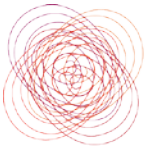
CoSN
LEADING EDUCATION INNOVATION

A COSN BEST PRACTICES WHITE PAPER

Smart Networks: Comprehensive Design Overview

Guidelines for School System Leaders



Brought to you by
Smart Education Networks by Design
a CoSN leadership initiative

November 2015

Table of Contents

Smart Networks: Comprehensive Design Overview

Intended for school district executive leaders, this document is designed to facilitate discussion, build understanding and prompt questions related to the design of a comprehensive network that provides not only adequate performance but consistent and reliable connectivity for students and staff. In addition, the structure of this document should be considered a framework for ongoing conversations related to the development of a SMART network. These items will be detailed below in an executive format and built out further with your Director of Technology or Chief Technology Officer.

Without a doubt, things are changing in our schools. While every school district is different, every district is responding to many of the same driving forces (1:1, BYOD, digital publishing, disaster preparedness, etc.) and these are placing increasing pressure directly on the network infrastructure. Today, districts that are implementing a digital transformation are at risk of hitting a wall, be it the cost and availability of increased internet capacity, the reliability of homegrown networks that have now become mission critical, or ageing or inadequate equipment.

In the past, a phone call to the Internet Service Provider for more bandwidth or upgrading network switches might have worked, but that is no longer a sufficient or sustainable response. Education networks need to be different by design.

This document will outline the rationale and approaches that support the development of Smart Education Networks.

Executive Overview

Traditional school networks, depending on size and geography, are generally not able to scale to support teaching and learning in a digitally transformational environment. Many "breaking points" occur as districts try to evolve existing networks for the future in the same way as the past.

Addressing individual network bottlenecks in isolation and piecemeal is likely to lead to wasted money as the next "breaking point" becomes the bottleneck and requires a different approach. Fortunately, numerous technology and market trends combine to create a "perfect storm" of opportunity to redesign and implement a roadmap towards the "New Education Network" that cost effectively provides far more capacity, reliability, flexibility, scalability, and manageability.

Network capacity demand becomes exponential in transformed teaching and learning environments. The demands on School Networks outpace affordability with traditional approaches: Smart Education Networks require a comprehensive redesign, not just a phone call to an Internet provider for more bandwidth.

Fortunately for districts that are large enough for the new demands to seem prohibitive, with comprehensive design, Smart Education Networks can be implemented that increase capacity and reduce costs by:

- Connecting to the Internet at an aggregation site such as an Internet Point of Presence (PoP) and controlling the Wide Area Network (WAN) from the schools to the PoP - giving districts a choice of multiple providers and other cost reducing connectivity such as Internet2 or state/education networks
- Building a WAN with multiple paths to increase reliability
- Shifting servers and services to a hosted data center
- Taking advantage of 3rd party network implementation and management to avoid needing to compete with industry for top-notch network architects and engineers

However, in order to accomplish this New Education Network design, the process must be approached holistically, with full understanding of the tradeoffs among the requirements and a comprehensive design that addresses them as a whole rather than in the traditional silos.

New Education Network Requirements

There are numerous demands on school networks that lead to "breaking" points in traditional design. These include:

- Once districts move to a 1:1 or BYOD environment, the growth on demand for network capacity becomes exponential. It is not unusual for districts to see 60% year over year growth - a doubling of capacity demand every 18 months. Over the lifetime of a 5 year technology plan, that reflects an order of magnitude increase in capacity needs. For districts, it can be resource prohibitive to plan for Internet costs that increase tenfold over a five year timespan.
- Education networks that have grown organically since the days before even computer labs are often not highly reliable. This is less of a problem when they are used primarily for administrative purposes, but once they become instrumental in instruction, the network becomes mission critical and requires much higher reliability than most districts can provide.
- Wireless access points, switches, and even the wiring in school buildings may not support growing levels of Internet capacity and may be incompatible with newer technology.
- Network appliances such as firewalls, security systems and filters may not have the capacity to support growing demand and are expensive to purchase when anticipating demand that has not yet been realized.
- Most districts are not able to afford full time network architects and engineers to scale and manage their networks. Those districts who develop those skills internally find themselves competing with industry for their newly skilled talent.

- Districts that require more servers and storage may find that expanding their data centers and making them robust enough to support mission critical systems is costly in terms of equipment, electricity, and manpower.
- Districts that rely heavily on remotely located or cloud resources will also need increased bandwidth to support those services.
- For many districts, the evolution of their networks does not include strategic planning or support for business continuity and disaster recovery.

School Networks for digital transformation require design for the following drivers:

- *Capacity:* The FCC target for education networks for 2017 is 1 Mbps per student. In addition to student usage, districts also need to consider administrative overhead such as state reporting, managing HVAC and lunch systems, IP Video Security Systems, VoIP, and student information systems (often an additional 30% demand or more). Many districts are finding that once they commit to 1:1 their network capacity demand curve becomes nonlinear, with demand often growing at 60% annually (though this number varies according the circumstances of each district).
- *Reliability:* District CTO's report that their superintendents, teachers, and students expect essentially zero downtime, much less any unplanned downtime. In practice, for many districts, this corresponds to overall network reliability (as experienced per student) of 3-5 "nines" 99.9% of reliability (8 hours - 5 minutes unplanned downtime annually).
- *Mobility:* Depending on district BYOD policies, one or more devices per student requires design for 10x-100x of the number of devices. This has evolved from the time when there was only one device per adult, or perhaps a class-sized computer lab. This means that the network must be sized to accommodate the addressing and number of connections maintained by these devices as well as affordably address security and access for them.
- *Scalability & Flexibility:* Because capacity demand grows so rapidly, the ability to scale Internet access and network appliances throughout the technology lifecycle becomes critical. Otherwise, technology installed at the beginning of the period will either be overkill initially, or become inadequate/obsolete before the 5 year plan period is completed. Similarly, as digital resources and software services are evolving very rapidly at the same time as their usage evolves through a digital transition, the ability to scale servers and services is also critical.
- *Sustainability:* Funding sources and mechanisms can impact how a network is designed. E-Rate incentivizes the near-term building out of fiber. The need for predictable long-term funding sources for infrastructure refresh causes some districts to shift expenses from CapEx to OpEx. Holistic design and careful road mapping of network build-out and upgrades can help ensure that funds are used optimally.
- *Agility:* As districts shift to digital transformation, classroom practice evolves - often rapidly. As a result the needs of teachers and students can change quickly and the ability of IT to respond quickly to these changes depend on a network that is designed to nimbly scale and reconfigure services and access as needed.

- *Maintainability:* The increased demands on education networks also requires that the networks become simpler, easier to maintain and perform optimally. This means that the networks incorporate greater operational automation, must be designed to be easy to monitor both for performance and for proactive maintenance/replacement of faulty hardware as well as for scaling capacity.

Market and Technology Trends

There are significant trends in education, markets, and technology that have combined to create the conditions that both require and enable Smart Education Networks. These trends are not static, but constantly evolving, creating an unprecedented need for flexible, adaptable infrastructure to support the rapidly evolving changes in teaching and learning in a technology environment.

Education Trends

The decreasing cost of mobile devices and Internet appliances such as web-based tools (Chromebooks, iPads, Tablets, etc.) are driving previously unaffordable 1:1 programs in an ever-increasing number of schools and districts. The prevalence of these devices in homes has similarly driven increased numbers of BYOD programs. Both of these trends are sparking the dissemination of innovations in digital educational resources as well as in pedagogical approaches such as flipped classrooms, inquiry-based learning, and student work published to authentic audiences. Technology in the classroom is also facilitating other student-centered approaches at scale such as problem- and project-based learning, innovation, and more. Education Technology and Education Practice are poised to enter a virtuous cycle, each driving the growth and maturation of the other.

Infrastructure growth is also driven by the shift to online assessments as well as implementation of and innovation in data-driven instructional approaches, and increased demands of data collection for federal and state reporting.

Market Trends

> *Through holistic design, utilizing E-Rate funding, and conducting competitive procurements, schools can lower their overall cost of Internet while increasing the capacity and service levels.*

In addition to more affordable devices, the costs of existing Internet appliances continually decrease as new, higher-capacity appliances come to market.

The cost of Internet access (not including transport) is decreasing and the cost of Internet per Mbps is lower at higher bandwidths. This provides an opportunity for districts to lower their overall Internet Access cost. However, the cost of Internet Transport – the district Wide Area Network (WAN) Ethernet connection from the district to the Internet port – has not decreased at the same rate as the Internet; therefore, districts are not always realizing the potential gains of lower Internet costs. Through holistic design, utilizing E-Rate funding, and competitive procurements, schools can lower their overall cost of Internet while increasing capacity and service levels.

The opportunity for high capacity Internet, high availability networks, cloud services, and available funding along with increasing demand for 24/7 access, disaster recovery, and security has driven Enterprises to cloud providers, Carrier Neutral Data Centers (CNDC) and colocation facilities. This market demand has provided an increase in "products" and "solutions" to meet the needs. CNDCs and cloud providers are now more available with a reduced cost structure that can benefit education clients.

Another market trend in K12 education is the use of both dark and lit fiber for the Wide Area Network transport. Fiber-based networks provide the capacity and scalability required for education networks. Infrastructure costs for fiber can be considered in a long term contract arrangement such as an Indefeasible Right of Use (IRU), long-term lease, service contracts and/or ownership.

The requirement of schools to provide high capacity, scalable, and highly available Wide Area Networks and Internet service has driven a change in the overall design of networks. Schools often investigate state, regional and/or collaborative services to augment or replace their current local Internet service model. A district may also investigate building a fiber-based solution both within their network and to an aggregation location where Internet Tier 1 providers, Internet 2, cloud and managed service providers are collocated such as in a Carrier Neutral Data Center, a regional or state aggregation point, or an education specific consortium location to mitigate risk and contain costs.

School districts have found that with diversification they can now provide services at a reduced costs. This reduction in expenditures allows for additional build-outs and designs to account for multiple paths, vendors and access. While support costs can increase, these New Networks allow districts flexibility with partners and improved service to the end user.

Technology Trends

> *Software Defined Networks, Software Defined Data Centers and the **convergence** of the networks and applications are emerging as the most significant and innovative trend in technology, changing the way networks are built for today and architecting them to be future ready.*

The availability of Infrastructure as a Service (IaaS) enables profound improvements in the scalability and flexibility of hardware resources such as servers, appliances and filters; as well as, access to software and services that support both instructional and enterprise purposes. These models are generally available as subscription services making it possible to shift funds from Capital Expenditures to Operational Expenditures so that it is easier to predict recurring costs. In addition, these services are instantly scalable with a phone call to modify service or automatically, in response to demand. These innovations have enabled significant cost efficiencies as well as innovative offerings.

