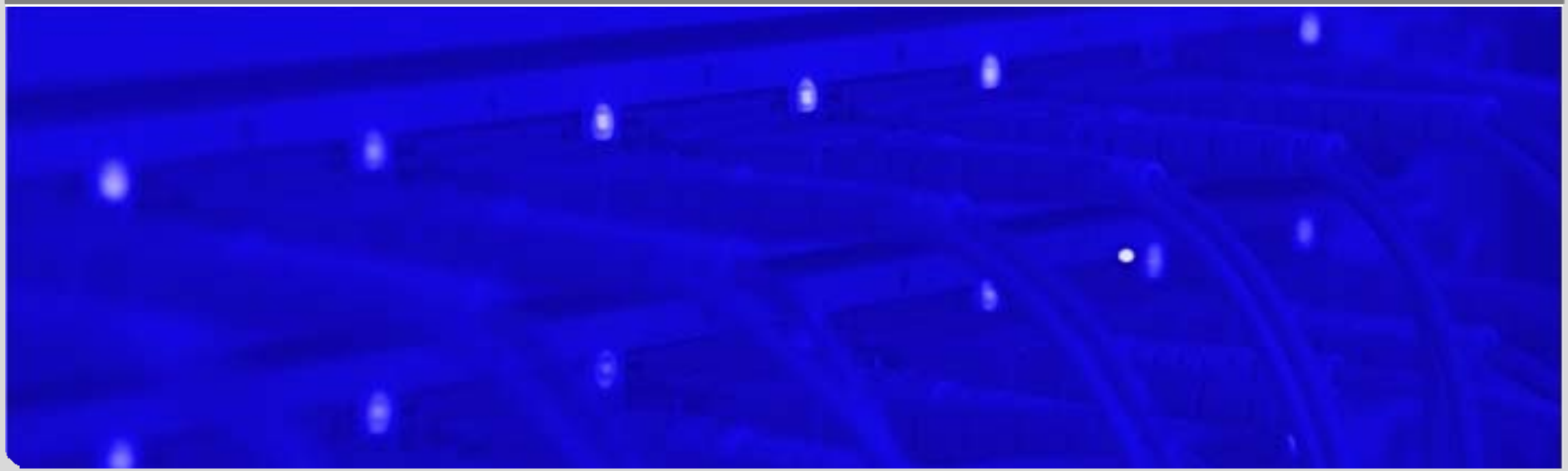
Next Generation Internet
2. Internet-Architektur — Prinzipien und Entwicklung

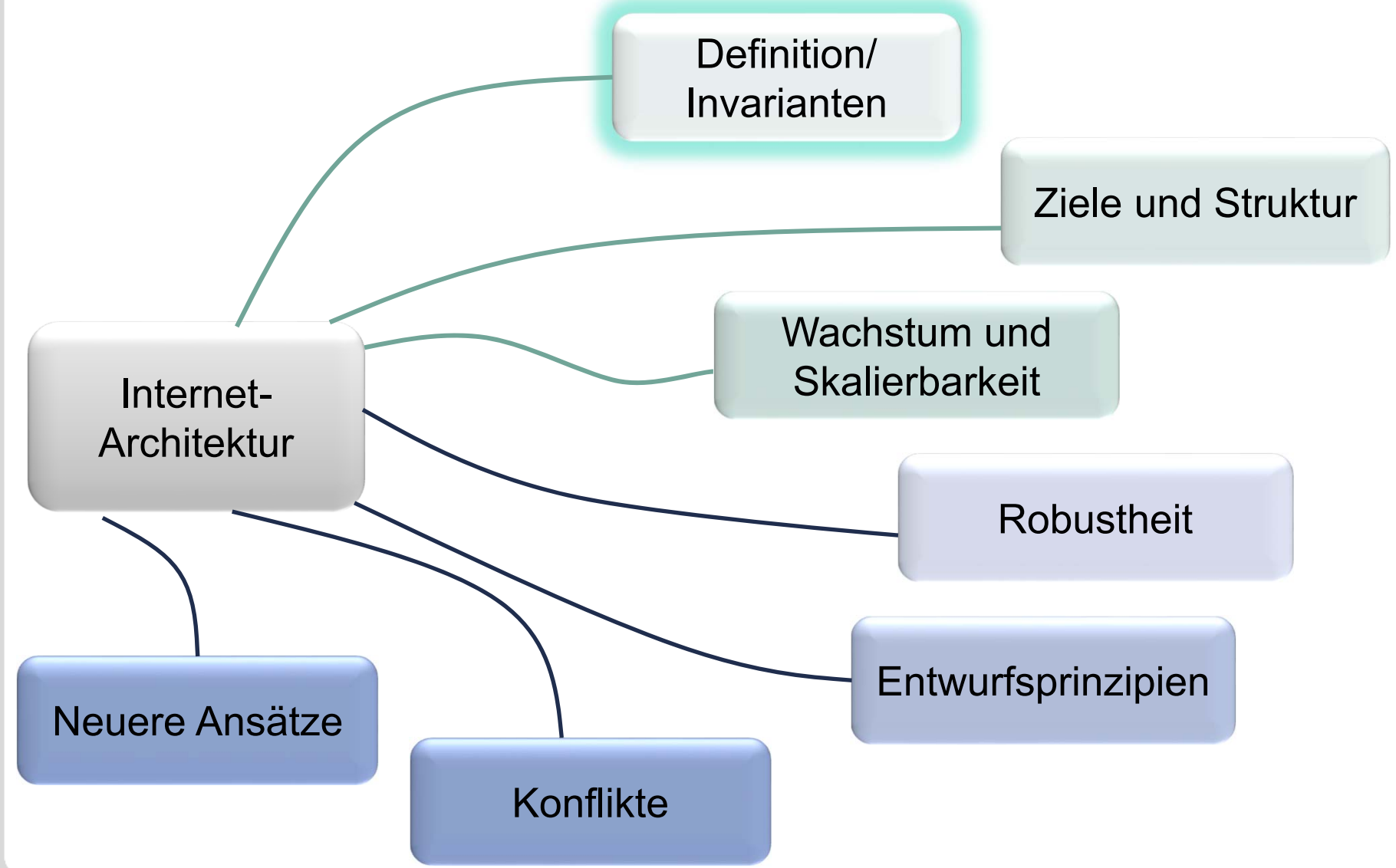
PD Dr.-Ing. Roland Bless
bless@kit.edu

INSTITUT FÜR TELEMATIK



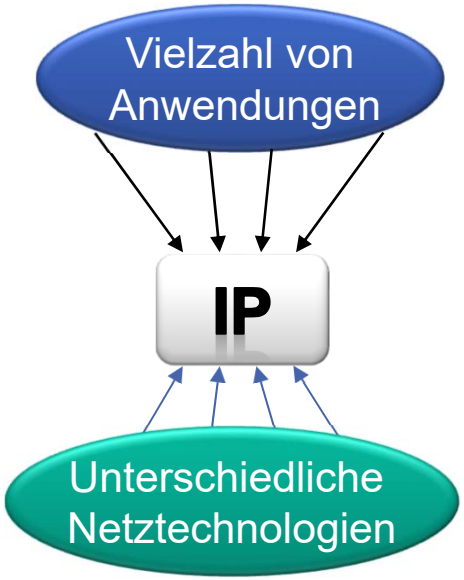
Kapitelübersicht

Institut für Telematik, Fakultät für Informatik
http://telematics.tm.kit.edu/


Definition/
Invarianten
Ziele und Struktur
Wachstum und
Skalierbarkeit
Internet-
Architektur
Robustheit
Entwurfsprinzipien
Neuere Ansätze
Konflikte

Erfolgsfaktoren des Internets

- Einfachheit
  - „dummes Netz“ – intelligente Endsysteme
  - Skalierbarkeit
  - Robustheit
- Offenheit: offener Standard
- Innovation „am Netzrand“
  - einfaches Ausbringen neuer Anwendungen
  - Einfluss der Nutzer



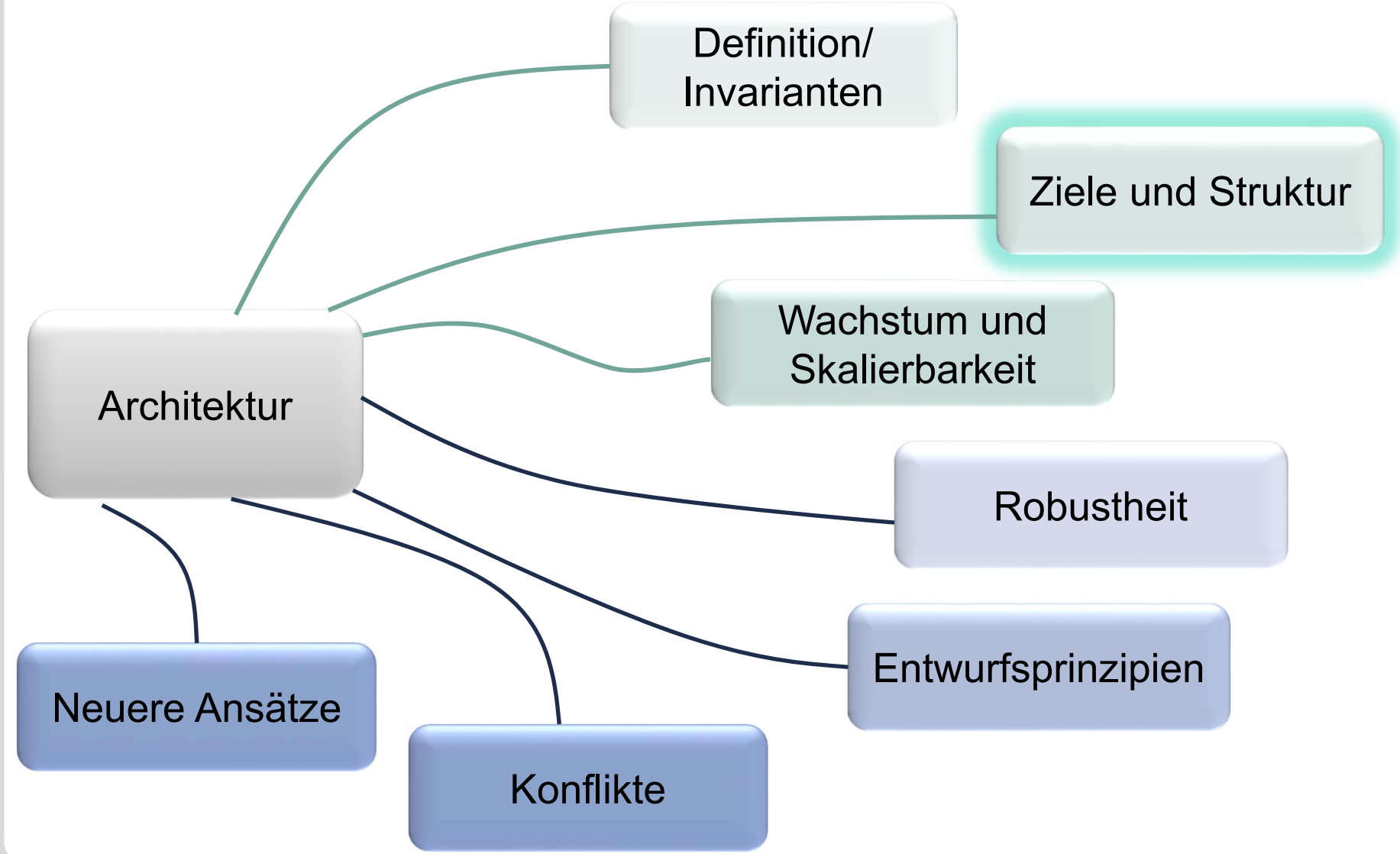
Was macht eine Architektur aus?

