

03.23.2026: CFS network architecture observations

From: M Bret Blackford (bret_blackford@yahoo.com)

To: kromain@cfserve.org

Cc: bret_blackford@yahoo.com

Date: Monday, March 23, 2026 at 07:14 PM CDT

Kevin,

I was able to visit Christian Family Services (CFS) today. I spent most of my time tracing the physical network cabling and put together the attached rough diagram. It attempts to show device connections, port usage, IP addresses, and the hardware that appears to be phone-specific.

From what I can tell, the diagram seems generally consistent with what you shared earlier, but would you take a look and let me know whether I have missed or misstated anything? My hope is that, once we agree on the current-state architecture, we can then think more clearly about possible next steps and phases.

If the attached architecture is accurate, my concern is that it leaves CFS with more dependency than ideal on both a specific ISP setup and a specific phone-related configuration. In my view, organizations should be able to change providers without requiring major network redesign or complicated reconfiguration.

I also think we should address the current 100 Mbps limitation in the existing switch/router path and move toward a network design that is more manageable, flexible, scalable, and supportable, while also providing better visibility into connections and traffic.

As we discussed earlier, I think UniFi could be a very good long-term fit for CFS. CFS does not need cutting-edge technology, but it does need a system that is stable, right-sized but flexible, and easier to support going forward.

My overall view is that the current design is understandable as an accumulated legacy solution, but it does not seem like the best long-term fit for CFS. That is especially true if our goals are visibility, maintainability, vendor flexibility, and ease of support. The current network appears to have been shaped in part by older phone and firewall dependencies, even though much of the application environment is now cloud-based. For a small nonprofit like CFS, I would recommend simplifying the core network, making the WAN edge more customer-controlled, and keeping any phone-specific legacy requirements as narrow and clearly documented as possible.

Attached are my current draft architecture diagram and the Fing scan information.

Thanks,

--- Bret

----- Forwarded Message -----

From: M Bret Blackford <bret_blackford@yahoo.com>

To: Kevin Romain <kromain@cfserve.org>

Sent: Sunday, March 22, 2026 at 07:13:52 PM CDT

Subject: Re: Questions re: CFS IT hardware

Kevin,

I re-read your email and realized I had misstated one point. Based on what you described, **the Cisco ASA is currently handling the primary routing/firewall role**, not the MikroTik RouterBoard. Even so, I do not think the current design is an ideal long-term fit for CFS.

I am still planning to stop by CFS this week to trace the physical cabling and better document how everything is connected. That should help me understand the current architecture more clearly before drawing any broader conclusions.

Thanks again for the helpful background.

--- Bret

On Sunday, March 22, 2026 at 06:47:22 PM CDT, M Bret Blackford <bret_blackford@yahoo.com> wrote:

Thanks, Kevin. This is very helpful.

I plan to visit CFS this week and see whether I can document the physical layout a little better. I am going to trace the Cat ethernet cables as best I can so I can better understand what is physically connected to what. I will also try and do a [Fing](#) scan.

One thing I especially want to confirm is whether the Charter/Spectrum router connects only to the MikroTik RouterBoard. My hope is that the Charter/Spectrum router is actually handling the routing and IP addressing, since that would make a transition to UniFi simpler. If instead it is just acting as a passthrough in bridge mode (like you indicate below) to the MikroTik, then the migration may be a little more involved. **I'd strongly prefer to get away from that model and have routing handled by the Charter/Spetrum replacement router (UniFi).**

Also, I looked up [Hawk iSolutions](#) and, based on their website (<https://www.hawkisg.com/> <**is this correct?**>), it appears they work with Ubiquiti/UniFi. That is encouraging, since it suggests they should understand what we are trying to accomplish with a move to UniFi and hopefully can assist if needed.

I will let you know what I find.

Thanks again,

--- Bret

On Sunday, March 22, 2026 at 05:50:22 PM CDT, Kevin Romain <kromain@cfserve.org> wrote:

Hey Bret,

See inline below.

I got some of the answers by looking at the configuration in ASDM.

The more I look at it, I believe the MikroTik device sits on the switch rather than the firewall.
See details and screenshots below.
I'll also add details on the static IPs.

