Application Note 53

Configure a Digi TransPort Router to use DMNR (Dynamic Mobile Network Routing)

Digi Technical Support
November 2015

Contents

1 INTRODUCTION

1.1 Outline

This application note describes how to configure a Digi TransPort router to use the Dynamic Mobile Network Routing (DMNR) service. DMNR is available on Verizon Wireless Private Networks. DMNR provides direct access to devices on the Local Area Network (LAN) at your company's sites by dynamically advertising locally IP subnets attached to the Digi TransPort's Ethernet interface(s). Please refer to Verizon Wireless for more details on DMNR and whether your network uses DMNR or is eligible for DMNR.

There are two distinct DMNR operating modes on the Digi TransPort:

1. *Connecting to a service provider's (e.g., Verizon Wireless) DMNR-enabled network*. In this mode the Digi TransPort router operates as a DMNR client only. The operational parameters are supplied by the service provider.
2. *Using the DMNR service to connect in client/server mode (TransPort router to TransPort router over an IP network)*. In this mode there is no DMNR network provider, and one TransPort will act as client and one as server. The primary use is for test purposes or for applications in which a normal GRE tunnel might be used but one of the following features is also required:
    a. NAT traversal of the tunnel.
    b. Authentication.
    c. No requirement for the Server to know the clients IP address (i.e. in the case the client has a dynamic IP address provided to it).
    d. Dynamic route updates on the server. No need for pre-configured routes as when the client registers its subnets these are added into the routing table on the server (they are removed if/when the tunnel goes down).

CLI commands are shown at the end of this document in the "CONFIGURATION FILE" section.

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.

Other assumptions are:

- The Digi TransPort at its factory default configuration (not necessarily a requirement, but used in this document).
- It has been registered and activated on the appropriate Verizon Wireless Private Network that supports DMNR in the case of using on Verizon Wireless.

Documentation: In addition to this guide, full Digi TransPort documentation, including the *Digi TransPort User Guide*, is available on the Digi tech support site at www.digi.com/support.

This application note applies only to:

Models: Digi TransPort WR11, WR21, WR41, WR44

Digi TransPort WR41 routers must have the *Protocol Switch* (or *Enterprise* software) option
Digi TransPort WR21 routers must have the *Enterprise* software option

Firmware versions: 5212 and later

Please note: This application note has been specifically written for firmware release 5212 and later; earlier versions of firmware do not support DMNR. Please visit www.digi.com/support for firmware updates or email tech.support@digi.com with related questions.

1.3 Suggestions and Corrections

Requests for suggestions, corrections or amendments to this application note are welcome and should be addressed to: tech.support@digi.com
Requests for new application notes can be sent to the same address.

1.4 Version

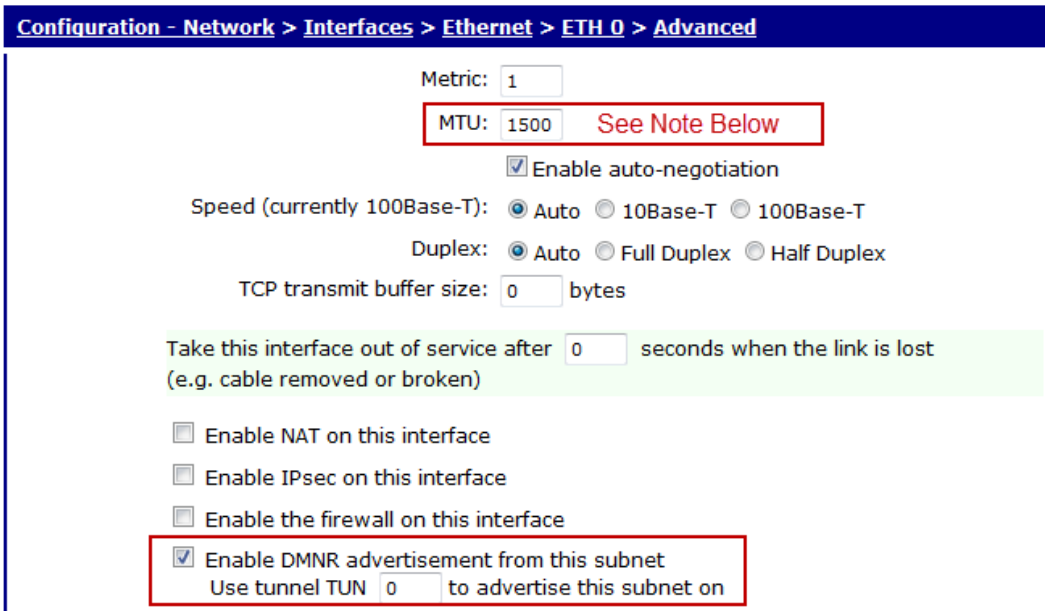
Version Number	Status
1.0	Published
1.1	Minor Updates (2014-March)
1.2	Add Static Route to HA, server mode section and minor edits (2014-June)
1.3	Added Home address details, updated screenshots to reflect GUI changes (2015-November)