- Eine Architektur verfolgt eine Menge von Zielen
  - Zwecks eines Gebäudes: Wohnhaus, Museum, Gefängnis?
  - Internet: Internetkonnektivität zwischen Netzen
- Wie passen und arbeiten die Teile zusammen?
  - Modularität, Dekomposition, Abhängigkeiten, Schnittstellen, Wiederverwendung, Design-Prinzipien
- Charakter/Wesentliche Merkmale der Architektur
  - Spezifische Eigenschaften
  - lassen sich nicht einfach austauschen → Invarianten
- Wiederverwendung erfolgreicher Teile/Konzepte
  - Entwurfsmuster

Invarianten


[ABEH+04]

- Jede Architektur hat Fixpunkte bzw. kleinste gemeinsame Nenner, die eine Weiterentwicklung hemmen oder unmöglich machen → Invarianten
  - Fundamente, grundlegende Struktur
  - Was sind Invarianten im Internet?
- Invarianten limitieren die Evolution der Architektur
  - Explizite Invarianten
    - absichtlich definierte Charakteristika, um die Flexibilität einzuschränken
    - Verlässlichkeit der Architektur
  - Implizite Invarianten
    - unabsichtliche Seiteneffekte des Designs


Definition/
Invarianten
Ziele und Struktur
Wachstum und
Skalierbarkeit
Architektur
Robustheit
Entwurfsprinzipien
Neuere Ansätze
Konflikte

Internet-Architektur: Entwurfsziele

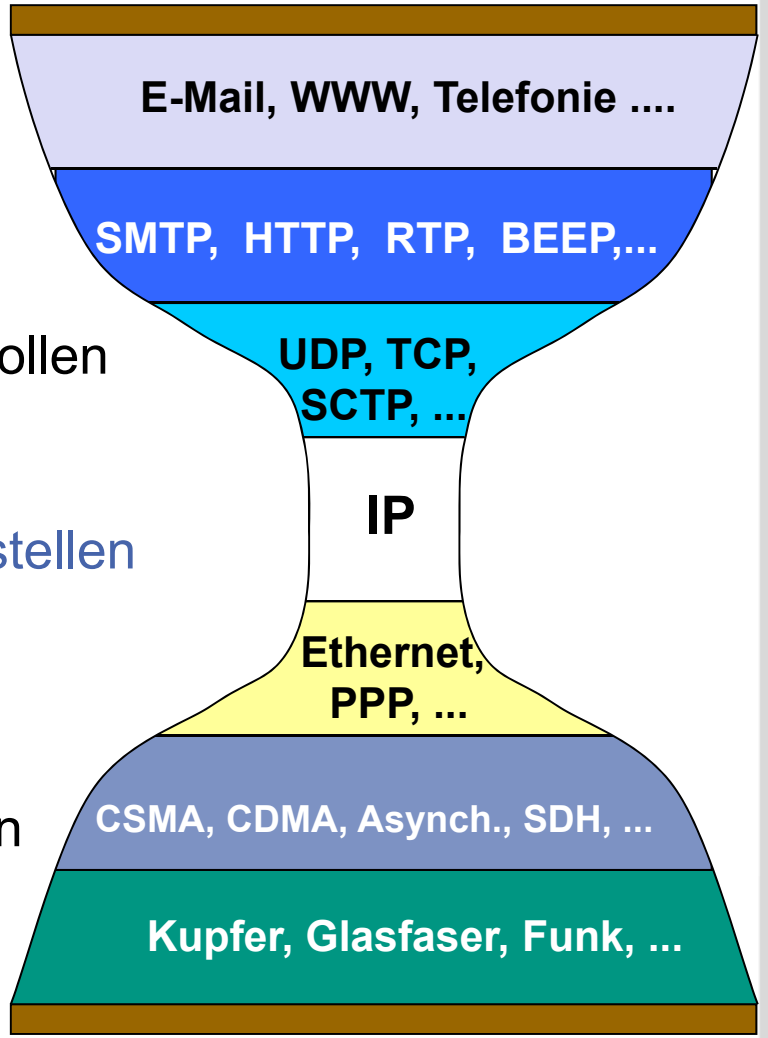
Paper von D. Clark *"The Design Philosophy of the DARPA Internet Protocols"* nennt:


[Clark88]

- Hauptziel: Internetworking, d.h. Verbinden existierender Netzwerke (→ Netz von Netzen)
- 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

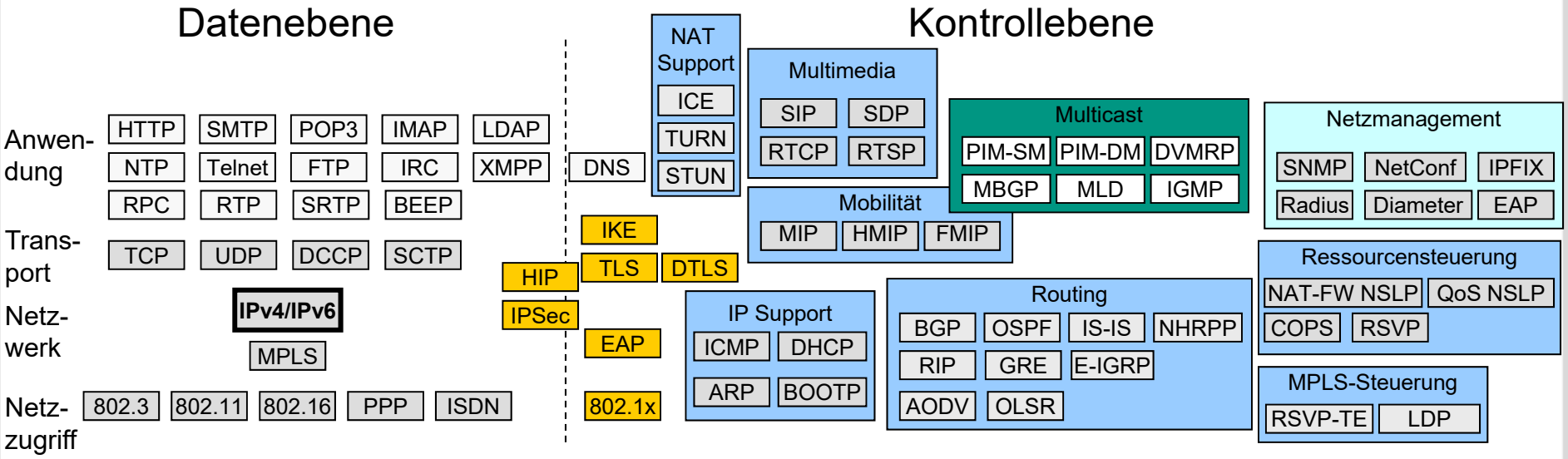
Das Sanduhr-Modell

- IP-Schicht ermöglicht
  - Größeres Netzwerk
  - Globale Adressierung
  - Verstecken von Netzwerk-Details und Änderungen vor Ende-zu-Ende-Protokollen
- Einziges Protokoll
  - Maximiert Interoperabilität
  - Minimiert die Anzahl der Dienstschnittstellen
- Schlankes Protokoll
  - Setzt kleinste gemeinsame Netzwerk-funktionalität voraus, um Anzahl der einsetzbaren Netzwerke zu maximieren
  - Ende-zu-Ende-Prinzip
  - Robustheit durch Zustandslosigkeit
- Siehe auch: http://www.iab.org/documents/docs/hourglass-london-ietf.pdf



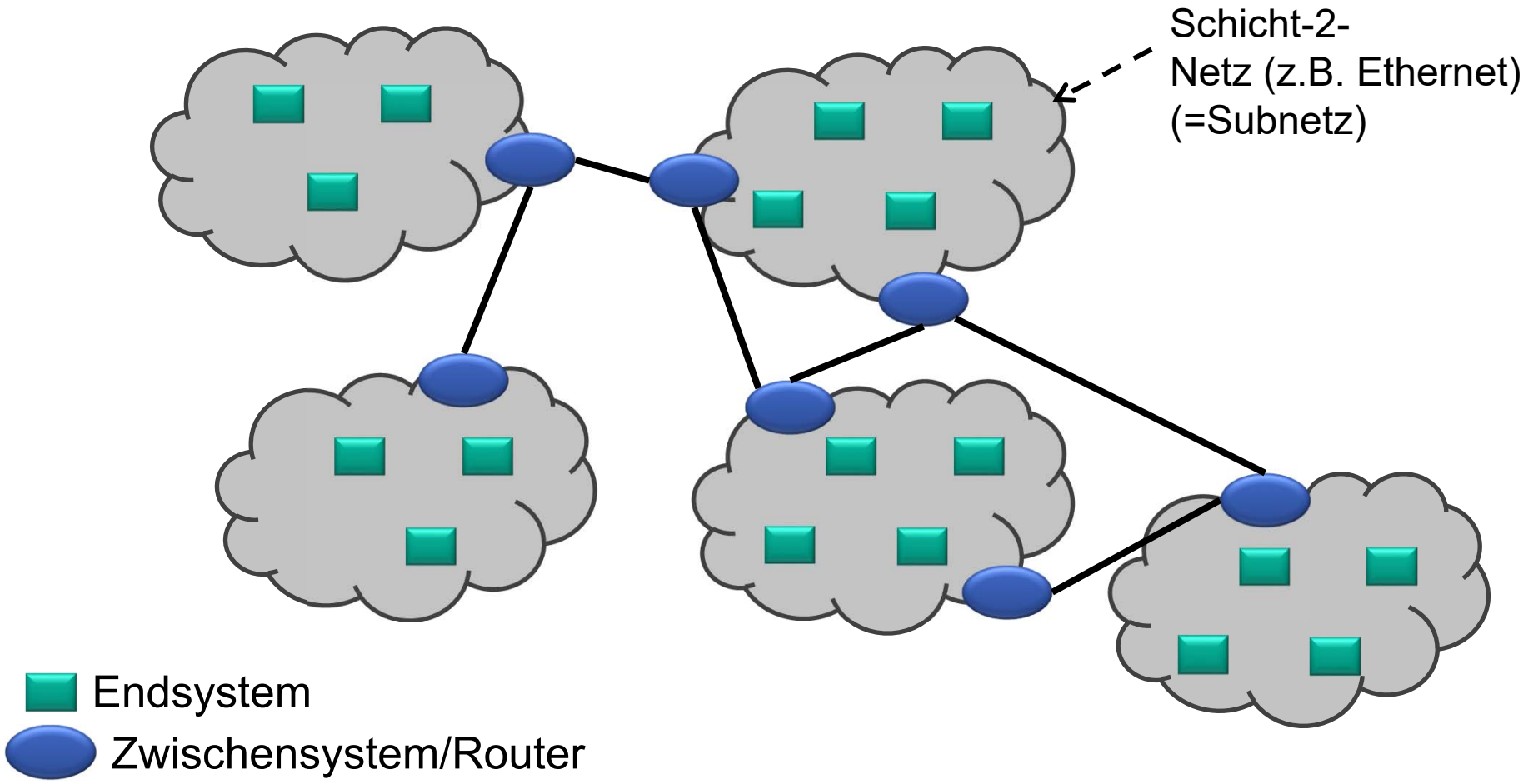
Schlanker Mittelteil?

