Introduction to Communication Networks

Ernst Nordström

Department of Economics and Social Sciences, Dalarna University
SE-781 88 Borlänge, Sweden
eno@du.se

December 5, 2008

Contents

1 Network services **5**

1.1 Service classification . . . 5

1.2 Service description on the packet level . . . 7

1.3 Service description on the connection level . . . 9

2 Principles of communication networks **11**

2.1 Network organization . . . 11

2.2 Core network . . . 12

2.3 Access network . . . 15

2.4 The seven layer OSI model . . . 16

2.4.1 Communication protocols . . . 16

2.4.2 Application layer . . . 16

2.4.3 Presentation layer . . . 17

2.4.4 Session layer . . . 17

2.4.5 Transport layer . . . 17

2.4.6 Network layer . . . 18

2.4.7 Data link layer . . . 19

2.4.8 Physical layer . . . 20

3 Internet **21**

3.1 New applications and QoS requirements . . . 21

3.2 Network organization . . . 21

3.3 Service providers . . . 22

3.4 Overlay networks . . . 22

3.5 Network security 23
3.6 QoS architecture 25
3.6.1 Flow aggregation 25
3.6.2 Service level agreement 26
3.6.3 Resource reservation 27
3.6.4 Signaling for resource reservation 27
3.7 The five layer TCP/IP model 27
3.7.1 Application layer 27
3.7.2 Transport layer protocols 30
3.7.3 Network layer protocol 30
3.7.4 Data link layer protocols 33
3.7.5 Physical layer protocols 34
3.8 Internet Engineering Task Force 35

4 History of communication networks **37**
4.1 Telephone networks 37
4.2 Internet 38
4.3 Data networks 38
4.4 Wireless networks 39
4.5 Multi-service networks 39

Chapter 1

Network services

1.1 Service classification

Three types of services are defined in Recommendation I.210 by International Telecommunication Union (ITU):

1. Bearer services;

2. Teleservices;

3. Supplementary services.

Bearer services provide the means of conveying information (speech, data, video etc.) between users in real-time without altering the content of the message. Bearer services are implemented by layers 1 to 3 of the OSI model. Teleservices combine the transportation function with information-processing functions implemented by OSI layers 4 to 7. Teleservices may be grouped into single media (e.g. speech) and multimedia services. There are six specified categories of multimedia services specified by ITU Recommendation F.700:

1. Multimedia conference services;

2. Multimedia conversational services;

3. Multimedia distribution services;

4. Multimedia retrieval services;

5. Multimedia messaging services;
6. Multimedia collection services.

The categories have the following meaning:

Conference services provides information exchange in real time between participating multiple end points. Examples of conference services include video conferencing.

Conversational services provides information exchange in real time between participating two end points. Examples of conversational services are video telephony and and high speed data transmission.

Distribution services are further classified by whether they allow the user to control the presentation or not. **Distribution services without presentation control** provide a continuous flow of information from a central source to an unlimited number of receivers connected to the network. The user cannot control the start and order of presentation of the broadcasted information. Examples are broadcast services for television and audio programmes. **Distribution services with presentation control** distribute information from a central source to a large number of users. The information is provided as a sequence of information entities (e.g. frames) with cyclic repetition. So, the user has the ability of individual access to the cyclical distributed information and can control start and order of presentation. One example of this service is full channel broadcast videography.

Messaging services offer communication between individual users via storage units with store-and-forward, mailbox and/or message handling. Examples of broadband messaging services are message handling services and mail services for moving pictures (films), high resolution images and audio information.

Retrieval services allow the user to retrieve information stored in information centers provided for public use. Examples of broadband retrieval services are retrieval services for film, high resolution image, audio information, and archival information.

Collective services provide for the transfer of information from multiple senders to one receiver with the information sink being the controlling entity.

Examples of teleservices are telephony, teletex and videotex.

Supplementary services supplements a basic telecommunication service (i.e. teleservice). Examples of supplementary services include the following: calling/connected line identification presentation/restriction, call forwarding (on subscriber busy, no reply, non reachable, or unconditional), call waiting, call hold, multiparty service, closed user group, advice of charge, and barring outgoing/incomming/roaming calls.

1.2 Service description on the packet level

The service contract negotiated as connection set up between the user and network contains a specification of the traffic and *Quality of Service* (QoS) at the packet level of the connection. The traffic parameters describe the characteristics of the source as follows:

- Peak packet rate (PPR): PPR is the maximum allowable rate at which packets can be transported along a connection.
- Sustainable packet rate (SPR): SPR is the average allowable, long-term packet transfer rate on a specific connection.
- Maximum burst size (MBS): MBS is the maximum allowable burst size of packets that can be transmitted contiguously on a particular connection.
- Minimum packet rate (MPR): MPR is the minimum allowable rate at which packets can be transported along a connection.

The declared traffic parameters are enforced at the entry to the network to ensure that the service contract is not violated.

The objective performance of the network service can be measured by QoS metrics. The QoS describes the network's ability to transport packets between boundary nodes and include the following parameters:

- Packet loss probability: ratio of the number of lost packets to number of offered packets.
- Maximum packet transfer delay: $(1 - \alpha)$ quantile of the distribution of time for packet transfer over the network.
- Packet delay variation: difference between the maximum and the minimum packet transfer delay.
- Throughput: number of successfully transfered bits per time unit as measured at the egress node.

Single packet losses will often be compensated for by a codec - but a burst of packet loss will result in broken speech or patchy video. The loss and delay and requirements of different services can vary substantially. Interactive voice and video services are sensitive to delay but can tolerate some loss. Data is sensitive to loss but can tolerate some delay.

The QoS requirements for the voice service is:

- ≤ 150 ms of one-way latency from mouth to ear (per ITU G.114 standard);
- ≤ 30 ms delay variation;
- ≤ 1 percent packet loss.

The QoS requirements for streaming video, such as IP multicast, executive broadcasts, and real-time training activities, are as follows:

- ≤ 5 s of latency;
- No significant delay variation requirements;
- ≤ 2 percent packet loss.

The QoS requirements for video conferencing can be applied as either a one-to-one capability or a multipoint conference:

- ≤ 150 ms of one-way latency from mouth to ear (per ITU G.114 standard);
- ≤ 30 ms delay variation;
- ≤ 1 percent packet loss.

The subjective performance as perceived by the user is measured by *Quality of Experience* (QoE) metrics. QoE defines the cumulative effect on subscriber satisfaction of all imperfections affecting the service. QoE is a often referred to in telephony and streaming video applications. This definition includes the human in the assessment and demands an appropriate weighting of diverse defects such as response time, interrupts, noise, cross-talk, loudness levels, frequency response, noticeable echos, and also includes Grade of Service. With the advent of digital networks new types of impairments, such as the effect of bit errors in codecs, arose together with a tendency to express QoS in terms of engineering parameters that can be measured objectively, eliminating the uncertainty of human subjectivity. This definition resembles the Mean Opinion Score (MOS) value, which is a subjective quality measure that can be predicted based on objective performance measures.

1.3 Service description on the connection level

The network is designed so that it offers sufficient Grade of Service (GoS) for the traffic offered at the connection level. Each ingress node of the core network is offered connections from a set of classes. Each class is characterized by

- Origin-destination node pair;
- Connection request inter-arrival time distribution;
- Connection holding time distribution;
- Source traffic parameters;
- Charging/pricing rule.

The GoS metrics include

- Connection blocking probability;
- Mean connection setup delay;
- $(1 - \alpha)$ quantile of connection setup delay distribution.

Chapter 2

Principles of communication networks

2.1 Network organization

The role of a communication network is simple: to transport information reliably between end systems. To accomplish this task a complex machinery of electronic hardware, optical fibers, and computer software is needed. The essential functionality of a network is its ability to route information to the appropriate destination.

