Fachhochschule Gelsenkirchen

Internet Availability System
→ Idea and Realization

Prof. Dr. (TU NN)
Norbert Pohlmann

Institute for Internet Security - if(is)
University of Applied Sciences Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet security.

Content

- Aim and outcomes of this lecture
- Idea/Concept of the Internet Availability System
- Routing
- Implementation
- Results
- Summary

Content

- **Aim and outcomes of this lecture**
- Idea/Concept of the Internet Availability System
- Routing
- Implementation
- Results
- Summary

Internet Availability System (IVS)
→ Aims and outcomes of this lecture

Aims

- To introduce an Internet Early Warning System with an availability approach
- To explore the structure of the Internet Availability System
- To visualize the routing of the Internet
- To analyze the results of the Internet Availability System

At the end of this lecture you will be able to:

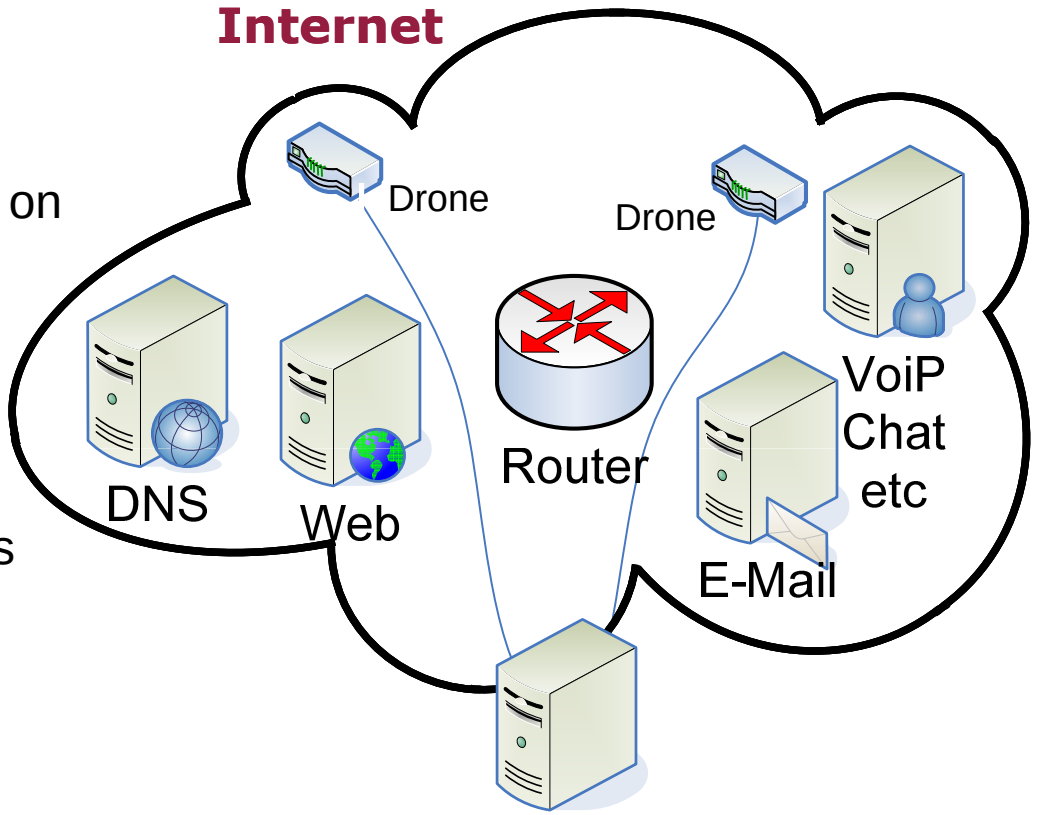
- Understand what is meant by the Internet Availability System.
- Know something of the structure of the Internet Availability System.
- Know what could be the results of the Internet Availability System.
- Understand the capabilities and limitations of the Internet Availability System.

Content

- Aim and outcomes of this lecture
- **Idea/Concept of the Internet Availability System**
- Routing
- Implementation
- Results
- Summary

Internet Availability System (IVS)
→ Idea

- Observation of the critical infrastructure **„Internet".**
- **Drones** are placed in strategically selected spots to gather information on availability.
- Different types of availability data could gathered
  - Important websites
  - DNS service
  - Communication routes of routers
  - E-Mail Services and Server
- **Parameter:** Quality of Service: Bandwidth, Bit Error Rate, Jitter, Delay, Packet Loss Rate
- A centrally managed **Evaluation System** is used to analyze the raw data and to display the detailed results in an intuitive manner.

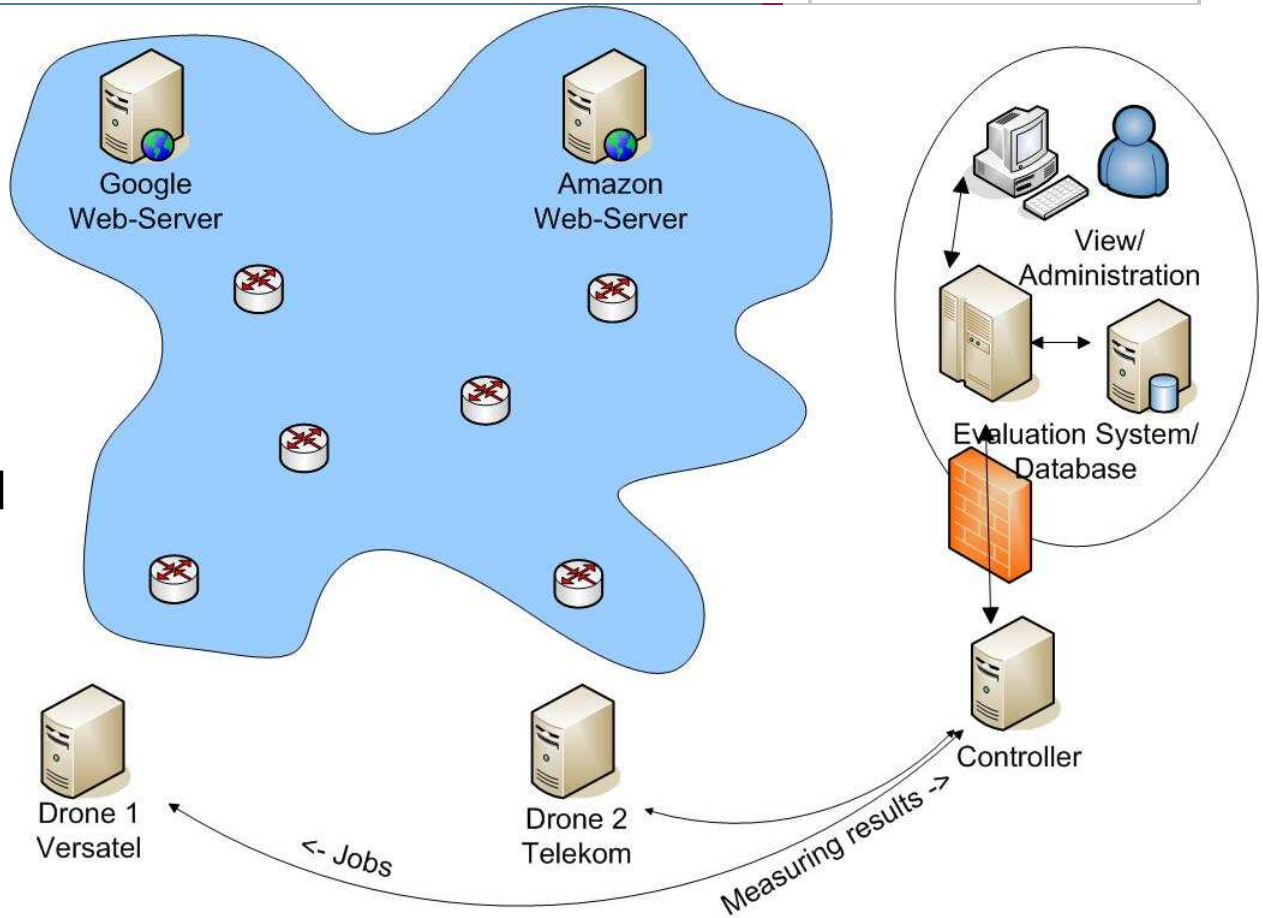


Drone: active Probe

Placement of the drones is done independent from third parties!

