



Application Note 42

Dynamic VPN tunnels using Egroups and MySQL with fail-over to local database

UK Support

November 2015

Contents

| | | |
|-------|--|----|
| 1 | Introduction | 4 |
| 1.1 | Outline | 4 |
| | Assumptions | 4 |
| 1.2 | Corrections | 5 |
| 1.3 | Version | 5 |
| 2 | MySQL Server Setup | 6 |
| 2.1 | MySQL Server - Initial Configuration | 6 |
| 2.2 | Create the MySQL Database and Tables | 11 |
| 2.2.1 | Login to the MySQL Server | 11 |
| 2.2.2 | Create the MySQL Database | 12 |
| 2.2.3 | Create a Table Within the Darabase | 13 |
| 2.2.4 | Enter the Site Specific Data into the Table | 14 |
| 2.3 | Create the Local Database File for the MySQL Fail-Over. | 15 |
| 3 | Dig vc7400 vpn concentrator configuration..... | 16 |
| 3.1 | Configure port ETH5 as a WAN gateway..... | 16 |
| 3.1.1 | Configure ETH 5..... | 16 |
| 3.1.2 | Configure a Default Route for Eth 5..... | 17 |
| 3.2 | VPN Configuration..... | 17 |
| 3.2.1 | Configure the IKE Responder..... | 18 |
| 3.2.2 | Configure the IPsec route | 18 |
| 3.2.3 | Configure the Egroup | 20 |
| 3.2.4 | Configure Local Database | 21 |
| 3.2.5 | MySQL Database Fail-over | 21 |
| 3.2.6 | Configure Login for the Local Database | 22 |
| 4 | Configuration Files | 23 |

Configure a VPN Tunnel Between Two Digi Transport Routers

Figures

| | |
|---|-------------------------------------|
| Figure 2-1: Eth 5 Configuration | 17 |
| Figure 2-2: Default Route 0 Configuration..... | 17 |
| Figure 2-3: Ike Responder Configuration | 18 |
| Figure 2-4: IPsec 0 Configuration..... | 20 |
| Figure 2-5: User 11 Configuration | 22 |
| Figure 2-6: SIM 1 Configuration | Error! Bookmark not defined. |
| Figure 2-7: PPP 1 Configuration..... | Error! Bookmark not defined. |
| Figure 2-8: IKE Responder Configuration..... | Error! Bookmark not defined. |
| Figure 2-9: Eroute 0 Configuration | Error! Bookmark not defined. |
| Figure 2-10: User 10 Configuration | Error! Bookmark not defined. |
| Figure 3-1: VC7400 Eroute 2 Configuration | Error! Bookmark not defined. |
| Figure 3-2: Ethernet IP Settings | Error! Bookmark not defined. |
| Figure 3-3: ConnectPort WAN VPN Global Settings | Error! Bookmark not defined. |
| Figure 3-4: ConnectPort WAN VPN Settings | Error! Bookmark not defined. |
| Figure 4-1: VC7400 IPsec Peers..... | Error! Bookmark not defined. |
| 4-2: Transport SR IPsec Peers | Error! Bookmark not defined. |
| Figure 4-3: VC7400 IKE SAs..... | Error! Bookmark not defined. |
| 4-4: Transport SR IKE SAs..... | Error! Bookmark not defined. |
| Figure 4-5: VC7400 IPsec Eroute 0 and Eroute 2 | Error! Bookmark not defined. |
| 4-6: Transport SR IPsec Eroute 0..... | Error! Bookmark not defined. |
| Figure 4-8: ConnectPortWAN Connections | Error! Bookmark not defined. |

1 INTRODUCTION

1.1 Outline

Dynamic VPN is a mode of operation is designed be used when the Digi Transport VPN concentrator is terminating a large number of VPN tunnels. The benefits of this method over a standard IPSEC VPN configuration are;

1. For a large number of VPN's, it keeps the size of the configuration file in the Digi router more manageable.
2. It eases configuration. The only the information stored in the config file is that which is common for all tunnels.
3. All information that is site specific, is stored in a MySQL database. This means that the performance and the number of VPN's that can be configured, is limited only by the SQL database and the Server on which it resides. Where as a standalone router is likely to be much less powerfull.

Basic Concept

Using Egroups, the Dig Transport router will create dynamic VPN tunnels using information gathered from a remote MySQL server. The router will update it's own local database which will be used for fail-over should the remote MySQL Server become unavailable.

The Digi router with the Egroup/MySQL configuration will be the VPN Concentrator. The remote initiator routers will normally not require an Egroup configuration as they will typically only need to connect to a single peer. In this example the VPN Concentrator will need only a single Encrypted Route (Eroute) configured. The Egroup will use the single Eroute as its base config for all dynamic VPN's that are created. Best practice for minimising the amount of configuration is If possible, to widen the subnet mask to encompass all the local and remote networks.

It is important to configure the Eroutes to time out on inactivity to free up sessions for other sites. The Digi will create a "Dynamic Eroute" containing all the settings from the base eroute and all the information retrieved from the database. At this point IKE will create the tunnel (IPSEC Security associations) as normal. The dynamic eroute will continue to exist until all the IPSEC Security Associates have been removed. At the point where the number of dynamic eroutes free is within 10% of the maximum supported in the platform (Digi model) the oldest Dynamic Eroutes (those that have not been used for the longest period of time) and their associated IPSEC Security Associations will be dropped until the number of dynamic eroutes free is above 10% of the total.

