Application Note 41

Ethernet WAN Failover to Cellular/Mobile

Digi Technical Support

July 2016
# Contents

1 Introduction ................................................................................................................................. 3
  1.1 Outline .................................................................................................................................. 3
  1.2 Assumptions.............................................................................................................................. 3
  1.3 Corrections ............................................................................................................................... 5
2 Version ......................................................................................................................................... 5
3 Digi Transport Configuration ......................................................................................................... 5
  3.1 Overview ................................................................................................................................. 5
  3.2 Ethernet 0 Configuration ......................................................................................................... 5
  3.3 Ethernet 1 Configuration ......................................................................................................... 9
  3.4 Mobile Interface Configuration .............................................................................................. 10
  3.5 Default Route 0 Configuration ............................................................................................... 12
  3.6 Default Route 1 Configuration ............................................................................................... 14
  3.7 Firewall Configuration ........................................................................................................... 14
  3.8 Save Configuration .................................................................................................................. 17
4 Testing ......................................................................................................................................... 18
5 Firmware version .......................................................................................................................... 23
6 Configuration File ........................................................................................................................ 24
  6.1 WR41 Configuration File ....................................................................................................... 24
1 INTRODUCTION

1.1 Outline

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 (AN) applies to:

**Model:** Digi Transport WR44v2

**Other Compatible Models:** All Digi TransPort models with 2 or more Ethernet ports.

**NOTE:** Configuration on other TransPort models will need the changes specifically described here for the WR44v2. For example, on a DR router, the W-WAN interface is PPP 3 not PPP 1 and changes will be required to the firewall rules, the default routes and to the actual PPP interfaces to replicate the same functionality on the DR model. At the time of writing, this AN was tested on a WR44v2 and found to have exactly the same failover capabilities once the necessary modifications had been made. If advice is needed on any aspect of porting this AN to another device, please contact Digi Technical Support for further advice and assistance.

**Firmware versions:** 5.123 and later
NOTE: This AN was specifically rewritten for firmware release 5.123 and later but the original AN was tested and working with TransPorts running earlier firmware and the previous GUI. TransPorts running earlier firmware will find that the screenshots may not accurately reflect what will be seen on those older routers. Contact tech.support@digi.com if you require this document for the older GUI.
**TransPort Ethernet to WWAN Backup**

**Configuration:** This AN 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 AN, the following applies:

A working gateway device is already presumed to have been configured with a point-to-point subnet.

### 1.3 Corrections

Requests for corrections or amendments to this AN are welcome and should be addressed to: tech.support@digi.com

Requests for new ANs can be sent to the same address.

### 2 VERSION

<table>
<thead>
<tr>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
</tr>
<tr>
<td>2.0</td>
</tr>
<tr>
<td>2.1</td>
</tr>
</tbody>
</table>

### 3 DIGI TRANSPORT CONFIGURATION

#### 3.1 Overview

- Configure Ethernet – Primary WAN eth 0 and Local LAN eth 1.
- Configure mobile – the backup default route will be via mobile/cellular connection.
- Configure the default routes – primary via eth 0, secondary via Mobile.
- Configure the firewall – permit traffic, interfaces out of service when failure is detected.
- Review and test – to check correct performance of the project.

#### 3.2 Ethernet 0 Configuration

This configuration is the Ethernet subnet to the gateway router. The gateway router is assumed to be already configured with a working internet connection and LAN interface, the WR44v2 configuration here should be modified for use with your own gateway router.
Navigate to **Configuration - Network > Interfaces > Ethernet > ETH 0** and enter the values below.

**Parameter** | **Setting**                  | **Description**               |
-------------|------------------------------|-------------------------------|
Description  | <Description of Interface>   | Use something here that will be meaningful to your setup e.g. “Test WAN 44v2” |
IP Address   | 192.168.3.2                  | Ethernet 0 IP Address        |
Mask         | 255.255.255.252              | Ethernet 0 Subnet Mask       |
Gateway      | 192.168.3.1                  | Eth 0 Gateway address        |

Click the **Apply** button.
Configure the WAN side interface with NAT, auto pings, and out of service options.

