Brandenburg
University of Technology
Cottbus

07·07·2010

TOPOLOGIEADAPTIERTE P2P-INFORMATIONSOVERLAYS

MICHAEL VOGEL

5. GI FG SIDAR GRADUIERTEN-WORKSHOP
REAKTIVE SICHERHEIT – SPRING, BONN

GLIEDERUNG

Brandenburg
University of Technology
Cottbus

Motivation

P2P Intrusion Detection

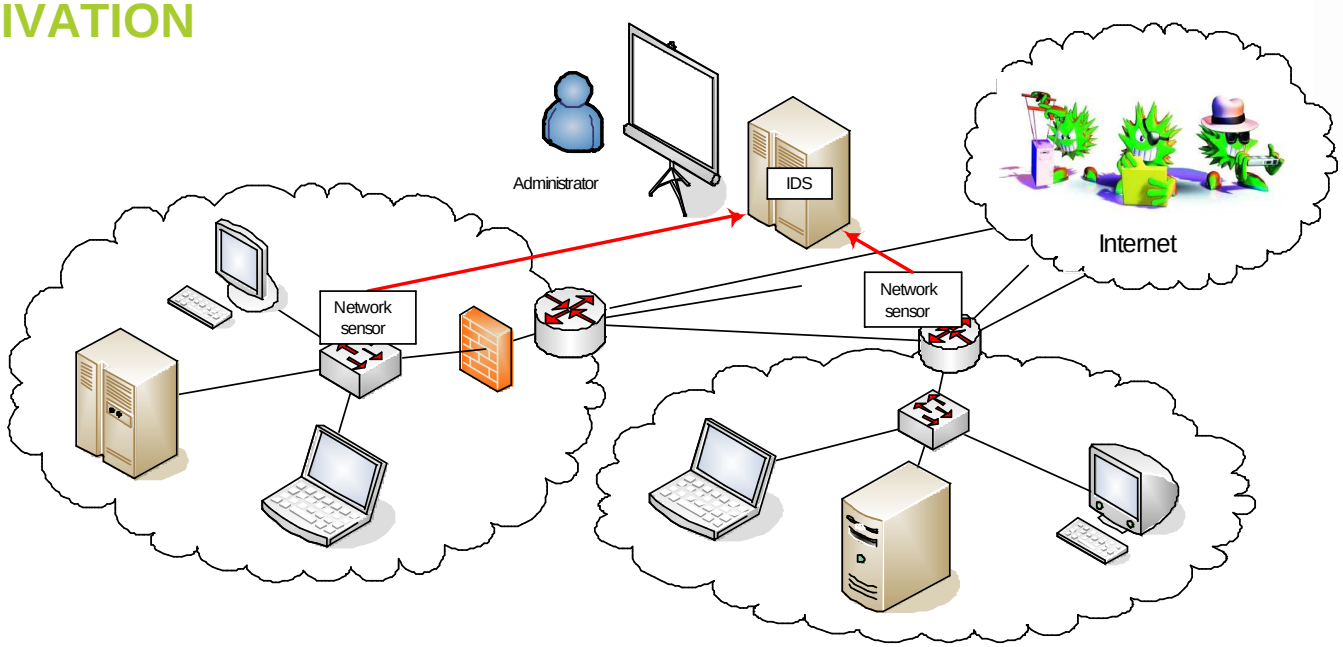
Topologie-Identifizierung

Topologie-adaptiertes Overlay

Offene Probleme

Zusammenfassung

MOTIVATION



Heutige Intrusion Detection Systeme:

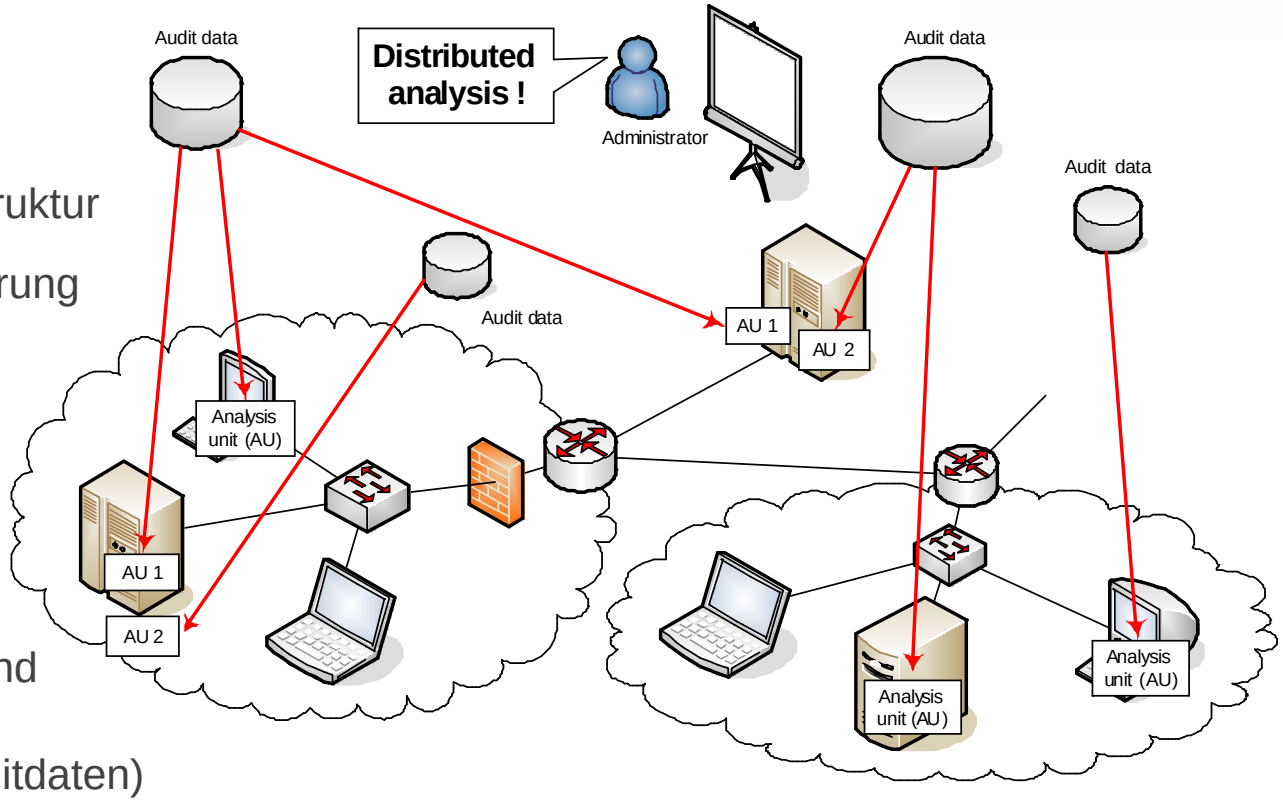
- Dedizierte statisch konfigurierte Hard- u. Software
- keine Redundanz (Kostenfaktor)
- Selektiver Schutz von Netzbereichen (Uplinks), kein globales Bild
- Verwerfen von Beobachtungsdaten bei hoher Last

