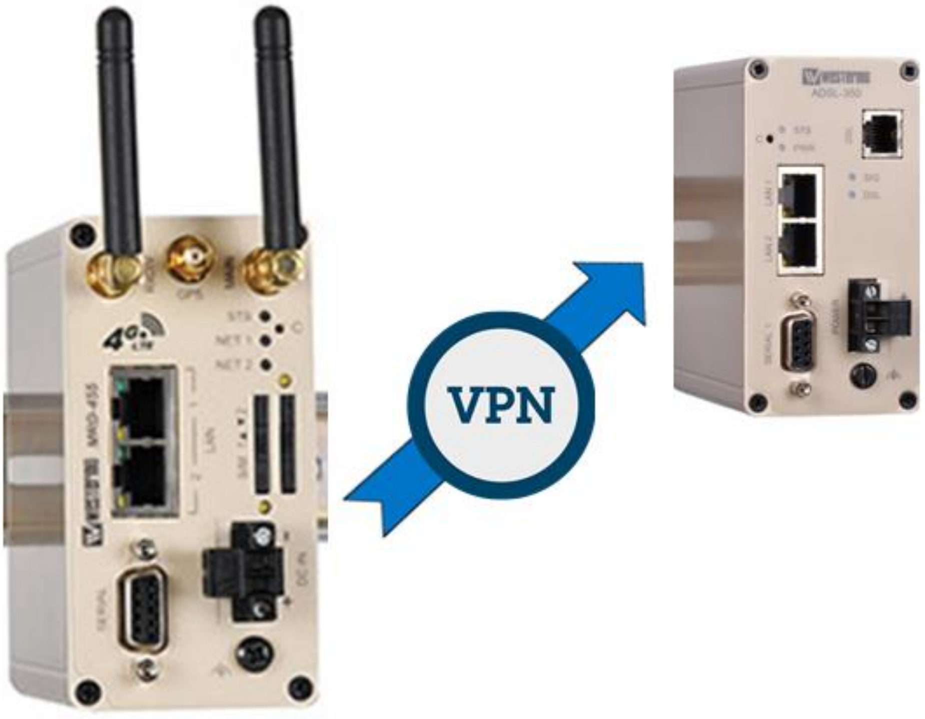
AN-001-WUK

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?

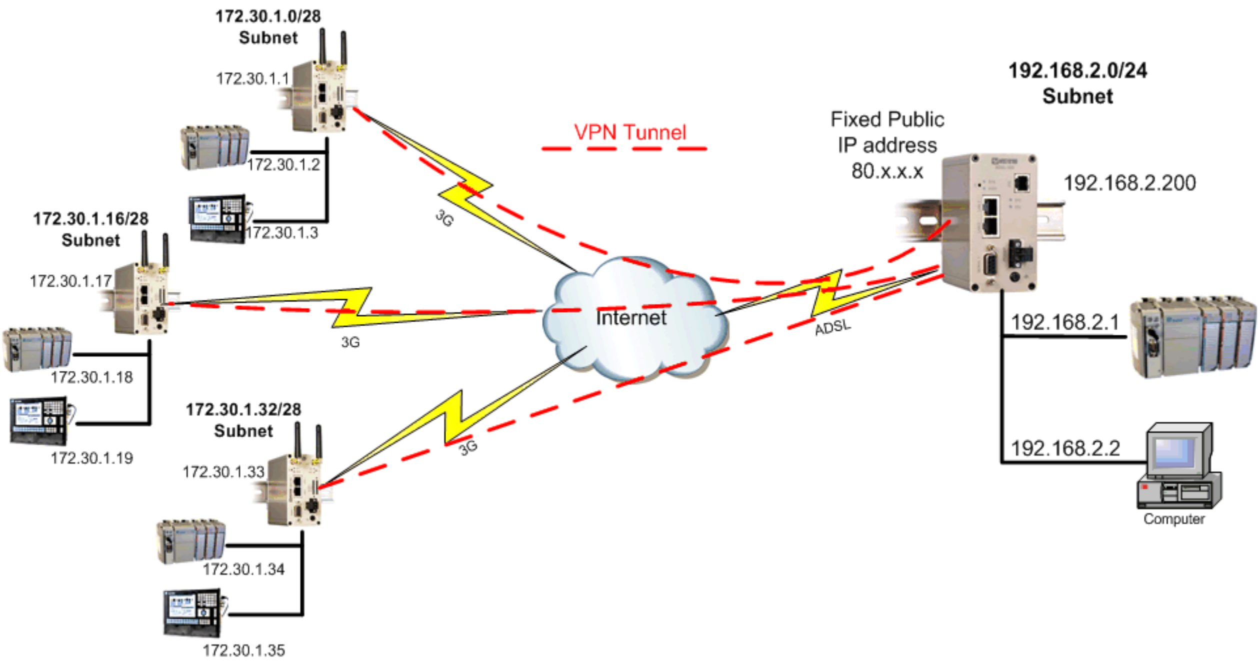
IPSec VPN's create a secure **V**irtual **P**rivate **N**etwork between two or more private LAN networks, over the internet.

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”.

Assummptions

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

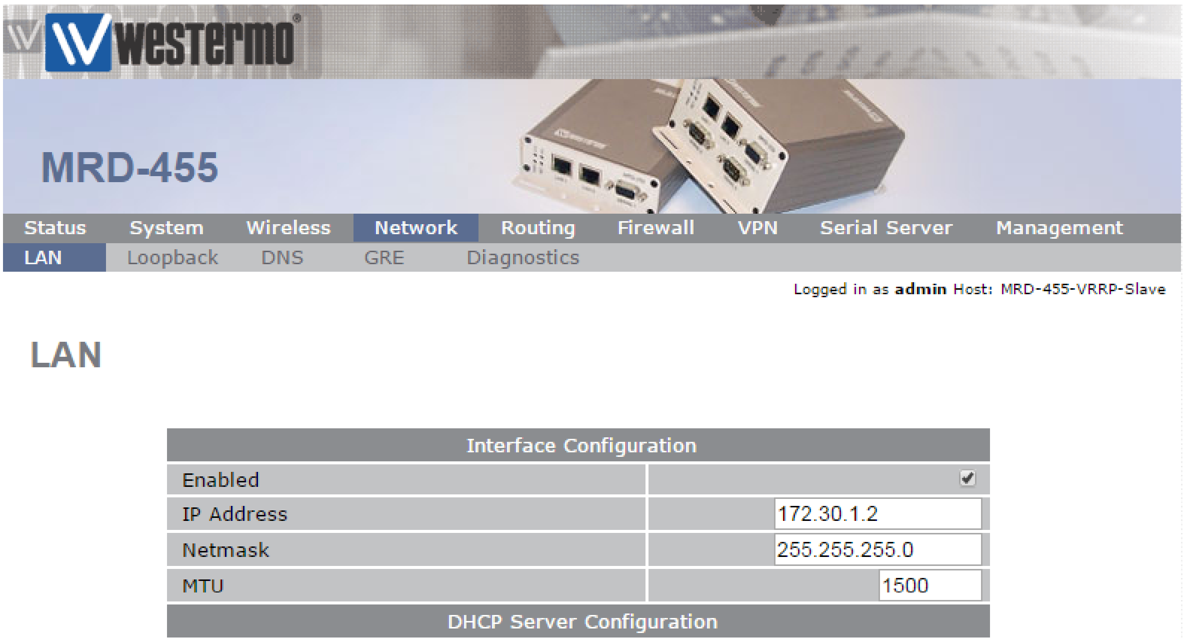
Requests for corrections or amendments to this application note are welcome and should be addressed to technical@westermo.co.uk

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

MRD-455 4G Router Configuration

LAN IP Address

Browse to Network → LAN



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

LAN

Interface Configuration	
Enabled	☑
IP Address	172.30.1.2
Netmask	255.255.255.0
MTU	1500
DHCP Server Configuration	

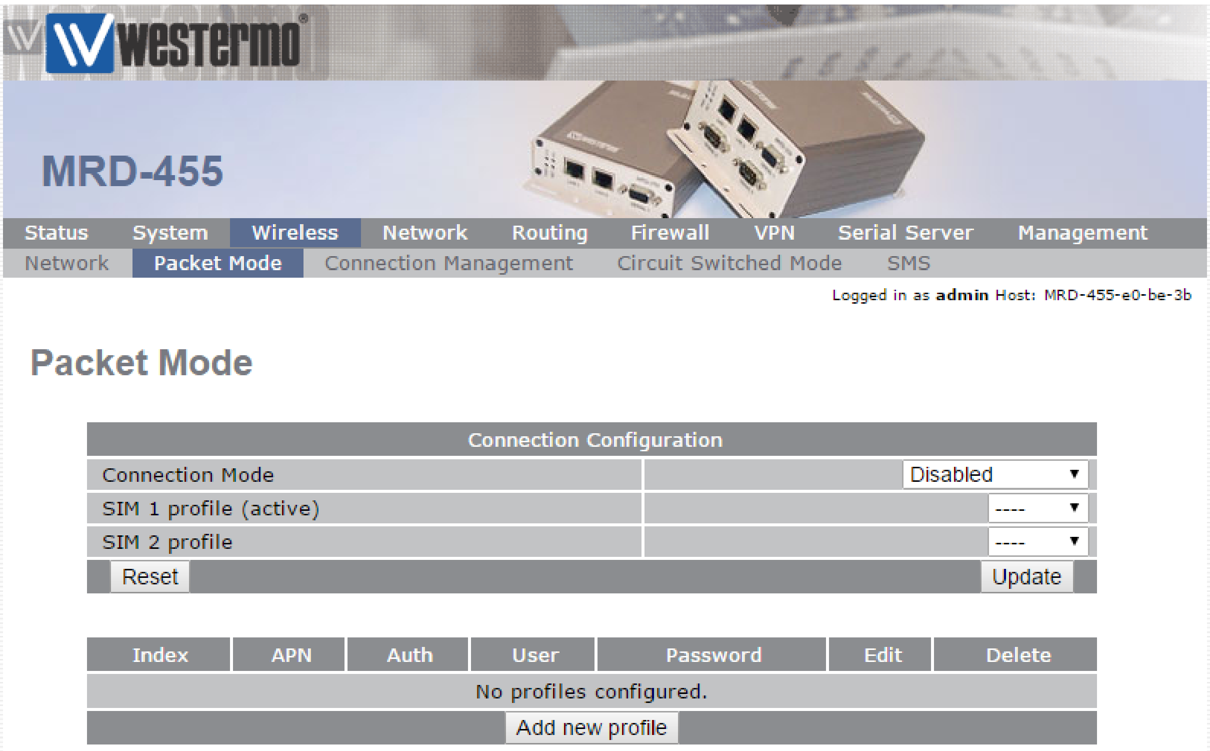
IP Address: 172.30.1.2

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

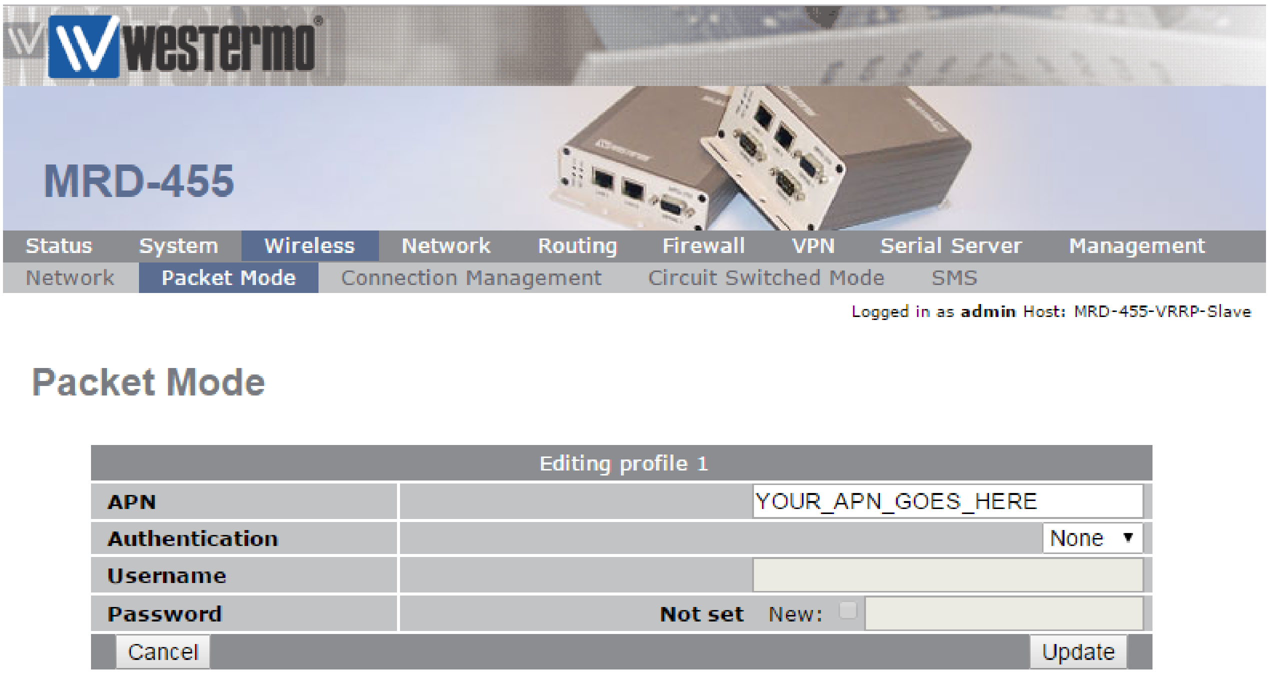
Logged in as **admin** Host: MRD-455-e0-be-3b