Click the **Apply** button.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Isolate / Hub mode</td>
<td>Port Isolate</td>
<td>Confirm the device is in Port Isolate mode, otherwise switch to Port Isolate mode</td>
</tr>
<tr>
<td>Take this interface out of service after (&lt;n&gt;) seconds when the link is lost</td>
<td>1</td>
<td>To enable fast failover if the cable is removed</td>
</tr>
<tr>
<td>Enable NAT on this interface</td>
<td>Ticked + IP address</td>
<td>Reveals options for NAT mode select either IP address or IP address and port</td>
</tr>
<tr>
<td>Enable Bridge on this interface</td>
<td>Unticked</td>
<td>If the device has Wi-Fi – then we will want to bridge to the LAN interface ETH 1</td>
</tr>
<tr>
<td>Generate Ping packets on this interface</td>
<td>Ticked</td>
<td>This option will reveal the settings for ping generation on this interface</td>
</tr>
<tr>
<td>Send (&lt;n&gt;) byte pings...</td>
<td>0</td>
<td>Size of ICMP packet to send</td>
</tr>
<tr>
<td>...to IP host...</td>
<td>(&lt;IP to ping&gt;)</td>
<td>Valid IP address to ping for link up/down testing</td>
</tr>
<tr>
<td>...every (&lt;n&gt;) seconds</td>
<td>10</td>
<td>Interval in hours, minutes and seconds for the test pings to be sent</td>
</tr>
<tr>
<td>Only Send Pings when this Ethernet interface is “In Service”</td>
<td>Ticked</td>
<td>This will allow the firewall to control the pings sent to recover the interface when connectivity is working again</td>
</tr>
</tbody>
</table>
### 3.3 Ethernet 1 Configuration

This is the LAN interface configuration for this implementation, so this interface is configured with the LAN gateway IP address used by clients. In this example, no DHCP server has been setup but this can be easily added to the configuration. It is presumed for this example that the clients on the LAN are configured with a static IP address in the range allocated to this interface and will use the ETH 1 address as their network gateway address. The subnet mask for this network is 255.255.255.0

Navigate to **Configuration - Network > Interfaces > Ethernet > ETH 1**

![Configuration - Network > Interfaces > Ethernet > ETH 1](image)

Changes to these parameters may affect your browser connection

Click the **Apply** button.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>&lt;Description of Interface&gt;</td>
<td>Use something here that will be meaningful to your setup e.g. “Test LAN 44v2”</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.0.254</td>
<td>Ethernet 1 IP Address</td>
</tr>
<tr>
<td>Mask</td>
<td>255.255.255.0</td>
<td>Ethernet 1 Subnet Mask</td>
</tr>
</tbody>
</table>
Mobile Interface Configuration

If a SIM PIN is required for the mobile connection then enter this also here. Otherwise, for most implementations, only the APN will need to be entered. Upon navigating to the Mobile Settings configuration page, input the appropriate settings and then click the Apply button.

Navigate to Configuration - Network > Interfaces > Mobile

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings on this page apply to the selected SIM</td>
<td>SIM: 1 (PPP 1)</td>
<td></td>
</tr>
<tr>
<td>Mobile Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Plan / APN:</td>
<td>&lt;Enter APN&gt;</td>
<td>Enter your ISP’s APN value here.</td>
</tr>
</tbody>
</table>

NOTE: In this environment, there was no need to enter a PIN for the SIM or a username and password for the connection. If a SIM PIN, username and password is required, it would be entered on this configuration page.

On the WR44v2, the wireless WAN interface is PPP 1. On other platforms such as the DR64 this will be PPP 3.
Navigate to Configuration - Network > Interfaces > Advanced > PPP 0 – 9 > PPP 1 > Advanced

**Configuration - Network > Interfaces > Advanced > PPP 0 – 9 > PPP 1 > Advanced**

- **Advanced**
  - Metric: 1
  - Allow this PPP interface to settle for \(0 \times 100\) milliseconds after the connection has come up

  - **Enable “Always On” mode of this interface**
    - Attempt to re-connect after \(0\) seconds
    - If a PPP interface that would be inhibited by this PPP is connected, attempt to re-connect after \(0\) seconds
    - Wait \(0\) seconds after power-up before activating this interface

  - Keep this interface up for at least \(0\) seconds

  - Click [here](#) to assign a timeband to this interface

  - **Add a route to** [check](#) if the peer's IP address is not negotiated

  - **Enable DNS inbound blocking**

  - **Forward IP broadcasts over this interface if this interface is on the same IP network as an Ethernet interface**

