

Specialized Attacks: Wireless

Tactics and Techniques for Wireless Attacks

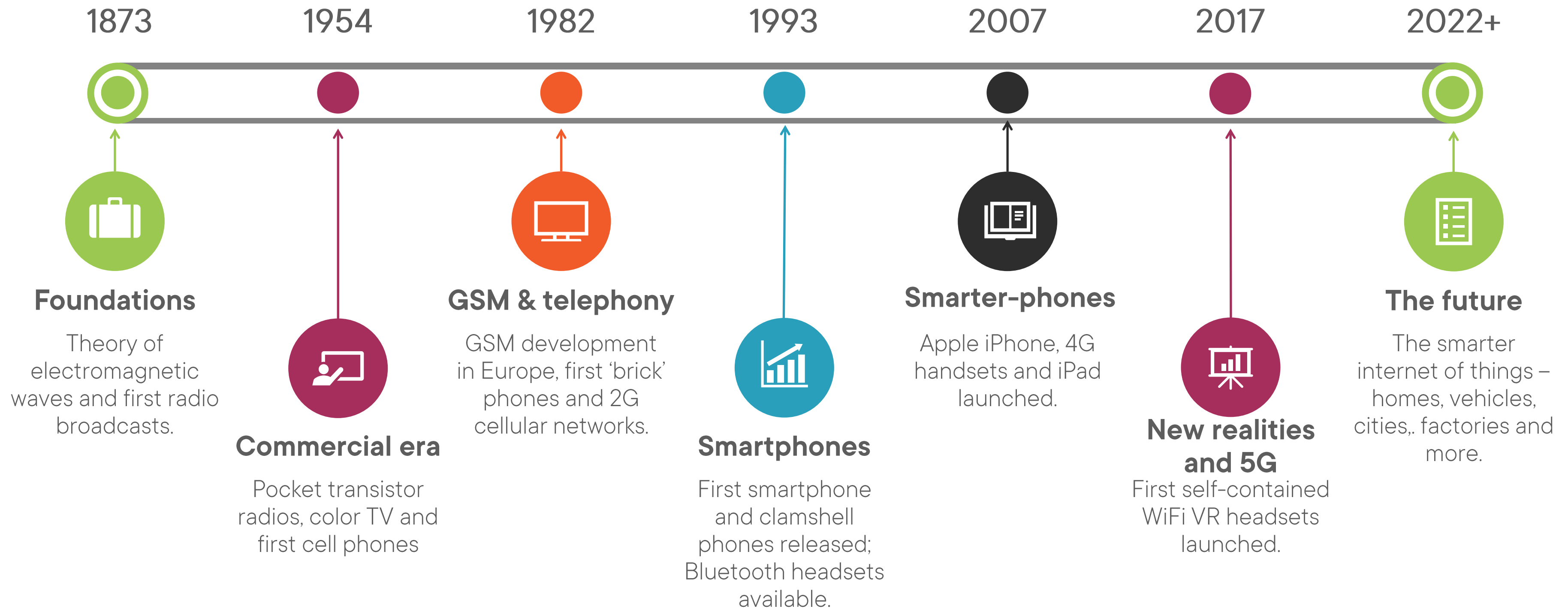


Matt Lloyd Davies

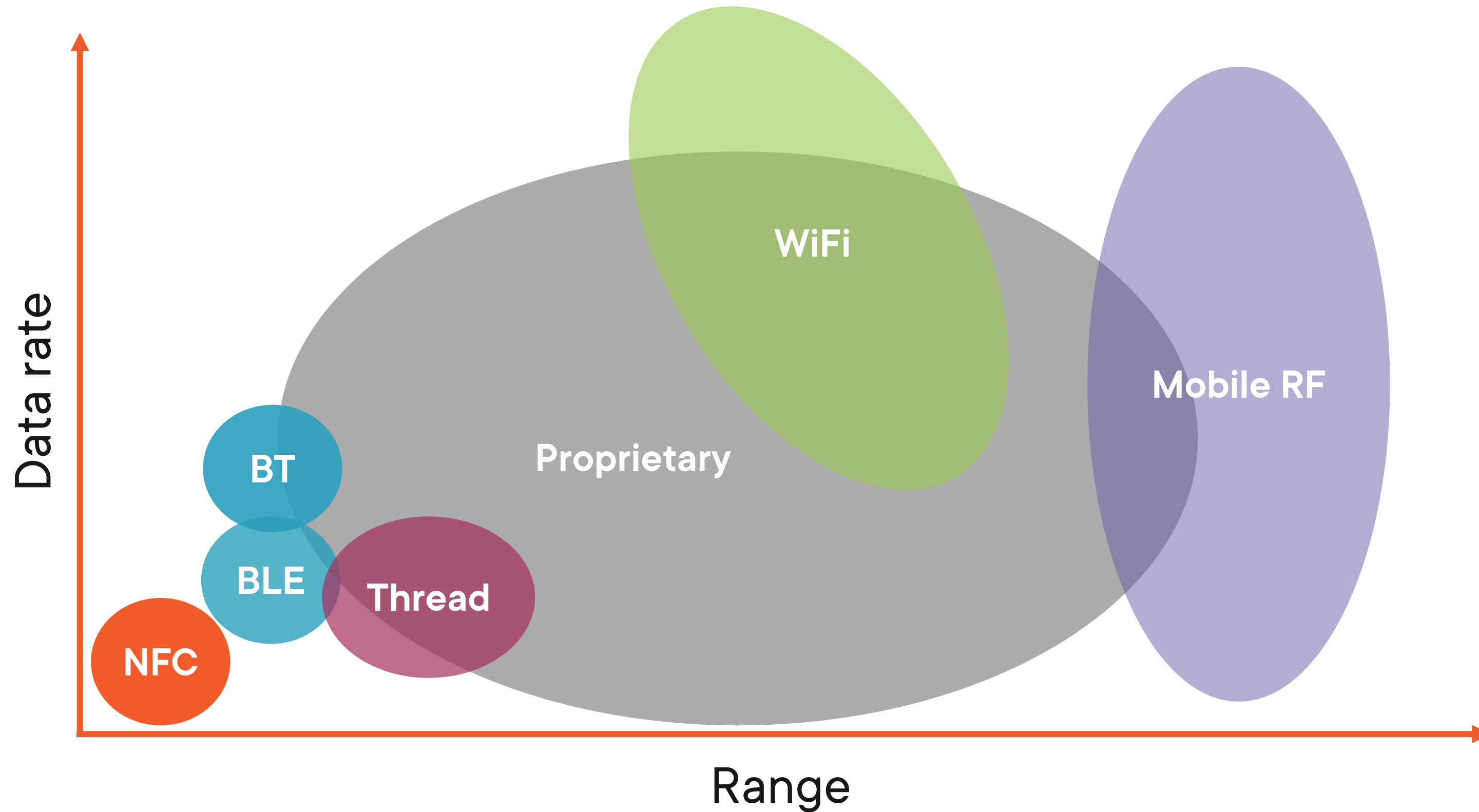
