AfNOG 2013
Wireless Networking

NSRC ICTP Ubuntunet ZAMREN

An unlikely introduction

You pay under $1 per Mbps/month in Europe

You pay about $1000 per Mbps/month in Zambia

I paid around $10 for unlimited mobile data in Tanzania.

I paid $60 for 3 GB in Zambia.

What's that go to do with wireless?

What s that go to do with wireless?
Everything.

Prices don't come down, they are brought down.

They are brought down by large numbers of users,
community and market pressure.
How are we gonna connect those?

Agenda for 2 days

Day 1

1 Introduction to WiFi, IEEE 802.11 standards and protocols, future outlook

2 Antenna fundamentals and link budget calculations

3 Integration into Wired LAN, Campus Wireless design Roaming considerations

4 Point to point links, Outdoor Deployment

5 (Solar) Powering networks

Agenda for 2 days

Day 2

1 Wireless security, authentication and access control

2 Access Points and client configuration

3 Wireless configuration lab - ?

FAQS & Discussion

4 Copperbelt University Case Study

SPECIAL EXTRA:

Free spectrum beyond Wifi: TV White Spaces

Introduction to 802.11 / WiFi

Sebastian Büttrich, NSRC - Last edit: June 2013

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
- Frequently Asked Questions

”Free” wireless

Licensed vs Unlicensed

- Most commercial wireless devices (mobile phones, television, radio, etc.) use **licensed** radio frequencies. Large organizations pay high licensing fees for the right to use those radio frequencies.
- WiFi uses **unlicensed / license exempt spectrum**, typically wihtout license fee.
- **Open spectrum, open standards, open technology** are the reason for wireless success.

”Free” wireless

And mobile data?

- As demands grow, mobile frequencies and standards struggle with carrying all the data.
- **The largest part of the data of the smartphone revolution is carried by open spectrum (WiFi).**

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.
- **Other interesting ISM bands:**

  around 433 MHz, 915 MHz, 17 Ghz

  \- **TV ”white space”** (50-800 MHz)

ISM bands

The ISM bands defined by the ITU-R are:

Frequency range		Bandwidth	Center frequency	Availability
6.765 MHz	6.795 MHz	30 kHz	6.780 MHz	Subject to local acceptance
13.553 MHz	13.567 MHz	14 kHz	13.560 MHz	
26.957 MHz	27.283 MHz	326 kHz	27.120 MHz	
40.660 MHz	40.700 MHz	40 kHz	40.680 MHz	
433.050 MHz	434.790 MHz	1.84 MHz	433.920 MHz	Region 1 only and subject to local acceptance
902.000 MHz	928.000 MHz	26 MHz	915.000 MHz	Region 2 only (with some exceptions)
2.400 GHz	2.500 GHz	100 MHz	2.450 GHz	
5.725 GHz	5.875 GHz	150 MHz	5.800 GHz	
24.000 GHz	24.250 GHz	250 MHz	24.125 GHz	
61.000 GHz	61.500 GHz	500 MHz	61.250 GHz	Subject to local acceptance
122.000 GHz	123.000 GHz	1 GHz	122.500 GHz	Subject to local acceptance
244.000 GHz	246.000 GHz	2 GHz	245.000 GHz	Subject to local acceptance

Source: wikipedia


Wi Fi ™
BELKIN
Skype
6:23 AM
skype
Menu
Contacts
Eee PC
ASUS
LINKSYS

802.11 standards - the old ones

	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

802.11 standards – the new ones

	Data rates [Mbps]	Freq [GHz]	channel access
ac	> 1000?	2.4/5	OFDM, MU-MIMO
ad	> 6000 (?)	60 (!)	keep in mind: mm waves! Very short range, LOS.
af	some 10-100?	0.2-0.8	aka **TV White Spaces** **NLOS!**

