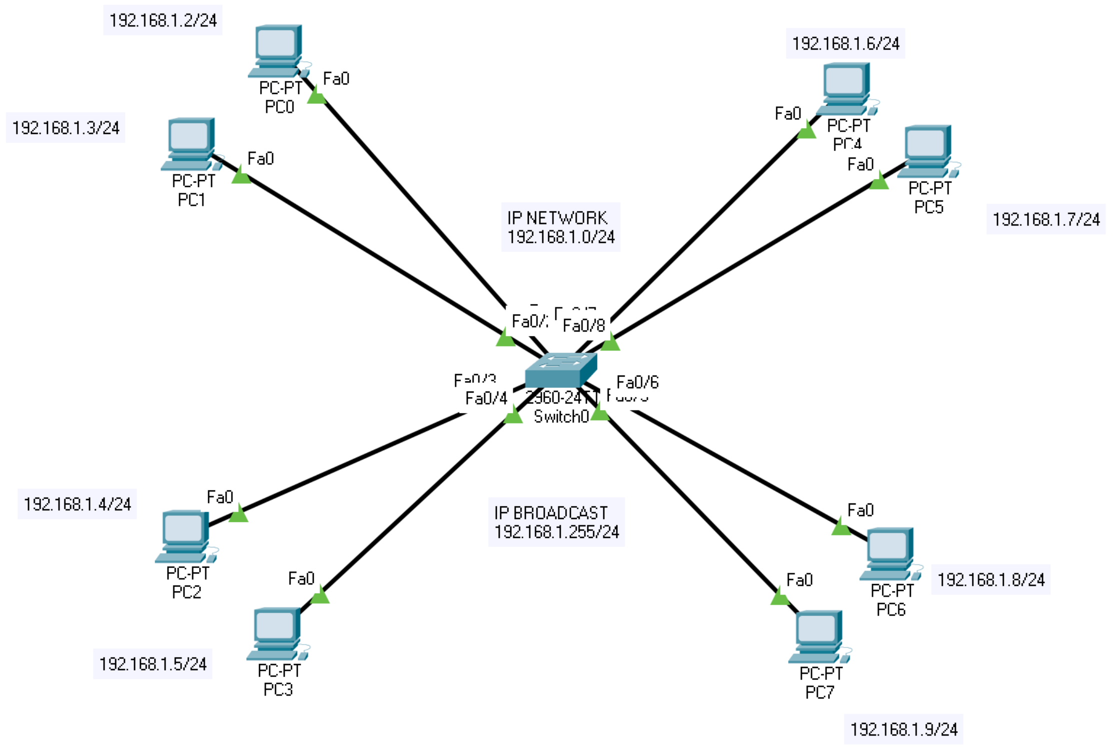
Project & Essay N° 1 - Week 1

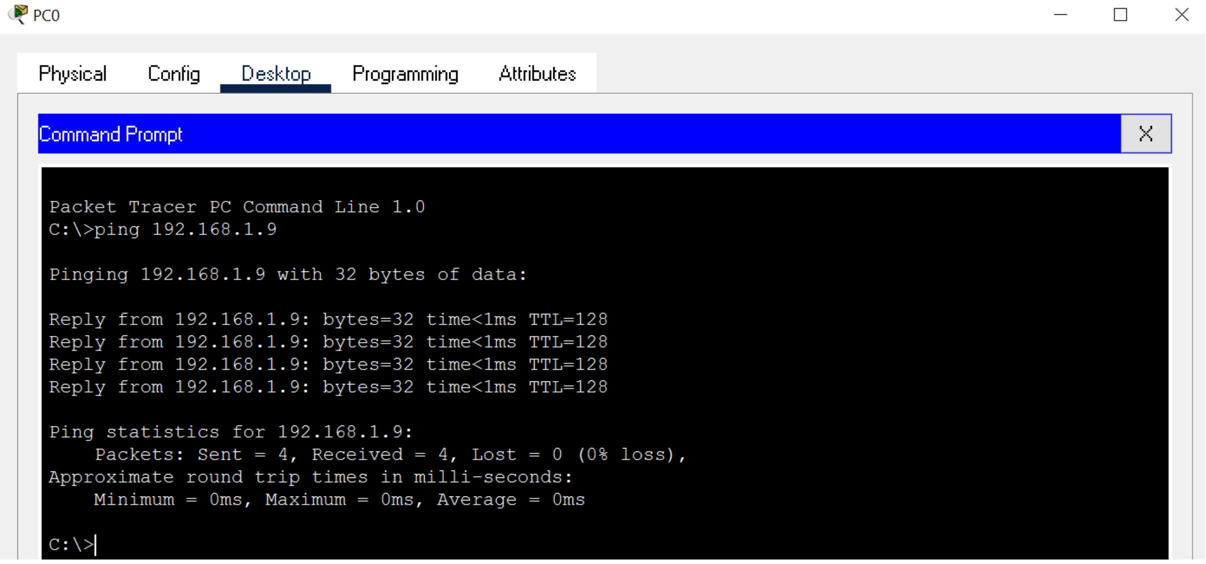
Today's project simulation asked us to create a segmented network of at least 8 devices divided in 4 different VLANs to explore the different variabilities of data exchange in a complex network. The first step to proceed through our task was to add a switch and 8 end-devices to our Cisco Packet Tracer network, as all of these clients will belong to the same Network IP (**192.168.1.0/24**) and therefore don't need a Router to connect them. All of the end-devices are then connected to a Layer 2 Switch, allowing us to communicate between clients pertaining to the same Network. Due to the fact that we're working with a classful Class C Network, the IP Host range is between 192.168.1.2/24 and 192.168.1.254/24, as 192.168.1.1/24 and 192.168.1.255/24 are occupied respectively by the Gateway IP(conventionally) and the Broadcast IP. We then choose freely from the available hosts to configure the single devices, with the following end result.

Barebone Network, no VLANs setup:



As we expect from the conditions of the initial setup, all of the devices are able to communicate through the switch, and we can verify this through a ping request from the command prompt in Cisco Packet Tracer. We'll use PC0 (192.168.1.2/24) and PC7(192.168.1.9/24) as the relevant examples for this exercise. PC0 pings PC7, which results in an ICMP and an ARP request (due to the fact that PC0 does not know the MAC address of PC7 yet) being submitted first and foremost to our Layer 2 Switch; receiving the IP address, the switch then sends out the ARP request on broadcast to all of the devices connected to it, trying to match and associate through the ARP table the MAC address corresponding to the IP we pinged. The switch then receives a reply from the only device it can match (in this case PC7), and the information is then sent back to PC0 which will now know the MAC address of PC7. With this last step, the connection between the two devices is completed, and they will now be able to communicate without any issues, as we can see in the screenshot below.

Ping between different clients before VLAN setup:



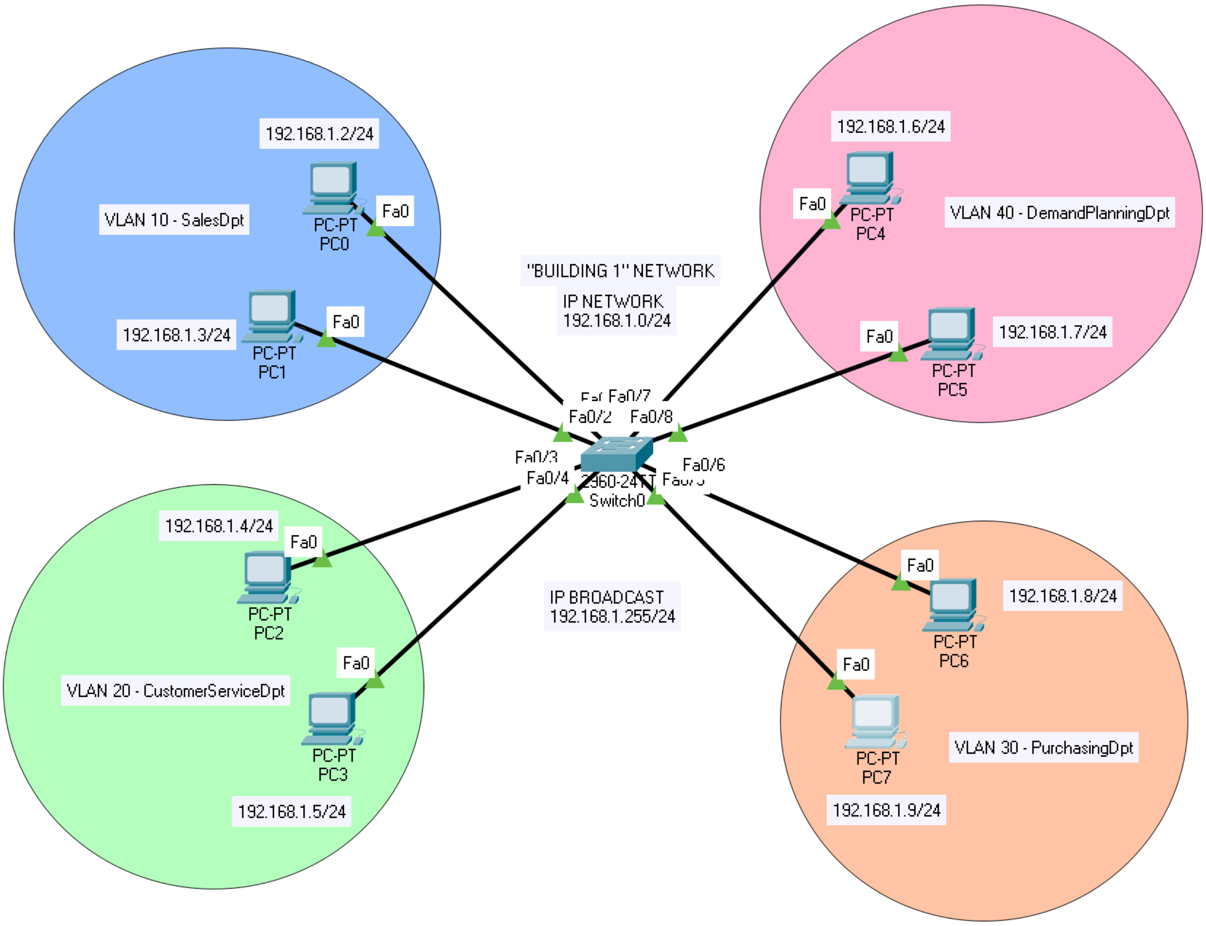
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.9

Pinging 192.168.1.9 with 32 bytes of data:

Reply from 192.168.1.9: bytes=32 time<1ms TTL=128
Reply from 192.168.1.9: bytes=32 time<1ms TTL=128
Reply from 192.168.1.9: bytes=32 time<1ms TTL=128
Reply from 192.168.1.9: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

It’s important to note that there will be no need for an ARP request anymore as both PCs now know all of the information needed to communicate between each other; in case of a new ping, it will only submit an ICMP request.

Once we established that the connection was set up correctly, we can now move to the second part of the exercise, which is to create a complex network divided in 4 VLANs, each one including 2 devices.