Network Virtualization (NV), Network Function Virtualization (NFV), and Software Defined Networking (SDN) are technology architectures and solutions that change the way networks and network related services are built and delivered for the organization. All of these technologies bring needed solutions to the requirements of security, performance, scalability, management, standards and lower long-term cost.

Software Defined Networks (SDN), Software Defined Data Centers and the ***convergence*** of the networks and applications are emerging as the most significant and innovative trend in technology, changing the way networks are built for today and architecting them to be future ready. Software Defined (SD) infrastructure provides protocols that allow the network to be dynamically managed and monitored by software rules rather than the individual programming of each element, even when the hardware is from a mixture of manufacturers. Network Virtualization (NV) makes it possible to perform functions that were previously handled by network appliances in software.

Network Functions Virtualization (NFV) enables the virtualization of firewall, Intrusion Detection, Intrusion Prevention, load balancing, DNS/DHCP, management and other network applications. NFV runs on high-performance x-86 platforms and it enables functions on selected networks as needed. NFV provides the benefits of security, segmentation, management throughout the network without the need for physical hardware. NFV can also reduce the need to overprovision – buying or allocating large hardware appliances that handle the whole network for the next three to five years. Instead, the district purchases functions for each specific area(s) based on need with the ability to scale and grow on demand.

Policy and Funding Trends

In 2014, the Federal Communications Commission (FCC) made sweeping changes to the Federal K12 Internet and Funding program, E-Rate. The January and December implementations of the E-Rate Modernization Order and the Second E-Rate Modernization Order represented the most significant changes since the program's inception in 1996.

The orders changed and prioritized the eligible services included within the program, increasing the funding levels from $2.4 billion to $3.9 billion annually, changing the schools funding schedules and levels, optimizing the program processes, transparency and systems. These changes can allow districts to create and manage detailed infrastructure and operations with more ease.

Changes to what is now called Category 1 services increased the ability of districts to fund last mile installations and pay for connectivity changes. Unlike in previous years, funds were specifically set aside for Category 2 funding to prioritize the installation of Wi-Fi and wired networks in schools. Additionally, the orders decrease and ultimately eliminate support for traditional telephony services within the program. Each of these changes impact operations, reporting, resilience, and support. Districts will need to address their technology and infrastructure planning with those changes in mind and account for these changes outside of USAC funding.

Usage Trends

Very different usage patterns have emerged as a result of the availability of new technologies and new digital resources combined with beneficial market trends and increased mainstream adoption of 1:1 and Bring Your Own Device (BYOD) programs in schools.

- *Internet as Destination:* Most school traffic is now intended for the Internet rather than internal operational systems such as payroll and student record management. Students are accessing digital resources for learning as well as using the Internet for research, publishing work, collaborating with other students or subject matter experts, playing educational games, etc. Even core school business systems such as Student Information Systems and Learning Management Systems are available as cloud-based services that many districts are shifting towards. This means that networks and security need to be optimized to support high capacity light-weight access to the Internet as well as limited access to district-hosted software, where it still prevails.

- *Ubiquitous Access:* Mobile students are accessing their learning resources and communities from within the classroom, from home, and anywhere in between. Districts must be intentional about enforcing role-based access and control to its network, software and services of differing levels of security and criticality from devices using non-district networks for access, such as mobile LTE devices or home Wi-Fi.

The usage trends of Internet as the Destination and Ubiquitous Access, in conjunction with digital content and broad adoption of wireless devices by all (BYOD), are combining to build the New Digital Learning Community.

The relationship between education, market, technology, policy and usage trends are tightly woven and should be considered when building an education network that will meet the needs of schools for both near and long-term build-outs. A clearly defined and agreed upon understanding from all stakeholders – community, administration, network architects and departments – is one of the most important aspects of building a new network to support the New Digital Learning Community.

New Education Network Design

Comprehensive and Integrated Design Approach

The design of the New Network consists of making tradeoffs and leveraging synergies among multiple interrelated systems. If different design teams evolve an isolated section of the design in a vacuum, the opportunity to leverage opportunities and make those tradeoffs is lost. If, however, the full design of the New Education Network is performed holistically, with all elements taken into account, the full cost and performance benefits made possible by current technology and market trends becomes available.

When a methodical approach is applied to designing the optimal network system by examining subsystem design simultaneously, the design outcomes can and should be different. The perfect storm of technology and innovation, policy, funding, and the digital revolution and the expectations of a digital society have enabled and demanded this opportunity for an Integrated Design approach. The Comprehensive and Integrated Design process with the addition of new components into the traditional network architecture is more complex than simply upgrading or expanding existing environment; however, it is a core and foundational approach to redesigning and changing the network to meet the needs of the next five years.

Integrated design demands a purposeful and articulated expectation that the designs of the subsystems will provide more than just interoperability of components. This design must not only meet current needs, but also it must be optimized for advanced functionality and service delivery as the result of the aggregated subsystems' designs and meet the projected needs of the district for the next three to five years.

Every district is different, and how comprehensive design is applied to a given district network will vary. However, there are trade-offs and practices that every district should consider when embarking on a Smart Education Network implementation.

