Network Architecture

NIH Enterprise Architecture

Version 2.0

8 February 2005

Table of Contents

List of Figures

List of Tables

1. Introduction

The network is a key component of IT infrastructure that covers all of the software, hardware and transport capabilities needed to provide connectivity across the NIH. As organizations rise to the challenge of delivering consistently high-quality support and high-availability connectivity for mission-critical applications, the complexity of the network infrastructure also increases.

This report establishes network architectural standards and guidelines across the NIH and specifies agreed-upon common components that can be implemented enterprisewide. The identification of network standards and guidelines will help minimize network complexity and reduce overall costs by ensuring that common network deployments (including design and structured cabling), network management services, remote access solutions and vendor equipment are implemented consistently across the NIH enterprise. The patterns and bricks documented in Sections 2 and 3 of this report provide the target state (i.e., "to-be" architecture) for networks. The bricks also include current-state (i.e., "as-is" architecture) information about the current NIH environment.

1.1 Network Domain Team

This report comprises the compilation of findings and recommendations derived from the joint NIH-Gartner Network Domain Team and the Enterprise Architecture project team. The Network Domain Team was comprised of 10 subject matter experts from various Institutes and Centers (ICs), including the Center for Information Technology (CIT), and was facilitated by Gartner. The domain team worked together for six weeks to update the first version of the architecture patterns and bricks. This report replaces version 1 of the NIH Network Architecture. The domain team recommendations were also reviewed with additional IC subject matter experts including John Dvorak (CIT), Mark Silverman (CIT) and Shawn Googins (OD), as well as Gartner subject matter experts. The Domain Team incorporated their suggestions, as appropriate, into this document. The IC representatives who contributed to this effort were:

- Adriane Burton, CIT
- Gene Cartier, CIT
- Robert Cox, NIAID
- Joe Klosky, NICHD
- Dennis McCloud, CIT
- Ron Milor, CIT
- John Morgan, NIA
- Christopher Stenger, OD
- Charlie Tate, NIEHS
- Anthony Trang, CIT
- Paul von Stein, NCI

1.2 Scope

For purposes of this document, the scope of the NIH network includes NIH locations (i.e., in the Metro D.C. area, the United States and the world), business partner sites,

universities, hospitals, and the Department of Health and Human Services (HHS) operating divisions (OpDivs). The network domain team analyzed all of the major technical elements required to provide data and Internet communications between these institutions and locations.

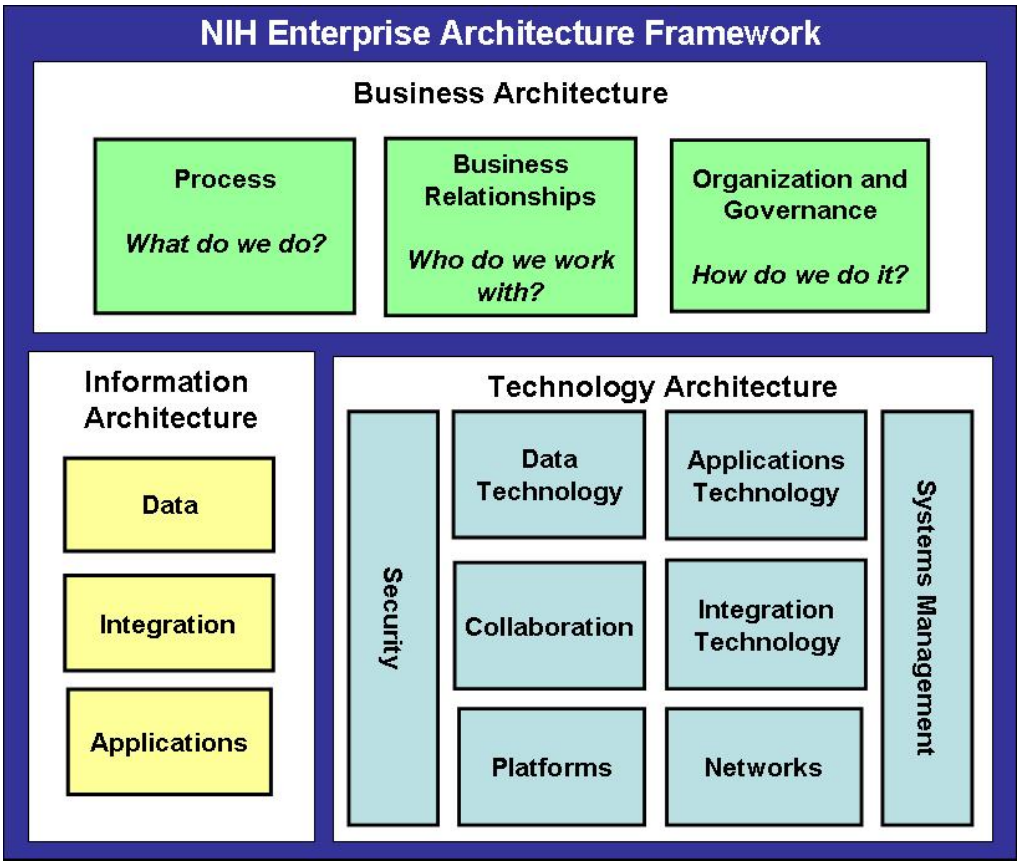
The technical scope of this document includes technical specification for commonly used network services, but does not cover some services that are considered to be either too new or not applicable to NIH's environment (e.g., Voice over IP (VoIP), video, call center technologies or IP storage technologies). The requirements to support these new services were addressed during the Network Architecture definition, and it was determined that those services and technologies may be defined in future iterations of the Network Architecture.

1.3 Network Domain in the NIH Enterprise Architecture Framework

The *NIH Enterprise Architecture Framework* and *NIH Enterprise Architecture Matrix* are based on the Federal Enterprise Architecture Framework (FEAF) and the FEAF Matrix.[1] The NIH EA Framework recognizes three distinct architecture components: the Business Architecture, Information Architecture and Technical Architecture. The NIH EA Framework is illustrated in Figure 1.

[1] Level IV of the FEAF, derived from the Zachman Framework

Figure 1. NIH Enterprise Architecture Framework



The Network Domain is part of the Technology Architecture within the NIH EA Framework.

The NIH Enterprise Architecture (EA) Matrix provides five *perspectives* or views of the architecture, at increasing levels of detail. The NIH EA Matrix is shown in Table 1.

Table 1. NIH Enterprise Architecture Matrix

	Data Architecture	Application Architecture	Technology Architecture
Planner Perspective	List of Enterprise Business Objects	List of Business Processes, plus multi-enterprise processes.	List of Business Locations and Business Partners
Owner Perspective	Semantic Model	Business Process Models (including multi-enterprise)	Business Logistics System, plus multi-enterprise logistics
Designer Perspective	Logical design patterns; Use enterprise business objects	Logical design patterns, by style	Integration technology for enterprise systems
Builder Perspective	Physical design patterns; Use shared database if applicable	Logical design patterns, by style	Physical design patterns; Use bricks from TRM or request a waiver. TRM includes security, NIH network and other infrastructure.
Subcontractor Perspective	Project scope	Use common services or APIs, if defined	

This architecture report addresses the Planner, Owner, Designer and Builder perspectives (reference Table 2).

Table 2. Network Alignment With the NIH Enterprise Architecture Matrix

	Data	Applications	Technology
Planner Perspective			■ **Network Scope (Section 1.2) —** Community-of-interest data for networked systems based on business drivers and requirements analysis.
Owner Perspective			■ **Principles (Section 1.4) —** Rules for the delivery of network services to the internal and external (Public/Private) NIH community.
Designer Perspective			■ **Patterns (Section 2.0) —** Framework for the topological design of networked systems.
Builder Perspective			■ **Bricks (Section 3.0) —** Specification of as-is baseline and strategic and tactical implementation recommendations for various technologies, standards, products and vendors.

1.4 Principles

The Network Domain Team reviewed the principles from the first version of the Network Architecture, verified that they were still valid and useful, and referenced the principles to ensure the architecture decisions reflected in this document are consistent with the principles. The principles listed below are high-level statements of the fundamental

values that guide the NIH Network Architecture. These network architecture principles apply across the entire NIH technical environment and embody the purpose and intent of networking at NIH. Each principle is universally accepted and stable so as to withstand changes in network technologies, processes and products. The principles maintain a clear relevancy with policy changes in NIH programs and management approaches, as well as reflect the general policy directions and framework of the Federal Government.

A rationale is provided for each of the principles in order to explain their importance and any business implications. While the statement of each principle should remain constant, the rationales and implications may evolve over time, as they respond to factors such as the current information management environment within NIH, internal initiatives, external forces, and changes in the NIH mission, vision and strategic plan.

Principle	Rationale
Principle #1 – Application Response Times The single NIH network will provide application response times acceptable to support the business need and cost effective bandwidth to satisfy the current and future networking needs of NIH users and external partners.	The network will not be overbuilt and will be efficient. The network should be designed to provide appropriate application response times at a reasonable cost. The network should also be able to accommodate future networking needs.
Principle #2 – Network Connectivity The network will provide high-quality, reliable, scalable and measurable network connectivity to all sites. All mission critical sites will be engineered with fault tolerance.	The quality of the network should be measurable, and all critical sites should have back-up.
Principle #3 – Service Level Agreements (SLA) The network will meet the network service level objectives agreed upon by IT management and NIH users and external partners. The network management systems will have the capability to measure and report end-to-end network service level statistics.	Service Level Agreements (SLAs) will be documented and network statistics and SLAs will be published to the end user community, as needed, to ensure network resources are aligned with business needs.
Principle #4 – Open System Standards Open system standards should be used for communication both within the enterprise and with suppliers and clients. Standard network interfaces and protocols will be defined, maintained and implemented.	Open systems will be used where feasible and cost effective, rather than proprietary solutions.
Principle #5 – Remote Access The remote access network will consist of a defined set of technical options for the delivery of reliable, cost-effective, secure and ubiquitous remote access capabilities.	Remote access will be designed and provisioned for use enterprise-wide.

1.5 Related Topics

1.5.1 NIH Centralized Network Services

In the continuing effort to improve service quality across the NIH enterprise, reduce cost, and comply with management and government mandates – including Administrative Restructuring Advisory Committee (ARAC) directives for consolidation – the NIH CIT group provides certain network services centrally. By providing network services centrally, NIH and its end-users benefit from improved efficiencies and standardized infrastructure deployment — which provides users with a common "look and feel", as well as reduced overall network management requirements.

The following services are provided centrally by CIT:

- Remote access VPN
- Remote access dial-up
- New building LAN and telephone cabling
- Wireless LAN
- Centralized network monitoring

The network service architecture for these services has been included in this document for completeness. If any of these services are required, please either call CIT directly or reference http://cit.nih.gov/nw-tc.html to find a contact for the service you require.

1.6 Summary of Key Decisions

1.6.1 Requirements for the Network Architecture

Through reviewing leading trends in the marketplace and HHS and NIH infrastructure directions, the Network Domain Team determined that the NIH Network Architecture should address the following requirements:

- Ongoing convergence of voice, data and video communications, as well as the introduction of storage area networks (SAN) into the IP enterprise network
- Emergence of VoIP and multimedia applications that will require greater quality of service (QoS) capabilities in the future
- The proliferation of new wireless standards and technologies, such as Blackberries, and the need to extend WiFi technology to larger geographies
- NIH's need to provide better visibility into network availability in support of problem determination, availability management and end-user support
- HHS's desire to consolidate network infrastructure, to reduce costs and to improve quality of service throughout the department
- The gradual expansion of CIT's role in managing the consolidated network infrastructure across the NIH ICs

Accordingly, the Network Refresh Domain Team endeavored to reduce the number of vendors and technologies to those that will provide the best long-term flexibility, functionality, maintenance and cost management.

1.6.2 Key Decisions

- In support of network consolidation and in order to improve ease of management and operational support of network infrastructure across NIH, new Local-Area Networks (LANs) will be implemented more consistently in terms of vendor, required features, design and configuration.
- New Wireless LANs will also be implemented more consistently in order to provide seamless support for stationary and roaming NIH users, as well as NIH's guests.
- NIH will support the 802.16 standard for broadband wireless networks in the near-term future.
- New router and switch configurations will incorporate a standard subset of required and optional features that will enable NIH to support future state-of-the-art network service capabilities.

- NIH remote users will have cost-effective, secure, high-speed access to NIH through Internet Service Provider (ISP) services and a centralized Virtual Private Network (VPN) remote access service infrastructure.
- NIH remote users can also use 1-800 and local number dial-up access, although this is likely to be slower and more expensive than using Internet ISP VPN services.
- Two options are available for network load balancing:
  - A Network-centric option that also provides network address translation
  - An Application-Centric option
- NIH will continue to deploy Cat6 and Fiber cabling for LANs.
- NIH will deploy 802.11g Wireless LANs (WLANs) in the Tactical and Strategic time frames.
- NIH will continue to displace legacy protocols with Transmission Control Protocol/Internet Protocol (TCP/IP) for most data transfer and multicasting for low-overhead broadcasting.
- NIH will continue to displace older videoconferencing protocols with H.32x in the tactical time frame and Session Initiation Protocol (SIP) in the strategic time frame.
- Network Management will be implemented in a more consistent manner across ICs to improve interoperability with a centrally managed network monitoring capability.
- NIH will procure products from a smaller set of vendors to improve manageability and consistency within the network infrastructure:
  - For routers and switches, Cisco Systems, Enterasys Networks and Extreme Networks are both Tactical and Strategic; Foundry Networks is Tactical
  - As part of the Wireless Consolidation, the wireless vendors will also be reduced to Cisco Systems and Enterasys Networks (both are deployed tactically)
  - Cisco Systems and F5 Networks will continue to be the Tactical and Strategic choices for network load balancing servers
  - Cisco Systems dial-up and Virtual Private Network (VPN) is Tactical and Strategic for Remote Access
  - Cisco Systems, Nortel Networks and Ciena will continue to be the Tactical and Strategic vendors for Campus/Metropolitan/Wide-Area Network (CAN/MAN/WAN) Optical Networking
  - The Strategic Network Management Tools for Availability Management are:
    - CA Unicenter or HP OpenView NNM

- CiscoWorks LAN Management Solution
- Fluke (Suite)

1.7 Benefits of the Network Architecture

In addition to the general benefits of Enterprise Architecture, stated elsewhere, the Network Architecture provides the following specific benefits:

- By selecting a target set of network standards and technologies, interoperability can be more easily ensured across the NIH
- Managing and monitoring network availability will be simplified and streamlined when the network infrastructure converges to the target state described in this document, resulting in cost savings and improved availability
- Patch management will be simplified, reducing the overall support costs for the network, because fewer patch releases need to be deployed
- Common elements reduce the overall network management burden, training and acquisition costs and pave the way to establishing and measuring network service-level objectives
- Network implementations can be deployed faster and with fewer maintenance issues because there is a common deployment plan

2.0 Network Design Patterns

Design patterns may be *logical* or *physical.* Logical design patterns do not specify specific technology platforms, products or brand names. A logical design pattern may be implemented by one or more related physical design patterns. Patterns provide design guidance to implementation teams and can occur in one domain or span multiple domains. Patterns provide a reference model (i.e., a "blueprint") for the technology elements that can be combined to solve a specific problem.[2]

2.1 Patterns 1 & 2 : LAN Minimum Configuration and High Availability Logical Patterns

2.1.1 LAN Description

A Local-Area Network (LAN) is a contained communications network that connects users within this contained area. By definition, a LAN is used within a building or a group of buildings. LANs can be either physically (separate switches) or logically (separate virtual local-area networks (VLANS) on the same switch[es]) separated into workgroup, access, distribution and core layers. Edge connections to non-NIH entities such as ISPs, HHS and other agencies are included in the distribution layer.

