ETSI

ETSI TECHNICAL REPORT

ETR 292

July 1997

Source: EP-TETRA

Reference: DTR/TETRA-01015

ICS: 33.020

Key words: TETRA, network management

Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Technical requirements specification; Network management

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 4 92 94 42 00 - Fax: +33 4 93 65 47 16

Contents

Blank page

Foreword

This ETSI Technical Report (ETR) has been produced by the Terrestrial Trunked Radio (TETRA) Project of the European Telecommunications Standards Institute (ETSI).

ETRs are informative documents resulting from ETSI studies which are not appropriate for European Telecommunication Standard (ETS) or Interim European Telecommunication Standard (I-ETS) status. An ETR may be used to publish material which is either of an informative nature, relating to the use or the application of ETSs or I-ETSs, or which is immature and not yet suitable for formal adoption as an ETS or an I-ETS.

Blank page

1 Scope

This ETSI Technical Report (ETR) provides an overview of the network management requirements in a Terrestrial Trunked Radio (TETRA) Voice plus Data (V+D) mobile radio system. The primary motivation of this ETR is to provide a starting point to facilitate central network management of TETRA systems from different manufacturers. After an overview of network management in TETRA, this ETR outlines the approach to the work, followed by the specification of the management services and information flows. Finally a standardization strategy for network management for TETRA is given.

The guiding principle in the examination of central Telecommunications Management Network (TMN) management services has been that the Central Network Management (CNM) facility will generally fulfil a monitoring role rather than a controlling role, although performing some limited controlling functions such as temporarily disabling and enabling individual subscribers.

With this constraint, an examination of the necessary central network management functions indicates that only a subset need to be standardized in order to support a high degree of inter-operability between different manufacturers' TMN management services. It appears that the following network management functionalities require access from the CNM facility (or, in the case of items d) and (g), require standardization in support of that access):

a) management of subscribers (for temporary actions only);

b) subscriber activity log and subscriber diagnostics;

c) access to system performance measurement data;

d) access to network management facilities;

e) fault and maintenance data;

f) testing and recovery of network support links, in particular the Local to Central Network Management link (LNM-CNM link);

g) accounting management.

It is clear that remote access to the LNM facilities from the centre will need to be supported by appropriate authentication and authorization procedures optionally including encryption over the LNM-CNM link.

In this ETR all of the local and central telecommunications management functions are examined and those that require to be standardized to allow remote CNM operation, as defined above, are identified. The local/central/local network management information flows required to support the CNM functions are studied and recommendations are made for defining TMN standard protocols and procedures.

2 References

This ETR incorporates by dated and undated reference, provisions from other publications. These references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this ETR only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] ITU-T Recommendation M.3020: "TMN Interface specification methodology".

[2] ITU-T Recommendation M.3200: "TMN management services: Overview".

[3] ITU-T Recommendation M.3400: "TMN management functions".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this ETR, the following definitions apply:

Base Station (BS): A physical grouping of equipment which provides the fixed portion of the air interface. One base station transmits and receives radio signals to and from a single location area (a single region of geographical coverage). A BS contains at least one Base Radio Stack (BRS).

cell: The smallest geographical area where TETRA services may be obtained, using a certain set of radio frequencies.

Cipher Key (CK): A value that is used to determine the transformation of plain text to cipher text in a cryptographic algorithm.

cipher text: The data produced through the use of encipherment. The semantic content of the resulting data is not available (ISO 7498-2).

decipherment: The reversal of a corresponding reversible encipherment (ISO 7498-2).

encipherment/encryption: The cryptographic transformation of data to produce cipher text. (ISO 7498-2).

entity: A point at which a packet is manipulated (e.g. sourced, sunk, routed or switched).

gateway: A device which will enable the interconnecting of two networks which inherently use different and incompatible protocols.

historical data: Record of a past event or series of events. Historical data from triggered events may start at some point in the past up to the present.

home location register: A database in the Mobile Station (MS) home system which keeps track of the position of the MS. The home location register is used to indicate where the MS should be paged.

key: A sequence of symbols that controls the operations of encipherment and decipherment.

key management: The generation, selection, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

network: A collection of subscriber terminals interconnected through telecommunications devices.

plain text: The unencrypted source data. The semantic content is available.

real time: Refers to the generation of network management information in a timeframe comparative to the real life process that it is controlling or monitoring.

signalling: The exchange of Information specifically concerned with the establishment and control of connections, and with management, in a telecommunication network.

site: Physical location within the network.

subscriber activity log: A system record which contains information on attach/detach ITSI; enable/disable terminal; registrations; location updates vs. time; call re-establishment; authentications; call start time, call end time, and called party; type of call; Supplementary Services invoked; whether uplink BER or MER are below an operator pre-determined threshold; plus any other relevant activity record.

subscriber data: A system record which contains information on the individual subscriber ITSI, GTSIs, Supplementary Services allowed, privileges allowed and other system accesses allowed.

subscriber management: The system functionality for dealing with subscribers to the system.

subscriber terminal: An equipment which an internal user can use to communicate with another user. Mobile Stations (MS) and Line Stations (LS) are the only types of subscriber terminal.

Supplementary Service: A Supplementary Service modifies or supplements a bearer service or a teleservice. A Supplementary Service cannot be offered to a customer as a stand alone service. It should be offered in combination with a bearer service or a teleservice.

Switching and Management Infrastructure (SwMI): All of the TETRA equipment for a Voice plus Data (V+D) network except for subscriber terminals. The SwMI enables subscriber terminals to communicate with each other via the SwMI.

transaction (packet transaction): All the processes and procedures associated with the transmission of one packet of information between peer network layer protocol entities on opposite sides of the air interface.

transaction (voice transaction): Part of a voice call comprising the transmissions of each talking party. The total of all transactions make up the call.

transferred account procedure: Name given to the central accounting procedure defined in the GSM standards. The transferred account procedure is used to allocate costs to roamed mobiles.

3.2 Abbreviations

For the purposes of this ETR, the following abbreviations apply:

ACL	Access Control List
ACSE	Associated Control Service Element
ASN	Abstract Syntax Notation
BER	Bit Error Rate
BIC	Barring Incoming Calls
BOC	Barring Outgoing Calls
BRS	Base Radio Stack
BS	Base Station
CK	Cipher Key
CMIP	Common Management Information Protocol
CMIS	Common Management Information Service
CMOT	CMIP Over TCP/IP
CNM	Central Network Management
CS	Control Supervisor
CUG	Closed User Group
DES	Data Encryption System
DGNA	Dynamic Group Number Assignment
EFD	Event Forwarding Discriminator
GDMO	Guidelines for the Definition of Managed Objects
GOS	Grade OF Service
GSM	Global System for Mobile communications
GTSI	Group TETRA Subscriber Identity
HLR	Home Location Register
I5	Interface between central and local network management systems
ISDN	Integrated Services Digital Network
ISI	Inter System Interface
ITSI	Individual TETRA Subscriber Identity
ITU	International Telecommunication Union
LA	Location Area
LNM	Local Network Management
LS	Line Station
MER	Message Erasure Rate
MFA	Management Functional Areas
MIB	Management Information Base
MS	Mobile Station
NMC	Network Management Controller
NMS	Network Management System
OSI	Open Systems Interconnection

PDN	Public Data Network
PDU	Protocol Data Unit
PSTN	Public Switched Telephone Network
PTN	Private Telephone Network
RFC	Request For Comments
ROS	Remote Operations Service
ROSE	Remote Operation Service Element
RSSI	Received Signal Strength Information
SDH	Synchronous Digital Hierarchy
SM	Subscriber Management
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
SS	Supplementary Service
SwMI	Switching and Management Infrastructure
TAP	Transferred Account Procedure
TCP/IP	Transmission Control Protocol/Internet Protocol
TEI	TETRA Equipment Identity
TETRA	TErrestrial Trunked RAdio
TIB	Task Information Base
TMN	Telecommunications Management Network
TNM	Telecommunications Network Management
UDP	User Datagram Protocol (TCP/IP-DoD)
V+D	Voice plus Data

4 Objectives and approach

4.1 Objectives

The purpose of this ETR is to examine the following:

a) the network management services that need to be standardized to achieve the required level of central management; and

b) the level to which the inter-system network management functions should be standardized.

4.2 Approach adopted

The issues of Inter-System Interface (ISI) functions (supporting normal operation of the network to provide service to subscribers), subscriber management and network management have been separated. An accepted framework for the standardization process is the ITU TMN methodology, ITU-T Recommendation M.3020 [1].

The first task was to identify the services required, rather than the functions (services are implemented by functions). Service descriptions have to identify who benefits from the service, e.g. network manager, dispatcher or subscriber. It was decided to define all network management services (local and central) and then extract the central ones needed to support interworking between management systems.

Once the services have been defined the aims stated in subclauses 4.1 a) and b) can be addressed.

4.3 Problems with the definition of management services using ITU methodology

A Telecommunication Management Network (TMN) is intended to support a wide variety of management functions which cover planning, operations, administration, maintenance and provisioning of telecommunication networks and services, ITU-T Recommendation M.3400 [3], paragraph 1.2.

A TMN management service is seen as an area of management activity which provides for support of an aspect of Operations, Administration and Maintenance (OAM) of the network being managed, described from the user perception of the OAM requirements, ITU-T Recommendation M.3200 [2], paragraph 1.

It was found that using the ITU methodology led to much overlap between categories of service definition, with duplication between the heading of the management service and the Management Functional Areas (MFAs) e.g. performance, fault, configuration etc.). The amount of detailed categorization required did not give a clear picture to guide network management development in TETRA, where the current objective

was to standardize a limited degree of interworking between network management systems of different TETRA systems at an early date.

