- **802.11h (Spectrum managed 802.11a):** The 802.11a standard was primarily designed for usage in the US U-NII bands. The standardization did not consider non-US regulations such as the European requirements for power control and dynamic selection of the transmit frequency. To enable the regulatory acceptance of 5 GHz products, dynamic channel selection (DCS) and transmit power control (TPC) mechanisms (as also specified for the European HiperLAN2 standard) have been added. With this extension, 802.11a products can also be operated in Europe. These additional mechanisms try to balance the load in the 5 GHz band.
- **802.11i (Enhanced Security mechanisms):** As the original security mechanisms (WEP) proved to be too weak soon after the deployment of the first products (Borisov, 2001), this working group discusses stronger encryption and authentication mechanisms. IEEE 802.1x will play a major role in this process.

Additionally, IEEE 802.11 has several **study groups** for new and upcoming topics. The group 'Radio Resource Measurements' investigates the possibilities of 802.11 devices to provide measurements of radio resources. Solutions for even higher throughput are discussed in the 'High Throughput' study group. Both groups had their first meetings in 2002. The first study group recently became the IEEE project 802.11k 'Radio Resource Measurement Enhancements.'

7.4 HIPERLAN

In 1996, the ETSI standardized HIPERLAN 1 as a WLAN allowing for node mobility and supporting ad-hoc and infrastructure-based topologies (ETSI, 1996). (HIPERLAN stands for **high performance local area network**.) **HIPERLAN 1** was originally one out of four HIPERLANs envisaged, as ETSI decided to have different types of networks for different purposes. The key feature of all four networks is their integration of time-sensitive data transfer services. Over time, names have changed and the former HIPERLANs 2, 3, and 4 are now called HiperLAN2, HIPERACCESS, and HIPERLINK. The current focus is on HiperLAN2, a standard that comprises many elements from ETSI's **BRAN** (broadband radio access networks) and **wireless ATM** activities. Neither wireless ATM nor HIPERLAN 1 were a commercial success. However, the standardization efforts had a lot of impact on QoS supporting wireless broadband networks such as **HiperLAN2**. Before describing HiperLAN2 in more detail, the following three sections explain key features of, and the motivation behind, HIPERLAN 1, wireless ATM, and BRAN. Readers not interested in the historical background may proceed directly to section 7.4.4.

7.4.1 Historical: HIPERLAN 1

ETSI (1998b) describes HIPERLAN 1 as a wireless LAN supporting priorities and packet life time for data transfer at 23.5 Mbit/s, including forwarding mechanisms, topology discovery, user data encryption, network identification and power conservation mechanisms. HIPERLAN 1 should operate at 5.1–5.3 GHz with a range of 50 m in buildings at 1 W transmit power.

The service offered by a HIPERLAN 1 is compatible with the standard MAC services known from IEEE 802.x LANs. Addressing is based on standard 48 bit MAC addresses. A special HIPERLAN 1 identification scheme allows the concurrent operation of two or more physically overlapping HIPERLANs without mingling their communication. Confidentiality is ensured by an encryption/decryption algorithm that requires the identical keys and initialization vectors for successful decryption of a data stream encrypted by a sender.

An innovative feature of HIPERLAN 1, which many other wireless networks do not offer, is its ability to forward data packets using several relays. Relays can extend the communication on the MAC layer beyond the radio range. For power conservation, a node may set up a specific wake-up pattern. This pattern determines at what time the node is ready to receive, so that at other times, the node can turn off its receiver and save energy. These nodes are called p-savers and need so-called p-supporters that contain information about the wake-up patterns of all the p-savers they are responsible for. A p-supporter only forwards data to a p-saver at the moment the p-saver is awake. This action also requires buffering mechanisms for packets on p-supporting forwarders.

The following describes only the medium access scheme of HIPERLAN 1, a scheme that provides QoS and a powerful prioritization scheme. However, it turned out that priorities and QoS in general are not that important for standard LAN applications today. IEEE 802.11 in its standard versions does not offer priorities, the optional PCF is typically not implemented in products – yet 802.11 is very popular.

