Requirements for the Internet2 Next Generation Network

by the Abilene TAC
March, 2005

1. Introduction

As planning for the Internet2 Next Generation Network gets underway the Abilene Technical Advisory Committee (TAC) respectfully submits this document into the planning process. The TAC recognizes that the networking needs of the Internet2 community are changing in ways unexpected just a few years ago. It also recognizes that those needs may no longer be supported by the networking philosophies that drove the first two generations of the Internet2 backbone network, Abilene. The most significant change is the existence of the National Lambda Rail (NLR) and the fiber facilities, and direct control over those facilities, it makes available to the Internet2 community. Already, the Hybrid Optical Packet Infrastructure Project is examining ways of supporting new services over the combined resources of Abilene and the NLR.

It may be that it's time to consider that IP is no longer the common bearer service. It is certain that IP will continue to be the bearer service for most Internet2 Next Generation Network traffic but it may not be the only service provided. Therefore, while most of this paper focuses on requirements for aspects of the network used to provide an IP bearer service it is recognized by the TAC that a demand exists for other potential services. Finding a balance between the next generation network strengthening the "production level" of the IP service, the network's support for experimentation, and its support for new services has been the center of much discussion. However, it does seem clear that the community would best be served by improving the IP service while exploring options for new services. Section #7 explicitly addresses new services that may fall outside the traditional IP bearer service.

The TAC also recognizes the difficulty in planning for a network that will likely not have its next generational upgrade until 2011, or even later. The existing transport agreement with Qwest expires in October of 2007. If the expected life of the next generation network is five years, then the planning horizon faced today is almost seven years, or more. The other side of that process also presents a challenge – a decision on the next generation architecture is expected by the end of this year.

The time-line, the facilities landscape, and the changing needs of the Internet2 community are all factors used by the TAC in creating this document. The following should be taken as the set of requirements that the TAC considers critical to meeting the needs of the community it represents.

2. Current Status

The current Internet2 infrastructure consists of the Abilene backbone network, a variety of regional networks that connect to the backbone, and campus networks that usually connect to a regional network, but in a few cases connect directly to the backbone.

Requirements for the Internet2 Next Generation Network

by the Abilene TAC
March, 2005

The Abilene network is a backbone network whose common bearer service is IP. There are eleven router nodes on the backbone with OC-192c framed DWDM circuits forming the backbone, as pictured in the following diagram:

Resiliency is provided by IP at layer 3 rather than at the SONET layer. The circuits are provided by Qwest Communications and connection to the backbone is provided through a unique arrangement between Internet2 and Qwest. Connectors need only bring a circuit to the nearest Qwest PoP rather than directly to a router node. The connection from the Qwest PoP to the router node is provided by the agreement between Qwest and Internet2. Abilene currently has 42 direct connectors and includes over 220 university and research participants.

The Abilene network provides advanced services that are not often found on the commodity network. Examples include IPv6 and IPv4 multicast, with IPv6 multicast to be provided in the near future. The IPv6 network is implemented in a dual stack, native configuration. MPLS tunnels are provided in special cases on an experimental basis. Abilene also plays a role in network research, providing a large database of network attributes collected for the research community, and is part of several projects looking at future architectures.

Abilene provides a high speed facility for the research and education community to experiment with new applications, including those based on video and audio, high speed file transfer protocols, and other collaborative applications, including those that use IPv6 or multicast. It provides a unique facility for the research and education community to develop new and innovative applications.

Abilene also connects to a large number of international networks that serve the world wide research and education communities. The current network also provides transit for many of the international networks as part of the International Transit Network (ITN) program.

3. General Use IP Network

Abilene's success at implementing both commodity transport and advanced services is largely due its seamless integration of robust networking technologies, as well as the professional management of its networking resources. Internet2's commitment to best-of-breed networking equipment has established its reputation for exceptional performance and reliability while constantly pushing the envelope in various aspects of IP networking technology. From operations and engineering to strategic network planning, the Internet2 community brings together its collaborative strengths to ensure Abilene meets the requirements of its constituents. This same methodology will continue to be applied toward The Internet2 Next Generation Network.

