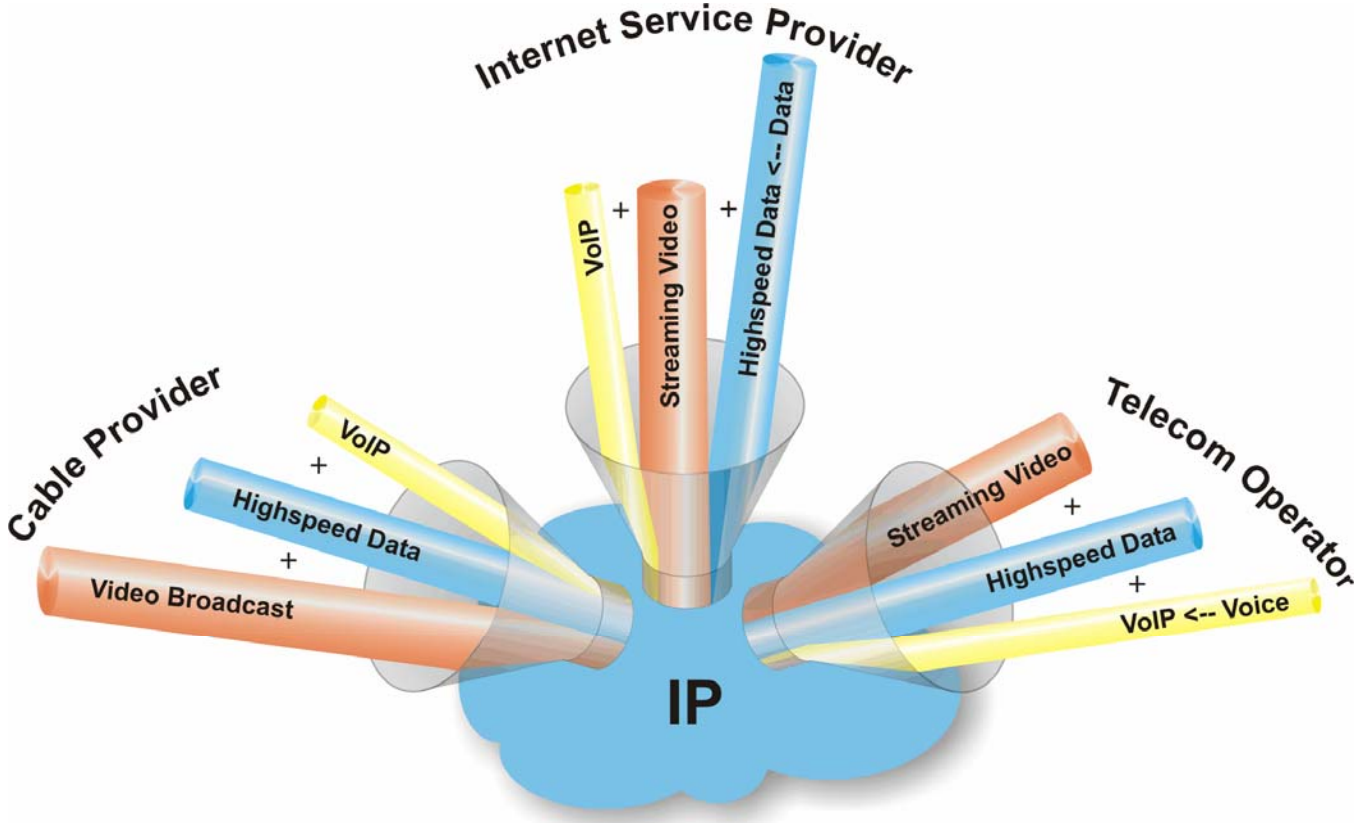
The Promise of Triple Play Services



- **'One Stop Shopping': all services from one provider**
- **Bundling Price below individual Service**
- **Seamless Customer Service: 'One Call, One Solution, One Bill'**
- **Increased Services, Applications, Solutons**

The Promise of Triple Play Services

- **Combined Voice, Broadband Data and Video Services delivered from the same Service Provider.**
  One stop shopping for the customer: End-Users can decide and select just one single communication platform to gain access to voice (e.g telephony), data (e.g internet browsing and e-mail) and video services (e.g. IP based video streams (IPTV), Video on Demand (VoD)).
  This also enables seamless customer service => One call, one solution, one bill.
  For service providers, this can become a marketing advantage and instrument for customer binding and could prevent alternative providers to enter the customer relationship.

- **Lower cost of Services.**
  Due to increasing competition and the reduction in access charges (depending on the choice of access technology), the customer can profit from reduced charges.

- **Reliable High-Speed Broadband Services.**
  Simultaneous transmission of phone calls, internet data and television services require provision of considerable bandwidth and a high degree of reliability (Quality of service, QoS) in the network right to customer premises.

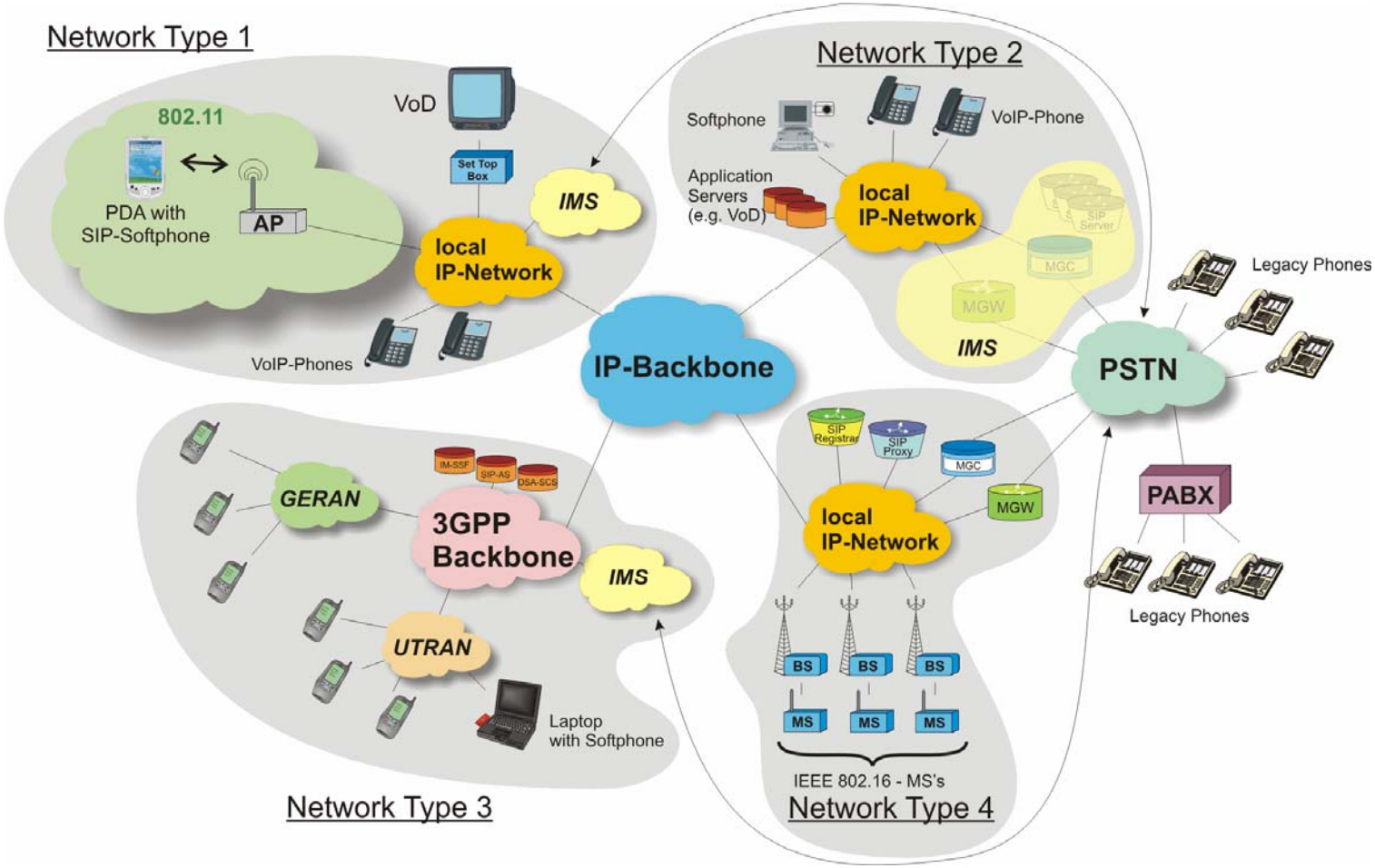
- **Increasing Services and provision of content.**
  With the provision of voice, data and video over one medium (or communication platform), new services will evolve. Also, competition will force the service providers to offer differentiated content and services to maintain customer satisfaction and to compensate for margin decrease.

