TransPort Training Program

TT007 – TransPort Wi-Fi

Wi-Fi Access Point, Client and Hotspot Configuration

Wi-Fi is 802.11 Standards

- **All standards defined and maintained by IEEE**
  - Institute of Electrical and Electronics Engineers
- **802.11**
  - Approved in July 1997
  - 2.4GHz
- **802.11b**
  - Approved in September 1999
  - 2.4GHz
- **802.11a**
  - Approved in September 1999
  - 5.0GHz
- **802.11g**
  - Approved in June 2003
  - 2.4GHz
- **802.11n**
  - Approved in September 2009
  - 2.4GHz
  - 5.0GHz

2.4 GHz Channel Restrictions

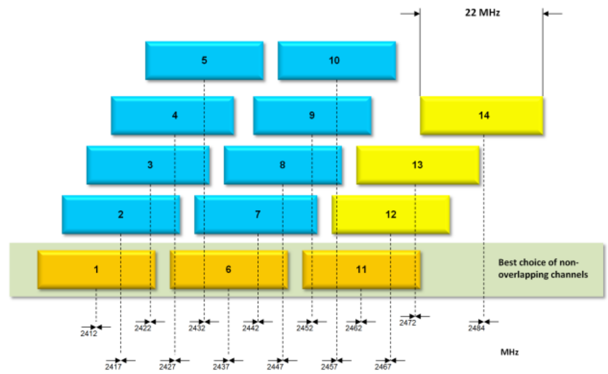
- Always select correct country
- 802.11 b/g/n (2.4 GHz)
  - Some channels are restricted in some countries
  - Channel 1,6,11 are none overlapping
- 802.11 a/n (5 GHz)
- 802.11 n
  - 2 x 2 MIMO mode

2.4 GHz Channel Restrictions

Channel	USA/Canada	EU	Japan
1	●	●	●
2	●	●	●
3	●	●	●
4	●	●	●
5	●	●	●
6	●	●	●
7	●	●	●
8	●	●	●
9	●	●	●
10	●	●	●
11	●	●	●
12		●	●
13		●	●
14			●

2.4 GHz Channel Overlap

- Never configure neighboring access points using overlapping channels
  - Overlapping channels cause performance degradation
  - Interference applies horizontally (same floor) and vertically (different floors) depending on network layout and surrounding building materials
- Channels 1, 6, and 11 are the best choice
  - Allows avoiding interference problems with neighboring access point configurations
  - Maximizes available shared bandwidth across the wireless network by providing up to three separate channels with up to 25 Mbps each.



802.11b/g have overlapping channels

802.11n Overview

- Delivers performance increase of about fives times compared to existing 802.11a/b/g networks
  - MIMO (multiple-input, multiple-output), packet aggregation and channel bonding (20/40 MHz wide channel options)
  - Current devices support up to 300 Mbps
  - Standard allows for maximum of up to 600 Mbps
- Improved range and robustness characteristics
  - Standard supports 2.4 GHz and 5 GHz frequency bands
  - MIMO smart antenna technology also allows for more robustness with better range performance
  - Applies also to legacy devices connected to 802.11n MIMO access points – improvements of up to 30% for 802.11a/b/g devices
- Backwards-compatibility with legacy devices
- 12 non-overlapping 5 GHz channels

802.11 Standards Overview

	802.11	802.11b	802.11a	802.11g	802.11n
Max Data Rate	2 Mbps	11 Mbps	54 Mbps	54 Mbps	600 Mbps
Max Throughput (approx.)	1 Mbps	7 Mbps	25 Mbps	25 Mbps	420 Mbps
Frequency	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz	2.4 / 5 GHz
Channel Width	22 MHz	22 MHz	20 MHz	22 MHz	20/40 MHz
MIMO/SDM	No	No	No	No	Yes, up to 4x4:4
Modulation	Frequency Hoping Spread Spectrum (FHSS) Direct Sequence Spread Spectrum (DSSS)	Direct Sequence Spread Spectrum (DSSS)	Orthogonal Frequency Division Multiplexing (OFDM)	Orthogonal Frequency Division Multiplexing (OFDM) Direct Sequence Spread Spectrum (DSSS)	Orthogonal Frequency Division Multiplexing (OFDM) Direct Sequence Spread Spectrum (DSSS)
Legacy Interoperability	802.11b/g	802.11/802.11g	None	802.11/802.11b	802.11a/b/g

