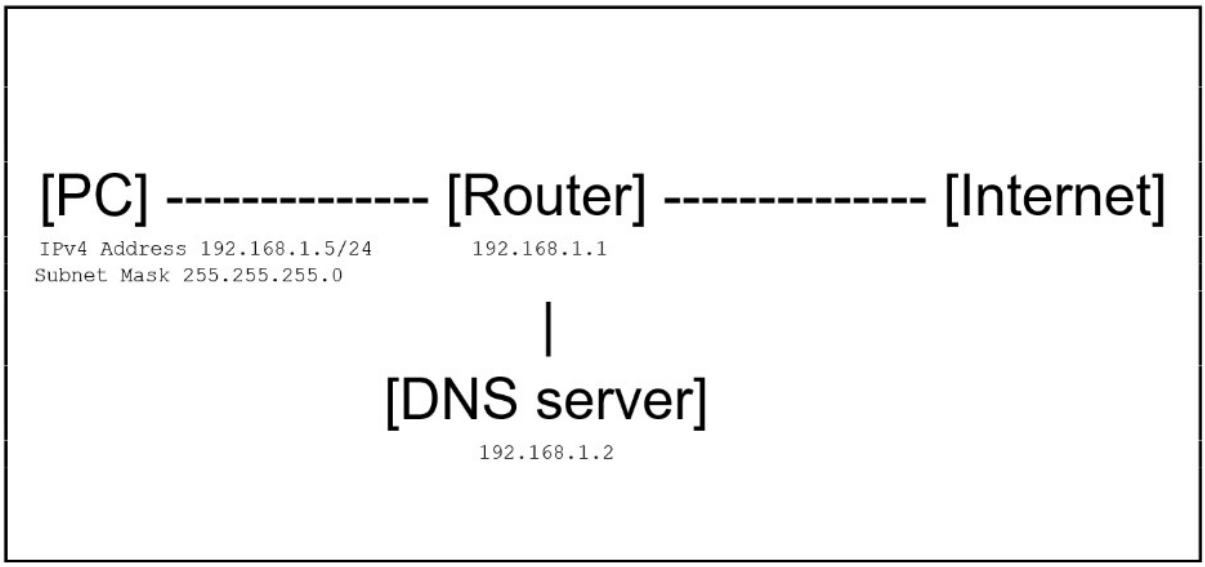

Diagram showing a PC, Router, and the Internet all connected in one row with a DNS server below connected to the router. The PC's IPv4 Address is 192.168.1.5/24 and the Subnet Mask is 255.255.255.0. The Router's IP is 192.168.1.1 and the DNS server's 192.168.1.2

Step 1: Initial connectivity check

1. Open the command-line interface on your computer (Press **Win** + **R** at the same time, then type "cmd" and press **Enter**).
2. Ping Google's website using its IP address to confirm employee reports that they can reach the website using the IP address.
   - **Command:** *ping 8.8.8.8*
   - **Expected result:** Successful ping replies.
   - **Output:**

```
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=10ms TTL=115
Reply from 8.8.8.8: bytes=32 time=10ms TTL=115
Reply from 8.8.8.8: bytes=32 time=10ms TTL=115
Reply from 8.8.8.8: bytes=32 time=10ms TTL=115

Ping statistics for 8.8.8.8:
     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
     Minimum = 10ms, Maximum = 10ms, Average = 10ms
```

   - **Interpretation:** Google is reachable using its IP address.
3. Ping Google's website using its domain name to verify employee reports that they can’t reach the website using the domain name.
   - **Command:** *ping www.google.com*
   - **Expected result:** The ping request could not find host www.google.com.
   - **Output:**

```
Ping request could not find host www.google.com. Please check the name
and try again.
```

Output showing unsuccessful ping request

   - **Interpretation:** Employee reports have been verified, Google can be reached using its IP address but not its domain name. The discrepancy between these two tests suggests that there is a problem with the DNS server so that needs to be checked next.

Step 2: DNS configuration check

1. Verify the DNS server settings on your computer. The DNS server IP address should be 192.168.1.2.
   - **Command:** *ipconfig /all*
   - **Expected result:** Correct DNS server IP address listed.
   - **Output:**

```
Windows IP Configuration

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : example.local
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection
   Physical Address. . . . . . . . . : 00-1A-2B-3C-4D-5E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DNS Servers . . . . . . . . . . . : 192.168.1.2
```

   - **Interpretation:** The DNS server IP address listed is 192.168.1.2, which matches the expected DNS server settings for the network. Remember, this company's network only has one DNS server. As an IT professional, you will likely encounter other configurations with multiple servers, in which case the *ipconfig /all* command would show the details of all the servers.

