

Wireless LAN

- WLAN:
 - Make use of a wireless transmission medium
 - Typically restricted in their diameter: buildings, campus, single room etc..
 - The global goal is to replace office cabling and to introduce high flexibility for ad hoc communication (e.g. Group meetings)

Wireless LAN advantages

- Flexibility: within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls.
- Planning: wireless ad hoc networks allow for communication without planning. Wired networks need wiring plans.
- Robustness: wireless networks can survive disasters, if the wireless devices survive people can still communicate

Wireless LAN disadvantages

- QoS: WLANs offer typically lower QoS. Lower bandwidth due to limitations in radio transmission (1-10 Mbit/s) and higher error rates due to interference
- Cost: ethernet adapter vs wireless LAN adapters

Wireless LAN disadvantages

- Proprietary solutions: slow standardization procedures lead to many proprietary solutions only working in an homogeneous environment
- Safety and security: using radio waves for data transmission might interfere with other high-tech equipment

Wireless LAN: main design goals

- Global operation: LAN equipment may be carried from one country to another and this operation should be legal (frequency regulations national and international).
- Low power: take into account that devices communicating via WLAN are typically running on battery power. Special power saving modes and power management functions.

Wireless LAN: main design goals

- Simplified spontaneous co-operation: no complicated setup routines but operate spontaneously after power.
- Easy to use: WLANs are made for simple users, they should not require complex management but rather work on a plug-and-play basis.

Wireless LAN: main design goals

- Protection of investment: a lot of money has been invested for wired LANs, WLANs should be able to interoperate with existing network (same data type and services).
- Safety and security: safe to operate. Encryption mechanism, do not allow roaming profiles for tracking people (privacy)
- Transparency for applications: existing applications should continue to work.

Basic transmission technologies for WLANs

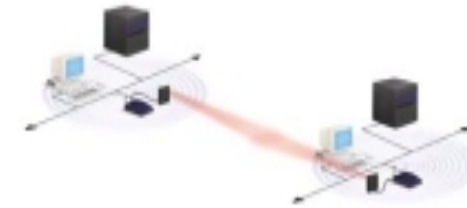
Infrared and radio

Infrared vs. radio transmission

- Infrared: based on transmission of infrared light
- Radio transmission: uses the radio transmission in the ISM free-license GHz range
- Infrared uses diffuse light reflected at walls or directed light if a line-of-sight (LOF) exists between sender and receiver

Infrared

- Infrared Technology (IR)
 - frequencies just below the visible light
 - cannot penetrate opaque objects, and low diffusion
 - line-of-sight limitates mobility
 - short range technology (indoor, PAN, LAN nets)
 - High data-rate potential



Luciano Bononi 2002

Infrared vs. radio transmission

- The main advantages of infrared:
 - sender and receiver are very cheap (integrated in almost all mobile devices available today)
 - No license is needed for infrared technology
 - Electrical devices do not interfere with infrared transmission
 - Shielding is very simple

Infrared vs. radio transmission

- The main disadvantages of infrared:
 - Low bandwidth compared with other LAN technologies
 - Limited transfer rate
 - Infrared transmission can not penetrate walls or other obstacles
 - For good transmission LOS is needed

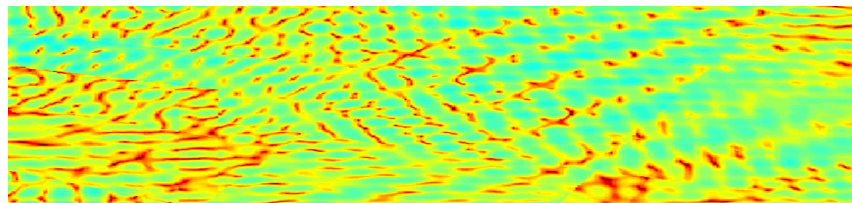
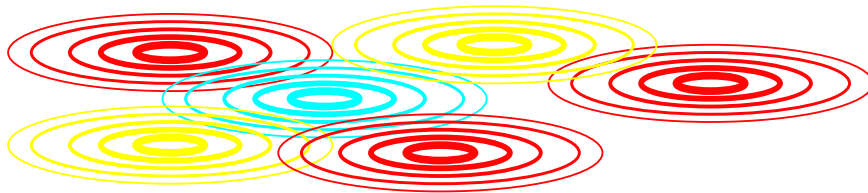
Infrared vs. radio transmission

