Computer Networks Practical
B. Sc. (Information Technology) Semester – III

By munotes.in

Updated 2023

Mumbai University

1. IPv4 Addressing and Subnetting

a) Given an IP address and network mask, determine other information about the
IP addresssuch as:

- **Network address**
- **Network broadcast address**
- **Total number of host bits**
- **Number of hosts**

Solution

To determine additional information about an IP address given the network mask, such as the network broadcast address, total number of host bits, and number of hosts, you can follow these steps:

1. Write down the IP address and network mask in binary format. Both the IP address and network mask are 32-bit binary numbers.

2. Determine the network address using the steps mentioned in the previous response.

3. Calculate the network broadcast address by performing a bitwise "OR" operation on the network address and the inverted network mask. This operation involves comparing each corresponding bit of the network address and inverted network mask and setting the result to 1 only if either of the bits is 1. Otherwise, the result is set to 0.

4. Count the number of host bits by subtracting the number of network bits from the total number of bits (32). The network bits are determined by counting the consecutive 1s in the network mask.

5. Calculate the number of hosts by raising 2 to the power of the number of host bits and subtracting 2. The subtraction of 2 is because the network

address and the network broadcast address cannot be used as host addresses.

Let's use an example to illustrate these steps:

Example:
IP address: 192.168.1.100
Network mask: 255.255.255.0

1. Convert the IP address and network mask to binary format:
IP address: 11000000.10101000.00000001.01100100
Network mask: 11111111.11111111.11111111.00000000

2. Determine the network address using the steps described earlier:
Network address: 192.168.1.0

3. Perform a bitwise "OR" operation to calculate the network broadcast address:
Network address: 11000000.10101000.00000001.00000000
OR
Inverted network mask: 00000000.00000000.00000000.11111111
=
Network broadcast address: 11000000.10101000.00000001.11111111 (192.168.1.255)

4. Count the number of host bits:
Number of network bits: 24 (determined by counting the consecutive 1s in the network mask)
Total number of bits: 32
Number of host bits: 32 - 24 = 8

5. Calculate the number of hosts:
Number of host addresses: 2^8 - 2 = 254

Therefore, for the given IP address and network mask, the additional information is as follows:
- Network address: 192.168.1.0
- Network broadcast address: 192.168.1.255
- Total number of host bits: 8
- Number of hosts: 254

b) Given an IP address and network mask, determine other information about the
IP addresssuch as:
• The subnet address of this subnet
• The broadcast address of this subnet
• The range of host addresses for this subnet
• The maximum number of subnets for this subnet mask
• The number of hosts for each subnet
• The number of subnet bits
• The number of this subnet

Solution

To determine the additional information about an IP address and network mask, such as the subnet address, broadcast address, range of host addresses, maximum number of subnets, number of hosts per subnet, number of subnet bits, and the number of the subnet, you can follow these steps:

1. Write down the IP address and network mask in binary format. Both the IP address and network mask are 32-bit binary numbers.

2. Determine the network address using the steps mentioned earlier.

3. Calculate the subnet address of this subnet by performing a bitwise "AND" operation on the IP address and the network mask. This will give you the subnet address of the network to which the IP address belongs.

4. Calculate the broadcast address of this subnet by performing a bitwise "OR" operation on the subnet address and the inverted network mask. This will give you the broadcast address of the subnet.

5. Determine the range of host addresses for this subnet by excluding the network address and broadcast address. The range will include all the addresses in between.

6. Calculate the maximum number of subnets for this subnet mask by raising 2 to the power of the number of subnet bits. The subnet bits are determined by counting the consecutive 0s in the network mask.

7. Calculate the number of hosts for each subnet by raising 2 to the power of the number of host bits and subtracting 2. The subtraction of 2 is because the network address and the broadcast address cannot be used as host addresses.

8. Determine the number of subnet bits by counting the consecutive 0s in the network mask.

9. Calculate the number of this subnet by performing a bitwise "AND" operation on the IP address and the inverted network mask, and then converting the result to decimal format.

