

Internet-Analyse-System

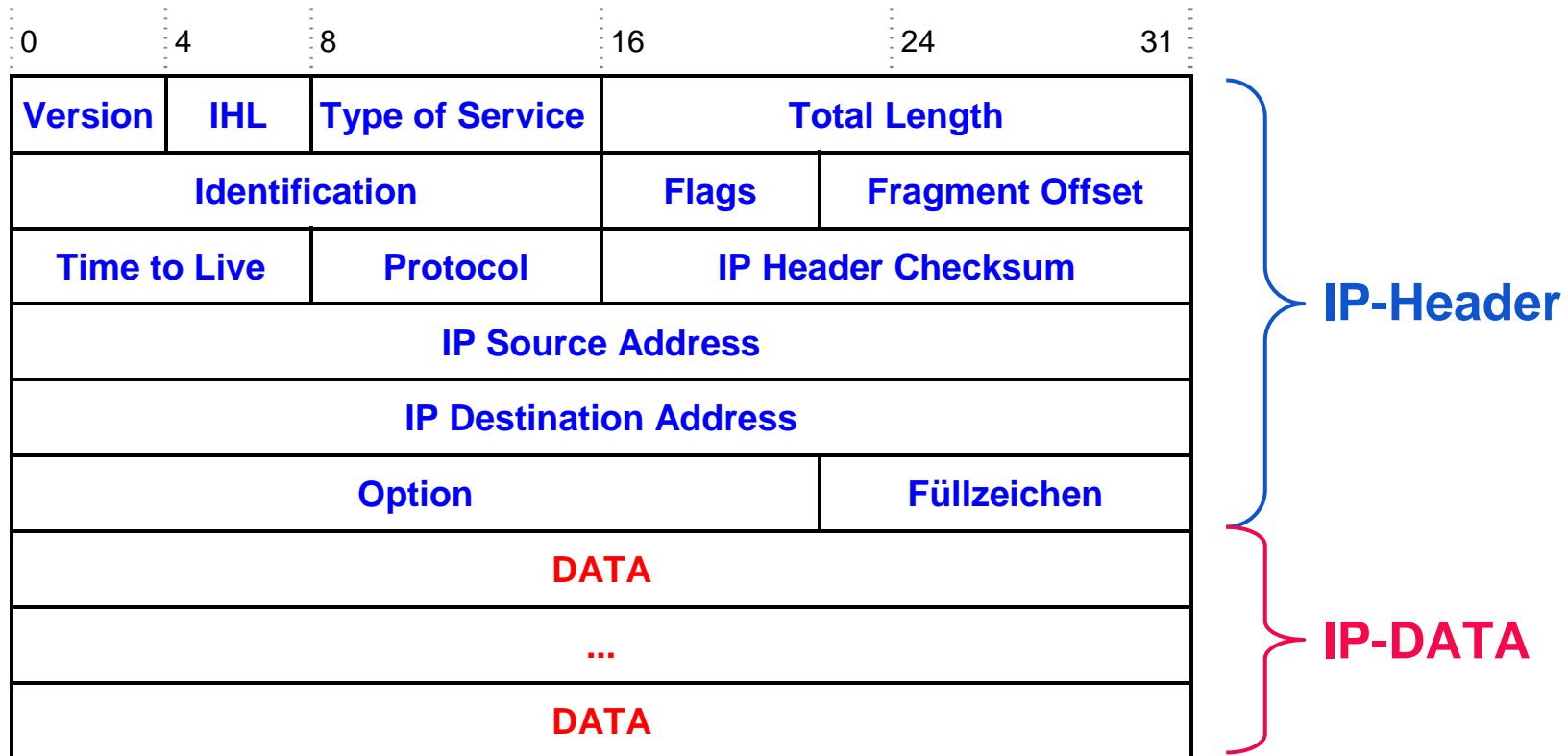
→ Beispiele

Prof. Dr. Norbert Pohlmann

Fachbereich Informatik

Verteilte Systeme und Informationssicherheit

IP-Paket, IP-Datagramm



Feldelemente des IP-Headers (1/8)

0	4	8	16	24	31
Version	IHL	Type of Service	Total Length		
Identification			Flags	Fragment Offset	
Time to Live	Protocol		IP Header Checksum		
IP Source Address					
IP Destination Address					
Option				Füllzeichen	

■ Version (Vers)

- Feldlänge: 4 Bit

■ Beschreibung

- Das Versions-Feld gibt die verwendete Version des IP-Protokolls an.
- In der Regel wird heute noch die **Version 4** verwendet, die Standardisierung der Version 6 ist jedoch abgeschlossen. (Codierung Version 4 = 4)

■ Internet Header Length (IHL)

- Feldlänge: 4 Bit, Einheiten: 4 Octet-Gruppen, Bereich: 5-15 (Standard: 5)

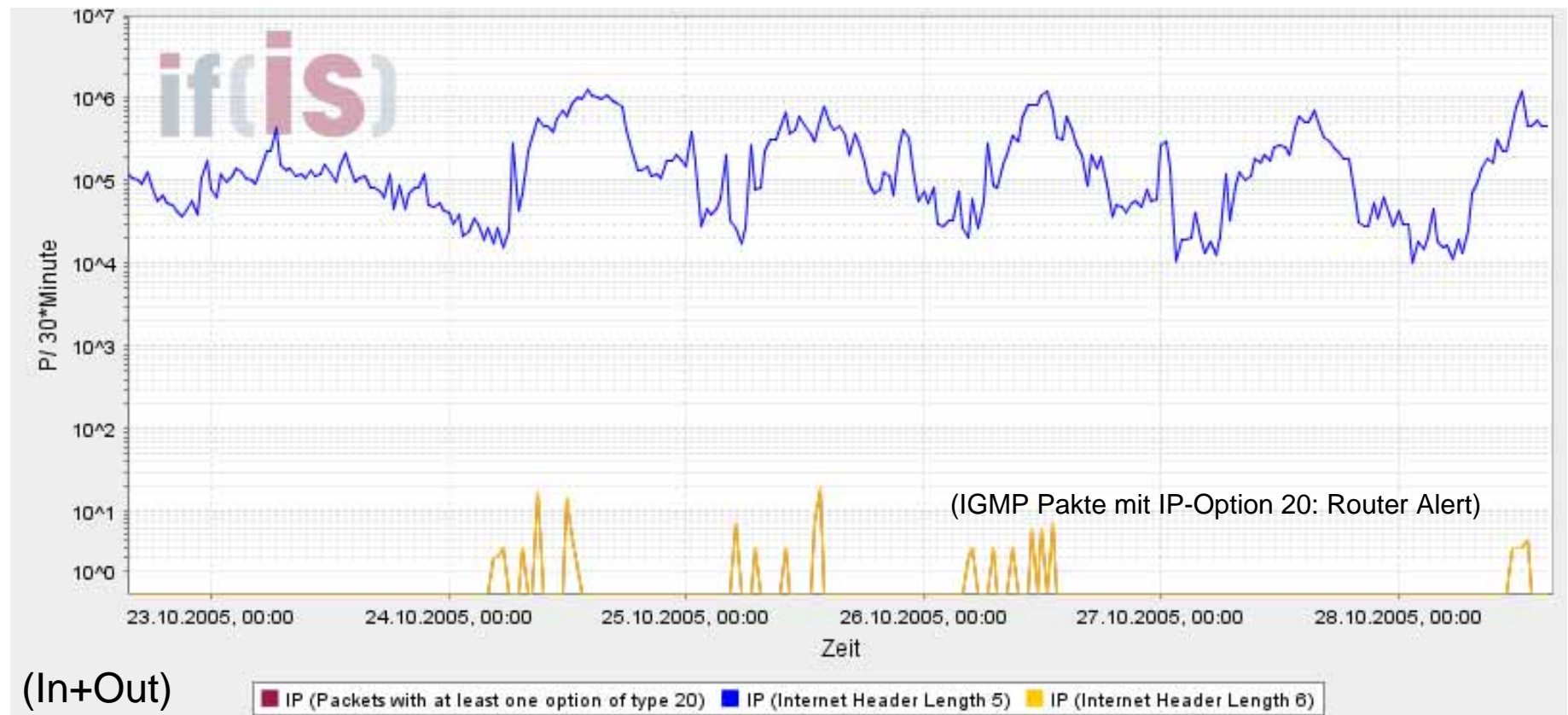
■ Beschreibung

- Die Internet Header Length steht für die gesamte Länge des IP-Headers, ausgedrückt in 32-Bit-Einheiten (4 Octets).
- Das IHL Length-Feld ist durch die variable Länge des Optionen-Feldes im IP-Header erforderlich, der am häufigsten verwendete Header hat die Länge von 20 Byte, das IHL-Feld enthält dann also den **Wert 5** (Mindestwert).

Internet-Analyse-System: FB Informatik

→ Internet Header Length (IHL)

- Nur Länge 5 und 6 vorhanden



Feldelemente des IP-Headers (2/8)

■ Type of Service (TOS)

- Feldlänge: 8 Bit

■ Beschreibung

- Dieses Feld gibt die gewünschte **Qualität des Dienstes** (Vorrang, Verzögerung, Durchsatz und Zuverlässigkeit) für dieses Datagramm an.
- Wird auch als Differentiated Service Code Point (DSCP) bezeichnet, siehe z.B. Differentiated Services (DiffServ) – REN2-Vorlesung: Quality of service
- Die angesprochenen Netzknoten können entweder den gewünschten Dienst erbringen oder leisten diesen Dienst oder Teile davon nicht.

■ Total Length (TL)

- Feldlänge: 16 Bit, minimaler Wert: 20

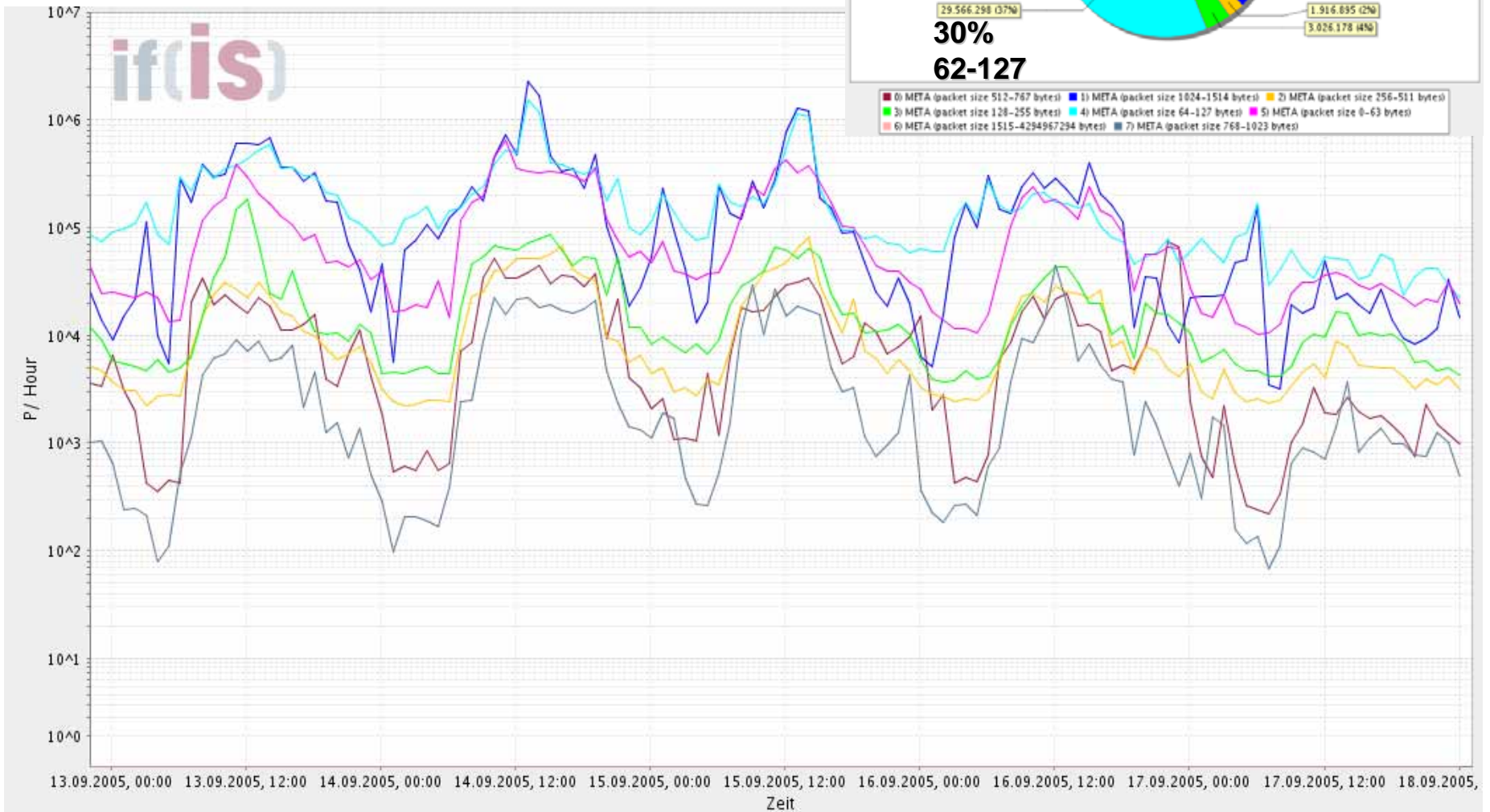
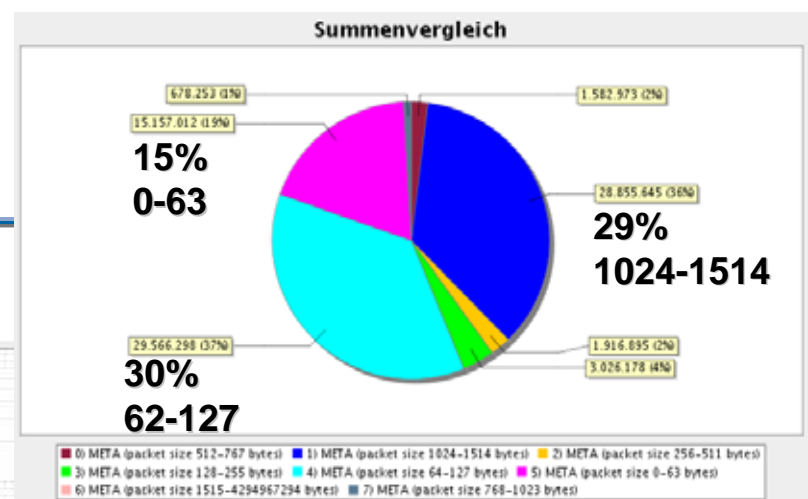
■ Beschreibung

- Dieses Feld gibt die Länge des Datagramms (sowohl **Kopf als auch Benutzerdaten**), gemessen in Octets an.
- Da dieses Feld 16 Bit lang ist, kann ein IP-Paket inklusive Header maximal 2^{16} oder 65.535 Octets lang sein.

0	4	8	16	24	31
Version	IHL	Type of Service	Total Length		
Identification			Flags	Fragment Offset	
Time to Live	Protocol		IP Header Checksum		
IP Source Address					
IP Destination Address					
Option				Füllzeichen	

IAS: FB Informatik

→ Total Length (TL)



Feldelemente des IP-Headers (3/8)

0	4	8	16	24	31
Version	IHL	Type of Service	Total Length		
Identification			Flags	Fragment Offset	
Time to Live		Protocol	IP Header Checksum		
IP Source Address					
IP Destination Address					
Option				Füllzeichen	

■ Identification (ID)

- Feldlänge: 16 Bit

■ Beschreibung

- Dieses Feld enthält eine eindeutige Identifikation des IP-Paketes, z.B. einen **Zähler**, der durch den absendenden Host vergeben wird.
- Dieses Feld wird bei der Reassemblierung von Fragmenten verwendet, um alle Teile einer Fragmentkette identifizieren zu können.

■ Flags

- Feldlänge: 3 Bit

■ Beschreibung

- Zwei Bits namens DF („don't fragment“ - 2. Bit) und MF („more fragment“ - 3. Bit) steuern die Behandlung des Paketes im Falle der Fragmentierung.
- Ist das DF-Bit gesetzt, darf das IP-Paket unter keinen Umständen fragmentiert werden, auch wenn es dann nicht mehr weiter transportiert werden kann und verworfen werden muss.
- Das erste Bit dieses Felds ist ungenutzt.

Feldelemente des IP-Headers (4/8)

- **Fragment Offset (FO)**

- Feldlänge: 13 Bit, Einheiten 8 Octet

- **Beschreibung**

- Dieses Feld gibt die Lage der Fragmentdaten relativ zum Anfang des Datenblockes im ursprünglichen Datagramm an.
- Bei einem **nicht fragmentierten** Datagramm oder beim ersten Fragment ist der Wert des FO immer **auf Null** gesetzt.
- Der FO definiert die Lage des jeweiligen Fragments als ein Vielfaches von 8 Byte (Grundeinheit der Fragmentierung).
- Durch die zur Verfügung stehenden 13 Bits sind maximal 8.192 Fragmente pro Datagramm möglich (65.536 Byte).
- Das FO-Feld ermöglicht dem Empfänger, mehrere Fragmente in der richtigen Reihenfolge zusammensetzen.

