High Speed Networks for Carriers

Karl J. Schrodi

Siemens AG, Information and Communication Networks,
81359 Munich, Germany
karl.schrodi@icn.siemens.de

Abstract. This paper focuses on high speed networks in a future public network infrastructure. 'Next Generation Networks' (NGNs), built on fast IP based packet switching technologies, will provide a unified platform capable of seamlessly supporting a variety of existing and future telecommunications and data services and applications. Requirements on and expected properties of NGNs as the new generation of carrier networks are discussed. An architectural overview reveals the major interfaces and related protocol issues. An implementation approach with emphasis on QoS, network resilience and operational cost issues is presented.

1 Introduction

High speed networks have long played a role in campuses and other closed environments for scienctific, research and educational purposes. Support from public networks was limited to the provisioning of transmission capacities for the interconnection of different high speed networking islands. Corporate business and industrial applications relied on the same scheme, since the public network was dedicated to and optimized for telephony services, and a public network infrastructure suitable for high speed information switching was not available.

Asynchronous Transfer Mode (ATM) [1] was initially intended to become the key technology for the introduction of generally available broadband telecommunication services in local and wide area networks and "the transfer mode solution for implementing a B-ISDN" [2]. However, ATM missed the path towards mass applications and, despite of its proven capabilities of fulfilling all major telecommunication networking requirements, it may finally find itself pushed back into the role of 'just another data link layer'.

The real drive towards higher speed and higher throughput in a public networking infrastructure found its origin in a different application area, which was known and used by a rather small community of data communication insiders only even less than ten years ago. Internet and World Wide Web (WWW) [3], [4] have become an almost unbelievable success story. Internet usage and traffic volume have grown almost

Acknowledgement. This work was partially funded by the Bundesministerium für Bildung und Forschung of the Federal Republic of Germany (Förderkennzeichen 01AK045). The author alone is responsible for the content of the paper.

G. Carle and M. Zitterbart (Eds.): PfHSN 2002, LNCS 2334, pp. 229–242, 2002.

explosively throughout the last decade and some predictions say that the traffic growth may continue at well beyond a factor of two per year for at least a few more years [5].

Basic internet principles and mechanisms are significantly simpler and easier to operate than ATM, since the Internet Protocol (IP) [16] based networking concept does not need a path infrastructure and offers a unified 'best effort' type of service only. IP based packet switching networks have been installed in parallel to the Public Switched Telephone Network (PSTN) and they have already outgrown the PSTN in transfer capacity. Having done the exercise with ATM, it was obvious that IP based packet technology could as well be used for carrying voice, video and any other kind of electronically conveyable communications. The resulting new type of network which converges the services and applications of the ancestor networks on a single IP based platform and is open for a variety of new services and applications, is often refered to as 'Next Generation Network' (NGN).

This paper approaches NGNs from the service and application point of view and derives from that the capabilities and properties expected from an NGN as an evolution towards high speed carrier networks. The key requirements from the networking point of view are discussed and an outline of an NGN architecture is presented. Finally a few guidelines for a possible solution approach are developed.

2 Next Generation Networks

2.1 Roots and Standardization Status

Just ten years ago telecommunication service providers and carriers were mainly focusing on telephony and possible evolutions of telephony-like services towards higher value audio, video and multimedia applications. Around the same time the general availability of personal computers (PCs) as affordable tools for desktop computing for business and home applications had created a demand for simple, cost efficient and easy to use data communications and information access. Internet technologies and related application services opened the gates for PCs and Local Area Networks (LANs) towards universal and ubiquitous information exchange.

Technology evolution has turned PCs into high performance terminals and the affordability of broadband access even for residential users via xDSL and cable modems fuels the demand for bandwidth, throughput and performance of the network. IP packet forwarding has moved from general-purpose processor software to dedicated hardware devices and has made state-of-the-art routers capable of serving high-speed interconnection links at wire speed possible. Such progress allows a steadily increasing variety of different new services and applications to be created and delivered via internet technology based infrastructures. The delivery of (voice) telephony services over IP based networks including the traditional 'best effort' internet has already become a reality. New dedicated NGN solutions will provide the capabilities, features and functions required for the deployment of high speed, high performance telecommunications and data services with true 'carrier grade' service characteristics.

