DAIMLERCHRYSLER

Securing Web Services using Firewalls

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

Structure of this Presentation

Internet Communication

- Basic Idea
- Technical Basis
- Protocols

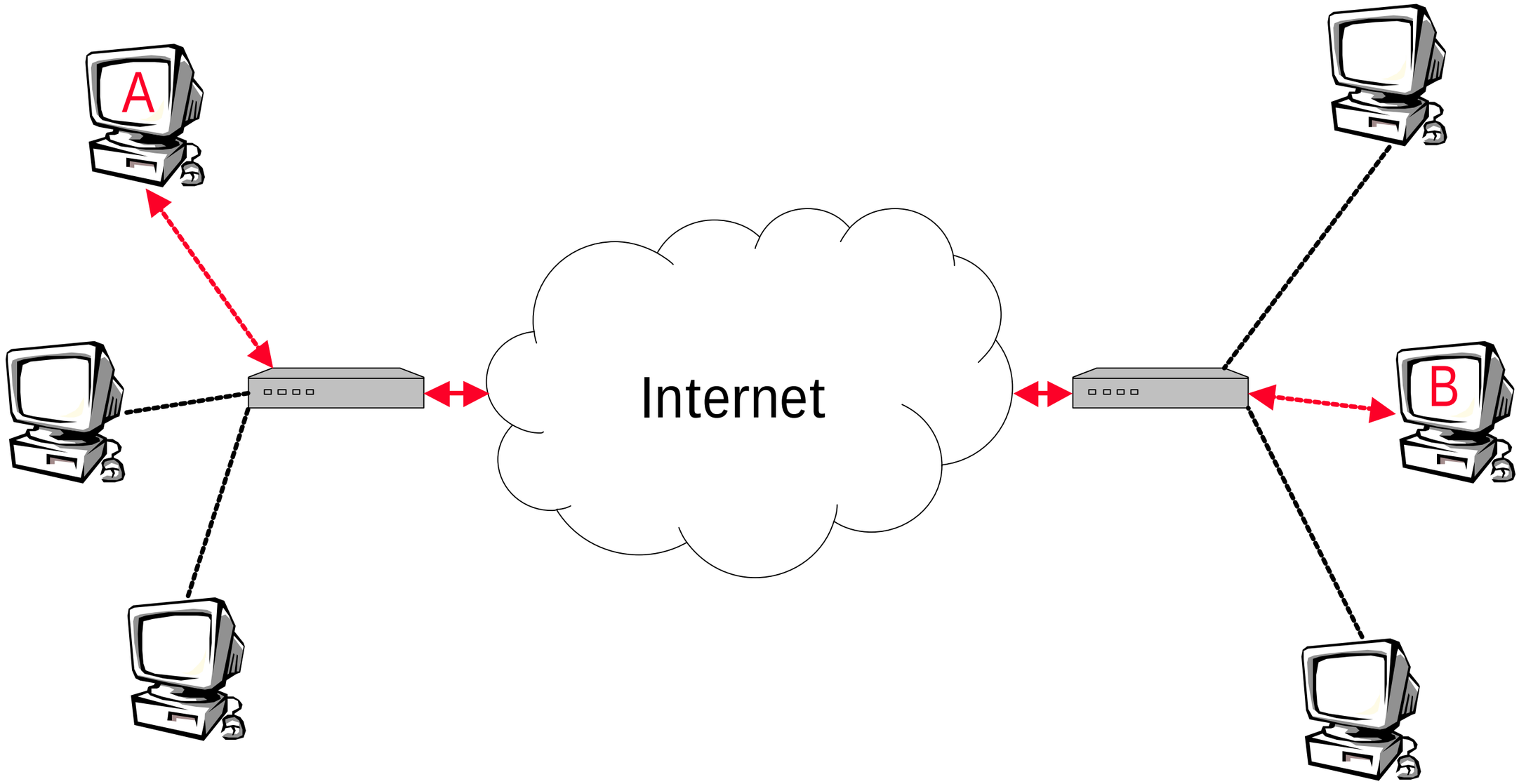
Web Services

- SOAP
- Description Model
- Implementation and Execution Model

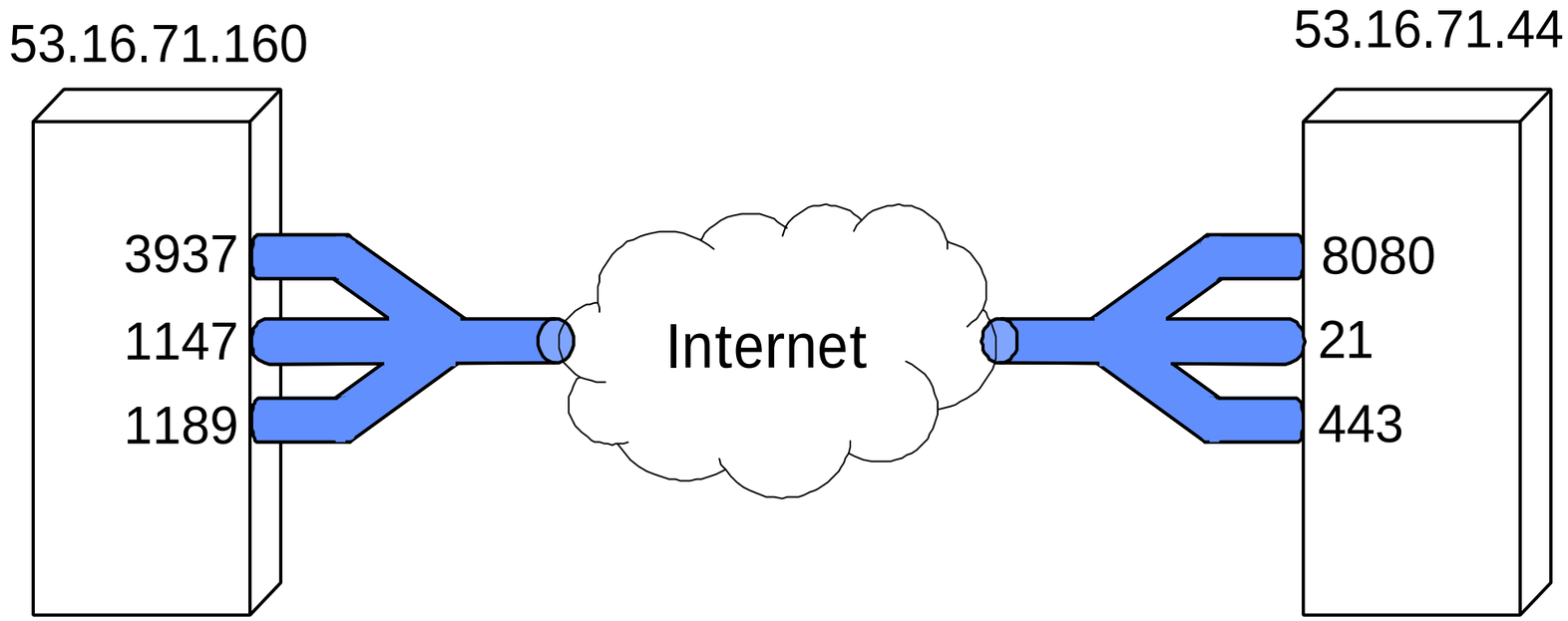
Firewalls

- Basic Idea
- Traditional Approaches
- "SOAP Firewalls"