- Wachstum der Komplexität



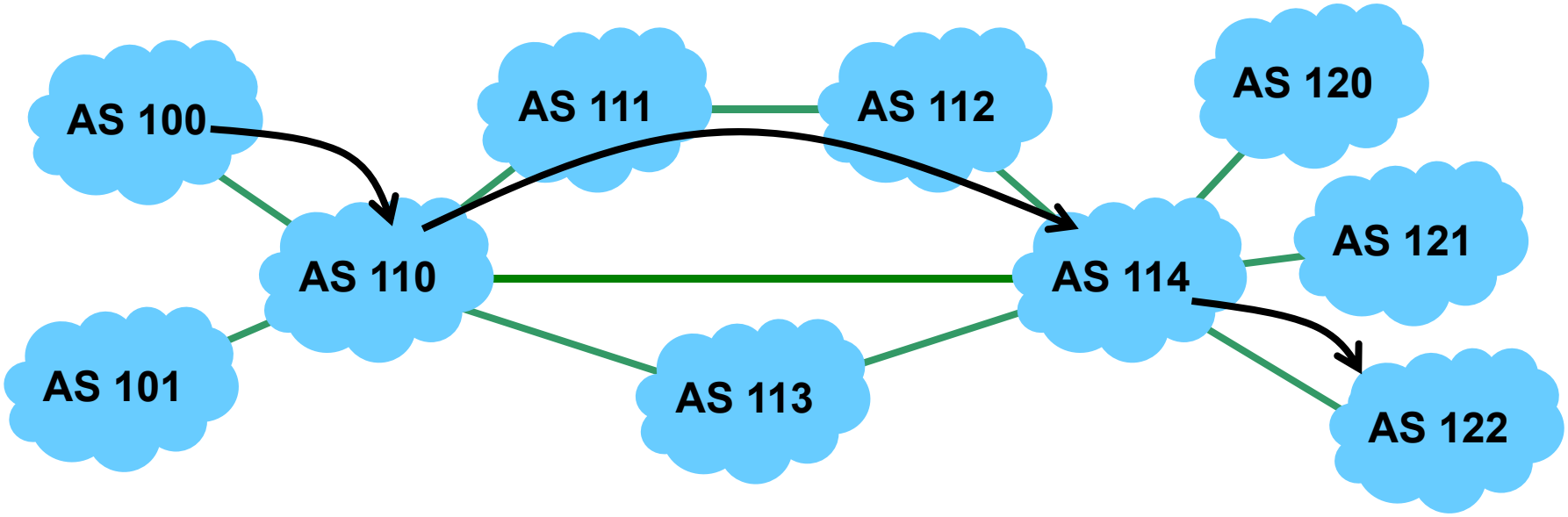
- Kontrollprotokolle machen inzwischen einen Großteil der Gesamtkomplexität aus
- TCP/UDP + HTTP als neuer Mittelteil?

Abstraktes Modell Interkonnektivität



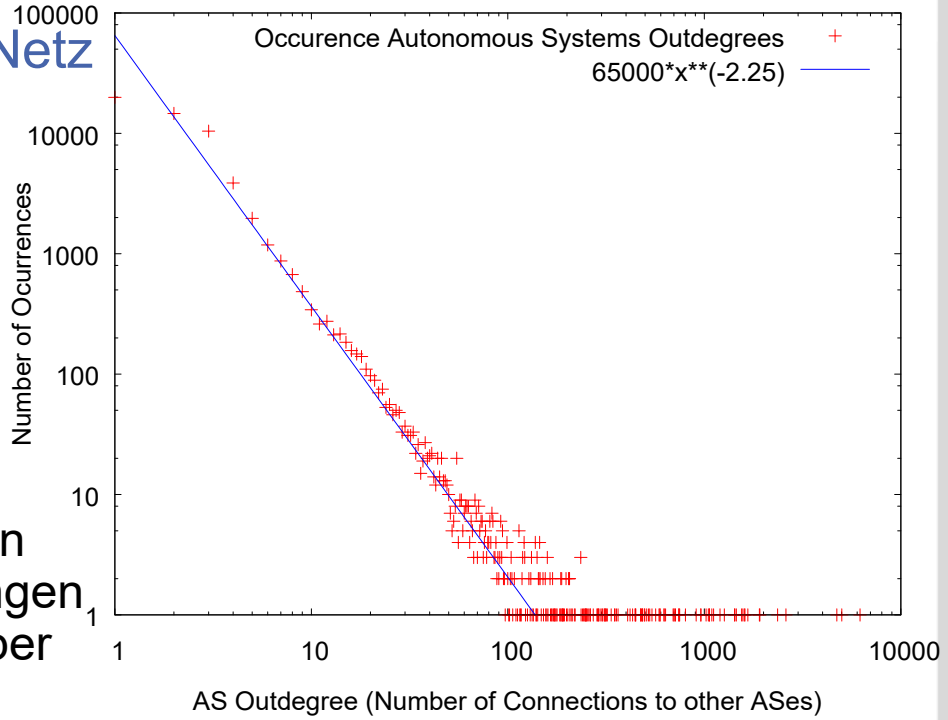
Abstrakte Sicht Globales Routing

- Autonome Systeme
- Interna verborgen (bis auf erreichbare Subnetze)



Small-World-Netze

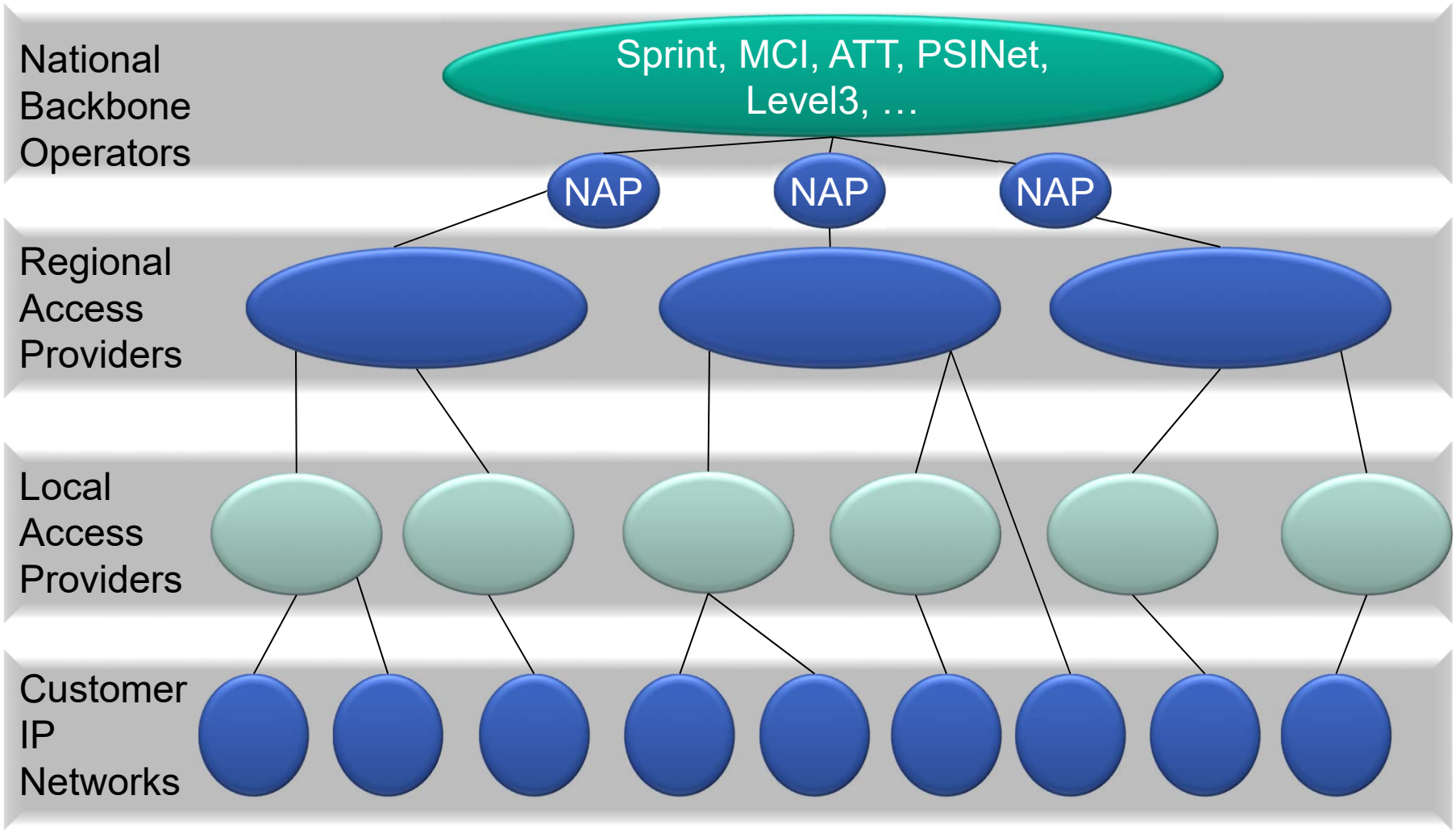
- AS Topologie ist ein Small-World-Netz
  - „Six degrees of separation“
- Power-Law-Eigenschaft
  - Unabhängig von Netzgröße und Zeitpunkt
  - Anzahl der Knoten mit L Kanten ist proportional zu L^{-k}
    - k > 0 ist eine Netz-spezifische Konstante
  - Bedeutet: Die Mehrheit der Knoten besitzen relativ wenige Verbindungen Einige wenige Knoten besitzen aber sehr viele Verbindungen
- Fehlertoleranz
  - Robust gegen zufällige Ausfälle
    - Zumeist sind Knoten mit nur wenigen Verbindungen betroffen
  - Anfällig gegen gezielte Angriffe auf Knoten mit vielen Verbindungen



AS Topologie vom 2017-04-23
57439 Autonome Systeme
158339 Verbindungen

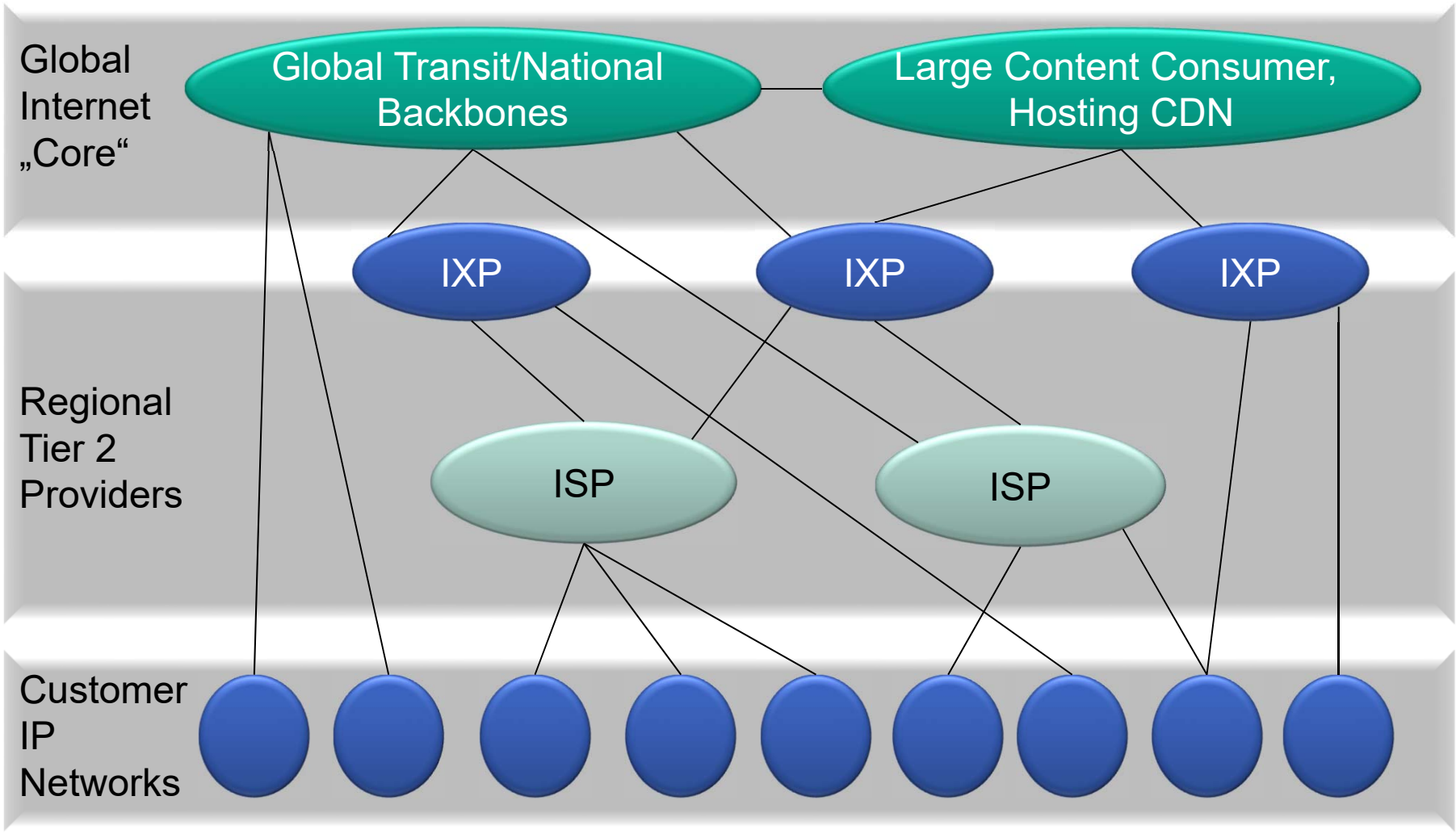
[FaFF99]