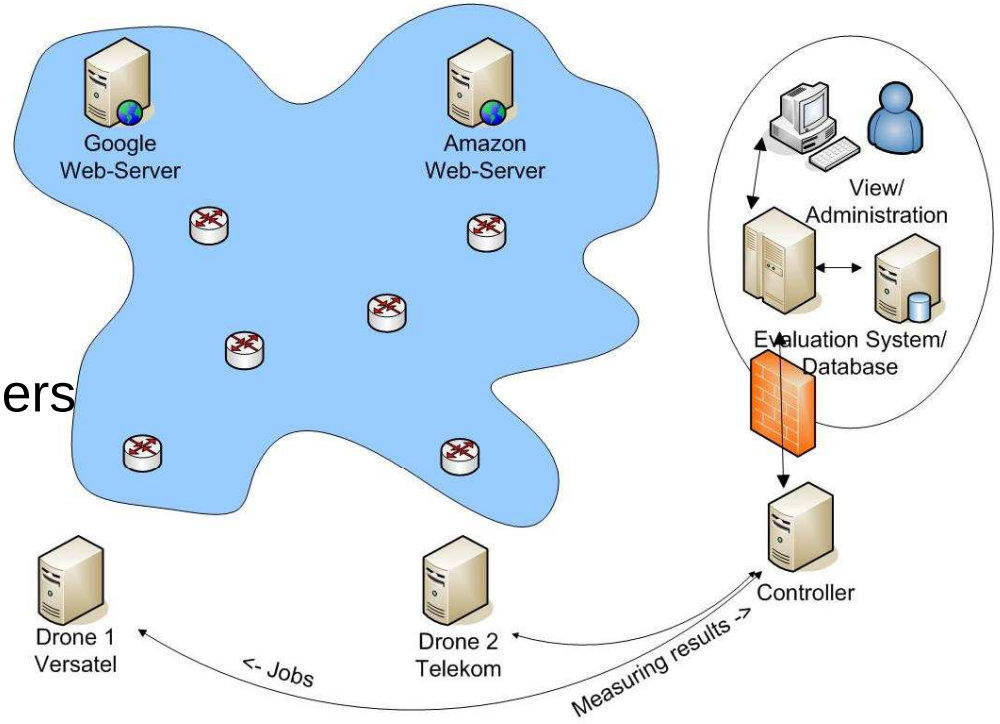
Internet Availability System (IVS) → Concept (1/3)

- Modules currently implemented for measurement
  - **HTTP**
    - Any file over HTTP
      - Welcome page
      - Dynamic linked page
    - Domain (www.heise.de)
    - Address (193.99.144.85)
  - **Traceroute (TR)**
    - Domain
    - Address



Internet Availability System (IVS) → Concept (2/3)

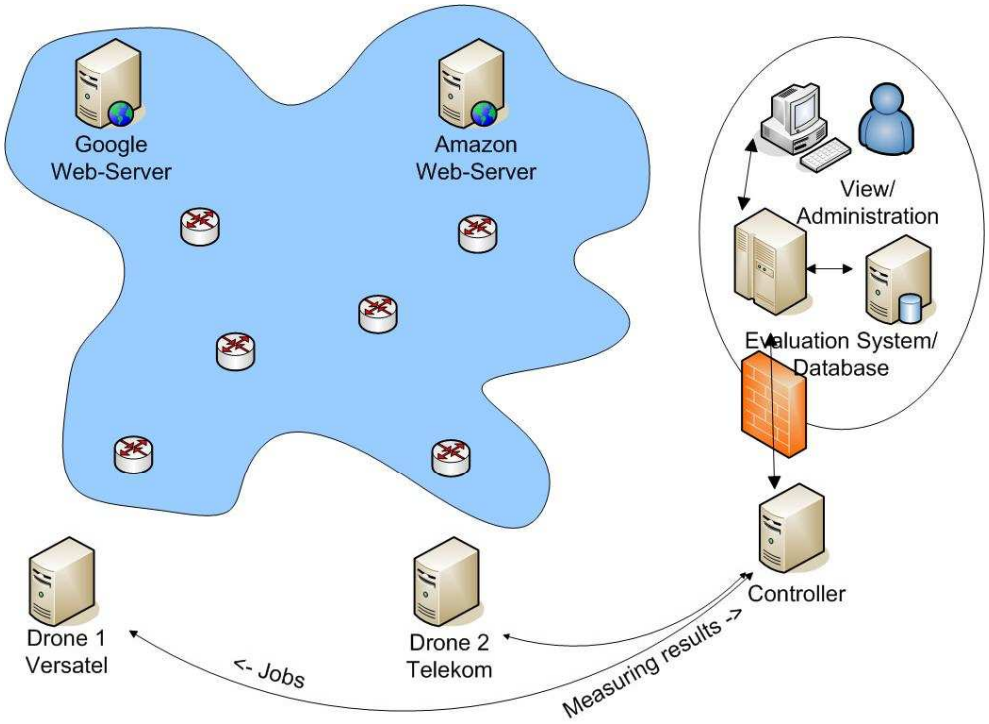
- **Drone**
  - The Drone is a measurement device and has modules (HTTP,TR)
  - Placed at Internet connections by various Internet Service Providers
  - Measures at a given interval
  - Communication only initialized by drone (no adaptation to firewall/NAT necessary)
    - Drone pulls jobs from controller
    - Sends results to controller



- **Controller**
  - Is the intermediate of the drone and the evaluation System
  - Placed at the DMZ of the operator of IVS

Internet Availability System (IVS)
→ Concept (3/3)

- **Evaluation System / Database**
  - Communicates with controller and administrator
  - Prepares data to be displayed by the view
  - Persistent storage of measuring results and of additional management data



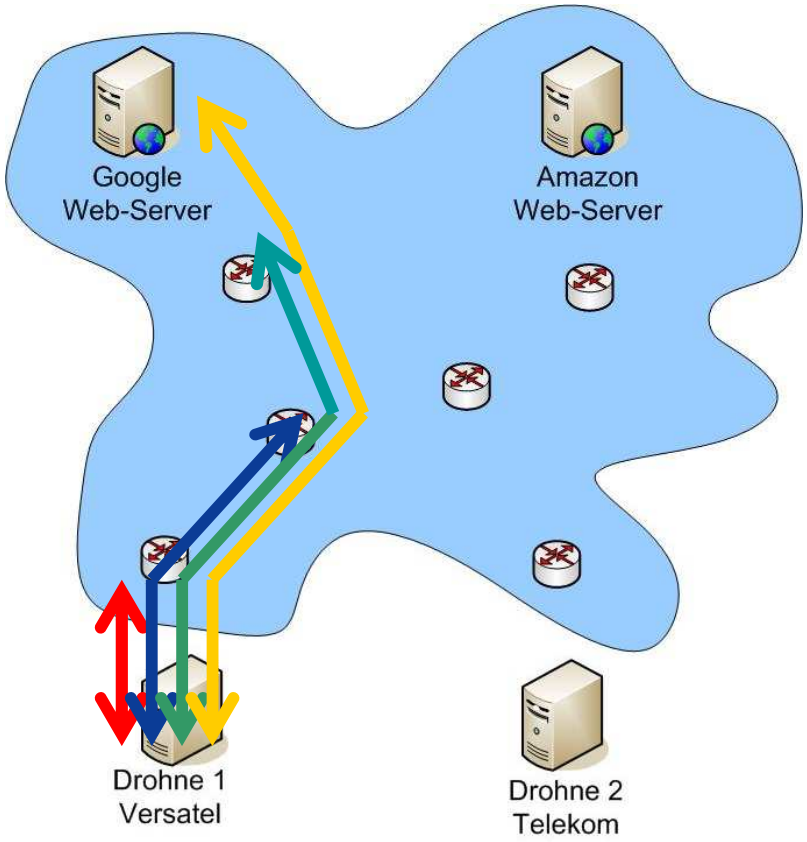
- **View / Administration**
  - Over a GUI the user can administrate jobs for specific drones
  - Drawing graphs and evaluation of the statistical results for a defined period
  - Indicates the current status of the drones, server and jobs

Content

- Aim and outcomes of this lecture
- Idea/Concept of the Internet Availability System
- **Routing**
- Implementation
- Results
- Summary

Internet Availability System (IVS)
→ How does traceroute work?

- The time-to-live field (TTL) of an IP packet is initialized by the original sender starting with the value “one”, which will allow only the packet to reach the first active hardware component (router).
- Each intermediate router (active component) decrements the value by one.
- If the field is decremented to zero, the packet is discarded and an error indication packet (ICMP “time exceeded”) is sent back to the original sender.
- The TTL value is incremented with each TR packet extending the range of the route.
- The source address of the ICMP “time exceeded” identifies the router that discarded the data packet.



