Voice over IP

MATTI PUSKA
ESPOO-VANTAA
INSTITUTE OF TECHNOLOGY
2005 - 2006

EVTEK

Table of Contents

Network Diagram Symbols **v**

1 Orientation to Voice over IP **7**
- 1.1 What is Voice over IP?
- 1.2 Voice over IP Promises
- 1.3 Problems, of course not!
- 1.4 Review
- 1.5 Quiz

2 Traditional Telephony Systems **14**
- 2.1 Terminals and Access Network
- 2.2 Switching
  - 2.2.1 Telephone Switches
  - 2.2.2 Signalling
- 2.3 Transmission
- 2.4 Quality of Service in Telephone Networks
- 2.5 Review
- 2.6 Quiz
- 2.7 Material

3 Packet Switched Data Networks **24**
- 3.1 Network Infrastructure
  - 3.1.1 Local Area Networks
  - 3.1.2 Metropolitan and Wide Area Networks
  - 3.1.3 Routing
  - 3.1.4 Internet
  - 3.1.5 Dimensioning
- 3.2 TCP/IP Protocols
  - 3.2.1 The Protocol Stack
  - 3.2.2 IP Addresses
- 3.3 Review
- 3.4 Quiz
- 3.5 Material

4 VoIP Protocols **31**
4.1 TCP/IP Infrastructure
4.1.1 LANs and WANs
4.1.2 IP Packets and UDP Datagrams
4.2 RTP and RTCP Application Layer Protocols
4.2.1 An RTP System
4.2.2 RTP Protocol
4.2.3 RTCP
4.2.4 RTCP-XR
4.3 Voice and Video Coding Protocols
4.3.1 Voice Coding
4.3.2 Video Coding
4.3.3 Choosing the Voice Coding Method
4.4 Signalling Protocols
4.4.1 H.323
4.4.2 Session Initiation Protocol
4.5 Mobile IP
4.5.1 Orientation to Mobile IP
4.5.2 Mobile IP Operation
4.5.3 IP Tunneling
4.6 ENUM
4.6.1 Internet Names and International Phone Numbers
4.6.2 ENUM Extensions to DNS
4.6.3 Number to URI Resolution
4.7 Security Issues and Solutions
4.8 Review
4.9 Quiz
4.10 Material

5 IP Telephony **71**
5.1 Traditional and IP Based Branch Exhanges
5.2 H.323 System
5.2.1 Building Blocks
5.2.2 Terminals
5.2.3 Gatekeeper
5.2.4 Multipoint Control Unit
5.2.5 Gateway
5.2.6 The Network
5.2.7 Registration, Admission and Status (RAS) Signalling
5.2.8 H.323 Location Services

5.3 SIP System
5.3.1 Practical SIP Components
5.3.2 SIP Services
5.3.3 Directory Services and SIP
5.3.4 SIP and Firewalls
5.4 IP Telephony Service Providers
5.4.1 Public Telecommunication Operators and PSTN Pricing
5.4.2 Public IP Telephony Services
5.4.3 Megaco/H.248
5.5 Review
5.6 Quiz
5.7 Material

6 Computer Telephone Integration **102**
6.1 The Concept
6.2 Application Programming Interfaces
6.2.1 Telephone API
6.2.2 Java Telephone API
6.2.3 Extensible Markup Language and VoiceXML
6.3 An Example CTI System
6.4 Review
6.5 Quiz
6.6 Material

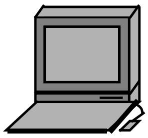
7 Network Quality of Service **111**
7.1 QoS Backgrounder
7.2 Packet Marking
7.2.1 Type of Service, IP Precedence and DSCP
7.2.2 VoIP Recommendation for Marking
7.3 Packet Classifying and Scheduling
7.3.1 First In First Out
7.3.2 Weighted Fair Queueing
7.3.3 Custom Queueing
7.3.4 Low Latency Queueing
7.3.5 Priority Queueing
7.3.6 Short VoIP Recommendation for Queueing
7.4 Traffic Shaping and Policing
7.4.1 Link Fragmentation and Interleaving
7.4.2 Traffic Shaping
7.4.3 Traffic Policing
7.4.4 VoIP Recommendation for Shaping and Policing

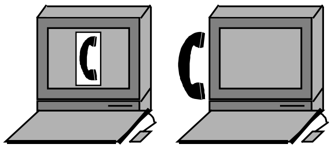
7.5 Congestion Avoidance
7.5.1 TCP Flow Control
7.5.2 Random Early Detection, Weighted Random Early Detection
7.6 Review
7.7 Quiz
7.8 Material

8 List of Acronyms **129**

Appendixes **143**
A: Erlang's First Formula
B: Voice Bandwidth Usage
C: DSCP Values

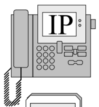
Network Diagram Symbols


Workstation

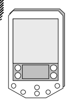

Workstations with IP telephony client application

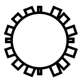

Multimedia workstation

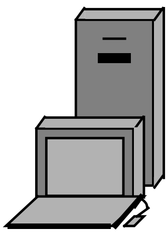

PSTN/ISDN phone set

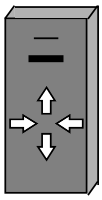


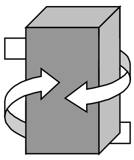
IP Phone

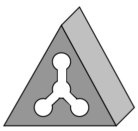

Personal Digital Assistant

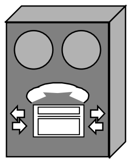

Process

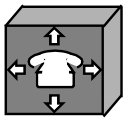

Server

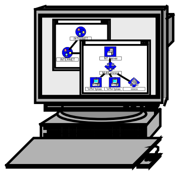

SIP Proxy Server

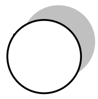

Gateway

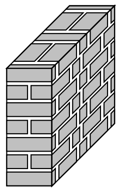

Directory Server

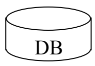

H.323 Gatekeeper


Private area Branch Exchange

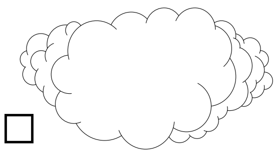

Network Management Station


Telephone exchange

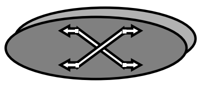

Firewall

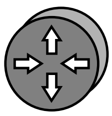


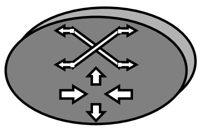
Database

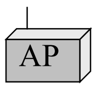

Network (generic)


Local Area Network

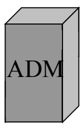

Switch


Router


Layer 2/3 switch



WLAN Access Point



SDH Add/Drop Multiplexer

1 Orientation to Voice over IP

1.1 What is Voice over IP?

In digital wireline telephone systems, a duplex circuit is opened between the caller and the callee, and analogue voice signals are sampled periodically, converted into digital words, carried over the Integrated Digital Network (IDN), and samples are converted back to analogue signal for the listeners earpiece. In TCP/IP LANs, intranets and in the public Internet, computers send messages according to user interaction. The messages are encapsulated into packets, with headers showing the destination, and intermediate IP routers relay the packets towards the destination based on the address information in the header.

Shortly put, Voice over IP (VoIP) is a technology where a **VoIP terminal packs voice samples into IP packets which are carried by a packet switched IP network**. The destination VoIP terminal then unpacks the samples and reproduces an image of the original analogue signal, as shown in Figure 1. Strictly speaking, a VoIP system only carries voice, but the same standards also cover video and multimedia conferencing.

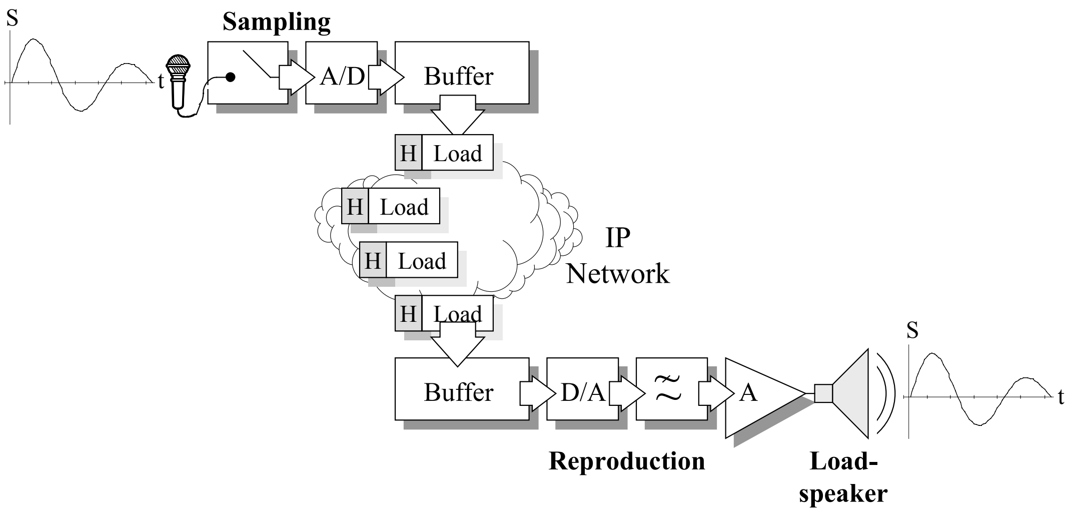


Figure 1: Principal Voice over IP operation.

Integrating data and voice traffic into a single IP network brings advantages, but also places challenges to product, network and system designers. Some of the existing application areas for VoIP are the following:

- IP telephony systems, where special phone sets and software terminals are directly connected to a TCP/IP network. The TCP/IP network elements switch and route the IP packets carrying user data to the destination, and an IP PBX handles call routing, rerouting, directory services and bandwidth management. An IP telephony system can be connected to traditional telephone networks (POTS, ISDN) through a gateway.

- An IP telephony system can be expanded with messaging services and EDP interfaces, to offer additional information based on the telephony information, but provided by external systems.

- An IP telephony system can be adopted as a service. Many Finnish service providers are offering VoIP solution as part of their IT infrastructure or Client/Server product sortiment, also including standard interfaces for corporate applications.

- Videoconferencing includes voice and moving picrure component. Many modern videoconferencing systems use a graphical workstation, equipped with a camera, a microphone and loadspeakers, as the terminal. The VoIP standards also include video and multimedia conferencing, and the IP network should give all real time data a higher priority than for ordinary data packets.

- Some companies already offer a possibility to make a "toll- free" Internet telephone call to their customer service center. A customer with a PC equipped with a sound card, a headset and a microphone, clicks a web link which opens a VoIP call to a service person. The call can be routed direcly from the Internet to the receiving IP telephony system or through a VoIP gateway to a traditional telephone set.

- Traditional telephones, IP telephony terminals and stand alone VoIP terminals can use private and public VoIP services. Some new generation IP Telephone Service Providers (IPTSPs) offer low rate long distance and international services, which are implemented with VoIP gateways and IP networks. Also some Internet access services includ IP based telephony service as an option.

- An Internet Service Provider (ISP) can bypass the subscriber line with a WLAN (Wireless LAN) access network, with cable modems or with some other technology. With minimal end user investments, the ISP can broaden its offering to voice services, without a need to use telephone access network for their customers. As shown in Figure 2, the voice calls can be routed, in an appropiate place, to a VoIP gateway with an interface to the PSTN (Public Switched Telephone Network).

- The core of third generation mobile networks is packet switched, and new mobile services are data oriented. Broadly speaking, also a 3G mobile network is a VoIP system.

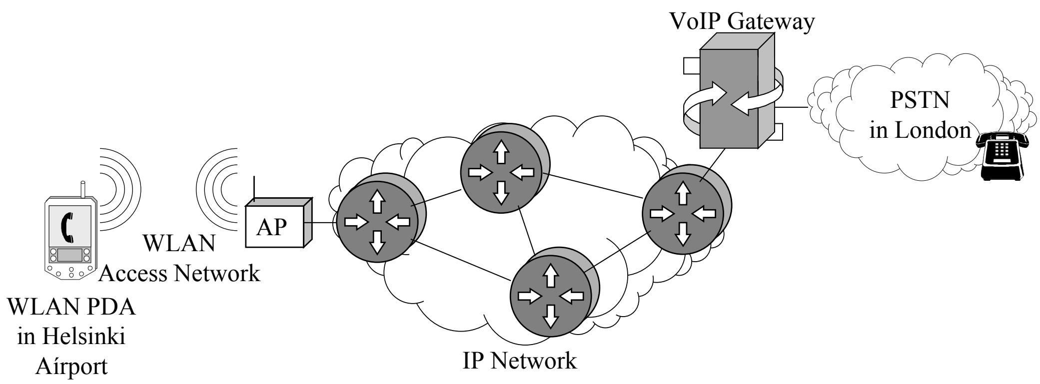


Figure 2: Bypassing the subscriber line and international telephone network with a WLAN and VoIP system.

1.2 Voice over IP Promises

There have been lots of discussions, standard drafts, product and service offerings, as well as debate about transmitting telephone calls and video conference sessions over the corporate intranet, and even over the public Internet, over the last few years. Let's have a look on the typical sales arguments, that are used to promote Voice over IP solutions.

The salesman will propably start with cost savings: when building a new office, when renovating an old one or when it has become the time to upgrade the data network or the telephone PBX, building a single infrastructure for all existing and future communication needs of the employees will lead to a lower total costs than when investing in two parallel systems. The single modern system will also promise to serve new communication needs and applications of the future: with the VoIP enabled network, you can bring high quality video conferencing on the desktop, you can introduce modern, effective and time saving eLearning and network based training systems, as well as any mentioned application xyz, without the need to invest in the infrastructure (*. The IP based telephone switches also promise lower prices, because they are based on international standards, and the customer is not dependent on a vendor specific PBX and feature phone sets. Configuration of an IP based phone exchange is easy, and any technician can do that with a few clicks on the intuitive browser interface, eliminating the additional cost and delay attached to the need of a specialist for a minor change on a traditional PBX. Most important, with a VoIP telephone system, you can

*) Perhaps, we might need a minor firmware and product generation upgrade, with a price tag of few tens of thoudands of Euros

direct long distance and international calls and video conferences between offices to your existing intranet (with no charge), achieving significant cost savings on telephone services. Altogether, a VoIP system offers **lower cost of ownership** than a solution with a parallel data network and a PBX system.

But this is not all: an IP based PBX offers a uniform user interface and **cost effective way to integrate all messaging services and EDP systems** together. Instead of a secretary taking messages and writing them on yellow tags or typing them as E-mail messages, the call can be automatically rerouted first to a mobile phone, then to a backup person and finally to a voicemail box. The called party can listen to her messages using a link on an E-mail, a cellular phone, a PDA or any terminal. When the telephone system is connected with the CRM or ERP system, workers in a call center will receive background information about the calling customer, like maintenance agreement, platform, backlog, invoicing or personal information, just before taking the call. The integration of telephone and EDP systems will give endless promises of better efficiency, higher quality of operations, better customer satisfaction and more sales.

The salesman will propably point out, that VoIP is not a new invention, but a natural development step from manual switchboards to modern digital telephone networks and beyond. He will point out, that central VoIP innovations, like voice coding, compression and packetization have already been successfully used in GSM mobile networks, transatlantic fiber optic cables and militaty communication systems, and the core of the third generation mobile networks will be based on packetized voice. The principle of distributed handling of IP packets is the very foundation of the Internet, and this idea is now adopted to telephony. It must be usable in your office, if the wordwide web of the Internet operates that way.

An argument in favour of the VoIP is, that this is the **natural direction of development**. Already at the end of the 1990's the amount of data on the basic "telephone" network well exeeded the amount of voice samples, and almost all the growth, which is dramatic, is based on the Internet and other IP based data applications. The existing network service providers will plan and implement their network enhancements based on the needs of the data applications, not just voice, and new innovative IPTSPs will introduce new attractive services.

For a starting network service provider, the IP telephony gives an attractive solution to open the business without the need to invest on the old circuit switched voice network infrastructure, instead using the existing IP backbone for voice services. The IP telephony system **makes the trunk capacity need lower**, because of the effective packet switched multiplexing, silence suppression and effective compression algoritms. Integrating the data and voice on a single network makes it possible to **introduce new innovative services**, which either wouldn't be possible with the circuit switched networks or would require massive investments in Intelligent Networking (IN) hardware, software and development platform.

1.3 Problems, Of Course Not!

But this is not the full story yet. Any new technology has its growing pains, and this certainly applies to VoIP also. We are trying to be neutral, and look at the potential problems of VoIP technology as well.

The first complaint is about the **voice quality** of VoIP calls. To keep it short, early experiences were awful. The first Internet telephone software products were optimized for low speed modem access, and used a sound card for voice encoding and decoding, on those days supporting only half-duplex operation. Combined with variable delays of the crowded Internet or an intranet, which was not VoIP enabled, lead to an experience that is hard to forget.

Although today's VoIP solutions are meant for business users and include optimized terminals, servers and intranets, which give priority or guaranteed bandwitdth for real time applications, the sound quality of a VoIP call is lower than the average quality of a call in wireline telephone networks. A circuit switched network can offer guaranteed low delay, but packetization, packet handling and buffering will often lead to an overall delay, which is well over 200 ms, and disturbs our internal schema of interactive telephone conversation. On networks that are used to transmit also other forms of information, a voice packet can arrive too late for reproduction. If a single bit error happens, the whole packet is dropped. When a packet often carries voice sampes for about 20 ms, the human ear senses multiple missing packets, and a telefax machine definitely drops the connection, if consequtive packets are missing.

The second counter-argument considers the **reliability** of the VoIP system. Traditional telephone networks are built with components, which are designed with reliability as the first target, consisting of redundant components and run by specialists that have years of experience. Comparing this to a system that uses PC hardware and Windows operating system as PBX, a network that was built to use a shared printer and run by people who are busy with end-user PC/Windows/application software support, will certainly favour the traditional approach. Reliability is not just a matter of prejudiction; central VoIP protocols have serious shortcomings concerning reliability and data security. There are not that many real experts on VoIP systems in Finland, so the odds to get one to design, another to implement and a third one to run our system is small.

VoIP is a young technology, and VoIP **standards are still evolving**, and do not guarantee full interoperability yet. Partially because of the delays in standardisation, partly for commercial reasons, most vendors have adopted their own extensions, modifications or implementations. On top of this, there are two "competing" standards for VoIP signalling: one prepared by the ITU-T (International Telecommunications

Union - Telecommunications Section), representing the telecommunication view, and the other prepared by the Internet society IETF (Internet Engineering Task Force). Anyway, the situation today is, that even standards based VoIP products from different vendors don't necessary work together.

To be able to use all features of the IP PBX, vendor specific IP telephone sets should be used. **IP phone sets are often high priced**, and the total purchase price for IP telephony system will be about the same as the price for a traditional telephone solution.

Most Finnish and European people have a **mobile phone**, and while employees are moving around, they cannot often use their fixed IP telephone. Integrating mobile phones on a VoIP system is a challenge. On the other hand, IP technology makes it possible to use new kind of terminals and access networks, like WLAN, to bypass mobile phone tariffs.

Designing an IP telephony system and a VoIP enabled network and integrating the system with existing circuit switched terminals, PBXes and the PSTN is a much more **complicated** assignment that implementing a legacy telephone system. There are well-known formulas, practices, design rules and experts for circuit switched telephony, but VoIP design methods are still evolving. Many implementation and integration problems must be handled as individual instances without a known solution.

The next two chapters will review traditional telephony and packet switched IP technologies, to provide basic knowledge in understanding the challenges of VoIP. Then we will focus on central VoIP and IP telephony technologies, standards and realisation principles. The last chapter will introduce some example product offerings.

1.4 Review

Voice over IP terminals pack voice samples into IP packets, which are carried by a packet switched IP network. VoIP technology is used in IP telephony systems, which may be easily integrated with corporate EDP systems, for packet based videoconferencing and for offering public telephone and value added services. Compared to the traditional circuit switched telephone network, VoIP promises cost savings regarding infrastructure, operation and long distance and international call charges, and easier integration with existing EDP and messaging systems. For a network service provider, IP telephony offers a lower priced alternative with high efficiency and adaptability. On the other hand, VoIP realisations may include shortcomings regarding service and voice quality, reliability, incompability and component pricing.

1.5 Quiz

- What is the main difference between a VoIP telephony and a traditional telephony system?
- Mention at least five advantages IP telephony promises, compared to traditional telephone systems.
- Mention at least five potential problems of IP telephony

2 Traditional Telephony Systems

2.1 Terminals and Access Network

Humans can hear frequencies from 20 Hz up to about 20 kHz, but the hearing of the higher frequencies gets worse with age. Human speech consists of frequency components in the 200 - 5 000 Hz range, depending on the speaker, and the telephone network is built to carry speech. A wireline telephone set includes a microphone, an ear piece, a ringing indicator (a bell), means to signal the number selection to the telephone exchange and a local loop connection. The speaker's voice is converted into an electrical signal and transmitted to the telephone network. Normally, a customer buys or leases a telephone set, makes a contract with the local telephone company and pays for the phone services. /Bjålie/

A local telephone operator builds the access network, consisting of local loops and access switches, and connects the access switches together to form the local carrier network. Various telephone operators connect their networks to form the global telephone network, and the subscribers can make local, long distance and international calls on reasonalble charges. With these charges, telephone companies get their investements paid and their operations costs covered.

In PSTN, signals in the local loop carry analogue signals. In most cases, analogue voice signal is converted to digital form in the local access switch, as shown in Figure 3. In most countries, excluding developing countries and some regions in Eastern Europe, the telephone network is fully digital.

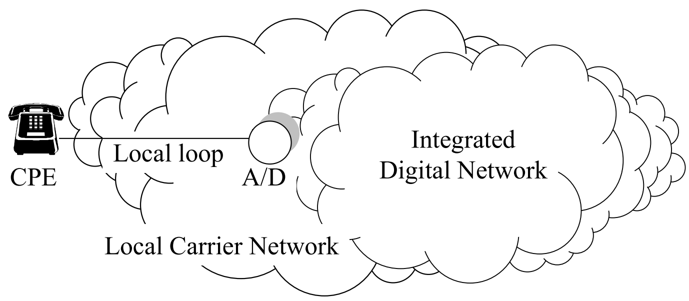


Figure 3: The local carrier network consists of local loops, access switches, local telephone exhanges and the transmission systems between switches.

The analogue to digital (A/D) conversion is done in phases, as shown in Figure 4. The G.711 PCM voice coding includes the following steps:

- The telephone network is designed to carry signals between 300 and 3 400 Hz. To eliminate aliasing and noise, the frequency of the voice signal is limited with a low pass filter.

- Next, samples are taken from the analogue signal in fixed time intervals. The sampling theorem says, that to be able to reproduce a 3 400 Hz signal, the sampling frequency must be at least 6 800 samples/s. 8 000 1/s was chosen as the sampling rate, producing one sample every 125 μs. The sampling rate is the same in all countries.

- The analogue samples are then expanded to make small samples near the zero level larger. The meaning of the expansion is to make the relative quantisation noise even for all signal strengths. When the samples are compressed with a reverse law at the other end, the original signal can be reproduced. The European expansion/compression follows A law, while μ law is used in North American networks.

- Now each expanded sample is converted to a digital number. The European system uses eight bits per sample, producing a bit stream of

  8 000 samples/s * 8 b/sample = 64 kbit/s.

  With eight bits, 256 distinguished levels can be coded. The MSB represents the sign of the signal, zero indicating a negative value.

  Also the Northern American system uses eight bit sampling, but the LSB is once in a while borrowed for signalling, leading to a bit rate of 56 - 64 kbit/s. Both coding variations are defined in the CCITT standard G.711.

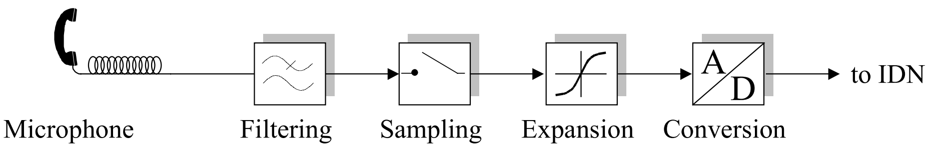


Figure 4: Analogue to digital conversion and PCM voice coding.

PCM voice coding produces a 64 kbit/s bit stream, and it is transmitted in the digital switching and transmission system. IRL, the access switch also converts incoming digital numbers from the opposite direction into analogue signals to be reproduced in the ear piece. For two way operation, a 64 kbit/s Full-Duplex channel is needed in the Integrated Digital Network (IDN).

Often companies and public organisations decide to buy or lease a Private Area Branch Exhange. The telephone sets are connected to the PBX and calls within the organisation are switched locally with no charge. The PBX is connected to the PSTN, normally with physical E1 or T1 interfaces, and subscribers compete of the limited number for outside lines. It is also possible to get local switching as a service.

2.2 Switching

2.1.1 Telephone Switches

Telephone switches listen to the signalling requests, make a circuit through the telephone network and handle digital signals. At the end of the call, the terminal signals a disconnect message and intermediate switches release the circuit. Switches also handle counting and logging: the call log and summary information is kept at the local exchange and transferred to the billing system periodically.

Telephone switches form a hierarchical tree: concentrators multiplex local loops to a single trunk connected to a regional switch, and regional transit level switches cover a whole tariffing region. International calls are handled by international transit level switches and there are national transit level switches to handle calls between different telephone operators within a single country.

A block diagram of a modern digital telephone switch is presented in Figure 7. Subscriber lines are normally concentrated into few trunks by concentrators, located near the subscribers. The switch has multiple E or T series trunk interfaces, which are used for concentrators, customer PBX's and for inter switch connections through the transmission system. The contents of the time slots are written to the RAM memory of the connection matrix or a Group Switch, and read from the right place at the right time to be sent to another interface. Reading and writing is controlled by the processor of the control part.

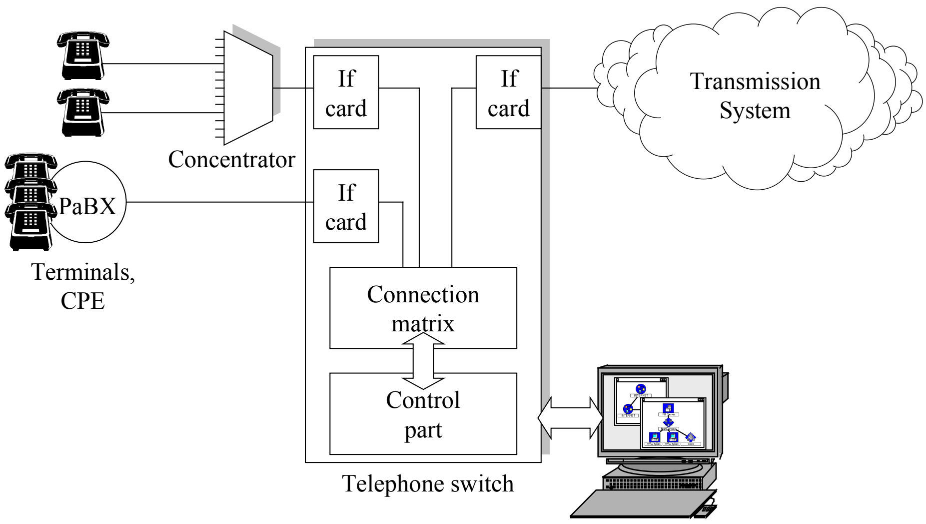


Figure 7: Block diagram of a digital telephone switch.

2.2.2 Signalling

Switching is controlled by signalling messages. The user (A subscriber) picks up the handset and dials the destination (B subscriber) number. **Subscriber signalling** pulses or tones are interpreted by the access switch, which analyzes the number, makes the routing decision and signals a connection request to the next switch. **Network signalling** messages propagate through the network of switches, until the access switch of the B subsriber is reached. This switch then sends an alert terminal signal to the destination telephone set, making the telephone ring. Private PBXs as CPEs can exchange additional **interexchange signalling** messages, which are used for additional services, like hunt groups, delayed or unconditional call forwarding and conference calls.

Modern phone terminals use Dual Tone Multi Frequency (DTMF) signalling for called number and network services. The digital PSTN network uses a common signalling channel T 16, according to the SS#7 (Signalling System Number 7). The SS#7 uses messages with headers, which distinguish the time slot in question. The fully digital ISDN uses similar messages, which are specified in the ITU-T standard Q.931. Between the subscriber terminal and the access ISDN switch messages are carried in LAPD (Link Access Protocol for the D channel) frames, that is specified in the standards I.441 and Q.921. The frame bytes are then transmitted using the D signalling channel of the BRI or PRI interface (see Figure 8). Between the switches, the Q.931 messages are carried by the Message Transfer Part of the SS#7 network (T16 in the E1 frame). The ISDN signalling can also carry some user to user information, like interexhange signalling messages between ISDN PBXs.

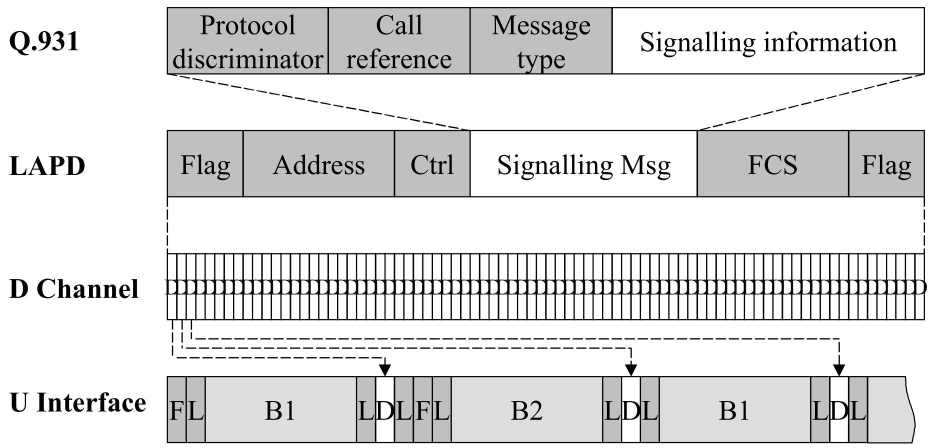


Figure 8: ISDN Subscriber signalling protocol stack.

Figure 9 on the next page presents an example of call setup and tear down on an IDSN network. The messages are the following (subscriber signalling messages are shown in **boldface**):

- The caller picks up the handset and selects the subscriber B number, to make a call. The telephone set sends a **Setup** message to the access switch, which returns a **Call Proceeding** message as the acknowledgement of a complete number received. These messages are transmitted using LAPD frames and D channel bytes.

- After the number analysis and the routing decision, the access switch sends an IAM (Initial Address Message), with the destination number, to the next switch on the path, using the SS#7 signalling channel. The intermediate switch or switches forward it to the next switch and reserve a B channel.

- Finally, the IAM reaches the destination access switch, which sends a Setup message to the receiving phone set, using the D channel and a LAPD frame. This makes the telephone ring, and an **Alert** message is returned by the terminal. The subscriber signalling message is interpreted as an Address Complete message, and returned to the caller access switch. The receiving switch also sends a Call Progress message, causing the access switch A to send an Alert signal to the caller terminal, which will generate a ringing tone.

- When the receiver accepts the call, the receiving ISDN telephone sends a **Connect** message, which propagates, as an Answer message through the network of switches. The access switch A sends a Connect message to the terminal of the A subscriber. The message also starts counting for billing. When the connect message reaches the caller, a B channel is established and the parties can start talking. The **Connect** subscriber messages are also **acknowledged**.

- A voice call can be terminated by either of the parties. The terminating person puts the handset back on hook and his phone set send a **Disconnect** message. The local access switch confirms receiving the message by a **Release** message, which is again acknowledged (**Release Completed**) by the subscriber terminal.

- The switch, that received the Disc, sends a Release message that propagates through the network, and frees the switching and transmission resources that were reserved for the B channel. The release messages are acknowleded with a Release Complete message. The access switch on the other end sends a Disconnect to the subsciber terminal, which sends a Release, that is again acknowledged by the switch. The message also stops counting.

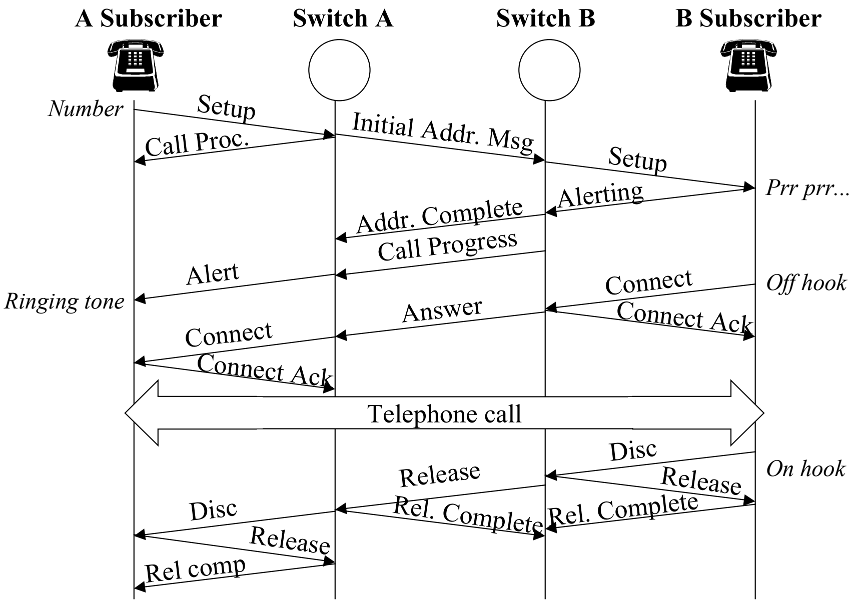


Figure 9: An ISDN call setup.

2.3 Transmission

Two switches are connected with a transmission system, which consists of the physical media and the multiplexers. For the physical connection, single mode fiber optic cables are often used, but also radio links and satellite connections have their role. The emitter sends an optical signal to the fiber, and the signal is converted into bits by a detector. The capacity of a SM fiber is enourmous, so it should not be wasted on a single E1 or T1 channel. A multiplexer can take numerous channels and concentrate them on a single high capacity trunk. Normally, time division multiplexing is used. SDH (Synchronous Digital Hierarchy) specifies a hierarchical system to multiplex lower capacity synchronous channels into a single trunk. Modern transmission systems include Wavelength Division Multiplexers and optical Cross Connect devices, which can multiplex and switch optical channels transparently.

Circuit switched switching and transmission systems are dimensioned based on blocking. A call is blocked, if the network cannot make the connection. The refusal can be based on lack of switching or transmission capacity. According to the national regulations, the nominal blocking level on the public telecommunication network must be kept under 1 % for long distance trunks and under 0,2 % for feeder trunks to the long distance switches.

The network is dimensioned to handle also the peak load. The amount of traffic during the busiest full hour is used as the dimensioning value. This can be read from the traffic statistics or estimated as a multiple of the characteristic traffic value and the number of subscribers. The network is dimensioned to offer a certain nominal blocking level, by looking, for the dimensioning value, the minimum number of switching elements that will lead to the nominal blocking level.

Erlang's first formula gives the blocking probability of a call (under certain conditions), when the traffic intensity and the number of lines is known. The formula is the following:

$$E_1(n;A) = \frac{\frac{A^n}{n!}}{1 + A + \frac{A^2}{2!} + \ldots + \frac{A^n}{n!}}$$

, where E is the blocking probability, A is the traffic intensity and n is the number of lines. Often precalculated tables are used, giving the number of lines for a given blocking probability. The appendix A includes some Erlang figures for 0,3 %, 1 %, 3 % and 5 % blocking propabilities.

Let's take an example. If a PBX with 100 extensions is connected to the PSTN, the amount of traffic can be estimated as the sum of the following components:

- incoming traffic from the PSTN for 100 extensions (* 100 * 50 mErl
- 50 % of the incoming calls of 30 persons redirected back to the PSTN interface to their mobile phones 30 * 0,5 * 50 mErl
- outgoing traffic from 100 extensions 100 * 50 mErl

making a total of 10,8 Erlang.

*) Traffic statistics from the PSTN show, that the traffic intensity for a business user is 30 - 60 mErl.

With the help of the Erlang formula and derived tables, we see that for a nominal blocking level of 1 % a trunk of 19 Full Duplex lines will handle the traffic(**. If only 0,2 % blocking is accepted, the capacity needed will be 22 lines.

A significantly higher block level can be accepted, if a leased line capacity between two PBXs with a PSTN connection is dimensioned, because extra spill traffic can be redirected through the PSTN (Figure 11). If a regional office has a PBX or an interface module with 100 extensions and 50 % of the incoming and outgoing traffic is between the headquaters and the regional office, the dimensioning value for the inter PBX trunk will be 5 Erl, needing only 9 lines, with a block level of 5 %. /Ericsson/ /Erlang/

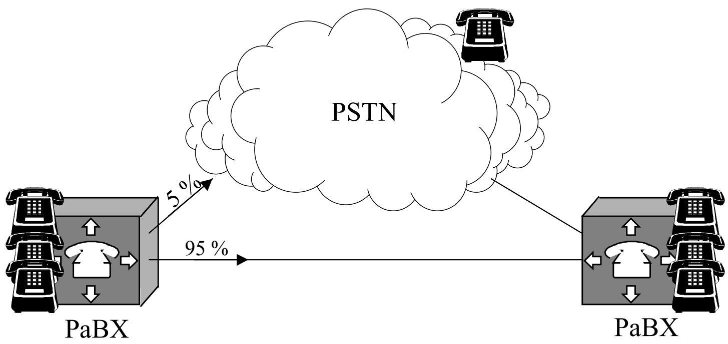


Figure 11: Using the PSTN as the backup for the PBX interconnection.

2.4 Quality of Service in Telephone Networks

A telephone user expects good quality service: block free availability and good quality connection at low price. If she is unhappy, she might select another carrier the next time.

The following technical details are expected by the user of public fixed line voice services:

- **High availability**, meaning low blocking probability. The service is judged as successful, if the caller hears a ringing tone, indicating that the target telephone is alerting. Most of the unsuccessful call attempts are caused by network blocking. The network is redundant, so device faults, that prevent the service, are very rare.

**) The 1 % blocking will mean an average of 36 s blocking during the busiest hour, while the 0,2 % blocking is only 7,2 seconds.

- **Low** end to end **delay**. Delay disturbs interactive conversation, because parties may start to talk at the same time. ITU-T regulations state the upper limit of 150 ms for end to end delay for calls, which are not routed through a satellite link, and 400 ms for international lines. The delay is sensed subjectively, but normally delays over a few hundred milliseconds are regarded as disturbing.

- **Low echo** level **and low echo delay**, most often generated by an imperfect hybrid, which converts the duplex local loop to two simplex IDN channels. With a speakerphone, the voice can leak also acoustically from the receiving loudspeaker to the microphone. Significant echo level with a delay of 15 ms or higher is considered disturbing.

- **Low noise** level. On the digital PSTN, noise is generated by the analogue subscriber line and the A/D quantisation. To minimize the effect of the latter, expanding is used before converting the samples to digital data.

- **Relatively low bit error rate** (BER). The human ear is quite insensitive to short errors, caused by the representation of an errornous byte, but if errors happen in bursts, they are more easily regarded as disturbing. A BER of 10^{-5} is considered negligible but noticeable, and 10^{-4} is considered irritating, but these figures are easily achieved by modern digital transmission systems. The ITU-T also defines limits for the maximum probability of high error minutes and seconds.

