To be published at 11th Annual Conference on
European Fibre Optic Communications and Networks "EFOC&N '93"
The Hague, NL, June 30 - July 2, 1993

A SIMPLE CONFIGURATION METHOD FOR INSTALLATION OF OSI SYSTEMS IN LANS

Georg Roessler, University of Stuttgart, Stuttgart, Germany

Summary

Configuration of networks is not an easy task, especially if functionally rich protocols like OSI protocols are used in the network. This paper presents a method that can make the initial configuration of systems during the installation phase of a network more efficient, provided the method is widely accepted, standardized and implemented. Main building blocks of the method are the management information to load to protocol stacks in order to make them operational, and a simple protocol to transfer the information in a LAN environment from an installation manager to all systems. The only requirement for the initial configuration is that all systems can be accessed using data link layer communication. For end systems using OSI protocol stacks the management information that enables Systems Management and access to the Directory Service is discussed in detail. This information is also compared with that needed in systems with TCP/IP protocol stacks.

1 Introduction

Network management of today's LANs is mostly based on SNMP [1] for the TCP/IP world, proprietary protocols or CMIP [12] for OSI networks. These protocols cover the operation and maintenance phases of the network lifecycle, where sufficient address information on the network layer and above can be used to allow communication between application processes. However, this information is not available during the installation of a network. SNMP and CMIP are therefore not suitable for this early network management phase.

For TCP/IP a solution is possible based on BOOTP [2]. For OSI, there is no comparable method. The only way is to configure systems manually, which is a rather cumbersome way especially in LANs due to their distributed nature and the potentially large number of systems.

This paper presents a new method to improve the efficiency of the system installation process in LANs. The method can be applied after network planning and cabling to establish logical relationships, which are necessary to start operation. It consists of two parts, namely the information to be propagated and the communication based on the data link layer. The paper concentrates on systems in LANs running OSI protocols as in this case the applicability of the method is obvious, but the method is not limited to this kind of systems.

The paper is structured as follows. Section 2 describes a scenario, how a network is planned, installed, and made operational following a systematic approach. The organization and communication aspects of the new method are described in section 3. Management information that is used for setting up communication is explained in section 4. Section 5 contains some remarks on security in SCMP. The paper concludes with a short summary.

2 Scenario for a Network Lifecycle

In this section a scenario will demonstrate how the new method fits into the lifecycle of a network. The lifecycle phases are one dimension of the management space depicted in figure 1.

Design and planning of a network usually starts with the user requirements. The network is designed top-down from a rough sketch to more detailed versions. For this phase in the network lifecycle, workstation-based tools may be used. These tools help optimize the network with respect to performance, cost, and availability. The outcome of the design and planning phase are plans for the cabling and configuration information for all network devices and end systems.

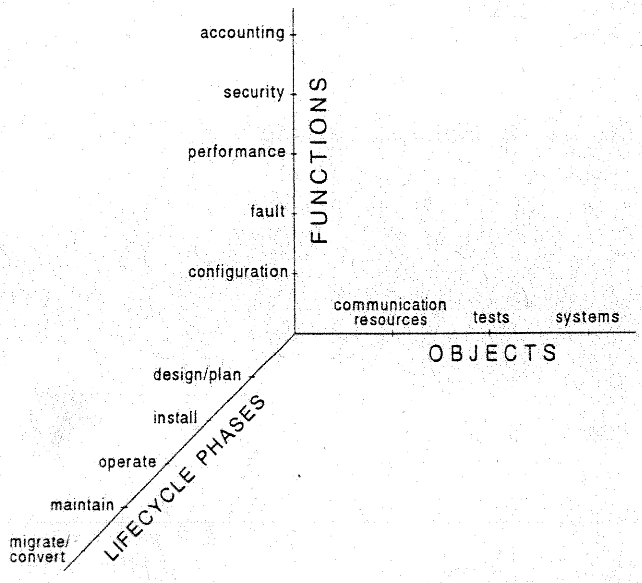

Figure 1: Management space

The installation phase consists of two steps. In the first one all cabling has to be carried out and tested, and all systems are connected to the cabled network. The focus of this paper is on the second step that deals with configuration of systems attached to the network. The main goal is to find a method how the configuration information generated during the planning phase is efficiently distributed to all systems. This task must be achieved under the condition that only the physical and data link layers are operational. It is assumed that the communication software of the higher layers is installed and gets started together with the operating system. All systems are neutral, however, i.e. they have no individual information from which they can be distinguished except their MAC-addresses.

