

APPLICATION NOTE AN-001-WUK

# HOW TO CONFIGURE AN IPSEC VPN

LAN to LAN connectivity over a VPN between a MRD-455 4G router and a central ADSL-350 broadband router with fixed IP address



# Introduction

## What is an IPsec VPN?

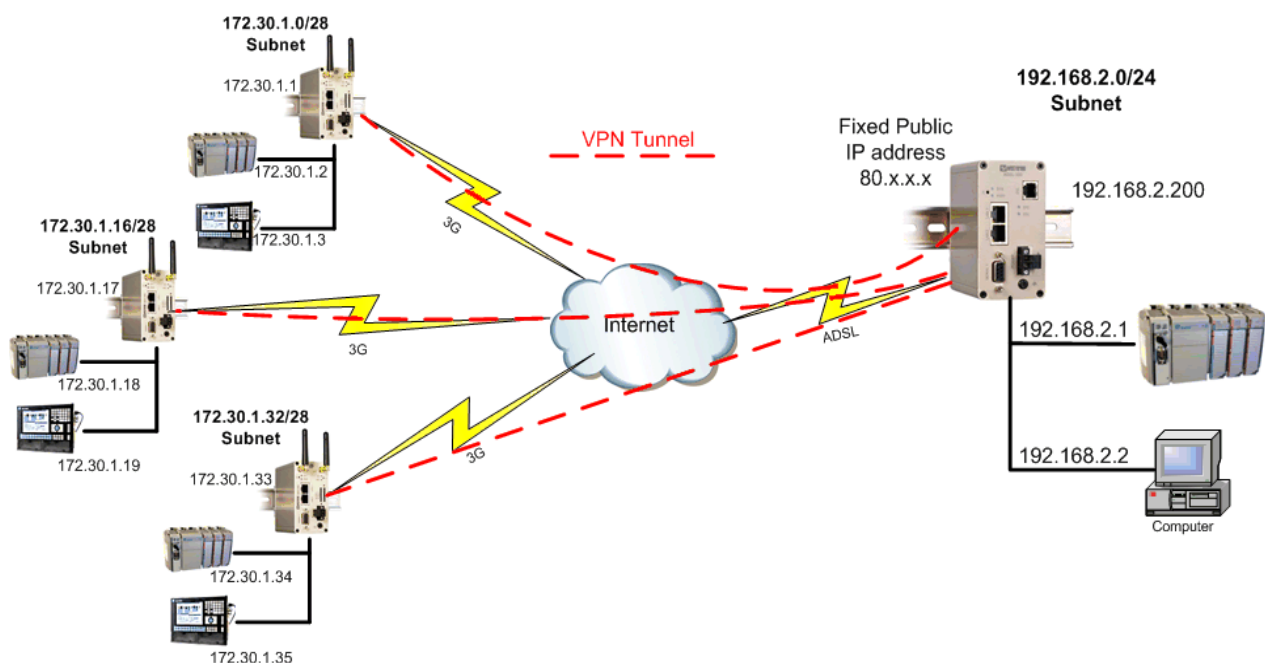
IPsec VPN's create a secure **Virtual Private Network** between two or more private LAN networks, over the internet.

The internet is generally accepted as a world wide insecure network, but using IPsec VPN's can make data transfer over the internet much more secure.

IPsec (Internet Protocol Security), utilises a selection of encryption and authentication algorithms which are grouped together under a common banner. Different combinations of these protocols can be used simultaneously to create a secure tunnel between two routers. Despite the fact that business critical data may be traversing over a wireless connection via the internet to your central office, the data itself is both encrypted and encapsulated with secure authentication up to a military grade level of data protection.

It is quite possible to use IPSEC to secure communications between multiple different sites, the diagram below shows three remote sites connecting back to a central location where a number of devices can communicate to the various outstation units.

**NB:** IPSEC will only provide security for the links **BETWEEN** the routers. You must not consider the routers themselves to actually be secure once a VPN is in place. Further security can be afforded through proper username management and implementation of a firewall



## Overview

The following pages show how to implement an IPSEC VPN between a pair of Westermo routers. The MRD-455 4G router will be the initiator because this will most likely be given a dynamic and NAT:ed IP address from the provider.

The ADSL-350 will be the responder because the ADSL IP address is known and is fixed. In nearly all cases, the responder router will be a DSL router which is located at a central location, such as company headquarters. In all cases the **RESPONDER** router will need to have a **fixed, publicly accessible IP address**.

Thanks to **Aggressive mode** IPsec with the addition of a feature known as **NAT-Traversal**, the initiating router does not require a fixed, publicly accessible IP address.

### Phase 1: IKE

Internet Key Exchange (IKE) protocol defines what parameters are used to negotiate the initial stage of the VPN connection, and provide security which is used in negotiating the second stage of the VPN. This involves the creation of “IKE SA’s”.

### Phase 2: IPsec

The IPsec transform defines the negotiation for the second stage of the VPN. This includes exactly what authentication and encryption will be used in the VPN tunnel, along with IP addressing information that allows data to flow from router to router. This involves the creation of “IPsec SA’s”.

## Assumptions

This application note applies to; MRD-455 4G router an ADSL-350 DSL router and assumes both are starting from a factory default configuration.

