

## **Gruppe 2**

Karsten Bükler  
Olaf Kellmerit  
Tobias Stahringer

### **INHALT**

- 1. Grundsätzliches zur Fehlerprävention**
  - 2. Allgemeines Troubleshooting-Modell**
  - 3. Troubleshooting-Modell für Ethernet**
  - 4. Mögliche Fehlerquellen auf Layer 1**
    - 4.1 Koax**
    - 4.2 Twisted-Pair**
    - 4.3 Fiber-Optic**
  - 5. Mögliche Fehlerquellen auf Layer 2 und 3**
- Anhang**

### **1. Grundsätzliches zur Fehlerprävention**

**Um Fehler von vornherein zu vermeiden ist es wichtig, für ein zuverlässiges Netzwerk-Design zu sorgen.** 70 bis 80 % der Fehler entstehen durch

- Unzureichend gut installierte Hardware
- Falsche Komponenten benutzt
- Netzwerke ohne Beachtung der Richtlinien
- Kombination aus o.g. Fehlern

Deshalb ist es wichtig von Anfang an auf Zuverlässigkeit zu achten. Dazu gehört, dass man die für Netzwerke vorgeschriebenen Richtlinien einhält. Des weiteren sollte man immer auf die Skalierbarkeit des Netzwerkes achten um auch zukünftiges Wachstum zu ermöglichen.

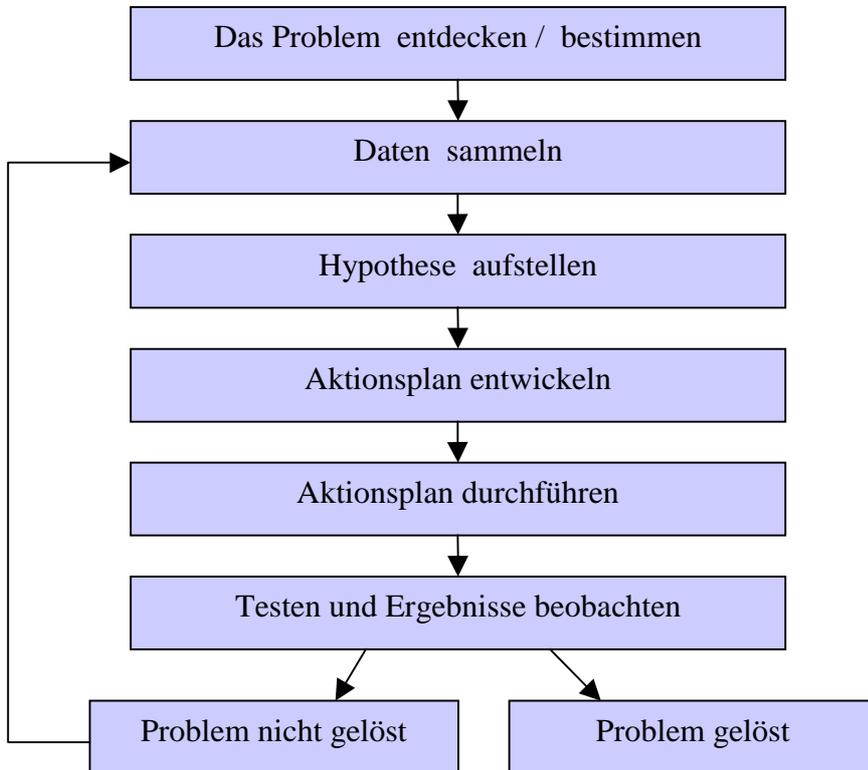
Notwendige Erweiterungen sollen nicht mit sogenannten provisorischen - „Übergangs-Netzwerken“ umgesetzt werden, sondern sorgfältig in das Gesamtkonzept eingebunden und dabei dokumentiert werden.

