1.6 HIPERLAN

HIPERLAN is a European (ETSI) standardization initiative for a High Performance wireless Local Area Network. Radio waves are used instead of a cable as a transmission medium to connect stations. Either, the radio transceiver is mounted to the movable stationas an add-on and no base station has to be installed separately, or a base station is needed in addition per room. The stations may be moved during operation-pauses or even become mobile. The maximum data rate for the user depends on the distance of the communicating stations. With short distances (<50 m) and asynchronous transmission a data rate of 20 Mbit/s is achieved, with up to 800 m distance a data rate of 1 Mbit/s are provided.

1.6.1 HiperLAN features:

- Range 50 m
- Slow mobility (1.4 m/s)
- Supports asynchronous and synchronous traffic
- Bit rate - 23.2 Mbit/s
- Description- wireless Ethernet
- Frequency range- 5 GHz

1.6.2 HIPERLAN 1

HIPERLAN1 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. Overtime, names havechanged and the former HIPERLANs 2, 3, and 4 are now called HiperLAN2, HIPERACCESS, and HIPERLINK. The current focus is onHiperLAN2, a standard that comprises many elements from ETSI‘s BRAN (broadband radio access networks) and wireless ATM activities.

ETSI 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 Wtransmit power. The service offered by a HIPERLAN 1 is compatible with the standardMAC services known from IEEE 802.x LANs. Addressing is based on standard 48 bit MAC addresses. Confidentiality is ensured by an encryption/decryption algorithm thatrequires the identical keys and initialization vectors for successful decryption of a datastream encrypted by a sender. An innovative feature of HIPERLAN 1, which many otherwireless 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. Thispattern 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.

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 bycompeting nodes.
- Contention: Eliminate all but one of the contenders, if more than one sender has thehighest current priority.
- Transmission: Finally, transmit the packet of the remaining node.

The dynamic extension is randomly chosen between 0 and 3 times 200 high bit rate. 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.

The contention phase is further subdivided into an elimination phase and a yield phase. The elimination phase is to eliminate as many contending nodes as possible. 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.

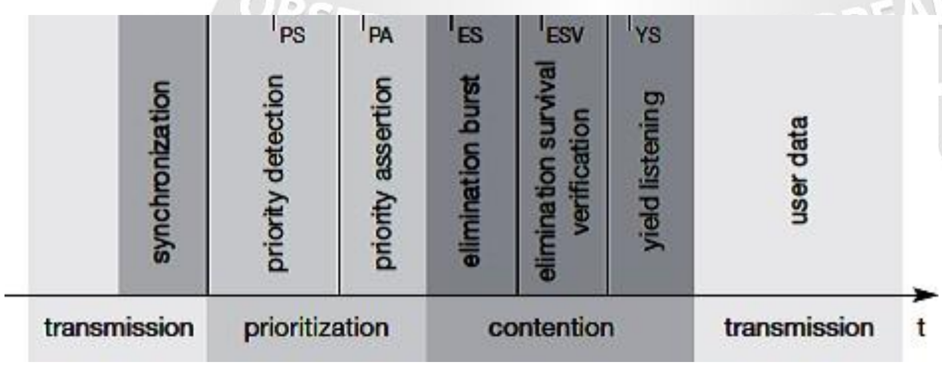

Fig. 1.17 Phases of HIPERLAN1

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

The above figure 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 hasa certain duration which is measured in numbers of slots and is determined by the variablesIPS, IPA, IES, IESV, and IYS.

1.6.3 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 gainsaccess 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 priority p, it has to listen into the medium for p slots (priority detection).
Consider for example, that there are three nodes with data ready to be sent, the packets of node 1 and node 2 having the priority 2, the packet of node3 having the priority 4. Then nodes 1, 2 and 3 listen into the medium and sense
slots 0 and 1 are idle. Nodes 1 and 2 both send a burst in slot 2 as priority assertion.
Node 3 stops its attempt to transmit its packet. In this example, the prioritization phase has taken three slots.

After this first phase at least one of the contending nodes will survive, the surviving nodes being all nodes with the highest priority of this cycle.

1.6.4 Elimination Phase

Several nodes may now enter the elimination phase. Again, time is divided into slots, usingthe elimination slot interval IES = 212 high rate bit periods. The length of an individual elimination burst is 0 to 12 slot intervals long, the probability of bursting within a slot is
0.5. The probability PE(n) of an elimination burst to be in elimination slot intervals long is given by:

- $PE(n) = 0.5n+1$ for $0 \leq n < 12$
- $PE(n) = 0.512$ for $n = 12$

The elimination phase now resolves contention by means of elimination bursting and elimination survival verification. Each contending node sends an elimination burst with length n as determined via the probabilities and then listens to the channel during the survival verification interval IESV = 256 high rate bit periods. The burst sent is the same as for the priority assertion.
A contending node survives this elimination phase if, and only if, it senses the channel is idle during its survival verification period. Otherwise, the node is eliminated and stops its attempt to send data during this transmission cycle.

