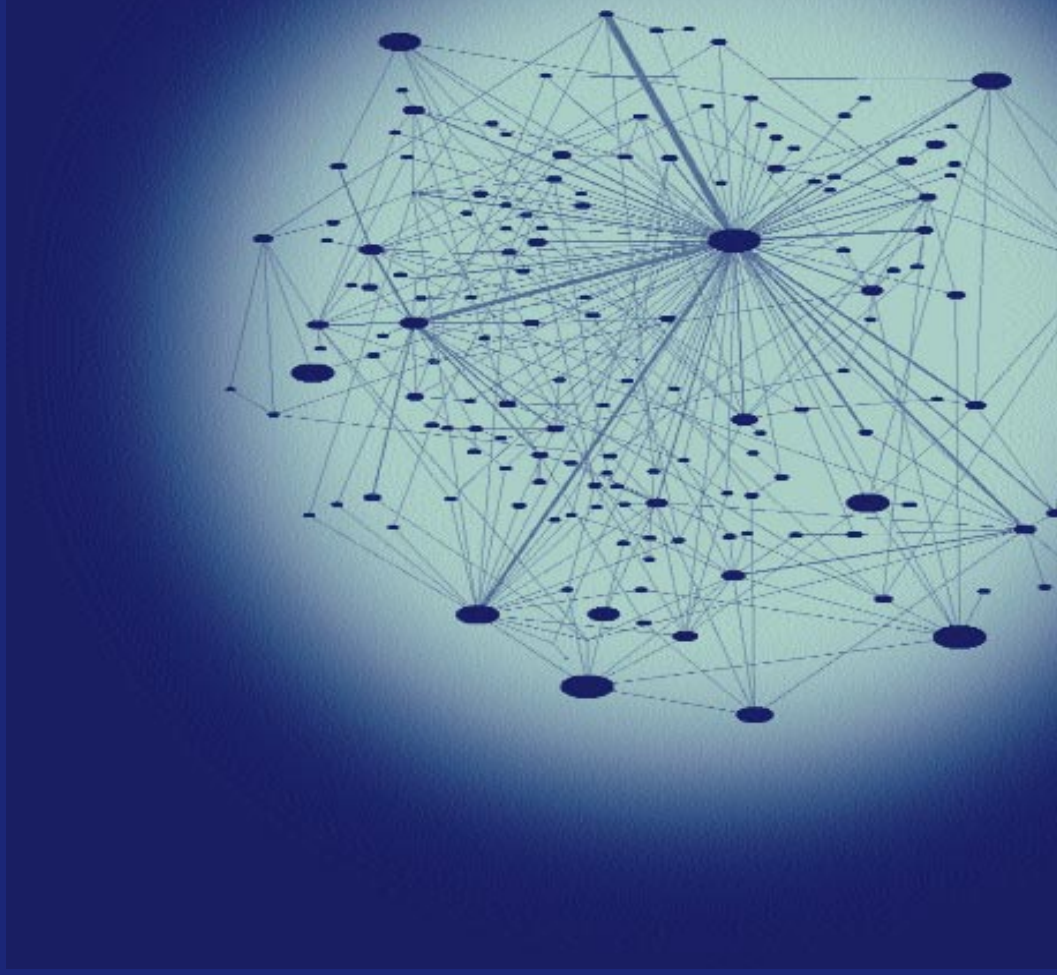
RESEARCH CHALLENGES FOR THE NEXT GENERATION INTERNET



May 12-14, 1997

Edited by
Jean E. Smith &
Fred W. Weingarten

COMPUTING RESEARCH ASSOCIATION

EDITED BY

Jean E. Smith and Fred W. Weingarten

CONVENED BY

Computing Research Association

CO-SPONSORED BY

Computing Research Association
Computer Systems Policy Project
Cross-Industry Working Team
Large-Scale Networking Group of the National Science and Technology Council's Committee on Computing, Information, and Communications R&D Subcommittee

Workshop funding provided by the National Science Foundation.

Cover art provided by Tamara Munzner (Stanford University), Eric Hoffman (Ibsilon), k claffy (UCSN/NLANR), and Bill Fenner (Xerox PARC). For further information, see http://www.nlanr.net/Viz/AS/. Partial support for the work was provided by the National Science Foundation.

Additional copies of this report are available from CRA. Send your request to:

COMPUTING RESEARCH ASSOCIATION
1100 17th Street, NW, Suite 507
Washington, DC 20036-4632
Fax: 202-667-1066; E-mail: info@cra.org
URL: http://www.cra.org

TABLE OF CONTENTS

PREFACE

Predicting the evolution of the Next Generation Internet is a daunting prospect. Experience demonstrates that no one was able to forecast precisely how the original Internet would grow and how it would be used. Surely the next generation version will have similar surprises in store.

Setting a research agenda for the NGI is not a simple task. However, this report reflects the deliberations of experts from business, government and academia who accepted the challenge to outline a research agenda that almost certainly will change and evolve as fast as the Internet itself. Some of the cross-cutting issues that emerged from the separate workshop sessions are responses to this dilemma. For instance, all groups called for more interaction with the applications researchers. Some talked about a "spiral" model of evolution, in which network researchers cycle from network research to application experiments, followed by more network research, and so on.

Some workshop participants recommended that the community step back and take a longer-term view in an attempt to envision more clearly how it would like to see this powerful technology evolve. Such an effort would make an important contribution to science and technology policy, but will require far more than a two-day workshop to achieve.

The NGI vision is, and may always be, a work in process. In the meantime, however, we believe that this report will provide a useful starting point for what can become a vitally important federal program. In some ways, most information technology research these days is moving toward a wholly new systems paradigm of interconnected, highly distributed computer/communications systems. NGI sits at the core of that effort.

On May 12-14, 1997, the Computing Research Association (CRA) convened a workshop in Vienna, Virginia, to bring together networking experts from industry, academia and government to develop a research agenda for the NGI. The Computer Systems Policy Project (CSPP), Cross-Industry Working Team (XIWT), and Large Scale Networking (LSN) Group of the National Science and Technology Council's Committee on Computing, Information, and Communications R&D Subcommittee joined CRA in co-sponsoring the workshop.

We would like to thank the plenary speaker, Anita Jones; the panel on networking history; and the speakers who participated in the opening session. All helped to provide a valuable context for the workshop discussions.

Our thanks to all of the workshop participants for their contributions. In particular, we wish to acknowledge the hard work of the session moderators and recorders who did a stellar job of pulling together cogent summaries of the often disparate views of attendees. David Clark played a key role in providing the charge to the workshop, guiding its progress, and summarizing the results at the closing session. Louise Arnheim wrote the report Summary. We thank them both.

Thanks to the reviewers of the various sections of this report, which has been strengthened by their comments and suggestions. The views expressed in the report do not necessarily reflect those of the reviewers.

We wish to thank members of both the program committee and federal steering committee for their guidance and assistance in workshop planning. The contributions of CRA staff Kimberly Peaks and Phillip Louis in organizing the workshop are gratefully acknowledged.

We would like to express our appreciation to the National Science Foundation (NSF) for funding the workshop, and to the NSF program staff for their support and concern for this important issue. However, the ideas and suggestions expressed are those of the authors and workshop participants. This report does not reflect NSF policy or the views of any particular participant.

In addition to this report, some of the workshop highlights have been captured in a brief videotape. Copies will be available from CRA in the fall.

JEAN E. SMITH
Workshop Coordinator

FRED W. WEINGARTEN
Computing Research Association

A. SUMMARY

Louise Arnheim

1. INTRODUCTION

Having grown from a research tool intended for a well-defined community to a powerful communications medium accessed by a worldwide citizenry, the Internet is at an important transition point. While exciting new applications in medicine, environmental science, crisis management and other disciplines are tantalizingly near, they remain out of reach. Today's Internet cannot scale to meet the number and nature of demands already placed on it, much less a new generation of more complex interactions. With three decades of experience, network researchers can engage in the type of collective self-reflection that comes from the ability to draw on the past.

According to Tom Kalil, National Economic Council, the Internet led to more than $200 billion in market capitalization.

The Next Generation Internet (NGI) initiative is about this transition: using the Internet's promise and its past to accelerate the rate of future network development. The Workshop on Research Directions for the NGI was the first step towards defining a research agenda for such development.

The importance of articulating that research agenda rests on four premises. First, the Internet has already had a tremendous impact on the economy. According to Tom Kalil, National Economic Council, the Internet led to more than $200 billion in market capitalization. We can only imagine what the next generation Internet might mean for the economy. Second, modern information technology applications increasingly are designed to integrate computers and high-performance data communications into fully distributed systems. Interconnection, the issue facing researchers in the late 1970s, is often an afterthought. Third, the capacity and capabilities of today's Internet are challenged by two issues: 1) scaling existing uses to a broader community of users, and 2) bringing new, sophisticated applications online. Thus, a more advanced architecture is needed. Finally, many of the possibilities envisioned for the NGI exhaust our current understanding of network design. Only through fundamental research can we move to a level that will help us realize those possibilities.

2. CONTEXT FOR THE NGI INITIATIVE

Although the research challenges of the late 1990s are significantly different from those of the late 1960s, one factor has remained constant: the need for government-sponsored network research and development. Such R&D is as critical to the NGI's future success as it was to the success of the original ARPAnet. The ARPAnet's origins can be expressed in two words: packet switching. The notion of sending data in packets was a revolutionary concept developed 30 years ago by researchers at the Defense Advanced Research Projects Agency (DARPA).

A decade later, network researchers faced a new challenge: linking together multiple packet networks. Meeting this challenge required a shared vision about what such networking would look like. From this shared vision, two new ideas were born: 1) an open architecture that allowed such networks to converse or "federate" with one another while remaining separate entities; and 2) communications protocols, or "rules" to govern those conversations.

By the early 1980s, this shared vision of networking caught the attention of additional federal agencies such as the Department of Energy, National Aeronautics and Space Administration and the National Science Foundation (NSF). In fact, federal funding for several "supercomputer centers" with an NSFnet as their backbone ultimately replaced ARPAnet. Towards the end of the decade, additional funding led to the creation of several regional networks in partnership with leading universities, and a "new" NSFnet emerged.

Today, packets of information travel among the domains of ".mil," ".gov," and ".edu," as well as the several million new users at ".com" and ".org." With a relatively modest level of government funding, data communications was revolutionized, a communications medium was born and a new commercial industry was created.

3. ROLE OF THE FEDERAL GOVERNMENT IN NETWORK RESEARCH

One of the fundamental lessons learned from this series of government-funded partnerships was an ability to identify those research issues the private sector was not inclined or willing to undertake on its own. As many workshop groups noted, this particular history lesson enabled them to identify areas where government-sponsored initiatives could be helpful to the NGI.

There are many reasons why commercial enterprises are not likely to engage in the type of collaborative research and development needed to hasten the NGI. Among those reasons

are: the rapid pace of product cycles; competitive pressures (making parties less willing to risk potential exposure of failure); industry fragmentation (making it difficult to address long-term issues); antitrust concerns; and the closing of many industrial research labs.

Funding for long-term research and development is still a role best served by the federal government. While commercial providers scramble to meet day-to-day customer demands, government can take the longer view.

4. NETWORKING RESEARCH AND THE "SPIRAL DESIGN"

Networking research and development is, of necessity, an iterative process—a "spiral design" requiring continuous feedback between network researchers and researchers (of various disciplines) testing applications on the network. These two activities are vertically coupled: networks drive the applications, and applications drive the networks. However, the achievement of real progress in network research requires that many applications be tried. Only in this manner can the common threads—or areas of further network research—be identified. Of necessity, such testing often takes place using the best information possible, within a limited period of time, and without the ability to engage in extended conversation with other researchers.

Further, in the course of both constructing these applications and experimenting with them, many more common application-oriented services will be identified. These services will then become appropriate for reuse through middleware concepts that arise with the development of still newer applications. As each development cycle is completed and then begins anew, the overall cost of constructing powerful network-centric applications will be reduced.

5. WORKSHOP PROCESS

The goals of the Workshop on Research Directions for the Next Generation Internet were to:

- Develop and publish an agenda for research needed to develop future high-speed data communication networking.
- Bring together academic and industry researchers to address these needs.
- Provide a publicly visible "kickoff" to the NGI initiative and generate interest in the computer science and engineering community.

On February 17, 1997, the Computing Research Association (CRA) issued a Call for White Papers. More than 100 papers were submitted by the closing date of March 27. The pro-

gram committee, responsible for providing the scientific leadership for the workshop, met on April 3 and selected 43 papers. For each accepted paper, one author was invited to attend the workshop. The papers were provided in advance to all attendees as background for the workshop discussions, but were not formally presented at the meeting. To highlight potential NGI applications, CRA also issued a Call for Videos on March 5. Seven were selected and were available for viewing at the workshop. Portions of these tapes also will be included in a short video of workshop highlights, currently in preparation.

In addition to attendees invited on the basis of papers submitted, other workshop invitations were issued based on the recommendations of the federal steering committee, program committee and sponsors. The objective was to convene a group of experts who would provide the views of industry, academia and government on the research agenda for the NGI.

On May 13, workshop participants met in plenary session before breaking into six separate working groups: applications, middleware, quality of service, Internet traffic engineering, security and architecture. During that session, David Clark urged participants to "take back the future" (lest commercial interests define the NGI) and use the limited time available to focus on consensus areas. Further, Dr. Clark encouraged participants to articulate what they thought should happen and, for the moment, dispel any constraints that might come to mind.

Group moderators were responsible for summarizing the findings of their groups. Following the workshop, these drafts were further refined and circulated widely for review. Comments and suggestions were considered and incorporated where appropriate. Below are summaries of these six group reports. The full versions appear in report sections B1 through B6.

In many respects, the workshop group process itself mirrored the way network research takes place in the "real world." Using the best information available and their collective expertise, each workshop group was assigned a task (developing a research agenda) to complete in a limited period of time and without the benefit of extensive interaction with other working groups (the Applications and Middleware groups did, however, meet together for a few hours on the workshop's second day). And, like participation on the Internet, participation in workshop proceedings was higher than anticipated, leading to congestion of a different sort, and standing-room-only situations in some workshop rooms.

6. WORKSHOP GROUP SUMMARIES

6.1 APPLICATIONS

Using a "spiral design" approach to understanding future network requirements and reducing the risks of misdefining the NGI.

Today's Internet and its underlying base technologies have been used successfully in a wide variety of applications. Realistically, however, the current Internet cannot support an emerging set of activities, many of which are essential to mission-critical applications in government, national laboratories, academia and business.

> The current Internet cannot support a number of important missions, including national security, economic competitiveness and social goals.

In fact, the limitations of today's Internet actually prevent these sectors from extensively pursuing a number of activities. For example, collaboration is a critical part of both science and business. Successful collaboration over the Internet, however, requires network access whose quality is high enough to allow ever-changing groups of colleagues to interact in real time and in a variety of ways. This type of access is not possible with today's small, static set of point-to-point connections.

While it is possible (in some cases) to use high-bandwidth, fixed connections or to simplify the applications themselves to allow operation with reduced network demand, these approaches do not address the larger and longer-term issues raised by the NGI.

To fully understand the trade-offs, basic requirements and network management requirements of the future network, researchers must be able to experiment with the "full-blown" versions of applications in testbed settings.

The Applications Group recommended a "spiral design" approach to defining the future Internet: that is, forcing the iterative design of the applications, the supporting middleware and management software, and the network on which the applications run.

6.1.1 Aggressive Scenarios

By selecting a few key examples of applications and then implementing them through aggressive, experimental scenarios, network researchers would be better positioned to conduct follow-on experiments, and reduce the risk of misdefining the NGI.