Communication networks are classified into voice, data and integrated networks. Voice networks have traditionally provided more intelligent network services than data and integrated networks. Data and integrated networks are based on the end-to-end principle which rely on end systems to enhance the service provided by the network. In principle this means that recovery from information transfer errors is initiated by the end systems and that the media coding/compression scheme may be adaptive to available network capacity.

Communication networks consists of a core network that interconnects end systems via access networks. The core network is implemented by a (i) wired network based on optical transport equipment and optical fibers, or (ii) wireless network based on satellites. The access networks have traditionally been based on wired technology such as coaxial and twisted pair cables. Wireless access networks, based on radio communication, play a dominant role in modern communication systems. Private core networks offers services to a restricted set of organizations. Public core networks offers services to everybody and charge a fee for using the network. Public core networks are classified as Public Switched Telephone Network (PSTN), Public Switched Data Network (PSDN), or Public Switched Integrated Network (PSIN).

2.2 Core network

The virtual network (VN) concept is commonly used in PSTNs and PSINs to provide efficient resource utilization and simple resource management in the core network. In its basic form the VN concept allows separation of capacity to individual VNs. Internet uses overlay networks and virtual private networks (VPNs) which are related to the VN concept but do not allow allocation of separate capacity to individual VNs. These techniques are based on packet tunneling principles and are used to enhance the communication services (e.g. peer-to-peer networking, security, QoS routing). Traffic engineering (TE) is used to design and optimize the VN topology and VN link capacities. The topology of the VN may be different from the physical network topology. A VN link defines a path (consisting of one or more physical links) between two VN nodes.

The network contains a TE controller that is responsible for traffic and capacity management and network planning in the core network. The TE controller can be centralized or distributed among the network nodes. Connection admission control, explicit routing, and VN and PN design are the responsibility of the TE controller.

Core networks have a flat or hierarchical network design. The latter represents the topological configuration to be expected with multiarea or multiautonomous (multi-AS, or multidomain) networks. The flat network model leads to better network utilization since

- Path selection is more constrained in a hierarchical network because some shortest path between nodes are excluded by the hierarchical rules imposed.
- Limited visibility in selecting paths in a hierarchical network is caused by the aggregation of network state information.

Fixed routing for hierarchical networks is based on a set of routing rules with the objective to carry as much traffic as is economically feasible on direct links between pairs of nodes low in the hierarchy. Best effort routing in Internet deploys fixed routing which selects the path with smallest number of hops (shortest path).

Dynamic routing for flat networks use a routing rule that is sensitive to the current time, network state or blocking event. Time-dependent dynamic routing use different alternative routing rules for different time periods. State-dependent dynamic routing selects paths based on the network state (number of calls in service on each link). Event-dependent routing offers the connection to the direct path and if this path is busy it tries an alternative path. If also the alternative path is busy the connection request is blocked. This event causes the system to randomly select a new alternative path which is used for the next connection request. QoS routing in Internet deploys a state-dependent dynamic routing rule that selects the path with the smallest number of hops with maximal available bandwidth (shortest widest path).

The PSTN is implemented by circuit switching while PSDN and PSIN are implemented by packet switching. In contrast to circuit-switching technology, packet switching tends to have lower switching node cost relative to transport, which leads to sparse VN topologies and relatively high-capacity VN links. Sparsely connected networks tend to minimize transport cost. Having few links tends to concentrate the network load, raising the load per link and the link capacity requirement. Circuit-switched PSTNs are typically highly interconnected by VN links (perhaps $> 70\%$ connected), whereas packet-switched PSDNs and PSINs are typically more sparsely connected (perhaps < 20 % connected).

The packet-switched network is built of packet routers [1] and optical transmission equipment. The packet routers consists of a switch core and multiple input and output controllers. Queueing of packets is possible at the input/output controllers, see Figure 2.1. Some routers use central queueing in the core. Most routers are able to switch the packets with no internal blocking in the core. The input controllers have queues to store packets waiting for switching to an output link. The output controllers have queues to store packets waiting to be scheduled for transmission.

Many connections share a communication output link. The packets within each connection arrives to the router in a random fashion since users generate packets on demand. Therefore, the rate of the aggregate packet arrival stream may momentarily exceed the output link capacity. During these periods the queue in the buffer will increase, and if the rate level persists the buffer will saturate forcing excess traffic to be discarded. The queue length decreases as long as the aggregate packet arrival is less that the output link capacity.

The network packets are broken up into smaller pieces and transported as frames on the links between the routers. The frames are data link frames in case the router is connected to a wired LAN such as IEEE 802.3 (Ethernet) or a wireless LAN such as IEEE 802.11 (WiFi). In case the router is connected to a WAN, the data link layer is sometimes considered obsolete, in which case the network packets are mapped directly onto physical layer frames.

[1] In the literature, the term “router” or “gateway” is used in an internetworking environment, while “label switching router” and “switch” is used in the context of MPLS and ATM networks, respectively. In this document we refer to the switching elements as “routers”

Deterministic multiple access (TDMA, FDMA, CDMA, WDMA) is used by physical core network by allocating different frequencies, time slots, codes or wavelengths to different users.

The PSIN solution provides economy of scale by using a single network infrastructure for all services which access the network via a common host-network interface. Realizing the PSIN by a packet-switched network allows the use of statistical multiplexing by taking advantage of that connections sharing the same links often have non-overlapping peak rate periods. Statistical multiplexing allows efficient network utilization and is the main advantage of packet switching over circuit switching.

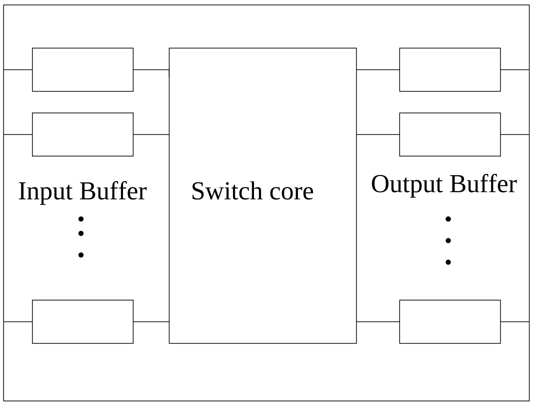

Figure 2.1: Anatomy of a packet switch/router

Interactive multimedia services with loss and delay requirements calls for careful management of network resources. Preventive control mechanisms forms the basis for traffic control in integrated networks. Traffic enforcement and connection admission control are part of preventive traffic control which aims at keeping the risk of network congestion within tolerable limits. Services that tolerates some delay and throughput variability can be managed by reactive flow and congestion control.

By adopting the notion of equivalent bandwidth, TE on the connection level in packet-switched and circuit-switched networks becomes equivalent. The equivalent bandwidth is a value between the sustainable (mean) rate and the peak packet rate. The equivalent bandwidth is based on statistical analysis of the source traffic behaviour. The connection's equivalent bandwidth is computed from the source traffic parameters and QoS requirements of all connections sharing the same path/links. The network should allocate a capacity that is equal to the equivalent bandwidth to maintain the QoS of the connections. More stringent QoS requirements means a larger equivalent bandwidth.

An important issue is the effectiveness and efficiency of the TE mechanisms. Effectiveness is measured in terms of proximity to the optimal TE solution in terms of QoS, GoS and operator profit, i.e, revenue from customer charges minus total network cost. Today, TE finds it practical use in the regional domain of Internet, i.e. in the shared network betweeen the local exchange and the backbone network. In the backbone domain packet loss and queueing delays are avoided by over provisioning of network capacity. An efficient TE solution in the regional network will result in fewer rejected connection requests and will increase the revenue.

2.3 Access network

Access networks are of the broadcast type. Many end systems (stations) share a common channel or link by using some multiple access scheme providing either deterministic access or random access. Deterministic access schemes gives guarantees on fixed throughput and delay and are suitable for real-time services. Random access schemes are not able to guarantee a certain throughput or delay. Resources can not be reserved in advance by connection admission control so this access scheme is suitable for non-real-time services.

