Application Note 37

GRE over IPSEC with a Cisco Router

UK Support

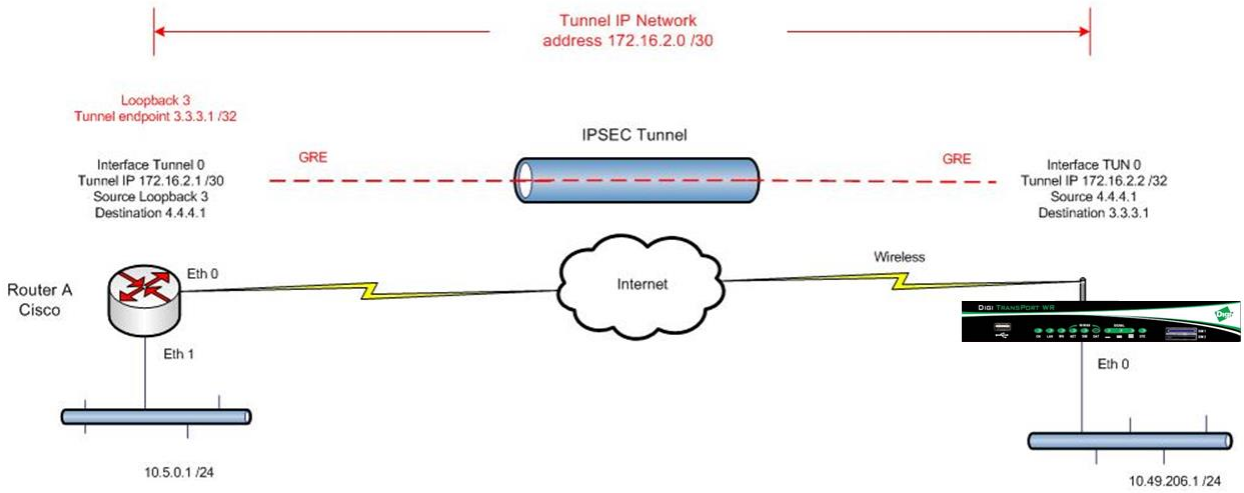
November 2015

Contents

1 INTRODUCTION

1.1 Outline

This document describes how to configure the TransPort router to establish a GRE tunnel connection to a Cisco router with IPSEC encryption. This solution would be used in a situation where a routing protocol such as OSPF is required as the GRE tunnel will be used to route the multicast packets. An IPSec tunnel secures the traffic between the 2 routers.



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).

This application note applies to;

Models shown: Digi Transport WR41

Other Compatible Models: All other Digi Transport products.

Firmware versions: All Versions newer than 5130

Please note: This application note has been specifically rewritten for firmware release 5.123 and later but the original application note was testing and working for routers running earlier firmware and the previous GUI. Routers running earlier firmware will find that the screen shots do not accurately reflect what will be seen on those older routers. Contact uksupport@digi.com if you require this document for the older GUI.

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.

It is assumed in this document that the TransPort router already has a working internet connection.

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
1.1	Re-branded to Digi Transport
1.2	Updated for new GUI

