Dienste und Anwendungen

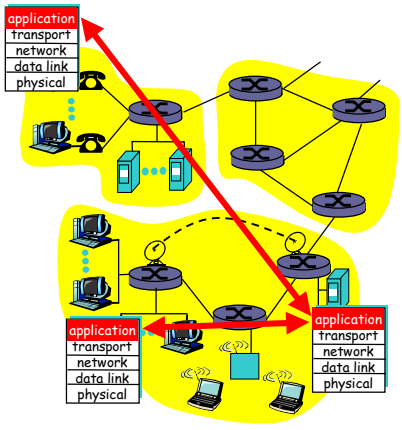
Kapitel 9

Dienste und Anwendungen

Kapitel: 9.1:
Internet-Dienste

Applications and application-layer protocols (1)

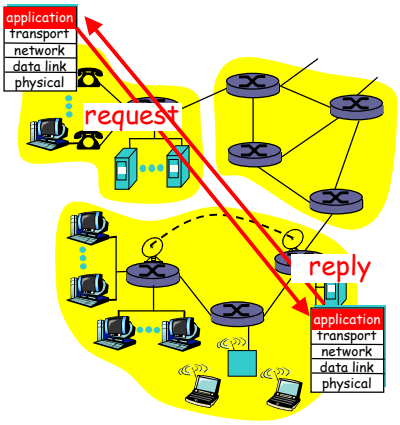
- Application: communicating, distributed processes
  - running in network hosts in "user space"
  - exchange messages to implement app
  - e.g., email, file transfer, the Web
- Application-layer protocols
  - one "piece" of an app
  - define messages exchanged by apps and actions taken
  - user services provided by lower layer protocols



Client-server paradigm

Typical network app has two pieces: client and server

- Client:
  - initiates contact with server ("speaks first")
  - typically requests service from server,
  - e.g.: request WWW page, send email
- Server:
  - provides requested service to client
  - e.g., sends requested WWW page, receives/stores received email



Application-layer protocols (2)

API: application programming interface

- defines interface between application and transport layer
- socket: Internet API
  - two processes communicate by sending data into socket, reading data out of socket

Q: how does a process "identify" the other process with which it wants to communicate?

- IP address of host running other process
- "port number" - allows receiving host to determine to which local process the message should be delivered

What transport service does an app need?

Data loss

- some apps (e.g., audio) can tolerate some loss
- other apps (e.g., file transfer, telnet) require 100% reliable data transfer

Bandwidth

- some apps (e.g., multimedia) require minimum amount of bandwidth to be “effective”
- other apps (“elastic apps”) make use of whatever bandwidth they get

Timing

- some apps (e.g., Internet telephony, interactive games) require low delay to be “effective”

Anforderungen ausgewählter Anwendungen

Anwendung	Datenverlust	Bandbreite	zeitsensitiv
Filetransfer	Kein Verlust	Elastisch	Nein
E-Mail	Kein Verlust	Elastisch	Nein
Web-Dokumente	Kein Verlust	Elastisch (wenige Kbps)	Nein
Echtzeitaudio/-video	Verlusttolerant	Audio: wenige Kbps bis 1 MB Video: 10 KB bis 5 MB	Ja, einige hundert Millisekunden
Gespeichertes Audio/Video	Verlusttolerant	wie oben	Ja: wenige Sekunden
Interaktive Spiele	Verlusttolerant	Wenige Kbps bis 10 KB	Ja: einige hundert Millisekunden
Finanzanwendungen	Kein Verlust	Elastisch	Ja und nein

Services provided by Internet transport protocols

TCP service:

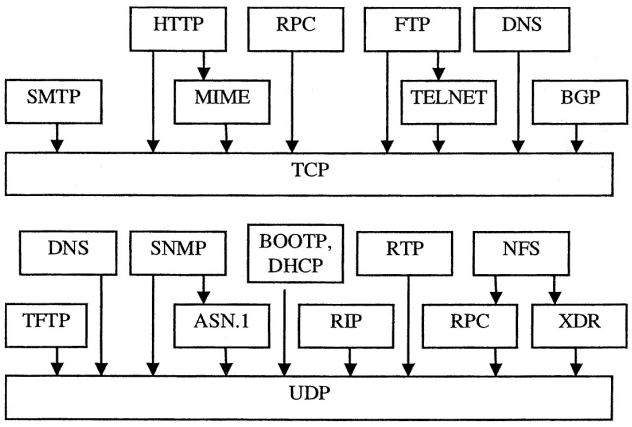
- connection-oriented: setup required between client, server
- reliable transport between sending and receiving process
- flow control: sender won't overwhelm receiver
- congestion control: throttle sender when network overloaded
- does not providing: timing, minimum bandwidth guarantees

UDP service:

- unreliable data transfer between sending and receiving process
- does not provide: connection setup, reliability, flow control, congestion control, timing, or bandwidth guarantee

Q: why bother? Why is there a UDP?

Internet-Dienste: Überblick



Verzeichnisdienste: Directories

- DNS (Domain Name System)
  - RFC 1034/5
  - dient der Abbildung von Endsystemen auf IP-Adresse
- X.500 Directory
  - Konzept der ITU-T für ein verteiltes Directory, einschließlich Verschlüsselung und Zertifizierung
- LDAP (Lightweight Directory Access Protocol)
  - RFC 1959, 2251
  - ist ein Zugriffsprotokoll für Directories gemäß X.500
  - ist weniger aufwending als OSI X.500-DAP
  - LDAP wird ergänzt durch LIPS (Lightweight Internet Person Schema) und LDIF (Lightweight Directory Interchange Format)

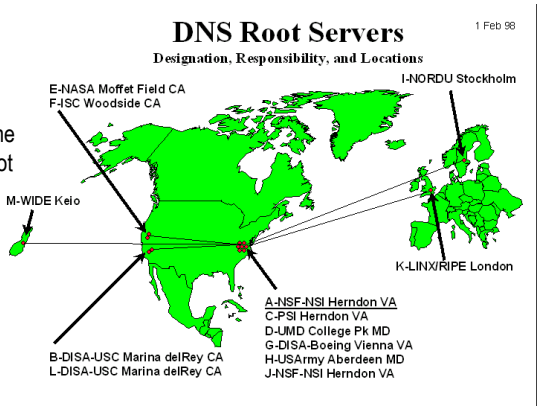
DNS (1): Domain Name System

- verteilte, in einer Hierarchie von Name Servern implementierte Datenbank und Protokoll der Anwendungsschicht zwischen Hosts und Name Servern
- Dienste:
  - Abbildung von Host-Namen auf IP-Adressen
  - Host Aliasing (mnemonisch - kanonisch)
  - Mail Server Aliasing
  - Lastverteilung zw. replizierten Servern
- DNS ist kritisch für das Funktionieren vom Internet

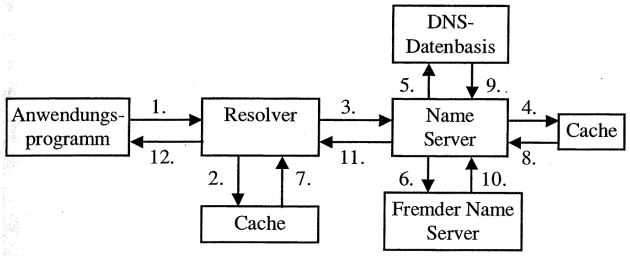
  Problem: Bottleneck, Verkehrsvolumen, Entfernung, Pflege
- Wegen Skalierung Hierarchie von DNS-Servern:
  - Lokaler Name Server, autorisierter Name Server, Root Name Server, vermittelnder Name Server

DNS (2): Root name servers

- contacted by local name server that can not resolve name
- root name server:
  - contacts authoritative name server if name mapping not known
  - gets mapping
  - returns mapping to local name server
- ~ dozen root name servers worldwide



DNS (3): Domain Name System

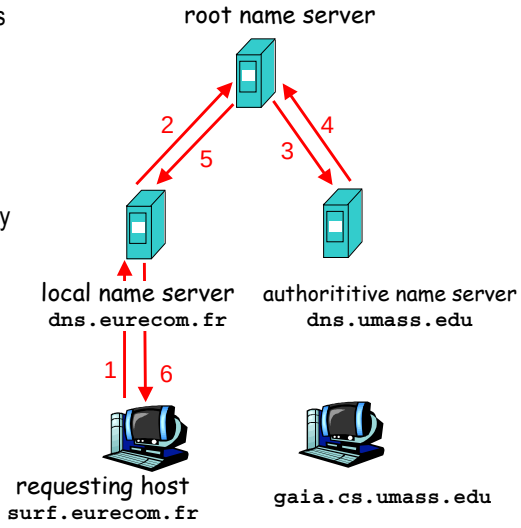


1. Anfrage an Resolver
2. Anfrage an Cache, falls positiv weiter mit 7, 12
3. Anfrage an Server
4. Anfrage an Cache, falls positiv weiter mit 8, 11, 12
5. Anfrage an Datenbasis, falls positiv, weiter mit 9, 1, 12
6. Anfrage an fremden Name Server, Antwort über 10, 11, 12

