# Techniques for automated Network Map Generation using SNMP


Glenn Mansfield, M. Ouchi, K. Jayanthi, Y. Kimura

Advanced Intelligent Communication
Systems Laboratories
6-6-3, Minami Yoshinari, Aoba-ku
Sendai 989-32, Japan.
Tel: +81-22-279-3310 FAX: +81-22-279-3640
e-mail: glenn@aic.co.jp

Kohei Ohta, Yoshiaki Nemoto

Graduate School of
Information Science
Aramaki Aza Aoba, Aoba-ku
Sendai 980-77, Japan.
Tel: +81-22-217-7140
e-mail: kohei@nemoto.ecei.tohoku.ac.jp



### Abstract

*Network configuration information is useful in producing a visual map of the network complete in all details. The visual map is an essential component for network management and operations. It is also possible to generate an inventory report of a network. The inventory report describes the nodes, networks, interfaces, addresses, protocols, speeds, etc. and is a valuable component for network planning and administration.*

*Unfortunately, network management is severely constrained in scope and effectiveness by the lack of any organized pool of network configuration information. In this work we present results of our efforts to develop tools and techniques for automatically and mechanically synthesizing network configuration related information from the Internet. These techniques, we believe, will be instrumental in generating the pool of network configuration information.*


## 1 Introduction

The growing and active interest in network management [GYM], which has concentrated mainly in the areas of fault and performance management on a local scale, is severely constrained by the lack of any organized pool of information about the network infrastructure itself.

Network configuration information, whether in graphical form or in report form, is an essential element for effective network planning, administration and managment[CMAN]. A visual map is necessary for an overview of the physical/logical network topology, to serve as an important input for management and administration of routes, traffic flow, network problems and policy and, as a pool of information for the public. A network inventory report is a valuable component for network planning and administration.

There are some sources of network related information which provide limited information of some particular aspect of the network (WHOIS[RFC 954],Domain Name System[DNS]. But these sources are very inadequate when considered for network management purposes.

## 2 The Network Map

Network configuration information, referred to as *network map* in the following, comprises of information about network objects. Gateways, routers, bridges, end-workstations, ethers, interfaces, etc. as well as networks themselves are network objects. The Map information will primarily cover the interconnections between the various network elements. It will also show properties and functions e.g. speed, charge, protocol, OS, etc. of the various network objects and the interconnections. The functions include the services provided by the network element. Other desirable information elements are policy related information, network name and address related information, network administration and management related information.

Other information that may be covered by the map are geometric and geographical. The geometric information describes how the map information will be displayed to a user. The geographical information describes the geographical location of the various network objects and can be used for showing the map in the context of a geographical map.

## 3 A framework for holding the Network Map

Since the scope of the map is global and the network itself is expanding, the *Network map* has certain inherent challenging issues to be tackled. The Network is huge and geographically distributed and as such spans several administrative and political areas. The Network and its configuration is controlled, managed and maintained in a distributed and autonomous manner.

In short, global network configuration information is unwieldy and growing continuously. It is impossible to service such information in a centralized fashion. So, a distributed database system is necessary. In this context, the X.500 Directory system [X.500-88] is an appropriate candidate on which the network map be implemented. The X.500 Directory is intended to be a very large and highly distributed database. It is structured hierarchically with entries arranged in the form of a tree in which each object corresponds to a node or an entry. Information is stored about an object as a set of attributes.

In [ND] a framework has been proposed for representing a communication network with all its related details and descriptions in the distributed X.500 Directory. [RFC 1608] contains the definitions of the various objects and attributes used for representing the Internet in the X.500 directory. Though the framework is ready, the major problems faced in deploying the framework are firstly to get the information there and then to keep it updated.

## 4 The *Map Generation problem*

The concept of layering has for all practical purposes hidden the network configuration details from users and applications. All decisions regarding switching and routing are taken care of at the networking level making it largely unnecessary for higher layer entities to know the network configuration. This has led to the present state where network configuration information is no longer available. The generation of a map of the Internet or, parts of it, is presently a non-trivial problem.

