

Configuration of Access Points and Clients

Training materials for wireless trainers



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



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.



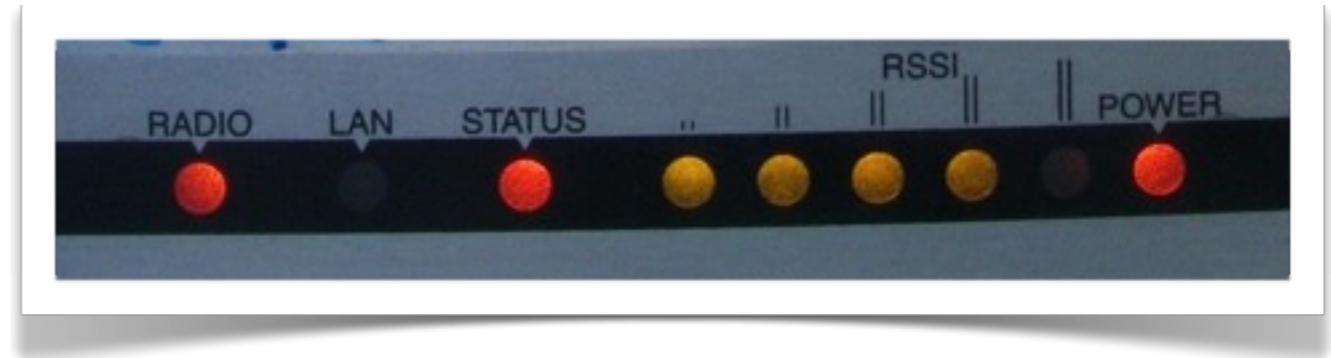
Get in touch with the device