- **Steady signal level**. Alternating attenuation or amplification on analogue transmission, and abnormal refraction and multipath propagation on radio links cause fading.

- **Reasonable frequency response**. We are used to the fact that the telephone network only carries frequencies of 300 - 3400 Hz, but we will notice any severe degradations. Often errors on the frequency response are caused by the terminal, not by the modern telephone network.

Data, telefax and video services are more sensitive to noise and bit errors. Also the echo, fading and amplitude distortion is interpreted as noise. Often Frame Check Sums can compensate for the effect of bit errors, but retransmissions degrade the practical capacity and bursty errors may disconnect a data or fax transmission. Analogue modems and telefax terminals measure the line quality and adapt their bit rate accordingly during the initial handshake procedure. Bit errors during the handshake period may lead to an unpractically low bit rate, which is used during the whole connection. /Ericsson/

2.5 Review

Modern public telephone networks consist of customer premises equipment, local loops and access switches, hierarchical telephone switches, transmission systems and network management solutions. In PSTN, the telephone set is analogue and A/D conversion takes place at the local access switch, and all switches and transmission equipment handle digital signals. The ISDN is fully digital, and the A/D conversion is handled by the ISDN voice terminal.

Telephone switches make bidirectional circuits through the telephone network and handle byte streams, which carry voice samples. In Europe switches offer time division E series interfaces, while Northern America uses T interfaces with similar principles. Inter switch connections are handled by transmission systems, which multiplex multiple channels on a single fiber optic or radio link. Transmission capacity is dimensioned based on traffic intensity and blocking level using the Erlang's formula or precalculated Erlang tables. A modern fixed line telephone network offers low delay, low echo, low noise, low bit error rate, steady, flat amplitude 64 kbit/s switched circuits with high availability and reliability but with low tariffs.

2.6 Quiz

- List the system components on POTS ordered from the caller to the called party
- How G.711 PCM voice coding operates?

How are trunk links on telephone networks dimensionned?

- List QoS parameters for a PSTN connection
- Calculate the bit rate for G.711 PCM voice coding
- What are the main functions of subscriber (terminal) signalling?
- Qhy NMS is needed in PSTN?

2.7 Material

/Bjålie/ Jan G. Bjålie et. al: Ihminen - Fysiologia ja anatomia. WSOY, 1999.

/Ericsson/ Understanding Telecommunications. Studentlitteratur, 1997.

/Erlang/ www.erlang.com

/Digital Link/ Digital Link: T1 Fundamentals. Digital Link, 1997.

Tuula Miettinen: Puhelinverkkojen merkinantojärjestelmiä. Insinöörityö, Evtek 2004.

3 Packet Switched Data Networks

3.1 Network Infrastucture

3.1.1 Local Area Networks

Local Area Networks (LANs) have become the standard way to connect office PCs, common peripherals, servers and communication servers together. For the user, the LAN connection offers access to common information, processing and communication resources. Workers with LAN attached computers can easily share information and use common data storage resources: project documents, customer and product databases, bookkeeping and ERP information to mention a few applications.

Modern LANs are based on **structured cabling systems**, where all office rooms have a dual wall outlet, which can be used for voice and data services. The horizontal twisted pair cabling is concentrated to Floor Distribution facilities, which are connected to a common Building Distribution facility with fiber optic cables. Wall outlets and backbone links can be flexibly connected to suitable communication devices.

Most LANs are based on the **Ethernet technology**. Traditionally all stations on an Ethernet segment compete for network access. Replacing the hubs and repeaters with Full Duplex **Ethernet switches** in floor and building distribution racks will eliminate collisions and contention problems of shared medium LAN. A hierarchical design of 10 Mbit/s Ethernet, 100 Mbit/s Fast Ethernet, 1 Gbit/s Gigabit Ethernet and 10 Gigabit Ethernet will bring the capacity exactly to those parts of the network, where high bandwitdth is needed. All Ethernet technologies share the same operation and design principles.

Figure 12 shows the topology of a typical LAN. Workstations and printers are connected to ports of workgroup switches with 100 Mbit/s 100BaseT connections using the horizontal cabling. The workgroup switches have a fiber optic Gigabit Ethernet connection to the backbone switch in the building distribution facility. When most of the traffic is directed from the workstations to the servers and back, the servers in the EDP room are connected to the backbone switch with high performance Gigabit Ethernet links. Also the communication devices, providing access to the corporate intranet and the public Internet are conneced directly to the backbone switch. For fault tolerance, a second backbone switch and redundant backbone fiber optic links may be added. Virtual LANs are used to divide stations into smaller broadcast domains.

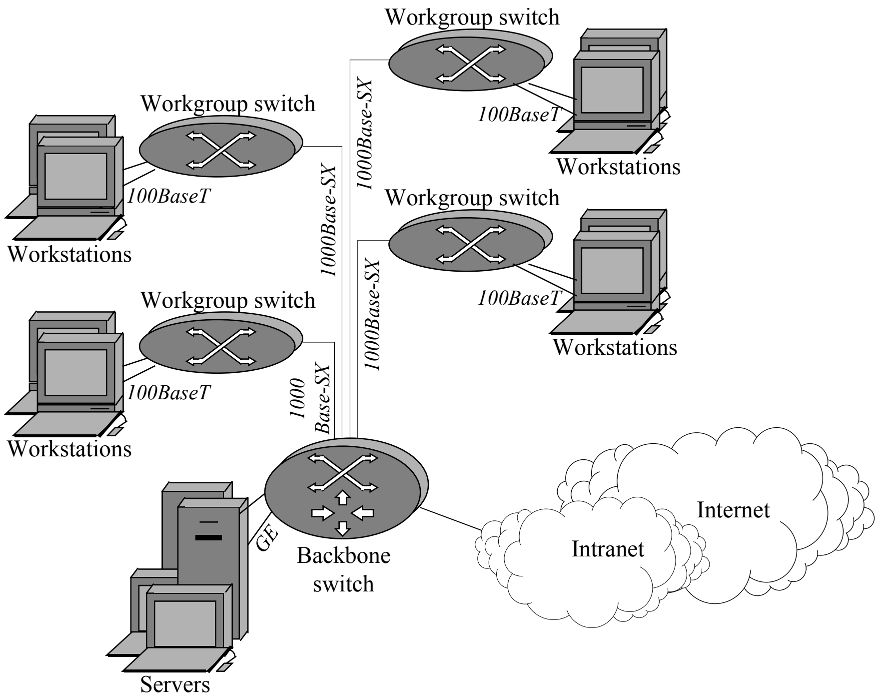


Figure 12: A hierarchical switched Ethernet LAN topology.

3.1.2 Metropolitan and Wide Area Networks

Traditional LAN technologies are intended for networks, that span one or two buildings. If greater distances are needed, technologies more suitable for this must be used. A Metropolitan Area Network (MAN) is used to connect different LAN segments together in a campus or on a city area. Switched Gigabit Ethernet and 10 Gigabit Ethernet with single mode and multimode fiber optic connections offer enough bandwidth for LAN interconnection and support for links up to tens of kilometers. A MAN can be run either by the user organisation or organisations, or by a network service provider, which offers public MAN services. Normally the public MAN network use fixed tariffing, so the price is independent of the network usage.

For longer distances, Wide Area Networking (WAN) technologies are used. WAN services are always offered by a network service provider. WAN technologies include leased lines (n*64 kbit/s), metro Ethernet and packet switched networks (MPLS, Frame Relay). Also access technologies, like ADSL, cable modems, WLANs and VPN can be used for LAN to LAN interconnection. Packet switched services and leased lines normally use flat tariffing, independent of the network usage. Normally, the connection speed affects the cost of the service quite heavily, within the limits of the technology.

Typically, a router is used as the Customer Premises Equipment. All WAN services include support for IP routing, but some services (like leased lines and ATM virtual circuits) are transpartent to the network protocols. The service can also include advanced routing options, like traffic prioritizing, Quality of Service and Service Differentiation.

3.1.3 Routing

For broadcast control hosts on switched Ethernet LAN are often divided into separate Virtual LANs. Because unicast and broadcast Ethernet frames are kept within a single VLAN, VLANs must be configured to separate IP subnets. It is also wise to keep the Ethernet traffic local within a single building, within a campus and within a company. To enable inter VLAN, inter building, inter campus and inter company traffic in a controlled way, routers are installed in IP subnet boundaries (Figure 14). An IP router inspects the IP header and passes packets towards the destination subnet based on its local routing table. A router can follow instructions on its access control list, while making routing decisions. To be able to route packets, the router must know the IP subnet topology and routes between subnets. For this reason, routers exchange topology information with other routers and builds local routing tables for best paths based on a routing protocol.

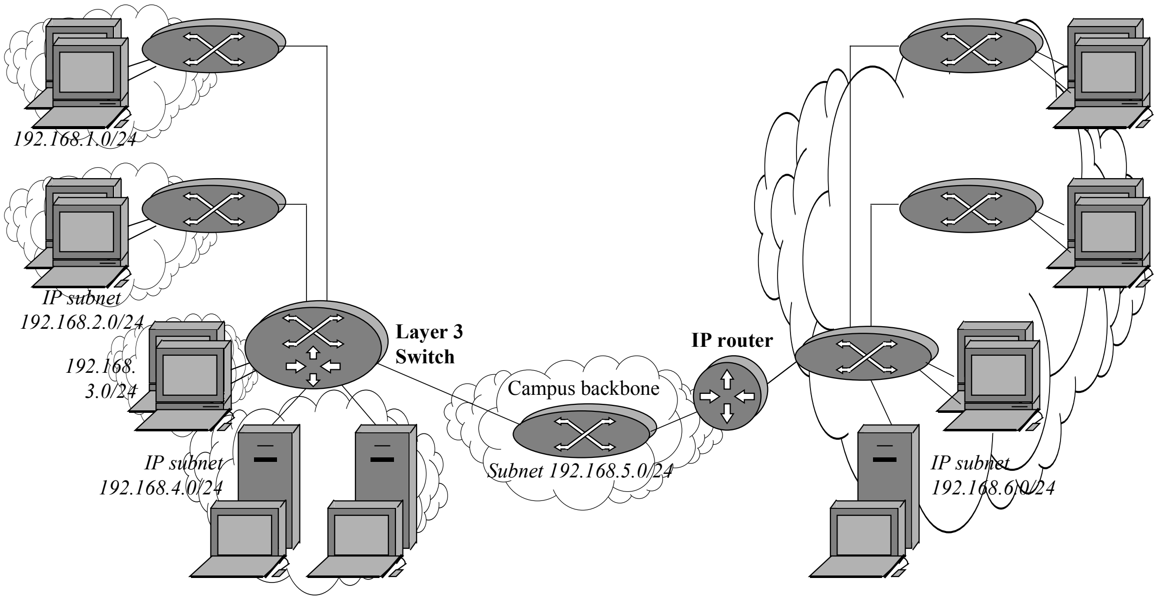


Figure 14: Routing between IP subnets.

3.1.4 Internet

The Internet is a public packet switched IP network, which spans the globe. For users, the Internet offers a wide variety of information and entertainment services. It is based on distributed intelligence where IP routers make independent routing decisions. The network is run by Internet Service Providers (ISPs), which offer Internet access service, routing services, bandwidth and additional services to home and business users. The network development is guided by the Internet Engineering Task Force (IETF), which publishes RFC documents (Request for Comment).

Besides the content, the Internet can also be seen as a WAN infrastructure. A public domestic network doesn't offer any guaranteed service, but some ISPs offer guaranteed international access and trunk capacity.

3.1.5 Dimensioning

Computer Networks, like LANs, operate based on packet switching, so the well established dimensioning methods for the circuit switching networks don't apply. Traffic volume on a LAN is hard to estimate, the growth rate may be very high when new network applications are introduced and the traffic profile varies between applications. On the other hand, overdimensioning doesn't necessary lead to higher operating costs, only to somewhat higher investments.

The target for LAN dimensioning is to ensure application usability and reasonable service level, despite the rapidly changing environment. When the initial values are unprecise, sophisticated mathematical dimensioning is not worth using. Instead, after choosing the LAN technology (which will be Ethernet in most cases), the network hierarchy is analysed to make sure that the flow of information is smooth and no bottlenecks exist.

When dimensioning the WAN connections, a compromise between the desired service level and the network service costs must be made. Normally network service providers use tariffs, where monthly fees depend heavily on the connection capacity. An approach to choose a service that just delivers the required service level, and making sure that the network concept can easily expanded to higher bit rates and additional points of operations, is often used.

3.2 TCP/IP Protocols

3.2.1 The Protocol Stack

The TCP/IP protocols are defined by the IETF on RFC documents. The main protocols on the stack, as described in Figure 16, are the following:

- **Internet Protocol** (IP) delivers IP packets end-to-end. For this, controlled IP addresses are used. An IP router, operating in the Internet layer, routes IP packets between IP subnets towards the final destination.
- Routers exchange topology information about the IP subnets and routes with Interior and Exterior **routing protocols** (RIP, OSPF, BGP etc.).
- Because routers and hosts must know the MAC address for the destination LAN host, address resolution between the MAC and the IP address is needed. **Address Resolution Protocol** (ARP) resolves the MAC address of a given IP by broadcasts. ARP only takes place between stations on the same IP subnet.
- **Transmission Control Protocol** (TCP) offers reliable transport of byte stream end-to-end. Sequence numbering, acknowledgements and checksums are used for reliability, while RWIN provides a simple flow control mechanism.
- **User Datagram Protocol** offers simple connectionless byte stream transport for applications that don't need reliability.
- Traditional **ARPA services** include Telnet remote terminal sessions, FTP file transfer, SMTP messaging and SNMP network management.
- **Newer services** include, among others, HTTP and HTTPS distributed hypermedia transmission, DNS name resolution, X.11 remote applications, NFS file services, RFC NetBIOS for PC networking, IRC for on-line chat and many others.

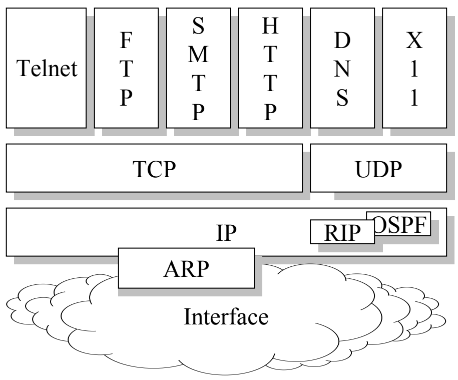


Figure 16: The TCP/IP protocol stack.

3.2.2 IP Addresses

The Internet Protocol specifies the global IP addressing scheme. An IP address is a 32 bit binary number, presented with four decimal numbers separated by commas. The address contains a network part and host part. The host part is assighed by the user organisation, while the network part is assigned by ICANN (Internet Company for Assigned Names and Numbers), by an ICANN authorized organisation or by an ISP from its address space. The separation between the network and the host part is represented by a subnet mask, which contains a TRUE bit for network part bits and a FALSE for host bits. Traditionally, IP addresses are divided to class A, B and C addresses with 8, 16 and 24 bit network part. The user organisation can use the remaining host bits for subnetting, changing the bits on the subnet mask to TRUE for the borrowed bits (*.

Public IP addresses are globally unique: the ISP or national authority will guarantee the uniqueness of the network part and the user organisation should make sure, that host addresses are unique within their network. If a firewall with Network Address Translation is used between the public and the private network, certain IP addresses can be used behind the NAT firewall (**.

Address configuration can be done manually to each host, or automatically from a DHCP server. The latter method includes a DHCP server with a central database of IP addresses. As shown in Figure 18, a DHCP client on a workstation, when booted, sends an address request (DHCP Discover) as a broadcast. The server returns an offer, and the client requests for the IP offered by the server. If multiple offers are received from redundant DHCP servers, only the first one will be requested. Finally the server acknowledges the lease. The server keeps a log of the leased addresses, the corresponding MAC addresses and the lease times, and repeats the offer well before the configured lease period expires. If a workstation is turned off for a longer period, it will propably receive a different address when booted. Additional IP, TCP, DNS and NetBIOS parameters may be distributed as DHCP options.

*) If a class C address of 192.168.33.0/24 is divided into eight subnets, three bits must be borrowed. The subnet mask will be 1111 1111.1111 1111.1111 1111. **111**0 0000 = 255.255.255.224 Each subnet will have 256/8 = 32 numbers, giving 30 usable IP addresses.

**) The IP addresses for private internets are the following:
10.0.0.0/8 network: 10.0.0.0 - 10.255.255.255
172.16.0.0/12 network: 172.16.0.0 - 172.31.255.255
192.168.0.0/16 network: 192.168.0.0 - 192.168.255.255

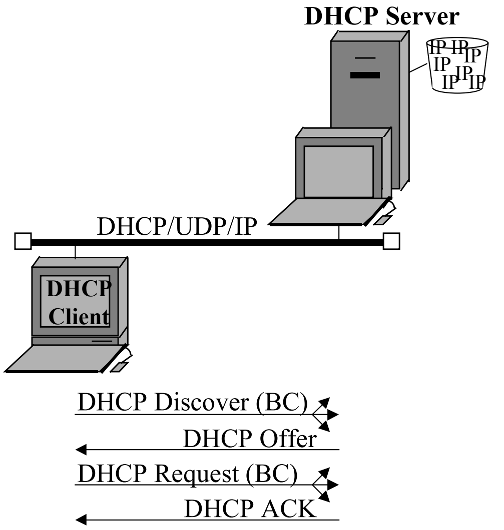


Figure 18: Dynamic Host Configuration Protocol.

3.3 Review

A modern LAN infrastructure, consisting of structured cabling, Ethernet switches, TCP/IP protocol and necessary Client/server hardware and software, connects workstations, printers and servers. The solution normally offers authentication, file, print, application and communication services. Also commuters may be offered a safe arrangement to use network resources with a help of a Virtual Private Network. Intra building LANs are connected together with a campus backbone, inter office communication is handled by corporate Intranet and normally users are offered access to the public Internet. LANs and MANs are dimensioned to quarantine smooth flow of data by trying to avoid bottlenecks. Often the solution is a hierarchical Ethernet, Fast Ethernet, Gigabit Ethernet and 10 Gigabit Ethernet network, so the choices are limited. When dimensioning Wide Area connections, a compromise between service level and costs must be considered.

Today, LANs, MANs, WANs and the Internet use TCP/IP protocols and applications. On the Internet layer, IP delivers IP packets end-to-end based on controlled IP addresses, routing protocol exchange topology information between routers and ARP resolves IP address to MAC address dependencies. Transport layer protocols include reliable connection oriented TCP and unreliable connectionless UDP, both transporting byte stream end-to-end. Application layer protocols offer communication services to applications. These include protocols for traditonal terminal sessions, file transfer, message exchange and network management and many newer protocols for new services.

3.4 Quiz

• List the networking components on campus LAN ordered from the workstation to the server on a server farm
• How are LANs dimensionned?
• How are WANs dimensionned?
• List typical network services, provided to a workstation user on a company
• What is the main difference between TCP and UDP transport?
• Give an example of a valid IP address

3.5 Material

/Wieger/ Holger Wieger: Indoor Wireless Local Area Network. Evitech, 2001.

/Ericsson/ Understanding Telecommunications. Studentlitteratur, 1997.

/Mäkitalo/ Esa Mäkitalo: Differentiated Services Architecture. KPNQuest, 2001-09-12

/Puska/ Matti Puska: Broadband Networks. Evitech Course Handouts, 2001

/DiffServ/ Cisco White Paper: DiffServ - The Scalable End-to-End QoS Model. Cisco Systems, 2001. Internet, <URL: http://www.cisco.com/warp/public/cc/pd/ioft/iofwft/prodlit/difse_wp.htm>

/RFC 2475/ S. Blake et. al. : An Architecture for Differentiated Services. RFC 2475. IETF, 1998.

/RFC 2274/ K. Nichols et. al: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. RFC 2274. IETF, 1998.

/RFC 2597/ J. Heinanen et. al: Assured Forwarding PHB Group. RFC 2597. IETF, 1999.

/RFC 2598/ V. Jacobson, K. Nichols, K. Poduri: An Expedited Forwarding PHB. RFC 2598. IETF, 1999.

/Puska/ Matti Puska: Network Management Systems. Evitech Course Handout, 2004.

4 VoIP Protocols

4.1 TCP/IP Infrastructure

4.1.1 LANs and WANs

The TCP/IP protocol stack is the most widely used set of protocols. The Internet handles IP packets and offers various TCP/IP based services. Private intranets also normally use IP routing, TCP/IP services and Internet server and client applications. Workstations and servers are connected to LANs, today often into ports of Ethernet switches. IP packets between different VLANs (Virtual LAN) are handled by IP routers. LANs on different buildings are connected through IP routers to a campus MAN and traffic between networks in different towns are routed with IP routers. Public WAN services also use IP routers as the customer premises equipment and to direct the packets to the destination.

4.1.2 IP Packets and UDP Datagrams

As shown in Figure 21, an **IP packet** consists of the following parts:

- IP protocol version, currently 4
- IP Header Length in four byte words, often coded by the protocol analyser as bytes
- Differentiated Services Field, including the DSCP (Differentiated Services Code Point) and two bits for Explicit Congestion Notification (ECN), which are currently unused. This field was formely called Type of Service
- The total length of the packet in bytes
- Packet identifier
- Flags for fragmentation control and more fragments
- Fragment offset, showing the place of the packet in a larger entity
- Packet lifetime (Time to Live, TTL) in router hops, which is used to kill lost packets
- Protocol identifier of the upper layer PDU in the data field of the packet
- Checksum of the IP header, ensuring header integrity
- IP address of the source node
- IP address of the destination node
- Options, if any, and possible padding to fill the header into full four byte words
- Variable length data, containing an upper layer PDU or a PDU fragment.

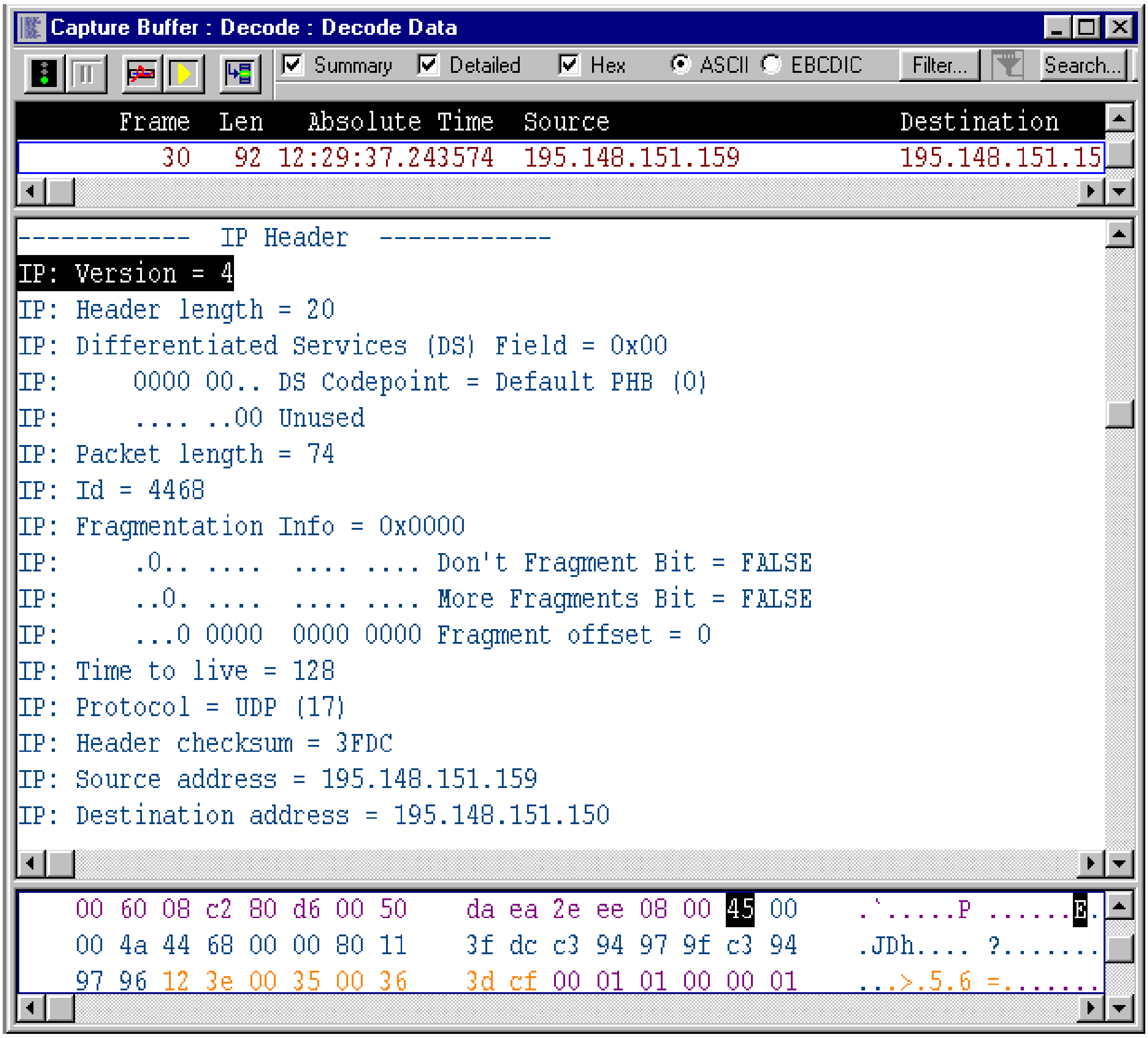


Figure 21: An IP header.

The example packet in Figure 21 carries a full UDP datagram, which needs no special service. Both the source and the destination node are propably on the same IP subnet.

TCP offers connection oriented end-to-end transport of bytes for applications needing reliable transport. Connectionless simple UDP is used for those applications that don't need or cannot take advantage of reliable transport. A **UDP datagram** contains the following fields (Figure 22):

- Source and destination TCP ports, which identify the session. The server listens to a well-known port, that is used by the client as the destination port. The source port on the client datagram is an arbitrary free number from 1024_{10} and above.
- The length of the datagram
- The checksum for the UDP header, which is used to detect any transmission errors on the datagram header.

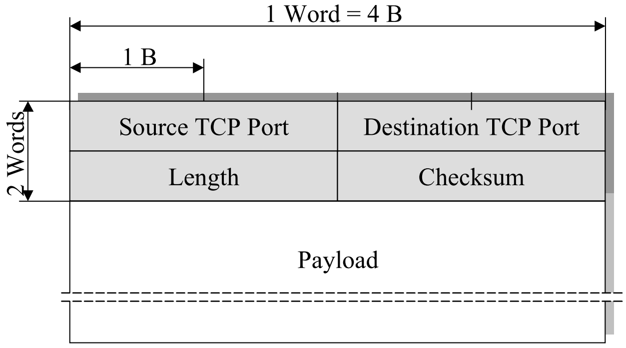


Figure 22: UDP datagram fields.

4.2 RTP and RTCP Application Layer Protocols

4.2.1 An RTP System

As shown in Figure 23, real-time data, like voice, can be transported over a packet switched network. The transmitter samples the signal, makes analogue to digital conversion and puts samples into a transmitter buffer. A chunk of samples are put on a packet, adding protocol headers and sent to a packet switched network. The receiving node receives the packet, stores it in a receiving buffer, extracts samples, make the digital to analogue conversion if needed and finally reproduces a copy of the original signal. Because a packet switched network cannot guarantee packet arrival order, fixed delay or provide synchronization, an additional application layer protocol must be used.

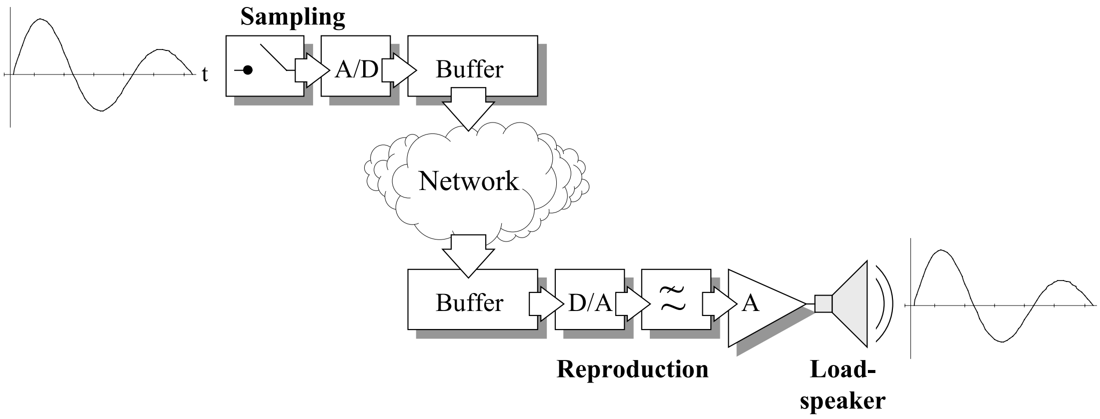


Figure 23: An example real-time transport system. /Puska/

4.2.2 RTP Protocol

TCP and UDP offer transport services to upper layer protocols. These include traditional ARPA services (Telnet, FTP, SMTP, SNMP), newer extensions like HTTP, HTTPS, TFTP, DHCP, POP3, IMAP4, NetBIOS name, datagram and session services, IRC, NNTP, SSH, SQL, DNS, NFS and X.11, to mention a few. Realtime Transport Protocol (**RTP**) **provides end-to-end transport functions for real-time applications** like IP telephony and video conferencing. The real-time application generates a byte stream, which must be received order and in due time by the other end. If a packet carrying for example voice samples is lost or delayed, there will be no time for retransmission before the reproduction time, so the unreliable and simple UDP service is used for RTP.

RTP follows the principles of application layer framing. It completes some missing UDP functions, which are critical to real-time applications. RTP offers timing information between the parties and detection of lost packets, and it returns the correct packet order, even after reordering by the network. An RTP message, shown in Figure 24, consists of a header and a data field and holds the following fields:

- RTP **protocol version,** currently version 2. This field is two bits long.
- **P and X bits**, indicating the existence of padding or an extension header. If padding is added, the last padding byte holds information about the length of the padding, which should be removed by the receiver.
- **CSCR Count** (Contributing Sources), which indicates the number of CSCR identifiers after the fixed header. The CSCR count field is four bits, making it possible to have up to 15 contributing sources.
- A **Marker bit**, which can be used to mark important events. The precise interpretation of the marker is defined by a profile.

- **Payload Type**, containing seven bits of information about the RTP user data media and coding.
- Two byte **Sequence Number**, which presents the number of the RTP message. The initial value is random, and each message increments this value.
- Four byte **Timestamp**, holding information about the time of the first sample in the message. The initial value of the timestamp is random and it will be incremented linearly. For multimedia conferencing, successive RTP messages can hold equal timestamp values.
- Four byte **Syncronization Source Identifier** for the source. This value is also random, to ensure the uniqueness of the syncronization sources during an RTP session.
- A 0 - 15 word list of **Contributing Sources**, if any. Multiple contributing sources are used by an RTP mixer, which resynchronizes, converts and combines packets from various incoming RTP sessions.
- Variable length **data**, containing voice or video information.

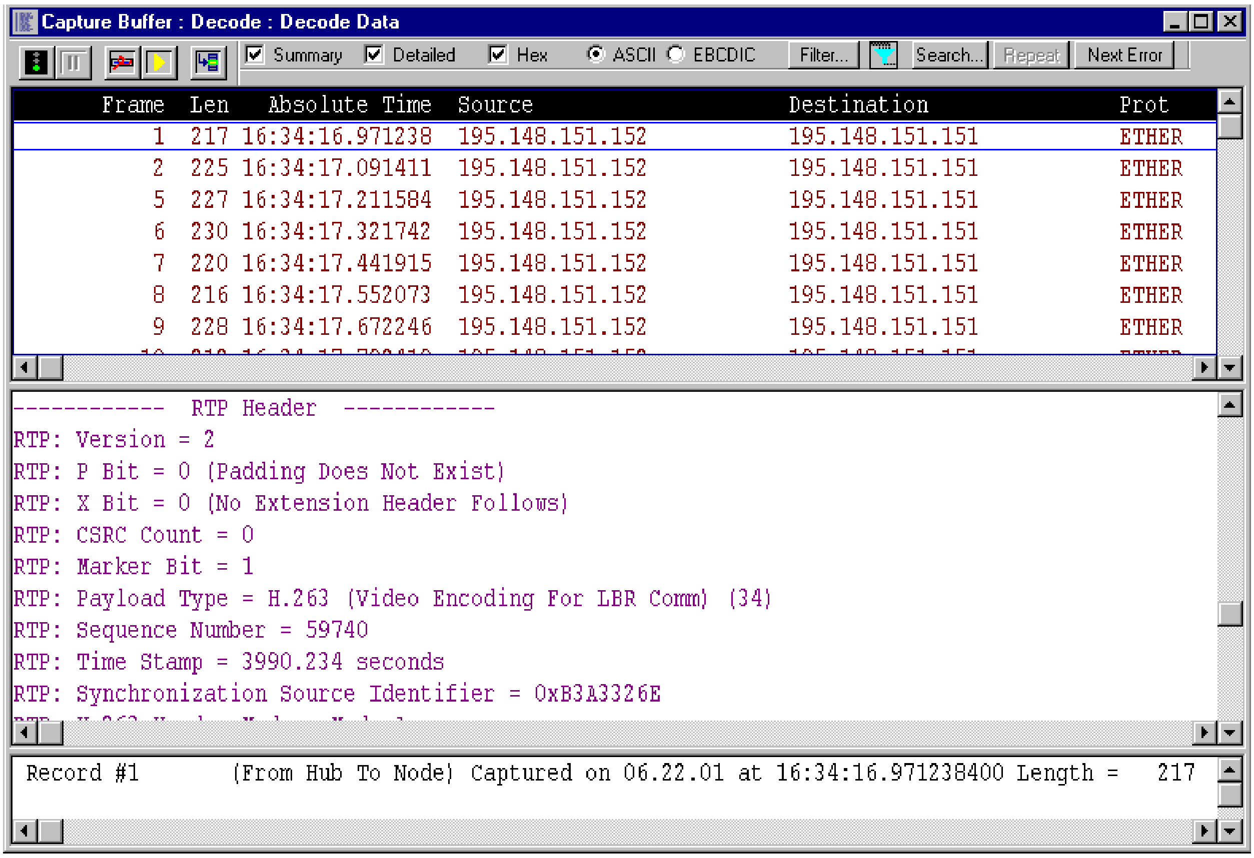


Figure 24: An RTP message, carrying low bit rate video.

The RTP messages don't use any standard TCP port, but the parties agree on the port during session negotiation. A free unassigned port witn an even number is used in both directions, and the next odd port is used for RTCP. Different RTP sessions and ports are used for different media, like voice and video, between the same parties. Each source sends RTP messages, which are not acknowledged. Often fixed period sampling is used, as in the case of Figure 24. In this case, a variable bit rate source generates variable length messages.

RTP offers means to detect lost or reordered packets, but it doesn't ensure timely delivery of packets or guarantee any Quality of Service. The unreliable UDP transport only detects bit errors on the UDP header, but doesn't offer any reliability or QoS quarantees. To ensure sufficient quality, external solutions, like prioritization or service differentiation must be used. /RFC 1889/

4.2.3 RTCP

Realtime Transport Control Protocol (**RTCP**) **is used for providing feedback** on the RTP transport, **for RTP source identification** and **for observing the number of participants**. Optionally, RTCP can also carry minimal session control information, like participant identification, which will be displayed on the user interface. The RTP sources use random and unique CSCR numbers, but to be able to synchronize different streams on a single application, a distinguished CNAME (Canonial Name) is distributed by the RTCP. The RTCP message rate is adapted to the bandwidth usage and to the number of participants, but the total bandwidth usage should be 5 % of the RTP bandwidth.

RTCP uses the following messages:

- Sender Report (SR), which is used for getting transmission and reception statistics from the senders
- Receiver Report (RR), for getting reception statistics from stations that are only receiving
- Source Description Items (SDES), for informing about the CNAME and other optional information of the sender
- Bye (BYE), indicating the end of participation
- Application Specific Functions (APP) • RTCP-XR (RCTP Extended Reports), that will be covered in Chapter 4.2.4.

In a two way RTP session, the new receiver should receive the CNAME on a SDES as soon as possible, to be able to associate various media from a single source. The reception statistics (SRs) should be sent as often as the bandwidth constrains allow, to maximise the reliability of the statistical information. The average interval between RTCP messages is not more than 5 seconds, but the actual interval varies randomly to avoid unintended synchronization. When an RTP session is terminated, a BYE message is sent. This only indicates that the party is finishing using this media. APP messages are only used in experimental implementations of new RTP applications, and messages with unknown names should be ignored.

Figure 25 shows the structure of the Sender Report, which consists of a header, a sender info and zero, one or multiple report blocks. The sender info includes both Network Time Protocol (NTP) and RTP timestamps for the report and the number of sent packets and octets. The timestamps can be combined with Receiver Reports to calculate the round-trip propagation time to receivers. The report block contains fractional and cumulative number of lost packets from this source, the highest received sequence number and an estimate of the variance of RTP packet interarrival time difference, the timestamp of the last SR and time elapsed since the last SR.

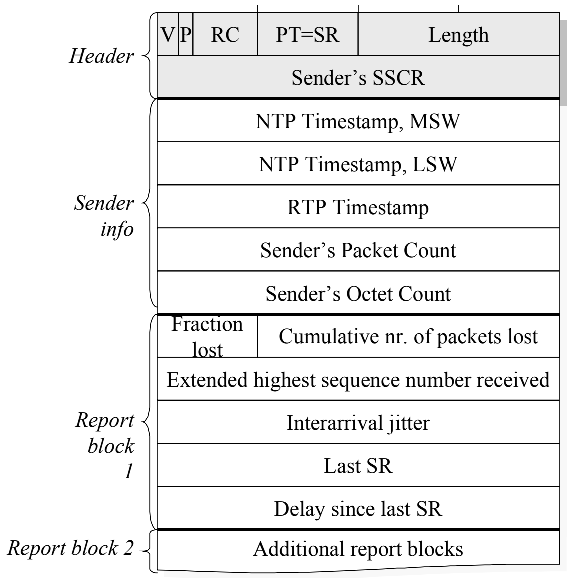


Figure 25: RTCP Sender Report Message.

The Receiver Report (RR) has the same format as the SR, but obviously it doesn't include the sender info. RTCP Sender and Receive reports can be used to calculate RTP packet loss rates, round-trip delays and interarrival jitter. For example, a growing jitter may be an early warning of network congestion.

Source Description messages include a short header and chunks of combined SSCR and SDES items. The mandatory SDES is the Canonial Name, which normally holds the username and the hostname (like mattip@keryx.evitech.fi). This will not quarantee CNAME uniqueness, but either the profile specifies additional syntax or the SSCR is used to identify the RTP source. Optionally SDES can also carry a user's full name, E-

mail address, telephone number, location information, a note or a private SDES extension.
The BYE message includes a similar header as SR and RR, and an optional reason for leaving and length information for the reason. The reason is given in clear text, e.g. "Camera maltfunction".

