# Application Note 9

## Using IPsec over a mobile network from a Digi TransPort router to a Cisco router

**November 2015**

# 1 CONTENTS

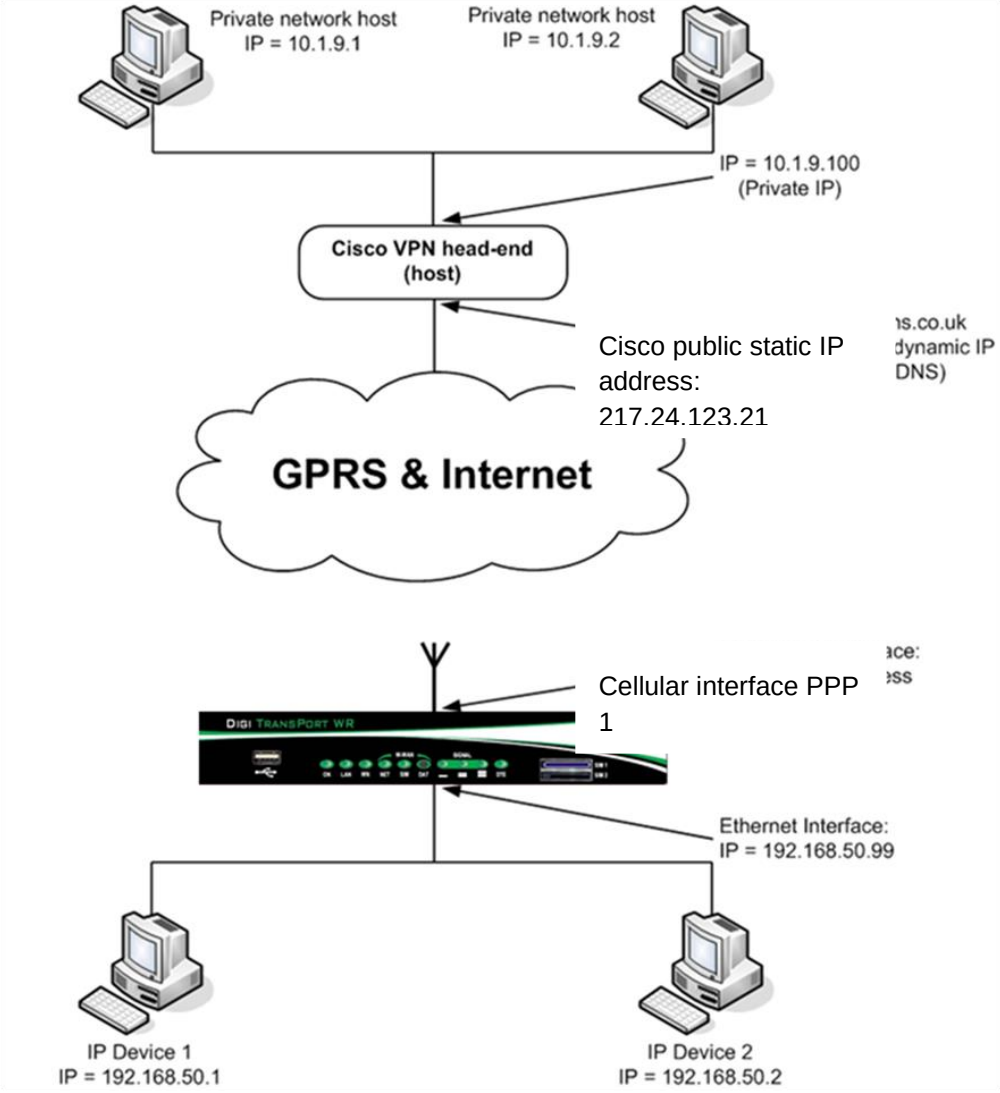
# 2 INTRODUCTION

## 2.1 Outline

It is often required to configure a Digi Transport router as one end of a VPN tunnel, where the other end is a Cisco device such as a 3725 series running the Ipsec security option.

This Application Note aims to enable the reader to easily configure the Cisco device to accept incoming VPN requests from a remote Digi Transport Wireless router e.g. WR, DR. HR models

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



## 2.2 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 Digi Transport is assigned a private dynamic IP address on its cellular interface and Ipsec will be used in "aggressive mode".

The Digi Transport's cellular IP address can be dynamic or static, public or 'private with NAT' and this configuration will still be valid but it will depend on the capabilities and the IOS version of the Cisco router.

If the Digi Transport's cellular IP address is "natted" this can still work, but the head-end device must support NAT traversal. The Digi Transport configuration detailed here will attempt to use NAT traversal automatically if required.

