THE IT LEADER'S NETWORK MONITORING CHECKLIST

INCREASING VISIBILITY TO REDUCE RISKS

NETWORK MONITORING: BEST PRACTICES

Though modern wireless networks are capable of handling more data than ever, their growing complexity presents significant visibility challenges for enterprise-level organizations. Network blind spots can leave an organization vulnerable in the face of cyber threats, stalled apps, traffic slowdowns and unexpected downtime— all of which can result in millions of dollars in lost revenue and compromised customer relationships.

Network monitoring is an absolutely crucial part of maintaining good enterprise network health. Network monitoring systems constantly survey a computer network for slowdowns and failures, and notify the administrator in the event of a problem. A strong network monitoring plan of action can help you spot and neutralize security threats, network congestion, bottlenecks and other vulnerabilities before they occur.

Wireless network monitoring isn't a passive activity. It requires a sound strategy, proactive planning and ideally, the support of a credible managed service provider (MSP) to get it right. Start strong by checking off all of the following best practices:

UNDERSTAND BASELINE NETWORK BEHAVIOR

Before you can identify problems on the wireless network, you need to know what's normal. Baselining network behaviors over a few weeks or months helps network administrators set thresholds at which alerts must be triggered.

MAKE AN ESCALATION PLAN

If your wireless network has multiple administrators taking care of different aspects (e.g., systems, security, virtualization), establish a policy to govern who should be notified when a problem is detected.

MONITOR EVERY SUB-NET AND SSID

Problems in your wireless network can start anywhere. That's why, in large and complex networks with multiple sub-nets and SSIDs, it's imperative to have eyes on every corner of your WLAN infrastructure.

CONFIRM DEVICE COMPATIBILITY

Does your IT environment include network devices from more than one vendor? If so, you have to make sure you're monitoring them all. Network monitoring tools from equipment vendors tend to focus on their own devices, so make sure all devices are accounted for.

INTEGRATE WITH OTHER TOOLS

All of your network monitoring tools need to be able to work together to provide a holistic view. Check to see whether your tools integrate with data analysis or alert applications to ensure you're not missing any blind spots that can lead to congestion or security vulnerabilities.

PLAN FOR FUTURE GROWTH

How much you can monitor with your system depends on your specific configuration or installation. When setting up a monitoring system, make sure to account for future growth so you don't have to make expensive separate purchases and upgrades as your wireless network grows.

MONITOR THESE METRICS

Once you've laid the groundwork for successful wireless network monitoring, these are the critical metrics you'll want to watch on a day-to-day basis:

- ☐ Availability of network and its devices during business hours, especially peak times

- ☐ Bandwidth utilization by apps and devices, as well as prioritization

- ☐ Network latency, packet loss and retransmission delays

- ☐ Data throughout and percentage of data packets successfully sent

- ☐ Connectivity between nodes and identification of malfunctioning connections that may be impacting peak levels

- ☐ Performance of critical services such as email services, application servers and storage systems

- ☐ Network uptime and bandwidth capacity challenges across multiple sites

- ☐ Condition and uptime of firewalls, antivirus protection, spyware and malware defenses

YOUR WIRELESS NETWORKING STRATEGY STARTS HERE

Forming and implementing a wireless network monitoring strategy is a comparatively small investment of time and money compared to what you risk by ignoring blind spots. If you can't see what's happening in every corner of your network, you're leaving your business exposed to security threats, bottlenecks, costly downtime, customer dissatisfaction and revenue loss. For any organization that relies on a solid IT network to stay up and running, network monitoring is a crucial step towards protecting your valuable business assets.

MANAGEMENT

NETWORK MONITORING

COST

SPEED

SECURITY

VISIBILITY

RELIABILITY
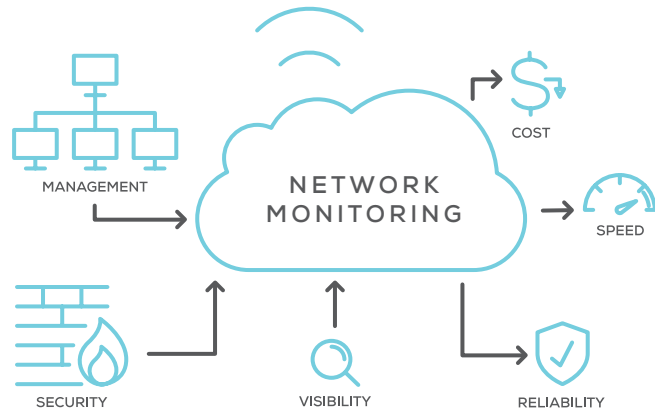
PARTNERING WITH A MWLAN EXPERT

Network monitoring is an ongoing task, so consider working with an MSP who can not only keep an eye on your network 24/7, but also manage all firmware and software upgrades on your behalf. Opting for centralized network management can help free up in-house IT resources and allow your employees to focus on building valuable customer relationships.

With a modern fiber-optic network spanning 180,000 miles across 29 states, Frontier is the provide of choice for Managed Wireless LAN solutions. We are proud to serve 93% of the Fortune 500. Contact us today to see what we can do for your business.

Contact Us

Speak with your Frontier® Business Consultant today.

Find out how Frontier Managed Wireless LAN can help your enterprise power performance without compromise.

877.468.6714

ENTERPRISE.FRONTIER.COM/MANAGED-WIRELESS-LAN