The Internet Engineering Task Force (IETF) [6] has proposed mechanisms like Integrated Services (IntServ) [7] and Differentiated Services (DiffServ) [8] for reservation of resources and differentiation of individual traffic flows in routers in order to facilitate service delivery with different levels of Quality of Service (QoS) in IP networks. Special protocols like RTP and RTCP [9], [10] have been designed to support and control the transport of real time applications as for example voice, audio or video communications across IP based networks. These are just a very few examples out of a variety of mechanisms and protocols that are discussed and proposed by IETF and many other standardization organizations as possible building blocks for a global set of NGN standards.

The most comprehensive framework has been initiated by the European Telecommunication Standards Institute (ETSI) with their TIPHON project [11]. Although initially mainly interested in the delivery of (voice) telephony services over IP based networks and the related interoperability issues between traditional telecommunications and IP worlds, TIPHON has subsequently broadened its charter towards more general issues of heterogeneous and multi-service packet networks. One of the key objectives of TIPHON's recently started NGN activity is a global consolidation and harmonization of NGN standardization in partnership with other organizations working in this field. The latest version of TIPHON documents (Release 3) is publicly available at [12].

2.2 Services and Applications

NGNs are intended to accommodate and facilitate the widespread deployment of 'classical' and future telecommunication services and applications together with 'traditional' and new internet services on a common IP based networking platform. A short look at some major differences in the type and nature of some possible services will indicate the size of the challenge.

Traditional internet services and applications are usually based on direct host to host (or host to server) communications. The role of the Internet Service Provider (ISP) is mainly restricted to subscriber authentication, authorization and accounting (AAA) and the provisioning of access to the network. All service/application related features and functions are completely hosted in and initiated from the application terminal (host). Applications are adapted to operate in an uncontrolled, resource shared and 'best effort' only network environment by the Transmission Control Protocol (TCP) [13], which takes care of reliable transport as well as adequate utilization and fair sharing of available network resources. Data throughput and delay for communications are unpredictable and the resource sharing can cause strong interdependencies between simultaneously active communications.

Classical telecommunication services usually employ service control instances provided by a service and/or network provider. These service control instances take care for the availability of network resources, e.g. a connection path, but they also may offer a variety of additional capabilities, features and functions to be requested by a user application (e.g. ISDN supplementary services). Communications run on dedicated paths using exclusively reserved resources and the transmission behaviour

in terms of throughput and delay etc. is predictable and 'guaranteed'. Consequently, there is no interdependency between different communications as long as the network design and dimensioning has been done properly. A major difference compared to internet services is that telecommunication service users traditionally expect a much better availability and reliability of their services.

The future of internet services will definitely include a more efficient usage from the application point of view (e.g. high-speed web surfing). Built on today's mechanisms this will definitely require a much faster (broadband) network. Another approach aims at a differentiation of service levels, e.g. to distinguish between gold, silver and bronze service. Future services and applications, still unknown yet, may raise additional requirements in terms of throughput, delay, reliability, security or whatever else. Evolution of telecommunication services still follows the vision of broadband real time services for true interactive (dialogue) communications, e.g. high quality audio/video communications up to the notion of 'virtual presence' (or 'telepresence'), in a fully multimedia enabled environment.

Converging all these services onto a common IP packet based NGN platform definitely requires a high speed QoS enabled network, i.e. a network with capabilities to deal with high volumes of data within well defined and distinct limitations on transfer delay and probability of loss. The network architecture has to be open and sufficiently flexible and scalable in order to accommodate new services and their specific requirements.

Flexibility and scalability are specifically important from the network control point of view. Different from telecommunication services, which usually create single, long duration data flows, many internet applications are composed from a multitude of short communication relations with different partner entities. This kind of behaviour may have to be extrapolated into future, yet unknown, NGN services with QoS requirements above the best effort service level.

