Enterprise High-Availability Network Design

Document de Proiectare Detaliată (LLD)

Realizat de: Fierea Cosmin-Andrei

1. Prezentare Generală a Proiectului

Obiectivul principal al proiectului este furnizarea unei infrastructuri reziliente, capabilă să asigure continuitatea afacerii prin eliminarea punctelor unice de eșec (**Single Points of Failure**). Designul se concentrează pe trei piloni centrali: redundanță (High Availability), scalabilitate pentru departamente viitoare și securitate cibernetică multi-strat.

2. Arhitectura Rețelei

Proiectul utilizează modelul ierarhic Cisco pentru a optimiza fluxurile de trafic și a facilita depanarea:

- Edge Layer: Un router Cisco 4321 (EDGE-ROUTER) care gestionează conectivitatea externă către ISP, politicile de securitate NAT și rutarea de frontieră.
- Core Layer: Două switch-uri Multilayer Cisco 3650 (CORE-1, CORE-2) care acționează ca motor de rutare inter-VLAN și gateway-uri redundante.
- Access Layer: Switch-uri de Layer 2 (ACCESS-1) care asigură conectivitatea terminalelor finale (PC, Laptop) segmentate pe departamente.
- Transit Segment: Un switch dedicat (TRANSIT-SW) facilitează legătura de tranzit între routerul Edge și ambele switch-uri din Core.

3. Detalii Tehnice Layer 2 (Switching)

3.1. Segmentare VLAN și Acces

Rețeaua este divizată logic pentru a izola traficul și a aplica politici de securitate specifice:

- VLAN 10 (IT): Subrețea 192.168.10.0/24.
- VLAN 20 (Sales): Subrețea 192.168.20.0/24.
- VLAN 30 (HR): Subrețea 192.168.30.0/24.

3.2. Redundanță și Agregare

- LACP EtherChannel: Switch-urile Core sunt interconectate prin Port-channel 1, agregând interfețele Gigabit 1/0/1 și 1/0/2 pentru a asigura o lățime de bandă de 2 Gbps și redundanță la nivel de link.
- Rapid-PVST+: Protocolul Spanning Tree este optimizat prin configurarea priorităților pe switch-urile Core pentru a menține controlul topologiei.

4. Detalii Tehnice Layer 3 (Routing & HA)

4.1. Înaltă Disponibilitate (HSRP)

Implementarea Hot Standby Router Protocol asigură un gateway virtual (VIP) pentru terminalele din fiecare VLAN:

- VIP: .1 pentru fiecare subrețea (ex: 192.168.10.1).
- CORE-1 (Active): Prioritate 110 cu funcția *preempt* activată pentru a relua rolul de master în caz de recuperare.
- CORE-2 (Standby): Prioritate implicită 100.

4.2. Rutare Dinamică (OSPFv2)

- OSPF este utilizat pentru propagarea automată a rutelor în interiorul rețelei:
- Area 0: Toate interfețele de tranzit și VLAN-urile sunt incluse în Backbone Area.
- Default Route: EDGE-ROUTER injectează ruta implicită prin comanda *default-information originate* către switch-urile Core.

5. Securitate și Servicii Rețea

5.1. Politici de Securitate

- Port-Security: Pe ACCESS-1, porturile sunt limitate la o singură adresă MAC folosind tehnologia sticky. Încălcarea politicii duce la blocarea portului (shutdown).
- Access Control Lists (ACL): ACL-ul extins SECURE_IT aplicat pe CORE-1 blochează traficul ICMP/IP de la departamentul HR (VLAN 30) către IT (VLAN 10).

5.2. Servicii (NAT & DHCP)

- NAT Overload (PAT): Translatarea adreselor din 192.168.0.0/16 către adresa externă 82.10.10.1 pe interfața G0/0/1 a routerului Edge.
- DHCP Server: Switch-urile Core distribuie adrese IP automat, exceptând intervalul .1 - .3 rezervat pentru VIP și IP-urile fizice ale switch-urilor.

