Karlsruher Institut für Technologie

Next Generation Internet
2. Internet-Architektur — Prinzipien und Entwicklung

INSTITUT FÜR TELEMATIK

Kapitelübersicht

I. Einführung
1. Einführung

II. Internet-Architektur
2. Internet-Architektur
3. NAT & IPv6
4. Dienstgüte

- 2.1 Wachstum und Skalierbarkeit
- 2.2 Entwurfsziele
- 2.3 Entwurfsprinzipien
- 2.4 Neuere Entwicklungen
- 2.5 Forschungsbedarf
- 2.6 Literatur

III. Multicast
5. Grundlagen
6. Multicast Routing
7. Multicast Transport

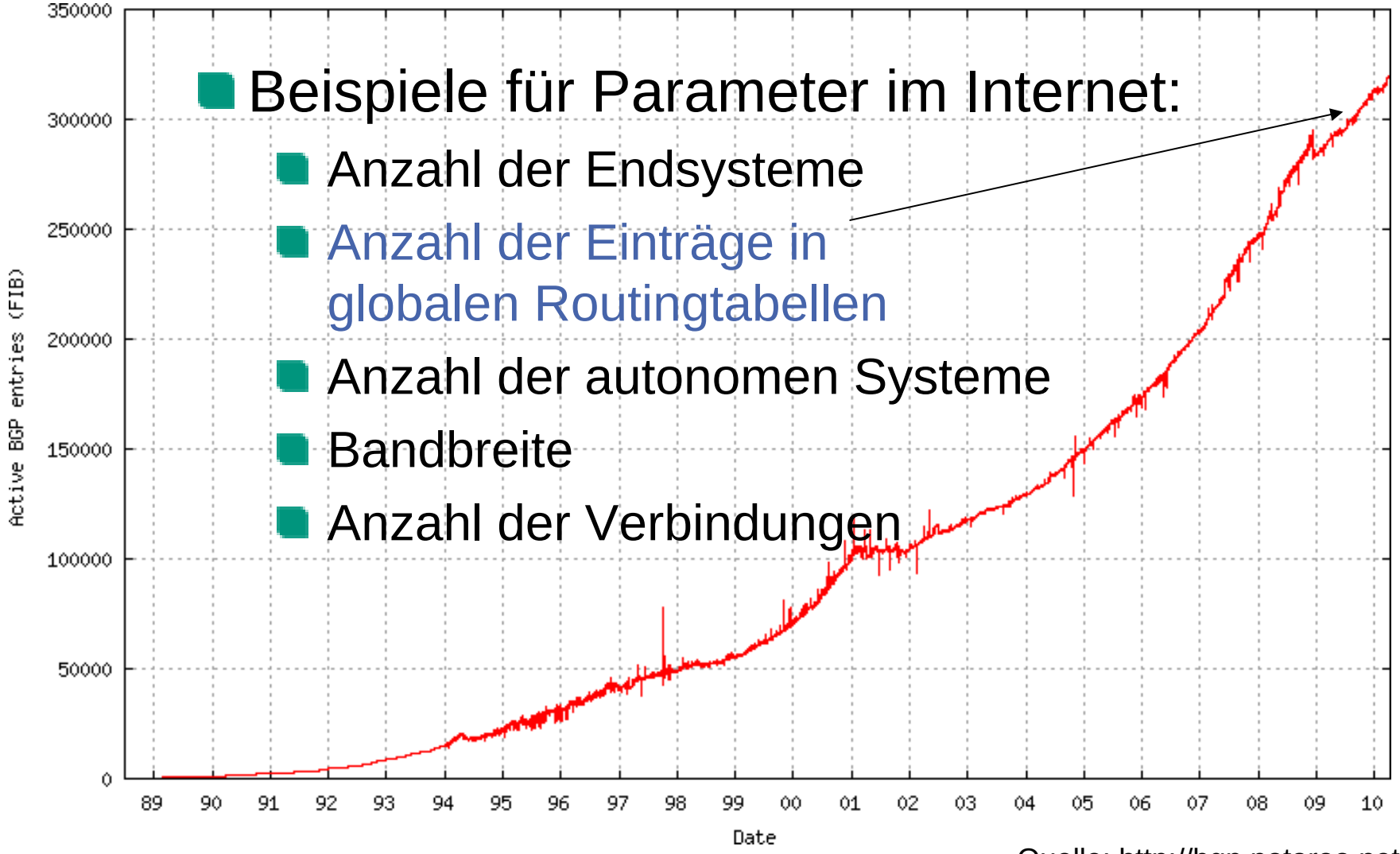
IV. Flexible Dienste und Selbstorganisation
8. Aktive Netze
9. Neuere Transportprotokolle
10. Peer-to-Peer

2.1 Wachstum und Skalierbarkeit

- Einzige Konstante im Internet: Ständige Veränderung
- Vor allem: Wachstum
- Technologischer Fortschritt bringt oftmals Steigerungen um Größenordnungen (z.B. Moore‘sches Gesetz, CPU, Bandbreite, Speicher)
- Generelle Frage: wie kommt das technische System damit klar?
  - Funktioniert es noch? Wie lange?
  - Nimmt die Leistung ab?

Beispiele: Wachstum im Internet

- Beispiele für Parameter im Internet:
  - Anzahl der Endsysteme
  - Anzahl der Einträge in globalen Routingtabellen
  - Anzahl der autonomen Systeme
  - Bandbreite
  - Anzahl der Verbindungen

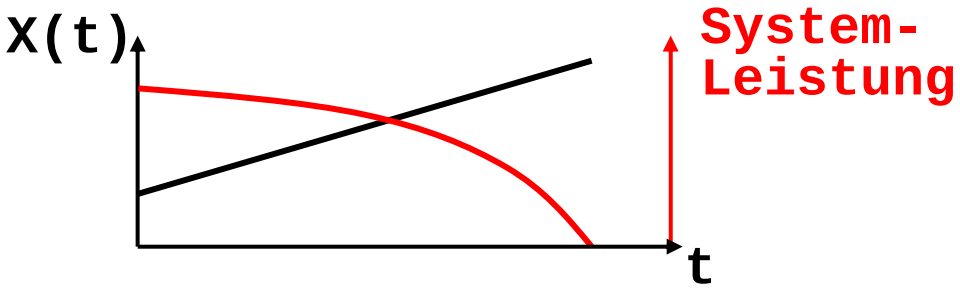


Quelle: http://bgp.potaroo.net

Bedeutung der Skalierbarkeit

- Das Internet hat das rasante Wachstum gut verkraftet
  → Es funktioniert noch!
  - Man sagt deshalb auch: es ist „skalierbar“?
  - Was bedeutet Skalierbarkeit?
- Begriff der Skalierbarkeit:

  Ein skalierbares System funktioniert auch bei starkem Wachstum (z.B. um mehrere Größenordnungen, d.h. über mehrere Skalen hinweg) bestimmter Parameterwerte des Systems
- Beispiel für keine bzw. schlechte Skalierbarkeit:



Skalierbarkeitsaspekte

- Skalierbarkeit bezieht sich auf bestimmte Systemparameter → welche berücksichtigen?
- Anwachsen um mehrere Größenordnungen betrachten, d.h. Steigerung um Faktor 10, 100, 1000, 10000, …
  → Funktioniert das System dann noch?
- Manchmal ist die Dynamik ein Problem
- Selbst lineares Wachstum bestimmter Parameter kann Problem sein!

2.2 Internet-Architektur: Entwurfsziele

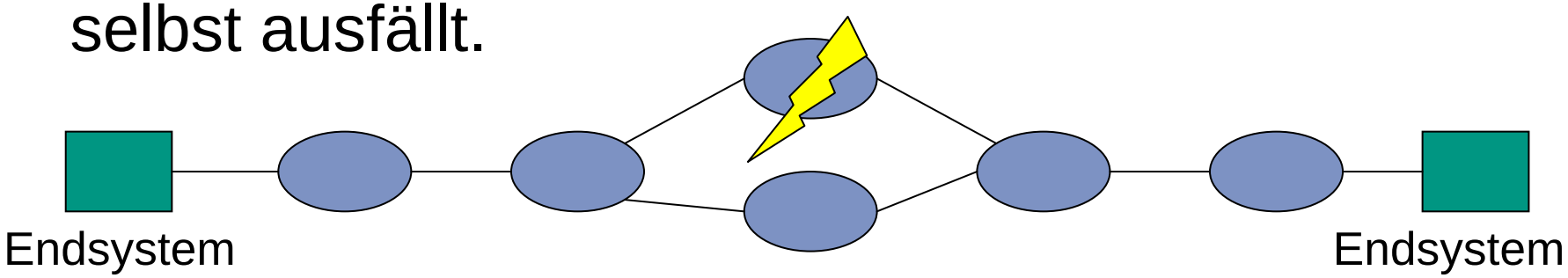
Paper von D. Clark *"The Design Philosophy of the DARPA Internet Protocols"* nennt:


[Clark88]

- Hauptziel: Internetworking, d.h. Verbinden existierender Netzwerke
- Weitere Ziele (in Reihenfolge der Wichtigkeit):
  - Robustheit
  - Unterstützung mehrerer Arten von Kommunikationsdiensten
  - Heterogenität: Berücksichtigung einer Vielfalt von Netzwerken
  - Verteiltes Management der Ressourcen
  - Kosteneffektivität
  - Anschluss von Endsystemen mit wenig Aufwand
  - Ressourcennutzung muss abgerechnet werden können

Robustheit gegen Ausfall

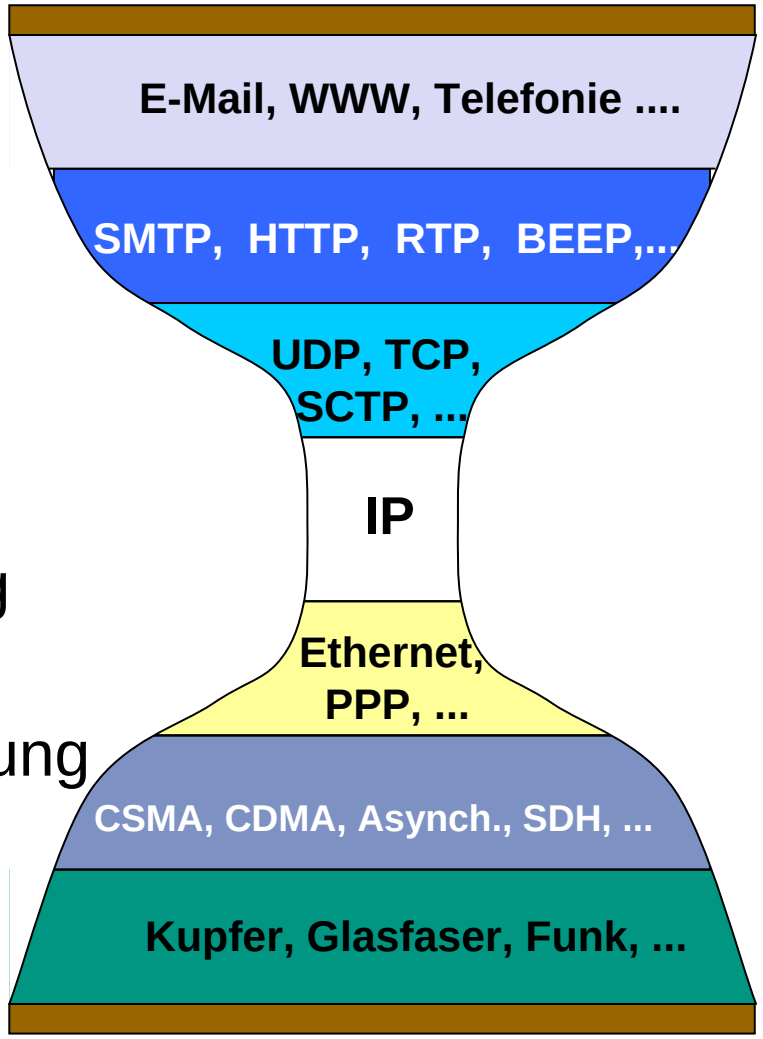
- „Fate-Sharing“: es ist akzeptabel Zustandsinformation, die mit einer Instanz assoziiert wird, zu verlieren, wenn die Instanz selbst ausfällt.



