Lab 6.2.2 Configuring Basic Bridge Settings

Estimated Time: 30 minutes

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

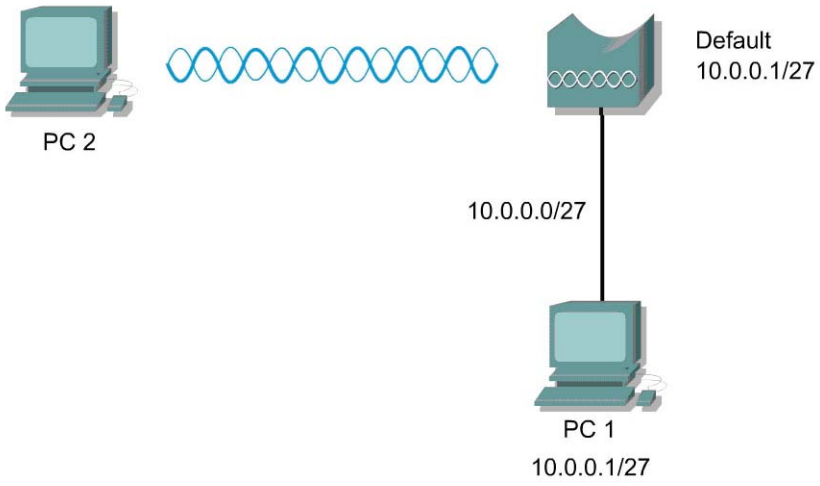
Objective

In this lab, the student will assign basic parameters to the bridge using the GUI and IOS CLI. The Express Setup and Express Security pages will also be accessed through a web browser to assign the IP address, subnet mask, default gateway, and SSID to the bridge.

Scenario

Basic configuration of a bridge can be done through the GUI or IOS CLI.

Topology



Preparation

The student PC should be connected to the bridge through an isolated wired network or crossover cable. The bridge should be set to factory defaults.

Tools and Resources

Each team will need:

- One bridge
- The bridge Power Injector
- A PC (PC1) that is connected to the same wired network as the bridge
- A wireless PC or laptop (PC2)

Command List

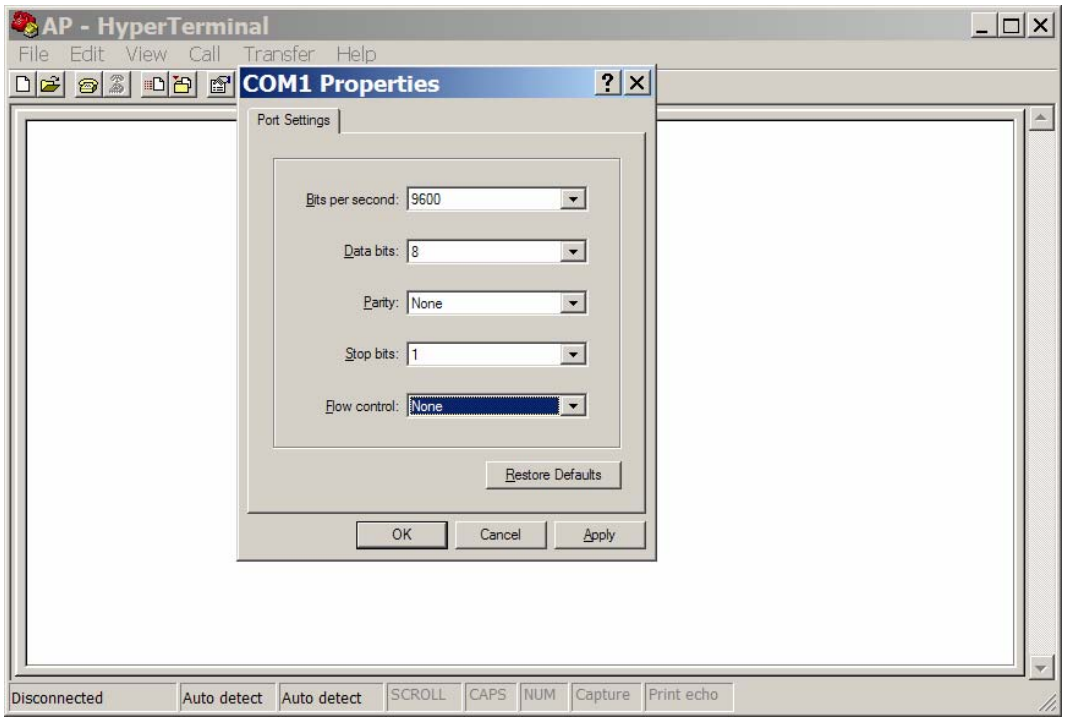
In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
configure terminal	Enter Global configuration mode
hostname	Set the hostname on the device
interface bvi1	Enter the virtual interface for the bridge
ip address	Set the IP address and subnet mask on the device
interface dot11radio 0	Enter the device radio interface
station role install | non-root | root [ap-only] | workgroup-bridge	Set the bridge role. Set the role to install, non-root, root or workgroup bridge. (Optional) If root mode is selected, the bridge can be used as a root bridge or a root AP. When set to ap-only mode, the fallback role of the radio can be selected as repeater or shutdown. If the Ethernet port of the bridge is disabled or disconnected from the wired LAN, the bridge can either shut down its radio port or become a repeater bridge associated to a nearby root bridge.
ssid ssid-string	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive. **Note:** Do not include spaces or underscore characters in SSIDs.
enable password *password*	The default password is Cisco. This commands allows an administrator to change the password
enable secret *password*	The default enable password is *Cisco*.
enable password level *level password*	The default is level 15 (privileged EXEC level). The password is encrypted before it is written to the configuration file.
show dot11 associations	View the associated wireless devices
show running-config	Display the current configuration of the device
show startup-config	Display the startup configuration of the device
copy running-config startup-config	Save the entries into the configuration file
show interfaces	Display interface information of the device
logging console 4	Turn off notification logging to avoid interruptions during configuration.

