

Report On The Updated Network Configuration of Oceanview

(Completed: 14th December 2023)

The following has been constructed as the updated network configuration for Oceanview:

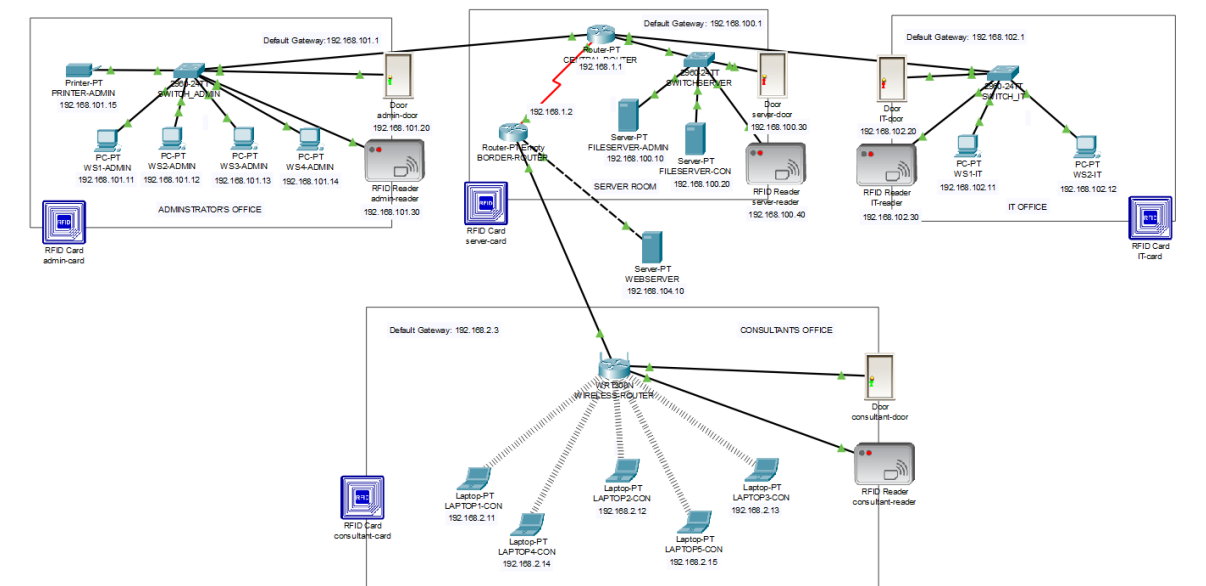


Figure 1 - Oceanview's Network Configuration

Introduction

This report will cover all the configuration's major security measures and recommendations which could be useful for Oceanview as the organisation continues to maintain and improve. The organisation could be defined as a small business, possessing confidential data with value such as financial information on its employees and its customers. Banham (2017) mentioned a 2016 study which stated that 55% of small businesses (employees fewer than 100 up to 1000) experienced a cyberattack in the previous 12 months, with 50% experiencing some data breach over the period with nearly 600 respondents within the research finding these companies. This means that Oceanview needs to make accurate considerations with the assumption that there could be a high chance of a data breach from an unknown vulnerability when maintaining the network.

Recommendations For Updated Network Configuration

Static IP Addresses & MAC Addresses

All Internet Protocol (IP) Addresses in the configuration are static which means they are allocated an address that is permanent. They could be needed for organisations who

maintain their own web server, other Internet connected servers and external devices (Google, 2023). This provides faster connections between devices in the network. In the configuration, the business has its own web server with a minimal number of devices, so it is a viable option. Also, it is good practice to produce a table of MAC addresses for all devices as MAC spoofing is a possibility for the attacker to hide their identity however this table will check all MAC addresses and any foreign MAC address will be blocked.