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 Cisco Adaptive Security Appliance and to configure them with basic routing functions.

Configure a VPN Tunnel Between Two Digi Transport Routers

This application note applies only to:

Model: Digi VC7400 VPN Concentrator, Transport WR, SR or DR and a Digi Connect and ConnectPort WAN.

Firmware versions: All firmware

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 Transport SR's IP address is dynamic
- IPSEC is to be used in "aggressive mode"
- Method is compatible with a Main Mode IPSEC VPN tunnel
- The version of MySQL server used in this application note is 5.1.44 but you can use any.

1.2 Corrections

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

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

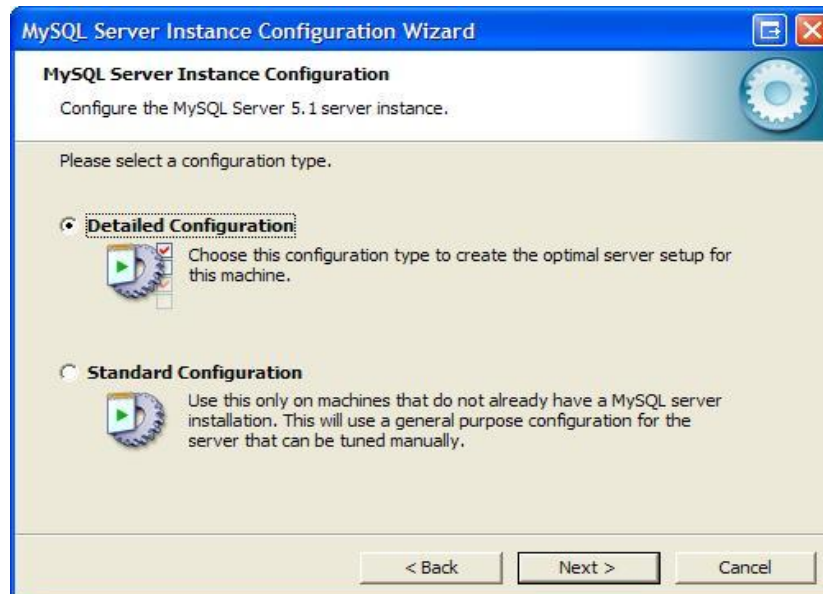
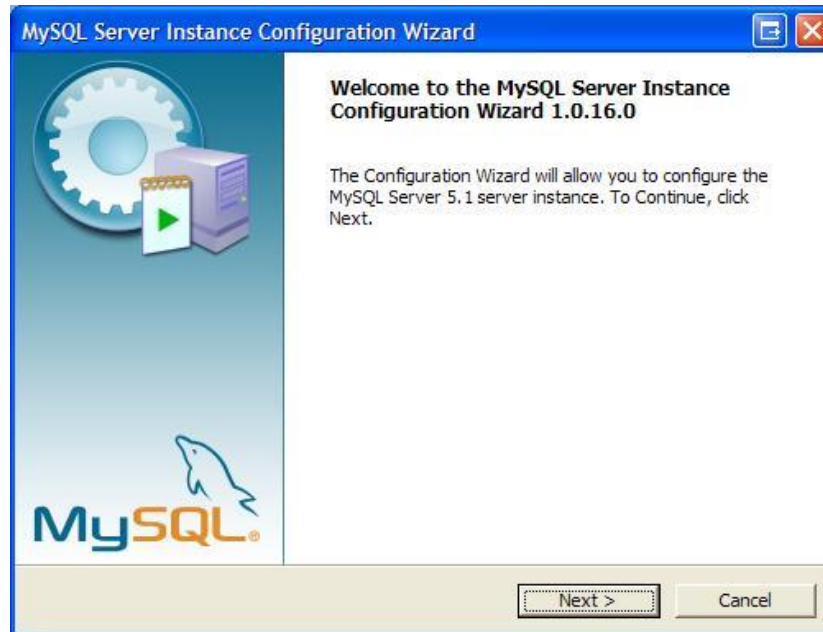
1.3 Version

| Version Number | Status |
|----------------|------------------------|
| 1.0 | Published |
| 1.1 | Digi Transport branded |
| 1.2 | Updated to new GUI |

