Application Note 48

WPA Enterprise Wi-Fi Client to Digi TransPort

September 2016
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  Introduction</td>
<td>4</td>
</tr>
<tr>
<td>1.1 Outline</td>
<td>4</td>
</tr>
<tr>
<td>1.2 Assumptions</td>
<td>5</td>
</tr>
<tr>
<td>1.1 Corrections</td>
<td>5</td>
</tr>
<tr>
<td>1.2 Version</td>
<td>5</td>
</tr>
<tr>
<td>2  Digi TransPort router configuration</td>
<td>6</td>
</tr>
<tr>
<td>2.1 Configuration overview</td>
<td>6</td>
</tr>
<tr>
<td>2.2 LAN interface configuration</td>
<td>6</td>
</tr>
<tr>
<td>2.3 WAN interface configuration</td>
<td>7</td>
</tr>
<tr>
<td>2.4 Wi-Fi Access Point configuration</td>
<td>8</td>
</tr>
<tr>
<td>2.5 DHCP “Wi-Fi only” configuration (optional)</td>
<td>9</td>
</tr>
<tr>
<td>3  Radius server configuration</td>
<td>10</td>
</tr>
<tr>
<td>3.1 Configuration overview</td>
<td>10</td>
</tr>
<tr>
<td>3.2 Create ZeroShell live CD</td>
<td>10</td>
</tr>
<tr>
<td>3.3 Configure network settings</td>
<td>10</td>
</tr>
<tr>
<td>3.4 Configure profile and save settings</td>
<td>11</td>
</tr>
<tr>
<td>3.5 Generate CA certificate and private key</td>
<td>13</td>
</tr>
<tr>
<td>3.6 Create remote user account</td>
<td>14</td>
</tr>
<tr>
<td>3.7 Export remote user certificate</td>
<td>15</td>
</tr>
<tr>
<td>3.8 Create authorized client</td>
<td>16</td>
</tr>
<tr>
<td>4  Wi-Fi client configuration</td>
<td>17</td>
</tr>
<tr>
<td>5  Additional notes</td>
<td>22</td>
</tr>
<tr>
<td>6  Testing</td>
<td>23</td>
</tr>
<tr>
<td>7  TransPort router configuration file and firmware version</td>
<td>24</td>
</tr>
<tr>
<td>7.1 TransPort router configuration file</td>
<td>24</td>
</tr>
<tr>
<td>7.2 TransPort router firmware version</td>
<td>26</td>
</tr>
</tbody>
</table>
Figures

Figure 1: Network diagram

Figure 2: LAN interface configuration

Figure 3: WAN interface configuration

Figure 4: Wi-Fi Access Point configuration

Figure 5: Set DHCP to “Wi-Fi only”

Figure 6: Save ZeroShell profile

Figure 7: Populate profile parameters

Figure 8: View / amend profile

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

Figure 10: Warning for CA setup

Figure 11: Create remote user account

Figure 12: Export remote user certificate

Figure 13: Create authorized client

Figure 14: DHCP status

Figure 15: Wi-Fi client connected
1 Introduction

1.1 Outline

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](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@digi.com

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

1.2 Version

<table>
<thead>
<tr>
<th>Version</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Published</td>
</tr>
<tr>
<td>1.1</td>
<td>Updated screenshots and verbiage</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.1.1</td>
<td>IP address assigned to ETH 0</td>
</tr>
<tr>
<td>Mask</td>
<td>255.255.255.0</td>
<td>Mask assigned to ETH 0</td>
</tr>
</tbody>
</table>
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:

![WAN interface configuration diagram](image)

**Figure 3: WAN interface configuration**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Plan / APN</td>
<td><code>&lt;APN&gt;</code></td>
<td>Enter the APN associated with the SIM</td>
</tr>
</tbody>
</table>
2.4 **Wi-Fi Access Point configuration**

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

In order to send data to and from this Wi-Fi interface, it must be bridged with at least one interface. This Wi-Fi interface is a member of Bridge instance 0 and therefore bridged to the following interfaces:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wi-Fi Node</td>
<td>1</td>
</tr>
<tr>
<td>Wi-Fi Node</td>
<td>2</td>
</tr>
<tr>
<td>Wi-Fi Node</td>
<td>3</td>
</tr>
<tr>
<td>Ethernet</td>
<td>0</td>
</tr>
</tbody>
</table>

- **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**

**WPA-802.1X Settings**

- **WPA Encryption**: 
  - TKIP
  - AES (CCMP)
- **Radius NAS ID**: BAY24
- **Radius Server IP Address**: 192.168.1.150
- **Radius Server Password**: 
- **Confirm Radius Server Password**: 

**Network Scanning**

Figure 4: Wi-Fi Access Point configuration
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable this Wi-Fi interface</td>
<td>Ticked</td>
<td>Tick to enable the Wi-Fi interface</td>
</tr>
<tr>
<td>Description</td>
<td>BAY Access</td>
<td>Enter text to describe this interface (in this example “BAY Access” is used)</td>
</tr>
<tr>
<td>SSID</td>
<td>BAY_Access</td>
<td>Enter a name that will be seen by clients and will identify the Wi-Fi network</td>
</tr>
<tr>
<td>Use the following security on this Wi-Fi interface</td>
<td>WPA-802.1X</td>
<td>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</td>
</tr>
<tr>
<td>WPA Encryption</td>
<td>TKIP</td>
<td>Select the appropriate encryption type. (AES (CCMP) was added for WPA2.)</td>
</tr>
<tr>
<td>Radius NAS ID</td>
<td>BAY24</td>
<td>Enter the NAS ID configured into the Radius server (in this example “BAY 24” is used)</td>
</tr>
<tr>
<td>Radius Server IP Address</td>
<td>192.168.1.150</td>
<td>Enter the IP Address of the Radius Server (in this example “192.168.1.150” is used)</td>
</tr>
<tr>
<td>Radius Server Password</td>
<td>digitest</td>
<td>Enter the shared key that is used to authenticate requests from this NAS to the Radius server (in this example “digitest” is used)</td>
</tr>
<tr>
<td>Confirm Radius Server Password</td>
<td>digitest</td>
<td>Confirm the shared key that is used to authenticate requests from this NAS to the Radius server (in this example “digitest” is used)</td>
</tr>
</tbody>
</table>