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-VRRP-Slave

Packet Mode

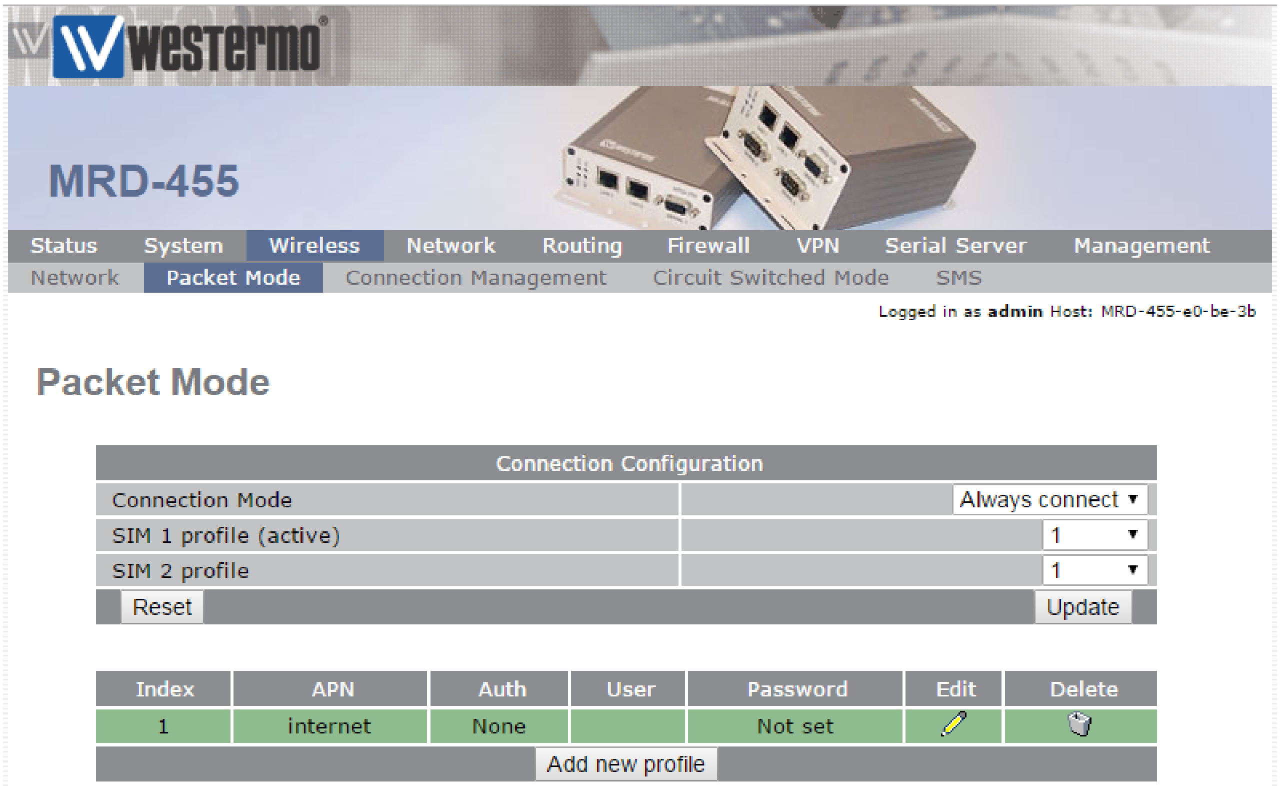
Editing profile 1	
APN	YOUR_APN_GOES_HERE
Authentication	None ▾
Username	
Password	**Not set** New: □
Cancel	Update

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.


westermo
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	Always connect ▾
SIM 1 profile (active)	1 ▾
SIM 2 profile	1 ▾
Reset	Update

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

Add new profile

Connection Mode: Always connect

SIM 1 profile: 1

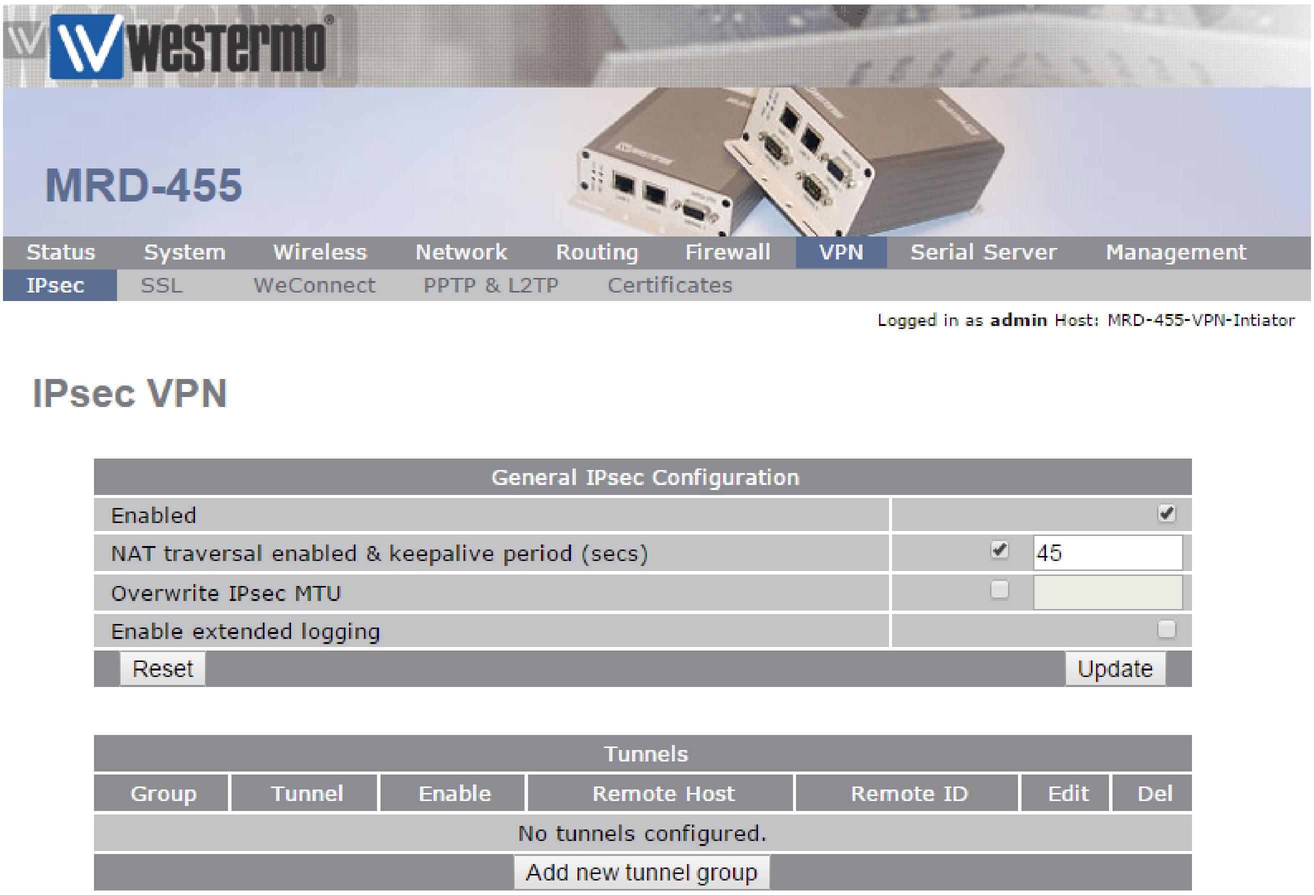
NB: In this example the SIM card in slot 1 will use profile 1. You can set up multiple profiles and assign them to either SIM slot 1 or 2 depending on the provider of the SIM card.

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

MRD-455 4G Router Configuration

IPSec VPN Tunnel Configuration (Initiator)

Browse to VPN → IPSec



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

IPsec VPN

General IPsec Configuration	
Enabled	☑
NAT traversal enabled & keepalive period (secs)	☑ 45
Overwrite IPsec MTU	☐
Enable extended logging	☐
Reset	Update

Tunnels

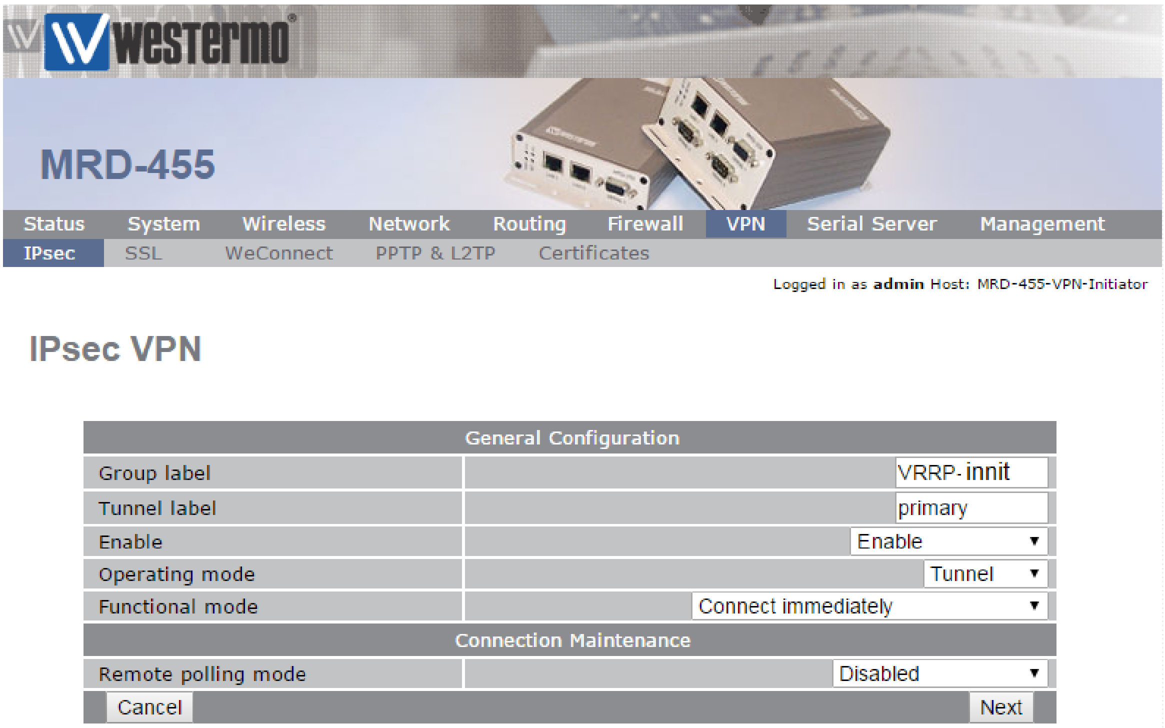
Group	Tunnel	Enable	Remote Host	Remote ID	Edit	Del
No tunnels configured.						

Add new tunnel group

Click **Add new tunnel group.**

MRD-455 4G Router Configuration

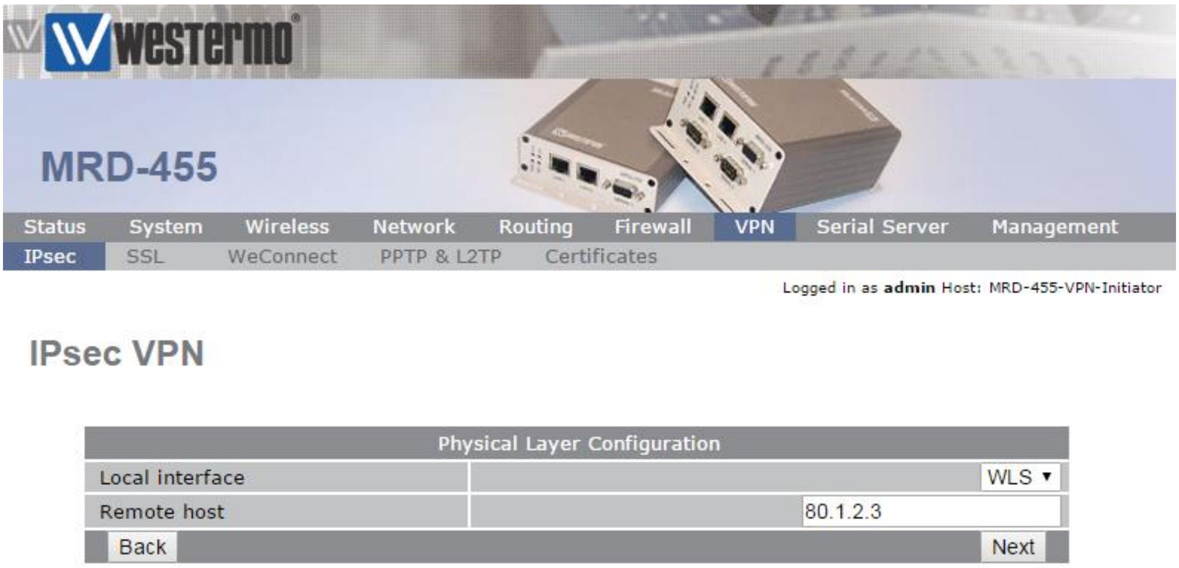
IPSec VPN Tunnel Configuration (Initiator)


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

General Configuration	
Group label	VRRP- innit
Tunnel label	primary
Enable	Enable
Operating mode	Tunnel
Functional mode	Connect immediately
Connection Maintenance	
Remote polling mode	Disabled

Group label: Free Text – tunnel description only
Enable: Enable
Operating mode: Tunnel (default)
Functional Mode: Connect immediately (i.e. tunnel initiator)