  - **Send LCP echo request packet to the remote peer**

  - **Generate Heartbeats on this interface**

- **Generate Ping packets on this Interface**
  - Send \(1\) byte pings to IP host 8.8.8.8 every \(0\) hrs \(0\) mins \(10\) secs
  - Send pings every \(0\) hrs \(0\) mins \(0\) seconds if ping responses are not being received
  - Switch to sending pings to IP host after \(3\) failures
  - Ping responses are expected within \(0\) seconds
  - **Only send Pings when this Interface is “In Service”**

  - **New connections to resume with previous Ping interval**

  - **Reset the link if no response is received within \(0\) seconds**

  - **Use the ETH 0 IP address as the source IP address**

  - **Defer sending pings if IP traffic is being received**

Click the **Apply** button.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable “Always On” mode of this interface</td>
<td>Not ticked</td>
<td>Disable “Always on” mode</td>
</tr>
<tr>
<td>Generate Ping packets on this interface</td>
<td>Ticked</td>
<td>Reveals auto ping options</td>
</tr>
<tr>
<td>Send (&lt;n&gt;) byte</td>
<td>1</td>
<td>Size of ICMP packet to send</td>
</tr>
</tbody>
</table>
TransPort Ethernet to WWAN Backup

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pings</td>
<td></td>
<td>Valid IP address to ping for link up/down testing.</td>
</tr>
<tr>
<td>...to IP host...</td>
<td>&lt;IP to ping&gt;</td>
<td></td>
</tr>
<tr>
<td>...every &lt;n&gt; seconds</td>
<td>10</td>
<td>Interval in hours, minutes and seconds for the test pings to be sent</td>
</tr>
<tr>
<td>Only send Pings when this interface is “In Service”</td>
<td>Ticked</td>
<td>Pings will only be sent when the PPP interface is active</td>
</tr>
</tbody>
</table>

### 3.4 Default Route 0 Configuration

Change the Default Route from the (default) PPP 1 interface to Eth 0. The mobile interface (PPP 1) will be deactivated whenever this interface is in service.

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

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

> Default Route 0

**Description:**

**Default route via**

**Gateway:** 192.168.3.1

**Interface:** Ethernet 0

**Use PPP sub-configuration:** 0

**Metric:** 1

Click the **Apply** button.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway</td>
<td>192.168.3.1</td>
<td>Ethernet Gateway address</td>
</tr>
<tr>
<td>Interface</td>
<td>Ethernet 0</td>
<td>Eth 0 to be selected as the default interface</td>
</tr>
</tbody>
</table>

Navigate to **Configuration - Network > IP Routing/Forwarding > Static Routes > Default Route 0 > Advanced**
Click the **Apply** button.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>When this route becomes available, deactivate the following interfaces</td>
<td>PPP 1</td>
<td>Select PPP 1 as the interface to deactivate</td>
</tr>
</tbody>
</table>
3.5 Default Route 1 Configuration

This interface will be configured as an on demand interface, which will stop the router from sending unnecessary traffic to test the interface connectivity when the interface is not in service. Where data bandwidth is charged, this will keep transferred data on the wireless WAN link to a minimum.

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

Click the Apply button.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>PPP 1</td>
<td>Selects PPP 1 as the next available default route</td>
</tr>
</tbody>
</table>

3.6 Firewall Configuration

The firewall rules needed for this AN are very simple. There are only two rules to add:

1. The first rule will enable the monitoring of the ICMP traffic exiting the Ethernet 0 interface. If the ICMP traffic fails then this interface will be taken out of service and the recovery ping process will verify when the test host is responding to test traffic again.

2. The second rule will enable the monitoring of the ICMP traffic exiting the PPP 1 interface. If the traffic fails then this interface will be taken out of service, the PPP interface is deactivated then re-activated in attempt to get the PPP connection working again. If this rule is activated there will be a short interruption to service whilst a working network connection is established.
The default firewall rule set included in a production device will by default allow all outgoing traffic and restrict incoming traffic. You may want to filter more traffic than this using the extensive capabilities of the TransPort firewall. Please refer to the TransPort User Guide for more details on what the firewall can do for you.
Navigate to **Configuration - Security > Firewall**

**NOTE**: Clicking the "Insert" button will insert the rule just ABOVE.

Click the "Insert" button and type (or copy/paste) the following rule:

```plaintext
pass out break end on eth 0 proto icmp from addr-eth 0 to 195.92.195.92 icmp-type echo inspect-state oos 10 t=3 c=3 d=3 r=ping,3,3
```

Click "OK" to add the ETH 0 rule that’s just above.

