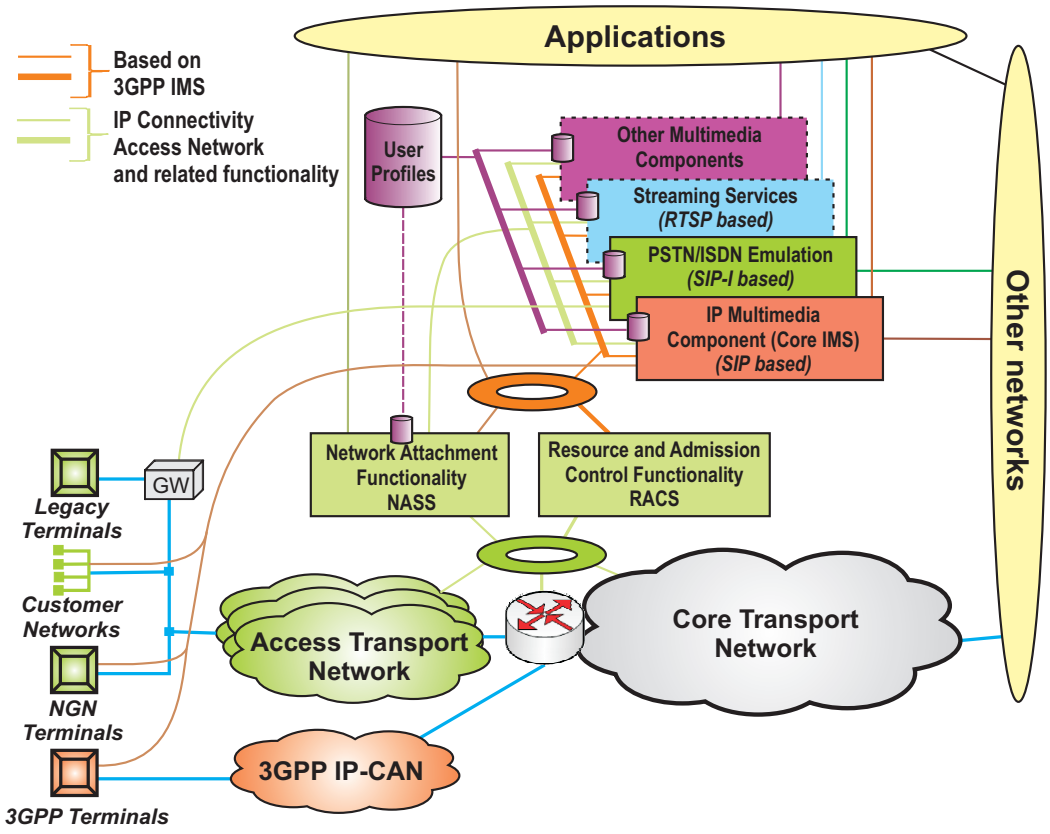
1.12 TISPAN

The TISPAN network architecture is based on 3GPP IMS, which is a basis for control and provision of the real-time conversation services (based on SIP protocol) [2], [9], [10]. 3GPP IMS architecture is extended in TISPAN NGN to support various types of access networks, such as xDSL, WLAN, etc.

TISPAN architecture is extended mainly by:

- Access networks control (QoS, access control and authentication),
- Co-ordination of various control subsystems via one transport network to control resources,
- Interworking and interoperability with public networks (legacy networks),
- Separation of the application layer from the connection control layer and the transport layer,
- Independence of access technologies from the call control layer and the application layer.

For services on other than SIP basis, the TISPAN NGN architecture can include other subsystems defined in TISPAN. Figure illustrates the NGN components and functionalities.



Architecture of a TISPAN NGN

1.13 Multimedia Services in NGN Environments

NGN Service Categorization

In parallel with standardization processes in the area of NGN architectures, the working groups of standardization institutions concentrate their work also to standardization activities in the area of new multimedia services and applications, like:

- categorization of NGN services and applications,
- service development processes, service implementation, service control and provisioning in the NGN environment, etc.

