Netzmanagement Versuch 1

1 Motivation Netzmanagement

- Größe, Wichtigkeit, ... der Rechnernetze
- Probleme (2.1.1.3a)
  - verteilt: Client-Server
  - heterogen: Unix, Win, Mac, Mainframe,...
  - dynamisch: neue PCs, Drucker,...
  - Komplexität: siehe Versuche ATM, Konfigurationsfiles (DNS)
  - verschiedene Administrations-/Organisations-Domänen: Zuständigkeiten,...

2 Untergliederung des NetzMgmts

- **Dimensionen (Einführung & 2.1.1.1)** Bild
  - Szenarien/„Objekte“: Netz/Komponenten, System, Anwendung, Dienste
  - Funktionsbereiche: Gruppierung nach Aufgaben
  - zeitliche Phasen
    - kurz = Minuten: Überwachung, Steuerung
    - mittel = Stunden: Eingriffe
    - lang = Wochen/Monate: strategisch
- **Funktionsbereiche (Einführung, 2.1.1.2)** Bild
  - Fault management
    - Überwachung des Zustandes
    - Sammeln und verarbeiten von Alarmen
    - Fehlerdiagnose
    - Fehlerauswirkungen ermitteln
    - Fehlerbehebung und Test
    - Trouble Tickets führen
    - Help Desk
  - Configuration management
    - Fortschreiben der Konfiguration (Update)
    - Umkonfigurieren der Ressourcen (z.B. im Fehlerfall)
    - Remote Konfiguration
    - Versionsverwaltung
    - Auftragsinitiierung & -verfolgung
  - Accounting
    - Erfassung von Verbrauchsdaten
    - Führen von Abrechungskonten
    - Zuordnung von Kosten zu Konten

    - Verwaltung und Überwachung von Kontingenten
    - Verbrauchsstatistiken
  - Performance management
    - Bestimmen von QoS-Parametern
    - Messungen Durchführen
    - Überwachung auf Leistungsengpässe
    - Aufbereiten der Meßdaten
    - Berichte zur Leistung
    - Kapazitätsplanung
  - Security management
    - Überwachung auf Angriffe
    - Verschlüsselung von Informationen
    - Authentifizierung
    - Sicherheits-Policy erstellen/durchsetzen

Bild

- **Disziplinen** (vgl. Szenarien)
  - Enterprise, Dienst, Anwendungs, Informations,
  - System- und Netzmanagement = Bereich fürs Praktikum

3 Managementwerkzeuge

3.1 Klassifizierung

Bild

- siehe Bild
- Internetwerkzeug: Tools wie `ping`, `traceroute`

3.2 SNMP-Tools

3.2.1 SNMP Überblick

Bild

- 2 Rollen: Manager, Agent (vertritt MO)
- MIB-Variablen:
  - Repräsentieren für das Management relevante Informationen über das MO.
  - Namensgebung durch Baumstruktur.
  - Protokoll-PDUs: (get, get-next, set, trap(nächstes Mal genauer))
  - Community-String als 'Passwort'

3.2.2 Komandozeilen Tools

3.3 Protokollanalysator

3.3.1 Einsatzgebiete im NM

- FcaPs

- Netzauslastung
- Lastverteilung
- Fehlerhäufigkeit / Fehlersuche
- Protokollierung von Verkehr
- Aktive Knoten / Top Talkers / ...