All RTCP messages are carried over UDP, using an odd port number next to the RTP port for the corresponding session. /RFC 1889/

4.2.4 RTCP-XR

The new extension for RTCP is Extended Reports (RTCP-XR), which provides detailed data for RTP stream management. RFC 3611 defines seven block types, but we will concentrate only on the VoIP Metrics Report. As shown in Figure 26, an RTCP message for VoIP Metrics Report Block includes the following fields /RFC 3611/:

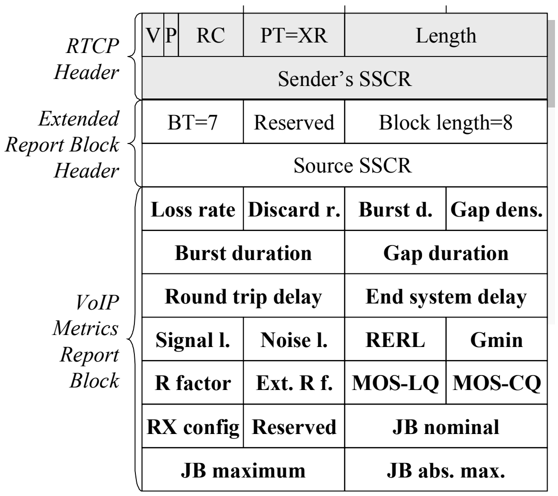


Figure 26: Stacked RTCP -XR Voice Metrics Report Message.

- Standard two word RTCP message header, with 207 in the Packet Type indicating an XR message.

- Two word Extended Report Block Header for stacking purposes. For efficiency, multiple XR report blocks may be carried in a single RTCP message, and blocks are separated by report block headers. For VoIP Metrics, value 7 is used in the Block Type field.

- Packet Loss and Discard Metrics, including the following fields:
  * Loss rate, which indicates the fraction of RTP messages that are lost by the network.
  * Discard rate, indicating the fraction of RTP messages that are discarded by the receiving station due to excessive jitter.

- Burst Metrics, defining the burst of lost or discarded RTP messages and the gap between bursts. During a burst time, loss and discard ratios are high, and during a gap these are low. The metrics include the following fields:
  * Burst density, indicating the fraction of RTP messages that are lost or discarded during a burst period.
  * Gap density, indicating the fraction of lost or discarded messages within inter-burst gaps.
  * Burst duration, which include the mean time for burst period.
  * Gap duration, containing the mean for gap period in milliseconds.

- Delay Metrics, containing the following information on both network and End System delays:
  - Round trip delay for the network in milliseconds
  - End system delay, containing internal delays for both the sending and the receiving station

- Signal Related Metrics, including the effect of non-packet elements affecting call quality for the received audio signal. These include:
  * Relative signal and noise level in dBm. These provide indication that the signal level may be too high or low.
  * Residual echo return loss, indicating effects of both electrical echo by the hybrid and acoustic echo by the speakerphone.
  * Gmin, which is a configuration parameter, and will be presented later.

- Call Quality or Transmission Quality Metrics, which measure the call quality directly. The Call Quality or Transmission Quality Metrics include the following:
  * R factor for voice quality of the RTP segment, using the 0 - 100 metric defined by ITU-T G.107. Value 94 indicates toll quality of the PSTN and 50 or less is regarded as unusable.
  * External R factor for the effect of the external non-RTP network for the voice quality.
  * MOS-LQ (Mean Opinion Score-Listener Quality), indicating the estimated MOS for voice, excluding the effect of delay. The original MOS scale is 1 - 5, and this field holds the MOS value multiplied with 10.
  * Mean Opinion Score for conversation quality, including the effects of delay.

- The following Configuration Parameters:
  * Gmin, i.e. gap threshold, which is used to distinguish burst and gap periods. This field holds the value for the maximum fraction of lost and discarded RTP messages during a gap.
  * Eight receiver configuration bits, including information about packet loss concealment and use and adjustment rate of adaptive jitter buffer.
  * One reserved byte for future enhanchements.

- Jitter Buffer Parameters, including the following:
  * Jitter buffer nominal, maximum and absolute maximum delay in milliseconds. The maximum is the current maximum, while the absolute maximum holds the largest value for adaptive jitter buffer in the worst case.

RTCP-XR is an optional amendment for Realtime Control Protocol. IP phones and gateways may send periodic Extended Reports as part of the normal RTCP message exchange, associated with every RTP stream. RTCP-XR data may be retrieved from the gateway using SNMP, RTCP messages may be decoded by a probe or protocol analyser on the network or VoIP terminals may report call-quality metrics to an IP PBX. In any case, RTCP-XR provides a rich set of data for monitoring and troubleshooting VoIP systems. /Clark/

4.3 Voice and Video Coding Protocols

4.3.1 Voice Coding

Traditional analogue telephone network carries frequencies from 300 to 3 400 Hz. The digital PSTN takes 8 000 samples a second and codes every sample with eight bits, after nonlinear decompression. The **G.711 PCM** coding produces a continous bit stream of 64 kbit/s and offers good voice quality. The PCM coding forms a reference point to other coding methods.

With compression, the bit rate can be reduced, but this results in poorer sound quality and the need for extra processing power. Basically, the more effective the compression (leading to lower bit rate or better quality), the more processing power is needed, often also leading to longer processing delays. An example hopefully clarifies the situation: Uncompressed Hi-Fi quality stereophonic CD sound needs 1,4 Mbit/s, while MPEG-1 Layer 3 audio compression produces about 130 kbit/s and a reasonable quality, but needing extra processing on MP3 players. Higher compression ratios will not be economical, because the extra processor power will cost more than the saving on the storage media [(*].

*) An MP3 player can store little over an hour of stereophonic music on a single 64 MB Smart Media memory module. The time is quite enough for storing a single CD disc.

Waveform compression is based on the fact that less than eight bits are used to code a voice sample. Instead of identifying the absolute sample value only the difference from the previous sample may be presented. Even quantisation steps will produce original quantisation noise and voice quality in suitable conditions, but this method cannot follow rapid changes on the signal, when the difference between two consequtive samples is large. The solution is to adapt the precision of the sample difference: smaller changes will use lower quantisation steps, while larger steps are used for larger changes. The **G.723** is an ITU-T standard, which uses **ADPCM** (Adaptive Differential Pulse Code Modulation), and produces 24 kbit/s or 32 kbit/s bit stream with quite small quality degradation. As shown in Figure 27, a signal channel exists between the transmitter and the receiver. Waveform coding produces a constant bit stream, but voice samples can be stored in a transmission buffer and a suitable cluster of samples is sent on an RTP message.

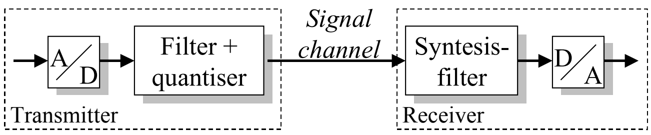


Figure 27: Waveform coding principle.

The previous method reaches compression ratios up to 3:1. With **voice source modelling** only the filter parameters of the voice source are quantisized and transmitted, and the receiver generates a signal and filters it based on these parameters (Figure 28). Vocoders produce very high compression ratios, 16:1 to 32:1, but the reproduced voice is often described as unnatural and robotic.

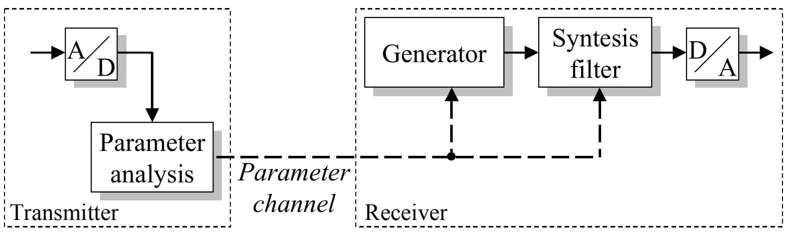


Figure 28: Vocoder, that is based on voice source modelling.

The most common vocoder method is **LPC** (Linear Predictive Coding). It models the human voice generation by a buzzing signal source at the end of a tube. The space between the vocal cords can be described with signal strenght and pitch frequency, and the cavity of larynx is described with resonance frequencies of the tube. The LPC transmitter analyses the voice signal by predicting the voice channel properties, by eliminating it's effects from the voice signal and by determing the strength and the pitch of the residual buzz. Only source and filter parameters are transmitted in the parameter channel. The speech is syntesized by filtering the signal from a controlled source with a filter, which is controlled by the received parameters. A set of signal samples are processed at a time, and usually one frame describes 20 ms of speech. Voice channel parameters are defined by solving the differential equation, which describes each sample as a linear combination of previous samples. **FS1015** LPC-10e coding produces 2,4 kbit/s bit stream, but voice quality is not suffecient for commercial applications.

Hybric codecs try to combine natural voice quality of waveform coding and low bit rate of vocoders, and they produce good quality voice with medium range compression ratios of 4:1 - 16:1. Also hybrid coding produces and transmits the control information for the syntesis filter using the parameter channel, but the signal channel transmits periodical residual signal in the signal channel (Figure 29). With CELP coding (Codebook Exited Linear Prediction) the transmitter selects the most suitable exitement signal from a codebook and transmits the code. The receiver generates the exitement using the same codebook and filters it with the syntesis filter. ITU-T standard **G.729** defines **CS-ACELP** coding (Conjugate Structure Algebraic Codebook Exited Linear Prediction), that produces good quality voice with 8 kbit/s bandwidth, but requires lots of calculation. **G.723.1** includes 6,3 kbit/s MPMLQ coding (Multipulse Maximum Likelihood Quantisation) and 5,3 kbit/s ACELP coding.

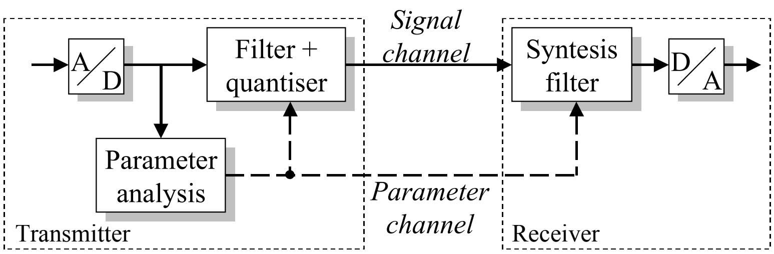


Figure 29: Hybrid codec operation.

IP telephones also use 13 kbit/s full rate **GSM** coding 06.10, which forms a 260 bit block from 160 voice samples. **RPE-LTP** coding (Regular Pulse Excitation - Long Term Prediction) calculates short term LPC filter parameters, that are used to refilter the same samples. Next phase divides residual signals into four 40 byte blocks and calculates long term prediction parameters for each block and the successive 120 samples. Finally the residual signal parameters are calculated for each block. Alltogether, the following parameters are transmitted between transmitter and receiver:

- short term LPC filter parameters, 36 bits every 20 ms, producing 1,8 kbit/s
- long term prediction parameters, 9 bits every 5 ms, equal to 1,8 kbit/s
- residual parameters, 47 bits every 5 ms, producing 9,4 kbit/s.

On a full duplex telephone call, a direction is only used 30 - 40 % of the time. **Silence suppression** detects the silent periods, and samples are sent only in the active direction. Because technical limitations with silence detection, about 50 % of the bandwidth is saved, while multiple calls are transmitted simultaneously.

Often samples for 10 - 30 ms are transmitted on a single UDP datagram. For example, 30 ms of G.723.1 ACELP contains:

I = 5,3 kbit/s * 30 ms = 159 bit = 19,9 B,

making a five word (= 20 B) UDP data field.

The output of both audio and video codecs are transported using the RTP application protocol. The G.723.1 data is encapsulated with a 12 byte RTP header, with a 8 byte UDP header and with a 20 byte IP header. The IP packet is then transmitted in an Ethernet LAN, using an Ethernet frame with an 18 byte header. The portion of the headers on an IP packet will be:

$$\frac{12B + 8 + 20B}{12B + 8B + 20 + 20B} * 100\% = 66{,}7\%$$

RTP header compression can compress the 40 byte header to 2 bytes (no UDP checksum send) or to 4 byte (with UDP checksums), making the portion of headers reasonable:

$$\frac{4B}{4B + 20B} * 100\% = 16{,}7\%$$

cRTP uses the tact that half of the UDP and IP header fields remain constant, and several RTP header fields differ with a constant value from message to message. cRTP extension for links with high delay, packet loss and reordering are specified on a separate standard.

The **RTP header compression** (cRTP) needs routers, that support this feature. The header compression also takes some processing power from the Intermediate Systems. cRTP offers the biggest advantage on lower speed WAN links with high RTP traffic portion, but care must be taken, that the CPU load on th compressing routew will not exceed 60 %. /ETSI/ /Otolith/ /RFC2508/ /RFC 3545/

4.3.2 Video Coding

Often a VoIP system is also used for business quality video conferencing, so I will shortly cover the video coding principles. A full motion CIF video (Common Intermediate Format) produces a 352 * 288 pixel frame every 33,3 ms. If every pixel is coded with 16 bits to produce 65 536 colors, the bandwidth need for an uncompressed CIF video would be:

R = 352 * 288 pixels * 16 bit/pixel * 30 1/s = 48,7 Mbit/s, which would need a dedicated switched Fast Ethernet connection end-to-end for every video stream. This solution is clearly unfeasible.

Video compression methods take advantage of the fact that in a frame, **successive pixels** often contain the same information. Think of the solid background or the chin on the forehead: instead of repeating the same pixel information 50 times, the codec can send the pixel information only once, with a command to repeat this pixel 50 times. Often variable length Huffmann coding, based on the run counts, is used for intraframe compression.

Another method is to use the fact, that **successive frames** contain mostly unchanging information. Instead of the full information (I) frame, only the predictive (P) difference information will be carried, and the receiver can calculate the full frame from the previous and the difference. Some methods calculate also bidirectional B frames from successive information and predictive frames. On each I, P and B frame, the intraframe compression is then used separately.

Advanced video compression algorithms also include pattern recognition and movement algorithms, that basically state, that the face on this frame is the same as in the previous, but the position has changed two pixels to the left.

The most common video compression methods are the following:

- ITU-T **H.261**, which uses a set of information and predictive frames, leading to the compression ratio of 10:1 without a significant reduction of video quality. The bit rate of the H.261 stream can be adapted to the channel by changing the frame rate and the portion of I frames. This simple coding is best suited for video conferencing applications, where the picture doesn't include rapid changes.

- **H.263**, also from the ITU-T, uses I, P and B frames, intraframe Huffmann coding and an optional movement algorithm, leading compression ratios of up to 100:1. This method can also follow rapid changes in the picture better than the previous one.

- **MPEG standards** (Motion Pictures Experts Group) from the IETF include versions 1, 2 and 4. They are intended both for video conferencing, TV broadcasting and video distribution. The MPEG-2 reaches a compression ratio of 200:1 with a quality suitable for commercial video broadcasting.

Advanced video coding systems use lots of processing power, if a high compression ratio and good picture quality are desired. Video conferencing systems are higher priced than IP telephones and they often include a powerful PC with a video card, and the price for the extra processing power is easily justified in stand-alone systems.

4.3.3 Choosing the Voice Coding Method

When selecting voice coding method, the following details should be considered:

- Coding methods supported by terminals. Almost all IP telephone sets and software clients support uncompressed G.711 coding. Other common methods include G.729, G.723.1 and GSM coding, the latter being especially popular in software based products. Normally code translations should be avoided because of the need of dedicated DSP equipment, so only one or two methods, which are supported by all terminals, are enough.

- Bandwidth usage compared to connection costs for the voice. One uncompressed bidirectional voice channel uses less than 0,1 % of the capacity of a switched Full Duplex Fast Ethernet, so inside a single LAN compression doesn't normally give any advantage (*. With slow wide area links voice compression, silence suppression and header compression may give considerable cost savings.

- Codec delay. A/D converter on circuit swithed telephone network sends a voice sample every 125 μs, but sample packetizing and processing produce extra delay on IP telephony systems. G.711 coding gathers 20 ms voice samples on a single RTP message and this simple coding method doesn't normally produce significant processing delays. G.729 and G.723.1 codecs use also future voice samples while processing a packet (Lookahead), that causes an additional delay of 5 - 7,5 ms. Also the processing delay is longer with these codecs: about 10 - 30 ms, so the G.723.1 codec alone may generate a 67,5 ms delay. Additional delays are caused by frame transmission on the network and dejitter buffer on the receiver. Table 2 presents the delay components, relative complexity and voice quality of some voice coding methods.

- Processing power needed: complex coding methods take more processing power from the terminal than the simple ones. When dedicated IP telephone sets or DSP cards are used, the extra processing is not a problem, but on a workstation with an ordinary sound card advanced coding methods require at least moderate processor and memory capacity.

*) If 40 workstations are connected with a single Gigabit Ethernet backbone link, and the traffic interest is 80 mErl per user, G.711 coded voice will take less than 0,08% of the GE backbone capacity.

- Sensitivity to packet loss, i.e. the portion of lost RTP messages or messages arriving too late of all messages. Different coding methods can recover packet loss differently: instead of the missing samples silence, noise or previous samples may be played or the missing samples may be calculated from the history data. The packet loss has the smallest affect on voice quality with G.711 and G.723.1 coding, while G.728 coding is especially sensitive to lost packets.

- Voice quality, including the effects of voice coding, end to end delay, delay variation, packet loss and echo. Because it is hard to measure voice quality technically, often persons subject to the test are used, who evaluate their subjective experiences on scale of 0 - 5 (MOS, Mean Opinion Score). Table 2 presents voice quality for some coding methods, when effects of delay, delay variation, packet loss and echo are eliminated. The trend is clear: the smaller the bandwidth, the poorer the sound quality.

Table 2: Bit rate, delay and voice quality of popular voice codecs.

Standard	Coding	Bit rate kbit/s	Delay, framing ms	Delay, Lookahead ms	Delay processing ms	Quality MOS	Complexity
G.711	PCM	64	0,125	0	0	4,3	
G.711	PCM	64	20	0	small	4,1	1
G.729	CS-ACELP	8	10	5	10	3,9	30
G.729.A	CS-ACELP	8	10	5	10	4,0	15
G.723.1	MP-MLQ	6,3	30	7,5	30	3,9	25
G.723.1	ACELP	5,3	30	7,5	30	3,7	25
06.10	RPE-LTP	13	20	0	10	3,7	5
FS1015	LPC-10e	2,4	20	2,5		2,4	10

4.4 Signalling Protocols

Signalling is used for voice calls and video conferencing **call establishment, call monitoring and connection teardown**, and for call registering and billing purposes. There are two sets of standards for VoIP telephony, video and multimedia conferencing: H.323 is an ITU-T standard, prepared by the telecommunication community, while SIP (Session Initiation Protocol) is the alternative IETF standard from the Internet community. H.323 is the older of these, and at this time (summer 2004) it is still better supported by hardware and software manufacturers, although SIP is getting more and more popular. The future will show which one of these solutions will survive, or if they will be replaced by a third one.

4.4.1 H.323

The H.320 series of standards specify multimedia conferencing on switched digital networks. H.323 is the framework standard for multimedia conferencing in packet switched networks that don't provide QoS guarantees. Only voice transmission must be supported by the H.323 terminals, while video and data conferencing are optional.

H.323 relies on the existing standards for voice and video coding, for data transmission, transport and networking. New elements are some signalling standards and the data conferencing standards. Figure 30 presents the H.323 protocol stack and standards, the most important being the following:

- While various network infrastructures, network and transport protocols are supported, the most common solution is to use the TCP/**IP** protocol stack. Voice and video data uses connectionless **UDP** transport, while most signalling protocols and the data conferencing uses reliable **TCP** transport.

- Voice and video data is carried in **RTP** messages. For voice, the G.711 PCM coding is mandatory. If video is supported, the terminal must include QCIF size H.261 (Quarter Common Intermediate Format, 176*144 pixels). The framework also specifies additional coding: G.723.1 ACELP, G.729 CS-ACELP, G.722 and G.728 LD-CELP for voice and H.263 for video. The standard only specifies protocols and coding methods, but an audio or video conferencing application must be implemented separately.

- Data conferencing can be transported over a reliable ISO or TCP/IP transport protocol. Above this lie T.124 GCC (Generic Conference Control), T.125 MCS (Multipoint Communications Services) and T.126 still image exhange or T.127 multipoint file transfer application protocol. Data conferencing applications may include a shared whiteboard and document sharing without a common application software.

- **RTCP** is used for connection monitoring. It provides connection statistics, which can be used by the parties included, by the central network management system and by the network service provider.

- H.225.0 includes signalling protocols for terminal signalling (**Q.931**) and for terminal to gatekeeper signalling (**RAS**, Registration, Admission and Status). The former is a subset of the ISDN subscriber signalling protocol, and the latter specifies terminal registration, call admission, bandwidth reservation and status monitoring with the gatekeeper.

- The **H.245** control channel carries information between terminals about the supported media and coding standards, opening and closing logical channels, flow control information and other general commands.

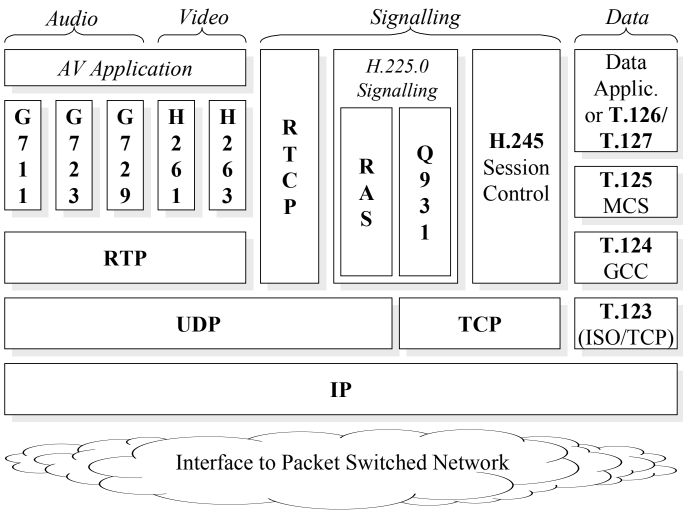


Figure 30: H.323 Protocol Stack.

The next example shows the connection setup phases on a simple voice call between two H.323 terminals. No gatekeeper is included in this example system. As shown in Figure 31, an H.323 VoIP call establishment includes the following layers:

- User of the leftmost terminal initiates a VoIP call, using an H.323 application. After possibly mapping the target person to an IP address, the initiating terminal sends a call setup signalling message. Because this will be carried using the TCP transport, a **TCP connection setup** first takes place, using the three way handshak (with SYN, SYN/ACK and ACK segments). The TCP segments are carried in IP packets, which are transmitted in Ethernet frames.

- The calling terminal sends **Q.931 Setup** message, including Bearer Capability (ITU-T coding standard, unrestricted digital info, packet transfer mode, packet mode call and H.323 voice call protocol), Display information (matti puska as the username) and User-User info (including the username as the H.323 identification, application software information, destination transport address type and contents and a unique conference id).

  This signal alerts the destination VoIP application and causes it to send an Alerting signal back. This message only includes a User-User Information Element, containing the protocol identification for H.225. When the receiver responds (picks up the handset ;-), a Connect message is sent to the originating node. The Connect message includes the bearer capability, receiver display string and User-User info with the receiving application and conference id. Q.931 signalling messages are encapsulated into UDP datagrams and IP packets.

- After the Q.931 call setup, **H.245 signalling** takes place. The initiating terminal sends a Terminal Capability Set message, including details about maximum audio delay jitter, multicast capability and media distribution capabilities. The other terminal first sends a Master Slave Determination, and then acknowledges the Terminal Capability Set message. Now the initiating terminal must acknowledge the Master Slave Determination, then the other party sends a Terminal Capability Set, which will be acknowledged. After these negotiations, the parties open two logical channels, one to each direction. The Open Logical Channel messages include coding and silence suppression details and H.225 parameters. Pay attention to the fact, that Terminal Capability Set and Logical Channel negotiations take place on both directions.

- After the Q.931 and H.245 signalling, the samples are sent using **RTP sessions**, one for each media and for each direction. RTCP provides feedback on the RTP sessions and identifies the RTP parties for channel synchronisation.

- An RTP session is disconnected with an H.245 End Session message, leading to Q.931 Release Complete messages. Finally the other party also sends an End Session message.

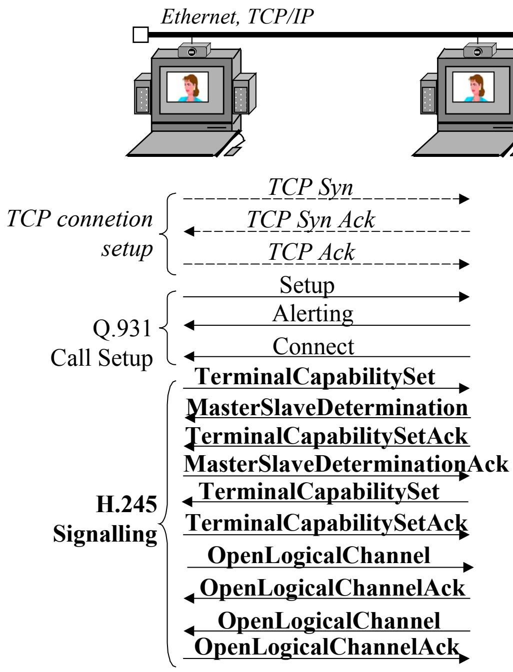


Figure 31: H.323 Call Establishment signalling.

If a gatekeeper is present, the call setup will start with terminal registration to the gatekeeper with ARQ/ACF RAS messages (Admission Request, Admission Confirmation) for both terminals. Additional Q.931 and H.245 messages will also be included. In this case the terminals are always slaves, so no Master Slave Determination is needed. After the Q.931 and H.245 call teardown, the terminals would then disengage from the gatekeeper with DRQ/DCF messages (Disengage Request, Disengage Confirm).

H.245 messages can be tunneled within the Q.931/H.225 signalling messages instead of using a separate TCP session for call control. This makes call setup time shorter, uses less resources and provides synchronization between call signalling and control. Fast Connect makes it possible to establish media connection for simple point-to-point calls with a single pair of messages by including a Fast Start element in the initial call setup message. The Fast Start element includes logical channel and media details and it will be acknowledged by faststart element within a Q.931 signalling message.

The Q.931 message header includes a protocol discriminator (08 for Q.931), a call reference length and data, and message type fields (Figure 32). The signalling information includes zero or more information elements (IEs), containing a type and a value. For variable length IEs, the length information is also provided. IE data is coded using ASN.1 PER encoding (Application Specific Notation number one, Packet

Encoding Rules). Fixed and variable length IEs are distinguished with the first bit of the information element coding. /Ensyclopedia/ /Teleware/ /Davidson, Peters/

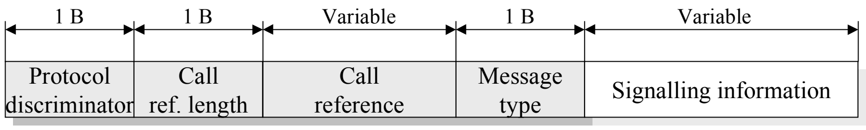


Figure 32: Q.931 message format.

4.4.2 Session Initiation Protocol

The **SIP stack** includes Internet signalling protocols for multimedia conference call establishment, maintenance and clearing. It was developed by the IETF MMUSIC group (Multiparty Multimedia Session Control) and is specified by the RFC 2543 in 1999. It is a simple Internet protocol, based on the Client/Server model and existing Internet protocols, like SMTP and HTTP. Messages are coded with clear text. The protocol stack, as presented in Figure 33, supports any audio and video coding over RTP. The signalling protocols include RTCP connection feedback and party identification, SIP for connection setup, maintenance and clearing, SDP (Session Discovery Protocol) for session parameter negotiation and optional SMIL (Synchronized Multimedia Integration Language), which defines the relations between various multimedia objects. Both the protocol stack and individual protocols are, following the Internet tradition, much simpler than the H.323 protocols. All signalling messages can be transmitted using either connectionless UDP or connection oriented TCP transport. The default SIP port is 5060.

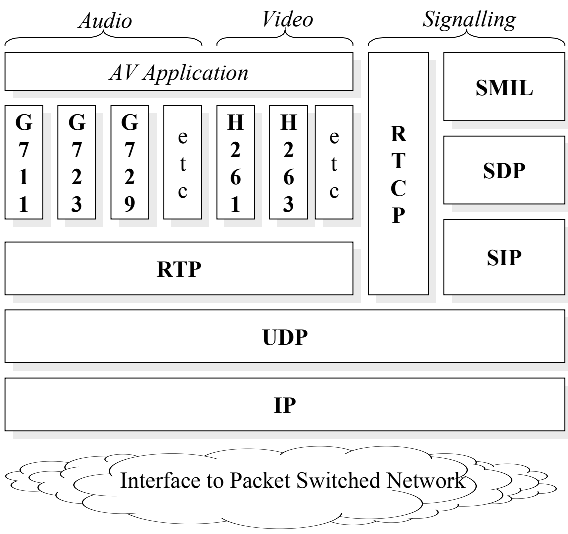


Figure 33: The SIP Protocol Stack.

A SIP system contains **User Agents and Servers** (see Figure 34). A User Agent, which acts on behalf of a user, contains a Client and a Server to initiate and receive calls. The Client always sends SIP requests and receives replies from a server. SIP servers can be categorized as Proxy Servers or as Redirector Servers. The Proxy Server makes a new request to the target on behalf of the actual Client. The Redirector Server sends a redirect response to the actual Client, so it doesn't need a client component.

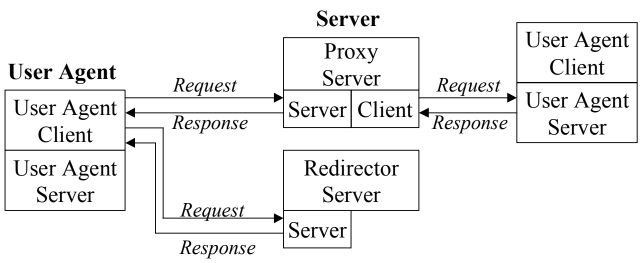


Figure 34: SIP Clients and Servers.

SIP messages are either requests or responses. The client component always sends requests, and the server sends responses. All messages are text encoded with UNICODE characters. Encryption and authentication can also be used, if supported by both parties. The messages contain rows, and each row has a header. A request always starts with a method (INVITE, ACK, BYE, CANCEL, OPTIONS, REGISTER), followed by other rows with headers. A response starts with a numeric response code, which is followed by other rows. There are 37 headers altogether, and they can be categorized into four groups, as shown in Table 4.

Table 4: SIP headers.

General-headers	**Entity-headers**	**Request-headers**	**Response-headers**
Call-ID	Content-Encoding	Accept	Allow
Contact	Content-Length	Accept-Encoding	Proxy-Authenticate
CSeq	Content-Type	Accept-Language	Retry-After
Date		Authorization	Server
Encryption		Contact	Unsupported
Expires		Hide	Warning
From		Max-Forwards	WWW-Authenticate
Record-Route		Organization	
Timestamp		Priority	
To		Proxy-Authorization	
Via		Proxy-Require	
		Route	
		Require	
		Response-Key	
		Subject	
		User-Agent	

In a simple SIP messaging example, shown in Figure 36, a User Agent on 2.0.0.1 wants to make a SIP call to the number +9002 on 2.0.0.2 (*. The User Agent sends an INVITE request, with the request URI, version, source host and user information. It also includes the target user and host.

The user agent on the target host receives the request, alerts the user and sends Trying and Ringing responses. After the user has accepted the call, an OK reply with the status code 200 is returned. The original caller acknowledges the reply with an ACK message to the target host. INVITE , OK and ACK messages also contain an SDP message for capability information.

During the call setup, important parameters, like IP addresses, the TCP port and the audio codecs, are negotiated. Now the user data can be transferred in RTP messages.

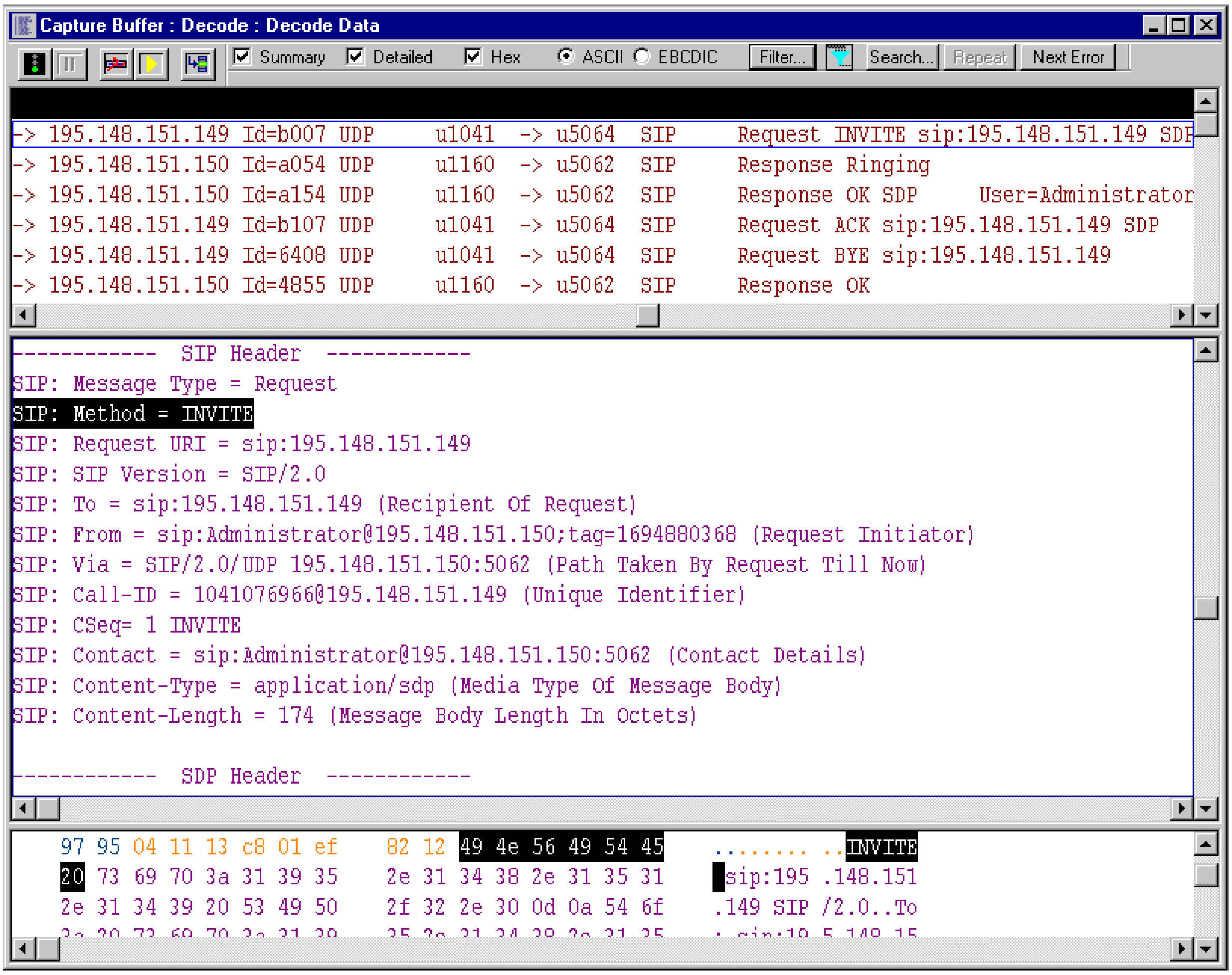


Figure 35: A SIP dialoque during a call establishment and teardown, and a closer look at an INVITE message.

*) The SIP URL can be specified with a user@host, with a phone_number@IP_address, or their combination.

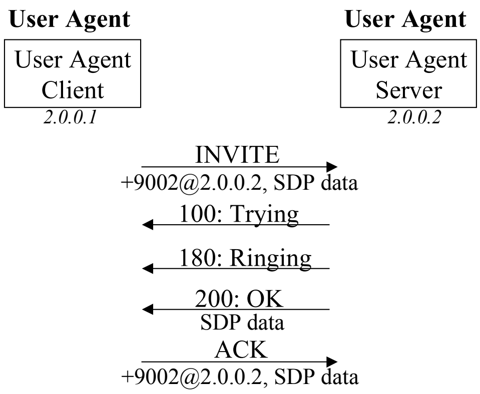


Figure 36: SIP Signalling example.

All SIP messages are encoded with UNICODE text. They have exactly the same format as SMTP messages: a start line, header fields, an empty field (CRLF) and a message body. All SIP headers (see Table 4) contain a name and a value, separated with a colon (:).

The initial SIP INVITE might look like this:

```
INVITE sip:+9002@2.0.0.2 SIP/2.0
Via: SIP/2.0/UDP 2.0.0. 1
From:  +9001@2.0.0.2
To: +9002@2.0.0. 2
Call-ID: ECDA F189-C1F23144-0-F95008C@2.0.0.1
User-Agent: Sipve AS5300, IOS 1 2.x, SIP enabled
Cseq: 100
Content-Type: application/sdp
Content-Length: 112

SDP details
```

The first Request-Line contains the method (INVITE), the request URI (sip:+9002@2.0.0.2) and the SIP version, separated with spaces. The response messages include a status line and generic, response and entity headers, a CRLF and the message body. The status line contains a numeric status code and a textual reason phrase. Some important status codes and phrases are given in Table 5 (*.

*) Pay attention to the similarity to the HTTP reason codes. For compatibility, the SIP specific reason codes have a x8x number.

Table 5: Some status codes and reason phrases for SIP responses.

Class	Code	Reason phrase
Informational		
	100	Trying
	180	Ringing
Success		
	200	OK
Redirection		
	300	Multiple Choices
	301	Moved Permanently
	302	Moved Temporarily
	305	Use Proxy
Client Error		
	400	Bad Request
	401	Unauthorized
	402	Payment Required
	403	Forbidden
	404	Not Found
	405	Method Not Allowed
	408	Request Timeout
	415	Unsupported Media Type
	482	Loop Detected
Server Error		
	500	Internal Server Error
	501	Not Implemented
	503	Service Unavailable
Global Failure		
	600	Busy Everywhere
	606	Not Acceptable

The **SDP protocol** describes media stream details, and SDP messages are transported inside SIP messages. SDP handles session parameters, like name, purpose, time, session media and media details, like addresses, ports, data formats, and optional parameters like bandwidth usage and contact person. The SDP message contains UNICODE encoded *type=value* pairs, one per line. The type is a single character and the value is a structured character line. An SDP message contains a session-level section and zero or more media descriptions, starting with the letter m. The session-level section starts with a v line and each media description line starts with the letter m. The type lines must appear in the order presented in Table 6.

Table 6: SDP session, media and time descriptions. Types presented in boldface are mandatory.

Type	Session description	Type	Media description
v	Protocol version	**m**	Media name and transport address
o	Owner/creator	I	Media title
s	Session name	c	Connection information
I	Session Information	b	Bandwidth information
u	URI of description	k	Encryption key
e	Email address	a	Media attribute lines
p	Phone number		
c	Connection information		
b	Bandwidth information		
Z	Time Zone adjustment	**Type**	**Time description**
k	Encryption Key	**t**	Time the session is active
a	Session Attribute lines	r	Repeat times, if any

An example SDP message, inside the INVITE SIP message, is the following:

```
v=0
o=SipveSystemsAS5300PrototypeVersion 7340 629 IN IP4 2.0.0.1
s=SDP Details Covered
c=IN IP4 2.0.0.1
m=audio  20134 RTP/AVP 0
```

The first line defines the major version number (v) for the SDP protocol. The second line (o) defines the session owner info: username, session id, running version, network type, address type and the address. In this case, the NTP timestamps are not used for session id and version, as recommended in the RFC document. The third and the last mandatory line, starting with the type identifier s, contains the session name.