5.3. Management Securizat

- SSH v2: Toate echipamentele permit administrarea de la distanță doar prin conexiuni criptate (port 22), serviciul Telnet fiind dezactivat.

6. Matricea de Verificare și Validare (V&V)

ID Test	Scenariu	Rezultatul Așteptat	Rezultat Actual	Status
VV-01	Conectivitate Externă: Orice host trebuie să acceseze IP-ul extern.	Trace complete (3 hops)	Trace complete	PASSED
VV-02	Ping din HR către IT (Test Securitate ACL)	ICMP Blocat (Destination host unreachable)	Unreachable	PASSED
VV-03	Test Failover: Dezactivare CORE-1 în timpul ping-ului	Sesiune activă (Ping-ul continuă prin CORE-2)	Sesiune Activă	PASSED
VV-04	Cerere DHCP din departamentul IT	Primire IP în range-ul 192.168.10.x	IP Alocat	PASSED
VV-05	Conexiune MAC neautorizată (Sticky)	Portul trece în err-disabled / Shutdown	Port Shutdown	PASSED

6.1 Note de Validare Tehnică

- Validare Connectivity: Traseele tracert confirmă faptul că traficul este direcționat corect prin gateway-urile redundante (CORE-1 și CORE-2) și ajunge la destinația externă prin routerul EDGE.
- Validare Security: Rezultatul testului VV-04 confirmă că Access Control List-ul (ACL) SECURE_IT configurat pe interfața Vlan30 a CORE-1 interzice activ traficul către segmentul IT (192.168.10.0).
- Validare Failover: Deși CORE-1 este trecut în starea "DEZACTIVAT", stațiile continuă să primească răspunsuri de la IP-ul 82.10.10.1, demonstrând convergența rapidă a protocoalelor HSRP și OSPF.

7. Scalabilitate și Viitor

- Scalabilitate:
  - Designul permite adăugarea facilă de noi switch-uri de acces sau VLAN-uri fără a afecta nucleul.
- Recomandări:
  - Implementarea Dual-Homing WAN (al doilea ISP).
  - Activarea DHCP Snooping și DAI pentru securitate L2 avansată.
  - Tranziția către IPv6 Dual-Stack și monitorizarea proactivă via SNMP/Syslog.

8. Concluzii

Proiectul a demonstrat cu succes implementarea unei infrastructuri de rețea ierarhice (Edge-Core-Access), capabilă să susțină cerințele critice ale unui mediu enterprise modern: disponibilitate ridicată, securitate granulară și gestionare eficientă a traficului.

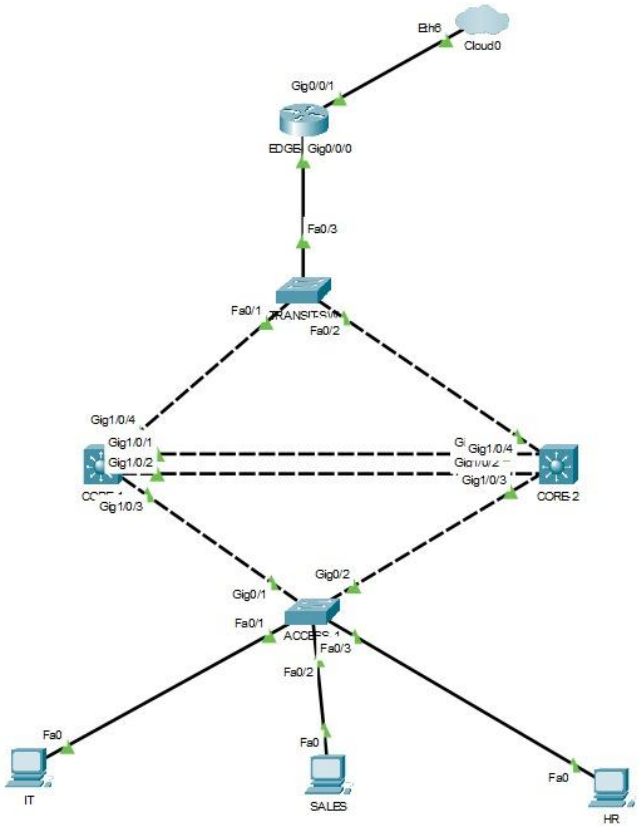
Prin utilizarea protocoalelor de redundanță la Layer 2 (LACP EtherChannel) și Layer 3 (HSRP), rețeaua elimină punctele unice de eșec. Testele de tip failover au confirmat că timpul de convergență este minim, menținând sesiunile de date active chiar și în cazul unei defecțiuni hardware majore la nivelul switch-urilor Core.

