X25 - Sniffer

ÖBB X25-Protokoll Analyzer

Bedienungsanleitung

Änderungshistorie

Version	Datum	Bearbeiter	Änderung
01	26.03.2001	H. Schön	Erstellung
02	26.03.2002	H. Schön	Erweiterung nach rework der Schnüfflersoftware und Erweiterung der Archivierungsscripts

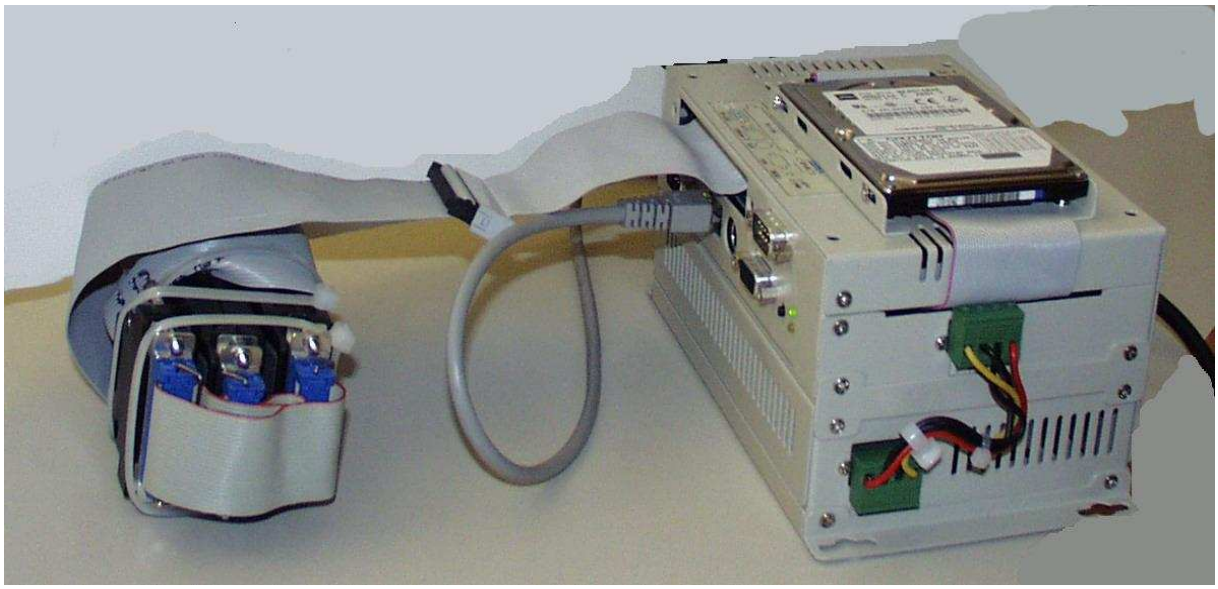
Inhaltsverzeichnis

Vorwort

Die Applikation x25sniffer dient der Diagnose von sicheren und nichtsicheren Datenverbindungen die entsprechend dem ÖBB X25 Pflichtenheft implementiert wurden. Der x25sniffer diagnostiziert sowohl einkanalige als auch zweikanalige X25 Verbindungen. Es werden die beiden Richtungen der Datenübertragung gleichzeitig aufgezeichnet und analysiert. Die Aufzeichnung erfolgt auf einer eingebauten Harddisk.

Der x25sniffer wird in die X.21 Leitung geschalten und beeinflußt die Datenverbindung weder elektrisch noch logisch. Aus Sicht der Applikationen die über die untersuchte X.21 Verbindung kommunizieren, kann keine Beeinflussung festgestellt werden.

Der x25sniffer ist Steckerkompatibel entsprechend CCITT X.21. Es existiert ein 15 poliger SUB-D male und ein 15 poliger SUB-D female. Damit kann die bestehende X25 Verbindung an einer beliebigen Stelle abgesteckt werden und der x25sniffer wird in die Verbindung eingeschleift.