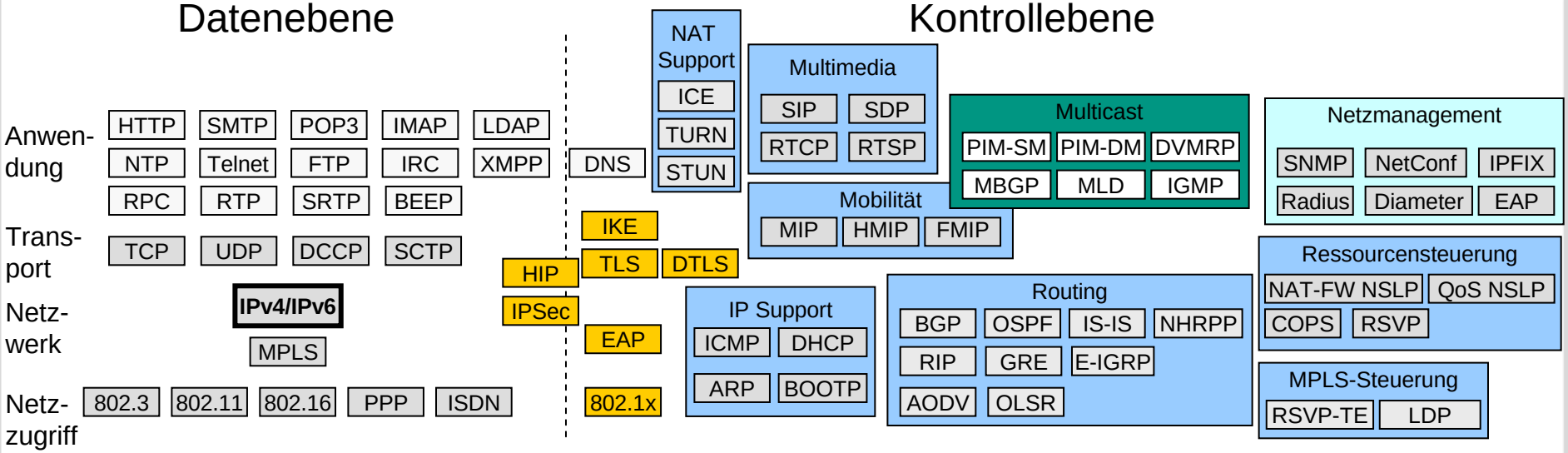
- Keinen Zustand im Netzwerk halten → stattdessen in den Endsystemen
- Datagramm-Konzept als Folge

Weitere Folgen

- Sanduhr-Modell
  - Einziges Protokoll
  - Globale Adressierung
  - Schlankes Protokoll
- Paketbasierte Kommunikation
  - flexibler als Leitungsvermittlung (weshalb?)
  - effizienter? → bessere Auslastung durch statistisches Multiplexing
  - schlechter abzurechnen



Schlanker Mittelteil?



- Kontrollprotokolle machen inzwischen einen Großteil der Gesamtkomplexität aus
- TCP/UDP + HTTP als neuer Mittelteil?

2.3 Entwurfsprinzipien: Ende-zu-Ende-Argument

- Welche Funktionalität wird benötigt?
- Wo sollen bestimmte Funktionen platziert werden?
  - In den Endsystemen/ Anwendungen?
  - Im Netzwerk?



[SaRC81]

- Wichtiges Entwurfsprinzip (erst 1981 explizit formuliert von Saltzer, Reed und Clark): Das Ende-zu-Ende-Argument (E2E argument)
  - Wissen und Hilfe der Anwendung notwendig → Funktionalität ins Endsystem
  - Keine anwendungsspezifische Funktionalität im Netz bereitstellen

E2E Argument – weitere Ziele/Folgen

- Innovationsschutz
  - Einfaches Hinzufügen neuer Dienste
  - Infrastruktur nur schwer zu ändern (vgl. Einführung Multicast, IPv6, ECN, usw.)
- Zuverlässigkeit und Robustheit
  - Gegen Ausfall und Fehlfunktion der Endsysteme und Netzwerkkomponenten
  - Wenn Netzkomponenten Zustand halten müssen, wächst Wahrscheinlichkeit für Verbindungsausfall mit zunehmender Netzgröße

Internet-Architektur: Prinzipien

- RFC 1958: „Architectural Principles of the Internet“
- Unabhängigkeit von Medium und Hardware-Adressierung


[RFC1958]

- Zustände (z.B. Routen, QoS-Garantien, Header Compression, ...) sollten „selbst-heilend“ sein
  - Adaptive Prozeduren und Protokolle zum Verwalten und Herleiten der Zustände
  - „Soft-State“-Konzept
  - Reduktion der Zustandsinformation auf Minimum (insbes. manuell konfigurierte Zustände)

RFC 1958 – Generelle Designpunkte

- Heterogenität
- Wiederverwendung bewährter Lösungen
- Skalierbarkeit
- Leistung und Kosten
- Einfach halten (keep it simple)
- Modularität
- Vermeide Optionen und Parameter wo möglich
  - verringern Usability und Interoperabilität
  - ansonsten: automatische Konfiguration und Aushandlung solcher Parameter
- Postel-Prinzip (s. ff. Folien)
- Zirkuläre Abhängigkeiten vermeiden

RFC 3439 – Richtlinien für Internet Backbone Provider

- "Some Internet Architectural Guidelines and Philosophy" (Ergänzung zu RFC 1958)

[RFC3439]

- Erfahrung: Große Netze sind anders zu konstruieren als kleine und mittlere Netze
  - Nicht-Linearitäten bei Architektur, Entwurf
    - Ursache: Verstärkungseffekt, denn kleine Ereignisse können große Wirkung zeigen, bis zur Instabilität (z.B. Resonanzverstärkung)
    - Beispiele
      - Tacoma Narrows Brücke

      - erhöhte Interkonnektivität im Internet führt zu komplexerer und langsamerer Konvergenz (z.B. Verteilung v. Routinginformation)
  - Gegenmaßnahme
    → lokale Änderungen rufen nur lokale Effekte hervor

Einfachheits-Prinzip (Simplicity Principle)

- Komplexität wird oft durch
  - Robustheitsanforderungen in unsicheren Umgebungen
  - sowie zusätzliche Komponenten, die über die normale Funktionalität hinaus erforderlich sind,

  erzeugt
- Komplexität verhindert effizientes Skalieren: erhöht monetäre und operationale Kosten
- Komplexe Systeme weisen oft schwer kontrollierbare Abhängigkeiten zwischen Komponenten auf → Kopplungsaspekte
- Daher Komplexität kontrollieren → einfache Lösungen suchen