- The main advantages of radio transmission:
 - Long-term experience for wide area networks and mobile cellular phones
 - Can cover larger area and can penetrate walls, furniture..
 - Does not need LOS
 - Current radio-based products offer higher transmission rates (10 Mbit/s)

Infrared vs. radio transmission

- The main disadvantages of radio transmission:
 - Shielding is not simple(this is also the main advantage), radio transmission can interfere with other senders or electrical devices can destroy data transmitted
 - It is only permitted in certain frequency bands
 - Very limited ranges of license-free bands are available but they are not the same in all countries

Radio transmission interference



Wireless network structures

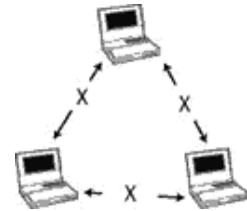
Infrastructure and ad hoc networks

Wireless network structures

- WLAN:

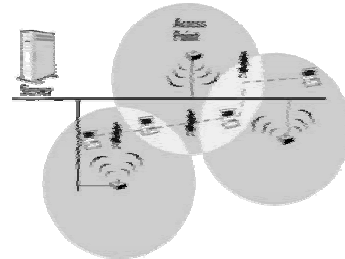
- Ad-Hoc:

- peer-to-peer (P2P) “on the fly” communication
 - the network “is” the set of computers
 - no administration, no setup, no cost?



- Infrastructure:

- Centralized control unit (Access Point, local server)
 - Roaming between cells
 - resource sharing and backbone connection



Luciano Bononi 2002

Infrastructure-based wireless network

- Communication typically takes place only between the wireless nodes and the access point. Not directly between the wireless nodes.
- Access point: acts as a bridge
- Access points with a fixed network can connect several wireless networks to form a larger network beyond the actual radio coverage

Infrastructure-based wireless network

- Design is simpler because most of the network functionality lays within the access point
- Collision may occur if medium access of the wireless node and the access point is not coordinated
- Useful for Qos guarantees such as minimum bandwidth for certain nodes

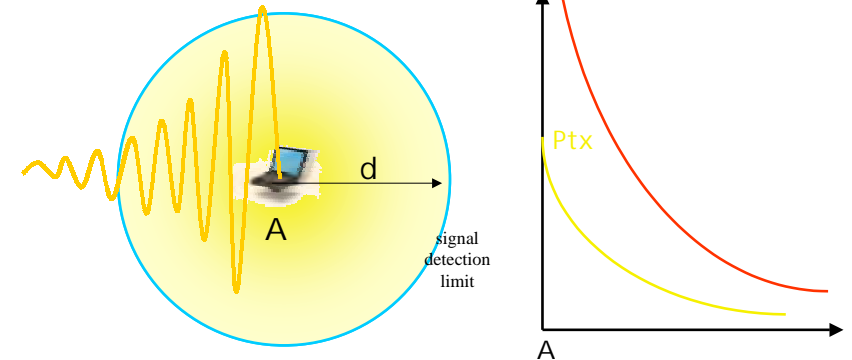
Infrastructure-based wireless network

- Lose some of the flexibility wireless networks can offer, they cannot be used for disaster relief
- Cellular phone are typically infrastructure-based networks for wide area
- Also satellite-based cellular phone have an infrastructure (the satellites)

Ad hoc wireless networks

- Do not need any infrastructure to work
- Each node can directly communicate with another node
- Nodes can only communicate if they reach each other physically (if they are within each other's radio range) or if other nodes can forward the message.

Radio transmission coverage



The range is a function of power transmission (P_{tx})
Signal strength reduces with d^2 (no obstacles)

Luciano Bononi 2002

Ad hoc wireless networks

- The complexity of each node is higher: medium access mechanisms, priority mechanisms to provide a certain QoS
- Exhibits the greatest possible flexibility (unexpected meetings, communication scenario far away from any infrastructure)

Infrastructure and ad hoc networks

- The two variant can be combined
- Networks that rely on access points and infrastructure for basic services (authentication of access), also allowing direct communication between the wireless nodes
- Ad hoc networks might only have selected nodes with the capabilities of forwarding data. Most of the node have to connect first to a special node in order to transmit data to the receiver if it is out of their range

Basic transmission technology for WLANs

IEEE 802.11
Bluetooth

IEEE 802.11

- Defines the characteristics of the physical layer (PHY) and medium access control layer (MAC) for wireless LAN
- Provide the same interface to higher layers as the others in order to maintain interoperability
- The 2.4 GHz ISM band was chosen for the standard, which is available in most countries around the world
- The original standard sets the access rate of 1 and 2 Mbps. The extension 802.11b define the access rate of 5,5 and 11 Mbps

