
THE MOST COMMON
SD-WAN
HICCUPS
ENTERPRISES FACE
COMMAND LINK
When performance drops and
things don't behave as expected.
www.commandlink.com

Most Common SD-WAN Issues

SD-WAN has transformed the way businesses manage their WAN infrastructure. However, as with any technology, SD-WAN is not without its challenges. Here are some of the **most common** SD-WAN issues faced by organizations:

Is it a Configuration Error?

- Mistakes in SD-WAN **policy** or **configuration** can lead to performance degradation, connectivity issues, or even security vulnerabilities.

- SD-WAN configuration errors refer to mistakes made **during the setup**, deployment, or ongoing management of an SD-WAN infrastructure. These errors can lead to network *downtime*, performance degradation, security vulnerabilities, and other undesirable outcomes.

Most common configuration errors:

- **Incorrect Traffic Policies:**

  - **Error:** Misconfigured traffic routing or prioritization rules that don't align with business needs.

  - **Solution:** Clearly define and document **traffic prioritization** based on business requirements. Regularly review and update policies, especially after significant network or business changes.

- **Poorly Defined Failover Rules:**

  - **Error:** Not configuring appropriate failover and redundancy mechanisms, leading to avoidable downtime during **link failures**.

- **Solution:** Define clear failover criteria and test these scenarios periodically to ensure seamless transition during outages.

- **Lack of Security Configurations:**

  - **Error:** Overlooking essential security settings like **encryption**, firewall rules, or intrusion prevention.

  - **Solution:** Adopt a security-first approach. Ensure all traffic is encrypted, define strict firewall rules, and integrate SD-WAN with other security tools.

- **Neglecting Quality of Service (QoS) Settings:**

  - **Error:** Not setting up **QoS** correctly, leading to latency-sensitive applications (like VoIP) experiencing performance issues.

  - **Solution:** *Prioritize* critical applications in QoS settings and regularly monitor and adjust based on traffic patterns.

- **Misconfigured Cloud Integration:**

  - **Error:** Incorrectly setting up connections to cloud service providers, causing performance or connectivity issues.

  - **Solution:** Collaborate with cloud providers during the setup phase and follow best practices for SD-WAN-to cloud integrations.

- **Not Updating Firmware/Software:**

  - **Error:** Using *outdated* software versions that lack new features or security patches.

  - **Solution:** Regularly check for updates and apply them in a controlled manner, ideally in a test environment first.

- **Ignoring End-to-end Encryption:**

  - **Error:** Only encrypting part of the traffic, leaving some segments of the network vulnerable.

  - **Solution:** Implement end-to-end encryption for all data in transit across the SD-WAN.

Do I Have Enough Bandwidth?

- Even with SD-WAN's ability to aggregate multiple links, if the collective bandwidth is insufficient for organizational needs, it can lead to network **congestion** and poor application performance.

- Identifying if your SD-WAN has inadequate bandwidth involves monitoring, measuring, and analyzing the traffic flowing through your network.

Here's how you can determine if your SD-WAN is suffering from bandwidth limitations:

- **Utilization Monitoring:** Use network monitoring tools that can provide real-time and historical data on bandwidth utilization. If your bandwidth usage consistently hovers near or at 100%, it's a clear sign of insufficient bandwidth.

- **Evaluate Critical Application Performance:** If latency-sensitive applications like VoIP, video conferencing, or real-time data processing are experiencing drops in quality or frequent disconnects, this might indicate inadequate bandwidth.

- **Check QoS (Quality of Service) Alerts:** Many SD-WAN solutions can send alerts when Quality of Service for prioritized traffic isn't being met due to bandwidth limitations.

- **Review Network Reports:** Periodically review network performance reports.

Spikes in usage or sustained high utilization levels during business hours are indicators.

- **Look for Symptoms:** Symptoms like slow file transfers, buffering during streaming, or lag in interactive applications can indicate bandwidth constraints.

