Application Note 10

IPSec Over Cellular using Digi Transport Routers

With Pre-shared key authentication

June 2012

Contents

1 INTRODUCTION

1.1 Outline

This application note aims to enable the reader to easily configure an IPSec VPN tunnel between two local area networks using a Digi Transport router at both ends of the tunnel.

The diagram below details the IP number scheme and architecture of this example configuration.

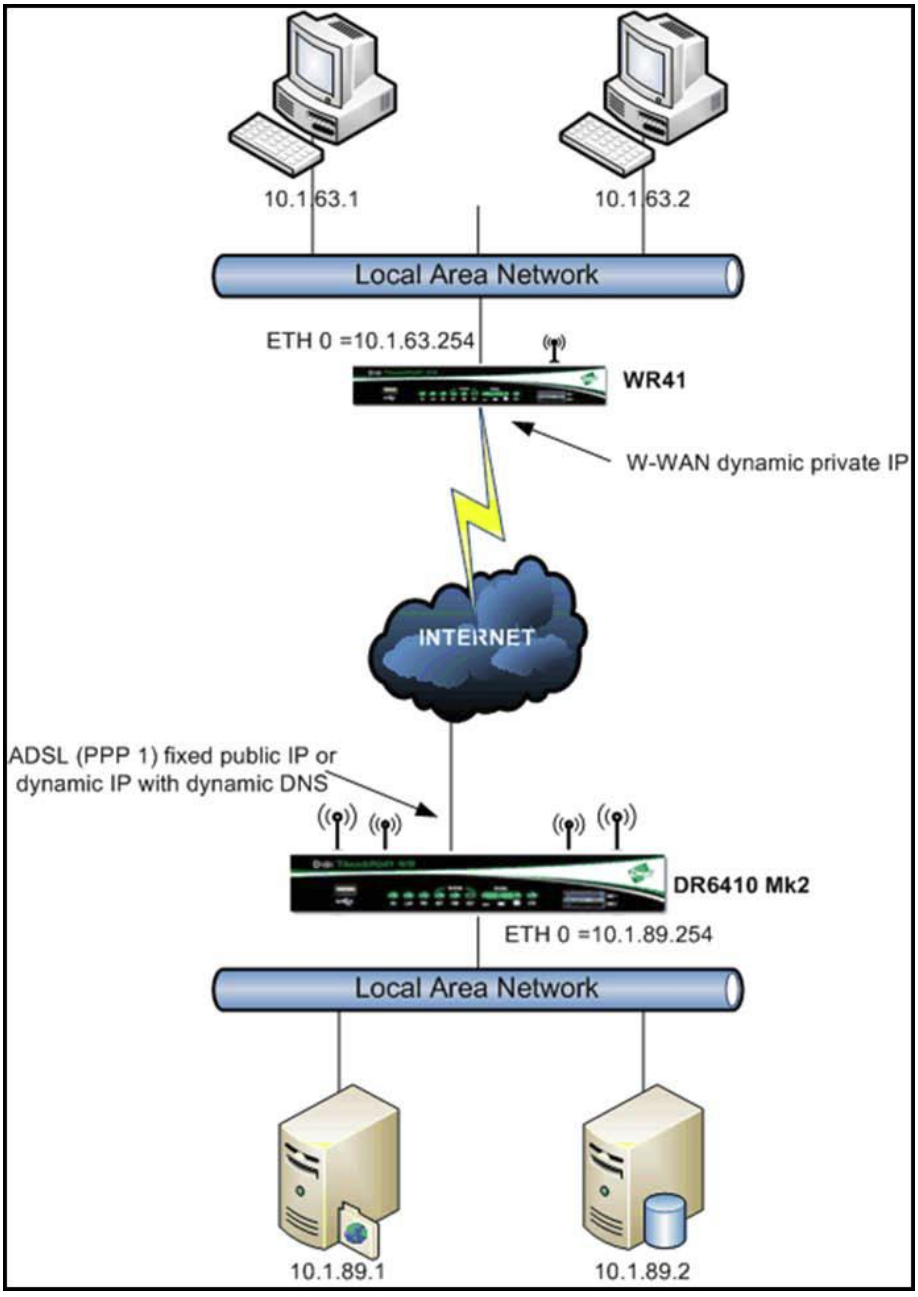


Figure 1-1: Overview Diagram

1.2 Assumptions

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product, and of the requirements for their specific application.
Configuration: This application note assumes that the WR41 will be connecting to a cellular network (i.e. GPRS, EDGE, 3G, HSDPA or HSUPA). Routers connecting to cellular networks are usually allocated a private IP address which would translate to a routable internet external IP at the border of the mobile internet network. In this case, the mode of IPSec needs to be "aggressive mode" with NAT-Traversal. The IPSec responder's IP address needs to be in the public address range and is either fixed or dynamic. In the case of the latter, a type of dynamic DNS hostname will be required because the IPSec initiator always needs to know where to connect.
This application note applies to;
Models shown: Digi Transport WR41 and DR6410 Mk2
Other Compatible Models: Digi Transport VC7400 VPN Concentrator, WR, SR or DR.
Firmware versions: All Versions
Configuration: This Application Note assumes the devices are set to their factory default configurations. Most configuration commands are only shown if they differ from the factory default.
For the purpose of this application note the following applies:
• The IPSec responder router's IP address must be in the public address range and fully routable.

1.3 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: uksupport@digi.com

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

1.4 Version

	Status
1.0	Published
1.1	Revision for new W-WAN usage in the web GUI post release 5.036.
2.0	Updated and rebranded
2.1	Fixed errors and updated

2 DIGI WR41 VPN INITIATOR CONFIGURATION

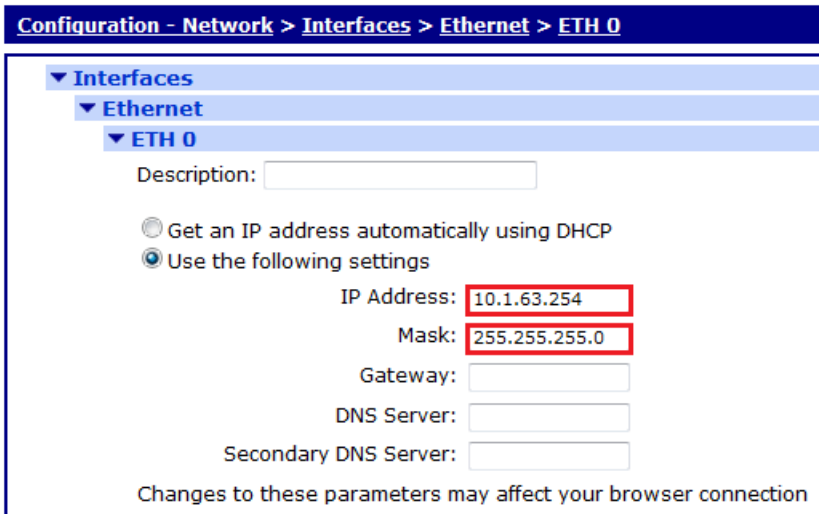
As with all Digi Transport routers you have the option of configuring the IPSec parameters either via the web interface or by writing a new configuration file. We will show the web configuration in this application note. Only the parts of the configuration files that specifically relate to the configuration of this example will be explained in detail. (The configuration files used for this application note can be found in their entirety at the end of this document).

2.1 Inside Ethernet Interface

Using the TransPort's web interface browse to:

Configuration - Network > Interfaces > Ethernet > ETH 0

Parameter	Setting	Description
IP Address	10.1.63.254	Enter the IP address of the LAN interface for the router
Mask	255.255.255.0	Enter the subnet mask



Click Apply

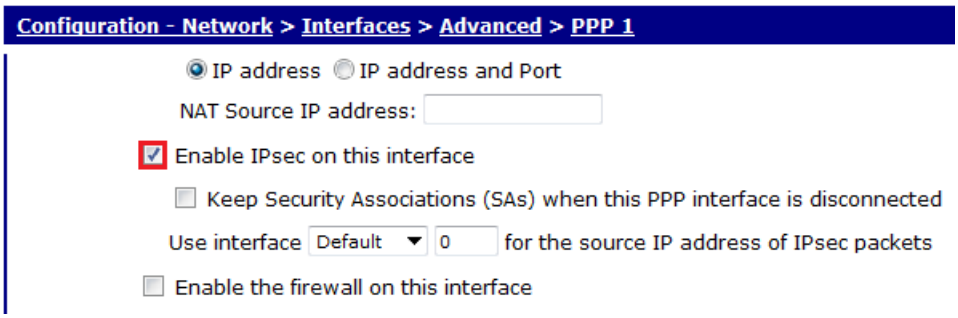
2.2 Cellular PPP Interface

IPSec is enabled on the outside interface; in this example the outside interface is the cellular interface PPP 1. IP analysis is also enabled on this interface for use during the testing phase.

