

Introduction to WiFi Networking

Training materials for wireless trainers



The Abdus Salam
**International Centre
for Theoretical Physics**

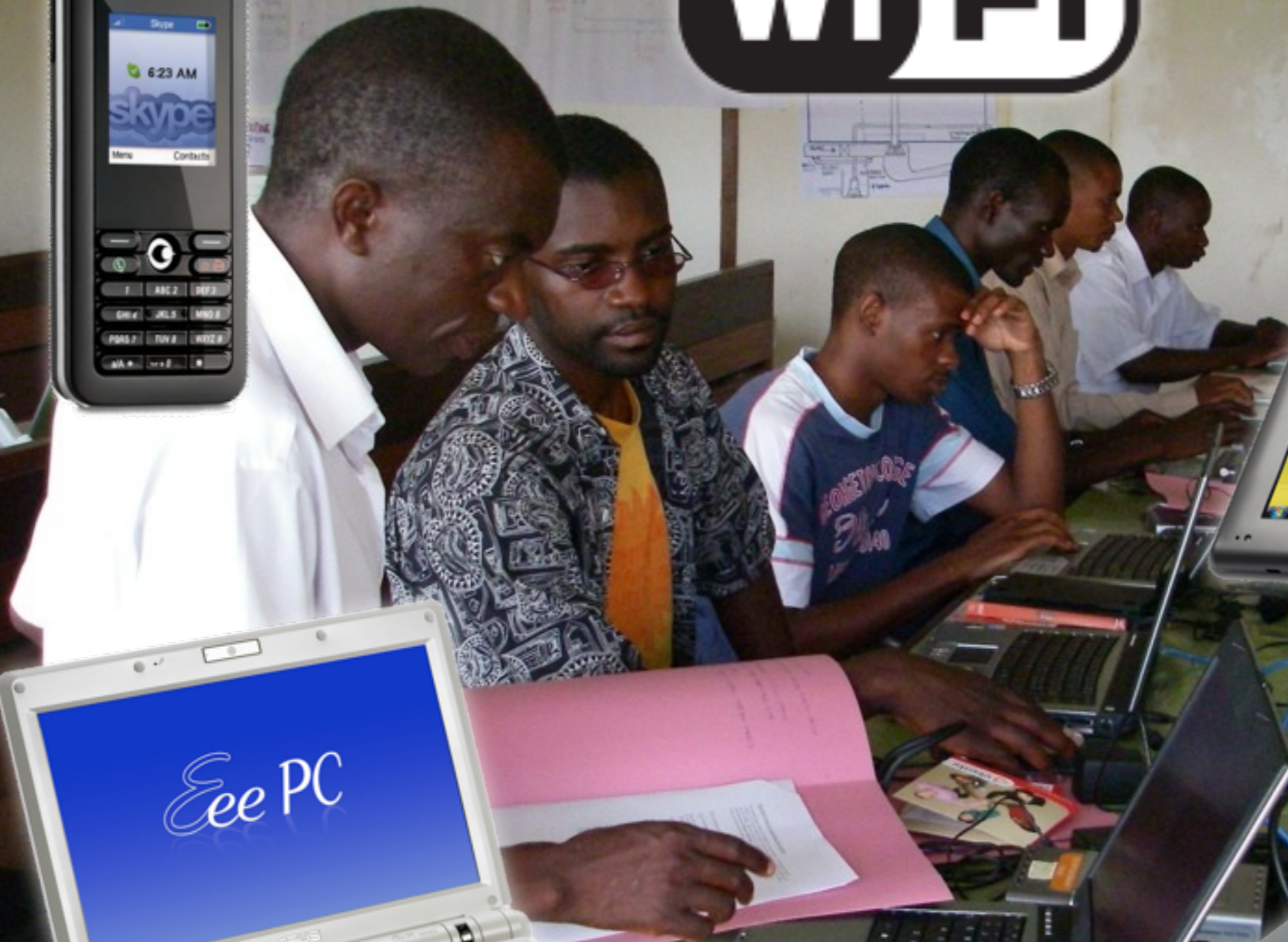


Goals

The goal of this lecture is to introduce:

- ▶ 802.11 family of radio protocols
- ▶ 802.11 radio channels
- ▶ Wireless network topologies
- ▶ WiFi modes of operation
- ▶ Strategies for routing network traffic
- ▶ Frequently Asked Questions

WiFi™



ISM / UNII bands

Most commercial wireless devices (mobile phones, television, radio, etc.) use licensed radio frequencies. Large organizations pay licensing fees for the right to use those radio frequencies.

WiFi uses unlicensed spectrum. License fees are not usually required to operate WiFi equipment.

- ▶ The *Industrial, Scientific and Medical (ISM)* bands allow for unlicensed use of 2.4-2.5 GHz, 5.8 GHz, and many other (non-WiFi) frequencies.
- ▶ The *Unlicensed National Information Infrastructure (UNII)* bands allow for unlicensed use of the lower part of the 5 GHz spectrum (USA only).
- ▶ In Europe, the *European Telecommunication Standards Institute (ETSI)* has allocated portions of the 5 GHz band.

Wireless networking protocols

The 802.11 family of radio protocols are commonly referred to as WiFi.

- **802.11a** supports up to 54 Mbps using the 5 GHz unlicensed bands.
- **802.11b** supports up to 11 Mbps using the 2.4 GHz unlicensed band.
- **802.11g** supports up to 54 Mbps using the 2.4 GHz unlicensed band.
- **802.11n** supports up to 600 Mbps using the 2.4 GHz and 5 GHz unlicensed bands.

- **802.16** (WiMAX) is not 802.11 WiFi! It is a completely different technology that uses a variety of licensed and unlicensed frequencies.

Compatibility of standards

AP

C
L
I
E
N
T

	802.11a	802.11b	802.11g	802.11n	802.16
802.11a	Yes			Yes @5GHz	
802.11b		Yes	Yes (slower)	Yes @2.4GHz	
802.11g		Yes (slower)	Yes	Yes @2.4GHz	
802.11n	Yes @5GHz	Yes @2.4GHz	Yes @2.4GHz	Yes	
802.16					Yes

Data rates

Note that the “data rates” quoted in the WiFi specifications refer to the raw radio symbol rate, not the actual TCP/IP throughput rate. The difference is called **protocol overhead**, and is needed by the WiFi protocol to manage collisions, retransmissions, and general management of the link.

A good rule of thumb is to divide the radio symbol rate by two to obtain the maximum practical TCP/IP throughput. For example, a 54 Mbps 802.11a link has a maximum practical throughput of roughly 25 Mbps. An 11 Mbps 802.11b link has a maximum throughput of about 5 Mbps.

MAC layer: CSMA vs. TDMA

802.11 WiFi uses **Carrier Sense Multiple Access (CSMA)** to avoid transmission collisions. Before a node may transmit, it must first listen for transmissions from other radios. The node may only transmit when the channel becomes idle.

Other technologies (such as WiMAX, Nstreme, and AirMAX) use **Time Division Multiple Access (TDMA)** instead. TDMA divides access to a given channel into multiple time slots, and assigns these slots to each node on the network. Each node transmits only in its assigned slot, thereby avoiding collisions.