DNS (4): Simple DNS example

host `surf.eurecom.fr` wants IP address of `gaia.cs.umass.edu`

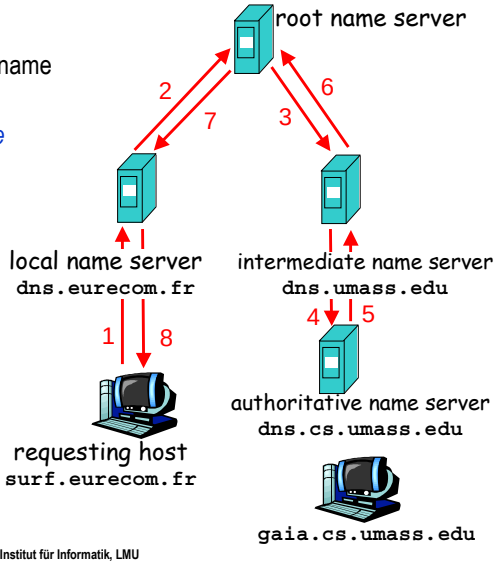
1. Contacts its local DNS server, `dns.eurecom.fr`
2. `dns.eurecom.fr` contacts root name server, if necessary
3. root name server contacts authoritative name server, `dns.umass.edu`, if necessary



DNS (5): example

Root name server:

- may not know authoratiative name server
- may know *intermediate name server:* who to contact to find authoritative name server



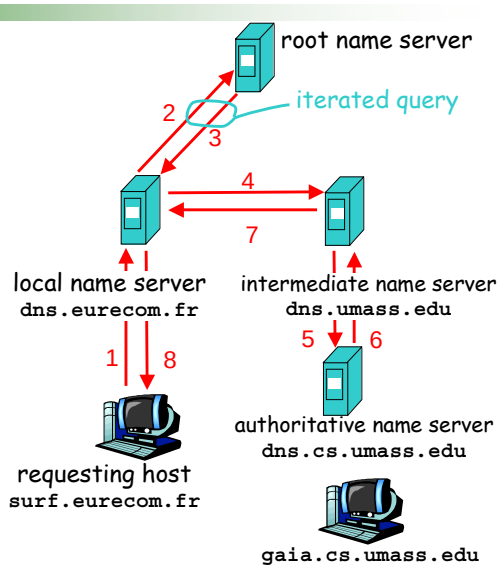
DNS (6): iterated queries

recursive query:

- puts burden of name resolution on contacted name server
- heavy load?

iterated query:

- contacted server replies with name of server to contact
- "I don't know this name, but ask this server"



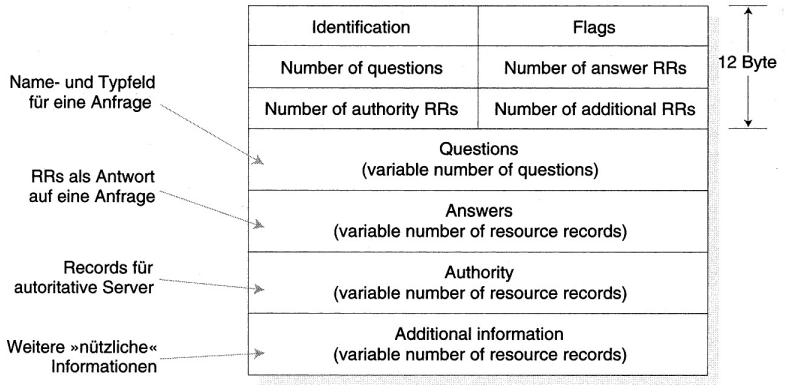
DNS (7): caching and updating records

- once (any) name server learns mapping, it caches mapping
  - cache entries timeout (disappear) after some time
- update/notify mechanisms under design by IETF
  - RFC 2136
  - http://www.ietf.org/html.charters/dnsind-charter.html

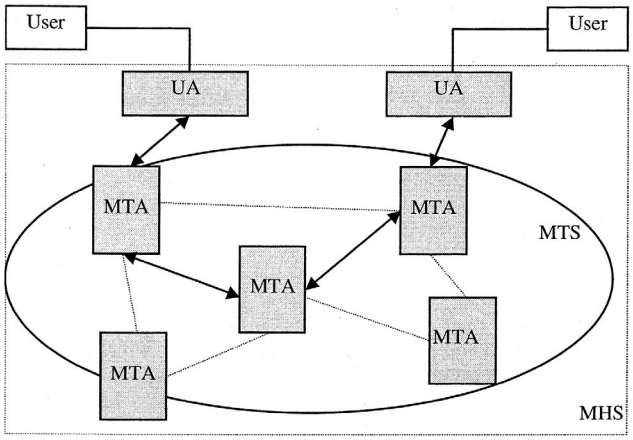
DNS (8): Resource Record

- Resource Record: (Name, Wert, Typ, TTL)
  - Typ=A: Name = Host, Wert = IP-Adresse
  - Typ=NS: Name = Domain, Wert = Hostname eines autor. Servers
  - Typ=CNAME: Wert = kanonischer Name für Alias Hostname
  - Typ=MX: Wert = Hostname eines Mailservers mit Aliasnamen
- DNS-PDU:
  - Identification: Anfrage ID
  - Flags: Query/Reply, Autoritative Bit, Recursion Desired, Recursion available
  - Number of: Längenfelder
  - Felder enthalten Resource Records

DNS (9): Format von DNS-Nachrichten



Message Handling Systeme (1)



Message Handling Systeme (2)

Begriffe aus der Internet-Welt

SMTP: Protokoll für den Transfer von E-Mail zwischen Mail-Servern, nutzt TCP und IP-Adressen.

Mail Server (Post Office): Server, der SMTP nutzt.

POP (Post Office Protocol): Protokoll zur Kommunikation zwischen Mail Server und Mail Client.

IMAP (Internet Message Access Protocol) : Nachfolger von POP.

Begriffe aus der OSI- bzw. ITU-T-Welt

X.400: Norm der ITU-T für E-Mail.

MOTIS (Message-Oriented Text Interchange System): ISO-Standard (ISO 10021) für E-Mail. Entspricht X.400.

MHS (Message Handling System): bezeichnet das Gesamtsystem aus MTS, MTA, UA.

MTS (Message Transfer System): die Menge aller MTAs.

MTA (Message Transfer Agent): entspricht dem Mail Server.

UA (User Agent): entspricht dem Mail Client.

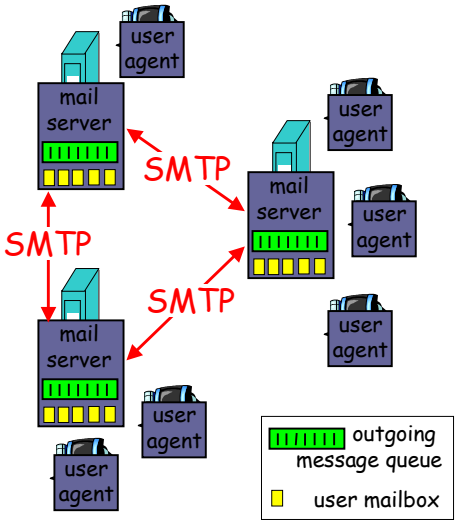
Electronic Mail: User Agent

Three major components:

- user agents
- mail servers
- simple mail transfer protocol: smtp

User Agent

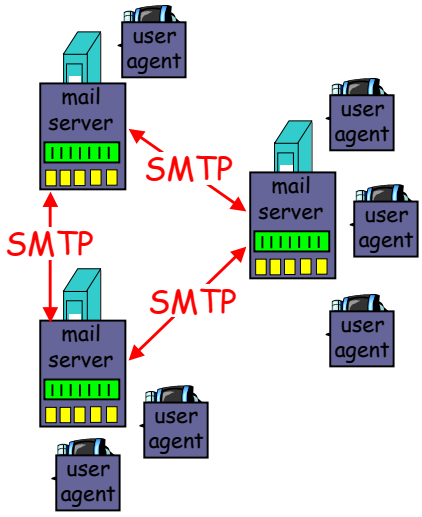
- a.k.a. “mail reader”
- composing, editing, reading mail messages
- e.g., Eudora, pine, elm, Netscape Messenger
- outgoing, incoming messages stored on server



Electronic Mail: mail servers

Mail Servers

- mailbox contains incoming messages (yet to be read) for user
- message queue of outgoing (to be sent) mail messages
- smtp protocol between mail server to send email messages
  - client: sending mail server
  - “server”: receiving mail server



Electronic Mail: Protokolle

- Zwischen Mailservern: SMTP (Push-Protokoll)
  - in RFC 822 ausschließlich ASCII-Text
  - in RFC 2045/6 Erweiterung auf MIME (Binärdaten)
- Zugangsprotokolle (zwischen User Agent und Mailservern)
  - IMAP (Internet Mail Access Protocol)
  - POP3 (Post Office Protocol)
  - HTTP (Hypertext Transfer Protocol) für browserbasierte Emaildienste