#### **Netzwerk-Dokumentation erstellen:**

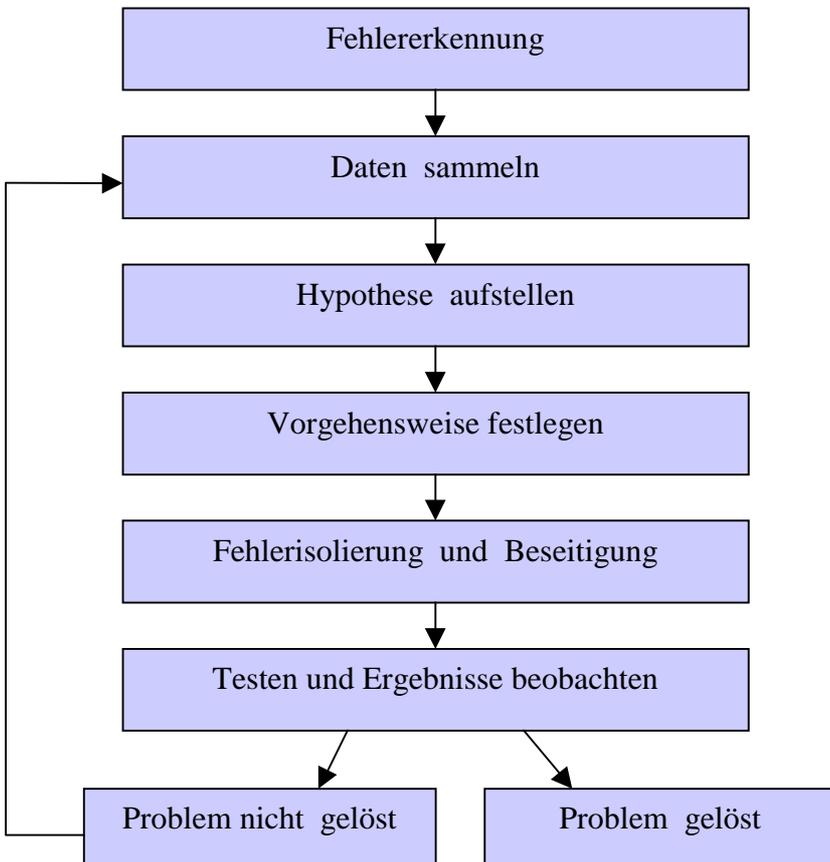
Um einen Überblick über gesamte Netzwerk mit allen Komponenten und der Verkabelung zu haben und um später langwierige Suchaktionen zu vermeiden ist es notwendig, eine komplette Netzwerk-Dokumentation zu erstellen. Dabei empfiehlt es sich, Dokumentations-Software zu verwenden. Die Beschriftung der Kabel und die Dokumentation der Verläufe hilft, die Zeit für die Fehlersuche zu verkürzen. Des weiteren sollte man die Bedienungsanleitung jedes Teils aufbewahren, um später einmal Hardware- und Inkompatibilitäts-Probleme besser erkennen zu können. Zusätzlich sollte man das fertiggestellte Netzwerk beobachten und Fehler-Level festlegen.

Dies ist notwendig, um später normales Kollisionsverhalten bzw. Überlast von „echten“ Netzwerk-Fehlern unterscheiden zu können.

## 2. Das allgemeine Troubleshooting-Modell:



## 3. Troubleshooting-Modell angewandt auf Ethernet



1. Problem entdecken/bestimmen: Fehlererkennung durch Fehlererkennungssoftware oder ein Problemreport eines betroffenen Users.
2. Daten sammeln: Analyse des Protokolls der Fehlererkennungssoftware. Beim User: gezielte Fragen stellen und so den Kern des Problems herausarbeiten und die Fehlerquelle eingrenzen
3. Hypothese aufstellen: aus den vorhandenen Daten eine Hypothese aufstellen. Die offensichtlichste/wahrscheinlichste Hypothese zuerst.
4. Aktionsplan entwickeln: Vorgehensweise zur praktischen Fehlerisolierung festlegen :

3 Wege: - Netzwerkpfad bestimmen  
 - Symptom duplizieren  
 - Isolierung durch binäre Suche (Netzwerke trennen)

5. Aktionsplan durchführen und Fehler isolieren:

Netzwerkpfad bestimmen: wo im Netzwerkpfad tritt der Fehler auf?

