Configuration of Access Points and Clients

Training materials for wireless trainers

The Abdus Salam
International Centre
for Theoretical Physics

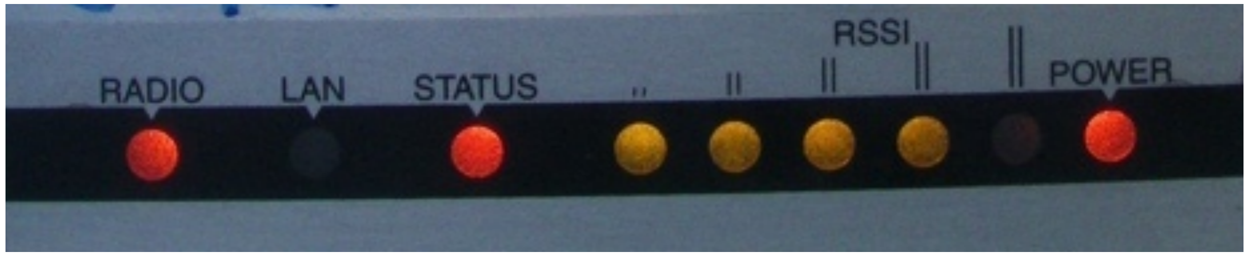
Goals

- 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 advices

Before to start a configuration

- get all User’s Manuals and Specification Sheets available for the devices you are going to deploy
- if you get second-hand devices, be sure to receive full information on their current –or last-known– configuration (e.g. password, IP addresses, etc.)
- keep ready on hands all the plans you have already done for the network you are going to deploy (link budget, network topology scheme and IP settings)
- be ready to take written notes of all settings that you are going to apply (specially passwords!)
- make backups of *last-known-good* configuration files

Get in touch with the device



- discover 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 on a 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 interface(s), sometimes called WLAN(s): one or more antenna connectors (or non-detachable antennas)
  - one or more Ethernet interface(s):
    - one or more ports for local network (LAN)
    - one port for uplink (also called WAN)
  - power input (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 trough the same UTP cable that carries the Ethernet data: this is called Power-over-Ethernet (PoE) and follows some standards.

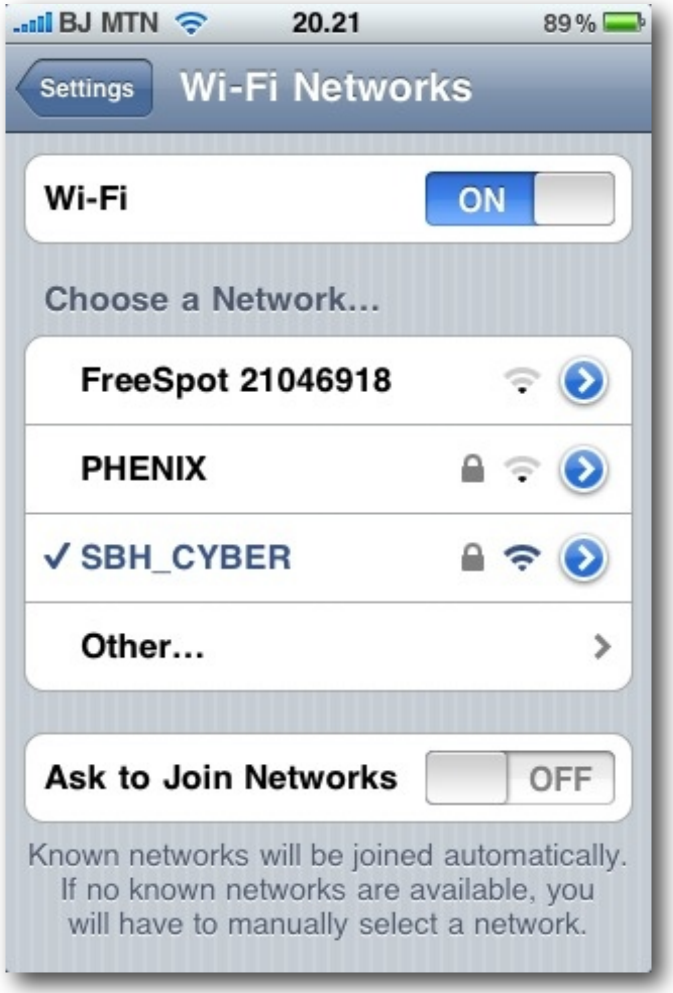
Get in touch with the device

- power button (not always present)
- reset button (often “hidden” in a small hole, can be pressed using a straightened paperclip): it may have different effects (like simple restart VS factory full reset) if pressed shortly VS for a longer time (even 30 seconds). Read the manual!

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

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)
  - Text interface (telnet, ssh): Linux or other OS
  - Software interface embedded in the system (when the AP/client is a computer or smartphone or other "smart" device, with its OS)



BJ MTN 20.21 89 %

Settings | Wi-Fi Networks

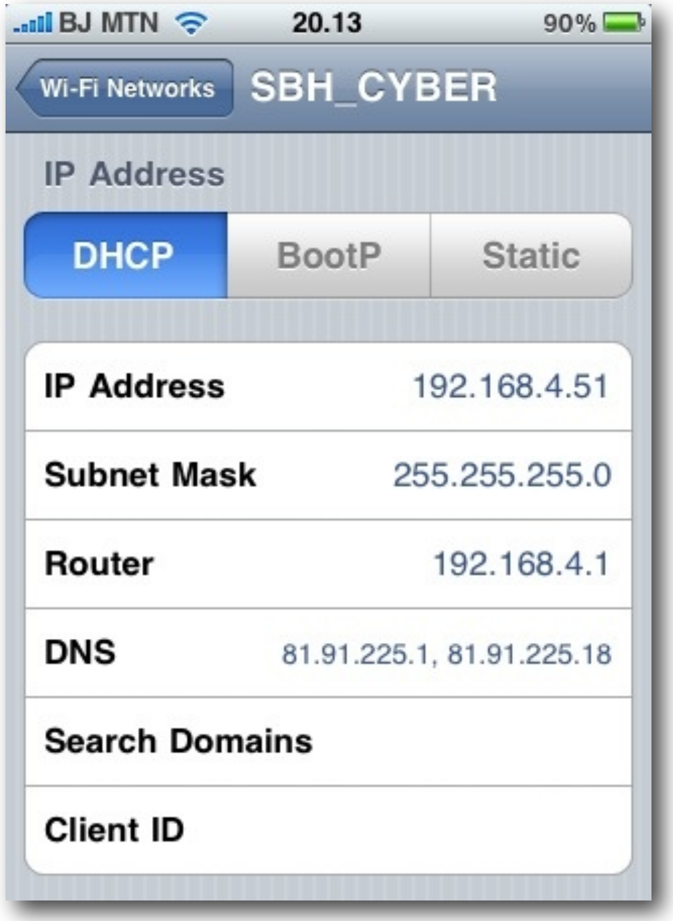
Wi-Fi: ON

Choose a Network...