Recent marketing reports (e.g. Gartner research) predict, that the provision of triple play services is a necessity for every local service provider in order to remain competitive and is a must for long-term survival.

Triple Play Services are based on an ‘All-IP’ network infrastructure.

Next Generation Networks and their Components

- **Typical Configuration and Interconnection of Next Generation Networks**



Next Generation Networks and their Components

Typical Configuration and Interconnection of Next Generation Networks

The figure illustrates the most likely configuration of NGN's and it provides information about the services offered (Triple-Play). Most interestingly, the figure includes two wireless access networks of which only one is based on 3GPP while the other one is based on WIMAX…

Network Type 1: Evolved ISP

This type of network now provides telephone services, VoD-services (Video on Demand) and obviously still standard ISP-services (not shown). Through the operation of public hotspots, the ISP also gets the flavor of wireless operation. All multimedia services and the VoIP-services are controlled through the operator owned IMS (IP Multimedia Subsystem).

Network Type 2: Former Telecom-Operator

The former Telecom-Operator still has strong ties towards the PSTN. As the figure illustrates, part of the IMS is a soft switch (⇔ combination of Media Gateway and Media Gateway Controller) which allows the VoIP-subscribers the communication with regular PSTN-subscribers. Note that this Telecom-Operator also operates a number of application servers for all kinds of services like VoD or Presence Services. Nothing hinders the Telecom-Operator to allow other operators like the Network Type 1 operator to also use these application servers.

Network Type 3: 3GPP Mobile Network Operator

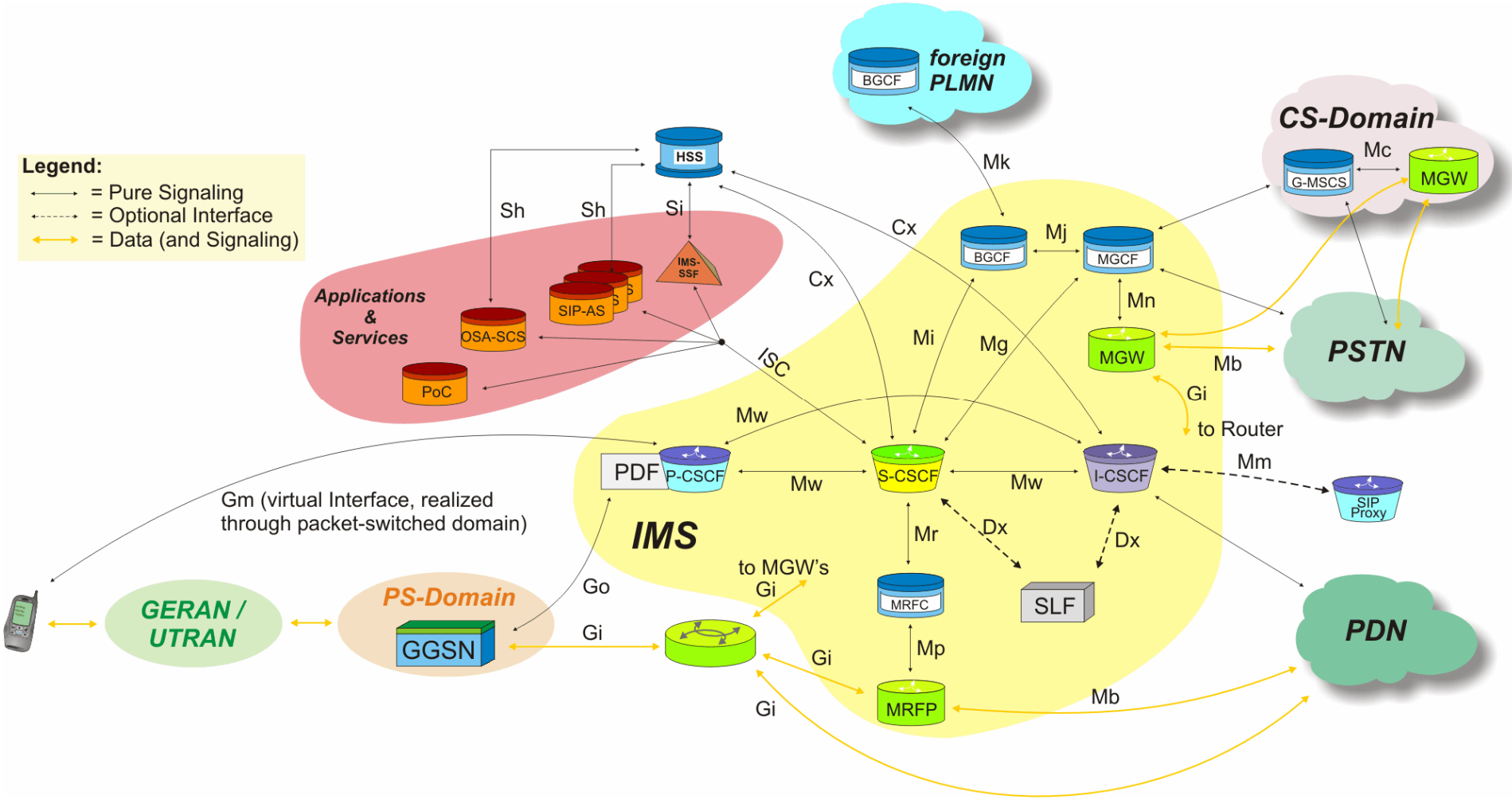
The 3GPP mobile network operator is no different from the previously mentioned operators with one exception: The primary way of accessing an IMS is through GERAN or UTRAN. With bandwidths of up to 2 Mbit/s, the 3GPP-network operator can offer similar or the same services as wireline operators (who are bandwidth limited through the physical limitations of DSL). In the long run, only the operator owned IMS interconnects calling mobile subscribers towards the PSTN. That's why we do not illustrate

Network Type 4: WIMAX Network Operator

The upcoming WIMAX-network operators may emerge to a combination of a wireless network operator and an evolved ISP. WIMAX is a very strong DSL-competitor and WIMAX has the potential to become a cellular standard. Note that in case of network type 4 we did not put in an IMS. Its functions are accomplished through a series of dedicated SIP-servers and soft switches.

Note: The last mile towards the customer for wireline operators is usually realized through DSL. Still, cable-TV operators may rather use their evolved cable-TV lines.

Architecture of the IMS



Architecture of the IMS

The figure illustrates the entire IMS (IP Multimedia Subsystem) architecture with all logical network elements. Note the following:

- ⇒ There is no requirement that each logical node is represented by a separate physical node.
- ⇒ In the figure, the orange colored lines represent the way that the media streams take. The black lines represent interfaces with pure signaling information transfer.
- ⇒ Dotted lines represent optional interfaces.
- ⇒ The Gm-interface between the UE and the P-CSCF is obviously a virtual interface that is physically realized through the packet-switched core network domain and the respective access network.
- ⇒ Please note that adjacent “Applications & Services” cloud that in this figure only illustrates the IMS-relevant network elements but which also comprises the SM-SC and the MMS-SC. The PoC-server is the “Push-to-talk-over-Cellular”-server.

