Federal Plan
For
Advanced Networking
Research and Development

PREPRINT VERSION

<u>June 11, 2008</u>

Table of Contents

Executive Summary

In the four decades since Federal research first enabled computers to send and receive data over networks, U.S. government research and development (R&D) in advanced networking has fueled a technological, economic, and social transformation. Today, networking is woven into the fabric of our society, a fundamental infrastructure for government operations, national defense and homeland security, commerce, communication, research, education, and leisure-time activities.

The Internet's phenomenal growth and elasticity have exceeded all expectations. At the same time, we have become captive to the limitations and vulnerabilities of the current generation of networking technologies. Because vital U.S. interests – for example, national defense communications, financial markets, and the operation of critical infrastructures such as power grids – now depend on secure, reliable, high-speed network connectivity, these limitations and vulnerabilities can threaten our national security and economic competitiveness. Research and development to create the next generation of networking technologies is needed to address these threats.

This critical R&D challenge was recognized by the Director of the Office of Science and Technology Policy (OSTP), who formed the Interagency Task Force on Advanced Networking to provide a strategic vision for future networked environments (see appendix 1 for the charge to the Task Force). The Task Force, established under the Networking and Information Technology Research and Development (NITRD) Subcommittee of the National Science and Technology Council (NSTC) and comprising representatives of 11 Federal organizations, developed this *Federal Plan for Advanced Networking Research and Development*.

This plan is centered on a vision for advanced networking based on a design and architecture for security and reliability that provides for heterogeneous, anytime-anywhere networking with capabilities such as federation of networks across domains and widely differing technologies; dynamic mobile networking with autonomous management; effective quality of service (QoS) management; support for sensornets; near-real-time autonomous discovery, configuration, and management of resources; and end-to-end security tailored to the application and user.

Four goals are set forth for realizing this vision:

1. Provide secure network services anytime, anywhere.
2. Make secure global federated networks possible.
3. Manage network complexity and heterogeneity.
4. Foster innovation among the Federal, research, commercial, and other sectors through development of advanced network systems and technologies.

The capabilities needed to achieve these goals are set forth in terms of the following five dimensions of networking research:

- Foundations
- Design
- Security
- Management
- Usability

The overall conclusions of the Task Force can be summarized as follows:

1. Improved networking security and reliability are strategic national priorities.
2. New paths to advanced networking are required.
3. Federal R&D efforts are needed for a spectrum of advanced networking capabilities.
4. Close cooperation is needed to integrate Federal R&D efforts with the full technology development cycle. This cycle includes basic and applied research, and partnerships with researchers, application developers, users, and other stakeholders
5. Testbeds and prototype networks are needed to enable research on network challenges in realistic environments

Responding to both the charge for a strategic vision of future networked environments and the Nation's urgent needs for enhanced networking security and reliability, this *Federal Plan for Advanced Networking Research and Development* provides dual, nested timeframes for the required capabilities. Appendix 2 (page 26) presents, in tabular form, detailed results of the Task Force analysis of Federal networking research needs. The table is designed to provide a range of policy and planning options for nested near-term and long-term timeframes. The near-term networking security timeframe highlights capabilities that have substantial impact on improving security in the current networking environment. These capabilities for shorter-term impact are indicated by underlining in the Appendix 2 table. (See also, Section 3: "Accelerated Networking Security Focus" on page 21.)

The longer timeframe focuses on the middle of the next decade and has as its goal fundamental advances in the networking landscape. The Appendix 2 table provides two categories of longer-term targets: those that are accessible under existing or planned programs (column 3) and those that require a more intensive effort (column 4). The magnitude of the change depends, in large part, on the category of targets selected. Selecting a mix of targets from the two categories can create a range of longer-term options.

1. Advanced Networking R&D: Fostering Leadership in the 21st Century

Introduction

In the four decades since Federal research first enabled computers to send and receive data over networks, U.S. government R&D in advanced networking[1] has fueled a technological, economic, and social transformation. Federal R&D investments led the way to the Internet, wireless mobile and optical networking, and an array of network-based applications that continue to reshape not just our society and economy, but societies and economies around the globe.

Across the United States and throughout the world, the fabric of interconnectivity linking data, devices, and applications to users on the move has become pervasive. Today, this information technology (IT) infrastructure is a fundamental infrastructure for innovation in government operations, commerce, communication, research, education, and leisure-time activities. Reliable high-speed networking – enabling nearly instantaneous communication as well as transmission, storage, and retrieval of vast quantities of data (e.g., text, images, sound, multimedia, signals) – is now indispensable to private-sector enterprises of every kind and to high-priority Federal missions such as national defense, homeland security, and advanced scientific research.

The economic impacts of networking range from contributions to robust growth of GDP and productivity to the rise of new multibillion-dollar corporations in networking equipment and services, the e-commerce sector, and innovative social-networking applications. Economists and IT experts predict a continuing rapid pace for development and deployment of new networking technologies, services, and applications over the next 10 years and beyond.

Many of these developments will reflect the convergence of networking with other technologies. Advanced networking technologies, in tandem with innovations in other IT components (e.g., miniaturization, automation, sensors, intelligent systems), radically expand the range of current and potential uses for computing systems and devices. Unmanned aerial vehicles, for example, became feasible through advances in both networked computing systems embedded in the physical structure and wireless technologies for remote command and control. Such emerging network-based applications have profound importance for the Federal government and the Nation's global economic competitiveness. Examples of networking application domains that represent strategic U.S. interests include aviation and transportation; the battlefield of the

---

[1] Advanced networks, as referred to in this report, include heterogeneous, anytime-anywhere networking and capabilities such as federation of networks across domains and widely differing technologies; dynamic mobile networking with autonomous management; quality of service (QoS); support for sensornets; near-real-time autonomous discovery, configuration, and management of resources; and end-to-end security tailored to the application and user.

future; critical infrastructure management; emergency preparedness and response; environmental monitoring; large-scale, data-intensive, and domain-specific scientific research; medicine and health care; and national security.

A Strategic National Priority

The President's Council of Advisors on Science and Technology (PCAST), the high-level private-sector panel that provides independent guidance to the President on key scientific issues facing the country, has recognized the central and critical role that advanced networking now plays in sustaining the Nation's military, scientific, economic, and technological preeminence. In its August 2007 report entitled *Leadership Under Challenge: Information Technology R&D in a Competitive World*, the PCAST states that "*U.S. leadership in advanced networking is a strategic national priority*."

Recognizing the strategic importance of advanced networking, on January 30, 2007 the Director of the White House Office of Science and Technology Policy (OSTP) established the Interagency Task Force on Advanced Networking and tasked it with: providing a strategic vision of future networked environments; identifying the challenges in supporting such environments with existing and developing technologies; and providing recommendations on a roadmap for research and research infrastructure to enable those future environments (see charge in Appendix 1, page 24).

In the *Federal Plan for Cyber Security and Information Assurance Research and Development* of 2006, Science Advisor to the President John H. Marburger writes:

> "*The Nation's Information Technology (IT) infrastructure – the seamless fabric of interconnected computing and storage systems, mobile devices, software, wired and wireless networks, and related technologies – has become indispensable to public- and private-sector activities throughout our society and around the globe. … The interconnectivity that makes seamless delivery of essential information and services possible, however, also exposes many previously isolated critical infrastructures to the risk of cyber attacks mounted through the IT infrastructure by hostile adversaries. … Safeguarding the Nation's IT infrastructure and critical infrastructure sectors for the future is a matter of national and homeland security.*"

Research and development are urgently needed to enable secure and reliable networking environments that can meet our Nation's needs.

Responding to both the charge for a strategic vision of future networked environments and the Nation's urgent needs for enhanced networking security and reliability, the *Federal Plan for Advanced Networking Research and Development* provides dual, nested timeframes for the required capabilities. This Plan is intended to guide both internal prioritization of agencies' networking investments and coordinated multi-agency R&D activities.[2]

The Internet Today: Success, Limitations, and Vulnerabilities

The researchers whose technical achievements made the Internet possible could not foresee the emergence of a wholly new, ultimately global, infrastructure able to support a wide range of human activities. The Internet's phenomenal growth (to more than a billion users worldwide) and elasticity (for example, enabling the World Wide Web, grid computing, and wireless connectivity) have exceeded all expectations. At the same time, we have become captive to the limitations and vulnerabilities of the current generation of networking technologies.

Because vital U.S. interests – for example, national defense communications, financial markets, and the operation of critical infrastructures such as power grids – now depend on secure, reliable, high-speed network connectivity, these limitations and vulnerabilities have national security implications. Moreover, they inhibit development of next-generation networking technologies and applications that can serve the anytime-anywhere, ubiquitous, ad hoc broadband connectivity needed to carry out critical Federal missions, spur economic innovation, and maintain a U.S. competitive edge in networking.

The original Internet design presupposed that network access would come through trusted host machines at the edges of the network. A single number – the Internet Protocol (IP) address – both identified the end system and described the topology of the network, which provided important transmission efficiencies. Further, the Internet end-to-end protocols assigned delivery assurance and congestion control to the edges of the network. These features have resulted in significant network security and manageability problems, which will only become more pronounced as the types and scale of Internet traffic expand. Today, increasing requirements to support wireless services and multi-hop relays for users on the move severely stress the edge protocols. Users increasingly connect to the Internet through mobile devices where the same number cannot be used to describe both the identity and location of the device because the location constantly changes. Providing security and QoS in Internet connectivity for mobile users remains a formidable technical challenge.

The early Internet design philosophy presumed good will. Network security was not a major consideration. Today, the Internet and the networks connected to it are constantly under attack by worms, viruses, denial of service, and other forms of malicious software. The same principle that relieves users of the need to know the location of their data

[2] While the focus of this plan is on long-term advanced networking research, it is understood that such programs are developed and implemented in the context of the agency's overall mission requirements and needs for operational networking capabilities including IPv6, Trusted Internet Connections (TICs), and IT Infrastructure Line of Business.

sources enables anonymous individuals or groups anywhere in the world to mount attacks that cannot be traced by network administrators and law enforcement. Defending against and recovering from network attacks cost government, the private sector, and individual computer users many billions of dollars annually.

To date, mobile networking, security, addressing, and other mechanisms for dealing with Internet limitations have been implemented through technical patches to the basic architecture. In many cases, these specialized patchwork extensions of the Internet have reached a practical limit, while increasing the overall fragility of the network. For example, vastly expanding the number of available fixed-node addresses through implementation of Internet Protocol version 6 (IPv6) will not diminish Internet security problems or foster new networking applications, such as multicast and distributed collaboration, that require stable, secure, uninterruptible high bandwidth from end to end. In fact, in the absence of significant advances through networking research and development, the various pressures now building on the Internet are highly likely to decrease transmission speeds and increase outages and interruptions in the years ahead.

Indeed, the current Internet's global-scale complexity has itself become an overarching intellectual and technical challenge for both network operators and researchers. The complexity is multi-dimensional, including vast amounts of heterogeneous hardware, software, and devices interconnected through vast numbers of large-scale autonomous networks and subnetworks operated by organizations and individuals with diverse interests and constantly changing degrees of cooperation and competition. Currently, we lack adequate theories and models to understand and manage this complexity. New scientific foundations – including innovative approaches to achieve simplicity and transparency – are needed to provide insight into Internet design requirements (such as scalability, security, and privacy) and to enable researchers and policy makers to address means of improving services (such as Web searching, content delivery, and Web-mediated community formation).

Government-sponsored and private-sector R&D address different aspects of networking development. The private sector is frequently focused on near-term product development, with limited incentive to invest in long-term and high-risk networking research, and massive infrastructure investments with multi-decade amortization (e.g., fiber optic networks); government-sponsored R&D, less constrained by near-term return on investment, can address a longer-term vision. Working together, networking researchers spanning government, industry, the national laboratories, and academia have forged a broad community that engages in ongoing information-sharing and collaborative activities that foster commercial uptake and product development for networking innovations. This broader community has participated in the development of the *Federal Plan for Advanced Networking R&D* and will be encouraged to join in implementation activities under the Plan.

Plan's Accelerated Networking Security Focus Option

This Plan provides two timeframes to address distinct needs. The core of the Plan – outlined in the text immediately below – focuses on the middle of the next decade with a comprehensive R&D plan for achieving a dynamic, new networking landscape. In addition, the Plan provides the option for an accelerated focus on capabilities to meet today's urgent national requirements for increased networking security, reliability, and cyber defense. The features of this nested, accelerated Plan option – described in Section 3 below (page 21) – align closely with the strategic Federal R&D objectives set forth in the April 2006 *Federal Plan for Cyber Security and Information Assurance Research and Development.*

The Strategic Vision: New Capabilities by Mid-Decade

U.S. leadership in advanced networking began with Federal requirements for capabilities not available commercially. Today, networking requirements for Federal missions range from the highest-bandwidth optical networks to low-power sensor networks deployed on battlefields. These requirements are far more complex and technically challenging than before, and far greater national interests are now at stake. This *Federal Plan for Advanced Networking Research and Development* describes an ambitious program of R&D to achieve fundamental advances that would meet future Federal needs and thus help sustain the Nation's long-term leadership in networking technologies amid growing international competition.

