Practical 2
Configuring LAN setup

Aim:

a) Planning and Setting IP networks
b) Configuring subnet
c) Study of basic network command and Network configuration commands. ipconfig, netstat, ARP, ping, trace route etc.
d) Basic network troubleshooting.
e) Configuration of TCP/IP Protocols in Windows / Linux.
f) Implementation of Drive/file sharing and printer sharing.

Part a) Planning and Setting IP networks

Planning and setting up IP networks involves several key steps and considerations to ensure a reliable, scalable, and secure infrastructure.

Following points are needed to be considered:

1) Define Network Requirements:
   We start by understanding the needs of the organization or project. Identify the number of devices to be connected, the expected network traffic, geographical locations, security requirements, and any future expansion plans.
2) Choose IP Addressing Scheme:
   Decide on the IP addressing scheme we would use, whether it's IPv4 or IPv6. For IPv4, we need to choose a private IP address range and ensure it doesn't conflict with any existing networks we might connect with.
3) Design Network Topology:
   Determine the network's physical layout and logical topology. Consider factors like the number and location of switches, routers, subnets, and how devices will connect to each other. This design should align with requirements and accommodate potential growth.
4) Subnetting:
   Divide IP address space into smaller subnets to help manage network traffic efficiently and improve security. Subnetting also enables us to isolate different departments or devices based on their functions.
5) Choose Network Equipment:
   Select routers, switches, firewalls, and other network equipment based on the network's size, expected traffic load, and the specific features and capabilities needed to meet our requirements.
6) IP Address Assignment:
   Decide how IP addresses will be assigned to devices. This can be done manually (static IP) for critical devices and servers, or dynamically (DHCP) for less critical devices. DHCP automates IP address assignment and makes it easier to manage larger networks.
7) Configure Network Devices:
   Set up the routers, switches, and firewalls based on the network design. Configure routing protocols, VLANs (if necessary), security policies, Quality of Service (QoS) settings, and any other required features.
8) Implement Network Security:
   Security is crucial in any network. Set up firewalls, intrusion prevention systems (IPS), and other security measures to protect against unauthorized access and potential threats. Regularly update firmware and keep security patches up to date.

9) Testing and Troubleshooting:
Before deploying the network in a production environment, conduct thorough testing to identify and resolve any configuration issues or performance bottlenecks. Verify connectivity, test for any security vulnerabilities, and ensure proper functioning of all network services.
10) Documentation:
Document the entire network setup, including IP addresses, subnet masks, network diagrams, device configurations, security settings, and any other relevant information. This documentation will be valuable for future troubleshooting, maintenance, and upgrades.
11) Monitoring and Maintenance:
Implement network monitoring tools to keep an eye on the network's health and performance. Regularly monitor for any anomalies, assess network usage patterns, and perform necessary maintenance tasks like updating firmware, renewing SSL certificates, and checking for security updates.
12) Network Scalability:
Plan for future growth and scalability. As the network expands, we must be ensured it can accommodate additional devices and increased traffic without major disruptions.

We do the following case-study in this respect

Consider a small business called "Smile Info-solution Inc.," which provides IT services to local businesses in their city. They need to plan and set up an IP network for their office to support their internal operations and offer IT services to their clients.

1. Define Network Requirements: Smile Info-solution Inc. has 30 employees, including 20 desktop computers, 10 laptops, 5 network printers, and a file server. They also want to set up a guest Wi-Fi network for visiting clients.

2. Choose IP Addressing Scheme: They decide to use IPv4 for their network and choose the private IP address range 192.168.1.0/24 for their internal devices. They'll use DHCP to assign IP addresses dynamically to employee devices and printers.

3. Design Network Topology: They plan to use a star topology for their office network. The main switch will connect to all the desktop computers, printers, and the file server, while a separate wireless access point will handle the guest Wi-Fi network.

4. Subnetting: They divide the IP address range into two subnets: one for employee devices (192.168.1.0/25) and one for the guest Wi-Fi network (192.168.1.128/26).

5. Choose Network Equipment: Smile Info-solution Inc. selects a business-grade router, a managed switch, and a wireless access point that supports VLANs to separate employee and guest networks.

6. IP Address Assignment: They configure DHCP on the router to assign IP addresses to employee devices and printers in the range 192.168.1.2 to 192.168.1.126. The guest Wi-Fi network will use DHCP for IP addresses from the range 192.168.1.130 to 192.168.1.190.