Abilene's services include: a best-effort IP routed transport to support everyday data transport needs of the Internet2's membership; a network experimentation facility to support both layer 2 and 3 connectivity requirements for experimenters and network researchers; an observatory (based on an open architecture design principle) that facilitates plug-n-play style network experimentation; surplus capacity to support temporal high-bandwidth demonstrations and the experimentation needs of the community; and, advanced services that include IPv6, multicast, and the most advanced network measurement capabilities in R&E. The Internet2 Next Generation Network will include the same capabilities as its predecessors and include new capabilities that add value to the community. It will look to be an early adopter of advanced services that will increase the value add proposition that separates it from commodity Internet service providers.

Traffic engineering or the ability to selectively choose a specific route through the common shared infrastructure has already proven to be a useful tool in support of technology demonstrations over Abilene. The expectation is that demand for this type of service will grow in the future. The Internet2 Next Generation Network will provide the capability to perform traffic engineering to uniformly utilize network capacity or customize routing for a specific requirement.

With Abilene's surplus capacity and best-of-breed network resources, quality of service has never been an issue, at least not on a daily operational basis. However, there have been times when a high-bandwidth experiment/application has created the need to classify network traffic and provide priority handling to ensure proper handling. In such situations, Abilene engineers require tuning ability of the network in order to guarantee the success of an experiment or demonstration while not diminishing the overall service for other network

users. For this reason, the Internet2 Next Generation Network should be prepared to support different service levels in the network.

General use IP network requirements

1. There must be a next generation IP backbone network and it must be designed and managed by Internet2.

2. The Internet2 Next Generation Network must continue to support the same services that it does today.

3. The Internet2 Next Generation Network must continue to be an early adaptor of advanced services (those not currently available through the commodity Internet) and must deploy those services as early as possible.

4. The Internet2 Next Generation Network must deploy an out-of-band network management capability to enable access to network equipment when the network is under duress. The requirement includes physically independent access (separate from the backbone) to the out-of-band network.

5. The Internet2 Next Generation Network must strive to provide commercial-like availability for the backbone network. Redundant paths should be engineered to protect against link failure between any two nodes. Redundant path convergence times should be less than 200 milliseconds.

6. The Internet2 Next Generation Network should have the capability to provide traffic engineering in order to uniformly utilize network capacity.

7. The Internet2 Next Generation Network should have the capability of supporting overlay networks in order to facilitate different methods of connectivity between Internet2 constituents and/or inter-PoP observatories.

8. The Internet2 Next Generation Network should have the capability to support different service levels (e.g. prioritized queuing) of IP service.

9. The Internet2 Next Generation Network should investigate providing commodity routing to its members.

4. Measurement & Monitoring

Requirements for the Internet2 Next Generation Network

by the Abilene TAC
March, 2005

It is generally accepted that network measurement and monitoring (M&M) is a critical aspect of successful wide-scale networking. Of particular interest to the R&E community is the end-to-end performance in multi-domain national level networks, where expectations are high but little companion M&M data is available. Unfortunately, M&M requirements are often given secondary consideration during the design phase of large scale network. It is imperative that as the next generation Internet2 backbone is being designed that it be designed to accommodate the latest capabilities from the Internet2 M&M community.

Of particular importance to the design of the next generation backbone is work of the E2Eepi (The End-to-End Perofrmance Initiative) working group. That group recommends the creation of a Global Network Measurement Infrastructure (GNMI), the support of which will need to be considered a requirement of the next generation backbone. As stated by the E2Eepi group the ability to predict end-to-end performance is the desired goal and in order to achieve that goal it is necessary that active and passive elements of the entire path be visible from all the involved administrative domains. While the security and privacy issues will need to be overcome the desired M&M can only be accomplished when the end-to-end system can be visualized as a federation of administrative domains with corresponding congruent GNMIs. From one perspective this is similar to the criteria of the Global Grid Forum (GGF) on data bases in which the grid system can work with a federated set of stored information.

