

**NGN**

Next Generation Networks  
What is New?

Klaus Rebensburg

---

---

---

---

---

---

---

---

**Ein Netz für alles durch Konvergenz!**

Quelle: 423

2

---

---

---

---

---

---

---

---

3

---

---

---

---

---

---

---

---



## QoS in diesem Zusammenhang (Wikipedia)?

**Quality of Service** = ordnungsgemäßes Funktionieren zusammenwirkender Komponenten eines Nachrichtennetzes. Qualitäts- und Fehlerparameter erfassen, aufzeichnen, mit denen der Betrieb der Technik laufend überwacht und ggf. gesteuert wird

QoS = Gesamtheit der Qualitätsmerkmale eines Telekommunikationsnetzes aus der Sicht der Benutzer eines bestimmten Dienstes.

**Verkehrsgüte Vermittlungstechnik** - gemessene und gewichtete Zählungen von Ereignissen:

- Falschverbindung: eine Verbindung, bei richtig eingegebener Rufnummer falscher Teilnehmer
- Doppelverbindung: eine Verbindung, mit Zuschaltung anderer Anschlüsse
- vorzeitige Trennung: Trennen einer Verbindung, ohne dass Rufer oder Angerufener das wollen
- keine Auslösung: Andauern einer Verbindung, obwohl die "Auslösung" verlangt wurde
- Zählstörung: unrichtige Erfassung der gebührenrelevanten Parameter einer Verbindung

**Verkehrsgüte** (engl.: grade of service), der von der jeweiligen Bemessung der Betriebsmittel

- abhängige und quantifizierbare Teil der QoS (Wartewahrscheinlichkeit, mittlere Wartedauer, Verlustwahrscheinlichkeit, Übertragungsgüte).
- **Blockierung**: der Zustand eines Netzes, in dem ein Verbindungsaufbau nicht zu Ende geführt werden kann, weil erforderliche technische Einrichtungen oder Ressourcen nicht verfügbar sind.
- **Verzug von Signalen der Verbindungssteuerung**: Beispiel: Zeitspanne zwischen den Signalen "abgehender Ruf" (Hörer ausgehängt) und "Wahlauflorderung" (Wählton) ist zu hoch

• **Sendungsverzug**: Zeitspanne, die zwischen dem Beginn der Eingabe am Ursprung und dem Beginn der Ausgabe am Ziel vergeht

Verkehrsgüte eines Nachrichtennetzes abhängig von der Bemessung der Anzahl von Leitungen (Kanäle) und

- Steuereinrichtungen.
- Im Telefonnetz sind die Vermittlungsstellen die Steuereinrichtungen,
- im Internet sind es die **Router**.

7

---

---

---

---

---

---

---

---

---

---

## NGN versus heutige Netzwerke

Der technologische Unterschied

- Abkehr von **Switch-basierten Netzen** zu paketvermittelnden IP Netzwerken. Für **Kommunikationsdienste-Anbieter** der aufwändige Vollzug eines Paradigmenwechsels in ihrer Infrastruktur.
- Übergang von **Hardwareintelligenz** zu flexibler **Softwareintelligenz**
- **Änderung** Bandbreite, Qualität und Anwendung im Verlauf einer Verbindung
- Trennung von Diensten / Anwendungen und Transportnetz
- Einführung von wenigen zentralen Call Servern und Ressourcen Managern
- **Freie Wahl des Nutzers** bezüglich der Transportnetze und der Anwendungen bei gleichzeitiger Möglichkeit, über **alle Transportnetze** auf **alle Services** und **Angebote** zugreifen zu können
- Weitgehende **Mobilität** des Nutzers an beliebigen festen Orten und/oder beweglichen Orten mit beliebigen Endgeräten alle Dienste/Angebote in Anspruch nehmen zu können
- Möglichkeit, **neue**, bisher unbekannte **Dienste** dem Kunden anzubieten

8

---

---

---

---

---

---

---

---

---

---

## ITU Forderungen zu genereller Mobilität

- **Unbeschränkter Zugriff** von Nutzern auf unterschiedliche Service Provider
- **Unterschiedliche Identifikations Schemata**, die auf IP Adressen aufgelöst werden zum IP Routing
- **Unified Service Charakteristika** für gleiche Dienste, wählbar durch den Teilnehmer
- Konvergenz der Dienste von **mobilen** und **festen** Netzen
- **Unabhängigkeit** der Service-bezogenen Funktionen von unterliegenden Transport Technologien
- Kompatibel zu Regularien hinsichtlich **Notfall Kommunikation** und **Sicherheit/Privacy**.