2 CONFIGURATION

2.1 Determine the Subnet(s) to be Advertised

Configure the Digi TransPort DMNR client router as shown below. In this example the subnet defined on Ethernet (ETH) 0 will be advertised on the DMNR tunnel. To configure this on the web interface browse to:

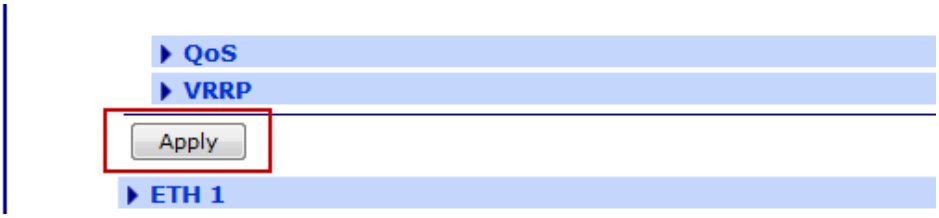
Configuration – Network > Interfaces > Ethernet > ETH0 > Advanced



Parameter	Setting	Description
Enable DMNR advertisement from this subnet	Checked	Enable DMNR on ETH0

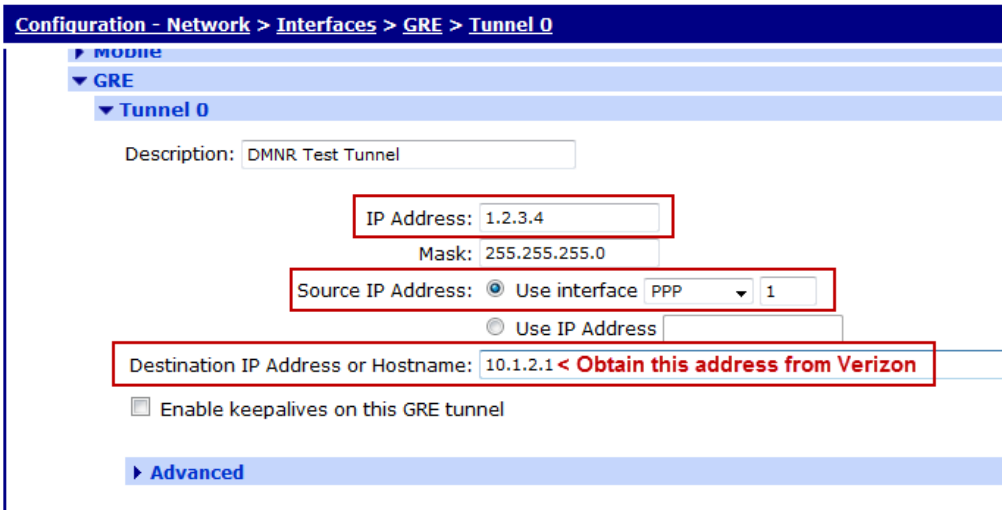
Note: The MTU size of the Ethernet interface is 1500. This is permitted to be different than the MTU size of the DMNR (GRE) tunnel defined below. The DMNR tunnel MTU will be smaller to take into account the required headers (i.e., the TUN interface will have a smaller MTU).

Click "**APPLY**" at the end of each step to apply the changes to the running config. It is okay to Save changes at each step, but is not necessary until the last step. Changes will be lost if the TransPort router is rebooted or power is lost before the applied changes are saved.



