Name: Andrew Hayes
E-mail: a.hayes18@universityofgalway.ie
ID: 21321503

CT3531

2023–10–13

Assignment 01: Expand the VLAN-Based Network

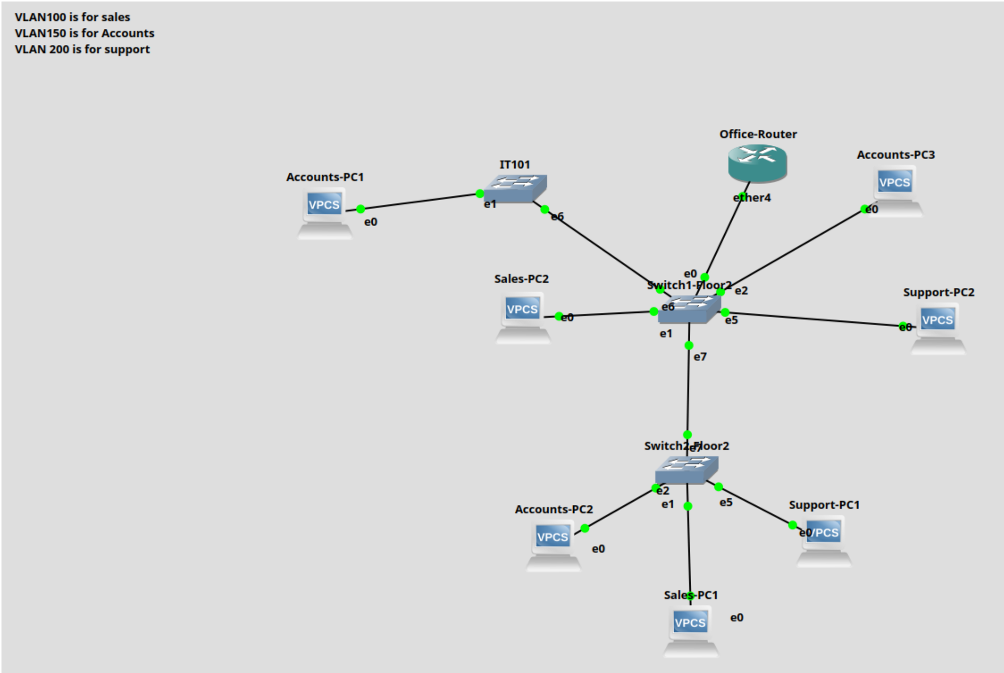

Figure 1: Network Topology

```
[admin@Office-Router] > export
# oct/12/2023 10:51:24 by RouterOS 6.49.6
# software id =
#
#
#
/interface ethernet
set [ find default-name=ether1 ] disable-running-check=no
set [ find default-name=ether2 ] disable-running-check=no
set [ find default-name=ether3 ] disable-running-check=no
set [ find default-name=ether4 ] disable-running-check=no
set [ find default-name=ether5 ] disable-running-check=no
set [ find default-name=ether6 ] disable-running-check=no
set [ find default-name=ether7 ] disable-running-check=no
set [ find default-name=ether8 ] disable-running-check=no
/interface vlan
add interface=ether4 name=VLAN100 vlan-id=100
add interface=ether4 name=VLAN150 vlan-id=150
add interface=ether4 name=VLAN200 vlan-id=200
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip pool
add name=dhcp_pool0 ranges=192.168.100.2-192.168.100.254
add name=dhcp_pool1 ranges=192.168.200.2-192.168.200.254
add name=dhcp_pool2 ranges=192.168.150.2-192.168.150.254
/ip dhcp-server
add address-pool=dhcp_pool0 disabled=no interface=VLAN100 name=dhcp1
add address-pool=dhcp_pool1 disabled=no interface=VLAN200 name=dhcp2
add address-pool=dhcp_pool2 disabled=no interface=VLAN150 name=dhcp3
/ip address
add address=192.168.100.1/24 interface=VLAN100 network=192.168.100.0
add address=192.168.200.1/24 interface=VLAN200 network=192.168.200.0
add address=192.168.150.1/24 interface=VLAN150 network=192.168.150.0
/ip dhcp-client
add disabled=no interface=ether1
/ip dhcp-server network
add address=192.168.100.0/24 gateway=192.168.100.1
add address=192.168.150.0/24 dns-server=8.8.8.8 gateway=192.168.150.1
add address=192.168.200.0/24 gateway=192.168.200.1
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1
/system identity
set name=Office-Router
[admin@Office-Router] >
```

