Mainstream Network Model

Guidelines to Upgrading Campus Networks

Version 2002
February 2002

an msi
Advanced Networking with Minority-Serving Institutions

Mainstream Network Model

Foreword

With guidance from Philip E. Long, Chief Information Officer at Yale University, more than 20 campus network specialists from 17 minority-serving institutions (MSIs) developed these guidelines. The group recognized that decision makers at many educational institutions realize the need to upgrade their campus networks but do not have the expertise and cannot afford consultants. These guidelines can assist networking personnel in making sound decisions about upgrading hardware, cables, and software through their own efforts, or by developing specifications and managing the work of contractors.

These networking specialists have participated in a four-year, $6 million grant from the National Science Foundation (NSF) to EDUCAUSE entitled "NSF Advanced Networking with Minority-Serving Institutions (AN-MSI)." Approximately 100 schools are partnering in AN-MSI, roughly equally divided into Hispanic-Serving Institutions (HSIs), Historically Black Colleges and Universities (HBCUs), and Tribal Colleges and Universities (TCUs). The project focuses on the following aspects of networking:

Executive Awareness — assisting campus decision makers in strategy and planning for effective installation, upgrading, and use of information technology

Resource Development — obtaining funding to help campuses afford the networking improvements identified by the project

Network Technology — improving the operation and support of campus networks through sharing expertise between schools and by partnering with industry

Internet Connectivity — initiating cooperative connectivity projects and innovative wireless and wired approaches to reaching both remote and urban campuses, resulting in greater bandwidth, better services, and reduced cost

Applications — promoting the use of the improved networks for high-performance research and educational purposes

Further information on AN-MSI is available at http://www.anmsi.org/.

While network specialists at MSIs prepared these guidelines primarily for use by MSIs, we encourage their use by any organization, educational or otherwise. We anticipate updating them periodically and publishing them in printed form and on the AN-MSI Web site. Inquiries and suggestions are most welcome, and can be made through the Web site or by addressing e-mail to info@anmsi.org.

David A. Staudt
AN-MSI Project Director
EDUCAUSE

AUTHORSHIP AND SOURCES

This document was conceived at a network workshop of the NSF AN-MSI grant Networking Committee on June 20th, 2000, led by Philip Long. He wrote this document based on notes of that meeting and additional material. It was subsequently iteratively reviewed with additional contributions by AN-MSI project participants, in particular the Networking Committee.

LEAD AND CONTRIBUTING AUTHORS AND REVIEWERS

Philip E. Long	Yale University
Al Anderson	Salish Kootenai College
Wendell Barbour	California State University–Bakersfield
Jack Barden	Turtle Mountain Community College
Tammy Belgarde	Turtle Mountain Community College
Laurie Burns	Internet2
Laura-Lee Davidson	Executive Leadership Foundation
Ricardo Diez	Interamerican University–Arecibo
Steve Dupuis	Salish Kootenai College
Art Gloster	Florida International University
Eric Harmon	Winston Salem University
John Hofmann	Bethune-Cookman College
John Hurley	Clark Atlanta University
Henry Ingle	University of Texas–El Paso
Ronnie Jefferson	Hampton University
Ron Langley	California State University–Bakersfield
Kelvin Lawrence	Sitting Bull College
Margaret Massey	Bethune-Cookman College
Tim McDonald	Oakwood College
Caitlin Myers	Northwest Indian College
Trent Myers	Northwest Indian College
Adebisi Oladipupo	Norfolk State University
Alex Ramirez	Hispanic Association of Colleges and Universities
John Smith	Langston University
Mark Trebian	Lac Courte Orielles Ojibwa College
Joyce Williams-Green	Winston Salem University

List of Acronyms

AN-MSI	Advanced Networking with Minority-Serving Institution
ATM	asynchronous transfer mode
CATV	cable TV
DHCP	dynamic host configuration protocol
DMZ	demilitarized zone
DNS	domain name service
ESSID	extended service set identifier
HBCUs	Historically Black Colleges and Universities
HSI	Hispanic-serving institution
IPSec	Internet security protocol
IPX	Internetwork packet exchange
ISDN	integrated services digital network
LAN	local area network
LDAP	lightweight directory access protocol
MSI	minority-serving institution
NIC	network interface card
NSF	National Science Foundation
OSI	open system interconnection
P2P	point-to-point
PSTN	public switched telephone network
SNMP	simple network management protocol
TCP/IP	transmission control protocol/Internet protocol
TCUs	tribal colleges and universities
UPS	uninterruptible power supply
VPN	virtual private network

1. Introduction

This document presents a "mainstream network model" aimed at a medium-sized college or university. It is intended to identify designs and issues for consideration by local planners when developing a specific network plan. The high-level model includes the following underlying goals for the network:

- *reliability* — the ability to deliver solid infrastructure to support critical services;
- *scalability* — the capability to expand to meet growth in usage;
- *full functionality* — the capacity to provide the full complement of network-based services needed by colleges and universities;
- *adaptability to future needs* — the potential for campuses to add significant new functions as they are identified;
- *continuous renewal* — the ability of routine life-cycle maintenance of the network to gracefully introduce continuing network advances, large and small; and
- *standards* — the guidelines used to manage the network at highest efficiency.

This model does not present adequate detail to serve as a plan; it provides a checklist of issues to consider and a set of "rules of thumb" to guide decisions that planners must make when developing a thorough campus network design. With a focus on principles and detailed specifications, planners should be able to scale this model to meet the needs of any campus system. References to additional details, standards documents, and much more can be found on the AN-MSI Network Model Web site at http://www.educause.edu/ir/library/pdf/EAF0101.pdf.

This document assumes familiarity with the network design principles outlined in P. E. Long's "Designing and Growing a Campus Network" (*EDUCAUSE Quarterly*, 23 (1), 2000: 40–45, 52). One of the critical issues identified there is the need for continuous renewal of networks. The specific technologies identified in this model when initially documented (Fall 2000) will age over time; the continuous renewal principle describes how an appropriately maintained network will continuously evolve and thereby renew its technology to remain up-to-date. Thus, this report does not target a particular time horizon, though it is safe to say that if not incremen-

tally revised, it will be largely obsolete by 2005.

A model like the one presented here addresses ideal situations (for example, designing a network for installation in a new building). In fact, most installations will be retrofits, with the network designer having to improvise to identify conduits or closet space, or take advantage of existing wiring that may not meet ideal standards. While the primary goal of this document is to identify a mainstream design point, it will also provide a few comments on retrofitting, including discussions of the potential and the challenges for various wireless options to meet particular needs. Regardless of any overall model, every network installation will require the detailed attention of a qualified network design team to determine the best design under the conditions that constrain particular installations.

After an overview (Section 2) a detailed discussion of a simplified set of network layers from the "bottom up" follows (Sections 3, 4, and 5). (Note that the layers discussed in this document are simplified; please refer to a variety of sources, such as http://www.rad.com/networks/1994/osi/intro.htm, for a detailed discussion of the formal open system interconnection (OSI) layers.) The final sections (6 and 7) discuss related issues, including the process of planning the network, the need for end-user support, and policies. In addition to the network model, considerable detail and design decisions are also illustrated in a set of companion profiles of institutional networks ranging across schools of various sizes, referred to here as appendices but available separately from the AN-MSI network model Web site.

This model is based on meeting and maintaining the current standard network practices as they change. This network model will efficiently support current network services for all campus needs, including academic and administrative applications such as standard Internet services, audio and video streaming, secure e-commerce applications, and so forth. This network model is not intended to support leading edge applications such as full-motion digital video; to do so would require adjustments to the network electronics and setup.

The described institution is a college with 1,000 students, 10 buildings, and a single campus. However, the model can be adjusted to fit smaller schools (for example, 500 students) and can easily be scaled to 25 buildings or more, or even to several campuses with up to 5,000 students. More complex installations will need more complex design adjustments. Scaling across schools of various sizes is illustrated in the companion profiles.

Institutional coordination is essential. Network planners need to coordinate with the local facilities department, data network staff, video staff, and others who will be building or supporting network related facilities or services. Equally important is communication with network planners. This includes not only existing network facilities such as wiring closets, but also new construction, routine or project renovations of spaces, and installation of sprinklers, elevators, or other apparently unrelated projects that might allow the installation of needed network pathways within or between buildings. Because network needs change quickly, it is important for network engineers to review architectural plans before final approval.

