ETSI TR 102 010 V1.1.1 (2001-11)

Technical Report

Digital Enhanced Cordless Telecommunications (DECT); DECT access to IP networks

Reference

DTR/DECT-A0174

Keywords

Data, DECT, Fax, IP, LAN, Modem, network,
PABX, Profile, WAN

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Project Digital Enhanced Cordless Telecommunications (DECT).

TRs are informative documents resulting from ETSI studies. A TR may be used to publish material which is either of an informative nature, relating to the use or the application of ENs or TSs, or which is immature and not yet suitable for formal adoption as an EN or an TS.

1 Scope

The present document describes the scenarios, services and related features for a wireless access to IP-networks using the Digital Enhanced Cordless Telecommunications (DECT) system. The reference configuration, network architecture and the network functional entities are described. Specific issues are further investigated.

The present document also identifies possible further standardization areas.

2 References

For the purposes of this Technical Report (TR), the following references apply:

[1] ETSI EN 300 175-1: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 1: Overview".

[2] ETSI EN 300 175-2: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 2: Physical Layer (PHL)".

[3] ETSI EN 300 175-3: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 3: Medium Access Control (MAC) layer".

[4] ETSI EN 300 175-4: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 4: Data Link Control (DLC) layer".

[5] ETSI EN 300 175-5: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 5: Network (NWK) layer".

[6] ETSI EN 300 175-6: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 6: Identities and addressing".

[7] ETSI EN 300 175-7: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security features".

[8] ETSI EN 300 175-8: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 8: Speech coding and transmission".

[9] ETSI EN 300 444: "Digital Enhanced Cordless Telecommunications (DECT); Generic Access Profile (GAP)".

[10] ETSI EN 301 649: "Digital Enhanced Cordless Telecommunications (DECT); DECT Packet Radio Services (DPRS)".

[11] IETF RFC2002: "IP Mobility Support".

[12] IETF RFC2543: "SIP: Session Initiation Protocol".

[13] IETF RFC1144: "Compressing TCP/IP Headers for Low-Speed Serial Links".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following definitions apply:

authentication: process whereby a DECT subscriber is positively verified to be a legitimate user of a particular Fixed Part (FP) and vice-versa

Fixed Part (FP): physical grouping that contains all of the elements in the DECT network between the local network and the DECT air interface

frame relay: transmission of a Service Data Unit (SDU) with frame boundaries maintained but without notification of correct or otherwise receipt of that SDU

interoperability: ability of a FP from one manufacturer and a Portable Part (PP) from another manufacturer to communicate, exclusively by means of reliance on a common protocol profile

mobile computing: use of portable computer type equipment in different locations

on-line media: availability of a wide range of copyright material, such as encyclopedias, maps, directories, timetables and newspapers, to users for access via telecommunications networks

Personal Intelligent Communicator (PIC): hand held computer, possibly with a pen based user interface, and the ability to communicate via data networks

Portable Part (PP): physical grouping that contains all elements between the user and the DECT air interface

NOTE: PP is a generic term that may describe one or several physical pieces.

roaming: movement of a PP from one FP coverage area to another FP coverage area, where the capabilities of FPs enable the PP to make or receive calls in both areas

teleservices: type of telecommunications services that provides the complete capability, including terminal equipment functions, for communication between users, according to protocols that are established by agreement

terminal mobility: ability to access a set of communications services, associated with a specific terminal, in different locations

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAA	Authentication Authorization and Accounting
ACAP	Application Configuration Access Protocol
ADPCM	Adaptive Differential Pulse Code Modulation
ARI	Access Rights Identity
BOOTP	Bootstrap Protocol
DHCP	Dynamic Host Configuration Protocol
DCL	Data Link Control
DNS	Domain Name Server
DPRS	DECT Packet Radio Service
FP	Fixed Part
FTP	File Transfer Protocol (Internet)
GAP	Generic Access Profile
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPUI	International Portable User Identity
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISUP	ISDN User Part
IWK	InterWorKing
LAN	Local Area Network
MAC	Medium Access Control
MLPS	Multi Protocol Label Switching
MTU	Maximum Transfer Unit
NAI	Network Access Identifier
NSP	Network Service Provider
NTP	Normal Transmitted Power
NWK	NetWorK
PABX	Private Automatic Branch Exchange
PARK	Portable Access Rights Key