Internet Communication – Basic Idea



Internet Communication – Manner of Operation



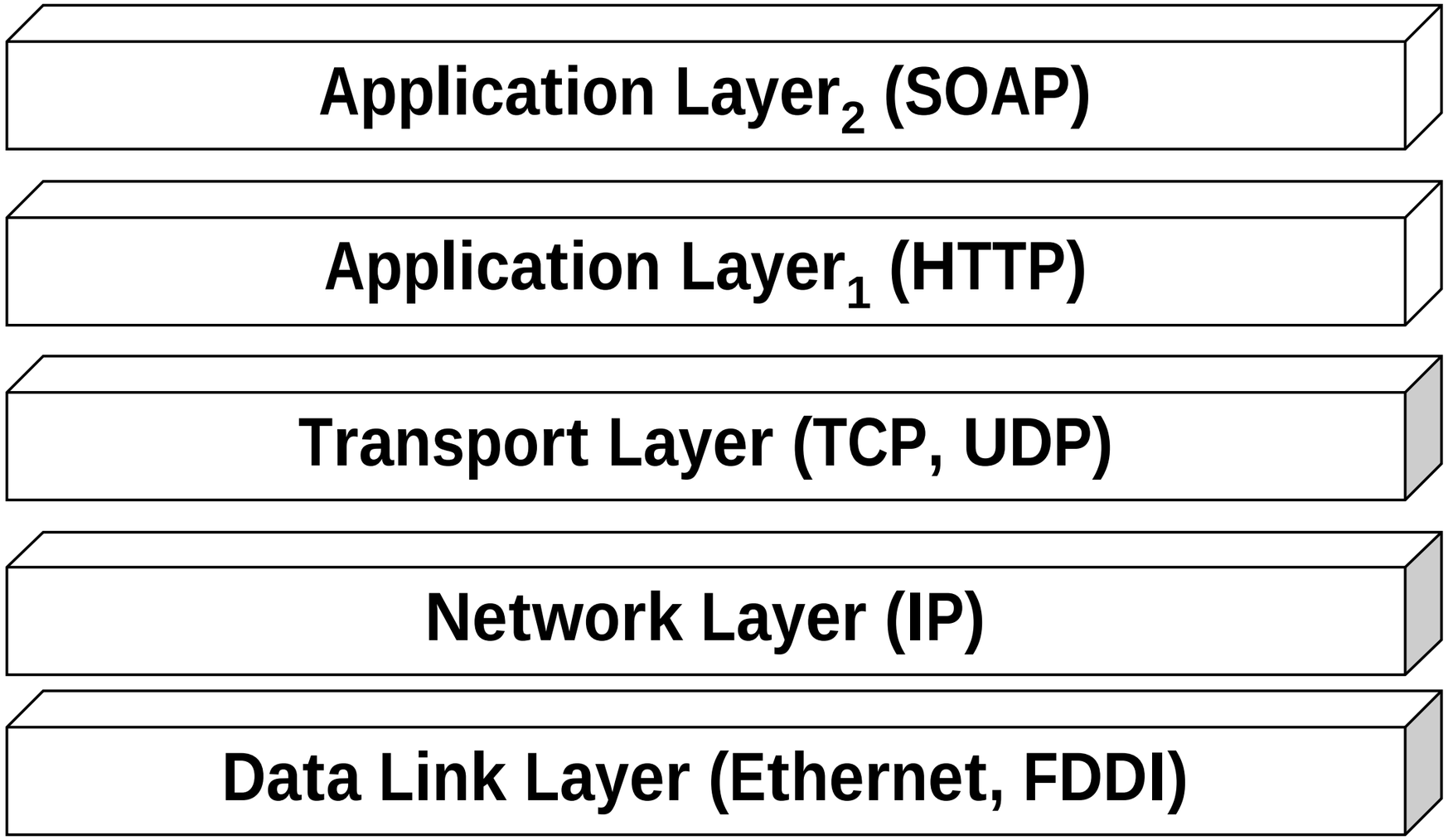
Addressing:

- Computer: IP Address (IP Protocol)
- Application: Port (TCP resp. UDP Protocol)

Port:

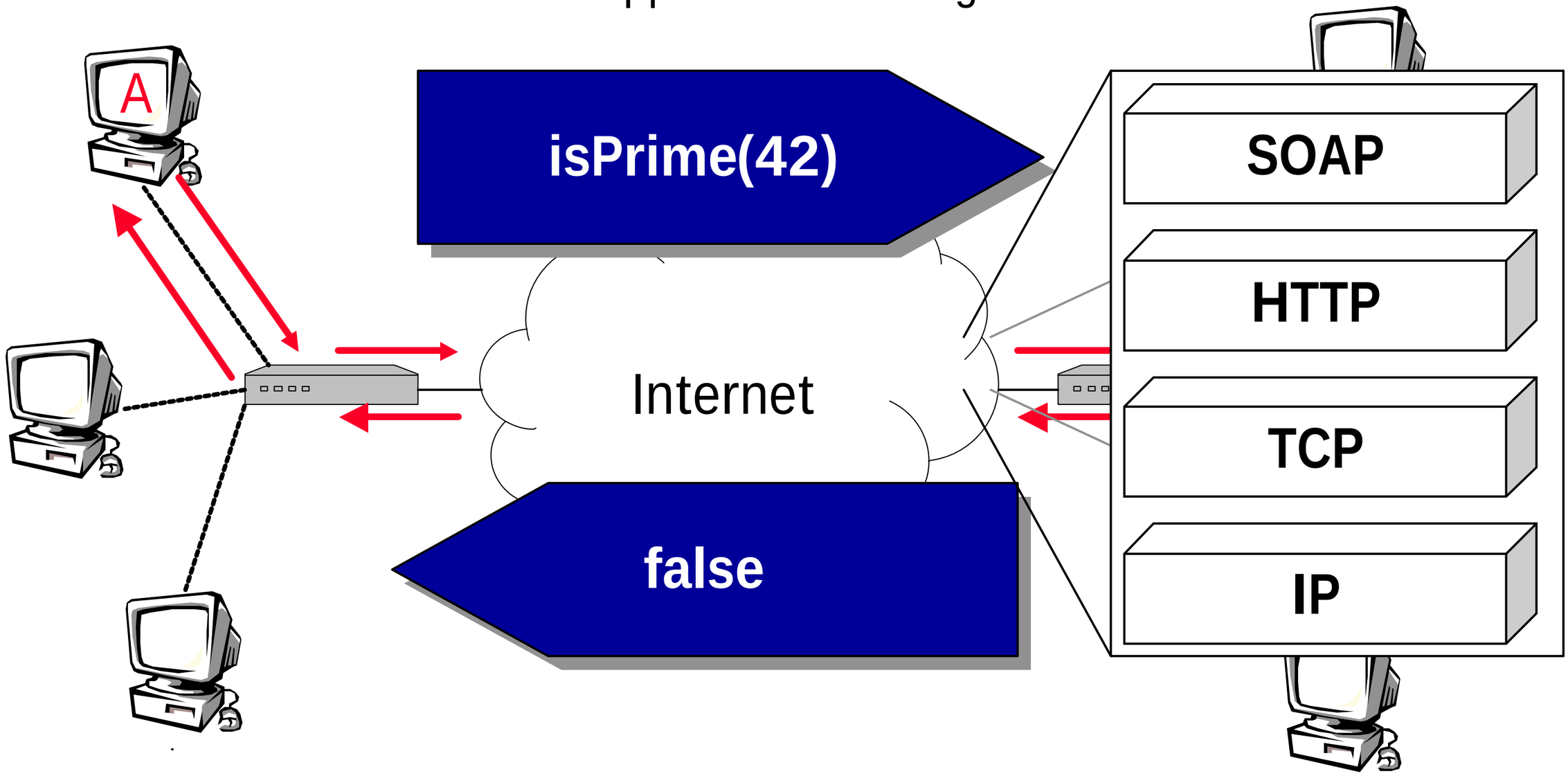
- Logical connection between client and server programs
- Distinction of several logical channels on the same network interface on the same computer
- Server software binds to assigned port