1.6.5 Yield phase
During the yield phase, the remaining nodes only listen into the medium without sending any additional bursts. Again, time is divided into slots, this time called yield slots with a duration of IYS = 168 high rate bit-periods. The length of an individual yield listening period can be 0 to 9 slots with equal likelihood. The probability PY(n)for a yield listeningperiod to be n slots long is 0.1 for all n, $0 \leq n \leq 9$.

Each node now listens for its yield listening period. If it senses the channel is idle during the whole period, it has survived the yield listening. At least one node will survive this phase and can start to transmit data. This is what the other nodes with longer yield listeningperiod can sense. It is important to note that at this point there can still be more than one surviving node so a collision is still possible.

1.6.6 Transmission phase
A node that has survived the prioritization and contention phase can now send its data, called a low bit-rate high bit-rate HIPERLAN 1 CAC protocol data unit(LBR-HBR HCPDU). This PDU can either be multicast or unicast. In case of a unicast transmission, the sender expects to receive an immediate acknowledgement from the destination, called an acknowledgement HCPDU (AK-HCPDU),which is an LBR HCPDU containing onlyan LBR part.

1.7 WATM(WIRELESS ATM)
Wireless ATM also called as wireless, mobile ATM, wmATM. It describes a transmission technology to specify a complete communication system. IEEE WLAN originates from thedata communication community whereas WLAN arise from the tele communication industry.

1.7.1 Development of WATM
- The wireless terminals are integrated into an ATM network for supporting differenttypes of traffic streams as ATM does in fixed network.

- ATM network will scale well from LANs to WANs & mobility is needed in localand wide applications.
- WATM offers QOS for adequate support of multimedia data streams.
- For telecommunication service providers, merging of mobile wireless communication & ATM technology will leads to wireless ATM.

1.7.2 Standardization of WATM

WATM is a specific broadband wireless solution which is significantly meets the architectural and performance goals needed. WATM has been driven by the wide acceptance of ATM switching technology as a basis for broadband networks which support integrated services with QoS control. ATM signaling protocol (e.g.,Q2931) for connection establishment and QoS control also provide a suitable basis for mobility extensions such as handover and location management.

1.7.3 Extension of ATM

The following more general extensions of the ATM system also need to be considered fora mobile ATM:

- **Location management:** Similar to other cellular networks, WATM networks must be able to locate a wireless terminal or a mobile user, i.e., to find the current access point of the terminal to the network.
- **Mobile routing:** Even if the location of a terminal is known to the system, it still has to route the traffic through the network to the access point currently responsible for the wireless terminal. Each time a user moves to anew access point, the system must reroute traffic.
- **Handover signaling:** The network must provide mechanisms which search for new access points, set up new connections between intermediate systems and signal the actual change of the access point.
- **QoS and traffic control:** In contrast to wireless networks offering only best effort traffic,and to cellular networks offering only a few different types of traffic, WATM should be able to offer many QoS parameters. To maintain these parameters, all actions such as rerouting, handover etc. have to be controlled. The network must pay attention to the incoming traffic (and check if it conforms to some traffic contract) in a similar way to today‘s ATM (policing).
- **Network management:** All extensions of protocols or other mechanisms also require an extension of the management functions to control the network.

1.7.4 Frame Format for WATM

Wireless header	ATM header (5 bytes)	ATM payload (48 bytes)	Wireless trailer

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

The ATM cells were operating on reliable optical channels that do not need acknowledgement. When the same packet format is used in a wireless environment, another additional 16 bytes for the PLCP header is used and a few more for a wireless MAC layer that makes the overhead so large that a 48 – byte payload length makes the transmission inefficient.

1.7.6 WIRELESS ATM ARCHITECTURE

Wireless ATM architecture is obtained by incorporating new wireless protocols at the access level and extensions into the standard ATM protocol stack which is shown in Figure. At the access level, new protocols are needed for:

• Physical layer radio channels between the mobile terminals and base stations,

• Medium access control (MAC) to arbitrate the shared use of the radio channels by the mobile terminals,

• Data/logical link control (DLC/LLC) to detect and/or correct the radio channel errorsand maintain end-to-end QoS.

• Wireless control to support such functions as radio resource management at the physical,MAC and DLC layers, as well as mobility management.