- FreeSpot 21046918
- PHENIX
- ✓ SBH_CYBER
- Other...

Ask to Join Networks: OFF

Known networks will be joined automatically. If no known networks are available, you will have to manually select a network.



BJ MTN 20.13 90%

Wi-Fi Networks | SBH_CYBER

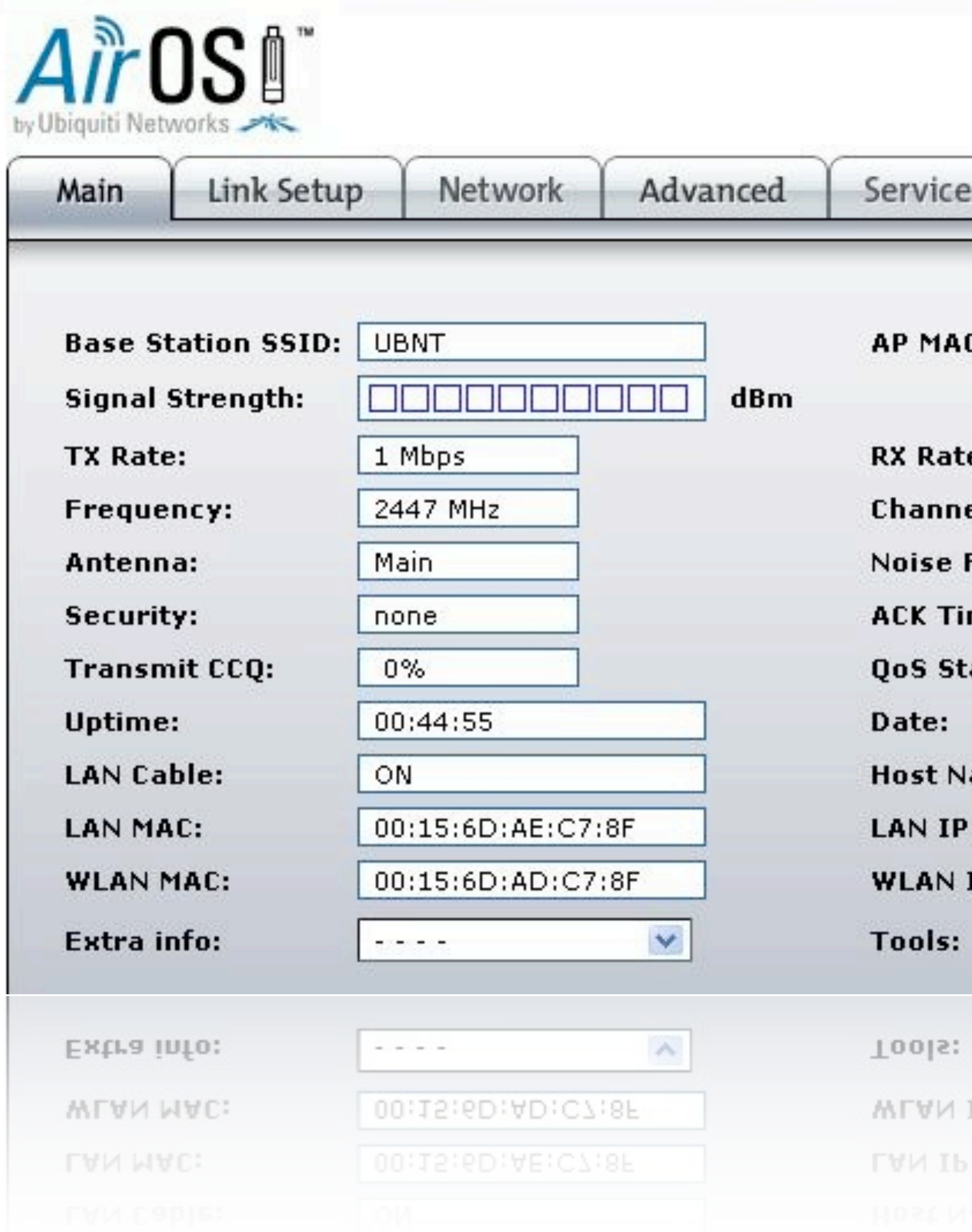
IP Address

DHCP | BootP | Static

IP Address	192.168.4.51
Subnet Mask	255.255.255.0
Router	192.168.4.1
DNS	81.91.225.1, 81.91.225.18
Search Domains	
Client ID	

User interfaces: GUI (web page)

- examples:
  - Linksys, Ubiquiti, most modern APs
- advantages: works with all browsers and operating systems
- disadvantages: static interface (do not reflect changes immediately), sometimes poor feedback, sometimes incompatible with less common browsers, it needs a working TCP/IP configuration
- notes: some recent implementation (e.g. Ubiquiti) are very good and use modern dynamic features of web to provide feedback and advanced tools



Base Station SSID: UBNT

Signal Strength: □□□□□□□□□□ dBm

TX Rate: 1 Mbps

Frequency: 2447 MHz

Antenna: Main

Security: none

Transmit CCQ: 0%

Uptime: 00:44:55

LAN Cable: ON

LAN MAC: 00:15:6D:AE:C7:8F

WLAN MAC: 00:15:6D:AD:C7:8F

Extra info: - - - -

AP MAC

RX Rat

Channe

Noise F

ACK Ti

QoS St

Date:

Host N

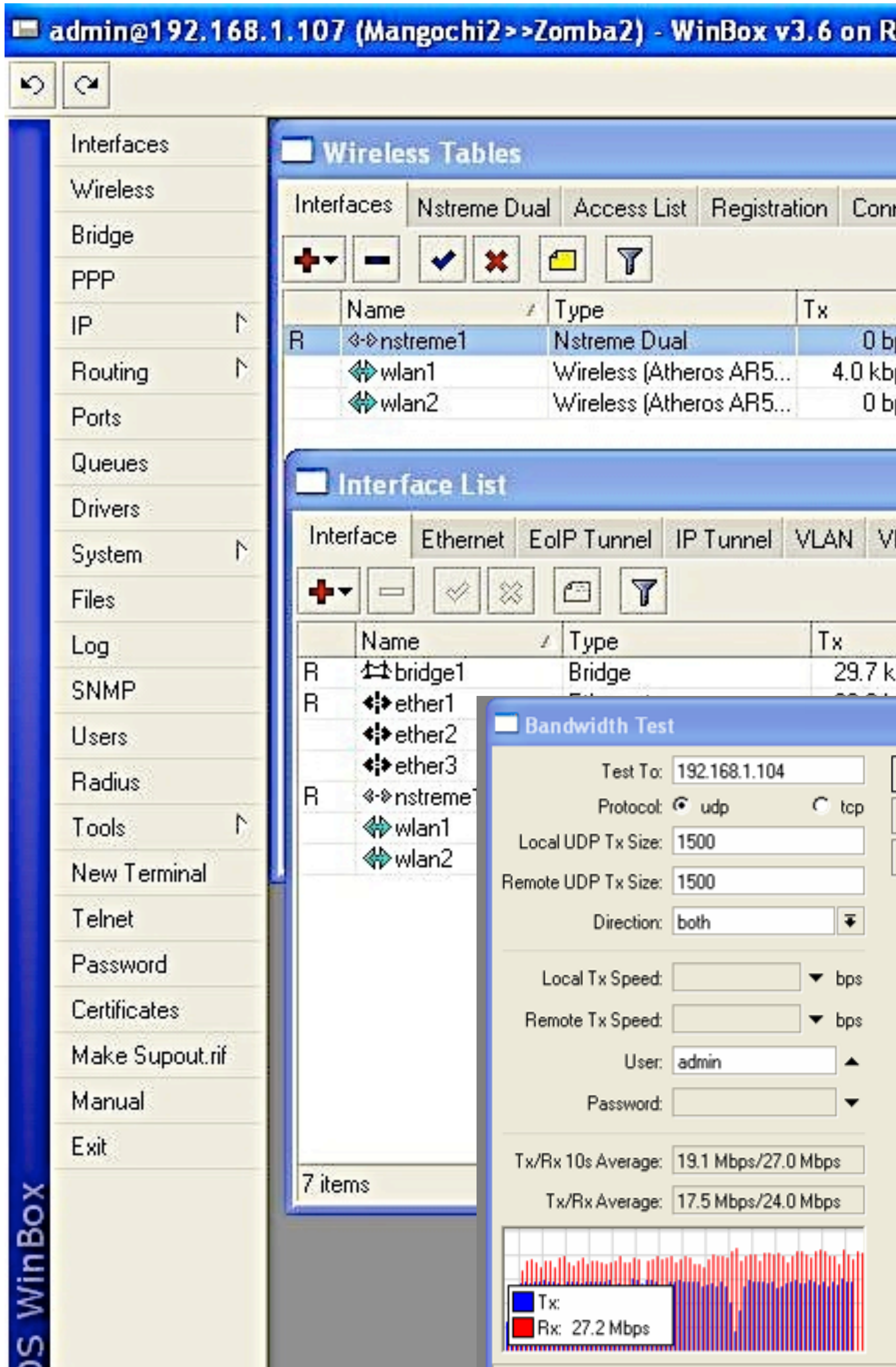
LAN IP

WLAN I

Tools:

User interfaces: GUI (software)

- examples:
  - Mikrotik *Winbox*, Apple *Airport Utility*, Motorola *Canopy*, most old APs had similar softwares
- advantages: usually powerful and appealing interfaces, often they allow batch configuration of multiple devices
- disadvantages: proprietary solutions, usually available for one OS only, you need to install the software before to start the configuration
- notes: Mikrotik Winbox is a very powerful solution to manage even large networks



Wireless Tables

Interfaces | Nstreme Dual | Access List | Registration | Conn

	Name	Type	Tx
R	nstreme1	Nstreme Dual	0 b
	wlan1	Wireless (Atheros AR5...	4.0 kb
	wlan2	Wireless (Atheros AR5...	0 b

Interface List

Interface | Ethernet | EoIP Tunnel | IP Tunnel | VLAN | V

	Name	Type	Tx
R	bridge1	Bridge	29.7 k
R	ether1		
	ether2		
	ether3		
R	nstreme		
	wlan1		
	wlan2		

