

Setting IPSec VPN connection between two SMC BR21VPN

Preparation

Company A

WAN IP: 192.168.34.109
LAN IP: 192.168.2.X

Company B

WAN IP: 192.168.34.111
LAN IP: 192.168.3.X

This example takes two SMC BR21VPN as work platform. Suppose Company A 192.168.2.10 create a VPN connection with Company B 192.168.3.10 for downloading the sharing file.

The Default Gateway of Company A is the LAN IP of the SMC BR21VPN 192.168.2.1 Follow the steps below:

- STEP 1** Enter the default IP of Gateway of Company A's SMC BR21VPN,192.168.2.1 and select **IPSec Autokey** in **VPN**. Click **New Entry**.
- STEP 2** In the list of **IPSec Autokey**, fill in Name with **VPN_A**.
- STEP 3** Select **Remote Gateway-Fixed IP or Domain Name** In **ToDestination** list and enter the IP Address.
- STEP 4** Select **Preshare** in **Authentication Method** and enter the **PresharedKey** (max: 100 bits)
- STEP 5** Select **ISAKMP Algorithm** in **Encapsulation** list. Choose the

Algorithm when setup connection. Please select ENC Algorithm (**3DES/DES/AES**), AUTH Algorithm (**MD5/SHA1**), and Group (**GROUP1, 2,5**). Both sides have to choose the same group. Here we select 3DES for ENC Algorithm, MD5 for AUTH Algorithm, and GROUP1 for group.

Necessary Item	
Name	vpn_a
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2
To Remote	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	192.168.34.111 (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	
Authentication Method	Preshare
Preshared Key	1122334455 (Max. 103 characters)
Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP 1

STEP 6 You can choose Data Encryption + Authentication or Authentication

Only to communicate in **IPSec Algorithm** list:

ENC Algorithm: **3DES/DES/AES/NULL**

AUTH Algorithm: **MD5/SHA1**

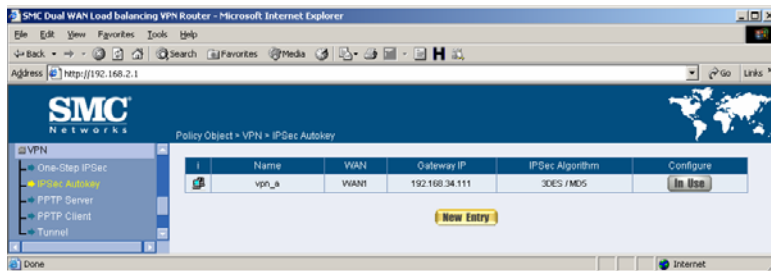
Here we select 3DES for ENC Algorithm and MD5 for AUTH Algorithm to make sure the encapsulation way for data transmission

IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
<input type="radio"/> Authentication Only	

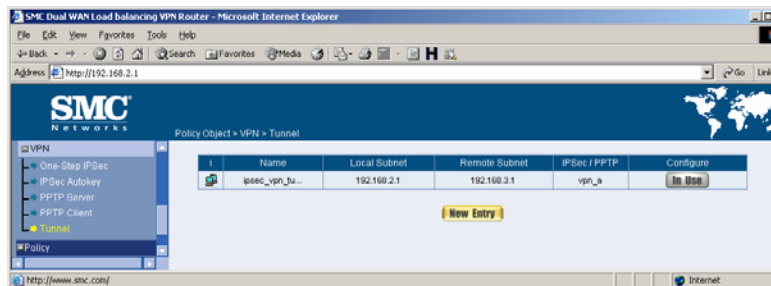
STEP 7 After selecting GROUP1 in **Perfect Forward Secrecy**, enter 3600seconds in **ISAKMP Lifetime**, enter 28800 seconds in **IPSec Lifetime**, and selecting Main mode in **Mode**.

Optional Item	
Perfect Forward Secrecy	GROUP 1
ISAKMP Lifetime	3600 Seconds (Range: 1200 - 86400)
IPSec Lifetime	28800 Seconds (Range: 1200 - 86400)
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode
My ID	(Max. 39 characters)
Peer ID	(Max. 39 characters)
GRE/IPSec	
GRE Local IP	
GRE Remote IP	
<input type="checkbox"/> Manual Connect	
Dead Peer Detection	delay 5 Second Timeout 60 Second (delay Range: 0 - 10, 0: means disable; Timeout Range: 1 - 100)

STEP 8 Complete the IPSec Autokey setting.



