Kapitel 3: Anwendungsschicht

3.1 Netzanwendungen

3.2 Web und HTTP (HyperText Transfer Protocol)

3.3 DNS (Domain Name System)

3.4 Weitere Anwendungsprotokolle

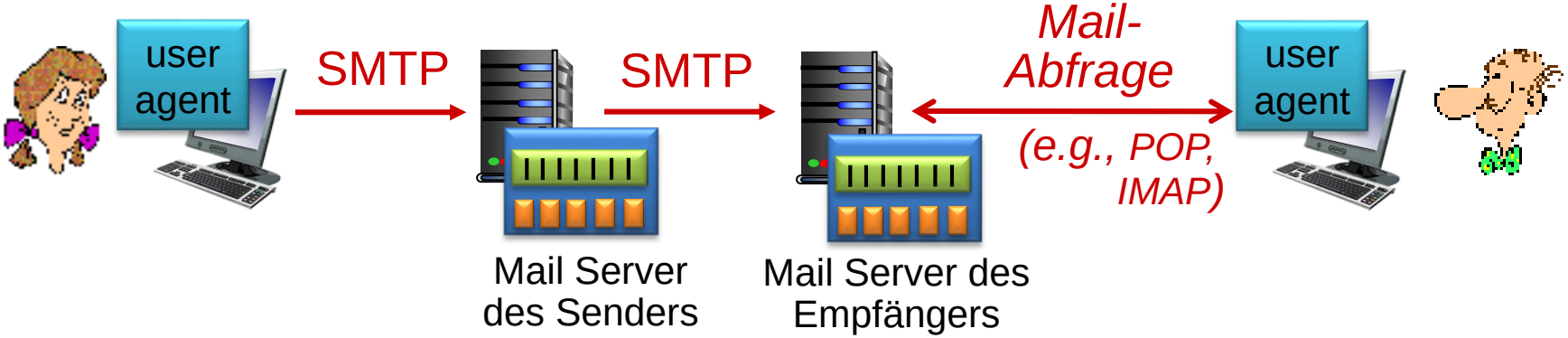
3.4.1 Mail-Protokolle

3.4.2 File Transfer Protocol (FTP)

3.5 Zusammenfassung

Mailprotokolle

- SMTP: Simple Mail Transfer Protokoll
  - Mail übertragen:
    - Mail Client zum Mail Server
    - Mail Server zu Mail Server
  - TCP Port 25
- STARTTLS: nutzt TLS auch auf „normalen“ Ports
  - Server signalisiert Client mit „STARTTLS“ Bereitschaft für TLS-Verbindung
- POP3: Post Office Protocol
  - Client holt Mail vom Mail-Server ab
  - TCP Port 110 (TLS: 993)
  - Aktionen: auflisten, abholen, löschen
- IMAP: Internet Mail Access Protocol
  - Client verwaltet Mail auf dem Server
  - Poll und Push (abrufen und benachrichtigen)
  - TCP Port 143 (TLS: 993)



SMTP

Prinzip: Kommando und Response

Test mit telnet -> Laborübung

Handshake evtl.
plus Authentisierung

Mail-Eingabe

Ende

```
S: 220 hamburger.edu
C: HELO crepes.fr
S: 250  Hello crepes.fr, pleased to meet you
C: MAIL FROM: <alice@crepes.fr>
S: 250 alice@crepes.fr... Sender ok
C: RCPT TO: <bob@hamburger.edu>
S: 250 bob@hamburger.edu ... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by
itself
C: Hallo!!!
   .
S: 250 Message accepted for delivery
C: QUIT
S: 221 hamburger.edu closing connection
```

IMAP

- Prinzip: Kommando und Response
- Test mit telnet -> Laborübung

- IMAP Kommandos:
  - login <username> <password> : authentisiert Nutzern
  - select <Mailordner> : setzt Mail-Ordner
  - fetch <Mail-Nummer> <Mail-Abschnitt> : lädt Abschnitt der Mail z.B. full, body[text], envelope
  - create <Mailordner> : legt neuen Mailordner an
  - delete < Mailordner> : löscht Mailordner
  - list "" "*" : listet alle Mailordnen
  - search <Suchkriterien> : listet Nummern der gefundenen Mails
  - copy <Mail-Nummer> <Mailbox> : kopiert Mail auf Server
  - close : beendet die Sitzung

Mail Sicherheit

- Wo liegen die Probleme?
  - Nutzer senden ihre Credentials einen Mail-Server
  - Mails enthalten vertrauliche Informationen, die sehr persönlich sein können oder sogar Credentials (Link zum Zurücksetzen des Passworts) enthalten können
    - Mails können natürlich auch auf Anwendungsebene verschlüsselt und zertifiziert werden, aber dafür benötigen die Anwender Zertifikate und müssen diese austauschen und benutzen
  - wir haben gelernt, dass z.B. über DNS Spoofing die Kommunikation an einen Fake-Mail-Server umgeleitet werden kann
    - ohne Authentisierung kennt dieser unser Passwort und unsere (unverschlüsselten) Mails
  - wenn es jemand schafft, den Datenverkehr mitzulesen, kennt sie unser Passwort und unsere (unverschlüsselten) Mails

