Introduction to 802.11 / WiFi

Goals

- **ISM bands**
- **802.11 family of radio protocols**
- **WiFi**
- **802.11 radio channels**
- **Channel Access**
- **Wireless network topologies**
- **WiFi modes of operation**
- **A first view on wireless routing network traffic**
- **Frequently Asked Questions**

”Free” wireless

Licensed vs Unlicensed

- Most commercial wireless devices (mobile phones, television, radio, etc.) use **licensed** radio frequencies.

  Large organizations (GSM companies) pay licensing fees for the right to use those radio frequencies.

- WiFi uses **unlicensed / license exempt spectrum**.

  License fees are not usually required to operate WiFi equipment.

ISM bands

- 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.
- **Other interesting ISM bands:**

  around 433 MHz, 915 MHz, 6 Ghz

  - maybe new **”white space”** (50-700 MHz)

What is WiFi?

- A trademark, owned by the WiFI Alliance - not a strict technical term.
- Better to speak of IEEE 802.11
- However, ”WiFi” is commonly used for the 802.11 family of wireless standards.


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

802.11 standards

	Data rates [Mbps]	Freq [GHz]	channel access
b	11	2.4	DSSS
g	54	2.4	DSSS, OFDM
a	54	5 GHz	OFDM
n	300/600*	2.4/5	all the above , MIMO
			*20/40 Mhz/channel
ac	> 1000?	2.4/5	OFDM, MU-MIMO
ad	> 6000 (?)	60 (!)	keep in mind: mm waves!
af	(lower)	0.7 a.o. ex-TV	aka White-Fi

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 rest is called protocol overhead.
- A good rule of thumb: the practical TCP/IP **throughput is about half the data rate**. 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.

Channel access schemes

How to organize access to the medium

- **Channel based access schemes**
  - Frequency Division Multiple Access (FDMA)
  - Time division multiple access (TDMA)
  - Code division multiple access (CDMA)
  - Space division multiple access (SDMA)
- **Packet based access schemes**
  - Carrier sense multiple access (CSMA)
- **Important as they impact performance**

802.11 channel access

802.11	DSSS, FHSS
a	OFDM
b	DSSS, 20 MHz/channel
g	OFDM
n	all the above, MIMO, 40 Mhz/channel
ac	OFDM, MU-MIMO, 80 Mhz/channel