Kopplungs-Prinzip

- Kopplungs-Prinzip
  - Wachsendes System
    → erhöhte Abhängigkeit zwischen Komponenten
  - Mehr Ereignisse gleichzeitig
    → Interaktion von Ereignissen wird wahrscheinlicher
    → Unvorhergesehene Wechselwirkung
- Beispiele
  - Routing Update Synchronisation
  - TCP Slow Start Synchronisation
  - Congestion Collapse
  - Ariane-5 Crash
  - AT&T SS7 Failure

[FlJa94]

[Jaco88]

[ESA96]

[Neum90]

Ariane-5

→ Synchronisation verhindern: permanent Zufall hinzufügen

Layering Considered Harmful

- Zahlreiche Mechanismen werden in verschiedenen Schichten wiederholt eingesetzt
  - Adressierung, Verbindungsaufbau, Fehlerkontrolle, Flusskontrolle, Fragmentierung
- Kapselung der Funktionen erschwert Optimierung
  - Es kann nur jede Schicht für sich optimiert werden
  - aber schichtenübergreifende Optimierung erhöht Kopplung zwischen den Schichten → verletzt Einfachheitsprinzip
- Zunehmende Schichtung und Abhängigkeiten zwischen den Schichten verletzten Einfachheitsprinzip
  - Reduktion der Komplexität am Beispiel IP Transport IP/ATM/SONET → IP/SONET/WDM → IP/WDM

Weitere Architektur-Richtlinien

Ebenfalls als gefährlich erachtet:

- Optimierung
  - erhöht meistens Komplexität, erzeugt engere Kopplung
- Überfrachtung mit Funktionen („Feature Richness“)
- Konvergenz-Schichten (z.B. IP over ATM)
- Universelles Interworking

Weitere Entwurfsaspekte

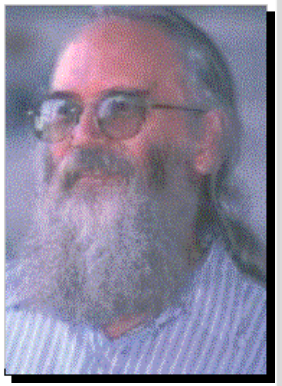
- RFC 3426 „General Architectural and Policy Considerations“
  - grundsätzliche Fragestellungen zum Protokoll-/System-Entwurf
  - keine Richtlinien, keine Checkliste
  - Diskussion und Erläuterung anhand zahlreicher Fallbeispiele (z.B. ECN)


[RFC3426]

- RFC 1122 „Requirements for Internet Hosts – Communication Layers“
  - gute Dokumentation und Diskussion der Entwurfsentscheidungen


[RFC1122]

Postel-Prinzip



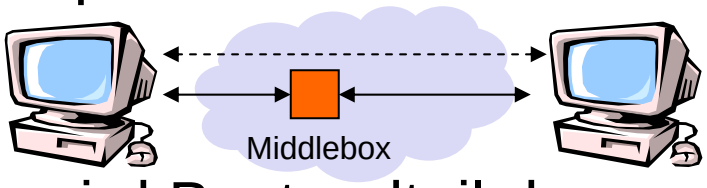
- Robustheitsprinzip (Jon Postel, siehe auch http://www.postel.org):
  "Be liberal in what you accept, and conservative in what you send" [RFC1122]
  - Software sollte auf jeden – auch wenn noch so unwahrscheinlichen – Fehler angemessen reagieren können
  - Eingehendes Paket kann beliebige Kombination von Attributen sowie Fehler enthalten
  - Annahme mutwilliger/böswilliger Erzeugung solcher Pakete

2.4 Neuere Entwicklungen (1)

- Viele Aspekte haben sich seit Anbeginn des Internets geändert
- „Bedrohungen“ für das Ende-zu-Ende-Argument?
  - Vertrauensverlust zwischen Endsystemen
    → Einführung von Sicherheitstechniken


[RFC3724]

  - Middleboxes (Proxies/NATs/Firewalls/Caches/...)
    → Bruch des Ende-zu-Ende-Prinzips
    (insbesondere bzgl. Sicherheitsmechanismen)



  - Neue Dienstmodelle: Dienstgüte wird Bestandteil des Dienstes (Streaming A/V) → Server werden verteilt und näher zum Nutzer platziert (z.B. Akamai, Realnetworks...)

Neuere Entwicklungen (2)

- Beispiel: negative Effekte durch Sicherheitstechniken
  - Rigoroses Filtern von ICMP-Paketen: kein PATH-MTU-Discovery
  - Filtern von Paketen mit gesetzten ToS-Bits: verhindert Explicit Congestion Notification
  - Private Adressierung in „Intranets“: Einschränkung der Erreichbarkeit und verfügbarer Dienste
- Mögliches Vorgehen für zukünftige Mechanismen, die scheinbar gegen das Ende-zu-Ende-Prinzip verstoßen: Zerlege E2E-Argument in Bestandteile
  - Innovationsschutz
    - Einführen neuer Mechanismen in Endsystemen einfacher
  - Zuverlässigkeit/Robustheit und Vertrauen
    - Sicherheit hinzufügen, wo nötig

Verlust der Internet-Transparenz

- Internet-Transparenz:  [RFC2775]
  - ursprüngliches Konzept eines einzigen universellen, logischen Adressierungsschemas
  - Mechanismen, durch die Pakete im Wesentlichen unverändert von Quelle zu Ziel fließen
- Verlust der Transparenz durch:
  - Intranets („Sicherheit“, Einschränkung der Anwendungen und Adresstransparenz, Netzadministrator hat Kontrolle)
  - Private Adressen (nicht eindeutig, Einschränkung der Erreichbarkeit und globalen Kommunikation)
  - Freiwillige Isolation (z.B. WAP-Proxies) und Partner-Netzwerke
  - Middleboxes:
    - Firewalls (Einschränkung Dienste und Erreichbarkeit)
    - Network Address Translators (NATs)
    - Application Level Gateways, Proxies, Caches
  - Dynamische Adressen (SLIP/PPP, DHCP)
  - Split-DNS
  - Tricks zum Lastausgleich

Tussle in Cyberspace

 [CWSR02]

