Future-Proofing Secure WAN

Fabric Security and Navigating the Quantum Threat with PQC

Ahmet Uncu
Global SE

BRKENT-2915

Webex App

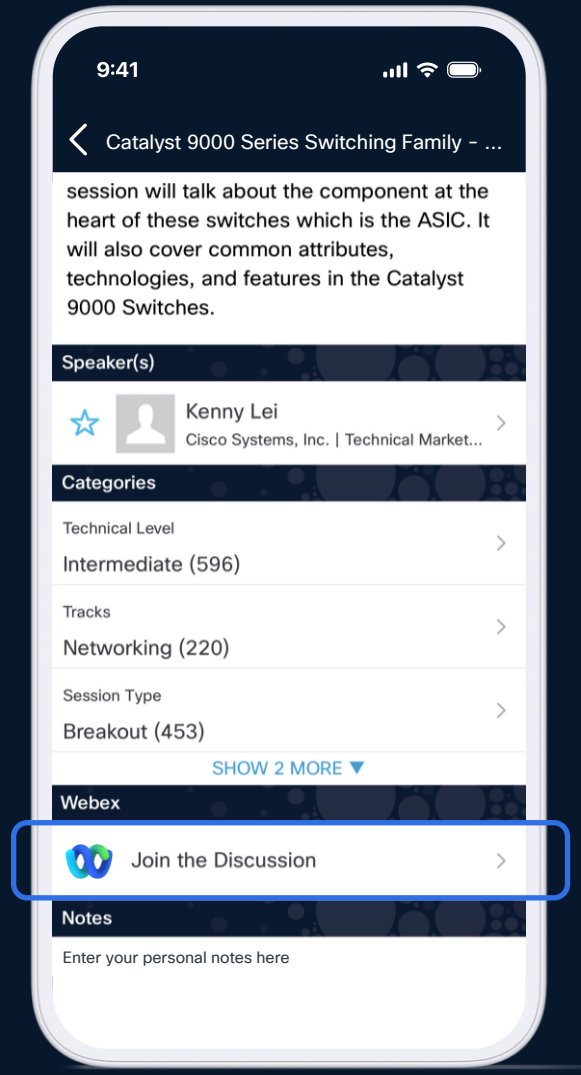
Questions?

Use Webex App to chat with the speaker after the session

How

1. Find this session in the Cisco Events App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 27, 2026.



© 2026 Cisco and/or its affiliates. All rights reserved.

Agenda

01 **Demystifying PQC**

What, Why, and How

02 **The Quantum Threat**

How Attackers Are Preparing and What's at Risk

03 **Preparing Your WAN for the Quantum Era**

How Cisco Supports Your Quantum-Safe Journey

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Demystifying PQC
What, Why, and How

CISCO Live !

Year 2000 Problem



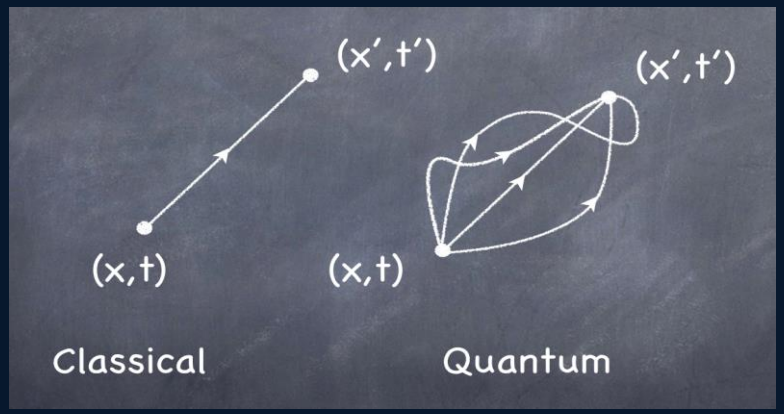
Important Terms to Know

Quantum-resistant	• Focuses specifically on resisting quantum attacks, often tied to specific algorithms. Algorithms that are believed to resist quantum attacks.
Quantum-safe	• Encompasses a holistic assurance of security against quantum threats, potentially including systems and implementations.
Post-Quantum Cryptography (PQC)	• A cryptographic discipline developing algorithms for a quantum future. NIST standardized algorithms (FIPS 203, 204, 205) sit here.
Hybrid (PQ/T)	• Refers to the combination of traditional cryptographic algorithms (such as Diffie-Hellman) with post-quantum cryptographic (PQC) algorithms (like ML-KEM). Both methods run side by side and their outputs are combined.
Crypto Agility	• The ability of a cryptographic system to easily switch between encryption algorithms or key sizes, ensuring adaptability to new security needs.

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

What Are Quantum Computers?



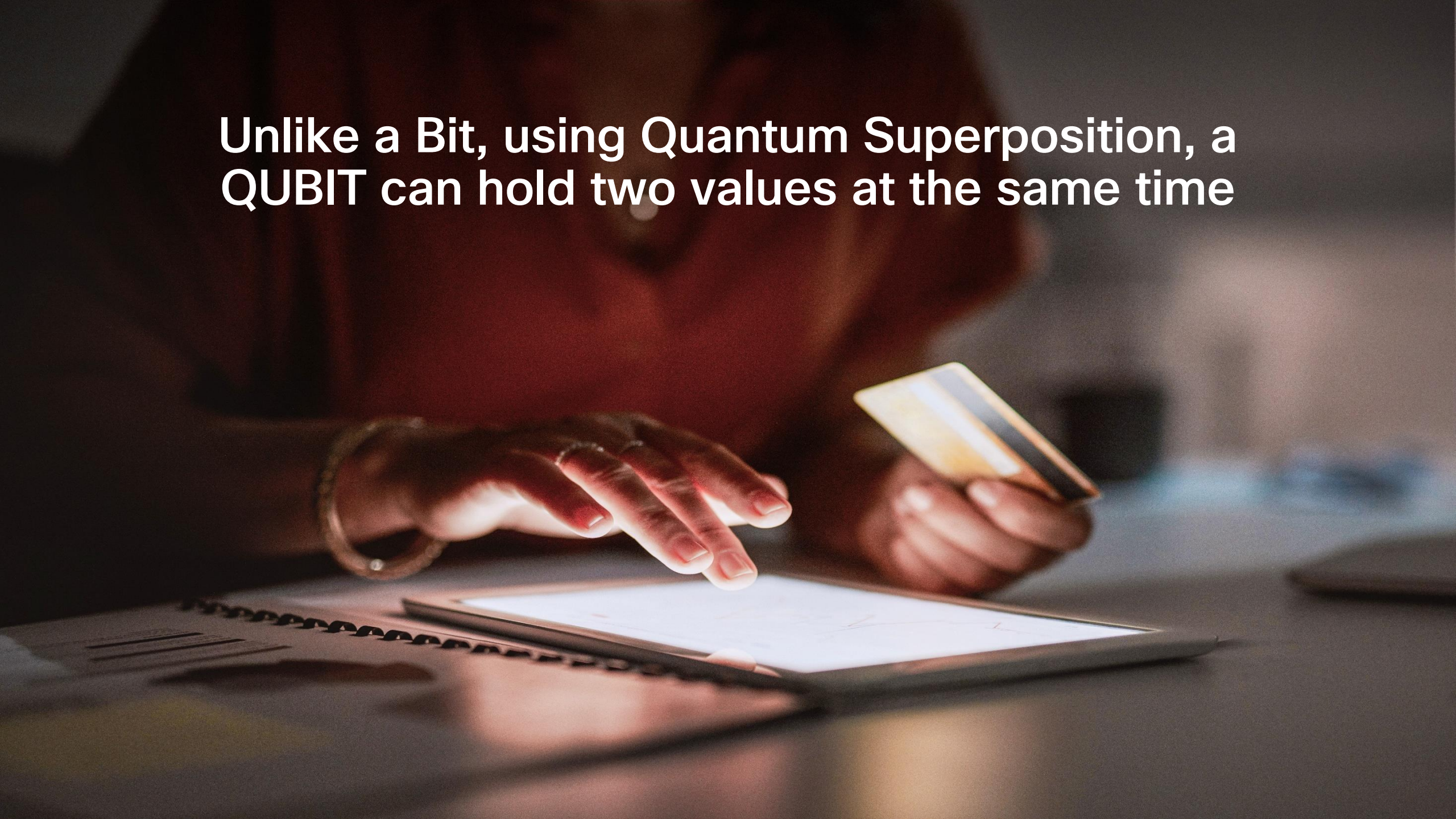
Supercomputers

- Based on binary values of bits 0 or 1
- Can compute values in parallel one at a time
- Takes multiples tries to solve a problem

