GOSIP IMPLEMENTATION GUIDELINES

MLM-MU-91-71-0003

By Harrell J. Van Norman

I INTRODUCTION

GOSIP (Government Open Systems Interconnection Profile) is a subset of ISO's OSI protocol standards relevant to US Government operations. As a Federal Information Processing Standard (FIPS), GOSIP is required by law for all Federal agencies. Mandatory standards-based communications products are required when purchasing functionality equivalent to what is specified in GOSIP. This unprecedented requirement by the Federal government has caused considerable confusion concerning practical implementation of relatively immature and untested technologies.

Many organizations desire the advantages of GOSIP, but already have substantial investment in one or more proprietary network architectures. Is immediate cutover to GOSIP practical? If not, can an evolutionary migration to GOSIP be successful and beneficial? Can current SNA networks, DECnet networks, and PC-based LANs be merged into a larger, organization-wide network based on GOSIP? This paper examines these questions by discussing the following considerations:

1) INTRODUCTION - A Brief Historical Context, looking at GOSIP from the bottom up and Benefits from GOSIP, describing the benefits of GOSIP migration.

2) STATE OF THE INDUSTRY - reviewing where GOSIP is today

3) MIGRATION STRATEGIES - defining the necessary stages involved

4) IMPLEMENTATION ALTERNATIVES - contrasting different environments

5) IMPLEMENTATION APPROACHES - outlining differing technologies

6) OTHER CONSIDERATIONS - highlighting registration and security

A recommended migration strategy and practical approaches for implementation provide guidance and direction. These techniques include using mixed protocol stacks, dual protocol stacks, gateways, multiprotocol routers and bridges. Other implementation considerations such as name and address registration and security provisions are also discussed.

FROM STANDARDS BODIES TO PROTOCOL STANDARDS

The International Standards Organization (ISO) is a voluntary, nongovernmental, international agency comprised of standards institutions. It develops standards to facilitate international exchange of goods and services and promote cooperation in intellectual, scientific, technological, and economic activity. ISO, founded in 1946, has issued more than 5000 standards on everything from screw threads to solar energy, including a vast array of communications standards. ISO's US member is the American National Standards Institute (ANSI).

In 1978 a subcommittee on Open Systems Interconnection (OSI) formed to develop a general architectural reference model for distributed information systems. The OSI Reference Model provides a layered structure for connecting dissimilar end systems. Functionality is distributed into seven layers so no one layer is overly complex and the number of layers is kept to a minimum, making the architecture less complicated. The top three layers - Application, Presentation, and Session - are responsible for processing information, the middle layer - Transport - ensures proper delivery of the information sent, and the bottom three layers - Network, Data Link, and Physical - provide a vehicle for physically transferring information from one system to another. The seven layers with their functions are listed below.

7 - Application - Provides end-user access to satisfy user needs.

6 - Presentation - Provides data format and code conversion.

5 - Session - Sets up and ends interaction between end-users.

4 - Transport - Provides for data integrity between end-users.

3 - Network - Selects a route and directs data to end-users.

2 - Data Link - Transfers information to other end of the link.

1 - Physical - Transmits bit stream to transmission media.

US GOSIP - A PROTOCOL PROFILE

GOSIP is based on Stable Implementation Agreements for OSI Protocols reached at the National Institute of Standards and Technology (NIST) Workshop for Implementors of Open Systems Interconnection, commonly called the NIST OSI Implementors Workshop. Here, OSI functional profiles are produced by selecting options that must be supported and specifying necessary implementation details outside the scope of the standards. As the sponsor of the OSI Implementors Workshops, NIST is responsible for defining and updating GOSIP as officially voted on by vendors and Federal computer users at the quarterly NIST Workshop. The agreements help ensure compatibility between vendor developed OSI products. Each new GOSIP version is approved 12 to 18 months before mandatory enforcement begins, allowing users time to prepare for each stage of implementation.

GOSIP VERSIONS - CURRENT AND FUTURE

GOSIP Version 1 includes two application layer protocols: X.400 Message Handling System (MHS) and File Transfer, Access and Management (FTAM). Routing and reliable transfer of data is through a single transport protocol class 4 and a connectionless network layer protocol (CNLP). Version 1 also supports interconnecting the following lower layer network topologies for LAN/WAN networking: CCITT Recommendation X.25; Carrier Sense Multiple Access with Collision Detection (IEEE 802.3); Token Bus (IEEE 802.4); and Token Ring (IEEE 802.5).

GOSIP version 2 was adopted April, 1991 with the date for mandatory enforcement October, 1992. Version 2 includes all Version 1 functionality plus the following protocols: Virtual Terminal (telenet profile and forms profile), Office Document Architecture, Integrated Services Digital Network (ISDN), and End System to Intermediate System (ES-IS) routing protocol. A connectionless oriented transport protocol and a connection-oriented service network layer protocol were also added in GOSIP Version 2.