Mail Sicherheit

- Abhilfe schafft TLS: der Server muss sich über ein Zertifikat authentisieren, das der Nutzer authentifizieren kann
  - IMAPS (IMAP über SSL/TLS) über Port 993
  - SMTPS (SMTP über SSL/TLS) über Port 465 (Implicit TLS)
    - Aufbauen des TLS Sockets vor Beginn der SMTP Session
  - ASMTP (SMTP Authentication) über Port 587
    - Aufbauen des TLS Sockets während der SMTP Session (STARTTLS)
    - erlaubt Konfiguration von Opportunistic TLS, d.h. Mail-Client und Mail-Server „verhandeln“, ob TLS genutzt wird (kein Problem, wenn Mail-Server TLS erzwingt, „Forced TSL“)
    - derzeit vermutlich noch am weitesten verbreitete Variante (auch HTWG)
- Implicit TLS vs. STRATTLS (nach RFC8314)
  - Implicit TLS soll Standard für Mail Submission werden
  - STARTTLS soll für eine Übergangszeit bleiben und dann verschwinden
  - Grund: höhere Komplexität und dadurch Implementierungs-und Konfigurationsfehler

Kapitel 3: Anwendungsschicht

3.1 Netzanwendungen

3.2 Web und HTTP (HyperText Transfer Protocol)

3.3 DNS (Domain Name System)

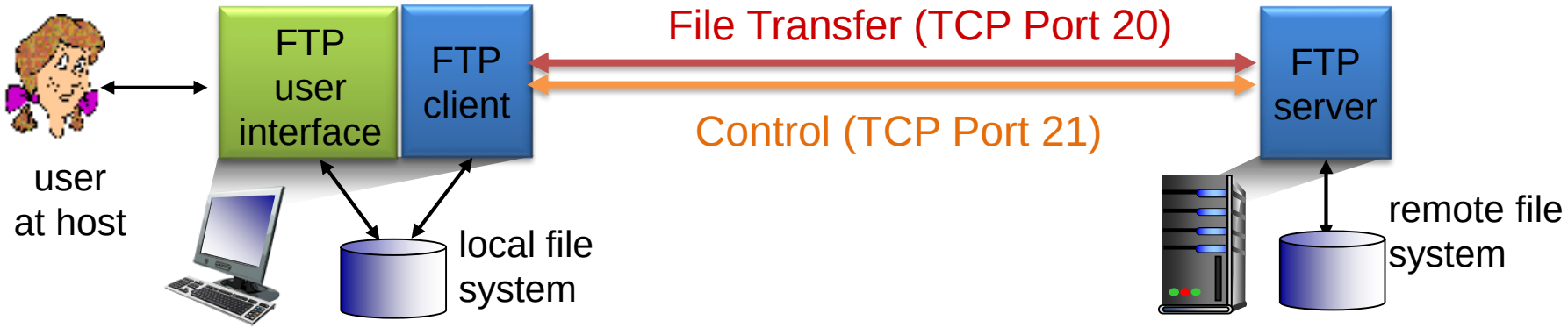
3.4 Weitere Anwendungsprotokolle

3.4.1 Mail-Protokolle

3.4.2 File Transfer Protocol

FTP

- FTP (File Transfer Protocol)
  - Protokoll zum Zugriff auf ein Dateisystem über ein Netz
  - Client öffnet Kontroll-Verbindung über TCP Port 20
  - Kommandos in Kontrollverbindung übliche "Dateisystembefehle" wie Verzeichnis wechseln (cwd, cdup), Dateien auflisten (LIST), Verzeichnis erstellen (MKD)/löschen (RMD)
  - Kommando "Datei übertragen" (RETR, STOR)
    - neue TCP Verbindung auf Port 20 für Dateiübertragung



Kapitel 3: Anwendungsschicht

3.1 Netzanwendungen

3.2 Web und HTTP (HyperText Transfer Protocol)

3.3 DNS (Domain Name System)

3.4 Weitere Anwendungsprotokolle

- 3.4.1 Mail-Protokolle
- 3.4.2 File Transfer Protocol (FTP)

3.5 Zusammenfassung

Zusammenfassung

- Zahlreiche Kategorien von Anwendungen mit heterogenen Anforderungen
  - Latenz: konstante und kurze Paketübertragungsdauern
  - Bandbreite:
    - kurzfristiger oder kontinuierlicher Bandbreitenbedarf
    - konstanter oder durchschnittlicher Bandbreitenbedarf
  - Datenintegrität: Toleranz gegen Paketverlust
  - Sicherheit: Authentizität und Geheimhaltung der Daten
- HTTP: Transfer von Web-Seiten und mehr
  - Entwicklung von HTTP/0.9 zu HTTP/3.0
  - Protokollaspekte: Nachrichten- und Formate
  - Proxies und Caching
- DNS:
  - verteilte Datenbank zum gegenseitigen Abbilden von Hostnamen und IP-Adressen