

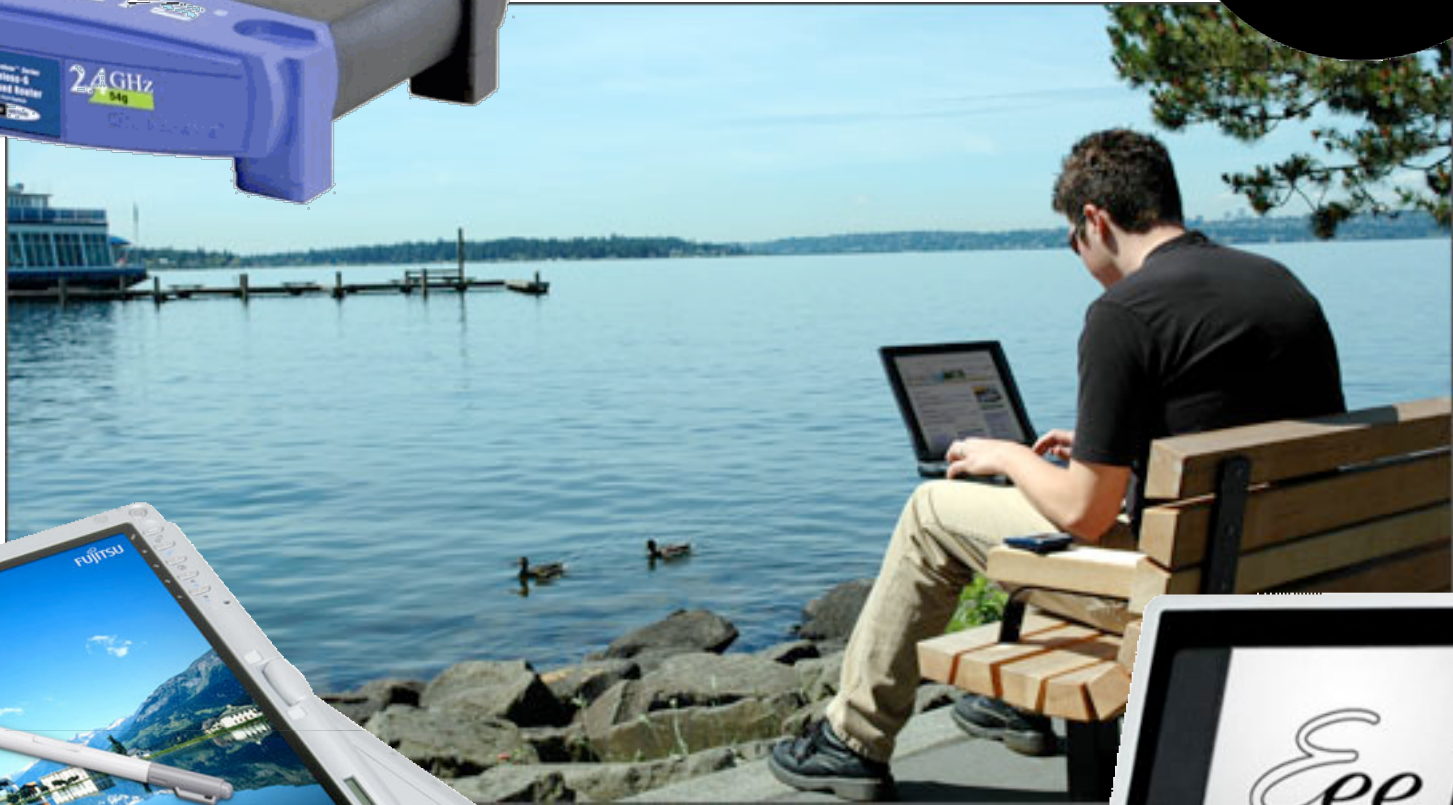
# Introduction to Wide-Area WiFi

AfNOG 2009 Wireless Tutorials  
Cairo



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

**WirelessU.org**



# 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 ISM and UNII bands.
- **802.11b** supports up to 11 Mbps using the 2.4 GHz ISM band.
- **802.11g** supports up to 54 Mbps using the 2.4 GHz ISM band.
- **802.11n** (draft) supports up to 300 Mbps using the 2.4 GHz and 5 GHz ISM and UNII bands.
- **802.16** (WiMAX) is not 802.11 WiFi! It is a much more complex technology that uses a variety of licensed and unlicensed frequencies.