Version 3 & 4 are not set in stone, however, considerable long range planing has been done. X.500 Directory Services, Virtual Terminal (page & scroll profiles), MHS 1988 Extensions, FTAM Extensions, and Fiber Distributed Data Interface (FDDI) are scheduled for version 3, to be required about 4th quarter 1993. In 1995, Version 4 is anticipated to include Transaction Processing (to be used by agencies such as the Internal Revenue Service and the Department of Defense), Remote Data Base Access, Electronic Data Interchange (EDI), and possibly Synchronous Optical Network (SONET). Subsequent GOSIP versions will include those protocols developed by OSI that reflect progress made by vendors in providing products with new services useful to federal agencies.

BENEFITS FROM GOSIP

How will all of the protocols specified within GOSIP benefit its users? First, it helps when creating organization-wide networks based on different LAN and WAN technologies. GOSIP can reduce the complexity and expense of integrating a variety of diverse LAN and WAN architectures under a stable communications platform. Second, GOSIP gives the possibility to chose the right system for the right job.

In a small organization with limited communication requirements, a small Unix machine can act as the X.400 server. In larger organizations, multiple machines or machines with greater processing power can be used. Thirdly, the spheres of information flow can be increased and better directed using GOSIP networks. Timely information can reach those concerned and provide a sound basis for decision making. Fourth, GOSIP reduces expenses since it is a more efficient way to communicate, eliminating the need to invest in multiple networking technologies. Complete network transparency across multivendor systems is provided by GOSIP. Over the long-term, purchasing and installing GOSIP technology will minimize total investment costs and reduce conversion costs. Current GOSIP products are available at relatively competitive prices. GOSIP's major benefit is minimizing total investment costs through extended life cycles, reducing conversion costs, and increasing modularity.

Reducing the number of protocol converters needed, the number of gateways required, and installation times necessary for networked systems combine to generate significant savings. With a unified approach to multivendor networking, only one type of network training, documentation, and software will be necessary. Taken together, this translates to reduced communication costs compared to the costs involved in designing, installing, and maintaining multi-vendor proprietary systems. GOSIP enables users to focus their resources on solving business problems instead of establishing and reestablishing methods of interconnecting differing computer systems.

II STATE OF THE INDUSTRY

GOSIP, a requirement for Federal users, is increasingly being adopted by non-Federal government organizations, such as state governments and private industry that sees a need to improve their interoperability. Users are moving to GOSIP to take advantage of competition created by the Federal mandates for standards-based products. Many state governments depend on Federal government funding, therefore maintaining interoperability is highly desirable. Industry in general is beginning to see there is a lot to be gained by moving to GOSIP. Lower priced products due to increasing competition and multi-vendor interoperability are two key advantages luring many network mangers toward GOSIP.

Robust product offerings are still on the distant horizon. Suppliers of GOSIP compatible products have lagged behind user demands for fully certified and functional offerings. A pressing need for additional utilities, tools, and adequate access controls within GOSIP products exists today. Initial product offerings are unnecessarily complex and lack an easy user interface. Even more disappointing is the tremendous inefficiency in performance demonstrated by many early GOSIP products. Compliance is achieved at the sacrifice of end-user performance. Protocol over-head accounts for some of this inefficiency, however, vendors could design applications that are optimized for operational efficiency. In light of these inadequacies, some users are waiting for vendors to develop products that satisfy both compliance requirements and user performance needs.

GOSIP products merely meeting minimal NIST's requirements for interoperability and conformance testing have yet to significantly impact the market. Until GOSIP-compliant products demonstrate and certify functionality through the proper means of testing, interoperability cannot be assumed. Users are ready to adopt GOSIP functionality, especially in the areas of X.400 MHS for linking different electronic mail systems, Virtual Terminal for allowing users to mix and match different makes of terminals and host computers, Office Document Architecture for offering a base-level for the exchange of documents among diverse systems, and FTAM for file transfer.

Users readily see the advantages of being able to procure new services and equipment in an open environment and not be enslaved to a proprietary structure. Many agencies have already reaped the benefits of standards-based computing, however, the market has not responded with a wide variety of mature and usable products. Nevertheless, the availability of GOSIP-compliant products is a strong argument to move to GOSIP now. In the coming months vendor offerings of certified GOSIP functionality that address user performance needs will be available. The law of supply and demand will prevail and efficient, GOSIP compatible products will be available at competitive prices.

TESTING MECHANISMS

Two types of tests, conformance and interoperability testing, are used to determine if products conform to GOSIP requirements and can interoperate with other GOSIP implementations. Conformance certification testing laboratories are accredited through the NIST National Voluntary Laboratory Accreditation Program (NVLAP) for particular protocols. The Defense Communications Agency (DCA) is assisting NIST in conformance testing GOSIP products, accrediting NVLAP test laboratories, and registering products for GOSIP compliance. DCA's Joint Interoperability Test Center (JITC) is maintaining GOSIP publicly available product registers of GOSIP conformance and interoperability.

