Application Note 57

TransPort simultaneous Wi-Fi Access Point and Client Mode setup

August 2016

Contents

1   INTRODUCTION

1.1 Outline

The Digi TransPort family of routers can be setup to work as a Wi-Fi Access Point (AP), and also work in Client Mode to connect into an existing Wi-Fi network. These features can be setup to run independently on the TransPort, or setup to run simultaneously in both modes.

There are 3 models of the Digi TransPort that support these Wi-Fi capabilities:

- Digi TransPort WR41
- Digi TransPort WR44
- Digi TransPort DR64

More product information on the Digi TransPort can be found at www.digi.com.

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.

Preconditions: This guide assumes that the TransPort has Wi-Fi Features

Models shown: Digi TransPort WR44v2

Other Compatible Models: All other TransPort products with Wi-Fi features

Firmware versions: All Versions

1.3 Corrections

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

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

1.4 Version

Version Number	Status
1.0	Initial release – 2012-May-15 (exQN28)
1.1	New AN draft
2.0	AN completed 7/2015
2.1	Updated screenshots and instructions for new web interface, rebranding (July 2016)

2 SCENARIO

In this AN, the following scenario will be considered:

TransPort simultaneous Wi-Fi Access Point and Client Mode setup
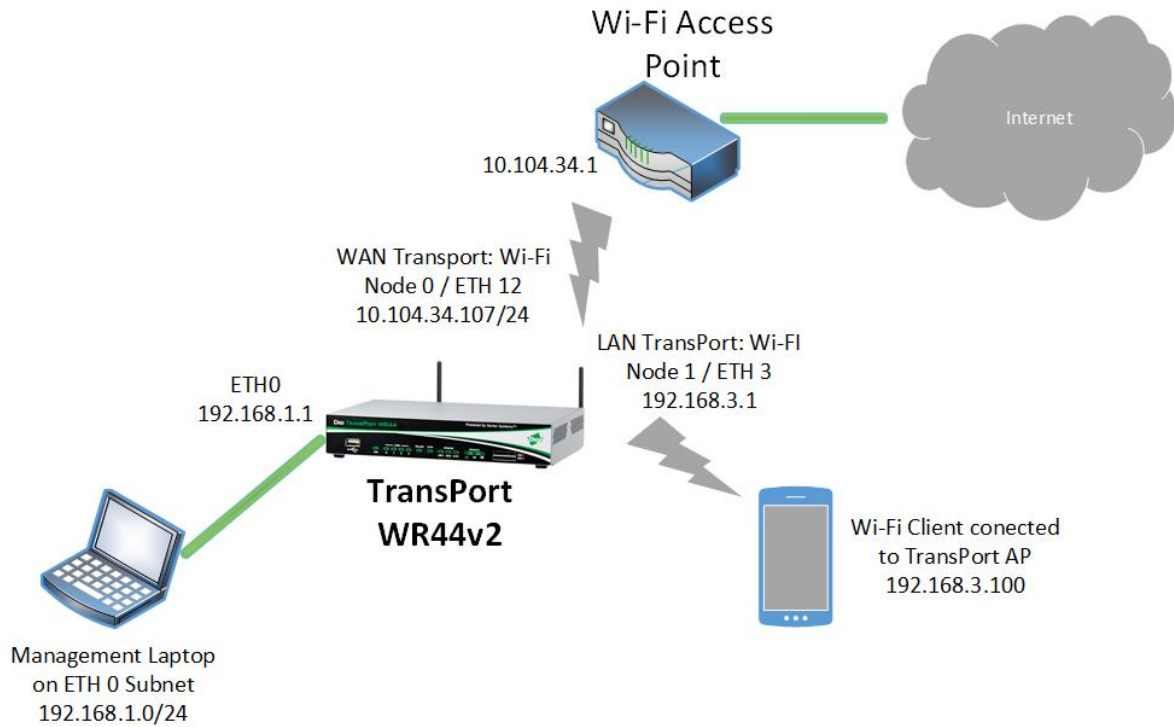
3 WI-FI CLIENT MODE SETUP

In the following sections, it will be shown how to configure the TransPort to act as a Wi-Fi Client. In order to access to the web interface, connect to the device default address 192.168.1.1 on ETH 0.