Quantum computers

- Based on qubits ,which exists in 0 and 1 at the same time
- Quantum computers can process multiple values at the same time
- The processing power and speed needed to process data diminishes significantly

© 2026 Cisco and/or its affiliates. All rights reserved.


Unlike a Bit, using Quantum Superposition, a
QUBIT can hold two values at the same time


Let's Make an Exercise Together
The Power of Exponential Growth

How Fast Quantum-Style Scaling Grows

Imagine we give €**1** to the first person.

With **bits**, everyone adds €1. However, with **qubits**, each subsequent person doubles the money received from the previous person.

Person	Bits	Qbits
1	1€	1€
2	2€	2€
10	10€	512€
20	20€	524,288€
30	30€	536,870,912€
44	44€	8,796,093,022,208€ (≈ 9 trillion)

© 2026 Cisco and/or its affiliates. All rights reserved.


The Quantum Threat
How Attackers Are Preparing and What's at Risk
CISCO Live !

Cryptographically Relevant Quantum Computers (CRQC)

- A Cryptographically Relevant Quantum Computer (CRQC) is a future generation of quantum computer powerful enough to break the public-key encryption systems that secure our digital world today.

The Challenges- (Why it is not yet available)

- The Scale Gap
- Environmental Sensitivity
- Error Correction Overhead
- Engineering Complexity

© 2026 Cisco and/or its affiliates. All rights reserved.

How Quantum Computers Break Today's Cryptography

Shor's Algorithm

- The primary threats to current cryptographic systems come from two key quantum algorithms: Shor's algorithm, which can efficiently factor large integers and solve discrete logarithm problems.

Algorithm	Based On	Classical Time (e.g., 2048 bits)	Quantum Time (Future)
RSA	Integer Factorization	~10^{20} years (secure)	~1 day (with 4,000 logical qubits)
DH	Discrete Log	~10^{20} years	~1 day
ECC	Elliptic Curve Log	~10^{8} years (for 256-bit curve)	~1 hour

https://blogs.cisco.com/developer/how-post-quantum-cryptography-affects-security-and-encryption-algorithms

© 2026 Cisco and/or its affiliates. All rights reserved.

How Quantum Computers Break Today's Cryptography

Grover's Algorithm

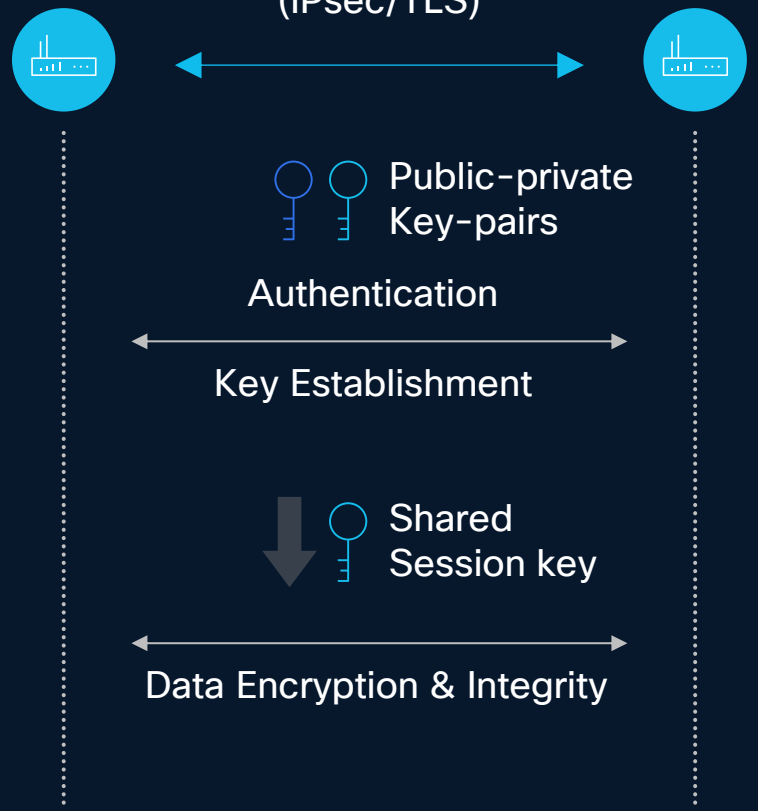
- Quantum computers can use Grover's algorithm to speed up brute-force attacks against symmetric encryption. The practical implication is that quantum computers effectively halve the security strength of symmetric encryption algorithms.

AES Key Size	Grover's Effective Attack	Effective Key Strength
AES-128	~2^{64} operations	Equivalent to 64-bit key
AES-256	~2^{128} operations	Equivalent to 128-bit key

https://blogs.cisco.com/developer/how-post-quantum-cryptography-affects-security-and-encryption-algorithms

© 2026 Cisco and/or its affiliates. All rights reserved.

Quantum Computing's Impact on Cryptography



Quantum-Resistant?

Asymmetric Cryptography

- Based on mathematically related public-private key-pairs
- Used for control plane operations
  - Authentication, Key establishment
- Example: RSA, DH, ECC

Large reliable Quantum computers can break RSA, DH, ECC!