Devices	Room	IP Addresses	Subnet Mask	Default Gateway	MAC Addresses
WS1-ADMIN WS2-ADMIN WS3-ADMIN WS4-ADMIN PRINTER-ADMIN admin-door admin-reader	Administrator's Office	192.168.101.11 192.168.101.12 192.168.101.13 192.168.101.14 192.168.101.15 192.168.101.20 192.168.101.30	255.255.255.0	192.168.101.1	0006.2AB8.E72C 0090.21EF.0E9E 0090.2BA9.0B90 000C.8522.EBDD 00D0.DC96.7D7C 00E0.A33A.E13A 0040.0B22.1CCB
LAPTOP1-CON LAPTOP2-CON LAPTOP3-CON LAPTOP4-CON LAPTOP5-CON consultant-door consultant-reader	Consultant's Office	192.168.2.11 192.168.2.12 192.168.2.13 192.168.2.14 192.168.2.15 192.168.2.20 192.168.2.30	255.255.255.0	192.168.2.3	00D0.BC6C.1B59 00E0.F7D9.35BB 00E0.B093.7E84 0090.0CC4.9B4E 0002.17D3.DDDD 00E0.8FB1.346B 0001.9687.BCB7
WS1-IT WS2-IT IT-door IT-reader	IT Office	192.168.102.11 192.168.102.12 192.168.102.20 192.168.102.30	255.255.255.0	192.168.102.1	00D0.FF5D.4022 000C.85EC.1EC7 0090.0C2C.E166 0001.426D.7E11
FILESERVER-ADMIN FILESERVER-CON server-door server-reader	Server Room	192.168.100.10 192.168.100.20 192.168.100.30 192.168.100.40	255.255.255.0	192.168.100.1	00E0.F920.273C 00D0.D31E.7488 00D0.582B.328C 0030.A33D.DDDB
WEB-SERVER	N/A	192.168.104.10	255.255.255.0	192.168.104.1	000A.F3EE.4018

This table contains all the static IP and MAC addresses of all devices connected to Oceanview's network. As stated in one of the requirements, only the IT has full access of everything, so this table ensures proper network management.

Access Control Lists

One of the specified requirements included was to stop devices in 'Administrator's Room' and 'Consultant's Room' from communicating with another and their servers (Administrator's cannot access Consultant file server, Consultant's cannot access Administrator file server). Access Control Lists (ACL) were implemented into the central router, providing limitations to users to access or deny interactions with other devices on the network. This will reduce the possible chance of an insider's attack from rogue employees and mitigate breaches by

cyber-criminals if there was the possibility of one or more devices within a room being hijacked (Sandhu & Samarati,1994).

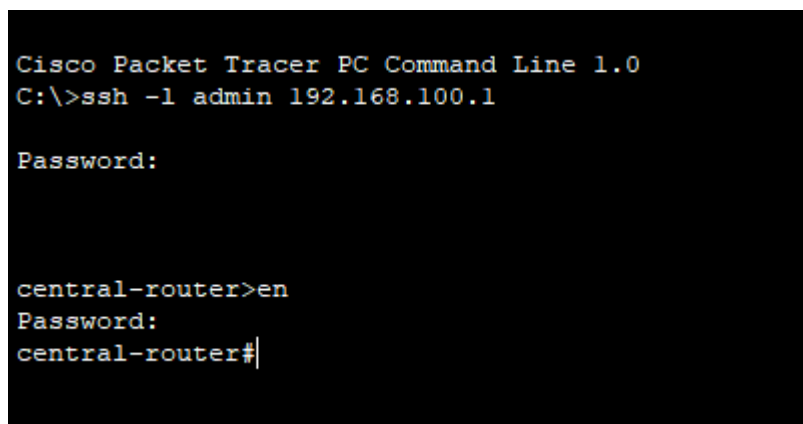
```
Extended IP access list 100
 10 deny ip 192.168.101.0 0.0.0.255 host 192.168.100.20
 20 deny ip 192.168.2.0 0.0.0.255 host 192.168.100.10
 30 permit ip any any (21855 match(es))
Extended IP access list 105
 10 deny ip 192.168.101.0 0.0.0.255 192.168.2.0 0.0.0.255
 20 permit ip any any (11913 match(es))
```

Figure 2 - (CENTRAL-ROUTER ACL Configuration)

Using SSH

To ensure data is transferred securely over the organisation's network, the Secure Shell network communication protocol was configured. Administrators and IT are able to access the network remotely on their workstations where they can modify the network configuration however, they require the username and password for the specific router.