Using the TransPort's web interface browse to:

Configuration - Network > Interfaces > Advanced > PPP 1

Parameter	Setting	Description
Enable IPSec on this interface	✓	Enable IPSec on PPP 1 interface

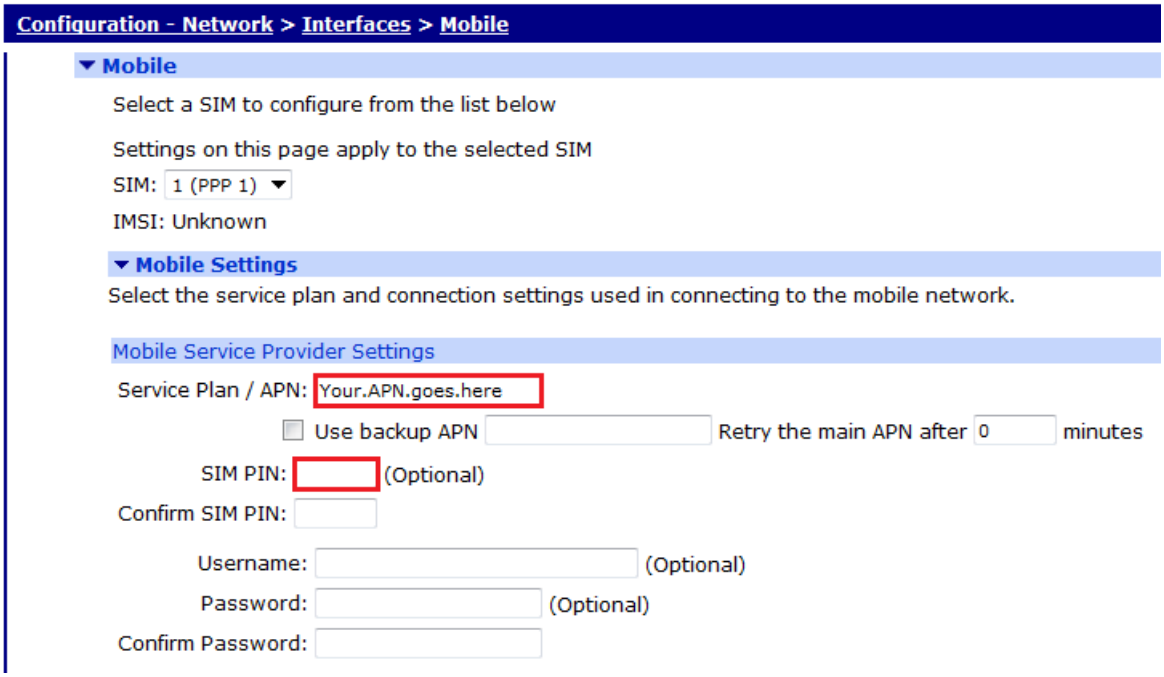


Click Apply

2.3 WR41 Wireless WAN (W-WAN) Module

Browse to **Configuration - Network > Interfaces > Mobile**

Parameter	Setting	Description
Service Plan/APN	internet	Enter the APN of your mobile provider
SIM PIN	0000	Enter SIM PIN if required



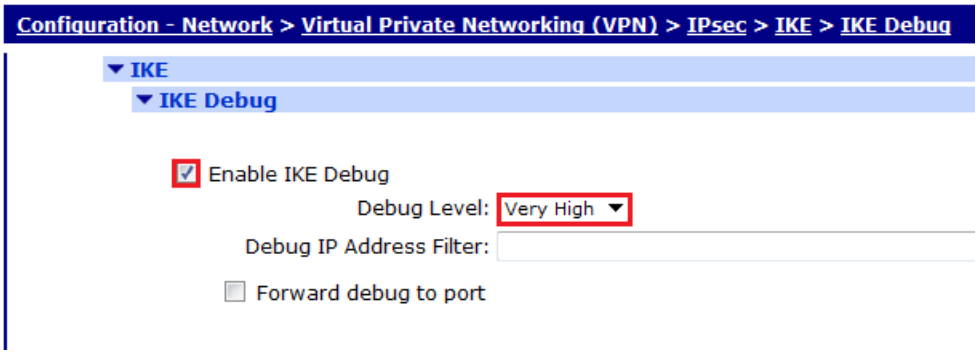
Click Apply

2.4 WR41 Phase 1-IKE

IKE is the first stage in establishing a secure link between two endpoints and has to be configured to match the settings on the VPN host Digi Transport. In this example 3DES and MD5 are used to encrypt and authenticate. Aggressive mode is enabled. MODP group 2 is used, meaning a 1024 bit key for the IKE Diffie-Hellman exchange. Set the IKE SAs to be removed when the IPSec SAs are removed. Set debug to very high as this will help diagnose any problems if the two units fail to build the VPN tunnel.

Browse to **Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE Debug**

Parameter	Setting	Description
Enable IKE Debug	✓	Turn on IKE Debugging
Debug Level	Very High	This will allow for detailed debugging and can be turned off once you are happy that this is working

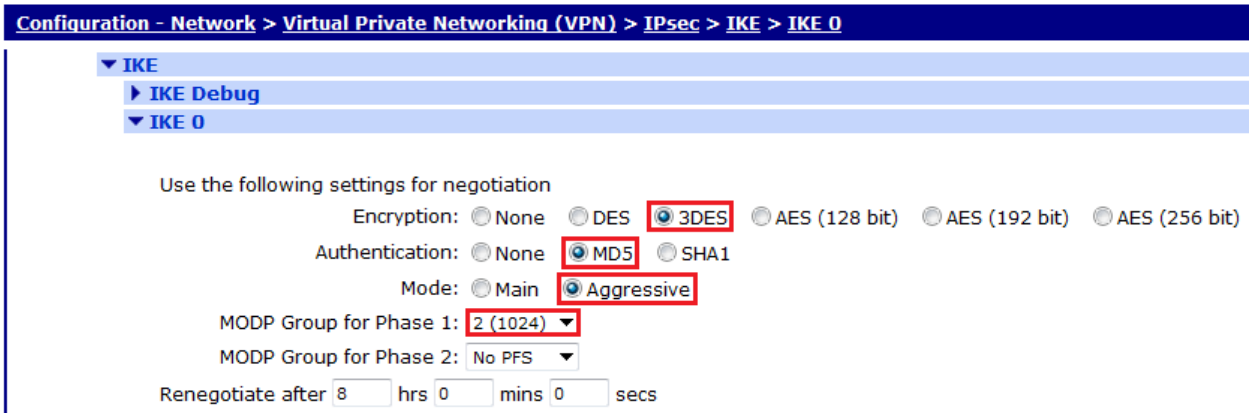


Click Apply

Next browse to **Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE 0**

And make the following changes :

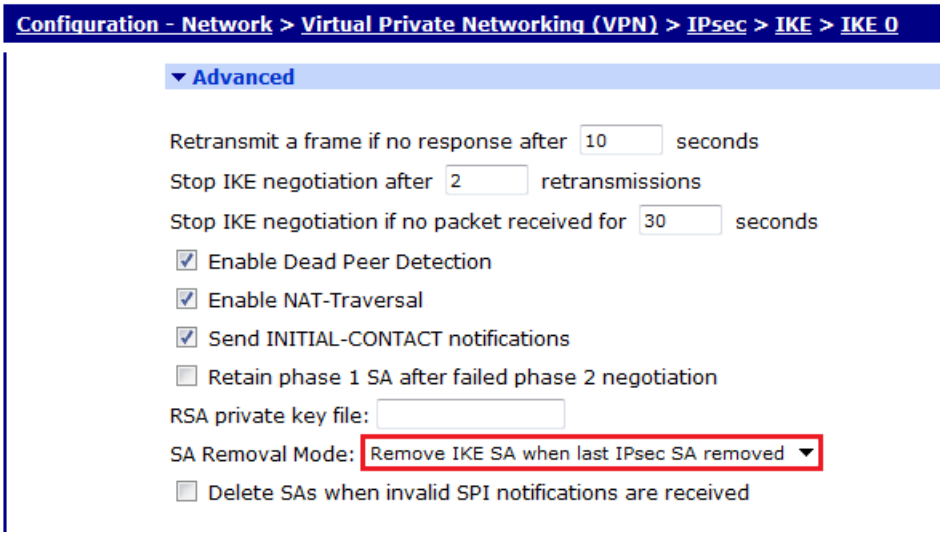
Parameter	Setting	Description
Encryption	3DES	The encryption algorithm to be used for IKE exchanges over the IP connection
Authentication	MD5	The algorithm used to authenticate the IKE session
Mode	Aggressive	Aggressive mode is used in this example
MODP Group for Phase 1	2 (1024)	The key length used in the IKE Diffie-Hellman exchange