PHY	PHYsical layer
PIC	Personal Intelligent Communicator
PP	Portable Part
PPP	Point-to-Point Protocol
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RSVP	Resource Reservation Protocol
SDU	Service Data Unit
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SS7	Signalling System N°7
TCP/IP	Transmission Control Protocol/Internet Protocol
TCP/UDP	Transmission Control Protocol/User Datagram Protocol
WAN	Wide Area Network

4 Scenarios and services

4.1 IP-data transfer

In figure 1, a basic scenario is given for IP-data transfer:

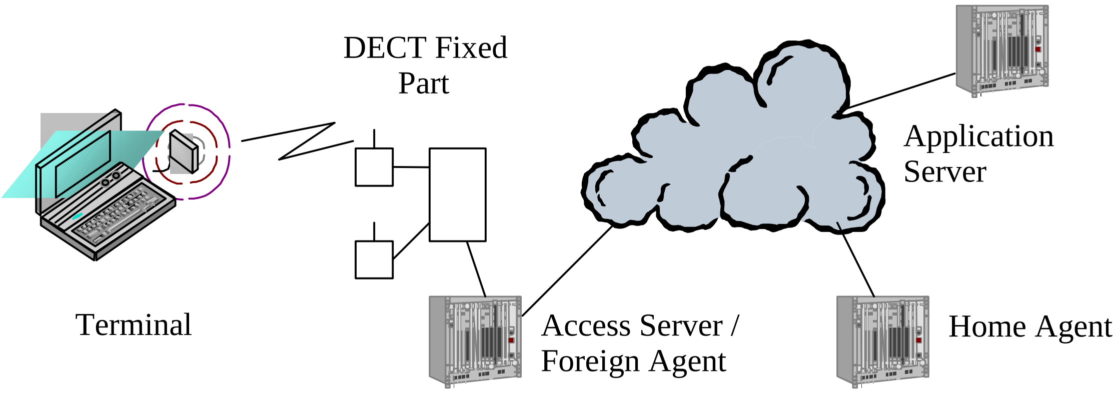

Figure 1: Basic data scenario

4.2 Voice service

In figure 2, a basic scenario is given for voice services:

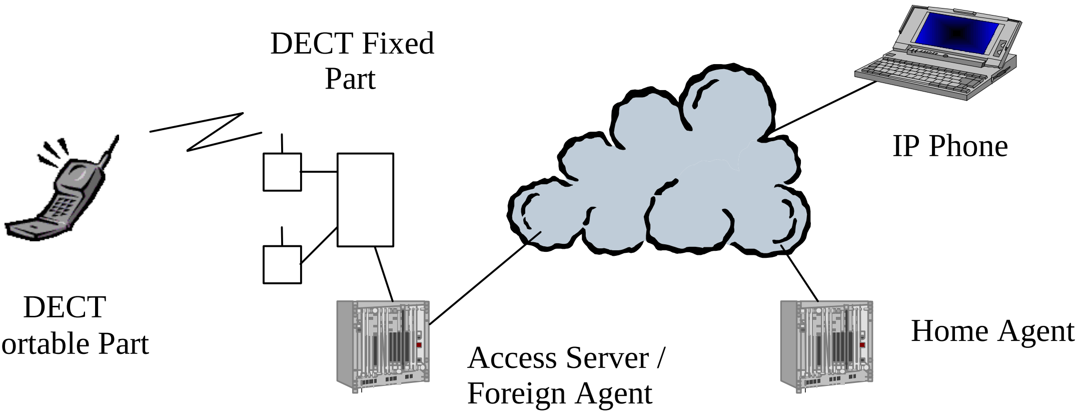

Figure 2: Basic speech scenario

4.3 Video and Multicast

Further scenarios are e.g. video transmission over IP and multicast (streaming, one way) over IP.

