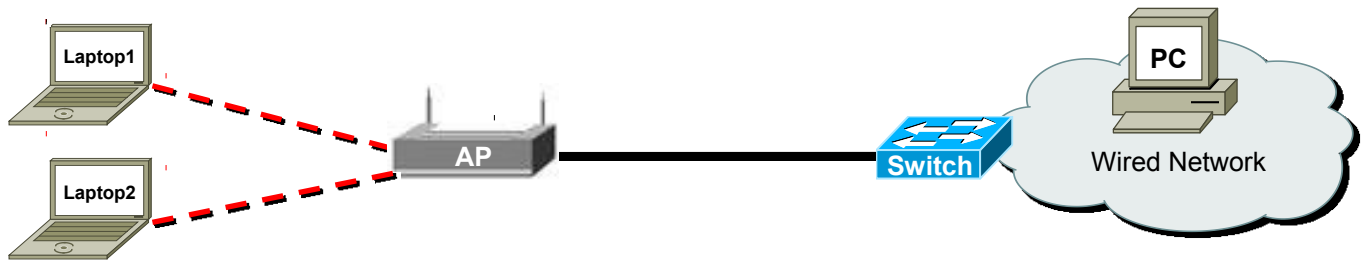


Lab 3.Wireless LANs

Objective

- Understand the LAN technologies of wireless LANs.

Topology



Host name	Interface	IPv4/IPv6 address	SSID
AP	Bridge Virtual Interface 1 (BVI 1)	IPv4: 192.168.1.201/24	N/A
	Dot11Radio 0	N/A	CCNALab_AP1 (Infrastructure mode) CCNALab_Adhoc12 (Ad hoc mode)
Switch	N/A	N/A	N/A
PC	FastEthernet	IPv4: 192.168.1.11/24	N/A
Laptop1	Wireless NIC	IPv4: 192.168.1.22/24	N/A
Laptop2	Wireless NIC	IPv4: 192.168.1.33/24	N/A

Part 1 - Wireless interface configuration of the access point.

Step 1 - Login to the access point.

1. Navigate to the access point's web utility. Start the web browser and set the URL to <http://192.168.1.201>



2. Login to the web utility. When prompted for a username and password, enter the blank username and the global password of "class".



(Note: The default login credentials are a blank username and default password. This is very insecure since it is the factory default and provided publicly.)

Step 2 - Configure the wireless network interface.

3. Select the role of the access point as "Access Point". Then enable the interface for IEEE 802.11 b/g wireless network.

Configure via: **NETWORK INTERFACES -> Radio0-802.11G -> SETTINGS**



4. What is the name of the interface of IEEE 802.11 b/g wireless network?

[Interface Dot11Radio0](#)

5. Modify the radio transmitter power from default value (MAX) to the minimum value (for example, -1 dBm), and modify the client power to local setting.

Configure via: **NETWORK INTERFACES -> Radio0-802.11G -> SETTINGS**

CCK Transmitter Power (dBm):	<input checked="" type="radio"/> -1 <input type="radio"/> 2 <input type="radio"/> 5 <input type="radio"/> 8 <input type="radio"/> 11 <input type="radio"/> 14 <input type="radio"/> 17 <input type="radio"/> 20 <input type="radio"/> Max
OFDM Transmitter Power (dBm):	<input checked="" type="radio"/> -1 <input type="radio"/> 2 <input type="radio"/> 5 <input type="radio"/> 8 <input type="radio"/> 11 <input type="radio"/> 14 <input type="radio"/> 17 <input type="radio"/> 20 <input type="radio"/> Max
Client Power (dBm):	<input checked="" type="radio"/> Local <input type="radio"/> 2 <input type="radio"/> 5 <input type="radio"/> 8 <input type="radio"/> 11 <input type="radio"/> 14 <input type="radio"/> 17 <input type="radio"/> 20 <input type="radio"/> Max

6. Calculate the value of transmitter power in the unit of mw.

$$-1 \text{ dBm} = \frac{0.78 \approx 1}{100} \text{ mw}$$

$$20 \text{ dBm} = \frac{100}{100} \text{ mw}$$

(Note: Power (in dBm) = 10 x Log (Power/1mW))

Step 3 - Configure the radio channel.

7. What channel is being using by the access point?

[Channel 11](#). (Answer will vary)

Verify via: **NETWORK INTERFACES -> Radio0-802.11G -> SETTINGS**

DefaultRadio Channel:	Least Congested Frequency <input type="button" value="v"/> Channel 11 2462 MHz
Least Congested Channel Search: (Use Only Selected Channels)	<div style="border: 1px solid black; padding: 5px;"> Channel 1 - 2412 MHz Channel 2 - 2417 MHz Channel 3 - 2422 MHz Channel 4 - 2427 MHz Channel 5 - 2432 MHz Channel 6 - 2437 MHz Channel 7 - 2442 MHz Channel 8 - 2447 MHz Channel 9 - 2452 MHz Channel 10 - 2457 MHz Channel 11 - 2462 MHz </div>

(Note: The default channel setting for the access point's radios is least congested. At startup, the access point scans for and selects the least congested channel.)

8. Disable the less-congested channel search and change the standard channel to:

[Ch1 – 2.412GHz](#), or [Ch6 – 2.437GHz](#), or [Ch11 – 2.462](#). (Answer will vary)

Configure via: **NETWORK INTERFACES -> Radio0-802.11G -> SETTINGS**

DefaultRadio Channel:	Channel 1 - 2412 MHz <input type="button" value="v"/> Channel 11 2462 MHz
Least Congested Channel Search: (Use Only Selected Channels)	<div style="border: 1px solid black; padding: 5px;"> Least Congested Frequency Channel 1 - 2412 MHz Channel 2 - 2417 MHz Channel 3 - 2422 MHz Channel 4 - 2427 MHz Channel 5 - 2432 MHz Channel 6 - 2437 MHz Channel 7 - 2442 MHz Channel 8 - 2447 MHz Channel 9 - 2452 MHz Channel 10 - 2457 MHz Channel 11 - 2462 MHz </div>

(Note: For the most consistent performance after a site survey, it is recommended that a static channel setting for each access point be assigned.)

9. Why it is good to change the wireless channel to be different from the default channel?

[It is less likely to interfere with other wireless devices at the same area.](#)

Part 2 - Wireless connection in infrastructure mode with open authentication.

Step 1 - Configure the SSID on the access point.