Current TransPort Wi-Fi Modules

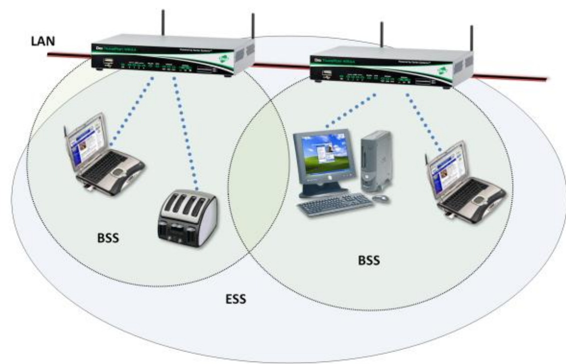
- Wi-Fi Modules
  - WR41v2 A/B/G/N (SparkLAN WUBR-507N)
  - WR44v2 A/B/G/N (Compex WLE200NX)
  - WR44v2 Dual A/B/G/N (Compex WLE200NX) * 2

This slide shows the Wifi Modules

TransPort Wi-Fi Operating Modes

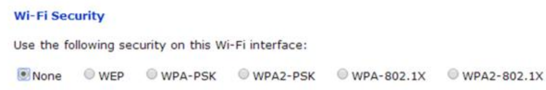
- Infrastructure mode is supported
- Adhoc mode is **not** supported.
- TransPort routers can be configured as an Access Point or a client.
- Basic Hotspot – Captive Portal Redirector
- Rouge AP Detection (WR44 only)
- Client and AP at same time - but same channel must be used for both on a single module router.
- Multiple SSID support

Infrastructure Mode:



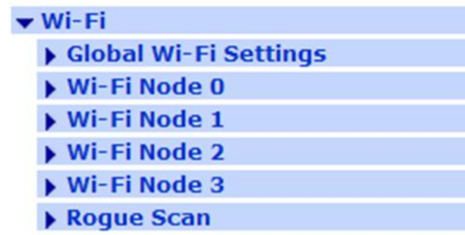
Security

- Support Encryption Algorithms
  - AES
  - TKIP
- Supported Authentication Methods
  - Open
    - No Security
  - WEP
    - Very Insecure
  - WPA
    - Good Security
  - WPA2
    - Better Security
  - Radius (802.1x) authentication
    - Normally used on corporate networks
    - Requires a username (Identity) as well as a password



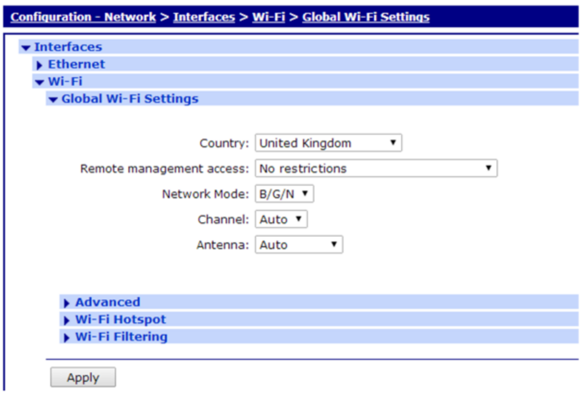
Wi-Fi Configuration Section

- Global Settings
- Wi-Fi Nodes 0-3
- Rogue Scan (WR44)

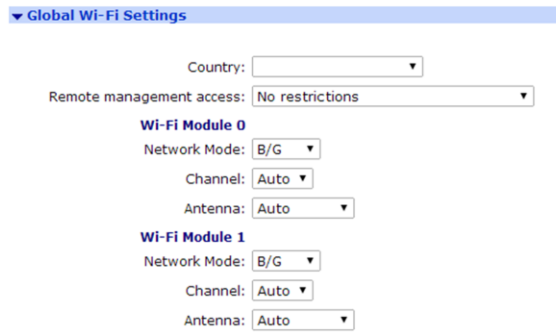


Global Settings

Single Wi-Fi Module:



Dual Wi-Fi Module:

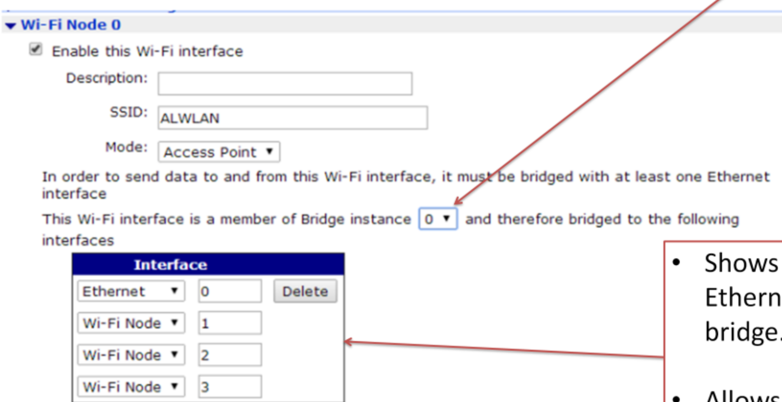


Access Point Configuration – Fundamentals.