[3GTS 23.002, 3GTS 23.228]

Abbreviations:

CSCF: _____

IMS-SSF: _____

SIP-AS: _____

PDF: _____

ISC-Interface: _____

HSS: _____

SLF: _____

OSA-SCS: _____

PoC: _____

BGCF: _____

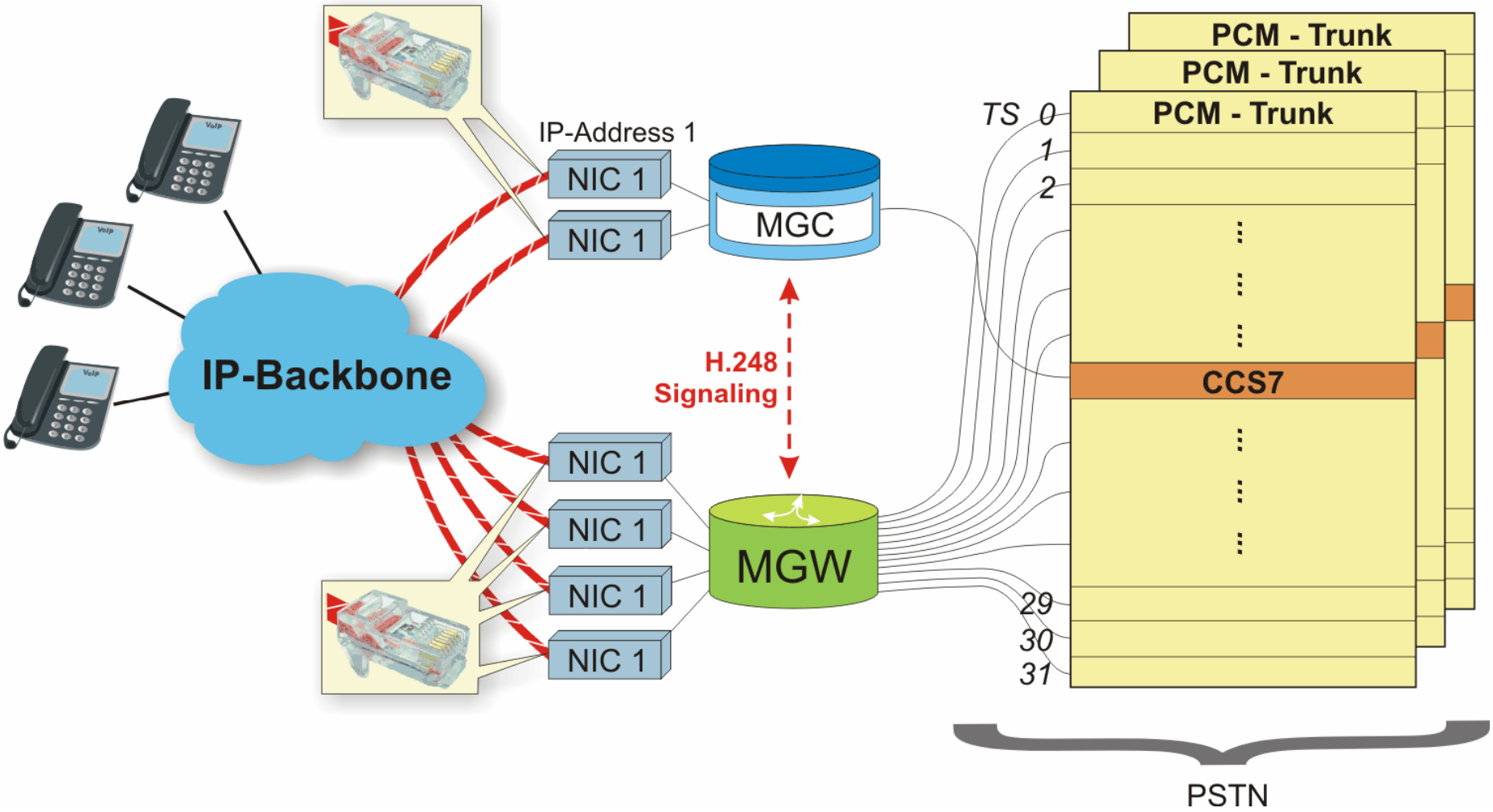
MGCF: _____

MRFC: _____

MRFP: _____

MGW: _____

Soft Switches and their Controllers



Soft Switches and their Controllers

⇒ Definitely very important components of next generation networks are the media gateways which are frequently also called “soft switches”.

⇒ As the figure illustrates, media gateways are controlled by a media gateway controller (MGC). In the 3GPP-terminology this MGC becomes the MGCF (Media Gateway Control Function).

Media gateways and media gateway controllers are required to interface IP-based communication towards the legacy PSTN.

⇒ The control function between MGC and MGW is performed through a protocol called H.248 (⇔ ITU-T terminology) or MEGACO (⇔ IETF-terminology / RFC 3015).

⇒ The H.248 / MEGACO protocol allows for the seizure and release of resources that are controlled by the media gateway. This also relates to the control and conversion of codec types (AMR, PCM a-law, PCM µ-law, …).

⇒ Accordingly, the MGC terminates the call control signaling information from both sides: The SS7-signaling (ISUP) from the PSTN as well as the IP-based call or session control information (usually H.323 or SIP).

⇒ On the other hand, the MGW terminates all PCM-links (⇔ timeslots on the different PCM-trunks) and it is able to interconnect these PCM-links to packet-switched resources on the IP-network side (usually identified through the combination of Source IP-Address / Source UDP-Port Number and Destination IP-Address / Destination UDP-Port Number).

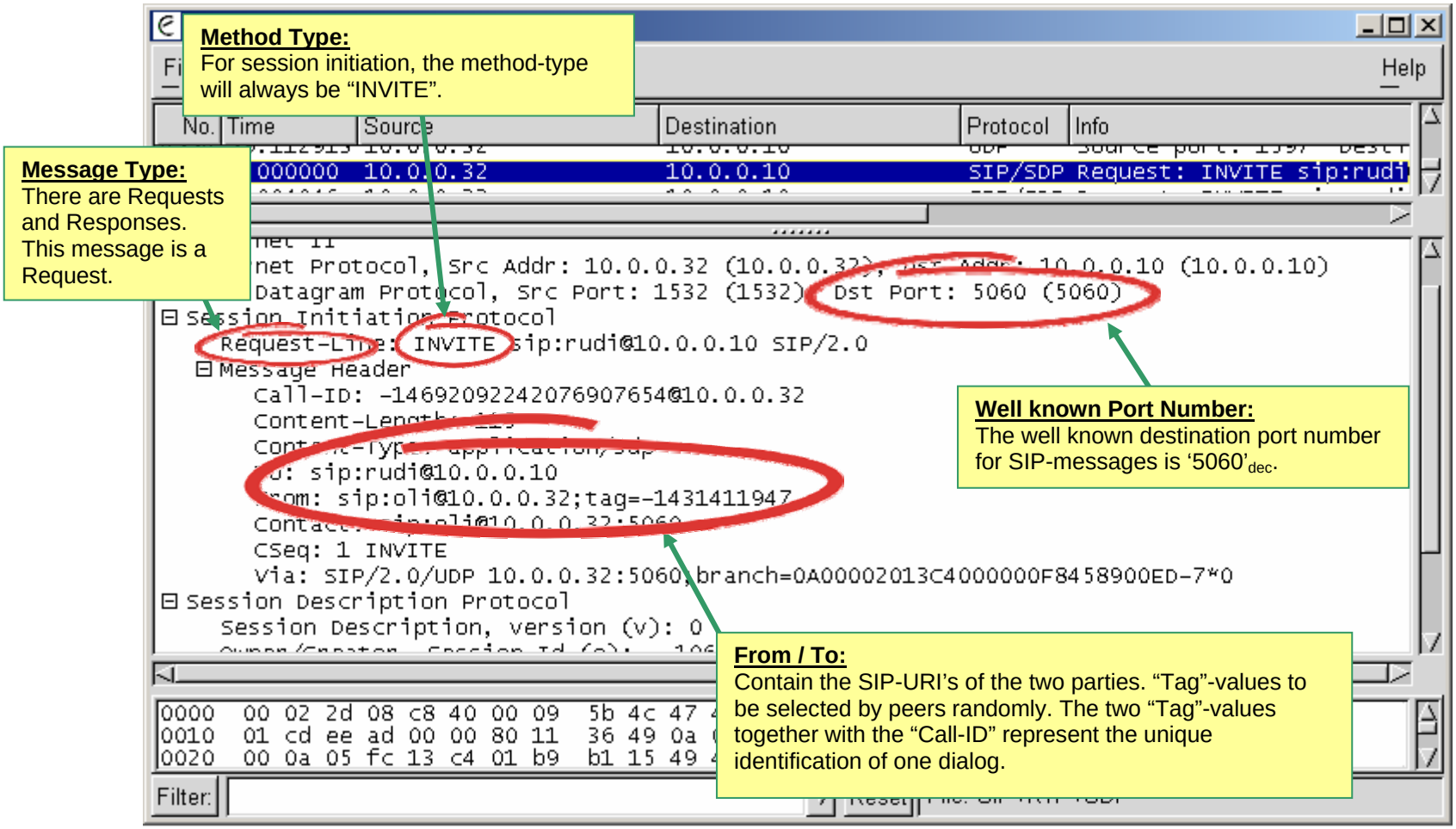
⇒ As the figure illustrates, media gateways and media gateway controllers usually are interconnected to the IP-network through more than one NIC (Network Interface Card) which means through more than one IP-address. This is done for load balancing and congestion control.

