Campus networks troubleshooting/supporting tools

Out Of Band Access / VPN / Remote Desktop / Traceroute / Packet capture / Network scanner / Looking Glass

Author:
Sami Ait Ali Oulahcen

Nouakchott, Mauritania
17-22 February 2025

Remote Access

Out-Of-Band (OOB) access

- How do you access a device when the network or the device itself is down ?

- You need an Out-Of-Band (vs. In-Band) network access

- For a full OOB network you need dedicated switches and a dedicated exit ADSL/4G/VSAT

OOB for network devices

- All managed network devices have a **console port**
- You can use a console server and connect it to your OOB network, this avoids you going physically to the device with a console cable and laptop

OOB for servers

- All enterprise servers have dedicated Baseboard management controller interfaces that support the **IPMI/redfish** standards like Fujitsu's iRMC, HP's iLO, Huawei's iBMC, Dell's iDRAC, or SuperMicro's BMC
- They show useful information like health of different server components ex. PSU, fans, hard drives, CPU, and RAM status
- Can also be used to remotely install the Operating System, and remotely access the server console

Remote access

- More often than not, you need remote access to your infrastructure
- This access needs to be secure, encrypted end-to-end, and restricted to the IT team
- A Virtual Private Network (VPN) does exactly this
- Many available options both commercial and opensource, we recommend **eduVPN** (Wireguard and OpenVPN based)

What is eduVPN

- Opensource and free VPN client/server tailored for the research and education community

- Two Offers: **Secure Internet** and **Institute Access**

- Institute Access enables remote access to internal resources

- Under the hood, you can choose to use OpenVPN and/or Wireguard

- Authentication is done through your existing directory services: LDAP, SAML, and RADIUS are all supported

eduVPN Institute Access

- Install on common Linux distros, Debian recommended

- Light on resources: for a team of 10-20 people, a 2vCPUs/2GB ram VM is more than enough

- After installing, contact the eduVPN team to be added to the apps

- Very easy to connect, apps available for all platforms

- For how to install and how to be added to the apps check the website https://eduvpn.org

مرحبا بك على eduVPN!

لاستعمال eduVPN، حمل التطبيق على جهازك أسفله!

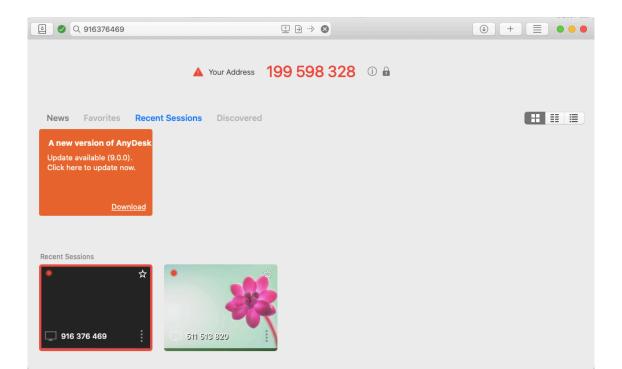| لينكس | آي أو إس | اندرويد | ماك | ويندوز |

Remote Desktop

- A great way to remotely access and diagnose issues on end-user devices

- Secure troubleshooting sessions from the comfort of your home/office

- Many available options: RustDesk (Free & Open source), AnyDesk (free for personal use)

Troubleshooting tools

Ping

- Basic yet effective method for identifying network issues

- Can be used to test reachability, latency, packet loss, fragmentation, number of hops and potential routing issues, and much more

- Notable ping options:

-c   +count (Stop after sending $count packets)

-s   +number of bytes to send

-D   Set the Don't Fragment bit

 -i / -f interval between each packet / Flood Ping

Traceroute

- Maps the route taken by packets across a network
- Helps identify where network delays or failures occur by pinpointing problematic routers or segments in the network path
- **Question: How does traceroute find out the routers which a packet traverses?**

Traceroute

- Maps the route taken by packets across a network
- Helps identify where network delays or failures occur by pinpointing problematic routers or segments in the network path
- **Question: How does traceroute find out the routers which a packet traverses?**
- Sends ICMP/UDP/TCP packets with gradually increasing Time-to-Live (TTL) values
- Receives ICMP "Time Exceeded" messages from intermediate routers
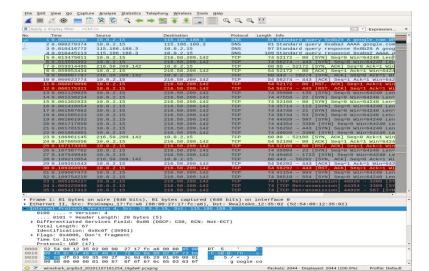- Constructs a list of hops between source and destination

Tracepath

- **Tracepath** is an alternative that relies on UDP and provides also Path MTU discovery along the path

- Simpler output and more user-friendly

- Doesn't need root or elevated privileges to run

- Ideal for basic diagnostics, particularly for detecting MTU issues along the route

- Included by default in most Linux distributions

Packet capture

- Process of intercepting and logging data packets as they traverse a network to analyze traffic patterns or diagnose issues

- Tools like tcpdump and Wireshark capture raw network data for inspection

- Key Components:

  - Headers: Source/destination IPs, ports, protocols

  - Payload: Actual data transmitted (i.e HTTP requests, DNS queries)

Packet capture in campus networks

- In campus networks, packet capture can help identify some common issues:

  - Slow bandwidth: too many retransmits/resets, bottlenecks

  - Security Threats: unauthorized traffic, ARP spoofing, DDoS attacks

  - Protocol misconfigurations: DHCP IP assignment, DNS responses

Tools for packet capture

- Wireshark: GUI-based tool for all platforms. Can be used for capture and analyses. Extensive filtering and deep protocol decoding.

- tcpdump: CLI-based tool for Unix-like systems. Lightweight with fast. Flexible filtering using BPF syntax. Can be used to capture data for deeper analysis in Wireshark

```
tcpdump -i ens32 port 8080
```

perfSONAR

- perfSONAR is an open-source network performance measurement framework designed for end-to-end monitoring

- Widely deployed in research and education networks, it helps diagnose and troubleshoot network issues across administrative domains.

perfSONAR integrated tools

- iperf/iperf3: Tests network throughput and performance
- OWAMP & TWAMP: Measures one-way and two-way packet delay and loss
- (reverse)traceroute: Identifies route paths and detects routing issues
- Visualization & Data Management: web-based dashboards and data archives for historical analysis and trend identification

Looking Glass

- Tool to view and analyze the routing and performance of networks from the perspective of different locations

- **Troubleshooting**: When network issues arise, looking glass tools can help identify where the problem lies—whether it's within a local network, with an ISP, or further upstream

- **Ping and Traceroute Tests**: Many looking glass services allow users to perform ping and traceroute tests from various locations. This helps in diagnosing latency issues and understanding the path that packets take to reach their destination

Questions ?