Click Apply

Then in the **Advanced** section:

Parameter	Setting	Description
SA Removal Mode	Remove IKE SA when last IPSec SA removed	Remove IKE SA when last IPSEC SA removed



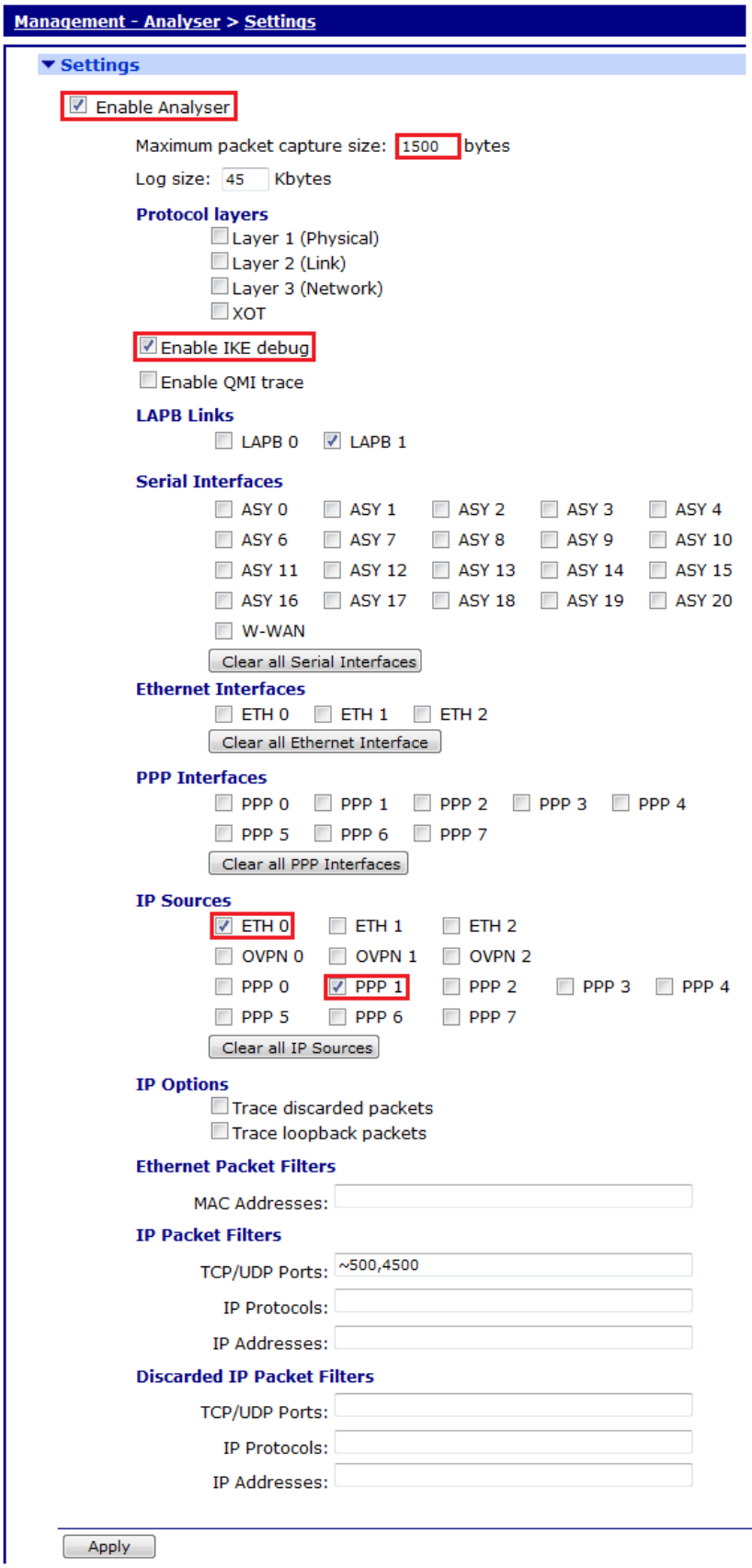
Click Apply

2.5 WR41 Configure Packet Analyser for Debugging

Browse to **Management - Analyser > Settings**

Configure the following settings

Parameter	Setting	Description
Enable Analyser	✓	Turn on the Analyser
Enable IKE Debug	✓	When this is ticked we will see IKE debug in the trace
Max packet capture size	1500	Capture any packet up to 1500 Bytes
IP Source	Eth 0	Enable logging for this interface
IP Source	PPP 1	Enable logging for this interface
IP Packet filter ports	500, 4500	Restrict the ports logged to show only IKE and IPSec


Management - Analyser > Settings
Settings
Enable Analyser
Maximum packet capture size: 1500 bytes
Log size: 45 Kbytes
Protocol layers
Layer 1 (Physical)
Layer 2 (Link)
Layer 3 (Network)
XOT
Enable IKE debug
Enable QMI trace
LAPB Links
LAPB 0
LAPB 1
Serial Interfaces
ASY 0
ASY 1
ASY 2
ASY 3
ASY 4
ASY 6
ASY 7
ASY 8
ASY 9
ASY 10
ASY 11
ASY 12
ASY 13
ASY 14
ASY 15
ASY 16
ASY 17
ASY 18
ASY 19
ASY 20
W-WAN
Clear all Serial Interfaces
Ethernet Interfaces
ETH 0
ETH 1
ETH 2
Clear all Ethernet Interface
PPP Interfaces
PPP 0
PPP 1
PPP 2
PPP 3
PPP 4
PPP 5
PPP 6
PPP 7
Clear all PPP Interfaces
IP Sources
ETH 0
ETH 1
ETH 2
OVPN 0
OVPN 1
OVPN 2
PPP 0
PPP 1
PPP 2
PPP 3
PPP 4
PPP 5
PPP 6
PPP 7
Clear all IP Sources
IP Options
Trace discarded packets
Trace loopback packets
Ethernet Packet Filters
MAC Addresses:
IP Packet Filters
TCP/UDP Ports: ~500,4500
IP Protocols:
IP Addresses:
Discarded IP Packet Filters
TCP/UDP Ports:
IP Protocols:
IP Addresses:
Apply