MOTIVATION

Brandenburg
University of Technology
Cottbus

Vision:

- Verteilte, robuste, redundante Beobachtungsinfrastruktur
- Dynamische Adaptierung an aktuelle Netzsituation



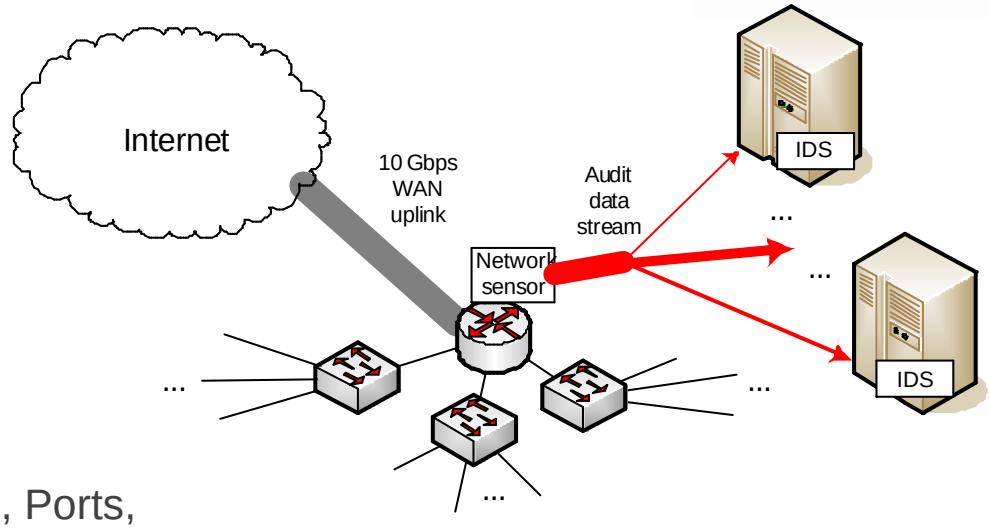
Ziel:

- Dezentralisierte, verteilte Erfassung und Analyse von Beobachtungen (Auditdaten)
- Nutzung bestehender Hardware (Endsysteme u. Netz)
- Robustheit gegen partielle Netz- u. Systemausfälle (z.B. Hosts, Uplinks)

PARTITIONIERUNG VON ANALYSEAUFGABEN

Brandenburg University of Technology Cottbus

Verschiebung umfangreicher Analyseaufgaben: Unmöglich!
→ Aufteilung von Aufgaben notwendig

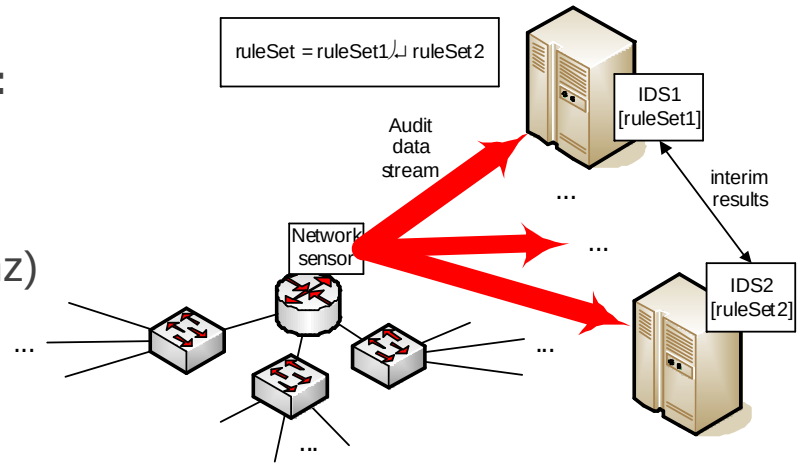


Aufteilung der Beobachtungsdaten
(kont. breitbandiger Datenstrom):

- z. B. Aufspaltung nach Quell- Ziel IP, Ports, Protokoll (Netzwerkbasierte IDS)