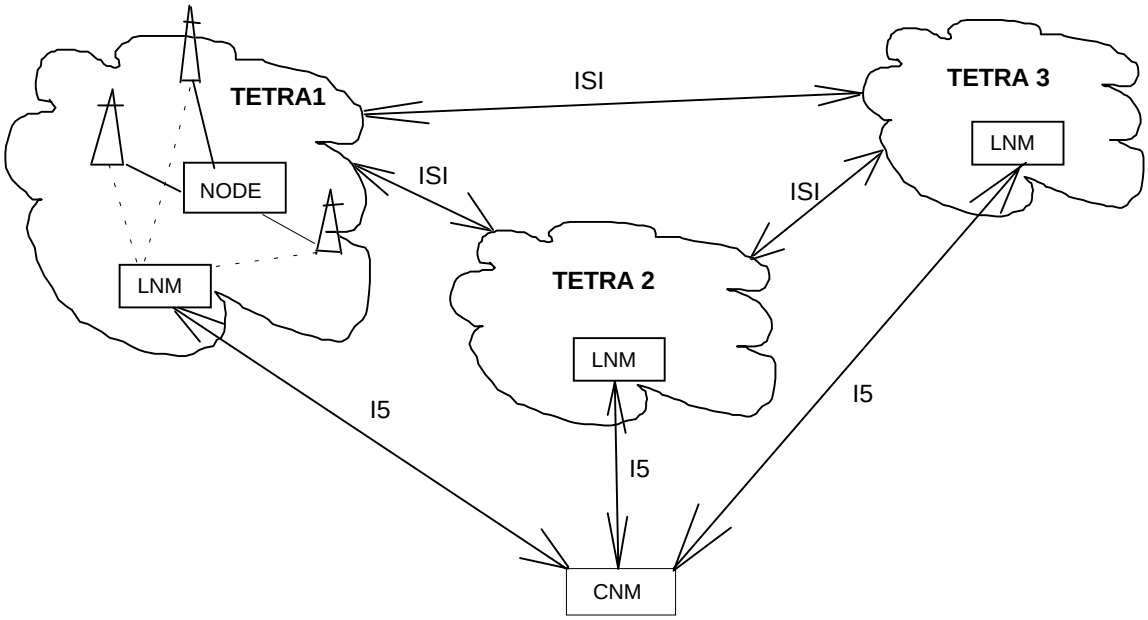
4.4 Simplified methodology

Because of the problems associated with use of the full ITU methodology, a simpler, alternative approach was employed, using parts of the ITU methodology to provide a clearer way to identify the standardization task. This alternative approach is detailed in clause 6.

5 Overview of network management in TETRA

5.1 TMN reference system architecture

The primary reason for addressing network mManagement is to facilitate central management of interworking between TETRA systems from different manufacturers (figure 1).



NOTE: This schematic diagram does not imply any specific architectural implementation within the individual TETRA networks.

Figure 1: Network management reference model

The reference system architecture assumes:

- a number (say up to 25) of individual TETRA systems which may be procured from more than one supplier;

- each TETRA system has its own Local Network Management (LNM) and Subscriber Management (SM) facility which handles all aspects local to the system itself;

- there is also a Central Network Management (CNM) facility which monitors or controls certain functions within and between the individual systems. Each system has a link to the CNM facility.

5.2 Role of players

The CNM system manager manages the CNM on a day-to-day basis.

The LNM system manager manages each TETRA system on a day-to-day basis, reconfiguring it dynamically as required. He manages subscribers and arranges maintenance when required. It is envisaged that each LNM system manager will have authority only to operate within their own system.

The Control Supervisor (CS) oversees several dispatchers in a single TETRA system and may carry out certain functions of the LNM system manager.

The dispatcher uses the facilities of the TETRA system to communicate with his organization's staff.

The individual subscriber uses the TETRA system to communicate with other subscribers or his dispatcher.

5.3 Non-standardized aspects

Certain aspects of network management in TETRA will only be performed at a local level and therefore do not need to be standardized. The following non-exhaustive list gives examples:

- performance management:
    - measurement data collection;
    - tracing data collection;
- fault or maintenance management:
    - alarm status monitoring;
    - alarm collection and logging;
    - alarm history handling;
    - diagnostics and test handling;
    - recovery;
    - equipment state handling;
- configuration management:
    - time management;
    - software management;
    - radio network management;
    - routing management;
- subscriber management:
    - subscriber basic data management;
    - basic service data management;
    - Supplementary Service management;
    - subscriber location;
    - group management;
    - Closed User Group (CUG) management.
- accounting management:
    - collecting and storing the accounting data (call logging);
    - billing;
- security aspects:

\
    - management of security of NMS;
    - security management (e.g. encryption key management).

5.4 Standardized aspects

The standardized aspects of network management which are proposed in TETRA are high-level functions which are carried out at a central entity performing the management of several TETRA networks. The proposed standardized network management functions are:

- performance management:
    - performance data transfer in standard format from the LNM to the CNM;

fault or maintenance management:

- alarm trigger corresponding to serious equipment failure;
- alarm trigger corresponding to serious security breach;
- alarm trigger corresponding to serious traffic alarm;

- subscriber management:
    - temporary withdrawal of registration permission;
    - restoration of registration permission (after temporary withdrawal);
    - subscriber activity history;
    - current status of a Subscriber;
    - initiate trace of future Subscriber activities.
- accounting management:
    - transfer of accounting data for users with wide roaming capability;
- security aspects:
    - security procedures (authentication and authorization).

6 TMN MS description

6.1 Reference Telecommunications Management Network

The reference TMN architecture model is shown in figure 1.

6.2 Basis for Telecommunications Management Network functionality

Network management for TETRA involves all activities of controlling, indication and logging in terms of usage and quality of service of TETRA networks with the aim of presentation of communication services with a defined degree of quality level.

MFAs are defined as:

- subscriber management;
- configuration management;
- traffic measurement;
- performance measurement;
- security management;
- charge (accounting) administration;
- fault management.

In reality some network management functions span several of these areas, for instance aspects of traffic measurement are used in configuration management, in performance measurement and in charge administration.

Another example of this overlap in functionality is in network management of the inter-system link bearers which would be provided as part of the link bearer network and be outside the individual TETRA network management. However, as a safety measure for the integrity of the overall system, activity and traffic levels on inter-system links should be monitored from the CNM facility. These are TETRA network functions which need to be carried out in real time so that re-routing of inter-system links can be arranged (via the configuration management function) when necessary.

By the very nature of network management many local and central network management operations are similar. Within the constraints of the particular implementation they may even be identical. Whilst every effort has been made in this document to capture all aspects of local and CNM, the emphasis has been placed on developing those network management functions, operations and information flows that need to be standardized to allow support of a common CNM facility.

6.3 Subscriber management

6.3.1 Management goals

The centre needs to be the focus of liaison with national sharers of the systems, and be able to inform them of localized problems in coverage/access/services etc.

The subscriber management is intended to present tools for subscriber administration from the operators point of view. These are activities for creating, updating and deleting subscriber oriented information. A distinction is made between temporary and permanent actions using different authorizations for starting these actions. Moreover, supervision of the data associated with the subscribers and the subscriber behaviour has to be done. Management of equipment has to be performed as well.

Some aspects of subscriber management may be achieved via normal Supplementary Services (SS), e.g. disabling of in coming or outgoing calls by the SS BIC or BOC, but some disabling functions may need to be done by the local or CNM system managers.

Interworking and migration of mobiles between different networks is achieved via the Inter-System Interface (ISI) and dynamic information to support this is exchanged on a call-by-call basis.

Other non-real-time information can be exchanged off-line between service providers.

6.3.2 Subscriber basic data management

Subscriber management is carried out locally for most subscribers. Call-based information is transported automatically between systems over the ISI. Subscribers with wide roaming capability may need to be managed from the central facility (for operational reasons).

Subscriber management needs a central network function which bars mobiles (e.g. stolen, spoof attempts) from accessing any of the systems. CNM needs ability to co-ordinate this action directly from the centre.

The system managers (central and local) have to be able to distinguish between a non-paying subscriber and a stolen/faulty mobile. To support this capability it is envisaged that separate independent databases based on subscribers identities (ITSIs) and equipment identities (TEIs) will be required.

6.3.2.1 Permanent actions

1) Creation of data for new subscribers. Includes all privileges, priorities and subscribed services.

2) Disabling of subscriber.

3) Updating of subscriber data in terms of subscriber and operator requirements (separate individual and group information).

4) Deletion of subscriber data (due to a subscriber request or operator decision).

Table 1

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	No	On demand	No	
2)	LNM system manager	Local	No	On demand	No	
3)	LNM system manager	Local	No	On demand	No	
4)	LNM system manager	Local	No	On demand	No	

NOTE: SS DGNA performs similar functions to dynamically create permanent groups with designated privileges, priorities and subscriber services and to allocate individuals to these groups.

6.3.2.2 Temporary actions

1) Temporary withdrawal of registration permission.

2) As 1.

3) Restoration of registration permission (after temporary withdrawal).

4) As 3.

Table 2

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	Yes	On demand		
2)	CNM system manager	Central	Close	On demand	LNM-CNM	To be standardized
3)	LNM system manager	Local	Yes	On demand		
4)	CNM system manager	Central	Close	On demand	LNM-CNM	To be standardized

6.3.2.3 Protection of subscriber data

1) Ensure the integrity and secrecy of subscriber data input by the LNM system manager.

2) Examination of presently stored data in terms of consistency and plausibility.

Table 3

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	No	On demand	No	
2)	LNM system manager	Local	No	On demand	No	

6.3.2.4 Subscriber activity log and subscriber diagnostics

1) Retrieving historical subscriber activities by accessing subscriber activity log for a defined period. Subscriber activity log to contain information on attach/detach ITSI; enable/disable terminal; registrations; location updates vs. time; call re-establishment; authentications; service delivery queuing delay; call start time, call end time, called party; call end reason (see note), type of call; Supplementary Services invoked; whether uplink BER or MER are below an operator pre-determined threshold; plus any other relevant activity record.

2) As 1.

3) Current status (attached/detached, in a call and if so identity of other parties, system identity where attached, site identity, date, time, type of call, SS invoked).

4) As 3.

5) Initiate trace of future subscriber activities. Trace to trigger on specific events (such as call re-establishment signalling, uplink BER below threshold, etc.) identified by the invoker of service.

6) As 5.

NOTE: See annex B for summary of call end reasons.