7. Configure Network Devices: They set up the router with appropriate routing protocols, firewall rules, and port forwarding to secure the network and allow remote access for their clients' devices when needed. The switch is configured with VLANs to segregate traffic from the two networks.

8. Implement Network Security: Smile Info-solution Inc. implements security measures like WPA2 encryption for the Wi-Fi network, access control lists (ACLs) on the router to control traffic flow, and enables firewall rules to protect sensitive data on their server.

9. Testing and Troubleshooting: Before deploying the network, they conduct testing to ensure proper connectivity, DHCP functionality, and network security. They troubleshoot and resolve any issues found during the testing phase.

10. Documentation: They document the network setup, including IP address allocations, network diagrams, device configurations, and security settings for future reference.

11. Monitoring and Maintenance: Smile Info-solution Inc. implements network monitoring tools to keep track of network performance and security. They perform regular maintenance tasks, such as updating firmware and reviewing logs for security incidents.

12. Network Scalability: They plan for potential expansion by leaving room for more devices on the employee subnet and guest Wi-Fi subnet, and ensuring the router and switch have capacity for additional connections.

With their IP network set up, Smile Info-solution Inc. can efficiently provide IT services to their clients and support their internal operations with a secure and scalable network infrastructure.

Part b) Configuring subnet

In order to configure a subnet, we consider the following example.
A company iSmile has 16 PCs connected in a single network, the company plans to create 4 Subnets each containing 4 PCs

To create four subnetworks, each with four PCs, we can use subnetting to divide the organization's network into smaller segments. We will use a Class C IP address range for this example, as it provides 256 IP addresses in total (ranging from 192.168.0.0 to 192.168.0.255).

First, let's find the subnet mask that allows for four subnets. Since 2^2 = 4, we need 2 bits for subnetting (2^2 = 4). The remaining 6 bits will be used for host addresses (2^6 = 64 - 2 reserved for network and broadcast addresses = 62 usable host addresses).
Subnet Mask: 255.255.255.192 (/26 in CIDR notation)
(26 bits for subnet + host, with 26 bits being 1111 1111 1111 1111 1111 1111 1100 0000)

Now, let's assign the IP addresses to each subnet:
Subnet 1:
Usable IP Range: 192.168.0.1 to 192.168.0.62
Network Address: 192.168.0.0
Broadcast Address: 192.168.0.63
Assigned IP Addresses:

PC1	192.168.0.2
PC2	192.168.0.3
PC3	192.168.0.4
PC4	192.168.0.5

Remaining addresses are not assigned

Subnet 2:
Usable IP Range: 192.168.0.65 to 192.168.0.126
Network Address: 192.168.0.64
Broadcast Address: 192.168.0.127.
Assigned IP Addresses:

PC1	192.168.0.65
PC2	192.168.0.66
PC3	192.168.0.67
PC4	192.168.0.68

Remaining addresses are not assigned

Subnet 3:
Usable IP Range: 192.168.0.129 to 192.168.0.190
Network Address: 192.168.0.128
Broadcast Address: 192.168.0.191
Assigned IP Addresses:

PC1	192.168.0.129
PC2	192.168.0.130
PC3	192.168.0.131
PC4	192.168.0.132

Remaining addresses are not assigned

Subnet 4:
Usable IP Range: 192.168.0.193 to 192.168.0.254
Network Address: 192.168.0.192
Broadcast Address: 192.168.0.255
Assigned IP Addresses:

PC1	192.168.0.193
PC2	192.168.0.194
PC3	192.168.0.195
PC4	192.168.0.196

Remaining addresses are not assigned

Each subnet will have its own unique range of IP addresses, with 4 usable addresses for PCs (since there are only 4 PCs in each subnet). The remaining addresses in each subnet are reserved for the network address and broadcast address.

Part c) Study of basic network command and Network configuration commands

1) **arp** : This diagnostic command displays and modifies the IP-to-Ethernetor Token Ring physical address translation tables used by the Address Resolution Protocol (ARP).