Balanced investment across campus for information technology is vital. Building a quality network is a critical — but not sufficient — piece of creating an overall campus information technology infrastructure. A high-speed connection to a five-year-old desktop computer is not optimal. Support and upgrades are as critical for end-user hardware and software as they are for the network.

To target the needs of the network planning audience, this document will focus on network issues. Most of the same principles and many of the same practices should apply across all campus information technology infrastructures.

2. Network Model Overview

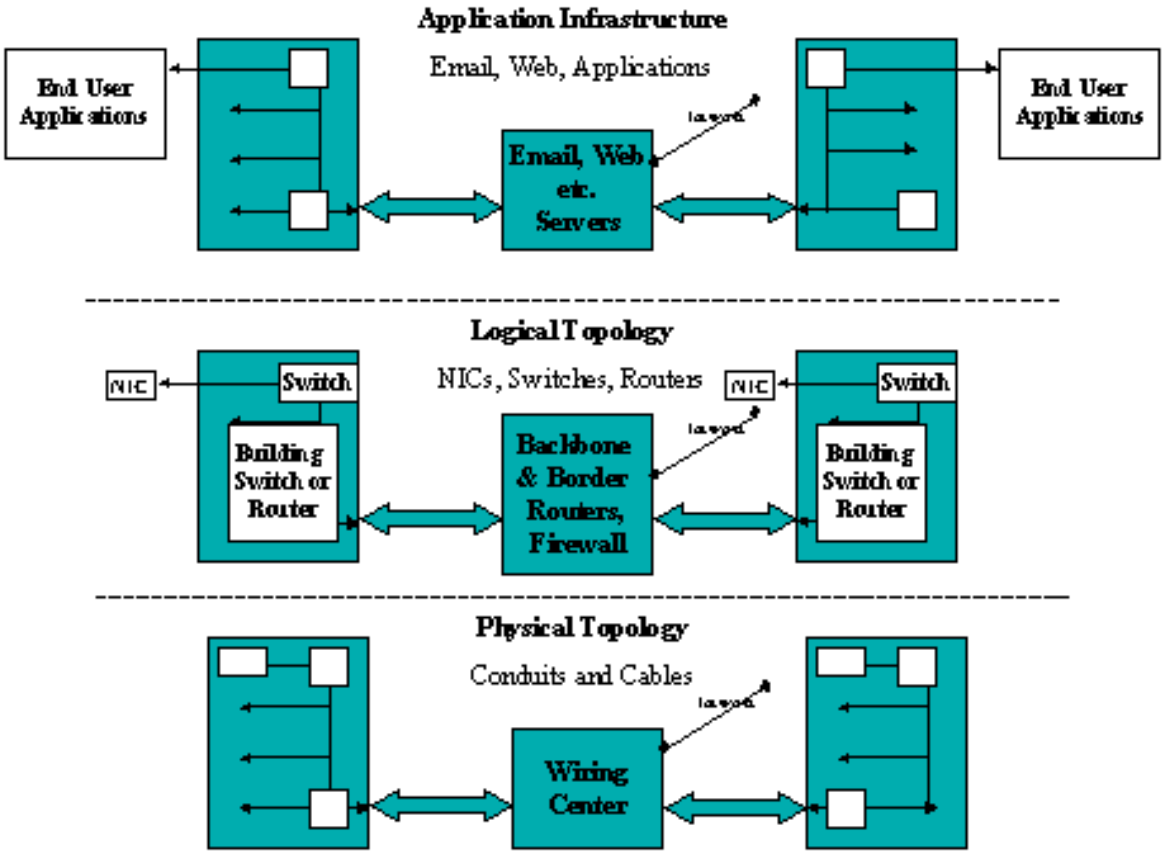
A campus network is constructed of three stacked layers: the physical topology, the logical topology, and the applications infrastructure. At the foundation of a network is the *physical topology* that conducts electrical or optical signals from one location to another. It consists of conduits, wiring closets, and related physical objects, including the cable, copper, or fiber that run through those conduits and closets. In the case of wireless connections, radio waves comprise the physical layer. A "star design," in which all building feeds connect to a common central location — the *wiring center* — provides significant advantages for managing networks, including diagnosing and repairing network problems. A star system does provide a single point of physical failure at the center of the star, but fully distributed or redundant wiring is a more expensive approach and is not currently common practice.

The *logical topology* includes the devices (hubs, routers, gateways, firewalls, and the network interface cards and the protocols they implement) that create the signals that travel over the physical layer. The protocols determine the formatting of messages by the signals, including network names and addresses, and the mode of information delivery.

The *applications infrastructure* turns messages into services. A variety of services can be constructed on a modern network, including voice communications, video distribution, and a number of data-based services. Core data application services include electronic mail, file directories, Web servers, and browsers.

Standard building blocks are used to construct and interconnect each layer. Thus, despite differences in each campus network, qualified network staff can readily understand and manage an existing network.

FIGURE 1.
A simplified diagram of a network's three layers. (Note, NIC represents the network interface card.)



These simplified network layers are illustrated in Figure 1. Details on the full seven-layer open system interconnection (OSI) network reference model are available on the ANMSI network model Web site.

3. The Physical Topology

The *physical topology* comprises the network cabling and the facilities in which it is located. Wiring closets represent points of network cable interconnection. Around the floor of a building, it is called a floor closet; for a building as a whole, it is a building distribution center; and for a campus it is referred to as the campus wiring center. *Pathway* represents the conduits, trays, hooks, surface molding, or other method of conveying network cable from one wiring closet to another. *Cabling* stands for the copper or fiber cables that carry network signals.

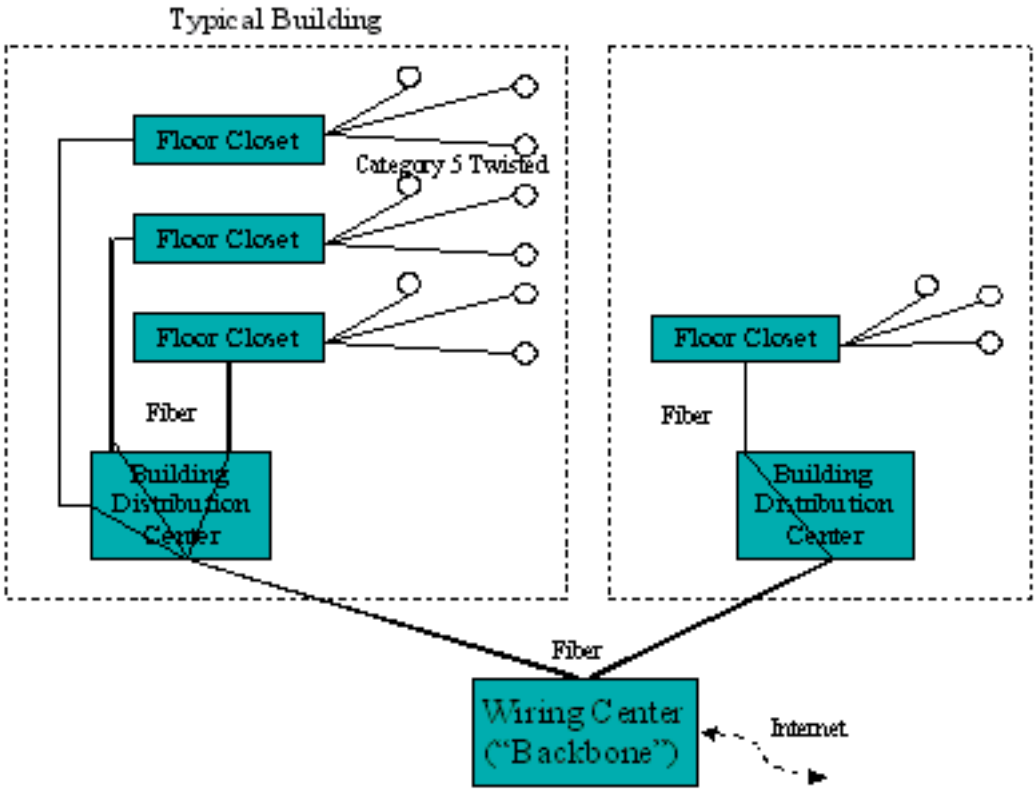
Figure 2 shows two buildings connected through a central wiring center. Additional buildings could connect to the wiring center in a similar fashion. The wiring center can be located in the best place to provide a central connection point, good security and environmental elements, adequate space, and so on. More complex campuses will have a small number of wiring centers that are interconnected, typically with redundant pathways.