Table 4

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	Dispatcher & LNM system manager	Local	Yes	Continuous or trigger	None	
2)	CNM system manager	Central	No	On demand	LNM-CNM	To be standardized
3)	Dispatcher and LNM system manager	Local	Yes	On demand	None	
4)	CNM system manager	Central	Yes	On demand	LNM-CNM	To be standardized
5)	Dispatcher and LNM system manager	Local	Yes	On demand or trigger	None	
6)	CNM system manager	Central	Yes	On demand or trigger	LNM-CNM	To be standardized

NOTE: **Item 1:** Access to the historical subscriber activities data has to be in real time but real time data from the system is not necessary. It is an implementation issue whether system information is stored and then archived after a suitable time, or whether information is overwritten on a cyclic basis (such as every 24 hours).
Item 2: Discrete information from the local historical log can be demanded by the CNM.
Items 3 and 4: It is expected that subscriber current status information is available in real time at the LNM facility. It may take finite time to relay this to the CNM facility but it is essentially close to real time.
Items 5 and 6: The trace of future subscriber activities is intended to provide the basis of:
a) diagnostic data gathering for substantiating subscriber fault reports;
b) surveillance of subscriber activities (e.g. tracking stolen mobile terminal).

Initiation of trace is on demand. After the trace has been initiated, information will be gathered on specific events or on all events after the trigger (as defined in the demand).

6.3.2.5 Equipment management

1) Central administration of data files concerned with equipment identification.

2) Local administration of equipment and programming of equipment characteristics.

3) Administration of "black list" equipment (stolen or faulty).

Table 5

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	CNM system manager	Central	No	On demand	None	
2)	LNM system manager	Local	No	On demand	None	
3)	CNM/LNM system manager	Central and Local	No	On demand	None	Regular update - not in real time

6.3.3 Supplementary service management

6.3.3.1 Permanent actions

1) Creation, deletion and modification of data for Supplementary Services.

2) De-activation and activation of Supplementary Services.

Table 6

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	No	On demand	None	
2)	LNM system manager	Local	No	On demand	None	

6.3.3.2 Temporary actions

1) Temporary disabling of a Supplementary Service.

2) Enabling of Supplementary Service after temporary disabling.

Table 7

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	Dispatcher and LNM system manager	Local	Yes	On demand	None	
2)	Dispatcher and LNM system manager	Local	Yes	On demand	None	

6.3.4 Migration management (individuals and groups)

Migration management is usually carried out locally (by inter-operator agreements) for individuals and groups. However, groups which migrate across individual system boundaries may need a central network information facility to support their operation.

Interrogation of home database and visitor database actions in support of migrating mobiles is performed autonomously in real time by the system. Management of migration, which involves granting the authority to migrate to the individual subscriber and informing the mobile's database which operator codes to prefer when seeking service outside of the home system is performed off-line in non-real time.

1) Grant migration privilege to individual or group. This information is stored in the SwMI.

2) As 1.

3) Inform mobile's database of preferred operator codes in visited systems.

4) Remove migration privilege from individual or group. Information stored in SwMI.

5) As 4.

Table 8

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	No	On demand	None	
2)	CNM system manager	Central	No	On demand	None	By post?
3)	LNM system manager	Local	No	On demand	None	At subscription?
4)	LNM system manager	Local	No	On demand	None	
5)	CNM system manager	Central	No	On demand	None	By post?

6.4 Configuration management

6.4.1 Management goals

System configuration management affects the functionality of the entire communications network. Consequently, it can only be performed by authorized personnel. Terminals dedicated to system configuration management are to be protected by appropriate access checking (see security management). Management of system configuration should be performed without interruption to the corresponding service. If system crashes are encountered after execution of system configuration management it has to ensured that the system can be satisfactorily returned to its previous operational state whilst the problems are resolved. After each system change suitable tests have to be performed to exclude possible secondary effects.

Two distinct aspects of configuration management can be identified:

- a slow acting management function corresponding initial set up and steady state system control;

- a fast acting management function corresponding to transitory fault control and also to deal with fluctuating traffic conditions. This latter aspect is sometimes called performance management since it deals with dynamic configuration management in order to optimize performance.

It is often difficult to separate these aspects of configuration management, except in very specific circumstances and usually concerning only a few network elements. Generally, the fluctuating traffic conditions will mainly affect the radio network part of the system.

The following general steady-state (non-real time) features of configuration management may be distinguished:

a) Specification of operator requirements in terms of services supported: teleservices, bearer services, Supplementary Services, network services etc. These are usually static and configured when the network is first set up.

b) Identification of required network elements. This initially entails identification of the individual network entities required to provide the required service and subsequently monitoring of these network elements to ensure correct operation.

c) System parameters to be specified. Corresponds to interpretation of grade of service parameters for the services in a) being mapped on to specific network elements identified in b).

d) Upgrades of hardware components (e.g. network elements or sub-elements), software contained in these components and overall system control software.

e) Reconfiguration of existing network elements.

f) Administration of system configuration.

Configuration management for the line network and the radio network aspects of TETRA are dealt with separately in the following subclause.

The overall requirements for efficient network management are:

- flexible system configuration; able to easily configure and reconfigure the system;

- equal set of central commands for equivalent functions in different suppliers' systems;

- automatic generation of lists of hardware of TETRA system e.g. BS, switches etc. Similarly lists of software versions for all administered network components.

  NOTE 1: If this were to be a central function it implies an agreed definition of generic network objects.

- LNM system manager able to produce a compatibility matrix in terms of hardware and software components which can be combined within the network management system.

  NOTE 2: This is off-line information.

6.4.2 General configuration management features

6.4.2.1 Operator requirements

It is expected that the basic network requirements will be defined in terms of standard teleservices, bearer services, Supplementary Services and network services. The task of the network manager will be to translate the required services and their corresponding grade of service into equipment specifications, radio channel requirements and line communication requirements.

6.4.2.2 Influenced network elements

Once the system has been configured the LNM system manager who is in day-to-day control of the equipment will need to compile and maintain a compatibility matrix which will keep track of hardware and software within the system. This matrix will be used for the co-ordination of system configuration measures (procedures, equipment and software) that maintain system integrity.

6.4.2.3 System parameters to be specified

Examples of area and call based parameters which may be associated with subscriber groups or individuals:

- maximum call duration;
- maximum time in database queues;
- priority oriented choice of connection paths dependent on service quality;
- availability of call re-routing, data connection, connection between cells;
- provision or withdrawal of teleservices, bearer services or Supplementary Services.

Examples of parameters for configuration of the entire network:

- network nodes, network elements;
- frequencies and encryption modes;
- interface protocols and specification of redundant connections;
- fall back modes, re-routings.

Examples of parameters to be specified by the system administrator:

- connection duration depending on the connection path;
- allowed length of queues;
- duration of residence in queues;
- maximum time of call signalling;
- connection hold time when no activity detected on the connection;
- priority of emergency call;
- characterization of the connection paths.

Clock synchronization would be local to each system but there may need to be some loose co-ordination to allow time-stamping of events from different networks.

6.4.2.4 Software management

A local administrative function. Central network management facility needs to be informed of, though not in real time:

1) Inclusion of improved versions of software, maintaining existing system characteristics.

2) Introduction of new system characteristics.

Table 9

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	No	On demand	No	
2)	LNM system manager	Local	No	On demand	No	

6.4.2.5 Administration of system configuration data

1) Management of installation, auditing, compatibility and tracking of software.

2) Availability of reload information involving all software components and data required for the correct functionality of each TETRA system.

3) Central archive facility. This is foreseen as a secure archive facility rather than an on-line back-up capability.

Table 10

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	No	On demand	No	
2)	LNM system manager	Local	No	On demand	No	
3)	CNM system manager	Central	No	On demand	No	Optional

6.4.3 Fixed network configuration management

6.4.3.1 Internal SwMI routing

Control of routing within each TETRA system is local to that system. There is no need for the CNM facility to have any knowledge of the routing within each network.

6.4.3.2 Communication interface management

6.4.3.2.1 Administration of system data

1) Co-operation with other TETRA systems in terms of required data (i.e. establishment of database that will be used in other parts of the communications interface management, such as management of routing information).

Table 11

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	No			Achieved by inter-op agreement or managed from centre

6.4.3.2.2 ISI management

Inter system routing may be co-ordinated from the centre, e.g. to re-configure inter-system links after link failures. Management of routing should preferably be based on existing telecommunications line equipment.

1) Permanent routing of ISI.

2) Temporary re-routing of ISI.

3) Introduction of additional network connections/routes.

4) Removal of existing network connections/routes.

5) Re-arrangement of routes for traffic harmonizing or as a security measure.

Table 12

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	No	On demand	No	Centre informed (note)
2)	LNM system manager	Local	Yes	On demand	No	Centre informed (note)
3)	LNM system manager	Local	No	On demand	No	Centre informed (note)
4)	LNM system manager	Local	No	On demand	No	Centre informed (note)
5)	LNM system manager	Local	Yes	On demand	No	Centre informed (note)
NOTE: Centre can optionally be informed.						

6.4.3.2.3 Gateway management

1) Creation of supervised gateway entities (i.e. installation).

2) Modification/deletion of supervised gateway entities (i.e. reconfigure, define address, define authority).

3) Blocking/deblocking of supervised gateway entities.

4) Restarting of supervised gateway entities.

Table 13

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	No	On demand	No	
2)	LNM system manager	Local	No	On demand	No	
3)	LNM system manager	Local	No	On demand	No	
4)	LNM system manager	Local	No	On demand	No	

6.4.3.2.4 Line Station (LS) interface management

1) Enabling/disabling of LS interfaces.

Table 14

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	No	On demand	No	

6.4.4 Radio network configuration management

Carried out locally. CNM facility may need to be informed of certain local actions, though not in real time. Depending on the management structure, CNM may be given access to individual systems network configurations to maintain a central database of individual system configurations for back-up/restoration purposes (see subclause 6.3.2.5).

6.4.4.1 Configuration

1) Creation, modification, deletion of supervised entities (site, transceiver, radio channel etc.).

2) Control channel management strategy.

3) Traffic channel management strategy.

4) Reset of equipment entity (i.e. deblocking of faulty entity).

5) Network map information.

6) Adjacent cell information at system boundary (this information will need to be regularly refreshed).

Table 15

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	No	On demand	No	
2)	LNM system manager	Local	No	On demand	No	
3)	LNM system manager	Local	No	On demand	No	
4)	LNM system manager	Local	No	On demand	No	
5)	LNM system manager	Local	No	On demand	No	
6)	LNM system manager	Local	No	Initial config and fault event	No	By local agreement

6.4.4.2 Reconfiguration of existing network elements

1) Reconfiguration as a result of traffic load analyses.

2) Permanent or temporary reconfiguration due to faults.

