Charity organisation - ”SikreNorge”

Job Nestor Bahner, 494300
Johannes Borgen, 494336
Abdisalan Mohamed Hussein, 494334
Thomas Løkkeborg, 473157

November 19, 2018

Abstract

SikreNorge is a non-profit charity organisation with locations all over Norway. In this report we discuss how we would implement a network infrastructure for the organisation.

Contents

1 Business case **1**

1.1 Background 1

1.2 Locations 1

1.3 Services 2

1.3.1 On-site company consultation 2

1.3.2 Teaching at learning centre 2

1.3.3 Network security laboratory 2

1.3.4 Public website 2

1.3.5 Management website 2

2 Security Policy **3**

2.1 Statement of policy 3

2.2 Responsibilities 3

2.3 Authorized access 4

2.4 Prohibited usage of equipment 5

2.5 Systems management 6

2.6 Violation of policy 7

2.7 Policy review and modification 7

2.8 Limitations of liability 7

3 Risk assessment **7**

3.1 Unauthorized access to confidential data 8

3.2 Branch loosing connection to HQ 8

3.3 Leakage of confidential information by employee or volunteer 8

3.4 DDoS on our website 9

3.5 Failure due to natural disaster at the HQ 9

3.6 Failure due to power outage at HQ 10

4 ICT and Network Infrastructure **10**
4.1 Layout and Diagrams . . . 10
4.1.1 Logical view . . . 10
4.1.2 Physical view . . . 11
4.2 WAN . . . 13
4.3 VLANs and Subnets . . . 13
4.4 Wireless . . . 14
4.5 Lab . . . 15
4.6 Branch network discussion . . . 15
4.7 HQ network discussion . . . 15
4.7.1 Layout . . . 15
4.7.2 Redundancy . . . 16
4.8 Methods for hardening . . . 16
4.8.1 Physical information security . . . 16
4.8.2 Securing the LAN . . . 17
4.8.3 Securing network infrastructure . . . 17
4.8.4 Endpoint security . . . 18

5 Our demo Packet Tracer implementation **19**
5.1 NAT . . . 19
5.2 WAN . . . 20
5.3 HQ demo configuration . . . 20
5.4 Branch demo configuration . . . 21
5.5 Wireless demo configuration . . . 21

6 Conclusion **22**

A Our demo Packet Tracer implementation **24**
A.1 Branch . . . 24
A.1.1 LC_R1 . . . 24
A.1.2 LC_S1_running-config . . . 26
A.1.3 LC_S2_running-config . . . 27

A.1.4 LC_S3_running-config 28
A.2 HQ 29
A.2.1 AccessSwitch-1 29
A.2.2 AccessSwitch-2 30
A.2.3 AccessSwitch-3 31
A.2.4 DistributionSwitch-1 32
A.2.5 DistributionSwitch-2 34
A.2.6 DistributionSwitch-3 35
A.2.7 HQ_ER1 36
A.2.8 HQ_R1 37
A.2.9 HQR2_running-config 39
A.3 (Physical) WLC configuration 41

1 Business case

SikreNorge is a non-profit charity organisation that provides information security services to businesses and institutions in Norway. The organisation seeks to secure Norway by helping those who would not otherwise have the means to prioritize security.

1.1 Background

The organisation is reliant on local expertise in each county in the form of volunteers and hired professionals. Volunteers are expected and encouraged to gain security competence through the experts. Good candidates for volunteers are students doing technical studies. Where possible the organisation will make agreements with local universities teaching information technology courses to encourage students to volunteer. The organisation is also open to volunteer work as part of theses and course projects. Volunteers of the organisation do work in exchange for practical information security experience. Both volunteers and hired professionals are expected to sign strict non-disclosure agreements regarding their work with businesses and institutions.

Financially SikreNorge relies on donations, government subsidies, and income from their webshop. Businesses who donate are encouraged to publicise their contribution to show that they support the organisation's mission. This way both the contributing businesses and SikreNorge receive good PR. Government subsidies are given with the intention and expectation that the organisation will use these means to support local, public and private institutions with information security tasks.

1.2 Locations

SikreNorge will establish learning centres in each of Norway's 18 counties. The headquarter lies in Oslo. Because of the county merges coming in a couple of years, then we may have to merge our branches.

Learning centres are meant as a hub for all the organisation's activities in the county. The centres have offices for local management and hired professionals. They also contain network sandbox areas for practicing network security, classrooms for security courses, lecture halls for seminars and general storage space. In addition to activities held at the centres, the organisation can send consultants into the field to do evaluation or configuration on-site. Consultants are a mix of local hired professionals, volunteers and staff.

The organisation's Headquarters, hereafter called HQ, provides the same services as learning centres, but also does the heavy lifting in terms of information technology services and infrastructure. The website, E-mail, databases and management applications are examples of services that are hosted here.

1.3 Services

The organisation includes a wide range of services, and the network must be set up to support these. Following is a brief discussion of key services, along with some infrastructure concerns.

1.3.1 On-site company consultation

Volunteers, hired professionals and staff can be sent out to do consulting on-site at businesses or institutions. Access to the organisation's internal services might be required during consultation, so the consultants should be able to reach them from on-site. Confidential information may be sent and received during this communication, so the technology chosen for this should focus on security.

1.3.2 Teaching at learning centre

Businesses and institutions may visit a learning centre to take courses or to receive guidance. During this stay they will naturally want internet connectivity. A visitors access rights should be restricted as much as possible.

1.3.3 Network security laboratory

Each learning centre has a laboratory where visitors can explore hardware and software to learn about vulnerabilities and best practises. Labs are meant to be a sandbox area for learning about information security. They should be set up with care so that experiments from the lab cannot interfere with the rest of the learning centres operations.

1.3.4 Public website

SikreNorge's website includes information about the organisation's offerings, online courses and a webshop. Some of the website's information and courses are built upon internal services, so the infrastructure should support communication to allow this. The webshop will sell T-shirts, coffee mugs, posters and more to further information security awareness and good practice. The shop allows buyers to register accounts for easy shopping.

1.3.5 Management website

The organisation uses a website separate to the public website to manage internal logistics. Registered staff, businesses, institutions and overview of future work are examples of information that can be found here.

2 Security Policy

2.1 Statement of policy

1. Scope and applicability:
   (a) Our organisation
      i. Every member is expected to know the content of our policy and comply. Ignorance is equal to non compliance.
   (b) Partners
      i. They are expected to learn and know the content because an equal understanding of security is key.
   (c) Guests/Trainees
      i. Must know key elements to ensure safe learning and usage when using our equipment. Coordinators must brief them before actual usage.

2.2 Responsibilities

1. Chief Executive Officer (CEO)
   (a) Responsible for the organisation's success.
   (b) Executives report to the CEO.
2. Chief Technology Officer (CTO)
   (a) Responsible for technology infrastructure:
      i. Identify and evaluate new technology.
      ii. Maintaining and improving existing systems.
      iii. Give and delegate counseling about technology to clients.
3. Chief Information Officer (CIO)
   (a) Responsible for IT and computer systems:
      i. Responsible for our web server.
   (b) Direct deployment of new technology in collaboration with CTO.
4. Chief Security Officer (CSO)
   (a) Responsible for the organizations security strategy and programs as well as safeguarding our intellectual property:
      i. Responsible for our personnel's security awareness and delegate counseling of clients regarding awareness.

5. Chief Information Security Officer (CISO)
    (a) Controls the overall structure of security and security management through our security policy.
6. All executives must have an IT-Security background, in conjunction with a management background.
7. Branch office security managers
    (a) Manage security for their branch office.
    (b) Report to CISO.
8. All executives and managers must adhere to security guidelines and practice consistently, as they are a possible single-point-of-failure in the security scheme.
9. Employees and volunteers
    (a) Be loyal to the organisation's security guidelines.
    (b) Understand our policy.
    (c) Validate understanding of policy.
    (d) Understand repercussions of policy insubordination.