5 Related features

5.1 User identification

Any user should be assigned with a user identifier that will be used by roaming and mobility functions to assess his identity when visiting different access networks. The identifier serves to uniquely identify a user as well as to identify the NSP the user is associated with. Anonymous user identifiers should be possible, in order to allow access to networks that do not impose any access control mechanism or require authentication.

5.2 Network Provider Discovery

Terminals should be informed about the identity and characteristics of the providers available at any time and place, and they should be able to establish or release associations with them.

5.3 Auto-configuration

Auto-configuration means, that the terminal will automatically discover and register the parameters that it needs to use to connect to the Internet. Typical users do not configure "low-level" parameters in their terminals; they interact with "high-level" or application customization parameters, like user profiles. Applications run automatically without any configuration intervention from the users, apart from the selection of the network provider they want to connect to. This means that all the parameters needed to work are auto-configured. Auto-configuration implies that not only all IP basic parameters should be known (address, mask, gateway address, DNS server address, etc), but also information about proxy services or typical applications configuration, like the location of the nearest web proxy with transcoding capabilities, e-mail relay or the zone gatekeeper.

Full auto-configuration of a mobile station should be preceded by a security (or optional an authorization, authentication and accounting) process. Only stations being granted the access to the network should be allowed to auto-configure.

Terminals should be prepared to receive multiple responses to a request for configuration parameters. Some installations may include multiple, overlapping auto-configuration servers, either to enhance reliability and increase performance. Or servers belonging to different network providers could coexist on the same access network.

It should be guaranteed that any specific IP address will not be in use by more than one mobile station at a time. Explicit mechanisms to detect address duplications and disable incorrectly configured terminals should be included.

As each network service provider will have its own IP network configuration and set of services, the auto-configuration of the terminals should be made independently for each different network service provider.

5.4 Mobility

A Roaming service, that allows terminals to get network services when visiting "foreign networks" is required. Roaming may be loosely defined as the ability to use any one of multiple Internet service providers, while maintaining a formal customer-vendor relation with only one.

In general, all the changes due to terminal mobility should be managed either at IP or DECT-network level, and be as transparent as possible to applications. Ideally, applications should only receive notification about changes in the QoS offered by the network due to mobility issues. All other details should remain hidden inside the protocol stack – for example, the IP address should not change from the application's point of view.

Handover is supported within a DECT Fixed Part.

5.5 Location information

Location information about the positioning of terminals could be provided for location based services.

5.6 Security

End-to-end authentication and encryption may be required for some applications.

5.7 Emergency services

Support of emergency services is required for some applications.

6 Reference configuration

In figure 3 is shown the reference configuration for the scope of present document:

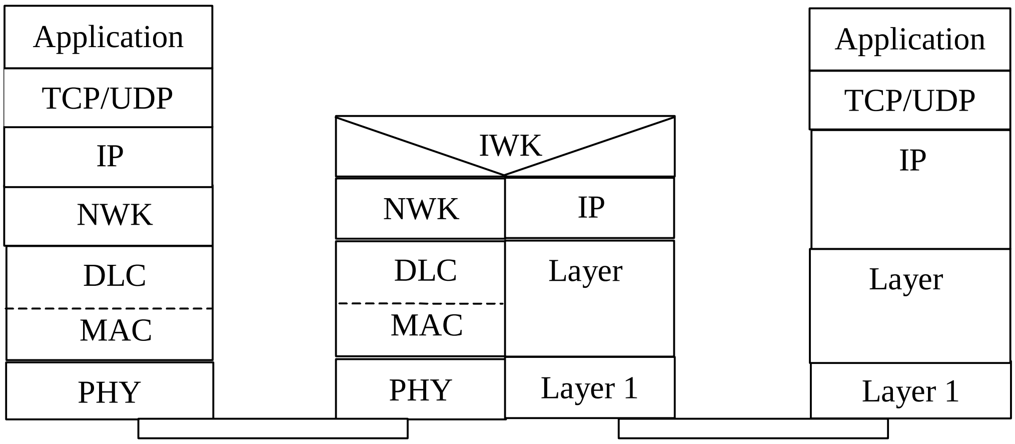

Figure 3: Reference configuration

7 Network Architecture

In figure 4 is shown the network reference architecture for the scope of the present document:

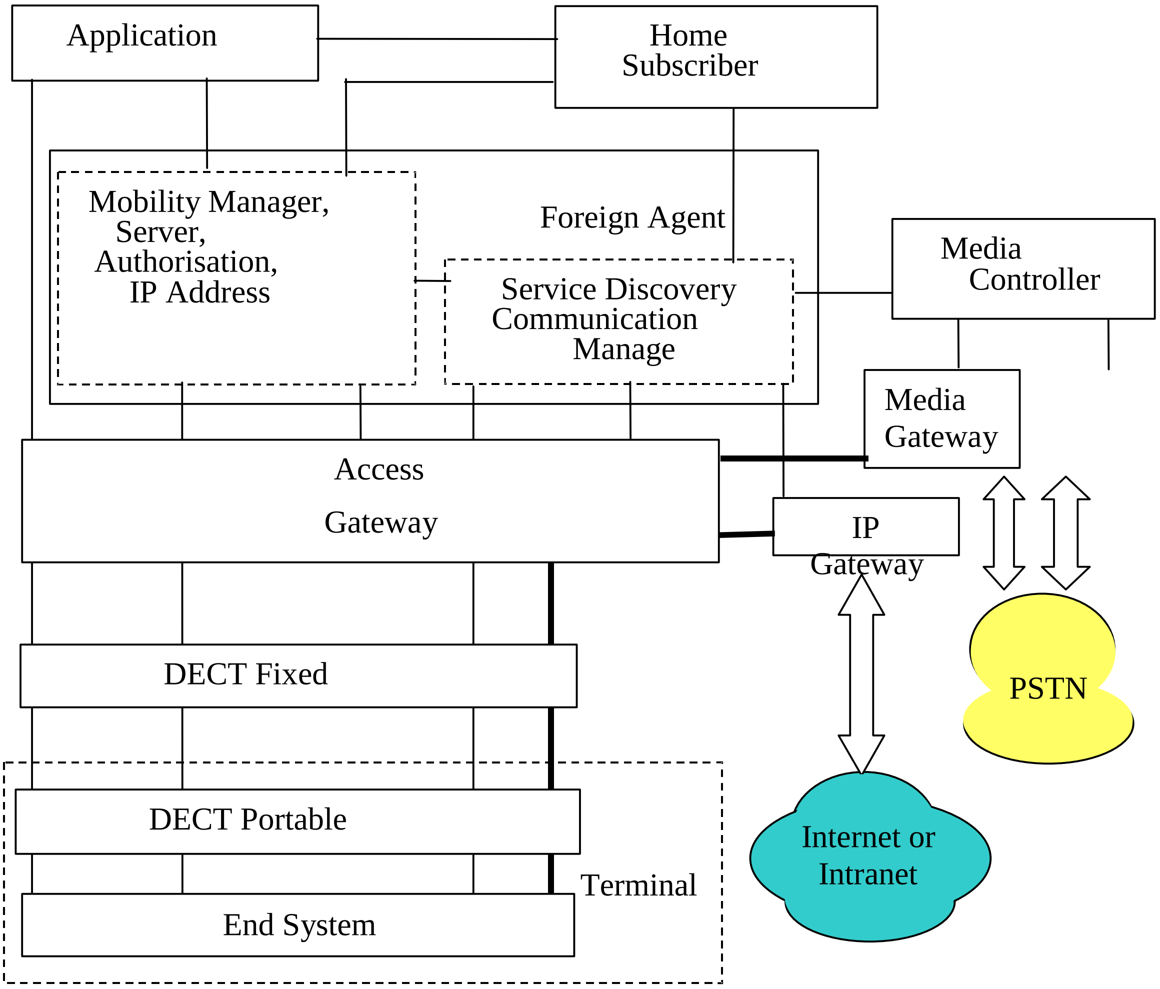

Figure 4: Network Reference Architecture

8 Network Functional Entities

This clause describes the Network Functional Entities comprising the Network Reference Architecture.

8.1 Access gateway

The Access gateway interfaces the access network and the IP network.