Once a GOSIP conformance testing laboratory is accredited for a particular GOSIP protocol it can run tests on a vendor's OSI products and determine their conformance to that US GOSIP protocol suite. Some of the accredited conformance testing laboratories and the protocols they are certified for are:

Bull HN in Phoenix, AZ for FTAM, MHS, Session, TP4 and CLNP;

CDA Inc. in Vienna, VA for X.25;

Control Data Corporation in St Paul, MN for MHS, Session, TP4, TP0, CLNP, and X.25;

Corporation for Open Systems in McLean, VA for FTAM, MHS, TP4, TP0, CLNP, X.25, and 8802.3;

Digital Equipment Corporation in Littleton, MA for FTAM, MHS, TP4, TP0, and CLNP;

Hewlett Packard in Cupertino, CA for MHS, Session, TP4, TP0, and CLNP;

IBM Corporation in Research Triangle Park, NC for X.25;

The National Computing Centre Ltd. in Manchester, England for FTAM, MHS, Session, TP4, TP0, and CLNP;

UNISYS in Paoli, PA for FTAM, MHS, TP4, TP0, and CLNP;

TITN-Alcatel Inc. in Pleasanton, CA for FTAM, Session, TP4, TP0, and CLNP.

Once a product has passed conformance tests they are ready to enter into the second phase of certification - interoperability testing. NIST has created the OSINET network for vendors who wish to certify their products in pair-wise interoperability testing. Here vendors can test GOSIP products against other implementations without having to negotiate with each vendor separately or buy the vendor's product and test in-house. GOSIP requires both conformance and interoperability testing to ensure compliance with the protocol standards. Commercial companies, however, are not under this restriction but are strongly cautioned against procuring non-certified products and assuming interoperability.

HOLES IN THE SPECS

Although GOSIP provides a stable basis for multi-vendor interoperability, it doesn't include functionality that many network managers feel is essential. Additionally, GOSIP imposes restrictions on the functionality it does provide, making it less attractive to non-govermental organizations. Lack of definition for Application Program Interfaces (APIs) and the absence of X.500 Directory Services are seen as major drawbacks.

GOSIP does not define specific API's that should be used to access the various layer services. All vendors provide API's to some layers in the protocol suite but it is up to the purchaser to specify which services are needed. Several vendors including AT&T, DEC, IBM and HP are working on creating consistent API's for use with Presentation, Transport, and CONS. The Network Management Forum is doing the same thing for X.400 MHS. Companies should be sure to ask vendors to specify what API's they support and at what layers.

Version 1 and 2 do not have any directory service specifications. Network managers wondering if they need a standards-based directory services must realize it will be essential in the long run. Almost all vendors supply some form of directory services product, whether it is X.500 or a proprietary solution. Even in the absence of the requirement, companies are strongly encouraged to verify X.500 is part of all product plans from their vendors. If a company plans on external electronic messaging or developing object-oriented applications in which network elements are defined and managed as separate objects, then X.500 is critical.

Why is X.500 so important? It is the directory service standard for OSI networks and the key to success for X.400 MHS, and FTAM. It is also the only worldwide standard for electronic mail directory, meaning non-OSI networks can benefit from X.500. This grand scheme for a global telecommunications directory will be distributed across many networks but will provide accessibility to all users, subject to security constraints. X.500 considers network users as objects, representing either people, computer processes, or anything else an organization wants to define. The practical outcome will be interconnections between directories maintained by organizations, public carriers, and information service providers. Like voice directories, public X.500 directories will come in white and yellow page versions. White pages directories identify organizational structures of departments and divisions complete with employee names. Yellow pages, in contrast, organize businesses by categories and provide minimal information. Because of security restrictions, X.500 directories will primarily be yellow page directories, allowing maximum access to limited information, such as sales and customer service numbers, cutting down on junk e-mail to individuals.

III MIGRATION STRATEGIES

Migration means moving from today's proprietary networking environments to standards-based GOSIP compliant systems. It requires careful planning whether the end result is a purely GOSIP network or one retaining significant proprietary elements within an GOSIP-based architecture. Since most organizations have considerable investments in existing ADP systems that need to be preserved whenever possible, it is not financially reasonable to move all systems to GOSIP in one all-encompassing changeover. In addition, initial GOSIP compliant products are immature and lack adequate user considerations. Furthermore, the GOSIP means of testing is still under development and does not fully guarantee interoperability. In light of these considerations, a phased deployment of GOSIP throughout an organizations computing systems is recommended.

Although GOSIP demonstrations have helped toward actual implementations, large-scale installations and market acceptance do not happen overnight. A phased approach to actual implementation is necessary to handle the accumulation of knowledge, the build-up of technology, and the migration from existing systems to multi-vendor networking. This avoids costly and potentially catastrophic disruptions of network services and minimizes interruptions to daily network operations.

No single plan can best define the migration of all proprietary networks to GOSIP, however successful transition requires a common organizing principle: a long-term, organization-wide plan. A GOSIP transition plan must be well designed, accurate, and thorough,

including more than just linking networks and nodes. However, before any planning can begin, the personnel who will plan and coordinate the migration to GOSIP must be identified. Furthermore, information about the migration must be publicized to everyone involved in the transition. Good communication helps to ensure an orderly and efficient transition.

