Application Note 40

Configure Ethernet Bridging

(Between Local and Remote TransPort Networks)

Digi Technical Support

June 2016

Contents

Figures

1 INTRODUCTION

1.1 Outline

This Application Note (AN) aims to enable the reader to easily configure an Ethernet bridge between two TransPorts over a Wide Area Network (WAN) link.

The diagram below details the IP number scheme and architecture of this example configuration.

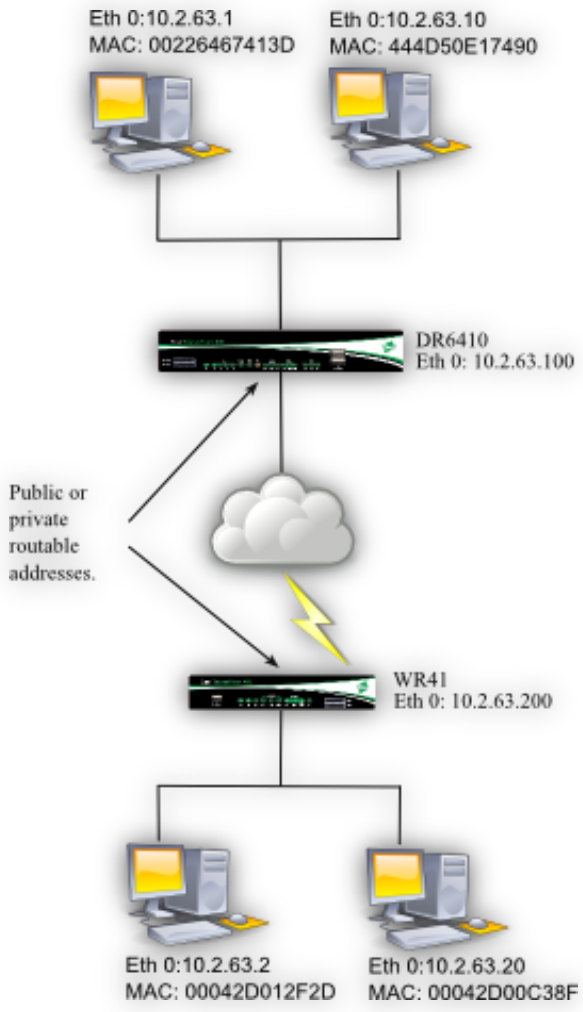


Figure 1-1: Network diagram

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.

Configuration: This AN assumes that the two TransPort devices are connected via routable public or private addresses. It is possible to allow bridging over W-WAN, ISDN and PSTN connections but note that the only restriction on the traffic sent across the link is done via MAC address filtering and that all Ethernet traffic will be bridged.

Users may wish to block the UDP ports configured for transmission of the bridged traffic from accessing any secondary connection via W-WAN, ISDN or PSTN, if only the main connection is to be used and to prevent bridging on secondary or tertiary network connections.

A WR41 with a cellular interface is being used as the "Remote" device in this AN, and this device is able to get a public address.

To use the Bridging functionality if the address assigned to the wireless interface is "NAT'ed" (not public) by the provider, adjust the configuration of the "Local" DR6410 at Site A to ensure that it is configured to initiate the bridge (refer to section 2.3 for further details), and that the "Remote" WR41 at site B is configured to listen for the incoming connection.

Please note that without encryption, the Ethernet traffic in this AN is passing over the network unencrypted and is potentially open to intercept. Therefore, there are security concerns that must be addressed in implementing this setup.

1.3 Caution

Please note that broadcast Ethernet traffic will be bridged over the WAN connection.

The only restriction on what traffic is bridged is done in the Ethernet > MAC Bridge options and no firewall restrictions are applied to this traffic.

On networks where there is a low capped limit or where charges are per megabyte (MB/GB) or per minute (as is the case on ISDN and PSTN) high network charges could be incurred after implementing the Bridging features described in this AN.

It is therefore highly recommend that interfaces which have flat rate charges such as unlimited dialup interfaces or ADSL or mobile broadband where there are no data or time limits for the transferred traffic are used.

A full security audit of the traffic is recommended as the transmitted traffic will be sent over the network unencrypted unless IPsec is used to encrypt the data.

1.4 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.

1.5 Version

Version Number:	Status
1.0	Published
1.1	Updated diagram and introduction
1.2	Updated to new web GUI
1.3	Updated screenshots and instructions for new web interface, rebranding (Jun 2016)

2 CONFIGURATION

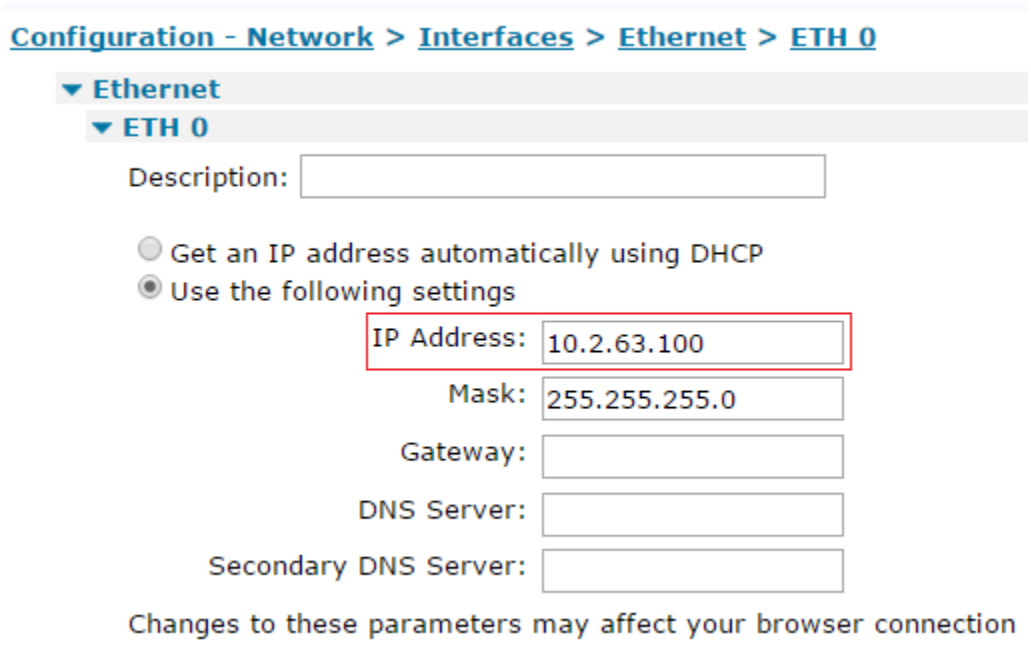
Only the parts of the configuration files that specifically relate to the configuration of this example will be explained in detail. The configuration files can be found in their entirety at the end of this document.

Please note that on all the sections below, click the '**Apply**' button at the bottom of the page to commit the changes.

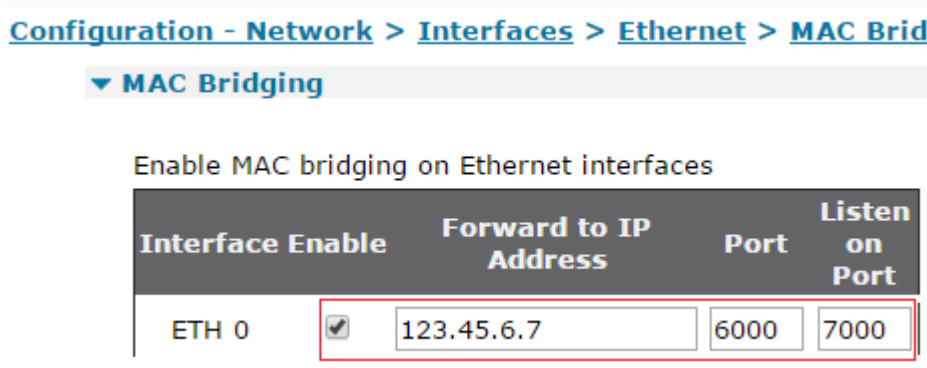
2.1 Configuration of "Local" Site A DR6410

2.1.1 Configure Local Ethernet Interface 0

First, configure the Ethernet interface with an IP Address:



Second, setup the bridging destination and the port to bridge on. If requiring two-way bridging then a listening port will also be needed:



Last, enable Ethernet and IP analysis for ETH 0:

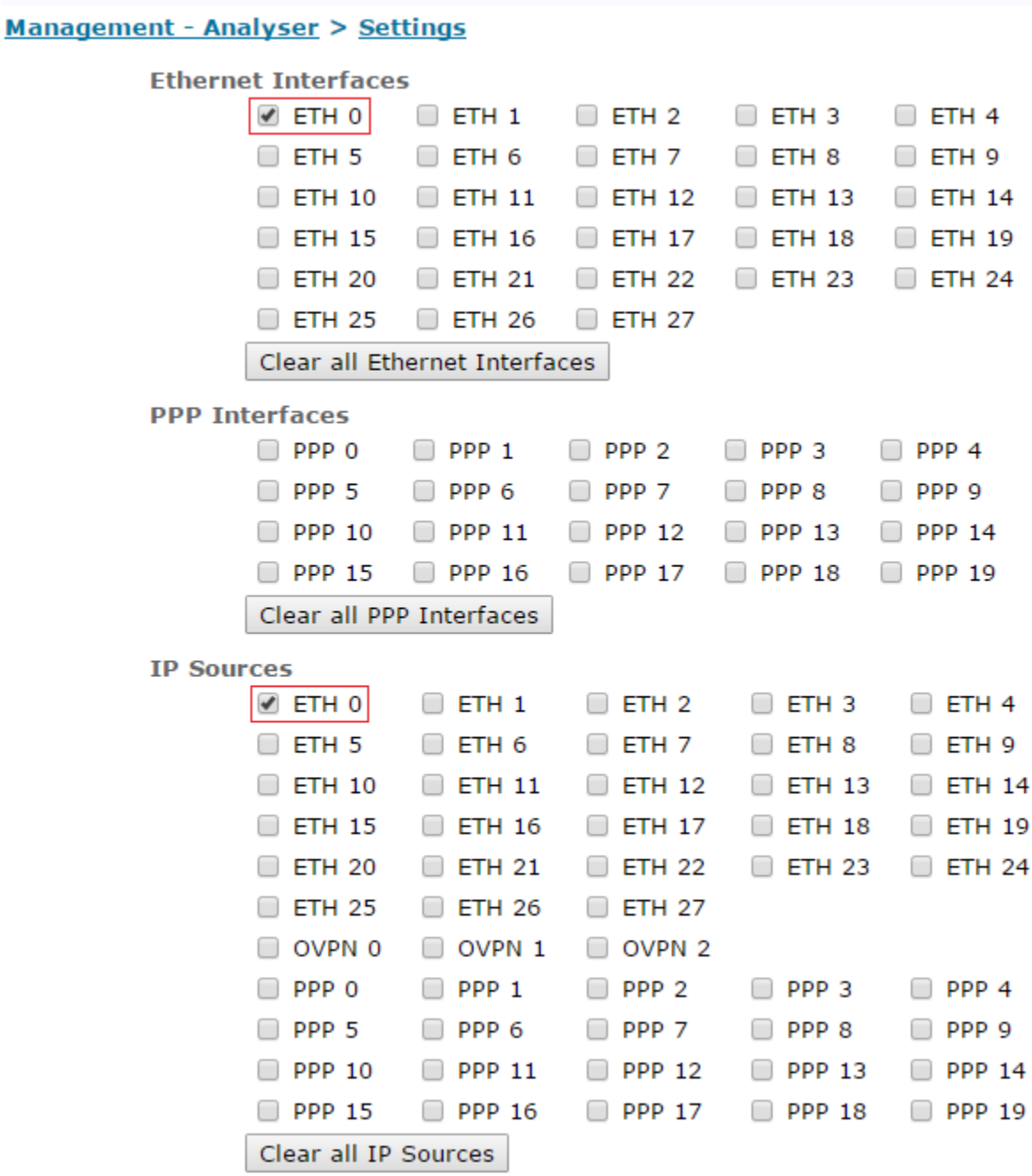
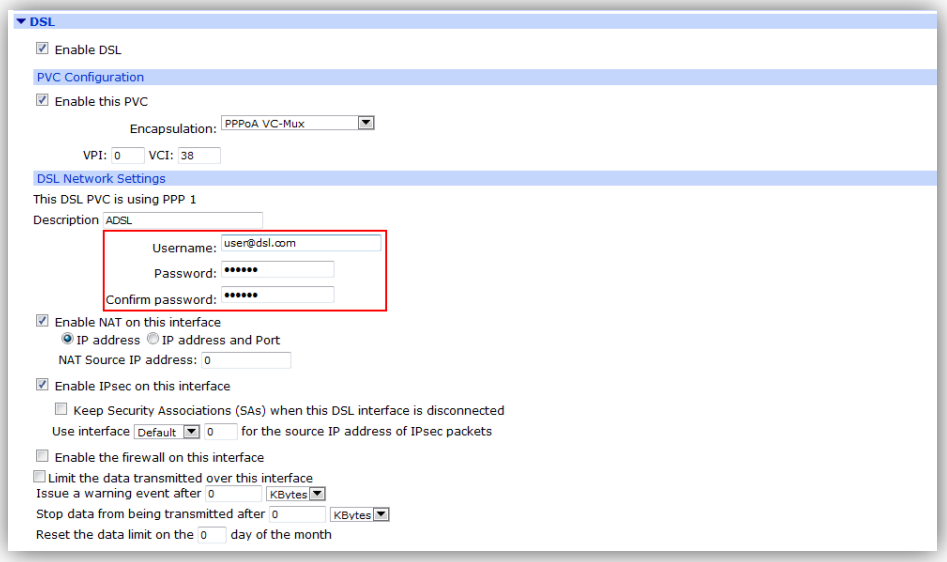