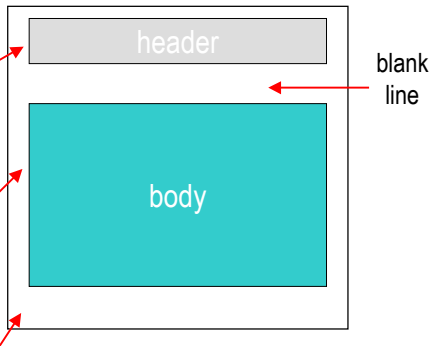
Electronic Mail: smtp [RFC 821]

- uses tcp to reliably transfer email msg from client to server, port 25
- direct transfer: sending server to receiving server
- three phases of transfer
  - handshaking (greeting)
  - transfer
  - closure
- command/response interaction
  - commands: ASCII text
  - response: status code and phrase

Mail message format

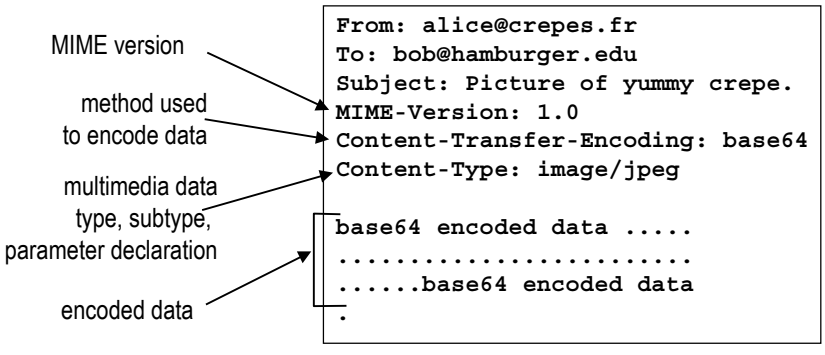
- smtp: protocol for exchanging email msgs
- RFC 822: standard for text message format:
- header lines, e.g.,
  - To:
  - From:
  - Subject:

  different from smtp commands!
- body
  - the "message", ASCII characters only
- line containing only `.'



Message format: multimedia extensions

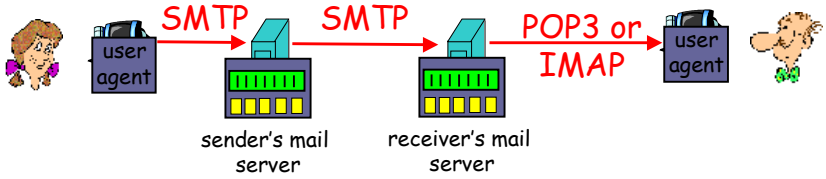
- MIME: multimedia mail extension, RFC 2045, 2056
- additional lines in msg header declare MIME content type



MIME (Multi-purpose Internet Mail Extension)

Content Type	Bedeutung
Application	Nicht näher spezifizierte binäre Datei, Daten für ein Programm. **Subtypen:** Octet Stream (Bytefolge) und Postscript.
Audio	Sprache, Musik, Geräusche. **Subtyp:** Basic.
Image	Festbild oder Grafik. **Subtypen:** GIF, JPEG.
Message	Eine vollständige E-Mail-Nachricht oder eine Referenz auf die Nachricht (Angabe einer Datei auf einem FTP-Server). **Subtypen:** RFC 822 (nach RFC 822 codiert), Partial (Nachricht wurde für die Übertragung aufgeteilt) und External-body (Nachricht auf Server abgelegt).
Multipart	Mehrteilige Nachricht, jeder Teil hat sein eigenes Content Type und Content Transfer Encoding. **Subtypen:** Mixed: unabhängige Teile mit jeweils eigenem Type und Encoding. Alternative: Dieselbe Nachricht, in verschiedenen Repräsentationen. Parallel: Teile müssen gleichzeitig dargestellt werden, z. B. zur Synchronisation von Bild und Sprache. Digest: Jeder Teil ist eine vollständige Nachricht nach RFC 822.
Text	Unformatierter oder formatierter Text. **Subtypen:** Plain, Richtext.
Video	Bewegtbild. **Subtyp:** MPEG.

Mail access protocols



- SMTP: delivery/storage to receiver's server
- Mail access protocol: retrieval from server
  - POP: Post Office Protocol [RFC 1939]
    - authorization (agent <-->server) and download
  - IMAP: Internet Mail Access Protocol [RFC 1730]
    - more features (more complex)
    - manipulation of stored msgs on server

POP3 protocol

authorization phase

- client commands:
  - user: declare username
  - pass: password
- server responses
  - `+OK`
  - `-ERR`

```
S: +OK POP3 server ready
C: user alice
S: +OK
C: pass hungry
S: +OK user successfully logged on
```

transaction phase, client:

- `list`: list message numbers
- `retr`: retrieve message by number
- `dele`: delete
- `quit`

```
C: list
 S: 1 498
 S: 2 912
 S: .
 C: retr 1
 S: <message 1 contents>
 S: .
 C: dele 1
 C: retr 2
 S: <message 1 contents>
 S: .
 C: dele 2
 C: quit
 S: +OK POP3 server signing off
```


WWW - World Wide Web (1)

- WWW besteht aus
  - Client: WWW-Browser
  - Server: WWW-Server
  - Objekte: Hypertext- und Hypermedia-Dokumente, Web-Seite
- Hypertext ist Text, der durch Links ergänzt wird

  Link ist Verweis auf andere Textstelle oder Dokument (Objekt)

  Link kann auf selbes Objekt, Objekt im selben Rechner, oder Objekt im Netz verweisen
- Hypermedia enthält zusätzlich zu Hypertext multimediale Anteile (Grafik, Video, Sprache), beschrieben mittels HTML (Hypertext Markup Language) oder Erweiterungen

WWW - World Wide Web (2)

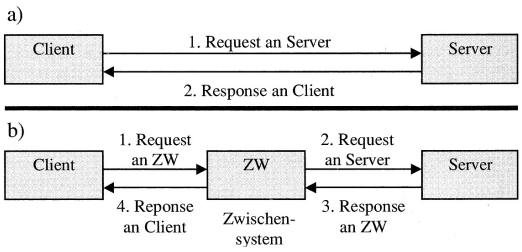
- URL (Universal Resource Locator) RFC 1738
  Lagerort eines Web-Dokuments durch Serverangabe und Pfadbezeichnung
- URN (Universal Resource Name)
  global eindeutiger langlebiger logischer Name für Objekt ohne Lagerort
- URI (Universal Resource Identifier) RFC 1630
  Objektbegriff für URL und URN

Aufbau einer URL

<Schema>:<schemaspezifischer Teil >	allgemeiner Aufbau einer URL
//<user>:<password>@ <host>:<port>/url-pfad>	schema-spezifischer Teil
http://<host>:<port>/<path><suchanfrage>	HTTP-URL
http://www.alfabeta.com/information/index.html (Transferprotokoll, Server, Verzeichnis, Dokument)	Bei-spiel

WWW - World Wide Web (3)

- HTTP (Hypertext Transfer Protocol) RFC 2068, 2616
  - Protokoll zum Transport von Anfragen/Objekten zwischen Browser, Server und Proxy
  - HTTP als Anwendungsprotokoll (Port 80) setzt auf TCP auf
  - HTTP ist zustandslos, pull-orientiert, unterstützt bidirektionale Übertragung und Caches im Browser bzw. Proxy



WWW - World Wide Web (4)

http: TCP transport service:

- client initiates TCP connection (creates socket) to server, port 80
- server accepts TCP connection from client
- http messages (application-layer protocol messages) exchanged between browser (http client) and WWW server (http server)
- TCP connection closed

http is "stateless"

- server maintains no information about past client requests

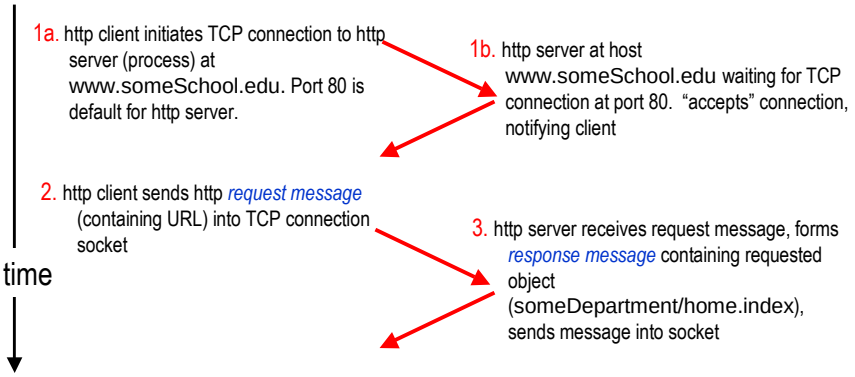
aside

Protocols that maintain "state" are complex!

