Application Note 56

Hotspot feature for Wi-Fi clients with RADIUS User Authentication on Digi TransPort.

Digi Support
November 2015
6.1 Checking Wi-Fi connection status ................................................................. 23
  6.1.1 Web GUI ................................................................................................. 23
  6.1.2 Command Line (CLI) ................................................................. 24
The command wificonn will display all the Wi-Fi clients connected and their status ........ 24
The command dhcp 12 status will display the DHCP Server status of Interface ETH 12 ....... 24

The command wificonn will display all the Wi-Fi clients connected and their status.
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1.3</td>
<td>Checking RADIUS Authentication logs</td>
<td>24</td>
</tr>
<tr>
<td>7</td>
<td>Configuration files</td>
<td>25</td>
</tr>
<tr>
<td>8</td>
<td>Customization</td>
<td>28</td>
</tr>
<tr>
<td>8.1</td>
<td>Configure Splashpage for WI-FI Hotspot</td>
<td>28</td>
</tr>
<tr>
<td>8.2</td>
<td>Change the image file</td>
<td>31</td>
</tr>
<tr>
<td>8.3</td>
<td>Load new splashpage and images onto the TransPort</td>
<td>31</td>
</tr>
<tr>
<td>9</td>
<td>Splashpage example file</td>
<td>33</td>
</tr>
</tbody>
</table>
This document describes how to configure a Digi TransPort as a Wi-Fi Hotspot Access Point and Radius authentication to provide Wi-Fi clients with Internet access through Cellular.

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.

This application note applies only to:

**Model:** DIGI TransPort WR41/44 with the Wi-Fi option.

**Firmware versions:** 5169 and later

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

**Please note:** This application note has been specifically rewritten for firmware release 5169 and later and will not work on earlier versions of firmware. Please contact tech.support@digi.com if your require assistance in upgrading the firmware of the TransPort router.

1.3 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.
3 CONFIGURATION

3.1 Mobile Interface Configuration

Configuration – Network > Interfaces > Mobile > Mobile Settings

Configure the Mobile settings for the SIM card to provide cellular connection to the Digi TransPort and allow Wi-Fi clients to have internet access through it.

![Configuration interface screenshot]
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIM</td>
<td>1(PPP1)</td>
<td>SIM card slot where the SIM card is inserted</td>
</tr>
<tr>
<td>APN</td>
<td>Internet</td>
<td>APN associated with the SIM card</td>
</tr>
<tr>
<td>SIM PIN</td>
<td>****</td>
<td>SIM PIN if there is one configured, else, leave blank.</td>
</tr>
<tr>
<td>Confirm SIM PIN</td>
<td>****</td>
<td>Confirm the SIM PIN if there is one configured, else, leave blank.</td>
</tr>
<tr>
<td>Username</td>
<td>User</td>
<td>Username for the configured APN. If not required, leave blank.</td>
</tr>
<tr>
<td>Password</td>
<td>****</td>
<td>Password for configured APN username. If not required, leave blank.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>****</td>
<td>Confirm password for configured APN username. If not required, leave blank.</td>
</tr>
<tr>
<td>Enable NAT on this Interface</td>
<td>Checked</td>
<td>Enable NAT on the PPP1 interface (IP Address is sufficient for most configuration)</td>
</tr>
</tbody>
</table>

Click **Apply** and **Save** to save the settings.

### 3.2 Ethernet Interface Configuration

#### 3.2.1 ETH 0 Configuration

Configuration – Network > Interfaces > Ethernet > ETH 0

![Image of ETH 0 configuration](image)

<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 of the Router’s ETH 0 interface</td>
</tr>
<tr>
<td>Mask</td>
<td>255.255.255.0</td>
<td>Subnet Mask of the Router’s ETH 0 interface</td>
</tr>
</tbody>
</table>
3.2.2 ETH 12 Logical Interface Configuration

Logical Interface Ethernet 12 will be used for Wi-Fi clients.