2.3 Transport Protocols

Two different transport protocols are used with traditional internet applications: the Transmission Control Protocol (TCP) [13] and the User Datagram Protocol (UDP) [14]. UDP offers a completely connectionless transport of individual data segments (datagrams) through IP networks, whereas TCP provides a reliable transfer of contiguous data, i.e. the notion of data streams, over IP based packet networks. A good overview on the current status of these protocols and their related mechanisms is given in [15]. The recently developed Stream Control Transmission Protocol (SCTP) [16] is intended for message-oriented applications, e.g. reliable transportation of signaling data.

TCP's emphasis is on reliable delivery of data even in case of adverse terminal or network conditions. For that purpose it offers specific flow control and congestion avoidance mechanisms which have been refined and improved over several generations of TCP/IP implementations. The basic mechanism behind TCP is its acknowledgement controlled sliding window based data transfer. This kind of mechansim works well as long as the relations between the triple of expected

throughput, window size and data-round-trip-delay can be kept within certain reasonable ranges and network and terminal buffers are well dimensioned. For high speed data transfer over wide area networks the inevitable physical propagation delay, which is ruled by the speed of light, may become a dominating parameter. Simply increasing the window size may affect the efficiency of flow control and congestion avoidance and jeopardize the objective of fair sharing of network resources. A careful tuning of window sizes and case by case selection of supporting mechanisms may improve, but probably not always solve the problem. Still, if there is no better alternative, the long time proven TCP will remain the protocol of choice.

As TCP aims for reliable delivery of data, even at the expense of delay (retransmission), it is not well suited for the transport of real-time applications. Congestion avoidance mechanisms, which are very useful in a resource shared, 'best effort' oriented environment, may be in contradiction to the target of sustained throughput with agreed QoS levels. The Real-Time Transport Protocol RTP [9], [10] has been specified as a mechanism to support end-to-end delivery of information with real-time characteristics in single ended as well as multicast applications and it may as well be applied for other QoS dependent services. RTP includes no flow control and since it does not include all necessary transport layer functions, it 'borrows' missing functions from an underlying transport protocol, which is usually UDP. RTP supports the applications with timing, sequencing, monitoring and other functions, but it does not provide any mechanisms to ensure timely delivery of data nor does it provide any means to guarantee delivery of data or a certain QoS. Lower layers are expected to provide suitable mechanisms to ensure these capabilities.

Since many of the future services and applications to be supported by NGNs are still unknown, it cannot be stated today whether the available set of transport protocols will be sufficient on the long run to link all NGN services and applications to the network.

2.4 Interoperability with Existing Networks

NGNs will provide a plenty of new services and applications on a new, special feature enabled, packet based networking platform. NGNs also will converge the full spectrum of already existing telecommunications and internet services on this same platform. A smooth introduction of NGN technologies will be based on a long-term coexistence of NGNs with traditional networking technologies.

This may be less critical with regard to the Internet since both networks are built from the same basic principles and mechanisms and their technological affinity will ease seamless interoperation. Needless to say, that interworking will only be possible on the basis of services and features that are supported by both technologies. The very fast growth of the internet has created a phenomenon never known by traditional telecommunication service providers and carriers. Equipment or even equipment family turnaround times down to less than three years have been reported from ISPs and IP network providers. Together with the desirability of 'better service' for end users and expected reductions in operational cost, this fuels the assumption that NGN

technology, if matured and available in time, could potentially absorb and replace the traditional internet within less than a decade.

In the telecommunications arena the situation is somewhat different. A huge base of telephone network equipment is installed and operating satisfactorily in the PSTN. As long as the operation of this equipment is economically justifyable, (in other words, as long as there is a sufficiently high number of subscribers satisfied with the services and applications offered by this technology,) there is no reason and no pressure to remove or replace this equipment. Finally, the success and the speed of deployment and dispersion of NGN services will play a decisive role.

