Network Risk and Security – Group 7 Project

DESIGN CONCEPT

Our Team of consultants has been hired to create a secure design of small modules that connect to the Govt. of Canada's provincial offices and then to the main office in Ottawa. This design provides remote network connectivity which is also secure and mitigates several risks. Our modular packages consist of a firewall, one router, two switches supporting 24 wired and 24 wireless IoT devices like laptops, phones, etc. Our provincial offices will have 1 WLC, RADIUS Server and the modules would have authentication enabled along with Wireless Access Points to connect remotely. Using a WLC in each province, creating IPsec tunnels and enabling security measures, we'll ensure our design is resistant to cyberattacks.

IP ADDRESSING

The provincial offices and their respective subnets are as follows:

Province	Subnet / IP Range	Subnet Mask	WAN
Alberta	192.168.1.1 - 192.168.1.62	255.255.255.192	1.1.1.1
British Columbia	192.168.2.1 - 192.168.2.62	255.255.255.192	2.2.2.2
Manitoba	192.168.3.1 - 192.168.3.62	255.255.255.192	3.3.3.3
New Brunswick	192.168.4.1 - 192.168.4.62	255.255.255.192	4.4.4.4
Newfoundland and Labrador	192.168.5.1 - 192.168.5.62	255.255.255.192	5.5.5.5
Northwest Territories	192.168.6.1 - 192.168.6.62	255.255.255.192	6.6.6.6
Nova Scotia	192.168.7.1 -192.168.7.62	255.255.255.192	7.7.7.7
Nunavut	192.168.8.1 - 192.168.8.62	255.255.255.192	8.8.8.8
Ontario	192.168.9.1 - 192.168.9.62	255.255.255.192	9.9.9.9
Prince Edward Island	192.168.10.1 - 192.168.10.62	255.255.255.192	10.10.10.10
Quebec	192.168.11.1 - 192.168.11.62	255.255.255.192	11.11.11.11
Saskatchewan	192.168.12.1 - 192.168.12.62	255.255.255.192	12.12.12.12
Yukon	192.168.13.1 -192.168.13.62	255.255.255.192	13.13.13.13

The IP tables for provincial offices are as follows:

Alberta

Device	Interface	IP	Subnet Mask
R1	G0/0	192.168.1.1	255.255.255.192
	G0/1	192.168.1.2	255.255.255.192
	G1/0	192.168.1.3	255.255.255.192
	WLAN (public)	1.1.1.1	
	G0/2	192.168.1.7	255.255.255.192
	G0/3	192.168.1.8	255.255.255.192
S1	G0/0	192.168.1.4	255.255.255.192
S2	G0/0	192.168.1.5	255.255.255.192
WLC	GigEth0	192.168.1.6	255.255.255.192
Radius Server	FastEth0	192.168.1.9	255.255.255.192

British Columbia

Device	Interface	IP	Subnet Mask
R1	G0/0	192.168.2.1	255.255.255.192
	G0/1	192.168.2.2	255.255.255.192
	G1/0	192.168.2.3	255.255.255.192
	WLAN (public)	2.2.2.2	
	G0/1	192.168.2.7	255.255.255.192
	G0/2	192.168.2.8	255.255.255.192
S1	G0/0	192.168.2.4	255.255.255.192
S2	G0/0	192.168.2.5	255.255.255.192
WLC	GigEth0	192.168.2.6	255.255.255.192
Other Access Points		192.168.2.10-62	
Radius Server	FastEth0	192.168.2.9	255.255.255.192

Manitoba

Device	Interface	IP	Subnet Mask
R1	G0/0	192.168.3.1	255.255.255.192
	G0/1	192.168.3.2	255.255.255.192
	G1/0	192.168.3.3	255.255.255.192
	WLAN (public)	3.3.3.3	
	G0/2	192.168.3.7	255.255.255.192
	G0/3	192.168.3.8	255.255.255.192
S1	G0/0	192.168.3.4	255.255.255.192
S2	G0/0	192.168.3.5	255.255.255.192
WLC	GigEth0	192.168.3.6	255.255.255.192
Other Access Points		192.168.3.10-62	
Radius Server	FastEth0	192.168.3.9	255.255.255.192