9

---

---

---

---

---

---

---

---

---

---

## ITU zum Packet-based Transfer

- Trennung von Kontrollfunktionen in Bearer Capabilities, Call/Session, Application/Service
- Service Provision **getrennt** von Netzwerk und offenen Schnittstellen
- Bausteine für Dienste, Anwendungen und Mechanismen (Real Time, non-Real Time Dienste und Multimedia)
- Breitband mit **Ende zu Ende QoS** und Transparenz
- **Interworking** mit herk. Netzen über **offene Schnittstellen**

10

---

---

---

---

---

---

---

---

## Lebensgefah? Gut behütet?

- Verschiedene Sichten:



11

---

---

---

---

---

---

---

---

## Unterschiedliche Interessenlagen



- **Traditionelle Festnetz Betreiber und Telefonanbieter** möchten Netz, Netzmanagement und Dienste weiterhin verkoppelt sehen
- Die **Mobilfunk Branche** möchten ihre 3G-Struktur (IMS) und ihre Mobilität durchsetzen
- Die **Internet Gemeinde** sieht keine Notwendigkeit für NGN, da sie auf ihre RFC Selbstorganisation vertraut
- **Breitband Provider** sehen ihre **Kabelnetze** als die Kommunikations- und Informationsplattform der Zukunft auch ohne NGN
- **Systemhersteller** wollen mit möglichst wenig Geräten den gesamten Markt bedienen
- **Endgeräte Hersteller** benötigen einheitliche und leistungsfähige Netz- und Applikationsschnittstellen, um einen großen Markt mit wenigen Gerätetypen bedienen zu können.
- **Dienste Anbieter** wünschen sich eine stabile, preiswerte Transportplattform, auf der sie unabhängig vom Betreiber per Software schnell und mit wenig Aufwand immer neue Produkte generieren und anbieten zu können.
- **Nutzer** möchten über schnelle Netzwerkzugänge alle Angebote bei garantierter Qualität überall nutzen

12

---

---

---

---

---

---

---

---

## NGN Elemente

- Next/New Generation Dienste (NGN) sind enthalten u.a. in Kommunikationslösungen für Netzbetreiber, Diensteanbieter und Unternehmen, damit diese für ihre Kunden oder Mitarbeiter u.a. Sprach-, Daten- und Video-Anwendungen bereitstellen können (Triple Play)
- Anforderungen von NGN: Integrationsfähigkeit untereinander + mit bestehenden IK Infrastrukturen,
- Beteiligt sind u.a. jede Art von IP/VoIP/AlloverIP-Diensten, H323, verkabelte und drahtlose Punkt-zu-Punkt- sowie Punkt-zu-Multipunkt Videokonferenzen, Bezahlsysteme, Prepaid Services und Parlay Gateways
- Elemente einer Breitband Infrastruktur, die mehrere dieser Dienste realisieren sind z.B. Media Gateway Controller, Session Controller, Border Controller, etc.,
- Aktuell wird auch die Einbeziehung mobiler Kommunikations-Infrastrukturen in Festnetzkonzepte Teil der NGN Bewegung
- Ein besonderer Problembereich sind umfassende Sicherheitsmechanismen der Kommunikation end-to-end, unter Berücksichtigung der Anwendungsfelder.

13

---

---

---

---

---

---

---

---

## Technische Anforderungen an NGN

- Paketorientiertes Kernnetz für möglichst alle Dienste,
- Quality of Service
- Offenheit für neue Dienste
- Trennung der Verbindungs- und Dienstesteuerung vom Nutzdatentransport
- Integration aller bestehenden, wichtigen Telekommunikationsnetze, vor allem der Zugangsnetze
- Application Server
- Multimedia-Dienste
- hohe Bitraten
- übergreifendes einheitliches Netzmanagement
- Mobilität
- integrierte Sicherheitsfunktionen.