Securitatea a fost integrată la fiecare nivel al arhitecturii. La marginea rețelei (Edge), NAT/PAT asigură accesul controlat la internet, în timp ce în interiorul rețelei (Core), listele de control al accesului (ACL) izolează eficient departamentele sensibile (ex: IT de HR). La nivelul de acces, politicile de Port-Security (Sticky MAC) garantează că doar dispozitivele autorizate se pot conecta la porturile fizice.

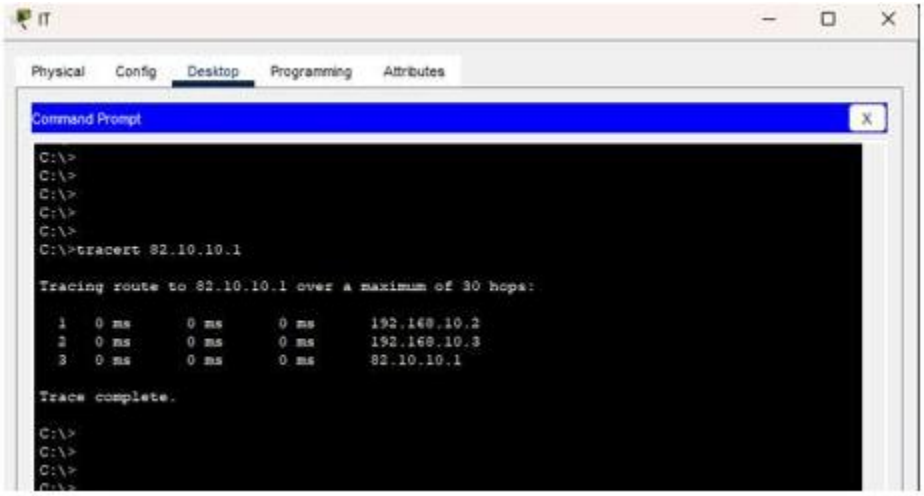
În concluzie, designul propus nu este doar o simulare funcțională, ci un model de arhitectură scalabil, pregătit pentru producție, care respectă cele mai bune practici din domeniu și standardele Cisco de înaltă disponibilitate.