Elimination-yield non-preemptive priority multiple access (EY-NPMA) is not only a complex acronym, but also the heart of the channel access providing priorities and different access schemes. EY-NPMA divides the medium access of different competing nodes into three phases:

- **Prioritization:** Determine the highest priority of a data packet ready to be sent by competing nodes.
- **Contention:** Eliminate all but one of the contenders, if more than one sender has the highest current priority.
- **Transmission:** Finally, transmit the packet of the remaining node.

In a case where several nodes compete for the medium, all three phases are necessary (called 'channel access in **synchronized channel condition**'). If the channel is free for at least 2,000 so-called high rate bit-periods plus a dynamic extension, only the third phase, i.e. transmission, is needed (called 'channel

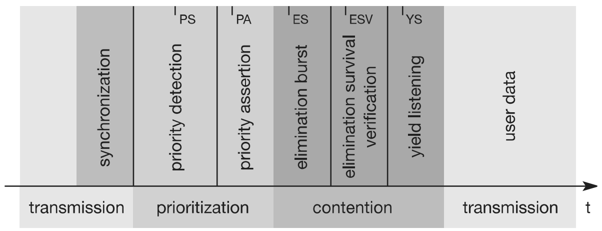


Figure 7.27
Phases of the HIPERLAN 1 EY-NPMA access scheme

access in **channel-free condition**'). The dynamic extension is randomly chosen between 0 and 3 times 200 high rate bit-periods with equal likelihood. This extension further minimizes the probability of collisions accessing a free channel if stations are synchronized on higher layers and try to access the free channel at the same time. HIPERLAN 1 also supports 'channel access in the **hidden elimination condition**' to handle the problem of hidden terminals as described in ETSI (1998b).

The contention phase is further subdivided into an **elimination phase** and a **yield phase**. The purpose of the elimination phase is to eliminate as many contending nodes as possible (but surely not all). The result of the elimination phase is a more or less constant number of remaining nodes, almost independent of the initial number of competing nodes. Finally, the yield phase completes the work of the elimination phase with the goal of only one remaining node.

Figure 7.27 gives an overview of the three main phases and some more details which will be explained in the following sections. For every node ready to send data, the access cycle starts with synchronization to the current sender. The first phase, prioritization, follows. After that, the elimination and yield part of the contention phase follow. Finally, the remaining node can transmit its data. Every phase has a certain duration which is measured in numbers of slots and is determined by the variables I_{PS}, I_{PA}, I_{ES}, I_{ESV}, and I_{YS}.

7.4.1.1 Prioritization phase

HIPERLAN 1 offers five different priorities for data packets ready to be sent. After one node has finished sending, many other nodes can compete for the right to send. The first objective of the prioritization phase is to make sure that no node with a lower priority gains access to the medium while packets with higher priority are waiting at other nodes. This mechanism always grants nodes with higher priority access to the medium, no matter how high the load on lower priorities.

In the first step of the prioritization phase, the priority detection, time is divided into five slots, slot 0 (highest priority) to slot 4 (lowest priority). Each slot has a duration of IPS = 168 high rate bit-periods. If a node has the access

layers. To cover special characteristics of wireless links and to adapt directly to different higher layer network technologies, BRAN provides a network convergence sublayer. This is the layer which can be used by a wireless ATM network, Ethernet, Firewire, or an IP network. In the case of BRAN as the RAL for WATM, the core ATM network would use services of the BRAN network convergence sublayer.

7.4.4 HiperLAN2

While HIPERLAN 1 did not succeed HiperLAN2 might have a better chance. (This is also written as HIPERLAN/2, HiperLAN/2, H/2; official name: HIPERLAN Type 2.) Standardized by ETSI (2000a) this wireless network works at 5 GHz (Europe: 5.15–5.35 GHz and 5.47–5.725 GHz license exempt bands; US: license free U-NII bands, see section 7.3.7) and offers data rates of up to 54 Mbit/s including QoS support and enhanced security features. In comparison with basic IEEE 802.11 LANs, HiperLAN2 offers more features in the mandatory parts of the standard (HiperLAN2, 2002). A comparison is given in section 7.6.

