



Application Note 74

How to configure a GRE over IPsec Tunnel
between two Digi TransPort WR Routers

September 2020

Contents

1	Introduction	3
1.1	Outline	3
1.2	Assumptions	4
1.3	Corrections	4
1.4	Version	4
2	HQ site configuration (Responder)	5
2.1	WAN Interface configuration	5
2.2	LAN Interfaces configuration	7
2.3	IKE/IPsec configuration	9
2.4	GRE Tunnel configuration	13
2.5	Static Route configuration	14
3	Remote site configuration (Initiator)	15
3.1	WAN Interface configuration	15
3.2	LAN Interfaces configuration	16
3.3	IKE/IPsec configuration	17
3.4	GRE Tunnel configuration	21
3.5	Static Route configuration	22
4	Testing the GREoverIPsec Tunnel	24
4.1	Checking the Tunnel status	24
4.2	Testing the Traffic over the Tunnel	27
4.2.1	Configuring Analyser	27
4.2.2	Ping test to HQ LAN 1	29
4.2.3	Ping test to HQ LAN 2	33
5	Configuration Files	37
5.1	Responder Configuration (WR21)	37
5.2	Initiator Configuration (WR11)	40

1 INTRODUCTION

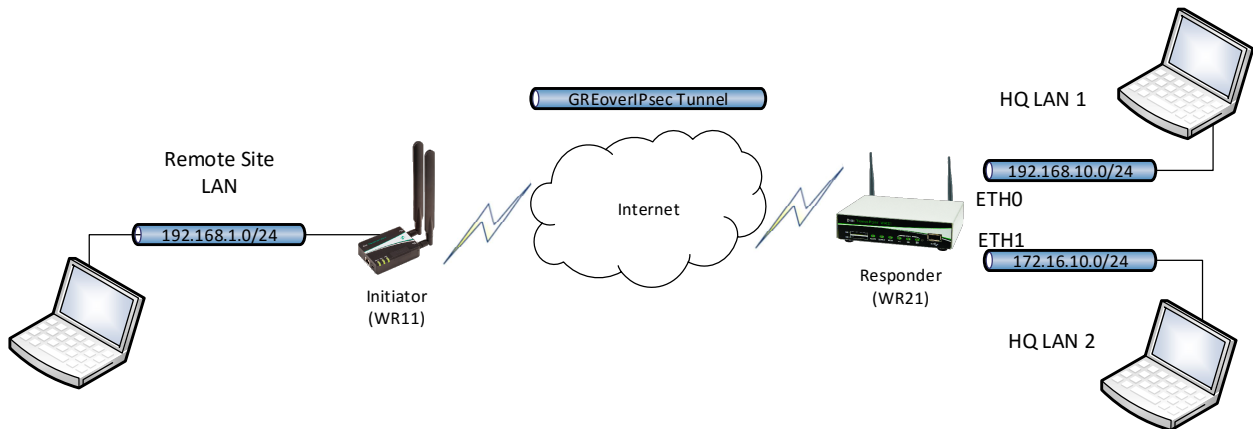
1.1 Outline

Using GRE over IPsec can be useful when there is the need to have diverse traffic on the IP sec tunnel, like IP multicast and dynamic routing protocols (you can find an example of configuring GRE over IPsec using BGP routing protocol here:

http://ftp1.digi.com/support/documentation/qn_020_gre_over_ipsec_with_bgp.pdf).

Another advantage of using GRE over IPsec is that it allows to have multiple non-contiguous subnet in a single tunnel, that would be not possible using only IPsec as in that case multiple tunnels, or a wider subnet including all of them, would be needed.

This document describes how to configure a GRE over IPsec tunnel between two TransPort routers, using static routes and multiple subnets, considering the following scenario:



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. It also assumes a basic ability to access and navigate a Digi Transport router and configure it with basic routing functions.

This application note applies only to:

Model: Digi Transport WR21 and WR11

Other Compatible Models: All Digi TransPort WR products (SarOS)

Firmware versions: This Application Note assume firmware 5.2.18.3 is used.

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.

1.3 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: tech.support@digicom.com.

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

1.4 Version

Version Number	Status
1.0	Published (October 2017)
1.1	Added date and minor fix (September 2020)

2 HQ SITE CONFIGURATION (RESPONDER)

The HQ site router will act as Responder of the GREoverIPsec tunnel, its configuration consists in configuring: the LAN/WAN interfaces (as per the diagram shown above), the IKE/IPsec settings, the GRE tunnel interface and the routing to the remote site LAN.

All these aspects will be explained in the subsections below.

2.1 WAN Interface configuration

In this example the WAN Interface of the responder is the Mobile one, so on the PPP 1 interface the IPsec must be enabled:

CONFIGURATION – NETWORK > INTERFACES > MOBILE

Interfaces

- Ethernet**
- Mobile**

Select a SIM to configure from the list below

Settings on this page apply to the selected SIM

SIM: 1 (PPP 1) ▼
IMSI: Unknown

Mobile Settings

Select the service plan and connection settings used in connecting to the mobile network.

Mobile Service Provider Settings

Service Plan / APN: internet.t-d1.de

☐ Use backup APN Retry the main APN after 0 minutes

SIM PIN: (Optional)

Confirm SIM PIN:

Username: (Optional)

Password: (Optional)

Confirm Password:

Mobile Connection Settings

☐ Re-establish connection when no data is received for a period of time

Mobile Network Settings

☒ Enable NAT on this interface

- ☒ IP address ☐ IP address and Port

☒ Enable IPsec on this interface

☐ Keep Security Associations (SAs) when this Mobile interface is disconnected

Use interface Default 0 for the source IP address of IPsec packets

☐ Enable the firewall on this interface

How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

Where:

Parameter	Setting	Description
Service Plan/APN	internet	Enter the APN of your mobile provider
Enable IPsec on this interface	✓	Enable IPsec on PPP 1 interface

2.2 LAN Interfaces configuration

On the LAN side of the HQ two ETH interfaces will be configured, in order to test the tunnel with two non-contiguous subnets:

CONFIGURATION – NETWORK > INTERFACES > ETHERNET > ETH 0

Configuration - Network > Interfaces > Ethernet > ETH 0

Interfaces

Ethernet

ETH 0

Description: HQ LAN 1

☐ Get an IP address automatically using DHCP

☒ Use the following settings

IP Address: 192.168.10.1

Mask: 255.255.255.0

Gateway:

DNS Server:

Secondary DNS Server:

Changes to these parameters may affect your browser connection

Advanced

QoS

VRRP

Apply

Where:

Parameter	Setting	Description
Description	HQ LAN 1	A memorable name for this Ethernet instance, to make it easier to identify. In this case this helps to distinguish between LAN1 and LAN2
Use the following settings	✓	Enables manual configuration of the IP addressing parameters
IP Address	192.168.10.1	This parameter specifies the IP address of this Ethernet port on LAN1
Mask	255.255.255.0	The subnet mask of the IP subnet to which the router is attached via this Ethernet port

CONFIGURATION – NETWORK > INTERFACES > ETHERNET > ETH 1

Configuration - Network > Interfaces > Ethernet > ETH 1

▼ Interfaces

▼ Ethernet

▶ ETH 0 - HQ LAN 1

▼ ETH 1 - HQ LAN 2

Description: HQ LAN 2

☐ Get an IP address automatically using DHCP

☒ Use the following settings

IP Address: 172.16.10.1

Mask: 255.255.255.0

Gateway:

DNS Server:

Secondary DNS Server:

Changes to these parameters may affect your browser connection

▶ Advanced

▶ QoS

▶ VRRP

Where:

Parameter	Setting	Description
Description	HQ LAN 2	A memorable name for this Ethernet instance, to make it easier to identify. In this case this helps to distinguish between LAN1 and LAN2
Use the following settings	✓	Enables manual configuration of the IP addressing parameters
IP Address	172.16.10.1	This parameter specifies the IP address of this Ethernet port on LAN2
Mask	255.255.255.0	The subnet mask of the IP subnet to which the router is attached via this Ethernet port