Internet Communication – Protocol Stack



Internet Communication

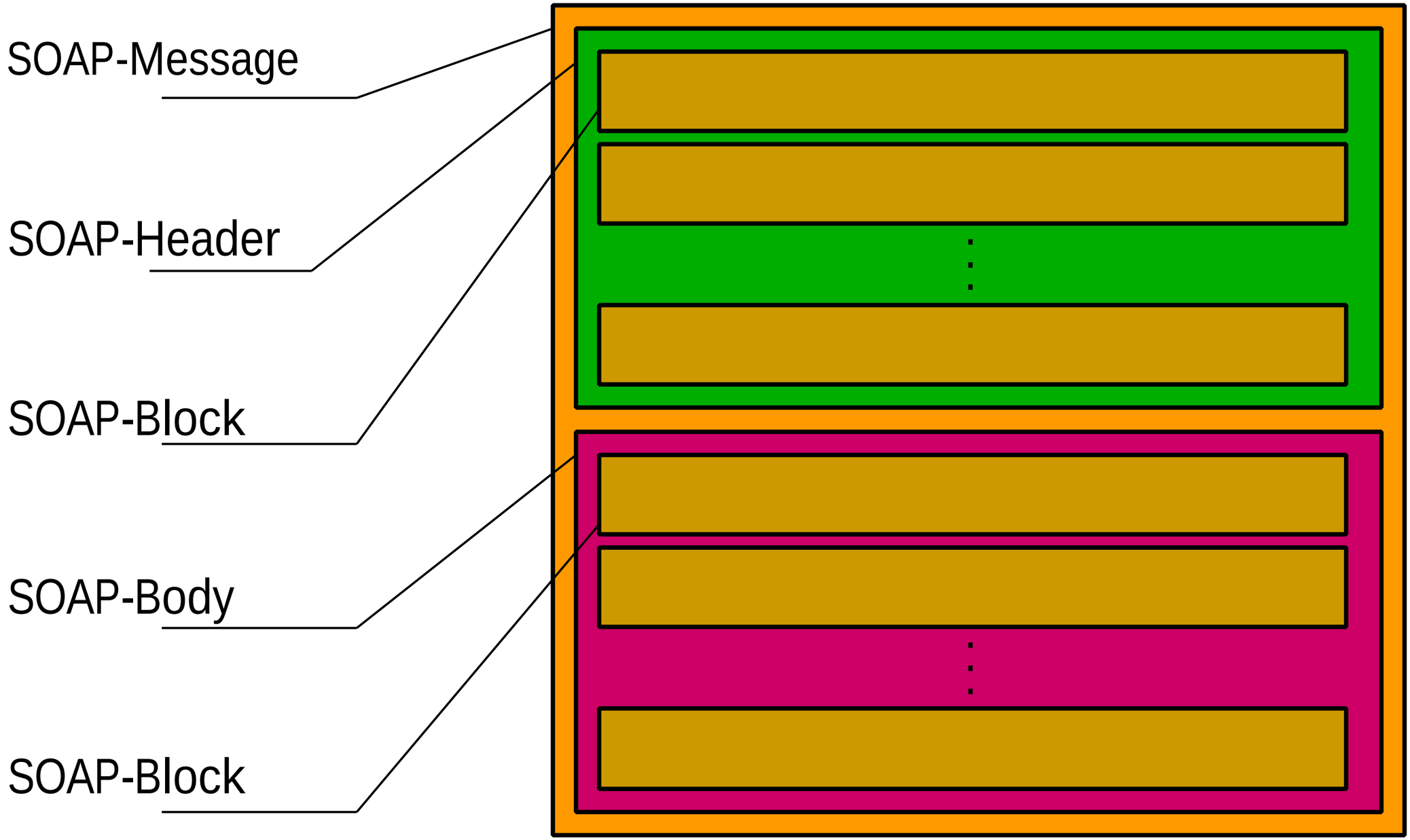
- Data transmission between applications – usage scenario



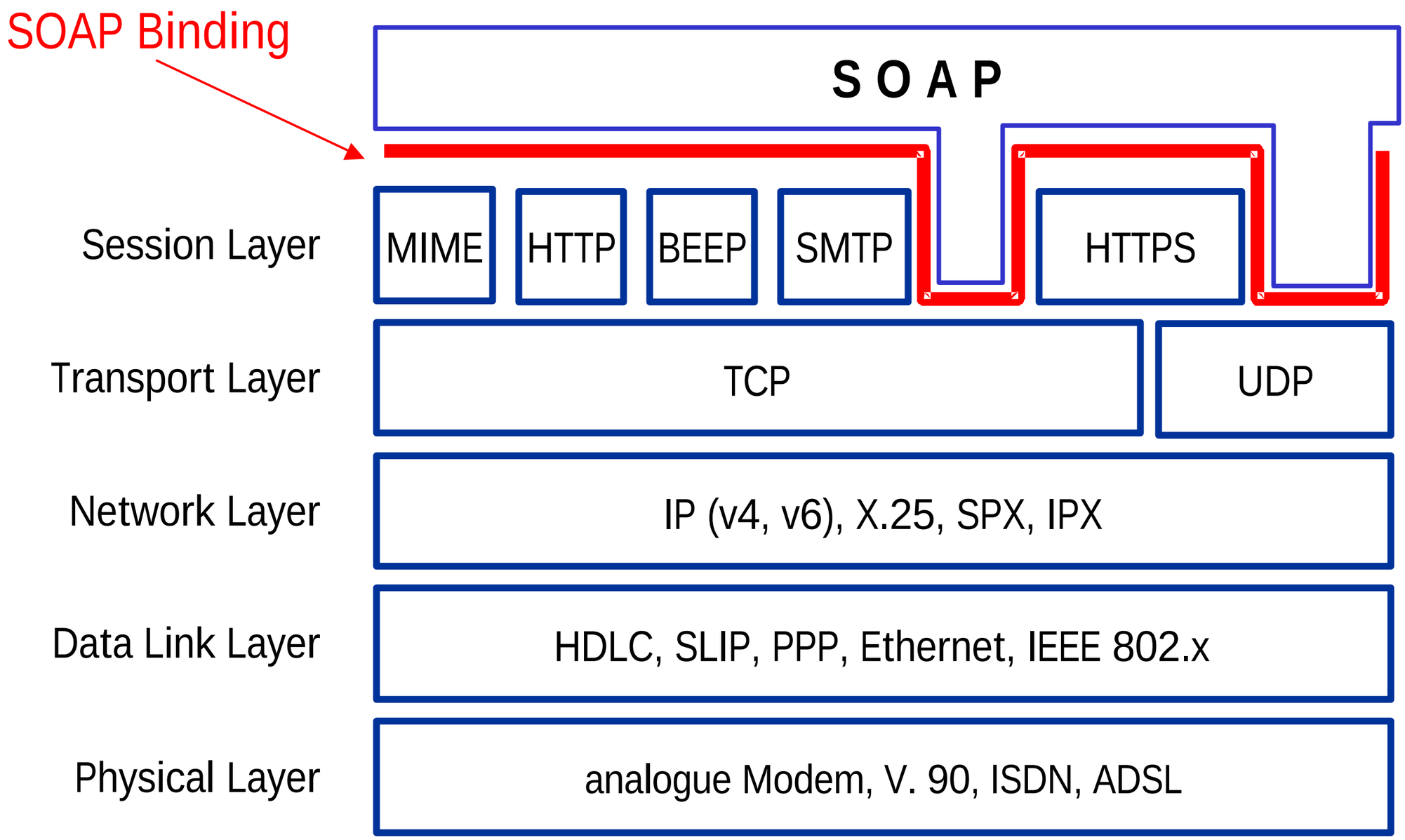
Excursus: The SOAP v1.2 Protocol

- Basic Idea: remote function calls and message exchange via XML
- In most situations
  - HTTP as communication protocol
  - Synchronous calls
  - RPC-Style
- Version 1.2 developed by the W3C "XML Protocol" Working Group
- Widely supported
- First "usable" Implementations available
- Structure:
  - SOAP Part 0: Introduction (non-normative document)
  - SOAP Part 1: Framework for the construction of SOAP messages
  - SOAP Part 2: Concrete usage of the framework,
    for example RPC via HTTP