## Corrections

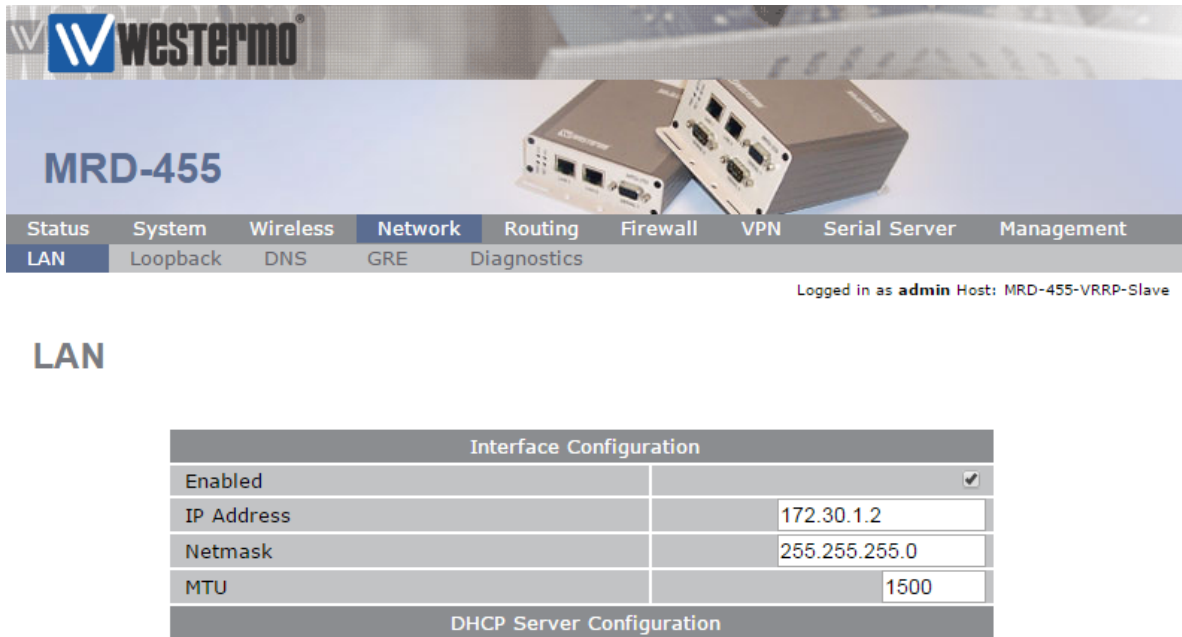
Requests for corrections or amendments to this application note are welcome and should be addressed to [technical@westermo.co.uk](mailto:technical@westermo.co.uk)

Requests for new application notes can be sent to the same address.

# MRD-455 4G Router Configuration

## LAN IP Address

Browse to Network → LAN



The screenshot shows the web-based configuration interface for the MRD-455 router. At the top, there is a navigation menu with tabs for Status, System, Wireless, Network, Routing, Firewall, VPN, Serial Server, and Management. The 'Network' tab is selected, and within it, the 'LAN' sub-tab is active. The interface shows the router's IP address as 172.30.1.2 and the netmask as 255.255.255.0. The MTU is set to 1500. The 'Enabled' checkbox is checked. Below the interface configuration, there is a section for DHCP Server Configuration.

Interface Configuration	
Enabled	<input checked="" type="checkbox"/>
IP Address	172.30.1.2
Netmask	255.255.255.0
MTU	1500

DHCP Server Configuration

**IP Address:** 172.30.1.2

**Netmask:** 255.255.255.0

# MRD-455 4G Router Configuration

## 4G Link

Browse to WIRELESS → PACKET MODE



**MRD-455**

Status System **Wireless** Network Routing Firewall VPN Serial Server Management

Network **Packet Mode** Connection Management Circuit Switched Mode SMS

Logged in as **admin** Host: MRD-455-e0-be-3b

### Packet Mode

Connection Configuration	
Connection Mode	Disabled ▼
SIM 1 profile (active)	---- ▼
SIM 2 profile	---- ▼
Reset	Update

Index	APN	Auth	User	Password	Edit	Delete
No profiles configured.						
Add new profile						

Click **Add new profile**.



**MRD-455**

Status System **Wireless** Network Routing Firewall VPN Serial Server Management

Network **Packet Mode** Connection Management Circuit Switched Mode SMS

Logged in as **admin** Host: MRD-455-VRPP-Slave

### Packet Mode

Editing profile 1	
<b>APN</b>	YOUR_APN_GOES_HERE
<b>Authentication</b>	None ▼
<b>Username</b>	
<b>Password</b>	Not set New: <input type="checkbox"/>
Cancel	Update

Enter the **APN** (Access Point Name) provided by your network SIM provider.

**NB:** Standard 4G/3G tariffs do not often require authentication

# MRD-455 4G Router Configuration

Browse to WIRELESS → PACKET MODE continued.



The screenshot shows the Westermo MRD-455 configuration web interface. The 'Wireless' menu is selected, and 'Packet Mode' is active. The 'Connection Configuration' section shows 'Connection Mode' set to 'Always connect', 'SIM 1 profile (active)' set to '1', and 'SIM 2 profile' set to '1'. Below this is a table of profiles:

Index	APN	Auth	User	Password	Edit	Delete
1	internet	None		Not set		

Buttons for 'Reset' and 'Update' are visible. An 'Add new profile' button is located below the table.

**Connection Mode:** Always connect

**SIM 1 profile:** 1

**NB:** In this example the SIM card in slot 1 will use profile 1. You can set up multiple profiles and assign them to either SIM slot 1 or 2 depending on the provider of the SIM card.

Refer to application note AN-004-WUK Dual SIM Failover.



# MRD-455 4G Router Configuration

## IPSec VPN Tunnel Configuration (Initiator)

Browse to VPN → IPSec



### IPsec VPN

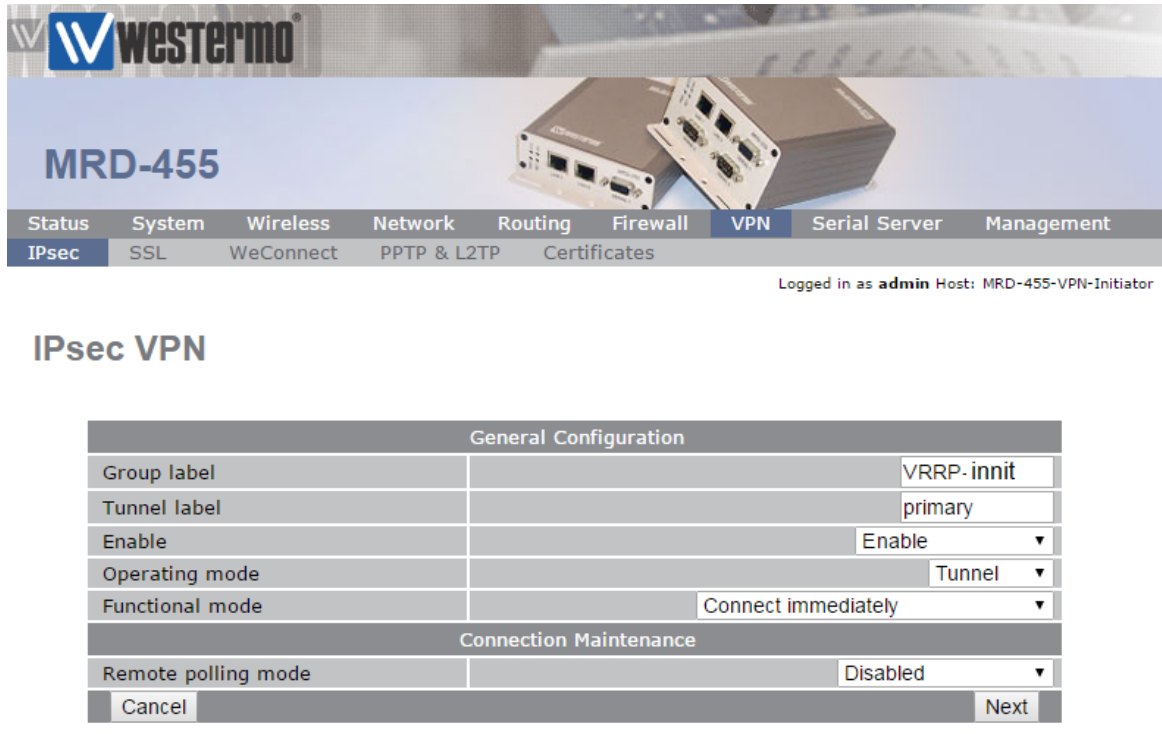
General IPsec Configuration	
Enabled	<input checked="" type="checkbox"/>
NAT traversal enabled & keepalive period (secs)	<input checked="" type="checkbox"/> 45
Overwrite IPsec MTU	<input type="checkbox"/>
Enable extended logging	<input type="checkbox"/>
<a href="#">Reset</a>	<a href="#">Update</a>