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

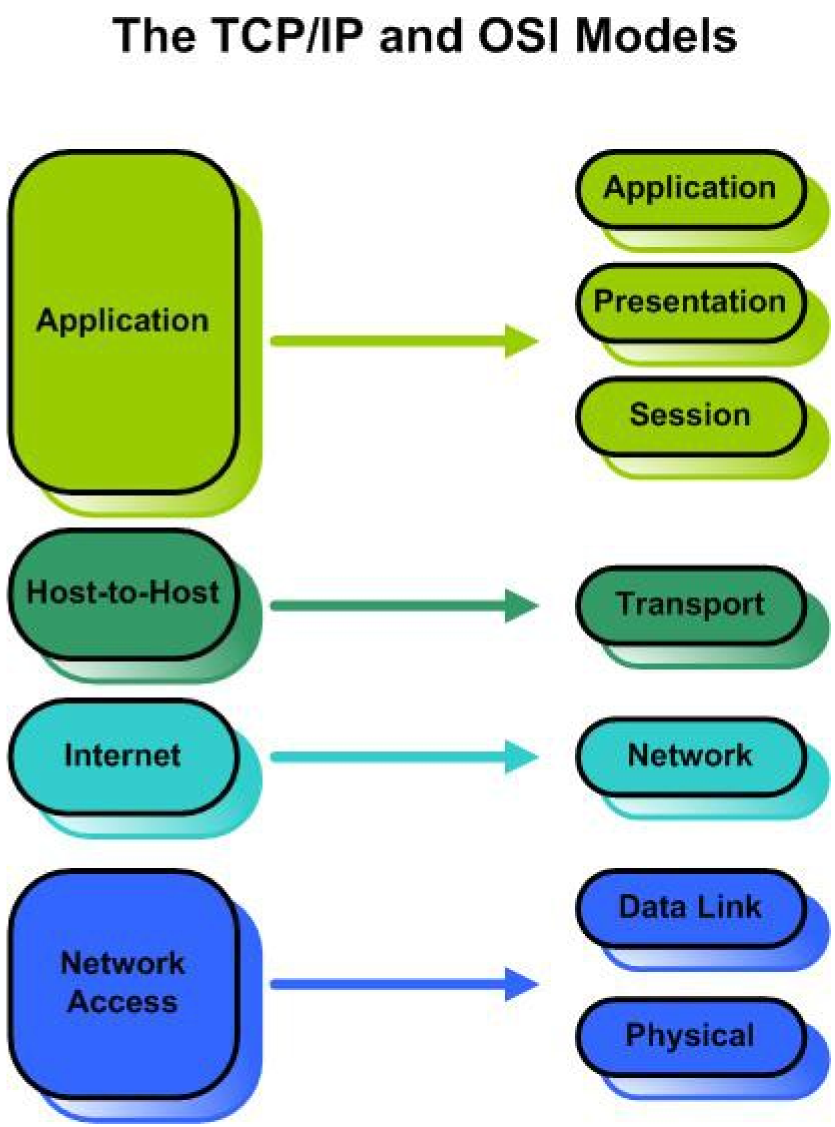
Compatibility of standards

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



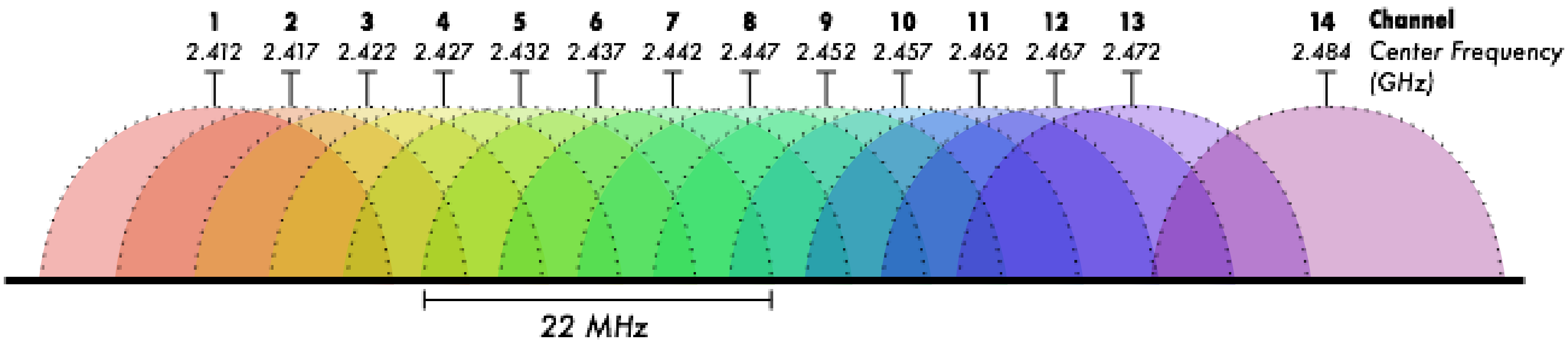
Layer 1/2

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

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

- Frequency / channel
- Radio operating mode (Managed, station/client, ad-hoc)
- Network name (SSID)
- Security features (e.g. WPA, WPA2)