3) Dynamic reconfiguration of the communications network radio resources to optimize traffic throughput or system access time. For example:

- temporary removal of connections for reduction of network administration effort;
- limitation of call duration;
- limitation of call attempts in case of originating calls;
- manipulation of random access parameters;
- reconfiguration of control channels (secondary/auxiliary);
- modify system mode of operation e.g. minimum mode, time shared mode;
- services for information of subscribers in case of disturbances;
- reservation of lines for special traffic modes;
- installation of additional temporary route combinations;
- temporary reorganization of traffic distribution.

Table 16

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	No	On demand	No	
2)	LNM system manager	Local	Semi	On demand	No	
3)	LNM system manager/Control Supervisor	Local	Yes	On demand	No	

6.5 Traffic measurement

6.5.1 Management goals

Traffic measurement in real time allows flexible adaptation of network configurations to the dynamic traffic requirements. The corresponding system connectivity data should be stored and should be retrievable on demand by the LNM system manager.

6.5.2 Traffic measures

1) Data collection and logging (traffic intensity + traffic type + traffic direction).
In particular the following information will be available:

a) uplink BER and MER per channel;
b) up and down link radio channel activities;
c) infrastructure entities activity log;
d) infrastructure line activity log;
e) individual subscriber activity log;
f) group subscriber activity log.

2) Report generation, event generation. For each of the following network entities:

- base site;
- network switching node;
- ISI;
- gateway or standard interface.

Table 17

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	Yes	Continuous		
2)	LNM system manager	Local	Yes	On demand		

The information gathered by this activity can be used to dynamically reconfigure system resources as described in subclause 6.4.4.2 or can be used to calculate the ongoing quality of delivered service as described in subclause 6.6.

6.6 Performance measurement

6.6.1 Management goals

The efficient evaluation of network management tasks is supported by creation of performance measurements statistics which are based on the results of performance measurements.

The central network management facility may collect performance data on the individual TETRA systems and on the inter-system links to confirm that the network and the links are working correctly and to obtain historical data of system usage. This function can be carried out in non-real-time, but for convenience all data should be in a compatible electronic format. Preferably the performance data would be accessible via the CNM-LNM link. It is anticipated that the raw traffic data would be generated locally and then manipulated locally to give outline performance measures. Some analysis of this data may be performed at the centre.

6.6.2 Administration of performance measurements

Central action is required to harmonize the parameters measured and the method of measurement in each system, but this does not have to be achieved in real-time.

Administration of performance measurements:

1) creation of new and modification of existing measurements;

2) deletion of existing measurements;

3) remote measurement;

4) activation and deactivation of measurements;

5) information processing of traffic measurements;

6) automatic statistic creation performed by the system administrator;

7) presentation of statistics data according to pre-defined criteria;

8) Logging of connectivity parameters.

The above GOS measurements are to be made for each:

- base site;

- network node;

- ISI;

- gateway/interface.

Table 18

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	No	On demand	No	
2)	CNM and LNM system manager	Central and Local	No	On demand	No	
3)	CNM and LNM system manager	Central and Local	No	On demand	No	
4)	CNM and LNM system manager	Central and Local	No	On demand	No	
5)	LNM system manager	Local	No	On demand	No	
6)	LNM system manager	Local	No	On demand	No	
7)	CNM and LNM system manager	Central and Local	No	On demand	No	
8)	CNM and LNM system manager	Central and Local	No	On demand	No	

6.6.3 Performance measurement data generation

The raw traffic data is generated under subclause 6.5. This data is then manipulated locally to produce system performance data that will allow historical instantaneous network load and other related network performance parameters to be established i.e. this subclause describes the periodic analysis of continuous data. The update rate locally and centrally will be application and implementation specific. The aim will be to provide sufficient data to verify service level agreements and to allow informed investigation of network performance complaints. Measurements have to be made available by the LNM to provide the following statistics to the CNM:

1) Levels of traffic produced by the users and by control signalling.

   a) number of active individual users per base station;
   b) number of registered individual users per location area;
   c) number of active user groups per base station;
   d) number of queued call requests by call type and average queue times per base station;
   e) number of emergency calls per individual user and per active talk group;
   f) number of single site calls and average duration;
   g) number of intra-system calls and average duration;
   h) number of inter-system calls and average duration;
   i) number of telephone access calls and average duration (per BS and per user group);
   j) total number of service requests per user group;
   k) total number of uplink data messages per user group;
   l) total number of downlink data messages per user group;
   m) average number of data packets per transaction for each user group;
   n) number of circuit data transactions per user group and average duration.

2) Measurements of the service quality.

   Service user aspects:

   a) Average and worst case call waiting times for different call types, call priorities, Supplementary Services invoked per BS (see note).

   b) Lost call rate on random access can only be estimated from the access channel collision rate. However, call failures can be measured precisely after successful initial access.

c) Blocking rate. Corresponds to failed call attempts due to unavailability of radio or line resources. System will queue the call request and then subsequently reject the request if resources do not become available within the time-out period.

NOTE: Can only be measured after successful access to the system.

Network operator/service provider aspects:

d) average uplink BER and MER per logical channel per base station;
e) worst case uplink BER and MER and associated subscriber unit per channel;
f) percentage utilization per radio traffic channel;
g) percentage utilization per line station;
h) percentage utilization per network link;
i) percentage utilization per major network entity (gateways, interfaces, switches);
j) random access channel collision rate;
k) random access channel throughput;
l) random access channel percentage utilization;
m) average queue length per priority;
n) average queue time per priority;
o) average queue length per priority per network link;
p) average queue time per priority per network link.

3) Measurements of system availability.

It is expected that this information is a summary of fault and maintenance data assembled elsewhere, giving equipment unavailability, partial availability, reduced performance availability.

a) radio Tx/Rx availability;
b) network node availability;
c) network link availability;
d) gateway availability (PSTN, ISDN, PDN, PTN);
e) ISI availability;
f) LNM-CNM link availability.

All of the system performance measurement data listed above should be available locally on a regular update basis. It is a manufacturer/network operator option how often the information will be updated. For analysing busy hour performance an update every 10 to 20 minutes would be suitable. For providing a running average system performance an update every hour may be adequate.

The resultant performance measurement data should be available centrally (individually or in total) in a standard format on demand.

Table 19

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	Yes	Continuous		
2)	LNM system manager	Local	Yes	Continuous		
3)	LNM system manager	Local	Yes	Continuous		

6.6.4 Performance measurement data storage

1) Data storage based on pre-defined parameters.

2) As 1.

3) Store all traffic data for a pre-defined time and arbitrarily long archiving duration.

4) As 3.

Table 20

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	No	As required	None	
2)	CNM system manager	Central	No	As required	None	
3)	LNM system manager	Local	No	As required	None	
4)	CNM system manager	Central	No	As required	None	

6.6.5 Measured performance data presentation

Central action is required to harmonize and display the parameters measured under subclause 6.6.3 but this does not have to be achieved in real-time. A defined electronic format for data transport to the CNM is required. Data presentation in this context refers to the availability of the data in a defined electronic format with defined protocol over the CNM-LNM link. Man-machine-interface presentation of the performance data at the LNM and CNM system manager consoles is an implementation issue and not proposed for standardization.

1) Data presentation locally by LNM system manager.

2) Data presentation centrally by the CNM system manager.

3) Processing of raw data locally resulting in a presentable format.

4) Processing of performance data at the CNM.

5) Graphic presentation of pre-processed performance data by creation of interfaces to commercially available graphic tools.

Table 21

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	No	On demand	No	
2)	CNM system manager	Central	No	On demand	No	
3)	LNM system manager	Local	No	On demand	No	
4)	CNM system manager	Central	No	On demand	No	
5)	CNM and LNM system manager	Central and local	No	On demand	No	

6.6.6 Performance measurement data transfer

Transfer of the performance measurement data from the LNM to the CNM is to be in standard format.

1) Performance data transfer in standard format from the LNM to the CNM.

Table 22

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	CNM system manager	Central	No	On demand	LNM-CNM	To be standardized

6.7 Security aspects

6.7.1 Management goals

The task of security management contains an enabling and a supervisory role together with a real-time implementation aspect.

The enabling role is to distribute security relevant information (such as encryption keys and authorization) to users and to systems in a controlled manner so that security features of the system can be supported.

The supervisory role is to:

- prevent unauthorized persons from gaining access to sensitive information;

- prevent unauthorized persons from gaining access to network services;

- prevent unauthorized persons from being able to modify network parameters (in particular the functionality or the technical quality of the network).

These supervisory objectives are supported by the real-time implementation aspects of the role. In particular by:

- encryption of network management information, with authorized personnel having the appropriate algorithms and keys;

- real time authentication/authorization of persons for use of the network services;

- real time authentication/authorization of persons for use of the network management services (locally and from the CNM facility).

6.7.2 Management of security of network management system

This subclause refers to control of operator access to network management facilities.

It is expected that security procedures will be carried out locally for all system elements. Each constituent system should be responsible for the security of each of its links to the outside world i.e. ISDN, PSTN, PDN, PTN, ISI, I5.

Security of inter-system links could be managed from the centre, but it would be more secure if each constituent system were responsible for its own links. Secure access procedures to the LNM facilities from the CNM facility will need to be standardized and perhaps also encryption algorithms to be used over the LNM-CNM links. This is considered further under subclause 6.7.4.

Security management functions:

1) Definition of different levels of permitted accesses to network nodes and network functions by specific types of authorized personal.

2) Supervision of access control (this is a management function which is at a higher level than the executive functions of items 3 and 4 below).

3) Access control to network management services in LNM facility.

4) Access control to network management services in CNM facility.

   NOTE: The security management functions 3 and 4 may incorporate:

   - authentication of the CNM from the LNM and vice versa;
   - encryption of data between LNM and CNM.

Table 23

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	No	On demand	No	
2)	CNM and LNM system manager	Central and local	No	On demand	No	
3)	LNM system manager	Local	No	On demand	No	
4)	CNM system manager	Central	No	On demand	No	

6.7.3 Security management (e.g. encryption key management)

Carried out locally for most subscribers.

For certain users who have wide roaming capability the function may be managed from the centre.

Need co-ordinated action from the high-level centre to counter any penetration of system security, e.g. initiating a key change in several TETRA systems quickly.