3.1 Global WiFi configuration

Configuration - Network > Interfaces > Wi-Fi > Global Wi-Fi Settings

Click Apply and Save the changes.

Please see the following table for details on settings:

Parameter	Setting	Description	CLI command
Country	United States	Set the Country that the device will be used in.	*wifi 0 country "United States"*
Network Mode	B/G/N	Set the Network Mode to either A,B/G,B/G/N, depending on the type needed.	*wifi 0 chanmode "bgn"*
Channel	1	Configure the Channel to match the channel that is being used by the Access Point the TransPort's client will be connecting to.	*wifi 0 channel "1"*

NOTE: For both Access Point and Client Mode to work simultaneously, the same channel MUST be used by both modes and must be hard coded in the setup. DO NOT use the default "Auto" option.

3.2 WiFi Node 0 configuration

Configuration - Network > Interfaces > Wi-Fi > Wi-Fi Node 0

Configuration - Network > Interfaces > Wi-Fi > Wi-Fi Node 0

▼ Wi-Fi Node 0

☑ Enable this Wi-Fi interface

Description: Wi-Fi Client (WAN)

SSID: Sample Access Point

Mode: Client

Link this Wi-Fi client interface with Ethernet: 12

Click here to assign a timeband to this interface

Wi-Fi Security

Use the following security on this Wi-Fi interface:

○ None   ○ WEP   ○ WPA Personal   ◉ WPA2 Personal   ○ WPA Enterprise   ○ WPA2 Enterprise

WPA-PSK Settings

WPA Encryption: ○ TKIP   ◉ AES (CCMP)

WPA pre-shared key: ••••••••   (8 - 63 chars)

Confirm WPA pre-shared key: ••••••••

▸ Network Scanning

Apply

Click Apply and Save the changes.

Please see the following table for details on settings:

Parameter	Setting	Description	CLI command
Enable this Wi-Fi interface	Ticked	Enable the Wi-Fi interface. If not already checked, check it to enable the Wi-Fi interface and reveal settings.	*wifinode 0 enabled "On"*
Description	Wi-Fi Client (WAN)	This parameter allows you to enter a descriptive name for the Wi-Fi interface to make it easier to identify.	*wifinode 0 descr* *"Wi-Fi Client (WAN)"*
SSID	Sample Access Point	When the Wi-Fi interface is configured to be a Client, this is the SSID of the Access Point you wish to connect to.	*wifinode 0 ssid* *"Sample Access Point"*
Mode	Client	The Wi-Fi interface can be run in various modes: • Access Point • Client • Rogue Detection (Scan for unauthorised Access Points)	*wifinode 0 mode "client"*
Link this Wi-Fi client interface with Ethernet \<n\>	12	When the Wi-Fi interface is configured to be a client, it must be bridged to a particular Ethernet interface. Bind this to an unused Ethernet interface, or even better use a logical Ethernet interface so all the physical Ethernet interfaces on the TransPort remain available to use by wired hosts. The logical interface number will vary depending on the platform in use, but the number is easily determined by browsing to Configuration - Network > Interfaces > Ethernet > Logical Ethernet Interfaces, and selecting the first available logical interface.	*eth 12 wificli "ON"*
Use the following security on this Wi-Fi interface	WPA2 Personal	Selects the security to match the security settings for the AP that the TransPort is connecting to: • None • WEP • WPA Personal (also known as "WPA-PSK") • WPA2 Personal (also known as "WPA2-PSK") • WPA Enterprise (also known as "WPA-RADIUS") • WPA2 Enterprise (also known as "WPA2-RADIUS")	*wifinode 0 security "wpa2psk"*
WPA Encryption	AES (CCMP)	The encryption algorithm to use to connect to the AP.	*wifinode 0 wpatype "aes"*
WPA pre-shared key	********	The pre-shared key (PSK) to use. It must be between 8 and 63 characters long.	*wifinode 0 esharedkey *********

NOTE: If you are unsure about the configuration of the AP to which the TransPort will connect, navigate to the "Network Scanning" section at the bottom of the Wi-Fi Node x settings and click the "Perform Network Scan" button. You should see a list of available AP SSIDs, and for each the security and channel details, as in the following example:

Configuration - Network > Interfaces > Wi-Fi > Wi-Fi Node 0

Perform Network Scan

Wireless Networks

SSID	MAC	Security	WPA Type	Signal	Channel	
Sample Access Point	00:80:48:69:8E:76	WPA2-PSK	AES	excellent	1	Connect
Finished Network Scan.						

