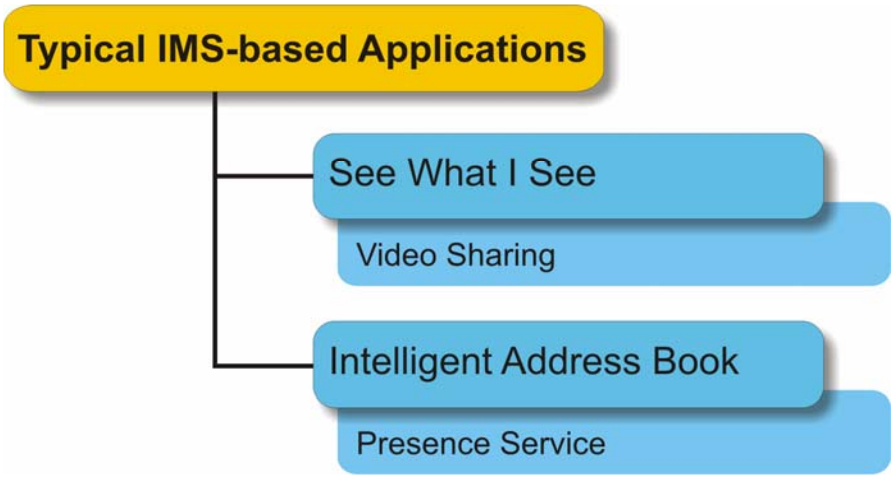
1

1.1 Commercial & Technical Reasons to introduce an IMS

1.1.1 Some typical IMS-based Applications for End Users



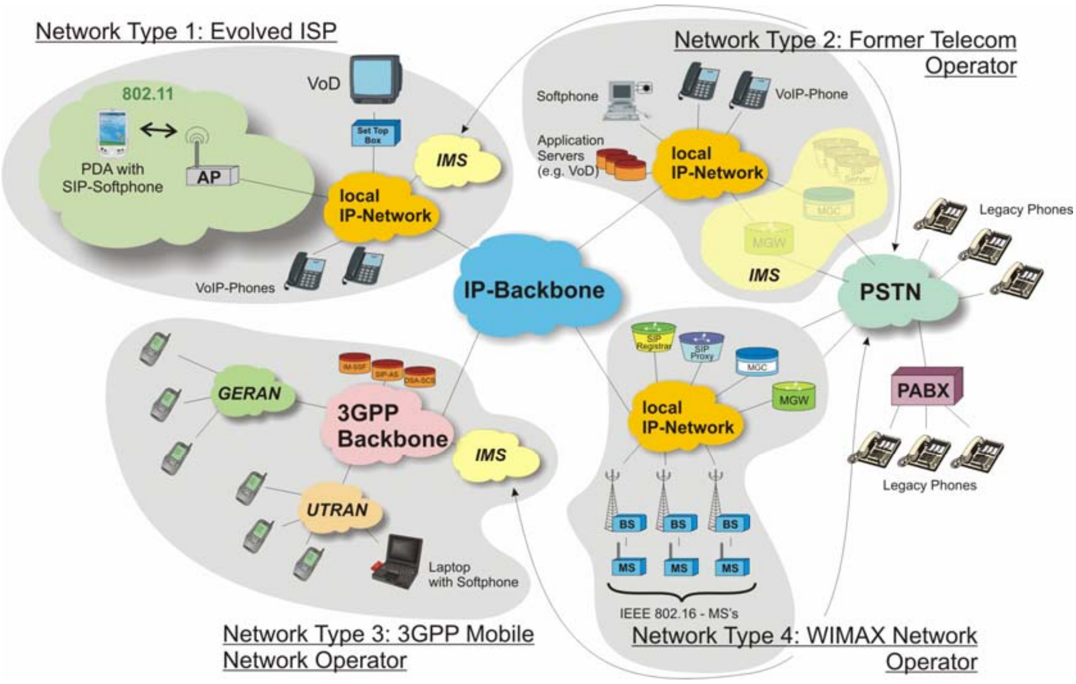
The objective of this section is to provide an idea about few different interesting services which are provided through IMS-based NGN's.

The key points of this section are:
1. The "See What I See" application allows the sharing of live video stream between mobile users.
2. The "Intelligent Address Book" application is enabled through presence service that allows a user to be informed about availability, reach ability and willingness of communication of another user.

At this point we have presented only a few IMS-based applications but a list of many other IMS-enabled services and applications is provided later in this chapter.

1

1.1.3 Next Generation Networks and their Components



The objective of section is to provide an overview of most likely configuration and interconnection of NGN's. This figure illustrates the interconnection of NGN's and also it provides the information about the services offered i.e. Triple-Play.

The key points of this section are:
1. Four types of access networks are shown in which there are two wireless access networks, one is based on 3GPP and other is based on WIMAX.
2. Presence of IMS and it's components within NGN's.
3. In the long run, only the operator owned IMS interconnects calling mobile subscribers towards the PSTN.

- **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 wire line 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 did not include the circuit-switched core network domain of the mobile network operator.

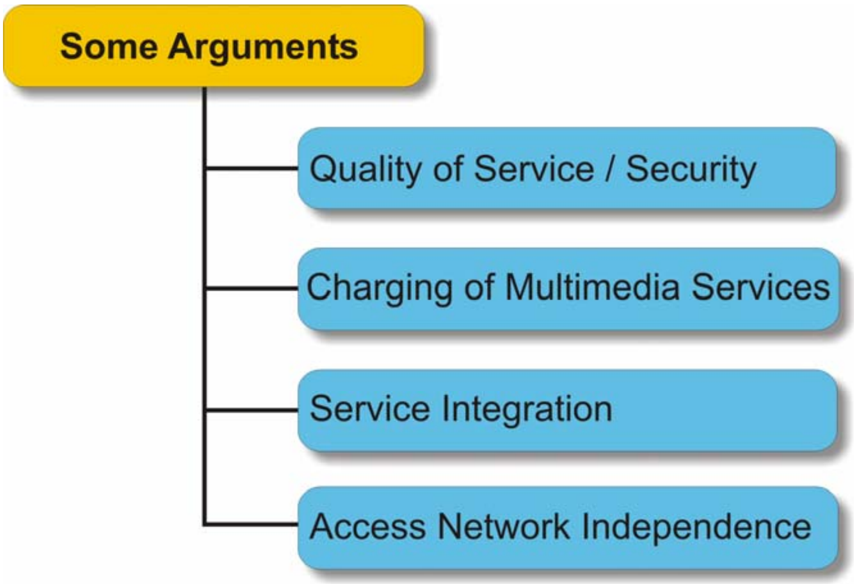
- **Network Type 4: WIMAX Network Operator**
  The upcoming WIMAX-network operators may emerge to a combination of a wireless network operator and an evolved ISP. WIMAX is a very strong DSL-competitor and WIMAX has the potential to become a cellular standard. Note that in case of network type 4 we did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

- **Abbreviations of this Section:**

3GPP	Third Generation Partnership Project (Collaboration between different standardization organizations (e.g. ARIB, ETSI) to define advanced mobile communications standards, responsible for UMTS)	**NGN**	Next Generation Networks
DSL	Digital Subscriber Line	**PSTN**	Public Switched Telephone Network
GERAN	GSM EDGE Radio Access Network	**SIP**	Session Initiation Protocol (RFC 3261)
IEEE	Institute of Electrical and Electronics Engineers	**UTRAN**	UMTS (Universal Mobile Telecommunication System)Terrestrial Radio Access Network
IMS	Internet Protocol Multimedia Core Network Subsystem (Rel. 5 onwards)	**WIMAX**	Worldwide Interoperability for Microwave Access (IEEE 802.16)
IP	Internet Protocol (RFC 791)	**VoIP**	Voice over Internet
ISP	Internet Service Provider	**MSs**	Mobile Stations
MGW	Media Gateway	**PDA**	Personal Digital Assistant

1

1.1.6.3 Why should one go for an IMS-based-Solution?



The objective of this section is to discuss through given arguments and in perspective of both network operator and consumers that why do we need the IMS.