⇒

The figure tries to indicate what makes soft switches so appealing to network operators:

- They are connected to the IP-network simply through standard IP-network cables (e.g. RJ-45). No error-prone patch panel wiring is necessary.
- They usually do not require sophisticated configuration but they use some auto configuration to obtain IP-addresses etc.
- They usually have a smaller footprint than their predecessors, the public exchanges of the SS7-world.

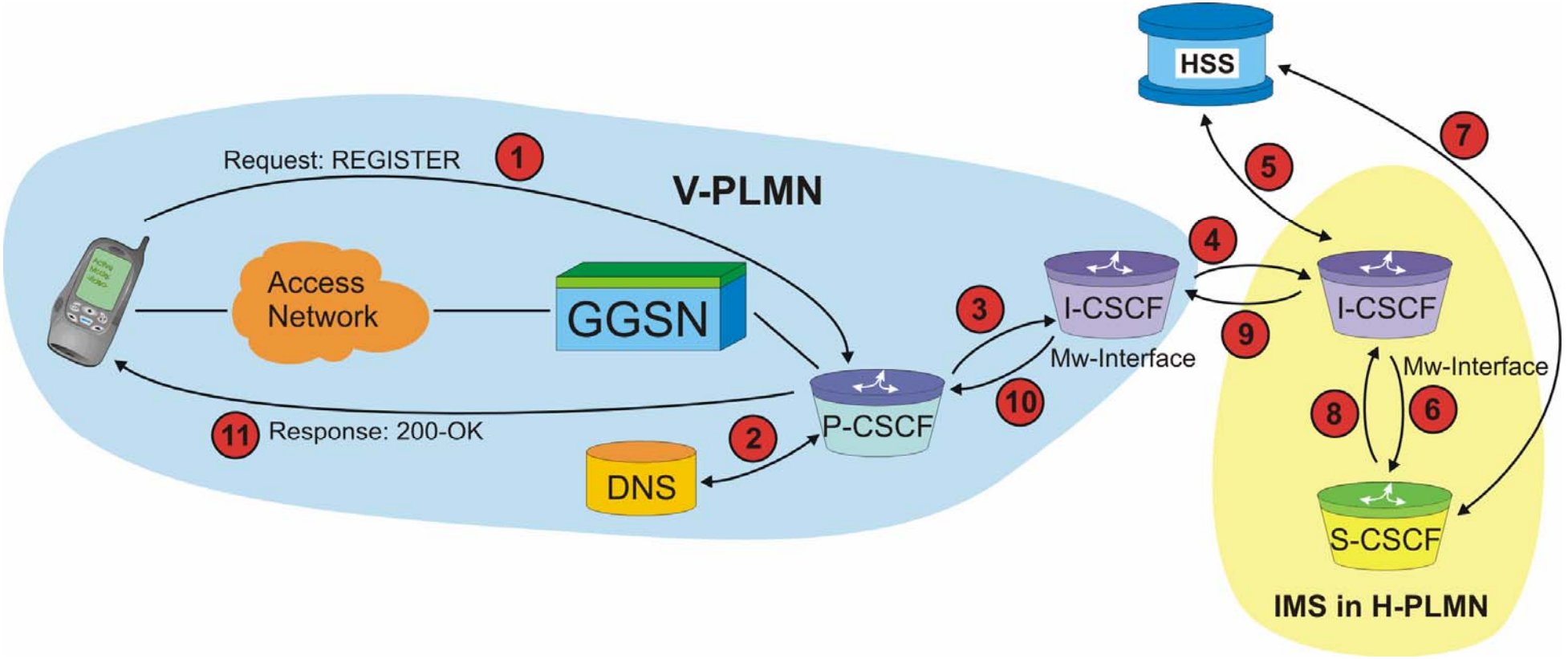
Request: INVITE-Message



Request: INVITE-Message

Intentionally left blank

Subscriber is Roaming



Subscriber is Roaming

The figure illustrates how a roaming subscriber registers to an IMS.

Most importantly, the MS will always register to his/her home IMS, irrespective of whether he/she is roaming or not.

