

DAIMLERCHRYSLER

Sicherung von Web Services durch Firewalls

Mario Jeckle, Barbara Zengler
DaimlerChrysler Forschungszentrum Ulm
{mario.jeckle, barbara.zengler}@daimlerchrysler.com
www.jeckle.de

Gliederung

Kommunikation im Internet

- Grundidee
- Technik
- Protokolle

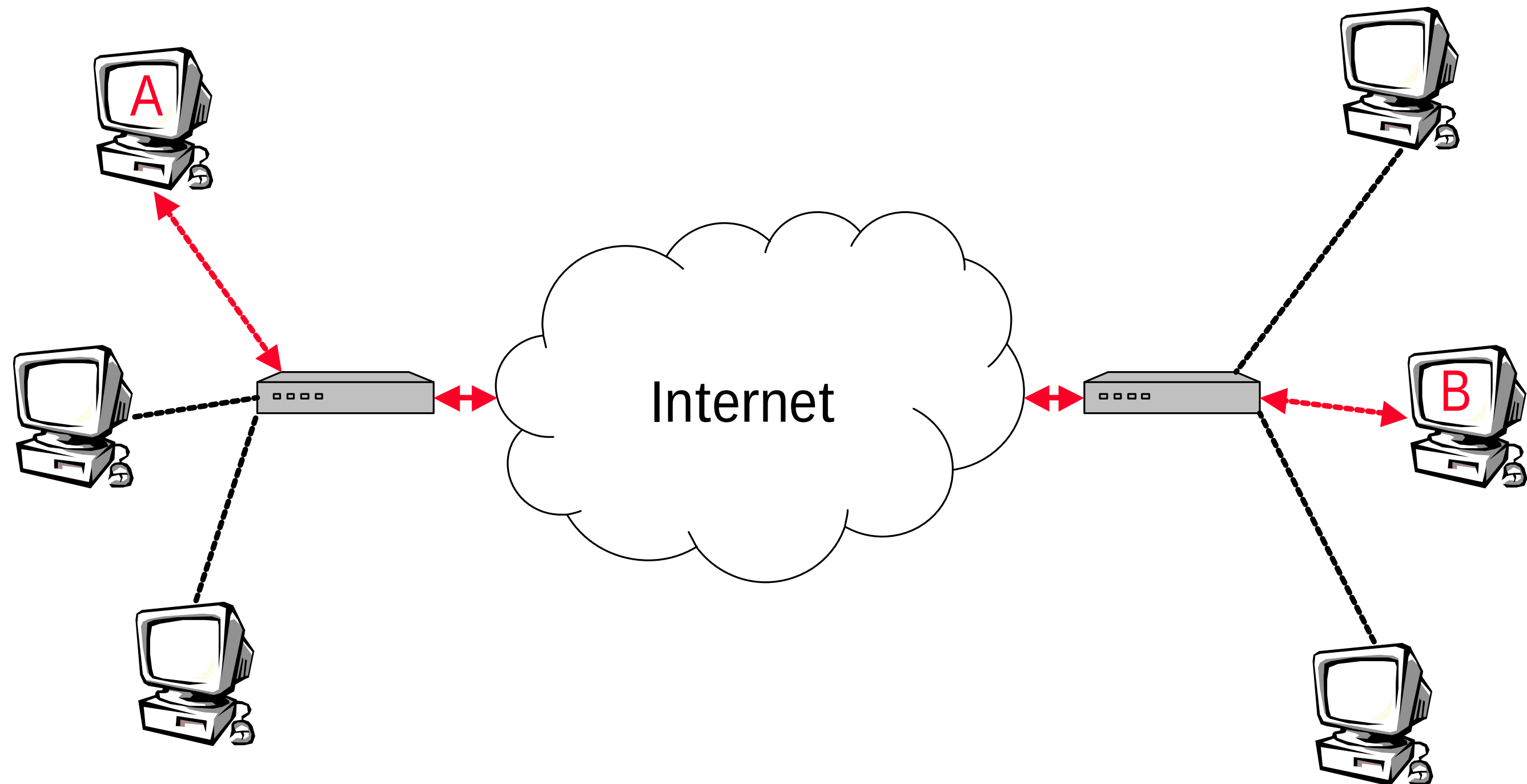
Web Services

- SOAP
- Beschreibungsmodell
- Implementierung und Ausführungsmodell

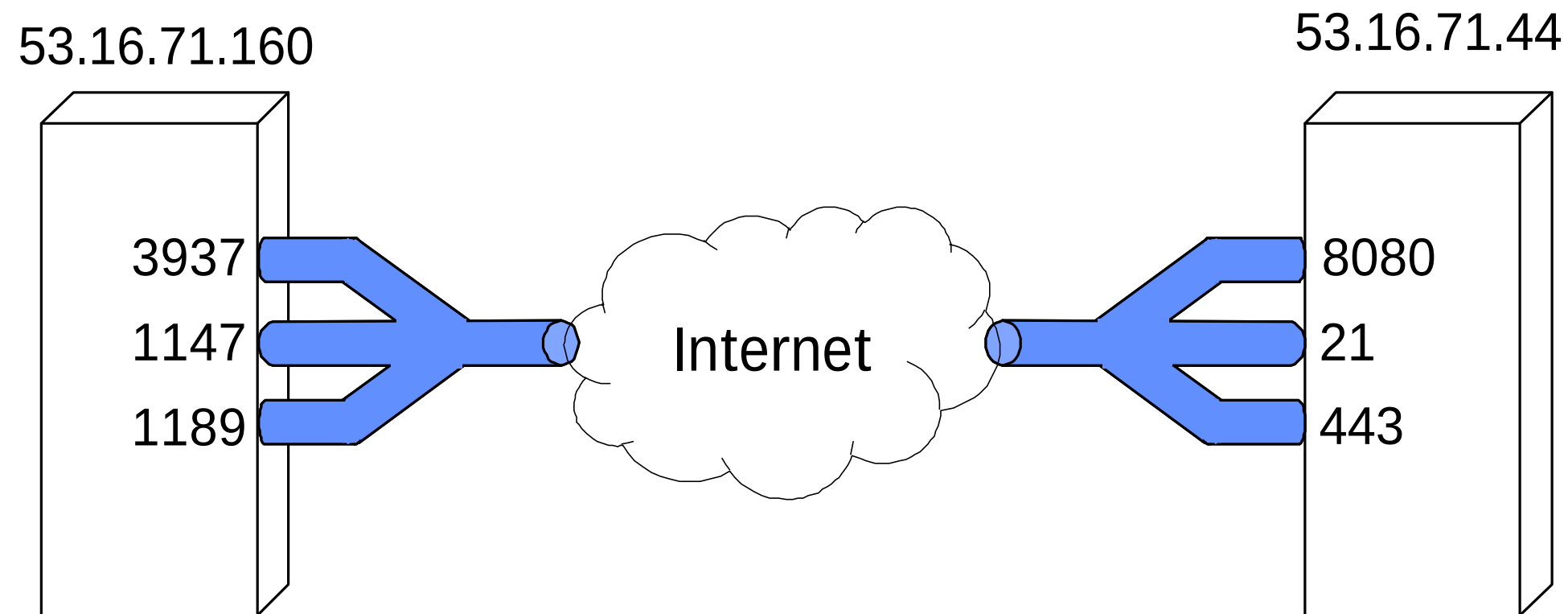
Firewalls

- Grundidee
- Klassische Ansätze
- „SOAP-Firewalls“

Kommunikation im Internet - Grundprinzip



Kommunikation im Internet - Funktionsweise



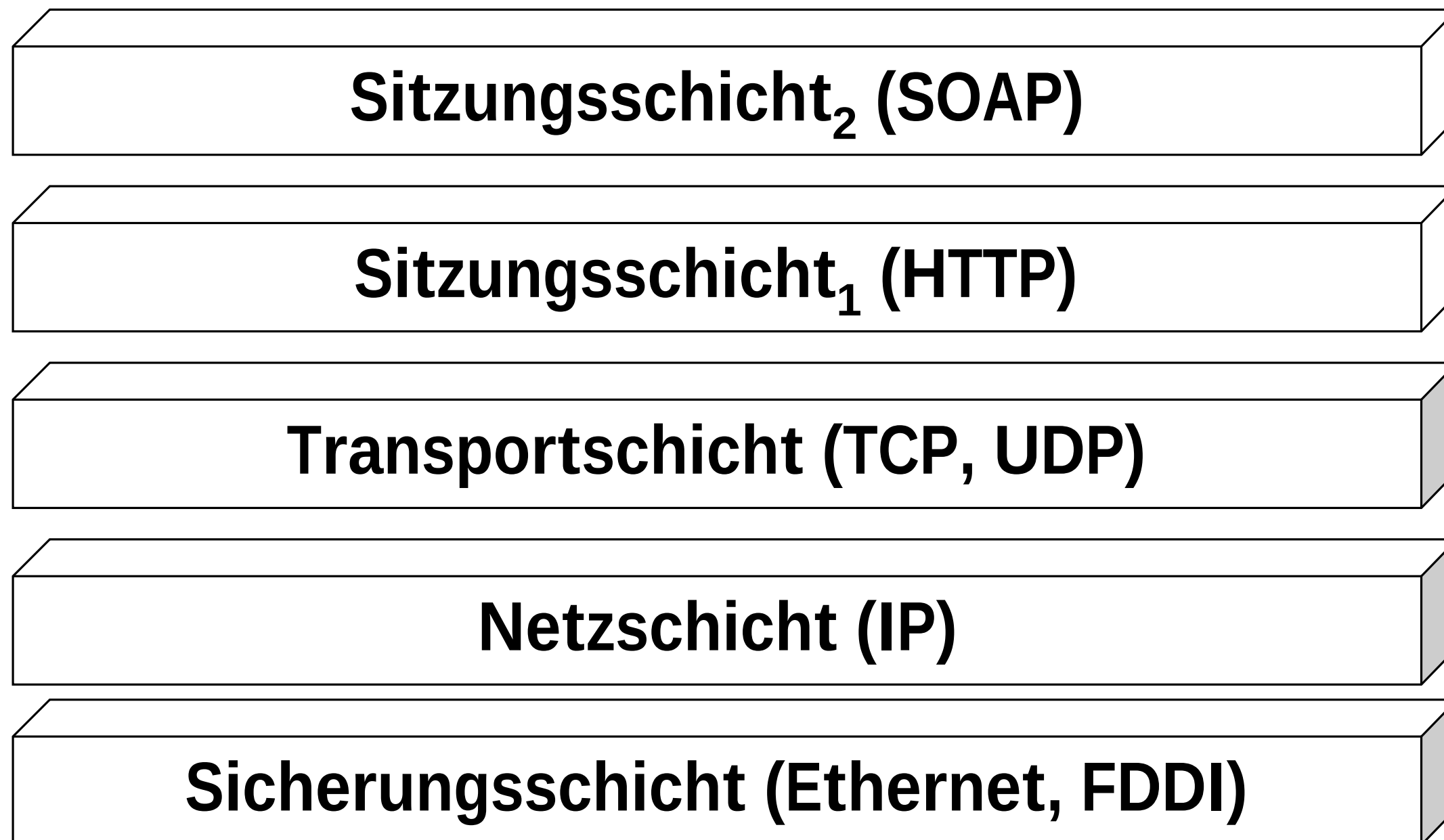
Adressierung

- Rechner: IP Adresse (IP Protokoll)
- Applikation: Port (TCP bzw. UDP Protokoll)

Port:

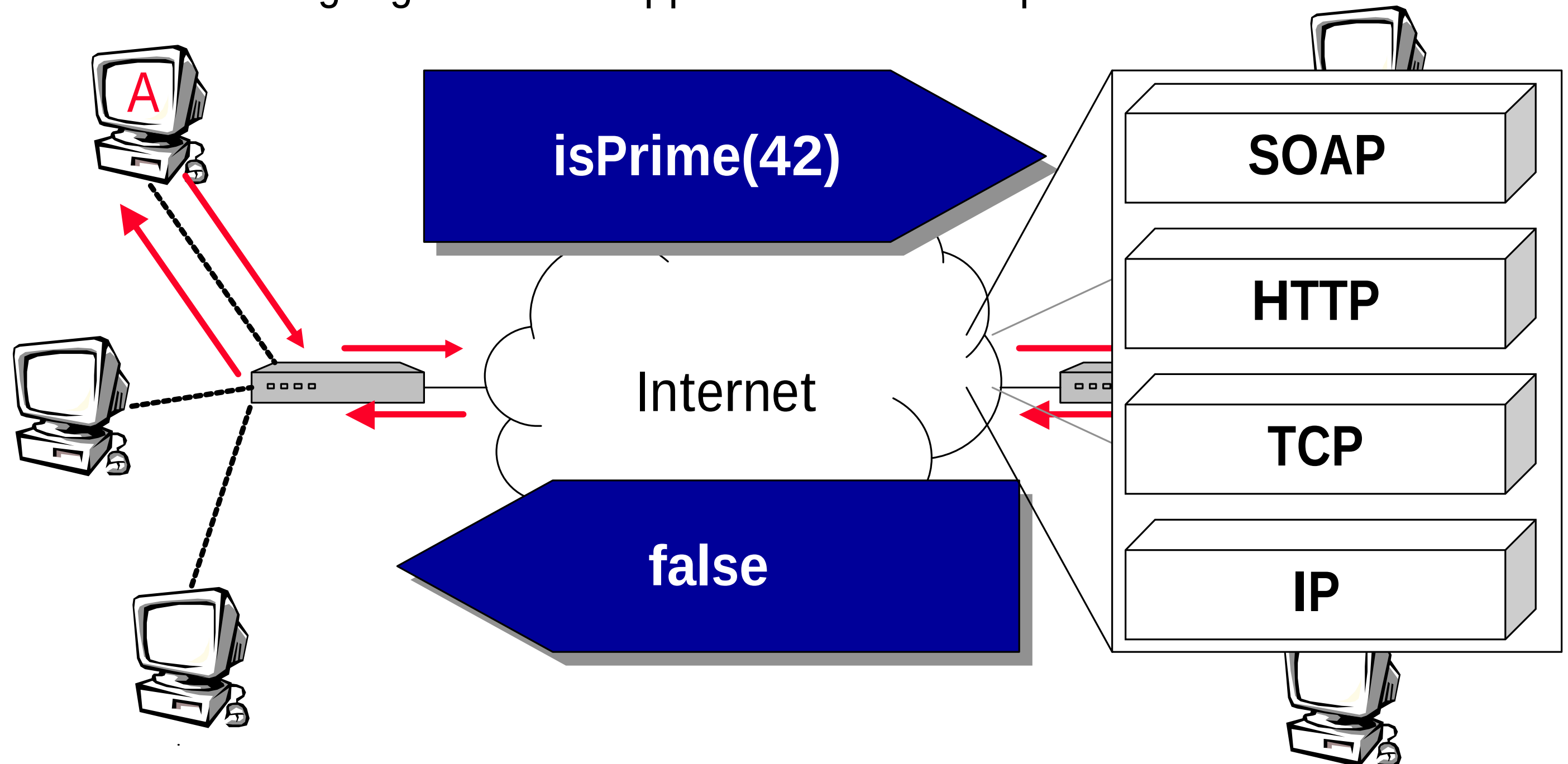
- logische Verbindung zwischen Client und Server Programmen
- Unterscheidung mehrere logischer Kanäle auf gleichem Netzwerk Interface auf selbem Computer
- Server Software „bindet“ an (assoziiert sich mit) zugewiesenen Port

Kommunikation im Internet - Protokollstack



Kommunikation im Internet

- Datenübertragung zwischen Applikationen -- Beispielszenario



Exkurs: Das SOAP v1.2 Protokoll

- Grundidee: Entfernte Funktionsaufrufe und Nachrichtenaustausch mit XML
- Zumeist
 - HTTP als Kommunikationsprotokoll
 - Synchrone Aufrufe
 - RPC-Style
- Version 1.2 durch die W3C-Arbeitsgruppe „XML Protocol“ erarbeitet
- Breit unterstützt
- Bereits in ersten (einsetzbaren) Implementierungen verfügbar
- Aufbau:
 - SOAP Part 0: Einführendes (nicht-normatives Dokument)
 - SOAP Part 1: Rahmenwerk zur Konstruktion einer SOAP-Nachricht
 - SOAP Part 2: Konkrete Nutzung des Rahmenwerks, beispielsweise für RPCs über HTTP