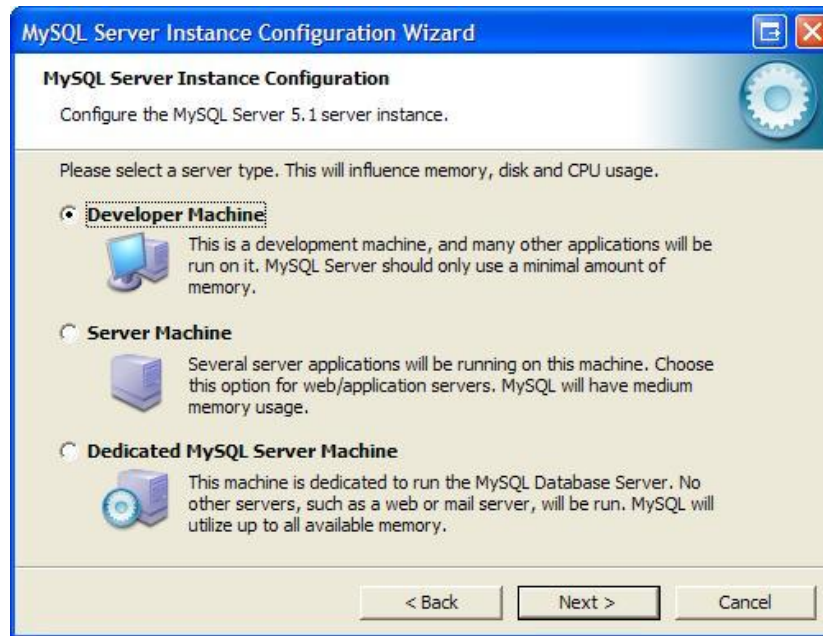
2 MYSQL SERVER SETUP

2.1 MySQL Server - Initial Configuration

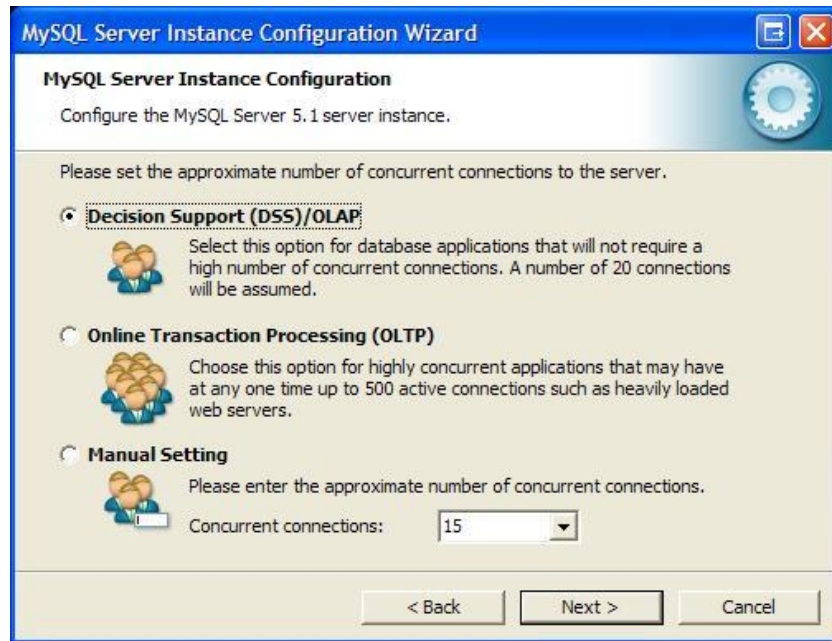
Using the MySQL Server Instance Config Wizard do the initial set up as follows;



Configure a VPN Tunnel Between Two Digi Transport Routers



Configure a VPN Tunnel Between Two Digi Transport Routers



MySQL Server Instance Configuration Wizard

MySQL Server Instance Configuration
Configure the MySQL Server 5.1 server instance.

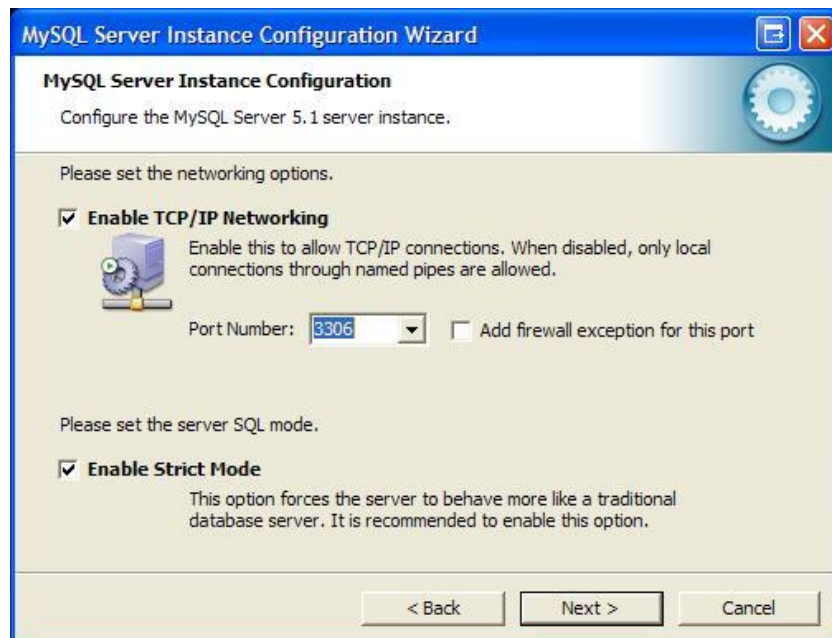
Please set the approximate number of concurrent connections to the server.

☒ **Decision Support (DSS)/OLAP**
Select this option for database applications that will not require a high number of concurrent connections. A number of 20 connections will be assumed.

☐ **Online Transaction Processing (OLTP)**
Choose this option for highly concurrent applications that may have at any one time up to 500 active connections such as heavily loaded web servers.

☐ **Manual Setting**
Please enter the approximate number of concurrent connections.
Concurrent connections:

< Back Next > Cancel



MySQL Server Instance Configuration Wizard

MySQL Server Instance Configuration
Configure the MySQL Server 5.1 server instance.

Please set the networking options.

☒ **Enable TCP/IP Networking**
Enable this to allow TCP/IP connections. When disabled, only local connections through named pipes are allowed.
Port Number: ☐ Add firewall exception for this port

Please set the server SQL mode.