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

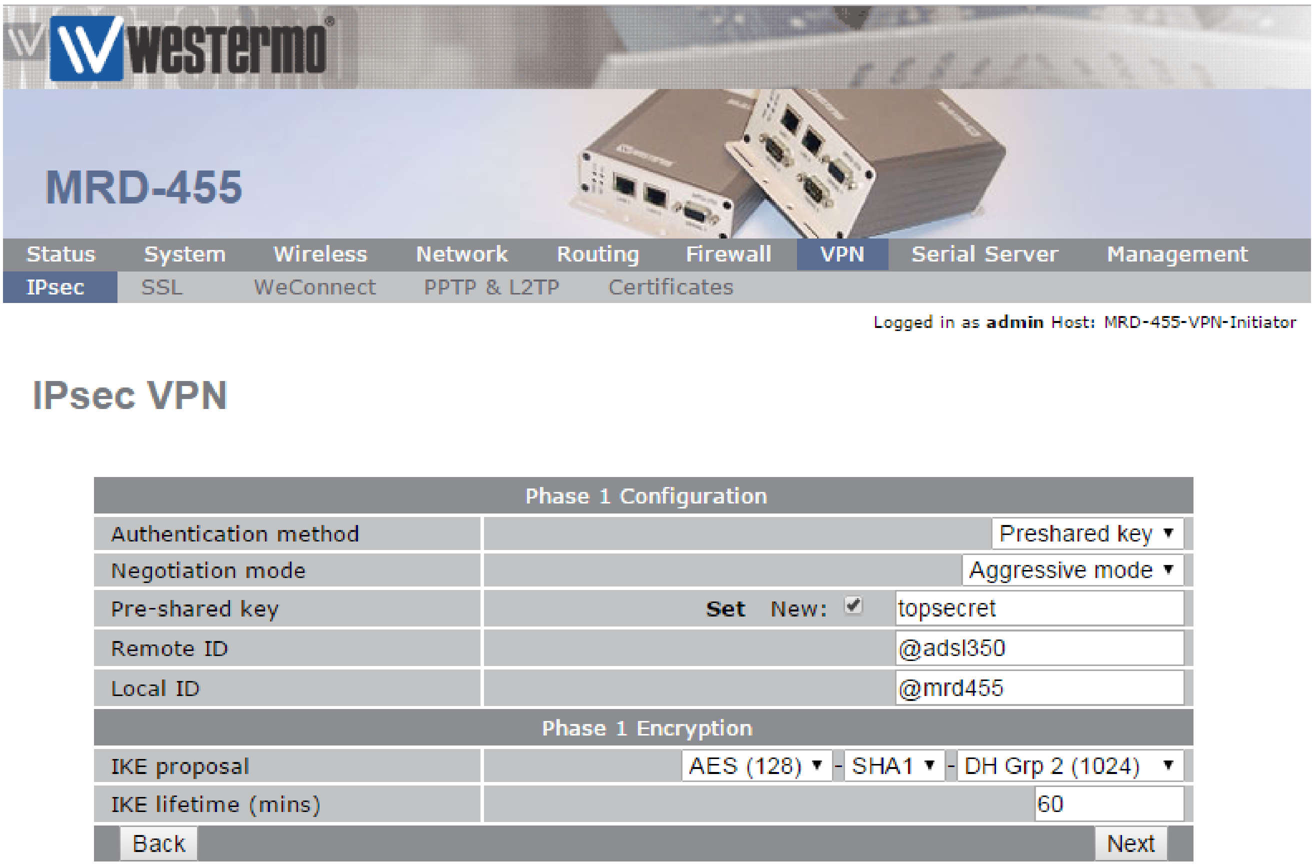
Physical Layer Configuration	
Local interface	WLS
Remote host	80.1.2.3

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)


westermo
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
Back
Next

Phase 1 Configuration	
Authentication method	Preshared key ▾
Negotiation mode	Aggressive mode ▾
Pre-shared key	Set New: ☑ topsecret
Remote ID	@adsl350
Local ID	@mrd455
Phase 1 Encryption	
IKE proposal	AES (128) ▾ - SHA1 ▾ - DH Grp 2 (1024) ▾
IKE lifetime (mins)	60

Authentication Method: Preshared Keys

Negotiation Mode: Aggressive Mode

NB: Aggressive Mode is for when the intitiator 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.

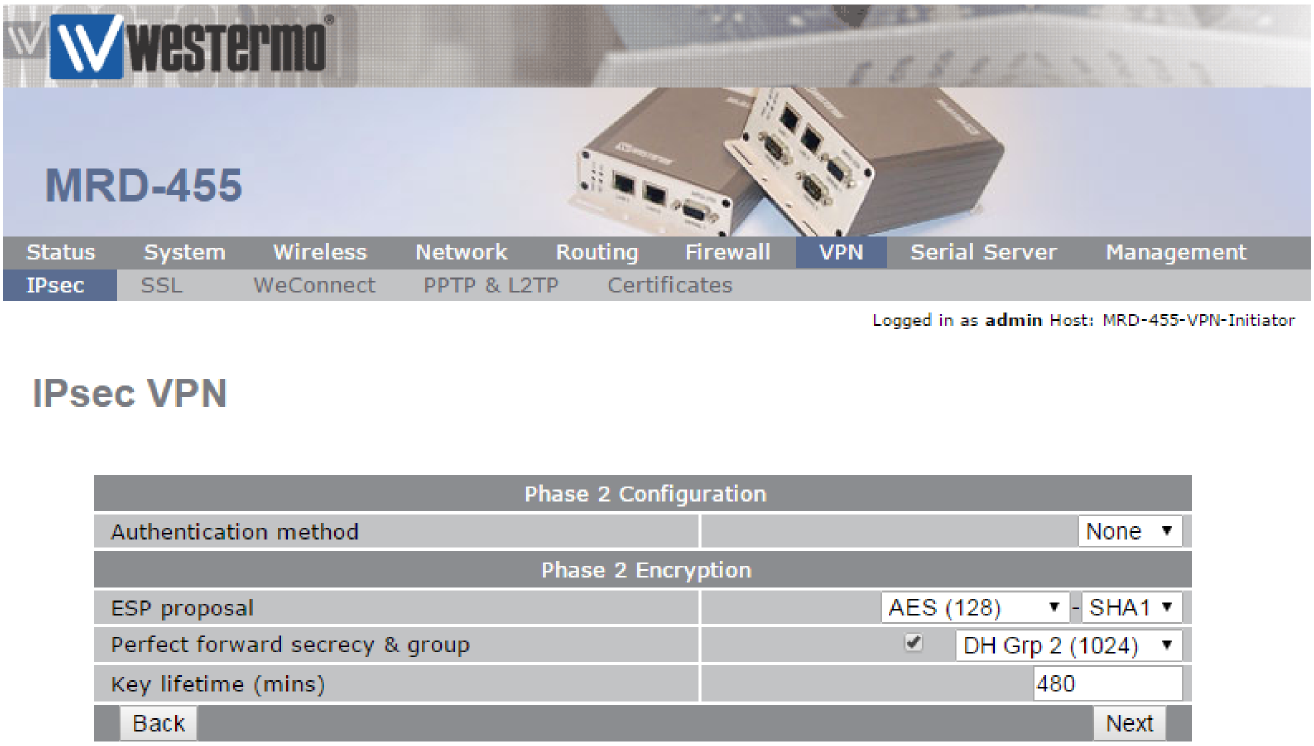
IKE proposal: AES(128)-SHA1-DH Group 2 (1024)

IKE Lifetime (mins): 60

MRD-455 4G Router Configuration

IPSec VPN Tunnel Configuration (Initiator)

Phase 2 (IPSec)


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

Phase 2 Configuration	
Authentication method	None
Phase 2 Encryption	
ESP proposal	AES (128) - SHA1
Perfect forward secrecy & group	☑ DH Grp 2 (1024)
Key lifetime (mins)	480

Authentication Method: None

ESP proposal: AES(128)-SHA1

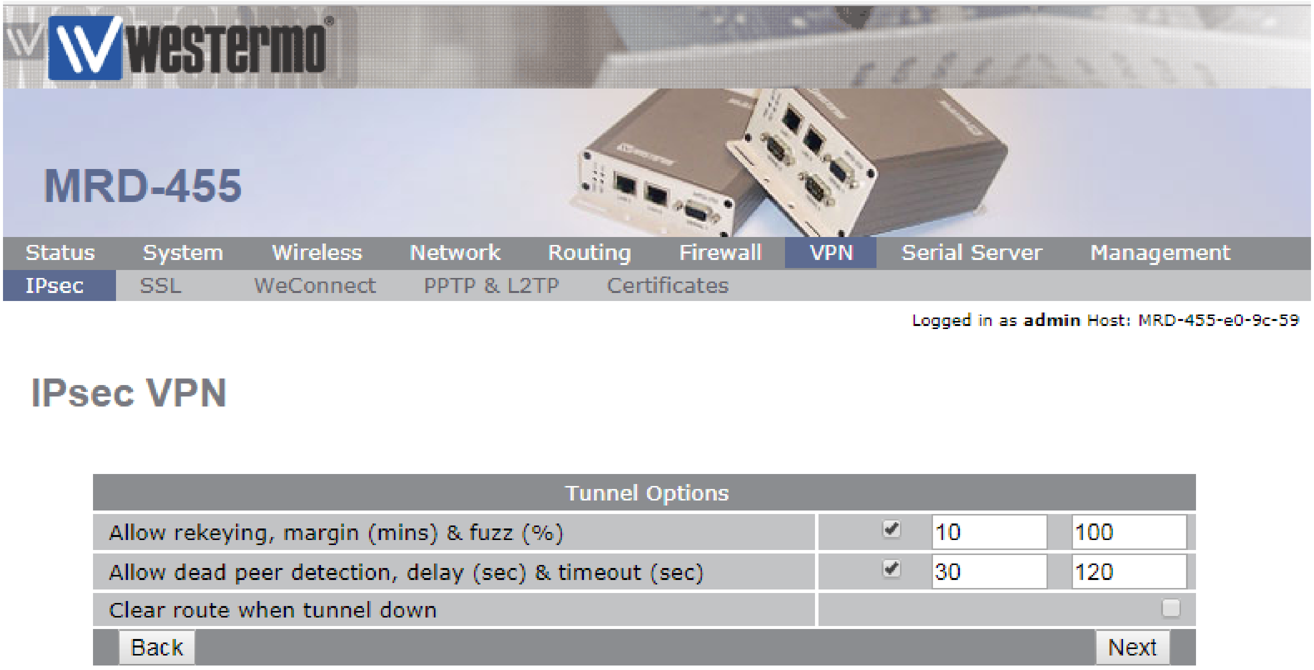
Perfect forward secrecy & group: ✓ DH Grp 2 (1024)

Key Lifetime (mins): 480

MRD-455 4G Router Configuration

IPSec VPN Tunnel Configuration (Initiator)

Tunnel Options

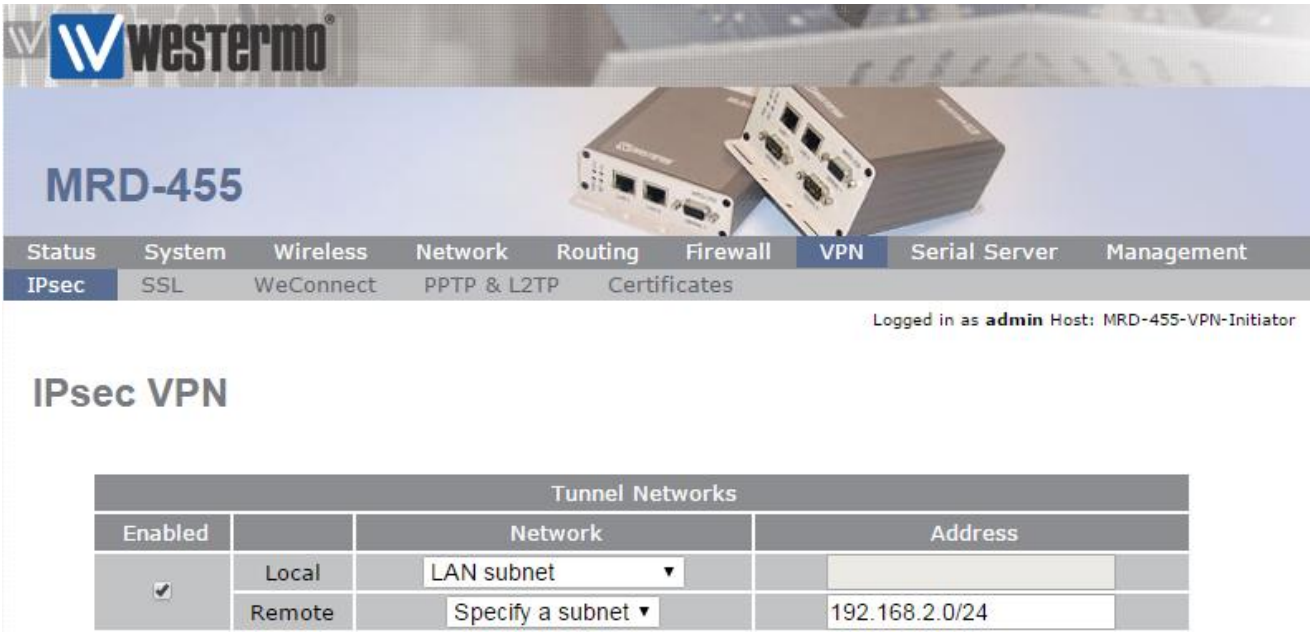


Tunnel Options			
Allow rekeying, margin (mins) & fuzz (%)	☑	10	100
Allow dead peer detection, delay (sec) & timeout (sec)	☑	30	120
Clear route when tunnel down	☐		