There are four recommended steps toward the eventual implementation of GOSIP in an organization. Bypassing any of these steps places a greater burden on subsequent phases.

1) GOSIP Pilot Installation
2) Creating GOSIP Subnets
3) Extended Coexistence
4) GOSIP Dominance

Pilot Installations

During the pilot phase the primary objective is to gain experience with constructs unique to GOSIP. Of particular importance is acquiring familiarity with naming, addressing, and registration of GOSIP objects. This formality of registration and management of naming and address structures is new to most organizations. Experience with name and address structures greatly facilitates design and implementation of hierarchical structures for an entire organization. Without the opportunity to gain some experience on a smaller scale, integrating GOSIP into production computers could present significant challenges.

The pilot phase allows OSI networks to be installed in isolated environments, in controlled circumstances, and serve the purpose of familiarization with new technology. This is sometimes referred to as

parallel networks, where multiple autonomous networks are supported concurrently. As initial pilots are successfully completed, additional network components and applications can be added. For example, once an X.25 backbone is verified operational, begin to add X.400 pilots to test their utility in the network. Pilot projects can grow in this manner into a full functional network offering parallel services and capabilities to that provided by the proprietary network. The main drawback to continued extension of a pilot phase into a fully operational parallel network is high communications costs caused by duplication of network functions and redundant network management. These pilot networks contribute to the knowledge build-up necessary to enter the second migration phase of creating GOSIP Subnets.

GOSIP Subnets

The second phase of GOSIP deployment involves creating one or more GOSIP subnets and integrating those subnets into the existing multivendor networks. These GOSIP networks are no longer in isolated controlled environments, but are becoming fully integrated into a portion of an organization's communication structure. This is sometimes referred to as the departmental strategy, where GOSIP implementations are limited to selected departments or subnets. These specific departments or subnets can utilize the GOSIP capabilities while not placing a burden on the communications backbone. Proprietary standards are still the primary vehicle for most communications, however, GOSIP is being integrated into specific production environments as technology implementations will allow. Application gateways are the primary means for interfacing between proprietary communications/applications and GOSIP communications/applications.

Extended Coexistence

The third stage involves expanding number the subnets where GOSIP is implemented, moving toward a phase of extended coexistence. During this stage organizations create GOSIP-only networks, replacing functionality that previously only proprietary networks could. Compatibility with older networks is assured through multi-protocol routers, encapsulation techniques, or gateway processors; ensuring that existing cabling plants can be utilized by both older proprietary protocols and the new GOSIP-based networks. Increasing numbers of subnets implement GOSIP as their primary communications protocols during this phase.

GOSIP Dominance

The final stage of GOSIP migration is the eventual dominance of GOSIP networks. Here, GOSIP replaces proprietary networking architectures as the industry accepted means of multi-vendor communications. Older proprietary networks become subnets to the GOSIP backbone. Figure X illustrates these four phases of migration from solely proprietary network architectures to GOSIP dominance.

Migration Plans

As stated earlier, proper planning is essential for effective transition from proprietary communications networks to GOSIP. Organizations need to appoint GOSIP migration coordinators to assist collecting data about the network, such as audits and network drawings, and identify any unique technical requirements, constraints, security considerations, testing, etc. Migration plans must be developed for each organization which employ a phased approach of moving from proprietary networks to GOSIP.

These migration plans need to include: schedules for various transition phases with start dates, milestones and completion criteria; GOSIP training; documentation development and review; replacement hardware and software ordering and installation; and pilot testing and verification.

Auditing your network to gather vital operational data is the first step of this migration process. Classes of hardware and software must be identified; circuit types, hardware types and revision levels must also be noted. Replacement hardware and software components must be identified and ordered. Implementing GOSIP requires identifying four areas of responsibility: Acquisition Authority, Protection Authority, Name Registration Authority, and Address Registration Authority. All Federal agencies should identify individuals for each area of responsibility.

Most organizations have individuals performing comparable duties as Acquisition and Protection Authorities. However, Name and Address Registration Authorities are effectively new requirements and responsibilities to support GOSIP. These Authorities are identified and described below.

Acquisition authorities are responsible for issuing procurement requests for GOSIP standard-based applications operating over networks using GOSIP standard-based protocols. The acquisition authority also must specify performance requirements as a function of the source end system, the destination end system, and the communications links, subnetworks, and intermediate systems between the two end systems.

Protection Authorities are necessary within GOSIP to define protection rules for an agency's security data. Security requirements for systems implementing GOSIP are identified and specified in the procurement document by the protection authority.

Address Registration Authorities are responsible for assigning and registering addresses used to identify specific components of the network. GOSIP's network addressing scheme is intended to uniquely identify each end system in the network in order to route data to it.

Name Registration Authorities are the individuals responsible for registering objects within the globally unique identifiers for OSI objects. This level of authority also may be delegated to lower organizational layers.