Layer one

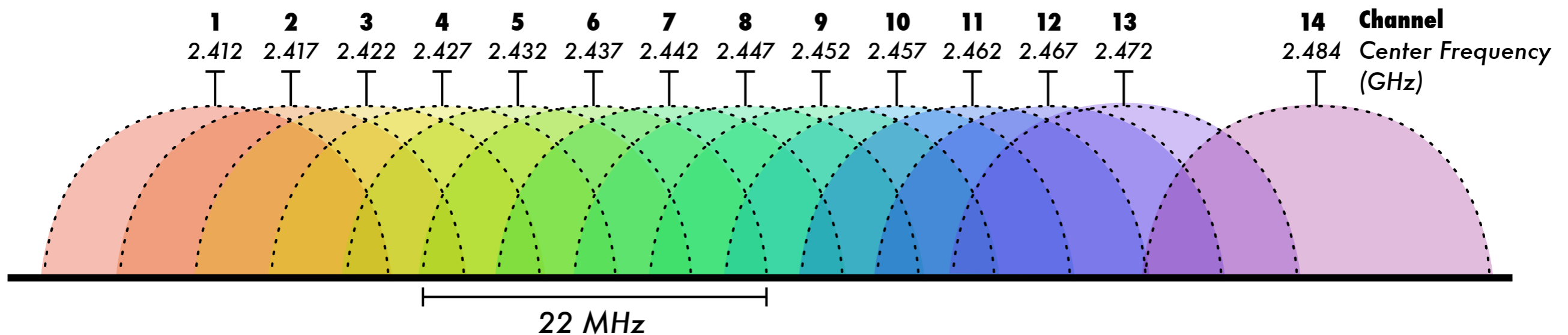
WiFi devices must agree on several parameters before they can communicate with each other. These parameters must be properly configured to establish “layer one” connectivity:

TCP/IP Protocol Stack	
5	Application
4	Transport
3	Internet
2	Data Link
1	Physical

- Radio channel
- Radio operating mode
- Network name
- Security features

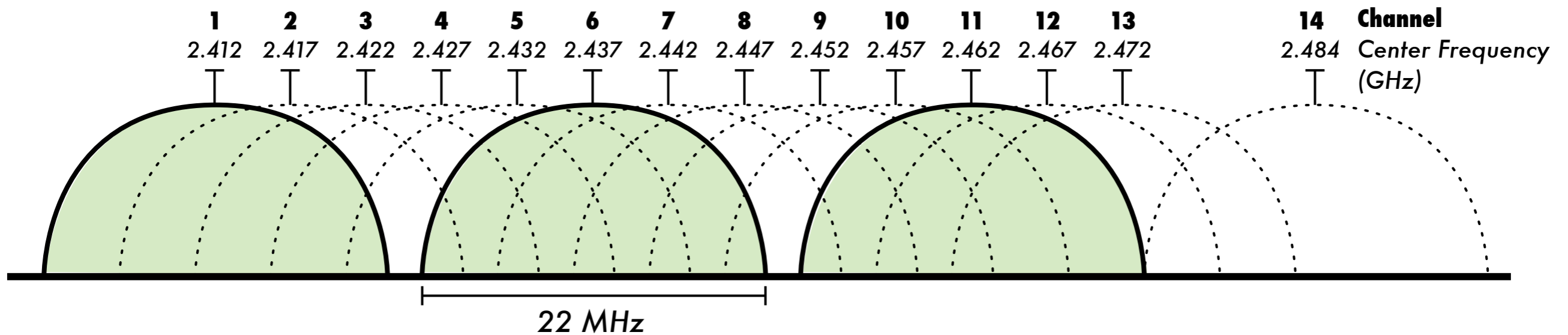


802.11 WiFi Channels

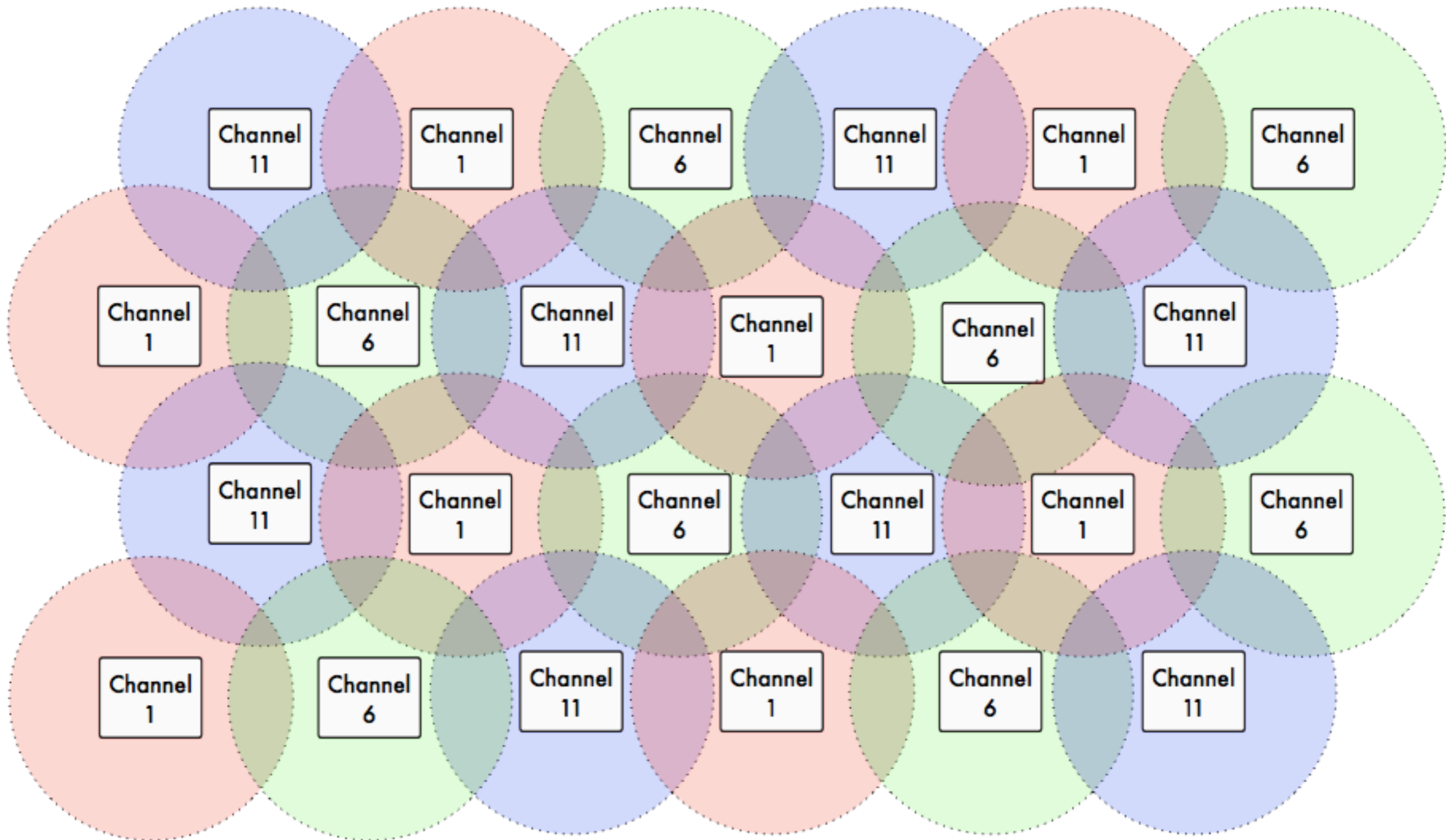


WiFi devices must use the same channel in order to communicate with each other. They send and receive on the same channel, so only one device may transmit at any time. This kind of connection is called **half-duplex**.