2.3 IKE/IPsec configuration

The IPsec tunnel must be configured with the following settings:

CONFIGURATION – NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC 0-9 > IPSEC 0

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

IP Routing/Forwarding

Virtual Private Networking (VPN)

IPsec

IPsec Tunnels

IPsec 0

Description: GREoverIPsec

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: 10.10.10.1

Mask: 255.255.255.255

☐ Use interface PPP 0

Remote LAN

☒ Use these settings for the remote LAN

IP Address: 10.10.10.2

Mask: 255.255.255.255

☐ Remote Subnet ID:

Use the following security on this tunnel

☐ Off ☒ Preshared Keys ☐ XAUTH Init Preshared Keys ☐ RSA Signatures ☐ XAUTH Init RSA

Our ID: HQsite

Our ID type: ☒ IKE ID ☐ FQDN ☐ User FQDN ☐ IPv4 Address

Remote ID: RemoteSite

Use AES (128 bit keys) encryption on this tunnel

Use SHA1 authentication on this tunnel

Use Diffie Hellman group 2

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

How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

Where:

Parameter	Setting	Description
Description	GREoverIPsec	Friendly name for the IPsec tunnel
Local LAN IP Address	10.10.10.1	Use this IP address for the local LAN subnet. This is usually the IP address of the router's Ethernet interface but in this case is a host IP address that does not actually exist (use an unused IP address from an unused subnet; it doesn't matter what is used). This one of the end points of the IPsec tunnel (so with mask /32 as below)
Local LAN Mask	255.255.255.255	Use this IP mask for the local LAN subnet.
Remote LAN IP Address	10.10.10.2	Use this IP address for the local LAN subnet. This is usually the IP address of the router's Ethernet interface but in this case is a host IP address that does not actually exist (use an unused IP address from an unused subnet; it doesn't matter what is used). This one of the end points of the IPsec tunnel (so with mask /32 as below)
Remote LAN Mask	255.255.255.255	Use this IP mask for the remote LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.
Use the following security on this tunnel	Preshared Key	Requires that both IPsec peers share a secret key, or password, that can be matched by and verified by both peers. To configure the PSK, a user will need configuring that matches the inbound ID of the remote peer and the PSK is configured using the password parameter. This is done via Configuration > Security > Users as shown below
Our ID	HQsite	When Aggressive mode is ON (as in this case), this parameter is a string of up to 20 characters. It is sent to the remote peer to identify the router
Our ID type	IKE ID	Defines how the remote peer is to process the Our ID configuration. Set to IKE ID.
Remote ID	RemoteSite	When Aggressive mode is ON (as in this case), this parameter is a string of up to 20 characters that identifies the remote peer. This setting should use the same text as the Our ID parameter in the remote peer's configuration.
Use () encryption on this tunnel	AES (128 bit keys)	The ESP encryption protocol to use with this IPsec tunnel
Use () Authentication on this tunnel	SHA1	The ESP authentication algorithm to use with this IPsec tunnel
Use Diffie Hellman group ()	2	The Diffie-Hellman (DH) group to use when negotiating new IPsec SAs.
Bring this tunnel up	On Demand	This controls how the IPsec tunnel is brought up, for the responder "On demand" option is chosen
If this tunnel is down and a packet is ready to be sent	Drop the Packet	Defines the action that is performed when the IPsec tunnel is down and a packet needs to be sent. For the responder the "drop the packet" option is chosen

How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

The IKE responder settings are set as follows:

CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IKE > IKE RESPONDER

▼ IKE

- ▶ IKE Debug
- ▶ IKE 0
- ▶ IKE 1
- ▼ IKE Responder
 - ☒ Enable IKE Responder
 - Accept IKE Requests with
 - Encryption: ☒ DES ☒ 3DES ☒ AES (128 bit) ☒ AES (192 bit) ☒ AES (256 bit)
 - Authentication: ☒ MD5 ☒ SHA1 ☒ SHA256
 - MODP Group between: 1 (768) and 14 (2048)
 - Renegotiate after: 8 hrs 0 mins 0 secs
 - ▶ Advanced

Apply

Where:

Parameter	Setting	Description
Enable IKE Responder	✓	Allows the router to respond to incoming IKE requests
Encryption	ALL ✓	The acceptable encryption algorithms
Authentication	ALL ✓	The acceptable authentication algorithms
MODP Group between x and y	1(768) and 14(1536)	The acceptable range for MODP group
Renegotiate after h hrs m mins s secs	8 hrs	How long the initial IKE Security Association will stay in force. When the IKE Security Association expires, any attempt to send packets to the remote system will result in IKE attempting to establish a new SA

Note: IKE settings can be narrowed down depending on the initiators needs.

How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

For the Pre-Shared key, a user needs to be configured with the Username as the ID of the initiator and the password as the Pre-Shared key:

CONFIGURATION – SECURITY > USERS > USER 10-14 > USER 10

The screenshot shows the configuration page for User 10. The breadcrumb trail at the top is "Configuration - Security > Users > User 10 - 14 > User 10". On the left, a tree view shows the navigation path: System > Users > User 0 - 9 > User 10 - 14 > User 10. The main configuration area contains the following fields: Username (set to "RemoteSite"), Password (masked with dots), Confirm Password (masked with dots), and Access Level (set to "None" via a dropdown menu). Below these fields is an "Advanced" section header. At the bottom of the page is an "Apply" button.

Where:

Parameter	Setting	Description
Username	RemoteSite	Name should match the Remote ID: value from Eroute 0
Password	****	Enter a password
Confirm Password	****	Re-enter the password
Access Level	None	This user will not be granted any admin access as only used as a pre-shared key

2.4 GRE Tunnel configuration

In order to configure the GRE Tunnel Interface, navigate to the following section and configure as explained below:

CONFIGURATION – NETWORK > INTERFACES > GRE > TUNNEL 0

Configuration - Network > Interfaces > GRE > Tunnel 0

Interfaces

- Ethernet
- Mobile
- GRE
 - Tunnel 0

Description: GRE Tunnel

IP Address: 10.10.0.1

Mask: 255.255.255.252

Source IP Address: ☐ Use interface ☒ Use IP Address 10.10.10.1

Destination IP Address or Hostname: 10.10.10.2

☐ Enable keepalives on this GRE tunnel

[Advanced](#)

Where:

Parameter	Setting	Description
Description	GRE Tunnel	A memorable name for this GRE instance, to make it easier to identify it.
IP address	10.10.0.1	The IP address of the virtual interface the tunnel uses. Use with the Mask parameter
Mask	255.255.255.252	Use this parameter with the IP address parameter to clarify the subnet in use on the virtual interface. This would normally be a 30-bit mask as this is a point-to-point link (255.255.255.252).
Source IP Address – Use IP Address	10.10.10.1	Specify a source address by manually assigning an address. This will be the same address configured in Eroute 0 Local LAN section
Destination IP Address or Hostname	10.10.10.2	This is IP address of the remote end of the tunnel. This will be the same address configured in Eroute 0 Remote LAN section

2.5 Static Route configuration

The last thing to configure is a static route so that the traffic directed to the Remote Site LAN will be routed into the GRE tunnel:

CONFIGURATION - NETWORK > IP ROUTING/FORWARDING > STATIC ROUTES > ROUTE 0

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

Interfaces

- ▶ Ethernet
- ▶ Mobile
- ▶ GRE
- ▶ Serial
- ▶ Advanced
- ▶ DHCP Server
- ▶ Network Services
- ▶ DNS Servers
- ▶ Dynamic DNS
- ▼ IP Routing/Forwarding
 - ▶ IP Routing
 - ▼ Static Routes
 - ▼ Route 0

Description:

Destination Network: Mask:

via

Gateway:

Interface:

Metric:

▶ Advanced

Where:

Parameter	Setting	Description
Description	RouteToRemoteSiteLAN	Friendly name for the static route
Destination Network-Mask	192.168.1.0-255.255.255.0	Remote Site LAN subnet with related mask
Interface	Tunnel 0	In order to route the traffic into the GRE tunnel, the "Tunnel 0" interface must be chosen

3 REMOTE SITE CONFIGURATION (INITIATOR)

The Remote site router will act as Initiator of the GREoverIPsec tunnel, its configuration consists in configuring: the LAN/WAN interfaces (as per the diagram shown above), the IKE/IPsec settings, the GRE tunnel interface and the routing to the remote site LAN.