New Brunswick

Device	Interface	IP	Subnet Mask
R1	G0/0	192.168.4.1	255.255.255.192
	G0/1	192.168.4.2	255.255.255.192
	G1/0	192.168.4.3	255.255.255.192

	WLAN (public) G0/2 G0/3	4.4.4.4 192.168.4.7 192.168.4.8	 255.255.255.192 255.255.255.192
S1	G0/0	192.168.4.4	255.255.255.192
S2	G0/0	192.168.4.5	255.255.255.192
WLC	GigEth0	192.168.4.6	255.255.255.192
Other Access Points		192.168.4.10-62	
Radius Server	FastEth0	192.168.4.9	255.255.255.192

Newfoundland and Labrador

Device	Interface	IP	Subnet Mask
R1	G0/0 G0/1 G1/0 WLAN (public) G0/2 G0/3	192.168.5.1 192.168.5.2 192.168.5.3 5.5.5.5 192.168.5.7 192.168.5.8	255.255.255.192 255.255.255.192 255.255.255.192 255.255.255.192 255.255.255.192
S1	G0/0	192.168.5.4	255.255.255.192
S2	G0/0	192.168.5.5	255.255.255.192
WLC	GigEth0	192.168.5.6	255.255.255.192
Other Access Points		192.168.5.10-62	
Radius Server	FastEth0	192.168.5.9	255.255.255.192

Northwest Territories

Device	Interface	IP	Subnet Mask
R1	G0/0 G0/1 G1/0 WLAN (public) G0/2 G0/3	192.168.6.1 192.168.6.2 192.168.6.3 6.6.6.6 192.168.6.7 192.168.6.8	255.255.255.192 255.255.255.192 255.255.255.192 255.255.255.192 255.255.255.192
S1	G0/0	192.168.6.4	255.255.255.192
S2	G0/0	192.168.6.5	255.255.255.192
WLC	GigEth0	192.168.6.6	255.255.255.192
Other Access Points		192.168.6.10-62	
Radius Server	FastEth0	192.168.6.9	255.255.255.192

Nova Scotia

Device	Interface	IP	Subnet Mask
R1	G0/0 G0/1 G1/0 WLAN (public) G0/2 G0/3	192.168.7.1 192.168.7.2 192.168.7.3 7.7.7.7 192.168.7.7 192.168.7.8	255.255.255.192 255.255.255.192 255.255.255.192 255.255.255.192 255.255.255.192
S1	G0/0	192.168.7.4	255.255.255.192

S2	G0/0	192.168.7.5	255.255.255.192
WLC	GigEth0	192.168.7.6	255.255.255.192
Other Access Points		192.168.7.10-62	
Radius Server	FastEth0	192.168.7.9	255.255.255.192

Nunavut

Device	**Interface**	**IP**	**Subnet Mask**
R1	G0/0 G0/1 G1/0 WLAN (public) G0/2 G0/3	192.168.8.1 192.168.8.2 192.168.8.3 8.8.8.8 192.168.8.7 192.168.8.8	255.255.255.192 255.255.255.192 255.255.255.192 255.255.255.192 255.255.255.192
S1	G0/0	192.168.8.4	255.255.255.192
S2	G0/0	192.168.8.5	255.255.255.192
WLC	GigEth0	192.168.8.6	255.255.255.192
Other Access Points		192.168.8.10-62	
Radius Server	FastEth0	192.168.8.9	255.255.255.192

Ontario

Device	**Interface**	**IP**	**Subnet Mask**
R1	G0/0 G0/1 G1/0 WLAN (public) G0/2 G0/3	192.168.9.1 192.168.9.2 192.168.9.3 9.9.9.9 192.168.9.7 192.168.9.8	255.255.255.192 255.255.255.192 255.255.255.192 255.255.255.192 255.255.255.192
S1	G0/0	192.168.9.4	255.255.255.192
S2	G0/0	192.168.9.5	255.255.255.192
WLC	GigEth0	192.168.9.6	255.255.255.192
Other Access Points		192.168.9.10-62	
Radius Server	FastEth0	192.168.9.9	255.255.255.192