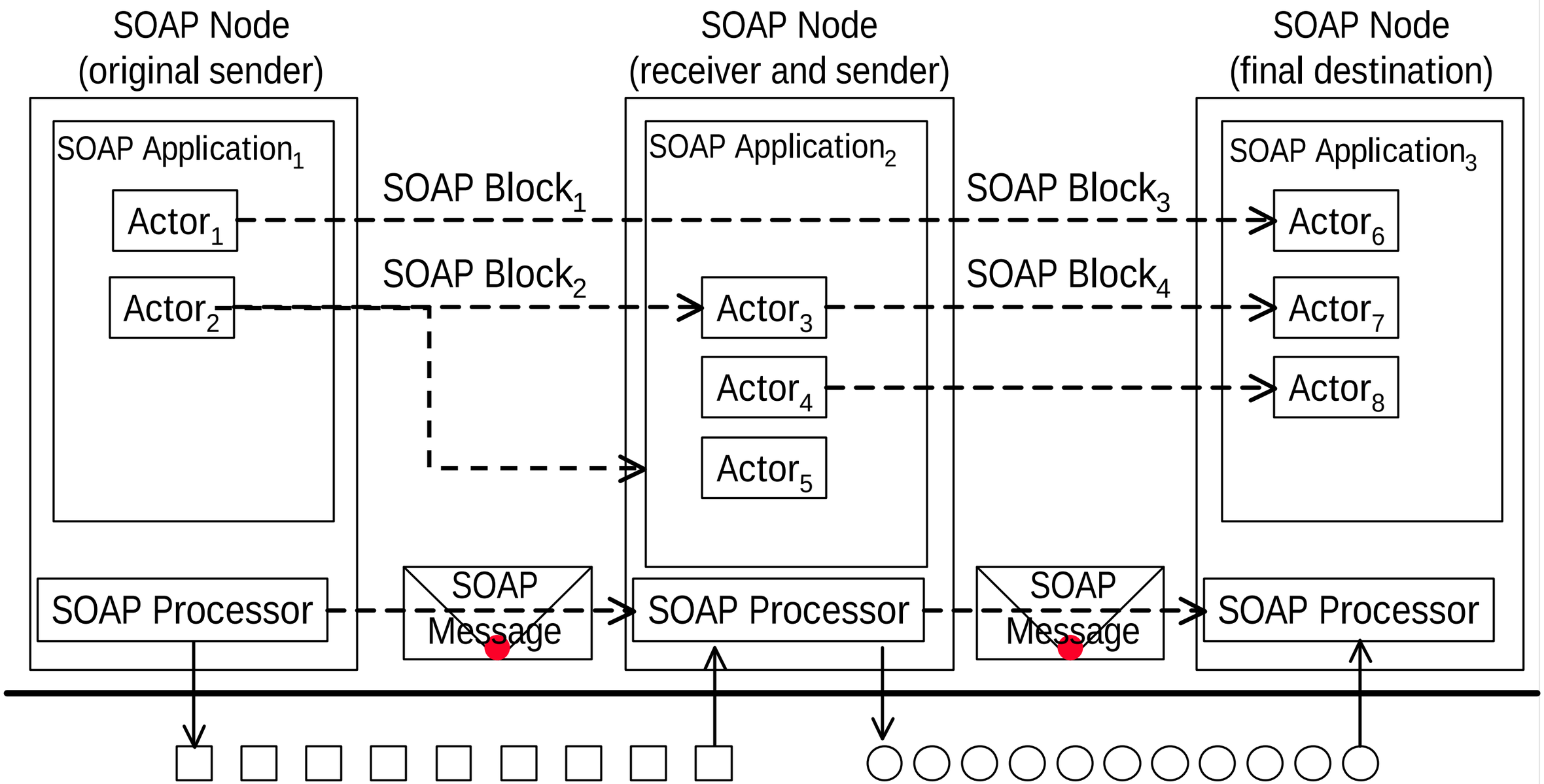
Excursus: The SOAP v1.2 Protocol – Message Structure



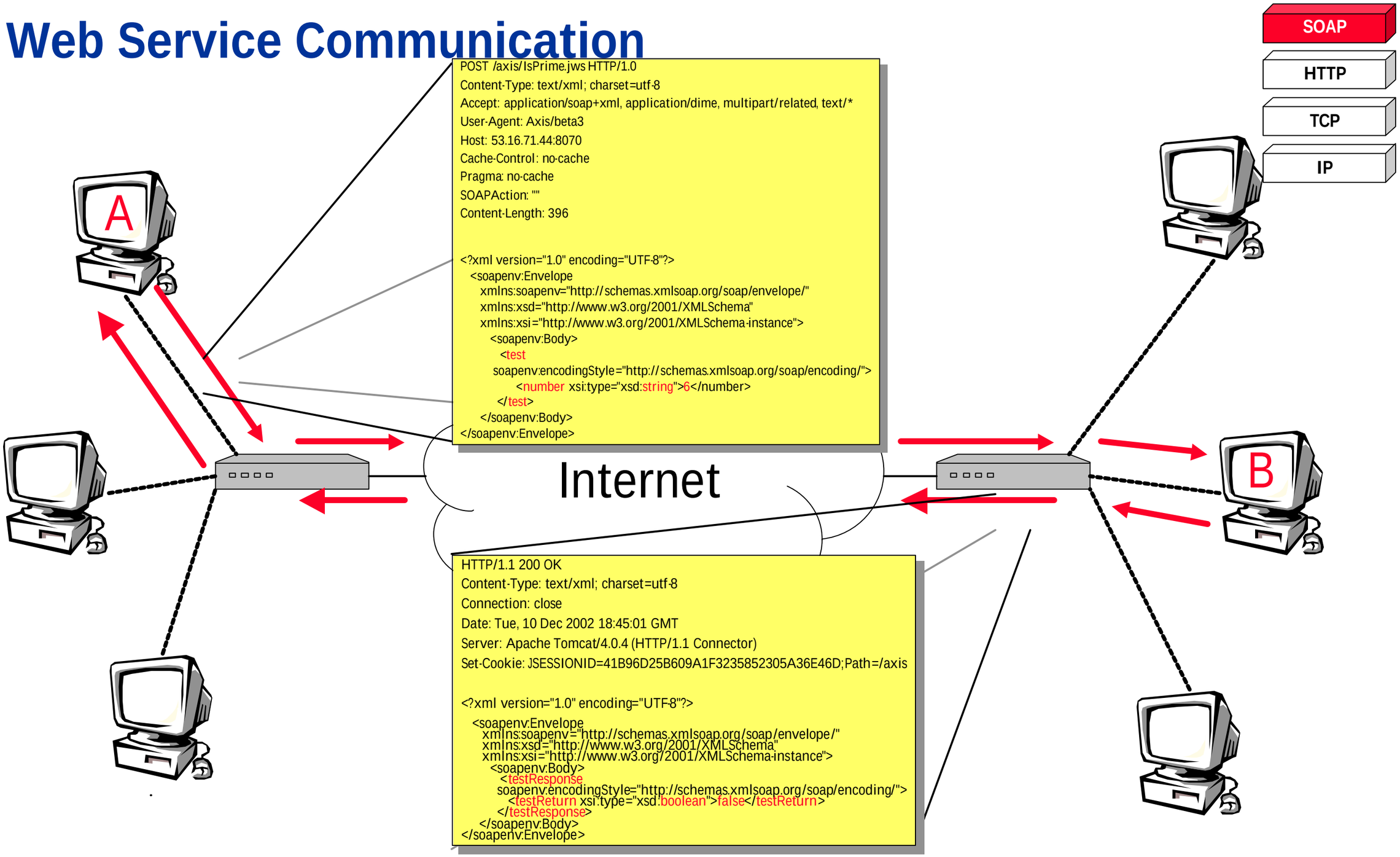
Excursus: The SOAP v1.2 Protocol – Protocol Independence



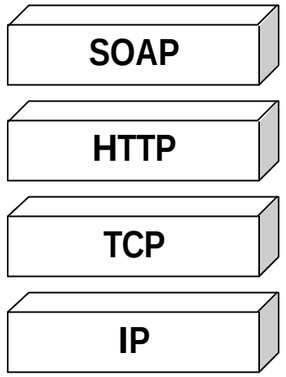
Excursus: The SOAP v1.2 Protocol --- Intermediaries