ITU-T Service Categorization

In the FGNGN WG1 Services and capabilities document the NGN services and applications categorization structure is introduced [11]. Actual set of services defined by ITU-T is introduced in this document:

1. Interactive-based services

- Real-time Conversational Voice services,
- Point to Point interactive multimedia services, including interactive real-time voice, video, white board and other media,
- Collaborative interactive communication services – multimedia conferences with files and applications sharing, e-learning, games, etc.
- Push to talk over NGN – PoN,
- *Instant messaging* (**IM**) and Messaging services (SMS, MMS, etc.),
- Group Messaging,
- Existing PSTN/ISDN emulation and simulation services,
- Data communication services (data transmission, fax, e-mail box, etc.),
- Data retrieval applications – telesoftware,
- Online applications (e.g. E-business),
- Voice control services.

2. Non Interactive-based Services

- Content delivery services (audio video streams creation, digital TV distribution services, financial information distribution, distribution of professional and medical images, e-publishing, etc.),
- Sensor Network services,
- Push services,
- Remote control/tele-action services, such as home applications control, telemetry, alarms etc.),
- Broadcast/Multicast Services,
- Over-the-Network Device Management.

3. Both Interactive-based and Non Interactive-based Services

- *Virtual Private Network* (**VPN**) services,
- Hosted and transit services for enterprises) – IP Centrex, etc.,
- Information services (e.g. traffic services-situation on the road, train/buss tickets, advanced push services, etc.),
- Presence and general notification services,
- 3GPP Release and 6/3GPP2 Release A OSA-based services.

4. Network Services

- *Basic Transport Service* (**BTS**),
- *Enhanced Transport Service* (**ETS**).

5. Regulated Services

- Emergency Telecommunication Services – citizen-department, department-department, department-citizen,
- Lawful Intercept Services,
- Broadcast Emergency Alerting Services.

ETSI Service Categorization

1. IP multimedia services

- IP multimedia applications,
- PSTN/ISDN simulation services – 3rd class,
- Instant messaging service,
- Presence service,
- Location service,
- Video Telephony service.

2. PSTN/ISDN Emulation services

3. Regulated services for both IP multimedia and PSTN/ISDN emulation

- Lawful Intercept Services,
- Emergency Call Services,
- Malicious Communication Identity Services,
- Anonymous Communication Rejection Services.

1.14 NGN Service Capabilities

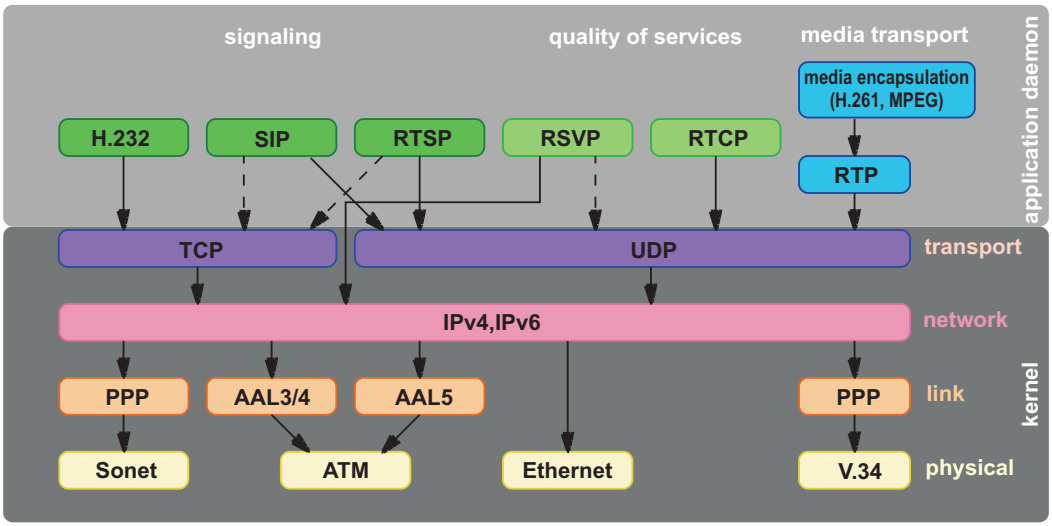
NGN platform should be able to provide the capabilities (infrastructure, protocols, etc.), so that it should be possible to develop, deploy/implement and manage all types of services (known and expected) [1], [12]. This involve the possibility to apply different types of media (audio, video, text, data), different types of encoding techniques, data services, conversation services, user and group transmission services, messaging services, real-time and Non-real time Conversational Voice services, data communication services, delay sensitive services, delay non sensitive services, etc. These types of services required the different speed of communication connection (from some kbps till hundreds of Mbps), which are required for the given service. These requirements have to be supported by the capabilities of the transport technologies.