Deterministic multiple access (FDMA, TDMA, CDMA) is used by wireless access networks offering real-time services (e.g. cellular networks, IEEE 802.16 WMAN, HIPERLAN2). TDMA and FDMA is a type of TDM and FDM where instead of having one transmitter connected to the receiver there are multiple transmitters. CDMA is always used in combination with Frequency Divison Duplex (FDD) or Time Division Duplex (TDD), i.e. a given frequency channel may be used for CDMA independently of signals on other frequency channels. TDMA is always used in combination with FDD.

Random multiple access is used by networks offering non-real-time services. The concept listen during transmission, used by wired Ethernet, can not be used in wireless networks due to the nature of the channel. The concept listen before transmitting is used by wireless networks offering non-real-time services. The concept listen before transmitting is used to minimize the risk of simultaneous transmission of many users. Some wireless networks such as IEEE 802.11 WLAN and IEEE 802.15 WPAN offer hybrid multiple access with one portion of the channel capacity devoted to deterministic multiple access and one portion devoted to random multiple access.

2.4 The seven layer OSI model

2.4.1 Communication protocols

The International Standards Organization (ISO) proposed in 1984 the Open Systems Interconnection (OSI) reference model for layered organization of communication protocols. A *protocol* is a set of rules defining how information should be exchanged between two entities. Each layer of the OSI model has its own protocol. The details of the protocol on a certain layer is hidden for other layers. Layer $n + 1$ use the service of the layer n immediately below it. The entities comprising the corresponding layers on different machines are called *peers*. In other words, it is the peers that communicate using the protocol. Between each pair of adjacent layers there is an *interface*. The interface defines which primitive operations and services the lower layer offers to the upper layer. The set of layers and protocols is called *network architecture*. Neither the details of the protocol implementation nor the specification of the interface are part of the network architecture. The set of protocols used by one system with one protocol per layer is called *protocol stack*.

2.4.2 Application layer

The application layer is a end-to-end protocol in the OSI reference model. It is only implemented by the hosts, not inside the network. Users access the network through fixed or mobile end systems that run some application. Multimedia applications integrates multiple media in a single application software. The users are presented information in the form of text, images, audio and video. Applications can be interactive such as conversational voice and video. Such applications have stringent requirements on the QoS. Applications such as voice/video messaging, streaming audio/video, fax have also stringent requirements on transfer reliability but can tolerate longer delays. Applications such as command/control (e.g. interactive games), transactions (e.g. e-commerce, web browsing, e-mail), messaging downloads (e.g. file transfer), and background transactions (e.g. Usenet) have different requirements on transfer delay but require zero information loss. Other issues at the application layer include synchronization between different media such as lip synchronization for video telephony, and security, such as secure transfer of files, electronic mails and WWW documents.

2.4.3 Presentation layer

The presentation layer is a end-to-end protocol in the OSI reference model. It is, among other things, concerned with the syntax and semantics of the information transmitted. A typical example is encoding data in standard agreed upon way. Most user programs do not exchange random binary strings. They exchange things such as people's names, dates, amounts of money, and invoices. These items are represented as character strings, integers, floating-point numbers, and data structures composed of several simpler items. In order to make it possible for computers with different representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used "on the wire". The presentation layer manages these abstract data structures and converts from the representation used inside the computer to the network standard representation and back.

The presentation layer also is responsible for coding and compression of images, audio and video. Compression is used to reduce the bandwidth requirement of multimedia packet streams. Compression works by reducing the redundancy in the information flow.

2.4.4 Session layer

The session layer is a end-to-end protocol in the OSI reference model. It allows users on different hosts to establish *sessions* between them. A sessions allows ordinary data transport, as does the transport layer, but it also provides enhanced services useful in some applications. A session might be used to allow a user to log into a remote timesharing system or to transfer a file between two hosts. One of the services of the session layer is to manage *dialogue control*. Sessions can allow traffic to go in both directions at the same time, or in only one direction at a time. A related session service is *token management*. For some protocols, it is essential that both sides do not attempt the same operations at the same time. To manage between activities, the session layer provides a token that can be exchanged. Only the side holding the token may perform the critical operation. Another service is *synchronization*. The session layer may provide a way to insert checkpoints into the data stream, so that after a system crash, only the data transferred after the last checkpoint have to be repeated.

2.4.5 Transport layer

The transport layer is a end-to-end protocol in the OSI reference model. Its main purpose is to facilitate reliable transport of transport protocol data units called segments between hosts. Transport protocols enhances the unreliable service of the network layer. Its functions include error detection, error recovery, flow and congestion control, user process identification, and security. Some transport protocols do not provide error recovery.

Error detection is based on giving each packet a sequence number, in order to detect lost packets, duplicate packets, and packets out of sequence. Bit errors can be detected by a checksum.

Error recovery is implemented by forward error correction (FEC) or backward error correction (BEC). FEC is suitable for real-time services which have no time for retransmissions. The mechanism is based on error correcting codes such as parity and Reed-Solomon codes. BEC is suitable for non-real-time service and retransmission of corrupt or lost packets. The mechanism relies on packet timers, positive and/or negative acknowledgments.

Flow control adapts the sender's transmission rate to the available storage and processing capacity at the receiver. The error recovery mechanism use special control packets to inform the sender about the desired transmission rate.

Congestion control adapts the sender's transmission rate to the available capacity in the network. The transmission rate feedback is normally carried by the same control packets as the error recovery and flow control mechanism.

User process identification selects which application software process should be end point of the transport connection.

Security deals with the privacy (blocking snooping and packet sniffing), and integrity (blocking message alteration) of messages, user authentication of user identities (blocking identify spoofing) and authorization of user access (verifying access rights).

If the transport connection requires high throughput, the transport layer might create multiple network connections to improve throughput. On the other hand, if creating or maintaining a network connections is expensive, the transport layer might multiplex several transport connections onto the same network connection.

2.4.6 Network layer

The network layer is responsible for functions such as addressing, fragmentation and reassembly, connection admission control, routing, error detection, error recovery, flow control, congestion control, traffic enforcement, traffic shaping, packet scheduling, network design, charging, pricing and security.

Addressing selects the destination and facilitates the routing och packets. Addresses are either local to a link, as in ATM and MPLS, or global to the network, as in IP. The routing tables in the routers contains an entries with pairs of address and output link IDs.

Fragmentation breaks a large protocol data unit up into small pieces that does not violate the maximum transmission unit on the data link layer.

Reassembly collects the fragments into a larger protocol data unit before delivery to the transport layer.

Connection admission control accepts/rejects connection requests so that (1) the QoS is acceptable for all network connections, (2) the GoS is acceptable for all network classes, and (3) the profit is maximized for the network operator.

Routing selects an route from the origin node to the destination node subject to the same optimization objective as connection admission control. With a connectionless network layer (e.g. IP), each packet within a session may choose its own path to the destination. With a connection-oriented network layer (e.g. MPLS, ATM), each packet follow the same path as the other packets within the connection.

Traffic enforcement monitors the traffic parameters and drops excessive packets or marks them as low priority susceptible for packet loss when the network becomes congested.

Traffic shaping controls the packet rate so that the actual connection traffic conforms with the declared traffic parameters.

Packet scheduling determines the order of packet transmission on the output link of the router.

Network design finds the topology and link capacities from an optimization procedure with the objective to maximize the revenue or minimize the network links costs subjects to absolute or relative GoS constraints.

Charging determines the scheme for accounting of network usage.

Pricing determines the monetary charge for each call/session.

2.4.7 Data link layer

The data link layer takes the raw transmission facility and transforms it into a line that appears free of undetected transmission errors to the network layer. The data link layer performs framing, which collects the bits from the physical layers into frames, typically contain 10s to 1000s of bytes. The framing can be done with a special bit sequence that detects start and end of the frame. The data link layer also deals with error detection, error recovery and flow control, and security.