10. Configure the wireless network name (SSID) to “ [CCNALab_AP1](#) ”. And enable the SSID Broadcast in beacon.

Configure via: **EXPRESS SECURITY**

Express Security Set-Up

SSID Configuration

1. SSID ☒ [Broadcast SSID in Beacon](#)

2. VLAN

☒ No VLAN ☐ Enable VLAN ID: (1-4094) ☐ Native VLAN

3. Security

☒ [No Security](#)

(Note: The SSID is case-sensitive and must not exceed 32 characters.)

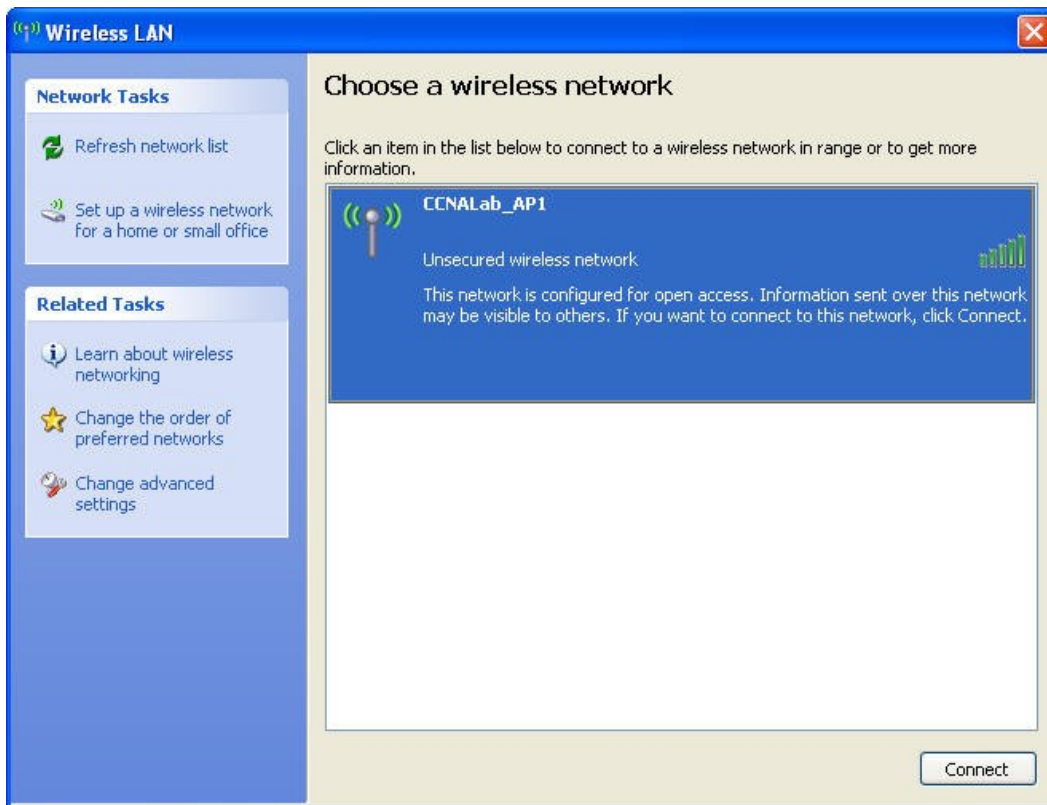
11. When selecting the “No Security” settings, what authentication and encryption protocol are used on the access point?

[This setting uses open authentication and no encryption key.](#)

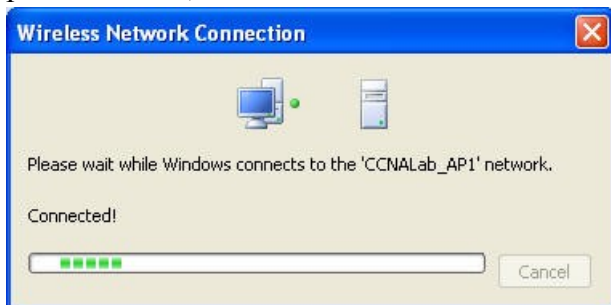
Step 2 - Connect the client to the access point

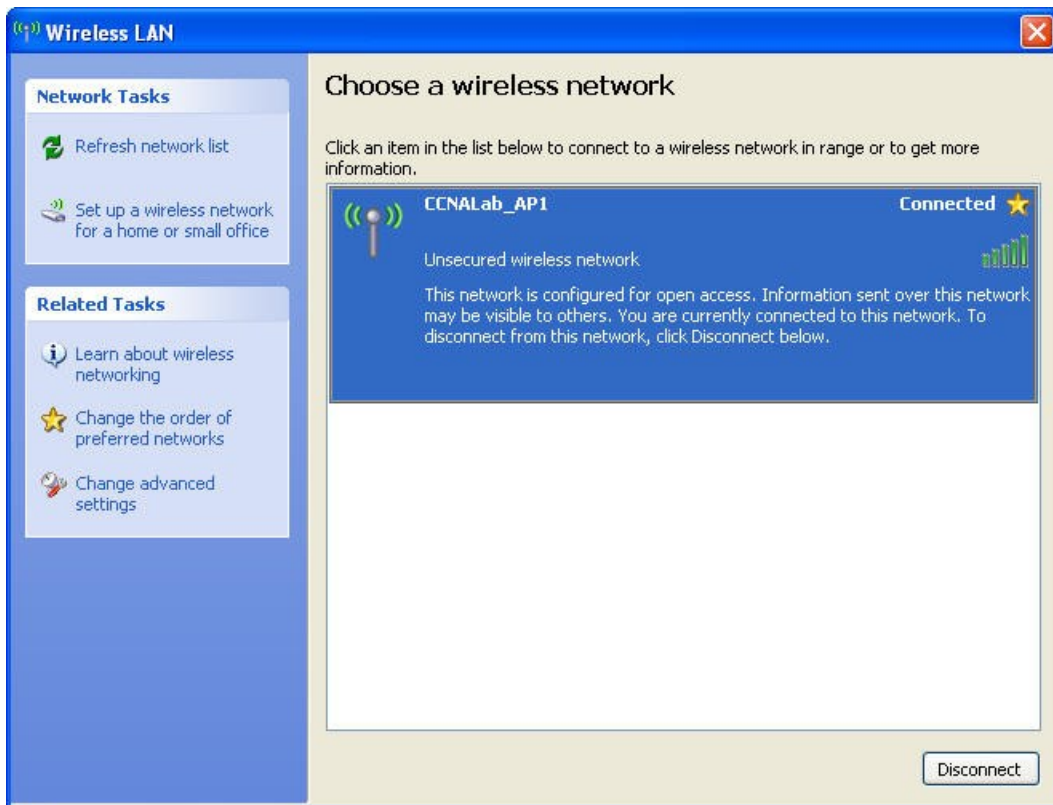
12. Connect the client to the access point.