+ One of the expected advantages of the NGN platform is the user comfortable and flexible access and control of multimedia services. At some time the NGN should provide the effective interface for service development, service providing and service management.

1.15 NGN Protocols

NGN protocol stack

The best way to show the functions of individual protocols in the hierarchy of NGN protocols platforms supporting voice transport over the packet networks or controlling of elements in NGN architecture is shown on Figure below with depicting the individual protocols and the OSI reference model layers they belong to.



Protocols for NGN

The protocols for the converged technologies and NGN platform can be divided into the following groups [4], [10], [12], [13], [14]:

- call control protocols (VoP signaling from the telecommunication point of view): SIP/SDP, H.323 [10], [12], [13],
- media gateway control protocols (components of the distributed VoP architecture): MGCP, Megaco/H.248 (protocol approved by both IETF and ITU-T),
- protocols for signaling transport: SIGTRAN, BICC, SIP-T, SIP-I,
- transport protocols: RTP, RTCP (in the sense of media transfer not RM OSI, as otherwise TCP/IP or UDP/IP is used for all),
- protocols for QoS support: RSVP, RTCP (RTCP is a transport one, but allows QoS support as well).

Other support protocols:

- DHCP, ENUM, DSN, COPS,

- **RTSP** (*Real-Time Streaming Protocol*) – protocol for creation of streams in the real time,
- IGMP/MLD.

1.16 Fundamental NGN Protocols

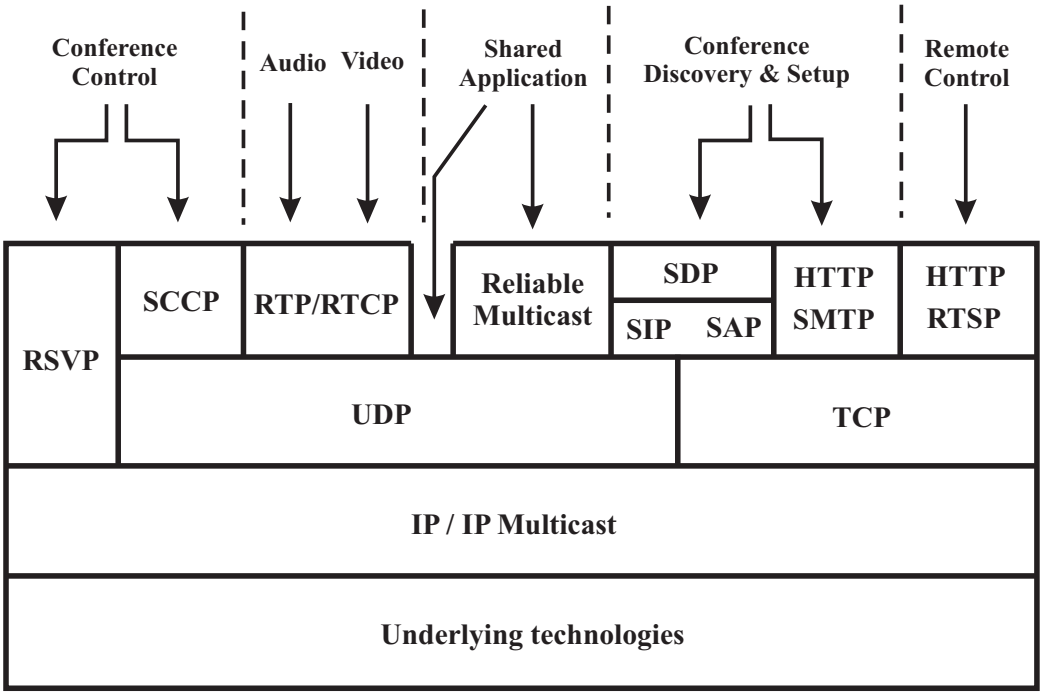
SIP protocol

Session Initiation Protocol (**SIP**) is an application-layer control protocol that handles the setup, modification, and tear-down of multimedia sessions. Media can be added to (and removed from) an existing session. SIP is used in combination with other protocols to describe the session characteristics to potential session participants. SIP is based on a request and response transaction model similar to HTTP. Each transaction consists of a request that invokes a particular method or a function on the server and at least one response.