Non-overlapping channels: 1, 6, 11



AP channel re-use



Wireless network topologies

Any complex wireless network can be thought of as a combination of one or more of these types of connections:

- ▶ ***Point-to-Point***

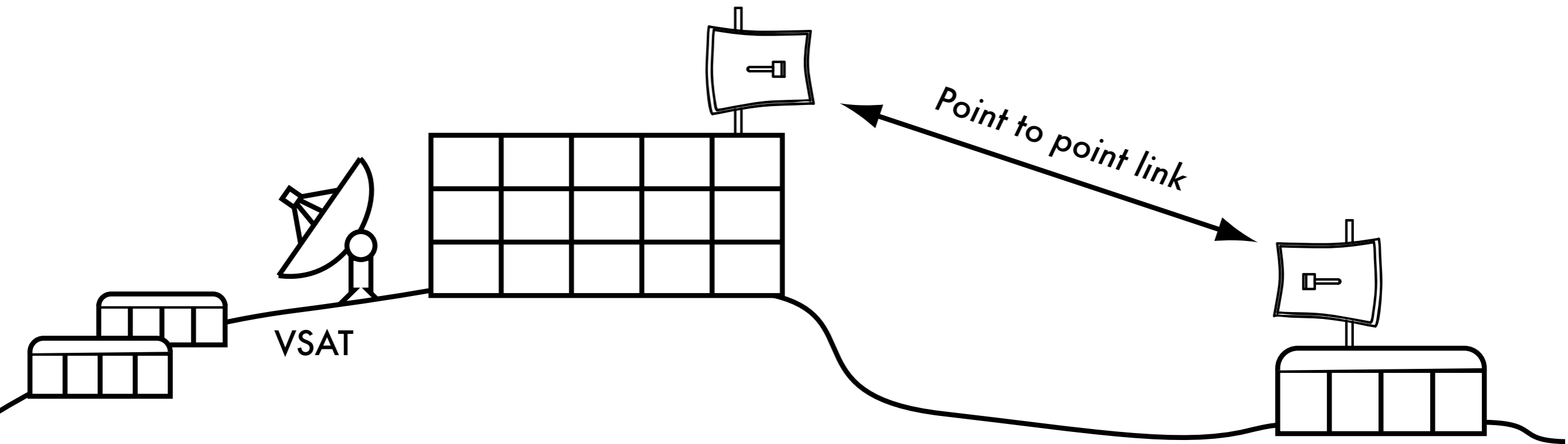
- ▶ ***Point-to-Multipoint***

- ▶ ***Multipoint-to-Multipoint***

Point to Point

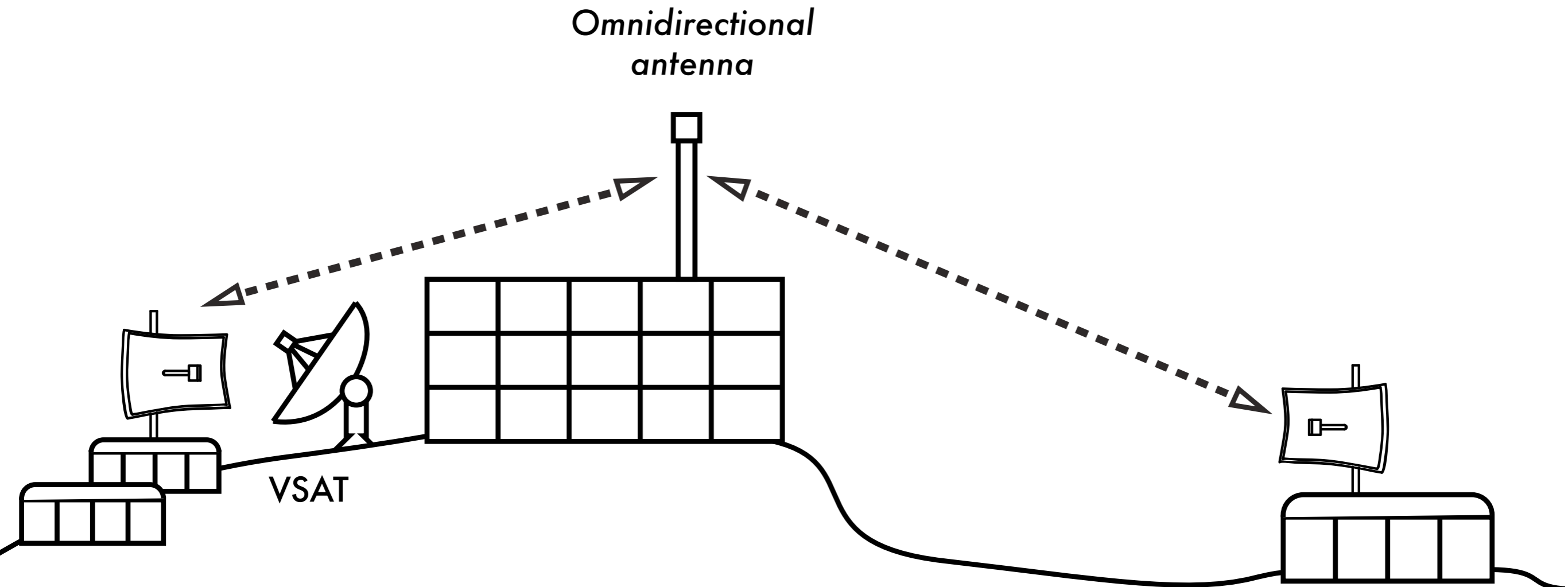
The simplest connection is the ***point-to-point*** link.

These links can be used to extend a network over great distances.



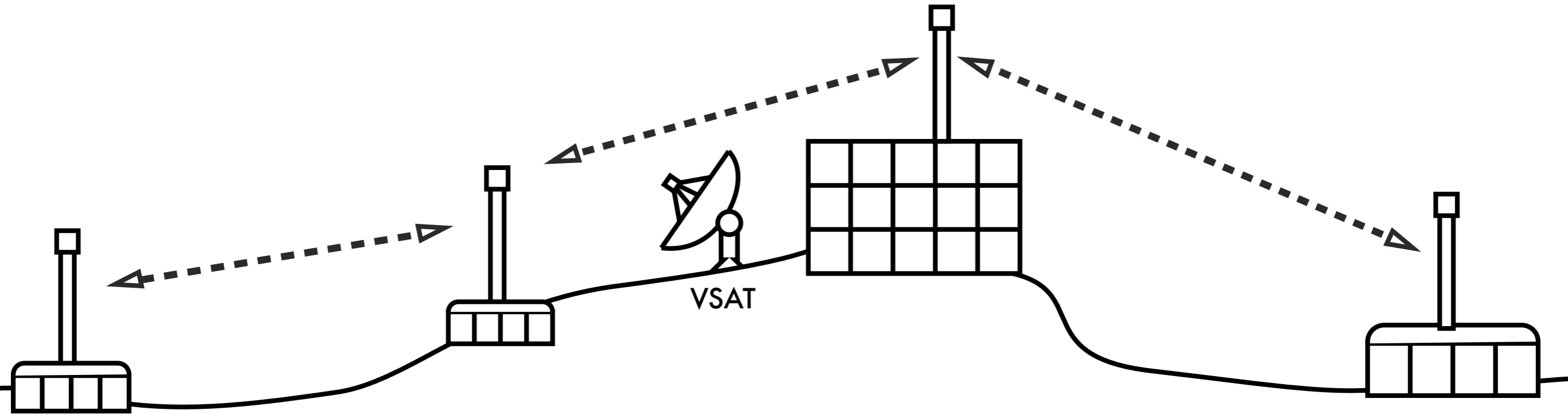
Point to Multipoint

When more than one node communicates with a central point, this is a ***point-to-multipoint*** network.