Tunnels						
Group	Tunnel	Enable	Remote Host	Remote ID	Edit	Del
No tunnels configured.						
<a href="#">Add new tunnel group</a>						

Click **Add new tunnel group**.

# MRD-455 4G Router Configuration

## IPSec VPN Tunnel Configuration (Initiator)



The screenshot shows the Westermo MRD-455 configuration interface. The 'VPN' menu is selected, and the 'IPsec' sub-menu is active. The 'General Configuration' section is expanded, showing the following settings:

General Configuration	
Group label	VRRP-init
Tunnel label	primary
Enable	Enable
Operating mode	Tunnel
Functional mode	Connect immediately

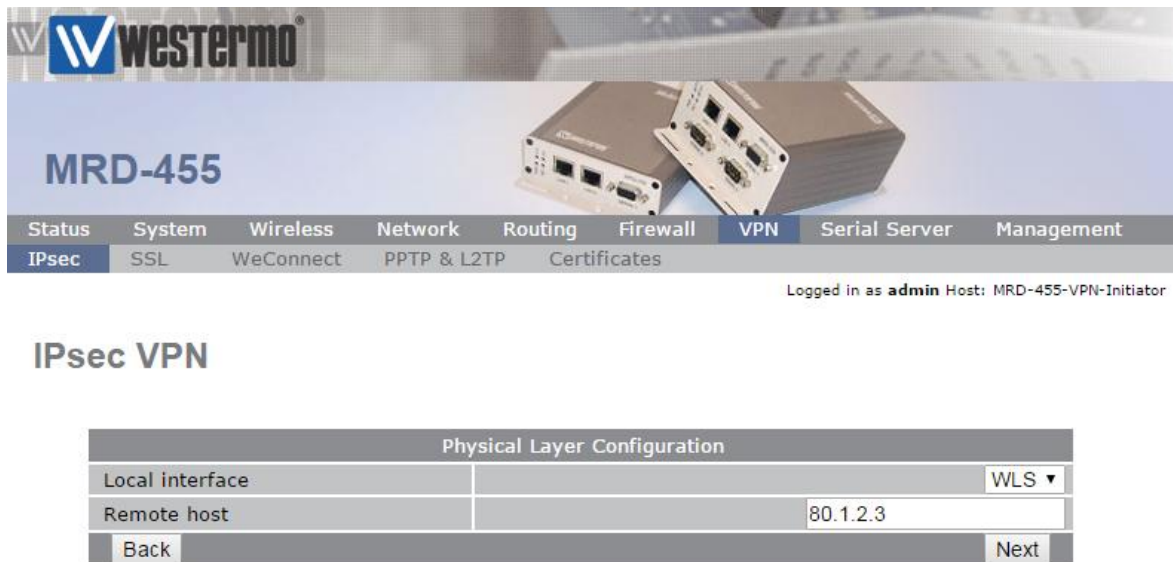
The 'Connection Maintenance' section is also visible, with 'Remote polling mode' set to 'Disabled'.

**Group label:** Free Text – tunnel description only

**Enable:** Enable

**Operating mode:** Tunnel (default)

**Functional Mode:** Connect immediately (i.e. tunnel initiator)



The screenshot shows the 'Physical Layer Configuration' section of the MRD-455 configuration interface. The settings are as follows:

Physical Layer Configuration	
Local interface	WLS
Remote host	80.1.2.3

**Local Interface:** WLS (i.e. the 4G wireless interface)

**Remote Host:** The static broadband IP address of **your ADSL-350**



# MRD-455 4G Router Configuration

## IPSec VPN Tunnel Configuration (Initiator)

### Phase 1 (IKE)



### IPsec VPN

Phase 1 Configuration	
Authentication method	Preshared key ▼
Negotiation mode	Aggressive mode ▼
Pre-shared key	Set New: <input checked="" type="checkbox"/> topsecret
Remote ID	@adsl350
Local ID	@mrd455
Phase 1 Encryption	
IKE proposal	AES (128) ▼ - SHA1 ▼ - DH Grp 2 (1024) ▼
IKE lifetime (mins)	60
Back	Next

**Authentication Method:** Preshared Keys

**Negotiation Mode:** Aggressive Mode

**NB:** Aggressive Mode is for when the initiator has a dynamic WAN IP address.

**Pre-Shared Key:** “top secret”

**NB:** Pre-shared key can be any alphanumeric string but must be identical on both routers (case sensitive).

**Remote ID:** @adsl350

**Local ID:** @mrd455

**NB:** The ID’s can be any string but the @ prefix is mandatory. ID’s must match on both routers.

**IKE proposal:** AES(128)-SHA1-DH Group 2 (1024)

**IKE Lifetime (mins):** 60

# MRD-455 4G Router Configuration

## IPSec VPN Tunnel Configuration (Initiator)

### Phase 2 (IPSec)



Logged in as **admin** Host: MRD-455-VPN-Initiator

### IPsec VPN

Phase 2 Configuration	
Authentication method	None ▾
Phase 2 Encryption	
ESP proposal	AES (128) ▾ - SHA1 ▾
Perfect forward secrecy & group	<input checked="" type="checkbox"/> DH Grp 2 (1024) ▾
Key lifetime (mins)	480
Back	Next