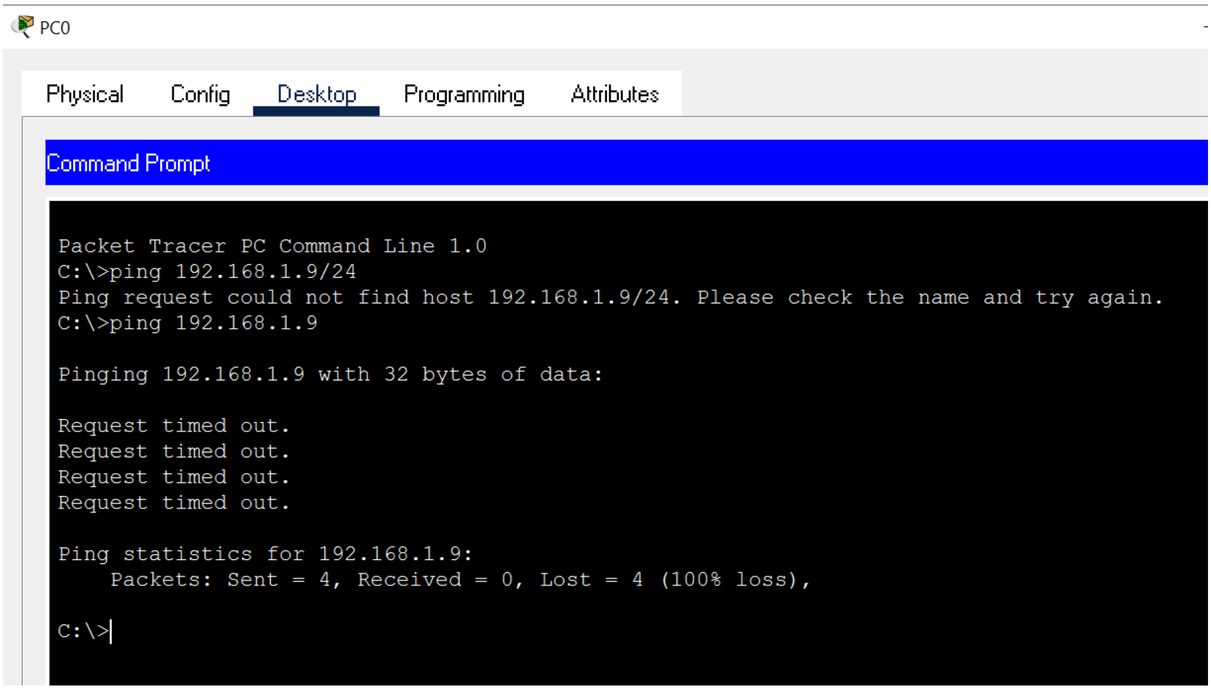
VLANs are usually setup to improve network traffic (as non-pertaining information gets cut-off) and for security (as a potential security breach would be isolated to the single VLAN instead of the whole network); due to this, it makes sense and it's almost always the case that VLANs are used to divide departments/work areas. For ease of understanding, I imagined this setup would be needed by a company to divide in 4 sub-sections one of their buildings' network: inside "**BUILDING 1"** network (**192.168.1.0/24)** we'll have **VLAN10 - SalesDpt, VLAN20 - CustomerServiceDpt, VLAN30 - PurchasingDpt and VLAN40 - DemandPlanningDpt**. All of these departments usually utilize different tools, master files and communications in a work setting, so it would be plausible that a company would need to keep them separated to avoid, for example, conflict of interest between Customer Service and Sales, aside from of course enhancing traffic, privacy and security. After we have a definite plan for the VLANs, we set them up through the switch: we assign FastEthernet0/1 and 2 to VLAN10, FastEthernet0/3 and 4 to VLAN20, FastEthernet0/5 and 6 to VLAN30 and FastEthernet0/7 and 8 to VLAN40.

The following screenshot shows how the network looks after the aforementioned VLAN setup:



To demonstrate the effective isolation provided by the VLAN, we try once again to have **PC0** ping **PC7**, the two devices which did indeed manage to communicate in our previous example. As we expected, the VLAN isolation is working correctly and the setup is working; PC0, now part of the SalesDpt VLAN, can’t reach PC7 which is now in the PurchasingDpt VLAN. The isolation is twofold: the information can’t leave VLAN10 but it also can’t enter VLAN30 from another department, meaning that if we had a device that wasn’t in a VLAN it would still not be able to enter VLAN30. Hereunder the screenshot of the failed ping from PC0 to PC7.