7 items

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

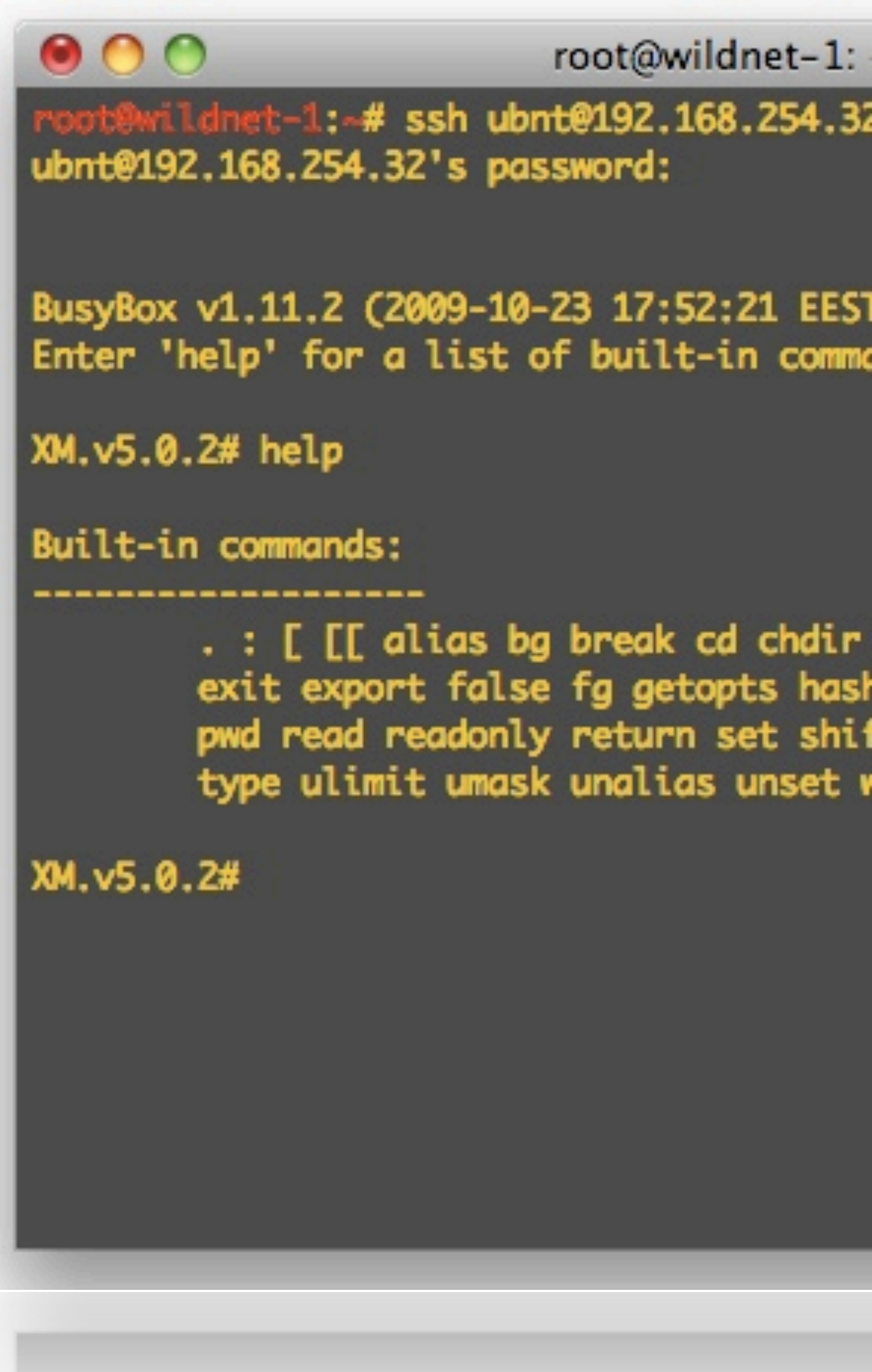
Tx/Rx Average: 17.5 Mbps/24.0 Mbps

Tx:

Rx: 27.2 Mbps

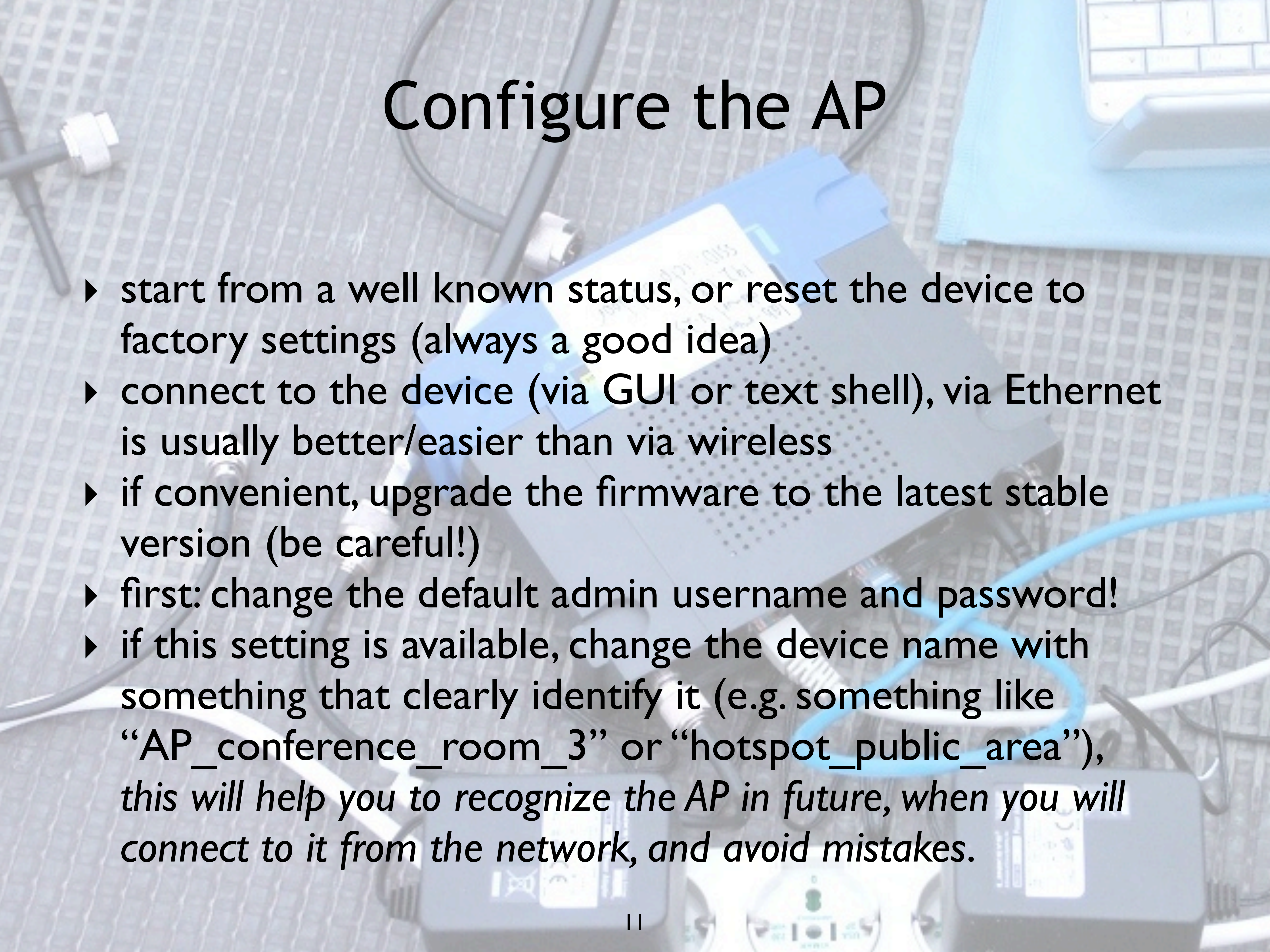
User interfaces: text shell

- you connect the device starting a serial or telnet or ssh session
- the configuration of the device is performed with commands executed in the host operating system (a flavor of Linux or a proprietary OS)
- examples:
  - Mikrotik (RouterOS), Ubiquiti (AirOS), high-end APs like some Cisco, PCboard-based APs
- advantages: very powerful, can be scripted
- disadvantages: difficult to learn



```
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
Enter 'help' for a list of built-in comma

XM.v5.0.2# help

Built-in commands:
-------------------
        . : [ [[ alias bg break cd chdir
        exit export false fg getopts hash
        pwd read readonly return set shif
        type ulimit umask unalias unset w

XM.v5.0.2#
```