Let's use an example to illustrate these steps:

Example:
IP address: 192.168.1.100
Network mask: 255.255.255.0

1. Convert the IP address and network mask to binary format:
IP address: 11000000.10101000.00000001.01100100
Network mask: 11111111.11111111.11111111.00000000

2. Determine the network address using the steps described earlier:
Network address: 192.168.1.0

3. Perform a bitwise "AND" operation to calculate the subnet address of this subnet:
IP address: 11000000.10101000.00000001.01100100
AND
Network mask: 11111111.11111111.11111111.00000000
=
Subnet address: 192.168.1.0

4. Perform a bitwise "OR" operation to calculate the broadcast address of this subnet:
Subnet address: 11000000.10101000.00000001.00000000
OR
Inverted network mask: 00000000.00000000.00000000.11111111
=
Broadcast address: 11000000.10101000.00000001.11111111 (192.168.1.255)

5. Determine the range of host addresses for this subnet:
Range: 192.168.1.1 - 192.168.1.254

6. Calculate the maximum number of subnets for this subnet mask:
Number of subnet bits: 8 (determined by counting the consecutive 0s in the network mask)
Maximum number of subnets: 2^8 = 256

7. Calculate the number of hosts for each subnet:
Number of host addresses: 2^8 - 2 = 254

8. Determine the number of subnet bits:
Number of subnet bits: 8 (determined by counting the consecutive 0s in the network mask)

9. Calculate the number of this subnet:
Number of this subnet: (IP address AND inverted network mask) converted to decimal format

For example, if the IP address is 192.168.1.100 and the network mask is 255.255.255.0:
IP address: 11000000.10101000.00000001.01100100
Inverted network mask: 00000000.00000000.00000000.11111111
Result of bitwise "AND" operation:
00000000.00000000.00000000.01100100 (0.0.0.100)

Therefore, for the given IP address and network mask, the additional information is as follows:
- Subnet address of this subnet: 192.168.1.0
- Broadcast address of this subnet: 192.168.1.255
- Range of host addresses for this subnet: 192.168.1.1 - 192.168.1.254
- Maximum number of subnets for this subnet mask: 256
- Number of hosts for each subnet: 254
- Number of subnet bits: 8
- Number of this subnet: 0.0.0.100

2. Use of ping and tracert / traceroute, ipconfig / ifconfig, route and arp utilities.

Solution

The utilities you mentioned, such as ping, tracert (or traceroute), ipconfig (or ifconfig), route, and arp, are commonly used networking tools to troubleshoot and gather information about network connections. Here's a brief overview of each utility and its typical usage:

1. Ping:
Ping is a utility used to test network connectivity between two devices. It sends ICMP Echo Request messages to a target IP address or hostname and measures the round-trip time (RTT) for the ICMP Echo Reply. Ping is commonly used to check if a host is reachable and to measure network latency.

Usage: `ping [IP address or hostname]`

2. Tracert / Traceroute:
Tracert (Windows) or traceroute (Linux/Unix) is a utility used to trace the route packets take from your device to a destination device or server. It shows the IP addresses of intermediate routers or hops along the path, helping diagnose network connectivity issues.

Usage: `tracert [IP address or hostname]` or `traceroute [IP address or hostname]`

3. Ipconfig / Ifconfig:
Ipconfig (Windows) or ifconfig (Linux/Unix) is used to display and configure IP network interfaces on your device. It provides information such as IP addresses, subnet masks, default gateways, and more. Ipconfig/ifconfig is useful for troubleshooting network configuration issues and verifying network settings.

Usage:
- Windows: `ipconfig` or `ipconfig /all` (detailed information)
- Linux/Unix: `ifconfig` or `ifconfig -a` (all interfaces)

4. Route:
The route utility is used to view and manipulate the IP routing table on your device. It displays the routing information, including the destination network, gateway, netmask, and interface. Route is useful for troubleshooting routing issues and managing network routes manually.

