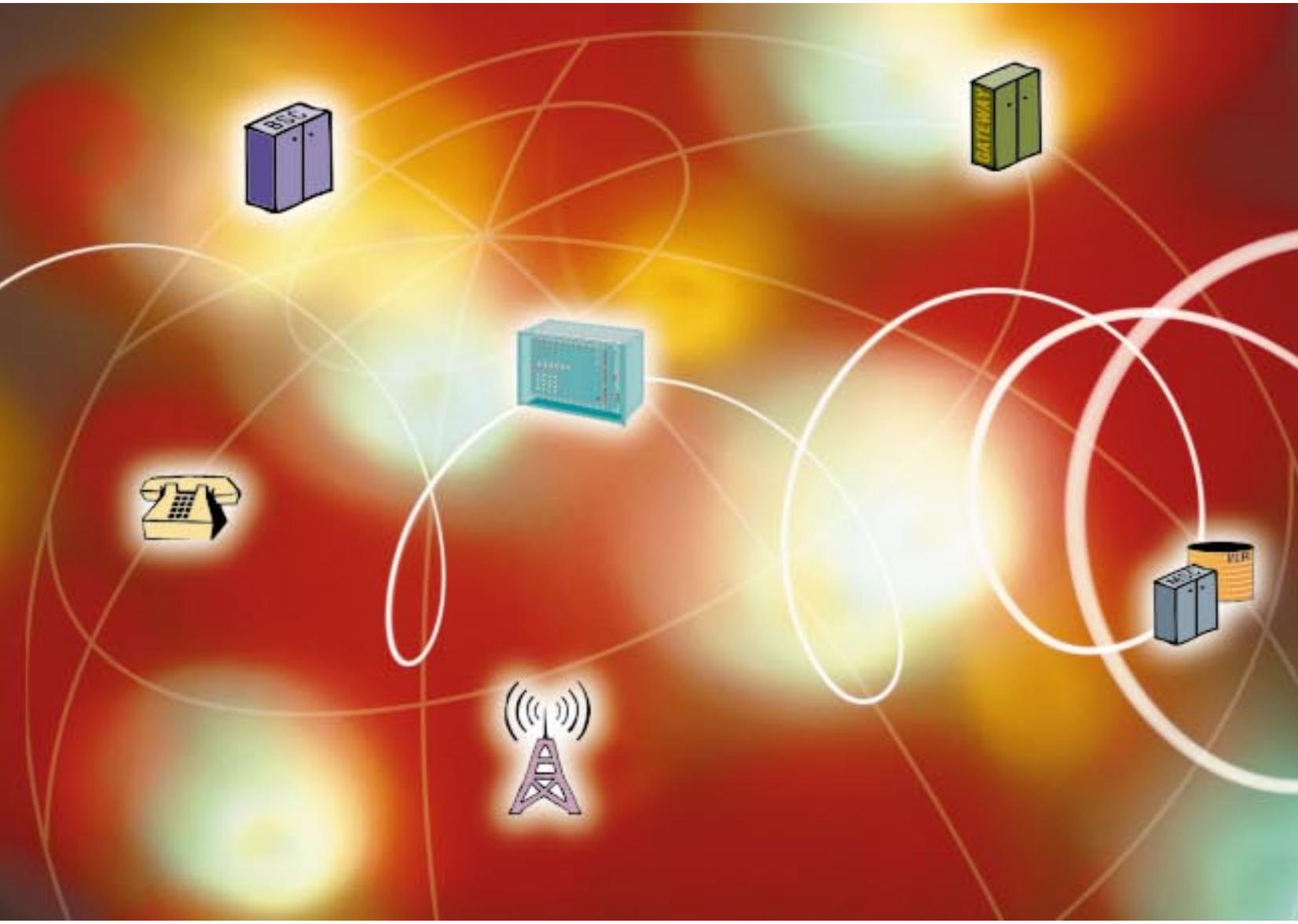