14

---

---

---

---

---

---

---

---

## NGN - Fragestellungen unter Einbeziehung drahtloser Technologien

- Welche Technologien „gehören“ zu NGN?
- Welche Dienste sind vom ganzheitlichen NGN Ansatz betroffen?
- Welche Probleme der Interconnection müssen gelöst werden?
- Wie erreicht man globales Roaming quer über mehrere Technologien?
- Denkbeispiel: Wie lässt sich ein Notruf über NGN realisieren?
- Wie werden CoS-Anforderungen erfüllt?
- Welche Realisierungen weisen den richtigen Weg zur Entwicklung von NGN?
- Welche regulatorischen Randbedingungen gibt es, wie müssen sie verändert werden?
- Welche Architektur ist geeignet, diesen Ansatz zu tragen? (Referenz-Architektur und Referenz-Punkte, Plattform-Gedanke, Netzelemente)
- Konzeption von Servern im NGN?
- Erhalt der Evolutionsfähigkeit des Ansatzes (Parallele zu IN)
- Interworking zwischen NGNs und zur bestehenden Welt, neue Internet Routing Konzepte, angepasste Intranet Routing Konzepte
- Verkehrsbetrachtungen, Traffic Engineering, MPLS, IntServ, DiffServ
- Transportnetz-Aspekte
- Steuerprotokolle (Status von H.323, SIP, MGCP, MEGACOOP, BICC ...; Vergleiche z.B. SIP vs. H.323, MGCP vs. MEGACOOP)
- Best-Effort Optimierung
- Dienstqualitäten mit CoS, Quality of Services
- Sicherheitskonzepte und -Aspekte
- Netzmanagement, Charging, Payment usw.
- Stand der Standardisierung und Stellenwert, Vorprodukte
- Kosten/Nutzen aus verschiedenen Sichten (Betreiber, Kunde, FOTS Betreiber, GSM Betreiber) der Migration zu NGN (am Beispiel Telefonie)

15

---

---

---

---

---

---

---

---

## 40 Anforderungen an ein NGN

- Ein sehr umfassender Katalog der Anforderungen an ein NGN wurde von der Siemens AG zur Vorlage bei ITU SG13 (alle Rechte bei SAG) eingereicht.
- The NGN shall provide at least the following service capabilities: authorization, authentication, offline & online charging, location, policy control, presence, session handling, provision of the bearer, message based information exchange
- The NGN shall support real-time and non real-time communication services
- The NGN shall support peer-to-peer and client-server communication types
- The NGN shall support services like: voice, multimedia (audio & video, incl. streaming), multiparty communication such as conferencing, messaging services, gaming, Internet access
- Within an NGN it shall be possible to offer and support standardized and non-standardized applications
- The NGN shall support fixed-mobile convergence
- The NGN shall support capability negotiation of IP multimedia applications to identify and select the available media components and resources, QoS etc. of IP multimedia sessions
- The NGN shall enable rapid service creation and deployment using service capabilities.
- The NGN shall accommodate different types of access. Services and applications as well as session and call control shall be independent of the access type in use.
- The NGN shall support a variety of different access technologies, e.g. DSL, cable, Ethernet, WLAN, cellular radio access
- The NGN architecture shall functionally separate transport plane, session and call control plane, application plane and management plane
- The NGN shall provide a unique interface between call and session control plane and application plane for access to and control of applications, provided, e.g., via OSGPARLAY, CORBA, IN
- The NGN architecture shall be independent of the specific applications to be supported
- The NGN shall provide interworking with the PSTN/ISDN
- The NGN shall support seamless interworking with GSM/GPRS mobile networks
- The NGN shall support interworking with existing fixed and mobile voice and IP data networks, including PSTN, ISDN, 2G and 3G Mobile Networks and the Internet. This includes basic voice calls between NGN users and users in PSTN/ISDN
- The NGN shall allow for IP multimedia sessions using a variety of different media types
- The NGN shall allow for IP multimedia sessions involving one or more IP multimedia applications
- The NGN shall support roaming and nomadism of users and terminals. It shall therefore provide a framework that comprises registration for users, registration of terminals independent of an association to a user, user profiles and database for user profiles, management of user and terminal mobility
- Users attached to their home network shall have access to services provisioned by their home network operator and 3rd party service providers. Roaming users, i.e. users attached to a visited network, shall have access to services provisioned by their home network operator, the visited network operator and 3rd party service providers.
- The NGN shall provide mechanisms for seamless handover for roaming users
- An NGN shall provide security from network operator and user perspective
- An NGN shall provide the possibility to establish trust relationships with other networks and with users. This includes the capability of the network to authenticate and authorize a single user and another network. A user should have the possibility to authenticate the network.
- IP multimedia applications shall be provided in a secure manner
- The NGN architecture shall allow for operators to limit the visibility of the network topology to authorized entities

