Application Note 50

Configure a Digi TransPort to be an L2TP over IPsec VPN server for Apple and Android tablets and smart phones

UK Support

November 2015

Contents

1 INTRODUCTION

1.1 Outline

Layer 2 Tunneling Protocol (L2TP) can be used to tunnel layer 2 frames and thus provide remote access to a private LAN. This VPN is also suitable to facilitate a secure connection when using a public Wi-Fi hotspot, ensuring that traffic from the client device cannot be sniffed or intercepted by someone else using the same hotspot.

IPSec is a standard for encryption and security, running L2TP over IPsec can therefore provide secure encrypted remote access to a private LAN. This is commonly known as a VPN or Virtual Private Network connection.

Android and Apple iOS provide a VPN client that is capable of running L2TP over IPsec. This application note explains how to configure a Digi TransPort router to act as an L2TP/IPsec VPN server for an Android or Apple iOS client.

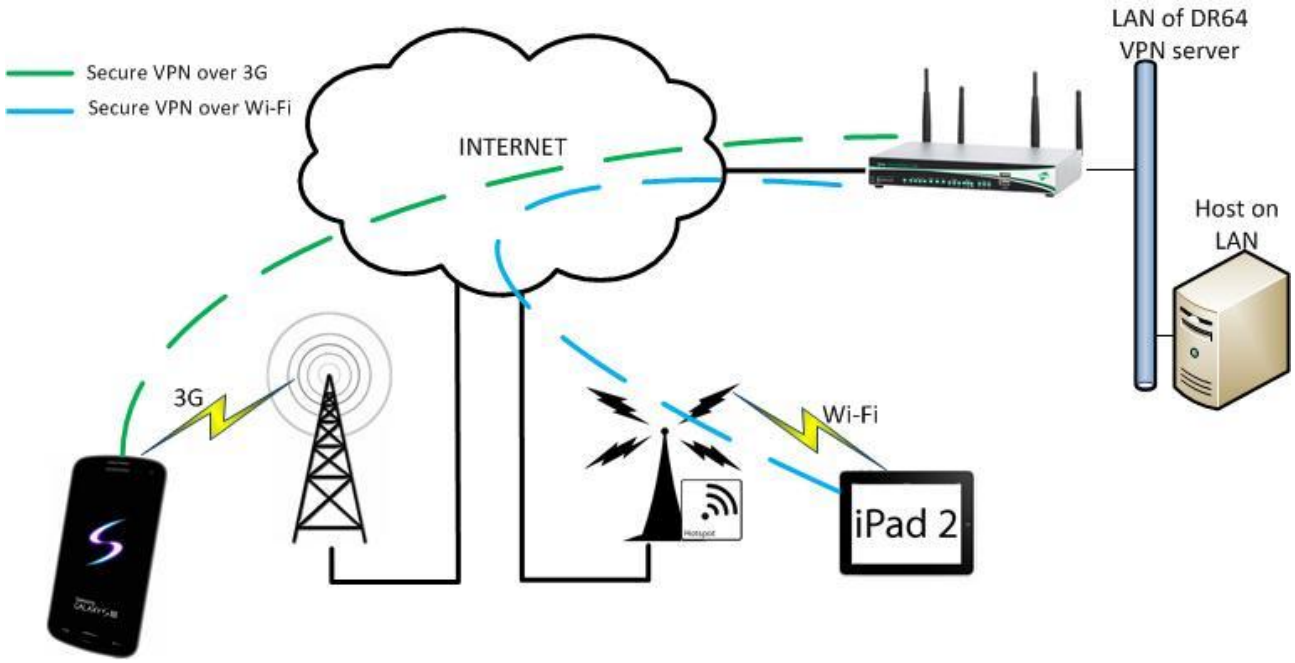
This solution works as long as the client has internet access, regardless of whether the connectivity is via Wi-Fi or a mobile network.

This application note explains the procedure of configuring a Digi TransPort DR64 router as a L2TP over IPsec VPN Server.

L2TP will run over the IPsec connection and the PPP connection will be negotiated over the newly established L2TP Pipe.

The remote clients will be using the bundled OS features and no extra 3rd party applications are required. This Application note will also take the user through the Android & Apple iOS configuration.

NB Although in this example the DR64 model is used, the same settings can be applied to all other Digi TransPort models. (Certain models may not have the IPsec encryption option enabled, if this is the case, please contact Digi Support for details on how to enable this option.)



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.

This application note applies to;

Models shown: Digi TransPort DR64 with firmware version 5156

Other Compatible Models: All Digi TransPort products.

Other suitable firmware versions: 4.967 or newer (GUI might look different to what is shown in this document, but the configuration is still valid)

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.

Users should have access to the Digi TransPort command line interface (via serial port or telnet) and also the web interface.

Other devices hardware & firmware versions:

Tablet: Apple iPad2 running iOS 5.1.1 (9B206)

Smart phone: Samsung Galaxy S GT-I9000 running Android 2.3.5 (Gingerbread)

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

Version Number	Status
1.0	Published

2 CONFIGURATION

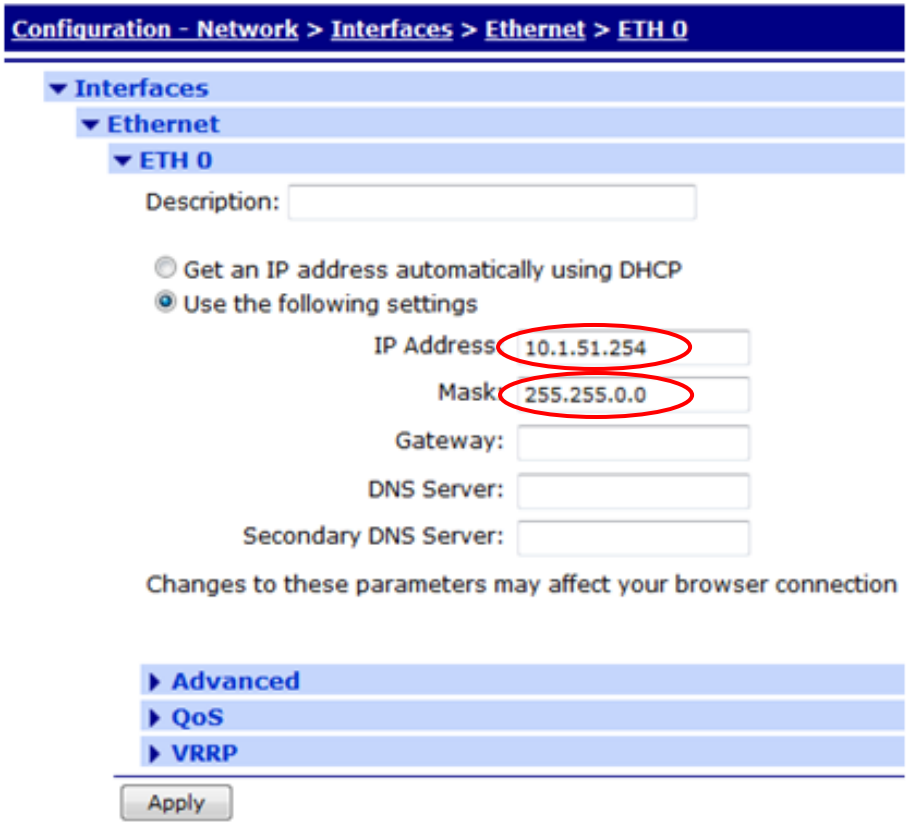
2.1 Configure DR64's LAN Interface

Assign an IP address and subnet mask to the Ethernet 0 interface. This is for the private LAN that the remote client requires access to.

Using the Digi TransPort's web interface navigate to

Configuration - Network > Interfaces > Ethernet > ETH 0

Configure the required IP address and subnet mask then click the 'Apply' button. Note that this step may have been done already and as such may not be required.



Parameter	Setting	Description
IP Address	*10.1.51.254*	Suggested IP address of server's LAN
Mask	*255.255.0.0*	Suggested mask of server's LAN

2.2 Configure DR64's ADSL (WAN) interface.

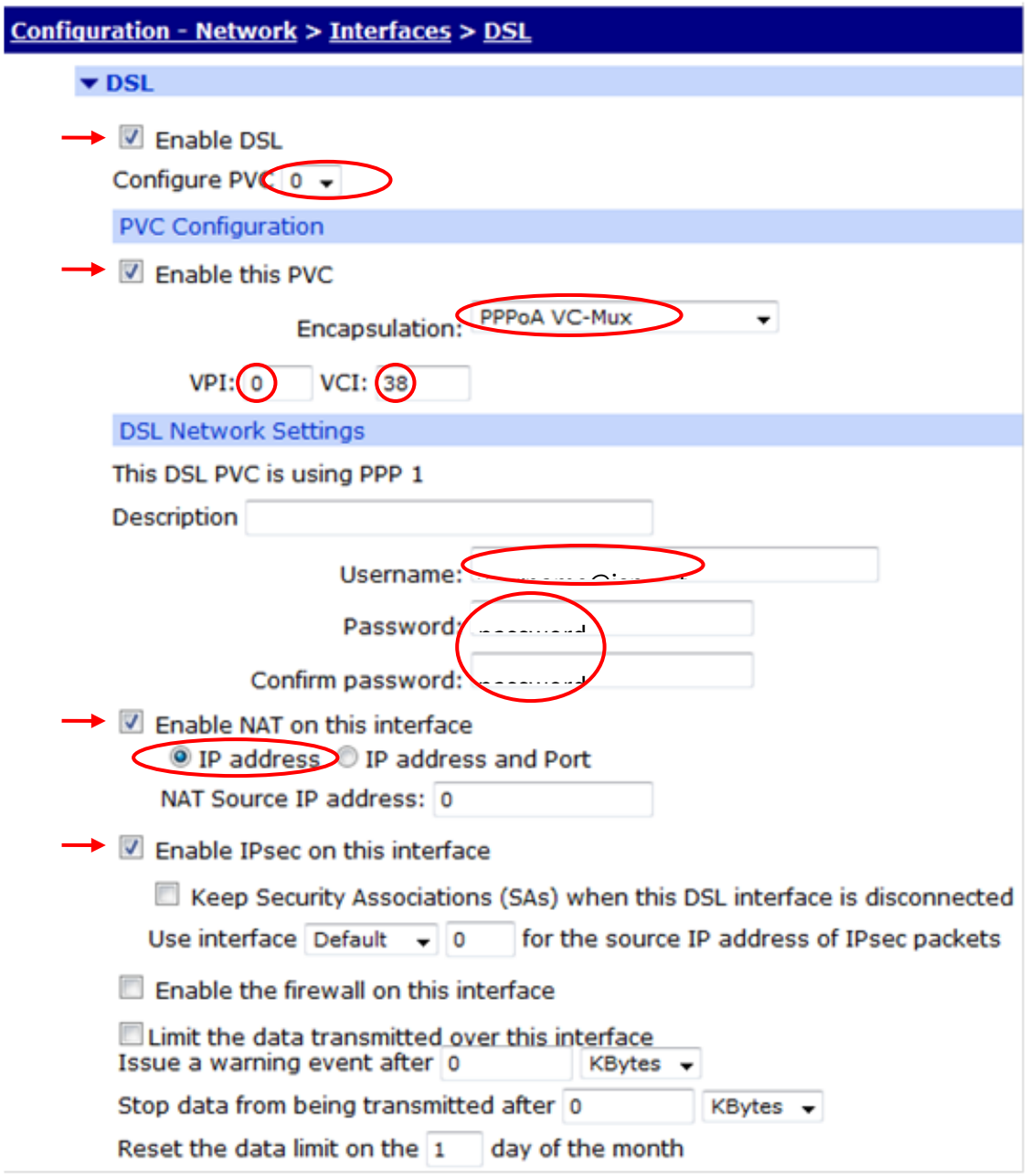
The Digi TransPort will be the VPN server and will need to be connected to the public Internet to allow clients to establish an L2TP\IPsec VPN. This can be any interface (depending on the connectivity used at the customer premises), but this Application Note will assume ADSL is used which is PPP 1.

Using the Digi TransPort's web interface navigate to
Configuration – Network > Interfaces > DSL

Enter the Encapsulation type, VPI & VCI settings, the ADSL username and password, these can be obtained from your ISP if not known.

Also ensure the PVC is set to '0' (zero), NAT is enabled & IPsec is enabled.

Click 'Apply' when settings are complete.



Parameter	Setting	Description
Enable DSL	*checked*	Enables the DSL parameters
Configure PVC	*0*	Sets the PVC to use
Enable this PVC	*checked*	Makes this PVC active
Encapsulation	*PPPoA VC-Mux*	The encapsulation method used by the ISP
VPI	*0*	The VPI for the ADSL service
VCI	*38*	The VCI for the ADSL service
Username	*user@isp.net*	The username for the ADSL service
Password	*password*	The password for the ADSL service
Confirm password	*password*	Type the same password in again
IPSec	*checked*	Enables IPsec on this interface.

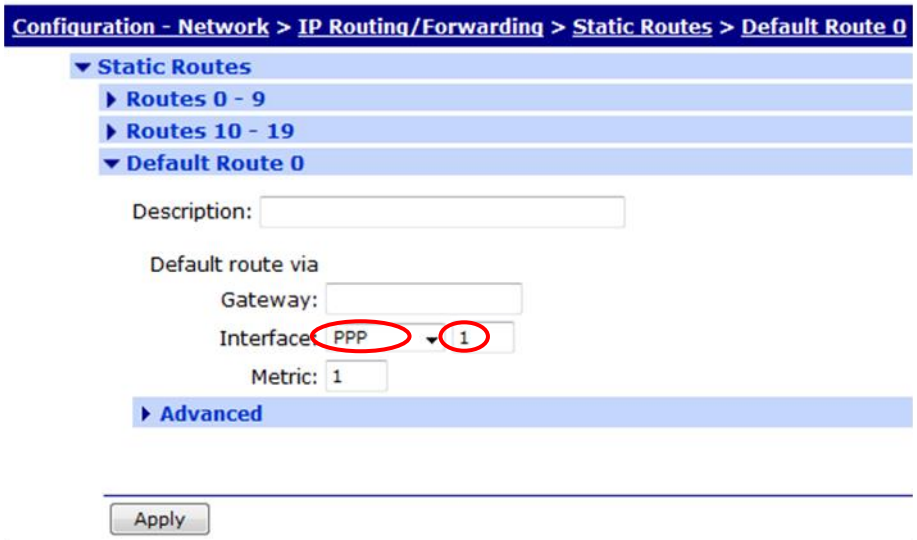
2.3 Configure DR64's Default Route

A routing table entry needs to be added to direct returning IP packets back through the VPN tunnel, so a default route is needed to point to WAN interface configured in step 2.2

Using the Digi TransPort's web interface navigate to

Configuration - Network > IP Routing/Forwarding > Static Routes > Default Route 0

Confirm the default route is correct or enter a new default route:



Parameter	Setting	Description
Interface	PPP 1	Routes traffic to the PPP 1 interface

2.4 Configure DR64's IKE settings – IPsec phase 1

L2TP will be used across an established IPSec VPN tunnel, so first an IPSec Security Association (SA) with an initiating peer will need to be established. These IPsec sections detail the configuration for responding to all the initiating IPSec Peers (tablets and smart phones).