The Access gateway:

- Conveys bearer streams between the access network and the IP network.
- Transports control streams between access network and IP network.
- Serves as the QoS Policy Enforcement point for control and bearer streams between the access network and the IP network.
- Accepts access network QoS authorization levels for propagation through the IP network (based on service provider's choice, e.g. using RSVP, MPLS, or DiffServ). This may include conversion between different QoS mechanisms.

- Forwards IP network QoS authorization levels for propagation through the access network using mechanisms appropriate to that access network.
- Asserts terminal and network requested QoS to bearer and control data packets.
- Provides firewall functionality as required.
- Allocates Access Gateway resources to support bearer stream requests based on Resource Manager QoS authorizations.

8.2 Access network

An access network is a network that allows terminals to attach or detach. The Access Network consists of the DECT Fixed Termination and the DECT Portable Termination.

8.3 Accounting

The accounting keeps track of the services, QoS, and multimedia resources requested and used by individual subscribers.

8.4 Application server

The application server stores and executes service logic to provide specific voice call and multimedia session services for subscribers. Application Servers may provide services to users that are not related to specific voice calls or sessions.

8.5 Authentication

The authentication verifies the identity of a requesting entity.

8.6 Authorization

The authorization verifies that the one or more services, the QoS, or the multimedia resources requested by a subscriber are allowed based on the services subscribed and policies of the service provider.

8.7 IP address manager

IP address manager controls network level address assignment and recovery of addresses within the address space of the network domain.

The IP Address Manager:

- Manages IP address allocation status.
- Allocates and de-allocates IP addresses.
- Accepts and handles allocation or de-allocation requests from the Terminal.

8.8 IP gateway

The IP gateway provides controlled access between the local IP network and other IP networks, such as the Internet, intranets or enterprise networks.

8.9 Location server

The location server stores all dynamic information associated with subscriber/terminal and service mobility. Location information will include both network location and geographic position.

8.10 Media gateway

A media gateway interconnects the local IP network to the PSTN or to circuit terminations.

8.11 Media gateway controller

A media gateway controller controls the bearer paths through a media gateway.

8.12 Mobility Manager

The Mobility Manager supports the movement of a mobile terminal across Administrative Domain boundaries as well as across Access Gateway boundaries.

The Mobility Manager:

- Supports IP level (i.e., network layer) mobility management.
- Updates the administrative domain location of the mobile subscriber and Terminal in the Location Server.
- Updates the Access Gateway address of the mobile subscriber and Terminal in the Location Server.
- Updates the currently assigned Subscriber care-of address.
- Provides IP level (i.e., network layer) registration support for subscribers and terminals.
- Requests subscriber authentication upon receiving registration requests via the Access Gateway, then propagates corresponding authentication response.
- May maintain subscriber authentication and authorization information to support handover (handoff) between administrative domains.
- Initiates handover (handoff) control for the macro terminal mobility and the inter-administrative domain terminal mobility upon receiving a handover (handoff) request via the Access Gateway.

8.13 Home agent

Stores subscriber objects containing subscriber identity, subscriber name, service preferences, terminal-to-service associations and transport authorization. Stores terminal objects containing bearer capabilities (e.g. voice packets, data rates), terminal capabilities (e.g. authentication type, call processing, specific tone generation, alerting options, notification options), teleservice capabilities (e.g. voice for different vocoders or codecs, data, short message services).

Stores service objects containing the location and service specific attributes (e.g. service authorization) for each particular service.

Stores the received Care of Address, in the case of roaming.

8.14 Public Switched Telephone Network (PSTN)

The PSTN is a circuit switched network controlled by ISUP. This includes the fixed networks and the circuit-switched portion of wireless service provider networks (e.g. Public Land Mobile Networks).

8.15 Service discovery and communication session manager

The service discovery server enables discovery of network services. It provides accessing terminals or other servers with addressing information, server attributes, supported interfaces, etc.

The communication session manager provides the controls for all sessions for a given subscriber.

8.16 Signalling gateway

A signalling gateway interconnects the local IP network to a legacy signalling (e.g. SS7) networks.