There are information services present that supply network related information. The WHOIS service of the various NICs in general offer the minimal registration information online. This includes Network - name, number, manager, primary & secondary nameservers, contact persons & addresses etc. The DNS service provides an online distributed database containing information about network name to address mapping and viceversa, mail exchangers, well known services, managers, etc. However, there is no place that in any manner provides information about the connectivity of the various network elements.

Network maps, wherever present, are manually generated. The problem with these maps is that in the context of the Internet, our target network, these maps become outdated and obsolete very fast. That is because of the rapid pace at which the Internet is changing and growing.

### 4.1 The Requirements

As a strategy to overcome this major problem of network map generation one has to think of alternatives that require minimal human intervention. Any plan that calls upon network operators or managers to deploy a server with the appropriate information or even to supply the requisite information is more likely to fail than not. This is more so because the incentives are not so obvious as was in the case of the ubiquitous DNS. The alternate strategies will have to scan for information that is present in the network itself. Any practical proposal for making a network map will have to be automated. This implies - that the required information is present *a priori* in some form. Further, the extraction of the information should not require new protocols as that would only increase the complexity of deployment.

One of the definitive sources for network configuration information is the network itself. The network-level entities must have the requisite configuration information which enables them to route the packets around the network. Therefore, network-level entities are a potential source of configuration information.

In the globally distributed network which comprises of network elements from diverse manufacturers, to extract network configuration information, standard management techniques will need to be employed. We have proposed the use of and experimented with the Internet Standard Simple Network Management Protocol (SNMP) to fetch configuration information from the various Standard Management Information Bases.

## 5 MIBs for Network Configuration Information

For purposes of routing a network is generally broken down in a hierarchical fashion. In the Internet there are the *Autonomous Systems* **AS** (in ISO jargon *Routing Domain*). The Internet is a collection of *Autonomous Systems*. In general the network level entities exchange configuration information with their peers and in the process gather enough information that enables them to chart the paths of packets along the networks. The information syntax and semantics differs depending on the implementation of the routing protocol and there several routing protocols deployed. Essentially there are two categories of routing protocols - one for interconnecting *Autonomous Systems* - the *exterior gateway protocols (EGP)* and - the other that runs within an *Autonomous System* - the *interior gateway protocols (IGP)*. Possibly the most widely deployed IGP is RIP[RFC 1388]. Notable among others are OSPF[RFC 1247]. These protocols are used for exchange of routing information among networks in a AS. Other routing protocols BGP[RFC 1267], IDRP[IDRP], etc. are used to exchange routing information among ASs. Our contention is that the entity realizing the routing protocol, be it RIP, OSPF or BGP, does have a picture of the network connectivity. A complete picture of the network can be generated by patching the pieces obtained from representatives of the different parts of the network.

The network configuration may be extracted from the network-layer entities using network management protocols by accessing the managed objects *(MO)* defined in the Management Information Base *(MIB)* for the respective entity. In the following we discuss some of the MIBs and their contents.

### 5.1 BGP-MIB information

The Border Gateway Protocol (BGP) is an inter-Autonomous System routing protocol. The primary function of a BGP speaking system is to exchange network reachability information with other BGP systems. This network reachability information includes information on the full path of Autonomous Systems that traffic must transit to reach these networks. The MIB that is used for controlling a BGP-3[RFC 1267] implementation are defined in [RFC 1269]. Apart from a few system variables, this MIB is broken into two tables: the BGP Peer Table and the BGP Received Path Attribute Table. The Peer Table reflects information about BGP peer connections, such as their state and current activity. The Received Path