The key points of this section are:
1. An operator with IMS can provide their customers a wide range of reliable, flexible and groundbreaking services that drives new revenues and creates competitive differentiation.
2. Guaranteed QoS, simple and built in charging system, integration of different services and independency to any specific access technology are those differences which formulate the requirement and significance of IMS over any existing systems and free products like, e.g., Skype, Messengers, x-lite with sipgate etc.

- **Quality of Service**
  The public internet providing free of charge services offers no guarantees about the amount of bandwidth a user gets for a particular connection or about the delay the packets experiences. For instance, the problem to maintain QoS with free VoIP is that the ISP or any other product who is offering free VoIP cannot easily differentiate free VoIP service from any further bandwidth consuming application in the access network. But on other hand, apart from bandwidth and latency issues, an operator with IMS and QoS aware IP-network can guarantee QoS since he knows that which service (e.g. VoIP) has been requested by the user. An IMS uses SIP-based network architecture and which provides Session-based control.

- **Charging of Multimedia services**
  IMS provides a flexible charging architecture, in terms of value, session-time or service and event based. The SIP/SDP-based network architecture of IMS allows operator to charge different multimedia services and provide reliable carrier-based services. It also creates new opportunities and can be much more attractive for end users. For example, video conferences can transfer large amount of data but the telecom operator can't charge them separately for this data. The flat-rate for all users would penalize the majority of users who are interested in downloading several Giga Bytes of movies per week.

- **Service Integration**
  IMS offers following advantages over existing system:
  ⇒ With IMS the integration of services is just easier due to centralized database.
  ⇒ Easier migration of applications from fixed to mobile users
  ⇒ Due to service independent Call Session Controllers, the CAPEX and OPEX is reduced.
  ⇒ Evolution to combinational services, e.g., the voice version of incoming text messages can be provided to blind users by combining instant messages and voice.
  ⇒ Faster deployment of new services based on standardized architecture
  ⇒ New services for all type of users (mobile, cable-TV or DSL-based) such as video sharing, push to talk over cellular, community services and content sharing etc.

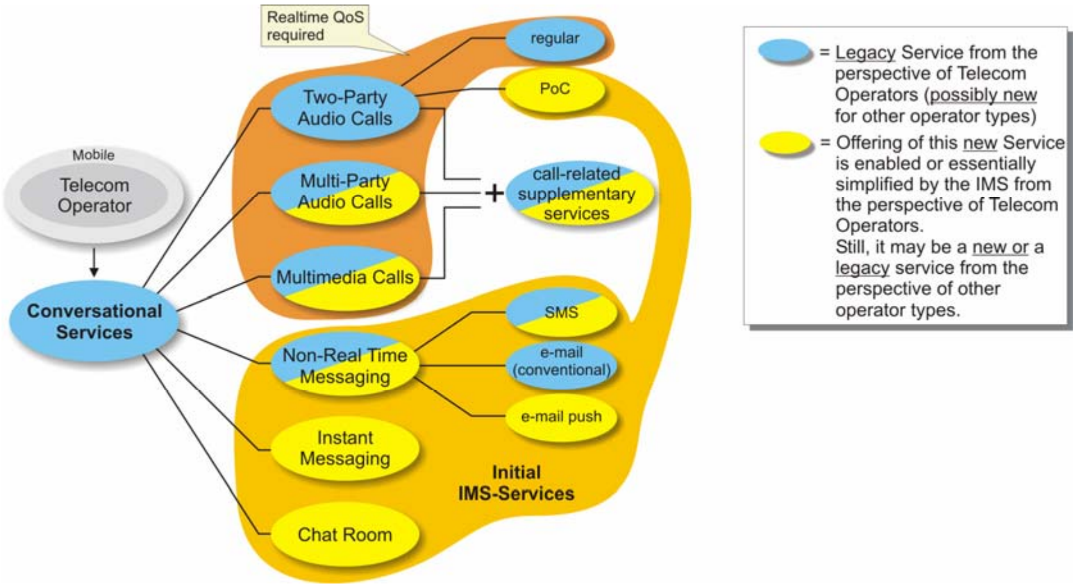
- **Access Network Independence**
  ⇒ The IMS core network is independent of any particular access technology.
  ⇒ Due to an IMS-based network the service delivery across various access technologies is simplified.

- **Abbreviations of this Section:**

CAPEX	Capital Expenditure	**QoS**	Quality of Service
DSL	Digital Subscriber Line	**SDP**	Session Description Protocol (RFC 2327, RFC 3266, RFC 3264)
IMS	Internet Protocol Multimedia Core Network Subsystem (Rel. 5 onwards)	**SIP**	Session Initiation Protocol (RFC 3261)
ISP	Internet Service Provider	**VoIP**	Voice over Internet Protocol
OPEX	Operational Expenditure	**TV**	Television

1

1.2.4.2 Conversational Services



The objective of this section is to depict the various different conversational services that may be offered through the IMS.

Key points of this section are:
1. The distinction between legacy conversational services (blue) and new conversational services (yellow) from the perspective of telecom operators.
2. The distinction between conversational services that do require real-time QoS and those do not.

Conversational services are the domain of telecom operators. Please note that the telecom operator may be a regular one or a mobile network operator.

- **Two-Party Audio Calls**
  As illustrated, this service type also contains PoC, because PoC is no longer a proprietary service when offered through the IMS.
  Note that (mobile) telecom offer close to perfect two-party audio call services without the IMS. It needs to be emphasized that for them the focus of the IMS therefore should not be on the provision of this kind of services, esp. initially. At a later stage, audio calls etc. may be migrated to the IMS to use only one service delivery platform.

- **Multiparty Audio Calls**
  The bullet is colored partly yellow because the conduction of multiparty calls becomes much more common, inherent and easy to use with the IMS.

- **Call-Related Supplementary Services**
  Any IMS-solution has to continue offering the legacy call-related supplementary services like caller representation, call on hold or call forwarding. However, the IMS will add new call-related supplementary services like "black lists" for callers or simultaneous forking.

- **Multimedia Calls**
  Through the IMS, the setup and selection of video calls will be simplified (although video calls have been around for quite some time). In addition, the IMS offers the combination of more media types than just audio + video. For instance, a service offering may combine audio + whiteboard + instant messaging to provide for advanced audio conferencing. Yet another example for multimedia calls is a "see what I see" service.

- **Non-Real Time Messaging**
  This bullet is colored partly yellow because some form of non-real time messaging has been there also prior to the IMS. However, SMS is (usually) a new service type for wire line telecom operators and definitely the famous e-mail push service is new.

- **Instant Messaging**
  Instant messaging has become an important means to communicate but it is a new type of service for telecom operators (both fixed and mobile).

- **Chat Rooms**
  The same applies what was said for instant messaging.

Please note the remarks on the right hand side of the graphics page. The color for new and legacy services only applies for telecom operators but not necessarily for other operator types, offering triple play services. One example is instant messaging which is a new service for telecom operators but which definitely is a legacy service from the perspective of ISP's.