Exkurs: Das SOAP v1.2 Protokoll -- struktureller Aufbau

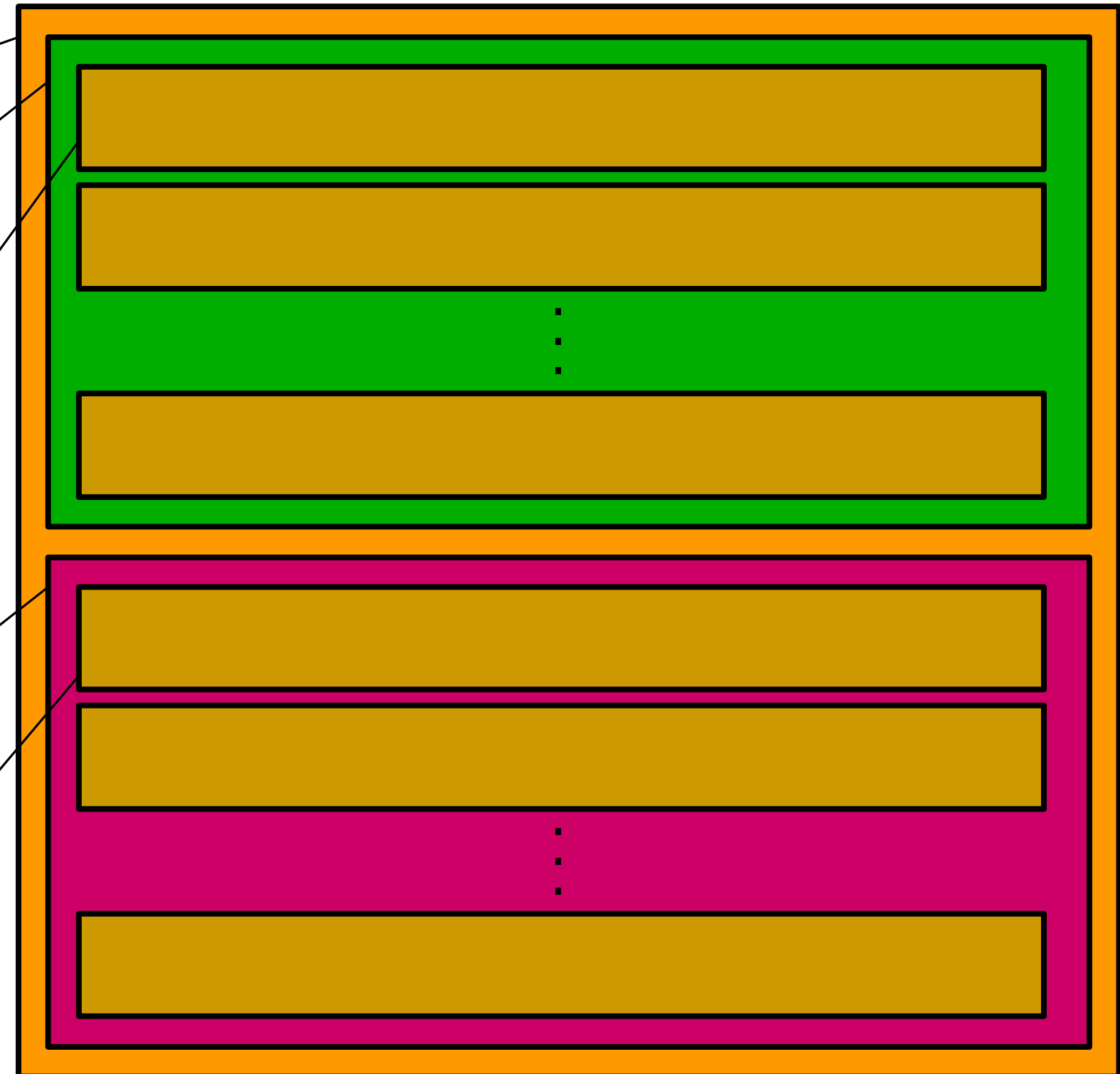
SOAP-Nachricht

SOAP-Header

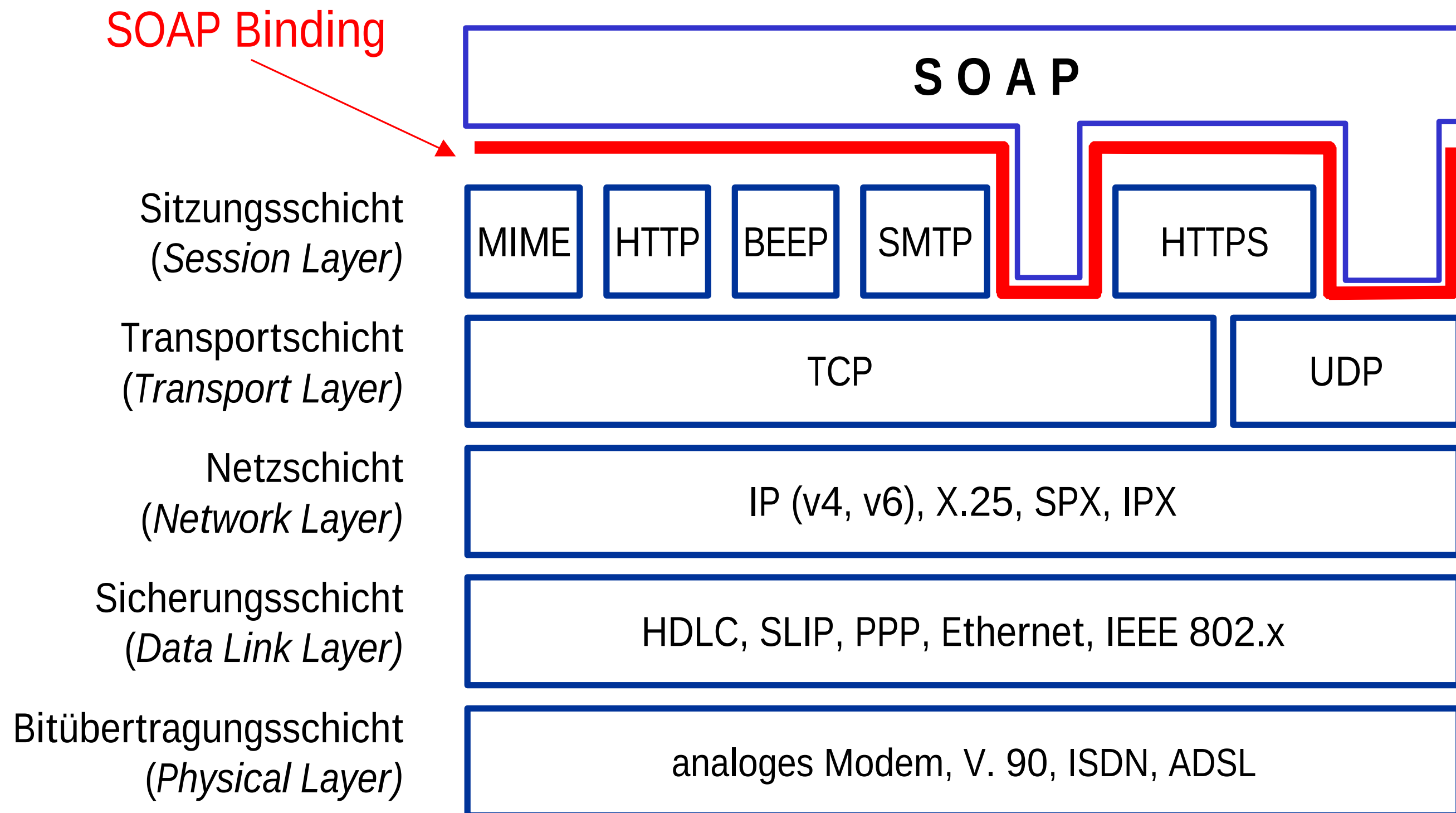
SOAP-Block

SOAP-Body

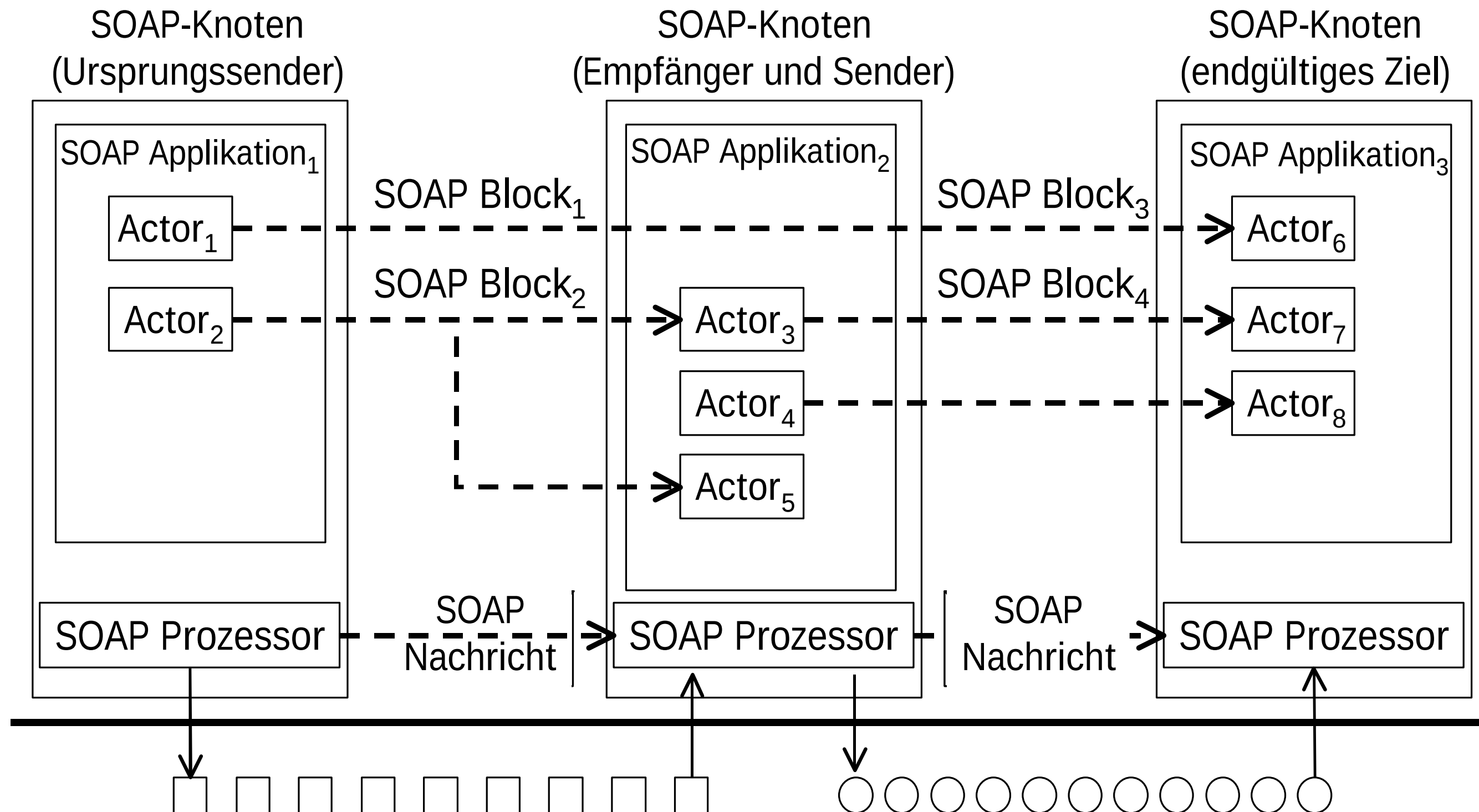
SOAP-Block



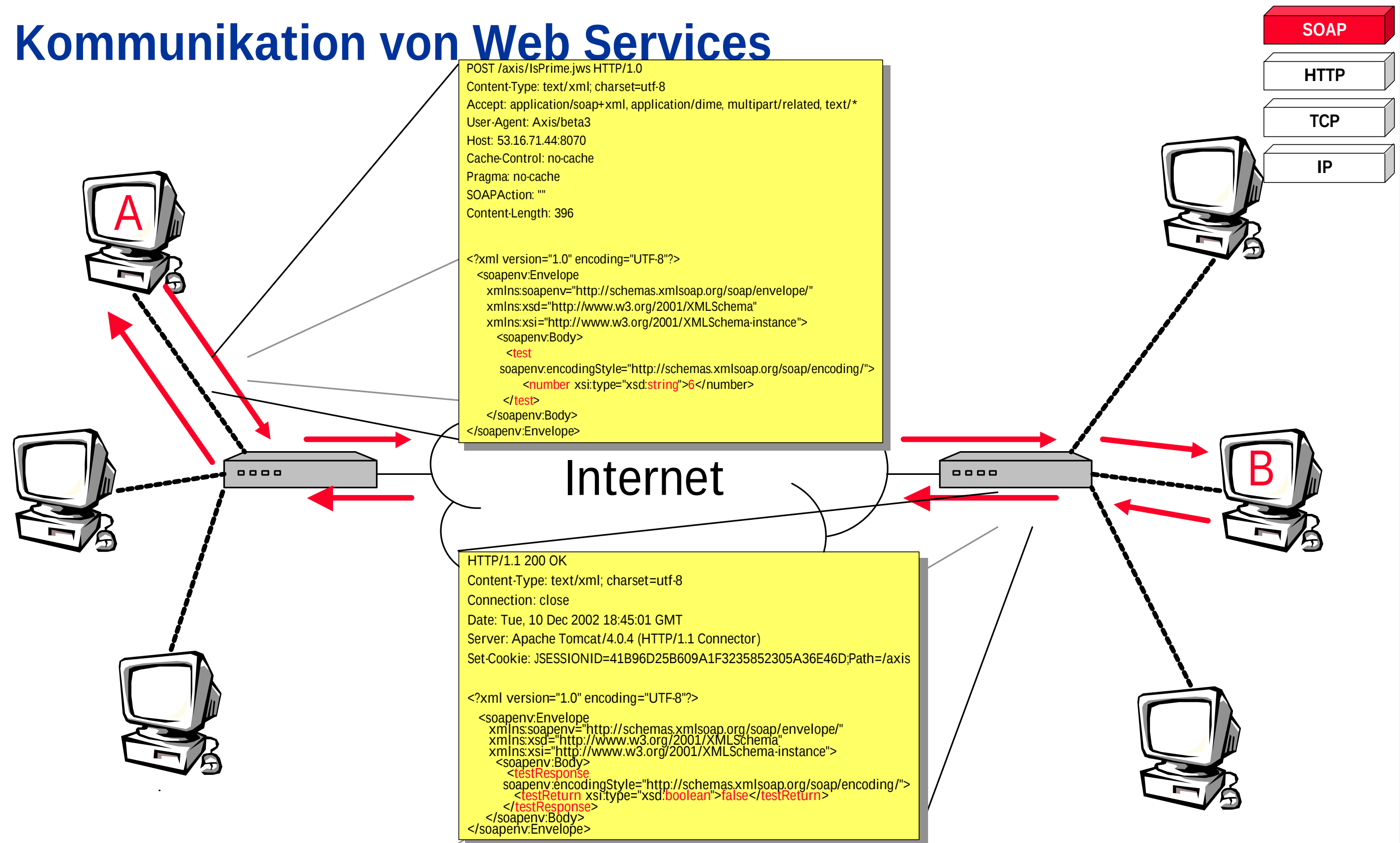
Exkurs: Das SOAP v1.2 Protokoll -- Protokollunabhängigkeit



Exkurs: Das SOAP v1.2 Protokoll --- Intermediäre

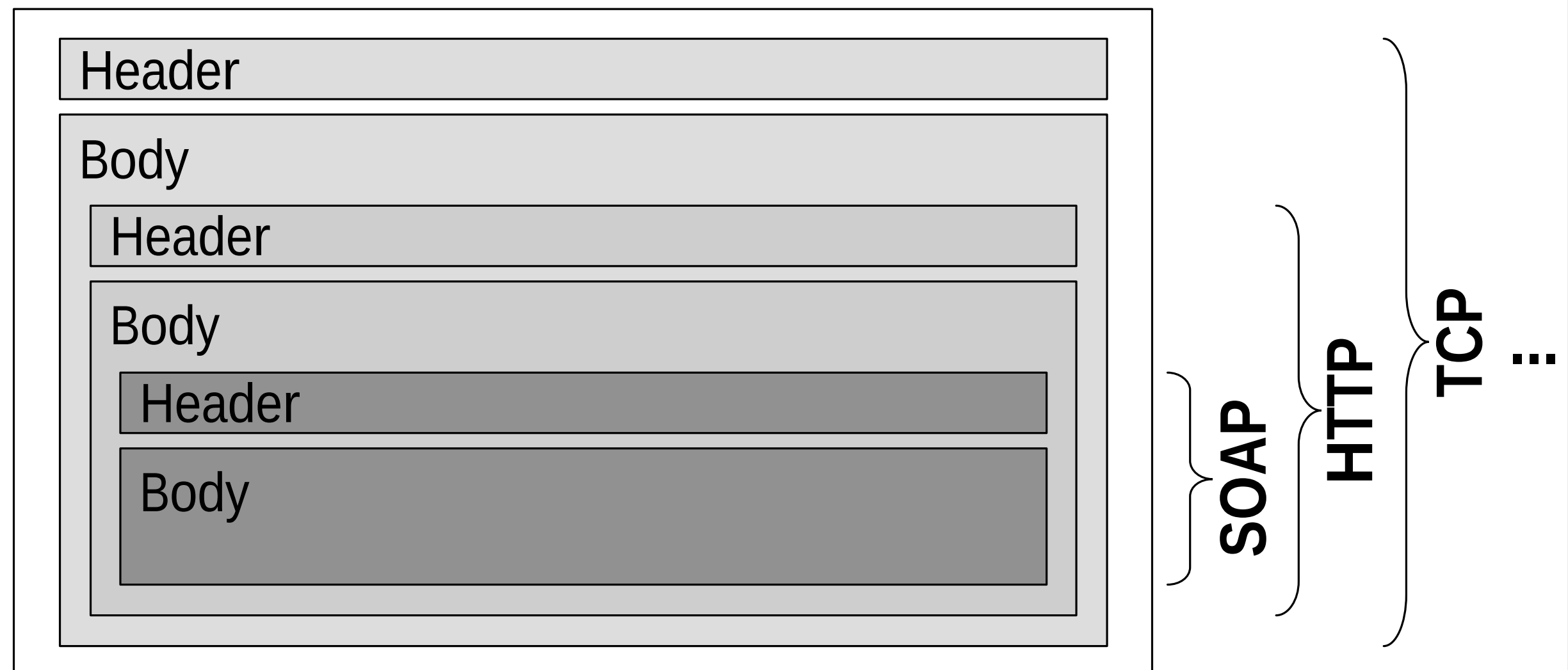
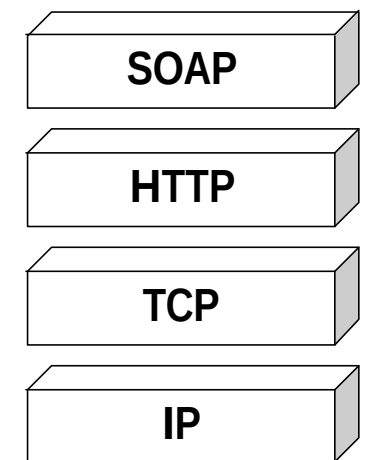


Kommunikation von Web Services



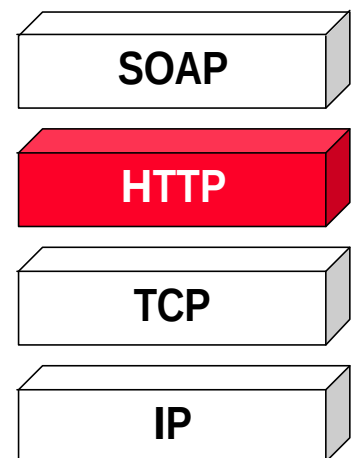
Kommunikation im Internet – Protokolle

- Datenübertragung zwischen Applikationen
- Datenpaket
 - Header: Protokollspezifische Information
 - Body: Nutzdaten



Kommunikation Im Internet – Protokolle

- Anwendungsschicht