Prince Edward Island

Device	**Interface**	**IP**	**Subnet Mask**
R1	G0/0 G0/1 G1/0 WLAN (public) G0/2 G0/3	192.168.10.1 192.168.10.2 192.168.10.3 10.10.10.10 192.168.10.7 192.168.10.8	255.255.255.192 255.255.255.192 255.255.255.192 255.255.255.192 255.255.255.192
S1	G0/0	192.168.10.4	255.255.255.192
S2	G0/0	192.168.10.5	255.255.255.192
WLC	GigEth0	192.168.10.6	255.255.255.192
Other Access Points		192.168.10.10-62	

Radius Server	FastEth0	192.168.10.9	255.255.255.192

Quebec

Device	Interface	IP	Subnet Mask
R1	G0/0	192.168.11.1	255.255.255.192
	G0/1	192.168.11.2	255.255.255.192
	G1/0	192.168.11.3	255.255.255.192
	WLAN (public)	11.11.11.11	
	G0/2	192.168.11.7	255.255.255.192
	G0/3	192.168.11.8	255.255.255.192
S1	G0/0	192.168.11.4	255.255.255.192
S2	G0/0	192.168.11.5	255.255.255.192
WLC	GigEth0	192.168.11.6	255.255.255.192
Other Access Points		192.168.11.10-62	
Radius Server	FastEth0	192.168.11.9	255.255.255.192

Saskatchewan

Device	Interface	IP	Subnet Mask
R1	G0/0	192.168.12.1	255.255.255.192
	G0/1	192.168.12.2	255.255.255.192
	G1/0	192.168.12.3	255.255.255.192
	WLAN (public)	12.12.12.12	
	G0/2	192.168.12.7	255.255.255.192
	G0/3	192.168.12.8	255.255.255.192
S1	G0/0	192.168.12.4	255.255.255.192
S2	G0/0	192.168.12.5	255.255.255.192
WLC	GigEth0	192.168.12.6	255.255.255.192
Other Access Points		192.168.12.10-62	
Radius Server	FastEth0	192.168.12.9	255.255.255.192

Yukon

Device	Interface	IP	Subnet Mask
R1	G0/0	192.168.13.1	255.255.255.192
	G0/1	192.168.13.2	255.255.255.192
	G1/0	192.168.13.3	255.255.255.192
	WLAN (public)	13.13.13.13	
	G0/2	192.168.13.7	255.255.255.192
	G0/3	192.168.13.8	255.255.255.192
S1	G0/0	192.168.13.4	255.255.255.192
S2	G0/0	192.168.13.5	255.255.255.192
WLC	GigEth0	192.168.13.6	255.255.255.192
Other Access Points		192.168.13.10-62	
Radius Server	FastEth0	192.168.13.9	255.255.255.192

For the modules, we'll use 10.0.0.0 range with 255.255.0.0 subnet mask. The reason behind this is the ability to assign as many hosts as we want in our modules. Since our modules will also be used by large farms, it is necessary that we use an IP range big enough to accommodate all the hosts.

Using this addressing will give us 65,534 usable hosts, that will easily fulfill the client demands.

Device	IP Address	Subnet Mask
Router	10.0.1.1	255.255.0.0
Switch1	10.0.1.2	255.255.0.0
Switch2	10.0.1.3	255.255.0.0
Access Point	10.0.1.4	255.255.0.0

NETWORK DIAGRAMS

Each module will have 1 router (R1 in this case), two switches capable of 24 interfaces each, with 24 devices capable of connecting wirelessly due to Wireless Access Point connected. The firewall here will be responsible for providing security and mitigating risks.

