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 the traffic


Wi Fi ™
BELKIN
Skype
6:23 AM
skype
Menu
Contacts
Eee PC
ASUS
LINKSYS
Wireless-G Broadband Router

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.

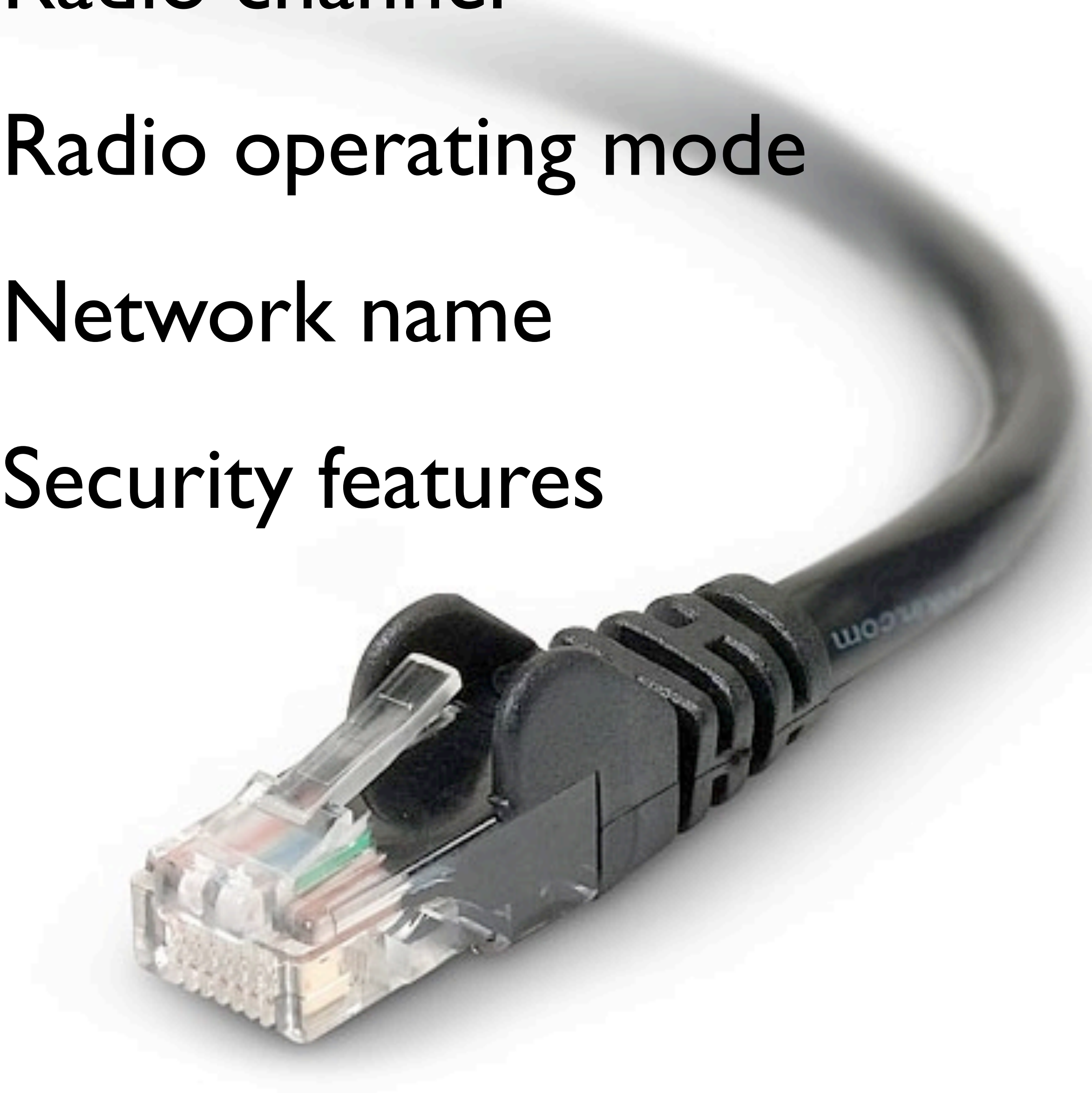
- ***802.16*** (WiMAX) is not 802.11 WiFi! It is a completely different technology that uses a variety of licensed and unlicensed frequencies.

Layer one

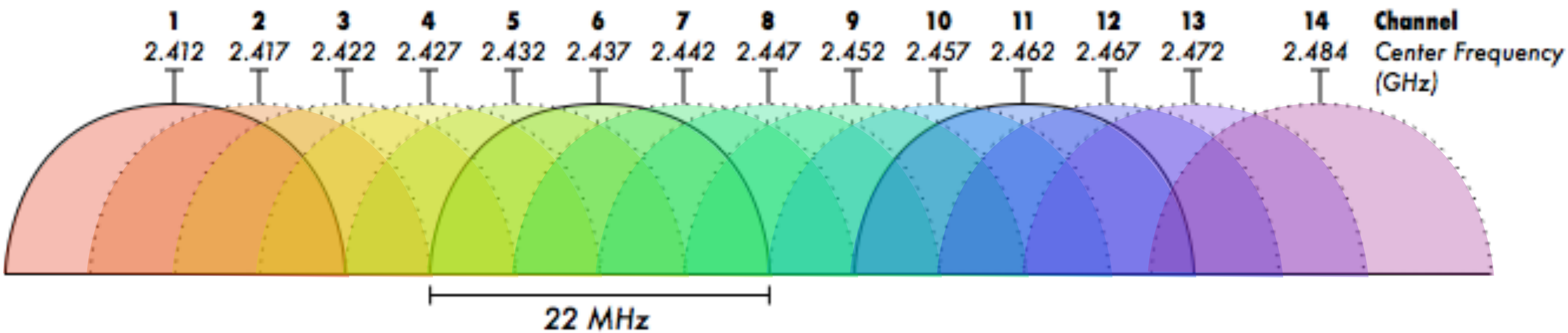
WiFi devices must agree on several parameters before they can communicate with each other. These parameters must be properly configured to establish "layer one" connectivity:

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

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

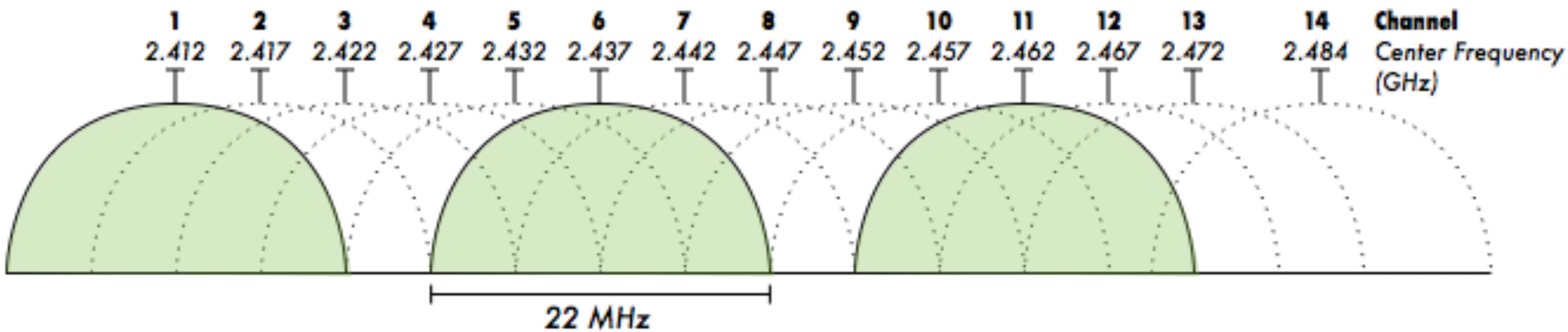


802.11 WiFi Channels

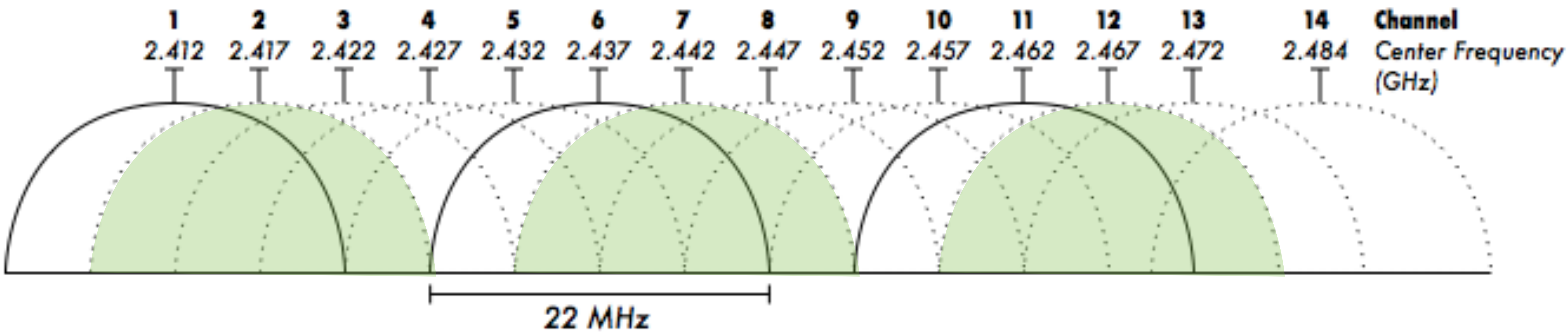


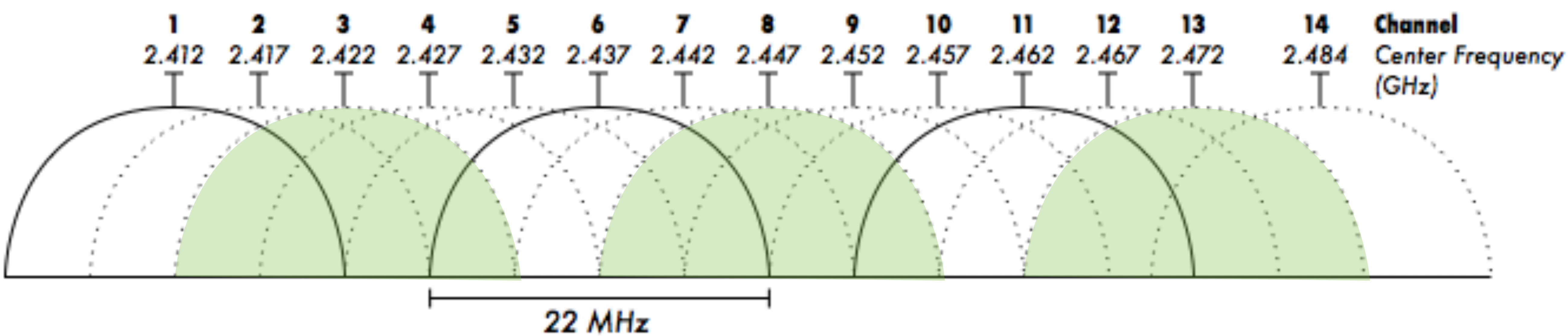
WiFi devices must use the same channel in order to communicate with each other. They send and receive on the same channel, so only one device may transmit at any time. This kind of connection is called “half-duplex”.