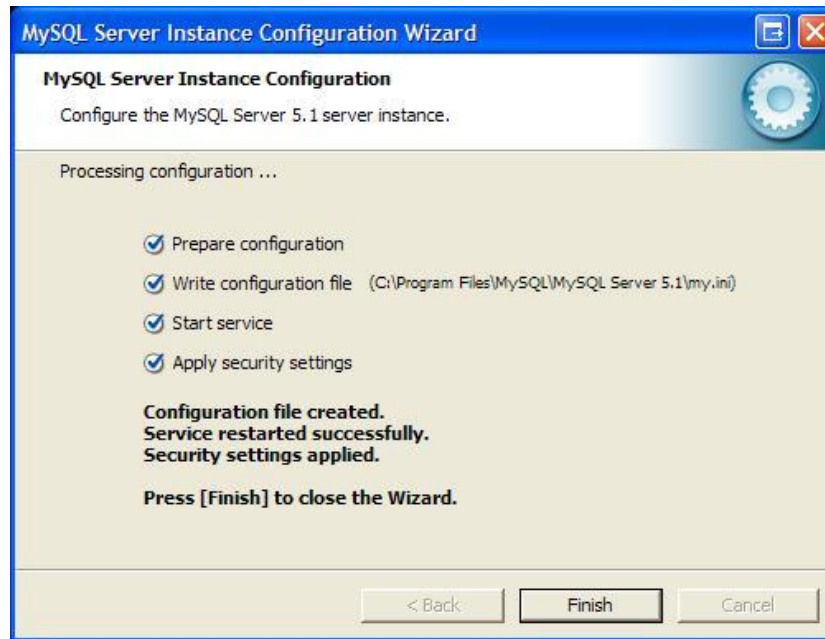
☒ **Enable Strict Mode**
This option forces the server to behave more like a traditional database server. It is recommended to enable this option.

< Back Next > Cancel

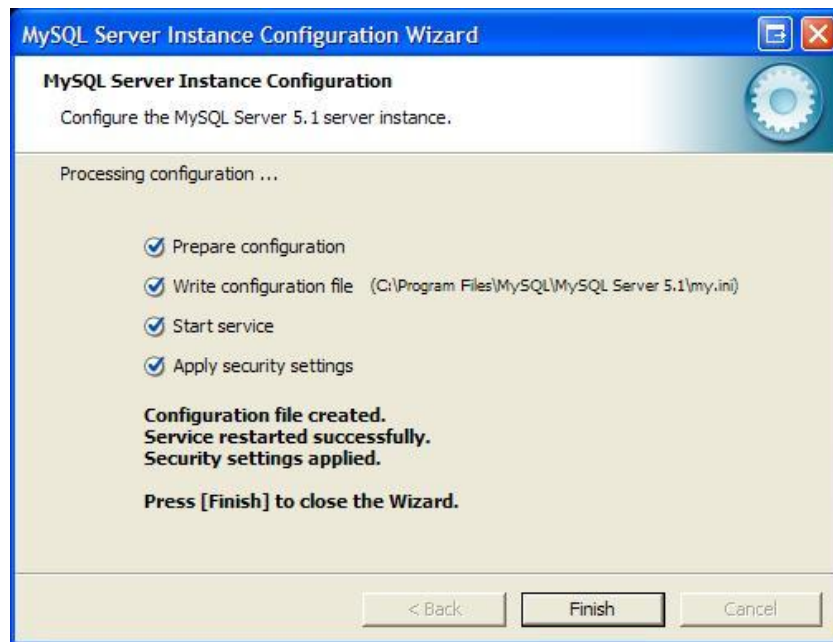
Configure a VPN Tunnel Between Two Digi Transport Routers



Configure a VPN Tunnel Between Two Digi Transport Routers



Configure a VPN Tunnel Between Two Digi Transport Routers



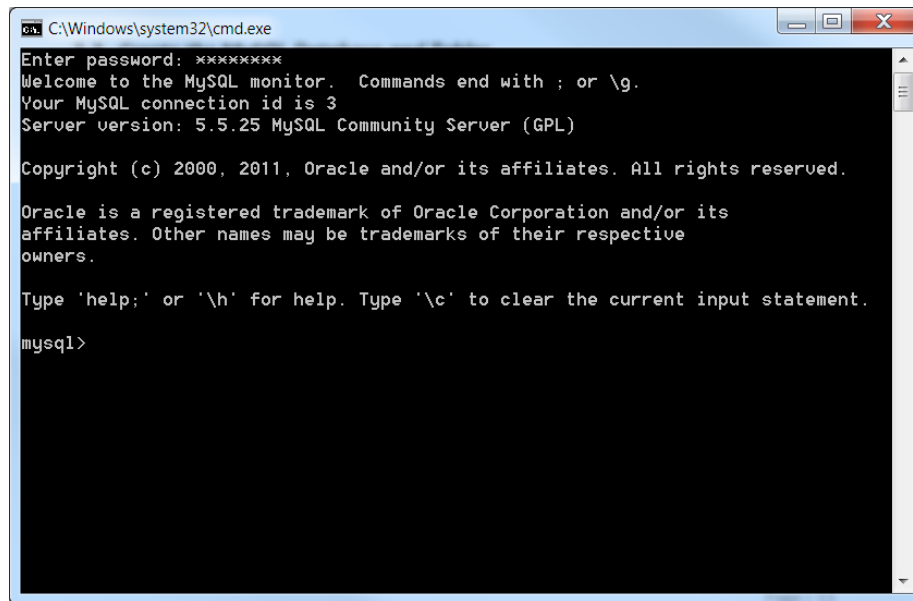
2.2 Create the MySQL Database and Tables

2.2.1 Login to the MySQL Server

Start > Programs > MySQL > MySQL Server > MySQL Command Line Client

You will then be prompted for you're the password you entered during the wizard.

