How to future-proof your network for the new AI ecosystem

Managing an enterprise network that can meet the demands of the new AI ecosystem requires a significant mindset shift. Read our checklist of questions to ask on the road to future-proofing your network.

Enterprise IT execs recognize that they need to upgrade their networks to provide the high-bandwidth, low-latency, resilient, secure multicloud connectivity necessary to support anticipated artificial intelligence (AI) traffic requirements.

Although few enterprises are currently building their own large language models (LLMs), generative AI is being embedded into virtually every popular commercial application that enterprise users rely on, from Salesforce Einstein to Microsoft 365 Copilot to Workday Illuminate to Adobe Firefly.

Managing an enterprise network for the demands of the new AI ecosystem requires a significant mindset shift. Organizations need to move beyond a point-to-point or point-to-multipoint mentality and begin thinking about the network as a mesh architecture, a fabric, that provides the appropriate modes of connectivity in a dynamic, flexible, scalable manner.

This fabric, which can include fiber optic waves, Ethernet, IP, and private networking, must have the capacity to connect data centers, cloud service providers, business partners, and sources of LLMs.

Here's a checklist of questions to ask on the road to future-proofing your network:

1. What do I estimate my workload requirements will be in the future?

Bandwidth requirements are constantly increasing as enterprises process more data at the edge, adopt hybrid/multicloud architectures, and deploy more internet of things (IoT) devices. On top of all that, AI workloads bring exponentially higher levels of traffic.

2. Am I thinking about the network in terms of an architecture that enables me to provide layers of demand capability?

One size doesn't fit all when it comes to wide area network (WAN) traffic. Organizations need the ability to match the requirements of the application with the appropriate transit mode.

LUMEN®

CIO

3. Do I understand how to secure AI-driven network traffic?

AI applications often contain an organization's most sensitive data, so all AI-driven traffic requires high levels of protection, including encryption, access controls, and authentication schemes.

4. Do I have visibility into network traffic for troubleshooting and performance optimization?

An LLM can be a black box, so organizations need visibility into AI systems.

5. Am I working with a service provider that has the bandwidth to meet my current needs and can scale when my requirements increase?

Just like there's a scarcity of high-powered GPU chips that power AI systems, there may be an impending scarcity of high-speed fiber. Organizations need to make sure their service provider has the capacity to handle increasing AI traffic requirements.

Conclusion: The Lumen perspective

For organizations on their digital transformation journey, it is clear that in today's environment, every AI strategy needs a cloud and data center strategy, a data strategy, and a network strategy.

Lumen is the network that AI leaders trust. Its Lumen Private Connectivity Fabric℠ offers a future-ready infrastructure that scales with the pace of digital innovation. With robust security measures and comprehensive operational support – including space, power, and network management by national teams – Lumen helps ensure that your business is well prepared for tomorrow's challenges.

Opt for Lumen nationwide deployment to mitigate risks and avoid the uncertainties of self-build projects while benefiting from rapid deployment that helps decrease your time to market. Our holistic approach extends beyond Lumen® Private Connectivity Fabric, delivering a tailored, all-encompassing suite of networking services.

For more information, visit: Lumen.com/PCF.

CIO

LUMEN®