Interworking with the PSTN will be based on telephony gateways, which are capable to distinguish and interwork voice telephony, fax and low speed dial-in internet access services. Conversion between TDM and IP packet based transport will have to be provided and a lot of peering issues, starting from proper QoS mapping up to tarifing and billing issues, will have to be solved. Realistically, a survival time of PSTN equipment of at least several decades has to be assumed.

3 Key Requirements on Next Generation Networks

In this section some key requirements on NGNs as a new generation of carrier networks are discussed. The selection is driven by those aspects, which are important for their classification as 'carrier grade'[1] networks.

3.1 Quality of Service (QoS)

QoS is always the first (and sometimes the only) requirement that pops up in discussions about multi-service packet networks. A quick and easy answer to the problem could be to dimension and operate the network at a unified service level that satisfies the requirements of the most demanding application. However, an economically justifiable network operation will require a differentiated treatment of the variety of services and applications according to their specific needs.

QoS mechanisms in packet networks have to respect the characteristics of the different traffic flows in terms of their variance or even a more pronounced burstiness up to the extremes of a direct or overlaid on-off behaviour. Statistical methods have to be applied in order to describe such kinds of traffic, to analyze their interactions in the network, and to understand the resulting effects in terms of throughput, delay and loss of packets. Finally, the capabilities of the applications to tolerate (or not) a certain level of impairments induced by the network determine their requirements.

[1] The term 'carrier grade' probably has its origin in the high speed router start-up scene, where it was used to indicate that a planned router product was intended to provide the same level of service, the same level of serviceability and all the other nice features and properties, that people were used to find in the well established and mature PSTN backbone switching technology of established (long distance) carriers.

As an example, a measure for a very demanding service can probably be derived from the already mentioned audio/videocommunication with the notion of 'virtual presence'. High quality, high resolution video requires sufficient throughput and low loss, real-time interactive human (dialogue) communications cannot tolerate too much delay. Intermediate levels could be marked by voice telephony, which can tolerate some packet loss as long as certain delay limits are not exceeded, and a privileged internet service, e.g. with guaranteed minimum throughput. At the low end are traditional best effort internet services.

Since the provision of individual QoS levels per application instance or individual data flow is not feasible, requirements are usually mapped to predefined network services (or traffic classes), that provide a certain well defined and 'guaranteed' level of QoS. Requirements not directly matching with a network service then have to be mapped to the next better one. Administration, operation and supervision of network services and especially the process of assigning network services to different data flows may still turn out to be quite complex and expensive. Therefore a proliferation of network services has to be avoided. A low single digit number is recommended.

QoS can be measured at the technical level in terms of throughput, packet loss and packet delay, and these are the parameters that usually are influenced (but not exclusively determined) by the network. The decisive judgment criterion, however, will always be the user's perception. The network has done a good job as long as the user has a working application and the impression of a good service. Doing more than necessary usually causes unnecessary cost. Therefore a good understanding of applications and their capabilities is inevitable for a good network design and proper network and traffic engineering.

Another important aspect of QoS is its need for control. QoS requires resources to be available at the place and time where and when they are needed. A proper allocation has to be done wherever resources are limited. Since network control performance is an important cost factor, a good network design has to reflect the impacts of resource control, application behaviour (e.g. single or multiple flows) and related usage patterns (i.e. frequency and duration of usage).

3.2 Resilience

Network resilience describes a network's capabilities to provide sustainable service at agreed QoS levels under varying traffic conditions and in spite of different kinds of impairments affecting it. Such impairments may be caused by network internal or external events and appear as temporary or local overload, unavailability of certain network resources or any other effects.

Circuit switching based telecommunication networks provide up to more than five nines (99.999%) of service availability, a level far beyond that of many of today's data networks. This difference is mainly based on much more local redundancy, intrinsically fault tolerant network nodes and faster fault recovery mechanisms combined with a higher stability of software deliveries. Packet networks may even achieve a higher overall survivability, but currently available mechanisms are comparably slow.

