Seamus Company Network Infrastructure Refresh Report

Network Infrastructure rebuilD

Damian Jevon Yates

Western Governors University

2020

[Problem Overview 3](#_Toc49666847)

[Related Works Review 4](#_Toc49666848)

[Changes to Infrastructure Environment 7](#_Toc49666849)

[Proposed Methodology Explained 8](#_Toc49666850)

[Goals, Objectives, and Deliverables 10](#_Toc49666851)

[Pre-Deployment Objectives 10](#_Toc49666852)

[Goal 1 – Audit Existing Network Infrastructure 10](#_Toc49666853)

[Goal 2 – Procure and Stage Services and Products 10](#_Toc49666854)

[Deploy & Monitor Objectives 11](#_Toc49666855)

[Goal 3 – Distribute Collapsed Network 11](#_Toc49666856)

[Goal 4 – Deploy and Configure Hardware 11](#_Toc49666857)

[Goal 5 – Post Network Installation Cleanup 12](#_Toc49666858)

[Goal 6 – Validate High Availability between Core, MDF, and IDF’s 13](#_Toc49666859)

[Goal 7 – Validate High Availability Core, Firewall Stacks, and Remote Sites 13](#_Toc49666860)

[Goal 8 – Migrate Wireless LAN Controller 13](#_Toc49666861)

[Goal 9 – Implement SNMPv3 13](#_Toc49666862)

[Post-Production Deployment Objectives 14](#_Toc49666863)

[Goal 10 – Decommission old hardware 14](#_Toc49666864)

[Goal 11 – Document and Diagram New Seamus Infrastructure 14](#_Toc49666865)

[Project Timeline 15](#_Toc49666866)

[Unexpected Happenings 16](#_Toc49666867)

[End of Project Results 17](#_Toc49666868)

[Works Cited 18](#_Toc49666869)

[Artifact 1 – Logical High-Level Network Diagram 20](#_Toc49666870)

[Artifact 2 – Original Logical Low-Level Network Diagram 21](#_Toc49666871)

[Artifact 3 – Logical Low-Level Network Diagram 22](#_Toc49666872)

# Problem Overview

The Seamus Renton Office and satellite offices were utilizing equipment and routing protocols that would not meet the needs of the new applications and hardware solutions that were to be implemented next year. With the completion of the project, both the deployment and migration of Seamus Corporation under-performing network infrastructure to a solution that now exceeds the requirements of the new application platform and operations. Seamus network infrastructure now has the capacity, resiliency, and security needed to meet government regulations, application platform requirements, and allows for future growth and expansion in the future.

Initial review of the previous infrastructure environment prompted our engineers to construct a plan to replace and configure both the core infrastructure and distributed elements at the various remote sites. Each of the core switches, firewalls, and associated cabling was replaced. All uninterrupted power supply & conditioning units were updated to meet the increased power requirements of the new infrastructure. Each of the distribution and access switches was replaced. Each of the firewalls, core and distribution switches were placed in a highly resilient configuration to mitigate equipment, service, or any other single break in communications within the network. To ensure minimal operational interference, engineers requested several windows for maintenance in which all disruptive processes were completed allowing all services and functions of the company to remain intact at all other times when possible.

Damian J. Yates, LLC estimated that the project cost of the project would be $201,500 and include 108-man hours provided by Damian J. Yates LLC. This projection included all hardware, cabling, as well as 2-year replacement warranty of the hardware. The actual cost of the project ended up being $199,941 with a total of 99-man hours being committed to the project. Damian J. Yates, LLC reaffirmed its commitment to providing 90 days of support to Seamus at no cost.

# Related Works Review

With the modernization of Seamus Corporation technology, the choice to use technology that adheres to an Open Standard adds several fiscal and operational benefits. Completing the move from the Cisco dependent routing protocol (EIGRP) to OSPF was the first step in this journey. Since the IETF has established OSPF as the standard for interior routing (Conde, 2016), all most every layer 2 device manufactured today supports the protocol. The previous infrastructure environment could run multiple routing protocols but due to the age and rated throughput of the equipment, it was suggested to Seamus Corporation to purchase nonproprietary hardware that supported OSPF natively. Juniper’s hardware cost, as well as its ability to accommodate the move to OSPF while ensuring bandwidth, throughput capacity, security, and resilience for the future applications, has placed the company in a better position for future expansion and integration of other infrastructure hardware.