### 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](image)

**Figure 5: Set DHCP to “Wi-Fi only”**
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](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](image)
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**

![Figure 7: Populate profile parameters](image_1.png)

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

![Figure 8: View / amend profile](image_2.png)
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

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:

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

![Create remote user account](image)

**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:

![Export remote user certificate](image)

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

Figure 13: Create authorized client
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**:

![Location and security settings](image1)

• Select **Install encrypted certificates**:

![Install encrypted certificates settings](image2)

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:

![Image of Wi-Fi settings on an Android phone]

- 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:

![Image of Wi-Fi settings on an Android phone]

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](image)

**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:

![Wi-Fi client connected](image)

**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 intra_off 5
lapb 3 mux_0710 ON
lapb 4 dtemode 0
lapb 4 dlc 1
lapb 4 intra_off 5
lapb 4 virt_async "mux0"
eth 4 mux_0710 ON
lapb 5 dtemode 0
lapb 5 dlc 2
lapb 5 intra_off 5
lapb 5 virt_async "mux1"
eth 5 mux_0710 ON
lapb 6 dtemode 0
lapb 6 dlc 3
lapb 6 intra_off 5
lapb 6 virt_async "mux2"
eth 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 phonenum "*98*1#"
ppp 1 IPAddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 use_modem 1
ppp 1 asdion 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_strl "+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 "+CGREQ=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 l1on 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 trents 1200
user 0 access 0
user 1 name "username"
user 1 epassword "KD51SVJDVVe="
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

<table>
<thead>
<tr>
<th>Component</th>
<th>Revision</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digi TransPort WR41-G1T1-WV1-XX(WR41v2) Ser#:164895</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Build Ver5.2.15.4.</td>
<td>Jun 22 2016 04:58:22</td>
<td>MW</td>
</tr>
<tr>
<td>ARM Bios Ver 6.75 v653 MHz B256-M256-F80-O100,0 MAC:00042d02841f</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Async Driver</td>
<td>1.19</td>
<td>Int clk</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>2.0</td>
<td></td>
</tr>
<tr>
<td>Ethernet Driver</td>
<td>1.11</td>
<td></td>
</tr>
<tr>
<td>Firewall</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>EventEdit</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>Timer Module</td>
<td>1.1</td>
<td></td>
</tr>
<tr>
<td>(B)USBHOST</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>L2TP</td>
<td>1.10</td>
<td></td>
</tr>
<tr>
<td>PPTP</td>
<td>1.00</td>
<td></td>
</tr>
<tr>
<td>TACPLUS</td>
<td>1.00</td>
<td></td>
</tr>
<tr>
<td>MODBUS</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>RealPort</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>MultiTX</td>
<td>1.00</td>
<td></td>
</tr>
<tr>
<td>LAPB</td>
<td>1.12</td>
<td></td>
</tr>
<tr>
<td>X25 Layer</td>
<td>1.19</td>
<td></td>
</tr>
<tr>
<td>MACRO</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>PAD</td>
<td>1.4</td>
<td></td>
</tr>
<tr>
<td>V120</td>
<td>1.16</td>
<td></td>
</tr>
<tr>
<td>TFAD Interface</td>
<td>1.12</td>
<td></td>
</tr>
<tr>
<td>GPS</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>SCRIBATS</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>BASTSK</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>PYTHON</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>ARM Sync Driver</td>
<td>1.18</td>
<td></td>
</tr>
<tr>
<td>TCP (HASH mode)</td>
<td>1.14</td>
<td></td>
</tr>
<tr>
<td>TCP Utils</td>
<td>1.13</td>
<td></td>
</tr>
<tr>
<td>PPP</td>
<td>1.19</td>
<td></td>
</tr>
<tr>
<td>WEB</td>
<td>1.5</td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td>1.1</td>
<td></td>
</tr>
<tr>
<td>FTP Client</td>
<td>1.5</td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td>1.4</td>
<td></td>
</tr>
<tr>
<td>IKE</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>PollANS</td>
<td>1.2</td>
<td></td>
</tr>
<tr>
<td>PPPPOE</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>BRIDGE</td>
<td>1.1</td>
<td></td>
</tr>
<tr>
<td>MODEM CC (Siemens MC75)</td>
<td>1.4</td>
<td></td>
</tr>
<tr>
<td>FLASH Write</td>
<td>1.2</td>
<td></td>
</tr>
<tr>
<td>Command Interpreter</td>
<td>1.38</td>
<td></td>
</tr>
<tr>
<td>SSLCLI</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>OSPF</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>BGP</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>QOS</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>FWRCTRL</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>RADIUS Client</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>SSH Server</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>SCP</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>CERT</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>LowPrio</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>Tunnel</td>
<td>1.2</td>
<td></td>
</tr>
<tr>
<td>OVPN</td>
<td>1.2</td>
<td></td>
</tr>
<tr>
<td>QDL</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>WiMax</td>
<td>1.0</td>
<td></td>
</tr>
<tr>
<td>iDigi</td>
<td>2.0</td>
<td></td>
</tr>
</tbody>
</table>