It is entirely possible to use another WR41 or other Digi Transport product
the Cisco in this example. All Digi Transport Ipsec products fully support I

Cisco public IP address:
217.24.123.21

The head-end Cisco must be assigned a public (not a "natted") IP address on its WAN interface. This can be static or dynamic. If dynamic, a DNS service must be use to assign the dynamic IP address to a static hostname which can then be used in the configuration.

**Note on Cisco NAT Traversal**:

NAT Traversal is a feature that is auto detected by VPN devices. There are no configuration steps for a router running Cisco IOS Release 12.2(13)T. If both VPN devices are NAT-T capable, NAT Traversal is auto detected and auto negotiated.

**Terminology:** The term cellular is used throughout this application note, but this can also refer to GPRS, EDGE, UMTS, WCDMA & HSPA mobile technologies.

**Models shown:** Digi Transport WR41

**Other Compatible Models:** All other Digi Transport products with Ipsec enabled, although this application note describes Ipsec over a mobile network, the same procedure can be applied to an ADSL or ISDN connection as long as the correct PPP instance is used when configuring the Digi Transport router.

**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.

## 2.3 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.

## 2.4 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 | Updated for web GUI changes for 5123 |
| 2.2 | Fixed errors & updated |
| 2.3 | Rebrand 2015 |

# 3 CONFIGURATION

## 3.1 Cisco Configuration

The first step is to obtain a command prompt at the 3725 and establish that the IPsec option has been installed. If it has not, you will not be able to enter the keyword “crypto” without getting an error. Remember as well that you need to be in Enable mode and have entered configuration mode (e.g. by typing “configure terminal”) to enter configuration commands.

Most of this is standard configuration, but where it relates to IPsec it is documented below so that you can see what is happening:

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

The entry below sets the host name of the Cisco. It is also the ID that the Cisco sends during the IKE negotiation.

```
hostname cisco

no logging on
enable password mypassword

memory-size iomem 15
ip subnet-zero
ip name-server 4.2.2.2
```

The entries below for the **I**nternet **S**ecurity **A**ssociation and **K**ey **M**anagement **P**olicy closely relate to the configuration of IKE on the WR41. The following entries cause the Cisco to use: **AES 128** for the encryption algorithm, **SHA1** for the hash algorithm (no configuration required as it is the default option), **pre-shared keys** for the authentication method, **Diffie-Hellman Group 2** and an IKE SA lifetime of **8000 seconds**.

```
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 2
 lifetime 8000
```

The following entry configures NAT-T keep-alives:

```
crypto isakmp nat keepalive 20
```

The following entry specifies that the peer that identifies itself as “transport” should use the pre-shared key “securePSK” and not try and use XAuth.

```
crypto isakmp key 0 securePSK hostname transport no-xauth
```

The following entry causes the Cisco to send its hostname to the peer as its identity instead of its IP address during the IKE negotiations:

```
crypto isakmp identity hostname
```

The following entry defines an IPsec transform set called “my_cellular_set”. This transform set contains the settings required for the IPsec. These are: ESP with the AES 128 for the encryption and ESP with SHA1 for the authentication.

```
crypto ipsec transform-set my_cellular_set esp-aes esp-sha-hmac
```

The following dynamic-map is required so that a remote peer with a dynamic IP address can establish an IPsec session with this Cisco:

```
crypto dynamic-map mydynmap 1
```

Any such peer must use the IPsec settings in the my_cellular_set transform set:

```
set transform-set my_cellular_set
```

And will only be allowed to route packets to and from the IP address range specified below in access-list 101:

```
match address 101
```

The following crypto map simply states that the dynamic-map should be used for any interfaces that reference this crypto map:

```
crypto map mymap1 20 ipsec-isakmp dynamic mydynmap
```

The Cisco is connected to the Internet and the private network via its Ethernet interfaces. The Crypto map must be applied to the WAN interface, this enables IPsec on the outside interface.

```
interface FastEthernet0/0
 ip address 217.24.123.21 255.255.255.240
 speed 100
 duplex full
 crypto map mymap1
!
interface FastEthernet0/1
 ip address 10.1.9.100 255.255.0.0
 speed 100
 duplex full
```

The following entries configure the default gateway:

```
ip route 0.0.0.0 0.0.0.0 217.24.123.29
```

The following entry allows IP access to and from the access-list specified below:

```
ip access-list extended access-list
```

The following entry defines access-list 101 which is referenced above:

```
access-list 101 permit ip 10.1.0.0 0.0.255.255 192.168.50.0 0.0.0.255
```

The following entries enable NAT on the outside interface:

```
access-list 1 permit 10.1.0.0 0.0.255.255
interface FastEthernet0/0
 ip nat outside
interface FastEthernet0/1
 ip nat inside
exit
ip nat inside source list 1 interface FastEthernet0/0 overload
```

Save the configuration:

```
copy run start
```

## 3.2 Digi Transport Configuration

On the Digi TransPort router you have the option of configuring the IPsec parameters either via the web interface or by writing a new configuration file.