The Seamus network used to function as a “Collapsed Core” design. Though this was not by design, it did not provide the needed resilience and bandwidth management controls (Allied Telesis, 2020). The smaller infrastructure warranted a collapsed core design at the time, keeping management and routing inside the Distribution/Aggregation layer of the network. This allowed routing and access changes to be controlled downstream from the core router or switch. With the new endeavors of the company and expected growth, the new infrastructure design segregates the functions within the network into 3 zones. Access Layer, “which provides user access to the network”. Distribution Layer, “which provides policy-based connectivity and controls the boundary between the access and core layers.” Core Layer, this layer “provides fast transport between the distribution switches within the enterprise campus. (CyberSecurity & Infrastructure Security Agency, 2017)” ( Cisco Networking Academy, 2014)

The implementation of SNMP within the infrastructure of the Seamus network allows for monitoring, reporting, and alert on the health of the infrastructure. Due to a known vulnerability that “allows attackers to read and modify any SNMP object”, special care was taken to secure the protocol and each device to be monitored (Taschner & Warren, 2008). This was accomplished by using SNMPv3 along with MIB whitelisting using SNMP views. The added whitelisting ensures that information cannot be written or read from unless the information is needed for monitoring or normal device re-configuration. (CyberSecurity & Infrastructure Security Agency, 2017) Before the implementation, Seamus engineers and technicians responded to faults within the infrastructure and resolved the issue without a firm understanding of why the fault which prevented them from taking the necessary action needed to mitigate the problem in the future. SNMP now allows Seamus to provide real-time and archive performance metrics, access-list violations, as well as a record of changes that are made.

To ensure that optimal performance and ROI, the use of converged networking was implemented at the corporate headquarters datacenter. This move ensures Seamus's ability to quickly respond to anticipated and unexpected needs to increase capacity. Projected leveraging of VOIP technologies out to remote sites and telecommuters, and the increased demand for data and video transmissions over internal and external networks are all factors that are in the future, planned or not. With the implementation of converged networking a reduction of the complexity and need for multiple cabling runs to and from network and storage devices as well as the servers that rely on them, have been realized. Also, increased control over QoS, availability, and traffic shaping capabilities have ensured that the network is prioritizing all traffic across its infrastructure (Belmans, Lambrette, Gurley, & Puopolo, 2009) thus reducing the poor performance of voice and video due to increased data demands during peak periods.

The improvements provided by converged networking has provided an immediate impact on the ROI on current operations at Seamus. The improved control and management capabilities introduced with the new infrastructure augments Seamus Corporation's ability to dynamically adjust availability, capacity, and security in direct response to the demands placed upon the network. (Hameed, Raza, Atta, & Lee, 2009) The move to OSPF will be critical in achieving the dynamic capability of the network allowing multiple fault-tolerant routes within the infrastructure. As additional resources are brought online to meet demands, the need to configure routes to new segments of the network manually is no longer needed. The 3-tier network design and improved network core configuration allow Seamus to easily bring up new segments of the network dynamically without adverse effect to performance or availability. Visibility and response to the performance, availability, and configuration of the network-enabled using SNMP will ensure prompt and appropriate responses to events detected and projected through monitoring and analysis of captured data.

# Changes to Infrastructure Environment

Seamus Corporation was operating on infrastructure equipment where 65% of the devices had ≤ 30 days before reaching the end of life/support. Seamus Corporation network equipment comprised of Cisco Catalyst switches and routers as well as two Cisco ASA firewalls, a single Cisco Wireless Controller, and a clustered implementation of Cisco Unified Communications Application Platform. The wireless site survey at each location revealed that 80% of the wireless access points in use were found to be running outdated firmware that did not contain security patches for numerous identified vulnerabilities. Physical servers totaled 52 which required a total of 2 switches to provide single network connectivity to each device.