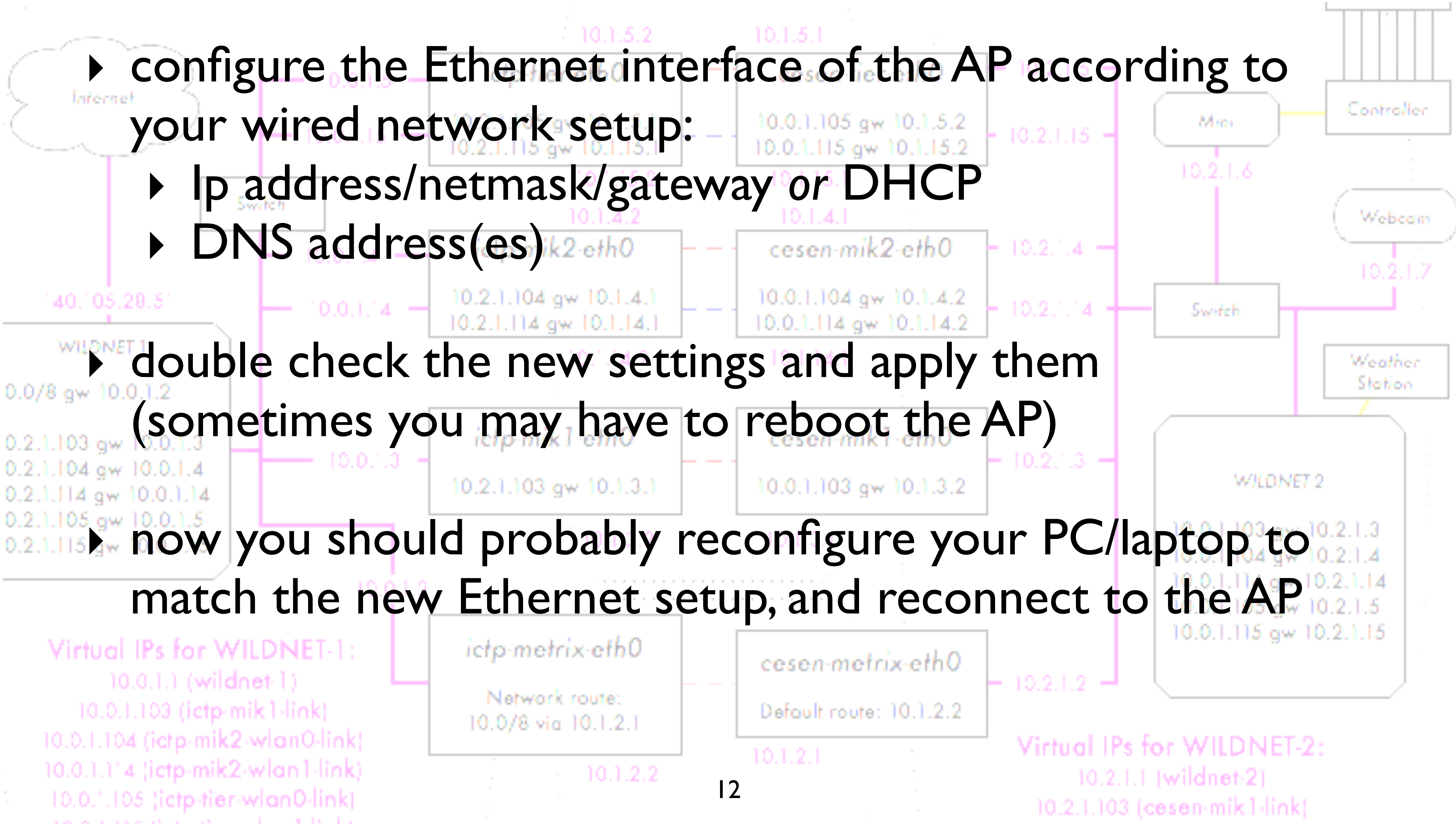
Configure the AP



- start from a well known status, or reset the device to factory settings (always a good idea)
- connect to the device (via GUI or text shell), via Ethernet is usually better/easier than via wireless
- if convenient, upgrade the firmware to the latest stable version (be careful!)
- first: change the default admin username and password!
- if this setting is available, change the device name with something that clearly identify 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 will connect to it from the network, and avoid mistakes.*