0	4	8	16	24	31
Version	IHL	Type of Service	Total Length		
Identification			Flags	Fragment Offset	
Time to Live		Protocol	IP Header Checksum		
IP Source Address					
IP Destination Address					
Option				Füllzeichen	

Feldelemente des IP-Headers (5/8)

- **Time to Live (TTL)**

- Feldlänge: 8 Bit

- **Beschreibung**

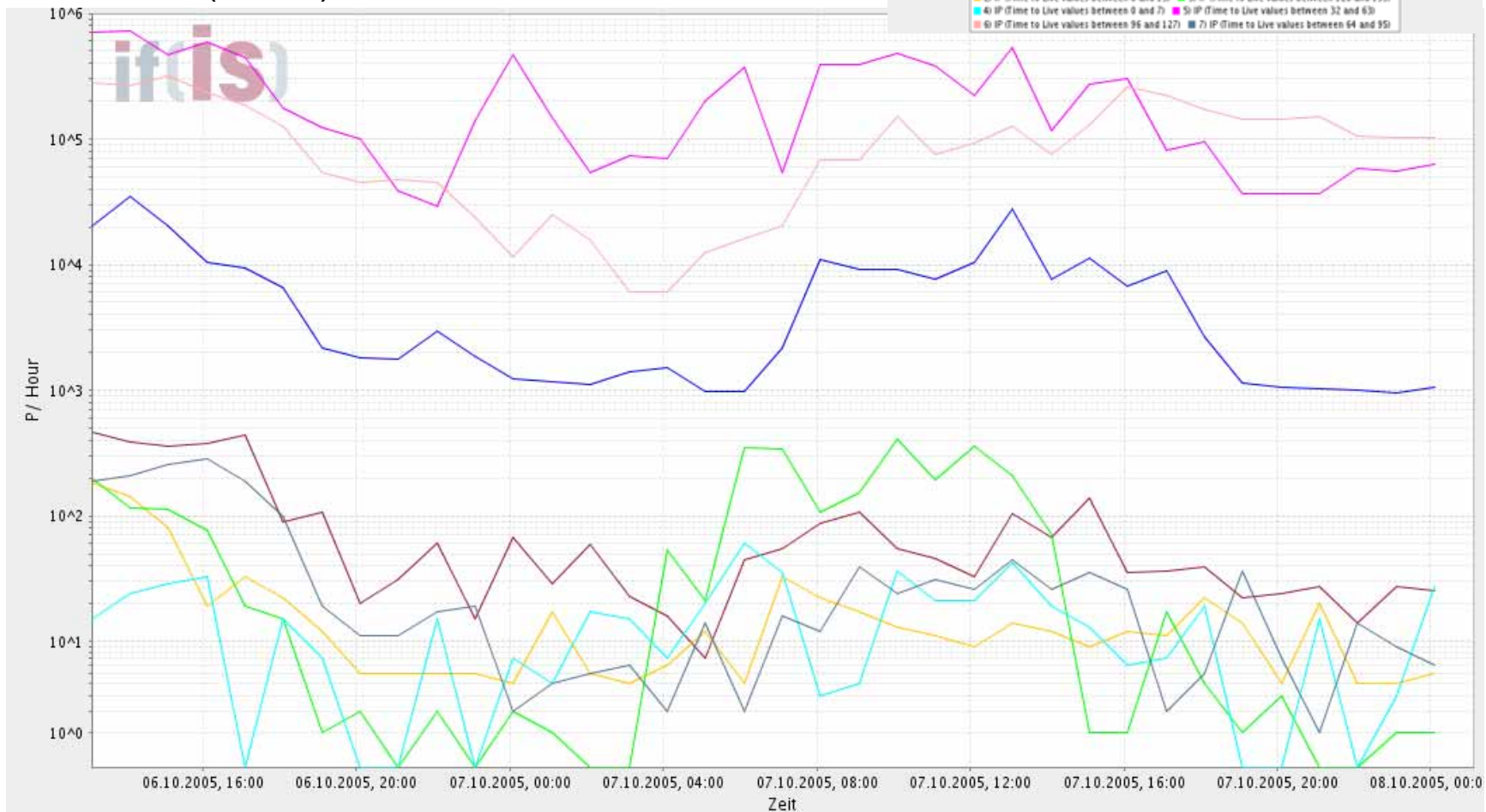
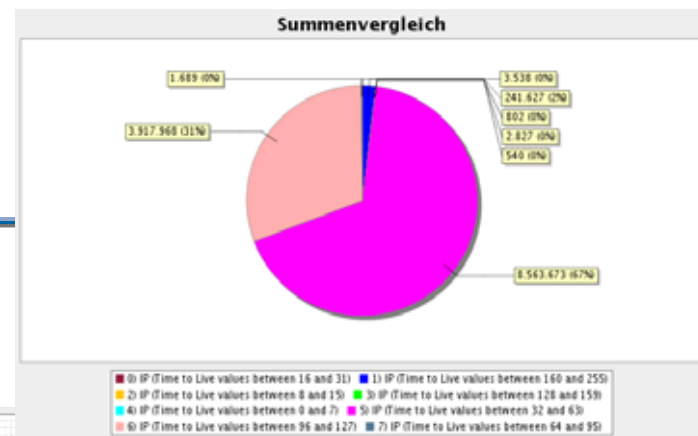
- Der absendende Host gibt an, wie lange das Paket im Netz verweilen darf, bevor es weggeworfen werden muss.
- Jedes Mal, wenn das Datagramm in einem Netzelement die Vermittlungsebene durchläuft, muss die IP-Einheit dieses Feldes mindestens um eins vermindern.
- Somit ist die Lebenszeit meist gleichbedeutend mit der Anzahl der Netzknoten, die von einem Paket maximal durchlaufen werden können (=hops).
- Wenn dieses Feld den **Wert 0** enthält, muss das Paket **weggeworfen** werden.
- Somit wird verhindert, dass ein Paket **endlos im Netz zirkuliert!**
- Der Absender des Paketes erhält in diesem Fall eine ICMP-Nachricht über den Vorgang.

0	4	8	16	24	31
Version	IHL	Type of Service	Total Length		
Identification			Flags	Fragment Offset	
Time to Live		Protocol	IP Header Checksum		
IP Source Address					
IP Destination Address					
Option				Füllzeichen	

IAS: FB Informatik

→ Time to Live (TTL)

- Linux: TTL Default 64
- Windows XP: TTL Default 128
- Router (Cisco): TTL Default 254



(In) IP (Time to Live values between 16 and 31) IP (Time to Live values between 160 and 255) IP (Time to Live values between 8 and 15) IP (Time to Live values between 128 and 159)
 IP (Time to Live values between 0 and 7) IP (Time to Live values between 32 and 63) IP (Time to Live values between 96 and 127) IP (Time to Live values between 64 and 95)

Feldelemente des IP-Headers (6/8)

- **Protocol (PROT)**

- Feldlänge: 8 Bit

- **Beschreibung**

- Dieses Feld enthält die **Identifikation des Transportprotokolls**, dem das Paket zugestellt werden muss.

Wert (dez.)	Protokoll	
1	ICMP	Internet Control Message Protocol
2	IGMP	Internet Group Management Protocol
6	TCP	Transmission Control Protocol
8	EGP	Exterior Gateway Protocol
17	UDP	User Datagram Protocol
47	GRE	Generic Routing Encapsulation Protocol
50	ESP	Encapsulated Security Payload
89	OSPF	Open Shortest Path First

- **IP Header Checksum**

- Feldlänge: 16 Bit

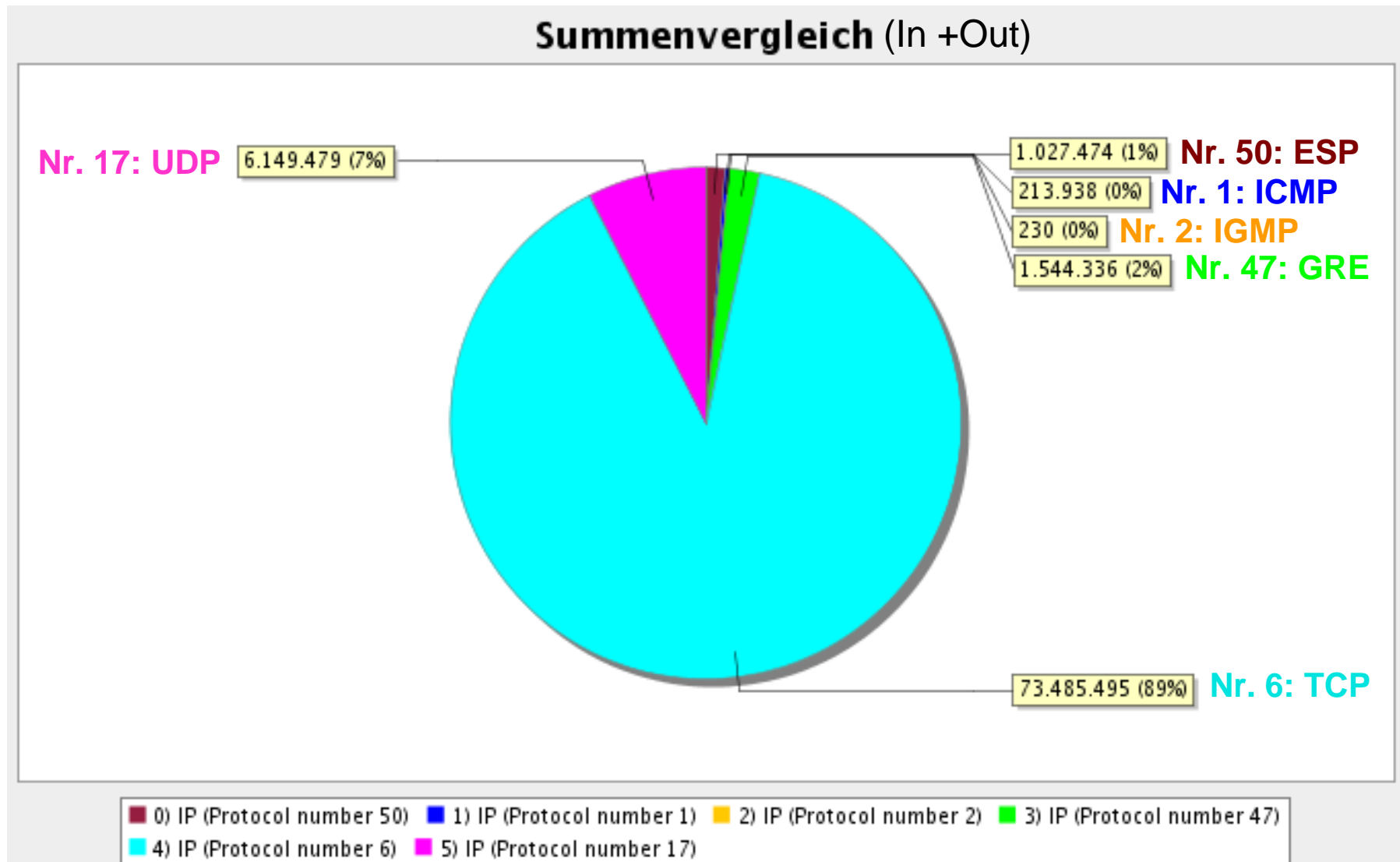
- **Beschreibung**

- Enthält eine **Prüfsumme**, die nur den **IP-Header** gegen Fehler sichert
 - Beim Durchgang durch einen Router verändert sich der Header (z.B. Herabsetzen von TTL um Eins) und die Prüfsumme wird neu berechnet.

0	4	8	16	24	31
Version	IHL	Type of Service	Total Length		
Identification			Flags	Fragment Offset	
Time to Live	Protocol	IP Header Checksum			
IP Source Address					
IP Destination Address					
Option				Füllzeichen	

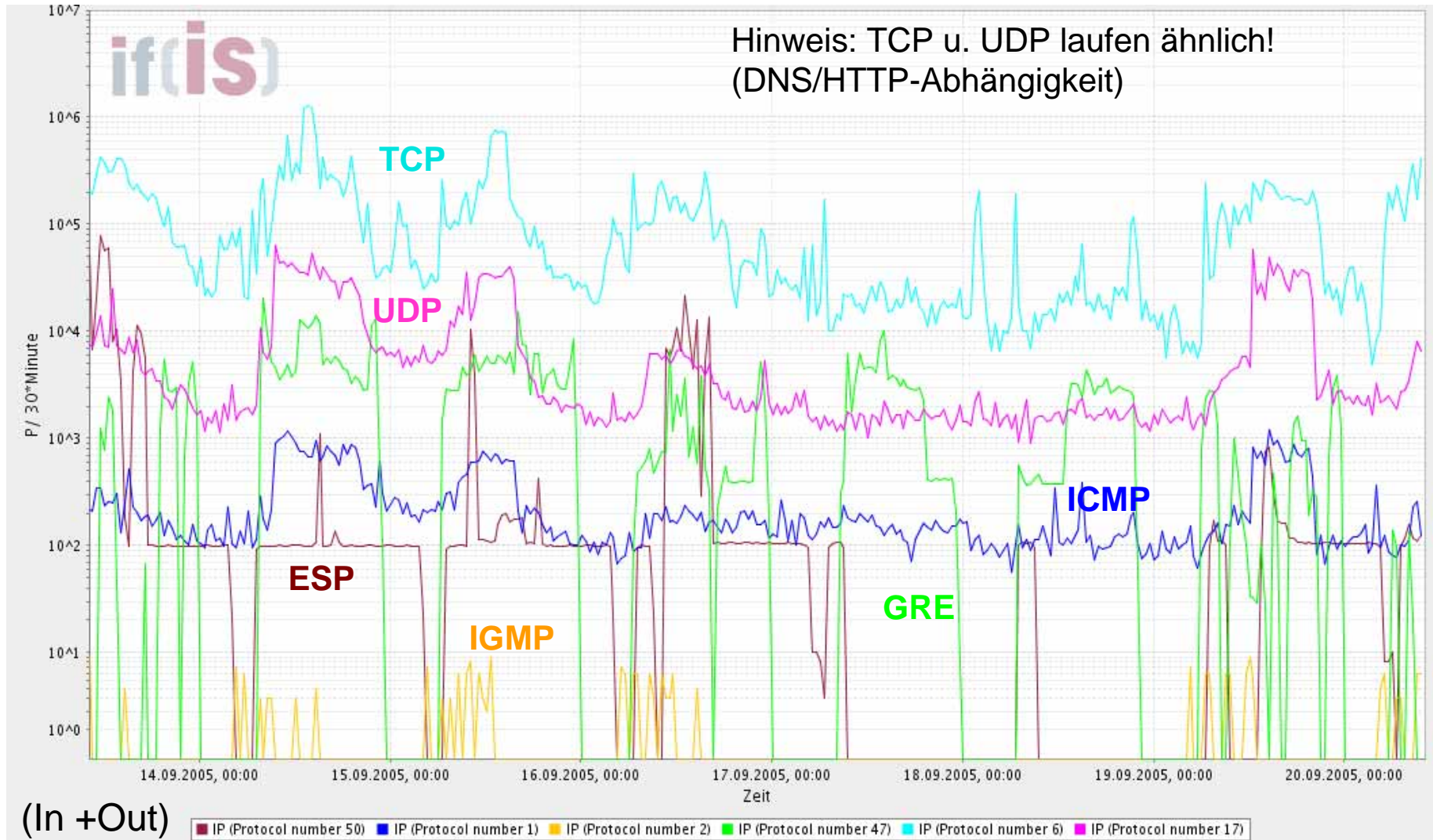
Internet-Analyse-System: FB Informatik

→ Protocol (PROT) – (1/2)



Internet-Analyse-System: FB Informatik

→ Protocol (PROT) – (2/2)



Feldelemente des IP-Headers (7/8)

- **IP Source Address (Source)**

- Feldlänge: 32 Bit

- **Beschreibung**

- Enthält die Internet-Adresse des Netzknotens, der das Datagramm erzeugt hat

- **IP Destination Address (Dest)**

- Feldlänge: 32 Bit

- **Beschreibung**

- Enthält die Internet-Adresse des Netzknotens, für den das Datagramm bestimmt ist

0	4	8	16	24	31
Version	IHL	Type of Service	Total Length		
Identification			Flags	Fragment Offset	
Time to Live		Protocol	IP Header Checksum		
IP Source Address					
IP Destination Address					
Option				Füllzeichen	

ICMP - Internet Control Message Protocol

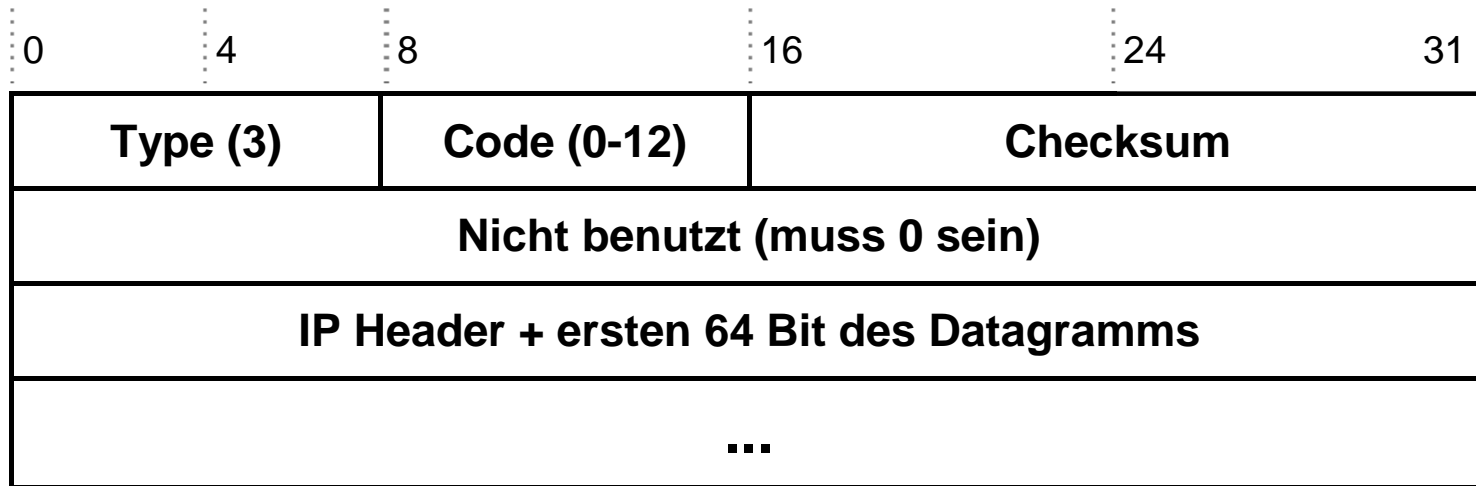
- Das Internet Control Message Protocol (ICMP) ist ein Protokoll der Vermittlungsebene und erlaubt es einer IP-Realisierung auf einem Rechner, an die IP-Realisierung eines anderen Rechners **Kontroll- oder Fehlermeldungen** zu schicken.
- Diese Möglichkeit wurde geschaffen, damit Router den Hosts (Rechnern) den Grund eines Fehlers bei der Zustellung eines IP-Paketes zustellen können.
- ICMP ist Bestandteil jeder IP-Implementierung und transportiert Fehler- und Diagnoseinformationen für IP.
- Das ICMP-Paket wird im Datenteil eines IP-Paketes transportiert, seine Transportprotokoll-Adresse im Protokoll-Feld des IP-Headers ist „1“.
- Dennoch wird **ICMP** nicht als ein Protokoll der höheren Schicht, sondern als **Bestandteil der Vermittlungsebene betrachtet**.

