Directory Enabled Networks

May 17,2000

Kerem ERZURUMLU
Department of Computer Science and Engineering
Hacettepe University

Abstract

DEN, Directory Enabled Networks, are networks where users and applications interact in a controlled way with network elements and network services to provide predictable and repeatable services to users, while also strengthening security and simplifying provisioning and management of network resources. Initiated by Cisco and Microsoft, DEN initiative is supported widely in the industry area by many companies. The information model and base schema of DEN are derived from CIM and X.500, plus some new concepts. The model structure is object-oriented modeling. DEN uses LDAP to access, manage, and manipulate directory information.

1. Introduction

As Internet develops, it is getting more and more complex to manage a network. The information about the nodes, or devices, attached to a network is stored in a special purpose database called directory. Directory service is the physically distributed, logically centralized repository of infrequently changing data that is used to manage a computing environment.

Networks are becoming increasingly complex. There are different types of network elements, each running a potentially different set of protocols and services over possibly different media. As a result, a network has too many different directory services for network administrators/roots to successfully and easyly management. For example, there are operating system directories (both for NT and UN*X), RADIUS directories, DNS directories, DHCP directories, etc. Administrating all of these directories might be a big headache and time consuming, because of their different user interfaces, incompatible data formats, dunlicate datas and many other problems.

In May 7 1997, Microsoft and Cisco announced a letter of intent in which Cisco will license Active Directory from Microsoft for use in managing network infrastructure and to provide richer network services. Both parts will jointly develop extensions to Active Directory to integrate advanced management of network elements and services. In September 24 1997, Cisco and Microsoft announced an initiative and draft specification for directory enabled networks. This open, industry-wide initiative intents to help customers develop rich network application that will work with offerings from a variety of network and directory vendors. It will also allow service providers to simplify service delivery and provide new sets of services for their customers.

DEN is based on Microsoft's Active Directory. But also works under other directory protocols which are communicated with LDAP. As an example a small model of DEN on user management will be explained later.

2. What Is a Directory Enabled Network?

There can be two answers to this question. The first is the simple answer:

Simple Answer: A directory-enabled network is one where user profiles, applications, and network services are integrated through a common information model that stores network state and exposes network information. This information then enables bandwidth utilization to be optimized; it enables policy-based management; it provides a single point of administration of all network resources; and all this serves to lower total cost of ownership, and improves the services that end-users can rely on regardless of their physical location.

Technical Answer: A directory-enabled network is one where users and applications interact in a controlled way with network elements and network services to provide predictable and repeatable services to users, while also strengthening security and simplifying provisioning and management of network resources. The directory-enabled network uses directory services to store critical information to facilitate access, management, and search operations. Users, applications, and services can be abstracted through profiles. A *profile* is a template of attributes and behaviors that describe an object or a set of objects. Profiles can be applied to a single user or a group of users. Profiles provide a higher level of abstraction for important system components — group, service, and network — while still providing the ability to model and operate on the fundamental building blocks of user, computer, and device. Put another way, profiles tell the system what needs to be done, not the specific steps necessary to do it. *Policies* define desired behavior between two or more objects. It is important to note that policy is separate from enforcement or auditing. In a network, policies apply to a broad range of different services, such as configuration, routing and switching, access control, and usage of services such as encryption and QoS. Centralized policies are the key to overall management of the network. Today, implementing and enforcing consistent policy of any type across a corporation manually is an expensive, labor-intensive, and error-prone proposition. This is due to the inherent complexity of managing many inter-dependent features across many different types of network elements. The "Enhancing Networking through Integration with the Directory Service" specification defines a standard way of storing the policies and profiles (the schema) as well as an information model that defines the desired interaction between objects on the network. The directory also represents objects that consume these network resources, such as users and applications. This allows directory-enabled network elements and applications to discover and enforce policy at the point where resources are consumed. This enables this specification to control the implementation of policy at the group or user level; the administrator can then *personalize* the network (in terms of what services are available) for individuals and groups of users and devices.

2.1 Directory Versus Databases

A directory is a special purpose database that contains information about the various resources available on a network. A directory service is quite different from a general DBMS in that directory information is attribute-based more descriptive in nature. These attributes give specific information about various objects to the clients of the directory service.

Directory services are optimized to store information that is frequently read, but not frequently written. So, directories are aiming at maintaining static information, such as user name, email address, passwords, device configuration parameters.

Directories enables to use more than one server. The responsible server of o leaf can be another machine with is far away from the original root server machine. This distributed structure is adds advantaje to directories.