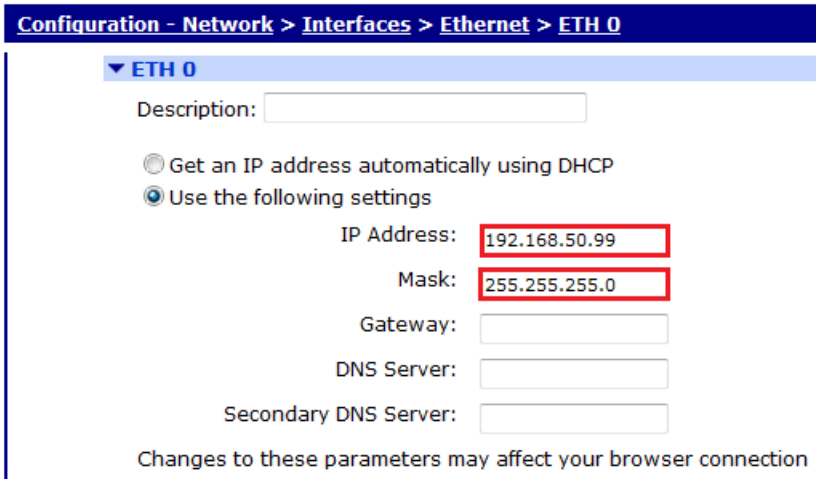
### 3.2.1 Interface configuration

This section relates to the configuration of the LAN and WAN interfaces.

#### *3.2.1.1 Configure the Digi TransPort's LAN IP address.*

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

| Parameter | Setting | Description |
|---|---|---|
| IP Address | 192.168.50.99 | Relevant IP address of the Ethernet port |
| Mask | 255.255.255.0 | Relevant subnet mask of the Ethernet port |

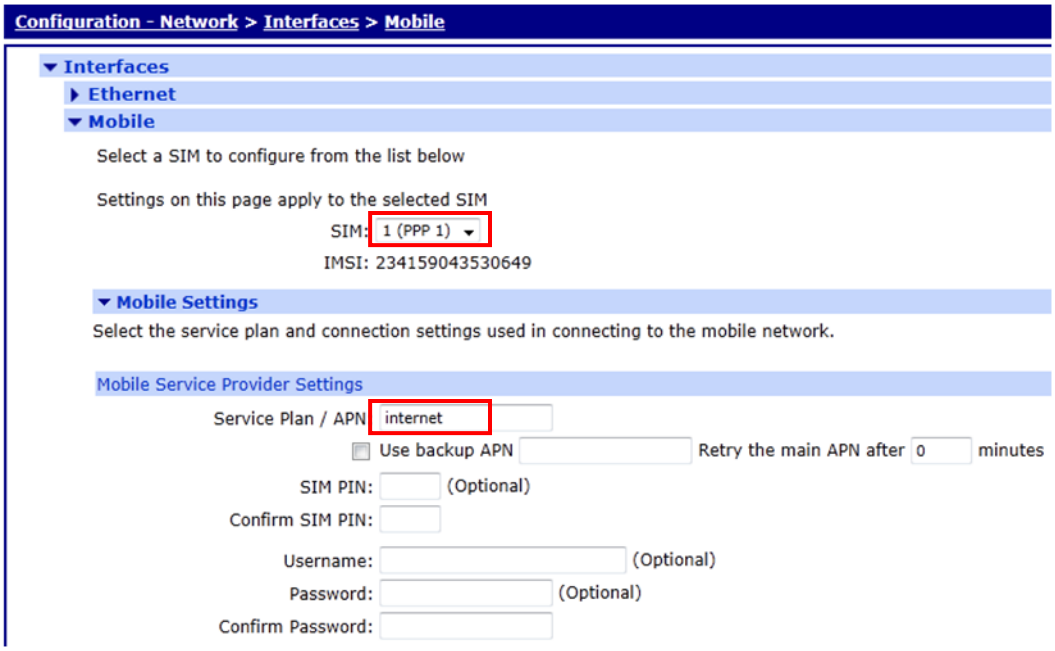



Remember to click "**Apply**" to save the changes.