Capability Development Lead



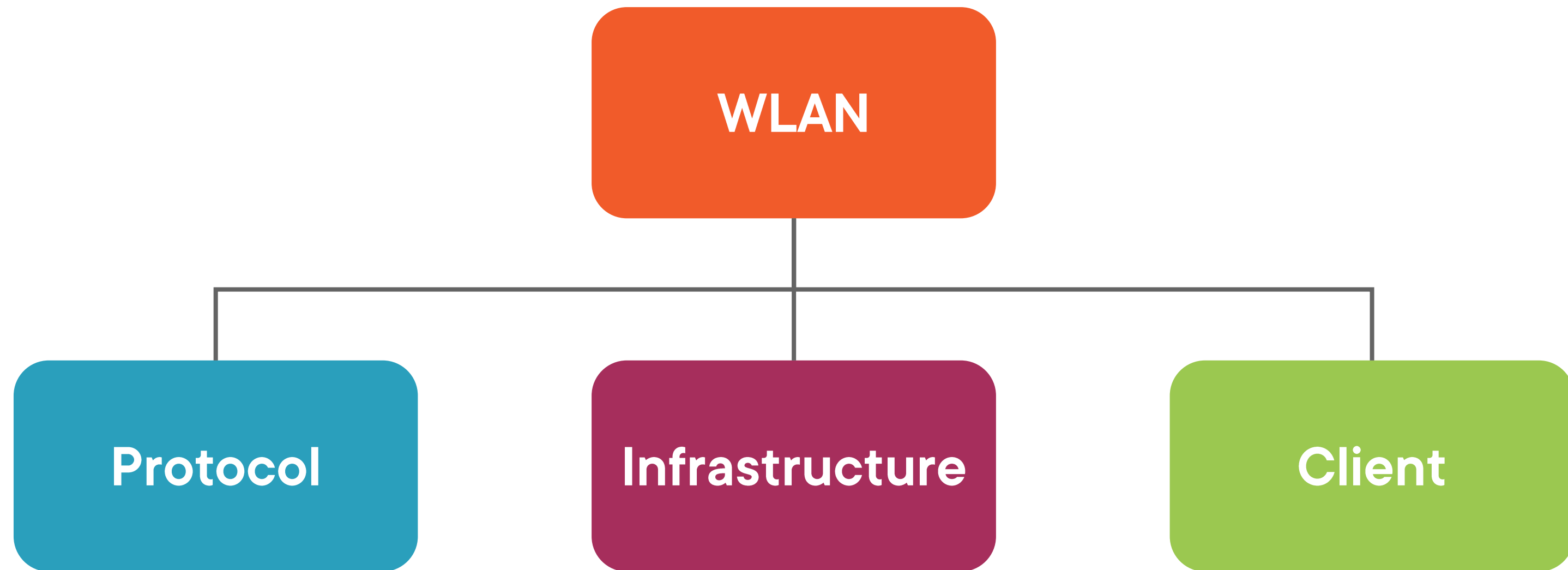
The Rise of Wireless Technologies



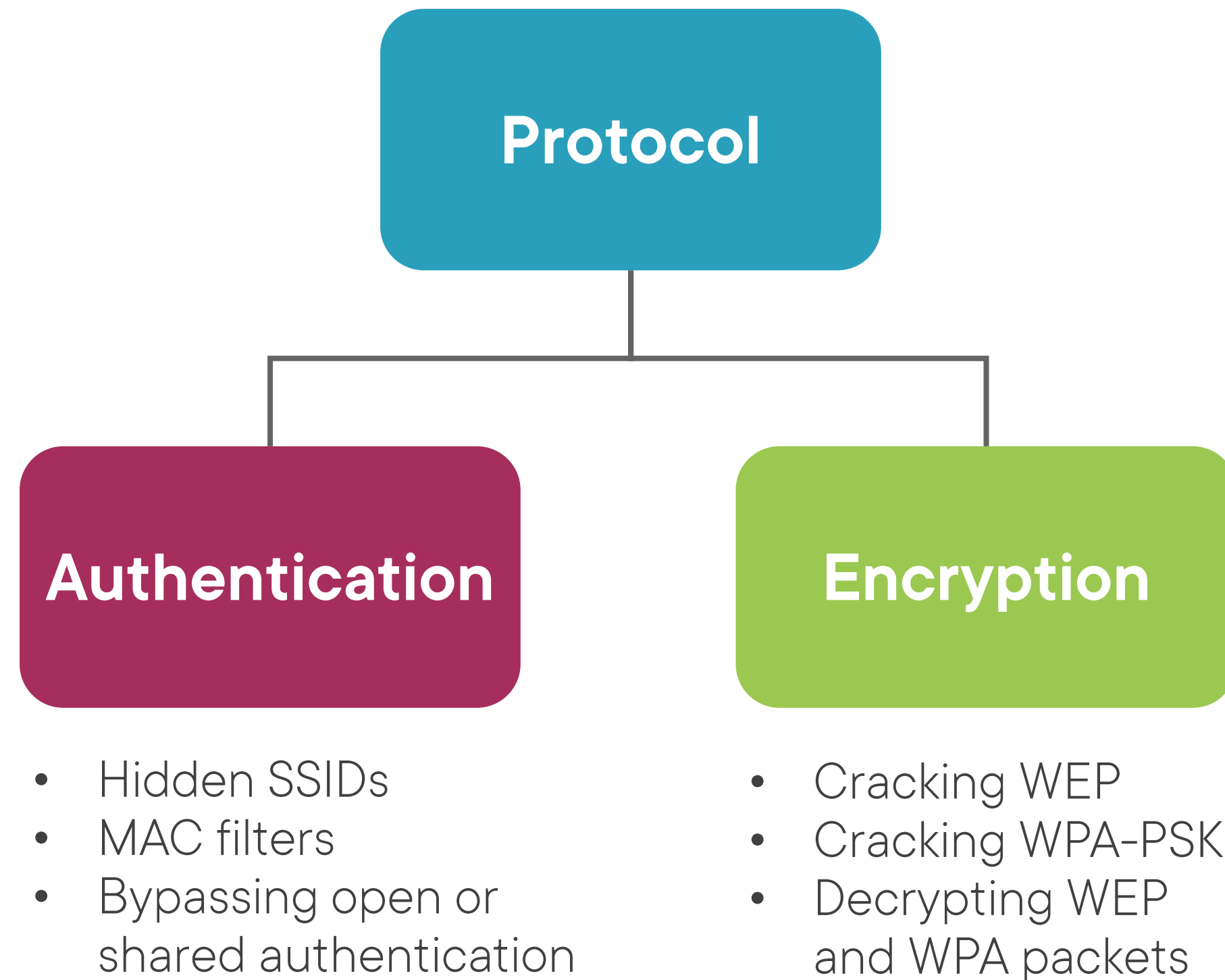
Wireless Technologies in Context



