Wireless LAN Concept

Robin Lin

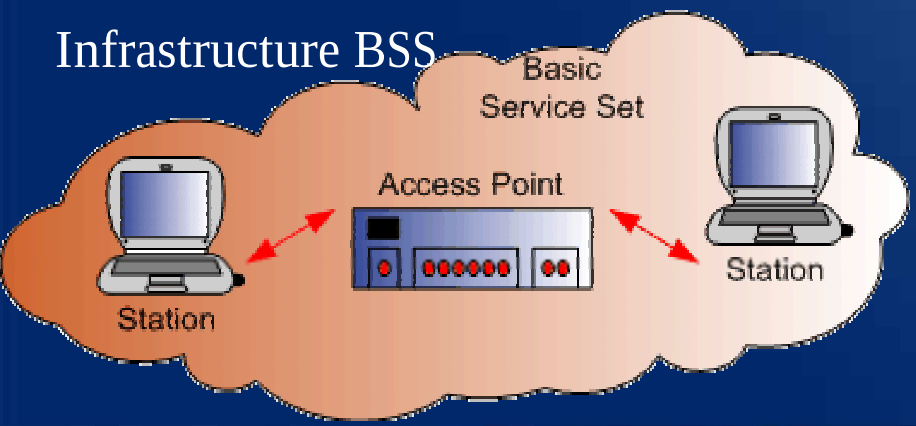
ICOM Senior Engineer

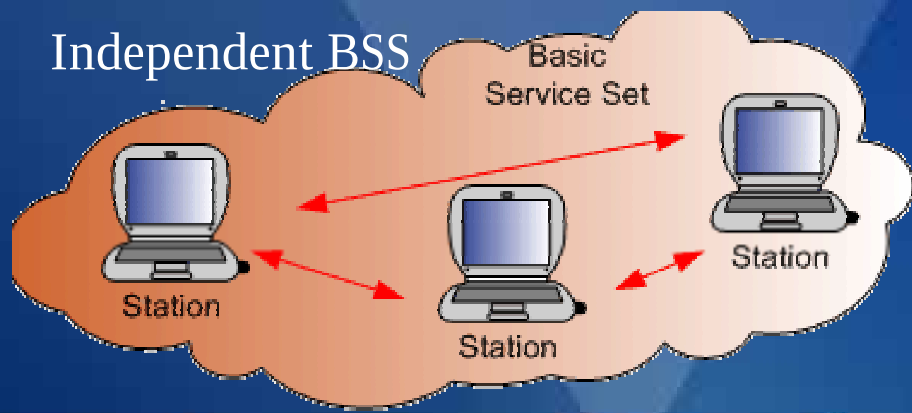
Glossary

- STA – Station
- AP – Access Point
- BSS – Basic Service Set
- BSSID – Basic Service Set Identifier
- IBSS – Independent BSS (Ad hoc)
- Infrastructure BSS
- ESS – Extended Service Set
- Channel
- WEP – Wireless Equivalent Privacy

BSS

- Basic Service Set
- A set of wireless devices communicate with each other
- The basic component of WLAN





SSID

- Service Set Identifier
- Name of a wireless local area network (WLAN).
- All wireless devices on a WLAN must employ the same SSID in order to communicate with each other.
- Case sensitive text strings.
- Maximum length is 32 characters.

SSID

- The SSID on wireless clients can be set either manually, by entering the SSID into the client network settings, or automatically, by leaving the SSID unspecified or blank.
- A network administrator often uses a public SSID, that is set on the access point and broadcast to all wireless devices in range.
- Some newer wireless APs disable the automatic SSID broadcast feature in an attempt to improve network security.

