ABSTRACT

The growing trend of corporate organizations to embrace intranet technology is accelerating the computing paradigm shift from a desktop-centric model to a network-centric one. Intranet revamps the enterprise LAN and WAN by adorning them with the glaze of Internet attire. As with any kind of network, intranet reliability is subordinate to the attention and effort put into its management. Since what characterizes an intranet is not only its network infrastructure but also its information content and the way it is created, shared, and stored, intranet management must extend beyond typical network management issues and encompass service management. In this article, the authors elaborate on intranet management and reflect on the challenges it poses.

An Outlook on Intranet Management

Raouf Boutaba, University of Montréal

Karim El Guemhioui and Petre Dini, Computer Science Research Institute of Montreal (CRIM)

It is a truism to say that the Internet, and particularly the World Wide Web, is pervading almost all areas of human activity. Our relationship to computers, as standalone machines and, more important, as fundamental building blocks of higher and more sophisticated working tools (namely networks) is being revolutionized. The universal acceptance of the Internet and the Web has resulted in a shift from a desktop-centric model of computing to a network-centric paradigm.

While the Internet has captured the interest of certain sectors (the research community, academia, etc.), intranets — that is, in-house networks based on Internet technology — are quietly replacing proprietary networks with interoperable enhanced platforms (e.g., with hypermedia support) based on relatively simple and inexpensive Internet tools. These technologies are progressing at a very rapid pace. The distinguishing feature of an intranet is that access to information published on it is restricted to clients in the intranet group. Historically, the idea is not very new, and has previously been accomplished through the use of local area networks (LANs) protected by firewalls. What distinguishes an intranet from a more traditional LAN or proprietary wide area network (WAN) is not the hardware infrastructure, but communication standards (those of the Internet) and services or information standards (those of the Web) upon which it is built. Otherwise, the tools used to create an intranet are basically identical to those used for Internet and Web applications [1].

The success of an intranet depends on three key factors: the technical infrastructure, content, and management [2]. The technical infrastructure consists of the networks, hardware, and software underlying the intranet. Content encompasses data and processes to support the special information needs behind the creation of the intranet. Finally, intranet management is the indispensable glue that permits the smooth and effective development and use of intranet content on top of an intranet technical infrastructure. Intranet management provides an instrument for planning, administration, and maintenance. These latter activities must be applied in an integrated manner to communication and distributed processing resources.

Until now, most of the emphasis in intranets has been on the implementation of the technical infrastructure and the development of special content. Little has been done to address the specific challenges raised by intranet management. In general, the management issues faced by an enterprise adopting intranet technology are closely related to the management policies and goals of the enterprise. Because of the myriad possible management policies and goals, it is important to consider the automation of as many intranet management tasks as possible. For that purpose, the management tasks must be appropriately structured and organized, and the management policies and procedures better formulated. In this article, we present some of the research efforts in this area and reflect on possible future trends in intranet management. The second section introduces foundational concepts and presents an intranet architecture. The third section reflects on basic intranet management issues. The fourth section presents a management model and an intranet management architecture. Finally, the fifth section concludes this article.

AN INTRANET OVERVIEW

"Intranet" is one of the latest buzzwords in the computer and networking area which unveils the still emerging and evolving nature of the field. Basically, an intranet is a network connecting a set of affiliated computers and devices using Internet protocols, such as Transmission Control Protocol/Internet Protocol (TCP/IP) and Hypertext Transport Protocol (HTTP), and technology (e.g., the Web, newsgroups, e-mail). In an intranet, the network nodes are confined within the enterprise that operates it, and are protected from the external world by one or more firewalls. Intranets can be implemented exclusively as internal distributed networks over LANs and WANs, or with an opening to the outside world through some Internet access, from behind a firewall. The former implementation is less concerned with security issues, although it can be subject to internal attacks. The latter implementation is definitely exposed to security breaches from the outside and requires special handling of the problem [3].

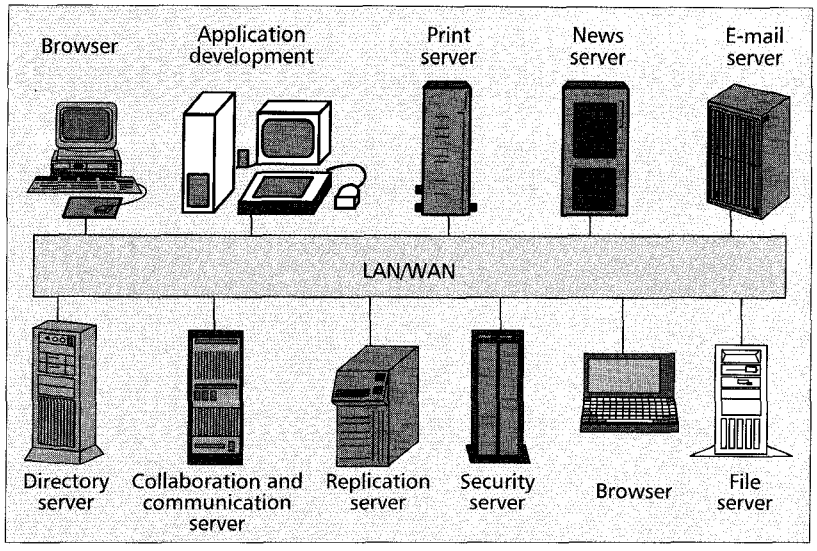
0163-6804/97/$10.00 © 1997 IEEE

THE INTRANET BOON

Intranets provide some of the most empowering and cost-effective technologies since the telephone. Although simple in architecture, intranets have the potential to change the way people work, learn, and process information. For example, hypertext markup language (HTML) authoring — the basic skill used to create intranet content — is fast coming within reach of any employee in the enterprise. Numerous HTML authoring tools (e.g., HoTMetaL, QuickSite, FrontPage, Claris HomePage) enable the quick and easy development of intranet content without special expertise.