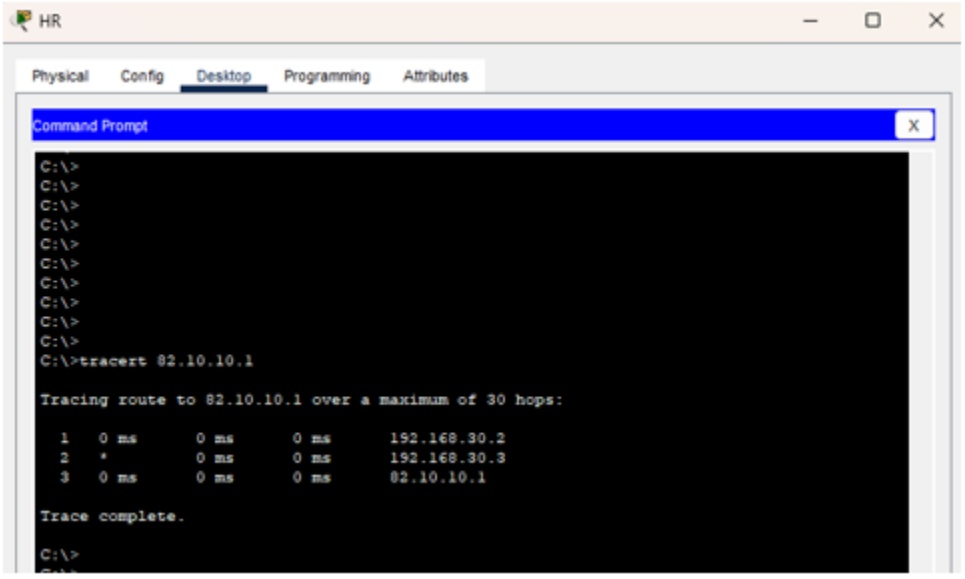
Anexe

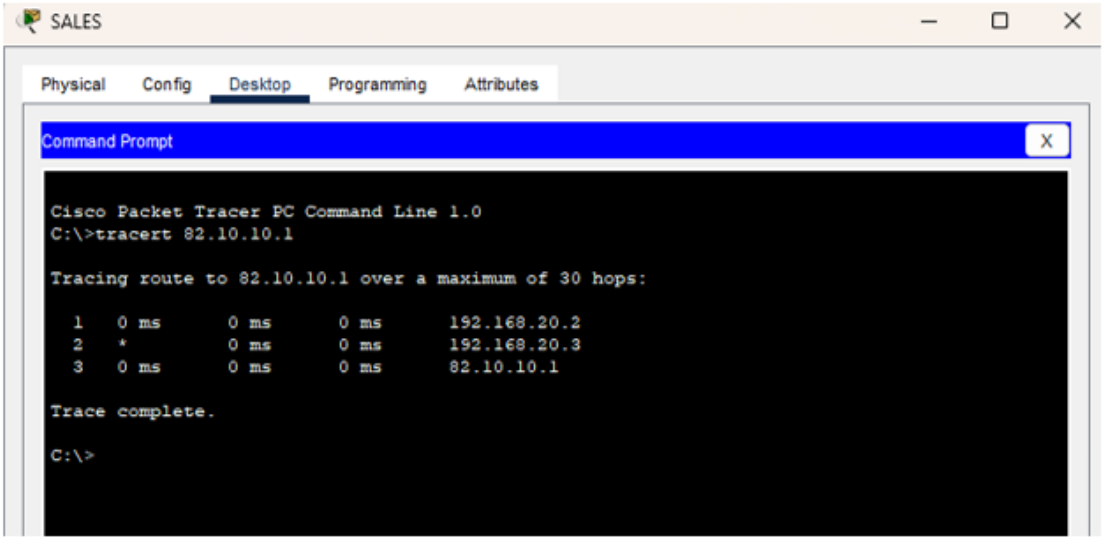
Topologia



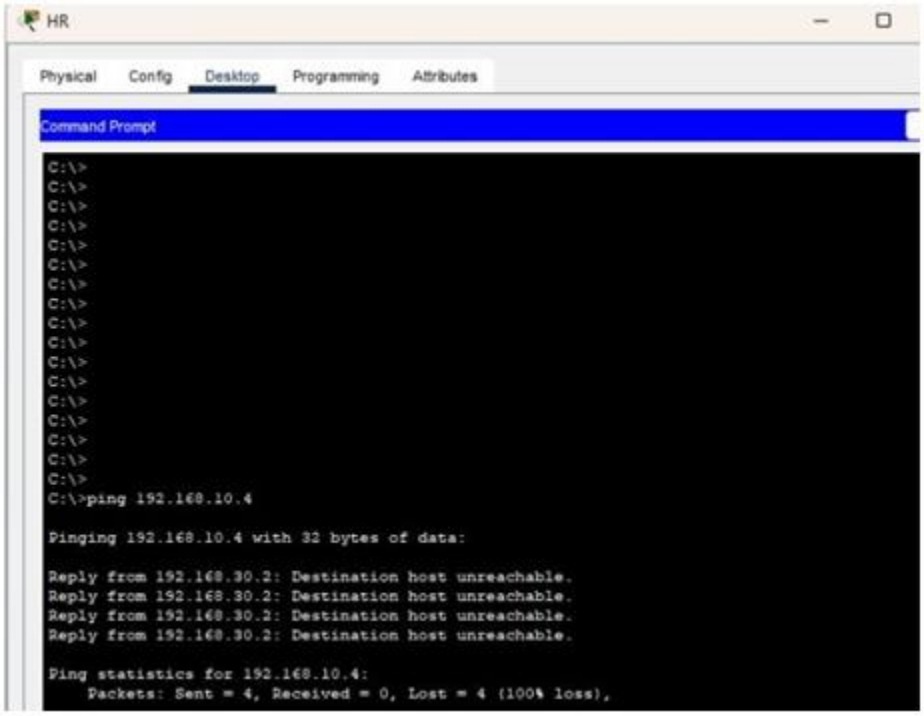
VV-01


IT
Physical
Config
Desktop
Programming
Attributes
Command Prompt
C:\>tracert 82.10.10.1
Tracing route to 82.10.10.1 over a maximum of 30 hops:
1 0 ms 0 ms 0 ms 192.168.10.2
2 0 ms 0 ms 0 ms 192.168.10.3
3 0 ms 0 ms 0 ms 82.10.10.1
Trace complete.


HR
Physical
Config
Desktop
Programming
Attributes
Command Prompt
C:\>tracert 82.10.10.1
Tracing route to 82.10.10.1 over a maximum of 30 hops:
1 0 ms 0 ms 0 ms 192.168.30.2
2 * 0 ms 0 ms 192.168.30.3
3 0 ms 0 ms 0 ms 82.10.10.1
Trace complete.

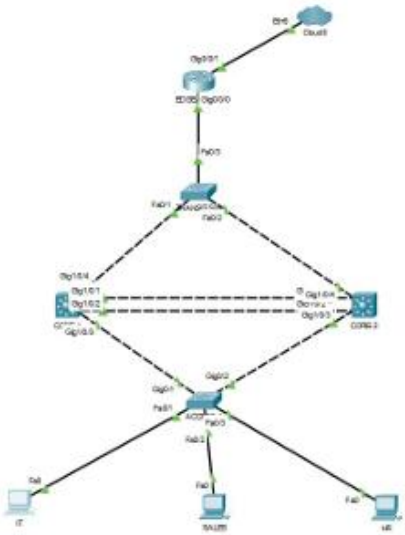

SALES