IEEE 802.11

Network configuration

- Network configurations:
 - Ad-Hoc (peer to peer)
 - Infrastructure
 - Cell = Base Service Set (BSS): 1 Base station required
 - Extended
 - multi-cell service = Extended Service Set (ESS): Base station is connected to wired backbones, or support the bridge function to other BSS
 - requires handoff management

IEEE 802.11

Basic Service Set (BSS)

- The basic building block of WLAN is the **BSS**
- BSS represents the coverage area where two or more stations (called **STAi**) communicate through a set of functions via the wireless connection
- A synonym of BSS is Ad Hoc Network

IEEE 802.11

Extended Service Set (ESS) [1]

- A **BSS** may be part of an extended network that is built connecting multiple AdHoc networks with a named **Distribution System (DS)**
- The **DS** may consist of wired and/or wireless connections
- Inside each BSS, the station Adapter connecting the BSS to the DS is named **Access Point (AP)**.

IEEE 802.11

Extended Service Set (ESS) [2]

- The DS and BSSs allow to create a wireless network of arbitrary size and complexity: **ESS**
- To access a wired network from the wireless one, the communication has to go through a portal which provides the integration between the two communication systems
- The **portal** (that could be integrated in the functionality of an AP) forms the internetworking unit to other LANs

IEEE 802.11

Extended Service Set (ESS) [3]

IEEE 802.11: Distribution System (DS)

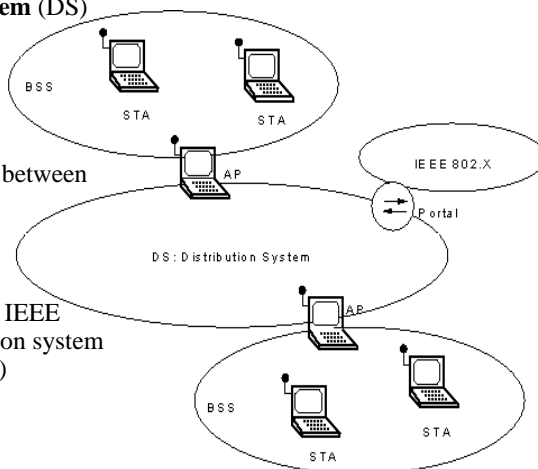
AP: Access Point

BSS: Basic Service Set

ESS: Extended Service Set

DS: Network to transmit packets between BSSs to realize ESSs.

Portal: logical entity to integrate IEEE 802.11 network and the distribution system (dedicated device or access point)

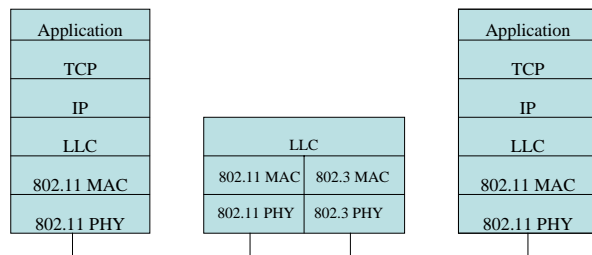


IEEE 802.11

Protocol architecture [1]

- The IEEE 802.11 fits into other standards for wired LANs
- The most common scenario is that of a IEEE 802.11 wireless LAN connected to an IEEE 802.3 Ethernet via a bridge
- Applications should not notice any differences. The higher layers (application, TCP, IP) look the same for the wireless node as for the wired node

Protocol architecture [2]



- The upper part of the data link control layer, the Logical Link Control (LCC) covers the differences of the Medium Access Control (MAC) layers needed for the different media

Protocol architecture [3]

- The standard only covers the PHY layer and the MAC layer
- The PHY is subdivided into a physical layer convergence protocol (PLCP) and the physical medium dependent sublayer (PMD)
- PLCP provides a carrier sense signal called clear channel signal (CCA) and a common PHY service access point (SAP) independent of the transmission technology
- PMD handles modulation and encoding/decoding of signals

Protocol architecture [3]

- The MAC management supports the association and re-association of a STA to an AP and roaming between different AP
- controls authentication mechanisms, encryption, synchronization of a STA with regard to an AP
- Controls power management to save battery power

Physical layer

- Three different physical layers: one layer based on infrared and two layers based on radio transmission
- All layers including the provision of the CCA signal and a SAP
- The CCA signal is needed for the MAC mechanism controlling medium access and indicates if the medium is currently idle
- The SAP give to the MAC layer a transfer rate of 1 or 2 Mbps