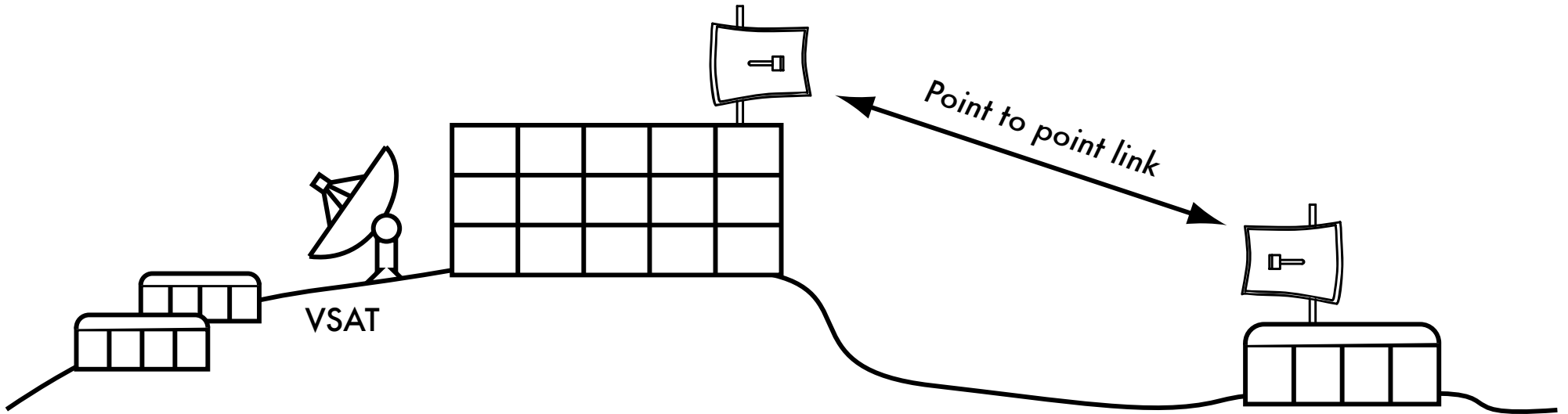
# Wireless network design

Any 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***

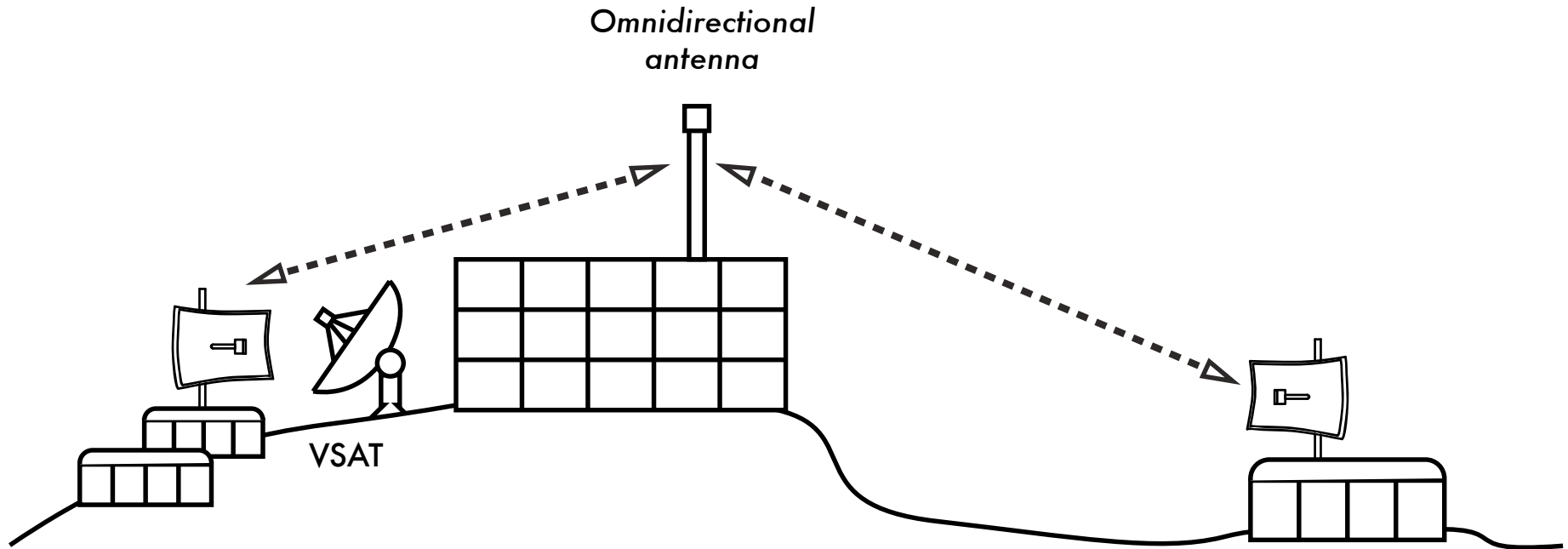
# Point to Point

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



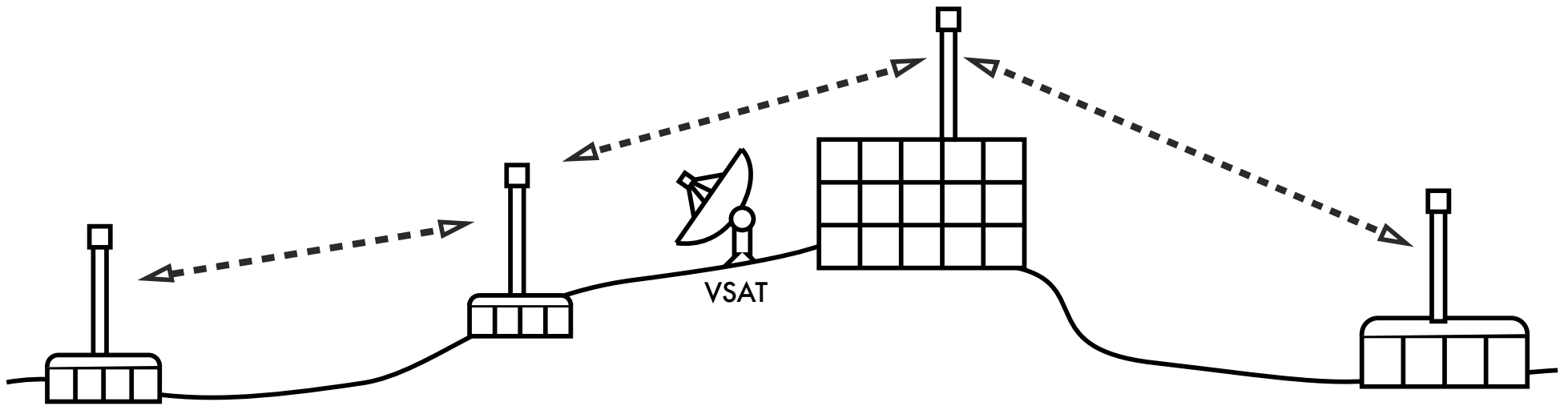
# Point to Multipoint

When more than one computer 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)



# Radio Modes

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

- ***Master*** (Access Point)
- ***Managed*** (also known as ***client*** or ***station***)
- ***Ad-hoc***
- ***Monitor***
- Other proprietary modes (e.g. Mikrotik Nstreme)

Radios may only operate in one mode at a time.\*