LANs are generally used to perform the following functions for networked users within a building:

- Access wider-area networks, such as Campus-Area Network (CAN), Metropolitan-Area Network (MAN) and Wide-Area Network (WAN), including the Internet, via a direct connection from the network, for external file transfer, e-mail, and other systems not connected to the LAN
- Send e-mail to other users on the network
- Send output to printers attached to the network
- Transfer data or software to or from other systems attached to the network

NIH's LAN design patterns recognize two types of LAN configuration, the *LAN Minimum Configuration* and the *High Availability Configuration*. Because both patterns are logical, discrete boxes are not required at each layer. In practice, multiple layers of functionality can be provided from within the same physical device (e.g., access/distribution router).

NIH uses the following layers for architecting and implementing LANs:

- Workgroup Layer: The workgroup layer is used to segment and connect servers and/or devices in a network.

[2] Technology represented by "bricks" or specific technologies inside a brick.

- Access Layer: The access layer connects the workgroup layer to the network.
- Distribution Layer: The distribution layer acts as an area and address aggregation point. Complex, CPU-intensive policy-based operations are usually performed at this layer. It lies between the access and core layer.
- Core Layer: The core layer is a highly reliable layer of the network, sometimes also referred to as the backbone. Its main function is to route traffic as quickly as possible and provide aggregation and summarization services.

Workstations are connected to the workgroup switch. Servers are connected to the server switch. The workgroup and server switches comprise the workgroup layer, which interfaces to the access layer, which provides access to the distribution and core layers. The distribution layer also contains edge routers, which are the demarcation point for NIHnet. The Security Architecture provides guidance on where and when to implement boundaries and protective services, which may occur between layers or within a layer.

The LAN Minimum Configuration and the LAN High-Availability Configuration patterns reflect two alternatives for LAN deployment. The determination of which alternative to adopt depends on the percentage of uptime required by the users and applications the LAN must support, and on funding considerations[3]. In practice, the availability requirements for each layer should be evaluated and then either the LAN Minimum or LAN High-Availability Configuration options should be implemented at each layer accordingly. For example, one group of users may need high availability at the workgroup and access layers, but not at the distribution layer; another group may need higher availability at the distribution layer, but not at the workgroup layer.

For sites in the NIH campus, routers and switches will be implemented as illustrated in the two LAN Patterns. For remote sites, the access switch and distribution routers may be combined into a single device that connects to a dedicated circuit, providing connectivity to the distribution layer in the NIH campus to access core backbone services. The following implementation considerations are not shown in these patterns but will also need to be addressed:

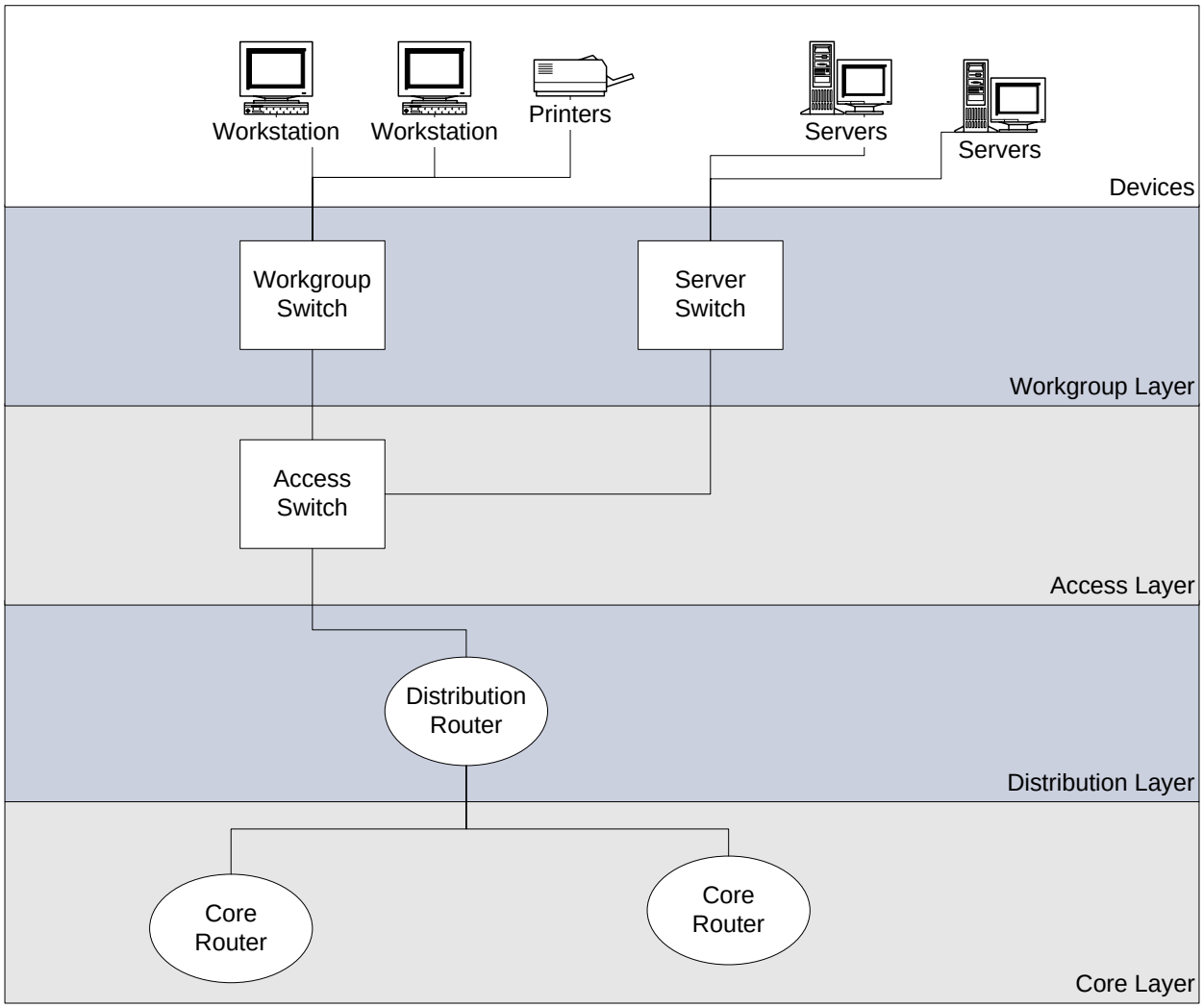
- Adequate space, power, heating, ventilation and air conditioning need to be in place before a LAN is implemented.
- Building occupancy conditions, such as whether the space is leased or owned, may influence LAN design. For example, a short-term leased building may consider using a wireless LAN deployment rather than a wired LAN implementation due to the cost of wiring and the inability to reuse the wiring once the lease is over.

[3] The cost of equipment increases as uptime requirements increase. For example, in the High Availability configuration all critical network components must be on Uninterruptible Power Supply (UPS) and, depending upon availability requirements, varying levels of power supply redundancy for UPSs may be required.

2.1.2 LAN Minimum Configuration Description and Solution

LAN Minimum Configuration Solution is for basic connectivity with expected minimum uptime of 99.5 percent. This configuration should be implemented for basic cost-effective LAN connectivity where uptime is not mission-critical and the number of users is relatively small.

Figure 2. Logical Design Pattern for LAN Minimum Configuration



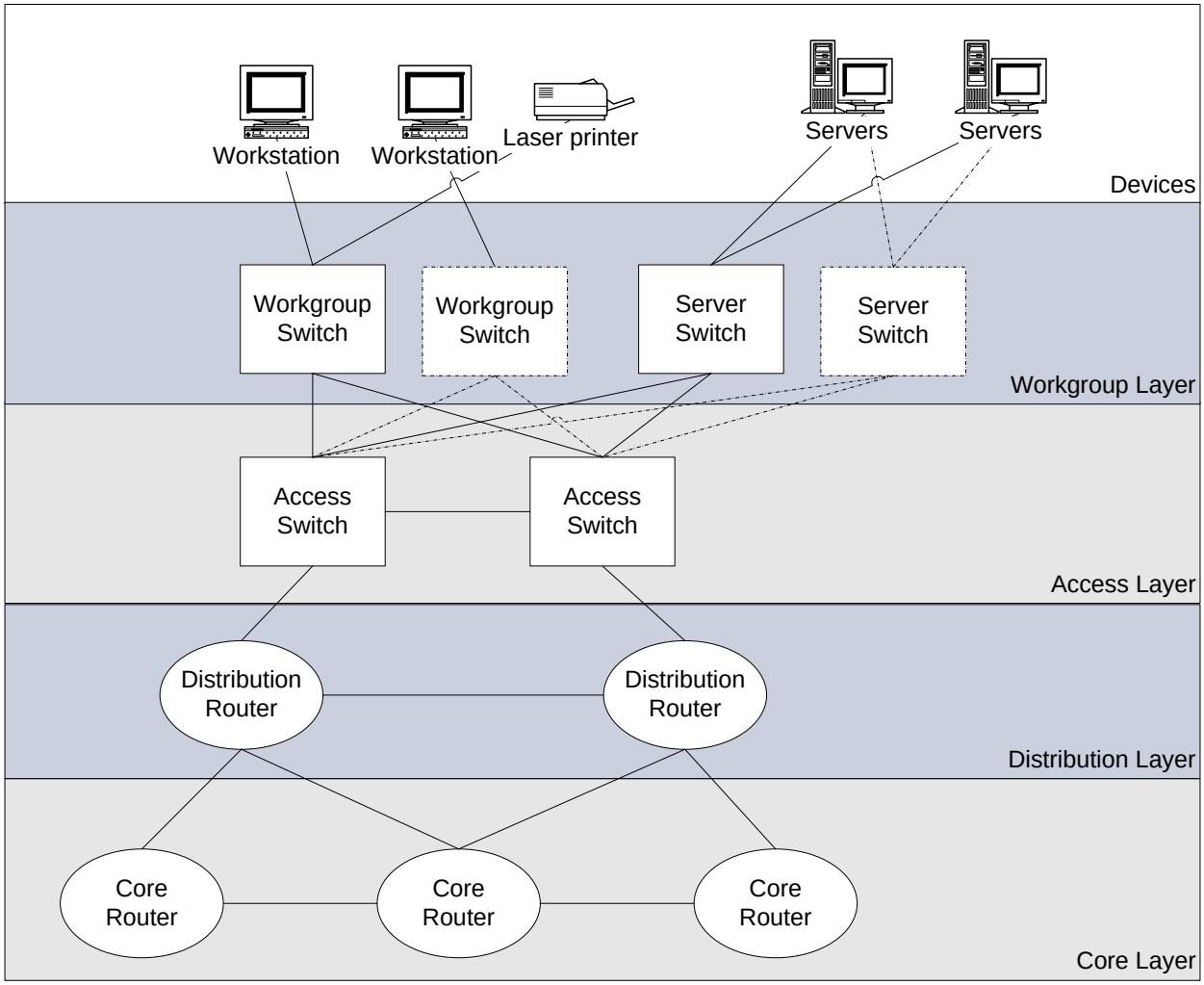
2.1.3 LAN High Availability Configuration Description and Solution

LAN High Availability Configuration Solution is for expected uptime of 99.999 percent or higher. At the device level, neighboring user devices are connected to alternate workgroup switches so that a switch outage will still allow some users to work unaffected or other users to use unaffected nearby machines. Redundant server

switches allow for redundant connections to the servers so that if one switch goes down, the server is still accessible without any remedial action required. This pattern also includes the addition of redundant access and distribution switches and redundant paths between them. The workgroup and server switches are dual-homed to the access switch. The distribution routers are dual-homed to core routers. Because the distribution and core routers are dual-homed, the failure of an access switch will not impact availability. The LAN High-Availability Configuration Solution can also include load balancing functionality, which is described in Section 2.5, Pattern 6: Network Load Balancing Pattern.

The high-availability configuration option should be used in mission-critical subnets, locations and data centers where uptime is critical to the mission of the NIH. For example, the Clinical Center provides healthcare to patients in research trials, and the impact of network connectivity downtime could be life-threatening for patient care; therefore, the High-Availability LAN configuration is an appropriate option to support this environment. Grants management is another mission-critical area for NIH. Since grant awards are often time-sensitive, especially around the end of the fiscal year, some subnets that support grants evaluation and notification processing may warrant the High-Availability LAN configuration solution. Calculated availability service levels (such as ≥99.5% or 99.999%) are predicted based on statistical probability and historical outage experiences of selected products and other factors, and are not guaranteed. It is important to work with the user community within the context of overall continuity of operations to understand when standalone operations will suffice as a backup method in the event that the cost of high-availability options may not be justifiable.

Figure 3. Logical Design Pattern for High-Availability LAN Configuration



2.1.4 Benefits

Benefits that are common to both patterns are as follows:

- Both the Minimum- and High Availability LAN patterns provide a consistent and manageable approach for provisioning LAN services across the NIH. These patterns can enable a breadth of configurations that are neither under- nor over-configured.
  - They allow the alignment of technical requirements to business needs by implementing LAN service levels based on availability requirements. For example, if only 99.5 percent uptime is required for a specific location, a design pattern can be developed for that requirement. Because they both have interchangeable layers, design patterns can be easily customizable for varying uptime requirements.