Die übertragenen Daten werden vom x25sniffer untersucht und schichtenweise dargestellt. In einem ersten Schritt werden die Daten auf HDLC-Framing untersucht und es wird die korrekte Übertragung des HDLC-Framings untersucht. Ist ein Frame aus HDLC-Sicht in Ordnung wird der Frame nach

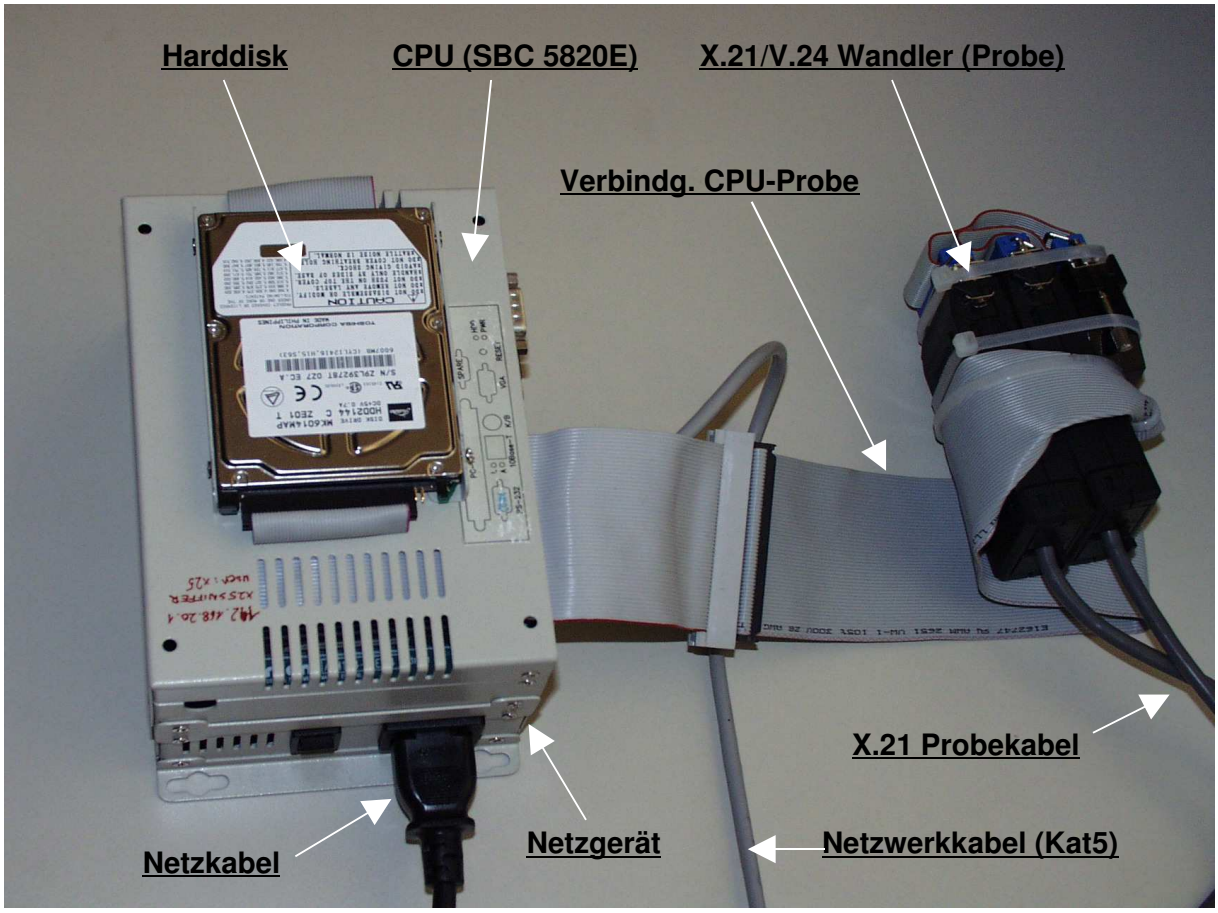
LAP-B Framing untersucht. Damit ist die Prüfung nach CCITT X.25 abgeschlossen und der Frame wird auf Einhaltung der Vorschriften entsprechend dem ÖBB X25 Pflichtenheft untersucht. In allen Schichten (HDLC, LAP-B, ÖBB-X25) werden die Telegramme immer im Klartext human-readable und zusätzlich als hexadezimaler Dump dargestellt. Die Datentelegramme werden mit Datum-Uhrzeit Stempeln versehen. Die Granularität der Zeitstempel beträgt 1 Millisekunde.