Currently, Seamus is operating on the latest revision of Juniper switches and routers. Each device is under a support contract with Juniper for 3 years. The ASA firewalls were replaced with Fortinet firewalls with the latest revision of the firmware and security software. 5 Warranty on these devices as the size and capability of these firewalls are expected to suit the needs of the company well beyond that period. Both the Wireless controller and UCS implementation remains in place at Seamus as separate projects are in place for their replacement soon. The 52 servers have been migrated over to the new network in preparation for the Server Consolidation Project that is currently in the planning phase. Environmental monitoring is no in place within the data center to allow for the monitoring of the climate within the datacenter. This additional monitoring is being used to gauge if augmentation of the power and cooling systems are needed.

# 

# Proposed Methodology Explained

The Waterfall methodology process was used to ensure a systematic approach to design, implementation, and maintenance of the new technology being proposed. The waterfall methodology is a structured methodology that requires the completion of one step in the process before the next can begin. Each of the seven steps Conception, Initiation, Requirements, Design, Implementation, Verification, and Maintenance were completed in succession.

The Conceptualization step comprised the Seamus Corp. identifying the need to modernize their network to accommodate the new technologies and goals the organization planned to embrace. Once the concept of delivering products and services via the cloud was realized, it was also noted that numerous key systems within the org would not support the desired functionality. The Initiation step of the methodology saw the formation of the project team which performed a Cost Benefits Analysis (CBA) to assess the desired goals, the perceived need, and the potential cost of the project to the organization.

With the completion of the CBA, the Requirements step of the methodology was initiated and work began on establishing the scope, objectives, and required deliverables of the project based on the concepts and ideas that were derived in the Conceptualization step. The project team began the work of collecting the requirements needed for each of the project goals and performed an analysis of the information gathered to produce a requirements document.

The creation of the requirements document marked the start of the Design step of the methodology process. The document was used to convey a clear and concise understanding of what was required to achieve the overall goals of the project and how to arrive at the final product. That understanding was used to produce a project plan which included the finalized scope, individual objectives, and deliverables that were needed to achieve the project's goal.

The Implementation step of the methodology started once the project plan was finalized. Products, Services, and other resources were brought together per the project plan to achieve the desired result of the project. Once the implementation of the project plan was completed, validation of the deployed solution began. A customer acceptance validation (CAV) was also conducted to ensure that Seamus Corp. had the opportunity to evaluate the performance of the solution to ensure it meets their expectations. Receipt of the results from the Verification step marked the beginning of the Maintenance step of the methodology. Feedback from the validation teams and the CAV were leveraged by the engineers to address reported deviations and deficiencies. Once all deficiencies are resolved during the validation stage, the solution was handed over to the customer for use, maintenance, and support.

# Goals, Objectives, and Deliverables

## Pre-Deployment Objectives

Pre-deployment objectives of the project included the goals needed in the collection and storage of performance data on all infrastructure assets. The procurement of all needed services, manpower, and hardware purchased, received, and staged occurred successfully.

### Goal 1 – Audit Existing Network Infrastructure

(Started Day 1. Completed in 2 days.)

Objective 1a - (**NOT PRODUCTION IMPACTING):** Collected Logs and KPI data from the datacenter, servers, network, and application devices and platforms.

Deliverable – Correlated logs and KPI data from the datacenter all network, server, and application devices and platforms were collected and stored on a secure medium.

Objective 1b – (**NOT PRODUCTION IMPACTING):** Collected existing Datacenter, Network, Server, and Application diagrams and documentation along with associated business processes surround each.

Deliverable – Electronic and paper diagrams and documentation of data center, network, server, and applications as well as the business processes supported by and supporting the aforementioned items were collected and stored in a secured location.

### Goal 2 – Procure and Stage Services and Products

(Started Day 1. Completed in 2 days. All vendors met or exceeded expected delivery times)

Objective 2a – (**NOT PRODUCTION IMPACTING):**  Created work orders for Datacenter power storage, conditioning, and generation needs, Datacenter Environmental Upgrades, Datacenter telecommunication additions, and modifications.