3.3 Ethernet interface configuration

The Ethernet interface that you will navigate to must match the Ethernet interface you bound the Wi-Fi client to in the 3.2 section. This example is using ETH 12 of the TransPort.

Configuration - Network > Interfaces > Ethernet > Logical Ethernet Interfaces > ETH 12

▼ Advanced

This interface is associated with: Wi-Fi 0

This device is currently in Port Isolate mode [Switch to Hub mode]

Metric: [1]

MTU: [1500]

Max Rx rate: [0] kbps

Max Tx rate: [0] kbps

TCP transmit buffer size: [0] bytes

Take this interface out of service after [0] seconds when the link is lost (e.g. cable removed or broken)

☑ Enable NAT on this interface
◉ IP address   ○ IP address and Port

Click Apply and Save the changes.

Please see the following table for details on settings:

Parameter	Setting	Description	CLI command
Description	ETH linked with Wi-Fi Client	This parameter allows you to enter a name for this Ethernet instance, to make it easier to identify.	*eth 12 descr "ETH linked with Wi-Fi Client"*
Get an IP address automatically using DHCP	Ticked	Selecting this option enables the DHCP client on this interface. In this case, the TransPort will receive the IP address from the AP it will connect to.	*eth 12 dhcpcli "ON"*
Enable NAT on this interface	Ticked	The Wi-Fi Client interface will be used to route IP traffic, so NAT will need to be enabled as well. Check the box for Enable NAT on this interface.	*eth 12 do_nat "1"*

3.4 Default Route configuration

In order to have the Wi-Fi Client interface acting as WAN interface, so that the traffic destined to the outside is routed out of it, it is needed to configure a default route having as outgoing interface the ETH interface that has been linked to the Wi-Fi Client node. In this example it is ETH 12:

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

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

▼ Default Route 0

    Description: Def Route for Wi-Fi Client

            Default route via
            Gateway:
            Interface: Ethernet ▼ 12
    Use PPP sub-configuration: 0
            Metric: 1

▶ Advanced

Apply

Please see the following table for details on settings:

Parameter	Setting	Description	CLI command
Description	Def Route for Wi-Fi Client	The text in this text box is used to assign a convenient and memorable description for the route.	*def_route 0 descr "Def Route for Wi-Fi Client"*
Interface	Ethernet 12	The interface used to route the packets is selected from the drop-down list and the interface instance number is entered into the adjacent text box. In this example, the ETH interface linked to the Wi-Fi client interface.	*def_route 0 ll_ent "ETH"* *def_route 0 ll_add 12*

4 WI-FI ACCESS POINT MODE SETUP

In the following sections, it will be shown how to configure the TransPort to act as a Wi-Fi AP.

Make sure to note the Channel and Encryption type that was used for the Client mode in the previous steps. These will be needed for the AP configuration.

4.1 Wi-Fi Node 1 configuration

The following instructions describe how to configure the TransPort to work as an AP:

Configuration - Network > Interfaces > Wi-Fi > Wi-Fi Node 1

Click Apply and Save the changes.