Configure via: When using Windows XP, click **Start -> Control Panel -> Network** Connections. Right click the icon and select **View Available Wireless Networks**. It is prompted with the available networks with the SSID of the access point.



13. Locate the SSID of “ CCNABlab_AP1 ” in the list of available networks and connect to it. After a period of time, the client will be connected.





14. Manually configure an IP address of the client.

Verify via: Click **Start** -> **Run** and type **cmd**, and at the command prompt use the **ipconfig** command.

```
Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.22
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
```

15. Test the IP connectivity. Ping from the client to the access point's LAN/Wireless interface.

At the command prompt, type "**ping 192.168.1.201**".

```
C:\Documents and Settings\Student>ping 192.168.1.201

Pinging 192.168.1.201 with 32 bytes of data:

Reply from 192.168.1.201: bytes=32 time<1ms TTL=255
Reply from 192.168.1.201: bytes=32 time<1ms TTL=255
Reply from 192.168.1.201: bytes=32 time<1ms TTL=255
Reply from 192.168.1.201: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Step 3 - Disable SSID broadcast on the access point.

16. Configure the SSID to "**CCNALab_API1**". And disable the SSID Broadcast in beacon.

(Note: Delete all the SSIDs before add a new SSID when using single SSID on the access point.)

Configure via: **EXPRESS SECURITY**

Express Security Set-Up

SSID Configuration

1. SSID ☐ [Broadcast SSID in Beacon](#)

2. VLAN

☒ No VLAN ☐ Enable VLAN ID: ☐ Native VLAN

3. Security

☒ [No Security](#)

(Note: When using SSID Broadcast, the wireless clients survey the local area for wireless networks to associate with, they detect the SSID broadcast by the access point. To broadcast the SSID, keep Enabled, the default setting. If do not want to broadcast the SSID, select Disabled.)

Verify via: EXPRESS SECURITY

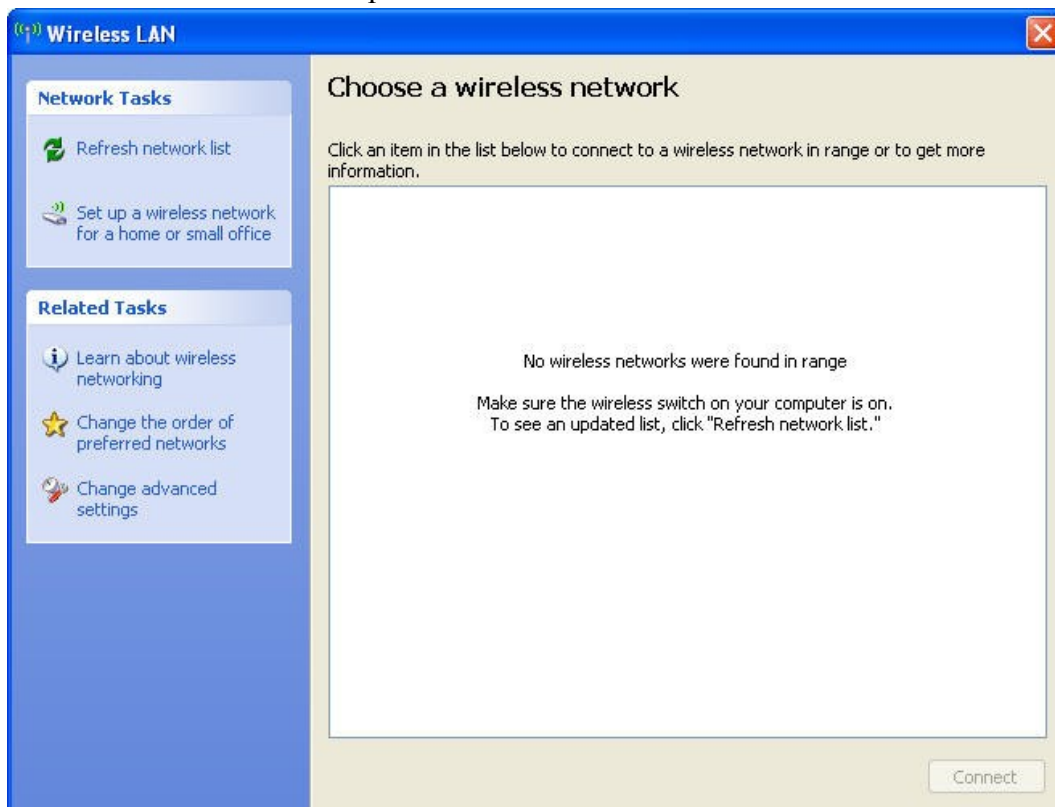
SSID Table							
Delete	SSID	VLAN	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID
<input checked="" type="radio"/>	CCNALab_AP1	none	none	open	none		

17. Why is it recommended to disable SSID broadcast?

It increases the security level by avoiding other people to snoop the SSID of the access point.

18. Verify that the SSID of the access point is no longer being broadcast. Scan for wireless networks on the client.

Configure via: When using Windows XP, click **Start -> Control Panel -> Network Connections**. Right click the icon and select **View Available Wireless Networks**. It is prompted with the available networks with the SSID of the access point.



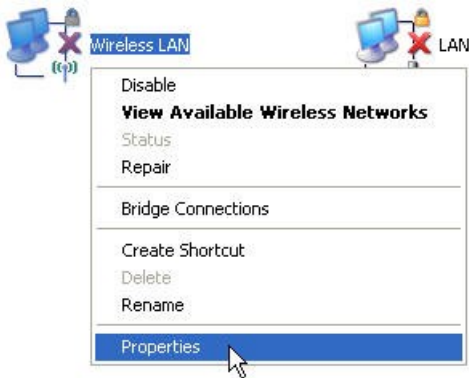
19. Does the SSID of the access point appear?

No.

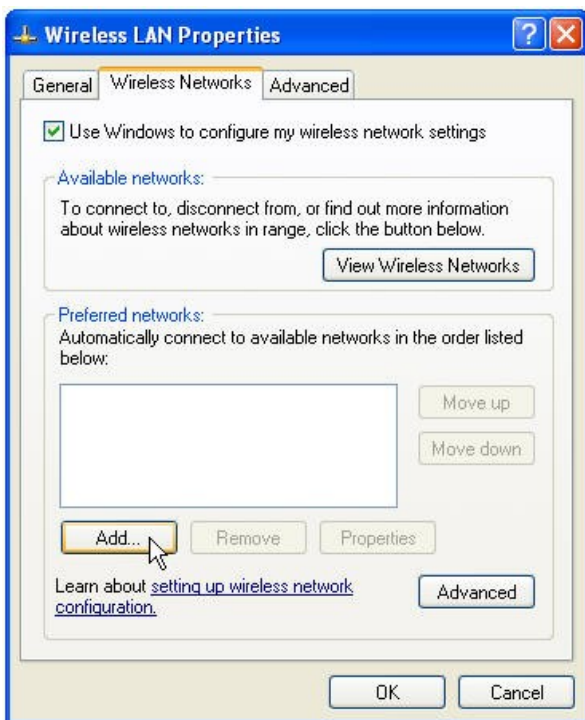
Step 4 - Connect the client to the access point.

20. Configuration a wireless connection in the client manually.

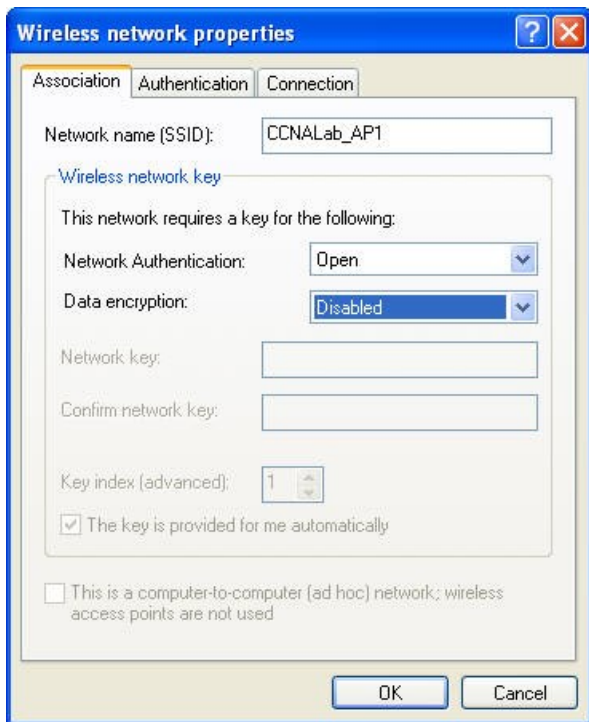
Configure via: When using Windows XP, click **Start -> Control Panel -> Network Connections**, right-click the **Wireless Network Connection** icon, and select **Properties**.



In the **Wireless Networks** tab, select **Add**.



In the **Association** Tab, enter “ CCNALab_AP1 ” as the SSID, and set the Data Encryption to Disabled. The client should now try to reconnect to the wireless access point.



21. Test the IP connectivity. Ping from the client to the access point's LAN/Wireless interface.

At the command prompt, type “*ping* 192.168.1.201”.