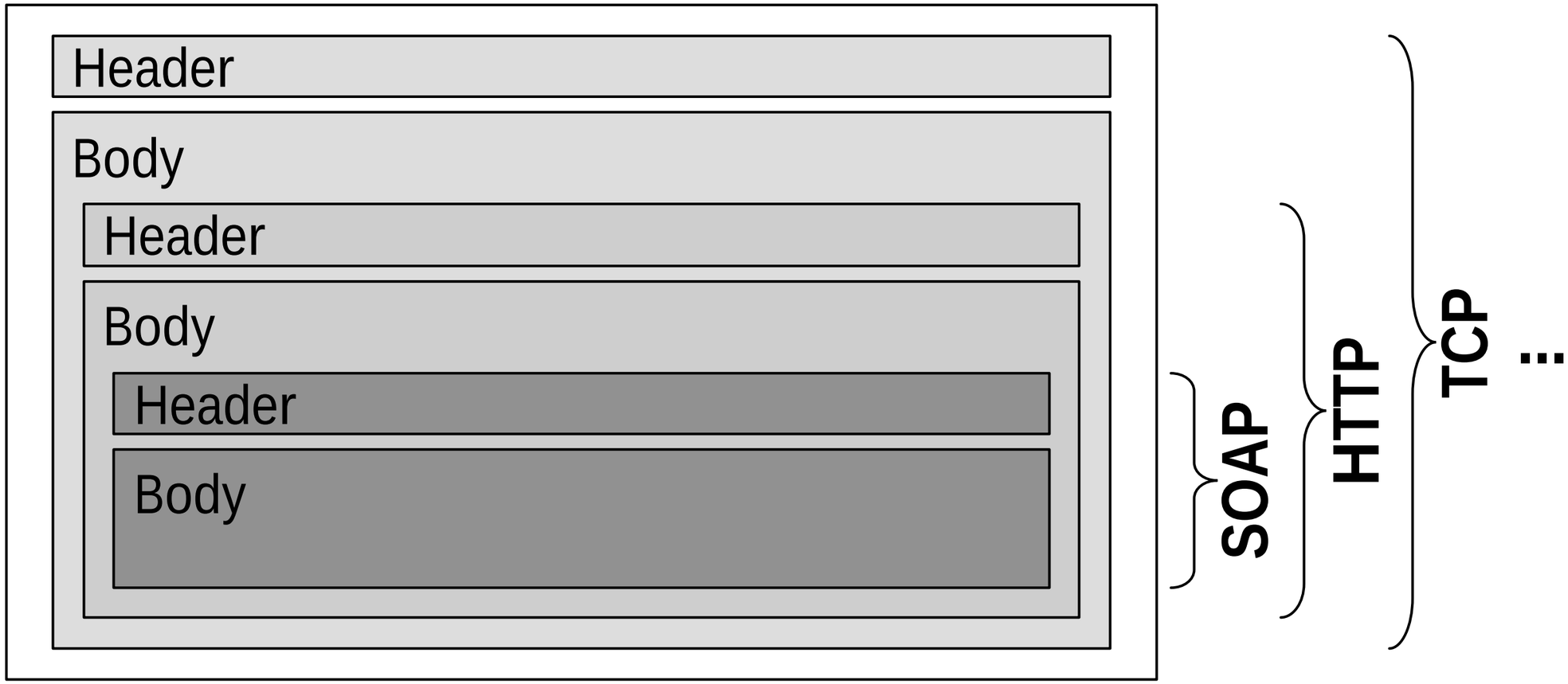
Web Service Communication



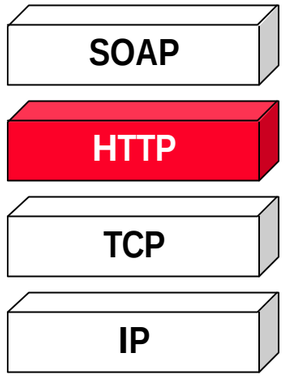
Internet Communication – Protocols



- Data transmission between applications
- Data packets
  - Header: protocol specific information
  - Body: payload



Internet Communication – Protocols

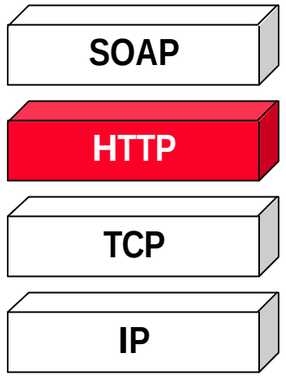


- Application Layer
  - Hypertext Transfer Protocol HTTP, SOAP v1.1-Request

```
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>
```

Internet Communication – Protocols

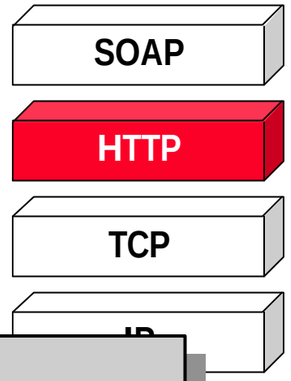


- Application Layer
  - Hypertext Transfer Protocol HTTP, SOAP v1.2-Request

```
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>
```

Internet Communication – Protocols

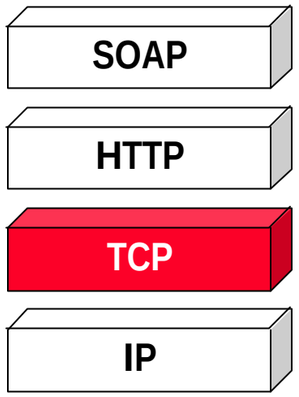


- Application Layer
  - Hypertext Transfer Protocol HTTP, SOAP-Response

```
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>
```

Internet Communication – Protocols

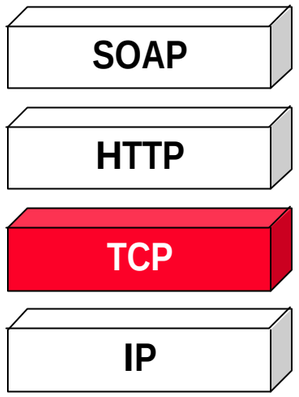


- Transport Layer
  - Transmission Control Protocol (TCP):
    - Source port
    - Destination port
    - Flags (connection oriented protocol)
  - User Datagram Protocol UDP:
    - Source port
    - Destination port

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

Source port (3937)

Internet Communication – Protocols

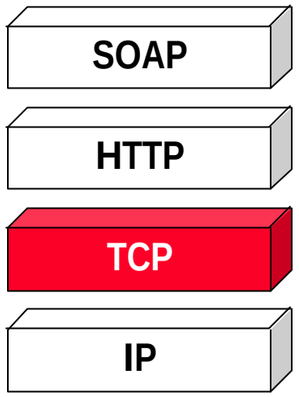


- Transport Layer
  - Transmission Control Protocol (TCP):
    - Source port
    - Destination port
    - Flags (connection oriented protocol)
  - User Datagram Protocol UDP:
    - Source port
    - Destination port

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

Destination port (8080)

Internet Communication – Protocols

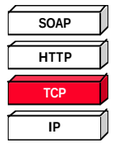


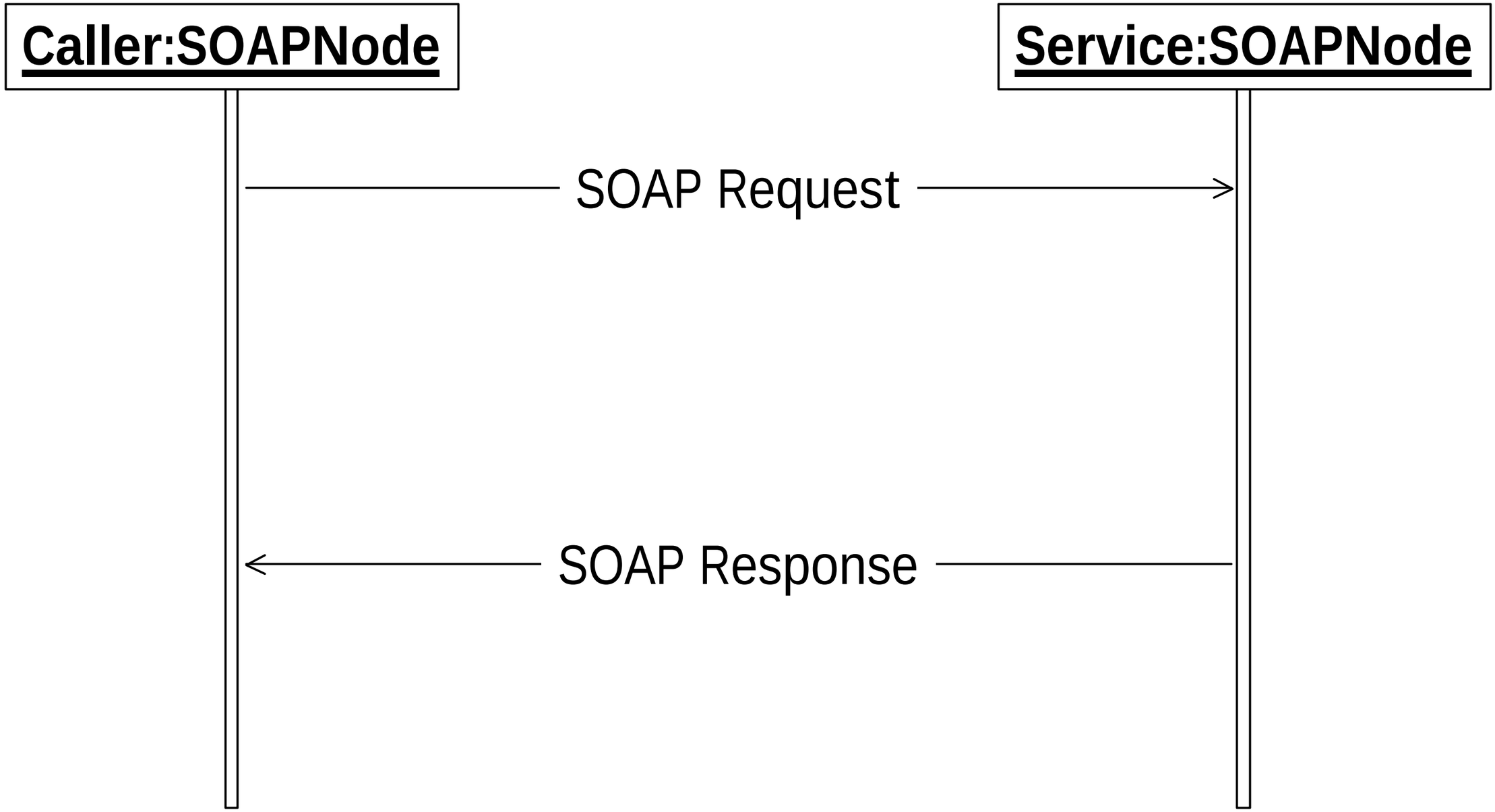
- Transport Layer
  - Transmission Control Protocol (TCP):
    - Source port
    - Destination port
    - Flags (connection oriented protocol)
  - User Datagram Protocol UDP:
    - Source port
    - Destination port