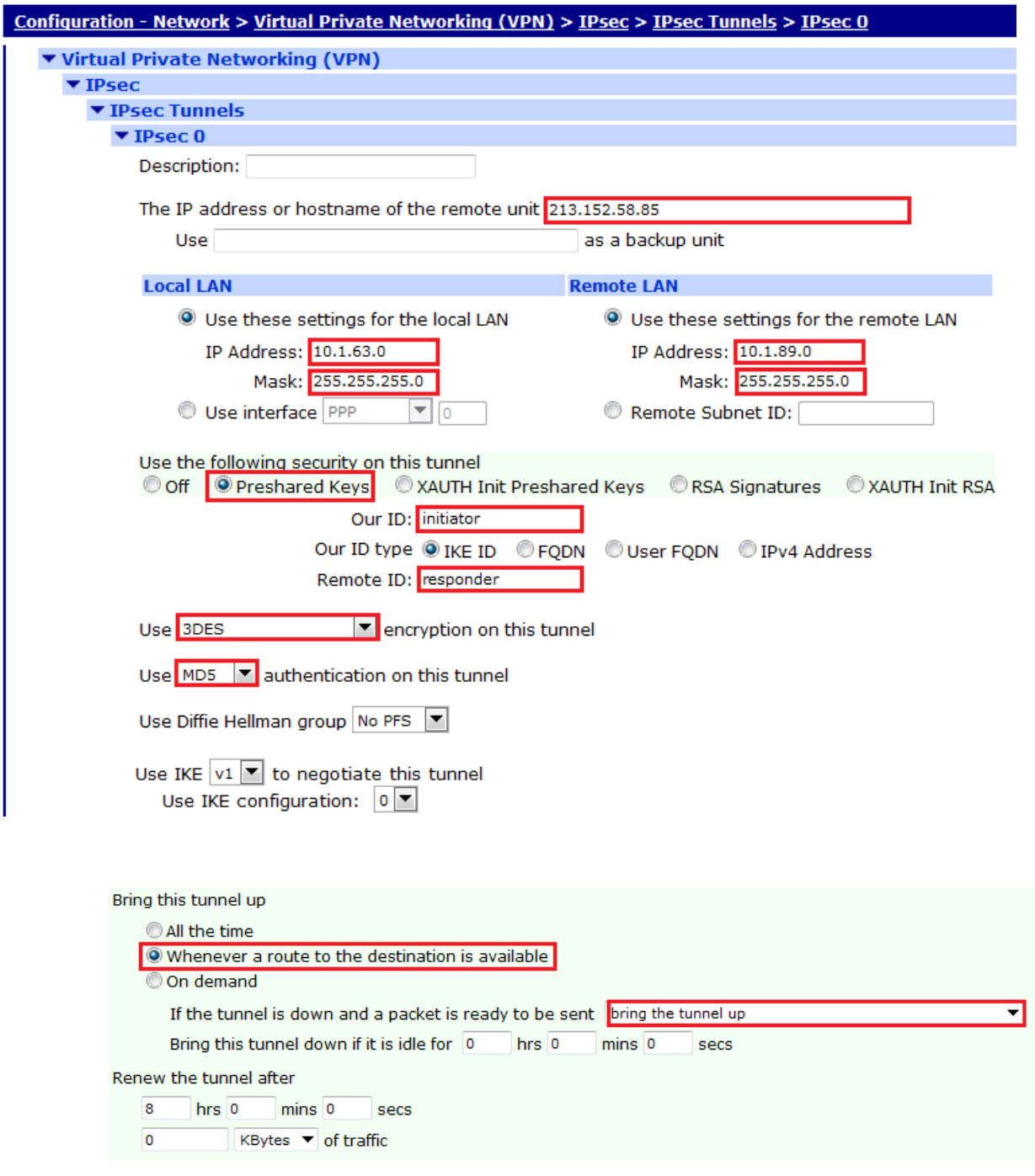
Click Apply

2.6 WR41 Phase 2 –IPSec

Next configure the Eroute (encrypted route).
This will determine what traffic is routed to the remote network over the VPN.

NB: In Aggressive mode the Peer ID and the Our ID can be any alpha-numeric value as long as they correspond with the remote VPN router, they are also case sensitive. In Main Mode, the outside interface addresses are expected to be used.

Parameter	Setting	Description
IP Address or Hostname of the remote unit	213.152.58.85	IP address of the VPN host machine
Local LAN IP Address	10.1.63.0	Packets will be directed through this tunnel if the source and destination IP matches
Local LAN Mask	255.255.255.0	Subnet mask for the network
Remote LAN IP Address	10.1.89.0	Packets will be directed through this tunnel if the source and destination IP matches:
Remote LAN Mask	255.255.255.0	Subnet mask for the network
Use the following security on this tunnel	**Pre-shared Keys**	Pre-shared keys will be used for authentication
Our ID	Initiator	The ID of the VPN initiator router (this router)
Remote ID	Responder	The ID of the VPN responder router (remote router)
Use ( ) encryption on this tunnel	3DES	The IPSEC encryption algorithm to use is 3DES
Use ( ) Authentication on this tunnel	MD5	The IPSEC ESP authentication algorithm is MD5:
Bring this tunnel up	Whenever a route to the destination is available	
If this tunnel is down and a packet is ready to be sent	Bring the tunnel up	


Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0
Virtual Private Networking (VPN)
IPsec
IPsec Tunnels
IPsec 0
Description:
The IP address or hostname of the remote unit 213.152.58.85
Use as a backup unit
Local LAN
Use these settings for the local LAN
IP Address: 10.1.63.0
Mask: 255.255.255.0
Use interface PPP 0
Remote LAN
Use these settings for the remote LAN
IP Address: 10.1.89.0
Mask: 255.255.255.0
Remote Subnet ID:
Use the following security on this tunnel
Off
Preshared Keys
XAUTH Init Preshared Keys
RSA Signatures
XAUTH Init RSA
Our ID: initiator
Our ID type IKE ID FQDN User FQDN IPv4 Address
Remote ID: responder
Use 3DES encryption on this tunnel
Use MD5 authentication on this tunnel
Use Diffie Hellman group No PFS
Use IKE v1 to negotiate this tunnel
Use IKE configuration: 0

Bring this tunnel up
All the time
Whenever a route to the destination is available
On demand
If the tunnel is down and a packet is ready to be sent bring the tunnel up
Bring this tunnel down if it is idle for 0 hrs 0 mins 0 secs
Renew the tunnel after
8 hrs 0 mins 0 secs
0 KBytes of traffic

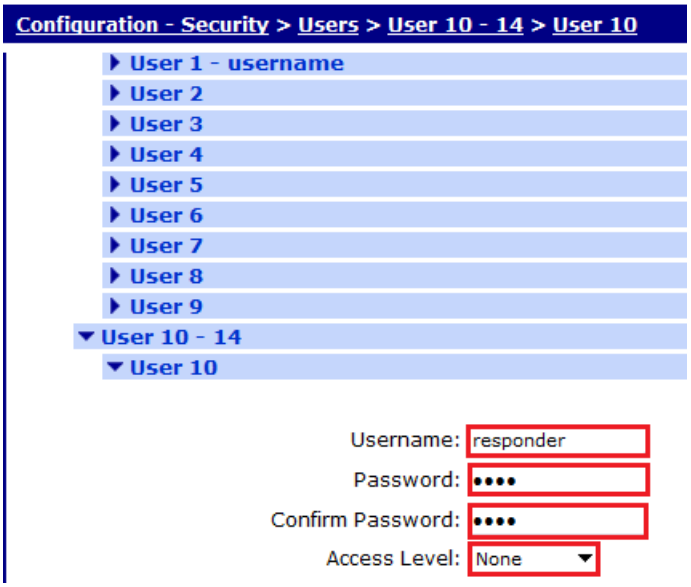
Click Apply

2.7 WR41 Initiator Pre-shared Key

In this section the pre-shared key is set up. The pre-shared key is enabled by creating a username with the name of the remote peer (Peer ID from the Eroute) and the password is the pre-shared key

Browse to **Configuration - Security > Users > User 10 - 14 > User 10**

Parameter	Setting	Description
Username	responder	Name should match the Peer ID: value from Eroute 0
Password	test	**Enter the password – in a production environment you will want to choose a more secure shared key than this**
Confirm Password	test	Re-enter the password
Access Level	None	This user will not be granted any admin access as only used as a pre-shared key



Click Apply

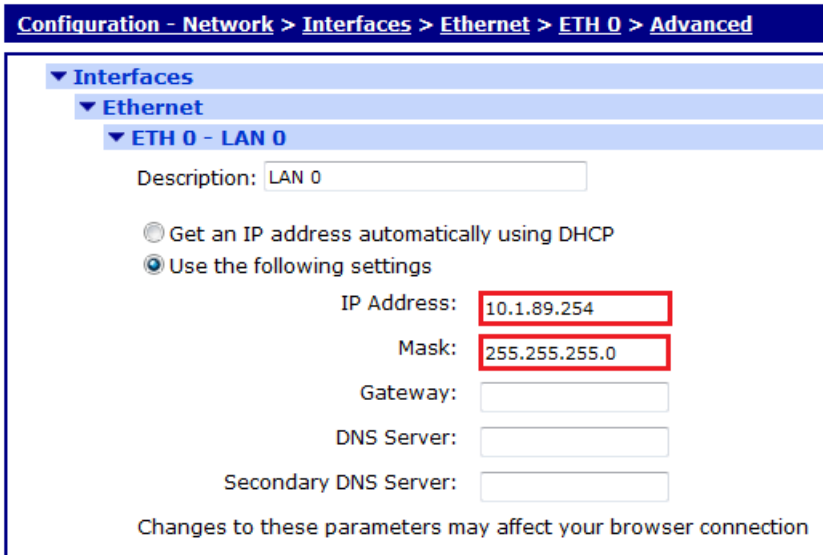
3 DR6410 VPN RESPONDER CONFIGURATION

3.1 Inside LAN Ethernet Interface

First, configure the Ethernet interface with an IP and set up monitoring:

Browse to **Configuration - Network > Interfaces > Ethernet > ETH 0**

Parameter	Setting	Description
IP Address	10.1.89.254	Enter the IP address of the LAN interface for the router
Mask	255.255.255.0	Enter the subnet mask