Among the main motivations drawing enterprises to embrace the intranet wave are the expected reduction in operating and maintenance costs and the accrued gains in worker productivity. These aspects have been extensively discussed elsewhere [4, 5]. Briefly, intranets provide a very flexible yet powerful means for quick and efficient dissemination of up-to-date information on all aspects of the enterprise life (e.g., corporate goals and plans, administrative procedures and forms, internal newsletter, employees benefit packages). Intranets allow faster and more efficient information retrieval. With electronic storage and dedicated search tools, users can quickly zero in on important information and avoid wading through lengthy paper-based lists and/or indexes.

Intranets promote constructive, even interactive, exchange of information (e.g., e-mail, groupware, corporate newsgroups, etc.). Entire concurrent engineering sessions can be conducted via the intranet. Critical information can be posted as soon as it becomes available, instead of having to wait for paper distribution. When appropriate, immediate feedback can be solicited. As a result, substantial savings in time and money can be realized by enterprises endowed with an intranet. There is less need for printed material, express mail and fax fees are reduced, lengthy face-to-face meetings can be kept to a minimum, and some expensive and time-consuming business travel can be avoided.



■ **Figure 1.** *Intranet architecture.*

A TYPICAL INTRANET ARCHITECTURE

Basically, an intranet is characterized by the communication infrastructure on which it is built, the set of services it provides, and the applications it supports. Figure 1 shows a synoptic view of an intranet architecture. Communication is ensured by the underlying LAN or WAN, and is usually based on TCP/IP. Intranet communications rely heavily on open standards and technology borrowed from the Internet.

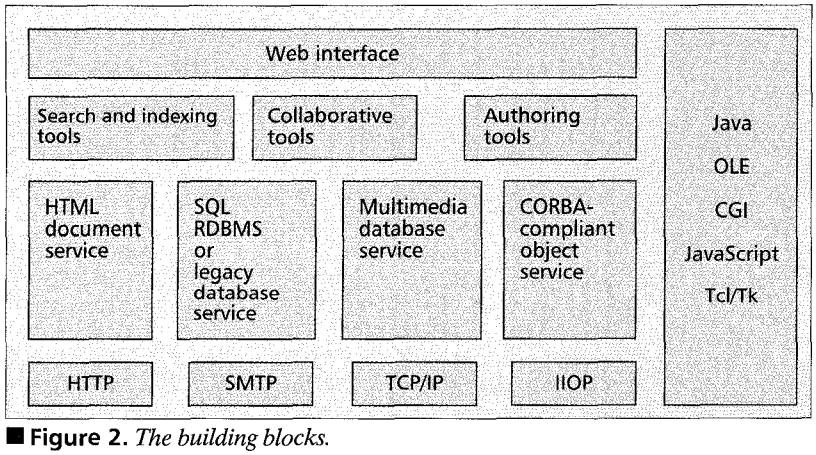
Intranets need appropriate support for creating scalable applications, conducting transactions, and enabling decision making. These capabilities are provided by a set of intranet services. It is important that the core services characterizing an intranet be built on open standards and protocols to preserve interoperability and vendor independence, and to provide the leverage necessary for the expansion and evolution of the technology outside proprietary solutions. The new term *full-service intranet* has been coined to describe this approach [6].

In its definition of the full-service intranet, the Forrester Report [6] identifies five core standards-based services: directory, e-mail, file, print, and network management. The Netscape team elaborates further on this concept and proposes a grouping of the full intranet services into two categories: user services and network services [7]. User services comprise information sharing and management, navigation, communication and collaboration, and application access. Network services are broken down into directory, security, replication, and management.

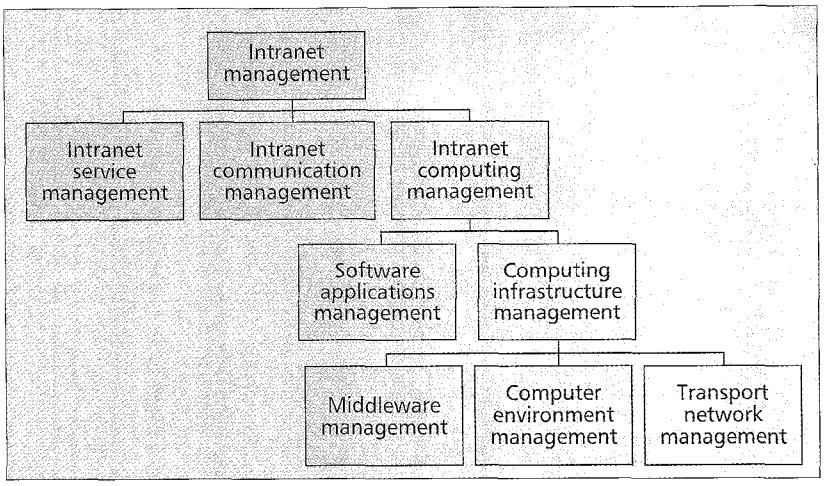
As shown in Fig. 2, a number of fundamental building blocks contribute to providing the required functionalities and sustaining the architecture depicted in Fig. 1. Basically, intranet documents are accessed via a Web interface. Several existing tools provide intranet-specific functionalities for searching or indexing documents, and for collaborative or authoring work. These tools can be used to support a set of services such as HTML, standard query language — relational database management system (SQL-RDBMS), legacy DB, multimedia DB, or Common Object Request Broker Architecture (CORBA)-compliant object services. These services, in turn, rely on dedicated protocols such as the Internet TCP/IP communication protocol, the Simple Mail Transfer Protocol (SMTP), the document-oriented protocol (HTTP), or the Internet Inter-ORB Protocol (IIOP). A set of Internet/intranet programming languages can be used to develop these tools and services.