For each administrative domain, there a number of components that would make up the GNMI.

- Common schema: data records, information requests, information responses follow the same schema.

- Manageable data repositories: manageability of data repositories from the perspective that here is a finite amount of time, space and money to house repositories for fruitful data mining., and a finite amount of storage to be maintained.

- Qualified data repositories: data is validated as not being corrupted.

- Common tests: tests that have a well defined scope, that have been validated, and periodically revalidated, refined where needed and new tests developed to fill voids of missing parameters. For example SNMP data retrieved from a network device is used instead of a test traffic generator/analyzer used in the network to simulate the desired client traffic flows.

- Standard (normal) operating parameters: under normal operating conditions of the network, with the corresponding traffic flows, what is acceptable? What is the normal range of expected values?

- Common analysis & diagnostic tools: validated and understood with respect to scope of application

Beyond the network requirements for M&M work in other areas are noted for completeness. Missing in the GNMI is the correlation of the functional characteristics of applications to specific M&M network characteristics. It would be useful, in some venue, to specify a class of applications which are sensitive to specific network characteristics and develop guidelines for application developers that have applications that are network dependent. This could entail also looking at operating system (protocol stack) parameters that the developer may need to test for sensitivity to default settings. Out of the correlation studies will hopefully emerge a library of case studies that document common set of application routines with high predictive values for network and operating system characteristics.

Measurements and Monitoring Requirements

1. A GNMI must be established for the Internet2 Next Generation Network to include not less than a common schema, test, data repositories, analysis, and debug tools.

2. The INTERNET2 community should work on end-user diagnostic tools that make use of the GNMI to give timely insight about paths of particular interest.

3. A searchable repository of problems and solutions (case studies) as well as establish a forum/email list where people communicate about performance problems not captured in one of the online case studies should be established.

4. The INTERNET2 community should continue to participate in activities that will lead to the better understanding of classes of applications that share common network requirements, define network characteristics, and create software libraries for getting good performance for networked applications based on their classification.

5. The INTERNET2 Community should continue to participate in activities that lead to an understanding of issues that limit the effectiveness and efficiency multi-administrative networks.

6. The INTERNET2 community should participate in research activities that lead to the expansion of the scope of components in the GNMI.

7. The Abilene Observatory should be continued.

.

5. Performance and Availability

For the purposes of this document network performance is defined as both network availability and a consistent level of packet transport as measures such as latency and jitter as they relate to the IP bearer service. As the concept of an R&E controlled common backbone has matured the reliance on that network for critical campus functions has grown. It is no longer acceptable to consider the campus interconnect as in any way experimental with respect to reliability or performance. For example, it is not inconceivable for a classroom activity that in some way relies on Internet2 connectivity every Tuesday and Thursday from 1pm to 2:30pm to find that an occasional outage or performance degradation. Given the real time requirements of this activity, such a perturbation is unacceptable. The success of the Internet2 concept has lead to the need for it to continuously raise the level of its own reliability and performance.

There is no longer any reason to expect that the standards set by the carrier industry can not be met by private networks that provide service to the R&E community. Some argue that it is not just achievable but necessary in order to meet the expectations of that community. (This is a reoccurring question of a network offering and supporting differentiated traffic flows at a cost.) At least one campus has designed in the capability for individual segments on its campus to connect themselves in such a way that the outage of a single backbone component, even for a routine task like maintenance, can be survived without notice. The value to the whole is significantly increased if every level of the hierarchy adapts the same principles and offers a higher level of service to those for which it provides service.