2.2 Configure the DMNR Tunnel

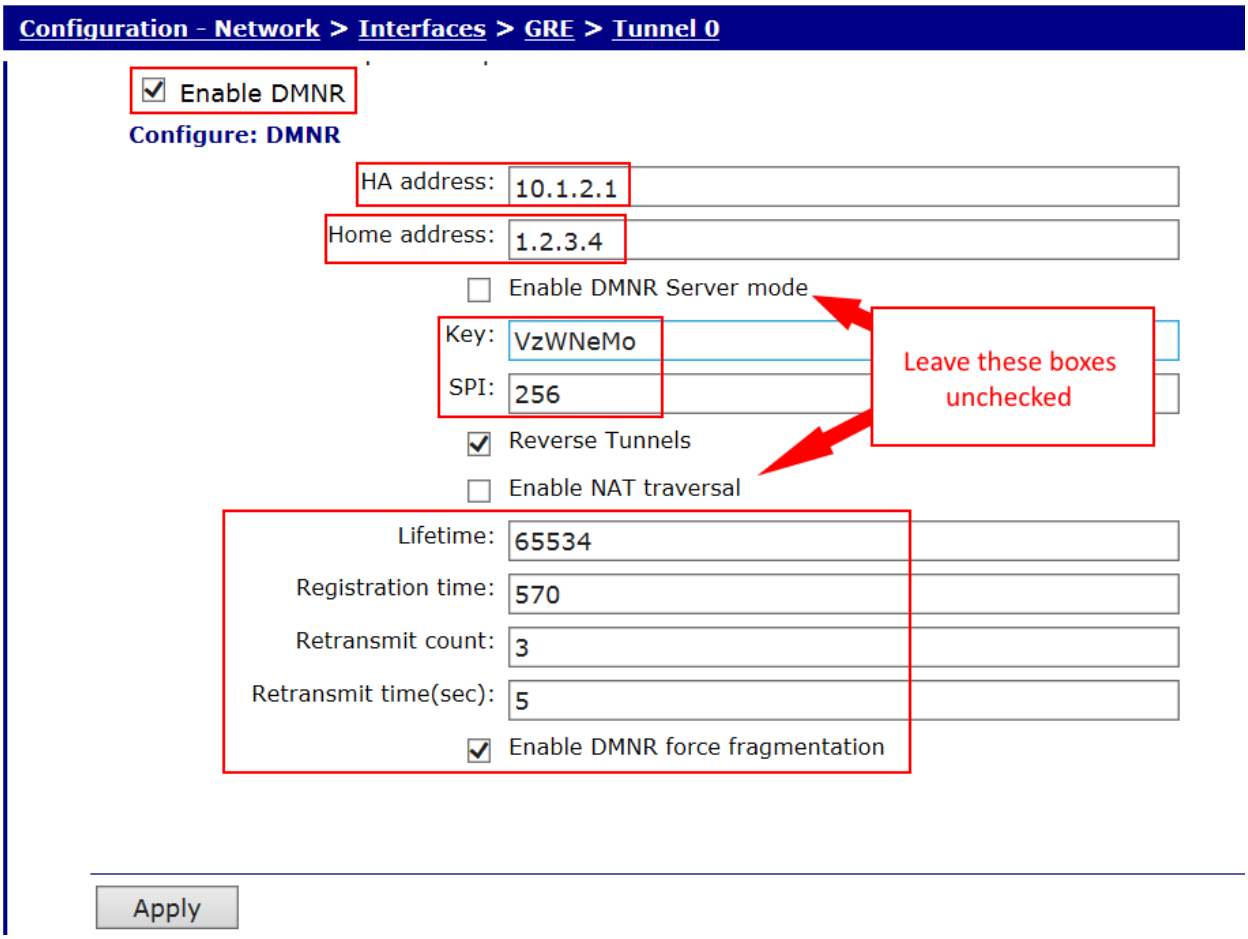
Configuration – Network > Interfaces > GRE > Tunnel 0



Parameter	Setting	Description
Description	DMNR Test Tunnel	Tunnel Description
IP Address	1.2.3.4	IP Address of the GRE interface. 1.2.3.4 is recommended.*
Source IP Address	PPP 1	The source address of the tunnel is normally the mobile interface IP address, which on most Digi TransPort routers is PPP 1
Destination IP Address or Hostname	Supplied by Verizon Wireless	The HA address will vary by gateway. This address is provided by Verizon Wireless.

* - The GRE interface is used to create a dynamic DMNR tunnel. This address is not used for routing, but as a dummy address for the DMNR tunnel. All DMNR client routers can use this same address. 1.2.3.4 is the recommended address. Your service provider may use of a different address.

Configuration – Network > Interfaces > GRE > Tunnel 0 > Advanced



NOTE: The GRE MTU default is 1400 bytes. It should be no greater than 1430. Please check with the DMNR service provider before making changes to the GRE MTU size.

Parameter	Setting	Description
Enable DMNR	Checked	Enable DMNR on this GRE tunnel
HA address	Supplied by Verizon	Home Agent address is the destination address for the DMNR registration requests.
Home address	1.2.3.4	Non-routable (placeholder) dummy IP address for the TransPort end of the DMNR tunnel. Leave it to default.
Enable DMNR Server Mode	Unchecked	For testing purposes; leave unchecked for Verizon DMNR
Key	VzWNeMo	Authentication key (normally VzWNeMo)
SPI	256	Security Parameter Index (normally 256)
Enable NAT Traversal	Unchecked	Leave unchecked for Verizon DMNR as the mobile IP address is not NAT'd
Reverse Tunnels	Checked	Reverse tunnels, build tunnel after registration
Lifetime	65534	The lifetime in seconds requested to the HA
Registration time	570	Registration interval in seconds
Retransmit count	3	Registration retries allowed
Retransmit time(sec)	5	Time delay between retries
Enable DMNR Force Fragmentation	Checked	Required by Verizon

Enable DMNR, when checked, will display the DMNR configuration parameters and enable DMNR.

HA address, Home Agent address is the destination address for the DMNR registration requests. In this case (and typically, but not always) the destination address for the registration request is the same as the destination for the GRE tunnel.
The HA address will vary by gateway, please obtain the appropriate address from your Verizon Sales Engineer / Solutions Architect.

Home address, is Non-routable and is used as a placeholder "dummy" IP address for the TransPort end of the DMNR tunnel. It may be the same on multiple routers. Any IP can be used, recommended to leave the default value of 1.2.3.4

Key, Authentication key. Required for authentication and is provided by the service provider.
For Verizon the value is always: VzWNeMo

SPI, Security Parameter Index. It will always be 256 unless otherwise indicated by the service provider. It is used in the authentication extension when registering.