WIMAX	Dyn TDMA
LTE	OFDMA/MIMO/SC-FDMA

3G mobile CDMA

2G mobile TDMA

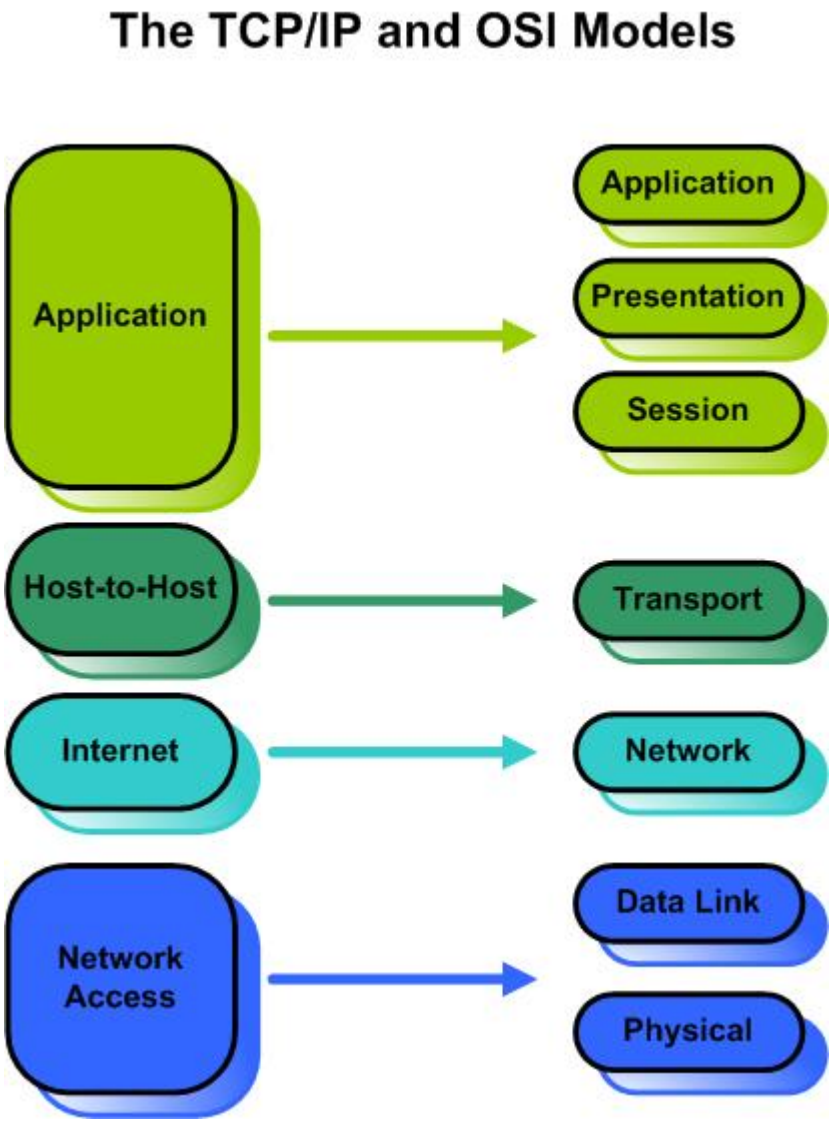
Bluetooth FHSS

Compatibility of standards

AP

CLIENT	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

Remember: layer thinking

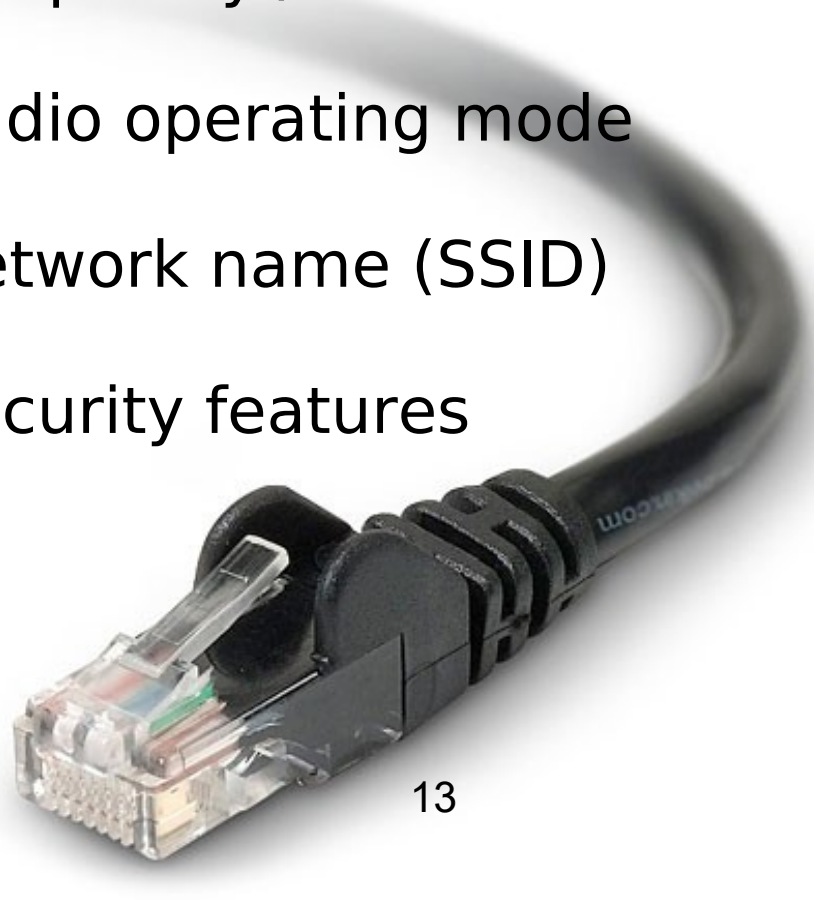


Layer one

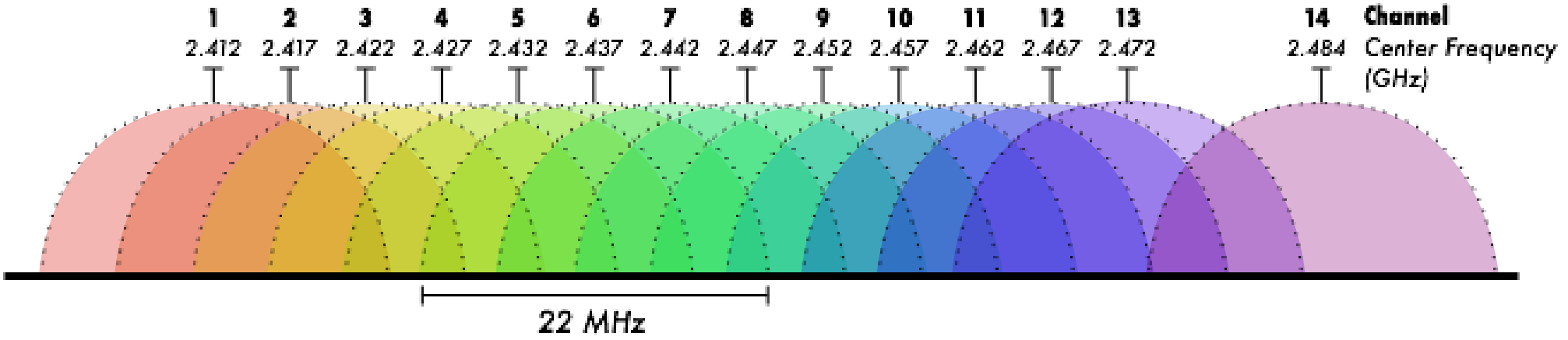
WiFi devices must agree on several parameters before they can communicate with each other. These parameters must be properly configured to establish “layer one” connectivity:

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

- Frequency / channel
- Radio operating mode
- Network name (SSID)
- Security features

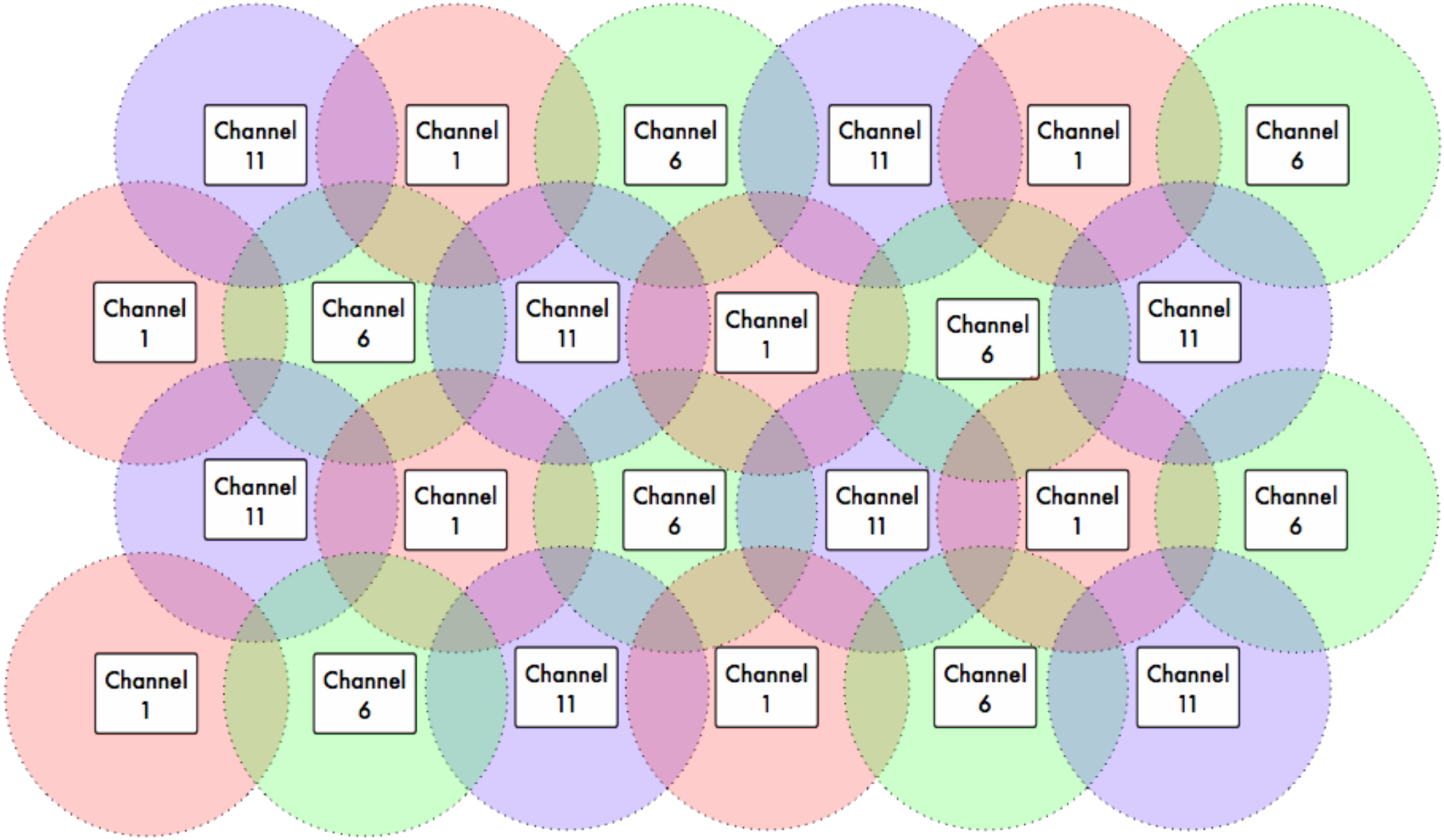


802.11 WiFi Channels



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

AP channel re-use



Remember this is theory :)