Non-overlapping channels: 1, 6, 11

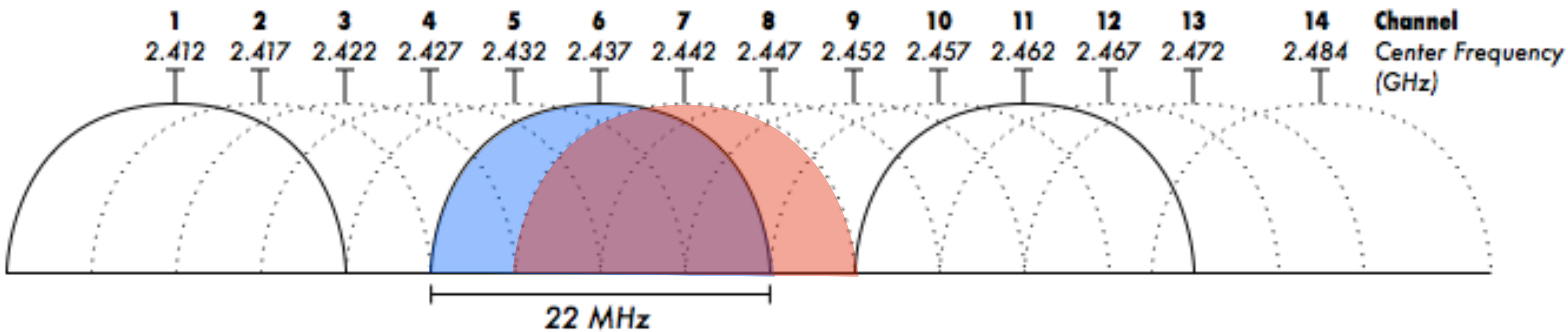


Non-overlapping channels: others

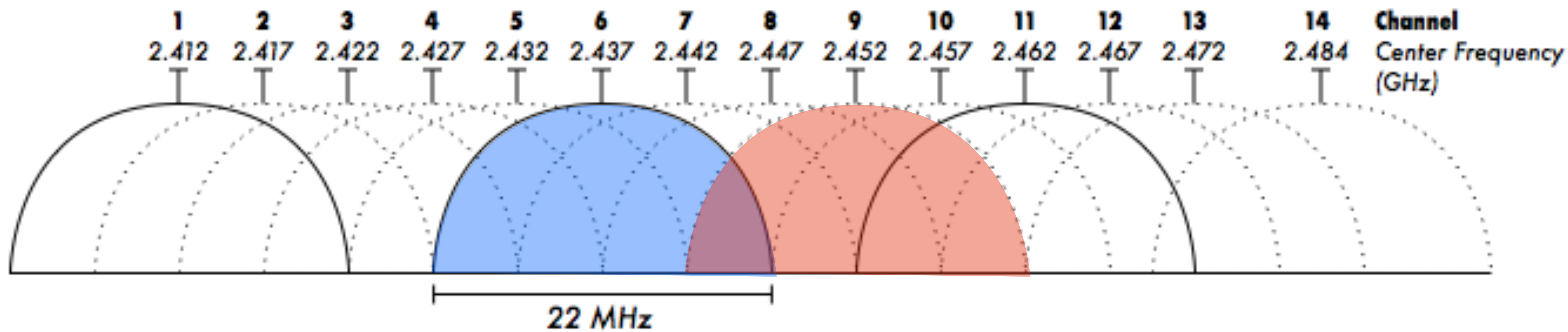




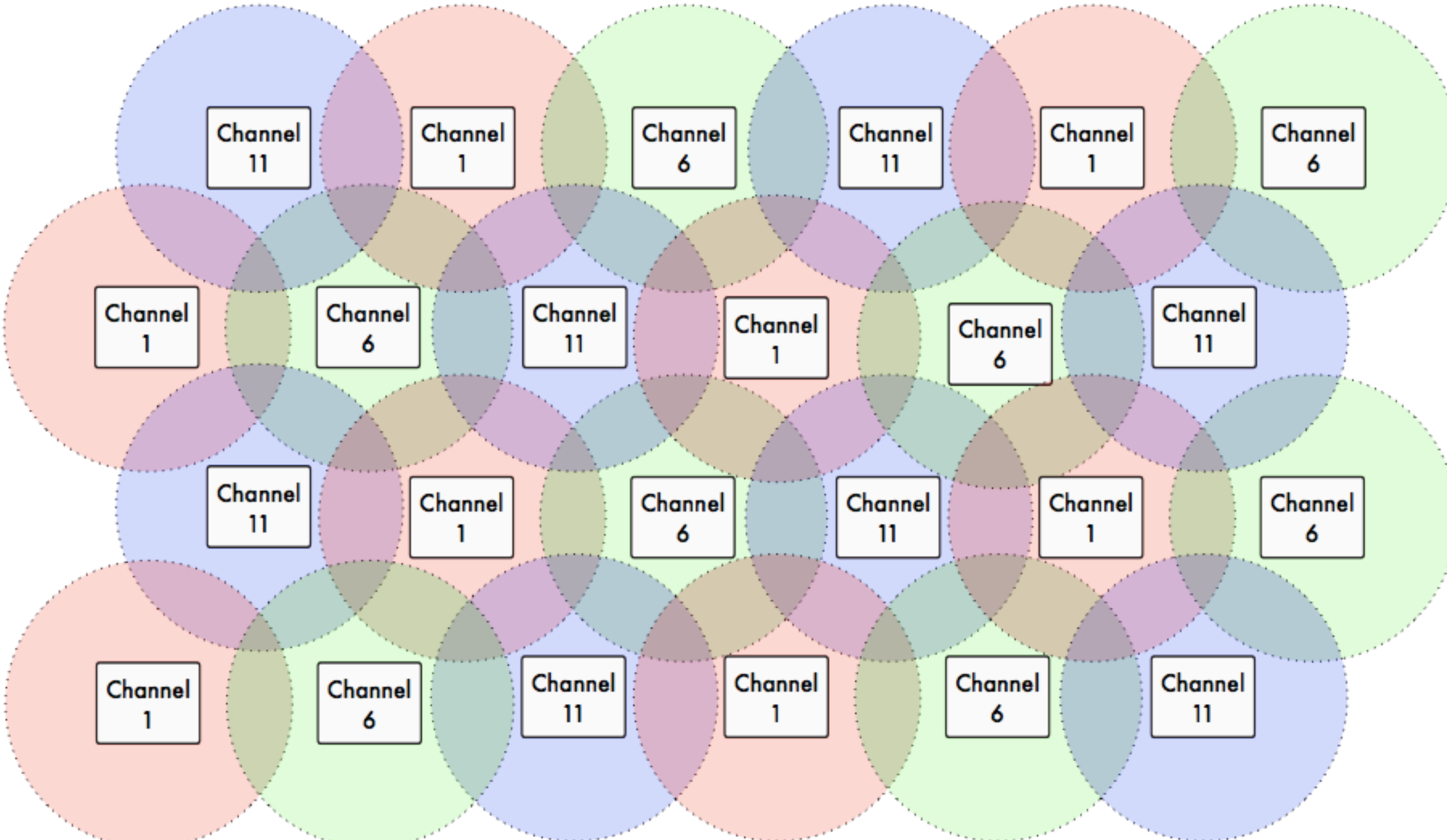
Adjacent channel interference



Non-adjacent channel interference



Channel re-use



Wireless network topologies

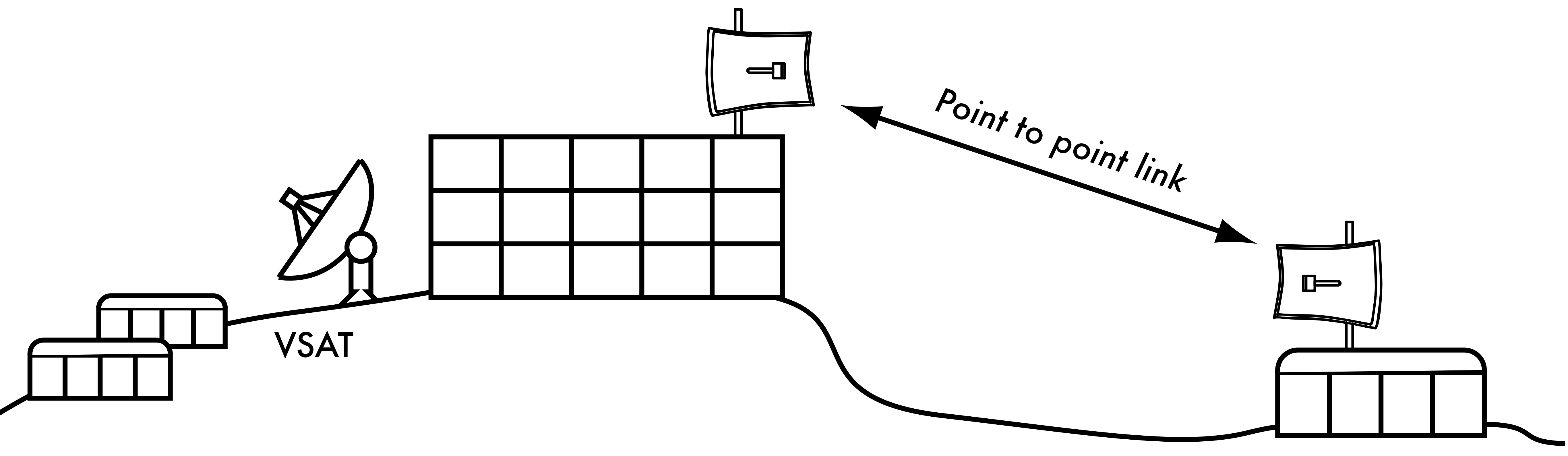
Any complex wireless network can be thought of as a combination of one or more of these types of connections:

- ***Point-to-Point***
- ***Point-to-Multipoint***
- ***Multipoint-to-Multipoint***

Point to Point

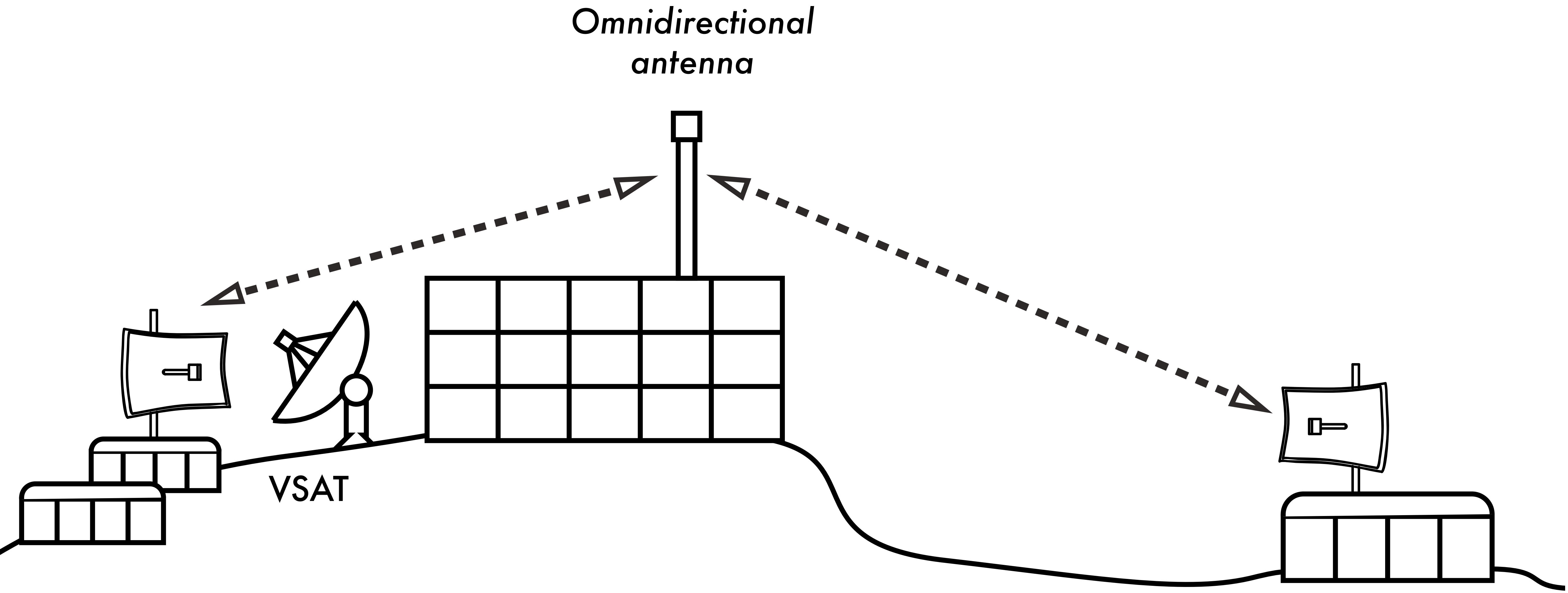
The simplest connection is the ***point-to-point*** link.