Internet-Topologie – früher (1995-2007)



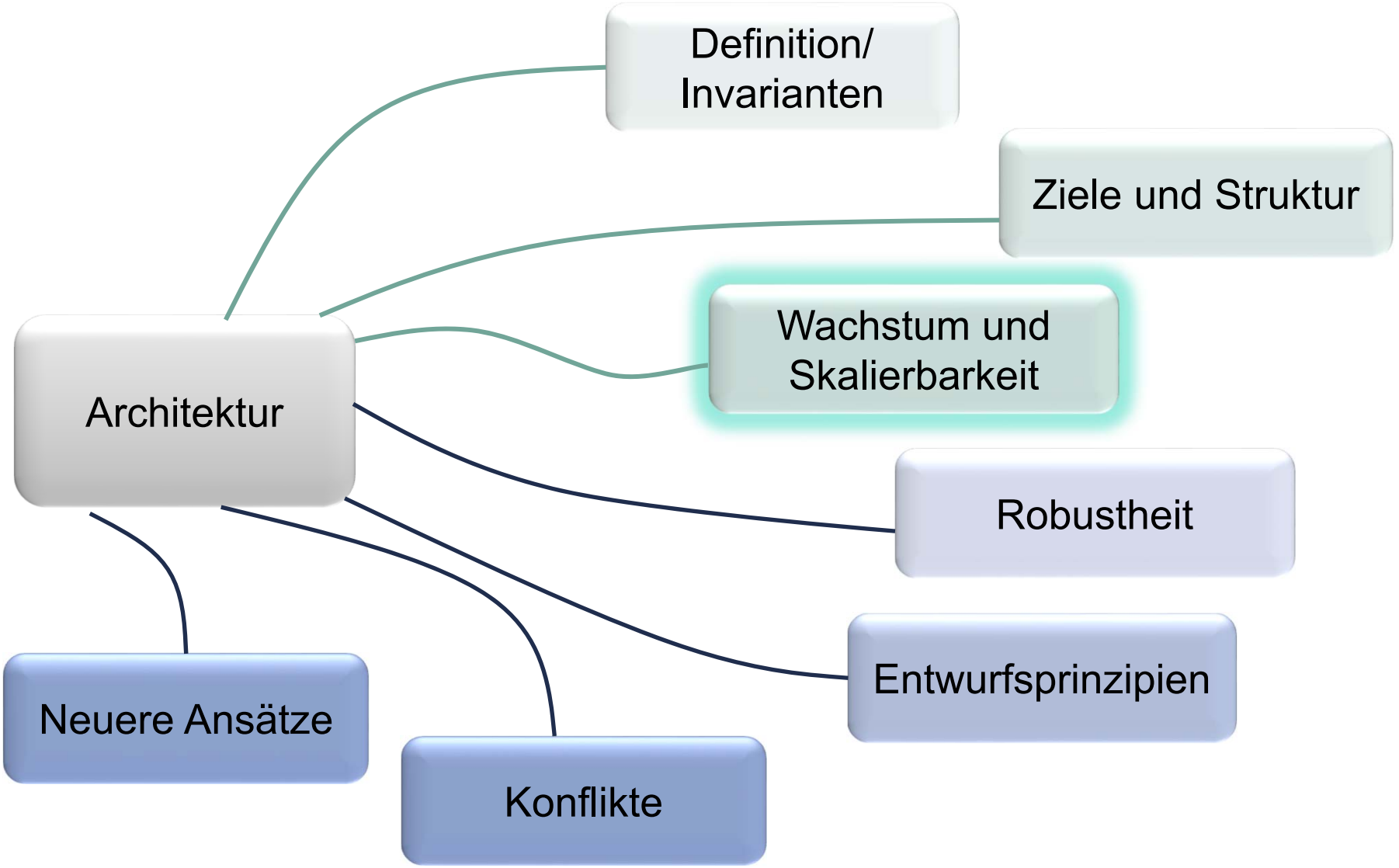
Internet-Topologie – heute

[Lab+10, Labo10]



Wandel zu neuen Strukturen

- Dichtere Vernetzung, kürzere Wege
- Verschiebung des Fokus von Datentransport zu Inhalten
  - Datentransporteure verlieren an Bedeutung
  - Verstärkter Kampf um Verbraucher
  - Bündeln verschiedener Mehrwertdienste
- Möglichst direkte Verbindung zwischen Inhalteanbieter und Verbraucher
  - Getrieben durch Kosten und Leistung

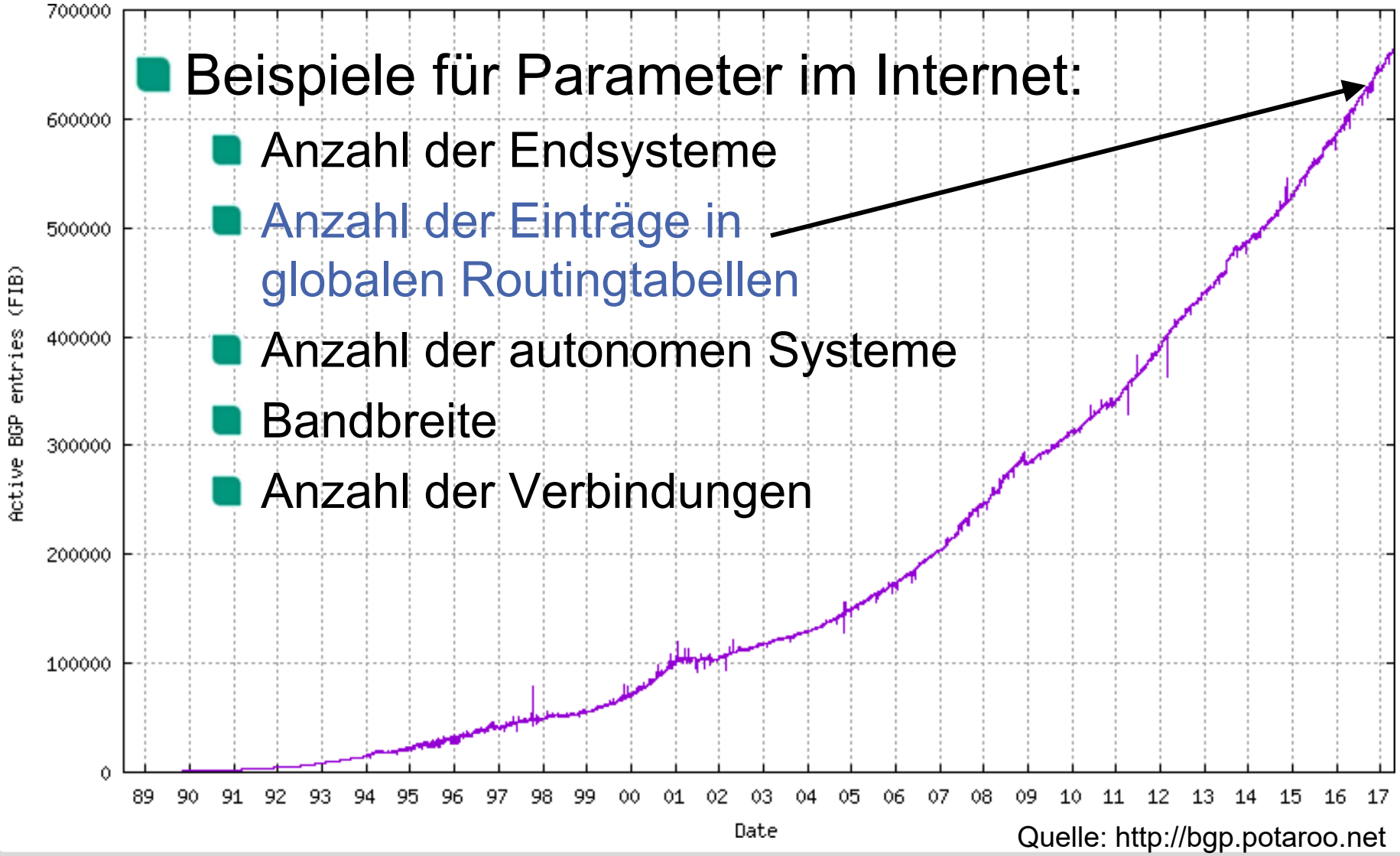

Definition/
Invarianten
Ziele und Struktur
Wachstum und
Skalierbarkeit
Architektur
Robustheit
Entwurfsprinzipien
Neuere Ansätze
Konflikte

Wachstum und Skalierbarkeit

- Einzige Konstante im Internet: Ständige Veränderung
- Vor allem: Wachstum
- Technologischer Fortschritt bringt oftmals Steigerungen um Größenordnungen bzgl. Bestimmter Parameter (z.B. Moore‘sches Gesetz, CPU, Bandbreite, Speicher)
- Generelle Frage: wie kommt das technische System damit zurecht?
  - 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



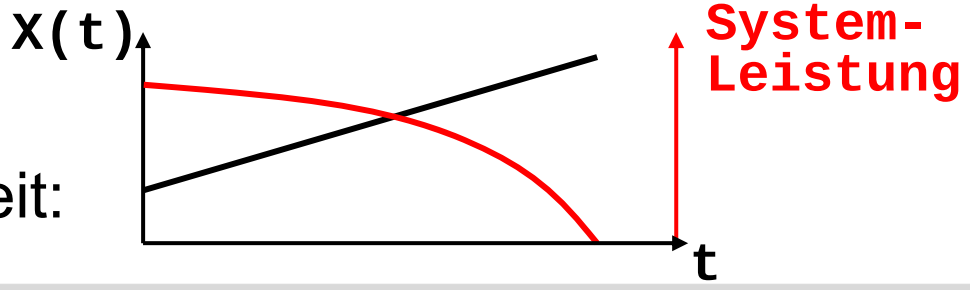
Quelle: http://bgp.potaroo.net

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:

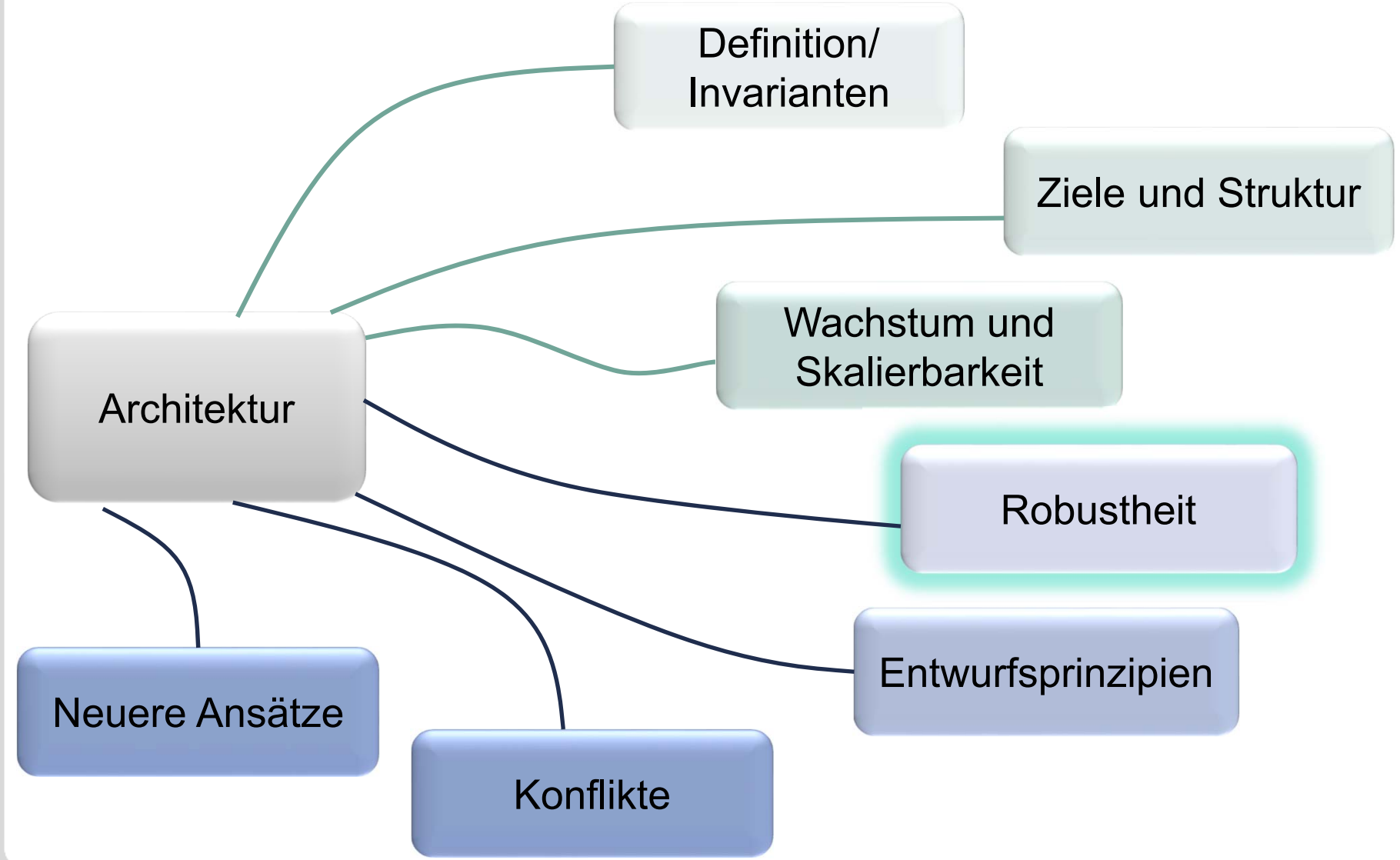
Ein skalierbares System funktioniert auch bei starkem **Wachstum** (z.B. um mehrere **Größenordnungen**, d.h. über mehrere Skalen hinweg) **bestimmter Parameterwerte des Systems** mit ausreichender Leistung

Beispiel für keine bzw. schlechte Skalierbarkeit:



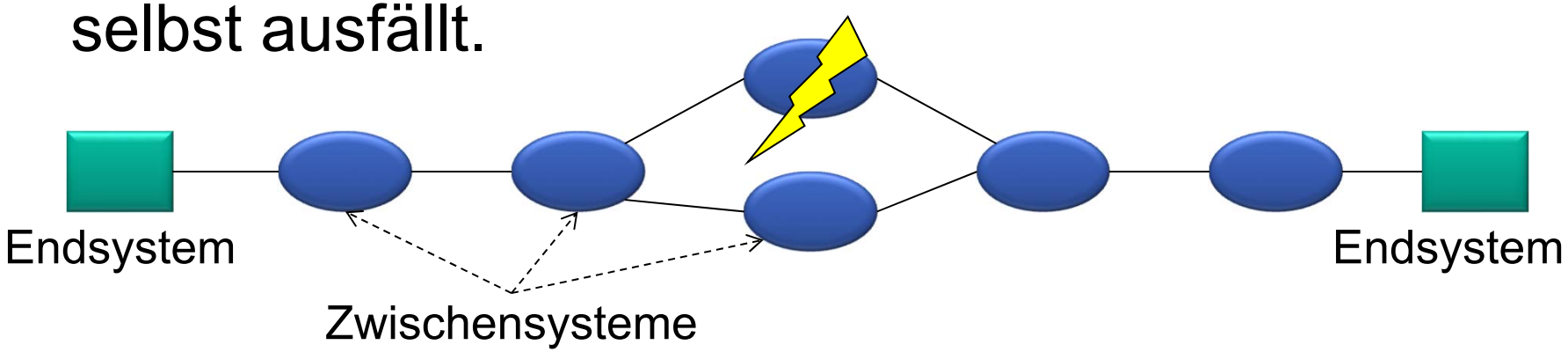
Skalierbarkeitsaspekte

- 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 darstellen!


Definition/
Invarianten
Ziele und Struktur
Wachstum und
Skalierbarkeit
Architektur
Robustheit
Entwurfsprinzipien
Neuere Ansätze
Konflikte

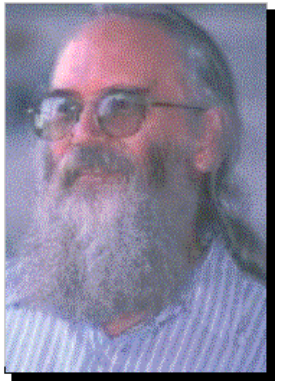
Robustheit gegen Ausfall

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

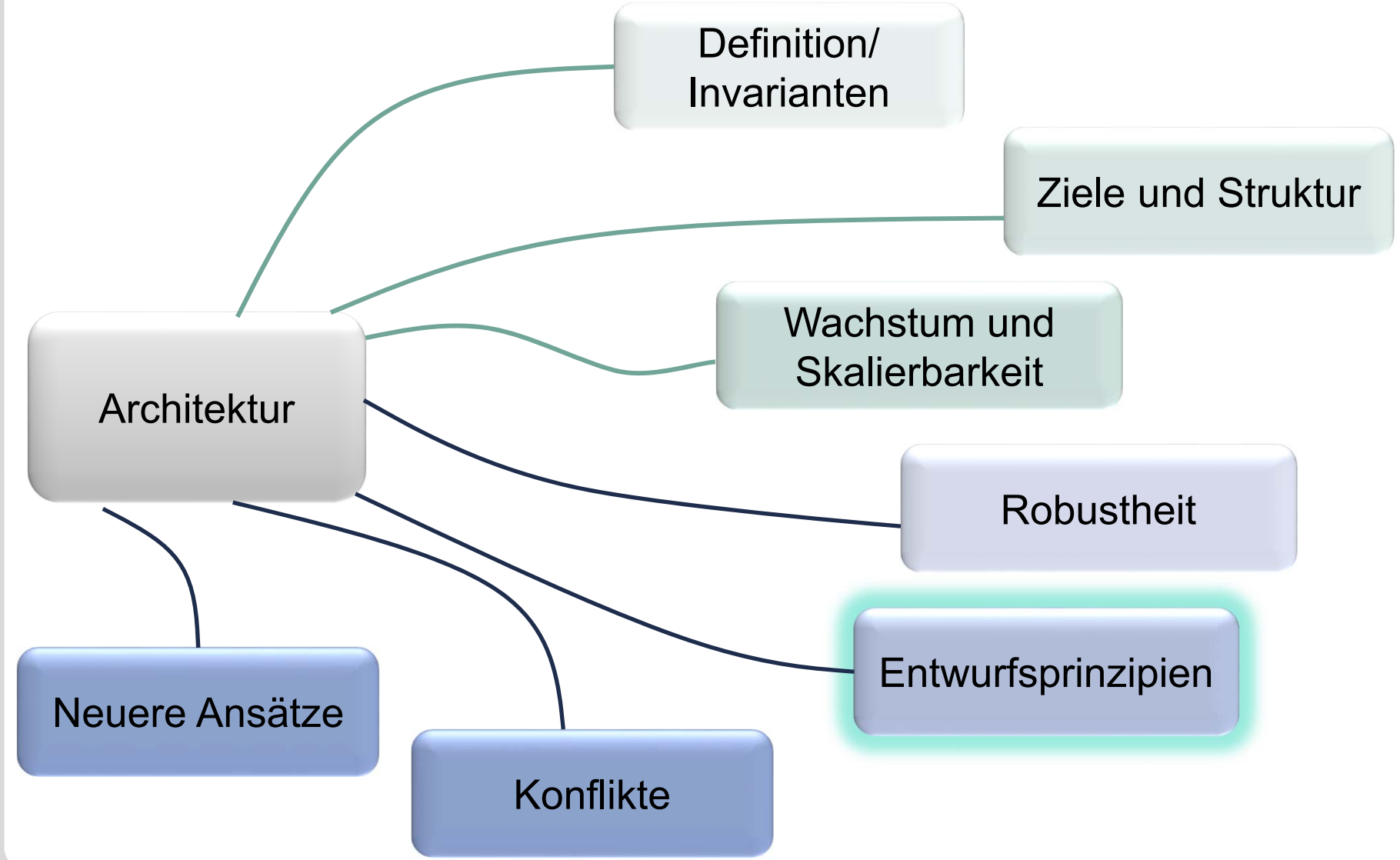


- Schicksal Endsystem → Schicksal der Verbindung
- Keinen Zustand im Netzwerk halten → stattdessen in den Endsystemen
- Datagramm-Konzept als Folge

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


Definition/
Invarianten
Ziele und Struktur
Wachstum und
Skalierbarkeit
Architektur
Robustheit
Entwurfsprinzipien
Neuere Ansätze
Konflikte

Entwurfsprinzipien: Ende-zu-Ende-Argument

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



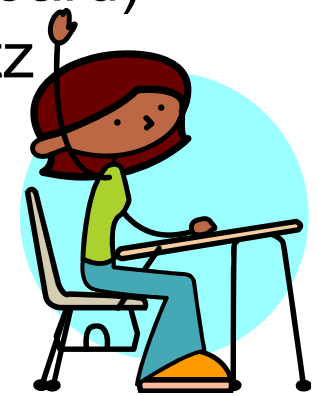
- Wichtiges Entwurfsprinzip (erst 1981 explizit formuliert von Saltzer, Reed und Clark): Das Ende-zu-Ende-Argument (E2E argument) [SaRC81]
  - wenn Wissen und Hilfe der Anwendung notwendig (insbesondere zur Behandlung von Fehlerfällen!) → Funktionalität ins Endsystem
  - Keine anwendungsspezifische Funktionalität im Netz bereitstellen

Ende-zu-Ende-Argument

- Minimalitätsprinzip
  - Vermeide, mehr als nur die wesentliche und notwendige Funktionalität ins Netzwerk zu integrieren
  - Es macht keinen Sinn, zuverlässige Übertragung im Netz zu realisieren, wenn die Endsysteme sowieso die Korrektheit prüfen müssen
  - Halte „unnötige“ Funktionalität aus dem Netzwerk fern → Keep it simple
- Auch manchmal Ende-zu-Ende-Prinzip genannt (aber nicht zu Verwechseln mit Ende-zu-Ende-Transparenz!)