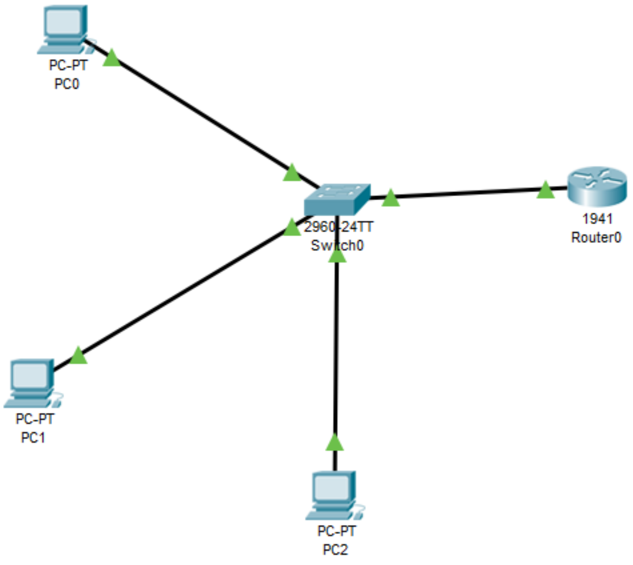
2) **ipconfig:**

   This diagnostic command displays all current TCP/IP network configuration values. This command is useful on computers running DHCP because it enables users to determine which TCP/IP configuration values have been configured by DHCP. If you enter only ipconfig without parameters, the response is a display of all of the current TCP/IP configuration values, including IP address, subnet mask,and default gateway.

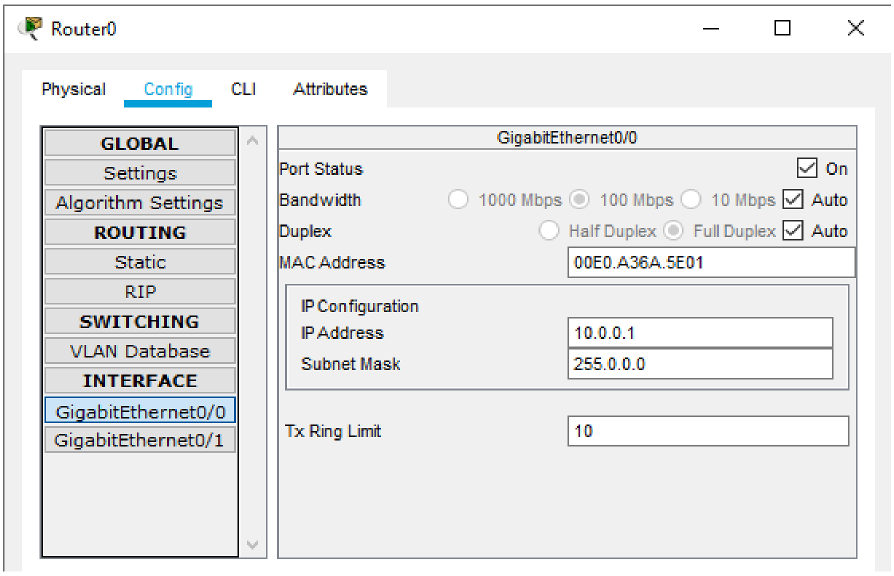
3) **ping:** This diagnostic command verifies connections to one or more remote computers.

4) **tracert:**
   This diagnostic utility determines the route taken to a destination by sending Internet Control Message Protocol (ICMP) echo packets with varying time-to-live (TTL) values to the destination.

We use the following example to demonstrate the use of the commands discussed in the previous sections



Configure the Router 0:



GigabitEthernet0/0

Port Status ☑ On

Bandwidth ○ 1000 Mbps ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 00E0.A36A.5E01

