Configuration of Access Points and Clients

Training materials for wireless trainers

This talk covers the procedure of configuring APs and clients.
It is intended to follow the lecture "Introduction to WiFi" (it's a pre-requisite!) and it has a duration of 60 minutes approx.
Version 1.2 by Rob, @2009-11-20
Version 1.4 by Ermanno, @2009-11-27
Version 1.5 by Rob, @2010-02-28
Version 1.6 by Rob, @2010-03-01
Version 1.7 by Rob, @2010-03-01 (additional minor notes)
Version 1.8 by Rob, @2010-03-12

Goals

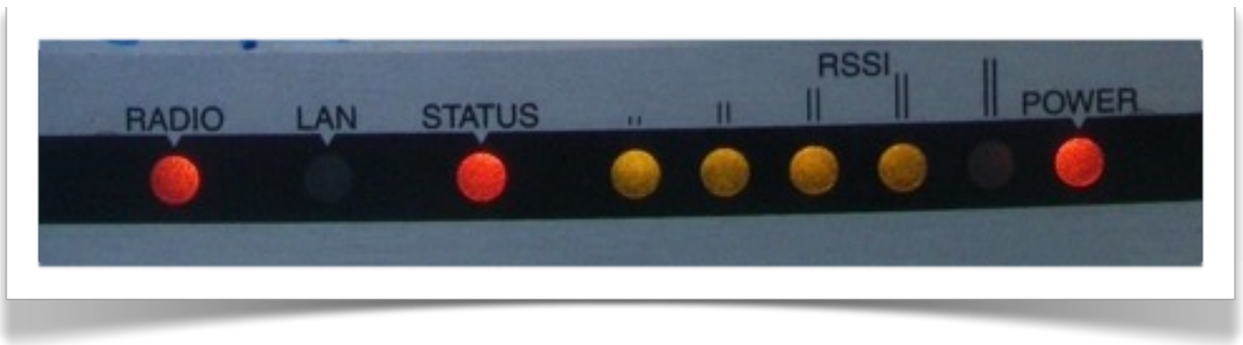
- To provide a simple procedure for the basic configuration of WiFi Access Points (and clients)
- To review the main settings that are available on common Access Points, and analyze their effects on the behavior of the network
- To suggest some practical tips and tricks and troubleshooting advice

Before you change anything!

- Download or otherwise obtain all **user's manuals** and **specification sheets** available for the devices you are going to deploy.
- If you have second-hand devices, be sure to receive full information on their current –or last-known– configuration (e.g. password, IP addresses, etc.)
- You should already have a plan on hand for the network you are going to deploy (including **link budget**, **network topology**, **channels** and **IP settings**).
- Be ready to take written notes of all settings that you are going to apply (especially **passwords**!)
- Make backups of **last known good** configuration files.

Get in touch with the device

Learn the meaning of all LEDs on the device.



They typically indicate:

- Presence of power (green color)
- Active ports / traffic (yellow/green color)
- Error status (red color)
- Received signal strength (LED bars, sometimes multicolor; some devices can even be set to light each LED at specific thresholds, e.g. *Ubiquiti*)

Sometimes, different meanings are associated to the same LED, using different colors and dynamics (e.g. LED is on/off/blinking at different speeds).

Get in touch with the device

Identify the different ports and interfaces:

- Radio interfaces, sometimes called WLANs: one or more antenna connectors (or non-detachable antennas)
- One or more Ethernet interfaces:
  - One or more ports for local network (LAN)
  - One port for uplink (also called WAN)
- Power input (5, 6, 7.5, 12V or other, usually DC):
  Be sure that the power supply matches the voltage!

NOTE: sometimes the power is provided to the device through the same UTP cable that carries the Ethernet data: this is called Power-over-Ethernet (PoE).

WLAN is short for Wireless LAN. LAN (Local Area Network) ports are typically bridged together, while the WAN (Wide Area Network) port usually provides firewalling and NAT functionality. Both type use an RJ45 type connector.

PoE will be explained in detail in the lecture, "Outdoor Installation Part 1".

Get in touch with the device

- Power button (not always present).
- Reset button (often "hidden" in a small hole, can be pressed using a straightened paperclip).

