

Lab 8.5.4.2_BR1310 Configuring Site-to-Site Wireless Link using Enterprise Security

Estimated Time: 45 minutes

Number of Team Members: Students will work in teams of 2.

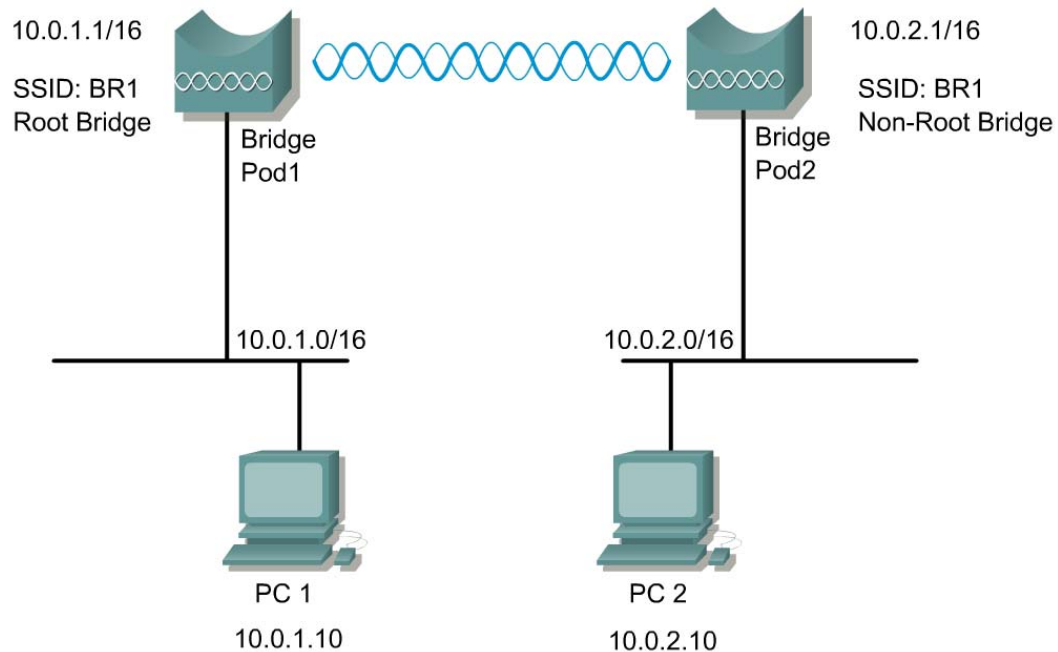
Objective

Configure a site-to-site bridged network using enterprise security features.

Scenario

A remote location located several miles away requires connectivity to the existing wired network. The connection can be bridged wirelessly with the use of two BR1310s. The company's security policy mandated a minimum of 128 bit WEP security for all wireless connections.

Topology



Preparation

In this lab, the following will be configured.

<u>Device Name</u>	<u>SSID</u>	<u>BVI Address</u>
BPod1	BR1	10.0.1.1/16
BPod2	BR1	10.0.2.1/16

Tools and Resources

Each team will require the following:

- Two wired LAN segments that will be bridged together
- Two Cisco BR1310
- PC with FTP server loaded and a file to transfer in the root directory of the FTP server

Step 1 Cable and power the bridge

- a. For each bridge, attach 2 rubber duck antennas to the RP-TNC connectors.
- b. Connect the power cable to the Power Injector and to a wall receptacle.

Step 2 Connect to the bridge and clear existing configurations

Connect a PC to the bridge power injector's serial port using a DB-9 to RJ-45 serial cable.

- a. Open a terminal emulator.
- b. Enter these settings for the connection:
 - Bits per second (baud rate): 9600
 - Data bits: 8
 - Parity: none
 - Stop bits: 1
 - Flow control: none
- c. Press **Return** to get started
- d. Enter privileged mode. **Cisco** is the default password.
- e. Turn off notification logging to avoid interruptions as you enter commands.

```
PodP#configure terminal
PodP(config)#logging console 4
```

- f. Erase the configuration with the following commands:

```
PodP#erase startup-config
Erasing the nvram filesystem will remove all files! Continue?
[confirm]          (press Enter)
[OK]
Erase of nvram: complete
PodP# reload
```

```
System configuration has been modified. Save? [yes/no]: N  
Proceed with reload? [confirm] (press Enter)
```

- g. After the system reboots, repeat the step to turn off notification logging.
- h. Assign an IP address and address mask to the BVI.

```
PodP(config)#interface bvi1  
PodP(config-if)#ip address 10.0.P.1 255.255.0.0
```

- i. Configure the PCs.
 - PC1 with an IP address of 10.0.1.10/16
 - PC2 with an IP address of 10.0.2.10/16

Step 3 Connect to the BR1310 through a web browser

- a. Connect an RJ-45 Ethernet cable to the Ethernet port on the bridge Power Injector. Connect the other end of the Ethernet cable to the wired network.
- b. Open a web browser, enter the bridge BVI address `http://10.0.P.1`, and press **Enter**.