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>tracert 82.10.10.1
Tracing route to 82.10.10.1 over a maximum of 30 hops:
1 0 ms 0 ms 0 ms 192.168.20.2
2 * 0 ms 0 ms 192.168.20.3
3 0 ms 0 ms 0 ms 82.10.10.1
Trace complete.

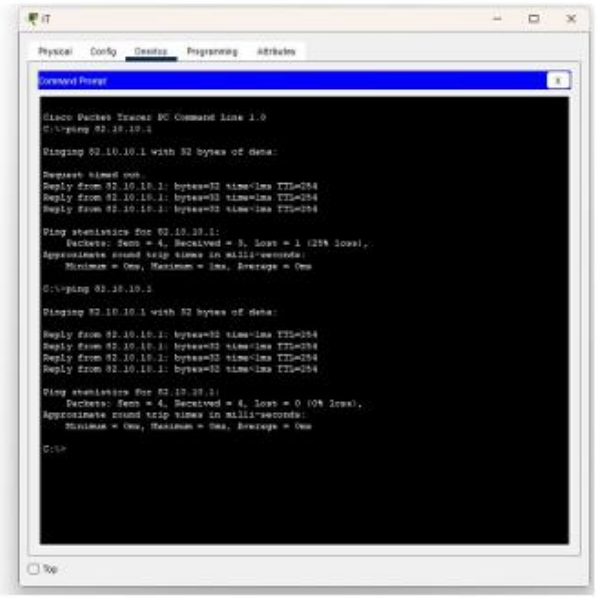
VV-02


HR
Physical
Config
Desktop
Programming
Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.10.4
Pinging 192.168.10.4 with 32 bytes of data:
Reply from 192.168.30.2: Destination host unreachable.
Reply from 192.168.30.2: Destination host unreachable.
Reply from 192.168.30.2: Destination host unreachable.
Reply from 192.168.30.2: Destination host unreachable.
Ping statistics for 192.168.10.4:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