- **Measure Bandwidth Directly:** Use tools or online services that can measure available bandwidth by sending packets and calculating the speed based on response times.

- **Traffic Analysis:** Deep packet inspection and traffic analysis can help determine which applications or users are consuming the most bandwidth. If critical applications are being starved of needed bandwidth, it's an indication that more is required.

- **Feedback from Users:** Often, end-users will be the first to notice and report issues. Consistent complaints about slow application performance can be an early warning sign.

- **Failover Frequency:** If your SD-WAN solution is frequently switching to backup connections because the primary link is saturated, it's a clear sign of inadequate primary link bandwidth.

- **Cloud and SaaS Performance:** If cloud-based applications or services perform poorly despite the cloud provider ensuring optimal performance on their end, the issue might be with your SD-WAN bandwidth.

Is my Hardware/Software Incompatible?

Some older network devices might not be fully compatible with SD-WAN solutions, leading to interoperability challenges.

Incompatible hardware or software can cause a range of issues in an SD-WAN deployment, from performance degradation to complete network failures.

Addressing these incompatibilities is crucial to ensuring a stable and efficient SD-WAN environment. Here's a step-by-step approach to fix such problems:

- **Diagnose the Problem:** Before diving into solutions, it's essential to understand the nature of the incompatibility. Use logs, diagnostic tools, and direct observations to identify the specific components causing the issue.

- **Check Version Compatibility:** Ensure that the SD-WAN software/firmware version is compatible with your hardware models. Often, newer software versions come with hardware requirements that older devices might not meet.

- **Hardware Upgrade:** If your current hardware is outdated or not supported, consider upgrading to newer models that are compatible with the SD-WAN solution you're deploying.

- **Downgrade Software:** If upgrading hardware isn't immediately feasible, and a recent software update introduced the incompatibility, consider temporarily downgrading to a previous stable version until you can upgrade your hardware.

- **Consult Vendor Documentation:** SD-WAN vendors typically provide documentation or compatibility matrices that outline which hardware models and software versions work best together. Always refer to these resources when planning updates or deployments.

- **Engage Technical Support:** Reach out to the SD-WAN solution provider's technical support team. They can provide guidance specific to the product you're using and might be aware of workarounds or patches to address the incompatibility.

- **Isolate Incompatible Components:** If only a segment of your network has incompatible hardware or software, consider isolating it temporarily to maintain network stability while you work on a resolution.

- **Test Configurations in a Lab Environment:** Before deploying new hardware or software configurations in a live environment, test them in a controlled lab setting to ensure compatibility.

- **Stay Updated with Vendor Notifications:** Regularly check for notifications or alerts from your SD-WAN solution provider. They often provide early warnings about potential compatibility issues with upcoming updates.

- **Review Change Management Protocols:** Ensure you have a robust change management process in place. Any changes to the network, whether hardware additions or software updates, should go through a review and testing process to catch potential incompatibilities.

Is it my ISP?

Problems with individual Internet Service Providers (like outages or performance degradation) can impact SD-WAN performance, especially if failover mechanisms are not appropriately configured.

Identifying SD-WAN failures specifically related to your ISP can be a bit tricky since SD-WAN inherently involves multiple factors, including equipment, configurations, and the underlay networks (ISPs).

Certain symptoms and tests can help pinpoint ISP-related failures in an SD-WAN environment:

- **Consistent Downtime or Unavailability:** If your SD-WAN connection is frequently down and this downtime coincides with your ISP's outage times, it's a clear indicator of an ISP-related issue.

- **Degraded Performance Metrics:** Monitoring tools can show key metrics like latency, jitter, and packet loss. If you observe a sudden spike in latency or increased packet loss specifically related to one ISP link, it could be an ISP issue.

- **ISP Link Bypass:** Modern SD-WAN solutions can intelligently select the best path for traffic. If you notice that a particular ISP link is consistently being bypassed or not used by the SD-WAN solution, it might be underperforming.