- Begin with a shared vision of the network's purpose. How will it be used today and five years from now? What is the goal for students and how will technology support that? A shared context is critical for making the important trade-offs. Without it, each functional area will optimize for their own sub-system leading to a degradation of the system overall.
- Create a cross-functional team with the job of understanding the infrastructure implications of different decisions regarding the digital environment. For instance:

    - Will the district support BYOD, where the network might be required to support students with 3 or more devices or will it support 1:1 where the district is responsible for purchasing and managing devices?
    - Will students access their learning community and resources only at school, or at home and places in between?
    - What levels of security and access is required for different software and services?
    - Will the students be using digital curriculum that require a daily simultaneous download of data to each device?
    - How will teachers be using technology in the classroom and what will their usage patterns look like?
    - What is the financial tradeoff between lower cost Internet appliances with higher bandwidth needs and more expensive devices?

- Take a "greenfield" design mentality. Without the requirements of strategic solutions and greenfield mentality, comprehensive design appears to be the traditional and normal process for design; however, districts must be careful not to fall into the refresh and grow process of existing platforms on an existing network without re-evaluating the overall network design options as they relate to other subsystem needs such as Internet capacity or the Application Delivery Platform. The critical and differentiating component of the Smart Education Network design process is comprehensive ***and integrated*** design of the network system as a holistic process. Once a comprehensive design is in place, the implementation can be staged over many years for optimal cost-effectiveness and budgetary alignment.
- Document the current network design including the Wide Area Network (WAN) and telephone systems and identify alternative providers of services in addition to the traditional vendors:

    - Identify the current Information and Communication Technology infrastructure within your community, region and state.
    - Identify potential network/fiber providers for your district.
    - Identify the providers of colocation, data center services and IP access to your community. This may include but not limited to professional Tier 3 or Tier 4 Carrier Neutral Data Centers in the closest metro, the closest termination point of IP Transit Internet services (or Internet Port services, local providers physical service location,

and higher education, research, state and regional networks physical demarcation locations.

- Revisit and update design frequently to respond to the changing environment.
- Mitigate the growing cost of Internet capacity by identifying the optimal physical location for obtaining Internet services. For many districts a Research and Education Network, an intergovernmental cooperative network, or an Internet Point of Presence (PoP) can offer multiple providers as well as virtualized software, storage, and network services. Conduct a cost trade-off between the cost of connecting fiber between the district and such a PoP and the cost reduction available due to eliminating vendor lock-in and reliance on single providers.
- Perform a cost analysis between building, leasing, or otherwise controlling the fiber in your Wide Area Network (WAN) in order to eliminate single-vendor dependence for Internet transport.
- Perform a Total Cost of Ownership analysis between maintaining a physical data center versus remote or virtualized services such as those available at a Carrier Neutral Data Center (CNDC) as a primary data center.
- Mitigate reliability issues by ensuring multiple paths on the WAN, electrical redundancy, and other measures. When making investments evaluate each for redundancy and cost individually. How likely is the failure being mitigated? What is the impact of the failure (single student, classroom, building, district?) How long would it take to repair or route around the failure?
- Consider a Network Function Virtualization Platform to support authentication, authorization and accounting for wired and wireless network, active directory, DNS/DHCP, firewall, load-balancing, security and DMZ services. The NFV platform can also support voice IP access services and Quality of Service. Because the NFV provides a significant amount of East-West traffic, Network Virtualization should be considered in the overall design for increased security.
- Identify an Application Delivery strategy. What are the requirements for enterprise, hosted, private/hybrid and public cloud services with respect to access, security, and so on.
- Develop a wide area network infrastructure that is built on a design that provides scalability, capacity, high availability and ease of management including an internal network transport layout (discussed below), an external connection options, estimated cost of POP co/location, Internet cost and options, and PSTN cost and option. Also, identify access to peering and/or state network services to augment the commodity Internet service.

In the majority of cases, a high level design with the Smart Education Network strategy Internet and IP services requirements and design solutions of the cost efficiencies and scalability alone will validate the need for the New Network Design Architecture. However, when the other service requirements for PSTN access, Application Delivery Platform, Network/Data Center solutions, Disaster Recovery/Business Continuity and Cloud services are considered through a

comprehensive and integrated design process, the New Network Design Infrastructure solution will clearly show both the immediate and long term strategic value to the district.

Note that for those districts where it is cost effective, moving their Internet access and data center to a PoP is the prime enabler for numerous cost efficiencies and improvements in ease of management, reliability, and scalability. For small districts, or districts that are highly geographically distributed, this approach may not be the most cost-effective. Each district must make those trade-offs holistically and independently.

Also note that these steps do not address the issue of human capacity for network architecture and management. For many districts it may be more cost effective, reliable, and sustainable to contract network design, build-out, and maintenance from a third party with service level agreements and built-in technology refresh than to compete with industry for highly qualified network specialists.

High Level Architecture for a New Education Network

Figures 1 and 2 (below) shows a traditional school network. It most likely evolved from supporting computers for administrators and teachers and a computer lab, all connected via Ethernet to now supporting some level of Wi-Fi in the school. Depending on the size of the district, evolving this network by simply adding more Wi-Fi access points in each building and a fatter pipe to the Internet from the district may become prohibitively expensive and/or cumbersome when moving to one or more devices per student and 1 Mbps/student capacity.