The next line is optional. Our example includes the connection information (c): the network type (IN for the Internet), address type (IPv.4) and the IP address. The last line gives media announcements, including media type (audio, video, application, data and control being the choices currently defined), TCP port, RTP transport protocol (audio/video profile over the UDP) and the media payload type, defined in the RTP Audio/Video profile.

The **SMIL language** (pronounced smile) makes it possible to integrate multimedia objects into a single synchronised presentation. SMIL documents are XML 1.0 documents (Extensible Markup Language). /RFC 2543/ /RFC 2327/ /Teleware/ /SMIL/

4.5 Mobile IP

4.5.1 Orientation to Mobile IP

Various wireless terminals, like laptop computers, PDAs and digital cellular phones, can use both wired 100BaseT and wireless WLAN, Bluetooth and G3 mobile networks for Internet and intranet access. When only ordinary version 4 or version 6 IP is used as the network protocol, transport and application layer connections (like RTP for real time IP telephony) are lost, when the terminal is moved from one attachement to another. This is due to the following facts:

- IP packets are routed between IP subnets, and every attachement (like 100BaseT wired Ethernet and 802.11b WLAN) must have a different IP subnet.

- IP router compares the network part of the destination address on the packet with its local routing table and forwards the packet towards the destination (Figure 36). The destination host is reached only if the packet contains a proper IP address from the destination subnet.

- Every IP host keeps a connection table, which identifies a connection with source IP address, source TCP port, destination IP address, destination TCP port quadruple, as shown in Figure 37. If any of these parameters is altered, the connection is lost. An example of connection table entries is the following (*:

```
[matti@linux matti]$ netstat -n -t
Active Internet connections (w/o servers)
Proto Rcv-Q Snd-Q  Local Address       Foreign Address       State
tcp       0     0  192.168.2.2:80  192.168.1.200:1176  ESTABLISHED
tcp       0     0  192.168.2.2:80  192.168.1.200:1175  ESTABLISHED
tcp       0     0  192.168.2.2:80  192.168.1.200:1174  ESTABLISHED
tcp       0   126  192.168.2.2:23  192.168.1.200:1173  ESTABLISHED
...
```

*) The screen capture is from a UNIX server. Parameter n displays values in numeric form, -t displays only TCP sockets. The netstat command is also usable in MS Windows platforms, but the parameters may be different.

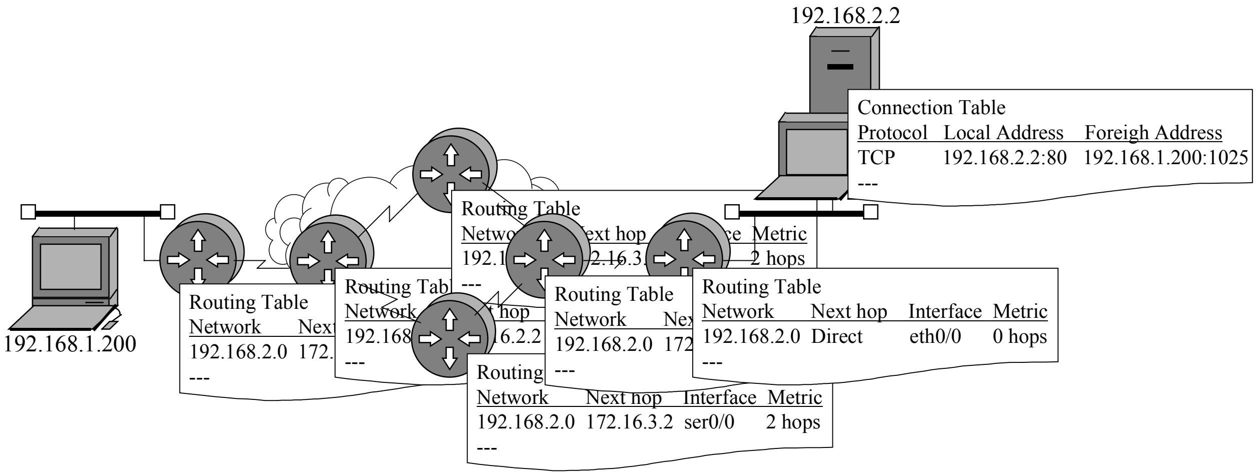


Figure 37: IP routing is based on local routing tables, while a connection is identified by source and destination IP address and TCP port.

Mobile IP, as defined in RFC 2002, addresses the problem by **using two IP addresses for mobile hosts: a fixed home address and an attachement dependent care-of address**. The static home address is used to identify transport layer connections, while the topology dependent care-of address is used by routers to reach the current mobile host location. A home agent maps the two addresses together, redirects and tunnels packets to the care-of address. Roaming is achieved by mobile node registration. The target server keeps the home address on its connection table, and doesn't know anything about the care-of address. Internet and Intranet routers read only the outermost care-of address and are able to route packets to the current attachement. /RFC 2002/

4.5.2 Mobile IP Operation

Every mobile host has a static home address, which is used to reach the node. If a Fully Qualified Domain Name (FQDN) is needed for the host, it will be mapped with the home address. On every visited attachements the mobile node must have a care-of address from the attachement subnet. DHCP can be used to automate address delivery. A home agent is needed on the home network to map addresses. Optional foreign agents may be used in foreign networks to assist home agent and mobile host discovery.

An ordinary Mobile IP connection includes the following steps (Figure 38):

1: Home and foreign agents advertise their presence with periodic ICMP Router Advertisement messages (Agent Advertisement). These messages make it possible for mobile nodes to discover whether they are connected to the home or a foreign network.

2: In home network, mobile node is reachable by its home address and operates without mobility services. All connections are identified by the home address.

3: When moved to a foreign network, mobile node obtains a care-of address either from the foreign agent (a foreign agent care-of address) or from a DHCP server (co-located care-of address). In some cases also a preconfigured co-located care-of address may be used.

4: On a foreign network mobile node registers its new care-of address with its home agent, using Mobile IP Registration Request and Reply messages. During registration the home agent updates its home to care-of address mapping. Registration may take place directly or through a foreign agent.

5: Correspondent Node sends packets to the home address of the mobile node, because this is the only address it knows. The home agent captures the packets and tunnels them to the care-of address. On the other end of the tunnel, foreign agent strips of the extra IP header and delivers packets to the mobile node.

6: Mobile node sends return packets directly to the Correspondent Node using standard IP routing mechanism. No tunneling is needed and packets don't pass through the home network.

7: When the mobile node roams to another attachement, it will ackquire a new care-of address and reregister it to the home agent. The correspondent node will not notice any difference, while it is sending packets only to the home address of the mobile node.

8: If the mobile node returns to its home network, it discovers this fact by receiving an Agent Advertisement from its home agent. It then deregisters with the home agent with Registration Request and Reply messages and starts operating without mobility services.

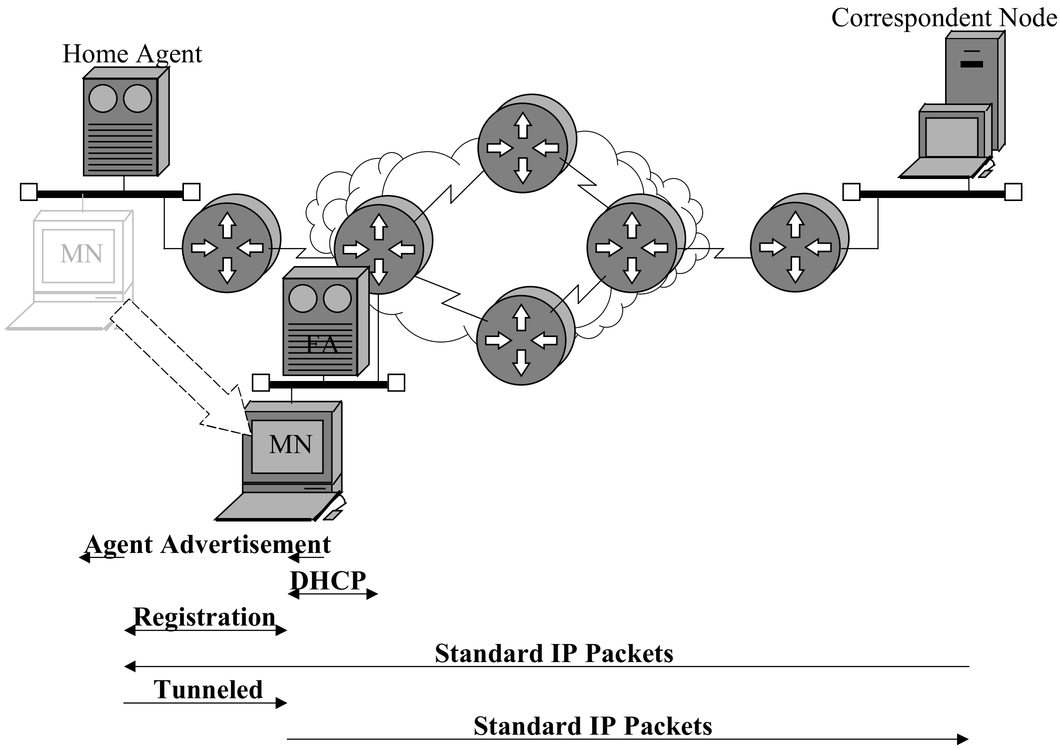


Figure 38: Home and Foreign Agent Advertisements, Mobile Node Registration and IP packet flow on a Mobile IP network. As shown, Mobile IP may lead into suboptimal routing.

IP packet flow on a Mobile IP network is shown in Figure 39. Mobile Node is reachable with its home address, and the correspondent node sends IP packets to the home network using standard IP routing. After registration, the home agent knows the care-of address, encapsulates the arriving IP packets with a new IP header and sends them through a tunnel to the foreign agent. This decapsulates the packets and forwards them to the mobile node using standard IP routing. Return packets are send directly from the foreign network to the correspondent node, without passing the home network, using standard IP routing. If the mobile node ackquires a co-located care-of address from a DHCP server, the end of the tunnel is situated at the mobile node and no Foreign Agent is needed. /Perkins/ /RFC 2002/

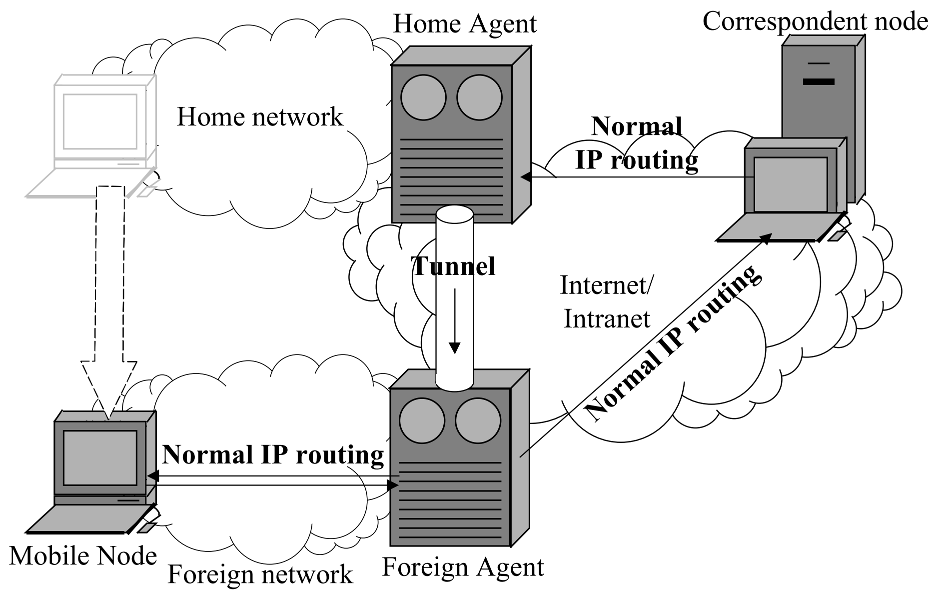


Figure 39: IP packet flow on a Mobile IP network.

4.5.3 IP tunneling

Correspondent Node knows the Mobile Node only by its Home Address (MH), and sends any IP packets to this destination. Packets are routed to the home network of the MN, and the Home Agent encapsulates them with a new IP header. This tunnel header includes the IP address of the Home Agent (HA) as the source, the Care-of Address of the Mobile node (COA) as the destination, i.e. tunnel end and 4 as the protocol identification to indicate, that the tunnel packet includes an IP packet. The foreign agent or the Mobile Node decaptulates the packet, exposes the original packet with the original addresses and forwards it to the Mobile Node. As shown in Figure 40, the original packet includes the IP address of the Correspondent Node as the source address, the Home Address of the Mobile Node as the destination and relevant protocol identification, 06 for TCP in our example.

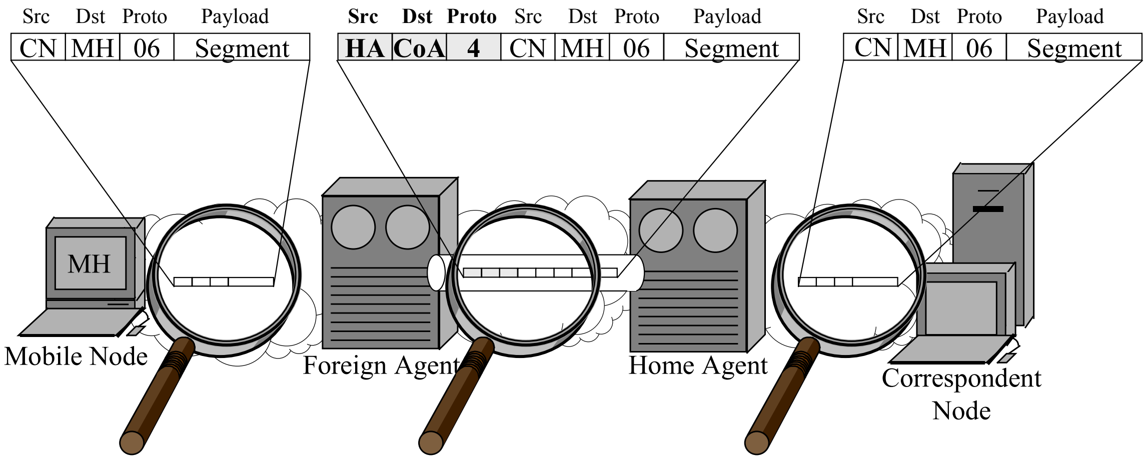


Figure 40: Addresses in Mobile IP tunneling.

Normally IP-within-IP encapsulation is used, preserving the full original IP header within the tunnel header. Another possibility is to use minimal encapsulation, which combines some pieces of information of the tunnel header with an inner minimal encapsulation header. This latter method reduces header overhead, but requires more complex processing in tunnel ends. /Perkins/ /RFC 1256/

4.6 ENUM

4.6.1 Internet Names and International Phone Numbers

DNS (Domain Name System) is a distributed name resolution system, that enables Internet users to surf by entering URL:s (like www.evtek.fi) and send E-mail by using name@organisation.top-level-domain mail addresses. The DNS system is based on DNS name servers with hierarchical responsibilities. A DNS server contains records for resources, as shown in Table 7.

Table 7: Some common DNS Record types.

DNS Record	Resolution	Records file
A	From FQDN to IP address	evtek.fi
MX	From Domain to mail server FQDN	evtek.fi
NS	From Domain to name server FQDN	evtek.fi
PTR	From IP address to FQDN	144.148.195.in-addr.arpa

On the other hand, public switched telephone network uses national and international numbering plans, that make it possible to call from to any terminal, regardles of the receiver local access provider, by simply entering either the subscriber number with or without the region prefix or a country code, region prefix and subscriber number from the keypad. The international telephone numbering is governed by E.164 regulations.

4.6.2 ENUM Extensions to DNS

ENUM is an extension to traditional DNS records, that makes it possible to find services in the Internet by using either a keypad on a telephone set or qwerty keyboard on a computer. ENUM adds a NAPTR (Naming Authority Pointer) record, that maps international E.164 numbers to Internet URI:s (Universal Resource Indicators). As shown in Figure 41, traditional DNS uses hierarchy to guarantee the uniqueness of a Fully Qualified Domain Name. The name space starts from the root, presented with a dot (.), and ICANN grants a limited amount of top-level domain identifications, for countries (like fi for Finland) or for certain types of organisatinons (like com for commercial organisations). In Finland, Finnish Communications Regulatory Authority grants site identifications, ensuring uniqueness of the fi branch. Companies or organisations may use group or local identifies based on their need. For reverse address to name resolution, in-addr.arpa identifiers are used. Pay attention to the fact that the highest DNS hierarchy is presented at the end of the FQDN, so the IP subnet information must be reversed for PTR resource records.

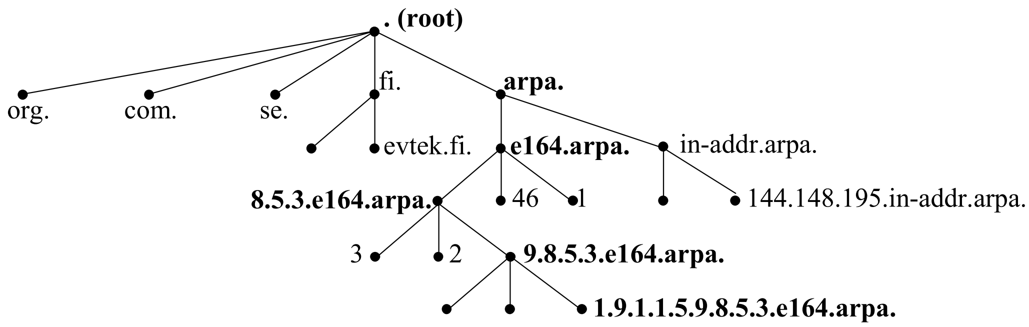


Figure 41: DNS name hierarchy.

ENUM adds e164 branch underneath the arpa, and this is used to hold records of international telephone numbers. Just underneath e164 there will be branches for international country codes (358 for Finland, 1 for USA etc). Because of the highest-at-the-end hierarchy, the phone numbers must be reversed (making Finland 8.5.3.e164.arpa.). Underneath this, there will be regional prefixes according to the national numbering plan, and subscriber numbers for each region.

4.6.3 Number to URI Resolution

The following procedure will be used to convert a phone number to DNS names:

1: The telephone number is presented as an international E.164 phone number, including country code, regional prefix and subscriber number (like +358 9 51 191)

2: All characters, expect digits, will be removed, including spaces and special characters. Our example phone number will be 358951191

3: The order of the digits will be reversed, leading to 191159853

4: A dot will be placed between each digit, resulting 1.9.1.1.5.9.8.5.3

5: .e164.arpa will be appended at the end of the character string. The result will be a Fully Qualified Domain Name for the E.164 phone number, 1.9.1.1.5.9.8.5.3.e164.arpa

When a phone call is to be made, a SIP User Agent or other ENUM capable terminal will issue an Invite message, containing the target FQDN. The target will be resolved by an authoritive DNS server to a Universal Resource Locator, that contains the protocol identification, username, group if any, site and top-level domain for the called person (Figure 42). The call will be handled by a server of the called organistaion, until the user terminal will be reached.

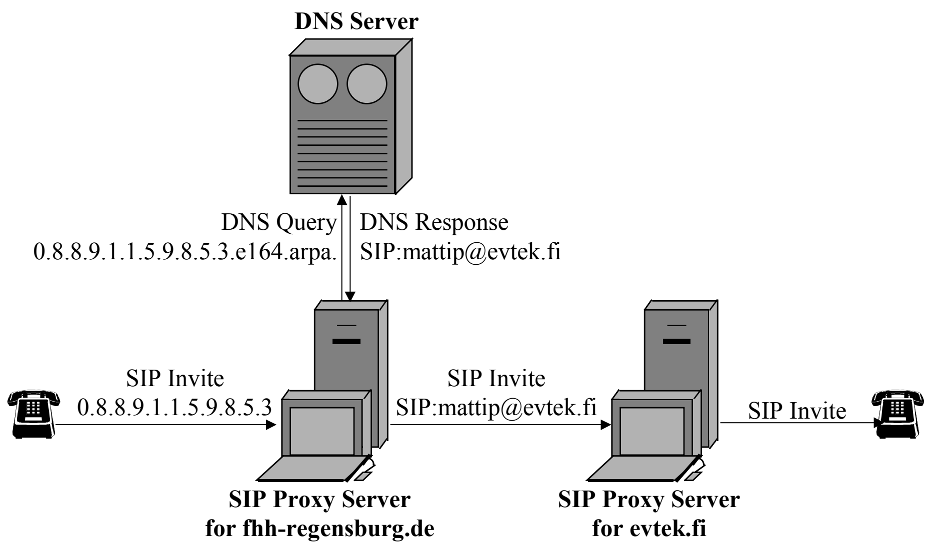


Figure 42: Making a call using ENUM.

ENUM applications may include voice calls, video conferencing, E-mail, instant messaging or virtually any application, that provides reachability.

4.7 Security Issues and Solutions

While Voice over IP technology is extensibly used in public telecommunication networks and for corporate telephone services, security concerns should be taken seriously. New legistlation puts hard demands on communication privacy both on public and private networks. On top of the standard PSTN security concerns, the following technical facts make packet based VoIP systems more vulnerable to misuse, tapping and service distruptions:

- It is much easier to tap a packet based IP network than a circuit switched telephone network. LANs, MANs and WANs are easier to access physically and frames or packets may be directed to a false location by manipulating address, routing or name information. By default, both signalling messages and voice data is transmitted in clear text, so call records and conversation contents are exposed to a sniffer.

- Subscriber identification is often based on terminal address or username and password. Frauding a MAC or IP addressis easy and passwords are often guessable, making it possible for the cracker to take a new user identity.

- Equipment, user, call routing and call record databases reside on standard servers, that are connected to corporate intranet. There is a risk that an attacker may list or manipulate subscriber information on the server.

- It is possible to distrupt IP telephony services by generating massive amounth of packets to IP PBX, gateway or database server, or to generate excessive faulty requests by manipulating signalling, control or data packets.

- Voice over IP is a new technology, making it an attractive target for various Internet hackers and crackers.

Besides physical and logical access security, encryption is often used to provide confidentiality, message authentication for integrity and key exchange technologies to distribute security credentials safely. Without diving into security policies, encryption algoritms, firewall configurations and other data security details (that are not the main scope of this course), I want to introduce Secure RTP. It is a standard based application layer authentication and encryption solution for RTP and RTCP streams.

SRTP encrypts the RTP payload, so a sniffer will retrieve useless noise instead of clear conversation. SRTP also inserts a Master Key Identifier (MKI) and Authentication Tag at the end of every RTP and RTCP message, which secures the message header and payload, and any alterations or reuse attempts will be discovered (Figure 43). SRTP is a lightweight authentication and encryption solution, that is easy to implement on low level IP phone terminals. Secure RTP doesn't specify any specific key exchange solution for Master Key distribution, and it doesn't protect signalling messages. /RFC 3711/ /Greenstreet/

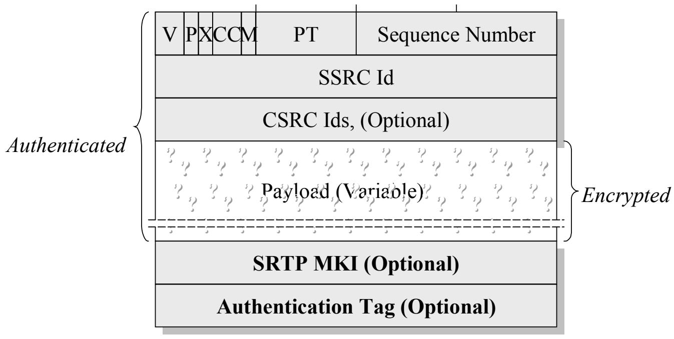


Figure 43: Secure RTP Message. RTCP messages will be authenticated and encrypted at the same way.

4.8 Review

Voice and video over IP systems encapsulate application information into RTP messages, which are transported in UDP datagrams in IP packets. Realtime Transport Protocol offers packet loss detection and packet reordering and timing, which are not included in connectionless UDP transport. It also provides media, coding and source identification. No standard port is defined for RTP, but parties agree on unused even port numbers, one for each full duplex media stream. RTCP, which provides feedback on RTP transport, detailed source information and multiparty conference participant information, uses the next odd UDP port. RTCP information may be used to monitor round-trip propagation time, to exchange username and hostname and reason for leaving the conference.

RTP messages carry voice and video information. If no compression is used, PCM voice codec produces 64 kbit/s fixed line telephone quality voice. Waveform coding may compress voice up to 3:1 by manipulating the signal waveform. Hybrid codecs combine natural voice quality and low bit rate, producing compression ratios up to 16:1. For even higher compression ratios up to 32:1, voice sound modelling, which only transmits model parameters, must be used, but the price is poor sound quality. Silence suppression saves in average additional 50 % of bandwidth. Compression must always be used for digitized video. Video compression methods use intraframe and interfame compression and reach 200:1 ratios with quality suitable for commercial video broadcasting. High video compression ratios also need lots of processing power from the terminal.

H.323 is an ITU-T standard for multimedia conferencing over packet switched networks without QoS guarantees. It uses existing TCP/IP, RTP, RTCP and coding standards and includes Q.931 signalling between terminals, RAS signalling between a terminal and a gatekeeper and H.245 signalling between terminals for media details, logical channels and flow control. Newer H.323 versions try to standardise every option and supplementary service, leading to an extremely complex package. SIP is the IETF alternative for a singnalling standard, prepared by the Internet community. Following the Internet principles, it reuses existing TCP/IP protocols and ideas and specify a simple layered protocol stack for signalling. SIP, on top of UDP or TCP transport, provides means to setup, maintain and clear multimedia sessions. SDP, transmitted inside SIP messages, offers session parameter negotiation and optional SMIL, on top of SDP, makes it possible to integrate multiple media streams into a single multimedia presentation. All SIP and SDP messages are encoded in clear text, while a SMIL document uses readable XML encoding.

4.9 Quiz

- List the protocol stack, i. e. the set of protocols, for VoIP voice data
- List three services, essential to Real time applications, that RTP adds to UDP transport
- List three services offered by RTCP
- What is the UDP port used for Realtime Transport Protocol (RTP)?
- What is the bit rate of G.711 PCM voice codec?
- Explain shortly the operation of G.723 ADPCM voice coding
- Explain shortly the operation of 2,4 kbit/s LPC voice coding
- Explain shortly the effect of silence suppression
- Why video compression is normally used?
- Why Compressed Realtime Transport (cRTP) is used?
- What is the highest compression ratio for acceptable voice quality?
- What is the highest compression ratio for accepable video conferencing?
- Why signalling is needed in a VoIP system?
- What standards body has published the H.323 standards?
- What signalling protocols are used in a direct call between two H.323 terminals?
- What signalling protocols are used between a H.323 terminal and a H.323 Gatekeeper?
- List the Q.931 messages during a call setup
- What standards body has published the SIP standard?
- List shortly SIP signalling protocols and their usage?

- Explain shortly the difference between the operation of a SIP Proxy Server and a SIP Redirector Server
- List the different fields of a SIP Respose Message

4.10 Material

/Puska/ Matti Puska: Broadband Networks. Evitech Course Handouts, 2003.

/RFC 1889/ H. Shulzrinne et. al: RTP: A Transport Protocol for Real-Time Applications. RFC 1889. IETF, Audio-Video Transport Working Group, 1996.

/ETSI/ GSM 06.10 (ETS 300 580-2): Digital cellular telecommunications systems (Phase 2); Full rate speech, Part 2: Transcoding (GSM 06.10 version 4.1.1) ETSI, 1998.

/Otolith/ Wil Howitt: Linear Predictive Coding (LPC). Otolith, 1995.

/Ensyclopedia/ An Internet Encyclopedia: Q.931 Protocol Overview. Internet, <URL: http://www.freesoft.org/CIE/Topics/126.htm>

/Teleware/ IP-puhe. Teleware Oy, course handouts.

/Michaely/ B. Michaely: In Depth H.323 Overview. Comverse Network Systems, 2000. Internet, <URL: http://www.h323.org>

/Davidson, Peters/ Jonathan Davidson, James Peters: Voice over IP Fundamentals. Cisco Press, 2000.

/RFC 2543/ M. Handley, H. Shulzrinne, J. Rosenberg: SIP: Session Initiation Protocol. RFC 2543. IETF, 1999.

/RFC 2327/ M. Handley, J. Jacobson: SDP: Session Description Protocol. RFC 2327. IETF, 1998.

/SMIL/ W3C: Synchronized Multimedia Integration Language (SMIL) 1.0 Specification. W3C Recommendation. W3C, 1998.

W. Yeong, T. Howes, S. Kille: Lightweight Directory Access Protocol. RFC 1777. IETF, 1995.

/LDAP HOWTO/ Luiz Ernesto Pinheiro Malere: LDAP Linux HOWTO. LDP, 2001.

/Perkins/ Charles E. Perkins: Mobile Networking Through Mobile IP. Internet, <URL: http://www.computer.org/internet/v2n1/perkins.htm>

/RFC 2002/ C. Perkins, ed.: IP Mobility Support. RFC 2002. IETF, 1996.

/RFC 1256/ S. Deering, ed.: ICMP Router Discovery Messages. RFC 1256. IETF, 1991. Configuring Mobile IP. Cisco, 2002. Internet, <URL: http://www.cisco.com/univercd/ cc/td/doc/product/software/ios121...>

/RFC 2508/ S. Casner, V. Jacobson: Compressing IP/UDP/RTP Headers for Low-Speed Serial Links. RFC 2508. IETF, 1999.

/RFC 3545/ T. Koren et. al.: Enhanced Compressed RTP (CRTP) for Links with High Delay, Packet Loss and Reordering. RFC 3545. IETF, 2003.

/RFC 3611/ T. Friedman et. al.: RTP Control Protocol Extended Reports (RTCP XR). RFC 3611. IETF, 2003.

/Clark/ Alan Clark: RTCP XR measures VoIP performance. Network World, 2003. Internet, <URL: http://www.networkworld.com/news/tech/2003/117techupdate.html>

/RFC 3711/ M. Baugher: The Secure Real-time Transport Protocol (SRTP). RFC 3711. IETF, 2003.

/Greenstreet/ Debbie Greenstreet: Security Challenges in VoIP Applications. Internet Telephony, October 2003.

5 IP Telephony Systems

5.1 Traditional and IP Based Branch Exchanges

A Private Area Branch Exchange (PBX) is a piece of Customer Premises Equipment (CPE), owned by the user organisation. A PBX concentrates subscriber telephone lines into trunk links that are connected to the Public Switched Telephone Network. Local calls within the organisation are done within the PBX, never pass the PSTN and are not tariffed. Traditionally, a PBX is a separate system, consisting of vendor specific hardware and software, and needing feature phones from the same manufacturer for additional services (see Figure 41). The only standards based interfaces are the E1/T1 trunk lines to the PSTN. The CTI API also includes vendor specific parts.

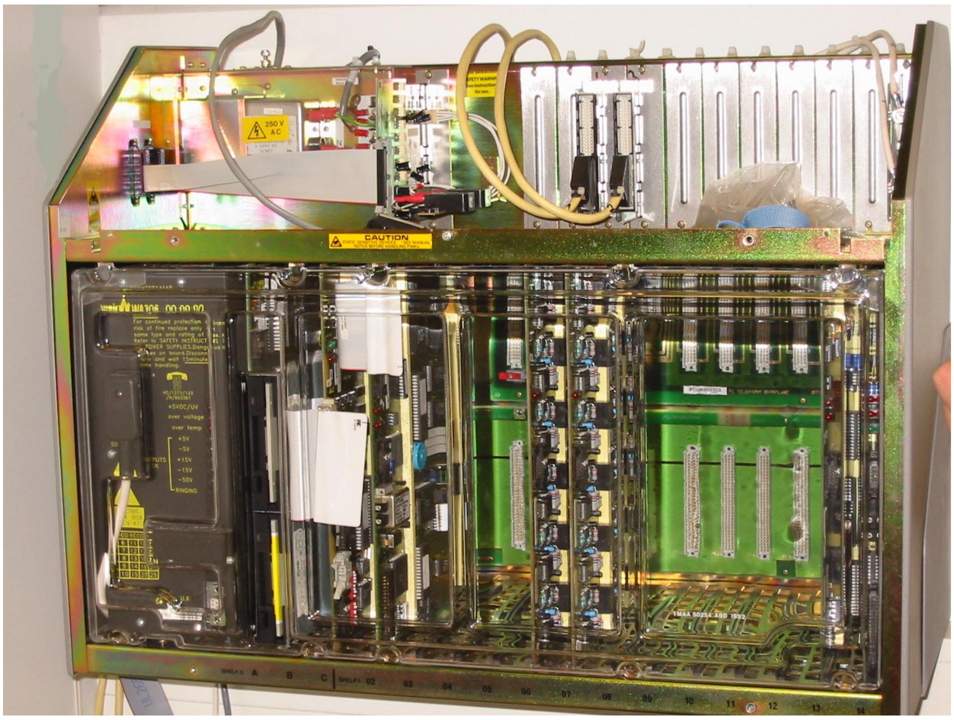


Figure 41: Nokia ISDX Private Area Branch Exchange.

PBXs on different factories and offices may be connected together with leased lines. This makes the PBXs from the same manufacturer act as a single exchange, so additional services, like call transfer, hunt groups and conference calls, are available to corporate users. Additional traffic, exceeding the trunk capacity, can be directed through the PSTN with normal tariffs.

A vendor specific PBX can be replaced by an IP PBX, which uses general purpose hardware, general purpose operating system and standards based network connection and protocols. As shown in Figure 42, terminals only contact the IP PBX for call setup. The IP PBX may provide directory services for the called party identification, it makes the call routing decision based on target information, assists on finding a suitable coding method supported by both terminals and the voice network and handles address resolution. Final call signalling can be done only between the terminals, and the voice traffic also travels directly between the terminals. When the call is terminated, the terminals inform the IP PBX, so the bandwidth reservation is cancelled.

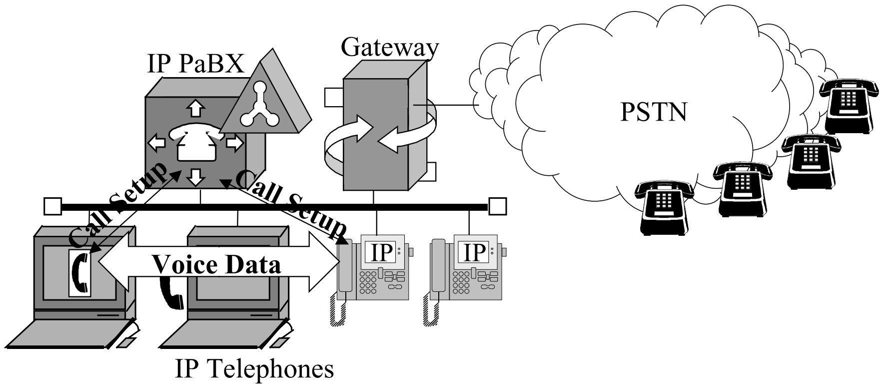


Figure 42: An IP Private Area Branch Exchange system.

The IP PBX has a normal LAN interface, and it uses TCP/IP protocols and standards based signalling protocols. IP telephones, like Ethernet attached feature phones, WLAN IP phones, software based IP telephones and systems with DSP hardware, are using TCP/IP protocols, RTP application protocol and a standards based signalling protocol. All network interfaces are open, so hardware and software components from different manufacturers should interoperate. Also video conferencing systems may be supported.

IP telephony terminals can be situated in the local LAN, in a WLAN (Wireless LAN), or in the corporate intranet. Limited access can be granted to terminals connected to the public Internet. If the IP PBX finds out that the destination lies on the PSTN, the call is routed to the gateway, which makes the necessary physical and logical conversions. Naturally also incoming calls from the PSTN are accepted and routed by the IP PBX. Standard APIs are provided to CTI applications.

An IP PBX offers a possibility to integrate all data and voice terminals in a single network infrastructure. Advanced coding methods make the bandwidth consumption lower. While only the call setup signalling travels through the IP PBX, a low speed connection is enough for the branch exchange. The system offers open interfaces, vendor independency and easier integration with the IT system. On the other hand, LAN telephony needs a totally different approach to network and server reliability than before. The technology is new and standards are still evolving, so early adopters must be prepared for technical and interoperability problems.

5.2 H.323 System

5.2.1 Building Blocks

As presented in the previous chapter, H.323 is an **ITU-T standard for multimedia conferencing** system and signalling **in packet switched networks**. An H.323 system consists of the following components (see Figure 43):

- **H.323 terminals** use H.323 signalling with other terminals and with the servers. They must support voice with G.711 PCM coding. Additional audio coding systems, as well as video and data conferencing are optional. H.323 voice terminals include Ethernet attached feature phones, IP telephony software, which uses the PC sound card and software coding, and products that use a dedicated DSP interface card on a PC. Video and data conferencing applications are also available.

- A **Gatekeeper** is an optional component in the H.323 standard, but needed for business systems. It controls the amount of H.323 traffic on the TCP/IP network with call admission. The gatekeeper may also perform name to address resolution services and address mapping between the IP and PSTN numbers. In H.323 products, directory services and advanced call handling is often performed in the gatekeeper server. Windows based gatekeeper software is normally commercial, but there are free Linux applications available.

- A **Gateway** is also an optional component, which provides connection to the PSTN, IDSN, traditional PBX and other H.32x terminals or an interface to traditional telephone sets. The gateway handles coding translation, signalling and call control conversions, and opens connections to the PSTN network. For circuit switched terminals, the gateway looks like a PBX.

- An **MCU** (Multipoint Control Unit) is an optional component, which is needed if the IP Telephony system supports multipoint conference calls between three or more terminals.

- **Border Elements** (BEs), also optional H.323 components, exchange address information and assist on call authorization between different administrative domains. A BE is often co-located with a Gatekeeper.

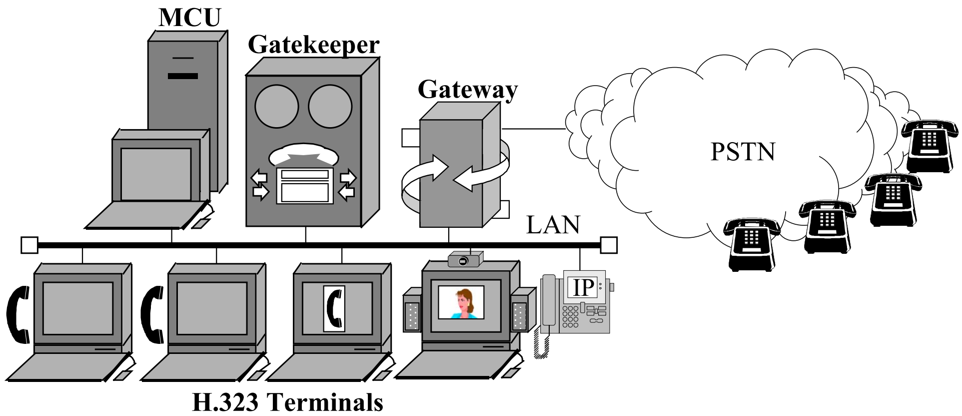


Figure 43: H.323 components.