An example of such a scenario would be extending digital library access to the public. Providing such access to other institutions and even primary schools demands a new level

of scalability and geographic distribution for both the network and the services involved. This type of scenario would not only drive the technologies in question, but also would tax proposed network abilities in a way that would ultimately help researchers improve or remedy network attributes more quickly. Further, scenarios like this would offer a clear, public demonstration of the NGI's benefits.

6.2 MIDDLEWARE

Systematically lowering the barriers to constructing Internet-centric applications.

Consider a vendor who wishes to sell the newest version of an extremely popular piece of software through the World Wide Web. Using secure http, the vendor provides purchases by credit card. In return, using a customer's public key, the company provides a private version of the software to the customers. The Web itself, in contrast with the browsers that provide the user interfaces, is part of what is known as "middleware." In addition, the credit card information exchange and distribution of public keys are middleware elements.

Middleware can be viewed as a reusable, expandable set of services and functions that is commonly needed by many applications to function well in a networked environment. These services often need to be used in various combinations with each other and with the variety of components built by application developers. The challenge is to preclude the need to "reinvent" an expensive tool kit over and over again for each interaction of applications.

For its research agenda, the Middleware Group outlined five enabling technologies (R&D) and concepts.

6.2.1 Multicast group communication and aggregation needs—*Most of today's production applications and applications-level protocols are based on the assumption of the ubiquitous availability of reliable point-to-point transport services. By establishing a comparable multicast protocol, or protocols, researchers would be able to explore an extensive range of new applications designs.*

6.2.2 Quality of Service (QoS) integration architecture—*The NGI would benefit from an overall framework of models, languages and protocols that permit distributed applications to specify desired QoS levels and to negotiate acceptable trade-offs and confidence levels.*

6.2.3 Semi-transparent session layers—*To provide effective end-to-end quality service, the QoS architecture must be populated with a new generation of layered, distributed system software.*

6.2.4 Dynamic monitoring and adaptive resource management—*Since the level of available resources will vary significantly from time to time, the ability to monitor and collect information on the status of resources will be needed.*

6.2.5 Brokering and negotiating technology for matchmaking—*Automated services such as "intelligent matchmakers" hold the potential for helping their human users manage a growing variety and complexity of Internet-related activities.*

6.3 QUALITY OF SERVICE

Providing mechanisms that allow for different levels of service at different costs.

The Internet was initially conceived and implemented as a centrally supported shared resource. Generally speaking, the growth in demand was met by increasing available resources. In that environment, a single service class, often called "best effort," was implemented and everyone had "equal rights" to available resources.

However, the requirements of time-sensitive applications, coupled with an explosion in user population size, have made simply adding more bandwidth an impractical solution. Consequently, methods now must be found to gracefully deal with the issue of who "gets" service when the network becomes congested.

Commercialization of the Internet has made the solution to this matter somewhat easier: no longer does everyone and everything have to be treated equally. It is finally possible to adopt a "want more/pay more/get more" approach, whether that approach is part of an actual payment system, enforced by peer pressure or mandated by funding agencies.

It is important to note that many existing and future applications will require a level of service that is better than "best effort." These applications include very-high-performance scientific applications, as well as emerging high availability commercial and industrial applications (e.g., backups of financial or manufacturing data, shared immersive environments, and time-critical applications such as just-in-time warehousing and manufacturing).

The Quality of Service Group called for R&D in six areas:

6.3.1 *Mechanisms that translate decisions about resource management and allocation, via authoritative adjudication, into network behavior in real time are needed. These mechanisms include brokering bandwidth to meet QoS requirements, flow control and admission control.*

6.3.2 Net control research—*Diagnostic tools built into the network are needed to determine the nature of a problem and identify its source. Such tools could identify someone who had "faked" payment for priority service.*

6.3.3 Multicast issues—*There is a need to explore an economic model for implementing access control in multicast sessions.*

6.3.4 Systems prototypes—*Prototypes must be large enough to allow for the testing of cross-hierarchical failures and of multicast across networks and architectures.*

6.3.5 Simulation—*With the NGI as a testbed, simulation might be one of the research tools leading to improved quantitative understanding of the network.*

6.3.6 Economic models—*Given scarce resources, how can values related to prioritization be expressed? How will the network discern the resulting prioritization?*

6.4 INTERNET TRAFFIC ENGINEERING

Obtaining, interpreting and using traffic data to enhance NGI capacity, performance and reliability.

Consider one youngster in Ohio playing an online, interactive game with a friend in Nevada, multiply that by millions of youngsters nationwide, and you have influenced the way bits of information are distributed and Internet traffic is directed.

Interactive games, online catalog shopping and many other applications are already taxing the Internet's ability to deliver traffic in a consistent, stable and reliable manner. Yet the ability to access data about network traffic, send it to various parties (e.g., operations centers, network planners and users), and do so in a way that does not interfere with either network or these applications is a long-standing research problem. The commercial sector—because of antitrust laws and competitive market pressures—is reluctant even to meet, much less share such valuable information. Therefore, in order to reap the intended benefits of such traffic-related research, any government R&D in this area must require commercial collaboration as a prerequisite.

As the Internet becomes more essential to national objectives, its ability to keep pace with performance and reliability objectives will become increasingly difficult. Merely setting aside additional capacity is not the answer. The essential reliability of the network cannot be achieved without significantly expanding the data, tools and methods available for traffic engineering. Additionally, network cost-effectiveness can only be assured by plan-

ning, provisioning and day-to-day traffic management, based on consistent objective knowledge of the network behavior and the traffic offered.

The Traffic Engineering Group recommended the following research agenda:

6.4.1 Traffic measurement and performance—*Open the NGI, and other government-sponsored testbeds, to appropriate traffic measurement and performance monitoring by the research and user communities.*

6.4.2 Performance metrics—*Define a basic set of standardized, unambiguous performance metrics that can support objective study and comparison across networks throughout the Internet.*

6.4.3 Metric usage—*Promote the use and availability of such metrics and tools throughout the existing Internet, as well as within the NGI networks described in Goal 1 of the NGI initiative (see Box 1).*

BOX 1. GOALS OF THE NEXT GENERATION INTERNET INITIATIVE

1. Connect universities and national labs with high-speed networks that are 100 to 1,000 times faster than today's Internet. These networks will connect at least 100 universities and national labs at speeds that are 100 times faster than today's Internet, and a smaller number of institutions at speeds that are 1,000 times faster. These networks will eventually be able to transmit the contents of the entire Encyclopedia Britannica in under a second.

2. Promote experimentation with the next generation of networking technologies. For example, technologies are emerging that could dramatically increase the capabilities of the Internet to handle real-time services such as high-quality videoconferencing. There are a variety of research challenges associated with increasing the number of Internet users by a factor of 100 that this initiative will help address. By serving as "testbeds," research networks can help accelerate the introduction of new commercial services.

3. Demonstrate new applications that meet important national goals and missions. Higher-speed, more advanced networks will enable a new generation of applications that support scientific research, national security, distance education, environmental monitoring, and health care.

Source: President William J. Clinton, speech delivered October 10, 1996, at Oak Ridge, Tenn.

6.4.4 Measurement archives—*Preserve measurements in archives that are available to the research and user communities (subject to the minimal necessary privacy and nondisclosure constraints) to allow consistent analysis over a long time scale and comparisons of performance and traffic behavior.*

6.5 SECURITY

Meeting existing concerns about security, while anticipating new ones raised by a new era in advanced networking and computing.

The current Internet is rife with security problems. Viruses and hacker attacks are commonplace. Attacks involving denial of service have struck public Web servers, and large portions of the Internet population have been left without service because of benign configuration errors. Ironically, while prospective users of the Internet's commercial applications are daunted by security concerns, the Department of Defense is using the same (public) Internet technology for its critical systems.

The Security Group developed an ordered list of ten areas where federal funding for research and development would be appropriate.

6.5.1 Infrastructure robustness—*The NGI will use the same routing protocols used in the current Internet. However, these protocols are quite vulnerable and "attacks" can easily deny or degrade service to large numbers of subscribers.*

6.5.2 Security policies—*The absence of scalable, dynamic security policies and corresponding enforcement mechanisms retards the sharing of information among collaborating researchers.*

6.5.3 Mobile code—*This type of security must also be enhanced if, for example, the promise of intelligent agents (set loose to search and/or retrieve information) is to be realized.*

6.5.4 Intrusion detection—*Detecting attacks in large-scale, distributed systems such as those likely to be part of the NGI is currently beyond our capabilities. DARPA-sponsored work on a common intrusion detection system (now underway) will provide a solid basis for future R&D in this area.*

6.5.5 Public Key Infrastructure (PKI)—*There is relatively little experience in deploying and managing large PKIs of the type that may be necessary to support emerging and future NGI applications. Government PKIs pose special problems because of the scale and diversity of the user population and the sensitivity of information made accessible (the recent*

Social Security Administration experience with Internet access to records illustrates the sensitivity issue).

6.5.6 Security management—*There is a need to improve the management of heterogeneous security systems (e.g., those which support intrusion detection).*

6.5.7 Cryptography—*Though many applications are beginning to rely on encrypted and/or authenticated communications, the algorithms commonly used today do not support the very high speeds envisioned for the NGI.*

6.5.8 Operating systems—*Most NGI users will be utilizing the same operating systems now being executed in the desktop and server computers through the Internet. However, the security of these systems is woefully inadequate, raising serious doubts whether such systems can be used as the basis for applications involving valuable data, experimental equipment, or even human lives.*

6.5.9 Software engineering—*Despite considerable R&D in this area (much of it government-funded) security-relevant errors introduced during the design and implementation phases of software system development are still the primary cause of system vulnerabilities.*

6.5.10 Network management—*Today's technology is not up to the task of supporting the type of infrastructure robustness envisioned for the NGI. To date, most industry work in this area has focused on "point" rather than "system" solutions, and there is no significant research being done on vendor platform systems that are large in scale, distributed and heterogeneous.*

6.6 ARCHITECTURE

Finding a structure that enables the effective integration of new technologies in a highly diverse and rapidly changing environment.

While the current Internet architecture is clearly the foundation for the NGI, it is built around a set of technology and application assumptions that may not apply to conditions during the next generation. Thus, a central research challenge for network researchers is finding a structure that enables the effective integration of new technologies into the NGI. Finding that structure may require consideration of architectural approaches that depart in significant ways from the current Internet architecture. With this in mind, the Architecture Group outlined four broad areas of study.

6.6.1 Network Services

Within the past decade, it has become necessary to expand the definition of Internet service to include support for multicast and quality of service. While considerable progress has been made in these areas, more work is necessary.

- Already, there is a need to develop mechanisms that enable ubiquitous multicast, virtual networking, the efficient handling of short-lived sessions and dynamic service creation.
- Of these four services, virtual networking in particular offers a straightforward mechanism for implementing experimental testbeds. Virtual networking allows the construction of multiple networks on a common infrastructure, enabling organizations to easily set up private networking domains governed by organization-specific policies.
- Within the NGI, virtual networks could be used as testbeds for system-level research that cannot be carried out safely in a production environment.

6.6.2 Network Management

The Internet's rapid growth (both in terms of size and range of services) is already straining the capabilities of network control and management. For example, the Internet's reliance on manual methods for configuring routers and performing other management functions is becoming increasingly impractical. Self-configuring and self-organizing systems are needed to automate key management and control functions at all levels.

6.6.3 Network Performance

Future growth in both the number of users and the data requirements of new applications will continue to drive the need for higher performance and more efficient systems. While technology advances will help meet those needs, it is important to note that such advances will not occur uniformly in all dimensions. Thus, in order to capitalize on such developments, new architecture approaches and new designs for key network components (e.g., routers, switches and end-systems) will be required.

6.6.4 Diversity and Change

As networks become larger and more complex, they also become more difficult to alter. The current Internet has been remarkably effective in dealing with diversity and change, but the challenges will increase significantly over time. The NGI initiative must develop systematic methods for coping with an ever-widening range of applications requirements, network technologies and persistent change.

B.1 APPLICATIONS

Moderator: Stuart Feldman

1. INTRODUCTION

The worlds of science, engineering, government and commerce have been revolutionized by the Internet. The essentially ubiquitous access, shared standards for transmitting and representing information, and low costs have changed the way people conduct business. The sea change was caused not by raw bandwidth, but by the shared protocols, applications and technologies of the World Wide Web. For many people, a world without electronic mail or access to Web information sources is unimaginable.

Nonetheless, the current technology cannot support a number of important missions, including national security, economic competitiveness and social goals (e.g., improved education and health care). It is routine to send small e-mail messages and even the occasional multi-megabyte file, and usually the information eventually reaches its destination. However, the current Internet is not suited to transmitting information that must arrive quickly, or to sending huge numbers of bits in a continuing stream or to many consumers. The current network and applications cannot realistically support a wide variety of activities that are essential to the missions of the national laboratories, research universities and laboratories, nor can they meet the needs of the general commercial and public user communities. People want to be able to collaborate with others without continual travel, take advantage of unique physical resources, search multiple information sources, and make these resources widely available.

> Researchers must be able to experiment with the "full-blown" versions of applications in testbed settings.

It is currently possible to approximate some of these applications by using high-bandwidth, fixed connections, by using best-effort transmission, or by simplifying the domain. To move to the next level of capability, however, it is necessary to experiment with the full-blown versions of these applications in realistic network environments to push the limits of scalability, or to derive applications to support potential users. Such efforts will help to identify the trade-offs, basic requirements and network management requirements of the future network.

The Next Generation Internet (NGI) promises underlying resources one or two factors of ten better than the current network, as well as guarantees of better service. The NGI is expected to operate on a wider variety of data and media types, to be used by a wider spectrum of people and organizations, and to be used routinely for mission-critical applications. Reaching these goals will, itself, be a significant achievement; however, it will only be important if the network is used to meet national goals and to produce important societal and economic returns on the investments. It is, therefore, essential that the NGI plans focus on those applications.

The amazing success and continued evolution of the Internet was unanticipated. The original network was designed to serve dozens of nodes, meeting the needs of hundreds of scientific experts for application-sharing and data transmission. (The original design almost limited the network to 256 nodes!) Instead, tens of millions of nontechnical people exchange electronic mail, join in discussions and look up information. The network has evolved enormously as the patterns of usage and access have changed. The learning process was difficult, but the results have been extremely useful. Although the future of the NGI is unpredictable, it is possible to begin to exercise the technology and identify its true limits by making intelligent choices for serious experiments on potential applications. These experiments could frame the next generation of standards and base technologies that will proliferate through the network. The lack of such experiments could result in bad decisions about network capabilities, and some grand opportunities will be missed by freezing designs too soon.

In addition to stressing the underlying physical abilities of the new network, applications will force the exploration of the programming model. They also will identify ways to reduce cycle times and the costs of fielding new and important uses. It is not sufficient that the physical network be able, in theory, to support a particular use; it must also be feasible to program the application and control the network with a reasonable amount of time and effort. Group members do not expect these prototypes to yield a simple result; rather, they anticipate the outcomes will make it easier to understand the interactions of programmability, network behavior and network resources.

2. APPLICATION-DRIVEN NETWORKING RESEARCH: THE SPIRAL RESEARCH MODEL

Throughout the Internet's history, there has been continuing feedback between networking capabilities sparking new uses, and new uses driving new protocols and network engineering. Group members view this as an essential and healthy phenomenon: it is not possible to foresee the uses of proposed network upgrades in detail, nor is it possible to pre-

dict interactions inside the network or trade-offs in the engineering without building the technology and testing it in real use.

Group members propose selecting a few key examples of applications and implementing serious experimental demonstrations. The work must be organized to maximize learning from each prototype—the goal is not to produce operational services, but to force the iterative design of the applications, the supporting middleware and management software, and the network on which the application will run. These projects must be run on a compressed schedule with ambitious but well-defined goals.