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

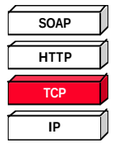
Flags
(PSH, ACK)

Internet Communication – Protocols





Internet Communication – Protocols



Caller:SOAPNode

Service:SOAPNode

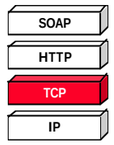
SOA

SOA

```
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">6</number>
        </test>
    </soapenv:Body>
</soapenv:Envelope>
```

Internet Communication – Protocols



Caller:SOAPNode

Service:SOAPNode

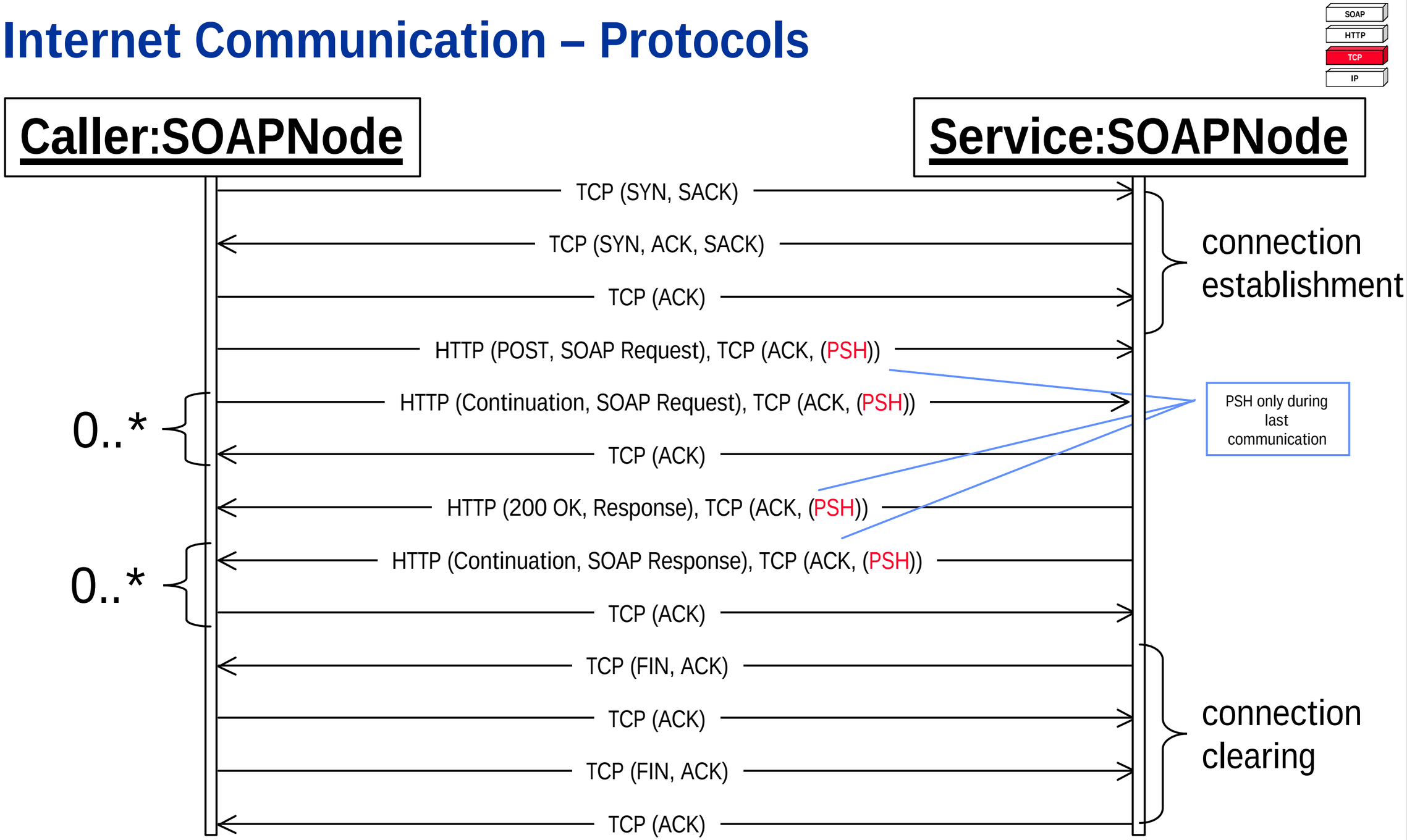
SOA

SOA

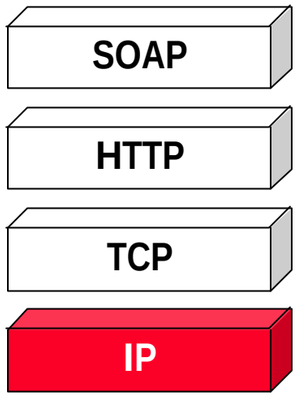
```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Connection: close
Date: Tue, 10 Dec 2002 18:45:01 GMT
Server: Apache Tomcat/4.0.4 (HTTP/1.1 Connector)
Set-Cookie: JSESSIONID=41B96D25B609A1F3235852305A36E46D;Path=/axis

<?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>
```

Internet Communication – Protocols



Internet Communication – Protocols

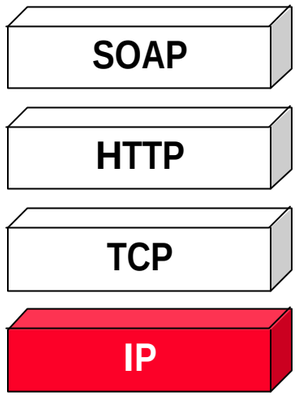


- Network Layer (Internet Protocol (IP)):
  - Addressing of computers in a network
  - Source address
  - Destination address
  - Payload protocol (TCP, UDP, ICMP, ...)

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

IP Version 4

Internet Communication – Protocols

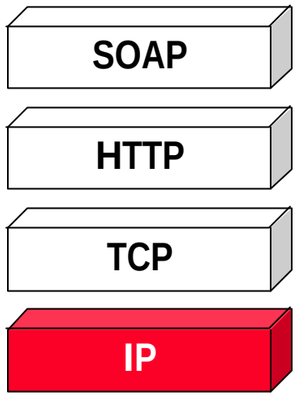


- Network Layer (Internet Protocol (IP)):
  - Addressing of computers in a network
  - Source address
  - Destination address
  - Payload protocol (TCP, UDP, ICMP, ...)

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

Differentiated Service Field

Internet Communication – Protocols

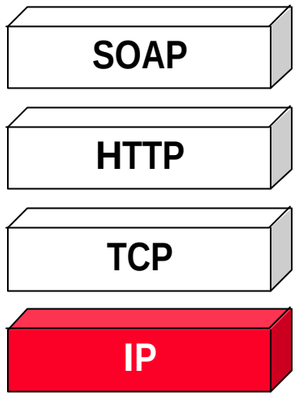


- Network Layer (Internet Protocol (IP)):
  - Addressing of computers in a network
  - Source address
  - Destination address
  - Payload protocol (TCP, UDP, ICMP, ...)

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

Don‘t Fragment

Internet Communication – Protocols

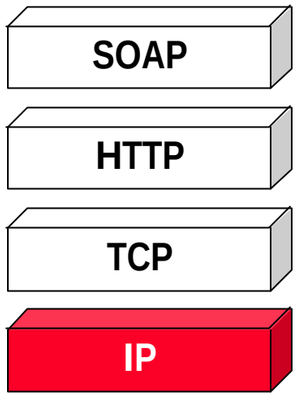


- Network Layer (Internet Protocol (IP)):
  - Addressing of computers in a network
  - Source address
  - Destination address
  - Payload protocol (TCP, UDP, ICMP, ...)

