



Wireless Checklist

Requirements Analysis

- What is the total number of users you want to connect wirelessly?
- What is the maximum number of users that will connect simultaneously?
- Do we need to give wireless access to guests?
- Are some wireless devices already present in the company?
 - Which ones? What brand? What wireless standards do they support?
- Which/how many PC/Palmtops are going to be used for a wireless access?
 - What is their OS (Operating System) ?
- Do we need to connect any printers and/or video cameras wirelessly?
 - Which ones and how many?
- Which applications do we want to use wirelessly?
- What is the speed required by the users and the applications used?
- What future growth (number of users, applications, coverage area) can we expect?

Site Survey

Existing Ethernet cabling

- how far can it be extended (max. length of an Ethernet Cat. 5 cable is 100 m.)
- existing switches and hubs (AP should be connected to a switch, not a hub)
- existing Ethernet ports

Where are the power outlets positioned?

Are there any UPS (Uninterruptable Power Supply) devices or is there a need for them?

Access Point positioning

Normally placed at the center of the coverage area, on the ceiling, with antennas pointing straight down.

Does Ethernet cabling and power reach the selected AP location?

Coverage tests

How many APs are needed?

If more than one, is roaming required?

More APs (max. 3) in the same coverage area can support more users and give them more bandwidth (set them to non-overlapping channels to avoid interference)

Is there a need for directional antennas?

Regulations

Antennas: European Directive 1999/05/CE

Security for Access Points

Change default settings:

Change default SSID (wireless network name); do not insert the company name into the SSID

Disable SSID broadcast

Change AP administrator's password

Disable remote AP management

Change default IP address of AP and internal network.

If the pc's are not too many, use MAC address filtering on the AP and enter the MAC address of the wireless cards

Limit AP transmission power in order to obtain coverage only where required, not outside

Enable adequate encryption:

WEP (64, 128 bit) -- minimum level

TKIP with WPA-PSK

AES with WPA/WPA2/802.11i

IPSec / L2TP with VPN

Keep firmware (software inside the AP) always at the latest level, then check often on the producer web-site for newer updates

Limit the number of the addresses allocated by DHCP server or use fixed addresses and disable the DHCP server.

Switch off the AP when not in use.

Separate the wireless network from the internal company network with a firewall, if possible.

Enable wireless authentication, if possible:

With WEP, it is better to use "open authentication" in order to not give away the encryption key

802.1x for port authentication, tied to an EAP method and to a RADIUS server (WPA/WPA2 Enterprise mode)

VPN

Security for HotSpot Use

Install and always activate personal firewall software on the pc

install, start, and keep updated anti-virus software

Keep the operating system updated (perform Windows Update regularly or automatically)

Disable optional file/desktop sharing

Enter personal userids and passwords only on safe web sites (padlock on the browser)

Regularly backup important data

Access Point Choice

Adherence to the standard 802.11g

Maximum speed

Use of only one wireless channel

Transmission Power levels

Removable antenna

Security features (the maximum is WPA2/802.11i with AES)

Maximum number of users supported, with margin for growth

Availability of "Power Over Ethernet" kit to supply electrical power to AP using Ethernet cable

Support for other wireless features: bridge, repeater, WDS

Other non wireless functions: ADSL modem , router, firewall, switch, print server

Vendor reputation and previous experience with vendor

Price

DIAL-UP
CONNECTIVITY



WIRELESS
NETWORKING



WIRED
NETWORKING



SECURITY:
ROUTERS AND
GATEWAYS



USRobotics®