```
C:\Documents and Settings\Student>ping 192.168.1.201

Pinging 192.168.1.201 with 32 bytes of data:

Reply from 192.168.1.201: bytes=32 time<1ms TTL=255
Reply from 192.168.1.201: bytes=32 time<1ms TTL=255
Reply from 192.168.1.201: bytes=32 time<1ms TTL=255
Reply from 192.168.1.201: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Part 3 - Wireless connection in infrastructure mode with WPA2

WPA2 is the WiFi Alliance interoperable implementation of the ratified IEEE 802.11i standard. WPA2 implements the Advanced Encryption Standard (AES) encryption algorithm with the use of Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). AES Counter Mode is a block cipher that encrypts 128-bit blocks of data at a time with a 128-bit encryption key. The CCMP algorithm produces a message integrity code (MIC) that provides data origin authentication and data integrity for the wireless frame.

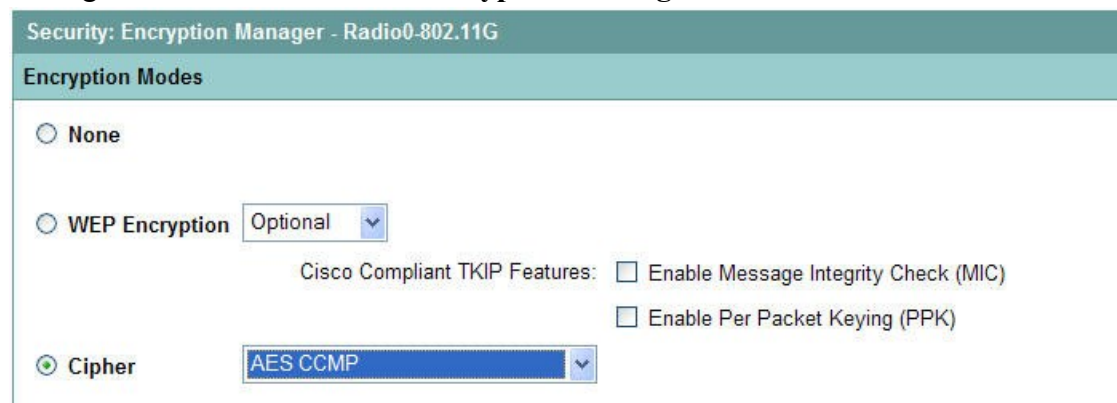
There are two modes in WPA2:

- In personal mode, it requires manual configuration of a PSK on the access point and clients. No authentication server is necessary.
- In enterprise mode, clients and authentication servers authenticate each other with the use of an EAP authentication method, and the client and server generate a Pairwise Master Key (PMK). With WPA2, the server generates the PMK dynamically and passes the PMK to the access point.

Step 1 - Configure WPA2 (personal mode) on the access point.

22. Configure Encryption Mode. Enables “AES encryption” with the use of Counter Mode with CCMP.

Configure via: **SECURITY -> Encryption Manager**



Security: Encryption Manager - Radio0-802.11G

Encryption Modes

☐ None

☐ WEP Encryption Optional

Cisco Compliant TKIP Features: ☐ Enable Message Integrity Check (MIC) ☐ Enable Per Packet Keying (PPK)

☒ Cipher AES CCMP

23. Configure the SSID with following settings:

(Note: Delete all the SSIDs before add a new SSID when using single SSID on the access point.)

- In SSID Properties, Configure the SSID to “ [CCNALab_AP1](#) ”.
- In Client Authentication Settings -> Methods Accepted, select “Open Authentication”.
- In Client Authenticated Key Management, select “Mandatory Key Management”. Then enable WPA.
- Enter the WPA Pre-shared Key (64 hexadecimal characters) as:

[1234567890123456789012345678901234567890123456789012345678901234](#)

(Note: WPA/WPA2 Pre-shared Key must contain between 8 and 63 ASCII text characters or 64 hexadecimal characters.)

