PRAY-ON-TETRA

DREILÄNDERECK-SYSOP-TREFFEN 2023

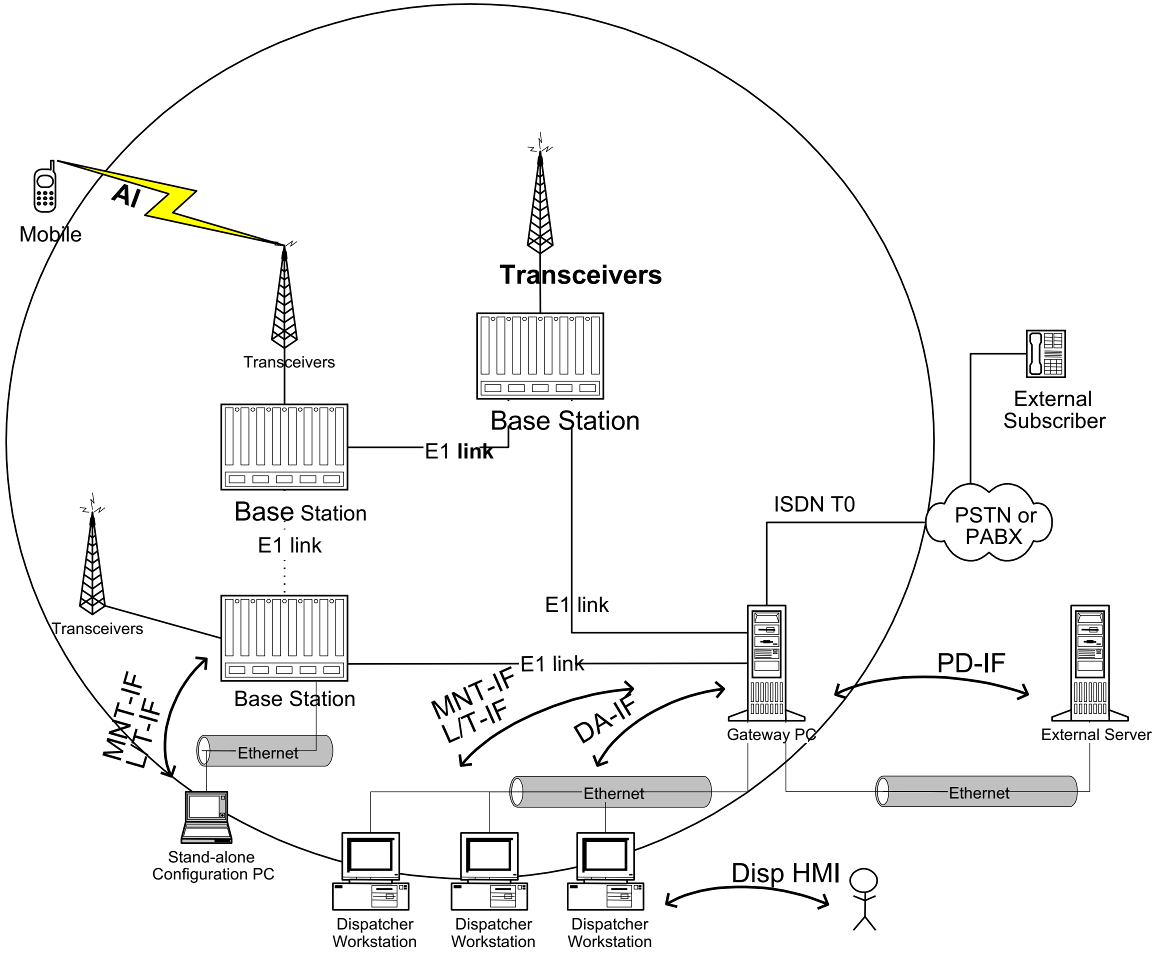
Artem DL5ABM

PRAY ON TETRA?

- Side project of BM team to research Motorola CTS-x00 linking capabilities
- TETRA TMO in HAM-TETRA
- Engineering Team
  - Artem DL5ABM – research and development
  - Simon DL1NE – research and testing
  - Stefan LZ1SEO – development and support
- Testing Team
  - Torben DH6MBT

COMPACT TETRA ARCHITECTURE

- Designed by DAMM and Frequentis, labled by Motorola
- Uses E1 closed-ring topology
- Up to 8 base-stations
- No need in dedicated network core
- Voice and signalling only over E1
- Proprietary <Inter-site Connect>
- Not compatible to ISI/E1
- Base-station controller (BSC411) runs on Windows NT 4.0 Embedded

