Praktikum Rechnernetze
Aufgabe 5: Netzmanagement mit Share- und Freeware Software

23. April 2001

Niels-Peter de Witt	Matrikelnr. 083921
Karsten Wolke	Matrikelnr. 083967
Helge Janicke	Matrikelnr. 083973

Inhaltsverzeichnis

1 Einleitung

In diesem Versuch haben wir einige Share- und Freeware Programme zur Messung und Analyse des Datenverkehrs in einem lokalen Netzwerk untersucht. Folgende Programme wurden verwendet:

- ETHLOAD
- ETHLOAD 2.0
- FERGIE
- GOBBLER
- MONET

In folgenden werden die zum Praktikum gestellten Fragen beantwortet und ein Funktionsüberblick über das Sharewareprogramm MONET gegeben.

2 Beantwortung der Praktikumsfragen

2.1 Frage 4: Vergleich von Beschreibung und tatsächlichen Funktion des Programms MONET

Siehe Kapitel Monet LAN analyzer LITE Version 1.5.

2.2 Frage 5: Fragen zum Programm ETHLOAD

1. **Welche Optionen stehen unter dem Programm ETHLOAD zur Verfügung?**

   - Anzeige der Frameübertragung von MAC zu MAC.
   - Anzeige der Framelängen ohne Vorspann mit Adressen und Checksummen.
   - Statistik für die letzten 5 sec, die 5 sec mit der höchsten Netzlast, sowie eine Statistik über die gesammte Messung. Angezeigt werden die mean interframe time, und der prozentuale Anteile der Netzkapazität (standardmäßig auf 10MBit).
   - Informationen wieviel, über welches Protokoll gesendet und empfangen wurde.
   - Informationen zu einzelnen Protokollen (NetBUI, DECNet, IP, LLC, Netware/DNS, OSI).
   - Detailierte Informationen zu IP.
     - ARP: Aufschlüsselung von IP-Adressen zu MAC-Adressen.
     - FRAGS: Größe der IP-Datagramm-Fragmente pro IP.
     - HOSTS:
       * MTU
       * größtest Fragment
       * Time To Live
       * verlorengegangene Datagramme
     - ICMP: Letzter gesendetes Frame mit Sender, Empfänger und den ersten 32 Byte.
     - LAST: Letztes IP-Paket.
     - OPT: IP-Pakete mit Optionen.
     - PROT: Statistik über die verschiedenen Protokolle der IP-Familie und deren Häufigkeit in Prozent.
     - RCVR: Empfängerstatistiken.
     - Sender: Senderstatistiken.
     - TCP:
       * Connection: Sender- und Empfänger-Adressen mit Portangaben.
       * DNS: Informationen über DNS-Server (Kein DNS-Server im Praktikumsnetz vorhanden)

    - EVENTS: Port - Port Verbindungen mit Zeitangabe und Statusflags, sowie Informationen über Window-Größe und Verlust.
    - LAST: Letztes TCP/IP Paket mit Sender- und Empfänger-Adresse sowie Sequenznummer, Anzahl der Bytes und Adressnummer.
    - MAIL: Informationen über POP und SMTP
    - NetBios: (wurde nicht benutzt ;o))
    - PORT: Statistik über die Hauptlast auf verschiedenen Ports.
    - STAT: TCP - Statistiken über die Anzahl der empfangenen und gesendeten Packete (IP zu IP)
  - UDP:
    - Port
    - DNS
    - Associations
    - BootP
    - NetBios / Novell
    - RIP: Auflistung der Router mit Last. (im Praktikum nur E0)
    - TFTP

2. **Bestimmung der höchsten Netzlast**
   Die höchste Netzlast lag bei 54.47 % der Maximalen Netzlast eines 10MBit - Netzes. Die Mean-Interframe-Time betrug 1.46 ms.

3. **Vergleich zu ETHLOAD 2.0**
   In der neuen Version 2.0 sind folgende Menüpunkte hinzugekommen:

   - Protokolle - LAN-Manager
   - Protokolle - VINES (nur registrierte Version)
   - IP-Protokol - NET: IP-Flows von IP nach IP in Prozent.
   - TCP/IP-Protokol - OTHERS: Einzelne Dienste aufgeschlüsselt.

2.3 Frage 6: Frage zum Programm FERGIE

Zuordnung der Anzeigen des Startbildschirms des Programms FERGIE:

- Oberes Fenster: Allgemeine Statistik über Empfang, Größe, Zeit und Treiber.
- Unten links: Statistik über Paketgrößen in Prozent.
- Unten mitte: Statistik über Protokol-Typen in Prozent.
- Rechts: Statistik über Rahmengrößen in Prozent (Schrittweite 75 Byte, von 0 bis 1500 Byte.

2.4 Frage 7: Fragen zum Programm GOBBLER

Was ist im oberen linken Fenster während der Messung zu sehen?
- Das obere linke Fenster ist das DEBUG- Fenster. Während der Messung wurde dort nichts angezeigt.

Analyse der aufgezeichneten Daten und Bedeutung der einzelnen Angaben im Informationsfenster.