- **High-throughput transmission:** Using OFDM in the physical layer and a dynamic TDMA/TDD-based MAC protocol, HiperLAN2 not only offers up to 54 Mbit/s at the physical layer but also about 35 Mbit/s at the network layer. The overheads introduced by the layers (medium access, packet headers etc.) remains almost constant over a wide rage of user packet sizes and data rates. HiperLAN2 uses MAC frames with a constant length of 2 ms.
- **Connection-oriented:** Prior to data transmission HiperLAN2 networks establish logical connections between a sender and a receiver (e.g., mobile device and access point). Connection set-up is used to negotiate QoS parameters. All connections are time-division-multiplexed over the air interface (TDMA with TDD for separation of up/downlink). Bidirectional point-to-point as well as unidirectional point-to-multipoint connections are offered. Additionally, a broadcast channel is available to reach all mobile devices in the transmission range of an access point.
- **Quality of service support:** With the help of connections, support of QoS is much simpler. Each connection has its own set of QoS parameters (bandwidth, delay, jitter, bit error rate etc.). A more simplistic scheme using priorities only is available.
- **Dynamic frequency selection:** HiperLAN2 does not require frequency planning of cellular networks or standard IEEE 802.11 networks. All access points have built-in support which automatically selects an appropriate frequency within their coverage area. All APs listen to neighboring APs as well as to other radio sources in the environment. The best frequency is chosen depending on the current interference level and usage of radio channels.
- **Security support:** Authentication as well as encryption are supported by HiperLAN2. Both, mobile terminal and access point can authenticate each other. This ensures authorized access to the network as well as a valid network operator. However, additional functions (directory services, key

exchange schemes etc.) are needed to support authentication. All user traffic can be encrypted using DES, Triple-DES, or AES to protect against eavesdropping or man-in-the-middle attacks.

- **Mobility support:** Mobile terminals can move around while transmission always takes place between the terminal and the access point with the best radio signal. Handover between access points is performed automatically. If enough resources are available, all connections including their QoS parameters will be supported by a new access point after handover. However, some data packets may be lost during handover.
- **Application and network independence:** HiperLAN2 was not designed with a certain group of applications or networks in mind. Access points can connect to LANs running ethernet as well as IEEE 1394 (Firewire) systems used to connect home audio/video devices. Interoperation with 3G networks is also supported, so not only best effort data is supported but also the wireless connection of, e.g., a digital camera with a TV set for live streaming of video data.
- **Power save:** Mobile terminals can negotiate certain wake-up patterns to save power. Depending on the sleep periods either short latency requirements or low power requirements can be supported.

The following sections show the reference model of HiperLAN2 and illustrate some more features.

7.4.4.1 Reference model and configurations

Figure 7.31 shows the standard architecture of an infrastructure-based HiperLAN2 network. In the example, two **access points** (AP) are attached to a core network. Core networks might be Ethernet LANs, Firewire (IEEE 1394) connections

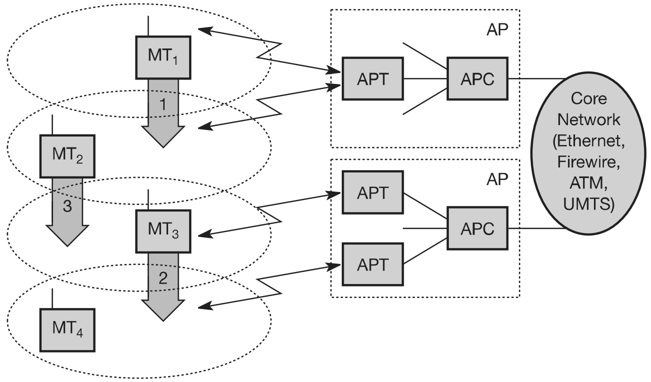


Figure 7.31
HiperLAN2 basic structure and handover scenarios

WLAN solutions, besides QoS, is the interworking of HiperLAN2 security and accounting mechanisms with the mechanisms of, e.g., UMTS. A more detailed comparison of the IEEE 802.11a WLAN approach and HiperLAN2 is given at the end of this chapter.