**Authentication Method:** None

**ESP proposal:** AES(128)-SHA1

**Perfect forward secrecy & group:** ✓ DH Grp 2 (1024)

**Key Lifetime (mins):** 480

# MRD-455 4G Router Configuration

## IPSec VPN Tunnel Configuration (Initiator)

### Tunnel Options



MRD-455

Status System Wireless Network Routing Firewall **VPN** Serial Server Management

IPsec SSL WeConnect PPTP & L2TP Certificates

Logged in as **admin** Host: MRD-455-VPN-Initiator

### IPsec VPN

Tunnel Options			
Allow rekeying, margin (mins) & fuzz (%)	<input checked="" type="checkbox"/>	10	100
Allow dead peer detection, delay (sec) & timeout (sec)	<input checked="" type="checkbox"/>	30	120
Clear route when tunnel down	<input checked="" type="checkbox"/>		
Back			Next

**Clear route when tunnel down:** ✓

Leave the rest at default

### Tunnel Networks



MRD-455

Status System Wireless Network Routing Firewall **VPN** Serial Server Management

IPsec SSL WeConnect PPTP & L2TP Certificates

Logged in as **admin** Host: MRD-455-VPN-Initiator

### IPsec VPN

Tunnel Networks			
Enabled		Network	Address
<input checked="" type="checkbox"/>	Local	LAN subnet	
	Remote	Specify a subnet	192.168.2.0/24

**Local:** Lan Subnet

**Remote → Specify a subnet:** 192.168.2.0/24

# MRD-455 4G Router Configuration

## IPSec VPN Tunnel Configuration (Initiator)



### IPsec VPN

General IPsec Configuration	
Enabled	<input checked="" type="checkbox"/>
NAT traversal enabled & keepalive period (secs)	<input checked="" type="checkbox"/> 45
Overwrite IPsec MTU	<input type="checkbox"/>
Enable extended logging	<input type="checkbox"/>
<input type="button" value="Reset"/> <input type="button" value="Update"/>	

Tunnels						
Group	Tunnel	Enable	Remote Host	Remote ID	Edit	Del
VRRP-innit	primary	Enable	80.X.X.X	@adsI350		
	<input type="button" value="Add backup tunnel"/>					
<input type="button" value="Add new tunnel group"/>						

**General IPsec Configuration.**

**Enabled:** ✓

**General IPsec Configuration.**

**Enable:** Enable

# ADSL-350 Broadband Router Configuration

LAN IP Address

Browse to Network → LAN



The screenshot shows the Westermo ADSL-350 web interface. At the top, there is a navigation menu with tabs for Status, System, ADSL, Network, Routing, Firewall, VPN, Serial Server, and Management. The 'Network' tab is selected, and a sub-menu shows 'LAN', 'Loopback', 'DNS', 'GRE', and 'Diagnostics'. The 'LAN' sub-tab is active. Below the navigation, the user is logged in as 'admin' on host 'ADSL-350-e0-4e-a6'. The main content area is titled 'LAN' and displays an 'Interface Configuration' table. The table has four rows: 'Enabled' (checked), 'IP Address' (192.168.2.200), 'Netmask' (255.255.255.0), and 'MTU' (1500). The IP Address and Netmask fields are highlighted with a red box.

Interface Configuration	
Enabled	<input checked="" type="checkbox"/>
IP Address	192.168.2.200
Netmask	255.255.255.0
MTU	1500

**IP Address:** 192.168.2.200

**Netmask:** 255.255.255.0



# ADSL-350 Broadband Router Configuration

## ADSL Link

Browse to ADSL → CONNECTION



Click Add new profile.



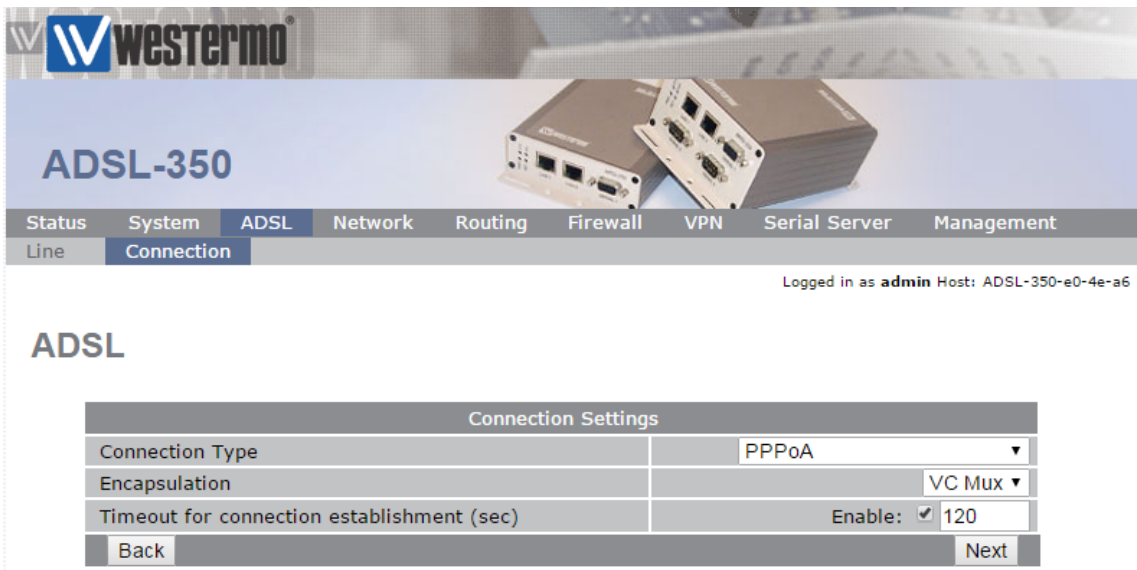
Default settings for a UK BT Broadband line.



# ADSL-350 Broadband Router Configuration

## ADSL Link

Browse to ADSL → CONNECTION continued..



