OD/OCIO and CIT/DNST
NIHRFC0039
Category: Standard

Brett Moseley and Steve Thornton
OD and CIT
March 2011

Campus Area Network (CAN), Metropolitan Area Network (MAN), and Wide Area Network (WAN) Pattern and Bricks V2.0

Status of this Memo

This document proposes a standard for the National Institutes of Health (NIH) and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

This standard **OBSOLETES** the CAN/MAN/WAN Optical Networking Brick (no NIHRFC number), dated February 8, 2005: http://enterprisearchitecture.nih.gov/ArchLib/AT/TA/CANMANWANOpticalNetworkingBrick.htm

Table of Contents

1 Introduction

This NIHRFC is an update to the Technical Architecture Standards for the CAN, MAN, and WAN Bricks and the CAN/MAN/WAN Pattern. The standard is being updated to reflect NIH's expanded use of the Dense Wave Division Multiplexer (DWDM) technology, which will increase bandwidth and reduce costs for NIH for the foreseeable future.

2 Background

NIHnet core network service includes the NIH backbone network that interconnects all local area networks (LANs) to the NIH data centers and central services and applications. The network also connects the HHS operating divisions and select local federal partners to the Internet via the Internet and Internet2 (Abilene) connections. It manages access between the ICs and between NIH and the outside world. Information carried by NIHnet includes biomedical, clinical, and administrative data. NIHnet is a wide area network (WAN) comprised of a physical infrastructure of cable, optical fiber, routers and switches, network management control systems, servers, and workstations. This infrastructure supports the NIHnet operation, wireless access points, and security control systems which include firewalls, intrusion detection systems (IDS), content filtering systems, and virus detectors.

3 NIHnet Scope

NIHnet is the NIH backbone network providing a high-speed, highly-available network infrastructure for NIH and interconnects the LANs of the 27 ICs with each other, with the commodity Internet, Internet2, HHS Operating Divisions, (OPDIVS) and other government agencies. NIHnet connects ICs and LANs collocated on the NIH campus (9000 Rockville Pike, Bethesda, and Maryland), numerous off-campus sites located in or close to the National Capital Region and field locations across the U.S. The data and information carried by NIHnet varies widely and includes biomedical, clinical, financial, and administrative data. NIHnet also provides LAN services at select locations.

In addition to maintaining the connectivity between the LANs of individual ICs, and wide area network (WAN) connectivity, NIHnet has facilities for wireless connectivity, remote access services including dial-up and secure virtual private network (VPN), and includes applications for network management. NIHnet is comprised of a physical infrastructure of cable, optical fiber, routers, switches, network management control systems, servers, and workstations which support the operation and function of NIHnet. NIHnet also includes wireless access points, on-ramp router access and specialized security control systems such as firewalls, gateways, intrusion detection systems (IDS), and content filtering systems for the operation and protection of the network infrastructure.

3.1 NIHnet Peering Relationship

NIHnet interconnects with other public, private, and Federal networks. These external networks are called "peers" and the act of interconnecting is called "peering."

3.2 Internet2 (http://www.internet2.edu/network)

The Internet2 Network is the U.S. research and education network that provides members with high-capacity, low-latency connectivity that avoids the congestion of the general Internet. The current network, fully redesigned and deployed in 2006 when it replaced Abilene, provides next-generation production services as well as a platform for the development of new networking ideas and protocols. NIHnet customers communicate with Universities, Labs, and other Federal research agencies through this “member-only” network.

3.3 HHSnet

HHSnet is a private network interconnecting all HHS Operating Divisions (NIH, FDA, CDC, CMS, IHS, etc.) and special partnering organizations. Data to and from other OPDIVs utilizes HHSnet. NIHnet maintains two fully redundant, fully diverse 1 Gbps connections to the HHSnet backbone.

3.4 NIH Consolidated Co-Location Site (NCCS)

Located in a commercial-operated, secure Data Center in Northern Virginia, the NCCS site provides an alternative hosting environment ideal for disaster recovery and active-active hosting sites. NIHnet provides a scalable 2000 Mbps of connectivity to the NCCS from the campus network. In addition, the NCCS is equipped with its own Internet and Internet2 connectivity, with 100% failover to NIHnet’s Internet and Internet2 peers.