In other words, the group recommends a "spiral" design approach to defining the next network: After each experiment, more will be known about the true requirements for all aspects, and researchers will be in a much better position to conduct the next experiment and reduce the risk of misdefining the NGI.

3. DIMENSIONS AND DIRECTIONS OF NETWORK IMPROVEMENT

NGI technology will improve some aspects of the underlying network. Although these improvements are essential, what is important ultimately is that applications become more capable and that users perceive improved results. Eliminating delays in moving information through operating systems and applications to the user interface can be as important as improving data switching and transmission. Equal weight must be given to driving applications as is given to network infrastructure.

3.1 BANDWIDTH

Traditionally, applications used little bandwidth, except for occasional downloading of large data files. Electronic mail messages often contain megabyte attachments, and downloading files in the many-megabyte range is routine. These patterns have already had dramatic impacts on network design. As access to huge data sources becomes more common, and as end-users need more video content, the demand for greater aggregate bandwidth will skyrocket. Application architecture will need to be changed to handle broadband data streams, as well as to make appropriate decisions.

3.2 DIFFERENTIAL CLASSES—QUALITY OF SERVICE

The term Quality of Service (QoS) refers to a wide variety of properties, including delay (latency), jitter (variance) and availability. Demands for improved quality are driven by needs for reliable and timely delivery of control signals, telemetry and human-oriented

data streams (audio, video, and tactile). Some of the most aggressive demands for low-delay interactions come from "twitch" game services and man-in-the-loop simulators; in the future, tele-immersive applications will impose even tighter requirements for differential support of QoS. Furthermore, to accommodate changes in the computational environment or the network, applications will require the capability to change dynamically the levels of quality they demand. As people and organizations begin to depend on Internet and NGI applications, they will require service that is continuously available. The current Transport Control Protocol/Internet Protocol (TCP/IP) was designed in part to handle failures in network nodes and links. Advances in application architecture and fundamentally new middleware are needed to provide services that are continuously available end-to-end, despite the failures of particular computing or network nodes.

Applications will require the capability to change dynamically the levels of quality they demand.

3.3 MULTICASTING

Although many packet networks run on broadcast media, there is relatively little use of controlled (limited scope) broadcasting ("multicasting"). Many applications would benefit from this capability, but multicasting is not currently supported on wide area networks. Applications either use a global broadcast on a local area network or they transmit multiple copies of the same information streams. Future collaborative applications will rely on multicast to keep communication costs down and performance high. However, until measurements are made of the behavior of new large-scale applications, it will not be clear how to optimize network performance or to make it easy to use new capabilities.

3.4 NUMBER OF NODES

Perhaps the biggest difference between the expectations for the original ARPAnet and those for the current Internet is in the number of users. The original network contemplated dozens of participants (perhaps a hundred). Currently there are millions of individual computers (nodes) and at least 50 million people who use the Internet (albeit mostly for e-mail and occasional World Wide Web access). These numbers have been approximately doubling every year, with no end in sight. Group members expect deeper penetration into the user base, and also a broadening of the applications that people use. Electronic commerce, as well as public data and government access applications, are obvious areas where millions of nodes will interact. There are clear implications for directory services, routing tables and application design to accommodate millions of nodes whose numbers continue to grow.

3.5 SECURITY

Privacy and security will be required by most applications. These demands are driven not only by traditional military and intelligence concerns, but also by rising public demands for secure financial transactions and personal records. Basic security is essential to trustworthy operations.

4. APPLICATION TECHNOLOGIES

Certain basic technologies will be common to many uses of the NGI. The first round of new applications will capitalize on these abilities, and will combine them in a variety of ways to create the new programming and human-computer interface paradigms. Therefore the initial experiments should be planned around these technologies, with an eye to testing the limits of implementability, manageability and performance.

4.1 DATABASE ACCESS

Concerns are being raised about the increasing size of some databases. The public World Wide Web currently contains hundreds of gigabytes. Large corporate databases often measure in terabytes. Large-scale simulations (such as those planned for the Advanced Scientific Computing Initiative projects) are expected to produce tens of terabytes per day. Earth-orbiting satellites will transmit petabytes of irreplaceable data.

In addition, users are demanding the ability to conduct far more sophisticated searches and analyses of multiple databases. Matching algorithms for genome databases and image and pattern queries require deep and expensive algorithms. Data mining of large databases can require enormous computations. A variety of architectures (decisions about moving data to the search or the search to the data, intermediate data and analysis servers, etc.) may be needed to meet these needs.

4.2 AUDIO AND VIDEO

Audio and video data will be part of most future Internet use. People enjoy talking and looking at other people. Motion also provides another dimension for understanding the relationships of information. Different qualities of audio and video require radically different bandwidths: compressed speech uses less than one kilobyte per second, while uncompressed CD-quality music uses around 200 kilobytes per second. Highly compressed, small-screen video can be transmitted at two kilobytes per second; high-definition TV requires several megabytes per second. Of necessity, the lower-quality streams are currently used, but comfortable communication requires the higher rates and immersive experience demands gigabits per second. Furthermore, people do not tolerate delay and

jitter. Interactive communication thus requires careful control of quality of service from one end of the application to the other.

4.3 REAL-TIME AND DELAYED COLLABORATION

Increasingly, groups want to interact across time and space. Collaborative technology is essential to supporting virtual enterprises, collaboratories, desktop videoconferencing and distance-independent learning. However, a variety of difficult technical problems must be solved to have satisfactory collaborations. In addition to control and synchronization of audio and video streams and shared access to information, collaboration requires managed interactions, maintenance of history and audit trails, and support of distributed protocols to provide appropriate levels of consistency.

4.4 DISTRIBUTED COMPUTING

Currently, most distributed computing is done either by the tight interconnection of processing elements on a backplane of a single high-performance computer or in a physically connected cluster. In the future, more large-scale computing will be done using geographically separated elements, either because the application demands more capacity than is available at any single node, site or enterprise, or because there are unique resources that must be accessed remotely.

Distributed computing is already a practical and important technology. It is used to run telecommunications networks, support important interactive simulations, and run multiuser games. There is a great deal of funding in the public and private sectors for extending the use of distributed technologies, and these applications increasingly will depend on high-bandwidth connections among the computing elements.

4.5 TELE-IMMERSION

Tele-immersion will enable users in different locations to collaborate in a shared, virtual or simulated environment as if they are in the same room. It is the ultimate synthesis of networking and media technologies to enhance collaborative environments.

In a tele-immersive environment, computers recognize the presence and movements of individuals and objects. They track their images and then permit them to be projected in realistic, multiple, geographically distributed immersive environments where the individuals can interact with each other and with computer-generated models. Tele-immersive environments can be used to advance a variety of applications, such as accelerating automobile design, designing new drugs, and facilitating collaborative environments for education, health care and entertainment.

Tele-immersive applications must combine audio, video, virtual worlds, simulations and many other complex technologies. They will require huge bandwidth, very fast responses and guarantees of delivery. Table 1 summarizes one view of the needs for a successful tele-immersive experience.

TABLE 1. NEEDS FOR A SUCCESSFUL TELE-IMMERSIVE EXPERIENCE

TYPE	LATENCY	BANDWIDTH	RELIABLE	MULTICAST	SECURITY	STREAMING	DYNAMIC QOS
Control	<30 ms	64 kb/s	yes	no	high	no	low
Text	<100 ms	64 kb/s	yes	no	medium	no	low
Audio	<30 ms	N x 128 kb/s	no	yes	medium	yes	medium
Video	<100 ms	N x 5 Mb/s	no	yes	low	yes	medium
Tracking	<10 ms	N x 128 kb/s	no	yes	low	yes	medium
Database	<100 ms	>1 GB/s	yes	maybe	medium	no	high
Simulation	<30 ms	>1 GB/s	mixed	maybe	medium	maybe	high
Haptic	<10 ms	>1 Mb/s	mixed	maybe	low	maybe	high
Rendering	<30 ms	>1 GB/s	no	maybe	low	maybe	medium

Source: Rick Stevens, Argonne National Laboratory.

5. SCENARIOS

Group members describe several scenarios that cannot be implemented without the physical capabilities and the application technologies proposed for the NGI. Several scenarios like these should be selected for realistic implementation and analysis to begin the experimentation needed to define the NGI.

5.1 REMOTE INSTRUMENT CONTROL

Until recently, it was necessary for scientists to undertake expensive and onerous travel to use unique or rare resources such as particle accelerators, telescopes and satellite-observing stations. Such travel was needed to control the equipment, participate in initial data analysis and meet with colleagues. In some cases, remote access is already possible through the use of special circuits or low-bandwidth telephone lines. In the future, as the costs of equipment rise and ownership is more commonly national and even global, there will be a need for remote and collaborative access to these instruments.

As an example, consider several groups of astronomers working together to observe a short-lived phenomenon (such as a supernova burst). The groups need general network support because they will not have a chance to install special circuits. They need broadband access to the telescope data to make decisions about what object to observe next,

and they require reliable and secure access to the controls to avoid conflict or damage. They may need simultaneous access to major databases (the various sky surveys and historical records) or to other major instruments, such as the Hubble Space Telescope and the Arecibo Radio Observatory.

5.2 DISTRIBUTED SIMULATION

Today, simulation applications come in many varieties, ranging from those that simulate complex physical systems that already tax the largest supercomputers to those that generate virtual architectures for electronic commerce. Simulation systems sometimes span several computing complexes or local networks, taking advantage of high-speed connections between them. As equipment becomes increasingly complex, simulating the behavior and interactions of various combinations will require ever more computation. Currently, distributed simulation engines representing upwards of 10,000 independent entities are being constructed over geographically dispersed sites, requiring dynamic networked connections with impressive bandwidth (100 Mb/s or more). Distributed simulation applications usually operate in a peer-to-peer (server-server) mode rather than the more commercially common client-server mode.

A situation that would strain the most ambitious NGI plan would be a near-disaster on a space vehicle. Teams from dozens of manufacturers would need to lash together remote computing resources to simulate a variety of scenarios. After possible solutions are identified, there would be run-throughs of the repair that would require full-scale virtual (tele-immersive) simulations, both on the ground and in space, for the people who will do the work.

Today, such simulations and virtual reality presentations are accomplished using low resolution and frame rate. (The recent problems on the Mir space station were approached in an effective but rough-and-ready manner because such tools were unavailable.) In the future, it would be desirable to eliminate the risks that such poor fidelity entails. A solution would require bandwidths of at least a Gb/s for the immersive participants and another Gb/s of network capacity to connect the simulation engines. To meet tight deadlines, the whole operation would demand high security, as well as high availability and low delay.

5.3 ENVIRONMENTAL CRISIS MANAGEMENT

Managing a natural disaster (such as an earthquake, forest fire or hurricane) would require access to massive data sources. Needs might include detailed satellite images of large areas over periods of time, as well as reliable communications to crews in the field and in crisis centers. The information must be available as soon as possible, and the resulting decisions must be disseminated securely and immediately. Different combinations of

information, software and personnel would be involved in each disaster, and separate simulations and displays would have to be created on the spot to support the special needs. Thus, highly flexible computing, as well as trustworthy access to immense amounts of information, would be key elements in managing major disasters in the future.

5.4 PUBLIC INFORMATION ACCESS

One of the great surprises of the rise of the World Wide Web has been the use of Internet resources in schools, museums and libraries. People who would have had no direct access to large collections of information can now use them routinely. As citizen access to government and student access to distributed libraries grow, there will be a rapid increase in the need for broadband data access and, increasingly, direct (interactive) audio and video connections to officials and experts.

Events of national importance or interest are likely to cause enormous peaks of activity. National political debates will be watched by students across the nation, with simultaneous searches of databases on current events, politics and history. Teachers will want to show archival information and assign students to study related events. In practice, there will be many searches and accesses of the same sources; such surges will demand considerable bandwidth, multicasting capability and database power.

As citizen access grows, there will be a rapid increase in the need for broadband data access and direct audio and video connections.

A different kind of intense use would result from a nationwide collaborative project that might be sponsored by a coalition of museums and libraries. Tens of thousands of participants would interact to simulate a historical event or to create a large-scale model. The activity would require high-quality surround video and virtual modeling, as well as long-running simulation and persistent data.

5.5 COLLABORATIVE R&D

As resources become more distributed around the nation, and more diverse populations of researchers become involved, there will be a need for ongoing collaborations. Although much can be accomplished by occasional phone calls and sharing of files, closer activities (such as shared access to experimental information and equipment) surely will become the norm, rather than the very rare exception.

6. FUTURE DIRECTIONS AND REQUIREMENTS

To speed the arrival of high-quality applications that will satisfy mission requirements, researchers need to initiate significant experiments that simultaneously create applications, fundamental middleware and new networks. The experiments must be significant in size and have highly visible milestones and strict deadlines. The goals should be: 1) to study the applications and scenarios themselves, 2) to provide requirements for the downstream components of the overall NGI design, and 3) to acquire useful information on access patterns and possible engineering trade-offs. By planning several cycles of experiments, the risks of an inadequate design or a premature freeze on decisions can be reduced.

The sooner exciting applications can be demonstrated, the more confidence the community will have that the research investments will bear fruit and that the future national network infrastructure can grow.

B.2 MIDDLEWARE

Moderators: David Farber and Richard Schantz

1. INTRODUCTION

In addition to the technical merits of Internet protocols, many other factors have contributed to the explosive growth of internetworking over the past several years. The ease and simplicity of robust Internet protocols, and the openly available Berkeley implementation, certainly promoted their availability on a variety of platforms. Client-server computing, work-flow automation and cost-effective Ethernet technology were factors that led companies to wire their campuses. And the development of middleware application frameworks like the World Wide Web, databases, message-oriented middleware and distributed object computing environments has allowed a wide community of people to develop uses of both private intranets and the public Internet. These frameworks, which help promote the rapid development of valuable and entertaining uses for networking, will be a hallmark of the Next Generation Internet (NGI).

Middleware application frameworks like the World Wide Web and distributed object computing will be a hallmark of the NGI.

Middleware can be viewed as a reusable, expandable set of services and functions that are commonly needed by many applications to function well in a networked environment. These common services and management capabilities that promote end-to-end interoperability, security, integrity and resource management will be key to providing a trustworthy system, one that manages the conflicting demands of a growing, complex mixture of applications designed to meet the needs of end-users. The NGI will not address all the problems of software application development; however, an important consideration is how to factor the architectural framework to achieve end-to-end operations that are as robust and efficient as the current communication protocols on which middleware and applications are built. To this end, group members agreed on a guiding principle for designing such an architecture, which makes this proposal distinct from the popular current solutions: the definition of an extensible but minimal middleware kernel needed to promote the inclusion and substitution of an expanding set of customizable services. Additionally, it is clear that public and open standardization will be an important component of broad implementation and deployment, a critical issue for the middleware

architecture of the NGI. Although standardization may not be a goal of the NGI, it will be an important component.

In designing and building new NGI applications, and perhaps new sorts of applications, it is important to understand how to create them cost-effectively. These may be applications that provide functionality to new types of users or, more immediately, applications that take advantage of the large scale afforded by the Internet.

Two examples may be useful. Consider a vendor who wishes to sell the newest version of an extremely popular piece of software through the World Wide Web. The vendor offers purchases by credit card using secure http. In return, using a customer's public key, the company provides a private version of the software to the customer. The vendor has a set of extremely popular Web pages that provide both the order form and online documentation.

In the second example, a group of high school astronomy students, located at schools that are widely dispersed, collaboratively explore models of galaxies in which any student can modify the laws of physics. Perhaps the simulation engine is a supercomputer remote from any of the students. All the students see all the changes made by others; the system provides the ability to pass control from one student to another, as well as audio and image communication among them all. By allowing the laws of physics to be modified, the system provides a virtual reality that could not exist outside the system.

Astronomy students could collaboratively explore models of galaxies in which any student can modify the laws of physics.

