Procedure - Troubleshooting a Slow Network

Intent of this document

This document is intended to speed up the process of diagnosing network slowness at a given location. By the end of this procedure, you should have enough information to determine the root cause and be able to either resolve the issue or develop an action plan to resolve the issue.

1/ Probe for more information (if applicable)

If you're receiving the complaint by phone, take the opportunity to get your bearings on the scope and details of the issue. However, if the complaint came to you by email or <ticketing system>, skip this step and only come back to it if you can't gather enough information in later steps to diagnose a root cause.

Questions:

1) Is it just the internet that's slow, or are internal connections also slow?
2) Is one user experiencing the slowness or many?
3) Is the slowness happening over a wired or wireless connection?
4) Is the issue consistent or intermittent? Is there a pattern or is it seemingly random?

The answers to these questions will help frame the information you gather as you investigate the issue.

2/ Determine if the issue is external or the firewall

It's always good to rule out the ISP before diving into device configuration changes. Investigating the ISP can also give you a sense of possible scope—even if only one user is reporting an issue, others could be affected who aren't yet speaking up.

Check packet loss & round-trip time

1) Open the site in Auvik.
2) Go to Inventory > All Services > Internet Connection Check.
3) Look to see if any of the ping checks on the IPs are slow to respond or have spiking packet loss.
4) Click on the firewall's public IP from the chart to get more detail into the packet loss and round-trip time.
5) If either metric is high (packet loss percentage is over 5% or round-trip time is over 200ms), you've likely found the source of the problem.
    a) Use the calendar icon to load more data. See if you can identify when the issue started. Engage <ISP name> or check their support page at <insert URL here>.

Check All Internet Connections & investigate traffic

1) Open the site in Auvik and go to the home dashboard.
2) Look at the All Internet Connections widget to see if any WAN links are approaching capacity.

3) If an interface is near capacity, open Auvik TrafficInsights to assess the increase in traffic.
   a) You can do a speed test to confirm the increased traffic is affecting network speed.
4) Use the graph range selector at the bottom of the TrafficInsights screen to narrow in on the time the performance issue was being experienced.
5) Use applications filters and Top N to determine if the traffic is business-related and likely to continue.
   a) If it's legitimate business traffic, investigate whether you can alleviate the capacity of the WAN link and redistribute the load. Or, if further action is needed, inform the <client or internal stakeholder>.
   b) If it's not legitimate business traffic, shut down the source of the traffic. To do this you can:
      i) Shut down the application that's consuming the bandwidth. See <**name of another SOP for this**> for more details.
      ii) Configure the firewall to block the traffic. See <**name of another SOP for this**> for more details.

3/ Investigate root cause device or connection

At this point, it's safe to assume an internal entity is the root cause of the slowdown. Now you'll want to narrow your search and gather data that shows there's a device or connection at the heart of the issue so you can move towards resolving it quickly.

Isolate potential devices

1) Use the topology map in Auvik to narrow down the affected users, what devices they're immediately connected to, and the possible paths between their endpoints and the firewall.
   a) If there's an alert icon on a key switch or firewall on the map, dig into the device. If instead a key physical connection (blue wire) is now yellow or red due to an alert, look into the connection's details as it may be the root cause. In either case, highlight the alert and click on the alert popup to get more details.
   b) If the affected users are on one or more VLANs, use the VLAN filter on the topology map to isolate trunk connections and overlapping devices.
2) Cross-reference the list of potential culprits with the All Alerts log and the Top Devices by Bandwidth report in Auvik, <and any other applicable reports from other tools>. When looking at the All Alerts log, see if there are entities firing high CPU or memory utilization. If the high utilization is on a router, it could be introducing latency or jitter and it might be the source of the issue.
3) Investigate devices that appear on more than one of the lists by clicking into their dashboards in Auvik.
4) Use <RMM tool or remote browser/management tool or device-specific tool> to assess the device's health further and see if a recent change was made. If you suspect it's an endpoint issue, follow the steps in <**endpoint troubleshooting SOP**>.
5) If you identify a root cause device, revert the change that put it in this state if you can. Otherwise, pass the details to an appropriate technician or develop a mutual plan of action with the <client or internal stakeholder>.