4 Campus Area Network (CAN) Brick

A Campus Area Network (CAN) is a computer network that interconnects Local Area Networks (LAN) throughout a limited geographical area, such as a university campus or corporate campus. A Campus Area Network is, therefore, larger than a Local Area Network but smaller than a Wide Area Network. A Campus Area Network is more flexible to build, upgrade, and operate, as all CAN resources are owned and operated within the organization's boundaries.

Table 1. Campus Area Network (CAN) Brick

Tactical Deployment (0-2 years)	Strategic Deployment (2-5 years)	Emerging (Technology to track)
■ Dark Fiber Owned and Operated by NIH supporting 10Gbps Coarse wavelength division multiplexing (CWDM) ■ Dark Fiber Owned and Operated by NIH supporting 40Gbps Dense Wavelength Division Multiplexing (DWDM)	■ Dark Fiber Owned and Operated by NIH supporting 40Gbps Dense Wavelength Division Multiplexing (DWDM)	■ TBD
Containment (No new deployments)	**Retirement (Technology to eliminate)**	**Baseline Environment (As of last review)**
■ ATM	■ None	■ Dark Fiber Owned and Operated by NIH supporting 10Gbps Coarse wavelength division multiplexing (CWDM) ■ Dark Fiber Owned and Operated by NIH supporting 40Gbps Dense Wavelength Division Multiplexing (DWDM) ■ ATM
Comments		
■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs for new products. ■ Some baseline products have been designated as 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 low as the selected Tactical and Strategic products. ■ From technical and economic perspectives, DWDM technology has the ability to provide potentially unlimited transmission capacity for the foreseeable future for NIH.		

5 Metropolitan Area Network (MAN) Brick

A Metropolitan Area Network (MAN) is a large computer network that spans a metropolitan area. MANs provide Internet connectivity for Local Area Networks (LAN) in a metropolitan region, and connect them to wider area networks like the Internet. MANs typically operate within 30 miles of the campus. Its geographic scope falls between a WAN (Wide Area Network) and a LAN. In the context of NIH, MANs provide connectivity between off-campus buildings to the core NIHnet on campus.

Table 2. Metropolitan Area Network (MAN) Brick

Tactical Deployment (0-2 years)	Strategic Deployment (2-5 years)	Emerging (Technology to track)
Primary ■ Leased Dark Fiber Operated by NIH Running 1Gbps service ■ Leased Dark Fiber Operated by NIH Running 10Gbps service ■ Leased Dark Fiber Operated by NIH Running 40Gbps Dense Wavelength Division Multiplexing (DWDM) Backup ■ Divergent Path Leased Fiber or Circuit (data capacity driven by business needs)	Primary ■ Leased Dark Fiber Operated by NIH Running 40Gbps Dense Wavelength Division Multiplexing (DWDM) Backup ■ Divergent Path Leased Fiber or Circuit (data capacity driven by business needs)	■ TBD
Containment (No new deployments)	**Retirement (Technology to eliminate)**	**Baseline Environment (As of last review)**
■ 100 Mbps	■ None	Primary ■ Leased Dark Fiber Operated by NIH Running 1Gbps service ■ Leased Dark Fiber Operated by NIH Running 10Gbps service ■ Leased Dark Fiber Operated by NIH Running 40Gbps service Backup ■ Divergent Path Leased Fiber or Circuit (data capacity driven by business needs) ■ 100 Mbps
Comments		
■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs for new products. ■ Some baseline products have been designated as 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 low as the selected Tactical and Strategic products. ■ From technical and economic perspectives, DWDM technology has the ability to provide potentially unlimited transmission capacity for the foreseeable future for NIH.		

6 Wide Area Network (WAN) Brick

A wide area network (WAN) is a computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries). This is in contrast with local area networks (LANs), campus area networks (CANs), or metropolitan area networks (MANs) which are usually limited to a room, building, campus or specific metropolitan area (e.g., a city) respectively.

