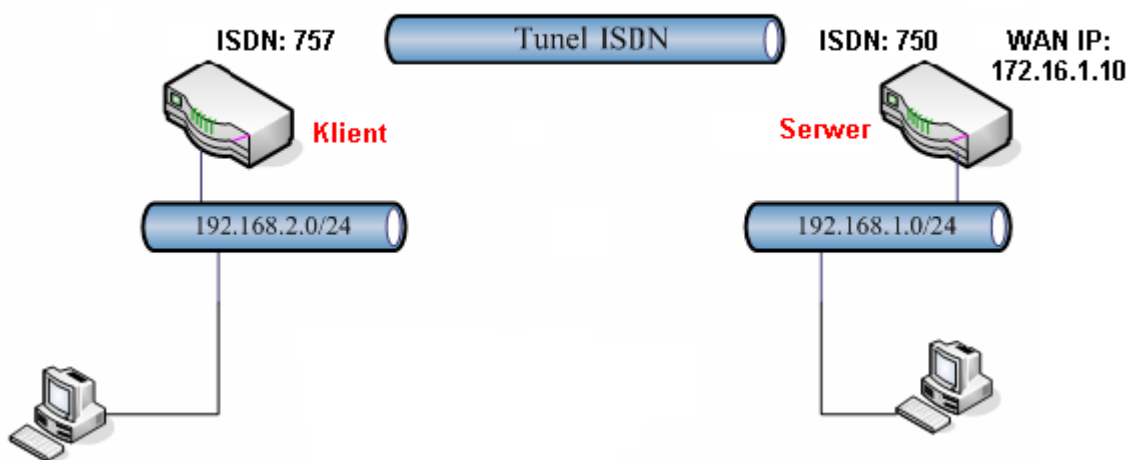


1. Konfiguracja serwera
2. Konfiguracja klienta
3. Status połączenia
4. Zdalny serwer jako brama do Internetu

Procedura konfiguracji została oparta na poniższym przykładzie.



Główne założenia:

- typ połączenia: LAN-LAN ISDN z routingiem pomiędzy podsieciami
- prędkość: 64kb/s
- klient ma tylko łącze ISDN
- serwer ma łącze ISDN oraz DSL

1. Konfiguracja serwera

Przejdź do zakładki **Interfejs ISDN>>Ustawienia ogólne** w panelu konfiguracyjnym routera. **Włącz** Interfejs ISDN (domyślnie powinna być zaznaczona opcja Włącz), wybierz **Polska** jako Kod kraju oraz wprowadź własny numer MSN w pola **Własny numer** i **Numery MSN dla routera**. W przykładzie użyto numeru 750.

Interfejs ISDN >> Ustawienia ogólne

ISDN

<div style="border: 2px solid red; padding: 2px;"> Interfejs ISDN <input checked="" type="radio"/> Włącz <input type="radio"/> Wyłącz Kod kraju Polska </div> <p>Tryb D-Channel</p> <p>ISDN1 <input type="radio"/> Punkt-Punkt <input checked="" type="radio"/> Punkt-Wielopunkt</p> <p>ISDN2 <input type="radio"/> Punkt-Punkt <input checked="" type="radio"/> Punkt-Wielopunkt</p> <div style="border: 2px solid red; padding: 2px;"> Własny numer 750 </div> <p><small>"Własny numer" to numer którym router prezentuje się zdalnym urządzeniom ISDN dla połączeń wychodzących.</small></p> <p><small>Przejdź do Ustawienia telefonu aby zmienić typ ISDN TE->NT.</small></p>	<p>Blokowane numery MSN</p> <p>1. <input style="width: 100%;" type="text"/></p> <p>2. <input style="width: 100%;" type="text"/></p> <p>3. <input style="width: 100%;" type="text"/></p> <p>4. <input style="width: 100%;" type="text"/></p> <p>5. <input style="width: 100%;" type="text"/></p>
---	--

Przejdź do zakładki **VPN i Dostęp Zdalny>>Protokoły VPN** w panelu konfiguracyjnym routera i sprawdź (lub zaznacz) czy jest włączony dostęp ISDN. Domyślnie włączona jest obsługa protokołów PPTP, IPSec i L2TP.

