



A School Network Plan for the Lalomanu Primary School: A Confederated Approach

By Richard Murphy
CEO, Lalomanu Foundation, Inc
May 28, 2026

1 Introduction

Currently, Sāmoa has a school network, which is derived from earlier school connectivity projects. The history of this network is found in the Foundation whitepaper *Telecommunications in Sāmoa since 2010 - focus: Internet Connectivity*, available on the Foundation website. Unfortunately, due to understaffing and the lack of operational funding, many schools do not have reliable connectivity. While the Ministry of Education, Sports, and Culture (MESC) promotes digital literacy, both for the teachers and the students, rural areas of the country need additional assistance. This plan is not set in stone and will be modified based on any school functional requirements, financial constraints, and policies published by the MESC and MCIT. This document is a design framework, not a blueprint. Once funding is acquired, an engineering implementation document will be created.

At the time of writing, the World Bank funded project titled Digitally Connected and Resilient Sāmoa (P180807) holds the most promise for resolving the reliability and sustainability conundrums that now exist. Also, the MESC has tendered connectivity for 80 schools and the tender closed on January 19, 2026. The tender awards page states that Digicel Sāmoa won Zone 3, which is where the Lalomanu Primary school is located. Additional details provided by the MCIT state that the service delivery will be through Starlink, at least initially. While better than no connectivity, Starlink typically does not deliver the full purchased capacity. The author's experience with it in the USA shows about 75% of the capacity is consistently delivered. It should also be noted that geo-location mechanisms will show the Sāmoan ground stations as being in New Zealand because this is where the regional Starlink interface to terrestrial networks is located.

1.1 Problem Statement

This plan is intended to address a number of issues that have plagued past school connectivity projects in Sāmoa:

- Long-term technical support for the schools
 - Software updates, security patches, new application installation, and usage reporting
 - Hardware maintenance
 - Resolving problems for the teachers (help desk)
- Scalability
 - Administering each school as an independent entity is a major job and cannot easily be done from Apia by the existing personnel of the MCIT
 - Economies of scale are lost

- No resource sharing between schools
 - The current models assume that all educational resources are outside of the schools and, in most cases, outside of Sāmoa. We envision that local content and inter-school communication could be very valuable to their teaching mission.
 - Given the envisioned capacity usage, there is no reason not to group several schools behind one firewall. This guarantees a uniform security policy with less staff effort and reduces the hardware cost.
- Training
 - This critical topic is addressed more completely in the Sustainability Plan. It is not feasible for this infrastructure to depend on technical support from Apia and likewise, it is not practical for the teachers to use digital resources without analyzing their requirements and providing them with the appropriate training. Self-education is good, some teachers will do this better than others, which can lead to inconsistent educational results.

1.2 Stakeholders

The key stakeholders are the teachers and their students. Everyone else is a secondary stakeholder whose needs may be addressed after those of the teachers and students. The secondary stakeholders are the MESC, the local community near Lalomanu, the MCIT, and finally the Lalomanu Foundation.

1.3 Success Criteria

Projects require metrics for measuring achieved goals, progress towards goals, and the return on investment¹ (ROI). These are implementation metrics. There are also operational metrics, the most important of which are discussed in 1.3.1

1.3.1 Key Performance Indicators (KPIs)

The KPIs can be divided into two areas: technical and educational.

- Technical (reported monthly)
 - Percentage of uptime per school. This refers to both Internet access and access to internal resources.
 - Number of hours spent troubleshooting and repairing ICT problems
 - Access statistics for key education resources
 - Capacity utilization and trends
- Educational (reported quarterly)
 - Number of students who use ICT resources during instruction
 - Number of times ICT resources were used by teachers during instruction
 - Classes incorporating ICT resources in the curriculum
 - At a more abstract level, student performance indicators, such as test scores, in order to measure the long-term effects of ICT usage.

1.3.2 Assumptions

This plan assumes the following:

- Electrical power availability. No immediate provision is made for solar power or uninterruptable power supplies (UPS).

¹ Here investment can be funding and hours spent working on the project

- A secure location for the equipment and storage server. This location should have proper ventilation and not be in an area where water or small animals can enter.
- A standard equipment half-rack or table for the equipment.
- For Lalomanu, a nearby location for the antenna mast to be installed and for guy wire anchors.
- At the Remote Sites, a roof area on the building housing the equipment for the Remote Node antenna.