Symmetric Cryptography

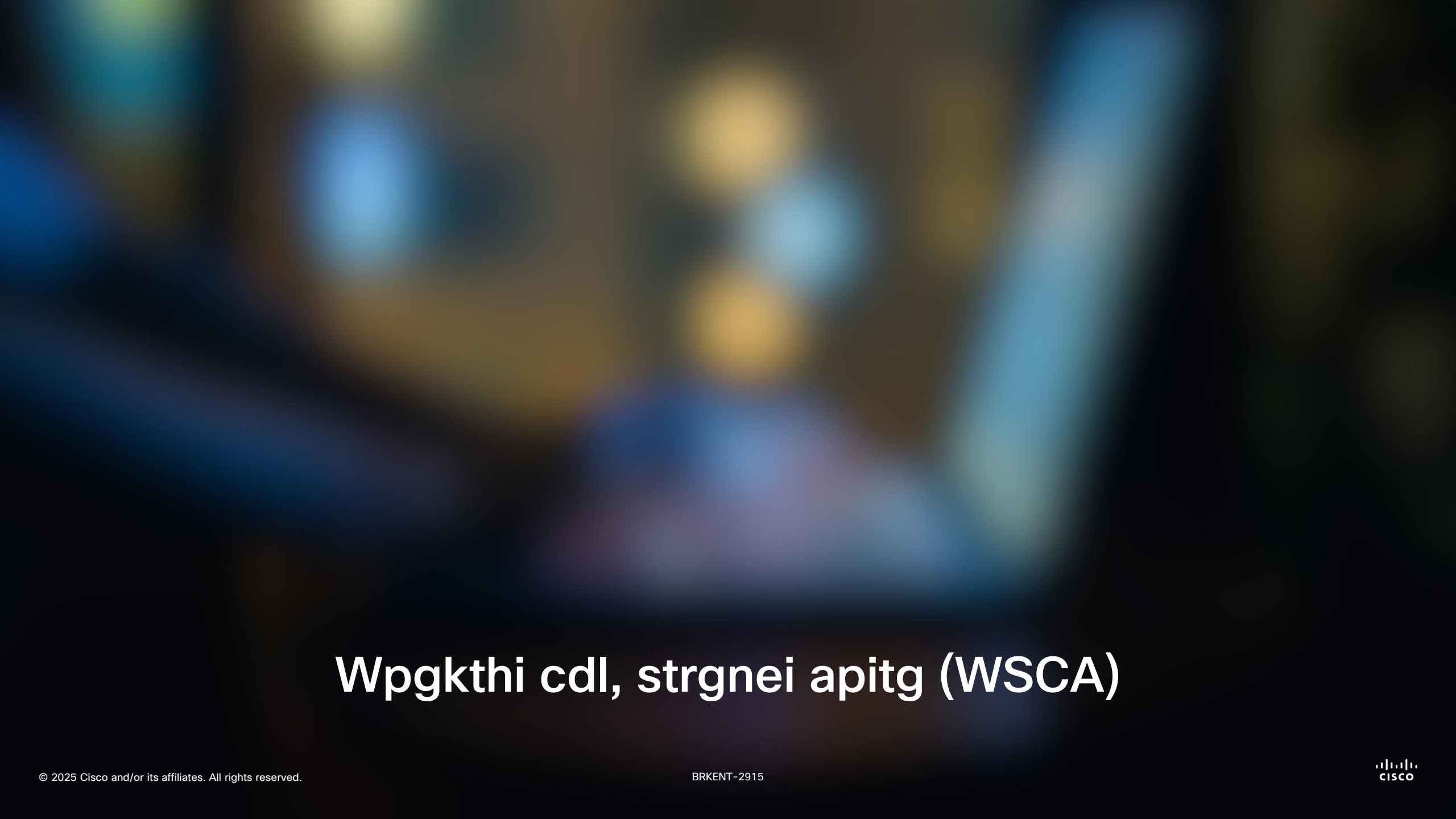
- Based on shared key
- Used for bulk data encryption & integrity
- Protection level based on key strength
  - Key size & entropy
- Example: AES-GCM

Symmetric crypto with large and high-entropy keys is resistant to Quantum computer attacks

© 2026 Cisco and/or its affiliates. All rights reserved.

Q-Day

© 2026 Cisco and/or its affiliates. All rights reserved.



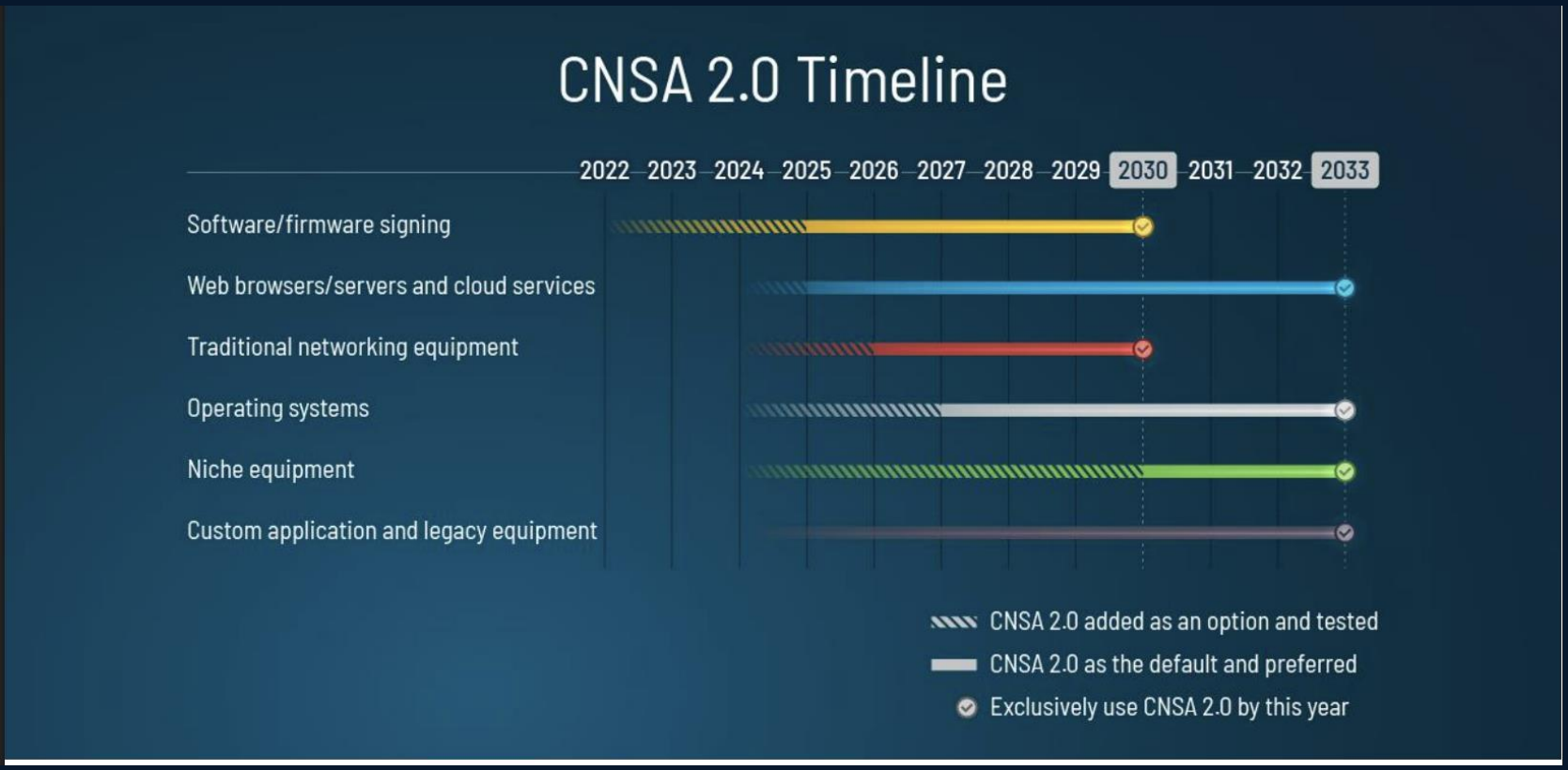
© 2025 Cisco and/or its affiliates. All rights reserved.