BSSID

- The BSSID is a 48bit identity used to identify a particular BSS within an area
- In Infrastructure BSS networks, the BSSID is the MAC address of the AP
- In Independent BSS or ad hoc networks, the BSSID is generated randomly
- For example:
  - 02:D0:01:01:71:18 (IBSS)
  - 00:90:4B:0B:14:7E (Infrastructure BSS)

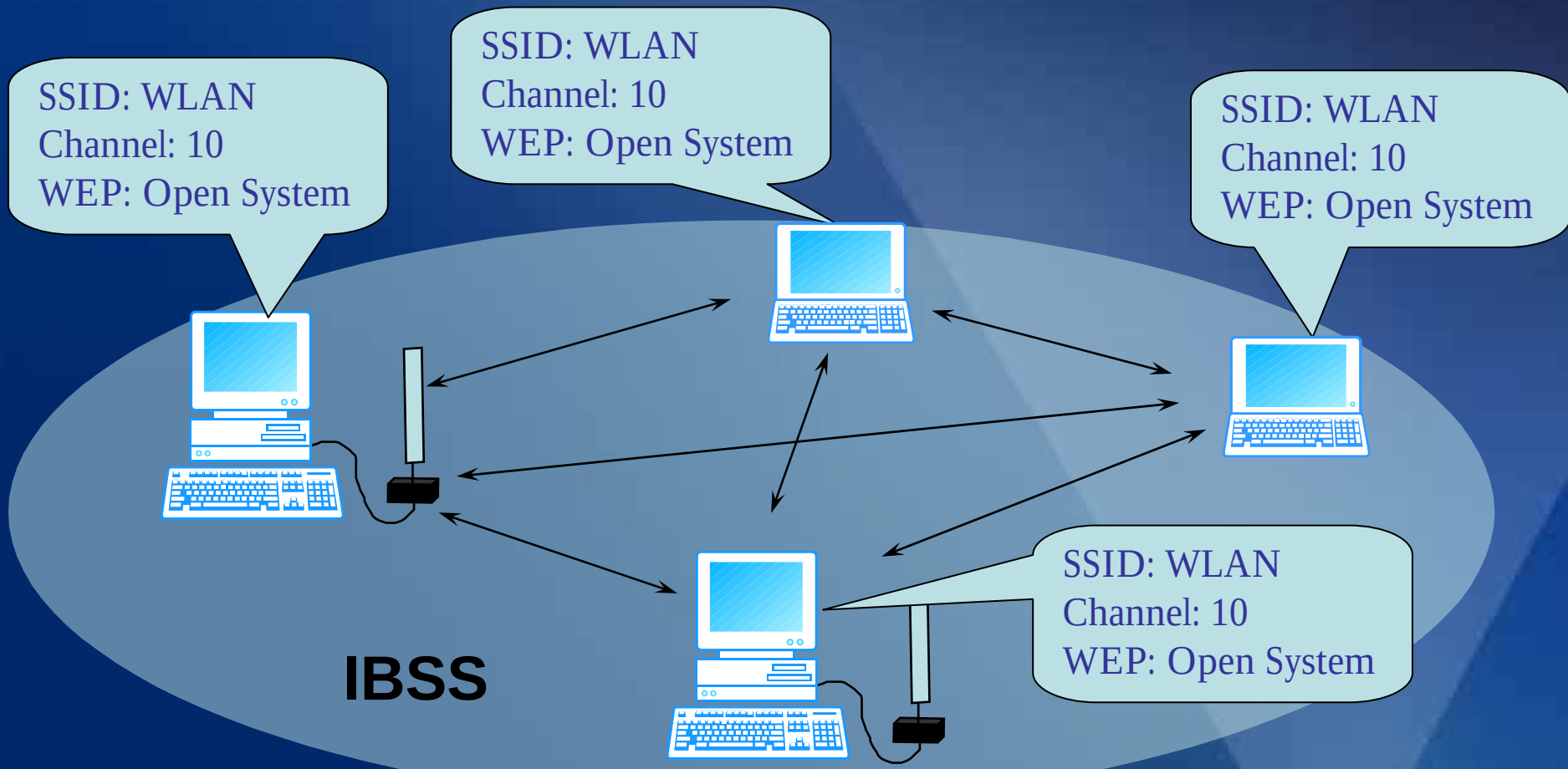
Independent BSS (IBSS)

- An 802.11 networking framework in which devices or stations communicate directly with each other, without any AP.
- Independent BSS is also referred to as peer-to-peer or Ad hoc.
- Useful for establishing a network where wireless infrastructure does not exist or where services are not required.

Independent BSS (IBSS)

- To establish a IBSS, all the devices or stations want to join have to change to IBSS mode and set the same SSID, channel and WEP settings.