It is important to realize that although the results of these management actions are carried out in real time the actual network management is performed off-line in non-real time. For example the authentication procedures are defined and installed off-line in a home database but are interrogated in real time during system operation.

Security management functions:

1) Authentication management.

2) Air interface cipher key management.

3) Individual cipher key management.

4) Group cipher key management.

5) Definition and provision of communication paths being secure in terms of required user-dependent security criteria.

6) Maintenance and analysis of security recording.

7) Auditing of security functions e.g. for encryption key change.

Table 24

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	Control supervisor and LNM system manager	Local	No	On demand	No	note 1
2)	LNM system manager	Local	No	On demand	No	note 1
3)	Control supervisor	Local	No	On demand	No	note 2
4)	Control supervisor	Local	No	On demand	No	note 2
5)	LNM system manager	Local	No	On demand	No	note 1
6)	CNM or LNM system manager	Central and local	No	On demand	No	note 1
7)	CNM or LNM system manager	Central and local	No	On demand	No	note 1
NOTE 1: Not to be standardized over LNM-CNM. Information could be exchanged off-line between LNM system managers. NOTE 2: Not to be standardized over LNM-CNM. Information could be exchanged off-line between control supervisors.						

6.7.4 Access to local network management facilities from the centre

This subclause refers to the communications between LNM and CNM.

Access to each LNM facility needs to have real time authentication and authorization.

1) Security procedures (authentication and authorization) to gain access to LNM facility from the CNM facility. Encryption over the LNM-CNM link may also need to be standardized.

Table 25

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	CNM system manager	Central	Yes	On demand	LNM-CNM	To be standardized

6.8 Accounting management

6.8.1 Management goals

Accounting management (charge administration) involves the aspects of tariffing, call information, charge association and billing.

6.8.2 Tariffing

1) Management of absolute tariff fixing. Because of tariff fluctuation, this has to be performed separately from the switch.

2) Information of subscriber association to tariffs will be administered within the switch of the call source.

Table 26

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	No	On demand	No	
2)	LNM system manager	Local	Yes	On demand	No	

6.8.3 Collection, storage and transfer of accounting data

For every call the following information will have to be logged:

- tme call commences;

- tme call ends;

- sbscriber identities involved;

- tleservices/bearer services/Supplementary Services used.

Collection and analysis of this information will be carried out locally. Note some degree of overlap with subclause 6.5 exists. It is anticipated that part or all of the accounting information will be required centrally on demand. The update rate for local accounts is an operator/manufacturer option. It is anticipated that once per hour or once per several hours would be typical.

Chargeable call data is a sub-set of the subscriber activity log corresponding to successful (chargeable) calls.

The separation of chargeable call data from the subscriber activity log (filtering) is performed at the local level before transmission to the CNM.

The accounting data should be available centrally (individual items or in total) in a standard format on demand. A standard procedure and protocol should be developed for interrogation from the CNM of the LNM subscriber activity log and LNM chargeable call data. It has been suggested that the GSM Transferred Account Procedure (TAP) may provide a suitable basis for getting this accounting data in a standard format.

1) Generation of the traffic information.

   a) Seconds of voice usage sorted by individual (individual calls).
   b) Seconds of voice usage sorted by user group (group calls).
   c) Seconds of telephone access sorted by individual and by user group.
   d) Dialled number and call duration per telephone access.
   e) Seconds of circuit data transactions per user group.
   f) Bytes of packet mode long data per individual and per user group.
   g) Bytes of packet mode short data per individual and per user group.
   h) Number of status messages per individual and per user group.
   i) Number of system control data packets sent and received between radio, control, console and gateway sites.
   j) Roamer usage information per TETRA system. Time, date, place roaming started/finished. Calls made, calls received. Other services used.

2) Storage of the above traffic information (see note).

3) Transfer of the above traffic information (see previous comment about the possibility of GSM TAP providing the basis for this standardization).

   NOTE: This information needs to be protected in case of equipment failure leading to total or partial corruption of the database.

Table 27

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	Yes	Continuous	None	
2)	LNM system manager	Local	Yes	Continuous	None	
3)	CNM system manager	Central	No	On demand	LNM-CNM	To be standardized

6.8.4 Cost association

1) Evaluation of the traffic load information.

2) Association in terms of usage of network nodes being involved in the distribution of traffic loads.

3) Association according to traffic loads generated by user organizations and/or subscribers.

Table 28

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	No	On demand	None	
2)	LNM system manager	Local	No	On demand	None	
3)	LNM system manager	Local	No	On demand	None	

6.8.5 Billing

Carried out locally.

For certain users who have wide roaming capability the information may be transmitted to the centre for collation and onward billing to subscribers. A common electronic format would be desirable.

1) Direct access to the subscriber data base to answer queries on bill.

2) Integrated solution including tariff dependent charge administration, creation, processing and archiving of charging data.

3) Bill information generation and printing.

Table 29

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	No	On demand	None	
2)	LNM system manager	Local	No	On demand	None	
3)	CNM and LNM system manager	Central and Local	No	On demand	LNM-CNM	Optional

6.9 Fault or maintenance management

6.9.1 Management goals

Fault Management involves the general functions for alarm supervision, logging of operation disturbances and executing corrective actions to restore the system to an operating condition in each TETRA system as well as providing test functions.

Fault management provides the following specific functionality:

1) Alarm in case of a fault (major fault displayed centrally otherwise only local indication).

2) Detection of exact location (diagnostics) of a fault (central in case of a fault concerning ISI or LNM-CNM, otherwise local).

3) Isolation of faulty equipment (central for ISI/LNM-CNM, otherwise local).

4) Activate stand-by systems (central for ISI/LNM-CNM, otherwise local).

5) Routine testing of equipment systems (central for ISI/LNM-CNM, otherwise local).

All fault and maintenance management within individual systems would be carried out locally.

6.9.2 Alarm status monitoring

Carried out locally for internal system elements. Serious alarm monitoring may be remoted to the central network management facility. Serious fault information presented to the CNM may be archived for future reference.

The intention is that the CNM would receive the outstanding alarm messages from a TETRA network when the LNM-CNM link is established (or in real time if the link is permanent). These alarms summarize the outstanding fault conditions that are sufficiently serious for possible CNM action. As each alarm clears a corresponding clear message would be sent to the CNM. Effectively the CNM would be working with paired reports, the first indicating an "object" failure and the second that the fault condition has cleared.

Functions for alarm supervision

1) The functionality of each TETRA system has to be separately supervised. This supervision includes monitoring and control of transfer links, power supplies, antennas and other equipment.

2) The fault recognition normally has to be performed in (close to) real-time (i.e. slight delay for confirmation may be tolerated). The error occurrence has to be indicated to the fault management by the corresponding network element. Serious fault indications are forwarded to the centre under items 6, 8 and 10 below.

3) Optical and acoustical messages in case of equipment failures.

4) Investigation and localization of failures up to board level.

5) Alarm trigger corresponding to serious equipment failure for example:

   a) For commercial power loss, node ID plus system element (radio equipment, control rack, console, gateway, interface; etc.).
   b) Low power and no power alarms for all transmitters.
   c) Indication of receiver failures (e.g. RSSI plus decoder correlation).
   d) Internal diagnostics failure result for radio, control, console, interface or gateway equipment.
   e) Failure of communications bus connecting network equipment.
   f) Out of service percentage per channel exceeded e.g. when equipment redundancy is inadequate.

6) As 5.

7) Alarm trigger corresponding to serious security breach e.g. burglary (site and node).

8) As 7.

9) Alarm trigger corresponding to serious traffic alarm (site, node, ISI, gateway plus condition such as queue length or queue time exceeded, uplink control channel BER limit exceeded, access control channel collision rate limit exceeded).

10) As 9.

Table 30

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	Yes	Continuous	No	
2)	LNM system manager	Local	Yes	Fault event	No	
3)	LNM system manager	Local	Yes	Fault event	No	
4)	LNM system manager	Local	Yes	On demand	No	
5)	LNM system manager	Local	Yes	Fault event	No	
6)	CNM system manager	Central	Semi	Fault event	LNM-CNM	To be standardized
7)	LNM system manager	Local	Yes	Fault event	No	
8)	CNM system manager	Central	Semi	Fault event	LNM-CNM	To be standardized
9)	LNM system manager	Local	Yes	Fault event	No	
10)	CNM system manager	Central	Semi	Fault event	LNM-CNM	To be standardized

6.9.3 Alarm collection and logging

Carried out locally for internal system elements. ISI alarms, and serious local alarms, are remoted for information to the central network management facility (see subclause 6.9.2). This is a real-time requirement.

The system manager (local or central) can specify the entity to monitor; the criteria for triggering the monitoring (polled or traps), poll interval, trigger level etc.

Collection and processing of operation disturbances.

1) Collection of operation information.

2) Logging of operational information.

3) Evaluation of operational information.

4) Reporting of operational information.

5) Calculation of error statistics.

Table 31

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	Yes	Alarm event	None	
2)	LNM system manager	Local	Yes	Continuous	None	
3)	LNM system manager	Local	Yes	On demand	None	
4)	LNM system manager	Local	Yes	On demand	None	
5)	LNM system manager	Local	Yes	On demand	None	

6.9.4 Alarm system parameter handling

Refers to adjustment of threshold values and alarm filtering parameters. Criteria would be agreed at system set-up by administrative action. Actions are real time but management is not.

Table 32

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	No	On demand		

6.9.5 Alarm history handling

Carried out locally.

1) Keeping of an event file including information like the kind of failure, time started and eliminated and description of fault elimination process.

2) Active interrogation of event files.

3) Archiving and access to alarm event files.

Table 33

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	No	Event driven	No	
2)	LNM system manager	Local	No	On demand	No	
3)	LNM system manager	Local	No	On demand	No	

The CNM entity may also keep a record of serious faults reported under subclause 6.9.2 items 6, 8 and 10.

6.9.6 Diagnostics and test handling

Most diagnostics and tests should be carried out within each local system. LNM-CNM links should be dealt with at each end of the link.

Processing of operation disturbances

1) Possibility of remote maintenance and diagnostics i.e. performed some distance from the network element but probably within each system.

Test functions

The following kinds of test processing can be distinguished.

2) The fault management instructs a network element to perform analyses of line and equipment characteristics. The test processing is done completely within the network element and the results will automatically be transferred to the fault management.