All these aspects will be explained in the subsections below.

3.1 WAN Interface configuration

In this example the WAN Interface of the Initiator is the Mobile one, so on the PPP 1 interface the IPsec must be enabled:

CONFIGURATION – NETWORK > INTERFACES > MOBILE

Configuration - Network > Interfaces > Mobile

▼ Interfaces

- ▶ Ethernet
- ▼ Mobile

Select a SIM to configure from the list below

Settings on this page apply to the selected SIM

SIM: 1 (PPP 1) ▼

IMSI: 262010050453499

▼ Mobile Settings

Select the service plan and connection settings used in connecting to the mobile network.

Mobile Service Provider Settings

Service Plan / APN: internet.t-d1.de

☐ Use backup APN: Retry the main APN after 0 minutes

SIM PIN: (Optional)

Confirm SIM PIN:

Username: (Optional)

Password: (Optional)

Confirm Password:

Mobile Connection Settings

☐ Re-establish connection when no data is received for a period of time

Mobile Network Settings

☒ Enable NAT on this interface

☒ IP address ☐ IP address and Port

☒ Enable IPsec on this interface

☐ Keep Security Associations (SAs) when this Mobile interface is disconnected

Use interface Default 0 for the source IP address of IPsec packets

☐ Enable the firewall on this interface

Where:

Parameter	Setting	Description
Service Plan/APN	internet	Enter the APN of your mobile provider
Enable IPsec on this interface	✓	Enable IPsec on PPP 1 interface

3.2 LAN Interfaces configuration

On the LAN side of the Remote site. One ETH interface will be configured:

CONFIGURATION – NETWORK > INTERFACES > ETHERNET > ETH 0

Configuration - Network > Interfaces > Ethernet > ETH 0

▼ Interfaces

▼ Ethernet

▼ ETH 0

Description: RemoteSiteLAN

☐ Get an IP address automatically using DHCP

☒ Use the following settings

IP Address: 192.168.1.1

Mask: 255.255.255.0

Gateway:

DNS Server:

Secondary DNS Server:

Changes to these parameters may affect your browser connection

▶ Advanced

▶ QoS

▶ VRRP

Where:

Parameter	Setting	Description
Description	RemoteSiteLAN	A memorable name for this Ethernet instance, to make it easier to identify.
Use the following settings	✓	Enables manual configuration of the IP addressing parameters
IP Address	192.168.1.1	This parameter specifies the IP address of this Ethernet port on LAN0
Mask	255.255.255.0	The subnet mask of the IP subnet to which the router is attached via this Ethernet port

3.3 IKE/IPsec configuration

The IPsec tunnel must be configured with the following settings:

CONFIGURATION – NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC 0-9 > IPSEC 0

[Configuration - Network > Virtual Private Networking \(VPN\) > IPsec > IPsec Tunnels > IPsec 0](#)

Description:

The IP address or hostname of the remote unit

Use as a backup unit

Local LAN	Remote LAN
<input checked="" type="radio"/> Use these settings for the local LAN IP Address: <input type="text" value="10.10.10.2"/> Mask: <input type="text" value="255.255.255.255"/>	<input checked="" type="radio"/> Use these settings for the remote LAN IP Address: <input type="text" value="10.10.10.1"/> Mask: <input type="text" value="255.255.255.255"/>
<input type="radio"/> Use interface <input type="text" value="PPP"/> <input type="text" value="0"/>	<input type="radio"/> Remote Subnet ID: <input type="text"/>

Use the following security on this tunnel

☐ Off ☒ Preshared Keys ☐ XAUTH Init Preshared Keys ☐ RSA Signatures ☐ XAUTH Init RSA

Our ID:

Our ID type: ☒ IKE ID ☐ FQDN ☐ User FQDN ☐ IPv4 Address

Remote ID:

Use encryption on this tunnel

Use authentication on this tunnel

Use Diffie Hellman group

Use IKE to negotiate this tunnel

Use IKE configuration:

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 this tunnel down if it is idle for hrs mins secs

Renew the tunnel after

hrs mins secs

KBytes of traffic

How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

Where:

Parameter	Setting	Description
Description	GREoverIPsec	Friendly name for the IPsec tunnel
The IP address or hostname of the remote unit	37.85.98.211	The IP address or hostname of the remote IPsec peer that a VPN will be initiated to.
Local LAN IP Address	10.10.10.2	Use this IP address for the local LAN subnet. This is usually the IP address of the router's Ethernet interface but in this case is a host IP address that does not actually exist (use an unused IP address from an unused subnet; it doesn't matter what is used). This one of the end points of the IPsec tunnel (so with mask /32 as below)
Local LAN Mask	255.255.255.255	Use this IP mask for the local LAN subnet.
Remote LAN IP Address	10.10.10.1	Use this IP address for the local LAN subnet. This is usually the IP address of the router's Ethernet interface but in this case is a host IP address that does not actually exist (use an unused IP address from an unused subnet; it doesn't matter what is used). This one of the end points of the IPsec tunnel (so with mask /32 as below)
Remote LAN Mask	255.255.255.255	Use this IP mask for the remote LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.
Use the following security on this tunnel	Preshared Key	Requires that both IPsec peers share a secret key, or password, that can be matched by and verified by both peers. To configure the PSK, a user will need configuring that matches the inbound ID of the remote peer and the PSK is configured using the password parameter. This is done via Configuration > Security > Users as shown below
Our ID	RemoteSite	When Aggressive mode is ON (as in this case), this parameter is a string of up to 20 characters. It is sent to the remote peer to identify the router
Our ID type	IKE ID	Defines how the remote peer is to process the Our ID configuration. Set to IKE ID.
Remote ID	HQSite	When Aggressive mode is ON (as in this case), this parameter is a string of up to 20 characters that identifies the remote peer. This setting should use the same text as the Our ID parameter in the remote peer's configuration.
Use () encryption on this tunnel	AES (128 bit keys)	The ESP encryption protocol to use with this IPsec tunnel
Use () Authentication on this tunnel	SHA1	The ESP authentication algorithm to use with this IPsec tunnel
Use Diffie Hellman group()	2	The (DH) group to use when negotiating new IPsec SAs.
Bring this tunnel up	All the Time	This controls how the IPsec tunnel is brought up, for the Initiator "All the time" option is chosen
If this tunnel is down and a packet is ready to be sent	Bring the tunnel Up	Defines the action that is performed when the IPsec tunnel is down and a packet needs to be sent. For the Initiator the "Bring the tunnel up" option is chosen

How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

The IKE responder settings are set as follows:

CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IKE > IKE RESPONDER

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

- Interfaces
- DHCP Server
- Network Services
- DNS Servers
- Dynamic DNS
- IP Routing/Forwarding
- 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 ☐ SHA256

Mode: ☐ Main ☒ Aggressive

MODP Group for Phase 1: 2 (1024)

MODP Group for Phase 2: 2 (1024)

Renegotiate after 8 hrs 0 mins 0 secs

Advanced

Apply

Where:

Parameter	Setting	Description
Encryption	AES (128 bit)	The encryption algorithm to be used for IKE exchanges over the IP connection
Authentication	SHA1	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
MODP Group for Phase 2	2 (1024)	The minimum width of the numeric field used in the calculations for phase 2 of the security exchange.