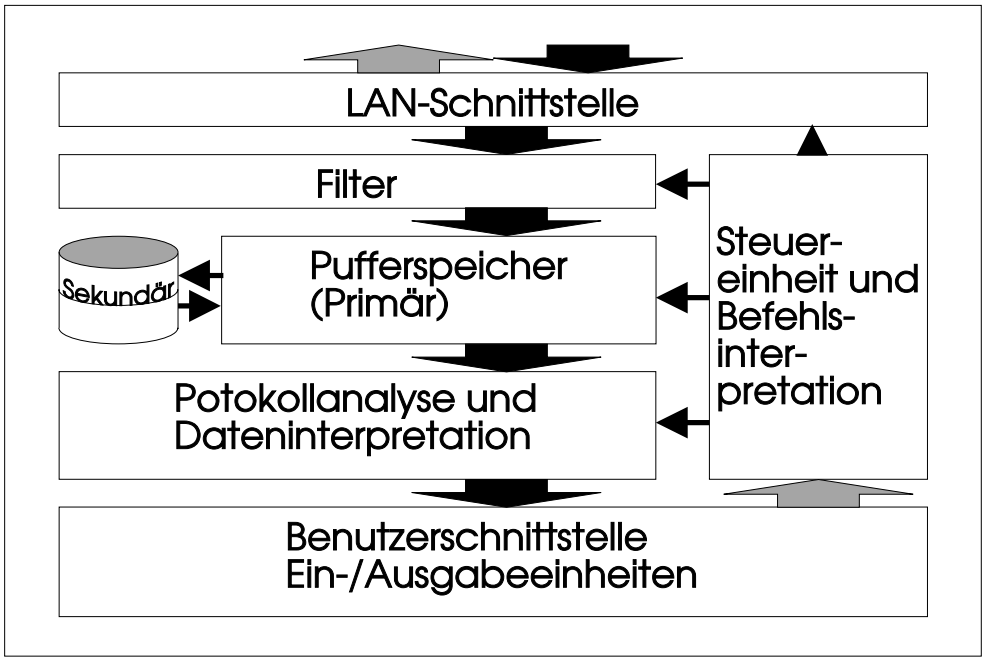
3.3.2 Anforderungen

von den Studenten per Fragespiel aufzählen lassen.

- Empfang des gesamten Netzverkehrs
- Filterung der ankommenden Daten
- Detailierte Onlineanalyse über alle Schichten
- Datenaufzeichnung zur Offlineauswertung
- Reports
- Statistische Auswertung
- Schwellwertüberwachung
- Einschränkung: nur lokale Sicht $\Longrightarrow$ keine End-to-End Auswertung

3.3.3 Architektur eines Protokollanalysators

von den Studenten aus den Anforderungen an der Tafel schrittweise entwickeln lassen.



3.3.4 Probleme

- LAN-Schnittstelle
  - Adreßkonflikte
  - Wechselbare Module teuer und fehleranfällig
  - Durchsatz muß für maximale Bandbreite ausreichen
- Filter
  - Geschwindigkeit muß ausreichen, um Netzbandbreite zu filtern
  - Hardware-Implementierung: schnell, nur einfache Ausdrücke
  - Software-Implementierung: langsamer, komplexe Bedingungen möglich
- Pufferspeicher
  - Muß mit Geschwindigkeit des Netzes mithalten können
  - Größe muß sinnvolle Samplingdauer erlauben
- Datenanalyse
  - viele Protokolle bekannt
  - Erweiterbar um benutzerspezifische
  - Online-Darstellung $\Longrightarrow$ erhebliche CPU-Last
- Steuereinheit
  - Skriptingfähigkeit
- Benutzerschnittstelle
  - Bedienbarkeit, Ergonomie
  - Anpaßbarkeit

3.3.5 Aktive Netzeingriffe

- Ping
- ARP-Request
- Fehlerhafte Station simulieren
- Durchsatztests

4 Protokolle

4.1 TCP

Bild

- Ziel: einheitlicher Transportdienst unabhängig von Schicht 1-3 mit wählbarer Güte
- OSI-TCP-QoS Parameter: siehe Handout
- Verbindungsaufbau
  - siehe Handshake

  - Grund 3-way handshake: Verbindungsaufbau durch Duplikat des ersten Pakets

- Datenübertragung
  - siehe Handshake

4.2 FTP

- RFC 959
- Dateiübertragung und Dateiverwaltung unabhängig vom jeweiligen Betriebssystem
- Ports auf Server-Seite: 21 Steuerung/Befehle, 20 Datentransfer
- Ablauf eines dir-Befehls
  - ftp <Rechner>
  - USER <name> # Login
  - PASS <passwd>
  - PORT(<port>) # Client-Port zu dem Server die Datenverbindung aufbauen soll
  - LIST # dir-Befehl
  - Server baut Datenverbindung zu entsprechendem Port auf
  - Datenübertragung
  - Datenverbindung schließen
- PASV (passive): Server liefert Port, an dem er auf Verbindungsaufbau von Client wartet (Firewall)
- Data Port (normal mit PORT oder PASV vereinbart)
  - Default auf Server-Seite: 21-1 = 20
  - Default auf Client-Seite: Steuerport