VPN i Dostęp Zdalny>> Protokoły VPN

Protokoły VPN

<input checked="" type="checkbox"/>	Włącz obsługę PPTP
<input checked="" type="checkbox"/>	Włącz obsługę IPSec
<input checked="" type="checkbox"/>	Włącz obsługę L2TP
<input checked="" type="checkbox"/>	Włącz dostęp ISDN

Przejdź do zakładki **VPN i Dostęp Zdalny>>Połączenia LAN-LAN**. Stwórz odpowiedni profil do obsługi połączenia (w przykładzie użyto profilu nr 1) i wprowadź odpowiednie dane.

Konfiguracja części **Ustawienia ogólne** zgodna z założeniami przykładu:

- wprowadź dowolną nazwę profilu
- zaznacz **Włącz profil**
- jako kierunek inicjacji wybierz **Dial-In** – 2930VSn odbiera połączenie od 2910VGi
- gdy połączenie ma być aktywne cały czas ustaw czas nieaktywności 0.

1. Ustawienia ogólne

<div style="border: 2px solid red; padding: 2px;"> Nazwa profilu od2910VGi <input checked="" type="checkbox"/> Włącz profil </div> <p>Połączenie VPN przez: WAN1 najpierw</p>	<p>Kierunek inicjacji <input type="radio"/> Oba <input type="radio"/> Dial-Out <input checked="" type="radio"/> Dial-In</p> <p><input type="checkbox"/> Zawsze aktywne</p> <p>Czas nieaktywności 300 sek</p> <p><input type="checkbox"/> Użyj PING dla podtrzymania</p> <p>PING na IP </p>
--	--

Konfiguracja części **Ustawienia Dial-In** zgodna z założeniami przykładu:

- w polu Protokół dla połączenia wybierz **ISDN**
- w polu **Użytkownik** wprowadź odpowiednią nazwę użytkownika. W przykładzie użyto użytkownika 'test'
- w polu **Hasło** wprowadź odpowiednie hasło. W przykładzie użyto hasła 'test'

3. Ustawienia Dial-In (odbiór wywołania z innego routera)

Akceptowane protokoły <input checked="" type="checkbox"/> ISDN <input type="checkbox"/> PPTP <input type="checkbox"/> Tunel IPsec <input type="checkbox"/> L2TP z polisą IPsec Brak		Użytkownik: test Hasło: ●●●● Kompresja VJ: <input checked="" type="radio"/> Włącz <input type="radio"/> Wyłącz
<input type="checkbox"/> Określ ISDN CLID lub Zdalna brama VPN Zdalny numer ISDN lub IP zdalnego serwera: <input type="text"/> lub ID: <input type="text"/>		Tryb uwierzytelniania IKE <input checked="" type="checkbox"/> Klucz IKE Klucz IKE: <input type="text"/> <input type="checkbox"/> Podpis cyfrowy (cert. X.509) Brak

- jeżeli chcesz dodatkowo weryfikować numer ISDN inicjującego połączenie zaznacz opcję **Określ ISDN CLID lub Zdalna brama VPN**, a w polu **Zdalny numer ISDN** wprowadź odpowiedni numer ISDN routera – klienta VPN. W przykładzie użyto 757

<input checked="" type="checkbox"/> Określ ISDN CLID lub Zdalna brama VPN Zdalny numer ISDN lub IP zdalnego serwera: 757 lub ID: <input type="text"/>

Konfiguracja części **Adresacja i routing oraz NAT wewnątrz połączenia** zgodna z założeniami przykładu:

- w przykładzie Zdalna podsieć: 192.168.2.0, Maska podsieci zdalnej: 255.255.255.0
 Zdalną podsieć możesz odczytać z adresu LAN routera. Np. gdy router na LAN-ie ma adres 192.168.2.1 / 255.255.255.0 , to zdalną podsiecią będzie 192.168.2.0 / 255.255.255.0 oczywiście przy założeniu, że wszystkie komputery „za routerem” mieszczą się w tej podsieci (np. 192.168.2.5 , 192.168.2.254, itp.)

