Identifying culprits by correlating PingPlotter "problem" patterns with network use.

Saved From:

https://www.pingman.com/kb/article/identifying-culprits-by-correlating-pingplotter-problem-patterns-with-network-use-

Question

I'm consistently seeing network problems on the first hop, which is inside my provider's network. How do I know what's causing it?

Solution

(Note that this might apply to hop 2, 3 or 4 - if it's the first hop inside your provider's network).

Let's say that you've collected some data in PingPlotter and notice that there is a pattern in PingPlotter that correlates to a network problem (see here for details on how to do that). Here are some best practices on how you might identify the culprit.

First off, bandwidth saturation is normal. High latency, packet loss, and performance problems are normal. If you decide to upload a 100gb backup .zip, it's really likely that you're going to use all the available bandwidth you have, and that's going to result in higher latency and packet loss (and worse VoIP calls and worse internet experience) while you're doing this. That's all fine and good as long as you know you're causing the problem.

It becomes painful, though, when you don't know what's causing the problem. If you're seeing a consistent pattern inside the PingPlotter data (periods of lost data, high latency), there are a variety of possibilities:

- Hardware failure of some kind.
- Wireless network problems.
- Overuse of network by some computer, device or process.
- Others.

A very effective technique to isolate this down is to systematically try to correlate the pattern you're experiencing with some activity.

We find that using a 2.5-second trace interval in PingPlotter does a nice job of capturing just about any event. While you're doing active troubleshooting, we recommend using this setting.

To isolate the problem, look at PingPlotter data before, during and after use of a suspected culprit.

If you think your wireless network is at fault (a common problem), collect data with PingPlotter, hook your computer up to a wired network, turn off wireless and see if the problem goes away. If your pattern repeats itself often, this may just take a few minutes. If it's a once-a-day event, then you'll need at least 2 "periods" of the issue not happening to say you have correlation.

Similarly, if you think a specific application is at fault, look at your use of this application and see if you can correlate the pattern in PingPlotter with your use of this application. If your latency increases every time you watch a streamed movie, then you have a pretty good idea that you're saturating the network with your streamed movie. If you sometimes see the pattern when you're streaming movies but not always, and you never see the problem when you're not, then you have a softer correlation and there's probably something else in your network that is complicit in the pattern. If the pattern happens when you're not streaming a movie, then you've lost your correlation and you can move on looking for other problems.

Ideally, you could do this with each of your network consumers. If you have 5 computers in an office and an HD TV with streaming capabilities, and a backup server that connects to a cloud backup system, then try eliminating each of these devices from the network and see if it changes your pattern.

Keep in mind that bandwidth is a shared resource, so anything that uses this network "bottleneck" point could contribute to the problem. Usually, you have one or two major contributors, though, and if you can identify those you can put together a plan for solving them (maybe buying more bandwidth, or getting a router that can limit network use for a specific application, or replacing a bad device).

As networks get more complex (more computers) this becomes more difficult - especially if you have a mission-critical application that you suspect is causing the problem. Sometimes, you can get some clarity on this based on time-of-day, or traffic patterns within that application.

In a perfect world, you'd have a border device (router, modem, etc.) that could tell you where the traffic was coming or going. In that case, you can watch the pattern in PingPlotter and when you see it start to happen, look at a report on your border router to see which applications (destinations, computers, ports) are using the bulk of the data, then you can work on a mitigation strategy.