2 CONFIGURATION

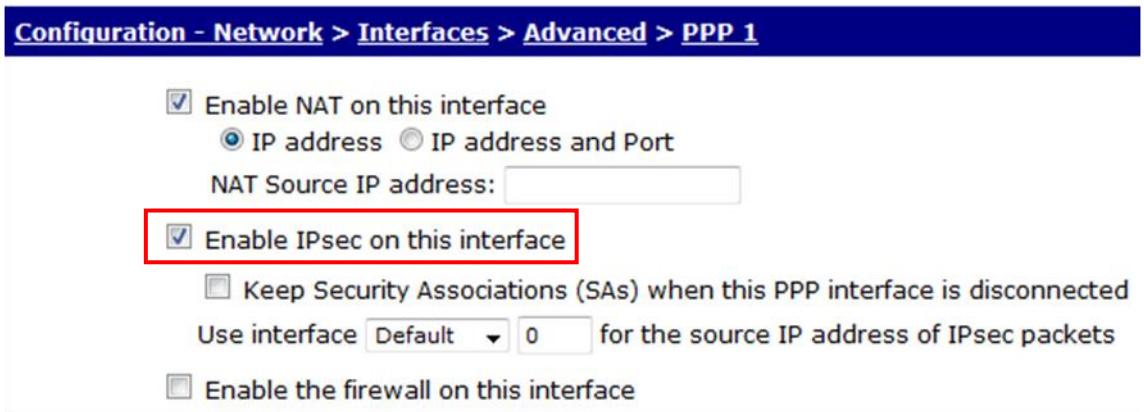
2.1 Configuration of PPP 1

This section will detail the changes needed to be made to PPP 1, it is assumed that the TransPort router has already been configured with a working internet connection on PPP 1.

Navigate to:

Configuration - Network > Interfaces > Advanced > PPP 0 - 9 > PPP 1

Enable IPsec on this interface



Parameter	Setting	Description
Enable IPsec on this interface	Ticked	Enables IPsec

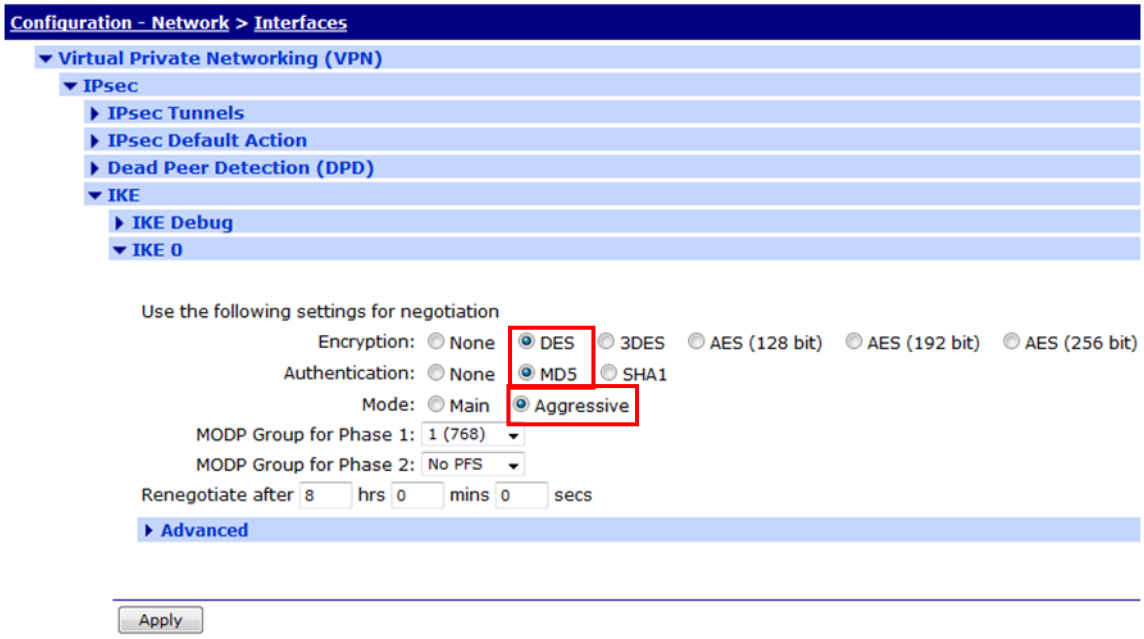
2.2 Configuration of IKE

This section will detail the changes needed to be made to IKE.

These settings are the equivalent of the Cisco Crypto configuration, configure the Cisco accordingly.