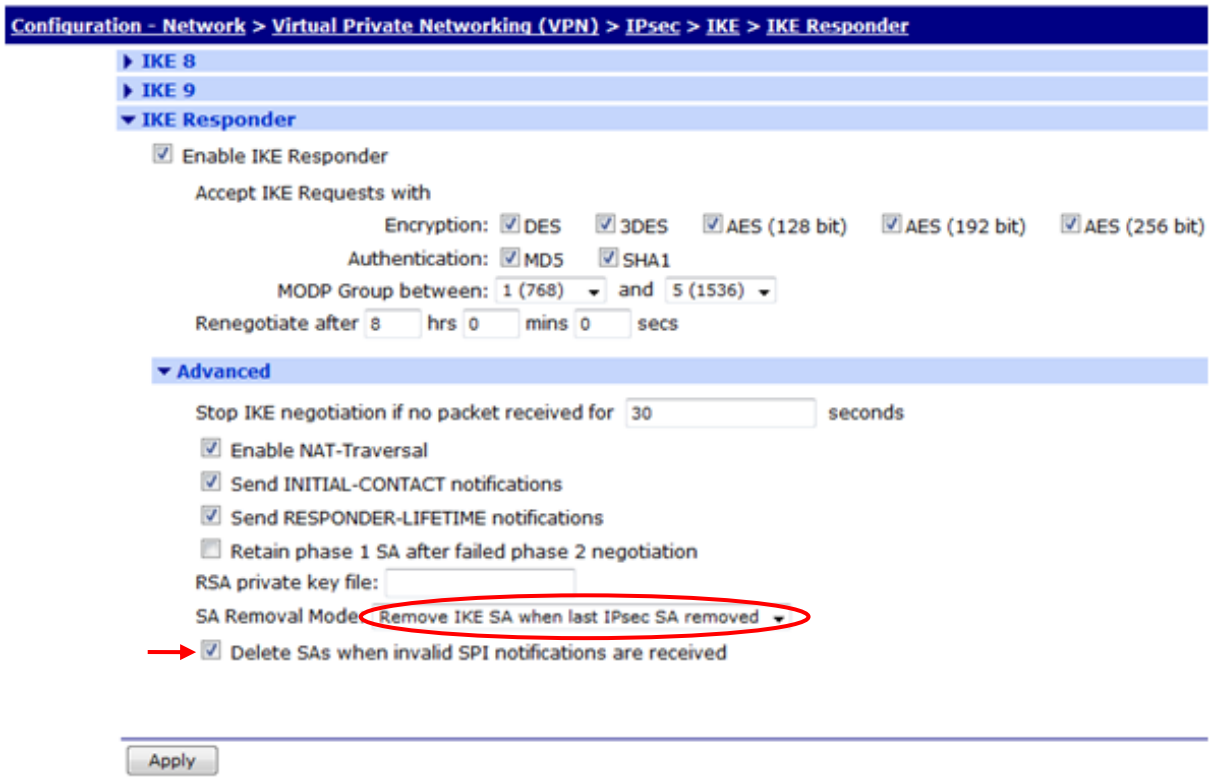
Internet Key Exchange (IKE) is used to associate two end points of a VPN tunnel, various parameters are exchanged including a secret 'key' that either end of the IPSec tunnel will use to encrypt and decrypt IPsec payloads.

Using the Digi TransPort's web interface navigate to
Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE Responder

Phase 1 of the VPN set up, IKE, is set by default to allow all combinations of authentication and encryption algorithm proposals. Only a couple of extra settings need to be configured.

Configure the VPN Phase 1, IKE, so that all relevant SAs are removed when a VPN is disconnected.

Leave all other settings at default values, as shown below.



Parameter	Setting	Description
SA Removal mode	Remove IKE SA when last IPsec SA removed	Ensures that IKE SAs are removed promptly
Delete SAs when invalid SPI notifications are received	Checked	Ensures that SAs are deleted if SPIs do not match

2.5 Configure DR64's IPsec phase 2 for Apple iOS devices

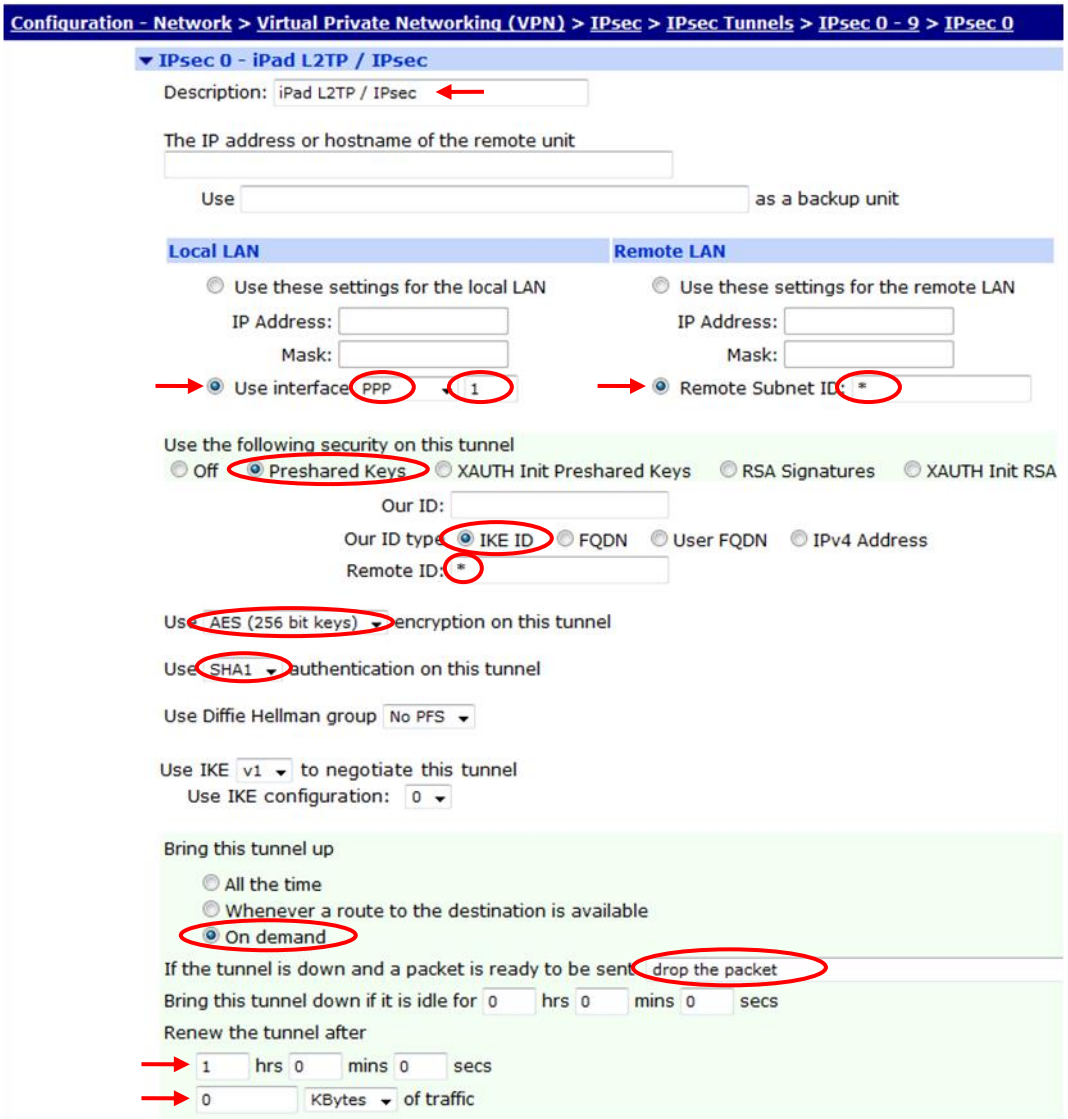
This section details configuration of the DR64 to negotiate with Apple iOS devices.

Do not try and use alternative values, the VPN will fail.

Using the Digi TransPort's web interface navigate to

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

Configure the basic settings as shown:



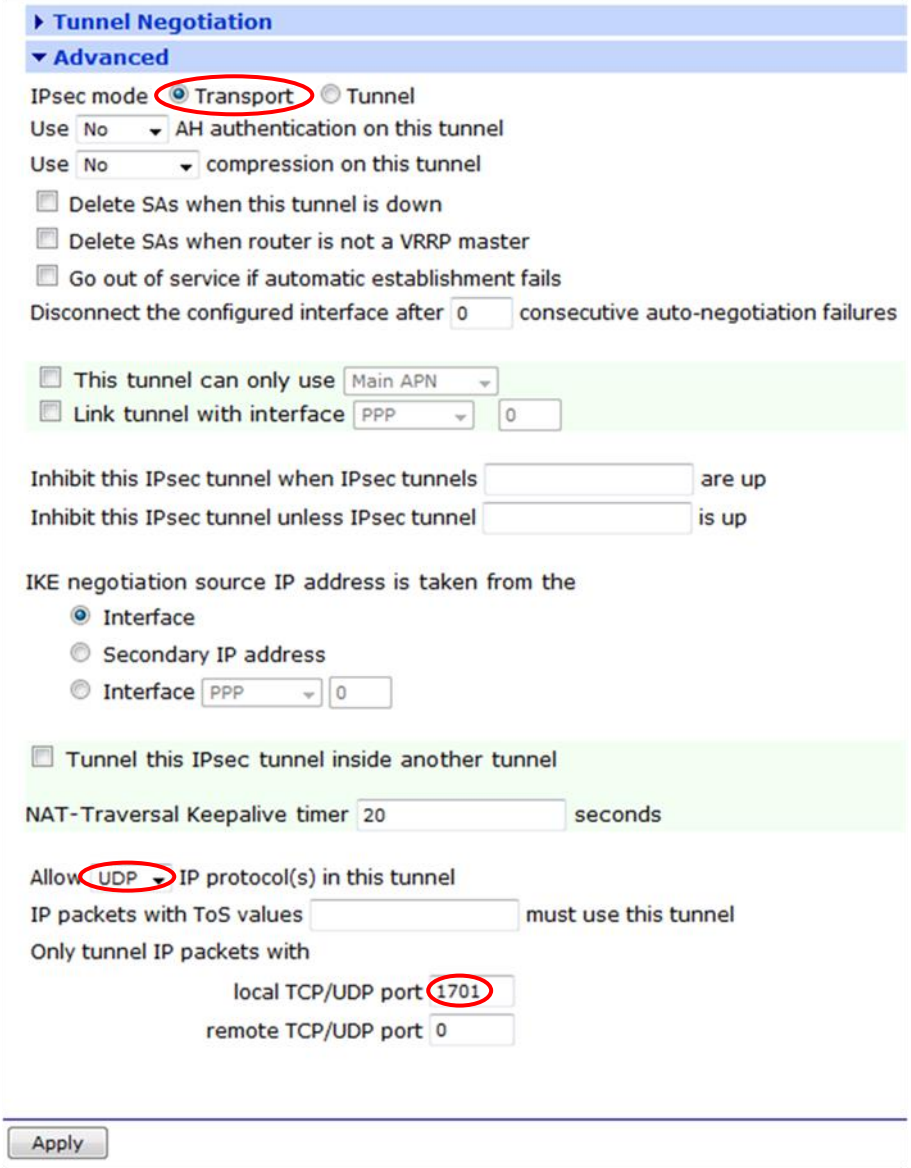
Parameter	Setting	Description
Description	iPad L2TP / IPsec	Friendly name for this VPN
Local LAN	Use Interface: PPP 1	Set this to the **WAN** interface configured earlier (Yes, WAN interface, not LAN)
Remote LAN	Remote Subnet ID: *	The ID this router expects to see from the peer. Asterisk = wildcard. Accept any peer ID.
Use the following security on this tunnel	Preshared Keys	Key to be used for IPsec will be populated in user table
Our ID	<leave blank>	Not used
Our ID Type	IKE ID	Type of IDs used
Remote ID	*	Any username can be used by the Peer
Use <enc> encryption on this	AES 256	ESP Packet Payload encryption Method to

tunnel		be used
Use <auth> authentication on this tunnel	SHA1	ESP Packet Authentication method to be used
Bring this tunnel up	On demand	Only raise the VPN when initiated by remote devices
If the tunnel is down and a packet is ready to be sent	Drop the packet	If the VPN is down, drop the packet.
Renew the tunnel after	1 hour 0 KBytes	Lifetime values to match the Apple iOS device

Click ‘Apply’, then scroll expand the ‘Advanced’ section directly below.

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0 - 9 > IPsec 0 > Advanced

Configure the Advanced settings as shown:



Parameter	Setting	Description
IPsec mode	Transport	Only IP payload is Encrypted within IPSec
Allow <prot> IP protocol(s) in this tunnel	UDP	Only UDP packets will cross Eroute
local TCP/UDP port	1701	Remote UDP port (L2TP) to use IPSec Eroute
*Local subnet IP address to negotiate (if different from above)	Public IP	If the Digi TransPort's WAN interface is NOT public (and IPsec traffic is forwarded to it from a public IP address) enter the public IP address here.
*Local subnet mask to negotiate (if different from above):	255.255.255.255	If the Digi TransPort's WAN interface is NOT public (and IPsec traffic is forwarded to it from a public IP address) enter 255.255.255.255 here.