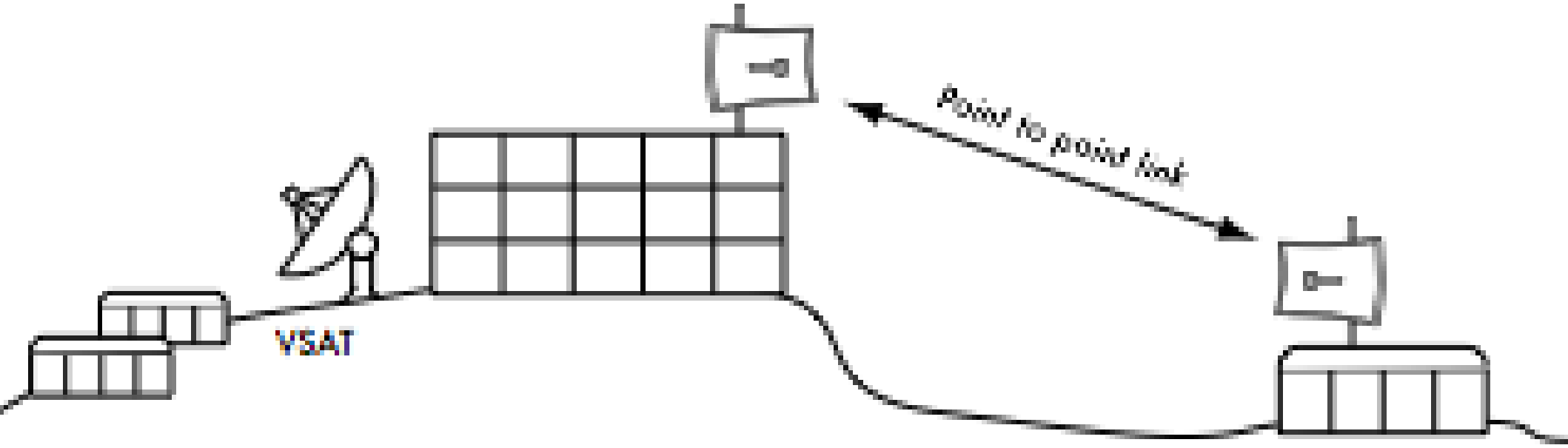
Wireless network topologies

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***

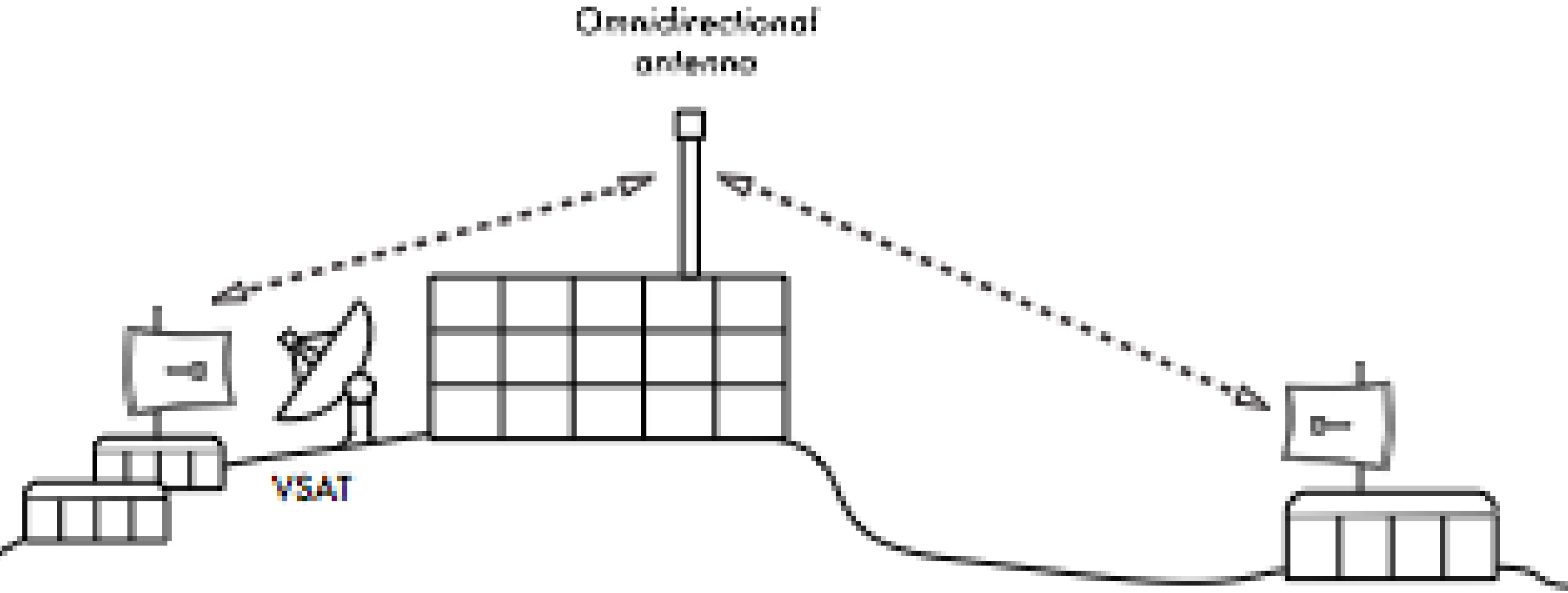
Point to Point

The simplest connection is the ***point-to-point*** link.
These links can be used to extend a network over great distances.