SPECIAL CASES

Many campuses have old buildings that require creativity and compromise to wire. For example, some buildings may not have the space for wiring closets on each floor; the building conduits may run vertically instead of today's typical horizontal runs; or there may be no conduits available. Planners need to use a combination of options to meet the varying needs. For example,

- Surface molding and wiring trays can be used to add wire where no buried conduits exist.
- Wiring closets can be small, wall-mounted cabinets.

FIGURE 2.
Typical physical topology for two buildings connected through a central wiring center.



- New risers can be installed in elevators, through "stacked" closets, or in combination with plumbing or sprinkler systems.
- Fiber station wiring can be used to eliminate the need for wiring closets in a building due to much longer runs (about 3,000 feet or 1,000 meters).
- A wireless local area network (LAN) can be used to eliminate the need for a wired infrastructure (see discussion below).

WIRELESS OPTIONS

Wireless LAN technologies could eliminate the need for wired networking in the future. A number of large campuses in the United States have made major campus-wide deployments of IEEE Standard 802.11 family technologies (802.11b) to good effect. With the rapid evolution of this technology (802.11a is now starting to be deployed, with 802.11g around the corner), the optimal timing for investment is

difficult to determine. Wireless networks, unlike wired, will always be able to support mobility. There is an increasing need for network service access from various random remote places instead of from fixed points located on a campus network infrastructure. A future challenge is how to achieve the seamless integration of both wired and wireless networks in a manner that allows for a common framework of service delivery. More detailed discussions of wireless LAN options appear in "General Cabling Issues" below. Wireless solutions are also in use today to meet the specific need for trunk distribution. A more detailed discussion of wireless point-to-point (P2P) options is provided in "Trunk Pathway and Cabling."

TRUNK PATHWAY AND CABLING

Documentation of a network pathway is very important. Without documentation, a critical pathway may be lost. A master "copy of record" of all pathways must be maintained by the appropriate campus organization. Networking organizations should keep updated copies of the master to facilitate network planning. The organization that has stewardship of the master copy is responsible for keeping it current and distributing updates to whomever else on campus may have copies. The campus unit responsible for telecommunications will also need to track installed and assigned cabling (see the discussion under "General Cabling Issues" below).

Trunk pathway connects buildings via conduit or tunnels (preferably), air, or other modes. Conduits should be plastic (not metal) to avoid electrically connecting the buildings; hardened (protected by concrete) against "backhoe events"; and conform to other standard practices. Conduits should be a minimum of 4 inches from each building to the campus wiring center for data wiring and telephone. Cable TV (CATV) and utility wiring may flow over telephone or data cables, or require separate pathway depending on local design. A good practice is to double the capacity required for immediate needs, as the cost of conduit is small compared to the construction costs. Spare 4-inch conduit should be installed and documented any time there is digging between buildings. Telecommunications or network engineering should be informed any time the campus adds connections, sprinklers, elevators, and so forth. It is essential that conduits and building entrances are engineered and terminated properly for drainage purposes and so on.

Trunk data cabling is the complement to single-mode and multi-mode fiber between all buildings and the campus wiring center. The standard is 12 pairs, and the minimum is 8 pairs, depending on the communications applications to be supported (for example, data, video, or utility). In some cases wireless P2P solutions can be used, especially where fiber solutions cannot due to right-of-way problems, distance, property ownership, and legacy building issues. Wireless bridges should be configured to connect only to the access points to which their antennae point and have security set to a custom extended service set identifier (ESSID, a wireless security ID) or to include encryption of all traffic.

Trunk voice cabling is typically multi-pair voice cable; the size is based on building

phone capacity plus 100 percent spare between all buildings and the campus wiring center. Trunk cable TV cabling is designed by a CATV designer, typically one or more RG62 trunk CATV cables. Wireless trunk connections are P2P building connections. These connections are achieved using infrared, radio frequency, and microwave technology and are intended for areas not served by pathway.

WIRING CLOSET ISSUES

This section presents minimum standards and considerations; campus, local, or national codes may override these specifications. In general, closets require isolated ground power and ventilation. They must be lit, secure (locked), and permit access to telecom and network staff. Consider the need for uninterruptible power supply (UPS) protection. Closets are preferably dedicated to network use. Also, consider the future addition of utility connections and security and fire equipment.

A *floor closet* will be needed within 300 feet (100 meters) of every network drop if copper data cable is used. The closet size should be based on the potential number of drops served (account for future needs as well as immediate needs). For up to 24 network connections, a small 3-by-5-foot wall-mounted, locked cabinet could be used. For more than 24 network connections, a standard, full-sized closet could be used. In new buildings or renovations, large closets should be built. As noted above, creative compromise in standard approaches may be needed with special conditions such as older buildings.

Building distribution centers need a full-sized closet adequate to receive riser and trunk pathway. The closet should be designed to hold active electronics and to facilitate cross-connect wiring. *Campus wiring centers* will contain substantial network electronics and other equipment. Characteristics are discussed in detail under "Standard Basic Network Design."

PATHWAY ISSUES

The best hedge against future need is to create empty pathway into which cable can be inexpensively pulled. However, empty pathway bears cost, both to construct and to maintain. Because it can be difficult or impossible to add cable to more than half-full conduits, replacing cable in conduits can often require removing the existing cable and drawing in the new cable. Pathway has a life cycle and must be considered for renewal, usually on a 25-year or a per-building renovation cycle.

Station pathway connects individual network wall jacks to floor wiring closets. The station pathway capacity equals 1-to-1.5-inch conduit equivalent capacity; the actual size depends on the wiring plan. Standard design calls for two network drops per person capacity in each room. A minimum design is one drop per person. In most cases two drops can be served by a single conduit or equivalent pathway (such as back-to-back boxes in a single wall serving two rooms).

Riser pathway connects floor wiring closets to building distribution closets. A separate riser is needed for each floor wiring closet. Standard installation requires one 4-inch con-

duit equivalent. The need for larger or smaller conduits depends on the number of drops and the type of cabling used. CATV distribution generally requires larger risers. Standard cabling practice (see the discussion below) uses fiber to the floor. Copper wire to the building distribution center may require larger risers.

GENERAL CABLING ISSUES

Documentation of all installed and assigned cabling is essential. Without the appropriate documentation, existing connections will be indiscriminately disconnected and new connections will take longer to install. Documentation should be created and recorded upon installation and maintained with moves, adds, and changes.

Station cabling connects a wall jack to the first active network electronic component.

Station data cabling is typically four pairs of Category 5E twisted pair copper cables from the wall jack to the floor wiring closet. Fiber cable to the desktop is an alternative, but compared to copper, fiber tends to cost more, has fewer connect/disconnect cycles, and takes more space in wall closets for cross-connects. Characteristically, connections require fiber to 100baseT converters. Fiber is normally used only where floor wiring closets are not easily available within 300 feet (100 meters) or for very high-speed service. Most network planners expect that fiber station cabling will become a standard as fiber management and equipment (termination, fiber switches) mature and become more cost efficient.

Station voice cabling typically uses four pairs of Category 5E twisted pair copper cables from the wall jack to the floor wiring closet. There it cross-connects to voice trunk cable all the way to the campus telephone switch. Category 5E cable serves well for voice and provides flexibility against possible failure or extra demand on data cable.

Station CATV video cabling typically requires RG62 coaxial cable from the wall jack to the CATV hub, usually at the building distribution center.

Station utility cabling normally requires four pairs of Category 5E twisted pair copper cables from the wall jack to the floor wiring closet, where it will cross-connect to a dedicated utility network or link to the campus data network.

A typical wall jack "drop" provides a full complement of cabling for all supported services. It requires four pairs of Category 5E data, four pairs of Category 5E voice plus coaxial cable, and/or an additional four pairs of Category 5E utility wiring. High-performance or specialty drops may include two fiber pairs to the wall jack. CATV coaxial cable will require a qualified CATV engineer to lay out the local design. The wall jack should use national-standard connectors. The requirements include RJ45 for data, RJ11 for voice, F connector for cable, and RJ-12 for digital voice if the local phone system is digital.

WIRELESS LAN OPTIONS

Wireless LANs allow the connection of individual computers to a LAN (Ethernet) using

IEEE 802.11 at 2.4 GHz (11.b, up to 11 megabytes; or 11.g, emerging) or 5 GHz (11.a, up to 54 Mb) wireless standards. Wireless base stations are hubs, thus, the total bandwidth (typically 11 or 54 Mb) is shared by all stations communicating with that hub. These base stations are installed at various locations to provide appropriate coverage. In order to achieve roaming (movement from one base station's coverage to another while maintaining a connection), base stations must be on a single subnetwork. As stated in the 1997 LucentWave LAN document, it requires significant engineering to provide consistent coverage, since metal, concrete, and paper absorb the 2.4 and 5 GHz spectrum. Prior to planning a wireless LAN, a network engineer should determine dead spots and areas of high absorption or blockage.