Multipoint to Multipoint

When any node of a network may communicate with any other, this is a ***multipoint-to-multipoint*** network (also known as an ***ad-hoc*** or ***mesh*** network).



WiFi radio modes

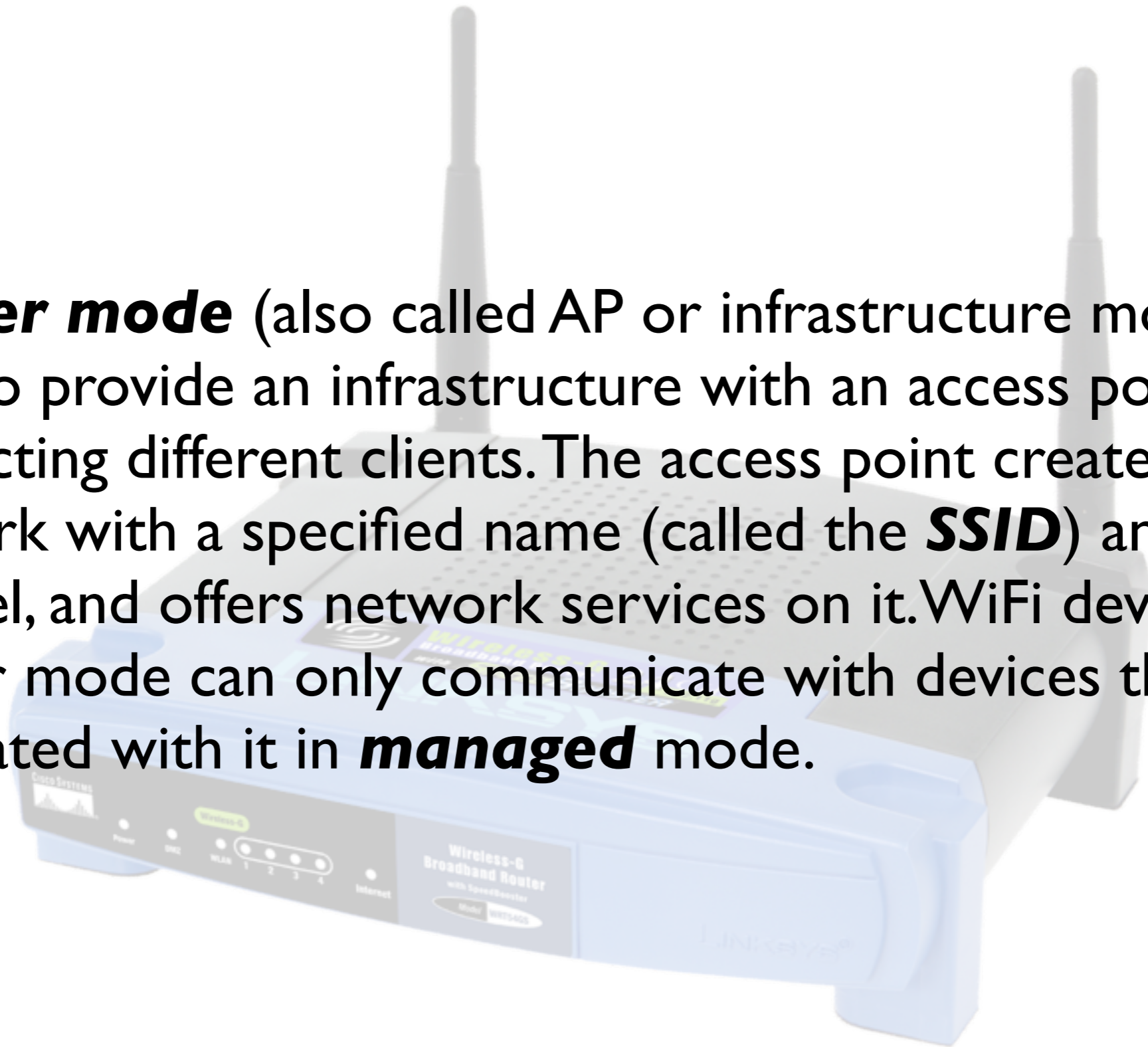
WiFi devices can be operated in one of these **modes**:

- ▶ **Master** (access point)
- ▶ **Managed** (also known as **client** or **station**)
- ▶ **Ad-hoc** (used for mesh networks)
- ▶ **Monitor** (not normally used for communications)
- ▶ Other proprietary non-802.11 modes (e.g. Mikrotik Nstreme or Ubiquiti AirMAX)

Each mode has specific operating constraints, and radios may only operate in one mode at a time.

Master mode

Master mode (also called AP or infrastructure mode) is used to provide an infrastructure with an access point connecting different clients. The access point creates a network with a specified name (called the **SSID**) and channel, and offers network services on it. WiFi devices in master mode can only communicate with devices that are associated with it in **managed** mode.



Managed Mode

Managed mode is sometimes also referred to as **client mode**. Wireless devices in managed mode will join a network created by a master, and will automatically change their channel to match it. *See PC*

Clients using a given access point are said to be **associated** with it. Managed mode radios do not communicate with each other directly, and will only communicate with an associated master (and only with one at a time).

Ad-hoc Mode

Ad-hoc mode is used to create mesh networks with:

- ▶ No master devices (APs)
- ▶ Direct communication between neighbors

Devices must be in range of each other to communicate, and they must agree on a network name and channel.