Figure 2-2: Site A Eth 0 Setup

Parameter	Setting	Description
IP address	10.2.63.100	Enter the IP address of the LAN interface
Forward to IP address	123.45.6.7	Enter the remote host WAN IP address

Port	6000	Port on Remote Host. Enter the port number to configure on the remote TransPort's 'MAC Bridge Listen Port (Host Mode)' setting
Listen on Port	7000	*Local Listening Port. This is required only if hosts on the remote site to locate hosts on the local network. This example demonstrates bi-directional bridging so both sites are also in listening mode*
Ethernet Interfaces	ETH 0	Turn on Ethernet analysis so that the bridged packets being sent to and from the remote networks can be seen, and verify that the bridge is working
IP Sources	ETH 0	Turn on analysis for this interface so as to permit troubleshooting if there are problems with the setup

2.1.2 Configure DSL Interface



Turn on IP analysis for monitoring and setup the username and password for the ADSL link:

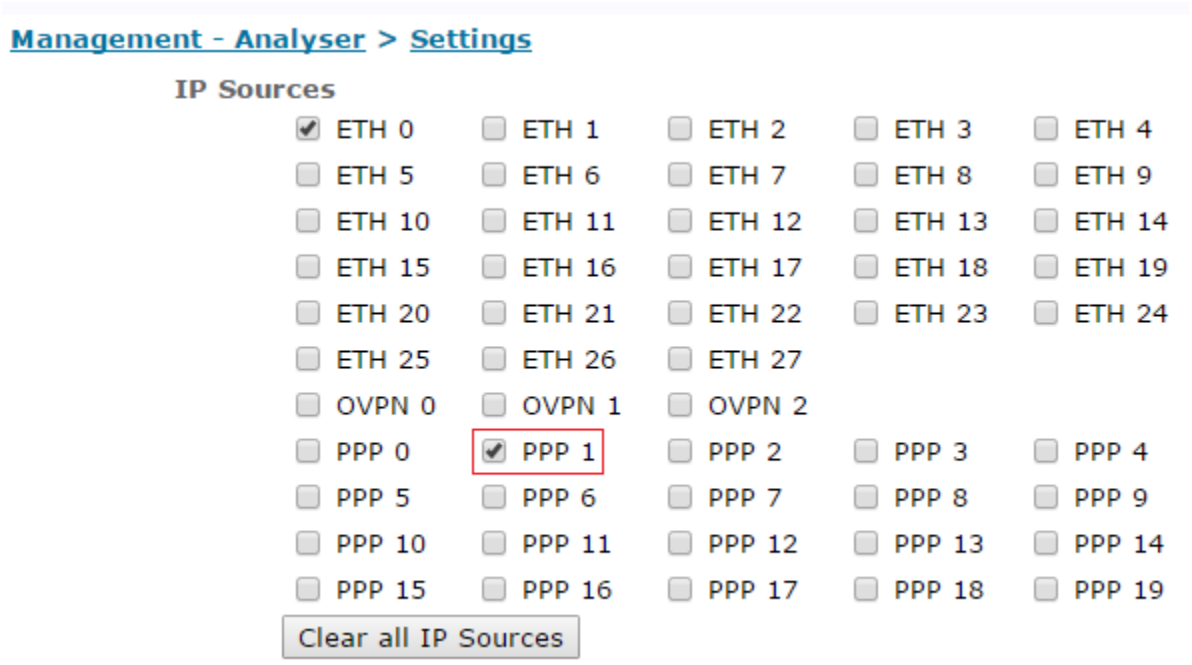


Figure 2-3: Site A DSL Setup

Parameter	Setting	Description
Username	Username	ADSL access username
Password	Password	ADSL access password
Confirm Password	Password	Confirm ADSL access password
IP Sources	PPP 1	Turn on analysis for this interface so as to permit troubleshooting if there are problems with the setup

2.1.3 Configure MAC Addresses to be Bridged

Up to 64 MAC address configurable values can be used to filter the traffic to be bridged. These addresses can be full addresses or partial addresses. Please note the minimum values are HEX pairs, so '00' or '0004' will work but '0' or "000" will not work. One HP laptop and one Micro Client Jr device are used at the Local Site A end of the connection to test:

```
444D50       Micro Client Jr
002264       HP laptop
```

To check what the MAC (physical) address is, CLI into the TransPort via telnet or SSH, or log into the web interface, navigate to **Administration - Execute a command**, and then issue the following command to ping the HP laptop's IP address (which must be known first):

```
ping 10.2.63.1 –e0
```

Once this is completed, issue the following command:

```
arp –a
```

An ARP table similar to the one below should be seen containing the machine's MAC address. The ARP table holds a list of 'Physical Address ' and 'IP Address' values held in the ARP cache:

```
arp -a
Command result

ARP Cache Size:300 entries, old entries reused:0 no arp matches:1194070
nb of entries:0
ETH 1:
  IP Address       Physical Address    Expiry    Retries    State
  10.2.63.10       44-4d-50-e1-74-90   187        3      found
  10.2.63.1        00-22-64-67-41-3d      219        3      found
nb of entries:2
nb of entries:0
nb of entries:0
nb of entries:0
nb of entries:0
nb of entries:0
nb of entries:0
nb of entries:0
nb of entries:0
nb of entries:0
OK
```

Part of a MAC address or the full address can be used to filter for bridging, so '00' can be used and this will bridge most Ethernet cards, or 00226467413D can be used to only bridge a certain device.

Please see the caution section here before setting up bridging and deciding on what addresses to bridge.

Bridge for a specific address 00226467413D (the HP laptop) and omit the other device on the network so that only traffic from the HP laptop is bridged:

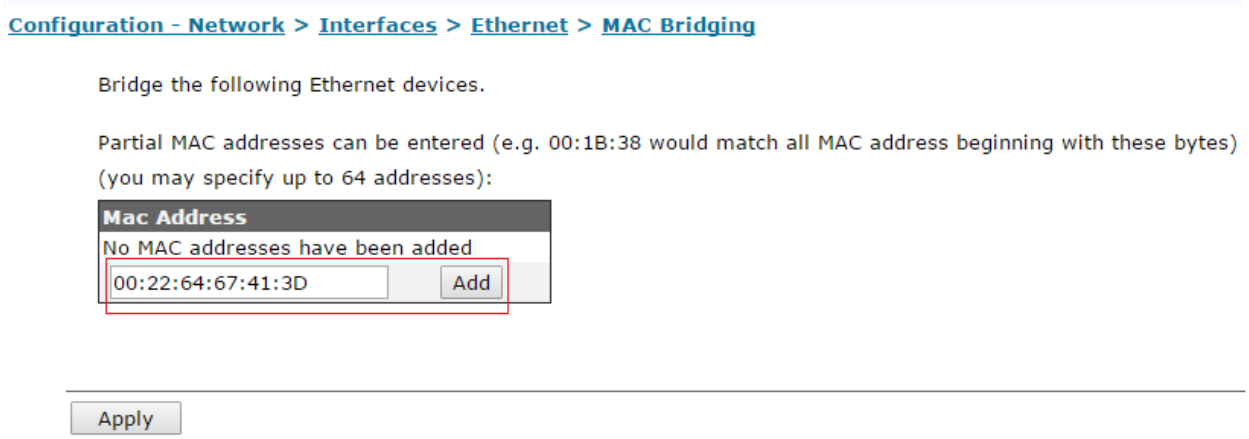


Figure 2-4: Site A MAC Filter

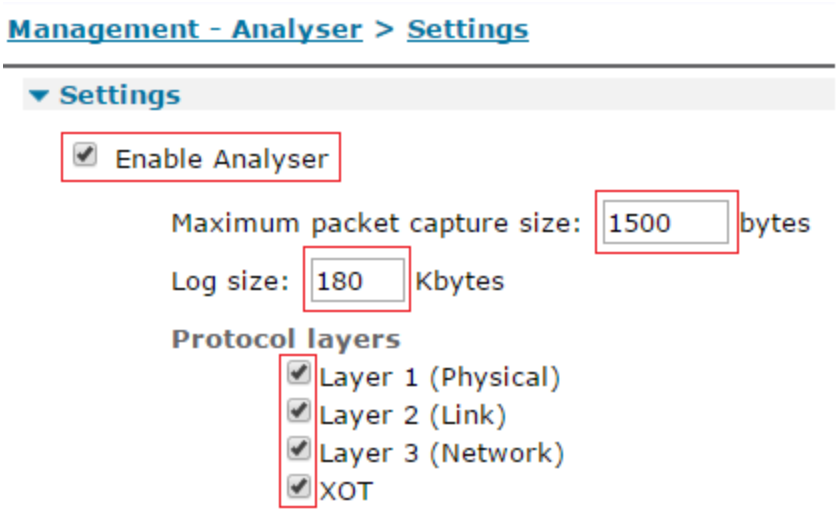
Parameter	Setting	Description
Mac Address	00:22:64:67:41:3D	MAC address to be bridged

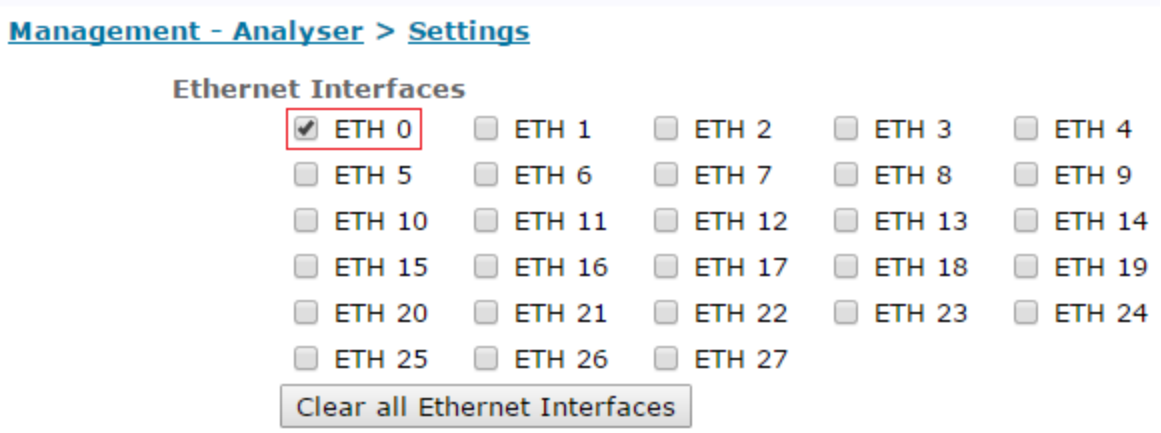
NOTE: From firmware version 5.151 and later an * can be used to denote that traffic from all source MAC addresses should be bridged.

