Short Introduction to Wireless

Campus Network Design & Operations Workshop

UNIVERSITY OF OREGON

Last updated 03 August 2020

NSRC
Network Startup Resource Center

This talk … a one-hour crash course

- What can we use wireless for
- What equipment to use/buy
- Where to place Access Points
- How to integrate wireless into the campus network
- How to secure the wireless network

- What can we use wireless for
- What equipment to use/buy
- Where to place Access Points
- How to integrate wireless into the campus network
- How to secure the wireless network

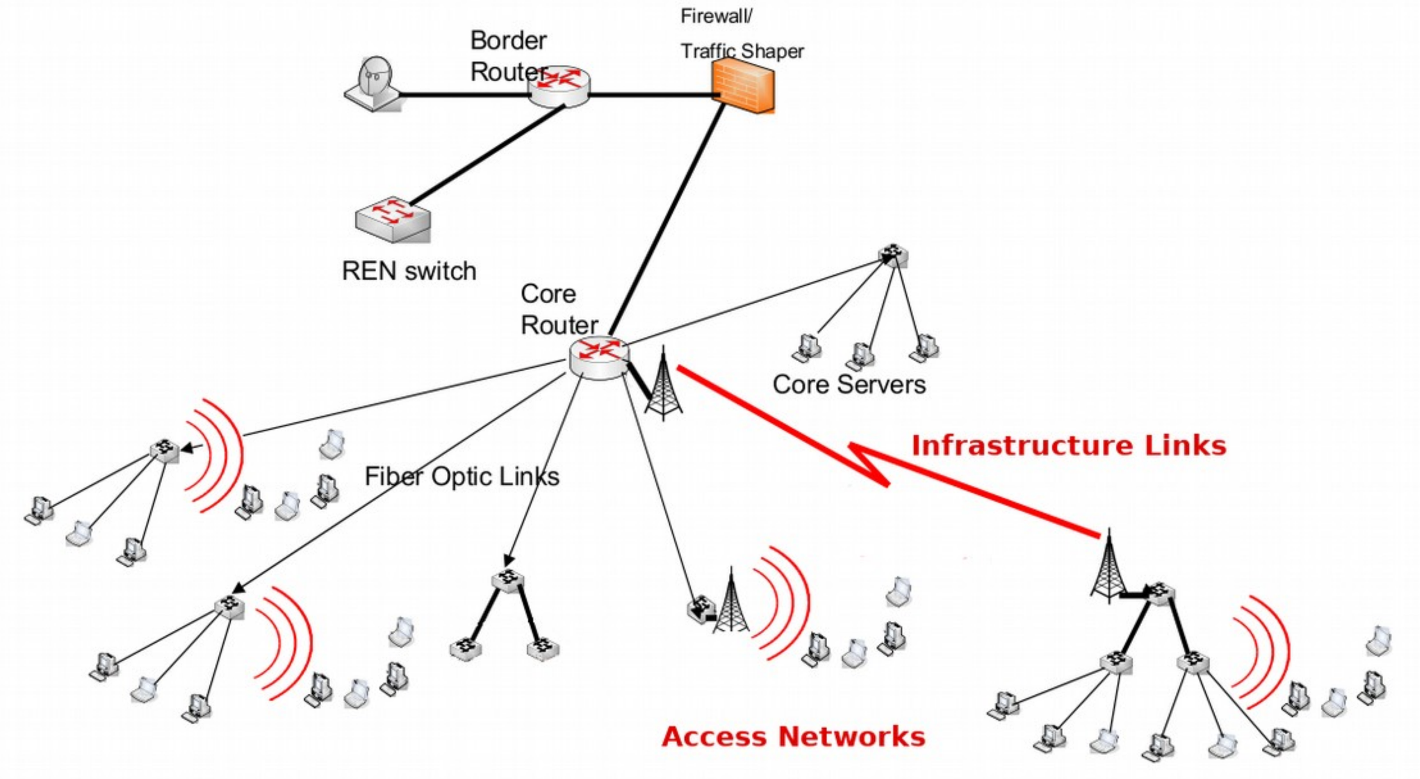
What can we use wireless for

- Wireless links can act as **backbone/infrastructure**, just like fiber
- Distances up to several 10 kms (even 100+ km)
- Speeds up to Gbps

What can we use wireless for

- Wireless links can act as **backbone**, just like fiber
- Wireless can act as **access network for users** and things
  - The most popular and most needed use of wireless
    - Remember the NREN starts with campus network!
  - Important to keep well separated! Users should be on access networks, not on infrastructure links!

What can we use wireless for



- What can we use wireless for
- What equipment to use/buy
- Where to place Access Points
- How to integrate wireless into the campus network
- How to secure the wireless network

What is Wi-Fi?

- When we say wireless access, this almost always means Wi Fi™
- A Wi-Fi Alliance Trademark
  - Not strictly a technical term
- Wi-Fi is commonly used to refer to the 802.11 family of wireless standards
- Wi-Fi can run in ISM (Industrial, Scientific, Medical) bands
- Wi-Fi is designed for shared spectrum

What equipment to use/buy

- The big question that always connects to **money**
- What is locally available and well supported?
- One fundamental decision: wireless LAN with **controller/management** (“enterprise wireless”)

  or with **home user equipment**?
- What is your ambition? What is the size of your network?

Managed vs. Unmanaged Wireless LAN

	Managed	Unmanaged
Size of Network	Good for large networks	Smaller networks (~10 APs or so)
Manual work	Less	A lot
Monitoring	Built-in	Do it yourself
Rogue AP detection	Yes	No
Price	Higher	Lower
Channel management (!)	Automatic, coordinated, intelligent	Largely manual, definitely need manual control

Some vendors

Managed/Enterprise:

Cisco, Extreme/Aerohive, Ruckus, Fortinet, Ubiquiti, Aruba/HP, ...

Home/Small office:

TP-Link, Netgear, Linksys, Engenius, Asus, and many more

The Enterprise class is $1000s, the home class is $100 (and below)

A favorite question

Can I re-use what I have lying round?

Yes, but it will be more work for you.

Multi-vendor networks are harder to maintain.

Consider using old gear in isolated places, maybe a Cafe, a public hotspot, …?

You can do fun things, but careful with what is manageable ...

Channel Management

- So we need to think about frequencies, standards, channels
- What frequencies of Wi-Fi can your phones and laptops work with?
    - ______
    - ______
    - And what is a frequency anyway?

Current 802.11 Standards

Standard	Data rate [Mbps]	Frequency [GHz]	Channel Access
802.11b	11	2.4	DSSS
802.11a	54	5	OFDM
802.11g	54	2.4	DSSS, OFDM
802.11n	150/300/600	2.4 / 5	DSSS, OFDM, MIMO
802.11ac	1300	5	OFDM, Mu-MIMO
802.11ax	11000 (?)	2.4 / 5	OFDM, Mu-MIMO

New Names: Wi-Fi x

802.11W	Year	New name / brand
802.11b	1999/2012	(Wi-Fi 1 unofficial)
802.11g	2003	(Wi-Fi 3 unofficial)
802.11a	1999/2012	(Wi-Fi 2 unofficial)
802.11n	2009	**Wi-Fi 4**
802.11ac	2013	**Wi-Fi 5**
802.11ax	(2020)	**Wi-Fi 6**
802.11ax with 6 GHz	(2020)	**Wi-Fi 6E**

Most equipment you can buy today – client and infrastructure – will support all of these up to 802.11ac. First 802.11ax is available. You might have older clients though? Do you?