# Master Mode

**Master mode** (also called AP or infrastructure mode) is used to create a service that looks like a traditional access point. The wireless card creates a network with a specified name (called the **SSID**) and channel, and offers network services on it.

Wireless cards in master mode can only communicate with cards that are associated with it in **managed** mode.

# Managed Mode

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

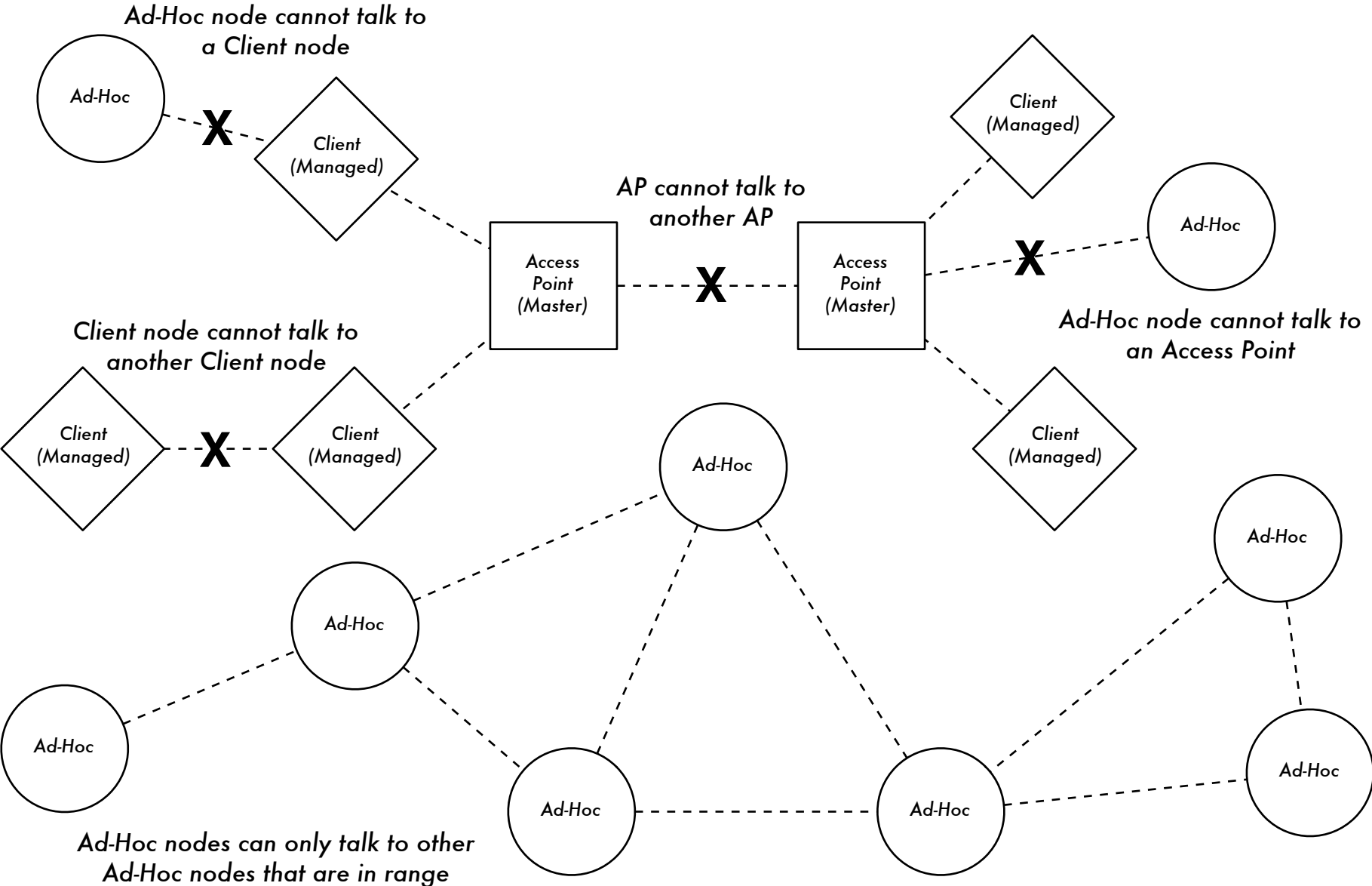
Clients using a given access point are said to be ***associated*** with it. Managed mode cards do not communicate with each other directly, and will only communicate with an associated master.