1.3.3 Constraints

The most relevant constraints that affect the objectives are:

- Any reoccurring cost for marine fiber capacity that is apportioned to these schools.
- Limited technical staff
- Availability of spares
- Time for teacher training that does not interfere with their instructional duties
- Degree of support from the MESC and MCIT
- Support lifetime of each hardware item

2 Design Overview

The confederation we propose consists of the following schools:

Table 1- Schools in the Confederation

School	Level	Site #
Lalomanu	Primary	1
Vailoa	Primary	2
Lotopue	Primary	3
Aleipata	College	4
Saleaumua	Primary	5
Samusu	Primary	6

These schools will share an Internet connection, which will have failover routing. They will also share a single firewall, router, caching server, and storage server. Lalomanu is designated the Base Site (BS) and the other schools are Remote Sites (RS-VAI, RS-ALE, etc). Schools can communicate with each other without passing traffic through the Internet. Sharing the Internet connection both lowers the cost per school and provides higher utilization of the link capacity. This latter point is important because most providers of Internet connectivity sell capacity, not quantity².

Each school will have three WLANs: one for teachers, one for students and one for community users. The student accessible network is filtered by the firewall to block access to adult websites, malware, crypto mining, gambling websites, and social media. The teacher network is somewhat more permissive. The cache server will hold frequently used content, thus preventing wasted bandwidth across the marine cables. Community users are not the general public; these are parents, trainers, government employees, and other visitors at the schools. They essentially use their WLAN to access the Internet and they will have very restricted, if any, access to the servers. This mechanism avoids having to assign and revoke user credentials for accessing the teacher or student networks.

² These plans are usually called “capped” plans because they allow a certain maximum amount of data to be moved per day, week, or month. “Metered” plans charge by the amount of data moved.

This scheme allows one set of key devices to be maintained at one location by one person. It also provides for a common firewall policy across all the schools, again lowering the administrative overhead and chances of configuration errors.

The RSs connect to the BS using fixed wireless stations, which can provide up to 800Mb/s link capacity per school. If a school does obtain a fiber link, the wireless link will serve as a failover path in the case of a fiber cut.

The servers are based on Linux and do not incur any licensing fees. They support a large number of applications that are licensed without fees and can share files over the network with PCs running Windows. This is intended to foster collaboration among the teachers at these schools by sharing lessons, exercises, and projects. Given the bandwidth between the schools, a teacher at one school can conceivably address a class at a different school. This confederation can operate autonomously from other schools. If the MESC has a closed School Net in the same sense as the Samoa National Broadband Highway (SNBH), the confederation can participate in this as well.

The section on sustainability proposes several mechanisms for technical support and training. It is important to note that all seven schools do not have to be connected at the same time. The confederation can consist of the BS at Lalomanu and two other schools, with the remaining four added when the funding for equipment is available. This three-school group can be considered a prototype where connectivity and performance issues can be worked out before adding more complexity.

2.1 Traffic Engineering Strategy

2.2 Failover Behavior

In the current design, a single point of failure is possible due to there being no redundant routers, switches, and Tarana Base nodes at the Lalomanu site. This is a cost-saving measure and devices that fail can be replaced from a small pool of spares. Zero down-time is not a realistic goal given the funding for this design. However, if funding is available, a hot spare Base node and router will be acquired. Given that the primary times of usage of this network is during the day on days that school is in session, hot spares can be put into service after hours and service will be restored for the next school day.

Internet access failover is automatic and works as described here. The edge router has two static default routes, one for the interface to the Starlink router³ and the other for its own interface to the external fiber optic network. The fiber network route has a lower metric⁴, so it is preferred over the route through Starlink. If the fiber network connection goes down, the router interface goes down and the static route is no longer valid. The remaining static route becomes the only default route and traffic now uses the Starlink backup. It should be noted that other types of failures, such as network failures beyond the first hop, will require a secondary failure detection mechanism to trigger the failover. This is described in section 3.3.3.

³ The router is operated in bypass mode, which means it functions as a layer-2 switch and its own WiFi is disabled.

⁴ This metric is called Administrative Distance in Cisco devices.

2.3 User Segmentation

There are three classes of users for this infrastructure: teachers, students, and community. Here, community users are considered to be users who have a vested interest in educational outcomes at these schools and the most obvious of these are the parents of the students. Optionally, local community leaders, government officials, and chiefs could be included as community users.

This segmentation is useful for several reasons:

- Resource access control
- Security policy differences
- Capacity allocation and traffic engineering
- Prioritization of needs and of help requests

This segmentation implies that share resources, such as file and content servers, will need either two physical interfaces (one for each VLAN) or a single interface that supports VLAN trunks. Since the client networks are distinct from the server networks, router Access Control Lists (ACL) can prevent, for example, a student laptop from accessing a teacher laptop using the Remote Desktop Protocol (RDP). It will not be possible for these same laptops to share file systems with each other.

2.4 Content Strategy

Content may be divided into two groups: locally produced content and external content. Some content classes are: instructional (lessons, presentations, lectures, handouts, quizzes and exams), measurement (student records, test results, other assessments), training (for teachers), and references (digital libraries). There is also operational content that includes records of the KPIs, serial numbers of all devices, and other data to be used for planning purposes.