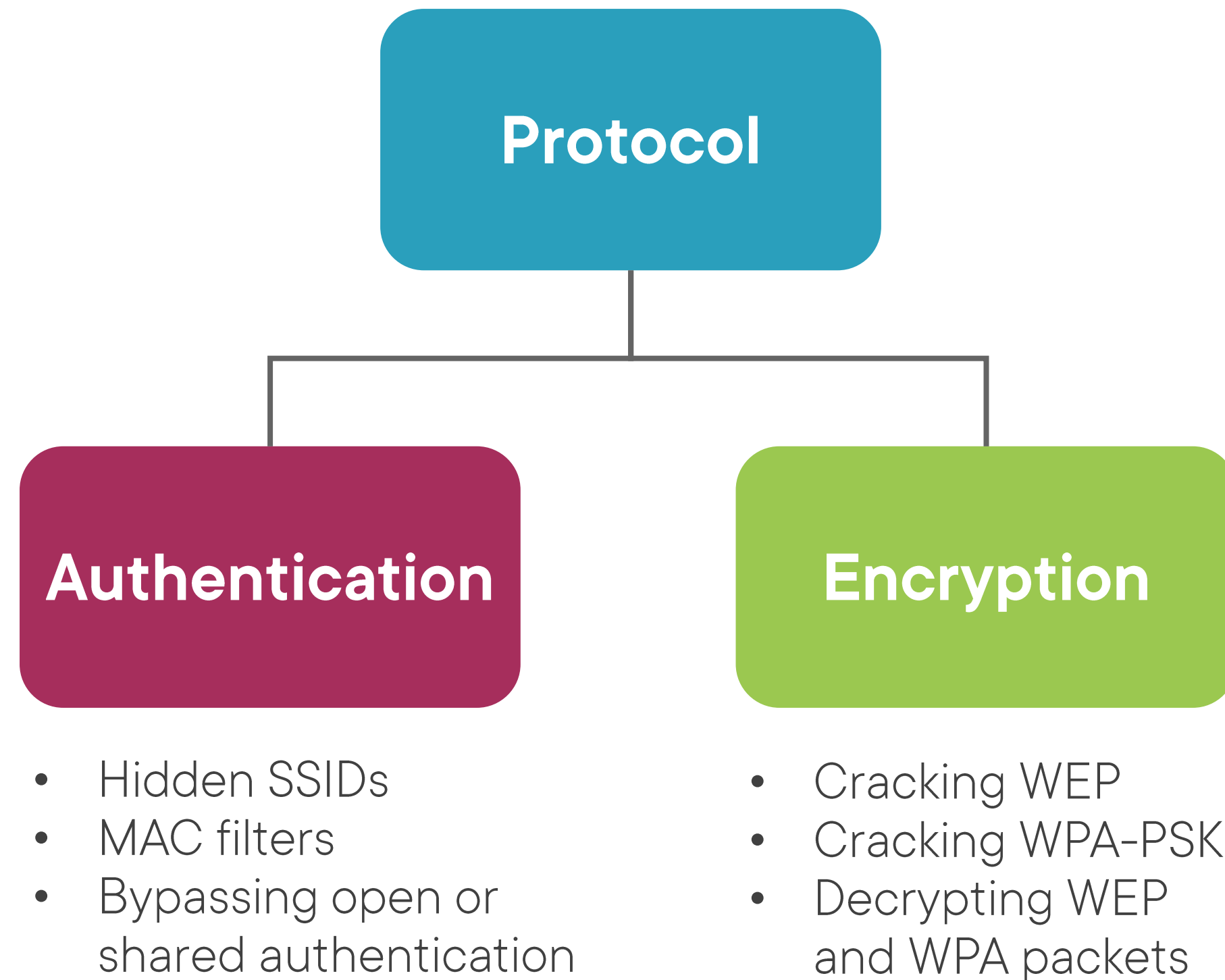
The Wireless Attack Surface



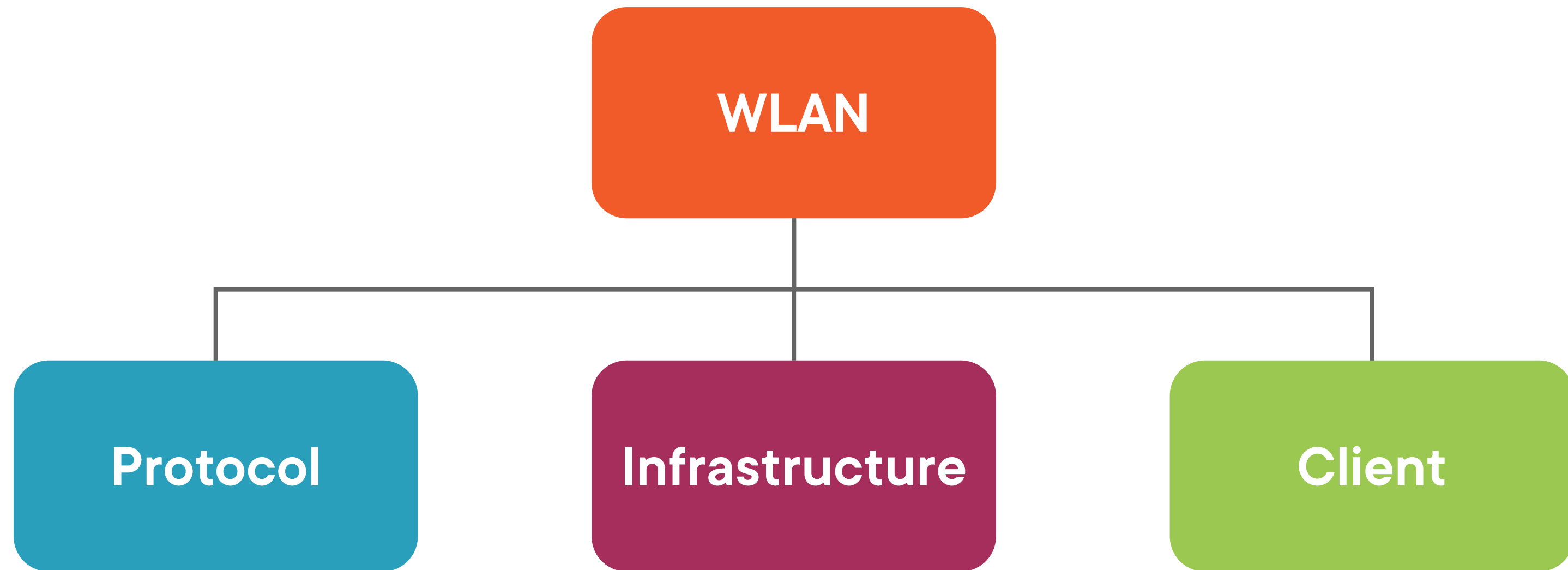
The Wireless Attack Surface



The Wireless Attack Surface



The Wireless Attack Surface