In the Plan's strategic vision, by the middle of the next decade advanced networks will be used in powerful new ways to support critical Federal missions including crisis response, the electronic battlefield, collaborative and domain-specific science, electronic health care, environmental and climate monitoring, and other areas. These networks will range from wireless sensors deployed in remote environments, to wireless connections linking supersonic aircraft, to fixed networks capable of transmitting exabytes (billions of gigabytes) of scientific data around the world.

To enable these capabilities, the Plan envisions a new, dynamic networking infrastructure that will use wavelength-routing optical switches with switching times on the order of a few nanoseconds. The infrastructure will span sub-wavelength circuits, wavelengths, and entire wavebands and fibers. Higher-layer nodes will provide interoperability among heterogeneous services (IP, MPLS, SONET, MSPPs, etc.). Distributed users of the network will be able to configure resources (networking, compute, storage, security, management, etc.) to create dynamic virtual private networks. Connectivity to the infrastructure will be supported across network domains and heterogeneous technologies.

Recognizing the growing importance of commercial mobile radio technologies and applications, the Plan envisions the integration of existing wired, wireless, and IP-based infrastructures into a Next Generation Network fabric supporting secure, end-to-end, heterogeneous, multimedia networking.

While this plan focuses on new capabilities by mid-decade, it is understood that Federal agencies with advanced networking R&D programs will continue to update their research programs as visions and needs change and as research results are integrated into deployed networks. Domain-specific science researchers, advanced networking researchers, program managers, commercial sector users and developers, and others with interests in advanced networking capabilities and research will continue to provide guidance on their changing needs and those of the larger society.

Strategic Vision's Technical Goals

Examples of mission-critical Federal applications that require revolutionary changes in our approach to networks are described on pages 12 and 16. An analysis of these and other applications across the Government resulted in an interagency consensus on high-priority Federal capabilities that need to be in place by the middle of the next decade. Realizing the strategic vision will require R&D advances toward four technically challenging goals:

1 **Provide secure network services anytime, anywhere.** Today's Internet cannot provide users with trustworthy (secure, private, and reliable) services anytime and anywhere they are needed. A new generation of concepts, technologies, and systems is needed to leapfrog current limitations. The new services would cover the spectrum of critical Federal and other user needs, from tailored intermittent messaging to soldiers in theatre to high-bandwidth data transfers in large-scale domain-specific scientific research collaborations. The services would be able to hide from users the complexity of the underlying infrastructure, which could include wired, wireless, static, and ad hoc networks deploying a wide variety of heterogeneous technologies. Today, operation and management of services across such networks is challenging. New technologies to manage trust and authentication in these environments, sophisticated middleware that enables cooperative control and fault diagnosis, and next generations of wired and wireless devices are required to make anytime-anywhere advanced services a reality.

Illustrative Goal 1 Application

A multinational group of task forces responding to a local conflict in an area with limited networking resources is able to coordinate information, resources, and command and control across the task forces. They establish an ad hoc wireless network federated across the heterogeneous technologies and equipment of each task force to provide support for: inputs from sensornets, sensors on personnel, and extremely dynamic airborne and satellite sensors; adaptive data and voice networks that maintain connectivity to enable command and control during a dynamic mission; security and privacy tailored to individual components; location-independent addressing; QoS management for priority mission needs; and distributed autonomous self-organization among the diverse entities with centralized oversight to provide responsiveness, avoid chaotic behavior, and improve network performance and reliability.

2 **Make secure, global, federated networks possible.** Fundamental research breakthroughs are needed to enable networks with differing capabilities and architectures to be linked together around the world to deliver end-to-end services that can meet users' requirements for performance, cost, privacy, security, and advanced services. This research must also enable multi-vendor, multi-carrier, multi-national deployment of end-to-end services with appropriate authentication, authorization, and accounting linkages.

Illustrative Goal 2 Application
A scientist at any university in the United States is able to request a massive dataset from an experiment in Europe and have the networks across his campus, his region, the Nation, and Europe negotiate the best way (federated across heterogeneous international networks) – including, for example, transmission protocols, network resources, federated network policies, QoS prioritization, and security – to deliver the data and provide all of the networks the information they need to manage the transfer and account for resources used.

3 **Manage network complexity and heterogeneity.** Future networks will be more complex and heterogeneous than the current Internet. They will link circuit-switched and packet-switched networks, high-speed optical paths, intermittent planetary-scale paths, sensor networks, and dynamic ad hoc networks. These varied network forms will involve millions or billions of interfaces that will change dynamically. Understanding the behavior of such systems remains, in itself, an enormous technical challenge. Intensive investigations are needed to discover appropriate scientific methods for modeling and analyzing unprecedented levels of network complexity. Such methods are a prerequisite for developing the critical tools that will enable network administrators to manage and control these networks, diagnose their faults and failures, and recognize and respond to attacks. Emphasis is needed on technical approaches to attain simplicity and transparency of design.

Illustrative Goal 3 Application
A new type of attack, capable of causing massive system failure and release of sensitive data, is launched against a networked system. The attack hits the kernel of the operating system and hardware, making it resistant to re-booting. With new technology designed to automatically manage a response across a complex system, the attack is quickly detected; a signature to stop it is synthesized, distributed out of band, and applied throughout the network, slowing the spread of the attack; the attack code is reverse-engineered so that a patch can be synthesized and distributed; the patch is installed to eliminate the vulnerability and restore all systems to an operational state.

4 **Foster innovation among the Federal, research, commercial, and other sectors through development of advanced network systems and technologies.** Key research, development, and engineering areas must be nurtured to assure continuous improvement of advanced network systems that meet the needs of applications.

Research addressing barriers to commercialization also is needed to facilitate uptake of emerging technologies and broad user adoption.

Illustrative Goal 4 Application

Residents in an urban mountain community become aware of a serious fire but do not know the best escape route, or even if they should remain in place. They lose power, so have no access to computers but do have access to cell phones. Sensors previously placed in the hills help track the fire. New technologies fostered by advanced networking research programs ("smart" cell phones connected through an ad hoc network), enable the residents to access each other, the sensors that track the fire, and central intelligent information servers that help them plan a route to safety. The system continues to work in the face of sensors and transmission towers destroyed by the fire and adversarial users.

The Federal government and its private-sector partners should enhance existing research programs to carry out comprehensive, complementary, and synchronized actions focused on attaining these high-priority goals. As networking visions, capabilities and research needs advance as a result of these actions, the Federal government and its private-sector partners should coordinate to focus their efforts on the changing research needs. Federal R&D progress toward the goals, in conjunction with complementary private-sector efforts, should accelerate the evolution of advanced networks including the Internet, as have previous Federal R&D advances.

Mid-Decade Advanced Networking Scenario #1: Civil-Military Crisis Response

In a major crisis, critical infrastructures are destroyed, disrupted, and seriously degraded, including those supporting communication, transportation, health care, electricity, and other resources. Responders must establish information services to coordinate operations within and across their diverse organizations as they tend to human and environmental needs and restore the damaged infrastructure. This is a challenge in natural disasters and accidents such as an explosion at an oil refinery, but when the crisis involves terrorism or other hostile actions, the response also must contend with potential adversarial activities.

Heavy military support for transportation, logistics, and infrastructure augmentation are likely to be required, and military command and control and information systems will potentially be the mainstays of the operation in the early stages, before other capabilities can be brought to bear. In adversarial situations, military and intelligence organizations will also contend with hostile activities and provide information collection and analysis capabilities to help inform the decision makers and the first responders.

First responders will need to assess the situation quickly and thoroughly to determine the location and status of local resources, identify additional resource needs, and plan and manage response actions. Distributed sensors and forward-deployed personnel will provide information on the status of the local population, roads, health care facilities, and weather, and on the ability of local personnel and agencies to participate in the response. Networks will link these sensors, systems, and individuals to one another and to the systems that provide situation assessment and command and control at the local, regional, and national levels. Intelligence, surveillance, and reconnaissance (ISR) systems will operate on the ground and in the air to support the full range of activities, including identifying, tracking, and targeting hostile entities.

The military, commercial, and nongovernmental organization networks will be interconnected to establish an ad hoc federation using the best available resources. Adaptive QoS and the ability to coordinate management of network resources will support reliable, responsive, and pervasive network-centric operations from the highest-level command and control locations to the forward-based responders. The network will be built from an ad hoc assembly of radio and free-space optical equipment to support highly dynamic requirements of personnel and devices on the move. It will extend into buildings, tunnels, and other locations where line-of-sight communications are obstructed, and it will provide gateways to national and global networks via airborne relays and satellites. It will support both data transfers and voice, often configured as dynamically changing multicast groups or voice nets. Contention for radio spectrum will be managed across the network and ISR systems to assure that information collection/dissemination requirements can be met.

Responders will be able to receive and transmit appropriately filtered and formatted requests for transportation, medical support, and logistic support with assured security.

Framework for Federal R&D Agenda

The framework for this Plan is the Federal R&D in advanced networking needed through the middle of the next decade to achieve the strategic vision of new government capabilities described above. This R&D includes a subset of the agency activities described in the Networking and Information Technology Research and Development (NITRD) Program's *Supplement to the President's Budget* plus additional networking research programs not reported under the NITRD Program. The NITRD Program in advanced networks (as defined in the budget supplement) is funded at approximately $462.4 million (FY 2008 Estimate); the activities included in the Plan represent fundamental networking research programs of about $204 million of this total. Operational issues, application-specific software, the deployment of advanced networks to support current Federal research and engineering efforts, and commercial development and deployment of new capabilities are considered to be outside the Plan's framework.

The Task Force analyzed the research needed to achieve each of the Plan's strategic vision goals by the 2015-2016 time frame, from the starting point of the current knowledge base and Federal capabilities for mission-critical objectives. For each of the Plan goals, the following five dimensions of networking research are considered:

Foundations: Develop architectural principles, frameworks, and network models to deal with complexity; heterogeneity; multi-domain federation, management, and transparency; end-to-end performance; and differentiated services.

Design: Develop secure, near-real-time, flexible, adaptive services with built-in intelligence to facilitate discovery, federation, and management of resources across domains and to increase the application robustness and resistance to attack even in extraordinarily complex systems and new ways of interconnecting networks to provide those services.

Security: Achieve a high degree of security even in complex, heterogeneous federation and policy environments, especially in the face of component failures, malicious activities, and attacks, while also respecting privacy and maintaining usability.

Management: Develop management methods and tools that enable effective deployment, control, and utilization of networks and resources in dynamic environments, across domains, and with ever-increasing network and application complexity.

Usability: Develop adaptable, user-centered services and interfaces that promote efficiency, effectiveness, and fulfillment of user needs without overwhelming users with unneeded data – while maintaining appropriate security.

Appendix 2 (page 26) presents, in tabular form, detailed results of the Task Force analysis of Federal networking research needs. The table's four columns identify: (1) specific capabilities needed to achieve each of the Federal Plan's four goals; (2) the current state of practice in each capability; (3) the expected results of the Federal agencies' existing and planned research programs, which are designed to satisfy the agencies' mission needs through the middle of the next decade; and (4) some of the significant challenges that could remain.

The Appendix 2 table is designed to provide a range of policy and planning options for two different timeframes. The accelerated networking security timeframe highlights capabilities that could have substantial impact on improving security in the current networking environment. These capabilities for near-term impact are indicated by underlining in the table. (See also, Section 3: "Accelerated Networking Security Focus.")

The core Plan focuses on the middle of the next decade and has as its goal fundamental advances to transform the networking landscape. The table provides two categories of longer-term targets: those that are accessible under existing or planned programs (column 3) and those that require a more aggressive effort (column 4). The magnitude of the change depends, in large part, on the category of targets selected. Selecting a mix of targets from the two categories can create a range of options.

The increased complexity of future networks requires thinking beyond traditional models for network research (i.e., focused on specific technologies). R&D should target the development of architectures and frameworks that can integrate many technologies to deliver the services needed for mission accomplishment. While incremental engineering advances are necessary in the near- and mid-term timeframes, R&D also must address the basic and applied research to build a more robust science base and to enable more effective engineering for the longer term. To maintain that focus, the coordinated Federal research efforts carried out under this Plan should especially emphasize three key aspects of the technology development and commercialization cycle:

- **Basic and applied research** in the full range of network hardware, software, security, and middleware needed to support the next generation of uses for networks and explore new paths to develop capabilities that cannot be supported on the current evolutionary path
- **Partnerships with application developers, users, and stakeholders** to test basic research ideas on real problems in areas including national security, support of scientific leadership, and human health
- **A range of testbeds and prototype networks** that enable understanding of the effects of, for example, scale and complexity on the entire networked system

A balanced basic and applied research thrust is necessary to fill the intellectual pipeline with visionary ideas and concepts that push beyond incremental change to suggest fundamentally new networking approaches. The second two emphases are essential to address the enormous and growing complexity of networks, which cannot be effectively understood or evaluated in limited-scale explorations. Partnerships with application developers provide the most powerful means of increasing understanding and analysis of network dynamics in real interactions with mission-critical applications such as large scientific collaborations or disaster recovery.

