# REPORT OF STEWARDSHIP BOARD, IT COMMITTEE TO BOARD OF DEACONS

# STATUS OF MOUNT OLIVE CHURCH AND SCHOOL IT INFRASTRUCTURE

# MAY 22, 2022

Submitted by:

Russ Hansen, Board of Stewardship Deacon
Amber Holberg, Member IT Committee
Dan Nessett, Member IT Committee

# INTRODUCTION

At the April, 2022 Board of Deacons meeting, the IT Committee of the Board of Stewardship was authorized to investigate the state of the Mt. Olive Church and School IT infrastructure with the following objectives:

- Determine how the school would integrate 15-20 new laptops purchased through a government grant into the existing IT infrastructure.
- Investigate the current state of the IT infrastructure to determine possible improvements.

This report presents the findings of the IT Committee in regards to these two objectives.

Details of the issues the Board of Deacons authorized the IT Committee to investigate were:

## Laptop Integration

The design for laptop integration is driven by the following requirements:

- 15-20 new laptops will be integrated into the school IT infrastructure.
- The laptops will be located in 3 classrooms.
- Network connection of the laptops will utilize WiFi.
- The laptops must have access to the internet.
- All students with approval should be able to use any Laptop.
- Teachers will not store sensitive information on student laptops.
- Laptops should be able to run Windows Pro.

## Improvements to the existing IT Infrastructure

The issues receiving attention for this part of the investigation were:

- How to possibility improve the current system used to back up the data held on the office computers.
- How to possibly improve the filtering of inappropriate internet content to protect Mt. Olive School students and the reputation of the congregation.
- How to improve the security of the existing WiFi networks.

# MEETING WITH IT CONTRACTOR

On Tuesday, May 3, 2022 Pastor McCall convened a meeting between the IT Committee and the contractor that provides IT Infrastructure services to the

congregation. At that meeting the attendees discussed the issues described in the previous section and developed options to enhance the IT Infrastructure to meet the objectives inherent in those issues. Further discussion of those options continued by email.

## Attendees

In order to introduce the parties to each other and indicate their expertise in addressing the issues that would come before them during the meeting, a brief summary of their professional qualifications and responsibilities was presented:

Pastor McCall – Head Pastor of Mt. Olive Lutheran Church and Head Master of Mt. Olive Lutheran School.

Russ Hansen – Deacon for the Board of Stewardship and head of the IT Committee. Master's Degree in Food and Nutrition. Had consulting business in Montana and Wyoming at Senior Care Centers for 30+ year during which he traveled a great deal and gained experience using the networks of various customers.

Amber Holberg – Member of the IT Committee (did not attend meeting). Web master for the School Web site. Master's Degree in Structural Engineering and a licensed professional engineer in Montana and Wyoming.

Dan Nessett – Member of the IT Committee. Web master for the Church web site and web admin for both the Church and School Web site. Ph.D. in Computer Science. Worked for 17 years at Lawrence Livermore National Laboratory (LLNL), one of the nation's two Nuclear Weapons Labs. Worked at Sun Microsystems as Solaris Security Architect (oversaw integration of Kerberos with NFS). Worked at 3Com as consulting engineer in Technology Development Center. Consulted with product divisions on security technology. Developed intellectual property for company. Was coinventor on Network Login patent, which was basis for IEEE 802.1x and 802.11i standards. Developed multilayer firewall, which was basis for 3Com product line.

Dan Denson – Head of Denson Technologies and our IT contractor. Before forming Denson Technologies was senior IT staff member at General Parts International, a company headquartered in Raleigh, North Carolina with a national presence. General Parts distributes motor vehicle supplies, accessories, tools, and equipment. While at General Parts, worked on Dec, Unix and Solaris systems. Currently his MSP has 10 IT clients, which are serviced by him and 2 part-time techs.

# Development of Recommendations

Before the meeting addressed the technological issues before it, the following points were made:

- There are no foreseen changes in relationship between IT contractor and church/school. Any additional work will be done by contractor. Members of the IT Committee have no interest in taking over any responsibilities for IT Infrastructure implementation.
- Before any recommendations are forwarded to the Board of Deacons, the IT Committee will consult with our IT contractor to ensure feasibility and smooth integration with the existing IT infrastructure.