Beispiel

- A/V-Konferenzanwendung auf mobilem Endgerät
  - Sitzung: 3 Datenströme (Video/Audio/Whiteboard) mit Reservierungen für garantierten Durchsatz
  - Wechsel zu anderem drahtlosen Zugangspunkt notwendig
  - Reservierung soll auch am neuen Zugangspunkt bestehen
- Sollte das Netzwerk sich um die Verbindungsübergabe (Session Handover) kümmern?
- Pingo http://pingo.upb.de/8577



E2E Argument – weitere Ziele/Folgen

- Innovationsschutz
  - Einfaches Hinzufügen neuer Dienste
    - in den Endsystemen am Netzrand
    - Infrastruktur muss nicht an Anwendungen angepasst werden
  - 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
- 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 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

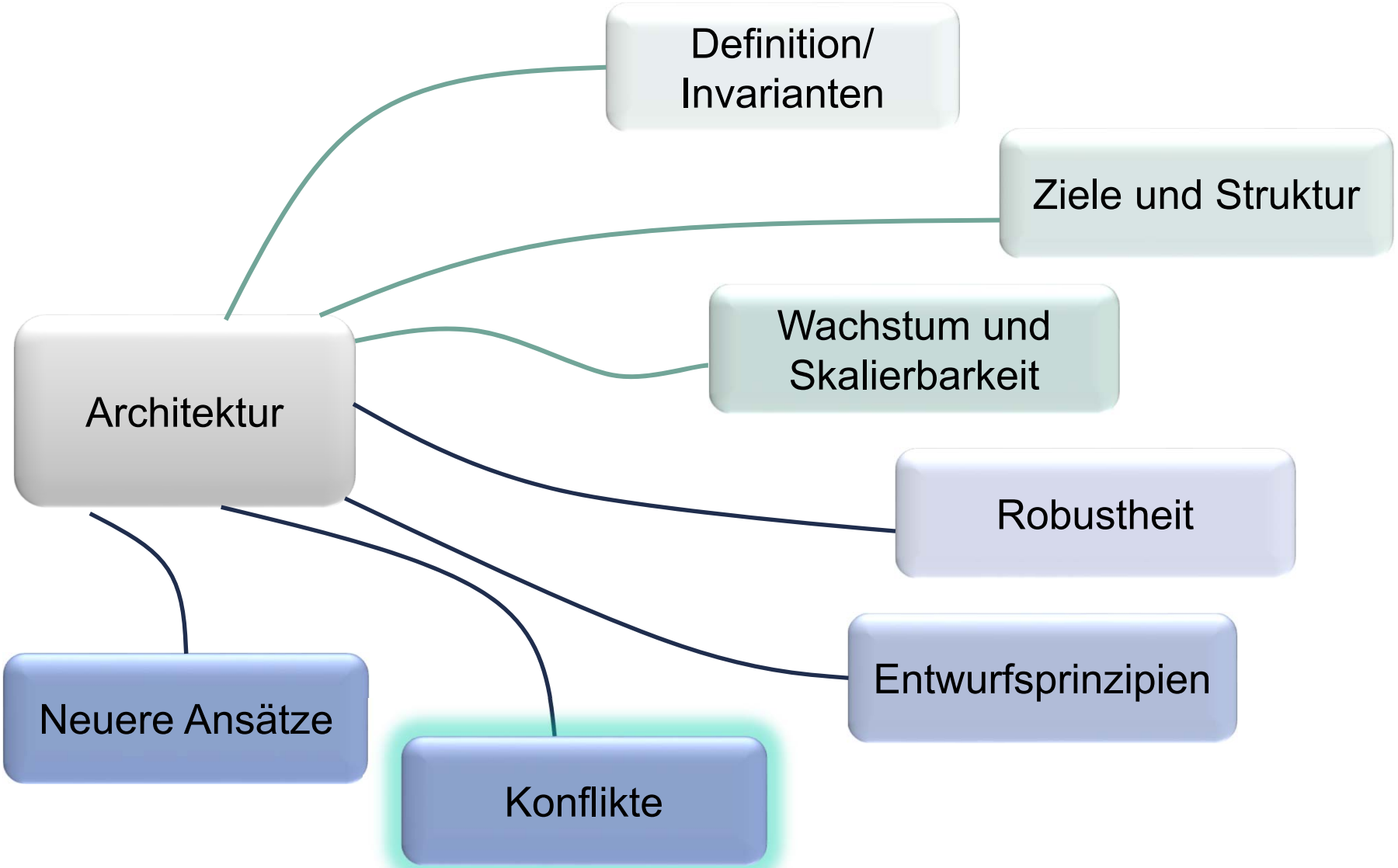
Weitere Architektur-Richtlinien

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
  - insbesondere in der Kontrollebene zu vermeiden
  - kombinierte Lösungen vereinen alle Nachteile
  - Interworking auf Datenebene beschränken: Umsetzung bzw. Kapselung am Netzrand möglich

Weitere Entwurfsaspekte

- RFC 3426 „General Architectural and Policy Considerations“ [RFC3426]
  - grundsätzliche Fragestellungen zum Protokoll-/System-Entwurf
  - keine Richtlinien, keine Checkliste
  - Diskussion und Erläuterung anhand zahlreicher Fallbeispiele (z.B. ECN)
- RFC 1122 „Requirements for Internet Hosts – Communication Layers“ [RFC1122]
  - gute Dokumentation und Diskussion der Entwurfsentscheidungen

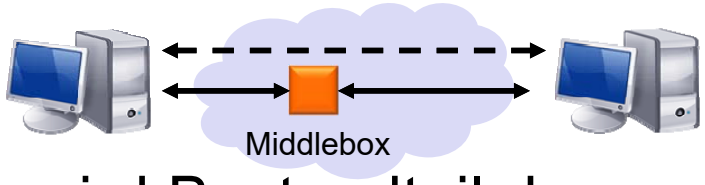

Definition/
Invarianten
Ziele und Struktur
Wachstum und
Skalierbarkeit
Architektur
Robustheit
Entwurfsprinzipien
Neuere Ansätze
Konflikte

Konflikte (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, Amazon Cloudfront, MS Azure CDN, Edgecast...)

Konflikte (2)

- Beispiel: negative Effekte durch Sicherheitstechniken
  - Rigoroses Filtern von ICMP-Paketen: PATH-MTU-Discovery funktioniert nicht mehr
  - 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)
  - 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
  - A/V-Tauschbörsen ↔ Musik/Film-industrie/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

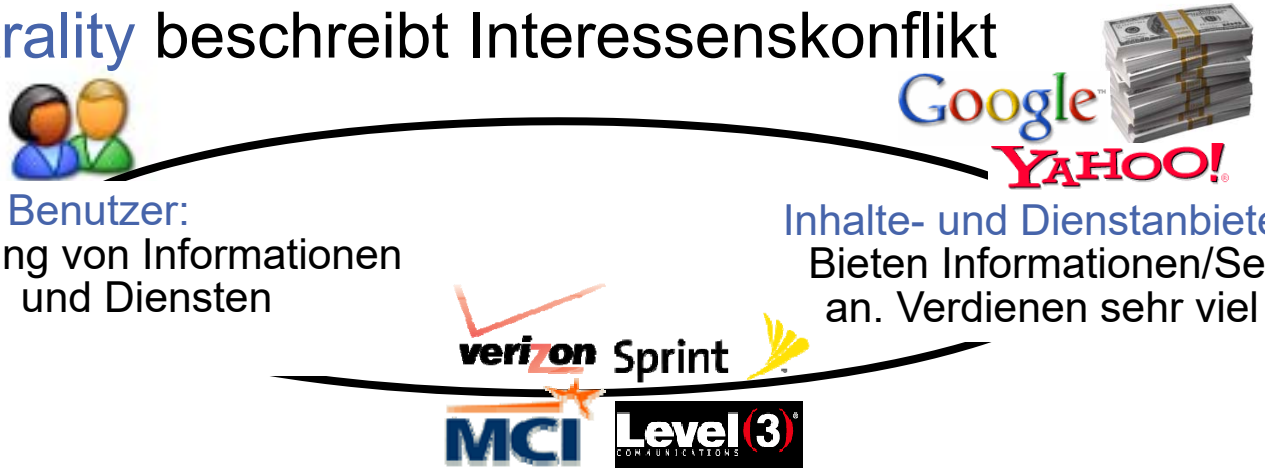
- Systemdesign sollte Spielraum bzgl. Nutzungs-möglichkeiten erlauben
  - unterschiedliche Möglichkeiten je nach Interessen
  - Konflikte sollten innerhalb des Systemdesigns ausgetragen werden und dieses nicht verdrehen oder verletzen
- Neue Prinzipien
  - Modularität entlang von Konfliktgrenzen
    - → 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 – Konflikte

- 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
  - Neue Anwendungen und Dienste werden gehindert
  - Kleine Inhalteanbieter haben das Nachsehen
  - Für Nutzer unklar, welche Ziele/Kriterien der Netzbetreiber verfolgt und welche Maßnahmen er ergreift
  - Aber: Priorisierung von Datenströmen im Rahmen von Dienstgüteunterstützung/Netzmanagement manchmal notwendig

Net Neutrality – Konflikte

- Ziel der „Net Neutrality“-Bewegung
  - Erhaltung der Netztransparenz: Alle Pakete, Inhalte und Dienste müssen gleichberechtigt im Internet transportiert werden.
  - Kein Blockieren
    - legaler Inhalte und Anwendungen
    - rein aus Netzbetreiberinteressen

Net Neutrality – Lösungen

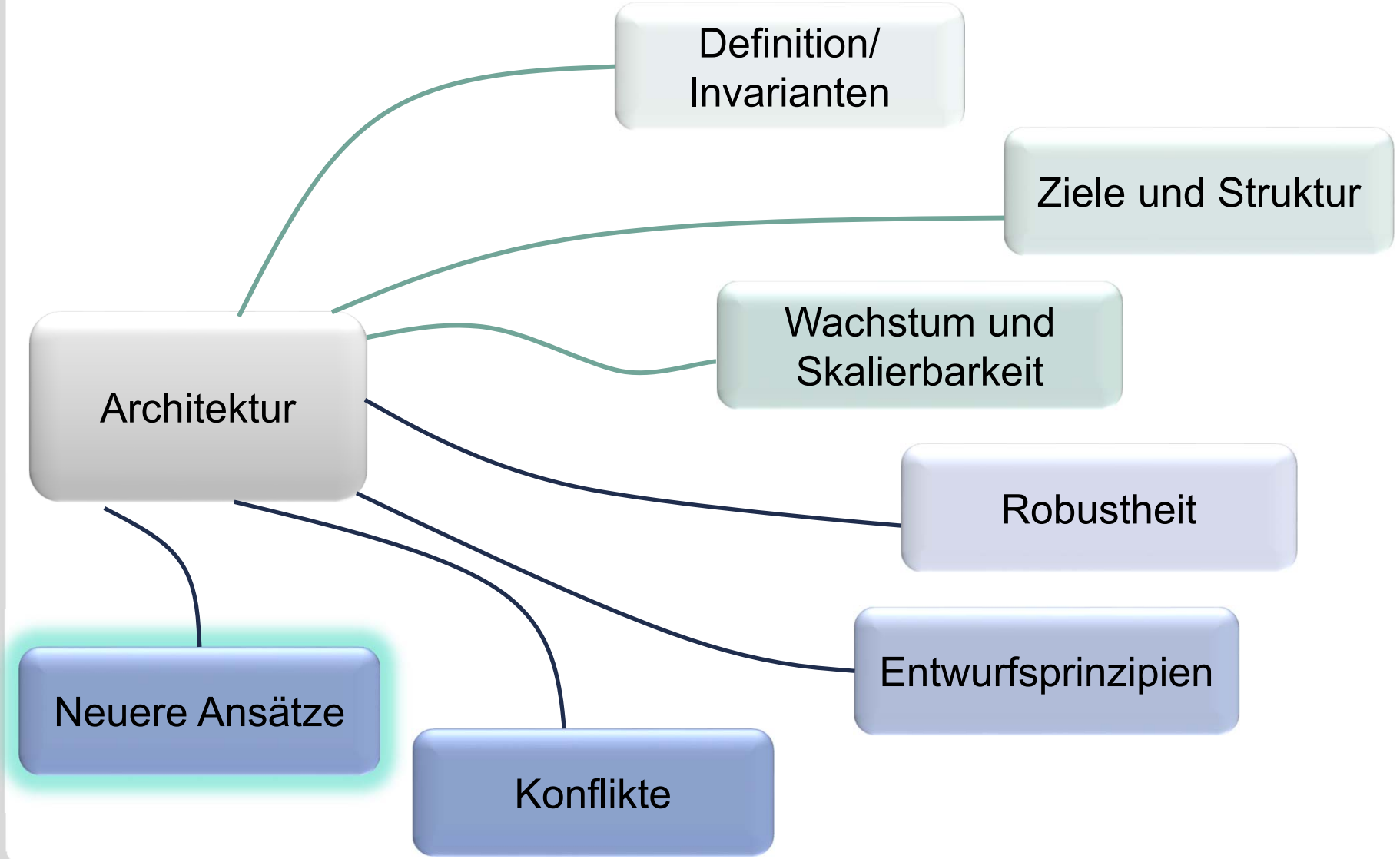
- Regulierung durch Gesetzgeber?
- Eingriffe seitens des Netzbetreibers
  - sinnvoll wenn es z.B. um Sicherheit geht
  - wenn es um intelligentes Ressourcenmanagement geht
    → Dienstgüteunterstützung
    - aber wenn möglich: nicht-diskriminierend gegenüber bestimmten oder einzelnen Anwendungen
  -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