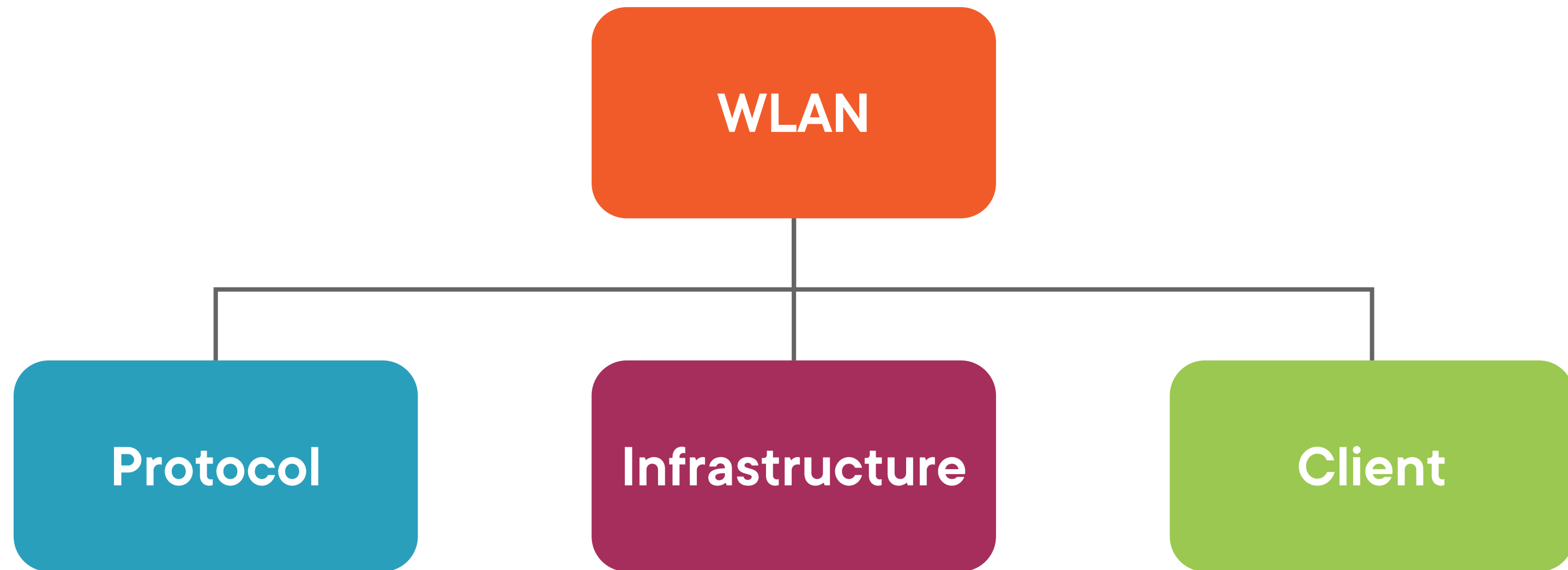
The Wireless Attack Surface

Infrastructure

- Cracking default accounts
- Deauth DoS attack
- Rogue access point
- Captive Portal
- Evil twin