Next, click the "Insert" button and type (or copy/paste) the following rule:

```plaintext
pass out break end on ppp 1 proto icmp from addr-ppp 1 to 195.92.195.92 icmp-type echo inspect-state oos 10 t=5 c=3 d=3
```

Click "OK" to add the PPP 1 rule that’s just above. You should now have 2 of the 3 rules added.

Click the “Insert” button and type (or copy/paste) the following rule:

```plaintext
pass break end
```

Click "OK" to add the final rule that’s just above.

Be sure to click the “Save” button, to write the firewall rules to the fw.txt file on the router’s FLASH.

The firewall configuration should look like this:

Scroll down to the Firewall configuration page to the Interface list and tick the boxes to enable the firewall on ETH 0 and PPP 1:

**Configuration - Security > Firewall**

The firewall can be enabled on Ethernet, PPP and GRE interfaces. Click [here](#) to jump to the GRE configuration page.

**Interface Enabled**

- ETH 0
- PPP 1

Click the **Apply** button to enable the firewall on those two interfaces.
NOTE: The IP address that is used in this environment for sending test pings to is not guaranteed to reply, so you should choose an IP address within your ISP’s or a public IP address that you own and have control of.

3.7  Save Configuration

Save the configuration to retain the config after reboot.
4 TESTING

From a device on the LAN configured on eth 1 (192.168.0.1), ping a public address. This can be the same address as used for the connectivity testing or any other address known to respond on both connections.

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Metric</th>
<th>Protocol</th>
<th>Idx</th>
<th>Interface</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.0/24</td>
<td>192.168.0.254</td>
<td>1</td>
<td>Local</td>
<td>ETH 1</td>
<td>UP</td>
<td></td>
</tr>
<tr>
<td>192.168.3.0/30</td>
<td>192.168.3.2</td>
<td>1</td>
<td>Local</td>
<td>ETH 0</td>
<td>UP</td>
<td></td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>2</td>
<td>Static</td>
<td>ETH 0</td>
<td>UP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>3</td>
<td>Static</td>
<td>PPP 1</td>
<td>DOWN</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The TransPort Analyser trace below shows that traffic is routing out of Eth 0, the default route. An ICMP echo reply (ping response) arrives from the source 192.168.0.1 on Eth 1 (the LAN interface) is sent out of Eth 0 to the gateway and a response is returned.
TransPort Ethernet to WWAN Backup

IP (Final) From LOC TO REM    IFACE: ETH 0
45             IP Ver:        4
00             Hdr Len:       20
00             TOS:           Routine
00             Delay:         Normal
00             Throughput:    Normal
00             Reliability:   Normal
00 26          Length:        38
00 03          ID:            3
00 00          Frag Offset:   0
00             Congestion:    Normal
                  May Fragment
                  Last Fragment
F8             TTL:           248
01             Proto:         ICMP
78 70          Checksum:      30832
C0 A8 03 02    Src IP:        192.168.3.2
C3 5C 5C 5C    Dst IP:        195.92.195.92
ICMP:
08             Type:          ECHO REQ
00             Code:          0
78 E5          Checksum:      58744

-------- 8-6-2011 16:39:43.840 --------
45 00 00 26 C8 B7 00 00 27 01 80 BC C3 5C C3 5C E...Ê.....€%ÃgL.
C0 A8 03 02 80 00 03 01 78 00 00 À¨....€å¢Æ...x..
00 01 86 4B 54 8C 00 00 00 00 00 00 00 00 00 00 00 00 ..†KTŒ...........
00 00 6B 21 FF FF ..k...