Step 1 Connect to the bridge using a console

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

b. Open a terminal emulator.



c. Enter these settings for the connection:

- Bits per second (baud rate): 9600
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: none

d. Press Return to get started

Step 2 Configure PC1

Make sure the bridge is connected to PC1 by way of a wired connection.

a. Configure the IP address, subnet mask, and gateway on PC1

1. IP address 10.0.0.2
2. Subnet Mask 255.255.255.224
3. Gateway 10.0.0.1

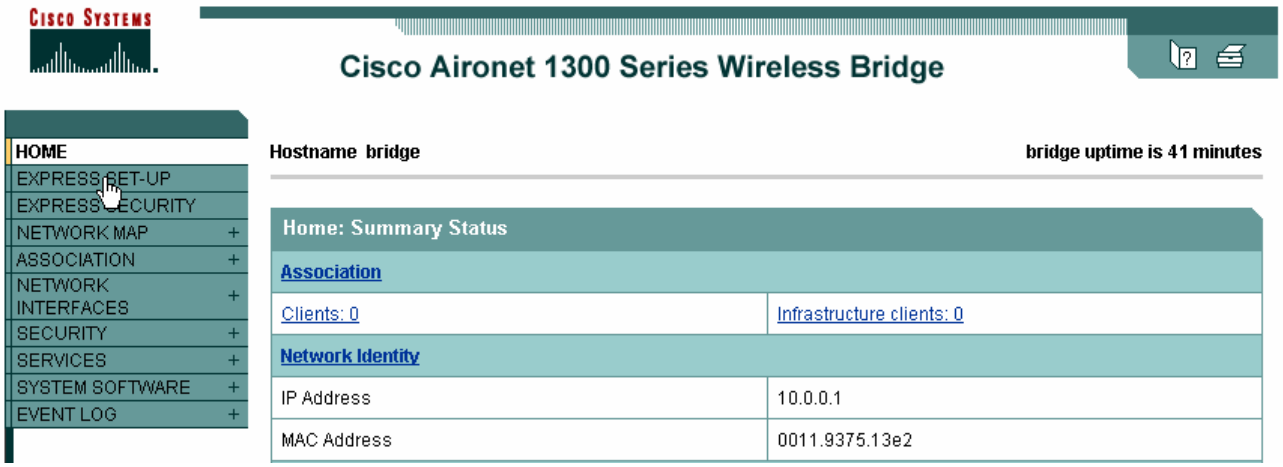
Step 3 Connect to bridge using the web browser

a. Open an Internet browser. The default IP address of a bridge from the factory is 10.0.0.1.

b. Type the bridge IP address in the browser address location field. Press **Enter**.