Configure a VPN Tunnel Between Two Digi Transport Routers



2.2.2 Create the MySQL Database

The name of the database will be called 'digidb'

NB: The commands entered by the user are in **bold**. The server response is in normal text.

```
mysql> create database digidb;  
Query OK, 1 row affected (0.00 sec)
```

Confirm that the database digidb has been created.

```
mysql> show databases;  
+-----+  
| Database |  
+-----+  
| information_schema |  
| digidb |  
| mysql |  
+-----+  
4 rows in set (0.00 sec)
```

Next tell the MySQL server to use the new database 'digidb' so that we can create a table within the 'digidb' database.

```
mysql> use digidb;  
Database changed
```

2.2.3 Create a Table Within the Darabase

Next we create a table called 'eroutes' within the 'digidb' database. At the same time we create the columns and fields for the table.

```
mysql> create table eroutes (
  -> `peerip` varchar(20) default NULL,
  -> `bakpeerip` varchar(20) default NULL,
  -> `peerid` varchar(20) NOT NULL default '',
  -> `password` varchar(20) default NULL,
  -> `ourid` varchar(20) default NULL,
  -> `remip` varchar(20) default NULL,
  -> `remmsk5` varchar(20) default NULL,
  -> PRIMARY KEY (`peerid`),
  -> UNIQUE KEY `Index_2` (`remip`)
  -> ) ENGINE=InnoDB DEFAULT CHARSET=latin1;
Query OK, 0 rows affected (0.08 sec)
```

Check that the 'eroutes' table has been created.

```
mysql> show tables;
+-----+
| Tables_in_digidb |
+-----+
| eroutes           |
+-----+
1 row in set (0.02 sec)
```

Check that the columns and fields within the 'eroutes' table have been created.

```
mysql> describe eroutes;
+-----+-----+-----+-----+-----+-----+
| Field      | Type          | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| peerip     | varchar(20)   | YES  |     | NULL    |       |
| bakpeerip  | varchar(20)   | YES  |     | NULL    |       |
| peerid     | varchar(20)   | NO   | PRI |         |       |
| password   | varchar(20)   | YES  |     | NULL    |       |
| ourid      | varchar(20)   | YES  |     | NULL    |       |
| remip      | varchar(20)   | YES  | UNI | NULL    |       |
| remmsk5    | varchar(20)   | YES  |     | NULL    |       |
+-----+-----+-----+-----+-----+-----+
```

7 rows in set (0.05 sec)

2.2.4 Enter the Site Specific Data into the Table

Enter the site specific data, which is individual for each remote router, into the eroutes table. The site specific data should be entered in the same order as the fields in the table;

E.g. Peerip, bakpeerip, peerid, password (which is the preshared key), ourid, remip and remmsk5.

Each row is inside brackets, each parameter is inserted between two ' ' and seperated by a comma.

9 Rows have been entered below, the first row will be the working example described in the rest of this document. The first 2 columns are left blank in this example because the remote peers have dynamic IP addresses and we will therefore be using aggressive mode IPSEC.

```
mysql> INSERT INTO `eroutes` VALUES
('','remote1','test1','vpncon','10.100.1.0',''),
-> ('','remote2','test2','vpncon','10.100.2.0',''),
-> ('','remote3','test3','vpncon','10.100.3.0',''),
-> ('','remote4','test4','vpncon','10.100.4.0',''),
-> ('','remote5','test5','vpncon','10.100.5.0',''),
-> ('','remote6','test6','vpncon','10.100.6.0',''),
-> ('','remote7','test7','vpncon','10.100.7.0',''),
-> ('','remote8','test8','vpncon','10.100.8.0',''),
-> ('','remote9','test9','vpncon','10.100.9.0','');
Query OK, 9 rows affected (0.05 sec)
Records: 9 Duplicates: 0 Warnings: 0

mysql>
Query OK, 9 rows affected (0.01 sec)
Records: 9 Duplicates: 0 Warnings: 0
```

Show the contents of the 'Eroutes' table.

```
mysql> select * from eroutes;
```

| peerip | bakpeerip | peerid | password | ourid | remip | remmsk5 |
|--------|-----------|---------|----------|--------|------------|---------|
| | | remote1 | test1 | vpncon | 10.100.1.0 | |
| | | remote2 | test2 | vpncon | 10.100.2.0 | |
| | | remote3 | test3 | vpncon | 10.100.3.0 | |
| | | remote4 | test4 | vpncon | 10.100.4.0 | |
| | | remote5 | test5 | vpncon | 10.100.5.0 | |
| | | remote6 | test6 | vpncon | 10.100.6.0 | |
| | | remote7 | test7 | vpncon | 10.100.7.0 | |
| | | remote8 | test8 | vpncon | 10.100.8.0 | |
| | | remote9 | test9 | vpncon | 10.100.9.0 | |

9 rows in set (0.00 sec)

2.3 Create the Local Database File for the MySQL Fail-Over.

The Digi Transport router is capable of storing a database file on its flash so that it can do a local MySQL look up should it lose connectivity with the remote MySQL server. The local database can be configured manually, or it can learn it's entries from the remote MySQL server.