#### *3.2.1.2 Configure the cellular module.*

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

| Parameter | Setting | Description |
|---|---|---|
| SIM | 1 | Select SIM 1 for the PPP 1 interface |
| Service Plan/APN | internet | The Access Point Name for the network |




Click Apply

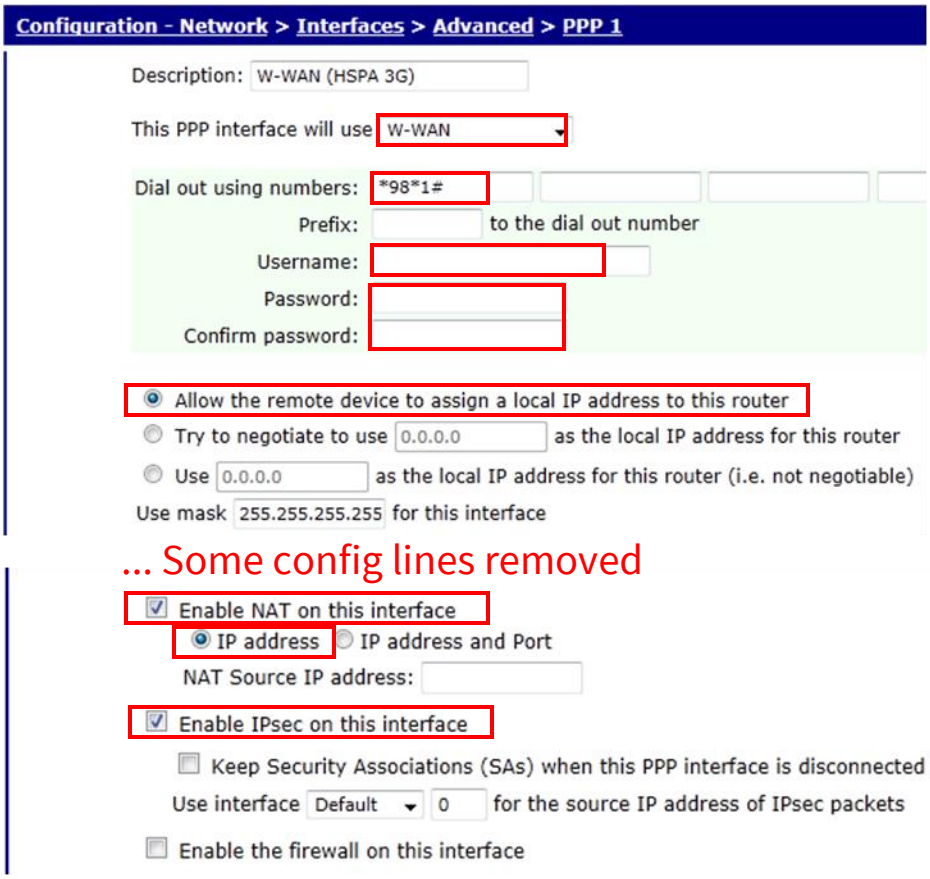
Note: The APN is dependent on the mobile operator, check with the service provider to obtain the correct APN.

### *3.2.1.3 Configure the WAN interface*

The following section configures the Digi Transport to use PPP 1 for the cellular interface. The username and password fields may or may not be required by the SIM. The PPP dial out number should not be changed from the default entry.

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

| Parameter | Setting | Description |
|---|---|---|
| Dial out using numbers | *98*1# | The number to call for outgoing PPP calls – do not amend this number it will be configured appropriately for your cellular module |
| Username | Username (optional) | The username to use when authenticating with the mobile operator |
| password | Password (optional) | Password to use when authenticating with the mobile operator |
| Allow the remote device to assign a local IP address to this router | Selected (default) | The ISP will assign this router an IP address using DHCP |
| Enable NAT on this interface | Ticked (default) | Traffic leaving PPP 1 interface will have NAT applied |
| Enable IPsec on this interface | Ticked | Enables IPsec on PPP 1 interface. |



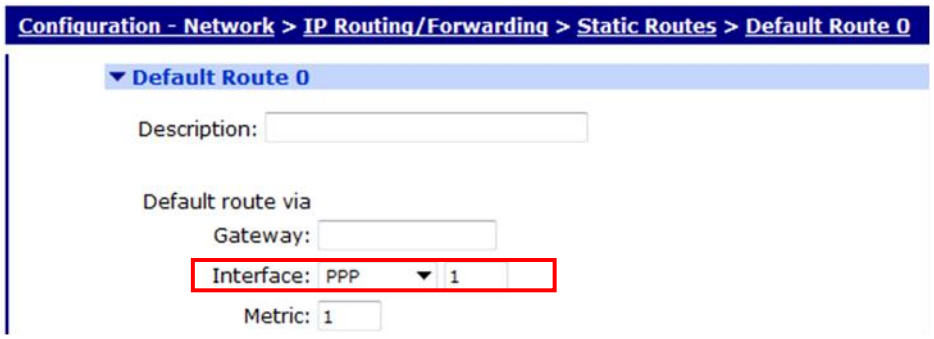

Click Apply

### *3.2.1.4 Configure the default route*

Confirm the default route is set to PPP 1 (the cellular interface).