The H.323 system components are just functional units, mentioned in the standard. The server components can be named and combined freely, or additional functions can be added to them. In many cases, call control, billing and directory services are also performed in the physical gatekeeper component.

5.2.2 Terminals

An H.323 terminal provides a bidirectional audio, video or data conversation. All terminals must suppport audio, with the ITU-T G.711 PCM coding. If video is supported, the video terminal must include H.261 coding. Intelligent terminals may also include T.120 data conferencing services, like a common whiteboard, file sharing and document sharing without a common application software. The standard offers optional lower bit rate G.723.1 and G.729 audio coding and H.262, H.263 and MPEG-4 video coding. Other optional parts are security, multipoint connections, camera control and channel aggregation.

An example H.323 audio terminal is a cisco 7940 feature phone, which is attached directly to an Ethernet LAN. The unit gets the power from a separate mains adaptor or from a switch feeding DC power to the terminals with unused pairs. While a workstation may be attached to the internal switch of the IP telephone set, a single twisted pair link is enough for the workplace. The device includes a large LCD display, multiple feature buttons, a speaker and all common feature phone functions. The operation of the feature buttons may be downloaded from the central server. Figure 44 includes a photo of the cisco 7940 IP telephone set.

Figure 44: cisco 7940 IP telephone. /Cisco/

Another example is the common Microsoft NetMeeting software, which includes all optional H.323 media. It uses the sound card of the PC, additional speakers and a microphone for audio, offering G.711 A law and µ law, G.723.1 and a selection of non-standard encoding methods, all with comprehensive settings. For video, only size and the selection between fast movement versus high quality is offered. As Figure 45 shows, the application includes various data conferencing tools, including program sharing, chat, shared whiteboard, file transfer and desktop sharing. The calls can be made using the Microsoft Internet Directory, with the target address or with speed dialing.

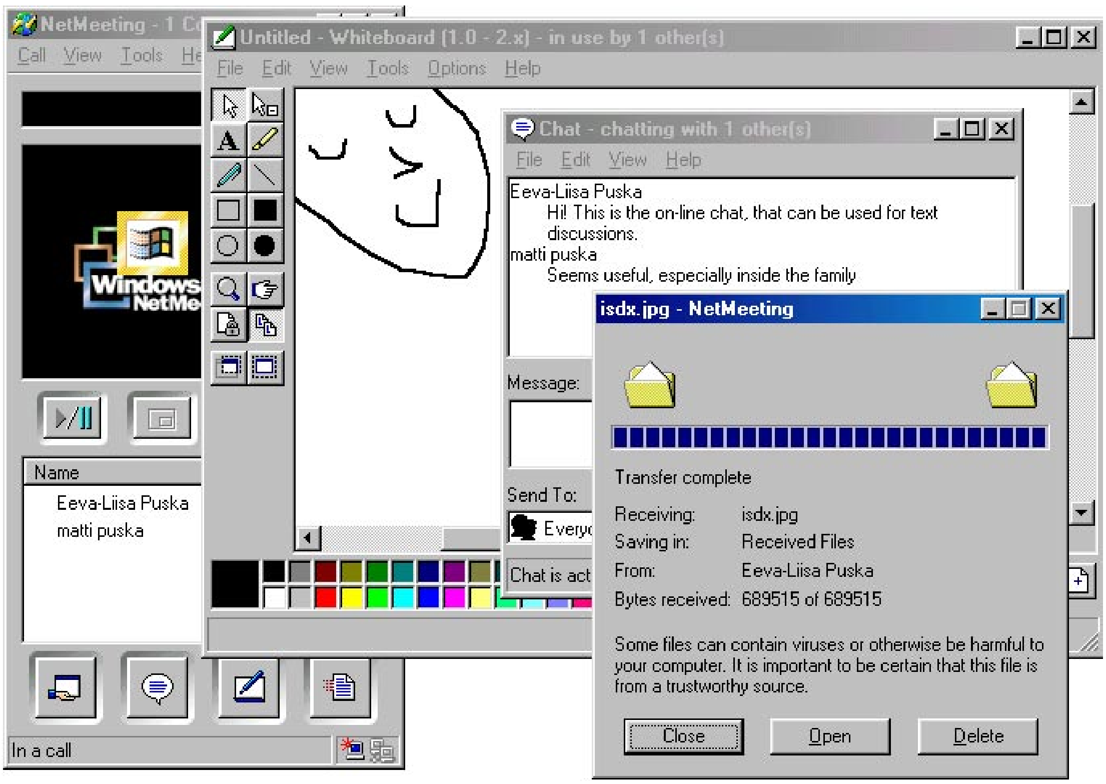


Figure 45: Microsoft NetMeeting version 3.0 data conferencing tools.

Often stand-alone H.323 terminals, like IP telephones, receive their IP settings using DHCP. DHCP leases an IP address to the terminal, and records the MAC address of the client. All necessary IP parameters can be distributed from the DHCP server, making terminal configuration easy (*.

The H.323 version 3 Annex F specifies a Simple Endpoint Type, which is intended for a lightweight user terminal, replacing a full featured H.323 terminal. A SET includes new terminal devices, like palmtop computers with H.323 audio, Ethernet telephone sets, text phones, cellular IP telephones and generation 2,5 or 3 mobile phones, supporting audio and data applications. Full blown H.323 terminals and SETs can take advantage of the H.323 mobility, which is also under construction, based on the H.323 version 4 basic definition choices (**.

5.2.3 Gatekeeper

A gatekeeper is an optional H.323 component. If it exists on the network, all terminals must use it. A gatekeeper is responsible for its H.323 zone, consisting of terminals, gateways and MCUs, as shown in Figure 46.

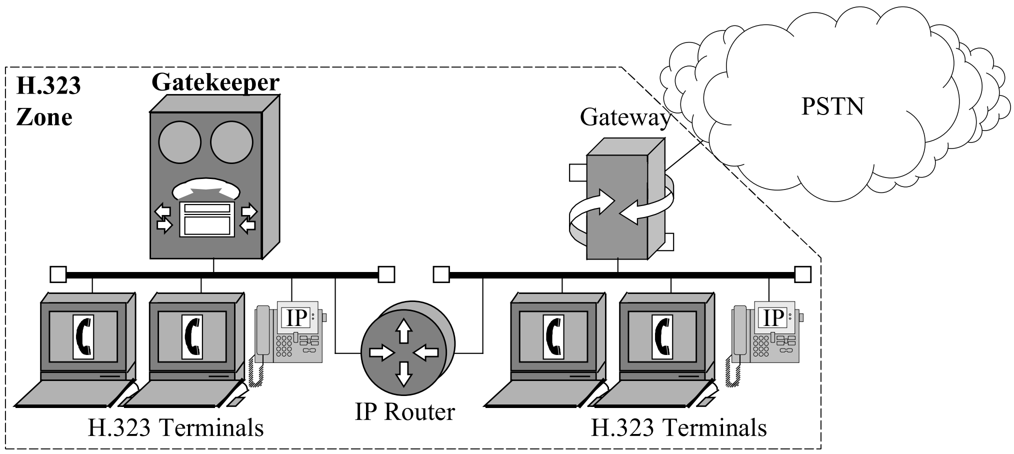


Figure 46: H.323 Zone.

*) Anyone who has tried to issue an IP address, a subnet mask and a default gateway address from the keyboard of a telephone set knows the difficulties.

**) IETF SIP is chosen as the only VoIP signalling protocol for UMTS and 3G mobile networks.

The mandatory functions for a gatekeeper are the following:

- Gatekeeper **transforms the H.323 aliasname** into an IP address of the terminal. To be able to perform this task, terminals register themselves to the gatekeeper, which keeps an up to date table. Other methods can also be used for name resolution.

- **Controlling terminal access** to the H.323 network. Admission control can be based on authorization, available bandwidth or some other criteria. As a null function, all terminals are allowed to join.

- **Controlling the bandwidth** used for H.323 connections. When making a call, the terminal sends a request, which is accepted or rejected based on the bandwidth reserve. A terminal may request for additional bandwidth during a call, and the request is processed by the gatekeeper. As a null operation, all calls are allowed.

- **Zone management**: the gatekeeper provides services to terminals, gateways and MCUs in its zone.

A H.323 gatekeeper can perform other optional functions, such as:

- Call authorization, based on the calling and called terminal, time of day or some other criteria
- Logging calls for statistics, bandwidth management or billing
- Processing signalling messages for call control
- Offering directory services, receiving queries and returning receiver information.

Signalling between a gatekeeper and an H.323 terminal is covered by the H.225.0 RAS standard, which is explained in chapter 5.2.7.

5.2.4 Multipoint Control Unit

A MCU is an optional H.323 component, which is needed for telephone, video, data and multimedia conferences between three or more terminals. Conference participants, often in different locations and zones, have different terminals, which may use different coding methods. The MCU controls and allocates conference resources and may perform translation between codecs. An MCU consists of a Multistation Controller (MC) and zero or more Multipoint Processors (MPs). The MC controls the conferences, provides capability negotiation and allocates conference resources if needed. One of these resources might be the MP, which processes audio, video and data streams centrally, and provides mixing and transcoding functions.

In a video switching conference, the audio and video stream follows the talker by voice activation. This kind of conference mode needs some practice, and is best suited for lecturing. A continuous presence conference uses video mixing, participants have video views of all parties, and only voice follows the talker. A MCU with a video MP is needed for a continous presence conference. An audio MP is used, if the parties use different audio transcodecs.

The H.323 standards also specify conference control. The terminals first make a call to the MCU. After Master/Slave determination and capability negotiations, the multiparty conference is established and contolled by the MCU.

5.2.5 Gateway

The gateway is also an optional H.323 component. It is only used, if the H.323 system is connected to a non-H.323 system, like H.320 ISDN video conferencing systems, PSTN or ISDN telephone networks or terminals, H.310 ATM video conferencing systems or V.70 audio & video systems.

As shown in the example of Figure 47, a gateway has two interfaces: an H.323 interface and a non-H.323 interface. The gatekeeper initiates a call to the PSTN, and the gateway sets up the call and provides signalling conversions (Q.931/H.245 to SS#7), as well as coding translations, if needed. The PSTN network sees the gateway as a digital PBX.

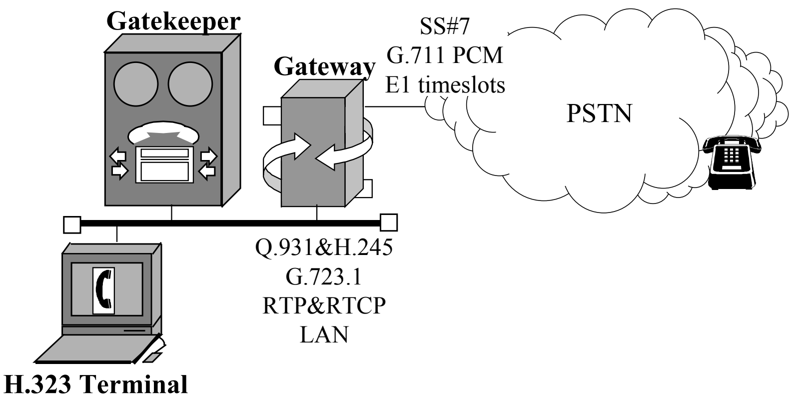


Figure 47: H.323/PSTN gateway.

The H.323 standard leaves many gateway details open. Number of simultaneous H.323 connections, and the audio and video conversion details are left to be specified by the vendor. A gateway, being a virtual component, can be combined with other H.323 servers.

5.2.6 The Network

The H.323 standard specifies multimedia conferencing protocols over a packet switched network. Normally H.323 terminals are attached to a switched Ethernet LAN, and leased line, Frame Relay or ATM connections are used between office LANs at the WAN. The network should support TCP/IP or IPX/SPX (Internet Packet Exchange/Sequentical Packet Exchange), the former being the most popular transport medium.

To guarantee adequate voice and video quality, a prioritisation and reservation method is often used. These include 802.1p, RSVP and DiffServ, which will be covered later.

The capacity needed for a call depends on the media and the coding being used. On top of the codec bit rate, also the RTP, UDP, IP and Ethernet headers, as well as the RTCP control messages must be considered. For voice calls, the following principles apply:

- G.711 PCM coding is often used in LANs. If 20 ms of voice samples are sent in a packet, the RTP data field will be:

  $\frac{20ms}{125\mu s} * 1B =$ 160 bytes, being an even multiple of four bytes.

  When we add 12 bytes for the RTP header, 8 bytes for the UDP header, 20 bytes for the IP header and 18 bytes for the Ethernet (making 58 bytes altogether), and reserve 5 % for the RTCP, we must reserve, for both directions

  $\frac{160B + 58B}{20ms} * 8b / B * 1{,}05 =$ 91,6 kbit/s

  for a full duplex G.711 call without silence suppression. If silent periods are removed from the audio stream, about a half of this capacity will do.

- On WAN links, some compression is normally used. For example, G.723.1 ACELP uses 5,3 kbit/s coding and packs 30 ms on a single packet, so the RTP data field must be at least

  $\frac{5{,}3kbit / s * 30ms}{8b / B} =$ 20 B

  Considering the TCP/IP four byte words, no padding bits are needed.

  Silence suppression saves at least half of the bandwidth, when the listening party doesn't transmit on the network. On a Frame Relay network, the data link header and the flag make up four bytes.

If a single IP packet is transported on a FR frame, the total average capacity for a full duplex G.723.1 call on a Frame Relay link will be:

$$\frac{20B + 44B}{30ms} * 8b / B * 1{,}05 = 17{,}9kbit / s$$

For multiple simultaneous calls, statistics smoothens the silence suppression effects and we can use half of the above-mentioned figure, i.e. 8 kbit/s.

If an H.323 client is situated on a different sides of a firewall than other clients and servers, as in Figure 48, the H.323 and RTP protocols pose great difficulties to the firewall operation. The first fact is that calls originate from both directions. The second problem is based on the complex mix of protocols: RTP and RTCP, which carry the media streams and control the use of dynamic ports, the H.245 connection may be opened inside a Q.931 connection, and the media are specified by H.245. Both TCP and UDP transport is used, the latter bringing additional problems to the firewall rules. Dynamic ports require H.323 protocol decoding on the firewall, but the variable length ASN.1 encoding makes it difficult to find the interesting address and port information.

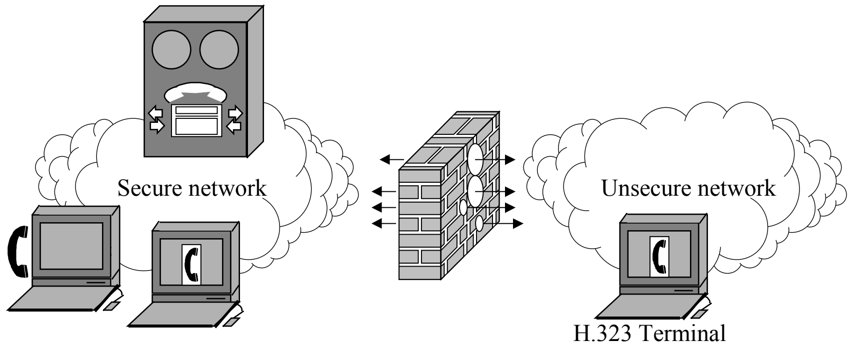


Figure 48: H.323 and firewalls.

A packet filtering firewall controls the packet flow by examining the IP, TCP and UDP headers. Dynamic UDP ports give no possibility to map incoming and outgoing UDP streams together. If a packet filtering firewall is used, all ports over 1 023 must be opened in both directions, a solution that will ruin most of the firewall protection. A circuit switching proxy firewall with H.323 support, may open a port for the response to the incoming connection request. An application proxy firewall implements part of the H.323 protocol stack, to be able to control both TCP and UDP connections. The firewall decodes the control information and makes the necessary address translations. An application proxy firewall is not transparent, but terminals must open the connection through the proxy, posing additional requirements for the terminal software.

Because IP Telephony and H.323 are becoming popular, firewall developers must add H.323 support to their products. At the moment, the support is often limited and may need the use of special client software.

5.2.7 Registration, Admission and Status (RAS) Signalling

H.323 terminals use H.225.0 RAS for signalling with the gatekeeper. If a gatekeeper exists on the network, the terminals must register themselves and ask for permission to make a call. The network may use RAS just between the terminals and the gatekeeper and pass other signalling messages between the terminals (Direct Endpoint Call Signalling). Another possibility is that all signalling messages travel through the gatekeeper, which has a full control over the connections (Gatekeeper Routed Call Signalling). The third alternative is to route the Q.931 signalling messages through the gatekeeper, but use the direct terminal-to-terminal path for the H.245 session control messages (Gatekeeper Routed Call with Direct H.245).

An example of a Direct Endpoint Call Signalling messaging is shown in Figure 49. When booted, the terminal tries to register itself with the gatekeeper. It may contact the known gatekeeper address (Static Discovery) or send a Gatekeeper Request (GRQ) to known GK multicast address 224.0.1.41 on port 1718 (Dynamic Discovery), and available gatekeepers reply with a Gatekeeper Confirmation (GCF). When the terminal selects one gatekeeper, it sends a Registration Request (RRQ) and indicates its address and name. The gatekeeper adds the data to its database and accepts the registration with a Registration Confirmation (RCF) message, or rejects the attempt with an RRJ. The registering may include a time limit, after which the terminal will be removed from the zone.

The terminal initiates an H.323 call with an Admission Request (ARQ) message to the gatekeeper, specifying the target and the requested maximum bandwidth. If the gatekeeper accepts the call, it sends an Admission Confirmation (ACF), specifying the admitted bandwidth, which can be lower than the requested. The ACF also specifies if the gatekeeper is included in future call setup and session control.

Now the originating terminal has permission to initiate the Q.931 call setup. After receiving a Setup, the called terminal asks permission to answer from the gatekeeper, with an ARQ, including the caller and bandwidth information. This permission is needed, because the parties may reside in different zones or only one terminal may use a gatekeeper. After the called user has answered the call, a Connect message is sent to the initiating terminal, a H.245 control channel is opened and H.245 session control messages are exchanged (*.

*) Additional TCP connection setup segments are needed for TCP based Q.931 and H.245.

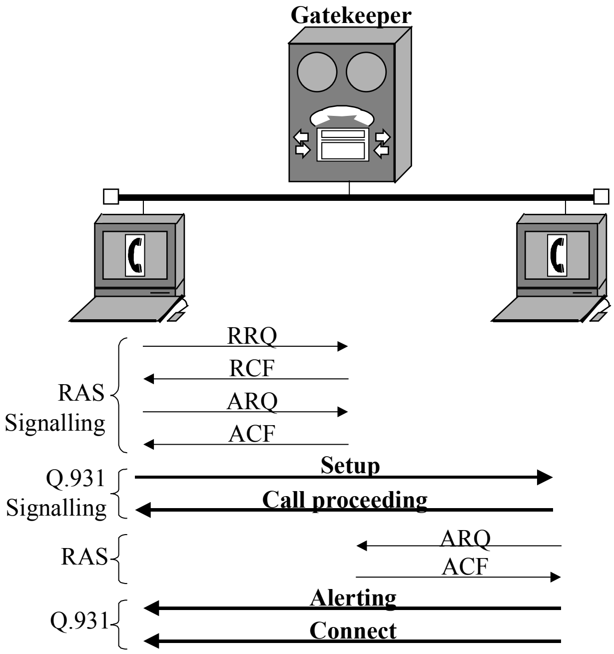


Figure 49: RAS Direct Endpoint Call signalling.

Additional RAS messages include Gatekeeper (GRJ) and Registration Reject (RRJ), Admission Reject (ARJ), Unregister Request and Confirmation (URQ, UCF), Bandwidth Request, Confirm and Reject (BRQ, BCF, BRJ), Location Request (LRQ) and Access Tokens, all having their specific function.

The called party is identified by the address, by the aliasname, by the H.323 URL or by using the directory information. An H.323 call is identified by multiple identifiers, namely the following:

- Call Reference Value (CRV), which identifies the H.225.0 messages. One CRV is used for RAS, another for call signalling.
- Call Id, which associates all messages within a call.

Additionally, conference calls are identified by a Conference Id, (CID), which associates all messages between all entities within a conference.

When Gatekeeper Routed Signalling is used, both the H.225.0 call and RAS signals, and the Q.931 call setup messages travel from terminals to the gatekeeper only (Figure 50). The terminal register itself with an RRQ, and the gatekeeper replies with an RCF. Then the originating terminal requests the permission for a call with an ARQ. After a positive ACF reply, it sends the Q.931 Setup to the gatekeeper, which resends it to the original destination. As shown in Figure 49, all Q.931 signalling takes place between a terminal and the gateway. The H.245 session control messages can be directed through the gateway or directly between the terminals. GRS gives greater control to the gatekeeper over the connections. /IEC/

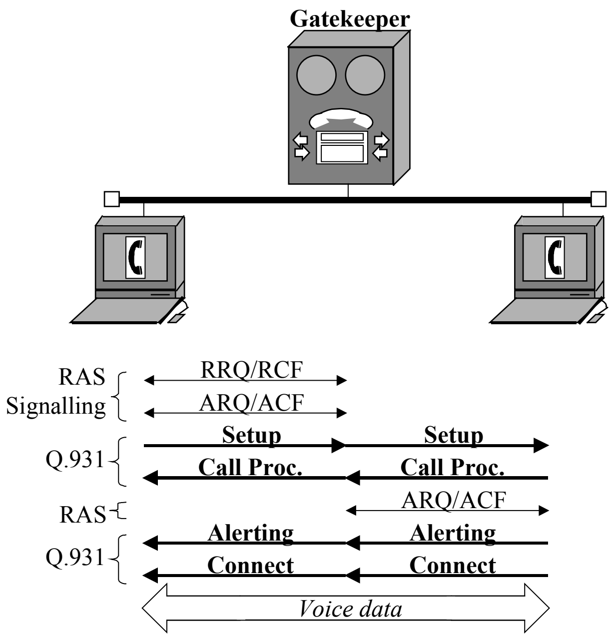


Figure 50: Gatekeeper Routed Signalling.

5.2.8 H.323 Location Services

H.323 terminals are identified by their IP addresses, but the users want to place calls by the target name, nickname, H.323 URL or by picking the receiver from the directory "phonebook". The gatekeeper handles address resolution between the friendly usernames and the terminal IP addresses. The resolution can use the following methods:

- Terminals register themselves with the gatekeeper, and the gatekeeper keeps a local database between the aliasnames and terminal addresses. We should, however, keep in mind, that H.323 aliasnames identify the terminal.

- H.323 URLs and usernames can be stored in a DNS server. The gatekeeper can request the target IP address from the DNS server.

- The H.323 usernames can be stored on a directory server, and the gatekeeper makes the request using LDAP. An LDAP server can provide private address lists, phonebooks and data search services, based on the central user directory.

- If the target information is not found from the local database, the gatekeeper can make a Location Request to the gatekeeper of another zone. The target gatekeeper may consult a DNS or LDAP server to find the requested data.

- The gatekeeper may send the request to a local Border Element, which may contact another BE in a foreign zone. The border elements may keep a local copy of the most often used targets, and also exchange address information without a call request.

- An H.323 service can be located using Telephony Routing Information Protocol (TRIP).

The H.323 version 4 states two alternative principles to handle user, terminal and service mobility. The annex H is based on Home and Visitor Location Functions (HLF, VLF), following the GSM principles. The development of this standard is moving slowly, and there are doubts on whether it will be finalised in time. The annex E allows H.323 terminals to access the VoIP network through an ISP and identify themselves as mobile phones. The PC application registers with the Mobile Swithing Center (MSC) with a help of a User Identity Module, for example a SIM card for the GSM network. After registration, the SIM HLR is notified, and calls will be directed through the H.323 network. Of course, a gateway is needed between the packet switched IP network and the circuit switched mobile network.

5.3 SIP System

5.3.1 Practical SIP Components

According to the IETF RFC 2543, a SIP system consists of Clients and Servers, which are using the **SIP protocol for multimedia call establishment, maintenance and clearing**. The client component always sends Requests, and the server sends Responses. Practical SIP systems consist of User Agents and Servers, which can be categorised in the following way:

- A SIP **User Agent** (terminal) contains the hardware and software components to make and receive IP telephone, video and data conferencing calls. When the User Agent initiates a call, it uses the Client component, and the Server component of the destination UA answers the call.

- A **Proxy Server** acts as a contact point, providing reachability services. A proxy may know a new contact address, and it relays the call signalling messages to the next proxy, redirect or UA. A proxy has both the Server and the Client components. A Proxy Server acts as a SIP message router. It keeps the state information during a SIP transaction (*, but is not aware of any existing calls. A Proxy may fork the request: several potential destinations may be tried at the same time.

- If a **Redirect Server** knows a new destination to the callee, it redirects the caller to this destination with a 3XX response (for example 301 Moved Permanently). Redirection is useful, if a subscriber changes the provider. A Redirect Server cannot fork the request.

- A **SIP Registrar** handles user location information. Users register their whereabouts with the Registrar, and the Registrar answers UA requests based on this information.

- The location information is kept on a **Location Server**, which performs the same functions as a Home Location Register on a GSM network.

SIP signalling offers the following functions:

- User location, including the mapping between callee identification and destination location information (IP telephone address, PSTN, ISDN or mobile telephone number, E-mail address or other reachability information), and reachability, including the possibility for a SIP user to register to be occupied, so she will not receive calls.

- Feature negotiation for one-to-one calls or conference calls. In multiparty conferences, the media mix of participants may be different.

- Call setup for two-party and multiparty calls

- Call participant management: an active call participant may invite new users or terminate an existing association.

- Call feature changes, making it possible to alter a terminal or media session features during an active call. For example, a call may be initiated as a bidirectional voice connection, but the parties agree to use also video. The media composition may also be altered because of the participants leaving.

*) A SIP server doesn't have to maintain state information even during the transaction time. If a stateless Proxy or Redirect Server receives a request, it generates a response and forgets the incident, and the messages contain all necessary information for processing and routing. The stateless server operation makes the system scalable.

SIP only handles call signalling. The SIP protocol carries SDP messages, which handle session parameters, like multimedia coding and bandwidth details. The media streams are carried using RTP and controlled by RTCP, both using connectionless UDP transport. This makes it possible to separate transport and application services: a customer may use NSP A for IP transport, company B for SIP signalling, telephone operator C for call termination, and least cost PSTN termination routing service from service provider D.

Other supporting protocols possibly needed in a SIP telephony system include DNS name resolution, LDAP directory, Telephony Routing over IP (TRIP) for gateway discovery, RSVP and DiffServ for Quality of Service on the IP network and Diameter for Authentication, Accounting and Authorization (AAA). SIP carries MIME content (Multipurpose Internet Mail Extension), making it possible to return a Web page as the result of a call invitation. /Sisalem/ /Schulzrinne/ /Fingal/

5.3.2 SIP Services

Basically, SIP provides **presence and location services**. As shown in Figure 51, a user registers her whereabout on her home SIP Registrar. The REGISTER request contains the contact IP address and expiration time. The Registrar saves the username and the contact address on a Location Server. Now the registrar can reply with correct contact information (provided, that the location data is valid).

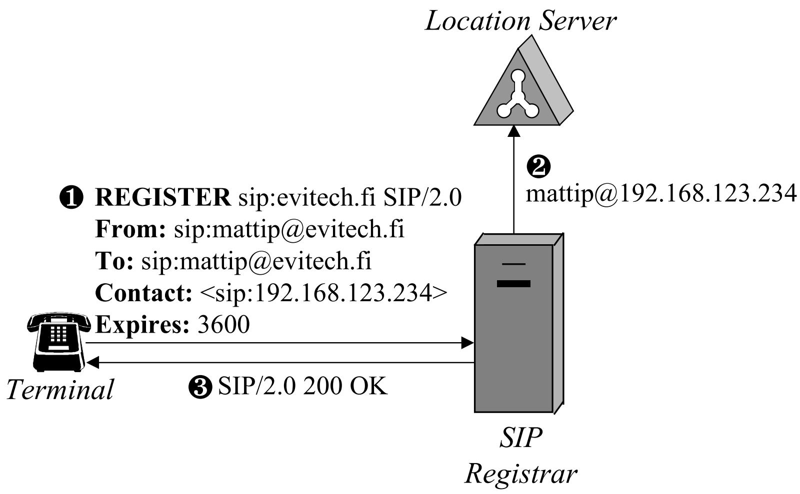


Figure 51: User registration.

Personal mobility provides the user with possibility to use different User Agents and addresses to receive calls to a single SIP URL. A REGISTER request binds a person to a device, and Proxy and Redirect Servers route an INVITE request to the right address and location.

In the example of Figure 52, user elpuska has the primary contact at sip.espoo.fi, but while working at the utu.fi she is reachable both from elpuska@lab.utu.fi and elpuska@office.utu.fi. A call can reach her from a foreign domain, even though she has made a faulty registration. The procedure used is the following:

1: When she travels to utu, she registers her lab address as a forwarding. A REGISTER request is sent to her home SIP server.

2: While in utu, she also registers her office address as a forwarder. Both addresses are added at the sip.utu.fi Location Server.

3: Last time, when she left utu, she set up her lab computer to forward all incoming call attempts to sip.espoo.fi. Now she doesn't remember this, but restarts her user agent, with this configuration.

4: When mattip@evitech.fi makes a call to her, the caller's user agent resolves the destination address and sends an INVITE message from the caller terminal to the callee SIP server.

5: The sip.espoo.fi receives the call request and tries to locate the user. The database contains registrations to utu.fi, so the INVITE is forwarded to elpuska@utu.fi after DNS name resolution.

6: The sip.utu.fi server receives the request and checks the location database.

7: The utu.fi Location Server finds two possible contact points.

8-9: The INVITE request is forked by the sip.espoo.fi server both to the lab and the office workstations simultaneously.

10: Let's first look at the lab phone. When receiving an INVITE, the user agent forwards the call to the sip.espoo.fi, according to the local (but now an outdated) configuration.

11. sip.espoo.fi rereceives the request, detects a loop and returns an error message 482 (Loop detected) to the sending host, lab.utu.fi.

12. The lab host tries its best to serve the incoming call request, and sends an error message to the host it received the request from.

13: At the same time, her office phone has been ringing. If there, she picks up the call, causing an OK message to be sent from the user agent to the local server, who sent the INVITE.

14: The SIP server of the utu.fi receives both the error and the call accept messages and forwards the positive reply back to the originating sip.espoo.fi proxy.

15: This forwards the reply to the original caller, who now knows the final destination. The servers can now discard any information about the call.

16: After this, the caller host uses the direct connection to the destination host for future SIP and SDP signalling. After the call establishment, the voice packets also take the direct route. When the call is terminated, the BYE request is exchanged directly between the parties.

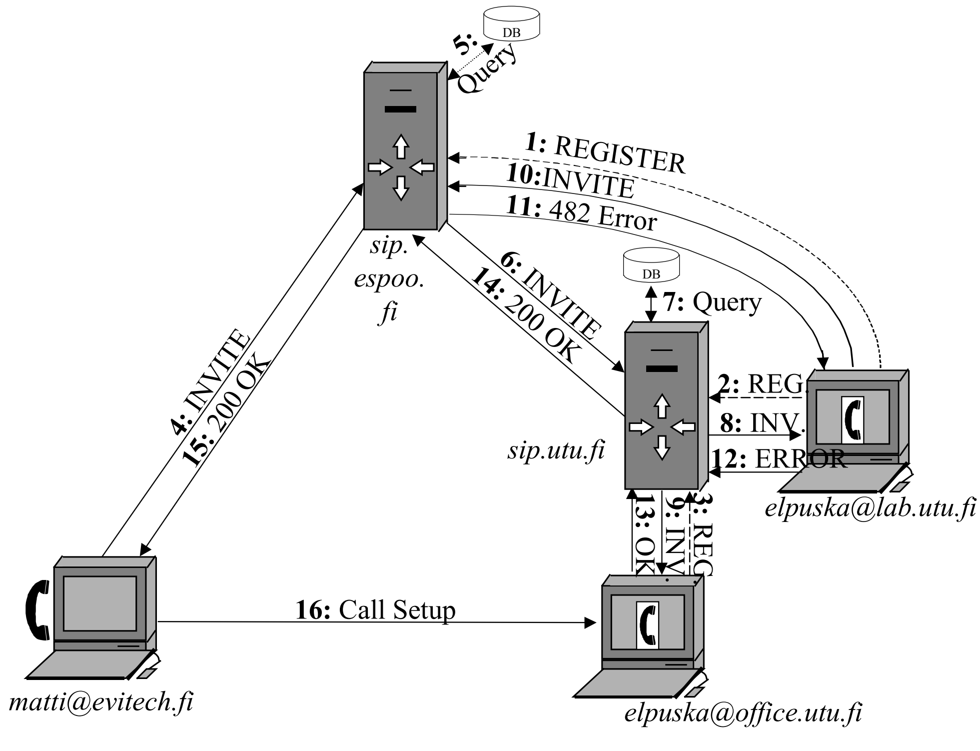


Figure 52: Personal mobility example.

Terminal mobility allows terminals (User Agents) to move between IP subnets, a service, like the one offered by the GSM and other mobile networks for network-specific mobile terminals. SIP mobility is based on Mobile IP. Mobile hosts inform their home proxy about their new location and session mobility is handled with reINVITE messages. Mobile IP allows hosts to be reached under the same address, regardless of their location. A mobile host registers a care-of-address with the home agent, and correspondent nodes send data to the home agent, which tunnels traffic to the final care-of-address.

Third generation mobile networks use SIP to establish and terminate IP telephony calls. The 3GPP consortium (Third Generation Partership Project) is working on detailed specifications to ensure interoperability.

Service mobility provides the possibility to use same services from different locations and devices. Services may include personal settings, address books and media preferences. The services may be located at the home server of the user, and calls are forced to travel through this server, or a service, located at an end system, is retrieved with the REGISTER message.

A SIP system also offers versatile **call transfer services**, like blind transfer unconditionally, operator assisted call transfer (while an operator makes sure, that the new callee is available), delayed call transfer (to the secretary if I don't answer in 20 seconds) and auto-dialer, to mention a few.

The open architecture of SIP makes it possible to build various additional services, which can be outsourced and commercialized. An example is **call screening** by a SIP Proxy Server (see Figure 53), a service that might be found useful by suspicous parents. Instead of trying to keep a local black list up-to-date, the SIP home telephone user can subscribe to a commercial filtering service filterlists.com and specify the banned destination categories. When a child is trying to make a call, the INVITE request will be forwarded to the Proxy, which performs a database lookup and makes a judgement whether to accept the call or not. For an unambigous target, the server returns a reject message with an explanation text. For targets that are not banned, the Proxy Server will redirect the call towards the destination.

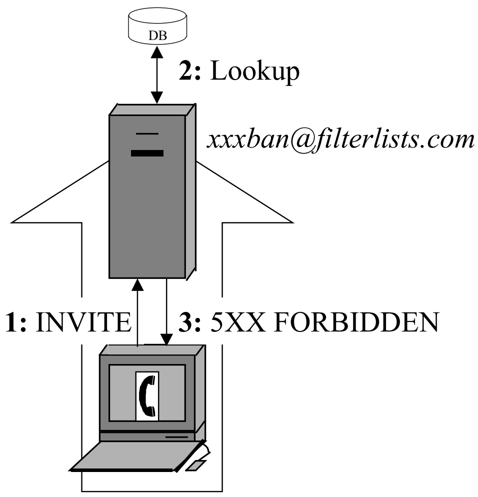


Figure 53: Call screening by a SIP Proxy.

5.3.3 Directory Services and SIP

SIP Systems use DNS for name resolution and LDAP and other directory services for subscriber identification. DNS maps a globally unique hierarchical DNS name to one or more hostnames or IP addresses. DNS lookups are based on a single key, and do not provide a possibility to combine several parameters. DNS is suitable for finding a server responsible for an organisation or for resolving the IP address of a given unique hostname.

For looking up individual subscribers, a more versatile service must be used. LDAP offers the possibility to search for a record, based on a combination of different parameters. An LDAP server can find the SIP URL for all users in the greater Helsinki Area with the first name of Matti, working for Evitech, giving courses on data communication and having a technical education. LDAP can also match Matti Puska, Matti H. Puska and Puska, Matti as a single record.

SIP can also provide a simple programmable directory service, based on the Location Server. The SIP directory may return different responses based on caller identity, required media, time of the day, distribution of current calls, order intake history data or other criterias. With this service, it is possible to create intelligent hunt groups. For example, while integrating an IP PBX with an operative bookkeeping system, incoming calls to a call center can be weighted to the service person who received most orders last week. /Schulzrinne2/

5.3.4 SIP and Firewalls

Configuring a firewall to pass SIP messages safely is easier than with the H.323. By default, SIP uses a well known TCP port of 5060 and UDP transport, but media streams are transported over RTP with dynamic high order ports. The RTP port is agreed on in the SIP messages, and the next odd port is used for RTCP.

A SIP enabled firewall must analyse SIP messages to determine the RTP port number and change the filter rules to open a port pair for a permitted IP telephony connection. SIP messages are coded with clear text, so they are easier to encode than ASN.1 coded H.323 messages. For this, an application level gateway is needed.

Network Address Translation poses additional problems to the firewall. All internal IP addresses are translated into one or more public addresses by NAT firewall, which totally hides internal addresses. But replacing the addresses in the IP header is not enough, because SIP and SDP messages include the host addresses, which should also be translated. If the NAT firewall cannot find free consecutive ports, it must signal the host about the situation with a 486 - Busy Here reply. For security, the hole must be closed right after the session is terminated, i.e. when the firewall discovers a BYE message.

Besides special SIP enabled application layer firewalls, Real Specific IP (RSIP) can also be used to control SIP based IP telephony passing between protected areas. As shown in Figure 55, internal clients request the public resource (address and address-port pair) from an RSIP server, running on the firewall. The internal client will then use this address and port for tunneling the IP telephony connection through the firewall. Datagrams with public IP addresses are then encapsulated into another UDP datagrams and IP headers with internal IP addresses and sent by the internal client to the RSIP Server, which checks the acceptability and removes the outer IP and UDP headers. Return messages from the outside realm will be encapsulated by the RSIP server. This solution lacks the possiblity to initiate RTP sessions from the outside. /Thernelius/

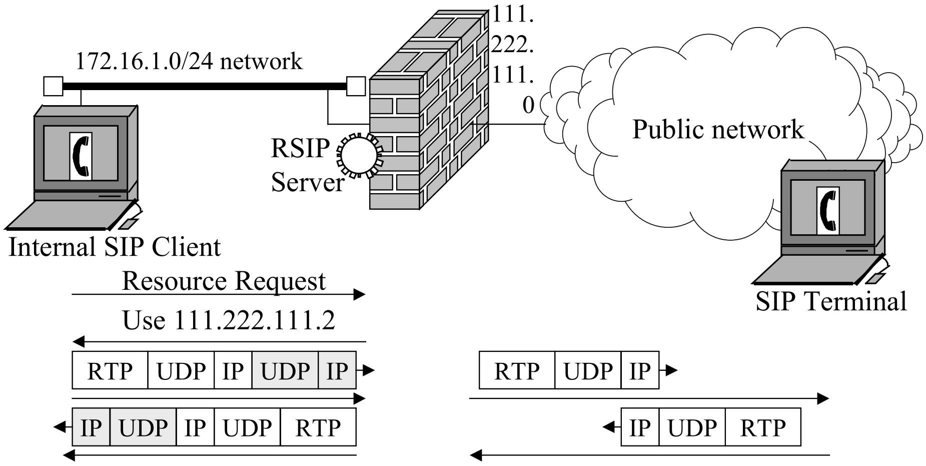


Figure 55: Real Specific IP.

