OCTOBER 26, 2024

Network Engineer Toolkit Documentation

Welcome to the **Network Engineer Toolkit**! This application is designed to assist network engineers with common tasks, providing a suite of tools to streamline network management, troubleshooting, and planning. Below is a detailed guide to each tool included in the application, explaining their functions, how they work, and how you can benefit from them.

AHMED M. ABDULMOHSEN

1. IP Scanner Tool

Function

The **IP Scanner Tool** allows you to scan a network for active devices, retrieving their IP addresses, MAC addresses, and hostnames. It provides a quick overview of all devices connected to a specified network segment.

How It Works

- **Network Input**: You enter a network range in CIDR notation (e.g., 192.168.1.0/24).
- **Scanning Process**:
  - The tool uses **ARP (Address Resolution Protocol)** requests to discover devices on the local network.
  - It sends ARP requests to all IP addresses within the specified network range.
  - Devices that are active respond with their MAC addresses.
- **Hostname Resolution**:
  - Attempts to resolve hostnames using reverse DNS lookups.
- **Multithreading for Speed**:
  - Utilizes multithreading to scan multiple IPs concurrently, improving scan speed.
- **Results Display**:
  - Displays discovered devices with their IP address, MAC address, and hostname.
  - Shows the total number of devices found.

How to Use

1. **Open the IP Scanner Tool** in the application.
2. **Enter the Network Range**:
   - Input the network you wish to scan in CIDR notation (e.g., 192.168.1.0/24).
3. **Start the Scan**:
   - Click the **"Start Scan"** button to begin scanning.
4. **View Results**:
   - Monitor the output area for the list of active devices.
   - The total number of devices found is displayed.
5. **Reset if Needed**:

    - Use the **"Reset"** button to clear the results and start a new scan.

Benefits

- **Network Discovery**: Quickly identify all devices connected to a network.
- **Troubleshooting**: Detect unauthorized devices or identify IP conflicts.
- **Inventory Management**: Maintain an up-to-date list of devices on your network.
- **Permissions**:
    - May require administrative privileges to perform network scans.

---

2. Subnet Calculator Tool

Function

The **Subnet Calculator Tool** assists in performing various IP network calculations, including CIDR calculations, subnetting, supernetting, and VLAN assignments. It helps you plan and manage IP address allocation efficiently.

How It Works

- **Input Fields**:
    - **Network Address**: Enter the base network address (e.g., 192.168.1.0/24).
    - **Number of Subnets**: Specify the number of subnets to create.
    - **Hosts per Subnet**: Indicate the required number of hosts per subnet.
    - **VLAN IDs**: Input VLAN IDs for VLAN calculations.
- **Calculation Types**:
    - **CIDR Calculation**: Computes network details based on CIDR notation.
    - **Subnetting**: Divides a network into smaller subnets.
    - **Supernetting**: Combines multiple networks into a larger supernet.
    - **VLAN Calculation**: Assigns IP address ranges to specified VLANs.
- **Results Display**:
    - Provides detailed information, including network addresses, broadcast addresses, subnet masks, number of hosts, and more.

How to Use

1. **Open the Subnet Calculator Tool** in the application.
2. **Enter the Network Address**.
3. **Select Calculation Type**:
   - Choose from **CIDR Calculation**, **Subnetting**, **Supernetting**, or **VLAN Calculation**.
4. **Provide Additional Inputs** (as required).
5. **Perform Calculation**:
   - Click the **"Calculate"** button.
6. **View Results**:
   - The output area displays the calculated information.
7. **Reset if Needed**:
   - Use the **"Reset"** button to clear inputs and results.

Benefits

- **Network Planning**: Simplifies subnetting and supernetting for network design.
- **Efficient IP Allocation**: Helps allocate IP addresses effectively.
- **VLAN Management**: Assists in assigning IP ranges to VLANs.

External Programs and Dependencies

- **Python Standard Library**:
  - Utilizes the ipaddress module.

---

3. Circuit Connection Checker Tool

Function

The **Circuit Connection Checker Tool** allows you to monitor the status of network circuits by recording circuit details, periodically checking connectivity via ping, and providing traceroute functionality for troubleshooting.

How It Works

- **Circuit Management**:
  - **Add, Edit, Delete Circuits**: Manage circuit details like name, number, location, and IP address.
- **Status Monitoring**:
  - Periodically pings each circuit's IP address to determine connectivity.
  - Updates the status as **Connected** or **Disconnected**.
- **Traceroute Functionality**:
  - Provides a **"Traceroute"** button for each circuit.
  - Performs a traceroute and displays the results.
- **Data Storage**:
  - Stores circuit information in a SQLite database for persistence.