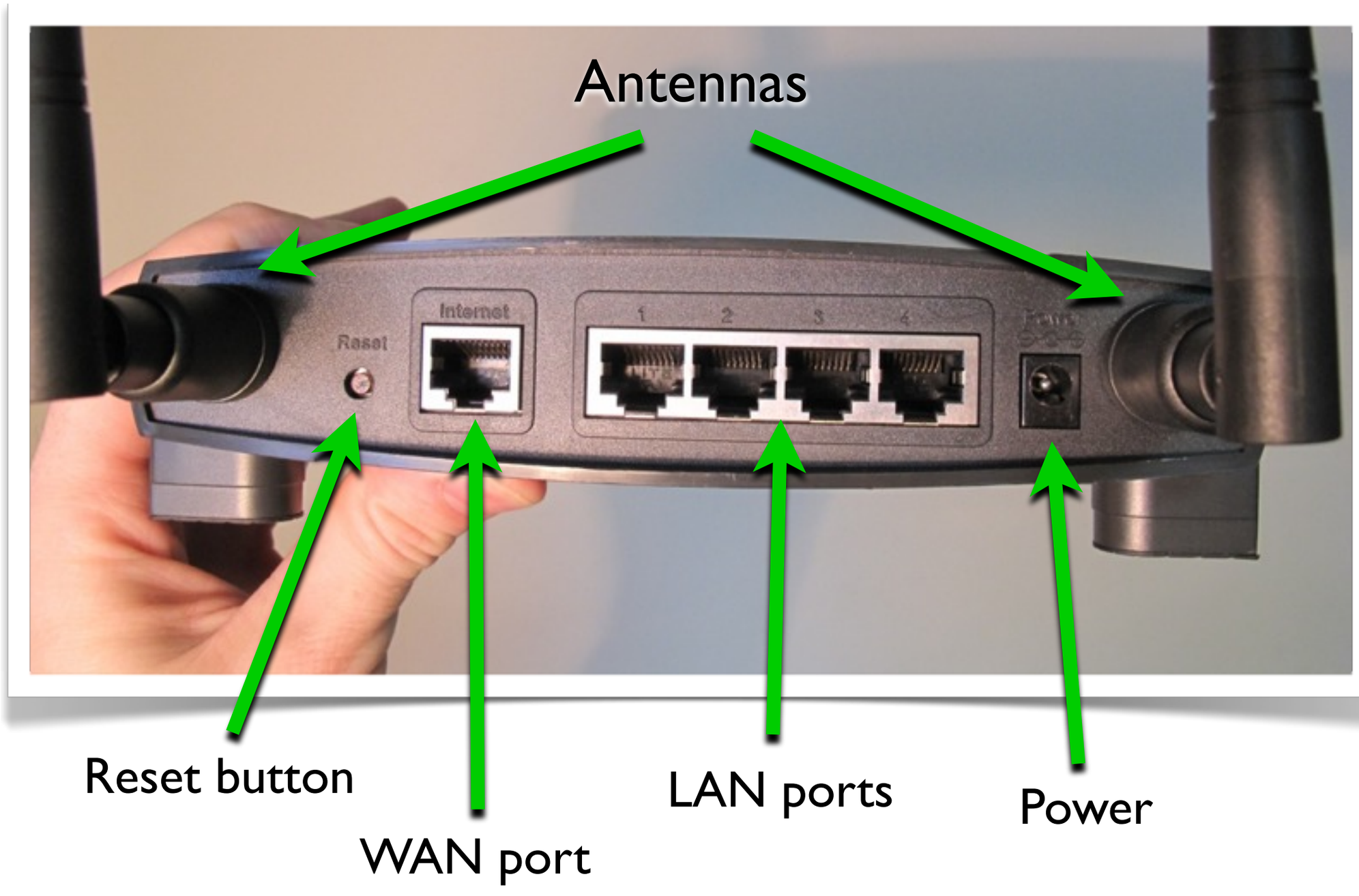
  The reset button may have different effects (from a simple restart to a factory full reset) if pressed briefly vs. for a longer time. It can take 30 seconds or more to trigger a full reset.

NOTE: to fully reset (i.e. reset to factory settings) a device that is in an *unknown* state may be a painful task! Be sure to keep written notes of critical parameters like the device IP address and network mask, and the administrator username and password.

If the critical information (IP address/netmask and admin user/password) are lost and the device is not responding, you may –as last resource– try to look for a factory reset button hidden inside the case, or some proprietary software provided by the manufacturer that can connect to the device with its MAC address, even if IP configuration is lost.