Telecommunication subscribers are used to such high levels of service availability supported by fault recovery mechanisms that in many cases leave no perceptible or at least no annoying impairments on their delivered services (respectively the related QoS) and this experience determines user expectations for existing and new services in NGNs. Substancial efforts will have to be made in order to provide mechanisms efficient and fast enough to comply with these expectations without giving up the advantages in flexibility, simplicity of operation and operational cost currently fueling the trend for a transition towards packet based NGN solutions.

3.3 Security

Reliable network operation is heavily related to network security. Network elements have to be protected against any kind of unauthorized access. Malicious intruders might attack network control information and disturb network control communications and network operation up to complete network failure. Intruders could steal or modify administrative or operational data, e.g. subscriber profiles or charging data record (CDR) information. Intruders could intercept user traffic and violate subscriber privacy.[2] They might even modify or destroy user traffic data. The unauthorized access issue is even more critical in IP based networks compared to traditional circuit switched ones, since in most cases network control communications will use the same mechanisms and even share network resources with user traffic. Special care will have to be taken on these aspects.

A related issue is unauthorized usage of network resources. Since all QoS agreements rely on the (controlled) availability of required network resources, any unexpected traffic might significantly impair the QoS of regular traffic. Special attention has to be paid to intentionally malicious user traffic that could aim at denial of service or at other impacts on traffic handling or traffic control (including signaling) related entities.

3.4 Scalability

Another aspect with potentially significant impact on network economics is scalability. NGNs should match the needs of small local operators as well as those of large international carriers. Network equipment should enable a seamless and ideally linear adaptation to increasing numbers of subscribers as well as changes in service utilization and traffic patterns. It has to be open to accommodate different requirements of new emerging services and applications. Scalability should cover all network components, capabilities and functions for simultaneous as well as independent adaptation.

[2] Note, that on the other hand lawful interception must be supported.

3.5 Serviceability

High reliability and service availability require a seamless operation of all vital network functions. Maintenance and service activities on network components should not impact the perceived functionality, quality and performance of user applications. Addition or change of equipment and introduction of new software releases for capacity, performance and/or functional upgrades should be possible during normal system operation and without traffic interruption. Modular systems should provide for independent maintenance of different modules and functions. Such requirements request a careful reflection in the architecture and design of network and equipment and their way of operation.

3.6 Economy

Many of different factors contribute to the overall economics of owning and operating a network. QoS, reliability and security contribute to initial procurement and depreciation as well as to any subsequent expenses. Further expenses for extensions and upgrades are heavily influenced by scalability and serviceability. The major cost contribution for a long-term ownership, however, may be accumulated from day-to-day operation and maintenance. Reduction of operational cost is propagated as a main driving force for convergence to IP based NGNs, and the reasoning behind is simplicity and ease of operation. To preserve this paradigm, significant attention should be focused on related issues through all phases of NGN lifetime starting with initial concepts.

4 Next Generation Network Architecture

NGN architecture is driven by several factors. They all end in the target of a converged, unified networking platform open for and capable of supporting a variety of different services and applications. Still, the network of the future will be much less unified than the incumbent PSTN. Telecommunication deregulation breaks monopolies and fuels competition and differentiation among carriers (network operators) and service providers. The resulting network (Fig. 1) is composed of several (NGN) network domains, which may be owned by different operators or service providers. Application services, either hosted in user terminals (internet model) or provided and controlled by service providers (telecommunications model), compete for transport resources provided and controlled by the network domains.