Similarly, the expectation level for the performance of the IP bearer service has continuously increased and all layers of the Internet2 hierarchy should be prepared to meet that expectation. Further, all levels should be encouraged to create similar target service levels and to publish those targets for the rest of the community. It seems reasonable to expect all levels that provide service to the R&E community would want their particular segment to match the service levels provided by other levels. The only way to insure the entire community is achieving a desired level is if all publish their targets. Additionally, automated tools are available for measuring the various parameters used to define a service level within any particular segment. It should soon be possible to expand those, or newer, tools to measure multiple segments, getting closer to true end-to-end measurements. The real-time results from these measurements must be available to community in general.

The Abilene TAC recognizes the hierarchical structure of the end-to-end network and that the Internet2 Next Generation Network is only one segment in the total connectivity chain. It also recognizes that the Internet2 Next Generation Network provides leadership in raising the capability of, and expectation level for, the entire hierarchy. It is desirable that

all levels of the hierarchy raise their levels to match those of the backbone. In particular the regional level must adapt themselves to meet the evolving capabilities of the backbone in order for individual campuses to also keep pace.

Performance Requirements

1. Within its IP core (the router and the transport used to interconnect those routers) there must be efforts made to avoid single points of failure.

2. All core components must be housed in facilities that can sustain an operational status in spite of the absence of commercial power.

3. Mechanisms must be in place that will allow the loss of one of those hubs without impacting established connections.

4. Routine maintenance activities that result in the loss of a connection must also result in an undetectable switch to the alternate hub.

5. A service level for the production component of the Internet2 Next Generation Network must be published and approved by the appropriate community representatives. The service level must include targets for at least loss, latency, and jitter.

6. Internet2 Staff must take the appropriate steps to insure that published service levels are being met and take timely and appropriate action when conditions are projected that may impact the service levels.

7. Tools that provide a real-time confirmation that the service levels are being met must be available to community members.

8. When appropriate end-to-end tools are available staff must insure that the core components participate in those measurements.

6. Peering

The intrinsic value of today's Abilene is peering. Abilene carries the IP prefixes to regional, national, and international research and education networks. This includes US federal networks, and corporate research partners. Internet2 has done an exemplary job in fostering peering with non-US networks and providing transit service via its ITN service. Peering has also been used as a tool to encourage the use of multicast by allowing commercial carriers to peer with Abilene. This posture must be the carried forth in the next generation of the network and in fact expanded upon. Moving forward we cannot rely on the rest of the world to continue to come to us. Internet2 has been evaluating links to our

neighbors in North and South America, Europe, Asia, and to under served areas and this planning should continue.

The Next Generation of the network should be service focused providing peering to IP based networks, transport/transit services for direct peering with optical networks, and future connectivity to emerging research networks. Targeted peering should also be a requirement to content based providers or user communities of interest to the Internet2 community.

- **Commercial (Private) Peering**

  Many ARP's (Advanced Regional Networks) have well established private peering relationships with commercial carriers and participate with the Quilt peering initiative. The benefits of the private peering include improved network performance to our "at home communities", cost savings to both parties, and the promotion and use of advanced applications to these communities. Commercial carriers get access to the regional research and education infrastructure, the ability to promote the peering connection and other services including commercial Internet access, metropolitan ethernet or optical transport services, video, and VoIP services to the campus or enterprise.

  As the per Mb cost of bandwidth continues to fall peering is weighted less on the potential cost savings and more on the benefits of performance, content, and user base. As an example, peering with cable providers has the benefit of a short path back to campus extending campus applications to our communities at home. As broadband penetration increases, and FTTC, or FTTH initiatives increase it will become possible to push advanced applications to our at home communities.

- **Targeted Peering**

  Our communities can identify common targets of interest and peering should be explored with the target. The target maybe a research center, corporate partner, federal site, or international site. The key is application, research, content or user base of common interest that would benefit our communities if peering were established. Policies issues and the AUP for the next generation service will need to be community discussion.

- **Optical Peering / Transport Interconnection Services**

  Beyond current optical initiatives the next generation of the Internet2 network should plan on transit/transport services to allow an individual or institution to directly peer across the fabric with other optical networks nationally and internationally.