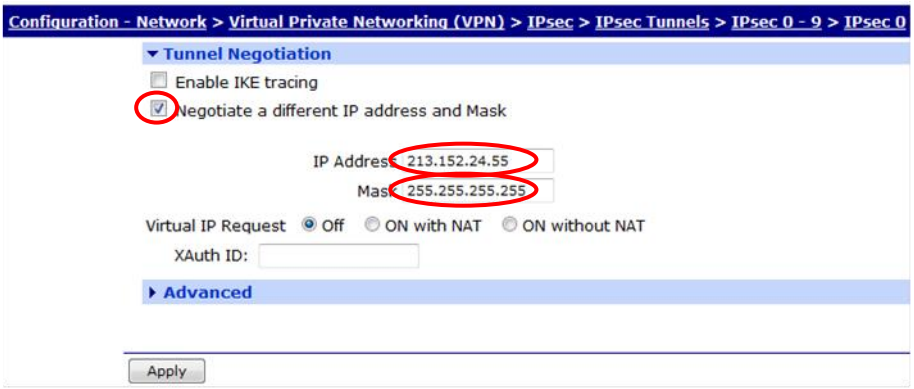
2.5.1 Additional step if this DR64 is not directly connected to the internet

If the DR64 is not directly attached to the internet, ie, it is behind a NAT router or firewall then this extra step is required. If the router is attached directly to the internet skip this step.

Browse to:

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0 - 9 > IPsec 0 > Tunnel Negotiation

Configure the negotiation settings as shown:



Parameter	Setting	Description
Negotiate a different IP address and Mask	checked	Enables negotiation of an alternative WAN interface address
IP Address	<Public IP address>	If the Digi TransPort's WAN interface is NOT public (and IPsec traffic is forwarded to it from a public IP address) enter the public IP address here.
Mask	255.255.255.255	If the Digi TransPort's WAN interface is NOT public (and IPsec traffic is forwarded to it from a public IP address) enter 255.255.255.255 here.

2.6 Configure DR64's IPsec phase 2 for Android devices

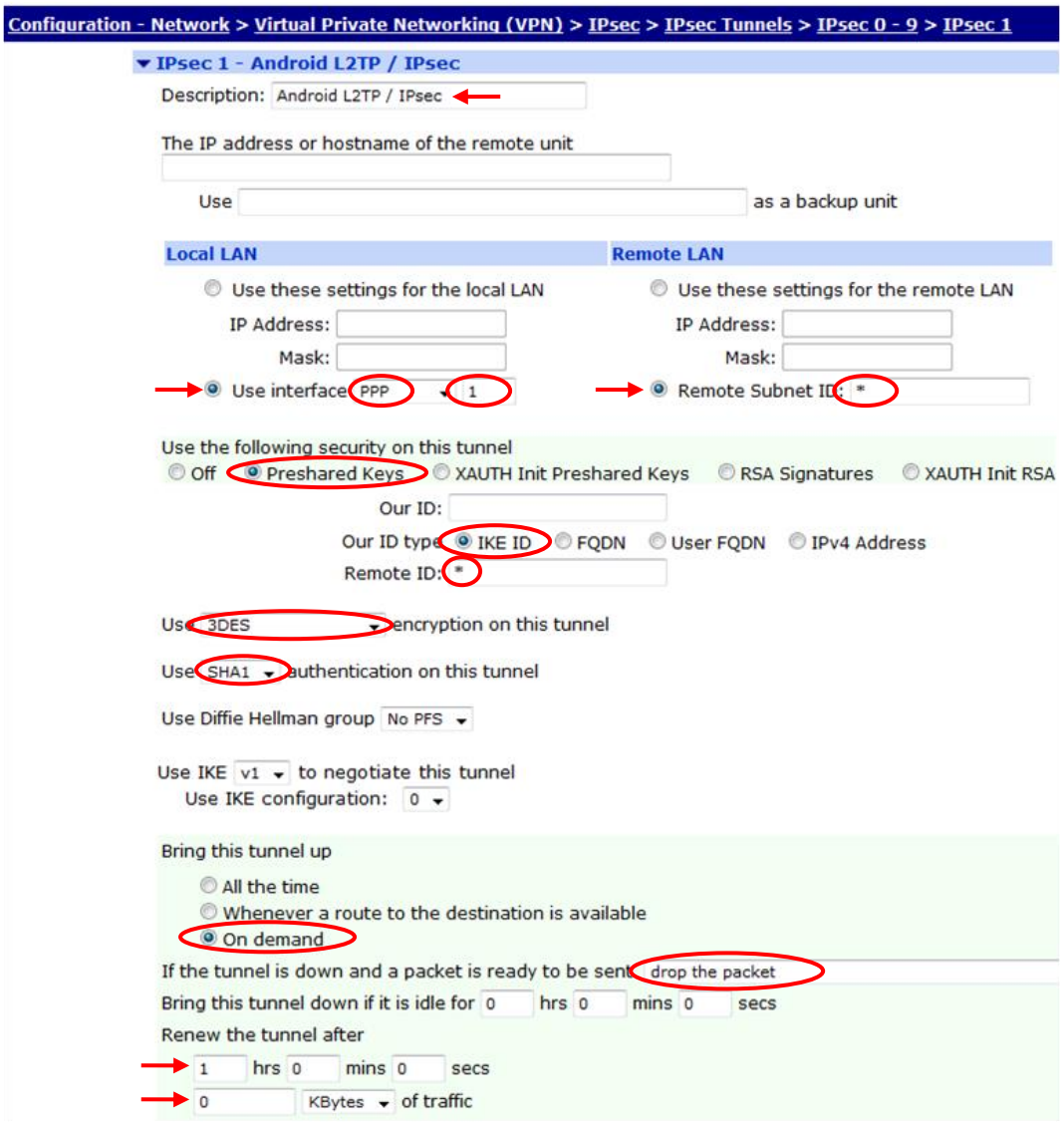
This section details configuration of the DR64 to negotiate with Android devices. The only difference between the Apple iOS (IPsec 0) settings and the Android (IPsec 1) settings is the encryption algorithm used. Apple iOS uses AES256, Android uses 3DES. All other settings are identical.

Do not try and use alternative values, the VPN will fail.

Using the Digi TransPort's web interface navigate to

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0 - 9 > IPsec 1

Configure the basic settings as shown:



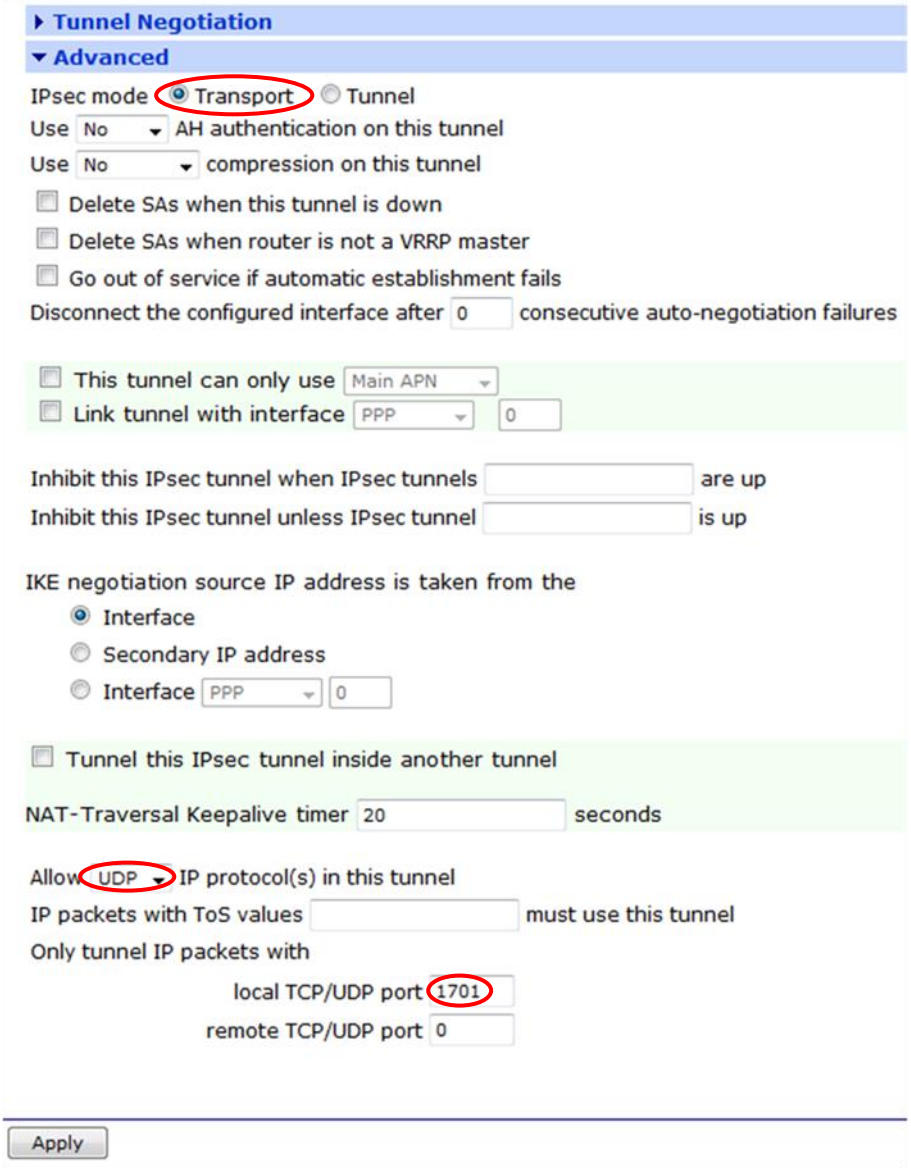
Parameter	Setting	Description
Description	Android L2TP / IPsec	Friendly name for this VPN
Local LAN	Use Interface: PPP 1	Set this to the **WAN** interface configured earlier (Yes, WAN interface, not LAN)
Remote LAN	Remote Subnet	The ID this router expects to see from the

	ID: *	peer. Asterisk = wildcard. Accept any peer ID.
Use the following security on this tunnel	Preshared Keys	Key to be used for IPsec will be populated in user table
Our ID	<leave blank>	Not used
Our ID Type	IKE ID	Type of IDs used
Remote ID	*	Any username can be used by the Peer
Use <enc> encryption on this tunnel	3DES	ESP Packet Payload encryption Method to be used
Use <auth> authentication on this tunnel	SHA1	ESP Packet Authentication method to be used
Bring this tunnel up	On demand	Only raise the VPN when initiated by remote devices
If the tunnel is down and a packet is ready to be sent	Drop the packet	If the VPN is down, drop the packet.
Renew the tunnel after	1 hour 0 KBytes	Lifetime values to match the Android device

Click ‘Apply’, then scroll expand the ‘Advanced’ section directly below.

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0 - 9 > IPsec 1 > Advanced

Configure the Advanced settings as shown:



Parameter	Setting	Description
IPsec mode	Transport	Only IP payload is Encrypted within IPSec
Allow <prot> IP protocol(s) in this tunnel	UDP	Only UDP packets will cross Eroute
local TCP/UDP port	1701	Remote UDP port (L2TP) to use IPSec Eroute
*Local subnet IP address to negotiate (if different from above)	Public IP	If the Digi TransPort's WAN interface is NOT public (and IPsec traffic is forwarded to it from a public IP address) enter the public IP address here.
*Local subnet mask to negotiate (if different from above):	255.255.255.255	If the Digi TransPort's WAN interface is NOT public (and IPsec traffic is forwarded to it from a public IP address) enter 255.255.255.255 here.

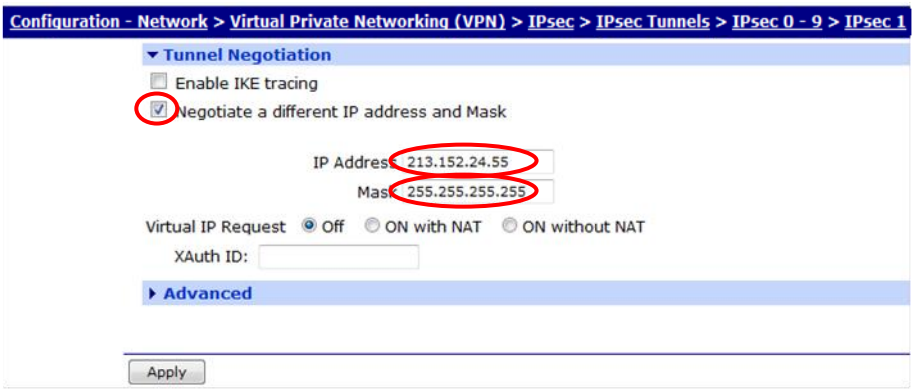
2.6.1 Additional step if this DR64 is not directly connected to the internet

If the DR64 is not directly attached to the internet, ie, it is behind a NAT router or firewall then this extra step is required. If the router is attached directly to the internet skip this step.

Browse to:

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0 - 9 > IPsec 1 > Tunnel Negotiation

Configure the negotiation settings as shown:



Parameter	Setting	Description
Negotiate a different IP address and Mask	checked	Enables negotiation of an alternative WAN interface address
IP Address	<Public IP address>	If the Digi TransPort's WAN interface is NOT public (and IPsec traffic is forwarded to it from a public IP address) enter the public IP address here.
Mask	255.255.255.255	If the Digi TransPort's WAN interface is NOT public (and IPsec traffic is forwarded to it from a public IP address) enter 255.255.255.255 here.