Deliverable – Confirmed Time and Date of vendor/contractor’s arrival.

Objective 2b – (**NOT PRODUCTION IMPACTING):**  Created work orders for Network, Server, and supporting equipment.

Deliverable – Tracking number obtained for each purchased item with time and date of arrival information obtained for all hardware.

## Deploy & Monitor Objectives

Deploy and Monitor Objectives included the goals needed to successfully install, configure, and monitor the new infrastructure equipment.

### Goal 3 – Distribute Collapsed Network

(Started Day 1. Completed in 12 days. 3a started on day 8.)

This goal required engineers to break-out the collapsed network into individual operating domains.

*Objective 3a – (****DEPENDENT ON GOAL 2) (NOT PRODUCTION IMPACTING):*** *Configured and Tested Routers, Switches, and Security devices.*

*Deliverable – Configured tested hardware upon arrival on day 8 of the project. Hardware packaged for shipment to designation locations on day 9 and shipped on day 10.*

*Objective 3b –* ***(NOT PRODUCTION IMPACTING):*** *Built base images and network configurations for new servers.*

*Deliverable – Server images & network device configurations stored on a secured local network share.*

### Goal 4 – Deploy and Configure Hardware

(Start Day 11. Completed in 9 days)

Objective 4a – (**DEPENDENT ON GOAL 3)** (**PRODUCTION IMPACTING)**: Installed new hardware and segregated routing layers. Pseudo “collapsed core” infrastructure distributed to allow networking assets to function within specific operating domains (OSPF Area).

*Deliverable – Old hardware powered off and removed from racks. New Hardware installed.*

*Deliverable – OSPF routing configured on the new infrastructure core.*

Objective 4b – (**PRODUCTION IMPACTING)**: Established redundant connections to and from core and distribution networking equipment. Coordinated with Network Engineers to test uplink and performance.

Deliverable – New Hardware configured for high availability.

Objective 4c – (**PRODUCTION IMPACTING):** Redistributed the existing EIGRP routes to OSPFv3 routing protocol for Corporate office network equipment. Coordinated with Network Engineers to test uplink and performance.

Deliverable – Corporate routers update route information via OSPF.

Objective 4d – (**PRODUCTION IMPACTING):** Installed new hardware and redistributed the existing EIGRP routes to OSPFv3 routing protocol for Snoqualmie office network equipment. Coordinated with Network Engineers to test uplink and performance.

Deliverable – Remote office router update routing information via OSPF.

Objective 4e – (**PRODUCTION IMPACTING):** Installed new hardware and redistributed the existing EIGRP routes to OSPFv3 routing protocol for Puyallup office network equipment. Coordinated with Network Engineers to test uplink and performance.

Deliverable – Remote office router update routing information via OSPF.

Objective 4f – (**PRODUCTION IMPACTING):** Installed new hardware and redistributed the existing EIGRP routes to OSPFv3 routing protocol for Auburn office network equipment. Coordinated with Network Engineers to test uplink and performance.

Deliverable – Remote office router update routing information via OSPF.

Objective 4g – (**PRODUCTION IMPACTING):** Installed new hardware and redistributed the existing EIGRP routes to OSPFv3 routing protocol for Olympia office network equipment. Coordinated with Network Engineers to test uplink and performance.

Deliverable – Remote office router update routing information via OSPF.

### Goal 5 – Post Network Installation Cleanup

(Start day 21. Completed in 4 days)

Objective 5a (**PRODUCTION AFFECTING):** Cleaned up and consolidated VLAN/Subnet databases across the network.

Deliverable – VLAN databases consolidated to Core Distribution Layer.

### Goal 6 – Validate High Availability between Core, MDF, and IDF’s

(Start day 25. Completed in 1 day)

This Goal required engineers to coordinate simulated failures to network links between MDF Core switch and IDF switches throughout the company.

Goal 6 – **(PRODUCTION AFFECTING):** Validated redundancy and fault alerting at the core and distribution layer.

Deliverable – Network resilience confirmed with all uplinks between devices in Core Network being offline.