7.5 Bluetooth

Compared to the WLAN technologies presented in sections 7.3 and 7.4, the Bluetooth technology discussed here aims at so-called **ad-hoc piconets**, which are local area networks with a very limited coverage and without the need for an infrastructure. This is a different type of network is needed to connect different small devices in close proximity (about 10 m) without expensive wiring or the need for a wireless infrastructure (Bisdikian, 1998). The envisaged gross data rate is 1 Mbit/s, asynchronous (data) and synchronous (voice) services should be available. The necessary transceiver components should be cheap – the goal is about €5 per device. (In 2002, separate adapters are still at €50, however, the additional cost of the devices integrated in, e.g., PDAs, almost reached the target.) Many of today's devices offer an infra red data association (IrDA) interface with transmission rates of, e.g., 115 kbit/s or 4 Mbit/s. There are various problems with IrDA: its very limited range (typically 2 m for built-in interfaces), the need for a line-of-sight between the interfaces, and, it is usually limited to two participants, i.e., only point-to-point connections are supported. IrDA has no internet working functions, has no media access, or any other enhanced communication mechanisms. The big advantage of IrDA is its low cost, and it can be found in almost any mobile device (laptops, PDAs, mobile phones).

The **history** of Bluetooth starts in the tenth century, when Harald Gormsen, King of Denmark (son of Gorm), erected a rune stone in Jelling, Denmark, in memory of his parents. The stone has three sides with elaborate carvings. One side shows a picture of Christ, as Harald did not only unite Norway and Denmark, but also brought Christianity to Scandinavia. Harald had the common epithet of 'Blåtand', meaning that he had a rather dark complexion (not a blue tooth).

It took a thousand years before the Swedish IT-company Ericsson initiated some studies in 1994 around a so-called multi-communicator link (Haartsen, 1998). The project was renamed (because a friend of the designers liked the Vikings) and Bluetooth was born. In spring 1998 five companies (Ericsson, Intel, IBM, Nokia, Toshiba) founded the Bluetooth consortium with the goal of developing a single-chip, low-cost, radio-based wireless network technology. Many other companies and research institutions joined the special interest group around Bluetooth (2002), whose goal was the development of mobile phones, laptops, notebooks, headsets etc. including Bluetooth technology, by the end of 1999. In 1999, Ericsson erected a rune stone in Lund, Sweden, in memory of Harald Gormsen, called Blåtand, who gave his epithet for this new wireless communication technology. This new carving shows a man holding a laptop and a cellular phone, a picture which is quite often cited (of course there are no such things visible on the original stone, that's just a nice story!)

In 2001, the first products hit the mass market, and many mobile phones, laptops, PDAs, video cameras etc. are equipped with Bluetooth technology today.

At the same time the Bluetooth development started, a study group within IEEE 802.11 discussed **wireless personal area networks (WPAN)** under the following five criteria:

- **Market potential:** How many applications, devices, vendors, customers are available for a certain technology?
- **Compatibility:** Compatibility with IEEE 802.
- **Distinct identity:** Originally, the study group did not want to establish a second 802.11 standard. However, topics such as, low cost, low power, or small form factor are not addressed in the 802.11 standard.
- **Technical feasibility:** Prototypes are necessary for further discussion, so the study group would not rely on paper work.
- **Economic feasibility:** Everything developed within this group should be cheaper than other solutions and allow for high-volume production.

Obviously, Bluetooth fulfills these criteria so the WPAN group cooperated with the Bluetooth consortium. IEEE founded its own group for WPANs, IEEE 802.15, in March 1999. This group should develop standards for wireless communications within a **personal operating space** (POS, IEEE, 2002c). A POS has been defined as a radius of 10 m around a person in which the person or devices of this person communicate with other devices. Section 7.5.10 gives an overview of 802.15 activities and their relation to Bluetooth.

