Name: Tarek Adel Ali

DevOps track (intern)

LinkedIn: https://www.linkedin.com/in/tarek-adel-857279197/

Q2 : Scenario

Your internal web dashboard (hosted on internal.example.com) is suddenly unreachable from multiple systems. The service seems up, but users get "host not found" errors. You suspect a DNS or network misconfiguration. Your task is to troubleshoot, verify, and restore connectivity to the internal service.

🛠️ **Your Task:**

1. Verify DNS Resolution: Compare resolution from /etc/resolv.conf DNS vs. 8.8.8.8.
2. Diagnose Service Reachability: Confirm whether the web service (port 80 or 443) is reachable on the resolved IP. Use curl, telnet, netstat, or ss to find if the service is listening and responding.
3. Trace the Issue – List All Possible Causes 🧪 Your goal here is to identify and list all potential reasons why internal.example.com might be unreachable, even if the service is up and running. Consider both DNS and network/service layers.
4. Propose and Apply Fixes ✅ For each potential issue you identified in Point 3, do the following:
5. Explain how you would confirm it's the actual root cause
6. Show the exact Linux command(s) you would use to fix it

🧠 **Note:** Please include screenshots that demonstrate how you identified and resolved the issue

🏆 **Bonus:** Configure a local /etc/hosts entry to bypass DNS for testing. Show how to persist DNS server settings using systemd-resolved or NetworkManager.

Part 1

Using dig

```
[root@localhost ~]# dig internal.example.com

; <<>> DiG 9.16.23-RH <<>> internal.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 50305
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;internal.example.com.          IN      A

;; AUTHORITY SECTION:
example.com.            5       IN      SOA     ns.icann.org. noc.dns.icann.org. 2025011625 7200 3600 1209600 3600

;; Query time: 53 msec
;; SERVER: 192.168.2.2#53(192.168.2.2)
;; WHEN: Mon Apr 28 15:29:59 EEST 2025
;; MSG SIZE  rcvd: 105

[root@localhost ~]#
```

Using dig @8.8.8.8

```
[root@localhost ~]# dig internal.example.com @8.8.8.8

; <<>> DiG 9.16.23-RH <<>> internal.example.com @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 59547
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;internal.example.com.          IN      A

;; AUTHORITY SECTION:
example.com.            1780    IN      SOA     ns.icann.org. noc.dns.icann.org. 2025011625 7200 3600 1209600 3600

;; Query time: 62 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Apr 28 15:33:12 EEST 2025
;; MSG SIZE  rcvd: 105

[root@localhost ~]#
```

Result:

So, the problem isn't just with the internal DNS server; even Google doesn't see the domain.

It's likely the domain isn't even registered online and should be an internal (private) DNS.

Part 2

For this step we will assume that the ip is 192.168.2.100
this ip is private cuz the domain has internal so cuz o that we assume a private ip

And secondly to make the tests of “curl, telnet, netstat, or ss to find if the service is listening and responding”

Using ping -c 4 192.168.2.100 to see if the assumed ip will respond or not

```
root@localhost:~
[root@localhost ~]# ping -c 4 192.168.2.100
PING 192.168.2.100 (192.168.2.100) 56(84) bytes of data.
From 192.168.2.150 icmp_seq=1 Destination Host Unreachable
From 192.168.2.150 icmp_seq=2 Destination Host Unreachable
From 192.168.2.150 icmp_seq=3 Destination Host Unreachable
From 192.168.2.150 icmp_seq=4 Destination Host Unreachable

--- 192.168.2.100 ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3106ms
pipe 3
[root@localhost ~]#
```

Then using curl http://192.168.2.100 to see of the server to see of the webpage is responded or not

```
root@localhost:~
[root@localhost ~]# curl http://192.168.2.100
curl: (7) Failed to connect to 192.168.2.100 port 80: No route to host
[root@localhost ~]# curl -k http://192.168.2.100
curl: (7) Failed to connect to 192.168.2.100 port 80: No route to host
[root@localhost ~]#
```

Checking for ports 80 and 443 using telnet 192.168.2.100 80

443

```
root@localhost:~
[root@localhost ~]# telnet 192.168.2.100 80
Trying 192.168.2.100...
telnet: connect to address 192.168.2.100: No route to host
[root@localhost ~]# telnet 192.168.2.100 443
Trying 192.168.2.100...
telnet: connect to address 192.168.2.100: No route to host
[root@localhost ~]#
```

Then check if the access to the ports 40|443 using ss -tuln | grep -E '80|443' or netstat -tuln | grep -E '80|443'

```
root@localhost:~
[root@localhost ~]# ss -tuln | grep -E '80|443'
[root@localhost ~]# netstat -tuln | grep -E '80|443'
[root@localhost ~]#
```

Part 3

DNS Issue:

There is no DNS record for internal.example.com, causing name resolution to fail.

Server Network Issue:

The server might not have a valid IP address or might not be properly connected to the network.

Firewall Configuration:

A firewall may be blocking ports 80 (HTTP) and 443 (HTTPS), preventing access to the server.

Web Server Application Issue:

The web server (e.g., Apache) might not be running or could have crashed on the target server.

Physical Network Issue:

There could be a hardware problem, such as an unplugged or faulty network cable.

Part 4

1. Confirm DNS Issue:

How to Confirm Use the following commands:

dig internal.example.com

How to Fix:

If there is a DNS resolution issue, you can temporarily add a manual entry to /etc/hosts:

echo "192.168.2.100 internal.example.com" >> /etc/hosts

2. Confirm Server Network Issue How to Confirm:

Ping the server IP: ping 192.168.2.100

How to Fix:

Ensure that the server has a valid IP address.

On the server, you can use nmtui to configure a valid static IP:

nmtui

3. Confirm Firewall Blocking How to Confirm:

firewall-cmd --list-all

How to Fix:

sudo firewall-cmd --add-port=80/tcp --permanent

sudo firewall-cmd --add-port=443/tcp --permanent

sudo firewall-cmd --reload

4. Confirm Web Server (Apache) Issue How to Confirm:

systemctl status httpd

How to Fix:

sudo systemctl start httpd

sudo systemctl enable httpd

5. Confirm Physical Network Issue How to Confirm:

Visually check the physical connection (cable) to the server.

How to Fix:

After fixing the cable, restart the network services:

systemctl restart NetworkManager

Bonus:

1. Configure Local /etc/hosts Entry

sudo nano /etc/hosts

Add the following line at the bottom:

192.168.2.100 internal.example.com

Save and exit: Press Ctrl + O, then Enter, then Ctrl + X.

Test the configuration: ping internal.example.com

If you get a reply, then the configuration is successful.

2. Persist DNS Server Settings using NetworkManager Steps:

Use nmtui

nmtui

Choose Edit a Connection. Select your active connection. Scroll down to the DNS section.

Add the desired DNS servers, for example:

8.8.8.8, 1.1.1.1

Save and exit.

Restart NetworkManager

systemctl restart NetworkManager