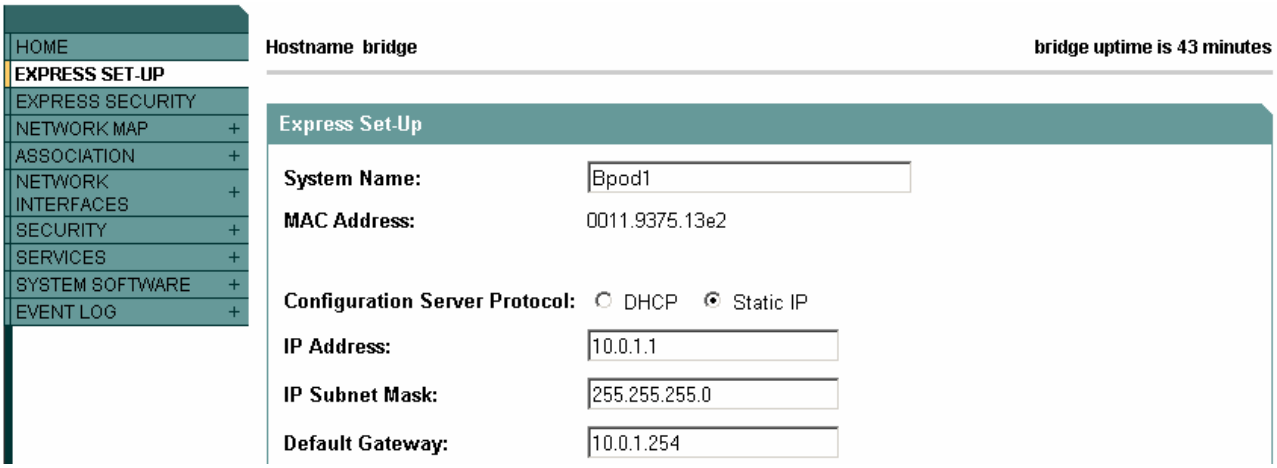
c. A log in screen appears. Type in the password of **Cisco** (case sensitive) and click OK.

d. When the bridge HOME page appears, click **Express Setup** from the left navigation bar.



e. Type a system name of BPod**P** (where **P** is the Pod or Team number) for the bridge in the System Name field.

f. Select **Static IP** as a configuration server protocol from the Configuration Server Protocol selections.



Step 4 Assign the IP address

Use the values in the table to configure the bridge and PC for each team.

Team	bridge Name	bridge Address	PC1 Address	PC2 Address
1	Pod1	10.0.1.1/24	10.0.1.10/24	10.0.1.12/24
2	Pod2	10.0.2.1/24	10.0.2.10/24	10.0.2.12/24

a. Type the IP address in the **IP Address** field.

b. Enter an IP subnet mask in the **IP Subnet Mask** field.