The timing of GOSIP transitions - when and how long - has considerable flexibility. The process and duration of transition varies depending on the size of the network, current hardware configurations, and the effectiveness of transition planning. The larger the network the longer it will generally require to complete the GOSIP transition.

IV IMPLEMENTATION ALTERNATIVES

There is a distinction between achieving GOSIP compliance for new systems that will only interact with other GOSIP systems and achieving GOSIP compliance for new or existing systems that need to communicate with systems that are not GOSIP compliant. In both cases, the preferred approach is to procure commercially supported products that have been certified for GOSIP compliance through both conformance and interoperability testing.

NEW SYSTEMS COMMUNICATING ONLY WITH GOSIP

The recommended solution for new systems communicating exclusively with other GOSIP compliant systems is to buy fully certified GOSIP compliant products. Users are encouraged to consult with suppliers to gain assurances that future GOSIP functionality will be supported in addition to the current version. GOSIP functionality that has been adopted but is in the 12 to 18 month waiting period prior to mandatory enforcement should be obtained if available or specified for future product upgrades. An example is differences within X.400 MHS; the 1984 standard adopted by version 1 uses a different Network Service Access Point (NSAP) Address Structure than the 1988 standard that is specified in version 2. It is important that products are upgraded to support the most current GOSIP version to maintain full compatibility with other end systems.

NEW SYSTEM COMMUNICATING WITH NON-GOSIP

In most operating environments, new systems will be required to communicate with both non-GOSIP, existing proprietary systems and with GOSIP networks. This results from requirements for all new systems to acquire GOSIP compliant capabilities when available, but still needing to interoperate with existing non-GOSIP systems. In addition, some new systems do not have commercially available GOSIP compliant products, such as CRAY supercomputers, therefore are limited to interoperate with existing non-GOSIP systems. In these environments implementing application level gateways are often the best solution.

EXISTING SYSTEM COMMUNICATING WITH GOSIP

Existing systems using proprietary communications protocols need to migrate to GOSIP to complete an organizations full transition to open, interoperable networking environments. During the later stages of GOSIP migration, existing systems will need to implement GOSIP communications capabilities. As GOSIP replaces proprietary networking as the industry accepted means of multivendor communications, existing proprietary networks will need to implement GOSIP functionality. As in the case of new systems needing to communicate with non-GOSIP, existing systems can often achieve GOSIP interoperability best through the effective use of gateways.

V IMPLEMENTATION APPROACHES

To obtain GOSIP benefits, various transition approaches can be used, and in some cases a combination of strategies is most appropriate, depending on existing networks, business and technical goals, or even customers profiles - commercial enterprise vs. governmental agency.

APPLICATION GATEWAYS - DUAL STACK

A gateway is a system that translates back and forth between two or more protocols. Lower level gateways (level three or below) are implemented in hardware to gain speed, whereas application gateways are software implementations used to gain flexibility and provide advanced services such as electronic mail or transparent file access across many different communications architectures. Dual stack, application gateways are useful vehicles for achieving interoperability between GOSIP and non-GOSIP compliant systems. Typically a single host processor manages a dual stack by containing two full communications protocol stacks. When data is received at a dual stack, application layer gateway, it is processed up the stack of the protocol associated with the incoming data. It then performs the necessary translation between application protocols and transmits the data using the protocols of the target system. For example, IBM's PROFs or DEC's All-in-one can be mapped to GOSIP's X.400 MHS. DECnet's initial GOSIP offering for VMS uses a dual stack implementation. Dual stack translation requires significant processing time and resources, so this approach is best suited for store and forward applications where response time is not critical, such as X.400 MHS or file transfer service. For example, a TCP/IP FTP to OSI FTAM gateway would allow TCP/IP users to send files to users on a OSI network.

The application gateway is ideal for phased implementations that minimize communications disruptions since they remain transparent to users. The specialized application gateway software runs above the application layer of both protocol stacks handling the format and protocol conversion, such as DEC All-in-one to X.400 MHS. Several companies specialize in gateway products: Interlink Corp. has been very successful in developing gateway technology to link DECnet and SNA networks; The Wollongong Group, Inc. provides TCP/IP protocol stacks for systems ranging from IBM-PCs to CRAY supercomputers; and Retix provides a low-cost application gateway for connecting dissimilar electronic mail systems with X.400 MHS. Application gateways are limited to the specific applications and protocol they support. This drawback tends to proliferate gateways, for example, a large network with 21 different e-mail packages would require 400 gateways (20 x 20).

Converting to a single, consistent base, such as X.400 MHS, dramatically reduces the number of gateways needed. Here using the gateway for conversion from proprietary applications to a GOSIP standard protocol offers significant advantages. For example, this approach takes each individual mail package: DECnet All-in-one, SNA PROFs, TCP/IP SMPT, etc. and converts them to the X.400 MHS protocol. The X.400 MHS data can then be shared among the various proprietary applications via the gateways. This limits the number of gateways to the number of proprietary applications, for example, the large network with 21 different e-mail packages now only requires 21 gateways rather than 400. Limiting the number of gateways required also greatly reduces cost and network overhead, while still maintaining a transparent user interface.