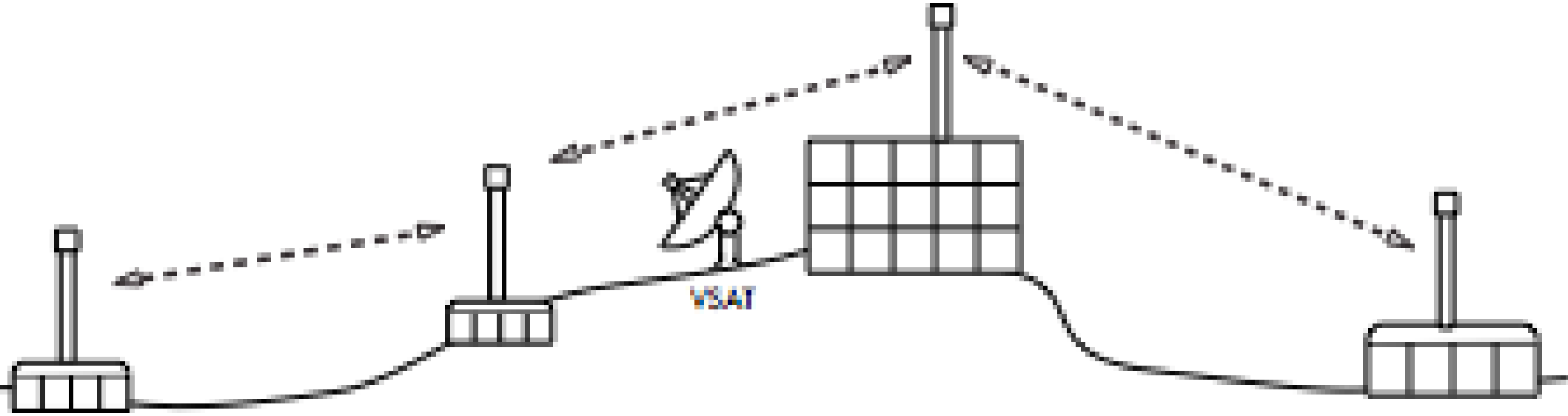
Point to Multipoint

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 / radios can be operated in one (and only 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)

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.

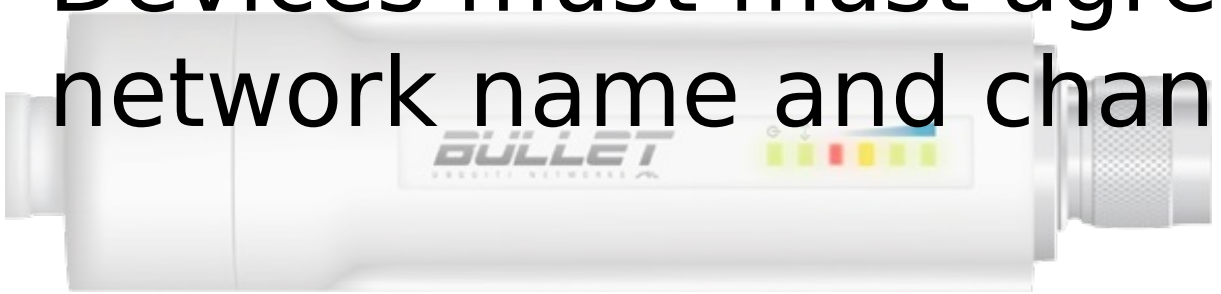
Managed Mode

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 (and only with one at a time).

Ad-hoc Mode

Ad-hoc mode is used to create one to one connections and mesh networks.
In this case, there is no master and client.
Devices must must agree on a network name and channel.