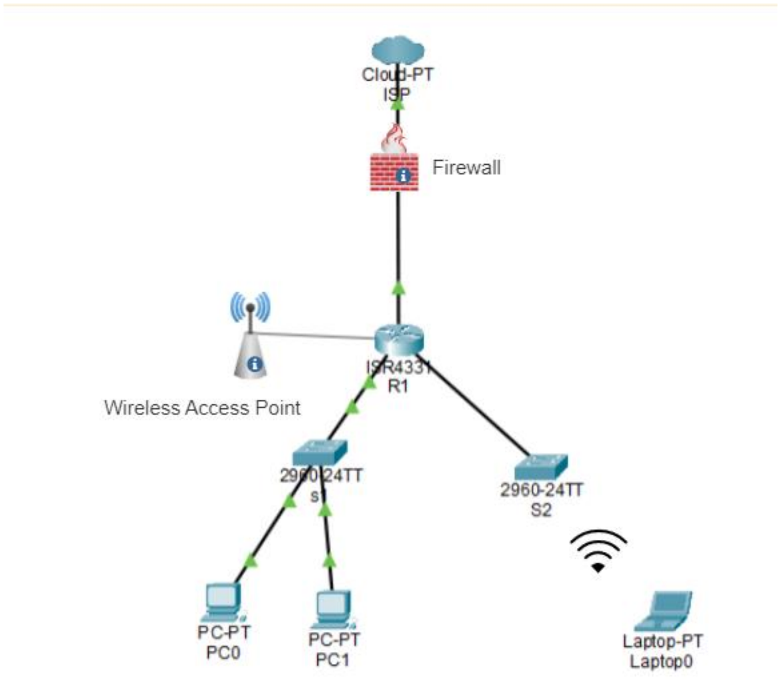

Figure 1: Network Diagram of the Module

Our provincial offices will have 1 WLC, 1 RADIUS server each because of the reasons explained in the following sections. They will be vital for our wireless connectivity and successful authentication, respectively.

Our network of provincial offices should look like this:

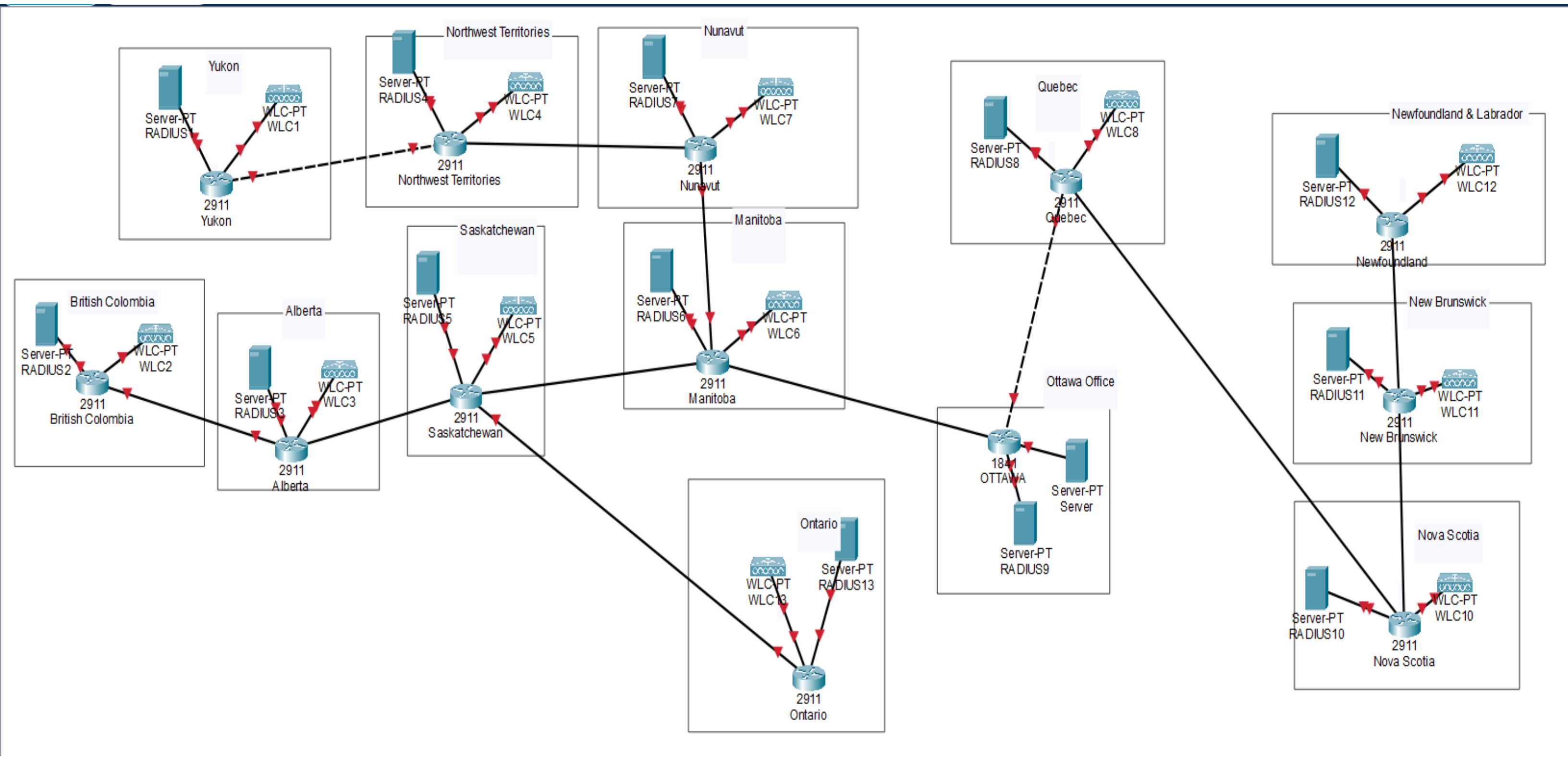

Figure 2: Provincial offices connecting to Ottawa

Hardware

We have tried to make our design as much cost-effective as possible by getting the equipment just right for the work, leaving some room for future expansion. For example, our Switches have PoE ports too in giving more functionality for future cases. We have chosen Linksys Access Points because they have in-built functionality to set up with up to 4 global RADIUS servers and support PoE as well.

For each module:

Hardware	**Model**	**Price (CAD)**
Router	Cisco Router ISR 900 – C941-4P	$1080.22
Switch	Cisco Catalyst 9200L	$1150
Access Point	Linksys LAPAC1200C-CA Business AC1200 Wi-Fi Access Point	$140
Cisco Firewall	ASA5505-50-BUN-K8	$1100

For each Province:

Hardware	**Model**	**Price (CAD)**
RADIUS Server	ASR5K-00-CSXXAAA	$900
WLC	Cisco 5500 Controller AIR-CT5508-12-K9 Cisco 5508 Series Wireless Controller	$6000

We will get a good WLC like the one mentioned above, which meets all our security and encryption requirements like WPA, IPsec, WEP, AES, TLS/SSL, IEEE 802.1X and RADIUS Authentication, accounting, and tunnel accounting.

SECURITY

Security is the most important part in any network. No matter how fast/redundant a network is, its becomes obsolete if proper security measures are not configured. Below are some examples of attacks we might face, and their possible solutions.

1) **ARP Poisoning Attacks:** Static ARP tables, switch security, encryption, network isolation.
2) **STP attack:** Configure PortFast feature and enable BPDU Guard.
3) **MAC address Flooding**: Port Security and assign one MAC address per port.
4) **MAC spoofing:** Enable Port Security and assign one MAC address per port.
5) **DHCP Spoofing:** DHCP snooping - switch goes into disabled mode if compromise is detected.
6) **VLAN Hopping attacks:** If we create VLANs in the modules, these might happen. This can be prevented by removing unnecessary trunk ports and VLAN tagging.

We'll take the above prevention steps as mentioned and will also do the following measures to secure our network while still providing reliable connectivity.

1) **Zone-Based Firewalls**: We'll set up Zone based firewalls in each module which separates the internal zone with the external. Since our module is connected to ISP, we will make the ISP OUT_ZONE and the rest of our network as IN_ZONE. Now we will be able to control traffic going from OUT_ZONE to IN_ZONE and vice versa.

   i) IN_ZONE to OUT_ZONE: Enable FTP and HTTP
   ii) OUT_ZONE to IN_ZONE: Enable TELNET, SSH, HTTP

