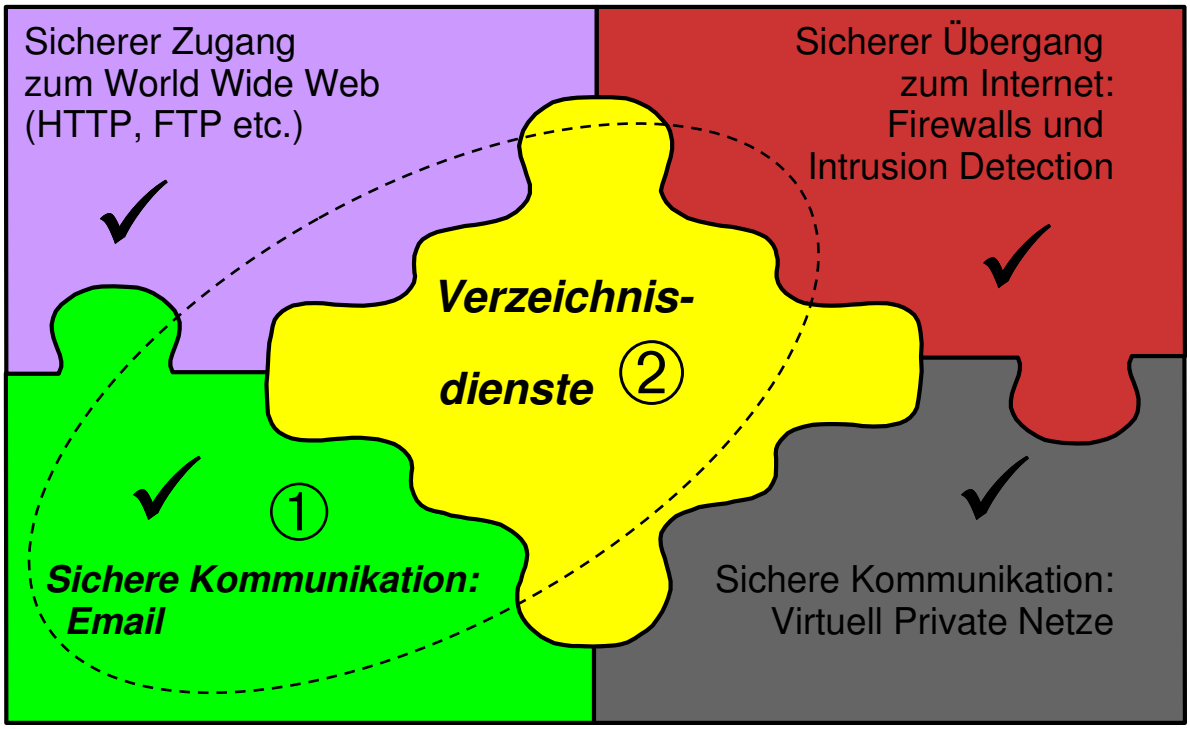
Vorherige Themen aus „Grundlagen“



Dienst: Verzeichnis
Einsatzgebiete

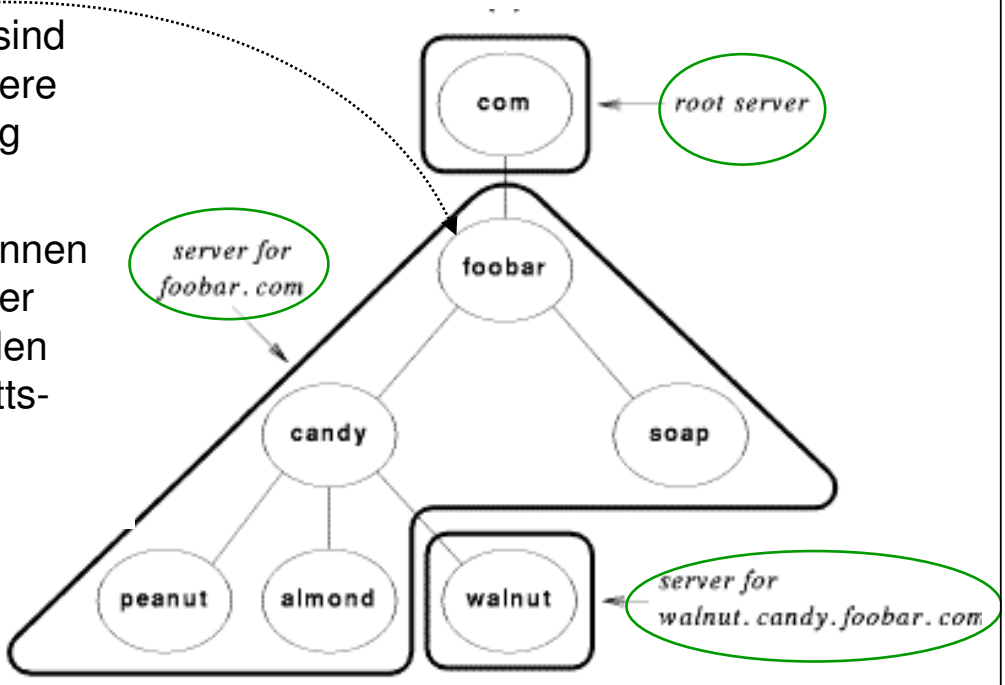
- A Directory is like a database...
  - you can put information in, and later retrieve it.

  ...but it is *specialized*. Some typical characteristics are...
  - designed for **reading** more than writing
  - offers a **static view** of the data
  - simple **updates** without transactions

- Netz (Schicht 3) - Endsysteme
  - Bestimmung von Eigenschaften / Lokalisierung
  - Domain Name *System* (DNS)
- Anwendung (Schicht 7)
  - Verwaltung von Objekteigenschaften
  - Lightweight Directory Access Protocol (LDAP)

Dienst: Verzeichnis
DNS: Architektur

- DNS-Server sind für 1 oder mehrere Zonen zuständig
- Subzonen können an andere Server „delegiert“ werden (auch ausschnitts-weise)



Dienst: Verzeichnis
DNS-Operationen

