A wireless access point (WAP) is a hardware device or configured node on a local area network (LAN) that allows wireless capable devices and wired networks to connect through a wireless standard, including Wi-Fi or Bluetooth. WAPs feature radio transmitters and antennae, which facilitate connectivity between devices and the Internet or a network.

A WAP is also known as a hotspot.

Wireless access points (WAP) may be used to provide network connectivity in office environments, allowing employees to work anywhere in the office and remain connected to a network. In addition, WAPs provide wireless Internet in public places, like coffee shops, airports and train stations.

A Wireless Access Point (WAP) is a networking device that allows connecting the devices with the wired network. A Wireless Access Point (WAP) is used to create the WLAN (Wireless Local Area Network), it is commonly used in large offices and buildings which have expanded businesses.

It is easier and simpler to understand and implant the device. It can be fixed, mobile or hybrid proliferated in the 21st century. The availability, confidentiality, and integrity of the communication and network are a responsibility and to be ensured about that.

A wireless AP connects the wired networks to the wireless client. It eases access to the network for mobile users which increases productivity and reduces the infrastructure cost.

Advantages of Wireless Access Point (WAP):

1. More User Access:

Normally the wireless router allows 10 – 20 users or devices to access the network. While the WAP allows 50 – 100 or more users or devices to access the network.

The WAP has a stronger ability to send and receives signals which enables high usage.

2. Broader Transmission Range:

A wireless router signals cover up to a dozen or 10 -12 meters. However, a wireless access point covers more than 100 – 300 meters.

The broad range is supremacy for the large cover offices or buildings for the bigger businesses. With this wireless access point, a user can easily roam that network.

3. Flexible Networking:

It is known that wireless networking except in homes, often involves many wireless devices and different networking patterns implanted based on the environment and requirements of the commercial locations.

Step 1: Arrange all devices as following

Step 2: Configure Access Points (A)

In Access point CS

Port 0, set

Port Status: on, Bandwidth: 100 Mbps, Duplex: Half Duplex

Port 1, set

SSID: CS, select WPA2-PSK and password to ciscopacket1

In Access point IT

Port 0, set

Port Status: on, Bandwidth: 100 Mbps, Duplex: Half Duplex

Port 1, set

SSID: IT, select WPA2-PSK and password to ciscopacket2

Step 3: Configure and Setup IP Address for all devices (PC’s)

Device Interface IPv4 address Other

pc-1

IP config 192.168.1.3

Default Gateway: 192.168.1.1

pc-2

IP config 192.168.1.4

Default Gateway: 192.168.1.1

pc3

IP config 171.16.10.2

Default Gateway: 171.16.10.1

pc4

IP config 171.16.10.3

Default Gateway: 171.16.10.1

pc-1 and pc-2

Wireless0 SSID: CS

WPA2-PSK password:

ciscopacket1

pc3 n pc4

Wireless0 SSID: IT

WPA2-PSK password:

ciscopacket2

Router2

F0/0 192.168.1.1

S0/0/0 20.0.0.1

RIP v2 20.0.0.0

192.168.1.0

Router3

F0/0 171.16.10.1

S0/0/0 20.0.0.2

RIP v2 20.0.0.0

171.16.10.0

Note: Change all port adapters with wireless adapter for all PC’s