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



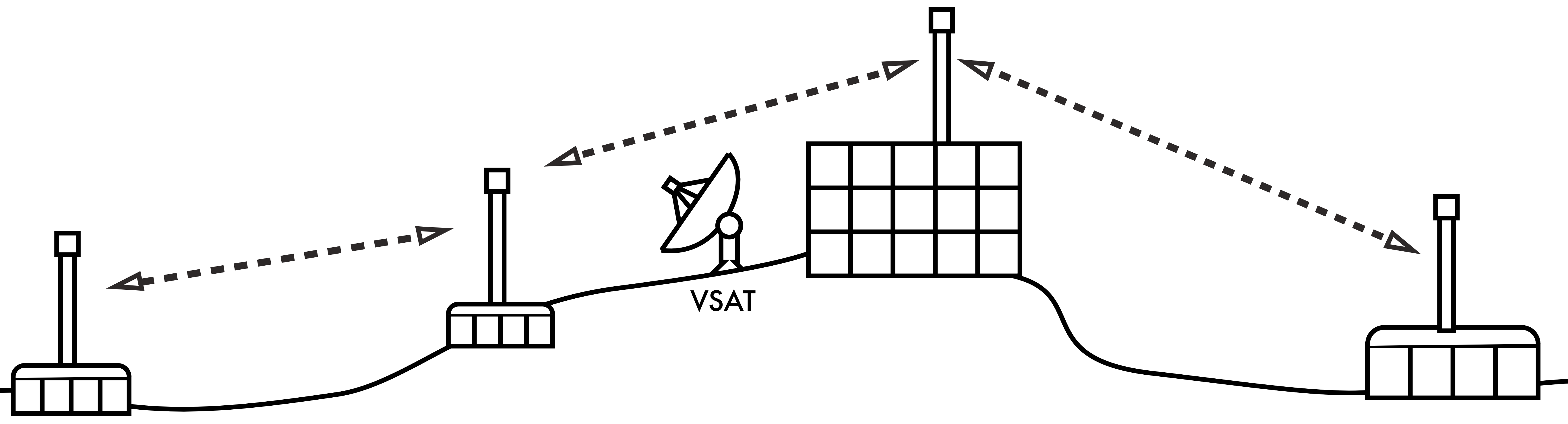
Point to Multipoint

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

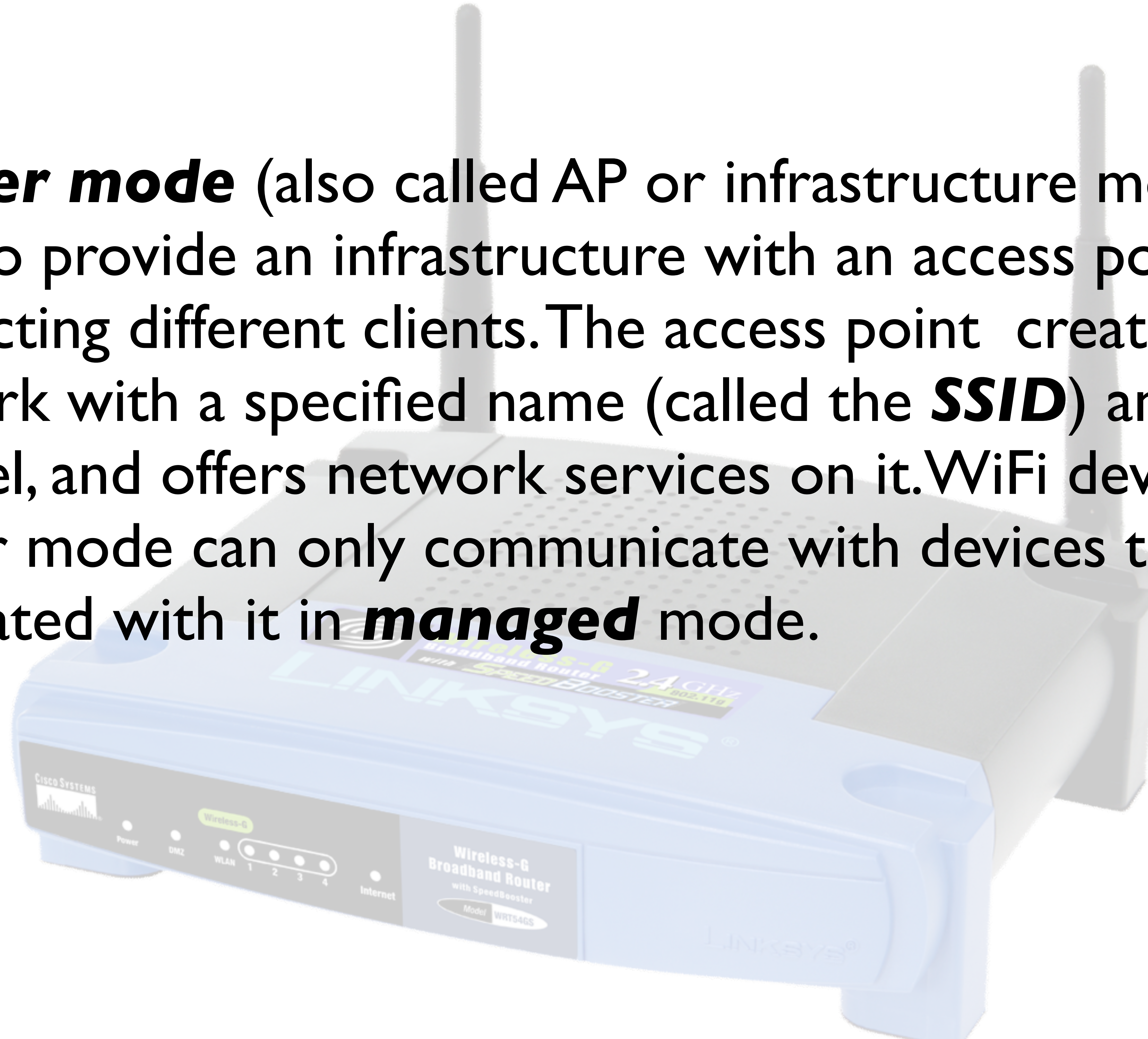
WiFi devices can be operated in one of these ***modes***:

- ***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. 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.

Ad-hoc Mode

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

- no master devices
- direct communication between neighbors

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

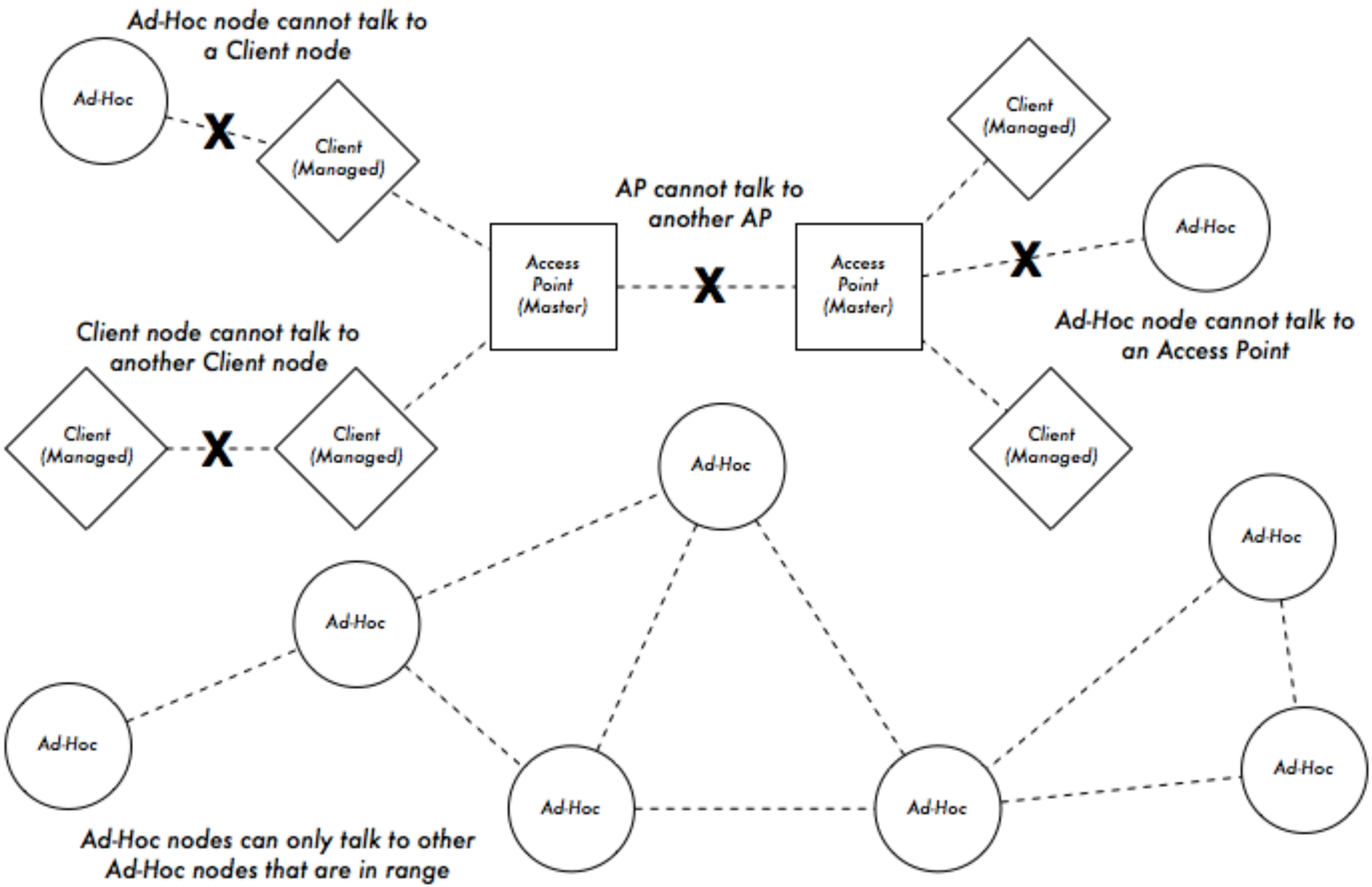
Monitor Mode

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 or
- observing spectrum usage in the local area.

It is not used for normal communications.

WiFi radio modes in action



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 (layers 2 and 1)

