

Christian Family Services

Current-State IT Architecture Review

*Prepared from on-site photos, Fing discovery results, Windows screenshots, and manual notes
13 March 2026*

Executive summary

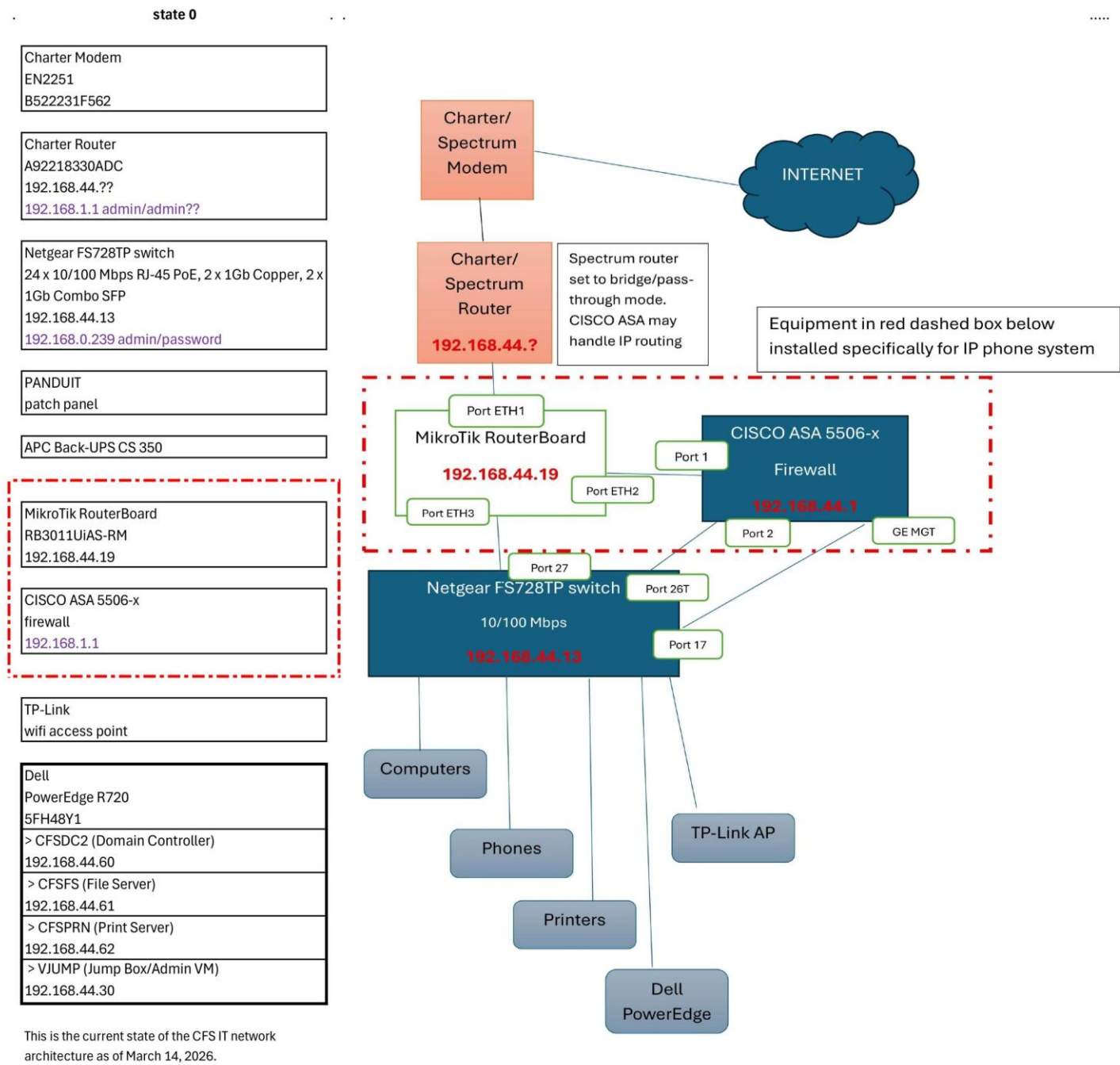
The CFS environment appears to have grown in layers over time. The most critical asset is likely the Dell PowerEdge R720, which appears to host multiple VMware virtual machines that support directory, file, print, and administration functions. The biggest immediate technical concern is the amber fault indication on Drive 0 of the R720, which may indicate a degraded or at-risk RAID set. The network stack also looks more complex than necessary, with Spectrum equipment, a Cisco ASA 5506-X, a MikroTik RB3011, and an older Netgear FS728TP switch all present in the path. The Netgear switch is managed-capable but is primarily a 10/100 Fast Ethernet PoE switch, which is a likely performance and lifecycle concern. Based on the evidence gathered so far, CFS should first stabilize and verify server health and backups, then identify the true default gateway and current switch configuration before simplifying the edge stack.