- Access Point mode works by switching layer 2 frames between Wi-Fi and wired Ethernet networks.
- Linking networks together at layer 2 is called bridging.
  - Example of layer 3 packets are IP packets
  - Examples of layer 2 frames are ARP requests
- To configure AP mode:
  - Configure SSID and security settings into the Wif-Fi node
  - Ensure that Wi-Fi node and at least one Ethernet instance is a member of the bridge
  - If there is no DHCP server on the network already, configure the DHCP server with the same instance number as the Ethernet interface in the bridge.

Access Point Configuration - Bridging

Controls which bridge instance the –Wi-Fi node is a member of



- Shows other Wi-Fi nodes and Ethernet interfaces in the same bridge.
- Allows Ethernet interfaces to be added and removed from the bridge instance.

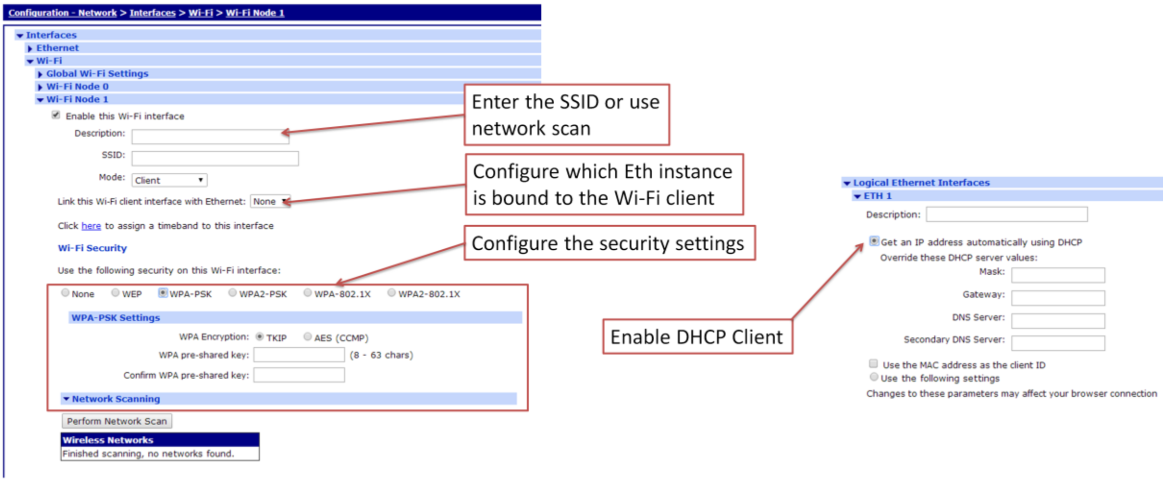
Multiple SSIDs

- To configure multiple SSIDs, configure multiple Wi-Fi Node instances.
- If the SSIDs are for the same back-end network, link them to the same bridge.
- If the SSIDs are for different layer 2 networks (e.g. different subnet) then multiple bridge instances and multiple Ethernet instances will be required.
- Note that routers with a single Wi-Fi module can only use one channel at once. This means all SSIDS must be on the same channel.
- Unlike some other (popular) access points, the Digi TransPort will ensure that different MAC addresses are used for each SSID. (Not to do so can cause problems with some clients.)