Similarly, testbeds provide real network environments at scale and with the ad hoc dynamics that researchers can use for experimentation, research, and development on both networking technologies and applications. In addition to advancing understanding, researchers in at-scale network environments can engage in “clean slate” research to develop competitive new approaches to the most challenging technical problems – such as how to make extreme network complexity manageable. Such at-scale foundational advances should accelerate adoption of useful new technologies. Further, testbeds enable demonstrations of the value of innovative applications as well as development of the networking standards that will drive future communications industries. Testbed demonstrations can include commercial participation to assure that new capabilities can meet standards and economic criteria for adaptation to the marketplace.

Federal work in scientific foundations for advanced networking is particularly important now to drive development of a new generation of approaches and technologies that can provide flexible network resources to enable dynamic scheduling, co-scheduling, allocation, configuration, and use based on user requirements and to increase the security, reliability, flexibility, and end-to-end performance of the Nation’s networking infrastructure. This Plan also directly supports the American Competitiveness Initiative’s (ACI’s) call for increased Federal investment in physical sciences research and in the tools of science – including advanced networking – to enhance U.S. leadership in scientific and technological innovation.

Mid-Decade Advanced Networking Scenario #2:
Large-Scale Scientific Research

Many domain-specific science instruments, applications and grids – including the Large Hadron Collider (LHC) at the European Organization for Nuclear Research (known as CERN), high-resolution multi-scale climate modeling, fusion energy (the international ITER project), nuclear physics analysis (the Relativistic Heavy Ion Collider [RHIC]), and the Open Science Grid (OSG)[3] – will be implemented with requirements to move petabytes of data in near-real time among distributed analysis and storage sites*. Physicists using LHC, for example, will have coordinated at sites throughout the world to increase the portion of data that can be analyzed from less than 10 percent to over 90 percent by moving unprecedented amounts of data among distributed analysis sites.

Reliable, near-real-time movement of these data will require moving an exabyte (one billion gigabytes) per year among worldwide sites. This will rely largely on ultra-reliable, high-capacity networking, requiring new transport protocols to move hundreds of gigabits per second of data transparently over networks among worldwide sites crossing political and network provider boundaries. Advanced networking capabilities will be needed to provide transparency across highly heterogeneous security policies (including identity management) and network provider technologies.

The development of dynamic network management will enable optimization of international high-capacity network links to assure priority data transport when needed, while allowing other uses at less demanding times. In an era in which large science projects are increasingly international, advanced networks will be critical to enable the Federal government to reap the benefits of its investments in these facilities. In addition, advanced networks will enable the best researchers to use the most important data to do the best science independent of the location of their institutions. All domain-specific scientists will be integrally involved in identifying user requirements and research needs and in developing and testing new capabilities.

[3] Other domain-specific research networks include:
- Laser Interferometer Gravitational-wave Observatory (LIGO)
- Network for Earthquake Engineering Simulation (NEES)
- Collaborative Large-scale Engineering Analysis Network for Environmental Research (CLEANER)
- National Nanotechnology Infrastructure Network (NNIN

2. Technical Discussion of Strategic Vision Goals

Each of this Plan's strategic vision goals presents challenges that require significant enhancements to the architectural, scientific, and engineering basis for networking. Meeting the goals will require increased understanding of how complex, dynamic, heterogeneous networks behave and how they can be managed and controlled. Advances will enable delivery of increased levels of service within natural constraints, such as the speed of light, or administrative constraints, such as limitations of the available radio spectrum. The following discussions briefly describe the technical challenges to be overcome.

Goal 1: Provide Secure Network Services Anytime, Anywhere

Goal 1 is to provide reliable, secure network services, unimpeded by user mobility and able to draw upon all available transport means in support of any application or service demand. Network resources can be managed to meet user needs and priorities, with a robust ability for distributed, real-time resource control and a mix of management and monitoring (some parts centralized with some parts distributed to end users so different monitoring and fault diagnosis tools tailored to the management and application needs can be used) to assure stability and responsiveness. Resource management contends with requests for scarce resources such as spectrum for radio links or QoS within an overall network that also includes optical and landline links. Networks can support a mix of high-throughput and low-throughput needs and can tolerate delay and disruption. Security and service protection can contend with adversarial actions, natural disasters, and unintentional interference and can maintain and restore services based on operational priorities as well as customer service agreements. The questions below suggest the research areas in which significant challenges need to be addressed.

- **Foundations**: Can we develop frameworks, architectures, and policies for protocols, services, and management that enable diverse applications over diverse and heterogeneous network transport technologies to provide end-to-end performance and differentiated levels of QoS and security?
- **Design:** How do we enable secure, near-real-time, flexible, adaptive end-to-end services for dynamic, heterogeneous environments? For example, a system to support medical interventions in a disaster area might require high bandwidth to send X-ray data and lower-bandwidth, ultra-low-jitter services for medical device control, both services preemptively scheduled and using wired and wireless technologies including ad hoc networks. Engineering such a system will require tools to federate heterogeneous capabilities to provide the necessary levels and guarantees of service.
- **Security:** How do we provide multi-domain identity management and secure access to services in the face of natural faults and attacks, particularly those that are previously unseen, can impact many components, that spread rapidly, and that modify themselves in transit? Mitigation methods must respect policy and privacy, particularly when sensors associated with humans are involved.

- **Management:** Can we develop techniques and tools to manage services that rapidly adapt to policies and changing availability of services with a high degree of automated functioning?
- **Usability:** Can we develop services that adapt to the rapidly changing needs and contexts (including social, economic, and legal) of users, deliver high performance, and hide complexity?

Goal 2: Make Secure, Global, Federated Networks Possible

Today's Internet is a federation of literally thousands of independent networks operated by all types of entities, from commercial telecommunications providers to small companies and non-profit organizations, worldwide. The current Internet approach to linking these networks together through the Border Gateway Protocol and Layer 3 peering has resulted in global connectivity; however, it does not support many of the advanced services or levels of assurance that will be required in the future. In addition, the federations of the future will include networks (e.g., wireless, mobile, ad hoc) with novel characteristics that must be integrated. The questions below highlight some of the critical areas of research in global federated networks that need to be addressed.

- **Foundations:** How do we develop architectural principles, such as design principles for network-to-network interfaces capable of learning, that will enable federations of networks to reliably provide a rich set of end-to-end services on demand? How can such federations share enough data across network boundaries to provide these services without compromising the integrity of the individual members of the federation?
- **Design:** How do we enable users to discover, schedule, and monitor resources across a federation without requiring them to become network wizards?
- **Security:** How do we provide protection of privacy, confidentiality, and property rights across varying technical, legal, and regulatory frameworks cooperatively among networks to cope with natural faults and attacks, given that each network has its own policies with attendant security and privacy needs? This cooperation must respect the needs of the individual networks but also be effective to stem attacks, especially previously unseen attacks.
- **Management:** How can networks work together across a federation to optimize their joint ability to deliver services to users in a way that scales to federations with hundreds of members? How do we provide out-of-band management channels to help diagnose and correct problems in the event of catastrophic failures?
- **Usability:** Can we build federations that seamlessly link different technologies, types of networks, and network administrations to enable users to flexibly develop new services and researchers to rapidly test new ideas?

Goal 3: Manage Network Complexity and Heterogeneity

Communications networks are among the most complex structures that have ever been developed. Billions of end nodes are interconnected by millions of devices scattered across the world and in some cases the solar system. In addition, only small islands within this system are controlled by a single entity. These systems can change their position in space and their topology of interconnection in time, sometimes rapidly. Often, the networks at all layers comprise multiple, simultaneous topologies that interact and change during the course of transactions. The result is a highly complex and interacting ensemble of dynamic, nonlinear processes that will exhibit chaotic and complex emergent behaviors and must be treated as such – not as the more stable and disciplined networks of the past. Understanding the behavior of this type of system is a critical prerequisite for networking advances, as is determining how to exercise a level of control that is appropriate. The questions below highlight some of the critical areas of research in complexity and heterogeneity that need to be addressed.

- **Foundations:** Is there a theory for complexity in networks that can lead to optimal architectural choices and enable us to describe, predict, and control the networks of the future?
- **Design:** How do we build new types of networks that integrate network devices and end systems in a way that adapts to the resources of all of the devices in real time and increases the robustness of these complex systems? What abstractions and principles of design can reduce complexity and provide more manageable systems?
- **Security:** Can we develop new theories and models for security in massive, complex networks including a control model of security; implementation of diversity, randomness, and deception to foil an attacker; and game theory to model an attacker and the defense?
- **Management:** How do we develop management tools and models that enable small groups of people to effectively deploy, control, and manage networks with exponentially increasing complexity?
- **Usability:** How do we build tools that enable automation of much of the management of complex networks and provide humans with the right information at the right time to enable human intervention when it is needed? For example, research is needed on a national public safety network using complex, tightly coupled networked systems to respond to terrorist attacks, natural disasters, and catastrophic accidents.

Goal 4: Foster Innovation among the Federal, Research, Commercial, and Other Sectors through Development of Advanced Network Systems and Technologies

Advanced networks are built on a number of fundamental technologies including software protocols, optical switching devices, semiconductor designs, and adaptable radio frequency (RF) technologies. New technologies are continually developed and implemented to enable new applications. Each fundamental technology must be integrated into the overall network. This integration is expected to significantly impact each of the first three goals – in some cases, in a truly disruptive way. The questions below highlight the areas in which significant challenges need to be addressed.

- **Foundations:** Can we develop automated, adaptive, and dynamic technologies to provide routing, transport, and management across heterogeneous network transport technologies, protocols, and policy domains?

- **Design:** How do we build technologies with a high degree of automated intelligence for dynamic adaptive interoperation of components and services across heterogeneous network transport technologies, protocols, and policy domains even while they are under attack?
- **Security:** Can we develop new security devices and technologies, including quantum cryptography and key distribution, tamper-resistant co-processors that enforce security policies or monitor other processors, trusted chips, minimal- or zero-kernel operating systems that are provably secure, new evaluation methods (including methods to analyze complex programs) for security, and hardware techniques that enforce separation of processes?
- **Management:** To what extent can we develop technologies to automatically manage services and resources (including power) across domains in heterogeneous environments? For wireless services, can we reduce system size and dynamically manage spectrum and power usage?
- **Usability**: How do we provide integrated photonic and electronic circuits to support high-capacity, high-data-rate functionality? How do we enable users to relearn, retrain, and adapt to the rapidly changing technologies?

3. Accelerated Networking Security Focus

While the longer-term goals in this Plan have targeted timeframes in the middle of the next decade, the Task Force recognized that some special focus and prioritization is needed to respond to current national networking security concerns. The networking security component of the Plan provides the option for accelerated R&D in certain areas to meet the national requirements for increased networking security, reliability and cyber defense. The special focus could help protect critical infrastructure and strengthen strategic networks in both routine and crisis situations.

Each of the four goal areas defined in Section 1 above includes capabilities that could accelerate progress towards a secure and reliable networking landscape. The selected capabilities are listed under each goal below. These capabilities –described in greater detail in the table of Appendix 2, where they are identified by underlining – align closely with the strategic Federal R&D objectives set forth in the April 2006 *Federal Plan for Cyber Security and Information Assurance Research and Development.*

The accelerated networking security component of this Plan embraces the same vision and framework as the core Plan component and comprises a subset of the same capabilities. Thus, pursuing the accelerated networking security focus effectively accelerates progress on the core Plan component.