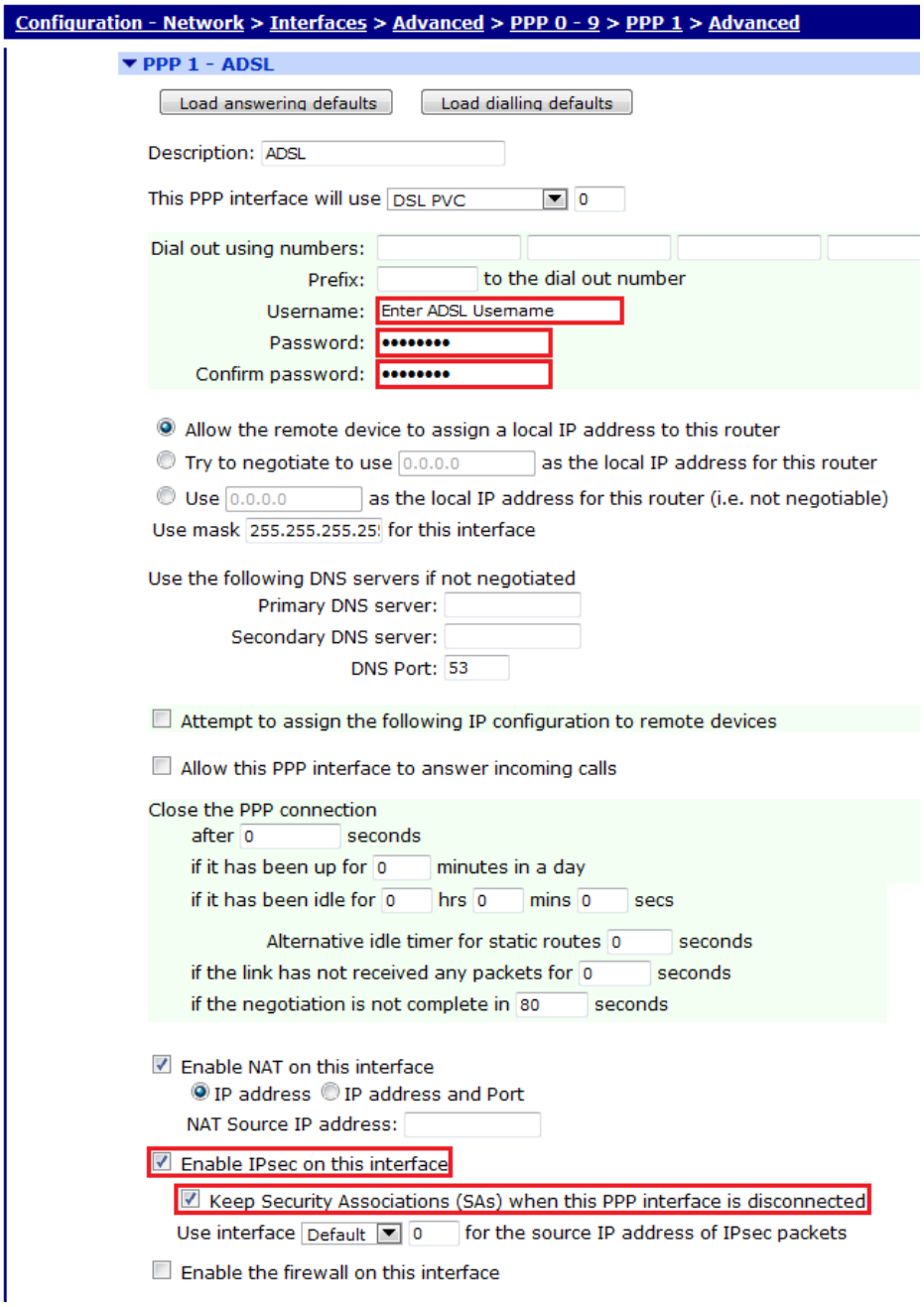
Click Apply

3.2 ADSL PPP Interface

In this example a DSL link is used, this link provided a static IP for the host Digi Transport. IPSec is enabled on this interface.

Browse to **Configuration - Network > Interfaces > Advanced > PPP 1**

Parameter	Setting	Description
Username	Your username goes here	ADSL access username
Password	password	ADSL access password
Confirm Password	password	Confirm ADSL access password
Enable IPSec	✓	Enable IPSec on PPP 1 interface
Keep (SAs) when this PPP interface is disconnected	✓	Keep the SAs when PPP 1 interface becomes disconnected

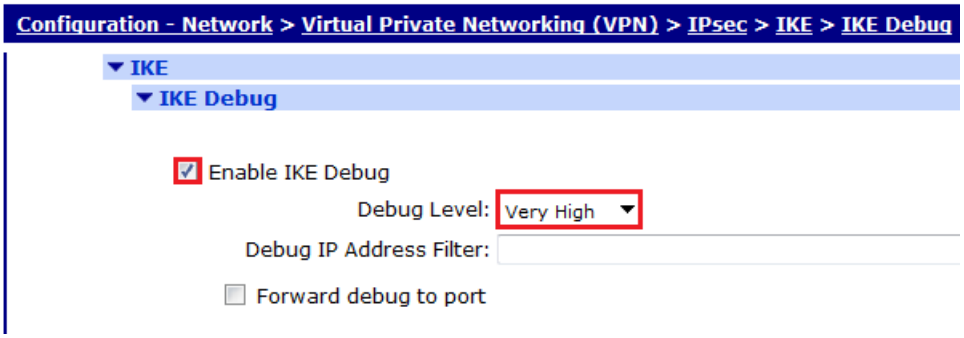


Click Apply

Next configure the DR6410 Packet Analyser for Debugging

Browse to **Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE Debug**

Parameter	Setting	Description
Enable IKE Debug	✓	Enables IKE debugging to be displayed on the debug port
Debug Level	Very High	Sets the level of IKE debugging



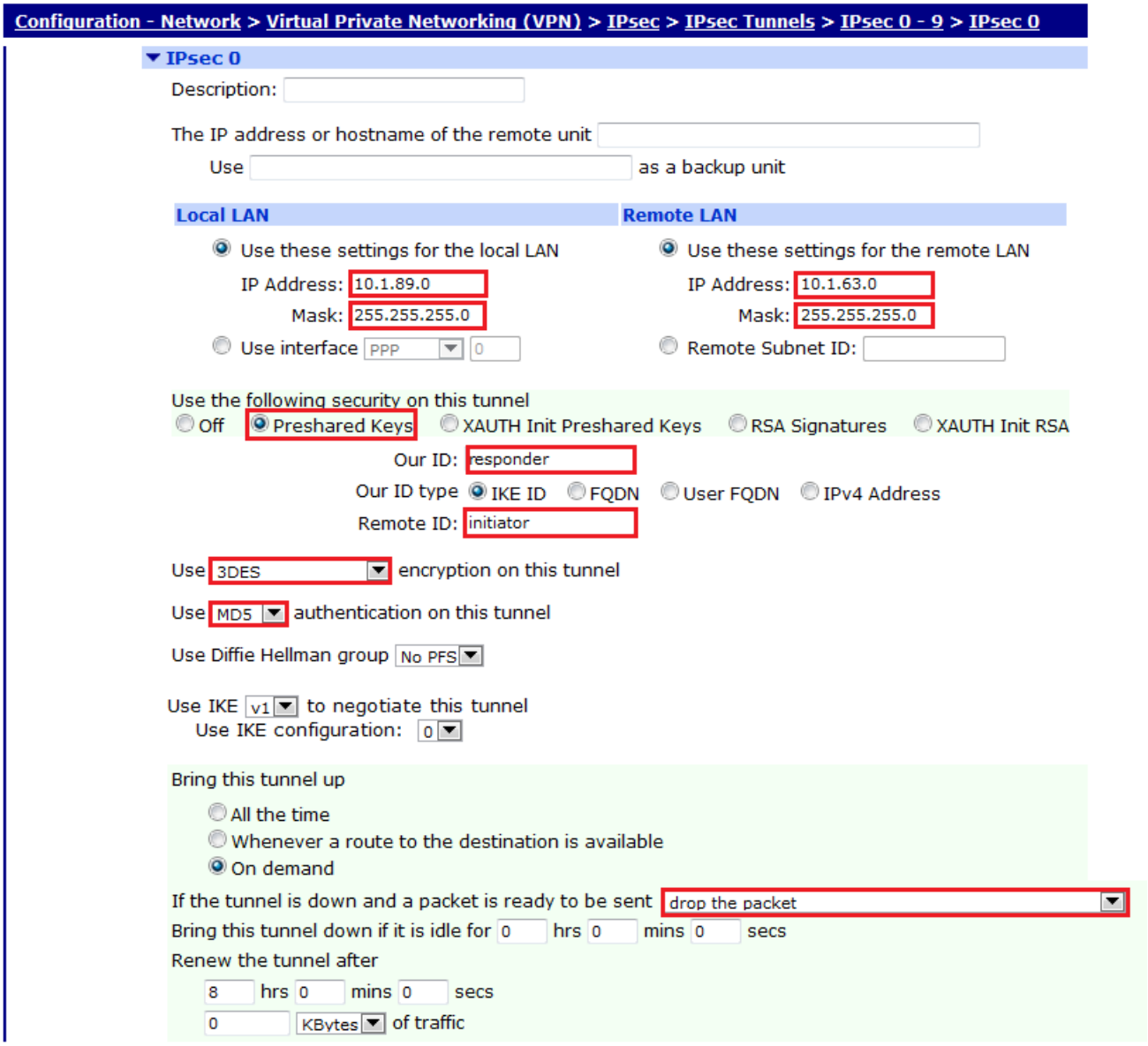
Click Apply

3.2.1 DR6410 Phase 2 – IPSEC

As this is the responder unit and the client doesn't have a static IP due to connecting over a cellular network, this router does not initiate the IPSec tunnel it is a responder only.