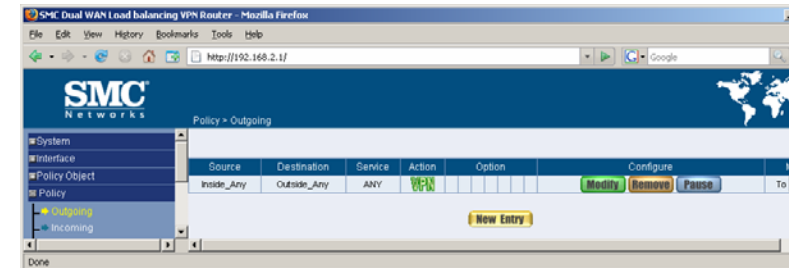
STEP 9 Enter the following setting in Tunnel of VPN function: (Click **New Entry**.)



- Enter a specific Tunnel **Name**.
- **From Source:** Select LAN
- **Subnet / Mask:** Enter 192.168.2.0 / 255.255.255.0
- **To Destination:** Select To Destination Subnet / Mask
- **Destination Subnet / Mask:** Enter 192.168.3.0 / 255.255.255.0
- **IPSec / PPTP Setting:** Select VPN_A.
- Select **Show remote Network Neighborhood**.
- Click **OK**.

Modify ipsec_vpn_tunnel Tunnel	
Name	ipsec_vpn_tunnel
From Local	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Local Subnet / Mask	192.168.2.1 / 255.255.255.0
To Remote	
<input checked="" type="radio"/> To Remote Subnet / Mask	192.168.3.1 / 255.255.255.0
<input type="radio"/> Remote Client	
IPSec / PPTP Setting	vpn_a
Keep alive IP :	
<input checked="" type="checkbox"/> Show remote Network Neighborhood	

STEP 10. Enter the following setting in **Outgoing Policy**:



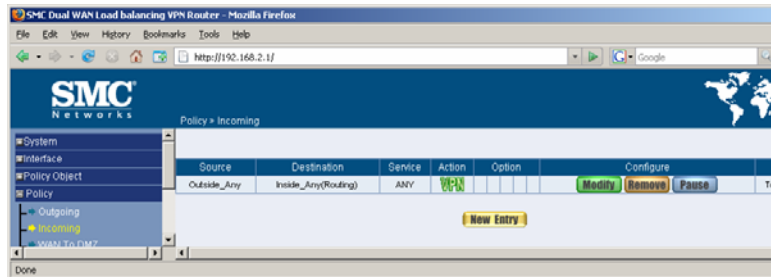
- Authentication User: Select All_NET.
- Schedule: Select Schedule_1.
- QoS: Select QoS_1.
- Tunnel: Select IPSec_VPN_Tunnel.
- Click **OK**

Comment : (Max. 32 characters)

Modify Policy

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Tunnel	ipsec_vpn_tunnel
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
M / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps (0: means unlimited)
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> (Range: 1 - 99999, 0: means unlimited)
MAX. Concurrent Sessions	<input type="text" value="0"/> (Range: 1 - 99999, 0: means unlimited)

STEP 11 Enter the following setting in **Incoming Policy**:



- Schedule: Select Schedule_1.
- QoS: Select QoS_1.
- Tunnel: Select IPSec_VPN_Tunnel.
- Click OK.

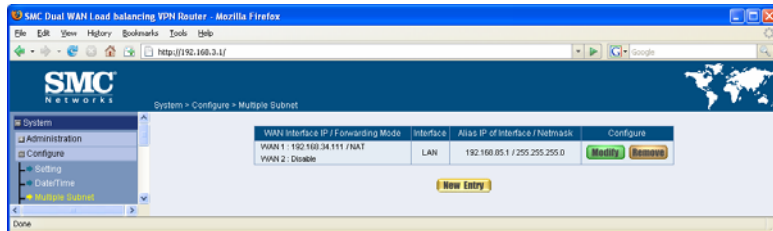
Comment : (Max. 32 characters)

Modify Policy

Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	None
Tunnel	ipsec_vpn_tunnel
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps (0: means unlimited)
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> (Range: 1 - 99999, 0: means unlimited)
MAX. Concurrent Sessions	<input type="text" value="0"/> (Range: 1 - 99999, 0: means unlimited)
NAT	<input type="checkbox"/> Enable

The Default Gateway of Company B is the LAN IP of the SMC BR21VPN 192.168.3.1. Follow the steps below:

STEP 1 Enter the following setting in **Multiple Subnet** of **System Configure** function:



STEP 2 Enter the default IP of Gateway of Company B's SMC BR21VPN, 192.168.3.1 and select **IPSec Autokey** in **VPN**. Click **New Entry**

STEP 3 In the list of **IPSec Autokey**, fill in Name with **VPN_B**.

STEP 4 Select **Remote Gateway-Fixed IP or Domain Name** In **To Destination** list and enter the IP Address

STEP 5 Select **Preshare** in **Authentication Method** and enter the **Preshared Key** (max: 100 bits)

STEP 6 Select **ISAKMP Algorithm** in **Encapsulation** list. Choose the Algorithm when setup connection. Please select
 ENC Algorithm (**3DES/DES/AES**)
 AUTH Algorithm (**MD5/SHA1**)
 Group (**GROUP1, 2,5**).