2.3 Authorized access

1. User access
    (a) Administration, management and other vital parts of the organizational systems must be separated from normal users.
    (b) Employees have a level of clearance, and access thereafter.
    (c) Executives have full access to systems, except those classified as secret.
    (d) Employees with access to confidential information or higher must sign a non-disclosure agreement.
    (e) Volunteers may have access to certain confidential information to perform their work, but their access is defined along the lines of a need to know basis.
    (f) Levels of classification, where higher levels have access of the lower:
        i. Official - All can access.
        ii. Confidential - Employees, volunteers
        iii. Restricted - Managers, Executives
        iv. Secret - CEO, board of directors
2. Fair and responsible use

(a) As a precaution, emails are to be treated critically:
    i. Hyperlinks must not be clicked, instead copied and pasted into the search bar.
    ii. Images not to be loaded before sender is verified.
    iii. Autoload should remain off by default.
    iv. Attachments not to be downloaded or viewed unless verified sender.
    v. The email server must have DMARC, SPF and DKIM.
(b) Passwords should follow NIST recommendations [4], meaning we prefer long and easily memorable passwords to short difficult ones.
(c) VPN required off-site.

3. Protection of privacy:
    (a) Must adhere to GDPR regulations.
    (b) Must also comply with regulations from Datatilsynet.
    (c) Must comply with Norwegian and international laws

2.4 Prohibited usage of equipment

1. Disruptive use and misuse
    (a) No personal equipment in restricted areas.
    (b) USB devices must only be issued by the organisation and only these can be used on organisation equipment.
    (c) Vital organizational equipment should not be brought off-site.
    (d) Restricted equipment must not be used for not-intended purposes:
        i. Web surfing.
        ii. email.
        iii. Farming (Unless intended).
        iv. Hosting (Unless intended).
        v. Packet sniffing (Wireshark, unless intended).
    (e) Users with high level of access must not use their accounts to perform non-vital and possibly compromising tasks:
        i. Web surfing.
        ii. Use email.

2. Copyrighted, licensed, or other intellectual property
    (a) Hard-copies must be shredded after they are no longer needed.
    (b) Photos of confidential material are not allowed.

2.5 Systems management

1. Management of stored materials
   (a) Authentication and authorization should be managed by an AAA server.
   (b) All access to restricted equipment and actions must be logged on a server.
   (c) Classified data need to be encrypted on the hard drive and in transfer - Partner and organizational data protected by non-disclosure contracts.
   (d) All organization equipment that have been used to store organization or partner information must be disposed of in a safe manner.
   (e) Hard drives must be destroyed by the organization itself.
   (f) Printers must be in an enclosed network, and classified documents should only be printed on secure organization printers.
2. Documentation
   (a) Important assets and equipment must be properly documented for the purpose of maintenance and operations.
   (b) All configurations must be stored on a safe server for easy system recovery.
3. Employer monitoring
   (a) Use of internet logged.
   (b) Organizational equipment inventory checked regularly.
   (c) Restricted area entry logged:
      i. Physical - ID card entry log.
      ii. Digital - Credentials log.
4. Virus protection
   (a) Each branch must have its own firewall mechanism to filter unwanted traffic.
   (b) Organization computers and smart-phones with internet connection must have anti-virus.
   (c) Email etiquette. See 2a.
5. Physical security
   (a) Limited access to restricted areas:
      i. Must use ID-card to enter: Server rooms and Offices for high clearance individuals.
   (b) Guest premises must be separated from working grounds and other vital instances.
6. Encryption
   (a) Within the organization the use of asymmetric encryption with security level equal to SHA 3 or higher must be enforced.

2.6 Violation of policy

1. Procedures for reporting violations:
   (a) As a security pushing organization, reporting violations of our policy is encouraged.
   (b) To ensure this practice the report can be submitted anonymously.
2. Penalties for violations:
   (a) Minor violations can result in revoked clearance and/or access.
   (b) Serious violations:
      i. Subject to dismissal.
      ii. Legal action.

2.7 Policy review and modification

1. Scheduled review of policy modifications for modification
   (a) This organization will actively seek to be in the front of information security, to ensure we are able to offer our services with satisfaction. This policy is therefore an iterative peace of document which is subject to alteration if needed as the CISO see fit.

2.8 Limitations of liability

1. Statements of liability:
   (a) This organization is not liable if an employee does not comply with our policy.
      i. The organization will assist in prosecution if necessary.

3 Risk assessment

In this section we address a few key risks related to our network infrastructure.

3.1 Unauthorized access to confidential data

Description: We may store information about our partners and others we offer services to. This data can be discovered security flaws or other compromising information. Unauthorized individuals may try to steal or view this information. Meanwhile, this data is vital for our organisation to perform our services.

Impact: Our organisation relies on our reputation. Therefore, the impact of losing confidential information is critical and in a worst case scenario put us out of business.

Likelihood: As this information is one of our most important assets, it is a target for people with mischievous intent. Therefore, the likelihood of someone trying to gain access and control over this information is great.

Verdict: Access to confidential data must be authorized, authenticated and logged. It must be stored encrypted on a safe server. In processing it must also be encrypted and never be transferred over unsecured links in plaintext. For telecommuters it is required to have an established VPN tunnel on secure equipment only intended for work.

3.2 Branch loosing connection to HQ

Description: Each branch is reliant on a WAN connection to HQ for services and management resources. This connection is made through a VPN tunnel.

Impact: Staff would loose access to all internal services, and networking equipment would loose access to management resources at the HQ. Staff and guests would still be able to browse the internet like normal.

Likelihood: We have redundant connections at the HQ, but each branch only has a single gateway router. This router is bound to fail every once in a while, and the connection will break with it. The connection could break the HQ end as well, and this a much more serious problem, although this should be very unlikely compared with the connection breaking at the branch end.

Verdict: This is an accepted risk. To solve this we would have to implement redundancy at each of our 17 branch locations, which would be costly. The problem is addressed at the HQ, however, as this is the main reason we have redundant gateways set up there.

3.3 Leakage of confidential information by employee or volunteer

Description: Since we rely on hired professionals and volunteers who must have some level of access to perform their work a risk is leakage.

Impact: We handle confidential data about our clients, so a leak would be catastrophic.

Likelihood: All employees are screened before they get access to the organisations resources. In addition, employees are on a need-to-know basis, so they only have access to

resources related to projects they are involved in. This decreases the likelihood somewhat, but as explained in the verdict we feel this problem should be addressed at a higher level.

Verdict: Network security measures like AAA and logging are in place to support mitigating the issue, but measures at higher levels than that defined by this report are needed, so we judge it to be outside our scope to address this fully.

3.4 DDoS on our website

Description: Our role as an information security organisation could make us a potential target for DDoS.

Impact: A DDoS would be targeted at our public website. This website going down means potential loss of income through donations and purchases in the webshop, but we deem this not to be a huge issue because we are a non-profit organisation, and wouldn't miss out on much due to a little downtime. However, the DDoS would put a strain on our gateway networking equipment, meaning internal services would be impacted.

Likelihood: We deem this to be fairly likely, as we are a public organisation focused around information security.

Verdict: This is an issue we have to address. Because the only publicly reachable resource is our website, and since that website does not contain any of our clients confidential information, we could set in place a process to bring our website up on a public cloud provider. We judge this to be beyond the scope of this project.

3.5 Failure due to natural disaster at the HQ

Description: A natural disaster could bring down our infrastructure.

Impact: The HQ going down due to natural disaster would likely mean a halt in all activity at both HQ and all branch locations. In addition we could loose data due to physical destruction of resources.

Likelihood: Not very likely, as we will place the HQ in a safe location.

