Best Practices for School Network Architecture and Design

Executive Summary

In the spirit of communion, solidarity, and subsidiarity and in support of the direction set by *From Strength to Strength: A Plan for the 21st Century Catholic Schools in the Archdiocese of Seattle* motivated the creation of these school technology best practice guidelines. The Office for Catholic Schools Information Technology Advisory Group (ITAG), a technology strategy committee of school technology leaders, has provided advice and consultation during the development of this document.

In many Archdiocese of Seattle schools, these best practices have been integrated into their technology architecture and design. The goal of this document is to formalize current practices and provide direction to school technology planning and support staff. One of outcomes has been to establish operation efficiencies via the adoption of common designs and processes for routine technology tasks. Common designs and practices reduce the learning curve to adopt and operate technology. Common designs and practices is a key factor in an emerging trend of informal inter-school collaboration loans of technology staff.

The focus of this document is to describe a technical strategy to segment IT network infrastructure into user communities.

Schools are a collection of several technology user communities (teachers/staff, students, visitors) with different roles and responsibilities. The focus of this document is to describe a technical strategy to tailor IT network infrastructure access to these user communities. The major motivation to adopt the following network architecture and design principles is to provide an additional layer of IT protection to block and filter critical and confidential information from malicious or inadvertent access by unauthorized parties.

Author: Tom O’Callahan

Technology Office, Office for Catholic Schools, Archdiocese of Seattle

Reviewers: OCS Information Technology Advisory Group (ITAG)

Date: 3/14/19

Best Practices for School Network Architecture and Design

Table of Contents:

Technical Summary:

Most schools have the IT network infrastructure capable of integrating network based separation of student and teacher/staff information access.

Introduction: This document provides best practices to schools to better manage student access to Internet content and improve the IT security posture to match the adoption of classroom student computer. The target audience is IT infrastructure planners and network designers. This network architecture describes a network design tailored for mobile, Wi-Fi network, student computers.

Most schools have completed or in the progress of putting student computers in the classroom, which is a substantial change to most previous designs, such as an dedicated computer lab room. These conveniently located classroom computers have enabled integration of more use of cloud-based curriculum. Several IT infrastructure upgrades have been critical to this transformation. The key infrastructure network design requirements are high performance, improved availability, and greater reliability. For educators and administrators there has been a parallel technology shift toward cloud based productivity applications (email, word processing, administration databases, etc) from older applications that had been locally installed on servers and desktops.

From the 1990s until a few years ago, most business and education IT environments centered on a local network and a server. These servers, mostly Windows and Apple systems, were storage and application space for most system computers. In particular, Window servers were designed to perform both the application and data storage. Recently cloud/Internet base alternatives to this design via G-Suite from Google and Office 365 from Microsoft have been increasingly affordable. As most schools move toward these cloud solutions, attention must be paid to the legacy environment. Schools' technology efforts must include not only the introduction of new technology but the careful removal of the old. The initial student computer model collected the computers in a common room and hard wired to a shared Local Area Network (LAN) for teachers, students, staff, servers and printers. The model worked provided there was technology staff and technology available, to constantly monitor student computer usage, to block undesirable situations, and perform maintenance on the systems. However, this limits the number of systems in use to the single classroom, which is far too few resources for most of today's curriculum.

The first Wi-Fi access points/routers were standalone devices; within the past ten years the technology advanced to mesh capable wireless systems. The standalone access points had not been integrated into a management and configuration system and required greater technology skills to manually optimize and monitor. The mesh capability greatly improved network fault resiliency, dynamic load sharing and roaming of devices. Modern integrated WIFI LAN Modern Optimizing a wireless network includes providing network access security and availability and the associated discrete design decisions.

This mesh network architecture leverages technology to allow greater efficiencies of a shared network infrastructure. This network architecture document describes a plan to provision separate networks with a network design technique using mature, stable and widely adopted technologies: virtual local area networks (VLANs) and wireless SSIDs. Most school wireless access point use SSIDs with easy to recognize network names. The network design integrates virtual local area networks (VLANs) with wireless network names as an addition network isolation element. This is a one time network configuration process and typically doesn't impose ongoing operational complexity.

Information access and security policy: All schools have some basic policies to filter or block student access to inappropriate or objectionable content. Incorporating technology for advanced user community isolation capabilities requires some planning but following adoption are provides ongoing flexibility and little ongoing operational complexity.