- They provide an efficient use of expensive network resources, such as printers, scanners, and other network devices.
- They provide the ability to aggregate large numbers of users onto expensive WAN transport services.

A benefit specific to the High Availability configuration is:

- The LAN High-Availability Configuration provides a greater opportunity to avoid outages that might impair the NIH mission or cause damage to its reputation through unplanned outages.

A benefit specific to the Minimum configuration is:

- The Minimum LAN configuration reduces costs relative to the High Availability configuration by eliminating equipment redundancy.

2.1.5 Limitations

A limitation of the High Availability configuration is:

- Implementing the LAN High-Availability configuration pattern is more expensive than the Minimum configuration pattern.

A limitation of the Minimum configuration is:

- The LAN Minimum configuration pattern does not provide the fault-tolerance and availability shown in the LAN High Availability Pattern.

2.2 Pattern 3: Wireless LAN Pattern

2.2.1 Description

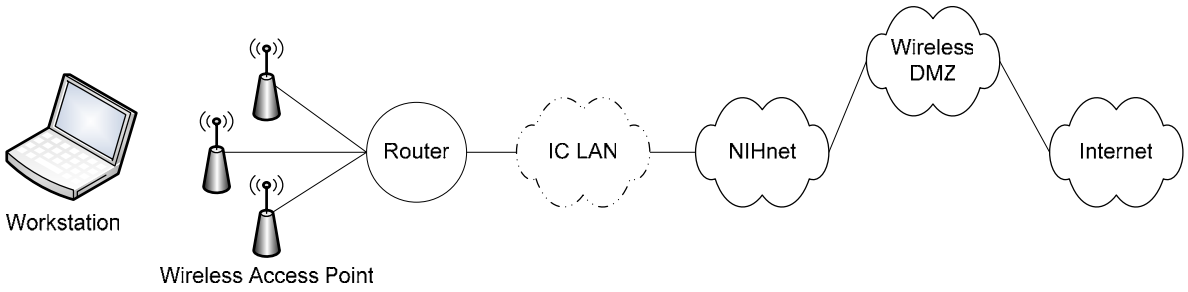
Wireless LAN (WLAN) is a LAN communication technology in which radio, microwave or infrared links replace the physical media (i.e., wires and cables). The IEEE 802.11x series of standards address WLAN standards. Four of the 802.11x standards address the physical layer, and, currently only two of them prevail in today's market: 802.11b (WiFi) and 802.11g, offering up to 11Mbps and 54Mbps, respectively.

- WLANs are primarily used in conference rooms and other common areas to provide access to network resources without the need to be at a specific desk
- WLANs are also used in temporary locations to connect users to the network
- As wireless devices become more prevalent, this pattern will become ubiquitous; however, will not displace wired LAN patterns
- Vendor-specific extensions should be avoided to ease interoperability and management, as well as to prevent additional security problems

2.2.2 Wireless LAN Solution

Figure 4 shows how a wireless workstation or device connects to a wireless Access Point (AP). The wireless APs are connected to a switch or router, which may connect to an IC LAN or directly to NIHnet. NIHnet is also connected to the Internet through a wireless DMZ.

Figure 4. Physical Design Pattern for Wireless LAN Solution

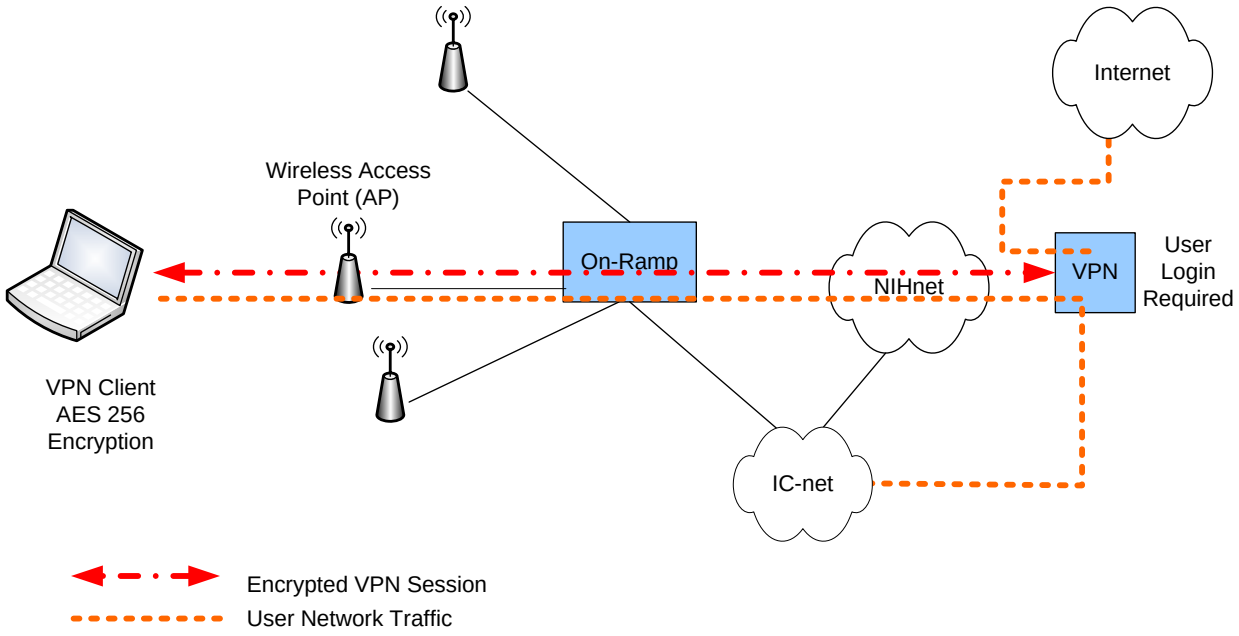


Compare this pattern to the Logical Design Pattern for NIH Wireless User with VPN (section 2.2.3) and the Logical Design Pattern for Wireless Guest User (section 2.2.4) to see how this physical configuration is used logically by two types of users. Note that the access points will not broadcast the SSID, so that the user will have to request that information from NIH in order to gain access to the wireless infrastructure. The VPN service is a centralized service provided and managed by CIT.

2.2.3 NIH Wireless User with VPN Solution

The Logical Design Pattern for NIH Wireless User with VPN (Figure 5) shows the logical view of how an NIH Wireless user uses VPN to connect to NIH networks and resources. The user establishes a VPN session using the On Ramp access method, which will require a user login. NIH users will then be granted access to NIH resources and networks through an encrypted VPN session, which will provide data privacy for all information being transmitted wirelessly through Advanced Encryption Standard 256 (AES 256).

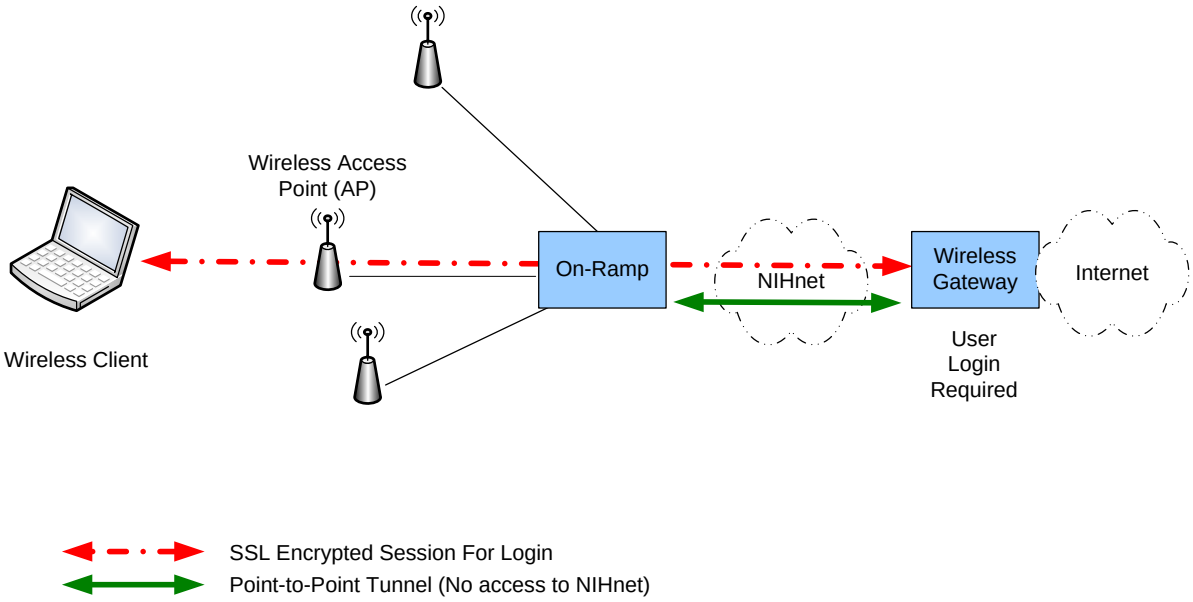
Figure 5. Logical Design Pattern for NIH Wireless User with VPN



2.2.4 Wireless Guest User Solution

The Logical Design Pattern for Wireless Guest User (Figure 6) shows how a wireless guest user can access the Internet or NIH resources through the wireless gateway. Because guest users will not have access to the VPN software, they will use a Secure Sockets Layer (SSL) encrypted session to be tunneled directly through to the wireless gateway. This gateway will require the same login that is available from the Internet in order to access any internal NIH resources. In this way, the external users can connect to the Internet and can use their extranet login to connect to any NIH resources which would otherwise be accessible from the Internet.

Figure 6. Logical Design Pattern for Wireless Guest User



2.2.5 Benefits of Wireless LAN Solutions

These benefits apply to all three Wireless LAN patterns.

- This approach supports multiple vendor client cards and access points
- The WLAN solution is scalable, can be centrally managed, meets security requirements, and adheres to NIH wireless policy
- Users must to load and initiate VPN client software in order to establish connectivity securely
- As shown in the logical design patterns, this approach addresses different classes of users

2.2.6 Limitations of Wireless LAN Solutions

These limitations apply to all three Wireless LAN patterns.

- These patterns require using a proprietary VPN to address security
- These patterns only address WiFi access through NIC cards; they do not address integrated wireless devices such as Blackberries or RFID readers
- Rapidly evolving technology and standards will require NIH to revisit and update these patterns frequently so that NIH can obtain the newest security, capacity and functionality capabilities

2.3 Pattern 4: CAN/MAN/WAN Pattern

2.3.1 Description

CAN, MAN, and WAN, which represent one pattern as depicted in Figure 7, are extensions of the networking capabilities performed by the LAN over a wider geographic distance. A CAN is used to network buildings within a campus, essentially providing a backbone capability that is accessible directly (not through a carrier) from each building. A MAN evolved from LAN designs, but is optimized for longer distances (i.e., up to 30 miles), greater speeds (i.e., more than 100 megabits per second) and diverse forms of information (e.g., voice, data, image and video). MANs generally cover an entire metropolitan area, such as a large city and its suburbs. A WAN covers a much larger area such as a city, state or country, and generally performs the same functions as a MAN, but tends to rely more on carriers to provide connectivity between sites.

A CAN is used at the main NIH campus to connect campus users in the various buildings onto NIH's network, NIHnet. A MAN is used to connect the main NIH campus to other NIH locations within the metropolitan area and the WAN is used to connect locations outside the metropolitan area. In-house fiber is used for the CAN and commercial carrier services are used for the MAN and WAN.

The majority of CAN/MAN and WAN services are centralized at NIH, with CIT taking the lead role in managing the core backbone network infrastructure. All ICs share the core backbone network. The core backbone network supplies connectivity between the ICs, as well as supplying access to the Internet.

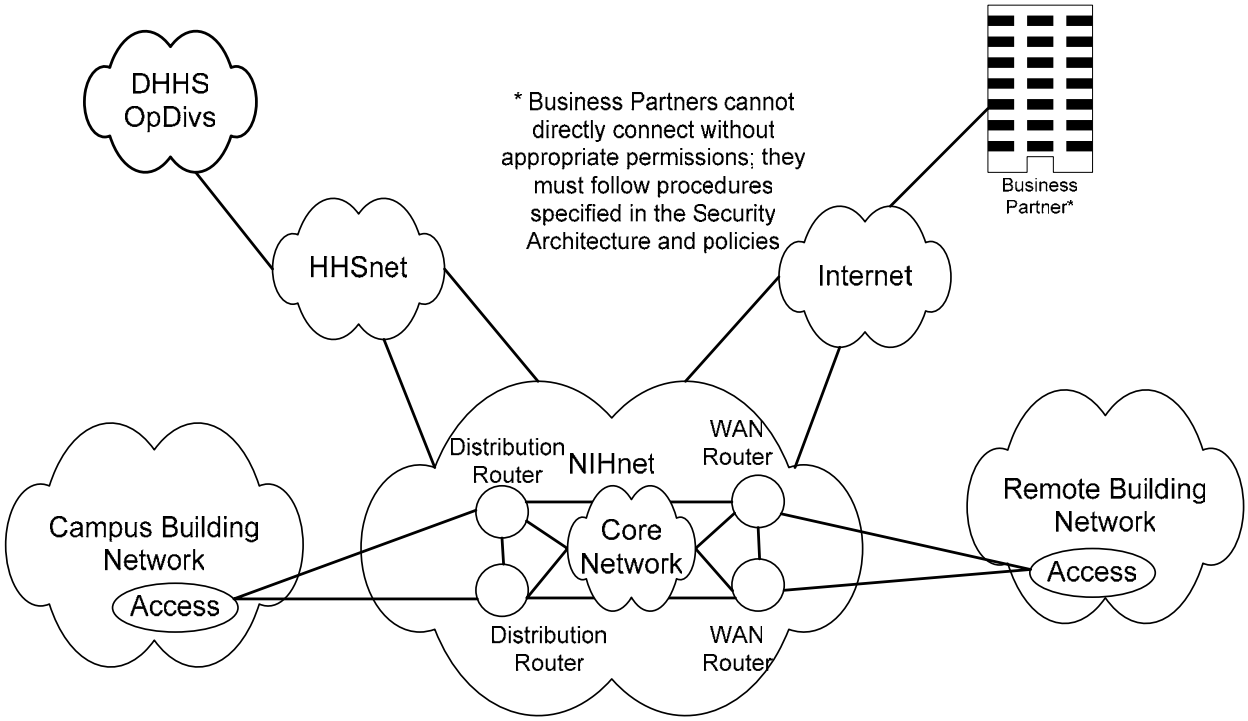
The backbone is being migrated from ATM to Gigabit Ethernet. Design is hierarchically based with an access layer, a distribution layer and a core layer. The core layer provides access to servers, farm networks and data centers. The distribution layer provides traffic flow control, high-level access and control and filtering. The access layer provides granular access and control and filtering.