A comment on speed and newest standard

- We all like to have the **newest, fastest, best!**
- But consider the throughput and how to transport it! **Where does your traffic go?**
- In a modern Wi-Fi network, each single user can generate several 100 Mbps! Imagine

  1000 users with 100 Mbps each … what is your ISP bandwidth?

Channel Management

- Two main frequency bands for access Wi-Fi
  - **2.4 Ghz band**
  - **5 Ghz band**
  - There are others, e.g. 60 Ghz, **upcoming 6 GHz**, but these two are the relevant ones today. All standard gear offers those.

Channel Management

- Within each frequency bands, there are channels:
  - **2.4 Ghz: 100 MHz total, 13 channels (most of world)**
  - **5 Ghz: 25 channels**
  - But channels overlap!

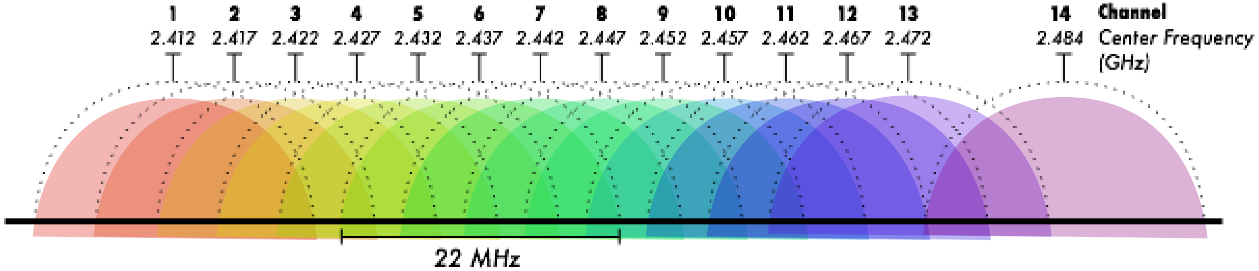
    In 2.4 GHz, there are only

    three (maybe four) non-overlapping channels!

802.11 5GHz Channels

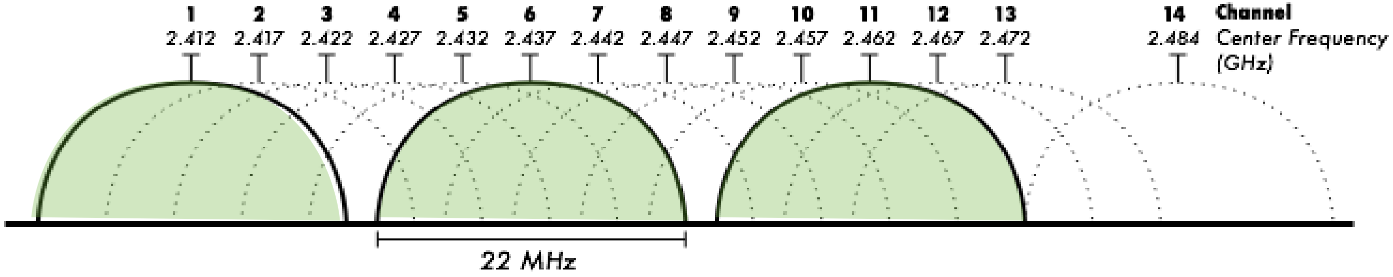
- 5 GHz has 25 non-overlapping channels:
  - U-NII-1: 5170-5250 has 4 of 20 MHz each
    - 36 ,40, 44, 48
  - U-NII-2A: 5250-5330 has 4 of 20 MHz each
    - 52, 56, 60, 64
  - U-NII-2C: 5490-5730 has 12 of 20 MHz each
    - 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144
  - U-NII-3: 5735-5835 has 5 of 20 MHz each
    - 149, 153, 157, 161, 165
- Wider channels allow bigger bandwidths

802.11 2.4 GHz Channels



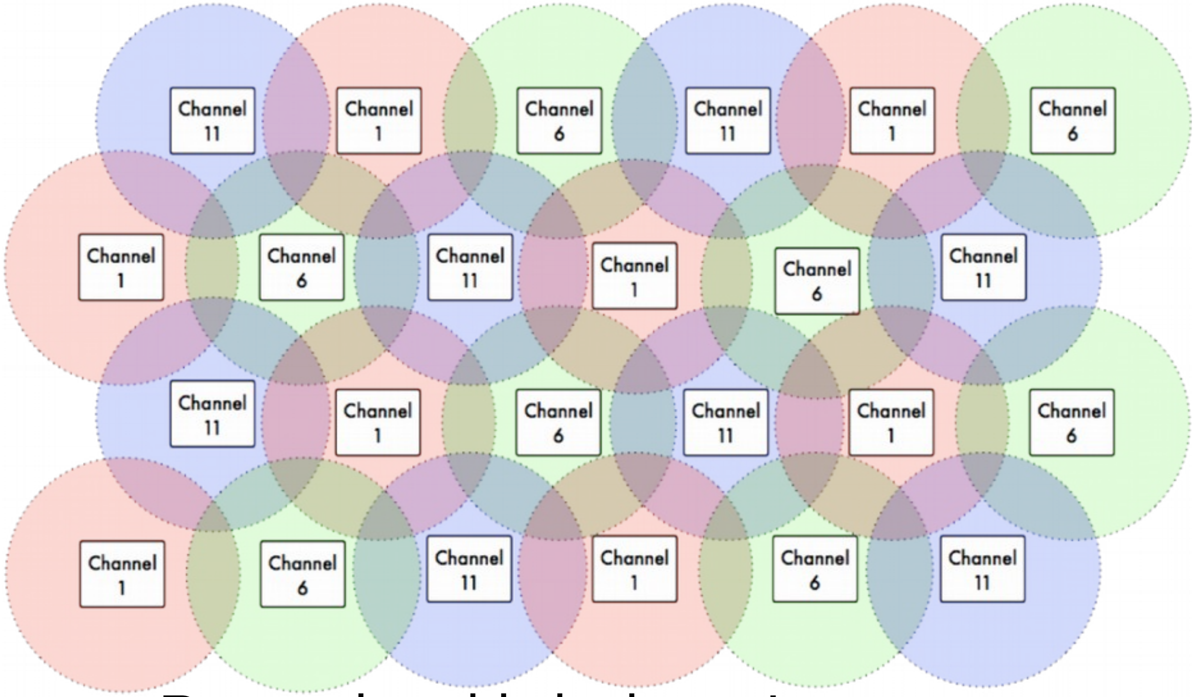
- Frequency bands are divided into channels
- 2.4 GHz has 14 overlapping channels of 22 MHz each
- 5 GHz has 25 non-overlapping channels of 20 MHz each
  - Country dependent
  - https://en.wikipedia.org/wiki/List_of_WLAN_channels
- Wi-Fi devices must use the same channel
- Wi-Fi devices send and receive on the same channel

Non-Overlapping Channels 1, 6, 11 (14)



- Not All Countries Allow All Channels!
- Channel 14 is not allowed in the USA
- What channels are used in your country?

Three Channel Coverage Design

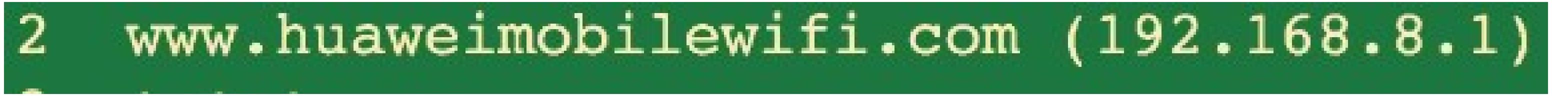


Remember this is theory!