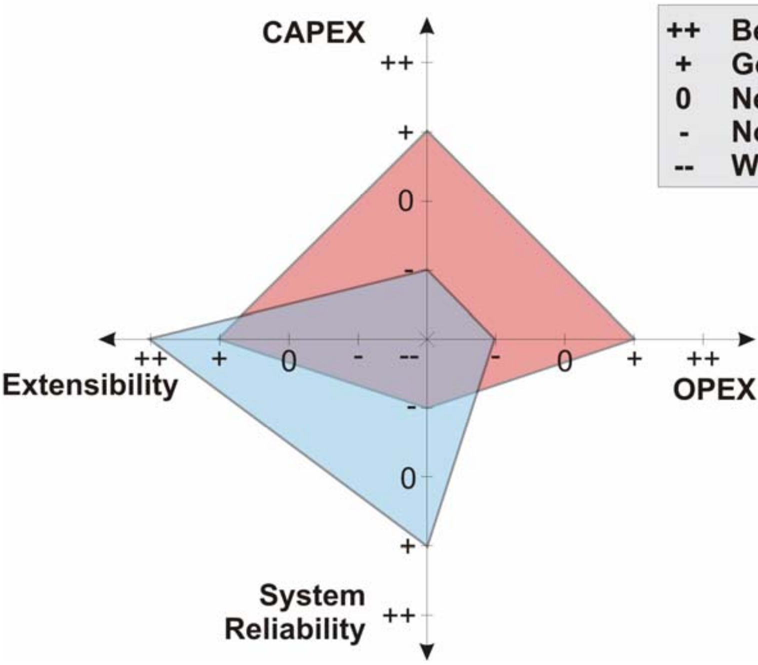
- **Abbreviations of this Section:**

IMS	Internet Protocol Multimedia Core Network Subsystem (Rel. 5 onwards)	**QoS**	Quality of Service
ISP	Internet Service Provider	**SMS**	Short Message Service (3GTS 24.011, 3GTS 23.040)
PoC	Push to talk over Cellular (3GTR 29.979 and various OMA-specifications)		

1

1.3.4.3 Comparison between Centralized and Split Architecture Approaches

Approaches \ Comparison Parameters	CAPEX	OPEX	System Reliability	Extensibility
Centralized Architecture	+	+	−	+
Split Architecture	−	−	+	++



++	Best / Better /Excellent
+	Good
0	Neutral
-	Not Good
--	Worst

The objective of this section is to compare two different IMS architecture implementation approaches with respect to different system evaluation parameters.

The key points of this section are:
1. With respect to CAPEX and OPEX, the centralized architecture approach to implement IMS in NGN's is better than split architecture approach.
2. With respect to System Reliability and Extensibility, the split architecture approach to implement IMS in NGN's is better than centralized architecture approach.

- **CAPEX**
  Capital expenditures are expenditures used by a company to acquire or upgrade physical assets such as equipment, property, industrial buildings. It refers to the cost of developing or providing non-consumable parts for the product, equipment or system.

- **OPEX**
  Operational expenditures are the on-going costs for running the product, equipment, business, or system. It is the counterpart of CAPEX. For example, the purchase of equipment or network components of telecom systems is the CAPEX, and the cost of different means which are used to run that equipment such as the cost of workers, electricity, facility expenses like rent and utilities are OPEX.

- **System Reliability**
  Reliability is the ability of a system to perform and maintain its functions in routine circumstances, as well as hostile or unexpected circumstances. It is the probability that the system will perform required functions for a specified period of time under stated conditions. It is also defined as the resistance to failure of a system and the capacity of a system to perform as designed.

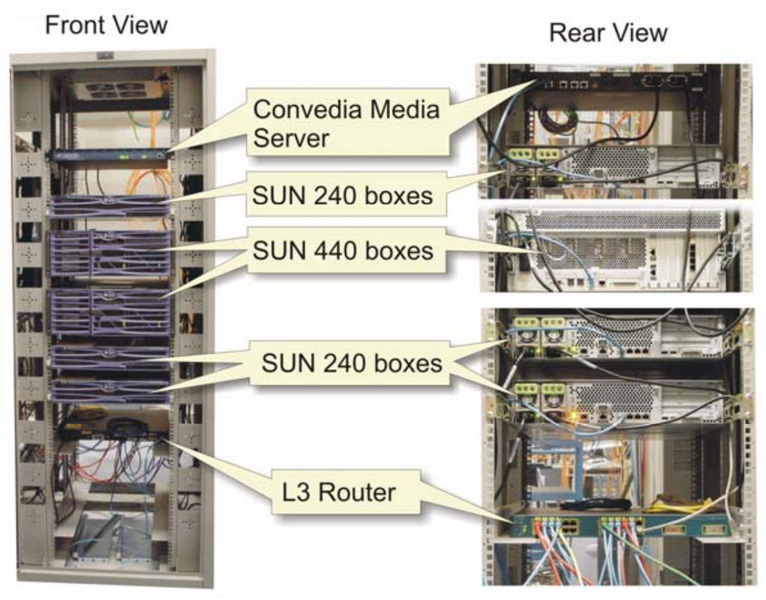
- **Extensibility**
  Extensibility is a systemic measure of the ability to extend a system and the level of effort required to implement the extension. It is a system design principle where the implementation takes into consideration future growth. In Systems Architecture, extensibility means that the system has been so architected that the design includes all of the hooks and mechanisms for expanding the system with new capabilities without having to make major changes to the system infrastructure.

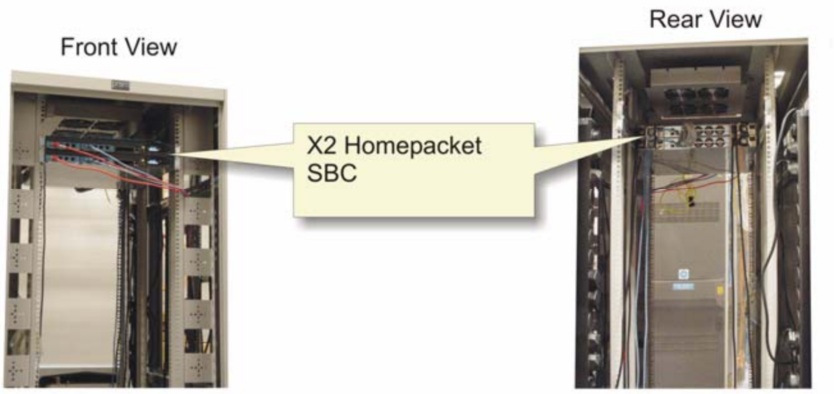
- **Abbreviations of this Section:**

CAPEX	Capital Expenditure	**NGN**	Next Generation Networks
IMS	Internet Protocol Multimedia Core Network Subsystem (Rel. 5 onwards)	**OPEX**	Operational Expenditure

1

1.4.2 Applications Servers hosted on SUN (240 & 440) Boxes for different Applications and Session Border Controllers–Front & Rear View





Note that an SBC is an advanced SIP-server with special functions. More details will be provided later.

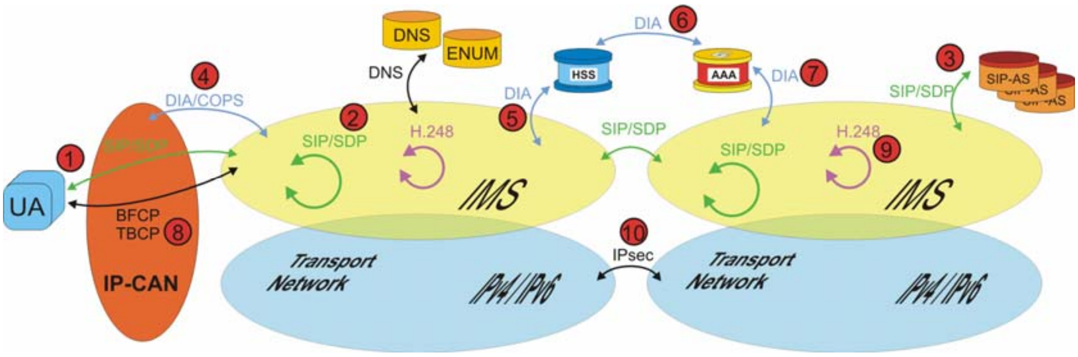
Room for your Notes

- **Abbreviations of this Section:**

L3	Layer 3 (network layer)	**SUN**	Originally stood for Stanford University Network
SBC	Session Border Controller (SIP term, usually a B2BUA with NAT-function and media gateway)		

2

2.1.2 Protocols within the IMS-Control Plane



The objective of this section is to highlight the various protocols that are used within the IMS-Control Plane.

The key points of this section are:
1. All protocols of IMS-control plane are used to carry signalling traffic.
2. None of these protocols is IMS-specific.

