pathSolutions

WHITE PAPER

4 Stages of Troubleshooting

Awareness, Confirmation, Identification, and Resolution

(877) 748-1777
Sales@PathSolutions.com
www.PathSolutions.com

Contents

(877) 748-1777
Sales@PathSolutions.com
www.PathSolutions.com

Troubleshooting Challenges

Troubleshooting problems is the bane of any network or UC team, as they typically struggle with a number of unknowns in their environment while mandated to achieve resolution and user satisfaction in a very short amount of time. The troubleshooting process consists of four stages: awareness, confirmation, identification, and resolution.

Recognizing what stage of the troubleshooting activity you're in allows for better coordination and understanding of troubleshooting process from a technical and managerial standpoint. It can also prevent teams from getting stuck, looking at the wrong type of information at the wrong stage.

Stage 1: Awareness

The awareness stage begins when a problem is reported. This generally occurs when a user reports a problem, or a monitoring system generates an automated alert about a problem. For example:

User calls at noon to complain about a poor quality VoIP call at 11:51am.

At this stage, a trouble ticket is usually created to track work performed. Additional information should also be collected that may help with resolution. For example:

- Is this the first time this problem happened?
- Who is the other caller?
- How is the problem characterized: clipping, missing parts of the conversation, dropped call, one-way-audio, or echo?

Awareness may also be triggered by a monitoring system. For example, a MOS score is tracked across the environment and generates an alert if MOS is too low from point-to-point. In this case, a ticket might be automatically generated with the relevant test results.

Stage 2: Confirmation

The confirmation stage is optional, but can sometimes reveal clues that help narrow the scope of troubleshooting and save time. In some cases, this is as simple as checking to see if the user really did have a problem. For example:

The CDR record for the call is checked, and it shows 6% packet loss for the call.

At this point, you know it's not a problem with the user or their handset, but an actual problem related to packet loss on the network.

Fact-finding can help identify why the problem occurred. Depending on the CDR analysis tool, you may be able to correlate this call with other calls that were also bad at the same time. For example, if all calls going through a particular gateway had packet loss at that time, most likely the cause is the gateway, or the network elements that are all common to those calls going to the gateway.

Packet analyzers or sniffers are other tools you can use to confirm a problem. If the packets in the VoIP call were captured, these tools would confirm that 6% of the packets were missing from the capture session. However, these tools merely confirm a problem exists, not what caused it.

Stage 3: Identification

Typically, problem identification is the most difficult part of the troubleshooting process as a great deal of information must be gathered from a number of different devices and locations and critically analyzed. Problem identification is made up of three distinct steps: data collection, correlation, and analysis.

Data Collection

The data collection step is challenging as there are many types and sources of information to collect. Sources include:

Logfiles

Device log files are typically collected by a centralized syslog server. The log information usually relates to critical device or interface operational messages like:

- Interface changed status to DOWN.
- CPU utilization over 95%.
- Device rebooted.

If the failure is a complete outage, then logfile information can be valuable for determining the fault as it shows messages that relate to the *exact time* of the outage.

Logfile information is easy to manually correlate since each logfile entry has a timestamp that can be checked to see if it relates to the problem or not. However, logfiles are not useful for troubleshooting packet loss, over-subscription, or delays since they provide a limited amount of information.

Device and interface configuration

Device configuration information may sometimes show misconfigurations like incorrect speed settings, or half-duplex connections that should be running at full-duplex. This

information should be available for all devices and interfaces in the enterprise so it can be included for consideration in the later troubleshooting stages.

Error counters

Network devices contain large numbers of error counters that can be queried to determine the network's operation and health. Some error counters may be presented via the CLI of the device. For most devices, a significant number of error counters can be queried via SNMP (with appropriate tools) to see how packets were processed, delayed, or dropped.

To determine if packet loss occurred during a reported event, error counters need to be historically tracked. Error counters should be tracked on all involved links, switches, and routers in the network so problems can be diagnosed when, where, and why they happened. This can be a daunting task for operations teams due to the vast amount of information that must be collected.

Correlation

Once all the information is collected, it should be correlated so that the specific data elements relevant to the problem can be brought into focus. This can be accomplished by considering two variables: time and path.

Time Correlation

If the event occurred at 11:51am, you can safely ignore information that occurred 10 minutes prior to, or after the event. That reduces the dataset to be evaluated, as the volume of data is decreased.

Path Correlation

Eliminate the devices and links that were not part of the conversation and focus on the links and devices that were part of it. This can be done manually if there is an accurate network diagram, or with automated path mapping solutions. Make sure that the path mapping activity includes layer-1, layer-2 and layer-3 visibility so important elements are not missing from the picture.

(877) 748-1777
Sales@PathSolutions.com
www.PathSolutions.com

Analysis

With the right data and correct analysis, accurate conclusions can be reached. For example:

> *The Finance2 switch interface #7 was used along the path for the call, and at 11:52 am, 6% of its packets were dropped due to FCS Errors. At the same time, 0 packets were dropped due to alignment errors, and 0 packets were dropped due to collisions.*

A senior-level engineer would evaluate this to mean that a cabling fault dropped packets at that time due to the presence of FCS errors and complete absence of alignment errors and collisions.

The problem with analysis is how to interpret information in order to move onto the fourth stage, resolution. Keep in mind that interpretation may require research into error counters and how they interact with each other to determine the root-causes of faults.

Stage 4: Resolution

This is the work needed to get an identified problem fixed. For example:

> *We replaced the cable on the Finance2 switch interface #7.*

Once the problem is fixed, do additional research to confirm that the resolution achieved results. In other words, repeat the confirmation stage to validate that the problem is not happening again. Alternatively, check the error counters to see if they no longer increment.

Optimizing the Troubleshooting Process

An overarching goal of the network troubleshooting process is to make it faster and easier. There are three ways to optimize the process:

- **Automated collection of information.** For example, if the network error counters, configuration, and logfiles from all network devices and links could be collected on a regular basis, you would have a powerful dataset to query.
- **Time- and path-based correlation.** Applying time- and path-based correlations to datasets so that all involved network elements can be assessed at the exact time of an event.
- **Built-in heuristical analysis of information.** Analysis of all error counters, along with plain-English answers to discovered problems speeds remediation.

This is what PathSolutions TotalView does: root-cause, plain-English troubleshooting anytime, anywhere in the network. Instead of an all-day or week-long process, TotalView troubleshoots and resolves problems in a few minutes.

TotalView tracks activity on all error counters at all times and generates a root-cause alert on the cause of a problem *when* it occurred. As a result, stages one through three (Awareness, Confirmation, and Identification) are skipped. Since TotalView provides plain-English answers to problems with its Network Prescription engine, all you need to do is implement the recommended fix. For example:

> *6% of the packets were lost on the Finance2 switch interface #7 at 11:52 am due to a cabling fault.*

Streamline your troubleshooting process by replacing the cable, and other problems, as soon as you are aware of them. That way, when your user reports a problem to you, you've already fixed it.

Additional Resource:

Webinar: Finding Packet Loss in the Network

(877) 748-1777
Sales@PathSolutions.com
www.PathSolutions.com