A trading floor Support centre employs 600 staff. They have recently expanded and as a result, need to move to a new building. A building has been identified but has no network. This means that before they can make to move out, new network service needs to be designed and implemented in the new building. Existing Network comprises of the following elements: The new building is expected to have three floors with two departments in each for example;

1. **First floor-** (Sales and Marketing Department-120 users expected, Human Resource and Logistics Department-120 users expected).
2. **Second floor-** (Finance and Accounts Department-120 users expected, Administrator and Public Relations Department-120 users expected).
3. **Third floor-** (ICT-120 users expected, Server Room-12 devices expected).

Therefore, as a key member of the Networks Team, you have been tasked to design a network for the new building. At this stage, logical design is required, which shows the measures that you would put in place to ensure that the new network meets the current business need and is future-proofed:

* Use Cisco Packet Tracer to design and implement the network solution.
* Use hieratical model providing redundancy at every layer i.e. two routers and two multilayer switches are expected to be used to provide redundancy.
* The network is also expected to connect to at least two ISPs to provide redundancy and each router to the connected to the two ISPs.
* Each department is required to have a wireless network for the users.
* Each department should be in a different VLAN and in different subnetwork.
* Provided a base network of 172.16.1.0, carry out subnetting to allocate the correct number of IP addresses to each department.
* The company network is connected to the static, public IP addresses (Internet Protocol) 195.136.17.0/30, 195.136.17.4/30, 195.136.17.8/30 and 195.136.17.12/30 connected to the two Internet providers.
* Configure basic device settings such as hostnames, console password, enable password, banner messages, disable IP domain lookup.
* Devices in all the departments are required to communicate with each other with the respective multilayer switch configured for inter-VLAN routing.
* The Multilayer switches are expected to carry out both routing and switching functionalities thus will be assigned IP addresses.
* All devices in the network are expected to obtain an IP address dynamically from the dedicated DHCP servers located at the server room.
* Devices in the server room are to be allocated IP address statically.
* Use OSPF as the routing protocol to advertise routes both on the routers and multilayer switches.
* Configure SSH in all the routers and layer three switches for remote login.
* Configure port-security for the Finance and Accounts department to allow only one device to connect to a switchport, use sticky method to obtain mac-address and violation mode shutdown.
* Configure PAT to use the respective outbound router interface IPv4 address, implement the necessary ACL rule.
* Test Communication, ensure everything configured is working as expected.

**Technologies Implemented**

1. Creating a network topology using Cisco Packet Tracer.
2. Hierarchical Network Design.
3. Connecting Networking devices with Correct cabling.
4. Configuring Basic device settings.
5. Creating VLANs and assigning ports VLAN numbers.
6. Subnetting and IP Addressing.
7. Configuring Inter-VLAN Routing on the Multilayer switches (Switch Virtual Interface).
8. Configuring Dedicated DHCP Server device to provide dynamic IP allocation.
9. Configuring SSH for secure Remote access.
10. Configuring OSPF as the routing protocol.
11. Configuring NAT Overload(Port Address Translation PAT).
12. Configuring standard and extended Access Control Lists ACL.
13. Configuring switchport security or Port-Security on the switches.
14. Configuring WLAN or wireless network (Cisco Access Point).
15. Host Device Configurations.
16. Configuring ISP routers.
17. Test and Verifying Network Communication.

Centrum wsparcia na parkiecie handlowym zatrudnia 600 pracowników. Niedawno się rozrosło i w wyniku tego musi przenieść się do nowego budynku. Został zidentyfikowany budynek, ale nie ma w nim sieci. Oznacza to, że zanim będzie można się przenieść, konieczne jest zaprojektowanie i wdrożenie nowej sieci w nowym budynku. Istniejąca sieć składa się z następujących elementów:

Oczekuje się, że nowy budynek będzie miał trzy piętra, na każdym z dwoma działami, na przykład:

* **Pierwsze piętro** – Dział Sprzedaży i Marketingu (120 użytkowników), Dział Zasobów Ludzkich i Logistyki (120 użytkowników).
* **Drugie piętro** – Dział Finansów i Rachunkowości (120 użytkowników), Dział Administracji i Public Relations (120 użytkowników).
* **Trzecie piętro** – Dział IT (120 użytkowników), Serwerownia (12 urządzeń).

Jako kluczowy członek zespołu sieciowego zostałeś/aś poproszony/a o zaprojektowanie sieci dla nowego budynku. Na tym etapie wymagany jest projekt logiczny, który pokaże środki, jakie wdrożysz, aby zapewnić, że nowa sieć spełni bieżące potrzeby biznesowe i będzie przyszłościowa.