Beispiel eines X25 Trace:

```
27.Mar.01 19:25:48.814 <- (23) INFO 7 4   LCN:1 DATA      > 01 e8 10 01 86 < (L2a-CRC: 50 78)
  L7-A : > 0d 7e 0b 49 6e ff 1c d9 8c ff 02 02 02 < (L7-CRC: 26 71) TFN=116=OK
  OeBB : Lebenstakt        [R__B:255 ZD_S:255]       PASSIV VERSx2 VAR.x2
27.Mar.01 19:25:48.816 <- (23) INFO 7 5   LCN:2 DATA      > 01 ea 10 02 86 < (L2a-CRC: d5 4d)
  L7-B : > 0d 7e 0b 49 6e ff 1c d9 8c ff 02 02 02 < (L7-CRC: d9 71) TFN=116=OK
  OeBB : Lebenstakt        [R__B:255 ZD_S:255]       PASSIV VERSx2 VAR.x2
27.Mar.01 19:25:48.817 -> ( 4) RR   5                     > 01 a1 1c a2 <
27.Mar.01 19:25:48.818 -> ( 7) INFO 5 7   LCN:1 RR        > 03 ae 10 01 81 < (L2a-CRC: 08 d7)
27.Mar.01 19:25:48.834 <- ( 4) RR   0                     > 03 01 a6 34 <
27.Mar.01 19:25:48.834 -> ( 4) RR   6                     > 01 c1 1a c1 <
27.Mar.01 19:25:48.835 <- ( 4) RR   1                     > 03 21 a4 15 <
27.Mar.01 19:25:48.835 -> ( 7) INFO 6 0   LCN:2 RR        > 03 c0 10 02 81 < (L2a-CRC: c6 ca)
27.Mar.01 19:25:50.554 <- ( 4) RR   2                     > 03 41 a2 76 <
27.Mar.01 19:25:50.554 <- ( 7) INFO 3 6   LCN:1 RR        > 01 6c 10 01 a1 < (L2a-CRC: 2d e2)
```

Aufbau des x25sniffer

Das folgende Bild zeigt den Aufbau des x25sniffer und benennt seine Componenten. Im Anschluß an das Bild werden die einzelnen Componenten und der Aufbau beschrieben.



Der X25 Leitungsanalysator (x25sniffer) besteht aus einem Singleboardcomputer SBC5820E der Firma Advantech. Der Singleboardcomputer besitzt ein 220 V Netzgerät und ein PC-Compatibles Pentium 200 Mhz Singleboard Computer Motherboard auf dem alle Componenten eines handelsüblichen PC (Harddisk-Controller, Floppy-Controller, serielle und parallele Schnittstellen, 10/100 Mbit Netzwerkkarte, Graphikkarte, Soundkarte, etc.) direkt auf dem Motherboard (Singleboard Computer) vorhanden sind.

Die Stromaufnahme des SBC (singleboard Computer) beträgt 5 V / 1,44 A. Damit werden nur ca. 7 Watt auf dem Rechnerboard verbraucht und die Ausführung kann lüfterlos ausgeführt werden (Lebensdauer).

