



Mahavir Education Trust's
SHAH & ANCHOR KUTCHHI
ENGINEERING COLLEGE
Chembur, Mumbai - 400 088
UG Program in Information Technology

Experiment No: 08				
Date of Performance:	14/10/2024			
Date of Submission:	14/10/2024			
Program Formation/ Execution/ Correction (06)	Timely Submission (01)	Viva (03)	Experiment Marks (10)	Teacher Signature with date

EXPERIMENT - 08

Aim: Network Management tools.

Theory:

Network management tools are critical for monitoring, managing, and optimizing network performance, especially in complex infrastructures such as Virtual Private Networks (VPNs). VPN monitoring tools are designed specifically to track VPN connections, assess network performance, and ensure the security of data transmission over secure tunnels. These tools help administrators monitor VPN usage, detect connection issues, analyze traffic, and troubleshoot VPN-related problems.

VPNs allow users to create secure connections over public or shared networks, ensuring privacy and data encryption. However, maintaining a VPN's performance and security can be challenging without proper monitoring tools. Tools such as SolarWinds VPN Monitor, PRTG Network Monitor, and Nagios help track key metrics like connection stability, latency, bandwidth usage, and possible security breaches. Effective VPN monitoring ensures that remote connections remain secure and functional, with minimal downtime and interruptions.

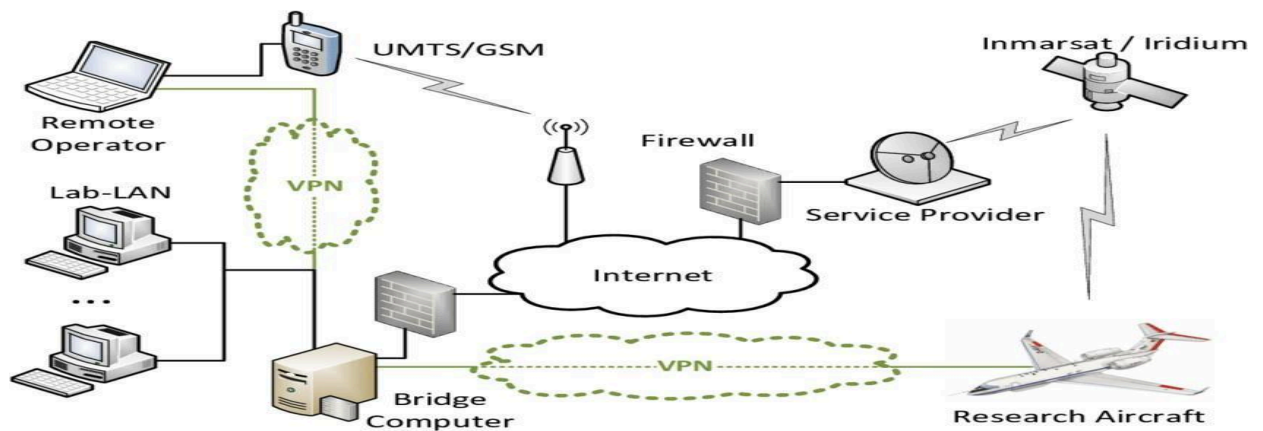
Procedure

1. Install VPN Monitoring Tools:
 - Set up VPN monitoring tools like SolarWinds VPN Monitor, PRTG Network Monitor, or Nagios.
 - Ensure that the VPN network is active and functioning on the system, and establish a VPN connection using a secure VPN protocol (e.g., OpenVPN, IPsec).
2. Monitor VPN Connections:
 - Launch the VPN monitoring tool and configure it to monitor the VPN servers and endpoints.
 - Ensure that the monitoring tool is connected to the relevant VPN devices, such as routers, firewalls, and VPN gateways.
3. Track Key VPN Metrics:
 - Use the VPN monitoring tool to track key metrics, including:
 - i. Connection Status: Monitor if VPN tunnels are up or down.
 - ii. Latency: Check for delays in data transfer within the VPN network.
 - iii. Bandwidth Usage: Measure the amount of data being transferred through the VPN connections.
 - iv. Uptime: Track the availability and reliability of the VPN connection.
 - v. Security Logs: Examine logs for unusual activity or unauthorized access attempts.
4. Set Alerts and Notifications:
 - Configure alerts for key events, such as when a VPN connection drops, unusual bandwidth usage is detected, or high latency occurs.