IEEE 802.11

MAC layer [1]

- Has to control:
 - Medium access
 - Support for roaming
 - Authentication
 - Power conservation
- The basic services provided by the MAC layer are the mandatory **asynchronous data service** and the optional **time-bounded service**
- In an AdHoc network only the asynchronous service is provided, Distributed Coordination Function (DCF)
- Both services for infrastructure-based networks, Point Coordination Function (PCF)

IEEE 802.11

MAC layer [2]

- **Distributed Coordination Function (DCF)**
 - DCF is mandatory
 - With DCF, 802.11 STAs contend for access and attempt to send frames when there is no other station transmitting. If another station is sending a frame, stations are polite and wait until the channel is free.
- **Point Coordination Function (PCF)**
 - Provide support for time-bounded delivery of data frames
 - the AP grants access to an individual STA to the medium by polling the station during the contention free period. STAs can't transmit frames unless the access point polls them first.

Bluetooth

- Bluetooth aims at so call AdHoc piconets: LAN networks with a very limited coverage without the need for an infrastructure
- One goal of Bluetooth is to provide local wireless access at very low costs
- It is a radio-based technology
- User scenarios:
 - Connection of peripheral devices
 - Support of ad hoc networking
 - Bridging of networks

Bluetooth

Physical layer [1]

- **Several limitations:**
 - Battery power: bluetooth devices will be integrated into typical mobile devices --> small, low power chips
 - Combined use for voice and data transmission --> support for multimedia data

Bluetooth

Physical layer [2]

- Bluetooth uses a frequency hopping/time-division duplex scheme
- The transmission takes place with a fast hopping rate of 1600 hops per second
- The time between two hops is called a slot
- Each slot uses a different frequency
- All devices using the same hopping sequence with the same phase form a **piconet**

Bluetooth

Physical layer [3]

- Relying on battery power it defines several low-power states for the device
- Every device which is currently not participating to a piconet is in STANDBY mode: listening for paging messages periodically
- The device listen to a subset of hop carries called **wake-up carries** (wake-up hop sequence is 32 hop in length and is cyclic)
- The subset of wake-up carriers is chosen basing on the device's identity

Bluetooth

Physical layer [4]

- The device visits every hop carrier of the wake-up carriers
- It correlates the incoming signal with the access code for the piconet derived from its own identity
- If the correlator triggers the device activates itself

Bluetooth

Physical layer [5]

- Any device can initiate a connection (master):
 - It sends a page messages if it knows the address of the receiver
 - It sends inquiry messages followed by a page message if it does not know the address of the receiver
 - The master unit sends 16 identical page messages on 16 different hop frequencies defined for the device to be paged (slave)
 - If the slave does not respond the master sends page messages on the remaining 16 wake-up hop carriers

Bluetooth

Physical layer [6]

- To save battery power a device can go into one of three low-power states:
 - PARK state: lowest duty cycle. It releases its MAC address but remains synchronized with the piconet. It occasionally listens to the traffic of the master
 - HOLD state: little higher power consumption. It does not release its MAC address
 - SNIFF state: highest power consumption. It listens at the piconet at a reduced rate. The interval for listening can be programmed (application dependent)

Bluetooth

MAC layer [1]

- In a piconet we have one device acting as a master, all other devices (up to 7) act as slaves
- The master determines the hopping sequence using its unique identifier and the phase of the sequence using its internal clock
- Within a piconet the master controls the medium access using a polling and reservation scheme

Bluetooth

MAC layer [2]

- Two services:
 - Synchronous connection-oriented link (SCO): standard telephone connections require symmetrical, circuit switching, point-to-point connections. (here the master uses a reservation scheme)
 - Asynchronous connectionless link (ACL): typical data applications require symmetrical or asymmetrical, packet switched, point-to-multipoint transfers. (here the master uses a polling scheme)

Bluetooth

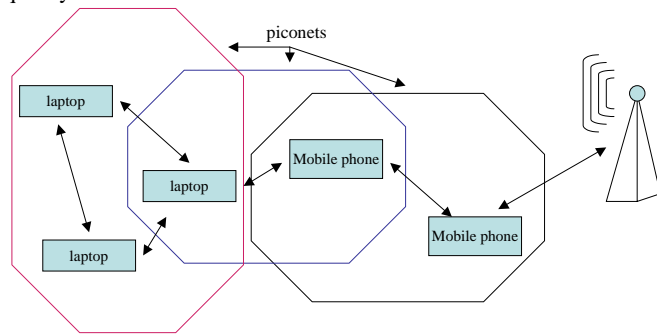
Networking [1]

