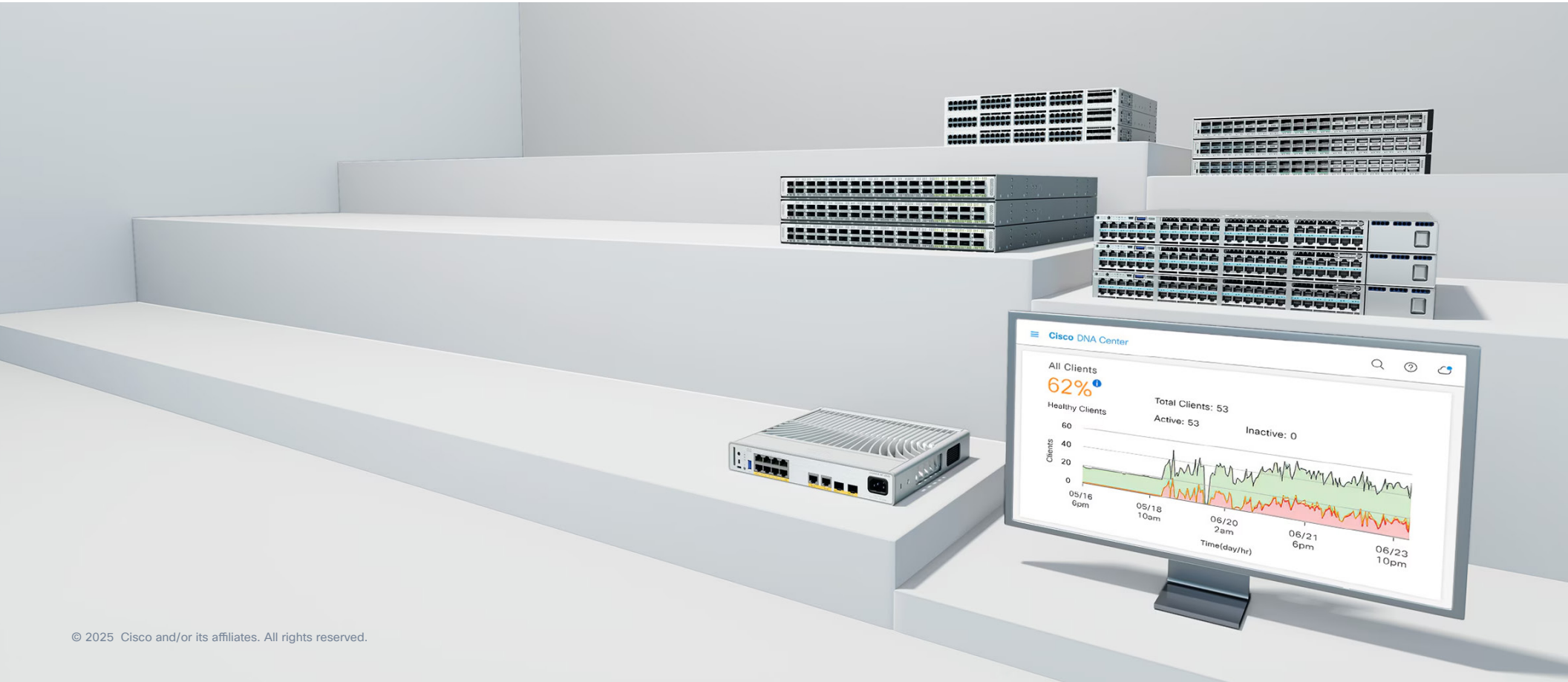
White paper

A Vision for Securing Networks in the Quantum Compute Era

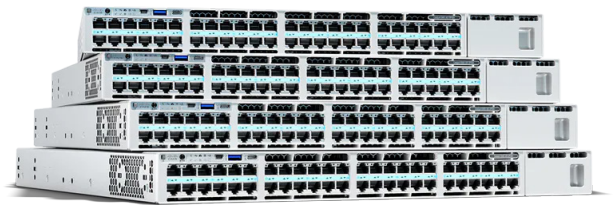


Introduction

Why network security must evolve for the quantum compute era

As quantum computing advances rapidly, it poses a significant threat to current cryptographic methods that protect sensitive data and communications. According to the National Institute of Standards and Technology (NIST), “If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet”[1]. Specifically, quantum computers will have the capability to attack current foundational cryptographic methods, such as RSA, ECC, and Diffie-Hellman (DH), that are the main lines of defense in securing today’s network communications.

One example of such an attack is “harvest now, decrypt later” (HNDL), where secret keys that encrypt data today can be revealed by quantum computers. In this scenario, attackers intercept and store large volumes of encrypted data now, even if they cannot decrypt it immediately, with the intention of decrypting it in the future when quantum capabilities become available. Once the secret keys are revealed, they are used to decrypt the data, exposing personal, industrial, financial, or military secrets. This means that information considered secure today could be at risk years down the line, making quantum compute an emerging threat vector that poses incredible risk and uncertainty to enterprise networks. Both sovereign nations and enterprises acknowledge that this is an emerging risk (and opportunity), and to address this threat, both government agencies and technology vendors are developing post-quantum cryptography (PQC), a new generation of cryptographic algorithms specifically designed to resist attacks from quantum computers.