Configuration – Network > Interfaces > Ethernet > ETH 12

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>10.10.10.1</td>
<td>IP Address of the Router’s ETH 12 logical interface</td>
</tr>
<tr>
<td>Mask</td>
<td>255.255.255.0</td>
<td>Subnet Mask of the Router’s ETH 12 logical interface</td>
</tr>
</tbody>
</table>

Configuration – Network > Interfaces > Ethernet > ETH 12 > Advanced

Configure the port to « Port Isolate mode »

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch to Port Isolate mode</td>
<td>Click</td>
<td>In Port Isolate mode the router will only respond to its Ethernet IP address on physical port. This port will be bridged to the Wi-Fi instance.</td>
</tr>
</tbody>
</table>

Click Apply and Save to save the settings.

You must reboot for this change to take effect
3.3 DHCP “Wi-Fi Only” Configuration for ETH 12

In this example, the Digi TransPort router will have a dedicated DHCP server for Wi-Fi clients only.

Configuration – Network > DHCP Server > Logical Ethernet Interfaces > DHCP Server for Ethernet 12
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable DHCP Server</td>
<td>Checked</td>
<td>Enable DHCP Server for this interface</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>10.10.10.100 – 10.10.10.200</td>
<td>Start and End of DHCP Range</td>
</tr>
<tr>
<td>Mask</td>
<td>255.255.255.0</td>
<td>DHCP Server Subnet mask for this interface. This must match the settings of Ethernet 12</td>
</tr>
<tr>
<td>Gateway</td>
<td>10.10.10.1</td>
<td>Gateway address. This must match ETH 12 address</td>
</tr>
<tr>
<td>DNS Server</td>
<td>10.10.10.1</td>
<td>Primary DNS Server, by default the TransPort will act as a DNS Server. This must match ETH 12 Address.</td>
</tr>
<tr>
<td>Secondary DNS Server</td>
<td>8.8.8.8</td>
<td>Set a Secondary DNS Server if required (in this example, Google’s public DNS Server)</td>
</tr>
<tr>
<td>Domain Name</td>
<td>*</td>
<td>Set the domain name to be used by the Wi-Fi clients.</td>
</tr>
<tr>
<td>Only send offers to Wi-Fi clients</td>
<td>Checked</td>
<td>Select this option to only send DHCP offers on this interface to Wi-Fi clients.</td>
</tr>
</tbody>
</table>

3.4 Wi-Fi Interface Configuration

3.4.1 Wi-Fi Global Settings Configuration

Configuration – Network > Interfaces > Wi-Fi > Global Wi-Fi Settings
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
<td>&lt;Chose&gt;</td>
<td>Select the Country where the device is used</td>
</tr>
<tr>
<td>Remote management access</td>
<td>Disable management</td>
<td>Do not allow Wi-Fi clients to log into the device and manage it</td>
</tr>
<tr>
<td>Network Mode</td>
<td>B/G/N</td>
<td>Chose which network mode to use</td>
</tr>
<tr>
<td>Channel</td>
<td>Auto</td>
<td>Let the router chose the best channel to use</td>
</tr>
<tr>
<td>Antenna</td>
<td>Auto</td>
<td>Use both Antennas for Wi-Fi</td>
</tr>
</tbody>
</table>

### 3.4.2 Wi-Fi Node 0 Configuration

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

![Wi-Fi Node 0 - Transport Hotspot](attachment:wi-fi-node-0.png)

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

- Ethernet 12
- Ethernet

Click here to assign a timeband to this interface.

**Wi-Fi Security**

Use the following security on this Wi-Fi interface:

- None
- WEP
- WPA-PSK
- WPA2-PSK
- WPA-802.1X
- WPA2-802.1X

Click Apply
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable this Wi-Fi interface</td>
<td>Checked</td>
<td>Enable Wi-Fi Node 0 interface</td>
</tr>
<tr>
<td>Description</td>
<td>TransPort Hotspot</td>
<td>Enter a description for this interface</td>
</tr>
<tr>
<td>SSID</td>
<td>Hotspot</td>
<td>SSID used for the hotspot and for clients to connect</td>
</tr>
<tr>
<td>Mode</td>
<td>Access Point</td>
<td>Wi-Fi mode for this interface</td>
</tr>
<tr>
<td>This Wi-Fi interface is a member of Bridge instance</td>
<td>1</td>
<td>Select the Bridge Instance 1 which contains Ethernet 12</td>
</tr>
<tr>
<td>Interface</td>
<td>Ethernet 12</td>
<td>Bridge this Wi-Fi interface with Ethernet 12</td>
</tr>
<tr>
<td>Enable station isolation</td>
<td>Checked</td>
<td>Station isolation will prevent wi-fi clients connected on the hotspot to communicate and be isolated.</td>
</tr>
</tbody>
</table>

Click **Apply** and **Save** to save the settings.