- Früher: gemeinsames Ziel der Internetgemeinde
- Heute: Kampf um Interessen verschiedener Parteien
  - Musiktauschbörsen ↔ Musikindustrie/Rechteinhaber
  - Private Konversation ↔ Abhörmöglichkeiten für Regierungen
  - ISP Interconnection ↔ ISP-Konkurrenz
  - Nutzer in Regierungs- und Firmennetzen durch Firewalls abgeschottet → Nutzer suchen Auswege (Tunneln, externe Zugänge, andere Routen, ...)
  - ISPs weisen nur eine öffentliche IP-Adresse zu → Nutzer schließen ganze Netzwerke darüber an

Tussle in Cyberspace: Neue Prinzipien

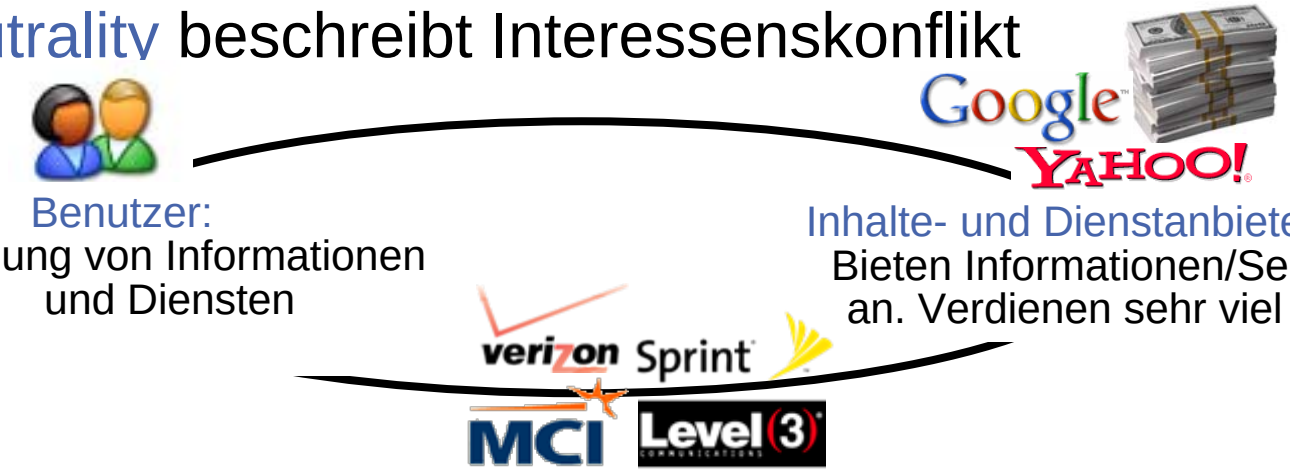
- Systemdesign sollte Spielraum bzgl. Nutzungs-möglichkeiten erlauben
  - unterschiedliche Möglichkeiten je nach Interessen
  - Konflikte sollten innerhalb des Systemdesigns ausgetragen werden und dieses nicht verdrehen oder verletzen
- Neue Prinzipien
  - Modularität entlang von Konfliktgrenzen
    - → Konflikte können keine Auswirkungen auf andere Bereiche haben
  - Berücksichtigung von Wahlmöglichkeiten innerhalb des Designs
    - → Je nach Bedürfnis der Parteien
    - Beispiel: Wahlmöglichkeit für die Interaktionspartner (z.B. Konfiguration der bevorzugten SMTP-, POP-, News-Server), aber: schlecht für naive Nutzer

Tussle in Cyberspace: Aspekte der Konflikte

- Lösung erfordert offene Schnittstellen (ermöglicht auch Wettbewerb)
- Sichtbarkeit der Wahlentscheidung (direkt oder indirekt über die Auswirkungen)
- Gegensätzliche/sich ergänzende Interessenskonflikte: Synergie: Vergütung von Diensten (Geld o. andere Werte)
- Konflikte dauern an, entwickeln und verändern sich
- Prinzip:
  Der Entwurf von Erweiterungen sollte eine Analyse beinhalten, welche Interessenskonflikte auftreten können und wie mit diesen umgegangen werden kann. Oftmals kann Wettbewerb richtungsweisend sein.

Net Neutrality – Netzneutralität

- Net Neutrality beschreibt Interessenskonflikt



[Crow07]

- ISPs/Netzbetreiber transportieren Verkehr, mit dem andere sehr viel Geld verdienen
- ISPs wollen auch daran partizipieren
  - Idee: Google-, E-Bay-, Amazon-, YouTube-Inhalte nur noch über ISP erreichbar, wenn dieser von den Anbietern entsprechend bezahlt wird.

Net Neutrality – Folgen

- Grundsatzfrage:
  Dürfen ISPs/Netzbetreiber Verkehr, den sie transportieren, beeinflussen?
  - Beispielsweise mittels Priorisierung, Filterung von Verkehr (z.B. kein VoIP-Verkehr via UMTS, kein P2P-Verkehr mehr)?
  - Probleme:
    - Bestimmte Inhalte dann nur noch über bestimmte Netzbetreiber (gut) zugänglich (YouTube-Zugang wird mit DSL-Anschluss von Betreiber X gekoppelt)
    - Neue Anwendungen und Dienste werden gehindert
    - Kleine Inhalteanbieter haben das Nachsehen
- Ziel der „Net Neutrality“-Bewegung
  - Erhaltung der Netztransparenz: Alle Pakete, Inhalte und Dienste müssen gleichberechtigt im Internet transportiert werden. Keine Diskriminierung!
  - Kein Blockieren
    - von legalen Inhalten und Anwendungen
    - rein aus Netzbetreiberinteressen

Net Neutrality – Lösungen

- Regulierung durch Gesetzgeber?
- Eingriffe seitens des Netzbetreibers
  - sinnvoll wenn es z.B. um Sicherheit geht
  - wenn es um intelligentes Ressourcenmanagement geht → Dienstgüteunterstützung
    - aber wenn möglich: nicht-diskriminierend gegenüber bestimmten oder einzelnen Anwendungen
  - sollten offengelegt und nicht willkürlich sein
- Kontrolle sollte auf Nutzerseite liegen
  - Vorgabe, wie bestimmte Daten behandelt werden sollen, z.B. Priorisierung oder explizite Dienstgütesignalisierung

