



Application Note 48

WPA Enterprise Wi-Fi Client to Digi TransPort

September 2016

Contents

1	Introduction.....	4
1.1	Outline.....	4
1.2	Assumptions	5
1.1	Corrections	5
1.2	Version.....	5
2	Digi TransPort router configuration	6
2.1	Configuration overview	6
2.2	LAN interface configuration	6
2.3	WAN interface configuration.....	7
2.4	Wi-Fi Access Point configuration	8
2.5	DHCP “Wi-Fi only” configuration (optional)	9
3	Radius server configuration.....	10
3.1	Configuration overview	10
3.2	Create ZeroShell live CD	10
3.3	Configure network settings	10
3.4	Configure profile and save settings	11
3.5	Generate CA certificate and private key	13
3.6	Create remote user account.....	14
3.7	Export remote user certificate	15
3.8	Create authorized client	16
4	Wi-Fi client configuration	17
5	Additional notes	22
6	Testing	23
7	TransPort router configuration file and firmware version	24
7.1	TransPort router configuration file.....	24
7.2	TransPort router firmware version.....	26

Figures

Figure 1: Network diagram.....	4
Figure 2: LAN interface configuration	6
Figure 3: WAN interface configuration.....	7
Figure 4: Wi-Fi Access Point configuration.....	8
Figure 5: Set DHCP to “Wi-Fi only”	9
Figure 6: Save ZeroShell profile	11
Figure 7: Populate profile parameters	12
Figure 8: View / amend profile.....	12
Figure 9: Customize the CA and generate certificate / private key.....	13
Figure 10: Warning for CA setup	13
Figure 11: Create remote user account.....	14
Figure 12: Export remote user certificate	15
Figure 13: Create authorized client	16
Figure 14: DHCP status	23
Figure 15: Wi-Fi client connected.....	23

1 Introduction

1.1 Outline

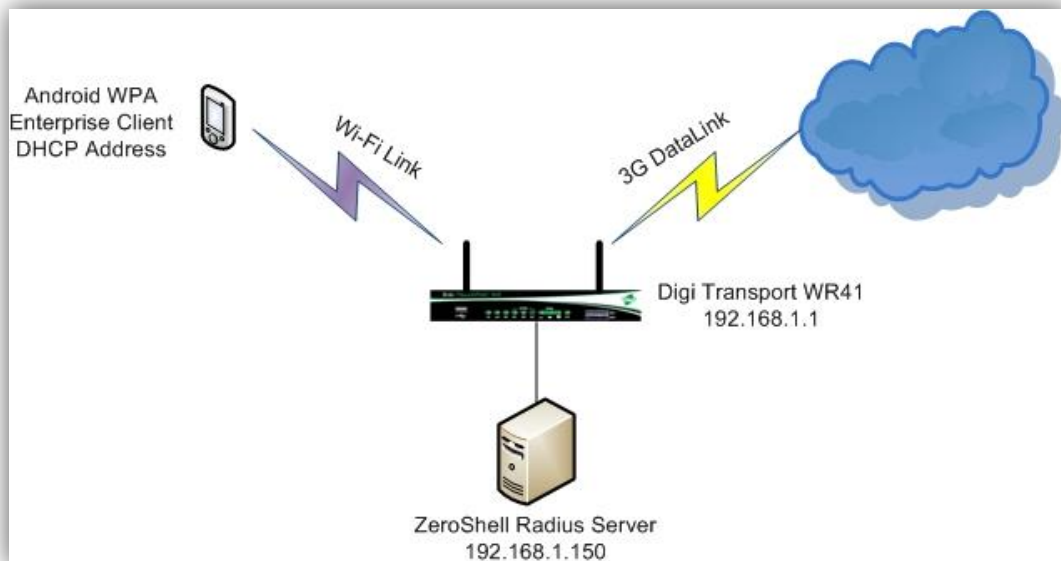


Figure 1: Network diagram

Digi TransPort – 192.168.1.1

Radius server – 192.168.1.150

Radius clients – 192.168.1.100 – 192.168.1.119

This Application Note shows the steps required to configure secure access for a Wi-Fi client to a Digi TransPort router that is configured as a Wi-Fi Access Point. Access for the client is authenticated using WPA-Enterprise (also known as WPA-802.1X) via a Radius server.

The particular example described in this document demonstrates how to connect an Android mobile phone to a Digi TransPort WR41v2 Wi-Fi Access Point, using WPA-802.1X (EAP-TLS) via a Linux-based Radius server for authentication. In Access Point mode the TransPort router acts simply as a “relay agent” between the client and the Radius server – that is, the authentication process occurs between the client and the server, with the TransPort router forwarding packets as necessary between the two devices.

To complete all of the steps shown in this Application Note, it is necessary to download the ZeroShell Linux distribution and to run it on a device that the Digi TransPort router can reach on a local test network. The example network described in this Application Note is shown in the diagram above.