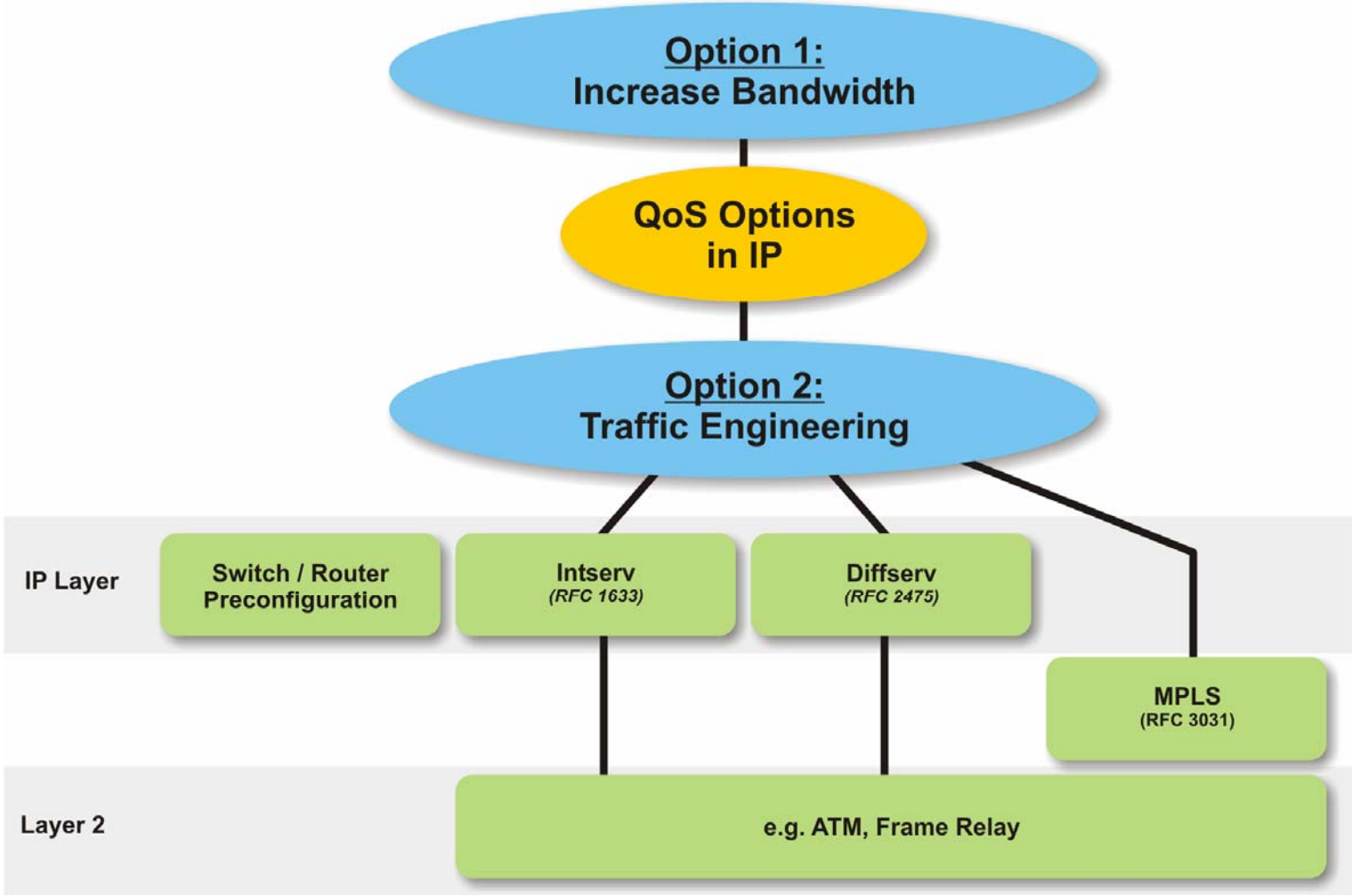
1. The MS sends a Request: REGISTER-message to the previously detected P-CSCF in the local IMS (V-PLMN). Note our considerations about the APN: If the APN is not set to default but to a GGSN in the H-PLMN then the subscriber would rather detect a P-CSCF in the H-PLMN.
2. The P-CSCF checks with a DNS-server to determine where to find the domain in which the subscriber wants to register (e.g. registrar.inacon.com). Note that this construct does not identify one particular registrar but only a domain which may contain many registrars.
3. In our case, the P-CSCF has got routing information and forwards the REGISTER to an I-CSCF (for topology hiding) in its own IMS. Alternatively, the P-CSCF could have sent the REGISTER directly to an I-CSCF in the H-PLMN of the subscriber. In our example, this step is done by the I-CSCF in the V-PLMN.
5. The I-CSCF interrogates the HSS of the subscriber to which particular S-CSCF to send the REGISTER message to. The I-CSCF may need to invoke the help of an SLF to do so if more than one HSS is there.
6. and 8. The I-CSCF forwards the REGISTER-message to the selected S-CSCF and the S-CSCF responds with a Response: 200-OK.

Note that alternatively, the S-CSCF could have rejected the REGISTER-message with a Response: 407-Unauthorized which would contain an authentication challenge for the MS. The S-CSCF obtains this authentication information from the HSS in the query illustrated as 7. In this case, the MS would calculate the respective authentication response and send it in another REGISTER-message to the S-CSCF.

9.+10.+11. In our case, the proxies in the middle will relay the Response: 200-OK back to the MS.

[3GTS 24.228 (6)]

QoS Options in IP-Networks



QoS Options in IP-Networks

Within the IETF, there are different strategies how to provide QoS in an IP-network:

- **Large bandwidth reserve**
  Still the most important technique used in real-world networks to control QoS in IP. Under utilized networks (< 50 %) usually provide sufficient reserves for most of the QoS requirements of actual applications.
- **Intserv (RFC 1633)**
  Intserv is based on the end-to-end establishment and reservation of resources prior to any information transfer. In that respect, Intserv establishes something like a tunnel for a specific data flow.
- **Diffserv (RFC 2475)**
  This approach reuses the "Type-of-Service" field in the IP-header to allow the tagging of IP-frames with different QoS-requirements.

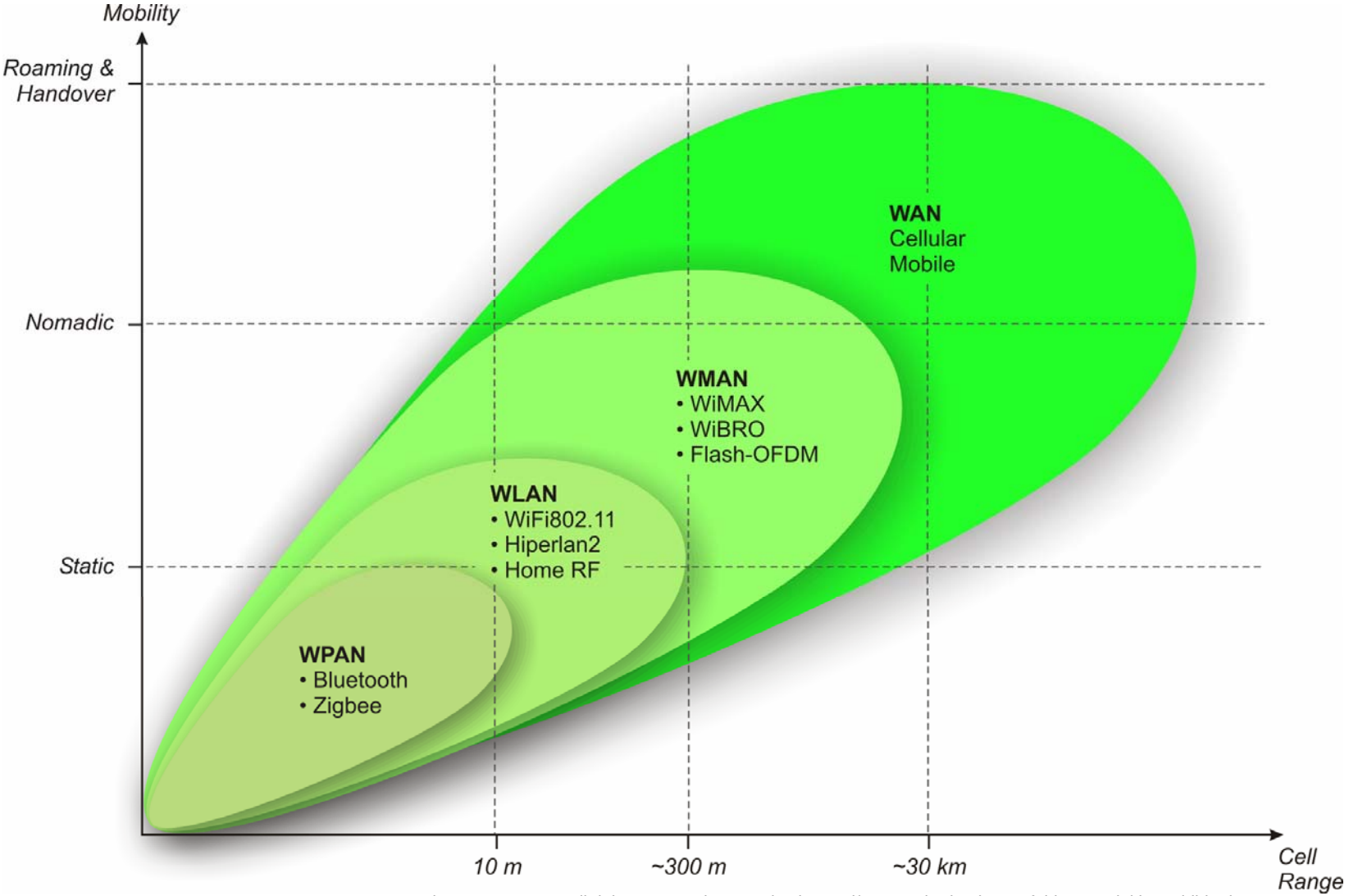
Note: Both strategies require that each device in a network can be configured and setup to provide a given QoS. This is usually not possible on the public internet.