The screenshot shows the Westermo ADSL-350 web interface. The navigation menu includes Status, System, ADSL, Network, Routing, Firewall, VPN, Serial Server, and Management. The 'ADSL' section is active, and the 'Connection' sub-tab is selected. The user is logged in as 'admin' on host 'ADSL-350-e0-4e-a6'. The 'ADSL' section contains a 'Connection Settings' table with the following fields:

Connection Settings	
Connection Type	PPPoA
Encapsulation	VC Mux
Timeout for connection establishment (sec)	Enable: <input checked="" type="checkbox"/> 120
<input type="button" value="Back"/> <input type="button" value="Next"/>	

Default settings for a UK BT Broadband line.



The screenshot shows the Westermo ADSL-350 web interface. The navigation menu is the same as in the previous screenshot. The user is logged in as 'admin' on host 'ADSL-350-e0-4e-a6'. The 'ADSL' section contains a 'PPP Settings' table with the following fields:

PPP Settings	
User	your_broadband_username
Password	Set New: <input checked="" type="checkbox"/> your_broadband_password
Service	
Authentication	Auto
Automatically obtain DNS	<input checked="" type="checkbox"/>
Debug to system log	<input type="checkbox"/>
MTU	1492
<input type="button" value="Back"/> <input type="button" value="Submit"/>	

**User:** Your broadband username

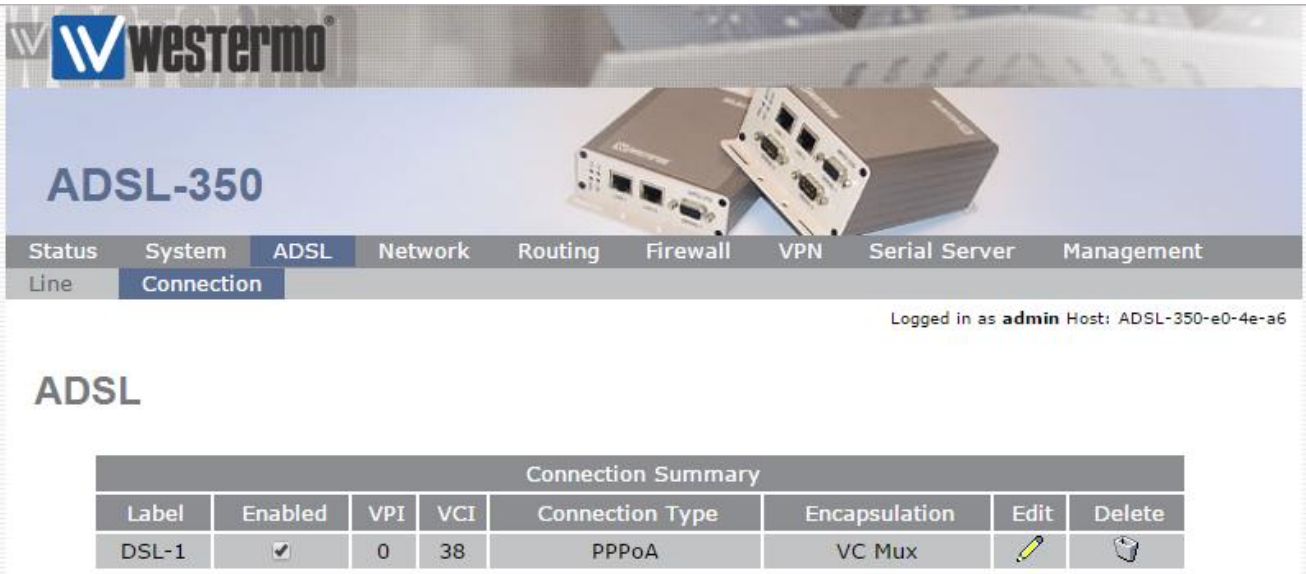
**Password:** Your broadband password

**NB:** These details are issued by your broadband provider.



# ADSL-350 Broadband Router Configuration

## ADSL Link

Browse to ADSL → CONNECTION continued..



The screenshot shows the Westermo ADSL-350 configuration web interface. At the top, there is a navigation menu with tabs for Status, System, ADSL, Network, Routing, Firewall, VPN, Serial Server, and Management. The ADSL tab is selected, and within it, the 'Connection' sub-tab is active. Below the navigation, the text 'Logged in as admin Host: ADSL-350-e0-4e-a6' is visible. The main heading is 'ADSL'. Below this is a table titled 'Connection Summary' with the following data:

Connection Summary							
Label	Enabled	VPI	VCI	Connection Type	Encapsulation	Edit	Delete
DSL-1	<input checked="" type="checkbox"/>	0	38	PPPoA	VC Mux		

### Broadband settings complete

**NB:** These are standard BT ADSL broadband settings. Contact your broadband provider for details.

# ADSL-350 Broadband Router Configuration

## IPSec VPN Tunnel Configuration (Responder)

Browse to VPN → IPSec



### IPsec VPN

General IPsec Configuration	
Enabled	<input checked="" type="checkbox"/>
NAT traversal enabled & keepalive period (secs)	<input checked="" type="checkbox"/> 45
Overwrite IPsec MTU	<input type="checkbox"/>
Enable extended logging	<input type="checkbox"/>
<a href="#">Reset</a>	<a href="#">Update</a>

Tunnels						
Group	Tunnel	Enable	Remote Host	Remote ID	Edit	Del
No tunnels configured.						
<a href="#">Add new tunnel group</a>						

Click **Add new tunnel group**.