These two examples highlight not only various aspects of middleware, but also features of middleware without which these situations could not exist. In the first example, the Web itself, in contrast with the browsers that provide the user interfaces, is part of middleware. In addition, the credit card information exchange and distribution of users' public keys are middleware elements. There are hidden services as well, such as the caching of Web pages to reduce the load on hot spots in the network. Without this service, not only might the server that is providing pages become overloaded, but traffic might overload certain parts of the network, making it unavailable to other users.

The astronomy students are dependent on the composition of the modeling facility with a multicast service that allows for shared control of the simulator, voice and perhaps the video links. None of these services or functions is part of the traditional Transport Control Protocol/Internet Protocol (TCP/IP) protocol suite. Nor would they be effective if each site implemented them in its own way. It is only because the services are available

to the community that they are effective. They are enabling technologies that must be provided by middleware.

It is more difficult to exemplify the creation of an infrastructure to support thousands or millions of applications on the network simultaneously or the collaboration among network-based components (e.g., running pieces of code). Although some forms of infrastructural services—such as some very early banking services and work on global naming and name resolution—are beginning to emerge, none is widespread. The Domain Name System is a global infrastructural service that is well understood to scale to the number of hosts, but certainly not to the many orders of magnitude large needed to name all objects of potential interest in the Internet.

There are even several competing efforts to provide network-based object models. What is required is a core architectural model that allows for commonality where it is needed and flexibility where variability and extensibility are needed. This model will provide the common base that currently is reinvented in each of many applications (thereby preventing interoperability), while allowing choices to be made by those applications where distinctions are important.

The remainder of this section discusses such a middleware architecture. It begins by describing a general architecture, including some central organizing principles. The architecture is further refined with a set of core services, functions and attributes, followed by research and development types of enabling technologies and concepts. The discussion concludes with a summary of programmatics.

2. GENERAL STRUCTURE OF MIDDLEWARE

Middleware can be viewed as an extremely simple "microkernel"—a reusable, expandable set of services and functions that many applications need to function well in a networked environment. These services often need to be used in various combinations with each other and with the variety of components built by application developers. To facilitate this function, middleware can be organized into three complementary parts:

- The "glue" or microkernel is the set of conventions and structures that allow the services to be combined with network and application functionality. The structures support the connecting of components in flexible, convenient ways, independent of where the items are located.
- Core services expand and control the set of services provided so they may grow (or shrink or be modified) over time without centralized administration. Core services also include those considered to be universally useful. While the functions are oriented

toward providing specific functionality (answering the "what does it do" question), attributes typically address the "how well" question. These aspects can be grouped under the category of "Quality of Service" because they deal not with the computational aspects of the application, but with the system properties and "feel" of the applications supported.

- Because group members anticipate that the set of services will expand as more applications need more services in common, the final category includes an ordering of service ideas beyond those needed to meet immediate application demands.

To design a coherent middleware model, group members identified an initial set of guiding principles. In an NGI research agenda, this list would need to be reviewed and refined. The principles include:

- *Minimality:* Base the architectural model on a microkernel approach, with extensions on top to accommodate the following principles.
- *Heterogeneity:* Allow for as much variation as possible, both below and above the middleware layer. Constrain functionality and services only where necessary for interoperability.
- *Longevity:* The growth of the Internet implies a growth in investment; this means that replacing the infrastructure becomes increasingly difficult. Therefore, the design must take a long-term view.
- *Evolvability:* If the model is to survive with Internet growth, it must be possible to change and enhance the middleware infrastructure to support the requirements of new applications and uses.
- *Location transparency:* To the degree possible (recognizing that it will always take longer to transmit information long distances than short), it should not be necessary to know about location. Location may change with great frequency, compared with the lifetime of at least some of the elements.
- *Modularity:* The best way to enable the composition and coordination of independent components is to allow for a clean and well-known separation, supporting abstraction as a means of hiding implementation and representation facts.
- *Efficiency:* Middleware is only an enabling set of features; as such, it must perform efficiently to avoid creating bottlenecks that will make the Internet unusable for desired purposes.
- *Observability:* An essential aspect of widely distributed systems is the ability to observe or monitor performance at every level of the application, at every location of distributed processing and data-handling components, and in the network itself.

This set of middleware principles needs to be reviewed in light of a comparable set of guiding principles that can be drawn from the applications and user communities.

3. SUPPORT FOR CORE SERVICES

Middleware needs to support certain core services related to current application needs and to organizing middleware services themselves. For discussion purposes, group members placed (somewhat arbitrarily) these core services into two main groups: functions and attributes.

Functions refer to services needed by applications and provided in a host-independent manner. Examples include connecting components, adding new components, naming and persistently storing items, and moving items around and finding them again. Attributes deal with properties that the "system" and "applications" themselves are supposed to have across the board, irrespective of the piece or pieces in question. These include services such as performance management, availability and dependability, security and access control, and services for managing time and adherence to external (to the system) time demands and requirements. Issues surrounding some of these services are briefly described.

3.1 CREATION, REMOVAL AND COMPOSITION

The Internet environment makes it desirable and necessary for applications to be composed of collections of modules, often built by different groups. Supporting and encouraging such development is more cost-effective because common components are used and reused. It must be possible to build distributed applications for large-scale data analysis from composable, high-performance modules, rather than building and tuning them from the bottom up every time a new variation is required.

3.2 MOBILITY, DYNAMIC LOCATION AND BINDING

Experience shows that systems constructed without provisions for easily moving and reconfiguring pieces are very difficult to use and maintain over time. The use of long-lived, globally unique identifiers that are independent of location is one solution. Within their lifetimes, many objects will move a number of times: their parent organizations may merge, split or dissolve; their home sites may become obsolete; new, improved schemes for handling them may be built; and so forth. The ability to embed a long-lived identifier into a link or other object without location or other semantic information implies that the meaning and use of the identifier need not change over the potentially long lifetime of the object. There is also a need to engineer separately a resolution mechanism, called "dynamic binding," to discover the location of the object when needed. Dynamic binding can occur at many stages of the program development and execution phases. However, a run-time dynamic binding mechanism is key to supporting run-time mobility.

3.3 PERSISTENT NAMING, STORAGE OF DATA AND CODE, AND LINKING

The capability to name, store and recall items is fundamental to all information systems. The Internet provides new dimensions to these features, including large-scale sharing, very-long-lived items, and many choices. Traditionally, names have provided three functions—identification, access, and semantics or mnemonics. One critically important feature that grew out of the Web experience is the ability to create links or relationships between objects. This idea can be extended in several directions. First, if links are first-class objects, they can link to each other. Second, they can also have more than two end-points, viewed as critically important to allow richer relationships. Third, by linking into the exposed abstract structure of their end-points, links are no longer dependent on a particular representation of their end-points. Lastly, by using unique identifiers, links can have a useful lifetime that is as long as any other object.

3.4 SECURITY: AUTHENTICATION, CERTIFICATION AND ACCESS CONTROL

Data owners must be able to impose conditions on the use of their data that are easy to specify and enforce. This requirement calls for security mechanisms that are generalized, distributed, transparent and strong. It should be possible to specify many different degrees and types of security, including none. Access control for entities must enforce the conditions of use imposed by the data owners. In addition, the access control needs to be easily available, administered, used and enforced; and it should be as distributed as the data, the data owners and the applications.

3.5 PERFORMANCE MANAGEMENT

A key issue for the NGI is the fragility of the applications with respect to the fluctuating resource base among multiple resource providers (both communication and otherwise). The immediate need is to provide services that can cope with the communication shortages and fluctuations, at the same time reducing the frequency with which performance problems occur (it is unlikely they will ever disappear entirely). Useful services that could be tailored to the variety of application needs through middleware include:

- Bandwidth management services and support for bandwidth-adaptive applications.
- Data compression to reduce network traffic demands.
- Caching to reduce unnecessary retransmission.

3.6 DEPENDABILITY, SURVIVABILITY AND REPLICATION

Beyond the performance effects of fluctuating or overutilized resources, there is the lack of dependability when key resources become unavailable or unusable. The network itself provides many alternatives when failures or shortages occur in one area, but it lacks the

organized (middleware) support for detecting, isolating and managing these failures. Ultimately, recovery is always based on some form of redundancy (a simple method being complete replication). With replication services, critical items are kept in multiple, up-to-date copies with provisions for switchover when failures occur. The main task for the middleware is making this service easy for Internet applications to embed and organize around the specific dependability needs of each application. A malfunction or corruption of a single implementation of some critical resource management function, if used throughout the Internet, often can result in a disastrous chain reaction. This possibility argues for policies that support significant heterogeneity in key resource areas in order to construct more dependable Internet-based applications.

> The network lacks the middleware support for detecting, isolating and managing failures or shortages.

3.7 TRANSACTIONS, TEMPORAL KNOWLEDGE AND TIME SERVICES

Transactions are important as a component of the services needed for multiparty communication, as well as for other purposes. Transactions allow for the clean success or failure of a coordinated activity, without exposing intermediate states. Transaction management services are beginning to appear, but transaction models need to be incorporated into a coherent model rather than being an "add-on" service. Many types of transactions have deadlines and/or operate on data whose validity expires with time, implying a need for timely transaction processing. New and effective scheduling algorithms have been developed that modify transaction priorities based on data and transaction deadlines, forcing transactions to delay processing if data are about to become invalid. In conjunction with improved notions of close similarity of value, transactions may proceed and commit if conditions are adequate, although not necessarily perfect. This capability allows transactions to be processed in a much more efficient and timely manner, especially in overload or crisis situations.

Temporal knowledge will also become more important with the need to provide real-time performance in various ways. Examples include commodity (open) real-time performance, quantifiable real-time performance, and maintaining the temporal validity of data. There is likely to be frequent composition of middleware services that support very dynamic applications. The real-time constraints of one or more components will create related time constraints on the composed whole. In a truly useful middleware environment, off-the-shelf commodity parts, each with real-time properties and controls, will be composed to meet overall real-time performance requirements. In turn, real-time performance will also have to be quantifiable and supplied at various levels of the system with

various levels of attempted guarantee, leading to designs with layered dependencies on performance guarantees and notification. Lastly, some data in the NGI, such as data collected from sensors or time-stamped (stock data), will include time intervals during which the data can be considered valid. The system must be able to keep such data valid continuously and to discard untimely data, perhaps as it is being conveyed. The resolution and dependability of network-based time services is central to this functionality and is being improved with ongoing research.

3.8 OTHER SERVICES

Group members identified a number of other services, including: configuration management; system management; ultra-large-scale storage repositories; cataloging; other forms of third-party meta-information; and support for agents as active knowledge creators and users.

3.9 OTHER ATTRIBUTES

Other important NGI middleware attributes were discussed by group members. While these are not elaborated here, they are listed for future consideration:

- Self-identification and self-description of the encapsulated abstraction of network-based objects, services and resources to enable more effective composition.
- Descriptions of the performance, implementation and representation of instances of objects, services and other resources to enhance selection and brokering among alternatives.
- End-to-end legal assurances and adjudication of disputes.

4. ENABLING TECHNOLOGIES (R&D) AND CONCEPTS

In this section, group members discuss several services and concepts that will provide immediate and high payoff by enabling broad development and deployment of new models of applications.

4.1 MULTICAST: GROUP OR MULTIPARTY COMMUNICATION AND AGGREGATION NEEDS

The vast majority of current production applications and application-level protocols are based on the assumption of the ubiquitous availability of reliable point-to-point transport services, as represented by the transmission protocol TCP. Using multicast as an alternative, perhaps with collaborative control of multicast transmission, will offer an opportu-

nity to explore an extensive range of new applications. Even within the research community there is still disagreement about whether multiparty communication should be an extension of two-party communication, or whether two-party communication is a simplification of more general multiparty communication.

Internet Protocol (IP) multicast as currently specified, even with the results from ongoing research, will be inadequate because: 1) application-to-application (end-to-end) multicast is required, rather than host-to-host; 2) higher-level semantics, such as synchronization of delivery, control of group membership, security and other policy controls, will become increasingly important features; 3) the interactions between multicast, multiparty communications and object replication schemes are not yet well understood; 4) policy control (for security, pricing, ownership, etc.) of the routing in the network may only be known by the applications, although it will have an impact on routing in the lower layers; 5) the ability (or lack thereof) to aggregate so that network resources and behavior (such as latency) can be managed more effectively, while still meeting the requirements of points 1 through 4 above, will continue to be a challenge. Establishing the ubiquitous availability of an appropriate multicast protocol or protocols as one of the engineering goals of Internet 2 will offer the opportunity to explore an extensive range of new application designs that employ group-oriented services as a fundamental component.

4.2 QUALITY OF SERVICE INTEGRATION ARCHITECTURE

Quality of Service (QoS) can be used as an organizing concept for integrating a number of otherwise separate attributes of the interactions between distributed components, beyond their functionality (e.g., the performance expected, the dependability, etc.). To do this, it is necessary to develop an overall framework of models, languages and protocols that permits distributed applications to specify desired QoS levels and to negotiate acceptable trade-offs and confidence levels. The algorithms that permit translation of high-level, application-specific views of QoS into low-level constraints on individual resources or services will need further development. There is also a need for monitoring technology that continuously measures delivered QoS and notifies applications when QoS "contracts" can no longer be honored and need to be renegotiated.

4.3 SEMI-TRANSPARENT SESSION LAYERS AND SERVICES

To provide effective end-to-end QoS, the QoS architecture must be populated with a new generation of layered, distributed system software that overcomes the limitations, while preserving the benefits, of layered abstractions. These "translucent layers" will augment traditional functional interfaces with control interfaces to permit higher layers to impose QoS or administrative policy constraints, or impart information necessary to meet the needs of higher levels. Dynamic adaptation mechanisms must be developed to permit lay-

ers to respond to negotiated QoS or to other policy constraints (propagated through the control interface) and environmental conditions. Special emphasis will need to be placed on supporting real-time reliability and security constraints, and on innovative designs that efficiently integrate communications and computation to satisfy application-specific requirements.

4.4 DYNAMIC MONITORING AND ADAPTIVE RESOURCE MANAGEMENT

From time to time, the level of available resources is likely to vary significantly. It will be necessary to have the ability to monitor and collect information on the status of resources, maintain a consistent distributed view of that status, profile applications to permit them to be mapped onto the most appropriate available resources, and dynamically allocate and schedule resources to meet end-to-end QoS constraints. Researchers will need to develop algorithms and resource management technologies to permit: 1) dynamic discovery of resources; 2) dynamic near-optimal allocation of heterogeneous resources to applications, balancing each application's end-to-end real-time QoS constraints against overall efficiency and fairness criteria; and 3) rapid dynamic reconfiguration in response to failures, workload variations, information warfare attacks or crisis response demands. Dynamic monitoring and reporting to applications when conditions change will also allow the option of adapting to changes, if the applications are so designed.

4.5 BROKERING AND NEGOTIATING TECHNOLOGY FOR MATCHMAKING

Constraint analysis, brokering and matchmaking are not new concepts. However, the new levels of understanding of knowledge and analysis achieved by continuously activated agents and avatars (or surrogates) have the potential to coordinate and negotiate for services and activities. Such automated services are capable of managing what otherwise may be, from the human user's perspective, unmanageable complexity. Simultaneously, the provision of many of the services and functions described earlier will enhance the capabilities of such agents, allowing them to act as more and more intelligent "middleware middlemen."

For example, intelligent matchmakers will connect users or other agents with appropriate products, services, programs or information. Matchmakers may also procure information for their clients from other matchmakers, and seek compromise solutions for multiple clients. Intelligent matchmakers can be regarded as a third-generation tool for Internet accessibility, where hypertext constitutes the first generation and search engines the second.