# Ad-hoc Mode

***Ad-hoc mode*** creates a multipoint-to-multipoint network when there is no master or AP available.

In ad-hoc mode, each wireless card communicates directly with its neighbors. Nodes must be in range of each other to communicate, and must agree on a network name and channel.

# WiFi radio modes in action



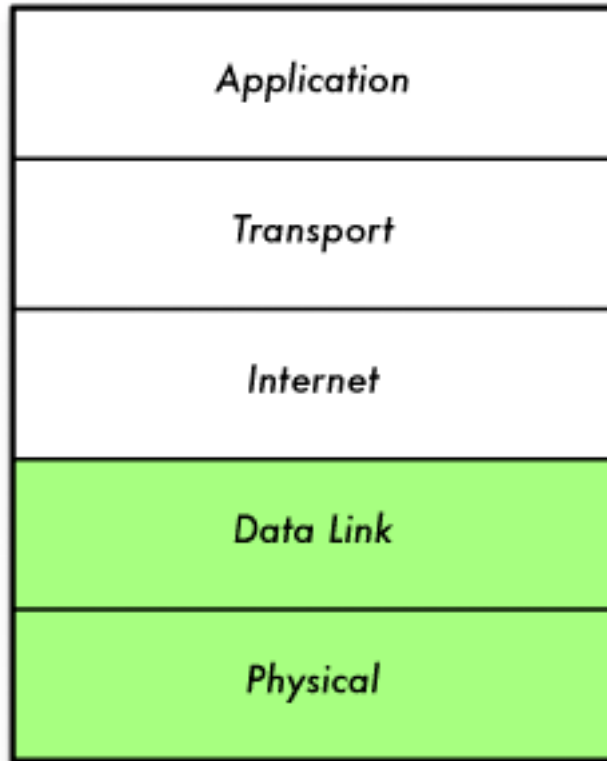
# Monitor Mode

***Monitor mode*** is used by some tools (such as Kismet) 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.

Monitor mode is not used for normal communications.

