Introduction to WiFi Networking

The Abdus Salam
International Centre
for Theoretical Physics

Marco Zennaro
Ermanno Pietrosemoli

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

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.**

802.11 family

IEEE 802.11 VARIANT	FREQUENCY BANDS USED
802.11a	5GHz
802.11b	2.4GHz
802.11g	2.4GHz
802.11n	2.4 & 5 GHz
802.11ac	Below 6GHz
802.11ad	Up to 60 GHz
802.11af	TV white space (below 1 GHz)
802.11ah	700 MHz, 860MHz, 902 MHz, etc. ISM bands dependent upon country and allocations

802.11 family

LOWER FREQUENCY MHZ	UPPER FREQUENCY MHZ	COMMENTS
2400	2500	Often referred to as the 2.4 GHz band, this spectrum is the most widely used of the bands available for Wi-Fi. Used by 802.11b, g, & n. It can carry a maximum of three non-overlapping channels.
5725	5875	This 5 GHz band or 5.8 GHz band provides additional bandwidth, and being at a higher frequency, equipment costs are slightly higher, although usage, and hence interference is less.It can be used by 802.11a & n. It can carry up to 23 non-overlapping channels, but gives a shorter range than 2.4 GHz.

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

CLIENT

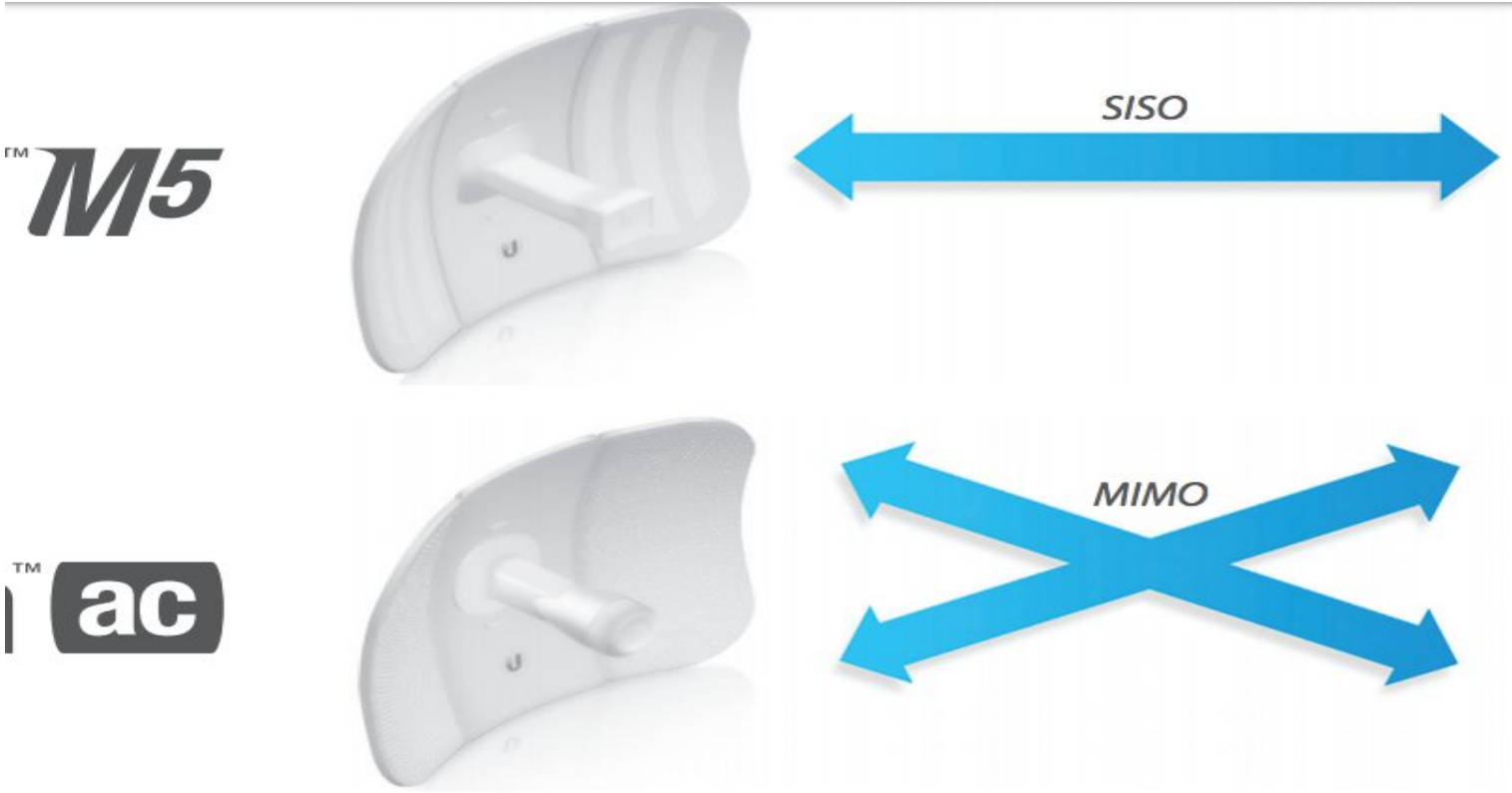
	802.11a	802.11b	802.11g	802.11n	802.16
802.11a	Yes			Yes @5GHz	
802.11b		Yes	Yes (slower)	Yes @2.4GHz	
802.11g		Yes (slower)	Yes	Yes @2.4GHz	
802.11n	Yes @5GHz	Yes @2.4GHz	Yes @2.4GHz	Yes	
802.16					Yes