### 3.4.3 RADIUS Client Configuration

**Configuration – Security > RADIUS > RADIUS Client**

![RADIUS Client Configuration](image)

RADIUS can be used to authenticate remote command, SSH, FTP and Web sessions. You can configure two servers. The secondary server is used if there is no response from the primary server. Local authentication can be used if there is no response from the configured servers. RADIUS accounting can be used to log authentication attempts.

**Primary Authorization Server**

- **Hostname**: 192.168.1.75
- **NAS ID**: ZSHELL
- **Password**: 
- **Confirm Password**: 

11
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>192.168.1.75</td>
<td>Enter the IP Address used for the ZeroShell RADIUS server (in this example 192.168.1.75)</td>
</tr>
<tr>
<td>NAS ID</td>
<td>ZSHELL</td>
<td>Enter the NAS ID configured into the Radius server (in this example “ZSHELL” is used)</td>
</tr>
<tr>
<td>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 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>

Click **Apply** and **Save** to save the settings.

### 3.4.4 Wi-Fi Hotspot Configuration

Configuration – Network > Interfaces > Wi-Fi > Global Wi-Fi Settings > Wi-Fi Hotspot
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Wi-Fi Hotspot on Wi-Fi Node 0</td>
<td>DNS Redirect Mode</td>
<td><strong>DNS Redirect Mode</strong> will result in the Transport intercepting any DNS queries and return its own address instead of the real address. <strong>HTTP Redirect Mode</strong> will authorise DNS queries to external server but web requests will be redirected to the router hotspot page prior to allow general network access.</td>
</tr>
<tr>
<td>Splashscreen filename</td>
<td>hs_login.asp</td>
<td>User Authentication Splashscreen web page file name to be used when clients connects the first time.</td>
</tr>
<tr>
<td>Each client can connect for</td>
<td>1 hrs</td>
<td>Time to allow clients to connect to before forcing a reconnection</td>
</tr>
<tr>
<td>Require Wi-Fi Client Authentication</td>
<td>Checked</td>
<td>Turn ON Wi-Fi client authentication to the ZeroShell Radius server</td>
</tr>
<tr>
<td>Use RADIUS instance</td>
<td>5</td>
<td>Use RADIUS instance 5 configuration</td>
</tr>
<tr>
<td>Hostname</td>
<td><a href="http://www.digi.com">www.digi.com</a></td>
<td>Optional : Allow domains exceptions (up to 4) that you wish to provide unrestricted access to (Clients connected and visiting this domain will not be required to accept the terms or authenticate on the hotspot splash screen page)</td>
</tr>
</tbody>
</table>

Click **Apply** and **Save** to save the settings.
RADIUS SERVER CONFIGURATION

4.1 Configuration overview

In this Application note, the ZeroShell Linux distribution (can be booted from live CD, USB or VMWare) will be used to configure a Radius server for WPA Authentication of the Wi-Fi Hotspot clients.

The latest version of ZeroShell can be downloaded from: http://www.zeroshell.org/download/

Steps 4.2 to 4.4 will go through downloading, booting and configuring ZeroShell

Steps 4.5 to 4.8 will go through Radius configuration and generally apply to any Radius server.

4.2 Create ZeroShell live CD

Download the latest version of ZeroShell from the web site above. There are number of versions available. The “ISO image for CD” version 3.1.0 booted under VMWare was used for this Application Note.

It is also possible to create a CD containing this image using the appropriate CD-burning software such as http://cdburnerxp.se/en/home.

When the CD has been created, choose an appropriate computer to act as the Radius server (not the one used to test the Wi-Fi hotspot) and boot it from the CD (it may be necessary to change the computer’s boot sequence to allow booting from the CD). ZeroShell does not require an especially fast computer, an old laptop or desktop machine can be used for this test.