Name of router	Username	Password
CENTRAL-ROUTER	admin	admin
BORDER-ROUTER	border	border



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 192.168.100.1

Password:

central-router>en
Password:
central-router#
```

Figure 3 – Using SSH on workstation's CLI

Wireless Network Security

This is essential to provide security to the consultants on their wireless network, but it is significant for securing the entirety of the network. Wi-Fi Protected Access 2 Personal (WPA2-PSK) security was placed within the consultant's wireless router with Advanced Encryption Standard (AES) used to encrypt data, meaning only the consultants can access the network using a pre-shared key consisting of a password more than 8 characters. However, the biggest vulnerability from this would be the password being leaked as this password is accessed by all in the room so any fired or rogue consultants could share this password outside of the organisation or to other sectors and the Service Set Identifier (SSID) is publicly seen which allows cyber-criminals to know the wireless network exists (Radivilova & Hassan, 2017).

SSID	con_wireless		
2.4 GHz Channel	1 - 2.412GHz		
Coverage Range (meters)	150.00		
Authentication <input type="radio"/> Disabled <input type="radio"/> WEP WEP Key <input type="text"/> <input type="radio"/> WPA-PSK <input checked="" type="radio"/> WPA2-PSK PSK Pass Phrase <input type="text" value="Kp7FnSExWF"/> <input type="radio"/> WPA <input type="radio"/> WPA2			
RADIUS Server Settings			
IP Address	<input type="text"/>		
Shared Secret	<input type="text"/>		
Encryption Type	AES		

Figure 4 – Consultant's wireless network configuration

WPA2-Enterprise is recommended to replace WPA2-PSK, but it would require an authentication RADIUS server which increases expenses. Until an additional server is added, to combat the drawbacks of WPA2-PSK the consultant network will need to go through high strictness measures:

- Every month or when a consultant is fired, the pre-shared key instantly changed
- All laptops counted at the end of the day

RFID Door, Reader & Keycard

Additionally, physical security must be considered. Radio Frequency Identification has been popular for contactless access to secure physical areas such as offices that involve a keycard and a reader (Rieback et al, 2006). This provides physical access control.

Registration Server Login

Username:

Password:

Don't have an IoT account? [Sign up now](#)

Physical Config Services **Desktop** Programming Attributes

Web Browser

[Conditions](#) [Editor](#) [Log Out](#)

IoT Server - Devices

▶ ● admin-door (PTT08103XYS-) Door

▶ ● admin-reader (PTT0810O11K-) RFID Reader

Actions		Enabled	Name	Condition	Actions
Edit	Remove	Yes	rfid valid	admin-reader Card ID = 101	Set admin-reader Status to Valid
Edit	Remove	Yes	rfid invalid	admin-reader Card ID != 101	Set admin-reader Status to Invalid
Edit	Remove	Yes	door unlock	admin-reader Status is Valid	Set admin-door Lock to Unlock
Edit	Remove	Yes	door locked	admin-reader Status is Invalid	Set admin-door Lock to Lock
Add					

Conclusion

In conclusion, the new network configuration for Oceanview has been discussed on its security measures and alternatives that could be implemented into the network as it improves to combat the ever growing cyber and physical threats that threatens its operation. As a result, the network configuration will be able to run to perform requirements however it could always become better.

Reference List

- Banham, R., 2017. Cybersecurity threats proliferating for midsize and smaller businesses. Journal of Accountancy, 224(1), p.75.
- Google.com, About static IPs for small business (2023), Available at: <https://support.google.com/fiber/answer/6078071?hl=en> (Accessed: December 12, 2023)
- Sandhu, R. and Samarati, P. (1994) 'Access control: principle and practice,' IEEE Communications Magazine, 32(9), pp. 40-48. <https://doi.org/10.1109/35.312842>
- M. R. Rieback, B. Crispo and A. S. Tanenbaum, "The evolution of RFID security," in IEEE Pervasive Computing, vol. 5, no. 1, pp. 62-69, Jan.-March 2006, doi: 10.1109/MPRV.2006.17.
- Radivilova. T and H. A. Hassan, "Test for penetration in Wi-Fi network: Attacks on WPA2-PSK and WPA2-enterprise," 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odessa, Ukraine, 2017, pp. 1-4, doi: 10.1109/UkrMiCo.2017.8095429.