Reality does not look this nice.

In reality ...

- you might have neighbours running Wi-Fi
- you might have guests running Wi-Fi (BYOD!)



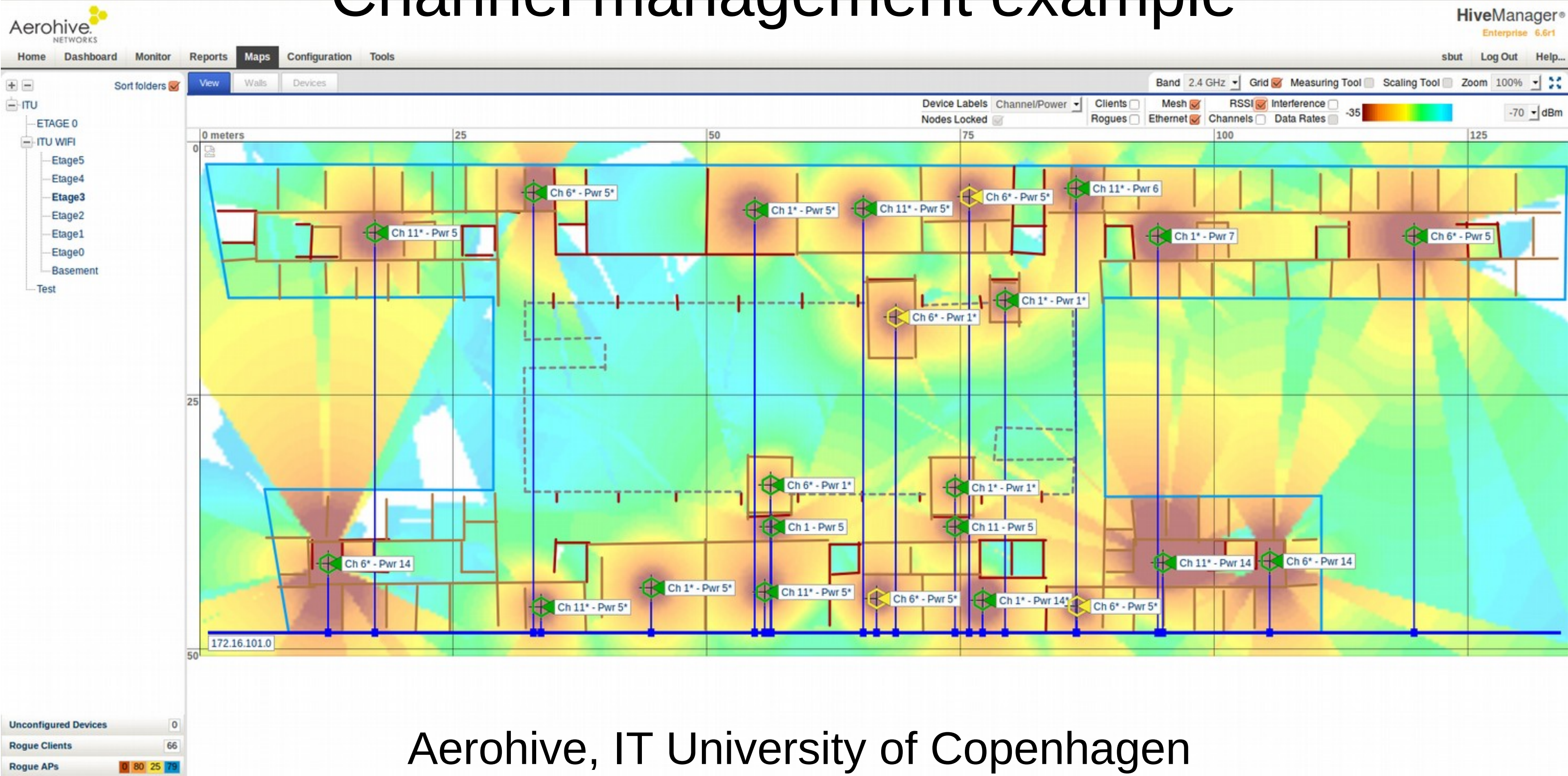
```
2  www.huaweimobilewifi.com (192.168.8.1)
```

(and how do you find out?)

- your buildings and sites are not so neatly arranged

All of this **makes automatic channel management very useful!**

Channel management example

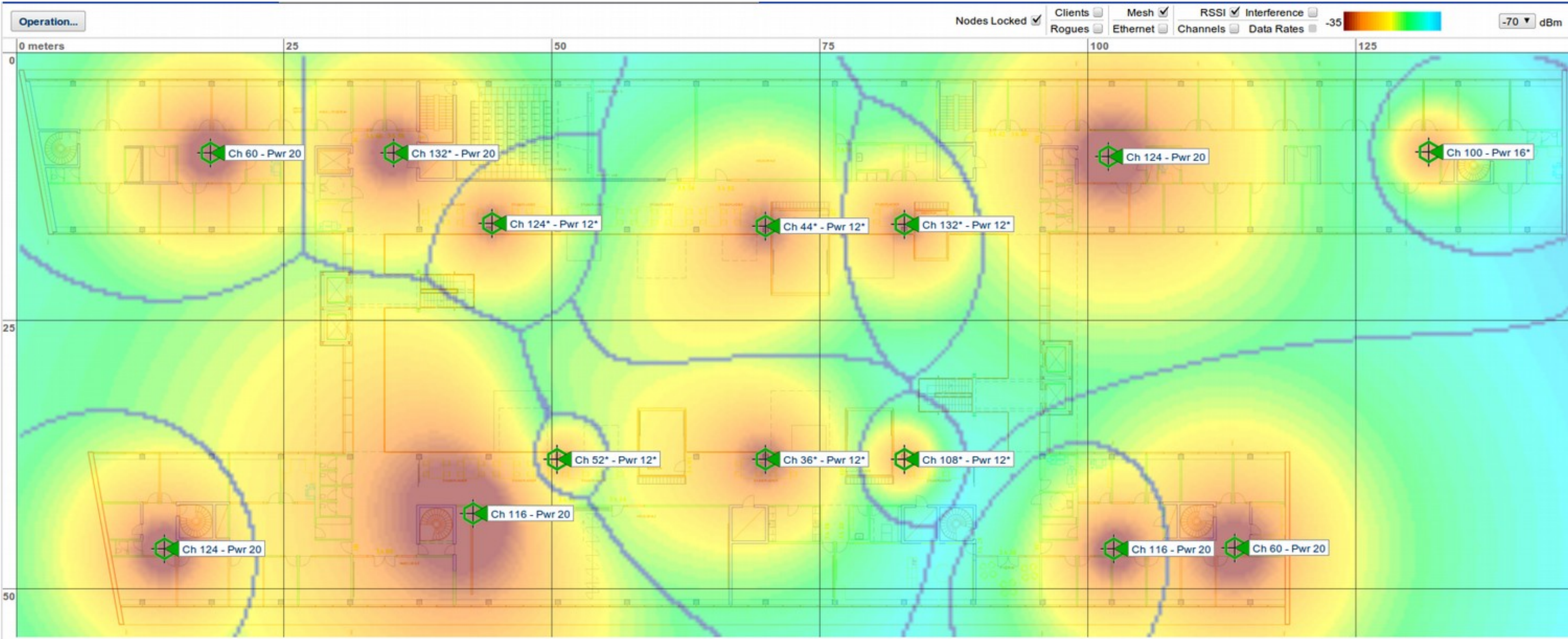


Band 2.4 GHz
Grid ☑
Measuring Tool □
Scaling Tool □
Zoom 100%
Device Labels Channel/Power
Nodes Locked □
Clients □
Rogues □
Mesh ☑
Ethernet ☑
RSSI ☑
Channels □
Interference □
Data Rates □
-35 … -70 dBm