From: M Bret Blackford <bret_blackford@yahoo.com>
Sent: Saturday, March 21, 2026 3:01 PM
To: Kevin Romain <kromain@cfserve.org>
Cc: Bret Blackford <bret_blackford@yahoo.com>
Subject: Questions re: CFS IT hardware

You don't often get email from bret_blackford@yahoo.com. [Learn why this is important](#)

Kevin,

When you get a moment can you find out the following ...

- 1. Is the **Spectrum router** in bridge mode or router mode?
It is in bridged mode. I believe we had them configure it that way when we installed the Cisco ASA.
- 2. What is the **WAN IP on the Cisco ASA**?
See below for more details.: ASA WAN / outside IP: 96.35.181.122 ASA inside IP: 192.168.44.1

3.

Interface	Name	Zone	Route Map	State	Security Level	IP Address	Subnet Mask Prefix Length	Secondary VLAN	Group	Type	MTU	Active MAC Address	Standby MAC Address
BV11	insideBV1			Enabled	100					Bridge Group	1,500		
GigabitEthernet1/1	outside			Enabled		0 96.35.181.122	255.255.255.248			Hardware	1,500		
GigabitEthernet1/2	inside			Enabled		100 192.168.44.1	255.255.255.0			Hardware	1,500		

- 4. Is the **MikroTik only for Hawki/phones**, or does it route any normal office traffic?
It is strictly for the IP phones. I welcome your suggestions here, if the phones should be on their own VLAN.
Something to note is that some of the PCs get a passthrough connection through the phones. It might be best to separate those if possible.
Currently they're on the same subnet as the other devices.

	Christian Family Service MTik	192.168.44.19	Routerboard.com
	192.168.44.169	192.168.44.169	Grandstream Networks, Inc.
	192.168.44.162	192.168.44.162	Grandstream Networks, Inc.
	192.168.44.160	192.168.44.160	Grandstream Networks, Inc.
	192.168.44.171	192.168.44.171	Grandstream Networks, Inc.
	192.168.44.168	192.168.44.168	Grandstream Networks, Inc.
	192.168.44.172	192.168.44.172	Grandstream Networks, Inc.
	192.168.44.163	192.168.44.163	Grandstream Networks, Inc.
	192.168.44.166	192.168.44.166	Grandstream Networks, Inc.
	192.168.44.161	192.168.44.161	Grandstream Networks, Inc.
	192.168.44.164	192.168.44.164	Grandstream Networks, Inc.
	192.168.44.170	192.168.44.170	Grandstream Networks, Inc.
	192.168.44.167	192.168.44.167	Grandstream Networks, Inc.

Static IPs

External: 122-126

Internal: 100-199

Hope this helps.

----- Forwarded Message -----

From: M Bret Blackford <bret_blackford@yahoo.com>

To: Kevin Romain <kromain@cfserve.org>

Cc: Bret Blackford <bret_blackford@yahoo.com>

Sent: Saturday, March 21, 2026 at 01:10:28 PM CDT

Subject: v2: CFS IT hardware thoughts before our call

Kevin,

Thanks for that detailed response. This was very useful and gives me a much better feel for the current CFS setup.

It is encouraging to hear that most of the main applications are cloud-based, even though some important infrastructure still remains on-prem, like domain authentication, file share, print services (all on the Dell PowerEdge), and parts of the phone environment.

Your comments on the Cisco ASA, MikroTik, static IPs, VPN, and VJUMP were especially helpful. Based on what you shared, I still think we are probably on solid ground to treat replacement of the current Spectrum/Charter router, the aging Netgear switch, and the TP-Link access point as a reasonable Phase 1 step, using a UniFi UDR7 and UniFi switch. That feels like a practical way to modernize the core network without trying to tackle every issue at once.

At the same time, I do not want to oversimplify anything, especially since the ASA and MikroTik are still involved today (for the phones). So I am not assuming those can be removed immediately without a better understanding of how everything is tied together.

I also do not think we need to wait on documenting all of the bad wall ports and cable drops before moving ahead with Phase 1. That seems like something we can work through afterward.

I think the next best step is probably just a quick phone call between you and me so I can better understand the current dependencies before I refine the plan further and share recommendations with Eric.