Key findings

- The live CFS LAN uses subnet 192.168.44.0/24 with default gateway 192.168.44.1, DNS server 192.168.44.100, and SSID “CFS”.
- Fing identified 35 active devices during the scan.
- Observed core infrastructure includes: Hitron EN2251 modem, Spectrum router/gateway, Cisco ASA 5506-X, MikroTik RB3011UiAS-RM, Netgear FS728TP switch, Panduit patch panels, TP-Link access point, and Dell PowerEdge R720 server.
- Fing identified active VMware virtual machines: VJUMP (.30), CFSDC2 (.60), CFSFS (.61), and CFSPRN (.62).
- The Dell PowerEdge R720 shows an amber/yellow indicator on Drive 0 and reportedly beeps occasionally, suggesting a storage or RAID alert that should be investigated promptly.
- The Cisco ASA 5506-X and MikroTik RB3011 may be duplicating network-edge or routing functions, but their exact roles are not yet fully confirmed.
- The Netgear FS728TP is a managed-capable older Fast Ethernet PoE smart switch and is a strong candidate for replacement after configuration review.

Inferred wiring / connectivity diagram

This diagram is the best current interpretation of Ethernet connectivity from the observed cabling, device labels, screenshots, and Fing discovery. Items shaded amber/red indicate uncertainty or review points.



Network overview

Item	Observed value
SSID	CFS
Provider	Spectrum Business
Observed public IP	96.35.181.122
Subnet	192.168.44.0/24
Default gateway	192.168.44.1 (device not yet conclusively identified)
DNS server	192.168.44.100
Observed DNS suffix / internal namespace	cfamily.local
Observed device count	35 online devices

Observed device list from Fing

The following list highlights the most important devices positively identified in Fing. Many additional “Generic” devices were present and should be classified later.

IP	Name	Type	Brand	Model	OS
192.168.44.15		Printer	HP		
192.168.44.18	CFSDT-01	Computer	Dell		Android
192.168.44.88	CFSDT-04	Computer	ASRock		Windows
192.168.44.30	VJUMP	Virtual Machine	VMware	Virtual Machine	
192.168.44.62	CFSPRN	Virtual Machine	VMware	Virtual Machine	
192.168.44.60	CFSDC2	Virtual Machine	VMware	Virtual Machine	
192.168.44.77	CFSDT-02	Computer	Dell		Windows
192.168.44.19	Christian Family Service MTik	Router	MikroTik	RB3011UiAS-RM	
192.168.44.70		Laptop	Apple		macOS
192.168.44.61	CFSFS	Virtual Machine	VMware	Virtual Machine	
192.168.44.86	CFSLT-08	Computer			Windows
192.168.44.150	KM486A09	Printer	Konica Minolta	bizhub C361i	
192.168.44.13		Switch	Netgear	ProSAFE 24 Port 10/100 PoE Smart Switch	
192.168.44.11	iPhone	Mobile	Apple	iPhone 13	iOS

Detailed device inventory and assessment

The table below combines observed evidence, inferred purpose, approximate platform age, known issues, and recommended next actions. Age estimates are approximate platform-era estimates, not guaranteed purchase dates.