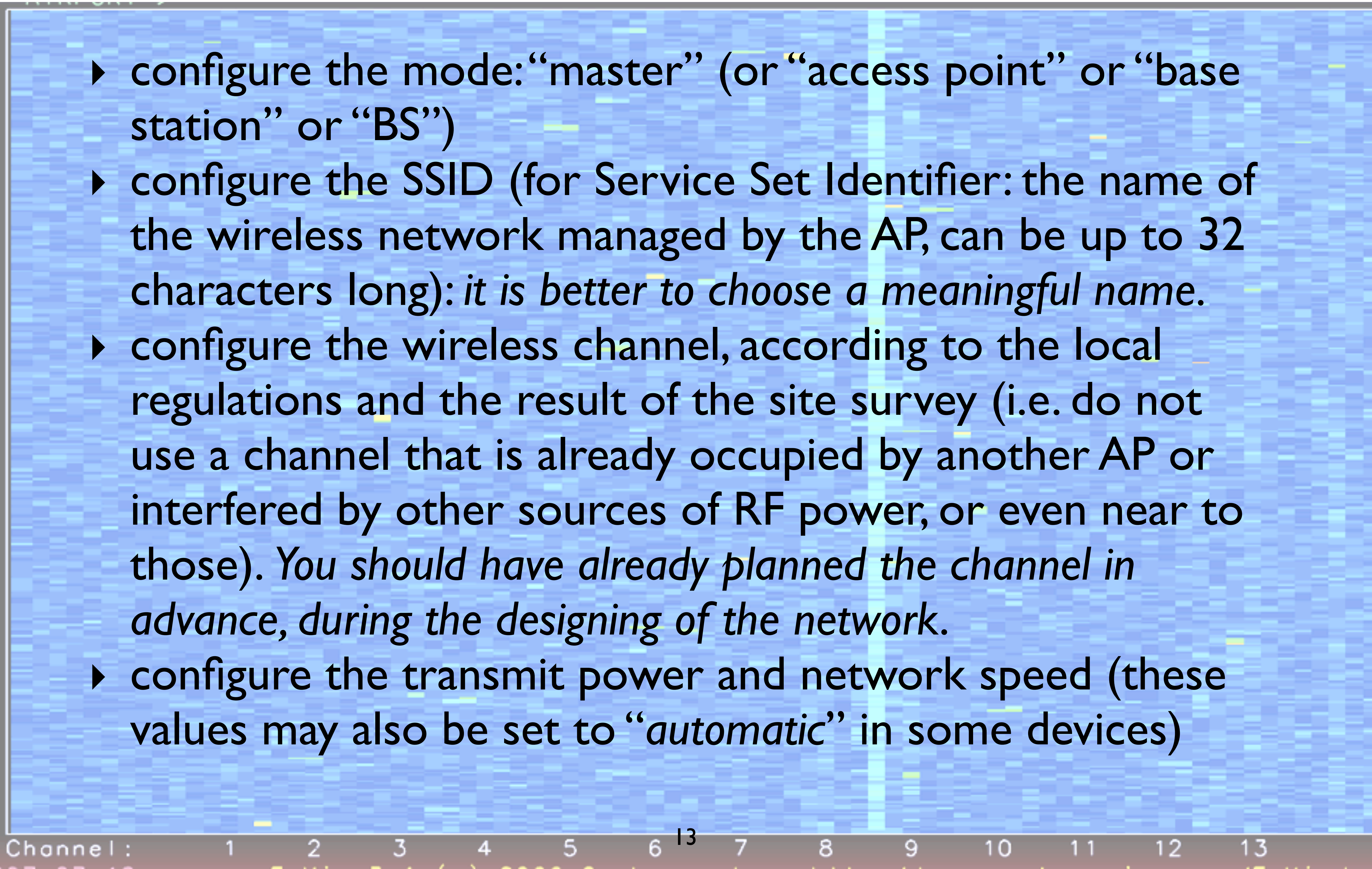
Configure the AP - IP layer

- 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 should probably 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” or “BS”)
- configure the SSID (for Service Set Identifier: the name of the wireless network managed by the AP, can be up to 32 characters long): *it is better to choose a meaningful name.*
- configure the wireless channel, according to the local regulations and the result of the site survey (i.e. do not use a channel that is already occupied by another AP or interfered by other sources of RF power, or even near to those). *You should have already planned the channel in advance, during the designing of the network.*
- configure the transmit power and network speed (these values may also be set to “*automatic*” in some devices)



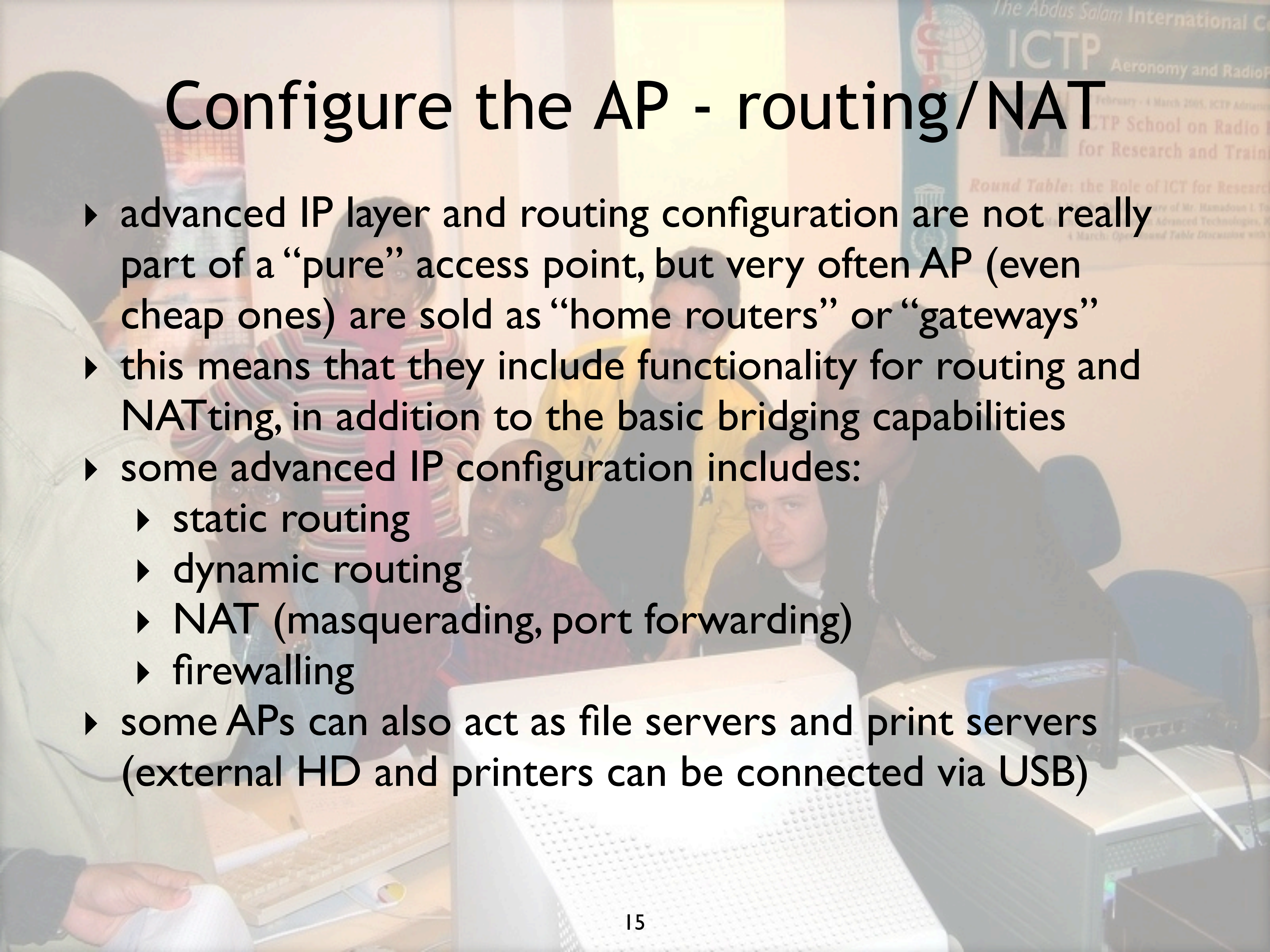
Configure the AP - security

- configure the level of security of the network, choose from the followings:
  - no security (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 the Access Control List (based on MAC addresses of clients)