Unconfigured Devices 0
Rogue Clients 66
Rogue APs 0 80 25 79

Aerohive, IT University of Copenhagen

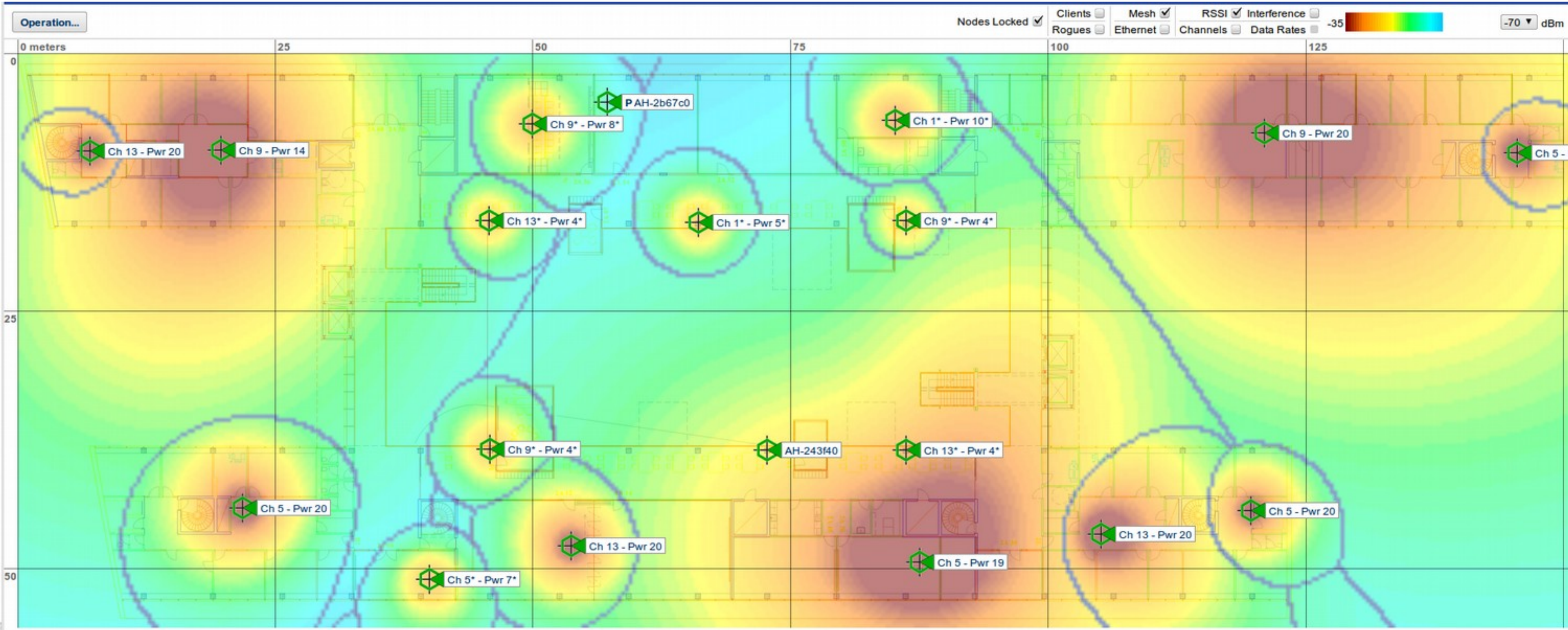
Channel management example



Nodes Locked ☑
Clients □ Rogues □
Mesh ☑ Ethernet □
RSSI ☑ Channels □
Interference □ Data Rates □
-35 … -70 ▼ dBm

Aerohive, IT University of Copenhagen

Channel management example



Operation...

Nodes Locked ☑ Clients □ Rogues □ Mesh ☑ Ethernet □ RSSI ☑ Channels □ Interference □ Data Rates □ -35 -70 ▾ dBm

Aerohive, IT University of Copenhagen

Avoid ...

- **Adjacent channels interference:**

  The worst you can have is Channel 1 and Channel 2 next to each other! Then it is better to be on same channel!

- What can we use wireless for
- What equipment to use/buy
- Where to place Access Points
- How to integrate wireless into the campus network
- How to secure the wireless network

Where to place Access Points

- That is quite simple: **where the target users are!**
  - But of course we need to know –
  - before and while running the network: we need

    site survey and monitoring -

    both are mandatory!

What is a Site Survey?

- A thorough look at all of your campus – the **physical layout**, the buildings, the trees, the cars, - everything!
- A look at the **wireless spectrum** – with standalone tools on laptops and phones (which do you know?), or, even better, with your Wi-Fi management system and your APs
- Don’t forget the **social/human factors**!

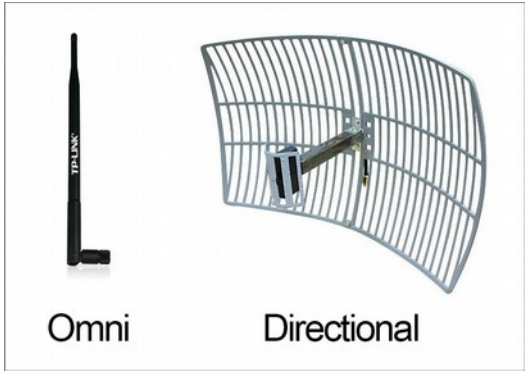
Getting the signal to the user: Antennas!

- Antennas are passive elements, bundling/directing wireless signal
- For user access, you mostly find

  Omni-directional antennas

  or

  Slightly directional antennas (patch, panel)



- For point-to-point links – different story: highly directional antennas!

Antenna pattern diagrams

- Part of a good antenna’s documentation
- Show a**ntenna gain in various directions**

  (azimuth, elevation)