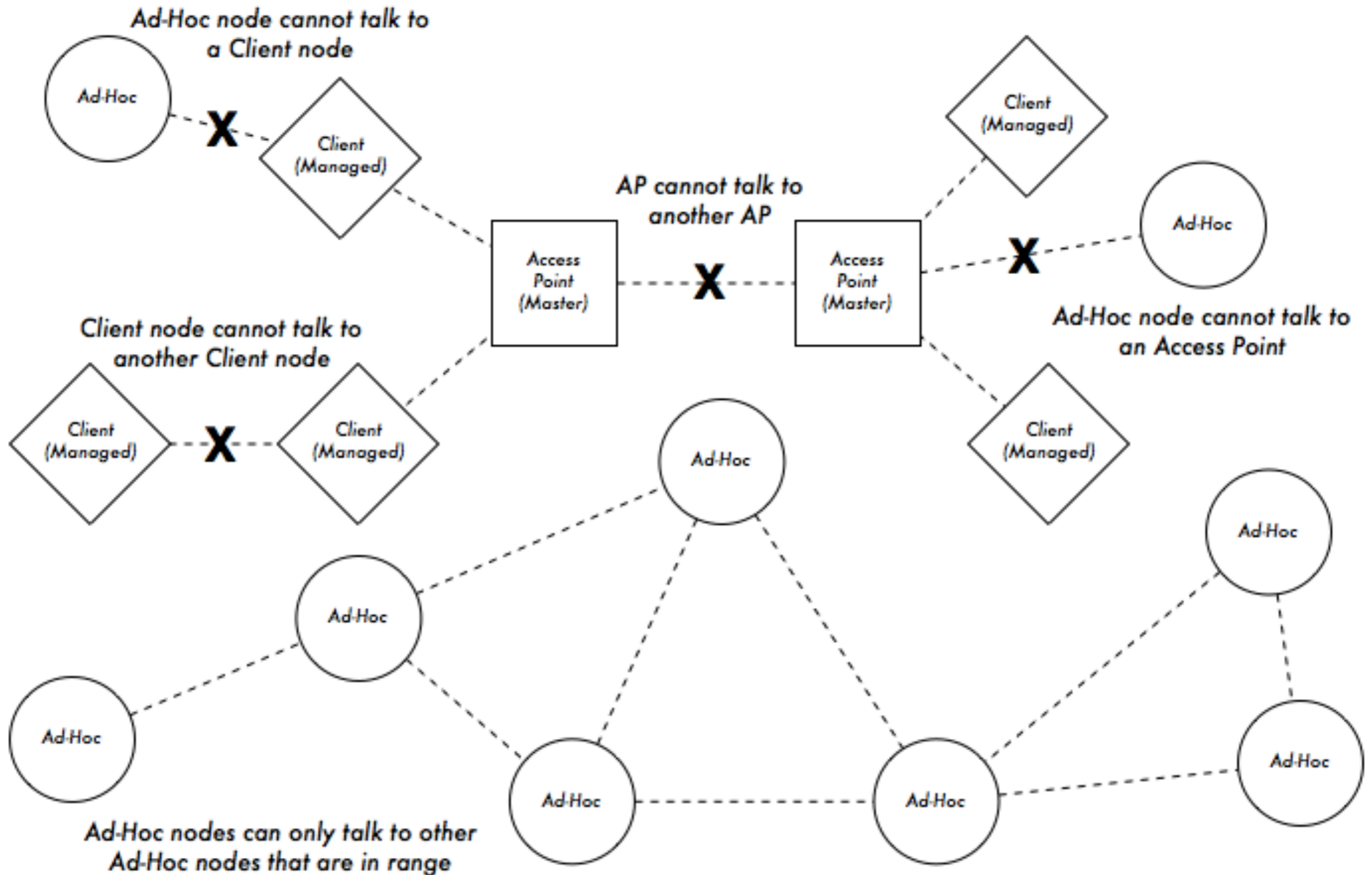
Monitor Mode

Monitor mode is used to passively listen to all radio traffic on a given channel. This is useful for:



- ▶ Analyzing problems on a wireless link
- ▶ Observing spectrum usage in the local area
- ▶ Performing security maintenance tasks

WiFi radio modes in action



Wireless Distribution System (WDS)


It is possible to allow Access Points to communicate with each other directly by using the WDS protocol. It can be useful, but it has several limitations.

- ▶ WDS may not be compatible with equipment from different vendors.
- ▶ Since WiFi is half-duplex, the maximum throughput is halved at each hop.
- ▶ WDS only supports a small number of connected APs (typically five).
- ▶ WDS cannot support some security features, such as WPA encryption.

Routing traffic

802.11 WiFi provides a link-local connection. It does **not** provide any routing functionality! Routing is implemented by higher level protocols.

TCP/IP Protocol Stack	
5	Application
4	Transport
3	Internet
2	Data Link
1	Physical



WiFi

Bridged networking

For a simple local area wireless network, a bridged architecture is usually adequate.

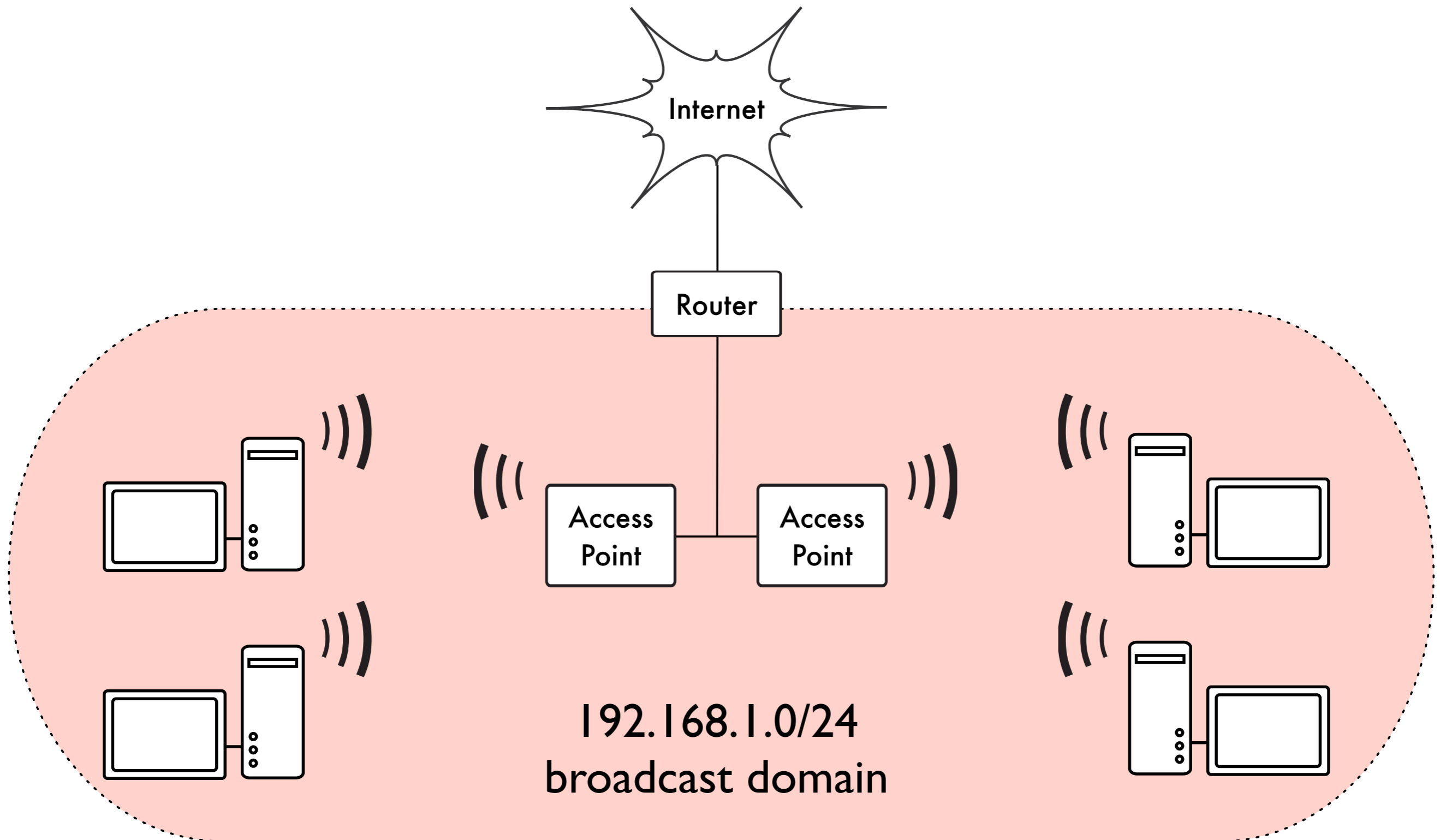
Advantages

- ▶ Very simple configuration
- ▶ Roaming works very well

Disadvantages

- ▶ Increasingly inefficient as nodes are added
- ▶ All broadcast traffic is repeated
- ▶ Virtually unusable on very large wide-area networks

Bridged access points



Routed networking

Large networks are built by applying **routing** between nodes.