Browse to **Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0 - 9 > IPsec 0**

Parameter	Setting	Description
Local LAN IP Address	10.1.89.0	Packets will be directed through this tunnel if the source and destination IP matches
Local LAN Mask	255.255.255.0	Subnet mask for the network
Remote LAN IP Address	10.1.63.0	Packets will be directed through this tunnel if the source and destination IP matches:
Remote LAN Mask	255.255.255.0	Subnet mask for the network
Use the following security on this tunnel	Pre-shared Keys	Pre-shared keys will be used for authentication
Our ID	Responder	The ID of the VPN initiator router (this router)
Remote ID	Initiator	The ID of the VPN responder router (remote router)
Use ( ) encryption on this tunnel	3DES	The IPSEC encryption algorithm to use is 3DES
Use ( ) Authentication on this tunnel	MD5	The IPSEC ESP authentication algorithm is MD5:
Bring this tunnel up	Whenever a route to the destination is available	
If this tunnel is down and a packet is ready to be sent	Bring the tunnel up	


Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0 - 9 > IPsec 0
IPsec 0
Description:
The IP address or hostname of the remote unit
Use as a backup unit
Local LAN
Use these settings for the local LAN
IP Address: 10.1.89.0
Mask: 255.255.255.0
Use interface PPP 0
Remote LAN
Use these settings for the remote LAN
IP Address: 10.1.63.0
Mask: 255.255.255.0
Remote Subnet ID:
Use the following security on this tunnel
Off
Preshared Keys
XAUTH Init Preshared Keys
RSA Signatures
XAUTH Init RSA
Our ID: responder
Our ID type IKE ID FQDN User FQDN IPv4 Address
Remote ID: initiator
Use 3DES encryption on this tunnel
Use MD5 authentication on this tunnel
Use Diffie Hellman group No PFS
Use IKE v1 to negotiate this tunnel
Use IKE configuration: 0
Bring this tunnel up
All the time
Whenever a route to the destination is available
On demand
If the tunnel is down and a packet is ready to be sent drop the packet
Bring this tunnel down if it is idle for 0 hrs 0 mins 0 secs
Renew the tunnel after
8 hrs 0 mins 0 secs
0 KBytes of traffic

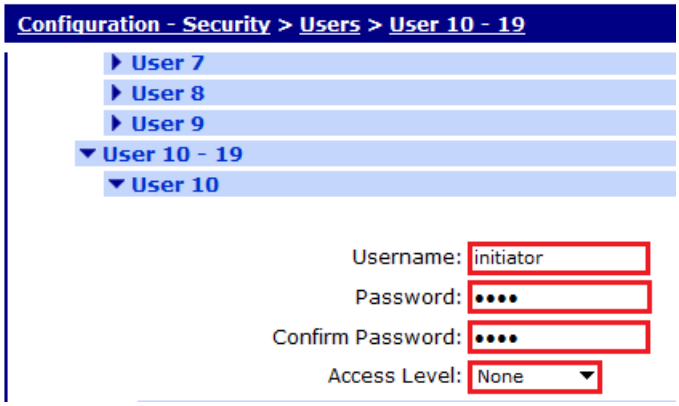
Click Apply

3.2.2 DR6410 Initiator Pre-shared Key

In this section the pre-shared key is set up, the pre-shared key is set up by creating a username with the name of the remote peer (responder) VPN id and the password is the pre-shared key.

Browse to **Configuration - Security > Users > User 10 - 14 > User 10**

Parameter	Setting	Description
Username	initiator	Name should match the Peer ID: value from Eroute 0
Password	test	Enter the password – in a production environment you will want to choose a more secure shared key than this
Confirm Password	test	
Access Level	None	This user will not be granted any admin access as only used as a pre-shared key



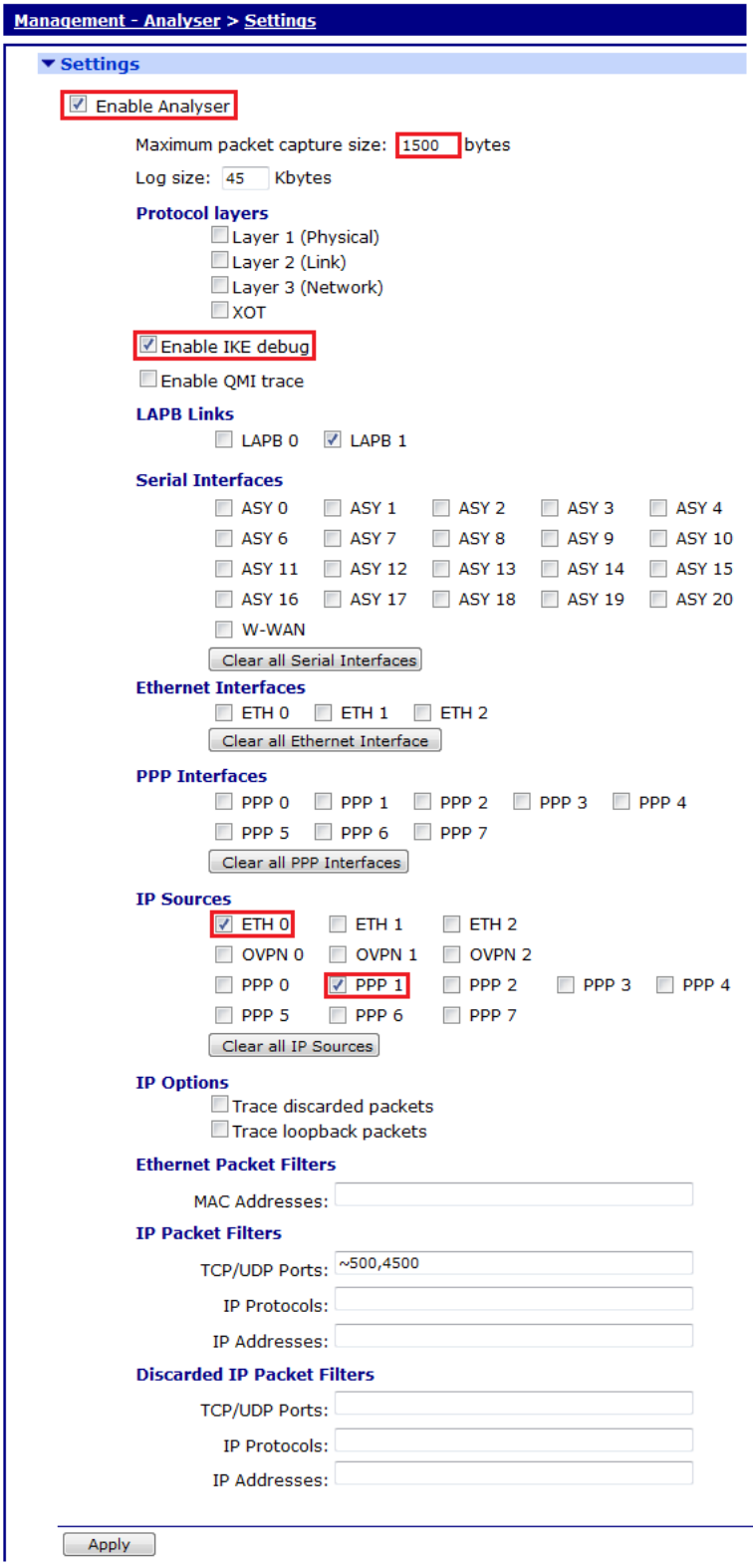
Click Apply

3.2.3 Configure the Analayser.

Browse to **Management - Analyser > Settings**

Configure the following settings -

Parameter	Setting	Description
Enable Analyser	✓	Turn on the analyser
Max packet capture size	1500	Capture any packet up to 1500 Bytes
Enable IKE Debug	✓	When this is ticked we will see IKE debug in the trace
IP Source	Eth 0	Enable logging for this interface
IP Source	PPP 1	Enable logging for this interface
IP Packet filter ports	500, 4500	Restrict the ports logged to show only IKE and IPSec


Management - Analyser > Settings
Settings
Enable Analyser
Maximum packet capture size: 1500 bytes
Log size: 45 Kbytes
Protocol layers
Layer 1 (Physical)
Layer 2 (Link)
Layer 3 (Network)
XOT
Enable IKE debug
Enable QMI trace
LAPB Links
LAPB 0
LAPB 1
Serial Interfaces
ASY 0
ASY 1
ASY 2
ASY 3
ASY 4
ASY 6
ASY 7
ASY 8
ASY 9
ASY 10
ASY 11
ASY 12
ASY 13
ASY 14
ASY 15
ASY 16
ASY 17
ASY 18
ASY 19
ASY 20
W-WAN
Clear all Serial Interfaces
Ethernet Interfaces
ETH 0
ETH 1
ETH 2
Clear all Ethernet Interface
PPP Interfaces
PPP 0
PPP 1
PPP 2
PPP 3
PPP 4
PPP 5
PPP 6
PPP 7
Clear all PPP Interfaces
IP Sources
ETH 0
ETH 1
ETH 2
OVPN 0
OVPN 1
OVPN 2
PPP 0
PPP 1
PPP 2
PPP 3
PPP 4
PPP 5
PPP 6
PPP 7
Clear all IP Sources
IP Options
Trace discarded packets
Trace loopback packets
Ethernet Packet Filters
MAC Addresses:
IP Packet Filters
TCP/UDP Ports: ~500,4500
IP Protocols:
IP Addresses:
Discarded IP Packet Filters
TCP/UDP Ports:
IP Protocols:
IP Addresses:
Apply

Click Apply

4 TESTING

4.1 Successful connection:

The event log shows the events occurring within the operating system. Here you can see the cellular interface (PPP 1) establishing followed by the VPN.