Many schools have, via the network modernization program, or via internal initiatives have upgraded their classroom networks to provide high speed Wi-Fi network access for student and teachers. Most of the schools have Wi-Fi network technology capable of separating network access so student and teacher computer networks are isolated and not shared. The ability to isolate networks provides a powerful method to build very granular network access user communities policies. Student computers can be built to incorporate network access filters so their access to the school network and Internet can be tightly managed. The capabilities to plan, build, manage, and operate policies to provide differential, role based, network access has become dramatically easier. Network equipment systems with Web/GUI management interfaces and centralized consoles have greatly simplified the technical skills needed to respond quickly computer access requests, integrate components, and troubleshoot.

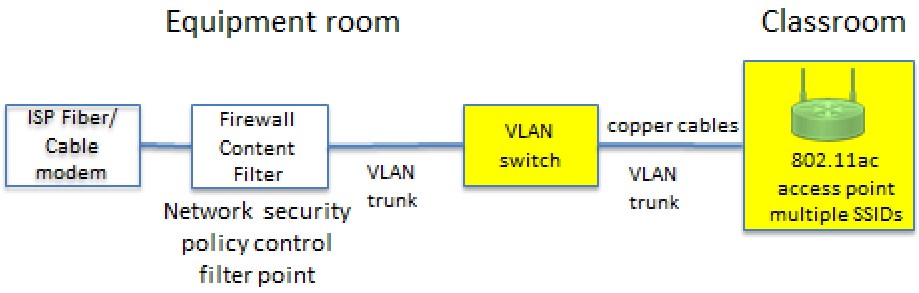
School Network Infrastructure Overview:

The basic network infrastructure components starting from the edge of the network to the Internet connection are:

1. WiFi access point (also called wireless router, AP, or WAP). This device advertises the school's wireless networks and enforces first level of network access policy. Access points are typically located in the classrooms and distributed in a manner so adjacent access points can automatically detect and serve computer in the event of an access point loss.

2. The LAN switch is a device located in the room where the network cabling terminates is a major starting point for troubleshooting reports of network slowdowns. The switch provides multiple Ethernet ports or interfaces to both hard wired and wireless access points. The switch plays a critical role in forwarding network traffic among access points, hard wired devices, firewall, and content filter. One of the key roles is distributing Virtual Local Area Network (VLAN) access.
3. The firewall and web content filter (also called security appliance) are often combined with the network routing. The more complex Internet access policies are maintained here. This is often one of the primary control points for enforcing the school's Child Information Protection Act (CIPA) policy. Differential policies for social network access for students v. staff are maintained here. The school's Internet modem is directly connected to the security appliance and in turn the security appliance connects to the LAN switch. This is the central location for network routing between Virtual Local Area Networks (VLANs) LAN switch.

Diagram A: Reference Network Topology and Components

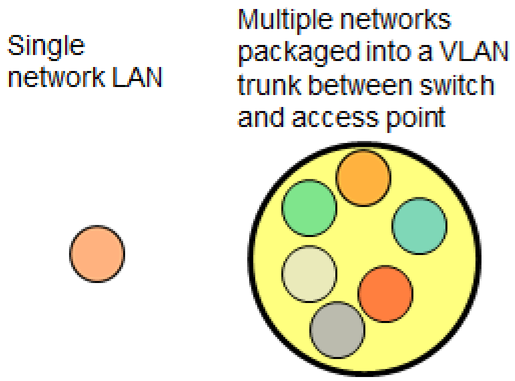


School Network Design Best Practices:

This section describes architectural objectives for a network based information access security model for school networks. The transition to this model with centralized network management systems can be completed via a plan with simple steps. Most schools that have participated in the network modernization program have adopted the following network design.

The wide range of devices a school network must support has introduced some challenges. The first step to addressing the challenge to consider is incorporating network infrastructure system that provides easy to use management console. VLANs on switches and wireless access points provide simple mechanisms to isolate and filter different operational and user communities. The network infrastructure should provide great flexibility to build network isolation policies via a combination of VLANs and WiFi SSIDs (wireless networks). VLANs and the associated VLAN trunking are fundamental network access control building blocks and have been IT standards for over 20 years. Other methods to restrict student network and content access also need to be considered by the IT architects.

Diagram B: LAN Connection Types


Single network LAN
Multiple networks packaged into a VLAN trunk between switch and access point

The typical school network user communities are:

1. The general purpose network. These are computers and systems critical to day-to-day operation. Schools typically “grandfather” hard wired computers to share this network. In terms of VLANs, typically this is the default VLAN, VLAN 1.
2. A network management network should used. Only network infrastructure components are allowed on the management network. This network provides a “lifeline” isolated path to access the network components when a suspected network event on a user network (ie the general purpose or WiFi networks) needs troubleshooting.
3. Wireless networks for WiFi network access. There may be several user community specific WiFi network access.
    a. At a minimum, the student WiFi networks should be isolated via a combination of unique WiFi networks, VLANs, and passwords from all other user communities. This is critical to maintain network based access filters directly on the wireless access point and/or on a VLAN capable network access content filter. This network needs to be designed so it can participate with seamless handoffs to adjacent wireless access points under fault, maintenance, or load sharing situations. Note: The inter-network filter design may need to allow manufacturer specific protocols such as Apple Bonjour.
    b. All networks should provide WiFi network with access restricted to teachers and staff. The network access filters on this network typically allow less restricted access to Internet content. The teacher and staff network has access to printers other resources that may not be appropriate for day-to-day student access.
    c. Commonly a school provides a guest network that is Internet only and has no access to any school IT infrastructure. Network based Internet speed and/or bandwidth throttles are often considered.
4. Physical security devices are often times on physically isolated network infrastructure so there is little possibility that any access from the school network. In situations requiring security to share the school’s network infrastructure a dedicated VLAN plus firewall filter should be used.
5. VoIP phones, servers, and associated infrastructure should use a network that is dedicated. Many phones provide a computer connection which allows sharing of the physical connection.

In this network design the LAN switch is built to provide a voice or auxiliary VLAN in addition to the data VLAN. The phones are discovered by the LAN switch and dynamically placed on the dedicated VLAN. Maintenance and monitoring of voice systems are commonly contracted out to a service provider. The operational responsibilities for voice infrastructure are often different than for computer networks so this should be considered when designing a network.

6. Bells and clocks may require a dedicated network. These devices may communicate with each other over a network using message formats that are not optimized for use on network with data devices.
7. Client/legacy functions – many older client computers require connectivity and services from legacy network components. Printers and scanners are often installed with a static IP on the LAN. The client computer's VLAN and its associated IP sometimes needs to on the same network as the legacy printers. Consider moving printers to a cloud based print sharing option, such as Google Cloud print, especially for the systems that use the printer only occasionally.

Other Design Considerations:

DHCP service: The DHCP should be provided by the component that is provides an easy user interface and simple to manage and monitor. The IT best practice has been to incorporate this operation function into a network component vs a Microsoft server.

DNS service: Cloud based computer systems and non-Microsoft domain computers should use an Internet based DNS server. Commonly, Google, Microsoft, or Internet providers provide highly available and reliable DNS service.

Appendix A: Brief Glossary

User Community Filters: policies built by the network administrators to allow or block access to a class of users. For example, different policies for student access to printers, specific or category of web content v. teachers and staff. The enforcement point for these policies may be based on the Wi-Fi SSID or wired connection.

Local area network: An Ethernet or wireless (Wi-Fi) network that provides a shared physical connection among computers, printers, servers.

VLANs: A method to logically partition a physical connection to provide sharing network equipment but maintaining isolation. VLAN are typically associated with a wired network. A LAN switch provides configuration capabilities to build inter-network connections.

SSID (service set identifier): A method to logically partition a Wi-Fi radio physical connection to provide sharing wireless access point network equipment but maintaining isolation. The network administrator configures user community specific wireless network names and access policies (passwords, keys).

Appendix B: VLAN Number Convention for Network Planners

This is a guide to naming VLANs. VLANs are locally significant to a switch (and SSID, network) and is typically a onetime configuration done at network installation. The VLAN is sometimes referred at a "tag number". The unique VLAN number must be consistent all along the network plan to provide contiguous logical network from the wireless access point network (SSID), LAN connection to the access point and the LAN connection to the firewall (router).

The key is to be consistent with the VLAN numbering. This describes a convention that pairs the VLAN number from the IP network subnet configured on the firewall. The "x" in the 2nd position of the address is assigned according to the zip code of the installation. This allows a unique address space if two such networks are merged in the future. The number in the third position of a 10.x.y.z IP address is used as the VLAN #. If the "y" is used by the Firewall, "y" is used for the VLAN #. A VLAN number that is link to the IP address can be very useful when troubleshooting a problem. If a computer or computers with IP addresses 10.x.16.n are reporting problems, the troubleshooting can directly start at VLAN 16 on the switch or AP instead looking up the IP address to VLAN assignment on the firewall/router first. Note that the Table A IP addresses have a large range of IP addresses to provide for building large networks (512 computers /23, 1024 computers /22) for future growth.

Table A: VLAN and IP Address Numbering

Firewall network address	VLAN # (matches the 3rd number sequence/octet of the network address)	User community/networked device	
existing address	1	Wired devices	
10.x.8.1	8	Staff wireless	
10.x.16.1	16	Student wireless	
10.x.199.1	499	Network infrastructure management	
10.x.32.1	32	guest/visitor	
any address	501	VoIP "auxiliary VLAN"	