IEEE 802.11 AC

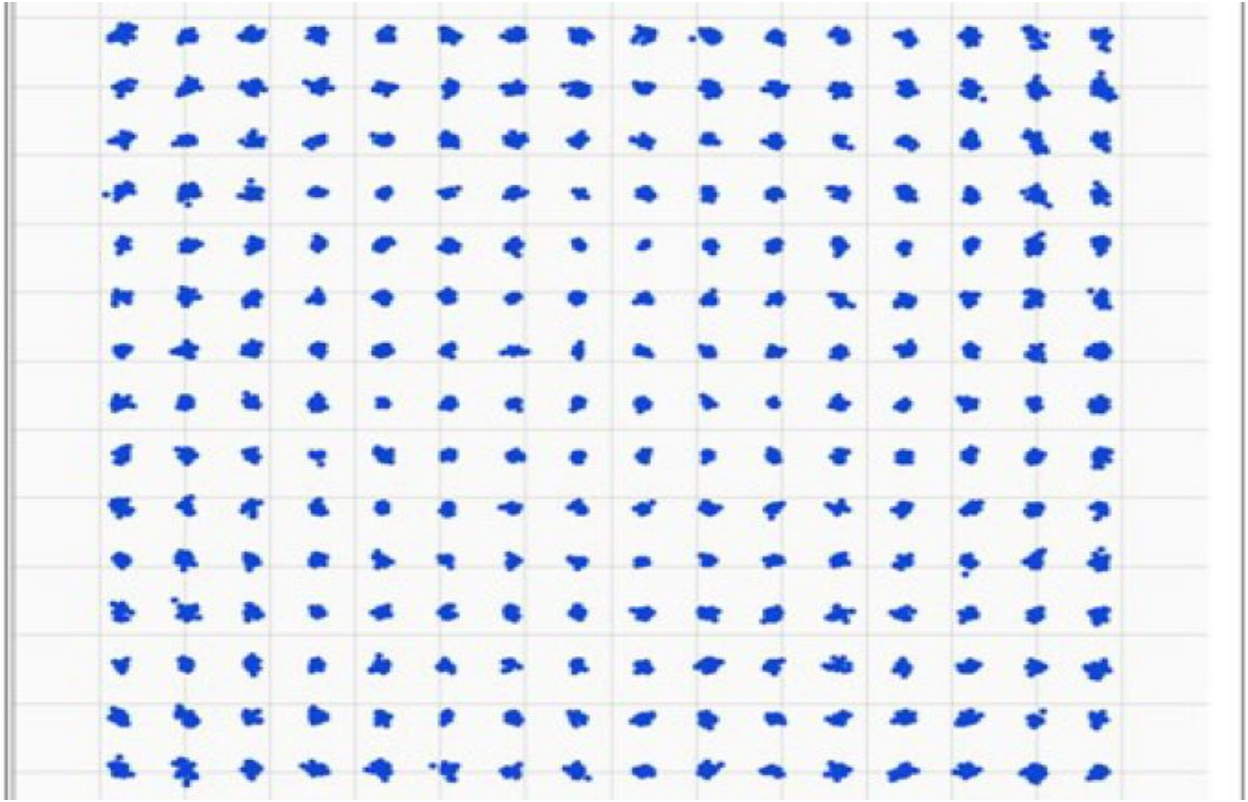
Improved performance by means of:

- Two or up to 8 Spatial streams (MIMO)
- Higher order modulation types (up to 256 QAM)
- Wider Channels bandwidth (up to 160 MHz)

IEEE 802.11 AC: MIMO



IEEE 802.11 AC, 256 constellation



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.

Data rates

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.

802.11ac offers a maximum theoretical data rate of 6 Gbps.

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 mode 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:

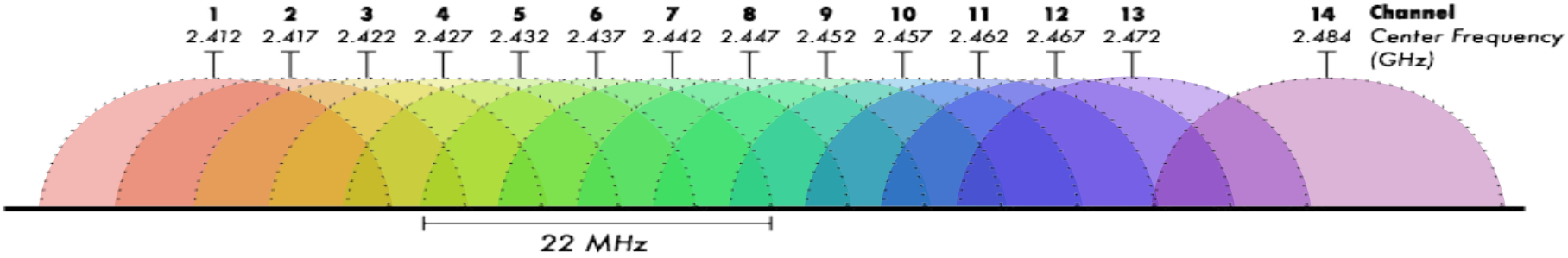
TCP/IP Protocol Stack	
5	Application
4	Transport
3	Internet
2	Data Link
1	Physical