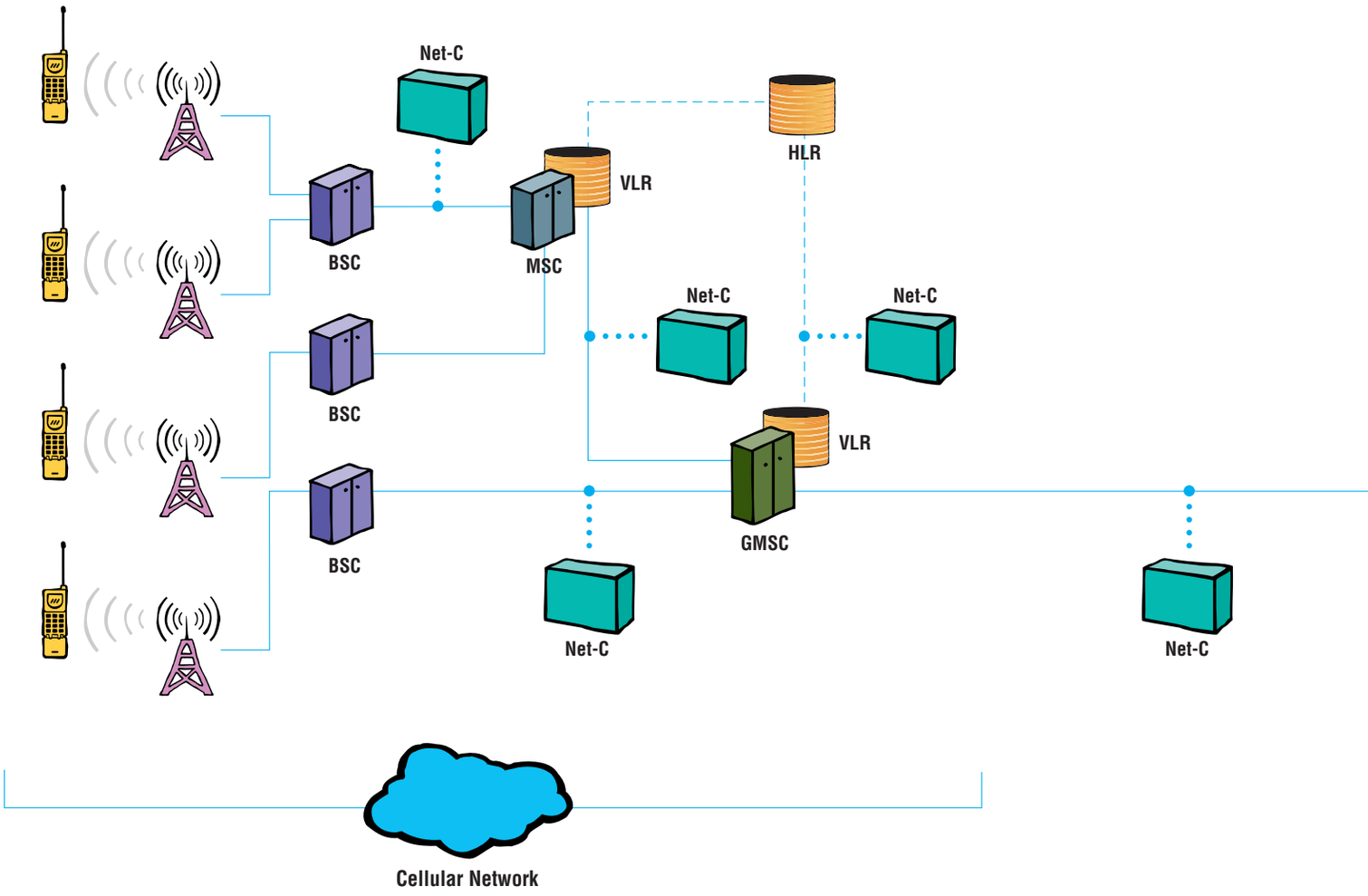
Tektronix