2.7 Configure DR64's L2TP settings for multiple sessions.

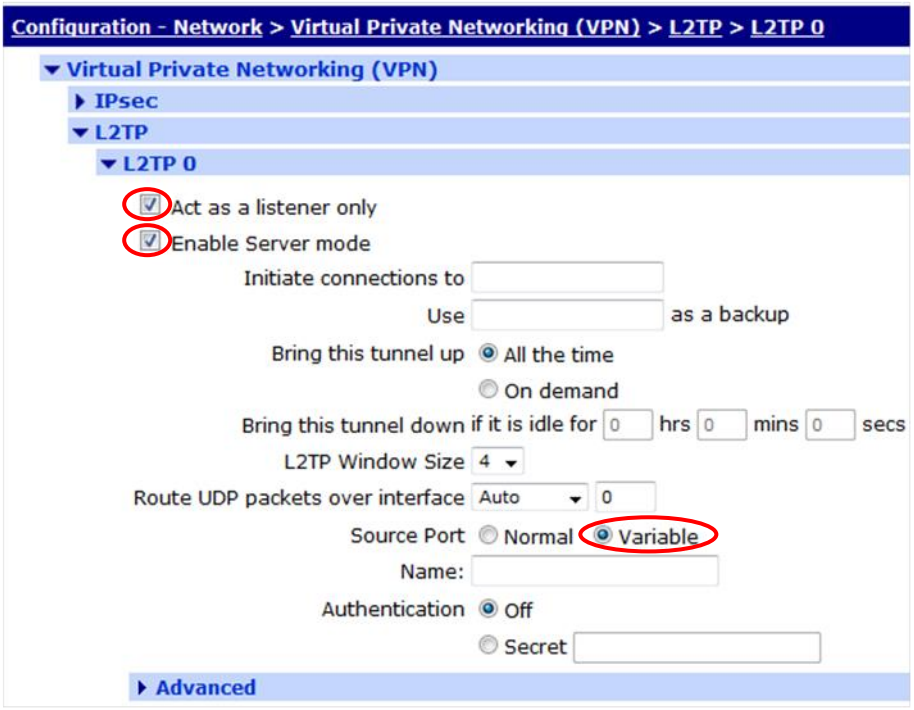
L2TP (Layer 2 Tunneling Protocol) will provide a tunnel through which a logical PPP connection can be established. When the Digi TransPort is configured to be an L2TP Server, the router listens on UDP port 1701 and terminates L2TP connections. It then only allows PPP frames to be passed in the L2TP "tunnel" between the Digi TransPort router and the remote device. As there is a need for multiple L2TP sessions, multiple L2TP instances will need to be created. In this Application Note L2TP instances 0 to 4 will be configured.

2.7.1 Configure L2TP 0

Using the Digi TransPort's web interface navigate to

Configuration - Network > Virtual Private Networking (VPN) > L2TP > L2TP 0

and enter the L2TP settings shown below.



Parameter	Setting	Description
Act as a listener only	checked	Sets L2TP 0 to Listen on UDP port 1701 (L2TP)
Enable Server mode	checked	Sets L2TP 0 to be a L2TP Server, not initiator.
Source Port	Variable	The remote devices will use variable source ports

2.7.2 Configure L2TP 1 - 4

Now continue configuring the L2TP instances 1 through to 4 with exactly the same settings as L2TP 0.

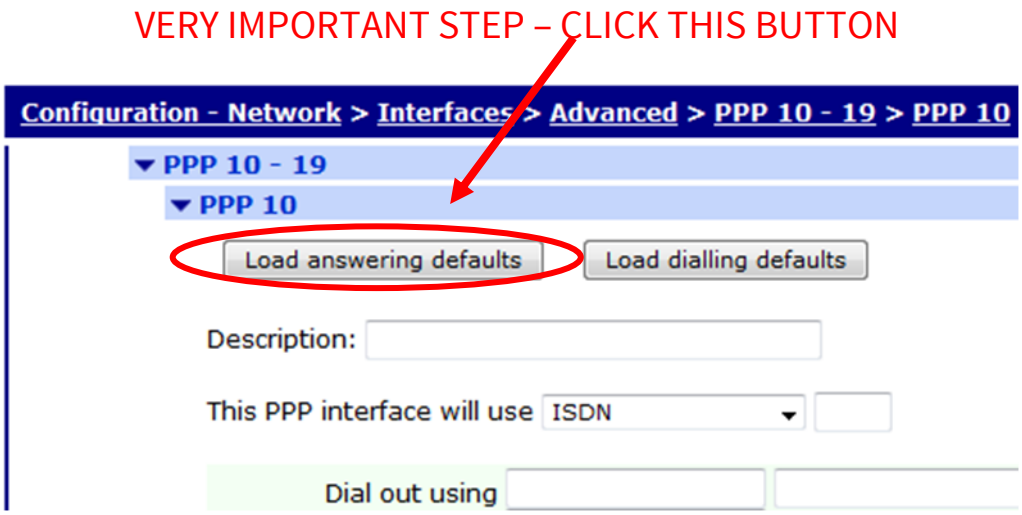
2.8 Configure DR64's PPP Settings.

PPP frames passed up from the L2TP layer will be terminated by a PPP instance. Again as there is a need for multiple PPP sessions, multiple PPP instances will need to be configured. In this Application Note PPP instances 10 to 13 will be configured.

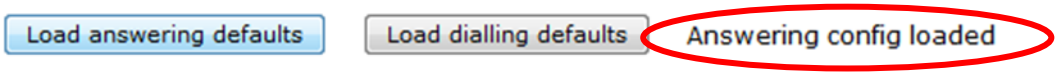
Using the Digi TransPort's web interface navigate to

Configuration - Network > Interfaces > Advanced > PPP 10 - 19 > PPP 10

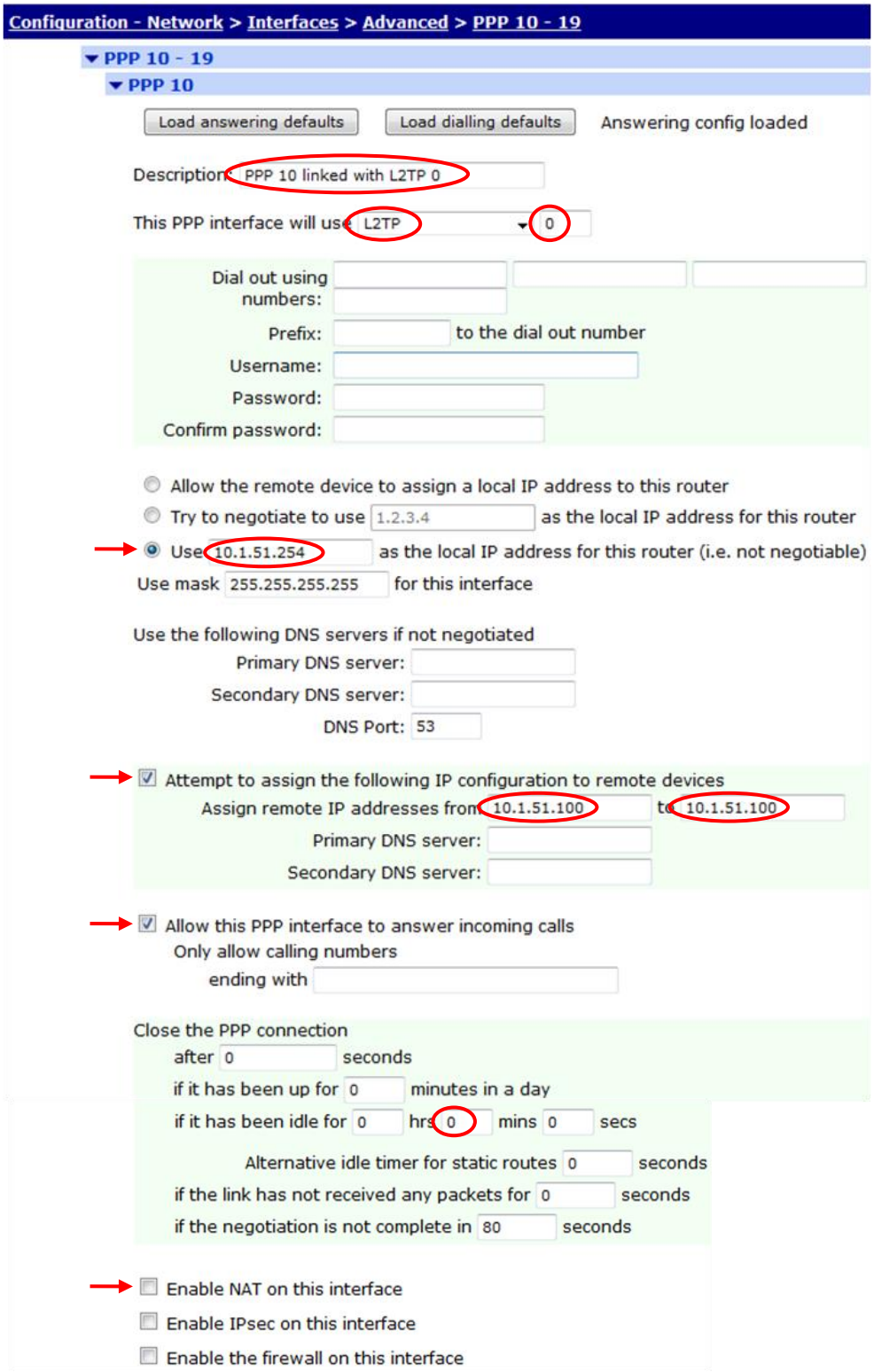
IMPORTANT Step: Click the 'Load answering defaults' button and then use the following steps to enter the remaining PPP settings.



Once the answering defaults have been loaded, a confirmation is shown:



Stay on the same page and configure with the settings detailed below.



Parameter	Setting	Description
Description	PPP 10 linked with L2TP 0	Friendly name
This PPP interface will use	L2TP 0	Specifies the lower layer this PPP will use
Use <ipaddr> as the local IP address for this router (i.e. not negotiable)	*10.1.51.254*	Will use this address as Local IP address
Attempt to assign the	checked	Enables IPCP to assign an IP address to the

following IP configuration to remote devices		remote device
Assign remote IP addresses from <ipaddr> to <ipaddr>	From *10.1.51.100* to *10.1.51.100*	Address to be assigned by PPP running over L2TP. Only 1 IP address in the pool
Allow this PPP interface to answer incoming calls	Checked	Will answer PPP calls on this interface
Close the PPP connection: if it has been idle for	0 hrs 0 mins 0 secs	PPP 10 will never close due to inactivity
Enable NAT on this interface	Not checked	No NAT or NAPT Translation

The above settings shown in *italics* are user dependant. See note below for details.

*** Note:** The "Assign remote IP addresses from <ipaddr> to <ipaddr>" setting specifies the IP address pool that will be used to assign addresses to the remote client for each PPP instance.

This address **can** if required (not must) be an address in the LAN subnet. The address **must not** be in use by another host on the same subnet as the DR64's LAN. If an address on the LAN subnet is specified, the Digi TransPort will use proxy ARP and so no routing changes will be required to any hosts on the LAN.

This IP address should therefore be **different for each PPP** instance that you configure. In this example an IP address on the same subnet as the private LAN has been chosen. You must ensure that no other hosts on the private LAN use this address.

It is perfectly acceptable to assign IP addresses to the remote clients that are in a different subnet to that of the private LAN. However if you choose to do this, hosts on the private LAN will need to use the Digi TransPort as the gateway for this subnet.

If you do choose to assign an IP address to the remote client that is on the same subnet as the Digi TransPort's local LAN, then you can choose whether broadcast packets should be routed to the remote unit by enabling the advanced PPP parameter "Forward IP broadcasts over this interface if this interface is on the same IP network as an Ethernet interface". The default and recommended value is to have this feature disabled.

The advantage of forwarding broadcasts is that software features that make use of broadcast packets and/or NETBIOS hostname to IP look up should work. The disadvantage is that an excessively large amount of traffic could be sent over the VPN tunnel thus rendering it expensive and/or slow.

2.9 Continue and configure PPP instances 11 – 13

Each answering PPP instance needs to be associated with a **different** answering L2TP instance and have a **different** IP address pool configured.

Use the tables of parameters below to configure the next 3 PPP interfaces.

Using the Digi TransPort's web interface navigate to

Configuration - Network > Interfaces > Advanced > PPP 10 - 19 > PPP 11

Parameter	Setting	Description
Description	PPP **11** linked with L2TP **1**	Friendly name
This PPP interface will use	L2TP **1**	Specifies the lower layer this PPP will use
Use <ipaddr> as the local IP address for this router (i.e. not negotiable)	*10.1.51.254*	Will use this address as Local IP address
Attempt to assign the following IP configuration to remote devices	checked	Enables IPCP to assign an IP address to the remote device
Assign remote IP addresses from <ipaddr> to <ipaddr>	From *10.1.51.10**1*** to *10.1.51.10**1***	Address to be assigned by PPP running over L2TP. Only 1 IP address in the pool
Allow this PPP interface to answer incoming calls	Checked	Will answer PPP calls on this interface
Close the PPP connection: if it has been idle for	0 hrs 0 mins 0 secs	PPP 10 will never close due to inactivity
Enable NAT on this interface	Not checked	No NAT or NAPT Translation

Using the Digi TransPort's web interface navigate to

Configuration - Network > Interfaces > Advanced > PPP 10 - 19 > PPP 12

Parameter	Setting	Description
Description	PPP **12** linked with L2TP **2**	Friendly name
This PPP interface will use	L2TP **2**	Specifies the lower layer this PPP will use
Use <ipaddr> as the local IP address for this router (i.e. not negotiable)	*10.1.51.254*	Will use this address as Local IP address
Attempt to assign the following IP configuration to remote devices	checked	Enables IPCP to assign an IP address to the remote device
Assign remote IP addresses from <ipaddr> to <ipaddr>	From *10.1.51.10**2*** to *10.1.51.10**2***	Address to be assigned by PPP running over L2TP. Only 1 IP address in the pool
Allow this PPP interface to answer incoming calls	Checked	Will answer PPP calls on this interface
Close the PPP connection: if it has been idle for	0 hrs 0 mins 0 secs	PPP 10 will never close due to inactivity
Enable NAT on this interface	Not checked	No NAT or NAPT Translation

Using the Digi TransPort's web interface navigate to

Configuration - Network > Interfaces > Advanced > PPP 10 - 19 > PPP 13

Parameter	Setting	Description
Description	PPP **13** linked with L2TP **3**	Friendly name
This PPP interface will use	L2TP **3**	Specifies the lower layer this PPP will use
Use <ipaddr> as the local IP address for this router (i.e. not negotiable)	*10.1.51.254*	Will use this address as Local IP address
Attempt to assign the following IP configuration to remote devices	checked	Enables IPCP to assign an IP address to the remote device
Assign remote IP addresses from <ipaddr> to <ipaddr>	From *10.1.51.10**3*** to *10.1.51.10**3***	Address to be assigned by PPP running over L2TP. Only 1 IP address in the pool
Allow this PPP interface to answer incoming calls	Checked	Will answer PPP calls on this interface
Close the PPP connection: if it has been idle for	0 hrs 0 mins 0 secs	PPP 10 will never close due to inactivity
Enable NAT on this interface	Not checked	No NAT or NAPT Translation

2.10 Configure DR64's User Table – IPsec Preshared Key

The **last** user instance will need to be configured with the IPSec Pre-Shared Key.