- **Direct ISP Connection Test:** Temporarily bypass the SD-WAN device and connect directly to the ISP link. Running speed tests and ping tests will give you a clear picture of the ISP performance without the SD-WAN overlay. If issues persist in this mode, it's likely an ISP problem.

- **Path Visualization Tools:** Some advanced SD-WAN solutions offer path visualization features that display the health and performance of different paths. This can be useful in identifying if a specific ISP path is experiencing issues.

- **Log Reviews:** Check the logs of your SD-WAN appliance. If there are frequent disconnections or errors related to a specific ISP link, it might point to an ISP-related issue.

- **Alerts and Notifications:** Set up alerts in your monitoring tools for specific performance thresholds. If you receive notifications related to a particular ISP link consistently, it warrants further investigation into that ISP. Applications like CommandLink's ITSM can integrate both services provided by CommandLink and 3rd party vendors enabling you to consolidate and monitor your entire technology stack within a single-pane-of-glass.

- **Compare Multiple Locations:** If you have multiple branches using the same ISP and all of them experience issues simultaneously, it's a strong indication of an ISP-related problem.

- **ISP Communication:** ISPs often send notifications about planned maintenance or outages. Keeping a record of these can help correlate any SD-WAN issues to potential ISP disruptions.

- **ISP Support:** Sometimes, the quickest way to identify an ISP issue is to contact the ISP's technical support. They might already be aware of

network-wide issues or can provide insights into potential problems in your specific location.

To accurately identify SD-WAN failures related to your ISP, it's crucial to have a systematic approach. Regular monitoring, documentation of issues, and proactive communication with the ISP will ensure that you can swiftly identify and address any ISP-related SD-WAN failures.

Do I have a Latency Issue?

Especially relevant for organizations that rely on real-time applications like VoIP or video conferencing. SD-WAN solutions might not always pick the optimal path for such traffic, leading to delays.

Latency issues in your SD-WAN network can lead to sluggish application performance, poor voice/video quality, and delayed data transfers.

Here's how you can identify if you have a latency issue:

- Utilize your SD-WAN's built-in monitoring tools or third-party network monitoring solutions.
- These tools typically provide real-time and historical data on latency across various network paths.
- If your SD-WAN solution supports it, check the latency between different SD-WAN nodes or branches.
- Consistently high latency or sudden spikes compared to baseline values can indicate issues.
- Sometimes, the first indication of a latency issue comes from users. Complaints about slow application performance, choppy voice calls, or video buffering can all be symptoms of latency problems.
- Utilize tools like `ping` to measure the round-trip time for packets between

two points in the network. Running regular ping tests can help determine if there's an increase in latency.

- SNMP Monitoring: Provides detailed metrics about a device's performance, utilization, health, and more. It can fetch information such as bandwidth usage, CPU load, memory usage, device temperatures, interface statistics, and many other performance metrics.

- Use the `traceroute` (or `tracert` on Windows) command to see the path that packets take through the network. This tool can help identify at which hop or node latency might be introduced.

- Modern SD-WAN solutions can choose the optimal path for traffic based on different criteria, including latency. If you observe that traffic is consistently being diverted away from a certain link, it might be due to higher latency on that link.

- Monitor the performance of latency-sensitive applications like VoIP and video conferencing. Tools specific to these services often provide metrics related to jitter and latency.

- APM tools can provide insights into how specific applications are performing, and they often include latency metrics. If applications hosted in certain locations or accessed over specific paths show degraded performance, it could point to latency issues.

- Establish a baseline for normal latency values in your network. Regularly comparing current latency metrics against these baselines can help detect any deviations.

- Reach out to your ISP to see if they're experiencing issues. Sometimes, latency can be introduced outside of your immediate network, especially if the ISP is having routing or infrastructure issues.

- Ensure there are no hardware issues, such as damaged cables or

malfunctioning equipment, which can contribute to increased latency.