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).

Get in touch with the device

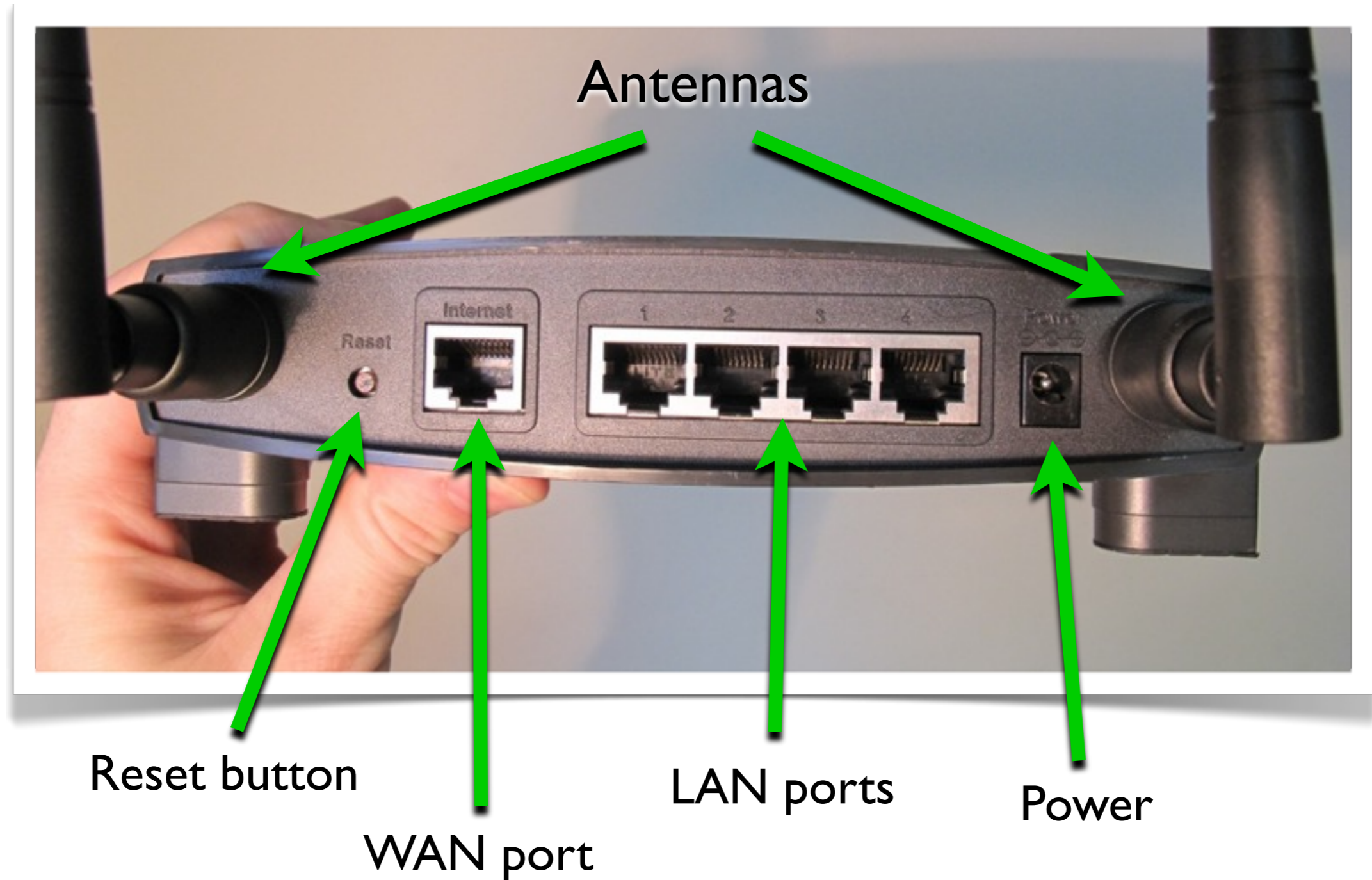
- ▶ Power button (not always present).
- ▶ Reset button (often “hidden” in a small hole, can be pressed using a straightened paperclip).