**Wymagania:**

1. Użyj **Cisco Packet Tracer** do zaprojektowania i wdrożenia rozwiązania sieciowego.
2. Zastosuj **hierarchiczny model**, zapewniając redundancję na każdym poziomie, tj. oczekuje się użycia dwóch routerów i dwóch przełączników warstwy 3 (multilayer switches) w celu zapewnienia redundancji.
3. Sieć musi łączyć się z co najmniej dwoma dostawcami usług internetowych (ISP) dla redundancji, a każdy router ma być podłączony do dwóch ISP.
4. Każdy dział musi mieć **sieć bezprzewodową** dla użytkowników.
5. Każdy dział powinien być w innej **VLAN** i w innym podsieci.
6. Użyj sieci bazowej **172.16.1.0** i przeprowadź podział na podsieci, aby przydzielić odpowiednią liczbę adresów IP dla każdego działu.
7. Sieć firmy jest połączona z publicznymi adresami IP (Internet Protocol) **195.136.17.0/30**, **195.136.17.4/30**, **195.136.17.8/30** i **195.136.17.12/30**, podłączonymi do dwóch dostawców usług internetowych.
8. Skonfiguruj podstawowe ustawienia urządzeń, takie jak nazwy hostów, hasła do konsoli, hasło enable, wiadomości banerowe, wyłącz IP domain lookup.
9. Urządzenia w wszystkich działach mają komunikować się ze sobą, a odpowiednie przełączniki warstwy 3 mają być skonfigurowane do routingu między VLAN-ami.
10. Przełączniki warstwy 3 będą realizować zarówno funkcje routingu, jak i przełączania, więc zostaną im przypisane adresy IP.
11. Wszystkie urządzenia w sieci mają otrzymywać dynamicznie adres IP z dedykowanych serwerów DHCP zlokalizowanych w serwerowni.
12. Urządzeniom w serwerowni mają być przydzielane adresy IP statycznie.
13. Użyj **OSPF** jako protokołu routingu do ogłaszania tras zarówno na routerach, jak i przełącznikach warstwy 3.
14. Skonfiguruj **SSH** na wszystkich routerach i przełącznikach warstwy 3 do zdalnego logowania.
15. Skonfiguruj **port-security** dla działu finansów i rachunkowości, aby pozwolić na podłączenie tylko jednego urządzenia do portu przełącznika, używając metody sticky do uzyskania adresu MAC i trybu naruszenia shutdown.
16. Skonfiguruj **PAT** (Przeciążenie NAT) z użyciem odpowiedniego adresu IPv4 interfejsu wyjściowego routera, zaimplementuj odpowiednią regułę ACL.
17. Przetestuj komunikację, upewnij się, że wszystko zostało skonfigurowane i działa zgodnie z oczekiwaniami.

**Zaimplementowane technologie:**

* Tworzenie topologii sieci przy użyciu Cisco Packet Tracer.
* Hierarchiczny projekt sieci.
* Łączenie urządzeń sieciowych odpowiednim okablowaniem.
* Konfiguracja podstawowych ustawień urządzeń.
* Tworzenie VLAN-ów i przypisywanie portów do VLAN-ów.
* Podział na podsieci i adresowanie IP.
* Konfiguracja routingu między VLAN-ami na przełącznikach warstwy 3 (Switch Virtual Interface).
* Konfiguracja dedykowanego serwera DHCP do dynamicznego przydzielania adresów IP.
* Konfiguracja SSH dla bezpiecznego zdalnego dostępu.
* Konfiguracja OSPF jako protokołu routingu.
* Konfiguracja NAT Overload (Port Address Translation - PAT).
* Konfiguracja standardowych i rozszerzonych list kontroli dostępu (ACL).
* Konfiguracja port-security na przełącznikach.
* Konfiguracja sieci WLAN (Cisco Access Point).
* Konfiguracja urządzeń hostów.
* Konfiguracja routerów ISP.
* Testowanie i weryfikacja komunikacji sieciowej.

### 1. ****Creating a network topology using Cisco Packet Tracer****

* **Otwórz Cisco Packet Tracer** i zacznij od dodania urządzeń do sieci. W zależności od wymagań, dodaj:
  + Routery (np. Cisco 2911)
  + Przełączniki warstwy drugiej (np. 2960) oraz warstwy trzeciej (np. 3560 lub 3650).
  + Komputery PC, laptopy, drukarki, tablety, serwery.
  + Access Point do sieci WLAN.
  + Kabel prosty lub skrosowany do połączenia urządzeń (prostego używaj do PC/switch, krosowanego do połączeń switch-switch lub router-switch).

### 2. ****Hierarchical Network Design****

Hierarchiczny design składa się z trzech warstw:

* **Warstwa rdzeniowa (core)**: np. Routery CORE-R1, CORE-R2, które łączą całą sieć z ISP.
* **Warstwa dystrybucyjna (distribution)**: Przełączniki wielowarstwowe (np. 3560 lub 3650), które zapewniają routing między VLAN-ami i obsługują połączenia pomiędzy sieciami VLAN.
* **Warstwa dostępowa (access)**: Switch’e dostępowe (np. 2960), do których podłączone są urządzenia końcowe jak PC, laptopy.