Finally, the building blocks sustaining the intranet architecture (Fig. 2) can be used to develop numerous applications distinguishing the intranet. These applications can be categorized into the following areas:

- E-mail, groupware, and team collaboration
- Real-time audio and video communication
- Information publishing and sharing



■ **Figure 2.** *The building blocks.*



■ **Figure 3.** *Intranet management classification.*

- Navigation and full text indexing and searching
- Various directories (of people, businesses, etc.)

From Premises to Intranet Management

Most corporate intranets run on existing network infrastructures, which reduces technical challenges to some extent. However, the need to migrate legacy applications to intranets' TCP/IP-based environments is far from being obvious, and can be a costly and time-consuming operation, even for large companies. This is just one of the many problems facing corporations planning to adopt intranet technology. Another very important point to keep in mind when choosing an intranet-centered model of work organization, is the necessity to ensure constant availability of the intranet computing and communication resources. Indeed, in this approach the intranet becomes the primary computing and communication infrastructure in the enterprise, through which all of its critical business is conducted. A (prolonged) failure of the intranet can seriously impair the functioning of the entire enterprise and even jeopardize its future. More than ever, proper and diligent management of the intranet must be at the top of the enterprise priorities in order for this technology to fulfill its role and reap the promised benefits. All the intranet constituents must be adequately managed, namely, communications, services, and applications (Fig. 3).

Managing Communications

Intranet communications usually occur through a corporate LAN or a set of distributed subnetworks interconnected by a metropolitan area network (MAN)/WAN network. The network or networks on which an intranet is built have management needs that are common to most computer network infrastructures, as well as specific requirements more tied to this particular technology and the context in which it operates.

In its simplest form, communication management requires specialized functions and techniques such as monitoring and event management. Basically, communication management involves monitoring servers and other devices on the network known as network elements (NEs). Simple protocols and services are used to configure and/or repair network connectivity, making more complex, higher-level services available. Simple Network Management Protocol (SNMP) [8] is used primarily in the management of TCP/IP-based ne tworks; however, many manufacturers have their own management protocols and tools.

In some cases, network management must accommodate different proprietary protocols and provide a uniform view of all management interactions. This entails handling a multiprotocol management environment. A framework must be provided for interoperability of the existing management platforms. One possible approach is to add on top of the existing management frameworks an integrating and unifying management environment such as Distributed Management Environment (DME) [9]. DME presents a unified view of all management information pertaining to SNMP and Common Management Information Protocol (CMIP) [8].

Managing the Services

A full-service intranet is characterized by a core of fundamental services such as those identified by the Netscape Team and briefly described below.

The information sharing and management service provides seamless and transparent content publishing across the intranet. It ensures that authorized users have the latest information. Many commercial products are available that ease the development of intranet content. This information can readily be made available and accessible from anywhere on the intranet.

The navigation service allows the retrieval of any piece of information or resource located on the intranet. Access control ensures that confidential documents are disclosed to authorized personnel only. Single or complex queries can be issued across the intranet. Indices and organized query results can be created and maintained.

The communication and collaboration service enables e-mail and discussion groups. The privacy of both must be ensured. An authentication mechanism must be provided. Sophisticated e-mail and/or discussion groups can incorporate multimedia content.

The application access service allows easy and uniform access to existing databases and legacy applications. New applications developed with Java can quickly be downloaded on any platform and easily accessed from a single interface.

The directory service tracks and manages information about users, access control, server configuration, and application-specific requirements. The service must overcome operating environment and application differences. This service can be managed from a central location, with information replicated whenever relevant.

The security service provides ways for resources to be protected against unauthorized users, for communication to be encrypted and authenticated, and for the integrity of information to be verified. This service must be managed centrally to preserve its integrity and consistency.

The replication service is in charge of spreading data across the intranet. Replication of heavily demanded information allows the load on some system resources to be eased.

The management service is in charge of ensuring the proper functioning of the underlying network. The features of this service were detailed in the previous subsection. This service should provide a unified, user-friendly, ubiquitous management interface that permits management of all servers and resources from anywhere on the intranet.

All the aforementioned services must be adequately managed through a common and integrated platform. This activity is called *service management* and can be summarized as the ability to negotiate, activate, and ensure service. It is concerned with service-related issues such as providing a service, ensuring a quality of service (QoS), restricting access to a service, providing a unified and consistent view of all services offered, handling interactions between supported services, and

so on. Service management has a broader scope than network management. The telecommunications management network (TMN) approach [10] proposes a responsibility model that describes management in terms of layers, and identifies the service management layer as subsuming the network management layer. Figure 4 shows the TMN hierarchical view of management and how a set of five well-defined management functions percolate through all the management layers. The semantics of the five management functions in the network management layer differs from the semantics of their counterparts in the service management layer. While network management usually consists of reactive management of the physical communication infrastructure, service management can be characterized as a proactive activity that puts the intranet customers in front. In the fourth section, we present a management architecture that emphasizes the central role played by the management of services in the effective deployment of full-service intranets.

Managing the Applications

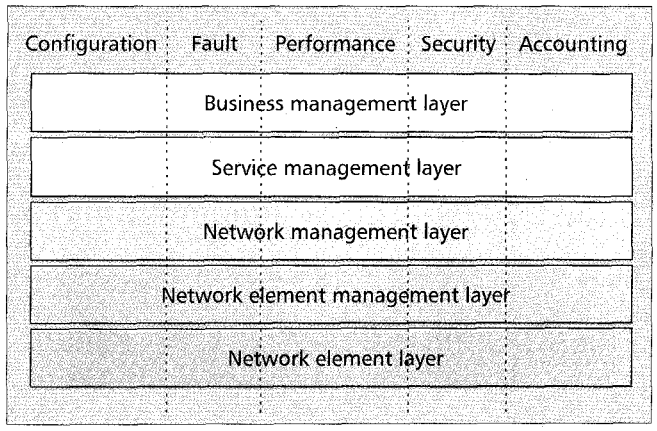
Application management is aimed at ensuring that the applications run properly and make the most efficient use of the resources at their disposal, the ultimate goal being to provide the best service possible at the lowest cost, even in case of partial system failures.