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

Leave the rest at default

Tunnel Networks



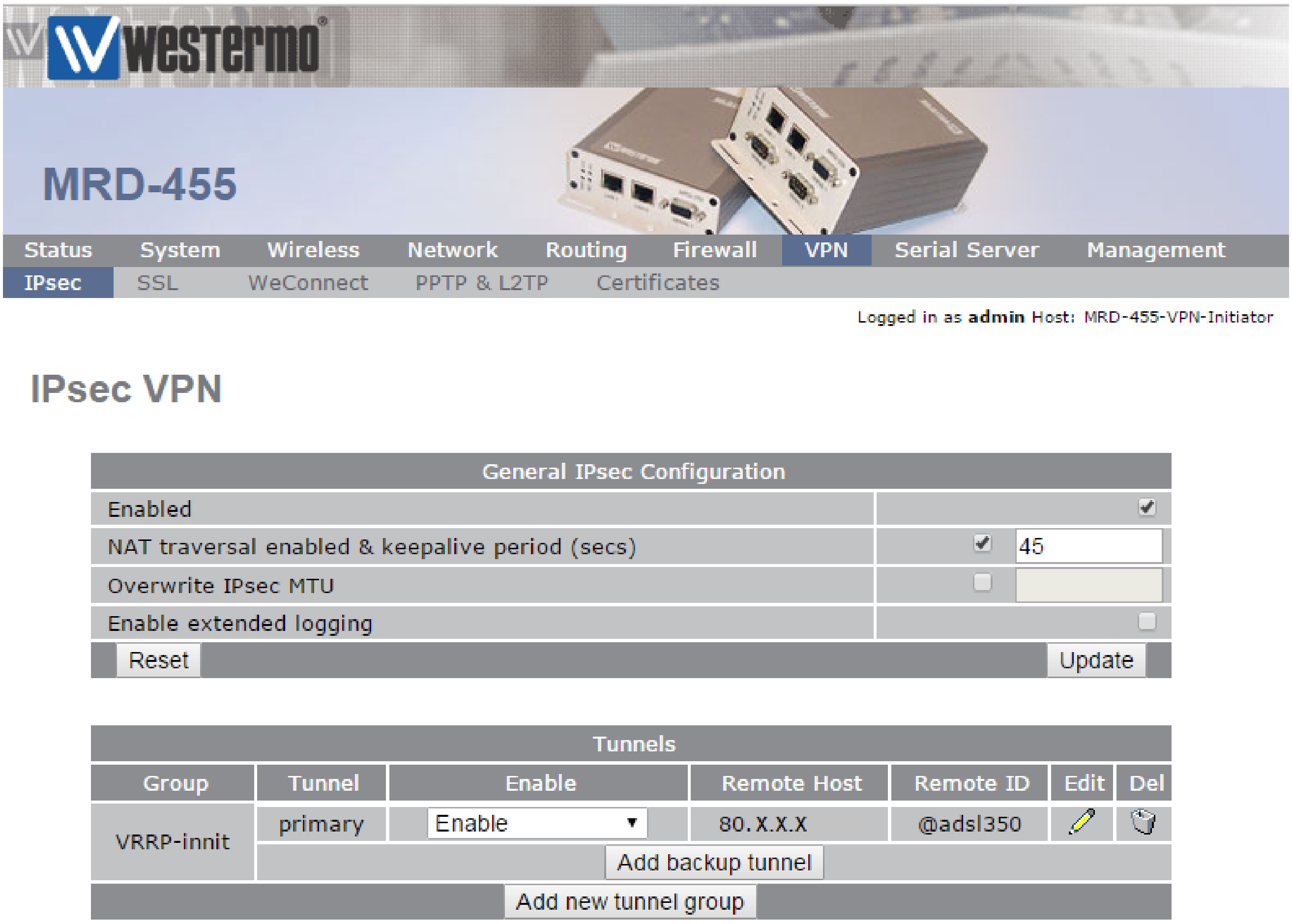
Tunnel Networks			
Enabled		Network	Address
☑	Local	LAN subnet ▾	
	Remote	Specify a subnet ▾	192.168.2.0/24

Local: Lan Subnet

Remote → Specify a subnet: 192.168.2.0./24

MRD-455 4G Router Configuration

IPSec VPN Tunnel Configuration (Initiator)


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

General IPsec Configuration	
Enabled	☑
NAT traversal enabled & keepalive period (secs)	☑ 45
Overwrite IPsec MTU	☐
Enable extended logging	☐
Reset	Update

Tunnels

Group	Tunnel	Enable	Remote Host	Remote ID	Edit	Del
VRRP-innit	primary	Enable ▾	80.X.X.X	@adsl350	✎	🗑
	Add backup tunnel					
Add new tunnel group						

General IPSec Configuration.

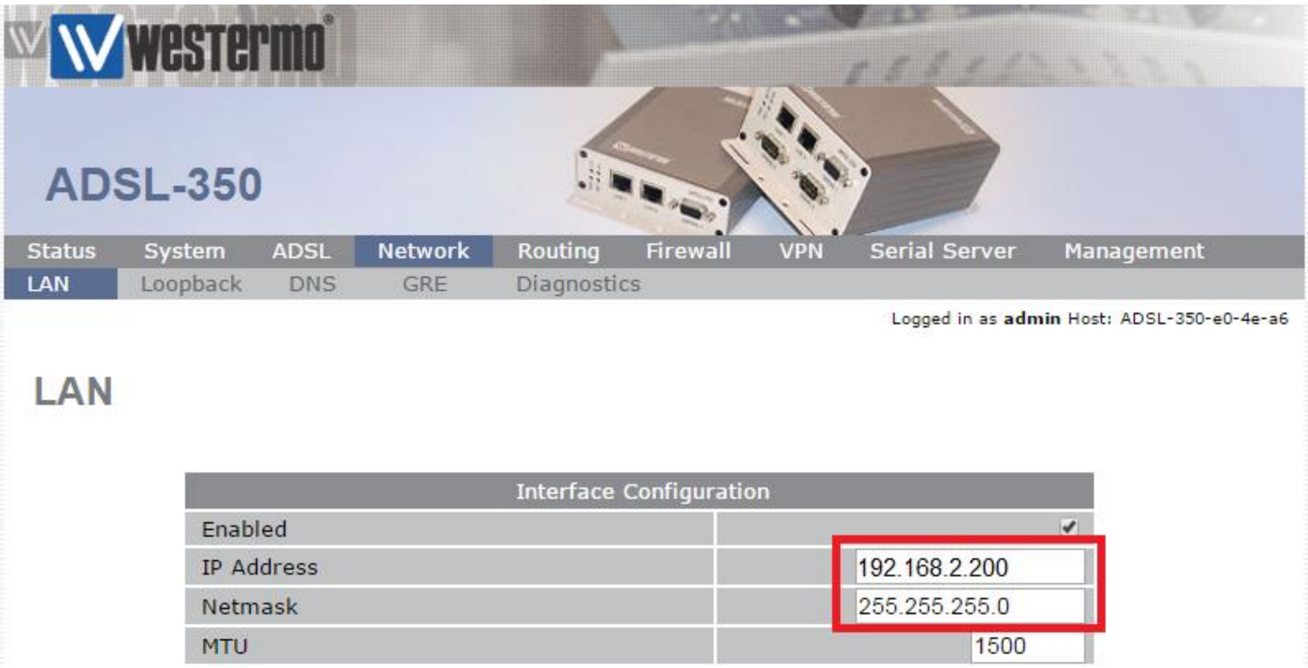
Enabled: ✓

General IPSec Configuration.
Enable: Enable

ADSL-350 Broadband Router Configuration

LAN IP Address

Browse to Network → LAN



Logged in as **admin** Host: ADSL-350-e0-4e-a6

LAN

Interface Configuration	
Enabled	☑
IP Address	192.168.2.200
Netmask	255.255.255.0
MTU	1500

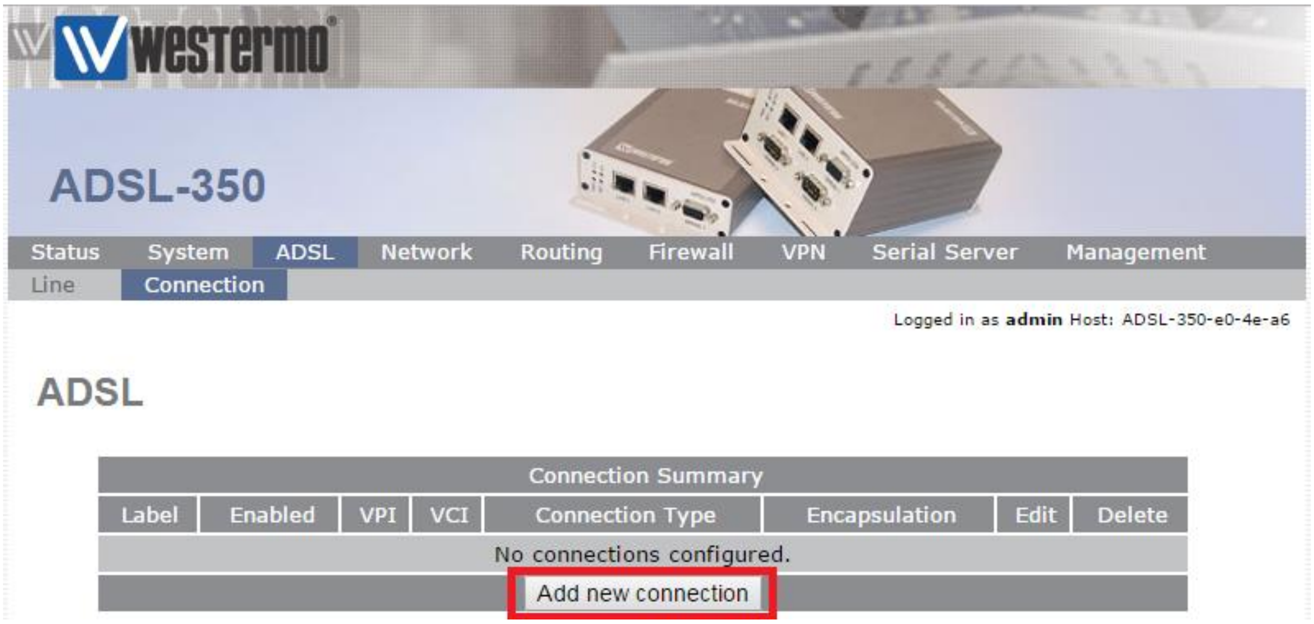
IP Address: 192.168.2.200

Netmask: 255.255.255.0

ADSL-350 Broadband Router Configuration

ADSL Link

Browse to ADSL → CONNECTION

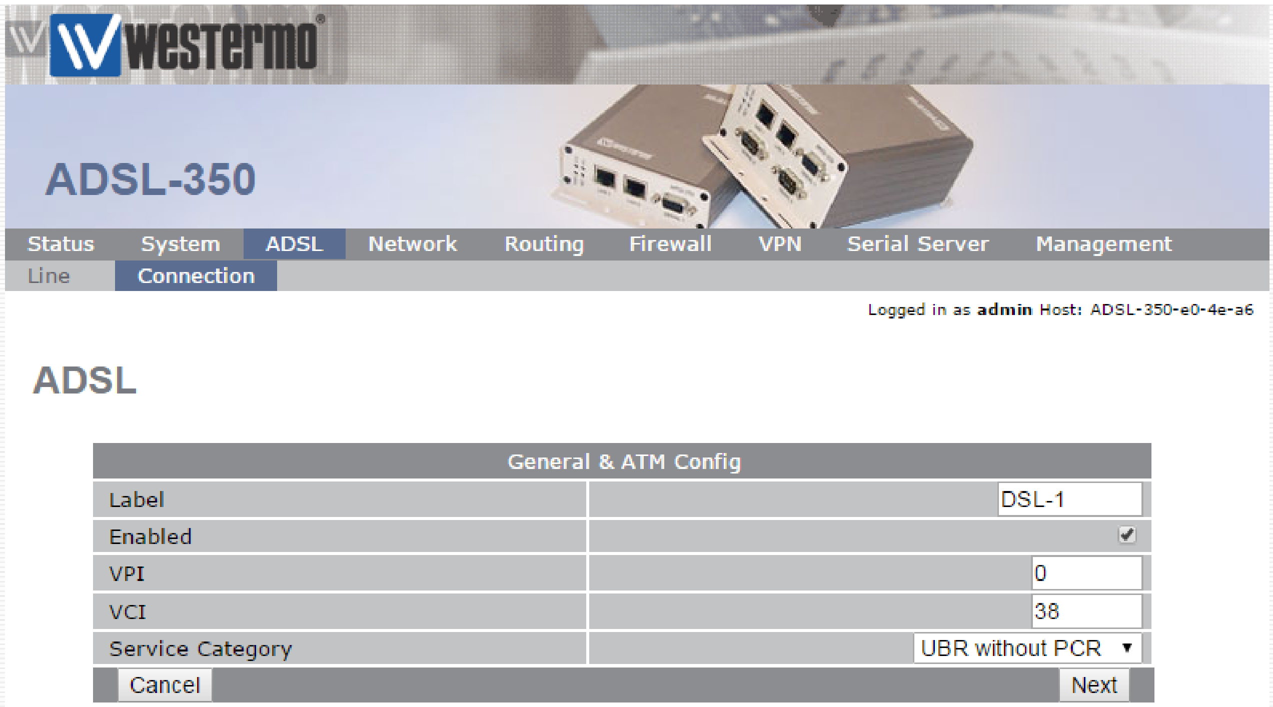

westermo
ADSL-350
Status System ADSL Network Routing Firewall VPN Serial Server Management
Line Connection

Logged in as **admin** Host: ADSL-350-e0-4e-a6

ADSL

Connection Summary							
Label	Enabled	VPI	VCI	Connection Type	Encapsulation	Edit	Delete
No connections configured.							

