TROUBLESHOOTING

COMMAND LINK

When visibility isn't enough
and action is required.

www.commandlink.com

SD-WAN TROUBLE SHOOTING

Identifying problems in an SD-WAN environment using monitoring and diagnostic tools often involves a systematic approach of isolating the issue.

Here's a structured process to pinpoint problems:

1. **Start with Alerts and Dashboards:**

   - Begin with the primary alerts and notifications from your SD-WAN dashboard, network monitoring, or security tools. These are designed to notify you of immediate issues.

   - Dashboards provide a quick glance into the current state of your network, including key metrics, device statuses, and recent events.

2. **Traffic Analysis:**

   - What to look for:

     - Unusual traffic spikes.

     - Unexpected traffic sources or destinations.

     - Incorrectly tagged or prioritized traffic.

     - Packet loss, latency, or jitter anomalies.

3. **Application Performance Monitoring (APM):**

   - If users are complaining about a specific application's performance, leverage APM tools to drill down into transaction times, server response

rates, and other application-specific metrics.

- Compare application performance across different network paths to identify if a particular path is the problem.

4. **Device Health and Status:**

   - Check the health of SD-WAN devices using the native SD-WAN dashboard or third-party monitoring tools.

   - Monitor CPU, memory utilization, temperature, and other vital stats. Overloaded or overheating devices can be a source of issues.

5. **Link Performance:**

   - Use tools to monitor individual link performance in your SD-WAN setup. This can help identify if issues are arising due to a particular ISP, link, or connection method.

   - Look for patterns: Are problems occurring consistently on a specific link or during certain times?

6. **Log Analysis:**

   - Centralized logging solutions can provide a wealth of information. Search logs for:

   - Error messages or warnings.

   - Configuration changes.

   - Security events or potential breaches.

   - Correlate events from different devices or applications to identify patterns or causative factors.

7. **Security Events:**

   - Review alerts from IDS/IPS systems for potential security incidents.

   - Unusual traffic patterns, denied connections, or detected threats can impact performance or block legitimate traffic.

8. **Synthetic Transactions:**

   - Use synthetic transaction tools to replicate user activities and see where slowdowns or failures occur.

9. **End-User Perspective:**

   - Endpoint monitoring and feedback from users can provide valuable insights. If users in a particular location are experiencing issues, it may indicate local network problems or SD-WAN edge device issues.

10. **Service Provider Insights:**

    - Review metrics and reports from ISPs or cloud providers. They might provide details about outages, performance degradation, or maintenance activities affecting your services.

11. **Documentation Review:**

    - Compare the current network state with documented baselines or previous configurations. Recent changes can often be a source of problems.

12. **Engage Vendor Support:**

    - If you're unable to identify the problem using your tools, engage the support teams of your SD-WAN or tool vendors. They may have deeper diagnostic tools or insights into known issues.

By systematically narrowing down the scope and using a combination of the tools at your disposal, you can effectively pinpoint where issues are arising in your SD-WAN environment. Once the problem area is identified, targeted troubleshooting can be employed to resolve the issue.

COMMAND LINK

Some things should be easy to manage.

Get a Demo