Both sides have to choose the same group. Here we select 3DES for ENC Algorithm, MD5 for AUTH Algorithm, and GROUP1 for group.

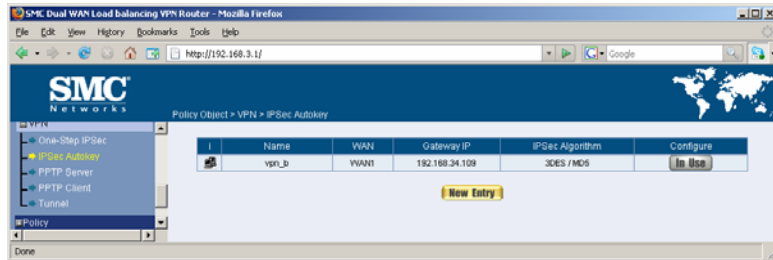
STEP 7 You can choose **Data Encryption + Authentication** or **Authentication only** to communicate in **IPSec Algorithm** list:
 ENC Algorithm: **3DES/DES/AES/NULL**
 AUTH Algorithm: **MD5/SHA1**
 Here we select 3DES for ENC Algorithm and MD5 for AUTH Algorithm to make sure the encapsulation way for data transmission.

Necessary Item	
Name	vpn_b
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2
To Remote	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	192.168.34.109 (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	
Authentication Method	Preshare
Preshared Key	1122334455 (Max. 103 characters)
Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP 1
IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
<input type="radio"/> Authentication Only	

STEP 8 After selecting **GROUP1** in **Perfect Forward Secrecy**, enter 3600 seconds in **ISAKMP Lifetime**, enter 28800 seconds in **IPSec Lifetime**, and selecting **Main mode** in **Mode**.

Optional Item	
Perfect Forward Secrecy	GROUP 1
ISAKMP Lifetime	3600 Seconds (Range: 1200 - 86400)
IPSec Lifetime	28800 Seconds (Range: 1200 - 86400)
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode
My ID	(Max. 39 characters)
Peer ID	(Max. 39 characters)
GRE/IPSec	
GRE Local IP	
GRE Remote IP	
<input type="checkbox"/> Manual Connect	
Dead Peer Detection delay	5 Second
Timeout	60 Second (delay Range: 0 - 10, 0: means disable; Timeout Range: 1 - 100)

STEP 9 Complete the **IPSec Autokey** setting

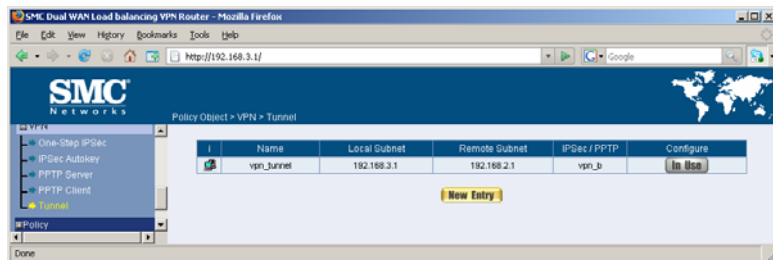


STEP 10 Enter the following setting in **Tunnel** of VPN function:

- Enter a specific Tunnel **Name**.
- **From Source:** Select LAN
- **From Source Subnet / Mask:** Enter 192.168.3.0 / 255.255.255.0.
- **To Destination:** Select To Destination Subnet / Mask.
- **To Destination Subnet / Mask:** Enter 192.168.2.0 / 255.255.255.0.
- **IPSec / PPTP Setting:** Select VPN_B.
- Select **Show remote Network Neighborhood**.
- Click **OK**.

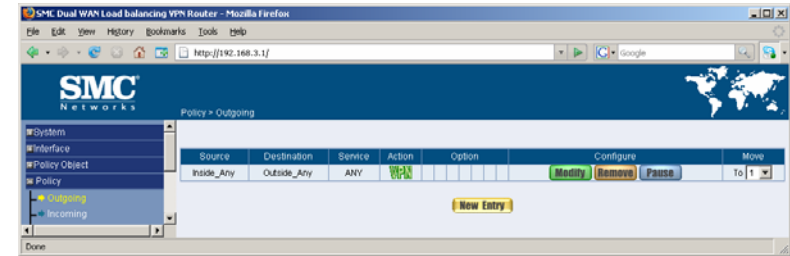
Modify vpn_tunnel Tunnel

Name	vpn_tunnel		
From Local	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ		
From Local Subnet / Mask	192.168.3.1	/	255.255.255.0
To Remote	<input checked="" type="radio"/> To Remote Subnet / Mask <input type="radio"/> Remote Client		
To Remote Subnet / Mask	192.168.2.1	/	255.255.255.0
IPSec / PPTP Setting	vpn_b		
Keep alive IP :			
<input checked="" type="checkbox"/> Show remote Network Neighborhood			



STEP 11 Enter the following setting in **Outgoing Policy**:

- **Authentication User:** Select All_NET.
- **Schedule:** Select Schedule_1.
- **QoS:** Select QoS_1.
- **Tunnel:** Select VPN_Tunnel.
- Click **OK**.