Broadcast networks have two additional issues in the data link layer: how to control access to a shared channel and how to address the hosts attached to the shared channel. The access control deals with issues such as bandwidth and buffer scheduling. A special sub layer of the data link layer, the medium access control (MAC) sub layer, deals with this problem.

2.4.8 Physical layer

The physical layer is concerned with transmitting raw bits over a communication channel. The design issues large deal with mechanical, electrical, and procedural interfaces, and the physical transmission medium, which lies below the physical layer. Issues include reliable transfer of bits, modulation of the signal, multiple access, bit voltage levels, time duration of a bit, how many pins the network connector has, and what each pin is used for. A final issue is security, e.g. detection of wiretapping.

Chapter 3

Internet

3.1 New applications and QoS requirements

The Next Generation Internet (NGI) will offer a rich set of applications with different performance requirements of network service. Applications such as voice over IP, IP television, video conferencing, distance learning, instant messaging, presence information, community services, multipart gaming, collaborative whiteboards will come to their full right when Internet supports QoS at full scale. New applications to be invented in the future that will make full use of the enhanced QoS capabilities.

Internet has traditionally offered best-effort service with no guarantees on successful or timely delivery of data. Some network domains are currently being upgraded with QoS capabilities, requiring modification of the traffic management software in the network nodes. The NGI will offer services with guarantees on limited loss, delay and delay-variation of data transfer.

3.2 Network organization

The Internet can be viewed as a collection of interconnected routing domains also referred to as autonomous systems. Each *routing domain* is a group of nodes (routers, switches and hosts), under a single (technical) administration, that share routing information and policy. The domains are organized in an hierarchy with three levels: backbone service providers, regional service providers, and organization (e.g. university or company). Each routing domain can be classified as either a *stub* or *transit* domain. A stub domain carries packets to and from local hosts. A transit domain passes traffic between other networks in addition to carrying traffic for its own hosts.

3.3 Service providers

Internet service providers (ISPs) reach the Internet via settlement free connections (*peering*) or buys wholesale Internet bandwidth (*IP transit*), from other ISPs. Pricing for IP transit is based on flat rate or usage-based model. The flat rate model gives a fixed price per megabit per second per month basis. The usage-based model consists of a committed part that is fixed and a variable part that depends on the volume (e.g. 95 percent quantile) of transmitted and received data.

ISPs are classifies by the Tier network hierarchy:

- Tier 1 networks peers with every other network to reach the Internet.
- Tier 2 network peers with some networks, but still purchases IP transit to reach some portion of the Internet.
- Tier 3 networks solely purchases transit from other networks to reach the Internet.

A multihomed customer can reach the Internet via several ISPs providing backup and load-sharing capabilities. A single-homed customer is dependent on the peering and IP transit agreements of its ISP to reach the other customers in the network.

3.4 Overlay networks

An *overlay network* are used to enhance the communication service provided by Internet. An overlay network is a computer network which is built on top of another network. Nodes in the overlay can be thought as being connected by virtual or logical links, each of which corresponds to a path, perhaps through many physical links, in the underlying network. Overlay networks can provide solutions for logical peer-to-peer networking, QoS routing, multicast, intelligent addressing etc. Peer-to-peer networking are common for file sharing of music and movies. QoS routing improves the loss and delay performance of standard best effort routing. Multicast sends packets to a subset of all subscribers. Intelligent addressing use distributed hash tables to route messages to a node through a specified file, whose IP address is not known in advance.

Previous proposals such as IntServ, DiffServ, and IP multicast have not seen wide acceptance because they require modification of all routers in the network. On the other hand, an overlay network can be incrementally deployed on end-hosts running the overlay protocol software, without cooperation from ISPs. The overlay has no control over how packets are routed in the underlying network between two overlay nodes, but it can control, for example, the sequence of overlay nodes a message traverses before reaching its destination.

3.5 Network security

The original Internet goal that anyone could send a packet to anyone was the root of the extraordinary growth observed in the mid-1990s. To quote Tim Berners-Lee (who coined the term hypertext in 1965) “There’s a freedom about Internet: As long as we accept the rules of sending packets around, we can send packets containing anything anywhere.”. As with all freedoms, however, there is a price. It’s trivial to forge the origin of a data packet or of an e-mail message, so that the vast majority of traffic on the Internet is unauthenticated, and the notion of identity on the Internet is fluid. Over the past 10 years, spam, fraud, and denial-of-service attacks have become significant social and economic problems.

Organizations also firewalls to attempt to isolate themselves, filtering to eliminate unwanted or malicious traffic, and virtual private networks to cross the Internet safely. A firewall sits between a remote user’s workstation or client and the host network or server. As the user’s client establishes the communication with the firewall, the client may pass authentification data to an authentification service inside the perimeter. A packet filter is a host-based or appliance-based application, which work on OSI layer 3 or 4, and blocks or allows network traffic based on a set of rules defined by the administrator. Modern packet filters can filter traffic based on many attributes like source IP, source port, destination IP or port, destination service like WWW or FTP. They can filter based on protocols, domains name of source, and many other attributes. A Virtual Private Network (VPN) is a private communications network used for secure communication over a public network such as Internet. VPNs can be cost effective and secure way for different corporations to provide users to the corporate network and for remote networks to communicate with each other across the Internet. VPN connections are more cost-effective than dedicated private lines; usually a VPN involves two parts: the protected or “inside network”, which provides physical and administrative security to protect the transmission; and a less trustworthy,”outside” network or segment (usually through Internet). VPNs use cryptographic tunneling protocols (e.g. IPsec, SSL/TLS, PPTP, L2TP) to provide secure communication.

The common solution to the security problem is to identify and authenticate the person or system you are communicating with, authorize certain actions accordingly, and if needed, account for usage.

The term of art is AAA (Autentfication, Authorization, Accouting).

IETF protocols such as EAP (Extensible Authentification Protocol) and RADIUS (Remote Authentification Dial-In User Service) are used to mediate AAA interactions. This form of AAA, however, authenticates the user only as a sender and receiver of IP packets, and is isn't used at all where free service is provided (e.g., in a coffee shop).

Cryptographic authentification is a powerful tool. Just as it can be used to verify financial transactions, it can in theory be used to verify any message on the Internet. Why, then, do we still have spoofed e-mail and even spoofed data packets?

For individual data packets, there is a solution known as IPsec (IP security), which is defined in a series of IETF specifications (but not universally) implemented. It follows the basic Internet architecture known as the end-to-end principle: Do not implement a function inside the network that can be better implemented in two end systems of a communication. For two systems to authenticate (or encrypt) the packets they send to each other, they have only to use IPsec and to agree on the secret cryptographic keys. So why this not in universal usage? There are at least three reasons:

- Cryptographic calculations that time during the sending and receiving of every packet. This overhead is not always acceptable except for very sensitive applications.

- Management of cryptographic keys has proved to be a hard problem, and usually requires some sort of preexisting trust relationship between the parties.

- Traversing firewalls and network address translators add complexity and overhead to IPsec.

For e-mail messages, mechanisms for authentication or encryption of whole messages have existed for years (known as S/MIMI and PGP). Most people don't use them. Again, the need for a preexisting trust relationship appears to be the problem. Despite the annoyance of spam, people want be to able receive mail from anybody without prior arrangement. Operators of Internet services want to receive unsolicited traffic from unknown parties; that's how they get new customers: A closed network may be good for some purposes, but it's not the Internet.

It's worth understanding that wheres normal end users at worst send malicious traffic (such as denial-of-service attacks, viruses, and fraudulent mail), an ISP can in theory spy on or reroute traffic, or make one server simulate another. A hardware or software maker can in theory insert "back doors" in a product that would defeat almost any security or privacy mechanism. Thus, we need trustworthy service providers and manufactures, and we must be very cautious about downloaded software.

To summarize the challenges in this area:

- How can identity be defined, authenticated, and kept private?
- How can trust relationships be created between arbitrary sets of parties?
- How can cryptographic keys be agreed upon between the parties in a trust relationship?
- How can packet origins be protected against spoofing at line speed?
- How can we continue to receive messages from unknown parties without continuing to receive unwanted messages?