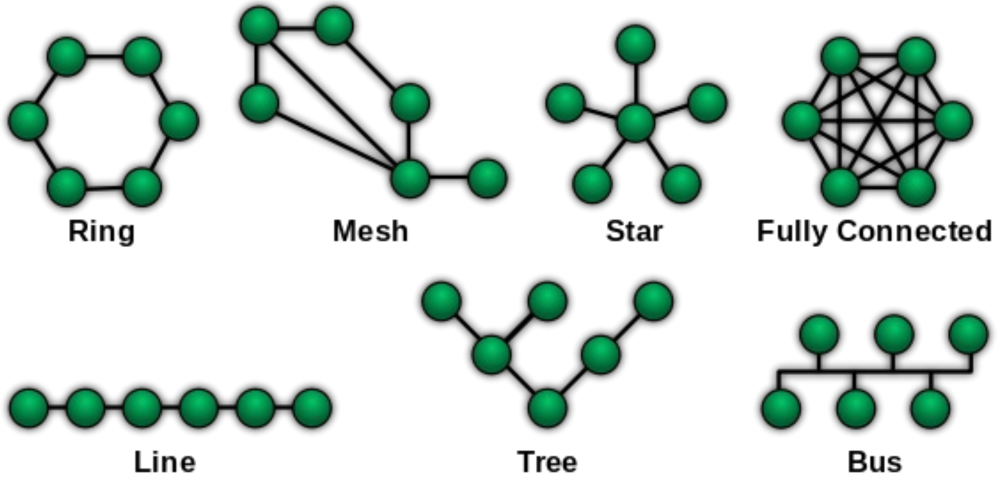


HAM-TETRA TYPICAL USE

- Low-entry approach
  - RF-gateway bridge (usualy mobile radio brick) + Raspberry / PC
  - Usualy – SVXLink (https://www.hamtetra.network)
  - Cons:
    - Single group per gateway simoultanous
    - Double transcoging ACELP – GSM/Speex/OPUS and back
    - No acrual ISSI/GSSI (FM-like UX, IDs of the brick are in use)
    - Lack of TETRA functionality outside local base-station
- High-entry approach
  - TDMoIP
  - Pros: fully-functional Inter-site Connect
  - Cons:
    - 2x 2 Mbit/s 8000 packet/s UDP connection
    - Requires very stable IP links
    - €€€ for TDMoIP gateway
    - Bad compatibility between different TDMoIP vendors

PROJECT GOALS

- Inter-Site Connect protocol research
- Switch to IP with low bandwith reliable connection
- Establish solution based on star topology with backward compatibility to bus tolopogy (non-closed ring)
- Direct base-station integration



CURRENT STATE

- Covered about 90% of Inter-Site Connect
- Designed and implemented base-station companion software – dummy
- Implemented reasearch-grade simple server backend – pray backend
- Implemented web-based protocol dissector and steam player – pray frontend
- All CTS TMO functions are available when connected over pray:
  duplex calls, SDS, LIP GPS, roaming/handover of calls between cells