Current products raise security concerns, since client access can be unauthenticated and unencrypted, and signals can be obtained outside buildings, in hallways, and so on. The standard wireless encryption protocol for LANs is known to be compromised (see Airsnort at http://airsnort.sourceforge.net/). Concerns can be addressed by use of secure sockets layer (SSL) or virtual private network (VPN) protected session connections.

Physical security of the access points, where the wireless LAN "meets" the wired network, is an issue because wireless receivers can be used in homes to provide wireless access to a cable modem or digital subscriber line (DSL) Internet connection. Consider placing the access points in a secure location and placing an external antenna in the area where wireless coverage is desired. External antennas provide greater reception and transmission strength, and should be considered for any installation where there will be multiple users. A remote-access, dial-in, user-service server with proxy service to lightweight directory access protocol (LDAP), NT domains, and Novell directories can be used with high-end access points to provide authentication for wireless users.

A wireless LAN is usually deployed to meet specific needs (see the discussion in "Introduction"). It offers an excellent solution for particular environments and applications, such as historic buildings, remote locations, networked classrooms, and open areas. It serves as a substitute for a wired infrastructure where building infrastructure limits the ability to provide wired connection and usage.

4. The Logical Topology

The logical topology (see Figure 3) includes the network electronics and protocols, plus Internet connections, network security, and network management. This section discusses each element in turn.

NETWORK ELECTRONICS

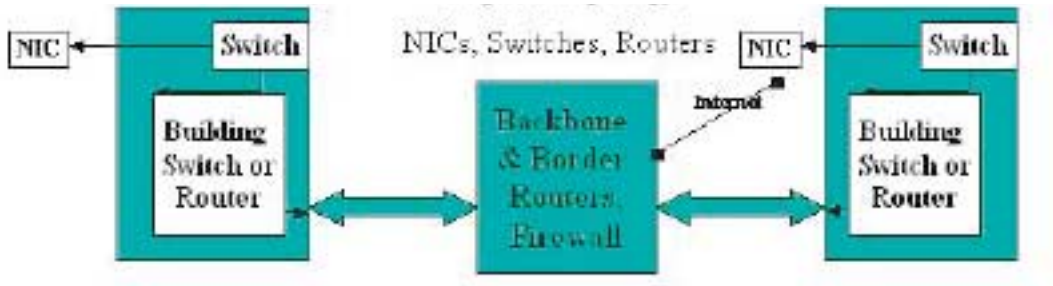
Because of its commercial success, Ethernet network technology — including substantial and continuing improvements in capacity and management options (The Commodity Goods Principle) — is used on most campuses. In the early 1990s limitations of the initial Ethernet design began to emerge and pose problems for network growth. To overcome these limitations, vendors developed a variety of other options. The most successful of these is *asynchronous transfer mode* (ATM). ATM offers several advantages over Ethernet, most importantly, guaranteed delivery of performance-sensitive data streams such as video. However, in 2001 an ATM network cost approximately 30 percent more than Ethernet when considering equipment and management costs for equivalent networks The physical topology design and wiring is the same for Ethernet and for ATM. Several schools have migrated to ATM and back to Ethernet, demonstrating this fact. A few schools run both ATM and Ethernet networks, allowing them to deliver the best services offered by both protocols.

NETWORK PROTOCOLS

At the network protocol level, in addition to transmission control protocol/Internet protocol (TCP/IP), some existing campus networks may be routing Novell Internetwork Packet

FIGURE 3.

Logical topology includes the electronic components that send signals via the cables and the protocols that turn those signals into messages. (Note, NIC represents the network interface card.)



Exchange (IPX) and/or AppleTalk protocols. Because these protocols are used less frequently, newer routers have trouble supporting and managing them, and staff who know these protocols are becoming scarce. Most mainstream campus network designs are phasing out such remaining legacy protocols in favor of TCP/IP, since both Novell and Apple networking services can now operate with full functionality using TCP/IP.

Details on setting up a system for network protocols follow.

Standard Basic Network Design

Cascading switches connected within a building concentrate to a single building feed, and each building feed connects to the campus wiring center. The wiring center contains a single switch or router that functions as the campus backbone. This provides the least expensive, and highly reliable, configuration widely used at campuses in 2001. A key disadvantage with this design is the lack of redundancy for backbone electronics and cable. This can be remedied by sophisticated design that involves multiple campus wiring centers with redundant core pathway.

Building Electronics

Cascading switches connected within a building concentrate to a single building feed. Consider local UPS, as discussed in "Wiring Closet Issues."

Campus Wiring Center

The campus wiring center is often located in the campus telephone or data center. It contains the connections to all buildings on campus and to the off-campus world. It must be secure and have built-in fire suppression. It must also incorporate UPS or some form of

backup power, depending on the local power company profile. Appropriately designed heating, ventilation, and air conditioning is essential. The layout should be designed for easy cable management. Consider cable, space, and operations management for

- wiring closets,
- the campus wiring center,
- machine rooms and server farms, and
- cable management and server set up.

The main campus wiring center equipment consists of a core router or switch — the collapsed backbone. It is the backplane of a high-speed router and has some efficiency advantages over an actual network backbone, similar to those that switches have over hubs. First, the core switch or router is nonblocking, thus it provides a very high-speed cross-connect between the building feeds. Second, collisions rarely occur, resulting in almost 100 percent full-duplex rated throughput. The typical standard configuration specs include a one-gigabit nonblocking backplane and a layer 3 switch frequently used in current configurations.

Other solutions are possible. For example, a router with layer 2 equipment is feasible. A consultant may be necessary to help configure this setup. The cost is approximately $15,000 to $100,000, depending on the scale and performance needed. One advantage is that this setup is easily upgraded by replacement during a normal equipment life cycle. However, it is necessary to provide a redundant power supply and possibly also a spare for the entire box.

All of the interface cards and all of the active components will need a maintenance plan. The options include

- On-site vendor maintenance (this can be expensive and typically slow)
- Depot maintenance (air-ship broken parts for 24-hour turnaround)
- Local spares with depot maintenance (staff must install)
- Warm spares (powered on nearby equipment, which has to be manually configured to become active) with depot maintenance
- Hot spares, or dynamic reconfiguration upon detection of a problem (this is costly and usually complex to configure)

If local resources allow, the most cost effective and responsive solution is generally local or warm spares with depot maintenance. All core equipment should have a spam port that lets network staff connect a protocol analyzer to track all traffic for troubleshooting purposes. The same vendor should be used for all core campus network components unless there is a vital business reason not to. Using a single vendor and equipment interface means easier staff training, especially for small campuses.

Subnet Architecture

A small campus network generally requires only a few subnets. Subnets are typically used to isolate servers. For example, a computer cluster and associated server may be isolated on a subnet to keep the traffic between them

from having to pass through the backbone. Or, a server farm may be isolated within a subnet protected behind a firewall or router filter.

Core Network Services

Details on configuration of core network services exceed the scope of this document. Three services should either be required or considered: domain name service (DNS), dynamic host configuration protocol (DHCP), and virtual private network (VPN) or Internet Security Protocol (IPSec). The DNS manages the translation of Internet domain addresses of the form (xxx.school.edu) into IP addresses (for example, 130.131.1.1). It must be operational for the network to correctly identify computers. Most campuses provide at least one, sometimes several, DNS servers, distributed across campus to provide load balancing as well as redundancy. The DHCP allows dynamic assignment of IP addresses to network clients. The VPN, or IPsec, provides the ability to create an encrypted and secure connection to the campus network from a remote client across an unsecured Internet location (say, from off-campus).

INTERNET CONNECTION

Bandwidth is a primary consideration in connecting to the Internet. Network management allows the monitoring of Internet connection use, so bandwidth can be adjusted according to demand. Costs vary widely based on geographical location and local provider option. For information on wireless Internet, see "Profile of Salish Kootenai College Wireless LAN," Appendix 1.