MULTIPLE PROTOCOL ROUTING AND BRIDGING

This strategy consists of a single computing system concurrently supporting multiple, coexisting protocols. For networks where it is impossible to standardize on a single protocol, the multiple protocol strategy offers an attractive solution. Examples of multiple protocol stacks include multiprotocol LAN routers simultaneously supporting OSI, TCP/IP, and DECnet communications protocols or LAN bridges tying two or more physically different LANs into one logical LAN. Essentially, this method allows multiple types of peer-to-peer connections within a given backbone network: TCP/IP to TCP/IP, GOSIP to GOSIP, DECnet to DECnet, and peer-to-peer SNA connections.

This strategy is most commonly seen in LAN internetworking environments using routers from Cisco, Wellfleet, Proteon, and others. However, most of these backbone nodes use proprietary protocols between nodes and only speak to like equipment. A more advanced approach is to use GOSIP-based internetworking routers and bridges that use GOSIP standard internodal ES-IS protocols. The multiprotocol routing and bridging strategy allows sharing of communications facilities and processing power among the multiple networks, thus reducing costs. As a result an organization can continue to operate its existing LAN networks while introducing new GOSIP applications. By establishing GOSIP capabilities while preserving existing networks and applications, multiple protocol stacks support a gradual integration of GOSIP into an existing environment. However, these solutions can be limited to a small network configuration and may not be appropriate for a larger organization-wide solution.

MIXED PROTOCOL STACKS

Mixed protocol stacks combine part of one protocol stack and the rest from another stack. Mixed protocol stacks, not supported in GOSIP, are either bottom-up or top-down. Bottom-up transitions substitute GOSIP lower layer protocols, such as X.25, for proprietary networking protocols. This provides connectivity between computing systems, not application interoperability. With the bottom-up approach, transition to GOSIP occurs in lower layers of the model, so existing applications remain unchanged. Since most vendors support connections to X.25 networks, diverse, multi-vendor equipment is accommodated. Using this method may save line costs through the sharing of a common industry standard network for most applications.

Top-down transitions implement GOSIP applications over an existing network such as TCP/IP or SNA. For example, FTAM and X.400 MHS can be transmitted over SNA networks, allowing users to receive the advantages of proven transport networks plus access to GOSIP applications. Top-down transition makes sense when GOSIP is a relatively small fraction of the total networking environment, however, as the number of GOSIP applications increases network performance may degrade. This does not permit interoperability between GOSIP and proprietary applications. Even GOSIP applications in a mixed top-down stack are not interoperable with pure stack GOSIP applications without gateways.

Dual stack application layer gateways offer more flexibility than mixed stacks without cumbersome limitations. Costs of dual stack application layer gateways do not differ significantly from mixed stack implementations. In light of these considerations is is usually advantageous for organizations to focus on application gateways.

VI OTHER CONSIDERATIONS

ADDRESS REGISTRATION

The Network Layer oversees end-to-end physical transfer of data, freeing higher layers from dependance on the physical network topology, such as ethernet, token ring, token bus, FDDI, X.25, ISDN, etc. These physical network topologies are referred to as subnetworks. Higher layers are isolated form the physical subnetwork through a logical network address scheme called Network Service Access Point (NSAP) addresses. These NSAPs identify destinations for data transmissions irrespective of the physical subnetwork. For example, a particular network can be assigned a new subnetwork address and still use the same NSAP address.

Describing the operation of the Network Layer helps to understand NSAP addresses and how information is routed from one user to another. For example, if user A wants to send data to user B then a protocol data unit is built by the sending protocols in stack A and transmitted to the receiving protocols in stack B. The remote user B is conceptually attached to a point, called a Network Service Access Point (NSAP), identified by an NSAP address. Thus, NSAP Address B identifies NSAP B and similarly NSAP Address A identifies NSAP A. NSAP addresses are relatively stable, globally unique identifiers of open systems. NSAP addresses have a structure composed of two parts. The first part is called the Initial Domain Part (IDP) and the second is the Domain Specific Part (DSP). The IDP identifies a high level registration authority and format for that class of NSAP addresses. The IDP itself consists of two parts, the Authority and Format Identifier (AFI) and

the Initial Domain Identifier (IDI). NIST is the GOSIP authority to administrator NSAPs and has been assigned the IDI value of 0005 under AFI 47. NIST defined the structure of the DSP and delegated the task of assigning all DSP addresses under its jurisdiction to the General Services Administration (GSA). The DSP has seven different fields that are described and illustrated below.

The first DSP field is the Format Identifier (DFI). GOSIP Version 1 had a format identifier of 1, but Version 2 slightly changed the DSP format, so it was assigned a format identifier of 2. Therefore, GOSIP Version 2 NSAPs have 47,5,2 as the first 3 identifiers.