Isolate potential wired connection issues

1) Use the topology map in Auvik to identify key connections for the affected users.
2) Bring up the dashboard of the main interface they're directly connected to and check if it's overloaded or not functioning as expected.
    a) If there appears to be a problem:
        i) Check the negotiation speed to ensure it's connected at the right level.
        ii) Check the alerts for the interface to see if anything stands out or if a change was made that could have affected it.
        iii) If possible, have the user connect into another interface to ensure it's not an endpoint issue. An easy way to do this is to have the user change their connection type by going from a wired connection to wireless.
3) Check the Top Interfaces by Bandwidth report to see if there's a less direct connection that isn't performing as expected and might be having a trickle-down effect on the user. Investigate the health of that interface.
4) Check for packet error alerts on relevant interfaces or devices. If there's an increase in the number of packet errors, there could be a Layer 1 issue like a bad cable or connection. Try to isolate the issue and investigate whether it can be solved remotely. Otherwise, go to the site to investigate further.
5) From the interface dashboard in Auvik, click on the parent device to go to the device's dashboard. Review the top interfaces on the device dashboard to identify if other interfaces are overloaded as well. Also review the device utilization graph to see if there are any obvious device issues, such as high CPU utilization or high memory utilization. Is only one interface overloaded or are other interfaces or the device itself experiencing issues?

Isolate potential wireless connection issues

If the users aren't wired in, the issue could be with the wireless connection.

1) Try to get a signal-strength reading on the endpoint having issues by <this process may differ depending on the machine>.
2) Dive into <access point monitoring tool> to see if there's any indication of latency or jitter on the access point.
3) You can also take a look at the device that's upstream from the access point to ensure the issue is isolated between the access point and endpoint(s).

Investigate endpoint if only one user is experiencing problems

If nothing network-related seems concerning and only one person has raised their hand about the issue, use <RMM tool> to remote into their device and follow the steps in <**endpoint troubleshooting SOP**> to identify the issue.

4/ Investigate network traffic patterns

If you can't identify a root cause device or connection, the problem seems to come and go somewhat randomly, and more than one person is affected, the issue may be sudden spikes in traffic.

Investigate recent traffic patterns

1) Open Auvik TrafficInsights for the site or firewall that affected users are connecting to.
2) Load a week's worth of data and use the timeline to identify spikes that align with slow network complaints.
3) Isolate the application causing the traffic spikes, then see if Top N identifies one source or multiple, and whether the traffic is business-related.
4) If one source:
    a) Rate-limit the traffic from the firewall if the traffic isn't business-related. Let <your business contact at the client or internal stakeholder> know what happened and that you've blocked future traffic like this from the firewall.
    b) If the traffic seems business-related, contact <your business contact at the client or internal stakeholder> to determine if the new behavior is expected to continue so you can gauge future capacity needs.
5) If multiple sources:
    a) Assess the timeline to see if the traffic has been growing over time. If so, bring the issue to <the client relationship manager>'s attention to open conversations about increased bandwidth and changes that need to be made to improve load distribution over the network. Ensure you provide them with the data from Auvik so they can demonstrate the bottlenecks in devices or connections.
    b) If the change is sudden, see if there's a clear culprit application that may align with a new business function that's recently been implemented. For example, maybe they've switched from desk phones to a VoIP application for calls. Again, bring this forward so you can work with them to support their network needs in future.
    c) If TrafficInsights doesn't provide enough granularity at the root cause application, set up a packet capture using <packet capture tool> on an interface that will capture most or all of the source devices. Do deeper analysis on the traffic flowing through the interface after <amount of time>.

5/ Wrap things up & document

Always remember to document your changes, observations, future plans, and resolutions in <ticketing system and documentation platform>. Follow up with the reporter of the issue to share your findings and resolution. If more extensive action items came out of this investigation, add them to any actions or capacity plans for this site to bring up during the next on-site or quarterly business review.