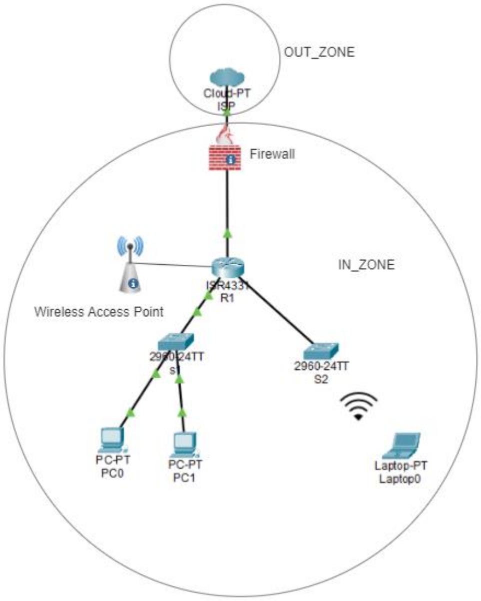

Figure 3: Zones created for each module.

2) **ACLs:** We can also define Network ACLs to configure the traffic to only those protocols that are needed and deny the rest of the traffic.

3) **IPsec Remote-Access VPN:** The remote access VPN will be set up from the modular package routers to the provincial offices over IPsec. Using the IPsec framework, we can use specific algorithms and can implement better ones over time without the need to patch existing IPsec standards. We'll use HMAC – MD5 algorithm to maintain the integrity of our data transfer.

4) **Using AES Encryption:** AES encryption is an efficient symmetric key cryptosystem which lets us choose our choice of key length out of 128, 192 or 256 bits. In this case, we'll be going with the AES 256-bit encryption to maintain the maximum security possible making it much harder to crack.

5) **Principle of Least Privilege:** Giving users only those permissions that they need to get their work done. This forms an essential part of Zero-Trust policy.

6) **Cisco IOS Login Enhancements** – This will allow the users to enhance the security of a router by configuring options to automatically block further login attempts when a possible denial-of-service attack is detected.

7) **Port Security** – This will protect the switch being flooded with unknown MAC addresses by limiting the number of MAC addresses learned per port. This will prevent multiple attacks.

8) **Firewall Setup** – Each module has an ASA Firewall that will protect against several attacks and keep our module secure and can also protect from zero-day attacks.

9) **Restricted Usage –** We can enable Wireless security to restrict visiting of unsecured websites or not safe for work websites to limit chances of getting infected with malware.

10) **Change SSIDs –** For wireless networks, it's best practice to never use default SSIDs for Wireless networks.

We will also be following the Cybersecurity frameworks and constantly updating the firmware to remove any vulnerabilities and mitigate new attacks. This webpage from Cisco is a good reference for our security team. Moreover, using IPS/IDS would be a great security practice which will greatly improve our network's security.

While all this is the technical aspect of security, it is important to realize Social Engineering is also one of the most common reasons behind security breaches, it is important that the users/employees get enough cyber training and are educated about these attacks, so they don't become victims to attacks and compromise the whole network's security.

SOFTWARE AND WIRELESS

So far, the only software we might need to use would be the security packages for our Cisco Devices, and VPN, if users in the Provincial offices want to connect to the Ottawa office or vice versa. Apart from the Site-to-Site VPNs, we can allow remote users to log in to company network using OpenVPN.

To set up Wireless accessibility in our network (between provincial offices and modules), we'll place WLC on each provincial office, with Access Points in each module. The Access points would increase the wireless network coverage in the modular packages. These access points are cheap and will be a cost-effective option to extend our wireless coverage throughout the modules.

We can use the WLC in the provincial offices to secure our provincial office wireless networks too. Ideally, we should create two Wi-Fi networks: one for the verified users and one for guests. The guest Wi-Fi will have limited permissions and it can't be used by the attacker. This mitigates multiple attacks at once, since unauthenticated users won't have access to services like Printing, internal sites, etc.

We'll use **WPA3 authentication** for our wireless network as it's the safest method of authentication and much harder to crack than the other options. Our WLC in each provincial office can support WPA3 and several security options can be set. We can also block certain IP addresses from reaching our network, define policies geographically limiting access from countries where we don't expect traffic from like North Korea, Russia, etc.