16

## 40 Anforderungen an ein NGN

- The NGN shall allow for a user to register with multiple terminals in parallel
- At any time the NGN shall be able to verify the identity of users and terminals
- Both telecom and Internet numbering and addressing schemes shall be supported by the NGN as user identities
- The NGN shall allow to have multiple user identities assigned to a single subscription
- Identities of NGN users, used e.g. for authentication, authorization and routing, shall be administered by the network operator and shall not be changeable by the user
- A user profile, i.e. a collection of user related data, shall be provided especially for and in support of authentication, authorization, service subscription information, subscriber mobility, location, charging
- The NGN shall support mechanisms for the network operator to guarantee the authenticity of a user identity presented for an incoming call to a user where the call is wholly within that operator's network
- The NGN shall be QoS enabled, provide end-to-end QoS within the network domain and support QoS across network domain boundaries
- The NGN shall provide mechanisms to negotiate QoS between networks users and applications
- The NGN shall allow operators to implement policy control for IP multimedia sessions
- The NGN shall support regulatory requirements especially with respect to emergency communications and lawful interception
- The NGN shall provide mechanisms that allow to present the identity of the connected party to the session originator
- The NGN network layer protocol shall be IP. Both, IPv4 and IPv6, shall be supported.
- The NGN architecture must not depend on the IP version used.
- The NGN shall provide mechanisms that allow a user to refuse an incoming session or accept only a subset of it
- The NGN shall support the negotiation to add or delete media components of IP multimedia applications during an IP multimedia session
- The NGN shall support the user initiated suspend and resume of an IP multimedia session
- The NGN shall allow the user to end an IP multimedia session at any time
- It shall be possible for the user or the network to identify an alternative destination for an IP multimedia session or individual media of an IP multimedia session.
- Redirection to alternative destinations may be initiated by the sending party, receiving party or the network on their behalf.
- The NGN shall support more than one IP multimedia session to be run by a user in parallel
- The NGN shall support activation of concurrent IP multimedia applications within IP multimedia sessions

17

## NGN bedeutet alles

NGNs haben den technischen Anspruch, spezifische Kommunikationsanforderungen von Anwendungen vielfältigster Art durch einen weltweiten, universellen Kommunikationsdienst befriedigen, basierend auf der Kopplung herkömmlicher Kommunikationsnetze und neuer Netztechnologien.

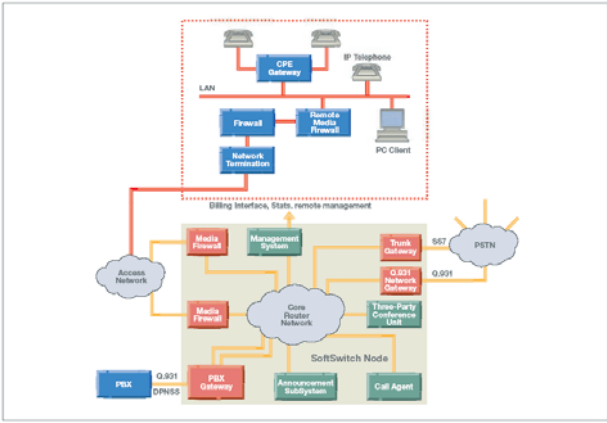
Universell heißt u.a. Unabhängigkeit vom

- Profil der Kommunikationsbeziehung sowie Art und Kombination der Medien:  
Multi-Service-Netz, Multimedia-Kommunikation, Multicastfähigkeit
- Typ des Endsystems  
Mensch oder Maschine mit fester, beweglicher oder bewegter Position
- Entfernung zwischen den Kommunikationspartnern

NGN (Next Generation Networks) bezeichnet ein Konzept und einen Rahmen für die Modifizierung herkömmlicher und die Entwicklung neuer Netztechnologien.