Goal 1: Provide Secure Network Services Anytime, Anywhere
Assure network, device, and information security, reliability, and availability for all types of users, network implementations (wired and wireless), and physical and logical topologies. R&D in:

Survivable Services:

- Shared situational awareness
- Minimized effect of denial of service
- Correct routing and forwarding of traffic in the face of attack
- Security for survivability
- New, adaptive transport protocols
- Dynamic negotiation of QoS

Protection of Information:

- Identification, authentication, and authorization across heterogeneous policy domains
- Fine-grained protection of data distributed across a network
- Alerts when information protection is threatened by unknown attacks
- New models for detection and prevention of release, accidental or otherwise, of proprietary and private information (exfiltration)

Goal 2: Make Secure, Global, Federated Networks Possible
Assure all members of an ad hoc federation that their systems and data are protected to the same degree as within their own domains. R&D in:

Multi-level Identity, Security, and Privacy across Domains:

- Support of access control at a fine-grained level
- Ability to move data and processes across domains while respecting security, privacy, and regulatory concerns

Policy-Enabled Security Management and Real-Time Adaptation:

- Ability to enforce policies in real-time under threat situations

Cooperative Defense against Cyber Attacks:

- Ability to operate normally through attacks
- Automated protection adapted to environment and policy

Goal 3: Manage Network Complexity and Heterogeneity

Provide capability to understand and manage services and assure security and availability across complex, self-organizing systems. Improve the usability of security and privacy applications to reduce human risks. R&D in:

Trust in Complex Environments:

- Trust models that accurately reflect the security state of nodes in a network and permit the automatic association of trust with nodes
- Metrics to support quantitative assessment of the trustworthiness of complex networks and systems
- Engineering methodologies, design principles, formal techniques, and modeling tools that can be used to facilitate the construction of secure networks of unprecedented complexity

Goal 4: Foster Innovation among the Federal, Research, Commercial, and Other Sectors through Development of Advanced Network Systems and Technologies

Improve ability to produce and verify trusted technologies, including software and devices; assure development partners that their products and data are protected. R&D in:

Secure Hosts/Devices:

- Secure development environments including the authentication of developers and the pedigree of code
- Design trustworthy hosts/devices such as virtualized, high assurance platforms
- Establish composability of system security properties
- Enable trustworthy execution of mission on potentially compromised networks / systems

4. Research Priorities and Federal Agency Research Interests

Networking Research Priorities

This Plan envisions new, dynamic networking capabilities including wavelength-routing optical switches with switching times on the order of a few nanoseconds, transparent interoperability among heterogeneous services (IP, MPLS, SONET, MSPPs, etc.), and the creation of dynamic virtual private networks. It supports the future ability to integrate existing wired, wireless, and IP-based infrastructures into a Next Generation Network fabric supporting secure, end-to-end, heterogeneous, multimedia networking. Appendix 2 identifies many of the capabilities needed to support this vision that will be enabled by 2015-2016 as a result of the current priorities and research programs of the Federal agencies. These programs are focused on the networking needs of the agencies to address their agency missions and are among their current priorities. Federal agencies with advanced networking R&D programs will continue to update their priorities and research programs as visions and needs change and as research results are integrated into deployed networks. These updates will be guided by input from domain-specific science and advanced networking researchers, program managers, commercial sector users and developers, and others with interests in advanced networking capabilities and research.

The NITRD program provides a forum for coordination among the Federal agencies on Networking and Information Technology Research and Development. In the Large Scale Networking Coordinating Group (LSN CG) of the NITRD Subcommittee, the Federal agencies present their networking research priorities, programs, and agendas to provide a common view across the agencies of the full spectrum of Federal networking priorities and research. This enables the Federal agencies to cooperatively develop research policies, priorities, and programs to address the dynamic, changing needs for networking research. Thus research priorities are developed on a continuing basis in consultation among the Federal networking research agencies.

Appendix 2 of this document identifies projected networking capabilities in the 2015-2016 time frame given the current Federal agency networking research programs. The appendix also identifies remaining network challenges and capabilities in 2015-2016 that are needed to empower the networking vision. These are the capabilities that could accelerate progress towards a secure and reliable networking landscape. They are near term priorities for networking research investments.

Federal Agency Research Interests

Federal agency research programs are designed to address the networking research needed to support the agency mission requirements. The Federal agencies have current networking research programs, presented in Appendix 3, to address the current priorities and needs of the agencies. Representative current research areas for the agencies include:

- NSF: Theoretical foundations, cyber trust, sensor systems, and applications support
- DoD: Dynamic secure wireless technologies, sensornets, secure networking in challenging environments
- DARPA: Dynamic secure wireless technology, heterogeneous networking, trustworthy systems, management of dynamic complex networks
- DOE/Office of Science: Petascale data transport, QoS, distributed large-scale science cooperation, secure Grid environments
- NASA: Large-scale data transfer, disruption tolerant networking, multicast
- NSA: Cognitive radio technology, Delay Tolerant Networks, control plane
- NOAA: Applications, data transport, and collaboration environments
- NIH/NLM: Large data set access, disaster response, applications (BIRN, caBIG, Visible Human, MedlinePlus)
- NIST: Architecture and standards for resilience/robust/secure networks, resilient mobile wireless, performance measurement
- USDA: Rural telecommunications technologies, sensornet testbeds

These basic interests, supporting the missions of the agencies, are expected to continue in the future. However, in the dynamic networking environment (where technical capabilities advance, new and changing applications need new types of network support, and responses to new security challenges are needed) agency research strategies and priorities must be responsive to opportunities presented by the changing landscape.

5. Conclusions

The overall conclusions of the Task Force can be summarized as follows:

1. **Improved networking security and reliability are strategic national priorities.**
   Advanced networking research not only empowers key Federal missions – national defense, homeland security, including emergency and disaster response, and leading-edge scientific research – but drives U.S. economic competitiveness and innovation throughout the private sector. This conclusion is consistent with that of the President's Council of Advisors on Science and Technology (PCAST) in its recent assessment of the NITRD program:
   "U.S. leadership in advanced networking is a strategic national priority."

2. **New paths to advanced networking are needed.**
   The current generation of networking technologies has inherent limitations and vulnerabilities. A research and development strategy is required that both ensures the emergence of new technologies, tools, and capabilities to strengthen network security and reliability, and supports rapid transfer of these technologies to the commercial sector. The path described in this Plan focuses on the networking research dimensions of Foundations, Design, Security, Management, and Usability.

3. **Federal R&D efforts will support a spectrum of advanced networking capabilities.**
   A spectrum of capabilities will create the advanced networking landscape of the future and this requires a broad Federal R&D effort. These capabilities include effective security, anytime-anywhere networking, the ability to manage network complexity and heterogeneity, and continuing innovation for networking leadership.

4. **Close cooperation is needed to integrate Federal R&D efforts with the full technology development cycle.**
   Close cooperation is needed among Federal research managers, researchers, application developers, users, stakeholders and international partners to develop and test basic research ideas on "real world" applications in areas including national security, support of scientific leadership, and human health.

5. **Testbeds and prototype networks enable research on network challenges in realistic environments.**
   Testbeds and prototypes offer a variety of settings ranging from the disruptive and unstable to production and at-scale environments. Some network research and development advances will necessarily be pursued on testbeds that must be disconnected or in a restrained environment to allow for disruptive network experimentation. Other forms of prototyping and trialing will occur with more mature ideas and development, in settings that may even blend into a production network environment. A number of testbed facilities, over a range of size, connectedness, ability to integrate with applications, and other dimensions

would support the diverse types and scales of experimentation and prototyping that, in the end, will achieve key advances in networking. Public-private partnerships can also leverage these Federal research resources for the development, adoption, and commercialization of research results and standards.

Appendix 1
Charge by the Director, Office of Science and Technology Policy

January 30, 2007

Dear Committee on Technology Members,

I am writing to inform you of the establishment of the Interagency Task Force on Advanced Networking under the Networking and Information Technology Research and Development Subcommittee. As detailed in the attached terms of reference, this group is charged with developing an interagency *Federal Plan for Advanced Networking Research and Development*.

The Federal government depends upon fundamental advances in networking technology for enhancing a wide range of applications including emergency response, national security and emergency preparedness communications, defense mission support, health care information technology, secure economic transactions, distributed intelligence applications, and advanced scientific computing. These applications share a need for faster, more secure, more reliable, and more robust networks than are currently available. Federal basic research investments enable accelerated development of these networks to support government needs, and can also lead to substantial improvements in commercially deployed networking that is an important driver of the U.S. economy.

The agency representation on the Task Force should, to the extent possible, reflect the full range of relevant Federal activities, missions, needs, and perspectives. Agency participation in the development of the Plan should be followed by full commitment to its implementation. Task force members are asked to produce a draft Plan by May 2007, to be followed by a final Plan as soon as possible thereafter. This schedule will allow timely input during the FY 2009 budget planning cycle and will require substantial time commitment by agency representatives. Department and agency leaders are asked to encourage and support the participation of their staff in this important activity.

Sincerely,

John H. Marburger, III
Director

FOR OFFICIAL USE ONLY

TERMS OF REFERENCE

Interagency Task Force on Advanced Networking

The Interagency Task Force on Advanced Networking (ITFAN) is hereby established under the Networking and Information Technology Research and Development Subcommittee of the National Science and Technology Council. The ITFAN is charged with developing an interagency *Federal Plan for Advanced Networking Research and Development* that will lay out a comprehensive research and development strategy necessary to facilitate the successful development of and transition to future network architectures. The Plan should include the following components:

1. A strategic vision for advanced networking that addresses the current and future networking needs of Federal agencies, the commercial sector, and the academic community.

2. Recommended scope and objectives for Federal advanced networking R&D to appropriately support the defined needs, and how these objectives relate to those of the private sector.

3. Identification of existing networking R&D programs and investments, a gap analysis of existing versus needed advanced networking R&D, and prioritization of advanced networking R&D needs.

4. Identification and prioritization of advanced networking R&D needs, including architectures, systems, services, R&D infrastructure, and technology transfer that must be advanced to strengthen the foundation for advanced networking technologies.

5. A process for developing an implementation roadmap that will guide future advanced networking R&D activities, including individual Federal agency and coordinated multi-agency activities. The process should ensure that the implementation roadmap will represent the full breadth of relevant agency activities, will identify specific agencies best able to carry out both individual and multi-agency activities based on expertise and facilities, and will reflect the relative priorities identified by the Task Force.

The *Plan* should also include an analysis of the appropriate roles for Federal investment in R&D to address the networking needs of the Federal government that are unlikely to be met by existing or future commercial networks. In particular, the advanced networking requirements of Federal agencies with a scientific research and development mission and Federal agencies with a homeland and/or national security mission should be recognized, particularly where agency missions are likely to be adversely affected by a lack of progress in advanced networking technologies.

John H. Marburger, III
Director, Office of Science and Technology Policy

FOR OFFICIAL USE ONLY

Appendix 2
Network Research Challenges, by Goal

This appendix presents in tabular form the results of the Task Force analysis of the Federal networking research program. For each of the Plan's strategic vision goals (subdivided into the research dimensions of Foundations, Design, Security, Management, and Usability), the table shows four categories of information. The first column of the table identifies a specific capability. The second column summarizes the current state of practice in that area. The third column displays the expected results of the Federal agencies' existing and planned research programs, which are designed to satisfy the agencies' mission needs through the middle of the next decade. The table's fourth column lists some of the significant challenges that could remain.

The table is designed to provide a range of policy and planning options for two different timeframes. A near-term timeframe highlights capabilities that could have substantial impact on improving security in the current networking environment. These capabilities for near-term impact are indicated in the table with text underlining.

The longer timeframe focuses on the middle of the next decade and has as its goal fundamental advances in the networking landscape. The table provides two categories of longer-term targets: those that are accessible under existing or planned programs (column 3) and those that require a more intensive effort (column 4). The magnitude of the change depends, in large part, on the category of targets selected. Selecting a mix of targets from the two categories can create a range of longer-term options.

Goal 1: Secure Network Services Anytime, Anywhere			
Capabilities for Foundations Goals	**Current Practice**	**Middle of Next Decade Projection**	**Remaining Challenges**
· **Service virtualization**	· Programmability only available on small-scale test beds · Concepts for service virtualization are known, but not yet widely tested or deployed	· Programmability in the software is available at distinct levels · Progress in self-configuration and dynamic adoption	· Virtualization for large-scale networking; wireless networks; security, and e-science research · Minimal-size resource controllers, programmable hardware and software, and optimized resource and scheduling models
· **Multicasting**	· Dynamic and heterogeneous multicasting demonstrated with limitations on scalability and	· Developing ability for dynamic and heterogeneous multicast. · Wireless users can change physical position yet remain connected	· Context, time, and location aware multicasting · Scalability and resource optimization for

		cross-domain functionality for the general Internet	· Automated management of group connectivity · High utilization of available link bandwidth over sporadic links	groups that span domains, change membership frequently, and involve heterogeneous technologies · Delivery assurance contending with diverse requirements, throughput and delay constraints · See also security challenges
	· **Quality of Service**	· QoS is primarily static, prearranged and constrained to single domains · Commercial capabilities provide setup of point-to-point services with guaranteed QOS within a single domain · Some applications can set the QoS field per the application requirement.	· Emerging ability for timely adaptation of QoS · QoS based upon mission parameters and developed automatically	· Dynamic and on demand end-to-end resource scheduling and allocation with guarantees · Unicast, multicast, and broadcast messaging with diverse levels of QoS
	· **Architectures for future services**	· Collections of mechanisms and schemes, but no holistic view in operational systems; some progress in research	· New Architectures reveal important functions like location and performance · New protocol stack and network management support robust mobile operations; higher data rate, less overhead and repetition	· Reference framework with new layers better adapted to heterogeneous, on-the-move networking; multimedia messaging; distributed control; network churning · Network protocols, services, management concepts that allow diverse applications over diverse transport network technologies, with different levels of QoS and security along an end-to-end path
	· **Distributed, self-organizing**	· All current adaptive, self-	· Scalability to tens of hundreds of nodes and	· Understanding and modeling of complex