Please see the following table for details on settings:

Parameter	Setting	Description	CLI command
Enable this Wi-Fi interface	Ticked	Enable the Wi-Fi interface. If not already checked, check it to enable the Wi-Fi interface and reveal settings.	*wifinode 1 enabled "ON"*
Description	Wi-Fi AP (LAN)	This parameter allows you to enter a descriptive name for the Wi-Fi interface to make it easier to identify.	*wifinode 1 descr "Wi-Fi AP (LAN)"*
SSID	TransPort AP	When the Wi-Fi interface is configured to be an Access Point, this is the SSID that will be advertised to the Wi-Fi clients.	*wifinode 1 ssid "TransPort AP"*
Mode	Access Point	The Wi-Fi interface can be run in various modes: • Access Point • Client • Rogue Detection (Scan for unauthorised Access Points)	*wifinode 1 mode "ap"*
This Wi-Fi interface is a member of Bridge instance <n> and therefore bridged to the following interfaces	0 ETH 3	When the Wi-Fi interface is configured to be an Access Point, in order to forward packets to and from the Wi-Fi interface, it must be bridged with an Ethernet <n> interface using a Bridge instance: - Select the Bridge instance from the dropdown menu (in this example the default value "0" is used) - The eth interface needs to be added in the list selecting "eth" from the drop down menu, setting "n" in the next blank box and click "add" (in this example ETH 3 is added)	*wifinode 1 bridge_inst "0"* *eth 3 bridge "ON"* *eth 3 bridge_inst "0"*
Use the following security on this Wi-Fi interface	WPA2 Personal	Selects the security to match the security settings for the Client(s) connecting to this TransPort: • None • WEP • WPA Personal (also known as "WPA-PSK") • WPA2 Personal (also known as "WPA2-PSK") • WPA Enterprise (also known as "WPA-RADIUS") • WPA2 Enterprise (also known as "WPA2-RADIUS")	*wifinode 1 security "wpa2psk"*
WPA Encryption	AES (CCMP)	The encryption algorithm to use to connect to this TransPort's AP: • TKIP • AES (CCMP)	*wifinode 1 wpatype "aes"*
WPA pre-shared key	********	The pre-shared key (PSK) to use. It must be between 8 and 63 characters long.	*wifinode 1 esharedkey ********

NOTE: When configuring Access Point mode and Client Mode to run simultaneously, **BOTH the Wi-Fi node 0 & Wi-Fi node 1 MUST use the same security method**. For example, if the TransPort's Client mode is configured to use WPA2 Personal security, the TransPort's Access Point must also be configured as WPA2 Personal. The PSK can (and should) be different for the AP configuration and the Client Mode configuration.

4.2 Ethernet interface configuration

The Ethernet interface that you will navigate to must match the Ethernet interface you bound the Wi-Fi AP to in the 4.1 section. This example is using ETH 3 of the TransPort.

Configuration - Network > Interfaces > Ethernet > ETH 3

Configuration - Network > Interfaces > Ethernet > ETH 3

ETH 3

Description: LAN ETH for Wi-Fi AP

Get an IP address automatically using DHCP
Use the following settings

IP Address: 192.168.3.1

Mask: 255.255.255.0

Gateway:

DNS Server:

Secondary DNS Server:

Changes to these parameters may affect your browser connection

Advanced
QoS
VRRP

Apply

Click Apply and Save the changes.

Please see the following table for details on settings:

Parameter	Setting	Description	CLI command
Description	LAN ETH for Wi-Fi AP	This parameter allows you to enter a name for this Ethernet instance, to make it easier to identify.	*eth 3 descr "LAN ETH for Wi-Fi AP"*
Use the following settings	Ticked	Selecting this option will allow manual IP configuration.	---
IP Address	192.168.3.1	Choose an IP Address for the LAN interface.	*eth 3 IPaddr "192.168.3.1"*
Mask	255.255.255.0	Choose a Mask for the LAN interface.	*eth 3 mask "255.255.255.0"*

4.3 DHCP Server configuration

In order to have the Wi-Fi clients that will connect the TransPort AP obtain an IP address, a DHCP server needs to be configured. This must be the DHCP server related to the ETH interface that's bridged to the Wi-Fi AP interface, so in this example it will be DHCP for Ethernet 3.

Configuration - Network > DHCP Server > DHCP Server for Ethernet 3

▼ DHCP Server for Ethernet 3

☑ Enable DHCP Server

IP Addresses: 192.168.3.100   to   192.168.3.119

to

to

Mask: 255.255.255.0

Gateway: 192.168.3.1

DNS Server: 192.168.3.1

Secondary DNS Server:

Domain Name:

Lease Duration: 14 days 0 hrs 0 mins

☐ Wait for 0 milliseconds before sending DHCP offer reply

☐ Duplicate Address Detection

☐ Only send offers to Wi-Fi clients

DHCP Relay

Forward DHCP requests to:

▶ Advanced
▶ Advanced DHCP Options

Apply

Click Apply and Save the changes.