Routing und Adressierung

- Routingtabellen wachsen zu stark
  - Site-Multi-Homing
  - Traffic-Engineering
  - Provider-unabhängige Adressen (nicht aggregierbar)

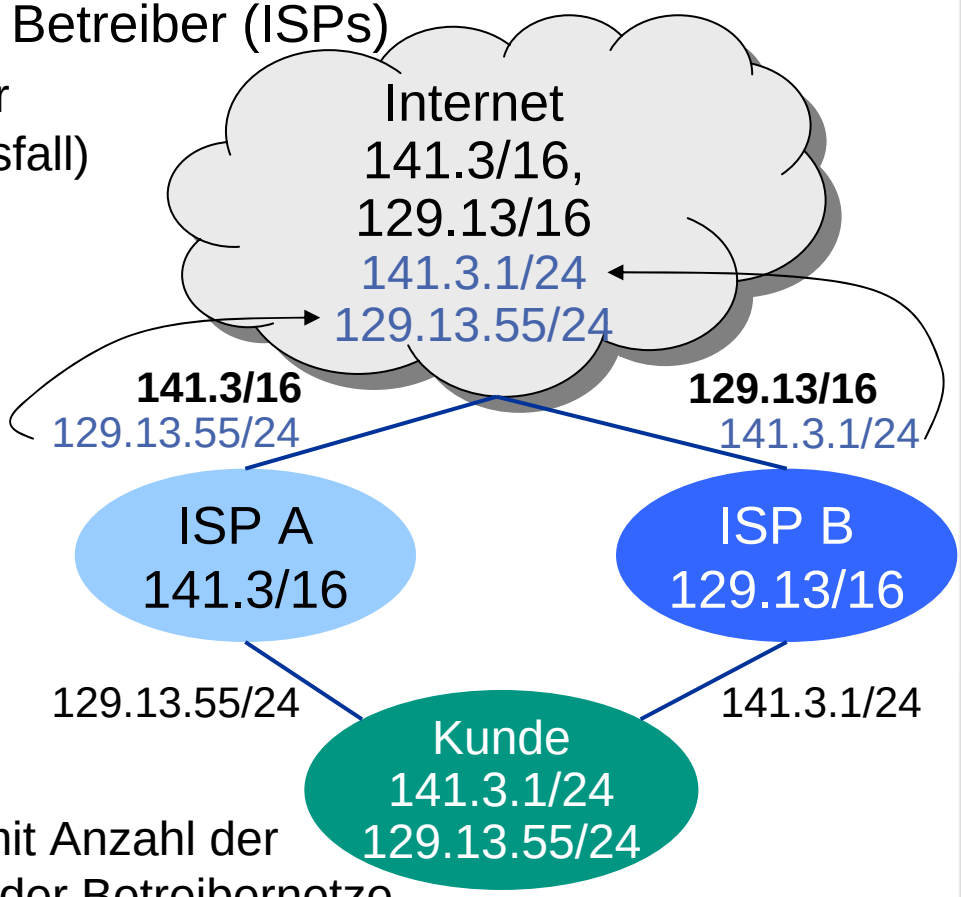
 [RFC4984]

- Architektur nicht auf Bedürfnisse ausgerichtet
  - Endkunden wollen
    - Multi-Homing
    - Kein Umnummerieren von IP-Adressen bei Providerwechsel
    - Provider-unabhängige Adressen
  - Provider wollen
    - Kontrolle über Datenverkehrsfluss
    - Kleine Routingtabellen

Site Multi-Homing

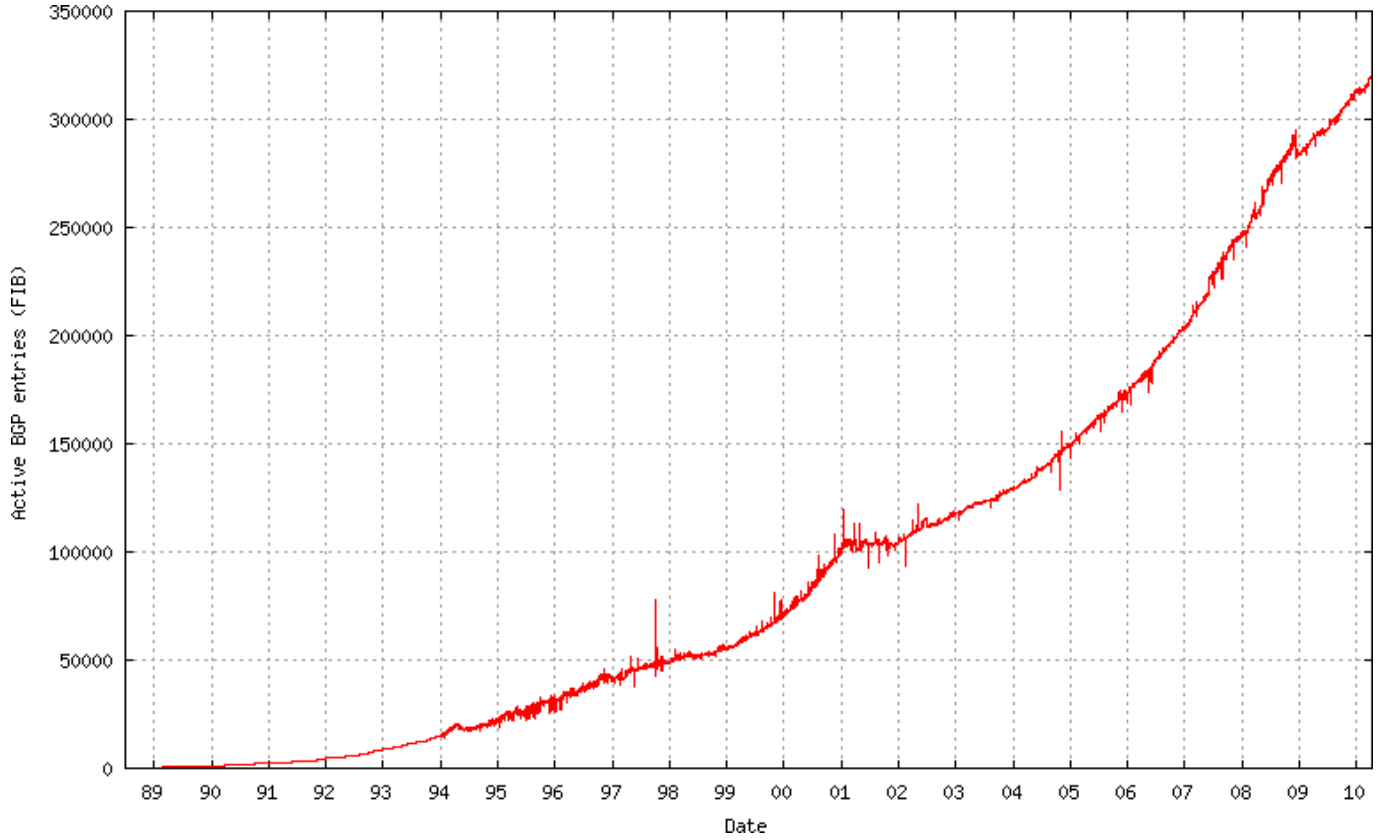
- Abhängigkeit vom Internet wird zunehmend größer
  → zuverlässige Konnektivität wichtig
- Internet-Anbindung über mehrere Betreiber (ISPs)
  - Verbesserte Toleranz gegenüber Ausfällen (einschließlich ISP-Ausfall)
  - Lastverteilung
- Situation heute:
  - Kundennetz hat zwei oder mehr Netzadressen

