A logo of a globe and a graduation cap

Description automatically generated

Digital Egyptian Pioneers Initiative

Graduation Project

2 Branch-Company Network

A diagram of a computer network

Description automatically generated

As Shown It’s a Simulation of Small company Has 2 Branches Main And 2nd Branch

The Main Idea Of Project To Implement Multiple Topics Of Network But Not A Simulation of Real Company (That’s Why Scheme Is Simple)

Let’s Begin ..

At The First Topics Covered In The Project :-

1-EtherChannel : To Enhance Speed Of Data Transfer To Be More Effective , And To Make a Cable Backup (in case of One Of Them Go Down) , Protocol Used (PagP)

2-VLAN : To Segment The Switch to Multiple Sectors , We Implemented Trunk to Make Same Sectors at Different Switches Connected

3-InterVLAN Routing : For The Router On The Left (at Main Branch) , We Made 5 Sub Interfaces And We Implement Multiple Functions On Them , One of Them InterVLAN Routing to Make Different Sectors Connected Together

4-DHCP : To Make Any Device Obtain IP Address Automatically , 3 DHCP Pools are Implemented , One For Each Sector (VLAN 10 , 20 , 30) , So You Can Expand Number Of Devices Easily

5-OSPF : To Make 2 Branches Connected Over WAN By OSPF . So OSPF Implemented On All Routers On The Scheme .

Routers In The Middle I Can Divide Them to 3 Groups Based In Their Functions

201.100.100.1 , 202.100.100.1 🡪 Routers In The Main Branch Which Are Considered As a Backup Of Each Other In Case Of One of them Go Down

207.100.100.1 , 207.100.100.2 🡪 Like The Previous Group But For The 2nd Branch

204.100.100.1 , 205.100.100.1 🡪 As Virtual ISP To Make The Idea Of Project Clear

6- HSRP : That’s The Protocol Used For First And Second Groups In The Previous Passage

7- Static NAT : For IT Administrator In The Main Branch To Be Able To Modify And Implement Changes On Devices In The 2nd Branch By Public IP

For IT Administrator , There Is One IT Admin at Each Branch , Their Roles Are not The Same as The One In The Main Branch Has All Permissions to Perform Any Change On Any Device In Both Branches , But 2nd Branch One Can Perform Change On Any Device But Not The Router In The Main Branch

8- ACL : List Contain Devices Who Are Permitted To Enter The Network And Who Are Not , All The Devices Has ACL But The Router In The Main Branch Has 2 ACLs , First One For Devics Who Permitted To Get Into The Network , 2nd one For Devices Who Are Permitted for Modifying The Settings Of The Router Remotely

9- SSH : To Make All Remote Connections Encrypted To Prevent Hacker From Accessing The Command I Typed To Modify The Device Remotely

Explanation Of The Mechanism Of The Network Through Different Cases To Show The Role Of Each Topic : -

Case 1 : A Device From VLAN 10 (192.168.1.4) Want to Connect Another One From VLAN 10 (192.168.1.2)

* Packets Would Go Directly To The Destination Through Trunk Settings As They Are Considered As One Network Because of VLANs

Case 2 : A Device From VLAN 10 (192.168.1.4) Want to Connect Another One From VLAN 20 (192.168.1.2)

* First The Device Would Forward The Packets To Router Through Trunk To Reach The Router , Then Router By InterVLAN Routing Will Forward The Packets to The Right Destination

Case 3 : A Device From VLAN 10 (192.168.1.4) Want to Connect Another One The 2nd Branch

* The Device Would Forward The Packets To Switch Then To The Main Router ,By InterVLAN Routing It Would Forward The Packets To One Of (201.100.100.1 , 202.100.100.1 ) As (The Main Router , 201.100.100.1 , 202.100.100.1 ) Are In The Same VLAN Which Mean That They Are Connected By (VLAN 1) . So The MAIN Router Would Forward Packets From VLAN 10 to VLAN 1 (InterVLAN Routing) , Packets Would Go To Designated Router Through Trunk , It Would Go To The Another Branch Through OSPF

Case 4 : A Device From External Network (Doesn’t Belong To Our Company) Want to Connect Any Device In Main Branch

* The Packets Would Be Forwarded To Main Router Which Has ACL , It Will Detect It If It’s Not Belong To Our Company , Router Will Discard These Packets

Case 5 : IT Admin Of Main Branch Want to Modify a Device In The Same Branch (192.168.1.3) For Example

* IT’s Device Would Forward Packets to The Device As All The Management VLANs Has The Same Network Of The IT Network , So They Are Connected Together By (VLAN 100)

Case 6 : IT Admin Of Main Branch Want to Modify a Device In The 2nd Branch (207.100.100.20)

* IT’s Device Would Forward Packets From (VLAN 100) to The Routers VLAN (VLAN 1) Then By OSPF Connection Would Be Established But First 207.100.100.20 Would Detect Whether The Coming Request is Permitted to Modify The Device Or Not By ACL Which Is Applied On VTY Lines

Case 7 : IT Admin Of 2nd Branch Want to Modify a Device In The Main Branch (192.168.1.3)

* Request Would Be Forwarded Through OSPF Till It Reach The Main Router , Main Router Would Detect Whether The Device Is Permitted To Pass Or Not By ACL , Then Forward It From (VLAN 1) To (VLAN 100) By InterVLAN Routing , Then Go to 192.168.1.3 Which Will Detect If The Device Is Permitted To Modify The Settings Or Not

Case 8 : IT Admin Of 2nd Branch Want to Modify The Main Router

* Request Would Be Forwarded Through OSPF Till It Reach The Main Router , Main Router Would Detect Whether The Device Is Permitted To Modify Or Not By ACL , But This Router Couldn’t Be Modified By Any Device Remotely Except The Main Branch IT