Verdict: The impact would be so catastrophic that we have to address this despite the low likelihood. Essential services and management systems will be placed in racks that can take a beating, and we will implement backup routines in place at a Norwegian company providing backup services. Then we are sure that physically loosing the resources at HQ does not mean loosing essential data.

3.6 Failure due to power outage at HQ

Description: A power outage at a branch location is a possible event.

Impact: A power outage means that all networking equipment at the HQ would go down. This effectively means that all activity at the HQ would halt, and all activity involving internal resources would halt at branch locations. The impact would be huge.

Likelihood: Fairly likely

Verdict: We mitigate this by installing UPS batteries for the services and essential networking equipment. This way services could shut down safely in the event of a power outage, or even operate as normal for a short amount of time.

4 ICT and Network Infrastructure

This section provides discussion around the networking implementation we decided on. Note that not everything discussed is implemented in our demo configuration. 5 explains our demo.

As previously stated we are a charity organisation that relies on donations, volunteer work and government subsidies. Due to this we have focused on cost reduction in our ICT implementation. This has caused us to mainly prioritize security and redundancy, while sacrificing performance in favor of cost savings.

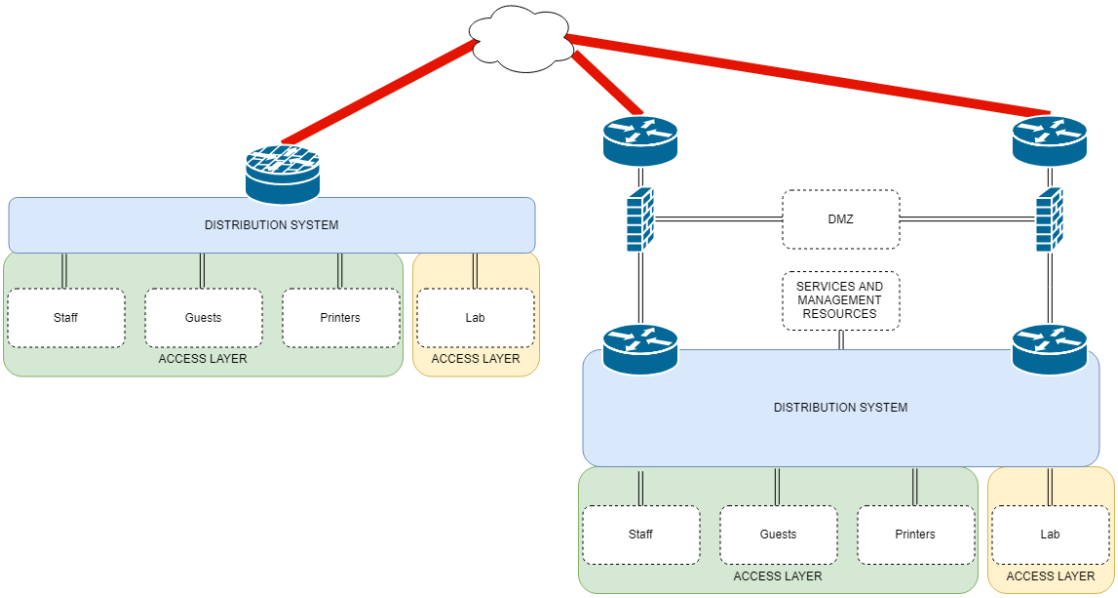
4.1 Layout and Diagrams

The following diagrams show a few different views of our network infrastructure. Short explanations of the diagrams are included.

4.1.1 Logical view

The diagram in Figure 1 shows a view of our infrastructure. We've put the routers inside the distribution system to show that we have chosen a collapsed core solution. Note that the "distribution system" on the branch location really just consists of a single router and a few switches, but we felt the terminology still fit. The "services and management resources" area is placed above the distribution system to indicate that this is given its own dedicated switches. The lab has its own access layer area in the diagram to indicate that it will be given special treatment.

Figure 1: Logical view of the network



4.1.2 Physical view

We've used screenshots of our Packet Tracer implementation to produce the diagrams seen in Figure 2 and 3.

Figure 2: Physical view of HQ

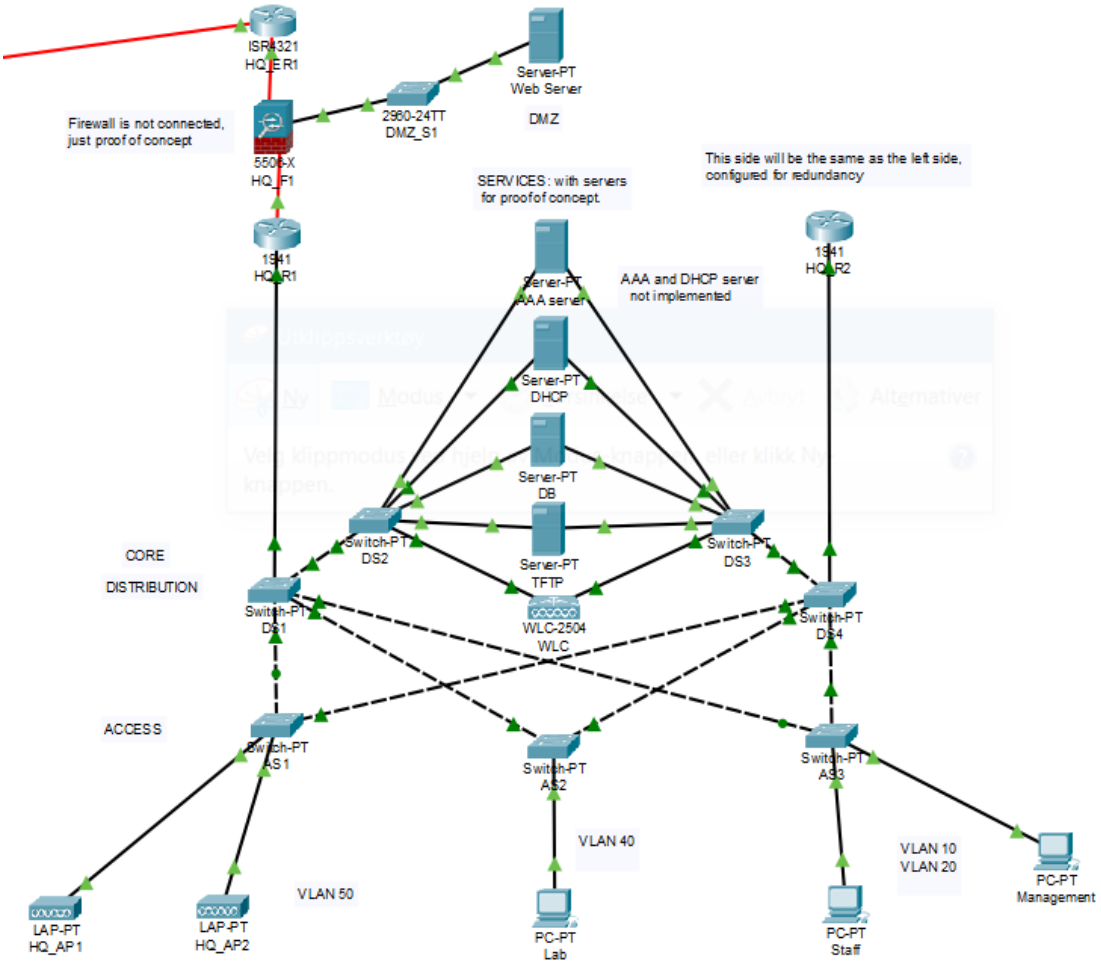
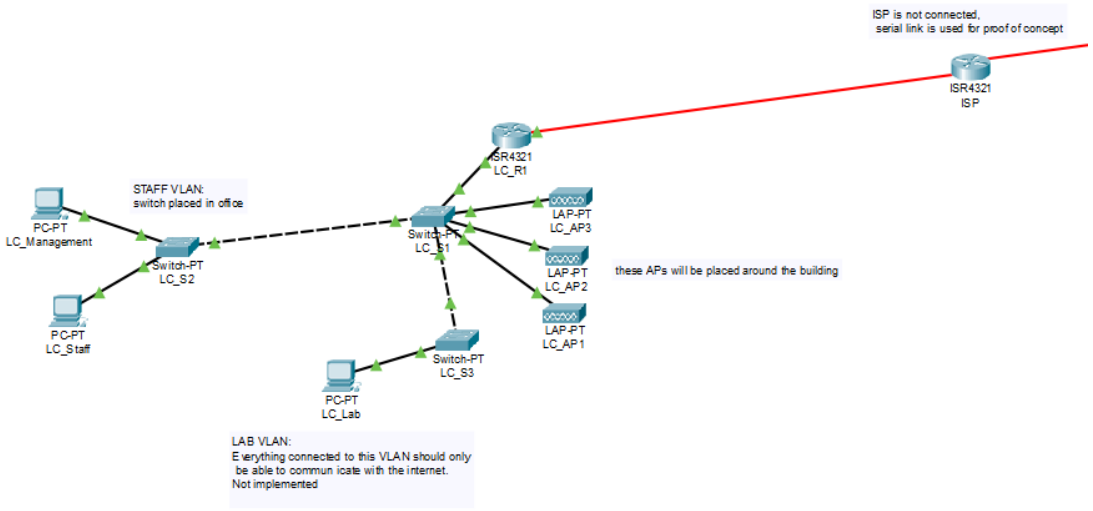