# The TCP/IP model

802.11 WiFi provides a link-local connection.



# Bridged networking

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

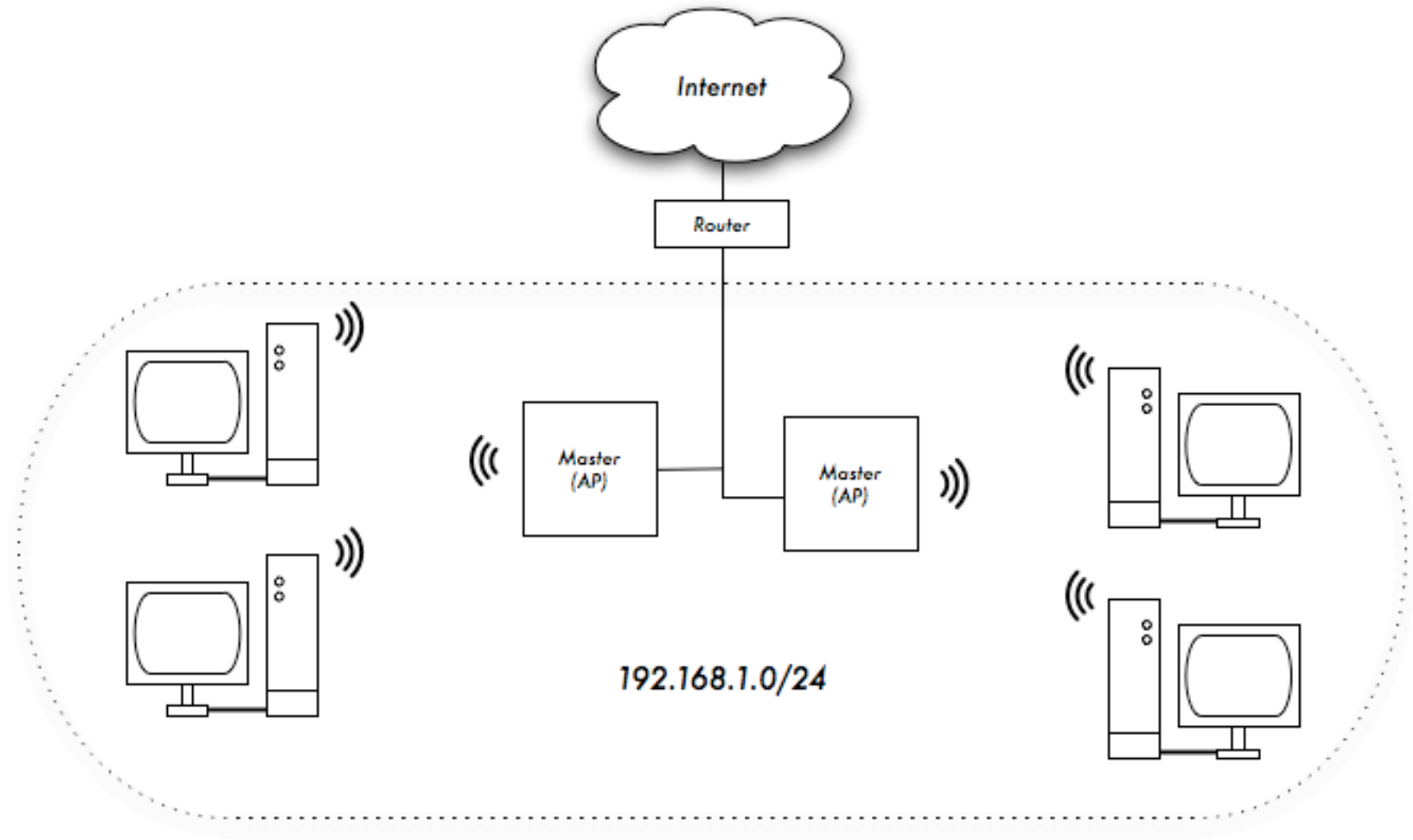
## **Advantages**

- 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

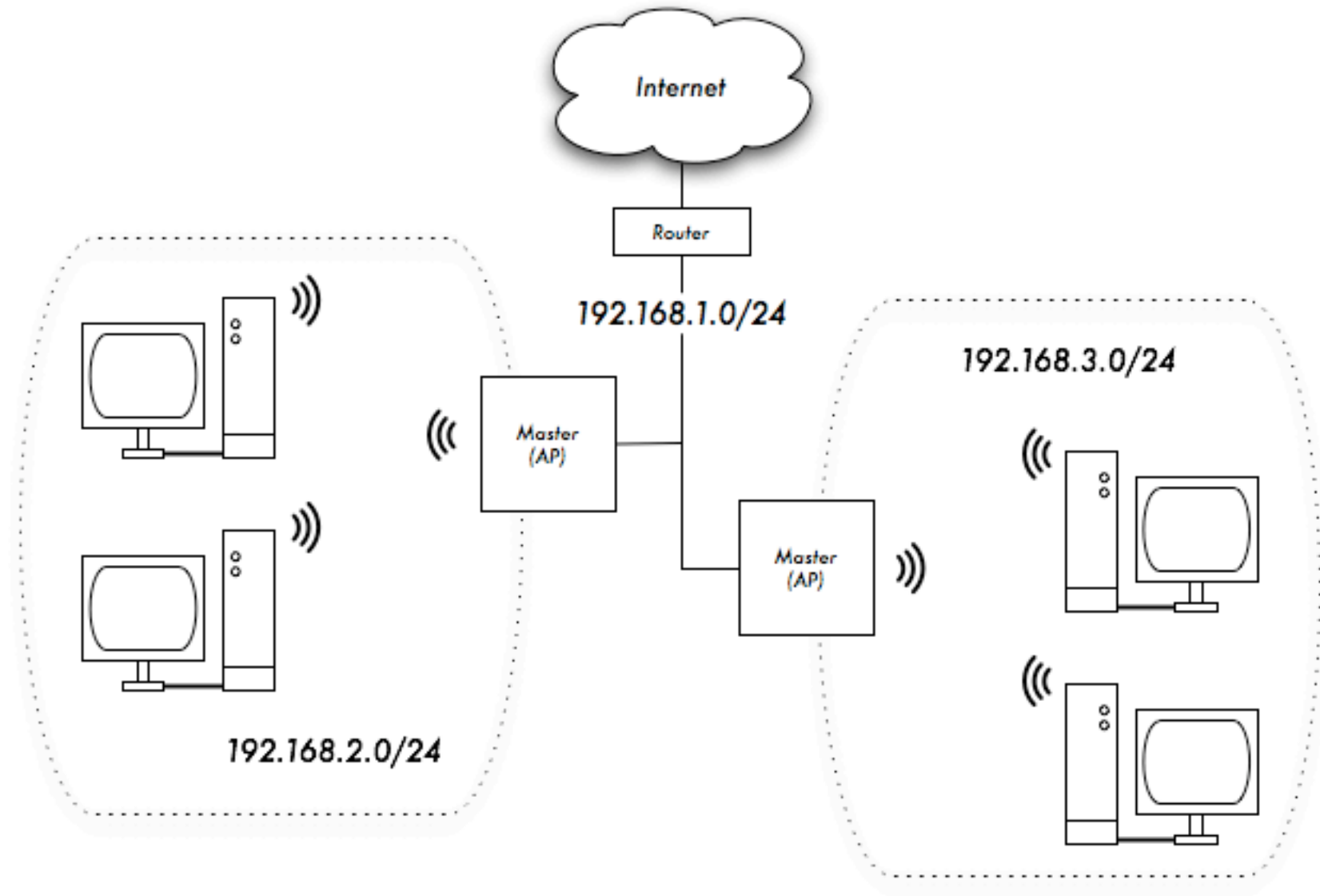


# Routed networking

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, HSLs, AODV) work very well with wireless networks, particularly when using radios in ad-hoc mode