Step 4 Configure the bridge settings

Configure the following settings from the **Express Set-Up** page:

<u>Parameter</u>	<u>BPod1</u>	<u>BPod2</u>
a. System Name:	BPod1	BPod2
b. Configuration Server Protocol:	Static IP	Static IP
c. IP address:	10.0.1.1	10.0.2.1
d. Subnet Mask:	255.255.0.0	255.255.0.0
e. Default Gateway:	10.0.1.254	10.0.1.254
f. Role in Radio Network:	Root	Non-Root

- g. Click **Apply** to save these changes.
- h. Navigate to the **Express Security** page and configure the SSID: **BR1**
- i. Verify the settings on both bridges. Navigate to the **Association** page to confirm that the bridges have associated.

Step 5 Test the connection

Verify client PCs are configured with the appropriate IP address. The only wireless devices in this topology will be the two wireless multi-function bridges used for the point-to-point connection.

- a. Once the wireless bridge link is configured properly, ping from PC1 to BPod2. Then ping from PC1 to PC2.
- b. If these pings are not successful, troubleshoot as necessary.
- c. Test layer 7 connectivity by browsing from PC1 to BPod2.
- d. Configure FTP or Web services on PC1 and PC2. Transfer a file from PC1 to PC2 and vice versa. Observe the download performance across the wireless link.
- e. What was the download speed in Mbps?

Step 6 Configure static WEP on both bridges

Follow these steps to set up WEP keys and enable WEP:

- a. From the **Security: Encryption Manager** page, click the radio button next to **WEP Encryption** and select **Mandatory** from the drop down list.
 - b. Select the radio button for **Encryption Key 1** in the Transmit Key column. Make sure that drop down list has **128-bit** selected for Key Size.
 - c. Click in the Encryption Key field and enter a WEP key. For a 128-bit encryption, the key will need to be 26 hexadecimal characters in length. Only the numbers 0-9 and the letters A-F can be used.
 - d. Record the key below.
-
- e. Click **Apply** to save the WEP Key.
 - f. Repeat the same steps on the other bridge.

Security: Encryption Manager

Encryption Modes

None

WEP Encryption Mandatory

Cisco Compliant TKIP Features: Enable MIC Enable Per Packet Keying

Cipher WEP 128 bit

Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input checked="" type="radio"/>	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	128 bit
Encryption Key 2:	<input type="radio"/>		128 bit
Encryption Key 3:	<input type="radio"/>		128 bit
Encryption Key 4:	<input type="radio"/>		128 bit

Step 7 Retest the connection

From either bridge, navigate to the **Association** page to view the status of the wireless link. If the bridges do not associate, troubleshoot the static WEP configuration.

- a. Once the wireless bridge link is functional, ping from PC1 to PC2 to test end-to-end connectivity.
- b. Repeat the FTP download process from PC1 to PC2. Observe the download performance across the wireless link.
- c. What was the download speed in Mbps? Did WEP have an impact on performance?

Step 8 Enable enterprise security

Once WEP is configured correctly, additional measures should be configured to secure the wireless link. Follow these steps to set up Per Packet Keying and MIC.

- From the **Encryption Manager** page, select the check boxes for the Cisco Compliant TKIP features.
- Click the **Apply** button. The wireless link will be lost with the other bridge.
- Configure the other bridge with the same security setting.
- The link should be re-established.

Security: Encryption Manager

Encryption Modes

None

WEP Encryption Mandatory

Cisco Compliant TKIP Features: Enable MIC Enable Per Packet Keying

Cipher WEP 128 bit

- What attack does TKIP prevent?

- View the Security Summary via the web browser for an overview of the security settings.

Security Summary

Administrators

Username	Read-Only	Read-Write
Cisco	✓	

Radio0-802.11G SSIDs

SSID	VLAN	Open	Shared	Network EAP
BR1	none	no addition		

Radio0-802.11G Encryption Settings

Encryption Mode	WEP		Cipher				Key Rotation
	MIC	PPK	TKIP	WEP40bit	WEP128bit	CKIP	
WEP-Mandatory	✓	✓					