- So, if packets are sent to the final destination, but with the ttl set to n, the router n hops along the path is forced to identify itself.
- TR can be implemented with TCP/UDP or ICMP

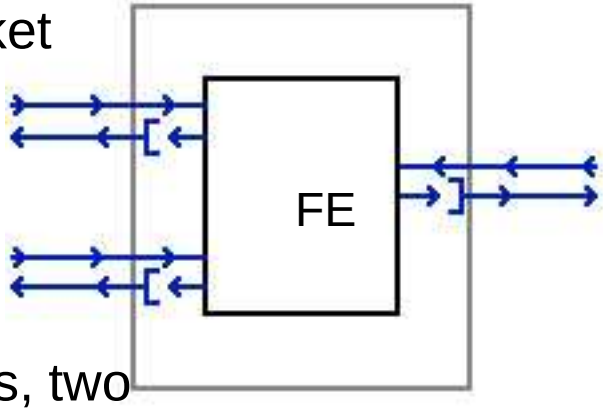
Internet Availability System (IVS)
→ Traceroute

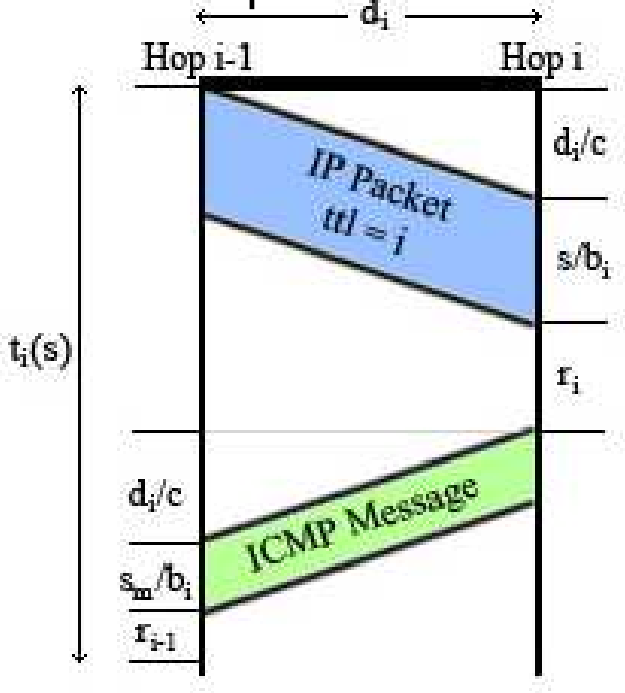
Traceroute

```
vmsuse80:/ # traceroute www.heise.de
traceroute to www.heise.de (193.99.144.71), 30 hops max, 40 byte packets
 1  gw502_48.informatik.fh-ge.de (172.16.48.2)  1 ms  1 ms  1 ms
 2  fb5gwint.informatik.fh-ge.de (172.16.0.5)  1 ms  1 ms  1 ms
 3  172.16.16.3 (172.16.16.3)  2 ms  2 ms  2 ms
 4  fb5gw.informatik.fh-gelsenkirchen.de (194.94.127.2)  3 ms  3 ms  3 ms
 5  193.175.172.2 (193.175.172.2)  3 ms  3 ms  3 ms
 6  ar-essen2.g-win.dfn.de (188.1.44.33)  6 ms  5 ms  5 ms
 7  cr-essen1-ge0-0.g-win.dfn.de (188.1.86.1)  5 ms  5 ms  5 ms
 8  cr-frankfurt1-po8-1.g-win.dfn.de (188.1.18.89)  16 ms  16 ms  16 ms
 9  ir-frankfurt2-po3-0.g-win.dfn.de (188.1.80.38)  15 ms  15 ms  15 ms
10  de-cix2.ffm.plusline.net (80.81.193.132)  16 ms  16 ms  15 ms
11  c22.f.de.plusline.net (213.83.57.53)  16 ms  16 ms  16 ms
12  www.heise.de (193.99.144.71)  16 ms  16 ms  17 ms
vmsuse80:/ #
```

Internet Availability System (IVS)
→ Round Trip Time (RTT)

- The time period between transmitting the TR IP packet and receiving the ICMP reply message is called Round Trip Time (RTT)
- A router contains links, queues and a forwarding engine (FE).
- Each time the TTL is increased by one, two new links, two new queues and one new forwarding engine are measured





- The RTT depends on the **distance d**, the **size of the packets s**, the **bandwidth b** and the **forwarding-** and **queue-time r** of the router
- **Forwarding time for hop n:**

$$T(n,s)=\sum_{i=1}^{n}\left[\frac{s}{b_i}+\frac{d_i}{c}+r_i\right]$$

$c = 3 \cdot 10^8$ m/s
(the speed of light)

- **RTT between two hops:**

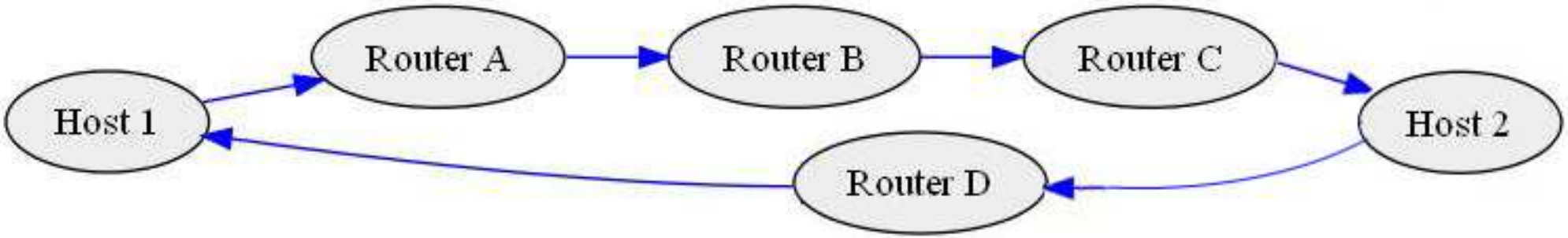
$$t_i(s)=\frac{s}{b_i}+r_i+\frac{s_m}{b_i}+r_{i-1}+\frac{2*d_i}{c}$$

Internet Availability System (IVS)
→ Asynchronous routing

- While the **forwarding time f** of each router is nearly the same the **queue time q** is **not predictable** (**r** = **q** + **f**)
- The **minimum RTT** to each router over time helps to get the time between two hosts by minimum influence of queue time

$$t_i(s) \approx \frac{s + s_m}{b_i} + 2\left[\frac{d_i}{c} + fi\right] \qquad if\ (f_{(i-1)} \approx f_i) \wedge (q_i \to 0)$$

- Normally, the routing is synchronous and the forwarding time of a packet is half of the Round Trip Time (RTT)
- But it is possible that the routing is asynchronous!

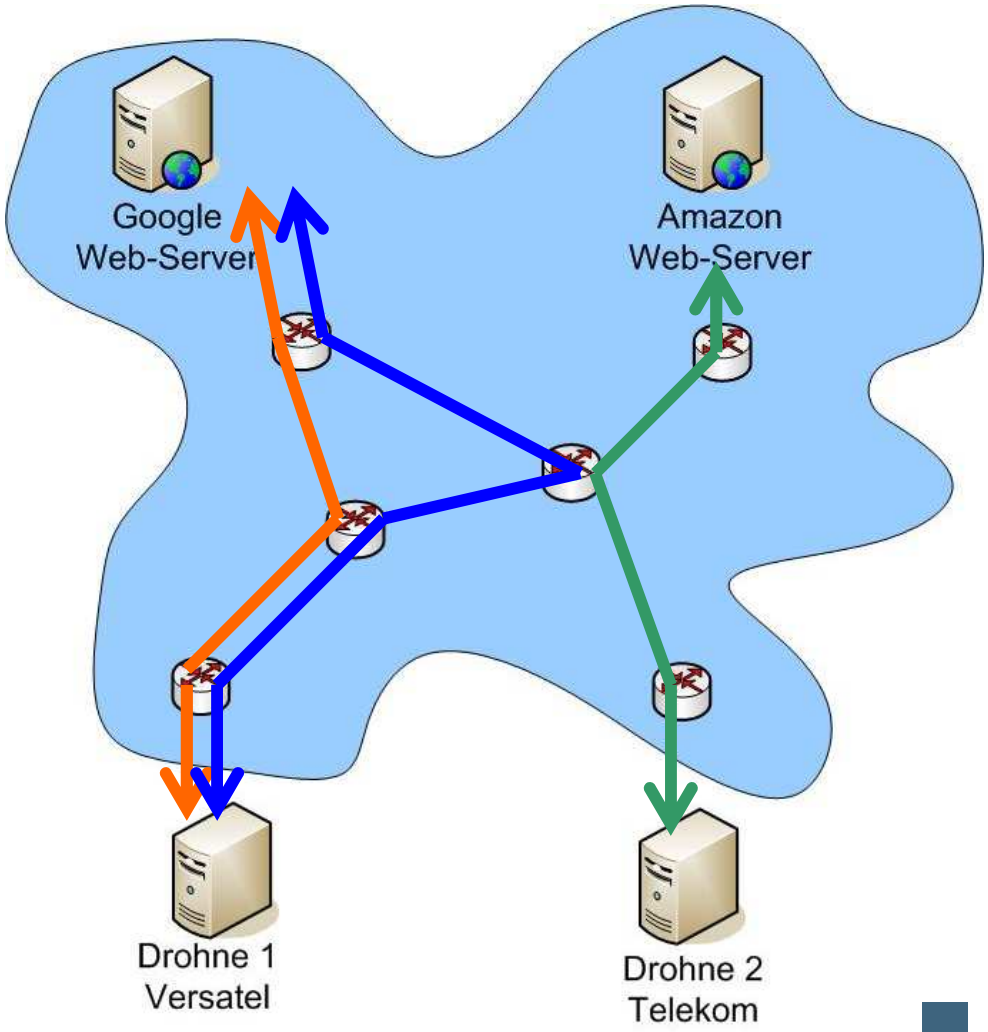


- Latency period (measured only in one direction) with complex time sync of both hosts could help