- **Traffic Engineering**
  The ability to route primary paths around known network bottlenecks and points of congestion to optimize network utilization and plan resources based on known demand. Requires mechanisms to precisely measure and control network parameters (⇔ Traffic Inspection). Effective use of Traffic engineering can substantially increase the usable network capacity.

- **Multi Protocol Label Switching, MPLS (RFC 3031)**
  Data transport and routing mechanism, that is transparent to the type of traffic. It provides connection oriented routing for groups of packets (flows) which share the same requirements (QoS, traffic demands) between endpoints of a MPLS domain. Fast traffic switching is enabled, as the Routers do not need to examine IP header or payload information but use the routing label information only. MPLS thus establishes a sort of tunnel for the transported layer 2 traffic. It interfaces to existing routing protocols such as RSVP, OSPF, BGP, LDP.

- [RFC 1633, RFC 2475, RFC 2998, RFC 3031]

Wireless Technologies



Wireless Technologies

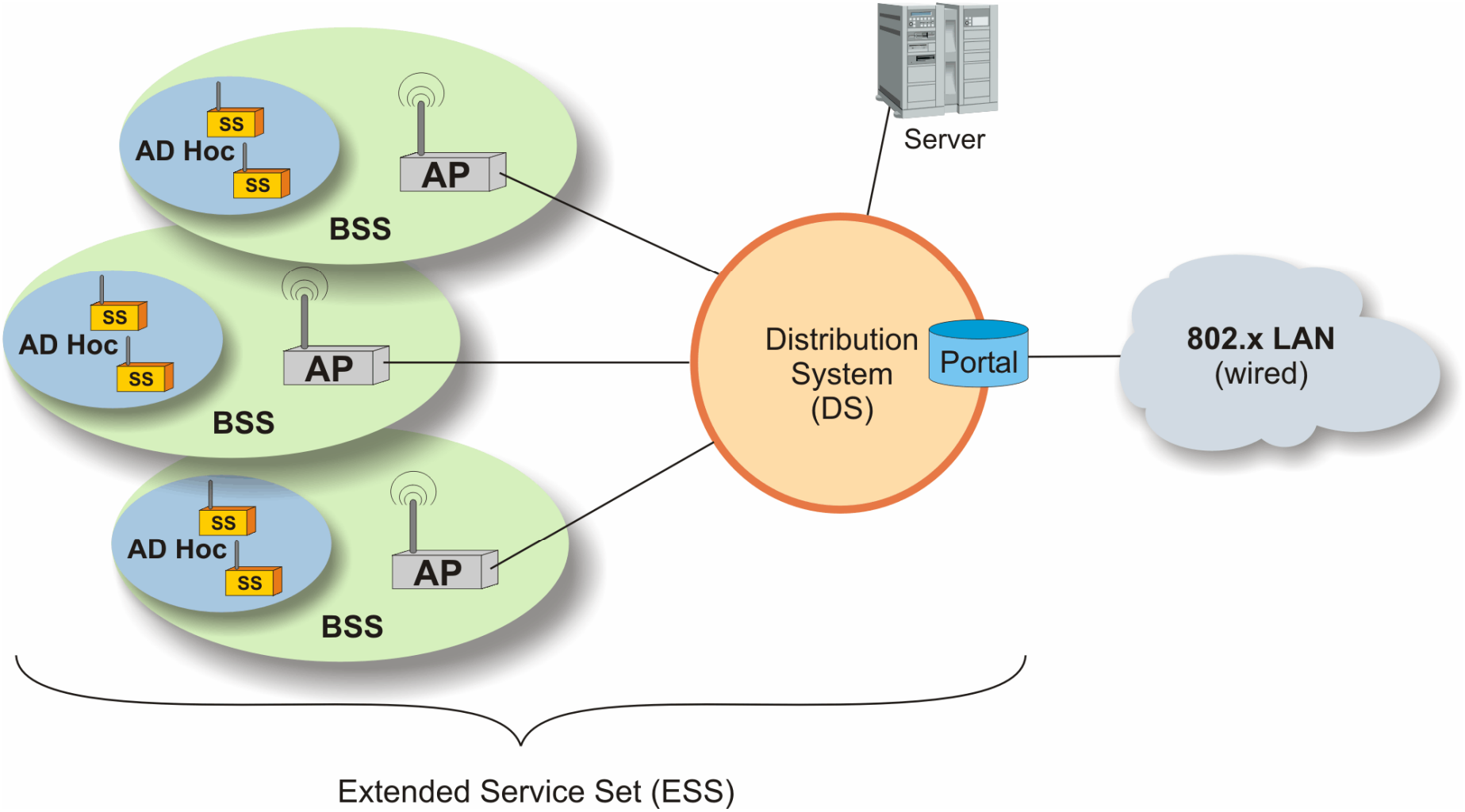
WPAN
The Wireless Personal Area Network (WPAN) interconnects devices centered on an individual person's workspace. Typically, a WPAN uses some technology that permits communication within about 10 meters.

WLAN
Wireless Local Area Network (WLAN) is a network in which a mobile user can connect to a LAN through a wireless radio connection. High-bandwidth allocation for wireless and the use of license free frequency bands make it possible to develop low-cost and easy-to-deploy networks.
Wi-Fi (Wireless Fidelity) has gained acceptance in many businesses, agencies, schools, and homes as an alternative to a wired LAN. Many airports, hotels, and fast-food facilities offer public access to Wi-Fi networks. 802.11 is an evolving family of specifications for WLANs, developed by the IEEE. The term Wi-Fi refers to the 802.11b specification. 802.11 standards use the Ethernet protocol and carrier sense multiple access with collision avoidance (CSMA/CA) for path sharing. The typical indoor range is up to 91 meters, while the typical outdoor range, with line of sight, can be up to 460 meters.

WMAN
Wireless Metropolitan Area Network (WMAN) is a network that interconnects users with computer resources in a large geographic area or region. It is also used to establish the interconnection of several local area networks by bridging them with backbone lines.
The 802.16 standard, amended this January by the Institute of Electrical and Electronics Engineers (IEEE) to cover frequency bands in the range between 2 GHz and 11 GHz, specifies a metropolitan area networking protocol that will enable a wireless alternative for cable, DSL and T1 level services for last mile broadband access, as well as providing backhaul for 801.11 hotspots. The new 802.16a standard (WiMAX) specifies a protocol that among other things supports low latency applications such as voice and video, provides broadband connectivity without requiring a direct line of sight between subscriber terminals and the base station (BTS) and will support hundreds if not thousands of subscribers from a single base station.

WAN
A wide area network (WAN) is a geographically dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a local area or a metropolitan area network.
There are several cellular technologies within a wide area data network, covering mobile voice and data services, such as GSM, GPRS, EDGE and UMTS.

WLAN Overview



WLAN Overview

WLANs are either used to replace wired LANs or to extend a wired LAN infrastructure.

Ad Hoc Network

This is the basic topology of an 802.11 network, consisting of two or more wireless nodes or subscriber stations. Such SSs can communicate directly with each other on a peer to peer level. These networks are often established on a temporary basis and are also referred to as Independent Basic Service Set (IBSS).

Basic Service Set (BSS)

Although a BSS could just be an Ad Hoc network, in most cases it includes a wireless base station, called Access Point (AP) in WLAN terminology. In that case, all the communication (between stations and between stations and a wired network) will go through the AP. These APs form part of a wired network infrastructure.