The database looks very much the same as the table in the remote MySQL server except in the Peerip and bakpeerip fields, you enter the local WAN IP address of the VPN concentrator (e.g. 217.34.133.22).

NB: The database should have the same name as the remote MySQL database with a .csv extension (i.e. 'digidb' in this example).

Here are the contents of the local database file (digidb.csv) used for this application note.

```
peerip[IP],bakpeerid[IP],peerid[K20],password[20],ourid[20],remip[UIP],remmsk[IP]
217.24.123.22,217.24.123.22,remote1,test1,vpncon,10.100.1.0,255.255.255.0
217.24.123.22,217.24.123.22,remote2,test2,vpncon,10.100.2.0,255.255.255.0
217.24.123.22,217.24.123.22,remote3,test3,vpncon,10.100.3.0,255.255.255.0
217.24.123.22,217.24.123.22,remote4,test4,vpncon,10.100.4.0,255.255.255.0
217.24.123.22,217.24.123.22,remote5,test5,vpncon,10.100.5.0,255.255.255.0
217.24.123.22,217.24.123.22,remote6,test6,vpncon,10.100.6.0,255.255.255.0
217.24.123.22,217.24.123.22,remote7,test7,vpncon,10.100.7.0,255.255.255.0
217.24.123.22,217.24.123.22,remote8,test8,vpncon,10.100.8.0,255.255.255.0
217.24.123.22,217.24.123.22,remote9,test9,vpncon,10.100.9.0,255.255.255.0
217.24.123.22,217.24.123.22,remote10,test10,vpncon,10.100.10.0,255.255.255.0
```

NB: Upload the .csv file to the router using FTP.

3 DIG VC7400 VPN CONCENTRATOR CONFIGURATION

3.1 Configure port ETH5 as a WAN gateway

In reality, any of the Ethernet ports on a Digi VC7400 can be used as a WAN port, however, port ETH 5 is designed to be the WAN port and supports Gigabit Ethernet (Gig-E). In this example, the VC7400 is configured with a cable modem as its WAN gateway and has a fixed public IP address.

The steps for this are:

1. Configure ETH 5 with the correct IP address and gateway etc.
2. Configure a default route for ETH 5

3.1.1 Configure ETH 5

Configuration → Network → Interfaces → Ethernet → ETH 5

| Parameter | Setting | Description |
|-------------|-----------------|---|
| IP Address: | 217.24.123.22 | Enter your own fixed IP address for the router |
| Mask: | 255.255.255.240 | Enter the appropriate subnet for your IP address range. |
| DNS Server: | 217.24.123.29 | Enter the IP address of the DNS Server |
| Gateway: | 217.24.123.29 | Enter the correct gateway address for the router |

Configuration → Network → Interfaces → Ethernet → ETH 5 → Advanced

| Parameter | Setting | Description |
|---------------------------------|---------------------|---|
| Enable NAT on this Interface: | IP address and Port | Use NAPT or NAT |
| Enable IPsec on this interface: | Checked | Enable IPsec on selected interface |
| Use interface | Default and 0 | Select the interface for the source IP address of IPsec packets |

Configure a VPN Tunnel Between Two Digi Transport Routers

Configuration - Network > Interfaces > Ethernet > ETH 5 > Advanced

ETH 5

Description: Outside Interface

☐ Get an IP address automatically using DHCP
☒ Use the following settings

IP Address: 217.24.123.22
Mask: 255.255.255.0
Gateway: 217.24.123.29
DNS Server: 217.24.123.29
Secondary DNS Server:

Changes to these parameters may affect your browser connection

Advanced

This interface is associated with physical port: ETH 5
This device is currently in Port Isolate mode [Switch to Hub mode](#)

Metric: 1
MTU: 1500

Speed (currently 1000Base-T): ☒ Auto ☐ 10Base-T ☐ 100Base-T ☐ 1000Base-T
Duplex: ☐ Full Duplex ☒ Half Duplex
Max Rx rate: 0 kbps
Max Tx rate: 0 kbps
TCP transmit buffer size: 0 bytes

Take this interface out of service after 0 seconds when the link is lost (e.g. cable removed or broken)

☒ Enable NAT on this interface
☐ IP address ☒ IP address and Port

☒ Enable IPsec on this interface
Use interface: Default for the source IP address of IPsec packets

☐ Enable the firewall on this interface

Figure 3-1: Eth 5 Configuration

3.1.2 Configure a Default Route for Eth 5

Configuration → Network → IP Routing/Forwarding → Static Routes → Default Route 0 .

In order for the Digi VC7400 to recognize Eth 5 as a gateway, a default route must be configured to point to that port. In this example, default route 0 is attributed to Eth 5

| Parameter | Setting | Description |
|--------------|----------|---|
| Interface: | Ethernet | Set Ethernet as the interface |
| Interface #: | 5 | Enter 5 as the Ethernet instance to use |

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

Default Route 0

Description:

Default route via

Gateway:

Interface: Ethernet 5

Use PPP sub-configuration: 0

Metric: 1

Figure 3-2: Default Route 0 Configuration

3.2 VPN Configuration

The Digi VC7400 will be the VPN Responder.

3.2.1 Configure the IKE Responder

Configuration → Network → Virtual Private Networking (VPN) → IPsec → IKE → IKE Responder.