ICMP - Internet Control Message Protocol

- Jede ICMP-Nachricht hat ihr eigenes Format, alle beginnen jedoch mit drei identischen Feldern:
 - einem 8 Bit TYPE-Feld, das die Art der ICMP-Nachricht angibt
 - einem 8 Bit CODE-Feld, das weitergehende Informationen enthalten kann
 - und einem 16 Bit CHECKSUM-Feld, das eine Prüfsumme über das ICMP-Paket enthält.
- **Die restlichen Felder des Paketes sind abhängig von der ICMP-Nachricht.**

ICMP - Internet Control Message Protocol

→ Beispiel: Destination Unreachable-Nachricht [22]



- Mit diesem Datagramm wird dem Absender mitgeteilt, dass sein Paket nicht zugestellt werden könnte.
- Das CODE-Feld enthält weitergehende Informationen zum Grund des Fehlers, wie z.B. „Network Unreachable (0)“ oder Fragmentierung „needed and DF set (4)“.
- Im Datenteil sind außerdem der Header des betroffenen Pakets und die ersten 64 Bit des Datagramms enthalten, woraus der Sender zweifelsfrei ermitteln kann, welches Paket gemeint ist.

ICMP - Internet Control Message Protocol

- Die von ICMP unterstützten Kontrollnachrichten sind:
 - **destination unreachable (Type 3)**
Ein Datagramm konnte nicht zugestellt werden, da ein Netzwerk oder Rechner nicht erreichbar war, ein Protokoll nicht betriebsbereit war, oder Fragmentierung notwendig gewesen wäre, aber durch das Flag-Feld (im IP-Header) verboten wurde.
 - **time exceeded (Type 11)**
Ein Datagramm wurde weggeworfen, da seine Lebensdauer ablief oder ein Fragment wurde weggeworfen, weil es zu lange in der Warteschlange für die Reassemblierung war.
 - **parameter problem (Type 12)**
Der Absender eines IP-Datagramms wird verständigt, dass das Paket aufgrund von fehlerhaften Angaben im IP-Protokollkopf weggeworfen werden musste.
 - **source quench (Type 4)**
Ein Netzwerkgerät wirft Datagramme weg, da es zu wenig Betriebsmittel (z.B. Zwischenspeicher) hat.

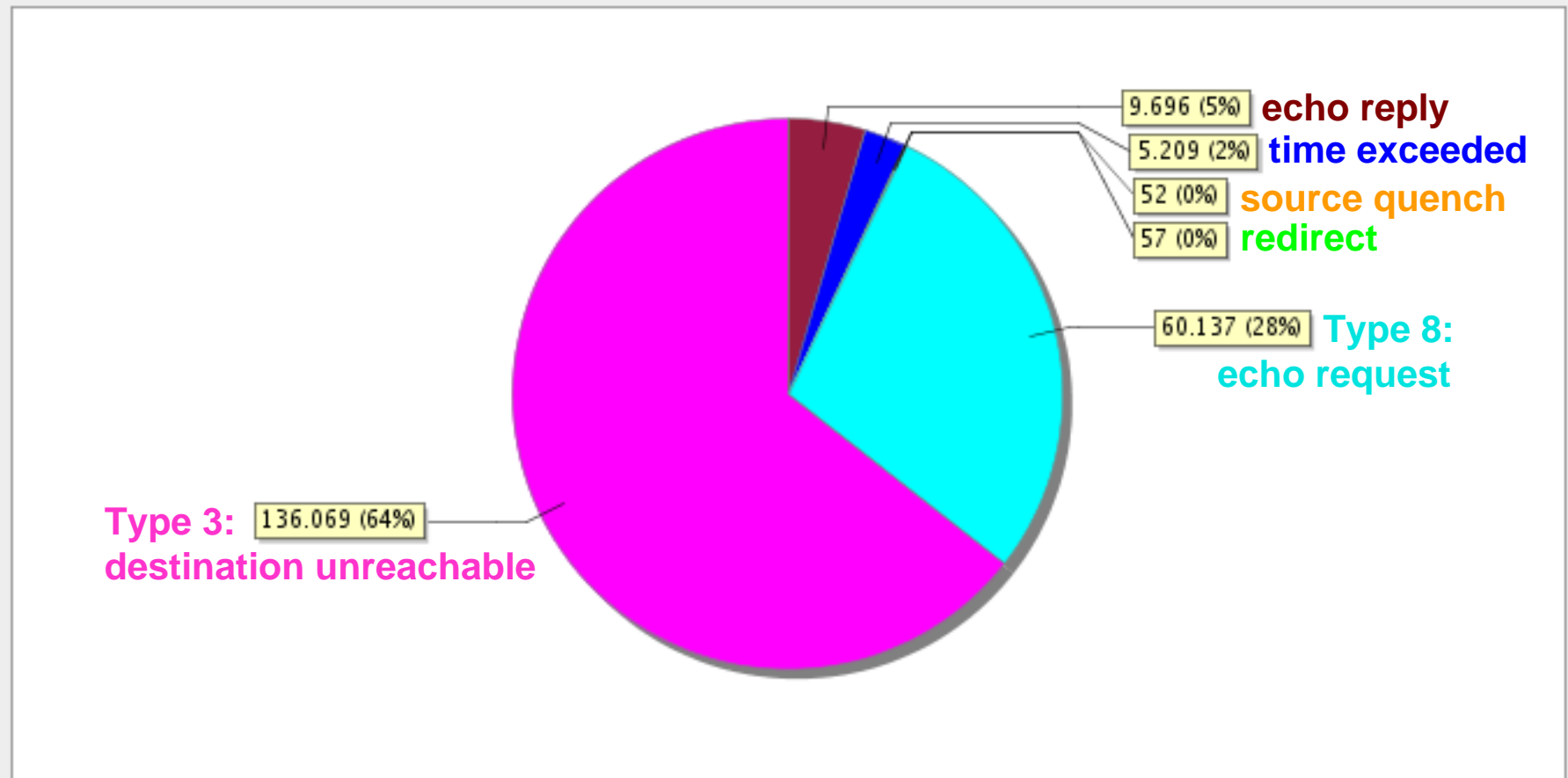
ICMP - Internet Control Message Protocol

- **redirect (Type 5)**
Wird ausgesendet, wenn ein Gateway erkennt, dass der Absender eines IP-Paketes dieses direkt an den nächsten Gateway senden könnte, d.h. ein unnötiger Umweg gegangen wird. Die ICMP-Nachricht enthält die Internet-Adresse des nächsten direkten Gateway (**Sicherheitsproblem!**)
- **echo request / echo reply (Type 8/0)**
Zum Test, ob eine IP-Adresse existiert, wird eine *echo request*-Nachricht gesendet. Nach Erhalt einer solchen Nachricht antwortet die empfangende Einheit mit einer *echo reply*-Nachricht.
- **timestamp request / timestamp reply (Type 15/16)**
Zum Feststellen der Verzögerung im Netzwerk zwischen zwei Netzwerkgeräten.
- **address mask request / address mask reply (Type 17/18)**
Zur Bestimmung der Subnetz-Adressmaske.

Internet-Analyse-System: FB Informatik

→ ICMP – (1/2)

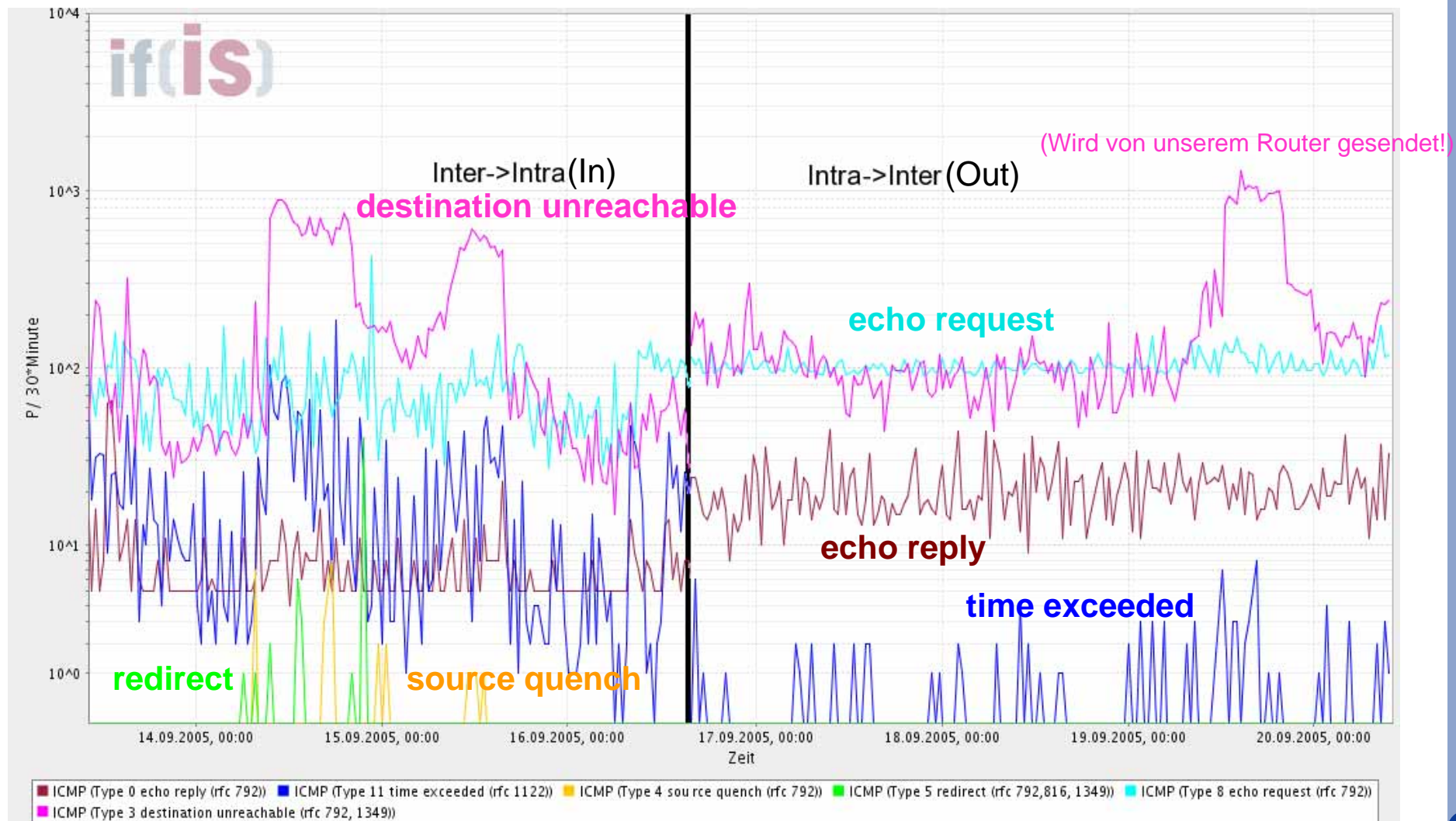
Summenvergleich (In +Out)



- 0) ICMP (Type 0 echo reply (rfc 792))
- 1) ICMP (Type 11 time exceeded (rfc 1122))
- 2) ICMP (Type 4 source quench (rfc 792))
- 3) ICMP (Type 5 redirect (rfc 792,816, 1349))
- 4) ICMP (Type 8 echo request (rfc 792))
- 5) ICMP (Type 3 destination unreachable (rfc 792, 1349))

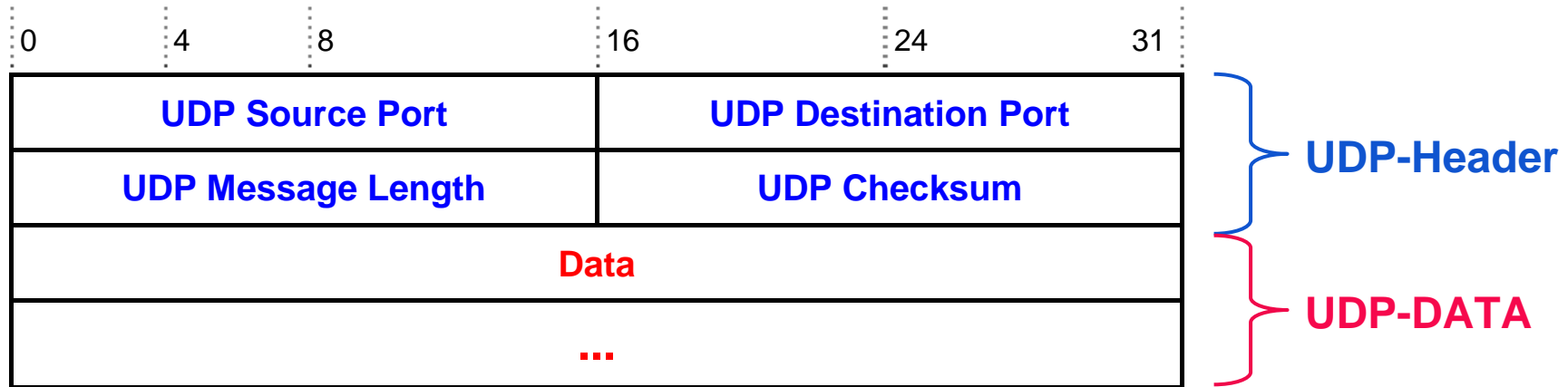
Internet-Analyse-System: FB Informatik

→ ICMP – (2/2)



UDP - User Datagram Protocol

→ Das Format einer UDP-Nachricht



■ Source Port, Destination Port

- Feldlänge: 16 Bit

■ Beschreibung

- Source- und Destination-Port sind 16-Bit UDP Ports, wobei der Source-Port optional ist.
- Wenn er benutzt wird, so ist dies der Port, an den Antworten geschickt werden können, ansonsten sollte der Wert 0 sein.