services	organizing processes, including Mobile ad hoc Networks (MANETs) have scalability and availability issues. · Local algorithms can provide some "self-correcting" behaviors but they are currently limited in scalability and stability · Lack of formal mathematical principles for understanding complex, adaptive behaviors	stability improvements for adaptive, self-organizing processes · <u>Emerging ability to understand state of complex systems sufficiently to establish mixed distributed and centralized monitoring and control processes</u>	systems will impact all aspects of dynamics, scalability, topology, and heterogeneity · Ability to respond to attacks or to contend with undesired emergent behaviors · Use of semantic web technologies to enable intelligent control, including tagging and federation of services across heterogeneous domains and semantics
Capabilities for Design Goals	**Current Practice**	**Middle of Next Decade Projection**	**Remaining Challenges**
· **Always available**	· Best effort delivery with potential for differentiated services on a prearranged basis · Domain access and interconnect prearranged by service agreements. · Heterogeneous internetworking with satellite communications backbone subject to Satcom availability and cost	· Near real-time management of spectrum contention · Wireless users can change location yet remain connected · Intelligent network maintains connectivity and message delivery · High utilization of available link bandwidth over sporadic links. · Improved data rates in urban settings by exploiting multiple pathways (multipath)	· Adaptable wireless networks that trade-off programmability and dynamic optimization of spectrum use · Capability for scalability, self-interference (co-site, near/far…) and adversarial interference · Capability to operate while under attack and in face of natural faults · Higher layer processes, protocols, and APIs to contend with network churn, disruptions, and outages · Dynamic inter-domain connectivity and resource management that accounts for variations in user demands and network state. · Services where infrastructure is

				lacking or damaged. · On-demand QoS per connection, session, or by reservation
	· **Reliable services on-the-move**	· Adaptation of Internet protocols to support nomadic and limited on-the-move services, but all Mobile Ad Hoc Networks (MANET) suffer scalability limitations due to frequency availability · Movement across domains without manual intervention, but not without brief disruption of service · Adaptive power control in wireless networks	· MANET ability to support clusters at medium scale · Smooth mobility within wireless clusters in one domain · Direct sequence spread spectrum improves robustness and capacity for mobile, tactical wireless networks and reduces dependence on infrastructure · Improved data rates in urban settings by exploiting multipath · Hybrid Free Space Optics/RF link and networking scheme that yields high availability and data rate · Wireless network scalability increases at least one order of magnitude · Networks adapt to loss of nodes and other topology changes	· Adaptive services (including security, privacy, and QoS) that reflect priorities with minimal disruptions during transitions · Wireless ability to move smoothly across domains · Adaptive solutions through new protocols to provide scalability, stability, and real time response for auto-(re)configuration and maintenance of services across all users and network domains · RF issues including spectrum constraints, co-site interference, near-far interference and adversarial intrusion and disruption in wireless portions of the network · Relays to contend with line-of-sight limitations · Develop models, policies, and management structures for adaptive mobile networks · Common interface standards for protocol conversion · Programmable and self-configurable network interfaces and protocols (including link and physical layer) for roaming through very diverse domains · Mobile user

				services adapted for individual users based on location, user tasks/interests, and current context · Individual privacy against intrusive tracking while on the move · Distributed network/storage to assure continuity of services under adversarial conditions
	· **Information at your fingertips**	· Network status information is available primarily at centralized network operations facilities · Minimal ability for users or gateway/cluster-head nodes to view and interpret status or automatically insert management change requests · Other types of information in data bases distributed across network are accessible with the aid of web crawlers and browsers, but tailoring to user needs is not supported in most cases · Limited demonstration of multicast network management enabling any node to access management services	· Emerging ability for high level nodes (gateways, cluster-heads) as well as formal network operations centers to view network status and insert change requests. · Initial ability of agents to identify and tailor data to user	· Complete network status information available and sharable across network entities end-end. · Embedded measurement in large scale testbeds with ability to support users at various levels of security during simultaneous experiments · State information at a level of abstraction suitable for understanding of status and with drill-down capability for proactive and reactive network management, diagnostics, and forensics · Intelligent data collection, storage and movement for use by applications and users
	· **Transport for heterogeneous mix of demands**	· Routing, switching, and service delivery protocols are predefined and optimized for either packet switched or circuit switched	· Hybrid packet and circuit switching improves transport efficiency by an order of magnitude · Knowledge-value oriented transport improves "effective QoS"	· Architecture and protocols to optimize transport according to message type and QoS requirements in real time. · Knowledge-value based multicast

		services · High data rate, long duration transport over packet switching supportable by reservation protocols, but little ability to adapt in near real time for a changing mix of diverse services demands	and ability to adapt to diverse demand. · Proactive link selection mechanisms optimize use of available diverse link types on platforms while adapting to environment and user demands · Hardware and software mechanisms increase throughput by a factor of 10 · Architecture, protocols, and control and management software for highly dynamic, multi-terabit global core fiber-optical networks	messaging adapted in real time to widely heterogeneous network states and individual user requirements · Optimize performance for ad hoc networks with diverse, unpredictable traffic loading and with uncertainties at the network physical level · Simultaneous, adaptive multiplexing of services ranging from high throughput, long duration transmissions to short burst traffic

Capabilities for Security Goals	Current Practice	Middle of Next Decade Projection	Remaining Challenges
· **Survivable services**	· Network defense mainly reactive, with forensic analytical ability but little proactive defense · Restoration relies mainly on manual processes. · Emerging mobile, tactical technologies provide automated survivability services · Scalability, dynamic range, and potential adversarial impacts are being investigated · Ad hoc coordination of disaster response and public safety networks	· <u>Shared situational awareness improves ability to contain damage to networks</u> · Automated ability to proactively adapt to attacks and to assist manual restoration processes. · <u>Minimized effect of Denial of Service (DoS) worm-based attacks (to include zero-day exploits). Objectives are automatic detection, quarantine, and recovery; containment to 1% of network functioning; recovery in minutes; high Probability of Detection /Low Probability of Failure</u> · Hybrid Free Space Optical/RF link and networking scheme for high availability and data rate, with physical media diversity to contend with attacks	· <u>In the face of attack, maintain correct routing and forwarding of traffic Provide differentiated services and preemption where needed</u> · Assurance for critical services in face of attacks and natural faults. · <u>Security for survivability; self-healing and disruptive tolerant mechanisms</u> · Contend with adversarial actions targeting distributed, self-organizing processes · Multilevel cross-domain situation awareness and control for cooperative defense. · Affordable

			· Policies and self-organizing technologies for disaster response and public safety networks	architectures for wide scale deployment of large scale network defense · Virtualization technologies for active network defense, to observe network services under stress or attack, and to “disinform” and confound malicious actors · New transport protocols that can adapt to different applications and transport media · Dynamic negotiation of QoS when under attack or subject to natural degradation or disruption
	· **Protection of information**	· Over-the-air key distribution but based largely on predetermined user addresses and locations · Severely limited ability for multi-level security and privacy	· Multi-level access controls within prearranged secure enclaves that can cross some domains	· Information protection for diverse needs (beyond multi-level security and compartmentalization) · Identification, authentication, and authorization of network devices/users across multiple heterogeneous policy domains, including device security posture, reputation, and geographic location · Fine grained protection of data distributed across a network · Alerts when information protection is threatened by unknown attacks · New models for detection and

			prevention of release, accidental or otherwise, of proprietary and private information (exfiltration) · Protection in face of exploitation of covert or cryptographic side channels · Identification of potential information flow channels but combined with dynamic analysis to have the potential to identify all flows in violation of a protection policy · Multilevel access privileges for heterogeneous multicast groups · Encryption while maintaining policy enforcement points and associated security services, e.g., intrusion protection and access control via firewalls
Capabilities for Management Goals	**Current Practice**	**Middle of Next Decade Projection**	**Remaining Challenges**
· **Topology and policy management**	· Minimal ability to change QoS policies and topologies over time or to coordinate priorities across domains · Different types of management systems available that do not interoperate. · Identity management in limited domains	· Automated assistance for management of priorities for classes of users within domains with manual enactment aided by predefined templates. · Manual network tuning replaced with automated adaptation · Identity management federated across multiple domains	· Automated policy adaptation to rapidly changing contexts to reflect availability of critical resources and mission needs · Delegation of management authority to the edges of the network, negotiation of authority, and management actions at boundaries of other domains · Distributed sharing of knowledge of network state, projected needs, and other basic factors, with cross domain

				access policies adapted to the current situation · Local decisions based on network service objectives · Optimize network management to prevent a need for over provisioning · Fully integrated network operations capabilities including: fault management, information assurance management, and proactive (near real time) management of routing and switching topologies and protocols
	· **Resource control and assignment**	· Predetermined QoS and resource control policies · Management and control relies mainly on static view of networks, throughput rates, and queues	· Near real time QoS management for selected users using manual control · Network and transport layer policy management to contend with hot spots and choke points · Application of network science to assist in monitoring of state and control of resources. · Dynamic allocation of RF spectrum in frequency, space, and time for increased utilization, robust dynamic connectivity; reduced spectrum management setup time and increased spectrum access · Hybrid, adaptive free space optics/radio frequency networking for high availability and data rate. · Networks are co-scheduled with other resources, such as computers and instruments	· Proactive, real time assignment of resources to satisfy current policies and QoS agreements · Mixed-initiative (human and automated) supervision of distributed, self-organizing, autonomous processes to assure stability, robustness, and optimized use of resources · Improved scalability and processing loads for large domain and cross domain applications · Real time feedback to network management system to drive adaptation of policies and QoS agreements within and across domains · End-to-end, near real time adaptation of resource coordination across

				domains for point-to-point and multicast services · Dynamic allocation of RF spectrum in frequency, space, and time among heterogeneous wireless networks

Capabilities for Usability Goals		**Current Practice**	**Middle of Next Decade Projection**	**Remaining Challenges**
	· **Services adapt to needs and contexts**	· Services unable to adapt to near real-time needs and are predefined by service level agreements and network throughput availability	· Emerging ability for information tailoring based on user needs · Initial ability for adapting QoS objectives to respond to needs and constraints for highest level users and within individual advanced network domains · Dynamically allocate RF spectrum in frequency, space, and time to increase effective use of spectrum and reduce spectrum management setup time	· Provide all users with information related to service availability · Allow all users to request and receive services based on needs, priorities (both local and global), and network capabilities · Capability for cross domain adaptation for QoS objectives · Dynamic service level agreements and information tailoring for inter-network quality of service · Architecture, standards, and protocols for applications to negotiate with the network for QoS adaptation · Adaptive handling of traffic in heterogeneous multicast groups and across heterogeneous networks · Function through network churning, delay, and disruption. · Automatic adaptation of upper layer protocols and processes in near-real-time
	· **Complexity hidden from users**	· User is aware of network limitations only in terms of service delays and	· On-screen advisories of current status · Ability to view projected status based on intent to establish	· Provide users with information at a level of abstraction and with visualization suitable to their needs

		disruptions	sessions that imply heavy use (e.g., VTC)	and capabilities · Automatically identify user capabilities and needs based on behaviors and context · Fault correlation for distributed, near real time diagnostics · Intuitive, user-friendly ability for non-expert users to correct problems with a button click
	· **High-performance middleware**	· Initial development of high-performance middleware · Commercial approaches to Service Oriented Architecture are informed by but not built on standards	· Expanded discipline science support by GRID technologies · Middleware supports specific application domains and communities of interest	· Middleware software and services to support rapid application development and deployment across domains and communities of interest · Real-time access to networked resources on a global scale · Combined management plane and middleware services for real-time access to networked resources on a global scale · Policy management to enable end-user access to network resources · Anticipate users' need for data and pre-fetch critical data based on AI projections of context and demand · Real-time adaptation of presentations and applications for end-to-end QoS optimization · Automatic translation and semantic mediation
	· **Complete transparency**	· Transactions require knowledge of IP address, URL, or formal user ID	· Emerging semantic web capability relieves requirement for specific IP address, URL, or user ID	Semantic web capability and ability for addressing based on location, context-based categories, as well as

				standard address, URL, and ID

Goal 2: Secure Global Federated Networks			
Capabilities for Foundations Goals	**Current Practice**	**Middle of Next Decade Projection**	**Remaining Challenges**
· **Architecture for global federated network**	· Seven-layer model oriented on relatively stable topologies · Adaptation for mobile, dynamic users requires significant cross layer interaction with manual coordination and configuration · No vertical integration of application (grid reservation and scheduling systems)	· Continued use of IP and seven layer model for most applications · New protocol stack and network management for robust Mobile Ad Hoc Network operations	· Services oriented on mobility, security, and adaptability in massive, dynamic, heterogeneous, network federations · Enabling distributed network systems to discover, self-organize, and share critical information to support federated e2e network services such as control and data planes signaling, security and QoS policies signaling, network management · Improved ability to coordinate multiple control plane architectures · Secure control plane architecture and protocols that integrate different technologies (QoS, MPLS, GMPLS, etc.) · Out-of-band management channels for diagnosing and correcting problems after catastrophic failure. The ability to probe a failed network from a separate infrastructure
· **Theory, techniques, and tools**	· Network control plane technologies (QoS, MLS, GMPLS) - MPLS-based QoS control plane accessible only by individual networks · Inter-domain services as best-effort IP peering arrangement limited	· Domain specific reservation systems · Inter-domain reservation accomplished via email and voice · Custom/domain specific implementation of QOS, MPLS, and GMPLS	· Performance models for complex adaptive networks, including interactions among networks of varying degrees of complexity · Performance models based on multiscale analysis · Virtualization models and architectures for federated networks

		to reachability information · QoS obtained with over-provisioning		· Protocols that scale to support diverse applications (e.g., real-time, streaming, mobile services, video, visualization) and transport technologies such as wireless, optical, sensor-net, and satellite · Automated and seamless coupling of federated network services to end application to make effective use of host software stack and network resources · New mathematical theories to model and simulate traffic engineering processes in large-scale federated networks · Inter-operable multi-domain MPLS and GMPLS