- At this point, we **need to understand the dB (decibel)**

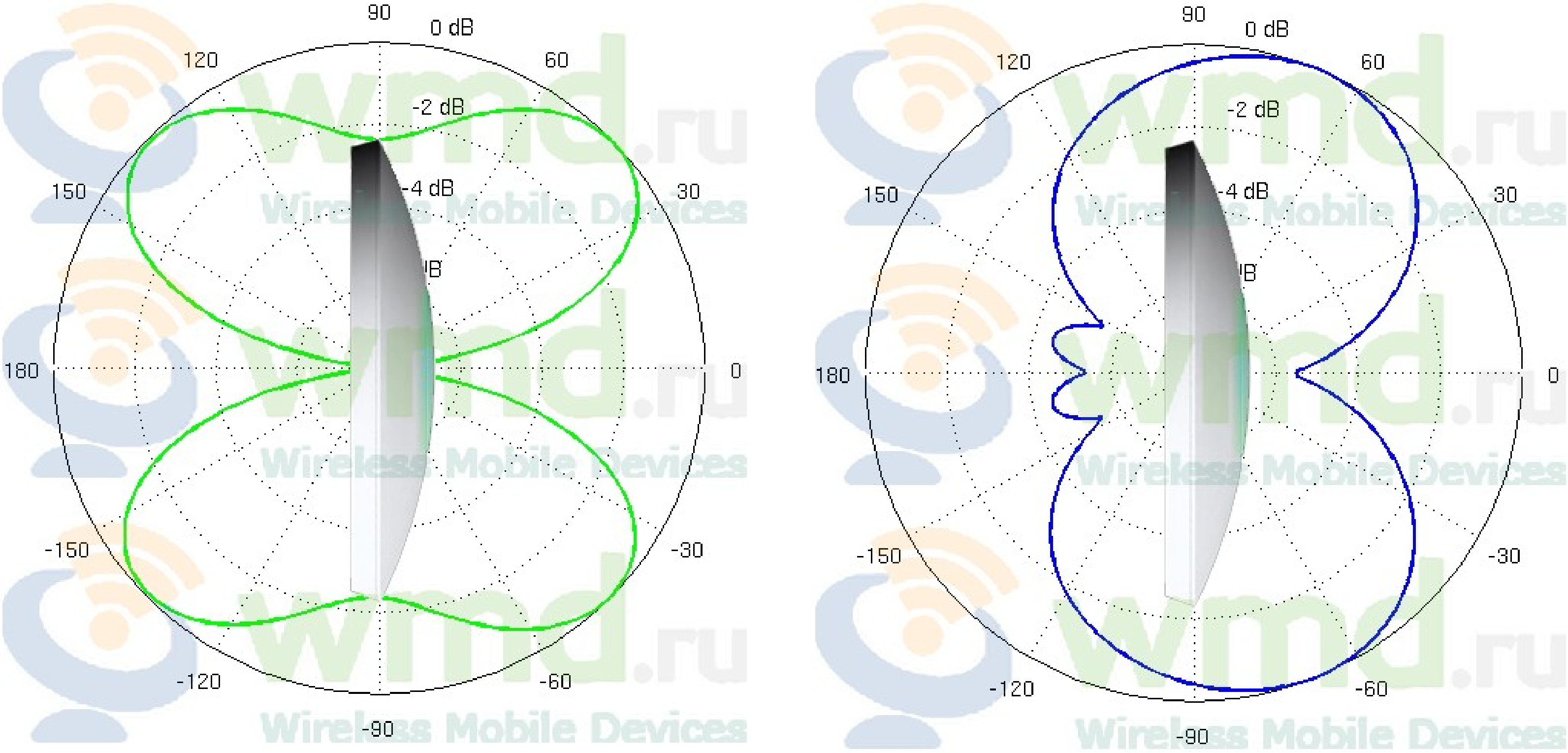
The decibel (dB)

- Definition: $10 * \text{Log}_{10} (P_1 / P_0)$
- 3 dB = 2x power
- 6 dB = 4x power
- 10 dB = 10x power = order of magnitude
- Calculating in dBs
- Relative dBs
  - dBm = relative to 1 mW
  - dBi = relative to ideal isotropic antenna

The dB: Examples

- dBm is decibels relative to 1 milliwatt
  - Transmitters have power in dBm
  - Cables have loss in dBm
  - 1 mW = 0 dBm
  - 100 mW = 20 dBm
  - 1 W = 30 dBm
- dBi is decibels relative to a perfect antenna
  - The “i” stands for isotropic
  - An omni antenna with 6 dBi gain
  - A parabolic dish with 29dBi gain

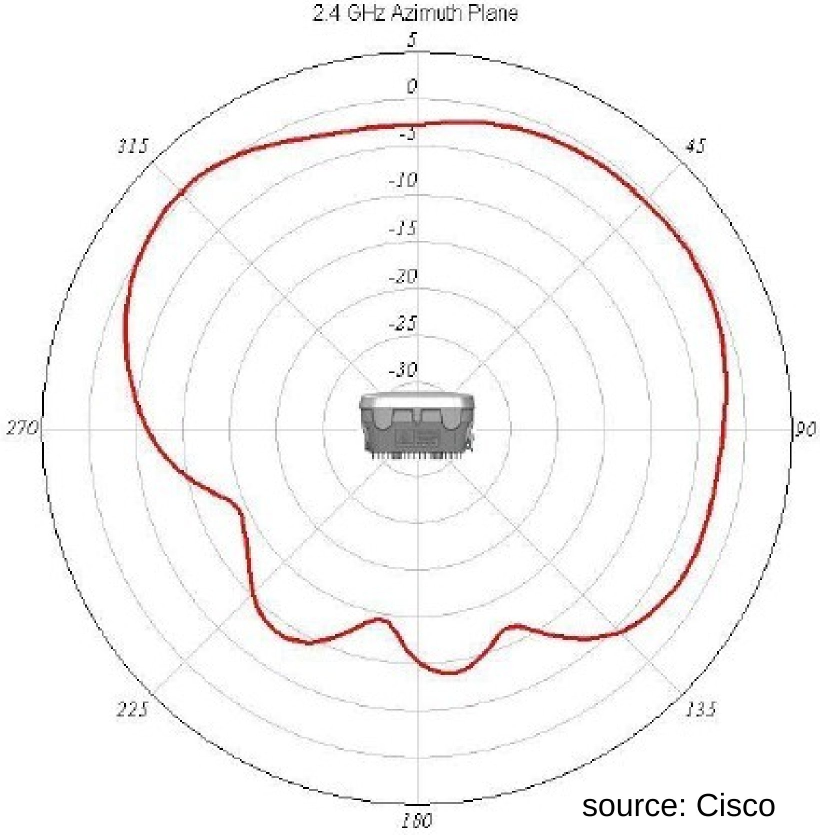
Antenna patterns



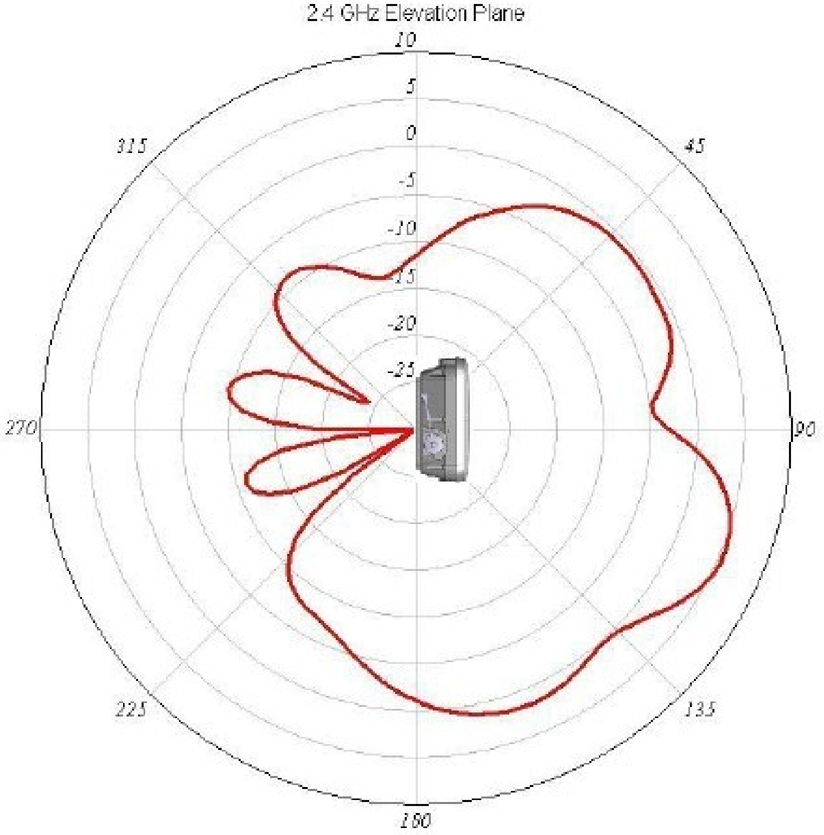
source: Ubiquiti Unifi

1530i 2.4 GHz Patterns (peak gain 3 dBi)