Table 3. Wide Area Network (WAN) Brick

Tactical Deployment (0-2 years)	Strategic Deployment (2-5 years)	Emerging (Technology to track)
■ Leased Dark Fiber Operated by NIH supporting 10Gbps Coarse Wavelength Division Multiplexing (CWDM) ■ Leased Dark Fiber Operated by NIH supporting 40Gbps Dense Wavelength Division Multiplexing (DWDM)	■ Leased Dark Fiber Operated by NIH supporting 40Gbps Dense Wavelength Division Multiplexing (DWDM)	■ TBD
Containment (No new deployments)	**Retirement (Technology to eliminate)**	**Baseline Environment (As of last review)**
■ None	■ None	■ Leased Dark Fiber Operated by NIH supporting 10Gbps Coarse Wavelength Division Multiplexing (CWDM) ■ Leased Dark Fiber Operated by NIH supporting 40Gbps Dense Wavelength Division Multiplexing (DWDM)
Comments		
■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs for new products. ■ Some baseline products have been designated as 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 low as the selected Tactical and Strategic products. ■ From technical and economic perspectives, DWDM technology has the ability to provide potentially unlimited transmission capacity for the foreseeable future for NIH.		

Note: Use of data path triangles can reduce the cost of divergent path engineering by creating a divergent path via another primary location. This WAN design principal in some cases can save significant amounts of money for path diversion. Consideration to geographics, existing data service, provider's facilities, and future data capacities are key design considerations.

It is important to note that NIH is connected to Internet2 directly. Contrary to Internet1 or Abilene, Internet2 provides nationwide connectivity as an aggregator of local or regional fiber high speed networks described as Peers, Participants, and Connectors.

7 CAN/MAN/WAN Pattern

CAN, MAN, and WAN, which represent one pattern 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 preferred technology for linking locations on campus, between campus and off-campus, or between off-campus and off-campus is Dense Wave Division Multiplexer (DWDM).

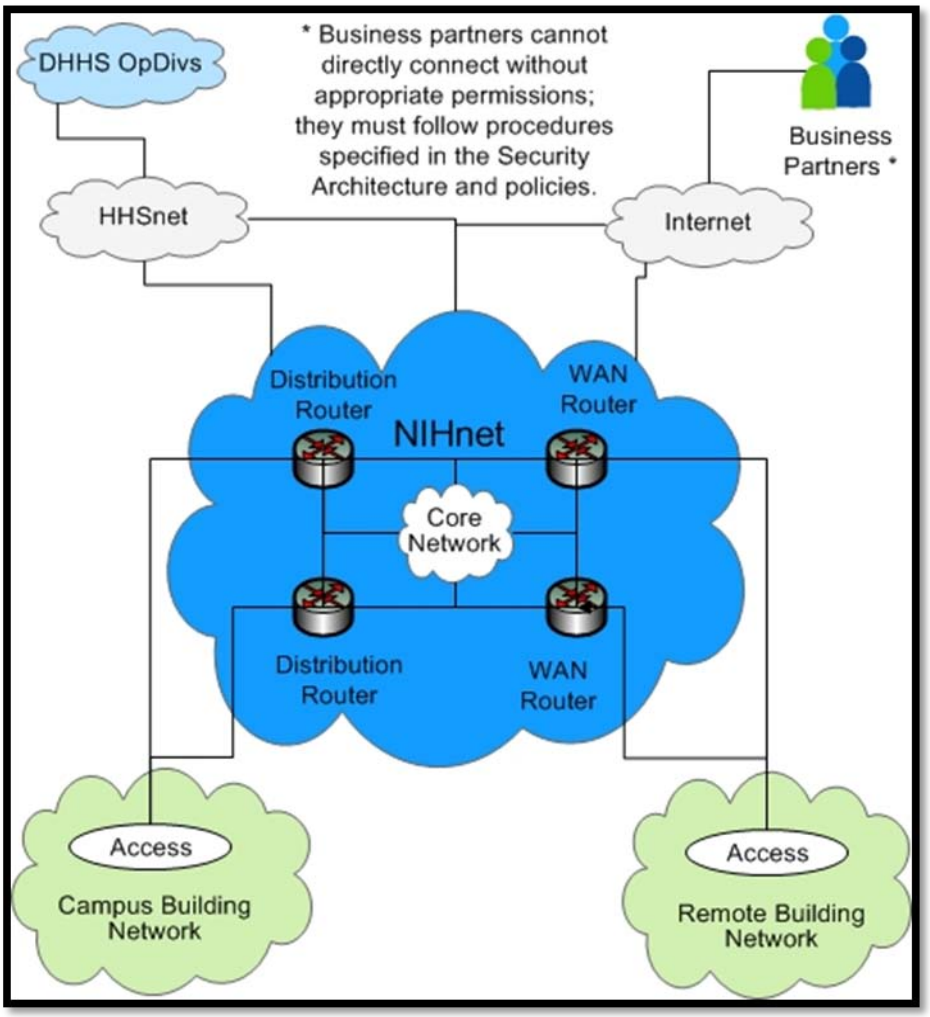
The majority of CAN/MAN and WAN services are centralized at NIH, with CIT taking the lead role in managing the core backbone network infrastructure. All ICs share the core backbone network. The core backbone network supplies connectivity between the ICs, as well as supplying access to the Internet. NIH is migrating DWDM technology to increase bandwidth and reduce costs for NIH for the foreseeable future.