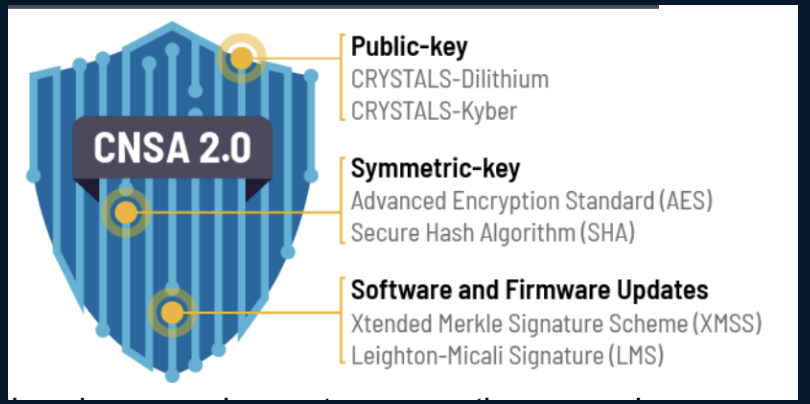


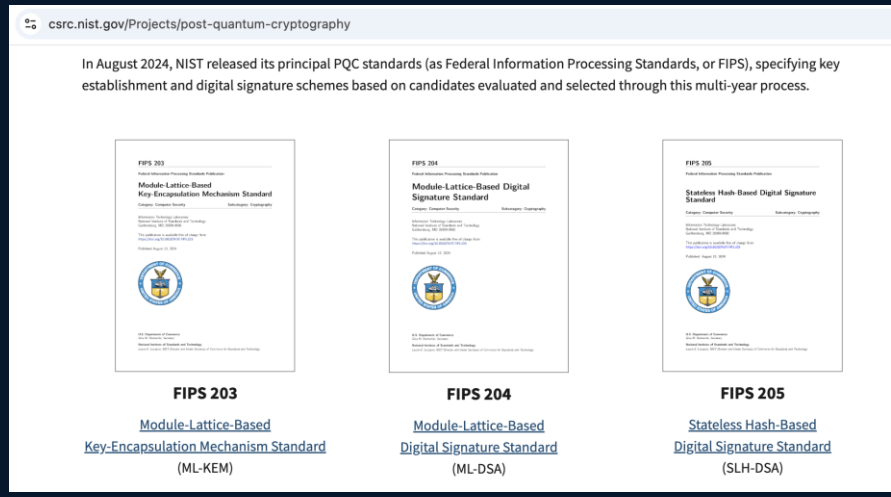
Harvest now, decrypt later (HDNL)

© 2025 Cisco and/or its affiliates. All rights reserved.

PQC Transition Timelines







© 2026 Cisco and/or its affiliates. All rights reserved.

NIST Quantum-Safe Algorithms

ML-KEM (FIPS 203)

- Based on CRYSTALS-Kyber
- Lattice-based
- Secures the exchange of keys over untrusted medium

ML-DSA (FIPS 204)

- Based on CRYSTALS-Dilithium
- Lattice-based
- Digital signature scheme for authenticity and integrity of data

SLH-DSA (FIPS 205)

- Based on SPHINCS+
- Stateless hash-based
- Digital signature scheme for authenticity and integrity of data

FN-DNA (FIPS 206) Draft

- Based on FALCON
- Lattice-based
- Digital signature scheme for authenticity and integrity of data

ML-KEM Use Cases

- Securing web connections
- VPN session key establishment

ML-DSA Use Cases

- Signing software and updates
- Secure boot
- Authenticating digital docs

SLH-DSA Use Cases

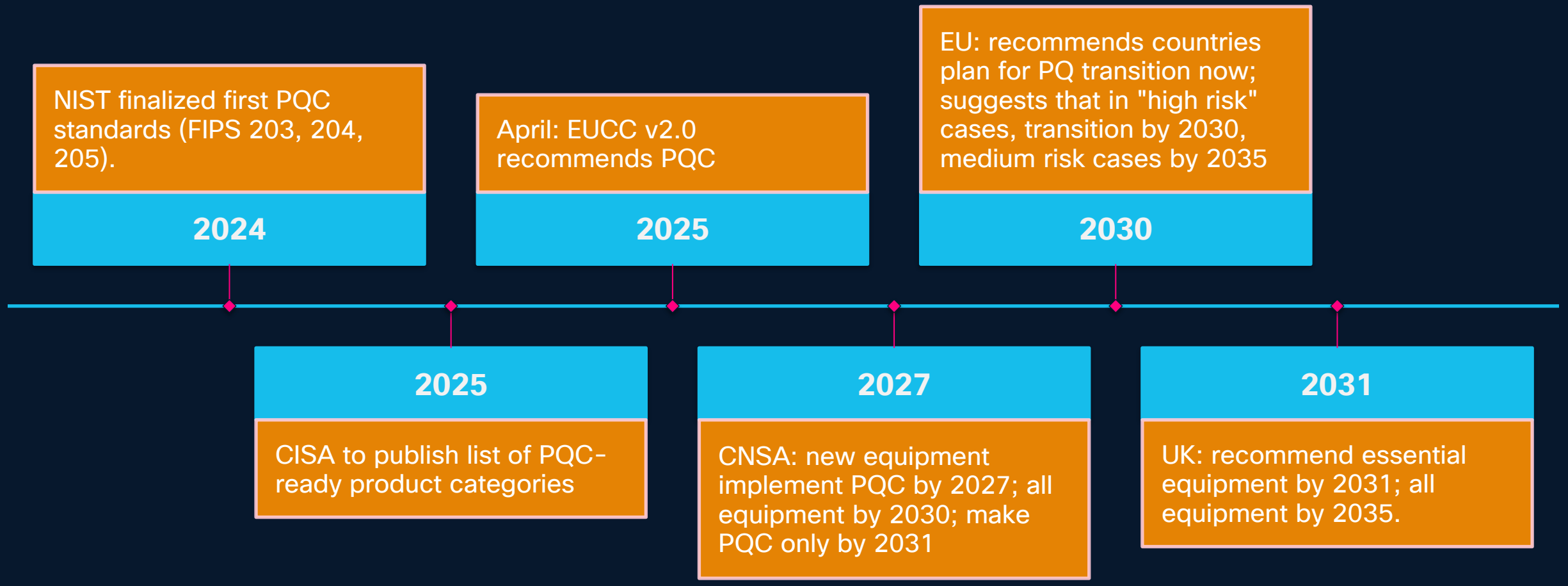
- Ultimately the same as ML-DSA but uses different cryptographic method

HQC (Draft)

- Serves as a backup for ML-KEM to diversify outside lattices
- Code-based (decoding random linear codes problem)

© 2026 Cisco and/or its affiliates. All rights reserved.

PQC Transition Timelines



© 2026 Cisco and/or its affiliates. All rights reserved.

Preparing Your WAN for the Quantum Era
How Cisco Supports Your Quantum-Safe Journey

CISCO Live !

Cisco SD-WAN Fabric Security – The Foundation



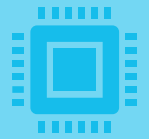
Integrity: Hardware-Anchored Trust

Uses the Trust Anchor module (TAm) to provide a hardware-level root of trust, ensuring that only authentic Cisco hardware and unmodified software can initialize.



Authentication: Zero-Trust Identity

Verifies every device and controller using a unique Secure Unique Device Identifier (SUDI) and automated PKI to ensure only authorized entities join the fabric.