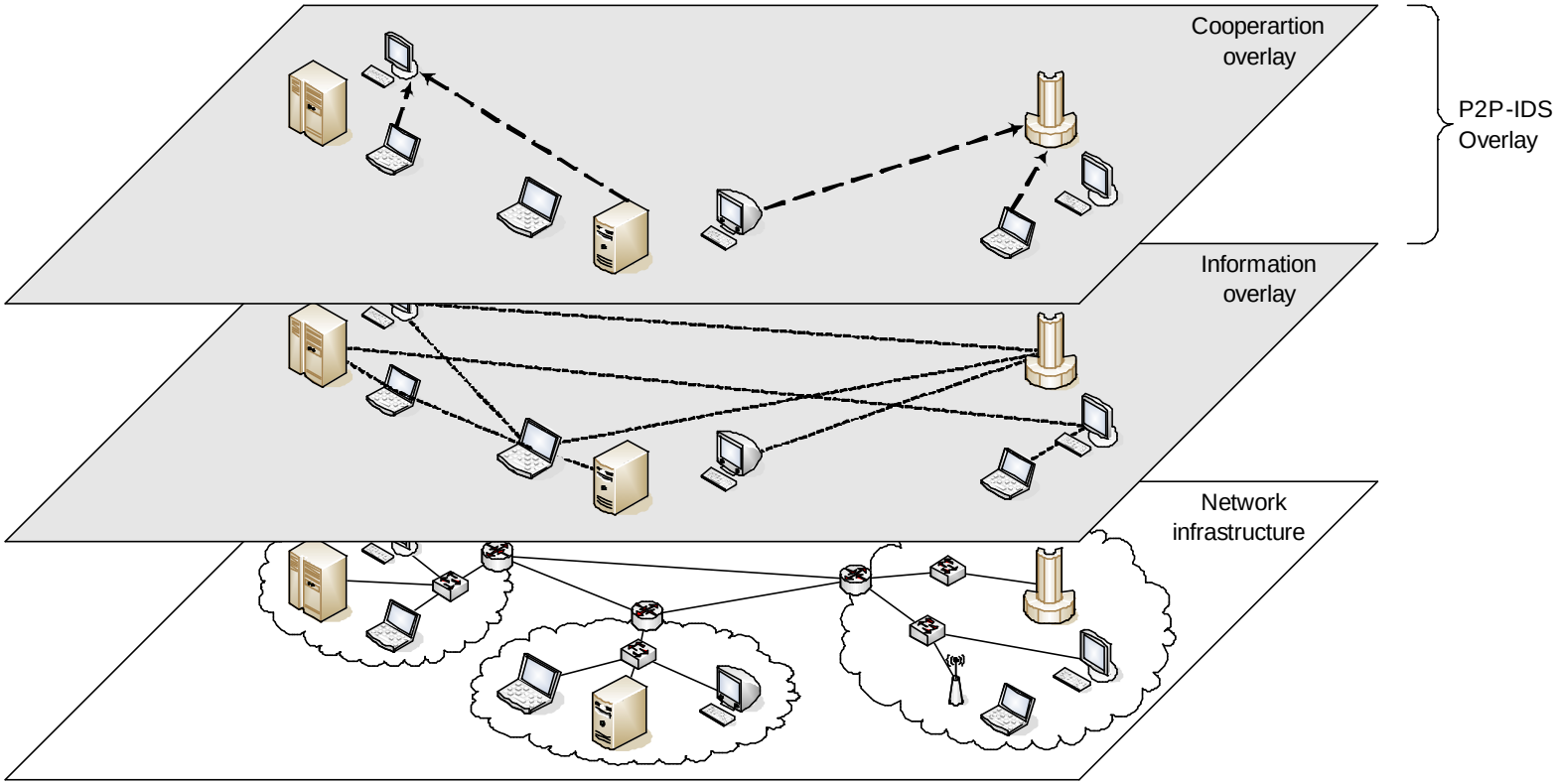
Aufteilung der Angriffssignaturen/Suchmuster:

- Datenduplizierung notwendig (hohe Netzlast)
- Austausch von Systemzuständen zw. kooperierenden IDS (erfordert geringe Netzlatenz)