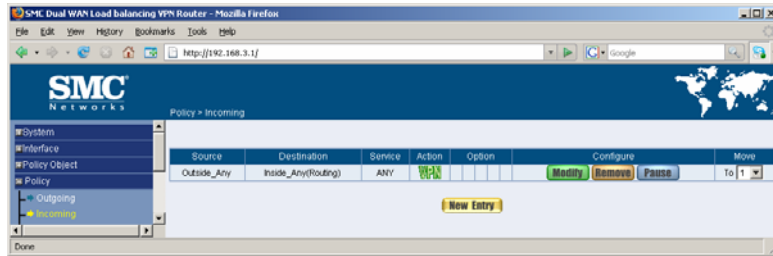
Comment : (Max. 32 characters)

Modify Policy

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Tunnel	vpn_tunnel
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps (0: means unlimited)
MAX. Concurrent Sessions Per IP	0 (Range: 1 - 99999, 0: means unlimited)
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)

STEP 12 Enter the following setting in **Incoming Policy**:

- **Schedule:** Select Schedule_1.
- **QoS:** Select QoS_1.
- **Tunnel:** Select IPSec_VPN_Tunnel.
- Click **OK**.



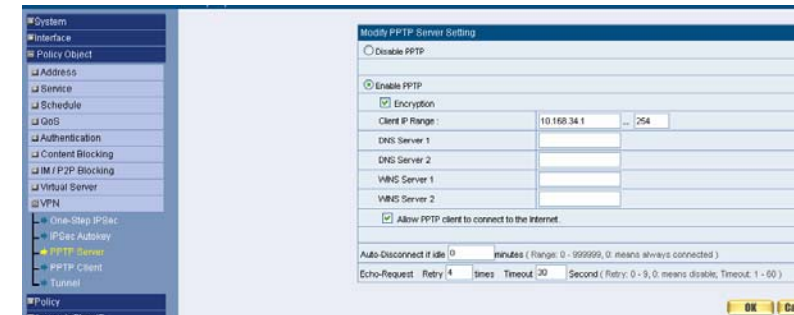
Comment : (Max. 32 characters)

Modify Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	None
Tunnel	vpn_tunnel
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps (0: means unlimited)
MAX. Concurrent Sessions Per IP	0 (Range: 1 - 99999, 0: means unlimited)
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)
NAT	<input type="checkbox"/> Enable

STEP 13 Complete IPSec VPN Connection

SMCBR21VPN: PPTP Server Configuration

- STEP 1. Enter PPTP Server of VPN function in the SMC BR21VPN .
 Select **Modify** and enable PPTP Server:
- Select **Encryption**.
 - **Client IP Range**: Enter 192.168.34.1-254.
 - Idle Time: Enter 0.



- STEP 2. Add the following settings in PPTP Server of VPN function in the SMC BR21VPN
- Select **New Entry**.



- **User Name**: Enter administrator.
- **Password**: Enter 1122334455
- **Client IP assigned by**: Select IP Range.
- Click **OK**.

The screenshot shows the SMC Networks configuration interface for a PPTP Server. The left sidebar lists various configuration categories, with 'VPN' selected. The main area displays the 'Basic PPTP Server' configuration form, including fields for User Name, Password, Client IP assigned to, and options for # Range, Fixed IP, and Manual Disconnect. Below the form is a table with columns for User Name, Client IP, Uptime, and a Configure button. The table contains one entry: PPTP_Connection with Client IP 0.0.0.0. Buttons for 'Modify' and 'Remove' are next to the entry. A 'New Entry' button is at the bottom.

User Name	Client IP	Uptime	Configure
PPTP_Connection	0.0.0.0	---	Modify Remove

STEP 3. Enter the following setting in **Tunnel** of **VPN** function:

- Enter a specific **Tunnel Name**.
- **From Source:** Select LAN
- **From Source Subnet / Mask:** Enter 192.168.2.1 / 255.255.255.0.
- **To Destination:** Select To Destination Subnet / Mask.
- **To Destination Subnet / Mask:** Enter 192.168.34.1 / 255.255.255.0.
- **IPSec / PPTP Setting:** Select PPTP_Server_PPTP_Connection.
- Select **Show remote Network Neighborhood**.
- Click **OK**.