Navigate to:

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


Configuration - Network > Interfaces
Virtual Private Networking (VPN)
IPsec
IPsec Tunnels
IPsec Default Action
Dead Peer Detection (DPD)
IKE
IKE Debug
IKE 0
Use the following settings for negotiation
Encryption: None DES 3DES AES (128 bit) AES (192 bit) AES (256 bit)
Authentication: None MD5 SHA1
Mode: Main Aggressive
MODP Group for Phase 1: 1 (768)
MODP Group for Phase 2: No PFS
Renegotiate after 8 hrs 0 mins 0 secs
Advanced
Apply

Parameter	Setting	Description
Encryption	DES	Enables the use of DES encryption
Authentication	MD5	Hash Algorithm to use
Mode	Aggressive	Enables aggressive mode

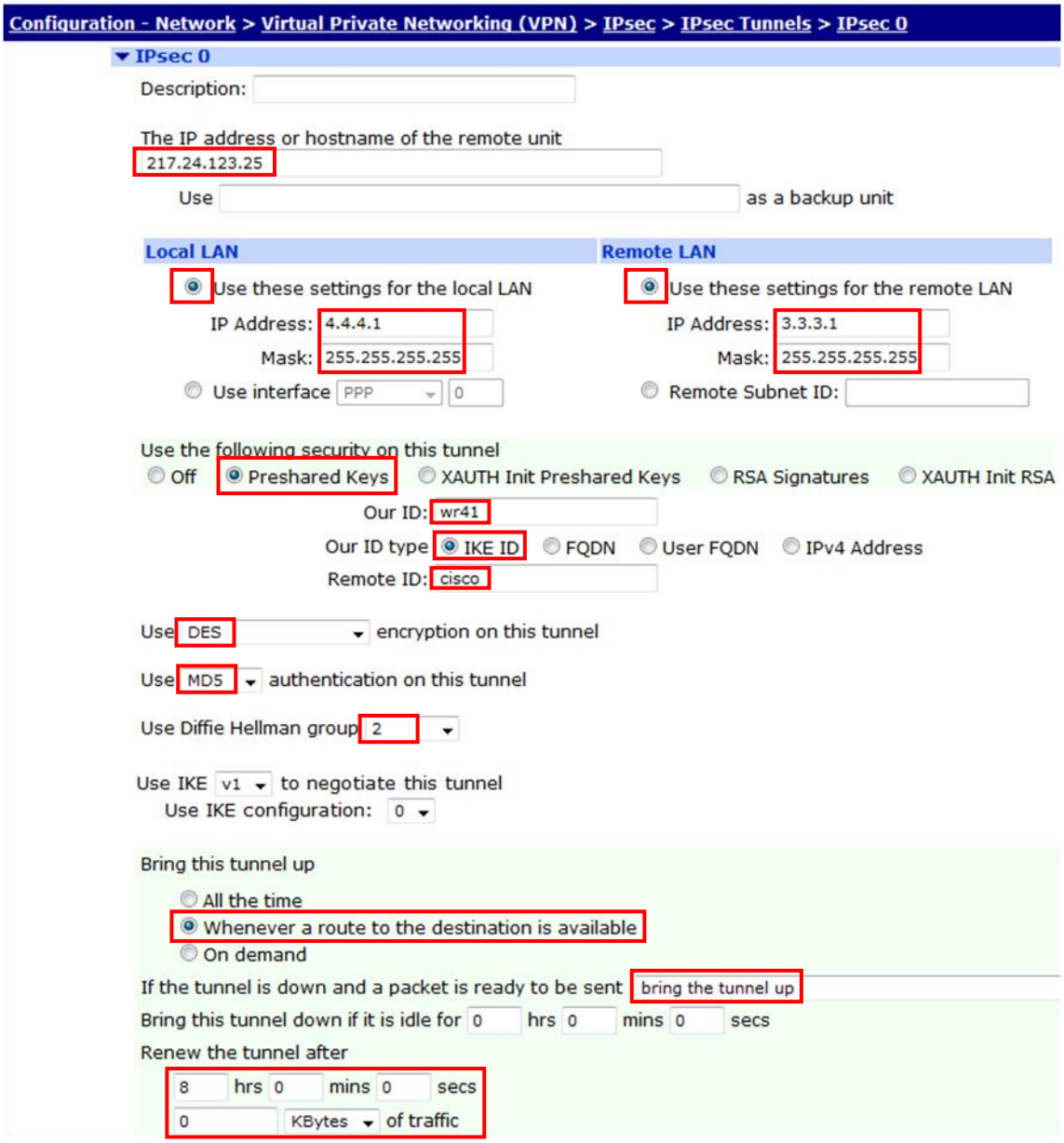
2.3 Configuring the Eroute

This section covers configuring the Eroute used to encrypt the GRE packets.

These settings are the equivalent of the Cisco Crypto configuration, configure the Cisco accordingly.

Navigate to:

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



Parameter	Setting	Description
The IP address or hostname of the remote unit	217.24.123.25	Internet IP address of the Remote Cisco router
Use these settings for the local LAN		
IP Address	4.4.4.1	TransPort router End point IP address of the GRE Tunnel
Mask	255.255.255.255	TransPort router End point Subnet Mask of the GRE Tunnel
Remote LAN		
IP Address	3.3.3.1	Cisco End point IP address of the GRE Tunnel
Mask	255.255.255.255	Cisco End point Subnet Mask of the GRE Tunnel
Use the following security on this tunnel		
Preshared Keys	Selected	Uses preshared key authentication
Our ID	wr41	ID of the TransPort router
Our ID type	IKE ID	Sets the ID type for authentication
Remote ID	cisco	Peer ID as set on the Cisco router
encryption on this tunnel	DES	Phase 2 Encryption algorithm
authentication on this tunnel	MD5	Phase 2 Authentication algorithm
Diffie Hellman group	2	DH group
Bring this tunnel up	Whenever a route to the destination is available	Creates an always on VPN when a valid route exists
If the tunnel is down and a packet is ready to be sent	Bring the tunnel up	If no SAs exist, create new SAs