Internet Availability System (IVS)
→ Routing

- The path of a route is changing over time

- **Cause of changing:**
  - Drop out of a router
  - High utilization of a router
  - Network management of network carrier
    - Commercial interests
    - Cost interests
  - …



Content

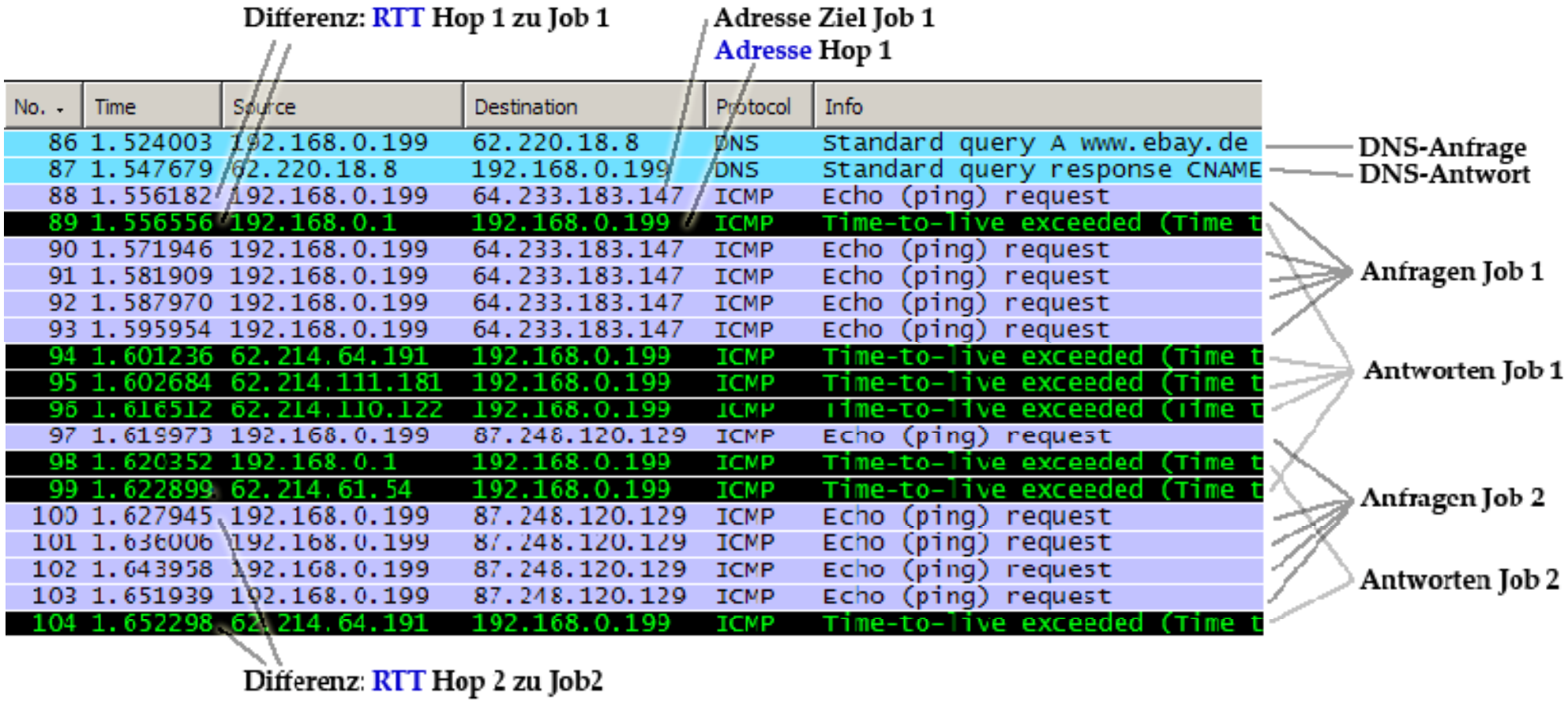
- Aim and outcomes of this lecture
- Idea/Concept of the Internet Availability System
- Routing
- **Implementation**
- Results
- Summary

Internet Availability System (IVS)
→ Measured values

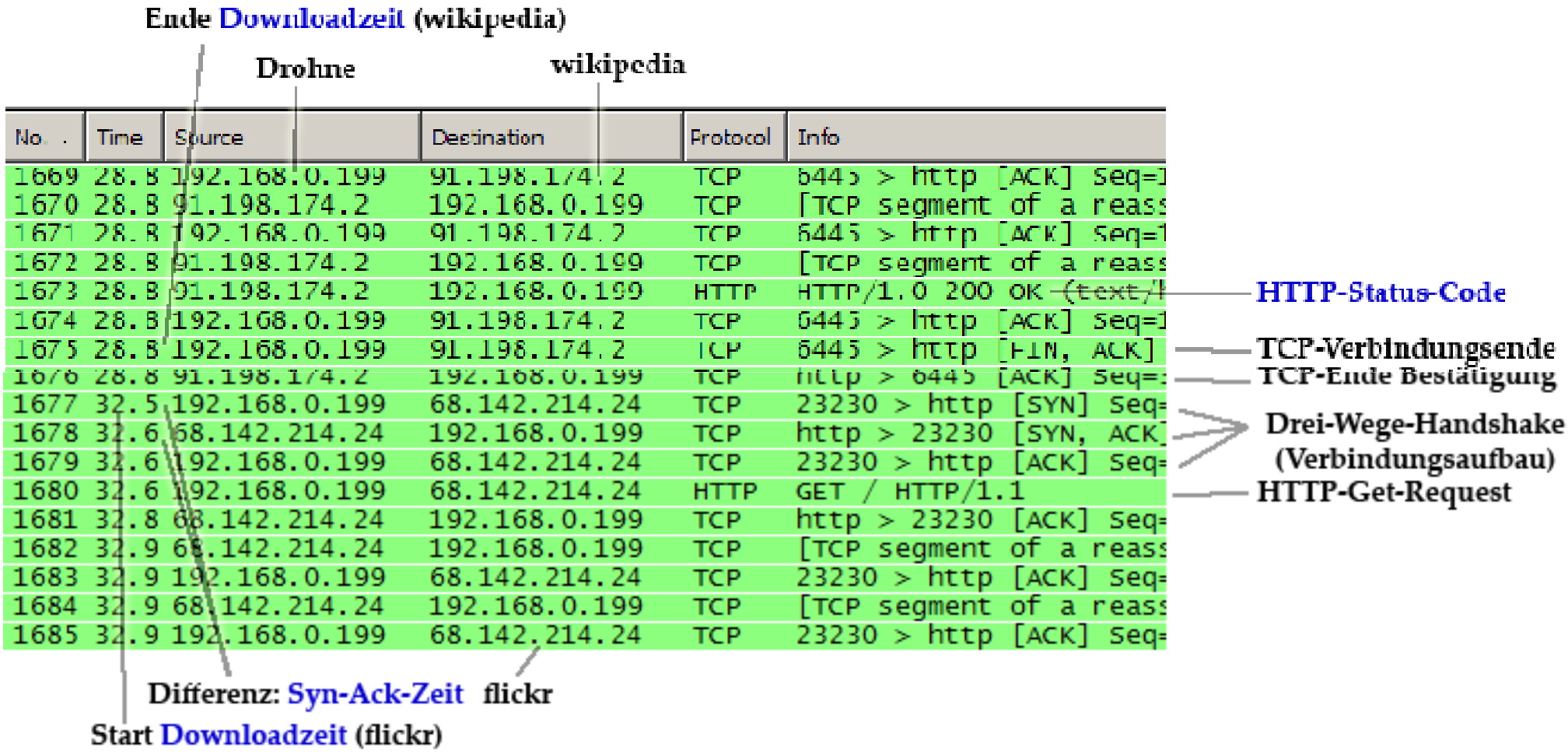
- **Traceroute**
  - RTT (min, max, avg, mdev)
    - Variable amount of IP packets can be sent (standard:3 per Hop)
  - IP, Hop-No.