IP (In) From REM TO LOC       IFACE: ETH 0
45             IP Ver:        4
00             Hdr Len:       20
00             TOS:           Routine
00             Delay:         Normal
00             Throughput:    Normal
00             Reliability:   Normal
00 26          Length:        38
C8 B7          ID:            51383
00 00          Frag Offset:   0
00             Congestion:    Normal
                  May Fragment
                  Last Fragment
27             TTL:           39
01             Proto:         ICMP
80 BC          Checksum:      32956
C3 5C C3 5C    Src IP:        195.92.195.92
C0 A8 03 02    Dst IP:        192.168.3.2
ICMP:
00             Type:          ECHO REPLY
00             Code:          0
80 E5          Checksum:      58752

-------- 8-6-2011 16:39:43.840 --------
Blocking ICMP on the Ethernet gateway router results the default route 0 (Eth 0) being taken out of service and the message below (“Default Route 0 Out Of Service,Firewall”) being created in the Event Log:

```
16:45:53, 08 Jun 2011,PPP 1 up <<<
16:45:51, 08 Jun 2011,PPP 1 Start IPCP
16:45:51, 08 Jun 2011,PPP 1 Start AUTHENTICATE
16:45:51, 08 Jun 2011,PPP 1 Start LCP
16:45:50, 08 Jun 2011,PPP 1 Start
16:45:50, 08 Jun 2011,Modem connected on asy 5
16:45:50, 08 Jun 2011,Modem dialing on asy 5 #:*98*1#
16:45:50, 08 Jun 2011,IP Act_Rq to PPP 1-0: s_ip[192.168.0.99] d_ip[195.92.195.92]
16:44:58, 08 Jun 2011,Default Route 0 Out Of Service,Firewall <<<
16:44:58, 08 Jun 2011,ETH 0 Out Of Service,Firewall
```

The log entry indicates that the default route 0 (Ethernet interface) has been taken out of service, and the message is being generated due to the blocking of ICMP traffic.
The output from route print below shows that Eth 0 is now out of service (OOS) and PPP 1 is up. PPP 1 can be seen in the Event Log extract above as up (“PPP 1 up”).

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Metric</th>
<th>Protocol</th>
<th>Idx</th>
<th>Interface</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.138.69.107/32</td>
<td>10.138.69.107</td>
<td>1</td>
<td>Local</td>
<td>-</td>
<td>PPP 1</td>
<td>UP</td>
</tr>
<tr>
<td>192.168.0.0/24</td>
<td>192.168.0.254</td>
<td>1</td>
<td>Local</td>
<td>-</td>
<td>ETH 1</td>
<td>OOS</td>
</tr>
<tr>
<td>192.168.3.0/30</td>
<td>192.168.3.2</td>
<td>-</td>
<td>Local</td>
<td>-</td>
<td>ETH 0</td>
<td>OOS</td>
</tr>
<tr>
<td>0.0.0.0/0/0</td>
<td>3</td>
<td>Static</td>
<td>1</td>
<td>PPP 1</td>
<td>UP</td>
<td></td>
</tr>
<tr>
<td>0.0.0.0/0/0</td>
<td>-</td>
<td>Static</td>
<td>0</td>
<td>ETH 0</td>
<td>OOS</td>
<td></td>
</tr>
</tbody>
</table>

The ping is now sent out of the PPP 1 interface and again is returned to the requesting device on 192.168.0.99.
TransPort Ethernet to WWAN Backup

Delay: Normal
Throughput: Normal
Reliability: Normal

00 26
Length: 38
00 07
ID: 7
00 00
Frag Offset: 0
Congestion: Normal
May Fragment
Last Fragment

F8
TTL: 248
01
Proto: ICMP
EC 21
Checksum: 60449
0A 8A 45 6B
Src IP: 10.138.69.107
C3 5C C3 5C
Dst IP: 195.92.195.92

ICMP:
08
Type: ECHO REQ
00
Code: 0
57 AE
Checksum: 44631

----- 8-6-2011 16:45:54.070 -----
45 00 00 26 3D B5 00 00 37 01 6F 74 C3 5C C3 5C
E.......7.otÃ.Ä.
0A 8A 45 6B 00 00 5F AE 52 56 00 07 02 78 00 00
.ŠEk...®RV...x..
00 01 86 4B C5 2F
..†KÅ.

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 26
Length: 38
3D B5
ID: 15797
00 00
Frag Offset: 0
Congestion: Normal
May Fragment
Last Fragment

37
TTL: 55
01
Proto: ICMP
6F 74
Checksum: 28532
C3 5C C3 5C
Src IP: 195.92.195.92
0A 8A 45 6B
Dst IP: 10.138.69.107
ICMP:
00
Type: ECHO REPLY
00
Code: 0
5F AE
Checksum: 44639

--------
----- 8-6-2011 16:45:54.070 -----
45 00 00 26 3D B5 00 00 35 01 00 5E C3 5C C3 5C
E.......5...Ä.Ä.
C0 A8 00 63 00 00 5F AE 52 56 00 07 02 78 00 00
Ä"c...®RV...x..
00 01 86 4B C5 2F
..†KÅ.