- **If you identify a latency issue, you might need to:**

  - Optimize the network path or prioritize latency-sensitive traffic using SD-WAN capabilities.

  - Re-evaluate and possibly upgrade your bandwidth, especially if bandwidth saturation is causing increased latency.

  - Engage with your ISP or switch to a more reliable one if the issue lies with their service.

  - Consider adding direct internet access (DIA) for critical applications to reduce the path and hops they take through the network.

Regularly monitoring and understanding the latency in your SD-WAN environment ensures optimal performance and a better user experience.

Is it a Brownouts?

Sub-optimal performance conditions, such as increased latency or minor packet loss, can degrade the quality of experience without causing a complete outage.

An ISP brownout refers to a temporary reduction or degradation in the quality or speed of internet service. Unlike a "blackout" where the service is completely down or unavailable, during a brownout, the service remains available, but it might not perform optimally or as expected.

Here are some characteristics and causes of an ISP brownout:

- **Reduced Speed:** Users might experience slower than usual download or upload speeds during a brownout. This might manifest as websites taking longer to load, files taking longer to download, or videos buffering more than usual.

- **Increased Latency:** The response times might be higher than usual, which can be particularly noticeable in real-time applications like online gaming or VoIP calls.

- **Packet Loss:** Some data packets might not reach their destination, causing interruptions in streaming, online gaming, or even regular browsing.

- **Jitter:** Variability in latency can cause jitter, which can affect voice and video call quality.

Causes of an ISP Brownout:

- **Network Congestion:** A sudden spike in traffic can overload the ISP's infrastructure, leading to slowed or degraded service. This can happen during major events, product launches, or even cyberattacks.

- **Infrastructure Issues:** Problems like malfunctioning hardware, damaged cables, or issues at data centers can cause intermittent disruptions in service.

- **ISP Throttling:** Some ISPs might intentionally slow down certain types of traffic during peak usage times or when a user exceeds a certain data cap.

- **Maintenance or Upgrades:** Sometimes, ISPs need to perform maintenance or infrastructure upgrades which can lead to temporary service degradations.

- **External Factors:** Natural disasters, large-scale power outages, or even accidents affecting key infrastructure can lead to brownouts.

- **Routing Issues:** Sometimes, the problem might not be with the ISP directly but with one of the intermediary networks or nodes the data passes through.

It's essential for users and businesses to monitor their internet connection quality regularly. Tools like ping, traceroute, or dedicated network monitoring solutions can help identify and quantify brownouts. If brownouts become

frequent, it might be worth discussing the issue with the ISP or considering alternative service providers.

It is a Security Issue?

While SD-WAN can enhance security, misconfigurations or lack of security features (like encryption or firewall capabilities) can expose the network to threats.

Determining if your SD-WAN has been compromised involves looking for indications of unauthorized access, data breaches, or other suspicious activities. Here are some steps and signs to help you determine if your SD-WAN has been compromised:

Is My SD-WAN Compromised?

- **Unusual Traffic Volumes:** An abrupt increase or decrease in network traffic can be a sign of a breach or malicious activity.
- **Odd Traffic Times:** Traffic during off hours, when nobody is expected to be working, can be suspicious.
- Traffic to Unusual Locations: If you notice traffic directed to or from unfamiliar IP addresses, especially those in foreign countries where you don't have business operations, it could be a sign of a compromise.
- Multiple failed login attempts or logins from unfamiliar IP addresses.
- Admin login activity during off-hours.
- Creation of new user accounts or modifications to existing ones without any administrative knowledge can be a sign of malicious activity.
- SD-WAN devices rebooting unexpectedly, failing over to other paths without reason, or configurations reverting to unknown states.

- Unexpected changes to data or applications accessible via the SD-WAN might indicate a compromise.

- Sometimes, external parties like your ISP or partners might notify you of suspicious activity originating from your network.