# Results of the Meeting

During the meeting, the attendees developed several proposed solutions to problems faced by the IT Infrastructure by integrating into it the new school laptops and also improving its security. Understanding these problems and solutions requires familiarity with the current IT Infrastructure architecture, which is now presented.

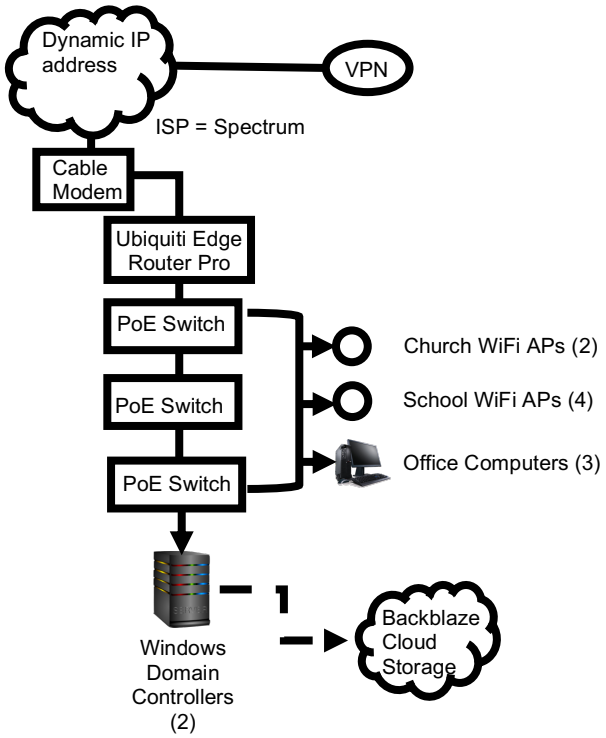


**Figure 1. Church/School Infrastructure**

It is important to keep in mind that while we may think of the IT infrastructure as divided into two components, one for the school and one for the church, in fact there is only one IT infrastructure shared by both the church and school. This affects the decisions made on how to modify it for the school laptop project. Changes to the infrastructure made to accommodate that project in most cases will affect both the church and school. Think of the IT infrastructure in the same way that the church/school water supply is implemented. There isn't a separate water supply for the church and one for the school. They share the same water supply and any changes to it affect both.

There are several aspects of the current IT infrastructure that constrain how we integrate the school laptop project into it:

- Our Internet Service Provider (ISP) is Spectrum. We have chosen to use an economy networking plan, which keeps costs low, but also means we are not allocated a static IP address. This means that the networking address that external systems use to contact us can change at any time. While this is generally not a problem, it does affect the scheme chosen to provide parental control functionality that prevents school students from accessing inappropriate web sites (e.g. adult web sites). This is discussed in more detail below.
- There is only one VPN supported at the moment for access from outside the church/school IT infrastructure to systems inside it. This VPN was created in order for the Business Manager to access her computer while helping her daughter with health problems.

# Upgrade Proposals

### *Upgrade WiFi Access Points*

Dan Denson pointed out that the current WiFi signal strength in the school classrooms is marginal and may not be able to support 15-20 new school laptops. The existing Access Points (APs) in the church and school are old and should be upgraded. Currently, there are 6 WiFi APs in the church and school. One is in the sanctuary, one is in the Parish Hall, and 4 are located along the School corridor. Some of the cabling from the network switches to the APs in the school is substandard (cut, then spliced together; running along the floor of the classrooms). Fixing this should not be expensive and is recommended.

**Recommendation:** Add 1 additional WiFi access point for upstairs and be prepared to purchase and install a second one if that doesn't completely resolve WiFi weak points. Upgrade the cabling in the school as needed.

