



Digi Cellular Gateway Application Example WAN Backup Scenarios

This document discusses several different methods where a Digi cellular gateway is used to provide failover to IP WAN connections via cellular networks. Other options are available, but these are the most common. In these examples the remote sites could be stores, restaurants, bank branches, substations, or any remote office or branch location.

There are two ways to connect the Digi gateway to the primary router:

- via a *WAN* Ethernet port (i.e., a port on a subnet separate from the LAN), or
- via a *LAN* Ethernet port

An Ethernet WAN port provides the simplest option since failover on the router is usually easier to configure. This mode also supports IP Pass-through where the mobile IP address is passed through to the router.

Failover via a LAN port is usually more difficult since a floating static route or similar must be configured with a higher metric to redirect traffic to the Digi gateway's Ethernet address.

It is important to note, that in cases other than VRRP, the Digi device itself does not do anything to initiate or terminate the failover connection. It is up to the primary router to redirect traffic in the event of primary WAN failure.

Also note that Digi cellular gateways are designed to maintain an always-on cellular connection which helps facilitate quicker failover. Even IPsec tunnels can be nailed up.

The configuration of the Digi gateway depends on the network design and in what mode the customer's network dictates. There are five main modes of operation:

1. NAT mode (the default) without IPsec VPN; in this mode either security is not required, or the devices or workstations provide the security, or a private wireless plan is used.
2. NAT mode plus IPsec VPN tunneling; this is likely the required mode for retail stores, banks, etc. where end-to-end encryption is required.
3. Pass-through mode can be used when the Digi gateway connects to a designated WAN Ethernet port on the router. There are four sub-modes of "pass-through" operation:
 - a. IP Pass-through (i.e., bridging) mode, where the Digi device passes *all* traffic except designated "pin-hole" management traffic through to the router. NAT and routing are effectively disabled. The router's WAN port assumes the mobile IP address. This is the easiest and most common mode.
 - b. GRE forwarding where GRE protocol traffic is forwarded through the Digi gateway's NAT to the router's WAN port and terminated on the router.

- c. IPsec ESP forwarding where VPN traffic is forwarded through NAT to the router's WAN port. Here the Digi device does not process the IPsec traffic.
 - d. NAT-T forwarding where IPsec-in-UDP/TCP ports such as UDP ports 4500 and 500 are forwarded to the router.
4. NAT Disabled; rarely used; static routes applied to the Digi gateway. This is usually only possible where the carrier provides a private plan – i.e., the traffic does not route via the Internet. VPN may be used if security requirements, such as PCI compliance, require it. The examples below show the more common VPN tunnel modes.
 5. VRRP. Here the Digi device not only helps with “last-mile” failover, but can also work to backup the router itself.

[Notes:

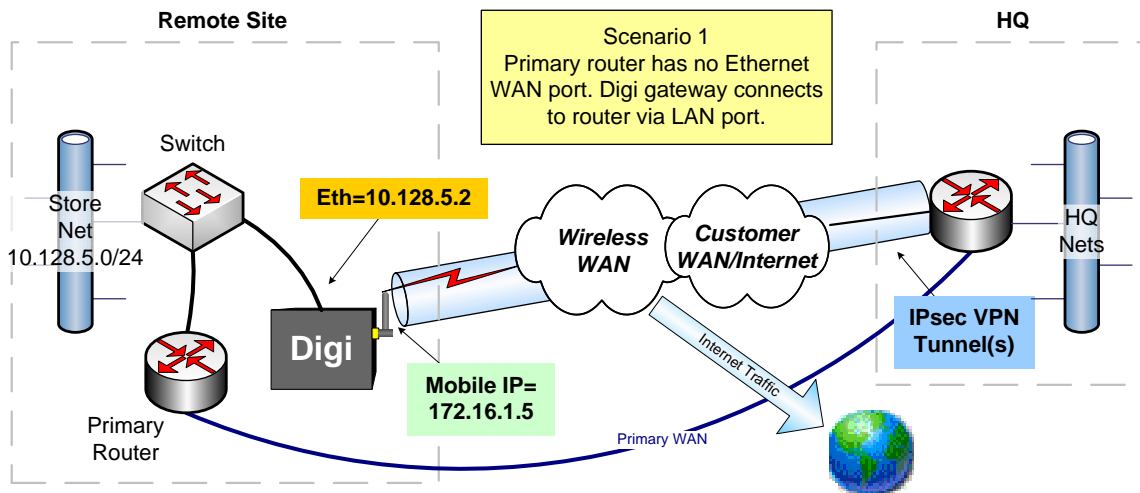
1: In most cases these same basic concepts can be applied when the Digi cellular gateway is used as the primary or only WAN connection.

