# GOVERNMENT OPEN SYSTEMS INTERCONNECTION: PROFILE IN PROGRESS

**Kevin L. Mills**

**The emergence of Open Systems Interconnection protocols, as specified within the U.S. Government Open Systems Interconnection Profile (GOSIP) Federal Information Processing Standard (FIPS), provides both an opportunity for, and a means of achieving, interoperability within multi-vendor networks. The GOSIP can easily benefit inexperienced users, yet provides the flexibility to serve more sophisticated users. The standard mandates specifications that will be met by a multitude of vendor products, with initial offerings already available. While meeting a useful set of initial networking needs, the FIPS will evolve to include new applications, improvements to the initial applications, new network technologies, and major new functions. GOSIP will permit government agencies to gain better control over their computer network procurements, accruing greater and greater cost savings as the number of government computer networks increases.**

*Mills* is chief of the Systems and Network Architecture Division of the National Computer Systems Laboratory at the National Institute of Standards and Technology. His division is responsible for GOSIP. He established the OSI Protocol Performance Research Program at NIST, which resulted in successful international collaboration among government, industry, and academic institutions to evaluate and enhance the performance of OSI protocols.

## INTRODUCTION

Computers are everywhere within modern society and the technology to send information between computers is ready to be employed. Soon the need to send information between large subsets of the growing number of computers will provide the push required to make data communications as ubiquitous as computers. The technology exists today in the form of local area networks (LANs), programmable branch exchanges (PBXs), and public data networks (PDNs). Reasonably high speed exchange of information across a variety of geographical ranges and organizational boundaries can be achieved. The limiting factor need no longer be the technology of the voice telephone network or the lack of physical interconnection between private data networks.

In 1979, the National Institute of Standards and Technology, NIST (formerly the National Bureau of Standards), established a program to create a set of standards for communicating information between computers manufactured by different suppliers. Along with an increase in the number of computers, NIST foresaw an increase in the variety of devices, resulting from three factors: 1) users making purchasing decisions without need to adhere to a company policy, 2) users requiring special capabilities available from a limited number of vendors, and 3) company regulations designed to encourage competitive procurements.

The intent of the NIST is to match the standards to products that vendors can be encouraged to build. The encouragement is derived from basing the NIST-established U.S. governmentwide standards upon

international standards for Open Systems Interconnection (OSI). Thus, a company building products for the U.S. government market can, presumably, meet the requirements of a world market. Basing U.S. government standards upon international standards has resulted in a substantial time lag, but has increased the probability that vendors of data communications products will meet the standards.

The first international OSI standards—Transport and Session—were completed in 1984. As early as 1983 it was clear that the emerging OSI standards would not lead to immediate development of interoperable products because the standards included incompatible options, classes, and subsets, and failed to make some hard implementation choices. With encouragement from major vendors, the NIST established in 1983 a series of workshops for implementors of OSI products. The workshops, open to all interested participants, focus on refining the OSI standards to reach a set of implementable and interoperable agreements. The decisions reached are documented in the OSI Implementor Agreements.

In 1988 the NIST issued the first Federal Information Processing Standard (FIPS) for OSI.[1] The FIPS is based upon the stable agreements document from the NIST-hosted workshop for implementors of open systems.[2] The FIPS includes the technical details necessary to specify exactly what a vendor must provide. These details are known as the U.S. Government Open Systems Interconnection Profile (GOSIP).[3]

## What Is GOSIP?

The GOSIP is a technical specification that permits a procuring agency to tell potential vendors what protocols are required to satisfy the agency's needs for interoperable data communications. It defines a set of mandatory protocols to support certain applications operating over a set of standard network technologies. Applications currently include file transfer, access, and management (FTAM) and electronic mail. Technologies include the Institute of Electrical and Electronic Engineers (IEEE) LANs 802.3, 802.4, and 802.5 and the Consultative Committee on Telephone and Telegraph (CCITT) Recommendation X.25 for a public data network (PDN) interface.

The number of applications and technologies supported by the GOSIP will grow over time and will likely include remote terminal access, office document interchange, directory services, transaction processing, integrated services digital network (ISDN), and the fiber distributed data interface (FDDI).