How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

For the Pre-Shared key, a user needs to be configured with the Username as the ID of the responder and the password as the Pre-Shared key:

CONFIGURATION – SECURITY > USERS > USER 10-14 > USER 10

The screenshot shows the configuration page for User 10. The breadcrumb trail at the top is "Configuration - Security > Users > User 10 - 14 > User 10". The left sidebar shows a tree structure: "System" (expanded), "Users" (expanded), "User 0 - 9" (expanded), "User 10 - 14" (expanded), and "User 10" (selected). The main configuration area contains the following fields:

- Username: HQsite
- Password: [masked with dots]
- Confirm Password: [masked with dots]
- Access Level: None (dropdown menu)

At the bottom of the configuration area is a link labeled "Advanced".

Parameter	Setting	Description
Username	HQsite	Name should match the Remote ID: value from Route 0
Password	****	Enter a password
Confirm Password	****	Re-enter the password
Access Level	None	This user will not be granted any admin access as only used as a pre-shared key

3.4 GRE Tunnel configuration

In order to configure the GRE Tunnel Interface, navigate to the following section and configure as explained below:

CONFIGURATION – NETWORK > INTERFACES > GRE > TUNNEL 0

Configuration - Network > Interfaces > GRE > Tunnel 0

Interfaces

- Ethernet
- Mobile
- GRE
 - Tunnel 0

Description: GRE tunnel

IP Address: 10.10.0.2

Mask: 255.255.255.252

Source IP Address: ☐ Use interface ☐ Use IP Address 10.10.10.2

Destination IP Address or Hostname: 10.10.10.1

☐ Enable keepalives on this GRE tunnel

[Advanced](#)

Where:

Parameter	Setting	Description
Description	GRE Tunnel	A memorable name for this GRE instance, to make it easier to identify it.
IP address	10.10.0.2	The IP address of the virtual interface the tunnel uses. Use with the Mask parameter
Mask	255.255.255.252	Use this parameter with the IP address parameter to clarify the subnet in use on the virtual interface. This would normally be a 30-bit mask as this is a point-to-point link (255.255.255.252).
Source IP Address – Use IP Address	10.10.10.2	Specify a source address by manually assigning an address. This will be the same address configured in Eroute 0 Local LAN section
Destination IP Address or Hostname	10.10.10.1	This is IP address of the remote end of the tunnel. This will be the same address configured in Eroute 0 Remote LAN section

3.5 Static Route configuration

The last thing to configure is two static routes so that the traffic directed to both HQ LANs will be routed into the same GREoverIpsec tunnel:

CONFIGURATION - NETWORK > IP ROUTING/FORWARDING > STATIC ROUTES > ROUTE 0

The screenshot shows the configuration page for a static route named 'Route 0'. The breadcrumb trail at the top is 'Configuration - Network > IP Routing/Forwarding > Static Routes > Route 0'. On the left, a tree view shows 'Network Services' expanded, with 'Static Routes' and 'Route 0' selected. The main configuration area includes: 'Description' set to 'ToHQLAN1'; 'Destination Network' set to '192.168.10.0' and 'Mask' set to '255.255.255.0'; 'via' section with 'Gateway' empty and 'Interface' set to 'Tunnel 0'; and 'Metric' set to '1'. An 'Advanced' tab is visible at the bottom.

Where:

Parameter	Setting	Description
Description	ToHQLAN1	Friendly name for the static route
Destination Network-Mask	192.168.10.0-255.255.255.0	HQ LAN 1 subnet with related mask
Interface	Tunnel 0	In order to route the traffic into the GRE tunnel, the "Tunnel 0" interface must be chosen

CONFIGURATION - NETWORK > IP ROUTING/FORWARDING > STATIC ROUTES > ROUTE 1

Configuration - Network > IP Routing/Forwarding > Static Routes > Route 1

- Interfaces
- DHCP Server
- Network Services
- DNS Servers
- Dynamic DNS
- IP Routing/Forwarding
 - IP Routing
 - Static Routes
 - Route 0
 - Route 1

Description: ToHQLAN2

Destination Network: 172.16.10.0 Mask: 255.255.255.0

via

Gateway:

Interface: Tunnel 0

Metric: 1

Advanced

Where:

Parameter	Setting	Description
Description	ToHQLAN2	Friendly name for the static route
Destination Network-Mask	172.16.10.0-255.255.255.0	HQ LAN 2 subnet with related mask
Interface	Tunnel 0	In order to route the traffic into the GRE tunnel, the "Tunnel 0" interface must be chosen

4 TESTING THE GREOVERIPSEC TUNNEL

4.1 Checking the Tunnel status

If all is correctly configured on both sides, the tunnel should go UP and that can be checked in the following section of the WEB UI:

Initiator:

MANAGEMENT - EVENTLOG

Management - Event Log

```
12:36:06, 04 Jul 2017,Erout 0 VPN up peer: HQsite
12:36:06, 04 Jul 2017,New IPsec SA created by HQsite
12:36:06, 04 Jul 2017,(8) IKE Notification: Initial Contact,RX
12:36:06, 04 Jul 2017,(9) IKE Notification: Responder Lifetime,RX
12:36:06, 04 Jul 2017,(8) New Phase 2 IKE Session 37.85.98.211,Initiator
12:36:06, 04 Jul 2017,(7) IKE Keys Negotiated. Peer: HQsite
12:36:05, 04 Jul 2017,(7) New Phase 1 IKE Session 37.85.98.211,Initiator
12:36:05, 04 Jul 2017,IKE Request Received From Erout 0
```

MANAGEMENT - CONNECTIONS > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS

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	VIP	
0	37.85.98.211	10.10.10.2/32	10.10.10.1/32	N/A	SHA1	AES(128)	N/A	0	0	28747	PPP 1	N/A	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	VIP	
0	37.85.98.211	10.10.10.2/32	10.10.10.1/32	N/A	SHA1	AES(128)	N/A	0	0	28747	PPP 1	N/A	Remove

[Remove All](#)

MANAGEMENT - NETWORK STATUS > INTERFACES > GRE

Management - Network Status > Interfaces > GRE

Interfaces

Ethernet

Mobile

GRE

#	Description	Oper. Status	IP Address	Mask	Source	Destination
0	GRE tunnel	Up	10.10.0.2	255.255.255.252	10.10.10.2	10.10.10.1

[Refresh](#)

How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

MANAGEMENT - NETWORK STATUS > IP ROUTING TABLE

Management - Network Status > IP Routing Table

▸ Interfaces
▸ IP Statistics
▼ IP Routing Table

Destination	Gateway	Metric	Protocol	Idx	Interface	Status
10.10.0.0/30	10.10.0.2	1	Local	-	TUN 0	UP
37.80.17.59/32	37.80.17.59	1	Local	-	PPP 1	UP
172.16.10.0/24	10.10.0.2	2	Static	1	TUN 0	UP
192.168.1.0/24	192.168.1.1	1	Local	-	ETH 0	UP
192.168.10.0/24	10.10.0.2	2	Static	0	TUN 0	UP

Default Routes

Destination	Gateway	Metric	Protocol	Idx	Interface	Status
0.0.0.0/0	37.80.17.59	2	Static	0	PPP 1	UP

Refresh Toggle Src Addr

Responder (HQ):

MANAGEMENT - EVENTLOG

Management - Event Log

```
14:36:03, 04 Jul 2017, (3) IKE SA Removed. Peer: RemoteSite, Successful Negotiation
14:36:01, 04 Jul 2017, Route 0 VPN up peer: RemoteSite
14:36:01, 04 Jul 2017, New IPsec SA created by RemoteSite
14:36:01, 04 Jul 2017, (3) IKE Notification: Initial Contact, RX
14:36:01, 04 Jul 2017, (3) New Phase 2 IKE Session 37.80.17.59, Responder
14:36:00, 04 Jul 2017, (1) IKE Keys Negotiated. Peer: RemoteSite
14:36:00, 04 Jul 2017, (1) New Phase 1 IKE Session 37.80.17.59, Responder
```