2. Check if the DNS server is reachable. If there are multiple servers, you would have to ping each one individually.
   - **Command:** *ping <192.168.1.2>*
   - **Expected result:** Successful ping replies from the DNS server.
   - **Output:**

```
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

   - **Interpretation:** The ping output shows that the device at IP address 192.168.1.2 is reachable, with all packets successfully sent and received without any loss.

3. After confirming that the DNS server settings are correct and the server is reachable, the next step is to use *tracert* to diagnose the network path between the computer and the DNS server or the target website and double-check that no packets are being delayed or dropped.
   - **Command:** *tracert www.google.com*
   - **Expected result:** The command should display each hop along the route to the target domain, including the response times for each hop, and there should be no delays or failures.
   - **Output:**

```
Tracing route to www.google.com [172.217.11.46]
over a maximum of 30 hops:
  1     1 ms     1 ms     1 ms  192.168.1.1
  2    10 ms     9 ms    10 ms  10.0.0.1
  3    12 ms    11 ms    12 ms  172.16.0.1
  4    25 ms    24 ms    25 ms  203.0.113.1
  5    50 ms    51 ms    50 ms  198.51.100.1
  6    70 ms    69 ms    70 ms  172.217.11.46
Trace complete.
```

- **Interpretation:** There are no apparent delays or failures along the network path. Now that you have verified that the DNS server settings are correct and that the server is reachable, the next step is a DNS resolution test to check the server's functionality in translating a domain name (like www.google.com) to its corresponding IP address.

Step 3: DNS resolution test

1. Use the *nslookup* tool to query the DNS server for the domain name.
   - **Command:** *nslookup www.google.com*
   - **Expected result:** The command should return the DNS server being queried along with the IP address of the domain name.
   - **Output:**

```
Server:  dns.example.local
Address:  192.168.1.2

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4003:c02::6a
          8.8.8.8
```

Output showing the DNS server is reachable and correctly processing DNS queries

- **Interpretation:** The *nslookup* output indicates that the DNS server at 192.168.1.2 is functioning correctly and successfully resolving the domain name www.google.com to its corresponding IP addresses, which include both IPv6 and IPv4 addresses. This confirms that the DNS server is reachable and correctly processing DNS queries. After verifying that the DNS server is functioning correctly and resolving domain names, clearing the DNS cache on the computer will ensure that any outdated or corrupted DNS entries are removed.

Step 4: DNS cache and service check

1. Clear the DNS cache on the computer.
   - **Command:** *ipconfig /flushdns*
   - **Expected result:** Successfully flushed the DNS Resolver Cache.
   - **Output:**

```
Successfully flushed the DNS Resolver Cache.
```

Output showing DNS Resolver Cache was successfully flushed

- **Interpretation:** Clearing the DNS cache ensures that any outdated or corrupted DNS entries are removed, which helps to resolve issues caused by stale DNS records. This allows the system to fetch fresh DNS data for domain name resolutions.

2. Restart the DNS Client service.
   - **Command:** *net stop dnscache && net start dnscache*
   - **Expected result:** The DNS Client service is stopped and restarted successfully.
   - **Output:**

```
The DNS Client service was stopped successfully.
The DNS Client service was started successfully.
```

Output showing the DNS Client service was stopped and then restarted successfully

- **Interpretation:** Restarting the DNS Client service ensures that the service is functioning properly and can process DNS queries correctly. This step helps to resolve any potential issues with the DNS Client service itself and ensures that fresh DNS queries are made.

Step 5: Verification

1. After clearing the DNS cache and restarting the DNS Client service, perform another *nslookup* to verify the DNS resolution.
2. Ping the domain name again to confirm the issue is resolved.

- **Command:** *ping www.google.com*
- **Expected result:** Successful ping replies.
- **Output:**

```
Pinging www.google.com [8.8.8.8] with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=10ms TTL=115
Reply from 8.8.8.8: bytes=32 time=10ms TTL=115
Reply from 8.8.8.8: bytes=32 time=10ms TTL=115
Reply from 8.8.8.8: bytes=32 time=10ms TTL=115

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 10ms, Average = 10ms
```

Output showing successful ping replies

- **Interpretation:** The successful ping replies from www.google.com indicate that the DNS resolution issue has been resolved, as the domain name now correctly resolves to its IP address. This confirms that the steps taken to clear the DNS cache and restart the DNS Client service were effective.