1 2 3

- **SIP and SDP**
  It is noticeable that SIP is used for end-user signaling (UNI) (bullet 1) as well as among SIP-proxies (NNI) (bullet 2) and towards application servers (bullet 3). However, SIP requires SDP to describe the media of a session and therefore, the previous statement also applies to SDP. [RFC 3261 (SIP), RFC 2327 (SDP) draft-ietf-mmusic-sdp-new-26.txt (SDP), RFC 3266, RFC 3264]

4 5

- **DIA (DIAMETER)**
  The DIAMETER Protocol (bullet 4 and 5) is very important as it allows the SIP-proxy servers to interrogate and interact with databases like the HSS (Home Subscriber Server). DIAMETER in general is there to exchange subscriber related information like:
  Bullet 5, 6 7: Is a subscriber authorized to use a service and provision of the authentication information for that subscriber etc.
  Bullet 4: QoS-Authorization over the Gq-interface. [RFC 3588, RFC 3589, http://www.diameter.org/, 3GTS 29.229, 3GTS 29.329]

4

- **COPS**
  The Common Open Policy Service Protocol is used for policing between the PDF and the PEP (bullet 4) [RFC 2748].

9

- **H.248 / MEGACO**
  H.248 / MEGACO (bullet 9) allow the MGC to control one ore more media gateways. Control relates particularly to the seizure and release of resources for user data transfer [ITU-T H.248, RFC 3015].

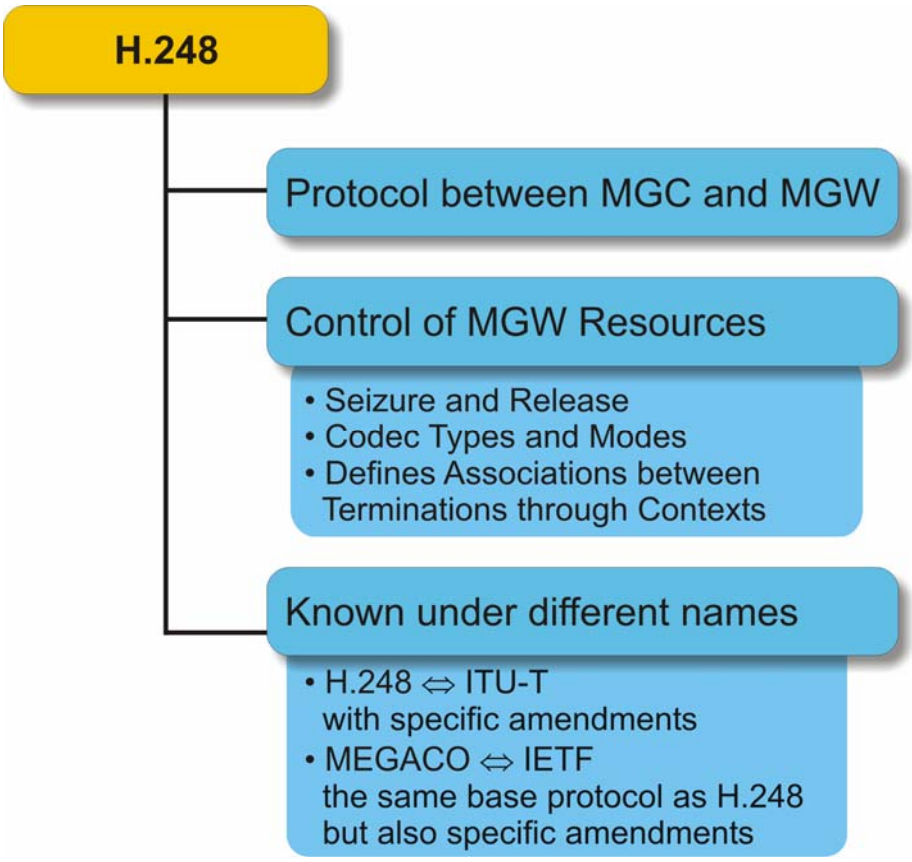
- **BFCP / TBCP** 8
  Binary Floor Control Protocol (bullet 8) and Talk Burst Control Protocol are used for floor control within the IMS. TBCP is restricted to use within the PoC-service [draft-ietf-xcon-bfcp-05].

- **IP, IPsec and TLS** 10
  The IMS uses IPv4 or IPv6 in the transport network and IPsec or TLS to provide for secure links between IMS-facilities.

- **Abbreviations of this Section:**

3GTS	3rd Generation Technical Specification	**PDF**	Policy Decision Function (Part of the IP Multimedia Subsystem)
BFCP	Binary Floor Control Protocol (draft-ietf-xcon-bfcp-05)	**PEP**	Policy Enforcement Point (3GTS 23.209)
COPS	Common Open Policy Service Protocol (RFC 2748)	**PoC**	Push to talk over Cellular (3GTR 29.979 and various OMA-specifications)
DIA	Diameter Protocol (RFC 3588, RFC 3589)	**QoS**	Quality of Service
HSS	Home Subscriber Server (3GTS 23.002). HSS replaces the HLR with 3GPP Rel. 5	**RFC**	Request for Comments (Internet Standards)
IMS	Internet Protocol Multimedia Core Network Subsystem (Rel. 5 onwards)	**SDP**	Session Description Protocol (RFC 2327, RFC 3266, RFC 3264)
IP	Internet Protocol (RFC 791)	**SIP**	Session Initiation Protocol (RFC 3261)
IPsec	Internet Protocol / secure (RFC 2401)	**TBCP**	Talk Burst Control Protocol
IPv4	Internet Protocol (version 4)	**TLS**	Transport Layer Security (RFC 2246 / RFC 3546 / formerly known as SSL or Secure Socket Layer)
IPv6	Internet Protocol (version 6)	**UNI**	User Network Interface
ITU-T	International Telecommunication Union – Telecommunication Sector	**NNI**	Network Node Interface
MEGACO	Media Gateway Control Protocol (ITU-T H.248 incl. Annex F – H and IETF RFC 3015)		

2.3.3 The H.248- / MEGACO-Protocol



The objective of this section is to introduce the H.248/MEGACO protocol which is used for the communication between media gateways and their controllers.

The key points of this section are:
1. The H.248-protocol from the ITU-T is actually the same protocol as MEGACO which is published by the IETF. Therefore, MEGACO / H.248 is a joined development of both organizations.
2. The H.248 / MEGACO-protocol is necessary, if the call control functions shall be physically located in a different device than the media provision functions. Therefore, H.248 / MEGACO is also referred to as Gateway Control Protocol.
3. This is the case, if the MSC's are replaced by MSC-Servers for the call control and MGW's for the media provision.

- **Principles of Media Gateway Operation**
  - ⇒ Media Gateways operate through so called contexts.
  - ⇒ Each context represents the association between different links that are interconnected through this context.
  - ⇒ The links are called terminations and represent e.g. AAL-2- or IP/UDP/RTP-bearer channels.
  - ⇒ Controlled by a MSC-S and through the H.248- / MEGACO-protocol, the MGW creates a context and adds terminations to this context.
  - ⇒ During the lifetime of a context, the properties (e.g. bandwidth) of these terminations may be modified. New terminations may be added while others are subtracted or moved to another context (handover).