Capabilities for Design Goals	Current Practice	Middle of Next Decade Projection	Remaining Challenges
· **Enable users to discover, schedule, and monitor resources across federations**	· Phone-based and email exchanges to coordinate sharing of information among users · Limited sharing of state information across domains to enable user services · Multicast and full sharing across heterogeneous network subject to security and policy restrictions · Web crawlers, directories, and other methods that place the burden on the user to find the right sources among a massive set · Minimal ability for individual users to schedule and monitor resources	· Phone-based and email exchanges to coordinate sharing of information among users · Search engines with advanced AI will improve ability to focus on relevant information	· Control and signaling plane technology that can assist the end users by seamlessly integrating diverse technologies (wireless, optical, packet switched, circuit switched, etc) to compose e2e path with user-defined characteristics · Tools to allow the users to view network monitoring, status reporting, and control information · Enable users to interact with network management to optimize performance to meet local demands while remaining globally consistent · Distributed policies engines to support

				multi-domain end-to-end QoS, security certificates, SLAs, etc.
	· **End-to-end services**	· Best-effort IP network · Significant overhead when conditions are dynamic	· Higher data rate, less overhead and repetition, less fragile comms in dynamic mobile environment · Service Level Agreements (SLAs) and science applications with modest end-to-end performance enforcements enabled	· End-to-end service optimization of traffic across autonomous domain boundaries · Multi-domain control plane signaling technologies that provide services such as circuit/bandwidth reservation, resource discovery and scheduling, network fault isolation across end host layers and federated domains · Cross autonomous system multicast synchronization · Traffic engineering of hybrid networks
Capabilities for Security Goals		**Current Practice**	**Middle of Next Decade Projection**	**Remaining Challenges**

	· **Multi-level identity, security, and privacy across domains**	· Limited capability, mainly relying on manual processes · Reliable certificate revocation not possible · Trusted switches, sanitization guards, low-high pumps provide limited ability to deal with multiple securities but transport requires segregation into virtual private cryptonets	· Increased automated capability in specific domains · Routers, switches, and end - user equipments support multiple security levels at the message or database entry level · PKI and related technologies support sub-compartmentalization within individual security domains	· <u>Multi-level security and accountability: support of access control at a fine-grained level</u> · <u>Ability to move data and processes across domains while respecting security, privacy, and regulatory concerns</u> · Moving data and applications in a Virtual Machine (VM) package across platforms/ domains, securing the identity of the VM, and providing access · Security of information flows determined by static analysis of program code and hardware and by dynamic analysis · Automatic transformation of data (e.g., downgrading) that crosses domains · <u>End-to-end security optimization across admin. domains</u> · Distributed IDs and coordination of certificate authorities · Methods to address insider attacks and forensics · Transform networking security into an engineering problem/solution by developing formal methodologies for specifying, developing, and testing cyber systems, and a formal language to specify networking security policies · Techniques to enhance capability of cyber tools · Concept of Quality of Cyber Protection (QoCP)

	· **Policy-enabled security management and real-time adaptation**	· Limited capability, mainly relying on manual processes · Policy is mostly static and predefined · Limited ability to preserve policies, privacy, security for users moving across domains	· Increased automated capability for a limited number of domains · Emerging capabilities for management and dynamic implementation of security policies for ad hoc situations	· Ability to automatically create, transform, and reason about policies that govern the movement of data and processes across domains · <u>Ability to enforce policies in real-time under threat situations. Mediation occurs at the network interfaces</u> · Pre-need negotiation: adaptive to changing contexts and threat · Automatic determination of releasability based on content and context as determined by a policy that is learned automatically
	· **Cooperative defense against cyber attack**s	· Very limited capability, mainly relying on manual processes	· Improved state awareness and ability to intercept attacks and prevent total collapse. Processes rely on manual intervention supported by the improved automated monitoring capabilities · Minimize effect of worm-based attacks through automatic detection, quarantine, and recovery; containment to 1%; recovery in minutes; high Probability of Detection/ low Probability of Failure · Transform isolated, vulnerable programs into self-defending teams · Commercial-off-the-shelf (COTS) software applications collaboratively diagnose and respond to problems (attacks, bugs)	· Ability to mitigate attacks (known and unknown) in a coherent and effective manner · <u>Cooperative, distributed information management that permits sharing of early indications data and alerts for real time, distributed, automated reasoning on threats and responses</u> · Ability to filter unencrypted information at line rate. Correlate in-flight monitoring data in real time with archived logging information to troubleshoot anomalous behavior

Capabilities for Management Goals	Current Practice	Middle of Next Decade Projection	Remaining Challenges
· **Enable inter-domain exchange of management information**	· Phone-based and email exchanges of network measurement · Management centralized within domains · Limited ability for visibility of network status across domains · Adaptation subject to individual domain policies and procedures	· Improved cross domain coordination with limits for end-to-end service optimization and in near-real-time · Reductions in federation overhead · Manual network tuning replaced with automated adaptation with remaining issues for cross-domain, cooperative management and control	· Interfaces that automatically determine releasability of sensitive data, but releasability changes with context as determined by a policy that is learned automatically · Shared awareness and distributed adaptation, subject to near real time controls on releasability of private and/or proprietary data and cross-domain control actions · Standards for publishing network management information · GPS and out-of-band distribution of network management information
· **Enable interdomain cooperation of networks to provide services**	· Cooperative but not fully collaborative · Best-effort network services predominate · Limited inter-domain MPLS-based QoS using custom phone and email exchanges (issues for emerging IP telephony, IPTV, etc.) · No inter-domain reservation systems · Little or no ability for end-to-end management and control other than prearranged policy agreements · Inability to deal with heterogeneous QoS policy agreements	· Emerging distributed self organization across domains · Advanced bandwidth/QoS guaranteed services over multiple networks for 10s to 100s of QoS channels or VLANs	· Automated End-to-end service-level optimization across administrative domains · Judicious combination of pre-need negotiation with adaptivity to reflect changing contexts and threats · Federated network management systems that enable local network management systems to collect and share critical information for diagnosing end-to-end faults · Intelligent network management systems

Capabilities for Usability Goals	Current Practice	Middle of Next Decade Projection	Remaining Challenges

	· **Evolvable platform for innovation**	· Inability to address the special needs for interconnecting new computing and networking technologies such as sensor network with Internet · Networks depend on traditional IP interdomain routing exchange · Complexity of global network is a barrier to new applications and services	· Progress extending sensor applications across the core of the Internet partitioned at the level of the sensor net · Hybrid Free Space Optics/RF link and networking scheme that provides high availability and data rate in challenging environments · Hybrid circuit/packet services will be available in select research and education domains.	· Seamlessly link wireless, sensor, and Supervisory Control and Data Acquisition (SCADA) control networks to wired networks · Enable application developers to rapidly test and deploy novel services across multiple administrative domains · Enable network managers to enter into Service Level Agreements and track success in meeting these SLAs across domains · Enable researchers to rapidly deploy multi technology, multi administration environments to test new ideas in network science

Goal 3: Complexity and Heterogeneity

Capabilities for Foundations Goals		Current Practice	Middle of Next Decade Projection	Remaining Challenges
	· **Understanding complexity**	· Minimal capability to understand behavior of highly dynamic, complex, adaptive networks · No well tested experimental paradigms to measure complexity · Simulations cannot be validated due to lack of test-beds at scale · Understanding of system state is oriented on networks with fixed topologies and with “snapshots” of static status with little understanding of the effects of derivatives or statistical distributions and relationships	· Developing capability to recognize emergent behaviors early enough to take action. Main reliance is on manual actions based on computer generated displays · Developing understanding of complex, adaptive processes limits the degree of dynamics, scalability, and heterogeneity for mobile ad hoc networking · Network state is estimated mainly based on “snapshots” and some degree of prediction and reasoning based on	· Understanding of highly complex networks and interconnections of complex networks of varying (and time dependent) degrees of complexity. · Temporal and spatial behavior models · Validated simulation/emulation environments that take network and environmental effects into account with high degree of confidence on accuracy · Fundamental science to enable models that can describe, predict, and

			derivatives and statistics will emerge	control the behavior of next generation networks · Improved mathematical basis for complex, adaptive systems to address interference, contention, and adversarial actions in mobile, ad hoc wireless networking
	· **Architectures for future networks**	· Architectures are based on traditional network theory and are fragile and unsuitable for many of the new, dynamic, ad hoc situations · Current architectural principles, standards, and protocols provide system designers and network managers with little support to contend with real time and near real time behaviors in complex, adaptive networks	· Introduction of a richer and more advanced set of application-support features · New IP protocol stack oriented on robust MANET operations will support higher data rate, less overhead and repetition, less fragile comms in dynamic mobile settings · Architecture, protocols, and control and management software for highly dynamic, multi-terabit global core fiber-optical networks	· Technical reference model oriented on mobile, wireless, complex adaptive networks · Architecture and protocols to deal with increasing cross-layer interactions as the "static" Internet evolves to a more dynamic and heterogeneous structure · Network architectures with built-in security, manageability, scalability, resiliency
	· **Advanced network design**	· Lack of good theoretical representations · Limited basis in network science leads to ad hoc, incremental changes to deal with problems as they arise · Designs are mainly an extension from initial Internet: protocols and concepts, with mobility and security accommodated as modifications constrained by the basic architecture. · Disruption or delay tolerance and delivery assurance in heterogeneous, multi-hop relays are major issues	· Beginning of cross-layer traffic engineering based on formal mathematical principles · Improvement for mobility, security, and delay/disruption tolerance · Manual network tuning replaced with automated adaptation in diverse networks	· A theory of networked computing addressing the increasing complexity of networks and interconnection of multiple networks of varying and time-dependent degrees of complexity · Artificial diversity; holistic optimization tools · Application of physical layer theoretical representations for network and protocol design
Capabilities for		**Current Practice**	**Middle of Next Decade**	**Remaining Challenges**

Design Goals		Projection	
· **Networks without borders, beyond gateways**	· Islands of different networks connected through gateways · Small research programs focus on different types of networks (sensor, wireless, etc.)	· Incremental improvements in layer 2 and 3 devices · More hybrid networks · Larger programs for more holistic research · Layers 1 and 2 provide ability for increased mix of wireless services and mix of broadband and narrowband transport · Enable wireless users to change physical position yet remain connected · Network assumes responsibility for message traffic · Improved utilization of available link bandwidth over sporadic links	· Enabling integration of diverse types of end systems into the heterogeneous, complex network · Continuous diagnosis with routers, gateways, etc. that can deal with threats to the network core · New mechanisms for heterogeneity to support an increased mix of wireless services and mix of broadband and narrowband transport · Improved ability to service increasing demands for heterogeneous work sessions, multicast groups, and other uses of group services where members have different capabilities and needs · Protocols and technology to achieve high-performance/throughput · Inter-domain technology to increase stability and decrease vulnerability of complex systems to maintain user services (including QoS and multicast) in adversarial environments

Capabilities for Security Goals	Current Practice	Middle of Next Decade Projection	Remaining Challenges
· **Trust in complex environments**	· No guarantees of security or privacy beyond highly secure, protected enclaves · Concern about massive collapse due to emergent behaviors and adversarial exploitation of tendencies toward chaotic behavior	· Improvement for both security and privacy with safe, “gated” communities · Cryptonet and application layer visibility improved with manual processes for management and	· Models of security and privacy that reflect the complexity of networks · Cryptologic-based methods to achieve revocable anonymity · Architectures to increase randomness