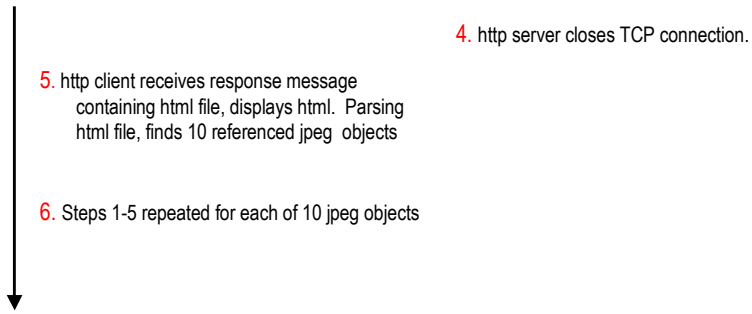
- past history (state) must be maintained
- if server/client crashes, their views of "state" may be inconsistent, must be reconciled

WWW - World Wide Web (5)

- Suppose user enters URL www.someSchool.edu/someDepartment/home.index (contains text, references to 10 jpeg images)



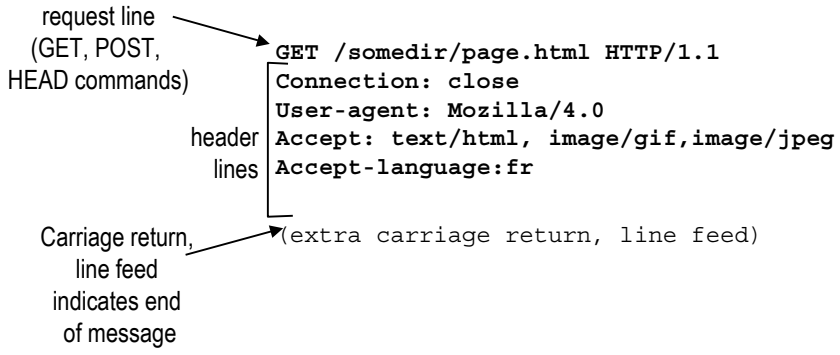
WWW - World Wide Web (6)



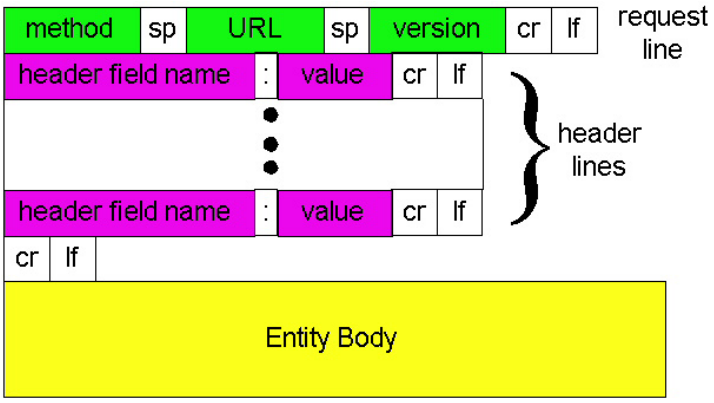
- non-persistent connection: one object in each TCP connection
  - some browsers create multiple TCP connections simultaneously - one per object
- persistent connection: multiple objects transferred within one TCP connection

WWW - World Wide Web (7)

- two types of http messages: *request, response*
- http request message:
  - ASCII (human-readable format)



http request message: general format



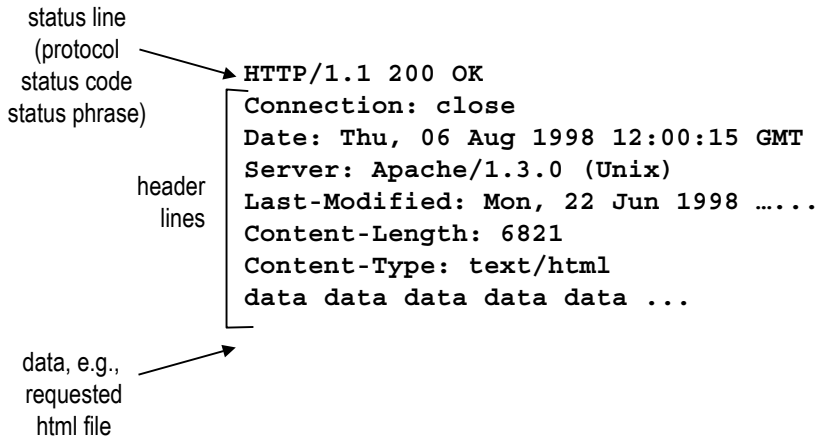
WWW - World Wide Web (8)

- Request-Methoden in HTTP 1.1

Methode	Bedeutung
GET	Mit GET ruft der Client die angegebene Internetadresse auf und holt dort die angegebene Datei vom Server.
HEAD	Mit HEAD holt der Client die Meta-Information zum angegebenen Dokument, nicht aber das Dokument selbst.
PUT *)	Mit PUT sendet der Client Informationen – in der Regel vollständige HTML-Dokumente – zum Server, wo sie abgelegt werden.
POST *)	Der Client sendet Daten an eine existierende URL auf dem Server. In der Regel sind dies Eingaben in Formulare, die vom Client mittels CGI an Server-Anwendungen übergeben werden sollen.
DELETE *)	Zum Löschen von Dokumenten auf dem Server. Voraussetzung ist, dass der Client entsprechende Rechte auf dem Server besitzt.
OPTIONS *)	Der Client kann Informationen über die innerhalb einer Request-Response-Kette möglichen Kommunikationsoptionen einholen.
TRACE *)	Ein Request wird vom Server so an den Client zurückgeschickt, wie er ihn empfangen hat. Für Testzwecke.

*) Optional. Die Methoden LINK, UNLINK wurden in HTTP 1.1 entfernt.

http message format: reply



WWW - World Wide Web (9)

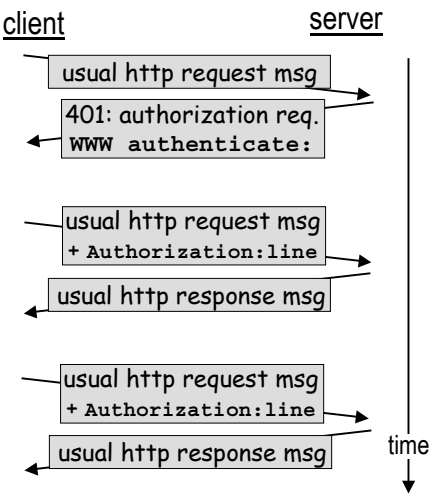
❑ HTTP Statuscodes (Ausschnitt) bei Antworten

Befehl	Erklärung
200	OK: Methode war erfolgreich.
201	Created: zusätzlicher Antwort-Header.
202	Accepted: Bestätigung für die verspätete Ausführung einer Methode.
203	Provisional Information: Nicht die Originalheaderversion; wenn Methoden von einem Proxy ausgeführt werden, wird Zusatzinformation in den Header geschrieben.
204	No Content: Methode war erfolgreich, jedoch keine Antwort im Rest der Response.
300	Multiple Choices: Der Server kann die angeforderte Information aus unterschiedlichen Dateien lesen.
301	Moved Permanently: Die angeforderte Seite ist umgezogen.
302	Moved Temporarily: Die angeforderte Seite ist vorübergehend umgezogen.
304	Not Modified: Nach dem im Header angegebenen Datum wurde nichts mehr an der Seite verändert.
400	Bad Request: Die Anforderung kann nicht ausgeführt werden.
401	Unauthorized: Client ist nicht berechtigt, auf diese Seite zuzugreifen.
402	Payment Required: zukünftiger Befehl für das elektronische Bezahlen einer Seite.
403	Forbidden: Ausführung der Methode verweigert.
404	Not Found: URL wurde nicht gefunden.
405	Method Not Allowed: Methode ist für diese Seite nicht erlaubt.
406	None Acceptable: Verarbeitung der Header ist nicht möglich.
407	Proxy Authentication Required: Proxies sollen verifiziert werden. Zukünftiger Befehl.
408	Request Timeout: Die Methode konnte innerhalb einer Zeitspanne nicht ausgeführt werden.
409	Conflict: Konflikt ensteht, wenn neuere Änderungen überschrieben werden.
410	Gone: Die gewünschte Seite ist nicht mehr vorhanden.
500	Internal Server Error: interner Serverfehler.
501	Not Implemented: Die Methode ist dem Server nicht bekannt.
502	Bad Gateway: Der Server hatte beim Versuch, auf einen anderen Server zuzugreifen, keinen Erfolg.
503	Service Unavailable: keine Möglichkeit die Methode im Moment auszuführen.
504	Gateway Timeout: Zeitspanne wurde überschritten beim Zugriff auf einen anderen Server.