4.3 Configure ZeroShell network settings

Once ZeroShell server has booted, a command line interface prompt is used to configure the IP address, mask, gateway and setting 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 192.168.1.75 was used for the server address: IP [192.168.1.1]: 192.168.1.75
- 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 be now possible to open a web browser and navigate to https://192.168.1.75 in order to configure the ZeroShell server via its web interface. Log in using the username admin and the admin password that was configured via the command line interface previously.

4.4 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 the VMWare local hard disk (ext4-formatted) 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:

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

4.5 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** from the top menu
- 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
A prompt will be seen warning that existing certificates will be deleted. Click **OK** to proceed.

### 4.6 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 ZeroShell server will now provide the option to export the user certificate – please see section 4.7 below.

**Export remote user certificate**

This example uses a Windows laptop as the remote access client, so it is necessary to export the user certificate using the “.pfx” format so that it can be imported in the Windows Certificate Management.

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:
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 in Windows, the password will need to be entered to allow the certificate to be installed.

4.8 Export Trusted CA certificate

- Select RADIUS
- Select Trusted CAs
- In the Trusted CAs list, click on the Hotspot entry
- Click the Export button
- Save the file to a location on the computer

Create authorized client
It is necessary to 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 accomplished 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 **ZSHELL** 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
5 CONNECT TO THE WI-FI HOTSPOT

Under Windows 7/8, Right Click on the Wi-Fi icon in the task bar

This should bring the Wireless network Connection menu. The "Hotspot" SSID should appear with "No Security". Select it and click Connect to connect to the Hotspot.
Opening a web browser to one of the Hotspot’s exceptions will display the page directly (like http://www.digi.com in our example)

However, opening a web browser to any other domain will prompt the user to login (using the previously created digi_test_user on the RADIUS server) and accept terms and conditions from the standard hs_login.asp page. This page can be customized or replaced by another page of your choosing and selected like shown in section 3.4.3

Upon clicking on Login, the web page will redirect to the right site.
6 TESTING

6.1 Checking Wi-Fi connection status

6.1.1 Web GUI

You can check the number of connected clients and their status on the Wi-Fi management page.

Management – Network Status > Interfaces > Wi-Fi

You can also check the DHCP status for clients under the DHCP Status page
6.1.2 Command Line (CLI)

The command `wificonn` will display all the Wi-Fi clients connected and their status:

Number of connected clients: 1
Number of client mode connections: 0

1 Node 8c:70:8c:70:8c:70
  Wi-Fi node : 0
  RSSI       : 42
  Flags      : ERP
  Power Save : Awake
  Mode       : N
  Neg. Rates : 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 Mbps
  TX Rate    : 117.0 Mbps
  RX Rate    : 130.0 Mbps
  Cap. Info  : ESS Short_Preamble Short_Slottime
  HT Cap.    : GREENFIELD SHORTGI20 RXSTBC(1) AMSDU(7935)
  Channel    : 1

OK

The command `dhcpl2 status` will display the DHCP Server status of Interface ETH 12:

<table>
<thead>
<tr>
<th>Entry: IP</th>
<th>hostname</th>
<th>MAC</th>
<th>expiry</th>
</tr>
</thead>
<tbody>
<tr>
<td>[10.10.10.100]</td>
<td>[DOR]</td>
<td>[8c:70:8c:70:8c:70]</td>
<td>20143 mins</td>
</tr>
</tbody>
</table>

OK

Checking RADIUS Authentication logs

Under: System, click on Logs.

You should be able to see this entry after a user has entered their login and password on the Splashpage:

01:01:18 Login OK: [digi_test_user] (from client ZSHELL port 0 via TLS tunnel)
01:01:18 Login OK: [digi_test_user] (from client ZSHELL port 0)
Digi TransPort WR44v2

```
wifi 0 country "France"
wifi 0 chanmode "bgn"
wifi 0 hotspot_f__name "hs_login.asp"
wifi 0 hotspot_lifetime 60
wifi 0 hotspot_auth ON
wifi 0 hotspot_radiuscfg 5
wifi 0 nocfg 1
wifinode 0 descr "TransPort Hotspot"
wifinode 0 ssid "Hotspot"
wifinode 0 hotspot 2
wifinode 0 isolation ON
wifinode 0 bridge_inst 1
eth 0 IPaddr "192.168.1.44"
eth 0 DNSserver "192.168.1.1"
eth 0 gateway "192.168.1.1"
eth 0 do_nat 2
eth 0 bridge ON
eth 12 IPaddr "10.10.10.1"
eth 12 do_nat 2
eth 12 bridge ON
eth 12 bridge_inst 1
eth 12 ipanon ON
eth 12 physadd -1
addp 0 enable ON
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 3 dtemode 0
lapb 4 dtemode 0
lapb 5 dtemode 0
lapb 6 dtemode 0
gps 0 asy_add 1
gps 0 gpson ON
ip 0 cidr ON
def_route 0 ll
hshosts 0 host "www.digi.com"
dhcp 0 respdelims 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "
dhcp 12 IPmin "10.10.10.100"
dhcp 12 IPrange 101
dhcp 12 lease 60
dhcp 12 wifionly ON
dhcp 12 mask "255.255.255.0"
dhcp 12 gateway "10.10.10.1"
dhcp 12 DNS "10.10.10.1"
sntp 0 server "time.etherios.com"
ppp 0 timeout 300
ppp 1 name "W-WAN"
p
ppp 1 phonenumber "*98*3#"
ppp 1 username "username"
ppp 1 epassword "KD5lSVJDVVg="
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
```
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 name "DSL"
ppp 3 l1iface "AAL"
ppp 3 username "Enter ADSL Username"
ppp 3 r_addr OFF
ppp 3 IPAddr "0.0.0.0"
ppp 3 l_addr ON
ppp 3 timeout 0
ppp 3 do_nat 2
ppp 3 aodion 1
ppp 3 autoassert 1
ppp 3 immoos ON
ppp 3 echo 10
ppp 3 echodropcnt 5
ppp 3 l_pap OFF
ppp 3 l_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
web 0 prelogin_info ON
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
ana 0 anon ON
ana 0 l2on OFF
ana 0 xoton OFF
ana 0 lapdon 0
ana 0 lapbon 0
ana 0 logsize 45
cmd 0 unitid "ss%" >
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 asyled_mode 2
cmd 0 tremto 1200
cmd 0 rcihttp ON
cmd 1 autocmd "ats31=7"
cmd 1 gpson ON
cmd 4 cmd_processor OFF
user 0 access 0
user 1 name "username"
user 1 epassword "KD5lSVJDVg="
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 "priv
radcli 5 nasid "ZSHELL"
radcli 5 server "192.168.1.75"
radcli 5 epassword "PDZxU1FJVEg=
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
cloud 0 ssl ON
This section describes how to create your own “Splash-screen” or “disclaimer” page on Digi TransPort Wi-Fi routers, and how to add your own graphics to the page. This “Splash-screen” page is shown when Wi-Fi users first access the Internet or external websites. A timer can be set so that users must “re-authenticate” via this page when the timer expires.

Refer to the Digi TransPort User Guide and Application Notes posted on www.digi.com/support for full details.

8.1 Configure Splashpage for WI-FI Hotspot

Download the sample hs_login.asp file. Go to Administration-File Management>WEB Directory.

Scroll down until you find the file hs_login.asp. Click on it and scroll up until you see the default splashpage. Right click anywhere in that image and choose ‘View Source’.
A new window will pop up (either an html editor if you have one or a web browser if you don’t).

Save that file as a .asp file (example: DigiSpl.asp).

NOTE: Digi TransPort file system file names must be 12 characters or less (including the “.”); typically in 8.3 format.
Reopen the .asp file either with an html editor (Notepad works fine). At about line 34 you’ll see this line: `<input name="cky" value="0" type="hidden">`. This needs to be changed to: `<input name="cky" value="<%write(cky);%>" type="hidden">`.

Save the file. You now have a working file that can be manipulated anyway you need.
You can now make changes to the file as needed; i.e. the disclaimer or any GIF or JPG images that you want to add. Keep in mind that all files need to be in the 8.3 format, so any files added must be named with 12 characters or less (example: image.gif).