18

PSTN und IP - Softswitch: Quelle www.marconi.com




---

---

---

---

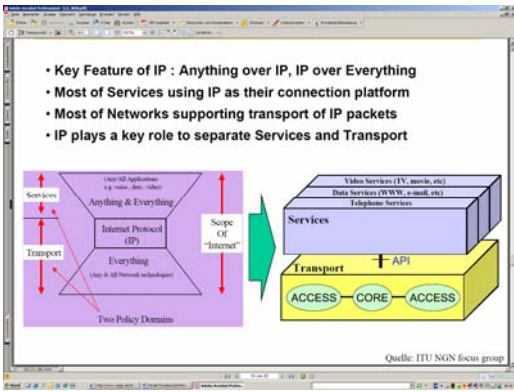
---

---

---

---

Trennung von Diensten und Transport



20

---

---

---

---

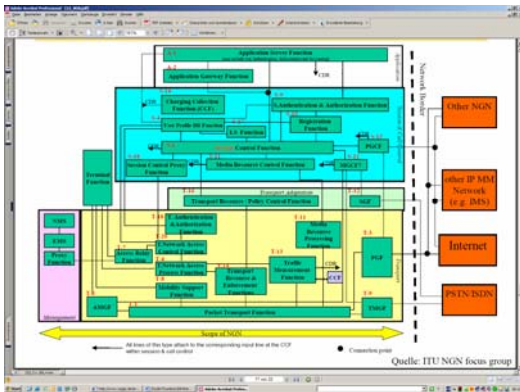
---

---

---

---

NGN Funktionelle Architektur



21

---

---

---

---

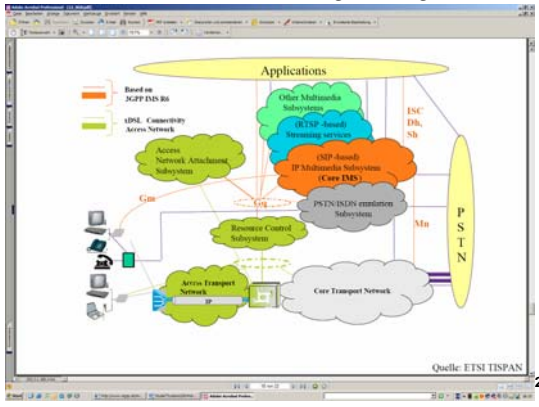
---

---

---

---

## NGN Architektur Diskussionsgrundlage ETSI



---

---

---

---

---

---

---

---

## Entspannung



- Durchhalten!!!

23

---

---

---

---

---

---

---

---

## SIP

- Session Initiation Protocol begleitet Verbindungen durch den Dschungel der Netze



24

---

---

---

---

---

---

---

---

## SIP Session Initiation Protocol 1

**SIP** der IETF im Gegensatz zu ITU-T H323 mit Blick auf das Internet orientiert sich an der Architektur gängiger Internet-Anwendungen. Dabei wurde von Beginn an auf leichte Implementierbarkeit, Skalierbarkeit, Erweiterbarkeit und Flexibilität geachtet.

- verwaltet beliebige Sessions mit einem oder mehreren Teilnehmern. Dabei nicht auf Internet-Telefonie beschränkt, sondern Sessions sind beliebige Multimediaströme, Konferenzen, Computerspiele
- Um jedoch ein Internet-Telefonat zu führen, braucht man mehr als nur SIP. SIP dient lediglich dazu, die Kommunikation zu ermöglichen – die eigentlichen Daten für die Kommunikation müssen über andere, dafür geeignete Protokolle ausgetauscht werden.
- Hierzu werden das [Session Description Protocol \(SDP, RFC 2327\)](#) und das [Realtime Transport Protocol \(RTP, RFC 1889\)](#) eingesetzt. [SDP](#) dient dazu, die zwischen den Endpunkten zu verwendenden Codecs, Transportprotokolle usw. auszuhandeln. Aufgabe von [RTP](#) ist es, den Multimedia-Datenstrom (Audio, Video, Text usw.) zu transportieren, d.h. die Daten zu kodieren, zu paketieren und zu versenden.

25

---

---

---

---

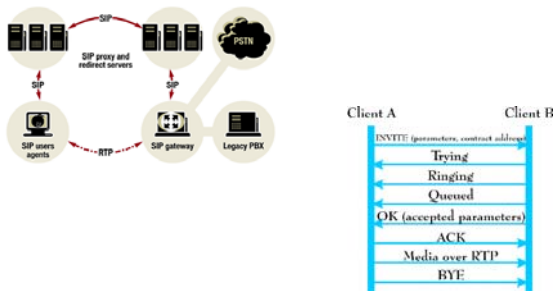
---

---

---

---

## SIP 2



26

---

---

---

---

---

---

---

---

## SIP 3

- SIP basiert unter anderem auf dem HTTP-Protokoll – es verwendet eine ähnliche Header-Struktur und ist ebenfalls ein textbasiertes Protokoll. Zur Schreibweise der Teilnehmeradressen wird das bereits von E-Mail bekannte Format benutzt: "sip:user@domain".
- Unterstützung findet SIP bereits in vielen Geräten diverser Hersteller und es scheint sich zum Standard-Protokoll zu entwickeln.
- SIP wurde auch vom 3rd Generation Partnership Project (3GPP) als Protokoll für Multimediaunterstützung im 3G-Mobilfunk (UMTS) ausgewählt.

27

---

---

---

---

---

---

---

---

## SIP Nachteile



- Zu den **Nachteilen** von SIP gehört, dass es zur Übertragung der Sprachdaten auf RTP zurückgreift.
- Die dafür verwendeten UDP-Ports werden dynamisch vergeben, was die Verwendung von SIP in Verbindung mit **Firewalls oder Network Address Translation** (NAT, RFC 2663) schwierig macht, da die meisten Firewalls bzw. NAT-Router die dynamisch vergebenen Ports nicht der Signalisierungsverbindung zuordnen können. Abhilfe für dieses Problem schafft der Einsatz von STUN (Simple Traversal of UDP over NATs), welches NAT-Router erkennt und umgeht, aber auch andere Protokolle wie IAX (InterAsterisk eXchange).
- Weiterhin sind auch viele Dienstmerkmale, die aus dem Festnetz bekannt sind, nicht im SIP-Protokoll selbst, sondern in **Erweiterungen** zum SIP-Protokoll definiert, so dass diese nicht von allen Endgeräten unterstützt werden. Im Gegensatz zu H.323 unterstützt SIP ausschließlich **Blockwahl**. Dies bedeutet, dass die Rufnummer erst in voller Länge gewählt werden muss und erst dann eine Verbindung aufgebaut wird.