The GOSIP is a powerful document that can be viewed on a simple or sophisticated level. In the simplest use, the GOSIP enables users to request standard applications operating over standard networks. By requiring adherence to the GOSIP specifications, the user can purchase equipment from a variety of vendors that will connect to a LAN or PDN and achieve interoperable transfer of files and electronic mail.

On a more sophisticated level, the GOSIP permits the interconnection of several standard networks into an internetwork and facilitates the operation of a reliable end-to-end service across that internetwork. The same GOSIP-specified applications interoperate over a single GOSIP network or a GOSIP internetwork.

While these points fulfill the goals of the GOSIP, a sophisticated user can quickly see additional advantages. For example, non-standard network technologies can readily be incorporated within the structure of a GOSIP-compliant internetwork to provide a uniform, reliable, interoperable end-to-end service to support GOSIP applications. As another example, user-unique applications not supported or mandated by the GOSIP can be implemented to use the transport service defined by the GOSIP.

In summary, the GOSIP permits users to procure standard applications operating over standard networks without limiting selection to a single vendor's product line. Further, the GOSIP allows construction of internetworks of global scope while retaining the desired property of multi-vendor interoperability. Finally, all of this is accomplished through an architecture that allows sophisticated users to incorporate non-standard networks and applications. These and other appropriate topics are covered in detail in the GOSIP Users Guide.[4]

### Important Properties of GOSIP

Companies should be aware of several important properties of the GOSIP that set it apart from a traditional federal standard. The GOSIP is based upon a set of implementor agreements developed by users and vendors of OSI products who attend a series of workshops hosted by the NIST. With past Federal Information Processing Standards (FIPS), the NIST has tended to make refinements of international standards on its own. OSI standards are so comprehensive in scope that considerable expertise is needed to reach intelligent refinements of the standards, and considerable room exists for honest technical and economic disagreement. Given the NIST objective of standard products rather than product standards, the establishment of the open workshop forum seemed the best means for reaching the necessary refinement of OSI standards. Thus, GOSIP specifies details reached through an open

process operated by potential users and suppliers of GOSIP-compliant products.

A second material quality of GOSIP is that it specifies data communications protocols that are part of available products or products already under development. The first OSI Transport layer products appeared in 1984, coincident with the June National Computer Conference. The first OSI internetwork products appeared in 1985, coincident with the November AUTOFACT demonstration. OSI electronic mail products became widely available starting in 1987 following a demonstration at the 1986 Hannover Fair in Germany. The first GOSIP-compliant file transfer products were announced in 1988. In general, a full array of GOSIP-compliant products were available following the June 1988 Enterprise Networking Event in Baltimore, and the number of vendors offering products and the capabilities of each offering increased significantly before mandatory application of the GOSIP FIPS in August 1990.

A third characteristic of the GOSIP is the cooperation leading to the document. The GOSIP was authored by a group of government representatives from nineteen federal agencies. This approach is intended to ensure that the FIPS meets the requirements of as many federal users as possible. As a related property the GOSIP states, with the first version, that there are known requirements for which OSI protocols are not presently available. For each such requirement a plan and time are given for including a solution in the document.

A fourth property of note is the adoption of the GOSIP as an experimental co-standard by the Department of Defense (DoD) prior to publication of the FIPS.

Once the FIPS was published the DoD cited the GOSIP as a full co-standard with the existing DoD military standard protocols. The GOSIP is the DoD's sole mandatory interoperable protocol standard as of 15 August 1990.

This seemingly bold move by the DoD can be attributed to three factors: 1) the DoD has long understood the advantages of nonproprietary, interoperable protocol standards and adopted their own such standards in 1982; 2) the DoD contributed substantially to the development of the GOSIP, ensuring that the DoD needs are met; and 3) the DoD understands the potential economic benefits of adopting commercial standards where they meet the DoD requirements. DoD leadership in the adoption and use of the GOSIP sends a strong signal to the vendor community that a large segment of federal users will be requiring the GOSIP protocols.

A final significant attribute of the GOSIP is its relationship to the Manufacturing Automation Protocols (MAP) and the Technical and Office Protocols (TOP), backed by General Motors and Boeing Computer Services, respectively. The MAP and TOP 3.0 specifications are largely based upon the same implementor agreements as the GOSIP. In fact, in the areas where MAP, TOP, and the GOSIP intersect they specify that products meeting one profile will interoperate with products meeting either of the others. And the area of intersection is quite large indeed. Thus, a vendor building products for one of the represented markets is likely to achieve marketability in the others. This carefully crafted relationship between MAP, TOP, and the GOSIP is intended to provide additional economic incentive to vendors to build interoperable OSI products.