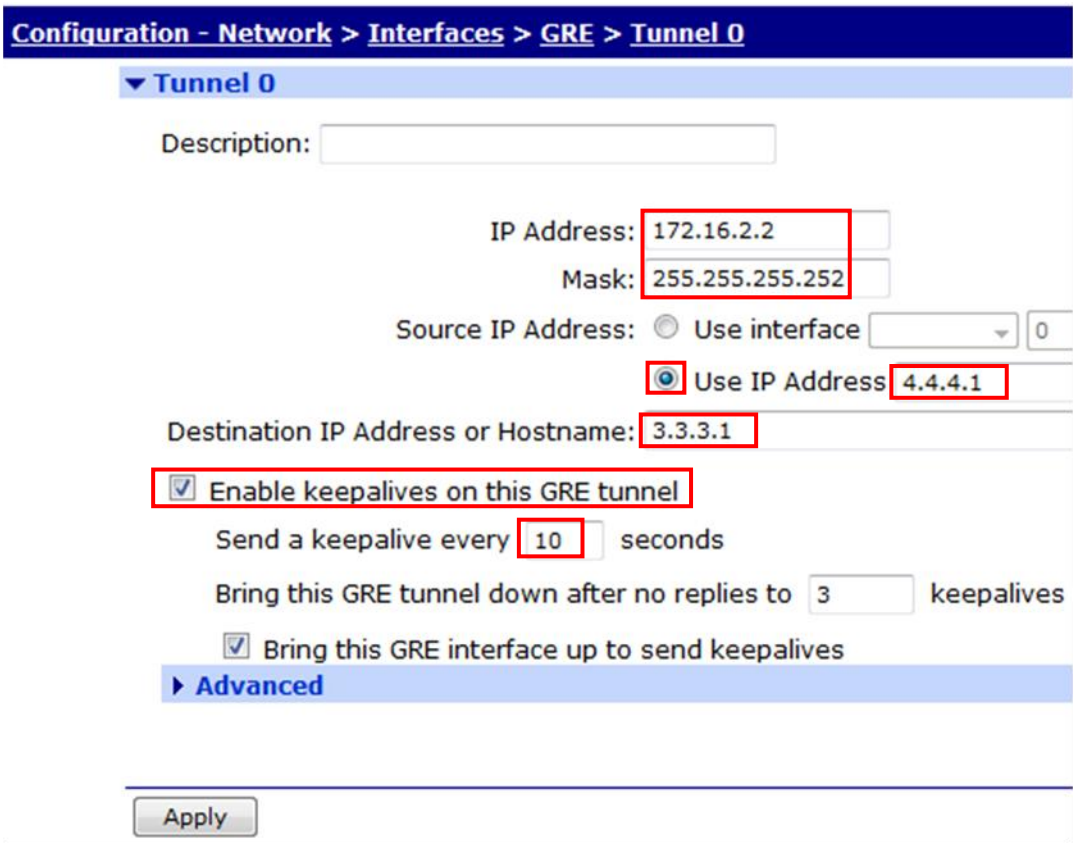
2.4 Configuration of TUN 0

This section shows the changes the GRE Tunnel interface configuration.

These settings are the equivalent of the Cisco Loopback interface configuration, configure the Cisco accordingly.

Navigate to:

Configuration - Network > Interfaces > GRE > Tunnel 0

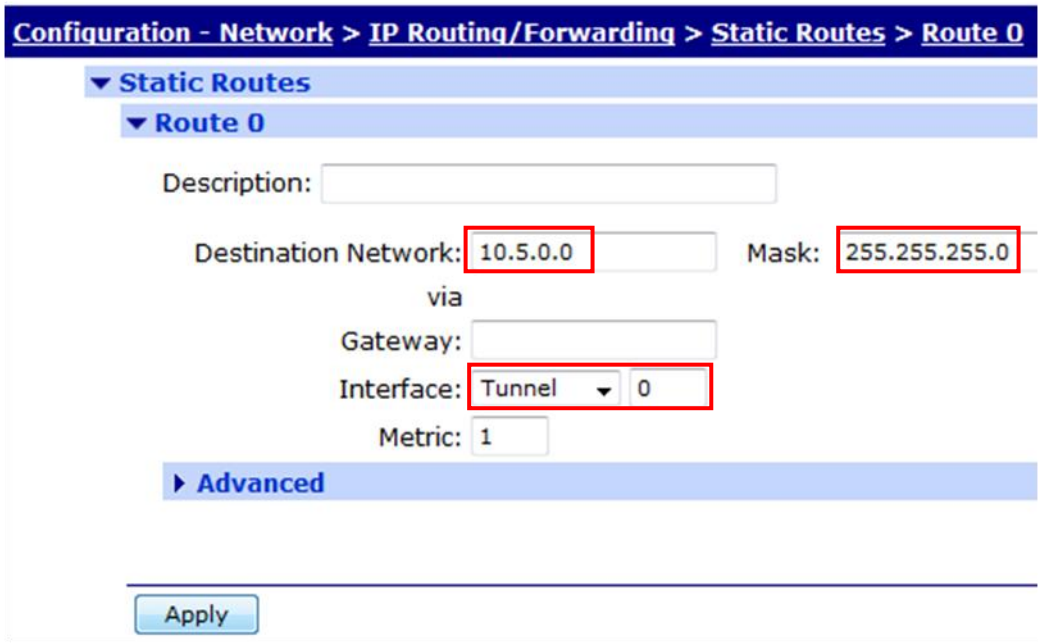


Parameter	Setting	Description
IP address	172.16.2.2	IP address of the GRE tunnel endpoint
Mask	255.255.255.252	Mask for the GRE tunnel endpoint
Source IP Address Use IP Address	4.4.4.1	GRE source address (treated at a host address)
Destination IP Address or Hostname	3.3.3.1	GRE dest address (treated at a host address)
Enable keepalives on this GRE tunnel	Ticked	Enables GRE keepalives
Send a keepalive every n seconds	10	GRE Keepalive delay interval in seconds

2.5 Configuration of route 0

This section shows the changes needed to be made to the routing table. This is so the router knows to route the traffic to the remote network over the GRE tunnel. A static route back to the WR41's LAN will need adding to the Cisco.