Management - Event Log

```
02:37:41, 01 Jan 2000,ETH 0 up
02:37:00, 01 Jan 2000,DTR Up ASY 0
02:27:36, 01 Jan 2000,(2) IKE SA Removed. Peer: responder,Successful Negotiation
02:27:07, 01 Jan 2000,Eroute 0 VPN up peer: responder
02:27:07, 01 Jan 2000,New IPSec SA created by responder
02:27:07, 01 Jan 2000,(2) IKE Notification: Initial Contact,RX
02:27:07, 01 Jan 2000,(2) New Phase 2 IKE Session 213.152.58.85,Initiator
02:27:07, 01 Jan 2000,(1) IKE Keys Negotiated. Peer: responder
02:27:06, 01 Jan 2000,(1) New Phase 1 IKE Session 213.152.58.85,Initiator
02:27:06, 01 Jan 2000,IKE Request Received From Eroute 0
02:27:06, 01 Jan 2000,PPP 1 up
02:27:04, 01 Jan 2000,PPP 1 Start IPCP
02:27:04, 01 Jan 2000,PPP 1 Start AUTHENTICATE
02:27:04, 01 Jan 2000,PPP 1 Start LCP
02:27:04, 01 Jan 2000,PPP 1 Start
```

And here you can see the DSL interface (PPP 1) establishing followed by the VPN.

Management - Event Log

```
16:42:07, 02 Jun 2011,PPP 3 down,LL disconnect
16:42:07, 02 Jun 2011,Event delay,Logger busy
16:41:57, 02 Jun 2011,PPP 3 down,LL disconnect
16:41:55, 02 Jun 2011,(3) IKE SA Removed. Peer: initiator,Successful Negotiation
16:41:53, 02 Jun 2011,Eroute 0 VPN up peer: initiator
16:41:53, 02 Jun 2011,New IPSec SA created by initiator
16:41:51, 02 Jun 2011,(3) IKE Notification: Initial Contact,RX
16:41:51, 02 Jun 2011,(3) New Phase 2 IKE Session 212.183.140.43,Responder
16:41:51, 02 Jun 2011,Event delay,Logger busy
16:41:47, 02 Jun 2011,PPP 3 down,LL disconnect
16:41:46, 02 Jun 2011,(1) IKE Keys Negotiated. Peer: initiator
16:41:46, 02 Jun 2011,(1) New Phase 1 IKE Session 212.183.140.43,Responder
16:41:37, 02 Jun 2011,PPP 3 down,LL disconnect
16:41:36, 02 Jun 2011,PPP 1 up
16:41:36, 02 Jun 2011,PPP 1 Start IPCP
16:41:36, 02 Jun 2011,PPP 1 Start AUTHENTICATE
16:41:36, 02 Jun 2011,PPP 1 Start LCP
16:41:35, 02 Jun 2011,PPP 1 Start AUTHENTICATE
16:41:32, 02 Jun 2011,PPP 1 Start LCP
16:41:32, 02 Jun 2011,PPP 1 Start
16:41:32, 02 Jun 2011,ATM PVC 0 up
16:41:32, 02 Jun 2011,ADSL 0 up
16:41:32, 02 Jun 2011,ADSL line: Up (7808 kbps down | 832 kbps up)
16:41:32, 02 Jun 2011,Event delay,Logger busy
16:41:28, 02 Jun 2011,ASY 8 assigned to usb-1-1 (Novatel Wireless HSDPA Modem)
```

4.1.1 IPSEC Security Associations

When a VPN is successful, the IPSec SAs can be viewed on both the Initiator and the Responder IPSec SAs list. This shows the peer IP the remote and local networks, the authentication algorithm and time left until keys are again exchanged.

4.1.2 Management - Connections > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels

TransPort DR64 (SN: 92903) Configuration and Management

Management - Connections > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec Tunnels 0 - 9 > IPsec Tunnel 0

IPsec Tunnel 0

Outbound V1 SAs

#	Peer IP Addr	Local Network	Remote Network	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left (secs)	Interface	
0	212.183.140.43	10.1.89.0/24	10.1.63.0/24	N/A	MD5	3DES	N/A	0	0	28308	PPP 1	Remove

Remove All

Inbound V1 SAs

#	Peer IP Addr	Local Network	Remote Network	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left (secs)	Interface	
0	212.183.140.43	10.1.89.0/24	10.1.63.0/24	N/A	MD5	3DES	N/A	0	0	28308	PPP 1	Remove

Remove All

Outbound V2 SAs

No Tunnels

Inbound V2 SAs

No Tunnels

Refresh

TransPort WR41 (SN: 102701) Configuration and Management

Management - Connections > Virtual Private Networking (VPN) > IPsec

IP Connections

PPP Connections

Virtual Private Networking (VPN)

IPsec

IPsec Tunnels

Outbound V1 SAs

#	Peer IP Addr	Local Network	Remote Network	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left (secs)	Interface	
0	213.152.58.85	10.1.63.0/24	10.1.89.0/24	N/A	MD5	3DES	N/A	0	0	28088	PPP 1	Remove

Remove All

Inbound V1 SAs

#	Peer IP Addr	Local Network	Remote Network	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left (secs)	Interface	
0	213.152.58.85	10.1.63.0/24	10.1.89.0/24	N/A	MD5	3DES	N/A	0	0	28088	PPP 1	Remove

Remove All

Outbound V2 SAs

No Tunnels

Inbound V2 SAs

No Tunnels

Refresh

5 CONFIGURATION FILES

5.1 Digi Transport WR41 (Initiator) Configuration

```
eth 0 IPaddr "10.1.63.254"
eth 0 ipanon ON
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 3 dtemode 0
lapb 4 dtemode 0
lapb 5 dtemode 0
lapb 6 dtemode 0
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
eroute 0 peerip "213.152.58.85"
eroute 0 peerid "responder"
eroute 0 ourid "initiator"
eroute 0 locip "10.1.63.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 remip "10.1.89.0"
eroute 0 remmsk "255.255.255.0"
eroute 0 ESPauth "MD5"
eroute 0 ESPenc "3DES"
eroute 0 lkbytes 0
eroute 0 authmeth "PRESHARED"
eroute 0 nosa "TRY"
eroute 0 autosa 1
eroute 0 debug ON
dhcp 0 IPmin "192.168.1.100"
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "192.168.1.1"
dhcp 0 respdelms 500
ppp 0 timeout 300
ppp 1 r_chap OFF
ppp 1 IPaddr "0.0.0.0"
ppp 1 phonenum "*98*1#"
ppp 1 timeout 0
ppp 1 use_modem 1
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 ipsec 1
ppp 1 ipanon ON
ppp 3 defpak 16
ppp 4 defpak 16
ike 0 encalg "3DES"
ike 0 aggressive ON
ike 0 ikegroup 2
ike 0 deblevel 4
ike 0 delmode 1
modemcc 0 info_asy_add 7
```

```
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "internet"
modemcc 0 link_retries 10
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
modemcc 0 sms_access 1
modemcc 0 sms_concat 0
modemcc 0 init_str_2 "+CGQREQ=1"
modemcc 0 init_str1_2 "+CGQMIN=1"
modemcc 0 apn_2 "Your.APN.goes.here"
modemcc 0 link_retries_2 10
modemcc 0 stat_retries_2 30
ana 0 anon ON
ana 0 l1on ON
ana 0 lapdon 0
ana 0 asyon 1
ana 0 ipfilt "~500,4500"
ana 0 ikeon ON
ana 0 maxdata 1500
ana 0 logsize 45
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 asyled_mode 2
cmd 0 tremto 1200
cmd 0 web_suffix ".wb2"
user 0 access 0
user 1 name "username"
user 1 epassword "KD5lSVJDVVg="
user 1 access 0
user 2 access 0
user 3 access 0
user 4 access 0
user 5 access 0
user 6 access 0
user 7 access 0
user 8 access 0
user 9 access 0
user 10 name "responder"
user 10 epassword "LDplTg=="
user 10 access 4
local 0 transaccess 2
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
```