2.1.4 Configure Logging

Double check that the Analyser is setup correctly. Remove any settings that do not match here. On the IP traces, only packets that are going to or from the ports 6000 or 7000 need to be seen.

Using a '~' (tilde) sign on any filter within the Analyser settings will cause the unit to only record traffic that matches the filter, and exclude all other traffic. Please be wary of combining tilde filters on port, protocol, and IP, as this can often result in NO results. For example, filtering for only port 80 and protocol 1 will usually result in no matches as there is no web traffic over ICMP.


Management - Analyser > Settings
Settings
Enable Analyser
Maximum packet capture size: 1500 bytes
Log size: 180 Kbytes
Protocol layers
Layer 1 (Physical)
Layer 2 (Link)
Layer 3 (Network)
XOT


Management - Analyser > Settings
Ethernet Interfaces
ETH 0
ETH 1
ETH 2
ETH 3
ETH 4
ETH 5
ETH 6
ETH 7
ETH 8
ETH 9
ETH 10
ETH 11
ETH 12
ETH 13
ETH 14
ETH 15
ETH 16
ETH 17
ETH 18
ETH 19
ETH 20
ETH 21
ETH 22
ETH 23
ETH 24
ETH 25
ETH 26
ETH 27
Clear all Ethernet Interfaces

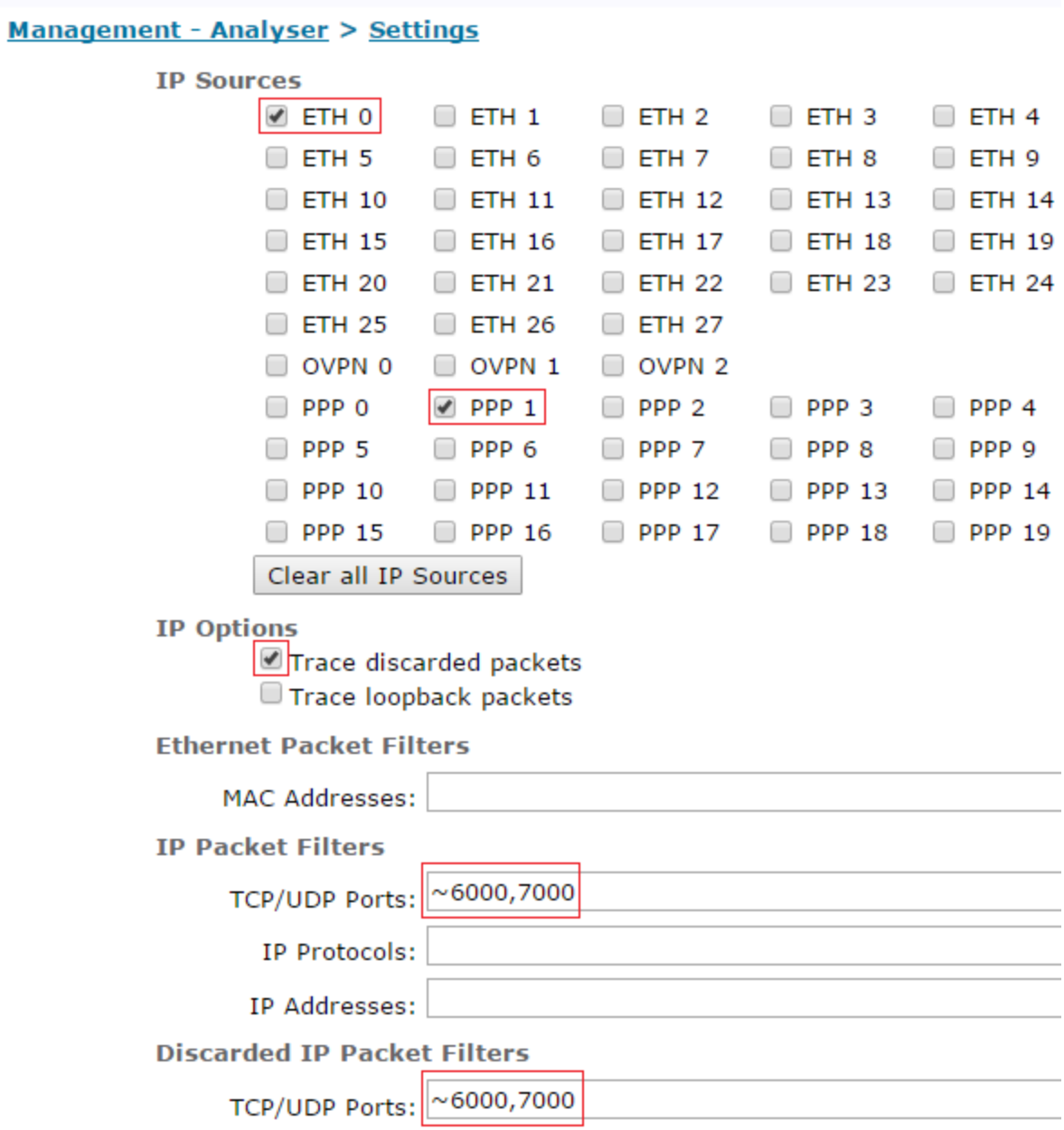


Figure 2-5: Site A Analyser Setup

Parameter	Setting	Description
Enable Analyser	Checked	Enable logging to the analyser trace
Maximum packet capture size	1500	Collect most full sized packets
Log Size	180	Set the Analyser to the maximum size
Ethernet Interfaces	ETH 0	Enable Ethernet logging for this interface
IP Sources	ETH 0	Enable IP logging for this interface
IP Sources	PPP 1	Enable IP logging for this interface
IP Options	Trace Discarded Packets	
IP Packet filters	~6000,7000	Traffic between the sites on the bridging ports only selected
Discarded IP Packet Filters	~6000,7000	Traffic between the sites on the bridging ports only selected

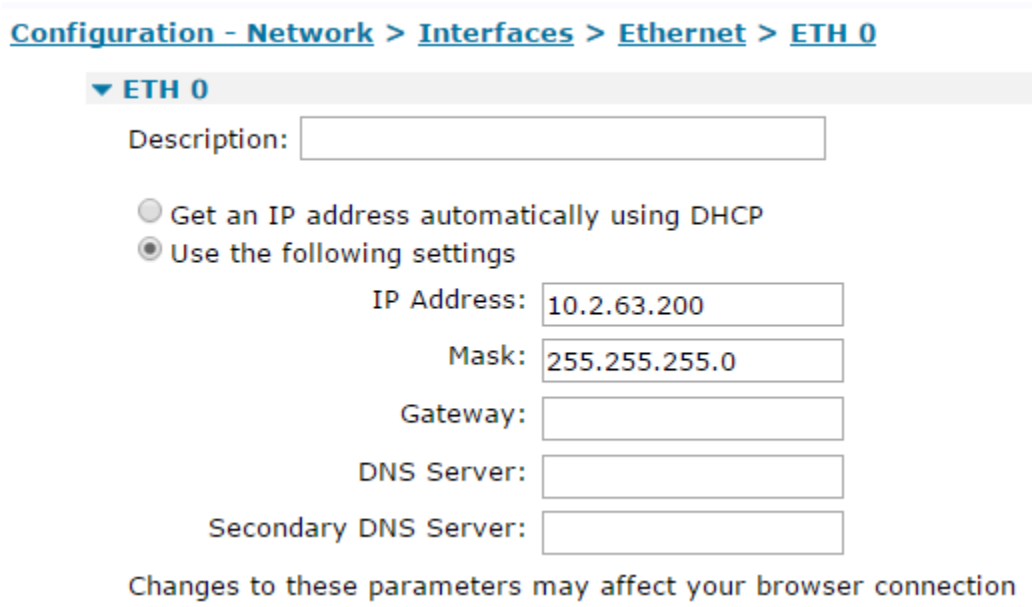
Save the config of "Local" Site A TransPort and move on to the next section.

2.2 Configuration of "Remote" Site B WR41

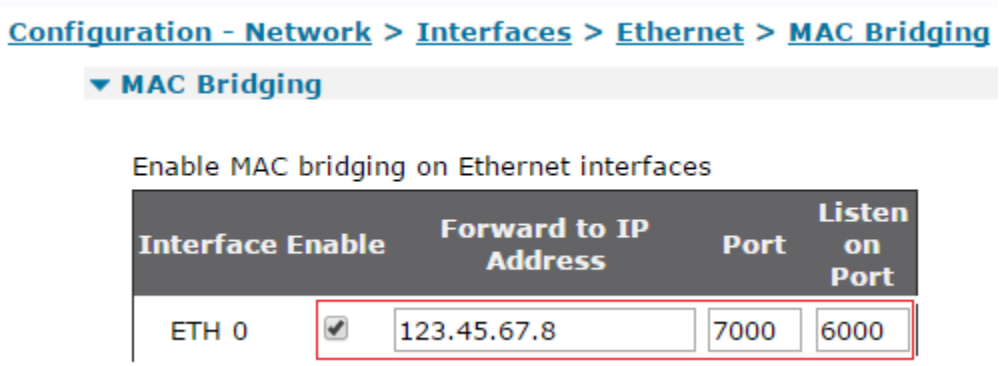
Please note that a cellular WAN interface is used here; please be aware of the caution regarding bandwidth charges above (in this case, excess bandwidth charges) that could be incurred as a result of bridging Ethernet networks.

2.2.1 Configure Local Ethernet Interface 0

First, configure the Ethernet interface with an IP address:



Second, setup the bridging destination and the port to bridge on. If requiring two-way bridging then a listening port will also be needed:



Last, enable Ethernet and IP analysis for ETH 0:

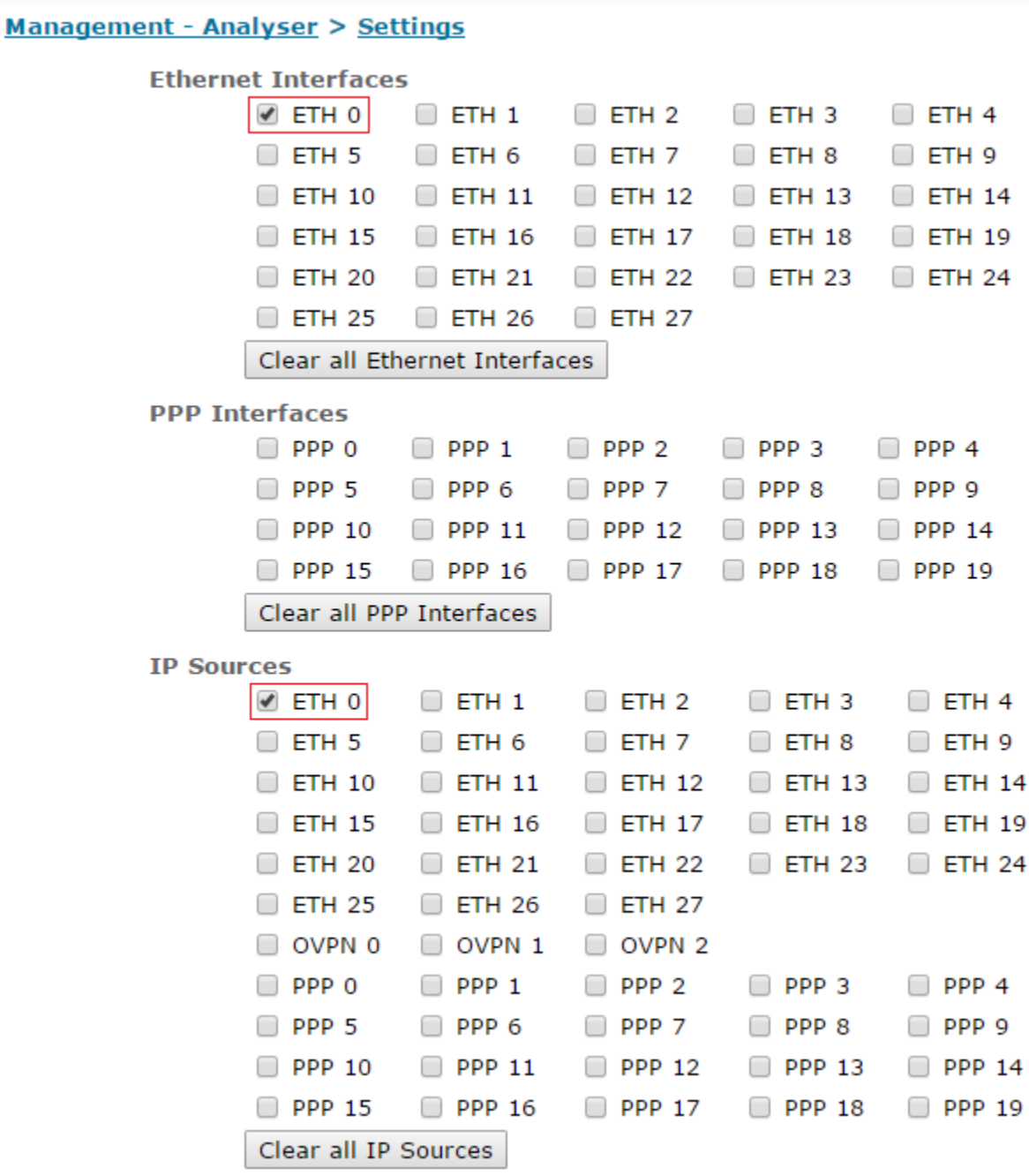


Figure 2-6: Site B Eth 0 Setup

Parameter	Setting	Description
IP address	10.2.63.200	Enter the IP address of the LAN interface
Forward to IP address	123.45.67.8	Enter the remote host WAN IP address