■ Length

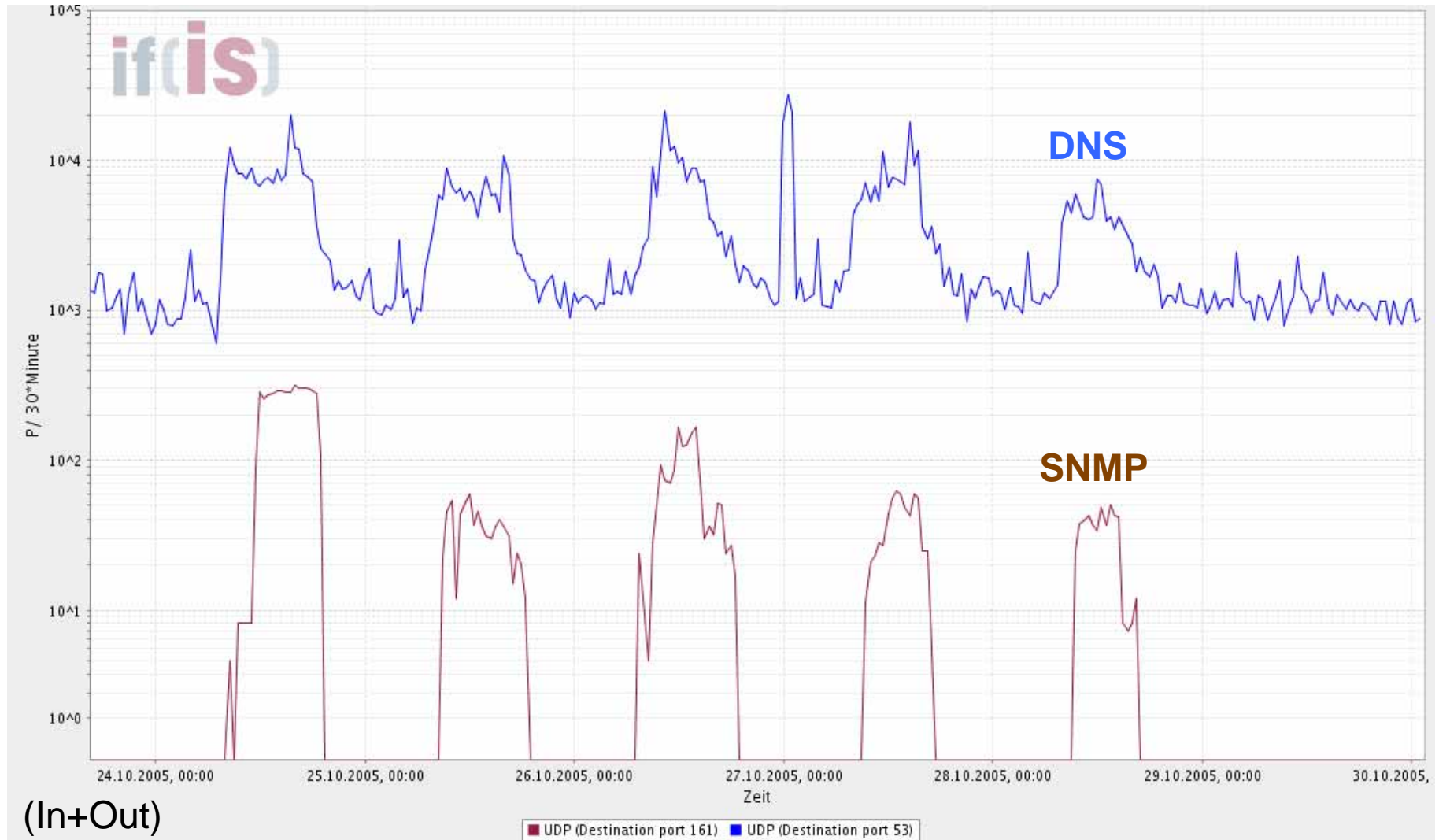
- Feldlänge: 16 Bit

■ Beschreibung

- Anzahl der Octets im UDP-Datagramm - UDP-Daten und UDP-Header. Der Minimalwert ist 8 - die Länge des Headers ohne Daten.

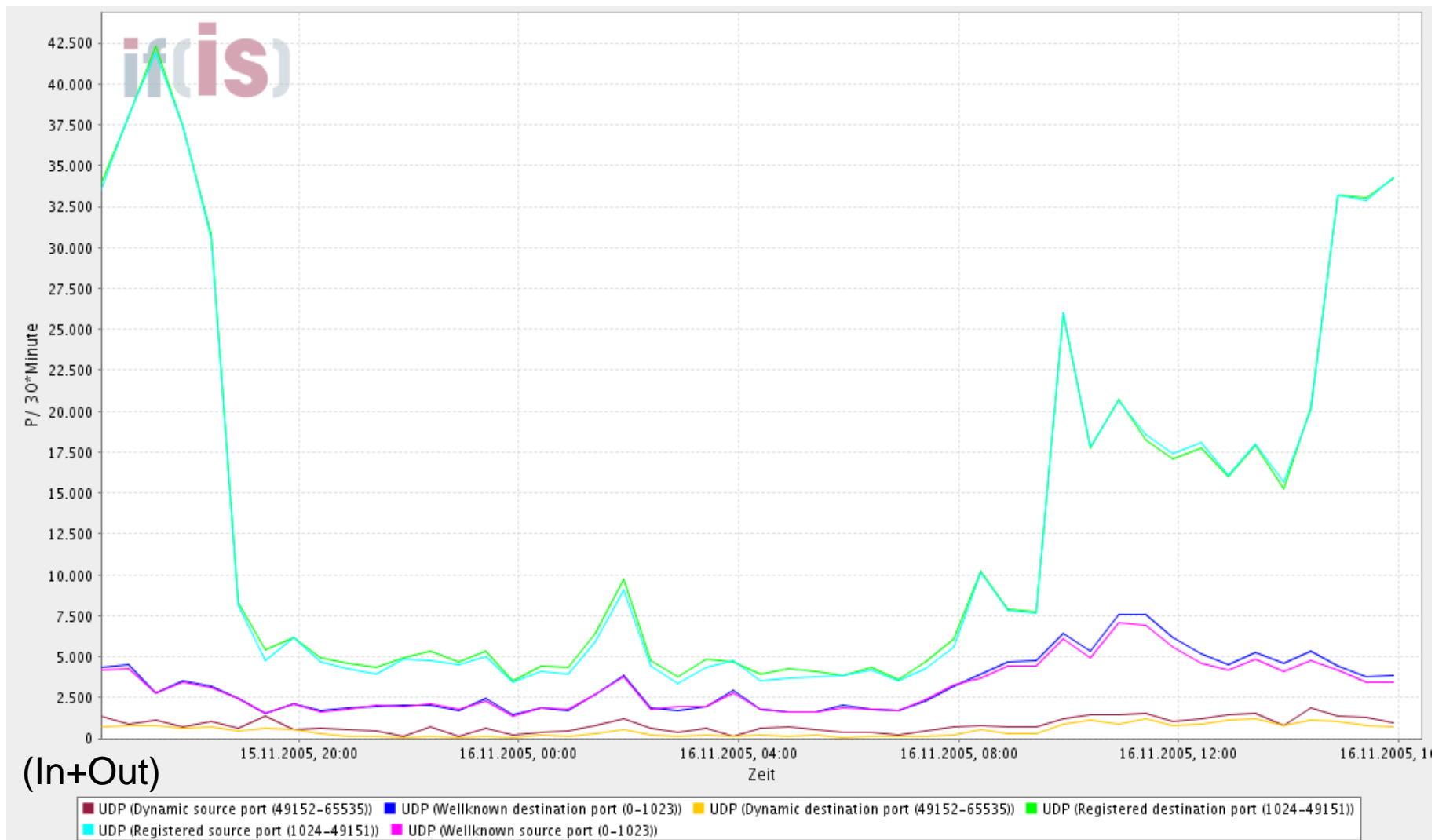
IAS: FB Informatik

→ Destination Port (UDP)



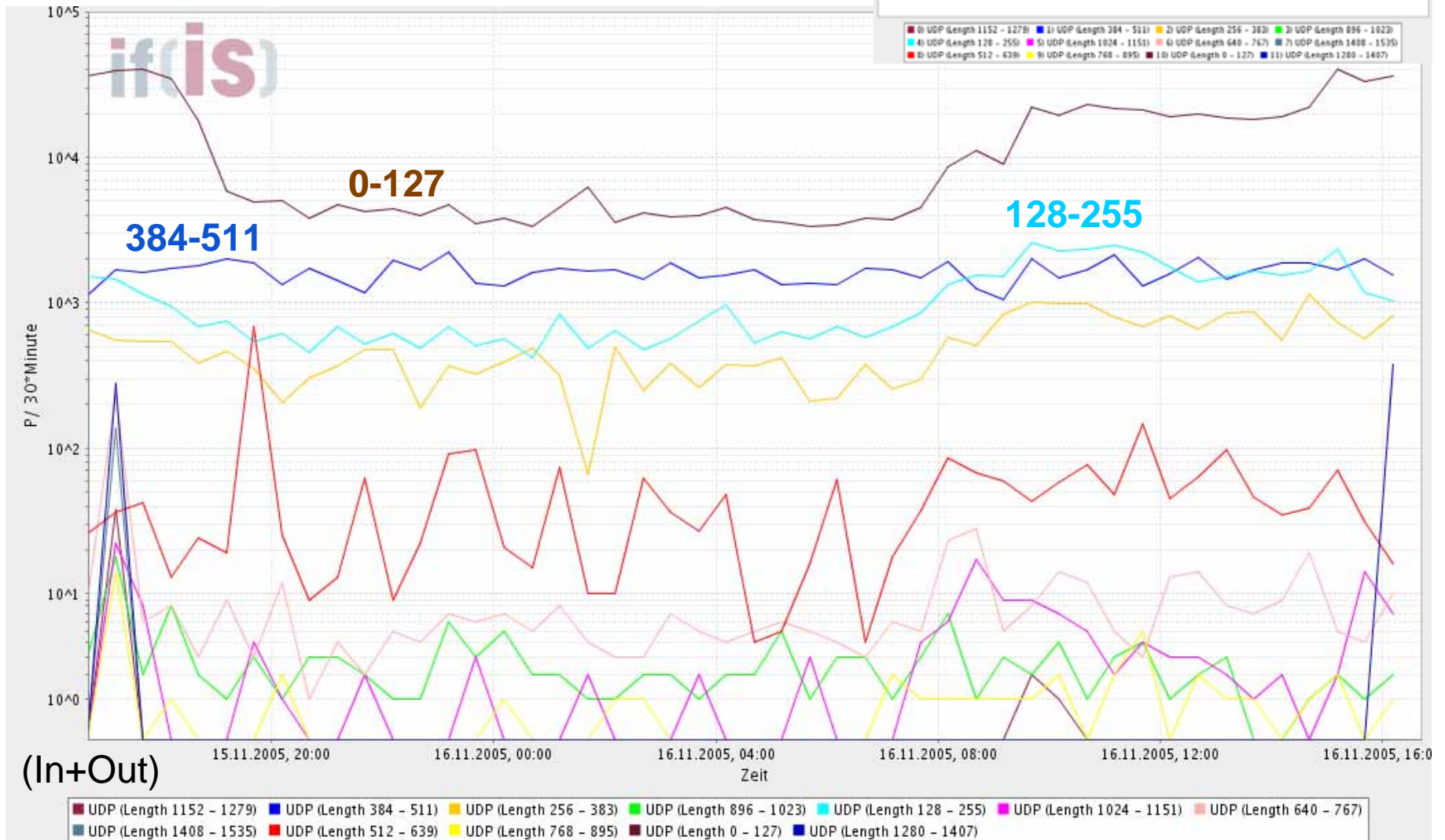
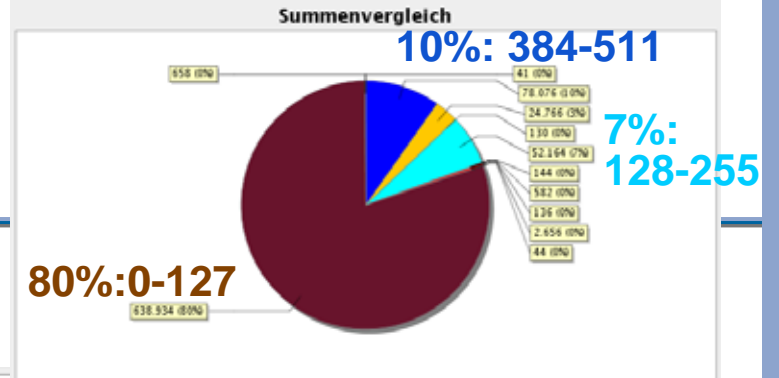
IAS: FB Informatik

→ Portverteilung nach Portgruppen

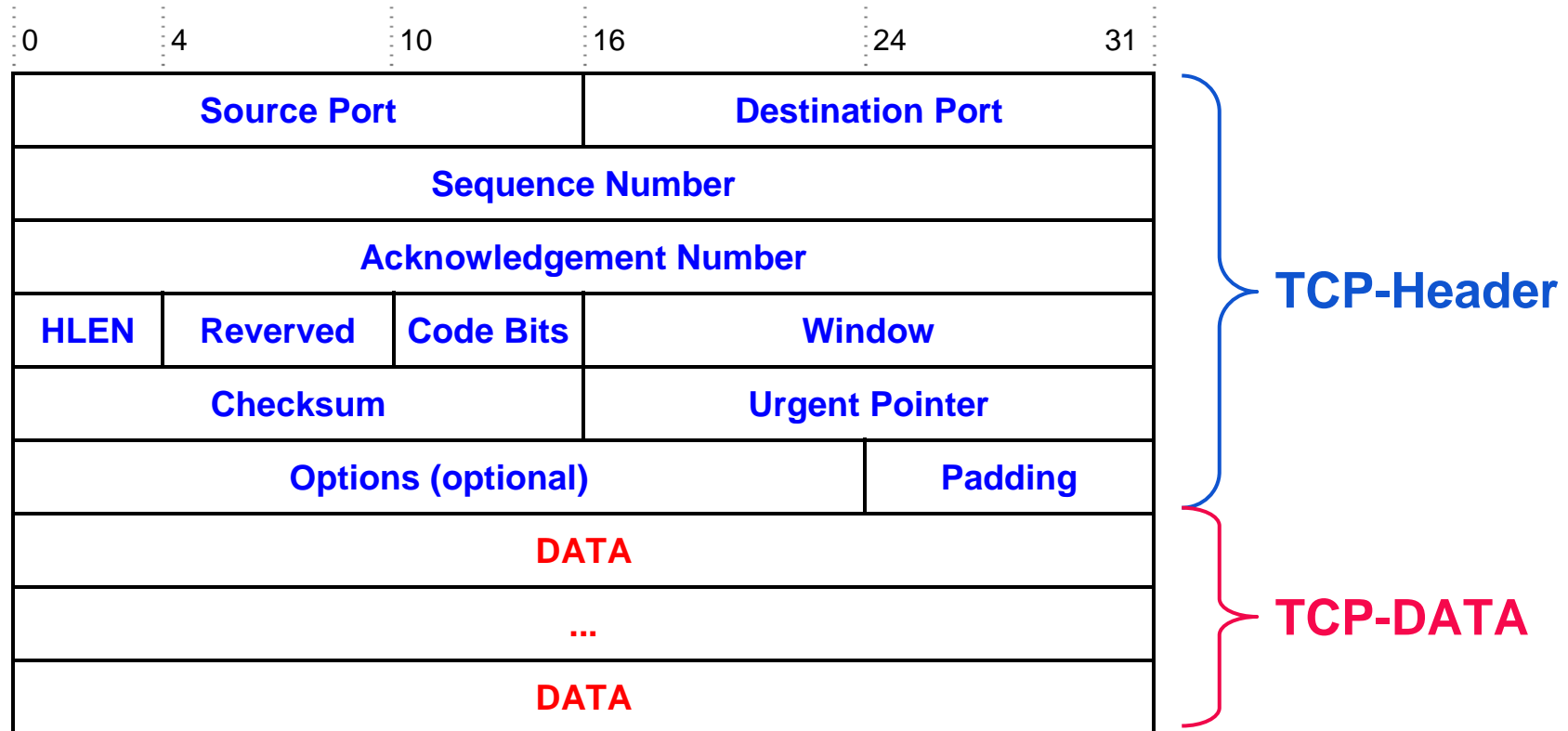


IAS: FB Informatik

→ Length



Das Format eines TCP-Paketes



Feldelemente des TCP-Headers (1/4)

- **Source- und Destination Ports**

- Feldlänge: 16 Bit

- **Beschreibung**

- Enthalten die Portnummern der Applikationen

- **Sequence Number**

- Feldlänge: 32

- **Beschreibung**

- enthält die Position des Pakets im Octet-Stream

- **Acknowledgement Number**

- Feldlänge: 32

- **Beschreibung**

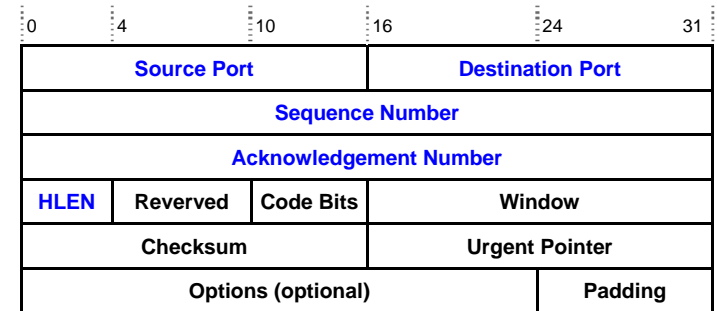
- enthält die Sequenznummer des Octets, welches der Empfänger als nächstes empfangen will