IETF is currently working on protocols for key exchange over Internet and spam prevention. These efforts have resulted in the IKEv2 standard (Internet key exchange, version 2) and the DKIM specification (Domain Keys Identified Mail). If successful, DKIM will allow a mail-sending domain to take responsibility, using digital signatures, for having taken part in the transmission of an e-mail message and to publish ”policy” information about how it applies those signatures.

3.6 QoS architecture

IETF has proposed Differentiated Services (DiffServ) as the QoS architecture for Internet. QoS service is offered by the premium service model and the assured service model. The *premium model* defines the *Expedited Forwarding* (EF) class which gives quantitative (absolute) statistical QoS guarantees. The *assured model* defines the *assured forwarding* (AF) class that provides qualitative (relative) QoS guarantees in the form of loss priorities.

3.6.1 Flow aggregation

DiffServ handles the resources in a fashion that is still is manageable when the number of flows gets very large. The scalability is achieved by avoiding management of per-flow states and per-flow packet scheduling. Instead flows from the same service class are grouped into behaviour aggregates that experiences the same per-hop-behavior (PHB). The flows from a service class that share a ingress or egress node are enforced by the same traffic conditioning rule. Inside the network, flows from the same class that share an output link in a router also gets the same scheduling treatment and therefore experiences similar per-node QoS. The flows from the same class that are offered to the same ingress-egress node pair receives similar end-to-end QoS. Before a packet enters a DiffServ domain, the IP packets is marked by the end-host or the first-hop router according to the service quality the packet required and entitled to receive. Within the DiffServ domain, each router needs to look at contents of the IP header or MPLS header to decide the proper treatment for the packet.

A DiffServ domain that is a contiguous set of DiffServ nodes that have implemented the same PHB mechanisms and operate with a common service provisioning policy set. A DiffServ region is a set of one or more DiffServ domains. DiffServ regions are capable of supporting differentiated services along paths which span domains within the same region.

3.6.2 Service level agreement

In order for a customer to receive differentiated services from its Internet Service Provider (ISP), it must have a service level agreement (SLA) with its ISP. The SLA may specify packet classification and re-marking rules and may also specify traffic profiles and actions to traffic streams which are in- or out-of-profile.

Traffic conditioning is done at ingress and egress boundary nodes of the DiffServ domain. Traffic conditioning performs metering, shaping, policing and/or re-marking to ensure that the traffic entering the DiffServ domain conforms to the rules specified by the traffic conditioning agreement.

The service-level specification (SLS) is part of the SLA. The contents of the SLS include the essential QoS-related parameters, including scope and flow identification, traffic conformance parameters, and service guarantees. Specifically, the traffic conformance parameters include five parameters:

- Peak rate p [bytes/s],
- Sustainable rate r [bytes/s],
- Maximum burst size b [bytes],
- Minimum policed unit m [bytes],
- Maximum packet size M [bytes].

3.6.3 Resource reservation

The bandwidth broker (BB) is a centralized or decentralized agent that has sufficient knowledge of resource availability and network topology to makes decisions on traffic and capacity management and network planning in its own domain. In its intra-domain role, the BB sends configuration parameters to the domain's routers. In its inter-domain role, a bandwidth broker establish bilateral agreements with neighbor domains. End-to-end QoS is provided by the concatenation of these bilateral agreements across domains, together with adequate intra-domain resource allocation.

3.6.4 Signaling for resource reservation

End hosts may use RSVP signaling within interact with a BB in the DiffServ domain in order to make resource reservations. RSVP was developped for the Integrated Services (IntServ) QoS framework, but has also been modified to fit DiffServ. IntServ manages the flows on an individual basis rather instead on an aggregate basis and is not a suitable QoS framework for Internet domains.

3.7 The five layer TCP/IP model

The TCP/IP reference model forms the basis for the global Internet. It was first defined by Cerf and Kahn in 1974. Compared to the ISO OSI reference model, the TCP/IP reference model contains fewer layers. The session and presentation layers are not present in the TCP/IP model. Instead these layers are incorporated in the TCP/IP application layer.

3.7.1 Application layer

The protocols at the application layer include:

- **DHCP**: Dynamic Host Configuration Protocol is a set of rules used by a host or router to allow the device to request and obtain an IP address from a server which has a list of addresses available for assignment.

- **DNS**: Domain Name Service stores and associates many types of information with domain names, but most importantly, it translates domain names (computer hostnames) to IP addresses. It also lists mail-exchange servers accepting e-mail for each domain.

- **FTP**: File Transfer Protocol is commonly used to exchange files over any network that supports the TCP/IP protocol.

- **HTTP**: Hypertext Transfer Protocol is a method used to transfer on the World Wide Web. Its original purpose was to provide a way to publish and retrieve HTML pages.

- **IMAP**: Internet Message Access Protocol is a protocol that allows a local client to access e-mail on a remote server.

- **IRC**: Internet Relay Chat is a form of real-time Internet chat or synchronous conferencing. It is mainly designed for group (many-to-many) communication in discussion forums called channels, but also allows one-to-one communication and data transfer via private message.

- **MIME**: Multipurpose Internet Mail Extensions is an Internet standard that extends the format of e-mail to support text in character sets other than US-ASCII, as well as non-text (e.g. video, audio, image) attachments, multi-part message bodies, and header information in non-ASCII character sets.

- **POP**: Post Office Protocol version is a protocol used to retrieve e-mail from a remote server over a TCP/IP connection.

- **SIP**: Session Initiation Protocol is a signaling protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences.

- **SMTP**: Simple Mail Transfer Protocol is the de facto standard for e-mail transmission across the Internet.

- **SNMP**: Simple Network Management Protocol is used by network management systems to monitor network-attached devices for conditions that warrant administrative attention.

- **SSH**: Secure Shell is a network protocol that allows establishing a secure channel between a local and remote host.

- **TELNET**: Teletype Network protocol is a client-server protocol for remote login on hosts on Internet.

- **BGP**: Border Gateway Protocol is the core protocol for inter-domain (i.e. between domains) routing on Internet.

- **OSPF**: Open Shortest Path First is a intra-domain (i.e. within domains) routing protocol on Internet

- **RIP**: Routing Information Protocol is a intra-domain routing protocol on Internet

- **IS-IS**: Intermedia System-to-Intermediate Systems is a intra-domain routing protocol on Internet

- **RPC**: Remote Procedure Call is technology that allows a computer program to cause a subroutine or procedure to execute in another address space (commonly on another computer) without the programmer explicitly coding the details for this remote interaction.

- **RTP**: Real-time Transport Protocol defines a standardized packet format for delivering audio and video over the Internet.

- **RTCP**: Real-time Transport Control Protocol provides out-of-band control information for an RTP flow.

- **TLS/SSL**: Transport Layer Security and Secure Sockets Layer are cryptographic protocols which provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, and other data transfers.

- **SDP**: Session Description Protocol is a format for describing streaming media initialization parameters.

- **SOAP**: Simple Object Access Protocol is a protocol for exchanging XML-based messages over a computer network, normally using HTTP.

- **L2TP**: Layer 2 Tunneling Protocol is a method for implementing virtual private networks.

- **PPTP**: Point-to-Point Tunneling Protocol is a method for implementing virtual private networks.

3.7.2 Transport layer protocols

The protocols at the transport layer include:

- **TCP**: Transmission Control Protocol is a connection-oriented protocol that is one of the core protocols of the Internet protocol suite, often simply referred to as TCP/IP. Using TCP, applications on networked hosts can create connections to one another, over which they can exchange streams of data using stream sockets. The protocol guarantees reliable and in-order delivery of data from sender to receiver. TCP is able to handle multiple connections by concurrent applications (e.g. Web server and e-mail server) running on the same host. TCP supports many of the Internet's most popular application protocols and resulting applications, including World Wide Web, e-mail, and secure shell.