Configure via: **SECURITY -> SSID Manager**

Security: Global SSID Manager

SSID Properties

Current SSID List

< NEW >

SSID:

CCNALab_AP1

VLAN:

< NONE >

Define VLANs

Backup 1:

Backup 2:

Backup 3:

Interface:

☒ Radio0-802.11G
☐ Radio1-802.11A

Network ID:

(0-4096)

Client Authentication Settings

Methods Accepted:

☒ Open Authentication: < NO ADDITION >

☐ Shared Authentication: < NO ADDITION >

☐ Network EAP: < NO ADDITION >

Server Priorities:

EAP Authentication Servers

☒ Use Defaults [Define Defaults](#)
☐ Customize

Priority 1:

< NONE >

Priority 2:

< NONE >

Priority 3:

< NONE >

MAC Authentication Servers

☒ Use Defaults [Define Defaults](#)
☐ Customize

Priority 1:

< NONE >

Priority 2:

< NONE >

Priority 3:

< NONE >

Client Authenticated Key Management

Key Management:

Mandatory

☐ CCKM

☒ Enable WPA

WPA

WPA Pre-shared Key:

••••••••••••••••

☐ ASCII
☒ Hexadecimal

Verify via: EXPRESS SECURITY

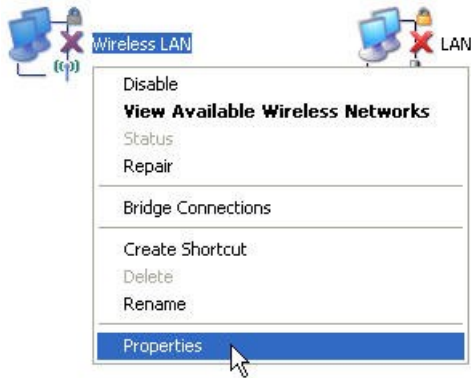
SSID Table							
Delete	SSID	VLAN	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID
	CCNALab_AP1	none	ciphers aes-ccm	open	wpa		

24. What authentication and encryption protocol are used on the access point now?
[This setting uses open authentication with WPA pre-shared key and AES encryption.](#)

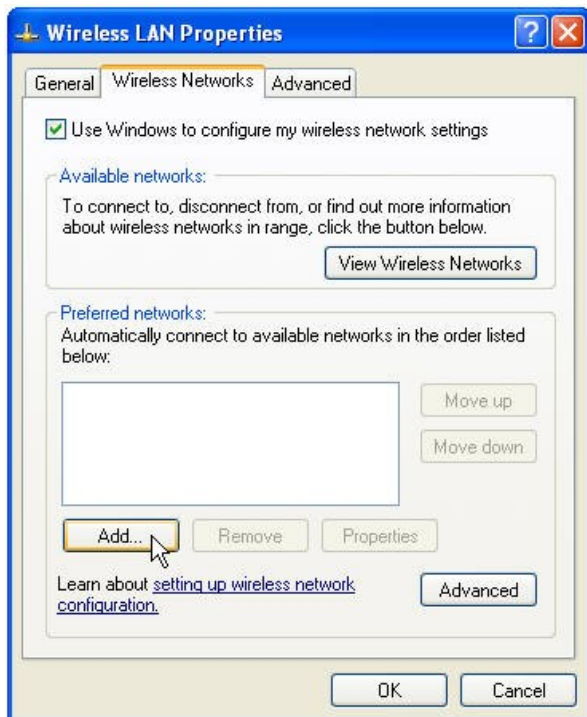
Step 2 - Configure WPA2 (personal mode) on the client.

25. Configuration a wireless connection in the client manually.

Configure via: When using Windows XP, click **Start -> Control Panel -> Network Connections**, right-click the **Wireless Network Connection** icon, and select **Properties**.



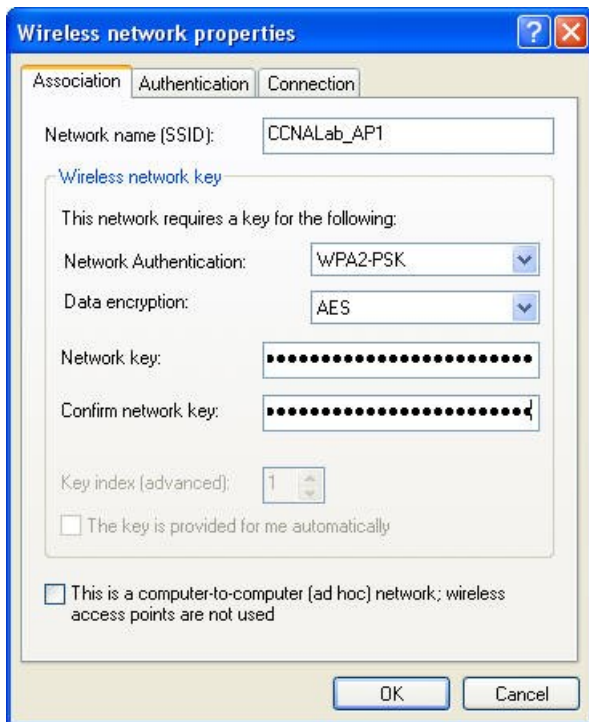
In the **Wireless Networks** tab, select **Add**.



In the Association Tab:

- Set the authentication to WPA2-PSK.
- Set Data Encryption to AES.
- Enter the network key of
123456789012345678901234567890123456789012345678901234

as configured before on the access point.
- Click OK.



(Note: If WPA is being used, the encryption algorithm is Temporal Key Integrity Protocol (TKIP). Similarly, if WPA2 is used, AES is required as the encryption algorithm. WPA2 offers a higher level of security than WPA because AES offers stronger encryption than TKIP.)

The client should now try to reconnect to the wireless access point.