  oder
  - Kunde hat Betreiber-unabhängige Netzadresse
- Problem:
  - Routen-Aggregation unwirksam
  - Globale Routingtabelle skaliert mit Anzahl der Kundennetze anstatt mit Anzahl der Betreibernetze



Routingtabellenwachstum

- Folge: starkes Wachstum der Routingtabellen [RFC4984]
- Prognose: Leistungssteigerung durch Hardware reicht nicht zur Kompensation



Identifikator/Lokator-Problematik

- Im Internet beinhaltet die IP-Adresse derzeit zweierlei:
  - Identifikation des Endsystems (Identifikator) als auch die
    - globaler Adressraum
  - Lokation des Endsystems (Lokator)
    - Adresse beinhaltet topologische Information für das Routing
- Diese Eigenschaft erschwert u.a.
  - Mobilität des Knotens
  - Multi-Homing
- Globale Adressierung überhaupt notwendig?
  - oftmals haben Netze nur beschränkten Geltungsbereich
- Ansonsten Abbildung ID → Lokator erforderlich
  - Dynamik und Komplexität im Mapping-System?
  - Aktuelle Arbeiten in der IRTF Routing Research Group

Ansatz LISP

[FFLM09]

- Möglichst wenig Veränderungen, keine Änderungen in den Endsystemen
- Trennung von Endpoint Identifier (EID) und Routing Locator (RLOC)
  - EID auch als Präfix organisiert, entspricht praktisch PI-Präfix
  - RLOC: heutige PA-Präfixe, aggregierbar
  - LISP: Locator/ID Separation Protocol
- Abbildungsfunktion EID-Präfix → RLOC erforderlich
- Endsystem schickt Datenpaket an Ziel-EID
  - Ingress Tunnel Router fügt Tunnel-Header mit RLOCs hinzu (wenn Abbildung bekannt)
  - Egress Tunnel Router entfernt Tunnel-Header wieder
- Probleme
  - spiegelt die Abbildung die aktuelle Erreichbarkeit wider?
  - Problem in das Mapping-System verschoben?

Content Centric Networking

- Paradigmenwechsel [JSTP+09]
  - bisher Kommunikation = Konversation zwischen zwei Endpunkten

  - geänderte Nutzung durch das Web
  - jetzt: Konzentration auf Inhalte
    - Interesse an bestimmten Inhalt → egal wie Inhalt transportiert wird
    - Integrität und Authentizität der Daten wichtig!
      → anderes Sicherheitskonzept
- Einbeziehung von Speichermedien
  - Transport über die Zeit
  - ermöglicht asynchrone Nutzung, Caching usw.
- Namensstruktur hierarchisch
  - z.B. /parc.com/people/van/presentations/FISS09

Staukontrolle

- Derzeitige Verfahren nicht gut für hohe Geschwindigkeiten oder hohe Latenzen geeignet
  - AIMD zu konservativ für hohe Geschwindigkeiten
  - hohe Heterogenität: langsame und schnelle Links, kleine und große Verzögerung → Skalierbarkeit
- Stabilität?
  - Konvergenz des Verfahrens garantiert?
- Fairness?
  - Flow Rate Fairness
  - Cost Fairness?
- Netzunterstützung?

Trend: Netzvirtualisierung

- Ändern der Infrastruktur aufwändig
  - Ausbringen neuer Protokolle und Mechanismen schwierig (IPv6, Multicast, ECN, usw.)
- Virtuelle Netze: virtuelle Knoten und virtuelle Links
  - mehrere virtuelle Knoten innerhalb eines physikalischen
  - Isolation der virtuellen Netze
- Vorteile
  - Parallele Existenz unterschiedlicher Architekturen
  - Netztopologie kann einfacher geändert werden
  - bessere Ressourcenauslastung/-nutzung durch Multiplexing und Migration
- Forschungsthema in 4WARD und G-Lab

2.5 Forschungsbedarf im Internet

- Das Internet steht ständig vor neuen Herausforderungen
- Beispiele für Forschungsthemen:
  - Namensgebung
  - Routing
  - Sicherheit
  - Netzwerkmanagement
  - Dienstgüte (QoS)
  - Staukontrolle (für Hochgeschwindigkeitsnetze)
  - Middleboxes
  - Internet-Entwicklung

FIND – Future Internet Network Design

- Initiative der NSF http://find.isi.edu/
- Zwei Hauptfragestellungen
  - Anforderungen an ein globales Netz in 15 Jahren? Wie sollte ein solches Netz aussehen, was sollte es tun?
  - Wie würde das zukünftige Netz vom heutigen Standpunkt aus konzipiert werden, wenn es komplett neu entwickelt würde?
- Anforderungen
  - Sicherheit und Robustheit
  - Einfacher zu managen
  - Nicht-technische Aspekte berücksichtigen
- Fokus auf Steuerung, Management, usw.