The screenshot shows the 'Modify pptp Tunnel' configuration page. The 'Name' field is set to 'pptp'. The 'From Local' section has 'LAN' selected with '192.168.2.1' and '255.255.255.0'. The 'To Remote' section has 'To Remote Subnet / Mask' selected with '192.168.34.1' and '255.0.0.0'. The 'IPSec / PPTP Setting' is set to 'PPTP_Server_administrator'. The 'Show remote Network Neighborhood' checkbox is checked.

STEP 4. Enter the following setting in **Outgoing Policy**:

- **Tunnel:** Select PPTP_VPN_Tunnel.
- Click **OK**

The screenshot shows the SMC Networks configuration interface for an Outgoing Policy. The left sidebar lists various configuration categories, with 'Policy' selected. The main area displays the 'Modify Policy' configuration form. The 'Tunnel' field is set to 'pptp'. Other fields include Source Address, Destination Address, Service, Schedule, Authentication User, Action, Tunnel, Action_VPN/Port, Traffic Log, Statistics, Content Blocking, M/P2P Blocking, GoS, and various session and bandwidth limits.

STEP 5. Enter the following setting in **Incoming Policy**:

- **Tunnel:** Select PPTP_VPN_Tunnel.
- Click **OK**.

The screenshot shows the SMC Networks configuration interface for an Incoming Policy. The left sidebar lists various configuration categories, with 'Policy' selected. The main area displays the 'Modify Policy' configuration form. The 'Tunnel' field is set to 'pptp'. Other fields include Source Address, Destination Address, Service, Schedule, Action, Traffic Log, Statistics, GoS, and various session and bandwidth limits.

How to create a VPN connection through the router with Windows Vista client

The environment:

We have the following network diagram to establish the VPN tunnel:

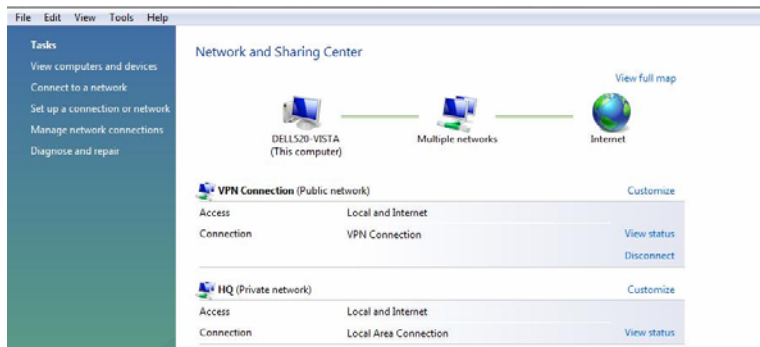
PC (client Windows Vista) ---- Internet ----- Router in bridge mode ---- SMCBR21VPN ---- PC (server Windows XP)

With the following definition of IPs:

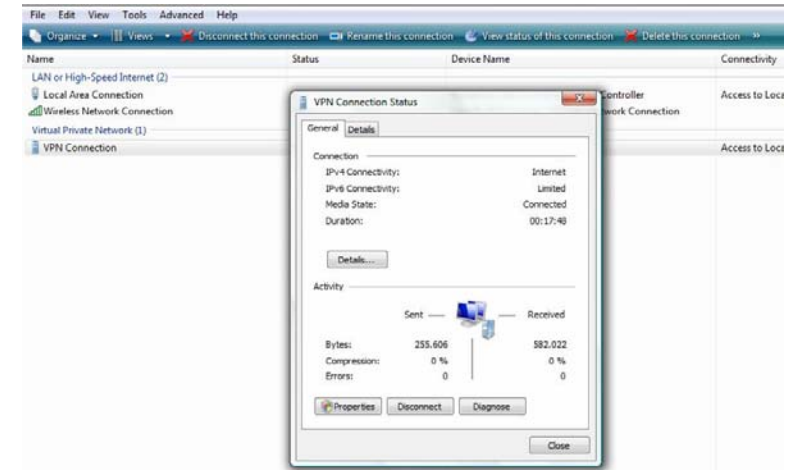
- a) PC client → 192.168.34.65
- b) Router in bridge mode → No IP address.
- c) SMCBR21VPN → LAN IP: 192.168.2.1 / WAN IP: 85.58.46.180
- d) PC server → 192.168.2.11

The procedure:

- 1) We proceed to create a new Virtual Private Connection (PPTP):