The next field is the Administrative Authority and it identifies who's responsible for the organization of the subsequent fields. Each agency within the federal government has been assigned a value for their respective Administrative Authority. The DOE, for example has been assigned the hexadecimal value A. The third DSP field is reserved for future use to encode further levels of routing information and is now always assigned the hexadecimal value F, so for all DOE organizations GOSIP Version 2 NSAP addresses begin with 47,5,2,A,F.

Routing Domain, the fourth DSP field, is used to specify an area for the purpose of routing, namely a set of End Systems and Intermediate Systems that operate according to the same routing procedures. Each organization's address registration authority applies for unique routing domain addresses. As a recommendation, organizations should request different NSAP routing domains when two end systems are too far apart to be connected by a LAN. Therefore, many organizations will only need one Routing Domain address specific to their location.

The next two NSAP fields are assigned by the individual organization's Address Registration Authority, similar to how telephone numbers or serial numbers are assigned. The Area field identifies a unique subdomain, like IBM systems or DEC systems, followed by the End System field. The End System uniquely identifies a system (ES or IS) within an Area, similar to network node numbers. Format, value, structure, and meaning of these fields is left to the administrator's discretion. The Address Authority assigns unique NSAP identifiers to each end computer system, for example an IBM system might be assigned 47,5,2,A,F,1,1,1, where a DEC AOS system could be 47,5,2,A,F,1,2,1 and another DEC system 47,5,2,A,F,1,2,2. The deeper the heiarchical address tree, the more overhead is required to maintain it. The last NSAP address field is NSAP Selector, identifies a direct user of the Network Layer service. This is usually a Transport entity. However, it can be used to identify direct users of the network service as well.

NAME REGISTRATION

GOSIP Name Registration Authorities are responsible for assigning unique object identifiers. In X.400 MHS, the objects are people and organizations, so Originator/Recipient Names (O/R Names) of people and organizations are assigned. This allows computers to accept mail addressed to valid users (SMITH) and reject those packets addressed to unidentified objects (SMUTH). In FTAM, the objects are various types of data, therefore a list of valid classes of file structures are used to screen input data according to predefined codes. Data codes are defined according to an organizations needs, such as MSWord, 123, Freelance, and Excell, or FD for Financial Data, Ml for Materials List, and PS for Product Specifications. If files with unidentified types were attempted to be transferred between systems, errors would result.

Fundamental guidelines for name registration include insuring names carry useful information and they are kept as short and practical as possible. It is worth noting, a namespace is not linked in anyway to address or routing information. Furthermore, X.500 is still under development, so X.400 MHS names are not coupled today with the directory services naming conventions. Attempts to produce names consistent with the X.500 specification is a beneficial long-term strategy.

SECURITY

While the term "Open Systems" implies that users of such systems intend that the system be open to others, the users always want to provide access to such systems only to authorized users for authorized purposes. Systems that process sensitive or vulnerable data, especially classified data, must be protected from a wide variety of threats. Security services are that capability provided to communicating open systems that ensures Authentication, Access Controls, Data Confidentiality, Data Integrity, and Non-Reproduction. Security mechanisms are the techniques to provide Encipherment, Digital Signatures, Access Control, Data Integrity, Authentication Exchange, Traffic Padding, Routing Control, and Notarization. Security services and mechanisms to support secure transfer of information are being developed internationally and domestically but will take considerable time. Data labeling is required for many security related services and is defined as GOSIP's Basic Security Option. This option contains two subfields, Classification Level and the Protection Authority Flag. The Extended Security Option is left to the definition of each community of users.

VII SUMMARY

Since GOSIP has been mandated for all federal agencies, the question of whether or not to migrate to open systems is not "if" but "when". The federal government saw the many benefits from GOSIP, lower system costs, greater vendor competition, easier support and network administration. We are living in an internetworking age, a time when connectivity with diverse, multi-vendor networks is essential. GOSIP will be the primary vehicle for adopting the networking technology of the future century.

Moving to open, interoperable networks from close proprietary systems doesn't happen overnight. The proprietary systems didn't magically appear and neither will GOSIP compatible systems. A well planned migration strategy is the first and most important step. The plan should include the four phases of initial pilot projects, GOSIP subnets, extended coexistence, followed by GOSIP dominance. This process takes time but will permit necessary networking expertise and skills to increase with each subsequent phase of the migration.

Application layer gateways will provide the primary means for GOSIP migration. Gateways will begin to open our closed networks to the world of interoperability with minimal impact to operational systems. Adoption of GOSIP makes good sense and it will save not just cents but significant long-term resources over current approaches.