# Routed access points



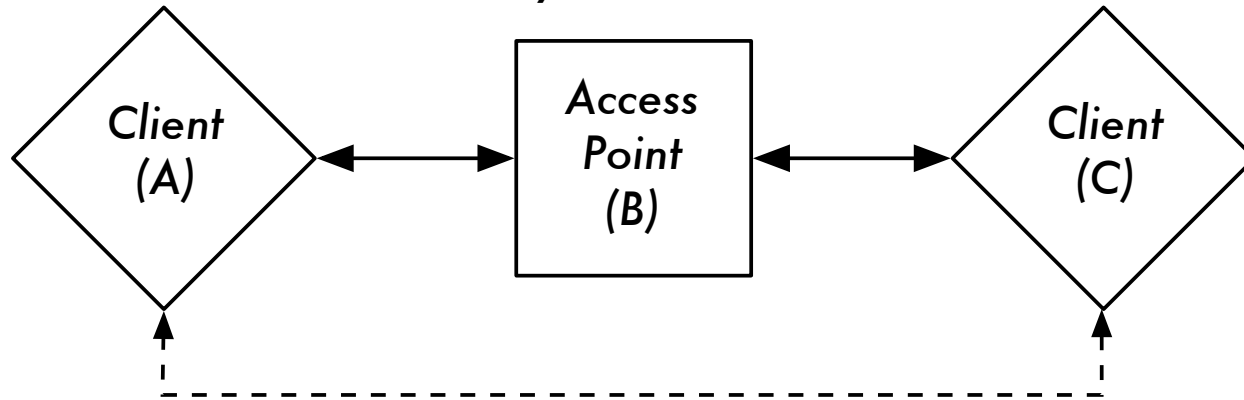
# Relaying traffic

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.

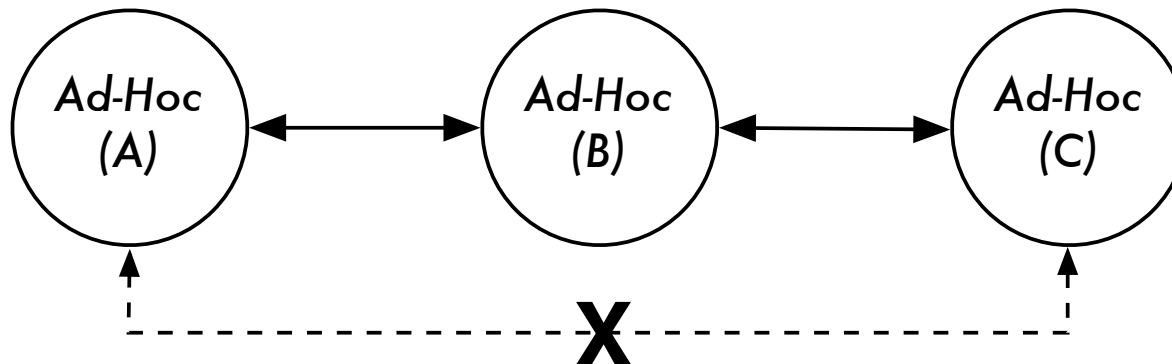
In infrastructure mode, clients must be within range of an access point. The AP will relay traffic between all associated clients, but clients **cannot** talk to each other directly.