### Goal 7 – Validate High Availability Core, Firewall Stacks, and Remote Sites

(Start day 26. Completed in 2 days)

Engineers coordinated managed outages between HQ and all remote sites.

Objective 7a – **(PRODUCTION AFFECTING):** Validated load balancing, fault alerting, and failover services between core, MDF, IDF, and remote sites.

Deliverable – Network operations continuity confirmed despite the loss of communications on any one link between MDF and all IDF’s at Corporate HQ.

### Goal 8 – Migrate Wireless LAN Controller

(Start day 28. Completed in 1 day)

Objective 8a – **(PRODUCTION AFFECTING):** Migrated Wireless LAN Controller from old Infrastructure to the virtual interface on the firewall.

*Deliverable – All wireless communications now traverse new infrastructure.*

### Goal 9 – Implement SNMPv3

(Start day 29. Completed in 2 days)

Objective 9a – **(NON-PRODUCTION AFFECTING):** Implemented SMNPv3 on each network device and disabled all older protocol versions.

*Deliverable – Alerting and Monitoring of the network are now possible.*

## Post-Production Deployment Objectives

Post-production objectives encompassed the goals needed to deliver the solution to the customer complete with documentation and metrics.

### Goal 10 – Decommission old hardware

(Start day 31. Completed in 2 days)

All out of band hardware is now decommissioned per Seamus Corporation policy.

Objective 10a – Devices either passed or nearing the end-of-life/end-of-support date have been decommissioned per Seamus Corporation's existing technology refresh policies. Reference “In Use Equipment EOL” table below

Deliverable – Old hardware from Seamus's previous infrastructure footprint reduced by 75%. Legacy hardware that remains in use will be decommissioned 365 days.

### Goal 11 – Document and Diagram New Seamus Infrastructure

(Start day 29. Completed in 8 days)

Objective 11a – (**NOT PRODUCTION IMPACTING):** Collected existing Datacenter, Network, Server, and Application diagrams and documentation along with associated business processes surrounding each.

Deliverable – Diagram of Physical layout of Seamus Network Infrastructure produced

Deliverable – Diagram of Logical layout of Seamus Network Infrastructure produced

Deliverable – Diagram of Physical layout of Seamus Power Distribution Infrastructure produced

*Deliverable –* Diagram of Logical layout of Seamus Power Distribution Infrastructure produced

*Deliverable –* Diagram of Physical layout of Seamus Network Infrastructure Wiring produced

*Deliverable –* Diagram of Port Map of all Switch, Router, Firewall, Dark and IDF ports produced

# Project Timeline

The project start date was tentatively set for November 30, 2020. The actual start date was November 30, 2020. Timeline is as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Start Date** | **End Date** | **Deliverable** | **Projected**  **Duration** | **Actual Duration** |
| 11/30/20 | 12/01/20 | Collection of Infrastructure Documentation and KPI completed | 1 - 3 days | 2 days |
| 11/30/20 | 12/01/20 | New Equipment and services ordered | 1 - 3 days | 1 day |
| 11/30/20 | 12/15/20 | New hardware received, tested, and preconfigured  Base device images and configuration generated and stored securely | 7 - 14 days | 12 days |
| 12/15/20 | 12/29/20 | New hardware installed  Old hardware powered off  Establish high availability for all relevant devices  Redistribute the existing EIGRP routes to OSPFv3 routing protocol at each site | 5 - 7 days | 9 days |
| 12/29/20 | 1/05/21 | Cleanup and consolidation of VLAN/Subnet databases across network completed | 3 - 5 days | 4 days |
| 1/05/21 | 1/05/21 | Validated redundancy at the core and distribution layer | 1 - 3 days | 1 day |
| 1/06/21 | 1/07/21 | Validated failover services between firewall and remote site IDF’s | 1 - 3 days | 2 days |
| 1/07/21 | 1/07/21 | Migrate *Wireless LAN Controller* from old Infrastructure to the virtual interfaces on the firewall | 1 day | 1 day |
| 1/08/21 | 1/09/21 | Implement SMNPv3 | 2 days | 2 days |
| 1/08/21 | 1/08/21 | Decommission old hardware | 1 -3 days | 1 day |
| 1/08/21 | 1/19/21 | Document and Diagram New Seamus Infrastructure | 7 – 10 days | 8 days |