2.3.2 CAN/MAN/WAN Solution

Figure 7, the Logical Design Pattern for CAN/MAN/WAN, shows how the network layers in the LAN patterns actually connect different sites within and to NIHnet. The core network at the center of this picture is the backbone of NIHnet. The WAN and distribution routers shown here correspond to the distribution routers shown in the distribution layer represented in Figures 2 and 3 (sections 2.1.2 and 2.1.3 respectively). The access routers in the remote building network and the campus building network were shown in the access layer of the LAN patterns. Internet connectivity is accomplished through the distribution or core layers. Please see the Security Architecture for guidance about implementing boundaries and protective services between or within layers. Other HHS Operating Divisions can connect to NIH resources through dedicated circuits to HHSnet which are connected to the distribution or core layers. Note that business partners will use the extranet capabilities of NIH to access

NIH resources through the Internet; direct connection to NIHnet can occur only after complying with security procedures, policies and architecture standards.

Figure 7. Logical Design Pattern for CAN/MAN/WAN



2.3.3 Benefits

- Cost savings are achieved through simplified design, more-efficient use of bandwidth, and enabling central management.
- Network devices can be scaled as the network grows, facilitating easier network expansion implementations. As each element in the network design requires change, the cost and complexity of making the upgrade is contained to a small subset of the overall design.
- Improved fault isolation is facilitated by structuring the network into smaller, easier to understand elements. Network managers can easily understand transition points in the network, which helps identify failure points more efficiently.
- By connecting a master access switch to the hubs, physical infrastructure can be reduced, eliminating duplication and effectively addressing redundancy.
- Redundancy can also be addressed at the distribution level to support multiple buildings with physically separated paths and routing diversity.

2.3.4 Limitations

- Due to cost constraints, WAN speeds cannot reach the same speeds as LAN, CAN and MAN. That is because, as distance increases, the cost for bandwidth increases.
- There are more potential points of failure on WAN due to the greater distances that separate NIH locations.
- NIH is reliant on carriers' ability to meet service-level agreements (SLAs).

2.4 Pattern 5: Remote Access Pattern

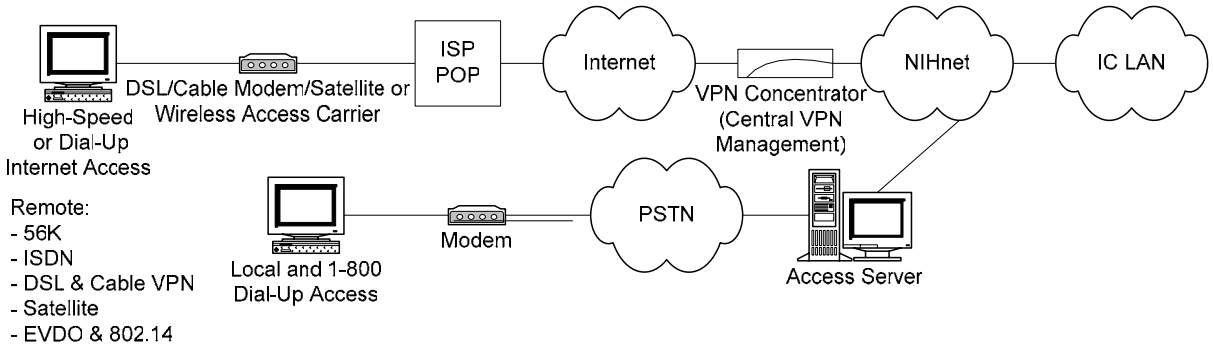
2.4.1 Description

Remote access provides the ability to securely log on to the network from a distant location through resources that are not managed by NIH. NIH personnel use remote access services when traveling or when working from home. CIT and IC network staff also use remote access to troubleshoot problems in the off hours. NIH business partners use remote access services to access certain data on NIH servers.

2.4.2 Remote Access Solution

Dial-up remote access requires a computer, a modem and remote access software to allow the computer to dial into the network over a telephone line, or Public Switched Telephone Network (PSTN), and connect to the network. Remote access via a Virtual Private Network (VPN) creates encrypted tunnels over an existing Internet connection between remote users and the network, thus securing the communications. Internet access in the diagram below is obtained via an ISP account.

Figure 8. Logical Design Pattern for Remote Access



2.4.3 Benefits

- This pattern can support centrally managed remote access services for NIH, which would result in cost savings due to reduced support and maintenance costs, including help desk

- Cost savings may be realized by reducing the number of remote access solutions that are deployed and managed at NIH.
- VPN is more cost-effective than 800 dial-up service
- VPN is more secure than dial-up services
- This design is scalable and robust
- Remote access users will achieve higher throughput speed by utilizing broadband capability in the VPN solution

2.4.4 Limitations

- NIH will need to address the fact that it is difficult to obtain quality SLAs from ISPs for VPN remote access services
- Users have to coordinate the acquisition and implementation of their own Internet connection
- Users have to load and configure their own software

2.5 Pattern 6: Network Load Balancing Pattern

2.5.1 Description

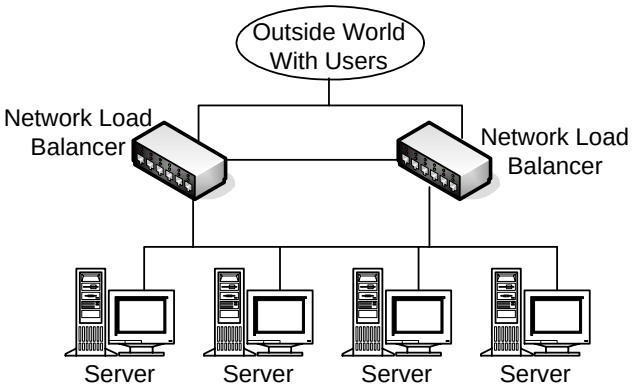
Load Balancing technology is used to balance workload across servers to improve availability, performance, and scalability. Network Load Balancers are implemented at the workgroup/server switch layer. Load balancing increases performance consistency and application availability and are therefore recommended for NIH enterprise applications.

2.5.2 Network Load Balancing Solution

This pattern illustrates two configurations for accomplishing load balancing — In-line and End-node. In both configurations, a one-to-one or one-to-many mapping can be used to access a specific server or a group of servers respectively. Additionally, both configurations offer multiple algorithms for mapping user requests to servers (e.g., round-robin, random, or depending on server utilization) and provide proxy services.

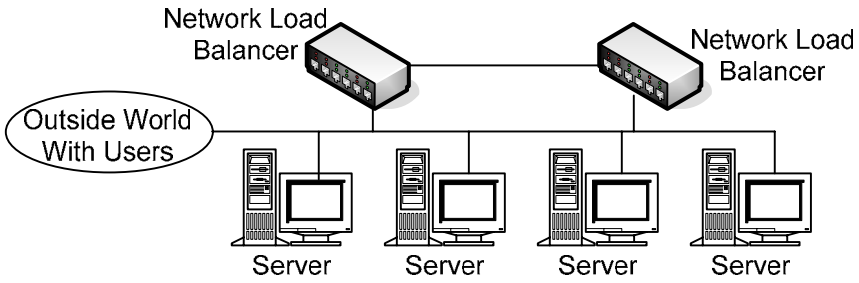
The In-line configuration, Figure 9, provides Network Address Translation (NAT), essentially acting as a filtering firewall. This configuration provides added security.

Figure 9. Logical Network Load Balancing Pattern – In-line Configuration



The End-node Configuration, Figure 10, does not provide NAT. Therefore the load-balanced servers can access other resources in the network directly without having to utilize the load balancers' proxy services; this facilitates access to backup and other services.

Figure 10. Logical Network Load Balancing Pattern – End-node Configuration



When deployed singly, a load balancer can improve performance by efficiently allocating workload across multiple servers. In order to deliver improved availability, the load balancers must be deployed in pairs, with hot standby configured. Otherwise, the load balancer can become a single point of failure for the servers. Note that this Network Architecture recommends deploying paired network load balancers in the two configuration options shown in Figure 9.

2.5.3 Benefits

The primary benefit of network load balancing, applicable to both configurations, is:

- These two options allow better performance and availability than when network are configured without load balancing capabilities.

The primary benefit of the In-line configuration is:

- The In-line option enhances security by providing NAT capabilities

The primary benefit of the End-node configuration is:

- The End-node option allows servers to directly connect with other network resources (e.g., backup services)

2.5.4 Limitations

- There are additional hardware, software and support costs required to implement load balancing, regardless of the configuration.

2.6 Pattern 7: Availability Management — Network Pattern

2.6.1 Description

Availability Management is an Enterprise Systems Management (ESM) discipline. Network Availability Management includes the administrative services performed in monitoring NIHnet and the IC networks, including network devices, network topology and software configuration, monitoring network performance, maintaining network operations, and diagnosing and troubleshooting problems.

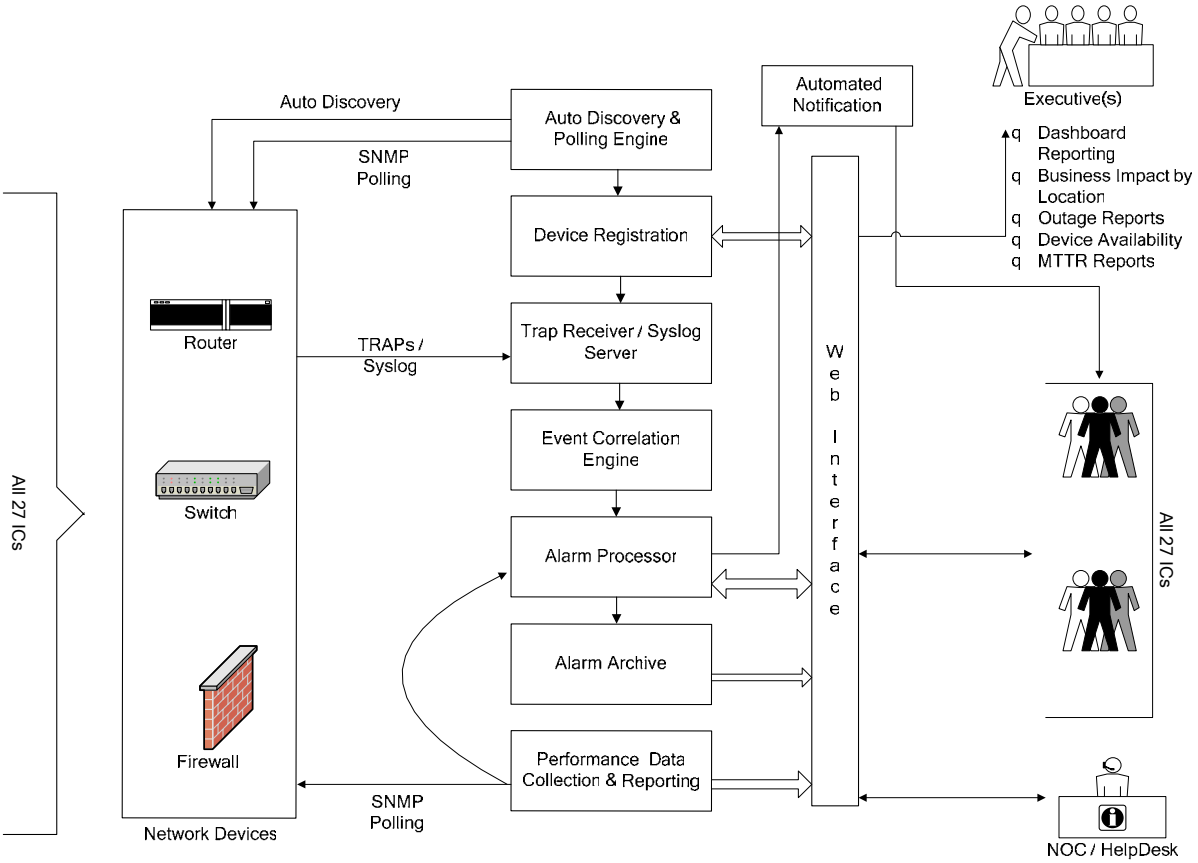
2.6.2 Availability Management — Network Solution

CIT and most ICs implement network management systems to manage their own community-of-interest networks. These systems generally reside within the data centers of the IC.

NIH will use Simple Network Management Protocol (SNMP) polling to provide device status Management Information Bases (MIBs) to the network management software for analysis. If a network availability situation warrants note or attention, then the network management software will automatically generate a notification or alert to the IC, Help Desk and operations personnel, as appropriate.

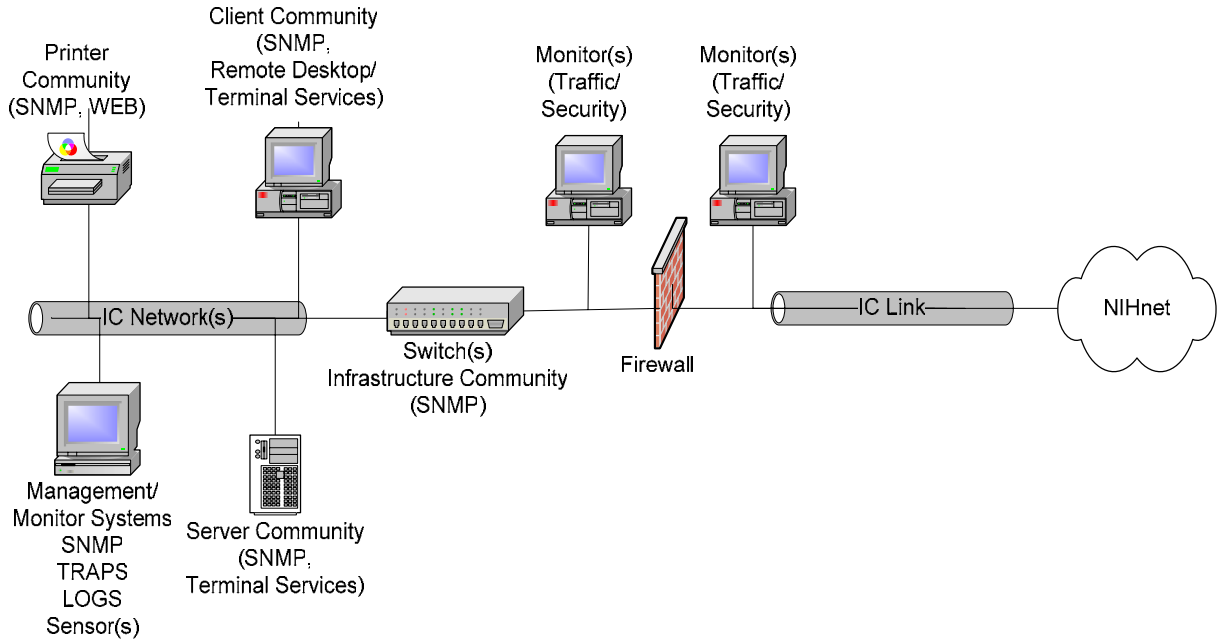
Figure 11 illustrates the centralized CIT network management solution for monitoring all 27 IC subnets and enterprise connections and resources.