If you suspect that your SD-WAN has been compromised:

- **Isolate Affected Devices:** Disconnect potentially compromised devices from the network to prevent the spread of malicious activity.

- **Change Credentials:** Reset passwords, especially for administrative accounts.

- **Investigate:** Use logs, traffic analysis, and other diagnostic tools to understand the nature and scope of the compromise.

- **Patch and Update:** Ensure all devices, software, and firmware are patched and updated to the latest versions.

- **Consult Experts:** Consider hiring or consulting with cybersecurity experts to assist in the investigation and remediation.

- **Strengthen Security:** Review and enhance security policies, train employees, and deploy additional security solutions as necessary.

Regular monitoring, timely updates, and adhering to security best practices can significantly reduce the risk of your SD-WAN infrastructure being compromised.

Is it a Last-mile Issue?

The "last-mile" of connectivity (e.g., the connection from a local ISP to a business) can become a bottleneck or point of failure.

Here are some signs that your SD-WAN might have a last-mile issue:

- **High Latency or Jitter:** Experiencing high latency or jitter, especially during peak hours, can indicate last mile congestion or quality issues.
- **Frequent Packet Loss:** Regular or significant packet loss might be a sign of an overloaded or unreliable last mile connection.
- **Inconsistent Bandwidth:** If your network speed fluctuates drastically or doesn't match the bandwidth you're supposed to get, it could be a last mile problem.
- **Connection Drops:** Frequent disconnections or the need to repeatedly reset your connection may point towards last mile issues.
- **Poor Voice or Video Call Quality:** Degraded quality in VoIP calls or video conferencing can be a result of last mile issues affecting real-time data transmission.
- **Slow Website or Application Loading Times:** If accessing websites or cloud based applications is consistently slow, especially during certain times of the day, it might be a last mile problem.
- **SD-WAN Failover Activation:** If your SD-WAN frequently switches over to its failover or backup connections, it might be due to instability in the primary last mile link.
- **ISP-Specific Problems:** Issues that only occur when using a particular ISP can indicate a problem with that provider's last mile infrastructure.
- **Neighbor Complaints:** If nearby businesses or residences using the same ISP also experience similar issues, it’s a strong indicator of last mile problems.
- **Performance Metrics:** Network monitoring tools showing poor performance metrics specifically for the last mile link.

Do I Have Overlapping IP Addresses?

With businesses often merging or connecting multiple networks, IP address overlaps can cause routing issues.

Overlapping IP addresses in SD-WAN environments can lead to routing issues, connectivity problems, and other network anomalies. It's essential to identify and address these issues promptly to ensure optimal network performance.

Here's how to identify SD-WAN overlapping IP address issues:

- **Symptoms of Overlapping IP Addresses:**
    - **Connectivity Issues:** Devices may experience intermittent connectivity or be unable to establish connections with certain network resources.
    - **Routing Anomalies:** Routers or SD-WAN appliances might report routing loops or inability to find a route.
    - **Unexpected Traffic Patterns:** Network monitoring tools may show traffic destined for one subnet getting delivered to another.
    - **Duplicate IP Warnings:** Network devices might report duplicate IP address warnings if they detect another device with the same IP on the network.
- **How to Resolve Overlapping IP Addresses:**
    - **Network Scanning:** Use network scanning tools or IP address management solutions to scan your network and identify IP addresses in use. Cross-reference the results with your allocated IP addresses to find overlaps.
    - **SD-WAN Configuration Review:** Check the SD-WAN device configurations, especially the defined IP subnets for each location. Ensure

there are no overlaps between sites or with other networks (like VPNs) connected to the SD-WAN.

- **Log Review:** Review logs on routers, SD-WAN appliances, firewalls, and other network devices. Look for errors, warnings, or notices related to IP address conflicts or overlaps.