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

| Parameter | Setting | Description |
|---|---|---|
| Interface | PPP | Default Route 0 is via PPP 1 |
| Interface# | 1 | |



Click Apply

## 3.2.2 IPsec configuration

The following sections relate to the IPsec VPN parameters

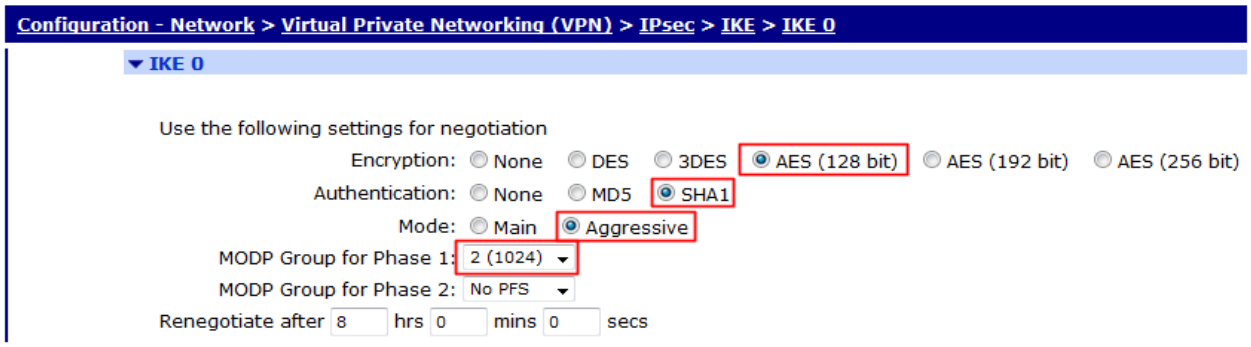
### *3.2.2.1 Phase 1 – IKE configuration*

Navigate to:
**Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE 0**

The Encryption and Authentication should be set to AES 128 & SHA1 to match the Cisco.

By default the IKE 0 configuration is in **Main Mode**, for cellular connections behind a service provider NAT/Firewall set this parameter to **Aggressive Mode**.

If unsure which mode to enable, use Aggressive Mode as there are less caveats with the configuration.