26. Check the status of the association of the clients.

Verify via: **ASSOCIATION**

Association						
Clients: 1						
View: <input checked="" type="checkbox"/> Client <input checked="" type="checkbox"/> Repeater Apply						
Radio0-802.11G						
SSID CCNalab_AP61 :						
Device Type	Name	IP Address	MAC Address	State	Parent	VLAN
ccx-client	NONE	192.168.1.22	0014.787a.02a3	Associated	self	none
Radio1-802.11A						

27. Test the IP connectivity. Ping from the client to the access point's LAN/Wireless interface.

At the command prompt, type “**ping** 192.168.1.201”.

```
C:\Documents and Settings\Student>ping 192.168.1.201

Pinging 192.168.1.201 with 32 bytes of data:

Reply from 192.168.1.201: bytes=32 time<1ms TTL=255
Reply from 192.168.1.201: bytes=32 time<1ms TTL=255
Reply from 192.168.1.201: bytes=32 time<1ms TTL=255
Reply from 192.168.1.201: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```


Step 3 - Configure WPA2 (enterprise mode) on the access point.

(Note: WPA2 in enterprise mode performs authentication in two phases. Configuration of open authentication occurs in the first phase. The second phase is 802.1x authentication with one of the EAP methods. AES provides the encryption mechanism.)

28. Configure the RADIUS server list.

(Note: Since using the access point itself as a local RADIUS server that runs EAP authentication, use the IP address of the access point in the RADIUS server list, use the ports 1812 and 1813 for local RADIUS server operation and use the IP address of the server as the shared secret.)

Configure via: **SECURITY -> Server Manager**

Corporate Servers

Current Server List

RADIUS ▼

< NEW >

Server: 192.168.1.201 (Hostname or IP Address)

Shared Secret:

Authentication Port (optional): 1812 (0-65536)

Accounting Port (optional): 1813 (0-65536)

Delete

Apply Cancel

Default Server Priorities

EAP Authentication	MAC Authentication	Accounting
Priority 1: 192.168.1.201 ▼	Priority 1: < NONE > ▼	Priority 1: < NONE > ▼
Priority 2: < NONE > ▼	Priority 2: < NONE > ▼	Priority 2: < NONE > ▼
Priority 3: < NONE > ▼	Priority 3: < NONE > ▼	Priority 3: < NONE > ▼

29. Configure Encryption Mode. Enables “AES encryption” with the use of Counter Mode with CCMP.

Configure via: **SECURITY -> Encryption Manager**

Security: Encryption Manager - Radio0-802.11G

Encryption Modes

☐ None

☐ WEP Encryption Optional ▼

Cisco Compliant TKIP Features: ☐ Enable Message Integrity Check (MIC) ☐ Enable Per Packet Keying (PPK)

☒ Cipher AES CCMP ▼

30. Configure the SSID with following settings:

(Note: Delete all the SSIDs before add a new SSID when using single SSID on the access point.)

- In SSID Properties, Configure the SSID to “ [CCNALab_AP1](#) ”.

- In Client Authentication Settings, select “Open Authentication” with “EAP”, and “Network EAP”.
- In Client Authenticated Key Management, select “Mandatory Key Management”. Then enable WPA.

Configure via: **SECURITY -> SSID Manager**

Security: Global SSID Manager

SSID Properties

Current SSID List

< NEW >

SSID:

CCNALab_AP1

VLAN:

< NONE >

Define VLANs

Backup 1:

Backup 2:

Backup 3:

Interface:

☒ Radio0-802.11G
☐ Radio1-802.11A

Network ID:

(0-4096)

Delete

Client Authentication Settings

Methods Accepted:

☒ Open Authentication:

with EAP

☐ Shared Authentication:

< NO ADDITION >

☒ Network EAP:

< NO ADDITION >

Client Authenticated Key Management

Key Management:

Mandatory

☐ CCKM