Devices like repeaters, hubs, star couplers or even bridges actually need no configuration specific to the network. As soon as there are agents and protocol stacks implemented on these devices, higher layer addresses may be needed like IP addresses to access SNMP agents. Routers and end systems always need some network dependent configuration to become operational. Today, this configuration task is often carried out manually for one system after the other. Some vendors also have developed proprietary protocols to remotely configure their machines.

A vendor independent method for all systems in a network as it is descibed in this paper improves the situation. The key features of the new method are the following.

- Configuration information is loaded to the target systems using two protocols, called SLTP (Simple Local Transfer Protocol) and SCMP (Simple Configuration Management Protocol).
- The target systems are distinguished by their MAC-addresses.
- SLTP is based on LLC Type 1 and provides a general reliable request-response style transfer mechanism, i.e. it is designed to carry remote procedure calls (RPCs).
- SCMP defines how the user data in SLTP is used for the configuration of systems. The new method as a whole will also be called SCMP for the rest of the paper because SCMP is one key element of the method.
- The configuration information consists mainly of names and addresses or selectors. SCMP has no notion of managed objects but handles attributes and actions.
- An SCMP agent on each target system passes the information to the local management of the system which moves the information to the right locations of the protocol stack.

A system should enrol with the Systems Management as soon as it has been configured with SCMP by the installation manager. For this purpose a notification is sent to the manager. The notification at the same time tests the Systems Management communication. The information necessary to access the directory service is added by the Systems Management.

For the operation and maintenance phases, Systems Management is used and thus the SCMP is no longer needed. For migration or conversion of a network, the access to systems via SCMP may prove useful.

3 Organization and Communication Models of SCMP

The purpose of SCMP is not to replace OSI Systems Management, but to complete it in the configuration management functional area for the installation of networks.

The organization model of SCMP is basically the same as for the Sytems Management. An SCMP agent on each target system receives SCMP requests from the installation manager. The agent does not carry out the requests but decodes and checks them before it passes the requests to the local management. The characteristics of the local management are outlined in the Management Framework, which forms part 4 of the OSI Basic Reference Model [8], and the Systems Management Overview [13]. However, the local management is not standardized because it depends heavily on the implementation of the protocol stack and on the operating system environment. The local management executes the request and returns the raw results, from which the SCMP agent generates the proper responses.

The main requirements of the communication protocols for the method are:

- simplicity as they are used only for configuration during the installation phase
- reliability
- MAC-addresses are the only means to distinguish systems because higher layer addresses will be set only during installation
- request–response style operation
- security

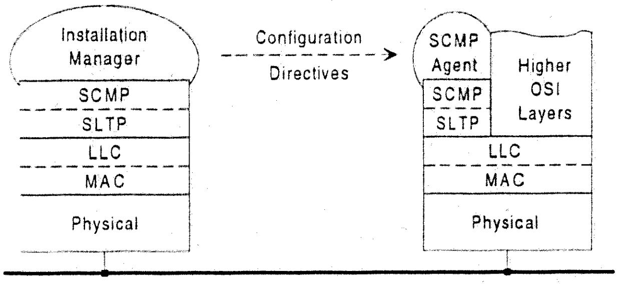

Figure 2: Collapsed architecture of SCMP

SCMP has a collapsed architecture like Mini-MAP (MAP – Manufacturing Automation Protocol) or CMOL (CMIP over LLC) [6]. The protocols are based on LLC Type 1 and all higher layer functionality is combined in two sublayers, in which the protocols SLTP and SCMP are used. The users of the SCMP service are an installation manager and the SCMP agents. Figure 2 depicts the resulting configuration.

SLTP provides reliable data transfer in half-duplex mode. In order to make the transfer reliable, SLTP uses implicit connections, i.e. with the receipt of the first data PDU, the connection is established. Connections are identified through the MAC-addresses of both sender and receiver. Therefore, only one connection between two systems is possible what is sufficient for configuration. The connection can be closed either explicitly by the installation manager or through a timeout after the last PDU in either of the SLTP protocol machines. Thus any deadlock situation resulting from problems in one of the systems or on the network can be resolved. Sequence numbering in combination with a retransmission timer is employed to insure reliable data transfer. When a connection is closed, the sequence numbers are reset. In order to allow large amounts of data to be transmitted, data may be segmented in a similar way as in the OSI transport protocol. The tag indicating the last data PDU belonging to a request or response is also employed as a token for the half-duplex mode operation. The token is initially assigned to the installation manager. Both protocol and service of SLTP have been formally described in LOTOS [5] and formal methods [16] and tools [3, 4] have been applied to verify the essential SLTP characteristics.