### 8.2 Change the image file

**NOTE:** Graphic types **gif** and **jpg** are supported. Other file types (e.g. png) are NOT supported. (Exceptions for gifs and jpgs are made to allow them to be accessed from the TransPort’s Web server if the user has not logged in to the TransPort itself.)

The hotspot.asp file contains the line `'<td colspan="3" rowspan="1"><img alt="Digi International" src="/images/logo.gif"></td>'`. Rename logo.gif as needed to the filename of the new gif file you created. Also, remove “/images" from address since the logo.gif is stored in the main (root) flash directory (see the example below). This is the only change to hotspot.asp needed for the images to be displayed.

### 8.3 Load new splashpage and images onto the TransPort

Use FileZilla or other ftp client to copy the files onto the TransPort. Windows Explorer (not Internet Explorer) works via `ftp://192.168.1.1` (assuming the Transport’s LAN IP address is 192.168.1.1). You will be prompted to login to the TransPort (username and password). Drag and drop your new file (and the gif file(s) you’ve created) directly into the TransPort file system. They will be listed in the default (flash) directory.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>

31
<table>
<thead>
<tr>
<th>Host</th>
<th>192.168.1.23</th>
<th>IP Address of the TransPort router</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>username</td>
<td>Username with Access Level : Super to log in to the TransPort router (default : username)</td>
</tr>
<tr>
<td>Password</td>
<td>password</td>
<td>Password for the user with Access Level : Super to log in to the TransPort router (default : password)</td>
</tr>
<tr>
<td>Port</td>
<td>21</td>
<td>Default FTP port.</td>
</tr>
<tr>
<td>DigiSpl.asp</td>
<td>-</td>
<td>Splashpage file</td>
</tr>
<tr>
<td>logo.gif</td>
<td>-</td>
<td>Image file</td>
</tr>
</tbody>
</table>

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

Select the drop down window called **Splashscreen filename**. Drop it down and the .asp file you loaded should appear (a reboot may be necessary if the file does not appear). Click the **HTTP Redirect Mode** or **DNS Redirect Mode** button for the appropriate Wi-Fi node on which the splashpage will appear.

**Apply** and **Save** configuration.

The Wi-Fi user should now be presented with the new page.
Bold characters are the changes made from the default hotspot.asp page.

```html
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<meta content="0" http-equiv="Expires">
<meta content="no-cache" http-equiv="Cache-Control">
<meta content="no-cache" http-equiv="Pragma">
<link type="text/css" href="style.css" rel="stylesheet">
<title>Digi TransPort Terms and Conditions</title>
<script language="javascript">
var params = new Array();

function getUrlVars() {
    var vars = {}; 
    var parts = window.location.href.replace(/\[?&\]+([^=&\]+)=([^&]*)/gi,
    function(m,key,value) {
        vars[key] = unescape(value);
    });
    return vars;
}

params = getUrlVars (window.location.href);

if( params["login_failure"] == undefined )
{
    params["login_failure"] = "0";
}
</script>
</head>
<body>
<form name="hotspot" action="/goform/hotspot" method="post">
<!--
<input type="hidden" name="hotspot_url" value="http://www.digi.com">
-->
<input name="cky" value="<%write(cky);%>" type="hidden">
</div>
<table style="width:100%;" border="0" cellpadding="2" cellspacing="2">
<tbody>
<tr align="center">
<td><img alt="Digi International" src="/images/beer.gif"></td>
</tr>
<tr>
<td rowspan="1"></td>
</tr>
<tr align="center">
<td colspan="3" rowspan="1">
Welcome to our Bus! <br>
If you drink then don't drive! Get home safe with us!! <br>
<br>
<br>
<br>
<br>
<br>
<br>
<br>
<br>
<br>
</td>
</tr>
</tbody>
</table>
</form>
</body>
</html>
```
<table align=center border="0" cellpadding="2" cellspacing="2">
<tbody>
<tr><td rowspan="1"></td></tr>
<tr><td colspan="2" style="text-align: center;">
<input name="accept" value="Accept" type="hidden">
<input name="saccept" size="20" value="Login" onclick="hotspot.accept.value='Accept'" type="submit">
</td></tr></tbody></table>

Copyright &copy; Digi International Inc. All rights reserved.

</div>
</form>
</body>
</html>