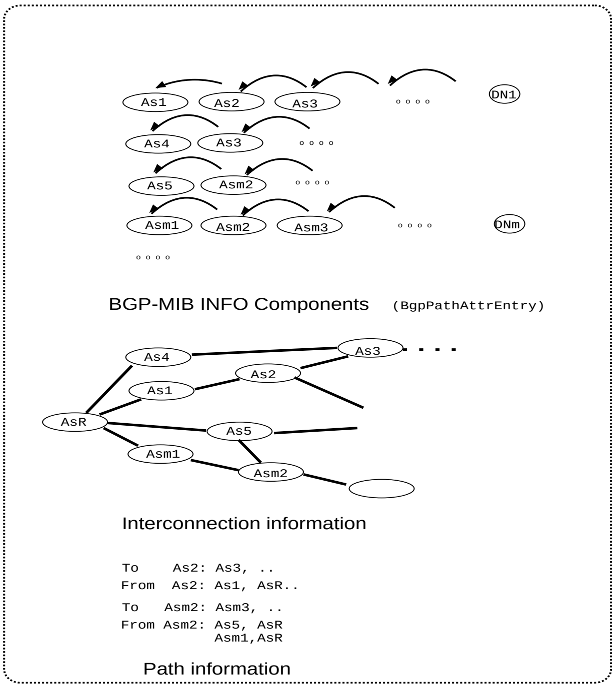


Figure 1: BGP-MIB information

Attribute Table contains all attributes received from all peers before local routing policy has been applied.

Of particular interest is the *bgpPathAttrASPath* which describes the set of ASs that must be traversed to reach the network. It describes the interconnections between the ASs and thus forms the basis of the AS-level Internet map. For example if the BGP-MIB contains a record that says that routing information about network N1 arrived at the BGP-router after traversing intermediate BGP-routers in Autonomous systems As1, As2, and As3, then the connectivity information synthesizer decides that the AS of the current BGP-router, which is the origin of the BGP-MIB, is connected to As1, which in turn is connected to As2, which in turn is connected to As3. And As3 contains the network N1. Apart from the interconnectivity information, it is also *learnt* that As2 is announcing to As3 the routing information from As1. This is the connectivity information.

## 5.2 OSPF-MIB information

OSPF is a link-state based routing protocol. It is designed to be run internal to a single Autonomous System.

Each OSPF router maintains an identical database describing the Autonomous System's topology. From this database, a routing table is calculated by constructing a shortest-path tree. The MIB that is used to manage an OSPF Version 2[RFC 1247] implementation is defined in [RFC 1253]. It consists, among others, MOs for the Area Data Structure, the Area Stub Metric Table and the Link State Database. The Area Data Structure describes the OSPF Areas that

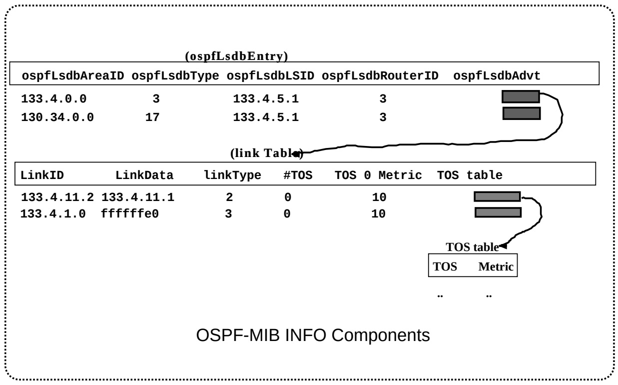


Figure 2: OSPF-MIB information

the router participates in. The Area Stub Metric Table describes the metrics advertised into a stub area by the default router(s).

Of particular interest is the Link State Database contained in the *ospfLsdbTable*. It contains the Link State Advertisements from throughout the areas that the host is attached to. The *Link State Advertisements* contain all the basic information necessary for drawing the network map of the area.

In figure 2, the router address and name is given by *ospfLsdbLSID*. The related link state details are given Link State Advertisement- *ospfLsdbAdvt*. The Link State Advertisement in turn contains of all the links from the specific router along with the costs for the various types of services. One piece of information that is missing is the information about the interface type. For this information it is necessary to refer to the interface table of the router - as is described in the next subsection.