Net-C



Global communications network monitoring for high efficiency, quality of service and fraud detection.

NET-C FOR MOBILE NETWORKS



Real-time traffic analysis at the E1 level

- Data collection at different network levels (GMSC, MSC, and BSC)

Quality of Service evaluation (In-service Non-intrusive Measurement Device, ITU-T P.561)

- Analysis of transmission quality parameters

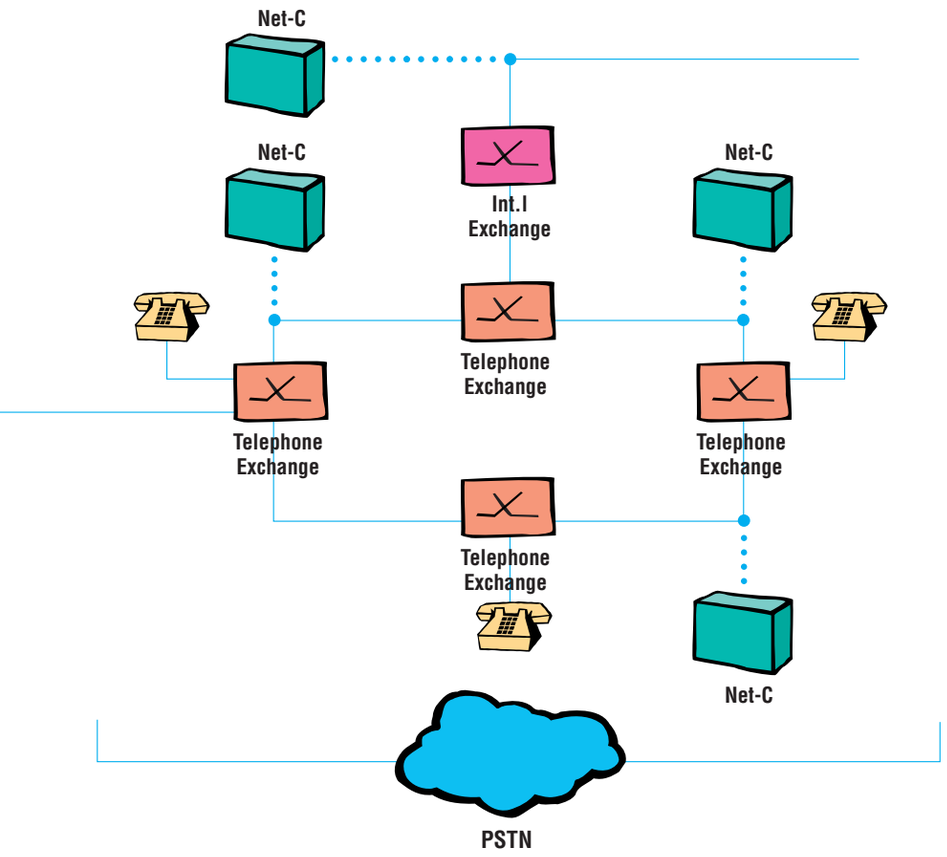
Real-time monitoring of subscriber activities

- Roaming analysis (MAP protocol)

Real-time Fraud Detection and Blocking

- Call-Back, Blue Box, and other in-band fraud
- Clone-detection activities
- Roaming fraud

Net-C for Fixed Networks



Real-time traffic analysis at the E1 level

- Signaling monitoring on local, transit and gateway switches

Quality of Service evaluation (In-service Non-intrusive Measurement Device, ITU-T P.561)

- Analysis of transmission quality parameters

Fax Quality analysis

- According to ITU-T E.45x

Real-time Fraud Detection and Blocking

- Call-Back, Blue Box, illegal landing and other in-band fraud

System Overview

Net-C is an in-service, non-intrusive monitoring system that interfaces to telecommunication networks at the E1 level. The system assists network managers in obtaining and maintaining high network efficiency, optimizing investment, measuring quality of service and reducing revenue loss due to fraud or network abuse.

Net-C is independent of the network equipment and is external to the network it monitors. This ensures both data collection at strategic nodes even during peak hours and uniformity of data from the whole network.

Basic Functions

Net-C monitors the signaling during the set-up, connection and release phases of a call to assess Quality of Service and detect network abuses. In particular, Net-C's distributed architecture, modularity and open system features make it easily adaptable to different applications and requirements. Net-C can be customized easily to suit national implementations of standard signaling systems.

Functional Description

Data collection

Peripheral Units provide simultaneous monitoring of a number of E1s, collecting and decoding signaling information, alarms and in-band information.

Triggered by the set-up and release phases of the calls, Net-C Peripheral Units can monitor the connection phase, where a conversation or a fax or data transmission takes place, in order to:

- get detailed information on traffic activity,
- assess the quality of the service being carried by the connection,
- detect voice band signals that can mean network abuses.

Net-C applications support both channel associated (CAS) and common channel (CCS) signaling systems and are easily customizable to different national implementations of standard signaling systems.