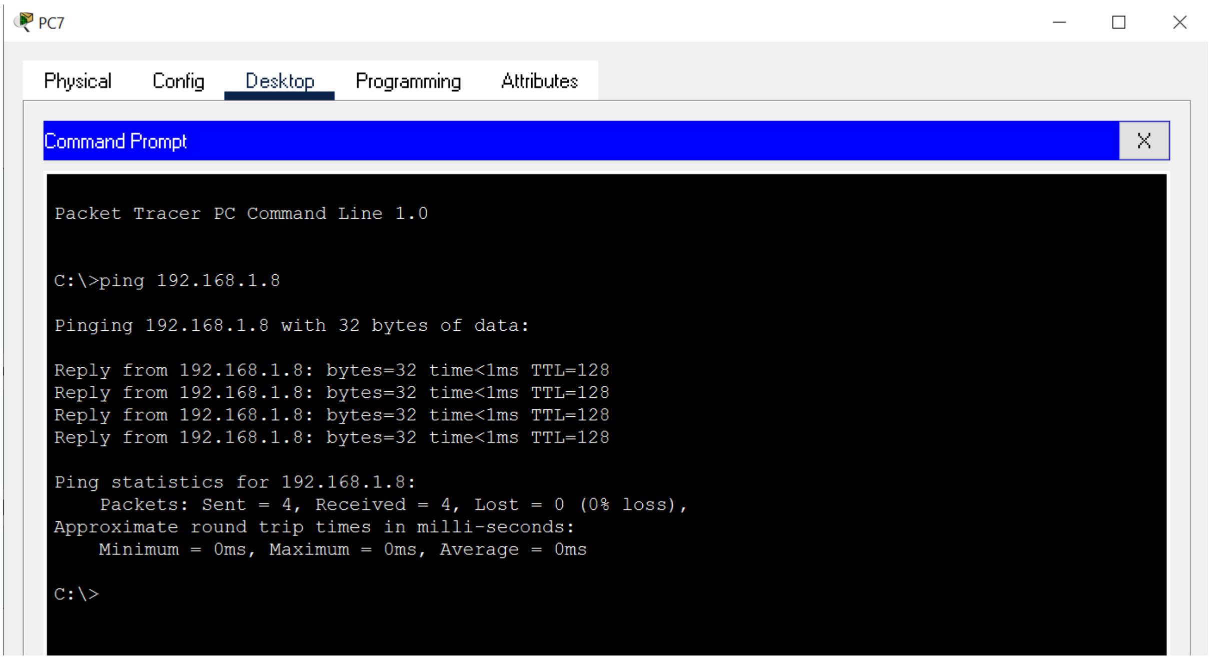
Ping between different clients after VLAN setup, the clients are in different VLANS:



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.9/24
Ping request could not find host 192.168.1.9/24. Please check the name and try again.
C:\>ping 192.168.1.9

Pinging 192.168.1.9 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.9:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Now instead, we need to demonstrate that devices in the same isolated environment can communicate between each other without issues, as that is arguably more important than isolating them from others. We'll use **PC7** and **PC6**(**192.168.1.8/24**), both belonging to **VLAN30 - PurchasingDpt.** As we expected, the devices can indeed communicate between each other, and the ping from PC7 to PC6 is successful, with a 0% loss of packets sent. We can now safely say that the VLAN is set up correctly, both for isolation from other departments and for efficient communication between the desired devices. Hereunder the last ping from PC7 to PC6.

Ping after VLANs setup between two clients belonging to the same VLAN:



```
Packet Tracer PC Command Line 1.0

C:\>ping 192.168.1.8

Pinging 192.168.1.8 with 32 bytes of data:

Reply from 192.168.1.8: bytes=32 time<1ms TTL=128
Reply from 192.168.1.8: bytes=32 time<1ms TTL=128
Reply from 192.168.1.8: bytes=32 time<1ms TTL=128
Reply from 192.168.1.8: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

We have this way respected all three aspects of the CIA model as well:

- confidentiality, as only authorized personnel will have access to the information isolated in the VLAN
- integrity, as all of the information was relayed correctly with 0 packets lost
- accessibility, as all of the devices inside of the VLAN are able to communicate information freely