☒ Enable WPA

WPA

WPA Pre-shared Key:

☒ ASCII
☐ Hexadecimal

31. Enable the SSID Broadcast in beacon.

Guest Mode/Infrastructure SSID Settings

Radio0-802.11G:

Set Beacon Mode:

☒ Single BSSID

Set Single Guest Mode SSID:

CCNALab AP1

☐ Multiple BSSID

Set Infrastructure SSID:

< NONE >

☐ Force Infrastructure Devices to associate only to this SSID

Radio1-802.11A:

Set Beacon Mode:

☒ Single BSSID

Set Single Guest Mode SSID:

< NONE >

☐ Multiple BSSID

Set Infrastructure SSID:

< NONE >

☐ Force Infrastructure Devices to associate only to this SSID

Step 4 - Configure the RADIUS server.

32. Configure the local authentication server.

- In Local Radius Server Authentication Settings, select LEAP.
- In Network Access Servers (AAA Clients), define the IP address and shared secret of the RADIUS server. (Use the IP address of the server as the shared secret.)
- In Individual Users, define the individual users.

Configure via: **SECURITY -> Local RADIUS Server -> General Set-Up**

Security: Local RADIUS Server - General Set-Up

Local Radius Server Authentication Settings

Enable Authentication Protocols:

☐ EAP FAST

☒ LEAP

☐ MAC

Network Access Servers (AAA Clients)

Current Network Access Servers

< NEW >

Network Access Server: 192.168.1.201 (IP Address)

Shared Secret:

Delete

Also, the configuration selects Text (or NT hash) for the password.

Individual Users

Current Users

< NEW >

Delete

Username: student1

Password: ☒ Text ☐ NT Hash

Confirm Password:

Group Name: < NONE > v

☐ MAC Authentication Only

Apply Cancel

Verify via: EXPRESS SECURITY

SSID Table							
Delete	SSID	VLAN	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID
	CCNALab_AP1	none	ciphers aes-ccm	open+EAP , network EAP	wpa		

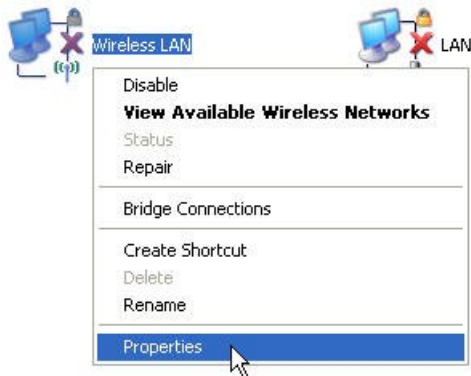
33. What authentication and encryption protocol are used on the access point now?

[This setting uses open authentication with EAP and AES encryption.](#)

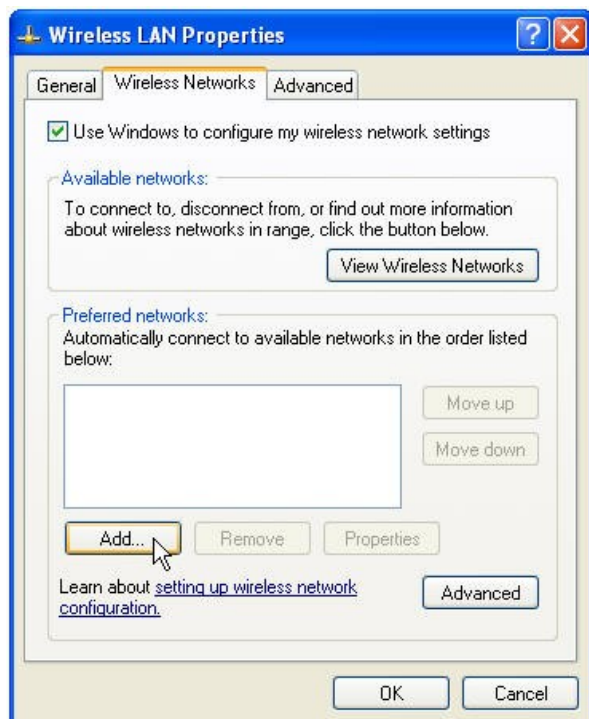
Step 5 - Configure WPA2 (enterprise mode) in the client.

34. Configuration a wireless connection in the client manually.

Configure via: When using Windows XP, click **Start -> Control Panel -> Network Connections**, right-click the **Wireless Network Connection** icon, and select **Properties**.

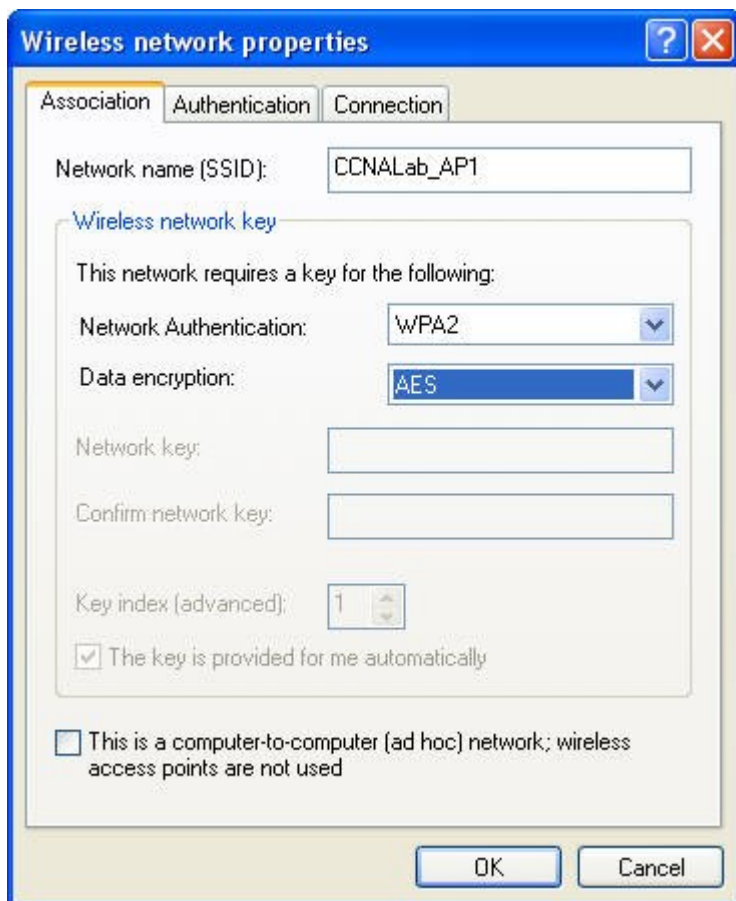


In the **Wireless Networks** tab, select **Add**.

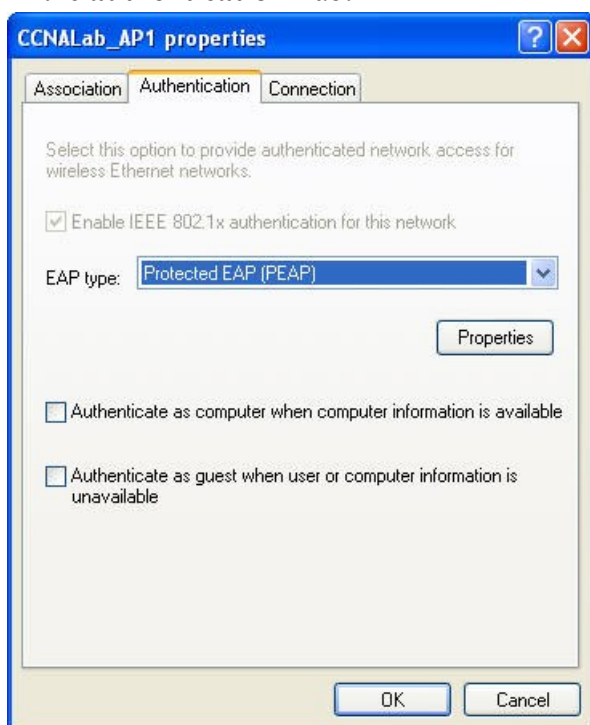


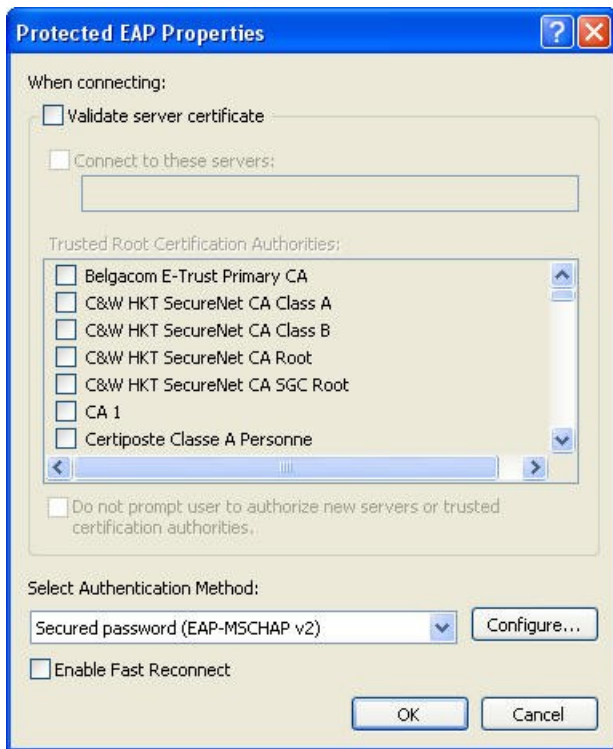
In the **Association** Tab:

- Set the authentication to WPA2.
- Set Data Encryption to AES.
- Click OK.



In the **authentication** Tab:





35. The client should now try to reconnect to the wireless access point. When the “Enter Wireless Network Credentials” window displays, enter the username and password. When authentication is successful, the client connects to the wireless LAN.



36. Check the status of the association of the clients.
Verify via: ASSOCIATION

Association						
Clients: 1						
View: <input checked="" type="checkbox"/> Client <input checked="" type="checkbox"/> Repeater						Apply
Radio0-802.11G						
SSID CCNALab_AP61 :						
Device Type	Name	IP Address	MAC Address	State	Parent	VLAN
ccx-client	NONE	192.168.1.22	0014.787a.02a3	Associated	self	none
Radio1-802.11A						

37. Test the IP connectivity. Ping from the client to the access point's LAN/Wireless interface.

At the command prompt, type “*ping* 192.168.1.201”.