GENI – Global Environment for Network Innovations

- Testeinrichtung für neue Netzwerkarchitekturen
  - Generisch, d.h. nicht auf spezielle Protokolle zugeschnitten, wie sonst bei Testbeds üblich
  - Erlaubt Ausprobieren neuer Netzarchitekturen
- Ziele
  - Erhöhung der Qualität und Quantität experimenteller Forschungsergebnisse in Netzen und verteilten Systemen
  - Beschleunigter Übergang von solchen Ergebnissen zu Produkten
  - Übergangsmöglichkeit zu neuem Netz, welches möglicherweise das Internet ablöst
  - Details: http://geni.net/

Weiterentwicklung im Internet: IRTF und IETF

- Internet Research Task Force www.irtf.org
  - Betrachtet längerfristige Entwicklungen
  - Führt Voruntersuchungen durch
  - Eher geschlossene Gruppen, aber offene Mailinglisten
- Internet Engineering Task Force
  - Behebung aktueller Probleme
  - Zeithorizont: Protokollentwicklung in 2–3 Jahren
  - Offene Standardisierung der heutigen Internetprotokolle

Weiterentwicklungen im Internet: die IETF

- Internet Engineering Task Force (IETF) www.ietf.org, edu.ietf.org [RFC3233]
- Ziel: Das Internet besser machen [RFC3935]
- Mission: Produce high quality, relevant technical and engineering documents that influence the way people design, use, and manage the Internet in such a way as to make the Internet work better.
- Behebung aktueller Probleme, Schaffen notwendiger Erweiterungen etc., kurzfristiger umsetzbare Lösungen
- Erstellt gültige Internet-Standards (Request for Comments, RFCs)

2.6 Literatur (1)

[Clark88] D. Clark, „The Design Philosophy of the DARPA Internet Protocols“. Proc SIGCOMM 1988, Sept 1988. http://www.acm.org/sigcomm/ccr/archive/1995/jan95/ccr-9501-clark.html

[Crow07] Jon Crowcroft: “Net Neutrality: The Technical Side of the Debate: A White Paper”, ACM SIGCOMMM Computer Communications Review, Vol. 37, Number 1, Januar 2007

[CWSR02] D. Clark, J. Wroclawski, K. Sollins, R. Braden: „Tussle in Cyberspace: Defining Tomorrow‘s Internet“, ACM SIGCOMM 2002, http://www.acm.org/sigs/sigcomm/sigcomm2002/papers/tussle.pdf

[ESA96] „Flight 501 Failure Report“ http://ravel.esrin.esa.it/docs/esa-x-1819eng.pdf, 19. July, 1996

Literatur (2)

[FlJa94] S. Floyd, V. Jacobson, „The Synchronization of Periodic Routing Messages“, IEEE/ACM Transactions on Networking, Vol. 2, No. 2, April, 1994, http://ieeexplore.ieee.org/search/wrapper.jsp?arnumber=298431

[FFLM09] D. Farinacci, V. Fuller, D. Lewis, D. Meyer: Locator/ID Separation Protocol (LISP), draft-farinacci-lisp-12.txt, März 2009, http://tools.ietf.org/html/draft-farinacci-lisp

[Jaco88] V. Jacobson, „Congestion Avoidance and Control“, Proceedings of SIGCOMM 1988, pp. 273–288, http://portal.acm.org/citation.cfm?id=52324.52356

[JSTP+09] V. Jacobson, D. Smetters, J. Thornton, M. Plass, N. Briggs, R. Braynard: “Networking Named Content”, ACM CoNEXT’09, December 1–4, 2009, Rome, Italy. http://conferences.sigcomm.org/co-next/2009/papers/Jacobson.pdf

[Neum90] P. G. Neumann, “Cause of AT&T network failure”, Januar 1990, http://catless.ncl.ac.uk/Risks/9.62.html#subj2

Literatur (3)

[RFC 1122] R. Braden. Requirements for Internet Hosts - Communication Layers. RFC 1122 (Standard), Oktober 1989. Updated by RFCs 1349, 4379. URL: http://www.ietf.org/rfc/rfc1122.txt.

[RFC 1958] B. Carpenter. Architectural Principles of the Internet. RFC 1958 (Informational), Juni 1996. Updated by RFC 3439. URL: http://www.ietf.org/rfc/rfc1958.txt.

[RFC 2775] B. Carpenter. Internet Transparency. RFC 2775 (Informational), Februar 2000. URL: http://www.ietf.org/rfc/rfc2775.txt.

[RFC 3233] P. Hoffman und S. Bradner. Defining the IETF. RFC 3233 (Best Current Practice), Februar 2002. URL: http://www.ietf.org/rfc/rfc3233.txt.

Literatur (4)

[RFC 3238] S. Floyd und L. Daigle. IAB Architectural and Policy Considerations for Open Pluggable Edge Services. RFC 3238 (Informational), Januar 2002. URL: http://www.ietf.org/rfc/rfc3238.txt.

[RFC 3426] S. Floyd. General Architectural and Policy Considerations. RFC 3426 (Informational), November 2002. URL: http://www.ietf.org/rfc/rfc3426.txt.

[RFC 3439] R. Bush und D. Meyer. Some Internet Architectural Guidelines and Philosophy. RFC 3439 (Informational), Dezember 2002. URL: http://www.ietf.org/rfc/rfc3439.txt.

[RFC 3724] J. Kempf, R. Austein und IAB. The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture. RFC 3724 (Informational), März 2004. URL: http://www.ietf.org/rfc/rfc3724.txt.

Literatur (5)

[RFC 4984] D. Meyer, L. Zhang und K. Fall. Report from the IAB Workshop on Routing and Addressing. RFC 4984 (Informational), September 2007. URL: http://www.ietf.org/rfc/rfc4984.txt.

[SaRC81] Saltzer, J., Reed, D., and D. Clark, End-To-End Arguments in System Design. 2nd International Conf on Dist Systems, Paris France, April 1981. ACM Transactions in Computer Systems 2, 4, November, 1984, pages 277–288. http://portal.acm.org/citation.cfm?id=357402

[Thal09] D. Thaler, Evolution of the IP Model, IETF Journal, Vol. 4, Issue 3, February 2009, http://www.isoc.org/tools/blogs/ietfjournal/wp-content/uploads/2009/02/IETFJournal0403.pdf

[WiDo02] W. Willinger, J. Doyle, „Robustness and the Internet: Design and evolution”, March 2002, http://netlab.caltech.edu/internet/