3) The analysis is performed by the fault management itself. In this case it only requests access to components to be tested from the network element and tests the components.

4) The results received during the test processing are to be evaluated appropriately.

5) Testing of internal SwMI support links.

6) Testing of ISI links.

7) Testing of the LNM-CNM links.

Table 34

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	Yes	On demand	None	
2)	LNM system manager	Local	Yes	On demand	None	
3)	LNM system manager	Local	Yes	On demand	None	
4)	LNM system manager	Local	Yes	On demand	None	
5)	LNM system manager	Local	Yes	On demand	None	
6)	LNM system manager	Local	Yes	On demand	None	
7)	CNM and LNM system manager	Central and Local	Yes	On demand	LNM-CNM	

6.9.7 Handling of equipment status

As part of the management of network elements it may be necessary to ascertain the status of particular equipment. This function is carried out locally.

Table 35

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	Yes	On demand	None	

6.9.8 Recovery

Recovery actions should be mainly carried out locally, although some re-routing of inter-system links (ISI and LNM-CNM) may be carried out from the centre.

1) Activation of basic network functions. The actual system data for automatic reconfiguration at resumption of normal operation will have to be stored.

2) Automatic change-over to substitute systems.

3) Blocking of disturbed elements and putting into operation of repaired network elements.

4) Automatic blocking of disturbed channels on request.

5) Protection measures against net disturbance due to faulty equipment.

6) Recovery of intra-system links (internal SwMI).

7) Recovery of ISI links.

8) Recovery of the LNM-CNM links.

Table 36

	User	Location	Real time	Trigger	Intersystem medium	Comments
1)	LNM system manager	Local	Yes	On demand	No	
2)	LNM system manager	Local	Yes	On demand	No	
3)	LNM system manager	Local	Yes	On demand	No	
4)	LNM system manager	Local	Yes	On demand	No	
5)	LNM system manager	Local	Yes	On demand	No	
6)	LNM system manager	Local	Yes	On demand	No	
7)	LNM system manager	Local	Yes	On demand	No	
8)	LNM and CNM system managers	Central and Local	Yes	On demand	No	

7 Information flows for standardized CNM-LNM services

7.1 Introduction

This subclause describes the messages which need to be exchanged to support the services identified for standardization between a Central Network Management (CNM) and a Local Network Management (LNM) system.

7.2 Assumptions and notes

7.2.1 Assumptions

a) All messages are to be date/time stamped unambiguously. (Some mechanism for approximate synchronization for message date/time stamping, within agreed limits, needs to be agreed).

b) All messages relating to subscribers are addressed to the Home Location Register (HLR) in the first instance.

7.2.2 Notes

a) The matter of authentication of the CNM requester (client) with the LNM provider (server) may require additional information to be contained in the messages.

b) The security of the information being passed between the Network Management systems needs to be considered and may impact upon the structure of individual messages or sequences of messages.

c) Definitions: Roaming — Within a system, i.e. across cells
Migration — Between different systems

d) In the descriptions below the direction of information flow is identified as, for example, "CNM-LNM" (meaning from the central to the local system).

7.3 Information flows

7.3.1 Subscriber basic data management - temporary actions

See to subclause 6.3.2.2.

7.3.1.1 Temporary withdrawal of registration permission

See to subclause 6.3.2.2, item 2.

CNM-LNM Request for temporary disabling of a subscriber.
Attributes: Subscriber identity.

LNM-CNM Acknowledgement
Attributes: Subscriber identity.
Confirmation that message has been received and database modified. If unsuccessful the reason should be given.

LNM-CNM Confirmation of successful subscriber disabling.
Attributes: Subscriber identity.
Date and time.

7.3.1.2 Restoration of registration permission (after temporary withdrawal)

See to subclause 6.3.2.2, item 4.

CNM-LNM Request for re-enabling of a subscriber.
Attributes: Subscriber identity.

LNM-CNM Acknowledgement
Attributes: Subscriber identity.
Confirmation that message has been received and database modified. If unsuccessful the reason should be given.

LNM-CNM Confirmation of successful subscriber re-enabling.
Attributes: Subscriber identity.
Date and time.

7.3.2 Subscriber diagnostics

See to subclause 6.3.2.4.

Information provided should include the attached/detached status of mobile, call-related information, such as the call originator ITSI, type of call, talkgroup GTSI when appropriate, SS invoked and location of subscriber. All messages have to include a time and date stamp.

7.3.2.1 Subscriber activity history

To detect change in pattern of use based on historical information recorded.

See to subclause 6.3.2.4, item 2.

CNM-LNM Request for historical information.
Attributes: Subscriber identity.
Parameters for which information is to be provided.

LNM-CNM Message(s) providing the information requested above If information or part of the information requested cannot be provided the reasons should be given.

CNM-LNM Message acknowledging successful receipt of all information; or message authorizing premature termination of messages(s), e.g. it is realized that the quantity of information is larger that can be handled.

Notes: This is historical information.

Just provide "recent usage" information, rather than results of some standardized analysis procedure. It will be for the CNM facility to analyse the data.

Parameters could include: attach/detach ITSI; enable/disable terminal; registrations; location updates vs. time; call re-establishment; authentications; call start time, call end time, called party; call end reason (see note), type of call; Supplementary Services invoked; whether uplink BER or MER are below an operator pre-determined threshold; plus any other relevant activity record.

NOTE: See annex B for summary of call end reasons.

7.3.2.2 Current status of a subscriber

See to subclause 6.3.2.4, item 4.

(Site, node, ISI, Gateway plus condition such as queue length or queue time exceeded, uplink control channel BER limit exceeded, access control channel collision rate limit exceeded).

CNM-LNM Request for current status information.
Attributes: Subscriber identity.
Parameters for which information is to be provided.

LNM-CNM Message containing information.

CNM-LNM Message acknowledging successful receipt of all information.

NOTE: Information could be both dynamic (current activity) and static (service entitlements).

Dynamic parameters could include: call start time, called party ID (individual or group), type of call, services used, site identity, attached/detached, disabled/enabled, time and date of events, attached/detached, in a call and if so Identity of other parties, System identity where attached).

Static parameters could include: service entitlements (ITSI and GTSI).

7.3.2.3 Initiate trace of future subscriber activities

See to subclause 6.3.2.4, item 6.

CNM-LNM Request for tracing initiation of future subscriber activities.
Attributes: Subscriber identity.
Parameters concerning future Subscriber Activities.

LNM-CNM Confirmation that the Trace of Subscriber Activities is active.
Attribute: Subscriber identity.

LNM-CNM Subscriber event driven message.
Attributes: Subscriber identity.
Event Code and any associated information.
Event Date and time.

CNM-LNM Message acknowledging successful receipt of message.

NOTE 1: Activities could include: attach/detach ITSI; enable/disable terminal; registrations; location updates vs. time; call re-establishment; authentications; call start time, call end time, called party; call end reason (note), type of call; Supplementary Services invoked; whether uplink BER or MER are below an operator pre-determined threshold; plus any other relevant activity record.

NOTE 2: See annex B for summary of call end reasons.

7.3.3 Performance measurement data transfer

See to subclause 6.6.6.

Transfer of performance measurement data from the LNM to the CNM in standard format.

7.3.3.1 Performance data transfer in standard format from the LNM to the CNM

See to subclause 6.6.6, item 1.

CNM-LNM — Request for transfer of performance data from LNM to CNM.
Attributes: Network component identity.
Parameters for transfer of performance data.

LNM-CNM — Message containing requested performance data.
If information or part of the information requested cannot be provided the reasons should be given.

CNM-LNM — Message acknowledging successful receipt of all information.

7.3.4 Access to network management facilities from the centre

See to subclause 6.7.4.

7.3.4.1 Security procedures (authentication and .authorization)

(To gain access to LNM facilities from the CNM facility)

See to subclause 6.7.4, item 1.

NOTE: Use protocols from existing standards, e.g. CMIP, SNMP.

Need to include requirement for changing passwords.

Encryption over the LNM-CNM link may also need to be standardized.

7.3.5 Fault and maintenance management

See to subclause 6.9.

7.3.5.1 Alarm trigger corresponding to serious equipment failure

See to subclause 6.9.2, item 6.

a) For commercial power loss, node ID plus system element (radio equipment, control rack, console, gateway, interface; etc.).

b) Half power and no power alarms for all transmitters.

c) RSSI plus decoder correlation to indicate receiver failures.

d) Internal diagnostics failure result for radio, control, console, interface or gateway equipment.

e) Failure of communications bus connecting network equipment.

f) Out of service percentage per channel exceeded e.g. when equipment redundancy is inadequate.

LNM-CNM — Alarm message.
Attributes: Network ID, network resource, location of source of alarm, any other associated parameter value(s).

CNM-LNM — Message acknowledging successful receipt of all information sent.

7.3.5.2 Alarm trigger corresponding to serious security breach, e.g. burglary

See to subclause 6.9.2, item 8.

CNM-LNM Alarm message.
Attributes: Network ID, network resource, location of source of alarm, any other associated parameter value(s).

LNM-CNM Message acknowledging successful receipt of all information sent.

7.3.5.3 Alarm trigger corresponding to serious traffic alarm

See to subclause 6.9.2, item 10.

Alarm trigger corresponding to serious traffic alarm includes: Site, node, ISI, Gateway plus condition such as queue length or queue time exceeded, uplink control channel BER limit exceeded, access control channel collision rate limit exceeded.

LNM-CNM Alarm message.
Attributes: Network ID, location of source of alarm, any other associated parameter value(s).

CNM-LNM Message acknowledging successful receipt of all information sent.

Notes: It is envisaged that the LNM will carry out most Performance Management and that raw and/or processed information would be available, in some common format, to CNM "Off-line".

However, during LNM "out-of-hours" working, alarms generated by traffic or performance levels exceeding their limits, may need to be routed to CNM.

Fault management: fault types and usage:

Table 37

System Entity	Identity	Fault Type	Usage
Entity type, e.g. base station, site	Entity ID	Security alarm	Intruder alarm, etc.
		Power failure	Loss of mains power; but reserve power available.
		Total power failure	Loss of all power including reserve; or loss of mains power at entity without reserve supply.
		Service loss	Loss of some equipment at entity resulting in reduced capacity available.
		Major equipment failure	Total loss of entity.