These important properties reflect the effort underlying the GOSIP. Combined resources of vendors and major users, applied since 1983, are resulting in an unusual opportunity to generate demand and supply simultaneously, for the economic benefit of both users and suppliers of data communications products.

## Evolution of GOSIP

In the initial FIPS, the GOSIP defines a minimal but useful set of applications and other services. This will encourage users to start buying and vendors to start selling. Addenda are planned to increase the functionality of the GOSIP as quickly as possible. The authors of GOSIP are committed to maintaining upward compatibility such that adding new functions to the document will not lead to incompatibility with the initial version.

The GOSIP FIPS refers to a complex set of functions requiring the use of best judgment on the part of the GOSIP authors, rather than adherence to a rigid schedule of revisions and addenda. It will be expanded over the next few years as some of the advanced requirements are included.

## The Challenges Ahead

The promulgation of data communications profiles, such as GOSIP, provides a first step toward creation of a successful marketplace for interoperable, multi-vendor networking products. Users will buy GOSIP products and vendors will sell them; however, four challenges must be met to ensure a GOSIP market that grows as fast and large as possible. The first challenge is creating effective, economical, and technically credible test policies and procedures for GOSIP. The second challenge is stimulating strategic and tactical planning within federal agencies, which is necessary to implement the provisions of GOSIP. The

international standards for Open Systems Interconnection (OSI). Thus, a company building products for the U.S. government market can, presumably, meet the requirements of a world market. Basing U.S. government standards upon international standards has resulted in a substantial time lag, but has increased the probability that vendors of data communications products will meet the standards.

The first international OSI standards—Transport and Session—were completed in 1984. As early as 1983 it was clear that the emerging OSI standards would not lead to immediate development of interoperable products because the standards included incompatible options, classes, and subsets, and failed to make some hard implementation choices. With encouragement from major vendors, the NIST established in 1983 a series of workshops for implementors of OSI products. The workshops, open to all interested participants, focus on refining the OSI standards to reach a set of implementable and interoperable agreements. The decisions reached are documented in the OSI Implementor Agreements.

In 1988 the NIST issued the first Federal Information Processing Standard (FIPS) for OSI.[1] The FIPS is based upon the stable agreements document from the NIST-hosted workshop for implementors of open systems.[2] The FIPS includes the technical details necessary to specify exactly what a vendor must provide. These details are known as the U.S. Government Open Systems Interconnection Profile (GOSIP).[3]

## WHAT IS GOSIP?

The GOSIP is a technical specification that permits a procuring agency to tell potential vendors what protocols are required to satisfy the agency's needs for interoperable data communications. It defines a set of mandatory protocols to support certain applications operating over a set of standard network technologies. Applications currently include file transfer, access, and management (FTAM) and electronic mail. Technologies include the Institute of Electrical and Electronic Engineers (IEEE) LANs 802.3, 802.4, and 802.5 and the Consultative Committee on Telephone and Telegraph (CCITT) Recommendation X.25 for a public data network (PDN) interface.

The number of applications and technologies supported by the GOSIP will grow over time and will likely include remote terminal access, office document interchange, directory services, transaction processing, integrated services digital network (ISDN), and the fiber distributed data interface (FDDI).

The GOSIP is a powerful document that can be viewed on a simple or sophisticated level. In the simplest use, the GOSIP enables users to request standard applications operating over standard networks. By requiring adherence to the GOSIP specifications, the user can purchase equipment from a variety of vendors that will connect to a LAN or PDN and achieve interoperable transfer of files and electronic mail.

On a more sophisticated level, the GOSIP permits the interconnection of several standard networks into an internetwork and facilitates the operation of a reliable end-to-end service across that internetwork. The same GOSIP-specified applications interoperate over a single GOSIP network or a GOSIP internetwork.

While these points fulfill the goals of the GOSIP, a sophisticated user can quickly see additional advantages. For example, non-standard network technologies can readily be incorporated within the structure of a GOSIP-compliant internetwork to provide a uniform, reliable, interoperable end-to-end service to support GOSIP applications. As another example, user-unique applications not supported or mandated by the GOSIP can be implemented to use the transport service defined by the GOSIP.