5. PROGRAMMATICS

The long-range, overarching goal for the NGI is systematically to lower the barriers to constructing Internet-centric applications through the use of middleware that supports open-architecture, robust, mission-critical applications that interoperate and coexist in the form of thousands of different applications. Group members see this happening in one-year, five-year and longer epochs, each building on the previous one. After one year, group members would anticipate supporting a common middleware framework, the microkernel, with a few important services of immediate need (e.g., replication, caching and data compression), along with the critical foundation for bootstrapping new services and integrating a number of QoS issues (e.g., bandwidth management). After five years, group members anticipate a large number of competing implementations of key services. The marketplace will then choose several options that will become universally available, and the group predicts a high degree of integration and interoperation to allow a complex organization to use the Internet for mission-critical operations. Beyond five years, group members anticipate that agents and avatars will be capable of negotiating with providers on behalf of users within this electronic marketplace of services to enable an order-of-magnitude improvement in the transparency of this environment. One of the major vehicles for achieving commonality is through the standards-setting process, which therefore deserves ongoing support.

B.3 QUALITY OF SERVICE

Moderator: Stewart Loken

1. INTRODUCTION

The Internet was initially conceived and implemented as a centrally supported, shared resource. As demands increased, they were usually addressed by increasing the available resources. In that environment, a single class of service, often called "best effort," was implemented that provided everyone with equal rights to the available resources. With the emerging needs of time-sensitive applications, together with an explosion in the size of the user population, it is no longer feasible to meet demand simply by adding bandwidth. In this new environment, any conceivable amount of additional bandwidth could easily be consumed by networking clients. As a result, new ways must be found to determine who gets service when networks become congested.

The commercialization of the Internet will ease this problem somewhat. Equal treatment on the Internet is no longer assumed. It is now possible to take a "want more, pay more, get more" approach through actual payments, accounting against priority tokens, peer pressure or the requirements of funding agencies and other groups.

Many applications—such as real-time conferencing, network-based collaborative work, facilities online and telemetry—need a level of service that is better than best effort. These are often very-high-performance scientific applications that are critical for meeting the requirements of mission agencies (e.g., Department of Defense, Department of Energy and NASA). Many telemedicine and educational applications also require a similar level of service, as do a number of emerging high-availability commercial and industrial applications. The latter include backups of financial, inventory or manufacturing data; shared, immersive environments; and time-critical applications such as just-in-time warehousing and manufacturing. The new electronic commercial applications have business-critical performance metrics that Quality of Service (QoS) must provide or businesses will continue to use dedicated lines.

QoS also will stimulate new applications (e.g., aircraft design codes) that have never been tried or perhaps even imagined. Unless the Next Generation Internet (NGI) can meet the high demands of applications like these, the result could be the creation of multiple networks. An Internet that supports QoS will not only add value, but will also reduce overall costs and improve service reliability. Different levels of prioritization, including national security requirements, must be supported by QoS. This feature may be especially critical when networks fail. A major issue, however, is how to meld the administrative authorities of government vs. financial control.

Service prioritizations in commercialized component networks of the Internet are beginning to emerge. The selected approaches are usually in the best interest of the specific component network, and may not work well at the systemic level of the Internet. Specifically, in a non-standardized environment it is difficult for multiple service classes to ensure predictable end-to-end performance across multiple administrative domains. Since the NGI needs to stress interoperability at a systemic level, it may not be appropriate to accept approaches that work mostly within the confines of a component network. The NGI initiative should investigate what approaches are being taken and work with vendors and service providers, but drive the solution space to a systemic level (i.e., make sure answers are applicable to the national and global Internet). It will also be important to investigate the needs of specific demanding applications, including needs versus simple desires, and determine whether the actual or anticipated pervasiveness of those applications justifies changes to the architecture.

Until very recently, a characteristic of the Internet was that the participation of those desiring network connectivity was nearly universal. Now, users requiring assured service at some level tend to establish private networks, which may reduce the efficacy of network connectivity. Because of this trend, group members think it is particularly important to explore in some detail the service expectations of, for example, the medical and financial communities. With these expectations in hand, a multilevel QoS research/economic plan can be developed to maintain near-universal connectivity with all of its benefits.

2. RESEARCH CHALLENGES

Group members identified a number of important R&D topics for consideration.

2.1 RESOURCE ALLOCATION

Flexible mechanisms must be created to translate management decisions on resource allocation, via authoritative adjudication, into network behavior in real time. These are needed for brokering bandwidth to meet QoS requirements, flow control and admission control.

- Admission control should ensure that QoS requests are not overallocated, via authentication. Whether QoS is controlled by receiver and/or sender remains unresolved.
- There must be end-to-end support for QoS. This will entail QoS quality routing, circuit setup and architecture issues across interagency boundaries and backbones. There must be QoS in operating systems and applications.
- The QoS model presented to users must be user-friendly and specified by users in the context of their work (whether commercial, scientific or military). These specifications must then be translated into an implementation plan, which should result in the creation of a physical communications structure that implements the administrative QoS decisions over the network topology. The final result must ensure successful commercial deployment.
- The R&D program must address how cross-network QoS requests are handled and how failures are handled (both technically and administratively).

The required technology must provide a billing and settlement infrastructure that supports negotiation and financial settlement of QoS agreements. In the absence of such an infrastructure to ensure that the provider will be compensated for providing enhanced service quality, no rational network service provider will do so. In turn, this provides a fundamental measure of success: significant progress has been made in the QoS area when an Internet user can purchase enhanced QoS in an end-to-end fashion, without resorting to the dedicated-line approach of private networks.

2.2 NETWORK CONTROL

How does one determine who is misbehaving on the network? Tools are needed to find the problem and define its source. These diagnostic tools should be built into the network. Some important examples include:

- Fault information and tolerance (including busy signal equivalents).
- Interoperable trouble tickets to manage an interoperable QoS environment.
- Inter-realm authentication.
- Maintenance of QoS across administrative boundaries.

2.3 MULTICAST ISSUES

How does one implement access control in multicast sessions, and what is the economic model (e.g., receiver-based billing)? The economic model should enhance the scaling of the Internet.

2.4 AGGREGATE QUALITY OF SERVICE

Many actual and envisioned uses of the Internet exhibit QoS requirements that span multiple connections and/or interactions, each of which may be rather short lived. For exam-

ple, electronic commerce motivates a seller to obtain service guarantees for all customers who access the seller's site; this is analogous to the ability of a merchant to buy sufficient Wide Area Telephone Service (800) bandwidth to ensure that customers will not encounter busy signals. Current QoS research and technology (e.g., RSVP) have focused on service assurance for individual connections over which a large quantity of data can be expected to flow. Fundamental research and technology development is necessary to efficiently provide QoS guarantees over connection aggregates where each connection may be short lived.

2.5 PROTOTYPE SYSTEMS

R&D must include the development of prototypes that allow various test implementations of QoS. A prototype must be provided that is large enough to allow for the testing of cross-hierarchical failures, and of multicast across networks and architectures.

2.6 SIMULATION

Improved quantitative understanding of the network would be useful and might be available from improved research tools. Simulation needs to be investigated as a suitable tool—the NGI should provide the needed testbed. Topics include:

- The effectiveness of simulation.
- Simulating the effect of application requests for QoS.
- Developing and validating the QoS model.
- Modeling an environment to simulate QoS over various architectures.

2.7 ECONOMIC MODEL

Given a scarce resource (network or funding), how does one express values related to prioritization and how does the network discern the resulting prioritization; and what is the time frame of such decisions? Group members recognize that this is an issue that is administratively or socially driven that may be expressed monetarily over some billing cycle. There is a need to define an economic model to promote infrastructure growth. Numerous billing issues need to be resolved under any business model so that customers get what they pay for.

Group members believe that an R&D program in QoS must address these critical issues. The work product of this activity, in collaboration with industry, has to be a stabilization of the performance predictabilities on the current, real-world Internet-at-large, not only on confined agency networks.

B.4 INTERNET TRAFFIC ENGINEERING

Moderator: Kim Claffy

1. INTRODUCTION

Internet traffic engineering has several characteristics that set it apart from other parts of the Next Generation Internet (NGI) initiative:

- It is an essential component of any infrastructure supporting other NGI areas.
- It has begun to receive attention within the operational Internet infrastructure from the Internet Service Providers (ISPs) themselves, although the attention is somewhat late and narrowly focused.
- It is confused at times with the field of network management, and often is perceived as less charming than other research areas.
- It is extremely difficult, if not impossible, to make reasonable progress without access to actual traffic data. Such data are difficult to come by without the consent of providers and a great deal of effort on their part, if they can provide data at all.

Internet "operations research" is perceived as neither, and thus does not receive intellectual or fiscal attention from either providers or research funding agencies. After more than two decades of Internet evolution, there is little methodology or even a set of intellectual or software tools available for characterizing Internet workload or performance, much less engineering a large-scale, multiprovider Internet infrastructure. Commercial ISPs continue to run their ever-thicker clouds by guesswork and intuition. They would welcome a set of tools to facilitate their interaction with the rest of the Internet, yet there is no indication that such tools will emerge from industry on its own. On the contrary, competitive market pressures and antitrust sentiments actually create disincentives for ISPs and vendors to cooperate and collaborate on engineering tools. This situation is one where the government can play the best of all possible roles—it can leverage modest funding to sanction and encourage industry to invest more funding in cooperative endeavors.

2. DIMENSIONS OF COMPLEXITY

ISPs struggle to keep pace with a workload that is increasing in several dimensions: the number of end-users, bandwidth per user, range of new and future applications, demand from customers for stronger predictability, and the internal need for greater efficiency as raw fiber capacity is squeezed to its limits.

To encourage commercial collaboration with NGI-funded research, the objectives must be applicable to the actual, evolving Internet.

To encourage commercial collaboration with NGI-funded research efforts (and government funding would be ill-advised without such collaboration), research objectives must be applicable to the actual, evolving Internet. In particular, traffic engineering research must create the mechanisms for making the future ubiquitous Internet efficient and robust for the next generation of transport technology, application requirements and constituents.

In this report, traffic engineering is discussed in terms of two principal components: 1) measurement (how do we know, what do we know), and 2) network modification and evolution in response to measurement (what do we do with what we know).

Two underlying principles are described:

- Both observation and modification span a wide range of time scales.
- Modifications may entail a change in logical behavior or in physical resources.

Traffic engineering jointly supports the effective, cost-efficient provision and expansion of Internet service through:

- Fault localization and identification.
- Provisioning and capacity planning.
- Identifying/directing responses to overload conditions.
- Improving the aggregate performance knowledge base for designing or redesigning Internet architecture.

To perform these roles, Internet providers, network managers and the research community must have consistent, accurate measures of various metrics of Internet performance and traffic. These measures cover not only the properties of individual flows and paths, such as throughput, loss, delay and jitter, but also broader scaling properties such as availability, reliability, fault resilience and resistance to intrusion or attack.

In the Internet infrastructure, measuring workload and performance extends beyond the role of conventional traffic engineering; well-designed measurement tools can assess and modulate performance at both the user and application levels. Indeed, this goal must be a vital consideration in the selection and design of specific metrics and the procedures for applying them. Examples of these additional roles include: provider rating, provider and access selection, pricing, advertising, contract definition and enforcement, quality-based routing, and research on the adaptation of network behavior applications to network performance.

Dissemination of measurement information is as vital as its acquisition and requires a stable infrastructure to distribute the appropriate information to the appropriate locations, such as operations centers, network architects, adaptive applications and end-users. Despite the wide scope of measurements needed, and the equally wide variety and location of extant tools (with widely varying timeliness constraints), it is essential to gather and dispense information in a way that ensures minimal impact on the network and the applications.

3. NGI TRAFFIC ENGINEERING PRINCIPLES

NGI-sponsored traffic engineering technology must support good practice and policy. Pursuing this goal—in the face of unanticipated future technologies, applications and user needs—will require:

- Extensible tools and data formats.
- Integration of data selection and analysis with routing, configuration and policy specification.
- Scalable measurement across a wide cross-section of the current Internet and the networks described in Goal 1 of the NGI initiative (see Box 1 in Summary).

Research must be guided by principles for both measurement and engineering.

3.1 MEASUREMENT PRINCIPLES

Measurement should provide for:

- Better engineering.
- The use of low-impact techniques.

- Incremental measurement and deployment, with algorithms to exploit existing data as well as to determine the minimal additional measurements needed for likely expanded requirements.
- Voluntary association.
- Self-discovery of measurement database(s) and peers.
- Distributed, cooperative implementation; statistical sampling.
- Timeliness.
- Meaningful aggregation across scale of detail.
- Resource accounting, allocation, profiling, and service models.
- Extensibility and configurability.
- Use/development of a set of standard metrics and tools.

To realize these goals, a measurement infrastructure must support:

- Configurability.
- Policy control, including data sanitizing and controlling access to data and configuration control.
- Local ownership of tools and databases.
- Autoconfiguration of tools to determine, for example, who is close by and the aggregation level.

3.2 ENGINEERING PRINCIPLES

Traffic engineering requires:

- Provisioning that reflects traffic needs.
- Routing mechanisms to express policy.
- Coherent mechanisms for implementing traffic engineering decisions.
- Feedback from performance measurements to traffic engineering at various time scales.
- Closer integration of policy, forecasting and measurement.
- Support for incremental network change (in the short and longer term).

4. CURRENT AND FUTURE ENVIRONMENT

Two recent examples of rapidly expanding traffic demands raise complicated issues:

- *Mass-market entertainment with its challenging workload characteristics*: its traffic is highly diverse; it involves the simultaneous use of multiple technologies, depending on level of interactivity; it has embedded different levels of relative intelligence of client and server; and it includes technology to support applications that measure and respond to network and server performance themselves.

- *Publication, distribution, and transactions such as software distribution, pay-per-use video and online catalog shopping.* Software distributors already experience transient traffic increases by a factor of 20 for several days following version releases. The popularity of intellectual property delivered online is growing and threatens to create traffic overloads if tens or hundreds of millions of end-user applications download information (sometimes automatically).

Such demands on the current Internet were not anticipated even a few years ago, and the next wave of application patterns will be equally difficult to predict. However, the direction of traffic engineering research must be responsive to the unexpected uses that will develop as a result of enhanced capacity, performance and reliability of the network. New applications and technologies will be deployed whether or not they are anticipated, and the measurement infrastructure must be able to detect their effects and trigger flexible responses.

The direction of traffic engineering research must be responsive to the unexpected uses that will develop.

5. RESEARCH AGENDA

The research challenges listed below address specific concerns and opportunities for building a measurement and engineering foundation for the NGI. What needs to be measured in order to evolve access and transport technologies? How do we model, plan, provision and manage a stable NGI in the face of evolving underlying technologies?

5.1 OBTAINING DATA

Traffic engineering data include measurements of network availability, reliability and stability, as well as traditional measures of loss, throughput, delay and jitter. Research challenges include:

- The need to develop the most efficient architecture for minimal collection, distribution, archiving and accessing of data, including methodology, tools, algorithms, and database structure to hold observations at a wide range of temporal and spatial granularity.
- The need to determine what levels of testing are essential and tolerable (nothing is “low impact” if 100 million people do it at once) and how to reconcile monitoring with privacy issues.
- Parasitic or passive monitoring to reduce the need for active measurement.

- A benchmarking suite for provider/performance comparisons.
- Support for an independent testing organization and cooperative interprovider measurement.
- Dynamic adaption of measurement type and volume.
- The need to scale monitoring technology and tools to very-high-speed networks and applications.
- The need to consider the emerging transparent, all-optical network architectures, where traffic is switched optically and intervening network elements do not have access to the contents of the traffic channel at all.