Services of the SCMP are defined to *get* and *set* attribute values and to trigger *actions*. Only one specific action is defined for SCMP. This action is called *Enable-Agent* and will be described in detail in the following section. To read attributes is useful to determine whether some attributes already contain sensible values. For the setting of attributes, the cases *set-replace*, *set-add* and *set-remove* are defined to deal with single-valued attributes and tables. In order to make the behaviour more robust against user errors, the set-add or set-remove operations and the action are defined to be invariant to repetition. When an entry is to be added to a table, it will be added only if it is not yet in the table. In either case the user will receive a positive response to indicate that the entry is in the table.

The SCMP PDUs fall into two groups, one for requests and the other for responses. For each group the first part of the PDUs has the same structure. Only the parts for the management information differ. Response PDUs contain an overall result which is independent of any specific operation or management information. If the operation has been successful, the desired attribute values or details for the action result are returned in the variable part of the PDUs. Otherwise, specific error information is returned.

4 Information Aspects of SCMP

4.1 Prerequisites for Systems Management Communication

It is necessary to know the prerequisites for Systems Management communication in order to fully understand the management information used with SCMP. The management information required consists of naming or addressing information and protocol parameters.

In order to identifiy an agent, a name must be assigned to it. In OSI, the application-process-title (AP-title) takes the role of a name. Multiple application-entities belonging to a single application-process are distinguished through their AE-qualifiers. There is a set of corresponding presentation addresses (the set comprises a single address in most cases) for each pair of AP-title and AE-qualifier. The presentation addresses can be retrieved from the *Application Title Directory Facility* (ATDF) [7] if only AP-title and AE-qualifier of an application-entity are known. The ATDF is part of the application layer management. It usually keeps some entries in a local table, and for the other requests it accesses the Directory Service via its directory user agent (DUA). The DUA communicates with a directory system agent (DSA) which provides access to the global directory.

The set of presentation addresses consists of multiple network addresses and a single selector on each of the higher layers. When the agent establishes or accepts an application association, it needs to know an appropriate application-context. Preferably, the application-context is selected from an international standardized profile (ISP) for which one or several application-contexts have been defined and registered.

For the other address information, no values are agreed or standardized. The selectors and the AE-qualifier for Systems Management communication could be fixed without constraining the applicability. The network addresses distinguish systems and therefore no predefined values for them may ever exist. Instead, the network operator has to select them according to his addressing scheme. The AP-titles have to be chosen by the network operator as well. The benefit of independents AP-titles is that they can be kept when a system is moved, while the network address usually must be changed.

In the case of the Systems Management agent, one more identifier is needed to name the topmost managed object of the containment tree. This object is always of class *system* and the identifier is the attribute *SystemId*.

Far less information is needed in order to configure a system for SNMP. The agent can be reached as soon as an IP address has been assigned to its system. The port numbers, which correspond roughly to the transport selectors, are fixed for SNMP. The agent has no AP-title and uses no SystemId attribute.

Incorrect protocol parameters may prevent systems from communication. This is mainly the case for the parameters of the transport and network layers. But it is possible to supply default values which should generally enable communication even if they are not optimal under the actual conditions.

The most common OSI protocol profile in LANs includes the transport protocol class 4 (TP4) [9] and the connectionless-mode network protocol (CLNP) [10] together with the end system-to-intermediate system protocol (ES-IS protocol) [11]. If SCMP is available anyway, it makes sense to set the protocol parameters via SCMP, too. On the transport layer, it is sensible to set the default protocol parameters for new transport connections. These protocol parameters include *retransmission time*, *maximum retransmission number*, *window time*, *inactivity time*, and *maximum TPDU size*. For the network entity the *NPDU lifetime* and *checksum option* should be set for CLNP and *holding timer*, *configuration timer*, *IS multicast address*, and *ES multicast address* for the ES-IS protocol.

4.2 Identifying the Resources

Protocol stack and agent may be present and running in a new system. They cannot become operational, however, unless the appropriate information is set. The key problem for the initial configuration is how something can be identified that has no name. This is the case for the agent and the system managed object. Only the system can be identified through its MAC-address.

The solution makes use of the fact that both the agent for the system's protocol stack and the corresponding system managed object are unique within a single system. The following paragraphs explain the steps to configure a system via SCMP until Systems Management can take over to complete the configuration. The protocol stack together with its local management as well as Systems Management agent and SCMP agent of the target system are assumed to be running. Typically, these elements are started together with the operating system.