In summary, the GOSIP permits users to procure standard applications operating over standard networks without limiting selection to a single vendor's product line. Further, the GOSIP allows construction of internetworks of global scope while retaining the desired property of multi-vendor interoperability. Finally, all of this is accomplished through an architecture that allows sophisticated users to incorporate non-standard networks and applications. These and other appropriate topics are covered in detail in the GOSIP Users Guide.[4]

### Important Properties of GOSIP

Companies should be aware of several important properties of the GOSIP that set it apart from a traditional federal standard. The GOSIP is based upon a set of implementor agreements developed by users and vendors of OSI products who attend a series of workshops hosted by the NIST. With past Federal Information Processing Standards (FIPS), the NIST has tended to make refinements of international standards on its own. OSI standards are so comprehensive in scope that considerable expertise is needed to reach intelligent refinements of the standards, and considerable room exists for honest technical and economic disagreement. Given the NIST objective of standard products rather than product standards, the establishment of the open workshop forum seemed the best means for reaching the necessary refinement of OSI standards. Thus, GOSIP specifies details reached through an open

process operated by potential users and suppliers of GOSIP-compliant products.

A second material quality of GOSIP is that it specifies data communications protocols that are part of available products or products already under development. The first OSI Transport layer products appeared in 1984, coincident with the June National Computer Conference. The first OSI internetwork products appeared in 1985, coincident with the November AUTOFACT demonstration. OSI electronic mail products became widely available starting in 1987 following a demonstration at the 1986 Hannover Fair in Germany. The first GOSIP-compliant file transfer products were announced in 1988. In general, a full array of GOSIP-compliant products were available following the June 1988 Enterprise Networking Event in Baltimore, and the number of vendors offering products and the capabilities of each offering increased significantly before mandatory application of the GOSIP FIPS in August 1990.

A third characteristic of the GOSIP is the cooperation leading to the document. The GOSIP was authored by a group of government representatives from nineteen federal agencies. This approach is intended to ensure that the FIPS meets the requirements of as many federal users as possible. As a related property the GOSIP states, with the first version, that there are known requirements for which OSI protocols are not presently available. For each such requirement a plan and time are given for including a solution in the document.

A fourth property of note is the adoption of the GOSIP as an experimental co-standard by the Department of Defense (DoD) prior to publication of the FIPS.

Once the FIPS was published the DoD cited the GOSIP as a full co-standard with the existing DoD military standard protocols. The GOSIP is the DoD's sole mandatory interoperable protocol standard as of 15 August 1990.

This seemingly bold move by the DoD can be attributed to three factors: 1) the DoD has long understood the advantages of nonproprietary, interoperable protocol standards and adopted their own such standards in 1982; 2) the DoD contributed substantially to the development of the GOSIP, ensuring that the DoD needs are met; and 3) the DoD understands the potential economic benefits of adopting commercial standards where they meet the DoD requirements. DoD leadership in the adoption and use of the GOSIP sends a strong signal to the vendor community that a large segment of federal users will be requiring the GOSIP protocols.

A final significant attribute of the GOSIP is its relationship to the Manufacturing Automation Protocols (MAP) and the Technical and Office Protocols (TOP), backed by General Motors and Boeing Computer Services, respectively. The MAP and TOP 3.0 specifications are largely based upon the same implementor agreements as the GOSIP. In fact, in the areas where MAP, TOP, and the GOSIP intersect they specify that products meeting one profile will interoperate with products meeting either of the others. And the area of intersection is quite large indeed. Thus, a vendor building products for one of the represented markets is likely to achieve marketability in the others. This carefully crafted relationship between MAP, TOP, and the GOSIP is intended to provide additional economic incentive to vendors to build interoperable OSI products.

These important properties reflect the effort underlying the GOSIP. Combined resources of vendors and major users, applied since 1983, are resulting in an unusual opportunity to generate demand and supply simultaneously, for the economic benefit of both users and suppliers of data communications products.

## Evolution of GOSIP

In the initial FIPS, the GOSIP defines a minimal but useful set of applications and other services. This will encourage users to start buying and vendors to start selling. Addenda are planned to increase the functionality of the GOSIP as quickly as possible. The authors of GOSIP are committed to maintaining upward compatibility such that adding new functions to the document will not lead to incompatibility with the initial version.