NOTE: security settings are often a hard choice, it may be difficult to balance a good protection from unintentional users with an easy access for authorized users. Anyway, these simple settings can offer only a basic protection, that can be overcome by malicious users.

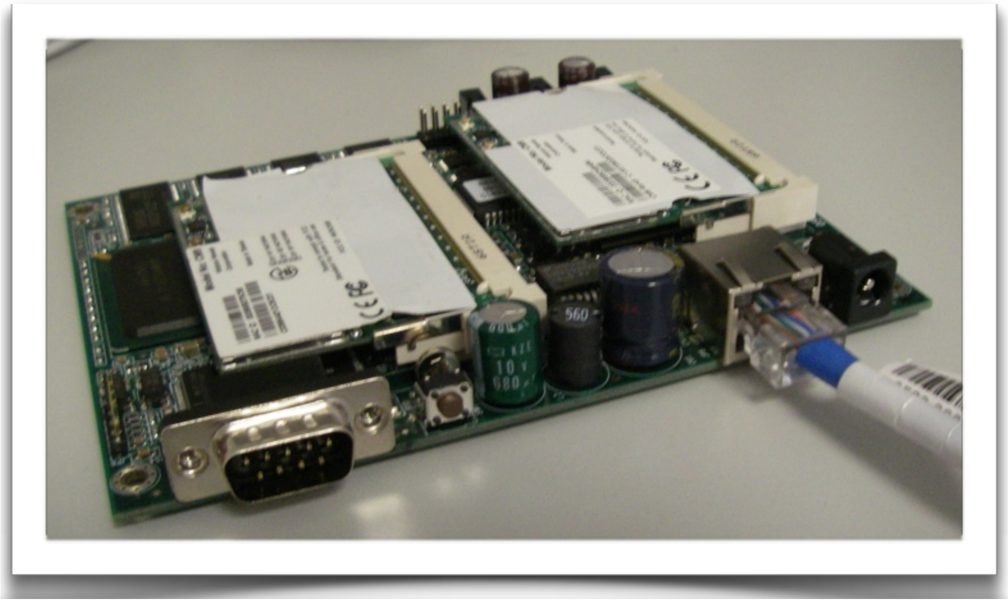
Configure the AP - routing/NAT

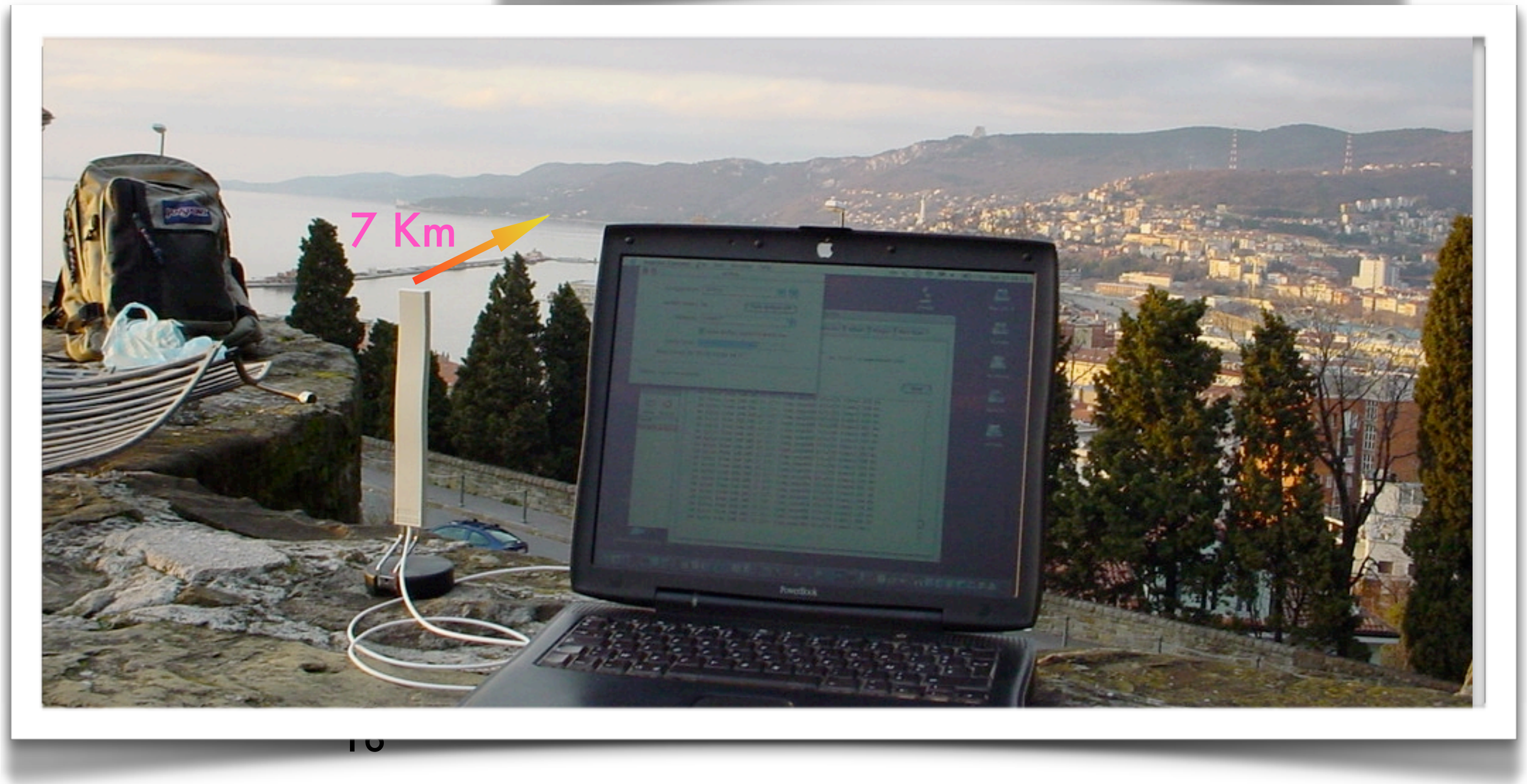
- advanced IP layer and routing configuration are not really part of a “pure” access point, but very often AP (even cheap ones) are sold as “home routers” or “gateways”
- this means that they include functionality for routing and NATting, in addition to the basic bridging capabilities
- some advanced 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)