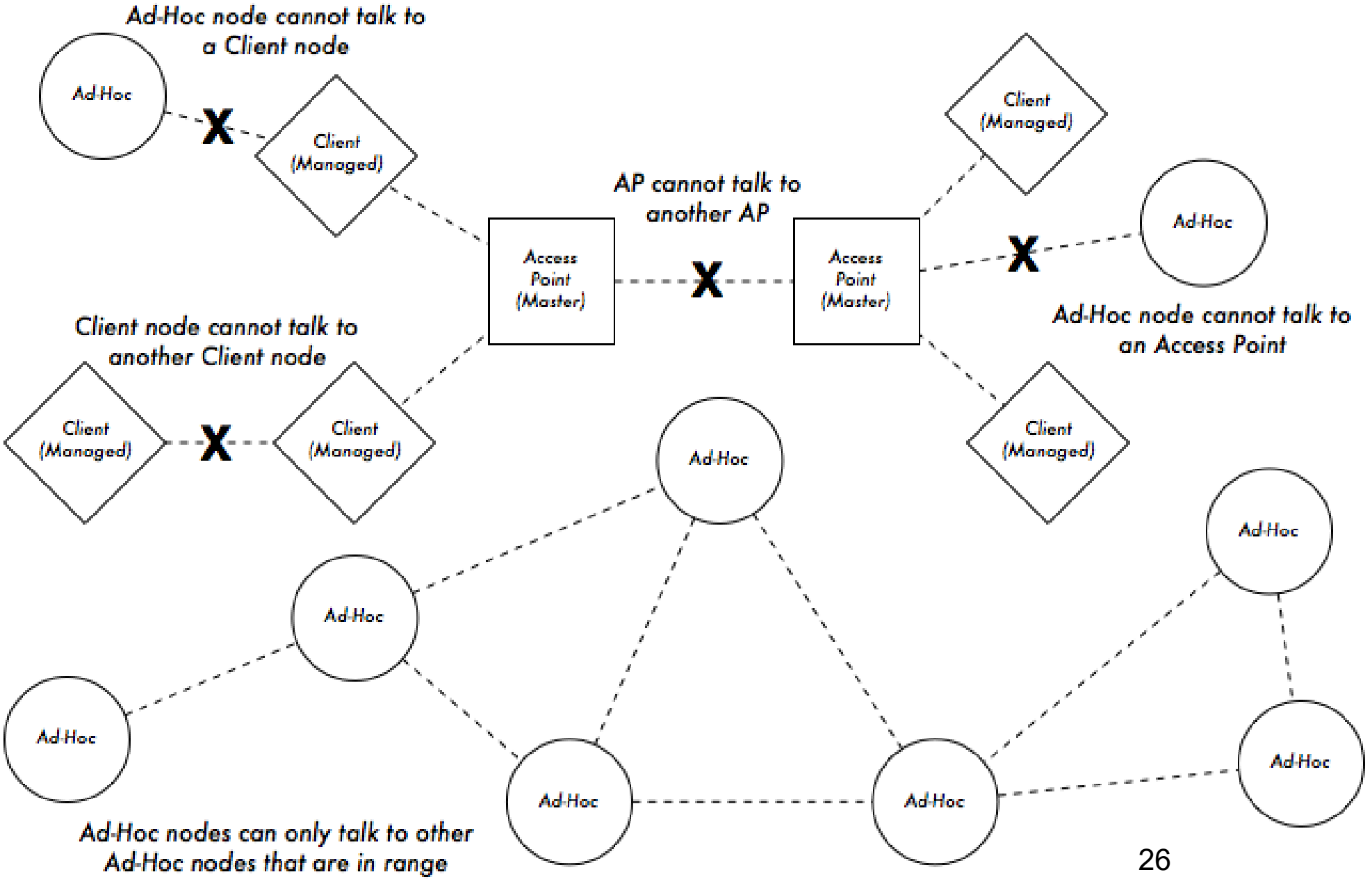


Monitor Mode

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



26

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.

Use of WDS is not recommended.

Routing traffic

802.11 WiFi provides a link-local connection.
It lives on Layer 1/2.
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 very simple local area wireless network, a bridged architecture is usually adequate.

Advantages

Very simple configuration

Roaming works very well

Disadvantages

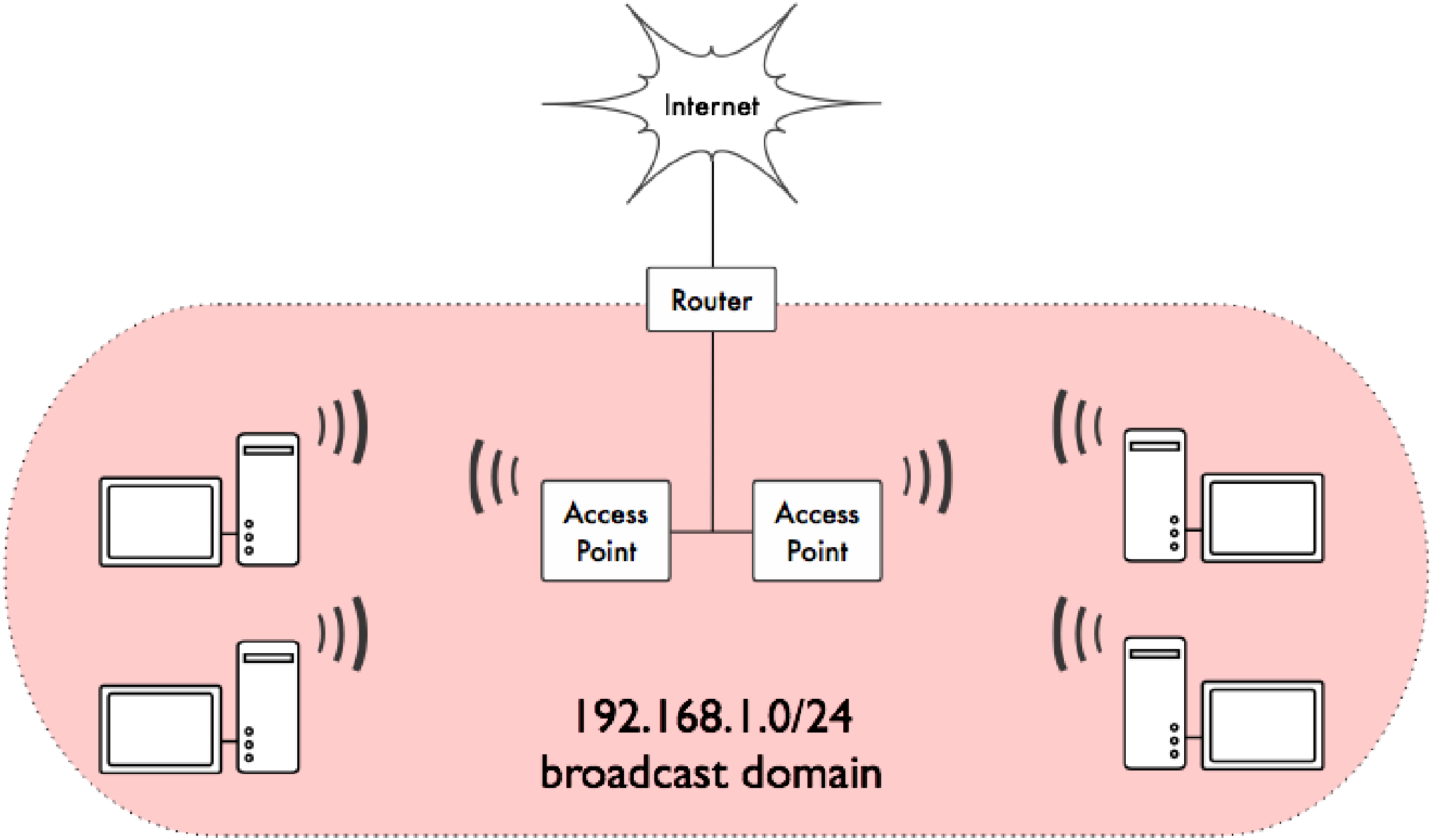
Increasingly inefficient as nodes are added.