Click **Add new profile**.


westermo
ADSL-350
Status System ADSL Network Routing Firewall VPN Serial Server Management
Line Connection

Logged in as **admin** Host: ADSL-350-e0-4e-a6

ADSL

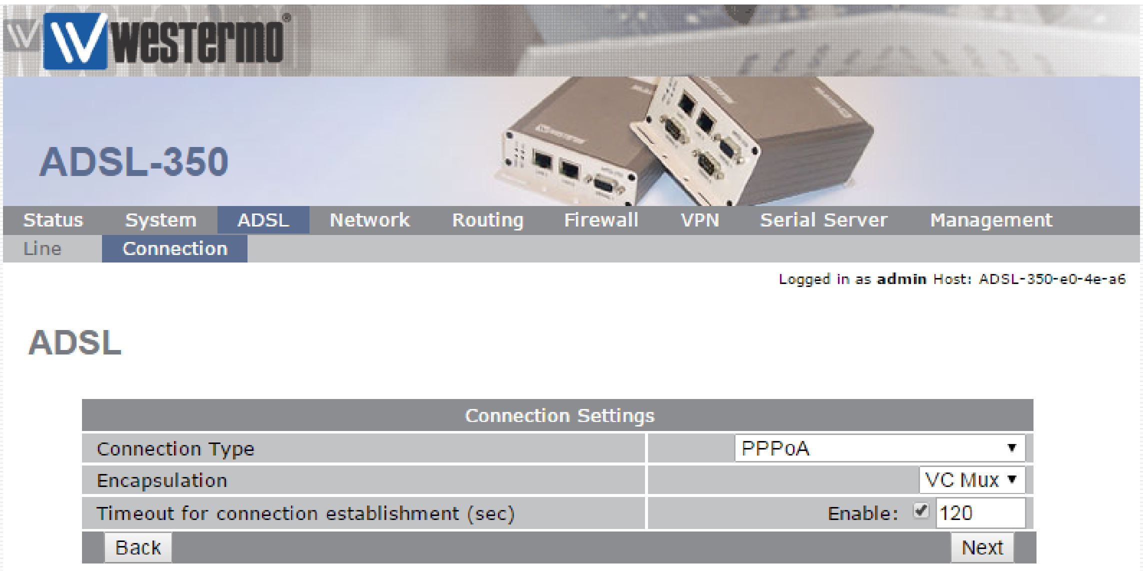
General & ATM Config	
Label	DSL-1
Enabled	☑
VPI	0
VCI	38
Service Category	UBR without PCR ▾

Default settings for a UK BT Broadband line.

ADSL-350 Broadband Router Configuration

ADSL Link

Browse to ADSL → CONNECTION continued..

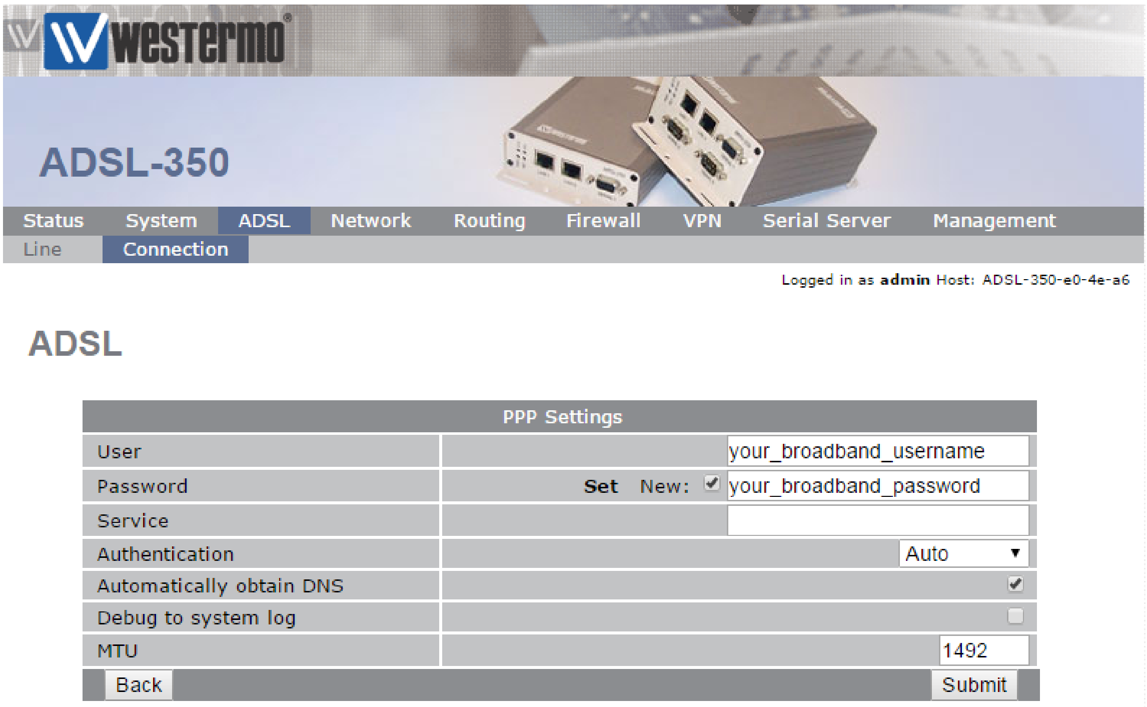


Logged in as **admin** Host: ADSL-350-e0-4e-a6

ADSL

Connection Settings	
Connection Type	PPPoA ▾
Encapsulation	VC Mux ▾
Timeout for connection establishment (sec)	Enable: ☑ 120

Default settings for a UK BT Broadband line.



Logged in as **admin** Host: ADSL-350-e0-4e-a6

ADSL

PPP Settings	
User	your_broadband_username
Password	**Set** New: ☑ your_broadband_password
Service	
Authentication	Auto ▾
Automatically obtain DNS	☑
Debug to system log	☐
MTU	1492

User: Your broadband username

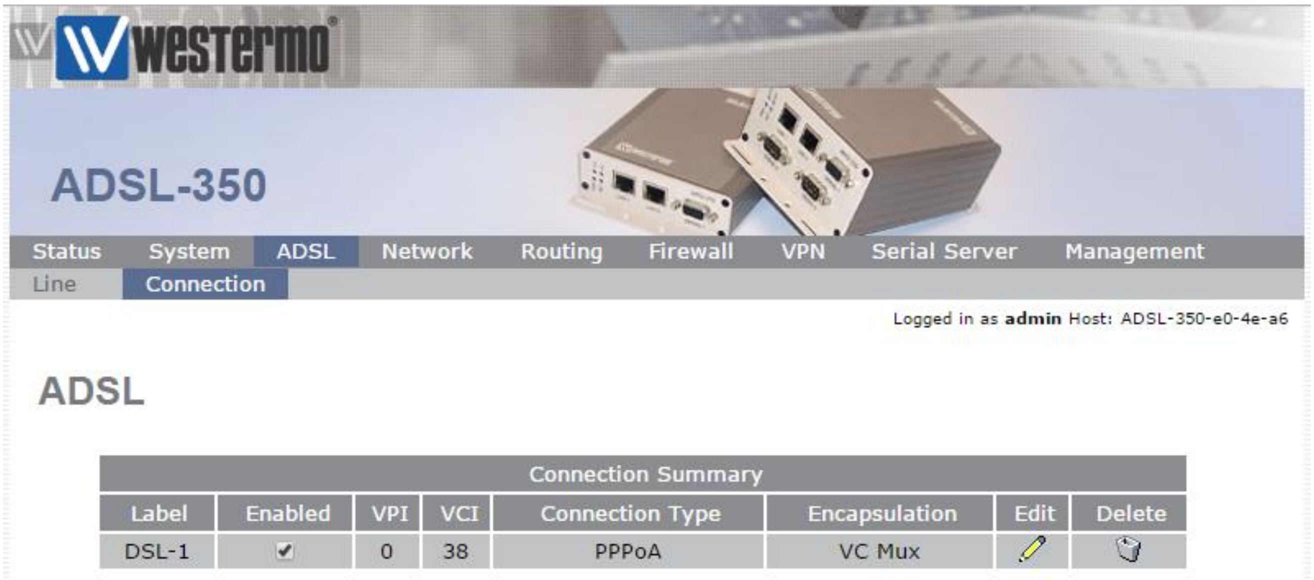
Password: Your broadband password

NB: These details are issued by your broadband provider.

ADSL-350 Broadband Router Configuration

ADSL Link

Browse to ADSL → CONNECTION continued..



Logged in as **admin** Host: ADSL-350-e0-4e-a6

ADSL

Connection Summary							
Label	Enabled	VPI	VCI	Connection Type	Encapsulation	Edit	Delete
DSL-1	☑	0	38	PPPoA	VC Mux	✎	🗑

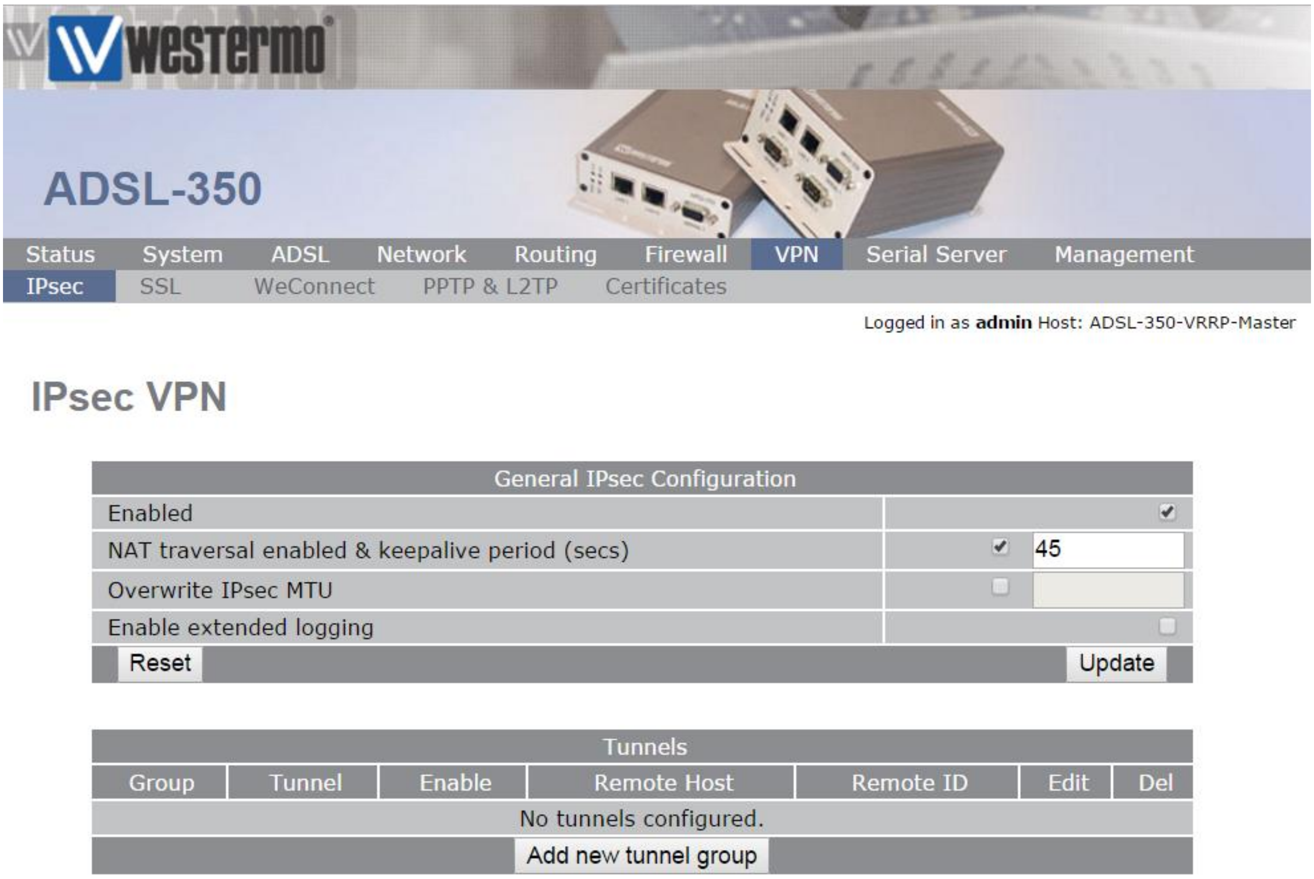
Broadband settings complete

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



Logged in as **admin** Host: ADSL-350-VRRP-Master

IPsec VPN

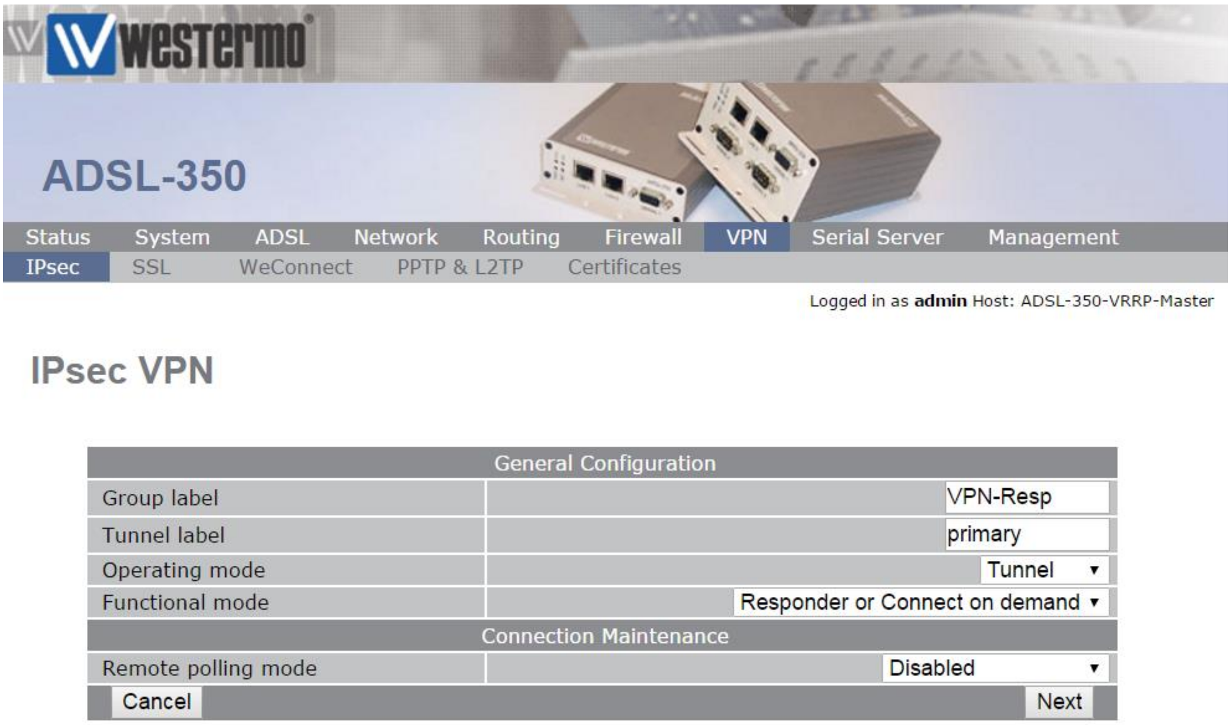
General IPsec Configuration	
Enabled	☑
NAT traversal enabled & keepalive period (secs)	☑ 45
Overwrite IPsec MTU	☐
Enable extended logging	☐
Reset	Update