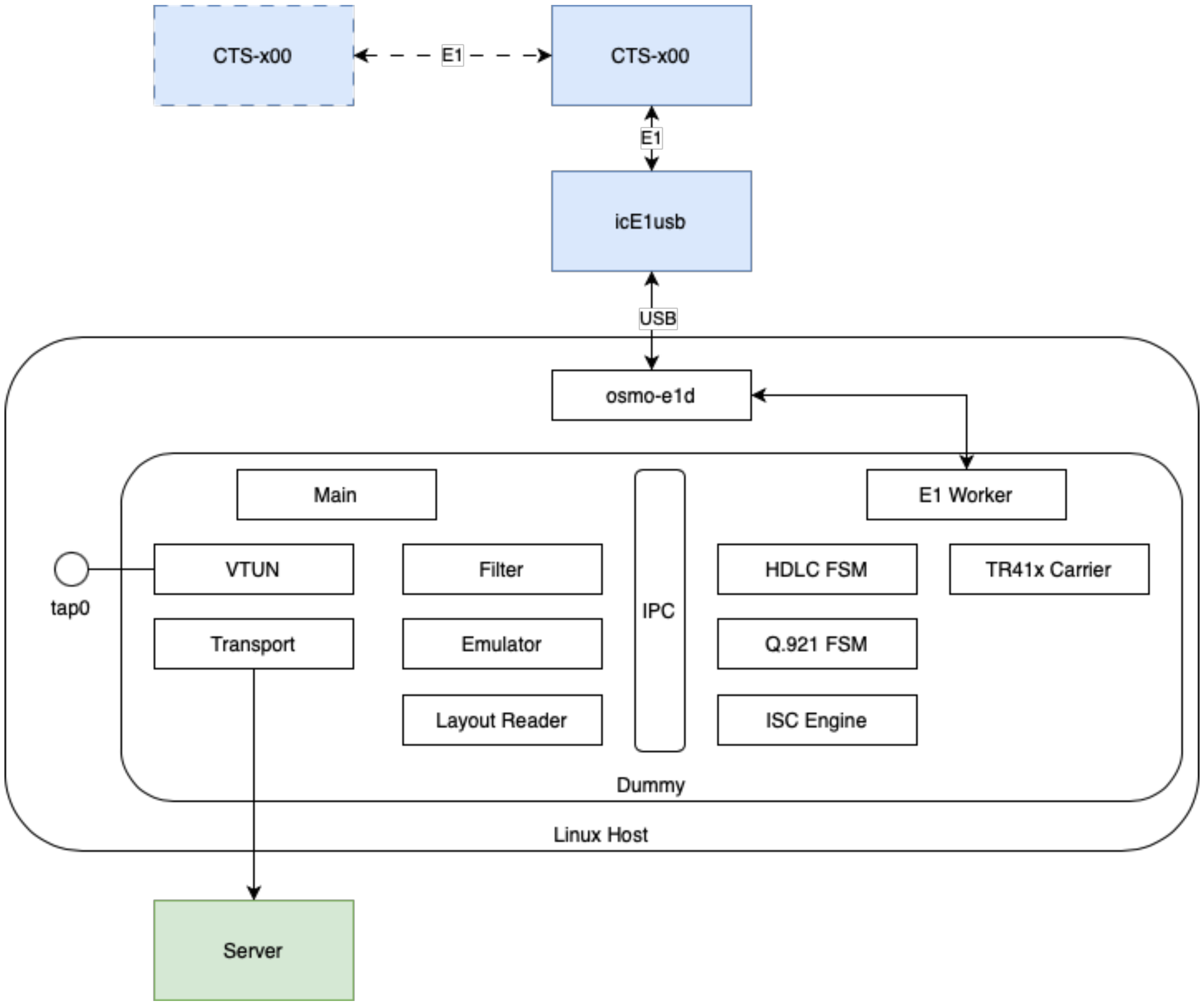
E1 INTERFACE

- Osmocom icE1usb
  - Available for ordering, not expensive
  - USB to connect to PC
  - Role (NE/NT) can be selected by jumpers,
    can be used with a regular network cable
  - User-space Linux driver, no need to change kernel
  - Supports required work mode (SUPERCHANNEL)
- https://wiki.brandmeister.network/index.php/E1/T1_Interface

DUMMY

- Gateway software to run on E1 connection
- Transmits application-level messages between CTS E1 and backend server
- Decodes/encodes full signalling stack:
  - E1 handler \
  - HDLC FSM - (normally done by IC on BSC411 board)
  - Q.921 FSM /
  - Inter-site Connect transport including priority management (normally done by ISCD2.EXE)
- Decodes/encodes E1 and pre-buffer carrier streams (normally done by BSC411/TR412 boards)
- Partially emulates BSS.EXE/GWS.EXE (presence / status updates)
- VTUN over E1 between CTS and host (does not forward to the server)
- Uses the same bss3.txt configuration file as a base-station
- Debian 11 arm64 or amd64, tested on Raspberry Pi 3*, CM4 and Intel x64 PC
- Typical IP bandwith 4-100 Kbits/sec

* Some revisions of Raspberry Pi 3 have issues with icE1usb connection stability due to USB NIC