Reverse Tunnels, this parameter is required unless otherwise indicated by the service provider. The client side creates the GRE tunnel after the registration has been accepted.

Lifetime, the lifetime in seconds requested to the Home Agent. The Home Agent will provide the actual lifetime to use when responding to a registration request so this value is unlikely to be used. It is just the initial request, but is required.

Registration time, there is a requirement to re-register periodically. This is a negotiated parameter between the DMNR client and server and specifies the Digi TransPort's intent in seconds with regard to this. If the server responds with a lifetime which is lower, then the server's value will be used. The TransPort will re-register when 90% of the lifetime of the tunnel has expired. Setting this to 0 means the lifetime indicated by the HA is the sole determination of how often re-registration takes place.

Retransmit count, when registering or re-registering this parameter controls how many retransmits are made in the event that a registration reply is not received.

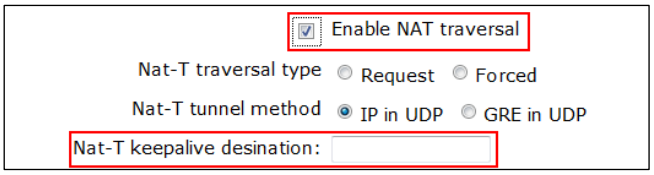
Retransmit time (secs), the time in seconds allowed for a response to a registration request, if no response is received to a registration request after this time, the router sends a new registration request.

Enable DMNR force fragmentation, required by Verizon Wireless.

2.3 OPTONAL: NAT Traversal (not required with Verizon DMNR)

SKIP this step unless advised to enable NAT by the DMNR service provider (where the mobile IP address will have NAT applied between it and the HA) or testing is being done with Digi TransPort DMNR Server mode where the DMNR client's WAN IP addresses is behind NAT.

Configuration – Network > Interfaces > GRE > Tunnel 0 > Advanced



Parameter	Setting	Description
Enable NAT traversal	checked	Enables NAT-T
Nat-T traversal type	Request	The NAT traversal type, Requested or Forced
Nat-T tunnel method	IP in UDP	The NAT traversal method. Obtain this from DMNR service provider.
NAT-T keepalive destination	10.1.2.1	Destination address for NAT-T keepalives. Obtain this from DMNR service provider.

Enable NAT traversal, when enabled the router will request NAT traversal along with the NAT traversal method.

Nat-T traversal type, if Request option is selected and the HA agrees to NAT-T it will be enabled and used. If Request is selected and NAT traversal is declined by the server a non-NAT-T tunnel can still be activated and registered. If Force is selected and HA declines NAT-T, the TUN interface will be remain DOWN.

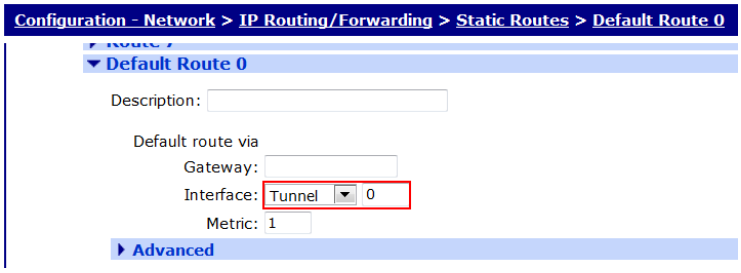
Nat-T tunnel method, needs to be obtained from the DMNR service provider (or in Server Mode match between the Server and the Client).

Nat-T keepalive destination, destination address for NAT traversal keep-alive packets. NAT traversal uses UDP headers to carry the tunnelled data, it is a requirement for keep-alives to be sent periodically to keep NAT entries from timing out. The destination address should be obtained from the DMNR service provider.

2.4 Configure the Default Route

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

As configured above, the normal source address for the Tunnel is the mobile interface, ppp 1. This configuration will route *all* traffic via the GRE tunnel. This default route will change its operational status and go UP or DOWN according to the status of the DMNR tunnel.

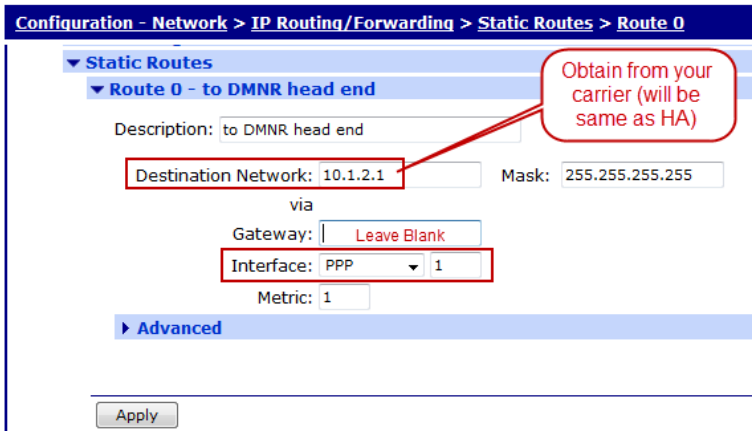


Parameter	Setting	Description
Interface	Tunnel 0	Configure Default Route 0 to send packets (that are not on local subnets) to tunnel 0

2.5 Add Static Route to DMNR Server (HA)

A static route is required to direct the DMNR / GRE traffic to the DMNR Server (HA).