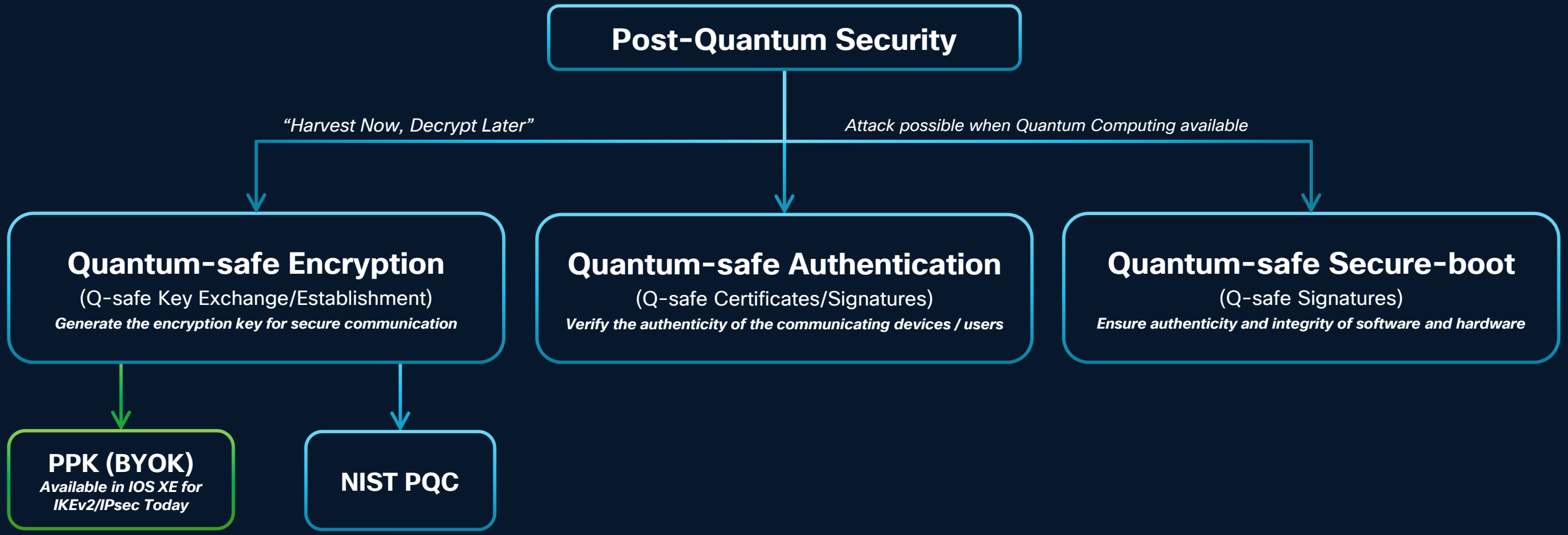
Privacy: Secure Control and Data Planes

TLS/DTLS connections for controllers and AES-256 IPsec for secure data plane communication.

© 2026 Cisco and/or its affiliates. All rights reserved.

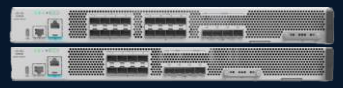
cisco

PQS Components



© 2026 Cisco and/or its affiliates. All rights reserved.

PQC with Cisco 8000 Series Secure Routers

Small Branch	Medium Branch	Large Branch	Campus Site	Data Center
				
Cisco 8100 Series Secure Router	Cisco 8200 Series Secure Router	Cisco 8300 Series Secure Router	Cisco 8400 Series Secure Router	Cisco 8500 Series Secure Router

- ✓ Manual and QKD based PPK solutions are supported on Catalyst 8000 Series Edge Platforms as well as Cisco 8000 Series Secure Routers
- ✓ Cisco 8000 Series Secure Routers will support NIST PQC solutions

© 2026 Cisco and/or its affiliates. All rights reserved.

Quantum-safe Crypto with ‘secure networking processor’

Security

- Inline Crypto
- PQ capable crypto engine
- Cisco Secure Firewall acceleration
- Built-in AI/ML Engine



Networking

- Integrated Hardware Accelerators
- Built-in Ethernet Controller
- Performance defined Power 30%+ power saving
- Programmable uCode

© 2026 Cisco and/or its affiliates. All rights reserved.

Protect your WAN from quantum attacks



Post-quantum Preshared Keys

- Manual PPK
- Dynamic PPK



Post-quantum Cryptography (PQC) Algorithms

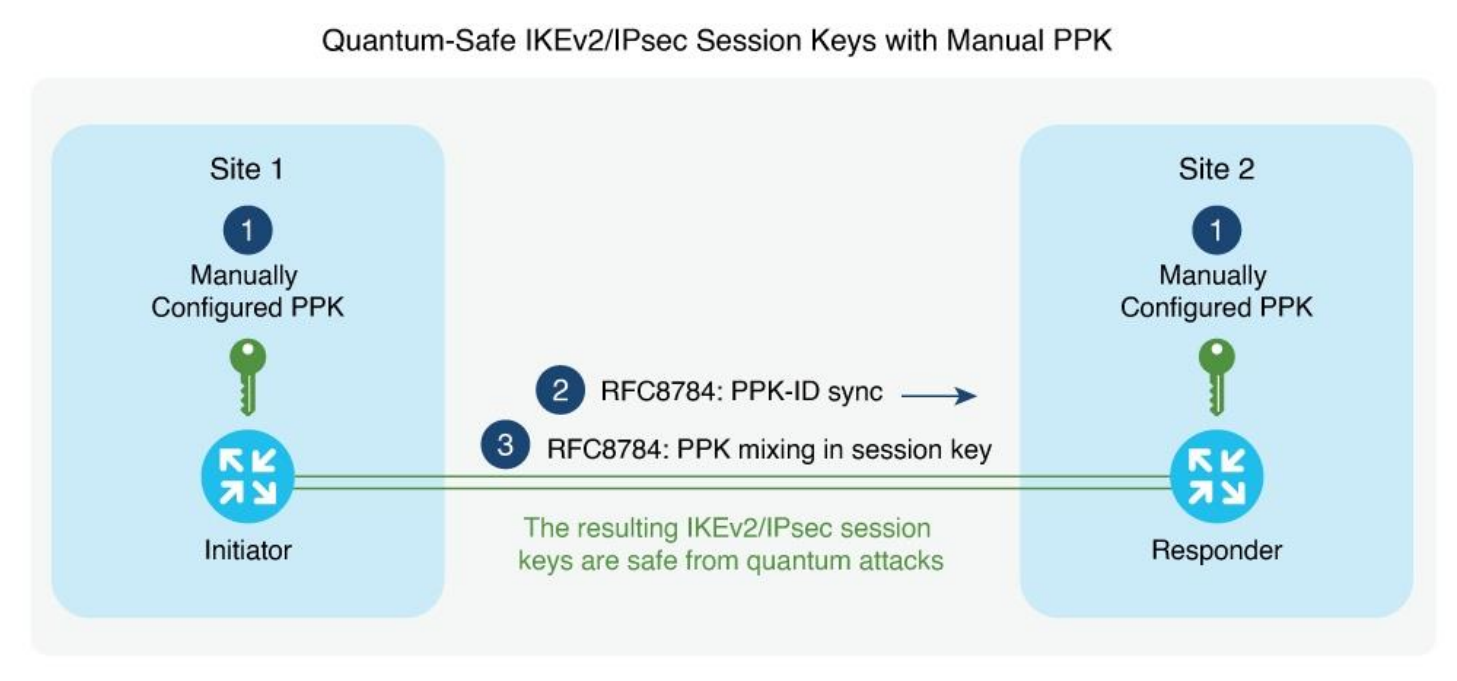
- ML-KEM (FIPS-203): Encryption
- ML-DSA (FIPS-204): Authentication
- LMS (NIST SP 800-208): Secureboot

© 2026 Cisco and/or its affiliates. All rights reserved.

Post-Quantum Pre-shared Keys (PPK)

Available Today

Manual Configuration



From Cisco IOS XE Release 17.12.1a	From Cisco IOS XE Release 17.11.1a
Cisco 1000 Series Integrated Services Routers	Cisco Catalyst 8000V Edge Software
Cisco Catalyst 8500 Series Edge Platforms	Cisco Catalyst 8300 Series Edge Platforms
	Cisco ASR 1000 Series Aggregation Services Routers

© 2026 Cisco and/or its affiliates. All rights reserved.

Manual Postquantum Preshared Keys

Manual - Configuration

```
crypto ikev2 keyring ppk-keyring
ppk manual id ppk_id key key
!
crypto ikev2 profile prof
keyring ppk ppk-keyring
!
crypto ipsec profile prof
set ikev2-profile prof
!
interface Tunnel0
tunnel protection ipsec profile prof
!
```

Configuration snippet only. Check official guide for full details.

https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m-sec-cfg-quantum-encryption-ppk.html

© 2026 Cisco and/or its affiliates. All rights reserved.