 - HyperText Transfer Protocol HTTP, SOAP v1.1-Anfrage

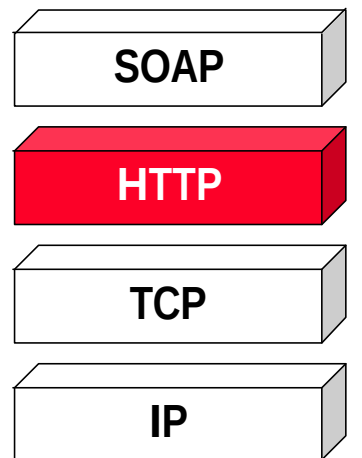


```
POST /axis/IsPrime.jws HTTP/1.0  
Content-Type: text/xml; charset=utf-8  
Accept: application/soap+xml, application/dime, multipart/related, text/*  
User-Agent: Axis/beta3  
Host: 53.16.71.44:8080  
Cache-Control: no-cache  
Pragma: no-cache  
SOAPAction: ""  
Content-Length: 396
```

```
<?xml version="1.0" encoding="UTF-8"?>  
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"  
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"  
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">  
  <soapenv:Body>  
    <test soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">  
      <number xsi:type="xsd:string">7</number>  
    </test>  
  </soapenv:Body>  
</soapenv:Envelope>
```