As in all phases of planning for the next generation of the network, closer ties and both strategic and tactical planning with the regional networks in the areas of optical design and optronics is required to ensure flexibility. Given the planning cycle this document must cover the opacity between backbone and regional network will become a requirement.

- **Peering as a Tool**

  Currently Abilene allows transit multicast peering with commercial providers as a means of promoting adoption of this technology. This should continue and peering should be used as a tool to encourage early adoption. Established guidelines should be maintained and reviewed as appropriate.

Peering Requirements

1. The Internet2 Next Generation Network must continue to be active participant in IPv4 and IPv6 unicast and multicast peering within the R&E community.

2. Targeted peering – The Internet2 community should actively identify peering targets of common interest to our communities.

3. The Internet2 Next Generation Network should investigate alternate AUPs that allow peering with targets of specific interest to the broader community.

4. Peering should continue to be used as a tool in the Internet2 Next Generation Network to encourage adoption of new technologies.

5. The Internet2 community should investigate Optical Peering/Transport to optical networks for direct peering.

7. Transport Services Offered by the Next Generation Network

It should be widely recognized that there has existed sometimes opposing views on the goals of the Internet2 backbone network since the concept of a community backbone was first discussed almost a decade ago. It should come as no surprise that disparate views on those goals still exist. One dimension in that discussion is a production oriented service versus a network that allows potentially disruptive experiments and demonstrations. Another is the desire to have the Intenet2 backbone deploy a variety of private networking

services versus the view that the focus for the backbone should remain on providing the best possible IP service.

The Abilene TAC represents both sides of both views. While much of this paper is focused on the service related to an IP bearer service much of the internal discussion has been about future transport services. It is expected that a variety of transport services will be possible. They may be based on existing technologies in a production oriented service, use a transport technology, or combinations of both. They may be connectionless or connection oriented. They may be provisioned in real time, hours, or days. They may be based on a specific application. Much is possible but it remains unknown what transport services will become important to the community during the lifetime of the next generation Internet2 network. It is, however, believed that some will reach community acceptance and that a concerted effort by the community to explore, test, and potentially deploy new transport services is well justified.

Requirements for the next generation transport services

1. The Internet2 Next Generation Network should be used to explore and test transport options that can support various private networking services.

Network Security

Internet2 Next Generation Network's security can be separated into two separate parts. The first is security in the classic sense, which includes authentication, authorization, accounting, packet filtering, etc. It is used to protect network resources from security threats that affect only the integrity of the network itself. Secondly, there is community security, which is a cooperative effort by all campus, RON, and backbone administrative domains to security threats as an integrated effort to thwart evolving threats. This section addresses both Intra-Network and Inter-Network(Community) security requirements for the Internet2 Next Generation Network Network.

9. Intra-Network Security

The Internet2 Next Generation Network hopes to significantly increase the services it provides Internet2 members. A dedicated research facility, a network data archive, new network measurement infrastructure, advanced services (IPv6 and multicast), as well as advanced restoration services expand an already service rich offering. The accompanying security responsibility has increased significantly as Internet2 Next Generation Network grows beyond just a core router infrastructure. These new services provide vulnerabilities

and potential security threats that need to be addressed in order to ensure Internet2 members receive the same level of service that they have come to expect from Abilene.