A clear separation between network control and service control with well-defined interface and protocol standards is required to make this model work. As a result, the

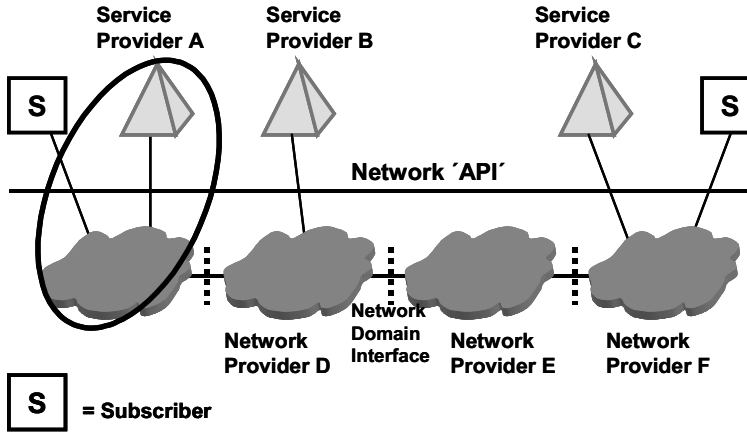

Fig. 1. A generic NGN architecture. Note, that Service Provider A also acts as Network Operator

network will form the envisaged universal platform providing some kind of a generic 'Application Programming Interface' (API) for the support of new services.

Network operators may employ different mechanism to ensure QoS, resilience and security within their different network domains. As a consequence, their definitions and implementations of network services (traffic classes) may differ and the probability to reach a consensus for a globally agreed and standardized set of 'well known network services' (that was achieved with ATM) may not be very high. Thus, the interface standards for network domain interoperation have to include mechanisms capable to cope with differing network service specifications. As an example, explicit QoS requirements could be signaled and the mapping to suitable network services could be done within the domains (Fig. 2).

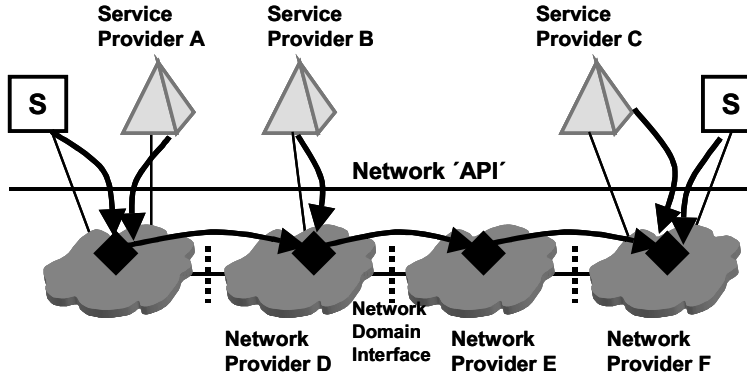

Fig. 2. QoS signaling relationships in a generic NGN architecture

Different applications may use different transport protocols and the different network domains may employ completely different lower layer mechanisms in order to achieve the required properties. Finally, the only remaining common denominator is the networking concept based on the Internet Protocol (IP) [16] (Fig. 3).

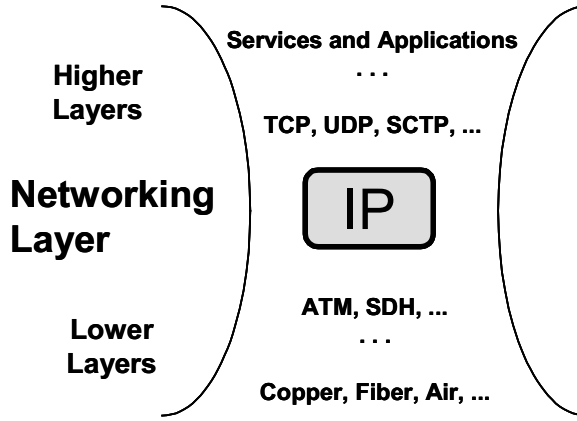

Fig. 3. Internet Protocol (IP) based networking is the common denominator of NGNs

5 A Few Considerations towards an Implementation

5.1 What Is Available

A good solution approach should fulfill all requirements, provide all the features and adhere to all the promises and expectations that have been built around the NGN idea. If we measure the hottest candidates of todays discussions against this objective, it may turn out as follows:

The RSVP based Integrated Services approach [7] succeeds with QoS, but at the expense of a very sophisticated and complex reservation procedure. There seems to be a wide consensus that RSVP does not scale for large networks or frequently changing connection environments. Besides, IntServ does not address network resilience issues.