Kommunikation im Internet – Protokolle

- Anwendungsschicht
 - HyperText Transfer Protocol HTTP, SOAP v1.2-Anfrage

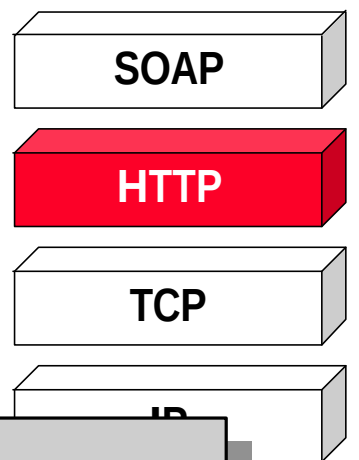


```
POST /axis/IsPrime.jws HTTP/1.0
Content-Type: application/soap+xml; charset=utf-8
Accept: application/soap+xml, application/dime, multipart/related, text/*
User-Agent: Axis/beta3
Host: 53.16.71.44:8080
Cache-Control: no-cache
Pragma: no-cache
SOAPAction: ""
Content-Length: 396
```

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <test soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
      <number xsi:type="xsd:string">7</number>
    </test>
  </soapenv:Body>
</soapenv:Envelope>
```

Kommunikation im Internet – Protokolle

- Anwendungsschicht
 - HyperText Transfer Protocol HTTP, SOAP-Antwort



HTTP/1.1 200 OK

Content-Type: application/soap+xml; charset=utf-8

Connection: close

Date: Tue, 10 Dec 2002 18:45:01 GMT

Server: Apache Tomcat/4.0.4 (HTTP/1.1 Connector)

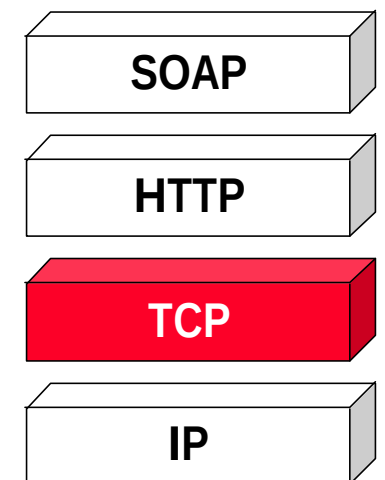
Set-Cookie: JSESSIONID=41B96D25B609A1F3235852305A36E46D;Path=/axis

`<?xml version="1.0" encoding="UTF-8"?>`

```
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <testResponse
      soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
      <testReturn xsi:type="xsd:boolean">>false</testReturn>
    </testResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

Kommunikation im Internet – Protokolle

- Transportschicht
 - Transmission Control Protocol (TCP):
 - Quellport
 - Zielport
 - Flags (verbindungsorientiertes Protokoll)
 - User Datagram Protocol UDP:
 - Quellport
 - Zielport

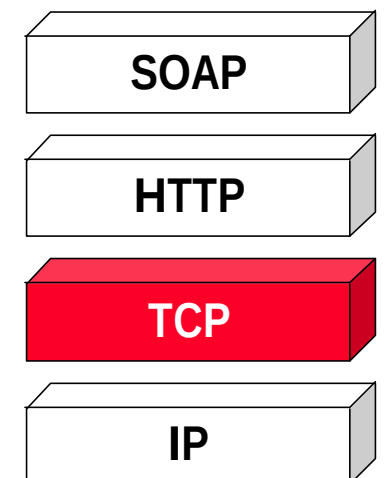


0F 61 1F 90 B8 8E D6 94 9D 5B 9B A3 50 18 44 70 95 0B 00 00

**Quellport
(3937)**

Kommunikation im Internet – Protokolle

- Transportschicht
 - Transmission Control Protocol (TCP):
 - Quellport
 - Zielport
 - Flags (verbindungsorientiertes Protokoll)
 - User Datagram Protocol UDP:
 - Quellport
 - Zielport

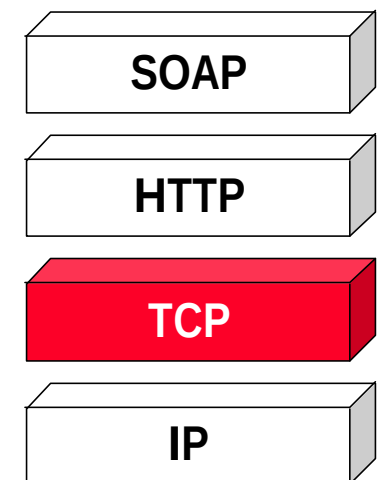


0F 61 **1F 90** B8 8E D6 94 9D 5B 9B A3 50 18 44 70 95 0B 00 00

Zielport
(8080)

Kommunikation im Internet – Protokolle

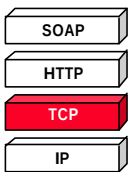
- Transportschicht
 - Transmission Control Protocol (TCP):
 - Quellport
 - Zielport
 - Flags (verbindungsorientiertes Protokoll)
 - User Datagram Protocol UDP:
 - Quellport
 - Zielport



0F 61 1F 90 B8 8E D6 94 9D 5B 9B A3 50 **18** 44 70 95 0B 00 00

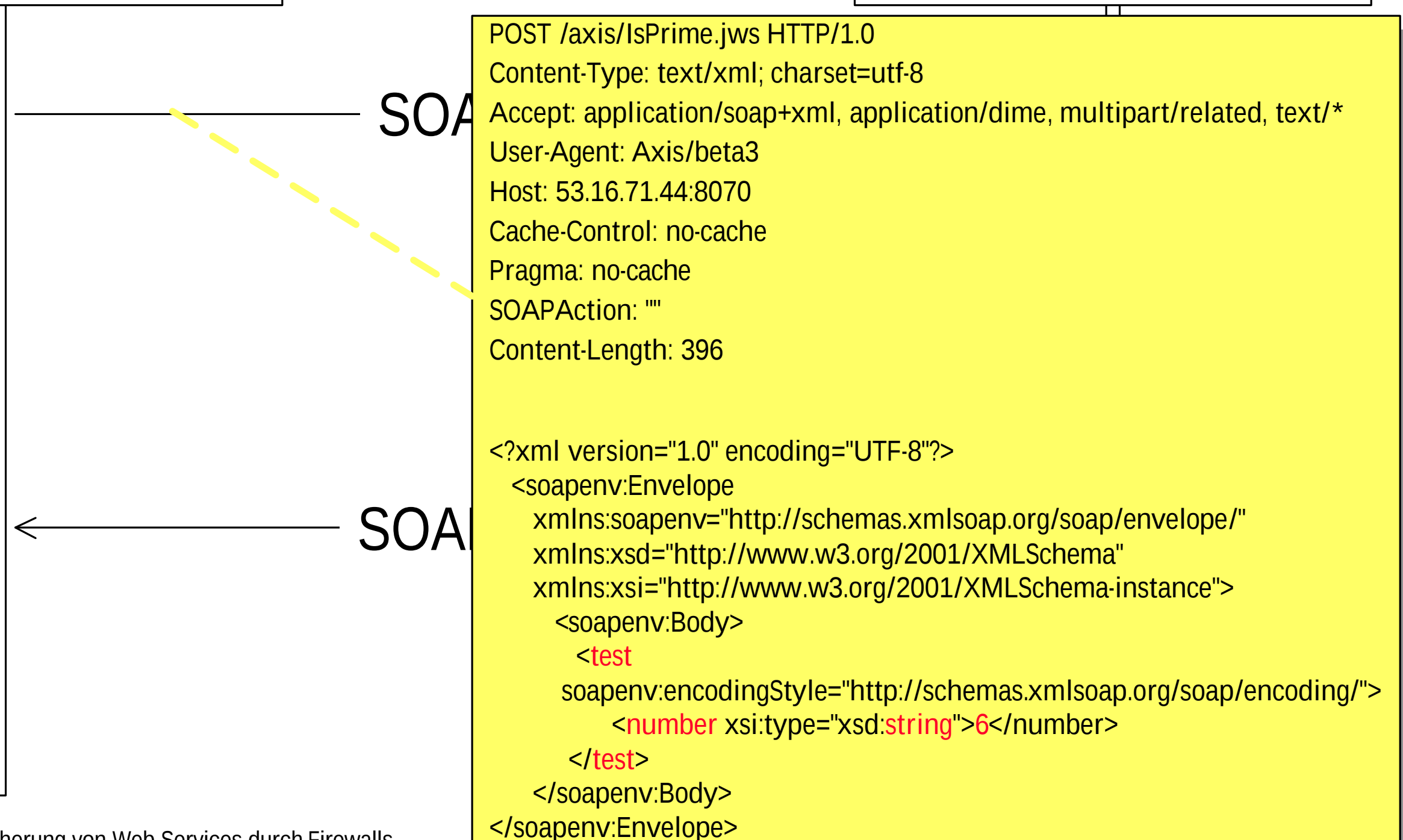
Flags
(PSH, ACK)