## 5.3 MIB-II information

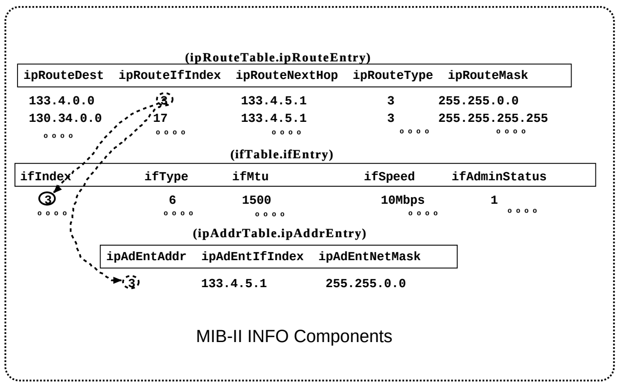


Figure 3: MIB-II information

The minimum information that must be available from a router is the MIB-II[RFC 1213]. This information is *sufficient* to draw the network map. Of course it involves examining all the routers in the domain for which the map needs to be drawn. Of particular interest among the various MIB-II tables are the

- *ifTable* containing information on the interfaces of the router.
- *ipRouteTable* containing the routing table of the router.
- *ipAddrTable* containing the router's addressing information.

The tables are interdependent and are looked up using the interface index as the key.

## 6 Synthesis of Configuration Information

In the following we describe a system which generates the network map and the network inventory report.

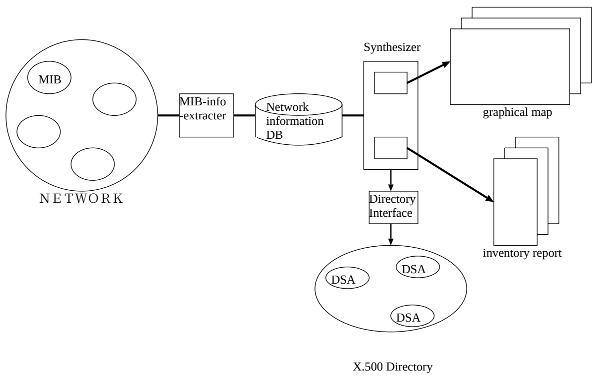


Figure 4: Configuration information synthesizer

The *MIB-info-extracter* is primarily an SNMP-based application that scans the appropriate MIBs of the network elements and generates the Network information DB. The *Synthesizer* has two components one generates a visual graphical map. The other generates an inventory report containing the system description, location, contact person, network type , address and protocols. The *Directory-Interface* is used to upload or update the information into the X.500 distributed directory.

## 7 Sample results

Table 1 shows the log of a run of the *MIB-info-extracter* which scanned the network elements in the domain *wide.ad.jp.* Figure 5 shows the map synthesized from the extracted Network information DB. This a top-level map showing the entire domain. More detailed maps are generated, too. For example figure 6 shows the detailed map of the *jp-gate.wide.ad.jp* network.

Performance figures of a prototype system is shown in Table 2 $\sim$ Table 4.

The inventory reports synthesized form the Network information DB are shown figure 7 and figure 8.