4. Adresacja i routing oraz NAT wewnątrz połączenia

Własny WAN IP: 0.0.0.0 IP zdalnej bramy: 0.0.0.0 <input checked="" type="checkbox"/> IP zdalnej podsieci: 192.168.2.0 <input checked="" type="checkbox"/> Maska zdalnej podsieci: 255.255.255.0 <input type="button" value="Więcej podsieci"/>	RIP dla VPN: Wyłącz Z lokalnej podsieci do zdalnej podsieci, wykonaj: Routing <input type="checkbox"/> Zmień trasę domyślną do tego tunelu VPN (Tylko dla pojedynczego WANu)
--	--

2. Konfiguracja klienta

Przejdź do zakładki **Interfejs ISDN>>Ustawienia ogólne** w panelu konfiguracyjnym routera. **Włącz** Interfejs ISDN (domyślnie powinna być zaznaczona opcja Włącz), wybierz **Polska** jako Kod kraju oraz wprowadź własny numer MSN w pola **Własny numer** i **Numery MSN dla routera**. W przykładzie użyto numeru 757.

Interfejs ISDN >> Ustawienia ogólne

ISDN		Blokowane numery MSN	
Interfejs ISDN	<input checked="" type="radio"/> Włącz <input type="radio"/> Wyłącz	1.	<input type="text"/>
Kod kraju	<input type="text" value="Polska"/>	2.	<input type="text"/>
Własny numer	<input type="text" value="757"/>	3.	<input type="text"/>
"Własny numer" to numer którym router prezentuje się zdalnym urządzeniom ISDN dla połączeń wychodzących.		4.	<input type="text"/>
		5.	<input type="text"/>

Przejdź do zakładki **VPN i Dostęp Zdalny>>Protokoły VPN** w panelu konfiguracyjnym routera i sprawdź (lub zaznacz) czy jest włączony dostęp ISDN. Domyślnie włączona jest obsługa protokołów PPTP, IPSec i L2TP.

VPN i Dostęp Zdalny>> Protokoły VPN

Protokoły VPN	
<input checked="" type="checkbox"/>	Włącz obsługę PPTP
<input checked="" type="checkbox"/>	Włącz obsługę IPSec
<input checked="" type="checkbox"/>	Włącz obsługę L2TP
<input checked="" type="checkbox"/>	Włącz dostęp ISDN

Przejdź do zakładki **VPN i Dostęp Zdalny>>Połączenia LAN-LAN**. Stwórz odpowiedni profil do obsługi połączenia (w przykładzie użyto profilu nr 1) i wprowadź odpowiednie dane.

Konfiguracja części **Ustawienia ogólne** zgodna z założeniami przykładu:

- wprowadź dowolną nazwę profilu
- zaznacz **Włącz profil**
- jako kierunek inicjacji wybierz **Dial-Out** – 2910VGi łączy się do 2930VSn
- gdy połączenie ma być aktywne cały czas zaznacz **Zawsze aktywne** - ustawisz czas nieaktywności -1.

VPN i Dostęp Zdalny>> LAN-LAN

Indeks : 1	
1. Ustawienia ogólne	
Nazwa profilu	<input type="text" value="do 2930VSn"/>
<input checked="" type="checkbox"/> Włącz profil	
Połączenie VPN przez:	<input type="text" value="WAN1 najpierw"/>
Kierunek inicjacji	<input type="radio"/> Oba <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-In
<input type="checkbox"/> Zawsze aktywne	
Czas nieaktywności	<input type="text" value="300"/> sek
<input type="checkbox"/> Użyj PING dla podtrzymania	
PING na IP	<input type="text"/>

Konfiguracja części **Ustawienia Dial-Out** zgodna z założeniami przykładu:

- w polu Protokół dla połączenia wybierz **ISDN**
- w polu **Numer docelowy** wpisz odpowiedni numer ISDN, do którego zestawiasz połączenie. W przykładzie użyto 750.
- w polu Typ łącza ISDN wybierz odpowiednią prędkość połączenia. W przykładzie użyto 64kbps czyli zajęcie jednego kanału B.
- w polu **Użytkownik** wprowadź odpowiednią nazwę użytkownika. W przykładzie użyto użytkownika 'test'
- w polu **Hasło** wprowadź odpowiednie hasło. W przykładzie użyto hasła 'test'