Quantum leadership and vision

Secure networking is the foundation of modern enterprise operations, and with the rise of the quantum era, organizations are beginning to recognize the urgent need to assess and adapt their security strategies for the quantum era. Network vendors must have the vision to anticipate and stay ahead of evolving quantum threats by building networks designed for long-term resilience. Cisco is committed to a future where network security is inherently robust against the risks posed by cryptographically relevant quantum computers (CRQCs). This commitment includes migrating from classical cryptographic algorithms, which are vulnerable to quantum attacks, to quantum-resistant alternatives. Our vision is closely aligned with industry-wide efforts, particularly following the NIST release of new quantum-resistant cryptographic standards. A comprehensive approach is essential: secure migration planning, rigorous risk assessments, and integration of PQC into a zero-trust security framework are all critical to safeguarding infrastructure. Cisco has long recognized the challenges that quantum computing presents to current encryption methods and is proactively investing in solutions to ensure a secure, quantum-ready future. Now, let's explore how Cisco is turning its vision into a quantum reality.

Quantum research and incubation

> Building a quantum-safe network necessitates a dual approach involving two highly specialized groups.

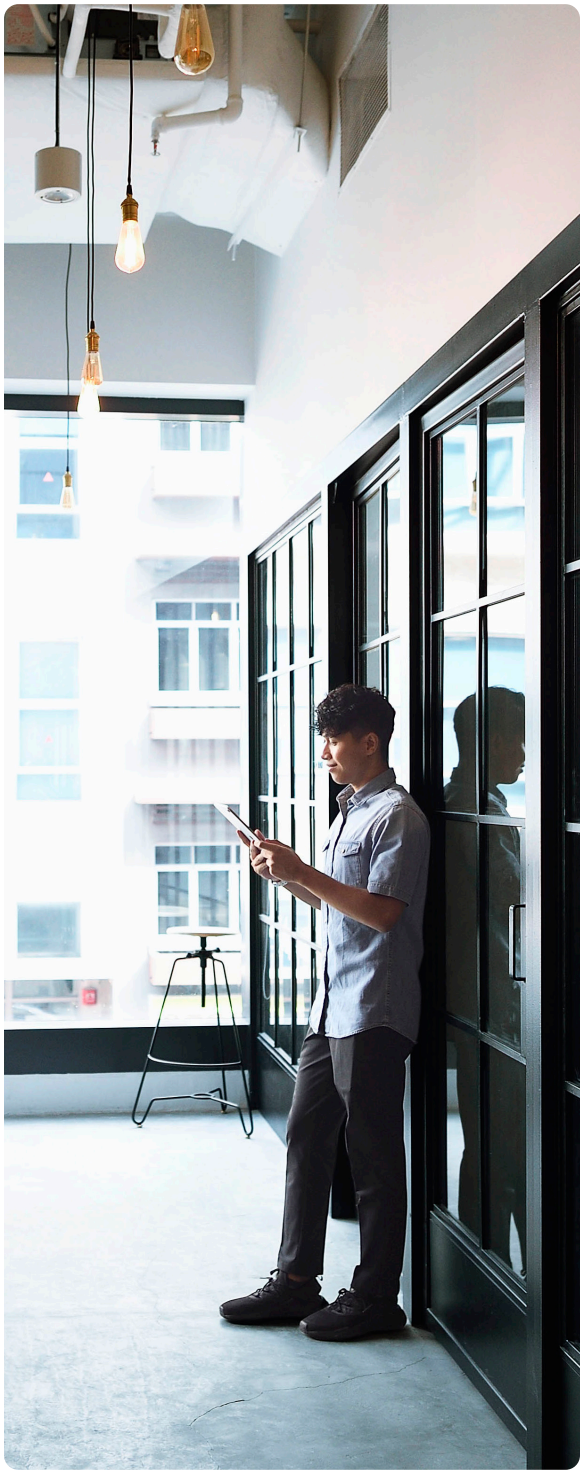
The first group focuses on fundamental research, delving into the theoretical and practical applications of new cryptographic techniques. Areas of focus explored in this research include complex mathematical problems, such as lattice-based, code-based, and hash-based cryptography, which at this time are believed to be intractable for quantum computers. By identifying and validating the next generation of algorithms, this group lays the groundwork for a secure network that can withstand quantum attacks. This research arm also collaborates with global academic institutions to advance state-of-the-art capabilities in this critical field. Cisco Research is proud to have contributed to research across industry and universities worldwide, producing more than 30 papers on quantum technologies.

The second group functions as an incubation engine, transforming research into foundational technology that can be applied to anticipate and address customer needs. Within this group, substantial investment is directed towards the development of quantum-related technologies, including quantum-safe cryptographic algorithms and protocols. Cisco Quantum Labs, as an incubator, actively explores and operationalizes standards, such as the PQC standards set by NIST, ensuring that the resulting solutions Cisco offers are not only theoretically robust but also practical and scalable for real-world deployment.