- ▶ **Static routing** is often used on point-to-point links.
- ▶ **Dynamic routing** (such as RIP or OSPF) can be used on larger networks, although they are not designed to work with imperfect wireless links.
- ▶ **Mesh routing protocols** work very well with wireless networks, particularly when using radios in ad-hoc mode.

Routed networking

As the network grows, it becomes necessary to use some sort of routing scheme to maintain traffic efficiency.

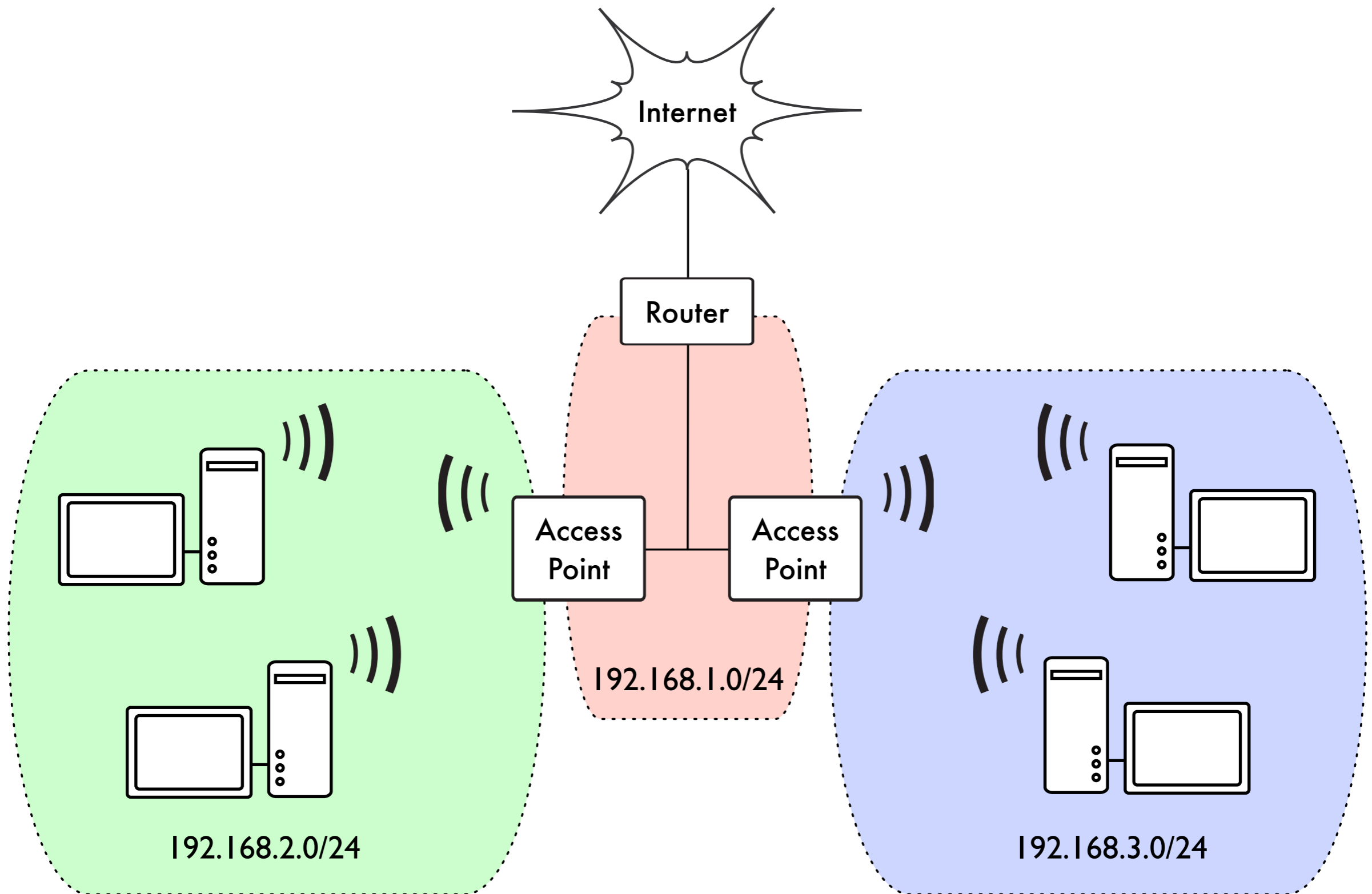
Advantages

- ▶ Broadcast domains are limited, making more efficient use of radio bandwidth
- ▶ Arbitrarily large networks can be made
- ▶ A variety of routing protocols and bandwidth management tools are available

Disadvantages

- ▶ More complex configuration
- ▶ Roaming between APs is not supported

Routed access points



Frequently Asked Questions

Frequently Asked Questions

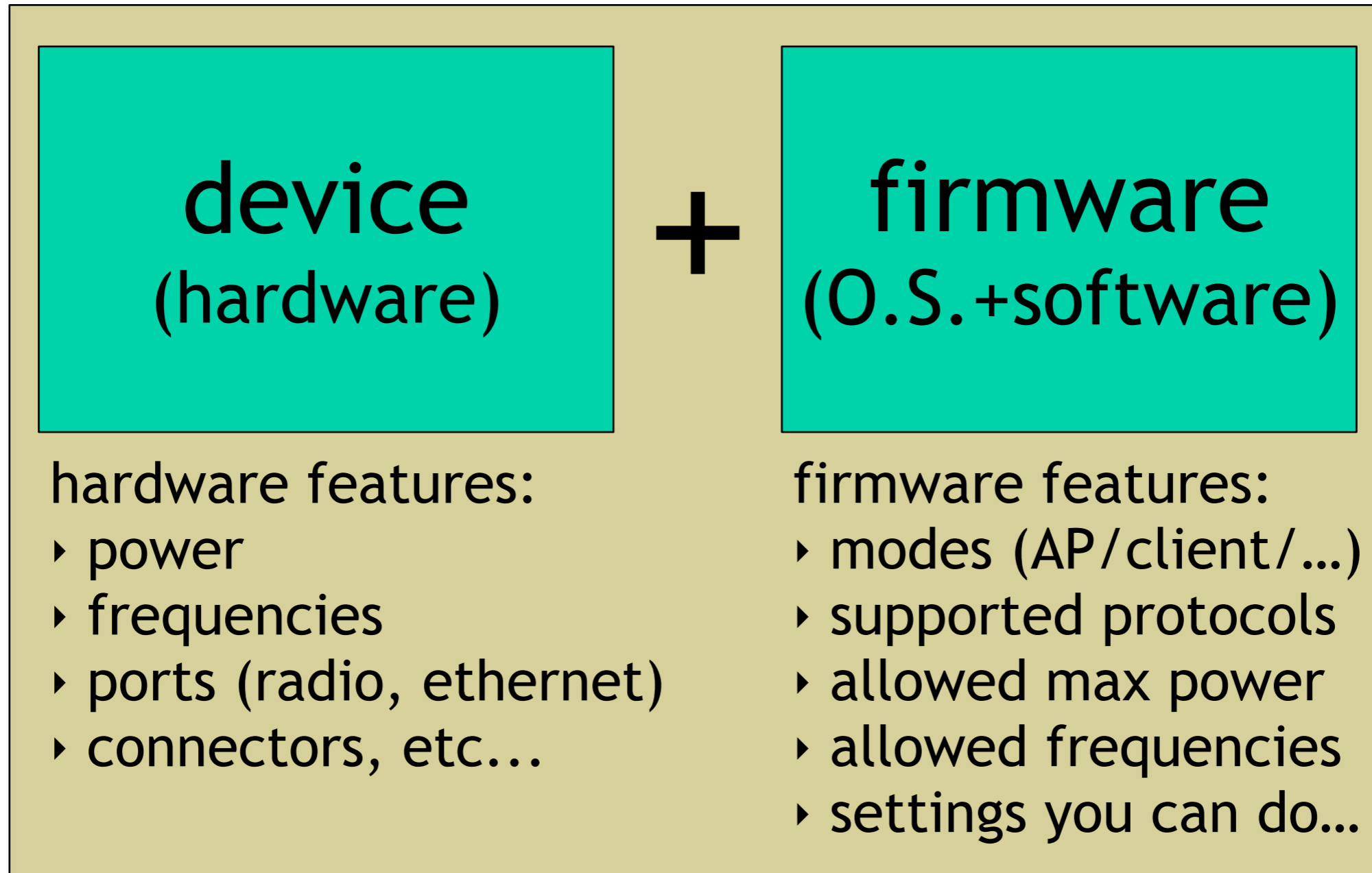
- ▶ How fast? (What does 54Mbps mean ???)
- ▶ How far can a network go? (the distance problem)
- ▶ How many clients can I connect to an AP?
- ▶ Are all my devices compatible?
- ▶ There are sometimes huge differences in price of APs, what should I buy?