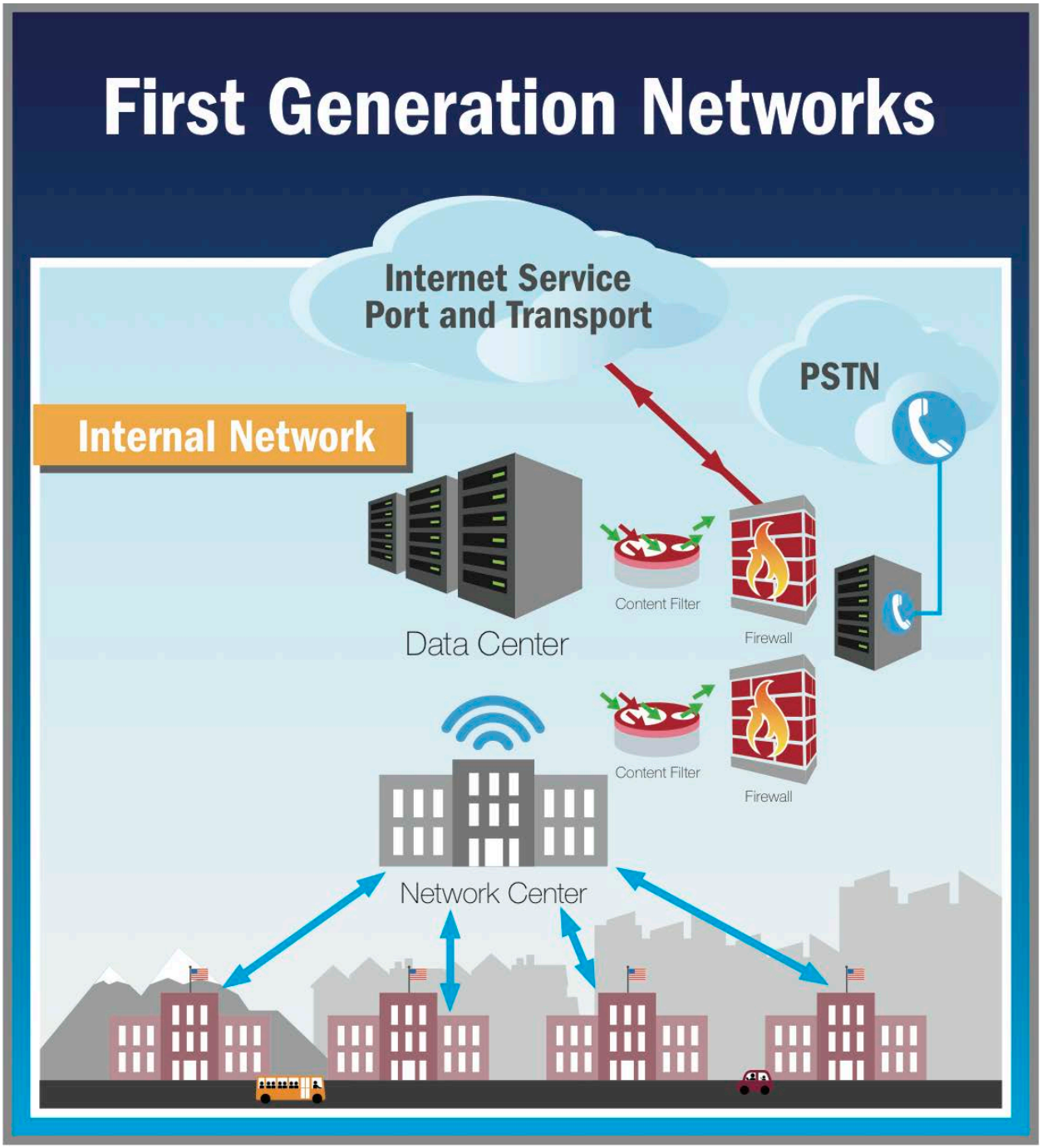


Figure 1: Traditional School Network Concept

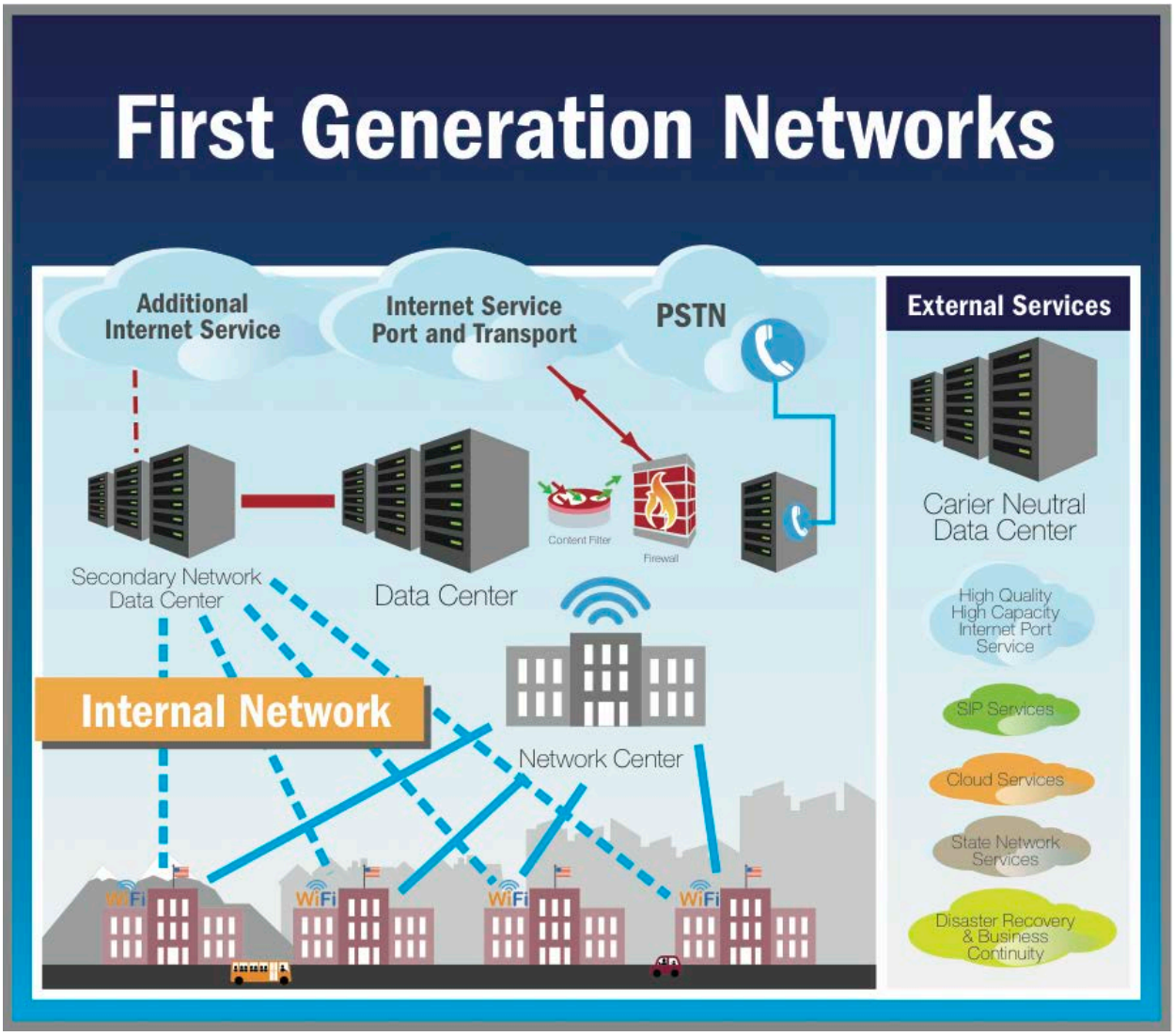


Figure 2: Early networks evolved to include external services

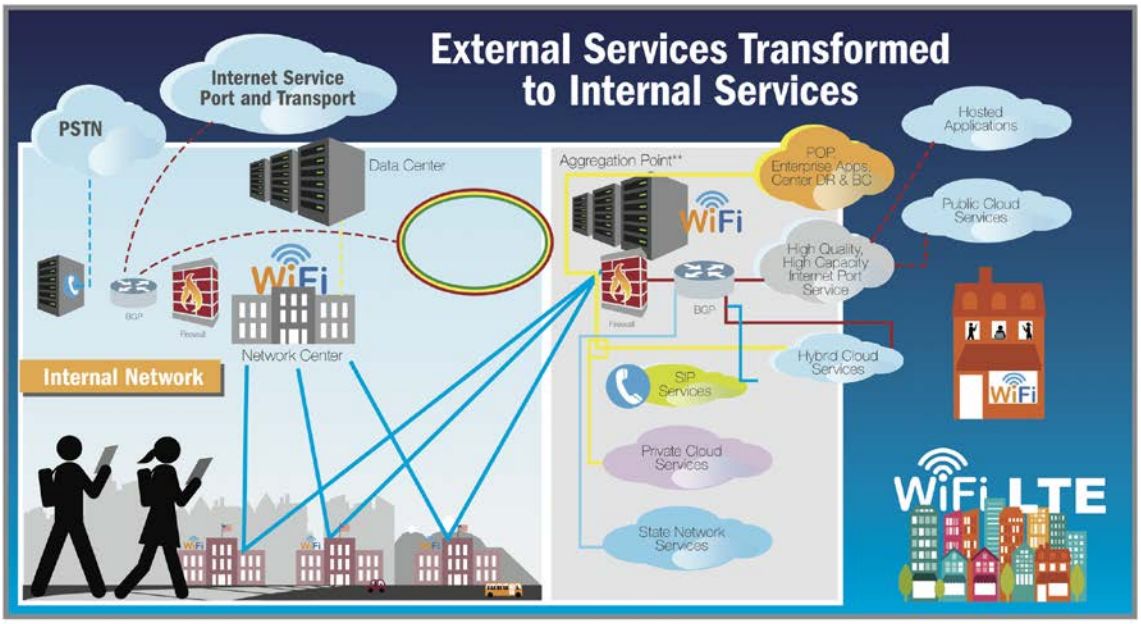


Figure 3 shows a High Level New Network Design Architecture that addresses the limitations.

Key design elements include:

- Aggregation Point of Presence. Identifying the location for your schools that provides access to the services required both near and long term and provides support for the innovative technology strategies that will bring value to your network. Schools are connected to an Internet Point of Presence where the district can leverage competition among service providers to get the best rates for Internet access. (Note this may mean the district can gain access to services from a carrier-neutral data center, from their state Research and Education Networks, state government, their local community college, or other.) For instance, Utah and Washington state both provide a K-20 network presence for their districts to help alleviate the overhead and burden for districts where the size of a district restricts access or knowledge.
- Accessing and leveraging peering agreements through ISPs, state and regional networks and Internet 2. Internet Peering is the process by which two Internet networks connect and exchange traffic. Tier 1 Internet providers exchange traffic with free and reciprocal peering agreements.
- Accessing and leveraging federal, state, and educational contracts for connectivity and equipment.
- Security is built into all aspects of the network including the basic layers of WAN transport and network access, wireless and Internet. The network provides access to the Internet and external services and provides access to internal resources to only appropriate devices and users and protects all internal services from both internal and external access.