Abilene's open architecture design along with its disciplined methodology for achieving its security goals has produced an outstanding record against security threats, while also enabling unparalleled support for both network researchers and production services for its members. Internet2 Next Generation Network's security plan is structured on a methodology defined by an iterative process involving the following steps:

- Insure the security and privacy of packet data transiting the routing infrastructure are in compliance with Internet2 policy.
- To protect information and network resources, harden and secure the network infrastructure against identifiable security threat.
- Establish an Internet2 Next Generation Network system baseline and prepare for unknown security threats by recognizing when system vulnerabilities have been exploited.
- Actively monitor Internet2 Next Generation Network to detect unusual or suspicious behavior using analysis tools, as well as external stimuli coming, e.g. user report and/or security bulletin.
- In case of intrusion, respond by analyzing the scope and damage inflicted, work to contain the damage, and attempt to eliminate intrusion reoccurrences, restore system to its original state, and notify the necessary parties.
- Using experience and new techniques or methods, improve existing security practices by incorporating useful feedback into the security process (harden and secure, prepare, detect, and respond).
- Participating in network security research, in particular research that addresses the unique needs of the Internet2 community.

This methodology must be asserted as a part of Internet2 Next Generation Network. The scope to which this applies will include the network infrastructure, out-of-band management, the observatory, and the various support systems.

Intra-Network Requirements

1. The Internet2 Next Generation Network must implement and publish a security policy and security plan.

2. The security policy must identify what network and/or infrastructure assets need to be protected (or made secure), e.g. confidential data and network resources. It must also identify what is trying to protect against. This would include malicious attacks against the network itself and unauthorized access to any network resources. The policy should also layout the mechanism through which exception, if any, are applied for and approved.

3. The security policy must be feasible and technically capable of being implemented.

4. The security policy must provide scope to define administrative and physical boundaries. It must identify the organization and matching responsibilities. It must qualify what network resources are protected and to what extent. It must include notification procedures.

5. The security plan must document and describe how the security policy is implemented.

6. The security plan must conform to Internet2 Next Generation Network's open systems design principle, which enables network elements to plug-and-play into the network through well defined interfaces and using standards based protocols.

10. Inter-Network(Community) Security

The security threats to institutional computational resources continue to increase at an alarming rate. Indeed, many attacks are now automated with each succeeding generation becoming more sophisticated. As the occurrence of security related incidences increase, it is imperative that network planners play an active role in the development of a comprehensive security architecture with the goal of reducing, and potentially eliminating, the severity of the attacks.

Abilene can no longer view itself as a seamless interconnect of regional, and through those, campus networks. Through active participation in research activities, experimentation with intrusion detection, and potentially a coordinated, automated response system, Internet2 Next Generation Network must become a member of a national hierarchical detection and prevention system that supports its community. The nature of attacks on campus networks and host is becoming automated and stealthy. As the nature of the attacks evolve so must the detection systems. Where it was once acceptable for a detection system to monitor a campus network at a single point and rely on human monitoring, it is now necessary to build a layered and coordinated defensive system that can scan real time events at various campus network locations. Expanding that model to include the R&E community's regional networks and the national backbone may become the only method that can effectively respond to the increasingly sophisticated attacks. It is expected that a defensive strategy based on human response times will soon no longer be sufficient for thwarting attacks and that some form of automated tools that are capable of real time network reconfigurations will be required. It seems prudent to plan now for what appears to be a logical extension of the future campus environment to include regional networks and the national INTERNET2 backbone.

Requirements for the Internet2 Next Generation Network

by the Abilene TAC
March, 2005

Internet2s next-generation network will need to continue to participate in existing security related monitoring and experimentation. For example, Abilene generates a real-time NetFlow traffic feed to the Research and Education Networking Information and Sharing Analysis Center (REN-ISAC) that is used by the REN-ISAC for security threat analysis. The traffic data are treated confidentially. Using the data, the REN-ISAC generates both public and confidential reports for analysis.

Inter-Network, Community Security Requirements

1. The Internet2 Next Generation Network must be designed in such a way that it is capable of participating in a hierarchical intrusion detection and prevention system.

2. Internet2 staff must be active participants in the testing and early deployment of automated, hierarchical intrusion detection and prevention systems.

3. When appropriate, an automated intrusion detection and prevention system should be deployed on the Internet2 Next Generation Network.

4. If appropriate, a manual intrusion detection and prevention system should be deployed on the Internet2 Next Generation Network.