Net-C can also monitor application protocols, such as MAP protocol. The system can then detect fraudulent calls and monitor customer activities in home and visitor networks. The data is organized into Call Detail Records (CDRs). The information contained in the CDRs can vary with the specific application.

System functions are completely automatic and user intervention is not required for normal operation. Once a Peripheral Unit is configured, it becomes completely autonomous, storing the collected data until the Central Unit polls it. The data is then transferred for consolidation and analysis.

Call-based monitoring

Data collected from Portable Units can provide detailed information on traffic activity. Each call or call attempt is checked, and network monitoring is performed non-intrusively on live communications.

Collected data includes:

- date and time
- Stream ID (or OPC and DPC)
- Timeslot or CIC ID
- call direction (incoming or outgoing)
- call duration (time between IAM and REL messages)
- conversation duration (the time between ANM or CON and REL messages)
- seizure type (subscriber, national, international)
- call origin (ISDN or non-ISDN)
- ISDN user part (requested, preferred or not requested)
- echo control device indicator (present, not present)
- redirection information (present, not present)
- A number (with address presentation restricted indicator and screening indicator)
- B number delay (between last digit and the first subsequent message)
- setup delay (between IAM and the first message on the call outcome)
- end of dialing (not received, undifferentiated, free, busy, or wrong number)
- answer (not received, not qualified, charged, not charged)
- release cause value (for CCS7 ISUP and TUP) and location (e.g. user, public network, transit network)
- calling party's category (e.g., national operator, ordinary calling subscriber, calling subscriber with priority, ...)
- called party's category (ordinary, pay phone)
- call category (e.g., voice 64 Kbit/s, fax group 2/3, fax group 4, ...).

CDRs are presented to the operator through a Windows interface, using different methods at different levels to fulfill each user's analysis requirements.

- Call Records provide for analysis at the individual call level. Complete Call Detail Records (CDRs) are displayed containing the detailed information for each call as measured by the Peripheral Units.
- Maps present a global view of network performance, giving a topological representation of the monitored network in terms of nodes and the connections among them. For example, depending on the values of the fax indexes, you can have a color change indicate the status of a specific connection.
- Graphs and histograms give a different view of the information presented in the call records and maps.

Quality of Service Assessment

Quality data analysis and storage

Data from the Peripheral Units is processed by the Central Unit to obtain information about the state and performance of the network. Depending on the type of quality analysis required and on the signaling system in use, the reports contain different kinds of information according to ITU-T P.561, E.45x.

INMD information for both conversation directions (according to ITU-T P.561)

- speech activity factor
- active speech level
- psophometric noise level
- echo loss
- speech echo path delay
- one-way transmission
- PCM coding error
- PCM threshold violation
- front-end clipping
- double talk

Fax quality information (according to ITU-T E.45x)

- error correction indication
- non-standard requirement
- transmission resolution
- protocol speed
- calling fax ID
- called fax ID
- calling fax manufacturer
- called fax manufacturer
- number of pages transmitted
- initial speed
- speed reduction indication
- cut-off indication
- phase in which the cut-off occurred
- image degradation indication (from RTP and RTN messages)
- efficiency rating (100% when all the pages are transmitted at the initial speed)

Data can be displayed as call records, maps, graphs and histograms.

International signaling systems supported by Net-C are:

- **CC7 ISUP**
- **CC7 TUP**
- **R2**
- **C5**
- **BSSMAP/DTAP (A-interface)**

Real Time Fraud Detection and Blocking

Net-C detects and, if necessary, blocks fraud activities:
- Call-Back and Blue Box
- "clone" activities
- roaming fraud

Call-Back and Blue Box

Call-Back and Blue Box frauds are typically carried out using DTMF signaling starting from the answer or from the end of dialing. Net-C can detect this event and, if required, block the fraudulent call by clearing the voice link.

To avoid this countermeasure, service providers normally offer access to Call-Back service via the operator at an additional cost. Net-C can fight this type of fraud by blocking the outgoing booking calls. Once the trigger, the number corresponding to the Call-Back service provider, has been detected, it is added to a blacklist, and all calls to that destination are suppressed by the Net-C system.

The system elaborates statistics of Call-Back and Blue Box calls: number of fraudulent calls, percentage of total number of calls, average duration, and other statistics based on destination and origin.