Usage:
- Windows: `route print`
- Linux/Unix: `route -n` or `ip route show`

5. Arp:
Arp (Address Resolution Protocol) is a utility used to view and manage the ARP cache, which maps IP addresses to MAC addresses on a local network. It displays the IP-MAC mappings stored in the cache and can be used to troubleshoot network connectivity problems related to address resolution.

Usage:
- Windows: `arp -a`
- Linux/Unix: `arp -n`

These utilities play an essential role in network troubleshooting, diagnostics, and configuration. However, the specific usage and available options may vary slightly depending on the operating system and version you're using.

3. Configure IP static routing.

Solution

To configure static IP routing, follow these general steps:

Step 1: Determine the network topology and routing requirements:
- Identify the networks or subnets in your network environment.
- Determine which routers will be responsible for forwarding traffic between these networks.
- Decide on the static routes you need to configure.

Step 2: Access the router's configuration interface:
- Connect to the router's management interface using a web browser or SSH.
- Log in with administrative credentials.

Step 3: Identify the routing table:
- Locate the routing table or routing configuration section in the router's interface.
- This may be under a section called "Routing," "Static Routes," or a similar name.

Step 4: Add static routes:
- Determine the destination network or subnet for which you want to add a static route.
- Identify the next hop or gateway IP address through which the router should forward traffic to reach that destination.
- Add the static route using the appropriate command or form in the router's interface.
- Specify the destination network/subnet, the next hop IP address, and any relevant metrics or administrative distances.

Step 5: Verify and test the routing configuration:
- Save the configuration changes.

- Test the connectivity between networks using the static routes.
- Verify that traffic is being routed correctly and that the desired connectivity is established.

Note: The specific steps and commands to configure static routing may vary depending on the router manufacturer, model, and firmware version. It's recommended to refer to the documentation provided by the router manufacturer for detailed instructions on configuring static routes for your specific device.

Additionally, it's important to ensure that the network addressing and subnetting are correctly configured on all devices involved, and that the static routes align with the network topology and addressing scheme.

4. Configure IP routing using RIP.

Solution

To configure IP routing using the Routing Information Protocol (RIP), follow these general steps:

Step 1: Access the router's configuration interface:
- Connect to the router's management interface using a web browser or SSH.
- Log in with administrative credentials.

Step 2: Enable RIP routing:
- Locate the routing configuration section in the router's interface.
- Enable RIP routing protocol.
- Specify the version of RIP to use (RIP v1 or RIP v2).
- Choose the interfaces on which RIP will be enabled.

Step 3: Configure network advertisements:
- Specify the networks or subnets that will be advertised by RIP.
- Assign the appropriate network addresses and subnet masks to the interfaces.
- Enable RIP advertisements for these networks.

Step 4: Set RIP timers and other parameters:
- Configure the RIP timers, such as update and invalid timers.
- Adjust the timers according to your network environment and requirements.
- Set other parameters such as authentication, hop count limits, and split horizon if desired.

Step 5: Verify and test the RIP configuration:
- Save the configuration changes.
- Verify that the router is sending RIP updates and receiving updates from neighboring routers.

- Check the routing table to ensure that RIP routes are being learned and propagated correctly.
- Test the connectivity between networks to verify that RIP is routing traffic properly.

Note: The specific steps and commands to configure RIP may vary depending on the router manufacturer, model, and firmware version. It's recommended to refer to the documentation provided by the router manufacturer for detailed instructions on configuring RIP for your specific device.

Additionally, ensure that all routers participating in RIP routing are configured with the same RIP version and have compatible settings for authentication and other parameters. Proper network addressing, subnetting, and connectivity between routers are also important factors for successful RIP routing.

5. Configuring Simple OSPF.

To configure a simple Open Shortest Path First (OSPF) routing protocol, follow these general steps:

Step 1: Access the router's configuration interface:
- Connect to the router's management interface using a web browser or SSH.
- Log in with administrative credentials.