Independent BSS (IBSS)



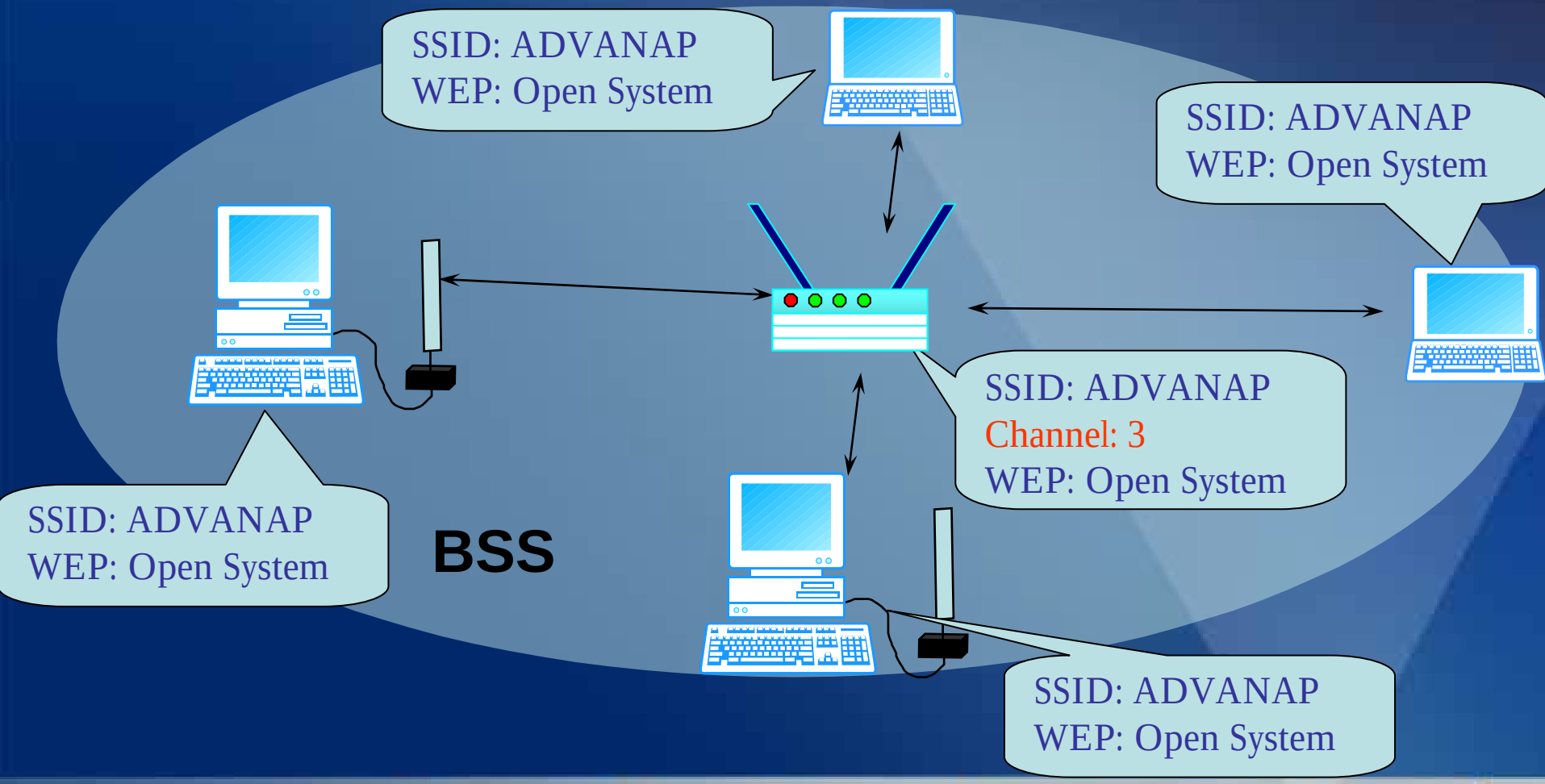
Infrastructure BSS

- An 802.11 networking framework in which devices communicate with each other by first going through an Access Point (AP).
- Bridge a wireless network to a wired Ethernet network.
- Most corporate wireless LANs operate in infrastructure mode because they require access to the wired LAN in order to use services such as file servers or printers.