Bridged networking

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

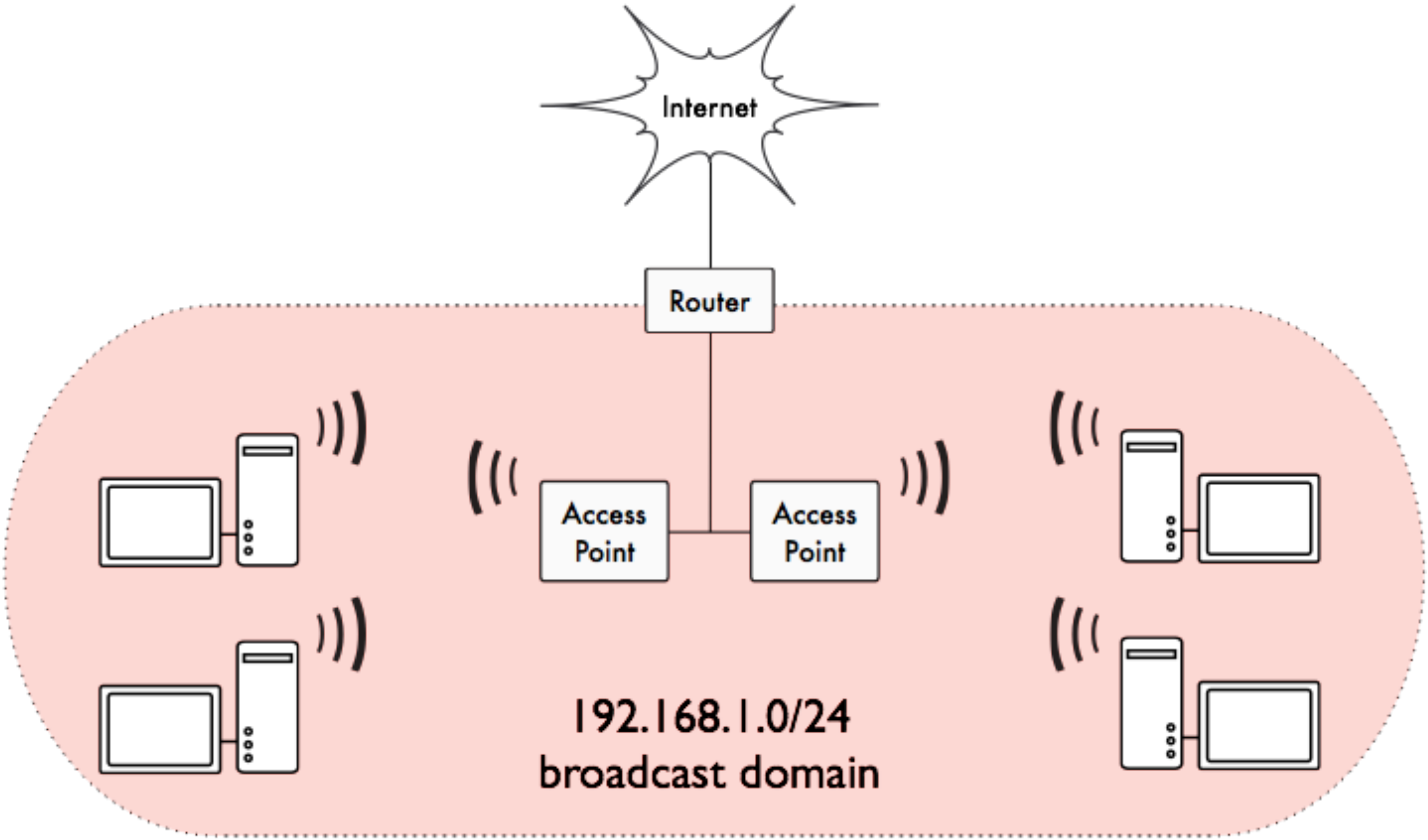
Advantages

- 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

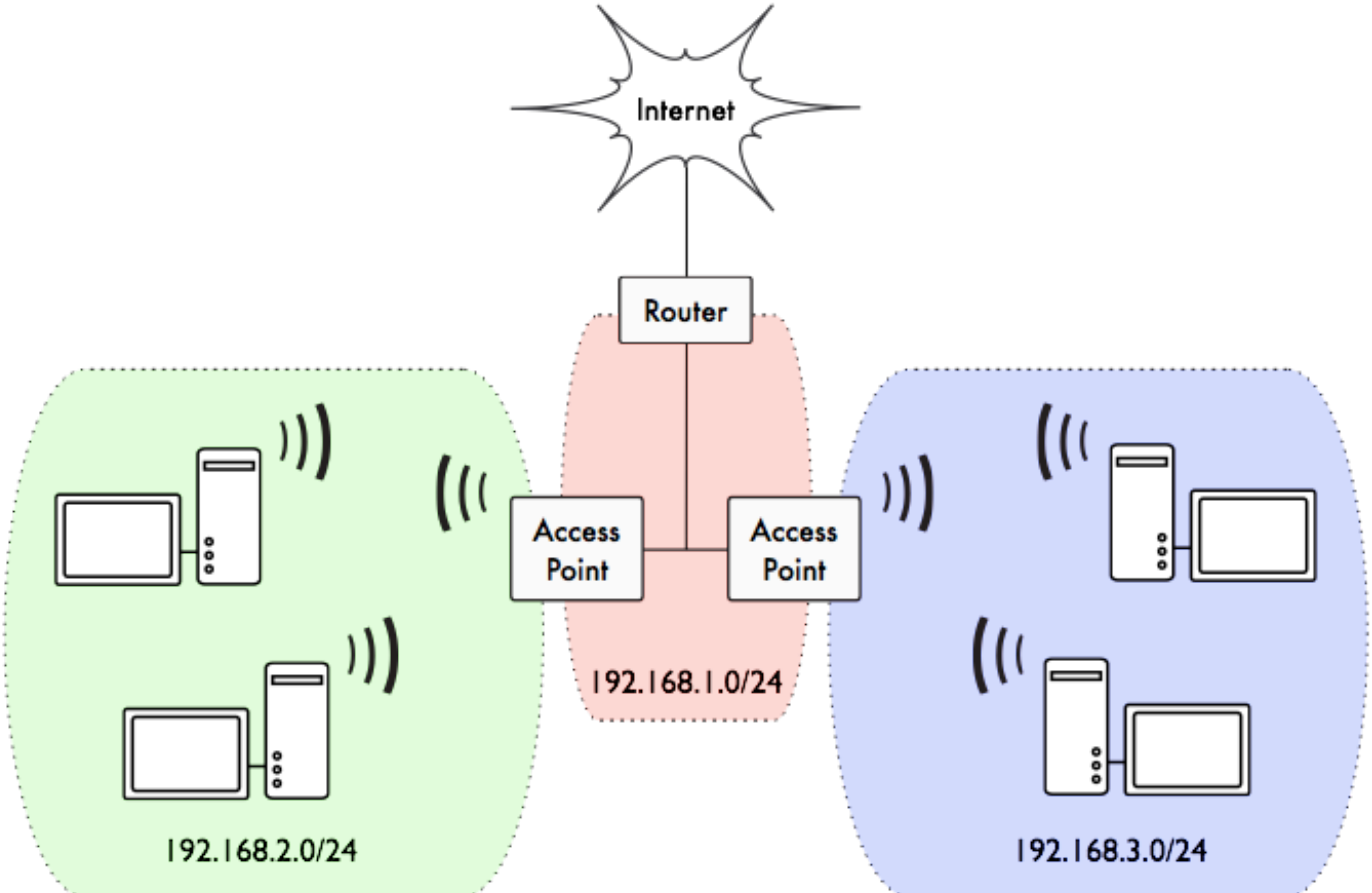


Routed networking

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*** (OLSR, B.A.T.M.A.N., HSLS, AODV) work very well with wireless networks, particularly when using radios in ad-hoc mode.

Routed access points



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

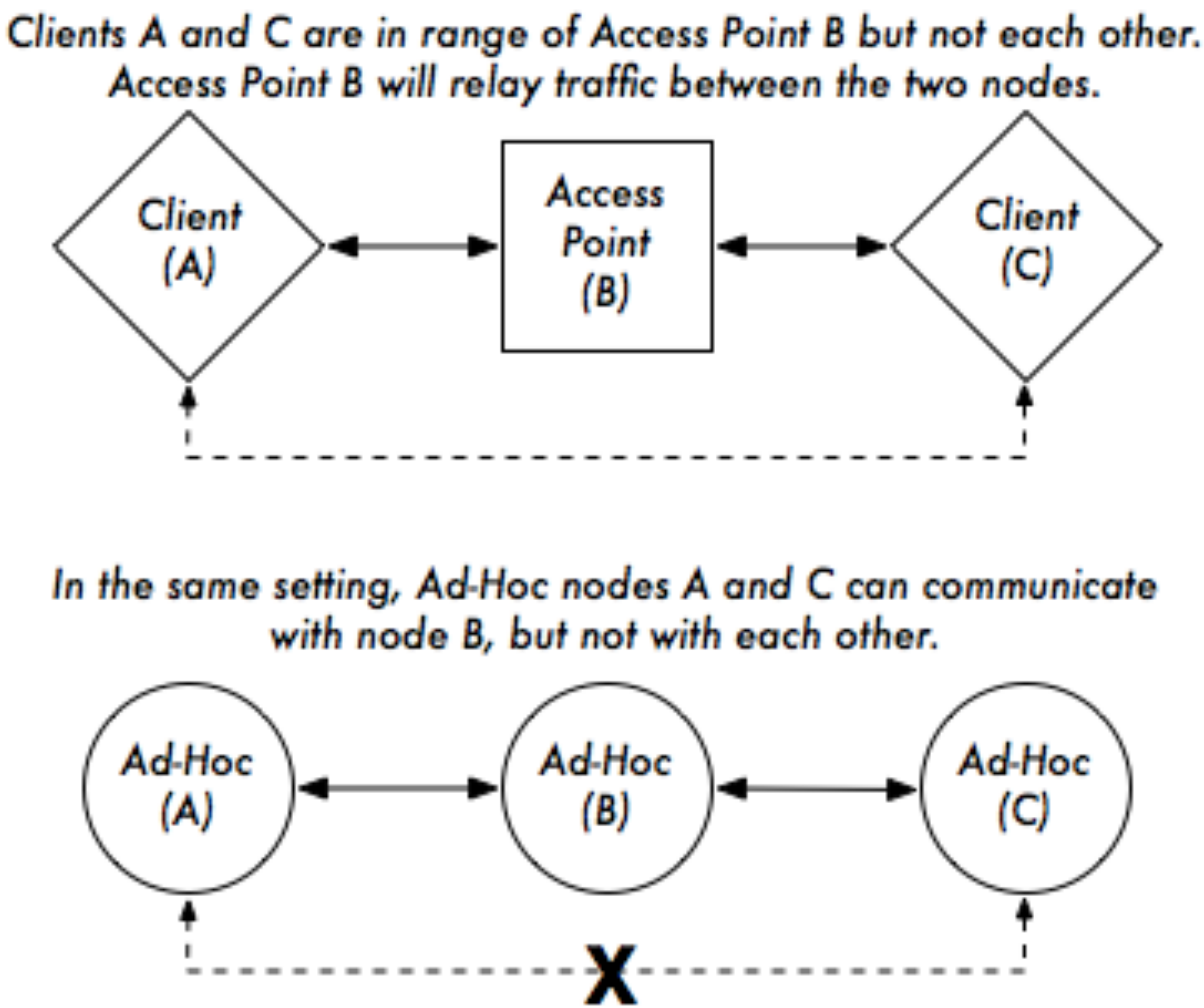
- More complex configuration
- Roaming between APs is not supported

Relaying traffic

In **ad-hoc mode**, all radios can communicate with each other as long as they are in range. They will **not** relay traffic for other nodes without an additional routing protocol.

In **infrastructure mode**, clients must be within range of an access point. The AP will relay traffic between all associated clients, but clients **cannot** talk to each other directly.