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

TCP

Internet Communication – Protocols

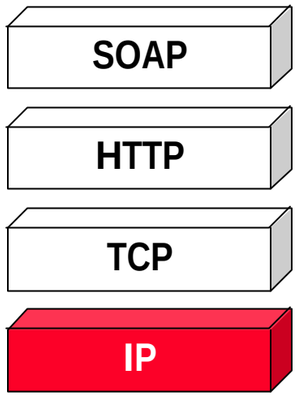


- Network Layer (Internet Protocol (IP)):
  - Addressing of computers in a network
  - Source address
  - Destination address
  - Payload protocol (TCP, UDP, ICMP, ...)

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)

Internet Communication – Protocols



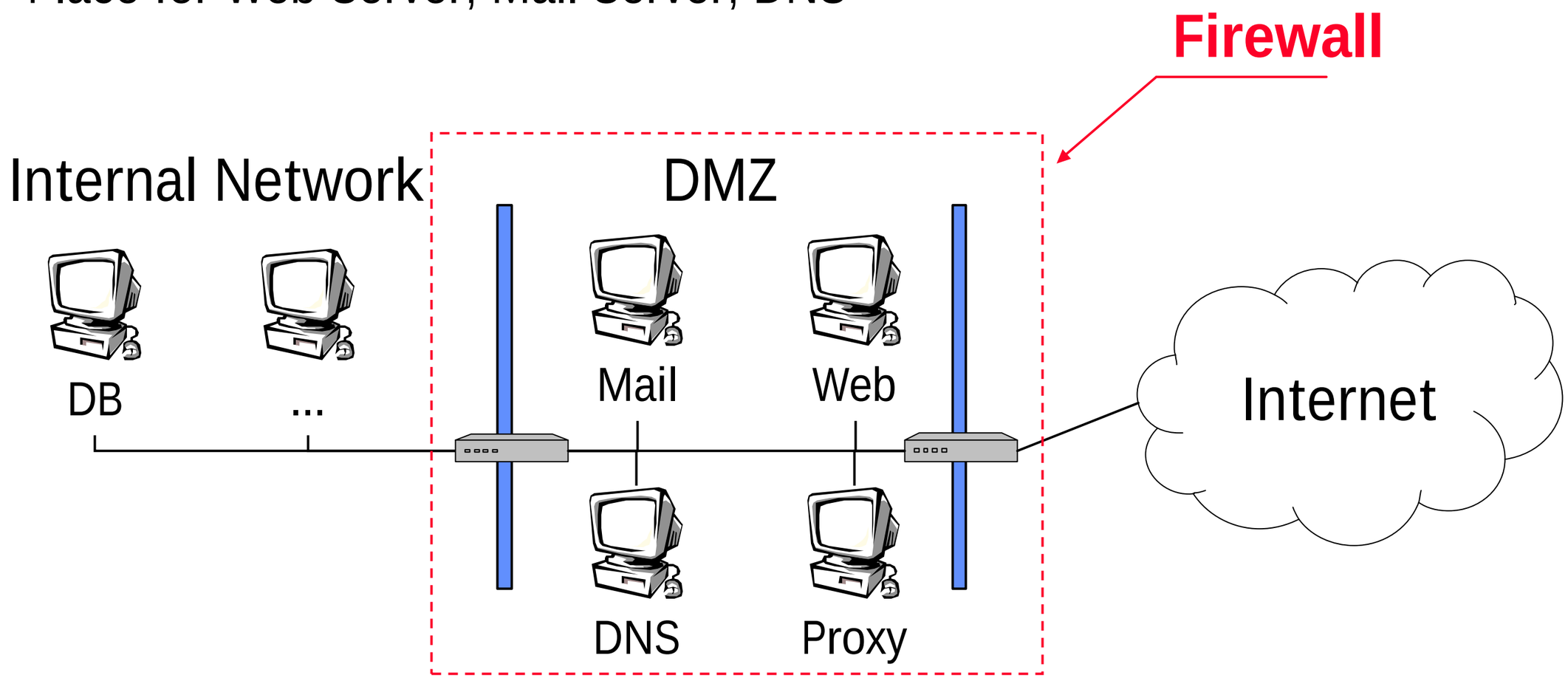
- Network Layer (Internet Protocol (IP)):
  - Addressing of computers in a network
  - Source address
  - Destination address
  - Payload protocol (TCP, UDP, ICMP, ...)

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

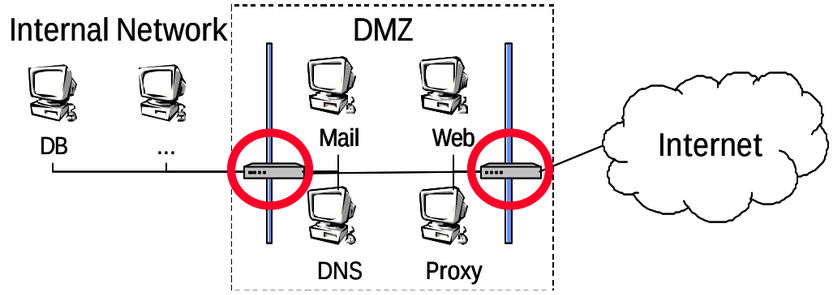
Destination
(53.16.71.44)

The Workings of a Firewall

- Protection against break-in into computer systems
- Intermediate between non-trustworthy hosts and internal network
- Located in DMZ (de-militarized zone)
- Place for Web Server, Mail Server, DNS



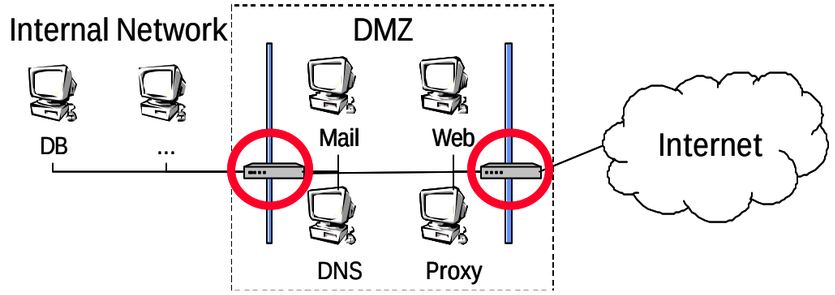
The Workings of a Firewall – Packet Filtering



Data Traffic Control

- Forward data packet to destination
- Drop data packet (no information for sender)
- Reject data packet (information for sender)
- Manipulate packet
- Forward packet to different destination (load balancing)
- Record information
- Trigger alarm
- Change filtering rules

The Workings of a Firewall – Packet Filtering



- Rules
  - Protocol
  - Source network address
  - Destination network address
  - Source port
  - Destination port
  - Packet size
- Stateless packet filter
- Stateful or dynamic packet filter
  - Tracking of network traffic
  - Dynamic packet handling
- Intelligent packet filter
  - Inspection of packet content, eventually modifications

The Workings of a Firewall – Content Filtering

Advantages:

- Packet filtering widely used (router, commercial and free products)
- Simple packet filters work very efficiently

Disadvantages:

- Filtering rules are often hard to configure and test
- Complex filters generate (heavy) load
- Not all security policies can be expressed via Filtering rules (e.g. user authentication); use of intelligent filters necessary

The Workings of a 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

- Transparent representative for a user or a service
- Application Level Gateway
- Accepts user requests
- Forwards user requests to service
- Used for caching purposes also

The Workings of a Firewall – Proxy

- Mixed system: packet filter and proxy
  - Packet filter intercepts connection, forwards it to proxy or works as a proxy itself

- Decisions on incoming requests
  - Different hosts: different capabilities
  - Forwarding of requests
  - User authentication

- Commonly used for outgoing data traffic
  Incoming traffic: useful for the purpose of load balancing and to increase security

The Workings of a Firewall – Proxy

Advantages:

- Intelligent filtering possible
- User authentication
- Understanding of application protocol allows effective logging

Disadvantages:

- Bad availability for new or seldom used protocols (services)
- Costly installation and configuration

SOAP and Firewalls

- Challenges:
  - SOAP is protocol independent
    => Identical content can be packed into different protocols
  - SOAP is a protocol itself
    => Evaluation of SOAP headers
  - SOAP is XML and therefore text
    => New kind of attacks (e.g. Denial-of-Service attacks) possible
  - Valid SOAP is not enough...
    => schema validity not always sufficient