Navigate to:
Configuration - Network > IP Routing/Forwarding > Static Routes > Route 0



Parameter	Setting	Description
Destination Network	10.5.0.0	This is the end point of the GRE tunnel
Mask	255.255.255.0	The Mask treats it as a single host
Interface	TUN 0	Wan interface to send the packets to

After clicking **Apply**, follow the link that appears and save the configuration to flash.

3 TESTING

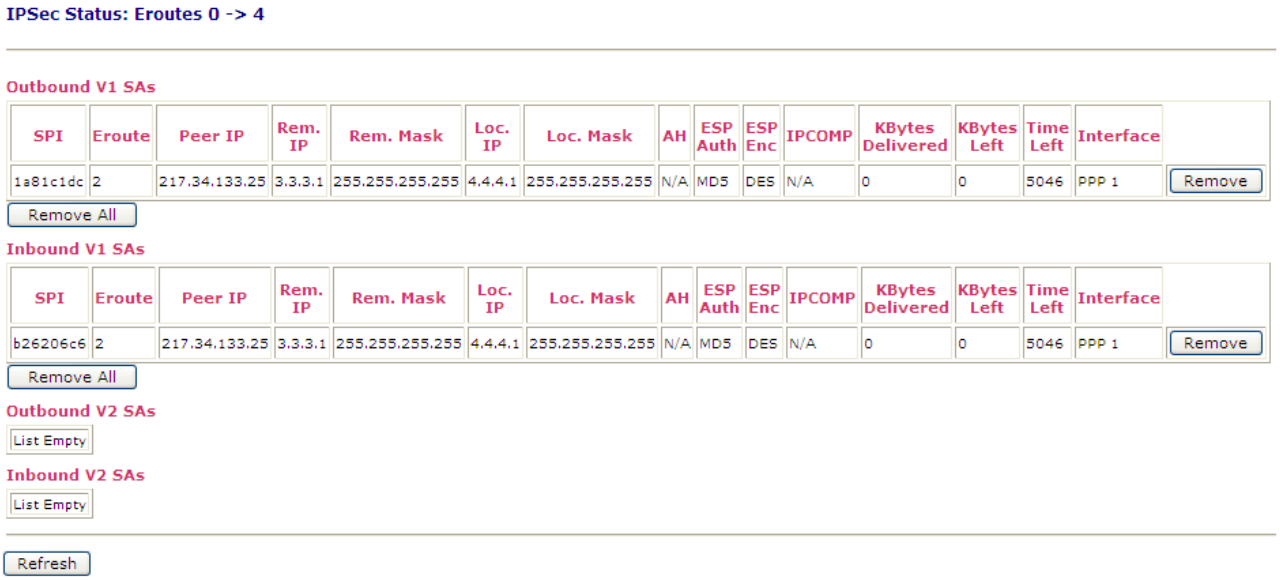
3.1 Checking the IPSEC tunnel

Firstly check the IPSEC tunnel has come up on the TransPort router.