Figure 2: Router Configuration

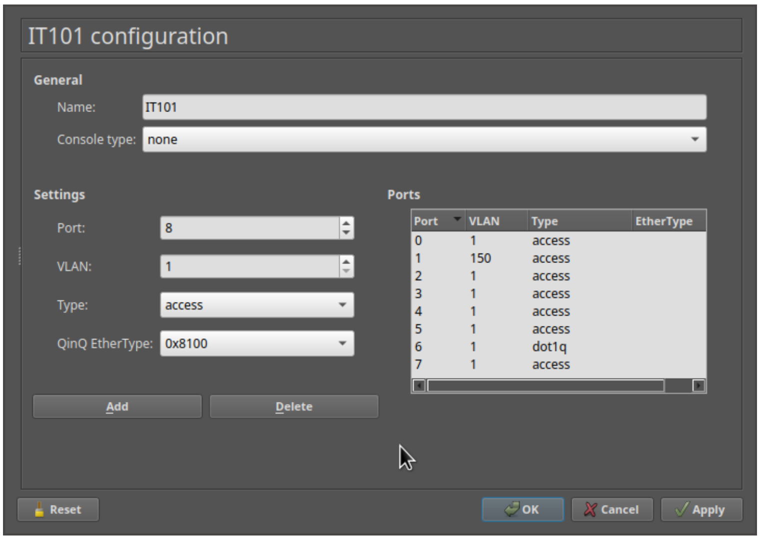

Figure 3: Configuration of the New IT101 Switch

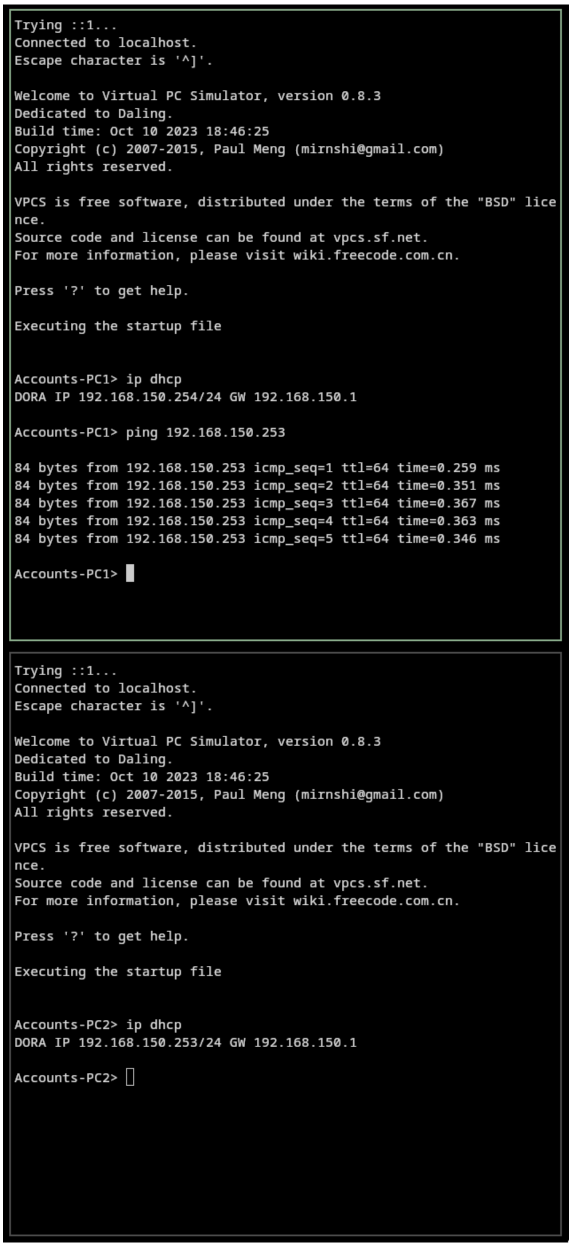

Figure 4: Verifying that The New VPC Devices in the Accounts VLAN Can Ping Each Other