5.2 INTERPRETING DATA

Analysis is the art and science of interpreting measurements, and developing the discipline of Internet data analysis will involve many components:

- Identifying meaningful, application-independent units of traffic to measure and model.
- Aggregating detailed measurement data and identifying the utility of levels of aggregation for different purposes.
- Handling the aging of data: working with inconsistent, incomplete, delayed or variable time-resolution data.
- Extrapolating to longer and shorter time scales.
- Capturing topology and its effects on interpreting data, including tools to automatically discover topology and configuration information, present and distribute it in a consistent, extensible format and use it to interpret and act on actual measurements.
- Detecting and diagnosing anomalous behavior.
- Providing utilities to post-process collected data, using a consistent format across network components. This task is more like filling a gap than actual research, but is essential to accelerating the technology transfer of NGI traffic research.

5.3 RESPONSE

Collecting and analyzing traffic behavior is of little use without tools that respond appropriately, enabling networks to recover from failures quickly, stably and automatically. Research challenges include the need for:

- Useful reporting to providers, site administrators and end-users in formats that support differentiated service contracts and facilitate routing and planning.
- Routing protocols to allow consistent, predictable responses to traffic behavior.
- Configuration tools to reduce human error and avoid unintended interactions among network elements.

- Fault localization tools to automatically identify errors, failures, unanticipated traffic and possible attacks.
- Automatic fault recovery and resilience with either precomputed fallback modes or dynamic route optimization and load balancing.
- Algorithmic methods to route traffic flow aggregates.
- Deeper understanding of traffic engineering dynamics to control fault scenarios and congestion.

5.4 LONGER-TERM EVOLUTION

In the longer term (5 years out), tools are needed to support:

- Design and engineering across levels of detail to support incremental change, multiple transport technologies, higher-level network performance requirements, fault tolerance and cost-effectiveness.
- Realistic simulation, emulation and forecasting.
- An "I-erlang," or some analog of the Erlang metric used in telephony, to characterize high-level Internet traffic in an application-independent way; a prerequisite to this task is acquiring a deeper understanding of how proposed characterizations depend on the nature of the dominant applications.

5.5 RECOMMENDATIONS

Achieving NGI performance goals in the context of a cost-effective, high-performance information infrastructure for the national commercial, education and research communities will depend on (and could be constrained by the absence of) several elements:

5.5.1 *The NGI and other government-sponsored testbeds must be open to traffic measurement and performance monitoring by the research and user communities, and must be instrumented to support traffic engineering research.*

5.5.2 *A basic set of standardized, unambiguous performance metrics is needed to support objective study and comparisons. To encourage the evolution of increasingly accurate, low-impact techniques, metrics should not require a specific tool or procedure, but each metric should have at least one feasible measurement technique.*

5.5.3 *The NGI initiative must promote the use and availability of such metrics and tools not only within the networks defined in Goal 1 of the NGI initiative (see Box 1 in Summary), but also throughout the existing Internet where legitimate core backbone data*

from multiple providers offer more rigorous testing and verification.

5.5.4 *Long-term analysis, profiling and performance comparisons imply the archiving of measurements, subject to necessary privacy and nondisclosure constraints.*

5.5.5
The NGI must support the development of:

- *Low-impact Internet measurement techniques.*
- *Traffic models that can incorporate such measurements into the design, engineering and operation of high-performance networks.*
- *Tools for fault identification and recovery based on such measured data, whether the disruption was caused by component failures, traffic load or a malicious attack.*

5.6 IMPORTANCE TO THE NATION

In addition to preserving U.S. technological leadership and providing critical support for NGI research, Internet traffic engineering will also foster competition for reliable, available, efficient, high-quality service. As U.S. economic and educational competitiveness grows more dependent on the Internet, the demand for performance and reliability increasingly will outstrip the supply. And experience has indicated that even a safe margin of overcapacity alone cannot protect against what will be increasingly visible stress modes: network failures, high-amplitude traffic variability, feedback and unintended interaction among applications, configuration errors and directed attacks. Robustness and reliability will continue to elude the infrastructure unless the data, tools and methods available for traffic engineering are expanded significantly.

5.7 GOVERNMENT SUPPORT IS VITAL

There are a number of reasons why government support for Internet traffic engineering research is critical:

5.7.1 *Historically, the definition of standards essential to commerce has required the active support of governments.*

5.7.2 *The thousands of separate networks that make up today's Internet have little economic incentive to individually devote resources to developing consistent, universal traffic engineering standards.*

5.7.3 *Unfortunately, individual network operators have at least two incentives to avoid publishing traffic and performance data: 1) the lack of standardized testing and reporting methodologies may expose them to potentially inaccurate comparisons, and 2) exposing*

failures unilaterally, especially when competitors are not doing so, puts them at a marketing disadvantage.

5.7.4 *Although there are independent enclaves of traffic engineering research, there is no motivation for coordinated study. The rapid and sometimes chaotic growth in the heterogeneous Internet requires objective, neutral solutions beyond the scope of any single provider or consortium of providers.*

5.7.5 *These complex issues require longer-term research to create the underlying understanding and techniques. Individually, no single segment of the fragmented Internet industry can address traffic engineering from the perspective of a larger Internet system. Collectively, with the encouragement of NGI research sponsorship, it is possible to use a broadly based government, academic and industry research approach to address the macroscopic longer-term issues.*

The history of Internet research has demonstrated the viability of leveraging a focused research funding package to accomplish significant long-term public interest goals. Indeed, several agency efforts already have provided the community with critical components and prototypes of the evolving infrastructure. Because these efforts have demonstrated sufficient benefit to a critical mass of providers, organizations and end-users, the advances have harnessed market forces to expand their scope.

B.5 SECURITY

Moderator: Stephen Kent

1. INTRODUCTION

The current Internet is rife with security problems. Viruses and hacker attacks are commonplace. Attacks causing denial of service have struck public World Wide Web servers, and benign configuration errors have left large portions of the Internet population without service. Many commercial uses of the Internet are inhibited because of concerns about the lack of security. At the same time, Department of Defense plans call for increased reliance on public Internet technology for critical systems. A coordinated, large-scale attack on the network could cause a lengthy service disruption for millions of users, seriously undermining confidence in the technology as a basis for future development. What will happen when new technologies and protocols are deployed in support of the Next Generation Internet (NGI)?

> Security problems are likely to worsen when new technologies and protocols are deployed in support of the NGI.

The answer is that these problems are likely to worsen. Some are a direct result of the increased bandwidth offered by the NGI network infrastructure, the increased computing resources available to subscribers, and the new applications that will use the NGI. However, many security problems are independent of these changes that mark the NGI as distinct from the current Internet. Some arise from general trends in computing and networking that also will be manifested in the NGI. Others are old problems inherited by the NGI that will not simply disappear.

So who will fund the research that is so critical to solving these security problems? Group members believe that industry will not invest R&D dollars for several reasons:

- Industry is concerned about maintaining a competitive edge in the marketplace, and generally concentrates on adding fancy new features to products. These additions create new opportunities for bugs that have adverse implications for security. Time-to-market pressures conflict with ensuring adequate security.

- Industry R&D on security has focused on point solutions that are not adequate to solve large-scale security problems or problems that cross product lines.
- Sometimes the government adopts a technology early or deploys a technology on a much larger scale than the commercial sector will achieve for some time. In such cases, industry cannot be relied on to fund the R&D required to solve the security problems encountered by early users.
- Industry has borrowed heavily from government-funded research. Industry builds COTS (commercial off-the-shelf technology) based on the low-hanging security fruit, which is the result of millions of dollars of government-funded research.

Group members believe that if government funding is not provided for security research, industry will not step in to fill the gap. The outcome would be an NGI that is even more vulnerable to security breaches than the current Internet.

A list of ten security research topics was created and prioritized by group members. Each area is considered appropriate for federal R&D funding. The prioritization was developed by voting and is subjective. However, it represents the views of the experts from industry, academia and government who attended the NGI workshop. The list of research challenges, in order of priority, includes: infrastructure robustness, security policies, mobile code, intrusion detection, public key infrastructure, security management, cryptography, operating system security, software engineering and network management.

If government funding is not provided for security research, industry will not step in to fill the gap.

2. RESEARCH CHALLENGES

2.1 INFRASTRUCTURE ROBUSTNESS

The current Internet is highly vulnerable to attacks that deny or degrade service to large numbers of subscribers. Reports of malicious attacks against the routing infrastructure are few, but several accidental errors have caused serious outages. The NGI will likely be based on the same routing protocols used in the current Internet, and thus these vulnerabilities are likely to persist. Recently there has been a modest amount of R&D on routing protocol security, mostly dealing with Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF). Most of this work addresses the integrity and authenticity of the routing protocol messages, and ongoing work is adding authorization to BGP to help

complete the picture. There has been, however, relatively little technology transfer; thus, there may be a need for federal funding to promote adoption of this technology in the marketplace.

Other security aspects of infrastructure robustness are not being addressed. For example, countermeasures to blunt attacks that exploit the self-healing aspects of network control algorithms, or congestion control algorithms, are not being investigated. If intrusion detection mechanisms are deployed in the NGI, opportunities will arise to exploit these mechanisms (e.g., by generating false alarms that can consume resources and overwhelm operators). Multicast and Quality of Service (QoS) mechanisms are likely to be supported in the NGI, but there are no authorization mechanisms to allow secure implementation of these features.

Group members observe that homogeneity in systems can lead to greater (common mode) vulnerabilities, but heterogeneity in systems is harder to manage. The commercial trend is towards platform homogeneity (e.g., Cisco and Microsoft). Lastly, the holy grail of robustness, graceful degradation in the face of hostile attacks, remains an elusive goal.

2.2 SECURITY POLICIES

Current security policies tend to be rather static, hard to manage, hard to adjust, crude (coarse-grained) and not directly under the control of end-users. These policies often are enforced by access control mechanisms, which are administratively directed, in firewalls and servers. This approach usually leads to one of two outcomes:

- Sharing of information among users, especially across administrative boundaries, is inhibited because the mechanisms are not responsive to users' needs and are difficult to administer.
- Users are able to share data freely across these boundaries, but intruders also gain easy access to the same data; thus, the data being shared are not significant in either quality or quantity.

To address these problems, R&D is needed to improve access control technology, with an eye toward improved management interfaces. There is general agreement that more dynamic, fine-grained access controls are required, yet such controls will be even harder to administer unless there is a substantial improvement in technology. Research is needed to provide users with the increased flexibility required to express and enforce access control policies that are more dynamic and fine-grained, consistent with overall administrative directives, while substantially improving the management interface for such controls. This is a difficult problem; it touches on areas of operating system security that have resisted practical solutions in the past. For example, without trusted path mechanisms, mali-

cious code can act with the assumed authority of an authorized user and grant inappropriate access to intruders. Also, the ability to provide fine-grained access control that is easy to administer has proven to be an elusive goal. The ongoing work in strongly typed language environments (e.g., Java) may help, but it is still too early to tell. Some feel that the level at which these mechanisms operate is still too low.

2.3 MOBILE CODE

Increasing interest in Java, ActiveX and intelligent agents creates many security concerns, most of which are just beginning to be examined. For code imported into a local environment (typical of Java and ActiveX), the problems focus on specification and enforcement of security policies relating to containment or confinement. This is also relevant to security policies, in that the ability to define and enforce fine-grained access control policies often is cited as a prerequisite for effective security in the mobile code environment. The granularity of access control required here may be comparable to, or even finer than, that required for the collaborative data-sharing alluded to above, depending on how mobile code is used in the NGI context. Again, the problem of specifying the access control policy, as well as enforcing it, is a critical one. Also, the need for very local, dynamic management of these policies is crucial because they must be enforced on a per-workstation basis, relative to each mobile code module. Group members noted that most models for mobile code security do not address denial or degradation of service concerns, and thus there is room for additional research here as well.

In this context, a research area with potential promise is that of "proof carrying code." This mechanism makes the mobile code developer aware of the containment or confinement security policy under which the code will execute. The developer then generates a proof that the code is consistent with the policy, and attaches the proof to the code. This proof can take the form of traditional formal method proofs, or it can be expressed in terms of explicit, run-time checks applied to the code to ensure conformance to the policy. Prior to executing the code, the proof is verified locally under the control of a user or local administrator. If the code is modified after the proof is generated but before it is validated, the proof will fail, and thus this technique is immune from such tampering. There has been only limited experience with use of this concept, but it seems promising.

Lastly, a more advanced form of the problem associated with mobile code security arises in the context of intelligent agents. These mobile code modules are sent out by users to gather information, perform various tasks on behalf of users, and the like. In contrast with the mobile code model commonly used today, where modules are usually created by vendors to execute on user machines, intelligent agents are envisioned as being created by users for execution on servers operated by vendors (of services). In addition to the concerns about mobile code security mentioned above, new questions arise about the confi-

dentiality of data acquired by an agent during its travels, protection of user monetary resources entrusted to the agent, and similar problems.

2.4 INTRUSION DETECTION

Measures that protect against intrusion are often inadequate in today's environment, increasing the need for detection mechanisms as part of an overall security strategy. State-of-the-art intrusion detection is represented by systems that detect known types of attack in individual computers or small-scale networks. However, attack detection in large-scale, distributed systems of the sort that will arise in the NGI is beyond current capabilities. Work is underway (sponsored by the Defense Advanced Research Projects Agency) on a common framework for detecting intrusion, which will provide a good basis for unifying future R&D in this area. Use of current systems often is hindered by complex interfaces and outputs that are difficult to interpret, suggesting that self-correcting and self-diagnosing systems might be appropriate areas for further research.

Even when detection is effective, tracking techniques often raise liability and privacy concerns.

Current systems for intrusion detection are limited in many ways. For example, many consume significant resources (e.g., storage, processing and network bandwidth) when attacks are detected, which creates opportunities to overload the systems with alarms to mask attacks. Most systems do a good job of detecting known attacks. However, identifying new attack scenarios is more difficult, although work in "non-self" detection systems has shown some initial promise. Coordination among systems operated by different administrative entities (e.g., for attacker tracking) is woefully inadequate. Even when detection is effective, tracking techniques often raise liability and privacy concerns, motivating the need for an interdisciplinary approach to R&D in this area.

2.5 PUBLIC KEY INFRASTRUCTURE

The promise of Public Key Infrastructure (PKI) is that it will enable many applications, based on its ability to authenticate large user populations, provide confidentiality for transactions and support nonrepudiation. Electronic commerce applications are obvious beneficiaries of PKI technology, as are applications such as mobile code security (via code signing).

The federal government is expected to be a big user of PKI technology and, based on the many PKI pilots underway in various agencies, may be an early adopter. Moreover, unlike

the many evolving private (commercial) PKIs, government PKIs pose special problems that result from the scale and diversity of the user population and the sensitivity of the information made accessible by the use of PKIs. The recent experience of the Social Security Administration (SSA) in providing access to its records via the Internet illustrates the sensitivity issue, and both the SSA and the Internal Revenue Service are good examples of systems with very large user populations.

Areas ripe for R&D include: determining the impact of failures on large-scale systems; certificate revocation problems for very large PKIs; and managing the complexity of interconnectivity among PKIs operated by various government agencies and private sector providers. Here, too, interdisciplinary R&D is appropriate, as economics, law, sociology and technology all impinge on the successful, secure operation of PKIs on a governmental scale.

2.6 SECURITY MANAGEMENT

Relatively little R&D has focused on how to manage the various security technologies. In addition to the design and implementation vulnerabilities cited below (e.g., in the context of software engineering), system security breaches often are attributable to management vulnerabilities. Poor management interfaces lead to misconfigurations that result in unauthorized access, such as the relatively poor interfaces provided for managing router filter tables.

One unsolved problem is determining how to manage security across multiple protocol layers in environments characterized by vendor heterogeneity. Here, too, as fine-grained access control becomes a more common requirement (e.g., as mentioned earlier in the mobile code and security policies discussions), management becomes more difficult. The need to express security policies and to communicate them across administrative boundaries further strains current systems. Apropos the earlier discussion of infrastructure robustness, one might imagine negotiating quality of service for security in the NGI with a network service provider, but such support is well beyond the capabilities of current technology. This area is appropriate for government funding because industry research currently focuses only on point solutions, relevant to specific product lines. In contrast, government R&D can address the issues in a systemwide fashion.