5.4 IP Telephony Service Providers

5.4.1 Public Telecommunication Operators and PSTN Pricing

Telecommunication services are regulated in most countries. Until the 80's or 90's, telecommunication services could only be offered by a licenced company, and often a single (government owned) company held the only license: Deutsche Telekom in Germany, France Telecom in France and so on. In Finland, the government PTT (then renamed Tele, then Sonera, now Telia Sonera) held the license to serve most of Finland, while bigger towns were served by local telephone companies, often co-operative: Helsinki Telephone Company (nowadays Elisa Communications), Tampere Telephone Company (nowadays Soon Communications) and Oulu Telephone etc. To offer national services, the private co-operative telephone companies formed the Finnet union. In USA and Canada, AT&T was divided by a court order into Regional Bell Operating Companies (RBOCs), and each company could serve only their local area. Long distance calls were offered by Inter Exchange Carriers (IECs), but the RBOCs had to keep away from the inter LATA (Local Access Transport Area) services.

Heavy regulation and local monopolies lead to high prices, inefficient operation and slow development. In the mid 90's, deregulation opened the telecommunication markets. The Open Network Provision was seen by the EU as a means to promote European competitiveness over Northern America and East Asia. It stated that after a certain transition period, (almost) all telecommunication services will be opened for competition and the traditional (incumbetent) Public Telecommunication Operators (PTOs) must lease their access and transmission capacity to new teleoperators. The new US Telecommunications Act in 1996 made it possible for new companies (like Cable Television companies) to offer telephone services but keeps the RBOCs away from the inter LATA services, until they open their regional monopolies. In Canada, public long distance voice services were opened for competition in 1992, local calls in 1997 and international calls in 1998. To make sure that the rural areas in Canada (* would also be served, the service providers were ordered to pay a contribution of their international traffic, and the money will be used for incumbent local carriers.

Prices for public voice services are dependent on distance, and often based on operator, telecommunications and country areas. An example of the non-discounted price of a three minute call from Espoo is presented in Figure 56. The price structure is as follows:

- A call to Helsinki is a local call, and the subscriber is charged for the Elisa service with the local call tariff of 12 cents for a call plus 1 or 1,7 cents/minute, including v.a.t, in June 2004 (**.

- A call to Tampere is a long distance call, including the local access rate to Elisa and the long distance tariff. Long distance services are offered by multiple operators, and the subscriber can choose his/her favorite provider with a prefix number, or with an agreement.

- Calls to Copenhagen, Hannover and Cape Town are international, and the charge includes the local access rate to Elisa and an international tariff, according to the price list of the selected international carrier. The latter is again selected with a prefix.

*) The land area of Canada is 9,971 million km^2, while the population is only 30,5 million. This makes the population density of only 3,1 inhabitants/km^2. This should be compared with the population density of Finlad (16,7 inhabitants/km^2) or Germany (230 inhabitants/km^2).

**) During the summer 2002 Elisa Communications removed all discounts for calls during evenings and weekends.

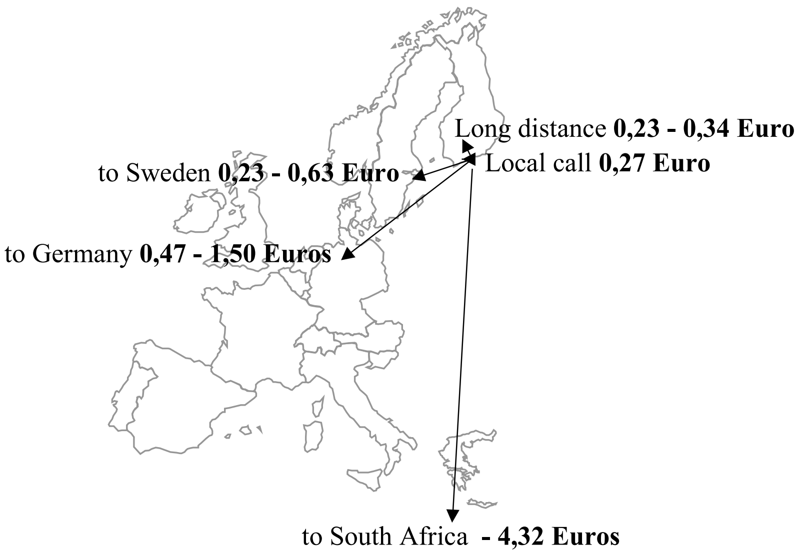


Figure 56: Examples of a three minute local, long distance and international call prices from Espoo Finland according to 22.6.2004 tariffs.

The pricing structure reflects the operator costs. Making a call consumes switching capacity and a time slot is needed for call routing. The subsriber line and local access switches are built and maintained by the local carrier, which also charges the customer. For long distance and international calls and calls to mobile terminals, contributions of the egress PTOs are also needed. The international settlement system governs the co-operation of international carriers. The originating PTO (which gets the subsriber payment) makes a compensatory payment to the terminating PTO for its efforts (see Figure 57). The settlement payment tariffs are based on bilateral agreements between the PTOs and on the agreed accounting rates. The transit traffic statistics are periodically examined and the net settlement fee is paid, often being equal to half of the accounting rate multiplied by the minute difference. Nowadays, the traffic is often unbalanced (*, forcing the settlement rates downwards. The settlement costs still make up some 20 % of the international tariffs.

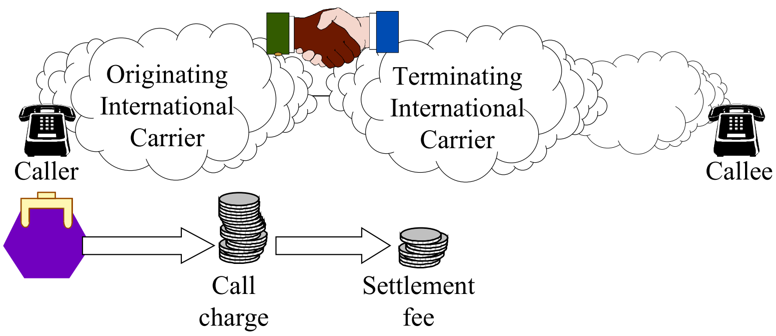


Figure 57: The international settlement system.

*) Calls are more often originated from the financial capitals and terminated in developing countries, making the accounting rates a sosioeconomical issue as well.

In Finland, the local access rate is distinguished from the mobile, long distance and international tariffs. While the subscriber gets a single phone bill from the local PTO, this is transferring the fees for the long distance and international calls made using a foreing operator, to the relevant PTOs. In many countries, local calls are free (i.e.bundled with the basic fee), so the PTO's must make an agreement of how to divide the charge. /ITU/ /FCC/

5.4.2 Public IP Telephony Services

Public Telephone Operators' attitude to IP Telephony is at least two-sided: On one hand the PTO can achieve substantial investment and capacity savings with the standards based IP backbones and new revenue with the intelligent add-on services, made possible by the IP protocol. On the other hand new low priced IP services will threaten the existing price structure, based on the monopolistic or oligopolistic market position of a traditional PTO. The view is often dependent on the history and market position of the PTO: the market leader sees the new technology as a threat to its revenue streams, and the market entrant sees the IP telephony as a means to penetrate the market with minimum costs and with maximum service offerings.

IP telephony can be used by the PTO's at least by the following ways:

- The existing circuit switched network infrastructure of telephone exchanges and SDH transmission systems can be gradually replaced with IP routers and all-optical networks. The cost savings are dependent on cheaper equipment (standards based routers versus vendor specific exchanges), more effective use of transmission capacity (packet switching versus circuit switching) and savings on international connectivity (bypassing the settlement system). The cost savings may be used to respond to the price corruption by new market entrants. If the price flexibility is high, a small price reduction can generate much new traffic.

  As shown in Figure 58, IP is only used at the center of the telephone network. Subscribers make calls as before, but voice data is routed from the digital telephone exchanges to the IP backbone. To ensure voice quality, conservative compression and Frame Relay or ATM links are often used. Most exchange manufacturers offer IP or ATM interfaces, so no additional gateways are necessary.

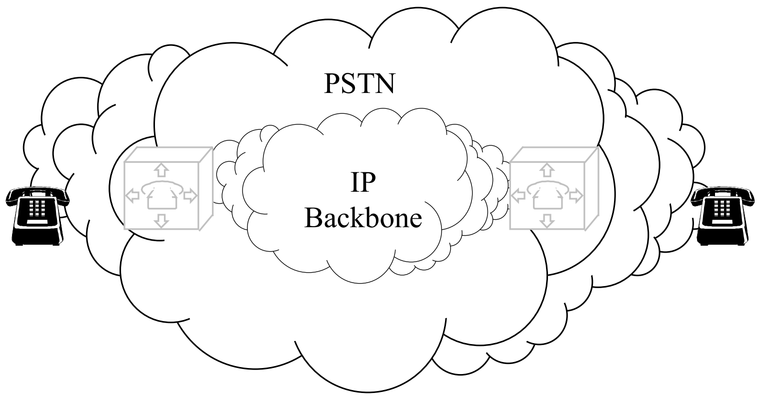


Figure 58: Using IP as the backbone of the PSTN.

- New IPTSPs mainly use the IP telephony system to route and transport voice calls (Figure 59). With calling card services, the subscriber buys a prepaid phone card (actually an identification number printed on a plastic card), makes a call to the announced local telephone number and gives the id number and called phone number details, often with DTMF keystokes and voice assisted instructions. The gateway of the IPTSP then makes the call and routes it through its IP network to the gateway nearest to the receiver. The egress gateway then routes the call to the local access network. The IPTSP doesn't need an invoicing system, and normally doesn't pay international settlement fees. Because a gateway is needed at the receiving end, the service provider needs a partner or presence in each receiving country. This normally puts limits to the service offerings, because some countries ban IP telephony or put heavy technical, financial and bureaucratic limitations to PTO operations.

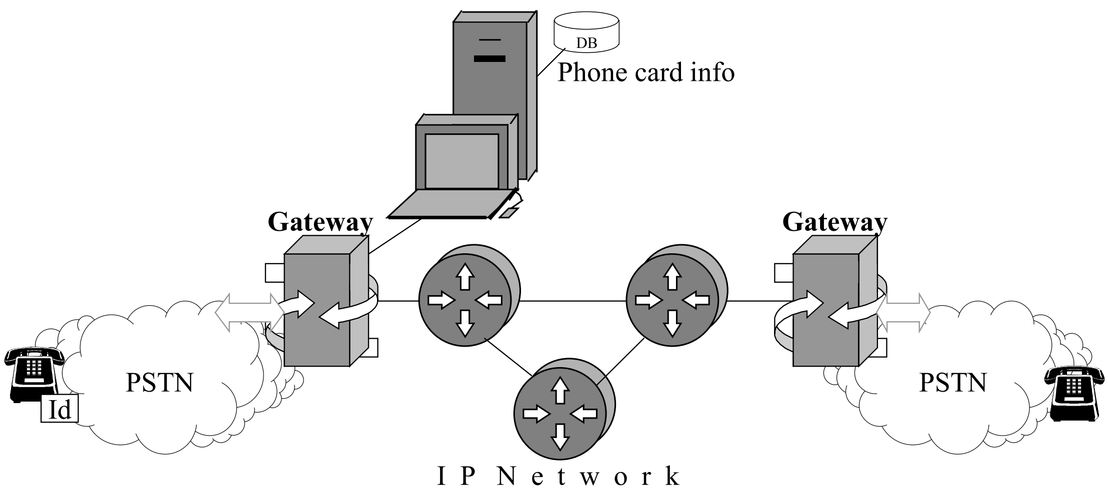


Figure 59: IP Telephone Service Provider.

If IP telephony is allowed and the IPTSP has local provider status and access to the national billing system, the service provider may publish a prefix number for long distance and international voice services. Now the subsriber dials the callee number with the prefix normally, and the call is routed through the local gateway to the IP network. For example, Song Networks uses 99577 prefix for international IP telephone calls from Finland. These tariffs are significantly lower than competiting circuit swithed services: the price of an IP call is 46 - 50 % lower than the circuit switched service offering by the same company for most Central European countries.

- An IPTSP may use the cheap IP telephony service offerings as a bait to get new customers, or to promote new value-added call routing and messaging services at attractive prices.

- An ISP or an independent service provider may use the broadband Internet access to bypass the local carrier. Telia Sonera, Elisa and Ipon Communications offer IP based voice services for private users and companies in Finland.

The regulatory situation of IP telephony varies from country to country. The attitude can roughly be categorized into three groups, which are:

- Countries, that include IP telephony within their standard regulatory system, or do not have special regulations on IP telephony. Countries like Estonia, New Zealand and the United States have no specific prohibitation for VoIP, in fact the US exempts IP telephony from the international settlements system. EU countries, Hungary and Iceland do not consider VoIP services as voice telephony. Some countries, like Japan and Singapore, permit these services, but put light conditions to services considered real time. Austalia, Canada and China, on the other hand, also permit VoIP services, but treat real-time voice services the same way as ordinary telephone services and including them in the settlement system.

- Countries, that treat voice and fax services differently depending on whether the public Internet or a private IP network is used. Most countries in this category are developing countries or former Soviet Union nations, now independent, allowing the use of private IP networks but prohibiting the use of the Internet. Kyrgyzstan, Moldova and Sri Lanka make exceptions, allowing the use of the public Internet, but prohibiting private IP networks!

- Countries that prohibit VoIP services both on the public Internet and the private IP networks. Most of these countries are developing countries that regard the international settlement system as an important source of cash flow and VoIP as a threat to this income. Countries in this group include for example Albania, Cuba, Eritrea, India, Nigeria, Pakistan and Romania, but also Israel and Turkey.

According to the ITU estimate, the VoIP portion of international calls was 3 % at the end of 1999, but the market share for IP telephony calls is significantly smaller in domestic calls. Different estimates show 150 - 220 % annual growth for IP telephony services, a growth that is easy to achieve, when the starting level is low. The global voice and telefax market was estimated to exceed 520 billion USD (over 150 times the Finnish national budget) in 1998, while IP services, including data, Internet access, VPN and VoIP, reached "only" 55 billion USD. In Finland, mobile telephone penetration is larger than that of the PSTN, so the main interest is in mobile voice and data services. /ITU/ /Teleware/

5.4.3 Megaco/H.248

Megaco (Media Gateway Control) / H.248 is a joint IETF /ITU-T standard for Gateway control. As shown in Figure 60, it specifies a **simple protocol between the Media Gateway**, which converts circuit switched voice samples into packet based RTP messages, **and the Media Gateway Controller**, which makes the necessary signalling conversion. It provides a low level control for the MG to connect incoming streams from one type of network to another. In packet switched networks, RTP is used to carry the data streams and H.323 or SIP is used for signalling. In circuit switched networks, the voice and video samples are carried in PCM or SDH timeslots, and SS#7, ISUP or an equivalent system is used for signalling. Megaco also supports distribution of call control and media streams.

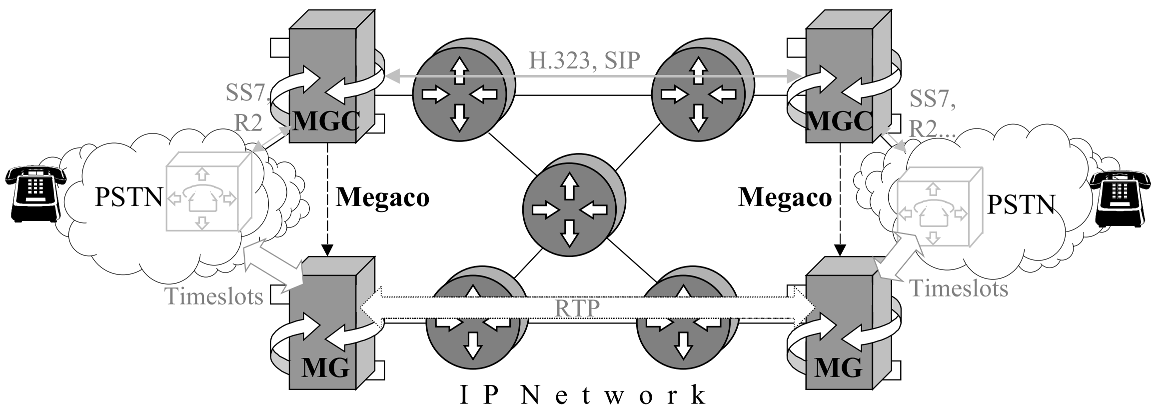


Figure 60: A Megaco/H.248 system.

Megaco defines terminations, contexts and messages. A **termination** represents a stream, which is entering or leaving the Media Gateway, for example an ISDN voice channel or an RTP stream. The termination has properties like dejitter buffer size, which are inspected and modified by the Media Gateway Control. Some terminations are set up automatically, others are created when needed and released after use. The latter type represent a flow of RTP packets. The MG gives a TerminationID to the termination.

One or more terminations are mixed and connected together as a **context** (see Figure 61). A simple bidirectional voice call has a physical termination to the PSTN and one ephemeral for the RTP stream on the packet switched network, like the lowest context on the figure below. A context of three or more terminations is needed for a conference call. Contexts are created and released by the MG, under the command of the MGC, and they are identified by ContextIDs.

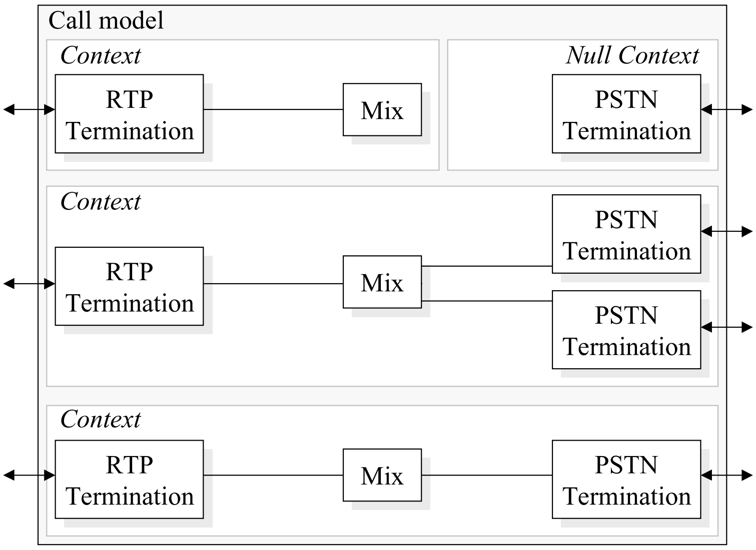


Figure 61: Terminations and Contexts in the Megaco call model.

The Media Gateway can also generate tones, announcements, ringing and other signals a user can hear. Megaco includes means to apply and control signals to terminations, so the user will get normal call progress indications, like the ringing tone. The MG can also detect asynchronous events, such as off hook on a phone or DTMF key, and report them to the Media Gateway Controller for signalling procedures.

Megaco uses the following **commands** for terminal, context, event and signal manipulations:

- An Add command creates a new context or adds a new termination to an existing one.
- A Subscract command removes a termination from an existing context. If no termination remains after the subscract, the context will be released.
- A Move command moves the termination from one context to another.
- Modify changes the termination state.
- AuditValue returns information about the termination, context and MG capabilities, as does the
- AuditCapabilities command.
- ServiceChange creates a control association between the MG and the MGC.
- The MG uses the Notify command to inform the MGC about an event that the controller is interested in.

A **package** is a predefined set of properties, events, signals and statistics, which are implemented on a set of terminations. The base set of packages include analogue and digital loops, DTMF messaging and RTP. Besides the standard packages, any organisation (like an equipment vendor) may define their own package. /NetworkMagazine/ /RFC 3015/ /SAMK/

5.5 Review

An IP PBX uses general purpose hadware, operating system, network connection, APIs and standard TCP/IP protocols, and handles messages for call setup and teardown, while voice data travels directly between terminals. An H.323 system consists of H.323 terminals and optional gatekeeper, gateway, MCU and Border Element servers. H.323 terminals may be hardware or software based or lightweight Simple Endpoint Type user terminals. A gatekeeper transforms H.323 aliasnames into IP addresses and controls the RTP bandwidth and terminal access, if implemented. An MCU is needed for conference calls and a gateway offers interfaces for non H.323 systems, like the PSTN. When dimensioning an H.323 network, we must add the effect of layer 2, IP, UDP and RTP headers into the codec bit rate. Because H.323 uses variable port numbers and ASN.1 coding, a firewall between H.323 system components poses additional challenges.

An IETF SIP system consists of User Agents, Proxy and Redirect Servers, SIP Registrars and Location Servers. The servers offer presence and location services, personal, terminal and service mobility, call transfer services and an easy way to implement additional services. Often DNS is used to resolve names to IP addresses, while an LDAP directory offers versatile search possibilities. Technically SIP support on a firewall is simpler than for H.323 because of the well known SIP port and the textual encoding of SIP messages, but manufacturer interest is dependent on the commercial pressure.

Traditional Public Telephone Operators could take advantage of IP telephony by replacing their circuit switched network infrastructure gradually with IP routers, but their attitude is varying. New PTOs can directly implement the IP telephony system and innovatiove services, and use the public PSTN as access networks. The market and regulatory situation varies from country to country, and so does the offering of IP based services. It seems that the new technology is first adopted in international calls.

A gateway is needed between the circuit switched telephone network and the IP network. Megaco/H.248 standard defines a simple protocol between a Media Gateway and Media Gateway Controller, both logical components of a gateway. Megaco defines terminations, contexts and messages and offers a standard way to integrate the signalling conversion component with the media conversion component.

5.6 Quiz

- Are the signalling messages travelling through an IP PBX?
- Are voice packets travelling through an IP PBX?
- List all H.323 system components
- What are the functions of an H.323 Gatekeeper?
- When and why an MCU (Multistation Control Unit) is needed in an H.323 system?
- When and why an H.323 Gateway is needed?
- Why voice compression is often used on WAN links?
- What additional services does a directory server offer on an H.323 system?
- List all SIP system components
- Why a Proxy Server is (often) needed on a SIP system?
- List examples of various SIP services
- Why the SIP protocols are technically easier to handle for a firewall than H.323?
- List some of the major changes in telephone service provider's business environment during the last 15 years.
- How much does a five minute call from Espoo to Rovaniemi cost? Which operators benefit from this sum?
- Which operators benefit from the phone call fee for a call from Espoo to Paris?
- Which are the technical methods for a telephone service provider to take advantage of IP telephony?
- What is the estimated percentage of IP telephony from international calls?
- Where does Megaco/H.248 protocol take place?

5.7 Material

/RFC 2543/ M. Haldley, H. Schulzrinne et. al: SIP: Session Initiation Protocol. RFC 2543. IETF 1999

/Cisco/ Cisco Systems Web pages. Internet, <URL: http://www.cisco.com>

/Sisalem/ Dorgham Sisalem, Jiri Kuthan: Understanding SIP. Iptel.org. Internet, <URL: http://www.iptel.org/>

/Shulzrinne/ Henning G. Schulzrinne, Jonathan D. Rosenberg: The Session Initiation Protocol: Providing Advanced Telephony Services Across the Internet. Bell Labs Technical Journal. October-December 1998.

/Fingal/ Fredrik Fingal, Patrick Gustavssson: A SIP of IP-telephony. Master's Thesis, Lund Institute of Technology, Lund University. Lund University, 1999.

/Schulzrinne2/ Henning Shulzrinne, Jonathan Rosenberg: Signaling for Internet Telephony. Columbia University, Dept. of Computer Schence Technical Report CUCS-005-98. Columbia University, 1998.

/Thernelius/ Fredrik Thernelius: SIP, NAT, and Firewalls. Master's Thesis, Kungliga Tekniska Högskolan. 2000.

/ITU/ Report of the Secretaty-General on IP Telephony. World Telecommunication Policy Forum (WTPC 2001), Geneva, 2001. ITU, 2001.

/FCC/ Federal Communications Commission: Telecommunications Act of 1996. FCC, 2000. Internet, <URL: http://www.fcc.gov/telecom.html/

/NetworkMagazine/ Doug Allen: Megaco and MGCP. Network Magazine, 5.10.2000. Internet, <URL: http://www.networkmagazine.com/article/NMG20001004S0013>

/RFC 3015/ F. Cuervo et. al: Megaco Protocol Version 1.0. RFC 3015. IETF, 2000.

/RFC 2805/ N. Greene, M. Ramalho, B. Rosen: Media Gateway Control Protocol Architecture and Requirements. RFC 2805. IETF, 2000.

/Teleware/ IP-puhe. Teleware Oy, course handouts.

/SAMK/ Jani Peltola: Media Gateway Control. Satakunta Polytechnic, course handouts. Satakunta Polytechnic, 2001

6 Computer Telephone Integration

6.1 The Concept

EDP systems include hardware and software components, which are used for data processing to provide business operations supporting services. EDP systems include databases of information, which is essential or important to the business: stock inventory, customer information, service contracts and price lists to mention a few. A telephone system makes it possible to make and receive calls outside and within the company. At the minimum, a PBX includes a table, that maps terminal connections and subscriber numbers together. A modern PBX often includes subscriber identifier text, personal reachability information and other personal settings.

Computer Telephone Integration includes a physical and logical connection between the EDP computers and the PBX, which offers call management services. The CTI system enhances call handling by combining the data from an EDP database with the telephony data, like caller id, or provides additional information on the callee, based on the combination of telephone data and EDP data storages.

A properly implemented CTI system may improve the efficiency, effectiveness and profit of an organisation that does business over the phone. Typical CTI applications include but are not limited to the following:

- Customer service Call Centers, where the PBX sends the caller id to a database server, and receives customer details, which can be used for call routing or displayed.

- Similarly, outbound calls can be directed by the customer database, and telephone sales agents automatically call preselected numbers. Call success statistics can be fed back to the database to build reachability information and customer profiles.

- Interactive Voice Response systems are used instead of switchboard operators or for automatic service or order intake. The caller is given a synthesized voice response, and he can make selections or enter numeric data with the DTMF keypad. The IVR system can amend personal service during the night or peak times.

- Unified Messaging can improve employer reachability. If an incoming call is not answered, it will be directed to a messaging server, which plays back a personal greeting, asking to leave a message. The caller message is recorded and the callee can retrieve it from her telephone, mobile phone or from her workstation.

The CTI technology integrates different messaging systems and media to a single solution, making it possible to retrieve E-mail messages over the phone or listen to voice messages as E-mail attachments.

An example of a CTI application is a helpdesk receiving customer calls and solving customer problems. When a customer makes a call, the caller id, i.e. subscriber A identification, is transferred to the receiving PBX using the PSTN signalling (see Figure 62). The IP PBX can pass this information to an external application server, which consults the customer database to make a decision on the skill group. The group information is then fed back to the PBX, which places the call to this hunt group.

When a free helpdesk person, with enough knowledge of the platform of this particular customer, picks up the call, the PBX can retrieve additional information about the customer hardware and software platforms, version data, service contract status with information about recent contacts, open offers and accounting history. This information will be sent to the workstation of the helpdesk person, who picked up the call, and he or she already knows the background data and will be prepared to help the customer in an appropiate way. If the contact and customer information are up-to-date, the system will minimise the time required for transmitting the platform information verbally and eliminate errors inherent to inaccurate verbal descriptions.

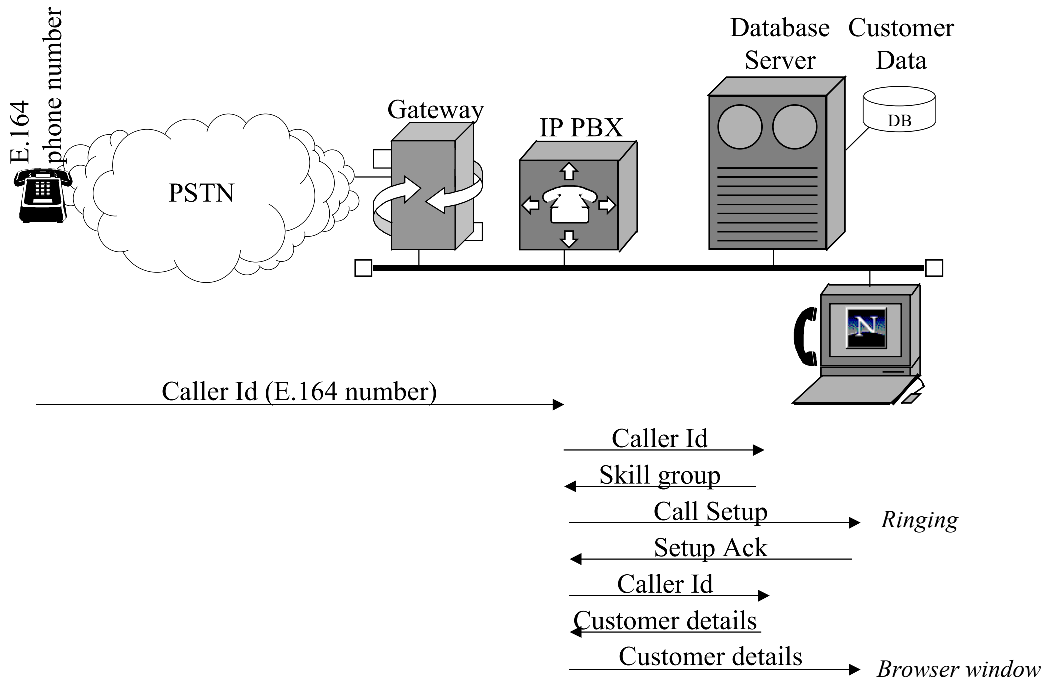


Figure 62: An example CTI application on a help desk.

It should be emphasized that CTI applications are not IP PBX specific, but have existed with traditional circuit switched PBXes for a long time. IP telephony just provides standard interfaces and APIs, which make CTI systems more attractive to implement.

6.2 Application Programming Interfaces

An Application Programming Interface (API) provides a standard interface to the telephone system. Often the CTI application is run on a separate platform on an application server. The most common component on the telephony system side is the PBX, but the terminal, like feature phone, IP telephone or workstation, can also be accessed directly.

6.2.1 Telephone API

Telephone API (**TAPI) is a Microsoft programming interface for intelligent call handling and Computer Telephone Integration applications**, both to the traditional circuit swithed telephone network and to IP Telephony. TAPI offers simple and universal routines to make a connection between two or more computers and to access all media streams.

TAPI 3.0 implements the object oriented COM model (Common Object Model) for C, C++ and Visual Basic programmers to develop TAPI applications. The main parts of the TAPI 3.0 are as follows (see Figure 63):

- **TAPI 3.0 COM API**, which provides call, media stream and directory control functions. It controls both Telephony Service Provider Interface (TSPI) and Media Stream Provider Interface (MSPI). Control is based on a group of simple COM objects, namely TAPI, Address, Terminal, Call and CallHub.

- **TAPI Server**, which describes the telephone services so, that they can be used both through the TAPI 3.0 and the former version, TAPI 2.1.

- **TSPI Interface**, which joins the protocol dependent call handling with protocol dependent network procedures. PSTN, ISDN and ATM networks are supported, as any other network or a device through a third party device driver. For LANs, the TCP/IP stack is used both for H.323 and IP Multicasting. The PSTN is used through a Unimodem driver.

- **MSPI Interface**, which provides a uniform way to handle media streams of a call. The main handler is DirectShow API, and all DirectShow telephony services need the MSPI.

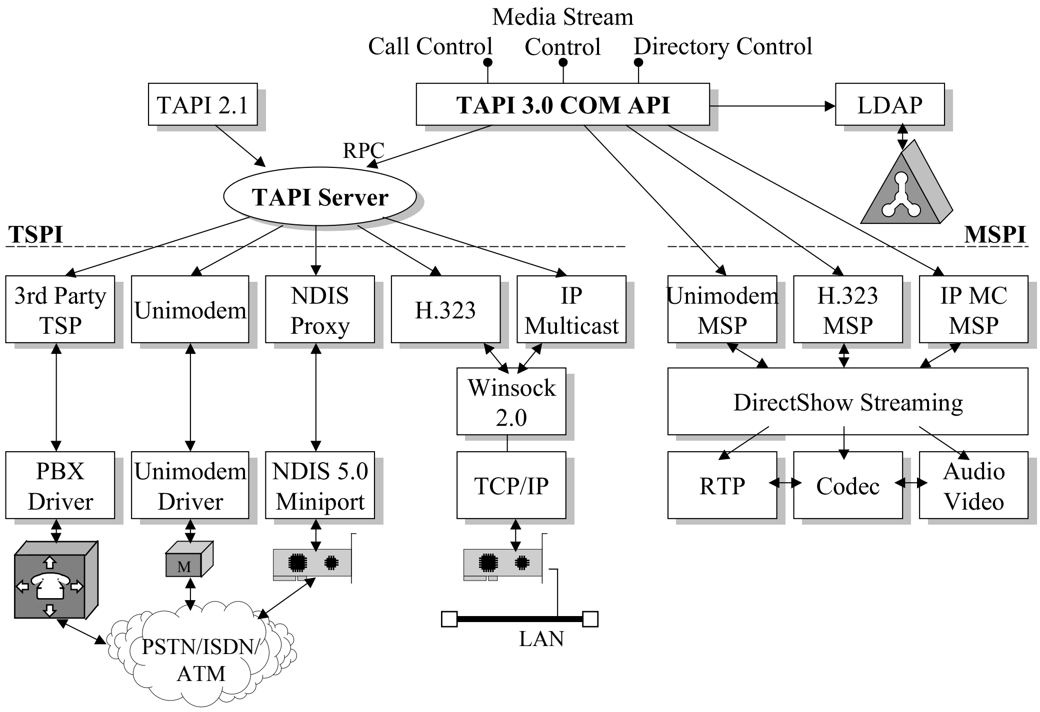


Figure 63: Telephone Application Programming Interface.

TAPI 3.0 supports RSVP, Packet Scheduling, 802.1p prioritisation and IP TOS/DSCP QoS, depending on the transmission network. /Teleware/

6.2.2 Java Telephone API

Java is a standard object oriented programming language to produce portable applications. The Java byte code is translated and excecuted in any Java Virtual Machine (JVM). **JTAPI is the Java API for telephony call control**, including a set of classes, interfaces and operation principles, which constitute the javax.* package. JTAPI implementations are the interface between a Java CTI application and telephony services. JTAPI provides access to the following areas of functionality:

- Call control, including control and observation of call processing.

- Physical telephone device control, including monitoring and control of one or more user interface elements of a telephone. These elements include the display, buttons, indication lamps, auditory components and hook switch.

- Media services, including manipulation and processing of the media streams associated with calls. Media streams can be tone generation and detection, telefax processing, voice record and playback, and converting text to speech (speech syntesis) and speech to text (automatic speech recognition).

- Administrative services for telephony, including startup, shutdown and management of telephony resources.

JTAPI does not provide access to signalling protocols or non telephony services, for example the telephone user interface components, which Java based telephones will likely need. Additional Java interfaces are needed for power management, messaging, Web browsing and SNMP support. /jtapi/ /jtapi2/

6.2.3 Extensible Markup Language and VoiceXML

XML (Extensible Markup Language) is a HTML alike markup meta language, which includes a possibility to define private tags. While HTML uses a predefined set of tags to describe the structure and to a limited extent also the outlook of a Web document, **XML can be used to describe the information context**. Some vendors use a set of XML tags to describe new user interface pages of IP telephones and multimedia terminals (see Figure 64). The terminal needs an XML browser and a display, and it communicates with the Web Server using HTTP.

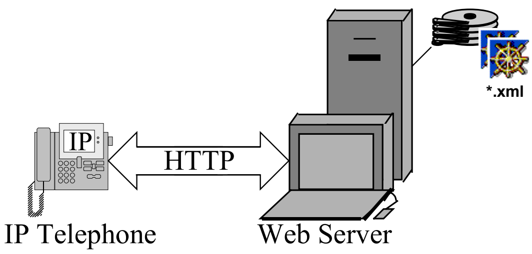


Figure 64: XML documents can describe user interface components for IP telephones.

VoiceXML is a markup language, accepted by the World Wide Web Consortium (W3C) as the basis of Dialog Markup Language. The VoiceXML consortium includes over 300 participants, both traditional and non traditional telephony vendors, and first VoiceXML products already exist. **VoiceXML represents human to computer dialogs**. The client is a voice browser with audio output and input, both with voice and keypad tones. The language looks much like HTML, using starting and ending tags, preferably intended for readability. A simple VoiceXML file might be the following:

```
< ?xml version="1.0"?>
   < vxml application="greeting.vxml" version="1.0">
      < form id="ThanksForCalling">
         < block>
            < prompt>
                Nice to hear from you
                <audio src="http://www.puska.fi/wellcome.wav">
            < /prompt>
         < /block>
      < /form>
   < /vxml>
```

The language includes tags for forms (<form>), field items (<field>, <record>, <transfer>, <object>, <subdialog>), control items (<block>, <initial>), for user input (<field>, <prompt>, <grammar>, <catch>), and program flow control (<goto>, <if>, <else>, <elseif>), as well as for variable definition and initiation, and for scope (<var>, <block>, <filled>, <catch>, <assign>). The VoiceXML browser ignores white spaces, but intention is recommended for readability. /voicexml/

6.3 An Example CTI System

An example of Computer to Telephony Integration is the Cisco CallManager IP PBX, which provides documented interfaces for external applications. Cisco offers some CTI applications, like Workflow, Intelligent Voice Response System and Contact Center, and promotes a partnership program for third-party add-on software.

As shown in Figure 65, CallManager performs call processing and provides an SQL interface for the configuration database and a CTI interface for the external application server, which is running on a separate platform. The CTI applications have a role on call processing, and they can also perform media termination, like voice messaging, or control media termination stations. The application server may also use LDAP directory access or SMTP E-mail protocols. The application platform provides an Application Programming Interface, which is used to write CTI applications. The application software uses a TAPI or JTAPI interface for the application platform and the CallManager interface, SQL for the database access and LDAP for accessing directory services. The selection between TAPI and JTAPI is a matter of needs, preferences and expertise.