Its crucial to make sure the Access points are secured to prevent attacks like piggybacking, where attackers in the wireless range might steal data. Using at least WPA2 encryption on ALL access points, preferably WPA3 will mitigate these risks.

AUTHENTICATION AND LOGGING

This part covers the AAA aspect of computer networking. AAA stands for Authentication, Authorization and Accounting.

Authentication refers to the process of verifying a user and confirming they are what they're claiming to be, and authorization is the process of assigning an authenticated user certain controls/access to a network.

Together AAA forms a crucial part in any secure network and it's necessary to use proper authentication and logging methods.

There are mainly two types of authentication methods: Local Database and Server Based.

In local database authentication, user account authentication is set up locally using global configuration mode, and login local line configuration is done by setting up console, VTY ports with passwords. While this method provides accountability, it's not scalable to multiple routers on the network. But it can be used as a backup in case a stronger form of authentication fails.

Server based authentication requires a RADIUS/TACACS+ server to centrally store authentication database and is the most preferred method in Enterprise environments like ours. It also supports following authentication methods:

- Digital certificates
- One-time passwords
- Changeable passwords
- Static passwords
- UNIX authentication using the /etc/password file
- NT database authentication

So, in this case, we'll mainly focus on Server based authentication and if possible, set up local database authentication as a backup to provide redundancy.

For Server-based authentication, we recommend using a RADIUS server due to the following reasons:

1) It supports a wide range of devices. In a big enterprise network like ours, we'd by limited by just Cisco devices if we opt for TACACS+.
2) Encrypts all communication.
3) Authentication and Authorization is recorded.
4) Secure and protocol exchanges are encrypted.

While our devices have been secured, we can also enable RADIUS authentication on VPNs like OpenVPN. This would provide a web interface for authentication too.

We'll also use 802.X based Authenticator in between the RADIUS server and client workstations to enable port-based security. "802.1x is port-based access control and authentication protocol that restricts unauthorized workstations from connecting to a LAN through publicly accessible switch ports.
The authentication server authenticates each workstation that is connected to a switch port before making available any services offered by switch or the LAN." *(Richardson, 2022)*

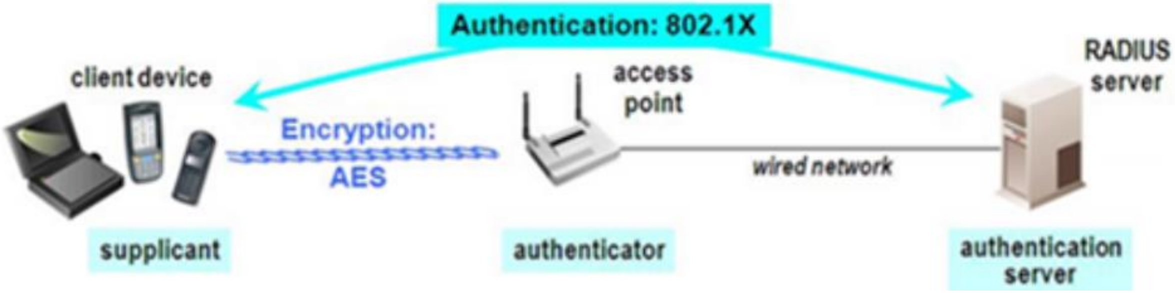

Figure 4: Example of RADIUS authentication.

RADIUS Authentication will also be configured on our Access Points in each module.

Logging:

Logging falls under the accounting category in AAA.

We'll be using syslog to enable logging on to our Cisco devices. We can use the default configuration and add timestamping of log messages for our convenience and better security insights.

To prevent logging of unwanted events, we should **set the logging levels to 4 and more**. Below is a table with Logging level keywords and their corresponding information.

Level Keyword	Level	Description	Syslog Definition
emergencies	0	System unstable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

The following Logging types will be configured: Console Logging, Terminal logging and syslog logging.

On our WLC, we can enable logs by going to System > Management > Logs to generate logs regarding our Wireless connections. The Access Points also have logs/GUI called Linksys Cloud Manager.

The syslog messages would then be sent to our local servers in each province, and ultimately to our Ottawa server. In case there's a network issue within our modules, the flash memory within the devices will store some logs that can be useful for us.