- Durchführung verschiedener „Abbildungen“
  - Name → IP-Adresse (A)
  - IP-Adresse → Name (PTR)
  - Name → Mailhost (MX)
  - Zone → Zoneninformation (SOA)
  - Name → Textuelle Information (TXT)
  - Zone → Public Key (KEY)
- Auflistung von Zonen und Einträgen
  - meist nur an explizit autorisierte Systeme zugelassen
- Aktualisierung von Einträgen (Dynamic DNS)
  - Unterstützung Systeme mit wechselnden IP-Adressen, z.B. mobile Systeme

Dienst: Verzeichnis
DNS: Betriebsaspekte

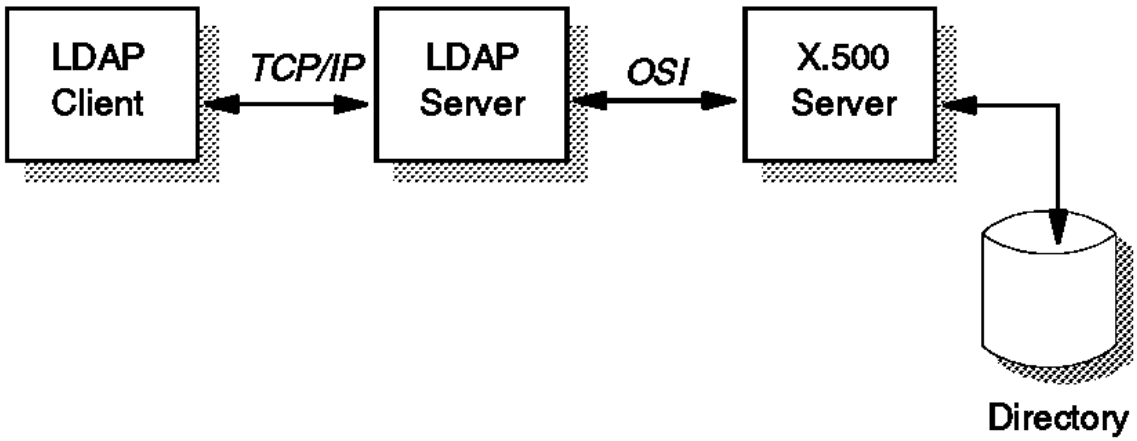
- Basis-Element der Internet-Infrastruktur
  - Hohe Verfügbarkeit
  - Schneller Zugriff
- Verbesserung durch
  - Caching Server
    - Cache für bereits abgefragte Information bis zu einem Timeout
  - Secondary Server
    - ebenfalls zuständig für eine Zone
    - befragt regelmäßig den Primary Server nach neuer Information, oder
    - nach einem NOTIFY