2. Ustawienia Dial-Out (inicjacja do innego routera)

Protokół dla połączenia <input checked="" type="radio"/> ISDN <input type="radio"/> PPTP <input type="radio"/> Tunel IPSec <input type="radio"/> L2TP z polisą IPSec Brak		Typ łącza ISDN 64k bps Użytkownik test Hasło •••• Uwierzytelnianie PPP PAP/CHAP Kompresja VJ <input checked="" type="radio"/> Włącz <input type="radio"/> Wyłącz	
Numer docelowy (dla ISDN) IP/nazwa DNS serwera VPN. (np. 5551234, draytek.com lub 123.45.67.89) <input type="text" value="750"/>		Tryb uwierzytelniania IKE <input checked="" type="radio"/> Klucz IKE <input type="radio"/> Podpis cyfrowy (cert. X.509) Klucz IKE <input type="text"/> Brak	

Konfiguracja części **Adresacja i routing oraz NAT wewnątrz połączenia** zgodna z założeniami przykładu:

- w przykładzie Zdalna podsieć: 192.168.1.0, Maska podsieci zdalnej: 255.255.255.0

4. Adresacja i routing oraz NAT wewnątrz połączenia

Własny WAN IP <input type="text" value="0.0.0.0"/> IP zdalnej bramy <input type="text" value="0.0.0.0"/> <input checked="" type="checkbox"/> IP zdalnej podsieci <input type="text" value="192.168.1.0"/> <input checked="" type="checkbox"/> Maska zdalnej podsieci <input type="text" value="255.255.255.0"/> <input type="button" value="Więcej podsieci"/>	RIP dla VPN Wyłącz <input checked="" type="checkbox"/> Z lokalnej podsieci do zdalnej podsieci, wykonaj <input type="text" value="Routing"/> <input type="checkbox"/> Zmień trasę domyślną do tego tunelu VPN (Tylko dla pojedynczego WANu)
--	---

3. Status połączenia (od strony klienta)

Aby „obudzić” połączenie należy zainicjować dowolny ruch w kierunku routera. Wystarczy np. zwykły ping. Wybierz Menu Start a następnie Uruchom i wpisz cmd . Następnie wykonaj polecenie: ping adres_hosta_w_LAN-ie -t (patrz rysunek poniżej, gdzie host posiada adres LAN-owy 192.168.1.10). Po zainicjowaniu połączenia otrzymasz poprawną odpowiedź na ping – świadczy ona o poprawnej komunikacji.

```
C:\>ping 192.168.1.10 -t
Badanie 192.168.1.10 z użyciem 32 bajtów danych:
Upłynął limit czasu żądania.
Odpowiedź z 192.168.1.10: bajtów=32 czas=24ms TTL=126
Odpowiedź z 192.168.1.10: bajtów=32 czas=24ms TTL=126
Odpowiedź z 192.168.1.10: bajtów=32 czas=24ms TTL=126
Odpowiedź z 192.168.1.10: bajtów=32 czas=24ms TTL=126
Odpowiedź z 192.168.1.10: bajtów=32 czas=24ms TTL=126
Odpowiedź z 192.168.1.10: bajtów=32 czas=24ms TTL=126
Odpowiedź z 192.168.1.10: bajtów=32 czas=28ms TTL=126
Odpowiedź z 192.168.1.10: bajtów=32 czas=27ms TTL=126
Odpowiedź z 192.168.1.10: bajtów=32 czas=24ms TTL=126
Odpowiedź z 192.168.1.10: bajtów=32 czas=24ms TTL=126
Odpowiedź z 192.168.1.10: bajtów=32 czas=24ms TTL=126
Odpowiedź z 192.168.1.10: bajtów=32 czas=24ms TTL=126
Statystyka badania ping dla 192.168.1.10:
Pakiety: Wysłane = 13, Odebrane = 12, Utracone = 1 (<7% straty),
Szacunkowy czas błędzenia pakietów w milisekundach:
Minimum = 24 ms, Maksimum = 28 ms, Czas średni = 24 ms
Control-C
^C
```

O tym, czy połączenie zostało zainicjowane, możesz przekonać się wybierając **Status routera**(rysunek poniżej).