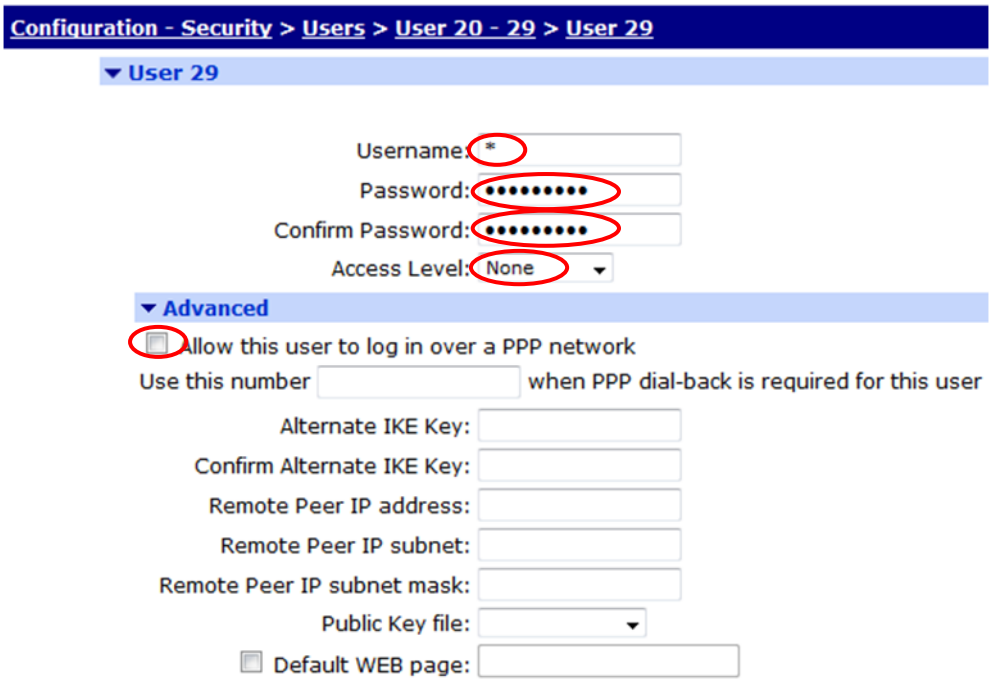
Using the Digi TransPort's web interface navigate to

Configuration - Security > Users > User n - n > User <last user instance>

Enter the username as * (the asterisk symbol) this is a wildcard and will match against all remote site IDs. Set and confirm the Pre-Shared Key in the password fields. Make sure this is a strong password.

The 'access level' specifies the router management access level, so set this to none.

As this user is being used for an IPsec Preshared Key, PPP logins should be disabled for this user. Other PPP users will be configured later for VPN logins.



Parameter	Setting	Description
Username:	*	Wild card to allow any Remote VPN client access
Password	*shared_secret_key*	Pre-Shared Key Remote VPN Client will use
Confirm Password	*shared_secret_key*	Pre-Shared Key Remote VPN Client will use
Access Level	None	Users knowing this password will not be allowed to log on to the router to administer it.
Allow this user to log in over a PPP network	Un-checked	This username & password cannot be used as a VPN username & password.

2.11 Configure DR64's User Table – VPN Users

Each VPN user should have their own username and password so it is possible to track users in the event log and remove logins when a user no longer needs VPN access.

In this example, 4 VPN users will be configured; Tom, Richard, Harry, Dave.

The **first** free (un-configured) user instance will be configured for the VPN user Tom.

Using the Digi TransPort's web interface navigate to

Configuration - Security > Users > User 0 - 9 > User 2

On your DR64, pick the first available free user if User 2 is already in use.

Set the username as the name of the VPN user.

Set and confirm this user's VPN password.

If this user needs router management access, then give the appropriate level of access, otherwise set this to None.

Parameter	Setting	Description
Username:	tom	VPN username
Password	*User-password*	VPN password
Confirm Password	*User-password*	VPN password
Access Level	None	Router management access level

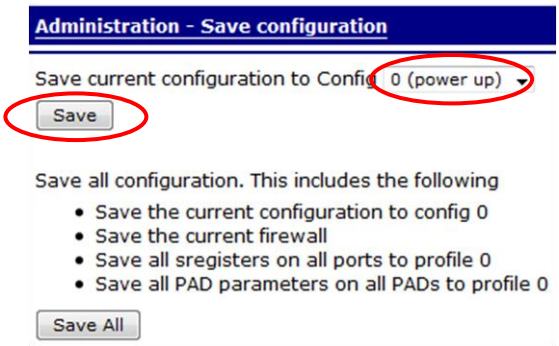
Repeat the process for users Richard, Harry & Dave by configuring the next 3 free user instances.

2.12 Save the DR64's configuration

Navigate to

Administration - Save configuration

Select the configuration to save as '0 (power up)', then click Save.



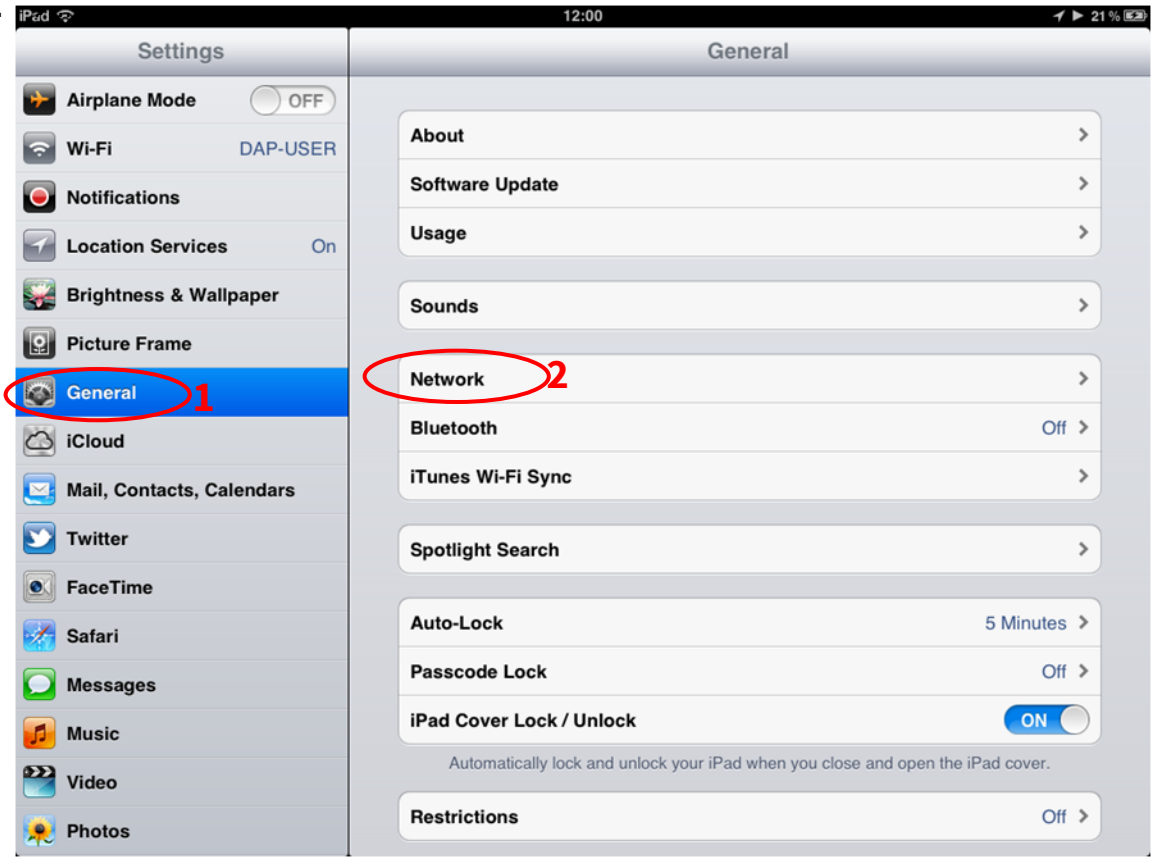
2.13 Configure VPN Client - Apple iOS (iPad2 – iOS 5.1.1)

L2TP will run over an IPSec connection between the iPad and the Digi TransPort, this in turn will run over the iPad's existing internet connection. The iPad's internet connection can be cellular or via Wi-Fi.

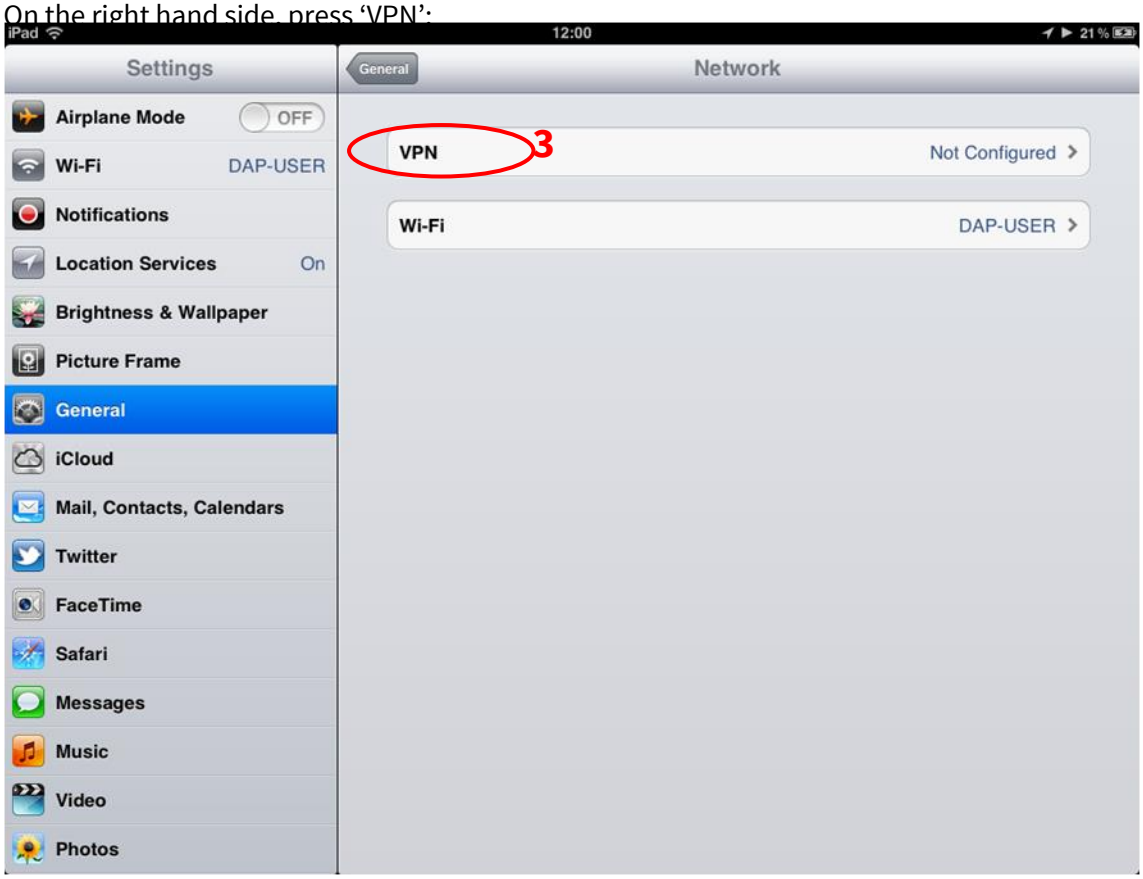
As there is a need for multiple L2TP sessions from multiple remote devices, this procedure will need to be replicated on as many remote iPads as needed.

On the iPad (or other Apple iOS device) navigate to:

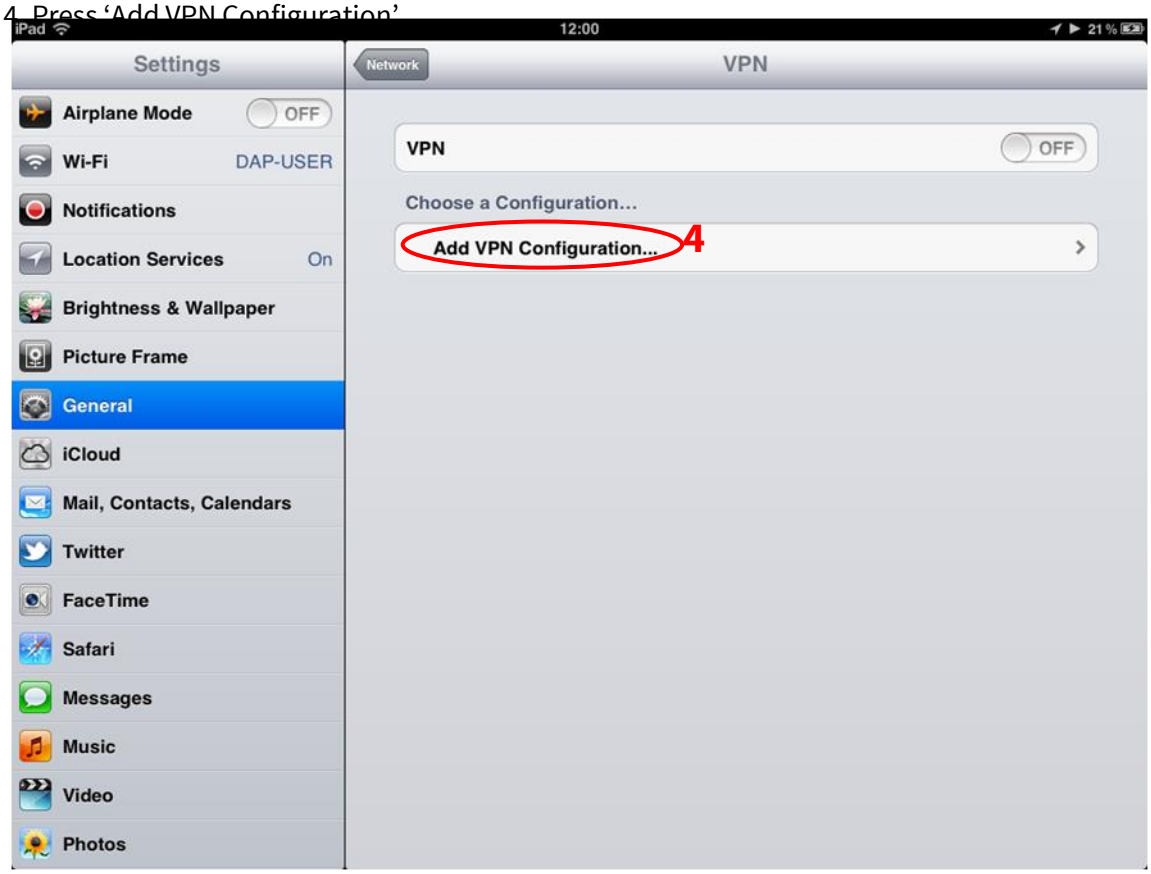
1. Settings > General



3. On the right hand side, press 'VPN':

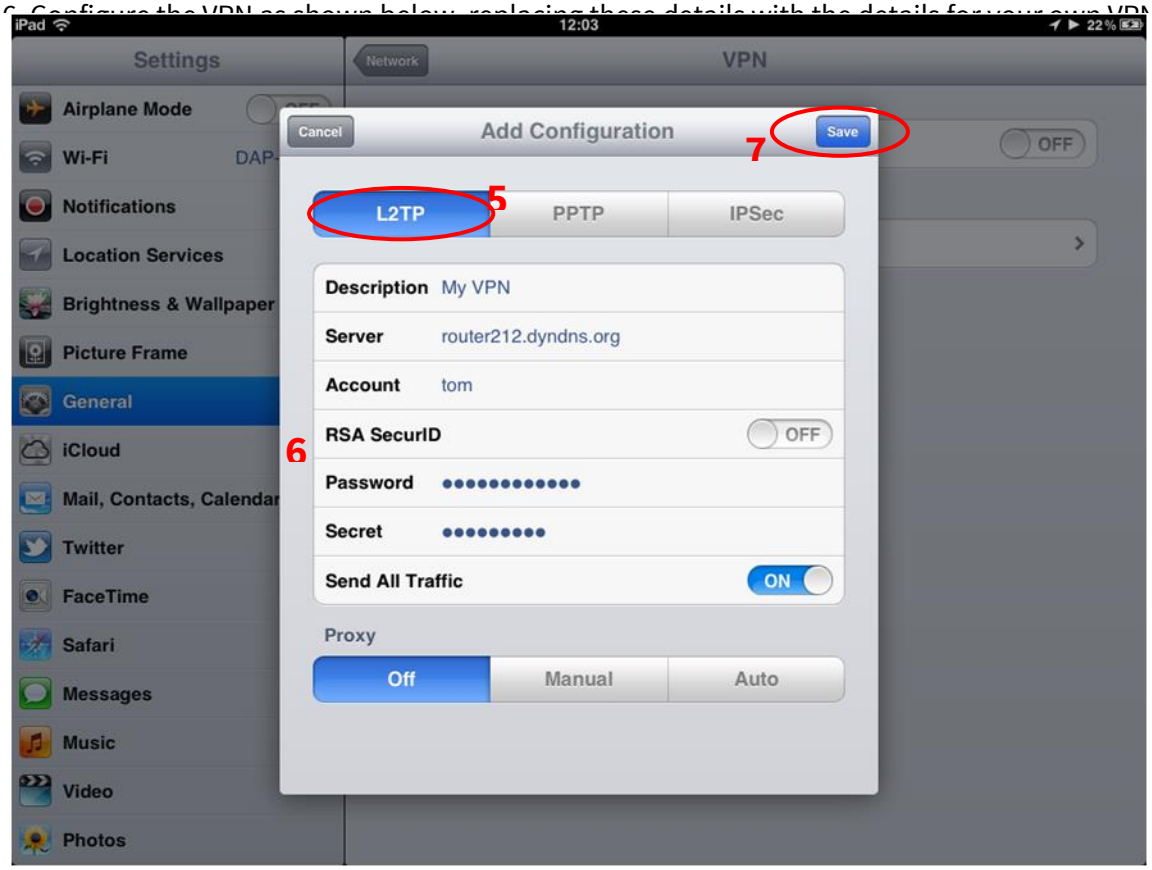


4. Press 'Add VPN Configuration'



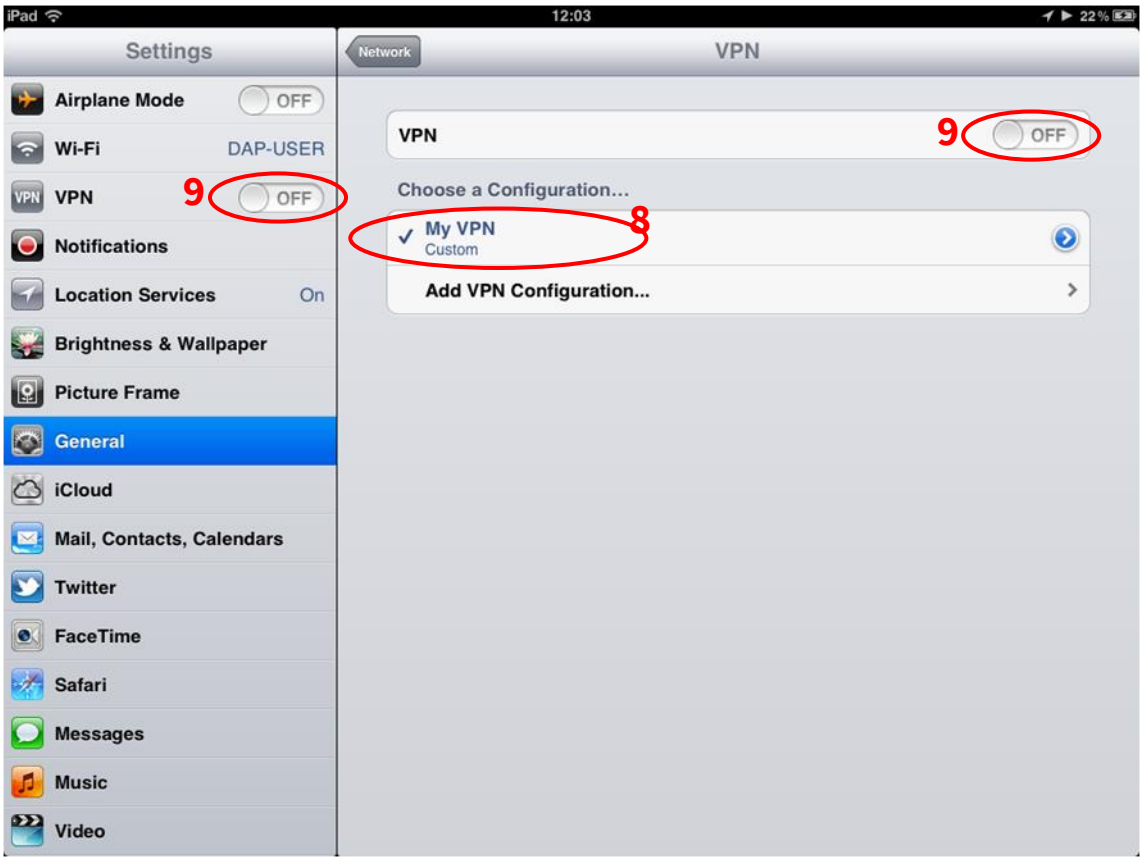
5. The VPN configuration screen is displayed. Select 'L2TP' from the VPN types, this is L2TP over IPsec. The option for 'IPsec' is for Cisco EasyVPN configurations.

6. Configure the VPN as shown below, replacing these details with the details for your own VPN

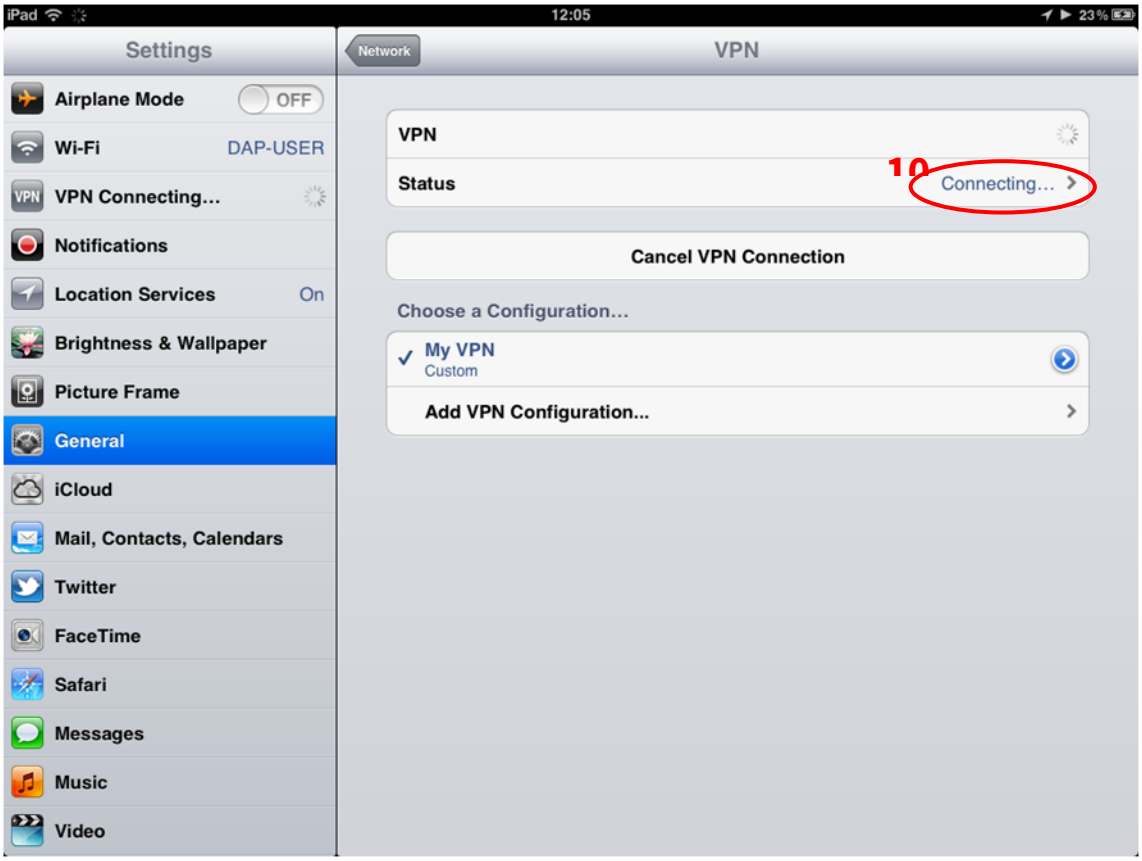


Parameter	Setting	Description
L2TP	Selected	This configuration is for L2TP over IPsec VPN
Description	*My VPN*	Friendly name for this VPN
Server	*DR64 WAN IP address or FQDN*	The public IP address or DNS name of the DR64 router
Account	tom	The username of the VPN user See step 2.11
RSA SecurID	OFF	Not used
Password	<password>	The password of the VPM user See step 2.11
Secret	<ipsec_psk>	The IPsec Pre-Shared Key See step 2.10
Send All Traffic	ON	Ensures ALL traffic is transmitted securely via the VPN
Proxy	Off	Not used

8. After pressing Save, the previous screen is shown again, but now with ‘My VPN’ shown.

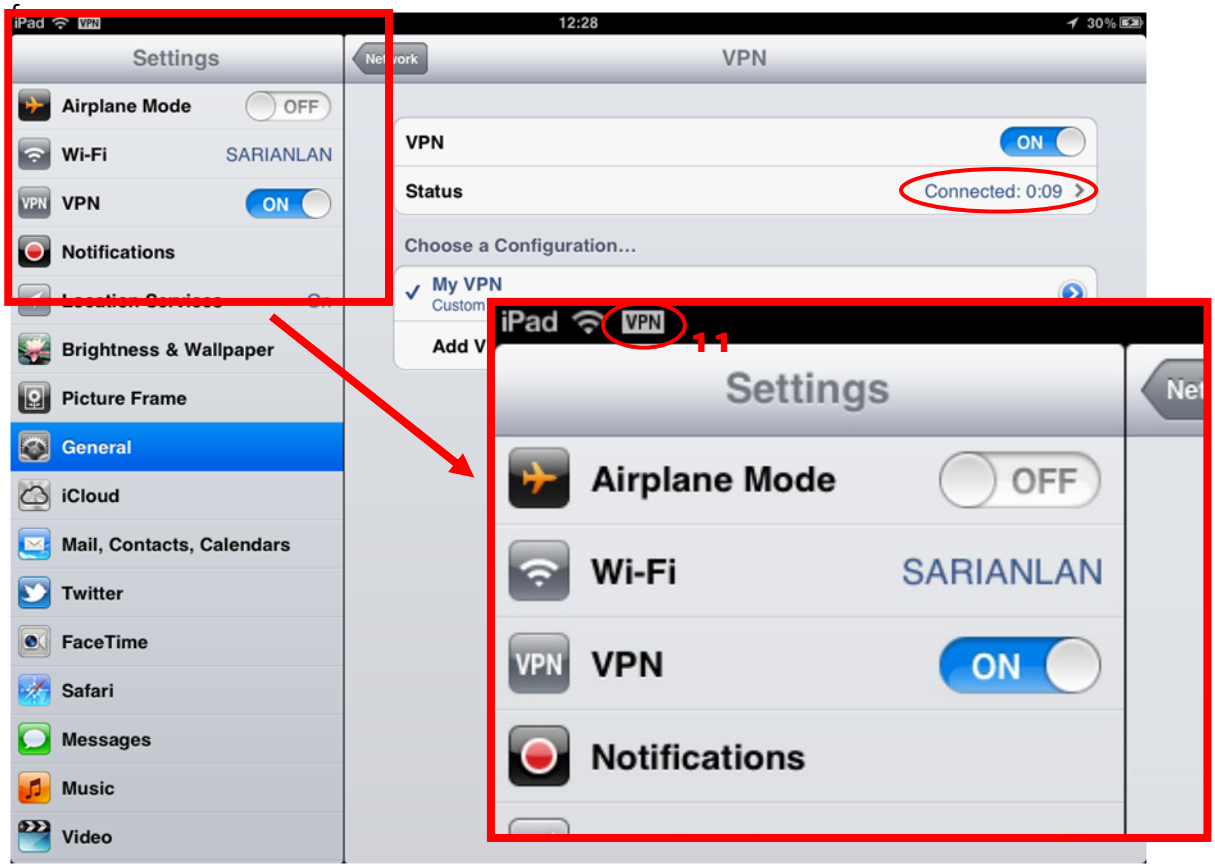


10. The screen will change and show the VPN status as ‘Connecting...’



11. When the VPN has successfully connected, a 'VPN' notification will show in the notification area.

The 'Status' bar will show 'Connected' and a timer to show how long the VPN has been connected



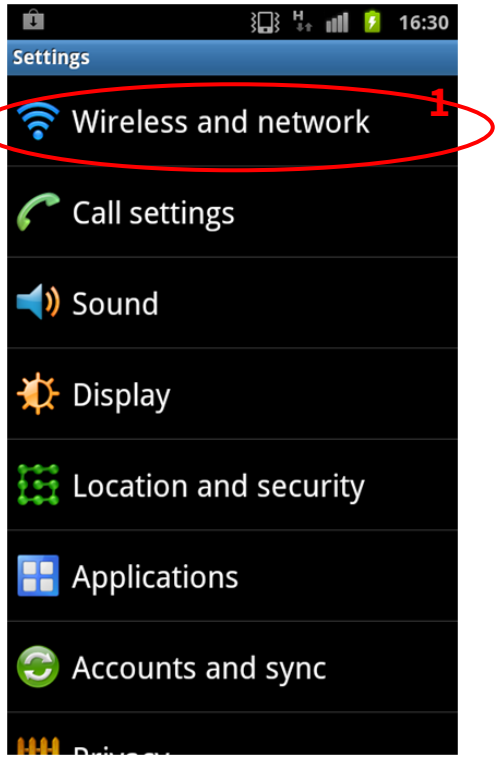
12. To close the VPN, move one of the VPN sliders shown in Step 9 to OFF. The 'VPN' notification will be removed from top notification area when the VPN disconnects.

