

13 The Cisco Troubleshooting Methodology

– Answer Key

This lab tests your network troubleshooting skills.

Troubleshoot Connectivity to DNS Server

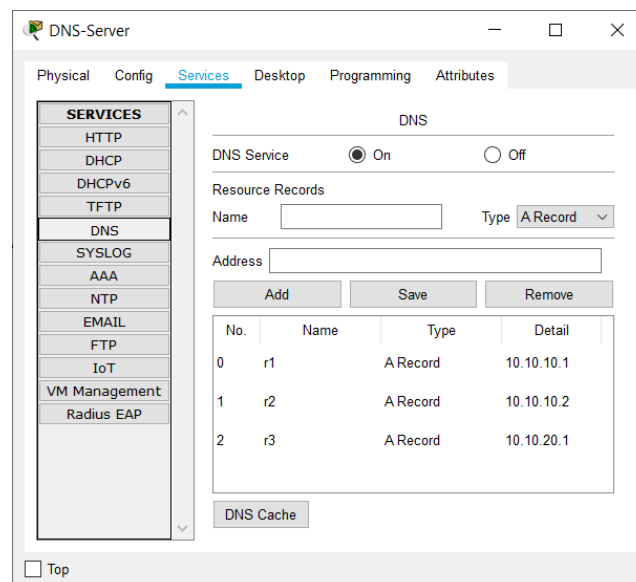
Note that routers cannot be DNS servers in Packet Tracer (it does not support the 'ip dns server' command) so we are using a Packet Tracer server device as the DNS server.

- 1) The host with IP address 10.10.10.10 has been configured as a DNS server and should be able to resolve requests for 'R1', 'R2' and 'R3'. Members of staff have complained that DNS is not working.
- 2) From R3, use Telnet to check if the DNS service appears operational on the DNS server at 10.10.10.10.

```
R3#telnet 10.10.10.10
Trying 10.10.10.10 ...
% Connection timed out; remote host not responding
```

- 3) When you have verified that DNS is not working, troubleshoot and fix the problem. You have fixed the problem when R3 can ping R1 by hostname. Note that there may be more than one issue causing the problem.

(You can click on the DNS server and then the 'Services' tab to check the server's DNS configuration.)



There is more than one way to troubleshoot the issue. A suggested workflow is shown below.

The first two questions to ask when troubleshooting a problem are:

1. Was it working before? If so, has something changed which could cause the problem? This will usually direct you to the cause.

This question is not particularly useful for our example as the DNS server has just been brought online for the first time.

2. Is the problem affecting everybody or just one particular user? If it's affecting just one user, the likelihood is that the problem is at their end.

In this case the problem is affecting all users, so the problem is likely on the server end or with the network.

The error message when we tried to Telnet was 'remote host not responding', so it looks like a connectivity issue.

Ping from R3 to the DNS server.

```
R3#ping 10.10.10.10
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2  
seconds:  
U.U.U  
Success rate is 0 percent (0/5)
```

The ping fails at the network layer so there is little point in checking the DNS service at higher layers until we fix this problem.

Rather than checking connectivity hop by hop, we can possibly save a little time by using traceroute.

```
R3#traceroute 10.10.10.10  
Type escape sequence to abort.  
Tracing the route to 10.10.10.10  
  
 1 10.10.20.2 0 msec 0 msec 0 msec  
 2 10.10.20.2 !H * !H  
 3 * *
```

The traceroute got as far as R2, which lets us know that R3 has the correct route to get to the DNS server, and the problem is probably between R2 and the DNS server.

R2 has an interface connected to the 10.10.10.0/24 network, so we don't need to check it has a route to the DNS server. We do need to check that the interface is up though.

```
R2#sh ip int brief
Interface                               IP-Address   OK? Method Status          Protocol
FastEthernet0/0                         10.10.10.2   YES NVRAM   administratively down down
FastEthernet0/1                         unassigned   YES NVRAM   administratively down down
FastEthernet1/0                         10.10.20.2   YES NVRAM   up              up
FastEthernet1/1                         unassigned   YES NVRAM   administratively down down
Vlan1                                    unassigned   YES NVRAM   administratively down down
```

There's the problem – FastEthernet0/0 facing the DNS server is administratively shutdown. Let's fix it.

```
R2(config)#interface f0/0
R2(config-if)#no shutdown
```

Next we'll try pinging from R3 to the DNS server again to verify we fixed connectivity.

```
R3#ping 10.10.10.10
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2
seconds:
...!!
Success rate is 60 percent (3/5), round-trip min/avg/max =
0/0/0 ms
```

That looks better – don't worry if the first one or two pings are dropped, there may be a delay while the ARP cache is updated. Next we'll verify DNS is working.

```
R3#ping R1
Translating "R1"...domain server (10.10.10.1)
% Unrecognized host or address or protocol not running.
```

The error message tells us the problem if we take the time to really read it – R3 is using 10.10.10.1 as its DNS server, but the correct address is 10.10.10.10.