INTERNET2

Internet2 is a partnership among institutions of higher education, the government, and industry whose mission is to build the Internet of the future. One of its major goals is the ongoing transfer of new technologies and capabilities to global production Internet. Internet2 activities in advanced applications, middleware, and network services are carried out by representatives from Internet2. Many of these activities focus on scaling and implementing various solutions for the research and education community as a whole. For example, work is under way on common directory schemas that will ultimately allow universities across the country to share resources and collaborate in more secure ways of authentication.

Other projects focus on deployment of multicast and other advanced network services in campus, regional, and national networks that connect Internet2 members. These services will eventually expand into the rest of the Internet. Work in digital video services will help support the growing need to provide distance education.

In the autumn of 2000, Internet2 launched an End-to-End Performance Initiative that will produce a number of information resources and tools enabling local technical and support staff to serve their campuses more effectively. Internet2 has also revised the Conditions of Use for Abilene, its high-performance backbone network, to expand access for state net-

works of educational institutions and organizations traditionally not members of the Internet2 community.

NETWORK SECURITY STRATEGIES

Security checkpoints are usually located in each application that connects to the network. However, the network can be configured in a way to minimize known security risks using different levels of access exclusion. Figure 4 illustrates several basic security components.

Network security strategy options include a proxy service, which allows end users from the Internet to connect to a local sever for authentication before receiving services from the local network. This proves particularly useful in providing end-user access to restricted services such as electronic library journals or in providing relay access to any services protected behind a firewall (discussion below). Another strategy employs a VPN server that allows connections from the Internet via an encrypted "tunnel" from the end-user's client computer directly into the VPN server. It protects traffic in that tunnel from "sniffing" and does not permit the end user full access to the campus network if the user is not local.

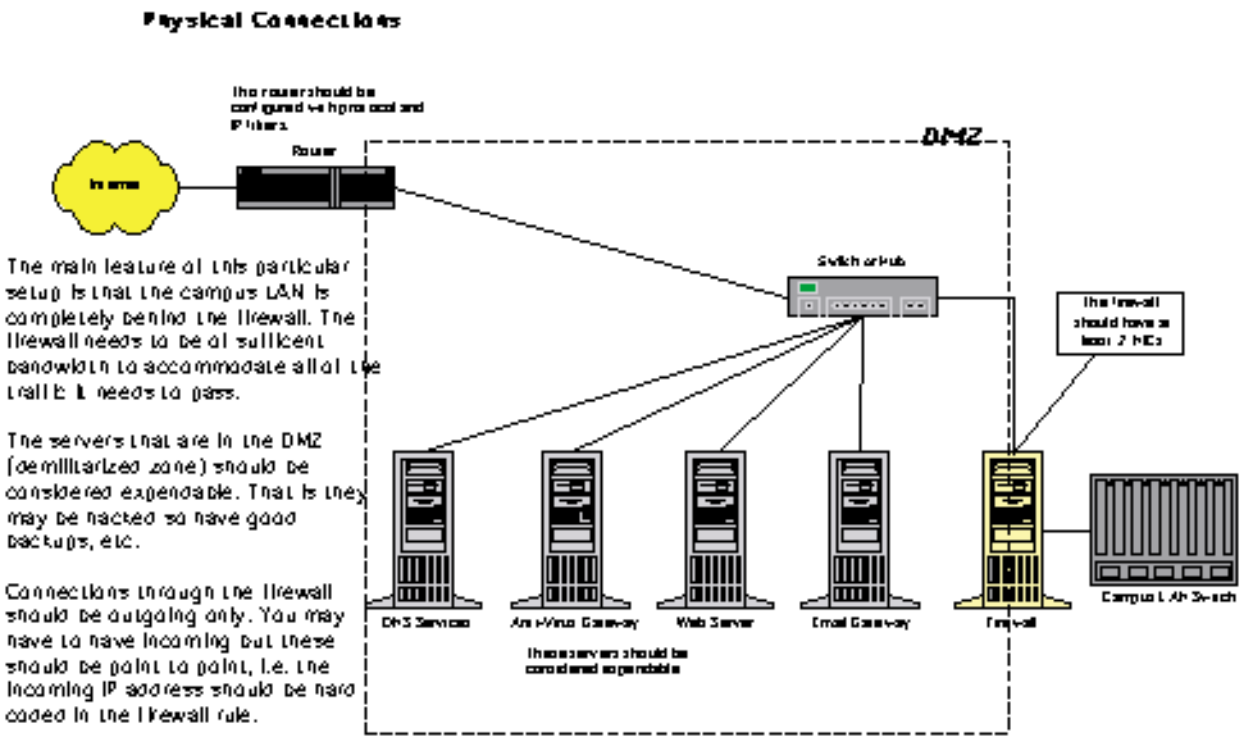
Even though nomenclature is not standardized, several common terms are used to describe routers that restrict the free flow of IP messages based on various conditions. A *border router* provides the point of connection to the Internet. It is typically used to deliver a variety of high-level coarse-grained network controls or *filters*, such as prohibition of certain IP protocols (such as Network File Service (NFS) or NetBios) or access to particular service ports (for example, unsecured telnet port ##). Fine-grained filtering, generally called *firewalling*, usually gives the ability to restrict access to particular applications, specify access lists, or provide other control points. For example, a firewall (router) could be programmed to restrict student services access to a specific set of campus computers, end users, or transactions of a particular format. While a firewall could provide substantial protection to applications, firewall programming is complex and expensive, and requires frequent maintenance and continuous management.

Firewall installations are often accompanied by a *demilitarized zone* (DMZ). This is the section of the network outside of the firewall that is more open to Internet access. Campuses that wish to provide maximum protection of applications will usually put them behind a firewall and install a proxy server in the DMZ. End users must then connect to the proxy server; only if they are accepted will they be allowed to access the protected applications. Even if the proxy server is compromised, other computers behind the firewall can be reached only through permitted transaction protocols.

While the firewall provides superior security when properly installed and configured, this can be difficult to achieve. Current mainstream practice generally takes full advantage of coarse-grained filtering at border routers. It does not employ firewall filtering at the application level, although this practice varies widely and evolves as new products improve.

A key security consideration for campuses is whether to exclude all activities other than

FIGURE 4.
A small-to-mid-sized LAN Internet connection illustrating good security practice.



the identified acceptable uses or to include all activities other than identified unacceptable uses. Corporations typically take the former approach, which provides high security but low flexibility. Increasingly, Internet service providers (ISPs) offer Internet connections using this approach, relieving the campus IT staff of installing and managing a border router or firewall. Historically, campuses have taken the latter approach, allowing all uses that have not been specifically shown to pose a threat. Because threats do arise on a regular basis, this approach generally requires local use and active management of a border router.

Network staff, or security staff in larger organizations, may also run security-scanning programs that will probe networked computers for known security risks. While network staff may manage such programs, the responsibility of fixing security weaknesses in applications systems usually lies with the system administrators for those systems.

Terry Gray at the University of Washington has published an excellent general discussion on security issues (http://staff.washington.edu/gray/papers/). His papers may be accessed from the AN-MSI Network Model Web site. In addition, EDUCAUSE has a task force

on security that is likely to develop more detailed explanations and recommendations for standard security practice (see http://www.educause.edu/security/). Figure 4 illustrates good security practice in a small-to-mid-sized campus network.

NETWORK MANAGEMENT

Network management includes the elements of documentation, monitoring, and growth or change.

Documentation

Several aspects of a network should be documented, including the logical maps and the physical maps. The logical map shows connections of the network devices, the network architecture (such as star versus ring), and the network's security structure. The physical map indicates the locations and capacities of lines as well as the locations of network devices and networked computers. Also beneficial is a network structure description detailing how the network is set up (a summary of the maps). The network inventory should also be documented. Sufficient documentation includes a list of hardware with configurations, original purchase date and price, and projected life cycle; a list of operating system (OS) versions and standards on each device; and application versions, standards, and maintenance levels. Additional elements that should be documented are network structure guidelines, security guidelines (the who, what, and why of the network's security), and network configuration (device configuration and configuration files, particular user names and passwords, network address structure, and so forth).

Monitoring

A network needs several different levels of monitoring. *Proactive monitoring* involves "work" by the network administrator, such as watching logs (machine error logs, network error logs, and hard-drive space). Some of this work can be automated by setting limit alarms that could e-mail information to an administrator. Reactive monitoring involves alarms that can be set to trigger when certain events occur (simple network management protocol (SNMP), remote monitoring, NT event logs, Unix log watchers, and so on). It could include programs that monitor the overall condition of the network, some of which provide both proactive and reactive monitoring. These applications include HP OpenView, BigBrother, and Multi Router Traffic Grapher.