Aktuelle FCC Regeln (13.4.2015)

- Kein Blockieren
  - kein betreiberseitiges Blockieren des Zugriffs auf legale Inhalte, Anwendungen, Dienste und nicht-schädliche Geräte
- Keine Drosselung
  - keine betreiberseitige Verschlechterung von legalem Internet-Verkehr auf der Basis von Inhalten, Anwendungen, Diensten oder nicht-schädlichen Geräten
- Keine bezahlte Priorisierung
  - keine Bevorzugung bestimmter legaler Inhalte gegenüber anderen legalen Inhalten aufgrund von Entgeltzahlungen
- Ziele
  - ISPs sollten Nutzer oder Randnetzbetreiber nicht schaden
  - für größere Transparenz sorgen
  - sinnvolles Netzmanagement erlauben → ohne direkte kommerzielle Absichten

EU Verordnung 10788/2/15

- Artikel 3 Absatz 3: „Anbieter von Internetzugangsdiensten behandeln den gesamten Verkehr bei der Erbringung von Internetzugangsdiensten gleich, ohne Diskriminierung, Beschränkung oder Störung, sowie unabhängig von Sender und Empfänger, den abgerufenen oder verbreiteten Inhalten, den genutzten oder bereitgestellten Anwendungen oder Diensten oder den verwendeten Endgeräten.“
- „Damit derartige Maßnahmen als angemessen gelten, müssen sie transparent, nichtdiskriminierend und verhältnismäßig sein und dürfen nicht auf kommerziellen Erwägungen, sondern auf objektiven unterschiedlichen technischen Anforderungen an die Dienstqualität bestimmter Datenverkehrskategorien beruhen.“
- Artikel 3 Absatz 5: „Netzbetreibern steht es frei, andere Dienste, die keine Internetzugangsdienste sind, anzubieten, die für bestimmte Inhalte, Anwendungen oder Dienste oder eine Kombination derselben optimiert sind, wenn die Optimierung erforderlich ist, um den Anforderungen der Inhalte, Anwendungen oder Dienste an ein bestimmtes Qualitätsniveau zu genügen.“


Definition/
Invarianten
Ziele und Struktur
Wachstum und
Skalierbarkeit
Architektur
Robustheit
Entwurfsprinzipien
Neuere Ansätze
Konflikte

Routing und Adressierung

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

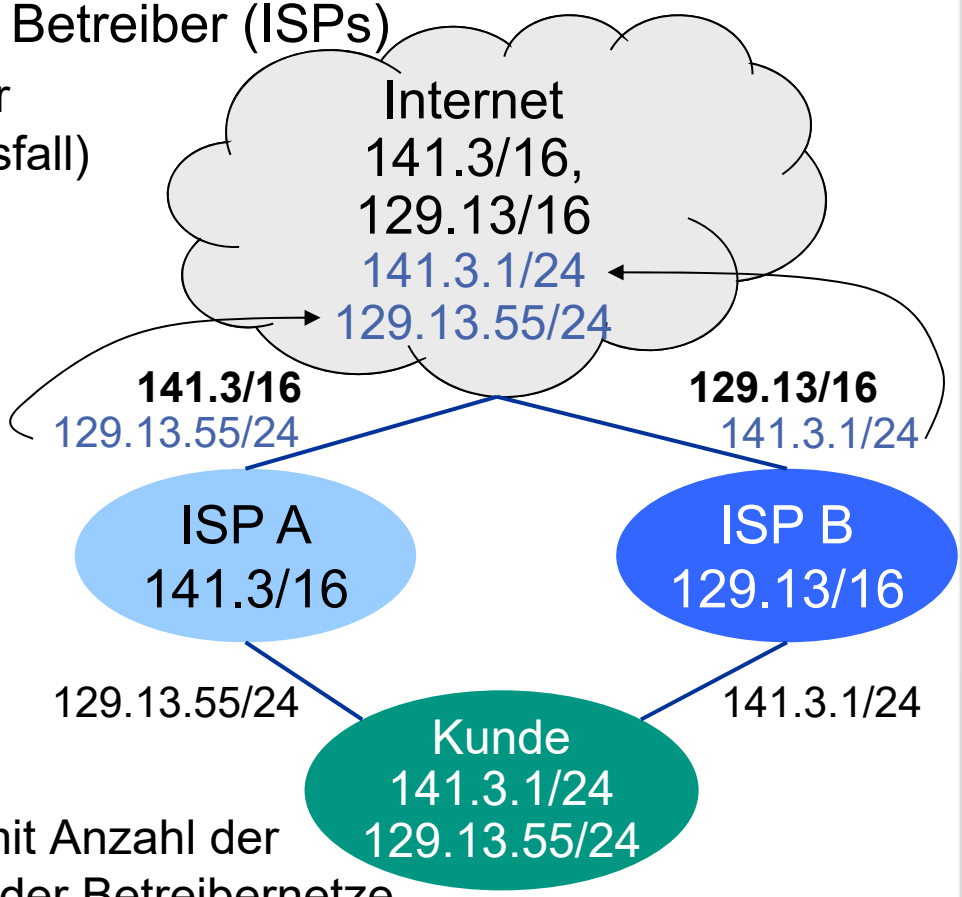
[RFC4984]

- 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

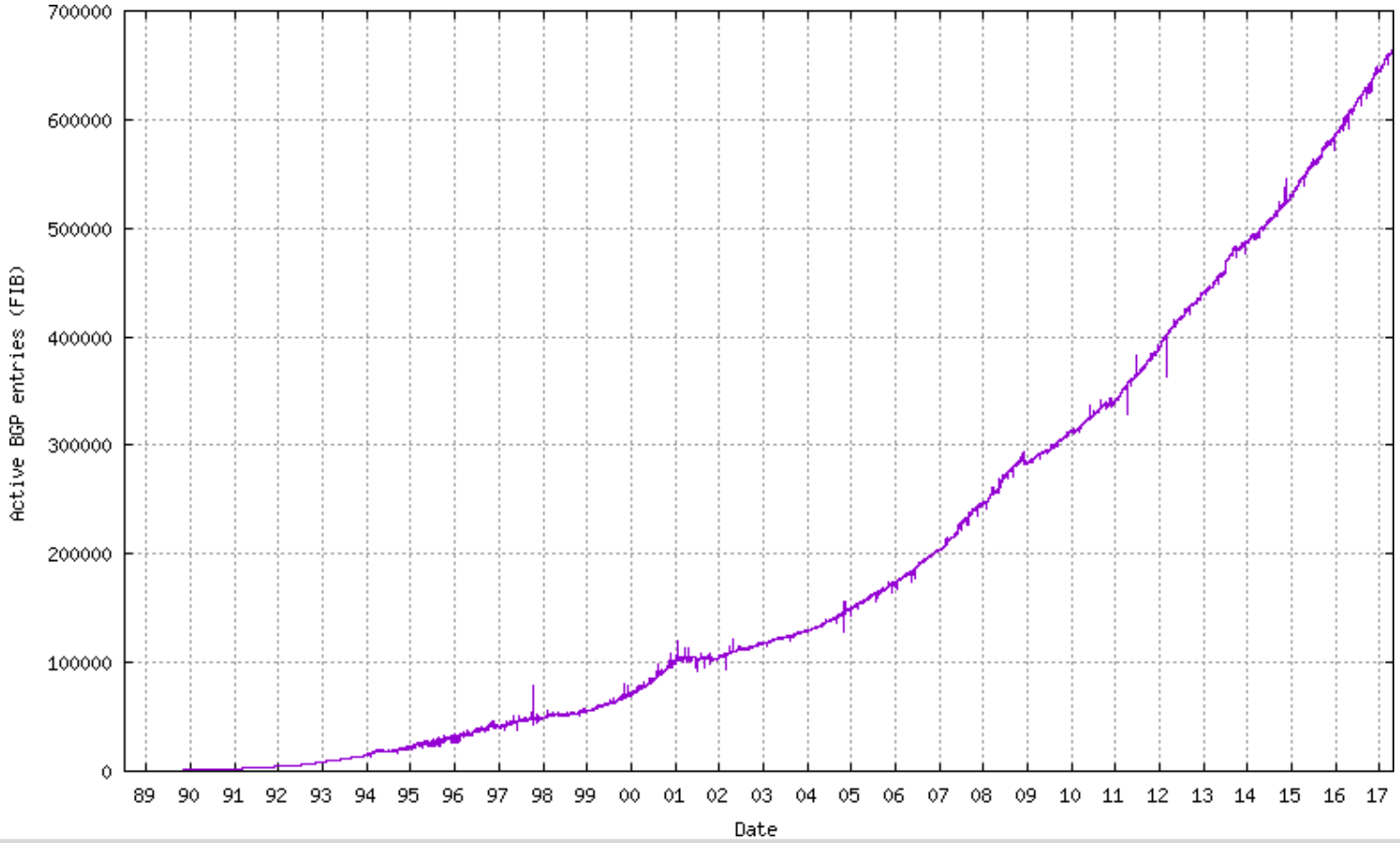
- Abhängigkeit vom Internet wird zunehmend größer
  → zuverlässige Konnektivität wichtig
- Internet-Anbindung über mehrere Betreiber (ISPs)
  - Verbesserte Toleranz gegenüber Ausfällen (einschließlich ISP-Ausfall)
  - Lastverteilung
- Situation heute:
  - Kundennetz hat zwei oder mehr Netzadressen

  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 hat die IP-Adresse derzeit zwei Funktionen:
  - Identifikation des Endsystems (Identifikator)
    - globaler Adressraum
  - Lokation des Endsystems (Lokator)
    - Adresse beinhaltet topologische Information für das Routing
- Diese überladene Semantik 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?
  - Erreichbarkeitsstatus der Lokatoren?
  - Untersuchung verschiedener Ansätze in der IRTF Routing Research Group

Identifier-Locator Network Protocol

[RFC6740]

- Identifier (I): topologieunabhängiger Name für Knoten
  - 64-bit
- Locator (L): topologiegebundener Name für IP-Subnetz
- I-L Vector beschreibt Bindung [I,L]
- DNS RR enthält [I,L] Informationen
- Paket enthält Quell [I,L] und Ziel [I,L]
- Keine Änderung
  - der meisten Anwendungen
  - der Netzinfrastruktur
- Einbettung für IPv6 einfach
- Erweiterung von ICMP für Locator Updates

Nutzung der Namen für Zustandsinformation der jeweiligen Schicht

Schicht	IP	ILNP
Anwendung	FQDN, IP Adresse	FQDN
Transport	IP Adresse	Identifier
Netzwerk	IP Adresse	Locator
Physische Schnittstelle	IP Adresse	MAC Adresse

Ansatz LISP

 [RFC6830]

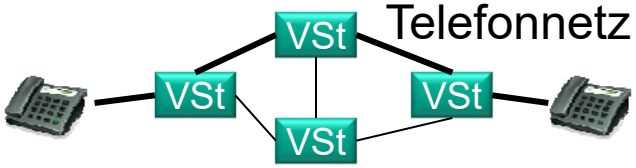
- Möglichst wenig Veränderungen, keine Änderungen in den Endsystemen
- Trennung von Endpoint Identifier (EID) und Routing Locator (RLOC)
  - EID auch als Präfix organisiert, entspricht praktisch PI-Präfix
  - RLOC: heutige PA-Präfixe, aggregierbar
  - LISP: Locator/ID Separation Protocol
- Abbildungsfunktion 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?