	· Insufficient ability to view and manage security and privacy in mobile/dynamic network situations · Denial of service is a critical problem and is handled mainly through reactive and forensic measures	control · Emerging ability to anticipate and respond to threats before damage spreads throughout network. Minimize effect of DoS worm-based attacks; automatic detection, quarantine, and recovery; containment to 1% degradation of the network functionality; recovery in minutes; high Probability of Detection/Low Probability of Failure · Automated channel switching capability in response to adversary jamming attack. · Transform isolated, vulnerable programs into self-defending teams · COTS software applications collaboratively diagnose and respond to problems (attacks, bugs)	to potential attackers, e.g., through artificial diversity · Trust models that accurately reflect the security state of nodes in a network and that permit the automatic association of trust with nodes · Ability to understand and respond to emerging threats including anticipating the threat posed by well resourced bad actors · Metrics to support quantitative assessment of the trustworthiness of complex networks and systems · Engineering methodologies, design principles, formal techniques, and modeling tools that can be used to facilitate the construction of secure networks of unprecedented complexity
Capabilities for Management Goals	**Current Practice**	**Middle of Next Decade Projection**	**Remaining Challenges**
· **Managing and controlling networks in the face of complexity**	· Depends on skilled operators · Relatively slow and cumbersome for adapting to near real time changes · No significant ability to deal with the special needs for controlling mobile ad hoc networks · Initial demonstrations of capabilities for limited degrees of heterogeneity, dynamics, and complexity	· Increasing ability to characterize complex network states · Improvement in available management tools · Developing ability for automated agents to support human-decision-making · Policy based management built to allow for QoS and other resource management changes in dynamic networks. · Prearranged management and	· Network management operations that allow automated self-organization with ability for manual and/or combined human-and-automated (mixed initiative) intervention supported by network visualization tools · Methods to gather, coalesce, process and store data about the current state of increasingly complex networks

		control of distributed, autonomous, adaptive networks · Presence of stable backbone networks will be needed to support relatively small ad hoc clusters and other users on the move · Response to disasters and military expeditionary operations will rely on broadband long haul support infrastructure · Wireless network technologies will support networks with scalability increased by at least one order of magnitude and with capability that adapts to mitigate hardware shortfalls and environmental conditions	· Improved ability for management and control of distributed, autonomous, adaptive networks to respond to dynamics, disruption, and changes in QoS requirements
Capabilities for Usability Goals	**Current Practice**	**Middle of Next Decade Projection**	**Remaining Challenges**
· **Adjustable autonomous networks**	· Adaptation and change require humans-in-the-loop · Responses to disasters and military operations will continue to need heavy infrastructure	· Exploration of intelligent technologies for autonomic behavior · Network wireless node based on commercial products supports network adaptation, scalability, and mitigation of hardware shortfalls and environmental conditions	· Control of massive, complex, autonomous networks · Networks that automatically accommodate to changing contexts and threats in a policy-aware manner · Mixed initiative, human-automated intervention to oversee and stabilize distributed self-organized processes
· **Human factors category**	· Mismatch between the service of the Internet, in terms of physical devices, and the needs of users, defined in terms of services	· Emerging improvements in usability and user comprehension	· Information visualization to help users understand the state of complex networks · Active visualization methods to suggest operational goals using visual metaphors · Social networking,

				game theoretic principles, and cooperative networking concepts

Goal 4: Technology

Capabilities for Foundations Goals	Current Practice	Middle of Next Decade Projection	Remaining Challenges
· **Routing schemes**	· Circuit or packet, but not both at the same time	· Merger of cellular and Internet routing and switching schemes and adaptation of protocols to incorporate best features	· Context aware communication devices · Transparent interoperability across heterogeneous technologies (packet/ switched, dynamic mobile/wired, satellite, and delay tolerant networking · Application based networking optimization · Technologies and mechanisms independent of assumptions and characteristics based primarily on wire-line networks. · Efficient wavelength conversion
· **Transport protocols category**	· IP (with TCP and UDP) dominates, with link layer switching for wireless access to backbones	· Continued emphasis of IP, with increased influence of wireless protocols · Enhancements to IP and new protocols enable wireless user to change physical location yet remain connected · Network assumes responsibility for message traffic · High utilization of available link bandwidth over sporadic links	· Adaptive cryptographic protocols supporting new architectural models · Dynamic transport layer technologies utilizing cross-layer information. · Reduce dependence on TCP for assurance of delivery over wireless networks, particularly for multi-hop transport over links of varying quality and stability · Transport protocols that can adapt and coordinate across layers in real time to optimize throughput

	· **Network science category**	· Rudimentary, based largely on queuing theory and routing protocols · Limited ability to operate adaptive, self-organizing networks beyond tens of nodes and in dynamically changing situations	· Increased use of graph theory to develop improved routing and transmission control protocols · Increased throughput, responsiveness, and reliability through the combined application of information theory and control theory to nodal and network design and operation	· Understanding man-made and natural networks to reflect a more comprehensive set of interactions, including interactions among complex networks of varying degrees of complexity and dynamics · Improved ability to address scalability and stability issues for self-organizing networks · Technologies and mechanisms independent of assumptions and characteristics · Distributed control systems theory to be deployed on networks · Understanding when to aggregate traffic, when to use multiple channels for traffic streams, and when to use complex modulation
	· **Optimization of signaling and processing, including modulation, coding, and transmission control**	· Current research on wireless modulation, coding, and transmission control to contend with channel error mechanisms and spectrum constraints and to allow design of small, low power, low cost equipment	· All aspects of message formation, coding, modulation, spectrum use, and delivery assurance predetermined · Hybrid cellular telephony and wireless LAN air interface protocols to improve efficiency · Order of magnitude improvement in dynamically allocating RF spectrum in frequency, space, and time to increase utilization, reduce dynamic connectivity spectrum management setup time, and increase spectrum access. Spectrum limitations increase for wireless services as data throughput and	· Interference avoidance and mitigation: both co-site and external, and scalable to massive, dynamic situations · Energy optimization · Spectrum agility: additional orders of magnitude improvement in spectrum use and adaptation to states at physical and link layers while maintaining service quality · Optimized, coordinated use of multi-domain radio and FSO links

		mobility demands increase · Gateways deal with transitions across media	
Capabilities for Design Goals	**Current Practice**	**Middle of Next Decade Projection**	**Remaining Challenges**
· **Integration of heterogeneous technologies**	· Mediators constructed manually based on publication of ontologies, standards, protocols, APIs, etc.	· Non-real-time automated construction of mediators · Gateways designed for interfacing multiple types of networks and end-user equipments and servers. · National scale testbeds that provide control and measurement supporting simultaneous experiments at different levels of security and confidentiality management and coupled to heterogeneous applications (IP, circuit-based, wireless, all-optical, sensors, satellites, etc.) · Cross-layer capacity management to assure aggregation of IP services in the optical layer	· Flexible network architecture and technical approaches to enable plug and play of new components · IP and WebSphere Platform Management (WPM) protocol integration, primarily at the control plane level · Near real-time mediation and adaptation of gateways · Increased intelligence in the network and at edges for mediating heterogeneity
· **Adaptability, survivability, interoperability**, **scalability, availability, manageability, reliability, securability, usability**	· Interoperability requires adherence to predefined standards, protocols, and formats · Reliability generally limited to best effort · Availability relies on predeployed infrastructure or preplanned mobile services · Survivability under physical and electronic attack is not built in for most services · Current research projects	· Interoperability based on predefined standards and protocols with formats and contents managed in near real-time to adapt to heterogeneity and changing situations · Predeployed infrastructure is the primary basis for availability. Ad hoc networking and airborne relay offer	· Interoperation of components and services at a level capable of supporting networking services over traditional, non-standard, and new system-wide architectures · Interoperability with in-network intelligence to adapt protocols for routing, switching, and information

		address wide range of "ilities" to support reliable ad hoc mobile services independent of predeployed infrastructure: QoS better than "best effort", adaptive data rate on a link by link basis, autonomous adaptation for both robustness and maximum throughput, contention with adversarial RF interference · Spam is proliferating and uncontrolled · Increased survivability and robustness of wireless services, e.g., adaptive layer one and two technologies and cross layer coordination of message packaging and error control · Adaptive relays to contend with line-of-sight limitations	services for high priority users · Advanced military systems provide order of magnitude increase in scalability, robustness, and adaptation for ad hoc dynamics and spectrum limitations · Developing proactive link selection mechanisms that address survivability and reliability by optimizing use of available diverse link types on platforms while adapting to environment and user demands · Improved data rates in urban settings by exploiting multipath · Hybrid Free Space Optics/RF link and networking scheme that yields high availability and data rate · Low cost handheld wireless devices based on commercial technology · Hardware and software mechanisms increase throughput by a factor of 10 · Wavelength-division-multiplexing LAN that can be used universally in any platform and transmit in analog and digital formats · Architecture, protocols, and control and management software for highly dynamic, multi-terabit global core fiber-optical networks · Enhanced performance, survivability and	packaging · Dynamic and distributed service resource control and pooling · Utilization of multi-topology (logical and physical) to increase network robustness · Tradeoffs in security vs. throughput (with complexity / resource consumption as constraints) · Scalable services across domains for ad hoc networking and airborne relay

			security over existing fiber; scalability for increase in capacity	
	· **Technologies for extreme environments**	· Small sensors with fixed capabilities · May not work in extreme environments · Long time for disaster recovery · Smart antenna	· Small sensors with integrated capabilities · Work in expected extreme environments · Disruption and delay tolerant networking capabilities · Improved time for disaster recovery · Low power, ultra-wideband sensors and comms systems · Robust comms in high multipath environments. · Low cost handheld wireless node based on commercial products: supports wireless network adaptation for up to tens of thousands of nodes, and mitigates hardware shortfalls and environmental conditions	· Unattended operations for extended periods · Small sensors respond to threats and environmental changes · Adapt rapidly to unexpected environments · Work through a disaster
Capabilities for Security Goals		**Current Practice**	**Middle of Next Decade Projection**	**Remaining Challenges**
	· **Trusted chips/components/systems**	· Trusted foundry for military and intelligence equipments but limited ability to assure trust in general purpose devices	· Trusted foundry for military, intelligence, and commercial equipments · Detection of security threats in chips, particularly those that are outsourced; enhanced chip-level support for cryptography, key management, secure booting, secure monitoring of computations to detect subtle attacks, attestation of programs	· <u>Trust at systems level to solve composability of trust problems similar to the composability of security systems</u>
	· **Quantum cryptography**	· Quantum Key Distribution (QKD) demonstrated at 100 KM · Commercial systems are just being introduced, but they are of limited	· QKD interoperability, e.g. with satellites · Threat models with emerging quantum computing are well	· Standardization of protocols and systems · New quantum protocols to support networking among quantum computers

		functionality · Short-distance functioning and low secure key rate · Engineering analysis and characterization are non-existent; threat models still need developing · Limitations remain in range, bitrate, media, and security · Service is inherently point-to-point	developed · Engineering analysis and characterization of quantum cryptography in large scale networking are well developed	and conventional computers · Quantum information and precision tests of quantum mechanics development of single photon engineering: high data rate, guaranteed single photon sources, low noise, high sensitivity, room temperature detectors, ultra-low loss fibers · Use of quantum entanglement in multiple dimensions · Multicast-capable architectures and associated protocols · Cross-domain, multi-hop reach. Long range at a practical key exchange rate
	· **Algorithmic cryptography**	· Preliminary research results in post-quantum cryptography		· Algorithmic cryptography that remains secure even with quantum computing
	· **Secure hosts/devices**	· No secure hosts/devices · Limited protection · Limited defense	· Defense against most attacks. · Protection set up and managed by humans. · Defense response initiated automatically · Wrap email and web browser applications with protective layer to prevent attacks on them from compromising host machine · Software to monitor integrity of operating system kernel data structures to detect sophisticated rootkit attacks · Systems that learn their own vulnerabilities to improve survivability over time, and	· Guaranteed secure hosts/devices. · Ability to operate normally through attacks. · <u>Automated protection adapted to environment and policy</u> · <u>Secure development environments including the authentication of developers and the pedigree of code</u> · <u>Design trustworthy hosts/devices such as virtualized, high assurance platforms</u> · <u>Establish composability of system security properties</u> · <u>Enable trustworthy</u>

		regenerate service after attack; survivability through redundancy, diversity, cognitive immunity and healing	execution of mission on potentially compromised networks/systems
· **Flexible chip designs**			· High performance programmable hardware with the flexibility of an FPGA and the complexity and performance envelope of an ASIC that can be loaded quickly with new code programmed with high-level tools
Capabilities for Management Goals	**Current Practice**	**Middle of Next Decade Projection**	**Remaining Challenges**
· **Spectrum management**	· Manual channel assignment · Little or no interference control for unmanaged bands (e.g. Wi Fi bands)	· Order of magnitude improvement in spectrum utilization. Emerging capability for intelligent netops to adjust basic assignments in near real-time	· Dynamic allocation, management, and brokering of spectrum while ensuring end-to-end quality of services in the full range of network technologies · Techniques for simultaneous, multi-function signaling, new multiple access techniques, and cross-domain coordination to provide order of magnitude improvement · Tailor messaging to decrease demand for spectrum
· **Power and energy management**	· Mix of preset transmission power and near real-time adaptation · Commercial cellular systems automatically adapt power at end nodes, switches, and routers to lowest power consistent with link quality requirements	· Hub-spoke networks, including cellular and MANET clusters exploit hardware for local power control to minimize interference and preserve battery life · Two orders of magnitude longer life for unattended ground sensors	· Systems consume, adapt, and generate power and energy to minimize energy consumption