Growth and Change

The growth of and changes in a network should be planned. This requires planning for growth of the number of network nodes, network bandwidth, or the physical campus. Planning for growth can be best managed by using baseline measurements and historical trends to project future needs. In addition, disaster planning that includes network, computer, and facility disasters as well as backup and recovery plans should be in place.

5. The Applications Infrastructure

The AN-MSI project will not address applications issues in detail. Still, they should be discussed, since the purpose of a network is the successful delivery of applications. Figure 5 indicates the core network applications, which include

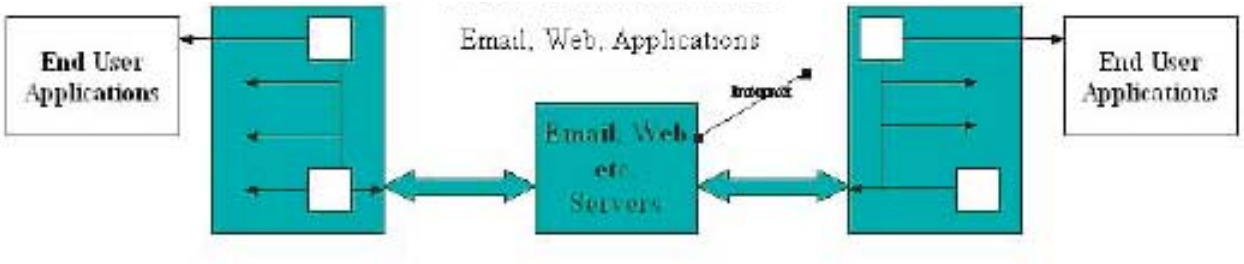
- Web servers,
- e-mail service,
- directories and enterprise back-up of file systems,
- file sharing,
- NetNews,
- Telnet,
- software distribution, and
- administrative applications, such as student services, human resources, general ledger; accounts payable, and accounts receivable.

Infrastructure issues common to all of these elements include network identification and authentication, application authorization, and security. Most schools adopt a network operating system environment to manage these issues. Typical environments include a locally managed set of either open source services such as Kerberos and LDAP, or vendor-provided environments such as Microsoft's NT or Windows 2000 domains with active directory and Novell services (running over IP).

SPECIALTY APPLICATIONS

Two types of video conferencing are available. Standard analog video conferencing requires H.320 — integrated services digital network (ISDN) — and an entire drop at the office. A cross-connection to the telephone switch and an ISDN video conferencing consultation are also required. IP-based video conferencing (H.323) operates through IP networks and

FIGURE 5.
The application infrastructure illustrating the core network applications.



works acceptably; however, it requires substantial spare bandwidth. Each classroom needs audio-visual wiring infrastructure within it, as well as appropriate voice/data/video (V/D/V) drops. A wireless setup is also an option (see the profile of a wireless classroom in Appendix 1). Laboratories used for teaching, training, research, or multimedia require additional drops and equipment for projection ability. Full-motion video distribution requires a local design. The network infrastructure requirements for distance learning vary, and high-performance computing should be considered.

EMERGING TECHNOLOGIES

Taking advantage of emerging technologies requires planners to consider the infrastructure, power supply, management, and quality of service issues involved as they begin an implementation.

IP Telephony

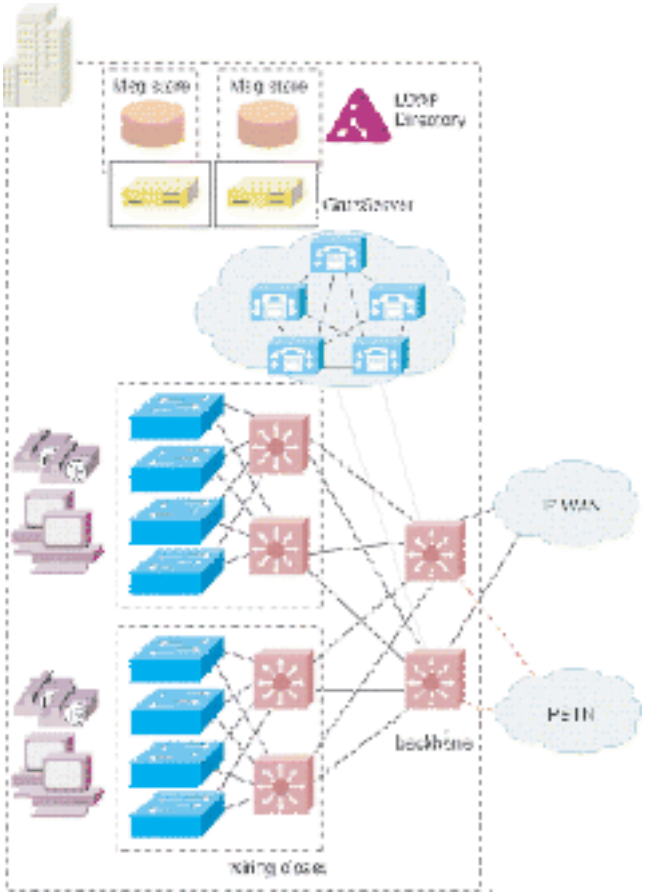
To successfully deploy an IP telephony solution requires considering the LAN infrastructure before adding voice to the network. The data network must be configured properly. The size of the network determines the components and platforms that can be used and the scalability, availability, and functionality of the network. A general IP telephony network appears in Figure 6.

One of the most important requirements of the IP telephony infrastructure is reliable power, usually achieved with a UPS.

Some common strategies for using UPS follow:

- *The wiring closet switches and downstream data center are backed up using UPS.* While this strategy ensures that power to the phones is maintained, power to wall-powered devices such as PCs can still fail.

FIGURE 6.
General IP telephony network, where PSTN is public switched telephone network, and IP WAN is Internet protocol wide-area network.



- *The whole building is backed up using UPS*. This protects all equipment from power failures.
- *A separate generator for power is provided and used as backup*. In this case UPS might still need to be added because there is usually a lag for the generator to produce enough power. The advantage of this strategy is that less battery time is needed for each UPS. In addition, a UPS can be configured with options such as SNMP management, remote monitoring, and alarm reporting.

Building an end-to-end IP telephony system requires an IP infrastructure based on layer 2 and layer 3 switches and routers with switched connections to the desktop.

IP Addressing and Management

Telecom networks, data networks, and servers are currently managed independently. Administrators can differentiate service issues fairly easily. Operational processes such as performance, capacity, provisioning, fault management, and inventory management are classically managed by separate groups without much interaction. Each group may also have its own independent support plan with unique goals or service requirements that meet existing needs. The IP telephony solution usually requires a new support model.

Network or IP Telephony Technology, Resiliency, and Configuration

Network technology, resiliency, and configuration constraints for IP telephony can be defined as any limitation or risk associated with the current technology, hardware, links, design, or configuration. Technology limitations cover any constraint posed by the technology. For example, no current technology allows subsecond convergence times in redundant network environments, which are critical for sustaining the quality of IP telephony voice across the network. Another limitation is the speed at which data can traverse terrestrial links, which is approximately 100 miles per millisecond. This is an important consideration in the deployment of wide-area network models (WANs).

Network hardware resiliency risk investigations should concentrate on hardware topology, hierarchy, modularity, redundancy, and mean time between failure along defined paths in the network. Network link constraints should focus on network links and carrier connectivity for enterprise organizations. Link constraints may include link redundancy and diversity, media limitations, wiring infrastructure, local loop connectivity, and long-distance connectivity.

Design constraints relate to the physical or logical design of the network and include everything from available space for equipment to scalability of the routing protocol implementation. All protocol and media designs should be taken into consideration in relation to configuration, availability, scalability, performance, and capacity.

Quality of Service

In a converged environment, all traffic travels through a single transport infrastructure, yet all traffic types are not the same. Data are bursty, loss-intolerant, and latency insensitive. Voice, on the other hand, is nonbursty, has some tolerance to loss, but is latency sensitive. Providing the required quality of service for each of these traffic types is challenging.

6. Network Planning and Governance

Campus voice, data, and video networks are increasingly important in providing communications infrastructure to the whole enterprise. The importance of voice services (telephony) is well understood. Data networks are increasingly subject to the same level of expectations for responsiveness, availability, and recovery as voice networks have been for many years.