PEER-TO-PEER IDS

Brandenburg
University of Technology
Cottbus

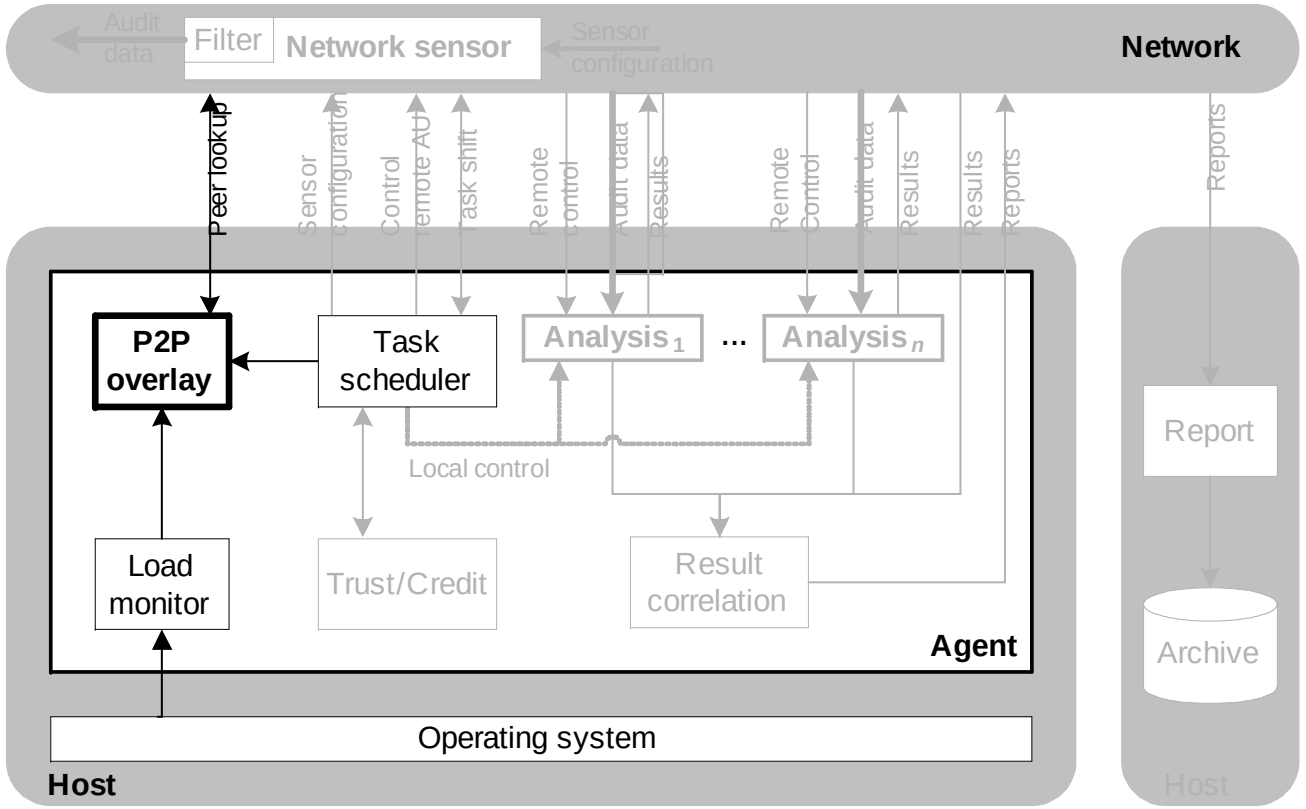


- **Informationsoverlay:** Suche nach verfügbaren entfernten Analyseressourcen
- K**ooperationsoverlay:** Aushandlung, Verwaltung von Kooperationen, Aufgabendelegierung

P2P INFORMATION OVERLAY

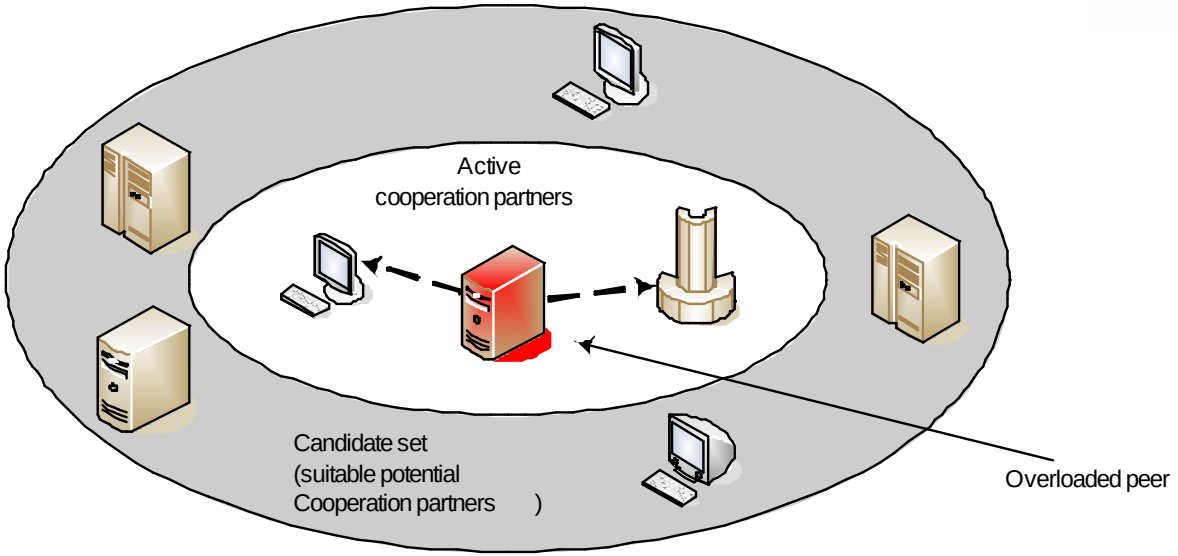
Brandenburg
University of Technology
Cottbus

- Kontinuierliche Erfassung freier Systemressourcen
- Verbreitung der Informationen im P2P Overlay
- Suche nach verfügbaren Ressourcen auf entfernten Peers im Overlay



AKTIVE UND POTENZIELLE KOOPERATIONSPARTNER

Brandenburg
University of Technology
Cottbus



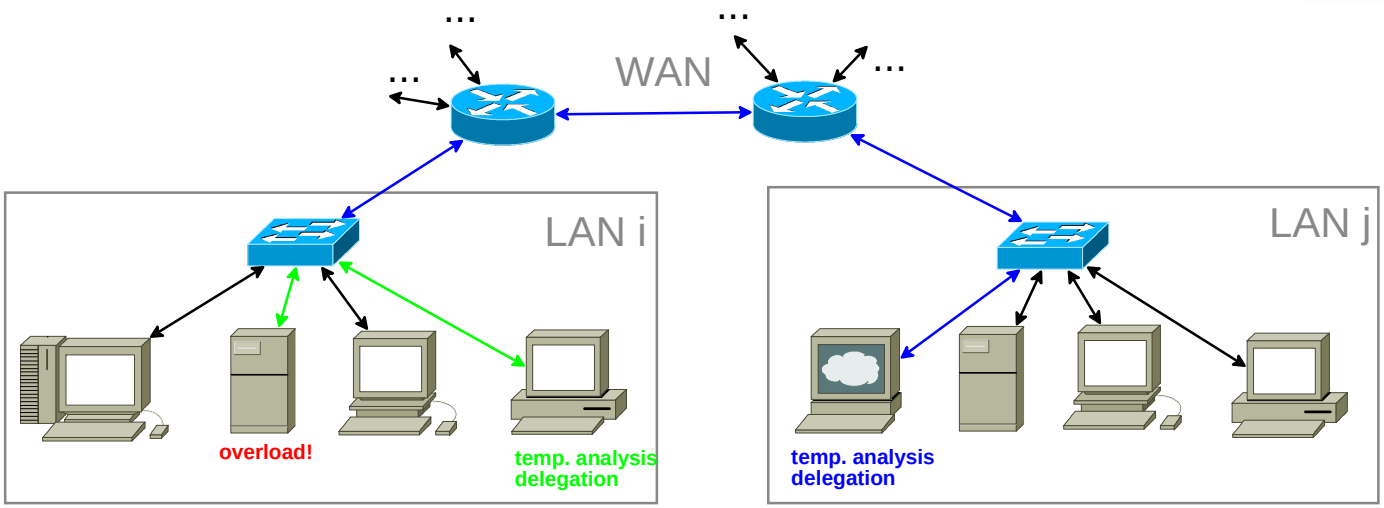
Kandidatenmenge: Kontinuierlich aktualisierte Liste geeigneter Kooperationspartner (Peers) mit passenden freien Ressourcen