5.2 Digi Transport DR6410 (Responder) Configuration

```
eth 0 IPaddr "10.1.89.254"
eth 0 bridge ON
eth 0 ipanon ON
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 3 dtemode 0
lapb 4 dtemode 0
lapb 5 dtemode 0
lapb 6 dtemode 0
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
def_route 1 ll_ent "PPP"
def_route 1 ll_add 3
def_route 2 ll_ent "PPP"
def_route 2 ll_add 4
eroute 0 peerid "initiator"
eroute 0 ourid "responder"
eroute 0 locip "10.1.89.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 remip "10.1.63.0"
eroute 0 remmsk "255.255.255.0"
eroute 0 ESPauth "MD5"
eroute 0 ESPenc "3DES"
eroute 0 lkbytes 0
eroute 0 authmeth "PRESHARED"
eroute 0 debug ON
dhcp 0 IPmin "192.168.0.1"
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.0.99"
dhcp 0 DNS "192.168.0.99"
dhcp 0 wifionly ON
ppp 0 timeout 300
ppp 1 IPaddr "0.0.0.0"
ppp 1 username "your ADSL username"
ppp 1 epassword "PTJ5WU1NRFM="
ppp 1 timeout 0
ppp 1 aodion 1
ppp 1 immoos ON
ppp 1 autoassert 1
ppp 1 ipsec 2
ppp 1 echo 10
ppp 1 echodropcnt 5
ppp 1 l1iface "AAL"
ppp 1 ipanon ON
ppp 3 l_pap OFF
ppp 3 l_chap OFF
ppp 3 l_addr ON
ppp 3 r_chap OFF
ppp 3 r_addr OFF
```

```
ppp 3 IPaddr "0.0.0.0"
ppp 3 username "ENTER WWAN Username"
ppp 3 epassword "KD5lSVJDVVg="
ppp 3 phonenum "*98*1#"
ppp 3 timeout 0
ppp 3 use_modem 1
ppp 3 aodion 1
ppp 3 immoos ON
ppp 3 autoassert 1
ppp 3 defpak 16
ppp 4 l_acfc ON
ppp 4 l_pfc ON
ppp 4 IPaddr "1.2.3.5"
ppp 4 IPmin "10.10.10.0"
ppp 4 username "Enter PSTN Username"
ppp 4 timeout 60
ppp 4 use_modem 3
ppp 4 defpak 16
ike 0 deblevel 4
modemcc 0 info_asy_add 9
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "Your.APN.Goes.Here"
modemcc 0 link_retries 10
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
modemcc 0 init_str_2 "+CGQREQ=1"
modemcc 0 init_str1_2 "+CGQMIN=1"
modemcc 0 apn_2 "Your.APN.Goes.Here"
modemcc 0 link_retries_2 10
modemcc 0 stat_retries_2 30
modemcc 0 sms_interval_2 1
ana 0 anon ON
ana 0 l1on ON
ana 0 lapdon 0
ana 0 asyon 1
ana 0 ipfilt "~500,4500"
ana 0 ikeon ON
ana 0 maxdata 1500
ana 0 logsize 45
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "sarian.router"
cmd 0 tremto 1200
cmd 0 web_suffix ".wb2"
user 0 name "username"
user 0 epassword "KD5lSVJDVVg="
user 1 access 0
user 2 access 0
user 3 access 0
user 4 access 0
user 5 access 0
user 6 access 0
user 7 access 0
```

```
user 8 access 0
user 9 access 0
user 10 name "initiator"
user 10 epassword "LDplTg=="
user 10 access 4
local 0 transaccess 2
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
wifi 0 enabled OFF
wifi 0 ssid "sarian.router.SN:%s"
wifi 1 enabled OFF
```

5.2.1 Digi Transport Firmware Versions

5.2.2 This is the firmware \ hardware information from VPN responder DR64:

```
Digi TransPort DR64-HXA2-WE2-XX(MkII) Ser#:92903 HW Revision: 7502a
Software Build Ver5129.  May 20 2011 12:13:20  9W
ARM Bios Ver 6.02 v35 197MHz B128-M128-F300-O0,2 MAC:00042d016ae7
Power Up Profile: 0
Async Driver              Revision: 1.19  Int clk
Ethernet Port Isolate Driver Revision: 1.11
Firewall                  Revision: 1.0
EventEdit                 Revision: 1.0
Timer Module              Revision: 1.1
AAL                       Revision: 1.0
ADSL                      Revision: 1.0
(B)USBHOST                Revision: 1.0
L2TP                      Revision: 1.10
PPTP                      Revision: 1.00
TACPLUS                   Revision: 1.00
MySQL                     Revision: 0.01
LAPB                      Revision: 1.12
X25 Layer                 Revision: 1.19
MACRO                     Revision: 1.0
PAD                       Revision: 1.4
X25 Switch                Revision: 1.7
V120                      Revision: 1.16
TPAD Interface            Revision: 1.12
SCRIBATSK                 Revision: 1.0
BASTSK                    Revision: 1.0
ARM Sync Driver           Revision: 1.18
TCP (HASH mode)           Revision: 1.14
TCP Utils                 Revision: 1.13
PPP                       Revision: 1.19
WEB                       Revision: 1.5
SMTP                      Revision: 1.1
FTP Client                Revision: 1.5
```

```
FTP                         Revision: 1.4
IKE                         Revision: 1.0
PollANS                     Revision: 1.2
PPPOE                       Revision: 1.0
BRIDGE                      Revision: 1.1
MODEM CC (Novatel 3G)       Revision: 1.4
FLASH Write                 Revision: 1.2
Command Interpreter         Revision: 1.38
SSLCLI                      Revision: 1.0
OSPF                        Revision: 1.0
BGP                         Revision: 1.0
QOS                         Revision: 1.0
RADIUS Client               Revision: 1.0
SSH Server                  Revision: 1.0
SCP                         Revision: 1.0
CERT                        Revision: 1.0
LowPrio                     Revision: 1.0
Tunnel                      Revision: 1.2
OVPN                        Revision: 1.2
TEMPLOG                     Revision: 1.0
Wi-Fi                       Revision: 2.0
iDigi                       Revision: 2.0
```

5.2.3 This is the firmware \ hardware information from VPN Initiator WR41:

```
Digi TransPort WR41-HXI1-DV1-XX(WR41v1) Ser#:102701 HW Revision: 7103a
Software Build Ver5125.  Apr 05 2011 10:58:42  ZW
ARM Bios Ver 5.95 v36 399MHz B128-M128-F80-O100,0 MAC:00042d01912d
Power Up Profile: 0
Async Driver                Revision: 1.19  Int clk
Ethernet Driver             Revision: 1.11
ISDN ST 21150 Driver        Revision: 1.7
Firewall                    Revision: 1.0
EventEdit                   Revision: 1.0
Timer Module                Revision: 1.1
(B)USBHOST                  Revision: 1.0
SDMMC                       Revision: 1.0
L2TP                        Revision: 1.10
PPTP                        Revision: 1.00
TACPLUS                     Revision: 1.00
MODBUS                      Revision: 0.00
LAPB                        Revision: 1.12
LAPD                        Revision: 1.16
TEI Management              Revision: 1.6
BRI Call Control Layer      Revision: 1.11
X25 Layer                   Revision: 1.19
MACRO                       Revision: 1.0
```

```
PAD                         Revision: 1.4
V120                        Revision: 1.16
TPAD Interface              Revision: 1.12
GPS                         Revision: 1.0
SCRIBATSK                   Revision: 1.0
BASTSK                      Revision: 1.0
PYTHON                      Revision: 1.0
ARM Sync Driver             Revision: 1.18
TCP (HASH mode)             Revision: 1.14
TCP Utils                   Revision: 1.13
PPP                         Revision: 1.19
WEB                         Revision: 1.5
SMTP                        Revision: 1.1
FTP Client                  Revision: 1.5
FTP                         Revision: 1.4
IKE                         Revision: 1.0
PollANS                     Revision: 1.2
PPPOE                       Revision: 1.0
MODEM CC (Option 3G)        Revision: 1.4
FLASH Write                 Revision: 1.2
Command Interpreter         Revision: 1.38
SSLCLI                      Revision: 1.0
OSPF                        Revision: 1.0
BGP                         Revision: 1.0
QOS                         Revision: 1.0
PWRCTRL                     Revision: 1.0
RADIUS Client               Revision: 1.0
SSH Server                  Revision: 1.0
SCP                         Revision: 1.0
CERT                        Revision: 1.0
LowPrio                     Revision: 1.0
Tunnel                      Revision: 1.2
OVPN                        Revision: 1.2
iDigi                       Revision: 2.0
```