MANAGEMENT - CONNECTIONS > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS

▼ 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	VIP
0	37.80.17.59	10.10.10.1/32	10.10.10.2/32	N/A	SHA1	AES(128)	N/A	0	0	28703	PPP 1	N/A

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	VIP
0	37.80.17.59	10.10.10.1/32	10.10.10.2/32	N/A	SHA1	AES(128)	N/A	0	0	28703	PPP 1	N/A

Remove All

How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

MANAGEMENT - NETWORK STATUS > INTERFACES > GRE

[Management - Network Status](#) > [Interfaces](#) > [GRE](#)

▼ Interfaces

▶ Ethernet

▶ Mobile

▼ GRE

#	Description	Oper. Status	IP Address	Mask	Source	Destination
0	GRE Tunnel	Up	10.10.0.1	255.255.255.252	10.10.10.1	10.10.10.2

Refresh

MANAGEMENT - NETWORK STATUS > IP ROUTING TABLE

[Management - Network Status](#) > [IP Routing Table](#)

▶ Interfaces

▶ IP Statistics

▼ IP Routing Table

Destination	Gateway	Metric	Protocol	Idx	Interface	Status
10.10.0.0/30	10.10.0.1	1	Local	-	TUN 0	UP
37.85.98.208/29	37.85.98.211	1	Local	-	PPP 1	UP
172.16.10.0/24	172.16.10.0	1	Local	-	ETH 1	UP
192.168.1.0/24	10.10.0.1	2	Static	0	TUN 0	UP
192.168.10.0/24	192.168.10.1	1	Local	-	ETH 0	UP

Default Routes

Destination	Gateway	Metric	Protocol	Idx	Interface	Status
0.0.0.0/0	37.85.98.211	2	Static	0	PPP 1	UP

Refresh Toggle Src Addr

4.2 Testing the Traffic over the Tunnel

In order to test that the traffic between the RemoteSite LAN and both HQ LANs is correctly transported through the GREoverIPsec tunnel, a simple ping test can be done from a Laptop on the Remote Site LAN to two hosts in the two different HQ LANs.

4.2.1 Configuring Analyser

In order to get a packet trace of the test traffic, the analyser on the Remo Site router must be configured as follows:

MANAGEMENT - ANALYSER > SETTINGS

Management - Analyser > Settings

Settings

- ☒ **Enable Analyser**
- Maximum packet capture size: bytes
- Log size: 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 3 ☐ ASY 4 ☐ ASY 5
 - ☐ ASY 6 ☐ ASY 7 ☐ ASY 8 ☐ ASY 9 ☐ ASY 10
 - ☐ ASY 11 ☐ ASY 12 ☐ ASY 13 ☐ ASY 14 ☐ ASY 15
 - ☐ ASY 16 ☐ ASY 17 ☐ W-WAN
 -
- Ethernet Interfaces**
 - ☐ ETH 0 ☐ ETH 1 ☐ ETH 2 ☐ ETH 3 ☐ ETH 4
 - ☐ ETH 5 ☐ ETH 6 ☐ ETH 7 ☐ ETH 8 ☐ ETH 9
 -
- PPP Interfaces**
 - ☐ PPP 0 ☐ PPP 1 ☐ PPP 2 ☐ PPP 3 ☐ PPP 4
 - ☐ PPP 5 ☐ PPP 6 ☐ PPP 7
 -
- IP Sources**
 - ☒ **ETH 0** ☐ ETH 1 ☐ ETH 2 ☐ ETH 3 ☐ ETH 4
 - ☐ ETH 5 ☐ ETH 6 ☐ ETH 7 ☐ ETH 8 ☐ ETH 9
 - ☐ OVPN 0 ☐ OVPN 1 ☐ OVPN 2
 - ☐ PPP 0 ☒ **PPP 1** ☐ PPP 2 ☐ PPP 3 ☐ PPP 4
 - ☐ PPP 5 ☐ PPP 6 ☐ PPP 7
 -

How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

Where:

Parameter	Setting	Description
Enable Analyser	✓	If ticked will reveal all Analyser settings options
Maximum packet capture size	1500	The number of bytes that are captured and stored for each packet. If the packet is bigger than the configured size, the packet is truncated. The usual value used is 1500
Log Size	180	The maximum size of the pseudo file ana.txt for storing the captured data packets. Once the maximum size is reached, the oldest captured data packets are overwritten when new packets are captured. Usually the maximum value is chosen: 180Kb (but the data is compressed so more than 180Kb of trace data will be captured)
Protocol layers	Layer 3 (Network)	The check-boxes under this heading specify which protocol layers are captured and included in the Analyser trace. In this case the the Network Layer (Layer 3) is chosen.
IP Sources		Selects the IP sources over which packets are captured and included in the Analyser trace. These sources include IP packet transmitted and received over Ethernet, PPP and OpenVPN (OVPN) interfaces.
ETH 0	✓	LAN Interface , in this example ETH 0 is used
PPP 1	✓	WAN Interface, in this example PPP 1 is used

4.2.2 Ping test to HQ LAN 1

From the command prompt of a laptop in the Remote Site LAN, try a ping to a host in the HQ LAN1:

```
Administrator: Command Prompt
C:\windows\system32>ping 192.168.10.100 -n 1

Pinging 192.168.10.100 with 32 bytes of data:
Reply from 192.168.10.100: bytes=32 time=1296ms TTL=126

Ping statistics for 192.168.10.100:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1296ms, Maximum = 1296ms, Average = 1296ms

C:\windows\system32>
```

Checking the trace in the **MANAGEMENT - ANALYSER > TRACE** section, it is shown that the ECHO REQ/REPLY packets are correctly encapsulated in the tunnel (GRE/ESP packets) sent/received via the PPP connection:

-----	4-7-2017	12:47:38.770	-----	
45	00	00	3C 25 F3 00 00 80 01 87 B5 C0 A8 01 64	E..<%.....d
C0	A8	0A 64 08 00 27 17 00 01 26 44 61 62 63 64		...d...'...&Dabcd
65	66	67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74		efghijklmnopqrst
75	76	77 61 62 63 64 65 66 67 68 69		uvwabcdefghi
IP (In) From REM TO LOC				
45		IP Ver:	4	
		Hdr Len:	20	
00		TOS:	Routine	
		Delay:	Normal	
		Throughput:	Normal	
		Reliability:	Normal	
00	3C	Length:	60	
25	F3	ID:	9715	
00	00	Frag Offset:	0	
		Congestion:	Normal	
			May Fragment	
			Last Fragment	
80		TTL:	128	
01		Proto:	ICMP	
87	B5	Checksum:	34741	
C0	A8 01 64	Src IP:	192.168.1.100	
C0	A8 0A 64	Dst IP:	192.168.10.100	
ICMP:				
08		Type:	ECHO REQ	
00		Code:	0	
27	17	Checksum:	5927	