Suche nach neuen Partnern (Peers) im Overlay falls:

- Zusätzliche Ressourcenbedarf (wachsende Last)
- Wegbrechende bzw. das Overlay verlassende aktive Kooperationspartner

GEEIGNETE KOOPERATIONSPARTNER

Brandenburg
University of Technology
Cottbus



Zwei Aspekte:

- Host: Partner mit geeignete Ressourcen: ausreichende freie CPU- u. Speicherressourcen, geeignete Analyseeinheiten, zeitliche Verfügbarkeit, usw.
- Netz: Datentransfers mit ausreichender (hoher Bandbreite), möglichst geringe Latenz

→ Auswahl bzgl. Netztopologie „naher“ Kooperationspartner

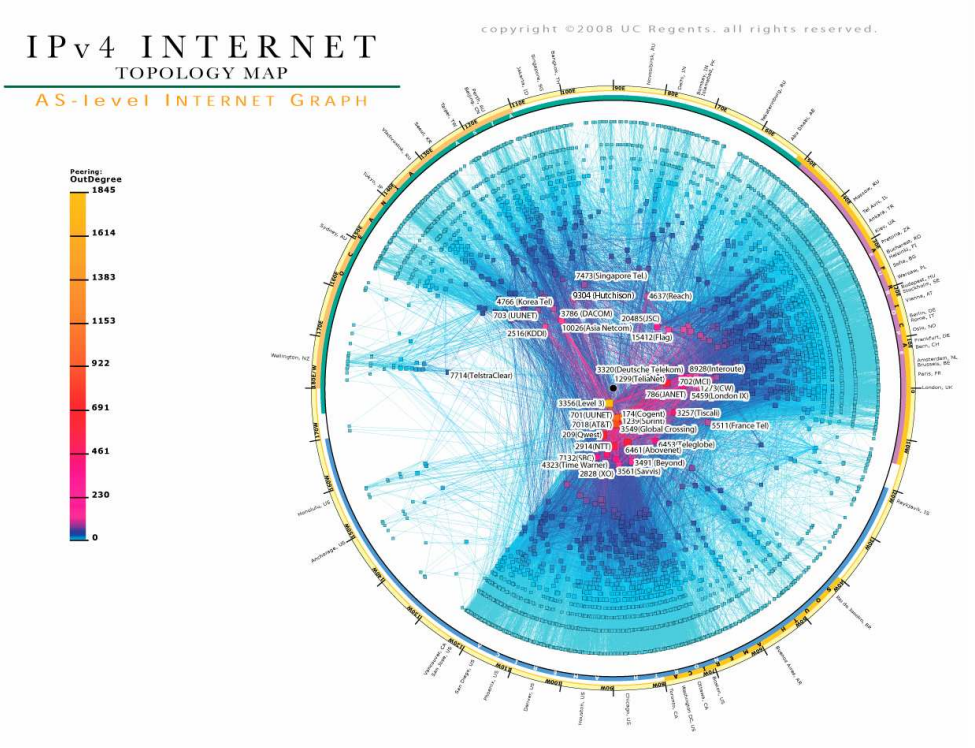
INTERNET-TOPOLOGIE

Internet:
- Verbund autonomer Systeme (AS):
- Peerings

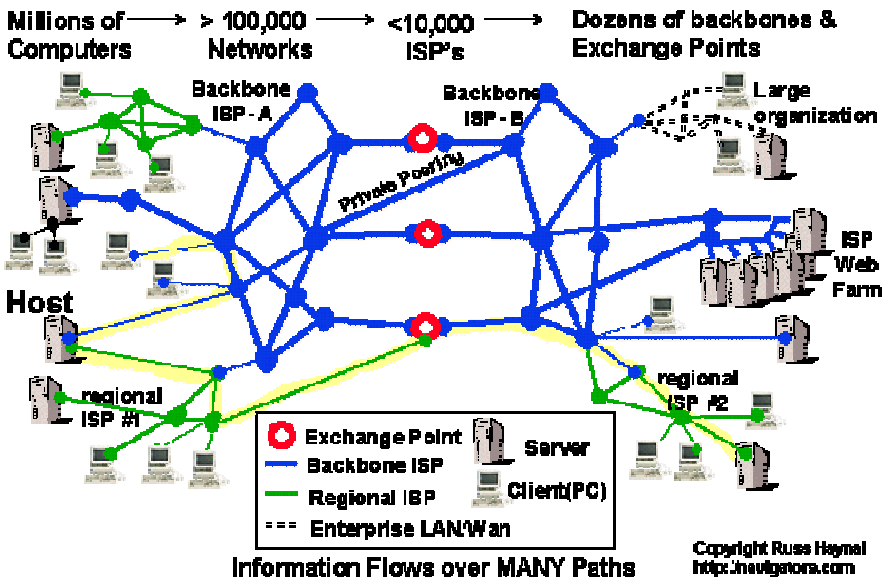
Autonomes System:
- Organisationseinheit
- bündelt meist mehrere Netze (CIDR)