The IKE Responder is set to a range of IPsec parameters. In order for the Initiator to connect, its parameters must fall within these ranges. Leave this page at factory defaults.

Figure 3-3: Ike Responder Configuration

Configuration → Network → Virtual Private Networking (VPN) → IPsec → IKE → IKE Debug.

For troubleshooting purposes, it is a good idea to enable debugging at level “Very High”.

| Parameter | Setting | Description |
|------------------|-----------|--------------------------------|
| Enable IKE Debug | ON | Enable IKE debugging |
| Debug Level: | Very High | Set debug to the highest level |

3.2.2 Configure the IPsec route

Configuration → Network → Virtual Private Networking (VPN) → IPsec → IPsec Tunnels → IPsec 0 – 9 → IPsec 0

Configure a VPN Tunnel Between Two Digi Transport Routers

The IPsec route is the phase 2 IPSEC part of the configuration. Normally you would configure an IPsec route for each VPN tunnel you terminate on the router. But as the router will be creating VPN tunnels dynamically, we will configure a single base route, with only the common parameters set for each tunnel.

| Parameter | Setting | Description |
|--|-------------------|--|
| Local LAN IP Address | 192.168.100.0 | Enter the IP address of the Local side of the tunnel |
| Local LAN Mask: | 0.0.0.0 | Enter the appropriate subnet for your IP address range. |
| Remote LAN IP Address | 10.100.0.0 | Enter the IP address of the remote side of the tunnel |
| Remote LAN Mask: | 255.255.0.0 | Enter the appropriate subnet for your IP address range. |
| Use the Following security on this tunnel: | Preshared Keys | Use Preshared keys for security |
| Our ID | vpncon | Enter the ID which is sent to the remote peer to identify the router. |
| Our ID type | IKE ID | Select the ID type the router is sending |
| Remote ID | * | Enter the ID which is sent from the remote peer to identify the router |
| Encryption on this tunnel | AES (128bit keys) | Select the Encryption used on this tunnel |
| Authentication on this tunnel | SHA1 | Select the Authentication used on this tunnel |
| Diffie Hellman group | No PFS | Select Diffie Hellman group used on this tunnel |

Configure a VPN Tunnel Between Two Digi Transport Routers

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

IPsec 0
Description: Route linked to dynamic VPN

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="192.168.100.0"/> Mask: <input type="text" value="0.0.0.0"/> <input type="radio"/> Use interface <input type="text" value="PPP"/> | <input checked="" type="radio"/> Use these settings for the remote LAN IP Address: <input type="text" value="10.100.0.0"/> Mask: <input type="text" value="255.255.0.0"/> <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

Figure 3-4: IPsec 0 Configuration

3.2.3 Configure the Egroup

Configuration → Network → Virtual Private Networking (VPN) → IPsec → IPsec Groups → IPsec Group 0

The IPsec Group links the IPsec route with the MySQL Database. Here we enter the IP address, login details of the MySQL server and the database name and relevant table name.

| Parameter | Setting | Description |
|--|---------------|--|
| Link this IPsec Group with IPsec tunnel: | 0 | Link the group with route 0 |
| Remote mask to use for tunnels: | 255.255.255.0 | Enter the subnet mask to use for remote LAN's. |
| Database Server IP/Hostname: | 10.1.19.253 | Enter the IP address of the MySQL Server |
| Database Login Username: | root | Enter the username of the MySQL Server |
| Database Login Password: | test | Enter the password of the MySQL Server |
| Database Name: | digidb | Enter the name of the MySQL database |
| Database Table: | eroutes | Enter the name of the MySQL table |

Configure a VPN Tunnel Between Two Digi Transport Routers

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

▼ IPsec Group 0

Link this IPsec Group with IPsec Tunnel: 0
Remote mask to use for tunnels: 255.255.255.0

Database

MySQL Server IP Address or Hostname: 10.1.19.253
MySQL Server Port: 0
Username: root
Password: ****
Confirm Password: ****
Database name: digidb
Database table: eroutes

Database Table Field Names
These define the names of the fields in which the following data is stored.

Remote subnet IP:
Remote subnet Mask:
Peer IP Address:
Backup Peer IP Address:
Peer ID:
Our ID:
Password:

Apply

Figure 3-5: IPsec Group 0 Configuration

3.2.4 Configure Local Database

The following needs to be configured via the router's command line interface

```
sql 0 dbsrvmem 500*  
sql 0 dbfile "digidb.csv"  
sql 0 dbname "digidb"  
sql 0 debug_opts 3
```

* The general rule of thumb when setting aside memory for the local database, is to double the size of the CSV file (KB) and add 100KB. So for a database of 200KB, you would set aside 500KB.

3.2.5 MySQL Database Fail-over

Configuration - Network → Advanced Network Settings

Set up fail-over from the remote MySQL database to the local database. We do this with the backup IP address feature by failing over from the remote MySQL server's IP address (10.1.19.253) to the local loopback IP address of the router (127.0.0.1).

| Parameter | Setting | Description |
|--------------------|-------------|--|
| IP Address: | 10.1.19.253 | Enter the IP address for the remote MySQL server |
| Backup IP Address: | 127.0.0.1 | Enter the loopback address of the router |
| Retry Time: | 30 | Configure the router to retry a connection at 30 seconds |
| Try Next: | Checked | Configure the router to try the next IP address if connection fails. |

Configure a VPN Tunnel Between Two Digi Transport Routers

Configuration - Network > Advanced Network Settings

| IP Address | Backup IP Address | Retry Time (seconds) | Try Next |
|---|-------------------|----------------------|-------------------------------------|
| No Backup IP addresses have been configured | | | |
| 10.1.19.253 | 127.0.0.1 | 30 | <input checked="" type="checkbox"/> |

Send "Backup IP" system messages to IP Address:

Figure 3-6: Backup IP address for database failover

3.2.6 Configure Login for the Local Database

Configuration → Security → Users → User 10 - 19 > User 10.