Wi-Fi security is a complex subject. The following Wikipedia page contains a good overview of WPA in general, and is useful for understanding how WPA-Enterprise/802.1X and EAP-TLS fit into the overall architecture of WPA: http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

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 to configure it with basic routing functions.

This Application Note applies to:

Model: Digi TransPort WR41v2 with Wi-Fi option

Other Compatible Models: Digi TransPort DR64 and WR44 models with Wi-Fi option

Firmware versions: 5.123 and later

Configuration: This Application Note assumes that the devices are set to their factory default configurations. Most configuration commands are shown only if they differ from the factory default.

1.1 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to:

Tech.Support@digicom.com

Requests for new application notes can be sent to the same address.

1.2 Version

Version	Status
1.0	Published
1.1	Updated screenshots and verbiage

2 Digi TransPort router configuration

2.1 Configuration overview

The TransPort router configuration requires the following steps:

- LAN interface configuration
- WAN interface configuration
- Wi-Fi Access Point configuration
- DHCP “Wi-Fi only” configuration (Optional)

On any production implementation, it is strongly recommended that some of the TransPort router’s default settings are changed. These changes should normally include, but are not limited to:

- Change the default usernames and passwords
- Change the default IP addressing scheme
- Configure and activate the firewall

2.2 LAN interface configuration

CONFIGURATION - NETWORK > INTERFACES > ETHERNET > ETH 0

The example configuration described in this document uses default settings for ETH 0. Therefore ETH 0 should already be configured as follows:

[Configuration - Network](#) > [Interfaces](#) > [Ethernet](#) > [ETH 0](#)

▼ Interfaces

▼ Ethernet

▼ ETH 0

Description:

☐ Get an IP address automatically using DHCP

☒ Use the following settings

IP Address:

Mask:

Gateway:

DNS Server:

Secondary DNS Server:

Changes to these parameters may affect your browser connection

▶ Advanced

Figure 2: LAN interface configuration

Parameter	Setting	Description
IP Address	192.168.1.1	IP address assigned to ETH 0
Mask	255.255.255.0	Mask assigned to ETH 0

2.3 WAN interface configuration

CONFIGURATION > NETWORK > INTERFACES > MOBILE > MOBILE SETTINGS

In this example the WR41v2 has a cellular connection as its WAN interface. This is configured as PPP 1. If a PIN number is required for the mobile connection this will also need to be entered here. For most implementations only the APN will need to be entered:

[Configuration - Network](#) > [Interfaces](#) > [Mobile](#)

▼ Interfaces

▶ Ethernet

▶ Wi-Fi

▼ Mobile

Select a SIM to configure from the list below

Settings on this page apply to the selected SIM

SIM: 1 (PPP 1) ▼

IMSI: Unknown

▼ Mobile Settings

Select the service plan and connection settings used in connecting

Mobile Service Provider Settings

Service Plan / APN: internet

☐ Use backup APN

SIM PIN: (Optional)

Confirm SIM PIN:

Figure 3: WAN interface configuration

Parameter	Setting	Description
Service Plan / APN	<APN>	Enter the APN associated with the SIM

2.4 Wi-Fi Access Point configuration

CONFIGURATION > NETWORK > INTERFACES > WI-FI > WI-FI 0

[Configuration - Network](#) > [Interfaces](#) > [Wi-Fi](#) > [Wi-Fi Node 0](#)

☒ Enable this Wi-Fi interface

Description:

SSID:

Mode:

In order to send data to and from this Wi-Fi interface, it must be bridged with at least one other interface

This Wi-Fi interface is a member of Bridge instance and therefore bridged to the following interfaces

Interface	
Wi-Fi Node	<input type="text" value="1"/>
Wi-Fi Node	<input type="text" value="2"/>
Wi-Fi Node	<input type="text" value="3"/>
Ethernet	<input type="text" value="0"/>

Add

☐ Hide SSID

☐ Enable station isolation

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

Wi-Fi Security

☐ Enable MAC address authentication

Use the following security on this Wi-Fi interface:

☐ None ☐ WEP ☐ WPA Personal ☐ WPA2 Personal ☒ WPA Enterprise ☐ WPA3 Enterprise

WPA-802.1X Settings

WPA Encryption: ☒ TKIP ☐ AES (CCMP)

Radius NAS ID:

Radius Server IP Address:

Radius Server Password:

Confirm Radius Server Password:

▶ Network Scanning

Figure 4: Wi-Fi Access Point configuration

Parameter	Setting	Description
Enable this Wi-Fi interface	Ticked	Tick to enable the Wi-Fi interface
Description	BAY Access	Enter text to describe this interface (in this example "BAY Access" is used)
SSID	BAY_Access	Enter a name that will be seen by clients and will identify the Wi-Fi network (in this example "BAY_Access" is used)
Use the following security on this Wi-Fi Interface	WPA-802.1X	WPA2-802.1X can also be used but please check intended clients for compatibility – for example not all Android releases work with WPA2-802.1X
WPA Encryption	TKIP	Select the appropriate encryption type. (AES (CCMP) was added for WPA2.)
Radius NAS ID	BAY24	Enter the NAS ID configured into the Radius server (in this example "BAY 24" is used)
Radius Server IP Address	192.168.1.150	Enter the IP Address of the Radius Server (in this example "192.168.1.150" is used)
Radius Server Password	digitest	Enter the shared key that is used to authenticate requests from this NAS to the Radius server (in this example "digitest" is used)
Confirm Radius Server Password	digitest	Confirm the shared key that is used to authenticate requests from this NAS to the Radius server (in this example "digitest" is used)

2.5 DHCP "Wi-Fi only" configuration (optional)

CONFIGURATION > NETWORK > DHCP SERVER > DHCP SERVER FOR ETHERNET 0

If DHCP is required only for Wi-Fi clients, this setting can be used to assign the DHCP pool to the Wi-Fi clients only:

[Configuration - Network > DHCP Server > DHCP Server for Ethernet 0](#)

► Interfaces

▼ DHCP Server

▼ DHCP Server for Ethernet 0

☒ Enable DHCP Server

IP Addresses: to

to

to

Mask:

Gateway:

DNS Server:

Secondary DNS Server:

Domain Name:

Lease Duration: days hrs mins

☒ Wait for milliseconds before sending DHCP offer reply

☐ Duplicate Address Detection

☒ Only send offers to Wi-Fi clients

Figure 5: Set DHCP to "Wi-Fi only"

Parameter	Setting	Description
Only send offers to Wi-Fi clients	Ticked	Select this option to restrict DHCP to Wi-Fi clients

3 Radius server configuration

3.1 Configuration overview

In this Application Note the ZeroShell Linux distribution (booted from live CD) is used to configure a Radius server for WPA authentication of the Wi-Fi clients.

The latest version of ZeroShell can be downloaded from: <http://www.zeroshell.net/eng/download/>

Steps 3.2 to 3.4 below are specific to downloading and configuring ZeroShell.

Steps 3.5 to 3.8 below apply generally to configuring any Radius server.

3.2 Create ZeroShell live CD

Download the latest version of the ZeroShell server from the website above. There are a number of versions available. The “ISO image for CD” version 2.0.RC1 was used for this Application Note.

Create a CD containing this image using appropriate CD-burning software.

A recommended free program for Windows is: <http://cdburnerxp.se/en/home>

When the CD has been created, choose as appropriate computer to act as the Radius server and boot it from the CD (it may be necessary to change the boot device order on the computer). For this example an old laptop was used, because ZeroShell does not require especially fast computer hardware.

3.3 Configure network settings

Once the ZeroShell server has booted from the CD, a text interface is used to configure the IP address, mask and gateway and to set the admin password:

- Type option: **<I> IP Manager**
- Select: **<M> Modify IP address**
- Press Enter to configure the default Ethernet address: **Interface [ETH00]:**
- Press Enter once more: **IP to modify [1]:**
- Type in the IP address for this interface. For this example 192.168.1.150 was used for the server address: **IP [192.168.1.1]: 192.168.1.150**
- Type in the subnet mask to be used for this connection. For this example the default 24-bit mask is correct, so simply pressing Enter leaves the mask as the default value: **Netmask [255.255.255.0]:**
- IP Status should be showing as “up”: **IP status [up]:**
- Press Enter to return to the previous menu
- Type option: **<G> Set Default Gateway**
- Enter the default gateway address
For this example 192.168.1.1 was used: **Default Gateway: 192.168.1.1**
- Type option: **<Q> Quit** (to previous menu)
- Type option: **<P> Change admin password**

- If prompted for the current admin password, type in the existing password - by default this may be 'ZeroShell'. However the default password may simply be blank, therefore it may be possible to simply press Enter when prompted for the current admin password.
- Enter the new password: **New admin password: <NEW_PASSWORD>**
- Confirm the new password: **Confirm password: <NEW_PASSWORD>**

It should now be possible to navigate to <https://192.168.1.150> to begin to configure the ZeroShell server via its web interface. Log in with the username **admin** plus the admin password that was configured via the text interface.

3.4 Configure profile and save settings

This step ensures that the ZeroShell server's settings can be saved to a USB flash drive or hard drive, since the live CD is read-only. ZeroShell supports the saving of profiles to disks with ext2, ext3, ReiserFS or FAT32 filesystems. It includes an in-built formatting utility, so for example it is possible to format a USB flash drive from within the ZeroShell interface. For this example an ext3-formatted USB flash drive was used.