Port	7000	Port on Remote Host. Enter the port number that will be configured on the remote TransPort's 'MAC Bridge Listen Port (Host Mode)' setting
Listen on Port	6000	Local Listening Port. This is required only if hosts on the remote site need to locate hosts on the local network. In this example, bi-directional bridging is utilized so both sites are also in listening mode
Ethernet Interfaces	ETH 0	Turn on Ethernet analysis so that bridged packets being sent to and from the remote networks can be seen, and verify that the bridge is working
IP Sources	ETH 0	Turn on analysis for this interface to enable troubleshooting if there are problems with the setup

2.2.2 Configure Analysis

In this example, a cellular WAN link is used, which provides a static IP address for the WR to connect to. **Please be aware of the caution note above regarding potential network charges**. We only need to set up monitoring here. Please note that if the wireless WAN connection requires a username and password, or if a SIM PIN is required, then this is done within the Mobile Configuration on the next item. The SIM we are using requires no username, password or PIN, so there is very little to configure in this page except the setting up of the monitoring:

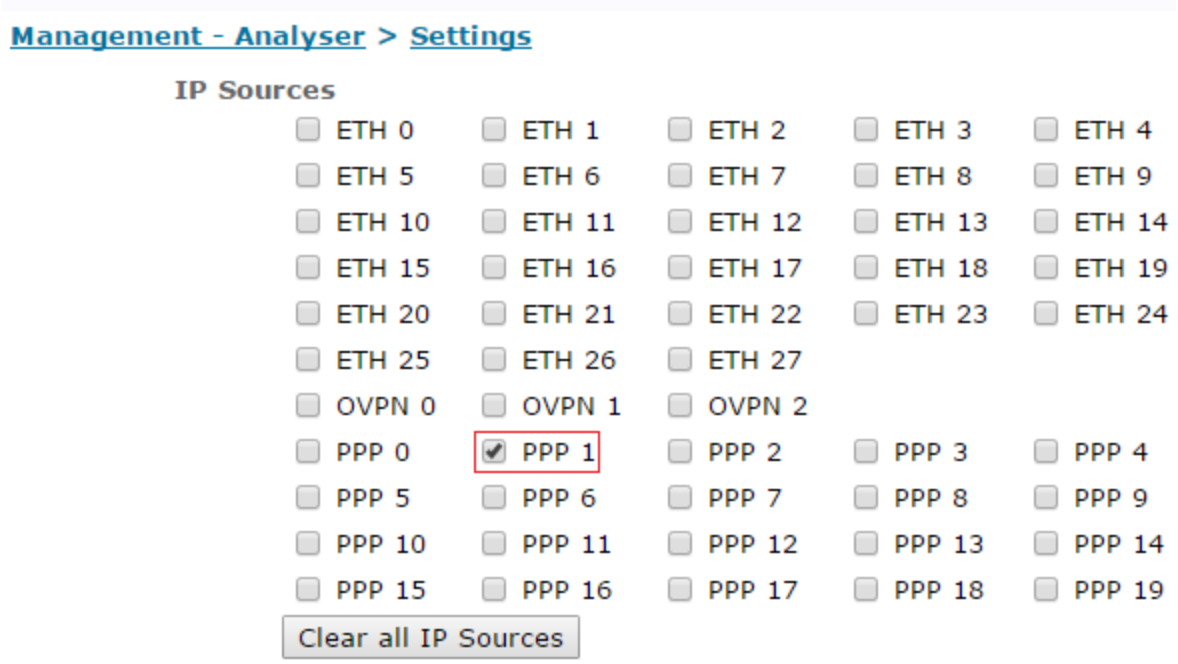


Figure 2-7: Site B PPP 1 Setup

Parameter	Setting	Description
IP Sources	PPP 1	Turn on analysis for this interface to enable troubleshooting if there are issues

2.2.3 Configure Mobile Interface

Here, the APN for the cellular WAN connection is entered. Please note that some wireless connections may require more settings such as a PIN, username, and password, to be setup on the PPP interface:

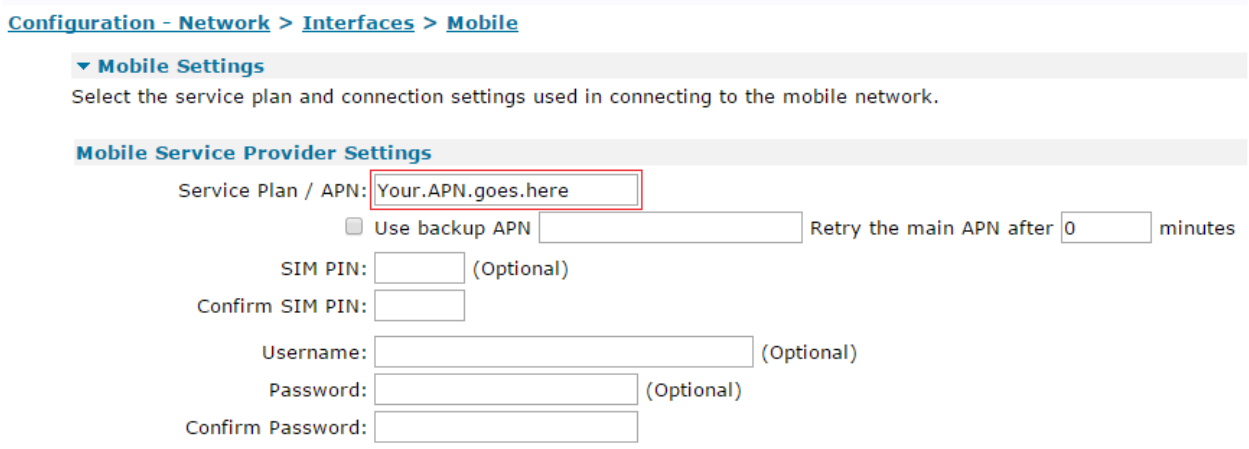


Figure 2-8: Site B APN Setup

Parameter	Setting	Description
APN	Your.APN.goes.here	Replace this with the proper APN (if required)

2.2.4 Configure MAC Addresses to be Bridged

Please see section above for more detail about how to determine what the MAC address is. The IP address of the device that is to be bridged in this example is 10.2.63.2; first test that this is responding OK:

```
ping 10.2.63.2 -e0
```

arp –a will again give us the IP addresses of devices on this network segment that the device has seen recently.

```
Command: arp -a
Command result

ARP Cache Size:100 entries, old entries reused:0 no arp matches:14
ETH 0:
  IP Address       Physical Address    Expiry    Retries    State
  10.2.63.2        00-04-2d-01-2f-2d      146        3      found
  10.2.63.20       00-04-2d-00-c3-8f      267        3      found
nb of entries:2
nb of entries:0
nb of entries:0
OK
```

Both of these devices are TransPorts (OID '00042D'). They could equally be PCs or any other Ethernet connected devices. As can be seen above, the MAC address needing to be bridged is **00042D012F2D**. Enter this into the bridge filter form:

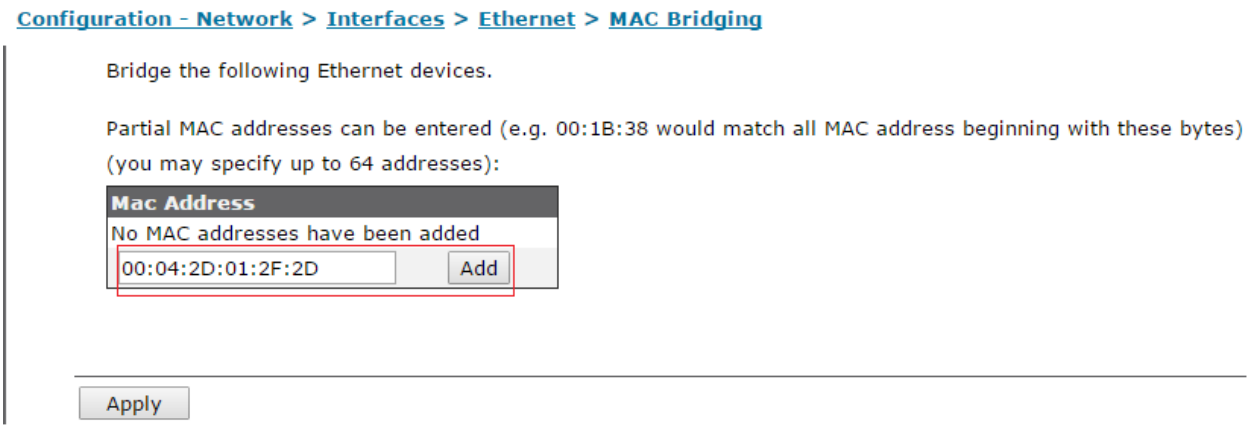


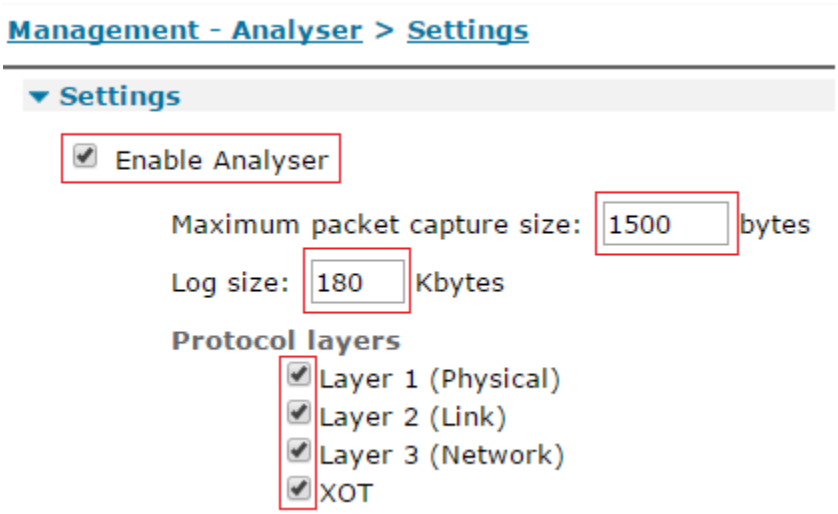
Figure 2-9: Site B Mac Filter Setup

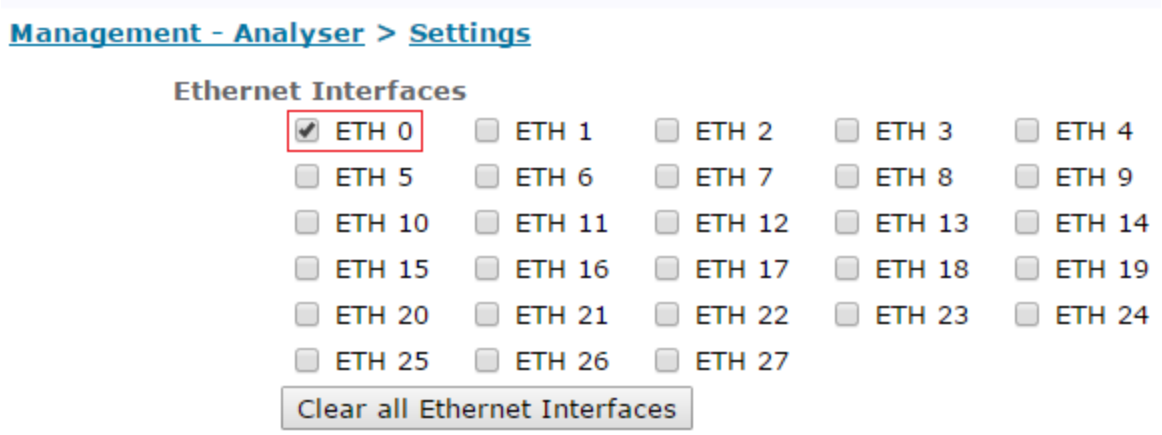
Parameter	Setting	Description
Mac Address	00:04:2D:01:2F:2D	MAC address to be bridged

2.2.5 Configure Logging

This is just to double check that the analyser is setup correctly. Remove any settings that do not match here. IP traces are only required for packets that are going to or from the ports 6000 or 7000.