# ADSL-350 Broadband Router Configuration

## IPSec VPN Tunnel Configuration (Responder)



### IPsec VPN

General Configuration	
Group label	VPN-Resp
Tunnel label	primary
Operating mode	Tunnel ▾
Functional mode	Responder or Connect on demand ▾
Connection Maintenance	
Remote polling mode	Disabled ▾
Cancel	Next

**Group label:** Free Text – tunnel description only

**Operating mode:** Tunnel (default)

**Functional Mode:** Responder or Connect on demand



### IPsec VPN

Physical Layer Configuration	
Local interface	DSL-1 ▾
Remote host has fixed address	<input type="checkbox"/>
Back	Next

**Local Interface:** DSL-1 (i.e. the broadband interface)

**Remote host has fixed address:** Uncheck.

**NB:** Allows connection from dynamic IP

# ADSL-350 Broadband Router Configuration

## IPSec VPN Tunnel Configuration (Responder)

### Phase 1 (IKE)



### IPsec VPN

Phase 1 Configuration	
Authentication method	Preshared key ▾
Negotiation mode	Aggressive mode ▾
Pre-shared key	Not set New: <input checked="" type="checkbox"/> topsecret
Remote ID	@mrd455
Local ID	@adsl350
Phase 1 Encryption	
IKE proposal	AES (128) ▾ - SHA1 ▾ - DH Grp 2 (1024) ▾
IKE lifetime (mins)	60
Back	Next

**Authentication Method:** Preshared Keys

**Negotiation Mode:** Aggressive Mode

**NB:** Aggressive Mode is for when the initiator has a dynamic WAN IP address.

**Pre-Shared Key:** “top secret”

**NB:** Pre-shared key can be any alphanumeric string but must be identical on both routers (case sensitive).

**Remote ID:** @mrd455

**Local ID:** @adsl350

**NB:** The ID's can be any string but the @ prefix is mandatory. ID's must match on both routers.

**IKE proposal:** AES(128)-SHA1-DH Group 2 (1024)

**IKE Lifetime (mins):** 60



# ADSL-350 Broadband Router Configuration

## IPSec VPN Tunnel Configuration (Responder)

### Phase 2 (IPSec)



### IPsec VPN

Phase 2 Configuration	
Authentication method	None ▾
Phase 2 Encryption	
ESP proposal	AES (128) ▾ - SHA1 ▾
Perfect forward secrecy & group	<input checked="" type="checkbox"/> DH Grp 2 (1024) ▾
Key lifetime (mins)	480
Back	Next

**Authentication Method:** None

**ESP proposal:** AES(128)-SHA1

**Perfect forward secrecy & group:** ✓ DH Grp 2 (1024)

**Key Lifetime (mins):** 480



# ADSL-350 Broadband Router Configuration

## IPSec VPN Tunnel Configuration (Responder)

### Tunnel Options



The screenshot shows the ADSL-350 configuration interface. The 'VPN' menu is selected, and the 'IPsec' sub-menu is active. The navigation bar includes: Status, System, ADSL, Network, Routing, Firewall, VPN, Serial Server, and Management. The sub-menu includes: IPsec, SSL, WeConnect, PPTP & L2TP, and Certificates. The user is logged in as 'admin' on host 'ADSL-350-VRRP-Master'.

### IPsec VPN

Tunnel Options			
Allow rekeying, margin (mins) & fuzz (%)	<input checked="" type="checkbox"/>	10	100
Allow dead peer detection, delay (sec) & timeout (sec)	<input checked="" type="checkbox"/>	30	120
Clear route when tunnel down	<input type="checkbox"/>		
Back		Next	

**Clear route when tunnel down:** Uncheck (applies to initiators only)

### Tunnel Networks



The screenshot shows the ADSL-350 configuration interface. The 'VPN' menu is selected, and the 'Tunnel Networks' sub-menu is active. The navigation bar includes: Status, System, ADSL, Network, Routing, Firewall, VPN, Serial Server, and Management. The sub-menu includes: IPsec, SSL, WeConnect, PPTP & L2TP, and Certificates. The user is logged in as 'admin' on host 'ADSL-350-VRRP-Master'.

### IPsec VPN

Tunnel Networks			
Enabled		Network	Address
<input checked="" type="checkbox"/>	Local	LAN subnet	
	Remote	Specify a subnet	172.30.1.0/24

**Local:** Lan Subnet

**Remote → Specify a subnet:** 172.30.1.0/24

# ADSL-350 Broadband Router Configuration

## IPSec VPN Tunnel Configuration (Responder)



The screenshot shows the Westermo ADSL-350 web interface. The navigation menu includes: Status, System, ADSL, Network, Routing, Firewall, VPN (selected), Serial Server, and Management. The VPN sub-menu includes: IPsec (selected), SSL, WeConnect, PPTP & L2TP, and Certificates. The user is logged in as 'admin' on host 'ADSL-350-VRRP-Master'.

### IPsec VPN

General IPsec Configuration	
Enabled	<input checked="" type="checkbox"/>
NAT traversal enabled & keepalive period (secs)	<input checked="" type="checkbox"/> 45
Overwrite IPsec MTU	<input type="checkbox"/>
Enable extended logging	<input type="checkbox"/>
<input type="button" value="Reset"/>	<input type="button" value="Update"/>

Tunnels						
Group	Tunnel	Enable	Remote Host	Remote ID	Edit	Del
VPN-Resp	primary	<input checked="" type="checkbox"/>	Any	@mrd455		
	<input type="button" value="Add backup tunnel"/>					
<input type="button" value="Add new tunnel group"/>						

**General IPsec Configuration.**

**Enabled:** ✓

**General IPsec Configuration.**

**Enable:** ✓

# ADSL-350 Broadband Router Configuration

## Firewall

By default, all incoming traffic to the router is blocked in the firewall. Therefore IPsec VPN traffic needs to be allowed in to the DSL interface.

Browse to **Firewall → Access Control**



## Access Control

External Access Control	Incoming Interface						
	DSL-1		VPN		GRE		
Default policy	Deny ▼		Allow ▼		Deny ▼		
Services	Allow	Port	Allow	Port	Allow	Port	
Web Server	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	80	<input type="checkbox"/>	80	
Secure Web Server	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	443	<input type="checkbox"/>	443	
Telnet Server	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	23	<input type="checkbox"/>	23	
SSH	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	22	<input type="checkbox"/>	22	
SNMP	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	161	<input type="checkbox"/>	161	
GRE	<input type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>		
Dynamic routing	<input type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>		
DNP3	<input type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>		
<b>IPsec VPN</b>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>		
Serial Server	<input type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>		
Respond to ICMP (Ping)	<input type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>		
Reset						Update	

In the **DSL-1** tick IPsec VPN to allow inbound VPN traffic.

# VPN STATUS

## MRD-455

Browse to **Status** → **Alarms**

Check that the **VPN** status is set to **No Fault**.