Each of the foregoing functions will require the following messages to be exchanged:

CNM-LNM Fault indication.

CNM-LNM Fault cleared/OK.

LNM-CNM Message acknowledging successful receipt of all information sent.

LNM-CNM Interrogation of status of function.

CNM-LNM Response with indication or cleared/OK message above.

7.3.6 Accounting management

See to subclause 6.8.

7.3.6.1 Transfer of accounting data

Accounting information shall be available centrally to a suitably authorized CNM system manager so that roaming mobile activity for accounting purposes can be forwarded to the home TETRA system.

See to subclause 6.8.3, item 3.

CNM-LNM Request for transfer of accounting data.
Attributes: Network ID.
Parameters for transfer of accounting data.

LNM-CNM Message containing requested accounting data.
If information or part of the information requested cannot be provided the reasons should be given.

CNM-LNM Message acknowledging successful receipt of all information.

8 Network management protocols

8.1 Introduction

This subclause is intended to give an introductory overview of management protocol standards, highlighting the advantages and disadvantages of the available options and recommending a suitable protocol for the TETRA network management. In particular CMIP (the OSI framework, incorporated into TNM and supported by the ITU) and SNMP (the framework supported by the Internet and representing a de-facto industry standard) are considered.

8.2 Concepts

The following subclause briefly covers the concepts of network management frameworks which underpin the use of standard protocols.

8.2.1 Structure of Management Information (SMI)

In order to achieve independence of actual management protocols, rules are constructed to identify information. This set of rules is known as the structure of management information (SMI). The SMI defines how to define new managed objects, places restrictions on their types and specifies rules for naming. If the collection of managed objects is viewed as a virtual store then it can be considered as the schema for the Management Information Base (MIB).

8.2.2 Managed objects

The term managed object is used as means to describe management information. It is actually used as an object oriented expression of this information. An object of object-type has associated with it entirely abstract syntax and semantics and is equivalent to an object class specification in an object oriented programming language. The term object instance is used to denote the existence of a particular instance.

The specification of managed objects, together with the agreed management protocol (CMIP, CMOT, SNMP), identifies uniquely the interoperable interface for co-operating management applications.

SMI + MIB + MANAGEMENT PROTOCOL = INTEROPERABLE INTERFACE.

8.2.3 Data representation

To express the format of the packets exchanged in a machine independent way, the formalism of Abstract Syntax Notation (ASN) is used to specify the PDU's and managed objects. Specifications use the OSI ASN.1 language which makes it unambiguous and allows it to be mechanically processed through suitable tools.

In the SNMP framework a small subset of the ASN.1 syntax is allowed, only the absolutely necessary types are used. There is no inherent penalty in having this small subset which stems from the SNMP axiom that management should have minimal impact on managed nodes. The restricted set of ASN.1 types provides for small code sizes at run-time.

The OSI framework also uses Guidelines for the Definition of Management Objects (GDMO). GDMO gives a checklist for managed object class definitions, including templates and packages, it allows for inheritance to be defined, properties to be imported from other standards, association of attributes, operations, behaviour and the definition of containment relationships.

8.2.4 Polling vs. event based management

There are two fundamental approaches to management; an event driven approach and a polling approach. Both can be used to notify management stations of extraordinary events.

The event based approach makes it the responsibility of the managed node to send an event to a management station when an event occurs. The advantage is that there is an immediate notification. The disadvantage is that resources are required to produce events. If many are generated or they contain large amounts of information, resources of the network element may be stretched. In this case a refinement is needed through thresholds and correlation. This in itself could prove resource hungry, depending upon its implementation.

The polling approach requires the management station to query the managed elements to get a status report. This interaction is easy to manage but will not reveal problems in a timely manner.

The OSI approach (CMIP/CMOT) uses the event driven approach, actually called EventReport, thresholding, sieving, correlation and Event Forwarding Discriminators (EFDs) are all used.

SNMP uses trap-directed polling (trap is the SNMP term for an event), when an event occurs a single simple trap is generated and sent to the manager node. The manager is responsible for initiating further interactions in order to determine the nature and extent of the problem.

8.2.5 Telecommunications Network Management (TNM)

The principal behind TNM is to provide an organized architecture to achieve interconnection between various types of management systems, using an agreed architecture with standardized interfaces. The logical architecture of TNM is based on a number of function blocks, which provide the general functions which enable TNM to perform management. The TNM information architecture is based on the manager agent concepts developed for OSI systems management. An object oriented information model is established which presents an abstraction of the resource (physical or logical) being managed. This model is made visible at a TNM interface. The generic TNM model is described in ITU-T Recommendation M.3100 [2].

8.3 Candidate protocols

8.3.1 SNMP

The SNMP architectural model contains a collection of network management stations and network elements. Network management stations execute management applications which monitor and control network elements. Network elements contain management agents which are responsible for performing the network management functions requested of them. SNMP is used to communicate management information between Management applications and agents.

The goal of SNMP is to minimize the number and complexity of management functions realized by the management agent itself. This keeps the development cost for management agents to a minimum and the simple set of management functions are easily understood.

SNMP is independent from the transport protocol used to transmit the messages. The preferred mapping is on UDP, however it can be used over many transport mappings. All SNMP implementations are required to accept messages which are serialized in 484 octets or less. Mappings are defined in RFC's and include Ethernet, TCP and even OSI.

SNMP V1

SNMP is an asynchronous request/response protocol. SNMP is used over an unreliable connectionless transport service, therefore it is possible that requests or responses may be lost, so it is up to the management application to decide when to re-transmit a request. SNMP is a simple protocol comprising of the following message set:

get-request - used to retrieve (read) managed objects for monitoring;

get-next-request - used to retrieve managed objects through traversal;

get-response - for the sake of simplicity the response to any of the request primitives is the get-response;

set-request - used to set (write) management information in order to perform actions that implement management decisions;

trap - when an exception event occurs the agent identifies those managers who wish to be notified and generates a trap PDU;

authentication - the notion of a community is used as the basis of the administrative framework, which is the relationship between the agent and one or more managers. A given community defines the level of access to the MIB handled by the agent.

SNMP V2

SNMP V2 (also called secure SNMP) is, strictly speaking, a set of extensions and changes to the SNMP V1 protocols. SNMP V2 replaces the community string with "parties", Access Control Lists (ACL's) and a modified mechanism to view the MIB. The scheme allows an SNMP entity to decide what access to allow to other SNMP entities and to provide a mechanism to allow two SNMP entities to exchange authenticated or private information. The MD5 Encryption standard (DES) is the proposed mechanism. Enhancements to the V1 protocol have been undertaken, several new PDU's added:

GetBulk - to allow more efficient retrieval of large amounts of data;

inform - This is similar to a confirmed trap;

trap - the new trap PDU uses the same format as all the other SNMP PDU's so that it can be handled by the same encoding/decoding routines as all other PDU's.

New MIB's have also been defined to allow manager to manager communication.

It is understood that SNMP V1 is a stable standard, but SNMP V2 is not yet stable.

8.3.2 CMIP

To be correct this should actually be CMIS (Common Management Information Service) which defines the services used to exchange management information defined in ITU-T Recommendation X.710. CMIP (Common Management Information Protocol) is actually the specification for the protocol mapping of CMIS onto the Remote Operations Service (ROS), see figure 2, over a full OSI stack (CMIP).

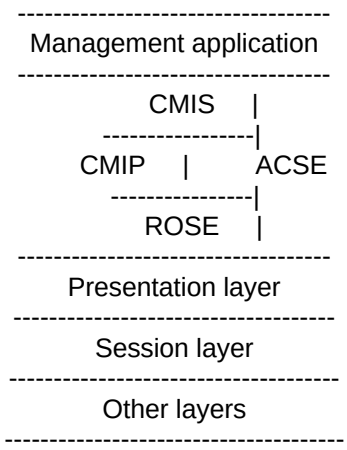


Figure 2: Protocol stack for CMIP

CMIP has a functionally rich message set:

M-CREATE - issued by a manager to create a managed object. Only available as a confirmed service;

M-DELETE - issued by a manager to delete a managed object(s). Only available as a confirmed service;

M-SET - issued by a manager to modify attributes of a managed object(s). Available as confirmed or unconfirmed service;

M-GET - issued by a manager to read the attributes of a managed object(s). Only available as a confirmed service;

M-CANCEL-GET - issued by a manager to terminate the return information from a previous GET operation;

M-ACTION - issued by a manager to perform an action on a managed object(s). Available as confirmed or unconfirmed service;

M-EVENT-REPORT - issued by an agent to convey management information resulting from a notification emitted by a managed object. Available as confirmed or unconfirmed service.

Using the GET, SET, ACTION and DELETE primitives a scoping and filtering service is available. A Base Object Instance can be specified (the node in the tree for which to start the scoping function), the scope of the managed objects to be selected can then be identified. A filter can then be specified in addition to this to provide a refinement to the selection. e.g. M-GET all instances of router objects that are out of service.

OSI management architecture

The major elements of the OSI management architecture are:

- Organization of management systems.

- Definition of management information.

- A set of management functions.

- Communication of management information.

The OSI management framework is presented in ITU-T Recommendation X.700, which presents the terminology and basic concepts. It also introduces the five functional areas of management (the set of management functions):

- Fault management.

- Configuration management.

- Security management.

- Accounting management.

- Performance management.

The systems management overview is presented in ITU-T Recommendation X.701 and introduces the concept of distributed systems management, interaction and communication and the relationship between management entities. It also identifies the underlying OSI services required by the management process.

8.3.3 CMOT (CMIP over TCP/IP)

CMIP uses ACSE and ROSE services on top of a full OSI stack. In order to use the Internet protocols a lightweight presentation protocol layer can be used directly on either TCP or UDP. This approach using CMIP over a slim OSI stack is known as CMOT (RFC 1189). The CMOT services and concepts are exactly the same as CMIP, it is only the stack that is different and hinders interoperability between applications running on two different stacks. Currently CMOT is not commonly used.

8.3.4 CMOL (CMIP over Link Layer)

CMOL maps CMIP onto the Link Layer protocol. The CMOL services and concepts are exactly the same as CMIP, just the stack that is different. This form of CMIS is very rarely used.