Navigate to:

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

The output should look similar to this below:



IPSec Status: Eroutes 0 -> 4

Outbound V1 SAs

SPI	Eroute	Peer IP	Rem. IP	Rem. Mask	Loc. IP	Loc. Mask	AH	ESP Auth	ESP Enc	IPCOMP	KBytes Delivered	KBytes Left	Time Left	Interface	
1a81c1dc	2	217.34.133.25	3.3.3.1	255.255.255.255	4.4.4.1	255.255.255.255	N/A	MD5	DES	N/A	0	0	5046	PPP 1	Remove

Remove All

Inbound V1 SAs

SPI	Eroute	Peer IP	Rem. IP	Rem. Mask	Loc. IP	Loc. Mask	AH	ESP Auth	ESP Enc	IPCOMP	KBytes Delivered	KBytes Left	Time Left	Interface	
b26206c6	2	217.34.133.25	3.3.3.1	255.255.255.255	4.4.4.1	255.255.255.255	N/A	MD5	DES	N/A	0	0	5046	PPP 1	Remove

Remove All

Outbound V2 SAs

List Empty

Inbound V2 SAs

List Empty

Refresh

3.2 Check the routing table

This stage will show the output of the routing table, either use a serial or Telnet connection, or alternatively from the Web interface navigate to **Administration - Execute a command** and do the following:

Type **route print** then press enter, the output should look like the following:

```
route print
------------------------------------------------------------
Interface Addresses:
--------------------
PPP 1: 10.171.173.217
ETH 0: 10.49.206.1
TUN 0: 172.16.2.2

Routes:
-------
  #    IP Address        Mask          Metric   Interface     Gateway
Dynamic Routes:
     10.49.206.1       255.255.255.0     1        ETH 0
     172.16.2.2        255.255.255.252   1        TUN 0

Static Routes:
  1: 10.5.0.0          255.255.255.0     1        TUN 0

Default Routes:
  0: 0.0.0.0           0.0.0.0           1        PPP 1
------------------------------------------------------------
```

3.3 Check the Statistics on TUN 0

Use a serial or Telnet connection, or alternatively from the Web interface navigate to **Administration - Execute a command** and do the following:

Type **tunstat 0** then press enter, the output should look like the following:

```
tunstat 0
Tun 0 stats:
   Admin Status          Up
   Oper Status           Up
   IP Address            172.16.2.2
   Mask                  255.255.255.252
   Source                4.4.4.1
   Destination           3.3.3.1
   Tx Packets            155646
   Tx Bytes              7471008
   Tx Errors             0
   Tx Discards           0
   Rx Packets            0
   Rx Bytes              0
   Rx Errors             0
   Rx Unknown Protocols  0
   Keepalives Sent       155
   Keepalives Rcvd       153
OK
```

3.4 Ping Check from the TransPort router to remote

This stage will send a ping packet over the tunnel, either use a serial or Telnet connection, or alternatively from the Web interface navigate to **Administration - Execute a command** and do the following:

Type **ping 10.5.0.1 –e0** then press enter, the output should look like the following:

```
Ping 10.5.0.1 -e0

Pinging Addr [10.5.0.1]

sent PING # 1
PING receipt # 1 : response time 0.17 seconds
Iface: TUN 0
Ping Statistics
Sent        : 1
Received    : 1
Success     : 100 %
Average RTT : 0.17 seconds

OK
```