Securing networking in the quantum era

The quantum era will introduce new challenges that require a fundamental shift in how networks are secured. With its proven legacy as a networking leader, Cisco recognizes that protecting infrastructure integrity is paramount. Examples of Cisco's leadership include the establishment of its Trust Center, as well as its separate Security and Trust Organization (S&TO). The latter is a dedicated group responsible for implementing Cisco Secure Development Lifecycle (CSDL) and ensuring the security and trustworthiness of Cisco products and services. This organization encompasses various teams focused on delivering secure products, responding to security concerns, and maintaining supply chain integrity.

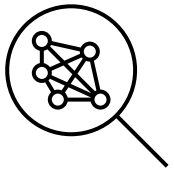
Cisco is taking a comprehensive approach to embedding quantum-resistant technologies deep into the layers of networking—from implementing NIST Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) to fortify the MACsec Key Agreement (MKA) protocol at the MAC layer, to hardening IKEv2 at the network layer, to deploying Cisco Secure Key Integration Protocol (SKIP) that enables quantum key distribution for PQC. Designing a quantum-safe network requires a comprehensive overhaul of cryptographic protocols, algorithms, and hardware components across the entire network stack.



Development and delivery of post-quantum cryptography

Cisco builds on this fundamental research and the company's deep roots in producing trustworthy solutions by developing and implementing quantum-resistant algorithms in its products. In addition to implementing NIST's PQC algorithms, the Cisco roadmap includes compliance with Commercial National Security Algorithm (CNSA) Suite 2.0 standards, expected to be required by 2027–2030, ensuring future-proof, quantum-safe security across Cisco products and infrastructure. The quantum-resistant cryptography technologies listed below are a sample of what is being developed and already available in some Cisco products and solutions, including:

Quantum-safe Secure Boot hardware since 2013: Several Cisco products, including the Cisco 8100 router, Cisco Catalyst 9500 network switch, and Cisco Firewall 4215, already provided quantum-safe Secure Boot using LDWM hash-based signatures (HBS), a precursor to the NIST-approved LMS. Cisco Secure Boot checks for signed images to help ensure that the code running on Cisco hardware has not been modified by a malicious actor.[2]



Active implementation of NIST post-quantum cryptography standards: Cisco is actively contributing to PQC standards and implementing into its products and solutions NIST-approved ML-KEM, as specified in NIST FIPS 203, and module-lattice-based digital signature algorithm (ML-DSA), as specified in NIST FIPS 204.

Quantum-safe security today for select Cisco devices: Cisco has implemented IETF RFC 8784, "Mixing Pre-Shared Keys in IKEv2," an extension to the IKEv2 protocol that allows the use of post-quantum pre-shared keys (PPKs) to strengthen security against quantum computer attacks. This feature is available on several Cisco devices, such as the Cisco 1000 Series Integrated Services Routers and Cisco Catalyst 8500 Series Edge Platforms with Cisco IOS XE 17.12.1a. Additionally, Cisco has developed its Secure Key Integration Protocol to enable the secure distribution of PPKs, a critical component for delivering quantum-safe keys to Cisco devices.[3]

Continued collaboration with standards organizations: As the major contributor to the IETF RFC 8784 standard, Cisco will continue to lead innovation and deployment of quantum-safe networking. Cisco Research, Cisco Quantum Labs, Cisco Security and Trust Organization, and Cisco product groups will continue to work closely with NIST, IETF, research groups, academia, and other industry groups to collaborate, contribute, validate and integrate standardized PQC algorithms into its solutions. This ensures interoperability and robust security aligned with emerging federal and international standards.

Conclusion

Building for the future

Network vendors must exhibit both leadership and vision as they navigate the challenges of the post-quantum cryptography era. This journey demands a strong commitment to ongoing research, the thoughtful implementation of PQC solutions, and the adoption of agile, standards-based security practices. By taking these proactive steps, vendors can lay the essential groundwork for resilient and secure networks that can withstand the advancements of quantum computing. For nearly four decades, Cisco has set the standard for innovation and security in networking, and today, the company is once again at the forefront: Cisco leads the way in protecting your network for the quantum future.

Notes

1. *Post-Quantum Cryptography*, National Institute of Standards and Technology, September 2025
2. *Quantum Cryptography: What's Coming Next*, Cisco, November 2024
3. *Security and VPN Configuration Guide*, Cisco IOS XE 17.x, Cisco, January 2021

Future-proof your critical infrastructure

To learn more about the latest Cisco innovations in secure, quantum-ready network infrastructure, explore our comprehensive solution portfolio. Unlock the performance, security, and intelligence you need to power real-time and AI-driven applications across campus, branch, and industrial environments.

Visit here to learn more:
https://www.cisco.com/site/us/en/solutions/networking/campus-branch-networking/index.html