# AP vs. Ad-hoc

*Clients A and C are in range of Access Point B but not each other.  
Access Point B will relay traffic between the two nodes.*



*In the same setting, Ad-Hoc nodes A and C can communicate  
with node B, but not with each other.*

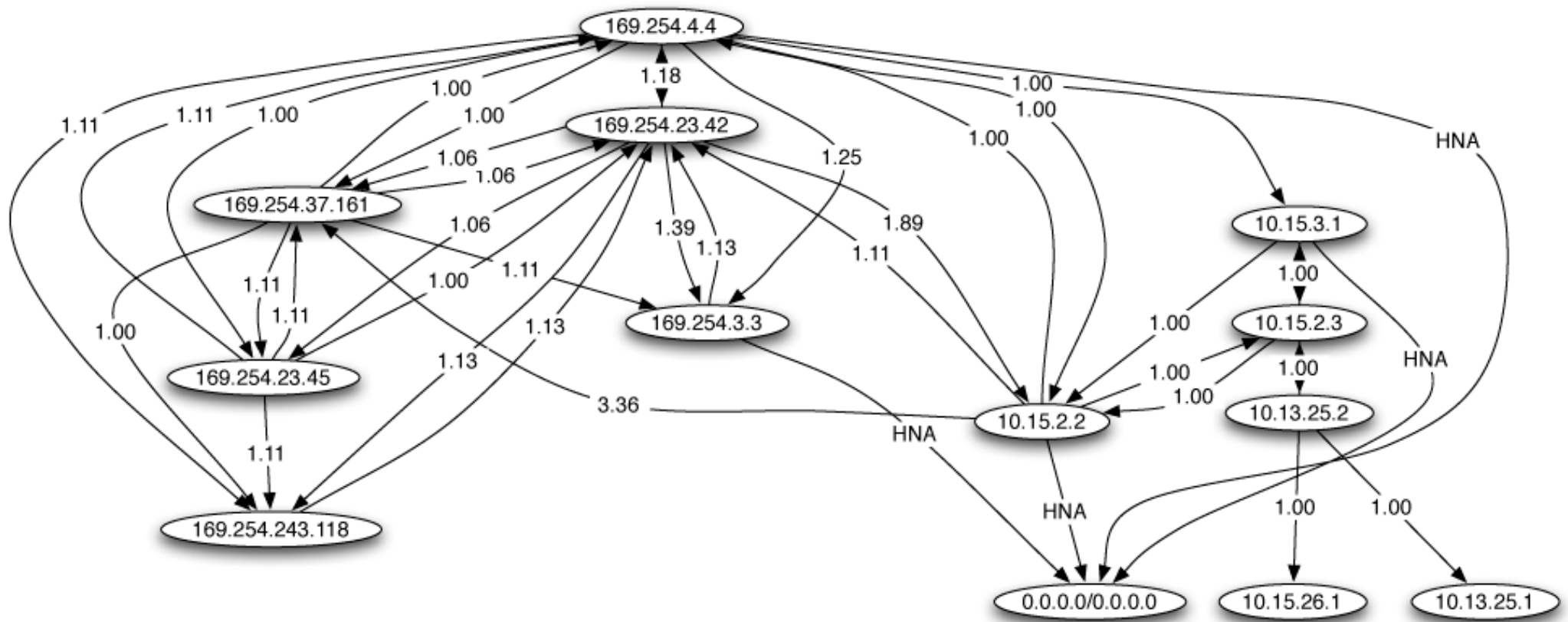


# Mesh = Ad-hoc + Routing

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 OLSR) may be applied to any physical network, including Master / Managed nodes, or even Ethernet.