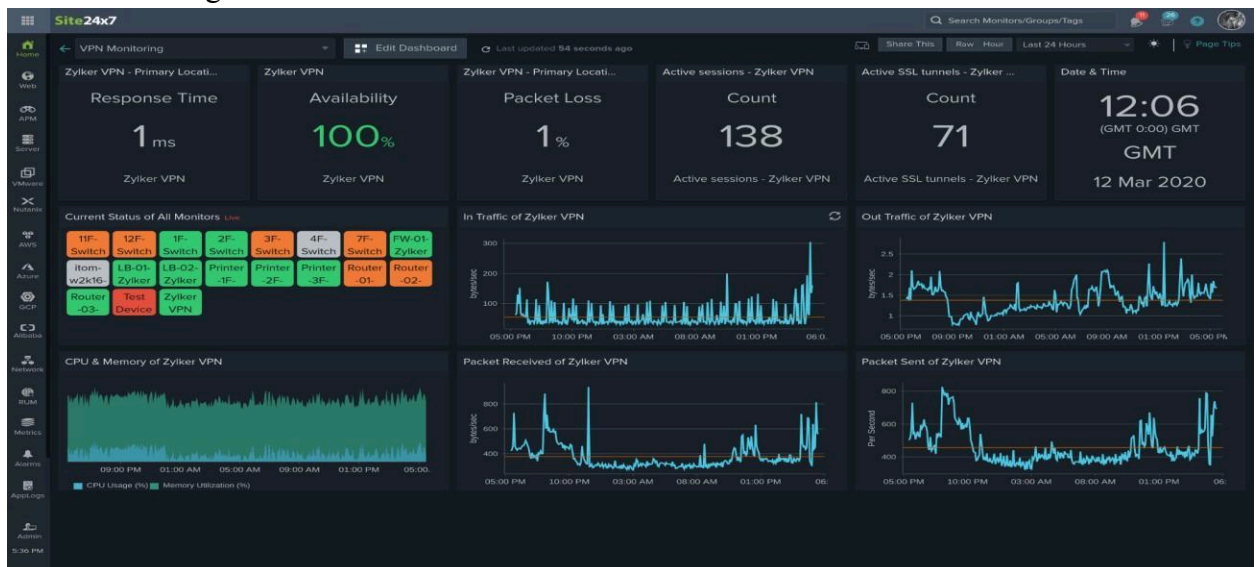
- Use email or SMS notifications to receive real-time alerts if the VPN experiences performance issues or security threats.
5. Analyze VPN Performance:
 - Continuously analyze the collected data to understand VPN performance trends.
 - Identify potential bottlenecks or issues affecting the VPN, such as high latency during peak hours or frequent disconnections.
 6. Save and Export Results:
 - Export performance logs and reports for future analysis.
 - Document findings related to VPN stability, performance, and any anomalies.

Output:

1. Network topology with VPN connection



2. VPN monitoring dashboard



Conclusion :

In this experiment, the use of VPN monitoring tools demonstrated the importance of monitoring VPN connections to ensure secure and reliable network access. VPN tools such as SolarWinds, PRTG, and Nagios provide comprehensive metrics like connection status, latency, bandwidth, and security, which are critical for maintaining the efficiency of a VPN network. Monitoring tools play a vital role in quickly identifying and addressing VPN-related issues, enhancing overall network performance, and ensuring that remote users maintain secure and stable connections. This experiment highlights how effective VPN monitoring can prevent disruptions, improve troubleshooting, and safeguard network security.