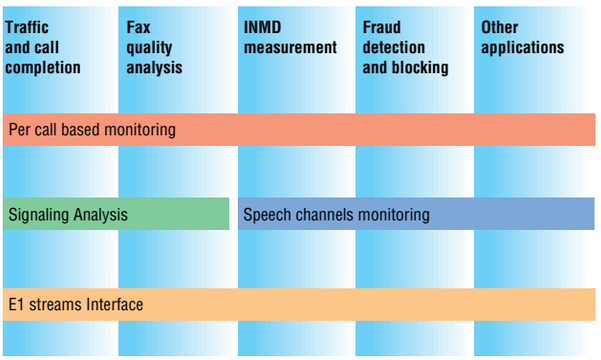
Clone activities and roaming frauds

Net-C can also be used to detect and block telephone fraud in the wireless network.

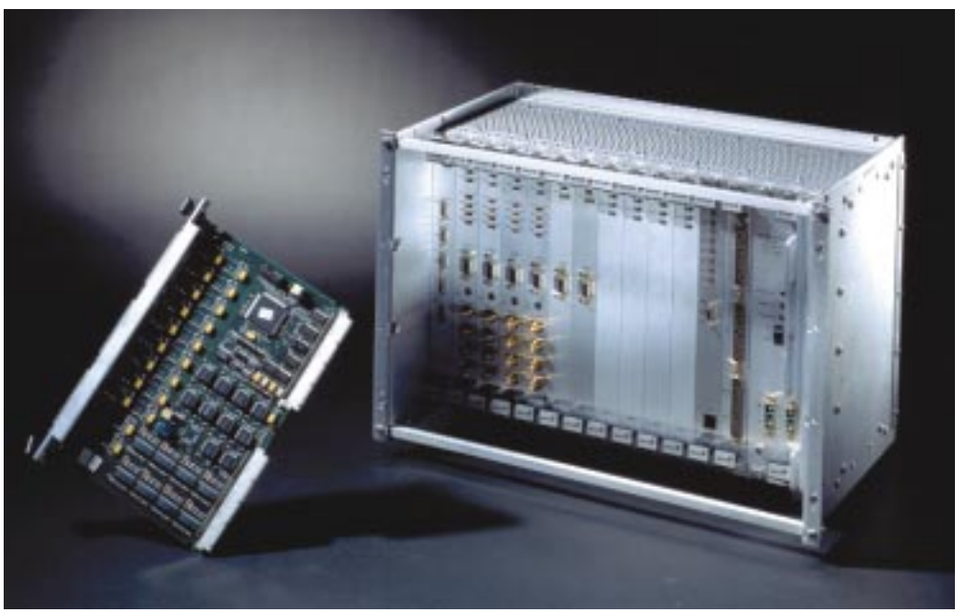
In the analog wireless environment, Net-C can use CDR information to detect clone activities such as unauthorized simultaneous calls originating from the same cellular telephone number. Net-C can generate alarms in case of suspicious behavior, such as long calls or calls originating or terminating on a blacklisted user terminal. It can also block fraudulent calls by clearing the voice channel.

In the GSM environment, Net-C is able to monitor the MAP protocol, which is the protocol used to exchange roaming information between GSM operators. With this information, the system can detect fraudulent activities in real-time, such as calls by unauthorized users.

The Net-C advantage in fighting mobile fraud is the detection and blocking of fraudulent activities in real time, allowing operators to immediately reduce revenue losses. Net-C is the ideal complement to fraud management systems based on traffic profiling.