### Alarms

13:55:51 26/10/2016

System	
Power On Self Test	Passed
Temperature (°C)	now: 31.75, min: 31.25, max: 31.75
Uptime	00:05:13
Wireless	
Network Status	No Fault
Connection Status	No Fault
Network	
LAN	No Fault
Loopback	No Fault
Services	
DHCP Server	No Fault
VPN	No Fault
Serial Server	Disabled

Double check that the VPN is connected by browsing to **Status** → **VPN**



### VPN

IPsec Connection Status							
Label	Tunnel	Status	Uptime	Time Since Rekey	Local IP	Connection Management	
						Status	Restarts
VRRP-Resp	primary	Connected	00:00:27	00:00:27	172.30.1.2	Disabled	

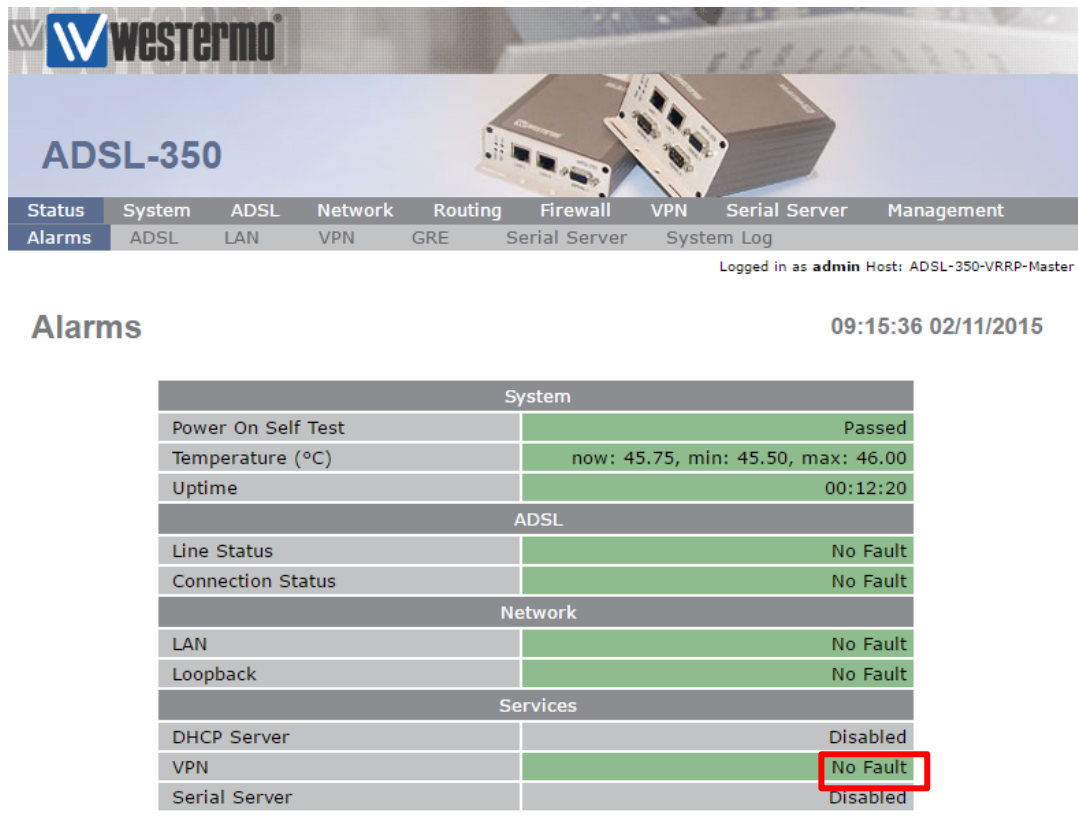
[Detailed IPsec status](#)

# VPN STATUS

## ADSL-350

Browse to **Status** → **Alarms**

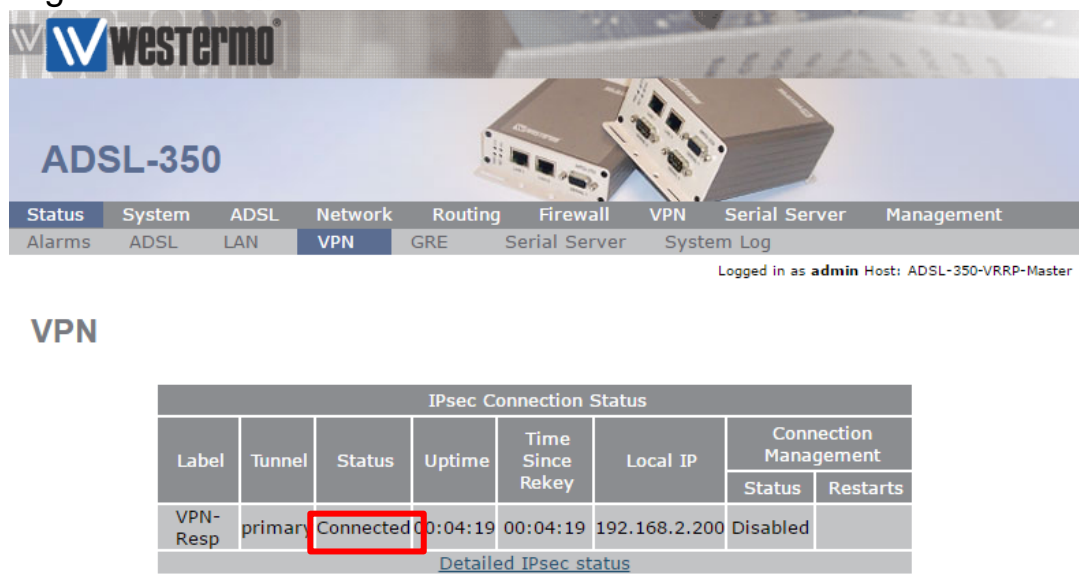
Check that the **VPN** status is set to **No Fault**.