Client Configuration Fundamentals

- Wi-Fi Node must be configured for Client Mode
- Wi-Fi Client must be linked (NOT bridged) with an Eth instance.
- Normally the Eth instance needs to be configured as DHCP client (to obtain an IP address from the network).
- Bridging to Ethernet is not possible in client mode because a Wi-Fi client can only send frames from a single MAC address.
- Networking scanning option will auto populate SSID and encryption and authentication settings for you.
- Enter the key or password

Wi-Fi Client Configuration



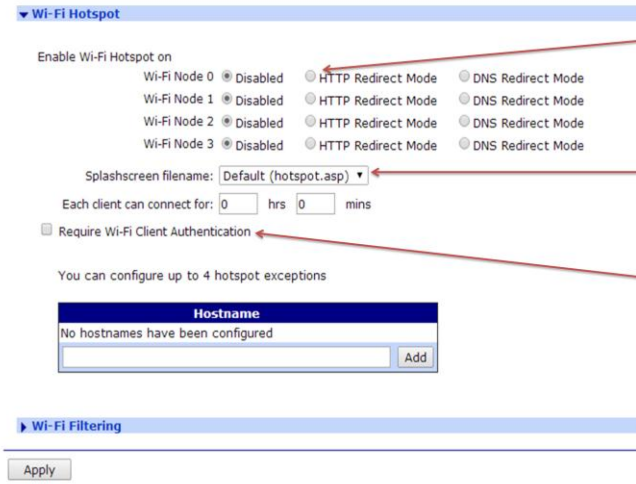
Wi-Fi Filtering

- Enable MAC based filtering
- Only allow pre-configured MAC addresses to connect
- Up to 64 MAC addresses can be configured

Hotspot

- Captive portal can use HTTP or DNS to redirect web traffic to local HTTP server splash screen. HTTP is the recommended method.
- Basic mode requires user agrees to terms and conditions in order to be granted Internet access.
- "Require Wi-Fi Client Authentication" mode requires user enters a username and password into a web form. These credentials are checked against a RADIUS server before allowing access. This allows a more sophisticated hotspot user management back end to be constructed.
- A captive portal in conjunction with a web page that requires the user to register and/or login is known as **UAM U**niversal **A**ccess **M**ethod.
- A number (currently 4) hostnames can be configured as exceptions. These addresses will not be re-directed to the HTTP splash screen. This is sometimes known as a "walled garden".

Hotspot Configuration Page



Select HTTP redirect for the Wi-Fi node to be the hotspot

Select the hotspot splash screen file, usually this must be edited.

If the users must enter a username and password to be checked against a RADIUS server, tick this box and ensure that the correct "Splash screen filename" is selected.

Hotspot .ASP file

- **A**ctive **S**erver **P**ages (**ASP**) are pages upon which the web server will execute code whilst serving.

- The ASP file cannot be download from the router in order to edit it, the web server will execute the code so you will not end up with the original file.

- Example hotspot ASP files can be found at the following location:

  http://ftp1.digi.com/support/firmware/transport/utils/hotspot/hotspot.zip

  - hotspot.asp requires acceptance of terms and conditions
  - hs_login.asp requires user login (via RADIUS)

- Edit the file to meet your requirements, then upload it to the root folder by the TransPort router's FTP server

```
    <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/logo.gif"></td>
        </tr>
        <tr>
          <td rowspan="1"></td>
        </tr>
        <tr align="center">
          <td>This is a sample Terms and Conditions page for the <br>
Digi TransPort Wi-Fi Hotspot functionality. <br>
This page can be used as a basis for a personalised Terms <br>
and Conditions page.<br>
You should create an ASP file which includes a button that performs<br>
the same "OnClick" action as the "Login" button on this page.<br>
You should then store your ASP page (and any images you may be using)<br>
on the flash directory of the TransPort device.<br>
You should then configure the Wi-Fi hotspot page to use your ASP file.<br><br>
          </td>
        </tr>
        <tr>
          <td rowspan="1"></td>
        </tr>
      </tbody>
    </table>
    <table align=center border="0" cellpadding="2" cellspacing="2">
      <tbody>
<script language="javascript">
        if( params["login_failure"] == "1" )
            {
            document.write( "<tr align='center'><td class='warning' colspan='2'>Login
            document.write( "<tr><td colspan='2'> </td></tr>" )
            }
</script>
        <tr align='center'>
            <td>
                Username:
            </td>
            <td>
                <input type="text" name="username">
            </td>
```

Hands-On Practical Session WIFI

HOPS Access Point

- Configure DHCP Server
- Configure Logical Interface
- Configure Wi-Fi Global
- Configure Wi-Fi Node

HOPS Client Mode

- Configure Logical Interface
- Configure Wi-Fi
- Configure Wi-Fi Node
- Configure Default routes

HOPS Wi-Fi Hotspot

- Upload a modified hotspot.asp file with your own message inside.
- Enable Basic Hotspot
- Testing