A few important concepts

I can give you answers to some questions, indeed :-)

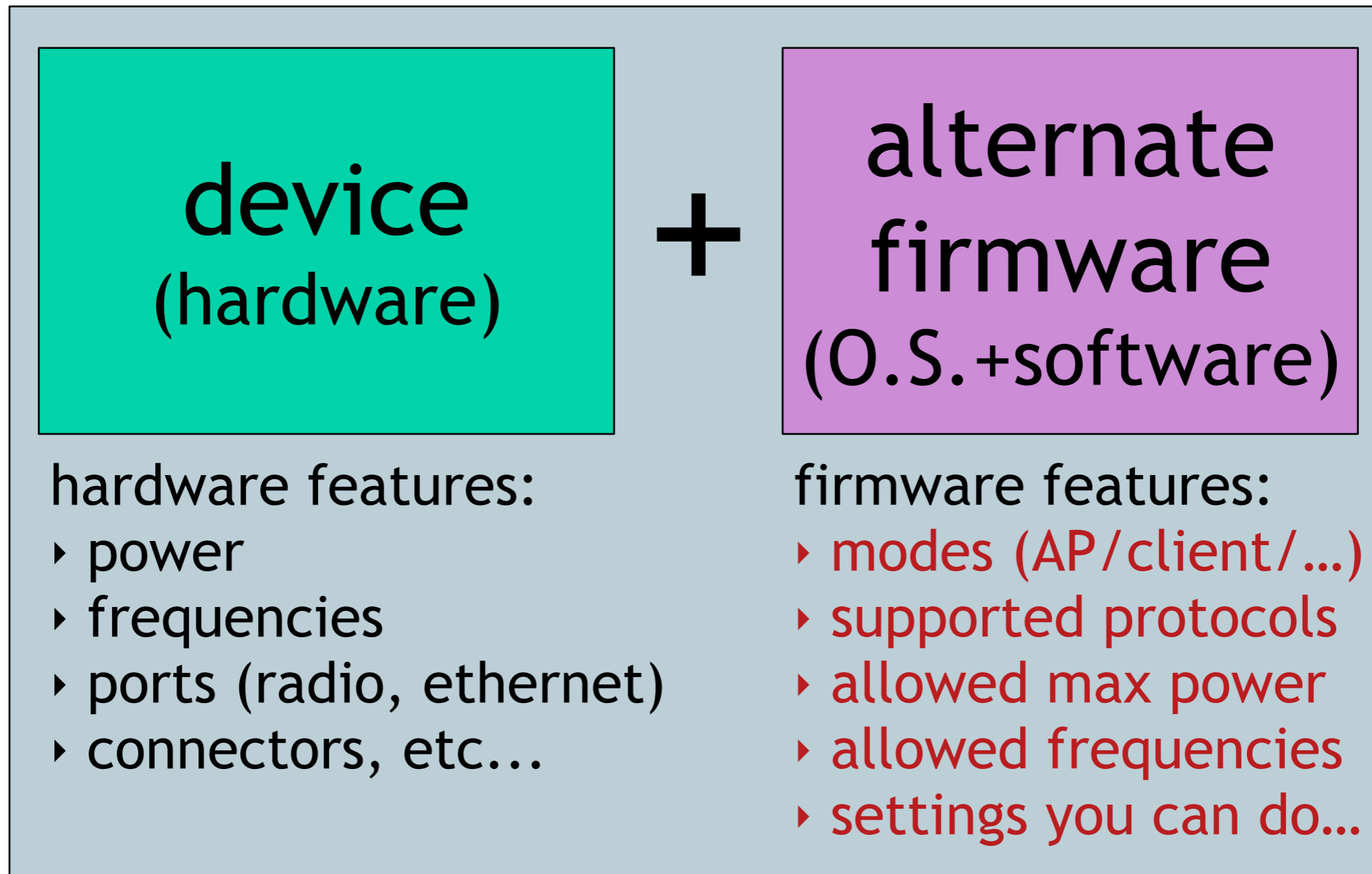
- ▶ What is a *device*?
- ▶ What is an Access Point (AP)? Can it be also a client? Are they *different* hardware?
- ▶ What is firmware? Why may I want to change it?
- ▶ I don't understand the differences between AP, device, firmware, protocols...