Using a '~' tilde sign on any filter within the analyser settings will cause the unit to only record traffic that matches the filter and exclude all other traffic – please be wary of combing tilde filters on port, protocol and IP as this can often result in no results as for example filter for only port 80 and protocol 1 will usually result in no matches as there is no web traffic over ICMP.




Management - Analyser > Settings
Ethernet Interfaces
ETH 0
ETH 1
ETH 2
ETH 3
ETH 4
ETH 5
ETH 6
ETH 7
ETH 8
ETH 9
ETH 10
ETH 11
ETH 12
ETH 13
ETH 14
ETH 15
ETH 16
ETH 17
ETH 18
ETH 19
ETH 20
ETH 21
ETH 22
ETH 23
ETH 24
ETH 25
ETH 26
ETH 27
Clear all Ethernet Interfaces

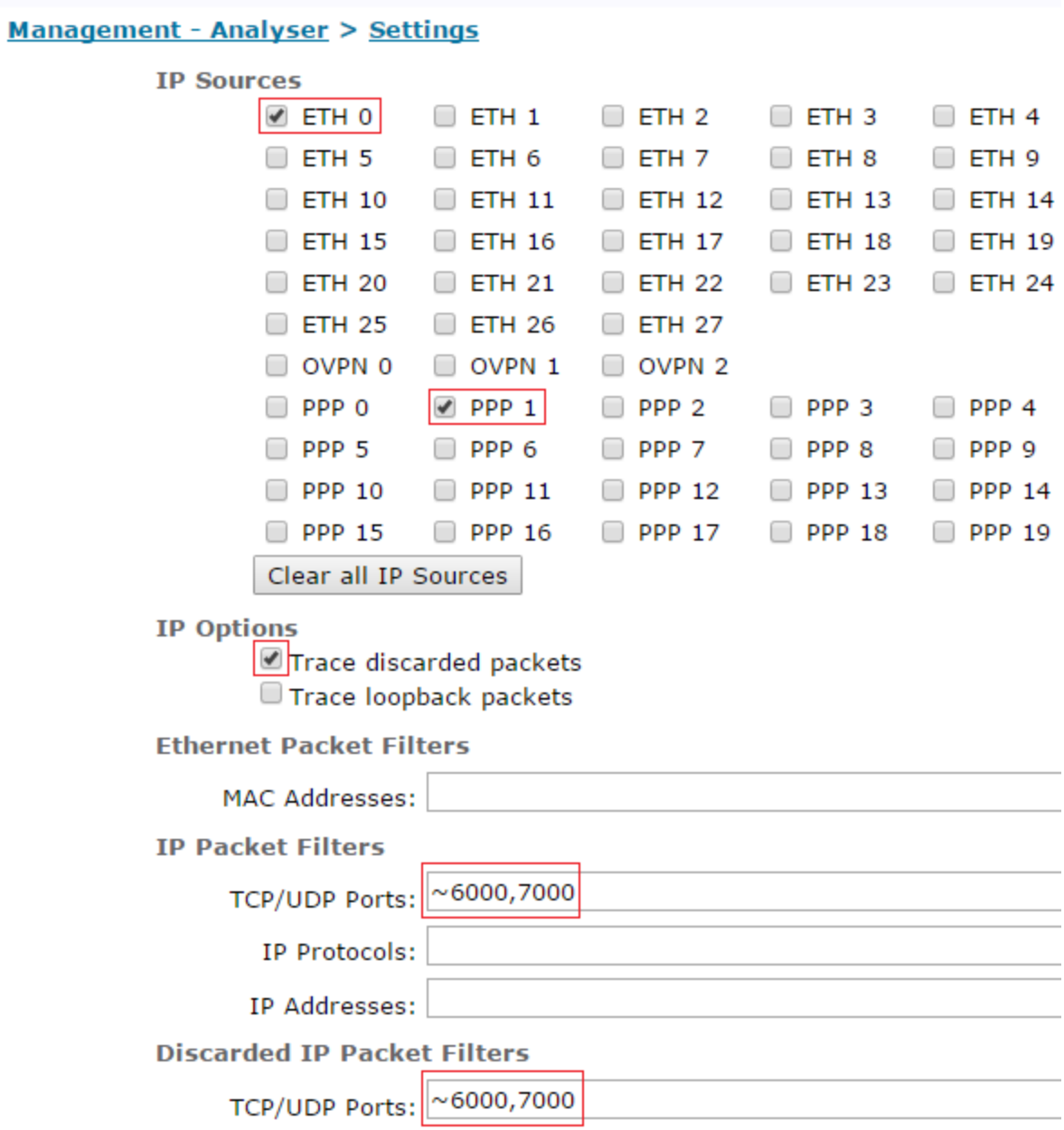


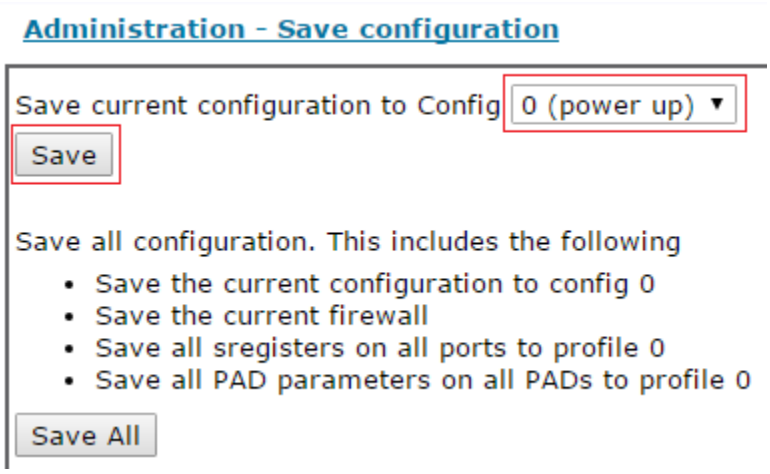
Figure 2-10: Site B Analyser Setup

Parameter	Setting	Description
Enable Analyser	Checked	Enable logging to the Analyser trace
Maximum packet capture size	1500	Collect most full sized packets
Log Size	180	Set the Analyser to the maximum size
Ethernet Interfaces	ETH 0	Enable Ethernet logging for this interface
IP Sources	ETH 0	Enable IP logging for this interface
IP Sources	PPP 1	Enable IP logging for this interface
IP Options	Trace Discarded Packets	
IP Packet filters	~6000,7000	Traffic between the sites over the bridge only
Discarded IP Packet Filters	~6000,7000	Discarded traffic between the sites over the bridge only.

2.2.6 Save the config

Once configured, save the configuration.

If the config is not saved, the above configuration steps will have to be repeated following a reboot of the TransPort!

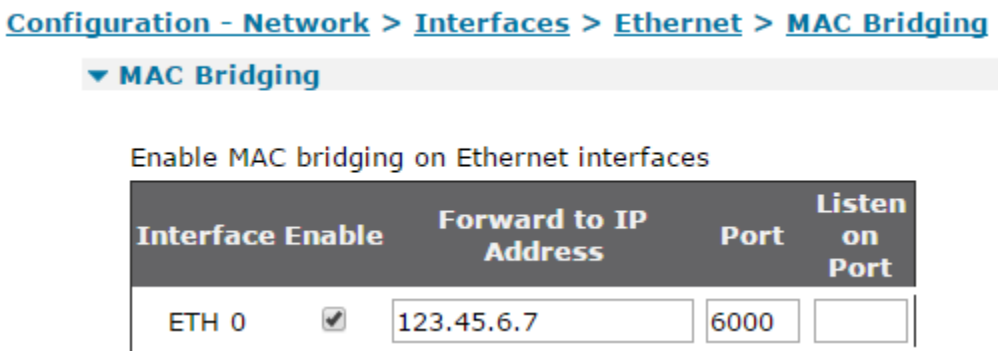


2.3 Alternate configuration for NAT

If the "Local" TransPort has a private IP address instead of a public IP address, only the Remote TransPort needs to be configured to listen. The Local TransPort needs to be configured to initiate the bridge via the public IP address of the Remote TransPort, connecting to the port that the Remote TransPort is configured to listen on.

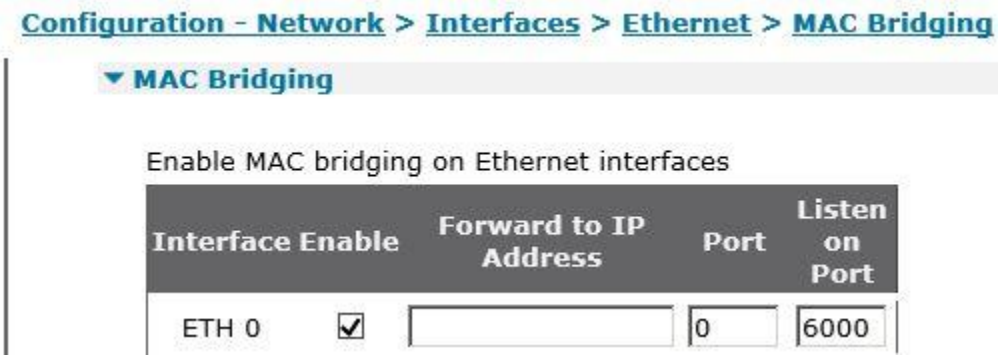
Be sure to also follow the "Configure MAC Addresses to be Bridged" instructions earlier in this section.

Local TransPort:



123.45.6.7 is the public IP address of the other Remote TransPort.

Remote TransPort:



3 TESTING

To test this setup, send a ping from 10.2.63.2 to 10.2.63.10:

```
ping 10.2.63.10
Pinging Addr [10.2.63.10]

sent PING # 1
PING receipt # 1 : response time 0.43 seconds
Iface: ETH 0
Ping Statistics
Sent         : 1
Received     : 1
Success      : 100 %
Average RTT  :  0.43 seconds

OK
```

This test was successful (100%).

A ping from 10.2.63.1 to either node attached to the WR41 was also successful, but a ping from 10.2.63.10 to either of the devices attached to the WR failed. A ping from 10.2.63.20 to either of the devices attached to the DR also failed.

Below is the successful trace showing the ping between 10.2.63.2 and 10.2.63.10. Please note that the trace below has been tidied up. Subsequent ARP requests sent and some NETBIOS traffic have been omitted.

STAGE	10.2.63.2	WR41	DR6410	10.2.63.10
1	ARP request >			
2		Packet encap 7000 >		
3			Packet Rcvd port 7000 >	
4				ARP Request >
5				< ARP Reply
6			< Packet encap from port 7000	
7		< Packet recd from port 7000		
8	< ARP Reply			
9	ICMP ECHO Request >			
10		Packet encap 7000 >		
11			Packet Rcvd port 7000 >	
12				ICMP ECHO Request >
13				< ICMP ECHO Reply
14			< Packet encap from port 7000	
15		< Packet recd from port 7000		
16	< ICMP ECHO Reply			

Traces:

The trace below is sectioned off and some traffic is excluded to make the conversation above easier to see.