FrameNr	timestamp	Source MAC	Dest MAC	Type	Len	Info
00014	215:402:034	0000E8CF5CE4	0000E49E768E	IP	1514	TCP

Framenr laufende Nummer der empfangenen Frames.

timestamp Zeitstempel in diesem Netzwerk.

source MAC MAC Adresse des Senders.

dest MAC MAC Adresse des Empfängers.

Type Typ des Protokols.

Len Rahmengröße in Byte.

Info Unterprotokolle des jeweiligen Protokol-Typs.

Detailierte Anzeige eines aufgezeichneten Rahmen der größer als 64 Byte ist.

- IP Datagram header:
  - MAC-Adresse Sender
  - MAC-Adresse Empfänger
  - Größe des Rahmens
  - TTL
  - Prüfsumme
  - IP-Adresse Sender
  - IP-Adresse Empfänger
- TCP segment header:
  - Port-Adresse Sender
  - Port-Adresse Empfänger
  - Sequenz
  - ACK
  - Dataoffset
  - Window
  - Flags
- Data: Nutzlast ...

2.5 Frage 8: Vergleich der Möglichkeiten der einzelnen Programme

Die Programme ETHLOAD und ETHLOAD 2.0:
Die beiden Programme bieten sehr gute statistische Funktionenen. Durch die Vielzahl der Menüpunkte sind diese Programme etwas unübersichtlich und benötigen einige Einarbeitungszeit. Wünschenswert wäre es, wenn man einzelne Rahmeninhalte näher analysieren könnte.

Das Programm FERGIE:
Sehr übersichtliches Programm mit ungewöhnlicher Menüführung. Übersichtliche Statistiken, über den Augenblickswert. Leider fehlten Langzeitstatistiken.

Das Programm GOBBLER:
Positiv ist die Möglichkeit Meßergebnisse zu archivieren. Auch bietet GOBBLER im Gegensatz zu anderen Programmen die Möglichkeit die Nutzdaten der einzelnen Pakete auslesen zu können. Allerdings sind keine Statistikfunktionen integriert. Es ist damit eine gute Ergänzung zu den anderen Programmen.

2.6 Frage 9: Der Promiscuous Mode

Der Promiscuous Mode ermöglicht einer Netzwerkkarte alle Pakete an höhere Schichten weiterzugeben, auch solche, die nicht an sie adressiert sind. Dies eine Grundfunktionalität die alle Netzwerkanalyzer brauchen. In diesem Mode wird das System sehr stark belastet, da jedes Paket das im Netzwerk verschickt wird, analysiert werden muß. Je nach Netzlast kann dies zu sehr hohem Rechenaufwand führen.

3 Monet LAN analyzer LITE Version 1.5

3.1 Funktionsumfang laut Beschreibung

- Tracen von IP-Packeten
- Einfangen von IP-/ ARP-/ RARP-Packeten
- Analysieren von IP-Packeten
- Dekodieren folgender Protokolle:
  - DLC
  - IP, ARP, RARP layer auf der Basis von DLC
  - TCP, UDP, ICMP auf der Basis von IP
  - DNS auf der Basis von UDP
  - Alles was über UDP oder TCP übertragen wird, wird als Daten dekodiert

3.2 Anzeige während der Messung

- Anzeige wieviele Packete empfangen wurden seit Trace-begin
- Anzeige wieviele Bytes empfangen wurden seit Trace-begin
- Anzeige, der Anzahl der nicht analysierten Frames
- Anzeige wieviele Frames einen Fehler hatten
- Anzeige der durchschnittlichen Pakete pro Sekunde
- Anzeige der durchschnittlichen Last in %
- Anzeige der maximalen Pakete pro Sekunde mit Zeit
- Anzeige der höchsten Byteanzahl mit Zeit
- Anzeige der höchsten Last in %

3.3 Detailierte Anzeigen nach der Messung

- Anzeige der Länge
- Anzeige von Start-Ziel-Adresse mit den jeweiligen Ports
- Anzeige des Protokoll-Typs
- Anzeige im TCP-Protokoll der Flags

Einige der obengenannten Punkte lassen sich noch detailierter anzeigen.

- Aufgliederung in diverse Header (DLC, IP, UDP, DNS, ...)
- Start-Ziel-Adresse als MAC und als IP
- verwendete Ports

- Welche Protokoll Versionen
- Welche Flags gesetzt wurden
- Ob fragmentiert oder nicht
- Header-Längen
- Größe in Oktetts
- TTL
- ToS
- Daten
- zusätzliche Anzeige des Packets als Hex-Dump und ASCII

3.4 Ist MONET sinnvoll im Labor einzusetzen?

Wir fanden dieses Programm wesentlich übersichtlicher als die im Praktikum verwendeten Programme. Es stach hervor mit einer intuitiv zu bedienenden Oberfläche. Desweiteren fanden wir Erläuterungen zu den verwendeten Abkürzungen und angezeigten Daten sehr hilfreich. Dies alles spricht für eine Verwendung des Programms MONET im Praktikum.
Gegen MONET sprechen die fehlenden statistischen Funktionen zur Netzwerklast-Analyse. Zudem werden in der freien Lite-Version nur wenige Protokolle unterstützt.