QUESTIONS

Q1) Identify cybersecurity threats (wired\ wireless) that your design mitigates and are there any that require additional controls?

A1) Our design mitigates several threats that are also mentioned in the Security part of this document. The design mitigates the following threats:

1) ARP Poisoning Attacks
2) STP attack
3) MAC address Flooding
4) MAC spoofing
5) DHCP Spoofing
6) VLAN Hopping attacks
7) MITM attacks (by using Remote access VPN)

There are a few more threats that our design can mitigate more efficiently, like getting the exact location of a rogue device using Cisco Wireless Control System Navigator. I has to bought separately and requires a few additional controls but is helpful in the long run.

Q2) What additional features would you recommend and how would you adjust your design to accommodate?

A2) We'll recommend the following things:

a) Cisco Wireless Control System Navigator for more insights on Wireless Networks. It is really helpful when detecting Wireless connectivity issues. The license can be bought for $3000 and can host up to 50 Access Points. This might not be the most cost-effective option but worth it when dealing with several Access Points and IoT devices.

b) Configuring an AP from one module to host devices in other module (when using several modules together) in case of a failure. This would be done by changing the settings for the Access Point.

c) Using an IPS/IDS can increase the overall security. Using Next-generation Firewalls (for small enterprises) would be cost effective, increase security as well as provide a GUI to visualize logs, trends. Popular NGFW brands include Cisco, Fortinet, Palo Alto, SonicWall, etc.

d) Establish a mesh network from Provincial offices to Ottawa office. With the right security controls attached, this would create a fault-tolerant link. For example, if British Columbia offices' can't directly send the data to Ottawa HQ, it can send it to Calgary's office which can then forward it to Ottawa. This could use Link Aggregation Control Protocol (LACP).

Q3) What would limit the scalability of your design?

A3) The following things can limit the scalability of our design:

a) The subnet for our provincial offices can have up to 64 hosts. We can change the subnet size to include more hosts.
b) Using 2 switches per module gives us the ability to connect 24 wired and 24 wireless IoT devices only. To scale or include more devices in our module, we'll have to add more switches.
c) Up to 1500 APs can register with our Cisco WLC 5500. While this seems enough for our current environment, it might possess some issues in a few years when thousands of modules are deployed. We can prevent this by upgrading the WLC or getting one more for each province.

Q4) Calculate the cost of the equipment in your module and is this cost effective?

A4) Our total cost of equipment in the module is $3470, which is cost-effective considering all the technology in a single module providing secure remote connectivity to the offices.

REFERENCES

Popeskic, V. (2011, December 14). Switch Security Attacks – Layer 2 Security. How Does Internet Work. https://howdoesinternetwork.com/2011/switch-security-attackshttps://howdoesinternetwork.com/2011/switch-security-attacks

Red Hat Customer Portal (n.d.). Red Hat Customer Portal., from https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html-single/system-level_authentication_guide/index

Richardson, S. (2022, November 3). Port Based Authentication - Routing Table. Cisco Certified Expert. https://www.ccexpert.us/routing-table/x-portbased-authentication.html

Wireless, RF (n.d.) ARP attack types. Retrieved December 9, 2022, from https://www.rfwireless-world.com/Articles/ARP-attack-types-MAC-flooding-and-ARP-Spoofing.html

Hardware Price Quotes:

https://www.router-switch.com/c921-4p.html

https://www.cdw.ca/product/cisco-catalyst-9200l-network-essentials-switch-48-ports-managed-r/5367780

https://www.router-switch.com/asa5505-50-bun-k8-p-591.html

https://itprice.com/cisco/asr5k-00-csxxaaa.html

https://www.router-switch.com/air-ct5508-12-k9-p-3547.html

https://www.amazon.ca/Linksys-LAPAC1200C-CA-Centralized-Management-Real-Time/dp/B07KVMJPQW/ref=asc_df_B07KVMJPQW/?tag=googleshopc0c-20&linkCode=df0&hvadid=335186302991&hvpos=&hvnetw=g&hvrand=14402445131994730506&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=1002216&hvtargid=pla-654494576282&psc=1