The main goals of application management can be summarized as follows:

- Maintenance of an appropriate QoS. This allows a good return on the investment and on the cost of the software by ensuring that the expected application services are fully provided.
- Adjustment to immediate needs for cost-effective utilization of the applications. We should be able to adapt an application to respond to users' needs very similar to the ones for which it was originally conceived. For example, an e-mail service could be adapted to replace a file transfer service between sites.
- Optimization of resource utilization such as files, documents, communication links, and peripheral devices. For example, the use of local disks must be maximized while resorting to communication links subject to billing must be minimized.

Trends in Intranet Management

This section presents current works on intranet management with an emphasis on modeling and architectural issues. Management problems experienced in Internet become particularly weighty in intranets due to their private nature. The typical Internet triplet of network elements, SNMP agents, and management stations running management tools does not suffice to properly manage intranets. First, intranet solutions with limited management capabilities to handle legacy documentation components will have low value to organizations. Second, particular intranet servers, such as those shown in Fig. 1, are not considered manageable components. Third, traditional SNMP-based agents are not powerful enough to locally take automated decisions, for example, to control all activities to prevent downtime from stalled intranets/Internet servers, or to automatically install a new version of a software when the current version is no longer accessible or the server on which it runs is down. These problems can be summarized by low automation, lack of customization, and low integration. Since these criteria are essential features to guarantee scalability, availability, and reliability in intranets, we present potential solutions and current trends to alleviate the negative impact of the aforementioned problems.



■ **Figure 4.** *TMN responsibility model.*

A Management Model

Several studies have shown the importance and impact an enterprise model can have to and on the management of the underlying information technology. This is particularly relevant for intranet management. Thus, before defining a management model and identifying the involved participants, we should examine the role and span of enterprise management.

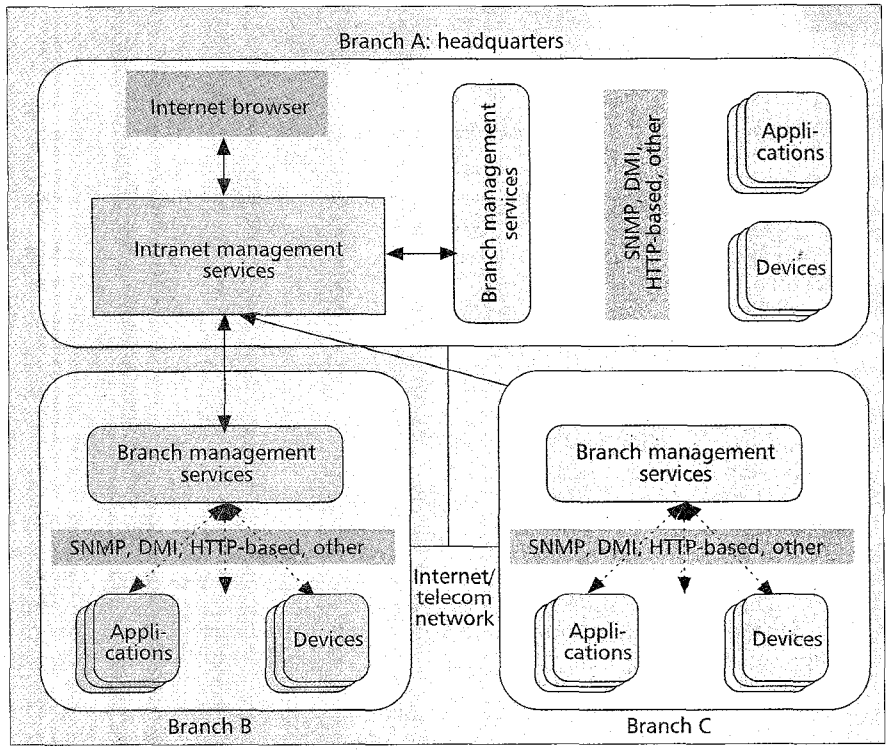
Management is necessary for proper functioning of the enterprise. It comprises the supervision and control of all the resources and activities required by the enterprise to reach its goals. These goals are set by CEOs who also determine the policies to follow to reach the defined objectives. In this context, management usually reflects a hierarchical structure. Regardless of the goals set, it is necessary that the enterprise activities be managed efficiently with respect to time and costs, and consistently with respect to the adopted policies. Management must also take into account the availability of resources and the market demand for products and services. Furthermore, it is critical for the enterprise to have control over the evolution of its business environment, the staff it employs, and/or the information technology it uses.

The management of the underlying information technology is likely to mirror the hierarchical organization of the enterprise, which relies on the delegation of management tasks among different managers [11]. At each level of the hierarchy, management can be modeled as a process by which a manager supervises and controls resources to reach the management goals. This process involves the following steps:

- Observing the resources; gathering information about their behavior and verifying their consistency with respect to the defined goals
- Making decisions based on the aforementioned observations and exercising appropriate control actions on those resources, in compliance with a predefined policy and according to a detailed plan
- Reporting local management results to a hierarchical superior

The strength of this model is its ubiquitous aspect that allows its uniform application to all levels of the management hierarchy. This recursive aspect of management implies several levels of refinement and specialization of management information and activities. For that purpose, mechanisms must be developed for the automation of these refinements and to relieve the human operator of an otherwise overwhelming decision-making task. The ultimate objective is to define a process for the derivation of control commands from abstract management goals, using management policies and plans [12]. This process is activated each time a new goal is defined (i.e., proactive management) or a significant event detected in a managed resource (i.e., reactive management).