Infrastructure BSS

- Compared to the IBSS, infrastructure BSS offer the advantage of scalability and centralized security management.
- To establish a infrastructure BSS, you have to setup a AP with a specific SSID and all the devices or workstation want to join have to set the same SSID as the AP.

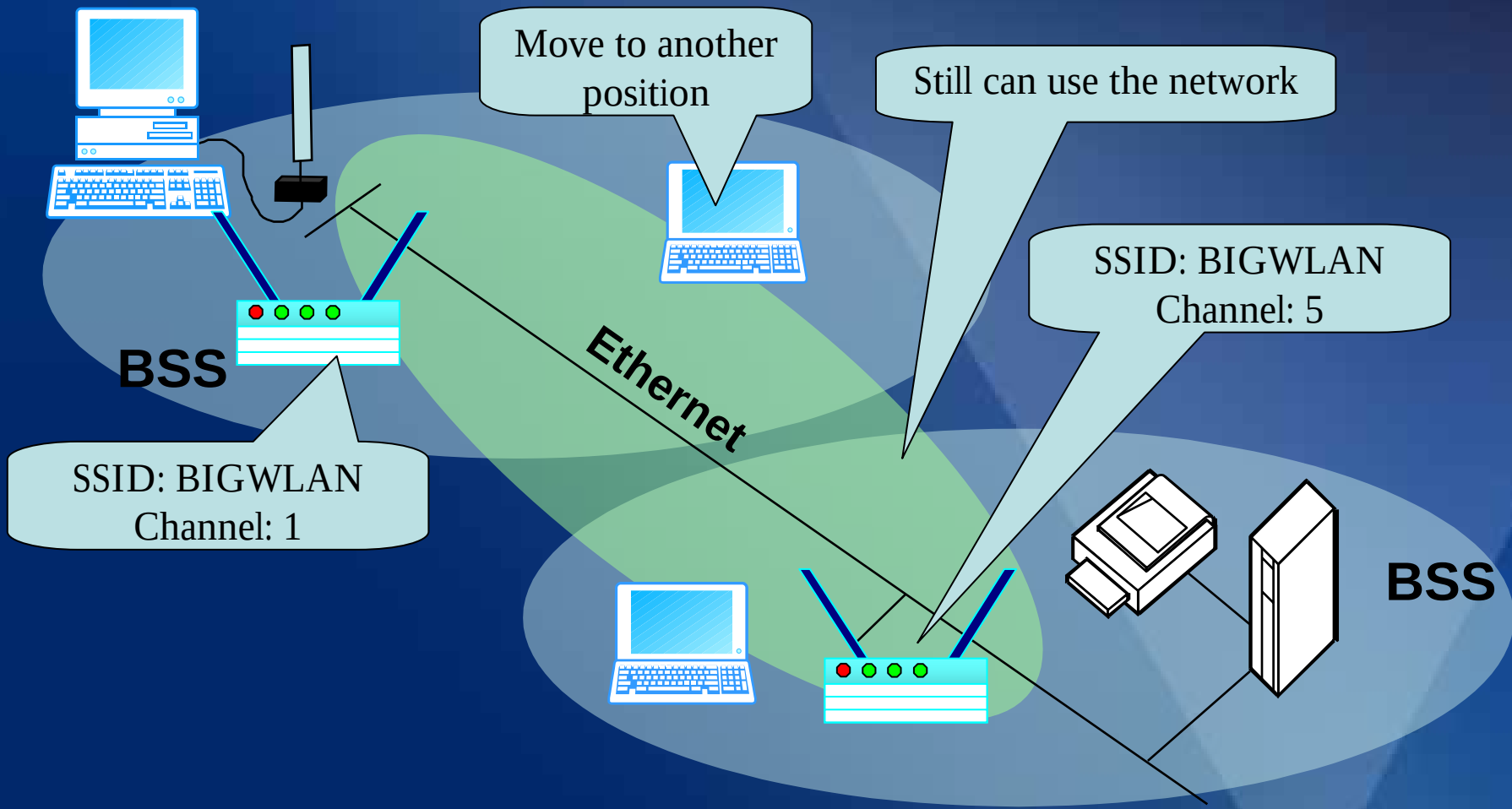