7.5.1 User scenarios

Many different user scenarios can be imagined for wireless piconets or WPANs:

- **Connection of peripheral devices:** Today, most devices are connected to a desktop computer via wires (e.g., keyboard, mouse, joystick, headset, speakers). This type of connection has several disadvantages: each device has its own type of cable, different plugs are needed, wires block office space. In a wireless network, no wires are needed for data transmission. However, batteries now have to replace the power supply, as the wires not only transfer data but also supply the peripheral devices with power.
- **Support of ad-hoc networking:** Imagine several people coming together, discussing issues, exchanging data (schedules, sales figures etc.). For instance, students might join a lecture, with the teacher distributing data to their personal digital assistants (PDAs). Wireless networks can support this type of interaction; small devices might not have WLAN adapters following the IEEE 802.11 standard, but cheaper Bluetooth chips built in.

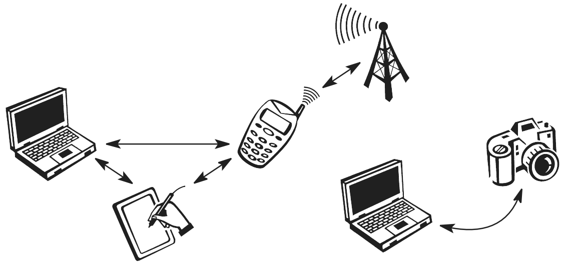


Figure 7.40
Example configurations with a Bluetooth-based piconet

- **Bridging of networks:** Using wireless piconets, a mobile phone can be connected to a PDA or laptop in a simple way. Mobile phones will not have full WLAN adapters built in, but could have a Bluetooth chip. The mobile phone can then act as a bridge between the local piconet and, e.g., the global GSM network (see Figure 7.40). For instance, on arrival at an airport, a person's mobile phone could receive e-mail via GSM and forward it to the laptop which is still in a suitcase. Via a piconet, a fileserver could update local information stored on a laptop or PDA while the person is walking into the office.

When comparing Bluetooth with other WLAN technology we have to keep in mind that one of its goals was to provide local wireless access at very low cost. From a technical point of view, WLAN technologies like those above could also be used, however, WLAN adapters, e.g., for IEEE 802.11, have been designed for higher bandwidth and larger range and are more expensive and consume a lot more power.

7.5.2 Architecture

Like IEEE 802.11b, Bluetooth operates in the 2.4 GHz ISM band. However, MAC, physical layer and the offered services are completely different. After presenting the overall architecture of Bluetooth and its specialty, the piconets, the following sections explain all protocol layers and components in more detail.

7.5.2.1 Networking

To understand the networking of Bluetooth devices a quick introduction to its key features is necessary. Bluetooth operates on 79 channels in the 2.4 GHz band with 1 MHz carrier spacing. Each device performs frequency hopping with 1,600 hops/s in a pseudo random fashion. Bluetooth applies FHSS for interference mitigation (and FH-CDMA for separation of networks). More about Bluetooth's radio layer in section 7.5.3.

A very important term in the context of Bluetooth is a **piconet**. A piconet is a collection of Bluetooth devices which are synchronized to the same hopping sequence. Figure 7.41 shows a collection of devices with different roles. One device in the piconet can act as **master** (M), all other devices connected to the

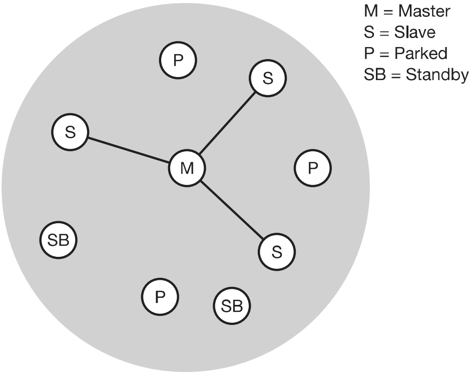


Figure 7.41
Simple Bluetooth piconet

master must act as **slaves** (S). The master determines the hopping pattern in the piconet and the slaves have to synchronize to this pattern. Each piconet has a unique hopping pattern. If a device wants to participate it has to synchronize to this. Two additional types of devices are shown: parked devices (P) can not actively participate in the piconet (i.e., they do not have a connection), but are known and can be reactivated within some milliseconds (see section 7.5.5). Devices in stand-by (SB) do not participate in the piconet. Each piconet has exactly one master and up to seven simultaneous slaves. More than 200 devices can be parked. The reason for the upper limit of eight active devices, is the 3-bit address used in Bluetooth. If a parked device wants to communicate and there are already seven active slaves, one slave has to switch to park mode to allow the parked device to switch to active mode.

