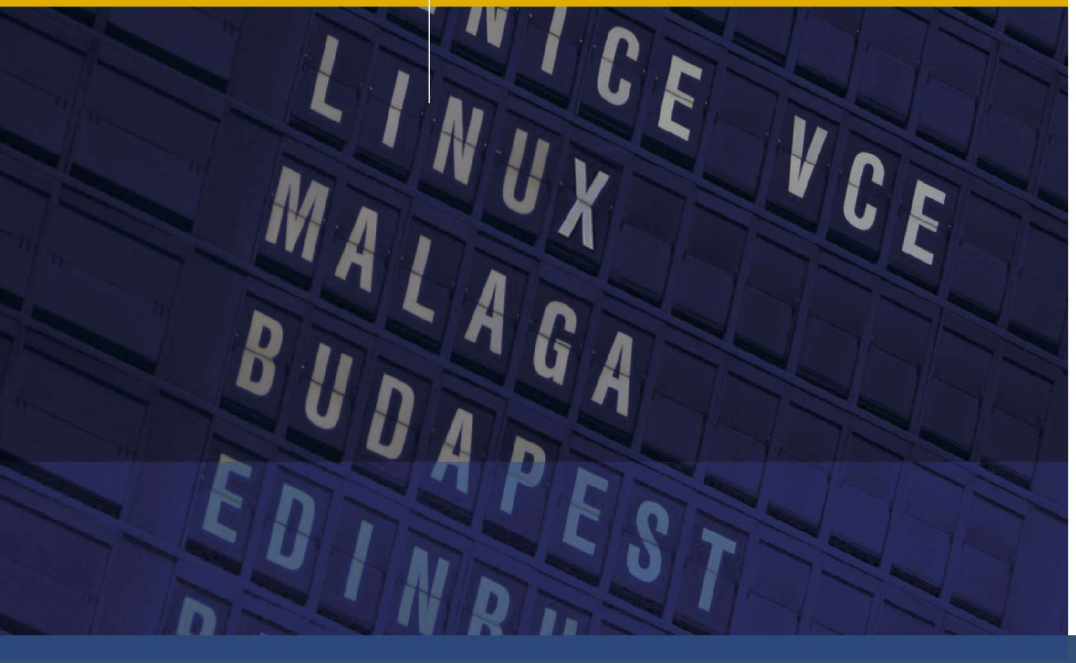
LINUX TAG

Where .com meets .org

Berlin
27 December 2004

Workshop: Reverse Engineering the SAP R/3 Client Protocol

...for every business



Nils Magnus
Jochen Kellner

21C3 Chaos Communication Congress
Berlin, Germany
December 27 29, 2004

Agenda

Overview of the SAP R/3 architecture (from a networker's point of view)

Problem of undocumented client protocol

Current findings

Workshop: reverse protocol details

Agenda

Why SAP R/3 should bother all of us

Overview of the SAP architecture
(from a networker's point of view)