Other strategies will be created by the teachers, but one over-arching general strategy is to use local content as much as possible. Local content can be in Gagana Sāmoa and will be tailored for the local needs. Note that, while schools can share local content resources, they can also maintain content specific to each school. For example, a math teacher at school A may prefer to teach a concept in a certain way, which a teacher at school B has a better outcome when teaching the concept in a different way. Shared resources do not imply that “one size fits all.”

We assume there will close collaboration with the MESC so that the recommended content sources are readily available. This does not rule out any teacher at any of the schools in the confederation requested additional content or uploading their own content.

2.5 Scalability

At least on Upolu, we believe that groups of five to ten schools can adopt this model with the address and VLAN plan as described. In order to interlink the confederations, we require a VPN to be established between them. To keep the configuration simple, a Primary site and a Secondary site will termination point-to-point VPN links from each confederation. This is a dual hub-and-spoke topology and is described in the separate Confederation VPN Plan document.

3 Detailed Design

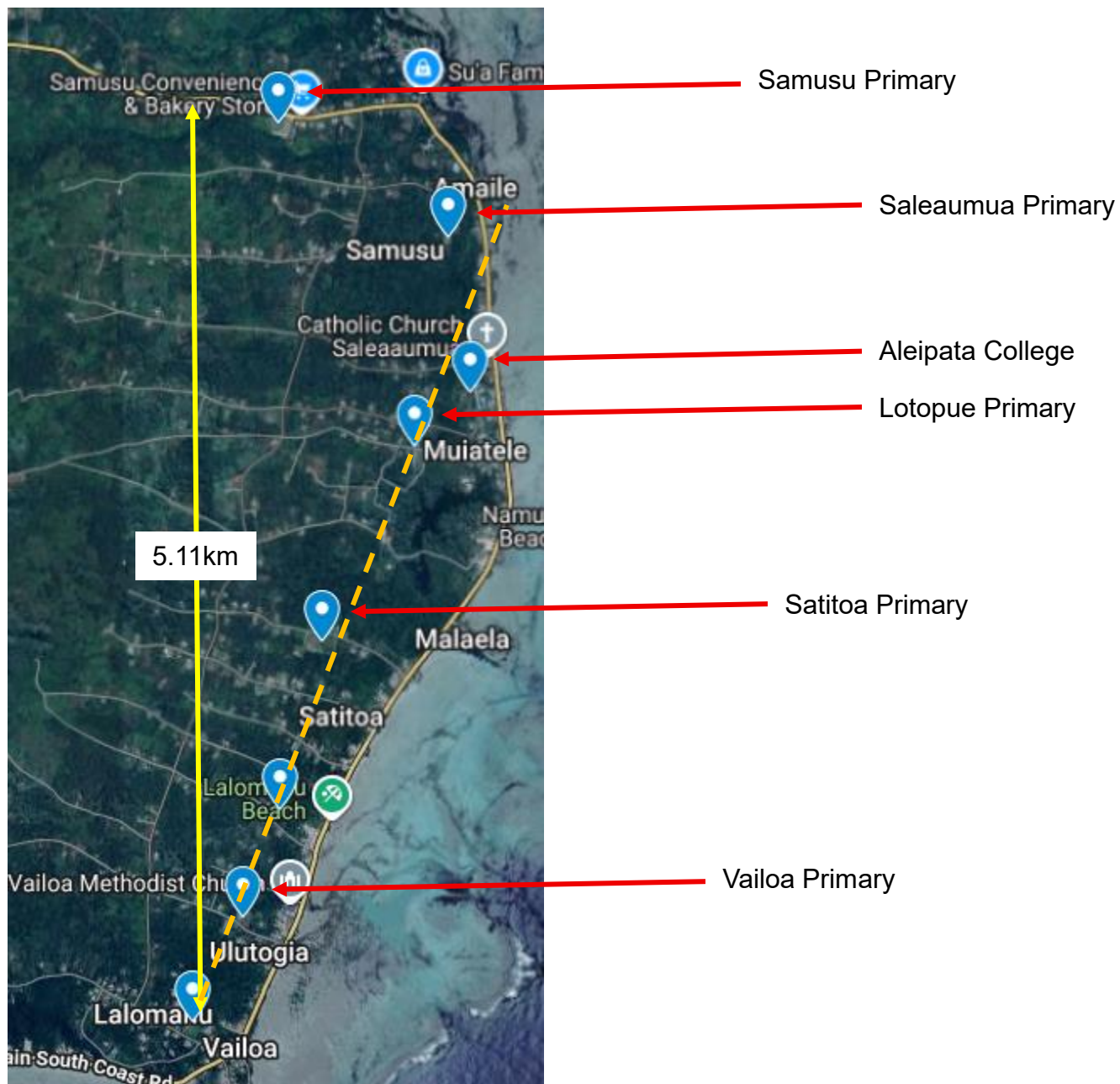


Figure 1- Proposed school confederation. The orange dashed line is the beam heading for fixed wireless, 22°