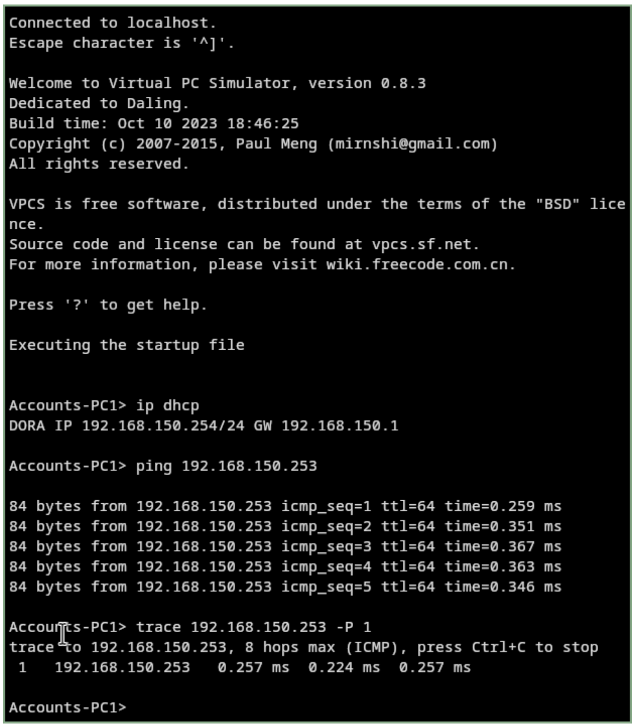

Figure 5: Running a Trace from a VPC to Another VPC in the Same VLAN (Same VPCs as in Above Figure)

When we run a trace from Accounts-PC1 to Accounts-PC2 (which are both on VLAN150), we can see that it only takes one hop to get from Accounts-PC1 to Accounts-PC2. Because these devices are in the same VLAN, they do not need to go through the router to address each other, and can reach other directly. When devices share a VLAN, they can communicate directly at the Data Link Layer.