Difficult to manage.

All broadcast traffic is repeated (!).

Virtually unusable on larger 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 very well with wireless links.
- ***Mesh routing protocols,*** with metrics suitable for wireless conditions, may work very well with wireless networks.

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

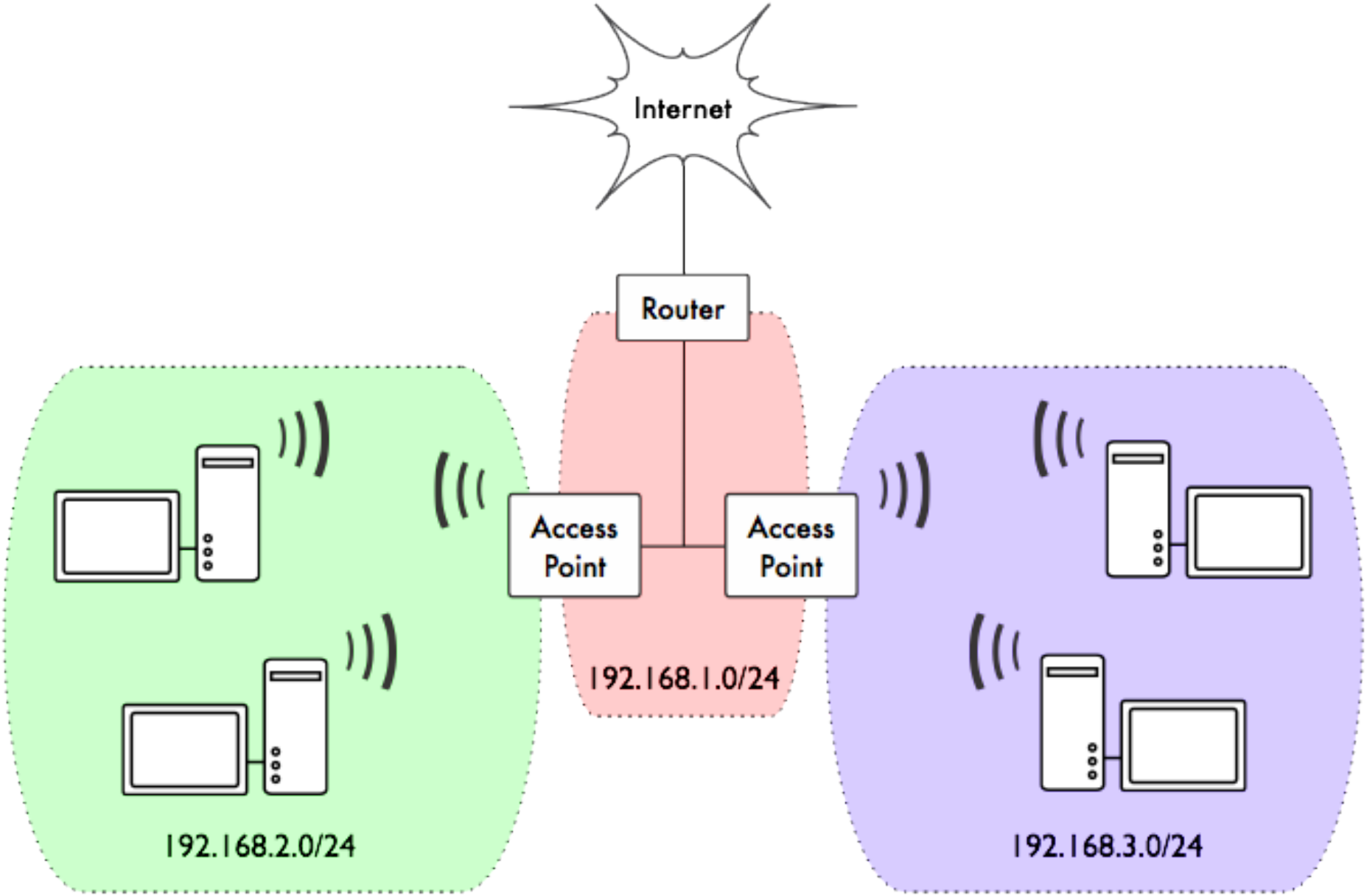
A variety of routing protocols and bandwidth management tools are available