Stage	WR41	DR6410
1	----- 1-7-2009 16:01:11.830 ------- FF FF FF FF FF FF 00 04 2D 01 2F 2D 08 06 00 01 .... 08 00 06 04 00 01 00 04 2D 01 2F 2D 0A 02 3F 02 .... 00 00 00 00 00 00 0A 02 3F 0A 00 00 00 00 00 00 .... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .... 46 A9 04 45 F©.E ETH From REM TO LOC IFACE: ETH 0 FF FF FF FF FF FF Dst. MAC 00 04 2D 01 2F 2D Src. MAC 08 06 Type: ARP ARP:	

	00 01 HW Type: Ethernet (1) 08 00 Prot Type: IP (2048) 06 HW Size: 6 04 Prot Size: 4 00 01 Opcode: Request (1) 00 04 2D 01 2F 2D Src. MAC 0A 02 3F 02 Src IP: 10.2.63.2 00 00 00 00 00 00 Dst. MAC 0A 02 3F 0A Dst IP: 10.2.63.10 ----------	

At this point, the MAC address of the target machine is not known, so the device on the WR41 network sends an ARP request for the MAC address of the device that has 10.2.63.10. Please note the source IP address. The TransPort sees this MAC address and checks the bridging table to see if this traffic should be bridged.

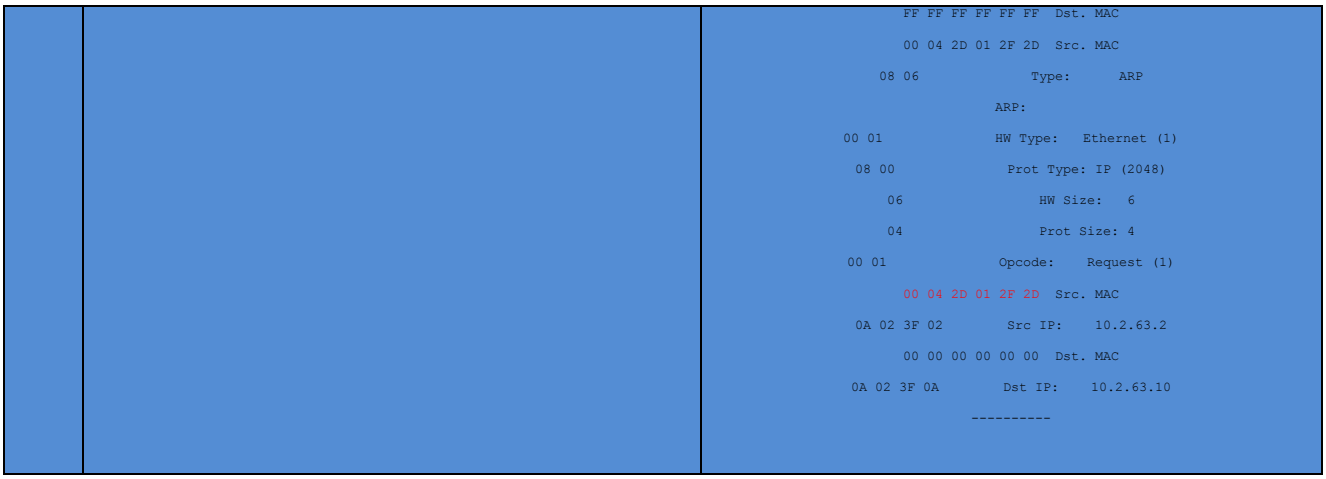
2 & 3	----- 1-7-2009 16:01:11.830 ------- 45 00 00 60 00 15 00 00 F9 11 29 8A 7B 2D 06 07 E.....ù.)Š{-.. 7B 2D 43 08 04 D6 1B 58 00 4C 9B CA FF FF FF FF {-C..Ö.X.L.Ê.... 0F FF 00 04 2D 01 2F 2D 08 06 00 01 08 00 06 04 ....-./-........ 00 01 00 04 2D 01 2F 2D 0A 02 3F 02 00 00 00 00 ....-./-..?..... 00 00 0A 02 3F 0A 00 00 00 00 00 00 00 00 00 00 ....?..... 00 00 00 00 00 00 00 00 00 00 00 00 46 A9 04 45 ....F©.E 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 60 Length: 96 00 15 ID: 21 00 00 Frag Offset: 0 Congestion: Normal May Fragment Last Fragment F9 TTL: 249 11 Proto: UDP 29 8A Checksum: 10634 7B 2D 06 07 Src IP: 94.197.41.59 7B 2D 43 08 Dst IP: 213.152.58.85 UDP: 04 D6 SRC Port: ??? (1238) 1B 58 DST Port: ??? (7000) 00 4C Length: 76 9B CA Checksum: 39882 ----------	----- 1-7-2009 16:01:39.950 ------- 45 00 00 60 00 15 00 00 F3 11 2F 8A 7B 2D 06 07 E.....ó.../Š{-.. 7B 2D 43 08 04 D6 1B 58 00 4C 9B CA FF FF FF FF {-C..Ö.X.L.Ê.... 0F FF 00 04 2D 01 2F 2D 08 06 00 01 08 00 06 04 ....-./-........ 00 01 00 04 2D 01 2F 2D 0A 02 3F 02 00 00 00 00 ....-./-..?..... 00 00 0A 02 3F 0A 00 00 00 00 00 00 00 00 00 00 ....?..... 00 00 00 00 00 00 00 00 00 00 00 00 46 A9 04 45 ....F..E 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 60 Length: 96 00 15 ID: 21 00 00 Frag Offset: 0 Congestion: Normal May Fragment Last Fragment F3 TTL: 243 11 Proto: UDP 2F 8A Checksum: 12170 7B 2D 06 07 Src IP: 94.197.41.59 7B 2D 43 08 Dst IP: 213.152.58.85 UDP: 04 D6 SRC Port: ??? (1238) 1B 58 DST Port: ??? (7000) 00 4C Length: 76 9B CA Checksum: 39882 ----------

The WR then adds a bridging header to the packet and sends this to the DR. The packet sent from the WR matches the packet received at the DR. Also apart from the header information:

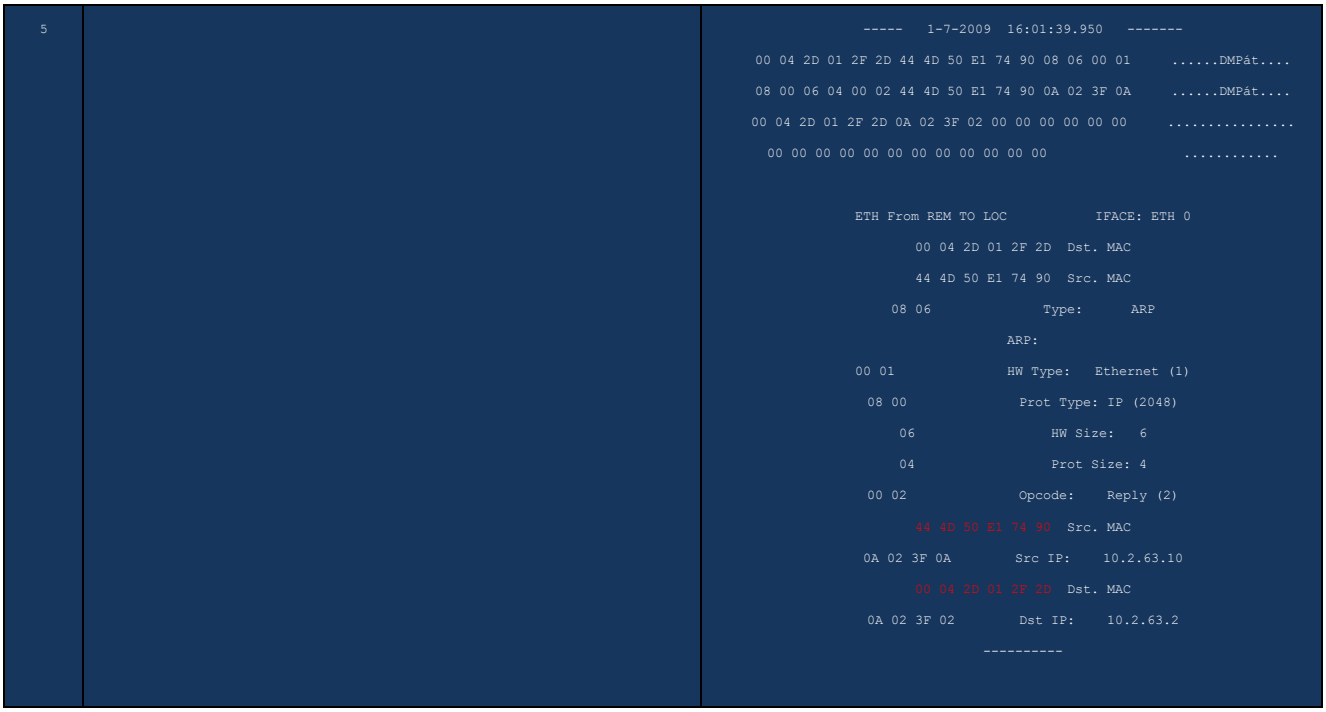
45 00 00 60 00 15 0o 00 F9 11 29 8A 7B 2D 06 07 7B 2D 43 08 04 D6 1B 58 00 4C 9B CA

The packet is identical to the one received on the Ethernet port of the WR in stage 1.

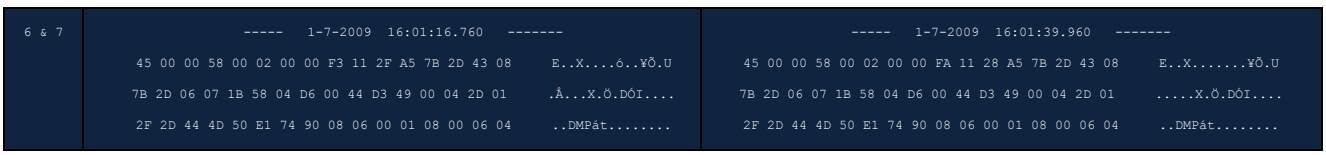
4		----- 1-7-2009 16:01:39.950 ------- FF FF FF FF FF FF 00 04 2D 01 2F 2D 08 06 00 01 ....-./-.... 08 00 06 04 00 01 00 04 2D 01 2F 2D 0A 02 3F 02 ....-./-..?. 00 00 00 00 00 00 0A 02 3F 0A 00 00 00 00 00 00 ....?..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .... 46 A9 04 45 00 00 F..E.. ETH From LOC TO REM IFACE: ETH 0