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

802.11 WiFi Channels

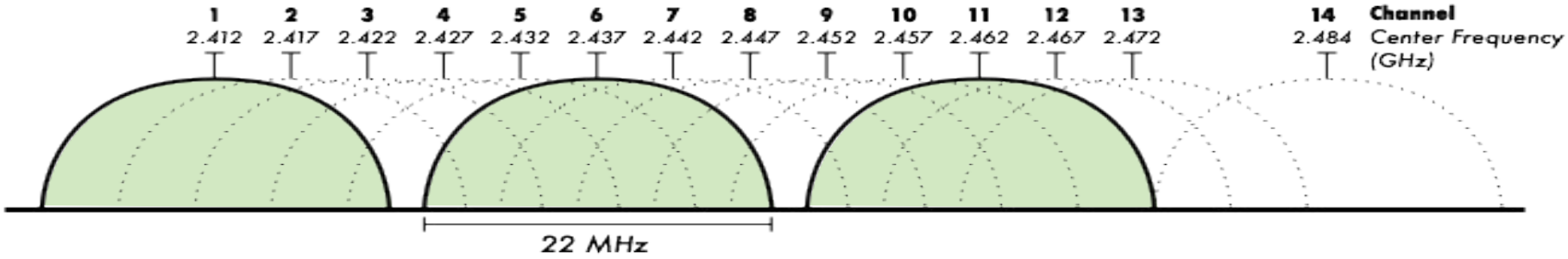
CHANNEL NUMBER	LOWER FREQUENCY MHZ	CENTER FREQUENCY MHZ	UPPER FREQUENCY MHZ
1	2401	2412	2423
2	2406	2417	2428
3	2411	2422	2433
4	2416	2427	2438
5	2421	2432	2443
6	2426	2437	2448
7	2431	2442	2453
8	2436	2447	2458
9	2441	2452	2463
10	2446	2457	2468
11	2451	2462	2473
12	2456	2467	2478
13	2461	2472	2483
14	2473	2484	2495