The Wireless Attack Surface



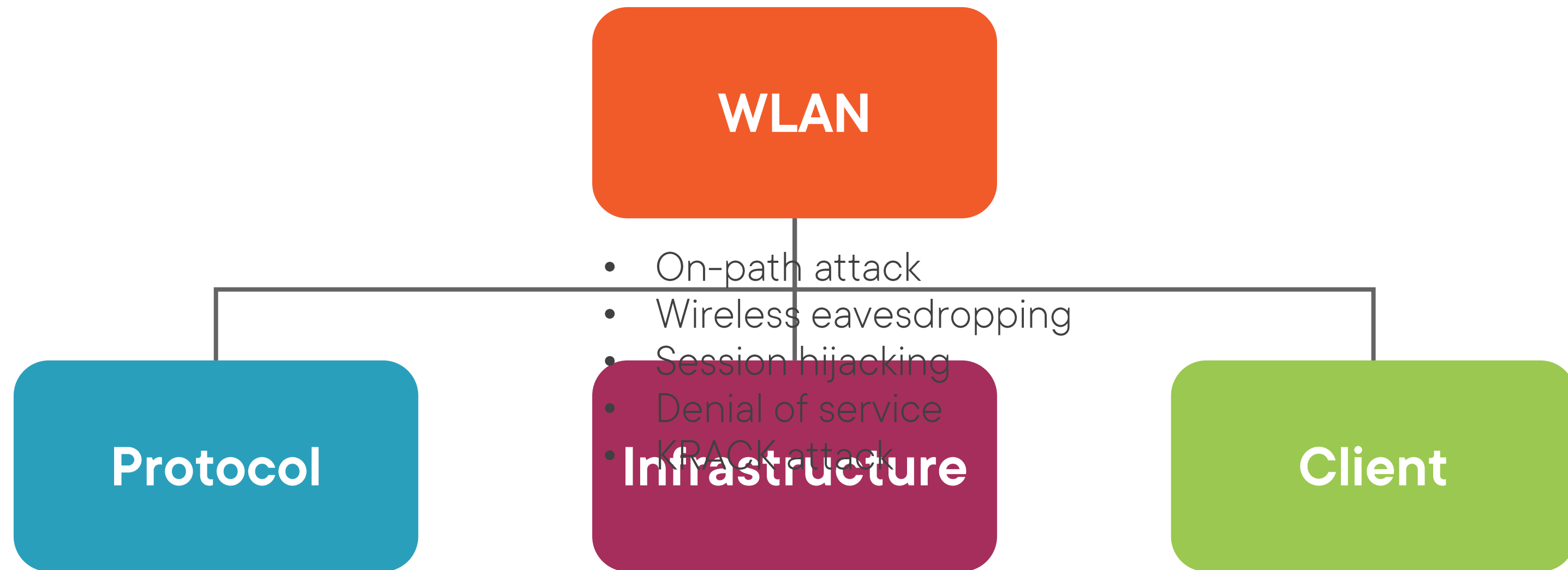
The Wireless Attack Surface

Client

- Mis-association attack
- Caffe Latte attack
- De-authenticating the client
- Cracking WEP with the Hirte attack
- AP-less WPA cracking



The Wireless Attack Surface



Course Pre-requisites

Linux command line basics

Networking

- TCP/IP
- Configuring wired and wireless networks

Radio concepts

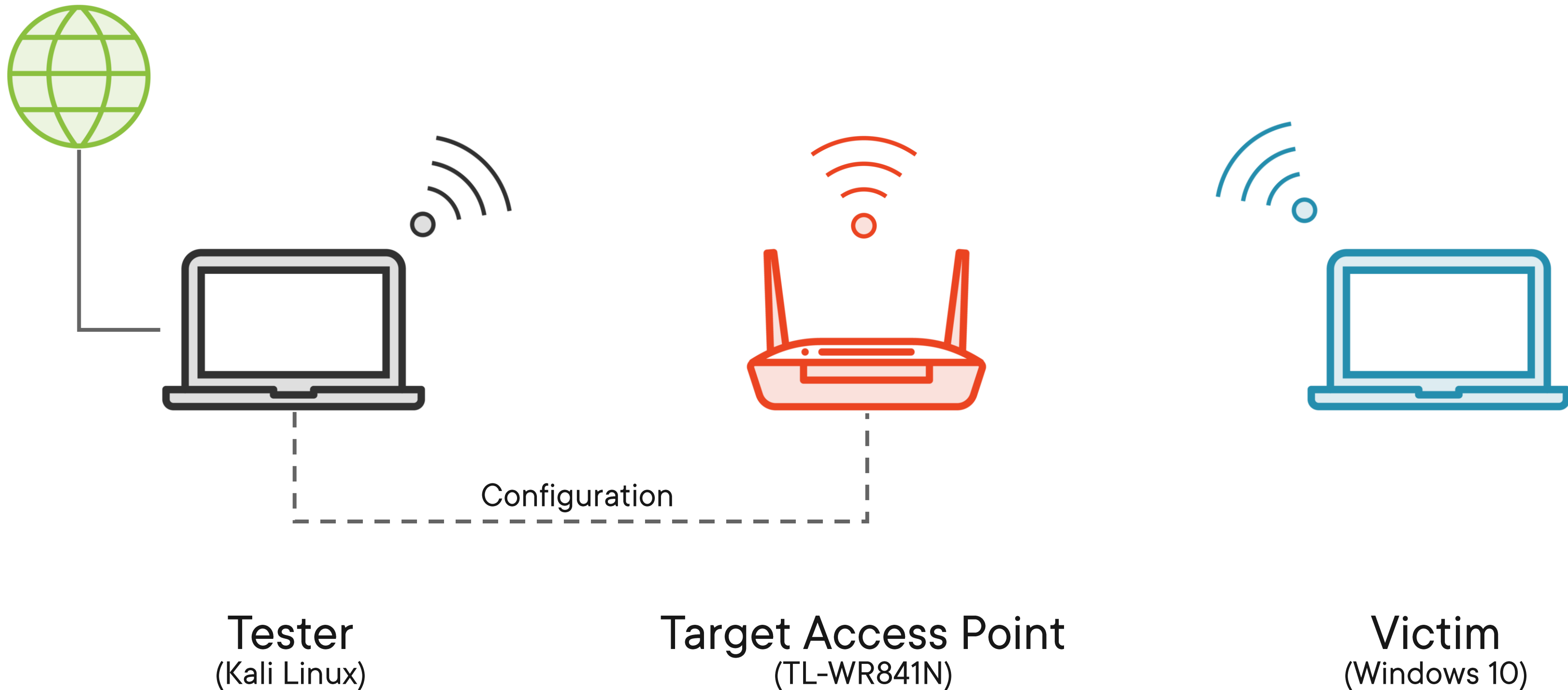
- Frequency, decibels, data rate, range



Building a Wireless Test Environment



Wireless Test Environment



tp-link

TP-Link Wireless N Router WR841N

Model No. TL-WR841N

Status

Quick Setup

Operation Mode

Network

Wireless

Guest Network

DHCP

Forwarding

Security

Parental Controls

Access Control

Advanced Routing

Bandwidth Control

IP & MAC Binding

Dynamic DNS

IPv6

System Tools

Logout

Status

LAN

Wireless 2.4GHz

WAN

Firmware Version:

0.9.1 4.17 v0001.0 Build 200903 Rel.58674n

Hardware Version:

TL-WR841N v14 00000014

MAC Address:

5C:A6:E6:B9:99:8A

IP Address:

192.168.0.1

Subnet Mask:

255.255.255.0

Operation Mode:

Router

Wireless Radio:

Enabled

Name(SSID):

TP-Link_998A

Mode:

11bgn mixed

Channel:

Auto(Channel 10)

Channel Width:

Auto

MAC Address:

5C:A6:E6:B9:99:8A

MAC Address:

5C:A6:E6:B9:99:8A

Support

App

Status Help

The **Status** page displays the Router's current status and configuration. All information is read-only.