Infrastructure vs. ad-hoc



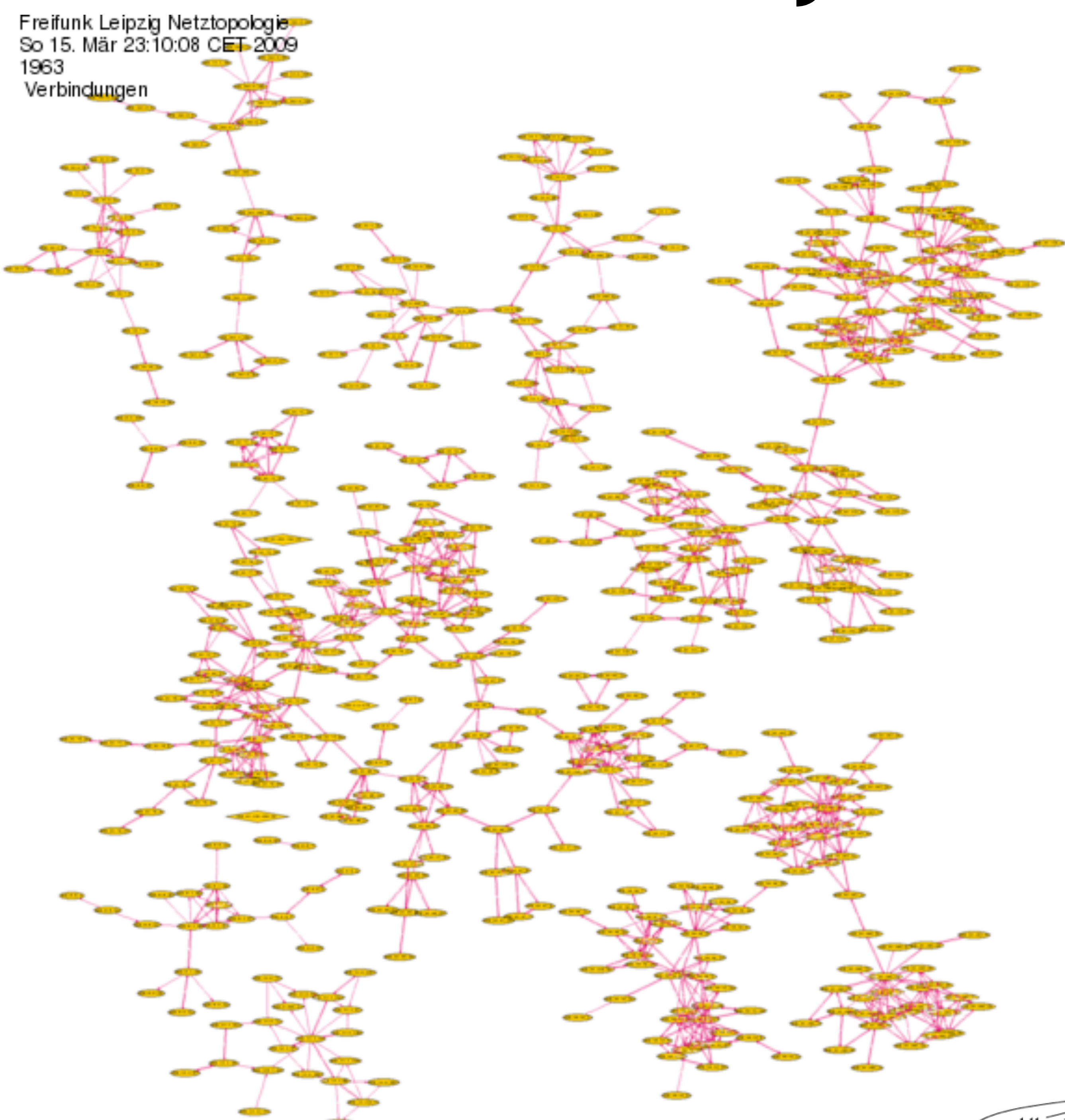
Mesh = ad-hoc + routing

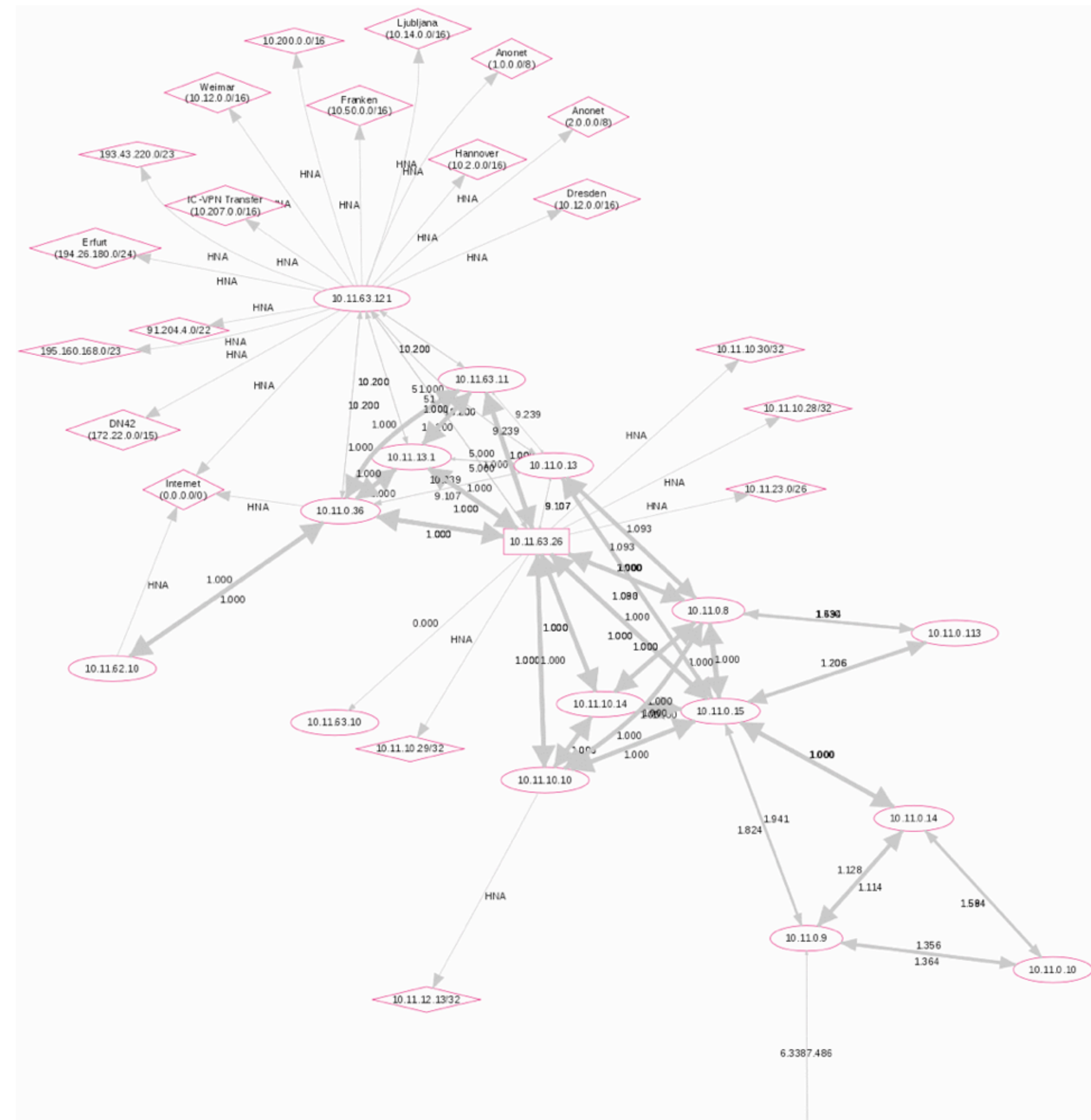
A ***mesh network*** (implemented with 802.11 equipment) is essentially

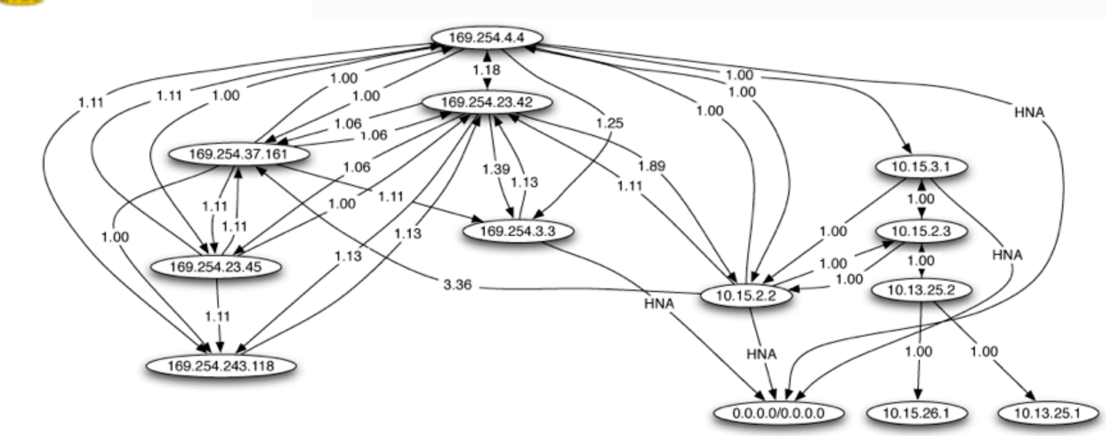
- a group of radios operating in ad-hoc mode,
- with some kind of routing applied.

Many **mesh routing protocols** (such as B.A.T.M.A.N. or OLSR) may be applied to any physical network, including WiFi devices in Master/Managed nodes, or even other physical network types (such as Ethernet).

