



4.9.2.3 Wireless Networking

Wireless Networks

Wireless networks allow devices to connect to a network without being physically connected to it.

WiFi – A wireless local area network that is based on international standards

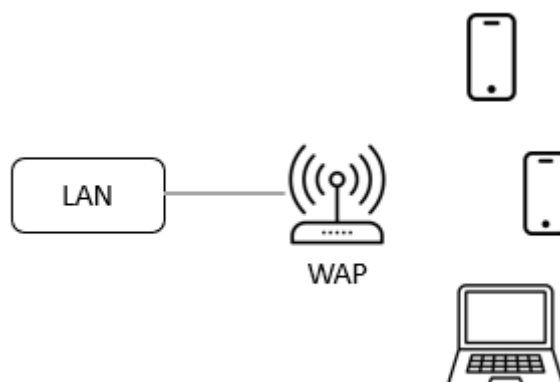
Devices need a **wireless network adapter** in order to connect to a wireless network and receive and transmit data wirelessly. Example WiFi dongle or WiFi PCIe Card



A wireless network adapter for a pc/laptop

A **wireless access point (WAP)** allows wireless devices to connect to a network and can provide a bridge between the wireless network and a wired network.

Devices connected to the same WAP share the available wireless bandwidth.





Wireless Security

As there is no physical connection, data transmitted wireless is more visible and networks with wireless access more vulnerable to unauthorised devices attempting to connect.

There are a number of methods used to secure wireless networks.

Strong Encryption

As transmitted data is visible during wireless transmission, it is important to use strong encryption to make sure the data is unreadable to unauthorised viewing.

WPA/WPA2 (WiFi protected access) can use a password/passphrase to authenticate devices and encrypt transmitted data.

SSID Broadcast Disabled

SSID (service set identifier) **is the name that identifies a wireless network.**

A network usually broadcasts its SSID so that devices can find it. **The broadcast can be disabled** so that the SSID does not appear in normal network searches. Users must then enter the SSID manually to connect.



MAC Address Allow List

MAC address are **unique physical addresses assigned to each device by their manufacturer.**

An allow list can be made of MAC addresses of devices that are allowed to connect to the network.

The wireless access point checks the MAC address of a device trying to connect to the network against the allow list before letting the device connect.



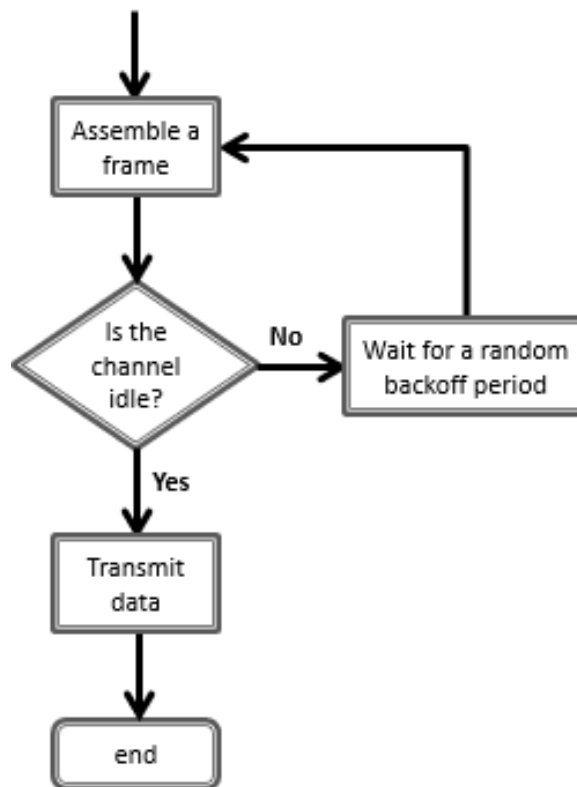


CSMA/CA Without RTS/CTS

Carrier sense multiple access with collision avoidance (CSMA/CA) is a **protocol used in wireless networks to avoid data collisions caused by multiple devices trying to transmit simultaneously.**

1. The device assembles a frame ready to transmit.
2. It listens out on the communication channel to check if it is idle.
3. If it is not idle it will wait a random period of time before checking the channel again.
4. If the channel is idle then the device will transmit the data.

While effective at avoiding collisions in small networks it cannot overcome the problem of hidden nodes.



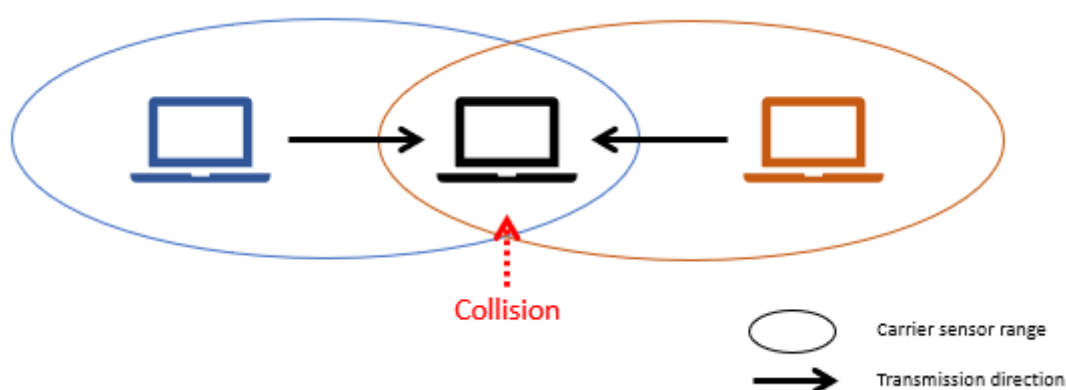


Hidden Node Problem

The hidden node problem is where devices on a wireless network cannot detect all devices on the network due to those devices being out of its range.

When listening out for an idle channel, a device may mistakenly detect the channel is idle while in reality there is a device transmitting that is hidden.

The CSMA/CA protocol can be modified to get around this problem by sending RTS (right to send) and CTS (clear to send) messages to ensure the channel is idle before transmission begins.





CSMA/CA With RTS/CTS

Carrier sense multiple access with collision avoidance with Request to Send/Clear to Send (RTS/CTS)

1. The device assembles a frame ready to transmit.
2. It listens out on the communication channel to check if it is idle. If it is not idle it will wait a random period of time before checking the channel again.
3. If the channel is idle then the device will transmit an RTS.
4. The receiver responds to the RTS with a CTS message. The CTS informs other devices in range that they should defer transmission for the specified period.
5. On receiving the CTS, the device starts to transmit. If a CTS is not received it will wait a random period of time before checking if the channel is idle again.
6. After the data is received, the receiver sends an ACK (acknowledgement).
7. If no ACK is received by the sending device then it will wait a time period before listening again to retransmit.
8. The ACK confirms to the sender that the data was received successfully. Other devices can then attempt to transmit when the channel becomes available.