Table 1: Summary : hosts accessed by SNMP

```
*---------------------------
* SNMP queries sent  to: (32 + 1 + 16)
*       HostsProcessed:  49
*     Recd replies from:  32
*       Incomplete from:  1
*       No replies from:  16
*---------------------------
* Elements found-
*             Hosts : 32
*        Interfaces : 215
*          Networks : 410
*---------------------------
Gateway                              Comments
================================ ================
wnoc-fujisawa-proteon2           SNMPOK
wnoc-tokyo-cisco7                SNMPOK
wnoc-kyoto-cisco                 SNMPNORES
wnoc-fujisawa-dnx                SNMPNORES
wnoc-tokyo-cnx                   SNMPNORES
wnoc-tokyo-otemachi              SNMPOK
wnoc-tyo-ss2                     SNMPOK
wnoc-hac                         SNMPOK
wnoc-kyoto-cisco26               SNMPNORES
wnoc-tyo-satgw                   SNMPNORES
wnoc-tokyo-nss                   SNMPNORES
wnoc-spk                         SNMPOK
wnoc-tokyo-cisco2                SNMPOK
wnoc-spk-sat                     SNMPOK
wnoc-tokyo-cisco6                SNMPOK
wnoc-snd                         SNMPOK
wide-sfc-gw                      SNMPNORES
wnoc-fujisawa-cisco3             SNMPOK
wnoc-kyoto-cnx                   SNMPNORES
wnoc-fujisawa-cisco6             SNMPOK
wnoc-tokyo-wellfleet             SNMPNORES
jp-gate                          SNMPOK
us-entry                         SNMPOK
wnoc-tokyo-sinet                 SNMPOK
wnoc-fujisawa-cisco              SNMPOK
wnoc-kyoto-cisco2                SNMPOK
wnoc-kyoto-cisco25               SNMPNORES
wnoc-tokyo-cisco5                SNMPOK
wnoc-kyoto-iij                   SNMPOK
wnoc-fujisawa-netblazer          SNMPNORES
wnoc-tokyo-igs                   SNMPOK
wnoc-kyo-ss2                     SNMPOK
wnoc-snd-ss2                     SNMPNORES
wnoc-fujisawa-cisco2             SNMPOK
wnoc-fujisawa-cisco5             SNMPOK
wnoc-kyo-ss5                     SNMPOK
wnoc-tokyo-netblazer             SNMPNORES
wnoc-tyo-news                    SNMPNORES
wnoc-nara-cisco                  SNMPOK
wnoc-nara-cisco2                 SNMPOK
wnoc-tokyo-cisco                 SNMPOK
wnoc-hij-cisco                   SNMPOK
wnoc-fujisawa-yamaha1            SNMPNORES
wnoc-spk-cisco                   SNMPOK
wnoc-tokyo-cisco3                SNMPNORES
jp-entry                         SNMPOK
wnoc-sfc-ipc                     SNMPOK
wnoc-fujisawa-cisco4             SNMPOK
wnoc-tyo                         SNMPOK
```