Azimuth

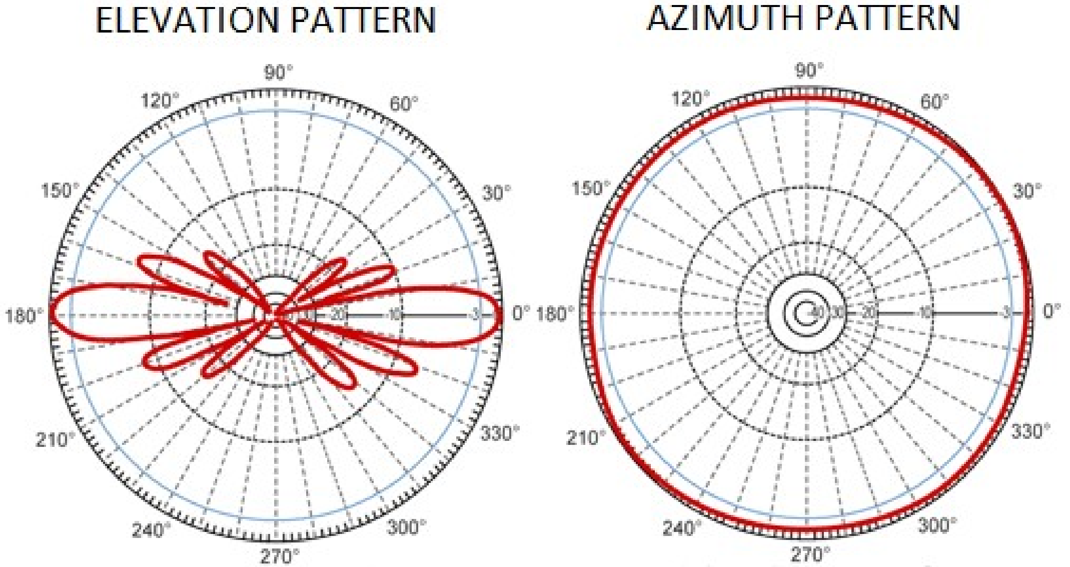


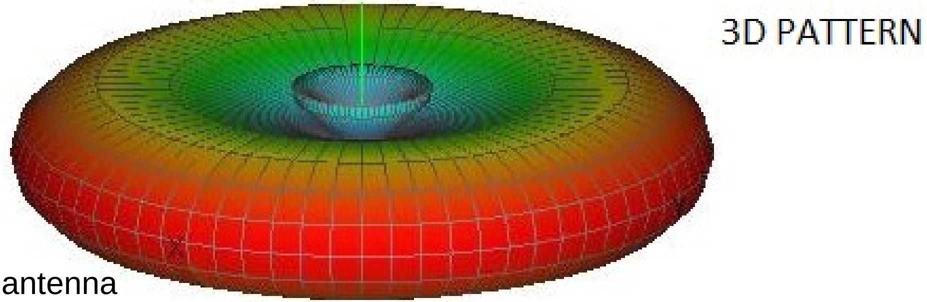
Elevation



source: Cisco

Who can tell what this is?





source: mpantenna

Getting the signal to the user: Antennas!

- When you know the Antenna patterns, make sure you point the signal at the users – not the wall or the ceiling or the sky!
- There will be several options, for example for indoor
  - On ceiling
  - On Wall
  - Under table

What gets in the way: Absorption

- Wireless signal is a wave

  (what is the wavelength, by the way?)

  for 2.4 GHz: _________

  for 5 GHz: _________

- Waves get absorbed, reflected, bent around corners (a little bit)

- Behaviour of the wave scales with wavelength

Radio Waves: Absorption

- Absorption: main causes are metal and water
- Metal in all forms, including for example
  metal grids in reinforced concrete wall, or as a thin layer on a window,
  pipes and cables, building infrastructure, cars …
- Water in all forms, including
  rain, fog, humid walls, humid vegetation … and there s a lot of water in …
  ______(who?)_____________
- Buildings & walls & roofs and so on
  also absorb, but it is hard to tell how much unless you measure

How many users per Access Point?

- Hard to give general rule, but ...
  - 10-20 power users
  - 100 moderate users
  - 200-300 if you really have to …
- Plan! Monitor!

Conclusion on AP placement

Where is the AP you are currently using?

What antenna do you think it has?

How has it been placed?

This talk … a one-hour crash course

- What can we use wireless for
- What equipment to use/buy
- Where to place Access Points
- How to integrate wireless into the campus network
- How to secure the wireless network

Wireless Integration in Campus Network

- Physical Installation
- Layer 2: SSID (network name) planning
- Layer 3: IP planning

<==> Authentication and Security

Wireless at Layer 2: SSIDs

- Wireless Modes
  - Master – used for Access Points
  - Managed – for Stations (Clients)
  - Ad-hoc – for Nodes in a Mesh Network
- SSID (Service Set Identifier)
  - The “Network Name”
  - Often Human Readable

Wireless at Layer 2: SSIDs

- SSIDs can provide **user information**:
  - MyUniv-Library
  - MyUniv-Dorm 1
  - MyUniv-AdminWing
- Tempting SSIDs are a bad idea (though obscurity is not security!)
  - Campus-Security
  - Finance-Department
- SSID choice has impact on:
  - Roaming
  - Network design

Roaming Considerations

- What happens when wireless clients move:
  - From one AP to another, in the same building?
  - From one building to another?
  - To a different part of campus, or a remote campus?
- Is it important to stay on the network, without interruption (for example, to have a Voice over IP chat or video chat)?
- Is it acceptable to log on again, when entering a new network zone?

Wireless Roaming

- Ability to move around and stay on the network
- Two kinds of roaming:
    - Nomadic: interrupted, yet able to pick up again
    - Seamless: uninterrupted, always on
- Users prefer Seamless Roaming
    - Avoids interruption
    - Avoids re-authentication
    - Keeps state and session

Roaming and SSIDs

- A key question:
  one SSID (for example MyUniversity) or many?
- From today’s experience,
  choose one (or few) SSID for all access
- Consider separate SSID for staff, student, guest –
  but it is not really needed, if you have personalized authentication

One SSID you should have

and it could even be your only SSID:

eduroam is the **global roaming SSID** for all educational institutions

Wireless at Layer 3

- Wi-Fi Routers can do many things
  - Routing, NAT, Firewall, DHCP, ...
  - These are Layer 3 functions!
- Keep Layer 3 functions in the wired core
  - You cannot scale a network with Wi-Fi Routers
- An Access Point simply bridges networks
  - This is a layer 2 function: 802.3 <-> 802.11
  - **Scalable networks use Access Points, not Wi-Fi Routers**
  - **We do not want NAT in our wireless network!**

Separate subnets for wireless?

- Wireless clients are fundamentally different from wired ones
  - Not bound to a location – they could be miles away!
  - So, if you build subnets by location, then wireless should have its own
- However, if you look from an organisational angle:
  - The user is the same user, whether wired or wireless
  - *Finance* is still *finance*, *sysadmin* is still *sysadmin*
- This connects to the question of authentication and security.