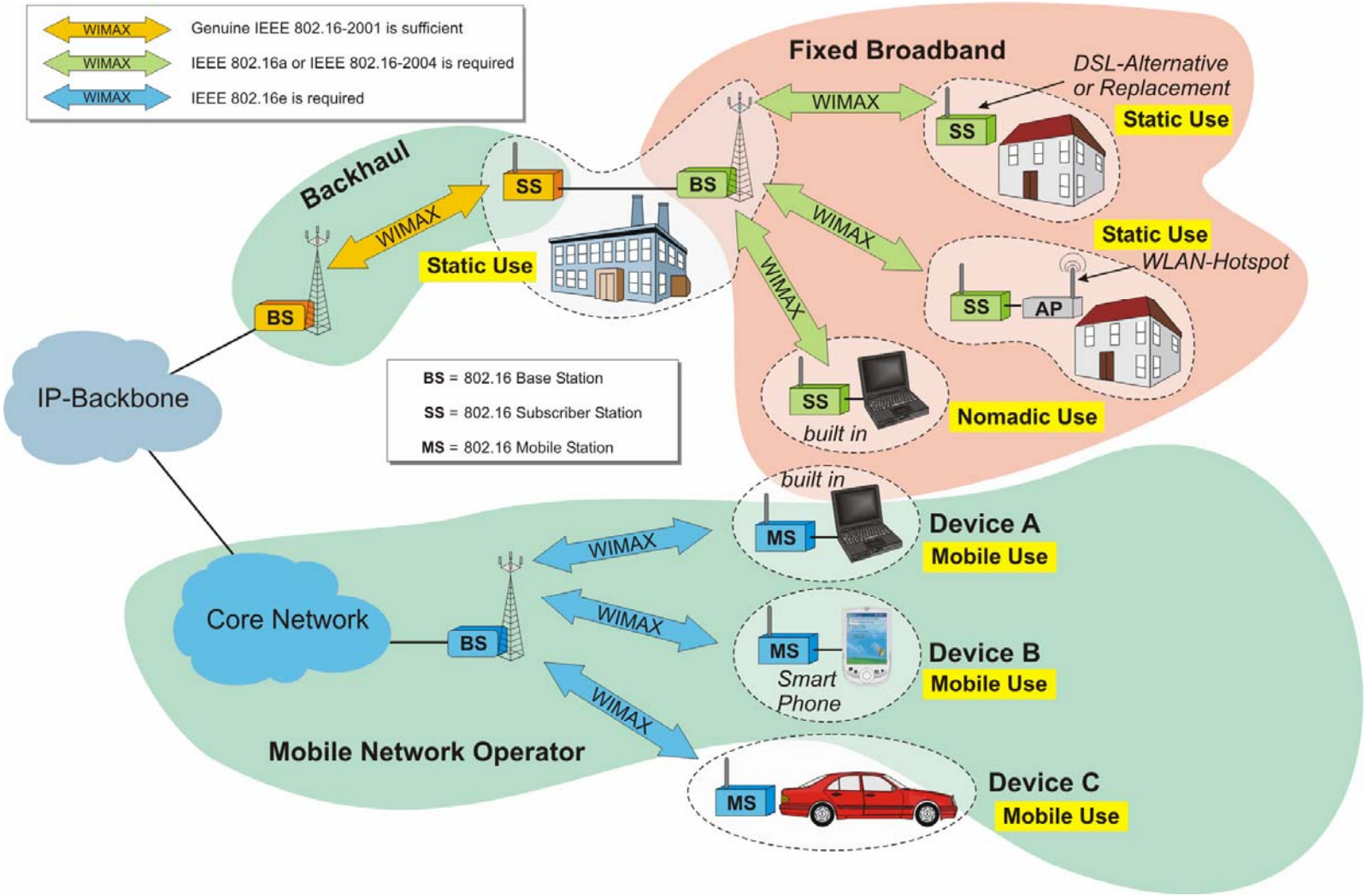
Extended Service Set (ESS)

An ESS is built through a series of overlapping BSSs, which are connected to a network infrastructure (Distribution System, DS). Such a DS normally is a wired Ethernet backbone LAN, but could also be any communication network. The whole ESS is seen by upper OSI layers as a single 802 network.

Portal

Bridge or Router attached to a DS to provide the integration with a traditional, wired LAN.

Example Configuration



Example Configuration

The figure illustrates how WIMAX can be used in different parts of a network for different applications

WIMAX in the Backhaul ⇔ The Genuine IEEE 802.16-2001 standard (10 – 66 GHz / LOS)

As illustrated here, this may mean that WIMAX is using WIMAX to relay user data between two points. WIMAX in the backhaul is really point-to-point and therefore related to directional antennas. As illustrated, WIMAX in the backhaul also means static use.

WIMAX for Fixed Broadband Access and Nomadic Users ⇔ IEEE 802.16a / IEEE 802.16-2004

Note how the "green" SS's are used in different ways: As DSL-replacement technology (⇔ static use) and in nomadic form built into a laptop computer. NLOS-operation is used to allow users a more flexible location independent use.

WIMAX as Cellular Technology ⇔ IEEE 802.16e

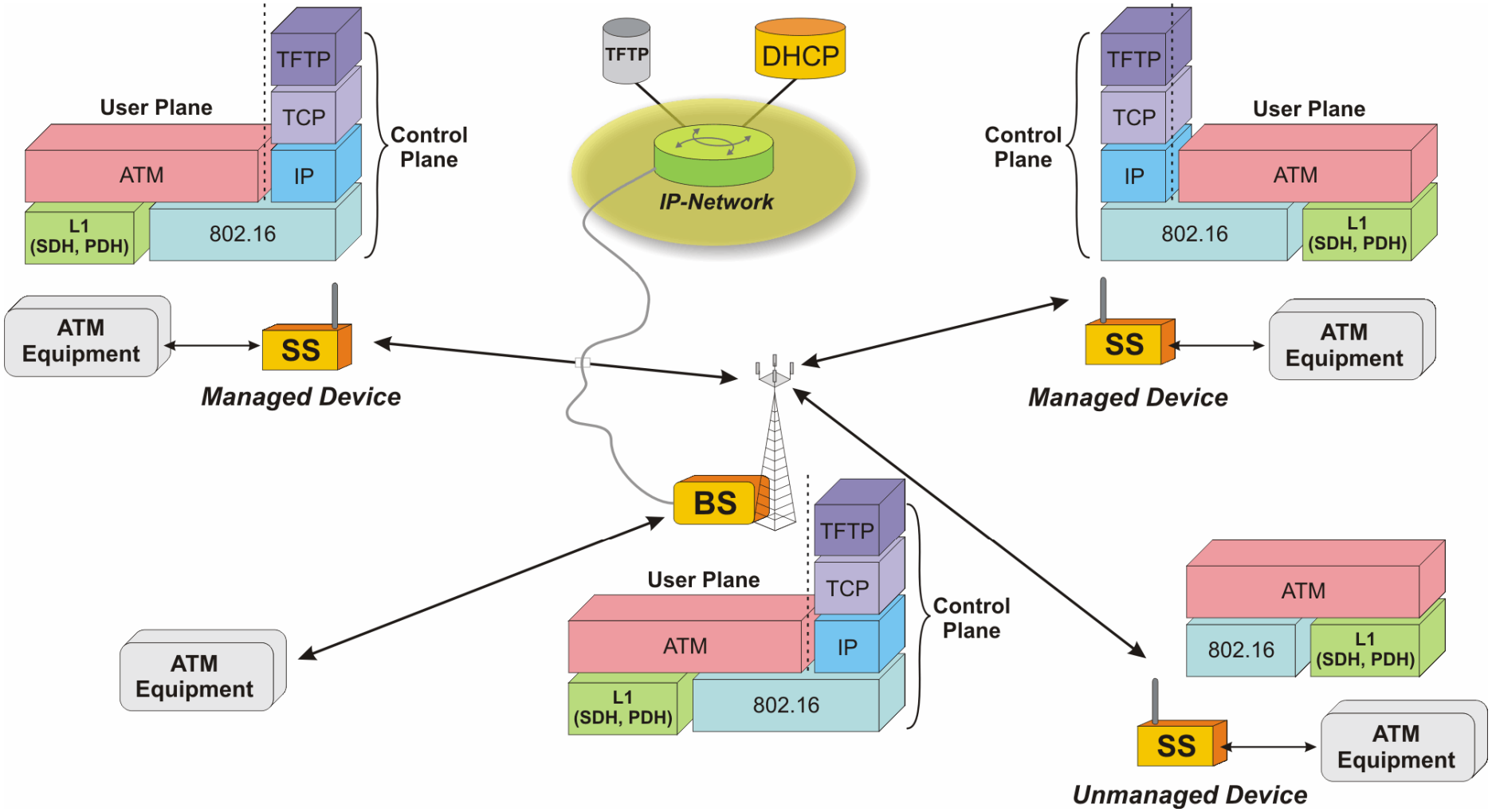
The three MS's indicate the different applications that WIMAX targets in the cellular domain:

⇒ Device A: The top MS is built into a laptop computer and provides the same services to a subscriber as GPRS- or UMTS-extension cards do today. The major difference between device A and the laptop with the green SS on top is the possibility to perform handover and other mobile scenarios.

