Section 3.0 Summary of Networking Research Needs

This section summarizes the networking research needs identified in the Section 2.0 scenarios organized by research categories.

3.1 Adaptive, Dynamic, and Smart Networking

Most of the breakout sessions identified a need for research into elements of adaptive and dynamic networking to support ad hoc and mobile wireless access. The discussions of zero-casualty war and the medical applications scenarios identified the need to dynamically respond to developing situations with ad hoc, high-assurance networks supporting secure multimedia capabilities. In these scenarios, not only are the situations changing but also the participants in the networking sessions are changing with resulting changes in service requirements such as networking services, security levels, and end user devices to be supported.

Ad hoc networking to support deployable sensors for on-site chemical or temperature monitoring will require knowing the locations of the sensors and organizing them into a network capable of meeting requirements such as cost, location precision, measurement capability, power, and networking capabilities. Research is needed on self-configuration, connectivity to existing infrastructure, organization, and adaptation. Tradeoffs among functionality, performance, and cost will need to be understood and managed. For example, data aggregation and compression within the sensors may reduce communication requirements but increase sensor costs. Aggregation and compression may also affect the quality of the information sent to the monitors since such processing often changes the informational content and precision.

Future networks will be orders of magnitude more complex than current networks and must be able to respond to changing environments and dynamic networking as sensor elements are added and deleted. For example, large sensor arrays will be subject to sensor attrition that will require adaptive, dynamic, and smart networking to maximize the effectiveness of the remaining sensors. Engineering and managing these networks increasingly will require incorporating smart elements to automatically respond to the changing elements and environments. Research should also address the dynamic trustworthiness of the system and the information it is producing as the sensors and network change. Network measurement is fundamental to determining the status of networking elements to provide a basis for smart networking.

Smart networking research is needed for:

- Enabling sensors, networks, and applications to work together to increase the range of data granularity the system responds to and reports; for example, applications may vary significantly in the precision of a specific data parameter they require, thereby allowing data, system, or cost tradeoffs
- Automatically managing networks of increasing complexity including self-organizing, self-diagnosing, and self-healing networks

- Anticipating and automatically responding to network instabilities
- Network-aware applications that automatically respond to available networking resources
- Application-aware networks that automatically reconfigure networks to improve applications support
- Adaptive distributed systems: Applications may adapt based on network-provided information and system feedback, or the network may adapt based on information provided by the applications, as in implicitly adaptive networks.

3.2 Measurement, Modeling, Simulation, and Scalability

The Internet has expanded at a phenomenal rate, often driven by the need for increased capacity and capabilities to support new "killer applications" that in the past have included TCP/IP, e-mail, the Web, and Web browsers. With the continued evolution of Internet-based applications, types of media transmitted (for example large images and video), increasing connectivity of embedded devices, and increased support for arrays of sensors, the Internet over the next 15 years is expected to grow by many orders of magnitude in the number of nodes connected, amounts of information passed, and the number of users and their usage. Revolutionary new applications barely foreseen today are expected to lead to even faster expansion of the Internet and demand for Internet services. Instabilities may appear because existing Internet technologies and their evolutionary extensions could be severely strained to cope with this growth. Several of the breakout sessions discussed the need for research to address the growth, scaling, and stability of the Internet.

Network measurement

Each of these breakout sessions discussed the need for metrics and measurement of network performance. We do not have standardized technologies for measuring end-to-end Internet performance, let alone standardized reporting of measurements for most Internet nodes. This is a fundamental requirement for identifying current and developing bottlenecks and instabilities and for measuring improvements in performance as new capabilities are incorporated into the Internet. In the recent past, researchers have consistently observed that increases in network link bandwidth do not translate into proportional increases in end-to-end throughput for their applications. Measurement is imperative to study the causes of such behavior and to support engineering and management of the network links to improve performance for the end user.

Measurement research needs include:

- Intrinsic instrumentation: Make measurement a fundamental part of all systems on the network
- Extensible Application Platform Interfaces (APIs): APIs must provide measurement details to support network engineering to improve the end-to-end performance of the application
- Data reduction, formatting, and storage: Network measurement data collected in this environment must be reduced and stored in a format useful to end users. This

requires not only efficient data storage but also data synthesis, analysis, and formatting capabilities.