User-server interaction: authentication

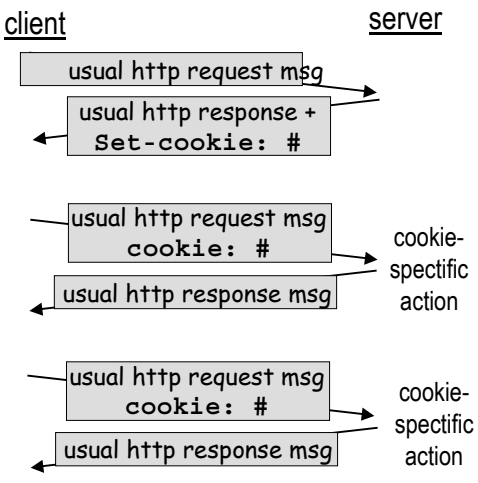
Authentication goal: control access to server documents

- stateless: client must present authorization in each request
- authorization: typically name, password
  - authorization: header line in request
  - if no authorization presented, server refuses access, sends `WWW authenticate:` header line in response



User-server interaction: cookies

- server sends "cookie" to client in response
- Set-cookie: #
- client present cookie in later requests
- cookie: #
- server matches presented-cookie with server-stored cookies
  - authentication
  - remembering user preferences, previous choices

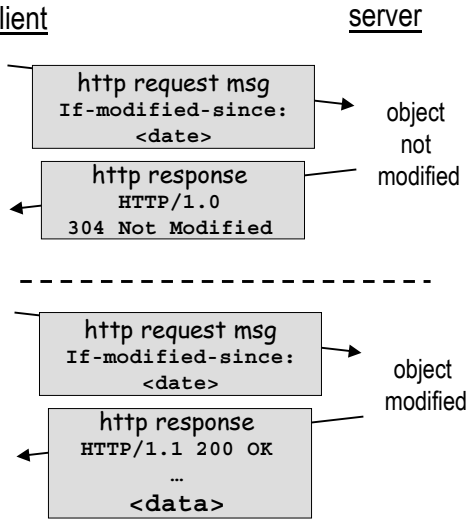


User-server interaction: conditional GET

- Goal: don't send object if client has up-to-date stored (cached) version
- client: specify date of cached copy in http request

  `If-modified-since: <date>`
- server: response contains no object if cached copy up-to-date:

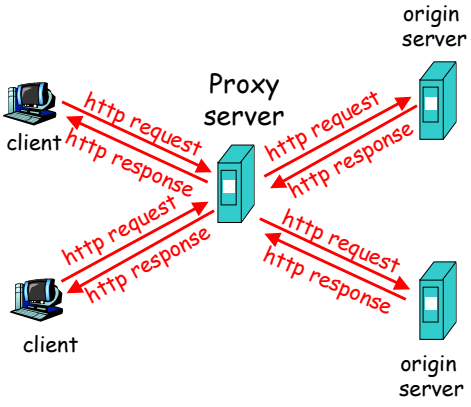
  `HTTP/1.0 304 Not Modified`



Web Caches (proxy server)

Goal: satisfy client request without involving origin server

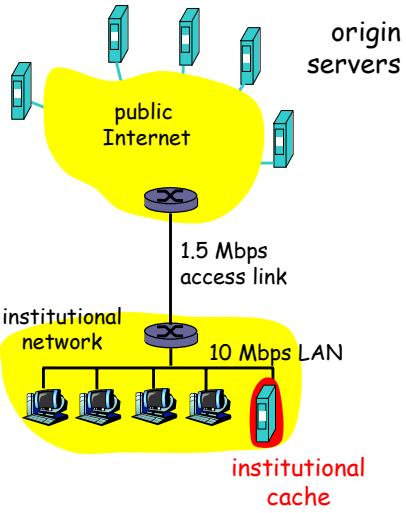
- user sets browser: WWW accesses via web cache
- client sends all http requests to web cache
  - if object at web cache, web cache immediately returns object in http response
  - else requests object from origin server, then returns http response to client



Why WWW Caching?

Assume: cache is “close” to client (e.g., in same network)

- ❑ smaller response time: cache “closer” to client
- ❑ decrease traffic to distant servers
  - link out of institutional/local ISP network often bottleneck

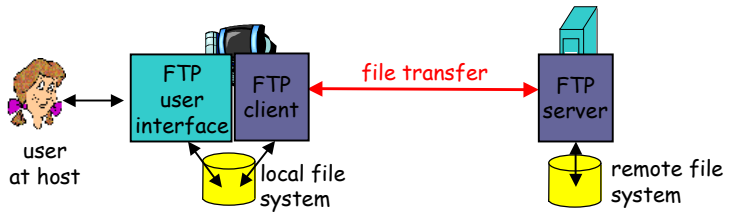


WWW - World Wide Web (10)

HTML (Hypertext Markup Language)

- ❑ Beschreibungssprache für Web-Dokumente mittels Markups (Tags) in Bezug auf Struktur und Layout
- ❑ HTML-Dokumente bestehen aus Header und Body. Neben Fließtext können Tabellen (tables) und Formulare (forms) verwendet werden. Links in Dokumenten werden durch Anker (anchor) angegeben, die eine URL enthalten.
- ❑ Es gibt mehr als 80 Tags (grundlegende, in Header, für Tabellen, Dokumentteiler, Textformatierungen, Links, Bilder, Formulare, Listen, Frameelement)
- ❑ CSS (Cascading Style Sheet): zur Präzisierung von Formatvorgaben
- ❑ Weitere Markup-Sprachen: SGML, XML, XHTML, VRML

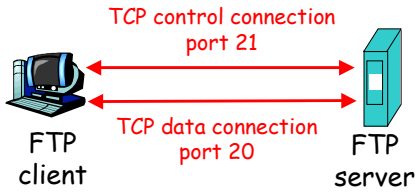
FTP (1): the file transfer protocol



- transfer file to/from remote host
- client/server model
- *client:* side that initiates transfer (either to/from remote)
- *server:* remote host
- ftp: RFC 959
- ftp server: port 21

FTP (2): separate control, data connections

- ftp client contacts ftp server at port 21, specifying TCP as transport protocol
- two parallel TCP connections opened:
  - *control:* exchange commands, responses between client, server.
    "out of band control"
  - *data:* file data to/from server
- ftp server maintains "state": current directory, earlier authentication



FTP (3): commands, responses

Sample commands:

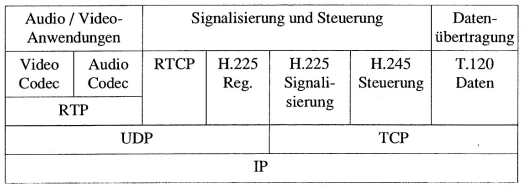
- sent as ASCII text over control channel
- `USER username`
- `PASS password`
- `LIST` return list of file in current directory
- `RETR filename` retrieves (gets) file
- `STOR filename` stores (puts) file onto remote host

Sample return codes

- status code and phrase (as in http)
- `331 Username OK, password required`
- `125 data connection already open; transfer starting`
- `425 Can't open data connection`
- `452 Error writing file`

Weitere Anwendungen

- Telnet RFC 854 - 861
- Usenet (Diskussionsforum) benutzt NNTP (Network News Transfer Protocol) RFC 1036
- IRC (Internet Relay Chat) Diskussionsforum in Echtzeit, RFC 1459
- eBusiness
- Groupware
  - Audio- u. Videokonferenzen, CSCW-Systeme



Application-Layer: Summary

- typical request/reply message exchange:
  - client requests info or service
  - server responds with data, status code
- message formats:
  - headers: fields giving info about data
  - data: info being communicated
- control vs. data msgs
  - in-based, out-of-band
- centralized vs. decentralized
- stateless vs. stateful
- reliable vs. unreliable msg transfer
- "complexity at network edge"
- security: authentication

Fragen zu Kapitel 9.1

- Ohne welche zusätzliche Internetanwendung funktionieren Mail, Filetransfer, Web nicht?
- Worin unterscheidet sich die Nutzung der Socket-Dienstschnittstelle für Anwendungen bei der Nutzung von TCP oder UDP
- Welche Haupt-Bausteine machen ein Email-System aus? Welche Protokolle werden zwischen den Bausteinen benutzt?
- Welche Hauptkomponenten machen ein Web-System aus?
- Wie ist eine URL aufgebaut?
- Realisieren SMTP bzw. HTTP ein Push oder Pull-Modell?
- Jeder Internet-Host hat mindestens einen lokalen und einen autorisierten Name-Server. Welche Rolle spielt jeder dieser Server im DNS?

