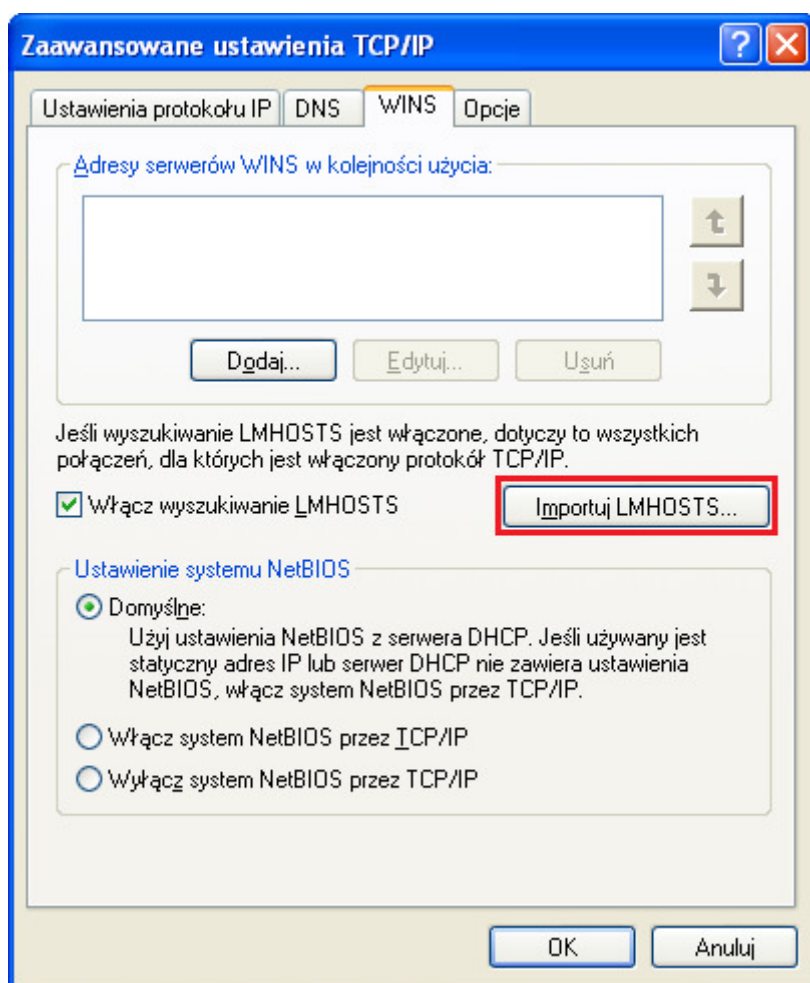


4.2. LMHOSTS

Stwórz plik z mapowaniami adresów IP na nazwy komputerów.



Następnie zaimportuj plik we właściwościach zaawansowanych TCP/IP karty sieciowej lub zapisz go do C:\Windows\System32\drivers\etc\ z nazwą 'lmhosts' (bez rozszerzenia).



Krzysztof Skowina
 Specjalista ds. rozwiązań sieciowych
k.skowina@brinet.pl