- National networking measurement archives: Provide a national archive to store network measurement data on a permanent basis. (Individual companies do not have the incentive to record and archive these data. Individual researchers do not have the resources required to provide the long-term archival storage.) A wide range of information should be stored, since we cannot now know what will later prove to be important.
- Ubiquitous inter-domain cooperation: Separate administrative authorities must agree upon a common set of measurement data that will be made available outside of their specific domains
- Correlation of measurements across levels: Data collected at the network connectivity, routing, end-to-end, and application levels must be correlated to provide a complete understanding of the system, to support network modeling and to provide a basis for network management.
- Synchronization of measurements: Measurements made at different levels and in different logical areas of the network must be time-synchronized to provide an instantaneous snapshot of network status and performance. The times when measurements are initiated must be synchronized and the ways timestamps are applied must be standardized.
- Modeling support: The measurement technologies must support network modeling to predict network failure modes, carry out network design and development, and enable network management.
- Security: The measurement system must support threat-evaluation models used to configure the network to withstand a wide range of possible attacks.
- Privacy: Measurement data must be securely transmitted to assure the privacy of individuals and administrative entities.
- New link types: The measurement and monitoring mechanisms will need to be adaptable to new link technologies such as optical networking.

Network modeling and simulation

Network modeling is needed to support research on network behavior and network management as the Internet grows in magnitude and complexity. Modeling is also needed to understand current network behavior and predict future behavior for assessing how new technologies will affect the stability of the Internet as they are introduced.

Network scalability

The network is expected to grow potentially by orders of magnitude, in the numbers of nodes, the amount of information, and the management complexity of the Internet. Current network architectures do not scale to handle these increases. A “science” of networked systems modeling is needed to understand how the Internet is likely to fail under increased loads, to fix potential problems before they occur, and to develop scalable architectures.

3.3 Trust: Security, Privacy, and Reliability

The Internet will be used for commercial, medical, scientific, and other uses only if users trust its security, privacy, and reliability. All of the workshop's scenarios inherently relied on this user trust. With the projected expansion of the Internet and the applications and media it carries, current issues in developing trust relationships will become more pervasive. The medical scenario relied on data access, consultations, and real-time collaborations with high assurance, security, and privacy. The disaster scenario identified the need to use distributed data and computing resources in near real time to support modeling and prediction and to support field units. The SWARMS scenario required security to protect against intrusion or espionage.

In some scenarios, it may be possible to quantify elements of security, privacy, and reliability associated with network elements or network links. Under these circumstances, "chains of trust" may be developed such that a user can choose networking paths based on highest overall trust or use information from specific network nodes that provide the highest confidence in the end product.

Trust may vary over time. Corroborating information may increase our confidence in information from some nodes or the networking architecture may change to a more reliable or secure pathway.

Security, privacy, and reliability research needs include:

- Quality of Service for critical applications in a complex environment that includes multiple providers, mobile and distributed access, and multimedia service (for example, for collaborations)
- Security, privacy, and reliability in dynamic, complex, and heterogeneous systems
- Scalability to accommodate heterogeneous environments and changing needs and hierarchies
- Trust modeling, configuring for trust, and responding to changing trust over time
- Trust retractability

3.4 Networking Applications

Each of the workshop scenarios relies on multiple networking applications. The workshop participants stressed the importance of developing these applications. Some of the applications identified in the scenarios that requiring networking research include:

- Telemedical remote collaboration with high assurance and security
- Sensornet: Self-organizing, dynamic, heterogeneous networks of sensors with network connectivity to remote resources
- Collaboratories: Support for interactions that are natural, intelligent, and secure, with multimedia capabilities and automated configuration
- Grid

- Hierarchical data delivery: Automatically develop and deliver data tailored to differing levels of an hierarchy

The workshop participants indicated that some of the potentially largest uses of the Internet will be for revolutionary applications not yet developed.