- **Use Diagnostic Tools:** Tools like `ping`, `traceroute`, or `pathping` can help diagnose routing issues related to IP address overlaps. For example, if a `traceroute` to a specific IP takes an unexpected path, it might be due to overlapping IPs.

- **Segmentation Checks:** If you're using network segmentation or VLANs in conjunction with SD-WAN, ensure that IP addresses are appropriately segmented and that no overlaps occur between segments.

- **Re-IP Conflicting Devices:** Change the IP addresses of the devices or subnets causing the overlap.

• **How to avoid IP Address Overlapping:**

- **Implement IP Address Management (IPAM):** Utilize IPAM solutions to manage, monitor, and allocate IP addresses across your network.

- **Regularly Review Address Assignments:** Periodically review and audit IP address assignments across the SD-WAN environment.

- **Documentation:** Maintain updated documentation of IP address allocations across the SD-WAN environment. This helps quickly identify any discrepancies or overlaps.

- **Use NAT:** In cases where overlapping IP addresses can't be avoided (e.g., mergers and acquisitions), consider using Network Address Translation (NAT) to translate overlapping addresses into non-conflicting ones.

- **Collaborate with Teams:** Regularly communicate with IT teams across different SD-WAN sites. Ensuring everyone is aware of allocated IP ranges can help prevent accidental overlaps.

By implementing proper IP address management practices and utilizing network monitoring and diagnostic tools, you can proactively identify and address overlapping IP address issues in your SD-WAN environment.

Is it a Suboptimal Path Selection?

Suboptimal path selection is an issue where your SD-WAN solution isn't choosing the most efficient or best-performing path for your network traffic. It can lead to degraded application performance, increased latency, packet loss, and other unwanted network behaviors.

Here's how to identify if your SD-WAN has a suboptimal path selection problem:

- **Unexpected Latency:** If certain applications or services are experiencing higher latency than expected, it could be due to the traffic being routed through a longer, less optimal path.
- **Uneven Bandwidth Utilization:** Monitoring tools might show that some links are overloaded while others are underutilized, which can indicate an imbalance in path selection.
- **Packet Loss or Jitter:** Excessive packet loss or jitter on a path that is supposed to be the best available route can hint at a path selection issue.
- **Network Monitoring Tools:** Modern network monitoring tools can provide insights into the paths taken by your traffic. If the paths shown are not the shortest or most efficient available, there might be a path selection issue.
- **Path Test Tools:** Use diagnostic tools like `traceroute` or path visualization tools to see the actual path your traffic is taking. Compare this to the

expected or optimal path.

- **Application Performance Degradation:** If specific applications start performing poorly without any other evident reasons, it might be due to them being routed over suboptimal paths.

- **Frequent Path Changes:** If the SD-WAN solution frequently changes paths, even when there isn't a clear reason like a link failure, it might be struggling to select the optimal path.

- **Consistency with Policy Definitions:** Review your SD-WAN policies. If traffic isn't flowing according to your defined policies, there might be a path selection issue.

Suboptimal Path Remediation:

- **Review SD-WAN Policies:** Ensure that your policies are correctly set up to prioritize critical applications and choose the best paths based on your business needs.

- **Calibrate Performance Metrics:** Adjust the metrics (like latency, jitter, loss) used by the SD-WAN solution to make path decisions.

- **Regularly Update SD-WAN Software:** Ensure that your SD-WAN solution is up-to-date, as vendors might release updates that improve path selection algorithms.

- **Use a Centralized Controller:** Some SD-WAN solutions use a centralized controller to make more informed path decisions based on a broader view of the network.

- **Manual Path Override:** If necessary, and if your SD-WAN solution allows, you can manually set preferred paths for specific traffic types or applications.

By regularly monitoring your network and understanding the behavior of your

SD-WAN solution, you can identify and rectify suboptimal path selection issues, ensuring the best performance for your applications and services.

Is it a Cloud Performance Issue?