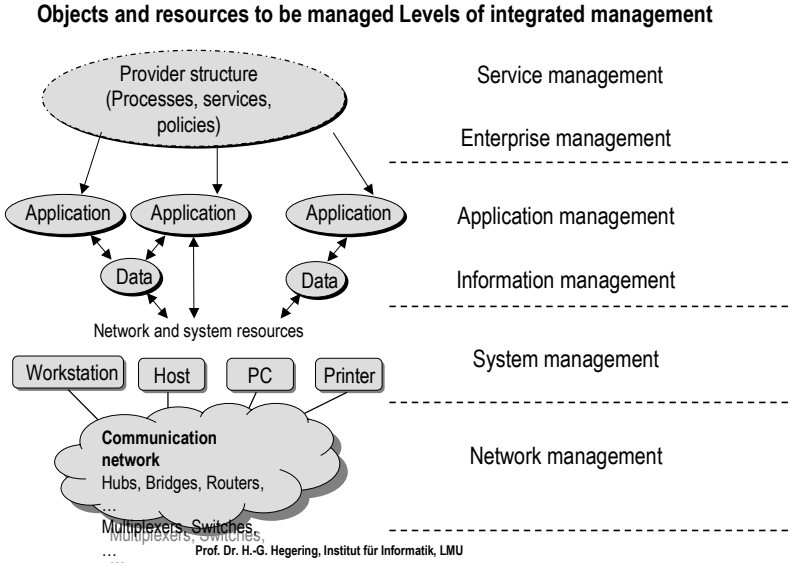
Dienste und Anwendungen

Kapitel: 9.2:
Internet Management

Warum Management ?

- Bisher nur Nutzungsfunktionalität in Form von Protokollen und Diensten besprochen
- Ein Netz und seine Dienste müssen aber mit konkreten Ressourcen, mit steuerbaren Dienstgüten, in konkreten Organisationen und mit belastbaren Zielvereinbarungen betrieben werden.
- Managementobjekte sind u.a. Verbindungen (auf jeder Schicht), Koppelelemente auf verschiedenen Schichten wie z.B. Hubs, Bridges, Switches, Router, Gateways, Multiplexer, ferner Protokollinstanzen, Endsysteme, Softwarekomponenten, Dienste, Anwendungen
- Zielvorgaben: Verfügbarkeit, Zuverlässigkeit, Sicherheit, Durchsatz, Reaktionszeiten, Lastausgleich, Kosten

Umfeld für kooperative IT-Infrastruktur



Netz-/Systemmanagement

- Gesamtheit aller Vorkehrungen und Aktivitäten zur Sicherstellung eines effektiven Einsatzes eines verteilten Systems und seiner Dienste bzw. Anwendungen
- Management ist betriebszielorientiert
- Management umfasst Personal, Verfahren, Programme, techn. Systeme
- Management betrifft Planung, Betrieb, Kontrolle, Einbettung in Organisationsformen

Netzmanagementdienste

- Benutzerverwaltung, Abrechnungsmanagement
- Sicherheitsmanagement
  (Bedrohungsanalyse, Sicherheitsmechanismen, Verschlüsselung, Authentifizierung, Zertifizierung)
- Fehlermanagement
  (Symptomerfassung, Eventkorrelation, Fehlerdiagnose, Fehlerbehebung, TT-Systeme)
- Konfigurationsmanagement
  (Generieren und Installieren von Systemen, Parameterfestlegung, Statusüberwachung, Versionsverwaltung, SW-Verteilung, Topologieplanung)
- Leistungsmanagement
  (Leistungsmessung, QoS-Parameter, Engpassanalysen, Auslastung, Kapazitätsplanung)
- Ressourcenmanagement (z.B. Bandbreiten, Wege)

Konfigurationsmanagement

- Konfigurieren heißt Anpassen von Systemen an Betriebsumgebungen
  - Neuinstallation von HW- und SW-Komponenten
  - Anpassen von SW:
    - patches, update, neue Versionen
  - Topologieänderungen bei Verbindungen und Geräten
  - Einstellen von Parametern
    - (Funktions-, Berechtigungs-, Last-, Protokoll-, Dienstgüte-, Anschlußparameter)

Fehlermanagement

- Überwachen des Netz-, System-, und Anwendungszustandes
- Entgegennehmen und Verarbeiten von Alarmen
- Feststellen von Fehlerfortpflanzungen / Eventkorrelation
- Diagnostizieren von Fehlerursachen
- Einleiten und überprüfen der Fehlerbehebung
- Betrieb eines Trouble Ticket Systems
- Führen eines User Help Desk

Leistungsmanagement

- Bestimmen von Dienstgüteparametern und Metriken
- Überwachen aller Ressourcen auf Leistungsengpässe
- Durchführen von Messungen
- Auswerten von History Logs
- Aufbereiten von Messdaten und Verfassen von Leistungsberichten
- Leistungsvorhersagen und Simulation
- Leistungs- und Kapazitätsplanung

Netzparameter für QoS

❑ Bandbreite	• access speed - bit rate • abhängig von der Übertragungstechnik
❑ Verzögerung	• access delay + transmission delay • = network transit delay (end-to-end delay)
❑ Delay Jitter	• Puffer- u. Bearbeitungszeiten in Knoten • Phasenschwankungen in Schwingkreisen • Temperaturabhängigkeit der Bauteile
❑ Fehlerraten	• Leitungsfehler, Paketfehler
❑ Synchronisation	• Bandbreite + Delay + Jitter

❑ Abhängig von der Verkehrssituation / Last

Abrechnungsmanagement, Benutzerverwaltung

- ❑ Namen- und Adressmanagement
- ❑ Autorisierung
- ❑ Accounting Management
  - Festlegen von Abrechnungsdaten
  - Erfassen von Verbrauchsdaten
  - Führen von Abrechnungskonten
  - Zuordnen Kosten zu Konten
  - Verteilen und Überwachen von Kontingenten
  - Führen von Verbrauchsstatistiken, Kundenprofilen
  - Festlegen von Abrechnungspolitiken und Tarifen

Beispiel: Web-Hosting (1)

- Abonnement-bezogene Parameter
  - Anzahl der einzurichtenden WWW Domänen
  - WWW Server (Anz. dedizierter Server, Anz. virtueller Server, Anz. v. Fremd-Werbe-Bannern)
  - Max. Datentransferrate im Monat
  - Max. verfügbarer Speicherplatz
  - Bandbreite der Anbindung an das Backbone
  - Max. Anz. der Benutzer für passwortgeschützte Seiten
  - Email: Max. Anzahl der Email-Aliases
  - Maximale Anz. gleichzeitiger Verbindungen
  - ...
- Nutzungsbezogene Parameter
  - Anz. der übertragenden Bytes/Pakete/Responses
  - Anzahl der Requests
  - Gesamtverweildauer (bezogen auf einen Nutzer)

Beispiel: Web-Hosting (2)

- Content-basiert
- FTP: Anzahl übertragener Bytes/Pakete, Content-basiert
- Email: Anz. geforwardeter Emails
- Dienstgüte:
  - Transaktionsdauer
  - Anzahl korrekt übertragener Responses
  - Anzahl der Verweise auf die Seite (Pflege von Suchmaschinen)
  - Downtime des Servers
- Management-bezogene Parameter
  - WWW Server (Detailgrad d. Statistiken, Anz. der Aktualisierungen)
  - WWW Seiten (Anzahl der WWW Seiten Updates durch den Kunden, Aufsatz für Web-Tools (z.B. Front-Page))
  - Sicherheit: Anz. Zertifikatgeschützter WWW Seiten, Gesamtanzahl der verwalteten Zertifikate, Anz. Neuausgestellter Zertifikate
  - ...

Sicherheitsmanagement: Teilaufgaben

- Durchführung von Bedrohungsanalysen
- Festlegung und Durchsetzen von Sicherheitspolitiken
- Überprüfen von Autorisierungen
- Feststellen einer Identität (Authentifizierung, Signaturen, Zertifizierung)
- Durchführen einer Zugriffskontrolle
- Sicherstellung der Vertraulichkeit und Datenintegrität
- Überwachung auf Sicherheitsangriffe
- Berichterstattung zur Sicherheit

Sicherheitsmanagement: Bedrohungen

- Passive Angriffe
  - Abhören von Informationen
  - Erstellen eines Nutzerprofils
  - unerwünschte Verkehrsanalyse
- Aktive Angriffe
  - Maskerade
  - Manipulation von Nachrichtensequenzen
  - Modifikation von Nachrichten
  - Manipulation von Ressourcen
- Fehlfunktion
- Fehlbedienung

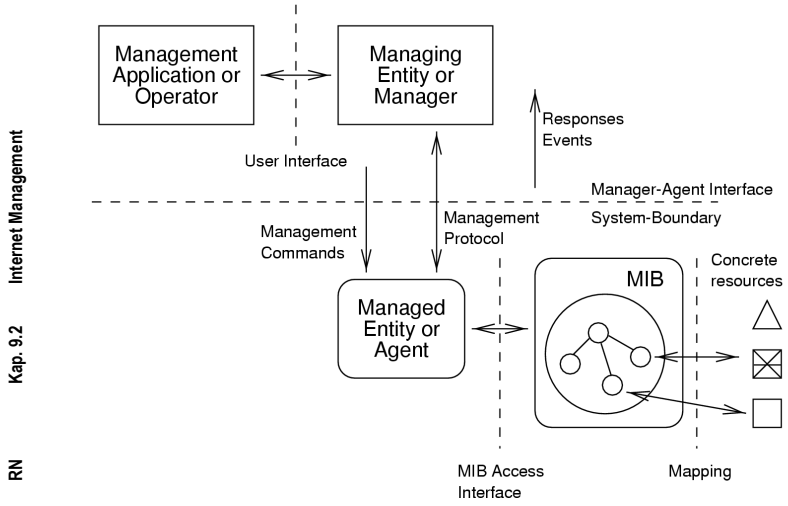
Control and Monitoring

- operational data: instantaneous information about resources
- error data: recording and monitoring of error events
- traffic and load data: device and connection related information
- performance data: analysis of thresholds, etc.
- security data: auditing, logging, etc.
- accounting data: service and resource utilization