One of the main problems which arises is that there are no



■ **Figure 5.** *An integrated intranet management architecture.*

two identical intranet architectures; therefore, no two intranets' managements are similar. The role of the manager is to customize and adapt standard management functions to ensure a reliable and efficient management of his/her intranet. Management domains and policies are two key elements for the customization and automation of the management process.

Management Domains and Policies

For intranet management to be effective and efficient, it must follow a clearly defined strategy. Several factors related to the environment affect the management strategy. Among the most relevant, we can mention:

- The enterprise goals
- Its organizational and administrative structure
- The interorganization relationships
- The technology
- The incremental character of networks and information processing systems, and therefore of intranets

The enterprise goals define why and how the intranet is used as well as the management policies that impact this use. Policy affects the importance given to intranet security and availability issues. These, in turn, determine the need for fault recovery and system performance monitoring; they also restrain interactions between organizations. Goals can vary depending on the type of enterprise. The overall goal of management is to maintain the service required by users and enable the evolution of the system by integrating new functionalities and/or new technologies. More specific goals can be to optimize the use of resources, to minimize costs, to maximize income, and to optimize service performance. For example, the goals assigned to an intranet belonging to a business organization reflect a business policy aimed at maximizing profits. The main objective of a military command and control system is to ensure constant availability, regardless of how much it may cost. A multi-organization system must compromise and agree on a policy that best serves the interests of the various participants.

The organizational and administrative structure of the enterprise affects the structure and style of management of its underlying intranet. Some aspects of management are taken up by individual departments, while others are centralized at a specific site or at some level of enterprise leadership. Management of large intranets, even within the same organization, requires interaction between somewhat autonomous administrative units implementing their own policies. Management relations between independent units are negotiated by these units so as to satisfy their respective policies and still reach the overall system management goals. The technical answer to this structuring requirement is to identify management domains where each domain exercises, on the resources and activities it encompasses, one or more management policies.

Large intranets are generally spread over several LAN and WAN network segments. LANs are usually owned by an enterprise, while WANs are often managed by a third party (e.g., telecommunications operator or Internet service provider). These multinetworks support several communication mechanisms, often divergent because constrained by different technologies. Communication suppliers and the organizations they interconnect must coordinate their heterogeneous management practices.

Information and communication technologies also impact the management strategy. Resources with basic management facilities restrain the efficiency of management policies that require extensive supervision and control. Intranets are made up of a large number of different and heterogeneous resources. Consistent management in a multivendor, heterogeneous environment requires management tools that comply with appropriate standards. These standards must commonly specify the goals and management policy in the same way standards specify communication protocols.

Intranets are incremental in nature and grow by interconnecting with additional components to meet new needs. A viable management strategy anticipates the fact that intranets and their management capabilities evolve incrementally. The management system incorporates management tools that will be upgraded each time more powerful tools become available. Management must take into account the fact that intranets are enriched with additional communication and processing facilities in an incremental way. It must also allow easy integration of new services.

A Management Architecture

An intranet management architecture should reflect the enterprise structure and its management hierarchy. Usually, an intranet within a company with multiple branches is composed of several intranet clusters. For example, Fig. 5 depicts the case of a company with three branches, A, B, and C, with A representing the company's headquarters. Typically, functional intranet branches represent administrative domains. In the previous subsection, we have detailed the role played by management domains in the achievement of the enterprise goals.

Intranet administration is likely to be centralized to facilitate management and reduce operating costs. Under this scheme, a manager at headquarters can administer remote servers in branch offices through an integrated, user-friendly,

Web-based interface. In compliance with this centralized management approach, we can define a layered intranet management architecture inspired by the standard model presented in Fig. 4. An illustration of such an architecture is shown in Fig. 5, where three visibility levels are defined: intranet, branch, and resource management.

The intranet management layer (IML) provides and end-to-end view of intranet services, communication, and computing resources involved in sustaining intranet applications. This layer could be subdivided into two sublayers, the user service management and network service management levels. The user service management level deals with the provision of intranet services to end users according to a contracted QoS and access rights. This level provides a unified user interface and interacts with the network service management level. The network service management level ensures the coordination of network and system resources involved in the intranet infrastructure. It also ensures interoperability with the public network operator or Internet service provider responsible for managing the network interconnecting the different intranet branches.

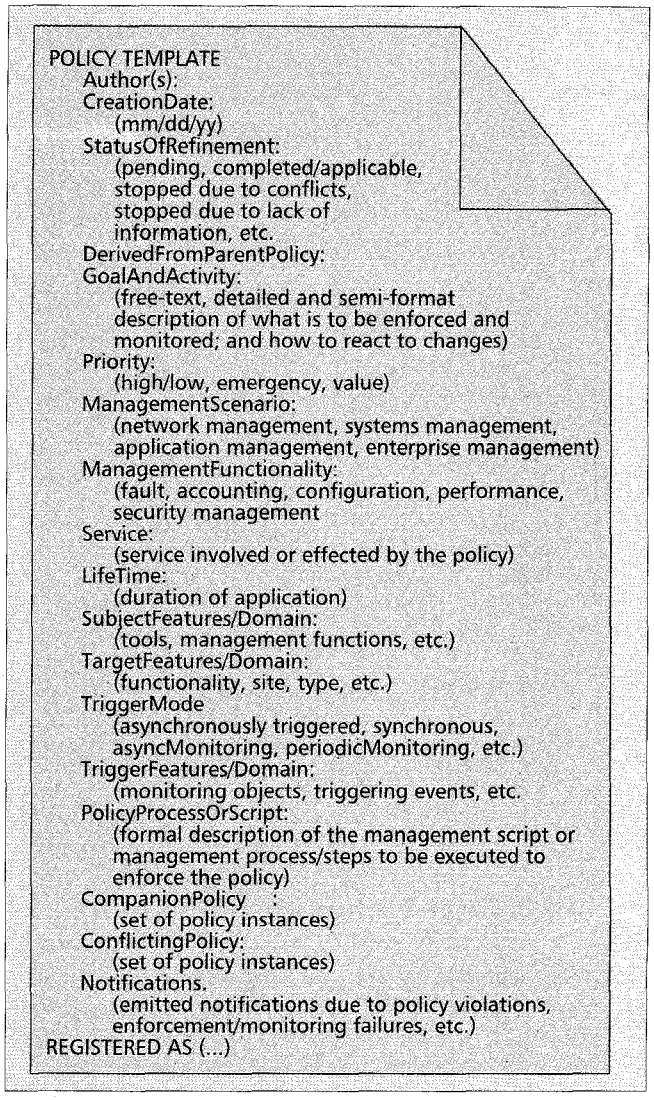
The branch management layer (BML) reveals the administrative structure of the intranet. It ensures the coordination of the services, systems, and network resources involved in an intranet branch. To some extent, this layer is similar to the IML in that it also provides user and network views of the intranet services, but at the level of a single intranet branch. Typically, the services considered here are those specific to the managed branch. The BML acts as a server to the intranet management aggregation layer and interacts with the resource management layer.