802.11 WiFi Channels

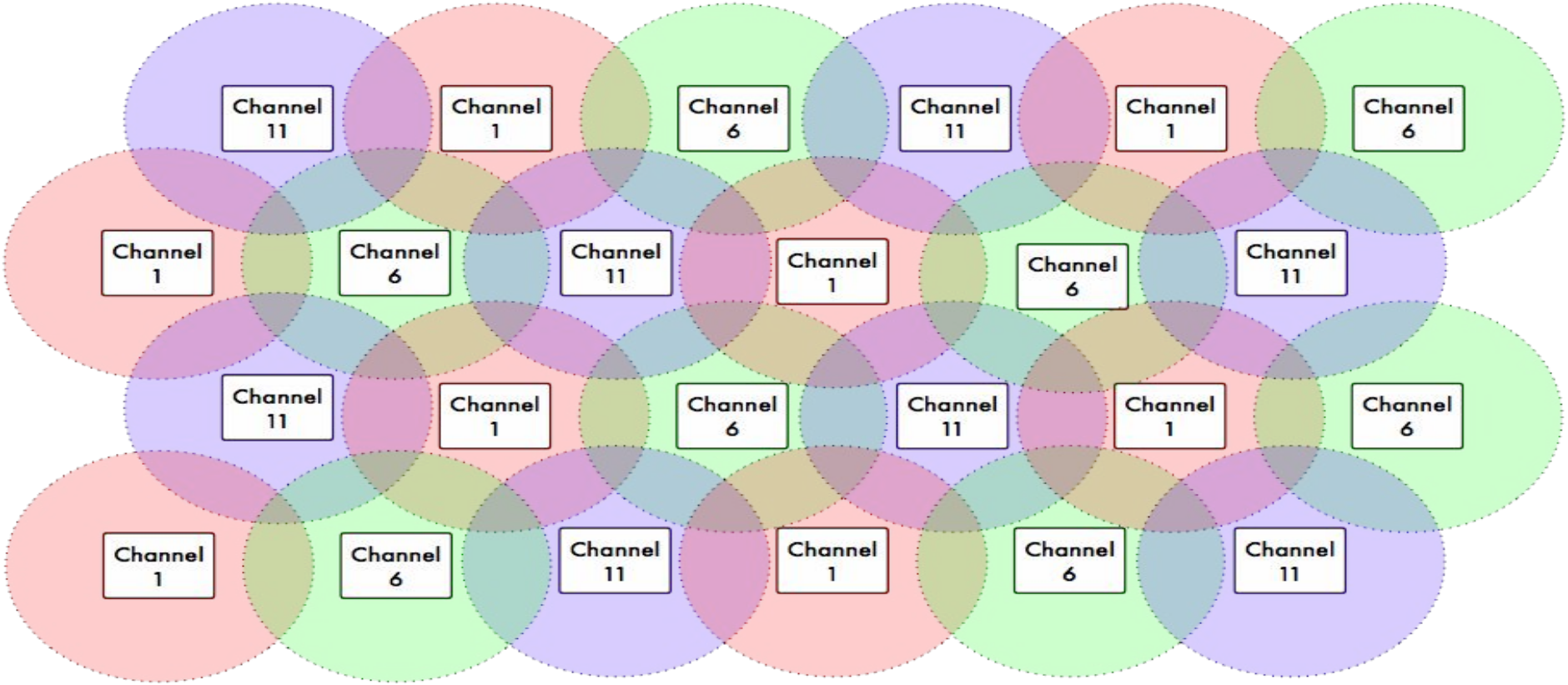


WiFi devices must use the same channel in order to communicate with each other. They send and receive on the same channel, so only one device may transmit at any time. This kind of connection is called ***half-duplex***.

Non-overlapping channels: 1, 6, 11



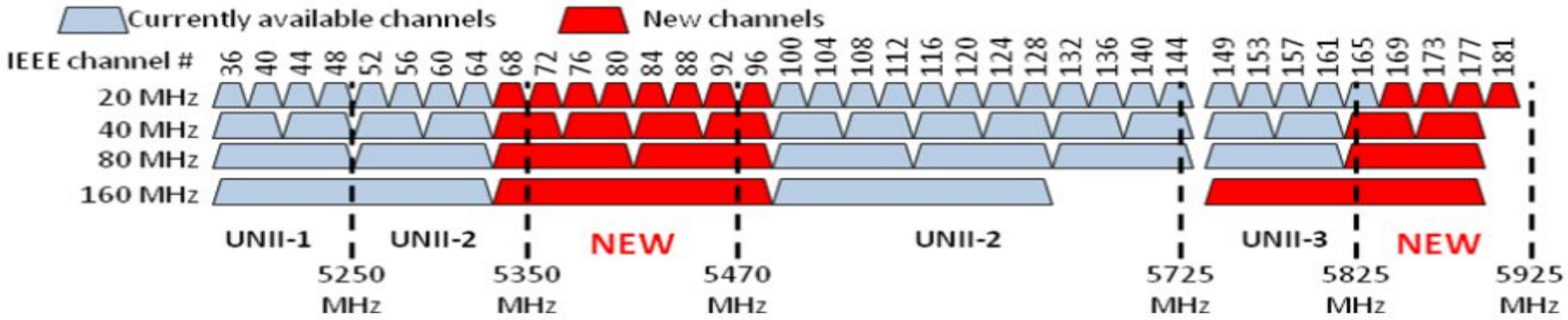
AP channel re-use



802.11 WiFi Channels

CHANNEL NUMBER	FREQUENCY MHZ	EUROPE (ETSI)	NORTH AMERICA (FCC)	JAPAN
36	5180	Indoors	✔	✔
40	5200	Indoors	✔	✔
44	5220	Indoors	✔	✔
48	5240	Indoors	✔	✔
52	5260	Indoors / DFS / TPC	DFS	DFS / TPC
56	5280	Indoors / DFS / TPC	DFS	DFS / TPC
60	5300	Indoors / DFS / TPC	DFS	DFS / TPC
64	5320	Indoors / DFS / TPC	DFS	DFS / TPC
100	5500	DFS / TPC	DFS	DFS / TPC
104	5520	DFS / TPC	DFS	DFS / TPC
108	5540	DFS / TPC	DFS	DFS / TPC
112	5560	DFS / TPC	DFS	DFS / TPC
116	5580	DFS / TPC	DFS	DFS / TPC
120	5600	DFS / TPC	No Access	DFS / TPC
124	5620	DFS / TPC	No Access	DFS / TPC
128	5640	DFS / TPC	No Access	DFS / TPC
132	5660	DFS / TPC	DFS	DFS / TPC
136	5680	DFS / TPC	DFS	DFS / TPC
140	5700	DFS / TPC	DFS	DFS / TPC
149	5745	SRD	✔	No Access
153	5765	SRD	✔	No Access
157	5785	SRD	✔	No Access
161	5805	SRD	✔	No Access
165	5825	SRD	✔	No Access