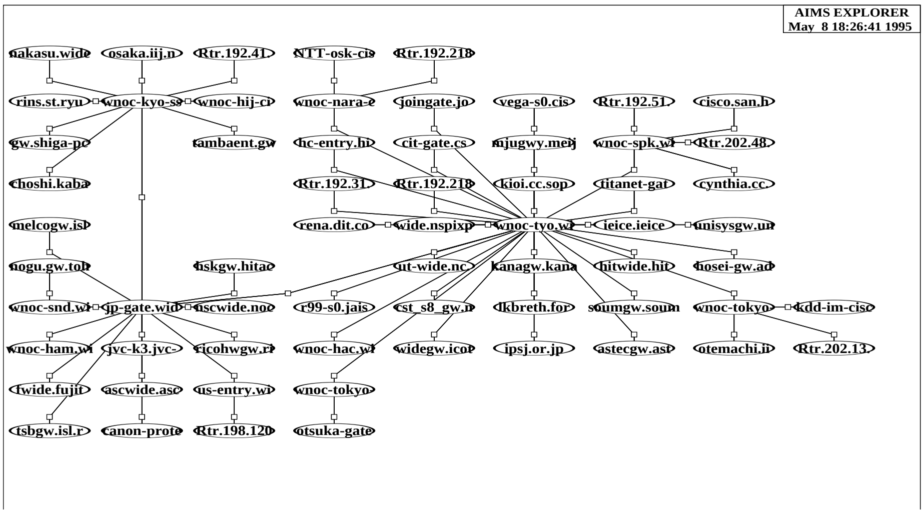


Figure 5: WIDE network map made from MIB-II

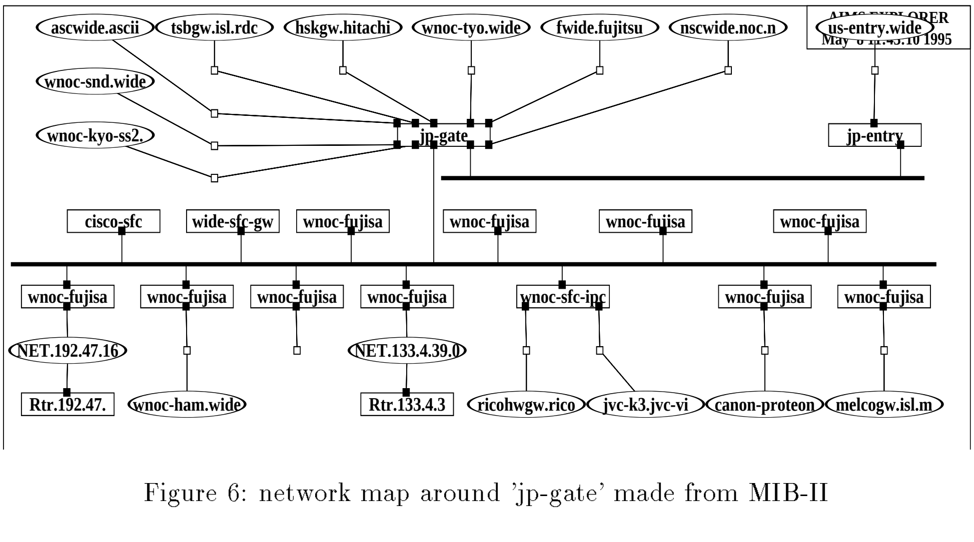


Figure 6: network map around 'jp-gate' made from MIB-II

# jp-gate

## jp-gate.wide.ad.jp

4BSD/ISODE SNMP

Fujisawa NOC, WIDE Project

Akira Kato <kato@wide.ad.jp>

| **RIP2** | **OSPF** | **BGP** |
|---|---|---|
| | | **Ver.4** |

| Address | Interface | Link | Remote address | Remote interface | Remote host |
|---|---|---|---|---|---|
| 133.4.11.1 | le0 | ether | 133.4.11.0 | | wide-fujisawa- |
| 133.4.1.1 | le1 | ether | 133.4.1.0 | | wide-jp-net |
| 133.4.2.1 | ptp0 | PTP | 133.4.2.2 | ptp0 | wnoc-tyo |
| 133.4.7.1 | ptp1 | PTP | 133.4.7.2 | ptp0 | wnoc-kyo-ss2 |
| 133.4.4.1 | ptp2 | PTP | 133.4.4.2 | ptp0 | wnoc-snd |
| --- | ptp4 | PTP | 202.249.12.2 | | hskgw.hitachi- |
| --- | ptp5 | PTP | 202.249.10.123 | | tsbgw.isl.rdc. |
| --- | ptp6 | PTP | 133.152.1.1 | | ascwide.ascii |
| --- | ptp7 | PTP | 133.160.28.1 | | fwide.fujitsu |
| --- | ptp8 | PTP | 133.179.213.31 | | nscwide.noc.ns |

Figure 7: Inventory report of jp-gate.wide.ad.jp

# wnoc-tyo

## wnoc-tyo.wide.ad.jp

4BSD/ISODE SNMP

Tokyo NOC, WIDE Project

Osamu Nakamura <osamu@cc.u-tokyo.ac.jp>

| RIP2 | OSPF | BGP |
|---|---|---|
| | | Ver.4 |

| | | | | |
|---|---|---|---|---|
| 133.4.3.2 / le0 | ether | 133.4.3.0 | | wide-tokyo-net |
| 133.4.2.2 / ptp0 | PTP | 133.4.2.1 / ptp0 | | jp-gate |
| --- / ptp5 | PTP | 133.156.1.1 | | rena.dit |
| --- / ptp6 | PTP | 133.123.1.1 | | lkbreth.foretu |
| 133.4.24.1 / ptp7 | PTP | 133.4.24.2 / ptp0 | | wnoc-spk |