- Select **Setup** from the **System** section of the left hand menu
- Select **Profiles**
- Select a partition to save the profile to – it may take a short while for the drive scan to complete:

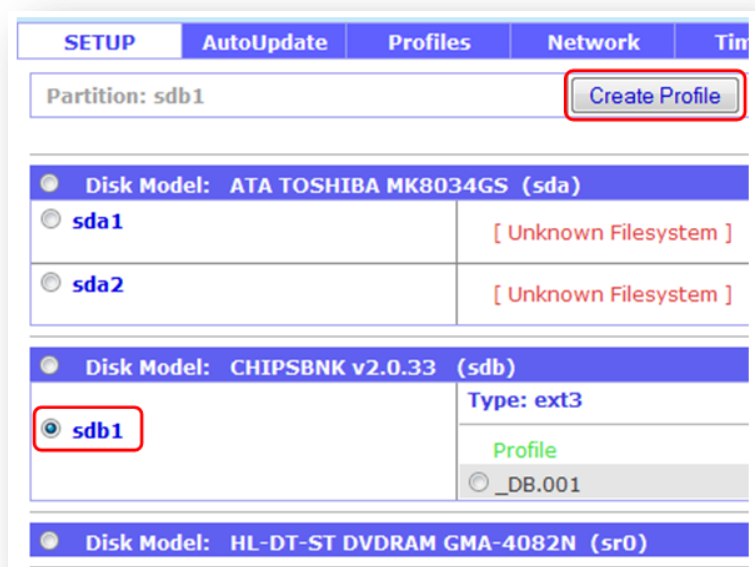


Figure 6: Save ZeroShell profile

A pop-up window will then prompt for the following parameters:

- Enter a **Description**
- Enter the **Hostname (FQDN)** of the server
- Enter a **Kerberos 5 Realm**
- Enter the **LDAP Base**
- Enter and confirm the **Admin Password** in the next two fields
- Select the correct **Ethernet Interface** (or accept the default if this is correct)
- Enter the **IP Address/Netmask** and **Default Gateway**
- Click **Create**

CHIPSBNK v2.0.33 (sdb)
New Profile on partition sdb1

Create Close

Description: UKSUPPORT Test WiFi
Hostname (FQDN): uksupport.digi.com
Kerberos 5 Realm: DIGI.COM
LDAP Base: dc=DIGI,dc=com
Admin password:
Confirm password:
NETWORK CONFIG
Ethernet Interface: ETH00 - Realtek Semiconductor Co., Ltd. RTL-8139/8139C/8139C+ (rev)
IP Address / Netmask: 192.168.1.150 / 255.255.255.0
Default Gateway: 192.168.1.1

Figure 7: Populate profile parameters

Saved profiles can be activated, deactivated, deleted or backed up from the following page:

Profile: _DB.001 (sdb1)

Activate Deactivate Info Delete Backup Backup without Logs Copy

Profile	Type	Capacity
Disk Model: ATA TOSHIBA MK8034GS (sda)		
sda1	[Unknown Filesystem]	Capacity: 74 GB
sda2	[Unknown Filesystem]	Capacity: 300 MB
Disk Model: CHIPSBNK v2.0.33 (sdb)		
sdb1	Type: ext3	Capacity: 969 MB
Profile	Description	
_DB.001	UKSUPPORT Test WiFi	
Disk Model: HL-DT-ST DVDROM GMA-4082N (sr0)		

Figure 8: View / amend profile

3.5 Generate CA certificate and private key

Please note: any desired changes to the default parameters for the CA (please see lower section in Figure 9 below) need to be applied *before* following the steps below:

- Select **X.509 CA** from the **Security** section on the left hand menu
- Select **Setup**
- Enter the **Common Name** you wish to use for the CA certificate
- Enter the **Key Size**
- Enter the **Country Name**
- Enter the **State or Province**
- Enter the **Locality**
- Enter the **Organization**
- Enter the **Operational Unit**
- Enter the **Email Address**
- Click **Generate** on the right side of the web interface

X.509 CA	List	Manage	CRL	Imported	Trusted CAs	Setup
CA Certificate and Private Key						
Common Name	Digi Test WiFi					
Key Size	1024 bits					
Validity (Days)	365					
Country Name	UK					
State or Province	West Yorkshire					
Locality	Ilkley					
Organization	DIGI.com					
Organizational Unit	UKSupport					
E-Mail Address	uksupport@digicom					
CA Default Parameters						
Key Size	1024 bits					
Certificate Validity (days)	365					
Export user/host certificates on the authentication page	No					
Apply						

Figure 9: Customize the CA and generate certificate / private key

A prompt will be seen warning that existing certificates will be deleted - click **OK** to proceed:

WARNING: if you continue with this operation you will lose all Certificates and Private Keys (Host and User Certificates too) and the Certification Authority will be reset. If you actually want it then press [OK]

OK Cancel

Figure 10: Warning for CA setup

3.6 Create remote user account

It is necessary to configure one or more remote user accounts, to enable Wi-Fi clients to authenticate with the Radius server. For this example only one remote user is configured:

- Select **Users** under the **Users** section of the left hand menu
- Click **Add**
- Enter a **Username** for the remote user
- Enter a **Firstname**
- Enter a **Lastname**
- Enter a **Password** then **Confirm** by entering it again - in this example **testuserpass** was used
- Other fields such as **Description** and **E-Mail** are optional
- Click **Submit** on the right side of the web interface

The screenshot shows the 'New User' form in the ZeroShell web interface. The form is divided into three main sections: 'Account Information', 'User Information', and 'RADIUS Accounting'. In the 'Account Information' section, the 'Username' field is filled with 'Digi_Test_User' and is highlighted with a red box. In the 'User Information' section, the 'Firstname' field is filled with 'firstname' and the 'Lastname' field is filled with 'lastname', both highlighted with a red box. In the 'RADIUS Accounting' section, the 'User Password' field is filled with 'testuserpass' and is highlighted with a red box. The 'Confirm' field is also filled with 'testuserpass' and is highlighted with a red box. The 'Submit' button is located on the right side of the form.

Figure 11: Create remote user account

The ZeroShell server will now provide the option to export the user certificate – please see section 3.7 below.

3.7 Export remote user certificate

This example uses an Android mobile phone as the remote access client, so it is necessary to export the user certificate using the standard “.pfx” format so that it can be imported into the Android phone. The user certificate includes the Radius server’s private key in addition to the certificate itself. The file should be protected with a password, so before clicking **Export** please ensure that the **Protected by password** option is ticked as shown:

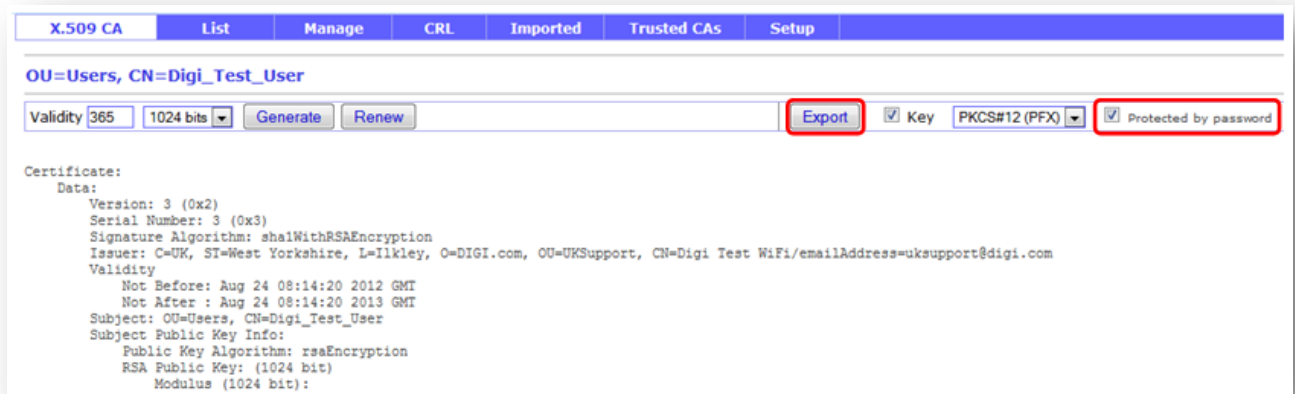


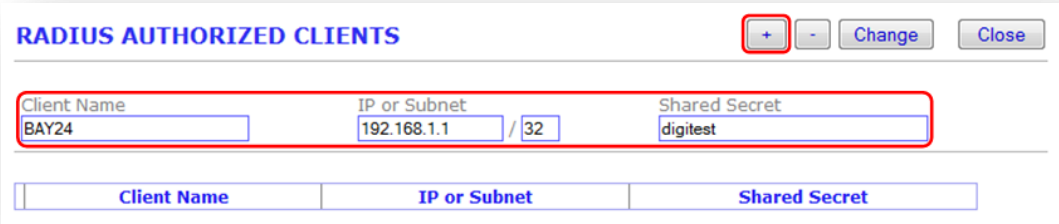
Figure 12: Export remote user certificate

This ensures that the “.pfx” file is protected by the password that was configured in the above step to create the user account. When the file is imported into the Android phone, the password will need to be entered to allow the certificate to be installed.

3.8 Create authorized client

It is necessary add the TransPort router as an authorized client in order to allow it to communicate with the ZeroShell server, and therefore to relay authentication traffic from and to the Wi-Fi client. Authentication between the TransPort router and the ZeroShell server is via a shared secret:

- Select **Radius** under the **Users** section of the left hand menu
- Select **Authorized Clients**
- Enter the **Client Name** (NAS ID) – in this example **BAY24** was used
- Enter the **IP or Subnet** of the TransPort router – in this example **192.168.1.1/32** was used
- Enter the **Shared Secret** – this must be the same as the “Radius server password” that was configured in the TransPort router - in this example **digitest** was used
- Click + to add this client



Client Name	IP or Subnet	Shared Secret
BAY24	192.168.1.1 / 32	digitest

Figure 13: Create authorized client

4 Wi-Fi client configuration

Firstly the “.pfx” file generated for the Wi-Fi client user in the section above needs to be transferred to the Android phone.