Problem of undocumented client protocol

Current findings

Workshop: reverse protocol details

The SAP R/3 universe

First of all: SAP is huge and confusing

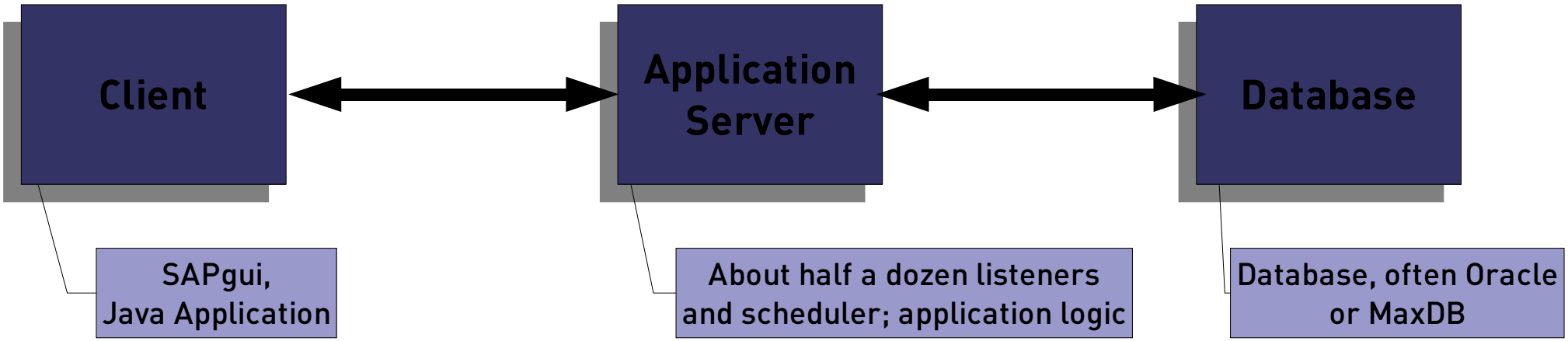
Sometimes difficult to understand SAP people or documentation

SAP makes a great deal of naming everything differently (DIAG, RFC, SAP-routers , ...)

The main achievment seems to be scalability

Simple SAP R/3 setup

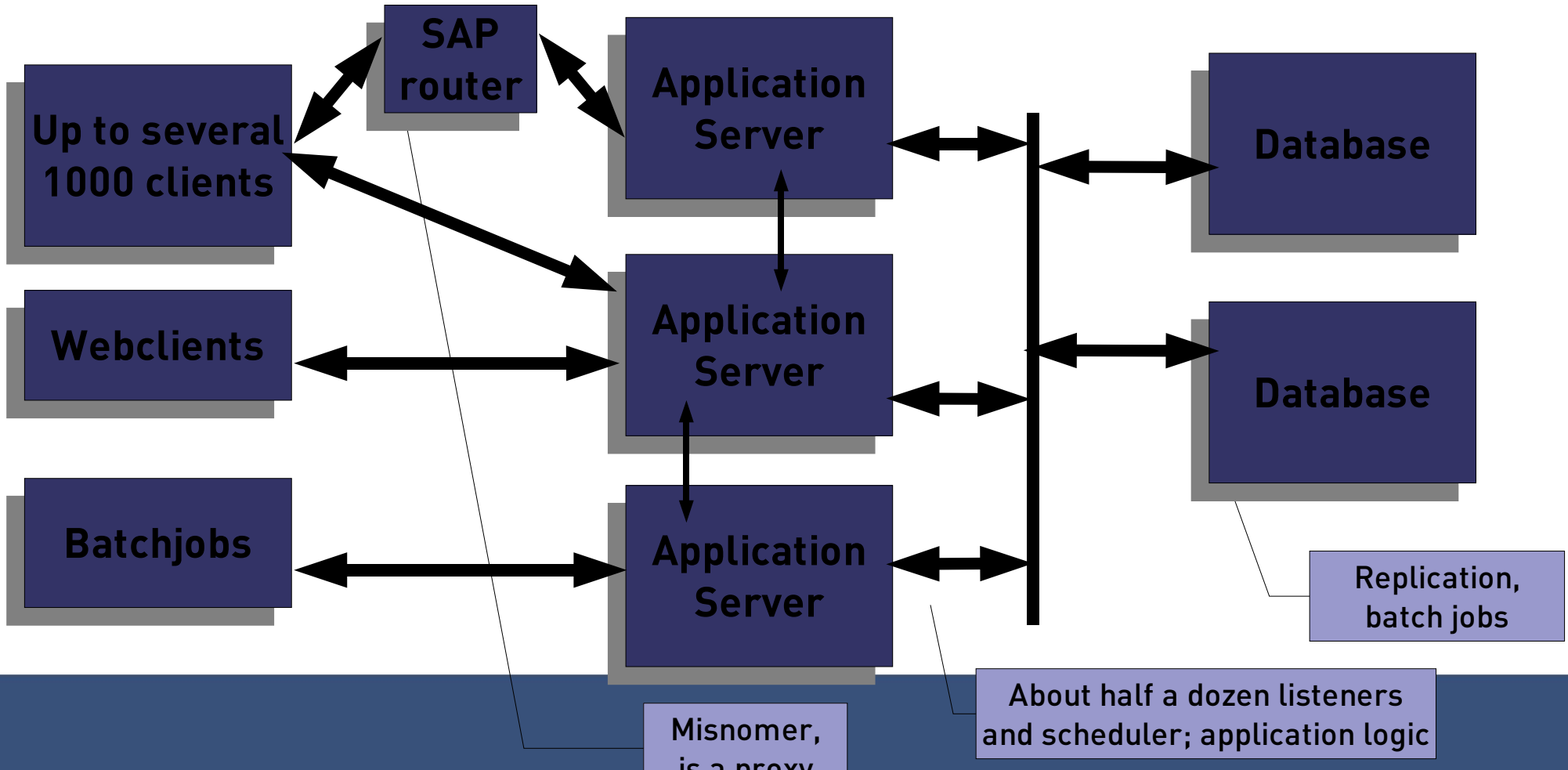
Old fashioned three tier database application