Figure 7.42 gives an overview of the formation of a piconet. As all active devices have to use the same hopping sequence they must be synchronized. The first step involves a master sending its clock and device ID. All Bluetooth devices have the same networking capabilities, i.e., they can be master or slave. There is no distinction between terminals and base stations, any two or more devices can form a piconet. The unit establishing the piconet automatically becomes the master, all other devices will be slaves. The hopping pattern is determined by the device ID, a 48-bit worldwide unique identifier. The phase in the hopping pattern is determined by the master's clock. After adjusting the internal clock according to the master a device may participate in the piconet. All active devices are assigned a 3-bit **active member address** (AMA). All parked devices use an 8-bit **parked member address** (PMA). Devices in stand-by do not need an address.

All users within one piconet have the same hopping sequence and share the same 1 MHz channel. As more users join the piconet, the throughput per user drops quickly (a single piconet offers less than 1 Mbit/s gross data rate). (Only having one piconet available within the 80 MHz in total is not very efficient.) This led to the idea of forming groups of piconets called **scatternet** (see Figure 7.43). Only those units that really must exchange data share the same piconet, so that many piconets with overlapping coverage can exist simultaneously.

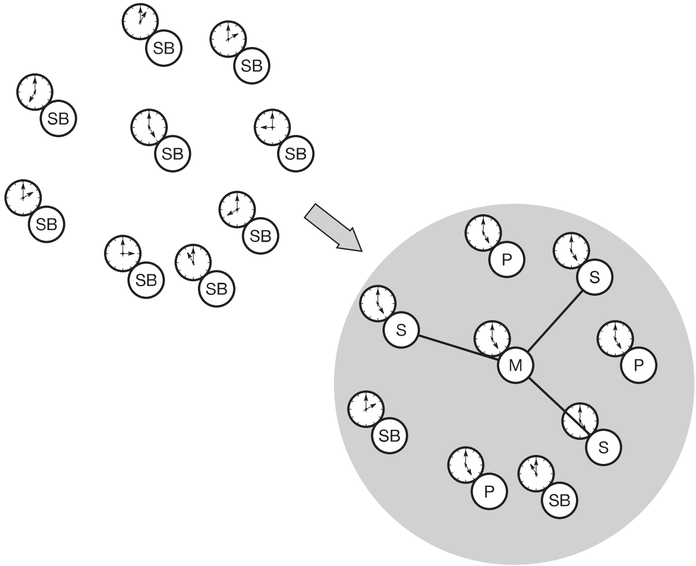


Figure 7.42
Forming a Bluetooth piconet

In the example, the scatternet consists of two piconets, in which one device participates in two different piconets. Both piconets use a different hopping sequence, always determined by the master of the piconet. Bluetooth applies **FH-CDMA** for separation of piconets. In an average sense, all piconets can share the total of 80 MHz bandwidth available. Adding more piconets leads to a graceful performance degradation of a single piconet because more and more collisions may occur. A collision occurs if two or more piconets use the same carrier frequency at the same time. This will probably happen as the hopping sequences are not coordinated.

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. After synchronization, it acts as a slave in this piconet and no longer participates in its former piconet. To enable synchronization, a slave has to know the identity of the master that determines the hopping sequence of a piconet. Before leaving one piconet, a slave informs the current master that it will be unavailable for a certain amount of time. The remaining devices in the piconet continue to communicate as usual.