SIP supports five facets of establishing and terminating multimedia communications:

- User location: determination of the end system to be used for communication;
- User availability: determination of the willingness of the called party to engage in communications;
- User capabilities: determination of the media and media parameters to be used;
- Session setup: "ringing", establishment of session parameters at both called and calling party;
- Session management: including transfer and termination of sessions, modifying session parameters, and invoking services.

SIP is a text-based protocol suggested and standardized in RFC 3261. SIP has been proposed as a part of a unit based of following protocols.



SIP protocol stack

Consequential protocols

A lot of SIP functions depend from other protocols. SIP defines establishment, termination and call modification and SIP use other protocols as *Real-time Transport Protocol* (**RTP**) for transporting real-time data and providing QoS feedback, the *Real-Time Streaming Protocol* (**RTSP**) for controlling delivery of streaming media, the *Media Gateway Control Protocol* (**MEGACO**) for controlling gateways to the *Public Switched Telephone Network* (**PSTN**), and the *Session Description Protocol* (**SDP**) for describing multimedia sessions. Therefore, SIP should be used in conjunction with other protocols in order to provide complete services to the users. However, the basic functionality and operation of SIP does not depend on any of these protocols.

SDP

SDP (*Session Description Protocol*) [4] is intended for describing multimedia sessions for the purposes of session announcement, session invitation, and other forms of multimedia session initiation.

When initiating multimedia teleconferences, voice-over-IP calls, streaming of video, or other sessions, there is a requirement to convey media details, transport addresses, and other session description meta data to the participants. SDP provides a standard representation for such information, irrespective of how that information is transported. SDP is intended to be general purpose so that it can be used in a wide range of network environments and applications. However, it is

not intended to support negotiation of session content or media encodings: this is viewed as outside the scope of session description.

An SDP session description includes the following:

- Session name and purpose
- Time(s) the session is active
- The media comprising the session
- Information needed to receive those media (addresses, ports, formats, etc.)

As resources necessary to participate in a session may be limited, some additional information may also be desirable:

- Information about the bandwidth to be used by the session,
- Contact information for the person responsible for the session.

RTP

The goal of this part is to present **RTP** (*Real Time Transport Protocol*) [14] in the way that it will be easily understandable also by a beginner. It contains deeper description of the main RTP protocol, but also protocols that stand next to RTP, cooperate with it and fill its gaps. The structure of RTP will be shown, to introduce the protocol body to the reader with a close view of its parts and theirs functions.

RTP provides end-to-end delivery services suitable for applications transmitting real-time data, such as audio, video or simulation data, over multicast or unicast network services. Real-time means that not only correct results are required, but also a sufficient time in which the result is delivered. That is why the delivery of the audio or video data is typically delay sensitive. According to this RTP use timestamp and control mechanisms for synchronizing different streams with timing properties.

RTCP

RTCP (*Real-time Transport Control Protocol*) [4] is an application layer protocol designed to control of data delivery in real-time and to measure the QoS. It is defined in RFC 3550 published in July 2003. RTP protocol uses the RTCP protocol, which transports the following additional information for the management of the session. RTCP is based on the periodic transmission of control packets to all participants in the session. The underlying protocol must provide multiplexing of the data and control packets, like UDP protocol that allows the multiplexing of RTP data packets and RTCP control packets. RTCP protocol requires the sending of information periodically by the participants of the session.

RTP packets only transport user's data, whereas RTCP packets only transport in real time the supervision.

Protocol RTCP performs these principal functions:

- Provide the information about the quality of the session (QOS) by means of feedback, which include the number of lost packets, the time return ticket and the gigue.
- Keep a trace of all the participants by a persistent transport-level identifier called CNAME (Canonical Name). Because SSRC (Synchronization Source Identifier) may change if a conflict or program restart occurs.

Control the media flow and adapt it to all the participants of the RTP session. By having each participant send its control packets to all the others, each can independently observe the number of participants. This information is used to calculate the rate at which the packets are sent.

DIAMETER

DIAMETER [4] is a member of "AAA" protocols collection, derived from its predecessor RADIUS protocol. It is a peer to peer protocol , used for handling service requests such as user validation, network resource control, connection and session management, wireless or roaming charging, billing applications etc.