Manual Postquantum Preshared Keys

Manual - Verification

```
Router# show crypto ikev2 sa detailed

IPv4 Crypto IKEv2  SA

Tunnel-id       Local                Remote               fvrf/ivrf         Status
   3        <src IP>/SrcPort     <Dst IP>/DstPort            none/none        READY

     Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: PSK, Auth verify: PSK, QR

!!! omitted output !!!

Quantum-safe Encryption using Manual PPK
```

https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m-sec-cfg-quantum-encryption-ppk.html

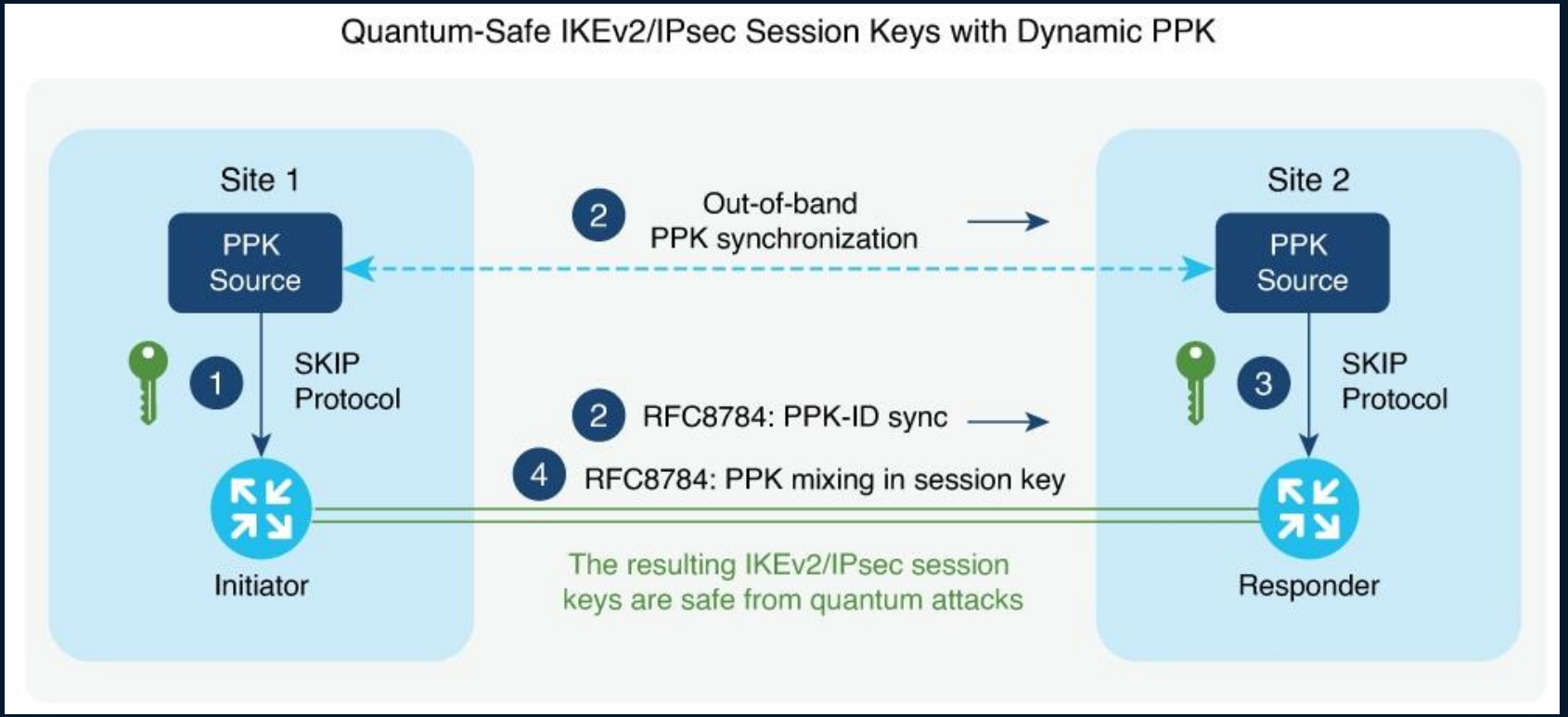
© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

PPK from Quantum Key Distribution (QKD)

Available Today

Using Secure Key Integration Protocol (SKIP)



© 2026 Cisco and/or its affiliates. All rights reserved.

PPK from Quantum Key Distribution

SKIP - Configuration

Configuration snippet only. Check official guide for full details.

```
crypto skip-client skip-client-cfg
server ipv4 10.10.0.4  port 9991
psk id psk-id1 key 0 cisco123
!
crypto ikev2 keyring ppk-keyring
peer 1
address 10.10.0.1 255.255.255.0
ppk dynamic skip-client-cfg
!
crypto ikev2 profile prof
match identity remote address 10.10.0.1
authentication local pre-share key cisco
authentication remote pre-share key cisco
keyring ppk ppk-keyring
```

https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m-sec-cfg-quantum-encryption-ppk.html

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

PPK from Quantum Key Distribution

SKIP - Verification

```
Router# show crypto ikev2 sa detailed

IPv4 Crypto IKEv2  SA

Tunnel-id       Local               Remote              fvrf/ivrf         Status
  3        <src IP>/SrcPort     <Dst IP>/DstPort           none/none        READY

      Encr: AES-GCM, keysize: 256, PRF: SHA256, Hash: None, DH Grp:20, Auth sign: PSK, Auth verify: PSK, QR

!!! omitted output !!!

Quantum-safe Encryption using Dynamic PPK
```

https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m-sec-cfg-quantum-encryption-ppk.html

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

PQC Solution using Quantum-safe algorithms

Available on 26.1

26.1.1 in autonomous mode Cisco 8000 Series Secure Routers supports a comprehensive quantum-safe encryption approach for WAN technologies.

Enabled Solutions:

- IKEv2 IPsec VPNs
- DMVPN & FlexVPN
- MACsec [EAP-TLS]
- Secure Shell (SSH)

© 2026 Cisco and/or its affiliates. All rights reserved.

ML-KEM for IKEv2 IPsec, DMVPN, and FlexVPN



- The ML-KEM algorithm provides a consistent security framework across all VPN architectures, including standard IKEv2 IPsec, DMVPN, and FlexVPN.
- Across these diverse deployment scenarios, ML-KEM functions to establish a quantum-resistant key exchange during the IKEv2 negotiation process.
- Enabling ML-KEM in the IKEv2 proposal extends this quantum-resistance to both hub-spoke and dynamic spoke-to-spoke tunnel establishments for DMVPN and FlexVPN.
- This ensures that the cryptographic keys used for encrypting and authenticating VPN traffic are fortified against potential future attacks from quantum computers.

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Quantum-safe algorithms

PQC ML-KEM for IKEv2 - Configuration

- IKEv2 Proposal

Defines cryptographic parameters (encryption, integrity) and enables PQC via the ake mlkem command for the initial key exchange.

- IPsec Profile

Binds the security policy to the tunnel interface and enables optional Perfect Forward Secrecy (PFS) for unique key generation per negotiation.

```
crypto ikev2 proposal ikev2proposal
 encryption aes-cbc-256
 integrity sha512
 group 21
 ake mlkem1024 required          Strict enforcement
!
crypto ipsec profile ipsec_profile_vti
 set pfs pqc-only
```

Configuration snippet only. Check official guide for full details.