The GOSIP FIPS refers to a complex set of functions requiring the use of best judgment on the part of the GOSIP authors, rather than adherence to a rigid schedule of revisions and addenda. It will be expanded over the next few years as some of the advanced requirements are included.

## The Challenges Ahead

The promulgation of data communications profiles, such as GOSIP, provides a first step toward creation of a successful marketplace for interoperable, multi-vendor networking products. Users will buy GOSIP products and vendors will sell them; however, four challenges must be met to ensure a GOSIP market that grows as fast and large as possible. The first challenge is creating effective, economical, and technically credible test policies and procedures for GOSIP. The second challenge is stimulating strategic and tactical planning within federal agencies, which is necessary to implement the provisions of GOSIP. The

third challenge is adding functions to later versions of GOSIP to provide directory services, dynamic routing, security, transaction processing, and electronic data interchange. The fourth challenge is fostering and successfully pursuing international collaboration in functional standards, procurement profiles, and testing. Beyond these four challenges lies the next horizon: integrated, interoperable network management.

The NIST GOSIP work plan is aimed at meeting the four challenges outlined here and at preparing for the network management challenges of the future.

### Challenge 1: GOSIP Test Policy and Procedures

Acquiring complex, computer-based systems is difficult. Usual industry practice involves formal buyer sign-off for such systems only after user acceptance tests are completed. User acceptance tests evaluate the proper function and performance of the system against user requirements. Today, complex computer systems are often implemented using components based on standards. Acceptance of such systems must not only evaluate function and performance, but also conformance to standards. When the standards apply to data communications, acceptance must also consider evaluation of interoperability with other system components implementing the standards. Thus, incorporation of data communications standards such as GOSIP into computer system acquisitions results in a need to evaluate conformance and interoperability in addition to the usual criteria of function and performance.

To assist buyers incorporating GOSIP into system acquisitions, timely, effective, and efficient tools are required for evaluation of conformance, interoperability, function, and performance. The tools envisioned by NIST are policies, procedures, and techniques, which should be in place by the date GOSIP is mandated for U.S. government procurements.

To serve as effective tools for establishing GOSIP conformance and interoperability of GOSIP-compliant systems, the policies, procedures, and techniques must be technically credible, must be accepted by vendors and buyers, must provide assurance of interoperability, and should serve as a basis for international recognition of national testing. Efficient tools will aid vendors during product development and will minimize the testing cost passed on to buyers. The NIST, in cooperation with major U.S. government users, is developing a GOSIP Conformance and Interoperability Testing and Registration FIPS.[5] The NIST, in collaboration with the Corporation for Open Systems (COS), will "exercise" the proposed procedures. The results of those trials will figure prominently in revisions prior to issuing the document as a FIPS.

The present plan is to require two phases of GOSIP testing and to facilitate an optional third phase. The first phase of testing will establish conformance to the standard. Upon successful completion of conformance testing a vendor will be required to establish interoperability with a GOSIP reference implementation (provided that NIST can identify such an implementation). Successful completion of this interoperability phase of testing establishes credentials for marketing the product as GOSIP-conformant. The optional third phase of testing will enable vendors to conduct bilateral interoperability tests, recording the results in publicly accessible databases. These testing phases should give buyers the necessary tools to establish conformance and interoperabilty of offered GOSIP-conformant products. For a complete discussion of these issues see the U.S. GOSIP Testing Program.[6]

### Challenge 2: Strategic and Tactical Planning

The GOSIP presents agencies an opportunity to take control of burgeoning incompatible computer equipment by establishing a long-term, strategic direction with tactical steps. The challenge is creating the awareness of this opportunity within affected agencies and transferring the knowledge necessary to seize the opportunity.

The establishment of an enterprisewide internetwork is a large job requiring leadership and planning by some technically competent group within an organization. In many organizations the proliferation of computers and local networks has occurred outside the control of any central management group; thus, a diversity of equipment has already been bought and installed. Every organization now faces, or soon will, the problems resulting from rapid buying of incompatible systems. The GOSIP presents an opportunity for agency management to assert some control over procurement, and can set a foundation for evolution to an effective interoperable set of networks of computers within the agency.