Dienst: Verzeichnis
Lightweight Directory Access Protocol (LDAP)

- Kommunikationsprotokoll für komplexere Verzeichnisse
- Informationsmodell für Syntax und (teilweise) Semantik der gespeicherten Information
- Strukturierung der Information durch Namensräume
- im Entstehen: ein **verteiltes** Betriebsmodell zur Beschreibung und Referenzierung der Daten
- Protokoll und Informationsmodell sind erweiterbar
- aber nicht:
  - Speichermodell
  - Programmierschnittstelle (anderer Standard...)
  - Implementierungsbeschreibung

Dienst: Verzeichnis
LDAP-Architektur

- Abgeleitet auf dem OSI-Standard X.500
- Vereinfachtes Zugriffsprotokoll für Clients



Dienst: Verzeichnis
LDAP - Zugriff und Operationen

- Transportprotokoll: TCP
- Verbindungsaufbau
  - authentifiziert oder anonym
  - eventuell verschlüsselt
- Verzeichnisoperationen:
  - Search: Und-verknüpfte Bedingungen auf Verzeichnisausschnitt
  - Read: ein Eintrag,
  - Add, Update, Move, Compare
- Informationsmodell (entspricht X.501)
  - Das Verzeichnis (Directory Information Tree - DIT) ist ein Baum
  - Eintrag identifiziert durch *Distinguished Name* (DN):
    - Sequenz von RDNs, wie in typischen Dateisystemen ...

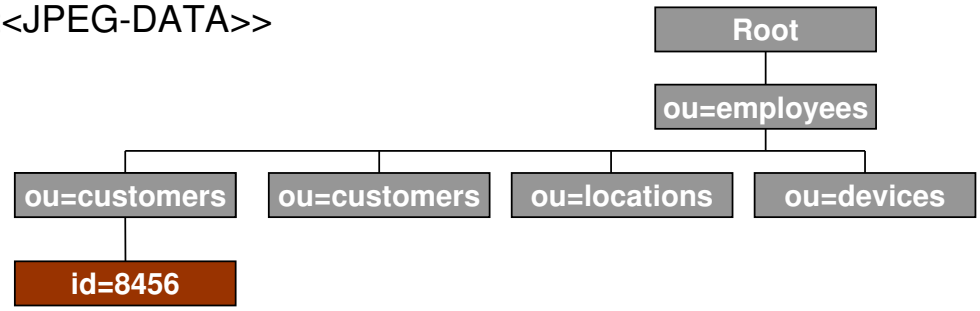
Dienst: Verzeichnis
LDAP - Informationsmodell

- Entry (Eintrag):

cn: Robert Seagal
cn: Bob Seagal
nr: 8456
mail: bob@dobbs.com
telephoneNumber: 54754-369
telephoneNumber: 54754-484
roomNumber: 3996
picture: <<JPEG-DATA>>

- Distinguished Name:

id=8456
ou=employees



Dienst: Verzeichnis
LDAP: Wozu wird es verwendet?

- Benutzer authentifizieren
  - Speicherung von Passwort-Information (gesichert durch Einwegverschlüsselung)
- Benutzer autorisieren
  - Anwendungsspezifische Rechte im Verzeichnis speichern
    - „Wer darf wohin surfen ?“
- Verteilte Aktualisierung
  - Jeder Eintrag/Baumabschnitt kann eigene Zugriffsrechte haben
- Physische Ressourcen verwalten
  - IT-Managementsysteme (z.B. Element Manager) können Informationen über Switches, Hubs und Firewalls zugriffsgesichert bereitstellen

Ende Verzeichnisdienste