Diameter sessions consist of exchange of commands and AVPs between servers and clients and unlike Radius, uses peer to peer architecture rather than more classic client/server scheme. Each node may initiate a message (request) at any time, as example, server may abort a service to specific user. Diameter is defined in terms of base protocol and a set of applications. This design allows protocol to be extended for new access technologies. The base protocol provides basic mechanism for reliable transport, delivery and error handling.

MEGACO/H.248

This protocol has been established to cover the need of IP networks and services to interoperate with traditional networks (e.g. PSTN) and provide the same services over both types of networks (IP, Traditional). This enables separation of call control from media conversion. Megaco/H.248 is defined as master / slave architecture based protocol which is used for communication between **MGC** (*Media Gateway Controller*, sometimes called a call agent or softswitch, which dictates the service logic of that traffic) and one or more decomposed **MG**s (*Media Gateways*), which converts circuit-switched voice to packet-based traffic.

Megaco/H.248 instructs an MG to connect streams coming from outside a packet or cell data network onto a packet or cell stream such as RTP. Megaco/H.248 is similar to MGCP from an architectural standpoint and the controller-to-gateway relationship, but Megaco/H.248 supports a broader range of networks, such as ATM.

SIGTRAN

In view of functionality and performance the user make high demands on modern telecommunication networks. Using **IP** (*Internet Protocol*) signaling messages will be transmitted over **TCP** (*Transmission Control Protocol*) or **UDP** (*User Datagram Protocol*). These transport protocols are not designed to meet the requirements given by a signaling system used in a circuit switched network like **PSTN/ISDN** (*Public Switched Telephone Network/Integrated Services Digital Network*). So the working group SIGTRAN was founded by the **IETF** (*Internet Engineering Task Force*) to develop a new protocol, based on IP, in consideration of given requirements by the existing switched telephone network.

This protocol, named **SCTP** (*Stream Control Transmission Protocol*) has some advantages in comparison to TCP. The SCTP offers a fundament to initiate and run secured transport connections using IP networks to transmit signaling information. Based on SCTP, several adaptation layers enable the transmission of upper layer protocols, i.e. **ISUP** (*ISDN User Part*), **SCCP** (*Signaling Connection Control Part*) and **DSS1** (*Digital Subscriber System No. 1*).

1.17 Supporting NGN Protocols

DHCP

DHCP (*Dynamic Host Configuration Protocol*) evolved from the BOOT protocol (BOOTP). Both protocols are described in RFC 2131 (DHCP) and RFC 951 (BOOTP).

DHCP includes all features known from BOOTP, that means an *Internet Software Consortium* (**ISC**) DHCP includes a BOOTP server and additional features along with a dynamic address assignment. Both protocols act for IP address assignment to nodes.

Therefore, the un-configured IP node sends a request for an IP address to a DHCP server. Then this DHCP server assigns an IP address to the client. Furthermore, this answer includes e.g. domain-name, IP address of the name-server or IP address from a router. The transmission of all configuration parameters will be proceeded automatically, depending of the chosen method.

DNS

The **DNS** (*Domain Name System*) protocol is used to link IP addresses with domain names. Usually, it is more convenient for people to remember names (ngnlab.eu) than IP addresses (147.175.103.213). IP addresses are required by the third layer of the network model to deliver the application data through networks. This chapter will highlight SIP/IMS specific use of DNS and not introduce the protocol itself.

Besides only storing a mapping between IP address and domain name, DNS contains additional information using various record types. DNS can handle for example certificate records, location information records, service information records and much more.

HTTP

The *Hypertext Transfer Protocol* (**HTTP**) is application protocol using the request/response mechanisms and is one of the most used protocols on Internet for web services.

A client sends a request to the server in the form of a request method, URI, and protocol version, followed by a **MIME**-like message (*Multipurpose Internet Mail Extensions*) containing request parameters and body content over a TCP connection with a server (HTTP session). Server is replay with response containing status line including the message's protocol version and a success or error code, followed by a MIME-like message containing server information, metadata and body content.

XML

In the following sections, **XML** (*Extensible Markup Language*) and its concept will be introduced. The protocol has been standardized by the **W3C** (*World Wide Web Consortium*). This section will not go into the very details of the protocol itself. It will rather provide the basics to understand the protocols which are based on XML. XML is a main mechanism for representing structured data. The data in XML documents is represented by a tree with nested elements. Each note in the tree represents an element.

