3. Student Activity

Student Activity: Networking Basics and System Monitoring

Welcome to the practical session on **Networking Basics and System Monitoring**. In this activity, you will practice using various commands and tools to understand how networks operate and how to monitor system performance. Follow the steps below and try each command on your own system. Remember to take notes and ask questions if you encounter any issues.

---

1. Basic Networking Commands

1.1 ifconfig

The `ifconfig` command is used to configure network interfaces on your system. It displays the IP address, subnet mask, and other details about your network interfaces.

Examples:

1. Display all network interfaces:

   ```
   ifconfig
   ```

2. Display a specific network interface (e.g., `eth0`):

   ```
   ifconfig eth0
   ```

3. Disable a network interface:

   ```
   sudo ifconfig eth0 down
   ```

1.2 ping

The `ping` command tests connectivity between your computer and another device on the network.

Examples:

1. Ping a website (e.g., Google):

   ```
   ping google.com
   ```

2. Ping a local network device (e.g., your router):

   ```
   ping 192.168.1.1
   ```

3. Ping with a specific number of packets:

   ```
   ping -c 4 google.com
   ```

1.3 netstat

The `netstat` command shows network statistics, including active connections and listening ports.

Examples:

1. Display all active connections:

   ```
   netstat -an
   ```

2. Display listening ports:

   ```
   netstat -l
   ```

3. Display network statistics with protocol information:

   ```
   netstat -s
   ```

1.4 ssh

The `ssh` command is used to securely connect to another computer over a network.

Examples:

1. Connect to a remote server:

   ```
   ssh user@remote-server
   ```

2. Connect with a specific port:

   ```
   ssh -p 2222 user@remote-server
   ```

3. Use a specific identity file for authentication:

   ```
   ssh -i /path/to/private_key user@remote-server
   ```

---

2. Configuring Network Interfaces and Troubleshooting Connectivity Issues

2.1 Configuring Network Interfaces

Use the `ifconfig` command to assign an IP address, subnet mask, and gateway to your network interface.

Examples:

1. Assign an IP address to an interface:

   ```
   sudo ifconfig eth0 192.168.1.100 netmask 255.255.255.0
   ```

2. Add a secondary IP address to an interface:

   ```
   sudo ifconfig eth0:1 192.168.1.101 netmask 255.255.255.0
   ```

3. Remove an IP address from an interface:

```
sudo ifconfig eth0 0.0.0.0
```

2.2 Troubleshooting Connectivity Issues

Follow these steps to troubleshoot network issues:

1. **Check the physical connection**: Ensure the network cable is plugged in or the Wi-Fi is connected.
2. **Check the IP address**: Use `ifconfig` to verify your device has an IP address.
3. **Ping the gateway**: Use `ping` to check if the gateway is reachable:

   ```
   ping 192.168.1.1
   ```

---

3. Managing Network Services

Network services run in the background and provide functionality like web servers or file sharing. Use `systemctl` to manage these services.

Examples:

1. Start a service (e.g., Apache):

   ```
   sudo systemctl start apache2
   ```

2. Stop a service:

   ```
   sudo systemctl stop apache2
   ```

3. Check the status of a service:

   ```
   sudo systemctl status apache2
   ```

---

4. Monitoring System Performance

Monitor your system’s performance using various tools to ensure it runs smoothly.

4.1 CPU, Memory, and Disk Usage

Examples:

1. Check CPU usage:

   ```
   top
   ```

2. Check memory usage:

   ```
   free -h
   ```

3. Check disk usage:

   ```
   df -h
   ```

---

5. Using System Monitoring Tools

Use these tools to monitor system performance:

5.1 htop

`htop` is an interactive tool that shows real-time information about CPU, memory, and process usage.

Example:

```
htop
```

5.2 iotop

`iotop` shows disk I/O usage, useful for identifying processes using a lot of disk resources.

Example:

```
iotop
```

5.3 vmstat

`vmstat` provides a summary of system performance, including CPU, memory, and disk usage.

Example:

```
vmstat
```

5.4 dstat

`dstat` combines the functionality of several monitoring tools into one.

Example:

```
dstat
```

---

6. Log Management and Analysis

Logs record events on your system and are essential for troubleshooting.

6.1 Viewing Logs with tail and grep

Examples:

1. View the last few lines of a log file:

   ```
   tail /var/log/syslog
   ```

2. Search for specific patterns in a log file:

```
grep "error" /var/log/syslog
```

3. Continuously monitor a log file:

   ```
   tail -f /var/log/syslog
   ```

6.2 Understanding Log Rotation

Log rotation archives old logs and creates new ones to prevent logs from taking up too much space.

Conclusion

In this activity, you practiced using essential networking commands and system monitoring tools. You configured network interfaces, managed network services, and monitored system performance. Continue practicing these commands to become more comfortable with them. If you have any questions, feel free to ask!