Thanks to the expedient and prompt delivery of services and product by 3rd party vendors, good weather, and reliability of the engineering and technical staff, the project completed ahead of the anticipated date. Acquisition of KPI and documentation completed without incident thanks to the meticulous record-keeping and documentation of the administrative staff and reporting tools utilized by the IT department. The acquisition of the hardware and its delivery on time played a pivotal role in the completion of Goal 3 ahead of schedule. This allowed our staff to begin work on pre-configuring and build base images for devices. Goal 4 encountered two problems during its implementation. One employee had car trouble on day 3 of the task and another fell ill 2 days before the start of the task. The engineering team, in conjunction with the installation technicians at the remote sites, performed flawlessly to implement and validate connectivity between the remote sites and corporate HQ. Management and the installation team are to be commended for completing the decommissioning process ahead of schedule. Lastly, the delivery of all artifacts and documentation concerning this project produced by the engineering and design team aided in ending the project ahead of the projected date.

# Unexpected Happenings

This project had very little deviation in its execution from the projected timeline and expected deliverables. There were several absences within the installation tech team which had an adverse effect on Goal 4. The project plan had an accommodation for the loss of 8-man hours, but the number of man-hours lost exceeded that buffer. To remain within the expected time to complete, several of the management staff stepped in to assist with remote office network communications set up. There was a blocking incident during Objective 4g that required the engineering team to troubleshoot the failure of the link between the sites. Site services were restored 2 hours after the initial report with the assistance of the circuit provider.

# End of Project Results

With the completion of this project, Seamus Corporation will have begun the new year with a brand new highly available, secured, and efficient network. Network efficiency, throughput, and resilience will have increased by an estimated 20%. Security within and at the borders of the infrastructure will now be driven by machine learning to aid in mitigating threats in real-time. Seamus Corporation will no longer suffer from outages caused by a single failure within the infrastructure or between sites.

At the end of the 90 days of post support, Damian J. Yates, LLC will present Seamus Corporation with a comprehensive report on the performance of the network since its inception and use on Jan 19. This report will show nominal network stress during peak times, results of scheduled test failover transitions, and descriptive fault alerts via SNMP. Because Seamus Corporation has no prior network performance metrics, Damian J. Yates, LLC will make itself available at 30 and 60-day point to provide a benchmark comparison of network flow and operations since the implementation of its new operations processes, hardware, and software installation. It is with these reports Damian J. Yates, LLC will show that the investment made in the new infrastructure meets, and hopefully exceeds the anticipated ROI.

# Works Cited

Cisco Networking Academy. (2014, 05 09). *Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design*. From Cisco Press: http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4

Allied Telesis. (2020). *Allied Telesis.* From Allied Telesis: https://www.alliedtelesis.com/sites/default/files/documents/white-papers/distributed\_collapsed\_backbone\_reva.pdf

Belmans, W., Lambrette, U., Gurley, H., & Puopolo, S. (2009, August). *Converged Network - IT Services.* From Cisco: https:///www.cisco.com/c/dam/en\_us/about/ac79/docs/wp/Network\_IT\_Services\_Part\_1.pdf

Coltun, R., Ferguson, D., Moy, J., & Lindem, A. (2008, July). *RFC 5340 - OSPF for IPv6.* Wilmington, DE: IETF. From https://datatracker.ietf.org/doc/rfc5340/?include\_text=1