LAN

The following parameters apply to the LAN port of the Router. You can configure them on the **Network -> LAN** page.

• MAC Address

- The physical address of the Router, as seen from the LAN.

• IP Address

- The LAN IP address of the Router.

• Subnet Mask

- The subnet mask associated with LAN IP address.

Wireless

These are the current settings or information for Wireless.You can configure them in the **Wireless -> Basic Settings** page.

• Operation Mode

- Indicates the mode which the device is working on.

• Wireless Radio

- Indicates whether the wireless radio feature of the Router is enabled or disabled.

• Name(SSID)

- The SSID of the Router.

• Mode

- The current wireless mode which the Router works on.

• Channel

- The current wireless channel in use.

• Channel Width

- The bandwidth of the wireless channel.

• MAC Address

- The physical address of the Router, as seen from the WLAN.

WAN

The following parameters apply to the WAN ports of the Router. You can configure them in the **Network -> WAN** page.

• MAC Address

- The physical address of the WAN port, as seen from the Internet.

• IP Address

- The current WAN (Internet) IP Address. This field will be blank or 0.0.0.0 if the IP Address is assigned dynamically and there is no connection to Internet.

• Subnet Mask

- The subnet mask associated with the WAN IP Address.

• Default Gateway

- The Gateway currently used by the Router is shown here.

• DNS Server

- The DNS (Domain Name System) Server IP addresses currently used by the Router. Multiple DNS IP settings are common. Usually, the first available DNS Server is used.

• Online Time

- The time that you are online. When you use PPPoE as WAN connection type, the online time is displayed here.

Secondary Connection

The Secondary Connection will be shown in this area.

tp-link

Status

Quick Setup

Operation Mode

Network

Wireless

- Basic Settings

- WPS

- Wireless Security

- Wireless MAC Filtering

- Wireless Advanced

- Wireless Statistics

Guest Network

DHCP

Forwarding

Security

Parental Controls

Access Control

Advanced Routing

Bandwidth Control

IP & MAC Binding

Dynamic DNS

IPv6

System Tools

Logout

TP-Link Wireless N Router WR841N

Model No. TL-WR841N

Wireless Settings

Wireless:

☒ Enable ☐ Disable

Wireless Network Name:

TP-Link_998A

(Also called SSID)

Mode:

11bgn mixed

Channel:

Auto

Channel Width:

Auto

☒ Enable SSID Broadcast

Save

Wireless Settings Help

Note: The operating distance or range of your wireless connection varies significantly based on the physical placement of the Router. For best results, place your Router:

- Near the center of the area in which your wireless stations will operate.
- In an elevated location such as a high shelf.
- Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
- With the Antenna in the upright position.
- Away from large metal surfaces.

Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the Router.

Wireless Network Name - Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network.

Mode - You can choose the appropriate "Mixed" mode.

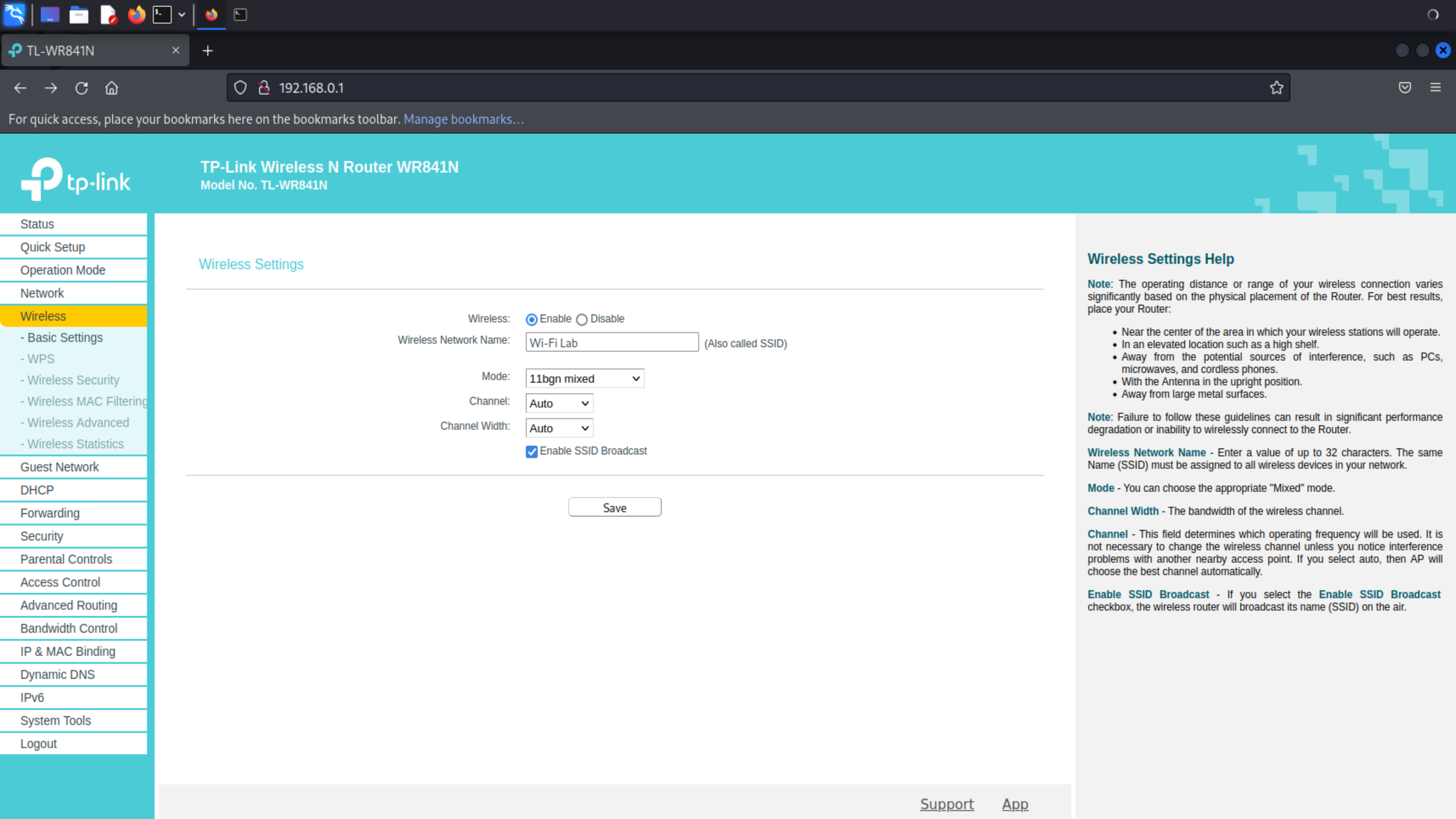
Channel Width - The bandwidth of the wireless channel.