2: This document assumes the wireless carrier provides an Internet connected plan. Many carriers can provide private wireless plans where traffic does not touch the Internet, thus providing more security. Check with your carrier for details.

3: Remote console management is also available using the Digi gateway's serial ports and the “Console Management” serial port profile. See the Console Management application note for details.]

NAT + IPsec VPN Split Tunneling

Here the Digi cellular gateway itself builds VPN tunnels from the remote site to each subnet necessary at the home office. (FYI: The ConnectPort™ WAN VPN supports 5 VPN tunnels; Digi Connect® WAN VPN supports 2 VPN tunnels.) Each remote site must be on its own separate subnet, i.e., a different subnet from the home office and from other remote sites.



How it works: In most cases, the Primary Router will be configured with a floating static route using a higher metric, such as 256, pointing to the Digi gateway's Ethernet IP address (e.g., 10.128.5.2). In some cases, an intelligent layer 3 VLAN switch could handle the routing and failover (note the Digi gateway does not support VLAN itself).

In either case, the Digi gateway will likely need to protect and encapsulate the traffic with IPsec. VPN policies on the Digi device might look something like (assuming the remote site net is 10.128.5.0/24 and this is a ConnectPort WAN VPN):

Source	Destination	Dept
10.128.5.0/24	10.10.0.0/16	Payroll/Benefits
10.128.5.0/24	10.11.0.0/16	IT (Mail servers, Intranet, etc)
10.128.5.0/24	10.12.0.0/16	Inventory Control
10.128.5.0/24	10.13.0.0/16	Marketing
10.128.5.0/24	10.14.0.0/16	Credit
Split Tunnel = yes		

Why use this scenario? There are two primary reasons:

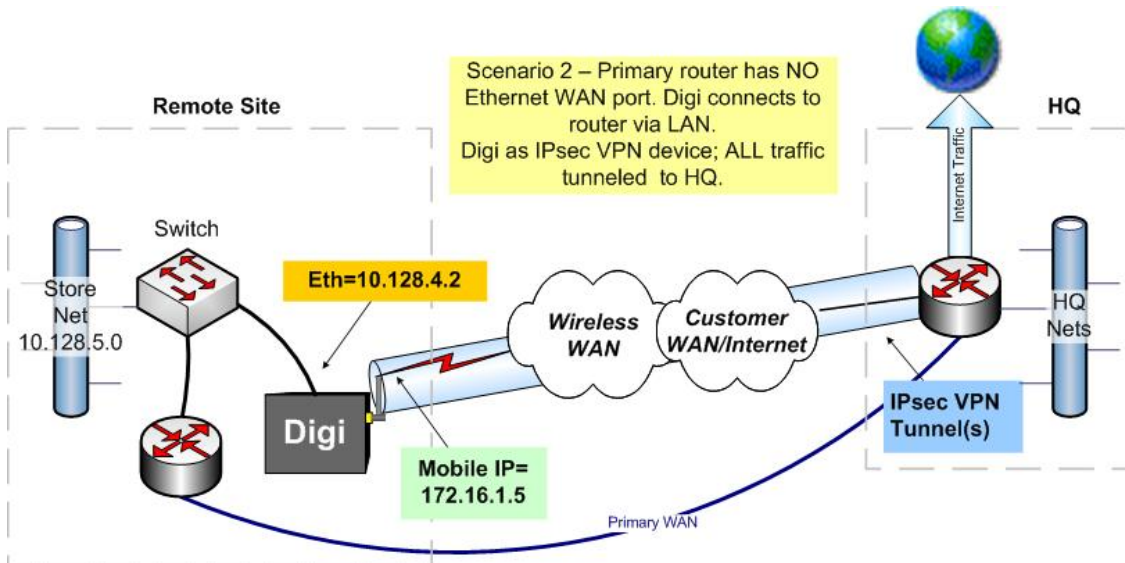
- (a) The primary router is connected to the Digi cellular gateway via LAN port or an Ethernet switch. It is likely the router cannot initiate a VPN tunnel from a LAN port; nor does the switch support VPN. Therefore the Digi device must create the VPN connection as required by the company's security policies for example to comply with PCI (Payment Card Industry) regulations.
- (b) Split tunneling where non-corporate Internet traffic flows outside the VPN tunnel(s) is acceptable (and assuming the wireless plan allows Internet traffic).