- All users within one piconet share the same 1 MHz channel
- As more users join the piconet, the throughput per user drops quickly
- We can form groups of piconets called **scatternet**

Bluetooth

Networking [2]

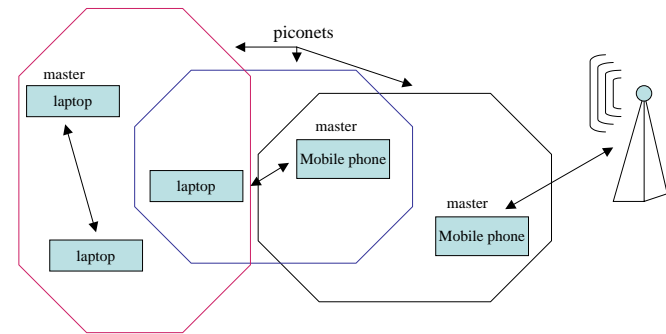
- Three piconets in which two devices participate in two different piconets
- All three piconets use different hopping sequence
- All piconets can share the total bandwidth available
- Adding more piconets leads to have more and more collision in a single piconets: a collision occurs if two or more piconets use the same carrier frequency for a slot



Bluetooth

Networking [3]

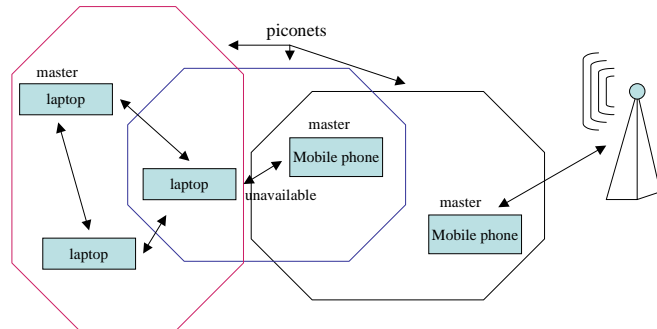
- If a device wants to participate in more than one piconet it has to synchronize to the hopping sequence of the piconet it wants to take part in
- If a device acts as slave in one piconet it simply starts to synchronize with the hopping sequence of the piconet it wants to join



Bluetooth

Networking [4]

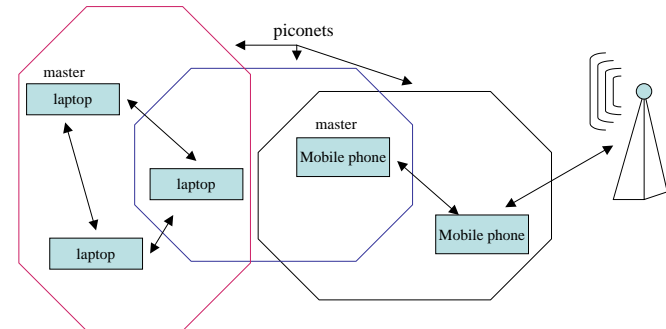
- After the synchronization it acts as a slave in this piconet and does not participate in the former any longer
- To enable synchronization it has to know the identity of the master of the piconet
- Before leaving one piconet a slave informs the current master that it will be unavailable for a certain amount of time



Bluetooth

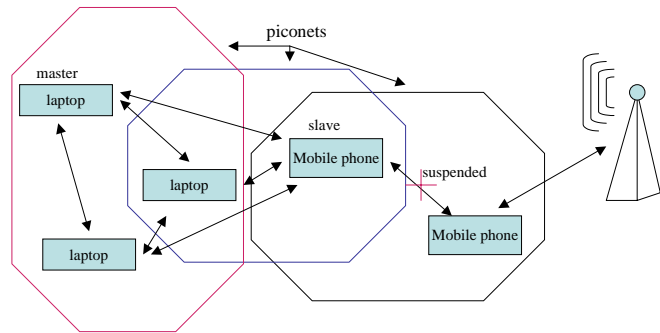
Networking [5]

- A master can also leave its piconet and act as a slave in another piconet
- A master of a piconet cannot act as master in another piconet



Networking [5]

- As soon as master leaves the piconet, all traffic within this is suspended until the master returns
- Communication between different piconets takes place through devices jumping back and forth between these nets



References

- “*Mobile Communications*”, Jochen Schiller, chapter 7 “Wireless LAN”, Addison Wensley 2000