Please see the following table for details on settings:

Parameter	Setting	Description	CLI command
Enable DHCP Server	Ticked	When checked, this checkbox opens up the page to reveal the DHCP server parameters	---
IP Addresses	192.168.3.100 to 192.168.3.119	Each of the three rows can be used to specify a different IP address pool. All pools should be within the same subnet. Using the CLI, this is specified slightly differently - a starting address and a range are specified instead.	*dhcp 3 IPmin "192.168.3.100"* *dhcp 3 IPrange "20"*
Mask	255.255.255.0	The value in this text box specifies the subnet mask used to on the network to which the TransPort is connected.	*dhcp 3 mask "255.255.255.0"*
Gateway	192.168.3.1	The value in this text box specifies the IP address of the gateway to be used by the clients of the LAN (in this example, the Wi-Fi clients). It is usually the IP address of the TransPort itself, as configured by the IP address of the Ethernet interface associated with this DHCP instance.	*dhcp 3 gateway "192.168.3.1"*
DNS Server	192.168.3.1	The value in this text box specifies the IP address of the primary DNS server to be used by clients on the LAN (in this example, the Wi-Fi clients). It is usually the IP address of the TransPort itself. Alternatively, this may be set to the IP address of an alternative DNS server on the LAN.	*dhcp 3 DNS "192.168.3.1"*

5 TESTING THE SIMULTANEOUS WI-FI ACCESS POINT AND CLIENT MODE

5.1 Checking the Client Mode

As soon as the Wi-Fi Client interface is configured (see section 3), the TransPort tries to connect to the specified AP.

The successful connection can be checked browsing to **Management - Network Status > Interfaces > Wi-Fi:**

This is showing that the Wi-Fi Node 0 is connected to the "Sample Access Point" AP that has been configured in section 3.

It is also useful to check if the ETH interface link to the Wi-Fi client interface has obtained the IP address via DHCP, and if the default route is UP:

Checking simultaneous AP and Client Mode

With the Client Mode UP on the TransPort and connected, try to connect a Wi-Fi-Client (for example an Android device) to the TransPort AP and try browsing a website:

Scan for Wi-Fi Aps and then select the "TransPort AP" SSID:
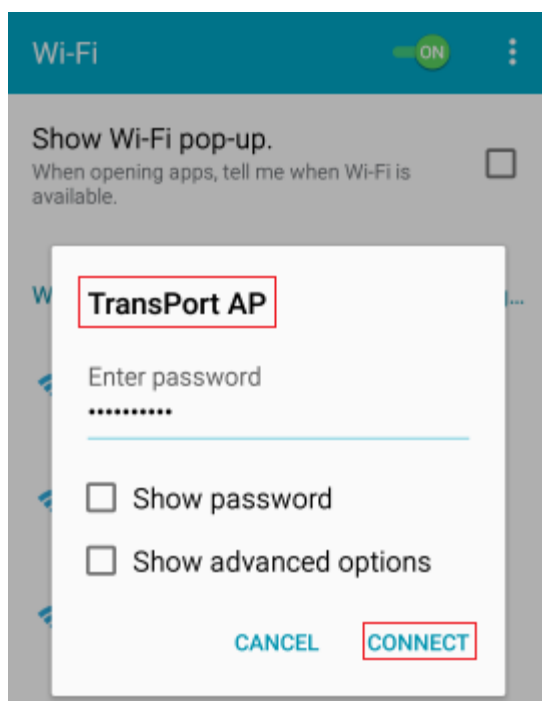
Confirm the Wi-Fi Client is connected:
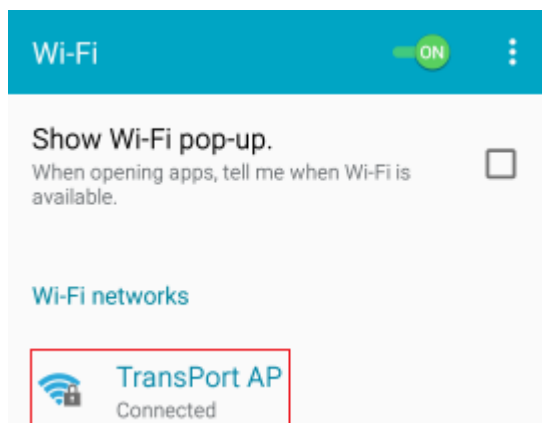
Confirm Internet access works:

The AP mode status can be also checked on the TransPort by navigating to **Management - Network Status > Interfaces > Wi-Fi:**

Management - Network Status > Interfaces > Wi-Fi

▼ Wi-Fi

    Module Detected: Yes (168C:002A)
    Admin Status: Up
    Operational Status: Up
    Channel Mode: B/G/N
    Channel: 1
    MAC Address: 04:F0:21:17:81:CE

    Bytes Received: 169365   Bytes Sent: 152015
    Packets Received: 1655   Packets Sent: 3086
    Receive Errors: 3331   Transmit Errors: 390
    Received Packets Dropped: 0

Number of Connected Wi-Fi Clients: 1

Node	Wi-Fi Node	RSSI	Flags	Power Save	Mode	Neg. Rates (Mbps)	TX Rate (Mbps)	RX Rate (Mbps)	Capability Info	
FC:C2:DE:	1	73	ERP,	Sleep	N	6.5, 13.0, 19.5, 26.0, 39.0, 52.0, 58.5, 65.0, 13.0, 26.0, 39.0, 52.0, 78.0, 104.0, 117.0, 130.0	6.5	52.0	ESS, Privacy, Short Preamble, Short Slottime,	Disconnect

Disconnect All Clients

Number of Access Point Connections: 1

Access Point	Wi-Fi Node	RSSI	Flags	Power Save	Mode	Neg. Rates (Mbps)	TX Rate (Mbps)	RX Rate (Mbps)	Capability Info	
Sample Access Point (00:80:48:69:8E:76)	0	87	-	Awake	G	1.0, 2.0, 5.5, 6.0, 9.0, 11.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0	1.0	48.0	ESS, Privacy, Short Preamble, Short Slottime,	Disconnect

Disconnect All Clients

Refresh

The IP assigned to the Wi-Fi Client device can be checked browsing to **Management – Network Status > DHCP Status:**

Management - Network Status > DHCP Status

▶ Interfaces
▶ IP Statistics
▶ IP Routing Table
▶ IP Hash Table
▶ Port Forwarding Table
▶ Firewall
▶ Firewall Trace
▼ DHCP Status

IP address	Hostname	Lease time left (mins)
192.168.3.100	android-23ed1600e9e7af5a	20154

Clear DHCP Entries

5.2 Checking the TransPort Event Log

After having both Client and AP mode connected, it can be useful to check the Event Log page to see what happened. In order to do this, navigate to **Management - Event Log**. Following there is an example of what should be shown, with some explanations:

```
*** When connecting the Android device to the TransPort AP, a "client joined" log is displayed: ***

12:55:54, 15 Jul 2016,Wi-Fi Node 1 client joined: FC:C2:DE:xx:xx:xx

*** The TransPort's Wi-Fi Client is connected to the "Sample Access Point" SSID ***

12:54:00, 15 Jul 2016,Wi-Fi Node 0 connected to Sample Access Point, RSSI:87
```