2.14 Configure VPN Client - Android (Samsung Galaxy S - Gingerbread)

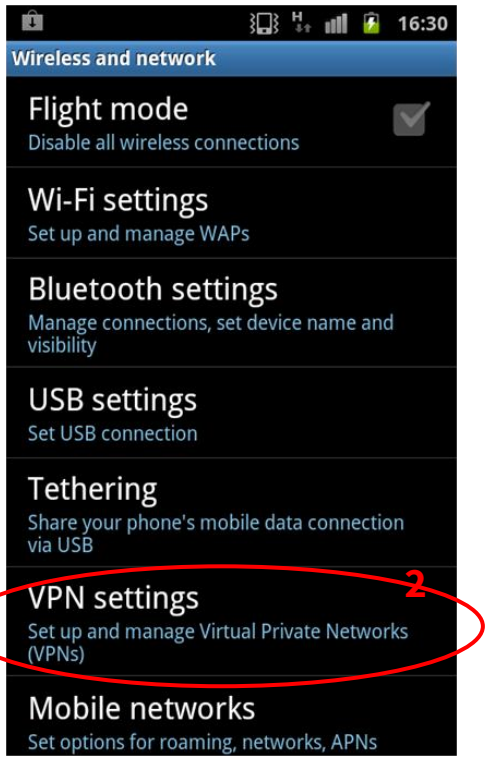
L2TP will run over an IPSec connection between the Android mobile and the Digi TransPort, this in turn will run over the devices existing internet connection. The internet connection can be cellular or via Wi-Fi.

As there is a need for multiple L2TP sessions from multiple remote devices, this procedure will need to be replicated on as many remote Android devices as needed.

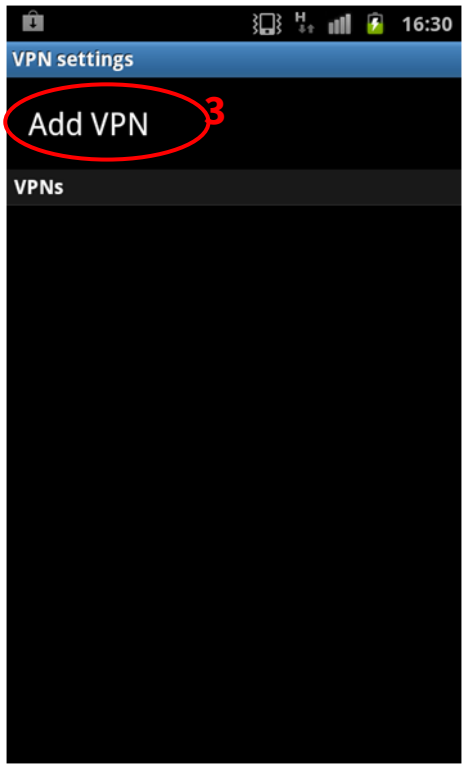
1. On the Android device navigate to the



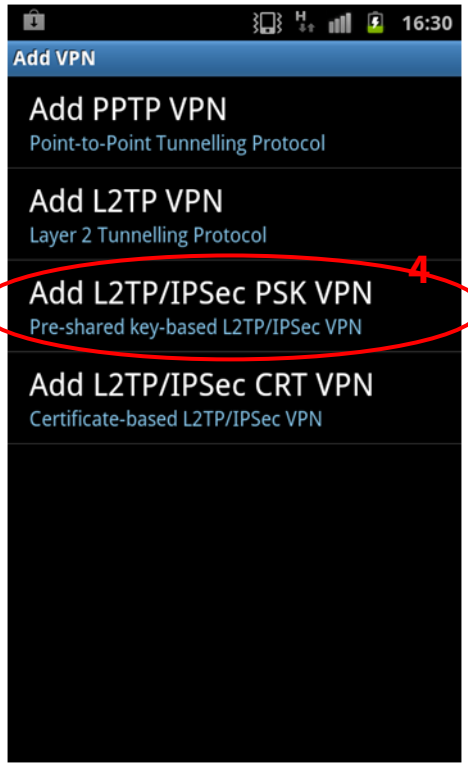
2. Press ‘VPN settings’



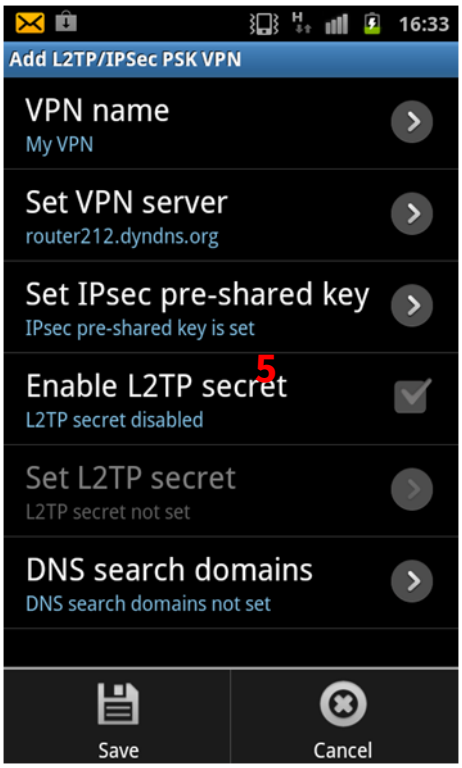
3. Press ‘Add VPN’.



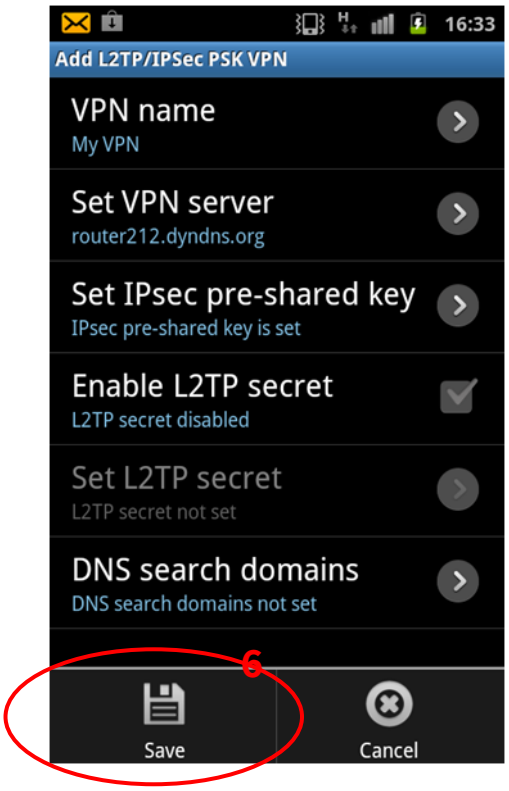
4. When the VPN options are shown, press



5. When the VPN settings screen appears, fill in

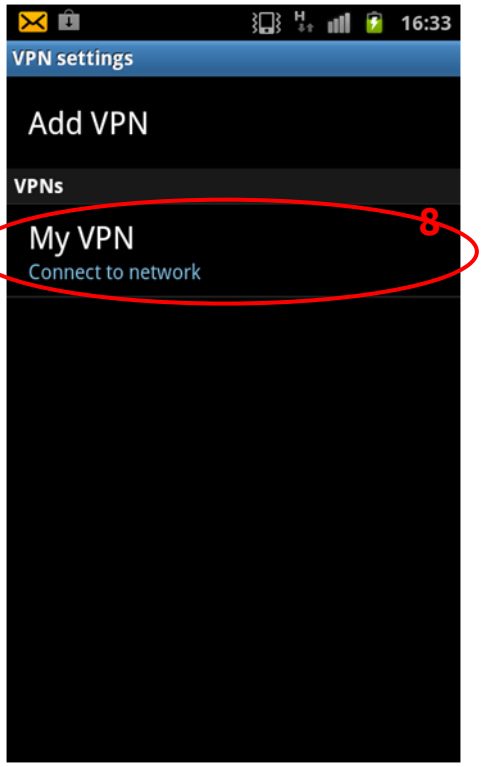


6. When the VPN settings are complete, press



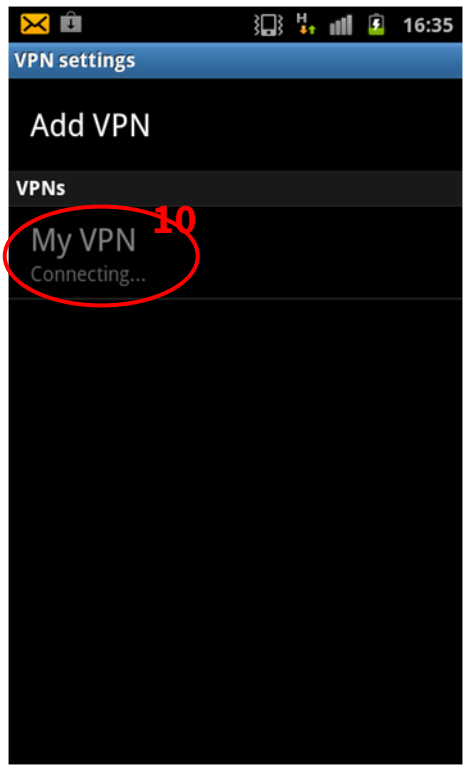
7. Enter the password for credential storage

8. The VPN is now saved. To initiate the VPN,

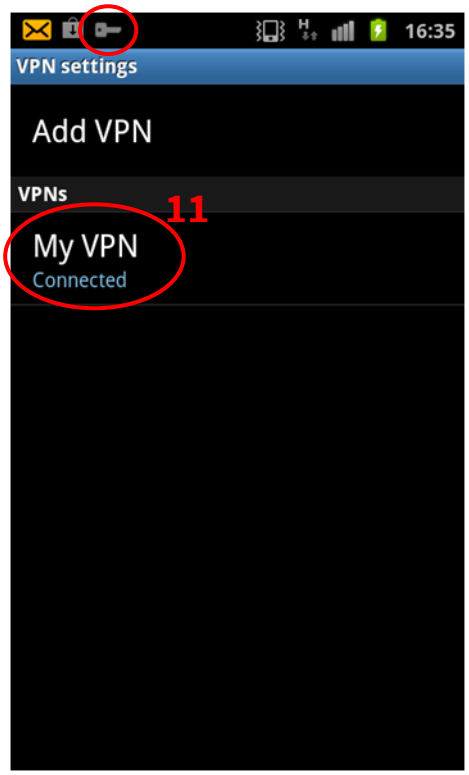


9. A prompt will appear requesting the VPN username and password. Fill in the details and press 'Connect'. This is the user configured in

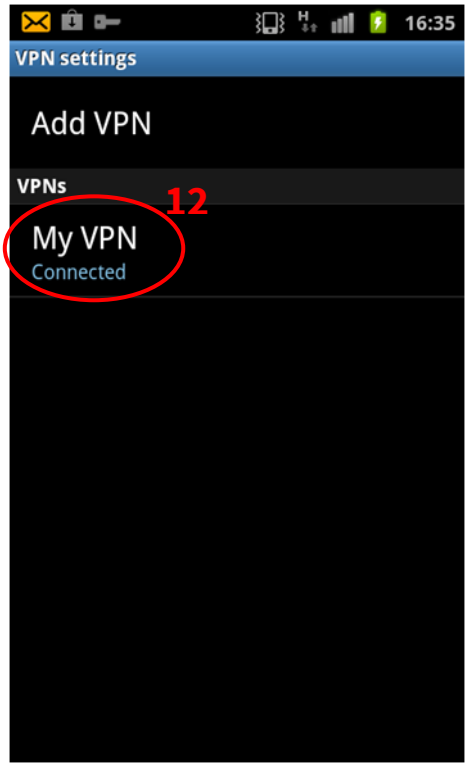
10. The VPN connection progress is shown



11. When the VPN connects, the status changes to 'Connected' and a key symbol appears in



12. To disconnect the VPN, press 'My VPN'



Parameters relating to step 5:

Parameter	Setting	Description
VPN name	*My VPN*	Friendly name for this VPN
Set VPN server	*DR64 WAN IP address or FQDN*	The public IP address or DNS name of the DR64 router
Set IPsec pre-shared key	<ipsec_psk>	The IPsec Pre-Shared Key See step 2.10
Enable L2TP secret	Un-checked	Not used
DNS search domains	Not set	Not used

3 TESTING

3.1 Events and status pages

This test stage will show that the IPSec/L2TP tunnel has been established.

When a remote device (tablet or smart phone) tries to establish a L2TP tunnel to the VPN Server an IPSec Security Association is established first, this allows the L2TP packets to be encrypted within the IPSec Tunnel.

On the DR64 VPN Server's Web GUI navigate to **Management - Event Log** and click on 'Clear Log'

Using one of the VPN configured devices (Apple or Android) initiate a VPN to the DR64 VPN server. After some brief negotiations the device's VPN client shall receive an IP address, via PPP, from the VPN Server.