8.4 Summary

The OSI approach is very general and views network management as another OSI application, using the same framework. CMIP uses a connection oriented model as part of the application layer entity. Though CMOT can operate on top of UDP, the OSI approach dictates a connection oriented reliable transport service, so that applications can concentrate on management activities and not replicate the transport layer functions.

A feature of the OSI model is that a lot of the management functions are implemented in the agent, e.g. thresholding, log control and are implemented through managed objects which allow managers to concentrate on management policy. The OSI management framework is heavily loaded to event reporting rather than polling. The scoping and filtering mechanisms provide a powerful mechanism to minimize interactions across the network.

The OSI facilities are complex to implement and place a lot of the processing involved on the agents. This is inappropriate for small network elements, as they may not be capable of running a full 7 layer stack. A lightweight protocol (CMOT) may solve some of these problems, however using the full power of ASN.1 and GDMO may still result in large code sizes.

SNMP places few requirements on the transport mechanisms so that almost all network elements will be able to support it. Its operations are simple, however it can emulate the semantics of more complex operations through careful information modelling. Processing is based mainly in the NMC which can run on more powerful machines. SNMP is however bandwidth hungry because of its polling oriented operation and it does not support bulk transfer well (however, SNMP V2 and other mechanisms can be used for this). The choice of simplicity has made SNMP the de-facto industry standard.

8.5 Recommendation

Taking into account the performance constraints placed on TETRA network elements and the relative size and complexity of TETRA networks (which are small in comparison to GSM and fixed telephony infrastructures), it would appear that SNMP provides the most appropriate solution for the TETRA network management protocol. SNMP places minimal requirements on the network elements and is applicable to small and medium size networks.

Selecting SNMP at this stage does not preclude the use of CMIP, as many commercial network management packages suitable for the CNM implementation support both CMIP and SNMP, allowing coexistance of the two protocols or a migration to CMIP at a later stage if necessary.

9 Standardization strategy for network management

A suitable basis for standardizing items related to TETRA network management is given by the TMN management service description according to clause 6. However, only the services destinated to be standardized have to be taken into account. For these CNM-LNM services, clause 7 specifies the corresponding information flows.

ITU-T Recommendation M.3020 [1] represents an appropriate framework for the standardization process for TETRA network management. In this recommendation, a methodology is specified which provides a description of the processes leading towards the definition of TMN interfaces. This methodology comprises two main areas of activity, application tasks and protocol tasks. Each of these tasks is associated to its corresponding Task Information Base(s) (TIB). Within the scope of this ETR, task 1 and its TIB A is already specified in clause 6 (in a simplified form). The tasks and its associated information bases are described briefly as follows (see ITU-T Recommendation M.3200 [2] for details):

Application tasks

Task 1: Describe TMN management services from the users perspective.

Each area of management activity which is supported by the TMN has to be identified. For TETRA network management, this task has already been performed (clause 6). However, for the reasons discussed in clause 4, a simplified description method has been used instead of strictly pursuing the full ITU methodology.

TIB A: TMN management services and goals.

A complete list of TMN management services with a brief prose description is to be provided. Clause 6 already contains this description for the management services destinated for TETRA networks.

Task 2: Describe TMN management context.

Roles, resources and TMN functions associated with a given TMN management service are to be specified.

TIB B: Management roles, resources and TMN management functions.

Descriptions of Roles, resources and TMN management functions for that part of the TMN management service selected in task 1 are to be listed.

TIB X: Generic and technology specific information models.

The TIB X contains the generic and technology specific information models, including the object class hierarchies for these models.

Task 3: Object modelling.

Identification of existing and new object classes needed to support the TMN management functions assigned to that part of the TMN management service selected in task 1.

TIB C: Object templates.

The object classes are specified using the templates from ITU-T Recommendation X.722. Object templates are specified in ITU-T Recommendation M.3100 and other information model recommendations.

TIB D: Object relationship diagrams.

Object relationship diagrams are specified in ITU-T Recommendation M.3100 and other information model recommendations. Applicable managed objects have to be used in task 4 to specify the management information schemas.

Task 4: Consolidation.

For each TMN management function in the function list it has to be checked if it is supported by one or more object classes. This task forms part of the iterative process of building the set of management services and models.

Task 5: Define management information schema.

For each type of managed system the management information schema has to be determined. The schema has to be checked from a managed system point of view.

TIB E: Management information schema.

A management information schema specifies the information model of a managed system as seen over a particular interface by a particular managing application or system. Management information schemas are specified in generic and technology specific information model recommendations.

Task 6: Determine communication requirements.

Sets of communication requirements for the most likely communication scenarios are created in this task.

TIB F: Requirements for communication.

The communication requirements contain the nature of communications and the frequency/service requirements for layer 7, delay, etc.

Task 7: Prepare documentation for protocol tasks.

The results of previous tasks should be examined to prepare the communication to be used in accomplishing the protocol tasks.

TIB G: TMN functional profiles.

The TMN functional profiles provide all the information necessary to perform the tasks associated with selecting and defining the protocols for the TMN interfaces.

Protocol tasks

Task 8: Analyse message needs.

Analyse the TMN functional profiles to determine broad characteristics of the message needs.

Task 9: Decide adequacy of existing protocols for each layer.

Evaluate from TIB H appropriate protocols from existing standard protocols which meet the needs defined in task 8.

TIB H: Existing protocols and TMN protocol suites.

TIB H provides the repository of existing standard protocol suites which task 8 draws from in order to minimize the number of protocols.

Task 10: Define new protocol requirements.

If a layer protocol in task 8 is not adequate to meet the message needs defined in task 8, additional/amended layer protocol requirements are defined. For the application layer, application protocol requirements aimed at the specific message needs of task 8 are specified.

Task 11: Define new layer services and protocols.

Corresponding to the first part of task 10, appropriate new/amended layer (N-1) services to support layer (n) are defined. Corresponding to the second part of task 10, application protocols aimed at the specific message needs chosen by task 8 are specified.

Task 12: Select layer services.

Select the service requirement from layer (N-1) to N, for 1 through 6 from the output of tasks 9, 10 and 11.

Task 13: Select layer protocols and form protocol suites.

Select all layer protocols from tasks 9 through 12 and define families of protocol suites including coding of information content, to support the specific management function(s).

A reasonable proposal in terms of the level of standardization is to use existing management information protocols like CMIP or SNMP. In this case, the main effort of standardization is associated with the application tasks (tasks 1 to 7) including its corresponding MIBs.

The usage of the above task-oriented concept is to be restricted to the activities between the CMN and the LNM. Customer requirements from different countries and from different user organizations should be taken into account. The standard should not define activities or elements within the network.

Annex A includes additional issues related to the standardization process.

Annex A: Additional issues of standardization, implementation, messages, databases and agent specification

Standardization issues:

Need to treat NWM as an evolving/developing standard.

Addition of new features could be classified as:

- Easy to do - could add to standard.
- Not so easy - manufacturers would only add under pressure.

Compare against ITU-T Recommendation M.3400 [3] where functions are defined. Where there is no correspondence (no mapping), then there is a problem.

Implementation issues:

Need a notion of an abstract network so manufacturers know what needs to be implemented.

Most manufacturers will have their own back-up arrangements, so no need for on-line back-up in configuration management.

Beware imposing a large structure onto small systems.

Message issues:

It may be simpler to use ordinary NWM messages and just extend these to CNM.

Pair fault alarms at the centre (alarm/alarm cleared).

Need well-defined behaviour to avoid accumulating old reports at the centre.

Database issues:

Difficulty of keeping all databases in step with each other, e.g. after system restoration following a failure, especially if they have to contain information on all system subscribers (e.g. 10 000 users). Easier to deal with direct questions relevant to the 1 subscriber of interest.

Detailed information at Local level. Define more abstract information at the centre. Message filtering LNM to CNM.

Keeping databases in step is a complex task. Many different implementations, so many different structures of databases.

Agent specification issues:

For those services which will be standardized, the following need to be considered:

Initial conditions - a set of initial conditions have to be determined for both the LNM and the CNM:

What initial information is required?
State of all elements
State of all Objects
See also LNM/CNM not available

Fall Back - In large local networks there may be instances where control will be transferred between management stations for purposes of backup, out of hours working etc. How will the CNM guarantee to get all information during the transfer?

Exception Conditions - These are going to be many and varied, however they will mainly fall into the following categories:

LNM-Not available:

If the LNM cannot respond to CNM requests, what will the CNM do?
How Many retries?

CNM-Not available:

If the CNM is not available, how should the LNM react?
Will store and forward be required?
What level of information loss is acceptable?
How long should a LNM try to contact a CNM before giving up, or trying an alternative CNM?
How will the CNM inform the LNM's that it is available?
How long should information (e.g. alarms) be held by the LNM?
On returning what information will the CNM require? every event since it was unavailable?

Operations not supported:

Unexpected messages.
Options not implemented.
LNM not able to carry out requests.
Exceptions returned by the CNM/LNM.

Conformance - This will be partially protocol dependent and functionally dependent.

Functions:

What functions are mandatory for LNM/CNM working?

Protocol:

What level of operations are supported as mandatory, Protocol Implementation conformance statement?
e.g. in the case of CMIP what level of scoping and filtering available?
for SNMP what security features are to be supported?

Replay - Will a replay facility of alarms etc. be required by the CNM?

Time stamping - If time stamping is required will this be the actual event date or sent date or both?

Annex B: Call end reasons

Call end reasons seen by the network can be considered under the following general headings:

Registration

success;

failure (denied by network, network overload, etc.);

Speech call

success:

- terminated by calling party;
- terminated by called party;
- terminated by network (e.g. call duration limit, pre-emptive emergency call);
- terminated by authorized user (e.g. dispatcher);

failure during set-up (speech or data):

- cancelled by calling party;
- cancelled by called party;
- called party not reachable;
- called party busy;
- network resources not available (e.g. time-out in queue, queue positions full, called party site failure, link failure);
- calling party validation failure;
- called party validation failure;
- system signalling problems (source site, destination site, link, etc.);
- invalid call request (e.g. unrecognized called identity, invalid PSTN no.);
- insufficient authorization (e.g. SS not authorized, bearer/teleservice not subscribed, etc.).

Call diversion

successful;

failed (invalid diverted party, invalid authorization, etc.).

History

Document history	
July 1997	First Edition

ISBN 2-7437-0674-0
Dépôt légal : Juillet 1997