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

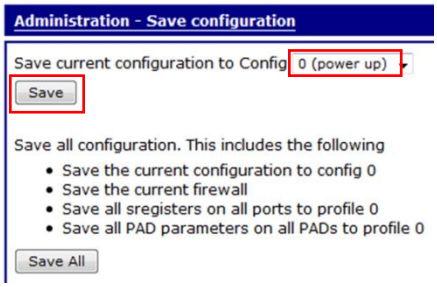


Parameter	Setting	Description
Destination Network	Obtain from Service Provider	Configure Static Route 0 to send packets to HA
Interface	PPP 1	Router Interface is PPP 1

2.6 Save configuration

Save the Configuration when the above changes are completed, if not done at the end of each step. Browse to **Administration - Save configuration**

Select the power up configuration (usually 0) and click 'Save'.



Changes will be lost if the configuration is not saved before a reboot.

2.7 Other configuration parameters that will affect DMNR registrations

The routing table is continually being monitored for any route or advertised subnet on the DMNR tunnel that changes state (i.e. goes "OOS" (out of service), or changes to "UP" from "OOS"). Any change in state will cause an immediate re-registration to be sent to the DMNR server. The Digi TransPort router has a range of features that can bring routes "UP" or take them "OOS" and these should be considered and all work in conjunction with DMNR.

Some typical configurations that might cause DMNR registrations to be sent:

a. Auto-pings.
b. Firewall configurations that monitor links could bring interfaces up/down.
c. VRRP. A transition from Master->Backup or from Backup->Master.
d. Ethernet connection physical status (if the Ethernet parameter "`eth x linkdeact y`" is set to "ON").

3 TESTING

Display the routing table to show the current status and if the TUN interface is up or down.

Administration – Execute a command (or CLI via SSH, Telnet or serial port)
route print

```
route print
       Destination          Gateway   Metric   Protocol  Idx Interface  Status
-------------------------------------------------------------------------------
         1.2.3.0/24          1.2.3.4      1      Local     -   TUN 0      UP
   10.211.179.83/32    10.211.179.83      1      Local     -   PPP 1      UP
       10.1.2.1/32    10.211.179.83      2     Static     0   PPP 1      UP
     192.168.1.0/24      192.168.1.1      1      Local     -   ETH 0      UP

         0.0.0.0/0          1.2.3.4      2     Static     0   TUN 0      UP
```

Default route 0 on TUN 0 is up.

The Event Log (**Management – Event Log** or **type eventlog.txt**) will show the tunnel come up or if there is a problem (note, newest entries are at the top):

```
19:30:47, 03 Oct 2013,TUN 0 up
19:30:47, 03 Oct 2013,DMNR tunnel 0 up
```

Management - Network Status > Interfaces > GRE (or CLI: “tunstat 0”) will show the status of the tunnel:

```
tunstat 0
Tun 0 stats:
   Admin Status           Up
   Oper Status            Up
   IP Address             1.2.3.4
   Mask                   255.255.255.0
   Source                 PPP 1 (10.211.179.83)
   Destination            10.1.2.1
   Tx Packets             204
   Tx Bytes               12648
   Tx Errors              0
   Tx Discards            0
   Rx Packets             220
   Rx Bytes               13844
   Rx Errors              0
   Rx Unknown Protocols   0
   Keepalives Sent        0
   Keepalives Rcvd        0
```

If the tunnel does not establish, the event log will provide information (**Management – Event Log** or **type eventlog.txt**).

In this case the remote DMNR peer, 10.1.2.1, is not responding:

```
19:32:38, 04 Mar 2014,DMNR tunnel 0 down, ,No registration reply
19:32:28, 04 Mar 2014,IP Act_Rq to TUN 0-0: s_ip[0.0.0.0] d_ip[10.1.2.1] d_port[434]
```

Verify the proper HA address has been entered and that a route has been added to the HA.

Here the Key and/or SPI do not match between client and server:

```
02:28:54, 01 Jan 1970,DMNR reg packet discarded, code:Mobile router operation not
          permitted,Authentication error
02:27:17, 01 Jan 1970,DMNR reg packet discarded, ,ID mismatch
```

Verify the proper Key and SPI configuration.

3.1 Using the Analyser to Capture DMNR Traffic

The TransPort's Analyser is a built-in packet capture tool. This is helpful to see the DMNR traffic, which uses UDP port 434 (Mobile IP), going through the mobile PPP 1 interface.