4 CONFIGURATION FILES

4.1 TransPort router Configuration Files

This is the configuration file from the TransPort router:

```
eth 0 IPaddr "10.49.206.1"
route 0 IPaddr "10.5.0.0"
route 0 ll_ent "tun"
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
eroute 0 peerip "217.24.123.25"
eroute 0 peerid "cisco"
eroute 0 ourid "wr41"
eroute 0 ouridtype 1
eroute 0 locip "4.4.4.1"
eroute 0 locmsk "255.255.255.255"
eroute 0 remip "3.3.3.1"
eroute 0 remmsk "255.255.255.255"
eroute 0 ESPauth "MD5"
eroute 0 ESPenc "DES"
eroute 0 ltime 8000
eroute 0 lkbytes 0
eroute 0 authmeth "PRESHARED"
eroute 0 nosa "TRY"
eroute 0 autosa 1
dpd 0 okint 120
dpd 0 failint 5
dpd 0 inact 60
dpd 0 maxfail 3
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 aggressive ON
modemcc 0 info_asy_add 5
modemcc 0 init_str "+CGQREQ=1,0,0,0,0,0"
modemcc 0 init_str1 "+CGQMIN=1,0,0,0,0,0"
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=1,0,0,0,0,0"
modemcc 0 init_str1_2 "+CGQMIN=1,0,0,0,0,0"
modemcc 0 apn_2 "Your.APN.goes.here"
modemcc 0 link_retries_2 10
modemcc 0 stat_retries_2 30
modemcc 1 link_retries 10
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "ss.2000r"
cmd 0 tremto 3000
cmd 1 gpson 1
cmd 3 cfilton 1
user 0 name "Sarian"
user 0 epassword "EA0iCxQc"
user 0 access 0
user 1 name "username"
user 1 epassword "KD5lSVJDVVg="
user 1 access 0
user 8 name "cisco"
user 8 epassword "NDpiV0BFSQ=="
local 0 transaccess 2
scep 0 app "pkiclient.exe"
tun 0 IPaddr "172.16.2.2"
tun 0 mask "255.255.255.252"
tun 0 source "4.4.4.1"
tun 0 dest "3.3.3.1"
tun 0 kadelay 10
tun 0 descr "Tunnel to Cisco"
```

4.2 TransPort router Firmware Versions

This is the firmware \ hardware information from the TransPort router:

```
Digi TransPort WR41 HSDPA/3G Router Ser#:56691 HW Revision: 4405a
Software Build Ver5130.  Apr 04 2007 11:15:57  YW
ARM Bios Ver 6.06 v31 200MHz B64-M64-F80-O100,0 MAC:00042d00dd73
Power Up Profile: 0
Async Driver              Revision: 1.19  Int clk
Ethernet Driver           Revision: 1.11
Firewall                  Revision: 1.0
EventEdit                 Revision: 1.0
SHIM                      Revision: 1.0
Timer Module              Revision: 1.1
L2TP                      Revision: 1.10
LAPB                      Revision: 1.12
```

```
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
ARM Sync Driver           Revision: 1.18
TCP                       Revision: 1.14
TCP Utils                 Revision: 1.13
PPP                       Revision: 1.18
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 (Novatel 3G)     Revision: 1.3
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: 1.1
OK
```

4.3 Configuration Files from other devices

```
Current configuration : 1895 bytes
!
hostname cisco
!
!
username wr41 password 0 XXXX
!
aaa new-model
!
!
aaa authentication login userlist group radius local
aaa authorization network grouplist group radius local
aaa session-id common
ip subnet-zero
!
no ip domain lookup
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key letmein hostname wr41
crypto isakmp identity hostname
!
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set my_enc_config esp-des esp-md5-hmac
!
crypto dynamic-map mydynmap 1
```

```
 set transform-set my_enc_config
!
crypto map mymap1 20 ipsec-isakmp dynamic mydynmap
!
interface Loopback3
 ip address 3.3.3.1 255.255.255.255
!
interface Tunnel0
 ip address 172.16.2.1 255.255.255.252
 ip ospf mtu-ignore
 tunnel source Loopback3
 tunnel destination 4.4.4.1
!
interface Ethernet0
 ip address 10.5.0.1 255.255.255.0
 full-duplex
!
interface FastEthernet0
 ip address 217.24.123.25 255.255.255.240
 speed auto
 crypto map mymap1
!
ip classless
ip route 0.0.0.0 0.0.0.0 217.24.123.29
ip route 4.4.4.1 255.255.255.255 FastEthernet0
ip route 10.49.206.0 255.255.255.0 Tunnel0
!
radius-server authorization permit missing Service-Type
!
```

4.4 Firmware\Hardware Information from other devices

```
cisco 1720 (MPC860T) processor (revision 0x501) with 41780K/7372K bytes of memory.

IOS (tm) C1700 Software (C1700-K9SY7-M), Version 12.2(15)T
c1700-k9sy7-mz.122-15.T.bin
```