Figure 3: Physical view of Branch



4.2 WAN

Our WAN topology is dual-homed where branches can only communicate with HQ but not other branches. HQ can communicate with every branch.

We use IPsec to create a site-to-site VPN tunnel from branches to the HQ. We chose VPN because it uses the public internet. Our traffic is encrypted, so security-wise this choice of technology should not restrict us. It does mean we have to settle for less performance though, but we're willing to accept this trade-off in favor of saving costs.

The WAN connection has two primary uses: To give Staff access to internal services located at the HQ, and to provide management access. In addition we also want to be able to VPN to HQ from an off-site location, so we need a VPN server with a pool of temporary IP addresses for remote commuters. This VPN connection would pass through an IPsec tunnel forwarded by the ISP to an off-site client.

4.3 VLANs and Subnets

The goal when designing our VLAN's and subnets was simplicity. We chose to subnet our private addresses from the 10.0.0.0/8 private address range, as it gave us plenty

of space to divide the subnets up how we wanted. We dedicate the second octet to indicate what location the subnet belongs to, where the value 1 indicates the HQ, and a value above 1 indicates a branch location. For example: 10.1.x.x is a subnet the HQ, and 10.2.x.x is a subnet at the first learning centre and so on.

This lets us create subnets that look very similar across locations, while letting a network engineer quickly see what location a particular IP address belongs to. We dedicate the third octet to indicate what VLAN the subnet belongs to, with the value of the octet being the same as the VLAN id. 10.1.10.x is a subnet for the management VLAN of the HQ, and 10.10.60.x is a subnet for the printer VLAN of location nr. 9.

Combined with the fact that we reserve the first 10 hosts for static IPs in each subnet range, this leaves us with 244 available dynamic host addresses. For the learning centres this is not a problem, as 244 guests are unlikely to be connected to the network at the same time. The HQ is more brittle, but we've concluded that 244 hosts should be enough there as well. Table 1 shows our VLAN's with their corresponding subnets. The character x refers to what location the subnet is on.

Table 1: Table of VLANs with corresponding subnets

VLAN Name	**VLAN ID**	**Subnet**	**Excluded addresses**	**Available addresses**
Management	10	10.x.10.0/24	10.x.10.1 - 10.x.10.10	244
Staff	20	10.x.20.0/24	10.x.20.1 - 10.x.20.10	244
Services	30	10.x.30.0/24	10.x.30.1 - 10.x.30.10	244
Lab	40	10.x.40.0/24	10.x.40.1 - 10.x.40.10	244
Guest	50	10.x.50.0/24	10.x.50.1 - 10.x.50.10	244
Printer	60	10.x.60.0/24	10.x.60.1 - 10.x.60.10	244
DMZ	70	10.x.70.0/24	10.x.70.1 - 10.x.70.10	244
Blackhole VLAN	99	N/A	N/A	N/A

4.4 Wireless

We've chosen to build our wireless solution with Wireless Access Controllers (WLC's) and Lightweight Access Points (LWAP's). As we want as few resources as possible to be placed at the branch locations, the WLC's will be placed at the HQ. We will have redundancy in WLC by the use of the "High Availability" features that Cisco provides. [2]

This means that the LWAP's at the branches might encounter situations with no access to WLC's, but as this connection will benefit from the same redundancy as the one provided for services this will be relatively rare. We'd rather put resources into our one HQ than to spread resources around to each of the 17 branches.

The WLC's and LWAP's use CAPWAP to communicate, meaning all LWAP's are connected to access ports on the management VLAN. This unifies how we set up our IP

addresses.

Our Wireless setup consists of two WLAN's, one for staff and one for guests. Both are configured with WPA2 level security. The staff WLAN is tagged to the staff VLAN, and the guest WLAN is mapped to the guest VLAN, this way staff and guest users connected over Wi-Fi will have the same rights as those connected physically.

4.5 Lab

The purpose of the labs was to provide an environment where visitors could experiment freely with information security concepts. This means that it is a security risk by design, so we have to be careful how we implement it. The labs will have their own physical switch, and the kinds of traffic that may pass through will be heavily restricted. Only browsing is allowed, so we restrict traffic to only established TCP for the protocols HTTP, HTTPS and DNS.

Some networking equipment will be placed in the lab to be used for experimentation, but we don't consider this a part of our network infrastructure.

4.6 Branch network discussion

As seen in Figure 3, the branch network is very simple. As all resources are located at the HQ, each branch only needs a router, a few switches and a few LWAP's to function. Each branch location will not have much traffic, so we can justify saving costs by placing the firewall, local DHCP server and the VPN termination at the router itself.

The LWAP's are configured through CAPWAP tunnels going to the WLCs at HQ. We could have set up redundant WLC functionality on each branch location, but decided against it because the cost of configuring this for each branch would be too high.

We don't consider the branch location as critical infrastructure. Rather than providing each branch location with redundancy, we place all resources at the HQ, and focus on providing redundancy there. This means that a branch might go down for a few days every once in a while. We consider this an accepted risk.

4.7 HQ network discussion

4.7.1 Layout

Initially we aimed for a three-tier architecture [1], but found that a collapsed-core architecture [5] suited our needs better. A collapsed-core architecture retains the redundancy

of three-tier, but sacrifices some efficiency in favor of saving costs.

We have two routers and two switches set up to combine the core and distribution layer into a single layer. The services and management resources are given special treatment and placed in its own segment of the network, while the rest of the network is set up to use access switches with connections to both distribution/core layer switches to provide redundancy.

Physically each access layer switch is configured with access ports based on what users are found around the switch. Switches placed in the offices will have staff and management ports, while switches in lecture halls and such will have guest ports. LWAP's are connected to management switchports.

4.7.2 Redundancy

As all of the branch locations rely on the HQ to operate, redundancy was an important topic to address. What really needs redundancy are the services and management resources. The fact that the rest of the HQ gets some redundancy is really just a bonus.

As shown in Figure 2, the HQ has two links to the ISP through a duplicated setup of routers and switches. Important services and management resources are placed in the middle of the network, in between the two routers, as shown. They have dual Ethernet connections, one going to each ISP link. This way, if any of the equipment forming one of the paths to ISP goes down, the services and management resources will still have internet connectivity.