### 3. ****Connecting Networking devices with Correct cabling****

* Używaj:
  + **Kabel prosty**: do połączeń PC -> Switch, Switch -> Router.
  + **Kabel krosowany**: do połączeń Switch -> Switch, Router -> Router.
  + **Kabel konsolowy**: do początkowej konfiguracji urządzeń.

### 4. ****Configuring Basic Device Settings****

Na każdym urządzeniu (router, switch):

bash

Skopiuj kod

enable

configure terminal

hostname <NAME>

no ip domain-lookup

enable secret cisco

line console 0

password cisco

login

exit

line vty 0 4

password cisco

login

exit

### 5. ****Creating VLANs and assigning ports VLAN numbers****

Na przełącznikach warstwy drugiej (2960):

bash

Skopiuj kod

enable

configure terminal

vlan 10

name SALES

vlan 20

name HR

interface range fa0/1 - 12

switchport mode access

switchport access vlan 10

interface range fa0/13 - 24

switchport mode access

switchport access vlan 20

exit

### 6. ****Subnetting and IP Addressing****

Załóżmy, że masz adresację sieci: 172.16.0.0/16. Podzielmy na podsieci VLAN-ów:

* VLAN 10 (Sales): 172.16.1.0/24
* VLAN 20 (HR): 172.16.2.0/24

Przydziel adresy IP dla VLAN-ów:

bash

Skopiuj kod

interface vlan 10

ip address 172.16.1.1 255.255.255.0

no shutdown

interface vlan 20

ip address 172.16.2.1 255.255.255.0

no shutdown

### 7. ****Configuring Inter-VLAN Routing (SVI)****

Na przełączniku warstwy trzeciej (3650):

bash

Skopiuj kod

interface vlan 10

ip address 172.16.1.1 255.255.255.0

no shutdown

interface vlan 20

ip address 172.16.2.1 255.255.255.0

no shutdown

ip routing

### 8. ****Configuring Dedicated DHCP Server device****

Na serwerze DHCP:

* Ustaw zakres dla każdego VLAN-u:
  + Sales: 172.16.1.10 - 172.16.1.254
  + HR: 172.16.2.10 - 172.16.2.254

W Cisco Packet Tracer:

* Kliknij serwer -> Services -> DHCP.
* Dodaj zakresy dla poszczególnych VLAN-ów.

### 9. ****Configuring SSH for secure remote access****

Na switchu warstwy trzeciej:

bash

Skopiuj kod

ip domain-name yourdomain.com

crypto key generate rsa

1024

username admin secret cisco

line vty 0 4

transport input ssh

login local

exit

### 10. ****Configuring OSPF as the routing protocol****

Na routerach:

bash

Skopiuj kod

router ospf 1

network 172.16.0.0 0.0.255.255 area 0

network 195.136.17.0 0.0.0.3 area 0

### 11. ****Configuring NAT Overload (PAT)****

Na routerze podłączonym do Internetu:

bash

Skopiuj kod

interface gig0/1

ip address 195.136.17.2 255.255.255.252

ip nat outside

interface gig0/0

ip address 172.16.0.1 255.255.255.0

ip nat inside

exit

access-list 1 permit 172.16.0.0 0.0.255.255

ip nat inside source list 1 interface gig0/1 overload

### 12. ****Configuring standard and extended Access Control Lists ACL****

Standard ACL (blokowanie IP):

bash

Skopiuj kod

access-list 10 deny host 172.16.1.50

access-list 10 permit 172.16.0.0 0.0.255.255

interface gig0/0

ip access-group 10 in

Extended ACL (blokowanie HTTP):

bash

Skopiuj kod

access-list 100 deny tcp any any eq 80

access-list 100 permit ip any any

interface gig0/0

ip access-group 100 in

### 13. ****Configuring switchport security (Port-Security)****

Na switchu:

bash

Skopiuj kod

interface fa0/1

switchport mode access

switchport port-security

switchport port-security maximum 2

switchport port-security violation restrict

switchport port-security mac-address sticky

### 14. ****Configuring WLAN or wireless network (Cisco Access Point)****

Na Access Point:

* Ustaw SSID, szyfrowanie WPA2:

bash

Skopiuj kod

interface dot11radio 0

ssid Company\_WiFi

authentication open

authentication key-management wpa version 2

wpa-psk ascii cisco123

exit

### 15. ****Host Device Configurations****

* Ustaw na komputerach dynamiczne pobieranie adresów IP (DHCP) lub statyczne przydzielanie IP, DNS.

### 16. ****Configuring ISP routers****

Na routerach ISP (ISP1, ISP2):

bash

Skopiuj kod

interface gig0/0

ip address 195.136.17.1 255.255.255.252

exit

router ospf 1

network 195.136.17.0 0.0.0.3 area 0

### 17. ****Test and Verifying Network Communication****

* Sprawdź **ping** między urządzeniami.
* Użyj komendy **traceroute** i **show ip route** na routerach, aby sprawdzić trasy.
* W Packet Tracerze przetestuj połączenia, wysyłając PDU (ping) między urządzeniami końcowymi.