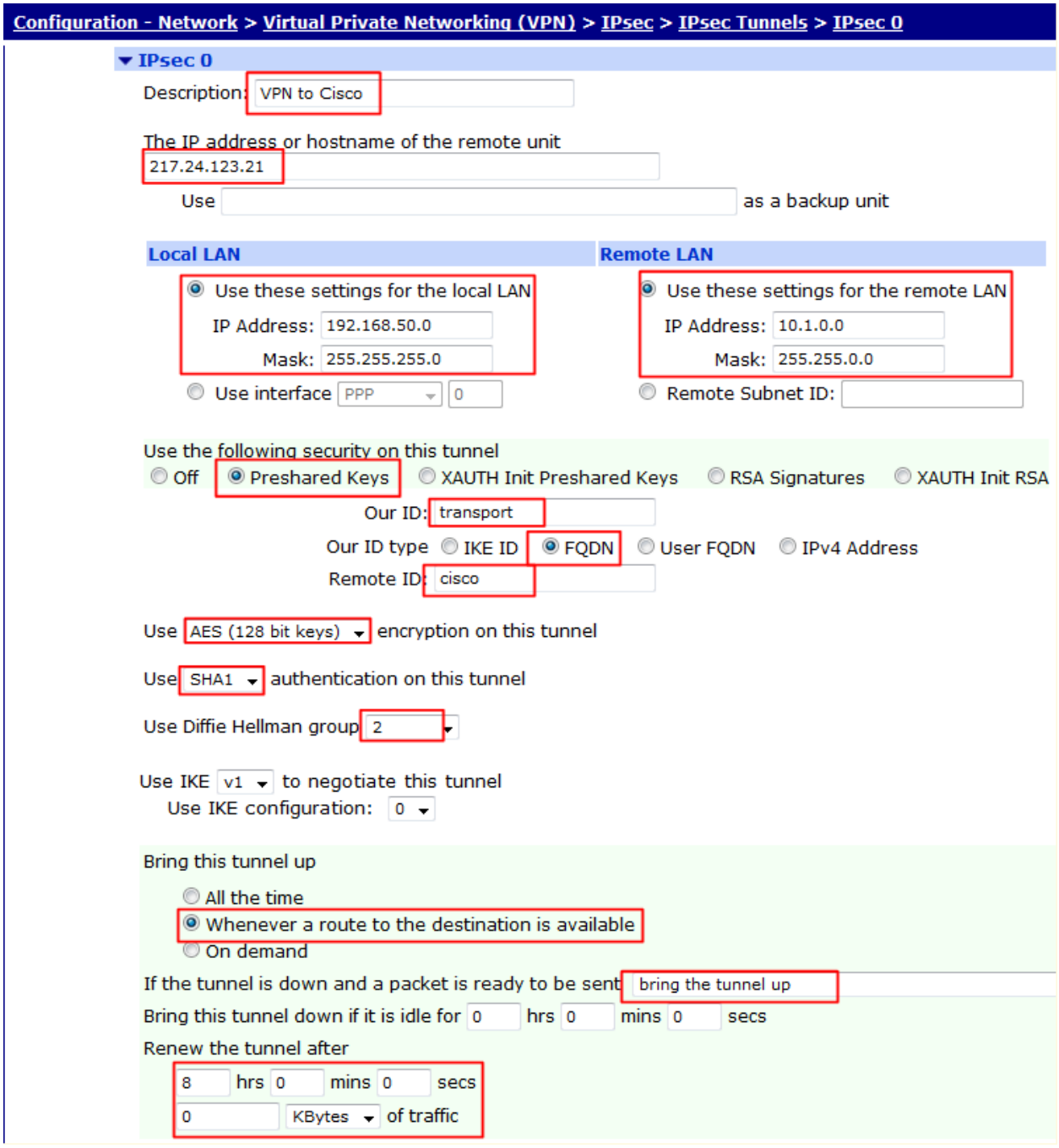



Click Apply

### *3.2.2.2 Phase 2 – IPsec configuration*

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

| Parameter | Setting | Description |
|---|---|---|
| The IP address or hostname of the remote unit | 217.24.123.21 | The public IP address of the Cisco router |
| Local LAN: IP address | 192.168.50.0 | Packets will be directed through this tunnel if the source IP matches these settings |
| Local LAN: Mask | 255.255.255.0 | |
| Remote LAN: IP address | 10.1.0.0 | And the destination IP matches these settings |
| Remote LAN: Mask | 255.255.0.0 | |
| Use the following security on this tunnel | Preshared Keys | Use Preshared keys as the IKE authentication method |
| Our ID | transport | The ID that the Digi Transport will send to the Cisco during the IKE negotiations |
| Our ID type | FQDN | This will send the ID of the Digi Transport as a Fully Qualified Domain Name |
| Remote ID | cisco | The ID that the Digi Transport expects to receive from the Cisco during the IKE negotiations |
| Use <ENC> encryption on this tunnel | AES 128 | The encryption algorithm to use |
| Use <AUTH> authentication on this tunnel | SHA1 | The authentication algorithm to use |
| Use Diffie Hellman group | 2 | The Diffie Hellman group to use |
| Bring this tunnel up | Whenever a route to the destination is available | Only packets matching the local & remote subnets will cause this Eroute to be activated |
| If the tunnel is down and a packet is ready to be sent | bring the tunnel up | If a packet matches this “eroute” and no SA exists then try to create one |
| Renew the tunnel after | 8 hours | The IPsec SA duration, set to a value less or equal to that of the Cisco’s ipsec “seconds” setting |
| Renew the tunnel after | 0 KBytes | The Digi Transport is configured not to expire the IPsec SA based upon volume of data |




Click Apply

### *3.2.2.3 Configure the Pre Shared Key*

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

The following parameters are required to store the pre-shared key for the IKE negotiations. The peer that identifies itself as “cisco” will use the pre-shared key “securePSK”. In order to do this, a user with the name “cisco” must be stored on the Digi Transport in the user configuration section, along with the

password which is the pre-shared key. As this user is only need for IPsec authentication, the Access Level should be set to “None”

| Parameter | Setting | Description |
|---|---|---|
| Username | cisco | Name should match the Peer ID: value from Eroute 0 |
| Password | securePSK | This password is the Pre Shared Key |
| Confirm Password | securePSK | Confirm the Pre Shared Key |
| Access Level | None | This user will not be granted any admin access |


Click Apply

### *3.2.2.4 Set up the analyser trace*

Configure the Analyser to assist with any troubleshooting that may be required.
Browse to **Management - Analyser > Settings**