- **UDP**: User Datagram Protocol is connectionless protocol that is one of the core protocols in the Internet protocol suite. Using UDP, programs on networked computers can send short messages known as datagrams to one another. UDP does not provide the reliability and ordering guarantees that TCP does. Datagrams may arrive out of order or go missing without notice. Without the overhead of checking if every packet actually arrived, UDP is faster and more efficient for servers that answer small queries from huge number of clients. Compared to TCP, UDP is required for broadcast (send to all on local network) and multicast (send to all subscribers). Common network applications that use UDP include DNS, streaming media such as IPTV, Voice over IP (VoIP), Trivial File Transfer Protocol (TFTP) and online games.

- **DCCP**: Datagram Congestion Control Protocol is a message-oriented transport layer protocol. Applications that might make use of DCCP include those with timing constraints such that streaming media and Internet telephony.

- **SCTP**: Stream Control Transmission Protocol is connection-oriented transport protocol. It provides some similar services as TCP - ensuring reliable, in-sequence transport of data with congestion control. The difference is that SCTP provides message-based multi-streaming, whereas TCP provides byte-based single-streaming.

3.7.3 Network layer protocol

The protocols at the network layer include:

- **IP**: Internet Protocol provides unreliable communication of data across a packet-switched internetwork. IP is a network layer protocol in the Internet protocol suite and is encapsulated in a data link layer protocol. The main features of IP is the unique global addressing capability amongst computers, routing of IP packets, and capability to fragment the IP packets into smaller pieces (to fit the maximum frame size at the data link layer) and to reassemble them again at the destination. The current version of IP in Internet is IPv4. Some operators have upgraded their routers to IPv6 which has a vastly larger address space, better support for QoS and security, and allows faster routing decisions provided no extension headers are used.

- **MPLS**: Multiprotocol Label Switching operates at an OSI model layer that is generally considered to lie between the traditional definitions of layer 2 (data link layer) and Layer 3 (network layer), and thus is often referred to as a “Layer 2.5” protocol. It can be used to carry many different kinds of network layer traffic, including IP packets, over virtual circuits. MPLS groups packets to be forwarded in the same manner into forwarding equivalence classes (FECs) and labels are used to mark the packets to identify the forwarding path. The assignment of a packet to an FEC is done once, at the entry point to the network. MPLS capable label switching routers (LSRs) then use the label to make packet forwarding decisions. MPLS packets are able to carry a number of labels in a last-in first-out stack, which is highly useful where two levels of routing are taking place across transit routing domains, such as widely deployed MPLS virtual private networks (VPNs). A sequence of LSRs defines a label switched path (LSP), which can be hop by hop where each node independently decides the next hop, and explicitly routed where the ingress node specifies the path to be taken. MPLS is able to work with any data link technology, connection oriented or connectionless.

- **ATM**: Asynchronous Transfer Mode is a cell relay, network and data link layer protocol which encodes data traffic into small (53 bytes; 48 bytes of data and 5 bytes of header information) fixed-sized cells. This is instead of variable sized packets (sometimes known as frames) as in packet-switched networks (such as IP or Ethernet). ATM is a connection-oriented technology, in which a connection is established between the two endpoints before the actual data exchange begins. ATM offers five service classes: Unspecified Bit Rate (UBR), real-time Variable Bit Rate (rt-VBR), non-real-time Variable Bit Rate (nrt-VBR), Available Bit Rate (ABR), Guaranteed Frame Rate (GFR). The ATM adaptation layer (AAL) is used to improve the service of the unreliable ATM layer. The AAL layer can be viewed as a form of transport layer which delivers end-to-end service. However, additional transport protocols may be used above the AAL layer, e.g. when TCP/IP or UDP/IP runs over AAL/ATM.

- **ARP**: Address Resolution Protocol is the method for finding a host's hardware address when only its network layer address is known. Due to the overwhelming prevalence of IPv4 and Ethernet, ARP is primarily used to translate IP addresses to Ethernet MAC addresses.
- **RARP**: Reverse Address Resolution Protocol is a network layer protocol used to resolve an IP address from a given hardware address (such as Ethernet address). It has been rendered obsolete by BOOTP and more modern DHCP, which both support much greater feature set than RARP.
- **ICMP**: Internet Control Message Protocol is one of the core protocols in the Internet Protocol suite. It is chiefly used by networked computers' operating systems to send error messages - indicating, for instance, that a requested service is not available or that a host or router can not be reached. ICMP differs in purpose from TCP and UDP in that it is usually not used directly by the user network applications.
- **IGMP**: Internet Group Message Protocol is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of IP multicast specification, like ICMP for unicast connections. IGMP is used for online video and gaming.
- **RSVP**: Resource Reservation Protocol is a network layer protocol designed to reserve resources across a network for an integrated services Internet. RSVP does not transport application data but is rather an Internet control protocol, like ICMP, IGMP or routing protocols. RSVP provides receiver-initiated setup of resource reservation for multicast or unicast data flows with scaling and robustness. RSVP can be used by either hosts or routers to request or deliver specific levels of QoS for application data streams or flows. It is worth noting that RSVP by itself is rarely deployed in Internet today. However, the traffic engineering extension of RSVP, or RSVP-TE, is becoming more widely accepted nowadays in many QoS-oriented networks.
- **IPsec**: IP security is a suite of protocols for securing IP communications by authentication and/or encrypting each IP packet in a data stream. IPsec also includes protocols for cryptographic key establishment.

3.7.4 Data link layer protocols

The protocols at the data link layer include:

- **GMPLS**: Generalized Multiprotocol Label Switching is an extension of MPLS to include the packet layer as well as the transport layer, with its optical network elements. As with MPLS, the GMPLS standard focuses on both routing and signaling parts of the control plane. By providing a common control plane for packet and transport layers, GMPLS enables end-to-end, dynamic bandwidth provisioning, optical transport networks, and thereby is a key enabler of intelligent optical networking. GMPLS differs from MPLS in that it supports multiple types of transport switching, including TDM, lambda, and fiber (port) switching. In MPLS, LSRs recognize either packet/cell boundaries and are able to process packet/cell headers. This is not necessarily the case with GLPMS LSRs. Transport switching may also be based on time slots, wavelengths, or physical ports.

- **Ethernet**: a large, diverse family of frame-based computer networking technologies for local area networks (LANs). The name comes from the physical concept of ether. If defines a number of wiring and signaling standards for the physical layer, through the means of network access at the Media Access Control (MAC) / Data Link Layer, and a common addressing format. Ethernet has been standardized as IEEE 802.3. Its star-topology, twisted pair wiring became most widespread LAN technology in use from the 1990s to the present, largely replacing competing LAN standards such as coaxial cable Ethernet, token ring, FDDI and ARCNET. In recent years, Wi-FI, the wireless LAN standardized by 802.11, has been used in addition or instead of Ethernet in many installations.

- **FDDI**: Fiber-Distributed Data Interface provides a standard for data transmission on a local area network that can extend in range up to 200 kilometers. The FDDI protocol uses as its basis the token ring protocol. In addition to covering large geographical areas, FDDI local area networks can support thousands of users. As a standard underlying medium it uses optical fiber. FDDI uses a dual-attached, counter-rotating token ring topology.

- **FR**: Frame relay consists of an efficient data transmission technique used to send digital information quickly and cheaply in a relay of frames over virtual circuits to one or many destinations from one or many end-points. Network providers commonly implement frame relay for voice and data as an encapsulation technique, used between LANs over a WAN. As of 2006 native IP-based networks have gradually begun to displace frame relay. With the advent of MPLS, VPN and dedicated broadband services such as cable modem and DSL, the end may loom for the frame relay protocol and encapsulation. There remain, however, many rural areas lacking DSL and cable model services, and in such cases the least expensive type of "always-one" connection remains a 128-kilobit frame relay line.