8.17 Terminal

A Terminal is a device with allows a subscriber or user to access the network to gain assess to communication services. The Terminal consists of the DECT Portable Termination and the End System.

A Terminal:

- Terminates bearer streams.
- Provides conversion of bearer streams to make them useful to the user (e.g. display text messages, provide audio, provide video or multimedia displays, provide data interfaces to other end user devices).
- Controls sessions.

9 Investigation of specific issues

9.1 User identification

For the identification of users the Network Access Identifier (NAI) could be used, which has a syntax similar to an e-mail address, two strings separated by an "@". The first part is made of a username and the second identifies the home NSP of the user.

9.2 Addressing and Mobility

When connecting to a network provider, the home IP address will probably be the one agreed when the contract with that provider was signed and will be the same independently of the point the terminal connects to the network. As the terminal moves, different care-of address will be assigned to the terminal to manage mobility, but the home address will remain.

9.2.1 Configuration and address allocation

Configuration can be divided up into three main areas.

Firstly, there is configuration of the lower layers and assignment of radio resources.

Secondly, there is the allocation of an IP address to the terminal. This could be carried out using a variety of options:

- Link layer procedures (e.g. analogous to PPP's IPCP).
- Autoconfiguration with duplicate address detection (IPv6 only).
- Use of another network layer autoconfiguration protocol (typically DHCP or BOOTP).

The second and third options require the network to allow local transmission and reception of IP packets by the terminal while it is configuring itself.

The final part of configuration is the configuration of "upper" layers within the terminal. This might relate to:

- Notification of information about addresses of network servers (e.g. outgoing mail server, DNS server, service location server).
- Notification of information about appropriate configuration parameters of transport and upper layer protocols (e.g. TCP parameters).

This sort of information is almost invariably provided by DHCP, and can be considered as purely an application layer function, which takes place (if at all) after the first two stages of configuration considered above.

9.2.2 Registration procedures and mobile IP

Registration procedures refer to the ability of the user to register the local address of their terminal at some well known global identity. The only class of local address to be considered is the IP address, allocated as described above in clause 9.2.1. Address registration procedures should be carried out preferably directly between terminals and remote servers and the DECT access network should be transparent to the protocols used to do this.

The macro mobility or mobility between several DECT domains should be controlled by mobile-IP. Mobile-IP offers to a terminal a unique address that is useful across the entire IP network. The delay introduced by mobile-IP to make registrations can be ignored if it is being used only for macro mobility.

In IPv6 mobility, a terminal can allocate dynamically for itself a care of address. In case of allocation, the terminal sends its address to the home agent that encapsulates packets to the visited network. So, when packets reach the gateway, it forwards them to the appropriate DECT access network.

In IPv4 mobility, the foreign agent could allocate a care of address to all visitors incoming to its domain. This address, called foreign agent care of address, can be shared between more than one terminal because of the small available address space in IPv4. In general, all packets are redirected by the home agent of the mobile node through the encapsulation protocol. The home agent uses the care of address to route packets to the visited network. So, at the arrival of a packet, the Foreign Agent should intercept the packet, to extract the care of address header and then send the rest of the packet to the appropriate terminal by using its permanent IP address. Because of security and configuration issues the deployment of foreign agent care-of addresses is administratively complex.

9.3 Auto-configuration

After having received some network announcements from the available network providers in the area, and, after having taken the decision to associate with a particular one, the auto-configuration phase begins.

Auto-configuration is typically based on client-server applications. Clients discover the parameters they need by sending requests to auto-configuration servers that centralize the information and guarantee an ordered allocation, e.g. the uniqueness of IP addresses. However, in other situations like home networks or small office networks neither the server nor the facilities needed to deploy an auto-configuration system will exist. Therefore, these networks will need auto-configuration protocols that require zero user configuration and administration and do not rely on information received from a centralized server.

During auto-configuration, the basic IP parameters are negotiated. Besides, the terminal gets information about proxy application services offered by the network provider or typical applications configuration, like the location of the nearest web proxy with transcoding capabilities, e-mail relay or the zone gatekeeper. The terminal configures the applications to use that proxy services and once the auto-configuration finishes, the applications can be run.