The Differentiated Services approach [8] is comparably simple and therefore it can scale. However, DiffServ does only provide a few elements of a complete QoS solution, i.e. some kind of an incomplete toolset (edge functions, per hop behaviours) for a differentiated treatment of traffic in a network. DiffServ also does not address network resilience issues.

A more comprehensive approach is Multiprotocol Label Switching (MPLS) [17], [18]. MPLS addresses (to a different extent) traffic engineering, resource reservation, reliability, security and scalability issues. Like ATM, MPLS employs a path infrastructure, which is used to direct ‘connection traffic’ (or ‘flows’), and like ATM,

with every issue it tackles, it packs another piece of complexity on its back. Finally, somebody will have to raise the question: isn't it just ATM - in a different colour?

5.2 The Case for a 'Stateless' Core

Traffic management with a path and connection based concept means complexity, complexity for setting up and maintaining the path infrastructure as well as for managing the resources within the different paths on each individual link along each path. This complexity requires the intelligence of well educated staff and in an environment with highly volatile connection traffic it requires permanent staff attention. Permanent attention of well educated staff is very expensive.

High reliability in a dedicated path concept means redundancy, which has to be provided, dedicated and reserved separately. This redundancy again has its cost. High network resilience requires fault tolerance, i.e. the capability to provide an adequate replacement of lost resources within a very short time in case of failures, so that the applications are not (or only marginally) affected. For that purpose either redundant paths have to be available and (pre)configured in parallel to the actually used paths (hot standby) or the control system has to be able to take care of rerouting, i.e. setting up of new paths and reconfiguration of all afflicted connections, within a very short time. This again may turn out to be quite costly. Additional effort may be required for adaptation of the path infrastructure in case of network extensions or with upgrades, etc..

The key issue with path and connection based concepts is the use of 'states' for each path and each connection in all network nodes and on all links, wherever resources may be shared between different paths and/or connections. States are managed through information exchange between related entities and they are manifested in the different entities as specific data sets or table entries. Every change related to a path or a connection results in at least one 'state change' in the network control system. It has been recognized as one of the key advantages of the Internet concept that it operates in a 'stateless', connectionless way.

5.3 A Proposal for a Connectionless NGN Domain

To take full advantage of the capabilities of IP based packet data transport it is proposed to limit any notion of connections or predefined paths to the borders of NGN domains. As a result, the core of the domain will operate in a 'stateless', connectionless manner. For the provision of QoS the overall capacity budget of the network is calculated and related shares are derived and allocated to the network borders. Network Admission Control (NAC) is done on both ingress and egress borders, in order to avoid egress congestion. Best effort traffic may run uncontrolled, because it can be pushed out by QoS traffic in case of congestion.

To prevent traffic congestion or hot spots inside the network, the network nodes are authorized to distribute the traffic autonomously over all reasonably useable paths towards the destination border. The distribution scheme may use a per packet or a

(local) per flow paradigm. Reasonably useable paths may include all outgoing links that approach the destination border without creating loops and within the specified QoS boundaries (e.g. delay limits). The knowledge about reasonably useable paths may be derived from link state information as usually exchanged by routing protocols.

The autonomous, local distribution of traffic opens new possibilities for network resilience. Provided that fast fault detection mechanisms are applied, faulty parts (links or nodes) in the network can be isolated from traffic almost immediately by a local reaction of their neighbour nodes, which changes their traffic distribution patterns. If network admission control has been done carefully, the QoS specifications will still be fulfilled and the user may not even note the event.