How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

```

-----
----- 4-7-2017 12:47:38.770 -----
45 00 00 54 00 16 00 00 F9 2F 99 4E 0A 0A 0A 02      E..T...../.N....
0A 0A 0A 01 00 00 08 00 45 00 00 3C 25 F3 00 00      .....E..<%...
7F 01 88 B5 C0 A8 01 64 C0 A8 0A 64 08 00 27 17      .....d...d..'.
00 01 26 44 61 62 63 64 65 66 67 68 69 6A 6B 6C      ..&Dabcdefghijkl
6D 6E 6F 70 71 72 73 74 75 76 77 61 62 63 64 65      mnopqrstuvwxyzabcde
66 67 68 69                                           fghi

ER 0-HQsite From LOC TO REM      IFACE: PPP 1
45                                IP Ver:          4
                                Hdr Len:          20
00                                TOS:              Routine
                                Delay:             Normal
                                Throughput:         Normal
                                Reliability:         Normal
00 54                            Length:           84
00 16                            ID:               22
00 00                            Frag Offset:      0
                                Congestion:         Normal
                                May Fragment
                                Last Fragment
F9                                TTL:             249
2F                                Proto:           GRE
99 4E                            Checksum:        39246
0A 0A 0A 02                      Src IP:          10.10.10.2
0A 0A 0A 01                      Dst IP:          10.10.10.1
-----
----- 4-7-2017 12:47:38.770 -----
45 00 00 98 00 16 00 00 FA 32 01 6B 25 50 11 3B      E.....2.k%P.;
25 55 62 D3 E4 15 10 C3 00 00 00 16 22 AE 55 D4      %Ub.....".U.
70 B8 16 37 1A B5 05 1E AA DC 43 C2 BB 6C 1B 6C      p..7.....C..l.l
38 48 6E F2 10 59 12 77 6B 79 62 4C DD 10 BA FB      8Hn..Y.wkybL....
35 1B 6B E6 2C 73 4B 05 00 80 69 F8 CF 5D 75 79      5.k.,sK...i..]uy
AF F5 BA 24 B3 9B 30 02 3B 55 63 43 37 62 3A 17      ...$.0.;UcC7b:.
9A FE C4 D8 5B 37 23 FE AF B6 A0 AC 42 1E 8D 19      ....[7#.....B...
12 11 6D C5 04 90 78 D4 C0 32 98 F3 7E 04 DD 25      ..m...x..2...~...%
17 69 7F 98 F7 E1 45 60 1B A3 8A 26 B5 41 00 34      .i....E`...&.A.4
B8 A9 22 3E AC 83 1E 31                                ..">...1

IP (Final) From LOC TO REM      IFACE: PPP 1
45                                IP Ver:          4
                                Hdr Len:          20
00                                TOS:              Routine
                                Delay:             Normal
                                Throughput:         Normal
                                Reliability:         Normal
00 98                            Length:           152
00 16                            ID:               22
00 00                            Frag Offset:      0
                                Congestion:         Normal
                                May Fragment
                                Last Fragment
FA                                TTL:             250
32                                Proto:           ESP

```

How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

```

01 6B          Checksum:      363
25 50 11 3B    Src IP:       37.80.17.59
25 55 62 D3    Dst IP:       37.85.98.211
-----
----- 4-7-2017 12:47:40.320 -----
45 00 00 98 00 15 00 00 F4 32 07 6C 25 55 62 D3  E.....2.l%Ub.
25 50 11 3B 36 44 13 D3 00 00 00 15 7D F5 8D 5D  %P.;6D.....}...]
6E FF 03 A0 35 9C E8 A4 11 C7 BC 4A D0 6D 99 D7  n...5.....J.m..
D7 BE 5A 32 98 F3 E5 90 3C C8 B9 B0 D0 55 85 68  ..Z2.....<....U.h
0E BD 7D 3A C9 EB 4F B9 C5 AF CF 17 E5 32 35 41  ..}:..O.....25A
E3 10 5D 9D 70 D7 1B 49 DA F8 48 85 0C F5 1D B4  ..].p..I..H.....
AF F9 F6 0A 15 10 6D 5A BD C4 ED 35 12 E4 99 77  ....mZ...5...w
4E 77 CF 0C 14 E9 41 3D 32 4C 5B BF EE 8A BD 93  Nw....A=2L[.....
4F 92 C0 9E 18 A3 D0 D3 51 EB BE DF 4C 1D B8 35  O.....Q...L...5
92 EC 76 C7 FA 12 1C 86  ..v.....

IP (In) From REM TO LOC      IFACE: PPP 1
45          IP Ver:          4
          Hdr Len:          20
00          TOS:             Routine
          Delay:             Normal
          Throughput:        Normal
          Reliability:        Normal
00 98       Length:          152
00 15       ID:              21
00 00       Frag Offset:     0
          Congestion:        Normal
          May Fragment
          Last Fragment
F4          TTL:             244
32          Proto:           ESP
07 6C       Checksum:        1900
25 55 62 D3 Src IP:          37.85.98.211
25 50 11 3B Dst IP:          37.80.17.59
-----
----- 4-7-2017 12:47:40.320 -----
45 00 00 54 00 15 00 00 F9 2F 99 4F 0A 0A 0A 01  E..T...../.O....
0A 0A 0A 02 00 00 08 00 45 00 00 3C 13 B7 00 00  .....E..<....
7F 01 9A F1 C0 A8 0A 64 C0 A8 01 64 00 00 2F 17  .....d...d.../.
00 01 26 44 61 62 63 64 65 66 67 68 69 6A 6B 6C  ..&Dabcdefghijkl
6D 6E 6F 70 71 72 73 74 75 76 77 61 62 63 64 65  mnopqrstuvwxyz
66 67 68 69  fghi

IP (Cont) From REM TO LOC    IFACE: PPP 1
45          IP Ver:          4
          Hdr Len:          20
00          TOS:             Routine
          Delay:             Normal
          Throughput:        Normal
          Reliability:        Normal
00 54       Length:          84
00 15       ID:              21
00 00       Frag Offset:     0
          Congestion:        Normal
          May Fragment

```

How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

```

F9          TTL:          Last Fragment
2F          Proto:        GRE
99 4F       Checksum:     39247
0A 0A 0A 01 Src IP:       10.10.10.1
0A 0A 0A 02 Dst IP:       10.10.10.2
-----
----- 4-7-2017 12:47:40.320 -----
45 00 00 3C 13 B7 00 00 7E 01 9B F1 C0 A8 0A 64  E..<....~.....d
C0 A8 01 64 00 00 2F 17 00 01 26 44 61 62 63 64  ...d.../...&Dabcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74  efghijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69             uvwabcdefghi

IP (Final) From LOC TO REM  IFACE: ETH 0
45          IP Ver:         4
          Hdr Len:         20
00          TOS:            Routine
          Delay:           Normal
          Throughput:      Normal
          Reliability:     Normal
00 3C       Length:        60
13 B7       ID:            5047
00 00       Frag Offset:   0
          Congestion:      Normal
          May Fragment
          Last Fragment
7E          TTL:           126
01          Proto:         ICMP
9B F1       Checksum:      39921
C0 A8 0A 64 Src IP:        192.168.10.100
C0 A8 01 64 Dst IP:        192.168.1.100
ICMP:
00          Type:          ECHO REPLY
00          Code:          0
2F 17       Checksum:      5935
-----

```


4.2.3 Ping test to HQ LAN 2

From the command prompt of a laptop in the Remote Site LAN, try a ping to a host in the HQ LAN2:

```

Administrator: Command Prompt
C:\windows\system32>ping 172.16.10.100 -n 1

Pinging 172.16.10.100 with 32 bytes of data:
Reply from 172.16.10.100: bytes=32 time=1647ms TTL=126

Ping statistics for 172.16.10.100:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1647ms, Maximum = 1647ms, Average = 1647ms

C:\windows\system32>
    
```

Checking the trace in the **MANAGEMENT - ANALYSER > TRACE** section, also for the traffic directed to the HQ LAN 2, it is shown that the ECHO REQ/REPLY packets are correctly encapsulated in the tunnel (GRE/ESP packets) sent/received via the PPP connection:

-----	4-7-2017	12:57:13.880	-----	
45	00 00 3C 08 3A 00 00 80 01	BA 06 C0 A8 01 64		E..<.:.....d
AC	10 0A 64 08 00 27 0B 00 01	26 50 61 62 63 64		...d..'...&Pabcd
65	66 67 68 69 6A 6B 6C 6D 6E	6F 70 71 72 73 74		efghijklmnopqrst
75	76 77 61 62 63 64 65 66 67	68 69		uvwabcdefghi
IP (In) From REM TO LOC		IFACE: ETH 0		
45	IP Ver:	4		
	Hdr Len:	20		
00	TOS:	Routine		
	Delay:	Normal		
	Throughput:	Normal		
	Reliability:	Normal		
00 3C	Length:	60		
08 3A	ID:	2106		
00 00	Frag Offset:	0		
	Congestion:	Normal		
		May Fragment		
		Last Fragment		
80	TTL:	128		
01	Proto:	ICMP		
BA 06	Checksum:	47622		
C0 A8 01 64	Src IP:	192.168.1.100		
AC 10 0A 64	Dst IP:	172.16.10.100		
ICMP:				
08	Type:	ECHO REQ		