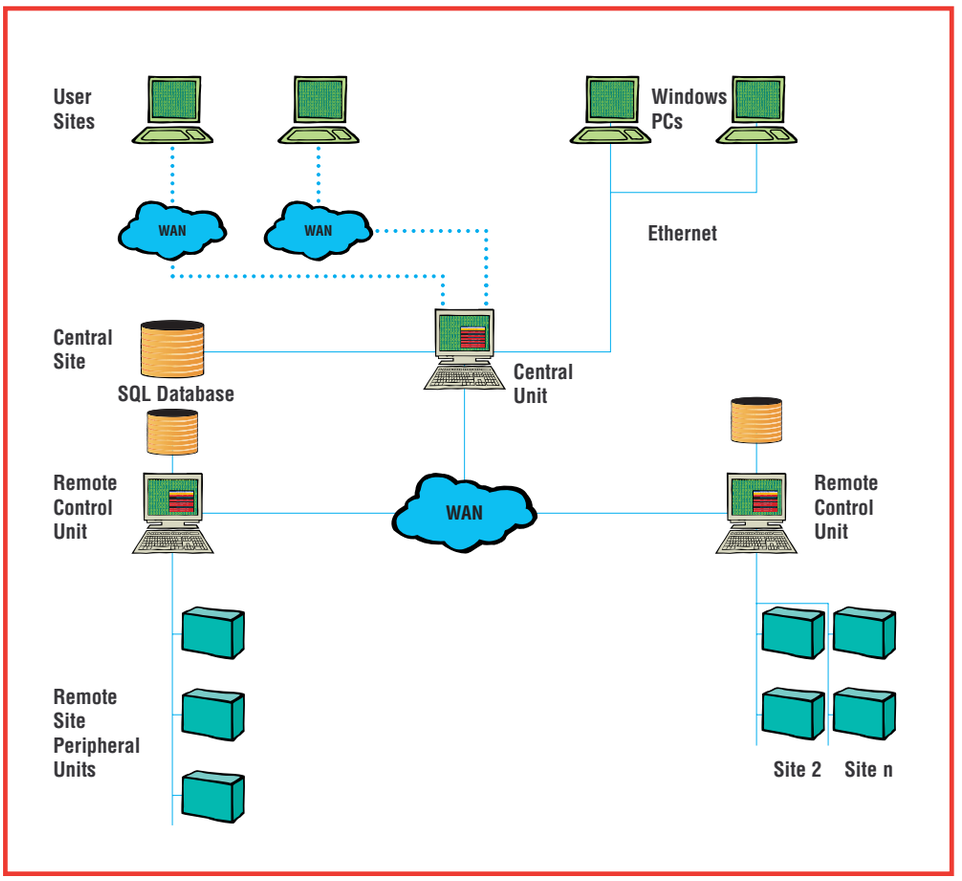


Net-C monitors the signal during set-up, connection and release phases of a call.



A global view of network performance can be provided through maps, giving a topological representation of the monitored network in terms of nodes and the connections among them.

System Architecture



Net-C is modular and scalable for maximum flexibility. System configuration ranges from small standalone units to a fully distributed system.

The main building blocks are:

- Peripheral Units connected to the network under observation
- Remote Control Units for local management and data collection from the Peripheral Units (optional)
- Central Unit to collect and analyze data from the Control Units or Peripheral Units and to display network information to the users.

Peripheral Units are connected to the telecommunications network through protected monitoring points or at the Digital Distribution Frame (DDF) level with T connectors that provide high impedance connection. Where intrusive monitoring is required for fraud blocking, measurement cards are inserted in series with the stream. Nonetheless, the insertion is guaranteed to safeguard continuity — even in case of equipment fault — as well as assuring that the signal is not significantly distorted or attenuated.

The fully distributed system contains Remote Sites connected to the Central Unit by a TCP/IP WAN.

The Central Unit provides temporary storage of information and management of the local Peripheral Units.

The Central Unit is a UNIX PC (SCO UNIX System V OS and Oracle® relational database) based on a Client/Server configuration.

User site client is a Windows® 95 computer connected to the Central Unit by WAN/LAN networks.

Net-C, a Modular System

The Net-C system can be upgraded and expanded in several ways, from a standalone transportable unit to a networkwide multi-site and multi-user system. Your system can grow from entry level to a complete system, preserving the hardware investment of the initial installation.

At the peripheral level, you can increase the number of monitored streams by simply adding interface boards into available slots or adding more Peripheral Units. In the same way, you can upgrade measurement capabilities by means of additional measurement boards.

The system can also grow by upgrading the software and adding new application boards to the existing installation.

Transportable Unit

The minimum configuration of the Net-C is a single Transportable Unit, which integrates the functions of one Peripheral Unit and one Central Unit. The Transportable Unit has different configuration capabilities than the Peripheral Unit, but it uses the same application boards and software. It has seven slots for interface and application boards, a CPU board, and a power supply at -72 to -38 VDC. It includes a notebook computer acting as a local controller that provides a simplified version of the Central Unit interface.

Portability

The unit can be moved to sites as needed, but can also be part of a distributed system when controlled by a remote Processing Unit.