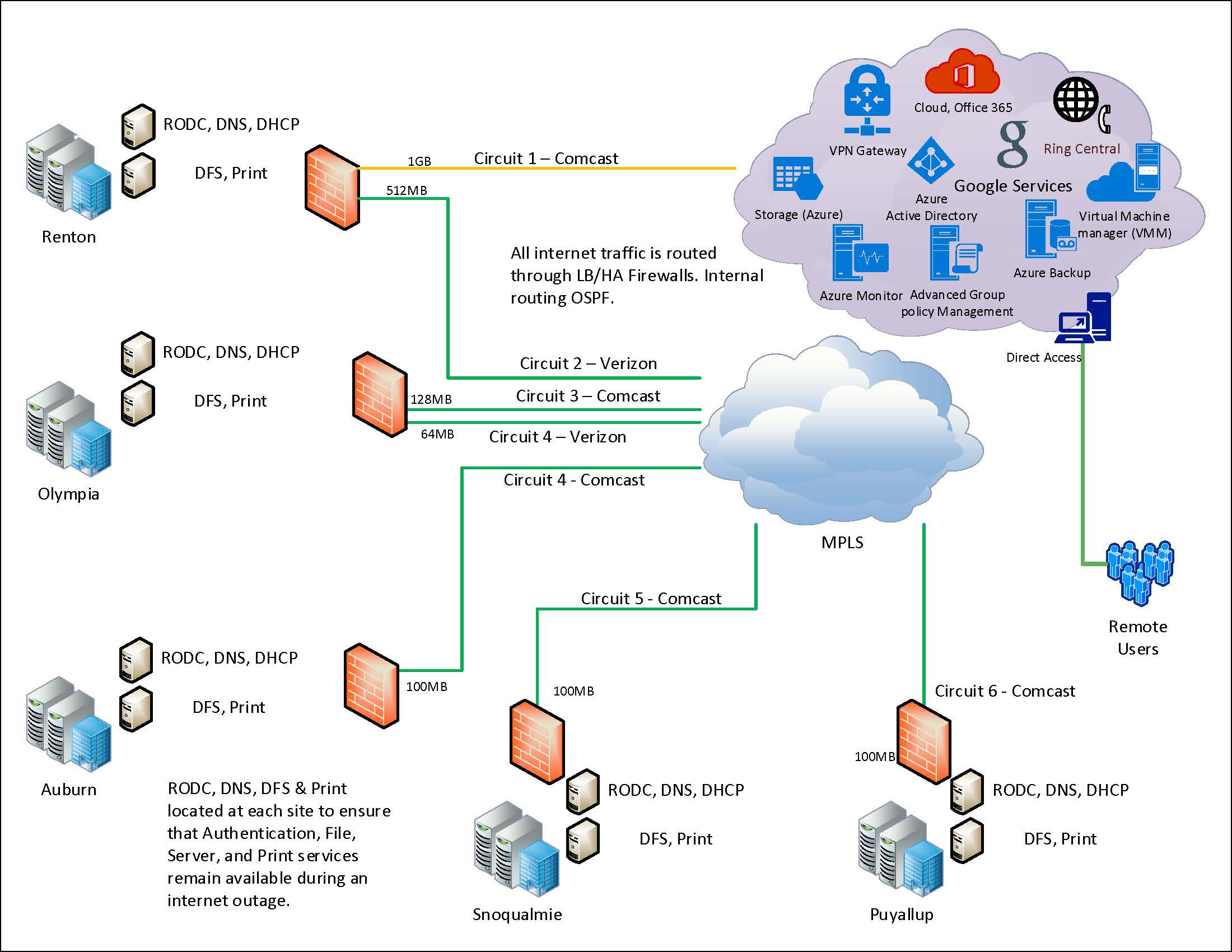
Conde, D. (2016, December). *OSPF versus EIGRP: The Case for Open Standards-based Routing.* From Juniper Networks: https://www.juniper.net/assets/us/en/local/pdf/whitepapers/esg-ospf-vs-eigrp.pdf

CyberSecurity & Infrastructure Security Agency. (2017, 6 5). *Alert (TA17-156A) Reducing the Risk of SNMP Abuse*. From CISA: https://us-cert.cisa.gov/ncas/alerts/TA17-156A