As we have have two gateways we need to use a "First Hop Redundancy" protocol to manage the default gateway. The options we looked at were HSRP, VRRP and GLBP. We went with GLBP because in addition to providing the redundancy we need, it also does load balancing, letting us utilize both of the gateway routers to their fullest. HSRP and VRRP would've provided redundancy, but not load balancing.

4.8 Methods for hardening

4.8.1 Physical information security

Premise access: The premises at HQ will be locked down. Access will be granted based on roles, and ID-cards will be used to enforce this. Guests do not have access to the staff area, staff do not have access to the main server room, and so on. In addition the main server room will be secured with video surveillance and a mantrap. This way potential unauthorized access will be monitored, and failed attempt will result in the attacker being trapped.

Device access: Physical management ports will be secured with passwords, or turned off completely if they are not in use.

4.8.2 Securing the LAN

As layer 2 can be the weakest link in our network infrastructure we will implement different methods to prevent or mitigate potential attacks:

Management and staff switch: Whereas labs have a separate switch, management and staff share the same switch. Staff and management computers are connected physically and for new users to connect an admin must configure a new access port. For additional security all access ports on this switch use PVLAN edge to make it more difficult for a man-in-the middle attack against management traffic.

STP manipulation attacks: Our switches, especially in HQ, are set up for redundancy and use STP to prevent loops. All access port will have configured with PortFast and BPDU Guard to prevent an attacker becoming the root bridge.

CAM table attack: To prevent flooding of a switch's CAM table all access ports have port-security implemented. This also helps mitigate a DHCP starvation attack.

VLAN hopping and double-tagging attack: To prevent an attacker from spoofing a switch trunk all ports have disabled DTP (auto trunking). Ports available to users are explicitly assigned as access ports. To prevent a double-tagging attack trunks have a native Blackhole VLAN. Ports which are not in use are disabled. They are also configured as access ports to the Blackhole VLAN to force awareness of the configuration when turned back on.

DHCP spoofing and DHCP starvation attacks: To prevent rogue DHCP servers and further mitigate DHCP starvation we will use DHCP Snooping. It will be enabled for all user VLAN's. While our upstream ports will be set to trusted, access port will have a limit to how many DHCP request it can send per second. However, we must take into account that it may take some time for the DHCP Snooping to finish the binding table.

ARP spoofing and ARP poisoning attacks: In interaction with DHCP Snooping we will use DAI (Dynamic ARP Inspection) to prevent ARP spoofing and poisoning. Then the switch relays only valid ARP replies. Like DCHP snooping it will be enabled for user VLAN's and trusted ports will be on the same upstream interfaces.

IP and MAC spoofing attacks: In addition we will implement IPSG (IP Source Guard) to prevent IP address and MAC address spoofing. It will be configured on untrusted access ports.

4.8.3 Securing network infrastructure

Securing the router: We use a defense-in-depth approach with a DMZ. Between our internal router and edge router we will have a firewall which will allow external networks

to access our web server. On our edge router we will disable unnecessary services with the use of Cisco's auto secure function [6]. This will also configure enable passwords and telnet vty input, which will be reconfigured. All management access to router must be with the use of AAA and SSH if not connected to the console port. Remote access must have an established VPN connection beforehand.

Firewalls: The firewall is the network's first line of defence, and it it vitally important that we have a good firewall implementation. We will use next-gen firewalls [3] in order to supply ourselves with both packet filtering and session analysis. With this we will always have a current threat picture due to the rapidly updating threat database of the firewall provider.

At a branch the firewall mechanism is on the router as we can not justify a dedicated firewall, reasoned by the small size of a branch network. However, in HQ we will have a dedicated firewall where it is implemented through a defence in depth structure. We route all traffic from the internet through the firewall mechanisms. This is to avoid split tunneling concerns. These concerns being that the users internet connection, if not filtered, may compromise the entire network; especially if the endpoint is a manager, as managers have clearance. We don't want to give a potential attacker this kind of access.

Authentication Authorization and Accounting: Users within our network will have role-based access. We will implement this with the use of a TACACS+ server. The system admin of the site will also have a local user if connection to the server is lost. For every user in staff and management we will implement port based authentication (802.1x). This is to ensure that every action and access can be properly authorized as well as logged. The logging will be handled by a server and devices must share a NTP server for accuracy of events logged.

ACL's: In our infrastructure everyone should not be able to communicate with certain devices, or other users. The lab could be a potential security threat to the rest of our network. Therefore, we will implement ACL's that allow the lab to only browse the internet, otherwise it should be a completely closed environment. Management is the only VLAN that should be able to talk to another user subnet through the router-on-a-stick. Management and staff may access printers. Guests will also be limited to only internet. Telnet will be explicitly disabled with the use of ACL. Branch staff may only access the database to get documents required in their work. Branch APs can communicate with the WLC and management can get config files from the TFTP server. In HQ management can access everything in a branch.

4.8.4 Endpoint security

All endpoint devices must have software that prevents infection and spread of malware. This being due to the especially vulnerable nature of endpoints because of their interactions with a user.

Traditionally this is done firstly by installing some kind of anti malware software, in order to detect and mitigate malware threats. We could also provide the endpoint host with a host based IPS, to monitor and report on their system. In accordance with this we can also install a host-based firewall to add to the security threats posed by incoming traffic, that may bypass the security measures of the network.

However, we did not decide to do this, as it simply is an outdated way of doing things on the scale we need it. Instead we opted for a more modern approach for endpoint security by using: Anti Malware Protection (AMP), Email Security Appliances (ESA), Web Security Appliances (WSA) and Network Admission Control (NAC). The combination of these different technologies and protocols gives us a good protection suite for the endpoint users and our whole network.

These technologies provide us with everything we need to efficiently secure the endpoints. Firstly AMP gives us an endpoint malware protection, secondly ESA provides us with email spam filtering even before the emails reach the endpoint. WSA allows us to filter and blacklist websites that are malicious and or reputably unsafe. Last but not least we have NAC which permits only authorised and policy-compliant systems to connect to the network.

On the endpoint host we should use some form of data encryption in case of loss or theft.

Now, we have all the tools we need to:

1. Discover, enforce and protect before an event.
2. Detect, block and defend during an event.
3. Scope, contain and remediate after an event.

5 Our demo Packet Tracer implementation

As part of the project we implemented part of our infrastructure in Packet Tracer. The configuration can be found in appendix A. This section will provide some discussion around the demo implementation.

5.1 NAT

We have not configured NAT. This is because we focused on getting the VPN working, instead of trying to simulate the internet. In reality each site would be behind a NAT configured on the edge routers.

5.2 WAN

The WAN connection is simulated with the use of a single serial connection between the HQ and branch. We chose to do this for simplicity. In reality they would not be directly connected, but would each be connected to an ISP which would provide internet access. The routing is done with the use of static routes.

5.3 HQ demo configuration

Figure 2 is taken from our PT implementation of the HQ. As you can see we have configured three access layer switches with a few machines attached to different access ports. The services and management resources area is set up with its own dedicated switches connected to the ”distribution system”, which is really just two switches connected to two gateway routers. The left gateway router shows the concept of how our defence-in-depth would be implemented, and also our IPsec connection to the branch location. The firewall is not plugged in, and the DMZ is not set up. In reality the firewall would be placed between the two routers, and traffic from the public web to our web server would be routed to the DMZ connected to the firewall, as illustrated by Figure 1. The setup would be duplicated on the right gateway router.

In reality we would like to use GLBP for ”first hop redundancy” and load balancing, but we did not figure out a way to do this in Packet Tracer. For demonstration purposes we configured HSRP on the routers instead.

The WLC would in reality be coupled with at least one standby controller, but we've only included one for the demo. It is plugged in, but does nothing. See 5.5 for further discussion on this topic.