The SystemId attribute can be assigned with a set-operation without explicitely identifying the system managed object. It is the task of the local management to find the location of the attribute. The AP-title of the agent and the (first) network address of the system cannot be assigned directly. The agent is a unique resource within a system, but all application-processes have AP-titles. In systems with complex protocol stacks (e.g. traditional data communication and multi-media integrated in a single stack) multiple distinct network addresses may be used. For that reason, it is better to take an indirect approach. The information is first transferred to the local table of the ATDF. Then the local management, which perfectly knows the structure of its protocol stack, is triggered to move the information to the right places.

The local management recognizes the entries from an additional field which contains the AP-type-title. The kind of application-process is described with this title. Thus it is perfectly suited to mark the entry for the agent and other special application-processes. Unlike the AP-titles, the AP-type-title is the same for all agents. Another entry is added for the manager to which the agent will enrol.

4.3 The Action Enable-Agent

After the installation manager has transferred all attributes to a system, it activates the Systems Management with the action Enable-Agent. Upon receipt of this action request the local management carries out the following steps. For this description, the action is assumed to be successful. The local management first checks whether the agent is already running. Then it looks for the absolutely necessary information, i.e. the SystemId attribute and the entry for the agent itself. The selectors for the agent and the network address are then assigned to the appropriate service access points (SAPs). Then the local management triggers the agent to start operation. The agent contacts the ATDF in order to retrieve its AP-title and AE-qualifier. If an entry of the default manager is available, the agent sends a notification to this manager. The result of this action is returned to the installation manager via SCMP.

If the agent is already operational when the action is requested, the scenario is much simpler. The response to the installation manager indicates that the agent is already active and returns its AP-title and the SystemId. The local management requests the agent to send another notification to its default manager. The network operator is alerted from this notification if somebody tries to manipulate systems via SCMP. If a fault may have occured, the communication of the agent can be tested with this action triggered by SCMP.

4.4 Access to the Directory Service

After successful completion of the action Enable-Agent, the manager continues to configure the system. The configuration of the access to the Directory Service is described here because it offers a general information service about network resources. The manager first reads the containment tree to get information about all resources of the system. Then it adds entries to the ATDF for both the DUA and the DSA and also adds necessary selectors to SAPs. The AP-title and AE-qualifier for the DUA can be directly assigned. The Systems Management is able to find the DUA provided both ATDF and DUA are modelled as managed objects and the ATDF contains a relationship attribute that points to the DUA. The standardization process for the management information is ongoing, but the proposals (e.g. in ISO DIS 10165-5 [14]) suggest that the assumption made above is reasonable. The entries for DUA and DSA contain AP-type-titles, too. Thus the DUA can find both its own entry and that of the DSA.

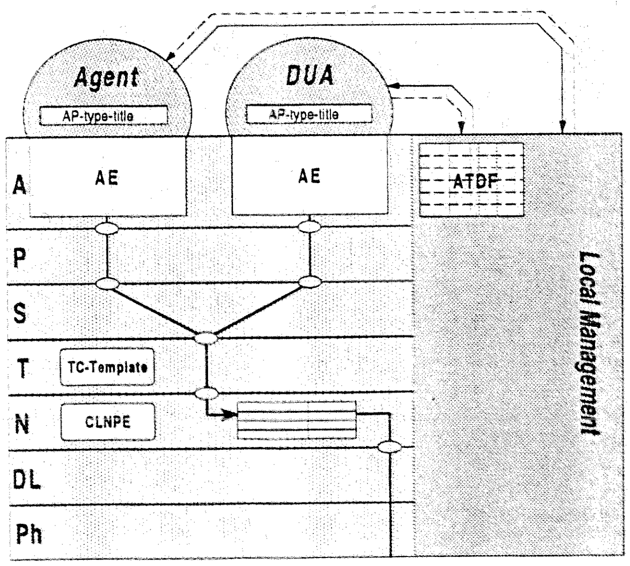

Figure 3: OSI protocol stack with agent and directory user agent

The resulting protocol stack together with agent, DUA and local management are depicted in figure 3. Moreover, the ATDF, the paths through the stack, and the managed objects containing the protocol parameters on layers 4 and 3 are shown.

The attribute values should be saved on disk or another non-volatile memory after the initial configuration. When the system is rebooted, the attributes are restored by the local management and the action Enable-Agent is carried out in the same way as via SCMP. The DUA has to retrieve its own AP-title and AE-qualifier from the ATDF. Both agent and DUA can also find their manager and DSA in the ATDF. This enables the system to get in contact with the outside world.