2.7 CRYPTOGRAPHY

Cryptography R&D has increased considerably in the public sector over the past decade. Still, a number of significant problems remain that are relevant to the NGI. For example, the NGI's very-high-speed transmission and switching capabilities exceed the performance of most current (symmetric) encryption and authentication (e.g., MAC) algorithm imple-

mentations. Therefore, faster algorithms will be needed in both hardware and software. Current signature algorithms also are slow, especially relative to NGI communication speeds, and they are needed to support multicast applications.

There is a need for research on cryptographic protocols and mechanisms to support multicast traffic, consistent with the anticipated growth in multicast applications in the NGI. There is a corresponding need for multicast key management protocols. Even some of the concerns expressed about cryptographic performance can be ameliorated by better protocol design (e.g., appropriate placement of header fields to facilitate pipelined processing of encrypted packets).

Lastly, key recovery has become a popular topic recently and may impinge on the NGI, to the extent that encryption is used as a confidentiality mechanism for stored and/or transmitted data. The requirements for key recovery systems differ, based on the requirements imposed by personal, corporate (including government agency) and law enforcement needs. This suggests that the problems of developing good key recovery systems are a function of what weights are assigned to each of these stakeholders. All of the existing proposals for key recovery techniques fall short in one or more respects. Also, there is no experience in managing large key recovery systems, so R&D is needed. As with PKI, the government may become an early adopter of such systems (based on the many ongoing pilot programs), which argues for federal funding of cryptography R&D.

There is no experience in managing large key recovery systems, so R&D is needed.

2.8 OPERATING SYSTEM SECURITY

An analysis of the Computer Emergency Response Team (CERT) advisories (conducted by Steven Bellovin of AT&T Laboratories) showed that about half of network security problems were attributable to security-relevant failures in software engineering that would not have been prevented by the use of cryptography. Many problems are related to operating system (OS) security vulnerabilities. The government has generously funded OS security R&D for more than 20 years, but little of this work has found its way into the most widely deployed computer systems. To a certain extent, this is a result of having focused R&D and technology transfer efforts on vendors who, ultimately, did not win the marketing war for desktop computers. Still, even the many Unix-based systems deployed today seem to have benefited very little from all of the government funding for a secure Unix.

The lack of good OS security hampers efforts in many of the areas cited earlier. For example, lack of support for process isolation (containment) hampers research in the areas of security policies and mobile code. Various approaches to improving OS security without rewriting the systems and changing interfaces have been tried, but with limited success. For example, appliqués on top of operating systems (e.g., OLE and CORBA) are limited, ultimately, by the lack of security in the underlying operating systems. Industry has increased its focus on additional security features, but there does not appear to be a matching interest in providing these features with high assurance.

Perhaps because of the long history of research in the security area, and the relatively small amount of deployed fruits of this investment, the current focus has turned to ideas from the fault tolerance and reliability areas. Thus approaches such as replication, diversity and "wrappers" are now being pursued. A related fundamental question is whether auditing and better audit tools can compensate for the use of insecure operating systems, given the residual audit-tampering vulnerabilities implied by the use of such systems. This also relates to the earlier discussion of intrusion detection. Other suggestions made during the workshop include pursuing notions of higher-layer abstractions for containment, and extending the encapsulation security offered by cryptography to the processing (vs. communication) environment.

A fundamental question is whether auditing and better audit tools can compensate for the use of insecure operating systems.

Lastly, operating system evaluation of certification standards is a source of continuing debate and is an area that might benefit from new research. There is significant experience with the style of security product evaluation used by the National Computer Security Center (NCSC), and some experience with the Information Technology Security Evaluation Criteria (ITSEC) approach. Several approaches were suggested by group members, including those used by Underwriters Labs, the Occupational Safety and Health Administration, the National Transportation Safety Board, as well as Generally Accepted Security Principles (GASP) (proposed in the National Research Council's report *Computers at Risk*). None seems completely satisfactory, and many broad issues (e.g., concerns over stifling innovation) arise with proposals that seek to give a government agency a substantial role in this area. This suggests a need for research on the policy aspects of these alternative approaches to ensure higher-quality security for operating systems.

2.9 SOFTWARE ENGINEERING

In many respects, software engineering is at the heart of most network security problems. As mentioned earlier, one analysis showed that about half were attributable to security-

relevant failures in software engineering that would not have been prevented by the use of cryptography. Despite the emphasis on widespread availability of strong cryptography as a countermeasure to network security attacks, cryptography is not a panacea. Rather, security-relevant errors introduced during design and implementation phases of software system development continue to be the major source of vulnerabilities in systems. There is no methodology for decomposing security requirements and allocating them to program modules in large systems, which makes it very difficult to develop large systems that conform to security policies.

Despite considerable R&D in software engineering security for more than two decades, much of it government funded, significant problems persist. The creation of ever-larger, more elaborate software systems continues to point to the inability to do a good job in this area. To foster the use of better techniques in industry, there is a strong need for better technology transfer of the results of previous government-funded research. Recent improvements in "light weight" formal methods are an example of a technology that has proven useful in limited contexts, such as hardware design and concurrent algorithms. However, there is increasing pressure on the software industry to provide frequent upgrades with expanded features that can be marketed quickly. Thus there is an urgent need to improve the quality of software engineering to reduce the frequency and severity of vulnerabilities attributable to design and implementation errors.

2.10 NETWORK MANAGEMENT

The final topic listed, security for network management, relates to the first entry on the list, infrastructure robustness. Secure network management is essential to system robustness; otherwise, denial or degradation of service can result from attacks such as spoofing of network management traffic. Most of the industry R&D conducted in this area focuses on point, rather than system, solutions. Like security management, there is no significant work on large-scale, distributed, heterogeneous vendor-platform systems.

Also, there has been little analysis of the privacy implications that arise as the volume of data collected by network management systems increases and includes larger user populations. Privacy is closely related to intrusion detection as well, and thus many of the same concerns raised earlier apply here as well. Tracking attackers across network management administrative boundaries is a problem that impinges on both areas. Secure network management is closely allied to several of the other R&D topic areas, including operating system security (to support the network management platforms) and mobile code (see the active nets DARPA R&D program). Note also the possible conflict between such subscriber security mechanisms as traffic flow security vs. monitoring to support capacity planning based on traffic flows. This area is ripe with R&D opportunities, and industry funding is not addressing these topics.

B.6 ARCHITECTURE

Moderator: Jonathan Turner

1. INTRODUCTION

During the past decade, there has been remarkable growth in the Internet as well as the applications that use it. In fact, the mass market for these services is rapidly becoming ubiquitous. This explosive growth has been enabled by the Internet architecture and the technological developments used to implement that architecture. At the same time, the Internet's rapid expansion, demands for new services, and users' rising expectations have exposed limitations that threaten to constrain its future development. Innovations are needed to meet these challenges if the Next Generation Internet (NGI) is to fulfill its rich potential.

The rapid development of underlying technologies also will have a major impact on the NGI's evolution. For example, integrated circuit technology is improving in cost/performance by a factor of two approximately every 18 months. Commercial systems for wavelength division multiplexing are just beginning to tap into the large reserve of unused bandwidth in existing fiber optic networks (most current transmission systems use less than one percent of the usable bandwidth in the fiber infrastructure). These developments create exciting new opportunities, but also exert great pressure on higher-level network components seeking to make new capabilities available to users. As the relative costs of different technology elements change, they cause a shift in the assumptions underlying much of the current Internet's design. This shift makes it necessary to re-engineer portions of the system to exploit the new capabilities.

Rapid development of underlying technologies will have a major impact on the NGI's evolution.

2. RESEARCH CHALLENGES

During the next decade, the number of users and networked devices is certain to exceed 10 billion and could easily reach into the trillions. The range of link and application data rates also will increase from a few bits per second to terabits per second. These challenges will be compounded by the wide range of application requirements related to network delay, delay variation and data loss, as well as by the growing number of mobile devices (ultimately, wireless devices will be at least as common as "wired" devices). Changes induced by rapid but uneven advances in the underlying technology, and the growth in both the number of Internet users and the resource needs of individual applications, will also be factors. Four of the research challenges facing network architects are: 1) network services, 2) network management, 3) network performance, and 4) diversity and change. These are summarized below.

2.1. NETWORK SERVICES

During the past decade, the definition of Internet service was expanded to include multicast and quality of service. While some future capabilities can be anticipated now, others will only become apparent when the time comes. A key research challenge for the NGI is to both provide for specific needs as they arise, and develop new mechanisms to facilitate the introduction of new services "on demand." While some of these services may be only loosely integrated with the core network components (e.g., switches and routers), other capabilities must be more tightly integrated to provide the greatest benefit. Summaries of some of the service capabilities that require either continued R&D or new research initiatives follow.

2.1.1. Ubiquitous Multicast

Multicast enables new and efficient applications, middleware services and network-level facilities. It has made possible an entirely new class of applications, including multiparty teleconferencing and distributed interactive simulation. Multicast also supports more powerful and robust middleware services, such as adaptive web caching and automatic resource discovery. Lastly, scalable multicast is a fundamental component of the technology necessary to enable network self-organization and autoconfiguration.

Scaling the Internet multicast capability to the very large sizes envisioned for the NGI raises several questions. These include how to maintain the memory and control state required to support extremely large numbers of concurrent multicast groups, and how to provide support for administrative heterogeneity in multicast routing. In addition, the problems of multicast address allocation and reclamation, multicast congestion control, and authentication remain unsolved. Extending multicast functionality to facilitate reliable data delivery also is an important challenge. Lastly, the quantitative characterization

of multicast applications—such as distributions of groups, group size and dispersion, multicast source dispersion and traffic patterns—is poorly understood.

2.1.2 Virtual Networking

Virtual networking is a concept that the data networking community has only just begun to explore. While lower-level network technologies include support for certain aspects of virtual networking, the Internet has yet to address it in a systematic and comprehensive way. Virtual networking makes it possible to construct multiple networks on a common infrastructure, allowing organizations to easily set up private networking domains governed by organization-specific policies. Within the NGI, virtual networks can also be used as testbeds for system-level research that cannot be carried out safely in a production environment.

While some mechanisms are available to support virtual networking (e.g., SONET cross-connects and ATM virtual paths), the concept has not been explored at other levels, and thus far has been applied principally to managing bandwidth. To increase the benefits of virtual networking, several goals must be achieved:

- Develop the technology to allow the interconnection (internetworking) of virtual networks when the virtual networks may be built at any layer of the network stack.
- Virtualize routing and forwarding components (including both route computation and traffic scheduling).
- Enable users to control the configuration of the virtual network, while network providers maintain control of the underlying physical resources.
- Develop methods that allow virtual networks to be configured (and reconfigured) dynamically with little or no manual intervention.

2.1.3 Efficient Handling of Short-Lived Sessions

The growth of the World Wide Web has led to rapid growth in the number of interactive data sessions that last for short periods of time (e.g., a few seconds), but transfer substantial quantities of data. Current Internet protocols are unable to significantly streamline the transfer of such data and they unduly constrain the data transfer rate, resulting in a poor response time. Methods of virtual circuit signaling are also poorly suited to such sessions, requiring excessive overhead for such brief data exchanges. New network services that can rapidly establish streamlined data paths for short-lived sessions can significantly improve the performance of such applications, as well as the efficiency with which they consume network resources.

2.1.4 Support for Dynamic Service Creation

Eventually, current approaches will be unable to meet the increasing demands for new network services. These mechanisms require global deployment and, consequently, are diffi-

cult to implement. However, if network platforms can be made programmable, or at least configurable in new ways based on an individual user's requirements, many of the barriers to deploying new network services will disappear. Achieving this objective is extremely challenging. It requires an operating environment in which software used to define new network services can execute, and an abstract model of network elements on which this software can operate.

2.2. NETWORK MANAGEMENT

Rapid Internet growth has exposed serious scaling issues in network control and management. In some cases, the impact on cost per user increases with the size of the network (e.g., multicast routing), making resolution of these issues essential to the Internet's long-term growth. In others, scaling problems are caused by the demand for new capabilities that place significant additional requirements on network equipment (e.g., per-flow Quality of Service (QoS) state). In cases where the impact on cost per user is independent of the network size, improving the cost/performance of underlying electronics technologies can relieve the pressure in the long term. At the same time, the short-term impact is considerable and requires immediate attention.

Current methods of network management, which are largely manual, cannot keep up with the Internet's rapid growth.

The Internet now serves a mass consumer market that has high expectations for reliability and ease of use. New mechanisms are needed to make the underlying infrastructure more reliable and more tolerant of component failures. Improvements are also needed in the ability of network operators to configure (and reconfigure) network equipment, identify trouble spots, take corrective action and plan for network growth. Current methods (largely manual) of network management cannot keep up with the Internet's rapid growth. Errors in manually configured routing tables or in routing protocol implementations cause frequent disruptions in network service. Furthermore, how routing policies are defined within different administrative boundaries can have a direct impact on the ability to build substantially larger networks. There is a need to better understand how these policies affect network scaling and how they could be implemented in ways that enable growth, rather than constrain it.

Self-configuration and self-organization techniques make networks easier to configure, manage and operate. Based on a set of rules or parameters, self-organizing systems can configure or reconfigure themselves to maintain a certain level of network service. Today's Internet technology is self-organizing in some ways (e.g., the selection of routes for traffic

flows), but there is a much richer set of possibilities. Indeed, if applied as a consistent architectural principal, self-organization can make it easier and more cost-effective to scale up networks to large sizes. It also can help to rapidly deploy network equipment in special situations, such as emergency response or military operations.

2.3. NETWORK PERFORMANCE

Growing demands on networks will keep the pressure on to improve the performance of network equipment. While advances in the underlying technology can help meet these demands, the rates of change vary widely among the different technology domains. New approaches are needed to best exploit these improvements.

For example, the performance of the forwarding engine (the part of switching and routing equipment that decides how to forward data as it comes in) needs to be improved. Scaling places tremendous pressure on forwarding technology. Faster networks require ever-faster forwarding technology, and current trends indicate that the rates at which users need to forward are growing faster than the rate of improvement in the underlying electronics (particularly memory) technology. Added to this challenge are the competing pressures of both traffic aggregation and separation, which place additional burdens on already strained forwarding elements of current switches and routers. While recently discovered algorithms promise significant improvements in forwarding performance, crucial aspects of the problem have not been addressed. Continuing performance pressures will drive the need for continuing improvements in algorithms.

Another key enabler of higher-performance networks is optical technology, but so far it has been applied primarily to point-to-point transmission. Incorporating optical technology more comprehensively into network equipment could potentially improve network capacities by orders of magnitude. However, optical technology is difficult to incorporate into network switches and routers because its logic and memory are very limited. Continuing research is needed to develop architectural models that exploit the tremendous strengths of optics, without sacrificing the flexibility and adaptability of the current Internet.

The performance of devices connected to networks is also a concern. These devices are often the weak link in providing performance to end-user applications. The quality of audio and video available on personal computers continues to be disappointing when compared with conventional consumer electronics. Problems with the performance of networked information servers are growing as user demands increase, often in unpredictable ways. New strategies for organizing data movement among network, application program and hardware components will be needed to realize the potential of the under-

lying technology. This may require new architectural approaches to end-system design at all levels from hardware to application programs.