Step 2: Enable OSPF routing:
- Locate the routing configuration section in the router's interface.
- Enable OSPF routing protocol.
- Specify the OSPF process ID for the router. This ID should be unique within the OSPF routing domain.

Step 3: Configure OSPF areas:
- Identify the networks or subnets that will participate in OSPF routing.
- Determine the OSPF area ID for each network or subnet.
- Assign the appropriate OSPF area IDs to the interfaces connected to these networks.

Step 4: Establish OSPF neighbors:
- Specify the OSPF neighbors or routers with which the router will establish OSPF adjacencies.
- Configure the neighbor statements on the router, specifying the IP addresses of the neighboring routers.

Step 5: Verify and test the OSPF configuration:
- Save the configuration changes.
- Verify that the router is sending OSPF updates and receiving updates from neighboring routers.
- Check the routing table to ensure that OSPF routes are being learned and propagated correctly.

- Test the connectivity between networks to verify that OSPF is routing traffic properly.

Note: The specific steps and commands to configure OSPF may vary depending on the router manufacturer, model, and firmware version. It's recommended to refer to the documentation provided by the router manufacturer for detailed instructions on configuring OSPF for your specific device.

Additionally, ensure that all routers participating in OSPF have compatible OSPF settings, including OSPF area IDs, OSPF process ID, network addresses, and subnet masks. Proper network connectivity between routers and correct configuration of OSPF interfaces and neighbor relationships are also essential for successful OSPF routing.

6. Configuring DHCP server and client.

Solution

To configure a DHCP server and client, follow these general steps:

Configuring a DHCP Server:

Step 1: Access the DHCP server's configuration interface:
- Connect to the DHCP server's management interface using a web browser or SSH.
- Log in with administrative credentials.

Step 2: Enable DHCP service:
- Locate the DHCP configuration section in the server's interface.
- Enable the DHCP service.

Step 3: Configure DHCP settings:
- Specify the range of IP addresses to be leased by the DHCP server.
- Set the subnet mask, default gateway, and DNS server addresses to be assigned to the DHCP clients.
- Define other DHCP options, such as domain name, lease duration, and any additional settings as required.

Step 4: Save and activate the DHCP configuration:
- Save the configuration changes on the DHCP server.
- Activate the DHCP service.

Configuring a DHCP Client:

Step 1: Access the DHCP client's configuration interface:
- Connect to the DHCP client's management interface using a web browser or SSH.
- Log in with administrative credentials.

Step 2: Configure DHCP client settings:
- Locate the network configuration section in the client's interface.
- Set the network interface to obtain an IP address automatically (DHCP client mode).
- Ensure that the client's network interface is enabled.

Step 3: Save and apply the DHCP client configuration:
- Save the configuration changes on the DHCP client.
- Apply the changes to the network interface.

Step 4: Verify DHCP lease:
- Check the network interface settings on the DHCP client.
- Verify that the client has obtained an IP address, subnet mask, default gateway, and DNS server addresses from the DHCP server.

Note: The specific steps and commands to configure a DHCP server and client may vary depending on the operating system and network device you are using. It's recommended to refer to the documentation provided by the device manufacturer for detailed instructions on configuring DHCP for your specific environment.

Additionally, ensure that the DHCP server and client are on the same subnet or connected through a router that can relay DHCP messages. Proper network connectivity and correct configuration of DHCP options (such as IP address ranges, subnet masks, and DNS server addresses) are crucial for successful DHCP operation.

7. Create virtual PC based network using virtualization software and virtual NIC.

Solution

To create a virtual PC-based network using virtualization software and virtual NIC (Network Interface Card), you can follow these general steps:

Step 1: Choose a virtualization software:
- Select a virtualization software that suits your needs. Popular options include VMware Workstation, VirtualBox, and Hyper-V.

Step 2: Install and set up the virtualization software:
- Download and install the chosen virtualization software on your host computer.
- Follow the installation instructions provided by the software vendor.