Before it is transferred the file extension must be changed from “.pfx” to “.p12” to enable the Android phone to recognise and install it.

The file transfer can be achieved in a number of ways, including via a USB cable, by email to an account that the Android phone has access to, via a network share or by using an Internet-based file storage service such as Dropbox.

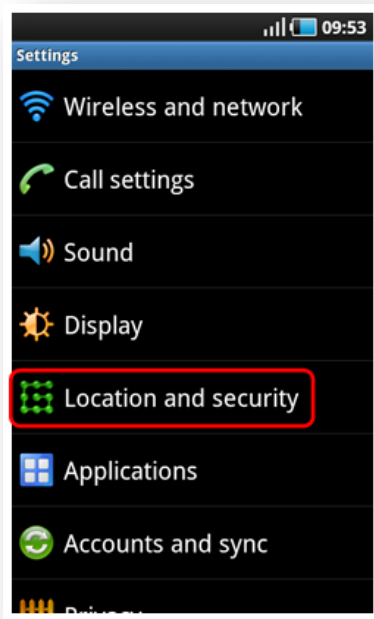
Depending on the model of Android device and the version of the Android operating system, it may be necessary to ensure that the “.p12” certificate file is transferred to an “external SD card”, rather than to the phone’s internal flash memory, in order for the phone to be able to find it.

Once the “.p12” file has been transferred to the Android phone, follow the steps below. Please note that the user interface varies between models of Android device and between versions of the Android operating system. The following screenshots are from a Samsung Galaxy S running Android version 2.2:

- Ensure Wi-Fi is enabled
- Press the **Home** button
- Press the **Menu** button
- Select **Settings**:



- Select **Location and security**:



- Select **Install encrypted certificates**:

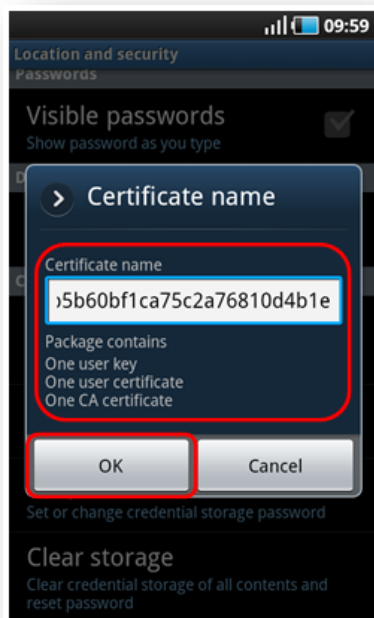


The phone should find the previously transferred “.p12” file, then prompt for the password that is protecting the file.

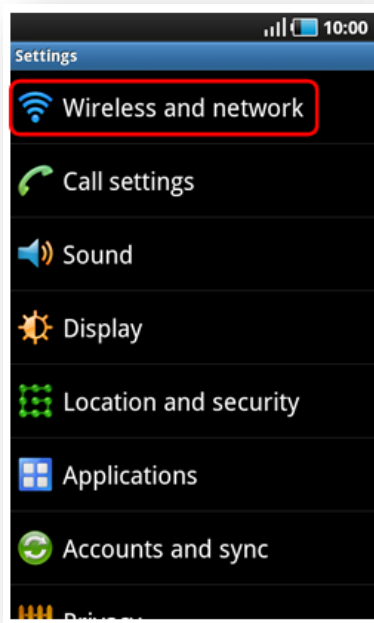
- Enter the password then click **OK** – in this example the remote user account was created in ZeroShell with the password **testuserpass**, so this is the password required to access the file:



- The phone should confirm the certificate name and that it contains a user key, a user certificate and a CA certificate. Click **OK** to install it:



- Return to the main **Settings** menu, then select **Wireless and network**:



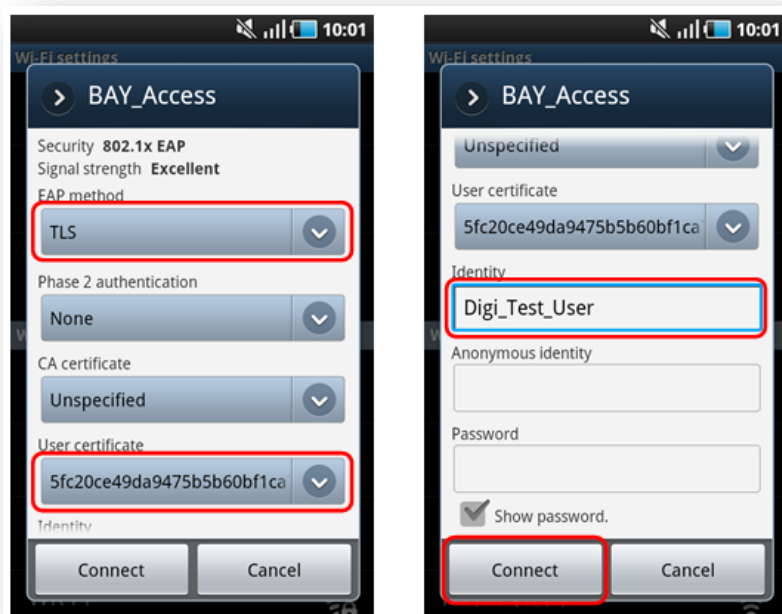
- Select **Wi-Fi settings**:



- Select the TransPort router's Wi-Fi access point from the list of available networks:



- Set the EAP method to **TLS**, select the previously installed certificate from the drop-down list as the **User certificate**, enter the **Identity** (this is the username configured for the remote access user on the ZeroShell Radius server, in this example it is **Digi_Test_User**), leave the password blank then click **Connect**:



The Android phone should connect successfully to the Wi-Fi access point, by authenticating with the Radius server using the identity (username) plus the user certificate.

5 Additional notes

When the TransPort router is operating in Wi-Fi Access Point mode, the authentication process takes place between the Wi-Fi client and the Radius server. The TransPort router acts simply as a “relay agent” between the client and server, forwarding packets as necessary between the two devices.

During testing it was found that it was possible for the Android client to authenticate with the ZeroShell server *without* the user certificate. This was achieved by setting the EAP mode to PEAP, then using the password that was set up for the remote user account in the ZeroShell server in place of the certificate (in this example the password was **testuserpass**).

It may be possible to force ZeroShell (or other Radius server) to authenticate via certificate only. If this is not possible with the Radius server being used, omitting the password from the Android configuration will ensure that it must authenticate using the certificate. Of course, it may be desirable in certain implementations to authenticate via password only rather than certificate.

The important point is that the TransPort router is not involved in the authentication process between the Wi-Fi client and the Radius server (although the TransPort router must authenticate *itself* with the Radius server, in order for the Radius server to allow it to forward authentication traffic from the client).

Therefore care should be taken to ensure that the Radius server and the client are configured correctly to ensure that the desired method of authentication is enforced.

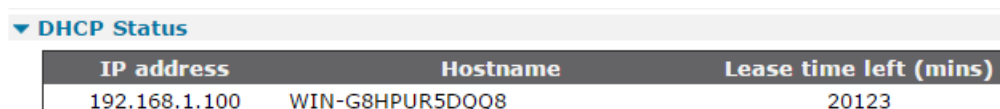
6 Testing

Issuing the following command will show that the TransPort router has issued an IP address via DHCP to the Android Wi-Fi client:

```
dhcp 0 status
Entry: IP [192.168.1.100], hostname [], MAC [b4:07:f9:c0:88:43], expiry 20154 (mins)
OK
```

This information can also be seen on the following page in the web interface:

MANAGEMENT - NETWORK STATUS > DHCP STATUS



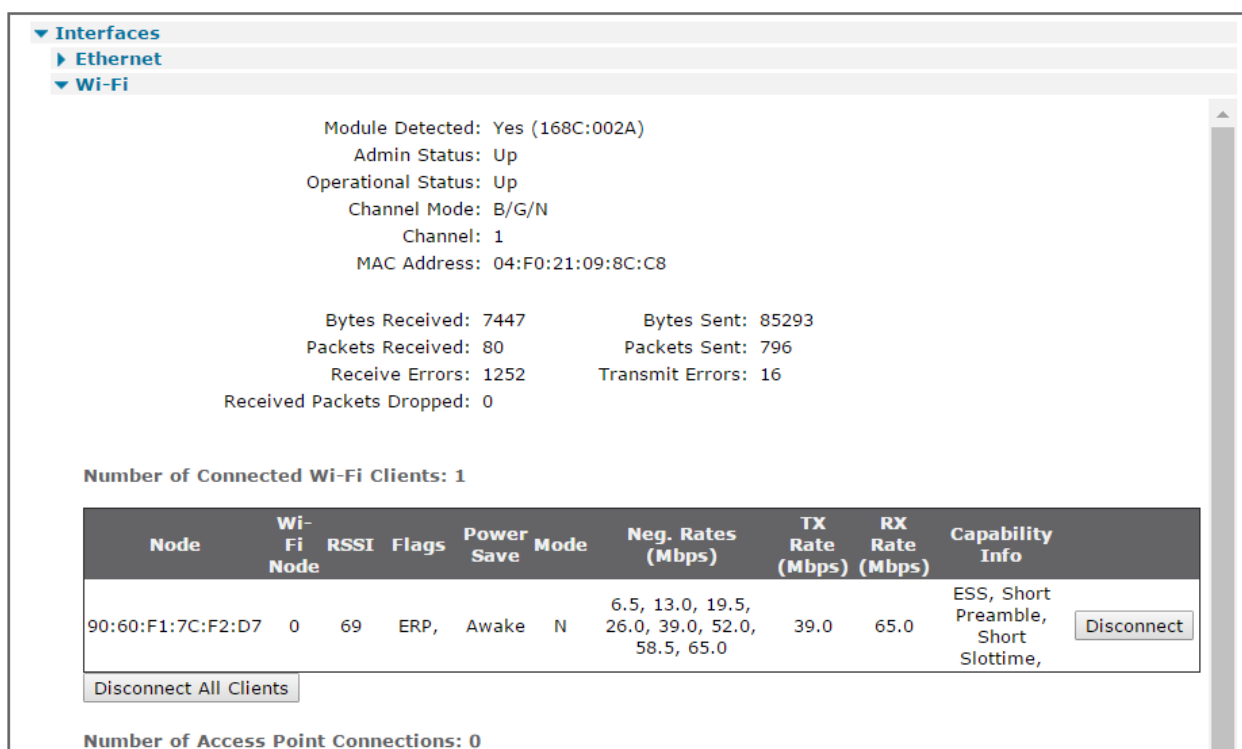
▼ DHCP Status		
IP address	Hostname	Lease time left (mins)
192.168.1.100	WIN-G8HPUR5DQQ8	20123