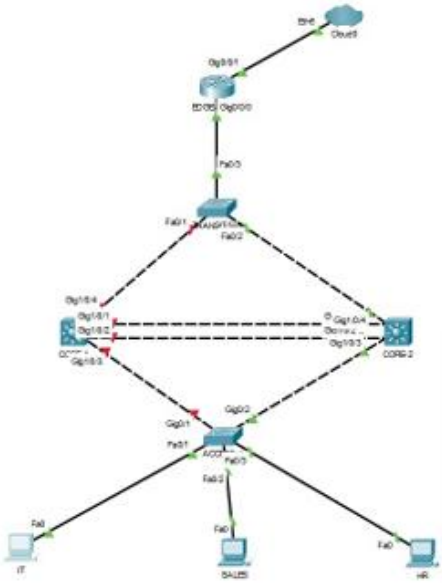
VV-3

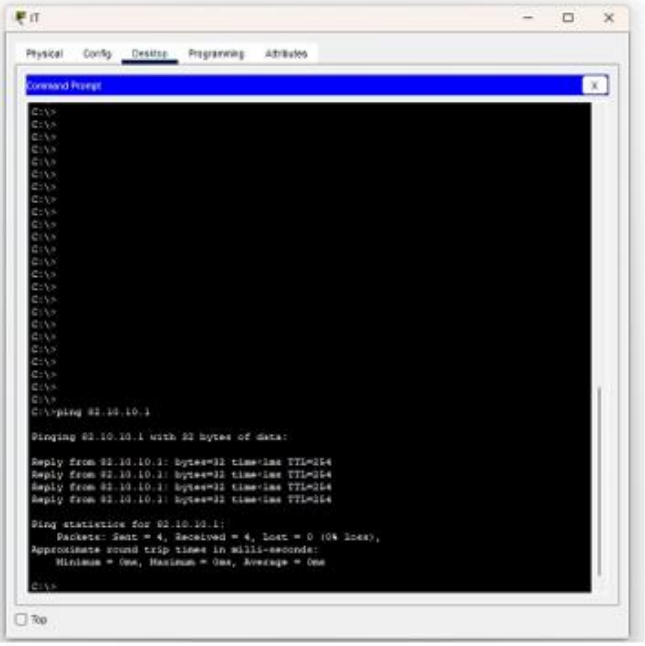
CORE-1-----ACTIV



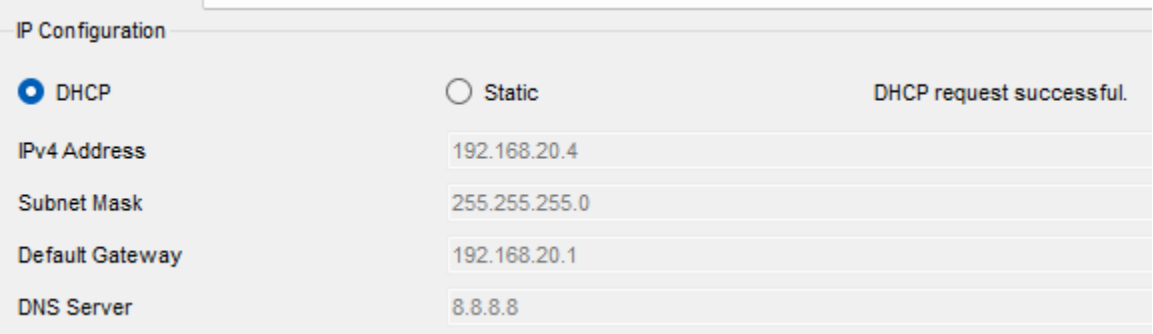


CORE-1----DEZACTIVAT

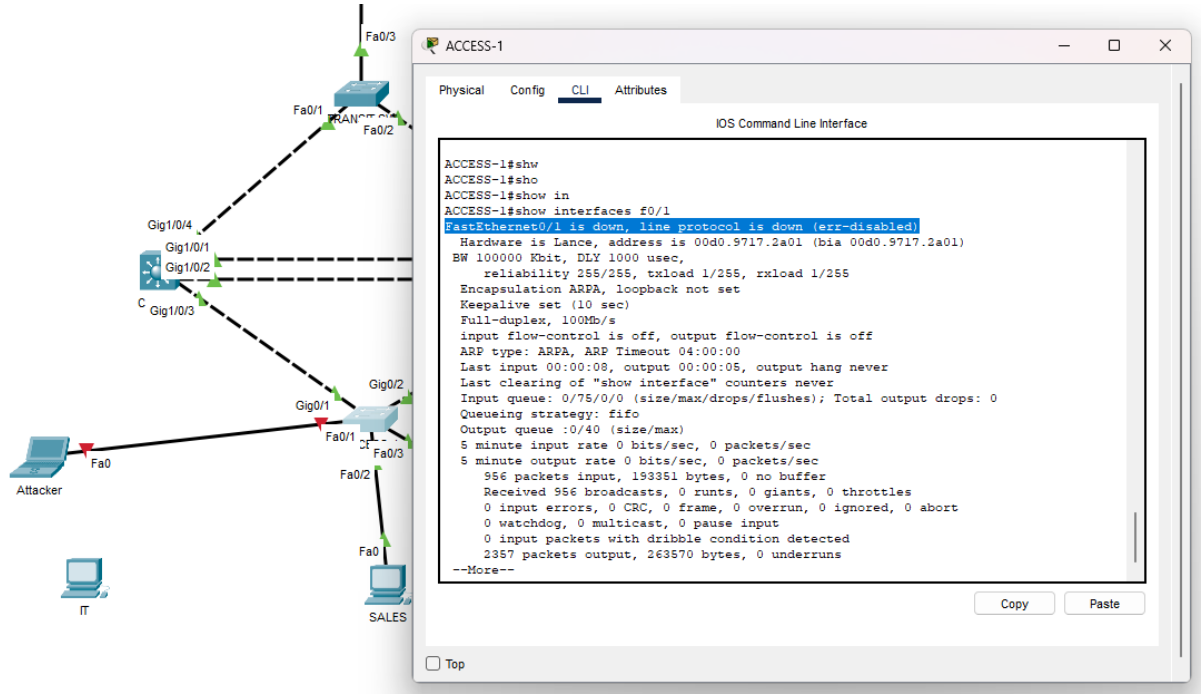




VV-04


IP Configuration
DHCP
Static
DHCP request successful.
IPv4 Address
192.168.20.4
Subnet Mask
255.255.255.0
Default Gateway
192.168.20.1
DNS Server
8.8.8.8

VV-05


Fa0/3
Fa0/1
Fa0/2
Gig1/0/4
Gig1/0/1
Gig1/0/2
Gig1/0/3
Gig0/2
Gig0/1
Fa0/1
Fa0/3
Fa0/2
Fa0
Attacker
Fa0
IT
SALES
ACCESS-1
Physical
Config
CLI
Attributes
IOS Command Line Interface
ACCESS-1#shw
ACCESS-1#sho
ACCESS-1#show in
ACCESS-1#show interfaces f0/1
FastEthernet0/1 is down, line protocol is down (err-disabled)
Hardware is Lance, address is 00d0.9717.2a01 (bia 00d0.9717.2a01)
BW 100000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
956 packets input, 193351 bytes, 0 no buffer
Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
2357 packets output, 263570 bytes, 0 underruns
--More--
Copy
Paste
Top