5 Security in SCMP

An important issue in network management is security. This section gives some hints how security is built into SCMP. A certain level of security is inherent to SCMP because routers can never be passed by SCMP.

Two levels of security have been worked out. The first level does without cryptographic mechanisms. Access is controlled using a list of MAC-addresses. This access list can be modified via SCMP or Systems Management operations.

The second level employs asymmetric cryptographic mechanisms to sign the requests [15]. Confidentiality of the requests is not ensured, but their integrity. The manager at the same time is authenticated. Thus no intruder can manipulate systems using SCMP. Use of cryptographic algorithms can only be justified, however, if they are also used for Systems Management.

6 Conclusion

The main sections of this paper have presented the building blocks of a method that makes the configuration tasks during network installation efficient, simple, and consistent with basic OSI concepts. The most important aspect of SCMP is the information that has to be brought to systems. This information is processed by the local management to make Systems Management and Directory Service operational. The simple protocols for transfering the information are the other building block of SCMP.

The main benefits of SCMP are:

- Information from the design and planning phase is used to configure the systems, which is more convenient and less error-prone than retyping the addresses for all systems.
- Not every system must be accessed physically.
- Usually the local configuration utilities implemented on different systems are dissimilar whereas with the installation manager all systems are configured in the same way. It is even possible to automate the configuration procedure. In this case, the sequence of the configuration steps is determined during the planning phase and a script for the installation manager is generated.

Implementation effort for the new method is reasonable as SCMP relies on the local management to access the attributes within the protocol stack. Implementation of the protocols SCMP and SLTP is simple and the protocol entities require few resources only. This has been proved in a prototype implementation which also validates the concepts of SCMP.

References

[1] J. D. Case et al., "Simple Network Management Protocol (SNMP)", Request for Comments 1157, DDN Network Information Center, SRI Int., May 1990.

[2] B. Croft and J. Gilmore, "Bootstrap Protocol", Request for Comments 951, Network Information Center, SRI Int., September 1985.

[3] J.-C. Fernandez and L. Mounier, "Verifying bisimulations on the fly", in: J. Quemada, J. Mañas and E. Vázquez, eds., *Formal Description Techniques, III*, Proc. IFIP TC6 3rd International Conference on Formal Description Techniques for Distributed Systems and Communication Protocols — FORTE 90, Madrid, Spain, 6 – 9 November 1990 (North-Holland, Amsterdam, 1991) 91 – 105.

[4] H. Garavel and J. Sifakis, "Compilation and verification of LOTOS specifications", in: L. Logrippo, R.L. Probert and H. Ural, eds., *Protocol Specification, Testing, and Verification, X*, Proc. IFIP WG6.1 10th International Symposium, Ottawa, Ont., Canada, 12 – 15 June 1990 (North-Holland, Amsterdam, 1990) 359 – 376.

[5] D. Hogrefe, *Estelle, LOTOS und SDL — Standard-Spezifikationssprachen für verteilte Systeme*, Springer-Verlag, Berlin, Heidelberg, 1989.

[6] IEEE 802.1B, "Draft Standard 802.1B - LAN/MAN Management", P802.1B/D18, 1991.

[7] ISO 7498-3, "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 3: Naming and Addressing", 1989.

[8] ISO 7498-4, "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 4: Management Framework", 1989.

[9] ISO 8073, "Information processing systems - Data communications - Connection Oriented Transport Protocol Specification", 1992.

[10] ISO 8473, "Information processing systems - Data communications - Protocol for providing the connectionless-mode network service", 1988.

[11] ISO 9542, "Information processing systems - Telecommunications and information exchange between systems - End system to Intermediate system routeing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473)", 1988.

[12] ISO 9596-1, "Information Technology - Open Systems Interconnection - Management Information Service Definition - Part 1: Common Management Information Service Protocol Specification", 1990.

[13] ISO/IEC 10040, "Information Technology - Open Systems Interconnection - Systems Management Overview", 1992.

[14] ISO/IEC DIS 10165-5, "Information Technology - Open Systems Interconnection - Structure of Management Information - Part 5: Generic Management Information", 1991.

[15] P. Janson and R. Molva, "Security in open networks and distributed systems", *Computer Networks and ISDN Systems* 22 (1991), pp. 323 - 346.

[16] R. Milner, *Communication and Concurrency*, Prentice Hall, Englewood Cliffs, 1989.