Wireless is less secure

- … and therefore we should keep it separate …

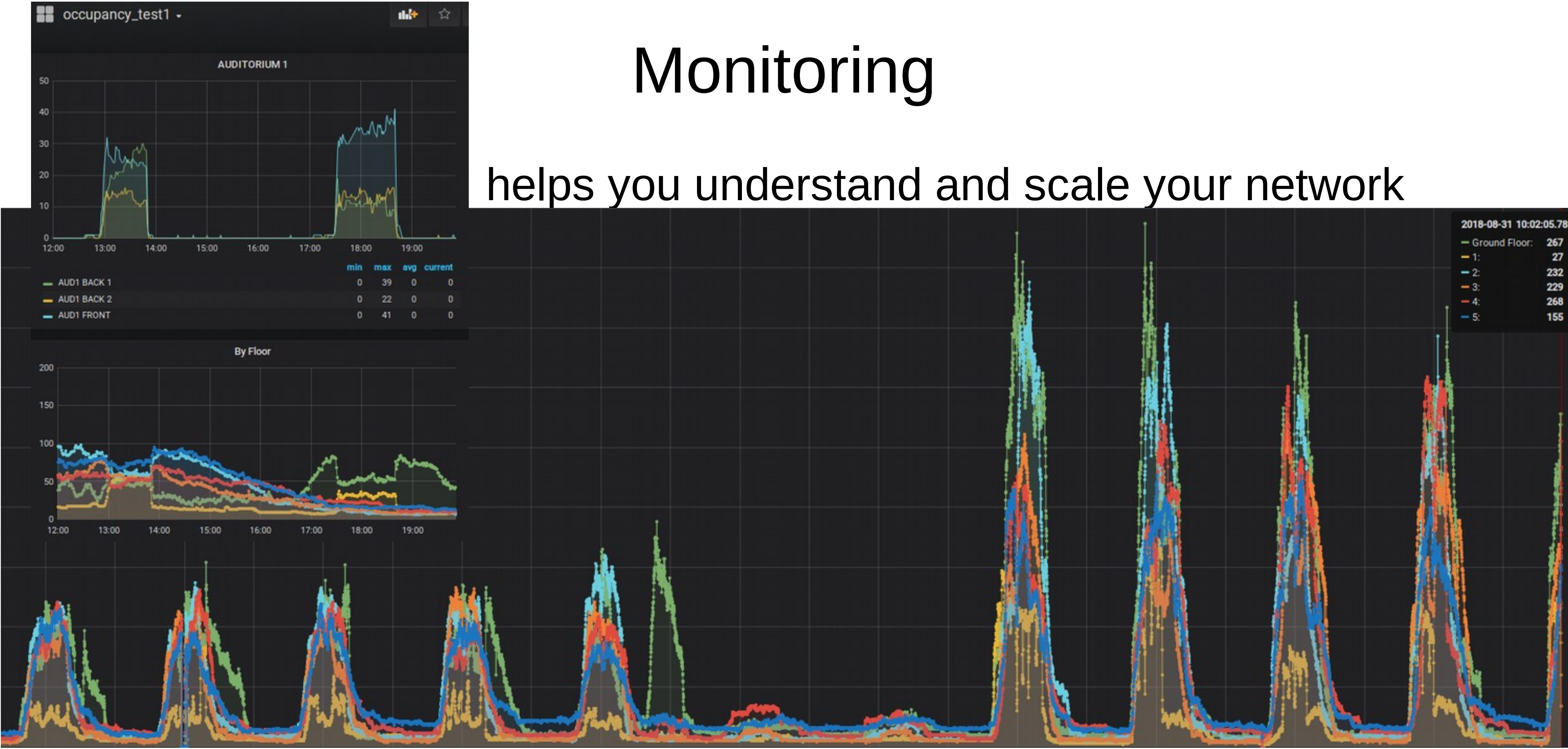
  No. That is a myth!

- **If wireless authentication and security is done right, your wireless clients are probably more secure than your wired ones**

  Do I need to sign in, to plug into an ethernet drop?

Monitoring

helps you understand and scale your network



	min	max	avg	current
AUD1 BACK 1	0	39	0	0
AUD1 BACK 2	0	22	0	0
AUD1 FRONT	0	41	0	0

2018-08-31 10:02:05.78

Ground Floor:	267
1:	27
2:	232
3:	229
4:	268
5:	155

UNIVERSITY OF OREGON

here: Grafana, InfluxDB from Wi-Fi API data

NSRC
Network Startup Resource Center

This talk … a one-hour crash course

- What can we use wireless for
- What equipment to use/buy
- Where to place Access Points
- How to integrate wireless into the campus network
- How to secure the wireless network

Wireless Network Authentication

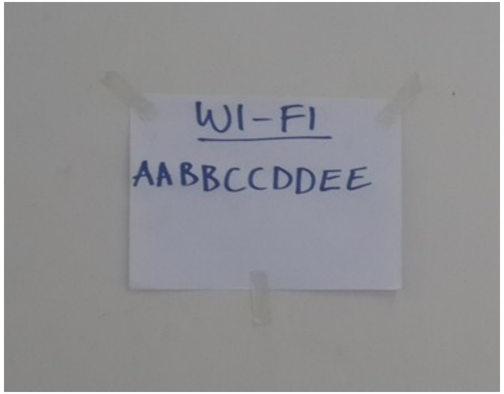
- Authentication can happen in many ways:
  - MAC Address Restrictions
    - Insecure and impossible to manage and scale
  - Pre-Shared Key based Authentication (“Wi-Fi Password”)
    - WPA-PSK – insecure, not scalable
  - Captive Portal Authentication
    - Better than a pre-shared key, but not the ideal
  - **802.1x based Authentication = Ideal!**
    - **Performed on centralized servers in the core**

MAC Address Restriction

- MAC addresses identify machines, not people
- MAC addresses are easily spoofed
- Adds a lot of work for the helpdesk
  - Move/add/change for end user devices
- MAC restriction ok for infrastructure links & IoT
- Not suitable for user access control

Pre-Shared Keys

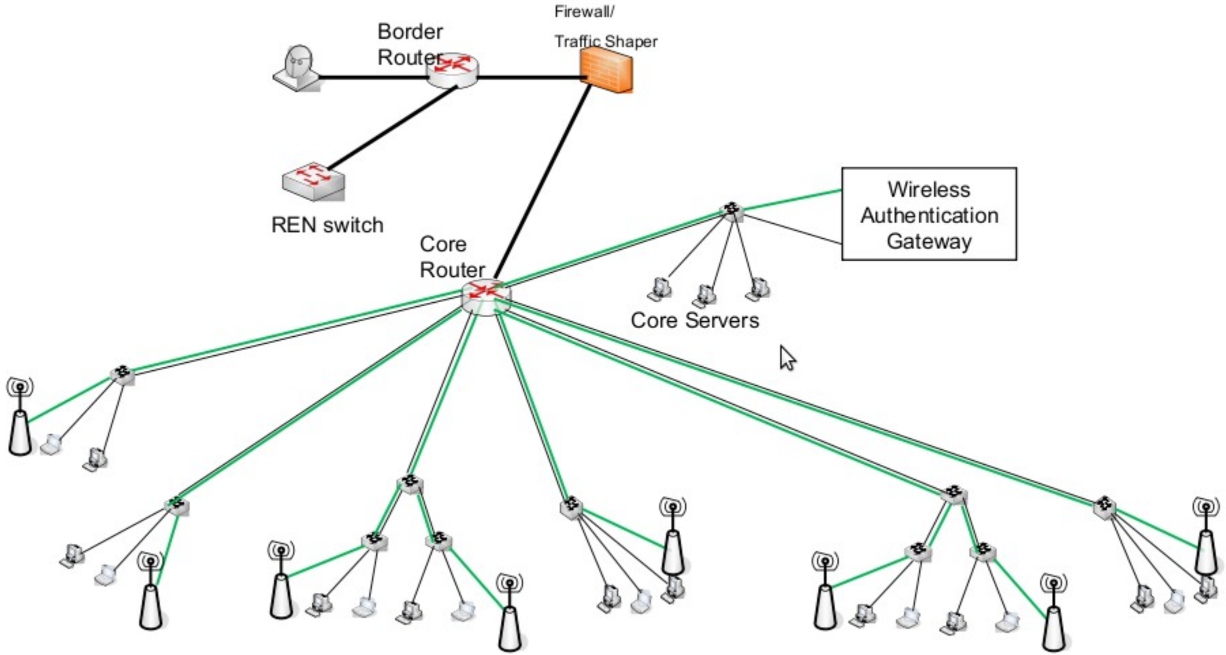
- Useful for some tasks
  - Non-critical Sensor devices with no Internet Access
  - Temporary Workshops
- Not recommended for General Use
  - Unless coupled with Portal-based authentication
- Keys will be shared!