Rapid Internet growth over past years has created the need for more robust, scalable and secure directory services. DEN provides a new paradigm for using directory services where the directory is an authoritative, distributed, intelligent repository of information for services and applications.

2.2 Profiles

In DEN, users, applications, and services can be abstracted through profiles. A profile is a template of attributes and behaviors that describe an object or a set of objects. Profiles provide a higher level of abstraction for important system components, while still providing the ability to model and operate on the fundamental objects. Profiles just tell the system what needs to be done, not the specific steps necessary to do it.

2.3 Policies

In a distributed networking environment, simply managing individual devices is no longer sufficient. Network administrators need to define and manage policies to control the network and its resources in a distributed, yet logically centralized, manner. Directories are simply databases; they are not designed to collect information from multiple sources and then make a policy decision.

In general, policies define what resources a given resource consumer can use in the context of a given application or service. Technically, a policy is a rule that instructs a network node on how to manage requests for network resources. It is essentially a mechanism for encoding business objectives concerning the proper use of scarce resources.

3. DEN Base Schema

The schema of a directory defines the set of objects that can be created in that directory and the set of attributes that can be used to describe those objects.

The DEN schema consists of abstract base classes from which all other network-specific classes are derived. The base classes are refined by specialization from the basic model for representing network elements, services, consumers, etc. Figure 1 shows the functional structure of the DEN base classes, with key classes defined by CIM, X.500, and DEN listed separately.

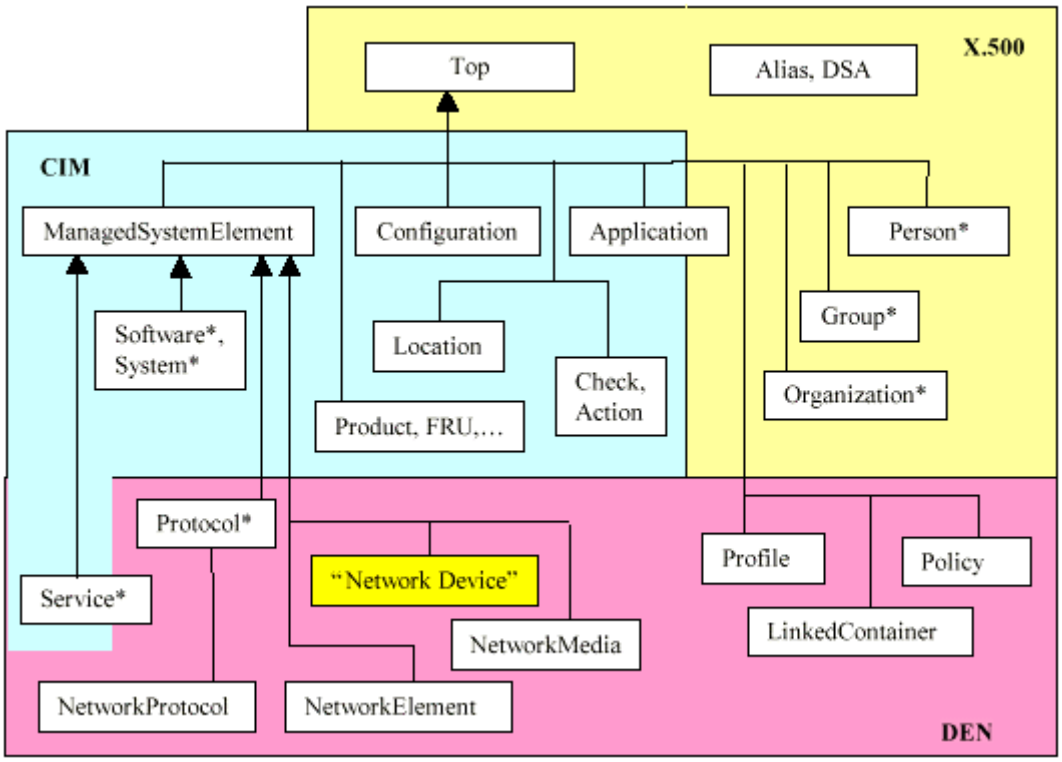

Figure 1. *Functional structure of the DEN base classes.*

DEN is the aggregation of concepts from the currently released version of the CIM specification (2.0), the currently released versions of the X.500 specification (1993 version), and a collection of new ideas. The new ideas build on the framework provided by CIM and X.500 in order to model network elements and services.