- **HTTP**
  - ***Window-Size=0*** (remote station is overloaded at moment)
  - ***Downloaded bytes,*** download time => bandwidth
  - ***Packets lost,*** packets send => Packet Loss Rate
  - ***Syn-Ack Time*** (3 way handshake)
  - TSval, TSecr (Timestamp of Server/Host – TCP-Option)
    - Not transmitted by most (safety risk)
  - ***HTTP-Status-Code***

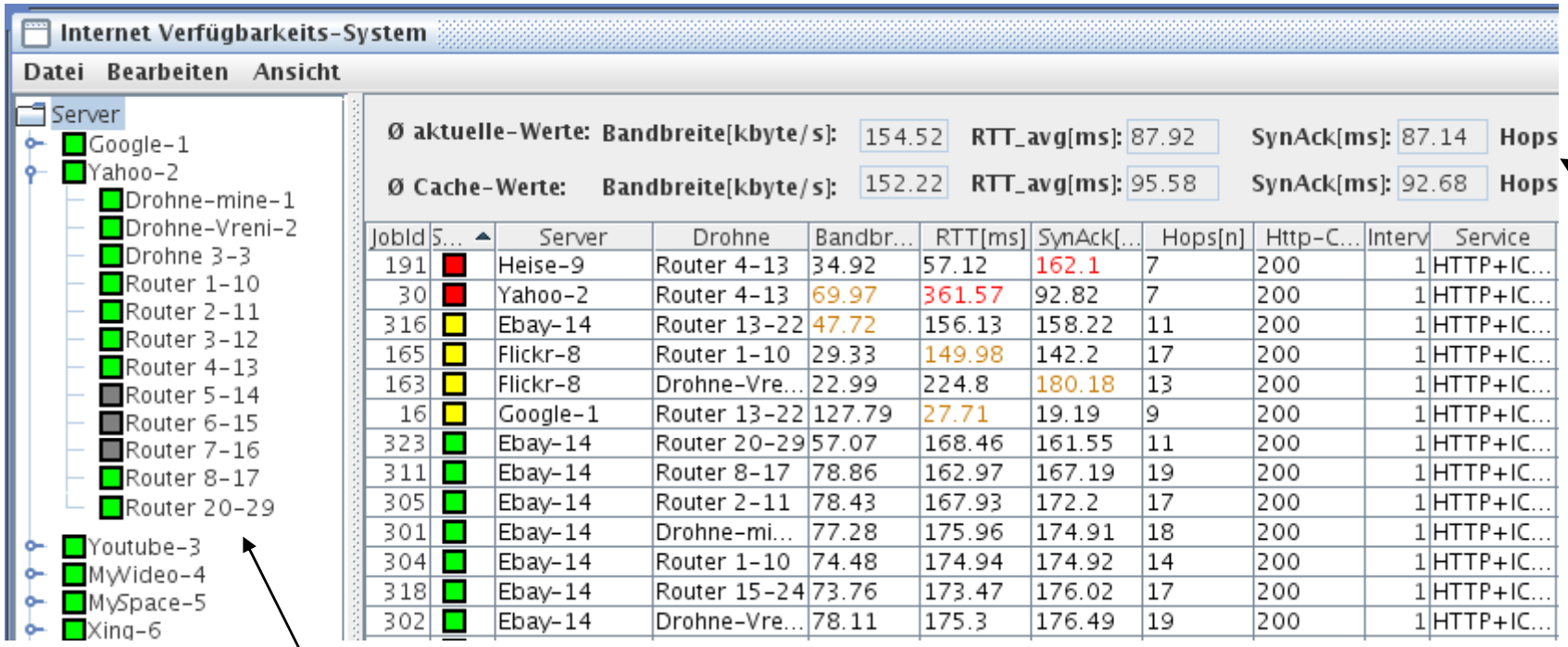
Internet Availability System (IVS)
→ Traceroute Modul



Internet Availability System (IVS)
→ HTTP Modul



Internet Availability System (IVS)
→ View/Administration(1/3)



- A Job is a request for a drone to measure one server/service
- Each single job has a status – the status of the server and drones are deduced from their jobs status

Internet Availability System (IVS)
→ View/Administration(2/3)

JobId	S...	Server	Drohne	Bandbr...	RTT[ms]	SynAck[ms]	Hops[n]	Http-Code	Interv	Service
108		MySpace-5	Router 13-22	68.76	201.46	177.47	18	200	1	HTTP+ICMP
302		Ebay-14	Drohne-Vreni-2	78.11	250.78	176.49	16	200	1	HTTP+ICMP
303		Ebay-14	Drohne 3-3	81.59	177.96	170.07	16	200	1	HTTP+ICMP

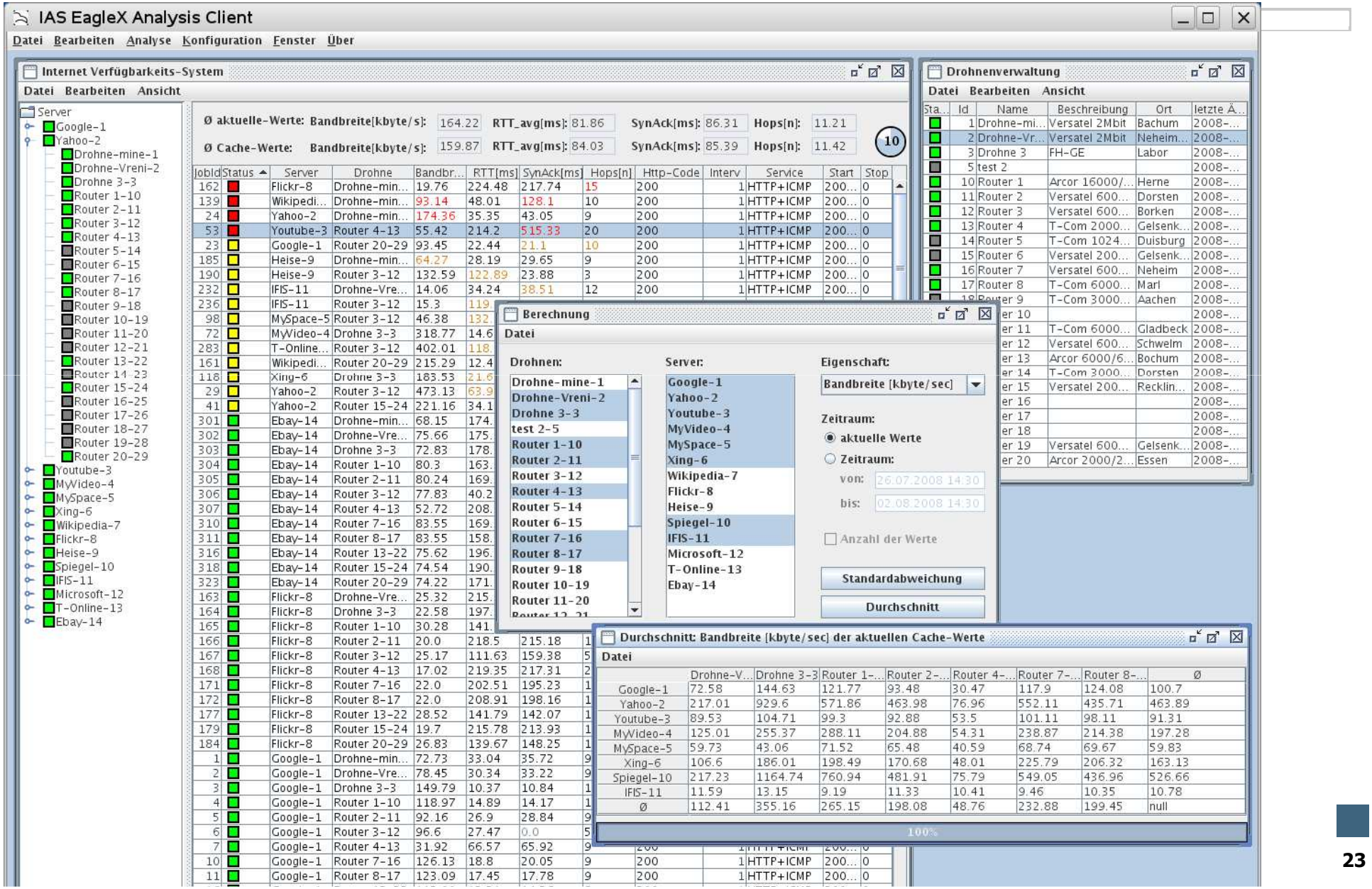
- Each job's status is calculated by the measured values: bandwidth, RTT, SynAck, Hops and HTTP-Code
- If one value deviate to the 2*Mdev the status turns to warning, if the deviation is over 4*Mdev the status turns to alarm/alert
- The average deviation is calculated by the last 60 values (by interval of 1 min => 60 min)
- If half of the jobs of a server/drone has the status warning/alarm → server/drone obtains the same status