Channel - This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point. If you select auto, then AP will choose the best channel automatically.

Enable SSID Broadcast - If you select the **Enable SSID Broadcast** checkbox, the wireless router will broadcast its name (SSID) on the air.

Support

App



TP-Link Wireless N Router WR841N
Model No. TL-WR841N

- Status
- Quick Setup
- Operation Mode
- Network
- Wireless
 - Basic Settings
 - WPS
 - Wireless Security
 - Wireless MAC Filtering
 - Wireless Advanced
 - Wireless Statistics
- Guest Network
- DHCP
- Forwarding
- Security
- Parental Controls
- Access Control
- Advanced Routing
- Bandwidth Control
- IP & MAC Binding
- Dynamic DNS
- IPv6
- System Tools
- Logout

Wireless Settings

Wireless: ☒ Enable ☐ Disable

Wireless Network Name: (Also called SSID)

Mode:

Channel:

Channel Width:

☒ Enable SSID Broadcast

Save

Wireless Settings Help

Note: The operating distance or range of your wireless connection varies significantly based on the physical placement of the Router. For best results, place your Router:

- Near the center of the area in which your wireless stations will operate.
- In an elevated location such as a high shelf.
- Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
- With the Antenna in the upright position.
- Away from large metal surfaces.

Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the Router.

Wireless Network Name - Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network.

Mode - You can choose the appropriate "Mixed" mode.

Channel Width - The bandwidth of the wireless channel.

Channel - This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point. If you select auto, then AP will choose the best channel automatically.

Enable SSID Broadcast - If you select the **Enable SSID Broadcast** checkbox, the wireless router will broadcast its name (SSID) on the air.