- An Internet infrastructure that leverages aggregation, high availability, NFV, scalability and security.
- Network Functionality is obtained as a service for flexibility, maintainability, and scalability, such as firewalls, filtering, security and 24/7 access.
- The district has control of its WAN transport in order to eliminate reliance on individual high-cost providers. The E-Rate Second Modernization Order changed to rules to support and encourage fiber solutions for WAN transport including dark fiber and lit fiber solutions. Wavelength services, generally Dense Wave Division Multiplexing (DWDM) service provides optical (dark fiber like) connections between two locations with protection options, scalability and support, are growing in availability as a WAN transport solution.
- Servers, Networks and Network Access Services are virtualized and provided by private, hybrid or public cloud solutions. A private cloud service, either built by the district or provided as an outsourced service, is a virtualized infrastructure with compute, network, security and storage designed to support the applications of the organization. Cloud infrastructure reduces hardware and increases scalability, reliability and availability and can eliminate the physical dimensions of space and location. Because secure, scalable network access is a basic component of any network , the Network Access Services (NetAS) become a priority service; therefore, Network Function Virtualization is a key consideration with building a New Network.
- An Application Delivery Platform for software and services that are most cost effectively hosted by the district on a virtualized platform (private or hybrid cloud) when possible. A Network Virtualization Platform to support the virtualization of Network Functions (NFV) instead of buying appliances.
- Build support for IPv6 into the network design.
- Utilize open, industry based standards and standards-based protocols to enable multi-vendor interoperability, ensure future functionality and innovation through Software Defined Networks automation.

Revisit and Review

A highly available, scalable, secure Internet service is the most important component of the Smart Education Network. The Smart Education Network considers all aspects of the Internet service including the Internet, the transport and additional options for providers including external Internet providers including Tier 1 and others, rather than the local phone and cable companies; and Internet 2 to augment the "commodity Internet" service. Commodity Internet is a general, commercially-available connection to the regular Internet, as opposed to a special-purpose restricted network like Internet2 or Education State networks.

ACRONYMS AND DEFINITIONS

AAA - Authentication, Authorization and Accounting. A framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services.

Application Delivery Platform. Usually a set of components that provide a delivery architecture (such as application use, creation, session controls and/or protocols) for a type of service that is delivered.

ARP - Address Resolution Protocol. A protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. For example, in IP Version 4, the most common level of IP in use today, an address is 32 bits long.

ASN - Autonomous System Number. A collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain that presents a common, clearly defined routing policy to the Internet.

BGP - Border Gateway Protocol or Service Provider Termination. A standardized exterior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS) on the Internet.

BYOD - Bring Your Own Device (aka… BYOT - Bring Your Own Technology). Refers to the policy of permitting students and staff to bring personally owned devices (laptops, tablets, and smart phones) to school, and to use those devices to access information and applications.

CapEx - or capital expenditure. A district expense incurred to create future benefit (i.e., acquisition of assets that will have a useful life beyond the tax year). For example, a district might buy new assets, like buildings, or equipment, or it might upgrade existing facilities so their value as an asset increases.

Cloud Services Platform – private, hybrid and public. Services made available to users on demand via the Internet from a cloud computing provider's servers as opposed to being provided from a company's own on-premises servers.

CMS/LMS - Digital Content and Learning Management Systems. Software applications used in the administration, documentation, tracking, reporting and delivery of network/Internet based courses or e-learning programs.

Colocation (colo). A data center facility in which a district can rent space for servers and other computing hardware. Typically, a colo provides the building, cooling, power, bandwidth and physical security while the customer provides servers and storage.

Commodity Internet Service. A general, commercially-available connection to the "regular" Internet, as opposed to a special-purpose restricted network like Internet2 or some other specialized backbone network. Generally, a commodity Internet connection offers no content, application protocol, or destination restrictions or quality-of-service controls.

Content Filter. The use of a program or device to screen and exclude information from access or availability Web pages or e-mail that is deemed objectionable.

CNDC - Carrier Neutral Data Centers. A data center which allows interconnection between multiple telecommunication carriers and/or colocation providers. Network-neutral data centers exist all over the world and vary in size and power.

DDoS - Distributed Denial of Service. A type of DOS attack where multiple compromised systems -- which are usually infected with a Trojan -- are used to target a single system causing a Denial of Service (DoS) attack.

DNS - External Domain Name Service. The way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

DMZ - Demilitarized Zone (sometimes referred to as a perimeter network). A physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet.

DR - Disaster Recovery and Business Continuity Plans and Systems. The area of security planning that deals with protecting an organization from the effects of significant negative events.

DWDM - Dense Wave Division Multiplexing. A technology that puts data from different sources together on an optical fiber, with each signal carried at the same time on its own separate light wavelength.

East-West. Traffic flows between DC devices and applications and never leaves the DC. “North-South” traffic is limited to traffic that enters and exits the DC. It is the sort of traffic that most DC security solutions focus on as it crosses the DC boundary.

E-Rate. The common term used in place of the Schools and Libraries Program.

Firewall. A part of a computer system or network that is designed to block unauthorized access while permitting inbound and outward communication.

FCC. Federal Communications Commission.

Firewall Security Equipment. Often categorized as either "network firewalls", where a firewall software appliance running on general purpose hardware, or a hardware-based firewall computer appliances filters traffic between two or more networks - or "host-based firewalls", where a layer of software on one host controls network traffic in and out of that single machine.

Gb - gigabit. The difference between a Gigabyte (GB) and a Gigabit (Gb) is the same, with a Gigabyte being 8 times larger than a Gigabit.