- Status can only be calculated if the drone sends its results continuously.
- If a drone doesn't send within 2*interval the status is set inactive

Internet Availability System (IVS)
→ View/Administration(3/3)

- The Global View implies in this context to two average values:
  - the average over all current values of one type like the average bandwidth, RTT, etc. (top row)
  - which can be compared to the average of the last 60 of these values at the bottom row of the figure.
- These values are specific for the Internet connections and servers which are measured
- The values indicate the complete view of all drones and servers and the route to them

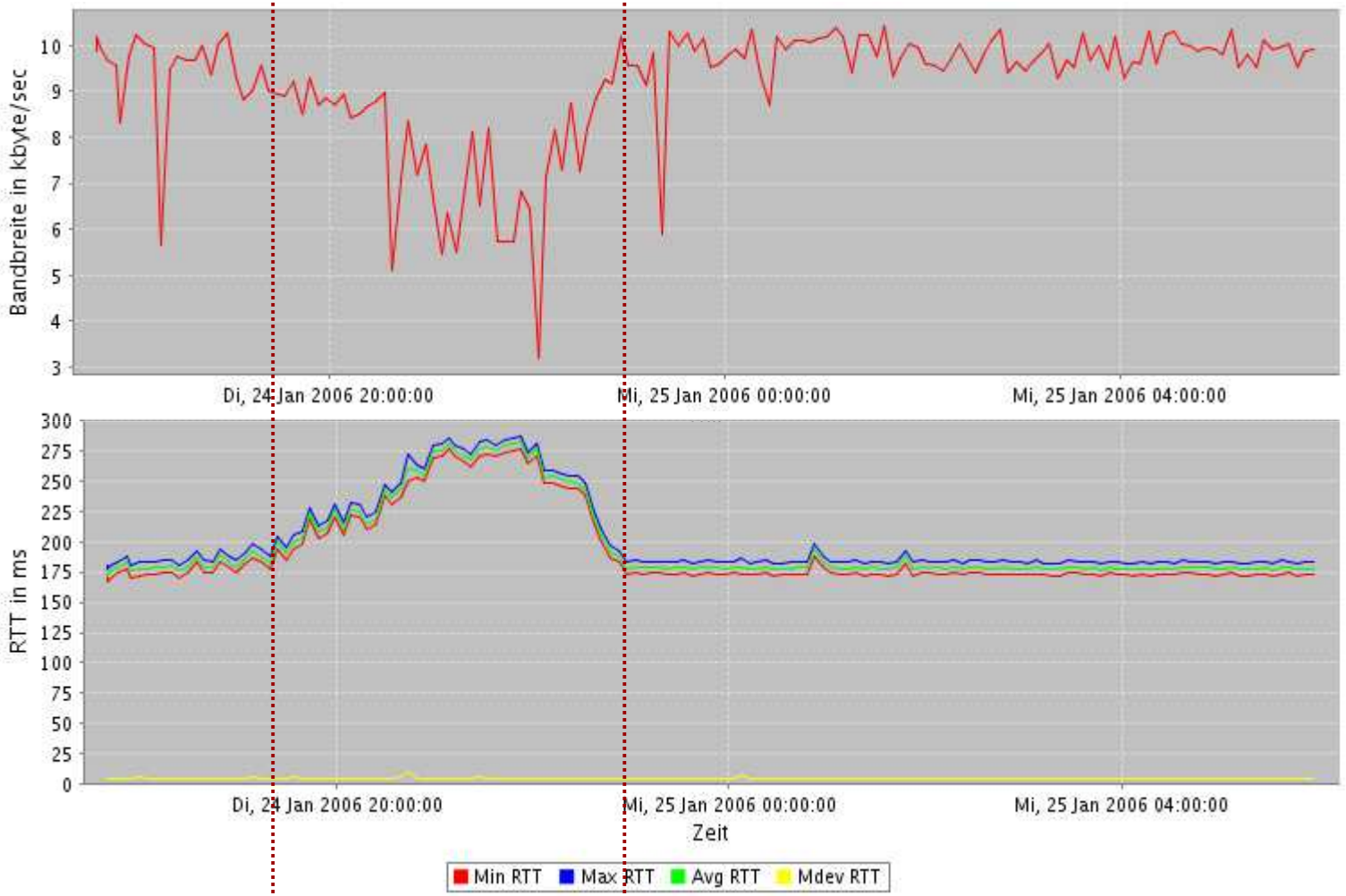
Internet Availability System (IVS)
→ Overview



Content

- Aim and outcomes of this lecture
- Idea/Concept of the Internet Availability System
- Routing
- Implementation
- **Results**
- Summary

IVS : Current State of Development
→ Bandwidth/RTT



rapidshare.de

File Sharing Portal

The most traffic and the lowest throughput occur between 6pm and 11pm

Computer Science Department

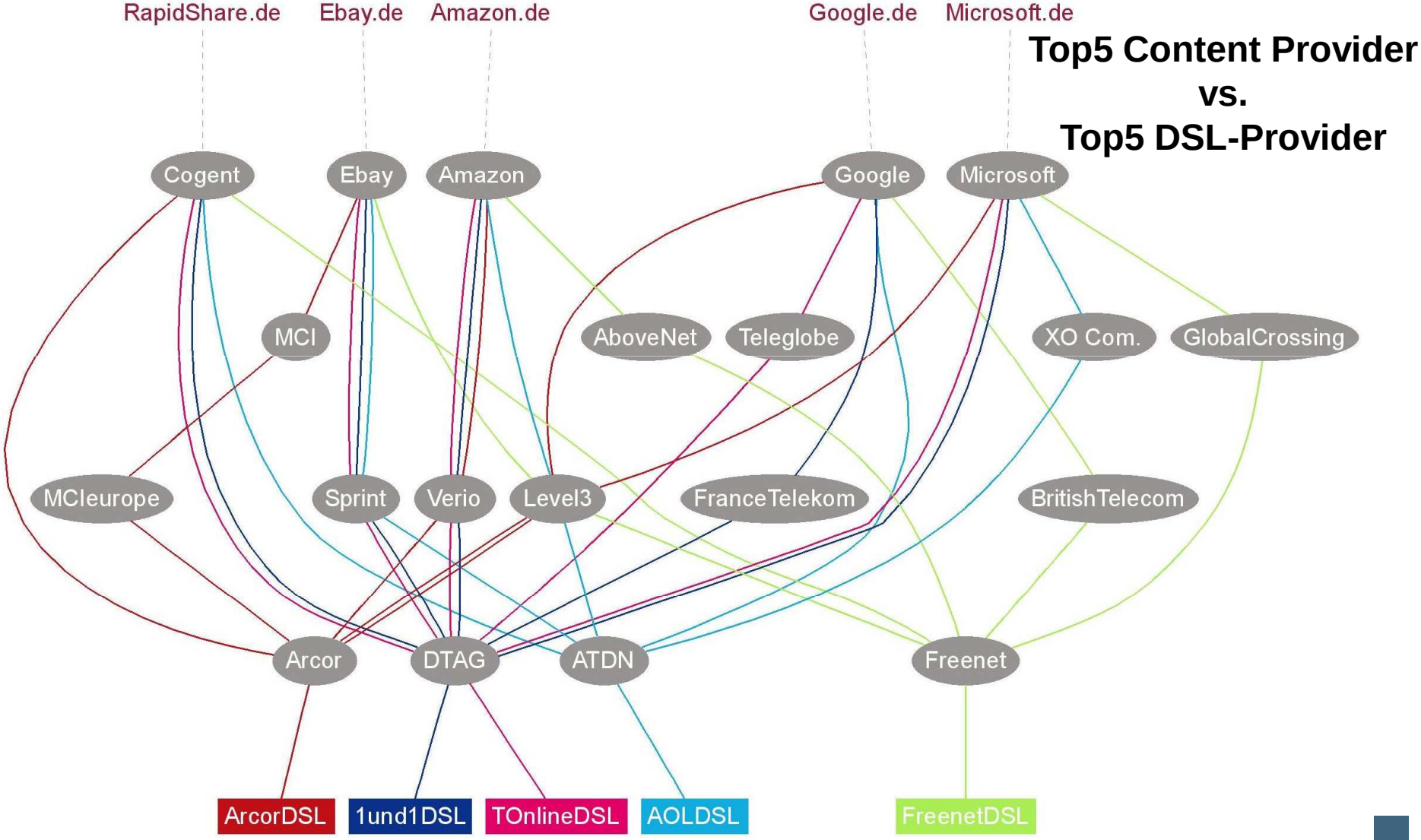
IVS : Current State of Development
→ Bandwidth/Hops