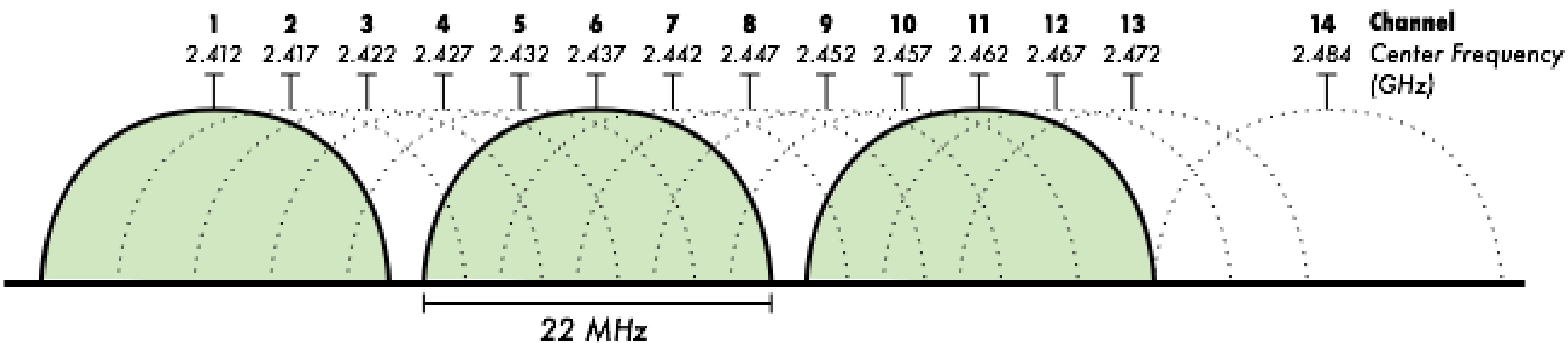
802.11 WiFi Channels



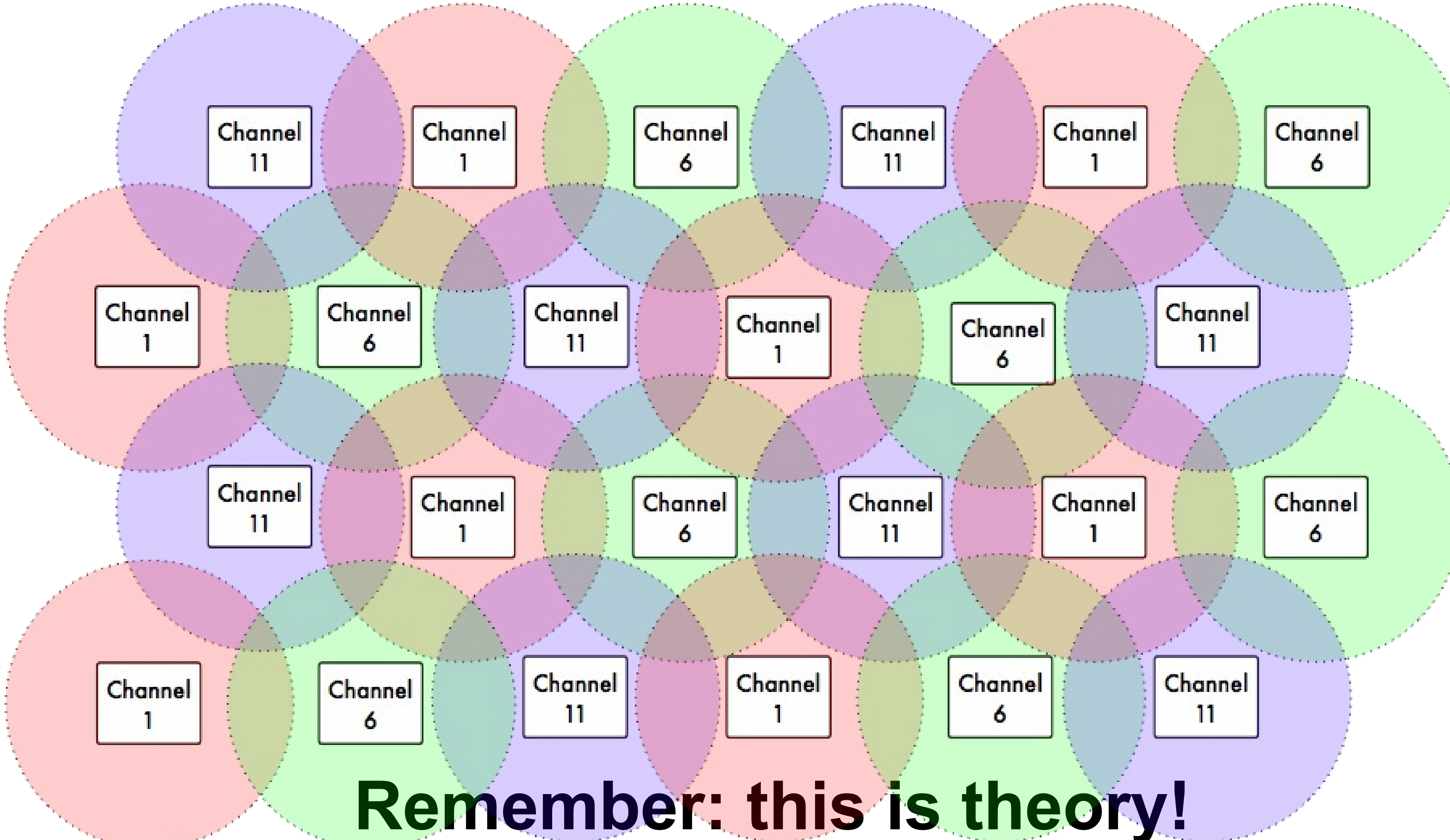
Frequency bands are further divided into channels, e.g. 14 channels of 22 MHz width each in the 2.4 GHz band.

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

Non-overlapping channels: 1, 6, 11



Channel design



Remember: this is theory!

Reality does not look that nice.