Step 3: Create virtual machines (VMs):
- Open the virtualization software and create multiple virtual machines.
- Specify the desired operating system for each VM during the creation process.

Step 4: Configure virtual networks:
- In the virtualization software, configure virtual networks to connect the VMs.
- Create virtual switches or network adapters to establish network connectivity between the VMs.

Step 5: Assign virtual NICs to VMs:
- Customize the virtual machine settings and assign virtual NICs to each VM.
- Specify the network adapter type and connect the virtual NICs to the appropriate virtual networks.

Step 6: Install operating systems on VMs:

- Install the desired operating systems on each VM using ISO files or installation media.
- Follow the OS installation process within each VM.

Step 7: Configure IP addressing and network settings:
- Within each VM, configure IP addresses, subnet masks, default gateways, and DNS server settings.
- Set up the network settings based on your desired network topology and requirements.

Step 8: Test network connectivity:
- Power on the VMs and verify network connectivity between them.
- Test connectivity by pinging or accessing resources between the virtual machines.

Note: The specific steps may vary depending on the virtualization software you choose. It's recommended to refer to the documentation provided by the virtualization software vendor for detailed instructions on creating virtual networks and configuring virtual NICs within their software.

By following these steps, you can create a virtual PC-based network using virtualization software and virtual NICs. This allows you to simulate a network environment and test various network configurations without the need for physical hardware.

8. Configuring DNS Server and client.

Solution

To configure a DNS (Domain Name System) server and client, follow these general steps:

Configuring a DNS Server:

Step 1: Choose a DNS server software:
- Select a DNS server software that suits your needs. Popular options include BIND (Berkeley Internet Name Domain), Microsoft DNS Server, and dnsmasq.

Step 2: Install and set up the DNS server:
- Download and install the chosen DNS server software on your server machine.
- Follow the installation instructions provided by the software vendor.

Step 3: Configure DNS zones and records:
- Determine the DNS zones you want to manage. This includes the domain names you wish to resolve.
- Set up zone files for each DNS zone, specifying the resource records (A, CNAME, MX, etc.) for the corresponding domain names.

Step 4: Configure DNS server settings:
- Customize the DNS server configuration file with the necessary settings, such as listening interfaces, forwarders, and caching parameters.
- Specify the authoritative name servers for your domains.

Step 5: Start the DNS server:
- Launch the DNS server software and ensure it starts correctly.
- Monitor the server logs for any potential errors or warnings.

Configuring a DNS Client:

Step 1: Access the client's network configuration:
- Open the network configuration settings on the client machine.
- This can usually be found in the Control Panel or Network Settings on Windows, or the network manager on Linux.

Step 2: Specify DNS server addresses:
- Locate the DNS configuration settings for the network interface.
- Specify the IP addresses of the DNS servers you want the client to use.
- You can enter the IP address of your own DNS server or use public DNS servers like Google DNS (8.8.8.8, 8.8.4.4) or Cloudflare DNS (1.1.1.1, 1.0.0.1).

Step 3: Test DNS resolution:
- Save the network configuration changes on the client machine.
- Open a web browser or use other applications that require DNS resolution to test if the client can resolve domain names correctly.

Step 4: Troubleshoot DNS client issues:
- If DNS resolution is not working correctly, check the client's DNS configuration for any errors or typos.
- Ensure the client has network connectivity to the DNS server.
- Consider clearing DNS caches on the client machine.

Note: The specific steps for configuring a DNS server and client may vary depending on the operating system and DNS server software you are using. It's recommended to refer to the documentation provided by the software vendor for detailed instructions on configuring DNS for your specific environment.

By following these steps, you can configure a DNS server to handle domain name resolution and set up DNS client machines to use the configured DNS server for resolving domain names. This enables efficient and reliable name resolution within your network.

9. Configuring OSPF with multiple areas.

Solution

To configure OSPF (Open Shortest Path First) with multiple areas, follow these general steps:

Step 1: Design the OSPF network topology:
- Identify the different areas in your network. Determine which routers will serve as area border routers (ABRs) and connect multiple areas.
- Plan the OSPF area structure based on your network requirements and hierarchical design principles.