Management - Analyser > Settings
Configure the Analyser as needed. Enable IP Sources on PPP 1; other interfaces and protocols are not needed in this instance, unless tracing of traffic on Ethernet ports is needed.

Traffic can be filtered *out* by entering the values (ports, IP addresses, etc) as needed, separated by commas. For example, to filter out Web go to IP Packet Filters, TCP/UDP Ports: and enter:

TCP/UDP Ports: 80,443

Filter in traffic, such as just the DMNR traffic, by preceding the values with tilde "**~**":

TCP/UDP Ports: ~434

Press Apply then Save the config if desired.

Management - Analyser > Trace
The Analyser trace is stored in the file **ana.txt**. **PCAP** files are also generated to allow viewing the trace in WireShark.

Here is a sample trace showing DMNR traffic leaving the "client" (10.187.216.148) to the DMNR HA "server" (10.1.2.1) and the response back:

```
-----   6-1-2000  04:14:12.970   -------
45 00 00 5E 00 48 00 00 FA 11 CA 13 0A BB D8 94     E....H....Ê...Ø”
A6 82 6C 61 07 DE 01 B2 00 4A F3 67 04 2F 00 00     ¦.la.Þ.².J.g....
45 00 00 3E 00 05 00 00 FA 2F CA 58 0A BB D8 94     E.........ÊX..Ø”
A6 82 6C 61 00 00 08 00 45 00 00 26 00 05 00 00     ¦.la....E.......
F9 01 50 AF AC 10 18 01 AC 10 01 01 08 00 F4 1C     ..P.............
0D 83 00 05 01 78 00 00 00 03 E7 33 0D AC           .ƒ...x.....3..

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 5E          Length:        94
00 48          ID:            72
00 00          Frag Offset:   0
               Congestion:    Normal
                              May Fragment
                              Last Fragment
FA             TTL:           250
11             Proto:         UDP
CA 13          Checksum:      51731
0A BB D8 94    Src IP:        10.187.216.148        ← this is the mobile IP
A6 82 6C 61    Dst IP:        10.1.2.1
UDP:
07 DE          SRC Port:      ??? (2014)
01 B2          DST Port:      ??? (434)
00 4A          Length:        74
F3 67          Checksum:      62311
----------
   -----   6-1-2000  04:14:16.100   -------
   45 18 00 5E 00 0E 00 00 EB 11 D9 35 A6 82 6C 61     E.......ë.Ù5¦.la
   0A BB D8 94 01 B2 07 DE 00 4A F3 67 04 2F 00 00     ..Ø”.².Þ.J.g....
   45 00 00 3E 00 05 00 00 FA 2F CA 58 A6 82 6C 61     E.........ÊX¦.la
   0A BB D8 94 00 00 08 00 45 00 00 26 00 15 00 00     ..Ø”....E.......
   FA 01 4F 9F AC 10 01 01 AC 10 18 01 00 00 FC 1C     ..OŸ............
   0D 83 00 05 01 78 00 00 00 03 E7 33 0D AC           .ƒ...x.....3..

   IP (In) From REM TO LOC       IFACE: PPP 1
   45             IP Ver:        4
                  Hdr Len:       20
   18             TOS:           Routine
                  Delay:         Low
                  Throughput:    High
                  Reliability:   Normal
   00 5E          Length:        94
   00 0E          ID:            14
   00 00          Frag Offset:   0
                  Congestion:    Normal
                                 May Fragment
                                 Last Fragment
   EB             TTL:           235
   11             Proto:         UDP
   D9 35          Checksum:      55605
   A6 82 6C 61    Src IP:        10.1.2.1
   0A BB D8 94    Dst IP:        10.187.216.148
   UDP:
   01 B2          SRC Port:      ??? (434)
   07 DE          DST Port:      ??? (2014)
   00 4A          Length:        74
   F3 67          Checksum:      62311
```

4 CONFIGURATION FILE

Digi TransPort WR21 running configuration from the "**`config c show`**" command is listed below**.** Pertinent DMNR and GRE commands are **highlighted**; these commands can be entered directly into the command line interface. Enter "**`saveall`**" to save the config after entering CLI commands.

NOTES:

- This is a sample configuration where DMNR was enabled on an otherwise factory default Digi TransPort WR21 Verizon LTE router.
- Some WebUI parameters shown above are not listed in the configuration, nor are required as they are at the factory default value.
- Complete parameter settings can be obtained by entering the entity and instance. E.g., "**`tun 0 ?`**"

```
eth 0 IPaddr "192.168.1.1"
eth 0 dmnr_reg ON
addp 0 enable ON
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 3 dtemode 0
lapb 4 dtemode 0
lapb 5 dtemode 0
lapb 6 dtemode 0
ip 0 cidr ON
route 0 descr "to DMNR head end"
route 0 IPaddr "10.1.2.1"
route 0 ll_ent "PPP"
route 0 ll_add 1
def_route 0 ll_ent "TUN"
dhcp 0 IPmin "192.168.1.100"
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "192.168.1.1"
ppp 0 timeout 300
ppp 1 name "W-WAN"
ppp 1 phonenum "*98*3#"
ppp 1 username "username"
ppp 1 epassword "KD5lSVJDVVg="
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 use_modem 1
ppp 1 cdma_backoff ON
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 pwr_dly 20
ppp 1 ipanon ON
ppp 1 r_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
modemcc 0 info_asy_add 4
modemcc 0 apn "none"
modemcc 0 link_retries 10
modemcc 0 stat_retries 30
modemcc 0 check_reg 0
modemcc 0 sms_access 1
modemcc 0 sms_concat 0
modemcc 0 link_retries_2 10
modemcc 0 stat_retries_2 30
modemcc 0 check_reg_2 0
```

```
ana 0 anon ON
ana 0 l1on 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 "KD5lSVJDVVg="
user 1 access 0
user 2 access 0
user 3 access 0
user 4 access 0
user 5 access 0
user 6 access 0
user 7 access 0
user 8 access 0
user 9 access 0
local 0 transaccess 2
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
tun 0 descr "DMNR Test Tunnel"
tun 0 IPaddr "1.2.3.4"
tun 0 source_ent "PPP"
tun 0 source_add 1
tun 0 dest "10.1.2.1"
tun 0 dmnr_enable ON
tun 0 dmnr_haddr "10.1.2.1"
tun 0 dmnr_key "VzWNeMo"
tun 0 dmnr_spi 256
cloud 0 ssl ON
```

5 OPTIONAL - DMNR SERVER MODE

5.1 Outline / Notes

DMNR Server mode is primarily used for testing in a non-DMNR enabled network environment. A Digi TransPort router acts as a DMNR server (i.e., HA) to terminate DMNR/GRE from a TransPort client. Server configuration is similar to setting up the Client configuration, with the changes shown below on the "Server" TransPort.

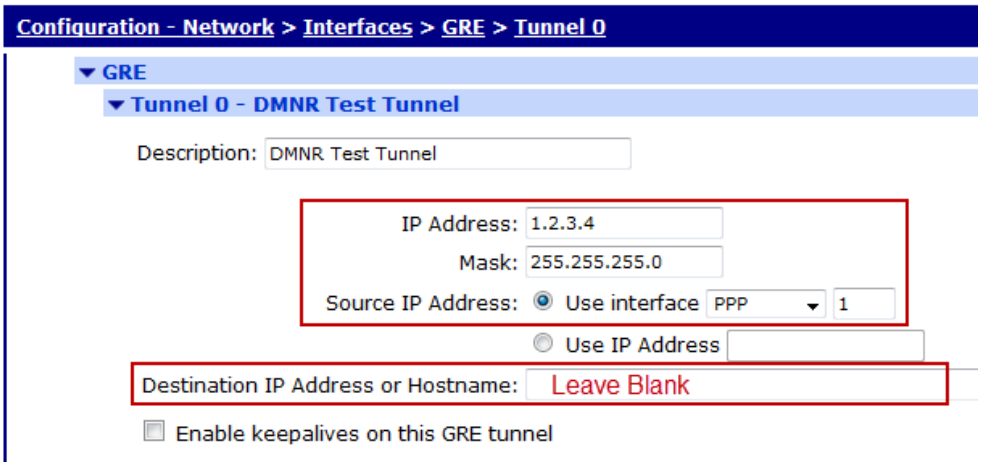
Notes:

- The WAN IP address of the Server must be accessible from the Client.
- The WAN port can be either mobile PPP (e.g., cellular), DSL, or Ethernet. Any of these interfaces can be used to test DMNR.
- No Static Routes are needed.