Figure 11. Logical Design Pattern for Network Availability Management



The IC High-Level Logical Design Pattern for Network Availability Management (Figure 12) illustrates how monitoring systems will monitor clients, servers, printers and network devices within an IC network; address space; and forward the appropriate messages and alerts to the central monitoring system. This approach allows information about network availability to be passed from within a private IP address space to the Central Network Management System to address existing private IP address spaces. No new private IP address spaces will be deployed, as CIT administers and centrally manages IP addresses within NIH. The Central Network Management System will have direct access through firewalls to monitor and manage the respective network devices. Please refer to the Security Architecture for instructions on how to enable secure SNMP traversal over the firewall. All local management systems must be configured to send out management and monitor messages to the local management console and the central management system simultaneously.

Figure 12. IC High-Level Logical Design Pattern for Network Availability Management



2.6.3 Benefits

- Together, these patterns support the NIH Network Operations Center (NOC) Capability and allow for performance monitoring and availability management across NIHnet
- By establishing procedures and criteria for forwarding system performance information and alerts to a central network management capability, critical outages may be prevented through proactive Fault Prediction and Problem Management
- This solution allows ICs to have their own Logical Network Views while providing backup management capabilities with 24/7 network monitoring through the NIH NOC
- This approach allows for predictive traffic analysis to enhance capacity planning

2.6.4 Limitations

- Development of such a system may be complex
- As the implementation of ESM progresses, this pattern will be expanded so that selected alarms and notifications are also passed to a Manager of Managers (MoM) that can incorporate network status into problem management and user-support activities.

3.0 Network Bricks

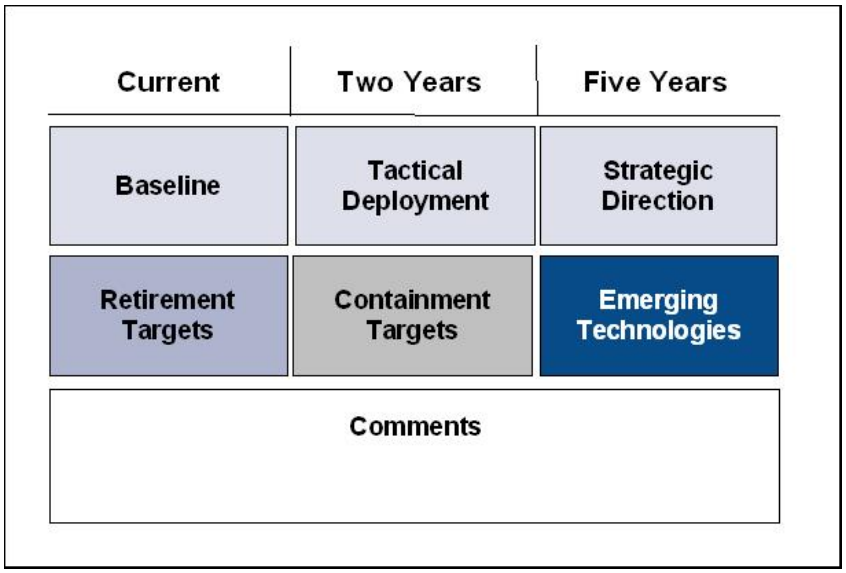
In the Technical Reference Model (TRM), baseline and planned technology choices for elements meet in a chart called a "brick". Bricks represent the physical building blocks of the enterprise IT systems — they identify specific technologies used to implement solutions. Bricks document both NIH's current (i.e., "as-is") environment and future (i.e., "to-be" or target) states. The planning horizon is five years.

Each brick captures:

- A description of the technology and its role
- Specific implications, dependencies, and deployment and management strategies
- Technology elements, categorized

A brick template is shown below:

Figure 13. Technology Planning "Brick"



The technology choices for architectural elements are categorized as follows:

- **Baseline** technologies include current technology and/or process element(s) in use.
- **Tactical** technologies are recommended for use in the near-term or tactical time frames (next two years). Currently available products needed to meet existing needs are identified here.

- **Strategic** technologies provide strategic advantage and might be used in the future. Usually, marketplace leaders are identified here, as they are likely to provide better benefits and meet the anticipated needs of the business.
- **Retirement** technology and/or process elements targeted for de-investment during the architecture planning horizon (five years).
- **Containment** includes technology and/or process elements targeted for limited (maintenance or current commitment) investment.
- **Emerging** technology and/or process elements are to be evaluated for future use based on technology availability and business need. These technologies may not be new to the marketplace, but are simply not yet in use at NIH. In this case, the products may be a fit for emerging needs at NIH.

The Network Architecture is currently comprised of the following bricks:

- Workgroup/Server Switch
- Access Router/Switch
- Distribution Router/Switch
- Core Router
- CAN/MAN/WAN Optical Networking
- CAN/MAN/WAN Transport
- LAN Cabling
- Communications Protocol
- Wireless LAN
- Network Load Balancing Server
- Remote Access Technology
- Availability Management — Network

3.1 Comments on Routers and Bricks

Routers and switches are the primary components of network architecture. A router connects two networks together. The connection can either be to another private NIH network or the public network, such as the Internet. Routers receive packets of information from computers or other routers on the network; they then send these packets to their destinations based on “addresses” at the beginning of the packets and a road map of the other computers and peripherals on the network.

Switches divide the network into several segments, each of which can operate without interference from traffic local to any of the other segments. Switching exists as a method of increasing bandwidth and reducing delay on the LAN/CAN/MAN.

Currently, NIH deploys routers and switches from more than 11 different vendors, which reduces the ability to aggregate spending volumes and increases the complexity and cost of maintaining all these products in the enterprise network. By reducing the number of vendors deployed to the four leading vendors, NIH will see improved service and a reduction in the total cost of ownership (TCO) to maintain these core network devices.

The following features should be used to distinguish a vendor's switch or router:

- Plug-and-play and auto-negotiation
- Hot-swappable modules (specific to modular switches)
- Link aggregation
- Flow control support
- Security (see Security Architecture for additional guidance)

3.1.1 Descriptions of Layers

Routers and switches have different operating characteristics and functional requirements, depending on the layer in which they are deployed. The NIH network architecture considers the following four layers:

- Workgroup layer consists of the routers and switches that connect devices (peripherals, workstations and servers) together into a local-area network
- Access layer connects the workgroup layer to the distribution layer
- Distribution layer provides aggregation from the access layer to the backbone and provides connectivity to dedicated CAN/MAN/WAN circuits
- Core Layer consists of routers and transport media that form the backbone of the network

3.1.2 Switch and Router Characteristics

The following tables summarize the required characteristics for each type of router and switch, depending on the layer it serves, organized by Open Systems Interconnection (OSI) layer. An 'x' in any column indicates that the specified functionality is required for that type of router or switch. If "optional" appears in the table, then that feature may not be required — please consult the feature descriptions and specific recommendations to determine which circumstances do not require a given feature.

Prior to configuring a switch or router, the following types of requirements should be gathered and analyzed:

- Capacity requirements — number of devices, connections and bandwidth.
- Availability requirements — will the switch or router be supporting mission-critical or life-support applications? What is the impact of downtime? If the router or

switch has high-availability requirements, then power redundancy and HSRP are required.

- Functional requirements — what types of usage are anticipated over the next three years.
  - If video or voice applications could be used by any users supported by this equipment, then Quality of Service (QoS), multicast and prioritization features are required to support the bandwidth service levels required by those applications
  - If AppleTalk or IPX devices will need to be supported, then tunneling is a required feature

Table 3, OSI Layer 1 – Media Types Supported, shows which media types must be supported by switches and routers at each network layer: copper, multimode fiber (MMF) or single mode fiber (SMF); 10 megabit, 100 megabit, 1 gigabit or 10 gigabit; half or full duplex.

Table 3. OSI Layer 1 – Media Types Supported

	Copper			MMF			SMF	
	10/Half	100/Full	1G/Full	100/Full	1G/Full	10G/Full	1G/Full	10G/Full
Workgroup	X	X		X	X			
Access		X	X	X	X		X	
Distribution			X	X	X		X	X
Core					X		X	X

Table 4 identifies which OSI Layer 2 features switches and routers must be able to support.

Table 4. OSI Layer 2 – Required Features

Layer 2 Features						
	Multicast	802.1q	802.1d	802.1s & 802.1w	Ether Channel	802.1p
Workgroup	X	X	X	X		X
Access	X	X	X	X	X	X
Distribution		X	X	X	X	X
Core					X	

The following are important characteristics of the Layer 2 feature requirements:

- Multicast features include Internet Group Management Protocol (IGMP) Snooping and Cisco Systems Group Management Protocol (CGMP). All three versions of IGMP are open protocols that allow a system to identify itself to a router or switch in order to receive specific multicast traffic. With IGMP snooping hardware, a router or switch can examine IGMP packets and build a forwarding

table. CGMP is proprietary to Cisco Systems equipment and runs between multicast routers and switches. Both aim to restrain multicast traffic to certain nodes so that the network is not flooded.

- 802.1q is an IEEE standard that defines the operation of Virtual LAN (VLAN) bridges.
- 802.1d is an IEEE standard for LAN spanning trees.
- 802.1s is a supplement to 802.1q that adds the facility for VLAN bridges to use multiple spanning trees.
- 802.1w is a supplement to 802.1d that allows for rapid reconfiguration of spanning trees.
- EtherChannel is a Cisco Systems technology that provides incremental trunk speeds between Fast Ethernet, Gigabit Ethernet, and 10 Gigabit Ethernet. The equivalent industry standard is IEEE 802.3ad.
- 802.1p is an IEEE specification for priority queues within LANs that provides traffic-class expediting and dynamic multicast filtering.

Table 5, OSI Layer 3 – Required Features, identify the important feature requirements of OSI layer 3.

Table 5. OSI Layer 3 – Required Features

	Multicast	HSRP	Port Channel	OSPF	EIGRP	BGP
Workgroup						
Access		X	X	X	X	
Distribution	X	X	X	X	X	X
Core	X		X	X	X	X

	Native AppleTalk	Native IPX	SNMP	Device Security	Tunnels	QoS
Workgroup			X	X		
Access			X	X	X	X
Distribution	X	X	X	X	X	X
Core	X	X	X	X		X

The following are important characteristics of the Layer 3 feature requirements:

- Multicast support can be provided by IGMP Snooping, CGMP or Protocol Independent Multicast (PIM), which uses existing unicast routing tables for packet forwarding, thereby introducing less overhead. PIM can be implemented in sparse or dense mode (SM or DM).

- Hot Standby Router Protocol (HSRP) is a Cisco Systems availability feature that allows a router to take over from a failed router, when properly configured. The equivalent industry standard is VRRP (Virtual Router Redundancy Protocol).
- Port channel is a channel on the router that allows the router to function between OSI layers 2 and 3.
- Open Shortest Path First (OSPF) protocol is an interior gateway protocol (IGP) that transfers packets from one network to an adjacent one.
- Enhanced Interior Gateway Routing Protocol (EIGRP) is a proprietary IGP from Cisco Systems.
- Border Gateway Protocol (BGP) is the interdomain routing protocol implemented in TCP/IP.
- Native AppleTalk and Native IPX (Internetwork Packet Exchange) refer to supporting those protocols natively on the switch, vs. tunneling.
- Simple Network Management Protocol (SNMP) is a TCP/IP protocol governing network management and the monitoring of network devices. SNMP v3 support is required at both Level 3 and Level 4.
- Device security refers to protecting the maintenance port of the router or switch.
- Tunnels refers to a technique that encapsulates data for transmission so that it doesn't need to be changed to accommodate differing network types or protocols.
- Quality of Service (QoS) refers to the supporting prioritization of different packet types to ensure that critical transmissions receive adequate bandwidth priority for time-sensitive applications, such as VoIP or videoconferencing.

In the following table . . .

Table 6. OSI Layer 4 and Other Features

	Layer 4 Features		Other Features		
	SIP	H.32x	Power Redundancy	SNMP v3	RMON
Workgroup	x	x	Optional	Optional	
Access	x	x	Optional	Optional	
Distribution	x	x	optional	Optional	x
Core	x	x	x	Optional	x

The following are important characteristics of the Layer 4 feature requirements:

- Session Initiation Protocol (SIP) is an Internet Engineering Task Force (IETF) application-layer signaling protocol for Multimedia Communication.
  - H.32x is a series of computing standards from the International Telecommunication Union (ITU) that address videoconferencing

- Power redundancy can be achieved through dual power supply, UPS and other means. The availability requirements and cost will be the primary drivers for determining what is appropriate.
- SNMP v3 can be added to a device with a microcode or firmware upgrade.
- RMON refers to supporting the IETF standard for Remote Monitoring that enables network managers to monitor sub-network devices via the MIB (Management Information Base).

There are also many security features, such as Intrusion Detection Services (IDS) and Intrusion Prevention Services (IPS), which may need to be included on switches and routers. Refer to the Security Architecture for requirements and recommendations on security features for routers and switches.

3.2 Brick 1: Workgroup/Server Switch

The workgroup and server switches provide connectivity to and between workstations and servers, respectively, within a network segment.