9.3.1 Basic IP auto-configuration

Before a mobile station is able to use any IP-based service, several configuration parameters and options need to be properly set inside the TCP/IP protocol stack. Some of them can be set to default or some pre-configured values. But the values for some other parameters cannot be guessed or assumed to have correct defaults, as they directly depend on the configuration of the access network being visited. They should be set every time the mobile station visits an access network.

The essential parameters that a station needs in order to become an "IP citizen" and have connectivity with other IP machines are the following:

- the IP address, to be used as the source and destination address of IP packets going out and coming to the terminal;
- the local sub-net mask in case of IPv4 devices, or the sub-net prefix in case of IPv6;
- the Maximum Transfer Unit (MTU) of the sub-net;
- the addresses of default routers in the sub-net;
- the address of a DNS server, used to resolve names into IP addresses.

At a minimum, the terminals should configure dynamically all these basic parameters listed above without user supervision.

If IPv6 is being used, the IP address is not unique for each interface. At least two addresses per interface will be used: a *link-local address* to communicate with machines in the same sub-net, and a *global address* to communicate with any machine on the Internet. In addition, one or more *site-local addresses* could be used to communicate with machines inside the same site. Besides, more than one global address could be used, for example, in case the terminal is connected to multiple providers simultaneously. Auto-configuration mechanisms, in case of using IPv6, should take into account this address multiplicity.

Allocation of IP addresses to hosts should follow the well-known IP rule that state that all systems in a logical IP sub-net should have addresses assigned from a common IP prefix. This rule that comes from the IP design principle that routing is based on network prefixes and not on host addresses, should be maintained when assigning addresses to mobile stations, in order to guarantee routing scalability. So, in principle, any mobile station should get an IP address from the sub-net it is visiting.

If the mobile station offers IP services to other users (for example, if it runs a web server or wants to receive e-mail messages directly), in some cases it may need to contact the Domain Name System (DNS) to update the map of its name to its present IP address. This could be the case, for example, of a mobile station using IP mobility which is moving to a different administrative domain and for some reason has been obliged to change its home address. The need of dynamic DNS updates depends highly on how mobility is managed, but, in case it is needed, network services should be in charge of that, relieving applications from doing it.

At present there are several ways to achieve auto-configuration for IPv4 and IPv6 hosts:

- *Dynamic Host Configuration Protocol (DHCP),* which has been defined for both IPv4 and IPv6.
- *Stateless Address Auto-configuration*, defined only for IPv6. It can be used separately or concurrently with DHCP to obtain configuration parameters.
- *PPP auto-configuration mechanisms*, based on IPCP options, which is widely used nowadays for assigning addresses to IPv4 dial-up users. It is also defined for IPv6.

9.3.2 Multicast address allocation

Some applications will make use of IP multicast services. Video distribution applications, news services that push information to a high number of users, videoconferences with a high number of participants are examples of applications that benefit from using IP multicast services.

Before sending data to a multicast group, applications choose the multicast address they will use. In some cases, this address will be fixed and known in advance. For example, in the case of the news service, a permanent multicast address could be assigned for that service. However, in other cases, multicast addresses should be assigned dynamically – for example, when a videoconference is started, and it should be guaranteed that no other application uses the same multicast address to avoid conflicts.

9.3.3 Service discovery

Apart from the basic IP configuration parameters, the auto-configuration process should allow terminals to automatically discover the resources available on an access network, as well as the parameters needed to use them.

Proxy servers that offer specific application services adapted for mobile terminals as well as general application servers will be offered in access networks. Besides, other services that require the physical access to hardware devices, like printers or fax gateways for example, could also be offered.

Therefore, in a typical scenario, each time a terminal visits a new access network, it will need to discover the location and characteristics of services like the following:

- WWW and FTP proxy server. This proxy server will typically include transcoding capabilities to adapt the information to the capacities of the terminal (resolution, colour depth, etc). So, the terminal (or, at the end, the WWW browser inside the terminal) will need information about the location of the server and its capabilities.