Get in touch with the device

Identify the different ports and interfaces.



WLAN is short for Wireless LAN. LAN (Local Area Network) ports are typically bridged together, while the WAN (Wide Area Network) port usually provides firewalling and NAT functionality.

Sometimes the same type of device has been produced with different power supply requirements. Make sure you have the right kind for your device.

User interfaces

Many options are possible for the user interface (i.e. the way to interact with the device and issue commands and change settings):

- Graphical User Interface (web page)
- Graphical User Interface (proprietary software application)
- Command Line Interface (telnet, ssh)
- Software interface embedded in the system (when the AP/client is a computer or smartphone with a display and its own OS)

GUI: graphical User Interface
CLI: Command Line Interface

GUI typically have several tabs. You must navigate through them to apply the required configuration.
It is preferable to connect your computer to the device by means of an Ethernet cable instead of the wireless interface for the purpose of configuration.

User interfaces: GUI (web page)

- Linksys, Ubiquiti, most modern APs

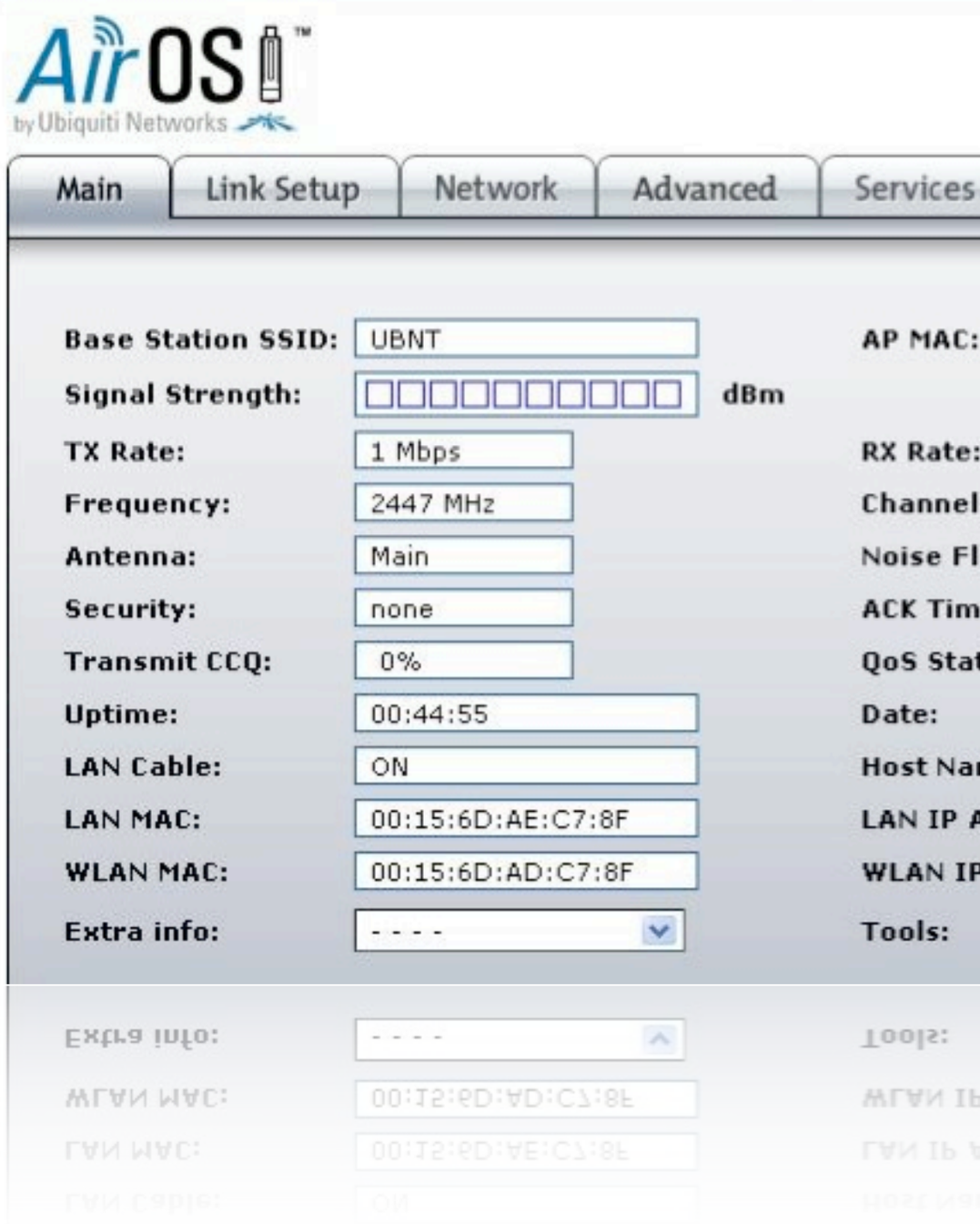
Advantages:

- Works with most browsers and operating systems

Disadvantages:

- Static interface does not reflect changes immediately
- Poor feedback
- Can be incompatible with some web browsers
- Requires a working TCP/IP configuration

- Some recent implementations (e.g. Ubiquiti) are very good and use modern dynamic web features to provide feedback and advanced tools.



Often it is required to click on **Apply**, **Change** or similar and then **Save** for changes to take effect.

User interfaces: GUI (software)

- Mikrotik *Winbox*, Apple *Airport Utility*, Motorola *Canopy*, many old APs

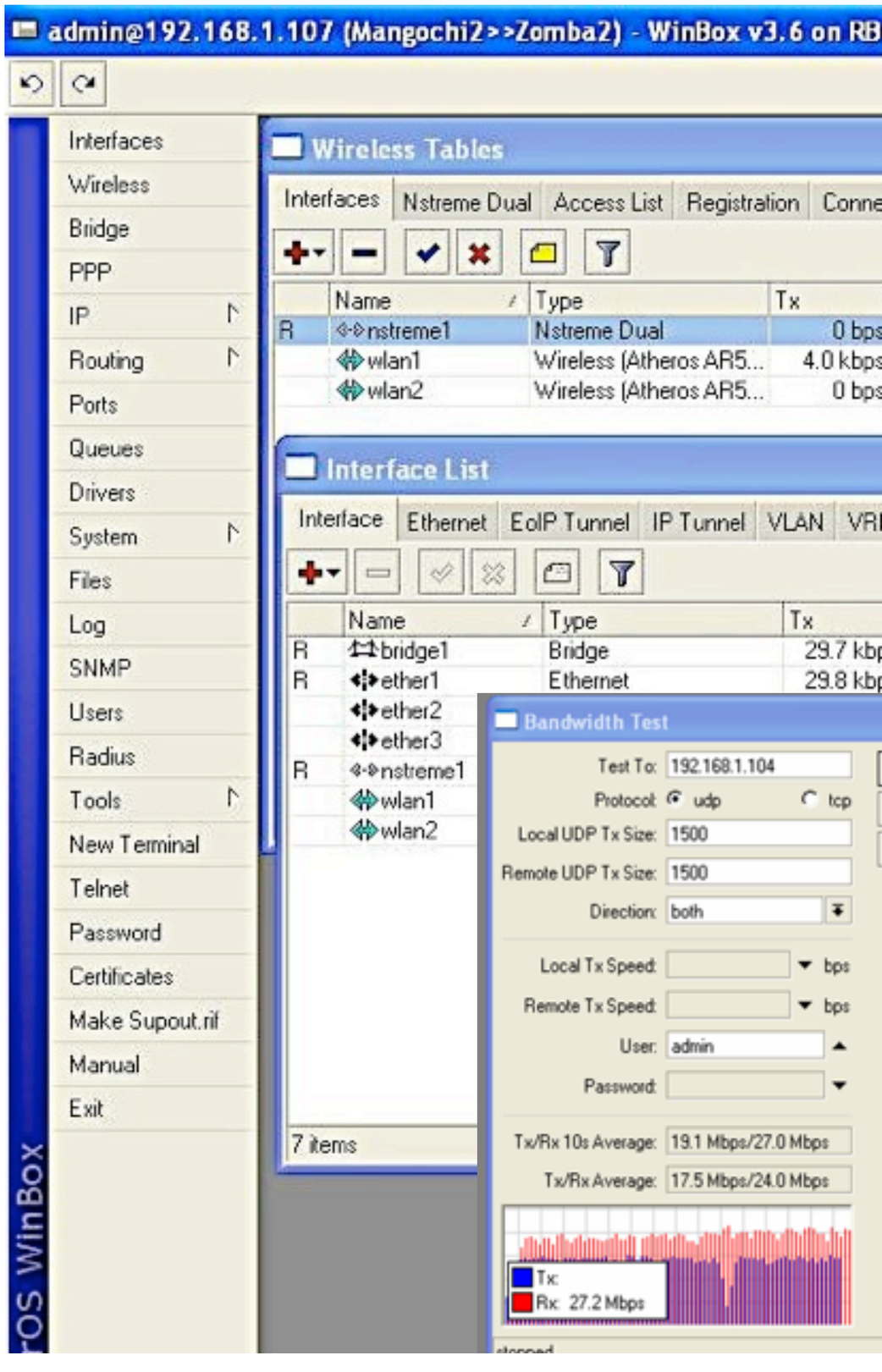
Advantages:

- Usually powerful and appealing interfaces
- Allow batch configuration of multiple devices

Disadvantages:

- Proprietary solutions
- Usually available for only one OS
- Software must be installed before starting configuration

- Mikrotik Winbox is a very powerful solution to manage even large networks



User interfaces: text shell

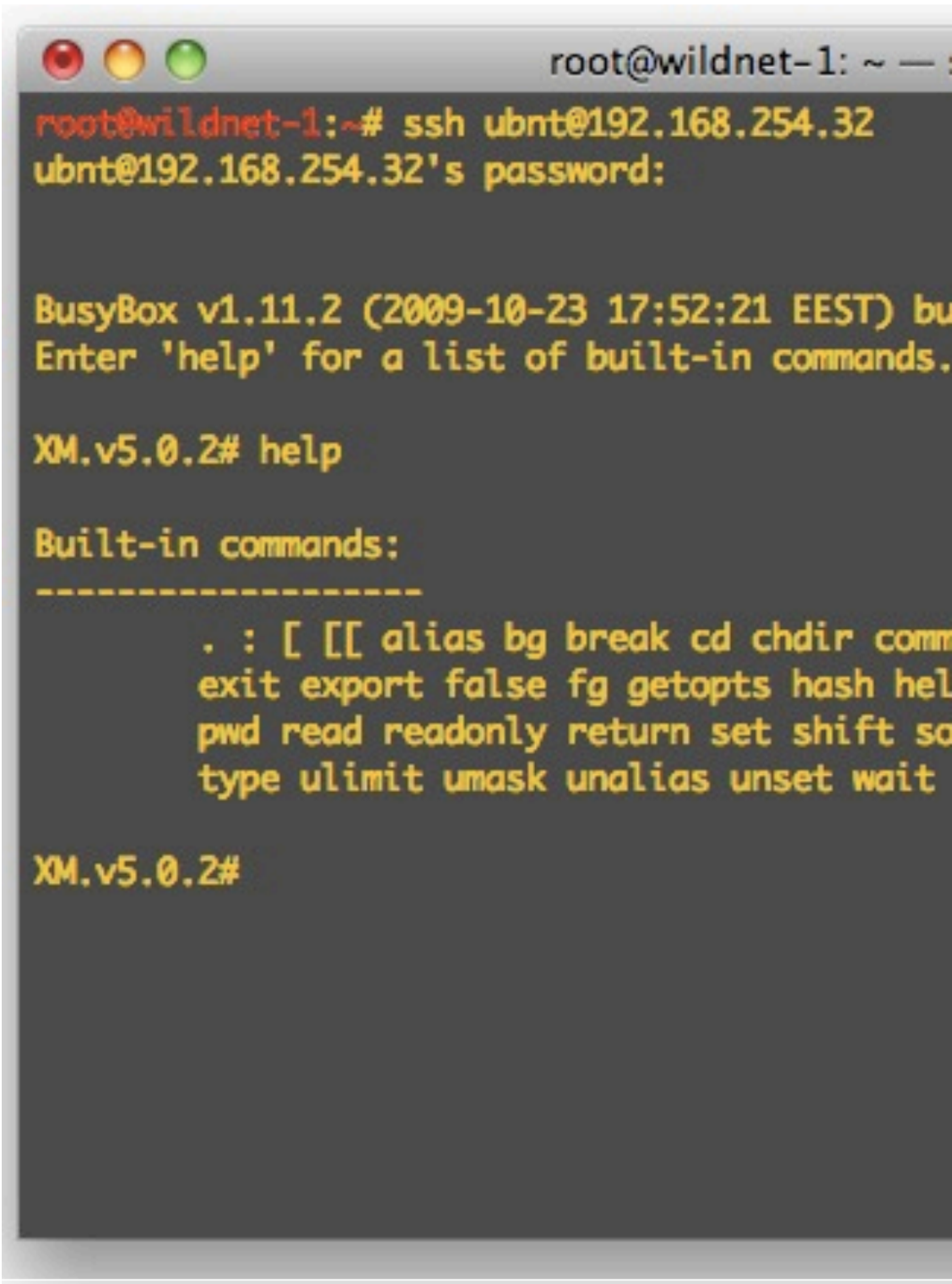
- Mikrotik (*RouterOS*), Ubiquiti (*AirOS*), high-end APs (*Cisco*), embedded PC-based APs
- Connect the device starting a serial or telnet or ssh session
- Configuration is performed with commands executed in the host operating system (usually a flavor of Linux or a proprietary OS)