The single most important strategic element for an agency is a clear and definitive policy concerning adoption of the GOSIP. Such a policy serves several goals. First, a clear and definite signal is sent to operating components of the agency that a future networking direction has been set. The operating units can then begin to seriously plan for a migration, knowing that departmental backing is assured. Second, computer and network suppliers are put on notice that the agency is going in the direction of the GOSIP. The suppliers can then reorient their marketing strategies appropriately.

Having announced a clear policy, an agency should require that each affected operating unit prepare

a migration or transition plan indicating the time goals and mechanisms for implementing the policy. Each operating unit is likely to face a unique situation, so individual plans must consider special requirements of the operating unit. Intelligent planning for, and adoption of, the GOSIP will pay dollar benefits over the long term. But it is unrealistic to expect an operating unit to adopt the provisions of GOSIP at an inappropriate point in the life cycle of its systems. Rather, adoption of the GOSIP should be coordinated with plans for replacing major computer systems. A useful example is the Department of Defense—a large user of networks and communicating computers.

The DoD issued a policy memorandum establishing GOSIP as a co-standard with existing DoD standard protocols. In August 1990, GOSIP became the sole mandatory standard within the DoD. As a tactical first step the DoD issued a model OSI implementation plan and required services and agencies in the DoD to create specific implementation plans.

Several independent DoD operating units are already procuring GOSIP products to gain operational experience, and others are specifying GOSIP in requests for proposal. Still other units are permitting vendors to offer either GOSIP or DoD protocols. In addition, over the next few years the Defense Data Network backbone will move toward complete use of the GOSIP protocols.

The DoD transition is eased by the fact that a policy of standard, non-proprietary, interoperable protocols has existed since 1982. Not only is movement to GOSIP consistent with existing DoD policy, but interoperation between existing DoD systems and new GOSIP-style systems simply requires gateways between the two protocol suites. Thus, an existing policy mandating a standard set of network protocols for the DoD makes rapid evolution to the emerging FIPS possible.

The model DoD OSI implementation plan establishes a method of interworking between existing systems and new systems based on GOSIP. In support of this approach, the NIST developed and tested, in cooperation with industry, gateways for electronic mail and file transfer between DoD and OSI protocols. The NIST also initiated an effort, in concert with agencies and universities, to produce a public domain version of GOSIP-compliant protocols.

The NIST prefers to support agency requirements in large, generally applicable programs affecting multiple organizations. Examples include the Defense Data Network, the Defense Message System, and FTS-2000. The NIST, already assisting the Veterans Administration, the General Services Administration, and the Department of Treasury on specific procurements, examines requests for assistance from agencies that are attempting to acquire GOSIP-compliant systems. This is a challenge that will grow until enough infrastructure and industry expertise is in place for the NIST role to recede.

### Challenge 3: Additional GOSIP Functionality

The GOSIP Version 1.0 is a minimal but useful subset of functionality. More applications are required, new network technologies can be useful, and added architectural capabilities are needed. The number of GOSIP applications is expected to grow over the next few years to include virtual terminal, document interchange, directory services, transaction processing, and electronic data interchange. With the inclusion of the virtual terminal protocol several basic terminal profiles are expected, such as TELNET, transparent-mode, and forms mode. Development of added profiles for terminals such as 3270 models is desirable. The Directory services application will require development of a GOSIP directory information tree structure that is consistent with the international standard and directory entry formats for GOSIP objects.[7]

Two new network technologies are candidates for inclusion in future versions of GOSIP. The integrated services digital network (ISDN) will provide digital access to a digital long-haul service. All existing and planned GOSIP protocols can take advantage of ISDN. The fiber distributed data interface (FDDI) will provide a high speed (100-200 Mbps) fiber optic token ring service that can provide a campuswide backbone interconnecting local area networks and long-haul facilities.

Additional architectural capabilities are needed within GOSIP to support U.S. government requirements for security and dynamic routing.

In support of security needs, the National Security Agency (NSA) and the NIST are developing a security model that is consistent with the OSI security architecture, and a common set of protocols, based on the secure data network system (SDNS), to support confidentiality, integrity, authentication, access control, and non-repudiation for OSI end-systems. The security protocols and unclassified mechanisms that result will be published as FIPS and subsequently referenced within GOSIP.