28

---

---

---

---

---

---

---

---

---

---

## SIP-Telefone



**SIP-Telefone sind ein neuer Typ von Telefonen auf der Basis von Voice over IP und SIP.**  
Das Gespräch wird dabei in einzelnen Datenpaketen über das Internet versendet.

### Vorteilhaft bei diesem Service ist:

- Es lässt sich wie ein gewöhnliches Telefon bedienen und sieht auch so aus.
- Telefonate im Inland sind in der Regel sehr günstig, da die Daten über das Internet geleitet werden und nur ein sehr kurzer Abschnitt bei einem Anruf auf ein reguläres Telefon über das alte System läuft.
- Für Telefonate in das Ausland werden ebenfalls die weltweiten Datenetze genutzt. Daher sind in der Regel bei Auslandsgesprächen nicht mehr als die gleichen Preise eines deutschen Ortsgesprächs zu bezahlen.
- Innerhalb des gleichen SIP-Anbieters kann sogar weltweit kostenlos telefoniert werden.
- Die SIP-Technologie funktioniert weltweit. Der Anschluss wird beliebig auf der Welt immer unter der gleichen, sogar deutschen Telefonnummer erreicht. Beispiel: Für ein SIP-Telefon wird eine Telefonnummer für London zugeteilt. Das SIP-Telefon wird jedoch in Stuttgart in das Netz eingeklinkt. Wird diese Nummer in London angerufen, so wird der Anruf automatisch und kostenlos nach Stuttgart verbunden. Das SIP-Telefon klingelt in Stuttgart. Theoretisch könnte sich das Telefon auch in New York oder in Melbourne befinden und dort klingeln.
- Die wegen der IP-Technologien auftretenden **Qualitätsmängel** in der Sprachübertragung werden durch zusätzliche technische Maßnahmen abgemildert.
- Das Telefon funktioniert **unabhängig von einem Computer**. Mit Zusatz-Software kann jedoch auch über den Computer der freigeschaltete Anschluss genutzt werden.

29

---

---

---

---

---

---

---

---

---

---

## Entspannung!



- Durchhalten!

30

---

---

---

---

---

---

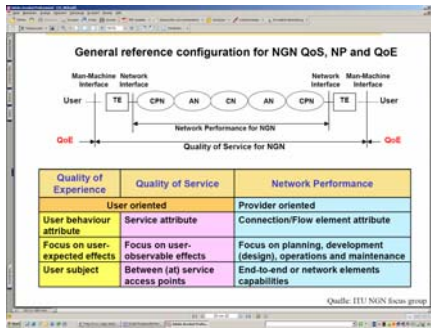
---

---

---

---

## NGN QoS



31

---

---

---

---

---

---

---

---

---

---

---

---

Noch 10!



- Entspannung

32

---

---

---

---

---

---

---

---

---

---

---

---

## NGN Security Motivation

### Motivation:

- Fortgeschrittene Multimedia (MM) Anwendungen wie Telefonie über paketbasierte Netzwerke, VoIP, interaktive (Video-) Konferenzen und Kollaboration, MM Messaging, Audio/Video Streaming und andere Anwendungen sind betroffen **von zahlreichen Sicherheitsbedrohungen** insbesondere in heterogenen Netzen. **Missbrauch, Böswillige Einmischungen in Kommunikation, Lauschangriffe und Denial-of-Service** Angriffe sind die größten heute bekannten Risiken paketbasierter IP Netzwerke.
- Nötig: Abgestimmte Maßnahmen und Konsens über gestufte Bewertungen hinsichtlich der Sicherheit und nachvollziehbaren Authentifizierung in den heutigen weltweiten Netzen insbesondere wegen der Heterogenität und der damit verbundenen Risiken

33

---

---

---

---

---

---

---

---

---

---

---

---

## Motivation durch Attacken 1

### Hindernisse der Network Address Translation

- Viele Unternehmen nutzen **Network Address Translation (NAT)** an der Grenze zwischen ihrem privaten Netzwerk und dem Internet.
- Das **NGN Session Initiation Protocol (SIP)** der IETF wird damit Teilnehmer lokalisieren und eine Verbindung aufsetzen, die wegen unterschiedlicher Strategien ohne einen verbindlichen Standard allerdings **nicht von allen Routern und Firewalls mit NAT weitergeleitet** werden kann.