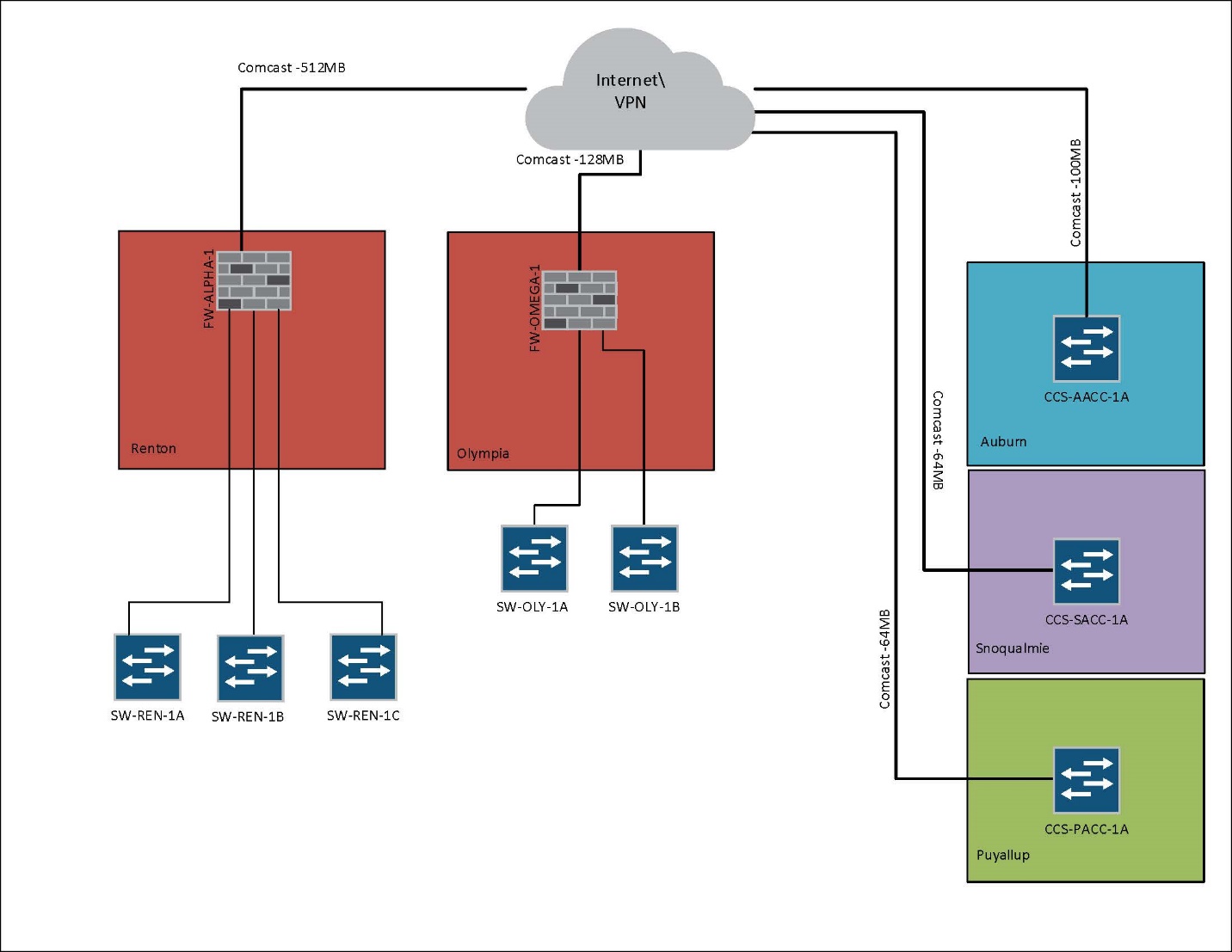
Hameed, S., Raza, A., Atta, B., & Lee, S. (2009). Converged Next Generation Network Architecture & Its Reliability. *ECMS 2009 Proceedings*.

Taschner, C., & Warren, D. (2008, 06 10). *SNMPv3 improper HMAC validation allows authentication bypass.* From CERT Coordination Center: https://www.kb.cert.org/vuls/id/878044/

# Artifact 1 – Logical High-Level Network Diagram



# Artifact 2 – Original Logical Low-Level Network Diagram



# Artifact 3 – Logical Low-Level Network Diagram