5.2 Configure DMNR "Server"

Configuration – Network > Interfaces > GRE > Tunnel 0

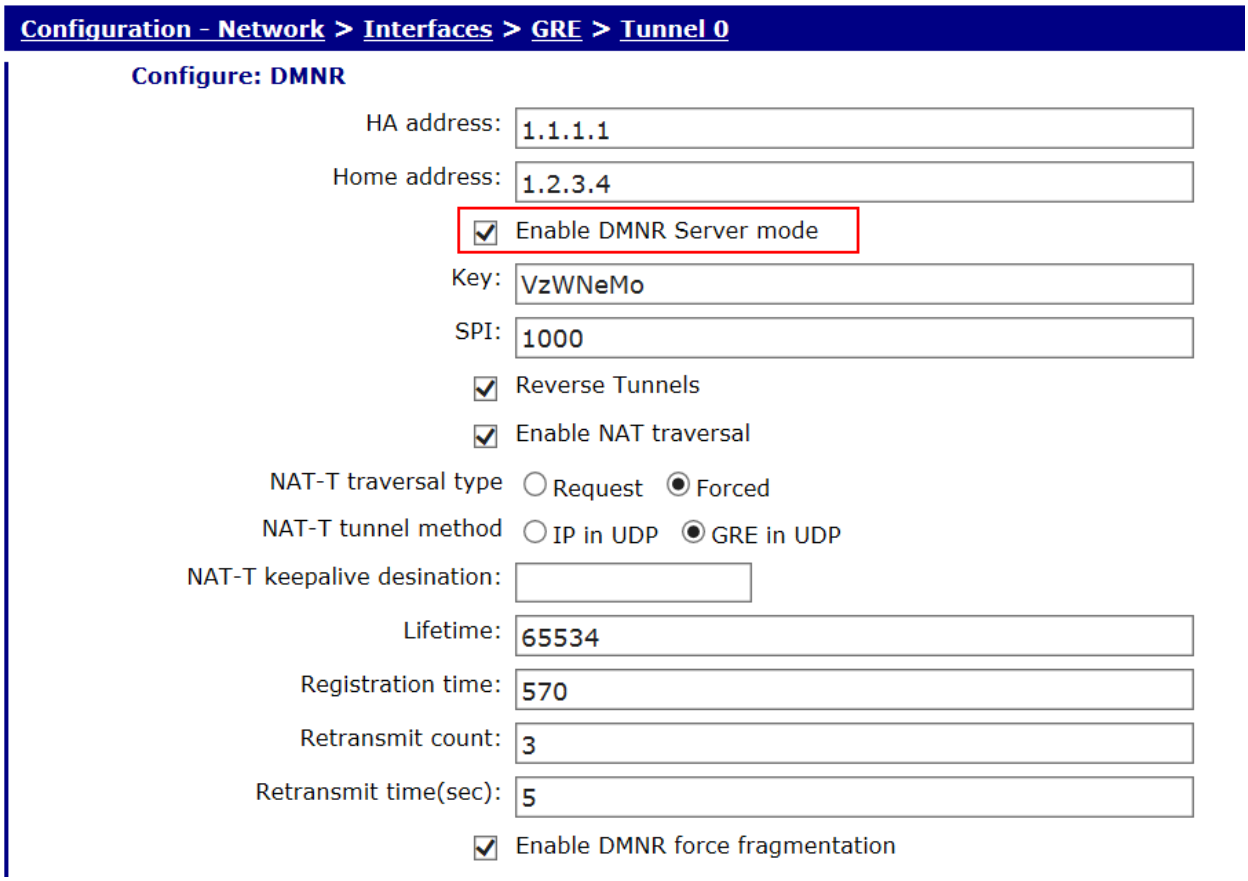
This is identical to the Client config, other than leaving the Destination IP blank to allow any WAN IP address to connect:



Parameter	Setting	Description
Description	DMNR Test Tunnel	Tunnel Description
IP Address	1.2.3.4	IP Address of the GRE interface. 1.2.3.4 is recommended.*
Source IP Address	PPP 1	The source address of the tunnel is normally the mobile interface IP address, which on most Digi TransPort routers is PPP 1
Destination IP Address or Hostname	BLANK	Leave Blank to allow ANY IP address to connect

Configuration – Network > Interfaces > GRE > Tunnel 0 > Advanced

Note any SPI and Key values can be used, but must *match* the client configuration.



Parameter	Setting	Description
Enable DMNR	Checked	Enable DMNR on this GRE tunnel
HA address	1.1.1.1	Can be any address. 1.1.1.1 works.
Home address	1.2.3.4	Non-routable (placeholder) dummy IP address for the TransPort end of the DMNR tunnel. Leave it to default.
Enable DMNR **Server Mode**	Checked	For testing purposes; leave unchecked for Verizon DMNR
Key	Any value; must match client	Authentication key (normally VzWNeMo)
SPI	Any value; must match client	Security Parameter Index (normally 256)
Enable NAT Traversal	As needed	Enable if the client's WAN (e.g. mobile) IP address is NAT'd
Reverse Tunnels	Checked	Reverse tunnels, build tunnel after registration
Lifetime	65534	The lifetime in seconds requested to the HA
Registration time	570	Adjust as needed for testing purposes
Retransmit count	3	Registration retries allowed
Retransmit time(sec)	5	Time delay between retries
Enable DMNR Force Fragmentation	Checked	Must match client

5.3 Testing and Verification

Follow the procedures above. Here are sample output from the server:

From the **Event Log**:

```
22:32:23, 08 Jan 2000,TUN 0 up
22:32:23, 08 Jan 2000,DMNR tunnel 0 up
```

route print:

```
route print
       Destination           Gateway   Metric   Protocol  Idx Interface  Status
-------------------------------------------------------------------------------
         1.2.3.0/24           1.2.3.4      1      Local     -   TUN 0      UP
  166.130.108.96/30   166.130.108.97      1      Local     -   PPP 1      UP
     172.16.1.0/24       172.16.1.1      1      Local     -   ETH 0      UP
     172.16.5.0/24      172.16.5.21      1      Local     -   ETH 1      UP
    192.168.1.0/24                       4       DMNR     -   TUN 0      UP

         0.0.0.0/0    166.130.108.97      2     Static     0   PPP 1      UP
```

Note the DMNR tunnel from the client's local LAN (192.168.1.0) shows in the Server's route table.