Kommunikation im Internet – Protokolle

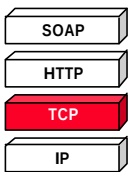


Aufrufer:SOAPNode

Dienst:SOAPNode

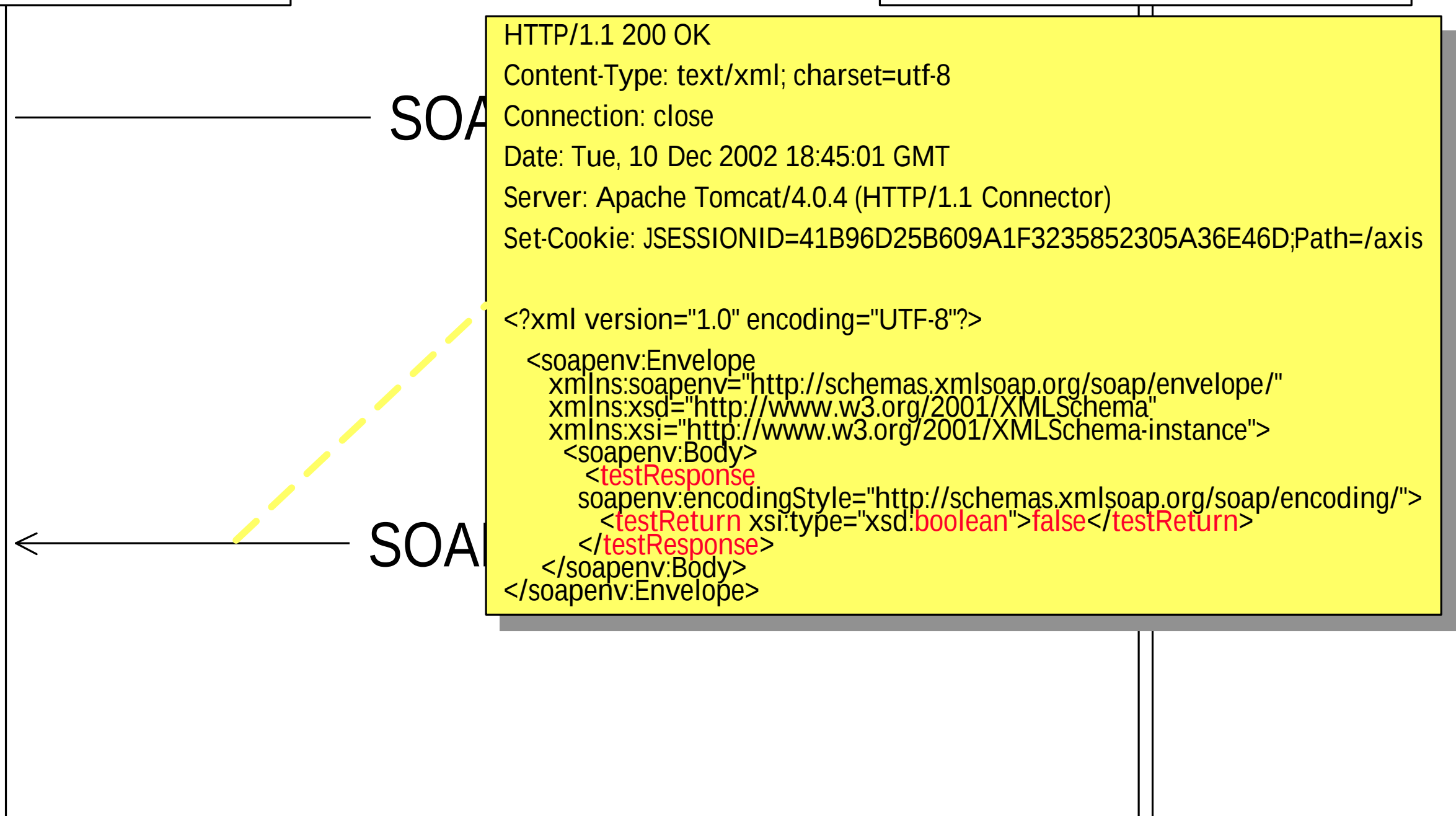


Kommunikation im Internet – Protokolle

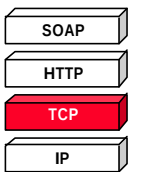
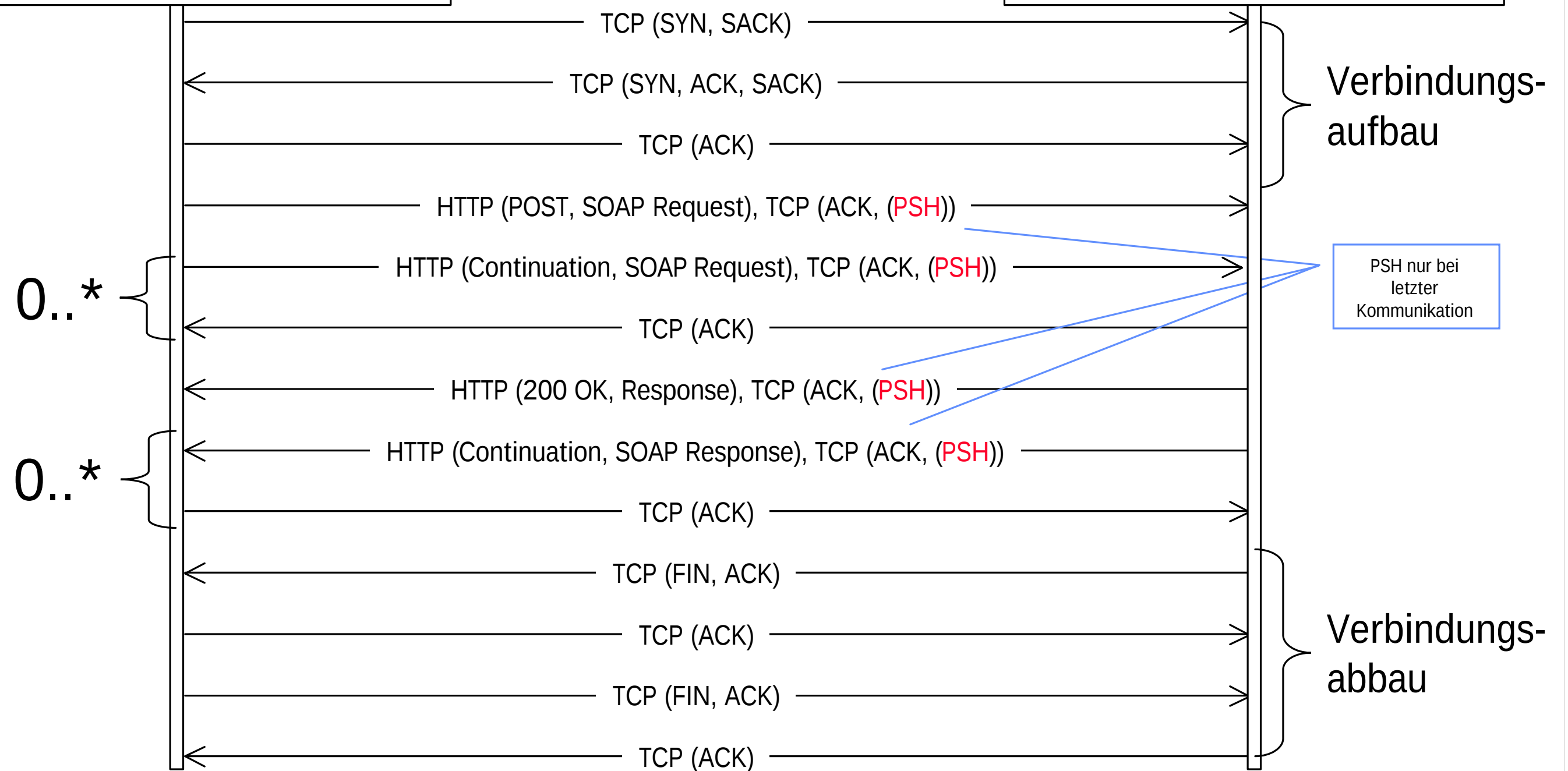


Aufrufer:SOAPNode

Dienst:SOAPNode

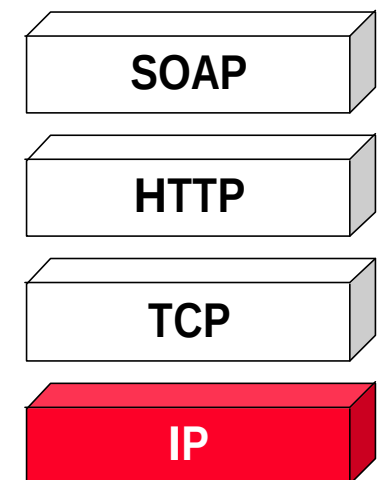


Kommunikation im Internet – Protokolle

**Aufrufer:SOAPNode****Dienst:SOAPNode**

Kommunikation im Internet – Protokolle

- Vermittlungsschicht (Internet Protocol (IP)):
 - Adressierung von Rechnern im Netzwerk
 - Quelladresse
 - Zieladresse
 - Nutzdaten-Protokolltyp (TCP, UDP, ICMP, ...)

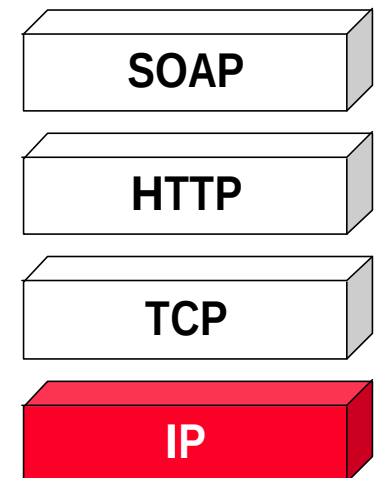


45 00 00 30 1C 76 40 00 80 06 E5 65 35 10 47 A0 35 10 47 2C

IP Version 4

Kommunikation im Internet – Protokolle

- Vermittlungsschicht (Internet Protocol (IP)):
 - Adressierung von Rechnern im Netzwerk
 - Quelladresse
 - Zieladresse
 - Nutzdaten-Protokolltyp (TCP, UDP, ICMP, ...)

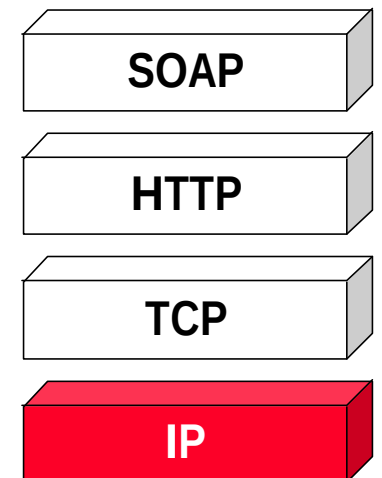


45 **00** 00 30 1C 76 40 00 80 06 E5 65 35 10 47 A0 35 10 47 2C

Differentiated Service Field

Kommunikation im Internet – Protokolle

- Vermittlungsschicht (Internet Protocol (IP)):
 - Adressierung von Rechnern im Netzwerk
 - Quelladresse
 - Zieladresse
 - Nutzdaten-Protokolltyp (TCP, UDP, ICMP, ...)