The details of the class hierarchy is beyond the content of this essay. Interested readers should refer to [3] for more details. Following is just a list of short descriptions of the base classes.

3.1 Overview of Base Classes Derived from X.500

- **Top**: Root of the directory tree.
- **Person**: Generic concept of a person, an employee, a person with a residence. DEN uses it as a client to bind network services to, or as owner/administrator of a device or a service.
- **Group**: Providing grouping constructs for users as well as devices.
- **Organization**: Business entity to which devices and services belong.
- **Application**: X.500 defines the ApplicationProcess and ApplicationEntity classes. DEN adds information so that these classes can be associated with network elements and services.
- **Alias, DSA**: Necessary entities for proper directory operation.

3.2 New DEN Classes

Enhanced and extended concepts defined by DEN:

- **NetworkService**: Root of the network service hierarchy.

- **NetworkProtocol**: Root of all network protocol classes.
- **Enhancements to PhysicalPackage and Card**: Extensions and enhancements to include the functionality required by network devices.
- **NetworkElement**: Logical aspects of a network element.

New concepts defined by DEN:

- **Policy**: Rule instructing a network node on how to manage requests for network resources.
- **Profile**: Template of attributes and behaviors that describe an object or a set of objects.
- **NetworkMedia**: Associating the particular media of a given interface with services that are running on it.
- **LinkedContainer**: Container class implementing a forward link.

Note that "Network Device" in the Figure 1 is not an actual class, but rather the abstraction of changes made to existing CIM classes to realize the physical characteristics of network devices.

4. LDAP (Light – Weight Directory Access Protocol)

The access protocol for DEN information is LDAP version 3. LDAP was designed to provide the most important functions of X.500 DAP, while making them much easier to implement in servers, and especially in clients. LDAP is specifically targeted at management applications and browser applications that provide read/write interactive access to directories. For detailed information about LDAP, please refer to RFC 2251 and other related RFCs (RFC 2252 - 2256).

5. An Example of DEN

The following scema is real. All the programs are writen and today they are working properly.

In a big hospital the patients' opreations are followed by computers with a client program. All data is stored on a database. All the billings are made by the records which are placed in database.

In this situation all workstations are Windows NT and because of the client program they can not be chanced with another operating systems. As a result there have to be a NT server to keep the passwords,DHCP info for workstations.

On the other hand, hence the NT server is not useful for internet/intranet deamons there have to be a second server which is UNIX. When a user is created on NT that user must have an e-mail adres and internet access. Adding the user by hand is the first solition. But then the password syncronation became a problem. It's bad luck that NT and UN*X does not use same directories for users.

The result is in DEN. Firstly a Directory server of Netscape is installed on UN*X. In the following step the programs of creating users, etc, is written by PHP. Then tool of Directory Syncronation for NT is used. Also a small program which generates /etc/passwd file is writen. After the all installation the NT server and UNIX server begin to share their passwords.

6. Conclusion

In my point of view directory based applications and management utilities will be the future of the network. Internet and local networking is getting more and more importance in nowadays. The management of the servers and local area network devices is getiing more and more complicated. So there must be a solution to simplfy the terible. DEN claims that it can solve the problems.

References

1. Cisco Systems, Inc., *Directory Enabled Networks (DEN) --Frequently Asked Questions*, 4.11.1997 ()

2. Semeria, Chuck & Fuller, Frank, *Directory-Enabled Networks and 3Com's Framework for Policy-Powered Networking*, 23.6.1998 (http://www.3com.com/technology/tech_net/white_papers/pdf/50066501a.pdf)

3. Tim Howes, et al, "*Understanding and Deploying Ldap Directory Services*," The MacMillan Network Architecture Series, 1999

4. Archie Reed, "*Implementing Directory Services; Microsoft Active Directory Novell NDS, Netscape NDS, Cisco/Microsoft Directory-Enabled Networks*," 1999

5. Nand Mulchandani, "*Ready For A Directory Enabled World*?" March 31, 1999

6. Cisco Systems Inc, "*Directory Enabled Networks*", Thu Jun 17 16:15:27 PDT 1999 (http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/diren.htm)

7. Cisco Systems Inc, "*Directory Enabled Networks, The Bible*", John Strassner, (http://www.ciscoexpo.ini.hu/cscden)

8. Microsoft Corporation, "*Policy Schemas For DEN*", (http://www.ietf.org/proceedings/98aug/slides/policy-bof-moore-slides-98aug)