NETWORK CONFIGURATION

Design and implement a network solution

Sergiusz Pieszak

Contents

1. Introduction

In the ever-evolving landscape of cybersecurity, the task of crafting a resilient network is critical. The task at hand involved constructing and constructing a secure [redacted] Infrastructure network, based on the IP address scheme 172.16.0.0/24. Tailoring solutions to the unique needs of the Information Assurance (IA) and Human Resources (HR) departments required a precise and strategic approach.

The IA department, comprising ten staff members, required both fixed and remote access, demanding a secure internet connection. Furthermore, a shared printer within the department required precise configuration. In parallel, the HR department, with five desktop users and a file server providing sensitive Personal Identifiable Information (PII), introduced an additional layer of complexity, requiring strict access restrictions.

Intermediary equipment, like switches, routers, and access points, were important in enabling seamless departmental connections. Configuration, which included subnets, IP addressing, and basic configurations such as time, passwords, and banners, constituted the foundation of a robust network.

2. Passwords

For the ease of the network's initial configuration, a temporary password called "pass" has been created. It is important to recognise that this password is temporary, the importance of quickly changing it with a strong, unique passphrase to abide by security regulations and strengthen network resilience. Cisco (no date) recommends that the “minimum password length is 8 characters”.

3. Subnetting Scheme

To accommodate the company's two departments and an additional point of internet access, subnetting the network with a /26 is optimal. This configuration provides four distinct subnets within the 255.255.255.192 subnet range, enabling the capacity for 62 connected hosts per subnet. The 172.16.0.192 – 225 ip range has intentionally been left, serving as a scalable reserve. If the company expands or decides to incorporate an additional department, they have a surplus of 63 available IP addresses available for allocation.

4. Connections

All connections utilize copper straight-through cables. As a general guideline, straight-through cables are utilized for dissimilar devices, while crossover cables are employed for similar devices. Therefore, the choice of copper straight-through cables is based upon this principle. Bridgehead IT (2020)

5. Internet facing subnet

The 172.16.0.0 – 63 subnet is the subnet that is responsible for connecting the office to the internet. Connected via the Ethernet 0/0 port with default gateway of 172.16.0.1. It includes the firewall and leaves plenty of space for any future additions to the network, such as honey pots and additional security devices.

6. External firewall

As the network hasn't been connected to the internet the firewall couldn't be configured.

To prevent DDoS attacks and respond swiftly to threats, the router has the capability to blacklist IPs. However, the risk of overload exists. The external firewall's purpose is to shield the router from potential overloads, such as DoS attacks, caused by attackers.

As stated by Varma, K. (2021) an interesting configuration is blocking all traffic by default and explicitly allowing only known services, this severely reduces the risk of breaches due to service misconfiguration. This is achieved by configuring the last rule in an access control list to deny all traffic, either explicitly or implicitly, depending on the platform.

7. Configuring the router

Using a /26 subnetting scheme requires the implementation of a router to facilitate communication between different departments. The choice of the 2911 router was based on its support for 3 gigabit Ethernet ports, as depicted in Figure 1. The router configuration was implemented through the Command Line Interface (CLI).

The router was initially enabled using the ‘en’ command. Default gateways were established in configure terminal mode by selecting the desired gigabit ethernet port using the 'int' command and assigning the IP address with the 'ip address [IP ADDRESS] [SUBNET MASK]' command.

Setting the clock in HH:MM:SS DATE format was the next step. Transitioning into configure terminal mode once again. Various configurations were then performed:

- The hostname was changed to 'mainRouter' to enable router identification within the network.
- Password protection was enabled to prevent unauthorized access to the router's configuration.
- A banner, encapsulated between dollar signs ($), was implemented to provide information when another technician conducts maintenance on the router.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#ip address 172.16.0.1 255.255.255.192
Router(config-if)#exit
Router(config)#int g0/1
Router(config-if)#ip address 172.16.0.129 255.255.255.192
Router(config-if)#exit
Router(config)#int g0/2
Router(config-if)#ip address 172.16.0.65 255.255.255.192
Router(config-if)#exit
Router(config)#clock set 12:51:00 7 December 2023
                  ^
% Invalid input detected at '^' marker.

Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#clock set 12:51:30 7 December 2023
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname MainRouter
MainRouter(config)#enable password pass
MainRouter(config)#banner MOTD $
Enter TEXT message.  End with the character '$'.
Hello! This is the main router. Subnetted into 4 networks consisting of 64 hosts. Subnet is
255.255.255.192$

MainRouter(config)#
```

Figure 1 – Router configuration in the CLI

8. HR Department

The ip range of 172.16.0.64 – 127 has been allocated for the HR Department, connected through the Ethernet 0/2 port with a default gateway of 172.16.0.65. A decision was made to introduce 5 PCs with an IP range spanning from 172.16.0.67 to 172.16.0.71. These desktops are linked via wired connections, utilizing copper straight cables, to a Cisco 2960-24TT switch (for a detailed configuration of this switch see the 'Configuring switches' heading on page 9)

The file server, with an ip address of 172.16.0.66, utilizes File Transfer Protocol (FTP), allowing secure file storage with distinct permissions for various users, ensuring a secure and controlled data environment. For instance, the 'Admin' account has full permissions, including Read, Write, Delete, Rename, and List functionality. On the contrary, the 'staffTest' account serves as an illustrative example for a staff PC, equipped with restricted permissions limited to Read, Write, and List actions. Both accounts are password protected.

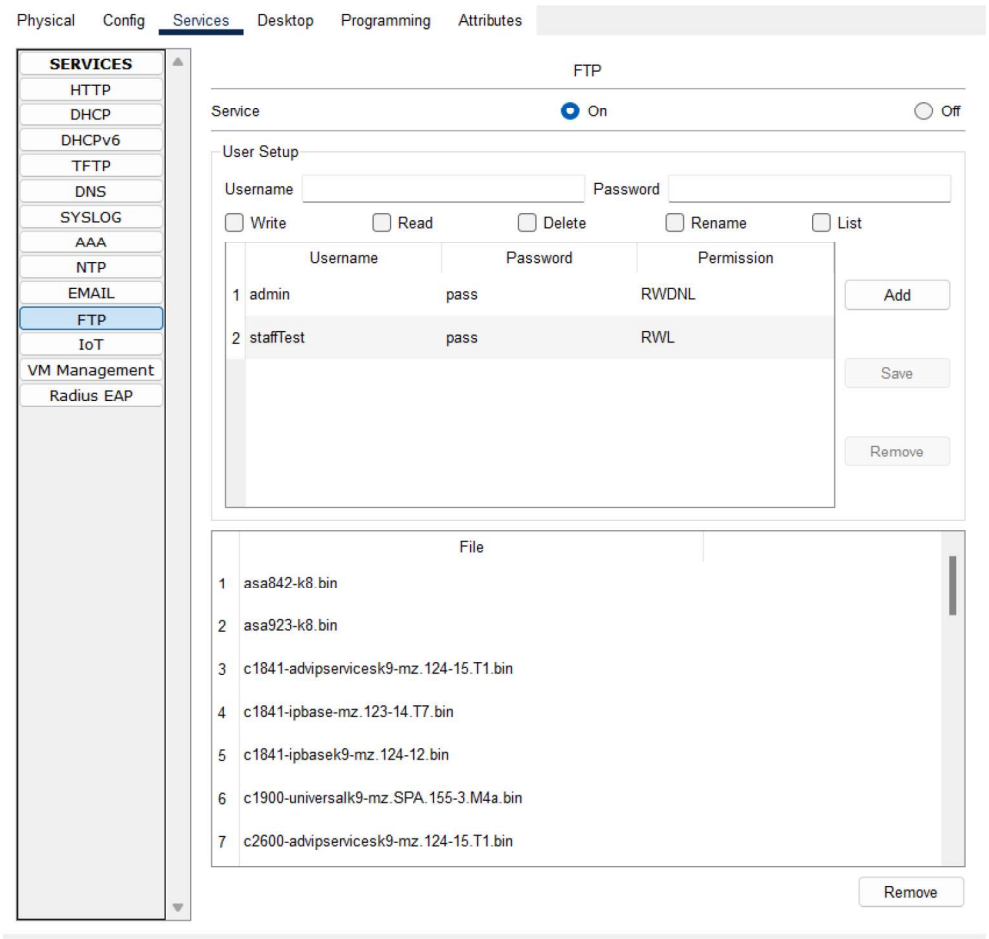

Figure 2 – Configuring the HR server with secure File Transfer Protocol

The printer was allocated its unique IP address, specifically set to 172.16.0.72, and assigned the departments default gateway, which is 172.16.0.65.

9. Access Control List

The HR Department must be configured to permit only outgoing traffic, restricting any inbound traffic. This configuration can be applied in two different ways, either through an internal firewall or through the routers Access Control List (ACL). To save on money and reduce the number of points of failure. The router option was chosen.

To implement this, it is necessary to block the default gateways of Gig0/0 and Gig0/1. The default gateway for Gig 0/0 is 172.16.0.1, and for Gig 0/1, it is 172.16.0.129. (Ed Goad, 2019)

Firstly, it is important to generate an access list, named as 'access-list 1.' Following this, the access list requires specific rules, namely 'access-list 1 deny 172.16.0.1' and 'access-list 1 deny 172.16.0.129.' These rules ensure the denial of incoming traffic originating from either of the router's other default gateways, in this case Gig 0/0 and Gig 0/1. To complete the configuration, the command 'access-list 1 permit any' is used, allowing for the unrestricted permission of any other incoming traffic.