User-Friendly Interface

The Windows-based user interface provides easy access to the information, as well as the possibility to post-process data through common graphical and spreadsheet applications.

Easy installation

Once you connect the unit to the streams and configure it, you can rapidly collect real-time information on the network for:

- traffic analysis
- quality analysis
- fax measurements
- voice-quality information
- fraud and network abuse detection

System Building Blocks

Central Unit

The Central Unit comprises one UNIX server with an Oracle database and one or more Windows clients, providing:

- management and control of all Peripheral Units and Remote Control Units
- collection of system-wide measurement records
- elaboration of network-wide information based on individual site data
- data presentation to the user
- interfaces to other applications

Remote Control Unit

The optional Remote Control Unit is a rack-mounted UNIX PC, providing:

- management and control of Peripheral Units
- collection of local measurement records

Peripheral Unit

The Peripheral Unit provides:

- E1 links interface (monitor or drop-insert)
- signaling analysis
- speech analysis
- traffic monitoring
- fax protocol analysis
- INMD measurements
- roaming monitoring
- fraud or Call-Back detection and blocking
- evaluation and storage of elementary measurement records

The Peripheral Unit is a 19" VME card cage with 13 slots for the following interface and application boards:

Demux board

The Demux board provides the interface to the 2 Mb/s PCM E1s. It is equipped with a CPU running the signaling analysis software and DSPs to analyze the tones over the voice band. The monitored signaling systems are both channel associated and common channel for voice streams.

Depending on the specific signaling system and application, the Demux board can interface to up to eight complete E1s (in INMD application to monitor voice streams). If additional voice-band measurements and analysis are required, the Demux board can decide to pass the voice channel to other application boards, like Fax Monitoring and INMD boards. For roaming monitoring, the Demux board is coupled with a PowerPC board that provides the required processing power.

Stream Interface board

The Stream Interface board provides functionality similar to the Demux board on a single bi-directional stream per board, but with the additional capability of being inserted in series with the streams, thus allowing, for instance, the blocking or disturbance of ongoing fraudulent activities. The Stream Interface board is designed for maximum reliability when connected to the network in a drop-insert mode.

Fax Monitoring board

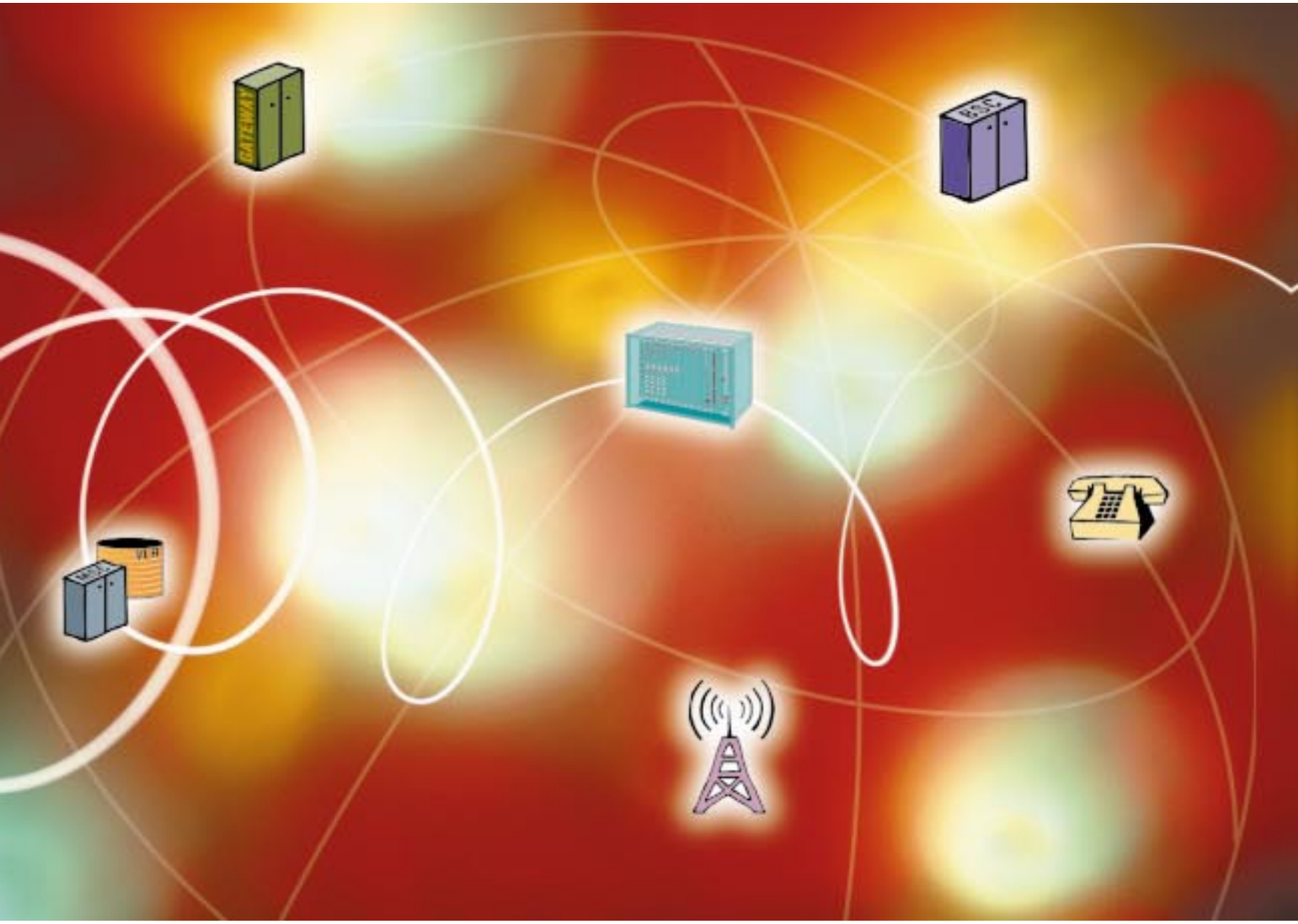
The Fax Monitoring board performs fax quality evaluation through analysis of the V.21 T.30 protocol between Group 3 machines according to ITU-T E.45x standards. This board works in combination with Stream Interface and Demux boards to gain access to the relevant fax connection.