3.1 Definitions

The key to a good multi-site network plan is to design the address allocations, VLAN designations, and SSID conventions in such a way that allows configuration errors to be spotted immediately. In this plan, *addresses* refer to IPv4 addresses. While all of the specified equipment supports IPv6, the use of IPv6 is covered in a separate planning document, which is only applicable if multiple confederations are implemented.

Each school is assigned a Site number, assigned to variable **S**, as shown in Table 1. This number is used to construct the IP subnets, VLANs, and SSIDs used at each school. The *users* of a particular resource are defined as 0 = students, 1 = teachers, and 2 = community⁵. The variable **U** is one of the three values listed. SSIDs consist of <school name>-**U**, where the school's name is all lower case. Writing **SU** indicated the concatenation of the symbols in the variable; no arithmetic operations are implied. The follow table enumerates the key values for each site in the confederation.

Table 2 - Subnets, VLANs, & SSIDs by school (orange = implementation in the last phase)

School	Subnet 10.S.SU.0/24	VLAN SU	SSID ⁶ <school name>-U	Net name ⁷
Lalomanu	10.1.10.0/24	10	lalomanu-0	school-nets
	10.1.11.0/24	11	lalomanu-1	school-nets
	10.1.12.0/24	12	lalomanu-2	comm-nets
Vailoa	10.2.20.0/24	20	vailoa-0	school-nets
	10.2.21.0/24	21	vailoa-1	school-nets
	10.2.22.0/24	22	vailoa-2	comm-nets
Lotopue	10.3.30.0/24	30	lotopue-0	school-nets
	10.3.31.0/24	31	lotopue-1	school-nets
	10.3.32.0/24	32	lotopue-2	comm-nets
Aleipata	10.4.40.0/24	40	aleipata-0	school-nets
	10.4.41.0/24	41	aleipata-1	school-nets
	10.4.42.0/24	42	aleipata-2	comm-nets
Saleaumua	10.5.50.0/24	50	saleaumua-0	school-nets
	10.5.51.0/24	51	saleaumua-1	school-nets
	10.5.52.0/24	52	saleaumua-2	comm-nets
Samusu	10.6.60.0/24	60	samusu-0	school-nets
	10.6.61.0/24	61	samusu-1	school-nets
	10.6.62.0/24	62	samusu-2	comm-nets
Device management across all sites	10.239.254.0/24	254	mgmt-99	mgmt-net
Services network	10.239.253.0/24	253	N/A	serv-net
Firewall external	192.168.1.0/24	N/A	N/A	ext-net
Firewall internal	192.168.2.0/24	N/A	N/A	int-net

The network schematic in Figure 2 illustrates where each subnet appears in the network topology. All devices making up this network are manageable from Lalomanu. The *serv-net* network is inside the firewall and connects the inside router to the firewall, along with the squid cache and the shared file server. The inside router provides DHCP to all the school networks. The *ext-net* network connects the outside firewall interface to the outside router. The outside is needed for the automatic failover between the terrestrial network and the satellite backup network. If this feature is not initially required, then the outside firewall and *ext-net* are not needed. This design, however, will show this functionality in place. The outside router is need if the community network is implemented.

⁵ Community use will not be allowed until educational use is well established.

⁶ An SSID with "-5G" appended is specific to that band, otherwise the SSID is for the 2.4G band.

⁷ Used for labeling the topology diagram.

The scheme shown in Table 2 scales up to 238 schools, which is only a consideration if different confederations communicate directly with each other using a VPN that does not involve NAT. Otherwise, the scheme can simply be repeated for each group of schools. Confederations of more than ten schools are discouraged until the data on the actual utilization of the network has been collected over a school year.

The wireless access points at each school have the ability to map each SSID to the corresponding VLAN (student use or teacher use), so the teacher networks will remain secure from unauthorized access using the WLAN.

3.2 Layer 2

The layer-2 (link layer in most protocol hierarchies) is implemented as a combination of Ethernet, IEEE 802.11 XY protocols (WiFi), and point-to-point bridging between Lalomanu and the other schools using Tarana Wireless devices, which appear as Ethernet switches to the physically connected networks.