Wireless network topologies

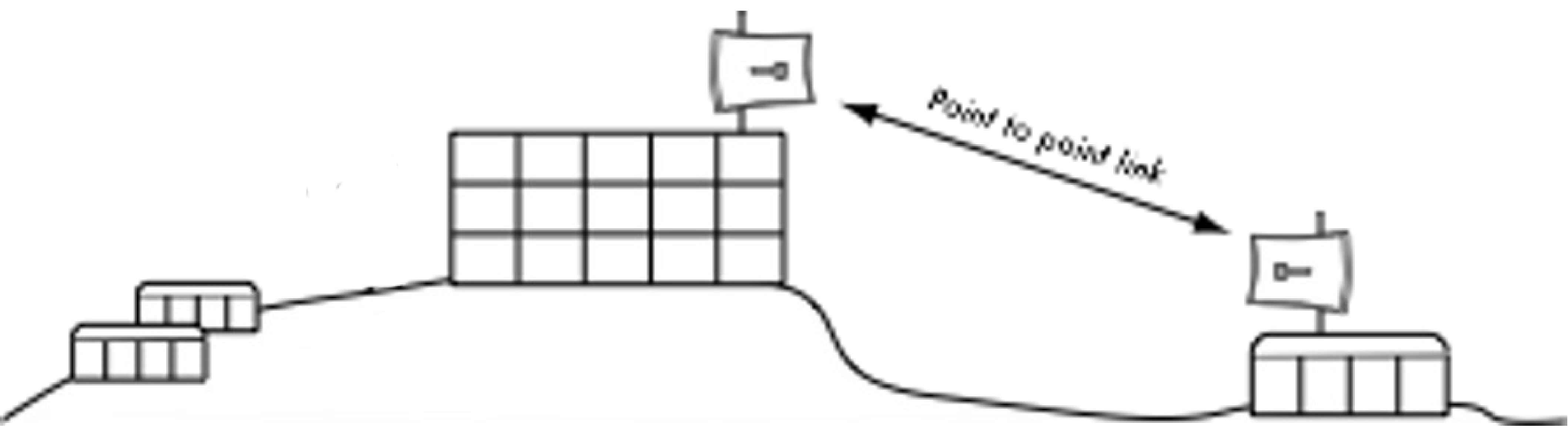
Any complex wireless network can be thought of as a combination of one or more of these types of connections:

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

Point to Point

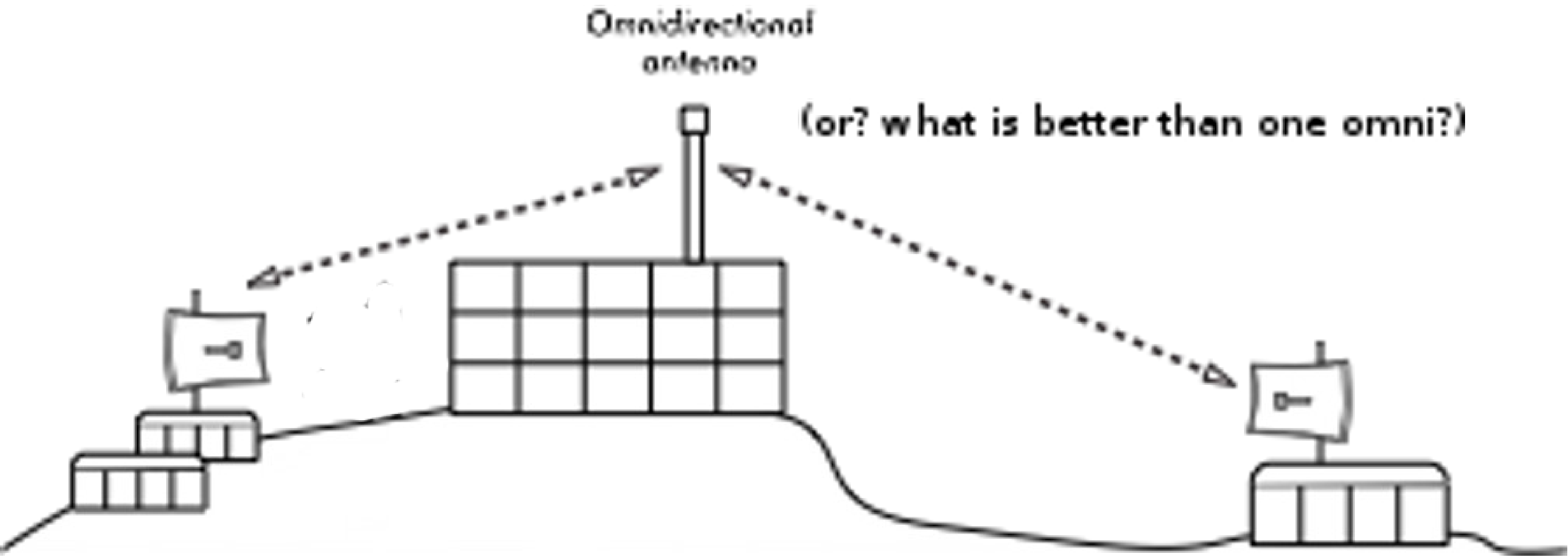
The simplest connection is the ***point-to-point*** link.