- **PPP**: Point-to-Point Protocol is commonly used to establish a direct connection between two nodes. It can connect computers using serial cable, phone line trunk line cellular, telephone, specialized radio links, or fiber optic links. Most ISPs use PPP for customers' dial-up access to the Internet.

3.7.5 Physical layer protocols

The protocols at the physical layer include:

- **Ethernet physical layer**: evolved over a considerable time span and encompasses quite a few physical media interfaces and several magnitudes of speed. The speed ranges from 3 Mbps to 10 Gpbs in speed while the physical medium ranges from bulky coaxial cable to twisted pair to optical fiber.

- **ISDN**: Integrated Services Digital Network is a circuit-switched telephone network system, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in better quality and higher speed than that available for PSTN system. More broadly, ISDN is a set of protocols for establishing and breaking circuit-switched connections, and advanced call features for the user. In a videoconference, ISDN provides simultaneous voice, viedo and text transmission between individual desktop videoconferencing system and group (room) video conferencing systems.

- **Modem**: Modulator-demodulator is a device that modulates an analog carrier signal to encode digital information, and also demodulates such a carrier signal to decode the transmitted information. Examples include cable modems, ADSL modems, "radio modems" and optical modems.

- **PLC**: Power Line Communication is a term describing several different systems for using power distribution wires for simultaneous distribution of data. The carrier can communicate voice and data by superimposing an analog signal over the standard 50 or 60 Hz alternating current. It includes Broadband over Power Lines with data rates sometimes above 1 Mbps and Narrowband over Power Lines with much lower data rates.

- **RS-232**: a standard for serial binary data interconnection between a Data Terminal Equipment (DTE) and a Data Circuit-terminating (DCE) Equipment). It is commonly used in computer serial ports. A similar ITU-T standard is V.24. For local communication between PC and external devices USB is now more common than RS-232.

- **SONET/SDH**: The Synchronous Digital Hierarchy (SDH) and Synchronous Optical Network (SONET) are European and US standards for communication over Time Division Multiplex (TDM) channels. SDH/SONET provides multiplexing of multiple digital channels, and operation, administration and maintenance. A SDH/SONET system consists of optical cross connects, add/dropp multiplexers, concentrators, repeaters, all connected by optical fibers in a ring topology. Both SONET and SDH can be used to encapsulate earlier digital transmission standards, such as the Plesiochronous Digital Hierarchy (PDH) standard or used directly to support MPLS, ATM or 10 Gbit Ethernet. Multiple SONET/SDH signals can be transported over multiple wavelengths over a single fiber pair by means of Dense Wave Division Multiplexing (DWDM).

- **G.709**: Interface for the optical transport network (OTN) is a standardized method for managing wavelengths in optical networks. G.709 allows the use of completely optical switches (optical cross-connects) without doing the expensive optical/electrical/optical conversions.

3.8 Internet Engineering Task Force

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The IETF Mission Statement is documented in RFC 3935. The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas (e.g., routing, transport, security, etc.).

Much of the work is handled via mailing lists. The IETF holds meetings three times per year. The IETF working groups are grouped into areas, and managed by Area Directors, or ADs. The ADs are members of the Internet Engineering Steering Group (IESG). Providing architectural oversight is the Internet Architecture Board, (IAB). The IAB also adjudicates appeals when someone complains that the IESG has failed. The IAB and IESG are chartered by the Internet Society (ISOC) for these purposes. The General Area Director also serves as the chair of the IESG and of the IETF, and is an ex-officio member of the IAB. The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. The IANA is chartered by the Internet Society (ISOC) to act as the clearinghouse to assign and coordinate the use of numerous Internet protocol parameters.

Chapter 4

History of communication networks

4.1 Telephone networks

Ever since the advent of the telephone in 1876 by Alexander Graham Bell, voice communication between distant locations have been possible. The first telephone networks introduced a few years later consisted of manually operated switching offices connected to each others and to the customers' telephones. In the late 1800s signals were analog and telephones were allocated a single channel per line for transmission. The copper-based twisted pair was introduced in the local loop between the customer and the local switching office in the 1890s. Development of the vacuum tube led to analog system employing FDM (Frequency Division Multiplexing) introduced in 1925. The human operators where replaced by electro-mechanical switches in the 1940s. The advent of the transistor in 1948 paved the way for computer controlled switches which were introduced in the 1960s. Starting in 1946 until the 1980s, the switches were inter-connected by coaxial cable. In the mid-1980s high-speed optical fibers were introduced in the switching network. The early systems used PDH which later was replaced by SONET/SDH which is based on Pulse Code Modulation (PCM) and Time Division Multiplexing (TDM). Until 1980s, telephone networks had an hierarchical topology with 5 national levels and one international level. Flat national network topologies and dynamic routing were introduced in many countries during the 1990s.

4.2 Internet

Paul Baran, employed at the RAND corporation in US, introduced in 1962 the concepts of packet-switching and distributed networks in his attempt to design a fault-tolerant US communication network which should survive a nuclear war. September 1969 marked the birth of ARPANET, the predecessor of Internet. ARPANET connected US universities which were supported by the US Department of Defense. In the late 70s the first version of the Internet Protocol (IP) and the Transmission Control Protocol (TCP) were introduced in ARPANET. In 1983 ARPANET became Internet. The definition of Internet being the global inter-connected collection of smaller networks which implements the TCP/IP protocol suite still holds today. The number of hosts in the Domain Name System (DNS) has evolved from 200 in 1981 to about 540 million in January 2008. The number of autonomous systems (domains) was 85,000 and the number of IP networks in the global routing table was 280,000 in January 2007. The history of Internet applications has landmarks such as the introduction of the first email system in 1971 and the introduction of world wide web, invented at CERN, Switzerland, in 1991. The following services dominated traffic on Internet in 2007: world wide web (46%), peer-to-peer file download and audio/video streaming (37%), newsgroup (9%), non-HTTP video streaming (3%), gaming (2%), and VoIP (1%).

4.3 Data networks

Samuel Morse's invention of the telegraph 1835 marked the start for data networks. Data networks offers a packet-oriented transport service without any guarantees on transfer delay. Historically, data network standards have evolved for both LANs and WANs. The first LAN standard, the Ethernet standard, came in 1976. Later, in 1985, the Token ring LAN standard was approved. In both these two LAN standards, stations are connected to a shared media which they access according to some control scheme. The first WAN standard, the X.25 standard, was approved by the ITU in 1976. X.25 is a packet- and connection-oriented transfer technique offering low bit rate (64 kbps) connections. Most Automatic Teller Machines (ATMs) are connected through X.25 over the D-channel using N-ISDN basic access. The Switched Multimegabit Data Service (SMDS) is a WAN network standard primary aimed at LAN connectivity. SMDS was developed by Bellcore in the early 1990s. SMDS is packet-oriented and connectionless.

4.4 Wireless networks

The first radio transmission across Atlantic Ocean was demonstrated in 1901 by Marconi. In 1920 the first public radio transmission took place in Germany. In the 1920s police radio in cars were introduced in metropolitan New York area. In 1946 the first mobile telephone service in USA was introduced by AT&T. Mircowave radio transmission was used for long-distance telephony in 1947. In 1949 Claude Shannon et al. developed the basic ideas of CDMA. In 1979 and 1981 the first generation (1G) analog cellular systems AMPS and NMT was introduced in USA and Sweden, respectively. Second generation (2G) cellular systems such as GSM, IS-95 and PDC were introduced in 1991 (Europe), 1993 (USA) and 1994 (Japan), respectively. Third generation (3G) cellular systems WCDMA/UMTS and CDMA2000 were introduced by first by Japan in 2001 and by Sweden in 2002. 3G operators in Europe use WCDMA/UMTS standard in the 1920-1980 MHz and 2110-2170 MHz frequency bands and the CDMA2000 standard in the 450 MHz band. Other important events in the history of wireless networks are the introduction of the IEEE 802.11 WLAN in 1997, Bluetooth WPAN in 2000, IEEE 802.16 WMAN in 2006.