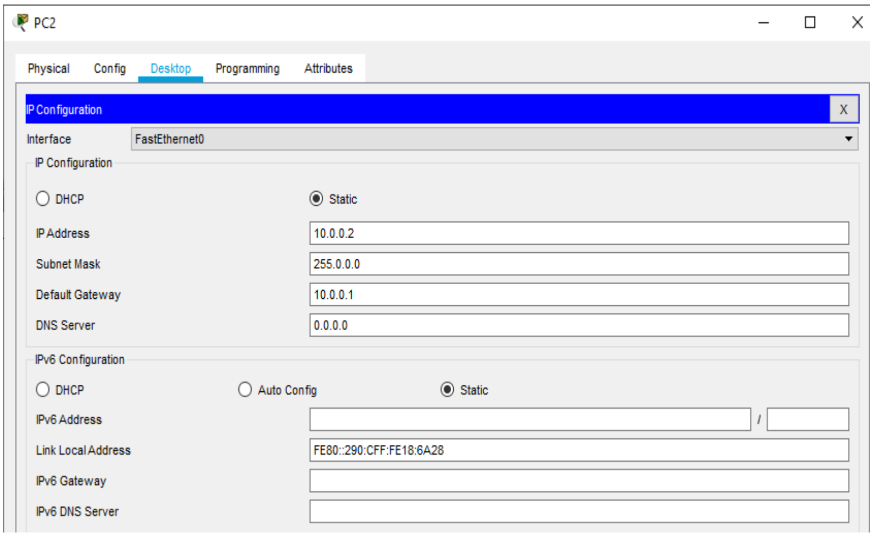
IP Configuration

IP Address 10.0.0.1

Subnet Mask 255.0.0.0

Tx Ring Limit 10

Configure PC2:



IP Configuration

Interface FastEthernet0

IP Configuration

○ DHCP ● Static

IP Address 10.0.0.2

Subnet Mask 255.0.0.0

Default Gateway 10.0.0.1

DNS Server 0.0.0.0

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

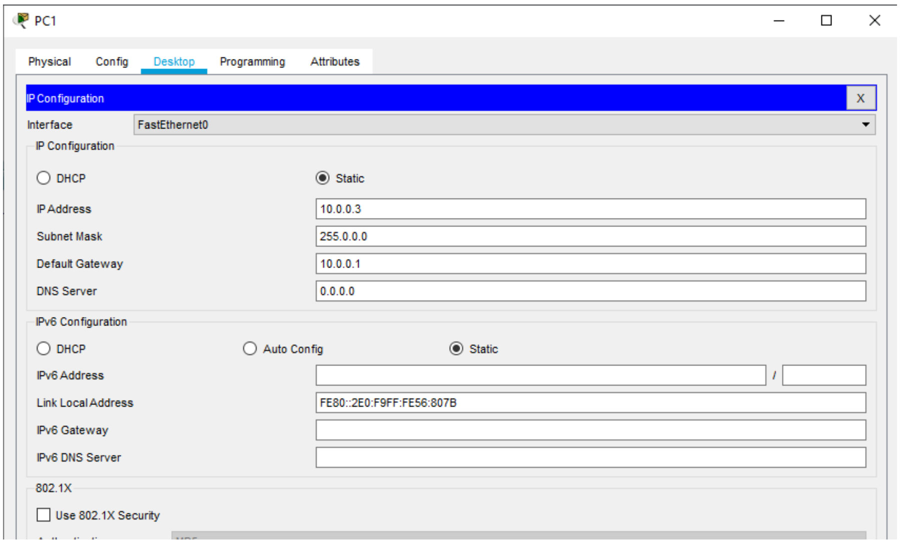
IPv6 Address /

Link Local Address FE80::290:CFF:FE18:6A28

IPv6 Gateway

IPv6 DNS Server

Configure PC1:



IP Configuration

Interface FastEthernet0

IP Configuration

○ DHCP ● Static

IP Address 10.0.0.3

Subnet Mask 255.0.0.0

Default Gateway 10.0.0.1

DNS Server 0.0.0.0

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address /

Link Local Address FE80::2E0:F9FF:FE56:807B

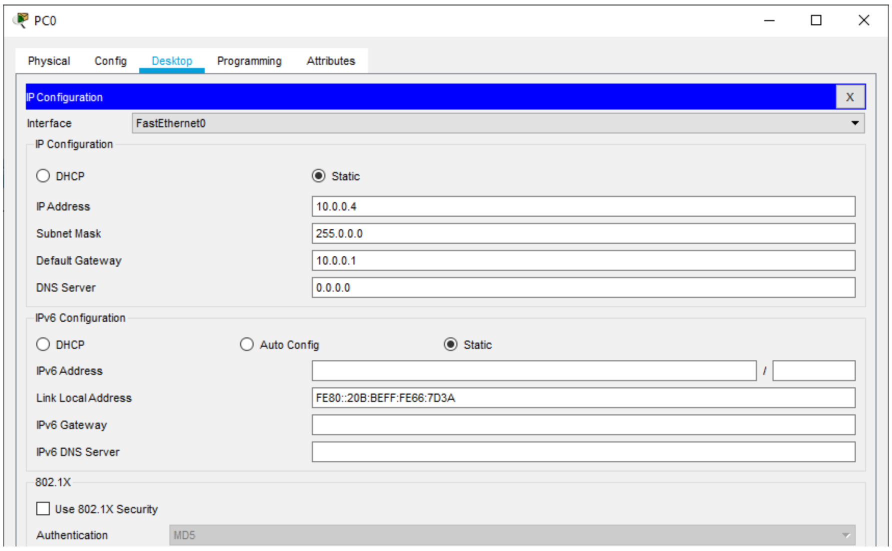
IPv6 Gateway

IPv6 DNS Server

802.1X

□ Use 802.1X Security

Configure PC0:



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IP Address: 10.0.0.4

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address: /

Link Local Address: FE80::20B:BEFF:FE66:7D3A

IPv6 Gateway:

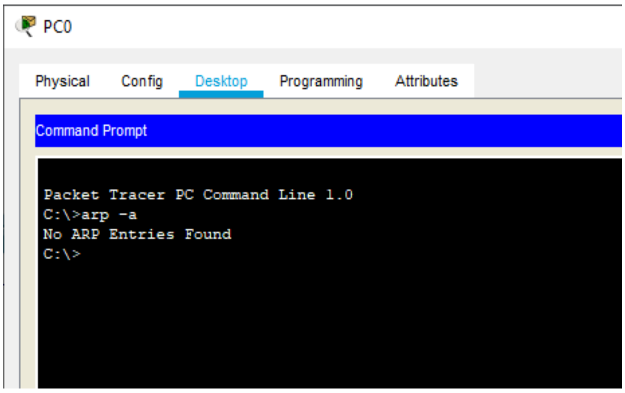
IPv6 DNS Server:

802.1X

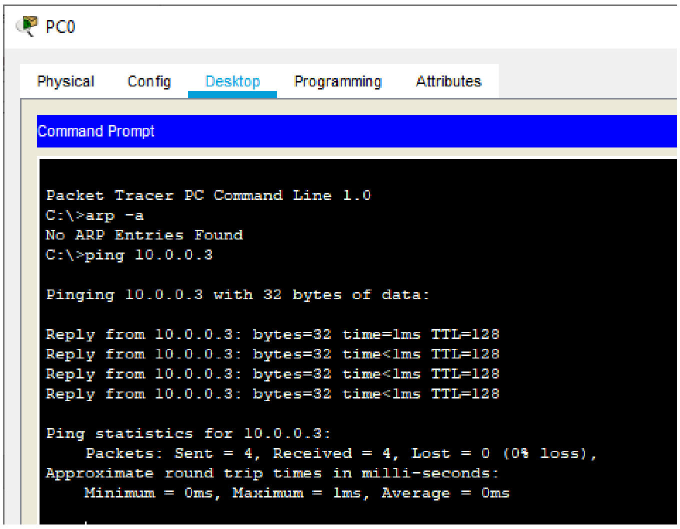
□ Use 802.1X Security

Authentication: MD5

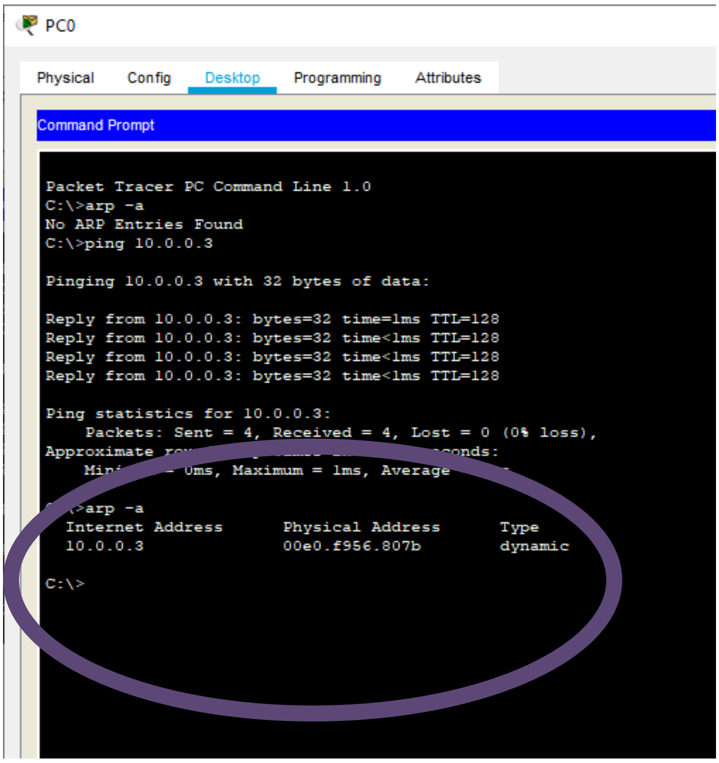
Next, we type the following commands in PC0