The 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.

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 LAN Minimum Configuration and LAN High Availability Configuration patterns. 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.

Diagram



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.

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).

8 Assumptions

NIHnet will continue to grow in the number of locations supported and in link speeds to all locations. Centralization, web based applications, and disaster recovery will fuel some of the growth of data link capacities and utilizations.

9 References

1. NIH Enterprise Architecture Website – Web Browser Brick http://enterprisearchitecture.nih.gov/ArchLib/AT/TA/WebBrowsersBrick.htm

2. What is a Brick ? http://enterprisearchitecture.nih.gov/ArchLib/Guide/WhatIsBrick.htm

3. How to Create and Publish a Technical Standard at NIH http://enterprisearchitecture.nih.gov/About/Approach/StandardsDevelopmentProcess.htm

4. NIHnet Services http://cit.nih.gov/NR/exeres/6A06415B-69B8-4226-888B-9C83DA1864F7

5. NIH Service Catelog for connectivity services http://cit.nih.gov/ProductsAndServices/ServiceCatalog/default.htm?Category=Connectivity+Services

6. NIHnet SLA agreement for network connectivity (Template) http://cit.nih.gov/NR/exeres/6A06415B-69B8-4226-888B-9C83DA1864F7

7. Internet2 Nationwide network http://www.internet2.edu/pubs/200904-Internet2CombinedInfrastructureTopology.pdf

8. To see a list of organizations participating in Internet2 and their associated network connector to Internet2 go to http://www.internet2.edu/network/participants/listParticipants.cfm

10 Contact

To contact the NIHRFC Editor, send an email message to EnterpriseArchitecture@mail.nih.gov

11 Security Considerations

All server implementations must include adequate security measures to ensure application and data integrity through enforcement of authentication and authorization, adequate physical security of hardware, network connectivity that complies with security regulations and guidelines, and ongoing cooperation and communication with the vendor to apply fixes to any security vulnerabilities that may become exposed in time.

12 Changes

Version	Date	Change	Authority	Author of Change
0.1	9/30/2009	Refresh of Brick		Helen Schmitz / Joe Klosky
0.2	10/5/2009	Small stylistic changes	NIHRFC0001	Anja Holovac/Kiley Ohlson – NIH OCITA
0.3	12/7/2009	Updated document based on comments		Joe Klosky
1.0	12/14/2009	ARB Approved		ARB
1.1	12/1/2010	Updated document to incorporate expanded use of DWDM at NIH.	N/A	Steve Thornton
1.2	3/9/2011	Editorial updates based on feedback during the NIH-wide review. There were no substantive comments.	N/A	Steve Thornton
2.0	3/22/2011	Approved by the ARB	ARB	Zahra Ashraf

13 Author's Address

Brett Moseley
NIH/CIT/DNST
10401 Fernwood Road, Room 1NE15
Bethesda, Maryland 20817
Phone: 301-402-2279
Email: Brett.Moseley@nih.gov

Steve Thornton
NIH/OD/OCIO/ITAO
10401 Fernwood Road, Room 3NW07
Bethesda, Maryland 20817
Phone: 301-594-4951
Email: steve.thornton@nih.gov