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



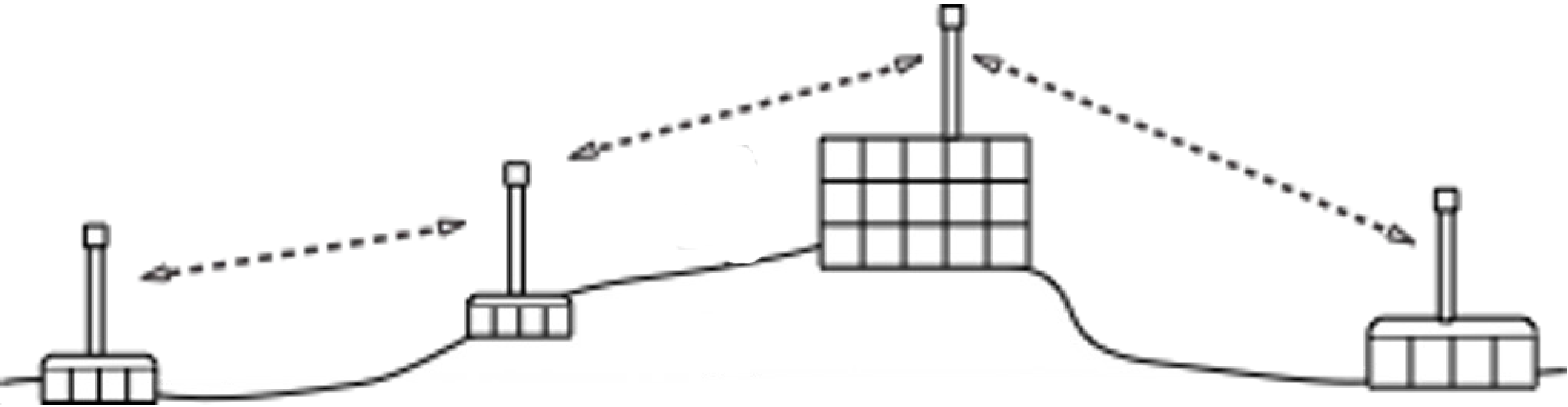
Point to Multipoint

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.

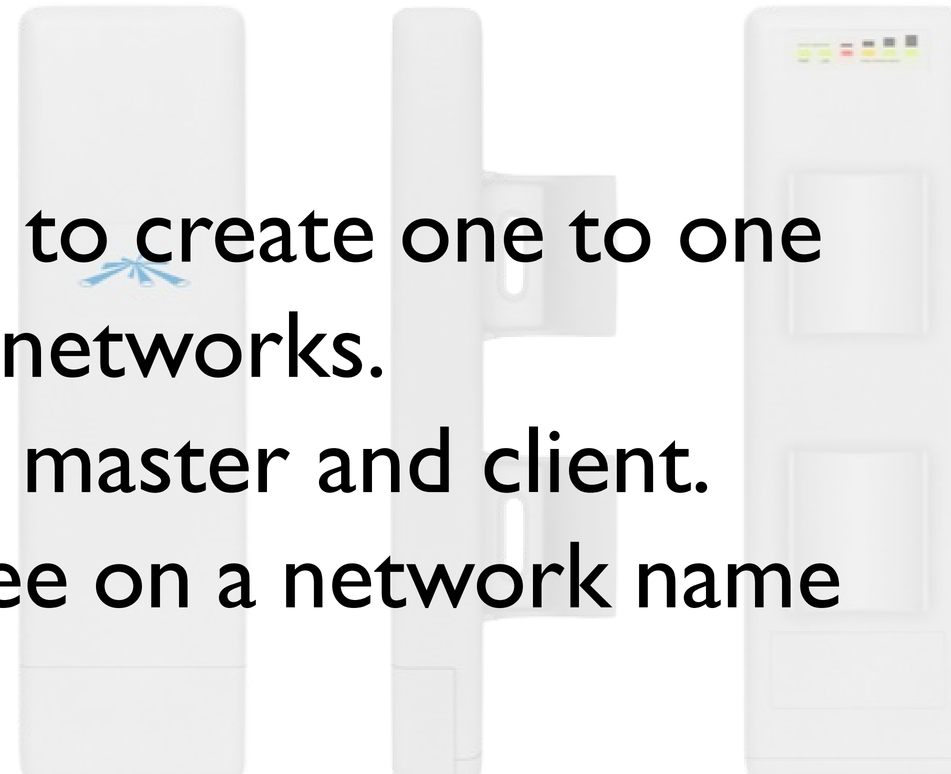
WiFi devices in master mode can only communicate with devices that are associated with it in ***managed*** mode.

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).

