QuanTalk

QUANTUM NETWORKS QUARTERLY DIALOGUE

October -December 2026 | Edition 10

Inside Networking

What does a network controller actually do?

Managing a network isn't just about adding devices. As networks grow across sites, keeping configurations, policies, software and backups consistent becomes a task of its own.

A network controller brings these tasks into one place. Instead of configuring devices individually, administrators can manage supported Access Points, switches and gateways centrally.

What can centralized management handle?

- Deploy network policies across devices
- Automate configuration backups
- Manage software updates
- Monitor devices across multiple sites
- Maintain consistent configurations

Where does Quantum Rudder fit in?

Quantum Rudder is the centralized controller for Quantum Networks infrastructure. It provides a single platform to manage Access Points, Switches and Gateways across sites.

Quantum Rudder can also automate configuration backups, software updates and network policy deployment, reducing repetitive device-by-device administration.

In simple words

Think of it this way:

Managing one device is easy. Managing hundreds of devices across multiple locations is different.

Quantum Rudder puts that work in one place.



Every business has different networking requirements. A hotel may need connectivity across hundreds of rooms, a campus may handle thousands of users, while a manufacturing site may depend on critical systems and IoT devices.

The hardware can be chosen around those requirements. But once everything is connected, how do you keep it secure and under control?

Who gets access? Which devices are allowed? What can they reach? And what happens when something goes wrong?

Without the right controls, even a well-built network can leave gaps:

- Unknown devices can gain access
- Users may get more access than they need
- Security issues can go unnoticed
- Troubleshooting becomes harder

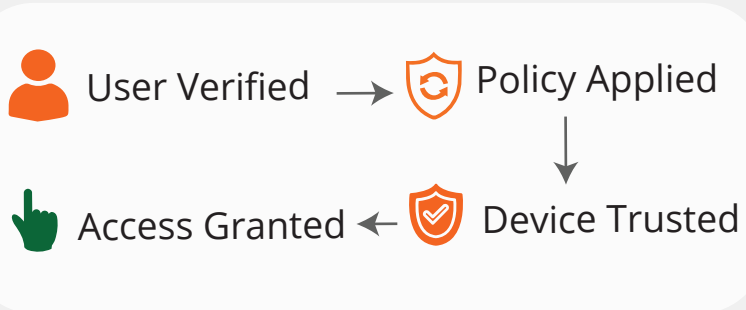
Connectivity gets everything connected. Control decides what happens next.

The answer is not more hardware. It is better control around the hardware already doing the job. QAM (Quantum Access Manager) controls user and device access, while QNMS (Quantum Network Monitoring System) provides visibility into the network and its devices.

What's New?

Simplified Zero Trust Access

Quantum Networks is simplifying Zero Trust access with security controls that work in the background, so users can get the access they need without adding unnecessary steps.



Better security shouldn't mean more inconvenience.

QuanTalk



A user being connected to the network does not mean they should have access to everything on it. Zero Trust Access starts with a simple approach: verify before granting access. It looks at the user, device and context before deciding what that user can access.

Depending on the risk and application, additional controls such as MFA and adaptive authentication can be applied before access is granted. For example, an employee accessing a business application from a managed device on the corporate network may get normal access. The same user connecting from an unknown device or unusual location may be asked for additional verification or denied access. This means users get access to what they need, when they need it and nothing more.

QUANTUM QLASSROOM

Click to know more

Where Learning Begins

More than 3,000 professionals have already been part of the Quantum Qlassroom journey through certifications, technical sessions and hands-on learning.

From wireless fundamentals to troubleshooting and deployment best practices, Qlassroom continues to bring practical networking knowledge closer to the Quantum community.

Have you started your Qlassroom journey yet?

CUSTOMER STORY

Manufacturing

Active Devices On Campus:

REDTAPE

12,000+

RED TAPE is a large campus, spread across 72 acres and 11 buildings, with a workforce of 1,400 and around 600 external visitors every day.

Red Tape was facing connectivity issues across the campus, particularly with roaming, failover and network stability. With thousands of devices relying on the network, these issues could affect important operations.

Quantum Networks deployed Access Points and managed switches across the campus to address these challenges. The deployment restored network stability and connectivity, allowing Red Tape to return to full-capacity operations.

Qafé QUANTUM™ Your Tech Café

Blogs | Webinars | Industry

Why Move Away from Open Networks?

Open Wi-Fi networks are convenient, especially in public spaces, offices and guest areas. However, they do not encrypt wireless traffic or authenticate users by default, leaving connections more exposed to interception and misuse.

As security and compliance requirements grow, organizations are moving towards Wi-Fi access models that offer better protection and control. The right choice depends on whether the network needs encryption, identity verification or both.

Key Takeaways

OWE

(Opportunistic Wireless Encryption)

Encrypts Wi-Fi traffic without requiring users to enter credentials. It protects the wireless connection but does not authenticate users.

Certificate-Based Authentication

Uses digital certificates to verify users or devices, allowing access without shared Wi-Fi passwords.

Identity-Based Access

Applies access policies based on identity, device and role, helping organizations control which network resources users can reach.

Explore more networking insights with Qafé Quantum.

Read the Full Blog