Infrastructure BSS



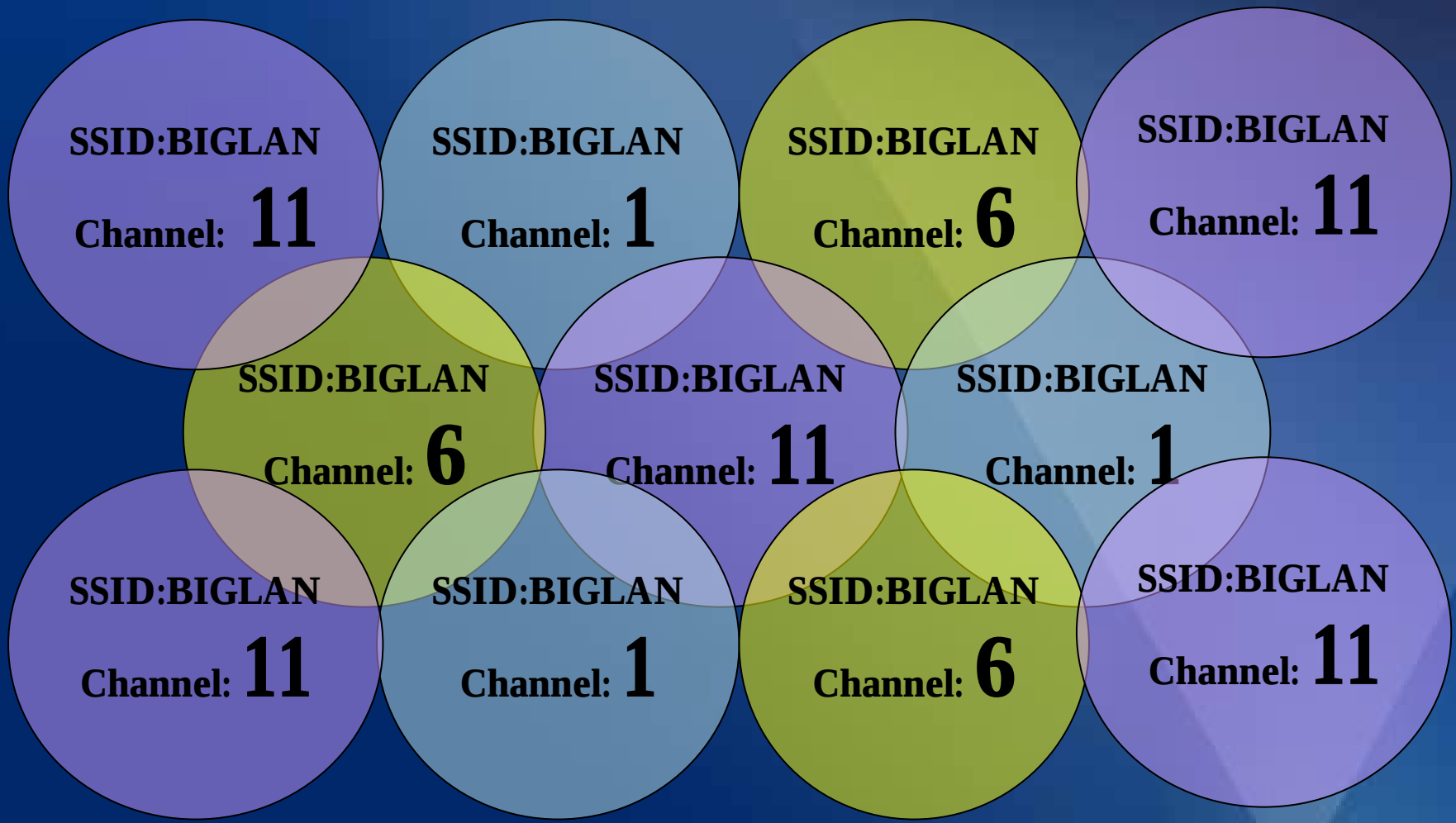
ESS

- Extended Service Set
- A set of two or more BSSs that form a single sub-network.
- Enables limited mobility within the WLAN.
- All the BSSs have the same SSID or as ESSID.
- When the BSSs have overlap, we can use different channel.
- Recommend more 5 channel gap. For example: 1, 6, 11