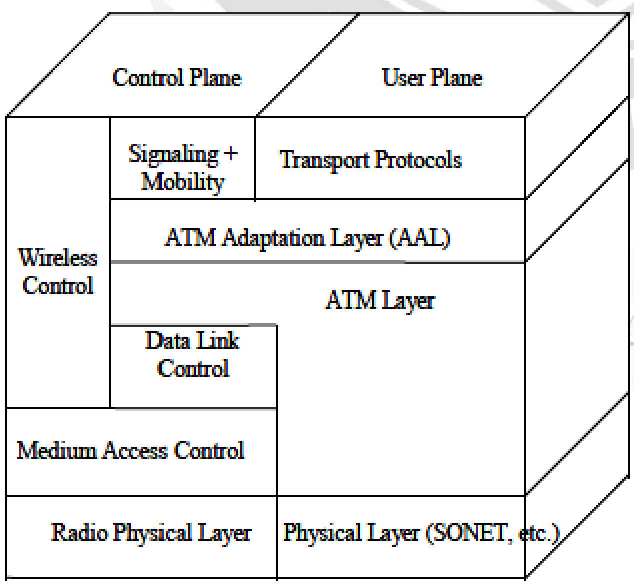

Fig. 1.18 Wireless ATM Architecture

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

WATM protocol architecture is based on integration of radio access and mobility features capabilities within the standard ATM protocol stack. A WATM system may be partitionedinto two relatively independent parts: a mobile ATM infrastructure and a radio access segment, each of which can be designed and specified separately. This facilitates standardization by multiple organizations and allows for gradual evolution of radio access technologies without having to modify the core mobile ATM network specification.

The WATM radio access structure consists of Radio Physical Layer (PHY),Medium Access Control (MAC), Data Link Control (DLC) and wireless control. The WATM DLC layer interfaces each ATM virtual circuit (both service data and signaling) with the ATM network layer above. An additional wireless control interface is provided within the controlplane to deal with radio link specific control functions such as initial registration, resource allocation, and power control.

1.7.7 Handover

As a mobile terminal moves from one place to another, it becomes necessary to hand overits ongoing connections from the old radio port to the new one. The decision to change the radio port is made either by the mobile terminal or the base station based on signal strength measurements.

There are three handover scenarios. In the first scenario, the old and new radio ports belong to the same base station. This case can be handled completely by the radio-level protocols. In the second scenario, the target radio port belongs to different base stations, with the old and new base stations connected to (and supported by) the same ATM switch.

This latter switch controls the rerouting of the connections from the old to the new base stations, and is called the crossover switch. In the third case, each of the two base stations is connected to its own access switch. An intermediate switch acts as the crossover switch for rerouting connections from the old to the new access switch.

The discovery and selection of the crossover switch is an important issue in handover. Unless handover occurs within the same base station, ATM-level protocols are said to berequired for discovery of crossover switch, path rerouting, etc.

There are two types of handovers:

1. Soft hand over
2. Hard hand over

In soft handover, the mobile terminal connections are passed to the new base station without interrupting communication with the old base station.

In hard handover, the connections are interrupted at the old base station and reestablished at the new base station. Only hard handover is supported in the current WATM specification.

1.7.8 Location Management

Location management is required to maintain the association between the mobile's physical location at a foreign switch and its permanent address at the home switch. To achieve this, a mobile terminal must register with the base station of every new service area it may enter. The main purpose of location management in wireless ATM networks is to allow a mobile terminal to use its permanent address in connection set-up messages regardless of its attachment to the network. In addition, location management incorporates features for access control, privacy, accounting and inter-provider roaming.

The functions of location management are handled by mobility-enhanced switches, location servers, authentication servers, and mobile terminals. The location server is a database of associations between the permanent and temporary addresses of mobile terminals. The temporary address identifies the location of the mobile terminal away from its permanent home address (switch). This database is queried and updated according to specific protocols.

On the other hand, the authentication server is a database containing secure information relating to the privacy and identification of each mobile terminal.
Location management is required in local and wide area WATM networks. Local location management enables any host connected to a switch to establish a virtual circuit with any mobile terminal moving between the base stations within a local network. Wide area location management permits mobile terminals attached to one local network to establish connections with hosts (or other mobile terminals) attached to remote network groups.

1.7.9 Mobile quality of service

Quality of service (QoS) guarantees are one of the main advantages predicted for WATM networks compared to, e.g., mobile IP working over packet radio networks.
While the internet protocol IP does not guarantee QoS, ATM networks do (at the cost of higher complexity). WATM networks should provide mobile

QoS (M-QoS). M-QoS is composed of three different parts:

- Wired QoS: The infrastructure network needed for WATM has the same QoS properties as any wired ATM network. Typical traditional QoS parameters are link delay, cell delay variation, bandwidth, cell error rate etc.
- Wireless QoS: The QoS properties of the wireless part of a WATM network differ from those of the wired part. Again, link delay and error rate can be specified, but

now error rate is typically some order of magnitude that is higher than, e.g., fiber optics. Channel reservation and multiplexing mechanisms at the air interface strongly influence cell delay variation.

- Handover QoS: A new set of QoS parameters are introduced by handover. For example, handover blocking due to limited resources at target access points, cell loss during handover, or the speed of the whole handover procedure represent critical factors for QoS.