Figure 8: Inventory report of wnoc-tyo.wide.ad.jp

Table 2: performance of making map (MIB-II)

| target domain | number of managed objects | number of connections | number of items in aims.cf file | CPU time (sec) |
|---|---|---|---|---|
| akita-u | 2000 | 300 | 60 | 20 |
| NTT | 7100 | 1800 | 45 | 43 |
| wide | 220000 ~ 270000 | 54000 ~ 65000 | 1250 ~ 1450 | 320 ~ 350 |

Table 3: performance of making map (BGP MIB)

| target domain | number of AS path | CPU time (sec) |
|---|---|---|
| wide | 2100 ~ 2200 | 5.3 ~ 8.9 |

| number of items in aims.cf | CPU time (sec) |
|---|---|
| 38 ~ 47 | 0.6 ~ 0.7 |

Table 4: performance of making map (OSPF MIB)

| target area | number of LSDB table | CPU time (sec) |
|---|---|---|
| spk, snd | 115 | 0.1 ~ 0.2 |
| tyo, jp-gate | 230 | 0.3 ~ 0.4 |

| number of items in aims.cf | CPU time (sec) |
|---|---|
| 7 ~ 11 | 0.4 ~ 0.5 |
| 170 ~ 180 | 4.1 ~ 4.2 |

## 8 Conclusion

We have presented results of our efforts to develop tools and techniques for automatically and mechanically synthesizing configuration related information from the Internet.

The attraction of the proposal lies in its simplicity. It uses existing mechanisms and protocols viz. SNMP network management protocols. The techniques are expected to have far reaching consequences in network operation and management. For the first time it will be possible to prepare a map of the whole Internet. A demonstration package is available at

*ftp://sh.wide.ad.jp/WIDE/papers/wg/softpage/map.tar.Z*

## References


[CMAN] G. Mansfield, K. Jayanthi, K. Higuchi, S. Noguchi. Configuration Management using the Directory Services. Proc of the National Conf. of the Information Processing Society of Japan, November 1992.

[DNS] Mockapetris, P.V. Domain names - implementation and specification. RFC 1035, November 1987.

[GYM] G.Mansfield et al. An SNMP-based Expert Network Management System. IEICE Transactions, August, 1992.

[IDRP] C. Kunzinger. draft-kunzinger-idrp-ISO10747-00.txt.*work in progress* April, 1994.

[ND] G. Mansfield, et.al. Mapping Communication Networks in the Directory. Computer Networks & ISDN Systems, Vol. 26, No. 3, November, 1993.

[RFC 1157] J. D. Case, M. Fedor, M. Schoffstall, J. Davin, "A Simple Network Management Protocol (SNMP)," May, 1990.

[RFC 1213] K. McCloghrie, M. Rose, "Management Information Base for Network Management of TCP/IP-based internets: MIB-II," March, 1991.

[RFC 1247] J. Moy. OSPF Version 2. August, 1991.

[RFC 1253] F. Baker, R. Coltun. OSPF Version 2 Management Information Base. August, 1991.

[RFC 1267] K. Lougheed, Y. Rekhter. A Border Gateway Protocol 3 (BGP-3). October, 1991.

[RFC 1269] J. Burruss, S. Willis. Definitions of Managed Objects for the Border Gateway Protocol (Version 3). October, 1991.

[RFC 1388] G. Malkin. RIP Version 2 Carrying Additional Information. January, 1993.

[RFC 1608] Johannsen, Th., G. Mansfield. Representing IP information in the X.500 Directory. March, 1994.

[RFC 954] Harrenstein, K., M.K. Stahl, E.J. Feinler. NICNAME/WHOIS. October, 1985.

[X.500-88] CCITT. The Directory - Overview of Concepts, Models and Services. Recommendations X.500 - X.521