- **HLEN**

- Feldlänge: 4

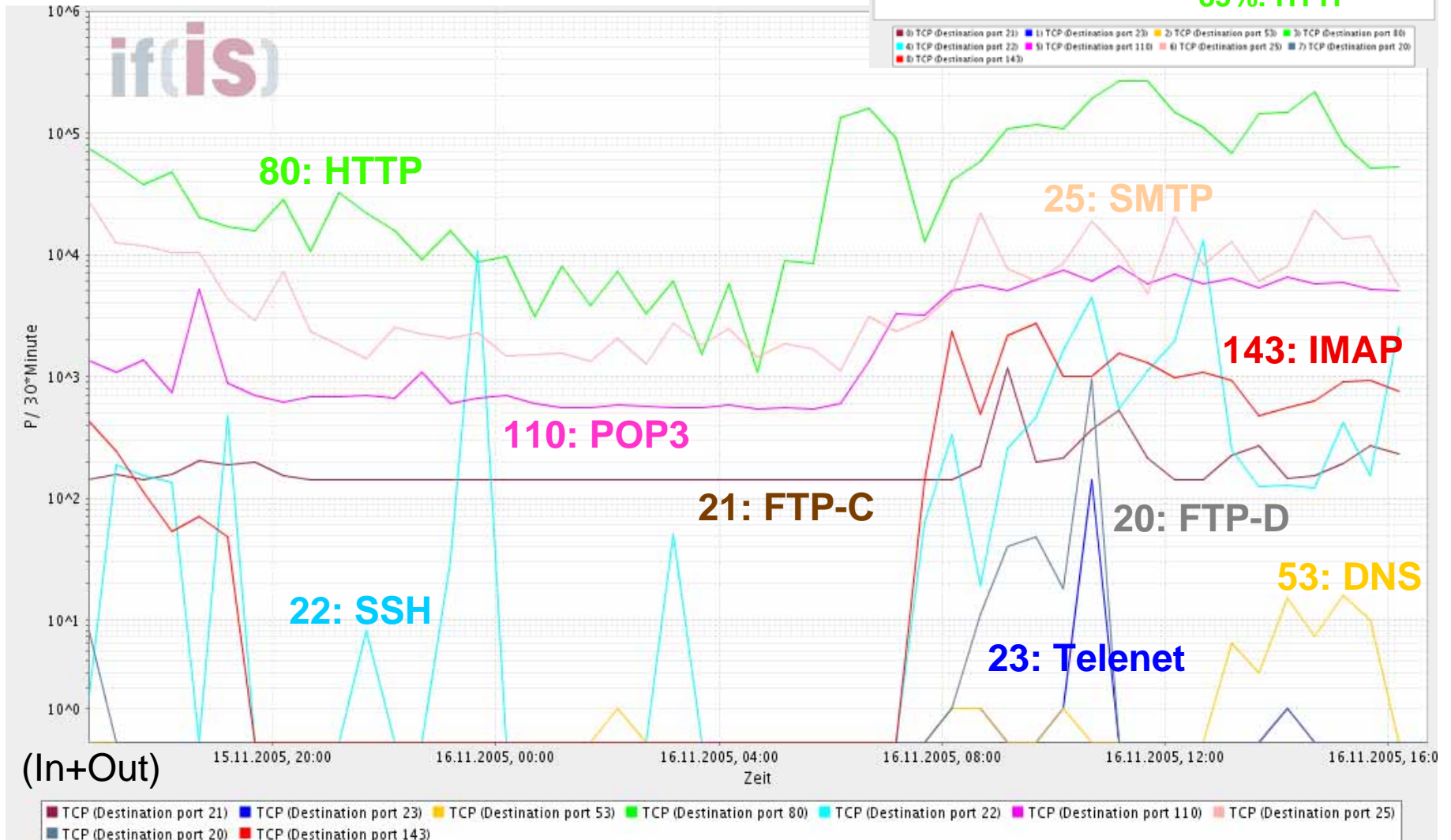
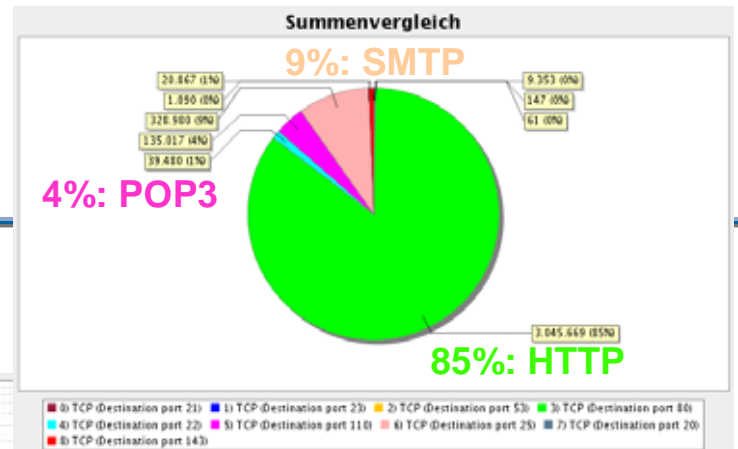
- **Beschreibung**

- Die Länge des Headers in 32-Bit Werten (da Options variabel ist)



IAS: FB Informatik

→ Destination Port (TCP)



IAS: FB Informatik

→ HLEN

HLEN: 8

NOP (2 Byte)

Timestamp (10 Byte)

HLEN: 7

MSS (4 Byte)

NOP (2 Byte)

SACK permitted (2 Byte)

HLEN: 10

NOP (2 Byte)

SACK (18 Byte)

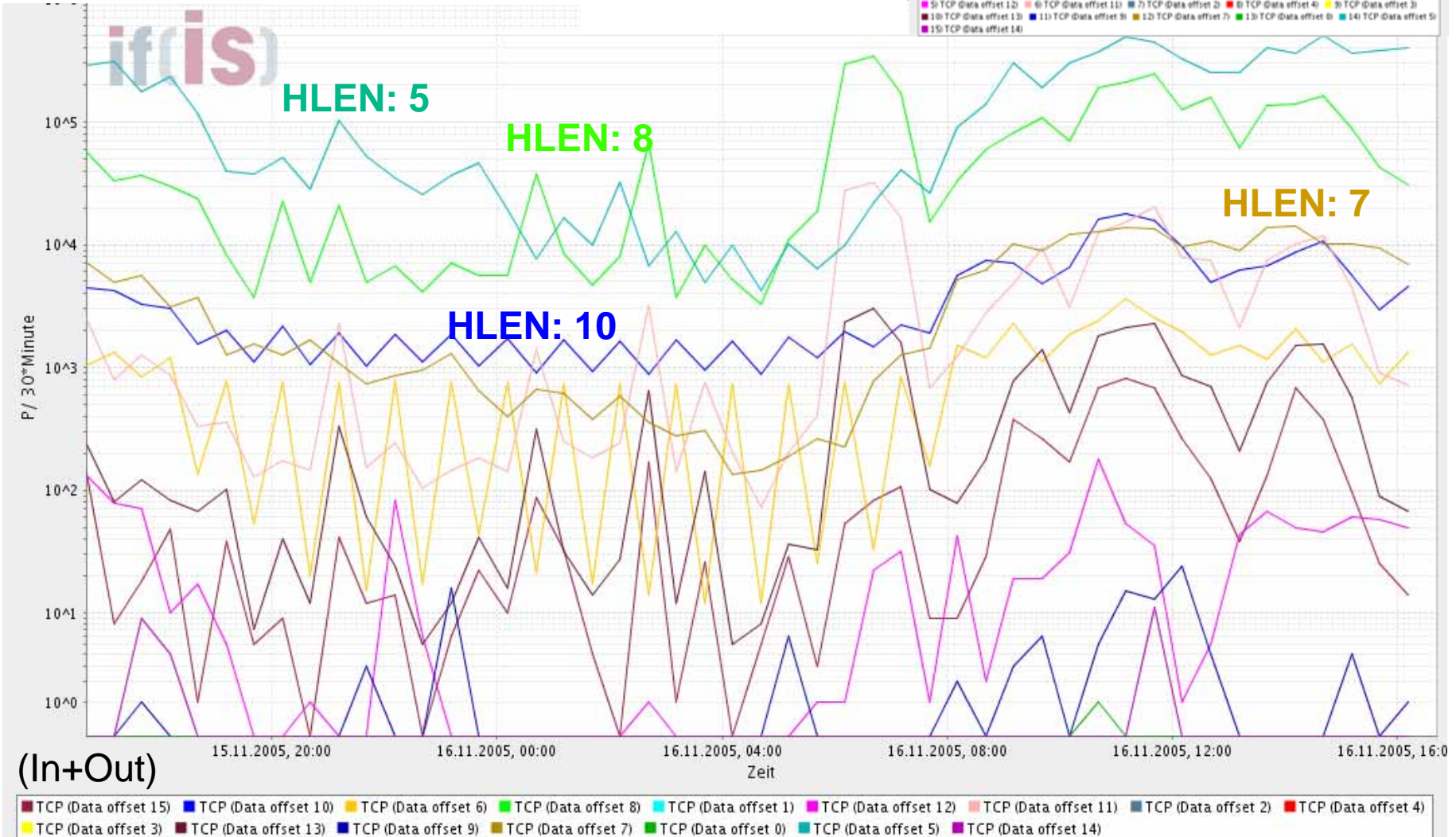
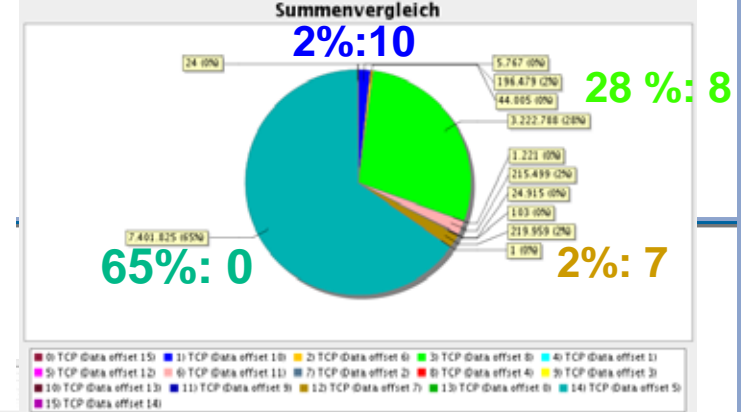
oder

MSS (4 Byte)

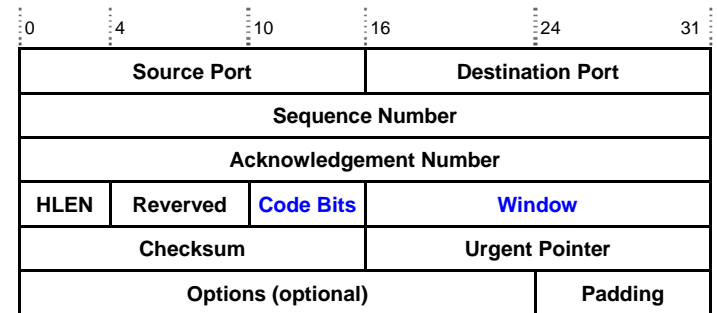
SACK permitted (2 Byte)

NOP (1 Byte)

WScale (3 Byte)



Feldelemente des TCP-Headers (2/4)



Code Bits

- Feldlänge: 6 Bit

Beschreibung

Bits (von links nach rechts)	Wenn gesetzt (=1)
URG	Urgent-Pointer ist gültig (Interrupt Nachricht)
ACK	Bestätigung eines Segments (acknowledgement Feld ist gültig).
PSH	(push) Der Empfänger soll die Daten der Anwendung so schnell wie möglich zur Verfügung stellen.
RST	Reset der Verbindung
SYN	Synchronisation der initialen Sequenz-Nummer bei Verbindungsaufbau
FIN	Der Sender hat das Senden seiner Daten beendet (Ende der Übertragung).

Window

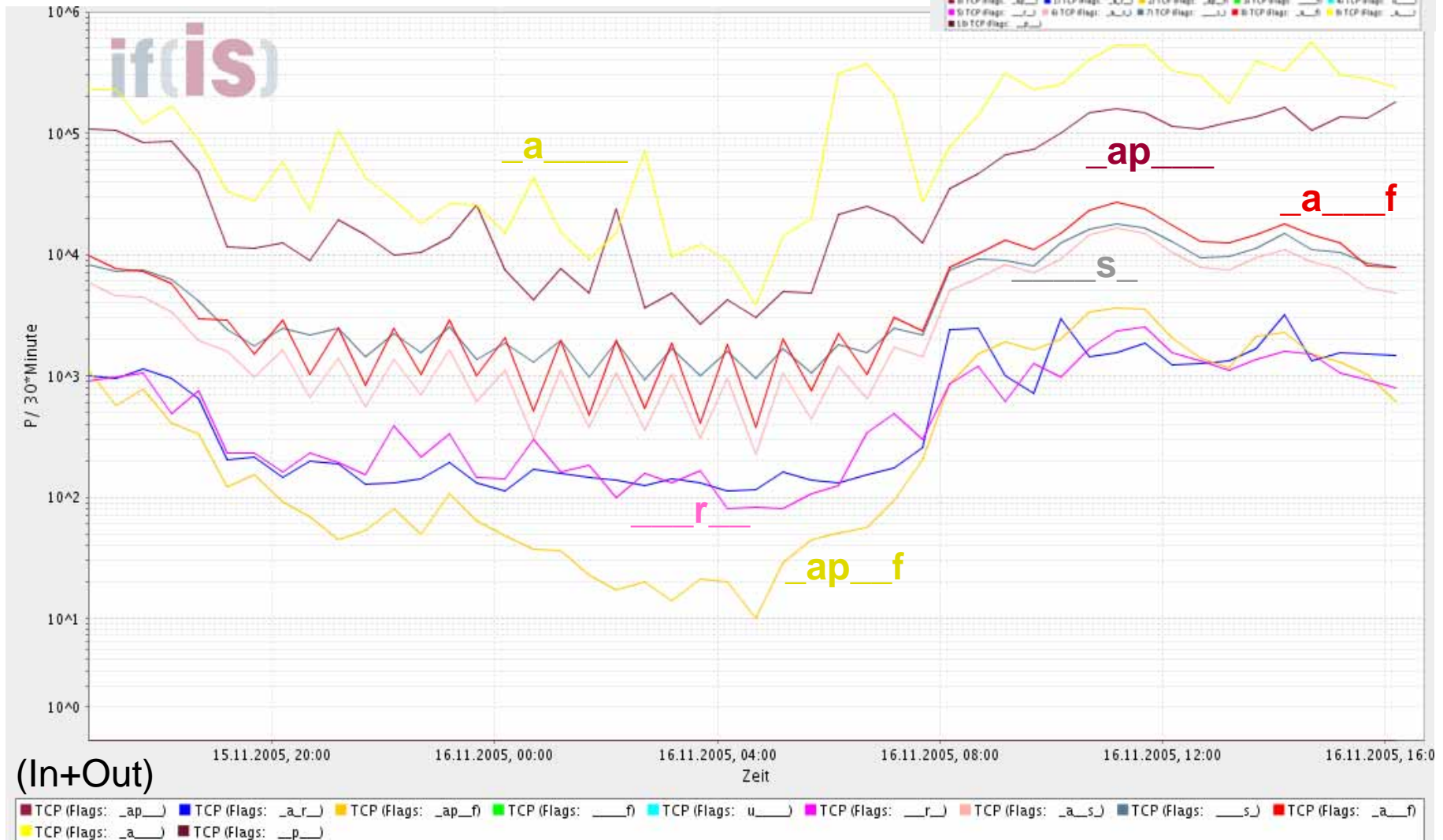
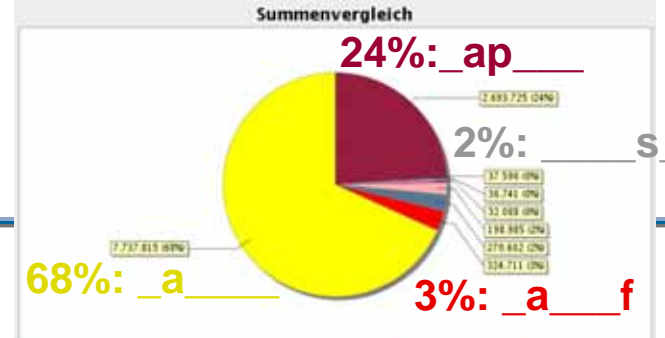
- Feldlänge: 16

Beschreibung

- Angabe der Größe des Empfangsfenster (Einheit in Octets und Vielfaches der Segment-Größe).

IAS: FB Informatik

→ Code Bits



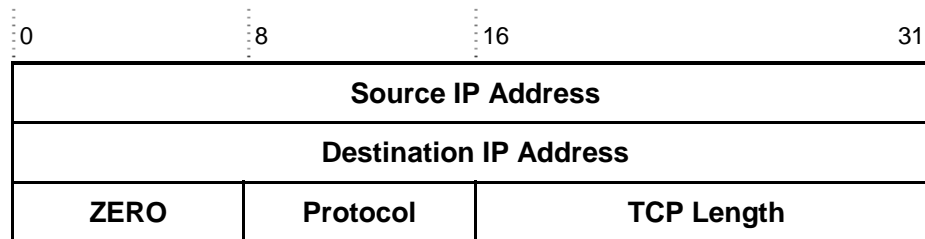
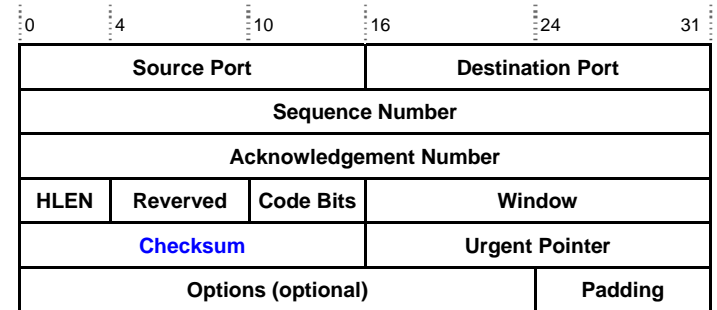
Feldelemente des TCP-Headers (3/4)

- **TCP Checksum**

- Feldlänge: 16 Bit

- **Beschreibung**

- Die Berechnung der Prüfsumme erfolgt, indem zuerst (wie bei UDP) ein Pseudo-Header vor das TCP-Segment gestellt wird.



- Der Pseudo-Header hat den Sinn festzustellen, ob das TCP-Paket den korrekten Empfänger erreicht hat.
 - Das Feld „Protocol“ enthält für TCP den Wert 6.
 - Das Feld „TCP-Length“ ist die Länge des gesamten TCP-Segments inklusive des Headers, aber ohne Pseudo-Header.
 - Berechnet wird die Prüfsumme als 16-Bit Einerkomplement-Summe über Pseudo-Header, UDP-Header und UDP-Daten (**Datenunversehrtheit!**).