Remove any ticks or options unless they as specified in the following table.

| Parameter | Setting | Description |
|---|---|---|
| Enable Analyser | Ticked | Enables analysis |
| Maximum packet capture size | 1500 | Captures the full packet |
| Log size | 180 | 180 is the maximum log size in Kb |
| Protocol Layers | 3 | Only layer 3 is required |
| Enable IKE Debug | Ticked | IKE debugging information is recorded |
| IP Sources | PPP 1 | PPP 1 IP data is recorded |
| IP Packet Filters: TCP/UDP Ports | ~500, 4500 | IKE & NAT-T traffic is recorded |

# 4 CONFIGURATION FILES

## 4.1 Digi Transport Command Line Configuration

Only the parts of the configuration file that specifically relate to the configuration of this example will be explained in detail. (The entire configuration file can be found at the end of this document).
The Digi Transport's Ethernet IP address:

```
eth 0 IPaddr "192.168.50.99"
eth 0 mask "255.255.255.0"
```

cellular Module configuration:

```
modemcc 0 apn "internet"
modemcc 0 link_retries 10
modemcc 0 stat_retries 30
```

The following section configures the Digi Transport to use PPP 1 for the cellular interface. The username and password fields may or may not be required by the SIM. The "ipsec ON" setting enables IPsec for the cellular (outside) interface:

```
ppp 1 IPaddr "0.0.0.0"
ppp 1 phonenum "*98*1#"
ppp 1 timeout 0
ppp 1 use_modem 1
ppp 1 autoassert ON
ppp 1 ipsec ON
ppp 1 ipanon ON
```

The default route to send packets to destinations not on a local interface is PPP 1:

```
def_route 0 ll_ent "PPP"
def_route 0 ll_add 1
```

The following section contains some global IKE settings:
Lifetime of the IKE session (should be equal to the Cisco's IKE lifetime):

```
ike 0 ltime 8000
```

Use aggressive mode rather than main mode:

```
ike 0 aggressive ON
```

The following Eroute settings mainly relate to IPsec and phase 2. The peer IP entry is the IP address of the Cisco host:

```
eroute 0 peerip "217.24.123.21"
```

The ourid entry is the ID that the Digi Transport will send to the Cisco during the IKE negotiations:

```
eroute 0 ourid "transport"
```

The "ouridtype 1" setting sends the ourid parameter as type FQDN to the Cisco:

```
eroute 0 ouridtype 1
```

Packets will be directed through this tunnel if the source IP matches:

```
eroute 0 locip "192.168.50.0"
eroute 0 locmsk "255.255.255.0"
```

And the destination IP matches:

```
eroute 0 remip "10.1.0.0"
eroute 0 remmsk "255.255.0.0"
```

The IPsec ESP authentication algorithm is SHA1:

```
eroute 0 ESPauth "SHA1"
```

The IPsec encryption algorithm is AES 128:

```
eroute 0 ESPenc "AES"
eroute 0 enckeybits 128
```

The Diffie-Hellman group is group 2:

```
eroute 0 dhgroup 2
```

The IPsec duration should be set to the same as that of the Cisco's ipsec "seconds" setting:

```
eroute 0 ltime 28800
```

The Digi Transport is configured not to expire the IPsec SA based upon volume of data:

```
eroute 0 lkbytes 0
```

The IKE authentication method to use is pre-shared key:

```
eroute 0 authmeth "PRESHARED"
```

If a packet matches this "eroute" and no SA exists then try to create one:

```
eroute 0 nosa "TRY"
```

Continually try to keep the tunnel (IPsec session) up regardless of whether we have any data to route:

```
eroute 0 autosa 1
```

User table configuration:
The following entries are here to allow access to the Digi Transport's management facilities.
Note, epassword is an enciphered password not plain text.
To enter the password as plain text: "user 1 password password".

```
user 1 name "username"
user 1 epassword "KD51SVJDVVg="
```

The following entry is required to store the pre-shared key for the IKE negotiations. The pre-shared key to be used with the peer that identifies itself as "cisco" is "securePSK".
Note, epassword is an enciphered password not plain text.
To enter the password as plain text: "user 1 password securePSK".

```
user 10 name “cisco”
user 10 epassword “Kzp1T1dJd295”
user 10 access 4
```