```
C:\Documents and Settings\Student>ping 192.168.1.201

Pinging 192.168.1.201 with 32 bytes of data:

Reply from 192.168.1.201: bytes=32 time<1ms TTL=255
Reply from 192.168.1.201: bytes=32 time<1ms TTL=255
Reply from 192.168.1.201: bytes=32 time<1ms TTL=255
Reply from 192.168.1.201: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```


Part 4 - Wireless connection in Ad Hoc mode.

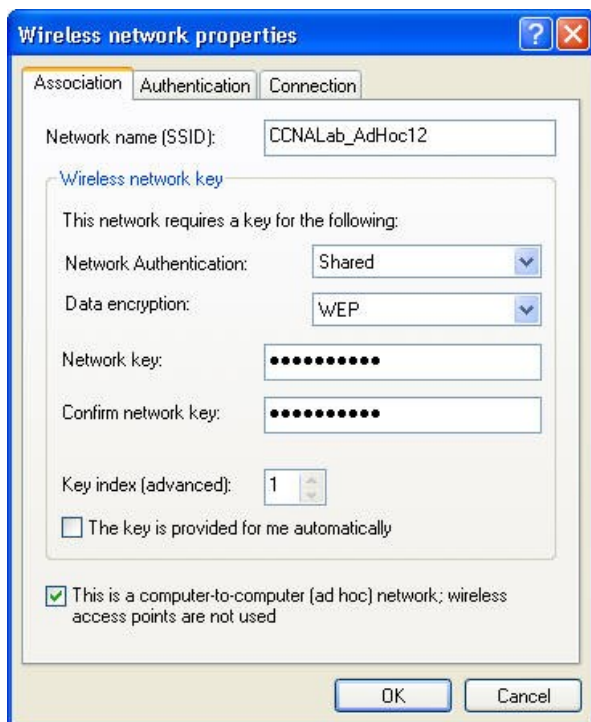


Step 1 - Configure Ad Hoc connection (with WEP) on a pair of clients.

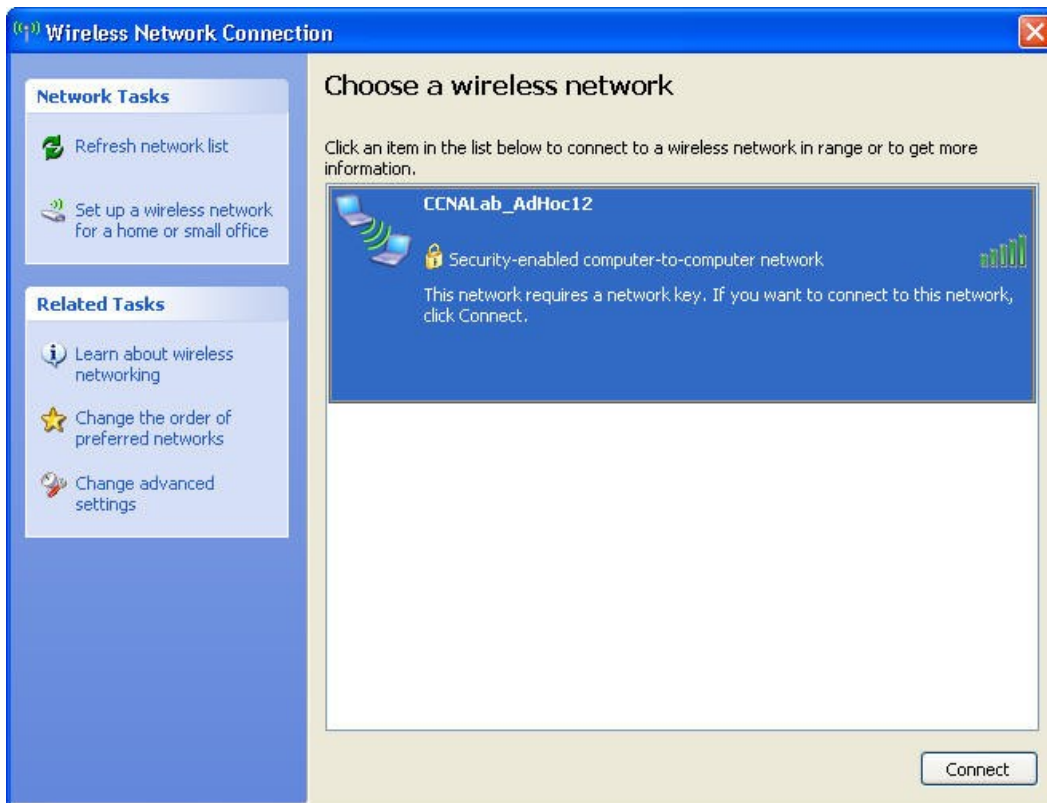
38. On one of the clients, navigate to the Network Connections page and right-click the **Wireless Network Connection** icon, and select **Properties**. In the **Wireless Networks** tab, select **Add** to create a new wireless connection.

In the **Association** Tab:

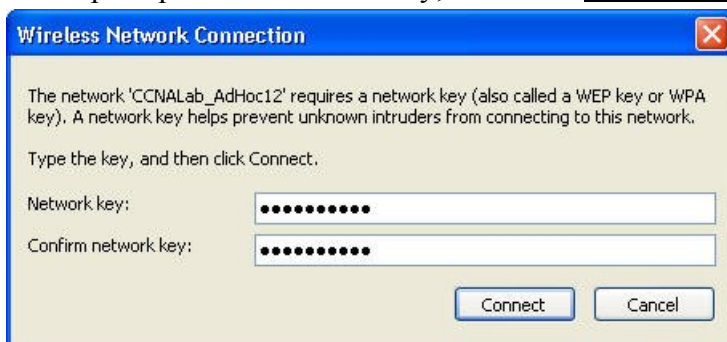
- Set the authentication to Shared.
- Set Data Encryption to WEP.
- Uncheck the box “This key is provided for me automatically” .
- Enter the network key of 1234567890 .
- Click OK.



39. On another client, scan for the wireless network.



40. When prompted for the WEP key, enter it as 1234567890 and click **Connect**.



Step 2 - Verify the Ad Hoc connection between clients.

41. Test the IP connectivity between the clients. Ping to each other to verify the wireless connection.

At the command prompt, type “*ping* 192.168.1.22”.