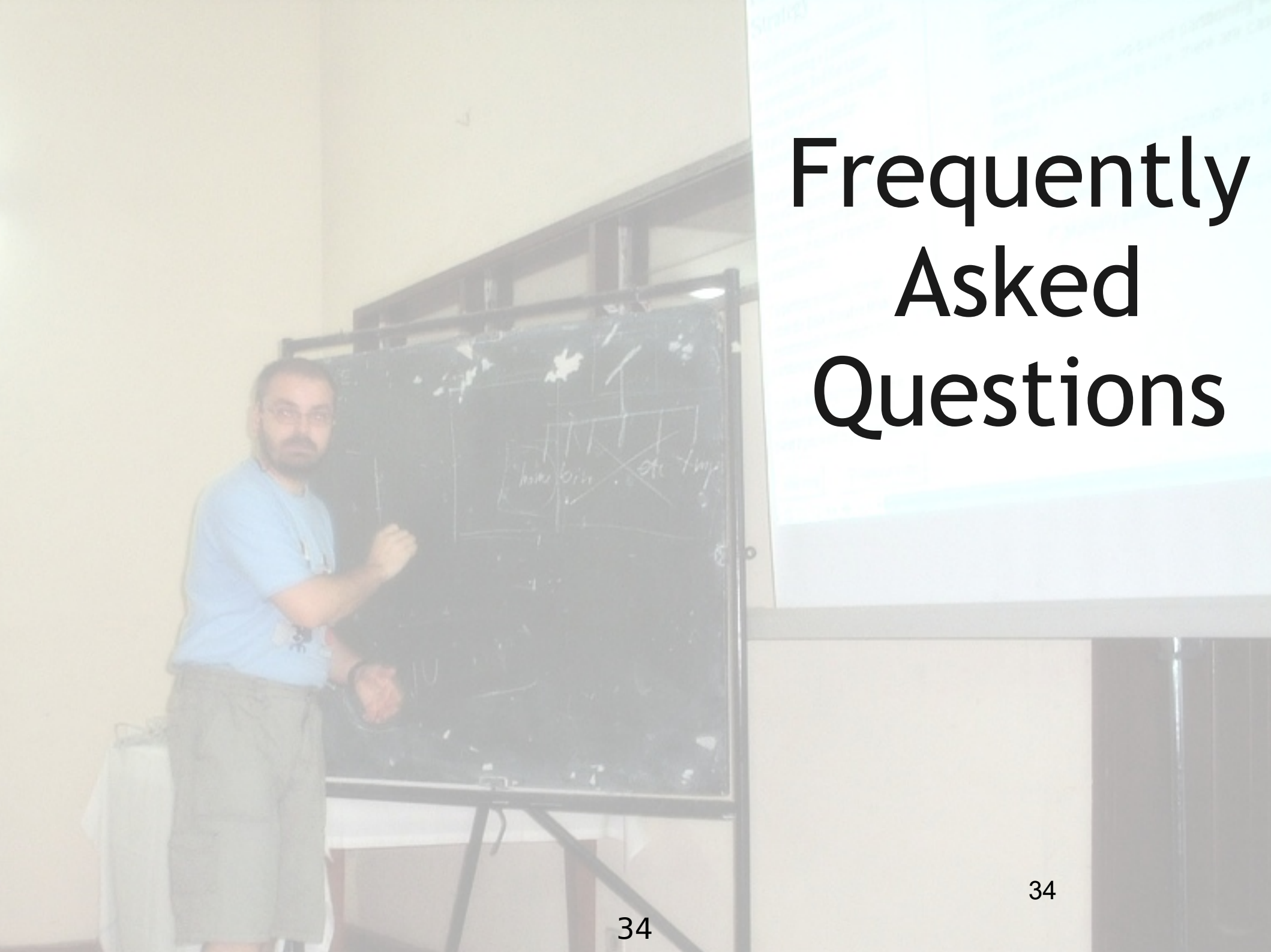
Disadvantages

More complex configuration

Roaming between APs is not supported

Routed access points





Frequently Asked Questions

34

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?

Acknowledgement

This Document is base on a document from
http://nsrc.org