802.11 WiFi Channels



Wireless network topologies

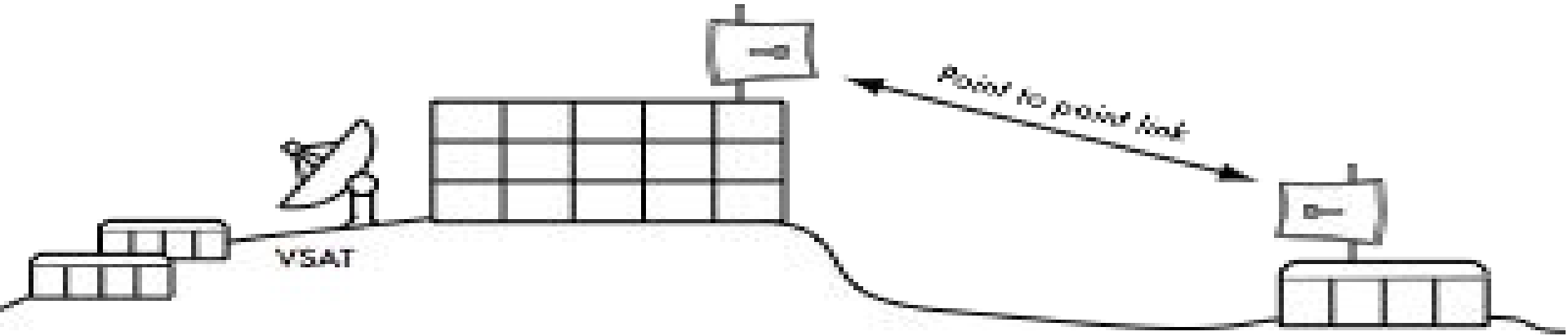
Any complex wireless network can be thought of as a combination of one or more of these types of connections:

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

Point to Point

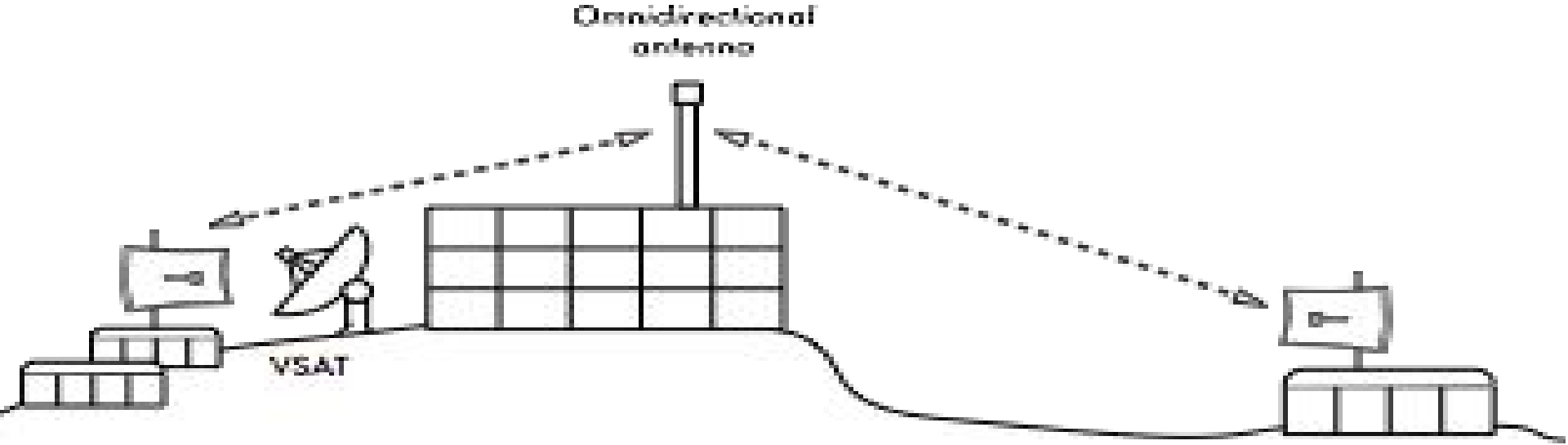
The simplest connection is the ***point-to-point*** link.

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



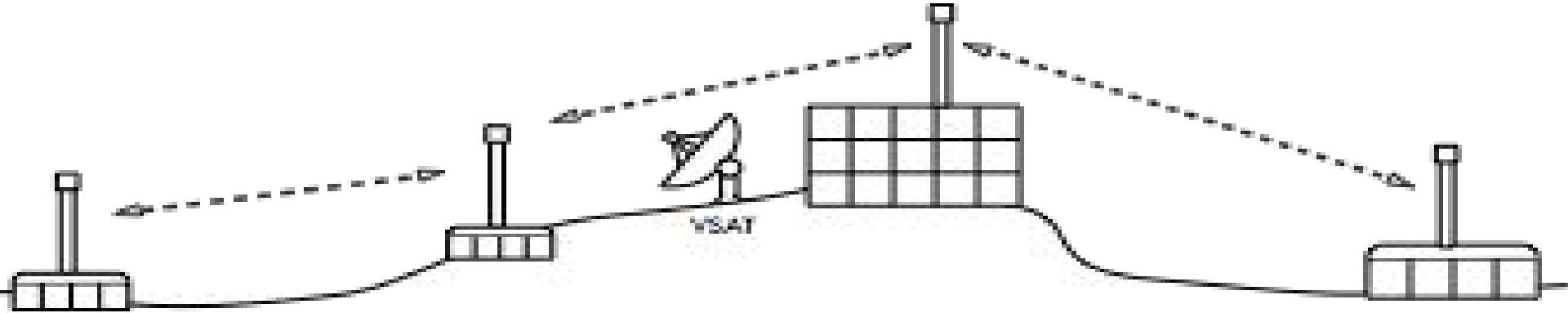
Point to Multipoint

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).