The initial version of GOSIP includes static routing only. That is, the path between end-systems is determined in advance rather than "dynamically," based on network conditions such as traffic and congestion. While acceptable for many applications, static routing does not meet the needs of advanced users such as the DoD. As international standards and implementor agreements develop for dynamic routing, the GOSIP will be updated to include the additional capability.

To support dynamic routing GOSIP requires three protocols: 1) routing between end-systems and entry intermediate systems (ES-IS); 2) routing among intermediate systems within a single domain, that is, administered by a single organization (intra-domain IS-IS); and 3) routing between intermediate systems of separately administered domains (inter-domain IS-IS). The ES-IS protocol is now available for computers connected to local area networks. The intra-domain IS-IS is under development within international standards groups, and the NIST is assisting the development of the standard and supporting test technology. The inter- domain IS-IS protocol is moving forward within the European Computer Manufacturers Association (ECMA); the NIST is a primary contributor to the ECMA report.

GOSIP Version 2.0 will include virtual terminal, ES-IS routing, office document interchange, and ISDN. GOSIP Version 3.0 may add directory services, intra-domain routing, and FDDI. The NIST is now performing the laboratory and standards work necessary to move solutions for security, transaction processing, and inter-domain routing into future versions of GOSIP.

### Challenge 4: International Cooperation

In an ideal world multi-national vendors could develop products, have them tested for conformance and interoperation, and ship them into any market around the globe with full knowledge that the product meets the market requirements. In the real world legitimate needs may exist requiring regional differences in product specifications and testing. With respect to OSI products such as those conforming to GOSIP, international cooperation is desirable to minimize regional differences, reduce the need for multiple product testing cycles, and get products to users more quickly and cheaply. The challenge is to resolve these issues while creating formal standards, developing functional standards, defining user profiles, and establishing national and regional testing requirements.

To facilitate international cooperation, international standards groups must strive to limit the options, classes, subsets, and ambiguities within formal standards. Past standards have admitted multiple solutions to a single problem in order to overcome political disagreements within the standards-making arena (e.g., multiple transport classes). These multiple solutions lead to problems later in the creation of functional standards and user profiles.

Once a formal standard is complete, a functional standard is required in order to select the options and subsets to implement and to settle unresolved implementation details such as naming and addressing rules, error codes, and size limits. Often, choices in functional standards are made differently in different regions of the world. The most desirable international cooperation would result in a single functional standard for each formal standard. Real technical and economic differences within regions of the world make such a result unlikely. The minimal acceptable level of international cooperation must lead to a selection of functional standards that are interoperable. As with the formal standards process, international harmonization of functional standards may increase the capabilities available in each region beyond the true needs of the region.

User profiles document a selection of protocols that are derived from functional standards, filling in specific details such as network naming and addressing. Aligning functional standards still leaves room for differences when *users* make choices for a profile. This is a difficult problem, particularly for vendors. Progress is possible and the situation is not nearly as bad as it could be; for example, the Manufacturing Automation Protocols (MAP), Technical and Office Protocols (TOP), U.S. GOSIP, and Corporation for Open Systems (COS) profiles are fairly well aligned.

The most serious problem for international cooperation is international recognition of tests, testing methods, and test results. To achieve cross-government certification of OSI products, functional standards, user profiles, tests, test methods, and test reports must be aligned. These are formidable challenges. The NIST is taking several initiatives to address these concerns.

The NIST, representing U.S. GOSIP, is engaging in discussions with other governments to analyze user profiles, identify differences, and determine why the differences exist. This should lead to elimination of unwarranted and inadvertent differences between user profiles. The NIST—leaders in development of U.S. GOSIP testing policy and procedures—has started dialogue with other governments regarding OSI testing requirements and is working to develop a technical basis for test recognition across governments.

## The Next Horizon: Integrated, Interoperable Network Management

The success of OSI will likely lead to deployment of large multi-vendor networks comprising a variety of components such as local area networks, large and small computers, workstations, personal computers, multiplexors, switches, modems, long-haul services, bridges, and routers. Sets of components are likely to be owned and operated by different management domains; for example, long-distance carriers might own and operate long-haul services, a private organization

might install and operate a set of private branch exchanges, and local users might own and operate computers, workstations, and local network components. Network managers responsible for end-user service in such a complex and varied environment will require an integrated, interoperable network management system. The need will be felt acutely, very soon. Such a need points to the next horizon, which is revealing a set of challenges to be met leading to standards for interoperable network management.

