Digi Connect® WAN/VPN Application Guide

Remote Site Fail-Over Routing or Load Sharing

Scenario

Primary remote site connectivity is via frame relay, leased line, VPN, DSL or cable modem. The Digi Connect WAN provides a backup connection from the remote site to the home office via a cellular data network. This document assumes this is a site-to-site connection where bi-directional traffic is required. Remote-only initiated VPN connections will be somewhat simpler than this example.

Theory of Operation

Initiating the fail-over (or backup) route via the Digi Connect WAN/VPN, and then going back to the primary route once the primary link is re-established, is the responsibility of the *Primary WAN router* and *not* the Digi Connect WAN/VPN. The Digi Connect WAN/VPN simply passes the traffic to/from the primary router's backup WAN port to/from the cellular network. This is accomplished by configuring the router's backup Ethernet port to have a higher metric (cost) route than that of the primary WAN connection.

When the primary route fails, routing protocols tell the router to start sending traffic via its backup WAN port to the Digi Connect WAN/VPN. Once the primary is re-established, routing protocols tell the primary router the least-cost route is available and traffic stops being sent via the Digi Connect WAN/VPN.

Note that the Digi SureLink™ mechanism that is standard with Digi Connect WAN/VPN devices maintains an always-on connection on the cellular network even if no traffic is flowing. This means the cellular-based backup route is immediately available.

The remote site router must have an Ethernet port that can be designated as a backup WAN port with the ability to re-route traffic when the primary WAN interface cannot reach the far-end. This second WAN port connects to the Ethernet port of the Digi Connect WAN, typically via an Ethernet crossover cable. In some cases, the router may be able to "backhaul" the connection via a LAN port.

The Digi Connect WAN/VPN uses Network Address Translation (NAT) where only the mobile IP address is visible to the outside. All outgoing traffic uses the Digi Connect WAN/VPN mobile IP address.

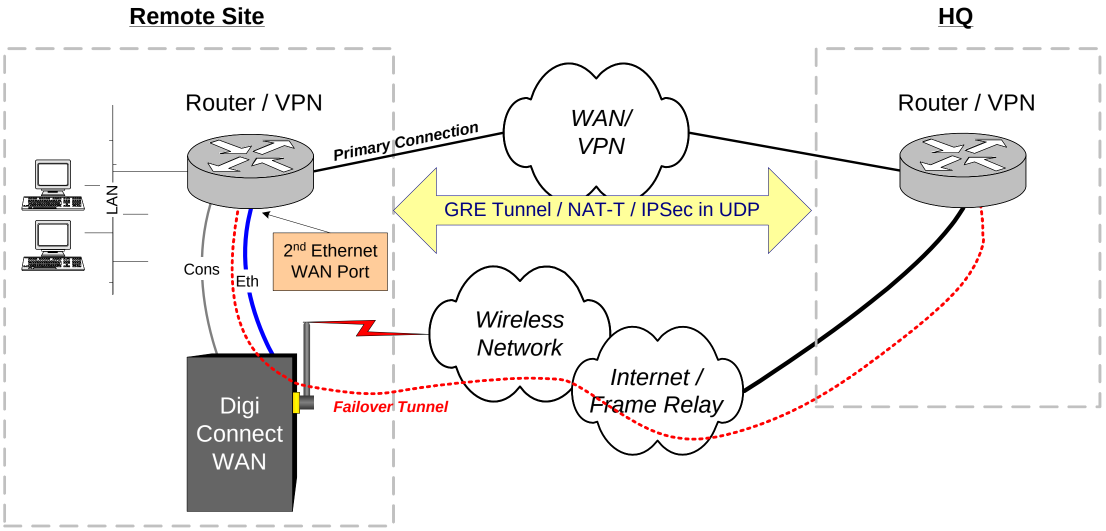
For incoming data, the Digi Connect WAN forwards IP traffic destined for a specific port, port range or GRE/IPsec protocol from the cellular interface to a private IP address on the Ethernet "side" of the Digi Connect WAN. The Digi Connect VPN can be used to tunnel date securely over the cellular network.

Since NAT changes IPsec headers, devices that support GRE, NAT-T* or IPsec in UDP* "tunneling" at each end of the connection may be required. As such, TCP/UDP port forwarding from the Digi Connect WAN's cellular interface to its Ethernet port is used to pass this incoming VPN traffic through the Digi Connect WAN to the router/appliance.

IPsec forwarding: Digi Connect WAN firmware revision D introduced IPsec forwarding where IPsec ESP tunnel-mode traffic can be forwarded to a specific Ethernet IP address. Current firmware is available via http://www.digi.com/support.

Console Port: As a side benefit, the Digi Connect WAN console port can configured for "Console Management" to provide SSH or telnet access. It can be cabled to console port of the router or VPN appliance to provide true diverse out-of-band console access.

Typical Diagram:



GSM APN Type: For GSM networks, remote site backup connections may require a *Custom* APN. A Custom APN allows for various IP addressing options, particularly static IP addresses, which are needed for most VPN connections. A custom APN should also support mobile terminated data which may be required in most site-to-site VPNs. An Internet APN may be used if the IPsec or GRE end-points support DDNS names.

Remote Site Router Requirements: Routers or VPN appliances such as those from Cisco may need to support *GRE, NAT-T* or *IPsec in UDP* for NAT traversal. The remote site router or VPN appliance must also have a mechanism, such as a *second WAN* Ethernet port or backhaul route, to redirect the traffic to be the failover or load sharing port. This second WAN port connects to the Ethernet port of the Digi Connect WAN.