As businesses increasingly rely on cloud applications, ensuring optimal connectivity and performance between SD-WAN and cloud providers becomes crucial. Misconfigurations or issues with cloud providers can affect SD-WAN performance.

Cloud performance issues in an SD-WAN environment can manifest in various ways, impacting applications and services hosted in public or private clouds. Identifying cloud-specific issues versus other types of network problems is essential for efficient troubleshooting.

Signs you have an SD-WAN cloud performance issue:

- **Cloud vs. On-Premises:** If cloud-based applications are performing poorly while on-premises applications are not, it might hint towards a cloud-specific issue.
- **Different Cloud Providers:** If applications in one cloud provider (e.g., AWS) are impacted but not in another (e.g., Azure), it can indicate a provider-specific issue.
- **Latency Issues:** Increased latency when accessing cloud-based resources when compared to historical data or baseline measurements.
- **Data Transfer Speeds:** Slower upload/download speeds to and from the cloud compared to expected benchmarks.
- **Application Responsiveness:** Cloud-hosted applications may become less responsive, leading to timeouts or slower processing times.
- **Error Rates:** Increased error rates or unusual patterns of errors can be seen in

cloud application logs or dashboards.

- **Path Selection:** If the SD-WAN system is consistently choosing a non-optimal path to route traffic to the cloud, it might indicate a performance issue with the preferred path.

- **Direct Cloud Connectivity Features:** If you're using SD-WAN features like AWS Direct Connect or Azure ExpressRoute and experience performance issues, it might be related to these direct connectivity setups.

Remediation Steps:

- **Review Cloud Resources:** Ensure the resources allocated to your cloud applications (like CPU, memory, bandwidth) are sufficient and not being maxed out.

- **SD-WAN Policy Adjustments:** Modify SD-WAN policies to optimize for cloud traffic, possibly giving it priority or directing it through a faster path.

- **Optimize Cloud Architecture:** Use cloud-native tools and features like load balancers, content distribution networks (CDNs), and regional deployments to distribute and manage traffic efficiently.

- **Engage with Cloud and SD-WAN Providers:** Sometimes, the issue might be on their end, so opening a support ticket can help identify and address the problem.

- **Continuous Monitoring:** Regularly monitor both SD-WAN and cloud performance metrics to catch and address issues proactively.

- **Hybrid Deployments:** If feasible, consider hosting critical applications in both on-premises and cloud environments to provide redundancy and performance optimization.

By regularly assessing the performance of your cloud resources in tandem with

your SD-WAN analytics, you can effectively identify and address any cloud performance issues in your network environment.

Scalability Challenges

As organizations grow, their SD-WAN solution might struggle to scale without performance degradation, especially if not initially set up with growth in mind.

Determining the need for new SD-WAN hardware involves monitoring your network performance, understanding the capabilities of your current hardware, and aligning with your organization's growth and objectives.

Here are some clear indicators that you might need new SD-WAN hardware:

- **Performance Degradation:** If you notice a consistent decline in network performance, increased latency, or frequent downtimes, it might be due to outdated or overburdened hardware.

- **Reaching Capacity:** If your network traffic has increased significantly and you're nearing or consistently hitting your hardware's throughput limits, it's an indication that you need an upgrade.

- **Hardware Failures:** Frequent hardware malfunctions, crashes, or the need for constant reboots are signs that your hardware is potentially reaching the end of its lifecycle.

- **Growth and Expansion:** If your organization is expanding, opening new branches, or expecting a significant increase in network users or traffic in the foreseeable future, it's wise to anticipate hardware needs.

- **Compatibility Issues:** New software versions or other integrated IT tools might not be compatible with older hardware. If you face compatibility challenges, new hardware might be the solution.

Being aware of these common issues can help organizations proactively

address potential challenges and ensure a smooth SD-WAN experience. Proper planning, regular monitoring, and ongoing maintenance are essential to mitigate these challenges.

COMMAND LINK

Some things should be easy to manage.

Get a Demo