3.2.1 VLAN Usage

VLANs are used to create separate broadcast/multicast domains. Traffic between VLANs must pass through the confederation router; devices on the same VLAN can communicate directly. All Ethernet switches support VLANs and provide both trunk and access ports. The Tarana equipment supports VLAN stacking, but this is not needed in this design because all VLANs have unique IDs across the confederation. Only the VLANs in use at each site are sent to the Remote Node at that site. This last action is achieved by limiting the VLANs that may be sent over a given trunk (VLAN pruning), which saves bandwidth.

The mgmt-net VLAN exists on all devices inside the firewall and every managed device will have an administrative port on this VLAN. This is the only VLAN that spans the entire confederation. It is not associated with an SSID and it is not reachable from other VLANs.

3.2.2 Loop Prevention

All Ethernet switches will run STP even though the network has a tree-like topology with no loops. This will prevent problems in the case of erroneous connections that introduce loops.

3.2.3 Port Security

For fixed devices, such as computers in a lab or shared storage servers, an additional layer of security comes from restricting ports to the MAC address of the authorized devices. Unused ports will be administratively disabled. This will prevent anyone from using an unauthorized device even if they connect to an Ethernet port.

3.2.4 Wired

The wired network consists of cat6A cables and 12-port managed switches that support VLANs, trunk ports, and MDIX autosensing of the DTE state. Trunk ports will be restricted to specific VLANs. Power over Ethernet will be used if it is the easiest way to power access points.

3.2.5 Wireless

There are two types of wireless in use: (1) the fixed wireless system of Tarana Base Nodes (BN) and Remote Nodes (RN) and (2) 802.11 wireless access points for end-device connectivity. All SSIDs will be protected by strong passwords. Each SSID will be for a single band⁶ rather than having the same SSID for both bands. We assume that most student devices will connect using 2.4GHz as it has

better wall penetration. It may become necessary to hide the school specific SSIDs to avoid connection attempts from unauthorized users

The topology of the area where the school confederation is located on Upolu is ideal for fixed wireless communications. The main impediments to wireless signals are trees. The BN antenna will be installed a 10m mast on the grounds of the Lalomanu Primary School. The side of this mast will also be used as a mounting point for the Starlink ground station antenna. The BN and RN will use the lowest band for the links, again because it has better penetration than the higher frequency bands. We anticipate the antennas for the RNs may be roof-top mounted and not require a mast.

3.2.5.1 RF Planning

Radio frequency use will be planned using the guidelines in the Tarana Wireless *G1 NETWORK PLANNING AND DEPLOYMENT GUIDE*. Because this initial deployment does not involve any problematic terrain, large structures, or sources of RF interference, we do not envision any special needs in this area.

3.2.5.2 Capacity Planning

This plan assumes the network capacity is shared equally among the confederation member schools. There are two scenarios that disrupt this assumption: (1) overall capacity needs exceed the available external link capacity and (2) a single school dominates the capacity usage. The use of content caching should prevent situation (1) from occurring. Limitations on student services, like video streaming and the use of multiplayer interactive games, will also help. Situation (2) will require a determination as to whether the capacity domination by one school is warranted by legitimate education needs. The use of monitoring tools will allow for usage to be tracked, applications identified, and trends spotted before they cause capacity problems.

Of course, if the capacity is stressed by legitimate uses, the divide and conquer approach is one way to relieve this. The increase cost will be for additional external connections and another BN for the schools that are split into their own confederation. An alternative approach involves QoS tagging, traffic shaping, and in some cases, rate limits. We do not envision capacity exhaustion to be an issue until all of the schools fully integrated digital tools and techniques into their curriculum. This will require a sustained effort over several years for this integration to occur.

3.3 Layer 3

The Layer 3 design provides routing between VLANs, connectivity to the Internet, and failover between the terrestrial and satellite links. Inter-VLAN routing is performed by the inside router located at the Base Site (BS) in Lalomanu. Each VLAN defined in Table 2 is assigned a corresponding gateway address on this router. Host number one will always be the VLAN interface address on the router. Devices within a VLAN use this gateway to communicate with other VLANs or external networks.

3.3.1 Routing

Routing between the BS and the Remote Sites (RSs) is accomplished using static⁸ routes. Given the relatively small size of the confederation and the static, predictable topology, dynamic routing protocols such as OSPF are not required in the initial implementation. However, a dynamic routing protocol will be introduced in the future if additional confederations are interconnected or if multiple redundant paths are deployed.

⁸ Most are *connected* routes and a single installed *default* route

Routing between the different user VLANs will be limited by interface Access Control Lists (ACLs).