Device	Purpose / role	IP / identifier	Approx. age	Observed issues	Recommended action
Hitron EN2251 cable modem	ISP handoff / cable modem	n/a observed	Likely ISP-supplied; exact deployment age unknown	No specific fault observed	Keep unless ISP changes service
Spectrum router / Wi-Fi gateway	Possible edge router, NAT device, and/or wireless gateway	n/a observed	Unknown	Role overlaps with ASA/MikroTik possible; exact active function not yet confirmed	Verify current role; possible simplification candidate
Cisco ASA 5506-X	Firewall / security appliance / possible VPN endpoint	not identified in scan	~2015 platform era	Older platform; role not fully confirmed; near/at end of useful support life	Verify whether still required; likely removal candidate if redundant
MikroTik RB3011UiAS-RM	Router / routing appliance	192.168.44.19	mid-2010s platform era	Active on LAN; exact routing / DHCP / VLAN role not fully confirmed	Review config before considering removal or replacement
Netgear FS728TP	Main rack switch; managed-capable smart PoE switch	192.168.44.13	late-2000s platform era	Primarily 10/100 Fast Ethernet access switch; possible performance bottleneck; managed config unknown	Export / review config; strong replacement candidate
Panduit patch panels & cable management	Passive cabling termination and cross-connect	n/a	age unknown	No issue observed; labeling appears limited	Retain; improve labeling and documentation
TP-Link access point	Wireless access point for office Wi-Fi	not identified in scan by model	age/model unknown	Exact model and management method unknown	Confirm model, power method, and controller/standalone status
Dell PowerEdge R720	Primary on-prem server; likely VMware host	host IP not yet confirmed	2012–2013 platform era	Drive 0 amber/yellow; occasional beeping reported; likely storage / RAID alert	Urgent: check RAID/PERC/iDRAC status and backups; medium-term replacement target
VMware VM: VJUMP	Likely jump/admin VM	192.168.44.30	unknown	Purpose inferred from name only	Confirm role, OS, owner, and backup
VMware VM: CFSDC2	Likely domain controller	192.168.44.60	unknown	Critical if serving directory/authentication	Confirm role, OS, owner, and backup
VMware VM: CFSFS	Likely file server	192.168.44.61	unknown	Critical if serving shared files	Confirm role, storage mapping, and backup
VMware VM: CFSPRN	Likely print server	192.168.44.62	unknown	Shared printing dependency likely	Confirm role and printer dependencies
HP printer	Shared network printer	192.168.44.15	unknown	No issue observed	Retain / document model and location
Konica Minolta bizhub C361i	Shared multifunction printer/copier	192.168.44.150	unknown	No issue observed	Retain / document support contact and usage
CFSDT-02	User workstation (Dell / Windows)	192.168.44.77	unknown	Observed on CFS domain-like network	Document owner and business function
CFSDT-04	User workstation (ASRock / Windows)	192.168.44.88	unknown	Observed on CFS domain-like network	Document owner and business function

Key risks and issues

- Possible degraded RAID or drive failure on the Dell PowerEdge R720 (Drive 0 amber, server beeping).
- Aging server platform likely hosting multiple critical VMs.
- Unclear ownership of the actual default gateway at 192.168.44.1.
- Potential overlap or unnecessary complexity across Spectrum gateway, Cisco ASA, and MikroTik router.
- Netgear FS728TP switch is an older managed Fast Ethernet platform and may constrain performance.
- Unknown current switch configuration (VLANs, PoE dependencies, management settings, uplink use).
- Unknown current backup posture for VMware host and guest VMs.

Simplification opportunities

- Move toward a simpler edge design: ISP modem → single modern firewall/router → single modern managed gigabit/PoE switch.
- Replace the Netgear FS728TP with a modern managed gigabit PoE switch after the current configuration is reviewed and documented.
- Retire the Cisco ASA 5506-X if it is no longer providing a unique security or VPN function.
- Retire or replace the MikroTik RB3011 only after confirming whether it handles routing, DHCP, VLANs, or inter-VLAN traffic that must be preserved.
- Plan medium-term migration away from the Dell PowerEdge R720 to newer host hardware or a cloud / managed alternative, depending on business requirements.

Recommended next steps

1. Immediately check the Dell PERC/RAID status, iDRAC logs, and backup status before any drive is removed or replaced.
2. Identify which device actually owns 192.168.44.1 (the true default gateway).
3. Export or inspect the Netgear FS728TP configuration to determine whether VLANs, PoE, management ACLs, or other features are in use.
4. Document the exact role of the Cisco ASA 5506-X and the MikroTik RB3011.
5. Confirm the VMware host, the purpose of each VM, and recovery / restore capability.
6. Label patch-panel ports, switch uplinks, and critical cable runs to improve supportability.
7. After the above is complete, design a simplified future-state network and migration plan.

Assumptions and caveats

- This document reflects observed evidence from the site visit and device discovery on 13 March 2026; some roles remain inferred rather than confirmed.
- Exact purchase dates, support contracts, and software versions were not fully available.
- Device purpose for several VMware guests is inferred primarily from hostnames and should be validated with administrative access.
- The wiring diagram is an inferred current-state map, not a certified as-built drawing.