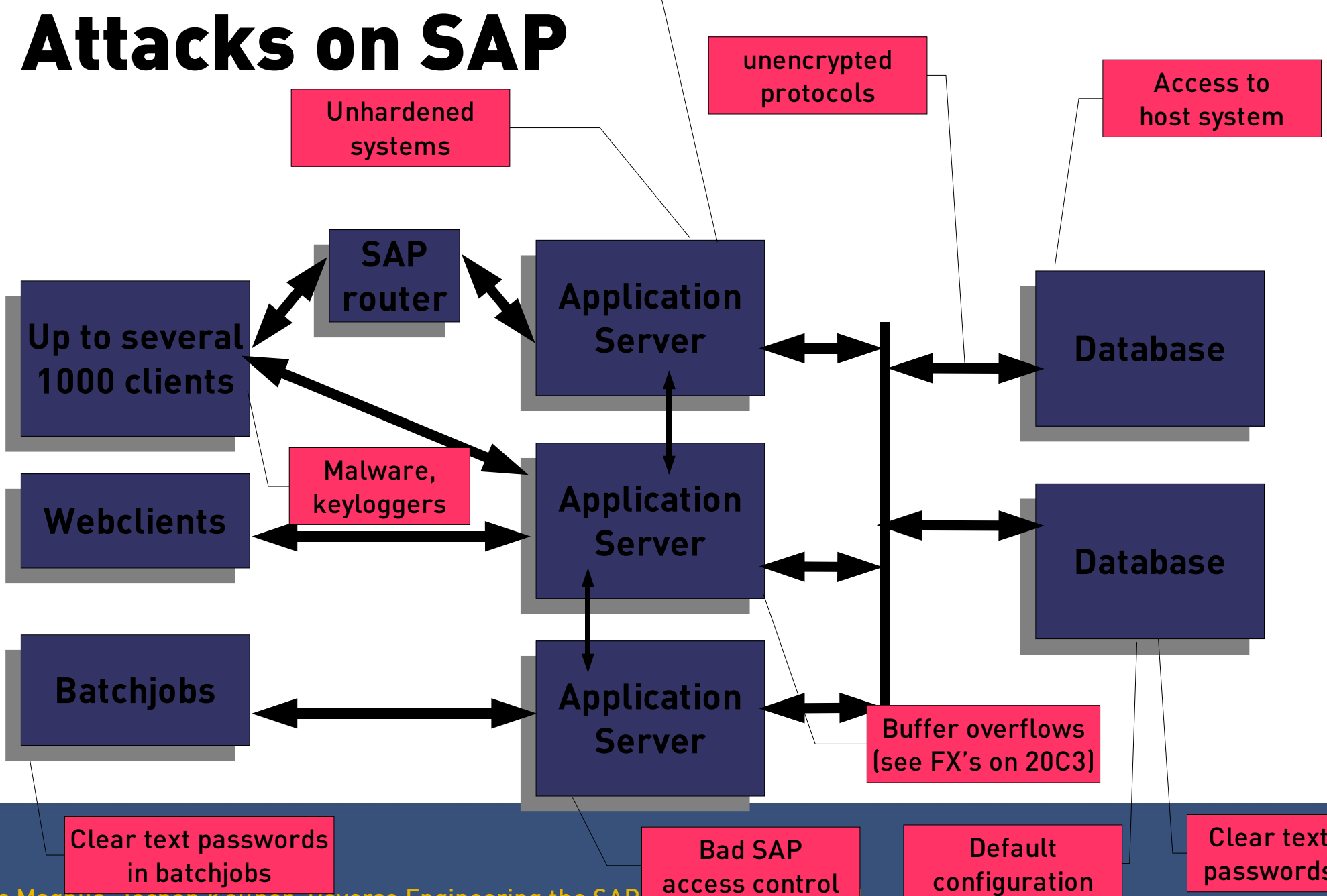
- Runs on a number of platforms
- Supports mainframes, Linux and even Windows
- Encapsulates most of the platform