3.3.2 Network Address Translation

Network Address Translation (NAT) is implemented on the firewall to allow all internal networks (10.0.0.0/8 space) to access the Internet using a single public IP address or a small pool of addresses provided by the ISP. Another important IP address feature is the use of the DHCP protocol to dynamically assign interface addresses, gateway addresses, and DNS server addresses on each subnet. The pool of available dynamic addresses covers these host numbers: 128 to 254. Addresses with host numbers 2 to 127 are statically assigned to devices that are not mobile, such as the storage server, printers, and PCs in the computer lab. These assignments can be configured to work only for specific MAC addresses, which prevents unknown devices from attaching the network. One of the more important advantages to the addressing and VLAN scheme described here is that the IP address of a device reveals exactly where the device is. For example, an address of 10.7.70.130 is a device connected to the student WLAN at the Samusu Primary school.

3.3.3 Failover Mechanisms

Failover between the primary fiber connection and the Starlink satellite connection is handled by the outside router. This router continuously monitors the availability of the primary link. Upon failure, traffic is automatically redirected to the satellite link. When the primary link is restored, traffic is reverted based on predefined policies to avoid route flapping. The mechanism for this is the use of weighted static default routes, where the lower weighted path is preferred. This route is disabled if the target interface is not operational, which leaves the lower-weighted route to direct the traffic to the backup provider.

For network failures beyond the first hop external router, active probing is used to check reachability every 20 seconds. This uses an ICMP ping of a well-known IP address on the Internet. This handles cases other than link failure, like upstream router failures, routing flaps, and misconfigurations. The edge router must implement the Cisco **ip sla** functionality or the equivalent commands if the router is not a Cisco model.

3.3.4 Inter-confederation communications

If communication between confederations is required, site-to-site VPN tunnels will be established between the respective firewalls. These tunnels will allow secure routing of internal subnets without exposing them to the public Internet. This scenario requires the use of a dynamic routing protocol, since non-directly-connected subnets will need to be reached.

3.4 Security

Security is centrally enforced at the firewall located at the BS. This ensures consistent policy enforcement across all schools while minimizing administrative overhead.

3.4.1 Overview

Firewall rules are organized by user category:

- Student networks: Highly restricted
- Teacher networks: Moderately restricted
- Community networks: Restricted with time-of-day controls (optional)

Student network restrictions include blocking:

- Adult content
- Gambling sites

- Cryptocurrency mining domains
- Known malware and phishing domains
- Social media platforms (subject to MESC policy)

Teacher networks allow broader access but still block known malicious domains and high-risk categories.

Access to the management network (mgmt-net) is strictly limited to authorized administrative devices. This network is not routable from any user VLAN.

Administrative access to network devices is restricted by:

- Source IP (mgmt-net only)
- Strong authentication credentials
- Encrypted protocols (SSH, HTTPS)

All firewall activity, including blocked traffic and allowed sessions, is logged. Logs are retained locally and may be exported to a centralized logging system for long-term analysis. Security updates for all systems (routers, firewall, servers) are applied on a regular schedule, with critical patches applied as soon as practical.

3.4.2 Identity and Authentication

In the Lalomanu school confederation, FreeRADIUS and Zentyal will work together to provide centralized Authentication, Authorization, and Accounting (AAA) across both wired VLANs and WiFi SSIDs. Zentyal will act as the directory and identity management system, maintaining user accounts, group memberships (students, teachers, administrators), and shared file services for educational content. FreeRADIUS will integrate with Zentyal's directory (via LDAP) to authenticate users when they connect to the network—whether through student or teacher SSIDs or their respective VLANs. Each login attempt will be validated against the central directory, ensuring that only authorized users gain access, while simplifying account management for the two IT administrators.

Authorization policies in FreeRADIUS will enforce role-based access controls tied to VLANs and SSIDs. Students connecting to the student SSID or wired VLAN will be placed into a restricted network segment with access to shared learning materials on the Zentyal server, filtered internet access, and limited administrative privileges. Teachers, authenticated through a separate SSID/VLAN, will receive broader access rights, including instructional resources, grading systems, and potentially elevated bandwidth or fewer content restrictions. Accounting features in FreeRADIUS will log connection times, session durations, and resource usage, giving administrators visibility into network activity across roughly 1,150 users. This design ensures secure, scalable access control while allowing both groups to seamlessly share common educational resources hosted centrally on Zentyal.

3.5 Monitoring and Management

A centralized monitoring system is deployed at the BS to provide visibility into the health and performance of the entire confederation. We believe that the open source Zabbix⁹ package offers all of the tools and data collection needed to provide a real-time window into the health and performance of the entire seven school network. This package will allow remote monitoring from Apia and from outside of Sāmoa.

⁹ <https://www.zabbix.com/>

The monitoring system tracks:

- Device availability (routers, switches, APs, wireless links)
- Bandwidth utilization per site and per VLAN
- Latency and packet loss across wireless links
- CPU, memory, and disk usage on servers
- Internet link status (primary and backup)

Alerts are generated when predefined thresholds are exceeded, such as:

- Device offline
- Link degradation
- High bandwidth utilization
- Server resource exhaustion

Alerts can be delivered via email or SMS to designated support personnel.