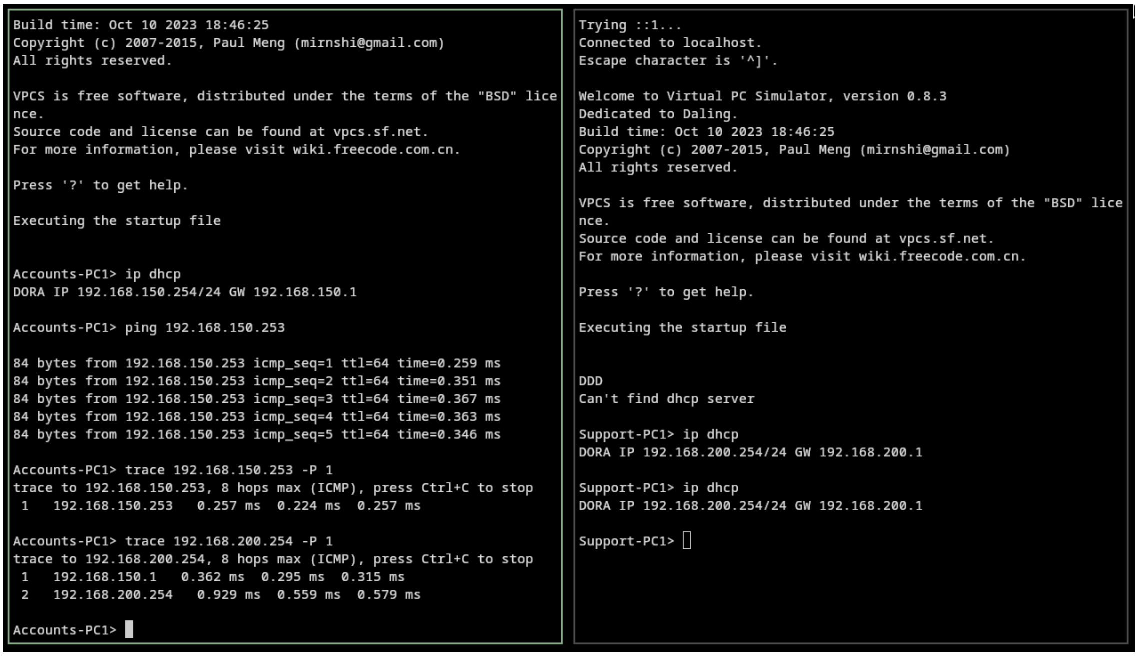

Figure 6: Running a Trace from a VPC to Another VPC in Different VLANs

When we run a trace from Accounts-PC1 to Support-PC1 (which are on different VLANs), we can see that it takes two hops to get from Accounts-PC1 to Support-PC1. Communication between separate VLANs requires routing, and therefore communicating between two devices on two different VLANs requires that the packets go through a router. The first IP in the trace is that of the router: `192.168.150.1` (or rather the IP of the gateway of VLAN150 on the router). The second IP in the trace is that of Support-PC1: `192.168.200.254`.

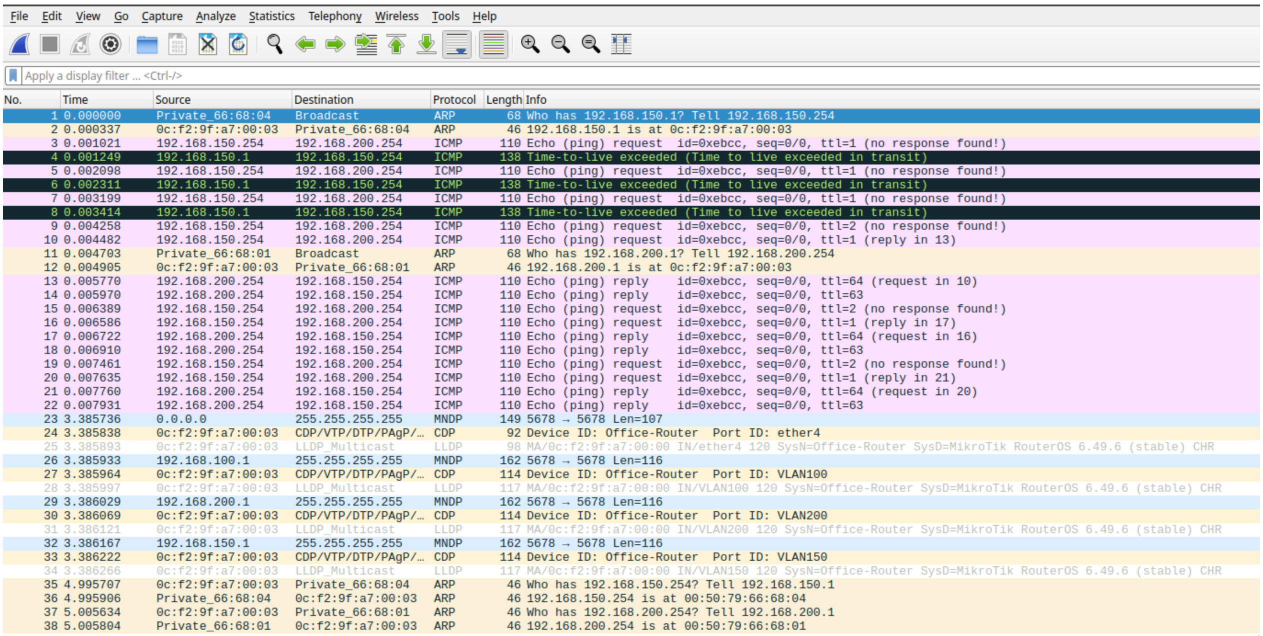

Figure 7: Packet Capture on the Link Connecting the Switch & the Router During a Ping between VPCs on Different VLANs