2.4. DIVERSITY AND CHANGE

The Internet has been remarkably successful in coping with a diversity of applications and underlying network technologies. The Internet Protocol (IP) service model (the so-called Internet hourglass) has been central to its success in dealing with heterogeneity. Other important features of the Internet include: its support for a multiplicity of delivery choices (e.g., unicast and multicast); its decentralized operation (the network operates without the need for any central coordination); and its ability to recover from a wide range of outages with a minimum of mechanisms. However, the continuing pressures of technology improvements and application demands are creating new challenges. Current network technology supports individual link speeds of up to 10 gigabits per second, and terabit link technologies are under development. At the same time, wireless links must operate at much lower speeds, giving rise to a network "dynamic range" of 10 orders of magnitude.

Applications also are imposing increasingly diverse requirements on networks. Interactive voice and video applications have much more limited tolerance for delay and delay variability than more traditional applications. They are, however, more tolerant of loss. Providing high-quality, consistent support for such applications on a network that is also carrying highly unpredictable data traffic has proven to be very challenging.

The Internet's ability to cope with heterogeneity and change is a tremendous achievement. No other large-scale network technology even approaches its ability to cope with a diverse and changing environment. It is important, therefore, to build on what has been learned and to carry forward those lessons into the next century. At the same time, it is essential to recognize that the networking environment is undergoing tremendous change and that new approaches may be needed to meet new challenges. Finding the right balance will be a central theme of NGI research programs.

3. INFRASTRUCTURE TO SUPPORT SYSTEMS RESEARCH

The NGI initiative offers a rare opportunity to dramatically upgrade the national networking infrastructure in support of the total research enterprise. By building on recent advances in networking technology, the NGI can offer unprecedented levels of performance, a variety of new services, and a more flexible infrastructure that can accommodate the introduction of additional capabilities in the future. Equally important, the NGI can provide an experimental environment to support the development of new networking

technologies and distributed systems. These, in turn, will fuel the advances that will allow the United States to maintain its preeminent position in this crucial technology domain.

Virtual networking is a key tool for enabling the configuration of experimental testbeds in support of systems research. Using virtual network concepts, multiple private networks can operate over shared transmission facilities. The concept can be applied at different network layers (IP, ATM, SONET, WDM). Lower-level implementations of virtual networking have the advantage of being able to directly support the construction of virtual networks at all higher levels. Higher-level implementations allow more flexibility in allocation of bandwidth among virtual links. In the near term, ATM virtual paths may offer the most straightforward mechanism for implementing experimental testbeds. ATM is widely available in commercial switches and can be used to support both ATM virtual networks and IP virtual networks. It would not support research activities in physical layer technologies or the use of a reconfigurable physical layer to provide dynamic support at the higher layers.

The importance of providing experimental testbed facilities cannot be overstated.

The importance of providing experimental testbed facilities cannot be overstated. The research community has played a central role in the development of the Internet protocols, the underlying technologies and the applications that use the network. To have an impact on the NGI, researchers must be able to transfer their ideas from the concept stage to effective system demonstrations. This cannot be done in the Internet itself, nor can lower-level system demonstrations be allowed to disrupt production uses of NGI facilities. Virtual networking offers a straightforward solution to this problem. Using virtual networking, systems researchers will be able to construct and operate substantial experimental systems under conditions that are similar to those in a production network environment. The systems that are successfully demonstrated and shown to be useful can then be migrated into the production NGI and, ultimately, into the broader Internet itself. One of the most important roles the government can play in NGI development is to create the R&D pathways that will allow research innovations to move systematically from the laboratory to the real world.

APPENDIX A

WORKSHOP PARTICIPANTS

Mike Ahdieh
Nortel

Robert Aiken
U.S. Department of Energy

Paul Amer
University of Delaware

William Aspray
Computing Research Association

Albert Azzam
Alcatel

Stephen Batsell
Oak Ridge National Laboratory

Steven Bellovin
AT&T Laboratories

Lou Berger
FORE Federal Systems Inc.

Kul Bhasin
NASA Lewis Research Center

David Black
The Open Group Research Institute

Javad Boroumand
University of Southern California/ Information Sciences Institute

Bruce Bottomley
National Security Agency

Hans-Werner Braun
University of California at San Diego

Laurence Brown
NCR

Charles Brownstein
Cross-Industry Working Team

Suzanne Burgess
DynCorp/Federal Networking Council

L. Jean Camp
Sandia National Laboratories

Gary Campbell
Tandem Computers Inc.

Roy Campbell
University of Illinois

Thomas Casper
Lawrence Livermore National Laboratory

Charlie Catlett
National Center for Supercomputing Applications

John Cavallini
DynCorp I&ET

Vinton Cerf
MCI

Vincent W. S. Chan
MIT Lincoln Laboratory

Ching-chih Chen
Simmons College

Kim Claffy
University of California at San Diego

David Clark
Massachusetts Institute of Technology

David Cooper
Lawrence Livermore National Laboratory

Stephen Crocker
CyberCash Inc.

Henry Dardy
Naval Research Laboratory

Steven Davis
Princeton Plasma Physics Laboratory

Peter Dean
Sandia National Laboratories

Steve Deering
Cisco Systems Inc.

Tom DeFanti
University of Illinois

Dick desJardins
National Aeronautics and Space Administration

Phillip Dykstra
Army Research Laboratory

Michael Eaton
Sandia National Laboratories

Donald L. Endicott, Jr.
Naval Command, Control and Ocean Systems Center

Deborah Estrin
University of Southern California/ Information Sciences Institute

Christine Falsetti
NASA Ames Research Center

David Farber
University of Pennsylvania

Stuart Feldman
IBM Research

Paul Ferguson
Cisco Systems Inc.

Bill Fink
NASA Goddard Space Flight Center

Darleen Fisher
National Science Foundation

Sally Floyd
Lawrence Berkeley National Laboratory

Ian Foster
Argonne National Laboratory

Eugene Freuder
University of New Hampshire

Samuel Fuller
Digital Equipment Corp.

Sherrilynne Fuller
University of Washington

Eran Gabber
Lucent Technologies, Bell Laboratories

JJ Garcia-Luna-Aceves
University of California at Santa Cruz

Randy Garrett
Defense Advanced Research Projects Agency

Lee Hammerstrom
NRO

Ted Hanss
Internet 2 Project

Gary Herman
Hewlett Packard Laboratories

David Houseman
Unisys Corp.

Sally Howe
National Coordination Office for Computing, Information, and Communications

Bertram Hui
Defense Advanced Research Projects Agency

Van Jacobson
Lawrence Berkeley National Laboratory

Marjory Johnson
NASA Ames Research Center

Norman Johnson
Los Alamos National Laboratories

William Johnston
Lawrence Berkeley National Laboratory

Robert Kahn
Corporation for National Research Initiatives

Tom Kalil
National Economic Council

Marianna Kantor
Los Alamos National Laboratory

Ken Kay
Computer Systems Policy Project

Jerry Kellenbenz
Apple Computer Inc.

Henry Kelly
Office of Science and Technology Policy

Chris Kemper
Los Alamos National Laboratory

Stephen Kent
BBN Corp.

Carl Kesselman
University of Southern California/ Information Sciences Institute

Ken Kliewer
Oak Ridge National Laboratory

Kenneth Klingenstein
University of Colorado at Boulder

Gary Koob
Defense Advanced Research Projects Agency

Luis Kun
Agency for Health Care Policy and Research

Larry Landweber
University of Wisconsin at Madison

Lars-Goran Larsson
Ericsson Inc.

James Leighton
Lawrence Berkeley National Laboratory/ESnet

Will Leland
Bellcore

William Lennon
Lawrence Livermore National Laboratory

Donald Lewine
Data General Corp.

Stewart Loken
Lawrence Berkeley National Laboratory

Mark Luker
National Science Foundation

Clifford Lynch
University of California

Allison Mankin
University of Southern California/ Information Sciences Institute

Richard Marciano
San Diego Supercomputer Center

Douglas Maughan
National Security Agency

Ray McFarland
National Security Agency

Alexander Merola
Lawrence Berkeley National Laboratory

Paul Messina
California Institute of Technology

David Meyer
University of Oregon

Michael Millikin
Softbank Forums

Gary Minden
University of Kansas

Doug Montgomery
National Institute of Standards and Technology

Robin Morel
Los Alamos National Laboratory

Bruce Murdock
Tektronix Inc.

Sandra Murphy
Trusted Information Systems Inc.

Michael Myjak
University of Central Florida

David Nagel
AT&T Laboratories

David Nelson
U.S. Department of Energy

Hilarie Orman
Defense Advanced Research Projects Agency

Craig Partridge
BBN Corp.

Vern Paxson
Lawrence Berkeley National Laboratory

Ian Philp
Los Alamos National Laboratory

Alexis Poliakoff
U.S. Department of Education

Parameswaran Ramanathan
University of Wisconsin at Madison

Robert Rarog
Digital Equipment Corp.

Kenneth Rehor
Bell Laboratories/Lucent Technologies

Ira Richer
Corporation for National Research Initiatives

Richard Schantz
BBN Corp.

Peter Selfridge
AT&T Laboratories

George Seweryniak
U.S. Department of Energy

Margaret Simmons
National Coordination Office for Computing, Information, and Communications

Michael Sobek
Sprint

Karen Sollins
MIT Laboratory for Computer Science

John Stankovic
University of Virginia

Carl Staton
National Oceanic and Atmospheric Administration

Rick Stevens
Argonne National Laboratory

Maureen Stillman
Odyssey Research Associates

George Strawn
National Science Foundation

Tatsuya Suda
National Science Foundation

Ivan Sutherland
Sun Microsystems Inc.

Jaroslaw Sydir
SRI International

Harold Szu
University of Southwestern Louisiana and Naval Surface Warfare Center

Stephen Tenbrink
Los Alamos National Laboratory

John Toole
National Coordination Office for Computing, Information, and Communications

Joe Touch
University of Southern California/ Information Sciences Institute

Mike Trest
ATMnet

William Turnbull
National Oceanic and Atmospheric Administration

Jonathan Turner
Washington University at St. Louis

Nian-Feng Tzeng
University of Southwestern Louisiana

Carolyn VanDamme
Computer Systems Policy Project

Douglas Van Houweling
University of Michigan

Grant Wagner
National Security Agency

James Walker
UNISYS

Fred Weingarten
Computing Research Association

Allan Weis
Advanced Network & Services

Roy Whitney
Jefferson Laboratory

Walter Wiebe
Federal Networking Council

Gio Wiederhold
Stanford University

Rick Wilder
MCI

Linda Winkler
Argonne National Laboratory

Stephen Wolff
Cisco Systems Inc.

Steve Wright
Hewlett Packard Laboratories

John Wroclawski
MIT Laboratory for Computer Science

James Yan
Nortel Technology

Kenneth Young
Bellcore

Lixia Zhang
University of California at Los Angeles

Steven Zornetzer
NASA Ames Research Center

APPENDIX B

REPORT REVIEWERS

Drafts of the session reports were reviewed at several stages by session participants. In addition to moderators and members of the program and federal steering committees, the following people responded to the request for comments on the final draft report.

David Black
The Open Group Research Institute

Hans-Werner Braun
University of California at San Diego

L. Jean Camp
Sandia National Laboratories

Ray McFarland
National Security Agency

Karen Sollins
MIT Laboratory for Computer Science

Maureen Stillman
Odyssey Research Associates

John Toole
National Coordination Office for Computing, Information, and Communications

Michael Trest
ATMnet

APPENDIX C

COMMITTEES AND CONTRIBUTORS

PROGRAM COMMITTEE

Guy Almes
Advanced Network and Services

Forest Baskett
SGI Inc.

Scott Bradner
Harvard University

Charles Brownstein
Cross-Industry Working Team

Vinton Cerf
MCI

Kim Claffy
University of California at San Diego

David Clark
Massachusetts Institute of Technology

David Farber
University of Pennsylvania

Stuart Feldman
IBM Research

Stephen Kent
BBN Corp.

Stewart Loken
Lawrence Berkeley National Laboratory

Jonathan Turner
Washington University at St. Louis

Douglas Van Houweling
University of Michigan

Stephen Wolff
Cisco Systems Inc.

Fred Weingarten
Computing Research Association

FEDERAL STEERING COMMITTEE

Bruce Bottomley
National Security Agency

Christine Falsetti
National Aeronautics and Space Administration

Bertram Hui
Defense Advanced Research Projects Agency

Thomas Kalil
National Economic Council

James Leighton
Lawrence Berkeley National Laboratory

Mark Luker
National Science Foundation

Alexander Merola
Lawrence Berkeley National Laboratory

George Seweryniak
U.S. Department of Energy

Margaret Simmons
National Coordination Office for Computing, Information, and Communications

Walter Wiebe
Federal Networking Council

RECORDERS, SPEAKERS, AND OTHER CONTRIBUTORS

Javad Boroumand
University of Southern California/Information Sciences Institute

Donald L. Endicott, Jr.
Naval Command, Control and Ocean Systems Center

Anita Jones
Department of Defense

Thomas Kalil
National Economic Council

Henry Kelly
Office of Science and Technology Policy

Will Leland
Bellcore

Allison Mankin
University of Southern California/Information Sciences Institute

Alexander Merola
Lawrence Berkeley National Laboratory

Paul Messina
California Institute of Technology

David Nelson
U.S. Department of Energy

Karen Sollins
MIT Laboratory for Computer Science

George Strawn
National Science Foundation

APPENDIX D

AGENDA

WORKSHOP ON RESEARCH DIRECTIONS FOR THE NEXT GENERATION INTERNET

Sheraton Premiere Hotel, Tyson's Corner, Vienna, VA

MAY 12-14, 1997

MONDAY, MAY 12, 1997

6:00 - 8:00 p.m. Registration and Informal Reception

TUESDAY, MAY 13, 1997

7:30 a.m. - 8:30 a.m. Continental Breakfast
Registration

8:30 - 8:45 Welcome and Opening Remarks
- Fred Weingarten, Computing Research Association
- Henry Kelly, Office of Science and Technology Policy
- Thomas Kalil, National Economic Council
- David Nelson, Department of Energy
- George Strawn, National Science Foundation

8:45 - 9:30 Historical Context Panel
- Charles Brownstein, Corporation for National Research Initiatives (Moderator)
- Vinton Cerf, MCI
- David Clark, Massachusetts Institute of Technology
- Robert Kahn, Corporation for National Research Initiatives
- Douglas Van Houweling, University of Michigan
- Stephen Wolff, Cisco Systems Inc.

9:30 - 9:45	Breakout Session Goals - David Clark, MIT
9:45 -10:15	Break
10:15 - 12:15	Convene Workshop Sessions 1. Security (Moderator: Stephen Kent, BBN Corp.) 2. Quality of Service (Stewart Loken, Lawrence Berkeley National Laboratory) 3. Architecture (Jonathan Turner, Washington University) 4. Middleware (David Farber, University of Pennsylvania, and Richard Schantz, BBN Corp.) 5. Applications (Stuart Feldman, IBM Research) 6. Internet Traffic Engineering (Kim Claffy, University of California at San Diego)
12:15 - 1:00	Lunch (videos available for viewing)
1:00 - 3:00	Workshop Sessions
3:00 - 3:30	Break
3:30 - 5:00	Workshop Sessions
5:30 - 8:00	Reception and Dinner

WEDNESDAY, MAY 14

7:30 - 8:30 a.m.	Continental Breakfast
8:30 - 10:00	Workshop Sessions
10:00 - 10:15	Break
10:15 - 12:00	Workshop Sessions
12:00 - 1:00	Lunch (videos available)
1:00 - 1:30	Plenary Session Guest Speaker: Anita K. Jones, Director Defense Research & Engineering Department of Defense
1:30 - 2:30	Closing Remarks: David Clark, MIT Moderators' Comments

Computing Research Association

COMPUTING RESEARCH ASSOCIATION
1100 17th Street, NW, Suite 507
Washington, DC 20036-4632
(202) 234-2111; Fax: (202) 667-1066
E-mail: info@cra.org; URL: http://www.cra.org