Historical data is retained to support:

- Capacity planning
- Troubleshooting intermittent issues
- Reporting to stakeholders (e.g., MESC, MCIT, funding agencies)

A simple dashboard is provided to give a high-level view of network status across all schools. When the proper firewall rules are installed, monitoring can be done from the MESC and MCIT or locations outside of Sāmoa. We envision monthly reports on each confederation being provided to the MCIT for further technical analysis and planning purposes.

3.6 Services

Other services for the schools, such as color printing, may be added at a later date. The implementation of these services is dependent on space and power constraints at the Base Site.

3.6.1 Squid cache

A caching proxy server is deployed to reduce bandwidth consumption over the Internet link. Frequently accessed content is stored locally, significantly improving response times and reducing repeated downloads over expensive international links.

The cache is particularly effective for:

- Software updates
- Educational videos
- Frequently accessed web resources

Cache size and retention policies are configured based on available storage and observed usage patterns.

3.6.2 Shared storage

A centralized file server provides shared storage accessible to teachers across all schools. This enables:

- Sharing of lesson plans
- Distribution of educational materials

- Collaborative development of teaching resources

Access controls are implemented to ensure that only authorized users can read or modify shared content. Regular backups of the shared storage system are performed to prevent data loss. Backups may be implemented with USB connected SSD drives and scripts to mirror file folders each night. Incremental backups may be used if there are large amounts of data to be protected.

3.6.3 Additional services

The following services may be deployed as needed:

- Local DNS caching resolver to reduce lookup latency and external bandwidth usage
- Offline educational content (e.g., Wikipedia, Khan Academy resources) for use during outages
- Software update mirrors for common operating systems and applications
- Basic communication tools (e.g., internal messaging or video conferencing between schools)

The implementation of additional services will be driven by teacher and student needs and the securing of funding for the needed hardware and software. A prerequisite for implement any service within the confederated network is sustainability.

4 Sustainability

Long-term sustainability is critical to the success of the confederation. A hybrid support model is recommended:

- One centrally trained technician responsible for the BS and overall network health
- One designated staff member at each school with basic technical training

This approach balances technical expertise with local responsiveness.

Training is provided at three levels:

1. Basic user support (teachers)
2. School-level technical support (designated staff)
3. Advanced network administration (central technician)

A modest monthly budget per school should be established to cover:

- Equipment replacement
- Internet service costs
- Stipends for support personnel

Spare equipment (switches, access points, cables) should be kept at the BS to allow rapid replacement in the event of failure. All equipment should be selected with a lifecycle of approximately 3–5 years, after which replacement or upgrade is planned.

Partnerships with vendors and donors can help reduce capital and operational costs. The Lalomanu Foundation believes a powerful operational synergy can be achieved with a partnership with the **Department of Information Technology and Systems** at the National University of Sāmoa.

See the Sustainability Plan for a detailed scenario, which would involve semester-long internships for the NUS students. These students would gain valuable experience across a range of network technologies while supporting a particular confederation of schools.

5 Implementation Plan

The deployment will proceed in three phases.

Phase 1 – Pilot (3 Schools)

- Deploy BS at Lalomanu
- Connect two Remote Nodes. Connecting the closest and the most distant schools will help in tuning the signal quality of the fixed wireless bridged network
- Validate connectivity, performance, and reliability
- Train initial staff

Phase 2 – Expansion

- Add remaining schools incrementally
- Monitor network load and adjust configuration as needed
- Expand training to additional staff

Phase 3 – Optimization

- Fine-tune firewall rules and QoS policies
- Optimize caching performance
- Introduce additional services as needed

Phase 4 – Allow community users with the permission of the school principals and PTA heads

A phased approach reduces risk and allows lessons learned to be incorporated into later stages. It also reduces the initial funding outlay.

6 Risk Analysis

The following risks have been identified:

- Power instability
 - Mitigation: Use UPS systems and surge protection; Use solar charging.
- Equipment failure
 - Mitigation: Maintain hot spares of critical devices at the BS; maintain the proper protective environment (temperature, humidity, filtered power) to prevent damage
 - Remediation: Keep off-line spares at Lalomanu for quick deployment to any school; full or bare metal backups will be kept in case of server failure
- Fiber outages
 - Mitigation: Automatic failover to satellite link
- Wireless link degradation (weather, vegetation)
 - Mitigation: Periodic inspection and continuous performance monitoring of wireless links
- Limited technical expertise
 - Mitigation: Training program and centralized support
- Theft or vandalism
 - Mitigation: Secure equipment installations and community involvement
- Bandwidth saturation
 - Mitigation: Use caching and traffic prioritization