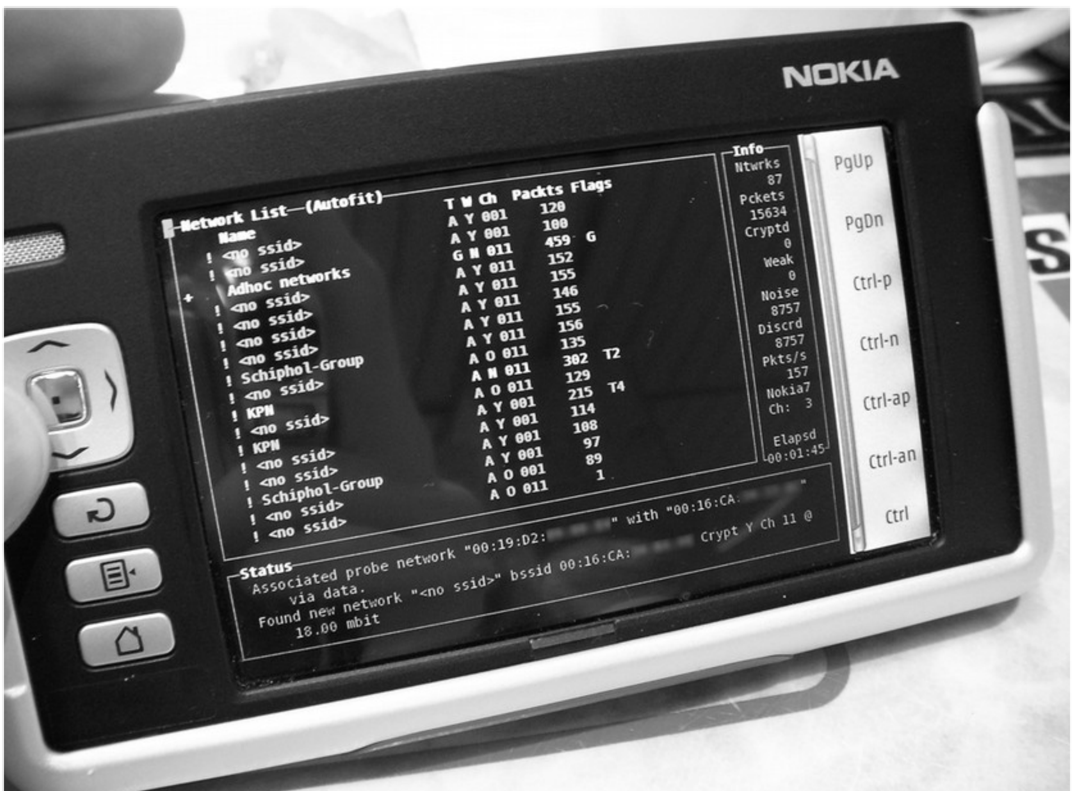
Ad-hoc Mode



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.

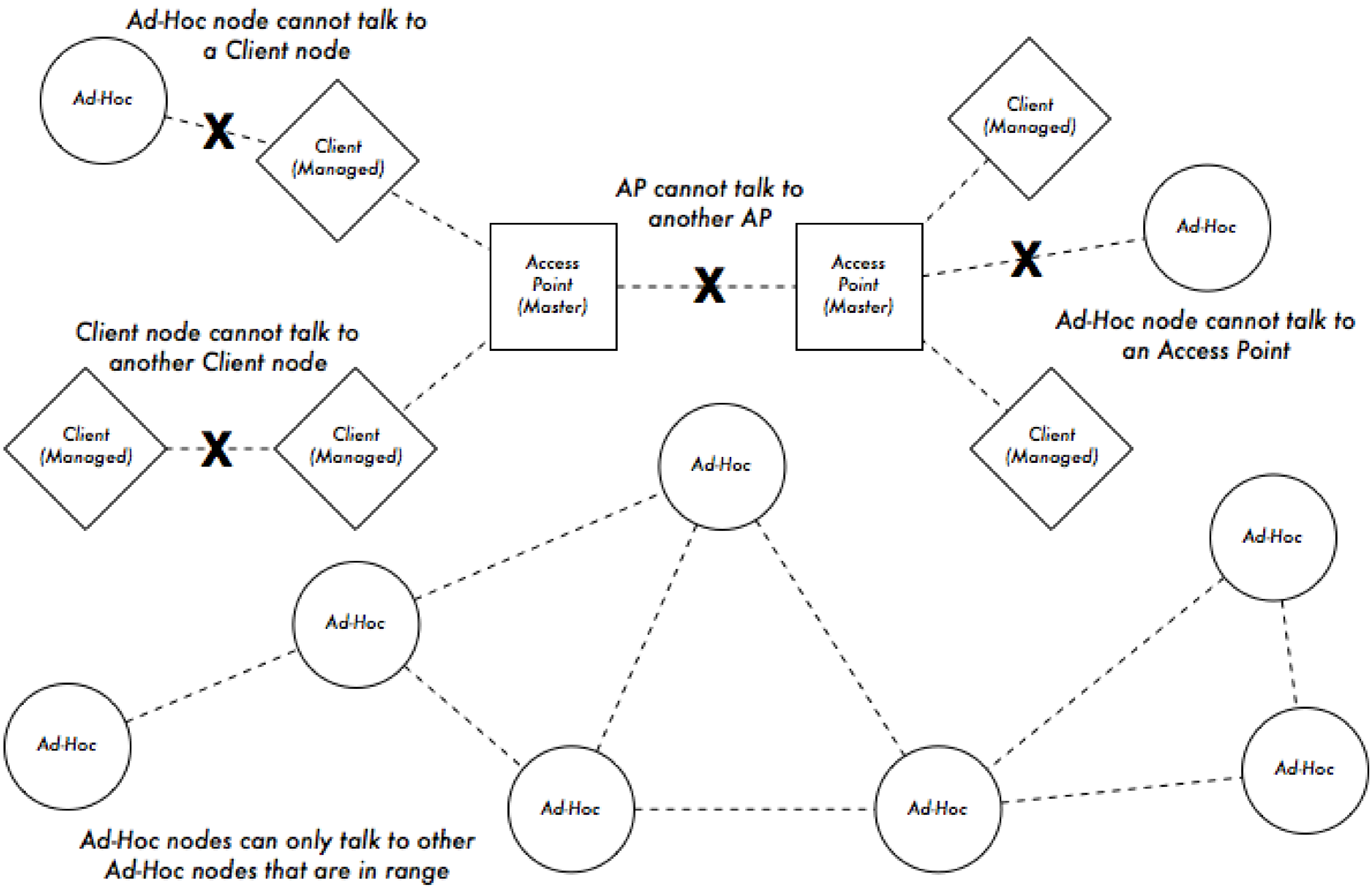
Monitor Mode

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



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).