Group	Tunnel	Enable	Remote Host	Remote ID	Edit	Del
No tunnels configured.						
Add new tunnel group						

Click **Add new tunnel group.**

ADSL-350 Broadband Router Configuration

IPSec VPN Tunnel Configuration (Responder)

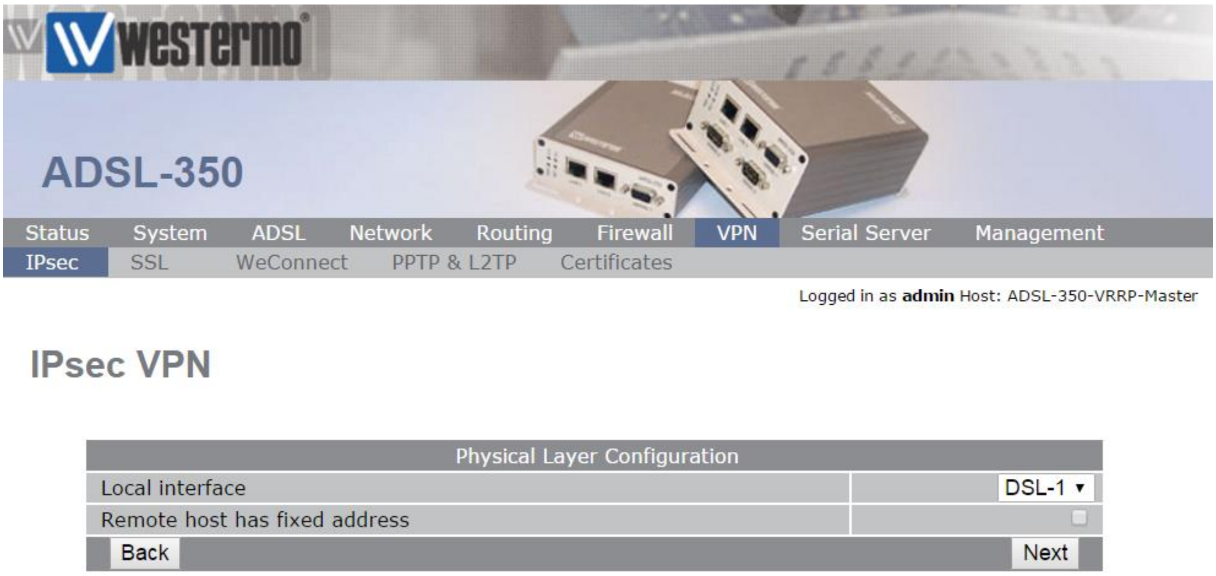

ADSL-350
Status System ADSL Network Routing Firewall VPN Serial Server Management
IPsec SSL WeConnect PPTP & L2TP Certificates
Logged in as admin Host: ADSL-350-VRRP-Master
IPsec VPN
Cancel
Next

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

Group label: Free Text – tunnel description only

Operating mode: Tunnel (default)

Functional Mode: Responder or Connect on demand


ADSL-350
Status System ADSL Network Routing Firewall VPN Serial Server Management
IPsec SSL WeConnect PPTP & L2TP Certificates
Logged in as admin Host: ADSL-350-VRRP-Master
IPsec VPN
Back
Next

Physical Layer Configuration	
Local interface	DSL-1
Remote host has fixed address	□

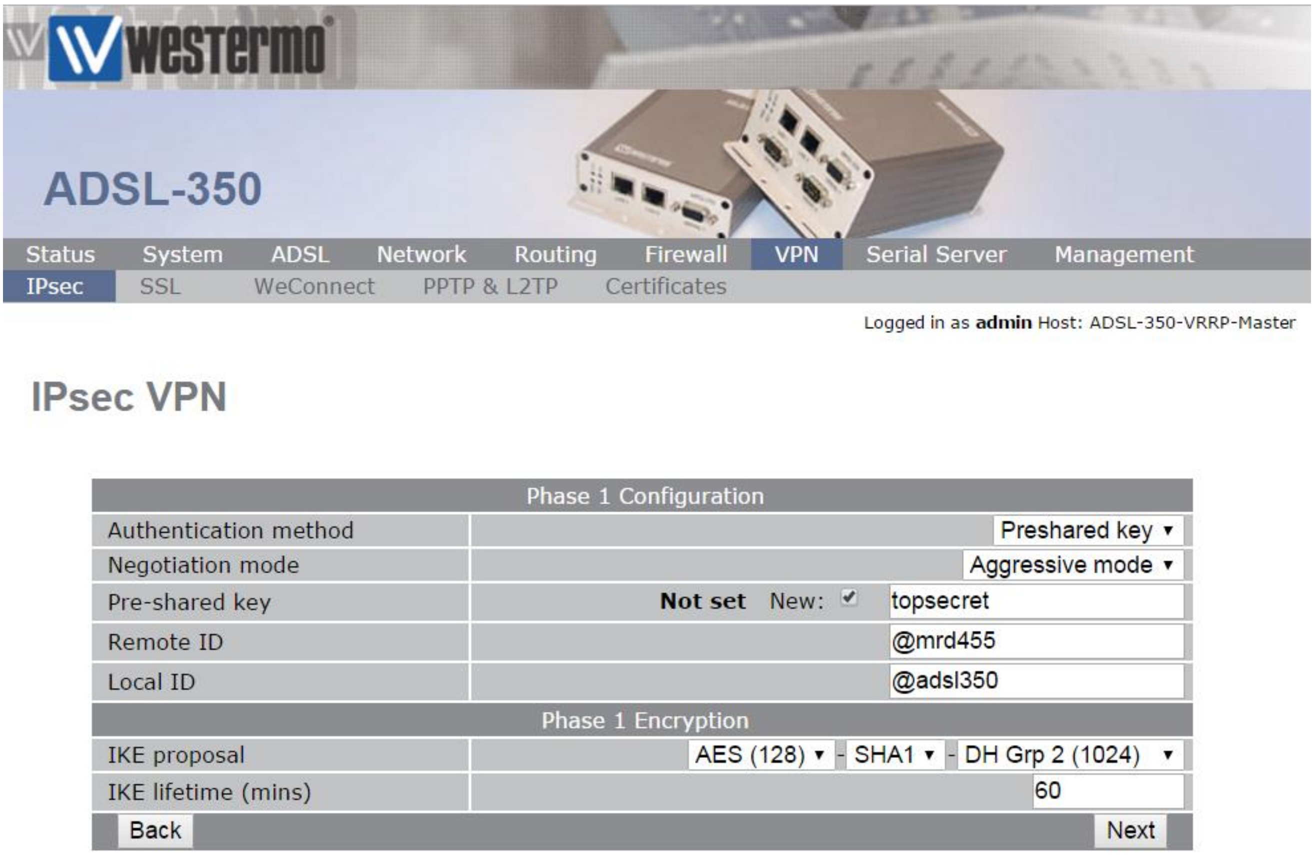
Local Interface: DSL-1 (i.e. the broadband interface)

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)



Logged in as **admin** Host: ADSL-350-VRRP-Master

IPsec VPN

Phase 1 Configuration	
Authentication method	Preshared key ▾
Negotiation mode	Aggressive mode ▾
Pre-shared key	**Not set** New: ☑ topsecret
Remote ID	@mrd455
Local ID	@adsl350
Phase 1 Encryption	
IKE proposal	AES (128) ▾ - SHA1 ▾ - DH Grp 2 (1024) ▾
IKE lifetime (mins)	60

Authentication Method: Preshared Keys

Negotiation Mode: Aggressive Mode

NB: Aggressive Mode is for when the intitiator 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.

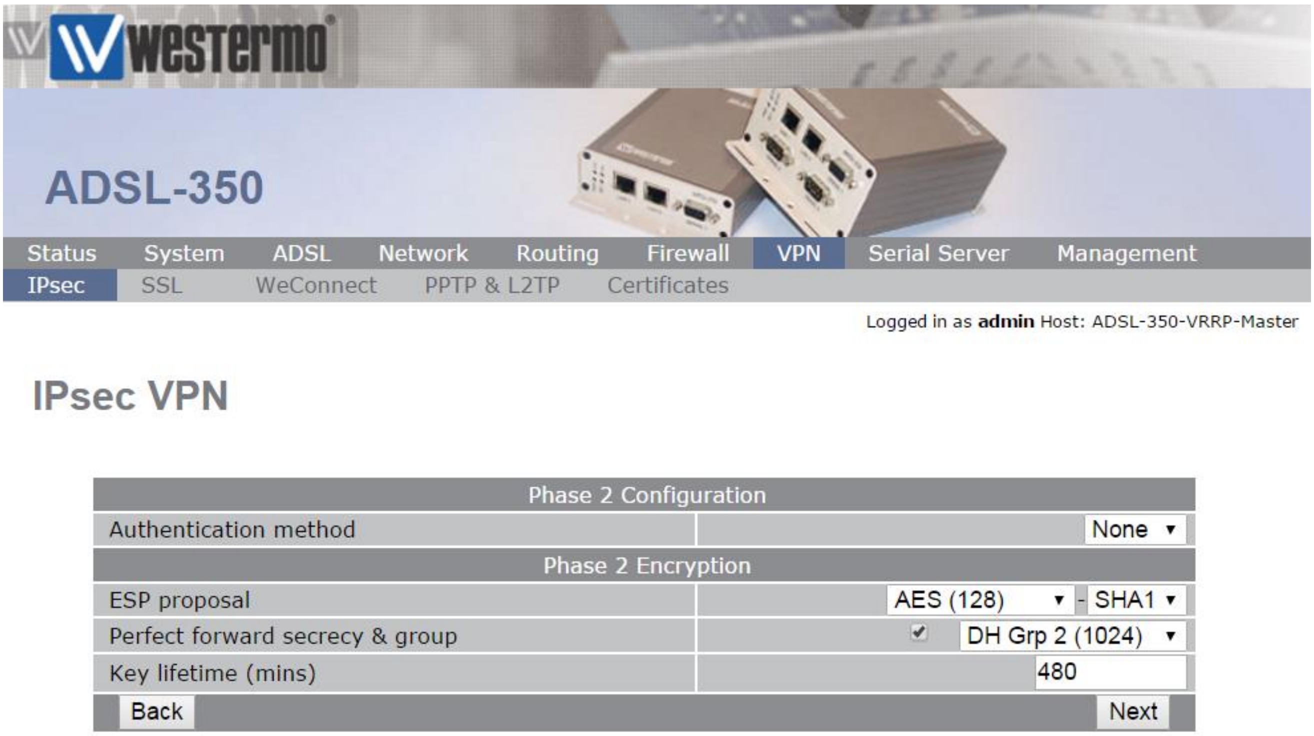
IKE proposal: AES(128)-SHA1-DH Group 2 (1024)

IKE Lifetime (mins): 60

ADL-350 Broadband Router Configuration

IPSec VPN Tunnel Configuration (Responder)

Phase 2 (IPSec)



Phase 2 Configuration	
Authentication method	None ▾
Phase 2 Encryption	
ESP proposal	AES (128) ▾ - SHA1 ▾
Perfect forward secrecy & group	☑ DH Grp 2 (1024) ▾
Key lifetime (mins)	480