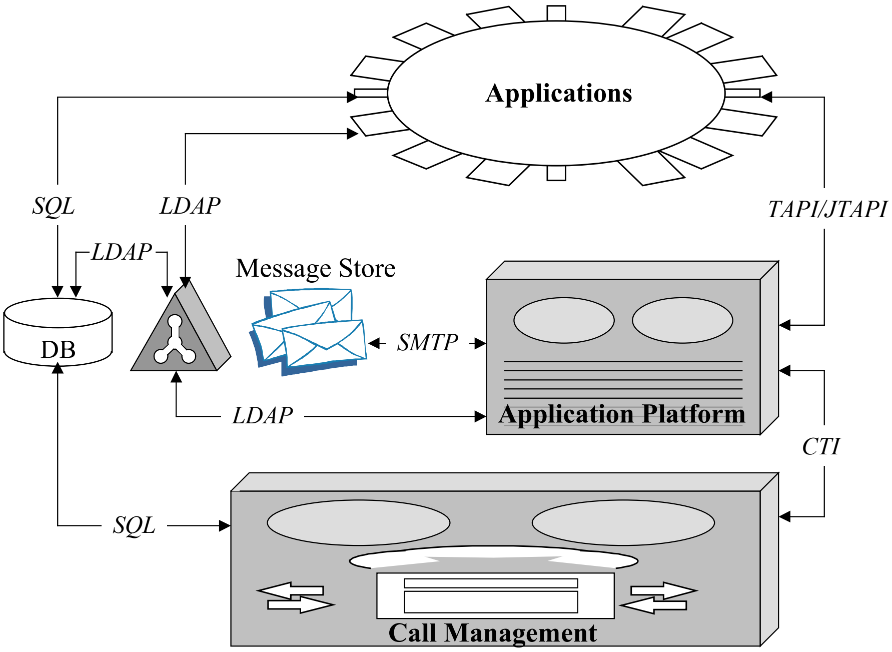


Figure 65: Cisco CallManager Application Infrastructure.

Next we will have a closer look at the Cisco implementation of TAPI, which is an abstract layer between the TAPI CTI application and the application platform (including hardware, operating system and transport protocols). As shown in Figure 66, TAPI is divided into the telephony application PC and the CallManager server PC. The TAPI application accesses communication controls through a Dynamic Link Library (Tapi32.dll or Tapi3.dll). The library communicates with the TAPI server process (TAPISRV.exe), using a private Remote Procedure Call (RPC) interface. The TAPI server then communicates with the Telephony Service Provider (Tsp.tsp) using a TSPI interface. The interface between the Cisco TSP on the Telephony application PC and the CallManager is known as CTIQBE (CTI Quick Buffer Encoding), a derivative of the Microsoft TAPI buffer format. The QBE defines C structures for copying from or to the output string. Finally, the CallManager controls the Cisco IP Telephone call setup using the Skinny station protocol over TCP.

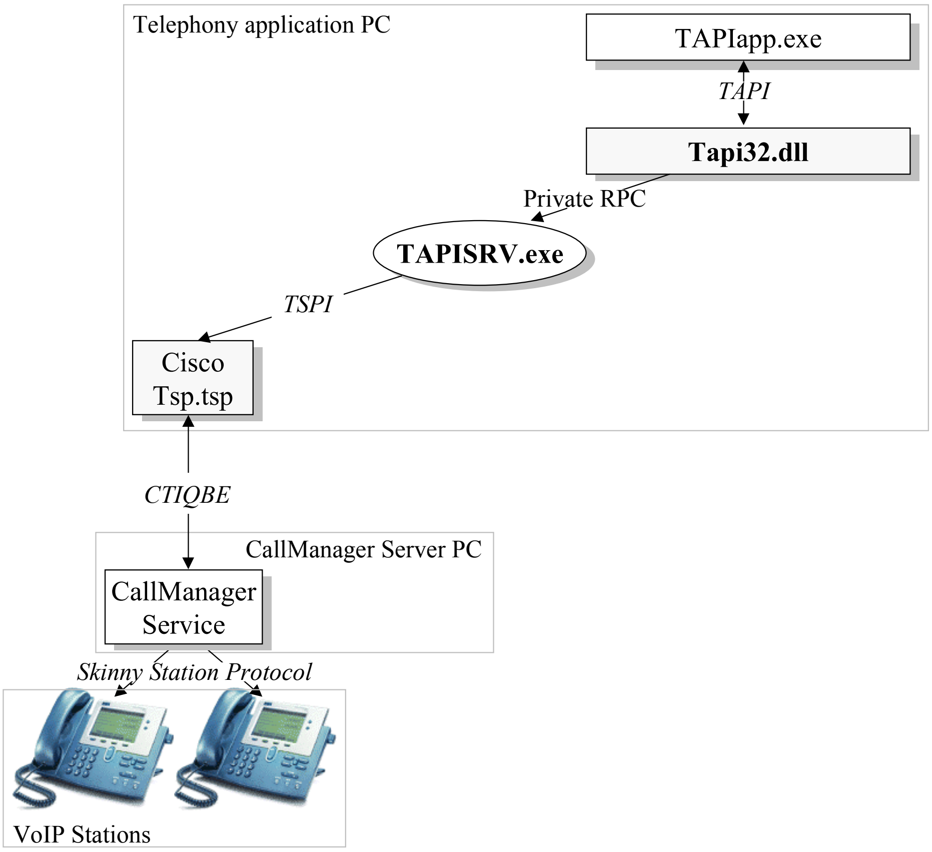


Figure 66: Cisco TAPI architecture. This should be compared with Figure 63, of the generic TAPI architecture.

JTAPI provides a similar API for Java based application development. It supports call and media stream control. As with Java in general, the JTAPI is more operating system independent, while TAPI is developed by Microsoft. CallManager for JTAPI supports Java packages for call control, Call Center and media, and various extensions for API usability, media termination and device roaming.

The XML language is used to create Web based pages for the Cisco 79xx IP telephones. The telephone set includes an XML browser and an LCD dot matrix display. Using XML, menus, text and graphics can be shown on the display. The user uses the navigator button to select a menu item, and receives the requested information from a Web Server. Example applications include stock quote. /CM/

6.4 Review

A Computer Telephone Integration system includes connection to operative EDP computers and telephone exchange, feeds call data to EDP and receives additional data, which is used for call forwarding or displayed on user terminal. The intention is to bring additional value to an organisation, which is doing business over the phone. IP telephony provides standard interfaces and APIs for CTI applications. These include Microsoft TAPI and Java JTAPI for an application server, and XML and VoiceXML for terminals. Object oriented TAPI includes control functions, TAPI Server for downword compatibility, and Telephony Service Provider Interface and Media Stream Provider Interface for network and media.

6.5 Quiz

- What is Computer Telephone Integration (CTI)?
- Give an example of a CTI application
- What is the main difference between a traditional circuit switched and IP based CTI interface?
- Who has developed the Telephone API (TAPI) interface?
- Why Media Stream Provider Interface (MSPI) is included in TAPI?
- What does VoiceXML describe?

6.6 Material

/Teleware/ IP-puhe. Teleware Oy, course handouts.

/CM/ John Alexander et. al.: Cisco CallManager Fundamentals. Cisco Press, Indianapolis, 2001.

/voicexml/ Eric D. Tober, Robert Marchand: VoiceXML Tutorials. VoiceXML, 2001. Internet, <URL: http://www.voicexml.org/tutorials/intro1.html>

/jtapi/ JTAPI Introduction. Sun Microsystems, 2001. Internet, <URL: http://java.sun.com/products/jtapi/

/jtapi2/ An Introduction to JTAPI (Java Telephony API). ECTF Framework White Paper, ECTF Secretariat, 1997. Internet, <URL: http://java.sun.com/products/jtapi/jtapi-1.2/JTAPIWhitePaper_o_7.html>

7 Network Quality of Service

7.1 QoS Backgrounder

WAN links on packet switched data networks are dimensionned to give acceptable response time with reasonable costs. Traditional data applications, like file transfer, remote printing and application services, generate bursty traffic, which tends to use all available bandwidth while the application transmits or receives. IP telephony, packetized video and other real time applications generate moderate bit rate UDP streams, which either have constant or variable bit rate, but need a certain bandwidth, delay and packet loss ratio. To quarantee proper voice quality on combined data and voice network, voice packets should be given preference over data (Figure 67). Generally speaking, **QoS allocates network resources to different applications** based on business needs.

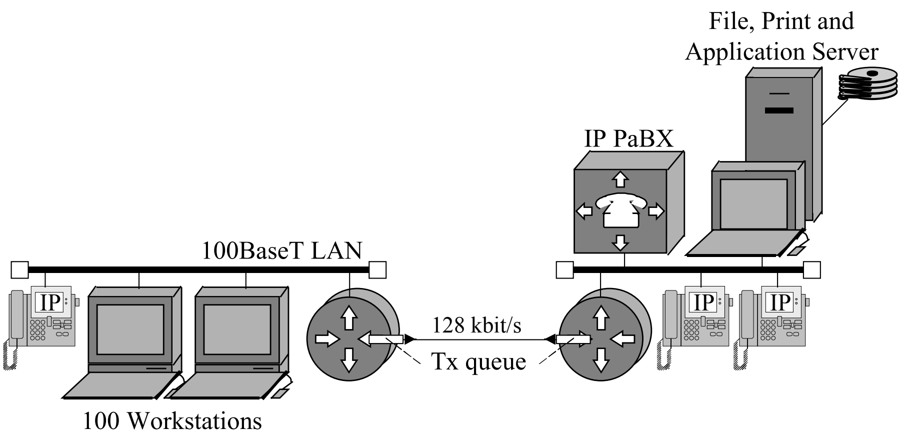


Figure 67: Delay critical voice packets need quaranteed portion of the network capacity.

A QoS solution may consist of the following functions (Figure 68):

- **Packet Marking**, in terminals or access routers, distinguishes and marks packets or flows from different applications needing different handling. Marking may be included in packets or it may use separate signalling messages.

- **Packet Classifying** in network nodes, which reads the marking and hands over packets to the queueing process.

- **Packet Scheduling** or queueing in network nodes, which places higher priority packets in priority queues and reshedules the packet flow.

- **Congestion Avoidance** methods, which try to detect high traffic periods and avoid possible network congestion by lowering transmission by non real time applications. Congestion Avoidance is not shown in Figure 68.

- **Traffic Shaping** in ingress access routers, to control that the amount of high priority traffic will not exceed traffic contract or rob the whole network capacity.

- **Traffic Policing** (not shown in Figure 68) in network nodes, to make sure that the subscriber keeps his traffic contract. At minimum, the contract includes a limit for the total or high priority traffic. More sophisticated contracts include limits for maximum and average bit rates and burst sizes for different traffic classes.

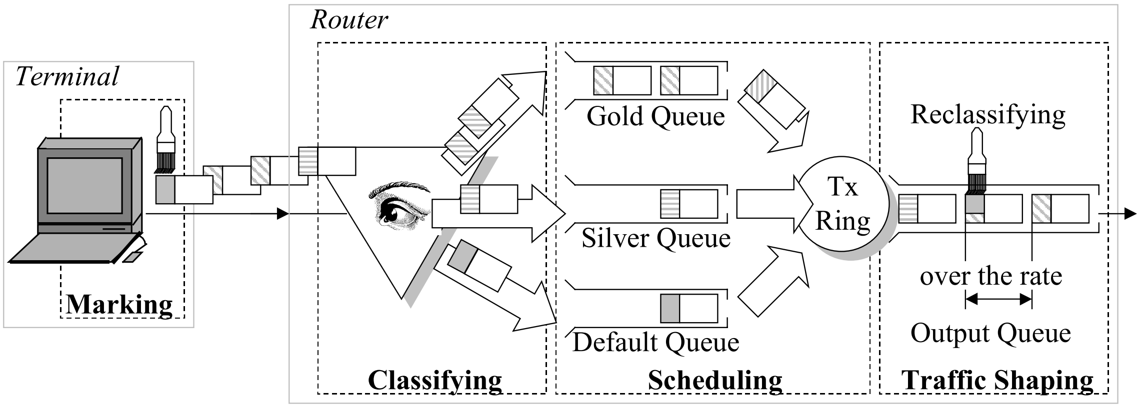


Figure 68: Most important Quality of Service functions.

QoS solutions adds network complexity, so the need should be carefully considered. Real-time applications need quaranteed delay, so some kind of QoS is needed on potentially congested network links. The LAN access for a VoIP terminal nornally offers enough capacity, and no special QoS configuration is needed. WAN links, on the other hand, serve multiple workstations and applications and when dimensioned, also the connection cost must be considered, leading to a need for a QoS solution. LAN backbones are something in between these cases, and the need for QoS should be considered case by case.

7.2 Packet Marking

7.2.1 Type of Service, IP Precedence and DSCP

Packets or packet flows should be handled differently based on their needs. For this, the traffic carrying **intermediate nodes must be able to distinguish the packets that need**

special treatment. To enable this, one of the following methods should be implemented:

- Differentiated Services (DiffServ), where each packet includes information about its importance.

- Integrated Services (IntServ), which uses a separate signalling protocol to distribute the reservation information for a flow. IntServ will not be covered here.

The DiffServ concept uses the third field on the IPv.4 packet, which contains a one byte TOS, IP Precedence or DSCP value (Figure 69). The former Type of Service used bits 2, 3 and 4 (* to request high reliability, high troughput or low delay, while IP precedence uses three MSBs to specity a Class of Service. The new DSCP uses the six MSBs to specify 64 standardized codepoint values to indicate the default, Assured Forwarding or Expedited Forwarding Per-Hop Behaviour. Many VoIP terminals and applications are able to set this field on IP packets (Figure 70). If not, the marking may be performed by a switch or a router, preferably as near the source as possible (**. In Cisco routers, the configuration is based on access control lists and policy routing. .

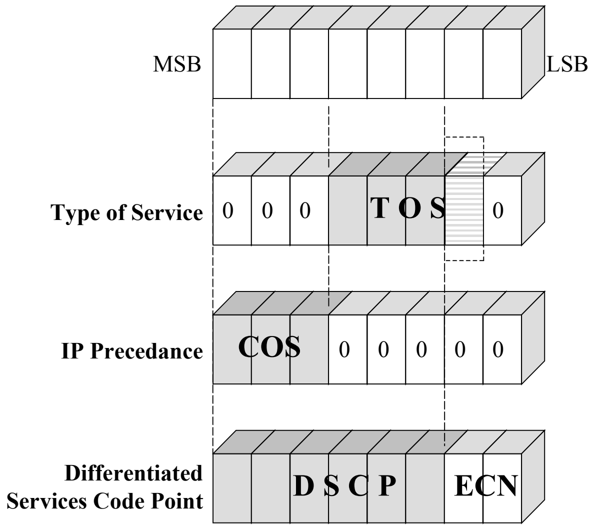


Figure 69: TOS, IP Precedance and DSCP byte on an IP packet.

*) Later, also the bit 1 was added for TOS marking.

**) Remarking IP Precedence and DSCP is needed to ensure, that a misconfigured or uncorrectly coded application will not get unnecessary high priority.

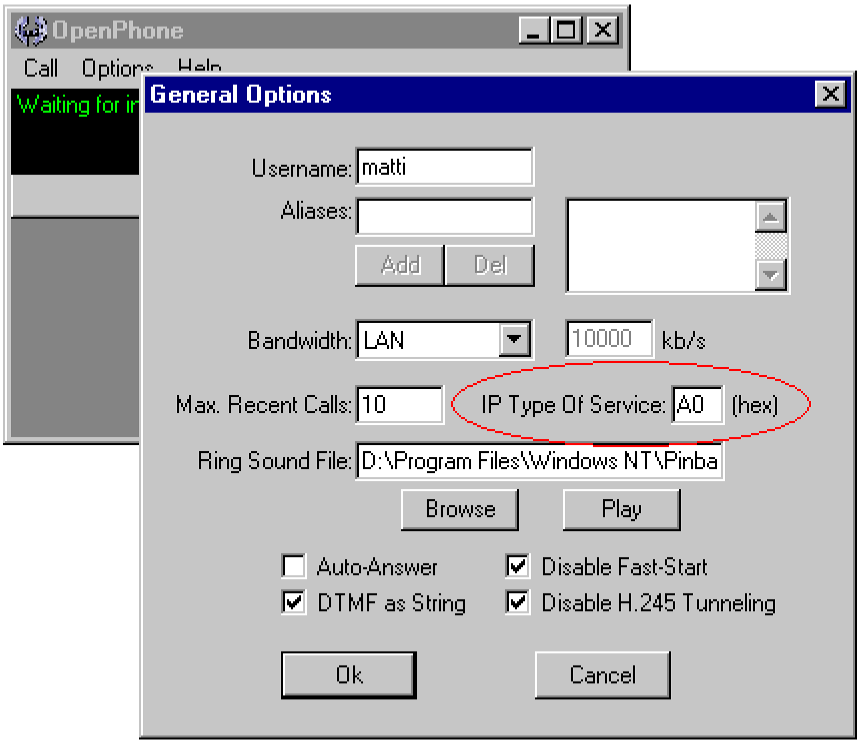


Figure 70: Marking critical (**101**0 0000 = A0) IP Precedence by OpenPhone application.

7.2.2 VoIP Recommendation for Marking

For network performance, packet marking should be used. DSCP marking should be favoured, if supported by network elements. VoIP and VoIP control packets should be classified as near the terminal as possible. Number of different classes should be kept in minimum: often two or three PHBs are enough for basic voice and data services.

If the terminal cannot mark packets with DSCP, this should be done in the nearest switch or router. Other applications besides VoIP shouldn't be relied on, but their packets should be reclassified to routine.

Queueing strategies on backbone routers should be consistent with the DSCP marking. Expedited Forwarding PHB needs Priority Queueing, while Assured Forwarding can use Custom Queueing or WFQ.

7.3 Packet Classifying and Scheduling

Incoming and outgoing packets are placed in queues in terminals, swithes and routers. If the processor load on the network element is not extremely high, queueing time in receive buffer is kept low. When multiple terminals send packets through the same backbone trunk or WAN link with limited capacity at the same time, packets must wait in transmit queue before being send (see Figure 71). **Queueing strategies** include democratic FIFO (First In First Out) and various solutions, which **give higher precedence or absolute priority to certain packets over the other** (*. There are no standards for queueing, and equipment vendors have their own implementations and names. The following chapters will cover operation and configuration of the most common queueing technologies.

7.3.1 Fist In First Out

FIFO queueing places all packets in a single queue and transmits them when bandwidth becomes available (Figure 71). FIFO doesn't include packet classification. Because it doesn't give any preferences, FTP file transfer may use all the available bandwidth, so RTP packets will arrive too late. Because of this fact, FIFO is not suitable on networks with real time applications.

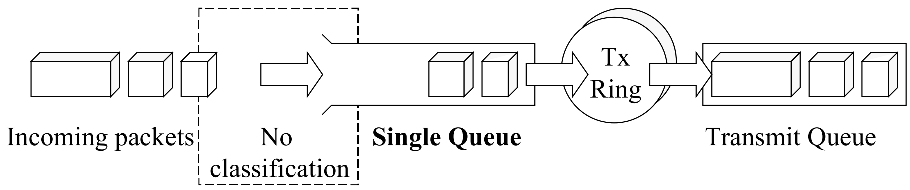


Figure 71: FIFO queueing.

Most switches and routers include optional FIFO queueing, but normally it is not the default. On most Cisco routers the default queueing strategy for serial interfaces is Weighted Fair Queueing, but FIFO can be enabled on an interface using `no fair-queue` interface configuration command.

*) While certain queueing strategies reorder the packet flow, the process is called packet scheduling.

7.3.2 Weighted Fair Queueing

Weighted Fair Queueing (WFQ) classifies packets based on their properties and places packets in multiple queues (Figure 72). Fair amount of bandwidth is given to each queue, so no single application can consume all available bandwidth. WFQ gives preference to low bandwidth applications, whose packets are served with low delay, while high volume traffic streams only get a fair share of the remaining capacity.

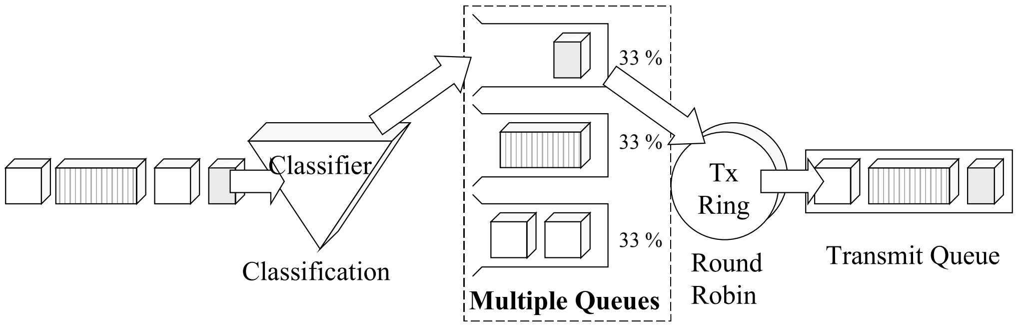


Figure 72: Weighted Fair Queueing principle.

Figure 72 shows only three queues, but real WFQ implementations use much more. WFQ dynamically identifies data streams based on several factors, including the following:

- source and destination IP address
- protocol type
- TCP or UDP port number
- DSCP, IP precedence or TOS value of the packet.

The Cisco implementation of WFQ adjusts queue lengths dynamically based on IP precedence, Frame Relay BECN and FECN bits and RSVP and RTP priority values. This allocates automatically more bandwidth to packet flows with higher IP precedence value. If a congestion is indicated by the Frame Relay Permanent Virtual Circuit, the queue length of the conversation encountering the congestion is lowered.

WFQ is the default queueing strategy on Cisco router interfaces with a bandwidth of 2,048 Mbit/s or less. When enabled manually with a fair-queue command, the following optional parameters can be configured:

- Congestive Discard Threshold, specifying the number of messages that are allowed on each queue. When a conversation reaches this threshold, new packets will be discarded. The default value is 64 messages and the value must be an integer power of 2 in the range 16 to 4096.

- Number of Dynamic Conversation Queues, which gives the number of queues for best effort conversations. This parameter can be configured to values 16 - 4096, the default being 64. The higher the value, the better service will be given to best effort traffic, meaning lower service for the RTP connections.

- Number of Reservable Conversation Queues, which specifies the number of reservable queues for RSVP reservations. The allowable range is 0 to 1000, zero being the default.

On a low capacity link with few users, we might want to give good service for VoIP traffic by reducing the number of queues for best effort services. If RSVP (Resource Reservation) is not used, the configuration will be the following:

```
ciscoRouter(config-if)#fair-queue 64 32 0
ciscoRouter(config-if)#exit
ciscoRouter(config)#exit
ciscoRouter#show interface serial 0
Serial0 is up, line protocol is up
  ...
  Queueing strategy: weighted fair
  Output queue: 600/1000/64/0 (size/max total/threshold/drops)
     Conversations  13/15/32 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated
```

In most cases WFQ automatically gives good service for VoIP, even with the default settings. WFQ will, however, not give absolute priority to packets carrying real time data. For this, priority queuing is needed. WFQ automatically identifies different data streams, places them in different queues and allocates link bandwidth fairly.

7.3.3 Custom Queuing

Custom Queuing makes it possible to divide the available bandwidth to particular protocols. Packets are classified into multiple queues based on configured access control lists, and each queue is served sequentically, giving a configured portion of the transmit capacity (Figure 73). Custom Queuing needs thorough understanding of the protocols and a lot of administrative work, but with proper configuration it offers detailed control over the packet flow. Also CQ doesn't offer absolute priority.

The Cisco implementation of CQ offers up to 16 output queues plus one for system messages. Traffic flows on the VoIP queue are defined using an access control lists.

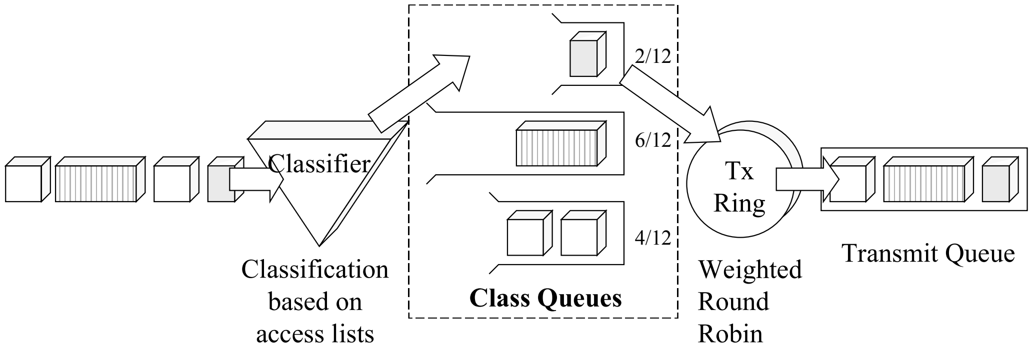


Figure 73: Custom Queuing.

7.3.4 Low Latency Queueuing

Low Latency Queueuing adds strict priority to Class Based Weighted Fair Queueuing. CBWFQ without LLQ provides weighted fair queues with configurable sizes based on defined classes. LLQ adds a single queue with strict priority for a configured class. Strict priority is needed by real time voice applications to reduce jitter. Only constant bit rate voice traffic should be assigned to the priority queue, because voice is well behaving traffic with known profile and needs a nonvariable delay.

Bandwidth is configured for the priority queue. If the strict priority traffic exceeds the allocated bandwidth during a congestion, some packets will be dropped, ensuring that nonpriority traffic will get a share of the capacity. The priority class traffic is allowed to exceed the bandwidth, if the interface is not congested.

In Cisco routers, LLC can ge used for serial links and ATM Permanent Virtual Circuits. The following example gives absolute priority with 200 kbit/s bandwidth for VoIP and VoIP control, and uses WFQ with multiple queues for all other packets. /LLQ/

```
ciscoRouter#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
cisco(config)#class-map voice
cisco(config-cmap)#match access-group 110
cisco(config-cmap)#exit
cisco(config)#policy-map llq200k
cisco(config-pmap)#class voice
cisco(config-pmap-c)#priority 200
cisco(config-pmap-c)#exit
cisco(config-pmap)#class class-default
cisco(config-pmap-c)#fair-queue
cisco(config-pmap-c)#exit
cisco(config-pmap)#exit
cisco(config)#
```

```
cisco(config)#int ser 0/1
cisco(config-if)#service-policy output llq200k
cisco(config-if)#exit
cisco(config)#access-list 110 permit udp any any range 16380 16480
cisco(config)#access-list 110 permit tcp any any eq 1720
cisco(config)#exit
```

7.3.5 Priority Queueing

In Priority Queueing (PQ) higher priority queues are given absolute priority. Packets, which are placed on the high priority queue by the classifier are serviced first until the high priority queue is empty. Next the medium priority queue are served and only after that the low priority queue. PQ ensures that the mission critical traffic always gets as much bandwidth it needs, but on an uncorrectly configured network the low priority traffic may not get any service.

On an interface of a Cisco router, PQ is enabled by `priority-group` command. The following configuration follows the previous example, but gives absolute priority to VoIP and VoIP control packets.

```
ciscoRouter#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
cisco(config)#interface serial 0
cisco(config-if)#ip address 192.168.1.1 255.255.255.0
cisco(config-if)#priority-group 1
cisco(config-if)#exit
cisco(config)#
cisco(config)#access-list 110 permit udp any any range 16380 16480
cisco(config)#access-list 110 permit tcp any any eq 1720
cisco(config)#priority-list 1 protocol ip high list 110
```

When PQ is used, special care must be taken to ensure, that high priority traffic will never rob all bandwidth. If only voice traffic is allocated to the high priority queue, traffic shaping or call admission will ensure, that also lower priority applications will get a portion of the link capacity. Various vendor specific alternatives of PQ and combinations of PQ and WFQ have been developed to overcome the limitations of priority queuing.

7.3.6 Short VoIP Recommendation for Packet Scheduling

In VoIP networks, queuing issues must be considered in LAN backbone trunks and WAN links, where multiple terminals and applications compete of limited trunk capacity. In many cases, WFQ is a good choice for the queuing strategy. It is easy to implement, but still offers some tuning possibilities. A misconfigured or improperly implemented WFQ will never starve other applications.

If more detailed control over queuing is needed, CQ, PQ or their alternatives should be used. Custom Queuing provides the possibility to provide a configured bandwidth for certain applications, which is normally sufficient in properly dimensionned VoIP networks. If strict priority is really needed, Low Latency Queueuing or Priority Queuing should be assigned on those interfaces that need to give absolute priority to VoIP. Additional techniques, like traffic shaping, must be used to ensure, that high priority traffic will never rob all the bandwidth from lower priority applications.

7.4 Traffic Shaping and Policing

7.4.1 Link Fragmentation and Interleaving

Queueuing may reschedule high priority packets, but finally VoIP packets have to wait in the transmit queue behind one or more data packets. Normally bulk file transfer, file and print services and Web browsing, uses the largest possible frame size to keep the portion of headers as small as possible. Serialization delay for a single 1 504 byte frame (* on a 128 kbit/s is 94 ms, which may take more than half of the total delay budget on a single router, and certainly produces too much delay variation. Large packets, i.e. **jumbograms, may be fragmented into smaller pieces** by the transmitter and reassembled by the receiver (Figure 74).

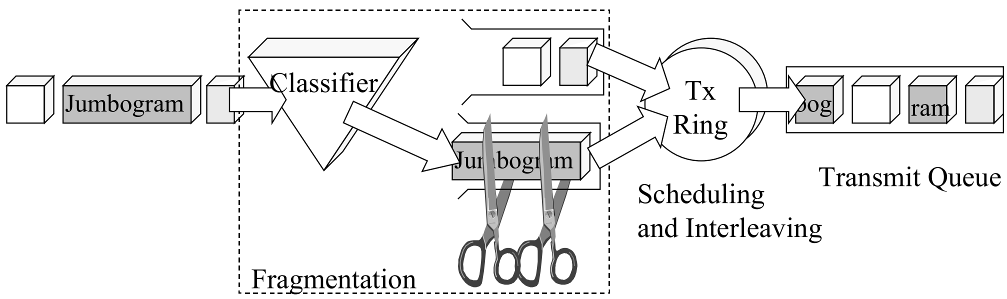


Figure 74: Link Fragmentation and Interleaving.

*) A 1.504 byte Frame Relay frame includes the Frame Relay header and can carry a full-size 1.500 byte Ethernet frame payload.

Fragmentation may take place in data link or network layer, but normally data link layer solutions are preferred because of their higher efficiency and their ability to eliminate possible Don't Fragment Bit problems. **Multi-Class Multilink PPP** (MCML PPP) is the standard fragmentation method in PPP links, but it needs a Multilink PPP configuration (*, although using a single physical connection. On a Cisco router, a dialer interface is needed both for ISDN and leased line connections. **`ppp multilink fragment-delay`** takes the blocking time in milliseconds as an argument.

```
ciscoRouter#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ciscoRouter(config)#interface serial 0
ciscoRouter(config-if)#bandwidth 128
ciscoRouter(config-if)#no ip address
ciscoRouter(config-if)#encapsulation ppp
ciscoRouter(config-if)#no fair-queue
ciscoRouter(config-if)#ppp multilink
ciscoRouter(config-if)#multilink-group 1
ciscoRouter(config-if)#exit
ciscoRouter(config)#
ciscoRouter(config)#interface Multilink 1
ciscoRouter(config-if)#ip address 192.168.1.1 255.255.255.0
ciscoRouter(config-if)#fair-queue 64 256 1000
ciscoRouter(config-if)#ppp multilink
ciscoRouter(config-if)#ppp multilink fragment-delay 10
ciscoRouter(config-if)#ppp multilink interleave
ciscoRouter(config-if)#multilink-group 1
```

In this configuration, IP address and queueing are omitted from the physical serial 0 interface, which only holds PPP encapsulation, PPP multilink and mapping to multilink group 1. The logical interface Multilink 1 holds the IP address, WFQ queueing, PPP multilink and MCML PPP configurations.

For Frame Relay interfaces, fragmentation is covered by **FRF.12** Frame Relay Forum standard. On Cisco routers, FRF.12 fragmentation size is configured in bytes with **`frame-relay fragment`** command, assigned from the map-class configuration mode. The created map-class name must also be attached to the DLCI identifier in use. The FRF.12 portion of the configuration is the following (**:

*) Originally Multilink PPP was designed to be used to bundle multiple PPP channels, like dual ISDN B channels, as a single higher capacity link.

**) frame-relay fragment takes the byte count as an argument. For a 128 kbit/s line, the configuration presented above will produce t= I/R = 320 * 8 b / 128 kb/s = 20 ms fragments.

```
ciscoRouter#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
ciscoRouter(config)#
ciscoRouter(config)#interface serial 0.66 point-to-point
ciscoRouter(config-subif)#frame-relay interface-dlci 66
ciscoRouter(config-fr-dlci)#class voip
ciscoRouter(config-fr-dlci)#exit
ciscoRouter(config-subif)#exit
ciscoRouter(config)#map-class frame-relay voip
ciscoRouter(config-map-class)#frame-relay fragment 320
```

7.4.2 Traffic Shaping

Traffic shaping is needed to **ensure, that the amount of high priority traffic will not use all available network capacity**, but a portion is left also for best effort services. Shaping is also needed in subrate E1/T1 services and in asymmetric Frame Relay interfaces to avoid situation where higher bandwidth overloads a lower access rate router interface. Normally traffic shaping is performed at the output of an edge router at customer premises. For shorter periods, router may buffer excessive packets and send them later (Figure 75). For longer excess periods, the shapener may reclassify or drop extra packets. Shaping always takes place in the output of the router.

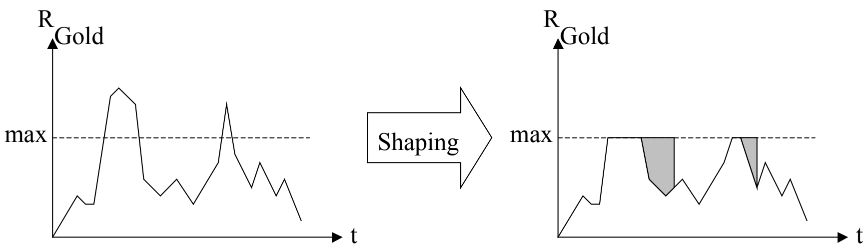


Figure 75: Traffic Shaping using buffering.

Cisco IOS includes Generic Traffic Shaping (GTS) and Frame Relay Traffic Shaping (FRTS) tools. **GTS** is configured **per-interface** and applies for output of the selected interface. GTS can use extended access lists to select the shaped traffic. It smoothens traffic by storing excessive packets on a buffer (Token Bucket). When the bucket is empty, the arriving packet is compared with the configured access rate and either send further (if it fits into the shaping rate) or placed on the bucket. If the bucket holds packets, the newly arrived packet is placed on the bucket. The shaper removes packets from the bucket in accordance to the configured rate (Figure 76). GTS uses Weighted Fair Queuing to hold the delayed traffic.

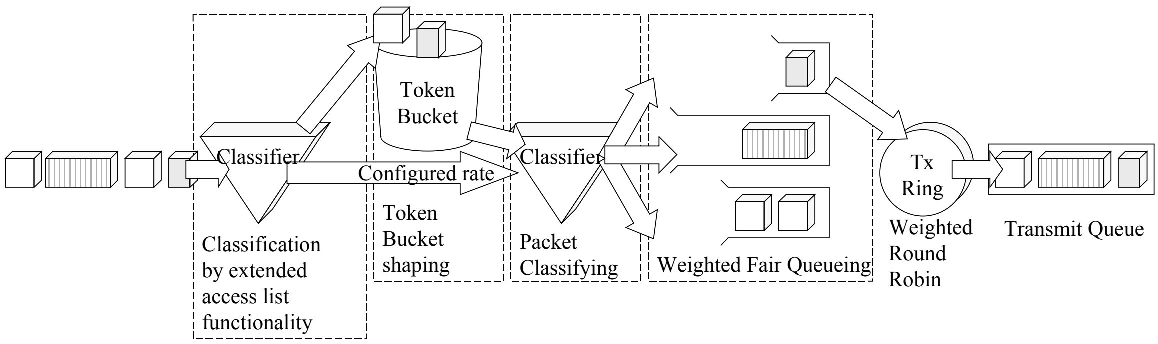


Figure 76: Generic Traffic Shaping operation.

GTS shaping is enabled on an interface with a **`traffic-shape rate`** command, followed by the bit rate that traffic is shaped to. Optional parameters include burst size and excess burst size, both in bits. The following set of commands include GTS configuration for access rate matching.

```
ciscoRouter(config-if)#ip address 192.168.1.1 255.255.255.0
ciscoRouter(config-if)#encapsulation frame-relay ietf
ciscoRouter(config-if)#traffic-shape rate 256000
```

When GTS is used to limit the amount of high priority traffic, only packets matching the extended access list is exposed to shaping. In this case, **`traffic-shape group`** command is used in the following way (* /Shaping/:

```
ciscoRouter(config-if)#traffic-shape group 110 192000
ciscoRouter(config-if)#exit
ciscoRouter(config)#exit
ciscoRouter#show traffic-shape

Interface   Se0
   Access Target Byte  Sustain  Excess   Interval Increment Adapt
VC List   Rate   Limit bits/int bits/int (ms)     (bytes)   Active
-  110    192000 1968  7872     7872     41       984       -
```

Also **FRTS** smoothens traffic patterns by delaying excessive packets and matches the effect of unbalanced access rates, but as the name implies, it can only be used in **Frame Relay virtual circuits**. FRTS is configured per DLCI (Data Link Connection Identifier). It uses Frame Relay BECN and FECN congestion notification bits to dynamically use more or less bandwidth. Delayed packets can be stored in WFQ, CQ or PQ queues.

*) The interval value is determined by dividing the sustain bits with the target rate, i.e. 7872b / 192000 b/s = 41 ms. This value is perhaps not optimal for a Frame Relay interface.

7.4.3 Traffic Policing

Both traffic shaping and policing let network administrators to define how much bandwidth a connection or application can use. While traffic shaping happens in the edge of the network and buffers excessive outgoing packets, **traffic policing** takes place in service provider or core network to **make sure, that a subscriber doesn't exceed amount of traffic stated in the service contract**. Because policing drops or remarks non-conformant packets, it should always be combined with traffic shaping on customer premises equipment.

Cisco routers with 12.0(5)XE IOS or later offer Committed Access Rate (CAR) tools for policing. Either the whole traffic or a selected portion of it, for example high priority packets, are compared with configured thresholds. Separate conform and exceed actions are configured: normally passing conformed traffic (transmit), but dropping (drop) or remarking (set-dscp-transmit, set-frde-transmit, set-prec-transmit, set-qos-transmit) excess packets with lower priority.

Configuring traffic policing includes the following steps:

- creating a traffic class and and specifying the matching criteria
- creating a traffic policy and mapping it with the traffic class
- specifying the max bit rate, normal burst, excess burst, conform action, exceed action and violate action
- attacing the service policy to an interface /Policing/.

7.4.4 VoIP Recommendation for Shaping and Policing

When preference is given to certain packets, traffic shaping should be used to ensure, that high priority traffic will not use all available bandwidth. Shaping is especially important, if service provider uses traffic policing. If access-rate mismatch is present, also the total amount of traffic should be shapened in the high-rate end.

Link Fragmentation and Interleaving should be used in links with a bit rate of 768 kbit/s or lower. When used, fragment size should be configured to give blocking delay of 10 - 15 ms. Selecting the LFI method is dependent on data link framing. For public Frame Relay networks, FRF.12 should be configured to match the service contract parameters.

7.5 Congestion Avoidance

7.5.1 TCP Flow Control

In pure data networks, most IP packets are from connection oriented TCP transport, and only well under 10 % is carrying UDP datagrams. Statistics from the Internet core show, that the most popular application layer protocols are HTTP, FTP, SSH, NNTP and peer networking. The most common UDP application is DNS, which is important but a DNS query/response pair generates very small traffic. In corporate Intranets, application layer distribution is dependent on the IT solution, but while file, application and print services use TCP transport, the TCP domination stays. VoIP implementation makes the UDP portion larger, but in most cases data applications still consume most of the bandwidth, especially if video is not included.