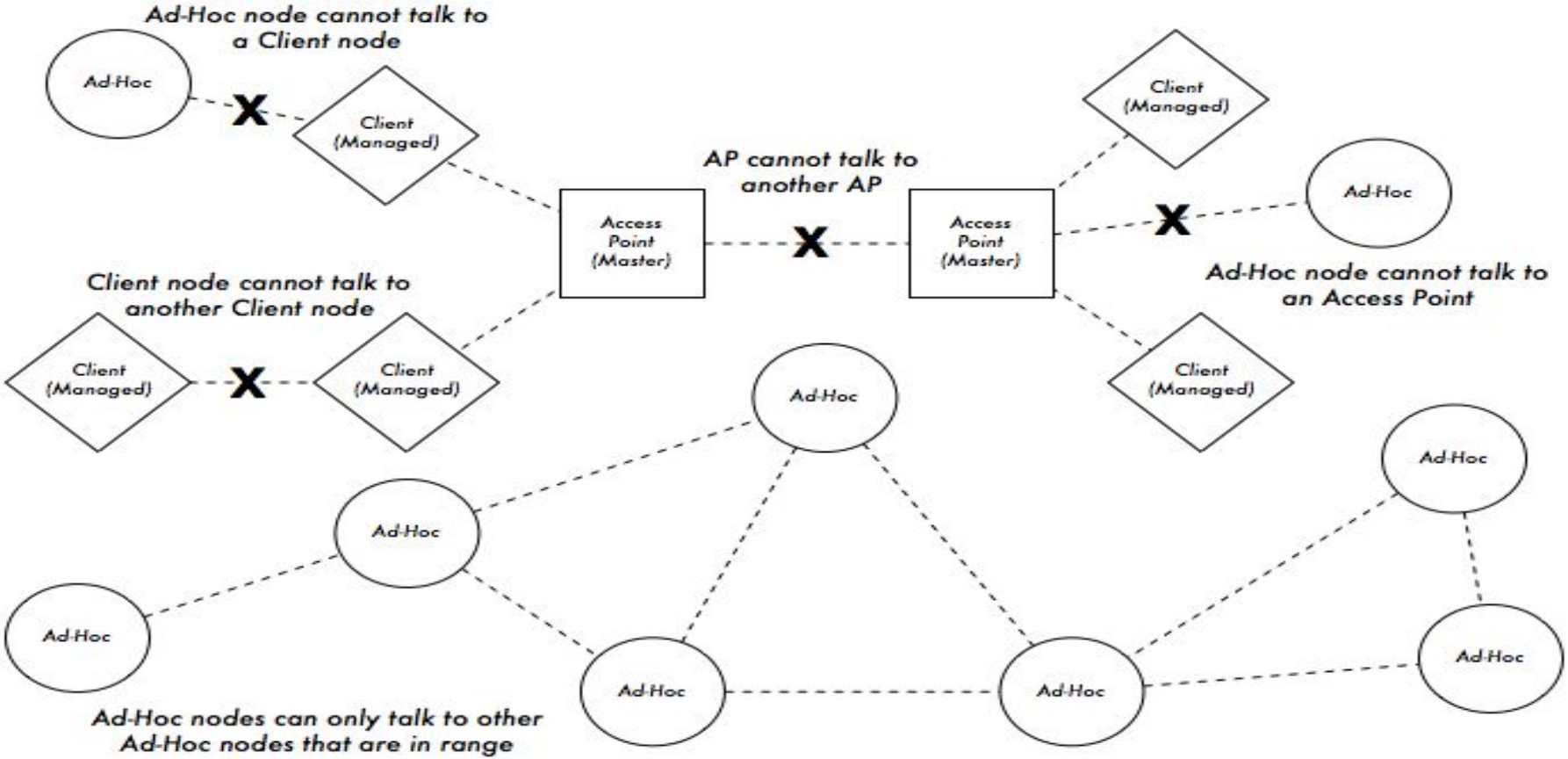


Terminology

- Station: Device that contains IEEE 802.11 conformant MAC and PHY interface to the wireless medium, but does not provide access to a distribution system. Also called **Client**.

- Access Point (AP) :Device that contains IEEE 802.11 conformant MAC and PHY interface to the wireless medium, and provide access to a distribution system for associated stations. Most often infra-structure products that connect to