Figure 14: DHCP status

MANAGEMENT - NETWORK STATUS > INTERFACES > WI-FI

This page in the web interface shows that the Android Wi-Fi client is connected:

[Management - Network Status](#) > [Interfaces](#) > [Wi-Fi](#)



▼ Interfaces

- ▶ Ethernet
- ▼ Wi-Fi

Module Detected: Yes (168C:002A)
Admin Status: Up
Operational Status: Up
Channel Mode: B/G/N
Channel: 1
MAC Address: 04:F0:21:09:8C:C8

Bytes Received: 7447 Bytes Sent: 85293
Packets Received: 80 Packets Sent: 796
Receive Errors: 1252 Transmit Errors: 16
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
90:60:F1:7C:F2:D7	0	69	ERP,	Awake	N	6.5, 13.0, 19.5, 26.0, 39.0, 52.0, 58.5, 65.0	39.0	65.0	ESS, Short Preamble, Short Slottime, <button>Disconnect</button>

Disconnect All Clients

Number of Access Point Connections: 0

Figure 15: Wi-Fi client connected

The Android client should be able to access the internet through the TransPort router's cellular data connection.

7 TransPort router configuration file and firmware version

7.1 TransPort router configuration file

```
wifinode 0 descr "BAY Access"
wifinode 0 ssid "BAY_Access"
wifinode 0 security "wparadius"
eth 0 IPaddr "192.168.1.1"
eth 0 bridge ON
addp 0 enable ON
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 3 dtemode 0
lapb 3 asyport 5
lapb 3 mux_0710 ON
lapb 4 dtemode 0
lapb 4 dlc 1
lapb 4 asyport 5
lapb 4 virt_async "mux0"
lapb 4 mux_0710 ON
lapb 5 dtemode 0
lapb 5 dlc 2
lapb 5 asyport 5
lapb 5 virt_async "mux1"
lapb 5 mux_0710 ON
lapb 6 dtemode 0
lapb 6 dlc 3
lapb 6 asyport 5
lapb 6 virt_async "mux2"
lapb 6 mux_0710 ON
ip 0 cidr ON
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
dhcp 0 IPmin "192.168.1.100"
dhcp 0 respdelms 500
dhcp 0 wifionly ON
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 (Edge 2.5G)"
ppp 1 phonenumber "*98*1#"
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 use_modem 1
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 ipanon ON
ppp 1 r_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
modemcc 0 asy_add "mux1"
modemcc 0 info_asy_add "mux2"
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
modemcc 0 sms_interval_2 1
modemcc 0 sms_access_2 1
modemcc 0 sms_concat_2 0
ana 0 anon ON
ana 0 llon ON
ana 0 xoton OFF
ana 0 lapdon 0
ana 0 lapbon 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"
radcli 1 nasid "BAY24"
radcli 1 server "192.168.1.150"
radcli 1 epassword "PDZxU1FJVEg="
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
idigi 0 ssl ON
idigi 0 sms_optin ON
```

7.2 TransPort router firmware version

```
Digi TransPort WR41-G1T1-WV1-XX(WR41v2) Ser#:164895
Software Build Ver5.2.15.4. Jun 22 2016 04:58:22 MW
ARM Bios Ver 6.75 v41 399MHz B256-M256-F80-O100,0 MAC:00042d02841f
Async Driver Revision: 1.19 Int clk
Wi-Fi Revision: 2.0
Ethernet 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
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
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
BRIDGE Revision: 1.1
MODEM CC (Siemens MC75) 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
QDL Revision: 1.0
WiMax Revision: 1.0
iDigi Revision: 2.0
```