How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

```

00          Code:      0
27 0B       Checksum:  2855
-----
----- 4-7-2017 12:57:13.880 -----
45 00 00 54 00 26 00 00 F9 2F 99 3E 0A 0A 0A 02    E..T.&.../.>....
0A 0A 0A 01 00 00 08 00 45 00 00 3C 08 3A 00 00    .....E..<:...
7F 01 BB 06 C0 A8 01 64 AC 10 0A 64 08 00 27 0B    .....d...d..'.
00 01 26 50 61 62 63 64 65 66 67 68 69 6A 6B 6C    ..&Pabcdefghijkl
6D 6E 6F 70 71 72 73 74 75 76 77 61 62 63 64 65    mnopqrstuvwxyzabcde
66 67 68 69                                         fghi

ER 0-HQsite From LOC TO REM    IFACE: PPP 1
45          IP Ver:      4
          Hdr Len:      20
00          TOS:        Routine
          Delay:        Normal
          Throughput:    Normal
          Reliability:    Normal
00 54       Length:      84
00 26       ID:          38
00 00       Frag Offset: 0
          Congestion:    Normal
          May Fragment
          Last Fragment
F9          TTL:        249
2F          Proto:      GRE
99 3E       Checksum:    39230
0A 0A 0A 02 Src IP:    10.10.10.2
0A 0A 0A 01 Dst IP:    10.10.10.1
-----
----- 4-7-2017 12:57:13.880 -----
45 00 00 98 00 26 00 00 FA 32 01 5B 25 50 11 3B    E....&...2.[%P.;
25 55 62 D3 E4 15 10 C3 00 00 00 26 CB C3 14 15    %Ub.....&....
B9 73 A2 39 99 0B BE E7 B6 F5 8A 0C DC 96 38 5C    .s.9.....8\
E4 BE 48 3E 48 6B DF 68 D9 14 D6 AD A9 C9 74 68    ..H>Hk.h.....th
F1 A0 DC E5 CB 66 64 67 98 0D 1E 7F 43 72 8B 23    .....fdg....Cr.#
C4 C0 58 23 17 B2 2F 9D 10 52 92 0E 3A 7C 0E F4    ..X#.../.R...|..
A0 C2 92 51 BC CE 7B 87 BD 83 C6 C6 DF 96 EC C7    ...Q...{.....
BA 1F 4C C7 04 2F D6 F6 CB 35 8F F2 5E 86 9F A4    ..L.../...5...^...
B1 33 15 7F 7E C4 E6 33 04 BF 78 B5 EA 3C C3 6F    .3...~...3...x...<.o
3A 7D A6 0D 09 0E 50 BF                          :}....P.

IP (Final) From LOC TO REM    IFACE: PPP 1
45          IP Ver:      4
          Hdr Len:      20
00          TOS:        Routine
          Delay:        Normal
          Throughput:    Normal
          Reliability:    Normal
00 98       Length:      152
00 26       ID:          38
00 00       Frag Offset: 0
          Congestion:    Normal
          May Fragment
          Last Fragment

```

How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

```

FA          TTL:          250
32          Proto:        ESP
01 5B       Checksum:     347
25 50 11 3B  Src IP:      37.80.17.59
25 55 62 D3  Dst IP:      37.85.98.211
-----
----- 4-7-2017 12:57:15.530 -----
45 00 00 98 00 1D 00 00 F4 32 07 64 25 55 62 D3  E.....2.d%Ub.
25 50 11 3B 36 44 13 D3 00 00 00 1D 7F D3 A4 E1  %P.;6D.....
2D C5 54 25 37 E0 9E 16 47 36 24 5E 57 42 65 AF  -.T%7...G6$^WBe.
BF 63 9A 23 02 5A 6A 15 89 3A 9E B3 F1 3F 46 A5  .c.#.Zj.....?F.
F3 05 AE EB 71 46 15 7E BC 9B 45 CB 95 5D 15 62  ....qF.~...E...].b
02 E9 80 2B EB 2E 78 48 E4 52 31 A7 89 B4 11 12  ...+...xH.Rl....
23 4E C1 A3 08 BD FA 95 13 59 5C 81 13 1F BE E6  #N.....Y\.....
2A 02 AE 27 DB 35 8A F4 81 60 D5 98 32 83 85 24  *...'5....`.2...$
58 CB 7D B7 D1 1F EE E7 DF DF C9 86 75 CE F3 CB  X.}.....u...
89 EE 07 BF 1A 78 6D 0A  ....xm.

IP (In) From REM TO LOC      IFACE: PPP 1
45          IP Ver:          4
          Hdr Len:          20
00          TOS:             Routine
          Delay:             Normal
          Throughput:        Normal
          Reliability:        Normal
00 98       Length:          152
00 1D       ID:              29
00 00       Frag Offset:     0
          Congestion:        Normal
          May Fragment
          Last Fragment
F4          TTL:             244
32          Proto:           ESP
07 64       Checksum:        1892
25 55 62 D3  Src IP:         37.85.98.211
25 50 11 3B  Dst IP:         37.80.17.59
-----
----- 4-7-2017 12:57:15.530 -----
45 00 00 54 00 1D 00 00 F9 2F 99 47 0A 0A 0A 01  E..T...../.G....
0A 0A 0A 02 00 00 08 00 45 00 00 3C 00 E8 00 00  .....E..<....
7F 01 C2 58 AC 10 0A 64 C0 A8 01 64 00 00 2F 0B  ...X...d...d../.
00 01 26 50 61 62 63 64 65 66 67 68 69 6A 6B 6C  ..&Pabcdefghijkl
6D 6E 6F 70 71 72 73 74 75 76 77 61 62 63 64 65  mnopqrstuvwxyz
66 67 68 69  fghi

IP (Cont) From REM TO LOC    IFACE: PPP 1
45          IP Ver:          4
          Hdr Len:          20
00          TOS:             Routine
          Delay:             Normal
          Throughput:        Normal
          Reliability:        Normal
00 54       Length:          84
00 1D       ID:              29
00 00       Frag Offset:     0

```

How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

```

Congestion:      Normal
                  May Fragment
                  Last Fragment
F9               TTL:      249
2F               Proto:    GRE
99 47            Checksum: 39239
0A 0A 0A 01      Src IP:   10.10.10.1
0A 0A 0A 02      Dst IP:   10.10.10.2
-----
----- 4-7-2017 12:57:15.530 -----
45 00 00 3C 00 E8 00 00 7E 01 C3 58 AC 10 0A 64  E..<....~..X...d
C0 A8 01 64 00 00 2F 0B 00 01 26 50 61 62 63 64  ...d.../...&Pabcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74  efghijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69              uvwabcdefghi

IP (Final) From LOC TO REM      IFACE: ETH 0
45                               IP Ver:      4
                                Hdr Len:      20
00                               TOS:          Routine
                                Delay:         Normal
                                Throughput:    Normal
                                Reliability:    Normal
00 3C                           Length:      60
00 E8                           ID:          232
00 00                           Frag Offset: 0
                                Congestion:    Normal
                                    May Fragment
                                    Last Fragment
7E                               TTL:         126
01                               Proto:       ICMP
C3 58                           Checksum:    50008
AC 10 0A 64                      Src IP:      172.16.10.100
C0 A8 01 64                      Dst IP:      192.168.1.100
ICMP:
00                               Type:        ECHO REPLY
00                               Code:        0
2F 0B                           Checksum:    2863
-----