6 CONFIGURATION AND FIRMWARE DETAILS

6.1 Configuration file

This is the configuration used for the purpose of this AN. The CLI commands relevant for the configuration of the Wi-Fi Client/AP settings are highlighted:

```
Command: config c show
Command result

wifi 0 country "United States"
wifi 0 country "United States"
wifi 0 chanmode "bgn"
wifi 0 channel "1"
wifinode 0 descr "Wi-Fi Client (WAN)"
wifinode 0 ssid "Sample Access Point"
wifinode 0 mode "client"
wifinode 0 security "wpa2psk"
wifinode 0 wpatype "aes"
wifinode 0 esharedkey "PDZxUxQeFB0="
wifinode 1 descr "Wi-Fi AP (LAN)"
wifinode 1 ssid "TransPort AP"
wifinode 1 security "wpa2psk"
wifinode 1 wpatype "aes"
wifinode 1 esharedkey "PDZxUxQeFB0="
wifinode 2 enabled OFF
wifinode 3 enabled OFF
eth 0 IPaddr "192.168.1.1"
eth 3 descr "LAN ETH for Wi-Fi AP"
eth 3 IPaddr "192.168.3.1"
eth 3 bridge ON
eth 12 descr "ETH linked with Wi-Fi Client"
eth 12 dhcpcli ON
eth 12 mask ""
eth 12 do_nat 1
eth 12 wificli 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 descr "Def Route for Wi-Fi "
def_route 0 ll_ent "ETH"
def_route 0 ll_add 12
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"
dhcp 3 IPmin "192.168.3.100"
```

```
dhcp 3 mask "255.255.255.0"
dhcp 3 gateway "192.168.3.1"
dhcp 3 DNS "192.168.3.1"
sntp 0 server "time.devicecloud.com"
dyndns 0 ifent "default"
snmp 0 v1enable OFF
snmp 0 v2cenable OFF
snmp 0 v3enable OFF
services 0 telnet OFF
services 0 ssh OFF
services 0 ftp OFF
services 0 asytcp OFF
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 firewall ON
ppp 1 use_modem 1
ppp 1 cdma_backoff ON
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 pwr_dly 40
ppp 1 r_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
web 0 prelogin_info ON
ftpcli 0 hostname "ftp1.digi.com"
ftpcli 0 directory "support/firmware/transport/MC7354_carrier_firmware"
modemcc 0 info_asy_add 7
modemcc 0 apn "none"
modemcc 0 link_retries 30
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
modemcc 0 sms_access 1
modemcc 0 sms_concat 0
modemcc 0 apn_2 "none"
modemcc 0 link_retries_2 30
modemcc 0 stat_retries_2 30
modemcc 0 sms_interval_2 1
modemcc 0 sms_access_2 1
modemcc 0 sms_concat_2 0
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 "WR44v2"
cmd 0 tremto 1200
user 0 access 0
```

```
user 1 name "username"
user 1 epassword "*"
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
sslcli 0 verify 10
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
templog 0 mb_autooff ON
templog 0 mo_autooff ON
cloud 0 ssl ON

Power Up Profile: 0
OK
```

6.2 Firmware and Hardware

Following is the result of the "id" command, showing firmware and hardware used for this AN.

```
Command: id
Command result

Digi TransPort WR44-L500-NE1-SU Ser#:xxxxxx
Software Build Ver5.2.15.4.  Jun 22 2016 12:24:12  LW
ARM Bios Ver 7.56u v45 800MHz B995-M1003-F80-O0,0 MAC:00042dxxxxxx
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
(B)USBHOST              Revision: 1.0
L2TP                    Revision: 1.10
PPTP                    Revision: 1.00
TACPLUS                 Revision: 1.00
MODBUS                  Revision: 0.00
MySQL                   Revision: 0.01
RealPort                Revision: 0.00
MultiTX                 Revision: 1.00
```

```
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
GPS                        Revision: 1.0
TELITUPD                   Revision: 1.0
SCRIBATSK                  Revision: 1.0
BASTSK                     Revision: 1.0
PYTHON                     Revision: 1.0
CLOUDSMS                   Revision: 1.0
ARM Sync Driver            Revision: 1.18
TCP (HASH mode)            Revision: 1.14
TCP Utils                  Revision: 1.13
PPP                        Revision: 5.2
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 (SIERRA LTE)      Revision: 5.2
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
SSH Client                 Revision: 1.0
CERT                       Revision: 1.0
LowPrio                    Revision: 1.0
Tunnel                     Revision: 1.2
OVPN                       Revision: 1.2
TEMPLOG                    Revision: 1.0
QDL                        Revision: 1.0
OK
```