Table 7. Workgroup/Server Switch Brick

Baseline Environment	Tactical Deployment	Strategic
■ 3Com ■ Asante ■ Cisco Systems ■ Cabletron Systems (now Enterasys Networks) ■ HP Compaq ■ JDS Uniphase ■ Marconi ■ Networth (now HP Compaq)	■ Cisco Systems	■ Cisco Systems
Retirement	**Containment**	**Emerging**
■ 3Com ■ Asante ■ Cabletron Systems ■ JDS Uniphase ■ Marconi ■ Networth (now HP Compaq)	■ HP Compaq	None
Comments		
■ Refer to section 3.1.2 Switch and Router Characteristics, for specific features that should be configured on workgroup/server switches. ■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products. ■ Some baseline products have been designated Retirement and Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.		

3.3 Brick 2: Access Router/Switch

Access routers and switches connect subnets to the distribution layer. In some cases, the access router/switch functionality is combined with the distribution and workgroup layer switches so that a single box performs the functions of access, distribution and/or workgroup layers.

Table 8. Access Router/Switch Brick

Baseline Environment	Tactical Deployment	Strategic
■ 3Com ■ Asante ■ Cabletron Systems (now Enterasys Networks) ■ Cisco Systems ■ Extreme Networks ■ Foundry Networks ■ HP Compaq ■ JDS Uniphase ■ Marconi ■ Networth (now HP Compaq)	■ Cisco Systems ■ Enterasys Networks ■ Extreme Networks ■ Foundry Networks	■ Cisco Systems ■ Enterasys Networks ■ Extreme Networks
Retirement	**Containment**	**Emerging**
■ 3Com ■ Asante ■ Cabletron Systems ■ JDS Uniphase ■ Marconi ■ Networth (now HP Compaq)	■ HP Compaq	■ Juniper Networks
Comments		
■ Refer to section 3.1.2 Switch and Router Characteristics, for specific features that should be configured on access routers and switches. ■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products. ■ Some baseline products have been designated Retirement and Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.		

3.4 Brick 3: Distribution Router/Switch

Distribution routers and switches connect the access layer to the backbone network. The distribution layer directs and filters traffic between access layer and the core layer.

Table 9. Distribution Router/Switch Brick

Baseline Environment (Today)	Tactical Deployment (Zero to two years)	Strategic (Two to five years)
■ 3Com ■ Asante ■ Cisco Systems ■ Cabletron Systems (now Enterasys Networks) ■ Extreme Networks ■ Foundry Networks ■ HP Compaq ■ Marconi ■ Networth (now HP Compaq)	■ Cisco Systems ■ Foundry Networks ■ Enterasys Networks ■ Extreme Networks	■ Cisco Systems ■ Enterasys Networks ■ Extreme Networks
Retirement	**Containment**	**Emerging**
■ 3Com ■ Asante ■ Cabletron Systems ■ Marconi ■ Networth (now HP Compaq)	■ HP Compaq	■ Juniper Networks
Comments		
■ Refer to section 3.1.2Switch and Router Characteristics, for specific features that should be configured on distribution routers and switches. ■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products. ■ Some baseline products have been designated Retirement and Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.		

3.5 Brick 4: Core Router

Core routers are part of the backbone, which also contains all the high-speed transport media. This layer does not provide any packet manipulation.

Table 10. Core Router Brick

Baseline Environment (Today)	Tactical Deployment (Zero to two years)	Strategic (Two to five years)
■ 3Com ■ Asante ■ Cabletron Systems (now Enterasys Systems) ■ Cisco Systems ■ Extreme Networks ■ Foundry Networks ■ HP Compaq ■ Marconi ■ Networth (now HP Compaq)	■ Cisco Systems ■ Foundry Networks ■ Enterasys Networks ■ Extreme Networks	■ Cisco Systems ■ Enterasys Networks ■ Extreme Networks
Retirement	**Containment**	**Emerging**
■ 3Com ■ Asante ■ Cabletron Systems ■ Marconi ■ Networth (now HP Compaq)	■ HP Compaq	■ Juniper Networks
Comments		
■ Refer to section 3.1.2 Switch and Router Characteristics, for specific features that should be configured on core routers and switches. ■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products. ■ Some baseline products have been designated Retirement and Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.		

3.6 Brick 5: CAN/MAN/WAN Optical Networking

This brick addresses optical networking when implemented as part of the network backbone. Storage-Area Networks (SANs) can also use this technology, but those standards will be architected in the server environment area of the Enterprise Architecture. These technologies are also used to attach to the backbone.

Table 11. CAN/MAN/WAN Optical Networking Brick

Baseline Environment (Today)	Tactical Deployment (Zero to two years)	Strategic (Two to five years)
Technology: ■ CWDM ■ Dark Fiber ■ Point to Point Fiber **Vendors:** ■ Cisco Systems ■ Ciena ■ Nortel Networks	**Technology:** ■ CWDM ■ Dark Fiber ■ Point to Point Fiber **Vendors:** ■ Cisco Systems ■ Ciena ■ Nortel Networks	**Technology:** ■ CWDM ■ Dark Fiber ■ Point to Point Fiber **Vendors:** ■ Cisco Systems ■ Ciena ■ Nortel Networks
Retirement	**Containment**	**Emerging**
None	None	■ DWDM
Comments		
■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products. ■ Some baseline products have been designated Retirement and Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.		

3.7 Brick 6: CAN/MAN/WAN Transport

NIH has migrated from an asynchronous transfer mode (ATM) backbone to a Gigabit Ethernet fiber backbone in the CAN environment using GBIC (Gigabit Interface Converter) technology to convert the serial electric signal to serial optical signals, and vice versa.

On a limited basis, Packet over SONET (Synchronous Optical Network)-based transport technology is used in the MAN/WAN environment as provided by service providers. Packet-over-SONET/SDH (POS) enables core routers to send native IP packets directly over SONET/SDH frames.

NIH is considering the future use of multi-protocol label switching (MPLS) as a transport mechanism. MPLS is a generic networking technique that combines many of the desirable features of technologies such as ATM and frame relay with the features of IP.

MPLS can deliver alternative QoS services for potential voice-over-IP deployment in the future.

Table 12. CAN/MAN/WAN Transport Brick

Baseline Environment (Today)	Tactical Deployment (Zero to two years)	Strategic (Two to five years)
■ ATM ■ Frame Relay ■ Private Line ■ SONET ■ TLS	■ MPLS for WAN ■ PoS for CAN/MAN ■ Private Line for WAN/MAN ■ SONET for WAN ■ TLS for WAN/MAN	■ MPLS for WAN ■ PoS for CAN/MAN
Retirement	**Containment**	**Emerging**
■ ATM	■ Frame Relay	■ MPLS
Comments		
■ ICs should seek advice from CIT on bandwidth and connectivity options to HHSnet. ■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products. ■ Some baseline products have been designated Retirement and Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.		

3.8 Brick 7: Wireless LAN

The role of a wireless LAN is to extend network coverage to allow for in-building or campus communication for mobile users. Wireless LAN (WLAN) equipment can also be used to create *ad hoc* networks for temporary situations such as conference registrations.

WLANs use electromagnetic waves to transmit data without physical connection to the access points (APs). APs act as a bridge between the LAN and wireless clients (also referred to as end users or wireless adapters). APs can support a small group of users in a given range; the theoretical number of clients supported by an 802.11b-based AP is 256 within a 100-foot range (the theoretical number of clients for 802.11a-based AP is 1,024). Depending on usage patterns, no greater 20–30 users are generally recommended for optimal performance. For example, e-mails with attachments require more bandwidth than e-mails with no attachments, and VoIP or video applications will require substantially more bandwidth.

The range of access points is related to speed. As the distance between AP and wireless client increases, the speeds decrease, and vice versa. Building materials, floor plans and environmental factors also affect the range. For example, Gartner estimates indoor and outdoor ranges to be 100 ft. (30 m.) and 200 ft. (60m.), respectively, for 802.11b. Using a site survey tool is recommended to measure signal strength at various locations throughout the site to determine the number of and positioning of APs.

There are four main physical-layer standards for WLANs: 802.11, 802.11b, 802.11a and 802.11g. The 802.11 is the first standard and is only found in legacy installations. It is discussed here for reference purposes and should not be purchased. The 802.11b reached dominance in late 2003 and has 11Mbps data rates in the 2.4GHz band. The 802.11a is the follow-up standard that is capable of reaching 54Mbps rates in the 5GHz range. The newest standard, 802.11g, increases data rates to 54Mbps in the 2.4GHz band and is backwards-compatible with 802.11b. The 802.11b, 802.11a and 802.11g can all operate in the same environment without causing interference with each other.

Table 13. Comparison of Wireless Local-Area Network Standards

	802.11 (1)	802.11b	802.11a	802.11g
Modulation Scheme	DSSS	DSSS	OFDM	OFDM Complementary Code Keying (CKK) Packet Binary Convolutional Coding (PBCC) optional mode for 22Mbps link rate
Theoretical Link Rates (2)	1 or 2Mbps	1, 2, 5.5, 11Mbps	6, 9, 12, 18, 24, 36, 48, 54Mbps	6, 9, 12, 18, 24, 36, 48, 54Mbps
Real World	1Mbps	6Mbps	33Mbps	
Frequency Band	2.4GHz	2.4GHz	2.4GHz; 5.8GHz	2.4GHz
Maximum Number of Independent Channels	Three channels (1, 6 and 11) indoor/outdoor	Three channels (1, 6 and 11) indoor/outdoor	Eight channels (four indoor, four in-/outdoor)	Three channels (1, 6 and 11) indoor/outdoor
Typical Range	150 ft indoors, 300 ft outdoors	Gartner estimates indoor and outdoor ranges to be 100 ft. and 200 ft., respectively	Gartner estimates 802.11a range is limited to 15–25 ft.	
Typical Number of Clients Supported per Access Point	The theoretical number of clients supported by an AP is 256, depending on usage patterns, 20-30 users are recommended for optimal performance.	The theoretical number of clients supported by an AP is 256, depending on usage patterns; 20-30 users are recommended for optimal performance	The theoretical number of simultaneous connections supported by an AP is 1,024	The theoretical number of clients supported by an AP is 256, depending on usage patterns, 20-30 users are recommended for optimal performance.
Transmit Power	Up to 100 mW	Up to 100mW (20dBm) 30mW (15dBm) most common Variable up to vendor	Up to 10 mW (20dBm) 30mW (15dBm) most common Variable up to vendor	Up to 100mW (20dBm) 30mW (15dBm) most common Variable up to vendor
Strengths	• First enterprise-class WLAN technology	• Meets today's requirements for wireless • Mature	• Faster data rates • Less interference • 32-bit bus architecture	• Compatible with 802.11b and 802.11a • Increases data rates to 2.4GHz to 54Mbps
Limitations	• Slow • No longer widely used	• Half-duplex • Prone to interference • WEP security breaches	• Consumes more power • Shorter range (to achieve 54Mbps cell size should be 25 ft.) • Not backward-compatible to .11b • No WiFi-certified products • Immature	• Effective data rate reduced when in the presence of 802.11b clients • 2.4GHz ISM band is crowded

NIH will have to resolve the challenge created by using Bluetooth, 802.11b and 802.11g because they all work in the 2.4GHz frequency. NIH, seeking to deploy systems integrating Bluetooth and 802.11b/g WLANs, should purchase WLAN products that incorporate technologies that have been designed to coexist.

Other relevant standards for 802.11 WLAN include:

- 802.11d — Supplement to the MAC layer in the base 802.11 WLAN standard. It aims to promote worldwide use of 802.11. It will allow access points to communicate information on the permissible radio channels and at acceptable power levels to user devices. The current 802.11 standards cannot legally operate in some countries, and the purpose of 802.11d is to add features and restrictions to WLAN systems that would allow them to operate within the specific regulatory guidelines of these countries.
- 802.11e — Supplement to the MAC layer to provide quality-of-service support for LAN applications. This will apply to all 802.11 physical-layer standards (a, b and g). The purpose is to provide classes of service with managed quality-of-service levels for data, voice and video applications.
- 802.11f — A recommended practice document. It aims to achieve access point interoperability within a multi-vendor WLAN network. The document defines the registration of access points within a network and the interchange of information between access points in case of the handover of users.
- 802.11h — Supplement to the MAC layer to meet the regulatory provisions for European 5GHz WLANs.
- 802.11i — Supplement to the MAC layer to provide improved WLAN security was approved in June 2004 to address several security improvements needed to make wireless communications an integral part of enterprise networks, although some concerns about interoperability remain. It applies to all 802.11 physical standards (a, b and g). The purpose is to provide an alternative to WEP with new encryption methods and authentication procedures. A key part of 802.11i is IEEE 802.1x, which addresses Wired Equivalent Privacy and WPA.
- 802.11n — Next-generation wireless LAN (WLAN) architecture involves definition of the Physical Layers (PHYs) and Media Access Control (MAC) layers to promote WLAN link rates beyond 200 megabits per second (Mbps).
- 802.15 — Working group of the IEEE addressing standardization of wireless Personal Area Networks (PANs).
- 802.16 — Broadband wireless standard, also known as Worldwide Interoperability for Microwave Access (WiMax), which aims to deliver multimegabit “last mile” wireless access over a distance of several kilometers with a data rate of 15Mbps over a 3- to 5-km. range. The following WiMAX standards are still being defined as of the date of this document:
  - 802.16b — Quality of Service
  - 802.16c — Interoperability and testing protocols
  - 802.16d — Access point standards
  - 802.16e — Support for mobile as well as fixed broadband

- 802.20 — IEEE standardization initiative for wireless metropolitan-area networks.

The Wireless LAN Brick shown below applies to both access points and Network Interface Cards (NICs). NIH aims to reduce the number of vendors in the wireless AP and NIC environment in order to achieve better cost discounts and to simplify patch distribution and network management.

Table 14. Wireless LAN Brick

Baseline Environment (Today)	Tactical Deployment (Zero to two years)	Strategic (Two to five years)
Technology: ■ 802.11b ■ 802.11g ■ Bluetooth **Vendors:** ■ Apple ■ Cisco Systems ■ Enterasys Networks ■ Intel ■ Lucent ■ Sony	**Technology:** ■ 802.11g **Vendors:** ■ Cisco Systems ■ Enterasys Networks	**Technology:** ■ 802.11g ■ 802.16
Retirement	**Containment**	**Emerging**
None	**Technology:** ■ Bluetooth ■ 802.11b **Vendors:** ■ Apple ■ Intel ■ Lucent ■ Sony	**Technology:** ■ 802.11e for QoS ■ 802.11n ■ WiFi security technologies and standards, such as 802.11i
Comments		
■ This brick is intended to address WLAN access points. ■ Deployment of Bluetooth technology for LAN functionality is on an exception basis only and is strongly discouraged. ■ New wireless deployments will be coordinated with CIT to ensure compatibility across NIH. ■ Cards must support industry-standard technologies 802.11b and 802.11g. ■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products. ■ Some baseline products have been designated Retirement and Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.		