t-online.net

Information Portal

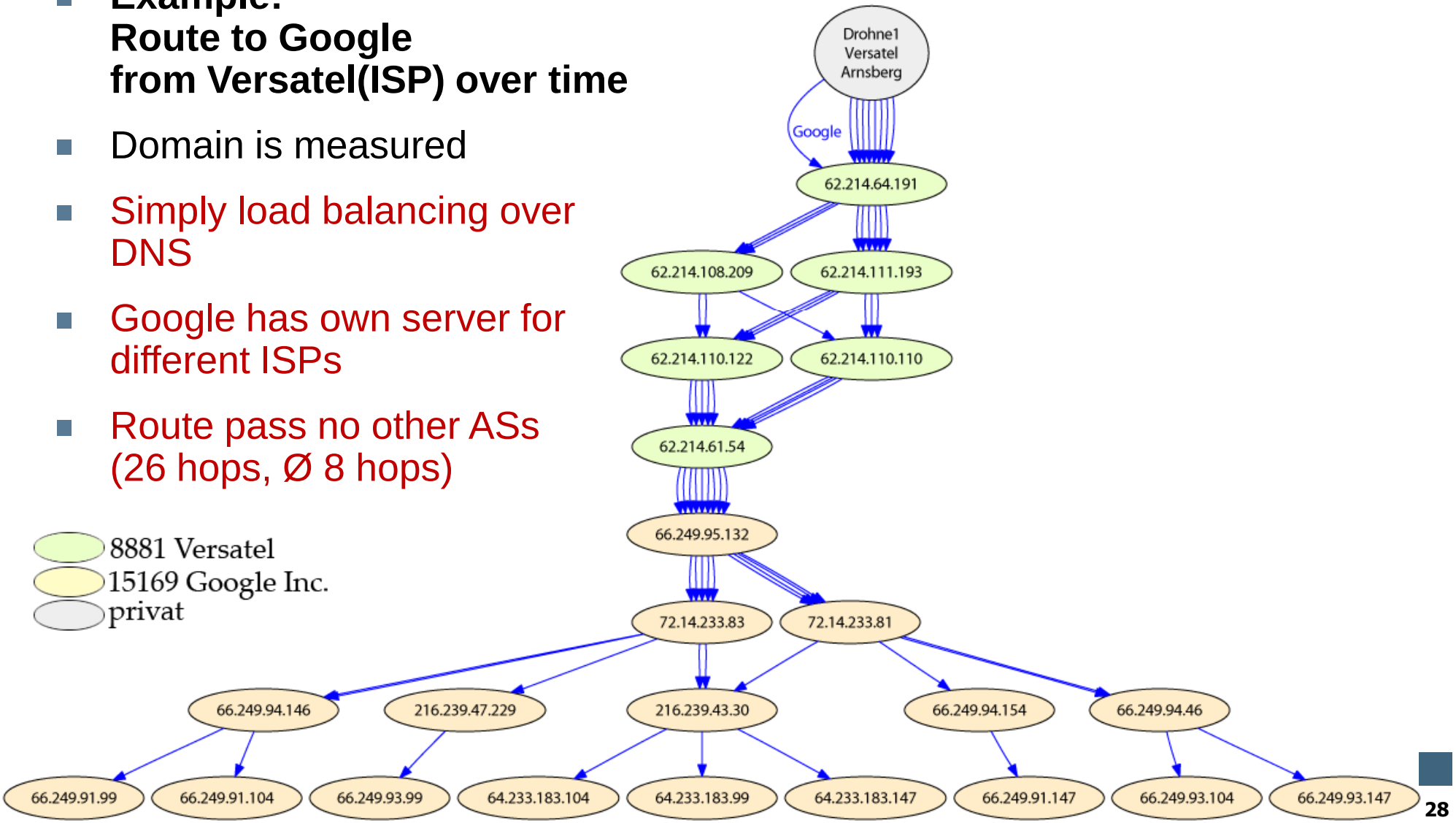
Different routings have an influence on the bandwidth

IVS : Outline of the Internet
→ Idea



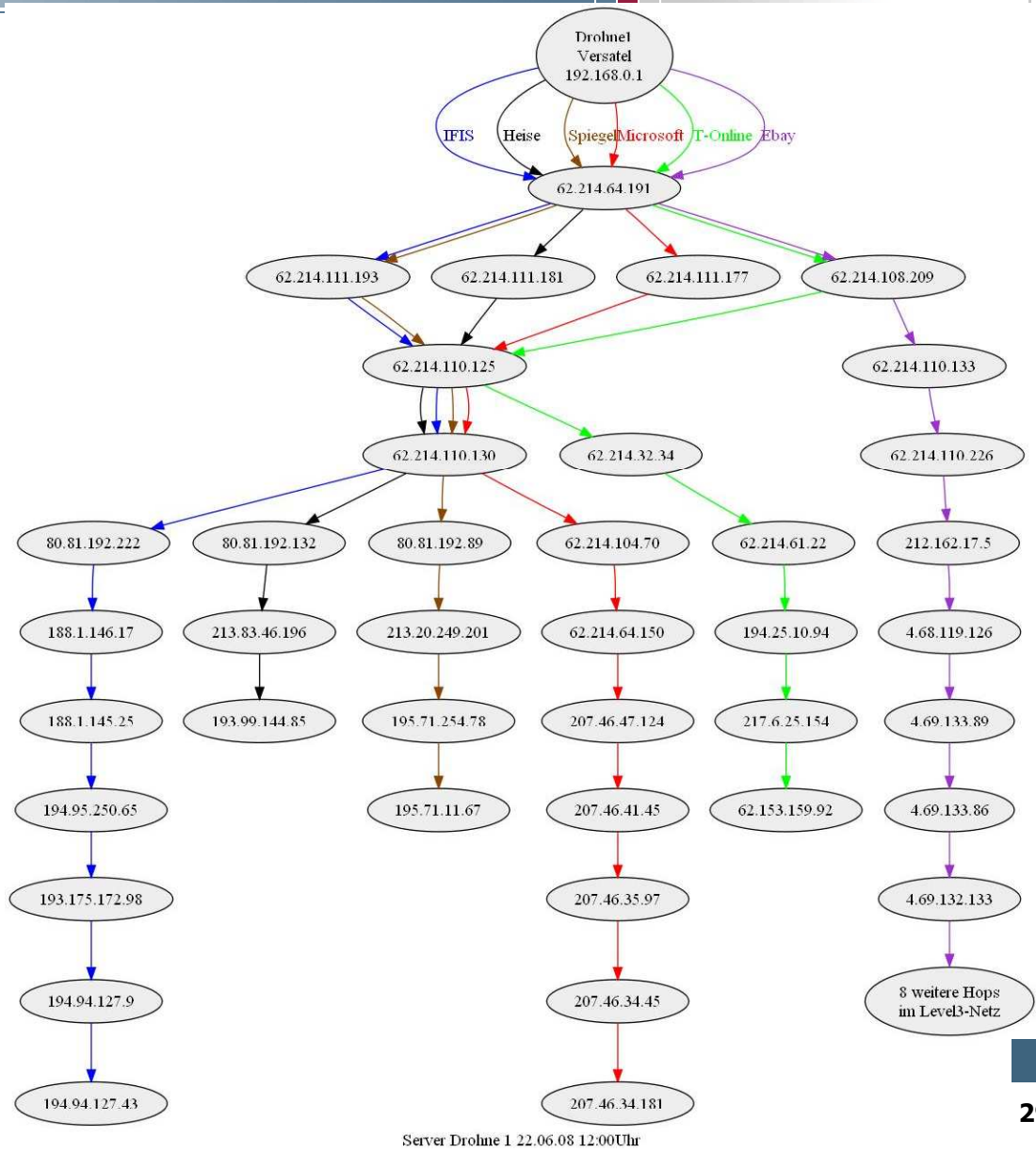
IVS : Outline of the Internet
→ Measurement readings (1/4)

- **Example:**
  Route to Google
  from Versatel(ISP) over time
- Domain is measured
- Simply load balancing over DNS
- Google has own server for different ISPs
- Route pass no other ASs (26 hops, Ø 8 hops)



IVS : Outline of the Internet
→ Measurement readings (3/4)

- **Example:**
  Route from a Versatel-Drone to different web server at point of time (few sec)
- Different ways after first AS (Versatel 62.214.x.x)
- High workload of a router (many packets in queue) not in Versatel-net affects only a single service not the entire connection