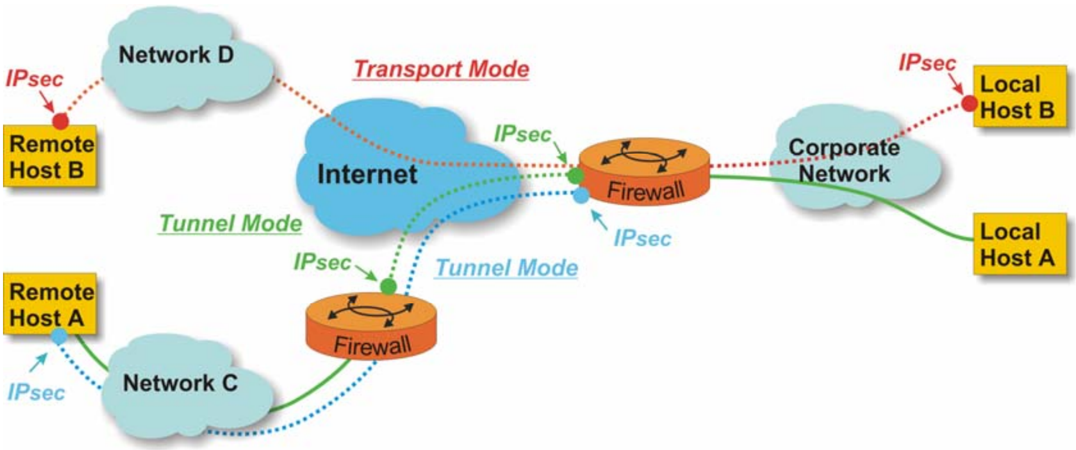
[ITU-T H248, IETF RFC 3015, 3GTS 29.232]

- **Abbreviations of this Section:**

3GTS	3rd Generation Technical Specification	**MGW**	Media Gateway
AAL-2	ATM Adaptation Layer 2 (for real-time services) (ITU-T I.363.2)	**MSC**	Mobile Services Switching Center
AMR	Adaptive Multirate Encoding (3GTS 26.090)	**MSC-S**	MSC-Server
IETF	Internet Engineering Task Force (www.ietf.org)	**PCM**	Pulse Code Modulation
IP	Internet Protocol (RFC 791)	**RFC**	Request for Comments Internet Standards)
ITU-T	International Telecommunication Union – Telecommunication Sector	**RTP**	Real-time Transport Protocol (RFC 3550, RFC 3551)
MEGACO	Media Gateway Control Protocol (ITU-T H.248 incl. Annex F – H and IETF RFC 3015)	**UDP**	User Datagram Protocol (RFC 768)
MGC	Media Gateway Controller		

2

2.3.6 IPsec



The objective of this section is to illustrate the basic principles of IPsec operation.

Key points of this section are:
1. IPsec enables the illustrated local hosts to exchange sensitive information over the insecure internet without the risk of MitM-attacks and avoiding eavesdropping.
2. IPsec may operate in transport mode (red) or in tunnel mode (green and blue) which results in different frame formats as we will present in the following sections.

- **IPsec in Tunnel Mode**
  The standard mode of VPN-operation is the tunnel mode. In tunnel mode, two network operators have negotiated a service level agreement (SLA) and have exchanged relevant security information. Whenever needed or permanently, an IPsec tunnel is established between the two networks. The end users who communicate between the two networks remain unaware of the security mode and of any details related to security.
  Another implementation of tunnel mode is indicated through the blue dotted line: Remote Host A has established an IPsec tunnel to the security gateway of the corporate network. This implementation is almost end-to-end as the communication through the blue link is secured also on its way through network C.

- **IPsec in Transport Mode**
  In transport mode we really have no VPN at all. As a matter of fact, in transport mode there needs to be an IPsec “tunnel” established between any two hosts on two different networks (in our example it is Remote Host B and Local Host B).

[RFC 4301, 4302, 4303]

Note that IPsec does not mandate or require any specific algorithms. IPsec only defines a framework to be used for secure IP-communication.

!

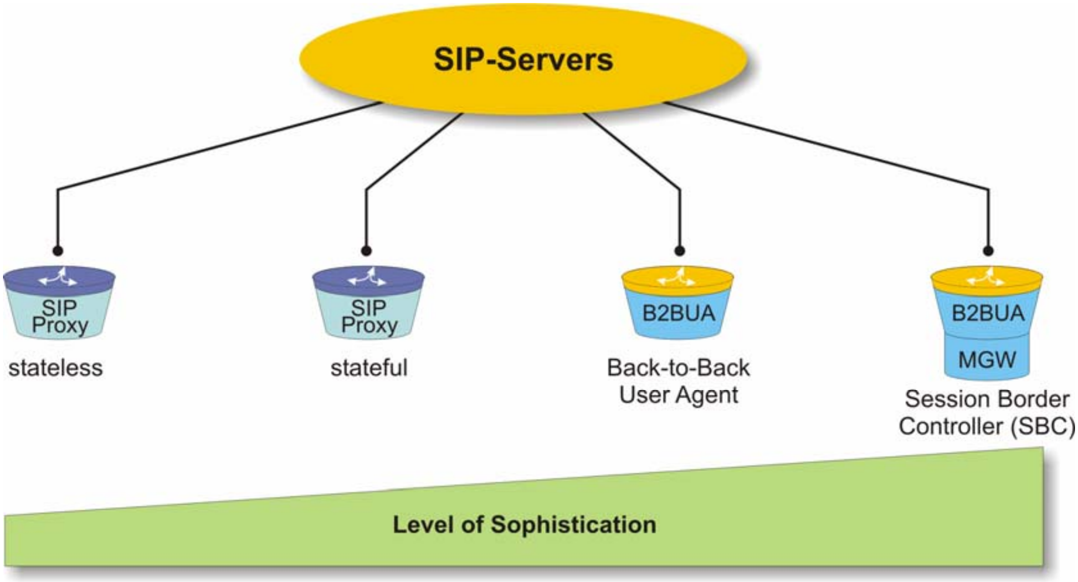
Room for your Notes

- **Abbreviations of this Section:**

IPsec	Internet Protocol / secure (RFC 2401)	**RFC**	Request for Comments (Internet Standards)
MitM	Man in the Middle	**VPN**	Virtual Private Network

3

3.1.2 Server Types (generic)



The objective of this section is to illustrate different types of SIP-servers with respect to their level of sophistication.

The key points of this section are:
1. A SIP-proxy is a device which is addressable by a SIP-user agent or by another SIP-proxy server through a SIP-URI.
2. SIP-proxies will relay SIP-messages somewhat closer to their destination.

- **Stateless SIP-Proxy Server**
  Unlike stateful proxies, stateless proxies do not maintain or observe the state of a SIP-transaction which is routed through them. That is why we did not include any UAC or UAS functions into the stateless proxy. Stateless proxies will also not retransmit SIP-messages. Still, stateless SIP-proxies will also inspect the content of SIP-messages and they may add header fields autonomously. However, like stateful SIP-proxies, a stateless SIP-proxy is not allowed to autonomously generate SIP-Requests. In contrast to stateful SIP-proxies, the stateless SIP-proxy cannot generate CANCEL-Requests. And stateless SIP-proxies cannot redirect a Request: INVITE-message to a new direction if they receive a redirection response (Response: 3XX) from a redirect server. And more, stateless proxies cannot be used for forking. More details about stateless SIP-proxies follow later in this section. [RFC 3261 (16.11)]

- **Stateful SIP-Proxy Server**
  In general, a SIP-proxy is a device which is addressable by a SIP-User Agent or by another SIP-proxy server through a SIP-URI (Uniform Resource Identifier). Usually, SIP-proxies will relay SIP-messages somewhat closer to their final destination. However, with one exception a SIP-proxy server is not allowed to generate SIP-requests autonomously. The exceptions are Request: CANCEL-messages which need to be generated by the proxy server e.g. after a called SIP-device has been ringing for some time and now the call shall be forked to the next possible device. Stateful SIP-proxy servers maintain and observe the state of every transaction which is routed through them. Note that they do not maintain dialog or call state, this is the domain of B2BUA's. Only Stateful proxies can be used as redirect server or as registrar. And only Stateful proxies can be used for forking. [RFC 3261 (16.2)]

- **SBC (Session Border Controller), B2BUA (Back-to-Back User Agent)**
  Note that the terms "Session Border Controller" or "SBC" have no representation in IETF standards as such.
  In practice, SBC's represent the combination of B2BUA's (which actually have been defined in RFC 3261) and media gateway like equipment that allows for media stream observation and even modification (e.g. change of codec type). Examples of SBC operation follow on the next side.
  Most importantly, B2BUA's represent SIP-proxy servers that act like user agents. That is, B2BUA's can autonomously generate SIP-Requests and they can autonomously terminate a session (through a Request: BYE) which is something that a SIP-proxy cannot do.
  When B2BUA's are also used for media transversal then they become SBC's.

What were the differences between stateful and staeless SIP-proxies?