The resource management layer (RML) describes connectivity, processing, and storage capabilities offered by individual physical and logical resources composing the intranet. The resources managed at this level are those involved from the user/application level through the system and network layers to remote service/server instances. These managed resources are monitored through standard protocols such as SNMP and Definition of Management Information (DMI) or any proprietary application programming interface (API). For example, a remote procedure call (RPC)-based mechanism can be used to instrument specific managed elements to overcome the SNMP unreliable message delivery. The HTTP protocol could also be used for the management of hypermedia-based applications.

Management Services for the Intranet

An intranet requires traditional management services to tune the configuration and to ensure high availability, security, backup, and recovery. Since intranets present characteristics which are specific to each enterprise, additional management services must be defined. Among these services, the domain and policy services are of particular importance in the context of intranet management and will be detailed in the following sections. A Web-based interface allows a uniform representation of management and functional information.

Domain Management Service — To satisfy protection and security concerns, and cluster management responsibilities, the management domains concept can be used. Management domains can be inside an intranet branch or can share several branches. This grouping may be used to apply a common management policy as derived from enterprise business goals, or to represent the organization structure as reflected by intranet branches. Each domain has its own manager which is responsible for applying appropriate policies corresponding to well-defined business goals. To manage intranet domains, a domain management service must handle domain creation, domain suppression, and domain evolution. This evolution must allow domain merging and domain partitioning. It must also enable the addition/removal of an object to/from a domain. The domain management service provides the underlying services required for naming and translation of path names to component identifiers and addresses.

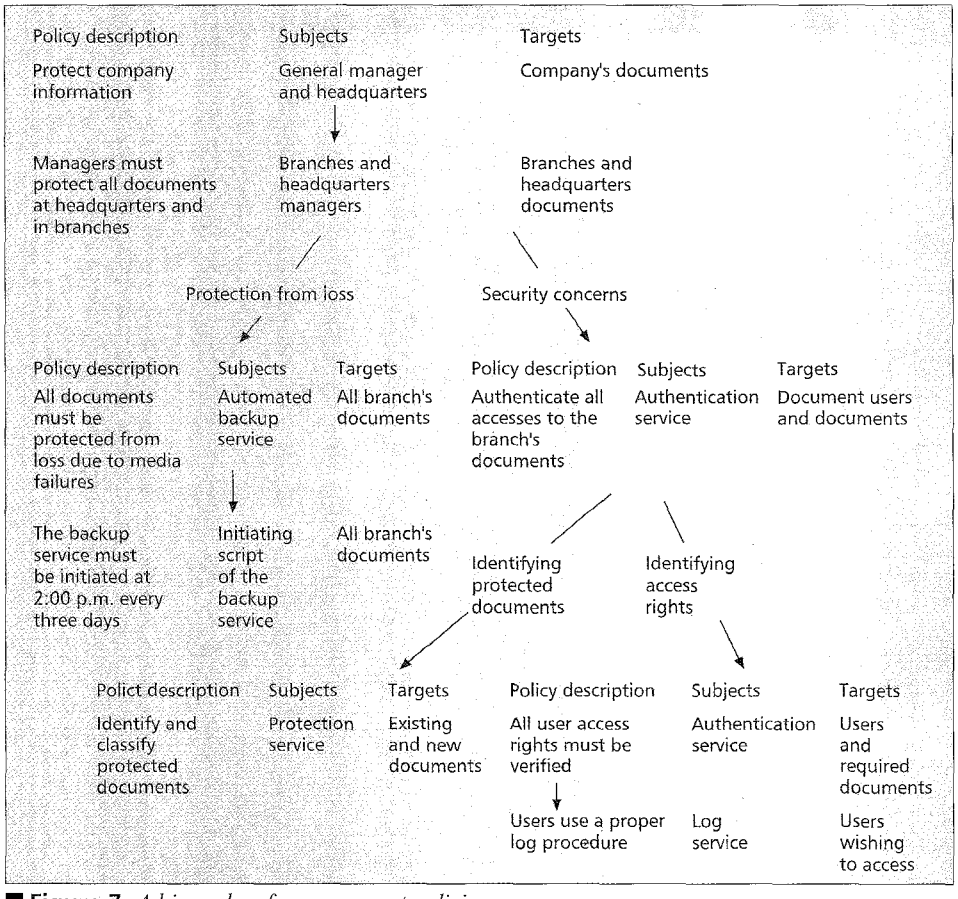


■ **Figure 6.** *A policy template.*

Policy Management Service — Automation of intranet management is based on management policies which reflect a precise definition of business goals that are usually less precise and subject to multiple interpretations. In a multibranch intranet, misinterpretations of enterprise goals within a branch may lead to total degradation of intranet services. A policy is a coherent set of rules with two related purposes:

- The definition of the goals of an organization
- The allocation of the resources to achieve these goals

A policy management service is intended to define, enforce, use, prohibit the use of, or destroy a policy. As shown in Fig. 6, a policy has particular static and dynamic properties which must be automatically managed. Static properties specify subject actors for performing a policy, target objects obeying a policy, or the lifetime of a policy [13]. Other static properties refer to companion policies requested to activate a given policy and the goals from which a policy is derived. Dynamic properties represent policy behavior as a set of rules. Rules specify constraints related to the state of the managed system and a set



■ **Figure 7.** *A hierarchy of management policies.*

of actions that apply to managed components. A management policy is not concerned with the performing of these actions. The role for performing these actions is played by appropriate services, commonly using SNMP primitives. Current applications provide such kinds of services. For example, a policy-based management approach has been adopted by Cisco [14] which proposes a virtual membership policy server within their line of products for switched internetworking.

Management policies are linked to each other in a hierarchy of policies that reflect the organizational structure of the enterprise. In this hierarchy, high-level policies are general formulations of the way managers must reach one or several enterprise goals. Low-level policies must satisfy high-level policies and are created or modified whenever the latter are defined or changed. They are directly applied to intranet managed resources, and they generally translate into one or more executable scripts. Figure 7 shows a hierarchy of policies relative to the protection of an enterprise's documents [15]. This hierarchy of policies would apply to an intranet with a management architecture similar to the one depicted in Fig. 5.

Scripts can be defined using management information base (MIB) structures [16]. For the manipulation of management scripts the following operations are useful:

- Transfer management scripts to managers
- Initiate, suspend, resume, and terminate management scripts
- Transfer arguments for management scripts
- Monitor and control running management scripts

Management scripts can be implemented using Java, JavaScript, Tcl/Tk, or Perl.

We have already emphasized the importance of providing an adequate platform and user interface for the management of all the aforementioned services. In the next section, we detail this point.

Web-Based Management

The existing heterogeneity of platforms and the proliferation of approaches and models for network management make applications development and network management very costly by requiring system administrators to deal with multiple technologies. The ever-increasing spread of intranets and the growing popularity of the Web and associated tools (e.g., Java, HTML pages) have spawned a number of research efforts and commercial initiatives aimed at applying these new technologies to the challenging problem of network and service management [17].

Web-based solutions to network and service management are attractive for several reasons. Web browsers present the same look and feel, and allow transparent access to every kind of information on the intranet Web, using a single well-established user interface. They provide access from anywhere on the intranet to a huge base of information spread across all the intranet machines and devices. Network managers don't need to use different tools through disparate, incompatible, and costly interfaces for the monitoring of their networks and services. New technologies, such as Java, facilitate upgrading to newly released versions. Installation of new versions of monitoring software in a network is complex and costly. Transparent and rapid downloading via a Java-enabled Web browser constitutes an attractive alternative. In addition, Java-based APIs not only provide standardized interfaces for managing an intranet through the Web, but also provide a good platform-independent solution in a distributed environment.

Lately, two proposals have been released to unify and standardize network management through the Web. The two proposed standards, Web-Based Enterprise Management (WBEM) [18] and Java Management API (JMAPI) [19] are not really direct competitive technologies in the sense that they have different philosophies. There are, however, areas where the two approaches overlap. WBEM is based on the concept that a new, revamped protocol is needed to communicate with managed devices through the Web. The JMAPI approach builds on the existing. It prefers the addition of an intermediate application interface that converts Web browser requests into some form the managed devices (more specifically their management protocols) can understand. The managed data is accessed and manipulated by Java applets invoked through the Web browser.

Several vendors have also started offering intranet Web-based management products (e.g., TME 10 from Tivoli, Solstice from Sun, Visual Uptime IMS from Visual Networks). Web-based solutions constitute a cost-effective way to reduce the heavy investments associated with dedicated consoles characterizing proprietary solutions.

Emerging development tools from independent vendors can map SNMP MIBs to HTML, CGI, Java, or C code running on

Web servers. Many of the products offered link MIBs to a Web page. However, network managers are on their own when it comes to designing applications and deciding such key issues as where databases are to be located. Some vendors use CGI scripts or proprietary mechanisms to link Web browsers to element managers, applications designed specifically to oversee a vendor's equipment. Basically, the vendors add a stripped-down Web server to the managed device, along with software that maps the data gathered by the device's SNMP agent to the server. It is then possible to perform a quick status check from any intranet location via a Web browser.

For the time being, browser-based managers are still fairly limited. The use of Java, with its built-in security mechanisms, has constraining side-effects. For example, Applets are not allowed to read or write files on a client's hard disk. Performance also remains an open issue. The delays associated with the conversion of SNMP (or other format) reports into HTML pages can be quite penalizing. Notwithstanding these current technical shortcomings, we envision the management of intranet networks and services through a uniform Web-based platform. By relying on the Web as the integrating interface, a unified presentation of all management information is provided, and a consistent style of invoking operations is followed.

Conclusion

Driven by the powerful combination of openness, cost-effectiveness, intuitive access to detailed information, and flexibility for customization, intranets are pervading all areas and activities of the corporate world. This movement of organizational networks toward intranet technology has far-reaching consequences on the whole enterprise structure and on its mode of operation. The enterprise memory, its nervous system, and its decision center are all embodied in one single structure, the intranet, which becomes the weakest link that can bring down the entire corporation. It is not certain that information technology managers and CEOs are devoting the appropriate care and effort to the management of the intranet that the situation requires.