Advantages:

- Very powerful
- Can be scripted

Disadvantages:

- Difficult to learn



Serial communications are for RS232 lines (usually on PC boards), many parameters are needed to establish the connection, most common are:

9600 bps / 8 bits / NO parity / 1 stop bit / NO handshaking

ssh is much safer that telnet from a security perspective (the latter should be avoided if possible)

Configure the AP

- Start from a known state, or reset the device to factory settings (always a good idea).
- Connecting to the device via Ethernet is usually easier than via wireless
- If convenient, upgrade the firmware to the latest stable version (but be careful!)
- Change the default admin username and password first!
- Change the device name with something that clearly identifys it (e.g. something like “AP_conference_room_3” or “hotspot_public_area”). This will help you to recognize the AP in future when you connect to it over the network.

Most devices with a web GUI have a default IP configuration on the network 192.168.0.0, but this is not a rule! Read the manual.

Firmware upgrade is often a risky procedure, be sure to adopt all precautions before attempt it (i.e. connect the device and the computer to a UPS, do not perform the firmware update while doing other tasks on the computer, check to have a valid firmware binary image, READ THE INSTRUCTIONS CAREFULLY!. If the procedure fails, you can end up with a unusable device that cannot be recovered (the so-called “brick”).

Remember to write down (and store in a safe place) all these settings, especially the admin username/password.

Configure the AP - IP layer

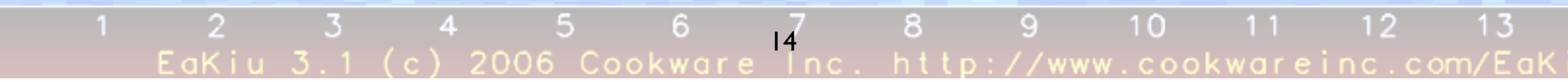
- Configure the Ethernet interface of the AP according to your wired network setup:
  - IP address/netmask/gateway *or* DHCP
  - DNS address(es)
- Double check the new settings and apply them (sometimes you may have to reboot the AP)
- Now you may need to reconfigure your PC/laptop to match the new Ethernet setup, and reconnect to the AP

If you are confident with what you are doing, you can postpone the IP configuration after the wireless setup, so to avoid the reconfiguration and reconnection of your PC or laptop. But in that way, if you make mistakes in both the wired and wireless interface setup, you may end up with an unreachable AP ;-) Therefore we advise you to do the critical configuration steps one at a time, and check the status of the device after each step.

Remember to write down (and store in a safe place) all IP settings

Configure the AP - physical layer

- Configure the mode: ***master*** (or ***access point*** or ***base station***)
- Configure the SSID (the name of the wireless network created by the AP, up to 32 characters long): *it is best to choose a meaningful name.*
- Configure the wireless channel, according to the local regulations and the result of the site survey. Do not use a channel that is already occupied by another AP or other sources of RF power. *You should already have planned the channel in advance, during the design phase.*
- Configure the transmit power and network speed (these values may also be set to "*automatic*" in some devices).



The mode can usually be configured among these choices: "master" (a.k.a. "access point", "base station", "BS"), "client" (a.k.a. "managed", "station", "client station", "CPE"), "monitor", "WDS" (Wireless Distribution System), and quite rarely some other variants.

Sometimes you don't want to set the SSID (Service Set Identifier) with a name that is easily associated with your company/institution. But remember that "security through obfuscation is not real security!", i.e. a hidden or fake/random SSID does not add much security to your network).

The choice of the best channel is sometimes a hard task, and you may need to perform a site survey with software tools (wireless sniffers) or hardware spectrum analyzers (like the WiSpy from Metageek and the AirView from Ubiquiti).