### Angriffspunkt Session Initiation Protocol

- Das SIP selbst trägt ein Sicherheitsproblem in sich, SIP Messages bestehen aus **unverschlüsseltem Text** und sind daher leicht **abzufangen** und zu **fälschen**. Obwohl es SIP Sicherheitsoptionen gibt, so fehlt es doch an einer robusten Methode, Sicherheitsoptionen auf dem Kommunikationsweg **auszuhandeln**.
- Die Internet Engineering Task Force (IETF) widmet sich diesem **"man in the middle"** Problem und anderen grundsätzlichen Sicherheitsmechanismen.

### Angriffspunkt Reliable Transport Protocol

- Datenverbindungen und Transport werden in NGNs vom **Reliable Transport Protocol (RTP)** verwaltet. RTP ist **angreifbar hinsichtlich des Abfangens von Nachrichten und unbefugter Veränderung**, so zum Beispiel bei der **Sender und Empfängeradresse**. Ohne **Verschlüsselung der RTP Calls** ist NGN nicht in der Lage, Sicherheit zu bieten vor Identitätsdiebstahl oder Änderung der Protokollinhalte.
- Erste Spezifikationen schlagen ein **Interim Verschlüsselungsschema** vor, überlassen jedoch unteren Protokollschichten die zukünftige Absicherung der Kommunikation. Es gibt also keinen verbindlichen Standard für ein **sicheres RTP**.

34

---

---

---

---

---

---

---

---

---

---

## Motivation durch Attacken 2

### Code und Script Attacken

- IP Telefone, insbesondere ausschließlich auf Software basierende Telefone sind **angreifbar durch ausführbare Codeteile oder Scripts**. Diese können Userdaten oder Verbindungen, aber auch NGN Interfaces manipulieren oder dazu dienen, verteilte Attacken mit Denial of Service zu verbreiten.
- Missbrauch von Diensten wie **Umleitung** der Dienste zu Gunsten der Angreifer und Berechnung derselben auf Kosten anderer Teilnehmer.
- VoIP Dienste z.B. in Firmennetzwerken benötigen ebenfalls **Privacy** hinsichtlich einzelner Mitarbeiter, aber auch insbesondere hinsichtlich Bewahrung von Geschäftsgeheimnissen.
- **Software Upgrade Mechanismen**, insbesondere der Fernwartung, bedürfen aufwändiger Absicherung, besonders dann, wenn sie der Aktualisierung der Infrastruktur oder der Betriebssysteme dienen.
- Verschärft tritt dieses Problem bei **drahtlosen Technologien** auf.
- Latent sind immer Risiken vorhanden, wenn Scripts transportiert werden, die in **Extensible Markup Language (XML)** geschrieben sind.
- Die IETF **media gateway control standards** befassen sich speziell mit Absicherung.

### Transition zu einem sicheren NGN

- Annahme, dass 2010 ein Gipfel der Sicherheitsbemühungen für ein sicheres NGN erreicht ist und von sämtlichen Providern akzeptiert werden muss.
- eGovernment wird bis dahin eine Reife erreicht haben, so dass NGN Sicherheit unabdingbare **Forderung der Installationen im öffentlichen und privaten Bereich** sein wird.

35

---

---

---

---

---

---

---

---

---

---

## ITU Study Groups Security

- SG 17 Security
- SG 9 MM security für IPCablecom, CableHome Systeme und Heimnetzwerk Sicherheit
- SG 13 NGN Projekt mit Security Aspekten
- SG 4 Management Security
- SG 19 Sicherheitsaspekte mobiler Kommunikation und gesetzliches Abhören



36

---

---

---

---

---

---

---

---

---

---






---

---

---

---

---

---

---

---

---

---

### ITU SG13 NGN Arbeitsprogramm

- Prinzipien und funktionale Architektur NGN
- Anforderungen und Framework NGN
- Open Access Management und Netzwerkmanagement NGN
- NGN Mobilität und Konvergenz Fixed-Mobil
- Netzwerk und Service Interworking in NGN Umgebungen
- Service Szenarios und Installationsmodelle
- IPv6 und NGN
- Interoperabilität von Satelliten mit terristrischen und NGN Netzwerken
- Netzwerk Terminologien
- Frame Relay
- Public Date Networks
- Protokolle und Service Mechanismen für Multi-service-Data Networks (MSDN)

---

---

---

---

---

---

---

---

---

---

### Die Alternative? Zu SIP? ITU H.323

**H.323 ist eine übergeordnete Empfehlung der ITU-T H.323 Serie**

Protokolle für audio-visuelle Kommunikation auf paketvermittelten Netzwerken. Anwendungen wie NetMeeting und OpenH.323 (für Linux).