Wireless Network Security Testing Tools

air-crack-ng

- aircrack-ng.org

Wireshark

- wireshark.org

create_ap

- github.com/oblique/create_ap

macchanger

- github.com/alobbs/macchanger

dnsspoof

- github.com/tecknicaltom/dsniff



aircrack-ng
Suite

airmon-ng

aireplay-ng

aircrack-ng

airodump-ng



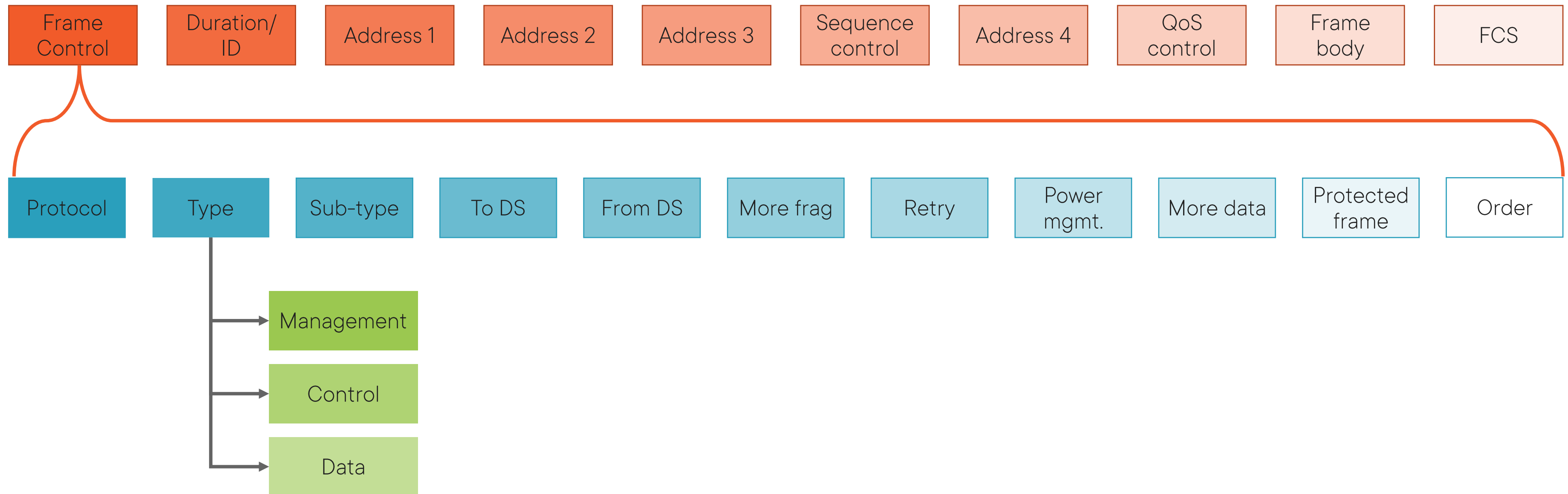
Demo



Sniffing and dissecting Wi-Fi frames



WLAN Frames



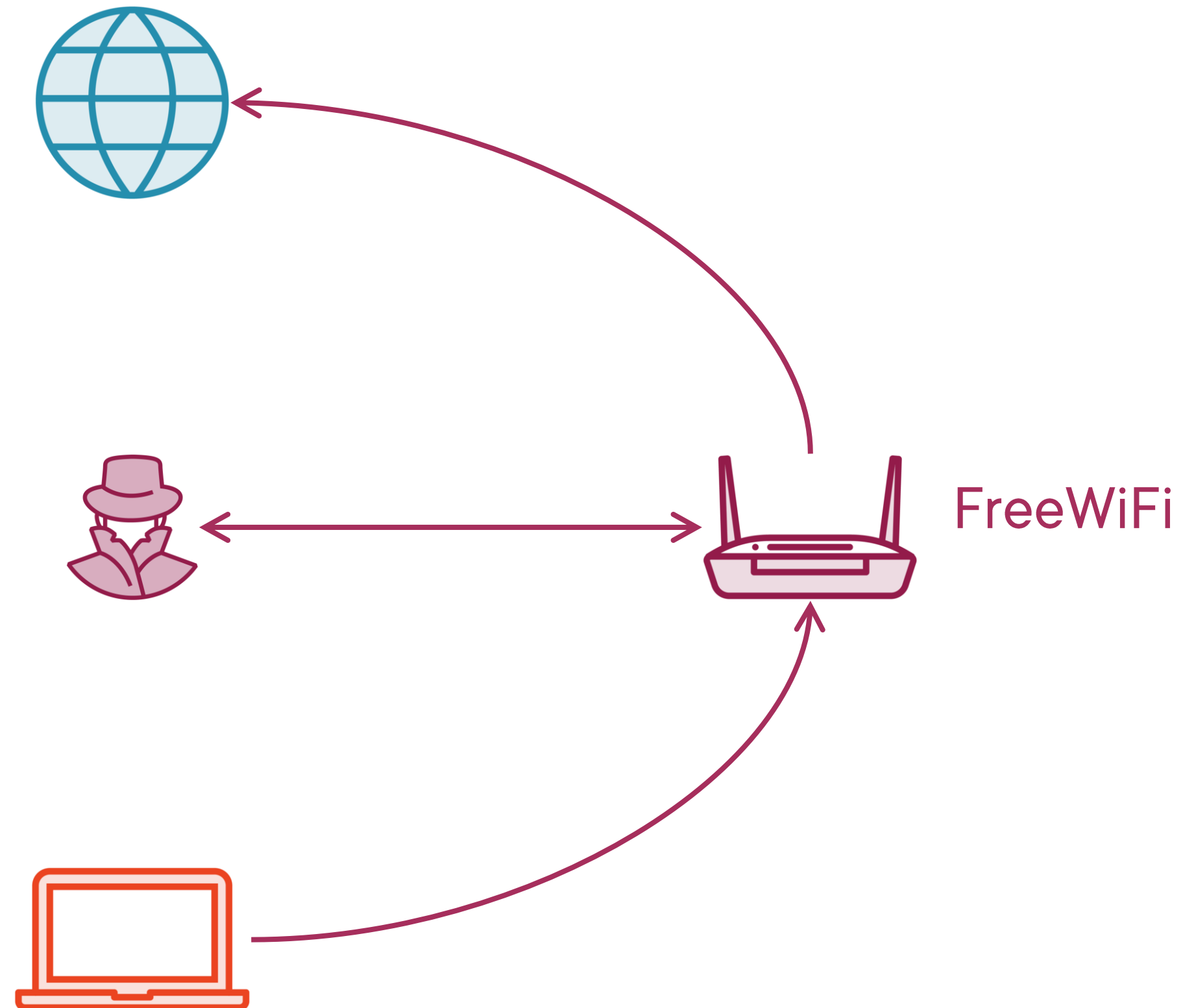
Demo



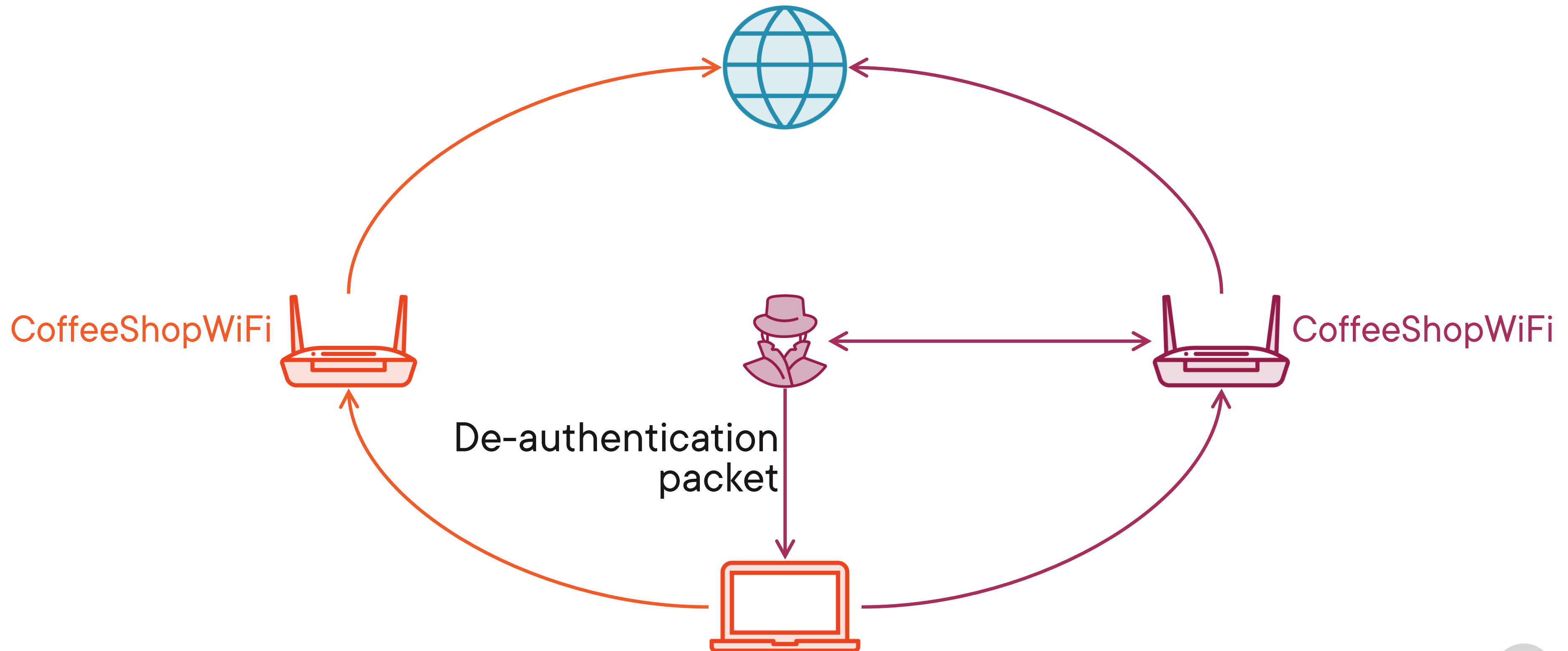
Creating a rogue access point



Rogue Access Point



Evil Twin



Up Next: Exploiting Wireless Authentication Weaknesses