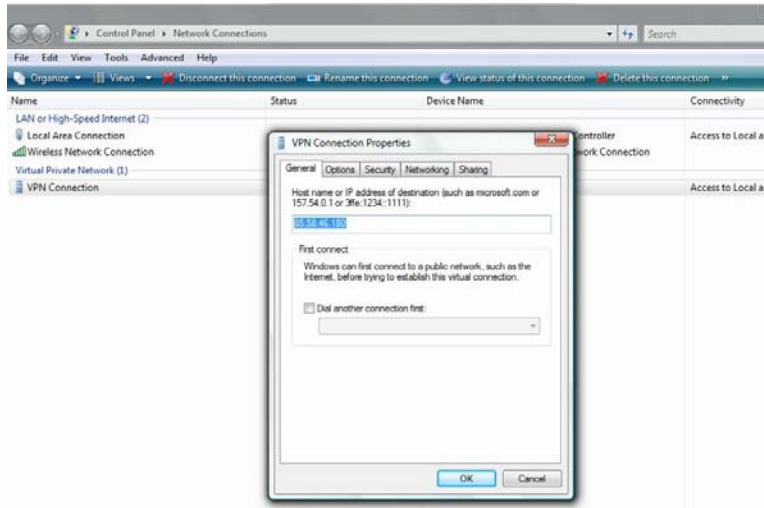
- 2) We define the properties of the connection:



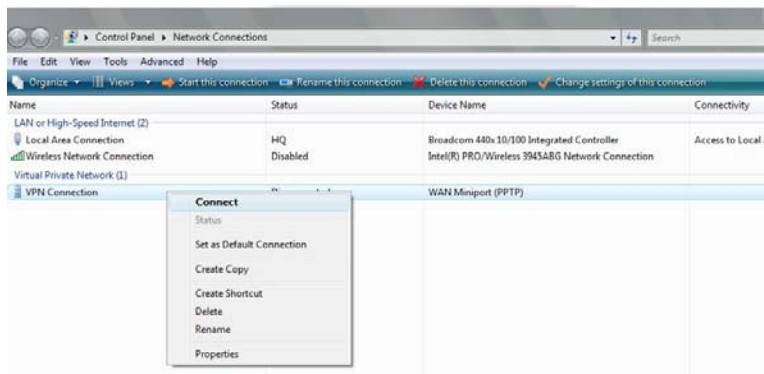
- 3) PPTP Virtual connection is created. Now we have to configure the profile:



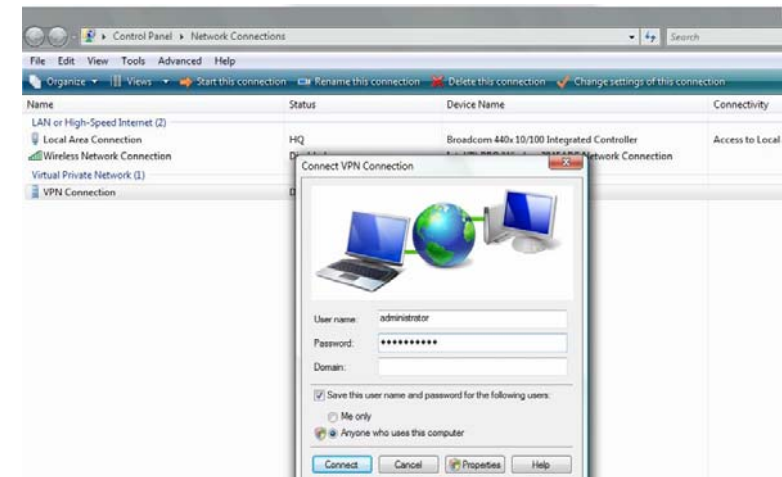
4) Now it has to be introduced the WAN IP of the router for the profile:



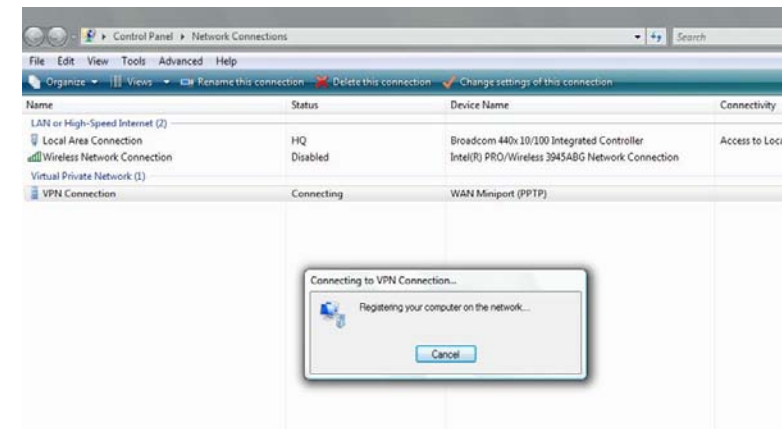
5) We try to carry out the connection:



6) Then it has to be introduced the user/password in the prompt that matches the configuration of the VPN router:



7) Finally the connection, if everything's ok, will be proceeded successfully registering the PC client on the tunnel:



Test:

Now we can test the connections like this:

a) To the WAN interface of the router:

```
C:\>ping 85.58.46.180
Pinging 85.58.46.180 with 32 bytes of data:
Reply from 85.58.46.180: bytes=32 time=68ms TTL=55
Reply from 85.58.46.180: bytes=32 time=68ms TTL=55
Reply from 85.58.46.180: bytes=32 time=67ms TTL=55
Reply from 85.58.46.180: bytes=32 time=68ms TTL=55
Ping statistics for 85.58.46.180:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 67ms, Maximum = 68ms, Average = 67ms
```

b) To the LAN interface of the router:

```
C:\Documents and Settings\Administrator>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=73ms TTL=64
Reply from 192.168.2.1: bytes=32 time=88ms TTL=64
Reply from 192.168.2.1: bytes=32 time=70ms TTL=64
Reply from 192.168.2.1: bytes=32 time=125ms TTL=64
Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 70ms, Maximum = 125ms, Average = 89ms
```

c) To the PC server:

```
C:\Documents and Settings\Administrator>ping 192.168.2.11
Pinging 192.168.2.11 with 32 bytes of data:
Reply from 192.168.2.11: bytes=32 time=89ms TTL=127
Reply from 192.168.2.11: bytes=32 time=131ms TTL=127
Reply from 192.168.2.11: bytes=32 time=131ms TTL=127
Reply from 192.168.2.11: bytes=32 time=98ms TTL=127
Ping statistics for 192.168.2.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 89ms, Maximum = 131ms, Average = 112ms
```

How to create a VPN connection through the router with Windows 2000 client

The environment:

We have the following network diagram to establish the VPN tunnel:

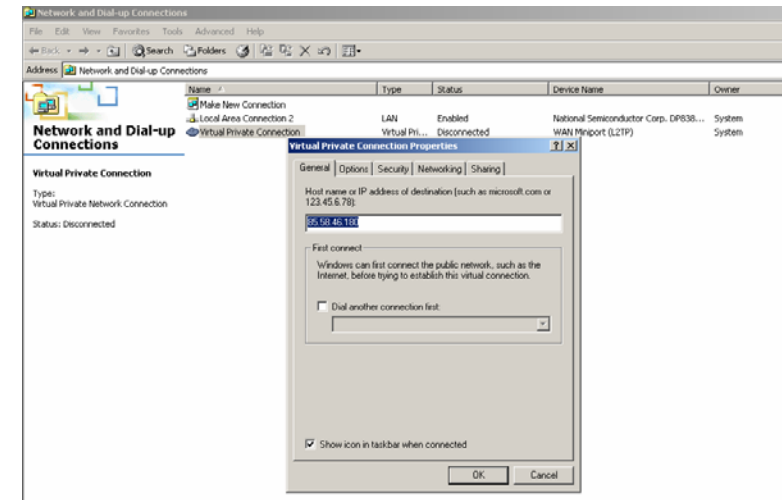
PC (client Windows 2000) ---- Internet ---- Router in bridge mode ---- SMCBR21VPN ---
- PC (server Windows XP)

With the following definition of IPs:

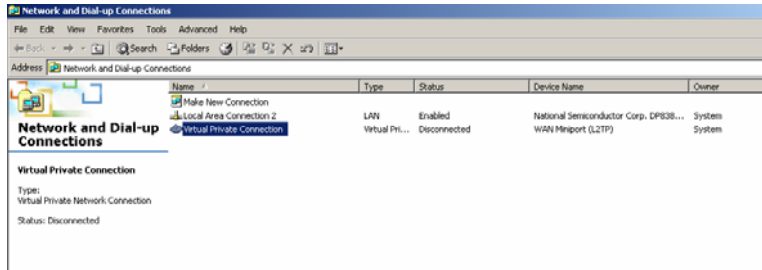
- a) PC client → 192.168.34.97
- b) Router in bridge mode → No IP address.
- c) SMCBR21VPN → LAN IP: 192.168.2.1 / WAN IP: 85.58.46.180
- d) PC server → 192.168.2.11

The procedure:

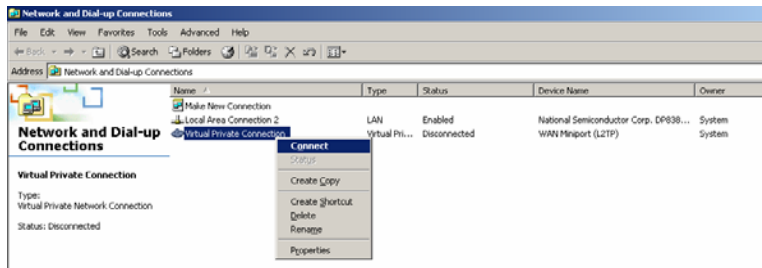
8) We create a new Virtual Private Connection (PPTP) with the WAN IP assigned to the SMCBR21VPN:



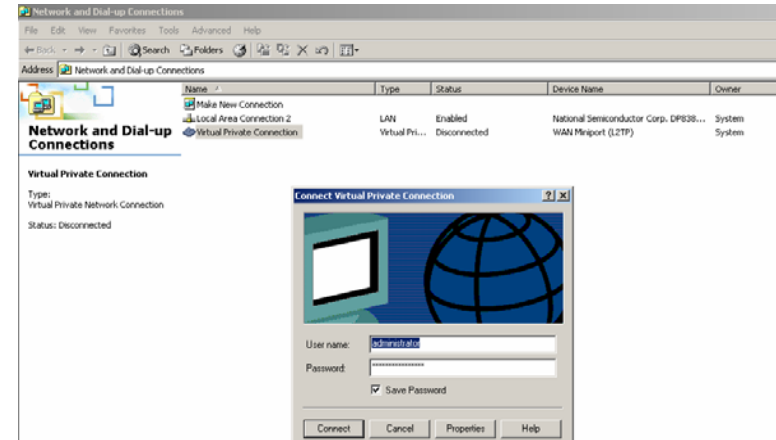
9) Once the profile for the PPTP Virtual connection is created...



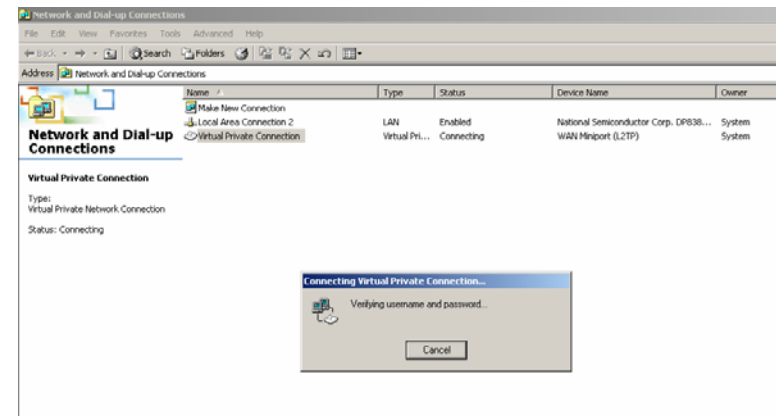
10) We connect to this one:



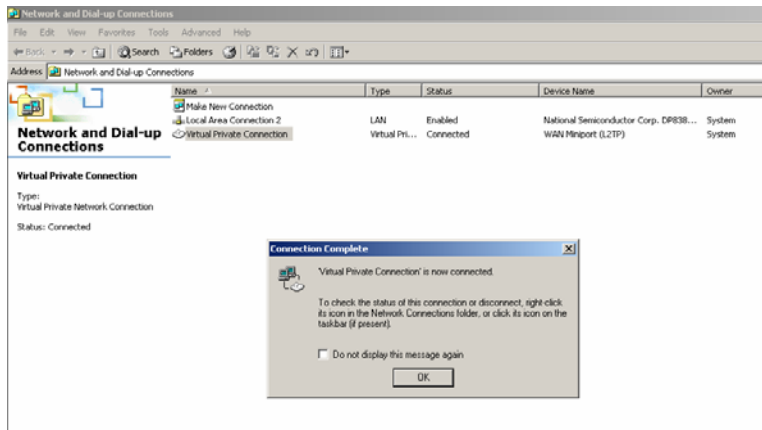
11) We introduce the user / password defined on the VPN router:



12) User/Password and connection will be verified:



13) If everything's ok, we will obtain this for the tunnel connection:



Test:

Now we can test the connections like this:

a) To the WAN interface of the router:

```
C:\>ping 85.58.46.180

Pinging 85.58.46.180 with 32 bytes of data:

Reply from 85.58.46.180: bytes=32 time=68ms TTL=55
Reply from 85.58.46.180: bytes=32 time=68ms TTL=55
Reply from 85.58.46.180: bytes=32 time=67ms TTL=55
Reply from 85.58.46.180: bytes=32 time=68ms TTL=55

Ping statistics for 85.58.46.180:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 67ms, Maximum = 68ms, Average = 67ms
```

b) To the LAN interface of the router:

```
C:\Documents and Settings\Administrator>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=73ms TTL=64
Reply from 192.168.2.1: bytes=32 time=88ms TTL=64
Reply from 192.168.2.1: bytes=32 time=70ms TTL=64
Reply from 192.168.2.1: bytes=32 time=125ms TTL=64

Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 70ms, Maximum = 125ms, Average = 89ms
```

c) To the PC server:

```
C:\Documents and Settings\Administrator>ping 192.168.2.11

Pinging 192.168.2.11 with 32 bytes of data:

Reply from 192.168.2.11: bytes=32 time=89ms TTL=127
Reply from 192.168.2.11: bytes=32 time=131ms TTL=127
Reply from 192.168.2.11: bytes=32 time=131ms TTL=127
Reply from 192.168.2.11: bytes=32 time=98ms TTL=127

Ping statistics for 192.168.2.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 89ms, Maximum = 131ms, Average = 112ms
```