This critical network infrastructure requires large and thoughtful investments by the campus, and these investments are typically increasing. Network planning and governance issues are critical in creating and maintaining a campus consensus on appropriate network services, capacity, and reliability. A consensus instigates the commitment to funding needed to meet those goals. This section outlines key issues in good-quality network planning and governance.

NETWORK PLANNING CHECKLIST

The planning process needs to include a communications plan to develop campus buy-in. The following are standard steps for planning and implementing a network:

- assess the current conditions,
- compare the conditions to the model,
- identify any gaps,
- set priorities and sequencing, and
- build a plan, including design, layout,

equipment, and ongoing resources (budget and staff).

WHO PLANS AND GOVERNS?

Network staff and collaborators usually do the actual planning work. A campus committee usually receives, reviews, and recommends the plan. It is recommended that the committee consist of the following individuals:

- CIO or lead IT officer (and network staff, depending on local practice)
- Librarian
- Faculty representatives
- Student representatives
- Administration
- Other user representatives
- Others, depending on school practice

HOW OFTEN TO PLAN

Network needs and technologies change constantly, so planning has to be ongoing. It is prudent to issue an annual updated plan with major revisions based on particular local issues.

BASELINE INFORMATION FOR PLANNING

Network staff can obtain several pieces of information necessary for planning, including the number of existing network connections, currently connected buildings, and currently connected campuses. Traffic patterns and bottlenecks must be identified. An inventory and the documentation of the existing network are essential for assessing current and future needs for staff and facilities, such as machine rooms for servers and wiring closets. Additionally, it is necessary to know what the existing network services are, such as

- data (IP, legacy protocols),
- video over IP (streaming or H.323 video conferencing),
- CATV,
- video distribution (P2P),
- voice, and
- utility service (for example, security and fire suppression).

Internet service provider options and capacity cost must be known, and it is prudent to incorporate some way to track the actual cost of building and maintaining the network.

ASSESS NEEDS AND RESOURCES

The staff and governance body should take into account the campus's needs and resources. New applications, such as distance learning, streaming media, and digital video conferencing, will require support. New programs (for example, a new engineering degree) will begin, the number of students will grow, and students will increasingly use the services offered. Each resource necessary for creating and maintaining the network, including the budget, the existing infrastructure, and the management capacity, needs assessment.

COMMON PLANNING TRADE-OFFS

There are common planning trade-offs to consider. An increased capacity in the number of users or bandwidth requires more resources. Improved reliability and redundancy require additional resources and make the network more complex. Improved security generally restricts service availability and also requires additional resources. The planning committee will need to set priorities regarding budget and reliability and security. For example, if budget is the highest priority, reliability and security standards will be set within the budget. Alternatively, if reliability and security standards are key priorities, funding may need to be found to achieve them.

WRITING A REQUEST FOR PROPOSAL

Requests for proposals (RFPs) provide a common approach for securing vendor bids on significant network technology or services. See Appendix 3 for a discussion of common practice for RFPs.

POLICY AND LEGAL ISSUES

Each campus should have a published network policy that addresses "standard" issues, such as security breaches, identity theft, excessive use of bandwidth, copyright, intellectual property, and so on. The staff and governance body should take responsibility for this. Refer to the EDUCAUSE policy Web site for sample policies and further discussion (http://www.educause.edu/policy/policy.html).

FUNDING STRATEGIES

Central funding is probably the best solution for small, nonresearch institutions. Budget plans must take into consideration the rapid and continuing growth in network resources, since normal budget growth cannot usually match network needs. Charging users is typically used only by research schools and can create a barrier to network use. Partnerships with vendors and schools, both nationally and locally, can be an effective funding strategy. A student technology fee should be supplemental and directly fund IT services. Keep in mind that this tactic may raise student expectations for more services. Grants are a critical piece of any funding strategy, including non-IT grants that have a technology component for equipment, consultation, and support. Schools should strive to develop a technology component within every grant.

MAINTENANCE AND SUPPORT

The budget must address several items:

1. Network equipment's three-to-five-year life cycle.
2. Maintenance contracts, vital to smooth operation.
3. Adequate resources, including staff salaries, training, and equipment.
4. Standard test equipment, including cable testers and a sniffer or protocol analyzer.

5. Network technology's always evolving nature, which can be costly to keep up with.

NETWORK STAFFING

To meet essential functions, the size of the staff must be scaled to the size and complexity of the network, allowing for a minimum of two people. The appropriate number of staff members must include personnel with all required skills and provide adequate redundancies to cover vacations and leaves. Where possible there needs to be flexibility for unforeseen job changes. Staffing depends on the particular support model: 100 percent local support, collegial support (remote technical support), or outsourced support. Outsourcing is widely discussed in other sources. However, there are some rules of thumb for outsourcing network services:

- Consider outsourcing only commodity services.
- Do not outsource any service that is core to program activities and still rapidly developing or changing. Data networking has not historically been a good candidate for outsourcing based on this rule, while traditional telephone service might have been.
- An outsource is only as good as local management. In other words, outsourcing must not mean an end to campus-driven planning.

COMMUNICATION STRATEGY

A coherent strategy is essential for communicating to end users which services are offered and what expectations they should have of those services. The following should be considered when forming a strategy:

- What will best serve your needs; data, voice and video, video conferencing, video streaming, Web service, etc.
- What service to expect (e.g., one 10 or 100 Mb switched for every desk)
- How to ask for service, report trouble, complain
- How the network is governed and how to influence policy
- Usually, particular services are defined by service level agreements (SLAs; see Appendix 2 for a sample)

7. Conclusion

Other critical success factors influence the results achieved. Staff must have interpersonal skills, for example. Staff ability and interest in customer service, not just technology, is critical to a successful network. Also, successful end-user support strategy is not, strictly speaking, part of the network, yet is essential to success.

Campuses have been working with voice, data, and video networks for many years, and some standard practices have emerged. This network model document attempts to identify and to provide ideas and basic checklists for building a campus network. Those of us who put this document together learned a lot in the process, but each of us has to adapt and verify these ideas as we apply them to our particular campuses. We hope you will find this useful when developing or reviewing your campus network and encourage you to visit the AN-MSI Web site (http://www.anmsi.org/) to see related resources or to offer your suggestions to improve this network model.

Resources

GRANT OPPORTUNITY REFERENCES

Richard M. Eckstein, ed., *Directory of Computer and High Technology Grants, 4th Edition* (Loxahatchee, FL: Research Grant Guides); ISBN 0-945078-13-7.

Arlene Krebs, ed., *The Distance Learning Funding Sourcebook: A Guide To Foundation, Corporate, and Government Support for Telecommunications and the New Media* (Dubuque, Iowa: Kendall/Hunt Publishing Company, 1998); ISBN 0-7872-0813-2.

WEB SITES

http://www.educause.edu/ir/library/pdf/EAF0101.pdf presents details, standards documents, and so forth, at the AN-MSI Network Model Web site.

http://www.anmsi.org/ offers information on AN-MSI.

http://www.rad.com/networks/1994/osi/intro.htm gives a detailed discussion of the formal OSI layers.

http://airsnort.sourceforge.net/ provides information regarding the standard wireless encryption protocol.

http://www.educause.edu/security/ offers detailed explanations and recommendations for standard security practice.

http://tii.calstate.edu/ is the generic link to a number of Technology Infrastructure Initiative (TII) documents.

http://tii.calstate.edu/StandardsandGuidelines/TIPGuidelines/TIPGuidelines.shtml is the specific link to the January 2002 draft of the Telecommunications Infrastructure Planning (TIP) Guidelines.