Complex SAP R/3 setup

Old fashioned three tier database application



Attacks on SAP



Attacks on SAP installations

Most SAP experts focus solely on application layer issues

- User priviledges, access control

System administrators don't touch SAP

Bad protection on OS level

Important: That's not necessarily SAP's fault

But: What do they do to help it?

Security provided by SAP

A lot of documentation

- Often incomprehensible for networkers

A number of documented APIs

- Plug-in encryption
- Access control

A set of recommendations

- Often not obeyed to by op staff

How to implement security

- Allocate lots of time
- Understand the system and the language
- Harden every server
- Place firewalls
- Encrypt data transmission

SAP client protocol

- Most attacks are commodity attacks that apply to every system
- Vulnerabilites to application server have been addressed by FX
- Client protocol between sapGUIs and application servers is often unprotected
- Once claimed encrypted , now officially disguised

Client protocol details

- Protocol internally called DIAG
  - (not to be confused with the RFC protocol of the same name!)
- Full specifications available only with NDA
- Stream based network connections
  - TCP, but potentially over several other protocols, too
- Some details are available within the SAP help

More details

TCP/3200 + *x*
where *x* is the instance identifier

C/S-based protocol, exchanging blobs

- 10 Request to AS
- 20 Response with form data and result data
- 30 New data and new requests
- 40 GOTO 20