Feldelemente des TCP-Headers (4/5)

0	4	10	16	24	31
Source Port			Destination Port		
Sequence Number					
Acknowledgement Number					
HLEN	Reserved	Code Bits	Window		
Checksum			Urgent Pointer		
Options (optional)				Padding	

■ Urgent-Pointer

- Feldlänge: 16 Bit

■ Beschreibung

- In manchen Fällen ist es notwendig, Out-of-Band Daten zu verschicken, die, selbst wenn im Empfangspuffer des Empfängers noch Daten vorliegen, sofort an die Applikation weitergegeben werden müssen.
- Dies ist z.B. bei einem Remote Login notwendig, wenn ein Abbruch des Login-Vorgangs erzwungen werden soll (Ctrl-C).
- Wenn ein Urgent-Pointer von TCP empfangen wird, muss TCP der Empfänger-Applikation den Urgent-Modus mitteilen, genauso, wie eine Rückkehr in den Normal-Modus nach Abschluss des Empfangs der Urgent-Pakete mitgeteilt werden muss. Wenn das URG-Bit gesetzt ist, weist der Urgent-Pointer auf die Position in den Daten innerhalb des Segments, wo die Urgent-Daten enden.

Feldelemente des TCP-Headers (5/5)

0	4	10	16	24	31
Source Port			Destination Port		
Sequence Number					
Acknowledgement Number					
HLEN	Reserved	Code Bits	Window		
Checksum			Urgent Pointer		
Options (optional)				Padding	

■ Options

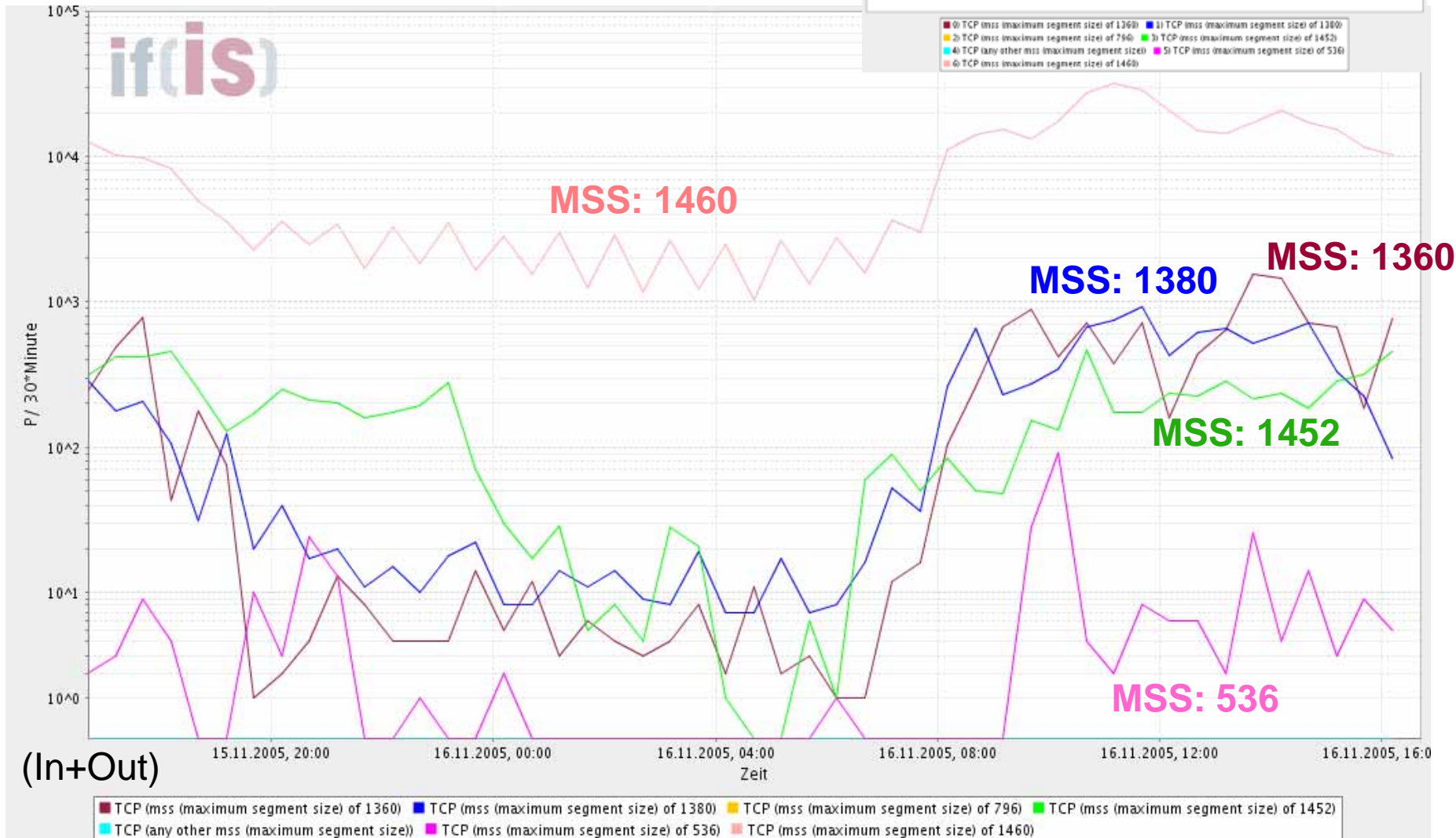
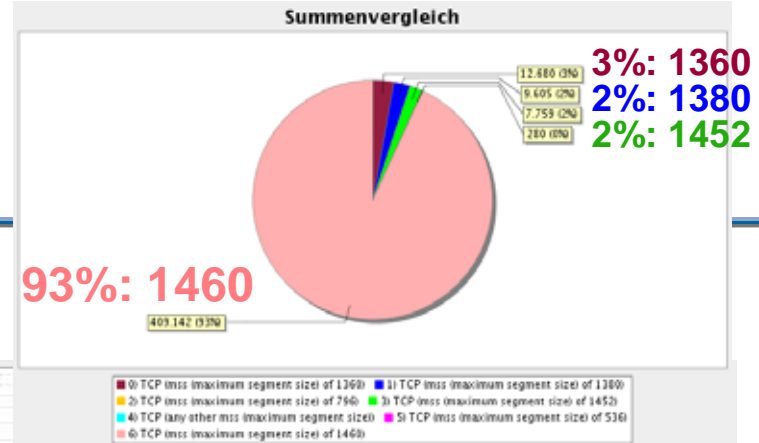
- Feldlänge: 24

■ Beschreibung

- Mit dem Option-Feld wird die maximale Größe des TCP-Segments zwischen Sender und Empfänger abgestimmt. Dies ist zur Ausnutzung der maximalen Bandbreite eines Netzes wichtig. Z.B:
 - MSS (Maximum Segment Size)
Legt die maximale Segmentgröße fest, die verarbeitet werden kann. Falls ein Rechnersystem diese Option nicht verwendet, werden 536 Byte als die Standardgröße für Nutzdaten verwendet. Die maximale Segmentgröße muss nicht in beiden Richtungen gleich sein.
 - WSopt (Window Scale)
Dieser Skalierungsfaktor wird beim Verbindungsaufbau ausgehandelt. Er bestimmt den Faktor mit dem der Wert im Window-Feld multipliziert wird. Der Faktor kann maximal den Wert 14 annehmen - Window folglich 1 Gigabyte.
 - SACK (Selective Acknowledgment)

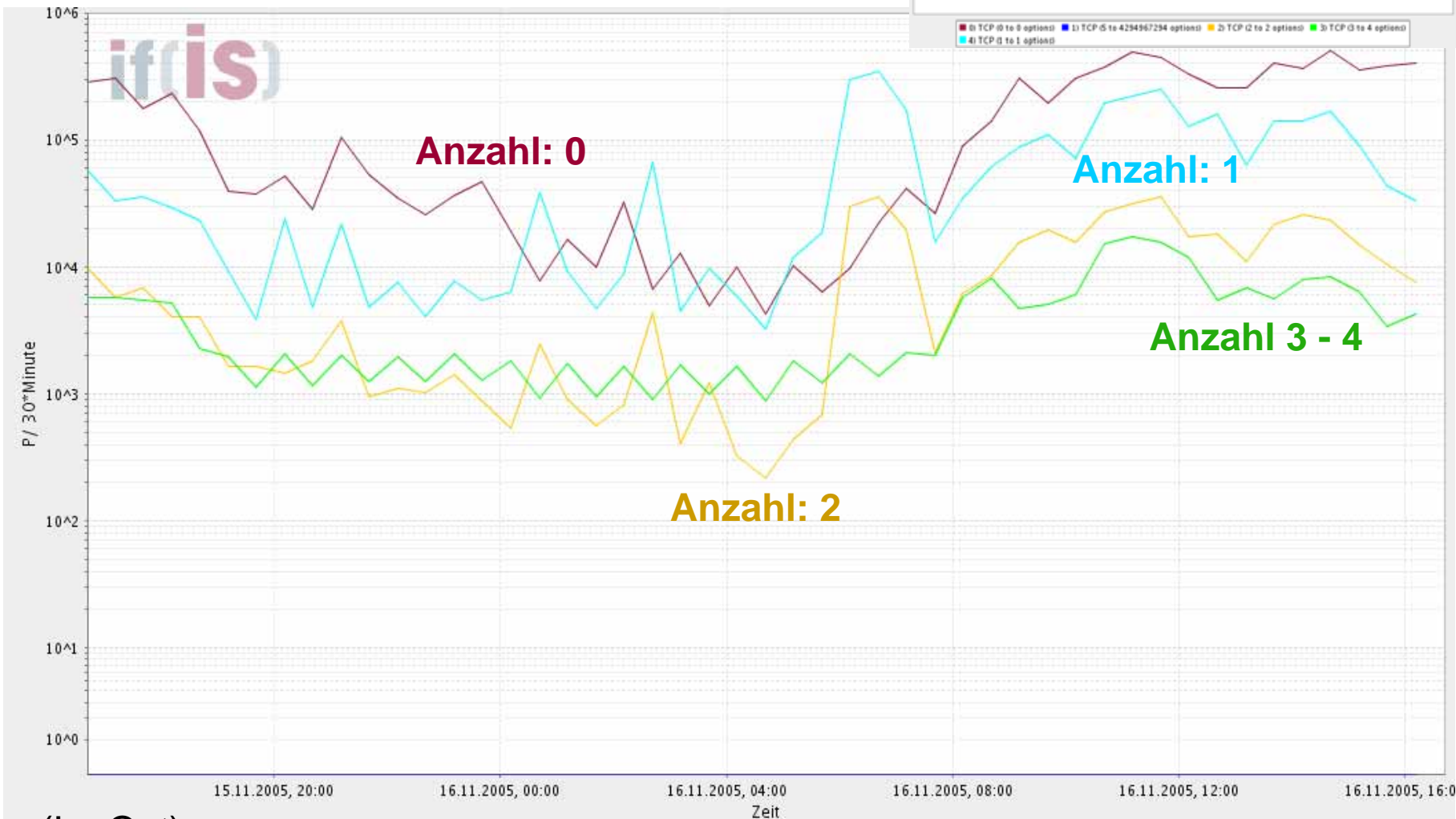
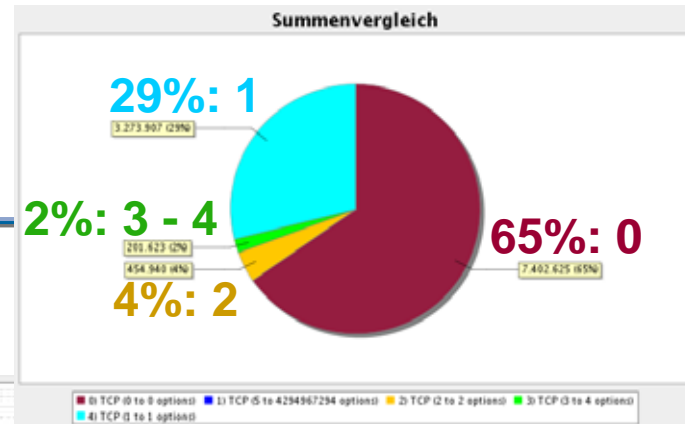
IAS: FB Informatik

→ Option: MSS



IAS: FB Informatik

→ Option (Anzahl)



(In+Out)

0 TCP (0 to 0 options) 1 TCP (5 to 4294967294 options) 2 TCP (2 to 2 options) 3 TCP (3 to 4 options) 4 TCP (1 to 1 options)

Hypertext Transfer Protocol (HTTP)

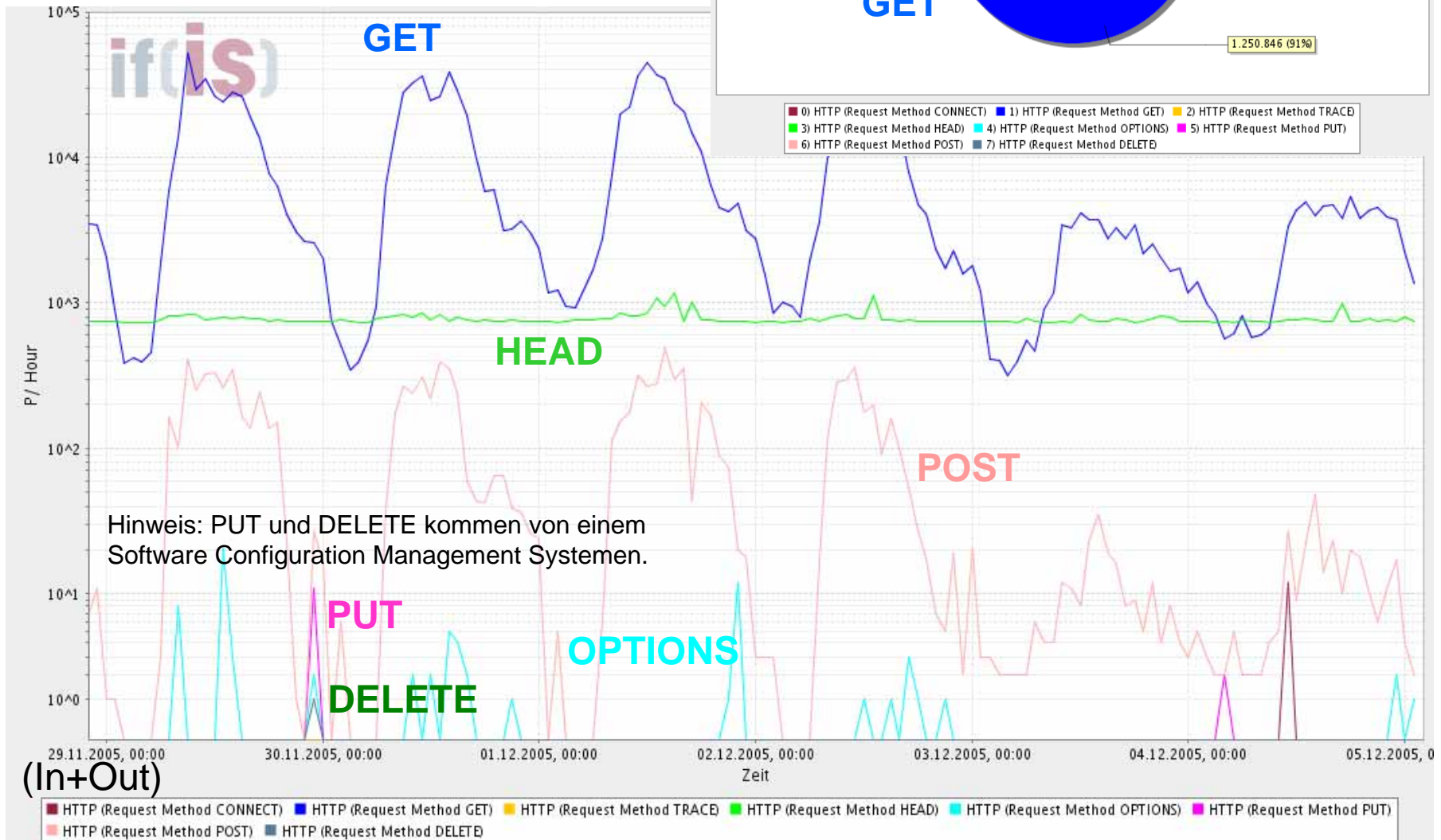
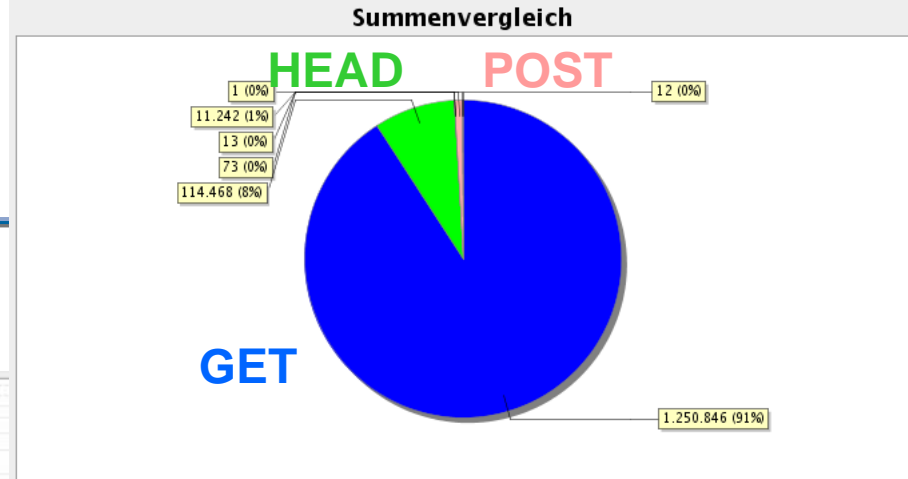
→ HTTP-Methoden - Überblick