IP (Final) From LOC TO REM
IFACE: ETH 1
45
IP Ver: 4
Hdr Len: 20
TransPort Ethernet to WWAN Backup

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOS:</td>
<td>Routine</td>
</tr>
<tr>
<td>Delay:</td>
<td>Normal</td>
</tr>
<tr>
<td>Throughput:</td>
<td>Normal</td>
</tr>
<tr>
<td>Reliability</td>
<td>Normal</td>
</tr>
<tr>
<td>Length:</td>
<td>38</td>
</tr>
<tr>
<td>ID:</td>
<td>15797</td>
</tr>
<tr>
<td>Frag Offset</td>
<td>0</td>
</tr>
<tr>
<td>Congestion:</td>
<td>Normal</td>
</tr>
<tr>
<td>TTL:</td>
<td>53</td>
</tr>
<tr>
<td>Proto:</td>
<td>ICMP</td>
</tr>
<tr>
<td>Checksum:</td>
<td>94</td>
</tr>
<tr>
<td>Src IP:</td>
<td>195.92.195.92</td>
</tr>
<tr>
<td>Dst IP:</td>
<td>192.168.0.99</td>
</tr>
<tr>
<td>Type:</td>
<td>ECHO REPLY</td>
</tr>
<tr>
<td>Code:</td>
<td>0</td>
</tr>
<tr>
<td>Checksum:</td>
<td>44639</td>
</tr>
</tbody>
</table>

The gateway router is then configured to allow ICMP. The WR44v2 detects the pings are successful and re-activates default route 0. The Event Log shows that the WR44v2 activated default route 0 (Eth 0) and disconnected PPP 1.

<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>16:57:05, 08 Jun 2011</td>
<td>Modem disconnected on asy 5, Normal Breakdown</td>
</tr>
<tr>
<td>16:57:03, 08 Jun 2011</td>
<td>PPP 1 down</td>
</tr>
<tr>
<td>16:57:03, 08 Jun 2011</td>
<td>Default Route 0 Available, Recovery</td>
</tr>
<tr>
<td>16:57:03, 08 Jun 2011</td>
<td>ETH 0 Available, Recovery</td>
</tr>
<tr>
<td>16:57:03, 08 Jun 2011</td>
<td>ETH 0 Recovery Completed, PING</td>
</tr>
</tbody>
</table>

5  **FIRMWARE VERSION**

Firmware version 5.2.15.4 was most recently used to re-test this project, and screenshots were updated at this time (revision 2.1 of this AN) to reflect the current GUI.
## 6 CONFIGURATION FILE

### 6.1 WR44v2 Configuration File

This is the config.da0 file used for the purpose of this AN:

```plaintext
eth 0 descr "Test WAN 44v2"
eth 0 IPaddr "192.168.3.2"
eth 0 mask "255.255.255.252"
eth 0 gateway "192.168.3.1"
eth 0 do_nat 1
eth 0 firewall ON
eth 0 pingip "8.8.8.8"
eth 0 pingint 10
eth 0 pingis ON
eth 0 linkdeact 1
eth 1 descr "Test LAN 44v2"
eth 1 IPaddr "192.168.0.254"

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
def_route 0 ll_ent "ETH"
def_route 0 deact_ent "PPP"
def_route 0 deact_add 1
def_route 1 ll_ent "PPP"
def_route 1 ll_add 1
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 (HSPA 3G)"
ppp 1 phonenum "*98*1#"
ppp 1 username "username"
ppp 1 epassword "KD5lSVJDVVg=
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 firewall ON
ppp 1 use_modem 1
ppp 1 pingip "8.8.8.8"
ppp 1 pingint 10
ppp 1 pingis 1
ppp 1 pingis ON
ppp 1 r_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
```
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 OFF
ana 0 l1on OFF
ana 0 lapdon 0
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 asyled_mode 2
cmd 0 tremto 1200
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
wifinode 0 enabled OFF
wifinode 0 ssid "digi.router.SN:%s"