The value of transmit power is also subject to local regulation, check in advance which is the maximum allowed by law, and try always to use the minimum value that fit your needs, in order to avoid interference with other networks (of your or others).

The choice of network speed is limited to the values that are part of 802.11a/b/g/n standards (up to 54 Mbps), but some vendors created extensions to the standards (often called "turbo" modes) of 100 Mbps or higher. These are non-standard and may not be able to interoperate with equipment from other vendors.

Configuring "backwards compatibility" modes (such as supporting 802.11b on 802.11g networks) will reduce the overall throughput available to your fastest clients. The Access Point must send the preamble at a slower rate for 802.11b clients, and actual communications between the client and the AP happen at 802.11b speeds. This takes more time, and slows down the otherwise faster 802.11g clients.

Configure the AP - security

- Configure the security features of the network:
  - No encryption (all traffic is in clear)
  - WEP (*Wired Equivalent Privacy*), 40 or 104 bits keys, it is flawed and therefore **deprecated**
  - WPA / WPA2 (*WiFi Protected Access*): PSK, TKIP and EAP
- Enable or disable (hide) the SSID broadcast ("beacon")
- Enable or disable an Access Control List (based on MAC addresses of clients)

NOTE: security settings are often a hard choice, and it may be difficult to balance good protection from unintentional users with easy access for authorized users. More complex security needs will require a more complex configuration and additional software.

There will be a lecture devoted to wireless security, with more information about these topics.

Hidden SSID and MAC filtering do not add much security, and are hard to maintain and a source of troubles for inexperienced users of the network.

MAC filtering is a weak security measure:
– A malicious client can capture packets and find our which MAC addresses have right to associate
– It can then change its own MAC address to one of the accepted ones and "fool" the access point

Configure the AP - routing/NAT

- Advanced IP layer and routing configuration features are often included in modern access points.
- This can include functionality for routing and Network Address Translation (NAT), in addition to basic bridging
- Advanced IP configuration includes:
  - Static routing
  - Dynamic routing
  - NAT (masquerading, port forwarding)
  - Firewalling
- Some APs can also act as file servers and print servers (external HD and printers can be connected via USB)

Configure the AP - advanced

- A few more advanced settings may be available for your AP, depending from the model/vendor/firmware/etc.:
  - Beacon interval
  - RTS/CTS
  - Fragmentation
  - Interference robustness
  - Vendor extensions to the WiFi standards
  - Other settings for long distance links (10 to 100 kilometers) and better security.

RTS/CTS (ready to send, clear to send) mechanism can help alleviate the problem of hidden nodes (clients that can "hear" the AP but not the other clients, therefore creating interferences to them)