For hardening we have implemented port-security, mitigated STP manipulation, CAM table attacks, VLAN hopping and double-tagging attacks. However, we have not implemented DHCP Snooping, DAI or IPSG. Since our implementation is mainly in packet tracer these commands did have some limitations or were absent. DHCP Snooping would allegedly only work for VLAN1, for others it would display this error: ”DHCP Snooping: The switch receives a DHCP DISCOVER message on an untrusted port. The device is not configured with a trusted port in the same vlan. The device drops the packet.”.

We have not implemented any of our services including the DHCP and AAA server. The DHCP pool for HQ and its VLANs are handled by the internal router. Secure management of devices like switches and routers in accordance with AAA is not implemented at all. In reality this is a big liability and would not be acceptable.

Our IPSec implementation defines ACLs that limit the communication from branch

to HQ and vice versa. Branch management can access the TFTP server. Branch staff can access the database for documents. Branch APs can communicate with the WLC. HQ management can talk to anyone in a branch for remote support and management.

5.4 Branch demo configuration

As all the branches have similar configuration, we only implemented one in our demo. Figure 3 shows our implementation. The router is very similar to how it would be configured in reality, the only difference being that a firewall mechanism has not been set up. The LWAP's connected to the main switch are intended to be placed around the building, and would get their configuration from the WLC at HQ.

The hardening of branch layer 2 is equal to our HQ implementation. Also missing inter-subnet ACL's on the router.

5.5 Wireless demo configuration

We had trouble with implementing WLC's and LWAP's properly in Packet Tracer, so we decided to configure a physical WLC as a proof-of-concept of how the WLC at HQ in our demo would look like. The exported configuration is provided in appendix A.3. Two WLAN's Staff and Guest are set up with WPA2+PSK security. Note that the addresses used in the configuration file are wrong. All addresses starting with 192.168 should really start with 10.1. We configured it like this because we had trouble with the 10.0.0.0/8 range in the Cisco lab.

6 Conclusion

We had apostasy and poor communication in the beginning of the project. Despite this we feel we have reached a result we can confidently say we are pleased with.

We are confident we could have implemented all the security measures described. Due to time-constraints we had to prioritize, however, so unfortunately some key topics of configuration were left out. AAA, inter-subnet ACLs, NAT, and simulating a connection to the internet are examples. We hope we provide enough theoretical discussion in our report to make up for this somewhat though. We want to note that we wasted a lot of time messing around with Packet Tracer, as we struggled to figure out what features are supported.

We are happy with the Security Policy, and feel it is complete. We've tried to actively enforce it when designing and implementing our network infrastructure.

We must admit our group collaboration was not very good in the beginning. However, when we moved from using Google Docs to using Github with Overleaf the group effort got a massive boost. The introduction of version control gave us a central tool to work around, while still allowing each member to work the way they wanted.

In conclusion we feel we have learned a lot from this project, both about networking and about group work. We have reached a satisfactory result, even though it in some places is lacking.

References

[1] Cisco three tier architecture explained. [Online; accessed 16-November-2018]. 15

[2] High Availability (SSO) Deployment Guide. [Online; accessed 16-November-2018]. 14

[3] Next-generation firewall. [Online; accessed 16-November-2018]. 18

[4] NIST Special Publication 800-63B. [Online; accessed 16-November-2018]. 5

[5] Small enterprise design profile reference guide - collapsed core network design. [Online; accessed 16-November-2018]. 15

[6] User security configuration guide, cisco ios xe release 3s - chapter: Autosecure. [Online; accessed 16-November-2018]. 18

[7] EMPSON, S. *CCNA Routing and Switching Portable Command Guide*. Cisco Press, 2017.

[8] HUCABY, D. *CCNA Wireless 200-355 Official Cert Guide*. Cisco Press, 2016.

A Our demo Packet Tracer implementation

A.1 Branch

A.1.1 LC_R1

```
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname LC_R1
!
!
!
!
ip dhcp excluded-address 10.2.10.1 10.2.10.10
ip dhcp excluded-address 10.2.20.1 10.2.20.10
ip dhcp excluded-address 10.2.40.1 10.2.40.10
ip dhcp excluded-address 10.2.50.1 10.2.50.10
ip dhcp excluded-address 10.2.60.1 10.2.60.10
!
ip dhcp pool VLAN_MANAGEMENT
 network 10.2.10.0 255.255.255.0
 default-router 10.2.10.1
ip dhcp pool VLAN_GUEST
 network 10.2.50.0 255.255.255.0
 default-router 10.2.50.1
ip dhcp pool VLAN_STAFF
 network 10.2.20.0 255.255.255.0
 default-router 10.2.20.1
ip dhcp pool VLAN_LAB
 network 10.2.40.0 255.255.255.0
 default-router 10.2.40.1
ip dhcp pool VLAN_PRINTERS
 network 10.2.60.0 255.255.255.0
 default-router 10.2.60.1
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
!
crypto isakmp key cisco123 address 10.0.1.1
!
!
crypto ipsec security-association lifetime seconds 1800
!
crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
!
crypto map CMAP 10 ipsec-isakmp
 set peer 10.0.1.1
 set pfs group5
 set security-association lifetime seconds 900
 set transform-set 50
 match address 101
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
```

```
!
interface GigabitEthernet0/0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/0.10
 encapsulation dot1Q 10
 ip address 10.2.10.1 255.255.255.0
!
interface GigabitEthernet0/0/0.20
 encapsulation dot1Q 20
 ip address 10.2.20.1 255.255.255.0
!
interface GigabitEthernet0/0/0.30
 encapsulation dot1Q 30
 ip address 10.2.30.1 255.255.255.0
!
interface GigabitEthernet0/0/0.40
 encapsulation dot1Q 40
 ip address 10.2.40.1 255.255.255.0
!
interface GigabitEthernet0/0/0.50
 encapsulation dot1Q 50
 ip address 10.2.50.1 255.255.255.0
!
interface GigabitEthernet0/0/0.60
 encapsulation dot1Q 60
 ip address 10.2.60.1 255.255.255.0
!
interface GigabitEthernet0/0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/1/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/1/1
 ip address 10.0.1.2 255.255.255.0
 crypto map CMAP
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 10.1.0.0 255.255.0.0 10.0.1.1

!
ip flow-export version 9
!
!
!APs can connect to WLC
access-list 101 permit ip 10.2.10.0 0.0.0.255 host 10.1.10.2
!Management can connect to the tftp server
access-list 101 permit ip 10.2.10.0 0.0.0.255 host 10.1.30.4
!staff can connect to the database
access-list 101 permit ip 10.2.20.0 0.0.0.255 host 10.1.30.3
!management in HQ can access branch and get replies
access-list 101 permit icmp 10.2.0.0 0.0.255.255 10.1.10.0 0.0.0.255 echo-reply
access-list 101 permit tcp 10.2.0.0 0.0.255.255 10.1.10.0 0.0.0.255 established
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

A.1.2 LC_S1_running-config

```
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname LC1_S1
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
 switchport port-security
 switchport port-security maximum 3
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet1/1
 switchport access vlan 40
 switchport mode access
 switchport nonegotiate
 spanning-tree guard root
!
interface FastEthernet2/1
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
 switchport port-security
 switchport port-security maximum 3
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet3/1
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
 switchport port-security
 switchport port-security maximum 3
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet4/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet5/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet6/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet7/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet8/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10-60
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet9/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10-60
```

```
 switchport mode trunk
 switchport nonegotiate
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

A.1.3 LC_S2_running-config

```
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname LC2_S2
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10-60
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet1/1
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
 switchport port-security
 switchport port-security maximum 3
 switchport protected
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet2/1
 switchport access vlan 20
 switchport mode access
 switchport nonegotiate
 switchport port-security
 switchport port-security maximum 3
 switchport protected
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet3/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet4/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet5/1
 switchport access vlan 99
```

```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet6/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet7/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet8/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet9/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

A.1.4 LC_S3_running-config