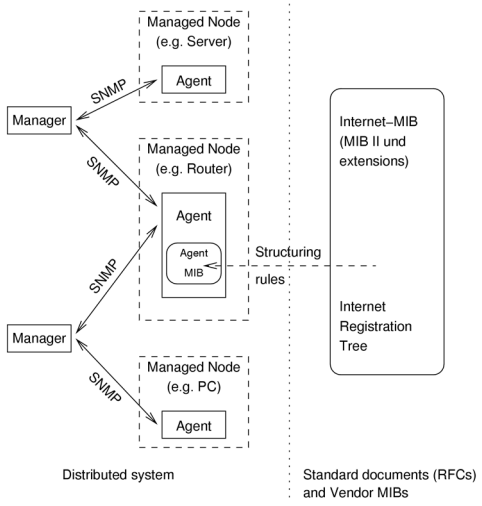
Weitere Managementfunktionen

- Inventory Management, Asset Management
- Service Management (creation, provisioning, subscribing, operation)
- Change Management
- Maintenance, Training, Logistics
- Informationsdienste
  - Allg. Informationsdienste (Blackboard)
  - Directory Services (yellow pages, mailing lists, distribution lists)
  - Dynamic information about users, resources, usage, etc.
  - Support and advice information (Hotline, CCC)

Management via MIB Manipulation



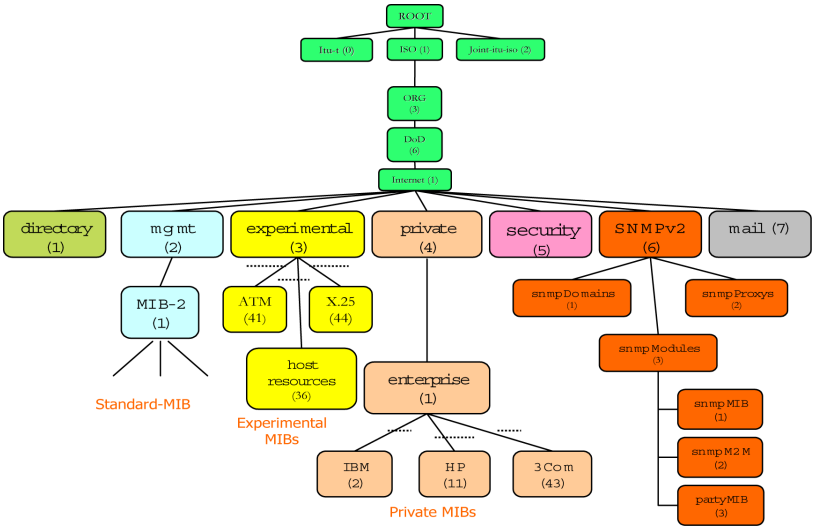
Internet-Architekturmodell und MIBs



Internet-Informationsmodell

- Modellansatz:
  - Datentypansatz
- Informationseinheiten:
  - einfache und zusammengesetzte Variable
- Informationseinheiten:
  - „managed objects“
    (trotz Fehlens eines objektorientierten Ansatzes)
- Identifizierung, Benennung der Objekte über den “Internet-Registrierungsbaum”
- RFC 1155: „Structure of Management Information“
  (bzw. RFC 1442 für Version 2 des Internet Management)

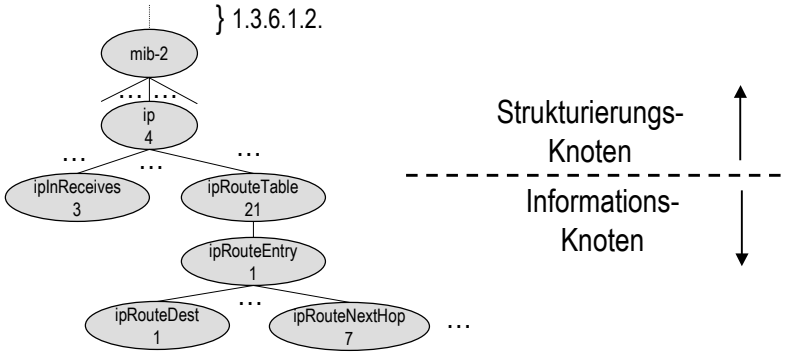
Internet Registrierungsbaum und Erweiterungen



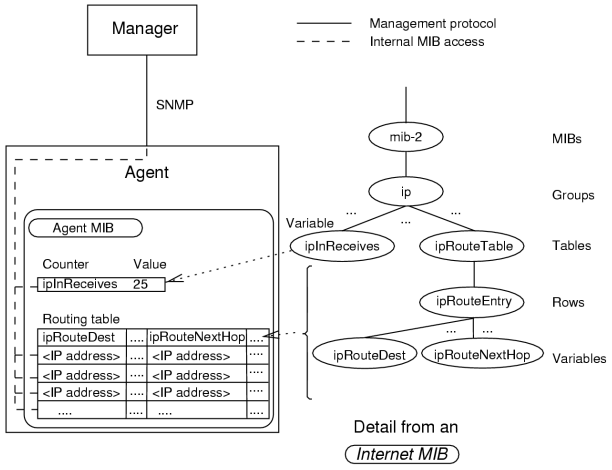
Knoten-Arten

- Zwei Arten von Knoten im Registrierungsbaum

(1) „Strukturierungs“-Knoten (2) „Informations“-Knoten



Agenten- und Internet-MIB



Syntax

- Syntax der Strukturierungsknoten

  mib-2 OBJECT IDENTIFIER : : = { iso(1) org(3) dod(6) internet(1) mgmt (2) 1 }

  ip OBJECT IDENTIFIER : : = { mib-2 4 }

- Syntax der Informationsknoten
  - ASN.1 – Makro OBJECT-TYPE

    <*Objektname*> **OBJECT-TYPE**

    SYNTAX <*Typangabe*>

    ACCESS <*Zugriffsmöglichkeiten*>

    STATUS <*Implementierungsanforderungen*>

    DESCRIPTION <*Informelle Semantik-Beschreibung*>

    : : = { <*Objektname des Vaterknotens*> <*laufende Nummer*> }
  - Simple Object Types → z.B. Zähler oder Zeichenreihe
  - Aggregate Object Types → Listen und Tabellen

Syntax: Beispiel

- Zähler ipInReceives

		Mögliche Wertebelegungen
ipInReceives	**OBJECT-TYPE**	
SYNTAX	Counter	Integer, Octet String, Object Identifier, Null, IpAddress, NetworkAddress, Counter, Gauge, Time Ticks, Opaque
ACCESS	read-only	read-write, write-only, not-accessible
STATUS	mandatory	optional, obsolete
DESCRIPTION		

„The total number of input datagrams received from interfaces, including those received in error.“

: : = { ip 3 }

Syntax: Beispiel

- Knotenart-Indikator ipForwarding

```
ipForwarding   OBJECT-TYPE

    SYNTAX     Integer { gateway (1),  -- entity forwards datagrams
                         host (2)      -- entity does NOT forward datagrams }

    ACCESS     read-only

    STATUS     mandatory
    DESCRIPTION
               „The indication of this entity is acting as an IProuter in respect to the
    forwarding of datagrams received by, but not addressed to, this entity.“
: : = { ip 1 }
```


Zusammengesetzte Objekte

- Listen und Tabellen
- Informelle Beschreibung einer Tabelle

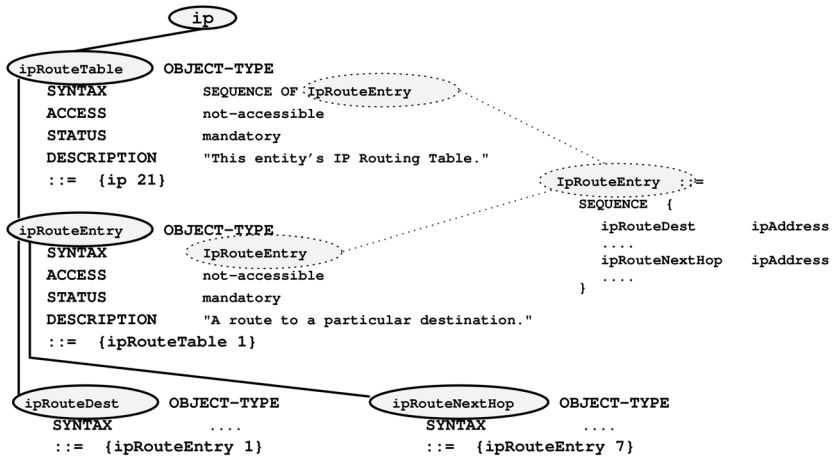
SEQUENCE OF { geordnete Liste beliebiger Länge von (gleichen) Tabellenzeilen,