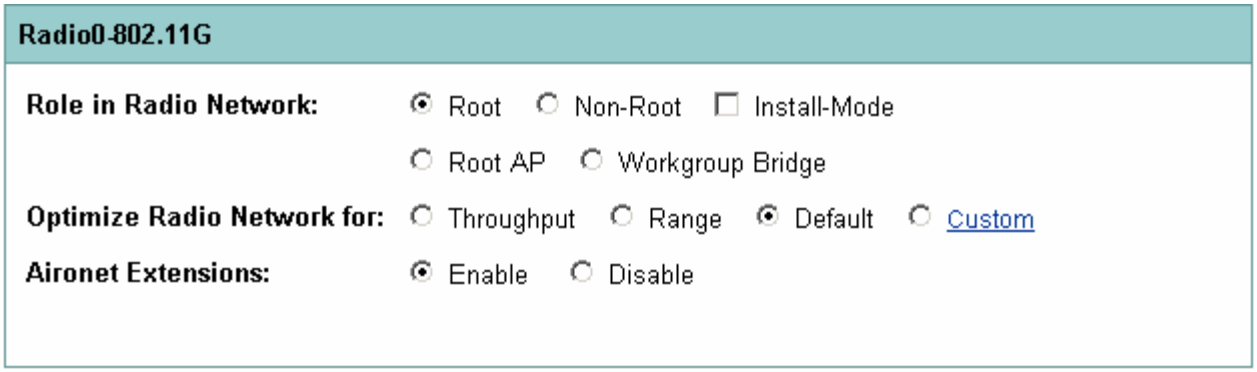
c. Enter the IP address of the default Internet gateway in the **Default Gateway** field. Assume the router address is 10.0.P.254.

d. Leave the **SNMP Community** field at the default value.

e. Set **Role in Radio Network** to Root.

f. Select Throughput for the **Optimize Radio Network** setting. **Note:** This setting will prevent association with 802.11b clients.

g. Click **Apply**.



Once the settings are applied the web connection to the bridge will be lost, since the PC and the bridge are no longer in the same IP subnet.

a. Reconfigure the IP address, subnet mask and gateway on PC1

1. IP address 10.0.P.10
2. Subnet Mask 255.255.255.0
3. Gateway 10.0.P.254

b. Reconnect to the bridge from PC1 web browser and verify the bridge settings from the Express Setup page.

Step 5 Configure SSID

After you assign basic settings to your bridge, you must configure security settings to prevent unauthorized access to your network. Because it is a radio device, the bridge can communicate beyond the physical boundaries of your worksite. Just as you used the Express Setup page to assign basic settings, you can use the Express Security page to create unique SSIDs and assign one of four security types to them.

a. Select the **Express Security** link from the left navigation bar to open the **Express Security Set-Up** page.

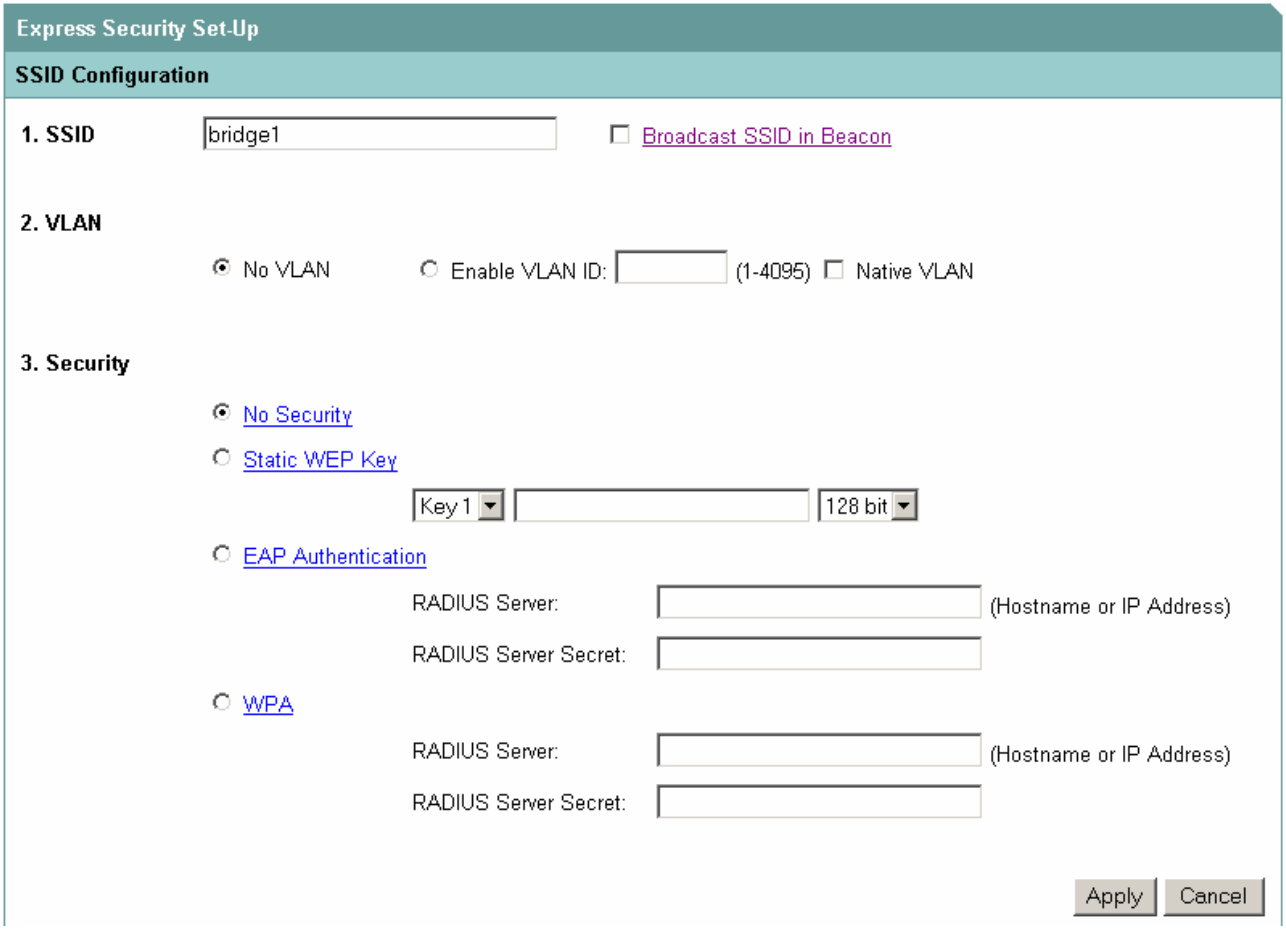
b. In the **SSID** field type the SSID for your pod:

I. Pod 1 SSID: bridge1

II. Pod 2 SSID: bridge2

c. Leave the VLAN and Security settings at their default values. This allows for open authentication.

d. Click **Apply** to save the settings.



Step 6 Connect to the bridge by way of a wireless PC

Using a laptop or desktop with a wireless adapter, connect to the correct bridge. Make sure the wireless device is not connected through the wired network.

a. Configure and select a profile to connect to the bridge. Make sure the SSID is configured in the profile to match the bridge.

b. Configure a unique **Client Name** in the profile, such as a first initial last name of one of the team members

c. Make sure to check or configure the TCP/IP settings of the laptop or desktop to connect to the proper IP network. Configure the wireless adapter with the static IP setting: 10.0.P.12/24.

Step 7 Verify the wireless connection

If the SSID on the bridge and client match, the client should be able to associate with the bridge. The association status can be checked on both the bridge and the PC.

a. From the bridge, navigate to the **Association** page to view all associated devices.

b. Does the wireless PC Client Name appear which was previously configured?

c. Record the MAC Addresses of the devices associated to this bridge. One of these should be the MAC Address of the laptop or desktop configured earlier.

MAC ADDRESS

d. Now check to see if the ACU icon in the system tray is green, which indicates a successful association. Double click on the icon to verify the correct **bridge Name** and **bridge IP Address.**

e. Now check to see if a connection to the bridge using a web browser can be achieved from the wireless device. Enter http://10.0.P.1 for the URL within the browser. Did the bridge GUI display?

f. Test connectivity to other devices by way of ping, Telnet, http, and ftp. This will vary depending on the devices connected and configured on the wired network.

Step 8 Access the bridge through IOS CLI

a. Open the HyperTerminal window on PC1. PC1 should still be connected through the console cable.

b. Enter privileged mode with the following command. ***Cisco*** is the default password.

```
PodP>enable
Password:
PodP#
```

c. Turn off notification logging to avoid interruptions as you enter commands.