The Abdus Salam International C
ICTP
Aeronomy and Radio
ICTP School on Radio
for Research and Train
Round Table: the Role of ICT for Researc

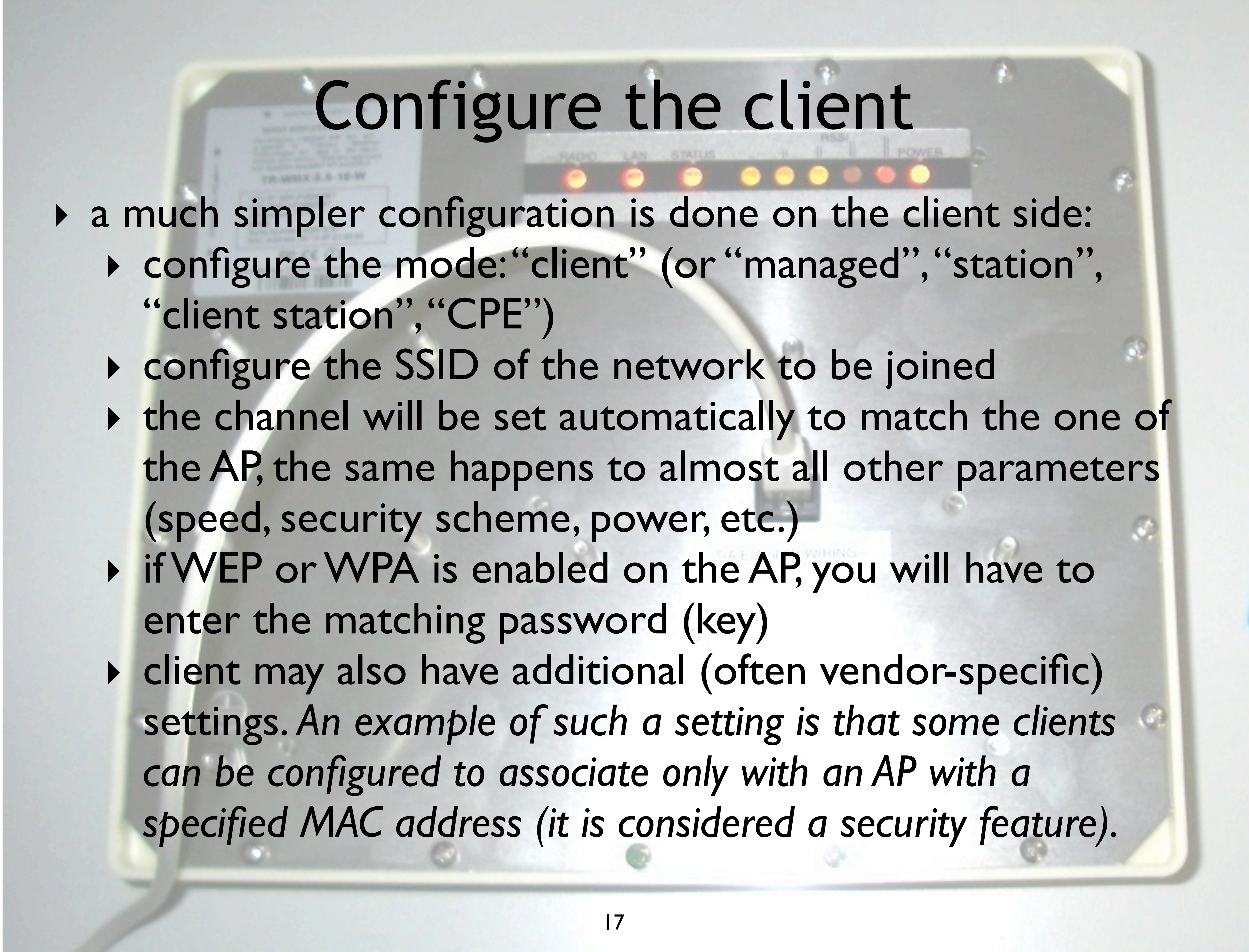
Configure the AP - advanced

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





Configure the client



- a much simpler configuration is done on the client side:
  - configure the mode: “client” (or “managed”, “station”, “client station”, “CPE”)
  - configure the SSID of the network to be joined
  - the channel will be set automatically to match the one of the AP, the same happens to almost all other parameters (speed, security scheme, power, etc.)
  - if WEP or WPA is enabled on the AP, you will have to enter the matching password (key)
  - client may also have additional (often vendor-specific) settings. *An example of such a setting is that some clients can be configured to associate only with an AP with a specified MAC address (it is considered a security feature).*

Hints

- follow the general guidelines for setting up wireless devices
- remember general steps (concepts) in setting up an access point or wireless client
- 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 scared of trying new settings, make experiments!

Hints - working outdoor

- try always to do the configuration of the devices (both APs and clients) well in advance and in an comfortable place (e.g. a laboratory), to work outdoor is more difficult and may lead to mistakes ("on-site" configuration = troubles)
- if you HAVE TO do a configuration outdoor, be sure to have enough battery charge on your laptop, to carry with you all information you may need (on paper, not in electronic format only) and to carry a notepad and take notes of all settings you are doing. Good documentation is paramount for future maintenance works on 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 producer/vendors websites, upgrade the firmware to the latest version (if there are suspects that the issue has been solved), try with a different clients/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

WIRELESS NETWORKING
IN THE DEVELOPING WORLD
SECOND EDITION
A practical guide to planning and building low-cost telecommunications infrastructure
wndw.net