Netz (z.B. BTU-Netz):
- Untergliederung in Subnetze (CIDR)

Subnetz / LAN:



http://www.caida.org/research/topology/as_core_network/historical.xml

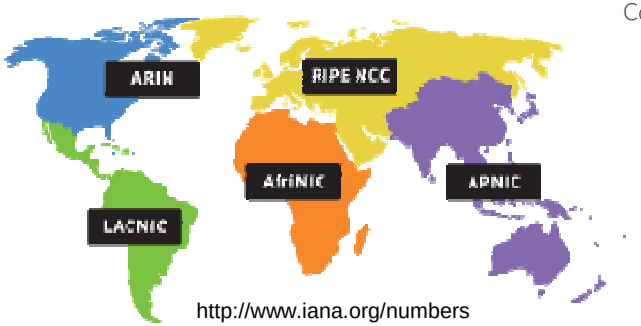


TOPOLOGIE-IDENTIFIZIERUNG

Brandenburg
University of Technology
Cottbus

Peer identifiziert eig. “Standort” in Netztopologie des Internets:

· öff. IP-Adresse (global erreichbar)



http://www.iana.org/numbers

IP-Adressvergabe:

IANA (Internet Assigned Numbers Auth.):

RIR – regionale Internet-Registrare (Kontinent):

· z.B. RIPE NCC, ARIN, APNIC

· feste Zuordnung Adressblöcke → RIR

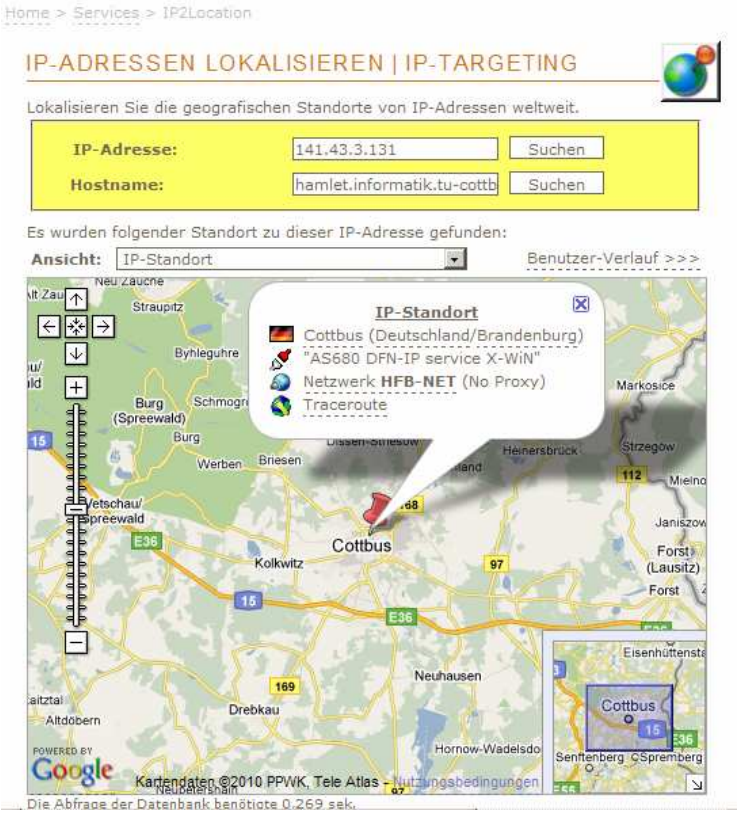
LIR – lokale Registrare: ISPs

Geolokation:

· Datenbanken/Webdienste

· Abbildung von IP-/Netzadressen auf geogr. Koordinaten

· Einträge teilw. ungenau od. fehlerhaft



TOPOLOGIE-IDENTIFIZIERUNG WAN

Brandenburg University of Technology Cottbus

Identifizierung AS, Netz:

- Autonomes System (AS-Nr.)
- Netz (*Netzname*)

→ *whois*-Dienst der RIRs:

```
[mvogel@hamlet ~]$ whois 141.43.3.131
[Querying whois.ripe.net]
% This is the RIPE Database query service.
...
% Information related to '141.43.0.0 - 141.43.255.255,
inetnum: 141.43.0.0 - 141.43.255.255
netname: HFB-NET
descr: Technische Universitaet Cottbus
country: DE
...
% Information related to '141.42.0.0/15AS680,
route: 141.42.0.0/15
descr: DFN-AGG-141.42
origin: AS680
mnt-by: DFN-MNT
source: RIPE # Filtered
```

Informationen:

- AS-Nr: 680 (DFN-IP service X-WiN)
- Netzname: HFB-NET (HS f. Bauwesen)

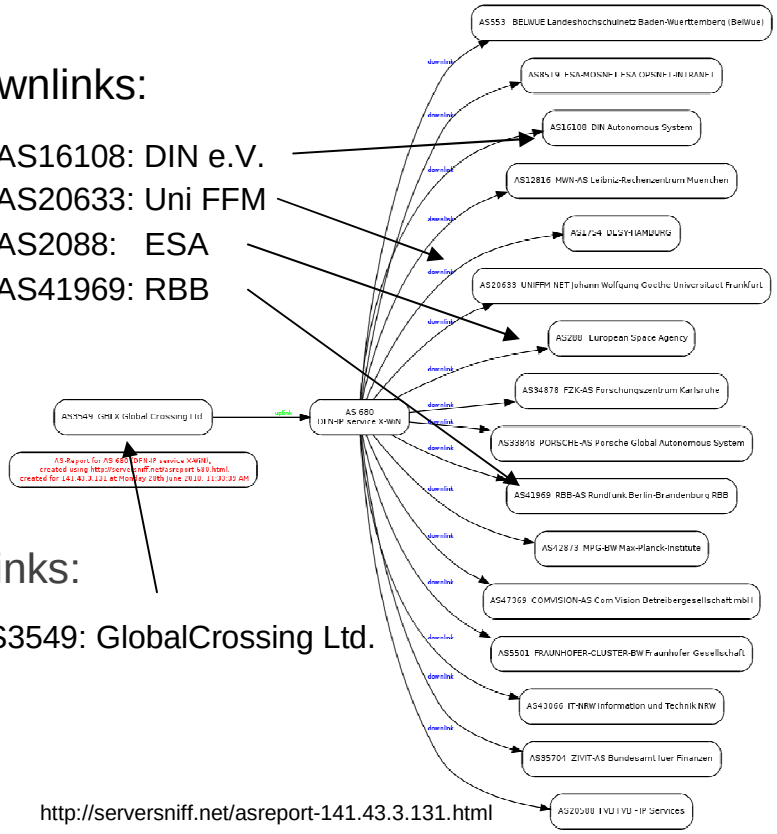
Identifizierung Routinginformationen:

- BGP Inter AS-Routing
- Peeringbeziehungen (Uplinks/Downlinks)
- Data sets von akad. Messungen

Bsp: AS608: DFN-IP Service X-WiN

- Downlinks:

AS16108: DIN e.V.
AS20633: Uni FFM
AS2088: ESA
AS41969: RBB



- Uplinks:

AS3549: GlobalCrossing Ltd.
...

http://serversniff.net/asreport-141.43.3.131.html

TOPOLOGIE-IDENTIFIZIERUNG LAN

Brandenburg University of Technology Cottbus

Identifizierung Subnetz:

· IP-Adresse

· Netzpräfix/Subnetzmaske (CIDR)

→***lokale Netzkonfiguration (DHCP)*:**

Bsp: `141.43.3.131`

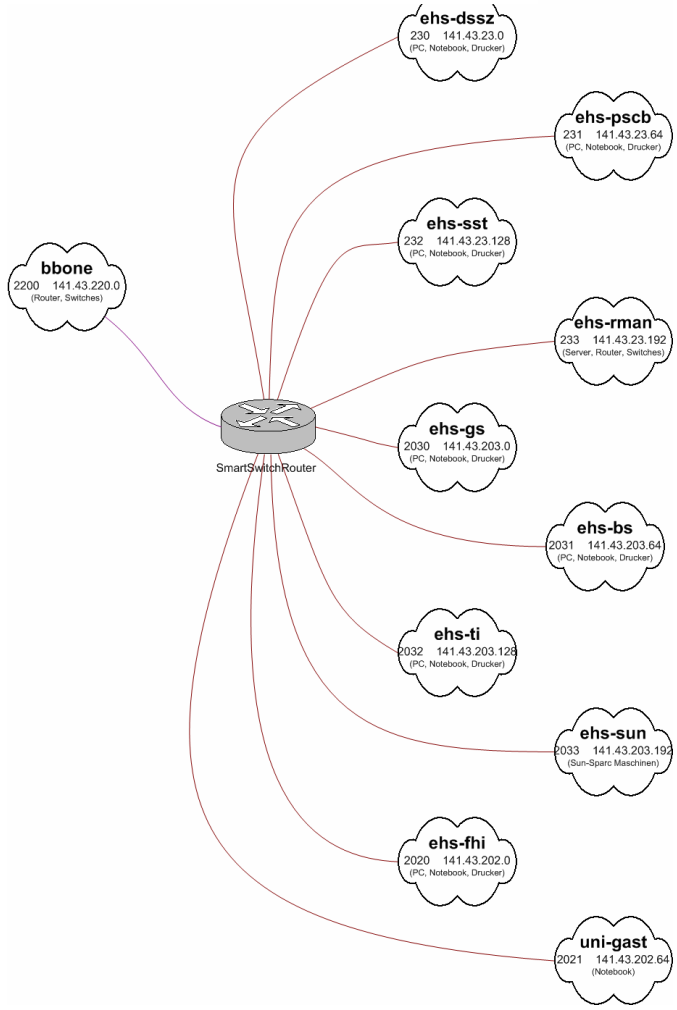
```
[mvogel@eros ~]$ ifconfig
eth0 Link encap:Ethernet  HWaddr 00:30:05:CF:CC:54
inet addr:141.43.3.131  Bcast:141.43.3.191  Mask:255.255.255.192
...
```

Subnetz: 141.43.3.128/26 → LS RNKS

weitere Subnetze an BTU:

141.43.23.0/26 → LS SST
141.43.203.64/26 → LS BS
…

Abb. Subnetze des Insituts (2004):



http://eiche.informatik.tu-cottbus.de/~lehmann/Sysadmin/EHS-Netze.png

TOPOLOGIE ADAPTIERTE OVERLAYS

Brandenburg University of Technology Cottbus

Andere P2P Overlays:

Filesharing (Gnutella, BitTorrent, …)

- i.a. keine Beachtung der Netztopologie:
- Auswahl optimaler Peers mit hoher Datentransferrate (Download)
- Latenz irrelevant

VoIP, Videokonferenz:

- ausreichende Bandbreite (Video-/ Audiodatenstrom)
- mgl. geringe Latenz

Bsp: Skype:

- Edge Peer: 1 Uplink, Relay Peer: 1-2 Uplinks, mehrere Downlinks
- Audio/Video: möglichst Direktverbind.
- Nutzung von Peers als Relayproxy (Firewalldurchdringung)

```
[mvogel@hamlet ~]$ netstat -b
...
TCP hamlet:3438 martinoli.fisica.unige.it:https ESTABLISHED 1728
[Skype.exe]
...
```