The general outline of what happened in this packet capture is as follows:

1. An ICMP ping is sent from Accounts-PC1 (which is on VLAN150) to Support-PC1 (which is on VLAN200). Ethernet frames that travel between VLANs need a tag that identifies the VLAN as per the 802.1Q protocol. However, the 802.1Q is not added by the VPC sending the ping; instead, the tag is added by the first switch that the frame passes through, in this case the IT101 switch. The IT101 switch will have encapsulated the packet with an 802.1Q header and added the VLAN information, including the priority bits, the VLAN ID of the VLAN to which the packet belongs, & the Canonical Format Indicator which indicates the canonical format of the MAC address. Therefore, by the time the packet reaches the Switch1-Floor2 switch, the VLAN tag has already been added to the frame.

2. The Switch1-Floor2 switch then forwards the encapsulated packet which now contains the 802.1Q header to the Office-Router router. This can be seen in the first ICMP packet that we captured going from `192.168.150.254` (Accounts-PC1) to `192.168.200.254` (Support-PC1):

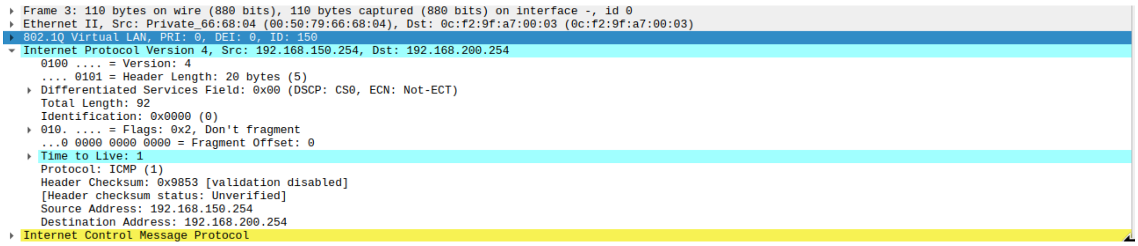

Figure 8: ICMP Packet Containing the 802.1Q Tag

3. We can tell what links require an 802.1Q header by checking whether they are trunks or access links: trunks expect packets to have an 802.1Q header so that the switches or routers that they are linking can know which VLAN they belong to. Access links do not expect an 802.1Q header, as the ports which access links join are specified to belong to a certain VLAN when the switch is configured. Therefore every packet traversing one of the trunk links, i.e. IT101 ↔ Switch1-Floor2, Switch1-Floor2 ↔ Office-Router, & Switch1-Floor2 ↔ Switch2-Floor2, requires a 802.1Q header. The last switch (Switch2-Floor2) before the destination VPC (Support-PC1) will remove the 802.1Q header, extracting the original ICMP echo request packet, and send it down the access link to Support-PC1.

4. The router is needed to facilitate the inter-VLAN communication; although, in purely physical terms, data could be transferred via the switches from Accounts-PC1 to Support-PC1 without having to go to the router, the router is needed to facilitate inter-VLAN communication over IP, as the VLANs have separate broadcast domains and the individual VPCs do not know which VLAN they belong to, if any. The router forwards the packets to the switch Switch1-Floor2, which passes them to Switch2-Floor2.

5. When the ICMP packets reach Switch2-Floor2, the 802.1Q header is stripped from them, as they have now traversed the last trunk link that they need to and are now going to pass over an access port to Support-PC1. Since we are capturing the

packets over the trunk link between a Switch1-Floor2 & Office-Router, we will never see a packet without an 802.1Q header, although they are in use for this ping.

6. When the echo request reaches Support-PC1, it send back an echo reply via Switch2-Floor2. The 802.1Q header will be added at Switch2-Floor2, and the process will repeat to route the packet across the trunks to the router, and then to the IT101 switch, where the 802.1Q header will be stripped and the packet forwarded back to Accounts-PC1, completing the ping.