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

Bridged networking

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

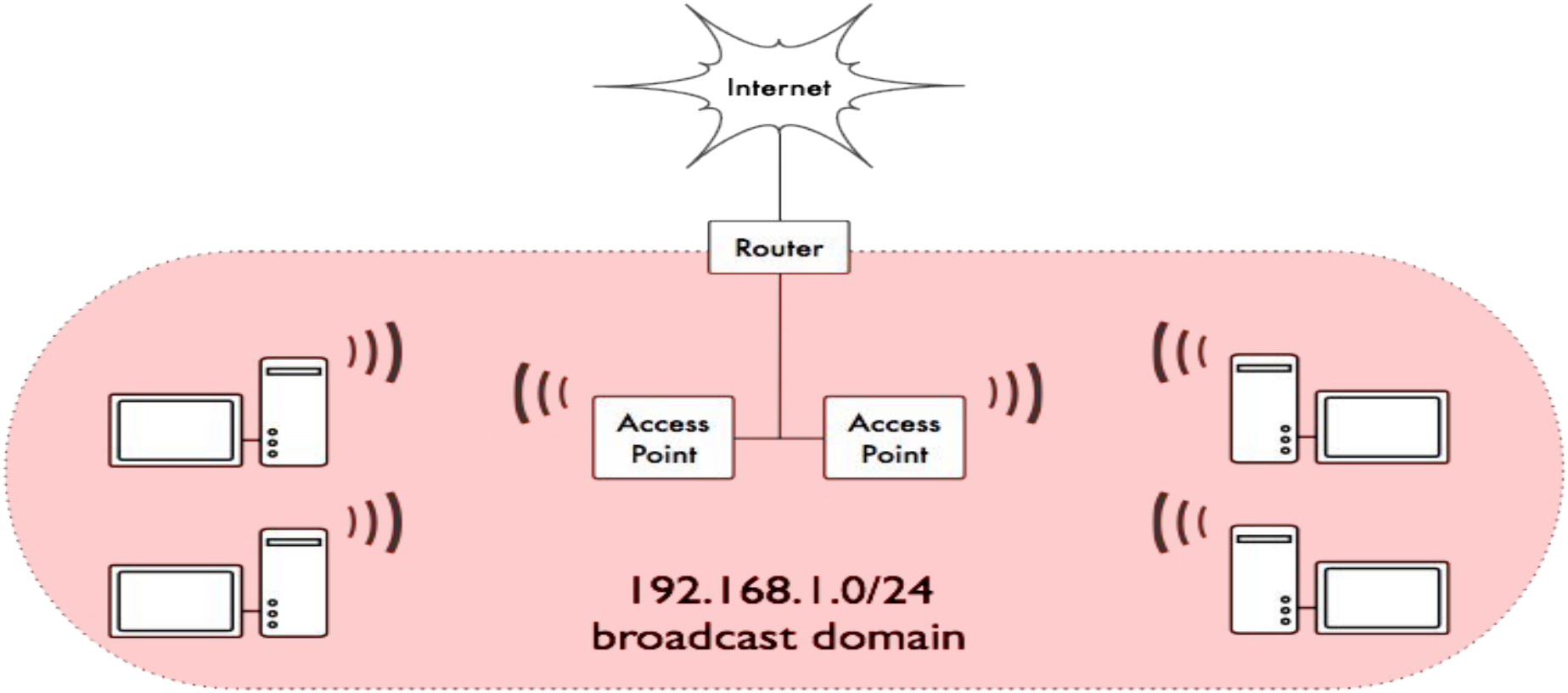
Advantages

- 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.