Der SBC 5820E besitzt zusätzlich einen 104 poligen Steckplatz der entsprechend der Industrienorm PC/104 ausgeführt ist. Auf diesem PC/104 Steckplatz ist im x25sniffer eine 4-fach serielle Schnittstellenkarte der Fa. Arcom eingebaut. Diese Schnittstellenkarte verfügt über 2 SCCs (serial controller chips) die je zwei serielle Kanäle mit bis zu 1 Mbit Datenübertragungsgeschwindigkeit beinhalten. Die SCC sind von der Bauart Zilog Z85230. Der Z85230 besitzt die Fähigkeit auch synchrone Protokolle dekodieren zu können. Bei der synchronen Datenübertragung werden die Bytes nicht mit fester Länge übertragen, sondern mit dem Verfahren „Bit-Stuffing“ werden zusätzliche Bits eingefügt. Aus diesem Grund können Daten auf X.21 Schnittstellen nicht mit asynchronen Chips (z. B. 16550) dekodiert werden.

Der Z85230 besitzt jedoch nur die elektrische Außenbeschaltung für V.24/RS232 Schnittstellen. Aus diesem Grund sind für die elektrische Umwandlung der X.21 Leitung noch zwei Wandler X21->V.24 notwendig. Die Wandler sind hinsichtlich DCE/DTE Verhalten unterschiedlich. Ein Wandler ist ein Übersetzer von X.21 DTE -> V24 DCE und der zweite Wandler ein V.24 DTE -> X.21 DCE. Werden nun diese beiden Wandler auf der V.24 Schnittstelle Rücken-an-Rücken geschaltet, ergibt sich bereits eine Probe-Schaltung mit der in einer X.21 Datenverbindung die Telegramme auf der V.24 Verbindung zwischen den Wandlern mitgelesen werden können. Durch die Verwendung von zwei Rücken-an-Rücken geschalteten Wandlern, kann sichergestellt werden das die X.25 Telegramme nicht beeinflußt werden, da aus Sicht der beiden Endgeräte die via X.25/X.21 kommunizieren und deren Verbindung untersucht werden soll, erkennen keinen Unterschied ob in der X.21 Verbindung Wandler vorhanden sind oder nicht. Alle Daten und Steuerleitungen werden von X.21 auf V.24 und wieder zrück von V.24 auf X.21 übersetzt.

Das Bild zeigt die beiden Rücken-an-Rücken geschalteten X.21/V.24 Wandler, mit den beiden X.21 Leitungen die zum Einschleifen in die X.21 Verbindung verwendet werden und dem 50-poligen Flachbandkabel, daß die synchronen V.24 Daten zur Z85230-SCC-Karte führt mit der die Daten von der Leitung abgegriffen werden.

In der Rücken-an-Rücken Verbindung zwischen den X.21/V.24 Wandlern werden die beiden Datenleitungen (V.24 Pin2 und Pin 3) und die beiden Clockleitungen (V.24 Pin 15 und Pin 17) abgegriffen und auf die beiden Kanäle des ersten SCC Chips der ARCOM 4-fach seriellen Schnittstellenkarte geschaltet. Damit kann die PC/104 Applikation aus dem SCC Chip 1 (Type Z85230) die X.25/X.21 Telegramme auslesen, ohne daß die untersuchte Datenleitung beeinflußt werden kann.

Technische Daten

Stromversorgung	220V / ca. 15 Watt
Analysierte Leitung	CCITT X.21 / X.25
Datenrate	automatisch taktsynchron zur verwendeten Geschwindigkeit auf der geprobten Leitung.
Bereich:	1 Hz bis 1 Mbit stufenlos
Aufzeichnungskapazität:	2 Giga Byte
Datenvolumen:	ca. 200 Tage bei 2 kanaliger Verbindung ca. 400 Tage bei 1 kanaliger Verbindung
Datenauswertung:	die Daten der untersuchten Leitung werden bereits im klartext lesbar und mit Timestamp versehen aufgezeichnet
Auswertung:	Die Datenpakete können von jedem Unix-kompatiblen Rechnersystem über die eingebaute 100 Mbit Ethernetverbindung abgezogen werden
Bedieninterface:	via Netzwerk : telnet, rlogin, ssh, ... direkt: via eingebaute Graphikkarte und eingebaute Maus-/Tastatur Schnittstelle durch anstecken eines handelsüblichen VGA-Monitors und einer Standard PC-Tastatur
IP-Adresse:	192.168.20.1
User-Account:	username: x25 passwort: x25
Root-Account:	username: root passwort: x25
Betriebssystem:	SUSE Linux 6.4