- HTTP wurde als allgemeines Client-Server-Protokoll entwickelt, um Dokumente in beide Richtungen übertragen zu können.
- Ein Client kann jede Methode oder Operation, die auf dem Server ausgeführt werden soll, anfordern, indem er eine Anforderungsnachricht mit der gewünschten Operation an den Server sendet.
- Liste der gebräuchlichsten Anforderungsnachrichten:

Operationen	Beschreibung
Head	Anforderung, den Header eines Dokuments zurückzugeben
Get	Anforderung, ein Dokument an den Client zurückzugeben
Put	Anforderung, ein Dokument zu speichern
Post	Bereitstellung von Daten, die einem Dokument hinzugefügt werden sollen
Delete	Anforderung, ein Dokument zu löschen
Trace	Anforderung, eine Anfrage aus "Trace"-Gründen sofort zurückzusenden
Connect	Für zukünftige Einsatzzwecke reserviert
Options	Anforderung, Eigenschaften des Servers und Dokumente abzufragen

IAS: FB Informatik

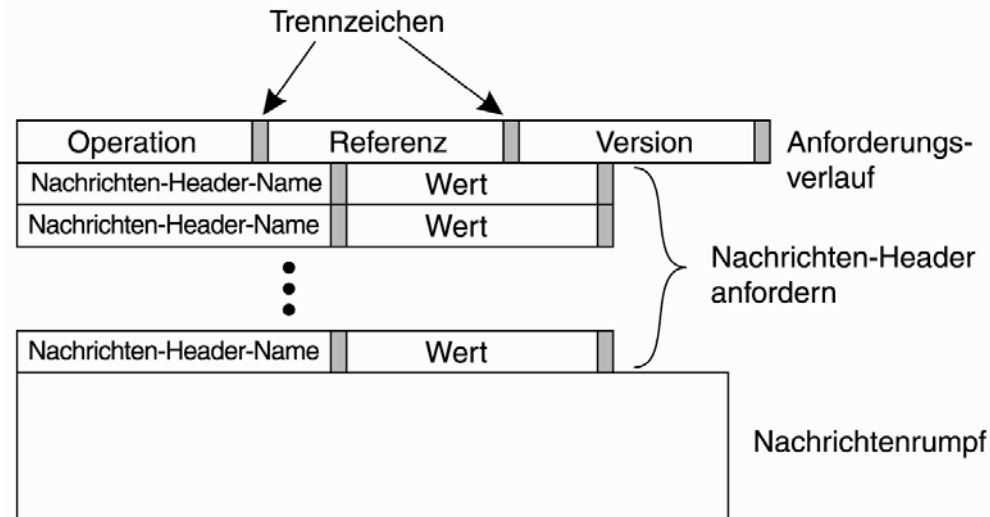
→ HTTP-Methoden



Hypertext Transfer Protocol (HTTP)

→ HTTP-Nachrichten - Aufbau der Anforderung (1/2)

- Die gesamte Kommunikation zwischen Client und einem Server findet über Nachrichten statt.
- HTTP kennt nur **Anforderungs- und Antwortnachrichten**.
- Eine Anforderungsnachricht besteht aus drei Teilen:



- **Anforderungsverlauf / Anforderungszeile:**
- **Nachrichten-Header:** Zusatzinformationen, die zwischen Client und Server ausgetauscht werden
- **Nachrichtenrumpf:** das eigentliche Dokument (z.B. PUT u. POST) in einem definierten Format

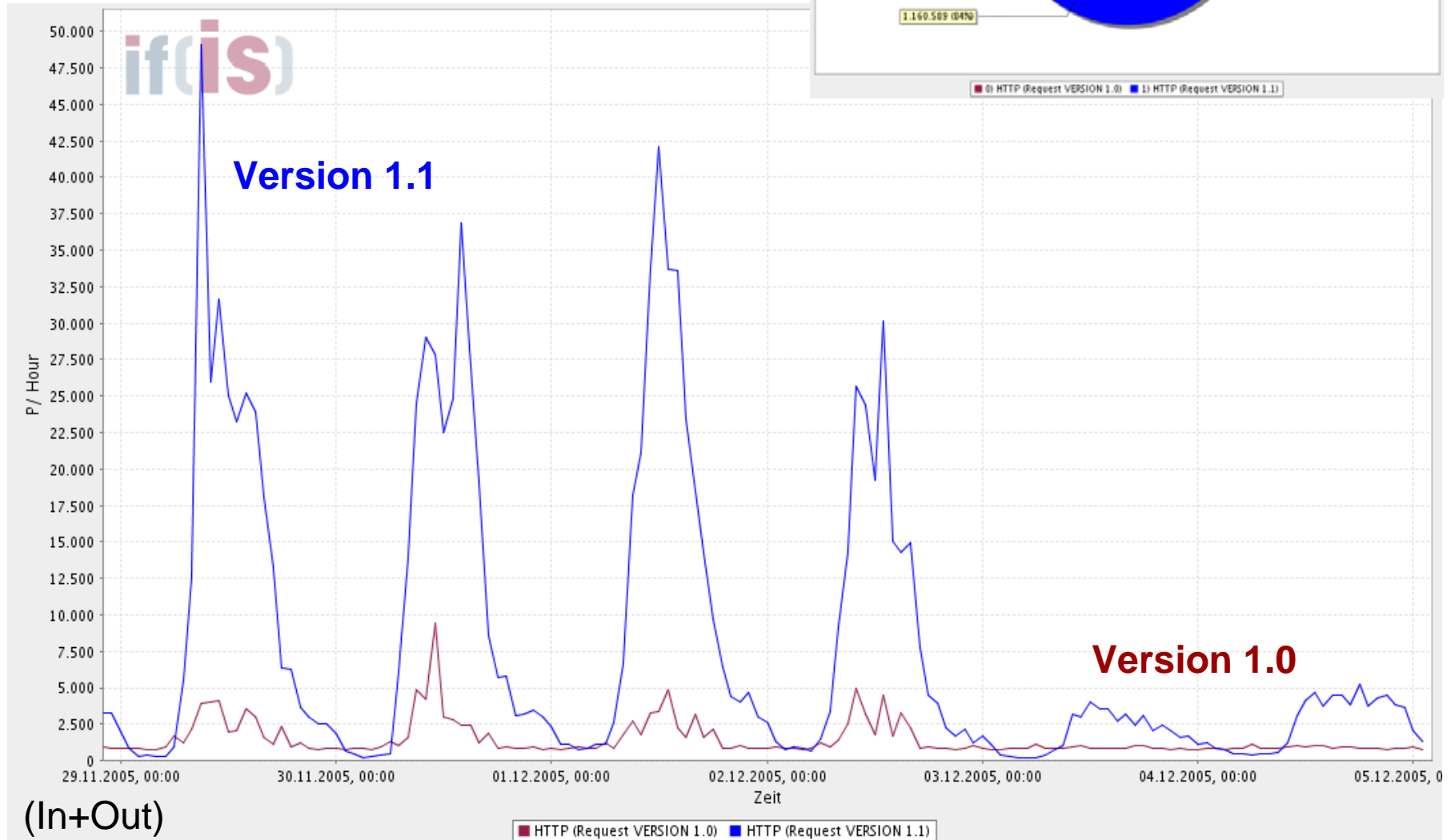
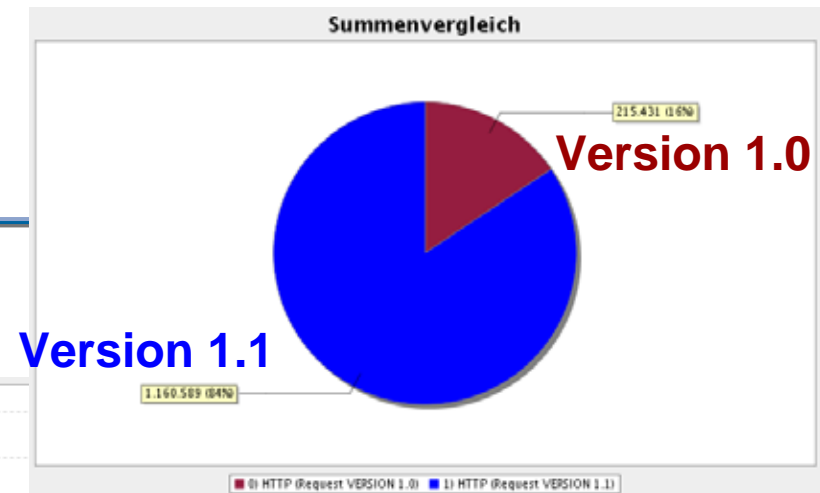
Hypertext Transfer Protocol (HTTP)

→ HTTP-Nachrichten - Aufbau der Anforderung (1/2)

- Die Anforderungszeile (Anforderungsverlauf) ist zwingend erforderlich und identifiziert die Operation, die der Client vom Server anfordert, zusammen mit einer Referenz auf das Dokument, das dieser Anforderung zugeordnet ist.
- Ein weiteres Feld wird verwendet, um die HTTP-Version zu identifizieren, die der Client erwartet.
- Anforderungszeile (Anforderungsverlauf)
 - Operation oder Methode: z.B. **GET**
 - Referenz (URL): z.B. **skripte.informatik.fh.gelsenkirchen.de**
 - Version: z.B. **HTTP 1.1**

IAS: FB Informatik

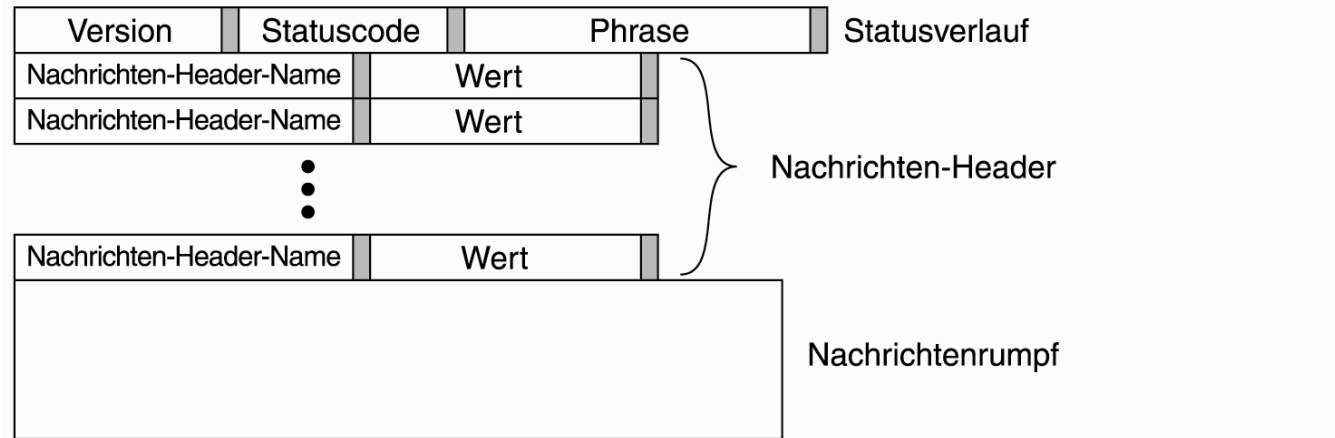
→ HTTP-Methoden



Hypertext Transfer Protocol (HTTP)

→ HTTP-Nachrichten : Aufbau der Antwortnachricht (1/2)

- Eine Antwortnachricht beginnt mit einer Statuszeile, die eine Versionsnummer sowie einen dreistelligen Statuscode enthält.



- **Statusverlauf:**
- **Nachrichten-Header:** Zusatzinformationen, die zwischen Client und Server ausgetauscht werden
- **Nachrichtenrumpf:** das eigentliche Dokument (z.B. GET) in einem definierten Format

Hypertext Transfer Protocol (HTTP)

→ HTTP-Nachrichten : Aufbau der Antwortnachricht (2/2)

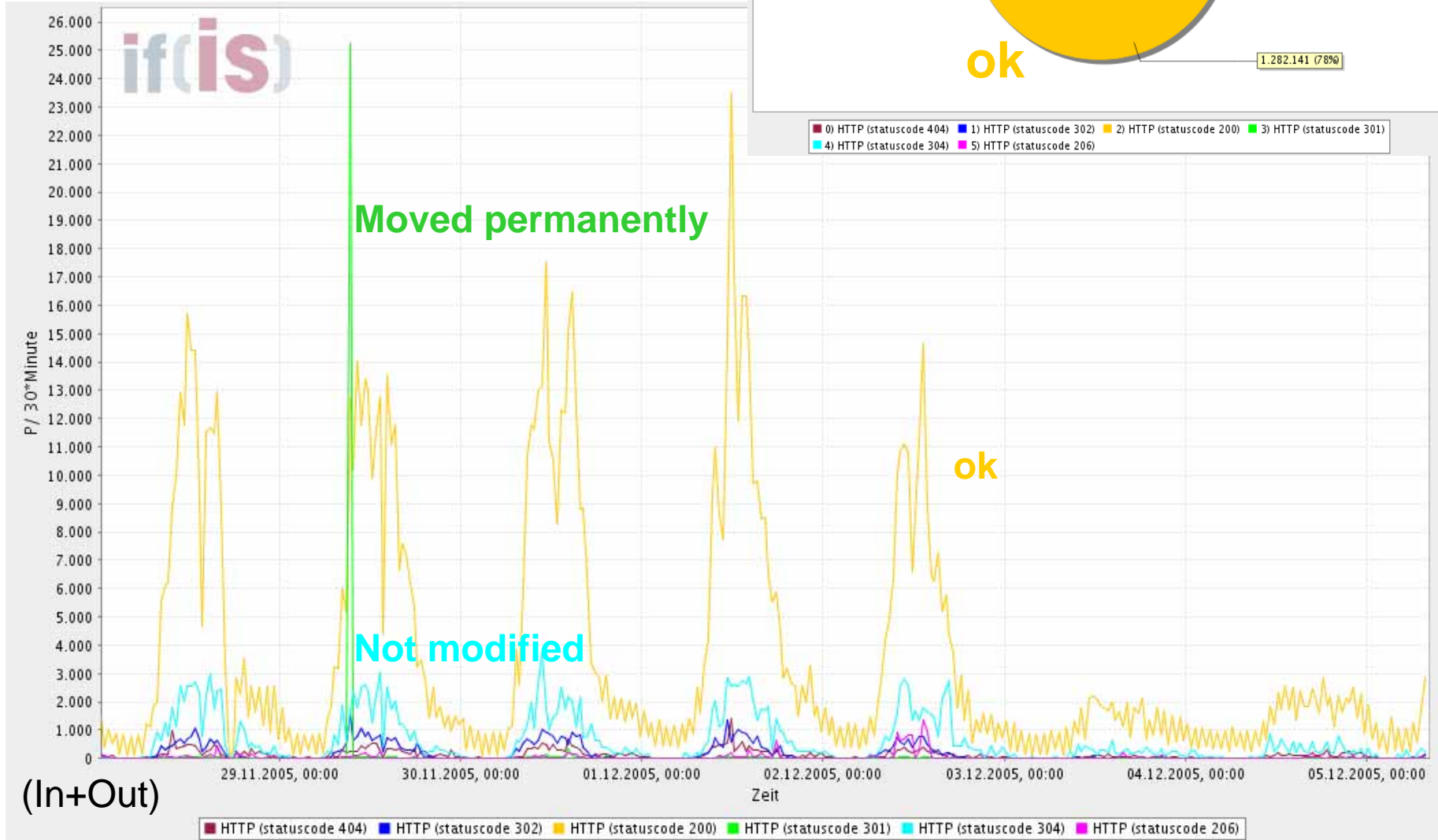
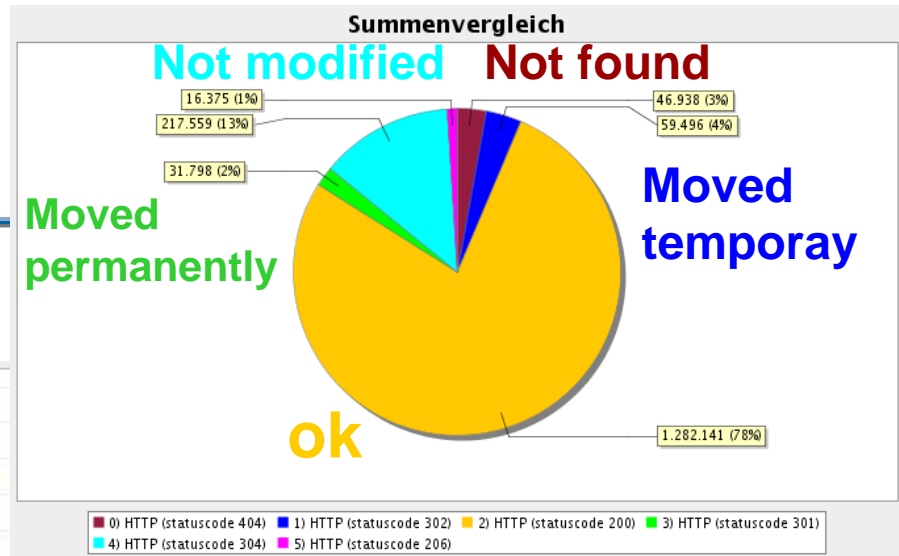
- Der Statusverlauf besteht aus:
 - Version: z.B. **HTTP 1.1**
 - Statuscode: z.B. **200** (*Erfolgreiche Anforderung*)
 - Phrase: z.B. **OK** oder NOT OK (*Beschreibung des Statuscodes*)