INMD board

The INMD (In-service Non-intrusive Monitoring Device) board performs all the measurements specified by the ITU-T P.561 recommendation for the evaluation of voice transmission quality over in-service live traffic. Like the Fax Monitoring board, the INMD board works with Stream Interface and Demux boards to gain access to the relevant channel where a conversation is ongoing.

Scanner access module

The E1s can be connected directly to the Demux or Stream Interface boards or can be optionally interfaced by means of a Scanner access module. The Scanner module implements a switch matrix with a selectable combination of inputs and outputs. The Scanner access module can be configured from the Central Unit through an interface that allows easy setup of calendar schedules.



For further information, contact Tektronix:

Worldwide Web: for the most up-to-date product information, visit our web site at: www.tektronix.com

ASEAN Countries (65) 356-3900; **Australia & New Zealand** 61 (2) 9888-0100; **Austria, Central Eastern Europe, Greece, Turkey, Malta,& Cyprus** +43 2236 8092 0; **Belgium** +32 (2) 715 89 70; **Brazil and South America** 55 (11) 3741-8360; **Canada** 1 (800) 661-5625; **Denmark** +45 (44) 850 700; **Finland** +358 (9) 4783 400; **France & North Africa** +33 1 69 86 81 81; **Germany** +49 (221) 94 77 400; **Hong Kong** (852) 2585-6688; **India** (91) 80-2275577; **Italy** +39 (2) 25086 501; **Japan (Sony/Tektronix Corporation)** 81 (3) 3448-3111; **Mexico, Central America, & Caribbean** 52 (5) 666-6333; **The Netherlands** +31 23 56 95555; **Norway** +47 22 07 07 00; **People's Republic of China** 86 (10) 6235 1230; **Republic of Korea** 82 (2) 528-5299; **South Africa** (27 11) 651-5222; **Spain & Portugal** +34 91 372 6000; **Sweden** +46 8 477 65 00; **Switzerland** +41 (41) 729 36 40; **Taiwan** 886 (2) 2722-9622; **United Kingdom & Eire** +44 (0)1628 403300; **USA** 1 (800) 426-2200.

From other areas, contact: Tektronix, Inc. Export Sales, P.O. Box 500, M/S 50-255, Beaverton, Oregon 97077-0001, USA 1 (503) 627-6877.

ISO 9001

4/99 WCI XXW–XXXXX–0

Tektronix