We fix that next. Don't forget to remove the incorrect entry first.

```
R3(config)#no ip name-server 10.10.10.1
R3(config)#ip name-server 10.10.10.10
```

Then test again.

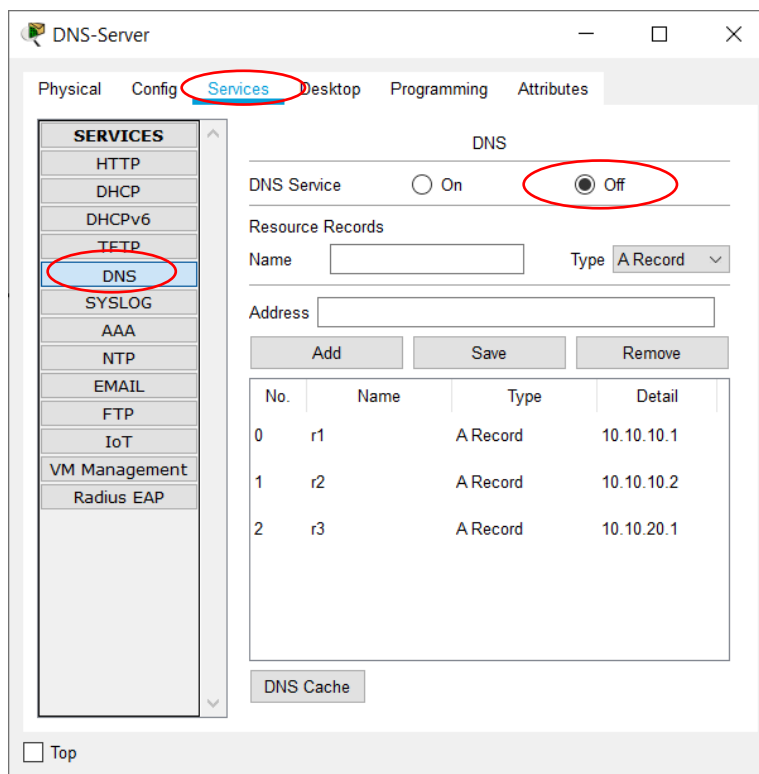
```
R3#ping R1
```

```
Translating "R1"...domain server (10.10.10.1)
```

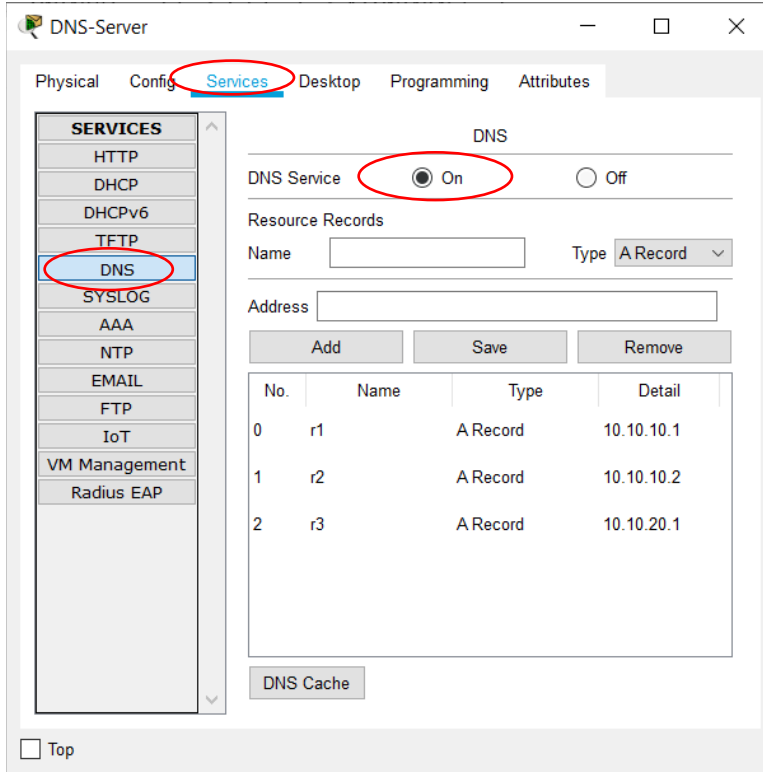
```
% Unrecognized host or address or protocol not running.
```

The error message is still there. We know we have connectivity and the DNS server configured correctly on R3, so the problem looks like it's on the DNS server.

Check the DNS service is running on the 10.10.10.10 host and that address records are configured for 'R1', 'R2' and 'R3'.



The address records are there but the DNS service is turned off. Turn it back on.



Time to test it from R3 again.

```
R3#ping R1
Translating "R1"...domain server (10.10.10.10)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2
seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/0/4 ms
```

That's the problem solved.

To summarise the issues: port FastEthernet0/0 was shut down on R2, R3 was using the wrong IP address for the DNS server, and the DNS service was not running on the server.

Problems in the real world are usually caused by just one error rather than three as in this case. This can still occur though, particularly when a new service is being deployed.