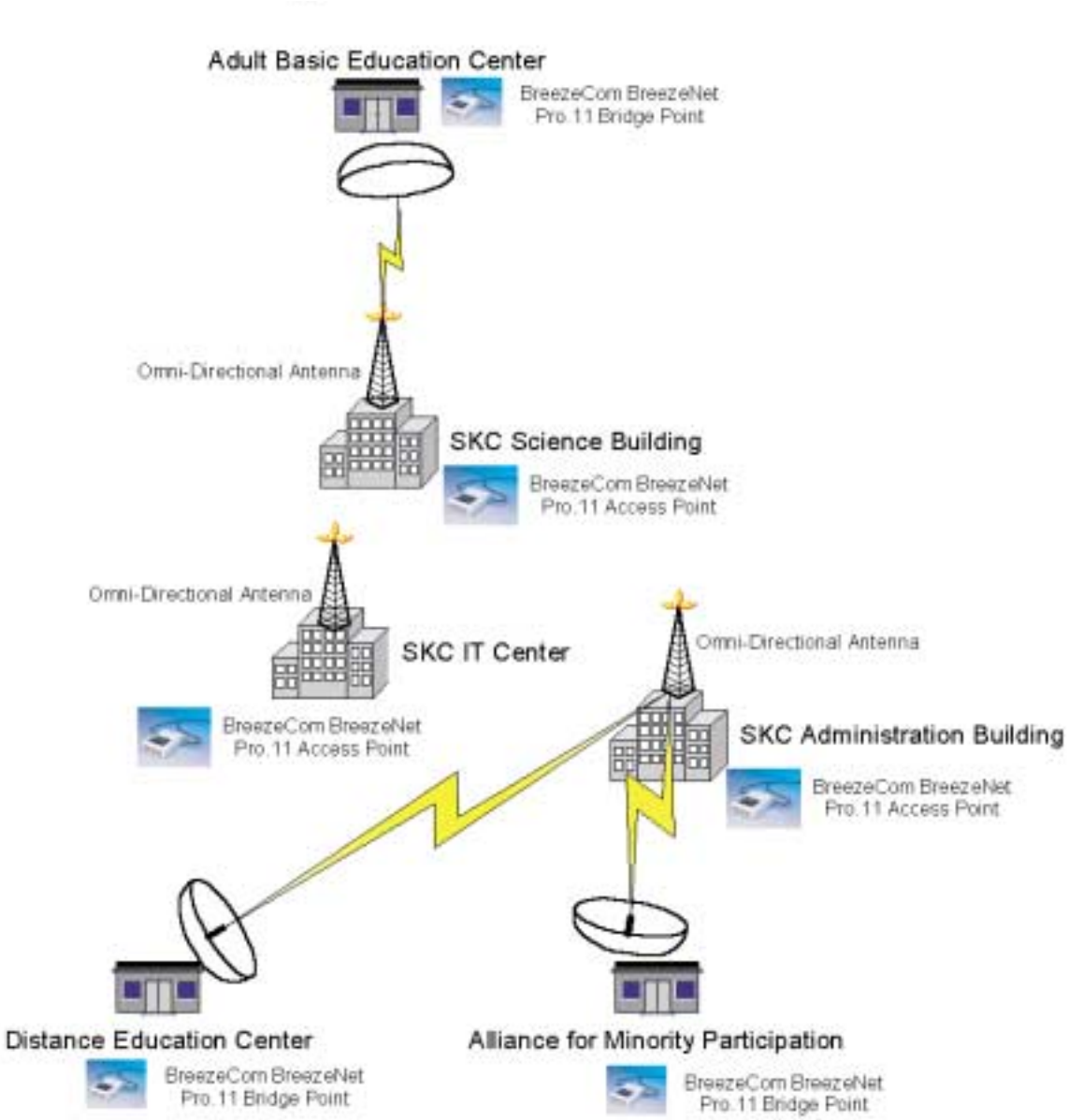
Appendix 1

Profile of Salish Kootenai College Wireless LAN

Salish Kootenai College (SKC) has several buildings for which installing fiber for networking was not an option. One building is a rental and not located on campus, but is within the distance limits of wireless. Another building is a temporary trailer, so it is not feasible to run fiber to it. In these circumstances it made sense to use wireless LAN infrastructure to connect these buildings to their campus LAN.

SKC chose a product that allowed both a P2P model (building to building) and a multiple P2P model (laptops connected to the campus LAN). The infrastructure used has an access point with antennas installed inside and outside, as shown in Figure 7. This access point connects directly to the campus LAN via Ethernet. The multiple antennas allow the access point to be used for building-to-building connections and laptop connections, giving users access to the campus LAN. A bridge point installed in the outlying buildings is connected to a switch, giving campus LAN access to computers in those outlying buildings. The access points can have multiple bridges, giving multiple outlying buildings access to the campus LAN via one access point. For security the wireless bridges are configured to connect only to the access points to which their antennas point and have security set to a custom wireless security ID (extended service set identifier, or ESSID).

FIGURE 7.
Salish Kootenai College wireless network.



Appendix 2

Model Service Level Agreement

This service level agreement (SLA) is written strictly from a network services point of view. On many campuses, basic desktop support is also provided as an integral part of network services.

SERVICE LEVEL AGREEMENT FOR STANDARD ETHERNET SERVICES

The Model College Network Services unit delivers 10-megabyte Ethernet connections via eight-pin RJ45 data network wall jacks available across campus.

Register: Apply to use a data network connection by contacting (*service contact*) to provide details of the computer to be connected and to receive an IP address. No equipment is to be connected to Model College's data network without advance registration except via approved "guest roaming services."

Use of all Model College Network Services is governed by applicable laws and the Model College IT Appropriate Use Policy available at (*link*) and at the Network Services office.

Fees apply as follows:

- Existing data network jacks will be activated and operated by Network Services at no fee.
- The end user is responsible for the cost of installing any new data network jacks required, including construction costs and Network Services fees (for example, a standard $200 Network Services installation fee for activating a newly installed network connection).

- The end user is responsible for providing all computer and network interface equipment, cables, and related material to connect to the data network wall jack.

Support: Network Services will verify that a given data network connection works with a properly configured machine. Management of the machine configuration and application suite is provided by Desktop Support Services.

Response to problems: Network Services always attempts to respond to and repair problems as quickly as possible. The following minimum standards of response apply:

- Network Services maintains 24-hour coverage, 7 days a week, to respond to network-wide system failures, with the initial response (response goal, for example, "within 4 hours").
- Network Services will respond to failures of individual data jacks or subnets within a single building or office area by (response goal, for example, the next business day.)

Agreement to this sort of SLA is implicit through the act of signing up for the service. Unique SLAs constructed to detail particular services, often between two particular parties, will include the following additional information:

Parties: *(Describe the parties to the SLA.)*

Description of Services: (*Insert an overall description of the service to be provided.*)

Scope of Work: *(Describe the work to be provided, including milestones, checkpoints, sign-offs, timeline, and so on. Smaller projects may include this information within the Description of Services.)*

Acceptance Criteria: *(Describe the conditions that will constitute successful delivery of the service. Smaller projects may include this implicitly or within the Description of Services.)*

Agreement: *(Provide names, dates, etc. of the parties agreeing.)*

Appendix 3

Generic Guidelines for Writing a Request For Proposal (RFP)

Many factors should be considered when writing a request for proposal (RFP) to get the desired results. The RFP must

- be unambiguous in its language,
- be concise, and
- provide a definitive and adequate timeline for project completion.

In addition to these RFP attributes, the institution should create an evaluation team that will develop clear proposal evaluation criteria.

LANGUAGE

Use terminology that is consistent and easily understood by potential responders to your RFP. Avoid cryptic acronyms unless they have been spelled out prior to use. An ambiguous RFP may generate undesired responses, frustration, and wasted processing time.

CONCISENESS

An RFP should not read like a quiz paper with "trick" questions or hidden meanings. Be concise and explicit in what you want accomplished. For instance, if you want to digitally archive files in an office and have them retrievable from a searchable database, then issue your RFP to explicitly include the keywords retrieval, searchable, and database.

TIMELINE AND DEADLINE

One of the goals of an RFP is to obtain the best job performance at an affordable cost and in a timely manner. The writer of the RFP must begin the process early and anticipate possible delays that can affect the project timeline. The timeline should be such that the expected completion date precedes the expiration of a relevant existing contract date and does not adversely affect current processes. Enough time for the winning bidder to complete the work should be factored into determining the project completion date.

The deadline for receiving an RFP should be clearly delineated. If proposals must be postmarked or received by a certain time and date, state that very clearly.

EVALUATION TEAM AND CRITERIA

An evaluation team should be formed to review all submitted RFPs. Along with members from the finance and business office, the team should have representatives from other departments that will be affected by the RFP's implementation. The team leader should be involved throughout the life cycle of the RFP (start to implementation).

While writing the RFP, develop criteria by which RFP responses will be evaluated and a successful one selected. However, do not include these evaluation criteria in the RFP. This prevents bidders from tailoring their responses to the criteria. Also, indicate the process, not the criteria, for evaluating the responses to the RFP. For instance, the top three bidders will be requested to make a presentation and demonstration to the evaluation team.

Finally, the team must comply strictly with all the evaluation rules, including not accepting late RFPs. The team should also consider any intellectual property issues that may surround the materials submitted in bids, especially those that do not succeed.

EDUCAUSE

4772 Walnut Street, Suite 206
Boulder, CO 80301-2538