Hersteller: Heimo Schön / 2002

Verbindung Notebook – x25sniffer

Die Verbindung von einem Notebook zum x25sniffer wird hergestellt über eine Netzwerkverbindung. Entweder über KAT-5 Kabel 1:1 über einen HUB oder über ein ausgekreuztes KAT-5 Kabel direkt zwischen die beiden Systemen.

Vorbereitungen am Notebook

Am Notebook sollte eine Linux Installation vorliegen. Zur reinen Bedienung (ohne download des Logfiles) sollte auch eine Windows Installation reichen – ist aber zur Zeit ungetestet.). Die Netzwerkkarteninstallation sollte abgeschlossen sein.

Legen Sie in der Datei /etc/sudoers für Ihren Useraccount eine Zeile an die wie folgt aussehen sollte:

```
berger ALL=(ALL) NOPASSWD: ALL
```

Überprüfen Sie die korrekte Funktion des Kommandos sudo, indem Sie eingeben:

```
sudo cat /etc/sudoers
```

Sie sollten dieses Kommando als User (z. B. berger) eingeben und trotzdem den Inhalt der Datei sudoers sehen. Als normaler User ohne sudo sollte das nicht funktionieren.

Kopieren Sie die Dateien von der mitgelieferten Diskette in das Directory des Users für den Sie die sudoers Rechte geöffnete haben:

```
cd
mkdir x25sniffer
cd x25sniffer
mkdir client
cd client
mcopy a:* .
```

Nun ist Ihr Notebook vorbereitet.

Netzwerkverbindung vorbereiten

Diese Kommandos sind nach jedem Reboot des Notebooks notwendig.

Wechseln Sie in das Directory x25sniffer/client. Dort finden Sie alle Scripts um die Verbindung herzustellen.

```
cd x25sniffer/client
```

Starten Sie das Script confeth um die Netzwerkkarte zu konfigurieren. Es wird auf der Netzwerkkarte ein Alias-Device eth0:0 angelegt, dem die IP-Adresse 192.168.20.6 zugewiesen wird. Die Routen auf das Device werden automatisch gesetzt. Confeth muß nur einmal nach dem Reboot des Notebooks aufgerufen werden.

```
confeth
```

Überprüfen Sie gegebenenfalls das neue Aliasdevice mit dem Kommando

```
/sbin/ifconfig
```

Es sollte das Device eth0:0 aufscheinen.

Bedienung des x25sniffer via Ethernet

Nachdem Sie nun die Netzwerkverbindung vorbereitet haben, können Sie durch Aufruf des scripts connect die Netzwerkverbindung herstellen und sich am x25sniffer anmelden.

```
connect
```

Es erscheint eine Anmeldemaske des x25sniffer. Nun geben Sie Username und Passwort ein. Beides ist mit x25 vorbesetzt:

```
Welcome to SuSE Linux 6.4 (i386) - Kernel 2.2.14 (0).
X25sniffer login: x25
Password: x25
```

Nach Eingabe des Kommandos dir werden folgende Dateien angezeigt:

dellog	Script zum Löschen des aktuellen Logfiles (nach dem Ablauf des Scripts dellog muß der Rechner entweder mit dem Script halt gestoppt werden oder mit dem Script reboot wieder gebootet werden, da für die Sniffer-Applikation kein Logfile mehr zur Verfügung steht.)
halt	Script zum Anhalten des Betriebssystems (nach ca. 40 Sekunden ertönen zwei Beeptöne im Abstand von ca. 2 Sekunden – danach kann der Rechner abgeschalten werden.)
reboot	Script zum Rebooten des Betriebssytems
start	das Script wird von inittab beim Booten zum Aktivieren der Schnüffler Applikationen verwendet (nicht für den Bediener)
x25sniffer	Applikation die vom Treibermodul die empfangenen Daten ausliest und und human-readable aufbereitet. Diese Applikation läuft im Hintergrund und wird vom Script start automatisch beim Reboot geladen.
z85230.o	Kernel-Treiber-Modul. Wird vom Script start automatisch beim Reboot geladen.