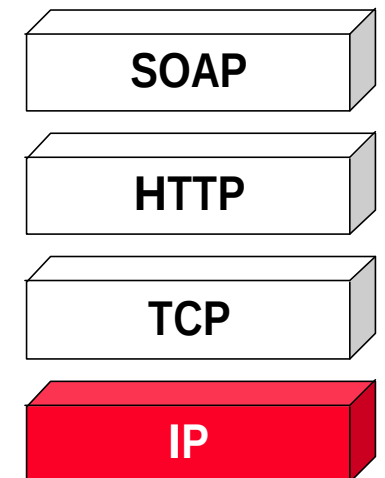


45 00 00 30 1C 76 **40** 00 80 06 E5 65 35 10 47 A0 35 10 47 2C

Don't Fragment

Kommunikation im Internet – Protokolle

- Vermittlungsschicht (Internet Protocol (IP)):
 - Adressierung von Rechnern im Netzwerk
 - Quelladresse
 - Zieladresse
 - Nutzdaten-Protokolltyp (TCP, UDP, ICMP, ...)

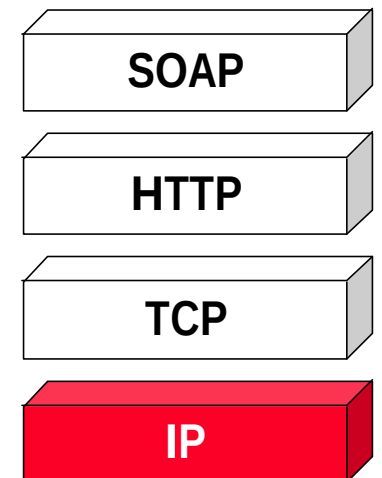


45 00 00 30 1C 76 40 00 80 **06** E5 65 35 10 47 A0 35 10 47 2C

TCP

Kommunikation im Internet – Protokolle

- Vermittlungsschicht (Internet Protocol (IP)):
 - Adressierung von Rechnern im Netzwerk
 - Quelladresse
 - Zieladresse
 - Nutzdaten-Protokolltyp (TCP, UDP, ICMP, ...)

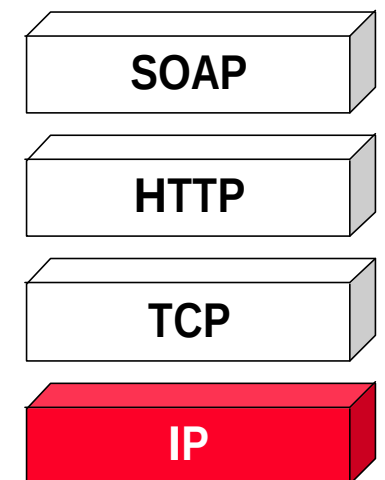


45 00 00 30 1C 76 40 00 80 06 E5 65 35 10 47 A0 35 10 47 2C

Source
(53.16.71.160)

Kommunikation im Internet – Protokolle

- Vermittlungsschicht (Internet Protocol (IP)):
 - Adressierung von Rechnern im Netzwerk
 - Quelladresse
 - Zieladresse
 - Nutzdaten-Protokolltyp (TCP, UDP, ICMP, ...)

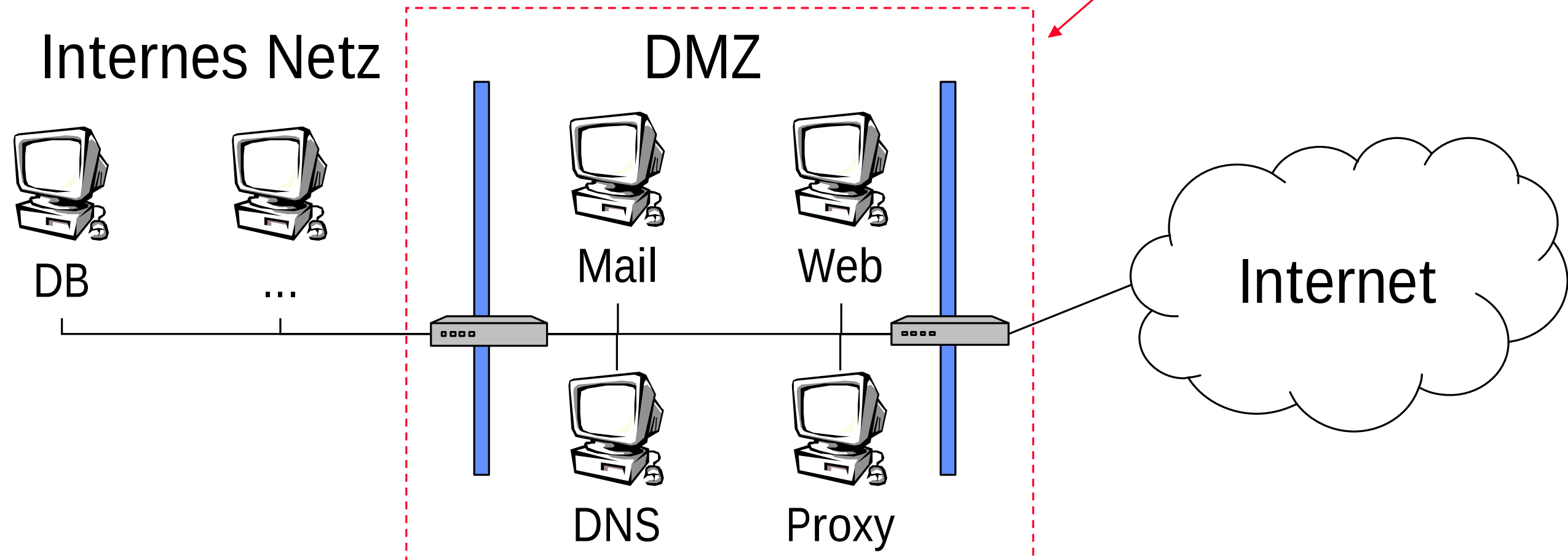


45 00 00 30 1C 76 40 00 80 06 E5 65 35 10 47 A0 **35 10 47 2C**

Destination
(53.16.71.44)

Funktionsweise einer Firewall

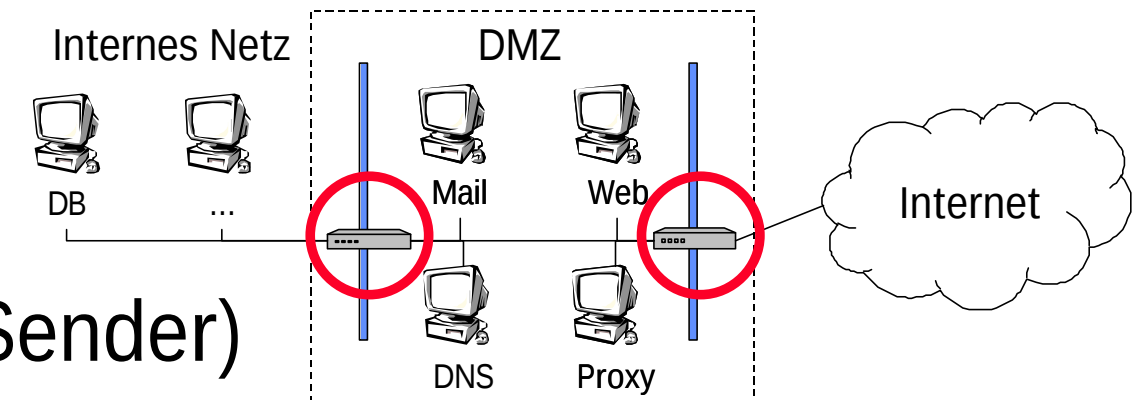
- Schützt Rechnersystem vor Einbruch
- Zwischenstation zwischen nicht-vertrauenswürdigen Hosts und internem Netz
- Angesiedelt in der DMZ (demilitarisierte Zone)
- Ort für Web-Server, Mailserver, DNS



Funktionsweise einer Firewall – Paketfilter

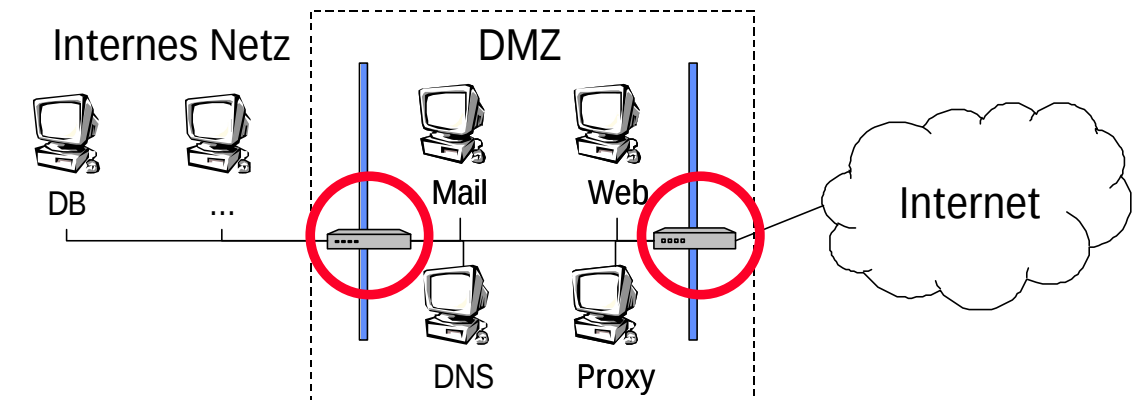
Steuerung des Datenverkehrs

- Paket an Ziel weiterleiten
- Paket verwerfen (keine Information für Sender)
- Paket zurückweisen (Information für Sender)
- Paket verändern
- Paket an anderes Ziel leiten (Lastverteilung)
- Information aufzeichnen
- Alarm auslösen
- Filterregeln ändern