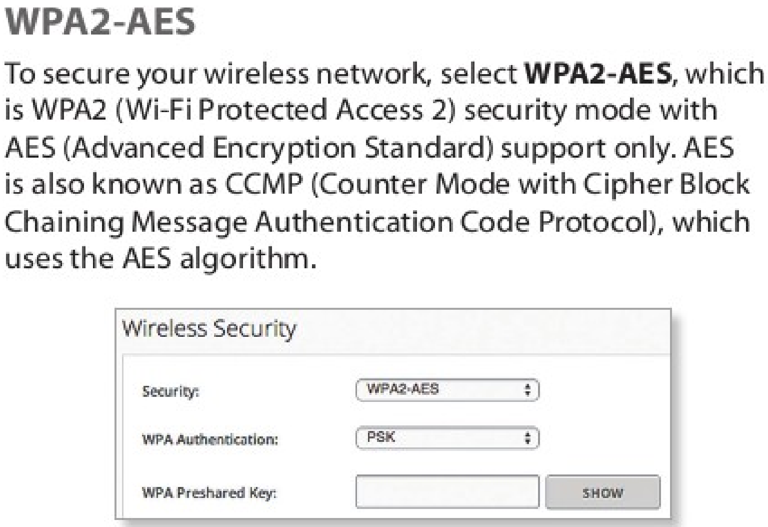
802.1x/WPA2 Enterprise Authentication

- 802.1x/WPA2 is the **only recommended scalable authentication** approach
- However, it **requires a complete, reliable and updated user database**, often in the form of AD (Active Directory), LDAP, but can also be a text file or a SQL database
- Remote Authentication Dial-In User Service (**RADIUS**) takes the role of talking to the wireless system

Authentication on wireless networks



802.1x/WPA2 Enterprise Authentication



WPA2-AES

To secure your wireless network, select **WPA2-AES**, which is WPA2 (Wi-Fi Protected Access 2) security mode with AES (Advanced Encryption Standard) support only. AES is also known as CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), which uses the AES algorithm.

Wireless Security

Security: WPA2-AES

WPA Authentication: PSK

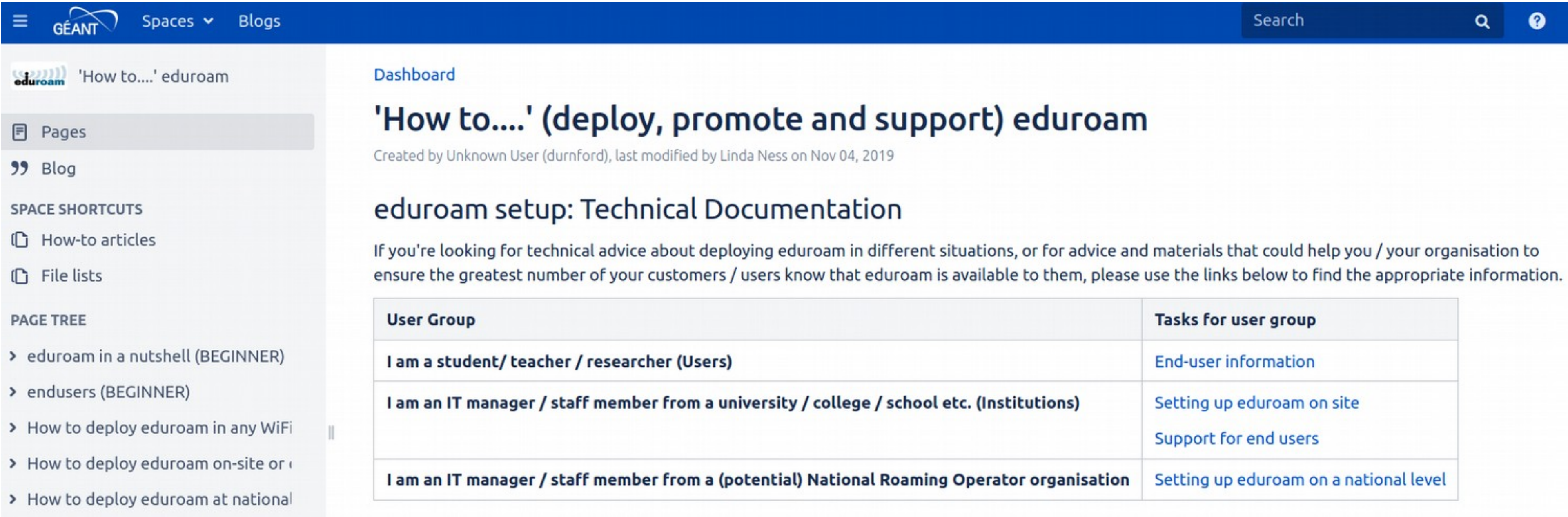
WPA Preshared Key:

- WPA2-AES is the only recommended security mode.

eduroam implements federated 802.1x authentication

- Great learning resource, user guides, also for general 802.1x

eduroam provides guidelines and doumentation



GÉANT
Spaces
Blogs
Search
'How to....' eduroam
Pages
Blog
SPACE SHORTCUTS
How-to articles
File lists
PAGE TREE
eduroam in a nutshell (BEGINNER)
endusers (BEGINNER)
How to deploy eduroam in any WiFi
How to deploy eduroam on-site or
How to deploy eduroam at national
Dashboard

'How to....' (deploy, promote and support) eduroam

Created by Unknown User (durnford), last modified by Linda Ness on Nov 04, 2019

eduroam setup: Technical Documentation

If you're looking for technical advice about deploying eduroam in different situations, or for advice and materials that could help you / your organisation to ensure the greatest number of your customers / users know that eduroam is available to them, please use the links below to find the appropriate information.

User Group	Tasks for user group
I am a student/ teacher / researcher (Users)	End-user information
I am an IT manager / staff member from a university / college / school etc. (Institutions)	Setting up eduroam on site Support for end users
I am an IT manager / staff member from a (potential) National Roaming Operator organisation	Setting up eduroam on a national level

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Our one-hour crash course covered

- What can we use wireless for
  - Infrastructure links & access networks
- What equipment to use/buy
  - Advantages of managed (“enterprise”) networks, channel management
- Where to place Access Points
  - Where the Users are … understanding antennas, signals, obstructions, ...
- How to integrate wireless into the campus network
  - Layer 2 (SSIDs), Layer 3 (IP planning)
- How to secure the wireless network
  - Best with 802.1x authentication in the core … and eduroam

Some things we should talk more about

- Radio physics underneath
- Point to Point, long distance links, link budgets, antennas
- Authentication and Security in-depth
- Tools to use

… but that is another one week workshop :)

Questions?