3.9 Brick 8: LAN Cabling

Structured cabling standards have been developed and published by NIH. Figure 2 and Figure 3 in the Patterns section of this report (sections 2.1.2 and 2.1.3 respectively) illustrate a high-level architectural standard that should be used as a guide when cabling network devices. The cabling standards document referenced in the LAN Cabling brick in the following table should be used for specific implementation guidelines.

For the next five to 10 years, NIH will continue to deploy Category 6 cabling for new installations and does not need to consider deploying higher-grade cabling.

- Category 6 solutions typically are priced at a 15–25 percent premium (including materials and labor) above Category 5e. When comparing the costs of cabling solutions, it is important to consider both materials and labor.
- Category 6 cabling delivers a usable bandwidth twice that of Category 5e. The Category 6 standard specifies a higher-quality cable that will more reliably support gigabit speeds and should be the cable of choice for all new NIH network installations.
- Category 6 also provides additional tolerance for some common cabling problems, such as external noise or sloppy installations. Thus, a Category 6 installation will result in fewer instances of labor-intensive cable troubleshooting.

Compared to other network resources, cable and wiring have long life spans, typically lasting seven to 12 years, and sometimes as long as 15 years. Therefore, at least two generations of network technologies are likely to be deployed over whatever cabling system NIH chooses to deploy today.

Poor cabling decisions are costly and potentially disruptive. Correcting cabling mistakes can cost anywhere from 140 percent to 250 percent of the original cost if it needs replacing once it is already in the wall or ceiling.

NIH should focus its backbone on multiple 1Gbps-over-fiber links, leading to 10Gigabit-over-fiber as traffic increases and prices decline. Alternatively, NIH can deploy copper where there is insufficient fiber to run multiple 1,000Mbps links.

Table 15. LAN Cabling Brick

Baseline Environment (Today)	Tactical Deployment (Zero to two years)	Strategic (Two to five years)
■ Cat. 5, 5e, 6 ■ Fiber Cabling (Multi-mode, Single-mode)	■ Cat. 6 ■ Fiber Cabling (Multi-mode, Single-mode)	■ Cat. 6 ■ Fiber Cabling (Multi-mode, Single-mode),
Retirement	**Containment**	**Emerging**
■ Cat. 5	■ Cat. 5e	■ Cat. 6 and Cat. 7
Comments		
■ Follow cabling standards specifications, as posted at these Web sites: ❑ http://www.cit.nih.gov/dnst/DNSTweb/CIS/tel_lan.htm ❑ http://www.cit.nih.gov/dnst/DNSTweb/CIS/utp.htm ■ Amp and Corning have typically been vendors for cabling. ■ CIT must certify, against cabling standards, any work that CIT does not perform or domplete. ■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products. ■ Some baseline products have been designated Retirement and Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.		

3.10 Brick 9: Communications Protocol

Communications protocols define the rules for sending blocks of data from one node in the network to another node and are normally defined in layers. A protocol specification defines the operation of the protocol and may also suggest how the protocol should be implemented.

Minimizing the number of protocols in use can benefit NIH by simplifying the environment and improving interoperability. Retirement of DecNet and use of TCP/IP as the primary protocol on NIHnet and subnets is recommended. SNA will be converted to IP. Data-link switching (DLSw) provides a means of transporting IBM Systems Network Architecture (SNA) and network basic input/output system (NetBIOS) traffic over an IP network. DLSw can be used to reduce SNA traffic over the WAN. Video will use the H.32x standard. AppleTalk, IPX and SNA will be contained with no more implementations. Minimizing the number of network protocols will have a significant return on the total cost of ownership (TCO) for network management.

Table 16. Communications Protocol Brick

Baseline Environment (Today)	Tactical Deployment (Zero to two years)	Strategic (Two to five years)
■ AppleTalk ■ DecNet ■ H.32x ■ IPX ■ Netbios ■ SNA ■ TCP/IP	■ H.32x ■ Multicast ■ TCP/IP	■ H.32x ■ Multicast ■ TCP/IP
Retirement	**Containment**	**Emerging**
■ DecNet	■ Apple Talk ■ IPX ■ SNA over DLSw	■ IP version 6 ■ SIP
Comments		
■ SNA will be converted to IP. ■ All video conferencing standards should be based on H.32x protocols. ■ IP addresses will be assigned, administered and centrally managed by CIT. No new private address spaces should be deployed. ■ Voice over IP (VoIP) is emerging within NIH. This network architecture anticipates the needs of VoIP, although any IC intending to implement VoIP should consult with CIT to ensure the infrastructure being implemented can be supported in a consistent manner. ■ DLSw can be used to transport SNA over IP until SNA is retired. ■ Session Initiation Protocol (SIP) is required to support VoIP. And as VoIP services are implemented at NIH, NIH should consider making SIP a tactical and strategic standard. ■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products. ■ Some baseline products have been designated Retirement and Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.		

3.11 Brick 10: Network Load Balancing Server

This brick shows NIH's direction for network load balancers that allow server workload to be distributed across multiple servers for greater end-to-end application availability.

Table 17. Network Load Balancing Server Brick

Baseline Environment (Today)	Tactical Deployment (Zero to two years)	Strategic (Two to five years)
■ Cisco Systems ■ F5 Networks ■ Foundry Networks ■ Nortel Networks	■ Cisco Systems ■ F5 Networks	■ Cisco Systems ■ F5 Networks
Retirement	**Containment**	**Emerging**
■ None	■ Foundry Networks ■ Nortel Networks	■ Cisco Systems ■ F5 Networks
Comments		
■ Coordinate any load balancing implementations through CIT for IP address space allocation. ■ Refer to Network Load Balancing Pattern in Section 2.5. ■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products. ■ Some baseline products have been designated Retirement and Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.		

3.12 Brick 11: Remote Access Technology

Remote access provides the ability to connect to the network from a distant location. This requires a computer, a modem and remote access software to allow the computer to dial into the network over a telephone line, cable or satellite service, and connect. Remote access via a virtual private network (VPN) creates encrypted tunnels over an existing Internet connection between remote users and the network data center.

Many ICs are deploying and managing their own remote access networks. Remote access at NIH is neither vendor-managed nor centralized. The deployment of multiple remote access infrastructures is unnecessary and inefficient.

Security of remote access services is always a concern, as the public network infrastructure is used to deliver these services to NIH users. The Security Architecture domain team report provides guidance on supplying security for the remote access design.

Table 18. Remote Access Technology Brick

Baseline Environment (Today)	Tactical Deployment (Zero to two years)	Strategic (Two to five years)
Technology: ■ Dial-up ■ VPN **Vendors:** ■ Cisco Systems (Dial-up and VPN) ■ Linux server for remote access	**Technology:** ■ VPN ■ Dial-up **Vendors:** ■ Cisco Systems (Dial-up and VPN)	**Technology:** ■ Centralized, NIH-wide VPN **Vendors:** ■ Cisco Systems (VPN)
Retirement	**Containment**	**Emerging**
■ None	■ Linux server for remote access	■ TBD
Comments		
■ Recommend retiring applications such as PC Anywhere. See Security policy for details. ■ VPN is preferred over dial-up for tactical deployments. ■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products. ■ Some baseline products have been designated Retirement and Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.		

This technical solution also allows for a corporate-wide ISP contract that can be offered as an alternative access method to users who generate the highest access charges. Such an agreement could provide VPN over local, nationwide and international dial-up access on a more cost-effective basis.

3.13 Brick 12: Availability Management — Network

Network management includes the administrative services performed in managing NIHnet and the IC networks, including network devices, network topology and software configuration, monitoring network performance, maintaining network operations, and diagnosing and troubleshooting problems. Network management requires the skillful integration of software tools, management processes and resources to provide enterprise managers with a coherent view of network availability and performance. This task becomes increasingly difficult as business applications become more reliant on and intertwined with network infrastructure and as users come to expect nearly unlimited, "free" bandwidth.

An NIH Network Operations Center will provide NIHnet with Performance Monitoring, Proactive Fault Prediction and Restoral, a method to identify critical outages and 24/7 network monitoring for all ICs.

A network management capability must be developed based on Simple Network Management Protocol (SNMP) version 3, and all network management solutions must interface to HP OpenView for compliance to this architecture.

Table 19. Availability Management — Network Brick

Baseline Environment (Today)		Tactical Deployment (Zero to two years)	Strategic (two to five years)
■ Atlantis Software PageManager ■ CA Unicenter ■ CiscoWorks LAN Management Solution ■ Custom scripts ■ Dell OpenManage ■ EMC Navisphere ■ Enterasys Networks NetSight Atlas Console Manager, ■ Enterasys Networks NetSight Policy Manager ■ Enterasys Networks NetSight Element Manager ■ Ethereal (OpenSource) ■ Fluke (Suite) ■ HP OpenView NNM ■ Ipswitch WhatsUp Gold ■ Locally developed tools ■ Mercury Interactive ActiveWATCH	■ Nagios (Open Source) ■ Nmap (Open Source) ■ Mercury Interactive SiteScope ■ Paessler IP Check ■ Peregrine InfraTools ■ Peregrine IND ■ Quest Software Big Brother ■ RRDtool (shareware) ■ SolarWinds Network Management Software ■ Thcrut (Open Source) ■ Wild Packets EtherPeek ■ winFingerprint (Freeware)	■ CA Unicenter ■ CiscoWorks LAN Management Solution ■ Fluke (Suite) ■ HP OpenView NNM ■ Nagios (Open Source) ■ RRDtool (shareware) ■ Wild Packets EtherPeek	■ CiscoWorks LAN Management Solution ■ Either HP OpenView or CA Unicenter ■ Fluke (Suite)

Retirement (Technology to eliminate)	Containment (No new deployments)		Emerging (Technology to track)
■ Quest Software Big Brother ■ Paessler IP Check ■ Peregrine InfraTools	■ Atlantis Software PageManager ■ Custom scripts ■ Dell OpenManage ■ EMCNavisphere ■ Enterasys Networks NetSight Management Suite ■ Ethereal (OpenSource) ■ IPSwitch WhatsUp Gold	■ Locally developed tools ■ Mercury Interactive ActiveWATCH ■ Micromuse Netcool/Webtop Client ■ Nmap (Open Source) ■ Thcrut (Open Source) ■ winFingerprint (Freeware)	■ Other leading or innovative network management products such as: ❑ Adlex ❑ NetQoS ❑ Voyence

Comments

- NIH needs to choose either the HP OpenView or CA Unicenter framework as the enterprise strength network management tool.
- Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products.
- Some baseline products have been designated Retirement and Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected Tactical and Strategic products.

4.0 Gap Analysis

The following items represent the gaps between the current-state network architecture and the elements that need to be developed in order to achieve the future-state network architecture vision.

- Router and switch vendors need to be reduced in order to achieve volume purchase savings and to simplify centralized configuration, management and software/patch distribution.
- Availability Management for Networks will be further refined as the ESM efforts to provide better end-to-end availability and visibility for enterprise systems defines standardized management processes, tools and data interchange for providing a single view of systems and infrastructure availability and management.
- The number of wireless vendors needs to be reduced in order to achieve volume purchase savings and to simplify centralized configuration, management and software/patch distribution.
- As remote access is centralized as part of network consolidation, the more expensive dial-up options should be phased out.
- Legacy protocols such as DECnet need to be removed from the network.

5.0 Next Actions

The following details the next actions that need to be implemented by NIH in order to begin the migration to the future-state network architecture:

- All new router and switch vendor deployments should use the vendors listed in the router and switch brick. This will help to reduce the number of vendors that need to be managed and reduce TCO.
- Today, network management systems exist within multiple ICs across NIH with different products and capabilities. All ICs should plan to participate in the NIH Centralized Network Monitoring System (CNMS) which offers an alternative to each IC needing to install its own system, and allows for ICs without existing network management capability to gain the benefits of a full-function network monitoring system. The CNMS system provides a consistent and cost-effective way to monitor networks at NIH. In addition, ICs with existing network management systems have the option to utilize the centralized system and gradually move away from their IC-specific systems.
- The NIH wireless infrastructure needs to become a secure utility for both staff and visitors. In this capacity, the wireless network needs to provide ubiquitous access both within, and external to, the physical building infrastructure. Wireless needs to be considered as a utility as critical as phone and traditional HVAC within all building spaces. To fulfill this need, the wireless network needs to evolve from a “best effort” solution to a “five nines” utility service.
- It is recommended that the Network Domain Team remain instituted to develop product standards and common, shared network deployments.
- At the next refresh of the Network Architecture, consider addressing VoIP if a business case can provide reasonable benefits for NIH. In that case, the impact to the data network needs to be fully understood and voice network architecture content needs to be developed to support those services.