- Die Bedeutung der Statuscodes:

Code	Bedeutung	Beispiel
1xx	Information	100 = Server stimmt zu, die Anforderung des Client zu bearbeiten
2xx	Erfolg	200 = ok; 204 = kein Inhalt vorhanden
3xx	Umleitung	301 = Seite verzogen; 304 = Seite im Cache noch gültig
4xx	Client-Fehler	403 = verbotene Seite; 404 = Seite nicht gefunden; 405 = Opera. nicht erlaubt
5xx	Server-Fehler	500 = interner Server-Fehler; 503 = versuch es später noch einmal

IAS: FB Informatik

→ HTTP-Statuscode



(In+Out)

Hypertext Transfer Protocol (HTTP)

→ HTTP-Nachrichten : Header (1/2)

Header	Quelle	Inhalt
Accept	Client	Der Typ der Dokumente, die der Client verarbeiten kann
Accept-Charset	Client	Die für den Client erlaubten Zeichensätze
Accept-Encoding	Client	Die für den Client erlaubten Dokumentenkodierung
Accept-Language	Client	Die natürliche Sprache, die der Client verarbeiten kann
Accept-Ranges	Server	Der Server akzeptiert Byte-Bereichsanfragen
Authorization	Client	Liste der Berechtigungen des Clients
Cookie	Client	Sendet ein zuvor gesendetes Cookie an den Server zurück
Connection	Beide	Erlaubt Client und Server Info über den gewünschten Verbindungszustand
Content-Encoding	Server	Wie der Inhalt des Dokumentes kodiert ist (z.B. gzip)
Content-Language	Server	Natürliche Sprache des Dokumentes
Content-Length	Server	Seitenlänge in Byte
Content-Type	Server	MIME-Type des Dokumentes
Date	Beide	Datum und Zeit der gesendeten Nachricht
ETtag	Server	Die dem zurückgegebenen Dokument zugeordneten Tags
Expires	Server	Die Zeit, wie lange die Antwort gültig bleibt
From	Client	E-Mail-Adresse des Clients

Hypertext Transfer Protocol (HTTP)

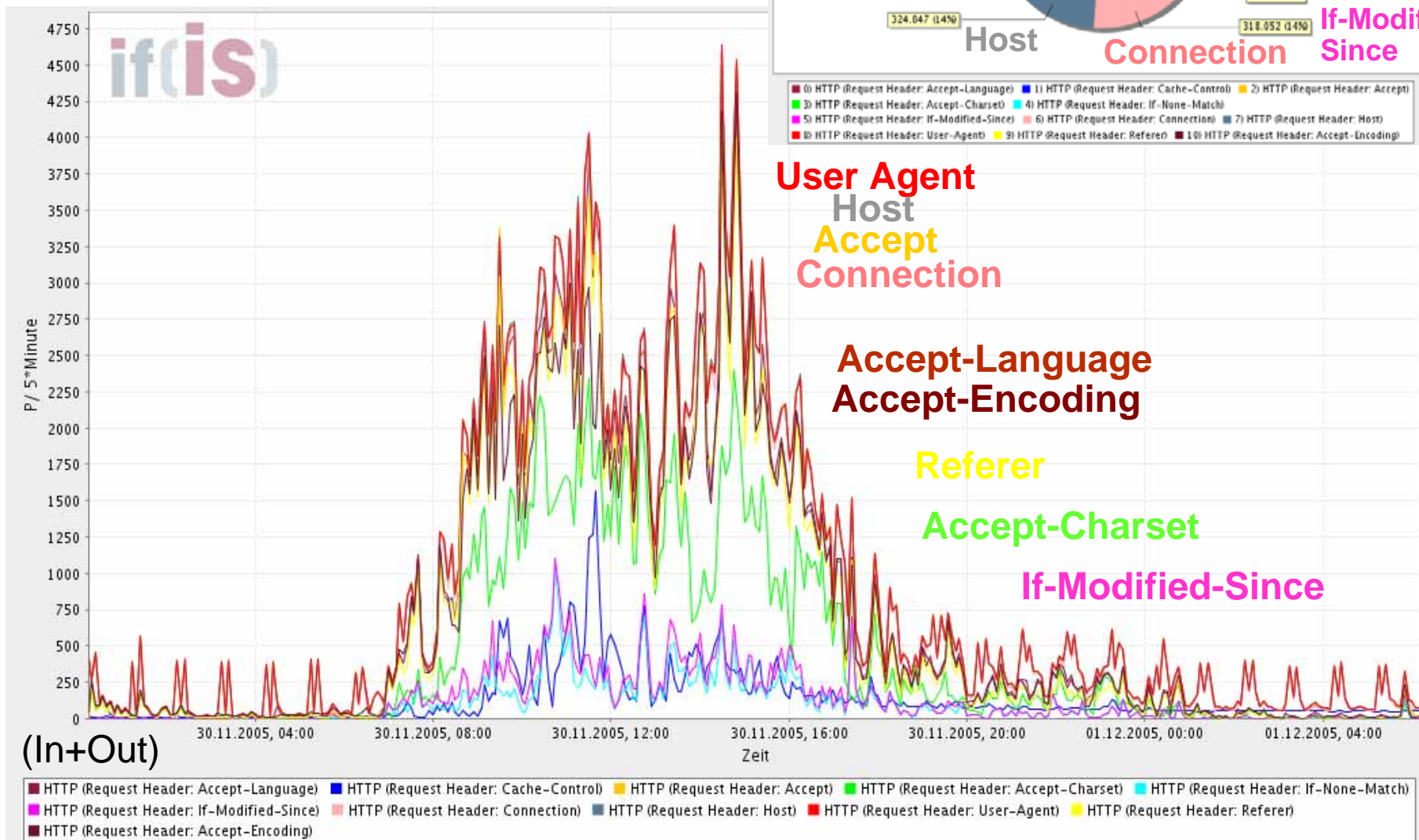
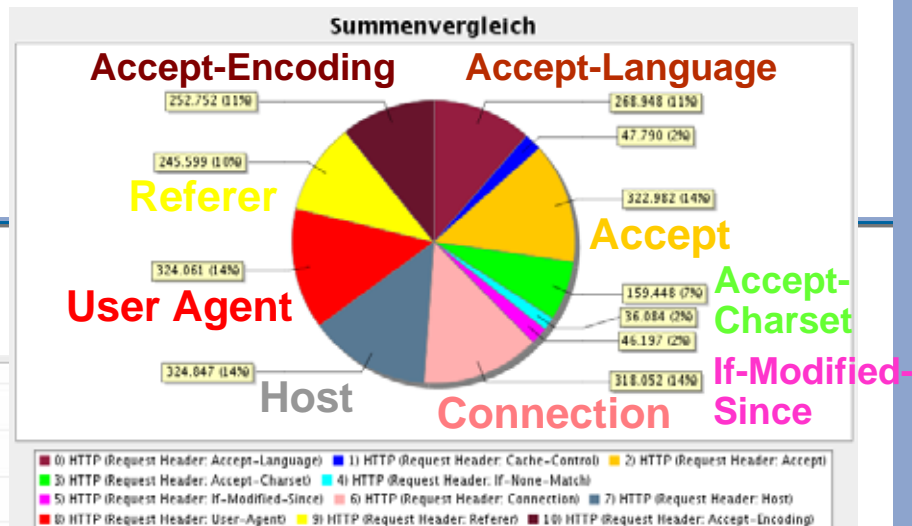
→ HTTP-Nachrichten : Header (2/2)

Header	Quelle	Inhalt
Host	Client	DNS-Name des Web-Servers
If-Mach	Client	Die Tags, die das Dokument haben sollte
If-None-Match	Client	Die Tags, die das Dokument nicht haben sollte
If-Modified-Since	Client	Weist den Server an, ein Dokument nur dann zurückzugeben, wenn es seit der angegebenen Zeit verändert wurde.
If-Unmodified-Since	Client	Weist den Server an, ein Dokument nur dann zurückzugeben, wenn es seit der angegebenen Zeit nicht verändert wurde.
LastModified	Server	Die Zeit, wann das zurückgegebene Dokument zuletzt verändert wurde
Location	Server	Eine Dokumentenreferenz, an die der Client seine Anforderung umleiten soll
Max-Forward	Client	Bestimmt die max. Anzahl von Hops die zwischen Client und Server zulässig sind
Referer	Client	Verweist auf das vom Client zuletzt angeforderte Dokument
Server	Server	Informationen über den Server
Set-Cookie	Server	Der Server möchte, dass der Client ein Cookie speichert
Upgrade	Beide	Das Applikationsprotokoll, zu dem der Sender wechseln will
User-Agent	Client	Informationen über den Browser und dessen Plattform
Warning	Beide	Informationen über den Status der Daten in der Nachricht
WWW-Authenticate	Server	Sicherheitsanforderung, auf die der Client antworten soll

IAS: FB Informatik

→ HTTP-Header

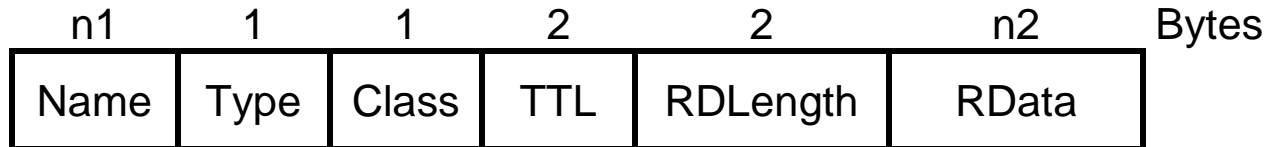
Hinweis: Es kommen alle Header vor, hier nur größer als 2 %.



Domain Name System (DNS)

→ Aufbau von DNS: Aufbau eines Resource Record (4/5)

- **Resource Records**, die im Name-Server gespeichert sind, bestehen aus insgesamt sechs Feldern.



Bezeichnung	Inhalt	
Name	Das Feld enthält den Namen der Domäne, der diesem Resource Record zugeordnet ist.	
Type	Das Zwei-Byte-Feld gibt den Type des Resource Record an.	
	A	Type = 1 RData enthält die zu "Namen" gehörende IP-Adresse
	NS	Type = 2 (NS = Name Server) RData enthält den Domänennamen des für "Name" zuständigen Domänenservers.
	CNAME	Type = 5 (CNAME = Canonical Name, kanonischer Name) RData enthält den Namen zu "Namen" (Aliasname)
	SOA	Type = 6 (SOA = Start Of Area, Anfrag der Zone) RData gibt den Anfang einer Zone an.
	PTR	Type = 12 (PTR = Pointer, Zeiger) RData enthält einen Zeiger auf eine IP-Adresse für das Reverse Mapping
	HINFO	Type = 13 (HINFO = Host Information) RData enthält eine ID für die Hardware und das Betriebssystem von "Name"
	MX	Type = 15 (MX = Mail Exchange) RData enthält den Domänennamen eines für "Name" zuständigen E-Mail Servers.
	TXT	Type = 16 Rdata enthält einen in doppelten Anführungszeichen eingeschlossenen Text.

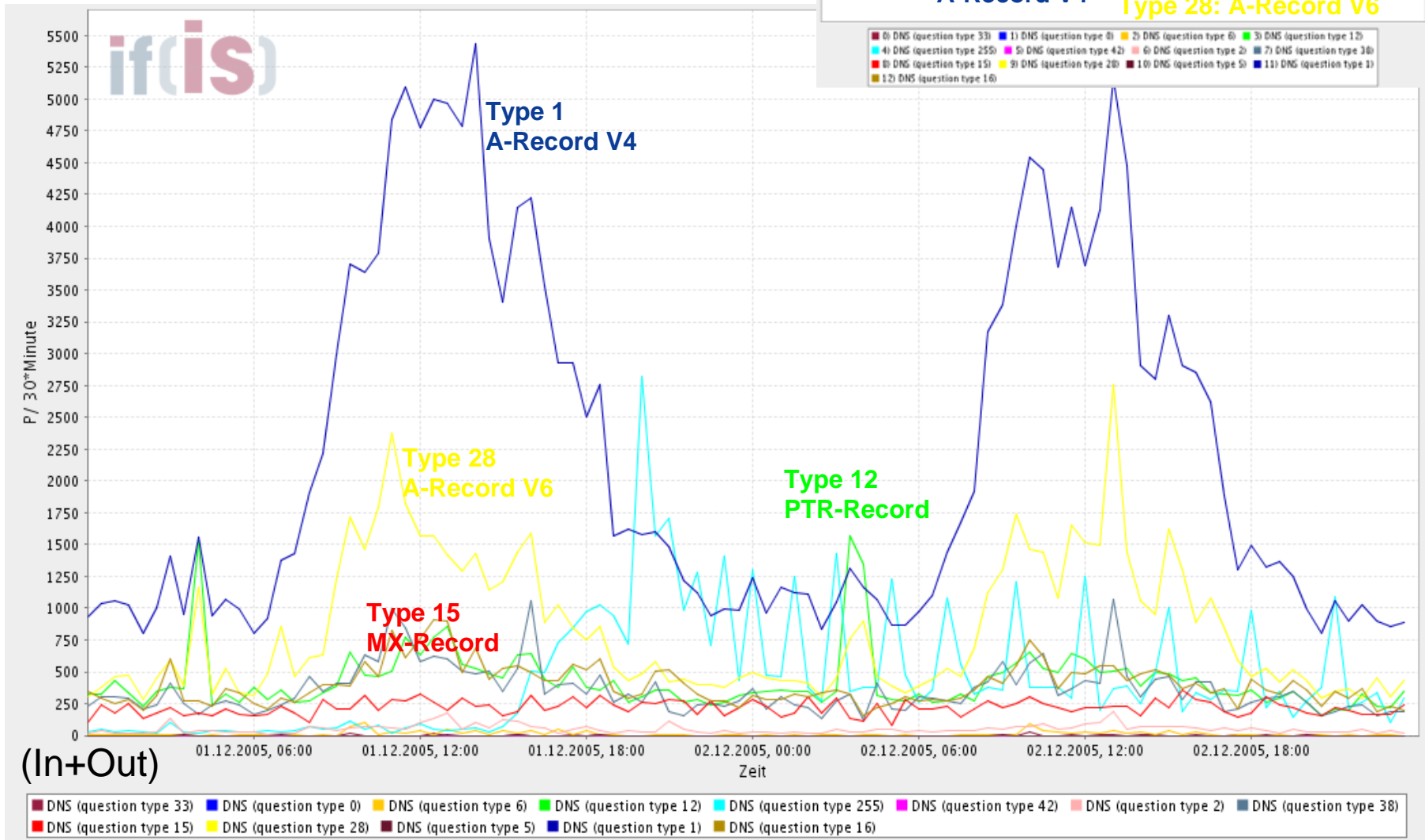
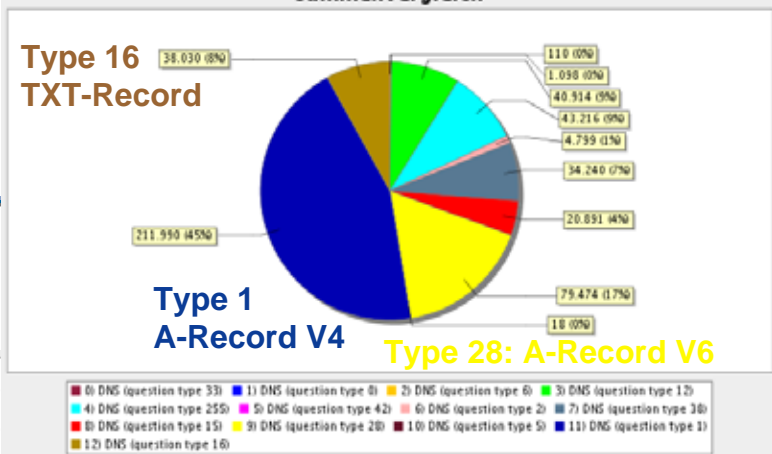
Domain Name System (DNS)

→ Aufbau von DNS: Aufbau eines Resource Record (5/5)

Bezeichnung	Inhalt	
Class	Mit diesem Zwei-Byte-Wert wird die Protokollfamilie beschrieben.	
	IN	Internet, Class = 1
	CS	CSNET, Class = 2
	CH	CHAOSnet, Class = 3
	HS	Hesiod, Class = 4
TTL	Mit diesem Vier-Byte-Wert wird die Anzahl Sekunden festgelegt, die ein Resolver den Resource Record in seinem Cache hält, bevor er ihn löscht und/oder eine Aktualisierung durchführt. TTL ist die Abkürzung für Time To Live.	
RDLenght	Dieser Zwei-Byte-Wert gibt die Länge des Felds RData in Byte an	
Rdata	Längenvariantes Feld, das abhängig von den Eintragungen in einigen der zuvor beschriebenen Felder unterschiedlich zu interpretierende Daten enthält.	

IAS: FB Informatik

→ Type



Internet-Analyse-System
→ Beispiele

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

norbert.pohlmann@informatik.fh-gelsenkirchen.de