```
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname LC1_S3
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 40
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet1/1
 switchport access vlan 40
 switchport mode access
 switchport nonegotiate
 switchport port-security
 switchport port-security maximum 3
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet2/1
```

```
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet3/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet4/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet5/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet6/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet7/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet8/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet9/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

A.2 HQ

A.2.1 AccessSwitch-1

```
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname HQ_AS_G
!
```

```
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
 switchport port-security
 switchport port-security maximum 3
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet1/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10-60
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet2/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10-60
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet3/1
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
 switchport port-security
 switchport port-security maximum 3
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet4/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet5/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

A.2.2 AccessSwitch-2

```
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname HQ_AS_L
!
!
!
```

```
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 40
 switchport mode access
 switchport nonegotiate
 switchport port-security
 switchport port-security maximum 3
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet1/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10-60
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet2/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10-60
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet3/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet4/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet5/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

A.2.3 AccessSwitch-3

```
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname HQ_AS_M&S
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
```

```
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
 switchport port-security
 switchport port-security maximum 3
 switchport protected
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet1/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10-60
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet2/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10-60
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet3/1
 switchport access vlan 20
 switchport mode access
 switchport nonegotiate
 switchport port-security
 switchport port-security maximum 3
 switchport protected
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet4/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet5/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

A.2.4 DistributionSwitch-1

```
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname HQ_DS1
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
```

```
interface FastEthernet0/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet1/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10-60
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet2/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10-60
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet3/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10-60
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet4/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet5/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet6/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet7/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet8/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10-60
 switchport mode trunk
 switchport nonegotiate
!
interface GigabitEthernet9/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10-60
 switchport mode trunk
 switchport nonegotiate
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

A.2.5 DistributionSwitch-2

```
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname HQ_DS2
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10-60
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet1/1
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet2/1
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet3/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10-60
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet4/1
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet5/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet6/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet7/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet8/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet9/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10-60
 switchport mode trunk
 switchport nonegotiate
!
interface Vlan1
 no ip address
 shutdown
```

```
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

A.2.6 DistributionSwitch-3

```
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname HQ_DS3
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10-60
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet1/1
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet2/1
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet3/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10-60
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet4/1
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet5/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet6/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet7/1
 switchport access vlan 99
```

```
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface FastEthernet8/1
 switchport access vlan 99
 switchport mode access
 switchport nonegotiate
 shutdown
!
interface GigabitEthernet9/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 10-60
 switchport mode trunk
 switchport nonegotiate
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

A.2.7 HQ_ER1

```
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname HQ_ER1
!
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
!
crypto isakmp key cisco123 address 10.0.1.2
!
!
crypto ipsec security-association lifetime seconds 1800
!
crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
!
crypto map CMAP 10 ipsec-isakmp
 set peer 10.0.1.2
 set pfs group5
 set security-association lifetime seconds 900
 set transform-set 50
 match address 101
!
!
!
```

```
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/1/0
 ip address 10.1.0.3 255.255.255.0
 clock rate 2000000
!
interface Serial0/1/1
 ip address 10.0.1.1 255.255.255.0
 clock rate 2000000
 crypto map CMAP
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 10.2.0.0 255.255.0.0 10.0.1.2
ip route 10.1.0.0 255.255.0.0 10.1.0.2
!
ip flow-export version 9
!
!
!WLC can connect to APs
access-list 101 permit ip host 10.1.10.2 10.2.10.0 0.0.0.255
!tftp server can reply to management
access-list 101 permit ip host 10.1.30.4 10.2.10.0 0.0.0.255
!Database can reply to staff
access-list 101 permit ip host 10.1.30.3 10.2.20.0 0.0.0.255
!management in HQ can access everything in branch
access-list 101 permit icmp 10.1.10.0 0.0.0.255 10.2.0.0 0.0.255.255 echo
access-list 101 permit ip 10.1.10.0 0.0.0.255 10.2.0.0 0.0.255.255
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

A.2.8 HQ_R1

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname HQ_R1
!
!
!
!
```

```
ip dhcp excluded-address 10.1.10.1 10.1.10.10
ip dhcp excluded-address 10.1.20.1 10.1.20.10
ip dhcp excluded-address 10.1.30.1 10.1.30.10
ip dhcp excluded-address 10.1.40.1 10.1.40.10
ip dhcp excluded-address 10.1.50.1 10.1.50.10
ip dhcp excluded-address 10.1.60.1 10.1.60.10
!
ip dhcp pool VLAN_MANAGEMENT
 network 10.1.10.0 255.255.255.0
 default-router 10.1.10.1
ip dhcp pool VLAN_STAFF
 network 10.1.20.0 255.255.255.0
 default-router 10.1.20.1
ip dhcp pool VLAN_SERVICES
 network 10.1.30.0 255.255.255.0
 default-router 10.1.30.1
ip dhcp pool VLAN_LAB
 network 10.1.40.0 255.255.255.0
 default-router 10.1.40.1
ip dhcp pool VLAN_GUEST
 network 10.1.50.0 255.255.255.0
 default-router 10.1.50.1
ip dhcp pool VLAN_PRINTERS
 network 10.1.60.0 255.255.255.0
 default-router 10.1.60.1
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO1941/K9 sn FTX1524Y2CP-
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 10.1.10.1 255.255.255.0
 standby 10 ip 10.1.10.10
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 10.1.20.1 255.255.255.0
 standby 20 ip 10.1.20.20
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 10.1.30.1 255.255.255.0
 standby 30 ip 10.1.30.30
!
interface GigabitEthernet0/0.40
 encapsulation dot1Q 40
 ip address 10.1.40.1 255.255.255.0
 standby 40 ip 10.1.40.40
!
interface GigabitEthernet0/0.50
 encapsulation dot1Q 50
 ip address 10.1.50.1 255.255.255.0
 standby 50 ip 10.1.50.50
!
```

```
interface GigabitEthernet0/0.60
 encapsulation dot1Q 60
 ip address 10.1.60.1 255.255.255.0
 standby 60 ip 10.1.60.60
!
interface GigabitEthernet0/0.70
 encapsulation dot1Q 70
 ip address 10.1.70.1 255.255.255.0
 standby 70 ip 10.1.70.70
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/1/0
 ip address 10.1.0.2 255.255.255.0
 clock rate 2000000
!
interface Serial0/1/1
 no ip address
 clock rate 2000000
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 10.2.0.0 255.255.0.0 10.1.0.3
!
ip flow-export version 9
!
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

A.2.9 HQR2_running-config

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname HQ_R2
!
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO1941/K9 sn FTX1524X14M-
!
!
!
!
```

```
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 10.1.10.2 255.255.255.0
 standby 10 ip 10.1.10.10
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 10.1.20.2 255.255.255.0
 standby 20 ip 10.1.20.20
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 10.1.30.2 255.255.255.0
 standby 30 ip 10.1.30.30
!
interface GigabitEthernet0/0.40
 encapsulation dot1Q 40
 ip address 10.1.40.2 255.255.255.0
 standby 40 ip 10.1.40.40
!
interface GigabitEthernet0/0.50
 encapsulation dot1Q 50
 ip address 10.1.50.2 255.255.255.0
 standby 50 ip 10.1.50.50
!
interface GigabitEthernet0/0.60
 encapsulation dot1Q 60
 ip address 10.1.60.2 255.255.255.0
 standby 60 ip 10.1.60.60
!
interface GigabitEthernet0/0.70
 encapsulation dot1Q 70
 ip address 10.1.70.2 255.255.255.0
 standby 70 ip 10.1.70.70
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
```

```
!
end
```