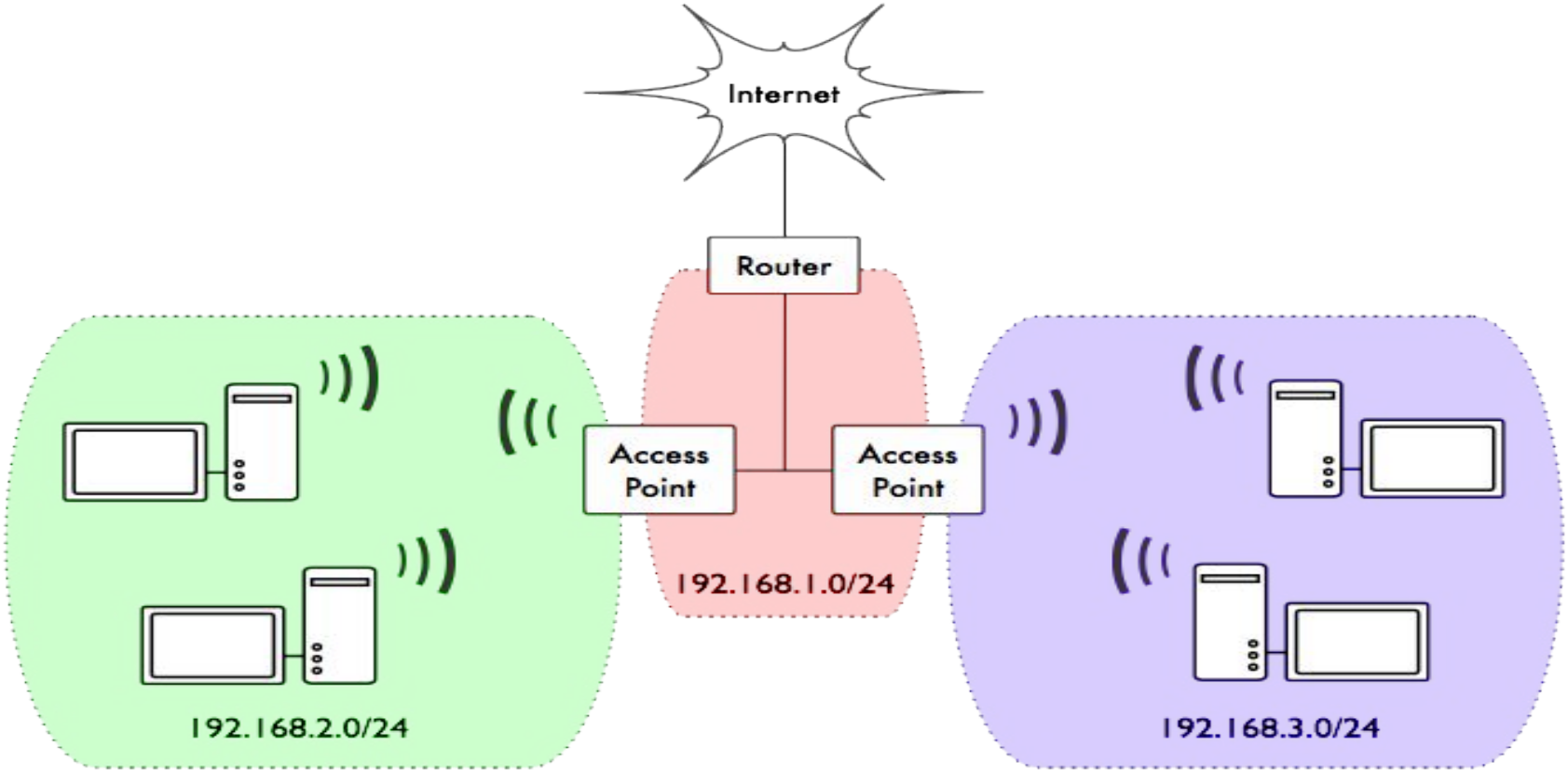
Advantages

- 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

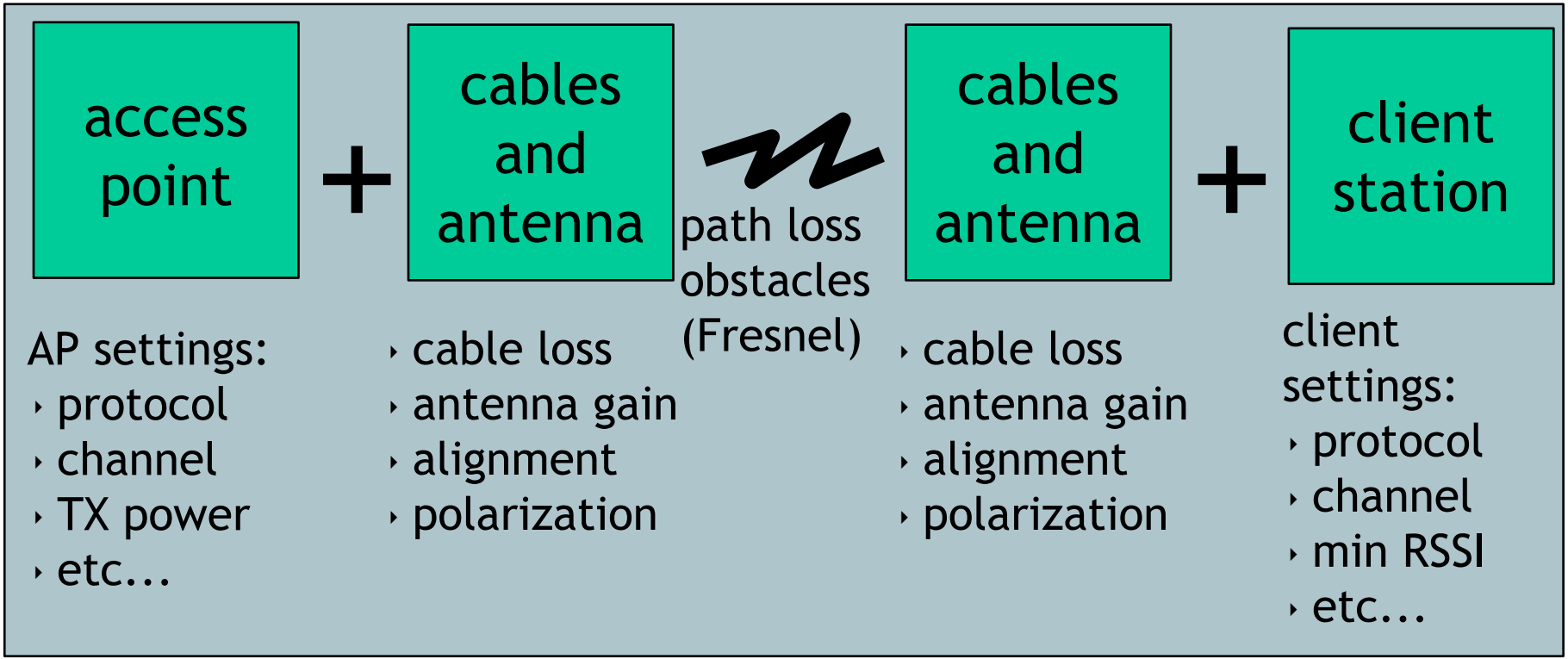
Disadvantages

- More complex configuration
- Roaming between APs is not supported

Routed access points



A link is composed of many parts



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/