The major drawbacks are (a) multiple policies must be defined for each remote subnet, (b) there is no control of Internet traffic outside the realm of the VPN policies, and (c) as with all IPsec VPNs there will be 20-30% or more overhead due to IPsec encapsulation.

NAT + IPsec VPN Tunnel All Mode

"Tunnel All" mode is similar to the above, except that ALL traffic from the remote site is tunneled back to the home office via IPsec – i.e., no split tunneling. In the Digi device's VPN policy, the remote subnet is defined as 0.0.0.0/0.0.0.0. All routing and inspection is then done at HQ.

Digi Cellular Gateway WAN Backup Scenarios



Here is a sample VPN Policy on the Digi gateway:

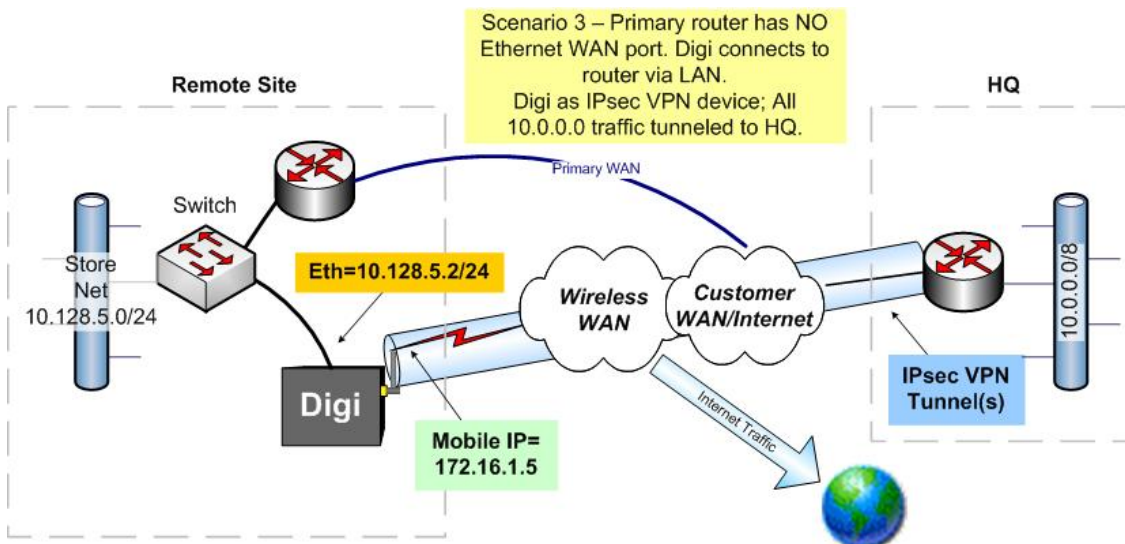
Source	Destination
10.128.4.0/24	0.0.0.0/0
Split Tunnel = NO	

Pros: All traffic is routed to the host network providing total control of Internet traffic and enhancing security at HQ. Only one VPN policy is needed for the remote site.

Cons: All traffic is routed to the host network so more management and capacity is required for routing, filtering and controlling Internet traffic at HQ.

NAT + IPsec Tunnel All 10.0.0.0 (or similar)

Here the Digi gateway allows extending the 10.0.0.0 network to 10.x.y.z remote subnets (or similar network configuration). This would allow split tunneling of traffic outside the 10.0.0.0 network but with only one VPN policy similar to:

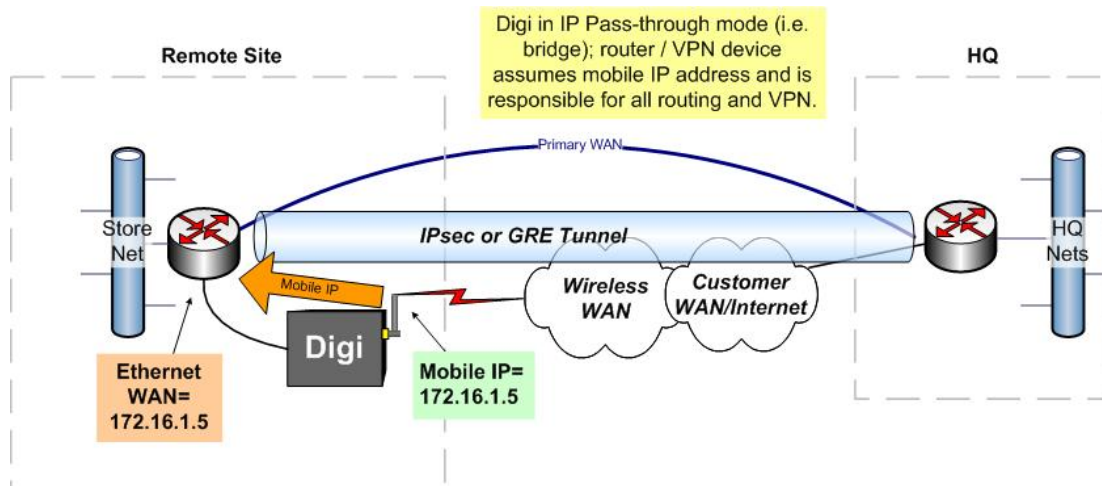


Source	Destination
10.128.5.0/24	10.0.0.0/8
Split Tunnel = yes	

Why use this method? This is somewhat a compromise between the two approaches above. It still allows split tunneling but simplifies the VPN policy configuration and helps facilitate a “flat” network.

IP Pass-through Mode

In this mode the Digi gateway passes the wireless carrier provided mobile IP address through to a router or VPN device. Here the Digi gateway performs much like a bridge. An Ethernet port on the attached device is designated as a “public” WAN port and assumes the mobile IP address. This address can be assigned statically or via DHCP. In this case, the primary router would likely terminate a VPN or GRE tunnel.



Why would you use this method? Here the primary router/VPN device controls all traffic except for Digi management traffic via “pinholes.” You may already be familiar with and prefer to use your existing routing and VPN policy setups.

However, the primary router/VPN device must have an available port that can be designated as a “WAN” port in a subnet separate from the remote site LAN network and the primary WAN port(s). Low-end routers typically have no such option. This option is usually used for primary connections.

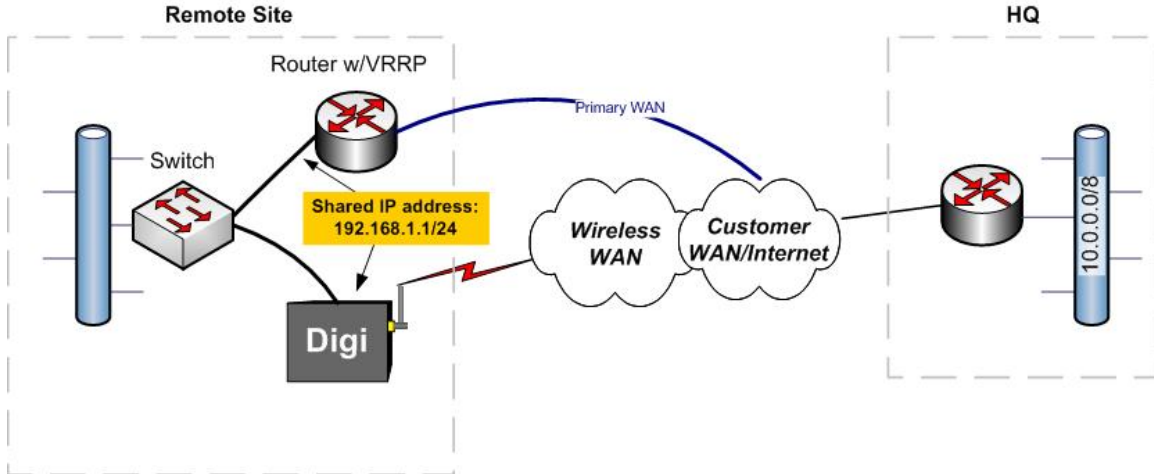
IP Pass-through mode provides management pinholes where the user can select protocols such as SSH, HTTP and telnet that terminate on the Digi cellular gateway itself to provide management functionality. Digi Connectware[®] Manager remote management is also still available.

VRRP

Digi cellular gateway firmware release 2.7 introduced support for VRRP. VRRP is an open standard used for router redundancy. Here the Digi gateway would be in “stand-by” mode until needed. The Digi device normally assumes the same IP address as the primary router.