Firewalls for SOAP

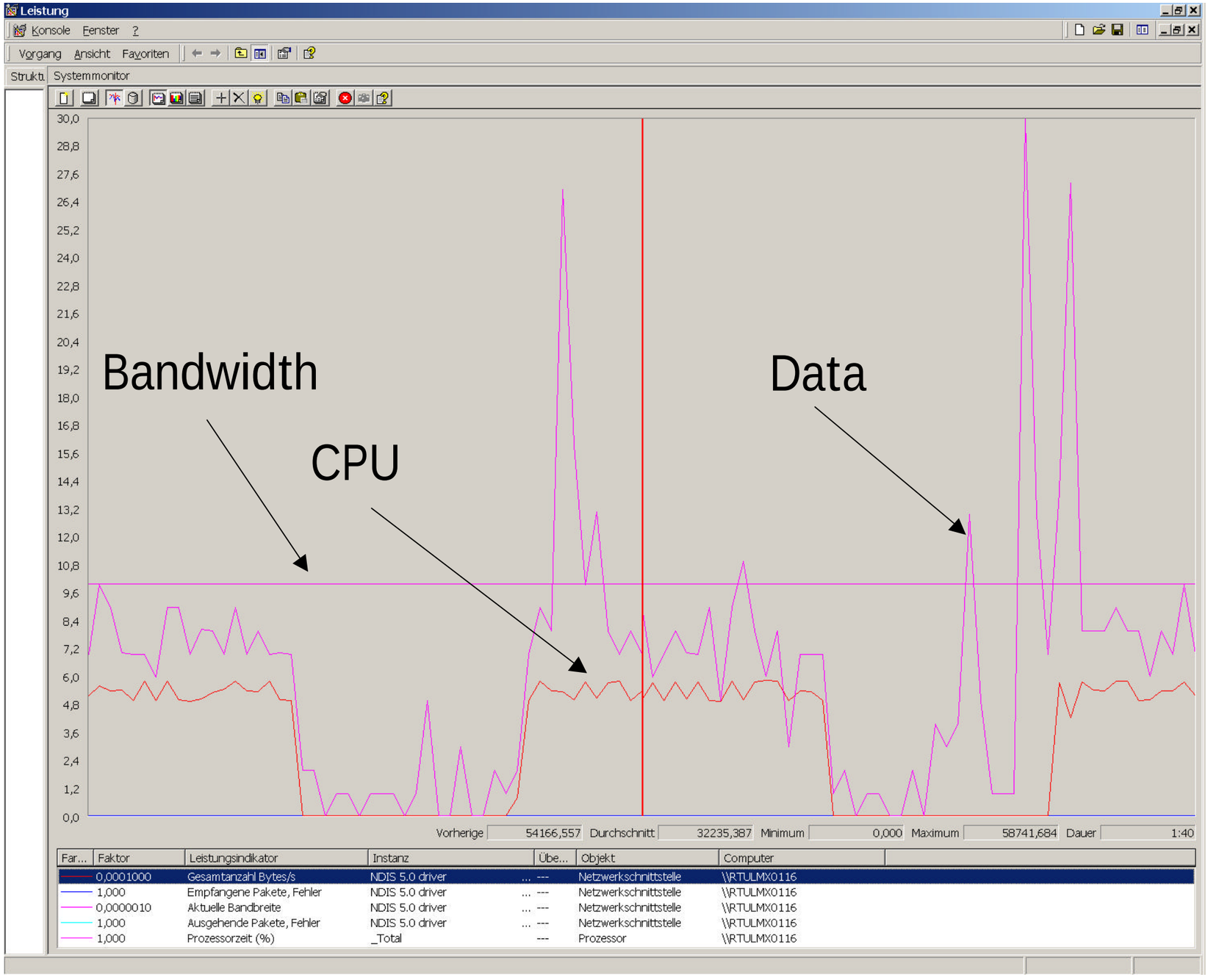
Considerations:

1. No Usage of SOAP Implementations which make use of programming languages‘ reflection mechanisms!
2. No usage of well known WWW ports
3. Consideration of SOAP communication semantics
4. Inspection of TCP traffic (e.g. the window size)
5. IP based (basic) authentication
6. Authentication and authorization via SOAP Content
   (e.g. WS-Security compliant signature and encryption header)
7. XML agnostic check of Body content
   (regular expressions)
8. XML based validation (use of (restrictive) XML Schema)

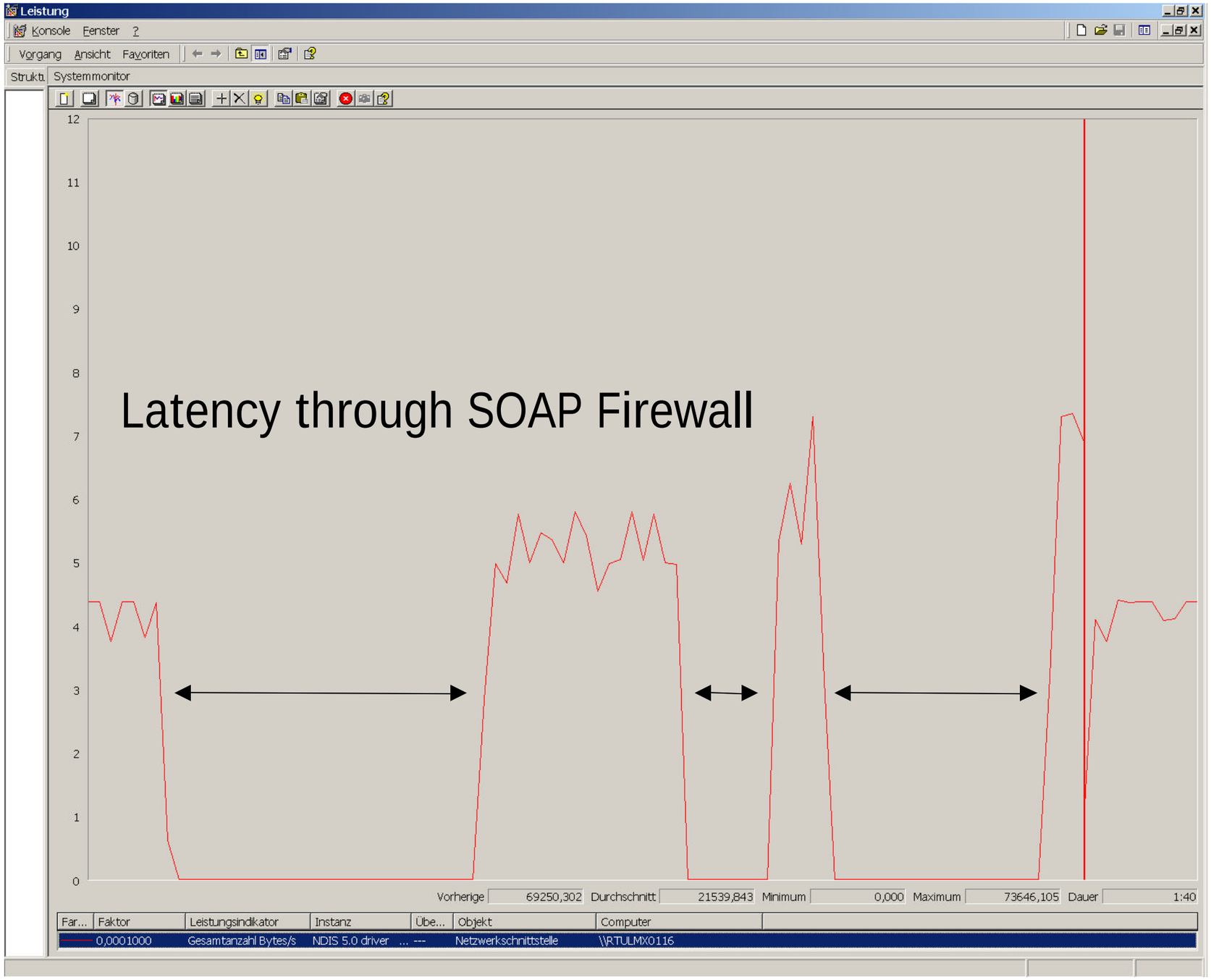
"SOAP-Firewalls"

- Currently: Idea or vision
- Scarcely (mature) products
- Integration into existing XML security standards desirable
- Essential decision:
  - Extension of a "classical" firewall
  - Additional firewall (layer)

Experience with "SOAP-Firewalls" – Server Side



Experience with "SOAP-Firewalls"– Client Side



jeckle.de - Mozilla

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop http://www.jeckle.de/ Print

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 Mitgliederverwaltun

jeckle.de

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

Applet tinyType started