Send me a few times that might work for you, and I will be glad to work around your schedule.

Thanks again,

--- Bret

On Saturday, March 21, 2026 at 12:37:26 PM CDT, Kevin Romain <kromain@cfserve.org> wrote:

Bret,

Thank you for the detailed overview and thoughts.

I'll answer what I can here and provide more details as we discuss further.

1. Most of the CFS key applications are cloud based. However, core infrastructure for domain level authentication, file share, print server and IP phones(MikroTik) are still on-prem.

2. Top priority from what I know of the network

a. Replacement of Netgear FS728TP – this has been discussed with management in the past year. However, we've not been able to make progress because of the availability of network partners. I would certainly prefer a Unifi setup going forward, for multiple reasons.

- b. Repair of bad wall network ports or physical cable runs. Mary or Jodi can provide a walkthrough of the problem areas.
- c. Migration to SharePoint/OneDrive completely, eliminating the dependence on local network shares. (This is mostly driven by business goals and management directives)
- d. Migration to Azure Active Directory(Entra ID)

Here are answers to some of the questions you asked.

“I also have a few questions I am hoping you can help answer:”

- Do you have the password for the Spectrum/Charter router? I would like to review any manual settings that might need to be carried over into a replacement router.

Spectrum manages this device, but will work with us to gather the config settings we need.

- Are any static IP addresses currently in use?

Yes, however I will need some time to look this up.

Current route goes from Spectrum Gateway to Cisco ASA, then out to Netgear switch and MikroTik(IP Phones)

- Are there any VPNs or VLANs in place today?

There is one VPN configured for remote access, however this is disabled as licenses have expired on the ASA firewall.

- Is there any remote access into the network, such as jump boxes or other remote-management methods?

VJUMP is currently configured for remote access for IT support but is limited to licensing on our end. If there is another tool that you use, we can setup the connection with a remote Teams session.

- I do not currently see evidence that the Cisco ASA 5506-X firewall or MikroTik RouterBoard are actively in use, but please let me know if I am mistaken.

Cisco ASA – currently serves as the primary firewall and creates routes for the local network and MikroTik device.
MikroTik – managed by Hawki Solutions – IP phone service provider.

- Would you be comfortable supporting a UniFi-based network? My expectation is that once configured, it should be relatively straightforward to manage and should not require frequent architectural changes.

Yes, sounds like a great idea. My home network is configured with a Unifi Cloud Gateway, so I'm familiar with the management side of things.

Regarding the domain account, I'm sure we can have that setup as we move further in the process. This can be covered when we configure the remote connector through the jumpbox.

Hopefully this answers most of your questions for now, but I'll attempt to answer additional questions when we discuss further.

Best regards,

Kevin

From: M Bret Blackford <bret_blackford@yahoo.com>

Sent: Saturday, March 21, 2026 10:25 AM

To: Kevin Romain <kromain@cfserve.org>

Cc: Bret Blackford <bret_blackford@yahoo.com>
Subject: CFS IT hardware thoughts before our call

You don't often get email from bret_blackford@yahoo.com. [Learn why this is important](#)

Kevin,

I wanted to send along my current thoughts on the Christian Family Services (CFS) IT hardware so you can see where my thinking is before we talk later today, or whenever is convenient.

At a high level, it appears that most, if not all, of the key CFS applications are now cloud-based (which is encouraging). If that is correct, then much of the current on-site hardware is no longer mission-critical in the way it once may have been. That suggests the network should primarily emphasize security, stability, and reliable internet access for those cloud-based systems.

As I have reviewed the current setup, it appears that some hardware may no longer be necessary and could potentially be removed to simplify the cabinet, reduce points of failure, and make the environment easier to maintain. I also noticed that the current main switch, a Netgear FS728TP, appears limited to 100 Mbps, which would create a bottleneck for the entire network.

Based on what I am seeing so far, I am leaning toward the following approach:

- Remove hardware that may no longer be needed, such as the MikroTik RouterBoard and Cisco ASA 5506-X, if they are in fact no longer serving an active role.
- Replace outdated equipment, including the Netgear 10/100 switch, Charter router, and TP-Link Wi-Fi access point.
- Migrate to a UniFi-based network platform for easier cloud-based management, ongoing support, better security, stronger Wi-Fi coverage, and gigabit network performance.
- Use equipment that can also scale later if CFS ever wants to add cameras, sensors, or IP phones.