On the **Management - Event Log** page click the 'Refresh' button to update the event log.

Each stage of the L2TP establishment will have been entered in the eventlog.

Read the event log from bottom to top (newest items at the top)

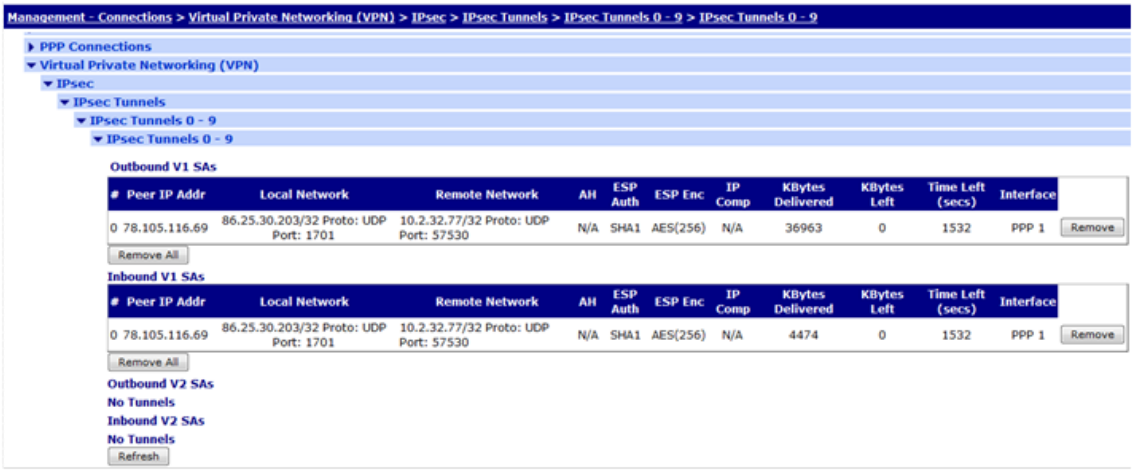
```
Highest PPP instance answers packets passed up from L2TP layer

08:42:00, 27 Jul 2012,PPP 13 up
08:41:59, 27 Jul 2012,PPP 13 Start IPCP
08:41:59, 27 Jul 2012,PPP Login OK by tom lvl 4
08:41:59, 27 Jul 2012,PPP 13 Start AUTHENTICATE
08:41:59, 27 Jul 2012,PPP 13 Start LCP
08:41:59, 27 Jul 2012,PPP 13 Start

L2TP Answering L2TP packets encrypted in IPSec tunnel

08:41:59, 27 Jul 2012,L2TP Call 3 up
```

```
08:41:59, 27 Jul 2012,L2TP Tunnel 0 up

IPSec SA up

08:41:59, 27 Jul 2012,(2) IKE SA Removed. Peer: 10.2.32.77,Successful Negotiation
08:41:59, 27 Jul 2012,Eroute 0 VPN up peer: 10.2.32.77
08:41:59, 27 Jul 2012,New IPSec SA created by 10.2.32.77
08:41:59, 27 Jul 2012,(2) New Phase 2 IKE Session 78.105.116.69,Responder

IKE SA up

08:41:58, 27 Jul 2012,(1) IKE Keys Negotiated. Peer:
08:41:58, 27 Jul 2012,(1) New Phase 1 IKE Session 78.105.116.69,Responder
```

Navigate to

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

This page will show the status of the newly established IPSec tunnel.

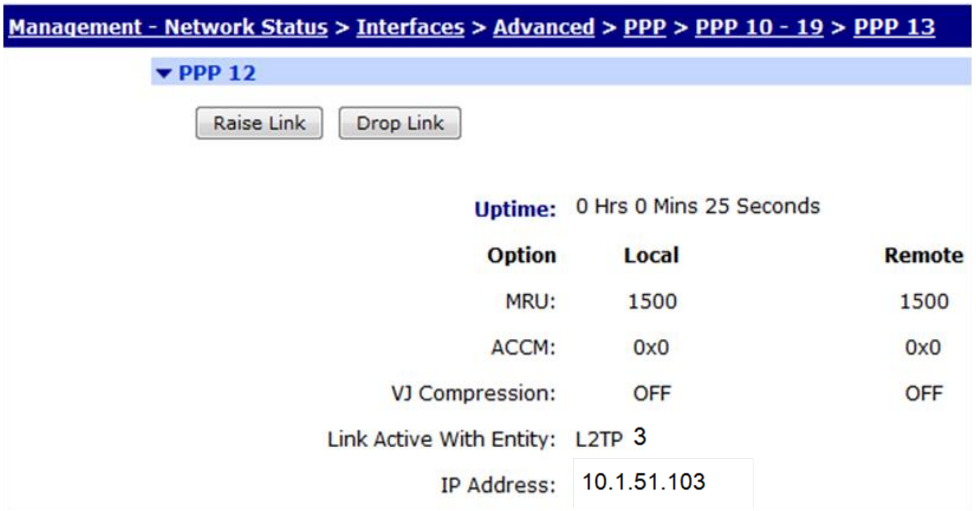


The Digi TransPort is designed to allow the highest numbered PPP instance to answer an incoming PPP call first.

Navigate to

Diagnostics - Status > PPP > PPP 10 - 14 > PPP 13 > View.

This will show the local IP address that the PPP instance is using and the L2TP instance that is associated with this PPP call.



The remote client will now have an IPsec secured L2TP tunnel running PPP to the VPN Server.

4 CONFIGURATION FILES

4.1 Digi TransPort Configuration Files

This is the configuration file from DR64:

```
eth 0 IPaddr "10.1.51.254"
eth 0 mask "255.255.0.0"

l2tp 0 listen ON
l2tp 0 swap_io ON
l2tp 0 rnd_srcport ON
l2tp 1 listen ON
l2tp 1 swap_io ON
l2tp 1 rnd_srcport ON
l2tp 2 listen ON
l2tp 2 swap_io ON
l2tp 2 rnd_srcport ON
l2tp 3 listen ON
l2tp 3 swap_io ON
l2tp 3 rnd_srcport ON

def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
def_route 1 ll_ent "PPP"
def_route 1 ll_add 3

eroute 0 descr "iPad L2TP / IPsec"
eroute 0 peerid "*"
eroute 0 locipifent "PPP"
eroute 0 locipifadd 1
eroute 0 remnetid "*"
eroute 0 mode "Transport"
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "AES"
eroute 0 proto "UDP"
eroute 0 locport 1701
eroute 0 ltime 3600
eroute 0 authmeth "PRESHARED"
eroute 0 enckeybits 256
```

```
eroute 1 descr "Android L2TP / IPsec"
eroute 1 peerid "*"
eroute 1 locipifent "PPP"
eroute 1 locipifadd 1
eroute 1 remnetid "*"
eroute 1 mode "Transport"
eroute 1 ESPauth "SHA1"
eroute 1 ESPenc "3DES"
eroute 1 proto "UDP"
eroute 1 locport 1701
eroute 1 ltime 3600
eroute 1 authmeth "PRESHARED"
eroute 1 enckeybits 128

def_eroute 0 nosain "PASS"
def_eroute 0 nosaout "PASS"

ppp 0 timeout 300
ppp 1 IPaddr "0.0.0.0"
ppp 1 username "user@isp.com"
ppp 1 password "password"
ppp 1 timeout 0
ppp 1 aodion 1
ppp 1 immoos ON
ppp 1 autoassert 1
ppp 1 ipsec 1
ppp 1 echo 10
ppp 1 echodropcnt 5
ppp 1 l1iface "AAL"

ppp 3 defpak 16
ppp 4 defpak 16
ppp 5 defpak 16
ppp 6 defpak 16
ppp 7 defpak 16
ppp 8 defpak 16
ppp 9 defpak 16

ppp 10 descr "PPP 10 linked with L2TP 0"
ppp 10 l1iface "l2tp"
ppp 10 r_addr ON
ppp 10 IPaddr "10.1.51.254"
ppp 10 mask "255.255.255.255"
ppp 10 DNSport 53
ppp 10 IPmin "10.1.51.100"
ppp 10 IPrange 1
ppp 10 ans ON
ppp 10 timeout 0
ppp 10 metric 1
ppp 10 netip "0.0.0.0"
ppp 10 ripauth 1
ppp 10 inrip ON
ppp 10 maxneg 80
ppp 10 l_accm "0x00000000"
ppp 10 r_accm "0xffffffff"
ppp 10 l_mru 1500
ppp 10 r_mru 1500
ppp 10 l_acfc ON
ppp 10 l_pap ON
ppp 10 l_chap ON
ppp 10 l_comp ON
ppp 10 l_pfc ON
```

```
ppp 10 r_callb 1
ppp 10 l_md5 1
ppp 10 r_md5 ON
ppp 10 r_ms1 ON
ppp 10 r_ms2 ON
ppp 10 lcn 1027
ppp 10 defpak 128
ppp 10 baklcn 1027

ppp 11 descr "PPP 11 linked with L2TP 1"
ppp 11 l1iface "l2tp"
ppp 11 l1nb 1
ppp 11 r_addr ON
ppp 11 IPaddr "10.1.51.254"
ppp 11 mask "255.255.255.255"
ppp 11 DNSport 53
ppp 11 IPmin "10.1.51.101"
ppp 11 IPrange 1
ppp 11 ans ON
ppp 11 timeout 0
ppp 11 metric 1
ppp 11 netip "0.0.0.0"
ppp 11 ripauth 1
ppp 11 inrip ON
ppp 11 maxneg 80
ppp 11 l_accm "0x00000000"
ppp 11 r_accm "0xffffffff"
ppp 11 l_mru 1500
ppp 11 r_mru 1500
ppp 11 l_acfc ON
ppp 11 l_pap ON
ppp 11 l_chap ON
ppp 11 l_comp ON
ppp 11 l_pfc ON
ppp 11 r_callb 1
ppp 11 l_md5 1
ppp 11 r_md5 ON
ppp 11 r_ms1 ON
ppp 11 r_ms2 ON
ppp 11 lcn 1127
ppp 11 defpak 128
ppp 11 baklcn 1127

ppp 12 descr "PPP 12 linked with L2TP 2"
ppp 12 l1iface "l2tp"
ppp 12 l1nb 2
ppp 12 r_addr ON
ppp 12 IPaddr "10.1.51.254"
ppp 12 mask "255.255.255.255"
ppp 12 DNSport 53
ppp 12 IPmin "10.1.51.102"
ppp 12 IPrange 1
ppp 12 ans ON
ppp 12 timeout 0
ppp 12 metric 1
ppp 12 netip "0.0.0.0"
ppp 12 ripauth 1
ppp 12 inrip ON
ppp 12 maxneg 80
ppp 12 l_accm "0x00000000"
ppp 12 r_accm "0xffffffff"
ppp 12 l_mru 1500
```

```
ppp 12 r_mru 1500
ppp 12 l_acfc ON
ppp 12 l_pap ON
ppp 12 l_chap ON
ppp 12 l_comp ON
ppp 12 l_pfc ON
ppp 12 r_callb 1
ppp 12 l_md5 1
ppp 12 r_md5 ON
ppp 12 r_ms1 ON
ppp 12 r_ms2 ON
ppp 12 lcn 1227
ppp 12 defpak 128
ppp 12 baklcn 1227

ppp 13 descr "PPP 13 linked with L2TP 3"
ppp 13 l1iface "l2tp"
ppp 13 l1nb 3
ppp 13 r_addr ON
ppp 13 IPaddr "10.1.51.254"
ppp 13 mask "255.255.255.255"
ppp 13 DNSport 53
ppp 13 IPmin "10.1.51.103"
ppp 13 IPrange 1
ppp 13 ans ON
ppp 13 timeout 0
ppp 13 metric 1
ppp 13 netip "0.0.0.0"
ppp 13 ripauth 1
ppp 13 inrip ON
ppp 13 maxneg 80
ppp 13 l_accm "0x00000000"
ppp 13 r_accm "0xffffffff"
ppp 13 l_mru 1500
ppp 13 r_mru 1500
ppp 13 l_acfc ON
ppp 13 l_pap ON
ppp 13 l_chap ON
ppp 13 l_comp ON
ppp 13 l_pfc ON
ppp 13 r_callb 1
ppp 13 l_md5 1
ppp 13 r_md5 ON
ppp 13 r_ms1 ON
ppp 13 r_ms2 ON
ppp 13 lcn 1327
ppp 13 defpak 138
ppp 13 baklcn 1327

ike 0 delmode 1
ike 0 invspidel ON

user 1 name "username"
user 1 password "password"
user 1 access 0
user 2 name "tom"
user 2 password "tom-password"
user 2 access 4
user 3 name "richard"
user 3 password "richard-password"
user 3 access 4
user 4 name "harry"
```

```
user 4 password "harry-password"
user 4 access 4
user 4 name "dave"
user 4 password "dave-password"
user 4 access 4
user 5 access 0
user 6 access 0
user 7 access 0
user 8 access 0
user 9 access 0
user 14 name "*"
user 14 password "presharedkey"
```

4.2 Digi TransPort Firmware Versions

```
Sarian Systems. Sarian DR6410-UIA Mk.II DSL2/2+ Router Ser#:92909 HW Revision: 7502a
Software Build Ver5159.  Jun 26 2012 12:23:12  9W
ARM Sarian Bios Ver 6.74 v35 197MHz B128-M128-F300-O100001,0 MAC:00042d016aed
Power Up Profile: 0
Async Driver              Revision: 1.19  Int clk
Wi-Fi                     Revision: 2.0
Ethernet Hub Driver       Revision: 1.11
ISDN ST 21150 Driver      Revision: 1.7
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
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
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 (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
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
iDigi                   Revision: 2.0
OK
```

4.3 iPad VPN proposal information:

Phase 1 proposal = AES256, SHA1, DH group 2, Lifetime 3600 seconds
Authentication method = Pre-Shared Keys
ID Type used = IPv4 address
Phase 2 proposal = ESP, AES256, SHA1, Lifetime 3600 seconds, Mode: UDP transport,
Local UDP port: Variable, Remote UDP port: 1701

4.4 Android (Gingerbread) VPN proposal information:

Phase 1 proposal = 3DES, SHA1, DH group 2, Lifetime 28800 seconds
Authentication method = Pre-Shared Keys
ID Type used = IPv4 address
Phase 2 proposal = ESP, AES256, SHA1, Lifetime 28800 seconds, Mode: UDP transport,
Local UDP port: Variable, Remote UDP port: 1701