Scanner result

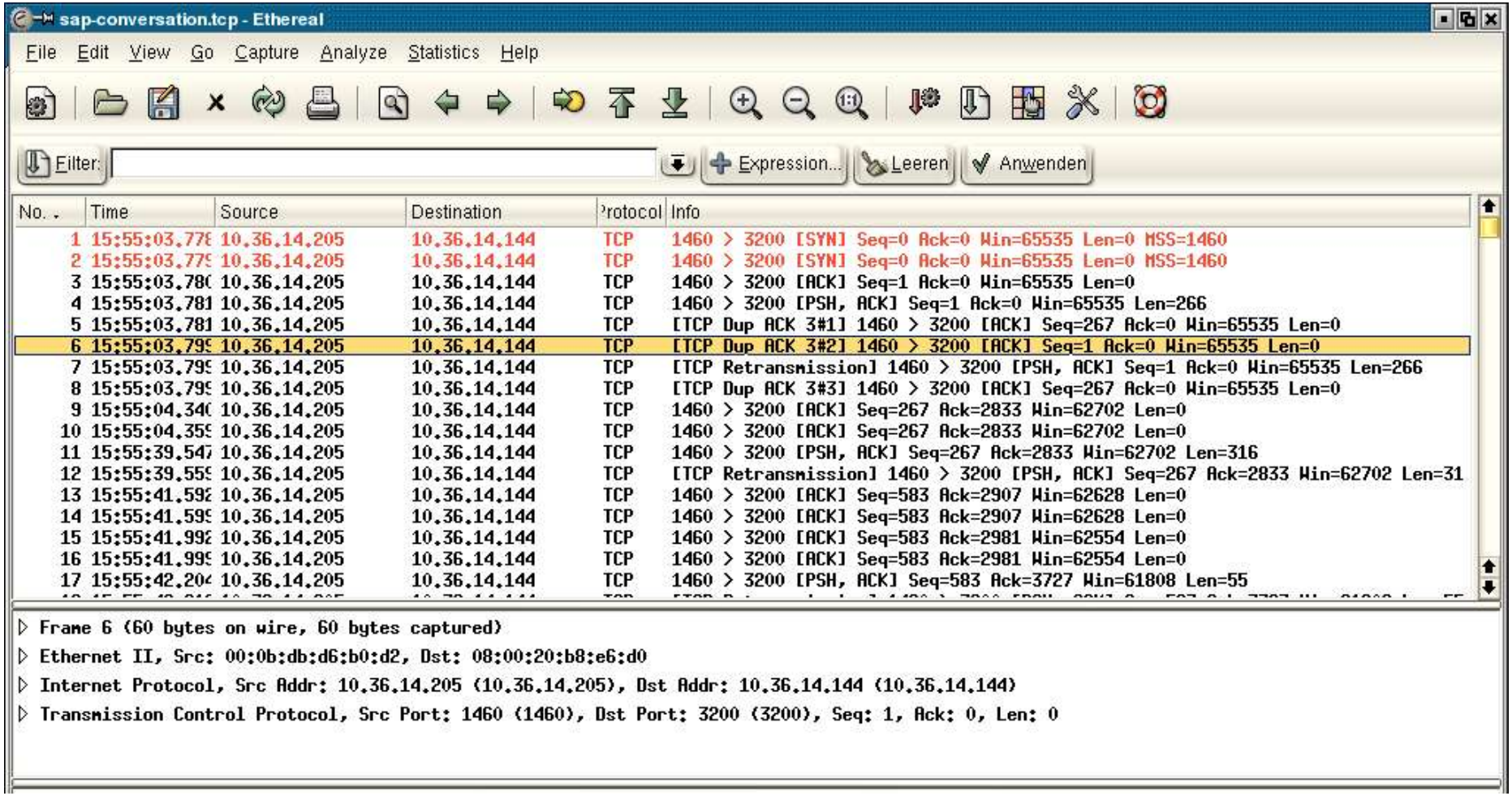
```
# nmap (V. 3.00) scan initiated as: nmap -sT -v -p3200-3900 -o nmap-tcp:03.txt 10.36.14.144

Interesting ports on (10.36.14.144):
      (The 694 ports scanned but not shown below are in state: closed)

      Port       State      Service
      3200/tcp   open       unknown
      3300/tcp   open       unknown
      3600/tcp   open       unknown
      3773/tcp   open       unknown
      3777/tcp   open       unknown
      3786/tcp   open       unknown
      3900/tcp   open       udt_os

# Nmap run completed -- 1 IP address (1 host up) scanned in 22 seconds
```

Trace (client side)



Block transmission

First 4 octetts are block length

A number of similiar starting octetts

Scrambled data payload

Starts with 0x1f 0x9d

From /etc/magic:

```
# standard unix compress
0      string        \037\235      compress'd data
>2     byte&0x80     >0            block compressed
>2     byte&0x1f     x             %d bits
```

Compressed data payload

- Looks like the LZC algorithm
- Also used in old-fashioned compress (1)
- Strings LZ.* can be found in sapGUI binary
- Just extracting the payload and using uncompres does not work
- Bit-length field is wrong

LinuxTag

Leading Free Software and Linux event

Talks and exhibition

Karlsruhe, Germany: June 22 25, 2005

Call for Papers still open until January 15:

http://www.linuxtag.org/

Contact

Nils Magnus
Program Chair, LinuxTag e. V.

University of Kaiserslautern
67653 Kaiserslautern
T +49-631-310-9371

magnus@linuxtag.org