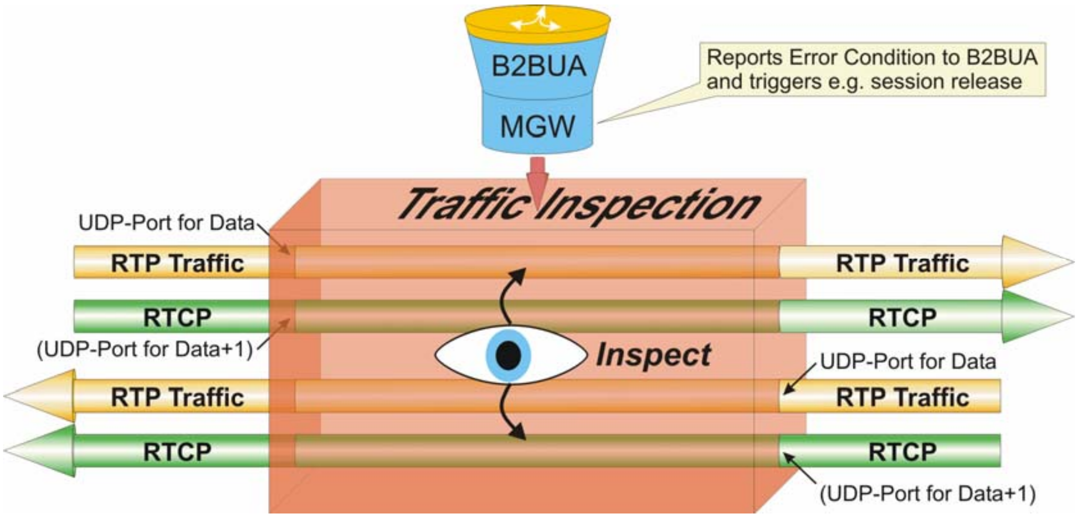
?

- **Abbreviations of this Section:**

B2BUA	Back-to-Back User Agent (SIP term / RFC 3261, RFC 3725)	**UAS**	User Agent Server (SIP-Term / RFC 3261)
IETF	Internet Engineering Task Force (www.ietf.org)	**URI**	Uniform Resource Identifier
RFC	Request for Comments (Internet Standards)	**SIP**	Session Initiation Protocol (RFC 3261)
SBC	Session Border Controller (SIP term, usually a B2BUA with NAT-function and media gateway)	**UAC**	User Agent Client (SIP-Term / RFC 3261)

3

3.1.5.2 Example: SBC for Traffic Inspection



The objective of this section is to illustrate an important task of traffic inspection or media stream observation performed by SBC.

The key points of this section are:
1. Traffic inspection is a legal requirement to provide for lawful interception.
2. The observation of the RTCP-reports may serve as means to improve session quality, e.g. through automatic codec type switching.

⇒ The SBC, combination of B2BUA and MGW, is best suited for this task.
⇒ RTCP has become more sophisticated and more powerful through the introduction of extended RTCP-reports RTCP XR RFC 3611 and through more sophisticated reporting options according to the internet draft draft-ietf-avt-rtcp-feedback-XX.txt.
⇒ If the Media Stream Observation reports back a fatal error of the media stream then it is the decision of the associated SIP-proxy server to terminate the session towards both peers.

Note that there are currently no rules as what needs to be considered a fatal error. It may for instance be that the MGW does not receive data packets for some O&M-configurable time.
[RFC 3611, RFC 4083 (14.1), draft-ietf-avt-rtcp-feedback-XX.txt]

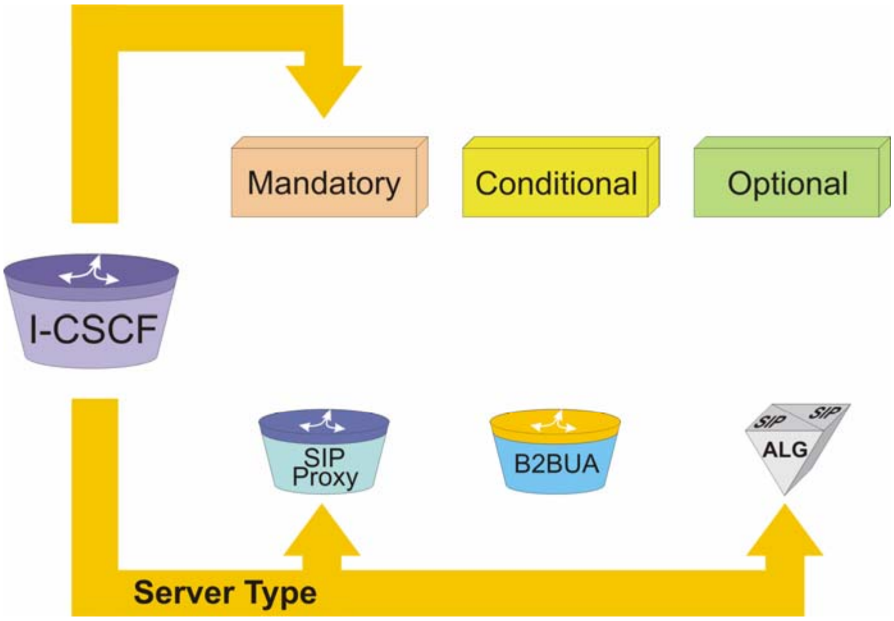
Room for your Notes

- **Abbreviations of this Section:**

B2BUA	Back-to-Back User Agent (SIP term / RFC 3261, RFC 3725)	**SBC**	Session Border Controller (SIP term, usually a B2BUA with NAT-function and media gateway)
MGW	Media Gateway	**SIP**	Session Initiation Protocol (RFC 3261)
O&M	Operation and Maintenance	**RTCP**	Real-time Transport Control Protocol
RFC	Request for Comments (Internet Standards)		

3

3.2.2.1 Characteristics of I-CSCF



The objective of this section is to illustrate the some genuine characteristics of I-CSCF in terms of its presence and type of the server in an IMS.

The key points of this section are:
1. The presence of the I-CSCF is a must in an IMS, considering its specific tasks of assignment of an S-CSCF during registration or routing an incoming transaction to the next hop.
2. I-CSCF needs to be a stateful SIP-proxy server [3GTS 24.229 (5.3.1.1), (5.3.2.1)]. That means that the I-CSCF needs to maintain transaction state. This applies in particular if topology hiding is applied.

⇒ Whether the I-CSCF incorporates in addition an IMS-ALG, depends on the necessity of IP-address conversion and NAT-interworking with external networks. In that respect, "external network" does not relate to the IP-CAN but rather to foreign IMS's, VoIP-networks and packet data networks in general.