- Video/Audio streaming proxy server. That is, a server with transcoding capabilities that will allow the terminal to have the video/audio streams adapted to its capabilities. This type of proxy server will be useful, for example, when big events – a football match – are broadcast to a high number of users with different terminal capabilities. Instead of having several copies of the video with different formats and qualities sent from the source, the proxy server could receive a copy with the highest quality demanded and translate it and send adapted copies to clients in the requested format.

- E-mail server (SMTP) for outgoing messages. It could be useful to relay all outgoing messages through an e-mail relay server, for accounting or security reasons.

- The Gatekeeper or SIP proxy for telephony over IP applications. Although methods exist to dynamically locate these servers automatically, there could be more than one of these servers available on a network (because they belong, for example, to different network service provider), so it could be useful to have them configured through the auto-configuration phase.

- Other services like: time reference (NTP) servers, localisation servers, printing servers, fax relays, etc.

At present, some specific IETF protocols try to address the service discovery:

- Dynamic Host Configuration Protocol (DHCP), which apart from addressing auto-configuration of basic IP parameters, includes additional fields to announce services and their parameters.

- Service Location Protocol, which provides a flexible and scalable framework for providing hosts with access to information about the existence, location and configuration of networked services.

- Application Configuration Access Protocol (ACAP), whose purpose is different from the previous ones, as its main objective is to allow users to access their application's configuration data from any network device.

9.4 Mobility Management

As a general principle, applications should be "as unaware as possible" about changes due to mobility of terminals. Whenever possible, all issues related to roaming and mobility should be treated in lower layer levels. For example, movement between cells inside an access network can be treated by the underlying sub-net layer. Or, movement between different access networks can be treated at IP level.

However, there can be situations where not all the issues due to mobility can be treated at lower layers. In these cases, applications should be informed about these events. For example, during a hand-over between access networks, QoS assigned to application flows could be temporarily reduced. Or, when moving to a new access network the QoS requested by some applications could not be guarantied, due to the lower bandwidth of the new network. Or, a hand-over between administrative domains could oblige to change the source IP address.

In all these situations were transparency cannot be achieved, the applications should be informed to allow them to react to those events.

Each time a user tries to access network services from a terminal, the network should execute several functions:

- Authentication, in order to assess the identity of the user;

- Authorization, to know if the user is allowed access to the network;

- Accounting, to account the resources the user requests.

These functions, jointly known as AAA, form the basis of the work being carried out in IETF AAA workgroup.

9.5 Header compression

For further study, see also RFC1144 [13].

9.6 Security

It is preferred to use end-to-end security, which can only be provided by the higher layers.

9.7 IPV4 and IPV6

DECT can support IPV4 as well as IPV6.

9.8 Voice service

If voice over IP is used in the fixed network, it seems to be more economic to transcode in the DECT Fixed Part the voice-over-IP data to the DECT ADPCM speech service, for transport across the air interface. The main advantages are that the IP overhead is removed and a minimum delay can be guaranteed.

10 Recommendations

It is recommended to produce a Technical Specification, that defines the additions which are necessary in the DECT standard to support roaming using IP mobility.

The DECT Fixed Part that gives access to an IP-network needs to broadcast its identity and it seems that for the system identification the existing DECT ARI-classes can be used as well as the existing PARKs can be used to determine the access rights. It may be useful to define one indication or class that means "unrestricted access" to this system (no specific PARK is required to get access to this IP-network).

For IP mobility the portable part will need to get during subscription registration an IP-identifier that indicates its home IP-address and the address of its home agent. This information should be provided by the portable part to the Fixed Part (and Foreign Agent) during the DECT location procedure. One possibility to exchange this information is to define a new IPUI-class for this type of Portable Part identity.

If voice over IP is used in the fixed network, it seems to be more economic to transcode in the DECT Fixed Part the voice-over-IP data to the DECT ADPCM speech service, for transport across the air interface. The main advantages are that the IP overhead is removed and a minimum delay can be guaranteed.

It is not necessary to broadcast the local sub-net-mask, if the standard DECT identity structure and location area indication (location area level) are used to define the paging/location areas. It may be useful to broadcast information about available service provider. Some further investigation should be done, if additional IP-Information may be broadcast.

History

Document history		
V1.1.1	November 2001	Publication