If the remote MySQL server becomes unavailable then router can use the local database for the VPN tunnels. Local access to the database must be authorised in the same way as the remote MySQL server. In effect the router logs in to itself using the same login credentials as for the MySQL server.

| Parameter | Setting | Description |
|-----------|---------|-----------------------------------|
| Name: | root | Enter username for local database |
| password: | test | Enter password for local database |

Configuration - Security > Users > User 10 - 19 > User 10

▼ User 10 - 19

▼ User 10

Username:

Password:

Confirm Password:

Access Level: ▼

► Advanced

Figure 3-7: User 10 Configuration

4 CONFIGURATION FILES

VC7400 – VPN Concentrator Configuration

```
eth 0 IPAddr "192.168.100.1"
eth 1 IPAddr "10.1.19.254"
eth 1 mask "255.255.0.0"
eth 5 descr "Outside Interface"
eth 5 IPAddr "217.24.123.22"
eth 5 mask "255.255.255.240"
eth 5 DNSserver "217.24.123.29"
eth 5 gateway "217.24.123.29"
eth 5 do_nat 2
eth 5 ipsec 2
sql 0 dbsrvmem 110
sql 0 dbfile "digidb.csv"
sql 0 dbname "digidb"
sql 0 debug_opts 3
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 2 dtemode 2
def_route 0 ll_ent "eth"
eroute 0 descr "Eroutelinked to dynamic VPN"
eroute 0 peerid "*"
eroute 0 ourid "vpncon"
eroute 0 locip "192.168.100.0"
eroute 0 locmsk "0.0.0.0"
eroute 0 remip "10.100.0.0"
eroute 0 remmsk "255.255.0.0"
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "AES"
eroute 0 ltime 28800
eroute 0 lkbytes 0
eroute 0 authmeth "PRESHARED"
eroute 0 nosa "PASS"
def_eroute 0 nosain "PASS"
def_eroute 0 nosaout "PASS"
egroup 0 dbhost "10.1.19.253"
egroup 0 dbuser "root"
egroup 0 dbepwd "Mip6CVY="
egroup 0 dbname "digidb"
egroup 0 dbtable "eroutes"
egroup 0 remmsk "255.255.255.0"
dhcp 0 IPmin "192.168.1.100"
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "192.168.1.1"
dhcp 0 respdelms 500
ipbu 0 IPAddr "10.1.19.253"
ipbu 0 BUIPAddr "127.0.0.1"
ipbu 0 retrysec 30
ipbu 0 donext ON
```

Configure a VPN Tunnel Between Two Digi Transport Routers

```
ppp 0 timeout 300
ike 0 deblevel 4
ana 0 anon ON
ana 0 llon ON
ana 0 asyon 15
ana 0 logsize 45
cmd 0 unitid "di%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 tremto 120
cmd 0 web_suffix ".wb2"
user 1 name "username"
user 1 password "password"
user 1 access 0
user 2 access 0
user 3 epassword "A==="
user 3 access 0
user 4 epassword "A==="
user 4 access 0
user 5 epassword "A==="
user 5 access 0
user 6 epassword "A==="
user 6 access 0
user 7 epassword "A==="
user 7 access 0
user 8 epassword "A==="
user 8 access 0
user 9 epassword "A==="
user 9 access 0
user 10 name "root"
user 10 password "test"
local 0 transaccess 2
sslsrv 0 certfile "cert01.pem"
sslsrv 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
```

WR41 – VPN Initiator Configuration

```
eth 0 IPAddr "10.100.1.254"
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 3 dtemode 0
lapb 4 dtemode 0
lapb 5 dtemode 0
lapb 6 dtemode 0
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
eroute 0 peerip "217.24.123.22"
eroute 0 peerid "vpncon"
eroute 0 ourid "remote1"
eroute 0 locmsk "255.255.255.0"
```


Configure a VPN Tunnel Between Two Digi Transport Routers

```
eroute 0 locipifent "ETH"
eroute 0 remip "192.168.100.0"
eroute 0 remmsk "255.255.255.0"
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "AES"
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 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "192.168.1.1"
dhcp 0 respdelms 500
ppp 0 timeout 300
ppp 1 r_chap OFF
ppp 1 IPaddr "0.0.0.0"
ppp 1 phonenum "*98*1#"
ppp 1 timeout 0
ppp 1 use_modem 1
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 ipsec 1
ppp 1 ipanon ON
ppp 3 defpak 16
ppp 4 defpak 16
ike 0 ltime 86400
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 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 web_suffix ".wb2"
```

Configure a VPN Tunnel Between Two Digi Transport Routers

```
user 0 access 0
user 1 name "username"
user 1 epassword "KD51SVJDVg="
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 "vpncon"
user 10 epassword "LDplThQ="
user 10 access 4
local 0 transaccess 2
sslsrv 0 certfile "cert01.pem"
sslsrv 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
```