SEQUENCE { wobei sich eine Tabellenzeile aus einer geordneten Liste fester Länge von einfachen Internet-Objekttypen ggf. unterschiedlichen Typs zusammensetzt

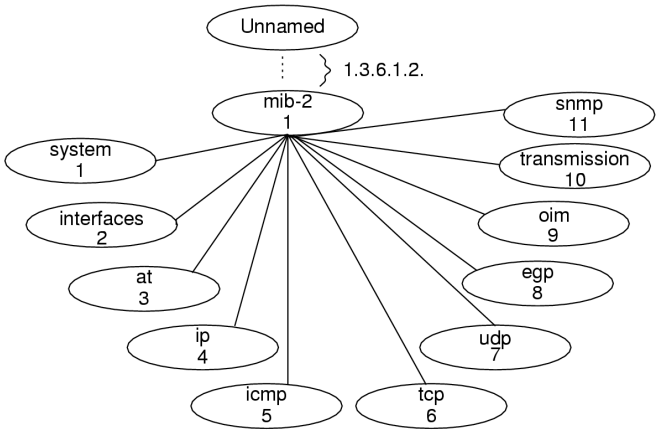
- Internet-Tabelle = SEQUENCE OF SEQUENCE (Einfacher Internet-Objekttyp 1 ... Einfacher Internet-Objekttyp N)

(Beliebig lange) Liste von — Tabellenzeilen

Beispiel: Tabelle



Internet MIB-II



The Internet-standard MIB-II (1)

- System Group
  - The system group must be implemented by all managed nodes, and contains generic configuration information:

System OBJECT IDENTIFIER :: = { mib 1 }

sysDescr:	description of device
sysObjectID:	identity of the agent software
sysUpTime:	how long ago the agent started
sysContact:	name of contact person
sysName:	device name
sysLocation:	device physical‘s location
sysServices:	services offered by devices

The Internet-standard MIB-II (2)

- Beispiel:

sysDescr	„4BSD/ISODE SNMP“
sysObjectID	1.3.6.1.4.1.4.1.2.1
sysUpTime	45366736
	(5 days, 6 hours, 1 minutes, 7.36 seconds)
sysContact	„Marshall Rose mrose@psi.com“
sysName	wp.psi.com
sysLocation	„Troy machine room“
sysServices	0x48 (transport, application)

The Internet-standard MIB-II (3)

- Interface Group (mandatory for all nodes)
  - Zahl der Interfaces, über die IP-Pakete kommen/gehen
  - Tabelle von Objekten für jedes Interface
    - Schnittstellenbeschreibung (Hersteller, Produkt, Version)
    - Typ (8.02.3/4/5, rfc 877-x25, lapb, T1, ...)
    - max IP-Paketlänge, Ü-Rate, Adresse
    - Status (up, down, testing)
    - diverse Zähler (received packets, faulty packets, …)
    - Länge Ausgabewarteschlange
    - …

Technologische MIBs (Experimental, Ausschnitt)

- LAN:
  - IEEE 802.3, 802.4, 802.5, 802.11, 802.12
  - Hub, Bridge
  - HIPPI, Fiber Channel
- MAN:
  - FDDI
- Internet:
  - PPP, OSPF, BGP, RSVP, IntServ, Diffserv, DNS
- WAN:
  - DS1/DS3, RS-232, SONET, SDLC, X.25, FR, ATM, SDMS,
- Sonstige:
  - Print, RDBMS

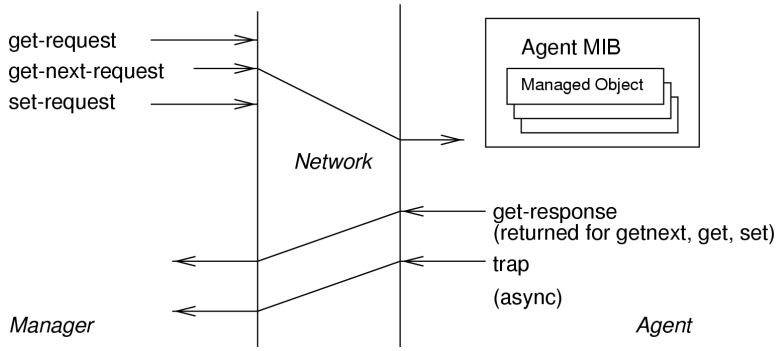
Internet MIBs für System und Application Mgmt.

- Host Resources MIB (RFC 1514)
- Mail Monitoring MIB (RFC 2249)
- X.500 Directory Monitoring MIB (RFC 1567)
- DNS Server/Resolver MIB Extensions (RFC 1611/12)
- Network Services Monitoring MIB (RFC 2248)
- Printer MIB (RFC 1759)
- Uninterruptable Power Supply MIB (RFC 1628)
- Relational Database Management System MIB (RFC 1697)
- System Application MIB (RFC 2287)
- Application Management MIB (RFC 2564)
- Application Performance Measurement MIB (Draft)
- WWW Service MIB (RFC 2594)

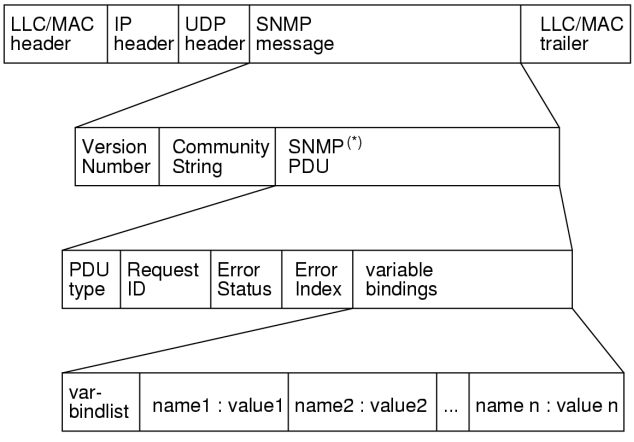
Internet-Kommunikationsmodell

- SNMP (Simple Network Management Protocol)
  - zentrale Bestandteil des Internet-Managements
    - Internet-Management = SNMP-Management
- Wesentliche Aufgabe von SNMP
  - Zugriff des Managers auf die vom Agenten bereitgestellte MIB (Get- und Set-Operation)
  - Informieren über Ereignisse, die im Agenten aufgetreten sind (Trap-Operation)

SNMP-Operationen



SNMP-Message Format



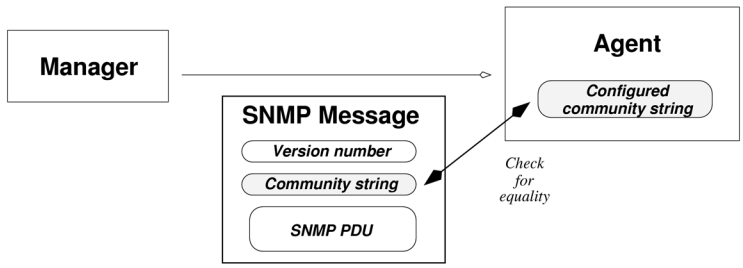
(*) Instead of a SNMP-PDU also a Trap-PDU may be contained in a SNMP-Message

Trap-PDU

- PDU-Type
  - 4
- Enterprise
  - OID des Trap erzeugenden Objekts
- Agent-address
  - Netzadresse des SNMP-Agenten
- Generic-trap
  - coldStart(0), warmStart(1),
  - linkDown(2), linkUp(3),
  - authenticationFailure(4),
  - egpNeighborLoss(5),
  - enterpriseSpecific(6)
- Specific-trap
  - weitere Informationen zu enterpriseSpecific
- Time-stamp
  - Zeit seit letzter Initialisierung
- Variable-bindings
  - Variablenwerte zum Trap

Internet Management: Communication model

- Security aspects: Community string (SNMPv1)



Internet Management: Communication model

- Security aspects: Community string (SNMPv1)
  - Mehrere Manager können auf einen Managed Node zugreifen
  - Community definiert Beziehung zwischen Agent und SNMP Application
  - Community Profile ist Paar aus MIB View und SNMP Access Rights
  - Authentifizierung über eindeutigen Community Name
  - Ermöglicht Festlegung administrativer Beziehungen zwischen SNMP Applikationen

aber: community strings werden ungesichert übertragen!

Wertung Internet-Management

- dominant in der Datenkommunikation
- sehr einfacher Ansatz in Bezug auf Informations- und Kommunikationsmodell
- Managementobjekte nur repräsentiert über Einfachvariable und Tabellen, ist zu simpel für die heutige Managementwelt
- Neuere Entwicklungen (Version2 und 3) erhöhen Übertragungssicherheit und Effizienz von SNMP und erweitern das Konzept in Richtung Funktionsmodell