How to Use

1. **Open the Circuit Connection Checker Tool**.
2. **Add a Circuit** by entering the required details.
3. **Monitor Status**:
   - The tool automatically checks and updates the status.
4. **Edit or Delete Circuits** as needed.
5. **Perform Traceroute**:
   - Click the **"Traceroute"** button for troubleshooting.

Benefits

- **Real-Time Monitoring**: Stay informed about circuit connectivity.
- **Troubleshooting**: Identify connectivity issues with traceroute.
- **Circuit Management**: Organize and maintain circuit information.

External Programs and Dependencies

- **SQLite**:
  - Used for storing circuit data.
- **System Commands**:
  - Uses ping and tracert commands on Windows.

- **Permissions**:
    - May require appropriate network permissions.

---

4. DNS Lookup Tool

Function

The **DNS Lookup Tool** allows you to query Domain Name System (DNS) records for a given domain or hostname, retrieving various DNS records such as A, AAAA, MX, NS, CNAME, and TXT.

How It Works

- **Domain Input**:
    - Enter the domain name or hostname to query.
- **DNS Query Execution**:
    - Uses DNS resolver libraries to perform DNS queries.
    - Sends queries to DNS servers to retrieve DNS records.
- **Record Types**:
    - Select the type of DNS record to query.
- **Results Display**:
    - Displays retrieved DNS records in a readable format.

How to Use

1. **Open the DNS Lookup Tool**.
2. **Enter the Domain Name** (e.g., example.com).
3. **Select Record Type**.
4. **Perform the Lookup**:
    - Click **"Lookup"**.
5. **View Results** in the output area.

Benefits

- **Troubleshooting DNS Issues**.
- **Network Diagnostics**.
- **Security Analysis**.

---

5. Latency and Jitter Tester

Function

The **Latency and Jitter Tester** measures network latency and jitter to a specified target, helping you assess the quality and stability of network connections.

How It Works

- **Target Input**:
  - Enter the IP address or hostname to test.
- **Measurement Process**:
  - Sends ICMP echo requests (pings) to the target.
  - Measures round-trip times for each packet.
- **Calculations**:
  - **Latency**: Average round-trip time.
  - **Jitter**: Variability in latency.
- **Results Display**:
  - Shows individual ping times, average latency, and jitter statistics.

How to Use

1. **Open the Latency and Jitter Tester**.
2. **Enter the Target Address**.
3. **Start the Test**:
   - Click **"Start Test"**.
4. **View Results**.
5. **Reset if Needed**.

Benefits

- **Network Performance Evaluation**.
- **Troubleshooting**.
- **SLA Verification**.

6. Netstat Viewer

Function

The **Netstat Viewer** displays active network connections, listening ports, and network statistics, allowing you to monitor network activity on your system.

How It Works

- **System Command Execution**:
  - Executes the netstat command appropriate for your OS.
- **Data Parsing**:
  - Parses the command output.
- **Results Display**:
  - Presents data in a table format within the application.

How to Use

1. **Open the Netstat Viewer**.
2. **Refresh Data**:
   - Click **"Refresh"**.
3. **View Connections**.
4. **Filter and Search** as needed.

Benefits

- **Network Monitoring**.
- **Security Analysis**.
- **Troubleshooting**.

External Programs and Dependencies

- **System Commands**:
  - Uses netstat.
- **Permissions**:
  - May require administrative privileges.

7. Network Interface Tool

Function

The **Network Interface Tool** provides information about the network interfaces on your system, including IP addresses, MAC addresses, interface statuses, and more.

How It Works

- **Interface Enumeration**:
  - Retrieves a list of all network interfaces.
- **Information Retrieval**:
  - Gathers details like IP address, subnet mask, MAC address, and status.
- **Results Display**:
  - Presents interface information in a table or list format.

How to Use

1. **Open the Network Interface Tool**.
2. **View Interfaces**:
   - The tool automatically displays interface information.
3. **Refresh Data**:
   - Click **"Refresh"** to update the information.

Benefits

- **Interface Management**: Monitor and manage network interfaces.
- **Troubleshooting**: Identify interface issues or misconfigurations.
- **Network Configuration**: Assist in network setup and changes.

---

8. Network Performance Tester

Function

The **Network Performance Tester** measures network bandwidth and throughput between your system and a target server, helping you assess network performance.

How It Works

- **Target Input**:
    - Enter the IP address or hostname of the server.
- **Performance Testing**:
    - Uses protocols like TCP or UDP to send and receive data.
    - Measures upload and download speeds.
- **Results Display**:
    - Shows bandwidth, latency, and packet loss statistics.

How to Use

1. **Open the Network Performance Tester**.
2. **Enter the Target Server**.
3. **Start the Test**:
    - Click **"Start Test"**.
4. **View Results**.

Benefits

- **Bandwidth Assessment**.
- **Troubleshooting**.
- **Network Planning**.

External Programs and Dependencies

- **iperf Library or Tool**:
    - Requires iperf installed on both client and server.