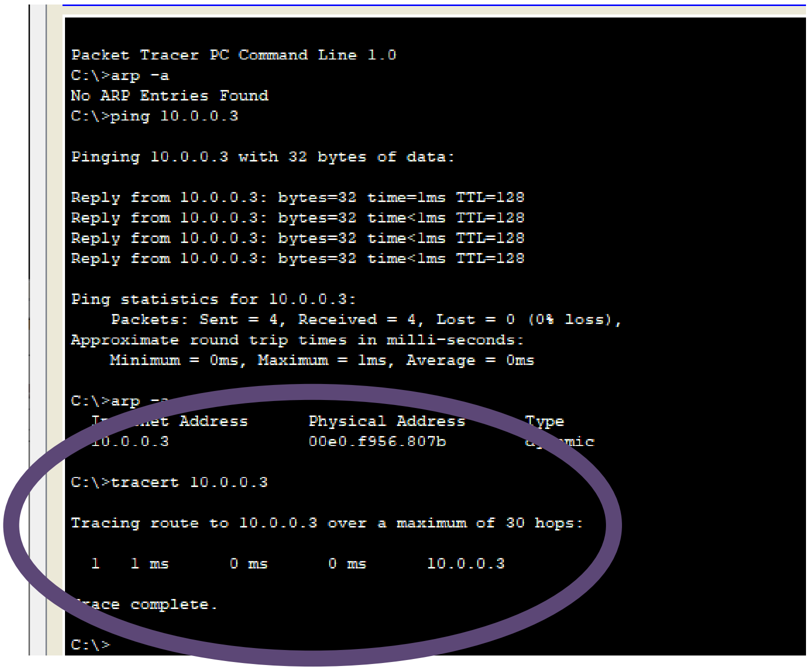
```
Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>
```



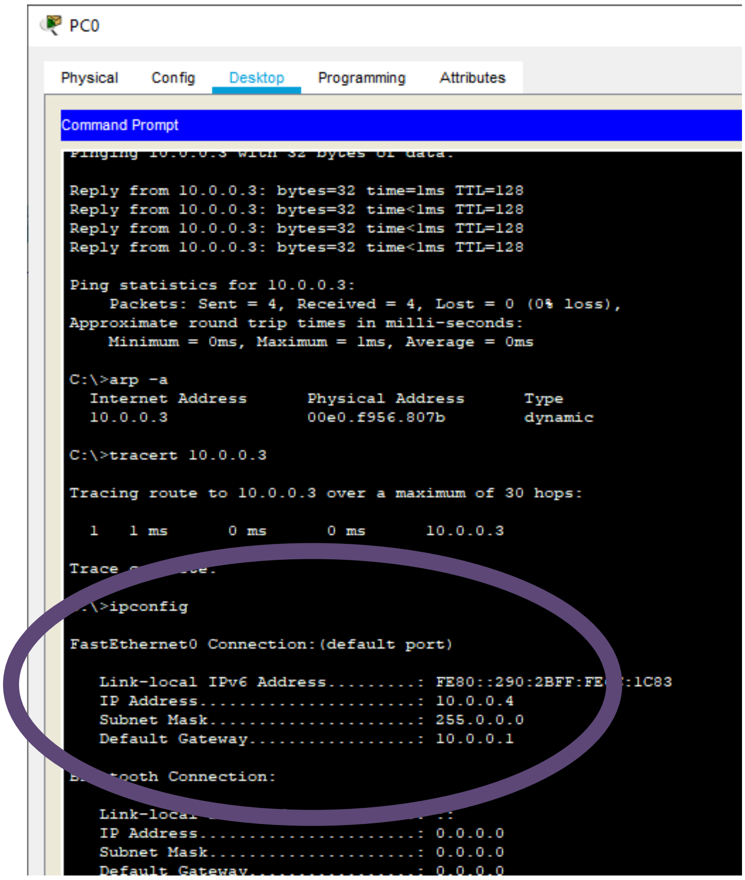
```
Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>ping 10.0.0.3

Pinging 10.0.0.3 with 32 bytes of data:

Reply from 10.0.0.3: bytes=32 time=1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```