Dynamic mesh





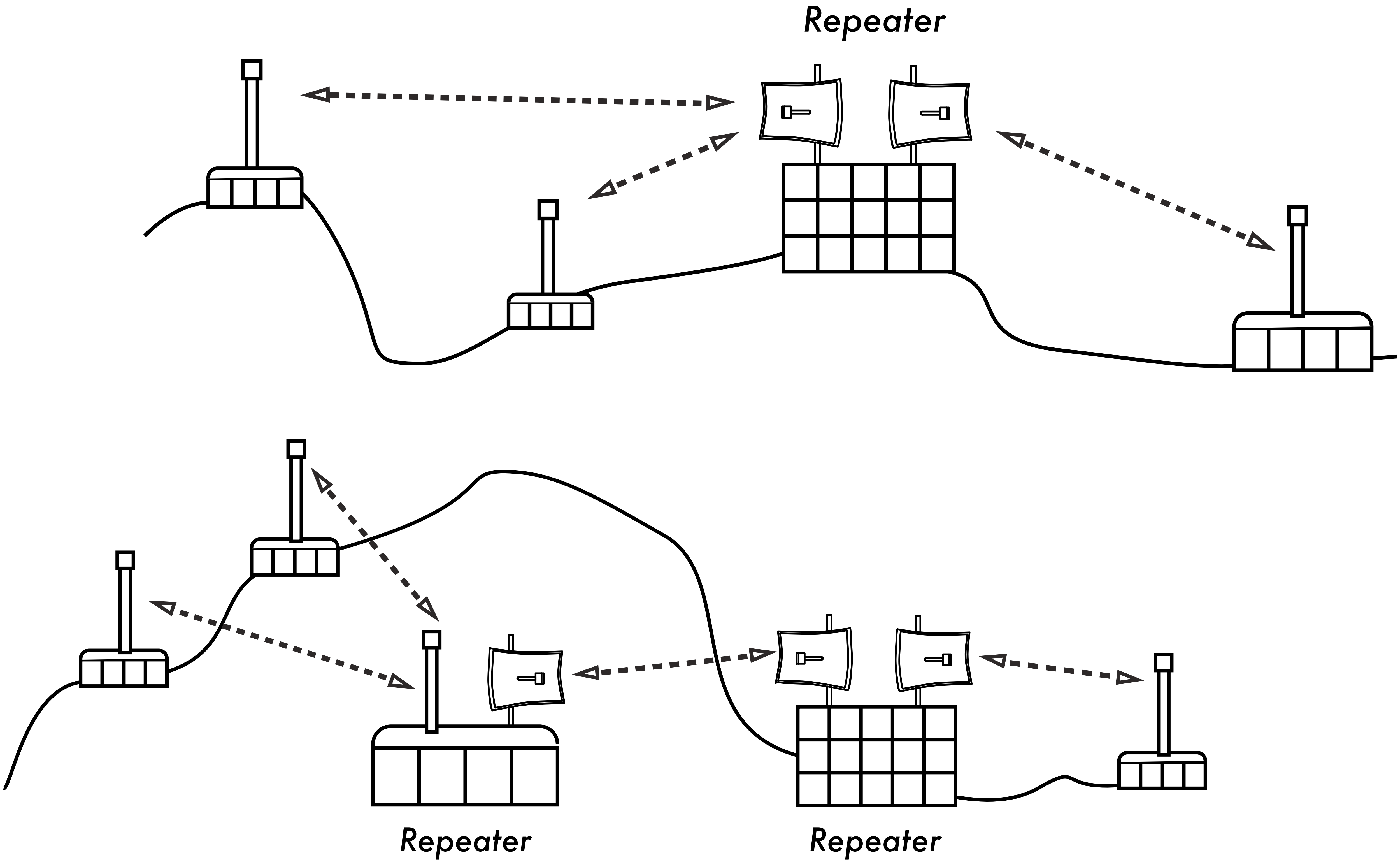


Repeaters

The most critical component to building long distance network links is ***line of sight*** (often abbreviated as ***LOS***). You must have a clear idea of the lay of the land between two points before you can determine if a link is even possible.

Repeaters are nodes that are configured to rebroadcast traffic that is not destined for the node itself. In a mesh network, every node is a repeater. In a traditional infrastructure network, nodes must be configured to pass along traffic to other nodes.

Repeaters



Problems with long distance 802.11

802.11 WiFi networks are designed to operate at relatively short distances (up to a couple of hundred meters). Range can be extended significantly by using high gain antennas, but this is not a complete solution.

Over long distances, a number of problems become apparent that are not handled well by the 802.11 protocol itself.

The “Hidden Node”

When two clients are in range of the same access point but not each other, their transmissions can interfere with each other. This condition is called a ***hidden node*** problem.

- Hidden node is alleviated somewhat by CTS/RTS (also known as channel reservation).
- CTS/RTS adds overhead, so you can specify a maximum packet size above which CTS/RTS is used.
- It is not perfect, but can help at a cost of maximum possible throughput. CTS/RTS should only be used with access points and clients, not ad-hoc networks.

Timing Issues

Due to the very fast timing of 802.11 frames, the speed of light becomes an issue at long distances. At approximately 15 km, standard timings are too short for acknowledgements to be received.

Some cards and drivers (such as Atheros) allow timings to be adjusted, permitting very long distance communications.

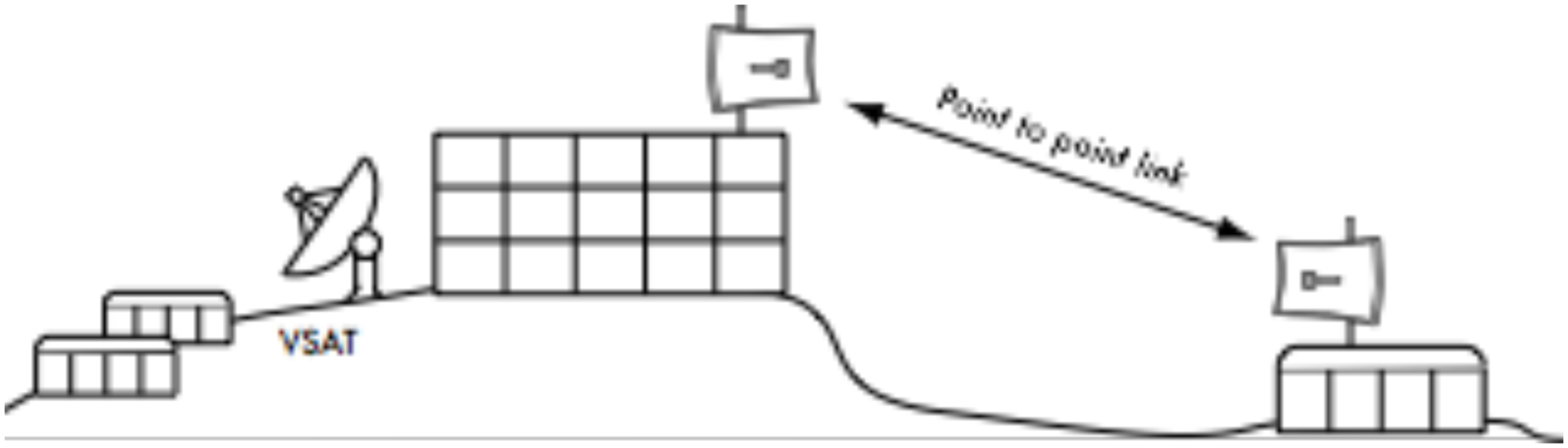
Proprietary protocols (such as Mikrotik Nstreme or Ubiquiti AirMAX) use TDMA to avoid these ACK timing issues.

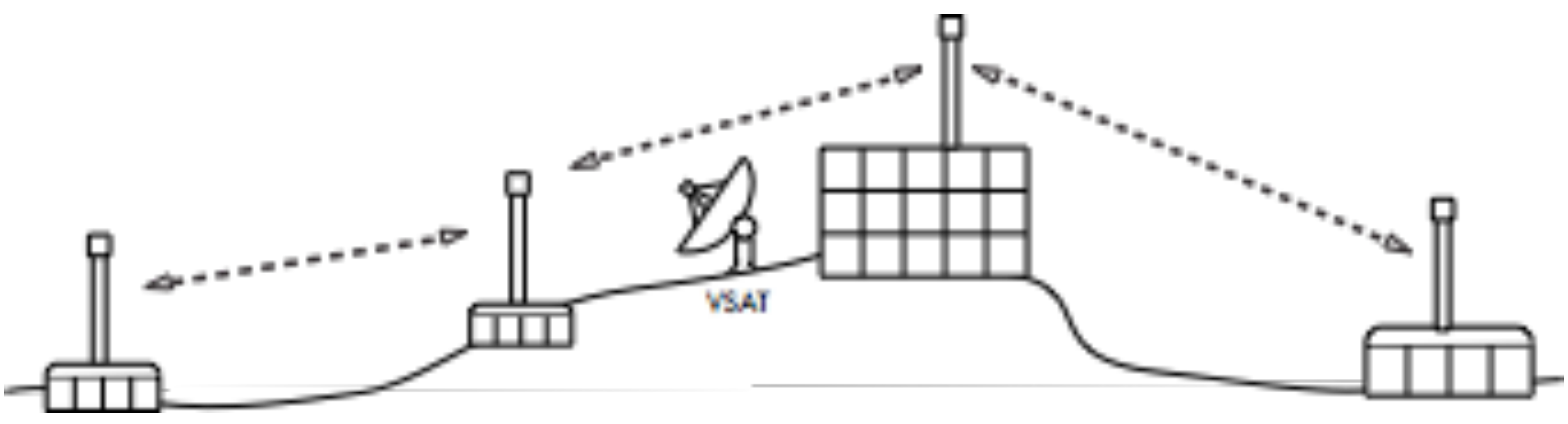
Anything is Possible

279+ Kilometer links can be made!