Remote Site Router/VPN Appliance Configuration:

- Router secondary/failover gateway: Digi Connect WAN's Ethernet port IP address
- Optionally a GRE or IPsec policy to use or NAT-T* tunneling for site-to-site VPN

HQ Router / VPN Appliance Configuration: The HQ appliance's tunnel peer address will be the Digi Connect WAN's mobile IP address. For this reason, a static mobile IP address is preferred on the Digi Connect WAN.

Digi Connect WAN Sample Configuration

1. Read and follow the quick-start guide for the Digi Connect WAN and optionally Digi Connectware® Manager if used.
2. Assign a static IP address to the Digi Connect WAN Ethernet port. (Note the default gateway may show, or change to, an address such as 10.6.6.6. This is normal as it is the GSM provider's network default gateway.)
3. Configure Forwarding via Network > IP Forwarding Settings as needed:

a. For *IPsec ESP Pass-thru*: Enable IPsec ESP pass-through and enter the IP address of the router or VPN appliance Ethernet port attached to the Digi Connect device.
b. For *GRE*: Enable GRE forwarding and enter the IP address of the router's WAN Ethernet port (the router attached to the Digi Connect WAN).
c. For *NAT-T* or *IPsec-in-UDP*: Create two UDP Port Forwarding entries for Ports 500 and 4500* (both source and destination ports) and enter the IP address of the router/appliance's WAN Ethernet port (the router attached to the Digi Connect WAN).
* UDP port 500 is for IKE/ISAKMP and rarely changes. Some appliances may use UDP ports other than 4500 for IPsec. Check the router/appliance documentation for acceptable UDP port numbers. Different port numbers for source and destination can also be used.

4. Press APPLY to accept the changes
5. Optionally configure IP Filtering and TCP service port settings to block any unwanted incoming traffic.

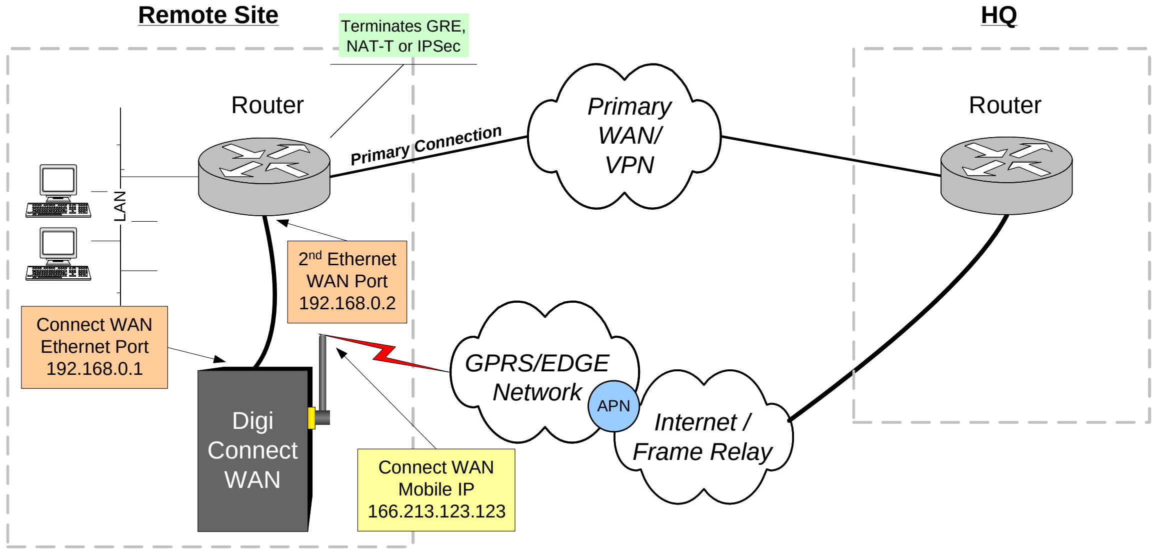
Example Configuration for IPsec-in-UDP (NAT-T) forwarding:

Refer to the diagram below using these IP addresses:

Device Interface	IP Address
Connect WAN Ethernet port	192.168.0.1
Remote site router's Ethernet WAN port	192.168.0.2
Connect WAN Mobile Link	166.213.123.123
HQ site router/firewall/VPN	206.123.123.123

The HQ router will use the Digi Connect WAN's mobile IP address (in this case 166.213.123.123) as its peer tunnel address.

IP Addressing Scheme:


Remote Site
Terminates GRE, NAT-T or IPSec
HQ
Router
Primary Connection
Primary WAN/ VPN
Router
LAN
2nd Ethernet WAN Port 192.168.0.2
Connect WAN Ethernet Port 192.168.0.1
GPRS/EDGE Network
APN
Internet / Frame Relay
Digi Connect WAN
Connect WAN Mobile IP 166.213.123.123

For a NAT-T (IPsec in UDP) configuration, create these entries on the Digi Connect WAN via Network > IP Forwarding Settings:

Protocol	Source Port	Destination IP Address	Destination Port
UDP	500	192.168.0.2	500
UDP	4500	192.168.0.2	4500

Press Apply. Failover or load-sharing traffic should now pass through the Digi Connect device.

If GRE or IPsec pass-thru are being used, configure forwarding on the Digi Connect WAN to forward traffic to the router's second Ethernet WAN port (in this case 192.168.0.2).

Client-to-Site VPNs: Port or GRE forwarding may not be required if the VPN is configured for client-to-site where the tunnel(s) is initiated only from the remote site.

Where to get more information

Refer to the Digi Connect WAN user documentation and Digi technical support website at www.digi.com/support for more information. Technical assistance is available at http://www.digi.com/support/eservice/eservicelogin.jsp.

For sales information, please contact Digi International at 952-912-3444.