© 2026 Cisco and/or its affiliates. All rights reserved.

Quantum-safe algorithms

PQC ML-KEM for IKEv2 - Verification

```
Router# show crypto ikev2 sa

IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         1.1.1.2/500           1.1.1.1/500           none/none            READY

      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      AKE group: AKE1: MLKEM1024
```

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

MACsec EAP-TLS 1.3 and (PQC)

Available on 26.1

ML-KEM for MACsec

- Combines line-rate MACsec Layer 2 encryption and data integrity with EAP-TLS
- Integrates TLS 1.3 and Post-Quantum Cryptography (PQC)
- A PQC key-exchange algorithm is negotiated if both endpoints are PQC-enabled and supported; otherwise, the session falls back to classic algorithms.

Configuration snippet only. Check official guide for full details.

```
eap profile EAP-PROFILE
method tls
!
!
access-session tls-version all
!
access-session pqc-type pqc
!
interface <interface-id>
 macsec
 authentication periodic
 authentication timer reauthenticate interval
```

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Management Plane

Available on 26.1

ML-KEM for SSH

Key Exchange Algorithms (KexAlgorithm) algorithms securely establish the shared secret key between the client and server used to encrypt the entire communication session. To defend against future quantum threats, new ML-KEM (Module-Lattice-based Key Exchange Mechanism) algorithms are now implemented in IOS-SSH.

- Available ML-KEM Algorithms for Configuration:
  - mlkem1024nistp384-sha384
  - mlkem768x25519-sha256
  - mlkem768nistp256-sha256

© 2026 Cisco and/or its affiliates. All rights reserved.

Management Plane

ML-KEM for SSH Configuration -Verification

```
Router(config)# ip ssh server algorithm kex ?
  mlkem768nistp256-sha256     MLKEM768NISTP256-SHA2 key exchange algorithm
  mlkem1024nistp384-sha384    MLKEM1024NISTP384-SHA2 key exchange algorithm
  mlkem768x25519-sha256       MLKEM768x25519-SHA2 key exchange algorithm
```

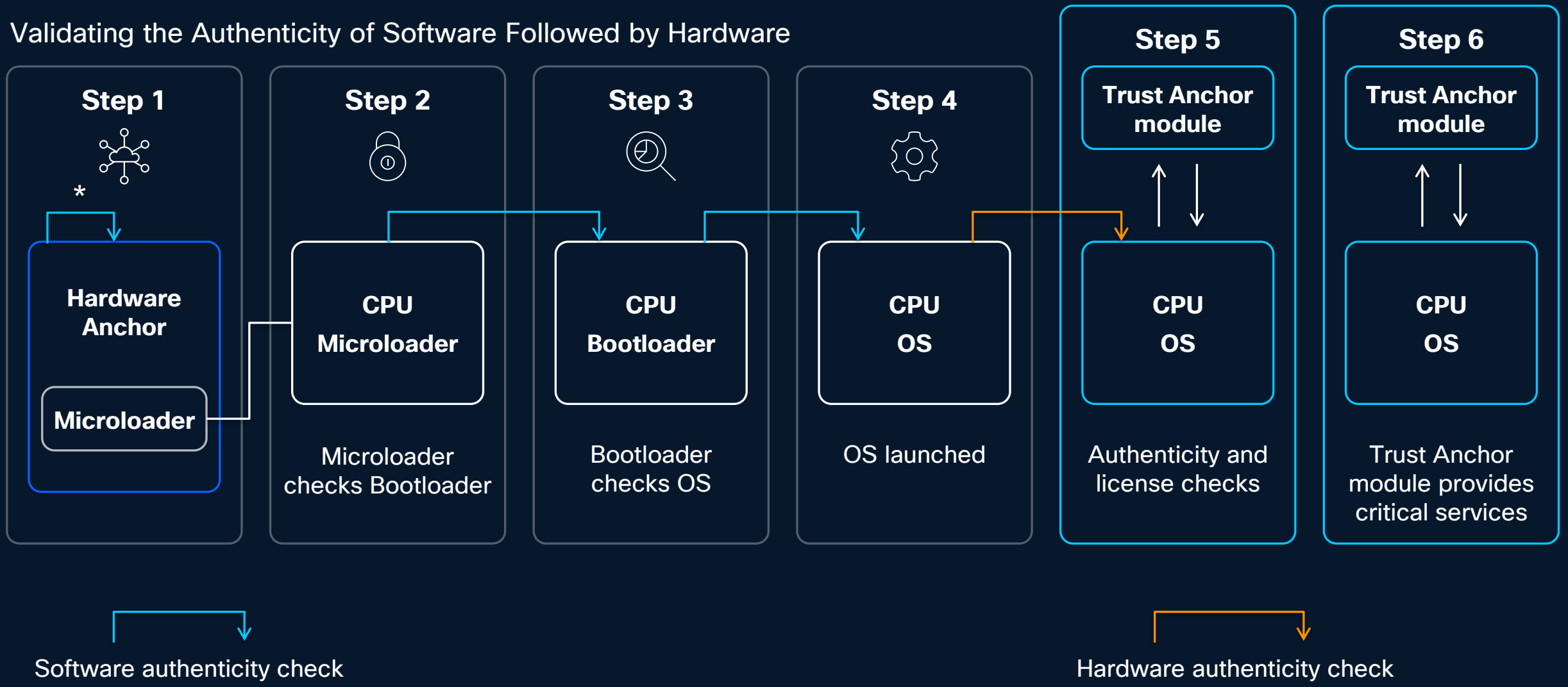
Configuration snippet only. Check official guide for full details.

```
Router#sh ip ssh
SSH Enabled - version 2.0

KEX Algorithms:mlkem1024nistp384-sha384,mlkem768nistp256-sha256,mlkem768x25519-sha256
.....
```

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Secure Boot



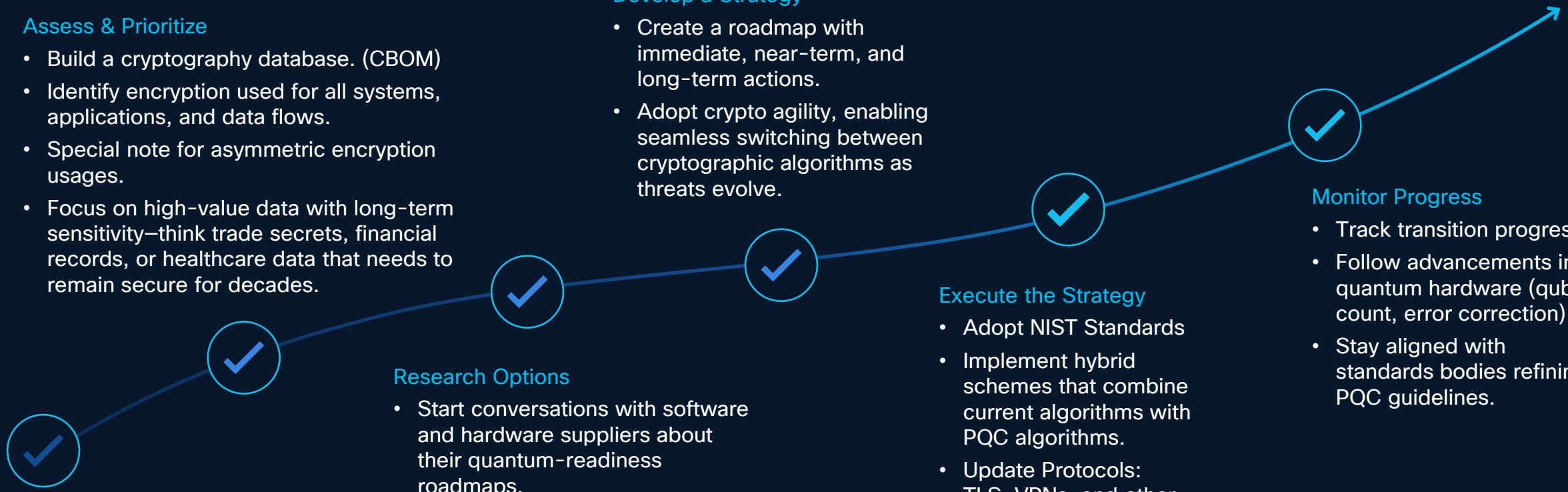
© 2026 Cisco and/or its affiliates. All rights reserved.