Kommandos am x25sniffer Prompt

Folgende Kommandos stehen am x25sniffer zur Verfügung:

dellog	Script zum Löschen der Logfiles (nach dem Ablauf des Scripts dellog muß der Rechner entweder mit dem Script halt gestoppt werden oder mit dem Script reboot wieder gebootet werden, da für die Sniffer-Applikation kein Logfile mehr zur Verfügung steht.)
halt	Script zum Anhalten des Betriebssystems (nach ca. 40 Sekunden ertönen zwei Beeptöne im Abstand von ca. 2 Sekunden – danach kann der Rechner abgeschalten werden.)
reboot	Script zum Rebooten des Betriebssytems
tail –f x25sniffer_temp_*	Mitlesen der gerade vom Schnüffler aufgezeichneten Telegramme. Beenden Sie das Mitlesen mit CTRL-C (Anm: um 00:00 Uhr wird ein neues Logfile angelegt. Daher um 00:00 das Mitlesen beenden mit CTRL-C und neu Starten mit CursorUP und ENTER).
exit	Verlassen Sie den x25sniffer durch Eingabe des Kommandos exit

Der Bedienablauf um am Schnüffler mitzulesen und am Ende der Arbeit das Logfile zu löschen und den Rechner anzuhalten wäre somit:

```
Anmeldung am Schnüffler
Username: x25
Paßwort: x25
tail –f x25sniffer_temp_*
CTRL-C
dellog
halt
(wenn Anmeldung via telnet erfolgt ist): exit
```

Eine Kommandosequenz mit der Sie das aktuelle Logfile am x25sniffer löschen und eine neue Testaufzeichnung starten, finden Sie im nächsten Kapitel.

Abholen des Logfiles

Das Abholen der Logfiles erfolgt z.B. mit ftp. Anmeldung an der Maschine 192.168.20.1 mit Username x25 und Paßwort x25 und Wechseln in das Directory sniffer_archiv (mit cd).

In diesem Directory liegen die gezippten Tagesfiles. Jedes Zipfile (z.B. **22Mar2002.zip**) beinhaltet ein gleichnamiges Logfile mit der Endung .log (**22Mar2002.log**).

Die Schnüfflerdaten werden im Homedirectory des Users x25 (/home/x25) aufgezeichnet in einem File sniffer_temp_<process-id>_<lfde.Nummer>.log Dieses File wird um 00:00 ins Directory sniffer_archiv kopiert umbenannt auf <datum>.log und gezippt in ein File <datum>.zip.

Im Directory sniffer_archiv existiert ein File **x25_sniffer_tempfiles_from_reboot.log** in dem bei jedem Reboot ein eventuell vom letzten Lauf liegengebliebenes Logfile (sniffer_temp_<process-id>_<lfde_Nummer>.log) archiviert wird.

Löschen der archivierten Logfiles

Das Löschen der Logfiles am x25sniffer erfolgt mit der nachfogenden Kommandosequenz, in der im Wesentlichen nur das Script dellog aufgerufen wird. Dellog säubert alle archivierten Logfiles von der Harddisk. Der Schnüffler ist dann wieder bereit für neue Aufzeichnungen. Soll auch eine gerade aufgerufene Aufzeichnung mit rm x25sniffer_temp_* gelöscht werden, ist ein Reboot des Schnüfflers erforderlich.

Anmeldung am Schnüffler
Username: **x25**
Paßwort: **x25**
dellog
rm x25sniffer_temp_*
reboot
(wenn Anmeldung via telnet erfolgt ist): **exit**