ESS


Move to another position
Still can use the network
SSID: BIGWLAN
Channel: 5
BSS
Ethernet
SSID: BIGWLAN
Channel: 1
BSS

Example of ESS



802.11b Channel

Channel	Frequency (GHz)	US/Canada	ESTI	France
1	2.412	v	v	
2	2.417	v	v	
3	2.422	v	v	
4	2.427	v	v	
5	2.432	v	v	
6	2.437	v	v	
7	2.442	v	v	
8	2.447	v	v	
9	2.452	v	v	
10	2.457	v	v	v
11	2.462	v	v	v
12	2.467		v	v
13	2.472		v	v
14	2.475			

◎ Most country allow to use channel 10. We choose this channel as default channel.

WEP

- Wireless Equivalent Privacy
- WEP uses the stream cipher RC4 from RSA Security Inc.
- There are two levels of WEP commonly available
  - based on a 40 bit encryption key and 24bit initialization vector (64bit encryption)
  - based on a 104 bit encryption key and 24bit initialization vector (128bit encryption).

Advance Configuration Parameters

- Beacon Interval
- RTS Threshold
- Fragment Threshold
- Preamble Type

Beacon

- The "heartbeat" of a WLAN, announcing the existence of the network, and enabling stations to establish and maintain communications in an orderly fashion.
- It carries the following information (some of which is optional):
  - The Timestamp.
  - The Beacon interval defines the amount of time between transmitting beacon frames.
  - The Capability Information lists requirements of stations that want to join the WLAN. For example, it indicates that all stations must use WEP.
  - The Service Set Identifier (SSID).
  - The Basic Rate Set.
  - The optional Parameter Sets.

Beacon Interval

- The amount of time between beacon transmissions.
- Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).

RTS Threshold

- RTS Threshold is the frame size above that an RTS/CTS handshake will be performed before attempting to transmit.
- RTS/CTS asks for permission to transmit to reduce collisions, but adds considerable overhead.
- Disabling RTS/CTS can reduce overhead and latency in WLANs where all stations are close together, but can increase collisions and degrade performance in WLANs where stations are far apart and unable to sense each other to avoid collisions.
- If you are experiencing excessive collisions, you can try turning RTS/CTS on or (if already on) reduce RTS/CTS Threshold on the affected stations.

Fragment Threshold

- Fragmentation Threshold is the maximum length of the frame, beyond which payload must be broken up into two or more frames.
- Collisions occur more often for long frames because sending them occupies the channel for a longer period of time, increasing the chance that another station will transmit and cause a collision.
- Reducing Fragmentation Threshold results in shorter frames that "busy" the channel for shorter periods, reducing packet error rate and resulting retransmissions.
- However, shorter frames also increase overhead, degrading maximum possible throughput, so adjusting this parameter means striking a good balance between error rate and throughput.

Preamble Type

- A preamble is a signal used in network communications to synchronize the transmission timing between two or more systems.
- Proper timing ensures that all systems are interpreting the start of the information transfer correctly.

802.11 alphabet

802.11	Base standard. 2.4 GHz and IR. DSSS and FHSS	Completed
802.11a	5 GHz OFDM 54 Mb/s	Completed
802.11b	2.4 GHz. DSSS. 11 Mb/s	Completed
802.11c	2.4 GHz. DSSS. 11 Mb/s	Completed
802.11d	Global Harmonization	Completed
802.11e	QoS enhancements	Ongoing
802.11f	Inter Access Point	Completed
802.11g	2.4 GHz. DSSS and OFDM. 54 Mb/s	Completed
802.11h	Spectrum and transmit power management	Completed

802.11 alphabet

802.11i	Security enhancements	Completed
802.11j	5 GHz operation in Japan	Completed
802.11k	Radio Resource Measurements	Ongoing
802.11m	Standard maintenance	Ongoing
802.11n	High Throughput	Ongoing
802.11p	Wireless access in vehicular environments	Ongoing
802.11r	Fast BSS transition	Ongoing
802.11s	ESS mesh	Ongoing
802.11T	Wireless Performance Prediction	Ongoing