In most situations, use of WDS is not needed and **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

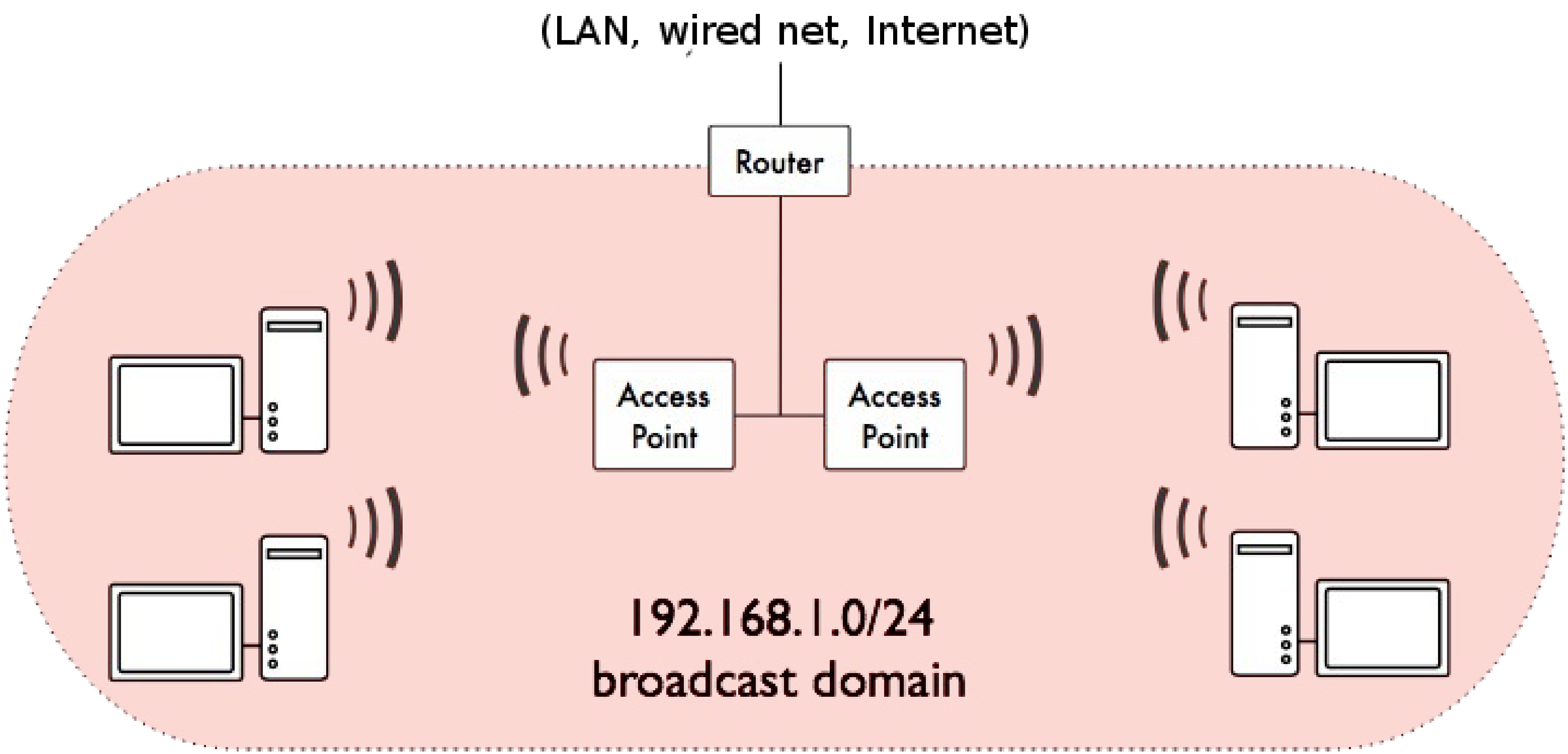
Increasingly inefficient as nodes are added