7 Glossary

Term	Definition
ACL	Access Control List (mechanism for limiting traffic through specified interfaces)
DHCP	Dynamic Host Configuration Protocol
DTE	Data Terminal Equipment
east-west	Traffic within a data center; can be between VLANs
IP	Internet Protocol; can refer to either version
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
MAC	Media Access Control (address – 48 bits)
MCIT	Ministry of Communications and Information Technology
MDIX	Medium Dependent Interface Crossover
MESC	Ministry of Education, Sports, and Culture (of Sāmoa)
NAT	Network Address Translation
SSID	Service Set Identifier (essentially the wireless network name)
STP	Spanning Tree Protocol
VPN	Virtual Private Network

Lalomanu Confederation Network

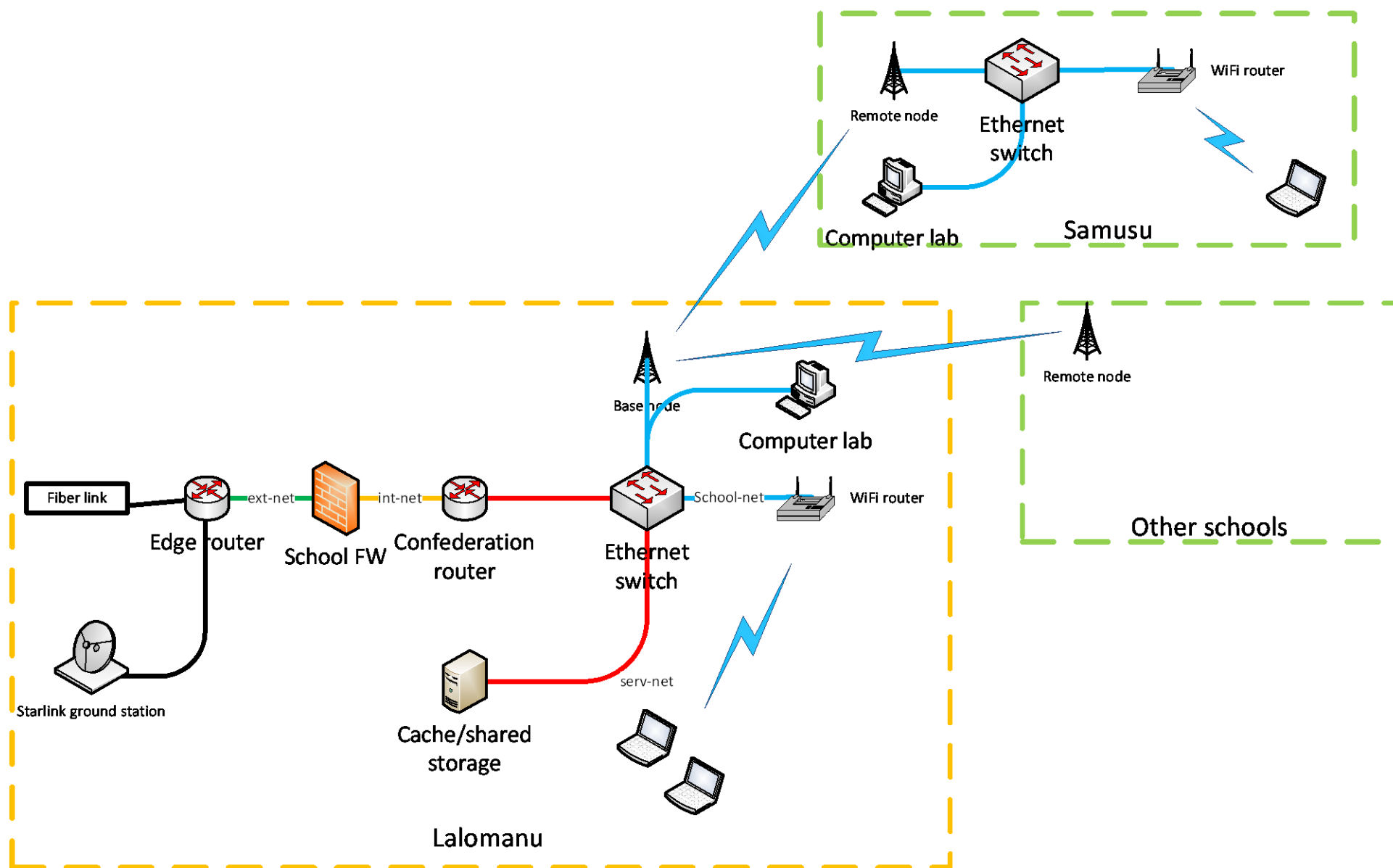


Figure 2 Topology of the Confederation Network