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.

Get in touch with the device

Identify the different ports and interfaces.



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)



User interfaces: GUI (web page)

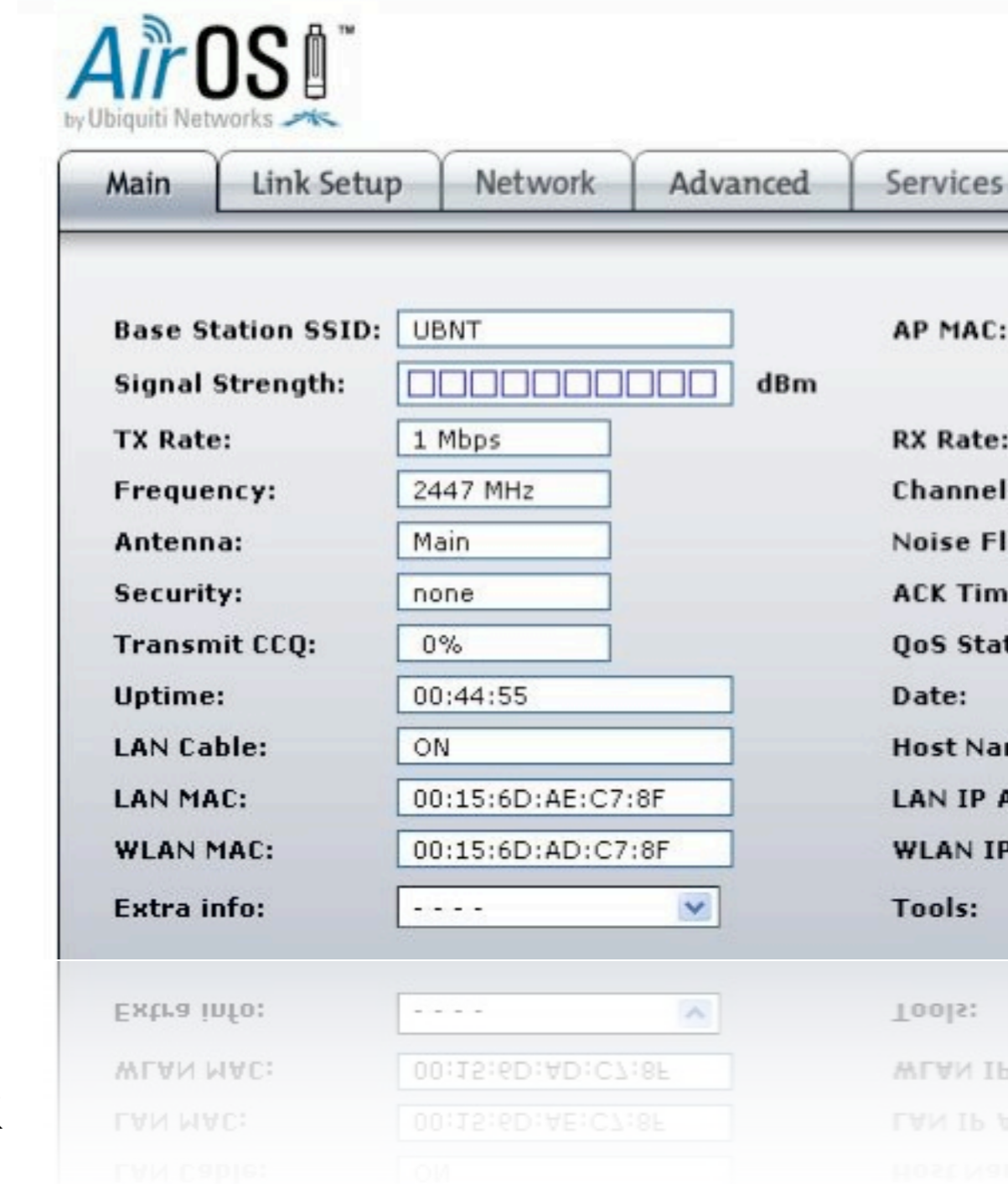
- ▶ Linksys, Ubiquiti, most modern APs

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.



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

admin@192.168.1.107 (Mangochi2>>Zomba2) - WinBox v3.6 on RB

Interfaces

Wireless Tables

Name	Type	Tx
nstmre1	Nstmre Dual	0 bps
wlan1	Wireless (Atheros AR5...	4.0 kbps
wlan2	Wireless (Atheros AR5...	0 bps

Interface List

Name	Type	Tx
bridge1	Bridge	29.7 kbps
ether1	Ethernet	29.8 kbps
ether2		
ether3		
nstmre1		
wlan1		
wlan2		

Bandwidth Test

Test To: 192.168.1.104

Protocol: udp tcp

Local UDP Tx Size: 1500

Remote UDP Tx Size: 1500

Direction: both

Local Tx Speed: bps

Remote Tx Speed: bps

User: admin

Password:

Tx/Rx 10s Average: 19.1 Mbps/27.0 Mbps

Tx/Rx Average: 17.5 Mbps/24.0 Mbps

Tx: Rx: 27.2 Mbps

User interfaces: text shell

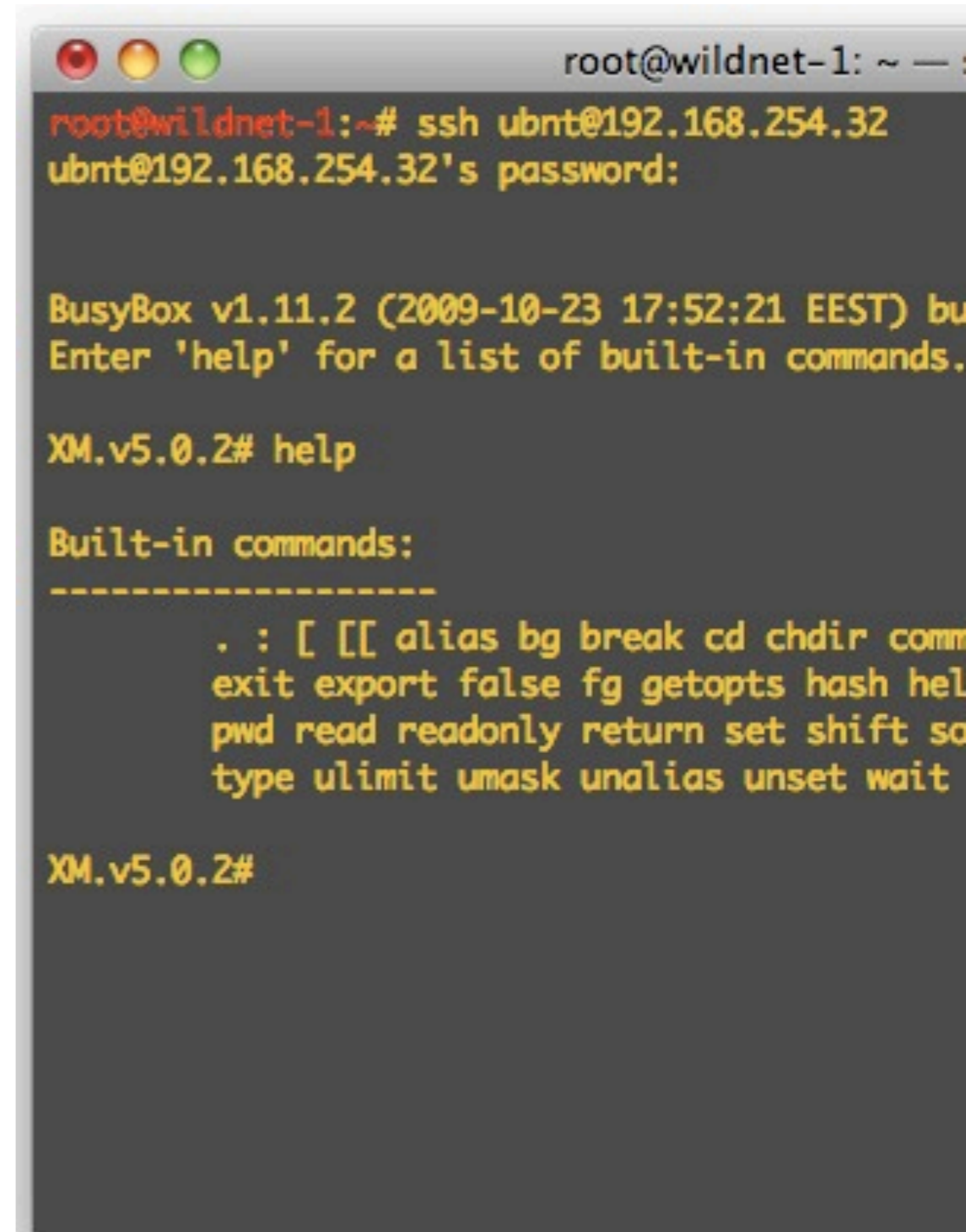
- ▶ Mikrotik (*RouterOS*), Ubiquiti (*AirOS*), high-end APs (*Cisco*), embedded PC-based APs
- ▶ Connect the device starting a serial or telnet or ssh session
- ▶ Configuration is performed with commands executed in the host operating system (usually a flavor of Linux or a proprietary OS)

Advantages:

- ▶ Very powerful
- ▶ Can be scripted

Disadvantages:

- ▶ Difficult to learn



```
root@wildnet-1: ~ —
root@wildnet-1:~# ssh ubnt@192.168.254.32
ubnt@192.168.254.32's password:

BusyBox v1.11.2 (2009-10-23 17:52:21 EEST) bu
Enter 'help' for a list of built-in commands.

XM.v5.0.2# help

Built-in commands:
-----
. : [ [[ alias bg break cd chdir comm
exit export false fg getopt hash hel
pwd read readonly return set shift so
type ulimit umask unalias unset wait

XM.v5.0.2#
```


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 identifies 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.

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

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).