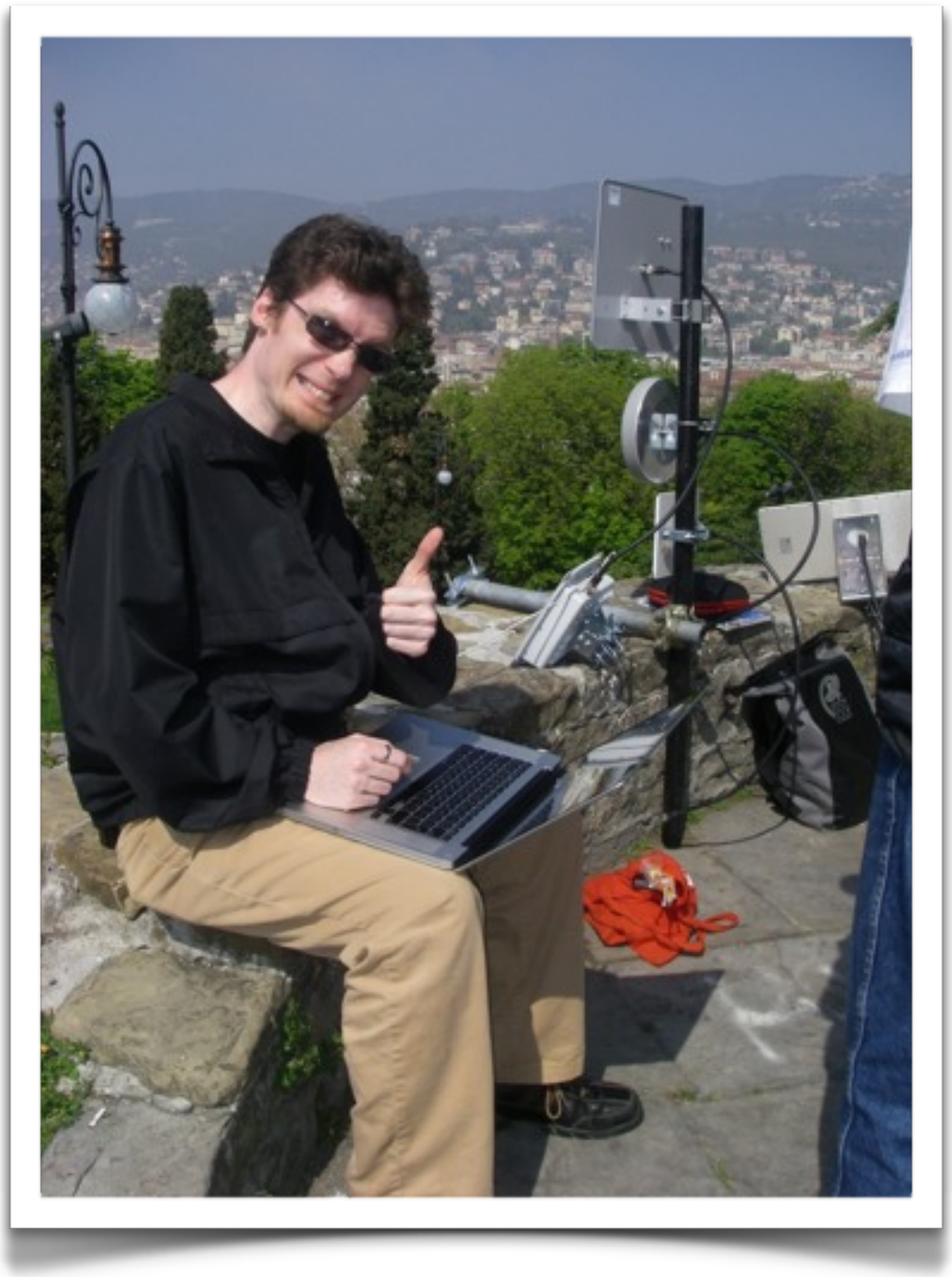
Configuration of the fragmentation can be used to increase performances in case of low signal (areas with marginal coverage, long links)

Configure the client

- Client side configuration is much simpler:
  - Configure the mode: **client** (or **managed**, **station**, **client station**, **CPE**)
  - Configure the SSID of the network to be joined
  - The channel, speed, and other parameters will be set automatically to match the AP
- If WEP or WPA is enabled on the AP, you will have to enter the matching password (key)
- Clients may also have additional (often vendor-specific) settings. *For example, some clients can be configured to associate only with an AP with a specified MAC address.*

Hints

- Follow the general guidelines in this talk to get started.
- Remember that the concepts in setting up an access point or wireless client are more important than the name a vendor may give to a particular feature.
- Focus on understanding what each parameter does and how they depend on each other.
- Concepts are not specific to vendors or devices – the important part is to recognize the basic settings, even if they come *under different names and in different colors*.
- Don't be afraid to try new settings, but keep a copy of your working configuration handy. Experiment!



Hints - working outdoors

- You should try to configure the devices (both APs and clients) well in advance and in an comfortable place (e.g. a laboratory). Working outdoor is more difficult and may lead to mistakes ("on-site" configuration = trouble).
- If you **must** do configuration outdoors, be sure to have enough battery charge on your laptop, carry all required information with you (on paper, not only in electronic format) and carry a notepad to take note of all of the changes you make. Good documentation is paramount for future maintenance in the field.

Troubleshooting (summary)

- Organize your work in logical steps and follow them.
- Read the manual, study the meaning of parameters and settings, do tests and experiments (don't be scared!)
- In case of problems, do a factory reset and try again
- If the problem persists, try again **changing one parameter/setting at a time**
- Still doesn't work? Google with relevant keywords (name of the device, etc.), search in forums and manufacturer / vendors websites
- Upgrade the firmware to the latest version.
- If you still have problems try with a different client/AP.

Use the theory of "known good" to simplify your troubleshooting technique. Each time you get the equipment to a "working" state, make a backup.

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/

See Chapters 5 and 9 of the book for more detailed information about the material covered in this talk.