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

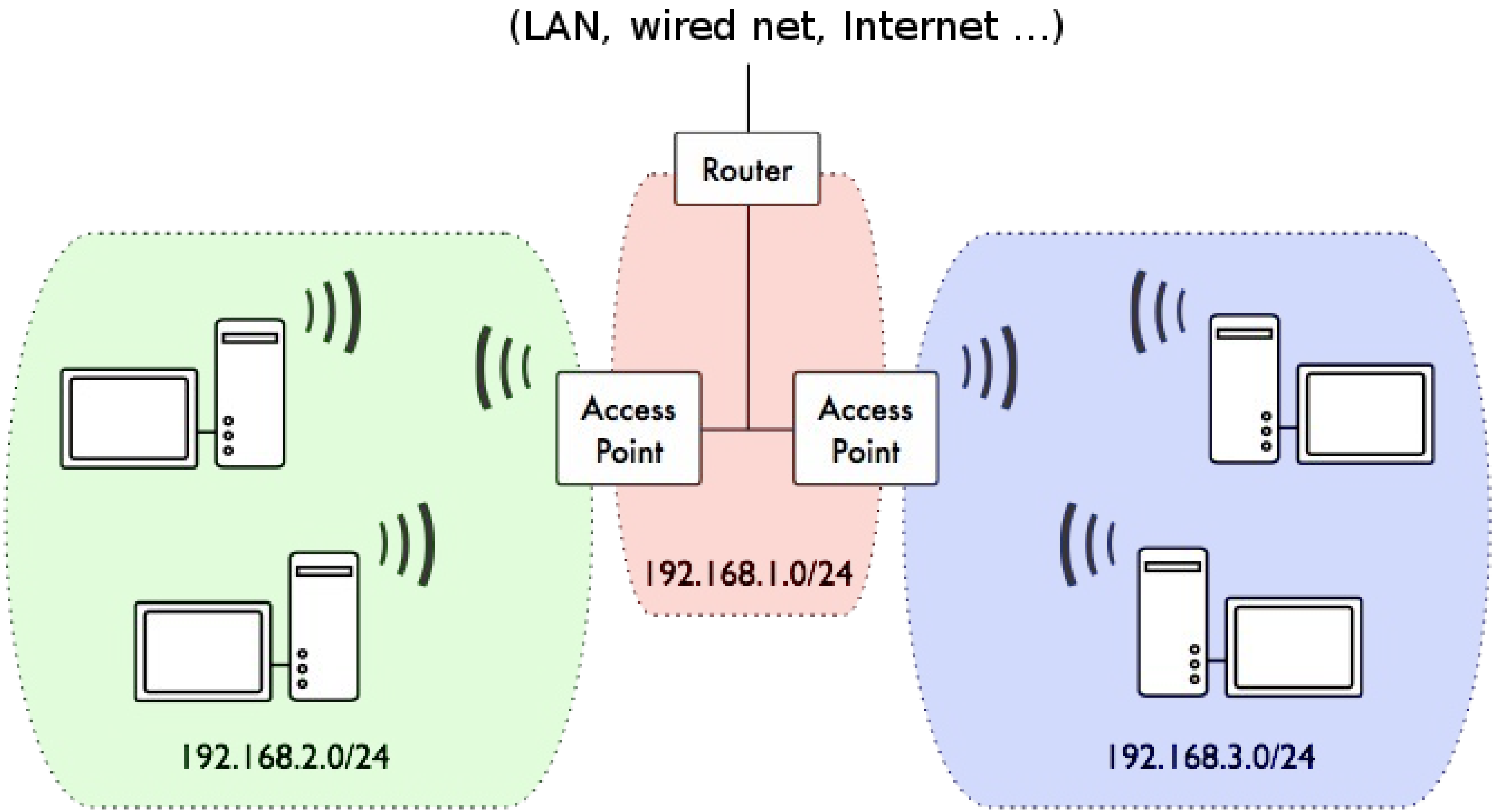
A variety of routing protocols and bandwidth management tools are available

Disadvantages

More complex configuration

Roaming between APs is not supported

Routed access points



Frequently Asked Questions

41

Frequently Asked Questions

- How fast?
- How far?
- How many clients?
- What should I buy?

How fast?

For end users:

802.11n can bring ~100 Mbps to a laptop, tablet or phone.
802.11ac will do more.

For point to point infrastructure:

We can do some 100 Mbps and up to 1 Gpbs over many kilometers.

How far?

How far does one access point reach?
That question does not make sense.
It is the sound of one hand clapping.
You can only talk about reach between two devices.

Sectored hotspots can cover a radius of some 100 meters,
Point to point links can go
100 km and more.

How many clients?

How many end users on one AP?

You can have 100 *very moderate* users on one AP.
More realistically, you might want 10, 20, 30 users on one AP.

Don't forget you ll have to carry their traffic somewhere.

How many clients?

What can we do today
(with the money we have)?

- 10 Mbps over 1 km for $100
- 150 Mbps over 10 km for $200
- 1 Gbps over 10 km for $3000
- Up to 100 km distance (and beyond)

- Simple hotspots for $50 per AP
- Managed access networks for $100 per AP

Future – new standards

- 802.11ac pushes speed limits

- TV White Space
  pushes NLOS distance limits

- (When) will they make it
  into laptops and phones?

Future – more devices

Example: Handling campus wireless

- The average user will have 2, 3 devices
- BYOD = Bring your own device
- How do i manage that?

Future – more traffic

Example: Handling campus traffic upstream

- If i give 1000 students 100 Mbps each, that's 100 Gbps …
- Golden rule for bandwidth:
  whatever i offer
  will be used to the maximum
- Where should i limit the speed?

Future – security and access

Campus: Challenges are changing

- The problem used to be
  keeping the outsider out

- The problem today tends to be the insider.
- *Rogue* access points are common.

- How do i manage

  access, accounts, passwords, keys

  for 10,000+ students and staff?

Learning more

- http://wirelessu.org
- http://nsrc.org
- http://wireless.ictp.it/
- http://wtkit.org/ Wireless Training Kit (ICTP/ITU)
- The **green book**: http://wndw.net
- http://wire.less.dk

Thank you!

Questions and comments?

sebastian@nsrc.org