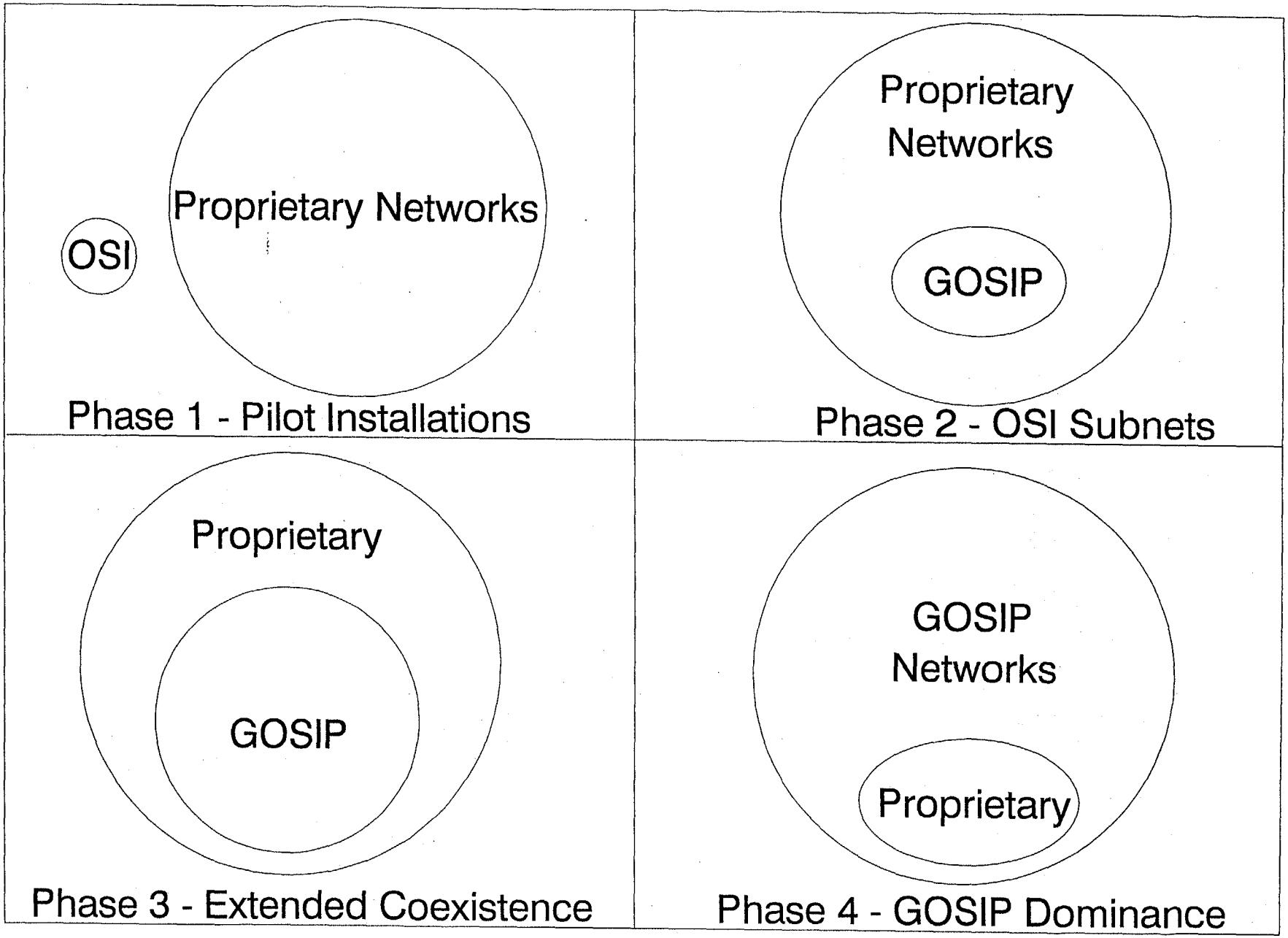
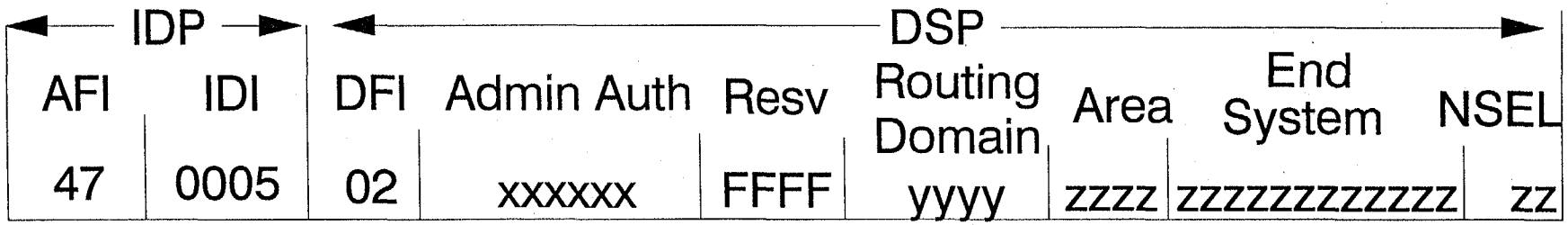


Figure 1. Four Phases of GOSIP Migrations

NSAP Address Structure

GOSIP Version 2



xx - Assigned For Each Federal Agency
yy - Assigned For Each Organization
zz - Assigned Within Each Organization

Figure 2. NSAP Address Structure for GOSIP Version 2