Elements can have attributes, but they are not mandatory. Furthermore, so called "leaf" elements can contain text content. XML documents require a declaration with version and encoding mandatory at the beginning. After this declaration, the elements and the XML encapsulated data itself follow. The elements, which can be used, are defined by the XML schema or **DTD** (*Document Type Definition*). As different and more definitions can be used within one document, XML is extensible.

XCAP

XCAP (*XML Configuration Access Protocol*) allows clients to read, write and modify data stored in XML format on a server. This can be done by mapping XML document sub-trees and element attributes to HTTP URIs which grants direct access, as for the reason that all content discussed so far is held in XML "containers". The XML files are stored on a so called **XDMS** (*XML Document Management Server*), which is usually a normal HTTP server. The standard describes the interface between client application and the server managing the XML data (e.g. presence resource lists or authorization data for presence management).

SOAP

SOAP (*Simple Object Access Protocol*) is also an application layer protocol. The protocol is used for the communication between applications over the internet. SOAP uses HTTP as lower transport layer protocol.

\+ The advantage using HTTP is its support by many applications (browsers, servers, mobile phones) and its easy and cheap implementation. Other protocols for remote communication do not join this advantage.

CORBA

CORBA (*Common Object Request Broker Architecture*) is also a standard that defines a protocol for remote procedure communication. It is defined by the **OMG** (*Object Management Group*). The core of CORBA is the so called **ORB** (*Object Request Broker*). The ORB is the middle-ware that describes the client/server relationship for the communication. The ORB is responsible to:

- Intercept a call from the client
- Find the correct object
- Pass it the parameters
- Invoke its method
- Return the results to the client

Thus, the process seems transparent to the client. It uses only the communication via CORBA. The realization of the actual distributed application does not need to be specified any further. The only standard required for the actual communication is the communication standard.

VoiceXML

VoiceXML is designed for creating audio dialogs that feature synthesized speech, digitized audio, recognition of spoken and **DTMF** (*Dual-Tone Multi-Frequency*) key input, recording of spoken input, telephony, and mixed initiative conversations. Its major goal is to bring the advantages of Web-based development and content delivery to interactive voice response applications.

The top-level element is of the XML description file is the <vxml> tag. It can contain two types of dialogues:

- Forms – To present information and gather input
- Menus – To choose the next step

1.18 Multimedia Services Control Protocol

MPEG is a standard for "the generic coding of moving pictures and associated audio information. The function of MPEG is to take analogue or digital video signals and convert them into packets of digital information that are more efficiently transported on modern networks This process of converting audio and video signal to digital form is called compression (or coding). Opposite process is called decompression (or decoding) when digital audio and video signal is converted to analog form. MPEG is a system for compression and encoding of digital multimedia content. MPEG standard compresses the video and audio into much less information as it needed before, consuming less transmission bandwidth. Level of compression depends on bandwidth requirements and also on level of quality.

MPEG 1

The default size for an MPEG-1 video is 352x240 at 30 fps for NTSC (352x288 at 25 fps for PAL sources). These were designed to give the correct 4:3 aspect ratio when displayed on the rectangular pixels of TV screens. For a computer-based viewing audience, 320x240 square pixels give the same aspect ratio. MPEG-1 delivers roughly VHS quality at 30 frames per second at 1.5 Mbps. It can be scaled up or down in size or bit rate, but range between 1.2 – 1.5 Mbps is the optimal bit rate.

MPEG 2

MPEG-2 needs about 6 Mbps to provide the quality movie on DVDs, although data rates up to 15 Mbps are supported. 720x480 is the typical 4:3 default resolution, while 1920x1080 provides support for 16:9 high-definition television. MPEG-2 is now arguably the most successful new consumer standard ever relative to its acceptance in the marketplace. Presently it is the predominant standard for existing digital video equipment worldwide. Based on MPEG-2, digital television (both *standard definition*, **SD**, and *high definition*, **HD**) has become the norm for broadcasting, replacing analog broadcast in all but standard terrestrial and cable television.