Three fundamental components must be in place before interoperable network management is possible. The first component is a set of protocols for exchanging network management information. The OSI protocols provide a solid foundation. Five OSI application layer protocols might be useful to support management information exchange: 1) the common management information protocol (CMIP) provides point-to-point transaction-oriented services supporting basic management functions; 2) the file transfer, access, and management (FTAM) protocol provides point-to-point transfer of bulk management information such as accounting data, routing tables, and performance data; 3) the transaction processing protocol provides synchronized, multi-party transaction services for initiating and completing coordinated management directives; 4) the electronic mail protocol (X.400) allows network operators to exchange management advisories; and 5) the Virtual Terminal protocol enables network operators to remotely access management systems to exercise proprietary network management software.

The second component required to support interoperable network management is an agreed set of managed objects, related attributes, and allowable management operations. Work on this component, unfortunately, has generally languished, although the NIST is acting to encourage progress.

The third component of interoperable network management is an agreed set of structure rules for management information. If results so far are any indication, initial standards on structure of management information will be minimally useful. Progress on this problem is expected to accelerate soon.

The NIST is taking several initiatives to reach the next horizon sooner. The NIST provides technical, editorial, and administrative supports for development of international network management standards. For example, a NIST representative chairs the American National Standards Committee on Network Management (X3T5.4).

The NIST published two reports: 1) a survey of network management standards activities,[8] and 2) a statement of network management functional requirements.[9] The NIST is developing a prototype implementation to match implementor agreements reached in the Network Management Special Interest Group within the OSI Implementors Workshop.

Network management standards are critical to user and vendor needs within the next few years; yet the current pace and lack of coordination among the various groups working on such standards is likely to retard progress and create confusion in the minds of users. A major initiative coordinated between users and vendors is required in order to focus energy in a productive direction to reach a useful result as soon as possible.

In summary, incompatible computers and networks are a growing problem within most government agencies. The promulgation of the GOSIP FIPS provides an opportunity and a means for agencies to assert some control over their destiny. A major example of the successful pursuit of such policies can be found within the DoD. Agencies should plan for action now, or expect incompatibilities within their networks of computers to become much worse over the next five years.

The NIST has identified four major challenges ahead for the U.S. GOSIP and has recognized a new set of challenges over the horizon: integrated, interoperable network management. The program of work within the NIST Systems and Network Architecture Division is organized to meet the challenges. The next few years ahead should be rewarding, productive, and interesting for vendors, buyers, and users of networking products and services based upon international standards.

## NOTES


1. G. Mulvenna, "Government Open Systems Interconnection Profile," Nat. Bur. Stand. (U.S.) Proposed Fed. Info. Process. Stand. Publ. (FIPS PUB), *Fed. Reg.* 52:208 (28 October 1987): 41399-550.

2. *Implementation Agreements for Open Systems Interconnection Protocols*, NBSIR 86-3385-7.

3. The U.S. Government OSI User's Committee, *U.S. Government Open Systems Interconnection Profile (GOSIP)*, 27 October 1987.

4. T. Boland, *Government Open Systems Interconnection Profile Users Guide*, NIST SP 500-163, August 1989.

5. J.S. Nightingale, *GOSIP Conformance and Interoperability Testing and Registration*, August 1990, available from Jean-Philippe Favreau, NIST, Building 225, Room B217, Gaithersburg, MD 20899.

6. J.P. Favreau, K. Mills, and J.S. Nightingale, "The U.S. GOSIP Testing Program," in *Proceedings of The 6th International Conference on the Application of Standards for Open Systems*, October 1990.

7. K. Mills and R. Colella, *Directory Services Functional Requirements*, May 1988, available from Joan Wyma, NIST, Building 225, Room B217, Gaithersburg, MD 20899.

8. C.M. Chernick, et al., *A Survey of OSI Network Management Standards Activities*, NBSIR-87-3593, NIST.

9. R. Arnoff, et al., *Management of Networks Based on Open Systems Interconnection (OSI) Standards: Functional Requirements and Analysis*, NIST SP 500-175, November 1989.