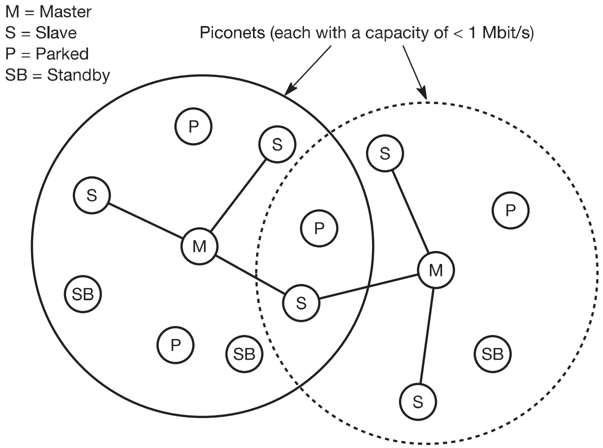


Figure 7.43
Bluetooth scatternet

A master can also leave its piconet and act as a slave in another piconet. It is clearly not possible for a master of one piconet to act as the master of another piconet as this would lead to identical behavior (both would have the same hopping sequence, which is determined by the master per definition). As soon as a master leaves a piconet, all traffic within this piconet is suspended until the master returns.

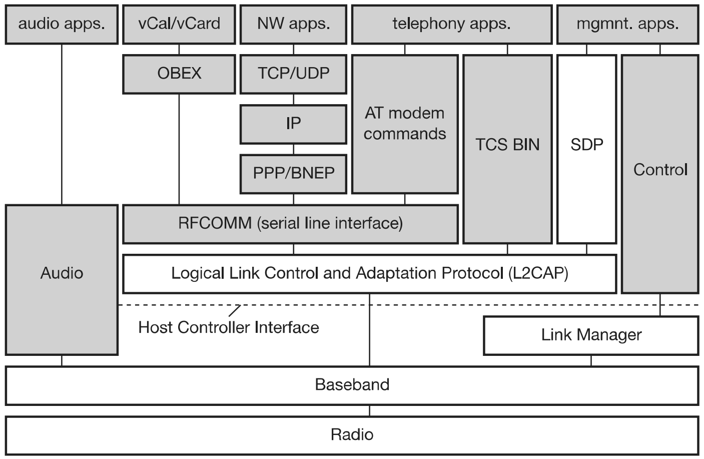
Communication between different piconets takes place by devices jumping back and forth between theses nets. If this is done periodically, for instance, isochronous data streams can be forwarded from one piconet to another. However, scatternets are not yet supported by all devices.

7.5.2.2 Protocol stack

As Figure 7.44 shows, the Bluetooth specification already comprises many protocols and components. Starting as a simple idea, it now covers over 2,000 pages dealing with not only the Bluetooth protocols but many adaptation functions and enhancements. The Bluetooth protocol stack can be divided into a **core specification** (Bluetooth, 2001a), which describes the protocols from physical layer to the data link control together with management functions, and **profile specifications** (Bluetooth, 2001b). The latter describes many protocols and functions needed to adapt the wireless Bluetooth technology to legacy and new applications (see section 7.5.9).

The **core protocols** of Bluetooth comprise the following elements:

- **Radio:** Specification of the air interface, i.e., frequencies, modulation, and transmit power (see section 7.5.3).
- **Baseband:** Description of basic connection establishment, packet formats, timing, and basic QoS parameters (see section 7.5.4).



AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol
SDP: service discovery protocol
RFCOMM: radio frequency comm.

Figure 7.44
Bluetooth protocol stack

- **Link manager protocol:** Link set-up and management between devices including security functions and parameter negotiation (see section 7.5.5).
- **Logical link control and adaptation protocol (L2CAP):** Adaptation of higher layers to the baseband (connectionless and connection-oriented services, see section 7.5.6).
- **Service discovery protocol:** Device discovery in close proximity plus querying of service characteristics (see section 7.5.8).

On top of L2CAP is the **cable replacement protocol** RFCOMM that emulates a serial line interface following the EIA-232 (formerly RS-232) standards. This allows for a simple replacement of serial line cables and enables many legacy applications and protocols to run over Bluetooth. RFCOMM supports multiple serial ports over a single physical channel. The **telephony control protocol specification – binary** (TCS BIN) describes a bit-oriented protocol that defines call control signaling for the establishment of voice and data calls between Bluetooth devices. It also describes mobility and group management functions.

The **host controller interface** (HCI) between the baseband and L2CAP provides a command interface to the baseband controller and link manager, and access to the hardware status and control registers. The HCI can be seen as the hardware/software boundary.