Status routera

Stan systemu		Czas pracy systemu: 0:4:31					
Status LAN		Podstawowy DNS: 194.109.6.66			Dodatkowy DNS: 168.95.1.1		
Adres IP	Pakiety TX	Pakiety RX					
192.168.2.1	1596	1425					
WAN 1 Status							
Włącz	Line	Name	Tryb	Czas aktywności			
Tak	Ethernet		---	00:00:00			
IP	GW IP	Pakiety TX	Prędk. TX	Pakiety RX	Prędk. RX		
---	---	0	0	0	0		
WAN 2 Status							
Włącz	Line	Name	Tryb	Czas aktywności			
Nie	Ethernet		---	00:00:00			
IP	GW IP	Pakiety TX	Prędk. TX	Pakiety RX	Prędk. RX		
---	---	0	0	0	0		
Status ISDN		>> Dial ISDN >> Rozłącz B1 >> Rozłącz B2					
Kanał	Aktywne połączenie	Pakiety TX	Prędk. TX	Pakiety RX	Prędk. RX	Czas aktywności	AOC
B1	do 2930VSn [192.168.1.11]	148	60	150	60	0:2:44	0
B2	Idle [---]	0	0	0	0	0:0:0	0
D	UP						

4. Zdalny serwer jako brama do Internetu (od strony klienta)

Powyższa konfiguracja umożliwia dostęp tylko do lokalnych zasobów sieci zdalnej.

Poniżej tablica routingu dla omawianego wyżej przypadku po zestawieniu połączenia ISDN. We wpisach nie ma trasy domyślnej – router wie jedynie o podsieciach: zdalnej 192.168.1.0 /24 i lokalnej 192.168.2.0 /24.

[Diagnostyka >> Pokaż tablicę routingu](#)

Tablica routingu		Odśwież
Key: C - connected, S - static, R - RIP, * - default, ~ - private		
C~	192.168.1.1/ 255.255.255.255 is directly connected,	ISDN
S~	192.168.1.0/ 255.255.255.0 via 192.168.1.1,	ISDN
C~	192.168.2.0/ 255.255.255.0 is directly connected,	LAN

Jak można było się spodziewać nie można nawiązać łączności z wp.pl.

```
C:\>ping wp.pl
Zadanie polecenia ping nie może znaleźć hosta wp.pl. Sprawdź nazwę i ponów próbę.
```

Aby zdalny serwer pełnił dodatkowo funkcję bramy do Internetu należy zaznaczyć funkcję **Zmień trasę domyślną do tego tunelu VPN** w profilu LAN-LAN.

4. Adresacja i routing oraz NAT wewnątrz połączenia

WAN IP (lokalny)	<input type="text" value="0.0.0.0"/>	RIP dla VPN	<input type="button" value="Wyłącz"/>
WAN IP (zdalny)	<input type="text" value="0.0.0.0"/>	Z lokalnej podsieci do zdalnej podsieci, wykonaj	
IP zdalnej podsieci	<input type="text" value="192.168.1.0"/>	<input type="button" value="Routing"/>	
Maska zdalnej podsieci	<input type="text" value="255.255.255.0"/>	<input checked="" type="checkbox"/> Zmień trasę domyślną do tego tunelu VPN (Tylko dla pojedynczego WANu)	
<input type="button" value="Więcej podsieci"/>			

Poniżej tablica routingu po zmianie trasy domyślnej po zestawieniu połączenia ISDN. We wpisach jest trasa domyślna oraz informacja o lokalnej podsieci 192.168.2.0 /24.

[Diagnostyka >> Pokaż tablicę routingu](#)

Tablica routingu		Odśwież
Key: C - connected, S - static, R - RIP, * - default, ~ - private		
S~	0.0.0.0/ 0.0.0.0 via 192.168.1.1,	ISDN
C~	192.168.1.1/ 255.255.255.255 is directly connected,	ISDN
C~	192.168.2.0/ 255.255.255.0 is directly connected,	LAN

Jak można było się spodziewać jest łączność z wp.pl.

```
C:\>ping wp.pl
Badanie wp.pl [212.77.100.101] z użyciem 32 bajtów danych:
Odpowiedź z 212.77.100.101: bajtów=32 czas=32ms TTL=121
Odpowiedź z 212.77.100.101: bajtów=32 czas=33ms TTL=121
Odpowiedź z 212.77.100.101: bajtów=32 czas=37ms TTL=121
Odpowiedź z 212.77.100.101: bajtów=32 czas=37ms TTL=121
Statystyka badania ping dla 212.77.100.101:
Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
Szacunkowy czas błędzenia pakietów w millisekundach:
Minimum = 32 ms, Maksimum = 37 ms, Czas średni = 34 ms
```

Krzysztof Skowina
Specjalista ds. rozwiązań sieciowych
BRINET Sp. z o.o.
k.skowina@brinet.pl