⇒ Device B: The smart phone pushes this application most likely a little further by providing the user VoIP-services as circuit-switched voice alternative over WIMAX.

⇒ Device C: The MS at the bottom is used in a car and illustrates the full and seamless mobility target of IEEE 802.16e.

Option A: Static Peers (with ATM as User Protocol)



Option A: Static Peers (with ATM as User Protocol)

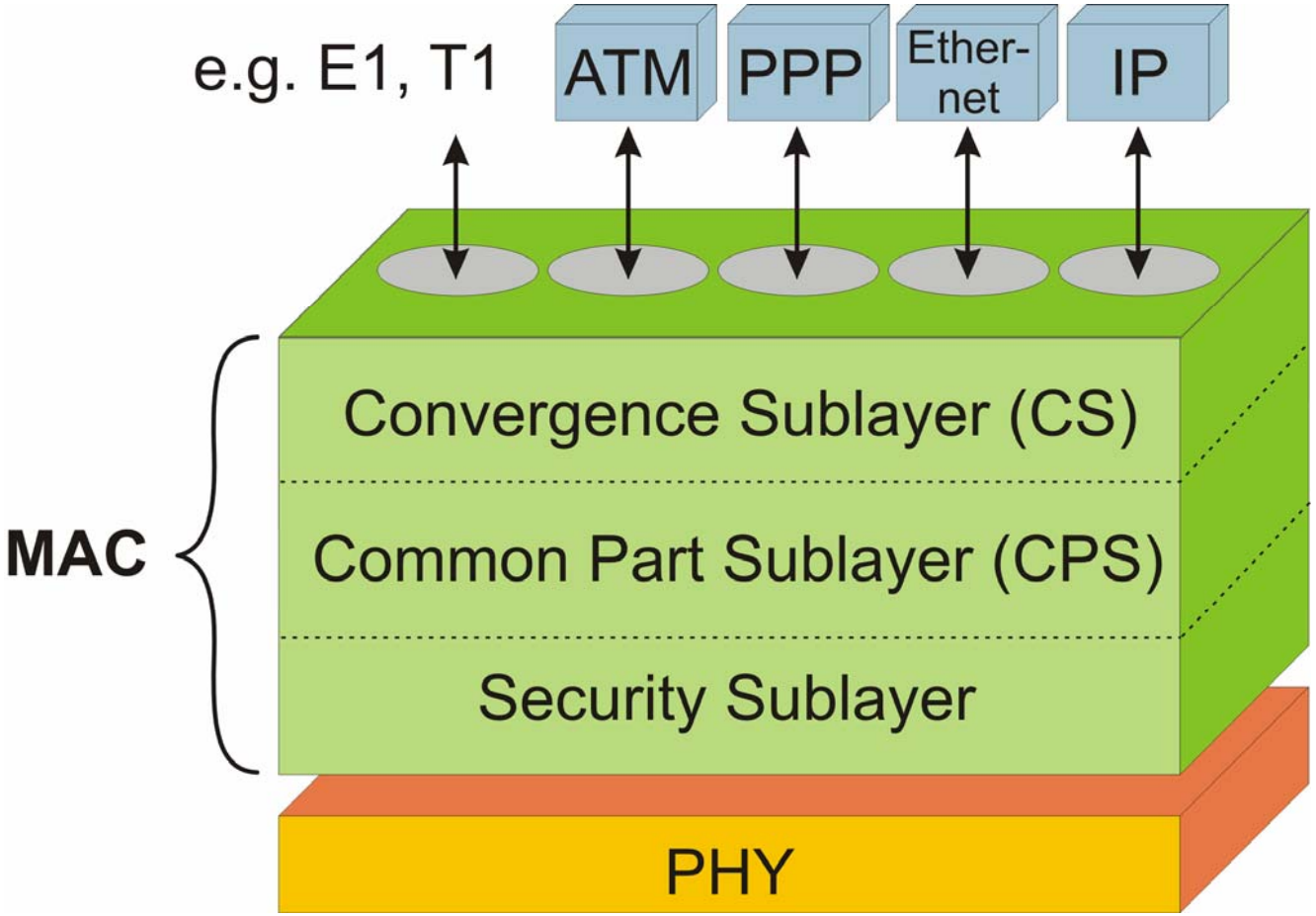
- **This simplest architecture option illustrates as example the provision of ATM connectivity through WIMAX / 802.16-2001 (Point-to-Point). Other application protocols could be for example IP, Ethernet or PPP.**
- **Note that the two SS's in the upper half distinguish between a user plane (⇔ ATM) and a control plane (⇔ IP) while the third SS in the lower half does not have an IP-based control plane.**
- **This additional control plane is an important feature of so called managed devices that can be controlled (e.g. SW-upgraded) by and through the TMN-network (Telecommunication Management Network) of the 802.16 network operator.**
- **SS's can be managed or unmanaged but they shall convey this capability to the network through the REG-REQ-message.**
  For a managed device, the BS will establish a secondary management connection (another CID (Connection Identifier)) to allow the control IP-traffic to be tunneled through.

Additional Information

⇒ The IP-address which is allocated to a managed device will most likely be a private IP-address.

Technology Overview

- **Overview of the Protocol Stack**



Technology Overview

Overview of the Protocol Stack

Note that any IEEE standard will only focus on and provide details of the PHY- and the MAC-layer. However, lots of functions that actually belong to radio link control (RLC) or radio resource control (RRC) are included in the IEEE 802.16 standard as part of the MAC-layer, most likely as part of the CPS (Common Part Sublayer).

Application Layer

WIMAX / IEEE 802.16 is suited to tunnel through between SS and BS PDU's from various application protocols like IP, Ethernet (IEEE 802.3), PPP or ATM. In addition, the standard is suited to operate as relay for E1- or T1- PCM-connections.

MAC-Layer (Medium Access Control)

The MAC-layer is divided into three sublayers. The security sublayer takes care of authentication and encryption while the common part sublayer fulfills all "real" MAC functions including those that many people would rather define within an RLC- or an RRC-layer.
Last but not least there is the convergence sublayer that streamlines and tailors user data PDU's for the transmission over an 802.16 physical link.

PHY-Layer (Physical Layer)

Depending on the very WIMAX / 802.16 variant, five different PHY's need to be distinguished:

⇒ The Wireless MAN-SC PHY for operation exclusively within the 10-66 GHZ frequency range.
⇒ The Wireless MAN-SCa PHY for operation exclusively within the 2-11 GHZ frequency range.
⇒ The Wireless MAN-OFDM PHY for operation exclusively within licensed bands of the 2-11 GHZ frequency range.
⇒ The Wireless MAN-OFDMA PHY for operation exclusively within the 2-11 GHZ frequency range.
⇒ The Wireless HUMAN-PHY for operation exclusively within the 2-11 GHZ frequency range.

[IEEE 802.16-2004 (1.3.4)]

Management

No management layer is illustrated but needs to be implemented as parallel protocol stack.
[IEEE 802.16-2004 (1.4)]