- H.323 behandelt auch die Kommunikation über öffentliche Telefonnetze und ISDN.

**IETF SIP Konkurrenz**

- Konkurrenz erhält H.323 durch das IETF SIP Protokoll, zunehmend für Signalisierungsaufgaben (wie zum Beispiel Rufaufbau, -abbau) eingesetzt.

**Gemeinsamkeiten, beide Protokolle für IP-Telefonie. H.323 auf Basis von ITU-T Protokolltechnologie**

- H.225, Rufsignalisierung, die Medien (Audio und Video), die Umwandlung des Datenstroms in Pakete, die Synchronisierung des Datenstroms und die Kontrolle des Nachrichtenformats.
- H.245, Nachrichten und Verfahrensweisen für das Öffnen und Schließen logischer Kanäle, die zur Übertragung von Audio, Video und Daten dienen; sowie den Austausch, die Kontrolle und Anzeige der Übertragungskapazitäten.
- H.450, zusätzliche Telefoniefunktionen, zur Abbildung von Leistungsmerkmale von ISDN auf IP
- H.323 nutzt etliche Protokolle, für die Lizenzgebühren bezahlt werden müssen. Als Alternative können Entwickler OpenH323 nutzen, das unter der MPL (Mozilla Public License) steht – siehe <http://www.openh323.org/>.

---

---

---

---

---

---

---

---

---

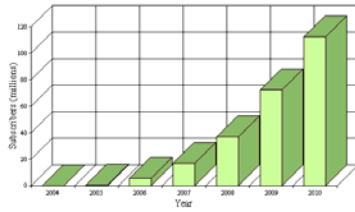
---



## Entwicklung NGN



NGN and 4G Subscribers



46

---

---

---

---

---

---

---

---

## CAT CARRIER

Whether you have an exuberant 'Tom' or just a kitten, you need our new **TABBY TOTE**™ feline transportation system. A few extra turns of the stabilizer screw and your cat will be safely secured and unable to use your leg as a scratching post.



47

---

---

---

---

---

---

---

---

## Kurz vor dem Ende



48

---

---

---

---

---

---

---

---

## Referenzen

- IETF: [SIP Working Group](http://www.ietf.org/html.charters/sip-charter.html) (<http://www.ietf.org/html.charters/sip-charter.html>)
- IETF: [RFC 2543](#)
- IETF: [RFC 3261](#)
- DiffServ (Differentiated Services) 02/99 - Transport Area
  - An Architecture for Differentiated Services (RFC 2475)
  - Definition of the DS Field in IPv4 and IPv6 (RFC 2474)
  - Assured Forwarding PHB Group (RFC 2597)
  - An Expedited Forwarding PHB (RFC 3246)
- MPLS (Multiprotocol Label Switching) 1997 - Routing Area
  - Multiprotocol Label Switching Architecture (RFC 3031)
  - MPLS Support of Differentiated Services (RFC 3270)
- TEWG (Internet Traffic Engineering) 12/00 - Sub-IP Area
  - Overview and Principles of Internet Traffic Engineering (RFC 3272)
  - Draft: Requirements for Inter-area MPLS Traffic Engineering
  - Draft: MPLS Inter-AS Traffic Engineering requirements
- NSIS (Next Steps in Signaling) 03/02 - Transport Area
  - IP signalling protocol (RSVP simplified)
- Siemens: NGN Service Requirements. Submitted to the ITU SG13 JRG-NGN, Jan. 2004
- ETSI TISPAN: Summary and follow-up in TISPAN, Dec. 2003
- Open H.323: <http://www.openh323.org/>

49

---

---

---

---

---

---

---

---

## Bücher

- [Next Generation Networks](#) von Gerd Siegmund, Hüthig Telekommunikation (Mai 2002)
- [Next Generation Networks](#) von Hans-Jörg Schilder Vde-Verlag (Oktober 2002)
- Ulrich Trick, Frank Weber : SIP, TCP/IP und Telekommunikationsnetze
- [Next Generation Intelligent Networks \(Artech House Telecommunications Library\)](#) von Johan Zuidweg, Han Zuidweg Artech House Publishers (1. Oktober 2002)
- Trick, Ulrich; Weber, Frank: SIP, TCP/IP und Telekommunikationsnetze. Oldenbourg, 2004

50

---

---

---

---

---

---

---

---

## Referenzen

- [International Packet Communication Consortium](#) früher
- [International Softswitch Consortium](#)
- [Parlay/OSA](#) IN Dienste in NGNs
- [Suns JAIN](#) Java IN Dienste in NGNs

51

---

---

---

---

---

---

---

---