*Upgrade the Domain Controllers*

Currently there are two mirrored Domain Controllers running Windows Server software. Services provided by these Controllers include a file server and user authentication. The file server data is backed up to Backblaze cloud storage. These servers run on very old hardware and are nearing the end of their useful lifetime. Dan Denson recommends the following:

1. Reduce the domain to the 3 computers used for the office work.
2. Eliminate the 2 mirrored Domain Controllers.
3. Manage the 3 Office PCs with an admin suite or continue to use a Domain Controller if available.
4. Perhaps run Shepherd's Staff on one of the office computers (but see next point)
5. Purchase 1-2 NAS (Network Attached Storage) systems to: 1) provide full backup of the office computer data, 2) Perhaps run Shepherd's Staff on a VM running Windows on the NAS, 3) Run other applications on the NAS as needed.
6. To handle NAS fails, (e.g., to accommodate a facility issue: fire/flood/lightning/etc), backup NAS storage with Backblaze.
7. To handle a hack of the NAS system (this is somewhat unlikely, but possible), cloud backups are versioned and restoration from just before the hack is just a download away.

The IT Committee believes only one NAS is necessary. Server failures are due in 99% of the cases to disk crashes. It is extremely rare for servers to crash due to Motherboard or RAM card failures (at least in the first 10 years). Since the NAS supports RAID, it is always possible to recover from a disk failure by replacing the disk and rebuilding the NAS. It is possible to run Domain Controller software on the NAS (see below), which the IT Committee recommends.

Both users and computers may be managed by Domain Controllers. Managing students in this way introduces significant IT administration overhead that would be very costly. Since each student will have an account on an application cloud (see below), it is only necessary to manage computers with the surviving Domain Controller running on the NAS.

**Recommendation:** Adopt the recommendations from Dan Denson with the provision that we purchase only one NAS. Since this system will not only act as a storage backup, but also as an application server and Domain Controller, we recommend purchasing a NAS with significant computing power, e.g., a Synology 1520+. This piece of equipment has 5 disk bays, of which only 3 need be populated at present with the remaining two reserved for future expansion of storage capacity.

### *Managing the traffic on the church/school network*

There are advantages of keeping the networking traffic that travels between the office machines separate from that traveling between school systems.

**Recommendation:** separate the network carrying church and school traffic into 2 VLANS. This will insure if one becomes compromised that eventuality does not compromise the other. (Note: If we decide to eliminate the members-only WiFi network, add a recommendation here to do that).

### *Laptop Application Software*

The School laptops require application software in order for students to prepare reports. It is assumed laptops will run the Windows operating system. The question then becomes which application suite to choose. There are three options:

1. Load the Microsoft office suite on each laptop.
2. Run applications in the Microsoft Office 365/education cloud.
3. Run applications in the Google Workspace for Education cloud.

These options have the following advantages and disadvantages:

> Option 1 Advantages: Students use and therefore gain experience with software that is standard for the business community (e.g., MS Word). This option supports fine-grained control of each laptop.
>
> Option 1 Disadvantages: This option requires significant IT support. Students can't work from home on projects unless they take a laptop home, which inevitably means some laptops will be lost. The option has higher purchase cost than the other two options.
>
> Option 2 Advantages: Students use and therefore gain experience with software that is standard for the business community (e.g., MS Word). This option supports fine-grained control of systems. Allows students to work from home on projects without taking laptops home.
>
> Option 2 Disadvantages: This option requires significant IT support with the associated costs. In order to work from home, it requires home access to the internet.
>
> Option 3 Advantages: Simplicity of setup. This option allows students to work from home on projects without taking laptops home. IT support and associated costs are minimal.

**Recommendation:** Choose option 3. Almost all schools with which Dan Denson is familiar have chosen this option. The advantages of using Microsoft software are minimal for K-8 students, since preparing them for business jobs is generally not a goal of K-8 education. Rather, that is something that occurs in High School. The attendant IT management costs of the first 2 options make them unattractive. For Google Workspace for Education pricing, see https://edu.google.com/intl/ALL_us/workspace-for-education/editions/compare-editions/.