This is the config.da0 file used for the purpose of this Application Note

```
eth 0 IPaddr "192.168.50.99"
eth 0 mask "255.255.255.0"
addp 0 enable 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
ip 0 cidr ON
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
eroute 0 peerip "217.24.123.21"
eroute 0 ourid "transport"
eroute 0 peerid "cisco"
eroute 0 ouridtype 1
eroute 0 locip "192.168.50.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 remip "10.1.0.0"
eroute 0 remmsk "255.255.0."
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "AES"
eroute 0 enckeybits 128
eroute 0 dhgroup 2
eroute 0 ltime 28800
eroute 0 lkbytes 0
eroute 0 authmeth "PRESHARED"
eroute 0 nosa "TRY"
eroute 0 autosa 1
dhcp 0 IPmin "192.168.1.100"
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "192.168.1.1"
ppp 0 timeout 300
ppp 1 name "W-WAN (HSPA 3G)"
ppp 1 phonenum "*98*1#"
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 ipsec 1
ppp 1 use_modem 1
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 ipanon ON
ppp 1 r_chap OFF
```

```
ppp 3 defpak 16
ppp 4 defpak 16
ike 0 encalg AES
ike 0 keybits 128
ike 0 authalg SHA1
ike 0 ikegroup 2
ike 0 ltime 8000
ike 0 aggressive ON
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 OFF
ana 0 l2on OFF
ana 0 l3on ON
ana 0 xoton OFF
ana 0 lapdon 0
ana 0 asyon 0
ana 0 ikeon ON
ana 0 ipportfilt "~500,4500"
ana 0 maxdata 1500
ana 0 logsize 180
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 asyled_mode 2
cmd 0 tremto 3000
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 "cisco"
user 10 epassword "Kzp1T1dJd295
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

Power Up Profile: 0
OK
```

## 4.2 Digi Transport Firmware Versions

The Digi Transport configuration above was tested on a Digi Transport WR41 with version 5129 firmware

```
ati5
Digi TransPort WR41-HXI1-DV1-XX(WR41v1) Ser#:12345 HW Revision: 4403a
Software Build Ver5129.  May 20 2011 10:46:57  ZW
ARM Bios Ver 6.02 v36 399MHz B128-M128-F80-O100,0 MAC:00042d003039
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
OK
```

## 4.3 Cisco Command Line Configuration

```
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname cisco

no logging on
enable password mypassword

memory-size iomem 15
ip subnet-zero
ip name-server 4.2.2.2
!
!
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 2
 lifetime 8000
crypto isakmp nat keepalive 20
crypto isakmp key securePSK hostname transport no-xauth
crypto isakmp identity hostname
!
!
crypto ipsec transform-set my_cellular_set esp-aes esp-sha-hmac
!
crypto dynamic-map mydynmap 1
 set transform-set my_cellular_set
```

```
 match address 101
!
!
!
crypto map mymap1 20 ipsec-isakmp dynamic mydynmap
!
!
!
!
!
interface FastEthernet0/0
 description WAN interface
 ip address 217.24.123.21 255.255.255.240
 ip nat outside
 ip virtual-reassembly
 speed 100
 duplex full
 crypto map mymap1
!
interface FastEthernet0/1
 description LAN interface
 ip address 10.1.9.100 255.255.0.0
 ip nat inside
 ip virtual-reassembly
 speed 100
 duplex full
!
!
no ip http server
no ip http secure-server
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 217.24.123.29
!
ip nat inside source list 1 interface FastEthernet0/0 overload
!
ip access-list extended access-list
no logging trap
access-list 101 permit ip 10.1.0.0 0.0.255.255 192.168.50.0 0.0.0.255
!
control-plane
!
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 password password
 login
line vty 5 1276
 password password
 login
!
```

```
!
end
```

## 4.4 Cisco Firmware Information

The Cisco configuration above was tested on a Cisco 1700 series router with version 12.2(17) firmware:

```
Cisco IOS Software, 3700 Software (C3725-ADVENTERPRISEK9-M), Version
12.4(15)T8, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Mon 01-Dec-08 19:46 by prod_rel_team

ROM: ROMMON Emulation Microcode
ROM: 3700 Software (C3725-ADVENTERPRISEK9-M), Version 12.4(15)T8, RELEASE
SOFTWARE (fc3)

Router uptime is 0 minutes
System returned to ROM by unknown reload cause - suspect
boot_data[BOOT_COUNT] 0x0, BOOT_COUNT 0, BOOTDATA 19
System image file is "tftp://255.255.255.255/unknown"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found
at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 3725 (R7000) processor (revision 0.1) with 249856K/12288K bytes of
memory.
Processor board ID FTX0945W0MY
R7000 CPU at 240MHz, Implementation 39, Rev 2.1, 256KB L2, 512KB L3 Cache
2 FastEthernet interfaces
DRAM configuration is 64 bits wide with parity enabled.
55K bytes of NVRAM.
16384K bytes of ATA System CompactFlash (Read/Write)

Configuration register is 0x2102

Router#
```