```
MainRouter>en
Password:
MainRouter#conf t
Enter configuration commands, one per line.  End wit
MainRouter(config)#access-list?
access-list
MainRouter(config)#access-list 1?
<1-99>
MainRouter(config)#access-list 1 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
  remark  Access list entry comment
MainRouter(config)#access-list 1 deny 172.16.0.1 0.0
MainRouter(config)#access-list 1 deny 172.16.0.129 0
MainRouter(config)#access-list permit any
                             ^
% Invalid input detected at '^' marker.

MainRouter(config)#access-list 1 permit any
MainRouter(config)#exit
MainRouter#
%SYS-5-CONFIG_I: Configured from console by console

MainRouter#exit
```

Figure 3 – Creating the access-control list for the router.

The next crucial step is to connect this list with the default gateway of the HR Department, specifically Gig 0/2 in this instance. This procedure involves selecting the Gig 0/2 gateway with the command 'int gig0/2' and then applying the ACL to the outbound direction. This ensures that any data that is trying to enter ‘outbound’ from the router is blocked. The command 'ip access-group 1 out' is used to execute this action.

```
Hello! This is the main router. Subnetted into 4 networks con
255.255.255.192

MainRouter>en
Password:
MainRouter#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MainRouter(config)#int gig0/2
MainRouter(config-if)#ip access-group 1 ?
  in   inbound packets
  out  outbound packets
MainRouter(config-if)#ip access-group 1 out
MainRouter(config-if)#exit
MainRouter(config)#
```

Figure 4 – Applying the access-group to the specified gateway.

It is shown in figure 5 that there is a ping being sent from the IA department to the HR department. As the access-group command is entered into the router the connection between the two departments is severed, and a ‘Destination host unreachable’ message is displayed.

