

Mitschnitte im Netzwerk

Immer dann, wenn bei Endgeräten die mit dem Netzwerk verbunden sind, Kommunikationsprobleme auftreten, für die sich keine Ursache festmachen lässt, ist es sinnvoll einen Mitschnitt auf dem Netzwerk aufzuzeichnen.

Wenn kein Netzwerkanalysegerät zur Verfügung steht empfehlen wir den Einsatz der Freeware „Ethereal“, die unter <http://www.ethereal.com> zum kostenlosen Download bereitgestellt wird. Vor der eigentlichen Installation von Ethereal, muss ein Capture-Treiber installiert werden. Auch das dazu benötigte Winpcap.exe File steht unter <http://www.ethereal.com> zur Verfügung. Als beste Plattform für den Betrieb von Ethereal hat sich bei uns Windows NT auf einem ausreichend performanten PC (ab Pentium II 350MHz mit Netzwerkkarte 10/100Mbit/s autosensing) erwiesen.

Vorbereitungen zur Aufzeichnung

Wo wird gemessen

In aller Regel kommunizieren zwei Endgeräte über eine bestehende Netzwerkinfrastruktur miteinander. Hier können Komponenten wie Switches, Hubs, Router, Bridges aber auch ISDN-Strecken mit einbezogen sein.

Deshalb sollte an den Standorten beider Endgeräte gemessen werden. Nur so kann kontrolliert werden, ob nicht schon auf dem Verbindungsweg Datenpakete verloren gehen, bzw. nicht weitergereicht werden.

Art des Anschlusses

Anschluss über HUB:

Ist ein Endgerät über einen HUB ins Netzwerk eingebunden, kann der PC mit dem mitgeschnitten werden soll einfach über ein Patchkabel mit an einen freien Port des selben HUB angeschlossen werden.

Anschluss über SWITCH:

Switches filtern den Datenverkehr auf dem Netzwerk. Das bedeutet, dass an jedem Port des Switches nur die Datenpakete weitergegeben werden, die per MAC-Adresse an das angeschlossene Endgerät adressiert sind. Ferner werden Broadcastpakete (Rundruf im Netz auf MAC-Adresse FF-FF-FF-FF-FF-FF) weitergeben.

Soll also der Datenverkehr auf einem speziellen Port mitgeschnitten werden, muss der entsprechende PC an einen Monitorport angeschlossen werden. Noch günstiger ist es den aufzeichnenden PC und das überwachte Endgerät über einen HUB, gemeinsam an einen Port am Switch anzuschließen. Nur durch den gemeinsamen Anschluss am HUB ist gewährleistet, dass PC und Endgerät exakt die selben Datenpakete empfangen.

Was wird aufgezeichnet

Einige Netzwerkanalysetools bieten die Möglichkeit, schon vor der Aufzeichnung des Mitschnittes eine Filterung der Datenpakete z.B. nach Adressbereichen oder Protokolltypen vorzunehmen. Gerade bei Problemen die nicht genau an einer Ursache festzumachen sind, sollten alle Datenpakete ungefiltert mitgeschnitten werden.