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)

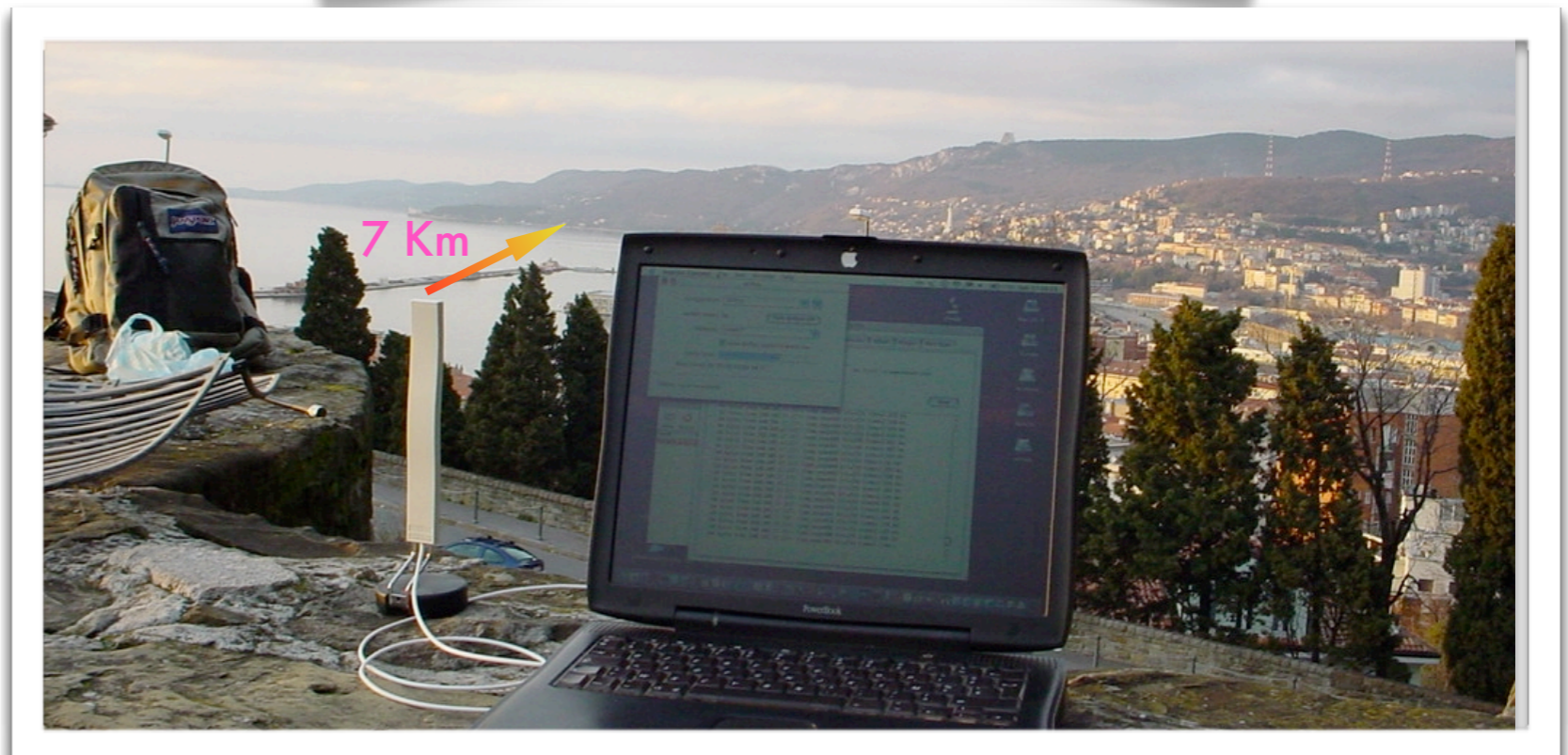
NOTE: security settings are often a hard choice, and it may be difficult to balance good protection from unintentional users with easy access for authorized users. More complex security needs will require a more complex configuration and additional software.

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.



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.

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/>