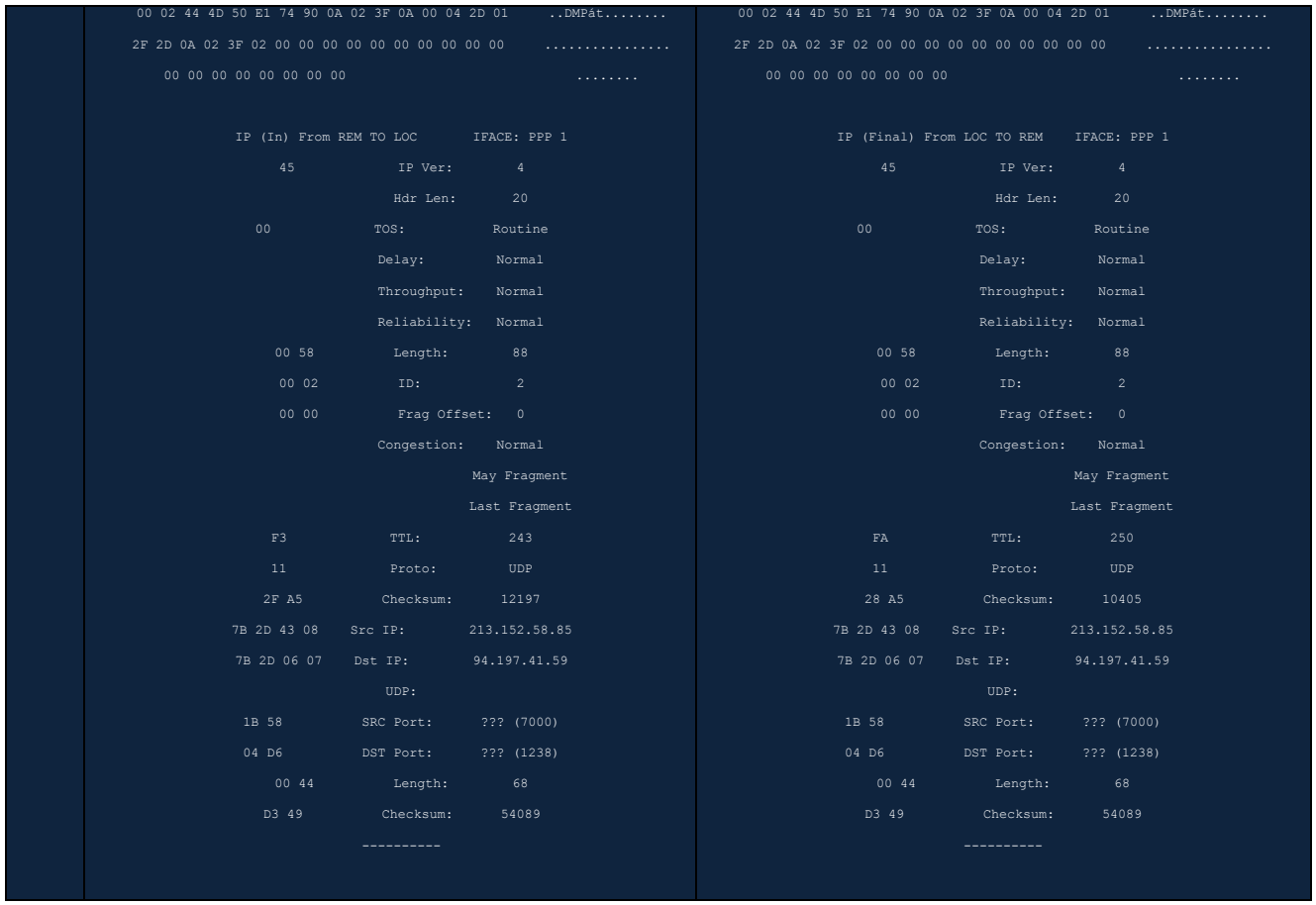


ARP request sent on the WR41 network is now sent out of Eth 0 on the DR network.

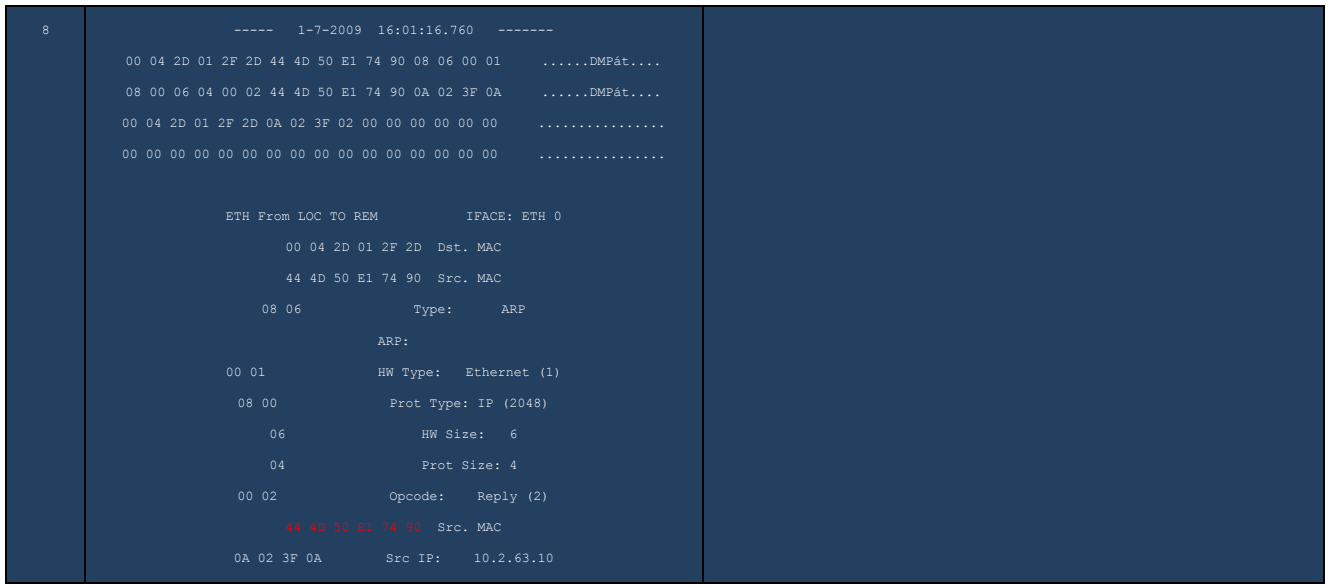


ARP reply to ARP request is received on the Ethernet port of the DR; now a MAC address for the destination device is seen. Please note that although this device can be pinged from the WR network, this MAC address is not in the MAC bridge table on the DR, so it is not possible to initiate a ping in the opposite direction from the 10.2.63.10 device.





The ARP reply is encapsulated and sent back to the WR41 router again. Notice that the packet without the bridging header is the same packet seen on the DR local network and is not encrypted.



```
                    00 04 2D 01 2F 2D  Dst. MAC
              0A 02 3F 02        Dst IP:    10.2.63.2
                           ----------
```

ARP reply is seen back on the WR41 local network. Now that a destination MAC address is found, a ping to the remote device can be sent.

```
9
                -----   1-7-2009  16:01:16.760   -------
     44 4D 50 E1 74 90 00 04 2D 01 2F 2D 08 00 45 00     DMPát........E.
     00 22 00 0F 00 00 F9 01 2F BC 0A 02 3F 02 0A 02     ........¼.....
     3F 0A 08 00 E7 26 A5 0E 00 0F 01 77 00 00 6A 44     ....ç.¥....w..jD
     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00     ................
           FE EE 30 1A                                          .î0.


          ETH From REM TO LOC           IFACE: ETH 0
                 44 4D 50 E1 74 90  Dst. MAC
                 00 04 2D 01 2F 2D  Src. MAC
               08 00              Type:      IP
                              IP:
               45              IP Ver:        4
                              Hdr Len:       20
             00             TOS:           Routine
                            Delay:         Normal
                            Throughput:    Normal
                            Reliability:   Normal
               00 22          Length:        34
               00 0F          ID:            15
                00 00          Frag Offset:   0
                              Congestion:    Normal
                                         May Fragment
                                        Last Fragment
              F9             TTL:           249
             01             Proto:         ICMP
            2F BC          Checksum:      12220
          0A 02 3F 02    Src IP:        10.2.63.2
          0A 02 3F 0A    Dst IP:        10.2.63.10
                        ----------
```

ICMP ping request Ethernet packet is seen on the WR41 network coming from the node set up for bridging and is sent to the remote network. Please note that any Ethernet packet from this node except a packet for the WR41 itself will be bridged.

```
10 & 11
                -----   1-7-2009  16:01:16.760   -------
     45 00 00 60 00 18 00 00 FA 11 28 87 7B 2D 06 07     E.........Å..
     7B 2D 43 08 04 D6 1B 58 00 4C AA 3F 44 4D 50 E1     ?.U.Ö.X.L.DMPá
     74 90 00 04 2D 01 2F 2D 08 00 45 00 00 22 00 0F     t........E.....
     00 00 F9 01 2F BC 0A 02 3F 02 0A 02 3F 0A 08 00     .....¼.........

                -----   1-7-2009  16:01:40.110   -------
     45 00 00 60 00 18 00 00 F4 11 2E 87 7B 2D 06 07     E.......ô......
     7B 2D 43 08 04 D6 1B 58 00 4C AA 3F 44 4D 50 E1     ?.U.Ö.X.L..DMPá
     74 90 00 04 2D 01 2F 2D 08 00 45 00 00 22 00 0F     t........E.....
     00 00 F9 01 2F BC 0A 02 3F 02 0A 02 3F 0A 08 00     ..ù.............
```

```
E7 26 A5 0E 00 0F 01 77 00 00 6A 44 00 00 00 00     ç.¥....w..jD....
00 00 00 00 00 00 00 00 00 00 00 00 FE EE 30 1A     ..............î0.

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 60          Length:        96
      00 18          ID:            24
      00 00          Frag Offset:   0
                     Congestion:    Normal
                                    May Fragment
                                    Last Fragment
      FA             TTL:           250
      11             Proto:         UDP
      28 87          Checksum:      10375
   7B 2D 06 07    Src IP:        94.197.41.59
   7B 2D 43 08    Dst IP:        213.152.58.85
                  UDP:
      04 D6          SRC Port:      ??? (1238)
      1B 58          DST Port:      ??? (7000)
      00 4C          Length:        76
      AA 3F          Checksum:      43583
                     ----------
```

```
E7 26 A5 0E 00 0F 01 77 00 00 6A 44 00 00 00 00     ç.¥....w..jD....
00 00 00 00 00 00 00 00 00 00 00 00 FE EE 30 1A     ..............þî0.

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 60          Length:        96
      00 18          ID:            24
      00 00          Frag Offset:   0
                     Congestion:    Normal
                                    May Fragment
                                    Last Fragment
      F4             TTL:           244
      11             Proto:         UDP
      2E 87          Checksum:      11911
   7B 2D 06 07    Src IP:        94.197.41.59
   7B 2D 43 08    Dst IP:        213.152.58.85
                  UDP:
      04 D6          SRC Port:      ??? (1238)
      1B 58          DST Port:      ??? (7000)
      00 4C          Length:        76
      AA 3F          Checksum:      43583
                     ----------
```

ICMP ping request is encapsulated and sent to the DR device.

12

```
          -----   1-7-2009  16:01:40.110   -------
44 4D 50 E1 74 90 00 04 2D 01 2F 2D 08 00 45 00     DMPát........E.
00 22 00 0F 00 00 F9 01 2F BC 0A 02 3F 02 0A 02     ......ù.........
3F 0A 08 00 E7 26 A5 0E 00 0F 01 77 00 00 6A 44     ....ç.¥....w..jD
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00     ................
   FE EE 30 1A 00 00                                   þî0...

ETH From LOC TO REM           IFACE: ETH 0
      44 4D 50 E1 74 90  Dst. MAC
      00 04 2D 01 2F 2D  Src. MAC
      08 00              Type:      IP
                  IP:
      45             IP Ver:        4
                     Hdr Len:       20
      00             TOS:           Routine
                     Delay:         Normal
                     Throughput:    Normal
                     Reliability:   Normal
      00 22          Length:        34
      00 0F          ID:            15
      00 00          Frag Offset:   0
```

		Congestion: Normal May Fragment Last Fragment F9 TTL: 249 01 Proto: ICMP 2F BC Checksum: 12220 0A 02 3F 02 Src IP: 10.2.63.2 0A 02 3F 0A Dst IP: 10.2.63.10 ----------

ICMP ping request is sent on the DR network.

13		----- 1-7-2009 16:01:40.110 ------- 00 04 2D 01 2F 2D 44 4D 50 E1 74 90 08 00 45 00 ......DMPát..E. 00 22 3E 59 00 00 40 01 AA 72 0A 02 3F 0A 0A 02 ...Y.....r..... 3F 02 00 00 EF 26 A5 0E 00 0F 01 77 00 00 6A 44 ......¥....w..jD 00 00 00 00 00 00 00 00 00 00 00 00 .... ETH From REM TO LOC IFACE: ETH 0 00 04 2D 01 2F 2D Dst. MAC 44 4D 50 E1 74 90 Src. MAC 08 00 Type: IP IP: 45 IP Ver: 4 Hdr Len: 20 00 TOS: Routine Delay: Normal Throughput: Normal Reliability: Normal 00 22 Length: 34 3E 59 ID: 15961 00 00 Frag Offset: 0 Congestion: Normal May Fragment Last Fragment 40 TTL: 64 01 Proto: ICMP AA 72 Checksum: 43634 0A 02 3F 0A Src IP: 10.2.63.10 0A 02 3F 02 Dst IP: 10.2.63.2 ----------

ICMP reply is received from the DR network device.