# Dynamic mesh

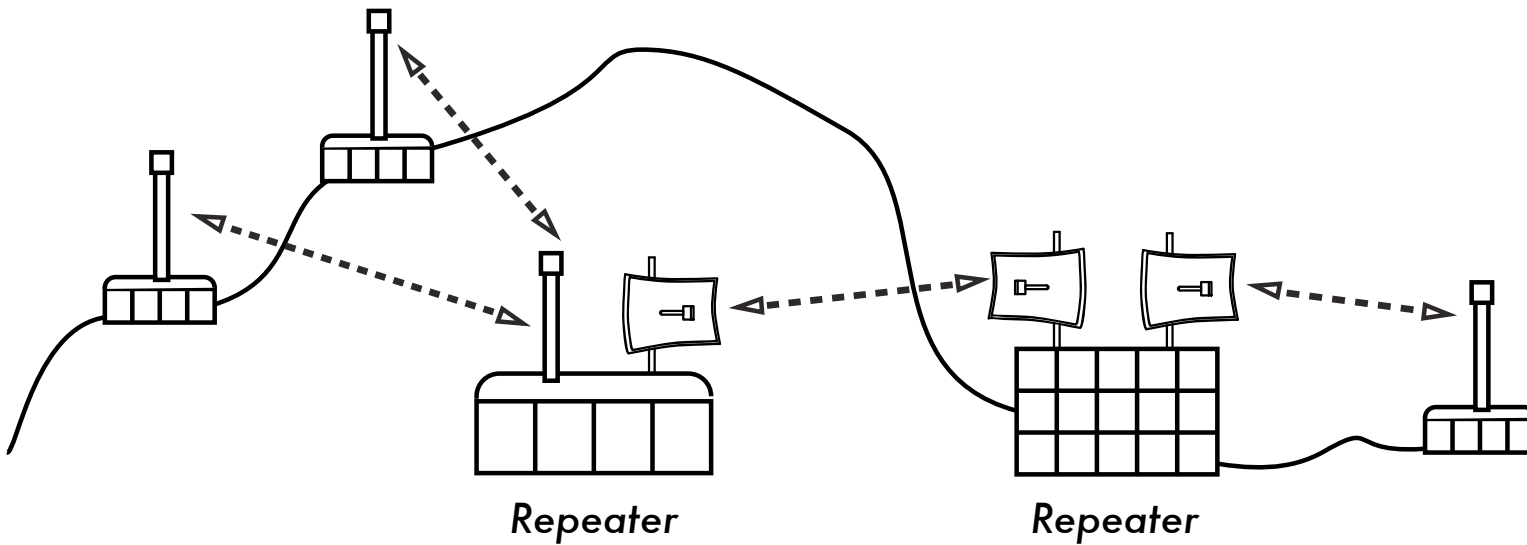
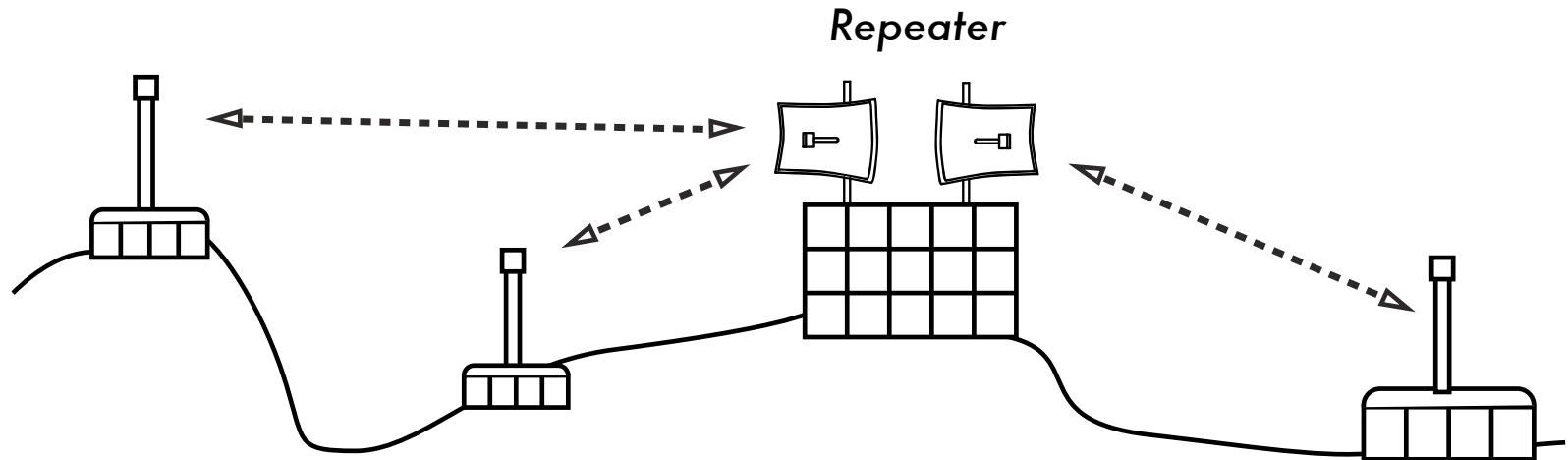


# Repeaters

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 networks were 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 (channel reservation)
- Specify a maximum packet size, above which CTS/RTS is used
- CTS/RTS is not perfect, but can help at a cost of overall throughput. It only applies when access points are used.

# Timing Issues

Due to the very fast timing of 802.11 frames, 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) use TDMA to avoid these ACK timing issues.

# Anything is Possible



279+ Kilometer links can be made!

# Credits

Portions of this talk were adapted from *Wireless Networking in the Developing World*, <http://wndw.net/>