Change History/Document Revisions

Date	Change Author	Change Authority	Change Event	Resulting Version
18 July 2003	David Reuben	Jack Jones	Original Production	1.0
2 Mar 2005	Blanton/Reuben/ Maoury	Jones/ Schmitz	Final draft for ARB Approval	2.0

Appendix A — Glossary of Terms

Appendix A — Glossary of Terms

Term	Definition
Access Layer	The access layer connects the workgroup layer to the network.
Access Point (AP)	The basic building block of a wireless local-area network infrastructure. Access points attach to a wired backbone and provide wireless connectivity to all devices within range. In a roaming infrastructure, as devices move out of the range of one access point, they move into the range of another.
Access Switch/Router	A device that connects workgroup switches and edge switches.
AES — Advanced Encryption Standard	Algorithm for encryption which has been selected by the National Institute of Standards and Technology as the replacement for Data Encryption System standard (DES). AES supports 128- and 256-bit key lengths.
ATM — Asynchronous Transfer Mode	A wide-area network (WAN) technology. ATM is a transfer mode for switching and transmission that efficiently and flexibly organizes information into cells; it is asynchronous in the sense that the recurrence of cells depends on the required or instantaneous bit rate. Thus, empty cells do not go by when data is waiting. ATM's flexibility lies in its ability to provide a high-capacity, low-latency WAN switching fabric that is protocol-, speed- and distance-independent, and that can support multiple types of information (including data, video, image and voice).
BGP — Border Gateway Patrol	The interdomain routing protocol implemented in Transmission Control Protocol/Internet Protocol (TCP/IP) networks. BGP-4 is a networking redundancy service based on Border Gateway Protocol (BGP). It enables an enterprise to route Information Protocol (IP) traffic destined for the same IP address via different network connections. In a BGP-4 environment, when a transmission comes from an Internet service provider's network, it will look for the primary router that connects to the enterprise's location. If that router becomes unavailable, the transmission will automatically be redirected to the backup router without interrupting the original transmission.
CAN	Campus-Area Network — used at the main NIH campus to connect campus users in the various buildings onto NIH's network, NIHnet
CGMP — Cisco Systems Group Management Protocol	Proprietary protocol for supporting IP multicast.
Content Networking	An enterprise's Web presence and preparedness to take advantage of Web technologies in its business processes.
Core Layer	The core layer is a highly reliable layer of the network, sometimes also referred to as the backbone. Its main function is to route traffic as quickly as possible and provide aggregation and summarization services.
CWDM	Coarse wavelength division multiplexing is a form of wavelength division multiplexing that has wider spacings between the wavelengths used than Dense WDM. Also, unlike other forms of WDM, it uses a far broader photonic band spectrum than other such systems, which often are confined to one or two bands. Up to 18 wavelengths can be sent using some schemes of CWDM. CWDM can be used over multimode and single-mode fibers although signal distances are generally shorter than

Term	Definition
	DWDM. The costs of deploying CWDM are significantly lower than DWDM.
Demarc	Demarcation point — a delineation point shown in network diagrams
Direct Sequence Spread Spectrum (DSSS)	Is the process in which a lower-frequency wave is superimposed on a wave of higher frequency that is fixed and constant (the carrier wave), thus modifying it to produce an information-bearing signal. DSSS "spreads" the signal across a broad band of radio frequencies and creates a redundant pattern called a "chip" to transmit; it is used in 802.11b WLANs.
Distribution Layer	The distribution layer acts as an area and address aggregation point. Complex, CPU-intensive policy-based operations are usually performed at this layer. It lies between the access and core layer.
DLSw — Data Link Switching	An IBM-developed technique for carrying Systems Network Architecture (SNA) traffic over a Transmission Control Protocol/Internet Protocol (TCP/IP) network. DLSw "tunnels" or encapsulates SNA traffic using the transport services of TCP/IP.
DMZ — Demilitarized Zone	Technical jargon for the protected subnet between an intranet and the public Internet.
Dual-Homed Connection	When a switch or router has a redundant connection to another switch or router. The purpose is to provide an alternative path in order to increase network availability for critical locations that can cost justify a dual-homed network design.
DWDM	Dense wavelength division multiplexing (DWDM) is a fiber-optic transmission technique that employs light wavelengths to transmit data parallel-by-bit or serial-by-character.
Edge Switch	A device that connects access switches and hubs.
EIGRP— Enhanced Interior Gateway Routing Protocol	A proprietary interior gateway protocol (IGP) from Cisco Systems — an enhanced version of Cisco Systems' Interior Gateway Routing Protocol (IGRP).
ESM — Enterprise Systems Management	Enterprise Systems Management (ESM) services are the processes and tools that monitor the hardware, software, applications, networks and operational elements in the IT environment. The primary objective of ESM is to improve the service levels provided by the IT environment.
Etherchannel	EtherChannel is a Cisco Systems technology that builds on 802.3 full-duplex Fast Ethernet to provide greater bandwidth for a campus backbone.
EvDO	The Evolution Data Only (EvDO) system is a wireless system that modifies the 1.25 MHz IS-95 radio channel structure to provide wireless broadband data services up to 2.4 Mbps.
GBIC-Gigabit Interface Converter	Transceiver that converts serial electric signals to serial optical signals, and vice versa. In networking, a GBIC is used to interface a fiber optic system with an Ethernet system.
H.32x	A series of computing standards from the International Telecommunication Union (ITU) that address videoconferencing. These include H.320, H.323 and H.324.

Term	Definition
H.320	An international "umbrella" standard for audio-conferencing and videoconferencing. It comprises many related standards, including H.261.
H.323	An umbrella standard for audio-conferencing and videoconferencing. It is a videoconferencing suite that has G.723 voice, T.120 collaborative and H.263 video components in a single session.
H.324	An international standard for videoconferencing over the public switched telephone network.
HSRP — Hot Standby Routing Protocol	A proprietary protocol from Cisco Systems that allows several physical routers to share an IP address and MAC address so that if one router fails, the others can takeover the workload without requiring user intervention.
Hub	An aggregation point for multiple locations.
IGMP — Internet Group Membership Protocol	Open standard for establishing memberships in multicast groups.
IPX — Internetwork Packet Exchange	A routing protocol, based on Xerox's XNS, developed by Novell and implemented in Novell's NetWare.
ISP — Internet Service Provider	A company that provides Internet access to its customers. The majority of ISPs are too small to purchase access directly from the network access point (NAP), and instead buy pieces of bandwidth that are available from larger ISPs. ISPs are different from online services, although these services sometimes also provide access to the Internet. Online services provide access to exclusive content, databases and online discussion forums that are not available outside the service.
LAN	Local-Area Network — a geographically limited or contained communications network that connects users within a defined area.
Layer 2 and 3 Switch	Layer 3 switching technology that integrates routing with switching to yield very high routing throughput rates in the millions-of-packets-per-second range. The movement to Layer 3 switching is designed to address the downsides of the current generation of Layer 2 switches, which functionally are equivalent to bridges. These downsides for a large, flat network include being subject to broadcast storms, spanning tree loops, and address limitations.
Link Aggregation	Is the aggregation of individual links onto a common trunk.
MAC	A protocol from the Institute of Electrical and Electronics Engineers, defining the methods used to gain access to the physical layer of a LAN — that is, Layer 1 of the Open Systems Interconnection (OSI) model.
MAN	Metropolitan-Area Network — is used to connect the main NIH campus to other NIH locations within the metropolitan area.
MIB — Management Information Base	A Simple Network Management Protocol (SNMP) flat-file, non-relational database that describes devices being monitored. Network management platforms monitor nodes by reading the value of the managed resources in the MIB. Management platforms can effect changes in managed resources by altering MIB values — for example, by establishing thresholds beyond which alerts are created.

Term	Definition
MMF — Multi-Mode Fiber	Fiber (optical cable) that supports or transmits multiple transmission modes (i.e., frequencies).
MoM — Manager of Managers	A centralized network management solution that interfaces individual network management systems from multiple vendors.
MPLS — Multi-Protocol Label Switching	A protocol that helps support quality of service in Internet Protocol (IP) networks. A router labels packets to assign different levels of service based on different priority levels. This helps ease congestion for high-priority network traffic, such as that needed for mission-critical applications.
Multicast	A signal transmitted to only a subset of potential destinations (as opposed to a broadcast), typically over an Internet Protocol (IP) network.
NAT — Network Address Translation	A function that translates the Internet Protocol (IP) addresses used in an internal IP network's addressing structure to fewer, external Internet IP addresses.
NOC — Network Operations Center	A data center term which refers to the "central nervous system" of operations.
OC-n — Optical Carrier Level N	The range of incremental rates defined for Synchronous Optical Network (SONET) fiber-optic transmission (see SONET). Levels in the hierarchy are ordered by the bit rate of their aggregated signals. The number after "OC-" represents the multiple of the foundation OC-1 rate, which is 51.84 megabits per second (Mbps).
Orthogonal Frequency Division Multiplexing (OFDM)	Transmits data in a parallel technique, as opposed to DSSS's "spread" technique, by slowing the symbol rate enough so that it is longer than the delay spread. OFDM is used in 802.11a and proposed 802.11g WLANs to establish an Ethernet scheme for data transmission. The data is mapped across several lower-speed signals effectively blocking interference because transmission is spread across all sub-carriers in parallel.
OSI — Open Systems Interconnection	A model developed by the International Organization for Standardization (ISO) for communications. OSI offers a standard, modular approach to network design that divides the required set of complex functions into manageable, self-contained, functional layers. These layers, starting from the innermost, are: Physical, Data, Network, Transport, Session, Presentation and Application.
OSPF — Open Shortest Path First	An interior gateway protocol (IGP) that transfers packets from one network to an adjacent one.
PIM — Protocol Independent Multicast	PIM is a widely used and routing-protocol-independent method for supporting multicast. When compared to other multicast protocols, PIM introduces less overhead onto the network because it uses the existing unicast routing table for packet forwarding.
POP – point of presence	The point to which the local telephone company terminates subscribers' circuits for access to long-distance service, or to dial-up leased-line or Internet communications.
PoS – Packet over SONET	Packet-over-SONET/SDH (POS) enables core routers to send native IP packets directly over SONET/SDH frames. POS provides lower packet overhead and lower cost per Mbit than any other data transport method.
Public Switched Telephone Network (PSTN)	The shared public network used to supply dial tone for basic voice and data services.

Term	Definition
QoS — Quality of Service	A negotiated contract between a user and a network provider that renders some degree of reliable capacity in the shared network.
RMON — Remote Monitoring	A specification that builds on the functionality of Simple Network Management Protocol (SNMP) by extending the definition of the SNMP management information base (MIB) to enable network managers to monitor sub-network devices via the MIB. RMON also enables the local collection of device data, thereby helping network administrators address the bandwidth constraints imposed by SNMP's device-polling design.
Routing Protocol	Protocol that accomplishes routing through the implementation of a specific routing algorithm. Examples of routing protocols include IGRP, OSPF and RIP.
Server Switch	A device that connects multiple servers.
SIP	Session Initiation Protocol is used to initiate interactive communication sessions of various types — including voice, video, chat, interactive games and virtual reality — between Internet users. A proposed standard of the Internet Engineering Task Force (IETF), the protocol is administered under the IETF's SIP Working Group.
SMF — Single Mode Fiber	An optical fiber with a small core diameter, allowing the propagation of a single light path.
SNMP — Simple Network Management Protocol	A Transmission Control Protocol/Internet Protocol (TCP/IP) protocol governing network management and the monitoring of network devices. Strictly speaking, SNMP is the Management Information Base (MIB) described in the SNMP standard; extensions to this MIB proposed by the Electronic Messaging Association permit the monitoring and reporting of all conforming messaging components through standard SNMP management tools for network components.
SONET — Synchronous Optical Network	An International Telecommunications Union standard for high-speed communications over fiber-optic networks. It offers synchronous transmission at speeds up to multi-gigabit rates — defined at various "Optical Carrier" (OC) levels — and includes features to enable multi-vendor interoperability, improved troubleshooting and network survivability.
SSL — Secure Sockets Layer	An Internet security standard developed by Netscape Communications. SSL offers session-level security — that is, after a secure session has been initiated; all information transmitted over the Internet during that session is encrypted. SSL also offers features such as server and client authentication as well as message integrity.
Switching Fabric	Is the combination of hardware and software that moves data coming in to a network node out by the correct port to the next node in the network. Switching fabric includes the switching units in a node, the integrated circuits that they contain, and the programming that allows switching paths to be controlled.
TCO — Total Cost of Ownership	A comprehensive assessment of information technology (IT) or other costs across enterprise boundaries over time. For IT, TCO includes hardware and software acquisition, management and support, communications, end-user expenses, and the opportunity cost of downtime, training and other productivity losses.

Term	Definition
TCP/IP — Transmission Control Protocol/Internet Protocol	A set of protocols covering (approximately) the network and transport layers of the seven-layer Open Systems Interconnection (OSI) network model. TCP/IP was developed during a 15-year period under the auspices of the U.S. Department of Defense. It has become a dominant standard in enterprise networking, particularly at higher-level OSI layers over Ethernet networks.
TLS — Transport Layer Security	A protocol designed to secure the privacy of communications over the Internet. It is defined in request for comment 2246 from the Internet Engineering Task Force.
TRM — Technical Reference Model	An enterprise architecture framework for technical infrastructure. Within the federal government this refers to one of five reference models developed by the Federal Enterprise Architecture Program Management Office. See www.feapmo.gov for more information.
UPS — Uninterruptible Power Supply	A device that provides temporary power upon failure of the main power source.
VLAN — Virtual Local-Area Network	A set of systems that, regardless of higher-layer addressing or location, is designated as a logical local-area network (LAN) and treated as a set of contiguous systems on a single LAN segment. VLANs can be proprietary or standardized using the Institute of Electrical and Electronics Engineers' 802.1q specification. Typical grouping parameters for VLANs include the port number of the hub, switch or router, the higher-layer protocol such as Internet Protocol (IP) or Internetwork Packet Exchange (IPX), the Media Access Control (MAC) address, and the traditional subnet. The goal of VLANs is to provide simpler administration and partitioning at the MAC layer.
VoIP — Voice over IP	Transmission of voice communications over Internet Protocol (IP) data networks, such as IP-based LANs, intranets or the Internet. Many carriers offer integrated services such as voice and data over a single "pipe".
VPN — Virtual Private Network	A system that delivers private communications services on a shared, public-network infrastructure, and provides customized operating characteristics uniformly and universally across an enterprise. VPN service providers define a VPN as a wide-area network of permanent virtual circuits, generally using asynchronous transfer mode or frame relay to transport IP. VPN technology providers often define "virtual private networking" as the use of encryption software or hardware to bring privacy to communications over a public or untrusted data network.
WAN	Wide-Area Network — is used to connect locations outside the metropolitan area.
WDM — Wave Division Multiplexing	A technology used to increase fiber-optic transmission capacity. Also see DWDM.
Web Optimization	Provides applications traffic management for Web-based applications. These functions include applications layer load balancing, connection management, route determination and others.
WLAN — Wireless Local-Area Network	A LAN communication technology in which radio, microwave or infrared links take the place of physical cables. Three physical media types of WLAN are available. The first two — direct-sequence spread spectrum (see DSSS) and frequency-hopping spread spectrum (see FHSS) — are

Term	Definition
	based on radio technologies that are not interoperable. The third is based on infrared, a non-radio technology based on light waves. Infrared can coexist with DSSS and FHSS radio-based systems in one enterprise network.
Workgroup Layer	The workgroup layer is used to segment and connect servers and/or devices in a network.
Workgroup Switch	A device that connects work stations, printers, hosts and servers to an access switch in the building

Client Contact Information

John F. Jones, Jr.
Chief IT Architect
Telephone: +1-301-402-6759
E-mail: jonesjf@mail.nih.gov

Gartner (Contractor Support) Contact Information

Terry McKittrick
Gartner Consulting
Telephone: +1-703-226-4779
Facsimile: +1-703-226-4702
E-mail: terry.mckittrick@gartner.com