Funktionsweise einer Firewall – Paketfilter

- Regeln
 - Protokoll
 - Quell-Netzwerkadresse
 - Ziel-Netzwerkadresse
 - Quell-Port
 - Ziel-Port
 - Paketgröße
- Zustandslose Paketfilter
- Zustandsgesteuerte oder dynamische Paketfilter
 - Verfolgen des Netzverkehrs
 - Dynamische Paketbehandlung
- Intelligente Paketfilter
 - Inspektion von Paketinhalten, möglicherweise Modifikationen daran



Funktionsweise einer Firewall – Inhaltsfilter

Vorteile:

- Paketfilterung weit verbreitet (Router, kommerzielle und freie Produkte)
- Einfacher Paketfilter arbeitet sehr effizient

Nachteile:

- Filterregeln oft schwer konfigurierbar und testbar
- Komplexe Filter erzeugen Last
- Nicht alle Policies durch Filterregeln durchführbar
(z.B. Benutzerauthentisierung); hier Einsatz von intelligenten Filtern nötig

Funktionsweise einer Firewall – Proxy

Proxy

- (1) Person authorized to act on behalf of another
- (2) Authority to represent somebody else

Oxford Advanced Learner's Dictionary of Current English, 4th Edition

- Transparenter Stellvertreter für Benutzer oder Dienst
- Application Level Gateway
- Entgegennahme von Benutzeranfragen
- Weiterleitung der Anfragen an den Dienst
- Einsatz auch für Cachingzwecke

Funktionsweise einer Firewall – Proxy

- Mischsysteme: Paketfilter und Proxy
 - Paketfilter fängt Verbindung ab und leitet sie an Proxy weiter oder fungiert selbst als solcher
- Treffen von Entscheidungen bei eingehenden Anfragen
 - Verschiedene Hosts: unterschiedliche Fähigkeiten
 - Weiterleitung von Anfragen
 - Benutzerauthentisierung
- Für ausgehenden Datenverkehr: gängig
Für nach innen gerichtete Verbindungen einsetzbar zur Lastverteilung und Erhöhung der Sicherheit

Funktionsweise einer Firewall – Proxy

Vorteile:

- Möglichkeit zur intelligenten Filterung
- Benutzer-Authentisierung
- Verständnis des Anwendungsprotokolls ermöglicht effektive Protokollierung

Nachteile:

- Schlechte Verfügbarkeit für neue oder selten eingesetzte Protokolle (Dienste)
- Installation und Konfiguration aufwendig

SOAP und Firewalls

- Herausforderungen:
 - SOAP ist protokollunabhängig
=> Dieselben Inhalte können in verschiedene Protokolle verpackt sein
 - SOAP ist selbst ein Protokoll
=> Auswertung der SOAP-Header
 - SOAP ist XML und damit Text
=> Neue Art von Angriffen (konkret Denial-of-Service-Attacken) denkbar
 - Gültiges SOAP allein ist nicht genug ...
=> Schemagültigkeit nicht immer hinreichend

Firewalls für SOAP

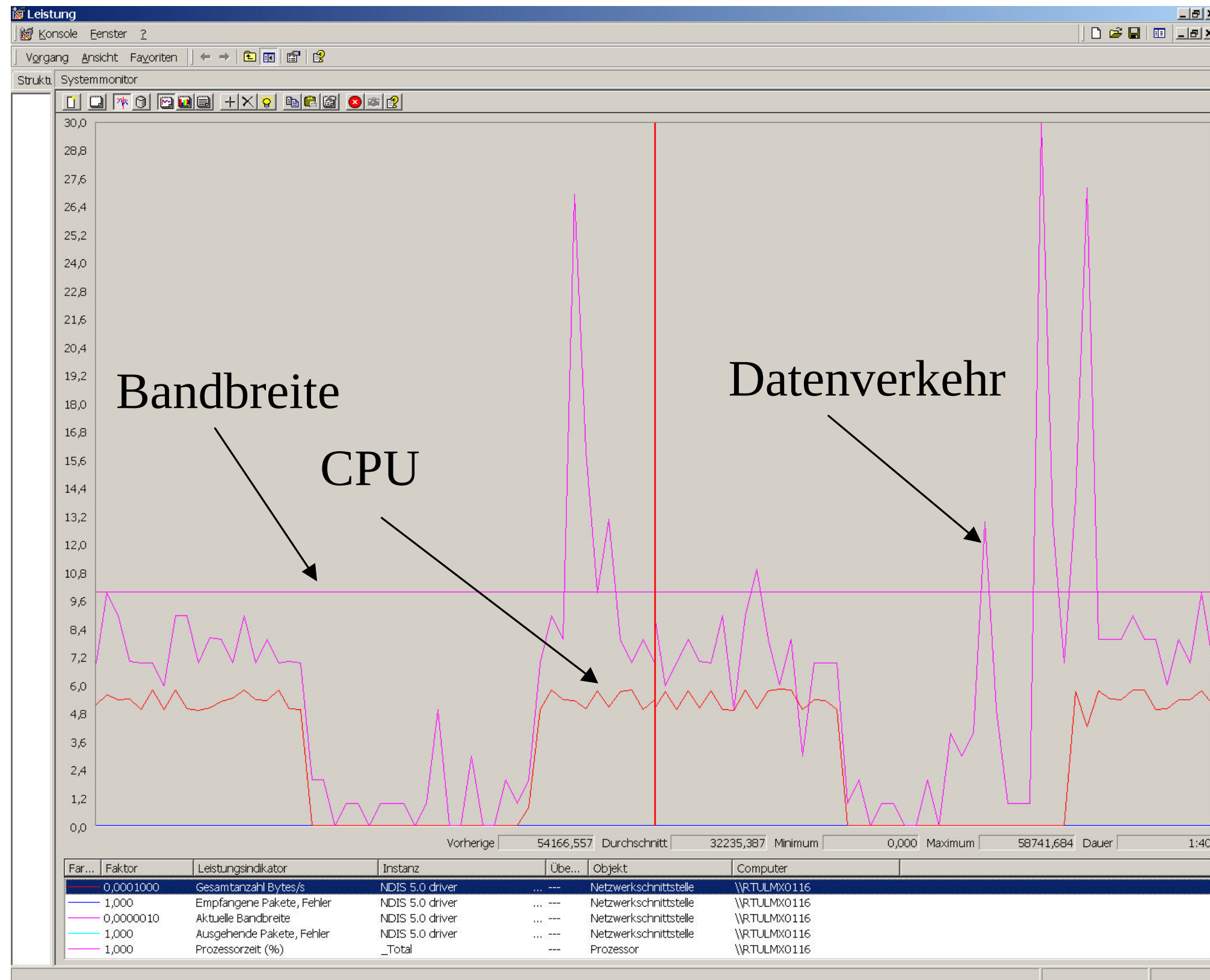
Ansätze:

1. Keine Überladung des WWW-Ports
2. Einbezug der SOAP-Kommunikationssemantik
3. Überwachung des TCP-Verkehrs (etwa der Window Size)
4. IP-Adressen-basierte (Basis-)Authentisierung
5. Authentisierung und Autorisierung über SOAP-Inhalte
(z.B. WS-Security konforme Signatur- und Verschlüsselungsheader)
6. XML-agnostische Prüfung von Body-Inhalten
(reguläre Ausdrücke)
7. XML-basierte Validierung (Nutzung von (restriktivem) XML-Schema)
 - Keine Nutzung von SOAP-Implementierungen die programmiersprachliche Reflektionsmechanismen ausbeuten!

„SOAP-Firewalls“

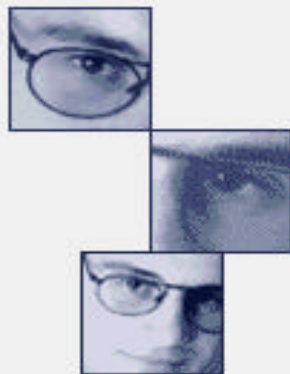
- Derzeit: Idee oder Vision
- Kaum (ausgereifte) Produkte
- Integration mit bestehenden XML-Sicherheitsstandards wünschenswert
- Grundsätzliche Entscheidung:
 - Erweiterung einer „klassischen“ Firewall
 - Zusätzliche Firewall(-schicht)

Erfahrungen mit „SOAP-Firewalls“ -- Serverseite



Erfahrungen mit „SOAP-Firewalls“-- Clientseite





Mario Jeckle ...
Dialog ...
Über diese Seiten ...
suchen ...
SiteMap
RSS Newsfeed XML
Was gibt's hier Neues?

Unified Modeling Language (UML)
eXtensible Markup Language (XML)
XML Metadata Interchange (XMI)
Web Services
XML Acronym Demystifier Project
XML-Strategie

Vorträge und Publikationen
Vorlesungen
Diplomarbeiten
GOOAL.net
XML-Arbeitskreis

Web Services Workshop *WS-RSD'02*
Web Services @ Berliner XML-Tage
Internet > Search Engines
Mersennesche Primzahlen
Feedback
Rotkreuz Mitgliederverwaltung

jeckle.de

Latest News ... on UML, XML, XMI, and Web Services