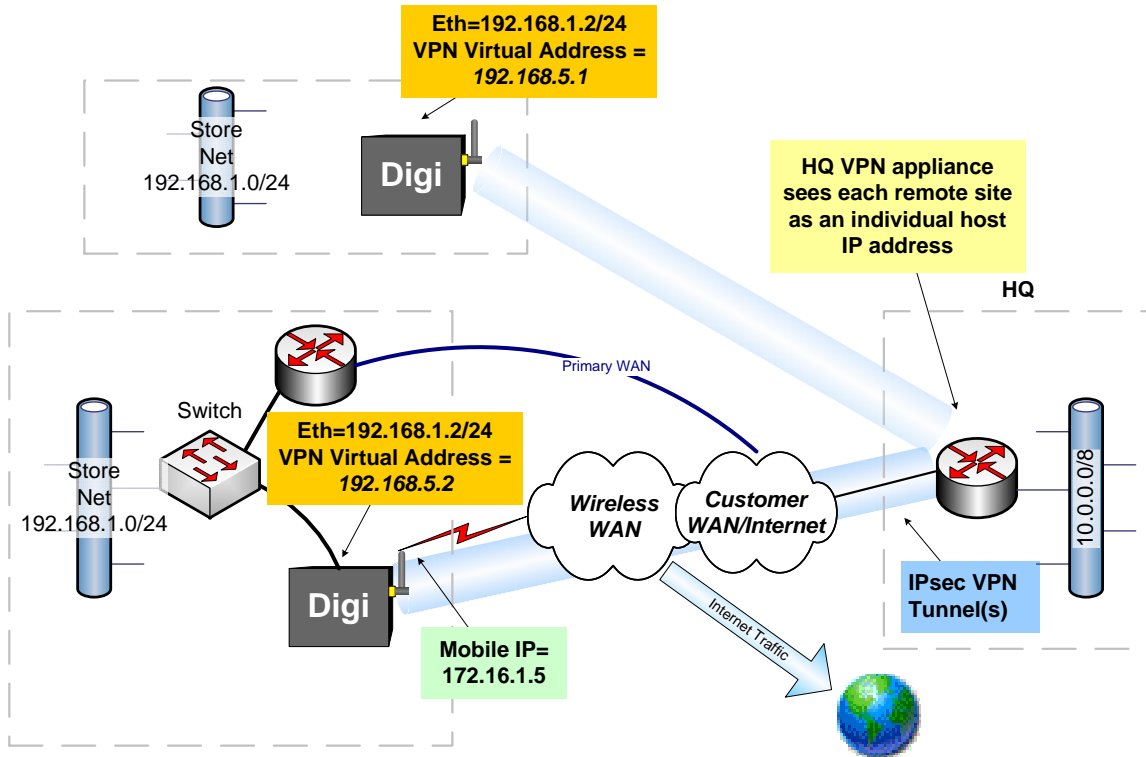
Digi Cellular Gateway WAN Backup Scenarios

In this case, the Digi gateway not only provides failover for the last mile, but in many cases, the router itself. So, if the router dies, all routing goes through the Digi device.



Virtual Host VPN Mode

This is a special case and rarely used in WAN failover. It provides sort of a “cookie-cutter mode” since it allows remote sites to all have the same IP subnet addresses such as 192.168.1.0/24. In this mode the local subnet attached to the Digi gateway is “NAT’d” via a VPN tunnel connection to a single IP address – the “virtual host.” Hence, the HQ VPN concentrator sees only a single IP address as the remote VPN network, similar to a VPN client.



This mode is useful where many sites, such as ATMs or retail remote sites, all use the same subnet; or where credit transactions are sent to a processor who has no control over the remote networks IP addressing. Just like with any NAT, IP forwarding entries may be needed to push inbound traffic through NAT. This scenario is typically used as a primary connection only.

Other Options

There are other options where the Digi cellular gateway remains in NAT mode and forwards IPsec ESP, GRE, or NAT-T traffic through to a router or VPN device. These methods may be chosen for any number of reasons such as security or specific functionality. These modes were supported before Digi implemented IP Pass-through but are still valid and used in some instances. One example is where the Digi gateway can create a DMZ where, for example, a web server is attached via Ethernet and is accessible from the outside, while a VPN firewall appliance is used to restrict LAN access to workstation. Here is a summary of these modes:

- GRE protocol is forwarded through NAT to a router on the remote site LAN.
- IPsec ESP protocol is forwarded through NAT to a router or VPN device on the remote site LAN. UDP port 500 for IKE should also be forwarded.
- NAT-T: Here IPsec traffic is encapsulated typically in UDP in order to traverse NAT firewalls. The UDP port is usually 4500. This port and UDP port 500 for IKE are forwarded through to Ethernet.

Further information and assistance is available at www.digi.com or by calling Digi at 952-912-3444. Technical documents including setup for specific VPN appliances, IP Pass-through, etc. can be found at www.digi.com/support.