```
Reply from 172.16.0.67: bytes=32 time<1ms TTL=127
Reply from 172.16.0.67: bytes=32 time<1ms TTL=127
Reply from 172.16.0.67: bytes=32 time<1ms TTL=127
Reply from 172.16.0.67: bytes=32 time=18ms TTL=127
Reply from 172.16.0.67: bytes=32 time<1ms TTL=127
Reply from 172.16.0.67: bytes=32 time<1ms TTL=127
Reply from 172.16.0.67: bytes=32 time<1ms TTL=127
Reply from 172.16.0.67: bytes=32 time<1ms TTL=127
Reply from 172.16.0.67: bytes=32 time<1ms TTL=127
Reply from 172.16.0.67: bytes=32 time<1ms TTL=127
Reply from 172.16.0.67: bytes=32 time<1ms TTL=127
Reply from 172.16.0.129: Destination host unreachable.
Reply from 172.16.0.129: Destination host unreachable.
Reply from 172.16.0.129: Destination host unreachable.
Reply from 172.16.0.129: Destination host unreachable.
Reply from 172.16.0.129: Destination host unreachable.
Reply from 172.16.0.129: Destination host unreachable.
Reply from 172.16.0.129: Destination host unreachable.
```

Figure 5 – Confirmation of the ACL working as the ping is interrupted.

10. IA Department

The ip range of 172.16.0.128 – 191 is designated for the IA Department, linked through the Ethernet 0/1 port with a default gateway of 172.16.0.129. A choice was made to incorporate 10 PCs with the assigned IP addresses ranging from 172.16.0.130 to 172.16.0.139. These computers are connected via wired connections, utilizing copper straight cables to a Cisco 2960-24TT switch.

Acknowledging that two staff members work remotely but occasionally attend on-site meetings, providing internet access was necessary, it was decided to enable connectivity for these remote workers via AccessPoint-PT. WPA2-Personal was chosen as the encryption method due to its recognized security effectiveness. As the company is still small the personal version of this encryption method is sufficient Ghimiray, D. (2022).

Printer was assigned its own ip address of 172.16.0.140 and provided with a default gateway of 172.16.0.129.

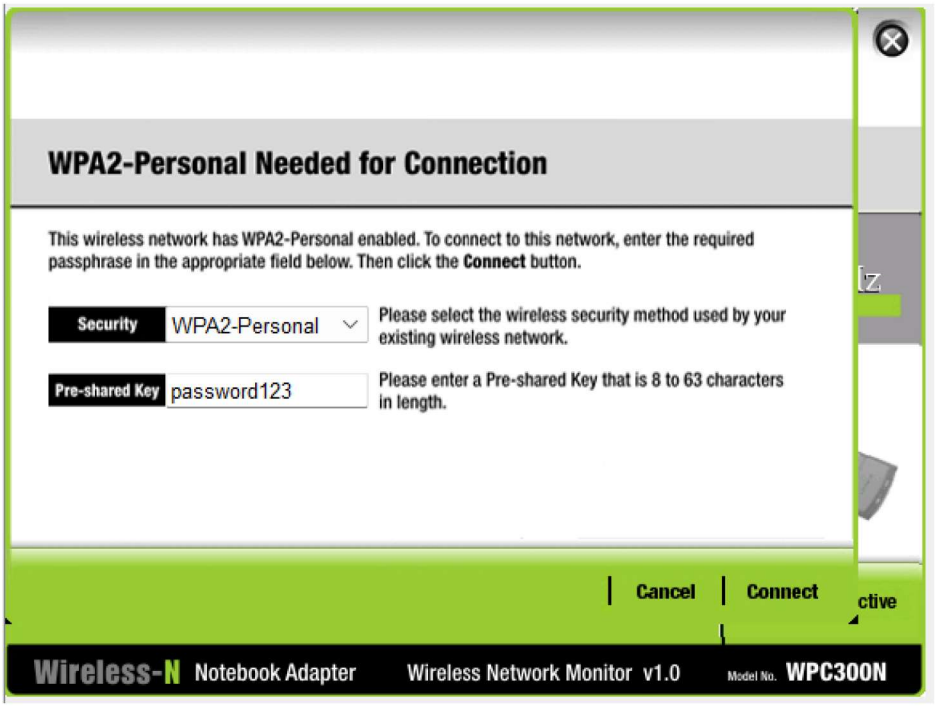

Figure 6 – Connectivity using WPA2-Personal for the 2 wireless devices.

11. Configuring switches

Configuring the switch for the IA and HR department is identical. Firstly, the router was enabled using the ‘en’ command. Setting the clock in HH:MM:SS DATE format was the next step. Transitioning into configure terminal mode. Where the hostname was changed. Then the password was enabled using ‘enable password’. Just like the router, a banner, encapsulated between dollar signs ($), was implemented to provide information when another technician conducts maintenance on the switch.

```
Switch>
Switch>en
Switch#clock set 12:59:00 5 December 2023
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname switch2
switch2(config)#enable password pass
switch2(config)#banner MOTD $
Enter TEXT message.  End with the character '$'.
Hello, this is the switch responsible for the HR Department
$

switch2(config)#
```

Figure 7 – Configuration of a switch.

12. Conclusion

In conclusion, the network setup was highly successful. The Access Control List (ACL) efficiently secured the HR department by blocking unauthorized incoming traffic. The access point was accurately configured, enabling secure wireless access for the two remote employees through the WPA2 encryption standard. All other devices were also successfully configured and connected to the network.

13. References

Bridgehead IT (2020) *Straight-Through vs. Crossover Cables: What's the Difference?* Available at: https://www.bridgeheadit.com/straight-through-vs-crossover-cables-whats-the-difference/ (Accessed: 1 December 2023).

Cisco (no date). *Password Strength and Management for Common Criteria*. Available at:https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960l/software/15-2_7_e/configuration_guide/sec/b_1527e_security_2960l_cg/password_strength_and_management_for_common_criteria.pdf (Accessed: 3 December 2023).

Ed Goad (2019) *Access List Activity 1*. Available at: https://www.youtube.com/watch?v=WXcSObjC41E (Accessed: 8 December 2023).

Ghimiray, D. (2022) *What Is WPA2 (Wireless Protected Access 2)?*. Available at: https://www.avg.com/en/signal/what-is-wpa2 (Accessed: 1 December 2023).

Varma, K. (2021) *Best practices for Internal and External firewall rules configuration*. Available at: https://www.linkedin.com/pulse/best-practices-internal-external-firewall-rules-kiran-varma/ (Accessed: 19 November 2023).