Authentication Method: None

ESP proposal: AES(128)-SHA1

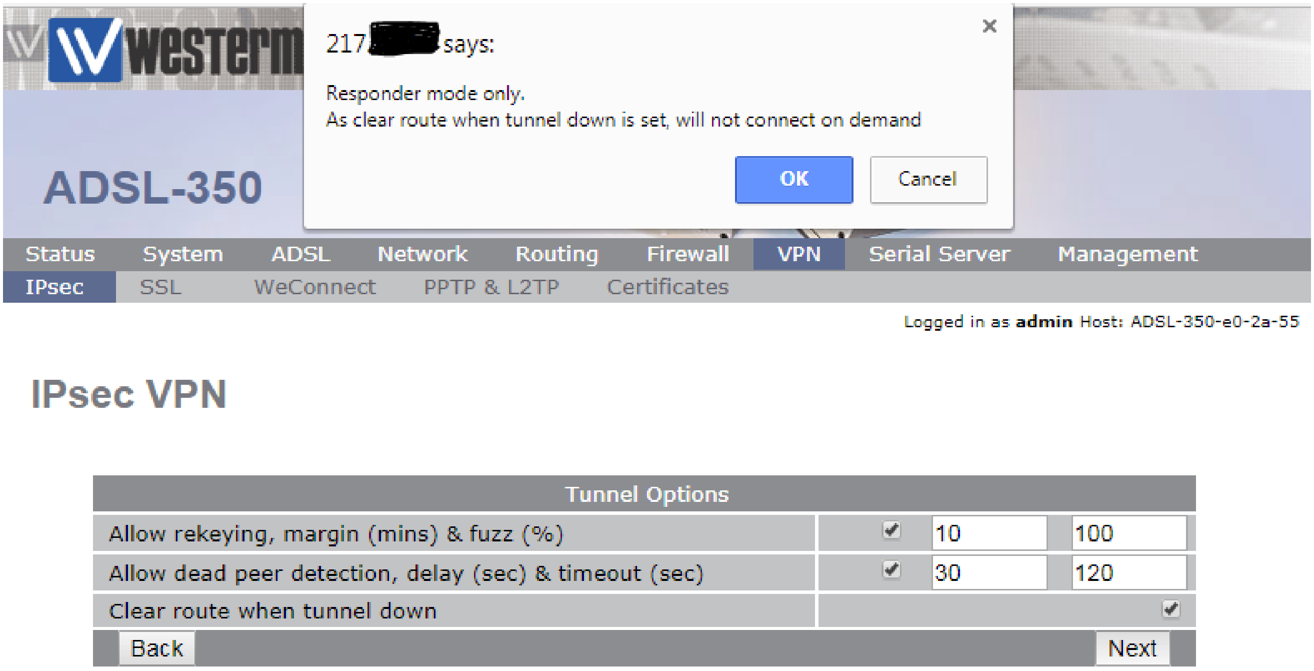
Perfect forward secrecy & group: ✓ DH Grp 2 (1024)

Key Lifetime (mins): 480

ADSL-350 Broadband Router Configuration

IPSec VPN Tunnel Configuration (Responder)

Tunnel Options


westermo
ADSL-350
Status System ADSL Network Routing Firewall VPN Serial Server Management
IPsec SSL WeConnect PPTP & L2TP Certificates
Logged in as admin Host: ADSL-350-e0-2a-55
IPsec VPN
OK
Cancel
Back
Next

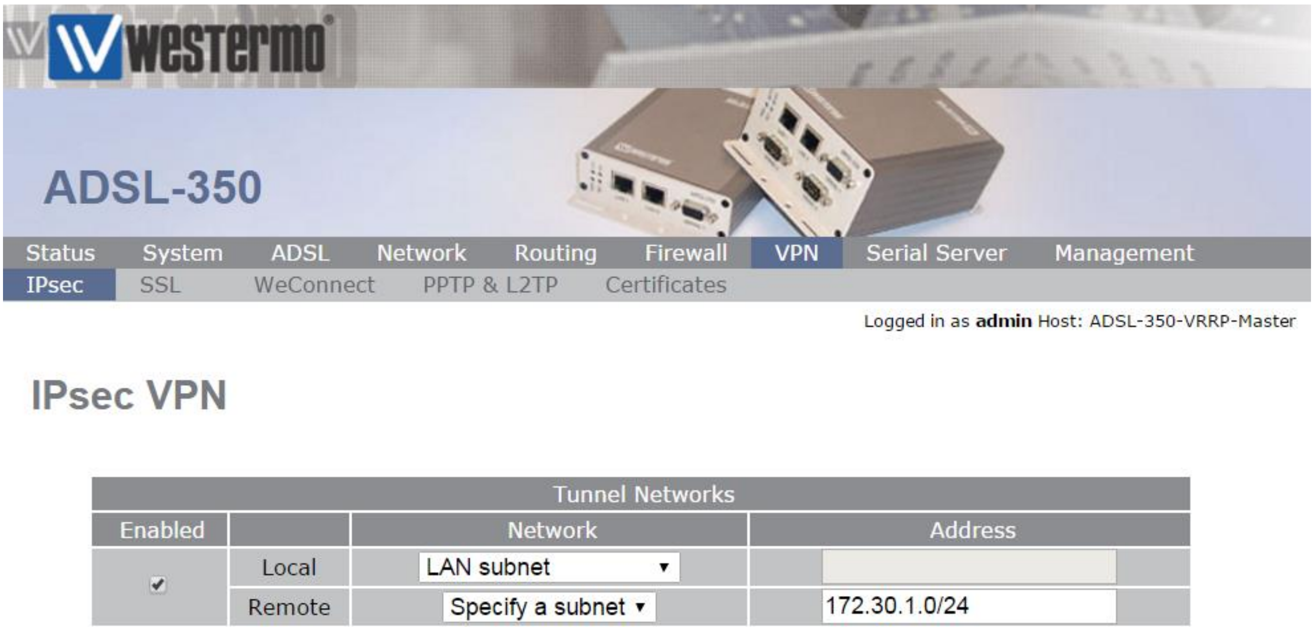
217[redacted] says:

Responder mode only.
As clear route when tunnel down is set, will not connect on demand

Tunnel Options			
Allow rekeying, margin (mins) & fuzz (%)	☑	10	100
Allow dead peer detection, delay (sec) & timeout (sec)	☑	30	120
Clear route when tunnel down			☑

Clear route when tunnel down: ✓

Tunnel Networks


westermo
ADSL-350
Status System ADSL Network Routing Firewall VPN Serial Server Management
IPsec SSL WeConnect PPTP & L2TP Certificates
Logged in as admin Host: ADSL-350-VRRP-Master
IPsec VPN

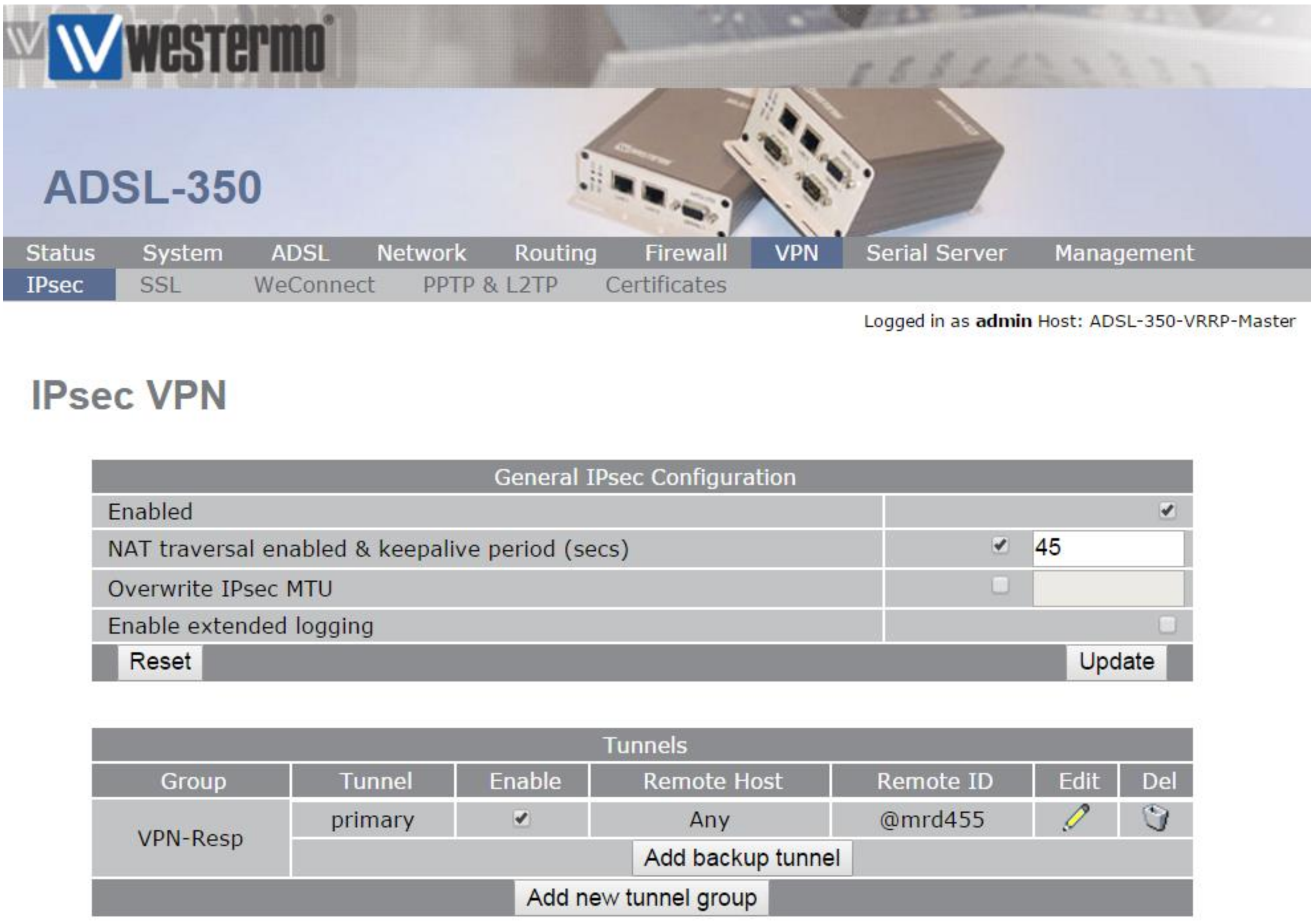
Tunnel Networks			
Enabled		Network	Address
☑	Local	LAN subnet ▾	
	Remote	Specify a subnet ▾	172.30.1.0/24

Local: Lan Subnet

Remote → Specify a subnet: 172.30.1.0./24

ADSL-350 Broadband Router Configuration

IPSec VPN Tunnel Configuration (Responder)


ADSL-350
Status System ADSL Network Routing Firewall VPN Serial Server Management
IPsec SSL WeConnect PPTP & L2TP Certificates
Logged in as **admin** Host: ADSL-350-VRRP-Master

IPsec VPN

General IPsec Configuration		
Enabled		☑
NAT traversal enabled & keepalive period (secs)	☑	45
Overwrite IPsec MTU	□	
Enable extended logging		□

Tunnels

Group	Tunnel	Enable	Remote Host	Remote ID	Edit	Del
VPN-Resp	primary	☑	Any	@mrd455		

Add backup tunnel
Add new tunnel group

General IPSec Configuration.

Enabled: ✓

General IPSec Configuration.

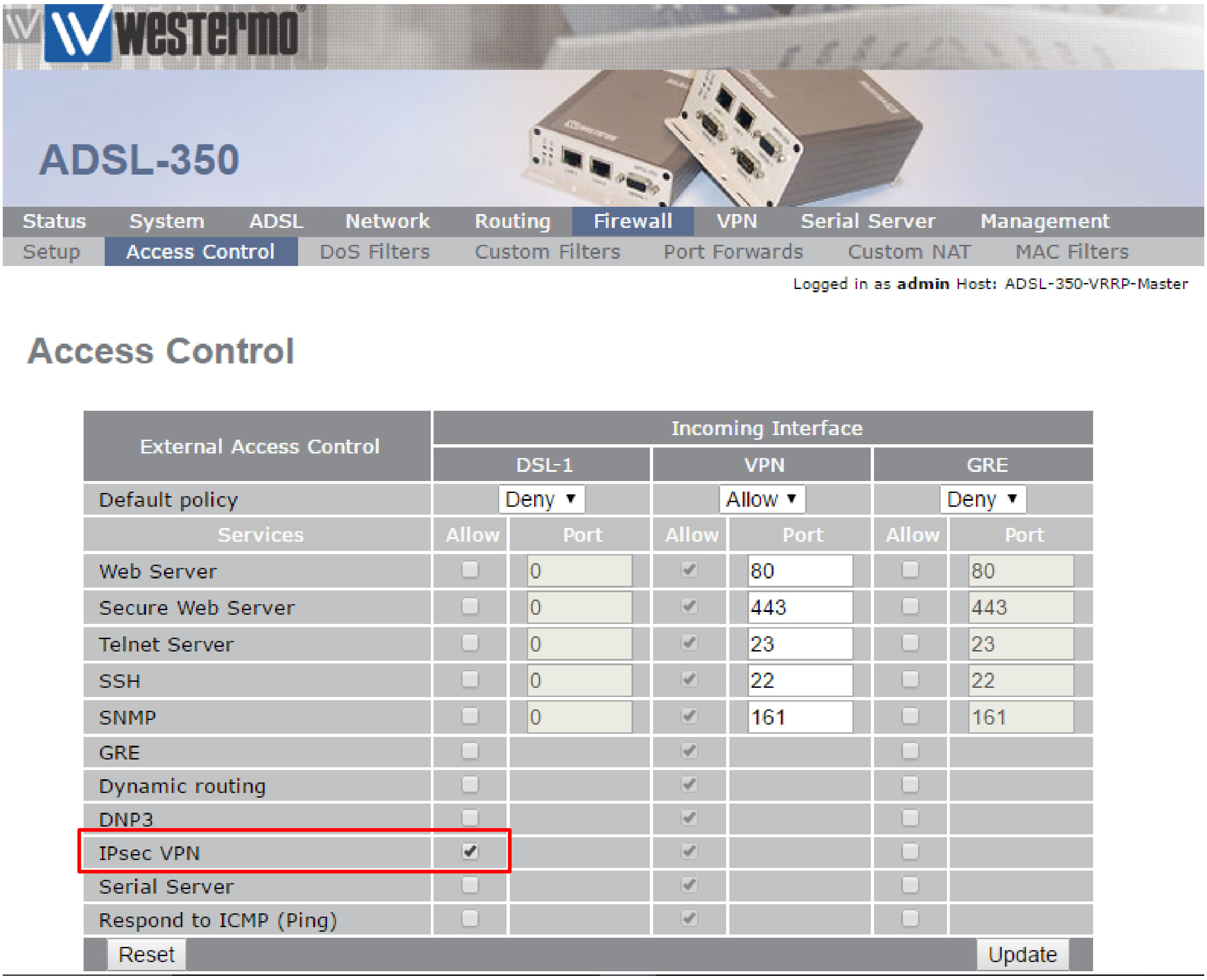
Enable: ✓

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 allowes in to the DSL interface.