Note:

- The target server must be running an iperf server instance.

---

9. Network Security Scanner

Function

The **Network Security Scanner** scans network devices and systems for vulnerabilities, open ports, and security issues.

How It Works

- **Target Specification**:
  - Enter IP addresses or network ranges to scan.
- **Scanning Process**:
  - Performs port scans to detect open ports.
  - Identifies services running on ports.
  - Checks for known vulnerabilities.
- **Results Display**:
  - Provides a report of findings.

How to Use

1. **Open the Network Security Scanner**.
2. **Enter Targets**.
3. **Configure Scan Options** (if available).
4. **Start the Scan**.
5. **View the Report**.

Benefits

- **Security Assessment**.
- **Vulnerability Management**.
- **Compliance Verification**.

External Programs and Dependencies

- **nmap**:
  - The tool may integrate with nmap for scanning.
- **Installation**:
  - Install nmap on your system.

---

10. Packet Sniffer Tool

Function

The **Packet Sniffer Tool** captures and analyzes network packets traversing your network interfaces, allowing in-depth network traffic analysis.

How It Works

- **Packet Capture**:
  - Uses network interfaces to capture packets.
- **Filtering**:
  - Apply filters to capture specific types of traffic.
- **Analysis**:
  - Displays packet details like source/destination IPs, protocols, payload data.
- **Results Display**:
  - Provides a live view of captured packets.

How to Use

1. **Open the Packet Sniffer Tool**.
2. **Select Network Interface**.
3. **Set Filters** (optional).
4. **Start Capturing**.
5. **View Captured Packets**.
6. **Stop Capturing** when done.

Benefits

- **Network Troubleshooting**.
- **Security Analysis**.
- **Protocol Understanding**.

External Programs and Dependencies

- **Scapy or PyShark**:
  - **Installation**:
- **Permissions**:
  - Requires administrative privileges.
- **Note**:
  - Ensure compliance with laws and policies regarding packet capturing.

---

12. Port Forwarding Tester

Function

The **Port Forwarding Tester** checks if a specific port on your network is open and accessible from the internet, verifying port forwarding configurations.

How It Works

- **Port Specification**:
  - Enter the port number and optionally the IP address.
- **Testing Process**:
  - Attempts to establish a connection to the specified port.
- **Results Display**:
  - Indicates whether the port is open and reachable.

How to Use

1. **Open the Port Forwarding Tester**.
2. **Enter Port Number** (and IP address if needed).
3. **Start the Test**.
4. **View Results**.

Benefits

- **Verify Port Forwarding Rules**.
- **Troubleshoot Connectivity Issues**.
- **Ensure Service Accessibility**.

---

13. SNMP Manager

Function

The **SNMP Manager** communicates with SNMP-enabled devices to retrieve management information, configure devices, and monitor network components.

How It Works

- **Device Configuration**:
    - Enter the IP address, SNMP version, and community strings.
- **Data Retrieval**:
    - Sends SNMP GET and WALK requests to retrieve data.
- **MIB Support**:
    - Uses Management Information Base (MIB) files for object identifiers.
- **Results Display**:
    - Shows device information, status, and metrics.

How to Use

1. **Open the SNMP Manager**.
2. **Configure Device Settings**.
3. **Retrieve Data**:
    - Perform SNMP GET or WALK operations.
4. **View Device Information**.

Benefits

- **Network Device Management**.
- **Performance Monitoring**.
- **Automated Configuration**.

MIB Files:

- May need to obtain and load specific MIB files.

---

14. Syslog Viewer

Function

The **Syslog Viewer** collects and displays syslog messages from network devices and systems, aiding in monitoring and troubleshooting.

How It Works

- **Syslog Collection**:
    - Listens on standard syslog ports (e.g., UDP 514) for incoming messages.
- **Message Parsing**:
    - Parses syslog messages to extract relevant information.
- **Results Display**:
    - Presents logs in a readable format with filtering options.

How to Use

1. **Open the Syslog Viewer**.
2. **Configure Listening Settings** (if necessary).
3. **Start Listening** for syslog messages.
4. **View and Filter Logs**.

Benefits

- **Centralized Log Management**.
- **Security Monitoring**.
- **Troubleshooting and Auditing**.

External Programs and Dependencies

- **Python Libraries**:
    - May use socketserver or third-party libraries.
- **Permissions**:
    - May require administrative privileges to listen on certain ports.

Conclusion

The **Network Engineer Toolkit** provides a comprehensive set of tools to assist with network management, troubleshooting, monitoring, and security. By utilizing these tools, you can streamline your workflow, improve efficiency, and maintain better control over your network infrastructure.

If you have any questions or need further assistance with any of the tools, please refer to this documentation for guidance. Enjoy using the Network Engineer Toolkit to enhance your network engineering tasks!