A.3 (Physical) WLC configuration

```
# WLC Config Begin <Mon Nov 12 16:54:49 2018>
! Number of APs: 1
! Power Supply 1: Absent
! Power Supply 2: Absent
! PID: AIR-CT2504-K9,  SN: PSZ19261RLK
! Product Version: 8.1.102.0
!
! ******************** PORT SUMMARY **********************
!
!            STP   Admin   Physical   Physical   Link   Link
! Pr  Type   Stat   Mode     Mode      Status   Status  Trap     POE
! -- ------- ---- ------- ---------- ---------- ------ ------- -------
! 1  Normal  Forw Enable  Auto       100 Full   Up     Enable  N/A
! 2  Normal  Disa Enable  Auto       Auto       Down   Enable  N/A
! 3  Normal  Disa Enable  Auto       Auto       Down   Enable  Enable  (Power Off)
! 4  Normal  Disa Enable  Auto       Auto       Down   Enable  Enable  (Power Off)
!
! ******************** CDP NEIGHBOUR SUMMARY **********************
!
! Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
!                   S - Switch, H - Host, I - IGMP, r - Repeater,
!                   M - Remotely Managed Device
!
! Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
! Switch           Gig 0/0/1         159            S I     WS-C2960+ Fas 0/2

transfer download filename superfile
transfer download serverip 192.168.10.11
transfer download path /
transfer upload filename superfile
transfer upload serverip 192.168.10.11
transfer upload datatype config
transfer upload path /
config mdns profile service add default-mdns-profile AirTunes
config mdns profile service add default-mdns-profile Airplay
config mdns profile service add default-mdns-profile HP_Photosmart_Printer_1
config mdns profile service add default-mdns-profile HP_Photosmart_Printer_2
config mdns profile service add default-mdns-profile HomeSharing
config mdns profile service add default-mdns-profile Printer-IPP
config mdns profile service add default-mdns-profile Printer-IPPS
config mdns profile service add default-mdns-profile Printer-LPD
config mdns profile service add default-mdns-profile Printer-SOCKET
config mdns profile create default-mdns-profile
config mdns service origin all AirTunes
config mdns service create AirTunes _raop._tcp.local. origin all lss disable
config mdns service origin all Airplay
config mdns service create Airplay _airplay._tcp.local. origin all lss disable
config mdns service origin all HP_Photosmart_Printer_1
config mdns service query enable HP_Photosmart_Printer_1
config mdns service create HP_Photosmart_Printer_1 _universal._sub._ipp._tcp.local. origin all lss disable query enable
config mdns service origin all HP_Photosmart_Printer_2
config mdns service query enable HP_Photosmart_Printer_2
config mdns service create HP_Photosmart_Printer_2 _cups._sub._ipp._tcp.local. origin all lss disable query enable
config mdns service origin all HomeSharing
config mdns service query enable HomeSharing
config mdns service create HomeSharing _home-sharing._tcp.local. origin all lss disable query enable
config mdns service origin all Printer-IPP
config mdns service create Printer-IPP _ipp._tcp.local. origin all lss disable
config mdns service origin all Printer-IPPS
config mdns service create Printer-IPPS _ipps._tcp.local. origin all lss disable
config mdns service origin all Printer-LPD
config mdns service create Printer-LPD _printer._tcp.local. origin all lss disable
config mdns service origin all Printer-SOCKET
config mdns service create Printer-SOCKET _pdl-datastream._tcp.local. origin all lss disable
config interface address management 192.168.10.10 255.255.255.0 192.168.10.1
config interface address virtual 192.168.255.254
config interface address dynamic-interface staff_interface 192.168.20.10 255.255.255.0 192.168.20.1
config interface address dynamic-interface guest 192.168.50.10 255.255.255.0 192.168.50.1
config interface dhcp management primary 192.168.10.1
config interface port management 1
config interface dhcp dynamic-interface staff_interface primary 192.168.20.1
config interface vlan staff_interface 20
config interface create staff_interface 20
config interface port staff_interface 1
```

```
config interface dhcp dynamic-interface guest primary 192.168.50.1
config interface vlan guest 50
config interface create guest 50
config interface port guest 1
config time ntp interval 10000
config time ntp server 1 129.241.0.123
config certificate generate webadmin
config ipv6 multicast mode multicast
config 802.11a cac voice sip codec g711 sample-interval 20
config 802.11a cac voice sip bandwidth 64 sample-interval 20
config 802.11b 11gsupport enable
config 802.11b cac voice sip codec g711 sample-interval 20
config 802.11b cac voice sip bandwidth 64 sample-interval 20
config mobility group domain mobility_group_1
config license boot base
config country NO
config network webmode enable
config network rf-network-name mobility_group_1
config network mgmt-via-wireless enable
config network multicast l2mcast disable service-port
config network multicast l2mcast disable virtual
config network multicast mode multicast 239.0.1.1
config network multicast mode multicast
config ap preferred-mode ipv4 all
config ap packet-dump truncate 0
config ap packet-dump capture-time 10
config ap packet-dump buffer-size 2048
config sysname wlc
config mgmtuser add encrypt admin 1 a74ca828ef76613bfa79b6b0ce7bcd65 1d89f36f05397b93149c6e6d2c139fbf9c3405e9 16
 ↪   d189c1ad81a41a30719b1eb862e3f479000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
 ↪   read-write
config wlan radius_server acct interim-update disable 1
config wlan radius_server acct interim-update disable 2
config wlan session-timeout 1 0
config wlan interface 1 staff_interface
config wlan session-timeout 2 0
config wlan interface 2 guest
config wlan mfp client enable 1
config wlan create 1 STAFF_WLAN STAFF_WLAN
config wlan mfp client enable 2
config wlan create 2 GUEST_WLAN GUEST_WLAN
config wlan wmm allow 1
config wlan broadcast-ssid enable 1
config wlan wmm allow 2
config wlan broadcast-ssid enable 2
config wlan security wpa akm 802.1x disable 1
config wlan security wpa akm psk set-key hex encrypt 1 8f88d1cf010317e837f165018aa2b474 edeeba6b3b64cef777638c3712e011ebe08fcfbc 48
 ↪   57e6138c40ef93656d314af0fd2116c030ec8a19ab7dbbbab3d240d0f557bb5a8b682669c2e43ce862cca4409571d06e0000000000000000000000000000000000000000000000000000000
 ↪   1
config wlan security wpa akm psk enable 1
config wlan security wpa enable 1
config wlan security web-auth server-precedence 1 local radius ldap
config wlan exclusionlist 1 60
config wlan enable 1
config wlan security wpa akm 802.1x disable 2
config wlan security wpa akm psk set-key hex encrypt 1 e4955ffa439c6dd54a687ca1451415e6 42431cd510badb76e563075ba5d2f63f351572e6 48
 ↪   aad796bfb0715fc7111152812ac81788e49c2f50aec62625c7e4b371fa54d7ac4e8ec262cbb900410162723c322fca4c0000000000000000000000000000000000000000000000000000000
 ↪   2
config wlan security wpa akm psk enable 2
config wlan security wpa enable 2
config wlan security web-auth server-precedence 2 local radius ldap
config wlan exclusionlist 2 60
config wlan enable 2
config sys-nas wlc
config database size 2048
config advanced probe-limit 2 500
config advanced 802.11a channel add 36
config advanced 802.11a channel add 40
config advanced 802.11a channel add 44
config advanced 802.11a channel add 48
config advanced 802.11a channel add 52
config advanced 802.11a channel add 56
config advanced 802.11a channel add 60
config advanced 802.11a channel add 64
config advanced 802.11b channel add 1
config advanced 802.11b channel add 6
config advanced 802.11b channel add 11
config advanced probe limit 2 500
config switchconfig strong-pwd lockout attempts mgmtuser 3
config switchconfig strong-pwd lockout time mgmtuser 5
config mesh convergence

# WLC Config End <Mon Nov 12 16:54:54 2018>
```