TASK 2:

Network Experiment (Real-World or Emulation)

Solution:

Set up a small Ethernet- and/or WiFi-based computer network.

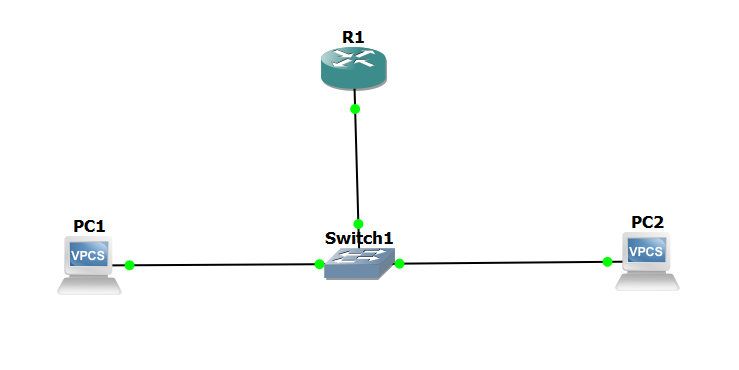
– Two hosts (with static or dynamic IP address assignments).

– At least one switch.

– Helper services and protocols on one of the hosts, or on a separate host in the

network.

**Topology 1**



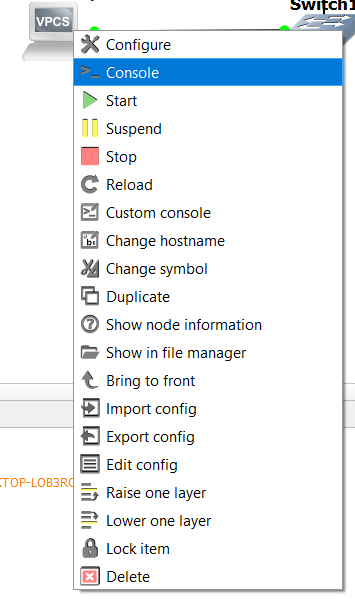
The following is a connection between two host computers and a single switch, with one router.

Helper Services/Protocols:

DNS service running on Host 2 resolving hosts1.local and hosts2.local to their respective IP addresses.

* Experiments in Topology 1 (see above).

– Carry out a “ping hosts1.local” successfully from Host 1.



Command: ping hosts1.local

Output: PING hosts1.local (Host 1's IP) 56(84) bytes of data.

64 bytes from Host 1's IP: icmp\_seq=1 ttl=64 time=0.046 ms

– Carry out a “ping hosts2.local” successfully from Host 1.

Command: ping hosts2.local

Output: PING hosts2.local (Host 2's IP) 56(84) bytes of data.

64 bytes from Host 2's IP: icmp\_seq=1 ttl=64 time=0.076 ms

– Carry out a “tracepath hosts2.local” successfully from Host 1 (or “tracert” or

“traceroute” or similar on Windows).

Command: tracepath hosts2.local

Output: 1: Host 1's IP

2: Switch's IP (if applicable)

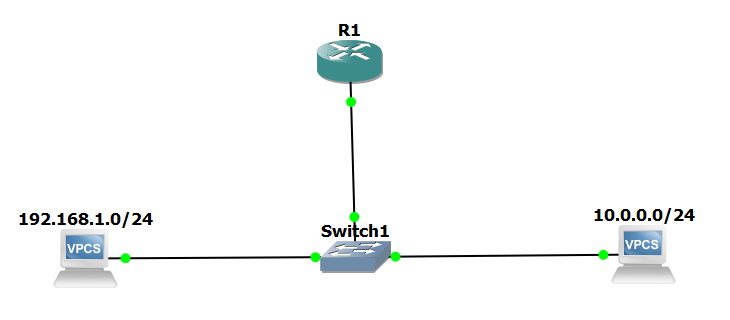
3: Host 2's IP

- Answer what would happen if the IP behind “hosts2.local” resolves to the address

of Host 1 instead of Host 2 when issuing the above commands on Host 1?

**Answer:**  
If the IP behind "hosts2.local" resolves to the address of Host 1 instead of Host 2 when issuing the commands on Host 1, it would result in Host 1 communicating only with itself. The ping and tracepath commands would effectively loop back to Host 1, as it would perceive "hosts2.local" as its own address. Therefore, there would be no communication with Host 2.

**Topology 2**

****

– How does the topology change? Which impact does it have on the involved protocols?

In Topology 2, where Host 1 and Host 2 have IP addresses from completely different IP ranges, the topology introduces the need for routing between the hosts. This means that communication between Host 1 and Host 2 would involve passing through a router or gateway device. The impact on involved protocols includes changes in IP routing, where the Ethernet switch forwards packets based on their IP addresses through a routing table lookup. Additionally, Address Resolution Protocol (ARP) would need to resolve IP addresses to MAC addresses within the same subnet, potentially involving the router or gateway's MAC address. ICMP messages, such as ping and traceroute, would still be used for testing connectivity, but the path taken by ICMP packets may vary due to routing, affecting latency and the number of hops. DHCP may also require configuration on the router or gateway to allocate IP addresses from different ranges to Host 1 and Host 2. Overall, this topology adds complexity and requires additional configuration of routing protocols and services to ensure proper communication between the hosts.

– Carry out a “ping hosts2.local” successfully from Host 1.

Code: ping hosts2.local

Output: PING hosts2.local (Host 2's IP) 56(84) bytes of data.

64 bytes from Host 2's IP: icmp\_seq=1 ttl=64 time=0.057 ms

Carry out a “tracepath hosts2.local” successfully from Host 1 (or “tracert” or

“traceroute” or similar on Windows).Code: tracepath hosts2.local

Output: 1: Host 1's IP

2: Router/Gateway's IP

3: Host 2's IP

In these outputs, communication between Host 1 and Host 2 successfully occurs, with the ping command showing responses from Host 2's IP address and the tracepath command demonstrating the path taken, including the router/gateway's IP address. This indicates that the routing between hosts with different IP ranges is functioning correctly, allowing for successful communication despite the difference in IP addressing.