Most TCP streams are rather short (90 % are 10 packets or less in each direction in the Internet core), but the remaining small number of long streams generate most of the transmitted TCP bytes (80 % in the public Internet). While TCP supports flow control and congestion management, it is possible to affect the biggest part of the traffic by implementing congestion avoidance to long TCP streams. While most traditional data applications are delay insensitive and TCP includes retransmission on errors, congestion avoidance only makes user response times longer but doesn't interrupt sessions.

TCP flow control is based on exchange of RWIN (Receive Window) values in TCP headers. A station informs the other party about its available receive buffer size with the RWIN. The initial RWIN value is quite conservative, but is enlarged exponentially, if network performance is good (slow start). A single retransmission is interpreted as congestion and the sending station slows down, as shown in Figure 78. Multiple dropped segments lead to a time-out, which puts the RWIN back to the initial value and restarts the slow start.

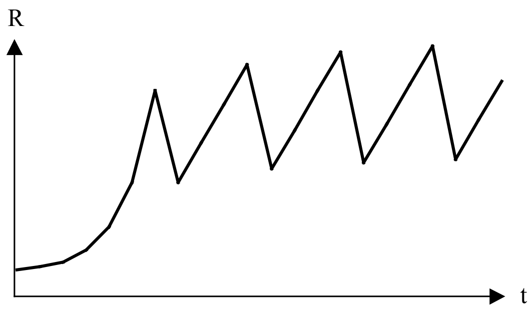


Figure 78: TCP Windowing mechanism in a long TCP session.

UDP is a connectionless unreliable transport protocol and doesn't include any mechanism for flow control or congestion management. VoIP applications use RTP over UDP for user data. Voice codecs generate constant bit rate streams, and there is no possibility to slow down the RTP source during a call. RTP and voice codecs include means to overcome low rate packet losses, but higher loss rate lowers voice and video quality. That is why intentional packet drop of RTP messages by congestion avoidance should be avoided. The amount of VoIP traffic should be limited with the use of admission control. /RFC 2581/

7.5.2 Random Early Detection and Weighted Random Early Detection

Congestion avoidance techniques monitor the link utilization and try to avoid congestion situations. If traffic level exceeds the threshold, packets are dropped from different flows, making TCP streams to lower RWIN value and slow down transmission.

Dropped packets are selected in different ways. The simplest way is to drop packets from the end of the queue (Tail Dropping), hoping that packets belong to multiple TCP streams. Random Early Detection stochastically discards packets, leading to a more even distribution of flows. Both these methods drop also UDP datagrams unnecessarily.

Cisco has developed Weighted RED. WRED takes also IP Precedence, DSCP and RSVP into account, when selecting droppable packets. The WRED algoritm discards lower priority packets selectively when interface starts getting congested, and when the lower priority sources slow down, more bandwidth will be available for higher priority packets. WRED follows the DiffServ principle and provides different performance characteristics for different classes of service.

WRED is enabled on an interface of a Cisco router using command **`random-detect`**, followed with an optional weighting constant. The exponential weighting constant determines the rate packets are dropped during congestion, the default of 10 dropped packets every 210 packets. The following example enables Weighted Random Early Detection on interface serial 0.

```
ciscoRouter#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ciscoRouter(config)#interface serial 0
ciscoRouter(config-if)#random-detect
ciscoRouter(config-if)#exit
ciscoRouter(config)#exit
ciscoRouter#show interface serial 0
Serial0 is up, line protocol is up
  ...
  Queueing strategy: random early detection (WRED)
```

WRED is recommended in highly utilized high-speed WAN links with high portion of loss tolerable protocols, like TCP. WRED shouldn't be used in links, which are mostly utilized by real time or other UDP applications.

7.6 Review

When both traditional data applications and real time VoIP applications use the same IP infrastructure, packets from the real time applications must be given preference over data to quarantee quality of voice and video representation. WFQ, CQ, LLQ and PQ queuing place VoIP packets to a high priority queue based on access control lists. PQ and LLQ also give absolute priority to selected packets.

To inform intermediate routers about the flow identification, end systems, workgroup switches and access routers may mark the DSCP field on the IP header. Now the core routers only have to read the DSCP value and select the target queue according to this.

Link Fragmentation and Interleaving breaks large packets into smaller pieces and interleave delay sensitive VoIP packets between the fragments, reducing the wait time of a small VoIP packet behind large packets from data applications. Data link layer fragmentation, like MCML PPP and FRF.12, should be preferred over network layer methods. Traffic shaping is used at the edge of the network to ensure, that the high priority traffic will not use all available network capacity. For this, soft methods, like buffering and reclassification are used. GTS and FRTS take into account the total bit rate, burst size and excess burst size. For Frame Relay, also flow control with BECN can be used. Traffic policing is performed in the service provider network to ensure, that subscribers don't exceed their service contract. Because hard methods, like dropping non-conformant portion of packets are used, policing should always be combined with traffic shaping.

On uniform networks, most of the packets and octets carry TCP segments. TCP flows support flow control with the RWIN mechanism. When early signs of congestion are noticed, Random Early Detection drops packets from different flows, causing multiple sessions to lower transmission rates. Weighted RED takes DSCP and RSVP into account and drops lower priority packets. When the low priority applications slow down, more capacity is left to higher priority real time application flows.

7.7 Quiz

- What does packet classification mean in QoS context?
- Where packet classification normally takes place?

- What does traffic shaping mean?
- Where traffic shaping takes place?
- What does queueing mean?
- What does congestion avoidance mean?
- Explain the operation of priority queueing
- Compare Weighted Fair Queueing and Priority Queueing regarding VoIP networks?
- Why should traffic shaping be used with Priority Queueing and Low Latency Queueing?
- Is there any difference on the service for VoIP between different queueing methods during a low loading condition on the interface in question? Why/why not?
- Why Link Fragmentation and Interleaving should be used in low bandwidth interfaces?
- List the performance related parameters for a Frame Relay traffic contract and give a short description of each.
- Why TCP provides congestion avoidance method while UDP transport doesn't?
- What are the most common congestion avoidance technologies used in routers?

7.8 Material

/RFC 2581/ M. Allman, V. Paxson, W. Stevens: TCP Congestion Control, RFC 2581. IETF, 1999.

/Shaping/ Configuring Generic Traffic Shaping. Cisco Systems, 2001. Internet, <URL: http://www.cisco.com>

/FRTS/ Configuring Frame Relay Traffic Shaping. Cisco Systems, 2001. Internet, <URL: http://www.cisco.com/warp/public/125/traffic_shaping:6151.html>

/LLQ/ Low Latency Queueing. Cisco Systems, 2001. Internet, <URL: http://www.cisco.com>

/Policing/ Traffic Policing. Cisco Systems, 2001. Internet, <URL: http://www.cisco.com>

/RSCP/ Configuring RSVP. Cisco Systems, 2003. Internet, <URL: http://www.cisco.com>

8 List of Acronyms

A

AAA	Authentication, Accounting and Authorization
AAL 2	ATM Adaptation Layer 2, a way to adapt Variable Bit Rate traffic with timing constrains into fixed sized ATM cells
AAL 5	ATM Adaptation Layer 5, a way to adapt variable length IP packets or Ethernet frames into fixed sized ATM cells
ABR	Available Bit Rate, an ATM traffic class
A/D	Analogue to Digital Conversion, the way to convert an analogue signal to digital numbers
ACD	Automatic Call Distribution, a CTI application for distributing incoming calls automatically, based on certain rules
ACELP	Algebraic Code Excited Linear Prediction, a voice coding method, based on voice source modelling
ACF	Admission Confirmation, an RAS response from the gatekeeper to the terminal, specifying the admitted bandwidth
ACK	Acknowledgement, a positive SIP response message
ACL	Access Control List, a way to filter IP packets based on packet and datagram/segment properties
ADM	Add Drop Multiplexer, SDH multiplexer to add or terminate channels on an SDH transmission system
ADPCM	Adaptive Differential Pulse Code Modulation, a voice coding system, which only transmits the difference of successive voice samples
ADSL	Asymmetric Digital Subscriber Line, a transmission system to achieve higher bit rates on an ordinary symmetric subscriber line
AF	Assured Forwarding, a Differentiated Services Per Hop Behaviour
AP	Access Point, a bridge between Wireless LAN terminals and the wired LAN network
API	Application Programing Interface, an interface, used by application software developers
ARJ	Admission Reject, a negative RAS response from the gatekeeper, indicating that the requested bandwidth is not admitted
ARP	Address Resolution Protocol, a way to find out the MAC address for a given network layer (normally IP) address
ARPA	Advanced Research Project Agency, the early public TCP/IP network in the USA that developed into the Internet
ARQ	Admission Request, an RAS request from the terminal to the gatekeeper for a specific target and bandwidth
ASIC	Application Specific Integrated Circuit, a custom made IC

ASN.1	Application Specific Notation number One, a presentation language used in NMS and H.323 systems
ATM	Asynchronous Transfer Mode, fast packet switched network, which uses fixed size cells

B

B	Bidirectional Frame, a picture frame on inter-frame video compression, that contains both predictive and historical information
Bc	Committed Burst, maximum number of bits that can be transmitted during an interval on a Frame Relay PVC
BC	Broadcast, a frame or a packet that is meant to all nodes on the broadcast domain
BCF	Bandwidth Confirmation, an RAS response from the gatekeeper for the bandwidth allocation
Be	Excess Burst, the maximum backlock, which can be used to save unused Bc values on a Frame Relay PVC
BECN	Backward Explicit Congestion Notification, a Frame Relay congestion control mechanism
BE	Border Element, an optional H.323 component, which exchanges address and authorization information between administrative domains
BER	Bit Error Rate, probability for a bit error on a digital transmission system
BGP	Boundary Gateway Protocol, a standards based external routing protocol
BRI	Basic Rate Interface, an interface for private customers to the narrowband ISDN network
BRJ	Bandwidth Reject, a negative RAS response from the gatekeeper, indicating that the requested bandwidth is not allowed
BRQ	Bandwidth Request, an RAS request from the terminal for a specified bandwidth
BT	Burst Tolerance, an ATM traffic parameter
B8ZS	Bibolar 8 Zero Substitution, a wire coding scheme used in North American PCM system

C

CAR	Committed Access Rate, cisco set of tools for traffic policing
CBWFQ	Class Based Weighted Fair Queueuing, a queueuing method, that provides configurable queue sizes based on defined traffic classes
CCITT	Comité Consultatif International Télégraphique et Téléphonique, international co-operative organisation for PTOs, nowadays called ITU-T
CD	Compact Disc, an audio disk containing stereophonic Hi-Fi music
CID	Conference Identifier, a RAS identifier for a conference call
CIF	Common Intermediate Format, 352 * 288 pixel video format

CIR	Committed Information Rate, the amounth of bandwidth that is always guaranteed for a Frame Relay PVC
CMIP	Common Management Information Protocol, the OSI network management protocol
CN	Canonial Name, an identifier for a directory record
CNAME	Canonial Name, a DNS record for an alternative name (nickname)
COM	Common Object Model, an object oriented programming model
COS	Class of Service, a nickname for 802.1p prioritization
CPE	Customer Premises Equipment, networking equipment owned or used by a customer, and situated on customer premises
CQ	Custom Queuing, a queuing solution
cRTP	RTP Header Compression, a way to compress RTP, UDP and IP headers
CRLF	Carriage Return Line Feed, the line termination signal
CRM	Customer Relations Management, an information system, containing data on customers
CRV	Call Reference Value, an identifier for H.225.0 messages
CS-ACELP	Conjugate Sructure Algebraic Code Excited Linear Prediction, a voice coding system, based on hybrid coding
CSCR	Contributing Source, a station that contributes to a mixed RTP stream
CTI	Computer Telephone Integration, the technology to integrate the PaBX with the EDP system, to provide additional services
CTIQBE	CTI Quick Buffer Encoding, an interface, specified by cisco, between a Cisco CallManager and an application PC

D

DCF	Disengage Confirm, a RAS signalling message by a gatekeeper to confirm a teardown
DDR	Dial on Demand Routing, a solution that opens and closes a dial-up connection on demand
DECT	Digital European Cordless Telephony, an European standard for cordless telephones, using a license free frequency band
DHCP	Dynamic Host Configuration Protocol, an application layer protocol for distributing IP addresses and other parameters to IP hosts
DLCI	Data Link Connection Identifier, an identifier for a Frame Relay PVC with local significance only
DN	Distinguished Name, a unique identifier for a directory record
DNS	Domain Name System, the system and application layer Internet protocol for resolving the IP address for a given hierarchical domain name
DRQ	Disengage Request, a RAS signalling message by a terminal to request for a teardown
DSA	Digital Signature Algoritm, an encryption system
DSP	Digital Signal Processing, technology to process signals digitally

DSCP	Differentiated Services Code Point, a field on IP V.4 and V.6 header, which can be used to mark packets in a certain flow
DTMF	Dual Tone Multiple Frequency, terminal signalling from a telephone keypad

E

ECN	Explicit Congestion Notification, two last bytes on a DS field of an IP packet, currently unused
EDP	Electronic Data Processing, system and services of computer hardware and software
EF	Expedited Forwarding, a Differentiated Services Per Hop Behaviour
EIGRP	Extended Inter Gateway Routing Protocol, a hybrid routing protocol by Cisco Systems
ERP	Enterprise Resource Planning, financial internal control and planning system
EU	European Union

F

FA	Foreign Agent, a Mobile IP component, which assists Mobile Node by relaying Registration Requests
FCS	Frame Check Sequence, an additional field on the frame trailer, which is used for error detection or error correction
FECN	Forward Explicit Congestion Notification, a Frame Relay congestion control mechanism
FIFO	First In First Out, a queuing mechanism
FQDN	Fully Qualified Domain Name, full DNS name for a station.
FR	Frame Relay, an ITU-T WAN interface for a fast packet switched network, that handles variable length frames
FRF.12	Frame Relay Forum standard 12, standard fragmentation method in Frame Relay interfaces
FRTS	Frame Relay Traffic Shaping, cisco realisation for traffic shaping in Frame Relay interfaces
FTP	File Transfer Protocol, an application layer Internet protocol for file retrieval

G

GCC	Generic Conference Control, a transport layer protocol for data conferences
GE	Gigabit Ethernet, an Ethernet like LAN technology offering 1 000 Mbit/s bit rate
GK	Gatekeeper, an optional H.323 component, which controls the amount of H.323 traffic on its zone

GRE	Generic Routing Encapsulation, an alternative way to encapsule IP packets in Mobile IP environment
GRJ	Gatekeeper Reject, an RAS message, which the gatekeeper sends to a terminal when terminal registration is rejected
GRQ	Gatekeeper Request, an RAS message that the terminal uses to discover the gatekeeper dynamically
GRS	Gatekeeper Routed Signalling, a way to route H.225.0, RAS and Q.931 signals through a H.323 gateway
GSM	Groupe Special Mobile, the pan European digital second generation mobile telephone system
GTS	Generic Traffic Shaping, cisco realisation for traffic shaping in serial interfaces
GUI	Graphical User Interface

H

HLF	Home Location Function, a H.323 database of users, needed for mobility
HLR	Home Location Register, a GSM database of users, needed for roaming
HSSI	High Speed Serial Interface, an ISO/IEC standard interface with high speed, up to 52 Mbit/s
HTML	Hypertext Markup Language, a markup language to describe the structure of a Web page
HTTP	Hypertext Transfer Protocol, an application layer Internet protocol for distributed multimedia systems

I

I	Information Frame, a video frame containing information about the full picture
IAM	Initial Address Message, an ISDN signalling message, which carries the destination E.164 number within the network
ICANN	Internet Company for Assigned Names and Numbers, an Internet company, which coverns IP addresses, DNS domain names and other identifications on the Internet
ICMP	Internet Control and Message Protocol, a set of messages for IP connection testing and error reporting
IDN	Integrated Digital Network, a digital telephone network, consisting of digital switches and transmission systems
IE	Information Element, a basic Q.931 signalling element
IEC	Inter Exchange Carrier, a long distance public telephone operator
IETF	Internet Engineering Task Force, a body to cordinate preparation of Internet standards
IMAP4	Internet Mail Access Protocol Four, a newer application layer Internet protocol to retrieve E-mail messages and attachments from the mail server to workstation

IN	Intelligent Networking, an add-on system to the digital PSTN to offer advanced call control functions
IOS	Internetworking Operating System, the OS for cisco routers
IP	Internet Protocol, the OSI network layer protocol, which is used on the public Internet and on private intranets
IPSEC	Secure IP, a standard way to build Virtual Private Networks
IPTSP	IP Telephone Service Provider, a Public Telephone Operator, which uses IP telephony to carry voice traffic
IRC	Internet Relayed Chat, an application layer Internet protocol for bidirectional text conversation
ISDN	Integrated Services Digital Network, fully digital multiservice network for voice and narrowband data applications
ISP	Internet Service Provider, a Network Service Provider, which offers access to the public Internet
ISUP	ISDN User Part, the uppoermost layer standard for ISDN network signalling
IT	Information Technology
ITU-T	International Telecommunications Union, Telecommunications Section, a union of Public Telephone Operators to control and cordinate the operation of national PTOs
IVR	Interactive Voice Response, a CTI application that gives synthesized voice responses to caller interaction, for example to DTMF keystrokes

J

JTAPI	Java TAPI, a Java based API for intelligent telephone handling
JVM	Java Virtual Machine, a Java client, which translates and excecutes the Java byte code

L

LAN	Local Area Network, on-premises digital network for workstations, servers and peripherals
LAPD	Link Access Protocol for the D Channel, data link layer subscriber signalling protocol used in the ISDN network
LAR	Local Access Rate, the clock rate of a Frame Relay connection
LATA	Local Access and Transport Area, the operating area of the local NSP. The LATA is used in the US for distinguishing local and long distance phone services
LCD	Liquid Crystal Display, a display to show black and white or colour text and images on a flat screen
LCR	Least Cost Routing, finding a way to route a call to the destination with the lowest tariff
LDAP	Lightweight Directory Access Protocol, an Internet protocol and system for distributed directory services

LDIF	LDAP Information File, a file format for LDAP data replication and retrieval
LLQ	Low Latency Queuing, a cisco queuing solution, which offers low latency for VoIP packets
LFI	Link Fragmentation and Interleaving, a system to fragment large packets on a slow link, to avoid unnecessary delays for real time traffic
LPC	Linear Predictive Coding, an advanced voice coding method, based on voice source modelling
LRQ	Location Request, an RAS request from the terminal to register user presence
LSB	Least Significant Bit, the bit with the lowest weight on a digital word
LSW	Least Significant Word, the four byte word with the lowest weight on a multi-word digital number

M

MAC	Media Access Control, the lower data link sublayer on IEEE/ISO LAN standards
MAN	Metropolitan Area Network, a campus or city wide backbone network to interconnect LANs
MC	Multistation Controller, an MCU component, which controls the conference
MCML PPP	Multi-Class Multilink PPP, standard fragmentation method in PPP links
MCR	Minimum Cell Rate, an ATM traffic parameter
MCS	Multipoint Communications Services, a protocol for multipoint data conferences
MCU	Multipoint Control Unit, an optional H.323 component, which controls the multiparty conferences
MD-5	Message Digest 5, a standard way to count one way hash to be used in user or node authentication
Megaco	Media Gateway Control, a joint ITU-T/IETF standard for gateway control
MG	Media Gateway, the Megaco component, which handles media streams between packet and circuit switched networks
MGC	Media Gateway Controller, the Megaco component, which handles signalling messages between packet and circuit switched networks
MGCP	Media Gateway Control Protocol, a standard for gateway control, nowadays known as Megaco
MIB	Management Information Base, a tree structure description for SNMP managed network elements
MIME	Multipurpose Mail Extension, a way to code a mail attachment type
MinCIR	Minimum Committed Information Rate, the amounth of bandwidth that a Frame Relay PVC gives after receiving a BECN congestion notification
MKI	Master Key Identification, an optional SRTP field

MLPPP	Multilink PPP, a way to use parallel PPP connections for a single connection
MMS	Multimedia Message Service, an add-on solution for sending and receiving short multimedia messages on digital mobile networks
MN	Mobile Node, a host which uses Mobile IP services for roaming
MMUSIC	Multiparty Multimedia Session Control, an IETF workgroup that develops multimedia standards
MO	Managed Object, the subject for network management
MP	Multipoint Processor, an MCU component that processes audio, video and data streams
MP3	MPEG 1 Layer 3, an audio coding system for stereophonic music
MPEG	Motion Pictures Experts Group, an IETF workgroup that develops video coding standards
MPLS	Multiprotocol Label Switching, a routing system where Edge Routers set up paths and mark packets, which are switched quickly by Core Routers based on the label information
MPMLQ	Multipulse Maximum Likelihood Quantisation, an advanced voice coding method, based on waveform coding
MS	Microsoft, a rather large software company
MSB	Most Significant Bit, the bit with the highest weight on a digital word
MSC	Mobile Switching Center, a GSM phone exchange
MSPI	Media Stream Provider Interface, an interface within the TAPI for media streams
MSW	Most Significant Word, the four byte word with the highest weight on a multi-word digital number

N

NAT	Network Address Translation, address translation system on a firewall, which hides internal addresses on the public Internet
NDIS	Network Driver Interface Specification, a generic interface for Network Interface Card drivers
NetBIOS	Network Basic Input Output System, a programming interface for PC networks
NFS	Network File System, distributed file services for UNIX hosts
NIC	Network Interface Card, an internal card plugged on a PC extension slot, that offers LAN connectivity
NMS	Network Management System, the technical facilities to ensure service availability on the network
NNTP	Network News Transfer Protocol, an application layer Internet protocol for electronic News services
NOS	Network Operating System, OS additions, which provide at least user authentication, file and print services for a networked workstation

NSP	Network Service Provider, a company offering telecommunication services
NTP	Network Time Protocol, an application layer Internet protocol, used to carry wallclock time information

O

OAM	Operations, Administration and Maintenance, network management functions
OSI	Open Systems Interconnection, a framework to model any network
OSPF	Open Shortest Path First, a standard link state routing protocol, based on the Dijkstra shortest path first algorithm

P

P	Padding, a field on the RTP header, which indicates that padding is added
PBX	Private Area Branch Exchange, a telephone exchange on customer premises, which connects the local subscribers to the PSTN
PC	Personal Computer, a hardware and software computer system for a single user
PCM	Pulse Code Modulation, a basic voice coding, based on equal interval voice samples and coding of each sample with 8 bits
PCR	Peak Cell Rate, an ATM traffic parameter
PDA	Personal Digital Assistant, a handheld computer offering at least calender, notepad, calculator and spreadsheet applications
PDH	Plesiochronous Digital Hierarchy, the hierarchical digital transmission system, which doesn't provide full synchronisation on the network
PDU	Protocol Data Unit, an encapsulation unit, containing a header and a data field
PER	Packet Encoding Rules, a way to encode ASN.1 data
PHB	Per Hop Behaviour, a way to describe DiffServ service levels
POP3	Post Office Protocol Three, an application layer Internet protocol to retrieve E-mail messages and attachments from the mail server to the workstation
POTS	Plain Old Telephone System, the circuit switched telephone network, which offers connections for analogue telephone sets
PPP	Point to Point Protocol, a standard way to encapsulate frames and packets on point-to-point WAN links
PQ	Priority Queuing, a queuing system
PRI	Primary Rate Interface, the 1,5 or 2 Mbit/s PBX interface to the narrowband ISDN network
PSTN	Public Switched Telephone Network, the public telephone network
PT	Payload Type, a field on the RTP header, which contains information about RTP user data

PTT	Post, Telephone and Telegraph, an old name for a finnish telephone service provider
PTO	Public Telephone Operator, a licenced service provider for telecommunication services
PVC	Permanent Virtual Circuit, a configured fixed virtual circuit, which packets follow on a packet switched network

Q

QCIF	Quarter Common Intermediate Format, 176*144 pixel video picture
QoS	Quality of Service, a set of methods to allocate scared network resources to applications
QSIG	A variant of ISDN D-Channel signalling

R

RADIUS	Remote Authentication Dial In User Service, user authentication for remote dialup users
RAM	Random Access Memory, volatile computer memory component
RAS	Registration, Admission and Status, the terminal to gatekeeper H.323 signalling protocol
RBOC	Regional Bell Operating Company, a Local Exchange Carrier in USA
RCF	Registration Confirmation, an RAS response from the gatekeeper for an approved terminal registration
RDN	Relative Distinguished Name, an identifier for a directory record
RED	Random Early Detection, a congestion avoidance method
RFC	Request for Comment, an Internet Standard with an RFC number, issued by the IETF
RIP	Routing Information Protocol, a standard distance vector routing protocol
RMON	Remote Monitoring, an SNMP MIB for monitoring network traffic remotely
RPC	Remote Procedure Call, a programming interface for distributed computing
RPE-LTP	, a hybrid voice coding system that is used in GSM network
RR	Receiver Report, an RTCP message, used for reception statistics
RRJ	Registration Reject, a negative RAS response from the gatekeeper, indicating that it will not accept terminal registration
RRQ	Registration Request, an RAS request from the terminal to register on a gatekeeper
RSIP	Real Specific IP, a method to pass commands and responses between SIP terminals and servers separated by a firewall
RSVP	Resource Reservation Protocol, an additional network layer protocol, which is used to make reservations for packet flow

RTCP	Realtime Transport Control Protocol, an application layer Internet protocol that provides feedback on RTP transport and identifies conference participants
RTCP-XR	RTCP Extended Report, an RTCP message type
RTP	Realtime Transport Protocol, an application layer Internet protocol, which is used to carry real time data streams
RTSP	Real-Time Streaming Protocol, a SIP protocol for commanding a media player
RWIN	Receive Window, a field on a TCP header

S

SASL	Simple Authentication and Security Layer, a protocol framework for client/server authentication
SCR	Sustainable Cell Rate, an ATM traffic parameter
SDES	Source Description, an RTCP message carrying information about the sender
SDH	Synchronous Digital Hierarchy, the hierarchical digital transmission system, which provides full synchronisation on the network
SDP	Session Discovery Protocol, an Internet standard for multimedia session parameter negotiation
SET	Simple Endpoint Type, a simple H.323 terminal type
SIM	Subscriber Identity Module, a card on a GSM Mobile Station, which identifies the subscriber
SIP	Session Initiation Protocol, an Internet standard for VoIP connection setup signalling
SM	Single Mode, a fiber optic fiber with a very thin core
SMB	Server Message Block, the application layer protocol for file and print services in Windows networks
SMDI	SCSI Musical Data Interchange, an interface between a computer and a electronical musical instrument
SMIL	Synchronized Multimedia Integration Language, a description language for multimedia objects
SMS	Short Message Services, a GSM add-on solution for sending and receiving short text messages on a Mobile System
SMTP	Simple Mail Transfer Protocol, an application layer protocol between Internet mail servers that is used to transport E-mail messages and attachments
SNMP	Simple Network Management Protocol, the network management protocol on the TCP/IP protocol stack
SONET	Synchronous Optical Network, the Northern American version of SDH
SQL	Structured Query Language, an application layer protocol for database queries

SR	Sender Report, an RTCP message, used for transmission and reception statistics
SRTP	Secure Real-Time Transport Protocol, application layer encrypted and authenticated protocol for transporting real-time data
SS#7	Signalling System 7, a common channel signalling system for digital telephone networks
SSCR	Synchronization Source Identifier, the identifier for the terminal on an RTP session.
SSH	Secure Shell, an Internet protocol, which provides secure connections with the help of encryption
STS-1	Synchronous Transport Signal One, the 51,84 Mbit/s basic frame for Northern American. SONET networks. Also called OC-1
STM-1	Synchronous Transport Module One, the SDH basic frame of 155,52 Mbit/s, equal to Northern American OC-3
STM-16	Synchronous Transport Module Sixteen, an SDH frame with 2,48832 Gbit/s bit rate
STM-4	Synchronous Transport Module Four, an SDH frame with 622,08 Mbit/s bit rate

T

TAPI	Telephone API, an API developed by Microsoft for intelligent telephone handling
TCP/IP	Transmission Control Protocol/Internet Protocol, the Internet protocol stack
TFTP	Trivial File Transfer Protocol, an application layer Internet protocol for simple file download
TMN	Telecommunications Management Network, the ITU-T standard for PSTN network management
TOS	Type of Service, a field on the IP V.4 field containing the DSCP code
TRIP	Telephony Routing Information Protocol, a way to locate an H.323 service
TSP	Telephone Service Provider, a company, which provides public telephone services
TSPI	Telephone Service Provider Interface, an interface within the TAPI for telephone services
TTL	Time to Live, a field on the IP header, which is used to discard lost packets

U

UA	User Agent, the SIP component to make and receive IP telephone calls with
UBR+	Unspecified Bit Rate Plus, an ATM traffic class

UCF	Unregister Confirmation, an RAS response from the gatekeeper, confirming the Unregister Request
UDP	User Datagram Protocol, connectionless transport protocol, which offers unreliable transport of a byte stream
UPS	Uninterruptable Power Supply, a device, which filters the mains power and supplies reserve power from batteries during a mains fault
URI	Uniformed Resource Idenfifier, a document or resource identifier, consisting of method or protocol and a hierarchical document identifier
URL	Uniformed Resource Locator, the Web address, consisting of protocol, host, directory and document information. URL is a subset of URI.
URQ	Unregister Request, an RAS request from the terminal to clear the registration on the gatekeeper

V

VLAN	Virtual LAN, a system to configure stations on a switched LAN into separate networks, which cannot communicate directly
VLF	Visitor Location Function, a H.323 database of visiting users, needed for mobility
VoATM	Voice over ATM, a standard way to route RTP voice packets over an ATM cell relaying network
VoFR	Voice over Fram Relay, a standard way to transmit RTP voice packets over a Frame Relay infrastructure
VoIP	Voice over IP, technology to transmit voice and multimedia calls on IP networks
VPN	Virtual Private Network, a method to use public networks to carry confidential traffic encrypted

W

W3C	WWW Consortium, a development consortium for Web interoperability development
WAN	Wide Area Network, wide area private or public computer network
WDM	Wawelength Division Multiplexing, a system to multiplex several digital channels on a single optical trunk transparently
WFQ	Weighted Fair Queuing, a queuing solution
WLAN	Wireless LAN, a local computer network, which uses radio or infrared transmission from the terminal to the access point
WRED	Weighted Random Early Detection, a congestion avoidance method
WWW	World Wide Web, the global network of servers and clients, which uses the HTTP protocol

X

X	Extension, a field on the RTP header, which indicates the existence of an extension header
xDSL	Digital Subscriber Line, a common term for different DSL technologies
XML	Extensible Markup Language, a meta markup language for describing information contents

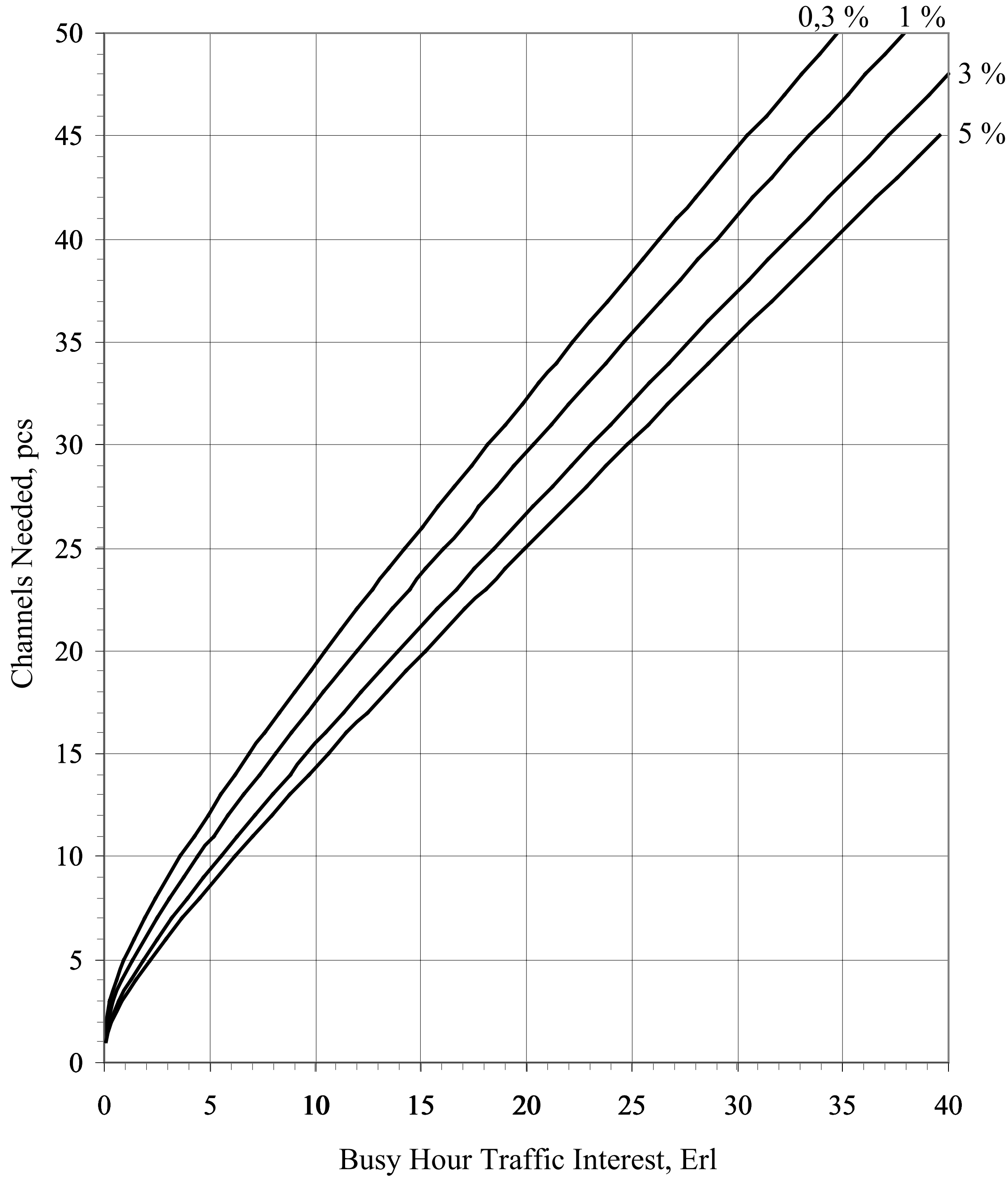
1

10GE	10 Gigabit Ethernet, fast Ethernet like LAN/MAN/WAN technology, offering 10 or 9,95328 Gbit/s data rates

3

3G	Third Generation Mobile Services.
3GPP	Third Generation Partnership Project, an industry consortium to promote interoperability in IP telephony calls in third generation mobile networks

Appendix A: Erlang's First Formula



Appendix B: Voice Bandwidth Usage

Bandwidth usage of a single half duplex channel for the most popular VoIP voice codecs, when RTP data is transmitted on Ethernet, Frame Relay and PPP frames. For full duplex conversations without silence suppression, a bandwidth value equal to the one found in table should be reserved for both directions. With silence suppression, the value given by the table should be multiplied with 0,5 - 0,6 for the average bandwidth usage.

Codec	Network	Codec kbit/s	Sampling ms	Sampling ms	Voice bytes	Padding bytes	Headers bytes	BW kbit/s	w. cRTP kbit/s
G.711	**Ethernet**	64	20		160	0	58	**87,2**	**73,2**
G.711	**Ethernet**	64		30	240	0	58	**79,5**	**70,1**
G.711	**802.1Q Ethernet**	64	20		160	0	62	**88,8**	**74,8**
G.711	**802.1Q Ethernet**	64		30	240	0	62	**80,5**	**71,2**
G.711	**Frame Relay**	64	20		160	0	44	**81,6**	**67,6**
G.711	**Frame Relay**	64		30	240	0	44	**75,7**	**66,4**
G.711	**PPP**	64	20		160	0	46	**82,4**	**68,4**
G.711	**PPP**	64		30	240	0	46	**76,3**	**66,9**
G.723.1	**Ethernet**	6,3	20		16	0	58	**29,6**	**15,6**
G.723.1	**Ethernet**	5,3		30	20	0	58	**20,8**	**11,5**
G.723.1	**802.1Q Ethernet**	6,3	20		16	0	62	**31,2**	**17,2**
G.723.1	**802.1Q Ethernet**	5,3		30	20	0	62	**21,9**	**12,5**
G.723.1	**Frame Relay**	6,3	20		16	2	44	**24,8**	**10,8**
G.723.1	**Frame Relay**	5,3		30	20	0	44	**17,1**	**7,7**
G.723.1	**PPP**	6,3	20		16	2	46	**25,6**	**11,6**
G.723.1	**PPP**	5,3		30	20	0	46	**17,6**	**8,3**
G.729A	**Ethernet**	8	20		20	0	58	**31,2**	**17,2**
G.729A	**Ethernet**	8		30	30	2	58	**24,0**	**14,7**
G.729A	**802.1Q Ethernet**	8	20		20	0	62	**32,8**	**18,8**
G.729A	**802.1Q Ethernet**	8		30	30	2	62	**25,1**	**15,7**
G.729A	**Frame Relay**	8	20		20	0	44	**25,6**	**11,6**
G.729A	**Frame Relay**	8		30	30	2	44	**20,3**	**10,9**
G.729A	**PPP**	8	20		20	0	46	**26,4**	**12,4**
G.729A	**PPP**	8		30	30	2	46	**20,8**	**11,5**

Appendix C: DSCP Values

The DS field on IP v.4 packet (former called TOS) includes the following fields, listed from the Most Significant Bit:

- three bit priority, indicating the default, Class Selector, Assured Forwarding and Expedited Forwarding PHP, and two different values for Class Selector and four values for AF. With the three bits, a total of eight different priority values are coded.

- three bit Drop Precedance, that identifies, individually from priority, the precedance to drop the packet in question during a congestion. Three Drop Precedance values are used, namely low (010), medium (100) and high (110).

- two bit Explicit Congestion Notification, that will, in future, carry indication of a congestion situation. Today, the ECN field is not used, and 00 is always inserted as the ECN value.

Priority	Priority value	Drop Prec.	DSCP	ECN	DS Field binary	DS Field hex.
Default	000	**N/A**	000 000	00	000 000 00	00
AF Class 1	001	**Low**	001 010	00	001 010 00	28
AF Class 1	001	**Medium**	001 100	00	001 100 00	30
AF Class 1	001	**High**	001 110	00	001 110 00	38
AF Class 2	010	**Low**	010 010	00	010 010 00	48
AF Class 2	010	**Medium**	010 100	00	010 100 00	50
AF Class 2	010	**High**	010 110	00	010 110 00	58
AF Class 3	011	**Low**	011 010	00	011 010 00	68
AF Class 3	011	**Medium**	011 100	00	011 100 00	70
AF Class 3	011	**High**	011 110	00	011 110 00	78
AF Class 4	100	**Low**	100 010	00	100 010 00	88
AF Class 4	100	**Medium**	100 100	00	100 100 00	90
AF Class 4	100	**High**	100 110	00	100 110 00	98
EF	101	**N/A**	101 110	00	101 110 00	b8
Class Selector	110	**N/A**	110 000	00	110 000 00	c0
Class Selector	111	**N/A**	111 000	00	111 000 00	e0