3.5 Networking Middleware

Networking provides connectivity among sensors, applications, end users, and distributed resources such as data repositories and computing facilities. Middleware assures that these elements work within a coordinated, transparent, and synchronized framework to provide end user services. Middleware can, for example, provide transparency among network service providers to seamlessly and securely transport information. Most of the workshop breakout sessions addressed the need to develop new middleware capabilities for networking.

The needs for enabling the Grid application illustrate many of the middleware networking needs, including:

- Vertically integrated, transparent, worldwide infrastructure for managing data and information, distributed storage, and access to computational resources
- Automated discovery of resources

Additional middleware needs identified in the scenarios include:

- Automated collaboratory setup, services, and toolsets
- Seamless, transparent service across heterogeneous network elements
- Control and management of dynamic networks
- Management of security, privacy, and reliability in a dynamic environment
- Automated measurement
- Productization to harden and standardize software by commercial developers

3.6 Testbeds

Workshop breakout session participants cited the need for testbeds to support networking research in performance measurement, security, privacy, reliability, active networking, adaptive mobile networks, intelligent networking, applications, and middleware. They also discussed the need for testbeds to bridge the transition from the research stage to successful commercialization of the technologies. An example is a Grid for high-energy physics research. Industrial participation in testbeds is often needed to develop and refine standards and to promote technology transfer.

3.7 Collaboration Environments

Networks support human interactions including human-to-human interactions such as collaborations and human-to-machine interactions such as access to distributed resources. Most of the breakout groups discussed the need for collaborations to be as good as face-to-face meetings or to have enhanced capabilities such as immersive environments or automatic translations, for example for international collaborations.

Some collaboration environment capabilities that the Internet should support include:

- Ubiquitous access with a plug-and-play capability
- Automatic configuration to accommodate the personal preferences and characteristics of the participants and the heterogeneity of their environments (including extreme differences such as PDA versus CAVE environments)
- Authentication, authorization, security, privacy, and access control
- Resource-sharing with remote collaborators
- Natural and intuitive interactions supported by virtual, immersive, and integrated environments that provide body language, visual, audio, textual, haptic, and olfactory capabilities
- Language translation
- Large-scale on-line virtual and physical models
- Expert consultation
- Whisper mode (support for side conversations)
- Automated supervisory oversight

3.8 Revolutionary Research

This report has identified many research areas that are important in assuring the future growth, functionality, robustness, and usability of the Internet. Evolutionary networking research is expected to result in improvements in these areas. However, high-risk revolutionary research may provide unexpected dramatic improvements that accelerate the capacity to meet the growing networking needs. Revolutionary research comes from revolutionary visions of research groups or individuals, adaptation of research from widely different disciplines, interdisciplinary collaborations, and other research initiatives.

Some areas of networking are in need of revolutionary research. For example, revolutionary research is needed to address the scalability issues that will be increasingly critical with the projected orders of magnitude increases in the number of network nodes, network users, and network traffic. Revolutionary research is needed to understand network behavior with these order of magnitude increases and to study networked systems' complexity. Disciplines such as chaos theory, economics, catastrophe theory, stochastic processes, and generalized control theory may contribute to these complexity studies.

3.9 Revisit Networking Fundamentals

The Internet is based on fundamental concepts, technologies, and standards such as the TCP/IP protocol that were developed and implemented decades ago. These standards and technologies have provided a robust infrastructure for the phenomenal Internet growth we have experienced since then, and which was not foreseen when they were developed. They may not be able to meet the still growing demands. For example, the Internet growth may exceed their ability to scale. Or some new technologies or a new protocol may provide greater efficiency, robustness, or ability to scale.

In 10 to 15 years, the core backbone network could well be Dense Wave Division Multiplexing (DWDM) optical with thousands of wavelengths per fiber. Broadly deployed network access will certainly be heterogeneous, incorporating broadband wireless, satellite, broadband wireline, and optical fiber with multiple wavelengths. Protocols and their associated services need to extend across these heterogeneous technologies with end-to-end transparent functionality. Fundamental changes may be required in addressing, routing, forwarding, and transport to support this increased scale and functionality. Revolutionary research, such as revisiting TCP/IP, can address basic issues of protocols, performance, complexity, and scalability.