I have attached a draft migration plan with more specific details.

Before I make any recommendation to Eric McPherson, I would really value your input and buy-in on the overall direction. **I also have a few questions I am hoping you can help answer:**

- Do you have the password for the Spectrum/Charter router? I would like to review any manual settings that might need to be carried over into a replacement router.
- Are any static IP addresses currently in use?
- Are there any VPNs or VLANs in place today?
- Is there any remote access into the network, such as jump boxes or other remote-management methods?
- I do not currently see evidence that the Cisco ASA 5506-X firewall or MikroTik RouterBoard are actively in use, but please let me know if I am mistaken.
- Would you be comfortable supporting a UniFi-based network? My expectation is that once configured, it should be relatively straightforward to manage and should not require frequent architectural changes.

My thought is that the attached migration plan could be completed with relatively low risk if the cutover were done over a weekend, and at a reasonable hardware cost of under \$1,000.

At this point I am treating the Dell PowerEdge R720 server as a Phase 2 item. I am not proposing changes to that system until after the network hardware is addressed. Active Directory and domain controller work is outside my main area of expertise, so I would definitely need more input from you before making any recommendations there.

Separately, **I think it may be helpful at some point for me to have a CFS email address and a user account that would allow me to log onto a CFS computer.** That would make it easier for me to do some work on weekends without needing staff assistance. This is not urgent, but it seemed worth mentioning for discussion.

I realize that is a lot for one email, but I thought it might help make our conversation more productive. I am mainly looking for your thoughts, concerns, and overall blessing on this direction before I refine the plan and make any recommendation to Eric.

Looking forward to hearing your thoughts on this!.

--- Bret

----- Forwarded Message -----

From: M Bret Blackford <bret_blackford@yahoo.com>

To: kromain@cfserve.org <kromain@cfserve.org>

Cc: Bret Blackford <bret_blackford@yahoo.com>; Eric McPherson <emcpherson@cfserve.org>

Sent: Tuesday, March 17, 2026 at 09:27:46 AM CDT

Subject: Possible time to talk re CFS IT environment

Hi Kevin,

My name is Bret Blackford. I serve on the CFS Board of Trustees and have an IT background. Eric McPherson initially asked if I could help clean up the wiring and overall clutter in the IT closet on the second floor. As I began looking into that it became clear that I first needed to identify the equipment and better understand the environment so I would not accidentally disturb something critical.

As I have worked through that process I have been reviewing the equipment and putting together a basic hardware architecture spreadsheet. I have realized it would be very helpful to talk with someone who has supported CFS over the years and knows the environment well. Eric mentioned that you have been a long-time IT resource for CFS, so I wanted to reach out and introduce myself.

I would appreciate the opportunity to spend 30 to 45 minutes with you to better understand the current CFS IT setup, any important history or dependencies I may not be seeing, and to get your thoughts on possible upgrade paths. I am trying to make sure I understand the existing environment before offering any recommendations to Eric.

If you have some availability this week or next, my schedule is fairly flexible and I would be glad to work around a time that is convenient for you.

Thank you, and I look forward to talking with you.

--- Bret

Bret Blackford

314-402-7086

Bret_Blackford@yahoo.com

Information contained in this email is privileged, confidential and protected under HIPAA regulations. It is intended only for the use of the individual or entity named above. If the reader of this email is not the intended recipient, please note that any dissemination, distribution, or copying of this transmission is strictly prohibited. If you have received this email in error please immediately notify us by telephone (314) 968-2216 or by emailing the sender.

Information contained in this email is privileged, confidential and protected under HIPAA regulations. It is intended only for the use of the individual or entity named above. If the reader of this email is not the intended recipient, please note that any dissemination, distribution, or copying of this transmission is strictly prohibited. If you have received this email in error please immediately notify us by telephone (314) 968-2216 or by emailing the sender.



CFS-network_v3.pdf

47.8 KB



CFS_3_23_26_3_36_56_PM.html

73.9 KB