→ Universita di Genova, GENUANET, AS 137 (GARR-B Backbone),

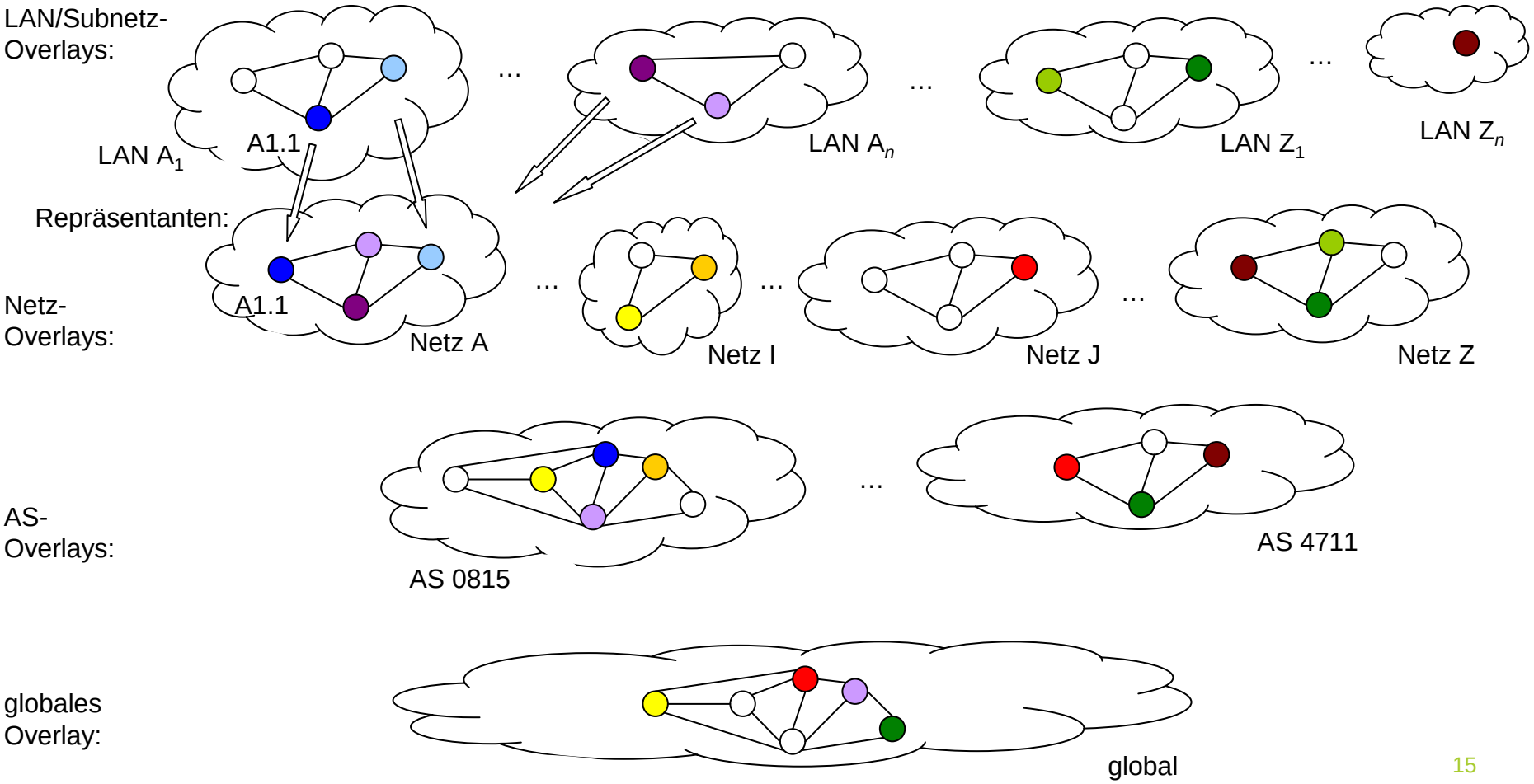
Route: AS806 (DFN) → AS20965 (Géant) → AS137 (GARR-B)

Beobachtung: Skype bevorzugt im DFN(BTU) Peers an deutschen od. europäischen Forschungseinrichtungen

mgl. Grund: Forschungsnetze stark bzgl. Latenz optimiert

P2P-INFORMATIONS-OVERLAY

Brandenburg
University of Technology
Cottbus



P2P-INFORMATIONS-OVERLAY

Brandenburg
University of Technology
Cottbus

Vorteil:

- Abbildung der Lokalitätsbeziehungen in die Overlay-Topologie
- Robustheit: bei Ausfall von Uplinks, Teilnetzen:
    - Aufspaltung des Overlays in Teil-Overlays
    - nur ohnehin nicht mehr erreichbare Peers verlassen das Overlay
    - dyn. Wiederherstellung des Overlays sobald Link wieder verfügbar

OFFENE PROBLEME

Brandenburg
University of Technology
Cottbus

Mechanismus für Latenzmessungen

- Detailliertere Bewertung potenzieller Kooperationspartner
- Repräsentantenbildung / Begrenzung der Messvorgänge
- Starten / Anfrage von Messaufträgen an entfernte Peers

Vermaschungsgrad des Overlays

- Adaptierung des Overlays an hierarchische Internet-Infrastuktur theoretisch nachteilig für Grad des Graphen / Robustheit
- dyn. Anpassung der Repräsentantenzahl an Churn-Rate

Repräsentanten in übergeordneten Overlays

- Repräsentantenüberwachung / -neuwahl

ZUSAMMENFASSUNG

Brandenburg
University of Technology
Cottbus

P2P-Informationsoverlays für verteilte Ressourcennutzung:

- Optimierung/Beachtung der Kommunikationswege / -aufwand
- Analyse der genutzten IP-Infrastruktur
- Adaptierung des Overlays an Infrastruktur
- selektiv zusätzliche Latenzmessungen für feingranulare Optimierung

Brandenburg
University of Technology
Cottbus

DANKE FÜR DIE AUFMERKSAMKEIT!

ANMERKUNGEN? FRAGEN?