Browse to **Firewall → 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	□	0	☑	80	□	80
Secure Web Server	□	0	☑	443	□	443
Telnet Server	□	0	☑	23	□	23
SSH	□	0	☑	22	□	22
SNMP	□	0	☑	161	□	161
GRE	□		☑		□	
Dynamic routing	□		☑		□	
DNP3	□		☑		□	
IPsec VPN	☑		☑		□	
Serial Server	□		☑		□	
Respond to ICMP (Ping)	□		☑		□	

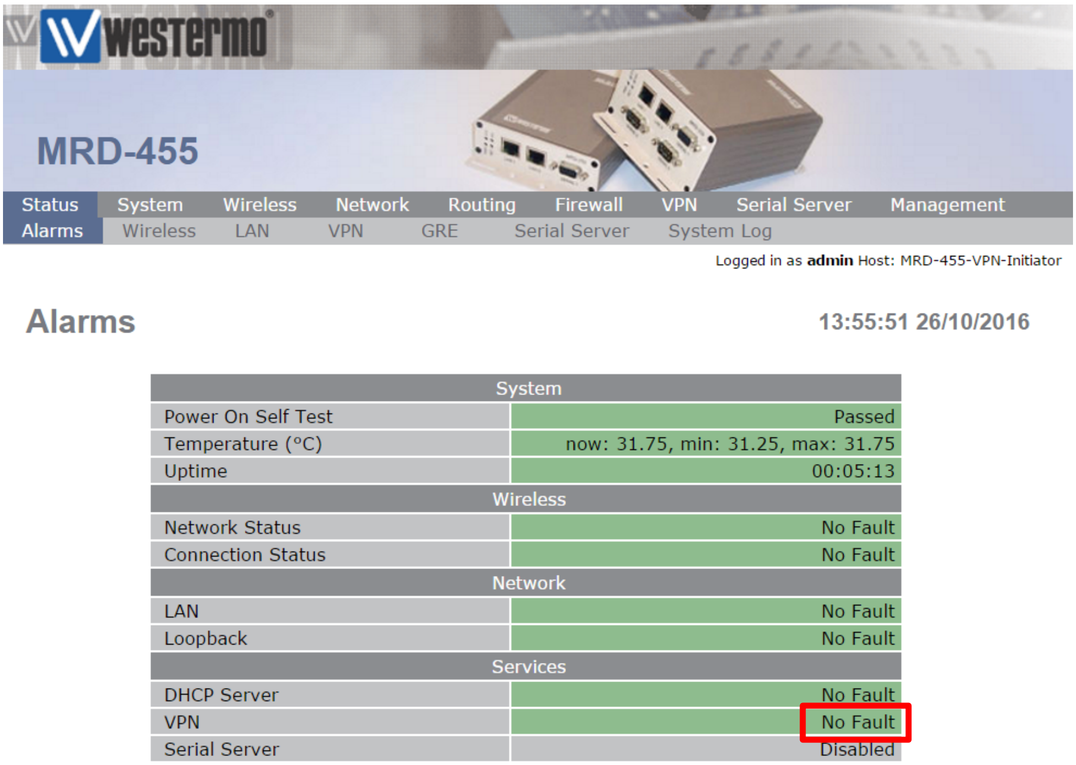
In the **DSL-1** tick IPSec VPN to allow inbound VPN traffic.

VPN STATUS

MRD-455

Browse to **Status → Alarms**

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

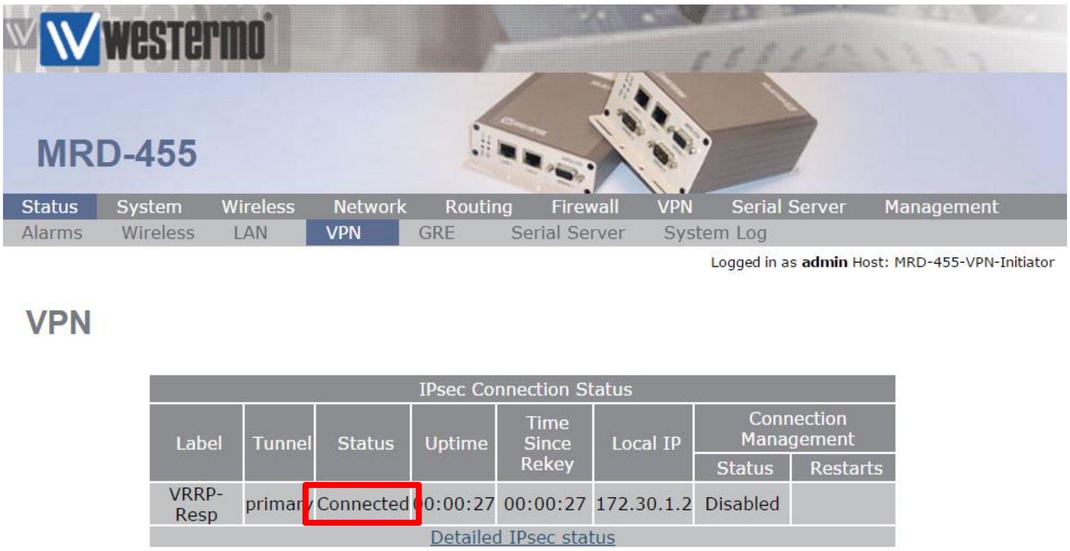


Logged in as **admin** Host: MRD-455-VPN-Initiator

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**



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

VPN

IPsec Connection Status

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

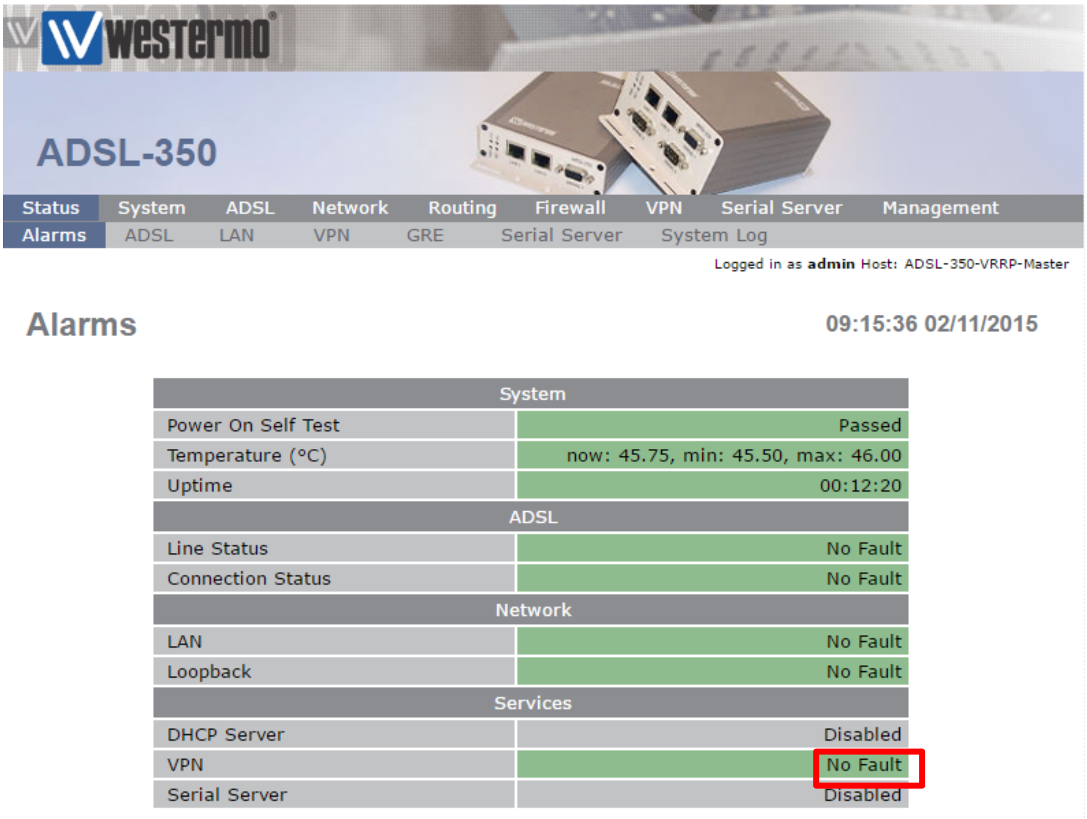
Detailed IPsec status

VPN STATUS

ADSL-350

Browse to **Status → Alarms**

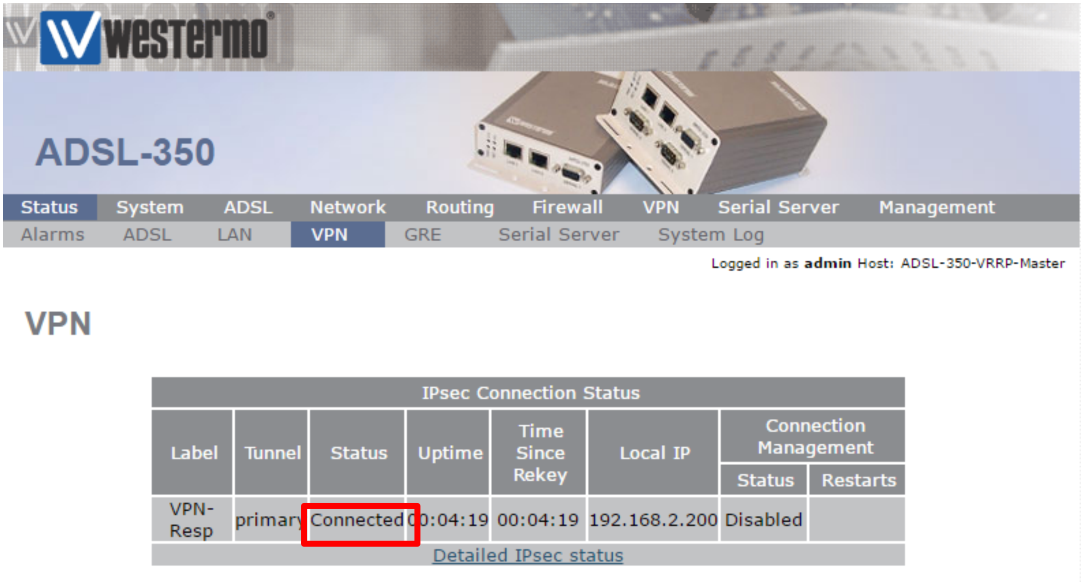
Check that the **VPN** status is set to **No Fault**.


westermo
ADSL-350
Status System ADSL Network Routing Firewall VPN Serial Server Management
Alarms ADSL LAN VPN GRE Serial Server System Log
Logged in as admin Host: ADSL-350-VRRP-Master

Alarms 09:15:36 02/11/2015

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**


westermo
ADSL-350
Status System ADSL Network Routing Firewall VPN Serial Server Management
Alarms ADSL LAN VPN GRE Serial Server System Log
Logged in as admin Host: ADSL-350-VRRP-Master

VPN

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

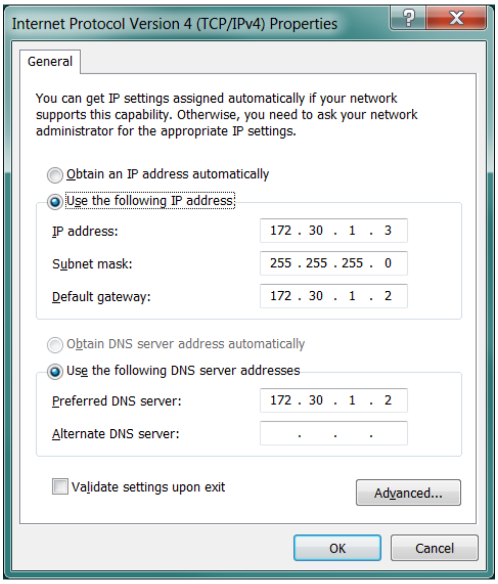
TESTING

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 172 . 30 . 1 . 3
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 172 . 30 . 1 . 2

○ Obtain DNS server address automatically
● Use the following DNS server addresses

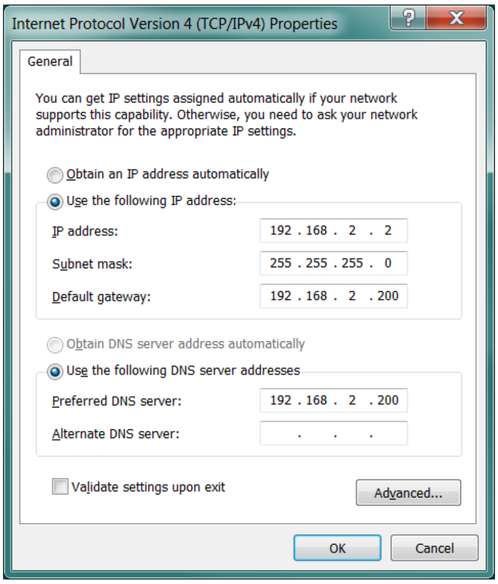
Preferred DNS server: 172 . 30 . 1 . 2
Alternate DNS server: . . .

□ Validate settings upon exit

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 2 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 2 . 200

○ Obtain DNS server address automatically
● Use the following DNS server addresses

Preferred DNS server: 192 . 168 . 2 . 200
Alternate DNS server: . . .

□ Validate settings upon exit

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	JM	Minor changes to wording and amend mistakes to DH groups	27/10/16
02	WN	Changes to “clear route when tunnel is down” for responder only.	22/01/18
03			
04			
05			
06			
07			

HEAD OFFICE

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 or scan the QR code with your mobile phone.