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

Step 9 Erase the configuration through CLI

a. 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)
```

Step 10 Configure Hostname

The system name, while not an essential setting, helps identify the bridge on your network. The system name appears in the titles of the management system pages.

a. Enter into configuration mode

```
bridge>enable
Password:Cisco
bridge#
bridge#configure terminal
bridge(config)#
```

b. Turn off notification logging to avoid interruptions as you enter commands.

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

c. Configure the host name with the following command:

```
bridge(config)#hostname PodP  (where P is the pod number)
Pod1(config)#
```


Step 11 Configure the Bridge Virtual Interface (BVI)

When you connect the bridge to the wired LAN, the bridge links to the network using a bridge virtual interface (BVI) that it creates automatically. Instead of tracking separate IP addresses for the Ethernet and radio ports, the network uses the BVI.

a. Assign an IP address and address mask to the BVI.

```
PodP(config)#interface bvi1
PodP(config-if)#ip address 10.0.P.1 255.255.255.0
```

Step 12 Configure passwords

a. Configure the enable password to *cisco*. Also, configure the secret password to *class*. The password is not encrypted and provides access to level 15 (traditional privileged EXEC mode access):

```
PodP(config)#enable password cisco
PodP(config)#enable secret class
```

Use the **level** keyword to define a password for a specific privilege level. After you specify the level and set a password, give the password only to users who need to have access at this level. Use the **privilege level** global configuration command to specify commands accessible at various levels.

b. Set the **configure** command to privilege level 15 and define *cisco* as the password users must enter to use level 15 commands:

```
PodP(config)#privilege exec level 15 configure
PodP(config)#enable password level 15 cisco
```

Step 13 Configure SSID

a. Configure an SSID with open authentication.

```
PodP(config)#interface dot11radio 0
PodP(config-if)#ssid bridgeP        (where P is the pod number)
PodP(config-if-ssid)#authentication open
PodP(config-if-ssid)#end      (or Ctrl-Z)
PodP#
```

Step 14 Check the running configuration and interface status

a. Display the current configuration of the device

```
PodP#show running-config
Building configuration...
Current configuration : 2660 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname PodP
[output omitted]
```

b. Display the condition and information of the device interfaces.

```
PodP#show interfaces
```


Step 15 Save and verify the configuration is saved to Flash

a. Save the current configuration of the device into the configuration file.

```
PodP#copy running-config startup-config
```

b. Verify the startup configuration saved in Flash.

```
PodP#show startup-config
```

Step 16 Connect to the bridge using a wireless PC

Using a laptop or desktop with a wireless adapter, connect to the correct bridge. Make sure the wireless device is not connected through the wired network.

a. Configure and select a profile to connect to the bridge. Make sure the SSID is configured in the profile to match the bridge.

b. Configure a unique **Client Name** in the profile, such as a first initial last name of one of the team members

c. Make sure to check or configure the TCP/IP settings of the laptop or desktop to connect to the proper IP network. Configure the wireless adapter with the static IP setting: 10.0.P.12/24.

d. Now check to see if the ACU icon in the system tray is green, which indicates a successful association. Double click on the ACU icon to verify the correct **bridge Name** and **bridge IP Address.**

Step 17 Verify the Associations

View the current device associations from the bridge CLI. The wireless device configured should appear in the association output.

```
PodP#show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [tsunami] :
SSID [bridgeP] :
Others:  (not related to any ssid)
PodP#
```

Step 18 Connect to the bridge remotely through Telnet

Follow these steps to open the IOS CLI with Telnet. These steps are for a PC running Microsoft Windows with a Telnet terminal application. Check your PC operating instructions for detailed instructions for your operating system.

a. From PC2, Open a Telnet session to the bridge located at 10.0.P.1

b. If Telnet is not listed in your Accessories menu, select Start > Run, type Telnet in the entry field, and press Enter.

c. At the username and password prompts, enter your administrator username and password. The default username is *Cisco*, and the default password is *Cisco*. The default enable password is also *Cisco*. The enable secret password is class. Usernames and passwords are case-sensitive.

```
C:\>telnet 10.0.P.1
User Access Verification
Username:
Password:
PodP>
```