MPEG 4

MPEG-4 and H.264 have a common heritage within the ISO and ITU standards committees. As a result the overall coding approach is quite similar. Both algorithms are based on a common heritage of DCT based, hybrid image coding, first used in H.261 and MPEG-1. A number of comparison tests have been performed between H.264 and MPEG-2/MPEG-4 on standard MPEG test material. For standard resolution (704x480, 60 Hz interlaced) video sequences to

achieve a PSNR level of 28, NBA must be coded at a rate of 5 Mbps using MPEG-2, but only 1.8 Mbps using H.264.

MPEG Audio Compression

MP3 is actually part of the MPEG-1 standard. The audio portion of the MPEG-1 specification contains three different compression schemes called layers. Of the three, Layer 3 provides the greatest audio quality and the greatest compression. At 8 kbps, MP3 will sound like a phone call – intelligible, but nothing that would ever be called high-fidelity. Good-quality music starts at about 96 kbps, but generally 128 or 160 kbps to would be closer to "CD quality".

RTSP

RTSP (*Real-Time Streaming Protocol*) is an application-level protocol for control over the delivery of data with real-time properties and its goal is streaming of multimedia over multicast and unicast in "one to many" applications. RTSP provides an extensible framework to enable controlled, on-demand delivery of real-time data, such as audio and video.

Sources of data can include both live data feeds (e.g. Live TV channels) and stored clips (e.g. Video On Demand). RTSP establishes and controls single or several data delivery time synchronized media sessions, provide a means for choosing delivery channels such as UDP, multicast UDP and TCP, and provide a means for choosing delivery mechanisms based upon RTP and control mechanism of streams upon RTCP. RTSP is not tied to RTP and RTCP. There is no notion of an RTSP connection – instead, a server maintains a session labeled by an identifier. An RTSP session is in no way tied to a transport level connection such as a TCP connection.

During an RTSP session, an RTSP client may open and close many reliable transport connections to the server to issue RTSP requests. Alternatively, it may use a connectionless transport protocol such as UDP. The streams controlled by RTSP may use RTP, but the operation of RTSP does not depend on the transport mechanism used to carry continuous media. The protocol is intentionally similar in syntax and operation to HTTP/1.1 so that extension mechanisms to http can in most cases also be added to RTSP.

IGMP

Internet Group Management Protocol (**IGMP**), allows Internet hosts to participate in multicasting. IGMP allows users to announce their intention to join particular multicast groups. These groups are identified by their unique Class-D IP addresses.

When a workstation wants to participate in a multicast group, it sends an IGMP "join" message to its local router. If multiple routers exist on a single segment, they can mutually elect a "*Designated Router* (**DR**)" to manage all of the IGMP messages for that segment. After a router receives one or more "joins" for a specific group, the router will forward any packets destined for that group to the appropriate interface. The router should only forward one copy of the data packet per interface.

If multiple receivers exist on a single interface they will all receive the same information by monitoring common multicast MAC and IP addresses. If the multicast group has receivers spread over several router interfaces, the router must replicate the packet and deliver a copy to each interface that contains registered users. This type of transmission activity can be immense, which is why IGMP is highly useful as a stateful protocol. The designated router regularly verifies that the attached workstations want to continue to participate in their respective multicast groups. The designated router sends periodic "queries" to the receivers. These queries are transmitted to a well-known multicast address (224.0.0.1) that is monitored by all systems. If the receivers are still interested in that particular multicast group, they will respond with a "membership report" message. When the router stops seeing responses to queries, it will delete the appropriate group from its forwarding table.

MLDv2

MLD (*Multicast Listener Discovery*) is de facto derivate of IGMP used in IPv6 networks. It is control layer protocol used to control multicast stream flow in IPv6 network. MLD and MLDv2 protocols are designed for use only in IPv6 network. This protocol is follower of IGMP in IPv4 networks used for joining some network node to multicast group. Multicast groups are separated by IP addresses. Procedure of joining some multicast group on network is to announce next routing point, which must be directly attached to some of the requester interfaces.

Node asks it need packets provided for some particular group. If router point have not access to some multicast group data, it must also join it on other interface(s) and forward this data to requester. Router point is sending request to next router point. This process must recursively continue to router point, where source of multicast group data is connected. Note that a multicast router may itself be a listener of one or more multicast addresses; in this case it performs both the "multicast router part" and the "multicast address listener part" of the protocol, to collect the multicast listener information needed by its multicast routing protocol on the one hand, and to inform itself and other neighboring multicast routers of its listening state on the other hand.