Use the proper technology

No single technology can solve all of your wireless needs. But by using multiple network technologies with inexpensive WiFi equipment, you can build extremely capable and flexible wireless networks.





FAQ about WiFi Networks

- 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

We 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 a firmware? Why may I want to change it?
- I don't understand the differences between AP, device, firmware, protocols...

A few important concepts

device
(hardware)

+

firmware
(O.S.+software)

hardware features:

- power
- frequencies
- ports (RF, eth)
- etc...

firmware features:

- modes (AP/client/...)
- supported protocols
- allowed max power
- allowed frequencies
- settings you can do...

all this together makes up your AP/client

Alternate firmware

device
(hardware)

+

alternate firmware
(O.S.+software)

hardware features:

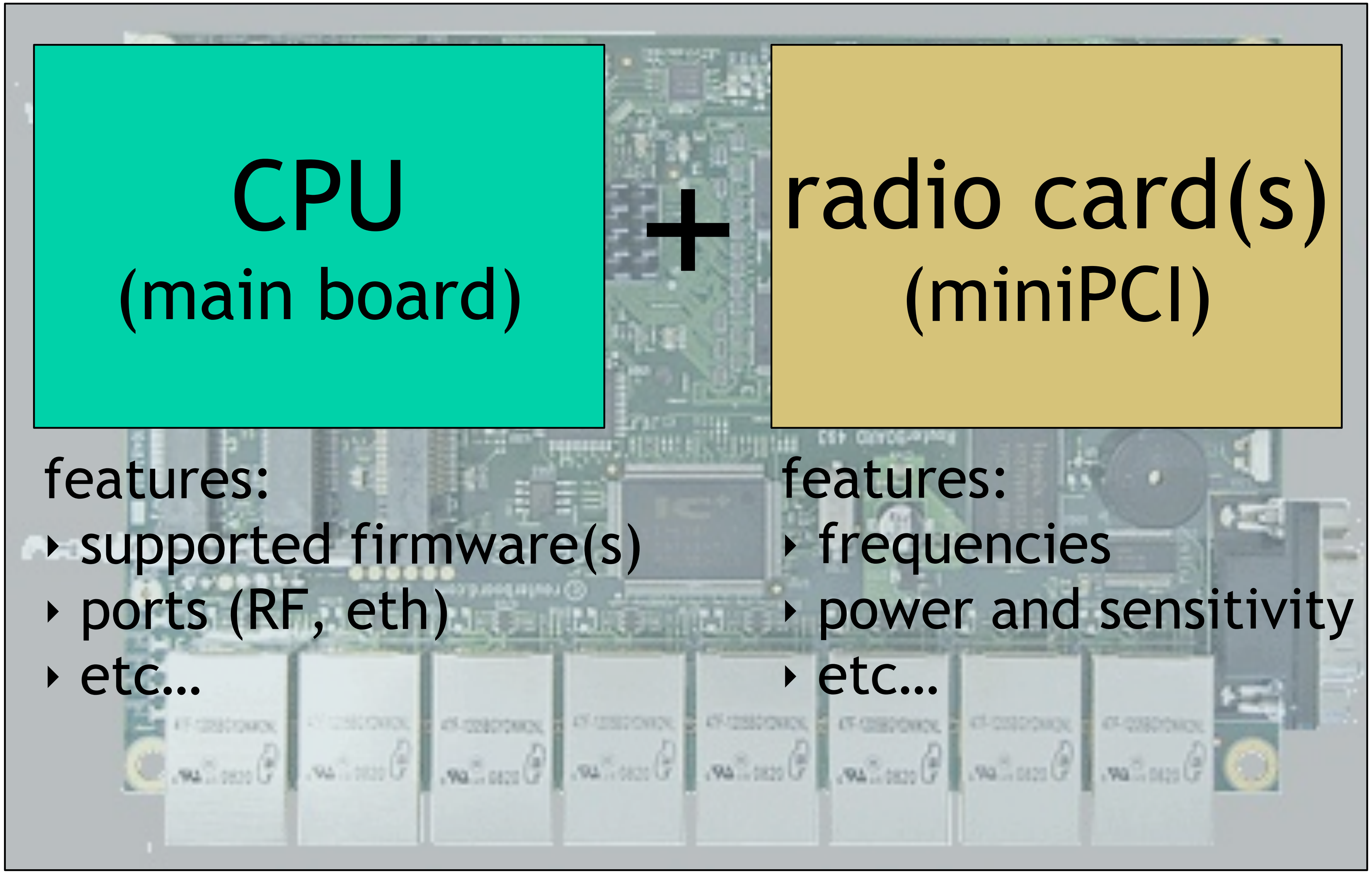
- power
- frequencies
- ports (RF, eth)
- etc...

firmware features:

- modes (AP/client/...)
- supported protocols
- allowed max power
- allowed frequencies
- settings you can do...

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

Modular hardware



CPU
(main board)

\+

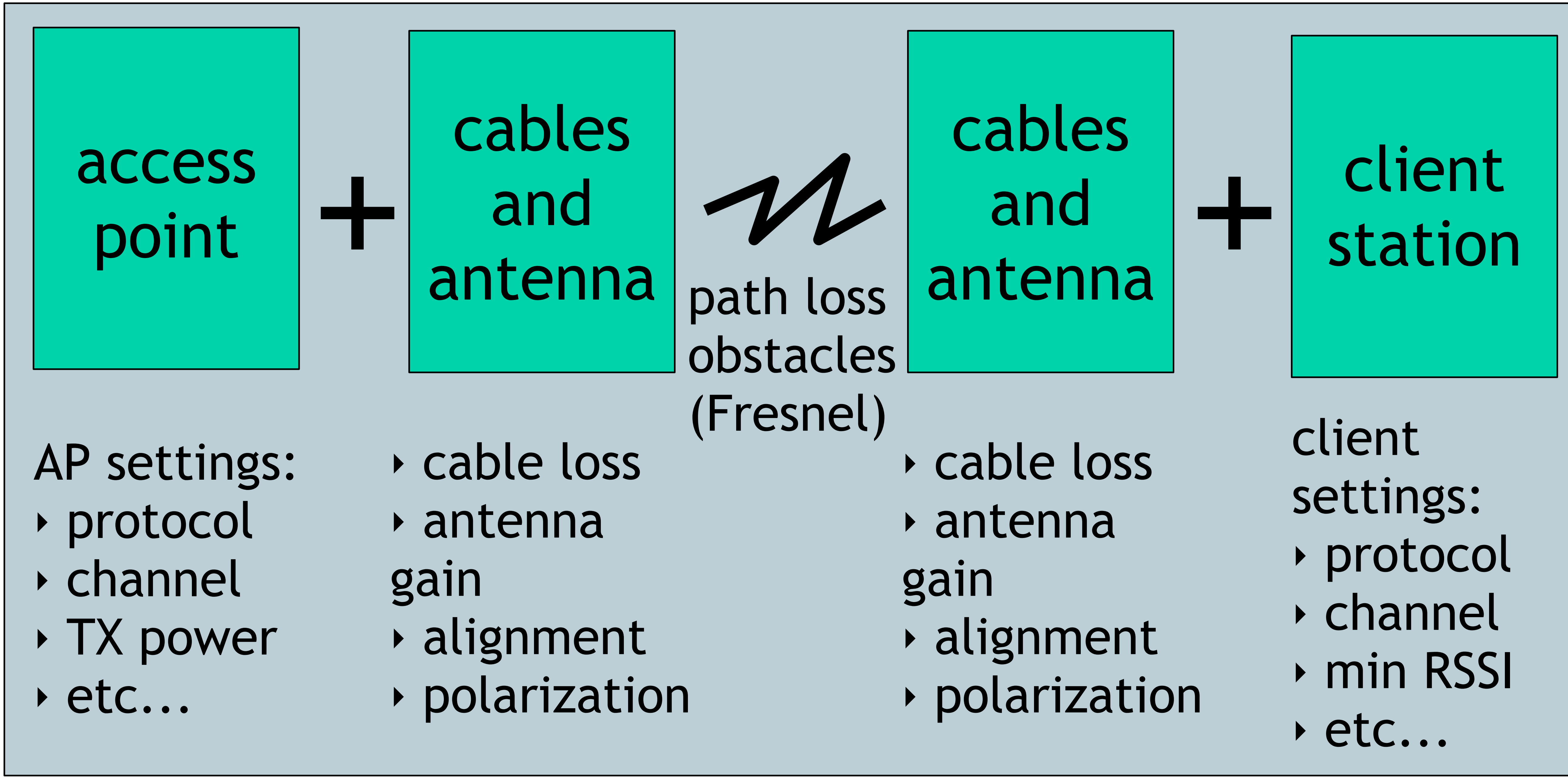
radio card(s)
(miniPCI)

features:
- supported firmware(s)
- ports (RF, eth)
- etc...

features:
- frequencies
- power and sensitivity
- etc...

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

A link is composed by many parts



in order to have a working link: all relevant setting should match AND 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