The screenshot shows the Westermo ADSL-350 management interface. The 'Alarms' tab is selected in the top navigation bar. The page title is 'ADSL-350' and the user is logged in as 'admin' on host 'ADSL-350-VRRP-Master'. The time is 09:15:36 on 02/11/2015. A table displays the status of various system components:

System		
Power On Self Test		Passed
Temperature (°C)	now: 45.75, min: 45.50, max: 46.00	
Uptime		00:12:20
ADSL		
Line Status		No Fault
Connection Status		No Fault
Network		
LAN		No Fault
Loopback		No Fault
Services		
DHCP Server		Disabled
VPN		No Fault
Serial Server		Disabled

Double check that the VPN is connected by browsing to **Status** → **VPN**



The screenshot shows the Westermo ADSL-350 management interface with the 'VPN' tab selected. The page title is 'ADSL-350' and the user is logged in as 'admin' on host 'ADSL-350-VRRP-Master'. The time is 09:15:36 on 02/11/2015. A table displays the IPsec Connection Status:

IPsec Connection Status							
Label	Tunnel	Status	Uptime	Time Since Rekey	Local IP	Connection Management	
						Status	Restarts
VPN-Resp	primary	Connected	00:04:19	00:04:19	192.168.2.200	Disabled	

[Detailed IPsec status](#)



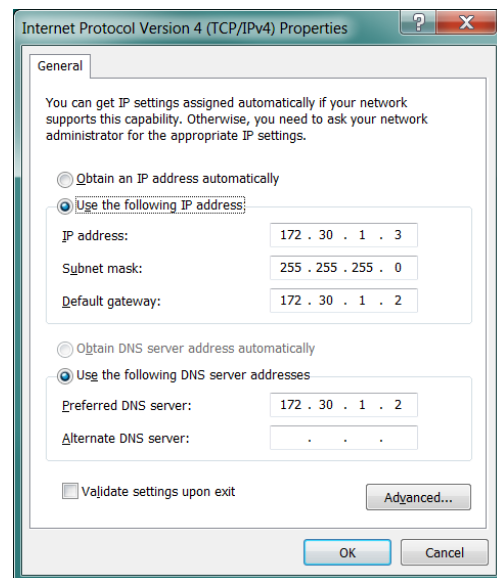
## TESTING

**NB:** The following assumes that the router settings have been applied exactly as set out in this application note.

### MRD-455

Connect an ethernet cable from a PC or Laptop to LAN port 1 on the MRD-455. Set your PC's TCP/IP settings as follows;

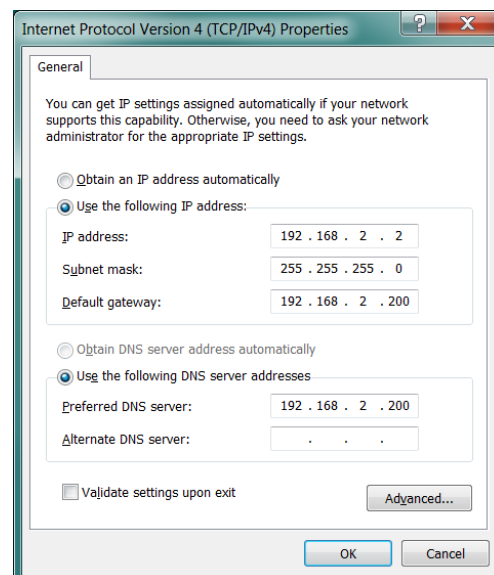
**IP address:** 172.30.1.3  
**Subnet Mask:** 255.255.255.0  
**Default Gateway:** 172.30.1.2  
**Preferred DNS Server:** 172.30.1.2



### ADSL-350

Connect an ethernet cable from a PC or Laptop to LAN port 1 on the ADSL-350. Set your PC's TCP/IP settings as follows;

**IP address:** 192.168.2.2  
**Subnet Mask:** 255.255.255.0  
**Default Gateway:** 192.168.2.200  
**Preferred DNS Server:** 192.168.2.200





## TESTING

**NB:** The following assumes that the router settings have been applied exactly as set out in this application note.

### MRD-455

From the PC (172.30.1.3) connected to the MRD-455, ping the PC (192.168.2.2) connected to ADSL-350. You should get replies.

```
C:\Windows\System32>ping 192.168.2.2
```

```
Pinging 192.168.2.2 with 32 bytes of data:  
Reply from 192.168.2.2: bytes=32 time=625ms TTL=126  
Reply from 192.168.2.2: bytes=32 time=585ms TTL=126  
Reply from 192.168.2.2: bytes=32 time=471ms TTL=126  
Reply from 192.168.2.2: bytes=32 time=534ms TTL=126
```

```
Ping statistics for 192.168.2.2:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 471ms, Maximum = 625ms, Average = 553ms
```

### ADSL-350

From the PC (192.168.2.2) connected to the ADSL-350, ping the PC (172.30.1.3) connected to MRD-455. You should get replies.

```
C:\Windows\System32>ping 172.30.1.3
```

```
Pinging 172.30.1.3 with 32 bytes of data:  
Reply from 172.30.1.3: bytes=32 time=579ms TTL=126  
Reply from 172.30.1.3: bytes=32 time=419ms TTL=126  
Reply from 172.30.1.3: bytes=32 time=442ms TTL=126  
Reply from 172.30.1.3: bytes=32 time=526ms TTL=126
```

```
Ping statistics for 172.30.1.3:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 419ms, Maximum = 579ms, Average = 491ms
```

## TROUBLESHOOTING

If you are having problems making a connection to the PC at the other end of the VPN tunnel. See the following checklist.

### VPN Status

On both routers browse to the **Status → Alarms** and **Status → VPN pages** and check the VPN is connected.

### PC Settings

On both PC's check that the Default Gateway is set to the IP address of your *local* router.

### PC – Disable all other connections.

To ensure your traffic is going via your Westermo routers and not over another network interface, disable all other connections on both PC's – particularly make sure WiFi is turned off and any other VPN's configured on your PC are disabled.

## Revision history for version 1.0

Revision	Rev by	Revision note	Date
00			
01		Minor changes to wording and amend mistakes to DH groups	
02			
03			
04			
05			
06			
07			



**H E A D   O F F I C E**

**Sweden**

Westermo  
SE-640 40 Stora Sundby  
Tel: +46 (0)16 42 80 00  
Fax: +46 (0)16 42 80 01  
info@westermo.se  
www.westermo.com

**Sales Units**

Westermo Data Communications

**China**

sales.cn@westermo.com  
www.cn.westermo.com

**France**

infos@westermo.fr  
www.westermo.fr

**Germany**

info@westermo.de  
www.westermo.de

**North America**

info@westermo.com  
www.westermo.com

**Singapore**

sales@westermo.com.sg  
www.westermo.com

**Sweden**

info.sverige@westermo.se  
www.westermo.se

**United Kingdom**

sales@westermo.co.uk  
www.westermo.co.uk

**Other Offices**



*For complete contact information, please visit our website at [www.westermo.com/contact](http://www.westermo.com/contact) or scan the QR code with your mobile phone.*