14 & 15	----- 1-7-2009 16:01:16.920 ------- 45 00 00 58 00 05 00 00 F3 11 2F A2 7B 2D 43 08 E..X....ó..¢Ð.U 7B 2D 06 07 1B 58 04 D6 00 44 D9 58 00 04 2D 01 .Å...X.Ö.DÙX....	----- 1-7-2009 16:01:40.110 ------- 45 00 00 58 00 05 00 00 FA 11 28 A2 7B 2D 43 08 E..X........?.U 7B 2D 06 07 1B 58 04 D6 00 44 D9 58 00 04 2D 01 .....X.Ö.DÙX....

```
2F 2D 44 4D 50 E1 74 90 08 00 45 00 00 22 3E 59     ..DMPát..E....Y
00 00 40 01 AA 72 0A 02 3F 0A 0A 02 3F 02 00 00     ....ªr.........
EF 26 A5 0E 00 0F 01 77 00 00 6A 44 00 00 00 00     ï.¥....w..jD....
00 00 00 00 00 00 00 00                             ........

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 58          Length:        88
00 05          ID:            5
00 00          Frag Offset:   0
               Congestion:    Normal
                              May Fragment
                              Last Fragment
F3             TTL:           243
11             Proto:         UDP
2F A2          Checksum:      12194
7B 2D 43 08    Src IP:        213.152.58.85
7B 2D 06 07    Dst IP:        94.197.41.59
               UDP:
1B 58          SRC Port:      ??? (7000)
04 D6          DST Port:      ??? (1238)
00 44          Length:        68
D9 58          Checksum:      55640
               ----------
```

```
2F 2D 44 4D 50 E1 74 90 08 00 45 00 00 22 3E 59     ..DMPát..E....Y
00 00 40 01 AA 72 0A 02 3F 0A 0A 02 3F 02 00 00     .....r.........
EF 26 A5 0E 00 0F 01 77 00 00 6A 44 00 00 00 00     ..¥....w..jD....
00 00 00 00 00 00 00 00                             ........

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 58          Length:        88
00 05          ID:            5
00 00          Frag Offset:   0
               Congestion:    Normal
                              May Fragment
                              Last Fragment
FA             TTL:           250
11             Proto:         UDP
28 A2          Checksum:      10402
7B 2D 43 08    Src IP:        213.152.58.85
7B 2D 06 07    Dst IP:        94.197.41.59
               UDP:
1B 58          SRC Port:      ??? (7000)
04 D6          DST Port:      ??? (1238)
00 44          Length:        68
D9 58          Checksum:      55640
               ----------
```

ICMP reply is encapsulated and sent to the WR by the DR.

16

```
-----   1-7-2009  16:01:16.920   -------
00 04 2D 01 2F 2D 44 4D 50 E1 74 90 08 00 45 00     ......DMPát..E.
00 22 3E 59 00 00 40 01 AA 72 0A 02 3F 0A 0A 02     ...Y....ªr......
3F 02 00 00 EF 26 A5 0E 00 0F 01 77 00 00 6A 44     ....ï.¥....w..jD
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00     ................

ETH From LOC TO REM           IFACE: ETH 0
00 04 2D 01 2F 2D  Dst. MAC
44 4D 50 E1 74 90  Src. MAC
08 00              Type:      IP
                   IP:
45             IP Ver:        4
               Hdr Len:       20
00             TOS:           Routine
               Delay:         Normal
               Throughput:    Normal
               Reliability:   Normal
00 22          Length:        34
3E 59          ID:            15961
```

	00 00 Frag Offset: 0 Congestion: Normal May Fragment Last Fragment 40 TTL: 64 01 Proto: ICMP AA 72 Checksum: 43634 0A 02 3F 0A Src IP: 10.2.63.10 0A 02 3F 02 Dst IP: 10.2.63.2 ----------	

ICMP reply is sent to 10.2.63.2 and devices have been successfully bridged across the Internet

4 CONFIGURATION FILES

4.1 DR6410 "Local" Site A configuration

This is the configuration file from DR6410 Site A TransPort:

```
eth 0 IPaddr "10.2.63.100"
eth 0 ipanon ON
eth 0 ethanon ON
eth 0 srcbHost "[WR41 SITE B IP ADDRESS]"
eth 0 srcbPort 6000
eth 0 srcbListenport 7000
bridgemac 0 mac "[ENTER MAC ADDRESS TO BE BRIDGED]"
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
def_route 1 ll_ent "PPP"
def_route 1 ll_add 3
ppp 1 IPaddr "0.0.0.0"
ppp 1 username "[ENTER ADSL USERNAME]"
ppp 1 epassword "[ADSL ENCRYPTED PASSWORD]"
ppp 1 timeout 0
ppp 1 aodion 1
ppp 1 immoos ON
ppp 1 autoassert 1
ppp 1 echo 10
ppp 1 echodropcnt 5
ppp 1 l1iface "AAL"
ppp 1 ipanon ON
ppp 3 l_pap OFF
ppp 3 l_chap OFF
ppp 3 l_addr ON
ppp 3 r_chap OFF
ppp 3 r_addr OFF
ppp 3 IPaddr "0.0.0.0"
ppp 3 username "ENTER WWAN Username"
ppp 3 epassword "KD5lSVJDVVg="
ppp 3 phonenum "*98*1#"
ppp 3 timeout 0
ppp 3 use_modem 1
ppp 3 aodion 1
ppp 3 immoos ON
ppp 3 autoassert 1
ppp 3 defpak 16
ppp 4 defpak 16
modemcc 0 info_asy_add 9
modemcc 0 init_str "+CGQREQ=1"
```

```
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "Your.APN.Goes.Here"
modemcc 0 link_retries 10
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
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
modemcc 0 sms_interval_2 1
ana 0 anon ON
ana 0 l1on ON
ana 0 xoton OFF
ana 0 lapdon 0
ana 0 lapbon 0
ana 0 ipfilt "~7000,6000"
ana 0 discardson ON
ana 0 discportfilt "~7000,6000"
ana 0 maxdata 1500
ana 0 logsize 180
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "Sarian.router"
cmd 0 tremto 1200
cmd 0 web_suffix ".wb2"
user 0 name "username"
user 0 epassword "KD5lSVJDVVg="
user 0 access 0
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
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
```

4.2 WR41 "Remote" Site B configuration

This is the configuration file from WR41 Site B TransPort:

```
eth 0 IPaddr "10.2.63.200"
eth 0 ipanon ON
eth 0 ethanon ON
eth 0 srcbHost "[DR6410 SITE A IP ADDRESS]"
eth 0 srcbPort 7000
eth 0 srcbListenport 6000
bridgemac 0 mac "[ENTER MAC ADDRESS TO BE BRIDGED]"
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
gps 0 asy_add 1
gps 0 gpson ON
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
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 ipanon ON
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 "3internet"
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 l1on ON
ana 0 lapdon 0
ana 0 lapbon 0
ana 0 asyon 0
ana 0 ipfilt "~7000,6000"
ana 0 discardson ON
```

```
ana 0 discportfilt "~7000,6000"
ana 0 maxdata 1500
ana 0 logsize 180
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "Sarian.router"
cmd 0 asyled_mode 2
cmd 0 tremto 1200
cmd 0 web_suffix ".wb2"
cmd 1 autocmd "ats31=7"
cmd 1 gpson 1
user 0 name “Sarian”
user 0 epassword "Dw0iCw=="
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
```

5 FIRMWARE VERSIONS

NOTE: As part of updating this document version to version 1.3, these steps have been tested and verified with TransPort WR21 and WR44v2 units running the current release firmware to-date, v5.2.14.5.

5.1 "Local" Site A DR6410

```
Digi TransPort DR64-HXA1-DE2-XX(MkII) Ser#:17000 HW Revision: 7503a
Software Build Ver5146+f9f14f.  Feb 23 2012 13:22:19  9W
ARM Bios Ver 6.29 v35 197MHz B128-M128-F300-O100000,0 MAC:00042d000000
Power Up Profile: 0
Async Driver              Revision: 1.19  Int clk
Wi-Fi                     Revision: 2.0
Ethernet Port Isolate Driver Revision: 1.11
Firewall                  Revision: 1.0
EventEdit                 Revision: 1.0
Timer Module              Revision: 1.1
AAL                       Revision: 1.0
ADSL                      Revision: 1.0
(B)USBHOST                Revision: 1.0
L2TP                      Revision: 1.10
PPTP                      Revision: 1.00
TACPLUS                   Revision: 1.00
MySQL                     Revision: 0.01
LAPB                      Revision: 1.12
X25 Layer                 Revision: 1.19
MACRO                     Revision: 1.0
PAD                       Revision: 1.4
X25 Switch                Revision: 1.7
V120                      Revision: 1.16
TPAD Interface            Revision: 1.12
SCRIBATSK                 Revision: 1.0
BASTSK                    Revision: 1.0
ARM Sync Driver           Revision: 1.18
TCP (HASH mode)           Revision: 1.14
TCP Utils                 Revision: 1.13
PPP                       Revision: 1.19
WEB                       Revision: 1.5
SMTP                      Revision: 1.1
FTP Client                Revision: 1.5
FTP                       Revision: 1.4
IKE                       Revision: 1.0
PollANS                   Revision: 1.2
PPPOE                     Revision: 1.0
BRIDGE                    Revision: 1.1
MODEM CC (Option 3G)      Revision: 1.4
FLASH Write               Revision: 1.2
Command Interpreter       Revision: 1.38
SSLCLI                    Revision: 1.0
OSPF                      Revision: 1.0
BGP                       Revision: 1.0
```

```
QOS                     Revision: 1.0
RADIUS Client           Revision: 1.0
SSH Server              Revision: 1.0
SCP                     Revision: 1.0
CERT                    Revision: 1.0
LowPrio                 Revision: 1.0
Tunnel                  Revision: 1.2
OVPN                    Revision: 1.2
TEMPLOG                 Revision: 1.0
iDigi                   Revision: 2.0
OK
```

5.2 "Remote" Site B WR41

```
Digi TransPort WR41-HXA1-DV1-XX(WR41v1) Ser#:140000 HW Revision: 7103a
Software Build Ver5146.  Feb 08 2012 12:24:12  ZW
ARM Bios Ver 6.55 v36 399MHz B128-M128-F80-O100,0 MAC:00042d000000
Power Up Profile: 0
Async Driver              Revision: 1.19  Int clk
Ethernet Driver           Revision: 1.11
Firewall                  Revision: 1.0
EventEdit                 Revision: 1.0
Timer Module              Revision: 1.1
(B)USBHOST                Revision: 1.0
SDMMC                     Revision: 1.0
L2TP                      Revision: 1.10
PPTP                      Revision: 1.00
TACPLUS                   Revision: 1.00
MODBUS                    Revision: 0.00
MultiTX                   Revision: 1.00
LAPB                      Revision: 1.12
X25 Layer                 Revision: 1.19
MACRO                     Revision: 1.0
PAD                       Revision: 1.4
V120                      Revision: 1.16
TPAD Interface            Revision: 1.12
GPS                       Revision: 1.0
SCRIBATSK                 Revision: 1.0
BASTSK                    Revision: 1.0
PYTHON                    Revision: 1.0
ARM Sync Driver           Revision: 1.18
TCP (HASH mode)           Revision: 1.14
TCP Utils                 Revision: 1.13
PPP                       Revision: 1.19
WEB                       Revision: 1.5
SMTP                      Revision: 1.1
FTP Client                Revision: 1.5
FTP                       Revision: 1.4
IKE                       Revision: 1.0
PollANS                   Revision: 1.2
PPPOE                     Revision: 1.0
MODEM CC (Option 3G)      Revision: 1.4
FLASH Write               Revision: 1.2
Command Interpreter       Revision: 1.38
SSLCLI                    Revision: 1.0
OSPF                      Revision: 1.0
BGP                       Revision: 1.0
QOS                       Revision: 1.0
PWRCTRL                   Revision: 1.0
RADIUS Client             Revision: 1.0
SSH Server                Revision: 1.0
SCP                       Revision: 1.0
CERT                      Revision: 1.0
LowPrio                   Revision: 1.0
Tunnel                    Revision: 1.2
OVPN                      Revision: 1.2
```

```
iDigi                    Revision: 2.0
OK
```