Symptom duplizieren: Situation nachbilden in der der Fehler häufig auftritt um das Auftreten des Fehlers zu provozieren (sinnvoll bei unterbrochenen Fehlern)

Isolierung durch binäre Suche: Netzwerk immer wieder halbieren und den Fehler eingrenzen. (einfach bei kaskadierten Systemen (Twisted Pair), umständlich bei Bus-Topologie)

Fehler gefunden? Geeignete Maßnahmen zur Fehlerbeseitigung durchführen

6. Testen und Ergebnisse beobachten: Funktionstest durchführen. Ist der Fehler jetzt weg?  
 Wenn ja, fertig. Wenn nein, wieder bei Punkt 2 einsteigen.

## **4. Mögliche Fehlerquellen auf Layer 1**

### **4.1 Koaxial Verkabelung**

- Falsche Kabellänge (zu lang)
- Falscher oder nicht vorhandener Endwiderstand
- Stecker locker

### **4.2 Twisted-Pair Verkabelung**

- Falsche Kabellänge (zu lang)
- Falscher Drahttyp (Kabelbruch)
- Falscher Kabeltyp
- Falsche Belegung der Anschlüsse
- Stecker locker
- „Nebensprechen“ aufgrund unzureichender Verdrillung

### **4.3 Fiber-Optic Verkabelung**

Keine Verwendung von elektrischen Signalen, daher Immunität gegenüber elektromagnetischen Feldern.

Glasfaser-Verkabelung wird meistens professionell installiert.

==> Starke Minimierung der möglichen Fehler

Verbleibende mögliche Fehler:

- Verbindungsstücke oder Stecker falsch installiert
- unsaubere Kabelenden

- Alterung der Komponenten
- Faserbruch

## **5. Troubleshooting auf Layer 2 und 3**

Sowohl auf der Sicherungsschicht (Layer 2) als auch auf der Netzwerkschicht (Layer 3) kann es zu Fehlern kommen. Anders als auf Layer 1 handelt es sich dabei nicht um physikalische Fehler bei der Bitübertragung sondern um Protokollfehler. Auf Layer 2 findet man diese Fehler über die Statistiken, die Hubs, Interfaces und Netzwerk-Überwachungs-Sonden über Ethernet-Rahmen-Aktivitäten und -Fehler bereitstellen. Auf Layer 3 findet man die Fehler über die Auswertungen der Daten, die von einem Protokoll-Analysator gesammelt werden.

### **Anhang:**

#### 1. IEEE 802.3/10 BASE 5:

- Segmentlänge maximal: 500m
- Segmente maximal: 5 (siehe Repeaterregel: 5 Segmente und 4 Repeater)
- Verkabelung: dickes Koaxkabel (yellow cable, gelbes Kabel)
- Übertragungsrate: 10 Mbits/s Basisband
- Wellenwiderstand: 50 Ohm

#### 2. IEEE 802.3/10 BASE 2:

- Segmentlänge maximal: 185m
- Segmente maximal: 5 (siehe Repeaterregel: 5 Segmente und 4 Repeater)
- Verkabelung: dünnes Koaxkabel
- Übertragungsrate: 10 Mbits/s Basisband
- Wellenwiderstand: 50 Ohm

#### 3. IEEE 802.3/10 BASE T:

- Segmentlänge maximal: 100m
- Segmente maximal: 5 (siehe Repeaterregel: 5 Segmente und 4 Repeater)
- Verkabelung: ungeschirmte, verdrehte Leitung
- Übertragungsrate: 10 Mbits/s Basisband
- Wellenwiderstand: 100 Ohm