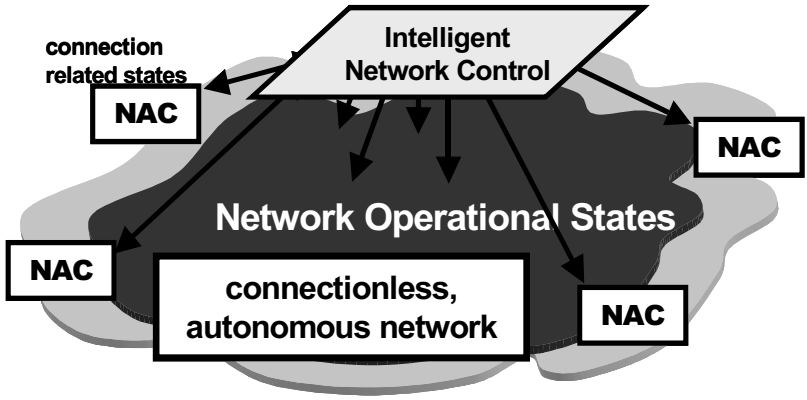

Fig. 4. Basic architecture of an autonomous, connectionless network domain

An intelligent control system can be put on top of this network domain. This control system takes the role of a network supervisor in terms of collecting information from the network and providing necessary corrective instructions, e.g. changes of strategies or parameters, to the NACs and the network nodes. Fig. 4 illustrates the basic architecture of this type of almost autonomous network domain, that should easily scale for new service and application demands (no user traffic related states in the core) and signifcantly reduce the operational cost for the operator (autonomous operation and adaptation to changing network/traffic conditions). For security and serviceability no extraordinary impacts are expected.

6 Conclusion

The Next Generation Network concept as a future high speed public network infrastructure has been introduced. Its origin and its operational environment have been described and the key requirements towards ‘carrier grade’ NGN solutions have been discussed. A related overall network architecture with its constraints and

interfacing issues has been presented and some requirements for standardization have been derived. Finally, a proposal for a possible NGN domain architecture has been presented. The proposal, based on a connectionless IP core, appears quite promising with respect to the overall requirements. We are performing further work in order to elaborate and prove the feasibility of this approach.

References

1. Händel, R., Huber, M.N., Schröder, S.: ATM Networks. Concepts, Protocols, Applications. Addison-Wesley (3rd Edition, 1998)
2. ITU-T Recommendation I.150: B-ISDN Asynchronous Transfer Mode Functional Characteristics (Geneva, 1991; revised Helsinki, 1993; Geneva, 1995)
3. Comer, D. E: The Internet Book. Everything you need to know about computer networking and how the Internet works. Prentice Hall International, Inc. (1995)
4. Krol, E.: The Whole Internet User's Guide & Catalog. O'Reilly & Associates, Inc., 2nd Ed. (1994)
5. Roberts, Lawrence G.: Internet Traffic Measurement 2000 and 2001. Keynote address at Metropolitan Communications Conference, San Francisco (January, 16th, 2002) (http://www.cibcwm.com/conferences/metrocomm/)
6. Internet Engineering Task Force, IETF (http://www.ietf.org)
7. IETF RFC 2210: The Use of RSVP with IETF Integrated Services (1997)
8. IETF RFC 2475: An Architecture for Differentiated Services (1998)
9. IETF RFC 1889: RTP: A Transport Protocol for Real-Time Applications (1996)
10. IETF RFC 1890: RTP Profile for Audio and Video Conferences with Minimal Control (1996)
11. Telecommunications and Internet Protocol Harmonization Over Networks, TIPHON (http.//www.etsi.org/tiphon)
12. ETSI TIPHON Documentation: Release 3 (http://portal.etsi.org/tiphon/Marketing_Release3.asp)
13. There is a plenty of literature on TCP/IP and its recent implementations. The original document is IETF RFC 793: Transmission Control Protocol (1981)
14. IETF RFC 768: User Datagram Protocol (1980)
15. Hall, E.A.: Internet Core Protocols: The Definitive Guide. O'Reilly & Associates, Inc. (2000)
16. The original document on the Internet Protocol is IETF RFC 791: Internet Protocol (1981). A good summary on the recent status is given in [15].
17. IETF RFC 2702: Requirements for Traffic Engineering over MPLS (1999)
18. Davie, B., Rekhter, Y.: MPLS. Technology and Applications. Academic Press, San Diego (2000)