3

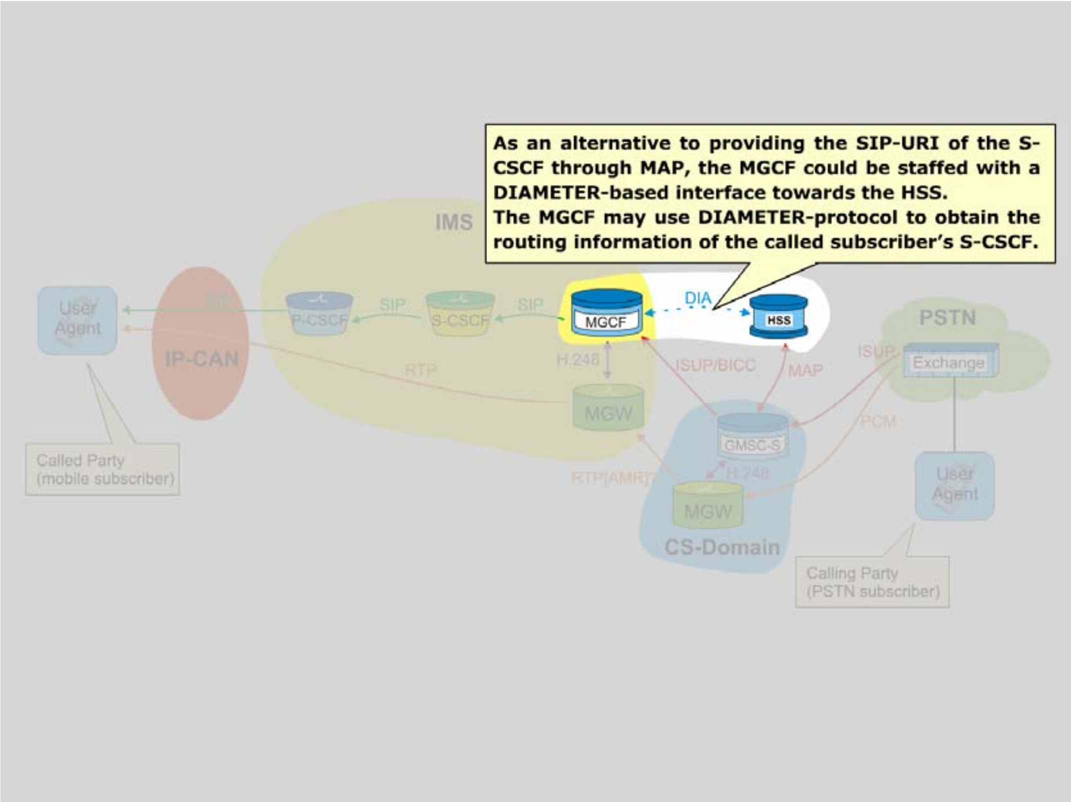
Room for your Notes

- **Abbreviations of this Section:**

3GTS	3rd Generation Technical Specification	**IP**	Internet Protocol (RFC 791)
ALG	Application Layer Gateway	**IP-CAN**	Internet Protocol - Connectivity Access Network (e.g. DSL, TV-Cable, WIMAX, UMTS)
CSCF	Call Session Control Function (SIP)	**NAT**	Network Address Translation (RFC 1631)
I-CSCF	Interrogating Call Session Control Function (SIP)	**S-CSCF**	Serving Call Session Control Function (SIP)
IMS	Internet Protocol Multimedia Core Network Subsystem (Rel. 5 onwards)	**SIP**	Session Initiation Protocol (RFC 3261)
		VoIP	Voice over Internet Protocol

3

3.3.4 IMS-Terminating Voice Call – Technical Realization (ctd)



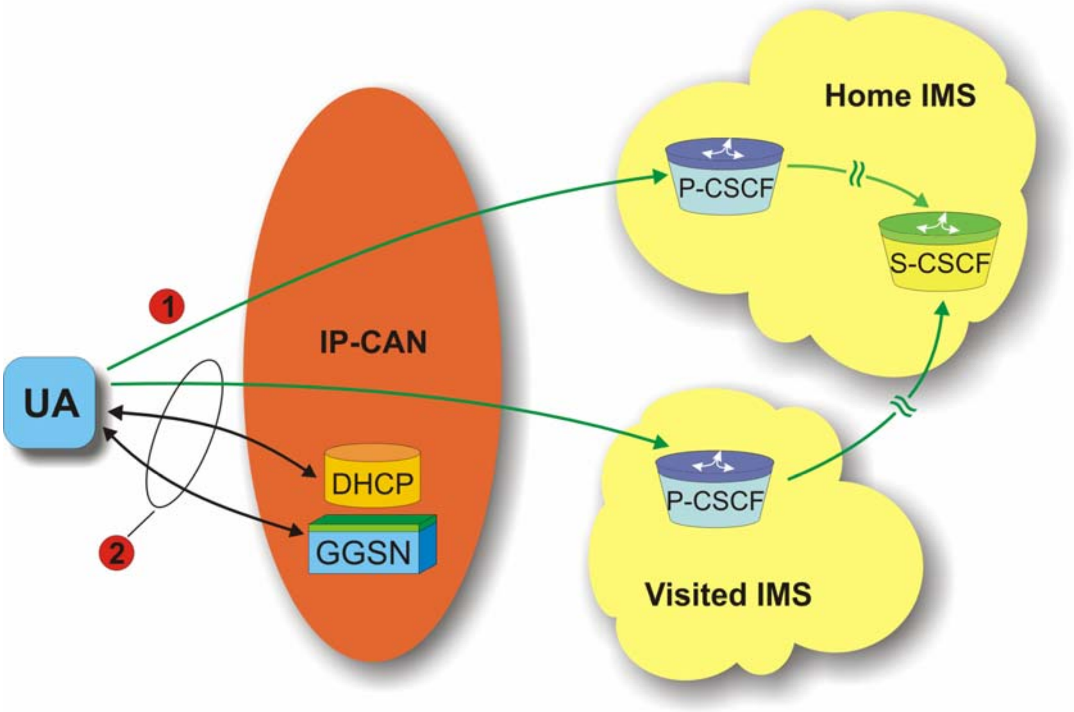
The objective of this section is to illustrate the next snapshot of the illustrated video clip.

Key point of this section are:
1. In case of non-3GPP-based networks without G-MSC, the incoming call could be directly routed towards an MGCF which in turn would need to ask the HSS for routing information.
2 Such an interface has not yet been defined.

The video clip can be downloaded through the internet. Please check with your vendor.

4

4.1.1 Different possibilities for the UA to find "its" Registrar



The objective of this section is to illustrate three different possible options for the UA to find its Registrar.

The key points of this section are:
1. Although the registrar may be accessed directly by the UA, it is more likely that some proxy like the P-CSCF will be accessed instead.
2. It is then the task of the proxy to route a registration message to the S-CSCF.

1

- **The "Preconfigured" Case**
  This represents the simplest option. The IP-address or FQDN (preferably) of the P-CSCF is hard coded into the software of the SIP-device or can be manually reconfigured by the user.

2

- **Option 2: SIP-Proxy Address is provided together with IP-address**
  Recent enhancements to DHCP allow a client to request the network's SIP-proxy address [RFC 3319 / RFC 3361]. In that case, the DHCP will of course provide the address of the very P-CSCF which is known to this IP-CAN. This is not necessarily the P-CSCF of the home IMS of the client. Of course, we don't want to preclude this although the figure gives this impression for simplicity.

Very interesting is the lower black arrow of option 2 which leads to a GGSN instead of a DHCP-server. This variant represents the GPRS/UMTS-specific way of obtaining an IP-address during PDP-context activation.
As through DHCP, the client may obtain his/her P-CSCF-address during PDP-context activation.