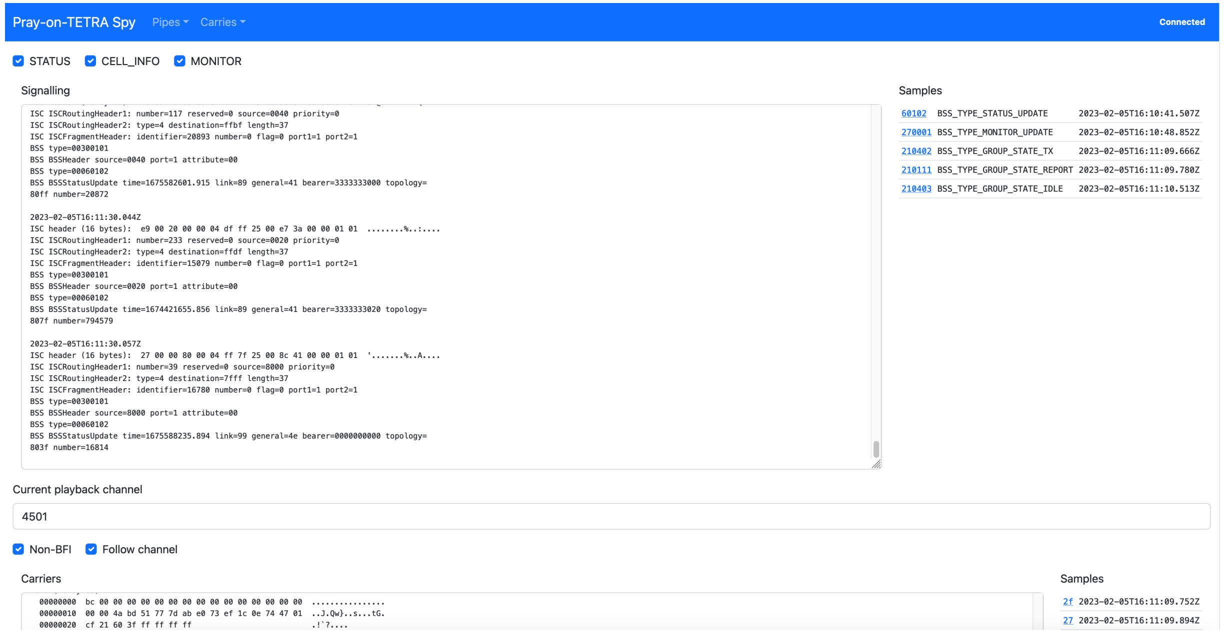

CTS-x00
E1
CTS-x00
E1
icE1usb
USB
osmo-e1d
Main
IPC
E1 Worker
tap0
VTUN
Filter
HDLC FSM
TR41x Carrier
Transport
Emulator
Q.921 FSM
Layout Reader
ISC Engine
Dummy
Linux Host
Server

DUMMY PROTOCOL DESIGN

- HTTP and WebSocket based
- Supports redirection (HTTP 301), safe HTTP authentication (digest, NTLM)
- Can use TLS
- 2-phase negotiation:
  - Service discovery and authentication
  - Socket connection establishment
- Pros:
  - Good NAT traversal
  - Can use intellectual descovering by geolocation, channel availability

PRAY BACK- AND FRONTENDS

- Develooped to support protocol reasearch and tests
- Backend
  - Very thin “reflector” with channels support (pipes)
  - Runs on node.js
- Frontend
  - Single-page web-application
  - Dissector implemented in C as a WebAssembly
  - ACELP codec ported as a WebAssembly



☑ STATUS ☑ CELL_INFO ☑ MONITOR

Signalling

```
ISC ISCRoutingHeader1: number=117 reserved=0 source=0040 priority=0
ISC ISCRoutingHeader2: type=4 destination=ffbf length=37
ISC ISCFragmentHeader: identifier=20893 number=0 flag=0 port1=1 port2=1
BSS type=00300101
BSS BSSHeader source=0040 port=1 attribute=00
BSS type=00060102
BSS BSSStatusUpdate time=1675582601.915 link=89 general=41 bearer=3333333000 topology=
80ff number=20872

2023-02-05T16:11:30.044Z
ISC header (16 bytes):  e9 00 20 00 00 04 df ff 25 00 e7 3a 00 00 01 01  ........%..:....
ISC ISCRoutingHeader1: number=233 reserved=0 source=0020 priority=0
ISC ISCRoutingHeader2: type=4 destination=ffdf length=37
ISC ISCFragmentHeader: identifier=15079 number=0 flag=0 port1=1 port2=1
BSS type=00300101
BSS BSSHeader source=0020 port=1 attribute=00
BSS type=00060102
BSS BSSStatusUpdate time=1674421655.856 link=89 general=41 bearer=3333333020 topology=
807f number=794579

2023-02-05T16:11:30.057Z
ISC header (16 bytes):  27 00 00 80 00 04 ff 7f 25 00 8c 41 00 00 01 01  '.......%..A....
ISC ISCRoutingHeader1: number=39 reserved=0 source=8000 priority=0
ISC ISCRoutingHeader2: type=4 destination=7fff length=37
ISC ISCFragmentHeader: identifier=16780 number=0 flag=0 port1=1 port2=1
BSS type=00300101
BSS BSSHeader source=8000 port=1 attribute=00
BSS type=00060102
BSS BSSStatusUpdate time=1675588235.894 link=99 general=4e bearer=0000000000 topology=
803f number=16814
```

Samples

```
60102  BSS_TYPE_STATUS_UPDATE       2023-02-05T16:10:41.507Z
270001 BSS_TYPE_MONITOR_UPDATE      2023-02-05T16:10:48.852Z
210402 BSS_TYPE_GROUP_STATE_TX      2023-02-05T16:11:09.666Z
210111 BSS_TYPE_GROUP_STATE_REPORT  2023-02-05T16:11:09.780Z
210403 BSS_TYPE_GROUP_STATE_IDLE    2023-02-05T16:11:10.513Z
```

Current playback channel

4501

☑ Non-BFI ☑ Follow channel

Carriers

```
00000000  bc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000010  00 00 4a bd 51 77 7d ab e0 73 ef 1c 0e 74 47 01  ..J.Qw}..s...tG.
00000020  cf 21 60 3f ff ff ff ff                          .!`?....
```

Samples

```
2f 2023-02-05T16:11:09.752Z
27 2023-02-05T16:11:09.894Z
```

To be continued..