A few important concepts



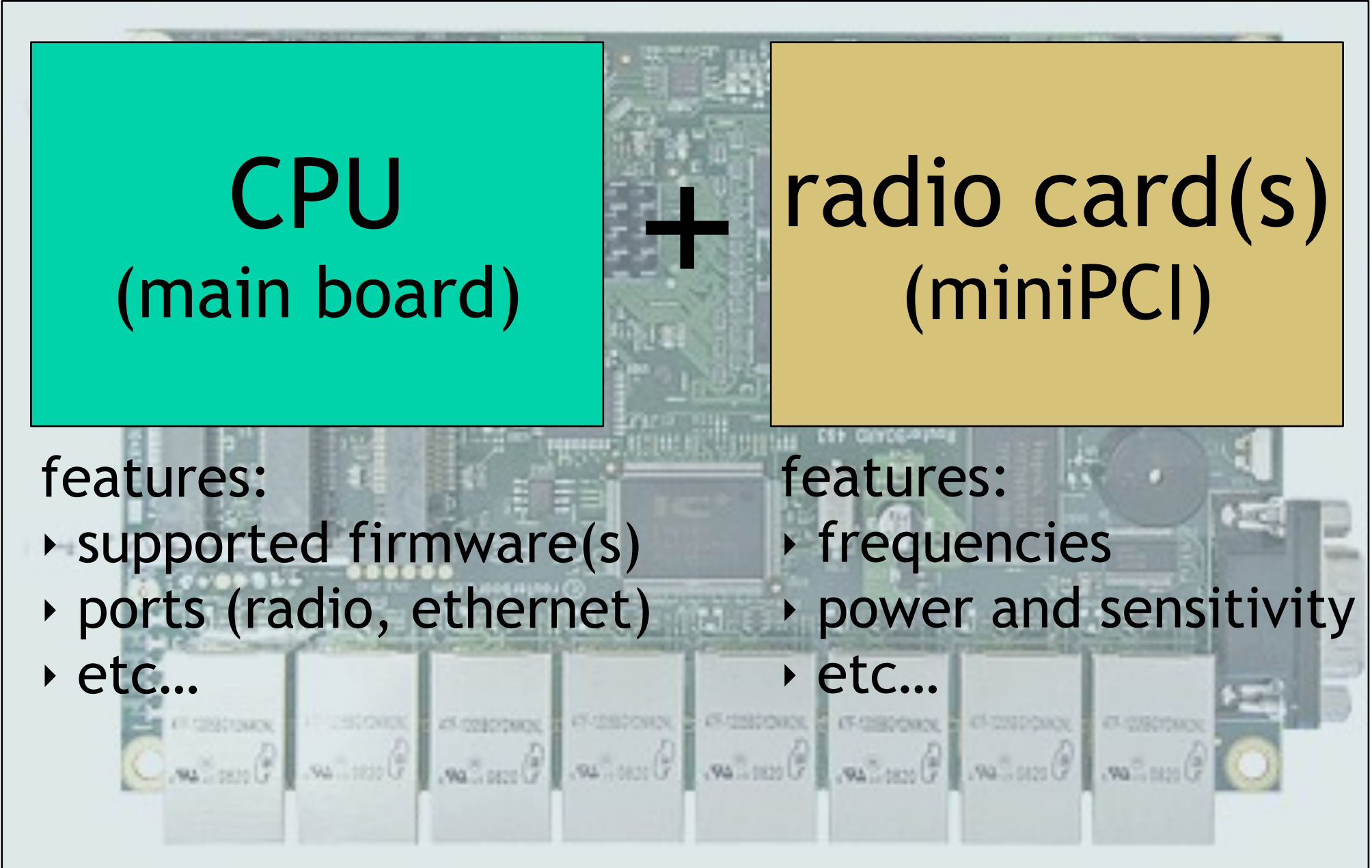
all of this together makes up your AP/client

Alternate firmware



the same device *with an alternate firmware*:
it may have some *new or better features*

Modular hardware

The diagram shows a central image of a circuit board with several components highlighted. On the left, a teal box contains the text 'CPU (main board)'. In the center, a large black plus sign is superimposed over the board. On the right, a yellow box contains the text 'radio card(s) (miniPCI)'. Below these boxes are two bulleted lists of features for each component. The background is a faded image of a circuit board with several radio cards inserted into slots.

CPU
(main board)

features:

- ▶ supported firmware(s)
- ▶ ports (radio, ethernet)
- ▶ etc...

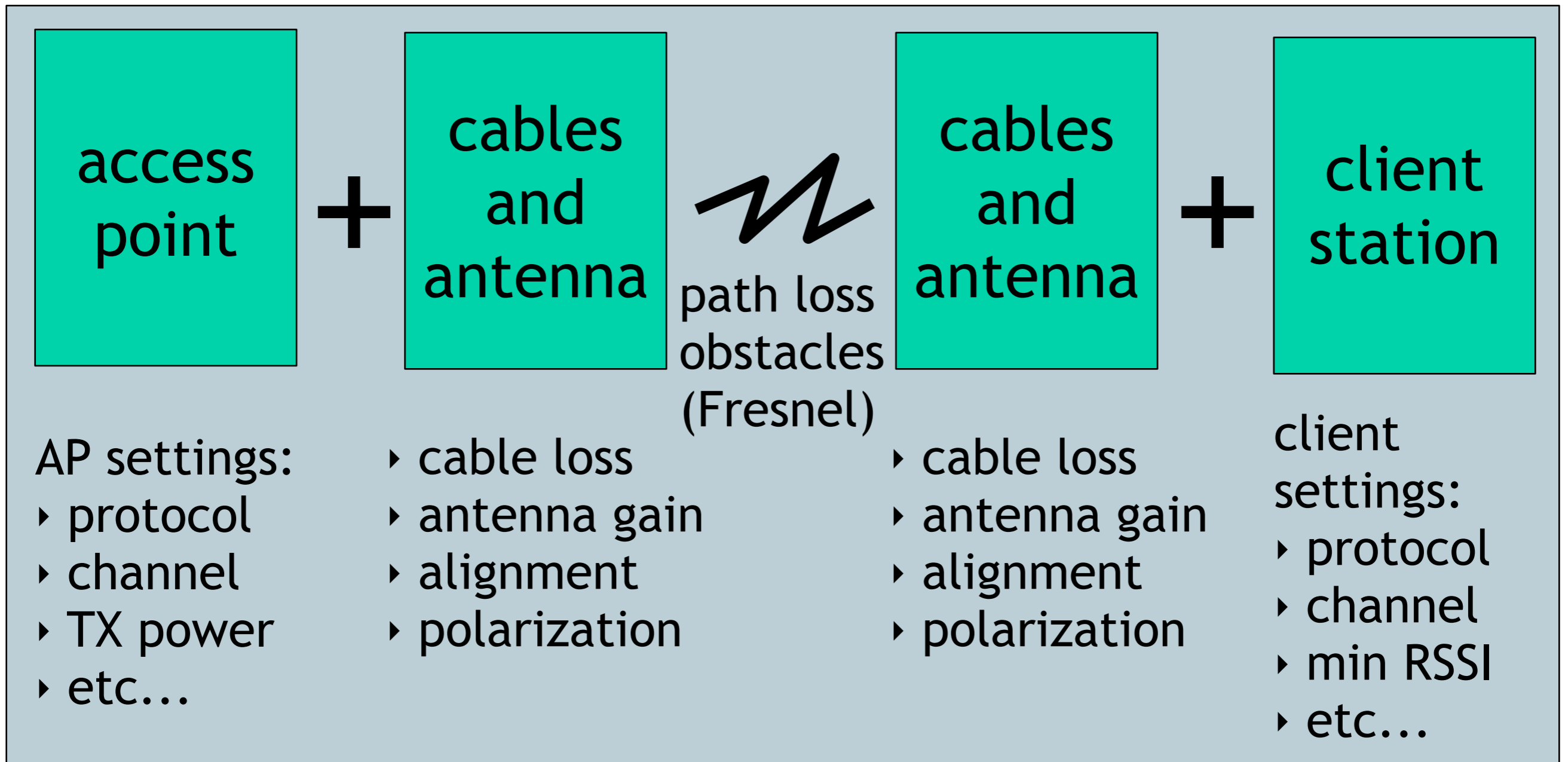
radio card(s)
(miniPCI)

features:

- ▶ frequencies
- ▶ power and sensitivity
- ▶ etc...

in some devices (ex: Mikrotik Routerboards)
you can change/add radio card(s)

A link is composed of many parts



In order to have a working link: all relevant settings should match
AND the link budget should allow for it

Thank you for your attention

For more details about the topics presented in this lecture, please see the book ***Wireless Networking in the Developing World***, available as free download in many languages at:

<http://wndw.net/>