```

5 CONFIGURATION FILES

5.1 Responder Configuration (WR21)

The config.da0 file and the hardware/firmware used on the Responder router for the purpose of this Application Note are shown below:

```
Command: config c show
Command result

eth 0 descr "HQ LAN 1"
eth 0 IPaddr "192.168.10.1"
eth 1 descr "HQ LAN 2"
eth 1 IPaddr "172.16.10.1"
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
route 0 descr "RouteToRemoteSiteLAN"
route 0 IPaddr "192.168.1.0"
route 0 ll_ent "TUN"
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
eroute 0 descr "GREoverIPsec"
eroute 0 peerid "RemoteSite"
eroute 0 ourid "HQsite"
eroute 0 locip "10.10.10.1"
eroute 0 locmsk "255.255.255.255"
eroute 0 remip "10.10.10.2"
eroute 0 remmsk "255.255.255.255"
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "AES"
eroute 0 authmeth "PRESHARED"
eroute 0 dhgroup 2
eroute 0 enckeybits 128
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"
snTP 0 server "time.devicecloud.com"
dyndns 0 ifent "default"
ppp 0 timeout 300
ppp 1 name "W-WAN (LTE)"
ppp 1 phonenum "*98*1#"
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 ipsec 1
```

How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

```
ppp 1 use_modem 1
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 r_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
web 0 prelogin_info ON
web 0 showgswiz ON
modemcc 0 info_asy_add 4
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "internet.t-d1.de"
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
modemcc 0 sms_access_2 1
modemcc 0 sms_concat_2 0
ana 0 llon ON
ana 0 lapdon 0
ana 0 asyon 1
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 rcihttp ON
user 0 access 0
user 1 name "username"
user 1 epassword "KD51SVJDVVg="
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 "RemoteSite"
user 10 epassword "PDZxU0FFQFU="
user 10 access 4
local 0 transaccess 2
sslcli 0 verify 10
sslsrv 0 certfile "cert01.pem"
sslsrv 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
```

How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

```
ssh 0 nb_listen 5
ssh 0 v1 OFF
tun 0 descr "GRE Tunnel"
tun 0 IPaddr "10.10.0.1"
tun 0 mask "255.255.255.252"
tun 0 source "10.10.10.1"
tun 0 dest "10.10.10.2"
cloud 0 ssl ON
```

Power Up Profile: 0
OK

'ati5'

Digi TransPort WR21-U22B-DE1-XX Ser#:237416 HW Revision: 2203a
Software Build Ver5.2.17.12. Mar 8 2017 13:55:28 WW
ARM Bios Ver 7.59u v43 454MHz B987-M995-F80-08140,0 MAC:00042d039f68
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	
(B)USBHOST	Revision: 1.0	
L2TP	Revision: 1.10	
PPTP	Revision: 1.00	
TACPLUS	Revision: 1.00	
MODBUS	Revision: 0.00	
RealPort	Revision: 0.00	
MultiTX	Revision: 1.00	
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	
GPS	Revision: 1.0	
TELITUPD	Revision: 1.0	
SCRIBATSK	Revision: 1.0	
BASTSK	Revision: 1.0	
PYTHON	Revision: 1.0	
CLOUDSMS	Revision: 1.0	
TCP (HASH mode)	Revision: 1.14	
TCP Utils	Revision: 1.13	
PPP	Revision: 5.2	
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	

How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

PPPOE	Revision: 1.0
BRIDGE	Revision: 1.1
MODEM CC (Huawei LTE)	Revision: 5.2
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
SSH Client	Revision: 1.0
CERT	Revision: 1.0
LowPrio	Revision: 1.0
Tunnel	Revision: 1.2
OVPN	Revision: 1.2
TEMPLOG	Revision: 1.0
QDL	Revision: 1.0
OK	

5.2 Initiator Configuration (WR11)

The config.da0 file and the hardware/firmware used on the Initiator router for the purpose of this Application Note are shown below:

```
Command: config c show
Command result

eth 0 descr "RemoteSiteLAN"
eth 0 IPaddr "192.168.1.1"
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
ip 0 cidr ON
route 0 descr "ToHQLAN1"
route 0 IPaddr "192.168.10.0"
route 0 ll_ent "TUN"
route 1 descr "ToHQLAN2"
route 1 IPaddr "172.16.10.0"
route 1 ll_ent "TUN"
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
eroute 0 descr "GREoverIPsec"
eroute 0 peerip "37.85.98.211"
eroute 0 peerid "HQsite"
eroute 0 ourid "RemoteSite"
```


How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

```
eroute 0 locip "10.10.10.2"
eroute 0 locmsk "255.255.255.255"
eroute 0 remip "10.10.10.1"
eroute 0 remmsk "255.255.255.255"
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "AES"
eroute 0 authmeth "PRESHARED"
eroute 0 nosa "TRY"
eroute 0 autosa 2
eroute 0 dhgroup 2
eroute 0 enckeybits 128
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"
snTP 0 server "time.devicecloud.com"
dyndns 0 ifent "default"
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
web 0 prelogin_info ON
ftpccli 0 hostname "ftp1.digi.com"
ftpccli 0 username "anonymous"
ftpccli 0 epassword "0TF5VFxBSElB"
ftpccli 0 directory "support/firmware/transport/radio_module_firmware/he910d"
ike 0 encalg "AES"
ike 0 keybits 128
ike 0 authalg "SHA1"
ike 0 aggressive ON
ike 0 ikegroup 2
ike 0 ipsecgroup 2
modemcc 0 info_asy_add 3
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "internet.t-d1.de"
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"
```

How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

```
modemcc 0 link_retries_2 10
modemcc 0 stat_retries_2 30
modemcc 0 sms_access_2 1
modemcc 0 sms_concat_2 0
ana 0 anon ON
ana 0 l2on OFF
ana 0 xoton OFF
ana 0 lapdon 0
ana 0 lapbon 0
ana 0 maxdata 1500
ana 0 logsize 180
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 tremto 1200
cmd 0 rcihttp ON
user 0 access 0
user 1 name "username"
user 1 epassword "KD51SVJDVVg="
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 "HQsite"
user 10 epassword "PDZxU0FFQFU="
user 10 access 4
local 0 transaccess 2
sslcli 0 verify 10
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
tun 0 descr "GRE tunnel"
tun 0 IPaddr "10.10.0.2"
tun 0 mask "255.255.255.252"
tun 0 source "10.10.10.2"
tun 0 dest "10.10.10.1"
templog 0 mo_autooff ON
cloud 0 ssl ON

Power Up Profile: 0
OK
```

How to configure a GRE over IPsec Tunnel between two Digi TransPort Routers

```
Digi TransPort WR11-U900-DE1-XX Ser#:319120 HW Revision: 3204a
Software Build Ver5.2.18.3. May 23 2017 09:43:42 1W
ARM Bios Ver 7.61u v46 360MHz B987-M995-F80-00,0 MAC:00042d04de90
Power Up Profile: 0
Async Driver          Revision: 1.19  Int clk
Ethernet Driver        Revision: 1.11
Firewall               Revision: 1.0
EventEdit              Revision: 1.0
Timer Module           Revision: 1.1
(B)USBHOST             Revision: 1.0
L2TP                   Revision: 1.10
PPTP                   Revision: 1.00
TACPLUS                Revision: 1.00
MultiTX                Revision: 1.00
LAPB                   Revision: 1.12
X25 Layer              Revision: 1.19
MACRO                  Revision: 1.0
PAD                    Revision: 1.4
X25 Switch             Revision: 1.7
TPAD Interface         Revision: 1.12
TELITUPD               Revision: 1.0
SCRIBATSK              Revision: 1.0
BASTSK                 Revision: 1.0
PYTHON                 Revision: 1.0
CLOUDSMS               Revision: 1.0
TCP (HASH mode)        Revision: 1.14
TCP Utils              Revision: 1.13
PPP                    Revision: 5.2
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 (Telit 3G)    Revision: 5.2
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
SSH Client             Revision: 1.0
CERT                   Revision: 1.0
LowPrio                Revision: 1.0
Tunnel                 Revision: 1.2
OVPN                   Revision: 1.2
TEMPLOG                Revision: 1.0
QDL                    Revision: 1.0
```