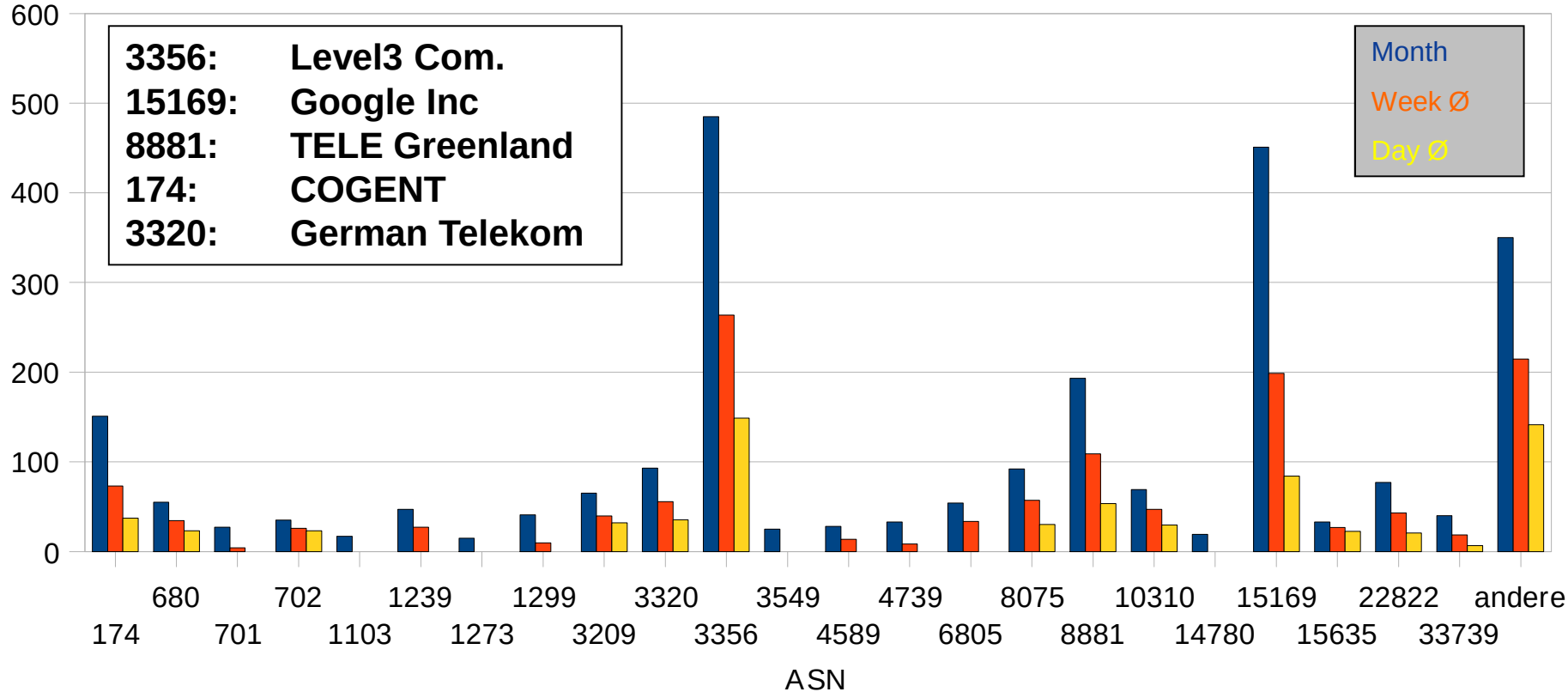


IVS : Outline of the Internet
→ Measurement readings (2/4)

- **Example:** Route to Spiegel, Wikipedia, if(is), Heise from different Versatel access at point of time
- **DE-CIX:** Germans largest Internet-Exchange-Point and second worldwide

Internet Availability System (IVS)
→ Different Router/Autonomous Systems

- Number of different routers and ASs (12 drones to 14 domains (35 servers))
  - Month (June 2008): **2495 routers** in **188 ASs**
  - Week (3. in June 2008): **1277 routers** in **122 ASs**
  - Day (2008.06.03): **699 routers** in **54 ASs**
- Hops of a route: **avg:11.76 Hops**, min: 4 Hops if(is), max: 21 Hops MySpace



Internet Availability System (IVS)
→ Calculation

- Statements to quality/speed of connections and servers
- The example below shows the average bandwidth of 6 drones to 14 servers over the period of one week
- Interval is 1 min - the average is composed of about 1.080 values
- Last row/column is the average of the entire column/row

Durchschnitt: Bandbreite [kbyte/sec] von: 02.06.2008 00:00 bis: 09.06.2008 00:00

Datei

	Drohne-mi...	Drohne-Vr...	Drohne 3-3	Router 2-11	Router 3-12	Router 4-13	Ø
Google-1	71.63	77.95	141.41	96.03	87.78	34.55	84.89
Yahoo-2	199.16	200.91	533.16	341.8	334.78	84.74	282.43
Youtube-3	74.92	75.77	83.67	79.74	75.11	52.06	73.55
MyVideo-4	122.54	122.18	245.34	198.12	201.99	59.49	158.28
MySpace-5	64.84	67.61	55.62	66.73	67.41	50.06	62.05
Xing-6	98.15	105.76	161.86	126.47	119.51	46.97	109.79
Wikipedia-7	125.44	129.48	330.84	170.72	164.78	68.17	164.91
Flickr-8	23.24	23.72	28.45	25.0	25.09	17.48	23.83
Heise-9	108.25	109.99	164.04	140.98	137.72	41.26	117.04
Spiegel-10	211.28	209.88	1149.48	472.84	444.95	81.82	428.38
IFIS-11	13.72	11.43	15.02	13.95	13.6	11.77	13.25
T-Online-13	203.99	209.42	512.0	371.58	346.5	81.01	287.42
Ebay-14	70.66	73.22	77.65	73.82	73.29	49.61	69.71
Ø	106.76	109.02	269.12	167.52	160.96	52.23	null

100%

Internet Availability System (IVS)
→ Evaluation

- **Top X: web server**
- Quite stable, change of the values over the period of several weeks <= 5%

Domain	average [kB/s]	mdev [kB/s]	Mdev [%]	Data size [kB]
Spiegel	373,58	5,27	1,41	154,8
T-Online	286,96	6,4	2,23	94,44
Yahoo	283,04	6,41	2,27	126,3
Wikipedia	177,4	3,54	2	36,17
MyVideo	158,56	7,96	5,02	56,39
Xing	119,16	3,06	2,57	18
Heise	118,82	3,28	2,76	51,54
Google	88,83	2,98	3,35	7,3
Youtube	77,53	2,4	3,09	72
Ebay	70,03	0,73	1,04	67,56
MySpace	62,58	2,74	4,38	63,94
Flickr	23,84	0,39	1,65	9,9
IFIS	13,19	0,17	1,27	23,8

Internet Availability System (IVS)
→ Evaluation

- **Top Y: Internet accesses**

Drohne	ISP	down [Mbit]	average [kB/s]	mdev [kB/s]	mdev [%]
Drohne 3	DFN	100	254,55	2,56	1
Router 13	Arcor	6	195,15	6,07	3,11
Router 7	Versatel	6	191,44	1,67	0,87
Router 8	Telekom	6	172,54	8,22	4,77
Router 2	Versatel	6	157,46	1,56	0,99
Router 3	Versatel	6	149,81	1,86	1,24
Router 11	Telekom	6	111,98	2,73	2,44
Drohne-Vreni	Versatel	2	103,68	1,9	1,83
Router 15	Versatel	2	103,53	1,16	1,12
Drohne-mine	Versatel	2	101,13	1,55	1,54
Router 5	Telekom	1	58,8	1,18	2,01
Router 4	Telekom	2	49,86	1,19	2,38

Content

- Aim and outcomes of this lecture
- Idea/Concept of the Internet Availability System
- Routing
- Implementation
- Results
- **Summary**

Internet Availability System (IVS)
→ Summary

- **The IVS has drones which measure the availability of servers/services!**
- Drones should be placed at various ISP to measure routes spreading through AS of different providers
- Routing can be asynchronous -> RTT is depending on routing
- The RTT is mainly depending on the queue time which can not easily be predicted
- Routing changes over time (multiples causes like DNS)
- The measured speed of different Internet connections differs although the routes have the same bandwidth
  - Due to small files and TCP mechanisms

Fachhochschule Gelsenkirchen

Internet Availability System
→ Idea and Realization

Thank you for your attention!
Questions?

Prof. Dr. (TU NN)
Norbert Pohlmann

Institute for Internet Security - if(is)
University of Applied Sciences Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet security.

Internet Availability System (IVS)
→ Literature

- [1] T. Ostermann, N. Pohlmann: „Internet-Verfügbarkeitssystem – Welche Qualität hat das Internet?", IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 2/2006
- [2] Thomas Ostermann: Internet-Verfügbarkeitssystem (internet availability system), Diploma Thesis, University of Applied Sciences Gelsenkirchen, 2006
- [3] Kilian Himmelsbach: Konzeption und Umsetzung einer modularen Architektur für das Internet-Verfügbarkeits-System (design and implementation of a modular architecture for the IVS), Diploma Thesis, University of Applied Sciences, Gelsenkirchen, 2008

Links:

Institute for Internet Security:
http://www.internet-sicherheit.de/forschung/aktuelle-projekte/internet-frhwarnsysteme/internet-verfgbarkeits-system/