### *Parental Controls on web sites available to IT Infrastructure users*

The availability of pornographic content on the internet imposes a duty of care requirement for the congregation to protect students at Mt. Olive School from accessing such content. The school stands ***in loco parentis*** for these students and it should make every reasonable effort to prevent them using the IT Infrastructure to access these sites. In addition, the church is a representative of Christ to the community. Its reputation would be significantly damaged if it was discovered that members used the congregation's WiFi connectivity to access pornographic content.

To meet these concerns, the IT Infrastructure should have controls in place that prevent users from accessing pornographic content through it. Fortunately, solutions exist to meet this objective. There are various DNS filtering solutions that block access to pornographic websites through a network. For example, OpenDNS, NextDNS, and CleanBrowsing are just a few examples of concerns that provide DNS filtering services. The Edge Router can be configured to filter all DNS requests and forward them to NextDNS.

NextDNS has the distinct advantage that it is free for customers who do not exceed 300,000 DNS queries per month. The cost for other DNS filtering services is between $110 and $300 per year. To get some idea of what it would take to generate this level of traffic, if a site generates a DNS query every 10 seconds constantly for a month, it would not exceed this limit. Given that Mt. Olive's network is not being used for significant periods of the day (e.g., midnight to 6 a.m.), it is very unlikely that it would generate 300,000 DNS queries per month.

However, if it does, one solution is to run a proxy DNS server on the NAS server to cache DNS lookups and configure that proxy DNS server to access NextDNS for non-cached DNS queries. This should reduce the DNS traffic to NextDNS to well below the free service limit.

**Recommendation:** Filter all network DNS query traffic using NextDNS directly or through a proxy DNS server running locally, which obtains authoritative DNS data from NextDNS.

*WiFi Security*

This is the only area in which members of the IT Committee and Dan Denson disagree. He proposes using a highly insecure WiFi protection scheme to secure WiFi data on the School WiFi network. The IT Committee recommends using a more modern and much more secure scheme. Without getting too far down into the weeds, the highly insecure scheme has the following disadvantages:

1. The scheme, called WPA2-PSK (sometimes called WPA2-Personal) uses a common encryption key derived from a readable password. This password is stored in the clear on every machine and is trivial to discover. Since all machines use the same encryption key, compromising one machine compromises them all.
2. WPA2-PSK is intended for use in homes, not in small to medium businesses (SMB). It is known and has been known for years that using WPA2-PSK in business networks introduces significant security threats which can lead to serious compromises of data. Discussion of the hazards of using WPA2-PSK in Enterprise networks are found in the following article:

   https://www.globalsign.com/en/blog/wpa2-personal-or-enterprise

The only advantage of WPA2-PSK is it is easy to manage.

The more secure scheme recommended by the IT Committee for use in the School is known as WPA2-Enterprise. There are several variants of WPA2-Enterprise. The one the IT Committee recommends is EAP-TLS. Its advantages are:

1. A new encryption key is distributed for every connection. There are no shared keys that are stored on all machines. Therefore, if one machine is compromised, the other machines are not.
2. EAP-TLS is widely used to protect business computing. It is the second most widely used security scheme after WPA2-PSK (which is used mostly for open WiFi networks such as those found in fast-food establishments, e.g., MacDonald's, and in homes).

The one disadvantage of EAP-TLS is it takes a bit more effort to install. However, once installed, it is as easy to use and manage as WPA2-PSK.

**Recommendation:** Use WPA2-Enterprise/EAP-TLS to secure the School's WiFi network. (See Appendix A for a discussion of the cost of using EAP-TLS)

# Summary

After meeting with Dan Denson, our IT Contractor, and discussing how the expected School purchase of laptops will fit into the existing IT Infrastructure and also how some existing flaws in it might be eliminated, the IT Committee makes the following recommendations:

1. Add 1 additional WiFi access point for upstairs and be prepared to purchase and install a second one if that doesn't completely resolve WiFi weak points. Upgrade the cabling in the school as needed.
2. Purchase a Network Storage System (NAS). Since this system will not only act as a storage backup, but also as an application server and Domain Controller, we recommend purchasing a NAS with significant computing power, e.g., a Synology 1520+. This piece of equipment has 5 disk bays, of which only 3 need be populated at present with the remaining two reserved for future expansion of storage capacity.
3. Separate the network carrying church and school traffic into 2 VLANS. This will insure if one becomes compromised that eventuality does not compromise the other. (Note: If we decide to eliminate the members-only WiFi network, add a recommendation here to do that).
4. Run school laptop applications on the Google Docs/Drive cloud.
5. Filter all network DNS query traffic using NextDNS directly or through a proxy DNS server running locally, which obtains authoritative DNS data from NextDNS.
6. Use WPA2-Enterprise/EAP-TLS to secure the School’s WiFi network.

# APPENDIX A – COST OF USING EAP-TLS

One consideration when choosing between WPA2-PSK and WPA-Enterprise/EAP-TLS is the cost associated with each option. The following information is provisional, since it is based on information gleaned from browsing the web, rather than on focused discussions with sellers of Windows operating system software.

One major advantage of WPA2-PSK is the cost of implementation. Basically, it is zero. Virtually every device supports WPA2-PSK.

EAP-TLS, on the other hand requires the use of Public Key Infrastructure (PKI), which is a complicated technology. Microsoft has greatly simplified the administration of PKI and when client machines are part of a Microsoft Domain (managed by a Microsoft Domain Controller), deploying EAP-TLS is relatively straightforward.

However, in order to integrate into a Microsoft Domain, client systems must run either Windows Pro or Windows for Education. Since laptops, out of the box, run Windows Home, in order for them to integrate into a Microsoft Domain their operating system must be upgraded from Windows Home to either Windows Pro or Windows for Education.

Without a Microsoft volume license agreement, it costs about $100 per machine to upgrade from Windows Home to Windows Pro. For 20 laptops, the total cost would be $2,000, which is a considerable amount. With a Microsoft license agreement, this cost may be considerably less. How much less depends on the particular volume license agreement the School has with Microsoft or another vendor of Microsoft software.

The cost of upgrading from Windows Home to Windows for Education is less clear. The information on costs associated with deploying Windows for Education, including upgrading from Windows Home to it, is a bewildering maze of special cases that are hard to evaluate. So, this report provides no guidance on this option.

The fundamental question becomes: is it worth the extra cost of upgrading Windows Home to one of the other versions of Windows in order to support EAP-TLS. This question is tied to that of managing the laptops separately or centrally through a Windows Domain Controller. This report holds that it is, for the following reasons:

1. Managing 15-20 laptops without the use of Microsoft Domain and Active Directory support is a daunting task. Machines managed independently tend to gather incidental software that eventually means they diverge from each other in terms of both stability and behavior. Central management allows

administrators to keep the software on the systems identical so they are fungible.

2. Updating Windows to ensure it is secure and stable is significantly easier when they are managed centrally. Central management supports installing security patches on all machines when they become available. Managing updates on machines individually is generally difficult and almost certainly will result in some systems being up-to-date and others out-of-date.
3. Managing the laptops centrally ensures they all have the same security settings and configuration data. Trying to keep this data synchronized is difficult and almost impossible when they are managed individually.
4. To mitigate the security threats inherent in WPA2-PSK, Dan Denson suggested using an Intrusion Detection System/Intrusion Prevention system (IDS/IPS). It is proposed these would detect any threats against the laptops coming from a compromised WiFi network. However, when the software on the laptops is managed individually, it is easier to load software on the laptops that is malicious and potentially compromises the system's integrity, especially if the laptops are taken home by students (where they would be available to family members). Managing software centrally supports software restriction polices that prevent the installation of unauthorized software. The IDS/IPS system cost is better spent upgrading the laptop operating systems to Windows Pro.
5. The use of Domains makes configuring EAP-TLS on each laptop simple. Without managing each laptop from a Domain Controller, configuration of EAP-TLS is possible, but several orders of magnitude more difficult. Since EAP-TLS is significantly more secure that WPA2-PSK, it's use increases the security of the School IT Infrastructure.