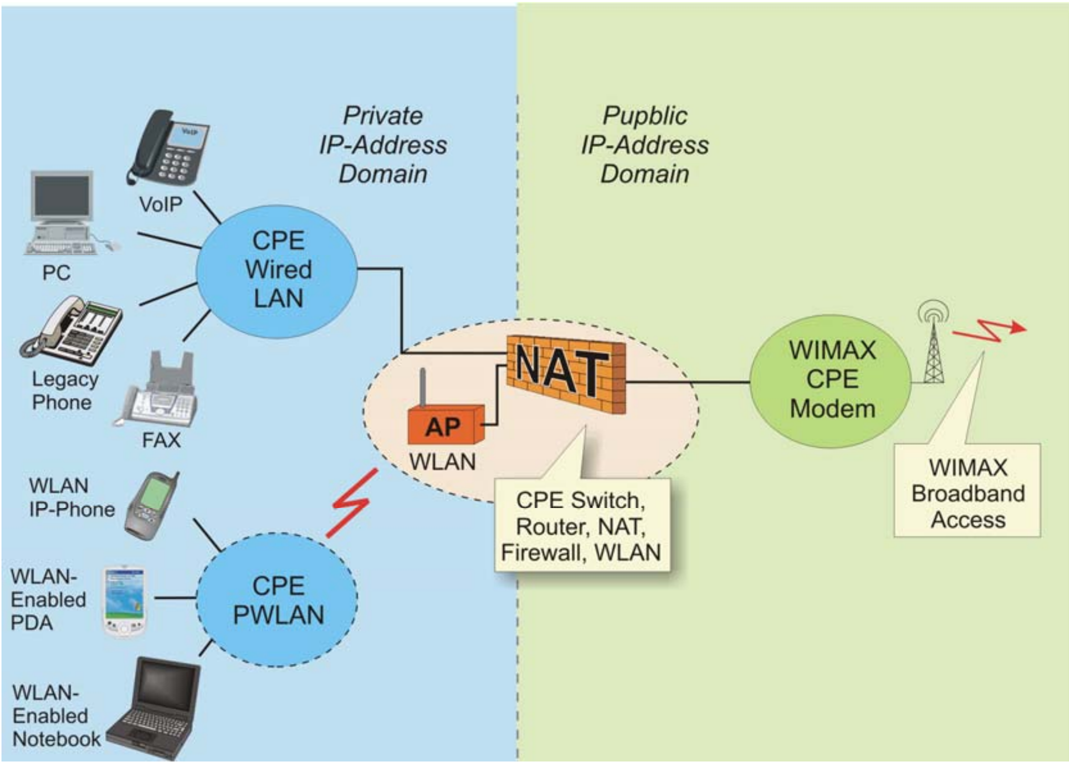
Room for your Notes

- **Abbreviations of this Section:**

CSCF	Call Session Control Function (SIP)	**IP-CAN**	Internet Protocol - Connectivity Access Network (e.g. DSL, TV-Cable, WIMAX, UMTS)
DHCP	Dynamic Host Configuration Protocol (RFC 2131)	**P-CSCF**	Proxy Call Session Control Function (SIP)
FQDN	Fully Qualified Domain Name. Fully qualified domain names consist of a host and a domain name whereas the domain name needs to include a top-level domain (e.g. 'de' or 'org'). Examples: 'www.inacon.de' and 'PC10.inacon.com' are fully qualified domain names. 'www' and 'PC10' represent the host, 'inacon' is the second-level domain, 'de' and 'com' are the top level domain.	**PDP**	Packet Data Protocol
GGSN	Gateway GPRS Support Node	**RFC**	Request for Comments (Internet Standards)
GPRS	General Packet Radio Service	**S-CSCF**	Serving Call Session Control Function (SIP)
IMS	Internet Protocol Multimedia Core Network Subsystem (Rel. 5 onwards)	**SIP**	Session Initiation Protocol (RFC 3261)
IP	Internet Protocol (RFC 791)	**UA**	User Agent (SIP-Term / RFC 3261)
		UMTS	Universal Mobile Telecommunication System

5

5.4 Customer Premises with WIMAX Access



The objective of this section is to provide an overview of the customer premise network architecture which is based on WIMAX access.

The key points of this section are:
1. Operator tends to create many wireless hot spots in different cities.
2. The architecture could be applied to both residential and business environments.
3. This is one possible option for wired and PWLAN end users to use WIMAX access.

⇒ A Public Wireless LAN or PWLAN is a region whereby users can access a network such as the Internet or company Intranet via a wireless enabled device providing they have sufficient authorization and authentication privileges to allow them access to the network. PWLANs are also known as WiFi zones, or hotspots.

⇒ The typical WiFi hot spot will feature then two to ten Access Points which are controlled by WLAN controllers.

⇒ This section describes the network design approach for a PWLAN access to be deployed by the operator in conjunction with IP MPLS core network with service provider voice capabilities.

⇒ The correct deployment configurations of standard equipment is needed for residential, small business, medium business, and large enterprise that allow, as much as possible, a “solution in a box” that is both easy to sell and easy to deploy.

Taken as separate functions, the following are the components which make up the customer premise network;

⇒ IP Broadband Network Access such as WIMAX

⇒ Customer Premise Home Gateway/Edge Router

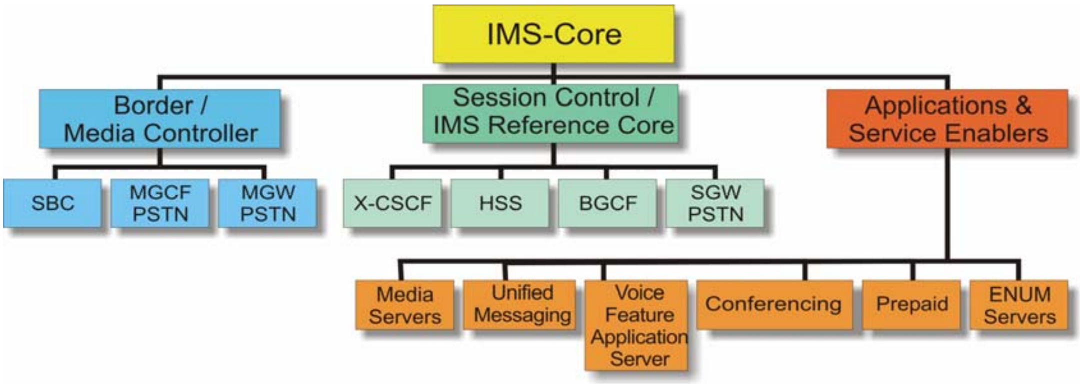
⇒ End user terminals e.g. IP Phone (fixed), Soft Client and IP Phone (WLAN).

Room for your Notes

- **Abbreviations of this Section:**

AP	Access Point (IEEE 802.11, 802.16)	**PDA**	Personal Digital Assistant
CPE	Customer Premises Equipment	**PWLAN**	Public Wireless Local Area Network
LAN	Local Area Network	**VoIP**	Voice over IP
MPLS	Multi Protocol Label Switching	**WIMAX**	Worldwide Interoperability for Microwave Access (IEEE 802.16)
NAT	Network Address Translation (RFC 1631)	**WLAN**	Wireless Local Area Network (IEEE 802.11)
PC	Personal Computer		

5.6 Distribution of IMS-Core Network Entities



The objective of this section is to illustrate the further distribution of IMS core network with respect to functionalities, usage and requirements of IMS-entities.

The key point of this section is that the operator's IMS-core network is further distributed so that it can be easily implemented into Control POPs and City POPs, i.e. followed split architecture approach.

.

Functioning details of some IMS-core elements are as follows:

- ⇒ HSS comprises the directory base of the IMS architecture.
- ⇒ Sylantro Application Server provides the Voice Feature Application Server for both residential and business (Centrex) hosted VoIP services. These provide the end-user with the traditional voice services they may be using today, as well as new multimedia services driven by innovation and enabled by the Internet.
- ⇒ Iperia Active Edge AS delivers voicemail features for both residential and business subscribers.
- ⇒ Ubiquity Speak Conferencing AS provides conferencing features.
- ⇒ Prepaid Server delivers prepaid features
- ⇒ ENUM Server provides SIP URI to TEL URI translation which is required for transporting calls in and out of the PSTN domain.
- ⇒ Media Servers and Media Gateways are used to transmit RTP traffic.
- ⇒ Media Servers comprising the different AS, e.g., Prepaid Servers
- ⇒ Sonus Media Gateway and Signaling Gateway provide full interconnection to existing circuit switched TDM networks and voice inter-domain operation, i.e. VoIP domain to PSTN domain.
- ⇒ SBC Provides the VoIP Core security and resolves the issue of providing VoIP services to the customer behind NAT.

Room for your Notes

- **Abbreviations of this Section:**

AS	Application Server	**PSTN**	Public Switched Telephone Network
BGCF	Breakout Gateway Control Function	**RTP**	Real-time Transport Protocol (RFC 3550, RFC 3551)
ENUM	E.164-telephone number to URI (Uniform Resource Identifier) translation (RFC 3761)	**SBC**	Session Border Controller (SIP term, usually a B2BUA with NAT-function and media gateway)
HSS	Home Subscriber Server (3GTS 23.002). HSS replaces the HLR with 3GPP Rel. 5	**SGW**	Signaling Gateway (SS7 IP)
IMS	Internet Protocol Multimedia Core Network Subsystem (Rel. 5 onwards)	**SIP**	Session Initiation Protocol (RFC 3261)
MGCF	Media Gateway Control Function	**TDM**	Time Division Multiplexing
MGW	Media Gateway	**URI**	Uniform Resource Identifier
NAT	Network Address Translation (RFC 1631)	**VoIP**	Voice over IP
		X-CSCF	Call Session Control Function (any, there is I-CSCF, P-CSCF and X-CSCF)