			· Efficient power-aware design and management for High Performance Computing (HPC) clusters	
	· **Size management**	· Devices at centimeter scale, including antennas and batteries	· Devices at millimeter scale, including antennas and batteries · Range limitations addressed by larger antennas for large cells and ad hoc relaying with links greater than a few hundred meters.	· Embedded hybrid devices of sub-micron size that can be networked adaptively to operate in a range of environments · Antenna designs, e.g., spray-on, embedded, and self-organizing antennas to allow reduction in total unit size and greater efficiency. Embed networking technology within equipment cases and implant some devices in humans
	· **Hardware and software to support small-scale uses, disadvantaged users**	· Small devices and users on-the-move are seriously constrained by power requirements, battery lifetime, and equipment costs · Apertures are unsuited to multimode, multiband applications · Devices do not adapt automatically to environment or service demands	· New power sources, parasitic energy capture, and power management provide order of magnitude improvement · High data rates require proximity to backbone access points for radio links · Software configured devices adapt in near real time to demands and constraints · Direct sequence spread spectrum comms technologies: improved capacity of robust, mobile wireless networks where only end user equipments are available to support services · Robust urban comms to penetrate buildings and underground facilities · Improved data rates in urban settings by exploiting multipath	· Low bandwidth environments and environments involving unobtrusiveness (and stealth) for use in medical and military applications · Conformal integration of wireless devices into user platforms, clothing, and other substrates · Reduce power requirements and increase power management ability through software and firmware architecture to provide order of magnitude improvement of effective lifetime · Advances in energy capture, power generation, and power management to enhance device lifetime by another order of magnitude

	· **End-to-end troubleshooting**	· Ad-hoc monitoring within domains used for troubleshooting	· Increased cross-domain WAN monitoring · Increased topology discovery · Increase in publicly available network monitoring data to assist with troubleshooting · Increased ability to troubleshoot multicasting networks, toolsets	· Protocols to locate hidden network devices · Ubiquitous topology discovery services · Integration with end host and application monitoring for complete end-to-end troubleshooting · Ability of end users to troubleshoot their network paths
Capabilities for Usability Goals		**Current Practice**	**Middle of Next Decade Projection**	**Remaining Challenges**
	· **High-capacity integrated photonic and electronic circuits**	· Optical and electronic circuits and functions on a single chip	· Photonic circuits fully integrated to support high data rate transfers · Tunable transmitters and receivers · Replace ring with mesh networks. · Integrated, surface-emitting panel architecture for millimeter wave transceiver arrays · Active electronically steerable arrays achieving high power density and low layer thickness; vastly greater "functional density" without compromising performance in other areas · All optical switching and circuit-based grooming; ultra-high capacity, long-range transmission	· Higher capacity networks that are reconfigurable, more flexible and lower cost. · Very high index, low loss optical materials · Continuing: All optical switching and circuit-based grooming; ultra-high capacity, long-range transmission
	· **Geo-location** · **Hands-free operation** · **Automatic negotiation of QoS across all layers** · **Cognitive human-system**	· GPS, cellular location, time difference of arrival (TDOA) RF processing · Some degradation of capability in urban environments	· GPS enhanced while outside in urban environments. · Selective precision of location	· Navigation within closed buildings

	interfaces **· Technology Watch (adapt emerging technologies from non-networking domains)**			

Appendix 3

Recent Federal Networking Research Programmatic Areas, by Agency

NSF GENI	Large-scale facility of programmable networked systems, wireless access networks, security/privacy, Management, theoretical foundations
Networking Broadly Defined (NBD)	Non-wireless broad range of basic research
Future Internet Design: FIND	Clean-slate design: sensors, mobile wireless, supercomputer interfaces, all-optical, delay tolerant/real-time, security, management, human factors, virtualization
Networking of Sensor Systems: NOSS	Protocols/algorithms, architecture, privacy/security, HW/SW, Network programming/support, smart sensors: NEON (Ecology), EarthScope, ORION (Oceans)
Wireless Networks (WN)	Technologies (cellular, ad hoc, mesh, DTN,…), applications-based problems, architecture, phenomena, technology-oriented projects, programmable wireless networks (ProWin)
Dynamic data driven application systems (DDDAS)	Sensor networks and computer networks, emergency response (wireless phone)
Cyber Trust	Cryptography, formal methods, defense against large-scale attacks, applications (critical infrastructures, health care,…), formal models, hardware
Theoretical Foundations	Network optimization, cooperative networks, rate adaptation, security, reference models, MIMO nets, cognitive nets
Information and Intelligent Systems	Data-centric, human-centric, autonomous/robust/flexible systems
Engineering	Integrative, hybrid, complex systems; electronics, photonics, device technologies; power, control and adaptive technologies

Network infrastructure	International Research Network Connections, testbeds (Dragon, Cheetah, PlanetLab)
DoD: Net-Centric Operations Army Programs Navy Programs	Jam resistance, security and information assurance Adaptive networks, lab-scale testbed; Information Assurance; network science (model, design, analyze, predict, control behavior of heterogeneous nets); network functioning in disparate environments; ad hoc networks of imaging and non-imaging sensors; tactical wireless network assurance; Antennas; COMPOSER (In-theater wireless network management); radio-enabling technology and network applications; encryption Network application design (Web, Grid, agent-based); middleware services (service discovery, security); infrastructure vs. ad hoc environments; cross-layer integration for better performance; interoperable networks for secure communications; next-generation networking (MANET, autoconfiguration, collaborative approaches); interoperability approaches and standards; common coalition technology and evaluation methodology; airborne networking; multi-agent system operation in distributed ad hoc networks; battlefield sensor systems; wireless underwater acoustic sensor networks; protocols for reliable, efficient data delivery
Air Force Programs	Transformational Communications Advanced Technology Study – Airborne Communications Layer; optical networking; RF Optical Comm; Assured Access Anti-Jam Com; Cognitive Network Nodes; Battlefield Air Targeting Network; Intelligent Information Routing for Airborne Networks

DARPA Programs	(I2RAN); Network Agent Technology; on board multi wavelength optical networking for air and space platforms; high capacity, reliable RF and optical networking for airborne networking; mobile routing and networking of airborne tactical data links and radios; quantum key distribution and secure mobile quantum communications; high capacity satellite user terminals for on the move communications; policy based network management for airborne networks; integration and validation of wireless network, data link, data packet, network node, communication satellite models and simulations; wavelength routing; cross layer optimization; flexible, secure, highly responsive, ad hoc networks; embedded processing for networks Wireless technology: dynamic spectrum allocation, low-cost wireless hand-held nodes Link strategic and tactical networks: Optical linked to RF, spread spectrum, agile coherent optical, highly connected topologies top guard against failure Global network capability: core optical networks architecture, protocols, control and management; data over optical links, control planes, trustworthy systems
DOE/Office of Science	Petascale data transport Distributed, large-scale science cooperation Grid infrastructure prototyping
NASA	Software defined radio Large-scale high-efficiency data transfer High performance intrusion detection/prevention Disruption tolerant networking: ground/spacecraft Multicast data proliferation Planetary networking/space networking Bandwidth on demand Ubiquitous, anytime, anywhere networking
NSA	Cognitive radio technology for global communications over a fractionalized spectrum Delay Tolerant Networks (Reliability with intermittent availability) Evolution of the network core Control plane evolution Evolution of wireless/mobile networking Network tomography

NOAA: Network support to applications	Networks to support applications Emergency response (Weather nowcasts/forecasts for firefighting, deployable sensors, remote computing) Ecological monitoring (Fisheries management) Leverage in situ sensors Anytime, anywhere access by citizens Collaboration support (phased array radars, petascale computing,…)
NIH, NIH/NLM: Network support to applications	Large disparate data set access Real-time diagnostics with digital images Assisted surgery (Priority, low latency, low jitter, trustworthy) Security and privacy Programs: BIRN, caBIG, Visible Human, MedlinePlus
NIST	*Internet Infrastructure Protection* – Architecture and standards for resilience/robust/secure networks. *Public Safety Communications*: Develop requirements, standards, and measurement and test technologies *Robust Mobility and Wireless Networks* - Develop standards, measurement technologies, and test tools *Measurement Science for Complex Information Systems* – Define a systematic method to measure, understand, predict and control macroscopic behavior in complex information systems *Quantum Information Networks* - engineering and measurement, quantum cryptographic algorithms/quantum key distribution systems
USDA	Rural telecommunications technologies Testbeds for real-time groundwater monitoring Enhanced net-centric warfare (NCW) network capabilities: chip-scale atomic clocks, disruptive tolerant networking, dynamic worm quarantine, self-regenerative (security-aware) systems

Appendix 4
Existing Findings and Workshop Results

The Federal agencies, recognizing the critical importance of networking to support Federal agency missions, U.S. science research, e-health, e-commerce, and other applications, have held a number of workshops over the last several years to identify needs and recommendations for networking research to assure the continued viability and growth of networks and to improve their reliability, security, and robustness. These findings (followed by a number indicating the workshop or report source – see the citation list at the end of this appendix) include:

- Future networks need to provide architecture and run time capabilities for the multi-layer Grid (7, 8)
- Future networks must provide a materially improved level of security, availability and resilience, including provision of privacy and accountability, in the context of diverse cultural and regional norms (2, 7, 8)
- Future networks must support ubiquitous secure connectivity and computing using wireless links and subnets (3, 7)
- Future networks will need to be intelligent, dynamic and responsive to evolving situations. They will need to be self-organizing, dynamic, and responsive to applications, to support application responsiveness to networks, and to provide automated network management and QoS (1, 7)
- Future networks need to support adaptive, network-centric computing (4, 7)
- Future network designs must have intrinsic support for mobility at multiple levels (3, 7, 8)
- Basic research is needed to understand network behavior; to study the complexity of networked systems; and to deal with emerging complex, adaptive, network-centric systems (1, 4, 7, 8)
- Future network testbeds need to bring together network and application engineers, integrate computer science and telecommunications communities, academia-industry-government research teams, and provide government-leveraged industry funding, spanning the country (5, 7, 8)
- The design of a new scheme for location and identity is a critical architectural requirement to address issues of security, mobility, routing, and regional autonomy (6, 7)
- A future Internet should be designed without the requirement of a single address space (6)
- Future requirements for wireless networking include (5):
    - A clean slate approach to wireless architecture
    - Location services
    - Self-organization and discovery
    - Security and privacy
    - Decentralized management
    - Support sensor networks
    - Cognitive radio support

Sources of findings

1. Interagency Working Group (IWG) for Information Technology Research and Development (IT R&D), report of the "Workshop on New Visions for Large-Scale Networks: Research and Applications," March 2001, available at http://www.nitrd.gov/subcommittee/lsn/lsn-workshop-12mar01/index.html

2. "Social and Economic Factors Shaping the Future of the Internet," workshop sponsored by NSF and the Organisation for Economic Co-operation and Development, January 31, 2007; proceedings available at http://www.oecd.org/document/4/0,3343,en_2649_34225_39046340_1_1_1_1,00.html

3. DARPA, Assurable Global Networking, Request for Information, December 21, 2006, available at http://www.darpa.mil/STO/solicitations/AGN/index.html

4. D. Raychaudhuri and M. Gerla, Editors. "New Architectures and Disruptive Technologies for the Future Internet: The Wireless, Mobile and Sensor Network Perspective," Report of NSF Wireless Mobile Planning Group (WMPG) Workshop, August 2005, available at http://www.geni.net/wmpg_draft_200508.pdf

5. Corporation for National Research Initiatives, "The Gigabit Testbed Initiative," Final Report, December 1996, available at http://www.cnri.reston.va.us/gigafr/index.html

6. David Clark et al for DARPA/ITO, "New Arch: Future Generation Internet Architecture," Final Technical Report, December 2003, available at http://www.isi.edu/newarch/iDOCS/final.finalreport.pdf

7. Interagency Working Group on Cyber Security and Information Assurance, "Federal Plan for Cyber Security and Information Assurance Research and Development," April 2006, available at http://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf

8. President's Council of Advisors on Science and Technology (PCAST), "Leadership Under Challenge: Information Technology R&D in a Competitive World; An Assessment of the Federal Networking and Information Technology R&D Program," August 2007, available at http://www.nitrd.gov/pcast/reports/PCAST-NIT-FINAL.pdf

Appendix 5
Membership of the Interagency Task Force on Advanced Networking

DOD

Brian Adamson	NRL
Robert Bonneau	AFRL
Cary Chabalowski	SAALT
James Cook	DREN
Santanu Das	ONR
Cynthia Dion-Schwartz	OSD
Antonio Fiuza	ARL
Brendan Godfrey	AFOSR
Genevieve Haddad	AFOSR
Mark Jacobs	AFOSR
*Howard Marsh	OSD
Paul Phister	AFRL

DOE/SC
*Daniel Hitchcock
Thomas Ndousse
George Seweryniak

NARA
Robert Chadduck

NASA
Kenneth Freeman
Kevin Jones
Tsengdar Lee
Calvin Ramon
Charles Rush

NIH/NLM
Jules Aronson
Michael Ackerman

NIST
David Su

NSA
William Semancik

NSF
Frederica Darema
David Du
Darleen Fisher
*Suzanne Iacono
Karl Levitt
Allison Mankin
Paul Morton
Guru Parulkar
Sylvia Spengler
Sirin Tekinay
Kevin Thompson
Ralph Wachter
Jie Wu

OSTP
*Chuck Romine

USDOJ
Vance Hitch
Eric Olsen

Supporting NCO Staff
Nekeia Bell
Sally Howe
Alan Inouye
Martha Matzke
Ernest McDuffie
*Grant Miller
Virginia Moore
Diane Theiss

* Members of the ITFAN Executive Committee