Network Working Group
Request for Comments: 1308
FYI: 13

C. Weider
ANS
J. Reynolds
ISI
March 1992

Executive Introduction to Directory Services Using the X.500 Protocol

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard. Distribution of this memo is unlimited.

Abstract

This document is an Executive Introduction to Directory Services using the X.500 protocol. It briefly discusses the deficiencies in currently deployed Internet Directory Services, and then illustrates the solutions provided by X.500.

This FYI RFC is a product of the Directory Information Services (pilot) Infrastructure Working Group (DISI). A combined effort of the User Services and the OSI Integration Areas of the Internet Engineering Task Force (IETF).

1. INTRODUCTION

The Internet is growing at a phenomenal rate, with no deceleration in sight. Every month thousands of new users are added. New networks are added literally almost every day. In fact, it is entirely conceivable that in the future every human with access to a computer will be able to interact with every other over the Internet and her sister networks. However, the ability to interact with everyone is only useful if one can locate the people with whom they need to work. Thus, as the Internet grows, one of the limitations imposed on the effective use of the network will be determined by the quality and coverage of Directory Services available.

Directory Services in this paper refers not only to the types of services provided by the telephone companies' White Pages, but to resource location, Yellow Pages services, mail address lookup, etc. We will take a brief look at the services available today, and at the problems they have, and then we will show how the X.500 standard solves those problems.

2. CURRENT SERVICES AND THEIR LIMITATIONS

In the interests of brevity, we will only look at the WHOIS service, and at the DNS. Each will illustrate a particular philosophy, if you will, of Directory Services.

The WHOIS service is maintained by the Defense Data Network Network Information Center, or DDN NIC. It is currently maintained at GSI for the IP portion of the Internet. It contains information about IP networks, IP network managers, a scattering of well-known personages in the Internet, and a large amount of information related specifically to the MILNET systems. As the NIC is responsible for assigning new networks out of the pool of IP addresses, it is very easily able to collect this information when a new network is registered. However, the WHOIS database is big enough and comprehensive enough to exhibit many of the flaws of a large centralized database. First, centralized location of the WHOIS database causes slow response during times of peak querying activity, storage limitations, and also causes the entire service to be unavailable if the link to GSI is broken. Second, centralized administration of the database, where any changes to the database have to be mailed off to GSI for human transcription into the database, increases the turnaround time before the changes are propagated, and also introduces another source of potential error in the accuracy of the information. These particular problems affect to different degrees any system which attempts to provide Directory Services through a centralized database.

The Domain Name Service, or DNS, contains information about the mapping of host and domain names, such as, "home.ans.net", to IP addresses. This is done so that humans can use easily remembered names for machines rather than strings of numbers. It is maintained in a distributed fashion, with each DNS server providing nameservice for a limited number of domains. Also, secondary nameservers can be identified for each domain, so that one unreachable network will not necessarily cut off nameservice. However, even though the DNS is superlative at providing these services, there are some problems when we attempt to provide other Directory Services in the DNS. First, the DNS has very limited search capabilities. Second, the DNS supports only a small number of data types. Adding new data types, such as photographs, would involve very extensive implementation changes.

3. THE X.500 SOLUTION

X.500 is a CCITT protocol which is designed to build a distributed, global directory. It offers the following features:

* Decentralized Maintenance:

Each site running X.500 is responsible ONLY for its local part of the Directory, so updates and maintenance can be done instantly.

* Powerful Searching Capabilities:
  X.500 provides powerful searching facilities that allow users to construct arbitrarily complex queries.

* Single Global Namespace:
  Much like the DNS, X.500 provides a single homogeneous namespace to users. The X.500 namespace is more flexible and expandable than the DNS.

* Structured Information Framework:
  X.500 defines the information framework used in the Directory, allowing local extensions.

* Standards-Based Directory Services:
  As X.500 can be used to build a standards-based directory, applications which require directory information (e-mail, automated resources locators, special-purpose directory tools) can access a planet's worth of information in a uniform manner, no matter where they are based or currently running.

With these features alone, X.500 is being used today to provide the backbone of a global White Pages service. There is almost 3 years of operational experience with X.500, and it is being used widely in Europe and Australia in addition to North America. In addition, the various X.500 implementations add some other features, such as photographs in G3-FAX format, and color photos in JPEG format. However, as X.500 is standards based, there are very few incompatibilities between the various versions of X.500, and as the namespace is consistent, the information in the Directory can be accessed by any implementation. Also, work is being done in providing Yellow Pages services and other information resource location tasks in the Directory.

However, there are some limitations to the X.500 technology as it is currently implemented. One price that is paid for the flexibility in searching is a decline in the speed of the searching. This is because a) searches over a part of the distributed namespace may have to traverse the network, and some implementations cache all the responses before giving them to the user, and b) some early implementations performed search slowly anyway. A second problem with the implementations is that for security reasons only a limited amount of information is returned to the user; for example, if a search turns up 1000 hits, only 20 or so are returned to the user. Although this number is tunable, it does mean that someone with a big search will have to do a lot of work. The performance of the

Directory, while increasing rapidly in the last two years, is still not able to provide real-time directory services for such things as routing protocols. However, work is being done to speed up service.

The X.500 Directory is taking us closer to the day when we will indeed have the entire world on our desktops, and X.500 will help insure that we can find whom and what we need.

4: FOR FURTHER INFORMATION

For a more detailed technical introduction to X.500 and an extensive bibliography, see "Technical Overview of Directory Services Using the X.500 Protocol", by Weider, Reynolds, and Heker. This is available from the NIC as FYI 14, RFC 1309. For a catalogue of X.500 implementations, see "A Catalog of Available X.500 Implementations", ed. Lang and Wright. This is available from the NIC as FYI 11, RFC 1292.

5: SECURITY CONSIDERATIONS

Security issues are not discussed in this paper.

6: AUTHORS' ADDRESSES

Chris Weider
Advanced Network and Services, Inc.
2901 Hubbard, G-1
Ann Arbor, MI 48105-2437

Phone (313) 663-2482
E-mail: weider@ans.net

Joyce K. Reynolds
Information Sciences Institute
University of Southern California
4676 Admirality Way
Marina del Rey, CA 90292

Phone: (310) 822-1511
E-Mail: jkrey@isi.edu