Step 2: Assign OSPF area IDs:
- Assign unique OSPF area IDs to each area in your network.
- Designate one area as the backbone area (Area 0) to which all other areas will connect.

Step 3: Configure OSPF on routers:
- Access the configuration interface of each router participating in OSPF.
- Enable OSPF routing protocol and specify the OSPF process ID.
- Configure the router as an ABR if it connects multiple areas.
- Assign the appropriate OSPF area ID to each router interface connected to an OSPF area.

Step 4: Establish OSPF neighbor relationships:
- Specify the OSPF neighbors or routers with which each router will establish OSPF adjacencies.
- Configure the neighbor statements on each router, specifying the IP addresses of the neighboring routers.

Step 5: Configure OSPF area settings:
- On each ABR, configure the OSPF area settings for the connected areas.
- Designate the backbone area (Area 0) on the ABR.

- Specify the area type (e.g., regular area, stub area, NSSA) for each connected area.

Step 6: Verify and test OSPF configuration:
- Save the configuration changes on each router.
- Verify that the routers are sending OSPF updates and receiving updates from neighboring routers.
- Check the routing table on each router to ensure that OSPF routes are being learned and propagated correctly.
- Test the connectivity between networks in different OSPF areas to verify proper routing.

Note: The specific steps and commands to configure OSPF with multiple areas may vary depending on the router manufacturer, model, and firmware version. It's recommended to refer to the documentation provided by the router manufacturer for detailed instructions on configuring OSPF with multiple areas for your specific device.

Additionally, ensure that all routers participating in OSPF have compatible OSPF settings, including OSPF process ID, OSPF area IDs, OSPF neighbor statements, and OSPF area type configurations. Proper network connectivity between routers and correct configuration of OSPF interfaces, neighbor relationships, and area settings are crucial for successful OSPF operation with multiple areas.

10. Use of Wireshark to scan and check the packet information of following protocols

- **HTTP**
- **ICMP**
- **TCP**
- **SMTP**
- **POP3**

Solution

To use Wireshark to scan and check packet information for the following protocols (HTTP, ICMP, TCP, SMTP, POP3), you can follow these steps:

Step 1: Install and launch Wireshark:
- Download and install Wireshark from the official website (https://www.wireshark.org/).
- Launch Wireshark on your computer.

Step 2: Select the network interface:
- Choose the network interface to capture packets from. It could be a wired Ethernet interface or a wireless interface.
- Select the desired interface from the drop-down menu in the Wireshark interface.

Step 3: Start capturing packets:
- Click on the "Start" button or press the Ctrl + E (Cmd + E on macOS) shortcut to begin capturing packets on the selected interface.

Step 4: Filter packets by protocol:
- In the filter field at the top of the Wireshark window, enter the filter expression for the desired protocol:
  - HTTP: `http`
  - ICMP: `icmp`
  - TCP: `tcp`
  - SMTP: `smtp`

- POP3: `pop3`

Step 5: Analyze packet information:
- As packets are captured and displayed in the Wireshark interface, you will see packets filtered according to the specified protocol.
- Click on individual packets to view detailed information about each packet, such as source and destination IP addresses, protocol-specific headers, payload data, and more.

Step 6: Apply additional filters and analyze packet details:
- You can further refine the analysis by applying additional filters or dissecting specific fields within the protocol headers.
- Use the various tabs and sections in the Wireshark interface to explore packet details, packet flow, and any additional information related to the selected protocol.

Note: When capturing packets with Wireshark, it's important to have the necessary permissions and legal rights to monitor the network traffic. Always respect privacy and security regulations when using network monitoring tools.

By following these steps, you can use Wireshark to scan and check packet information for protocols such as HTTP, ICMP, TCP, SMTP, and POP3. Wireshark provides a powerful toolset for capturing, analyzing, and troubleshooting network traffic at the packet level.