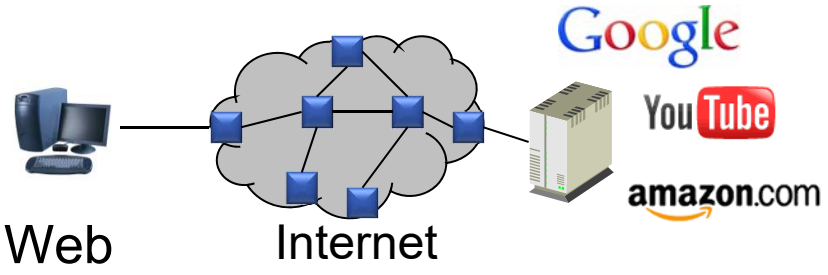
Content Centric Networking

- 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

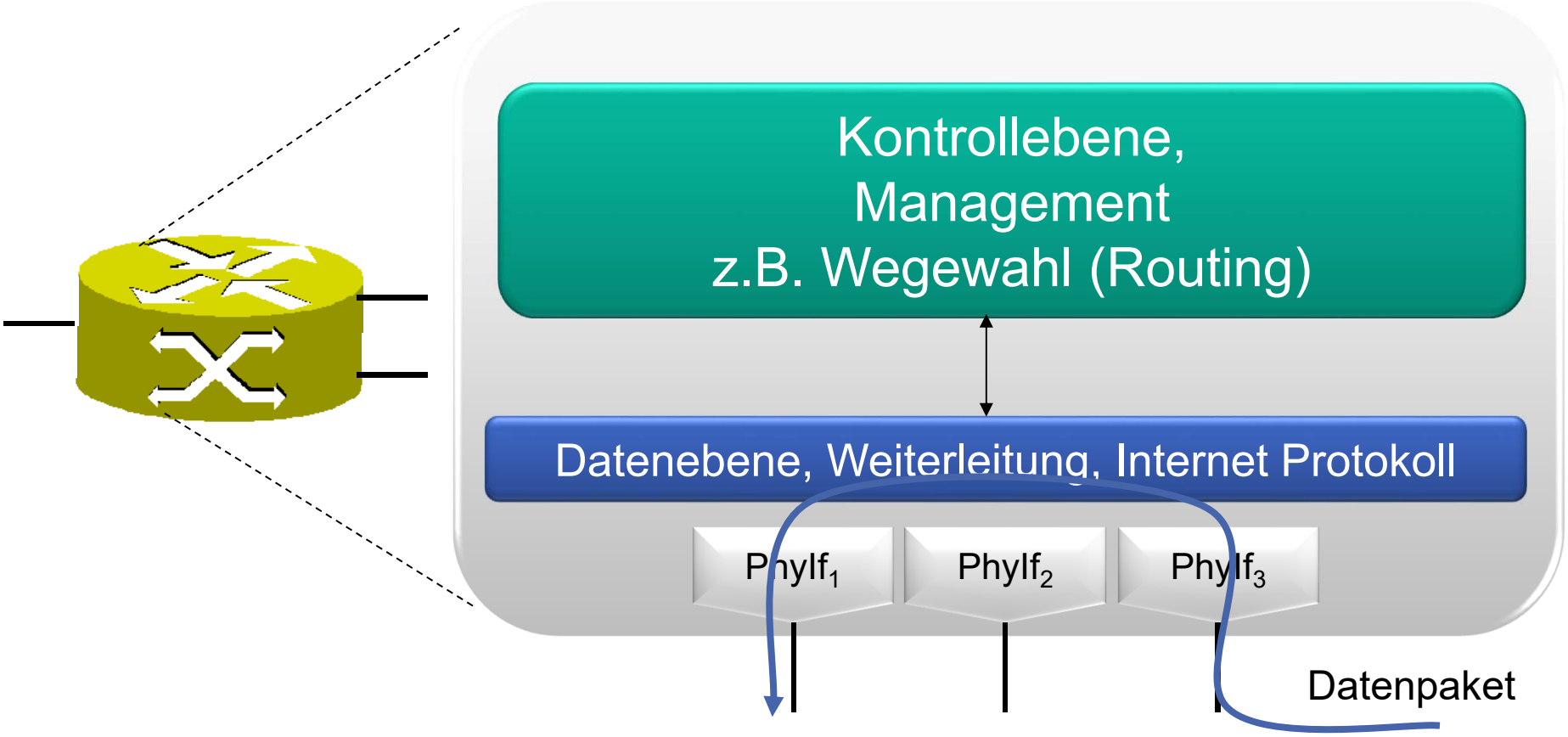
Staukontrolle

- 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?
  - Explizite Stauinformation aus dem Netz

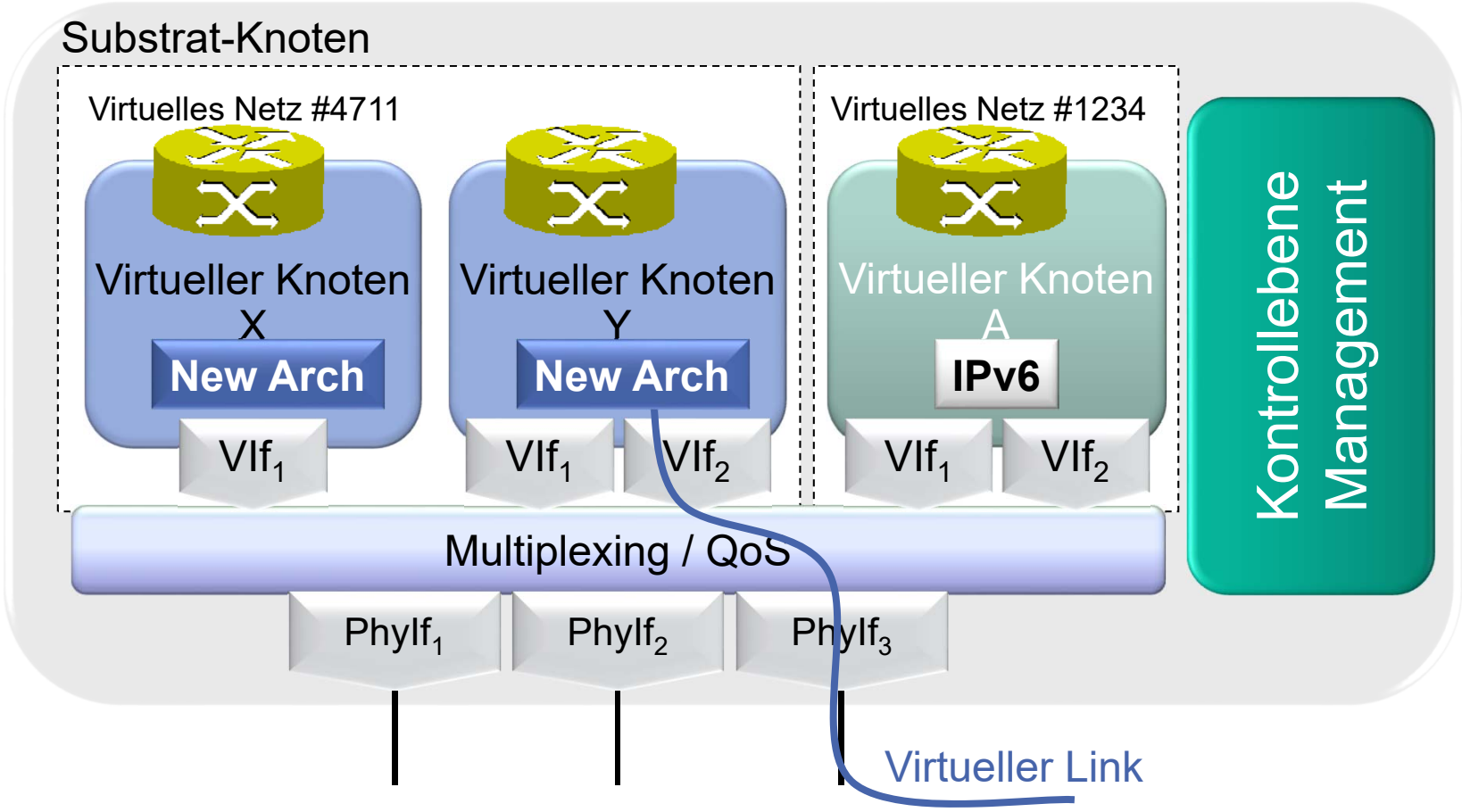
Wege zur Innovation

- Einbringen innovativer Ansätze – wie?
- Ändern der Infrastruktur aufwändig
  - Ausbringen neuer Protokolle und Mechanismen langwieriger Prozess (IPv6, Multicast, usw.)
  - Kein „Flag Day“ möglich
- Möglicher Ansatz: Netzvirtualisierung
  - 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

Normaler Router



Netzknoten mit Virtualisierungsunterstützung



Herausforderungen

- Erhöhte Managementkomplexität
  - Vielzahl virtueller Ressourcen
  - Monitoring, Fehlersuche
- Gemeinsame Kontrollebene notwendig
  - Etablieren virtueller Links zwischen Betreibern
  - technologie- und netzübergreifend
- Substrat immer noch wichtig
  - wie kann das ausgetauscht werden?
  - sogar während neue Technologien darauf verwendet werden?

Weitere Anforderungen an das Internet von morgen (nach Dave Clark)


[Clark09]

- bessere Verwaltbarkeit
- ökonomische Realisierbarkeit
- den gesellschaftlichen Anforderungen entsprechend
- Langlebigkeit – Möglichkeit zur Evolution
- Unterstützung für
  - das Rechnen von morgen
  - neue Netztechnologien
  - neue Anwendungen

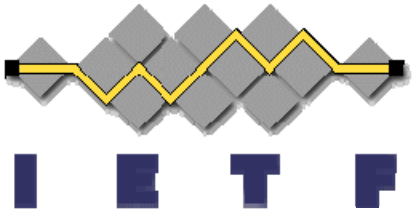
Forschungsbedarf im Internet

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

Weiterentwicklung des Internets?

- Internet Society www.isoc.org
  - kümmert sich um die Entwicklung und Verbreitung des Internets
- Internet Research Task Force www.irtf.org
  - Betrachtet längerfristige Entwicklungen
  - Führt Voruntersuchungen durch
  - Eher geschlossene Gruppen, aber offene Mailinglisten
- Internet Engineering Task Force www.ietf.org
  - 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)

Literatur (1)

[ABEH+04] B. Ahlgren, M. Brunner, L. Eggert, R. Hancock, S. Schmid. Invariants: a new design methodology for network architectures. In Proceedings of the ACM SIGCOMM workshop on Future directions in network architecture (FDNA '04), 2004. ACM, http://doi.acm.org/10.1145/1016707.1016719

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

[Clark09] D. Clark: “Toward the Design of a Future Internet”, Version 7.0, October 2009, Working Paper, http://groups.csail.mit.edu/ana/People/DDC/Future%20Internet%207-0.pdf

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

Literatur (2)

[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://esamultimedia.esa.int/docs/esa-x-1819eng.pdf, 19. July, 1996

[FlJa94] S. Floyd, V. Jacobson, „The Synchronization of Periodic Routing Messages“, IEEE/ACM Transactions on Networking, Vol. 2, No. 2, April, 1994, http://portal.acm.org/citation.cfm?id=187045

[FaFF99] M. Faloutsos, P. Faloutsos, C. Faloutsos: On Power-Law Relationship of the Internet Topology, ACM SIGCOMM, 1999

[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

Literatur (3)

[Labo10] C. Labovitz: Internet Traffic and Content Consolidation, Plenary presentation at IETF 77, http://www.ietf.org/proceedings/77/slides/plenaryt-4.pdf

[Lab+10] C. Labovitz, S. Iekel-Johnson, D. McPherson, J. Oberheide, F. Jahanian: Internet Inter-Domain Traffic, ACM SIGCOMM 2010, http://ccr.sigcomm.org/online/files/p75_0.pdf

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

[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.

Literatur (4)

[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.

[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.

[RFC 6740] RJ Atkinson und SN Bhatti. Identifier-Locator Network Protocol (ILNP) Architectural Description. RFC 6740 (Experimental), IETF, November 2012. URL: http://www.ietf.org/rfc/rfc6740.txt.

[RFC 6830] D. Farinacci, V. Fuller, D. Meyer und D. Lewis. The Locator/ID Separation Protocol (LISP). RFC 6830 (Experimental), IETF, Januar 2013. URL: http://www.ietf.org/rfc/rfc6830.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

Literatur (6)

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