In this article, we have emphasized the importance of all aspects of intranet management. We have shown that typical network management problems are just one facet of the issue, and that the management of intranet services is not to be overlooked. We have presented a management model and elaborated on management domains and policies. We have also reflected on an intranet management architecture that encompasses the communications and services aspects. Finally, we have shown how Web-based technologies can help provide an integrated intranet management platform.

References

[1] S. L. Telleen, *The Intranet Architecture*, Amdhal Corp., 1996.
[2] S. L. Telleen, *Intranets and Adaptive Innovation*, Amdhal Corp., 1996.
[3] W. Stallings, *Network and Internetwork Security—Principles and Practice*, IEEE Press, 1995.
[4] M. Hills, *Intranet Business Strategies*, John Wiley & Sons, 1996.
[5] P. Bodensiek, *Intranet Publishing*, QUE, 1996.
[6] T. J. Pincince, D. Goodtree, and C. Barth, "Network Strategy Service," *The Forrester Rep.*, vol. 10, no. 4, Mar. 1996; http://www.forrester.com.
[7] M. Andreessen *et al.*, "The Netscape Intranet Vision and Product Roadmap," Netscape Commun. Corp., 1996; available at http://www.netscape.com/comprod/at_work/white_paper/intranet/vision.html.
[8] W. Stallings, *SNMP, SNMPv2, and CMIP—The Practical Guide to Network-Management Standards*, Addison-Wesley, 1993.
[9] M. Autrata and C. Strutt, "DME Framework and Design," *Networks and Distributed Systems Management*, Morris Sloman, Ed., Addison-Wesley, 1994.
[10] ITU, "Principles for a Telecommunications Management Network," CCITT Rec. M.3010, Oct. 1992.
[11] G. Goldszmidt and Y. Yemini, "Evaluating Management Decisions via Delegation," *Proc. 3rd IFIP Int'l. Symp. Integrated Network Mngmt.*, Apr. 1993.
[12] R. Boutaba and S. Znaty, "An Architectural Approach for Integrated Networks and Systems Management," *ACM-SIGCOMM Comp. Commun. Rev.*, vol. 25, no. 5, Oct. 95.
[13] R. Wies, "Using a Classification of Management Policies for Policy Specification and Policy Transformation," *IFIP Conf. Integrated Network Mngmt. IV*, A. S. Sethi, Y. Raynaud, and F. Faure-Vincent, Eds., Chapman, 1995.
[14] Cisco, "Switched Management Migration Policy-Based Intranet Services," 1996; available at http://www.cisco.com/warp/public/734/cwswit/index.html.
[15] J. D. Moffet and M. S. Sloman, "Policy Hierarchies for Distributed Systems Management," *IEEE JSAC*, vol. 11, no. 9, Dec. 1993.
[16] D. Levi and J. S. Schoenwaelder, "Definitions of Managed Objects for the Delegation of Management Scripts," IETF Draft, Nov. 1996.
[17] K. El Guemhioui and R. Boutaba, "Webbification of Network Management," to appear in *Proc. NOTERE '97 Colloq.* (in French), Pau, France, Nov. 1997.
[18] WBEM Consortium, *The Web-Based Enterprise Management Initiative*, July 1995; available at http://wbem.freerange.com/.
[19] Java Management API, Sun Microsystems, 1996; available at http://java.sun.com/products/JavaManagement

Additional Reading

[1]Computer Associates, "Enterprise Management Strategy," 1997; available at http://www.cai.com/products/unicent/whitepap.htm.
[2] P. Rogers, "Publishing with World Wide Web Technology: Methodologies for the Internet and Intranets," *Imagic Commun.*, 1996; available at http://www.imagic.com.au/~magi/intra.htm.l
[3] M. Sloman, *Networks and Distributed Systems Management*, Morris Sloman, Ed., Addison-Wesley, 1994.

Biographies

RAOUF BOUTABA [M] (rboutaba@crim.ca) is currently an adjunct professor at the University of Montréal, Québec, Canada. He received an "Engineer" degree in computer science and engineering from the University of Annaba, Algeria, in 1988, and M.S. and Ph.D. degrees from the University of Paris VI, France, in 1990 and 1994, respectively. He was assistant professor at Evry University, France and technical leader in national and international projects including ESPRIT and RACE. His research interests include integrated network and system management, wired and wireless high-speed networks, and distributed and multimedia systems and applications. He is currently directing several research projects sponsored by the computer and telecommunication industry in these areas. He has served as general chair and co-chair of several international conferences, and as a guest editor of international journals.

KARIM EL GUEMHIOUI received M.S. and Ph.D. degrees in computer science and engineering from the University of Connecticut. He is currently a member of the research team in Telecommunications and Distributed Systems at the Computer Science Research Institute of Montreal. His research interests include object-oriented design approaches for parallel and distributed systems, reliable and high-performance distributed computing environments, and the application of Web technologies to network management. Dr. El Guemhioui was a Fulbright recipient in 1990.

PETRE DINI received a B.S. and an M.Eng. from Politechnic Institute of Timisoara, Romania, in computer engineering, and a Ph.D. in computer science from the University of Montreal. Until 1985, he worked as a project leader on the development of various industrial applications, including CAD/CAM, nuclear plant monitoring, and real-time embedded software in Romania. From 1985 to 1990, he was technical director and senior consultant developing enterprise manufacture networks. Since 1991 he has been involved in various Canadian projects related to formal techniques in object-oriented management applications for distributed systems, and to broadband services in multimedia applications, until early 1996. In 1996 he joined the Computer Science Research Institute of Montreal as a researcher on the Telecommunications and Distributed Systems team and is engaged in the specification and development of network management architectures. He has been a speaker at several international conferences and co-chaired the FIW '97 Workshop on Feature Interactions. His research interests are in automation of management systems, system reconfiguration under QoS constraints, feature interactions, pricing multimedia QoS mechanisms, and formalisms to specify and evaluate software architectures.