```
Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>ping 10.0.0.3

Pinging 10.0.0.3 with 32 bytes of data:

Reply from 10.0.0.3: bytes=32 time=1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>arp -a
  Internet Address      Physical Address      Type
  10.0.0.3              00e0.f956.807b        dynamic

C:\>
```



```
Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>ping 10.0.0.3

Pinging 10.0.0.3 with 32 bytes of data:

Reply from 10.0.0.3: bytes=32 time=1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>arp -a
  Internet Address      Physical Address      Type
  10.0.0.3              00e0.f956.807b        dynamic

C:\>tracert 10.0.0.3

Tracing route to 10.0.0.3 over a maximum of 30 hops:

  1   1 ms      0 ms      0 ms      10.0.0.3

Trace complete.

C:\>
```



```
Pinging 10.0.0.3 with 32 bytes of data:

Reply from 10.0.0.3: bytes=32 time=1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>arp -a
  Internet Address      Physical Address      Type
  10.0.0.3              00e0.f956.807b        dynamic

C:\>tracert 10.0.0.3

Tracing route to 10.0.0.3 over a maximum of 30 hops:

  1   1 ms      0 ms      0 ms      10.0.0.3

Trace complete.

C:\>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::290:2BFF:FE[illegible]:1C83
   IP Address......................: 10.0.0.4
   Subnet Mask.....................: 255.0.0.0
   Default Gateway.................: 10.0.0.1

Bluetooth Connection:

   Link-local IPv6 Address.........: ::
   IP Address......................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: 0.0.0.0
```

For the video demonstration of the above practical scan the QR code

Part d) Basic Network Troubleshooting

Basic network troubleshooting refers to the process of identifying and resolving common issues that can arise in a computer network. Following are some essential steps and techniques for basic network troubleshooting:

a) **Identify the Problem:** Start by gathering information from the user or by observing the issue yourself. Understand what specific problem the user is facing, such as no internet access, slow connection, or inability to access certain resources.

b) **Check Physical Connections:** Ensure all network cables are securely plugged in, and network devices like routers, switches, and modems have power and functioning indicators.

c) **Restart Devices:** Sometimes, network issues can be resolved by simply restarting the network devices. Power cycle the router, modem, and any other network equipment to see if it resolves the problem.

d) **Check Network Configurations:** Verify the network settings on the computer or device experiencing the issue. Look for correct IP configurations, subnet masks, gateway addresses, and DNS server settings.

e) **Ping Test:** Use the ping command to check the connectivity between the computer and other devices on the network or the internet. For example, try pinging the router, another computer on the network, or an external website.

f) **Check for IP Conflicts**: Ensure that there are no IP address conflicts on the network. Two devices with the same IP address can cause communication problems.

g) **Firewall and Security Software**: Temporarily disable any firewall or security software to check if they are blocking network access.

h) **Update Network Drivers:** Ensure that the network interface card (NIC) drivers are up to date. Outdated drivers can lead to connectivity issues.

i) **Test Different Devices:** If possible, try connecting the problematic device to a different network or connecting a different device to the same network to see if the issue persists.

j) **Check Router and DHCP:** Verify that the router is functioning correctly and that the DHCP server is assigning IP addresses to devices on the network.

k) **Trace Route:** Use the tracert (Windows) or traceroute (macOS and Linux) command to trace the path from your computer to a remote server or website. This can help identify network hops where there might be an issue.

l) **Check for Network Outages:** Check with your Internet Service Provider (ISP) or network administrator to see if there are any known network outages or maintenance activities in your area.

m) **Use Network Troubleshooting Tools:** Network troubleshooting tools like ipconfig, ifconfig, nslookup, and netstat can provide valuable information about network configurations and connections.

n) **Check Physical Environment:** Ensure that there are no physical obstructions or interference (e.g., walls, microwave ovens) that could affect wireless network connectivity.

Part e) Configuration of TCP/IP Protocols in Windows / Linux

Configuring TCP/IP protocols in Windows involves setting up IP addresses, subnet masks, default gateways, and DNS server addresses.
Following steps guide us to configuring TCP/IP protocols on a Windows computer:

a) Open Network Connections: Press the Windows key + R to open the Run dialog, then type ncpa.cpl and hit Enter. This will open the "Network Connections" window.

b) Select Network Adapter: Identify the network adapter you want to configure (e.g., Ethernet or Wi-Fi). Right-click on it and select "Properties."

c) Choose Internet Protocol Version 4 (TCP/IPv4): In the "Properties" window, scroll down the list of items to find "Internet Protocol Version 4 (TCP/IPv4)." Select it and click on the "Properties" button.

d) Configure IP Address Settings:
To use a dynamic (automatic) IP address, choose the option "Obtain an IP address automatically" and "Obtain DNS server address automatically." This is usually the setting for home networks and networks with a DHCP server.
To use a static IP address, choose the option "Use the following IP address" and enter the desired IP address, subnet mask, default gateway, and preferred/alternate DNS server addresses manually. This is common for servers or when using a specific network configuration.

e) Configure Advanced IP Settings (optional):
Click on the "Advanced" button to configure additional settings.
In the "IP Settings" tab, you can add multiple IP addresses (if needed) by clicking on "Add" and specifying the address and subnet mask.
In the "DNS" tab, you can configure DNS suffixes and register connections in DNS, among other options.
The "WINS" tab is typically not required for modern networks, as WINS (Windows Internet Name Service) is used for older Windows networking.

f) Internet Protocol Version 6 (TCP/IPv6) (optional):
You can also configure IPv6 settings in a similar manner by selecting "Internet Protocol Version 6 (TCP/IPv6)" and clicking on the "Properties" button.
The default setting is usually "Obtain an IPv6 address automatically," but you can choose "Use the following IPv6 address" to enter a static IPv6 address manually.

g) Confirm and Apply Changes: Once you've made the necessary configurations, click "OK" to save the changes and close the properties window.

h) Verify Connectivity: After configuring TCP/IP protocols, test the network connectivity to ensure everything is working correctly. Try accessing websites, ping other devices on the network, or use other network-based applications to confirm that the changes have been successful.

Remember that changing network settings can disrupt your network connection temporarily. If you encounter any issues or lose connectivity, you can revert to the previous settings or use the "Obtain an IP address automatically" option to obtain settings from a DHCP server, if available.

Part f) Networks Implementation of Drive/file sharing and printer sharing

Implementing drive/file sharing and printer sharing in a network allows multiple users to access shared files and use shared printers efficiently. These features can be set up on both small local networks (e.g., home networks) and larger corporate networks.
Implementing drive/file sharing and printer sharing in a Windows-based network as follows:

Set Up File Sharing:
File sharing allows users to access files and folders stored on a central server or on individual computers across the network.

Step 1: Share Folders:
Right-click on the folder you want to share and select "Properties."
In the Properties window, go to the "Sharing" tab.
Click on "Advanced Sharing" and check the box for "Share this folder."
Assign a Share Name (also known as a "Share Name" or "Share Path") that other users will use to access the shared folder.
You can set permissions to control who can access the folder and what level of access they have (read-only, read/write, etc.).

Step 2: Access Shared Folders:
Open File Explorer on another computer connected to the network.
In the address bar, type \\<IP address or computer name of the shared folder> and press Enter.
You should see a list of shared folders on that computer. Double-click on the folder you want to access and enter the appropriate credentials if required.

Set Up Printer Sharing:
Printer sharing allows multiple users to print to a single printer connected to a computer on the network.

Step 1: Share the Printer:
Connect the printer to the computer you want to use as a print server (the computer that will share the printer).
Open the Control Panel and go to "Devices and Printers."
Right-click on the printer you want to share and select "Printer properties."
In the properties window, go to the "Sharing" tab.
Check the box for "Share this printer" and provide a Share Name for the printer.

Step 2: Connect to the Shared Printer:
On other computers connected to the network, open the Control Panel and go to "Devices and Printers."
Click on "Add a printer" and then select "Add a network, wireless, or Bluetooth printer."
The shared printer should appear in the list. Select it and follow the on-screen instructions to install the printer driver and connect to the shared printer.