4.5 Multi-service networks

Multi-service networks have an important advantage over pure data networks, namely real-time service capabilities. Multi-service networks have evolved since the mid 1980s and standards exist today for LANs, MANs and WANs. The Token bus LAN standard was approved in 1985. An important application environment for Token bus is factory automation. The FDDI and DQDB MAN network were developed during the early 1990s. Multi-service WANs include Frame relay, Narrowband ISDN, Broadband ISDN/ATM and the Next Generation Internet. The Frame relay standard was developed in 1984 and was first seen as a competitor to the X.25 standard. Frame relay is designed to be efficient for fiber communication characterized by low transmission error rates. The N-ISDN and B-ISDN are standards of the ITU approved in 1984 and 1988, respectively. N-ISDN is circuit-switched and offers bandwidths up to 2 Mbps. B-ISDN is based on ATM which is a packet-switched technology and offers bandwidth from 155 Mbps to 1.6 Tbps. ATM has proven very successful in the WAN scenario and numerous Telcos have implemented ATM in their wide-area network cores. Also many ADSL implementations use ATM. However ATM has failed to gain wide use as a LAN technology and its complexity has held back its full deployment as the single intergrated network technology originally intended by the inventors. Currently is seems likely that gigabit Ethernet implementations (10Gbit Ethernet, Metro Ethernet) will replace ATM as the technology of choice in new WAN implementations. Cisco has offered DiffServ routers for deployment in Next Generation Internet since 2000. The DiffServ technology has been tested in numerous field trials. Today ISPs provide QoS service within single domains.

Bibliography

[1] A. Aftab, *Data Coomunication Principles for Fixed and Wireless Networks*, Luwer Academic Publishers, 2002.

[2] ATM Forum, “Traffic management specification”, Version 4.0, 1996.

[3] ATM Forum, “PNNI specification Ver 1.0, 1996.

[4] G. Apostolopoulos, D. Williams, S. Kamat, R. Guérin, A. Orda, T. Przygienda, “QoS routing mechanisms and OSPF extensions”, IETF RFC 2676, IETF RFC 2702, Available from ¡http://www.ietf.org/rfc/rfc2676¿, Aug. 1999.

[5] G. Ash, *Traffic Enigneering and QoS Optimization of Integrated Voice & Data Networks*, Morgan Kaufmann, 2007.

[6] D. Awduche, A. Chiu, A. Elwalid, I. Widjaja, X. Xiao, “Overview and principles of Internet traffic engineering”, IETF RFC 3272, Available from ¡http://www.ietf.org/rfc/rfc3272¿, May 2002.

[7] D. Awduche, J. Malmcom, J. Agogbua, M. O’Dell, J. McManus, “Requirements of traffic engineering over MPLS”, IETF RFC 2702, Available from ¡http://www.ietf.org/rfc/rfc2702¿, Sep. 1999.

[8] A.R. Bashandy, E.K.P. Chong, A. Ghafoor, “Generalized quality-of-service routing with resource allocation”, *IEEE Journal on Selected Areas in Communications*, Vol. 23, No. 2, pp. 450-463, 2005.

[9] O. Bedell, *Wireless Crash Course*, McGraw-Hill Professional, 2001.

[10] O. Billström, L. Cederquist, M. Everbring, G. Sandegren, Jan Uddefelt, “Fifty years with Mobile Phone”, *Ericsson Review*, No. 3, 2006.

[11] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss, “An architecture for differentiated services”, IETF RFC 2475, Available from ¡http://www.ietf.org/rfc/rfc2475¿, Dec. 1998.

[12] Braden R., Clark D. and Shenker S., Integrated Services in the Internet Architecture, IETF RFC 1633, 1994.

[13] R. Braden, L. Zhang. S. Berson, S. Herzog, S. Jamin, “Resource ReSerVation Protocol (RSVP) – version 1 functional specification”, IETF RFC 2205, Available from ¡http://www.ietf.org/rfc/rfc2205¿, Mar. 2002.

[14] T. Braun, M. Guenter, I. Khalil,”Management of Quality of Service enabled VPNs”, *IEEE Communications Magazine*, Vol. 39, No. 5, pp. 90-98, May 2001.

[15] K. Calvert, M. Doar, E. Zegura, “Modelling Internet topology”, *IEEE Communication Magazine*, Vol. 35, No. 6, pp. 160-164, 1997.

[16] G. Camarillo, *3G IP Multimedia Subsystem (IMS): Merging the Internet and Cellular Worlds*, John Wiley & Sons, 2005.

[17] B. Carpenter, K. Nichols, “Differentiated services in the Internet”, *Proceedings of the IEEE*, Vol. 90, No. 9, pp. 1479-1494, Sep. 2002.

[18] C. Eklund, R. Marks, K. Stanwood, S. Wang, “IEEE Standard 802.16: A Technical Overview of the Wireless MAN: Air interface for Broadband Wireless Access”, *IEEE Communications Magazine*, Vol. 40, No. 6, 2002.

[19] M. Engels (editor), *Wireless OFDM Systems: How to Make Them Work*, Kluwer Academic Publishers, 2002.

[20] S. Deering, R. Hinden, Internet Protocol Version 6 Specificaation, IETF RFC 1883, 1995.

[21] T. Janevski, *Traffic Analysis and Design of Wireless IP Networks*, Artech House, 2003.

[22] IETF, Internet Protocol Specification, IETF RFC 791, 1981.

[23] IETF, Transmission Control Protocol Specification, IETF RFC 793, 1981.

[24] ITU-T, ISDN service capabilities, B-ISDN service aspects, Recommendation I.211, 1993.

[25] ITU-T, Network performance objectives for IP-based services, Recommendation Y.1541, 2002.

[26] ITU-T, “Traffic control and congestion control in B-ISDN”, I.371, 2004.

[27] ITU-T, SG12, End-User Multimedia QoS Categories, Draft recommendaion, G.QOSrqt, 2002.

[28] J. Korhonen, *Introduction to 3G Mobile Communications*, 2nd edition, Artech House, 2003.

[29] F. Kuipers, P. Mieghem, T. Korkmaz, M. Krunz, “An overview of constraint-based path selection algorithms for QoS routing”, *IEEE Communications Magazine*, Vol. 40, No. 12, pp. 50-56, Dec. 2002.

[30] D. McDysan, ATM and MPLS theory and application: foundation of multi-service networking (standards & protocols), Osborne/McGraw-Hill, 2o02.

[31] K. Pahlavan, P. Krishnamnurthy, *Principles of Wireless Networks*, Prentice-Hall, 2002.

[32] J. Postel, User Datagram Protcol Specification, IETF RFC 768, 1980.

[33] P. Ramjee, *OFDM for Wireless Communications*, Artech House, 2004.

[34] E. Rosen, Viswanathan A. and Callon R,. Multiprotocol Label Switching Architecture, IETF RFC 3031, 2001.

[35] H. Schultzrinne, S. Casner, R. Frederick and V. Jacobson, A Transport Protocol for Real-Time Applications, IETF RFC 1889, 1996.

[36] J. Schiller, *Mobile Communications*, Second edition, Addison Wesley, 2003.

[37] *Wireless Telecommunications FAQ*, McGraw-Hill Companies, 2001.

[38] C. Smith, D. Collins, *3G Wireless Networks with WiMAX and WiFi*, McGraw-Hill Professional, 2004.

[39] C. Smith, D. Collins, *3G Wireless Networks*, McGraw-Hill Professional, 2007.

[40] P. Trimintzios, I. Andrikopoulos, G. Pavlou, et. al.,”A management and control architecture for providing IP differentiated services in MPLS-based networks”, *IEEE Communications Magazine*, Vol. 39, No. 5, 2001.

[41] D. Wong, *Wireless Internet Telecommunications*, Artech House, Incorporated, 2004.

[42] S. Yang, *3G CDMA2000 Wireless System Engineering*, Arthech House, 2004.