Greenfield. A project that lacks any constraints imposed by prior networks. An example of a greenfield network is the second generation of cell phone networks. The first cellular telephone networks were built primarily on tall existing tower structures or on high ground in an effort to cover as much territory as possible in as little time as possible and with a minimum number of base stations.

IC. Intermediate Cross-Connect Communication Closet. A subordinate data room that encloses telecommunications network systems and devices and may also be known as a wiring closet that contains access to panels and cabling within buildings.

Internet 2. Internet2 is an exceptional community of U.S. and international leaders in research, academia, industry and government who create and collaborate via innovative technologies. Together, we accelerate research discovery, advance national and global education, and improve the delivery of public services.

IDS - Intrusion Detection System. A type of security software designed to automatically alert administrators when someone or something is trying to compromise information system through malicious activities or through security policy violations.

IP - Internet Protocol. A unique string of numbers separated by periods that identifies each computer using the Internet Protocol to communicate over a network.

IPS - Intrusion Prevention System. Intrusion prevention is a preemptive approach to network security used to identify potential threats and respond to them swiftly. Like an intrusion detection system (IDS), an intrusion prevention system (IPS) monitors network traffic.

IPAM - Internet Protocol Address Management. A method of tracking and modifying the information associated with a network's Internet Protocol address (IP address) space. With IPAM, administrators can ensure that the inventory of assignable IP addresses remains current and sufficient.

IRU - Indefeasible Right of Use. A contractual agreement between the operators of a communications cable, such as submarine communications cable or a fiber optic network and a client.

ISP - Internet Service Provider. An organization that provides services for accessing, using, or participating in the Internet.

Layer 2. Refers to the Data Link layer of the commonly-referenced multilayered communication model, Open Systems Interconnection (OSI). The Data Link layer is concerned with moving data across the physical links in the network.

Layer 3. Refers to the Network layer of the commonly-referenced multilayered communication model, Open Systems Interconnection (OSI).

Load-balancing - distributes workloads across multiple computing resources, such as computers, a computer cluster, network links, central processing units or disk drives.

MAC - Machine Address Code. A unique machine identifier that is used when connecting to a network.

MC - Main Cross-Connect Communication Closet. The main data room that encloses telecommunications network systems and devices and may also be known as a wiring closet that contains access to conduits large enough for service personnel to access in order to service or install cabling/networks within buildings.

Mb - megabit. One thing that often gives people confusion is the difference between a Megabyte (used for file size) and a Megabit (used for download speeds). People often assume that a download speed of 1 Megabit per second (1 Mbps) will allow them to download a 1 Megabyte file in one second. This is not the case, a Megabit is 1/8 as big as a Megabyte, meaning that to download a 1MB file in 1 second you would need a connection of 8Mbps.

NAT - Network Address Translation. The virtualization of Internet Protocol (IP) addresses. NAT helps improve security and decrease the number of IP addresses an organization needs.

NetAS - Network Access Services. Provides districts with communication links to carrier and service provider wide area networks.

New Network Reference Architecture. A framework for viewing and planning a holistic approach to building a New Network for Education or Smart Education Network by Design designed and optimized to support the transformation to a digital living and learning environment.

NFV - Network Function Virtualization. A network architecture concept that proposes using the technologies of IT virtualization to virtualize entire classes of network node functions into building blocks that may be connected, or chained, to create communication services.

NV - Network Virtualization. The process of combining hardware and software network resources and network functionality into a single, software-based administrative entity, a virtual network.

OpEx - or operational expenditure. Opex is the money the district spends in order to turn inventory into throughput. Operating expenses also include depreciation of plants and machinery which are used in the production process.

POE+ - Power Over Ethernet. Distributing power over a CAT5 or CAT6 Ethernet cable to a target device that is not plugged into an AC wall outlet. PoE enables remote network devices such as access points, IP phones and surveillance cameras to be installed in locations far away from AC sources. It also eliminates the bulky AC adapter for each device.

PoP. A point of presence is an artificial demarcation point OR interface point between communicating entities. It may include a meet-me-room. In the US, this term became important during the court-ordered breakup of the Bell Telephone system.

PSTN. The world's collection of interconnected voice-oriented public telephone networks, both commercial and government-owned. It's also referred to as the Plain Old Telephone Service (POTS).

SDN - Software Defined Networking. An approach to computer networking that allows network administrators to manage network services through abstraction of lower-level functionality.

SEND - Smart Education Network by Design. CoSN, in conjunction with school district technology leaders, education network consultants and businesses developed the SEND Initiative guidelines for network design and a checklist for district network planning - See more at: http://www.cosn.org/SEND.

SSL - Secure Socket Layer Decryption and Inspection. The standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

Tier 1 Provider - A Tier 1 Provider (aka...Carrier). An Internet Service Provider (ISP) that can serves its coverage area entirely through settlement-free collaboration with other carriers, rather than having to pay tolls to other companies for using parts of a third party's IP network. Tier 1 Providers tend to have large coverage areas and large footprints, with a lot of infrastructure and massive financial resources.

Virtualization Hypervisor. A piece of computer software, firmware or hardware that creates and runs virtual machines. A computer on which a hypervisor is running one or more virtual machines is defined as a host machine. Each virtual machine is called a guest machine.

CoSN (Consortium for School Networking)
1025 Vermont Avenue, NW, Suite 1010
Washington, DC 20005
202.861.2672
info@CoSN.org

www.cosn.org