Customers can begin their PQC journey today with Cisco products that already implement quantum-safe standards

Quantum Safe Solutions	Available
RFC 9370 / IKEv2 (ML-KEM)	**IOS XE 26.1.1** – Cisco 8000 Series Secure Router: Traditional VPNs (February 26)
RFC8784 / IKEv2	PPK: Manual & SKIP • **IOS-XE 17.11** - Cat8300, Cat8000v, ASR1K • **IOS-XE 17.12** – ISR1K, Cat8500 • **IOS XE 17.15/17.18** – Cisco 8000 Series Secure Router PPK: Manual only
MACSEC	PPK: Cisco SKS & SKIP • **IOS XE 26.1.1** – Cisco 8000 Series Secure Router: Traditional VPNs (February 26)

© 2026 Cisco and/or its affiliates. All rights reserved.

Preparing for Quantum Computing Security Threats



Educate

Ensure IT, security, and leadership understand the quantum threat.

Assess & Prioritize

- Build a cryptography database. (CBOM)
- Identify encryption used for all systems, applications, and data flows.
- Special note for asymmetric encryption usages.
- Focus on high-value data with long-term sensitivity—think trade secrets, financial records, or healthcare data that needs to remain secure for decades.

Research Options

- Start conversations with software and hardware suppliers about their quantum-readiness roadmaps.
- PQC-usages, Hybrid solutions and crypto agility.

Develop a Strategy

- Create a roadmap with immediate, near-term, and long-term actions.
- Adopt crypto agility, enabling seamless switching between cryptographic algorithms as threats evolve.

Execute the Strategy

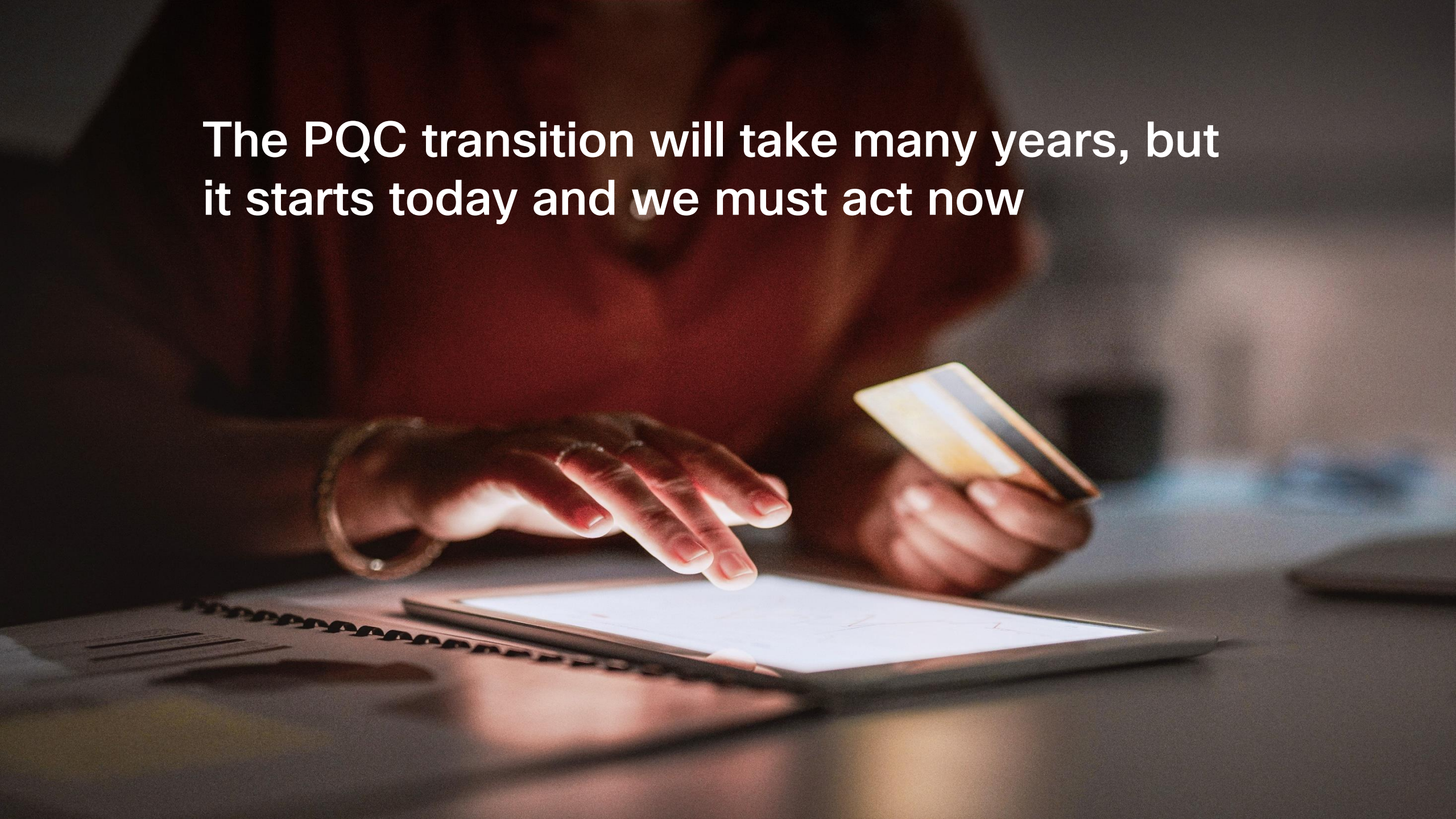
- Adopt NIST Standards
- Implement hybrid schemes that combine current algorithms with PQC algorithms.
- Update Protocols: TLS, VPNs, and other secure communication protocols to support PQC.

Monitor Progress

- Track transition progress
- Follow advancements in quantum hardware (qubit count, error correction)
- Stay aligned with standards bodies refining PQC guidelines.

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco


The PQC transition will take many years, but
it starts today and we must act now

Cisco has worked closely with NIST, IETF, and other groups to define protocols and security standards for PQC



2013
- Cisco cryptography experts authored Leighton-Diffie-Winternitz-McGrew (LDWM) hash-based signatures

2015
- LDWM begins shipping in Cisco products

2016
- SPHINCS+ stateless hash-based signature scheme submitted to the NIST PQC project

2017
- Cisco created the SKIP interface (quantum-safe pre-shared keys)

2018
- Cisco incorporated SKIP into devices and successfully verified operation with Quantum Key Distribution (QKD) vendors

2019
- Cisco authored Leighton-Micali Signature (LMS) hash-based signature algorithm
- SPHINCS+ revisions
- European Telecoms Standards Institute (ETSI) published QKD interface specification

2020
- RFC 8784 co-authored by Cisco

2022
- Cisco sponsored engagement with Open Quantum Safe (OQS)
- Commercial National Security Algorithm (CNSA) 2.0 Agorithms announced
- Univ of Waterloo funding to accelerate adoption of PQC research

2023
- Cisco contributed Leighton-Micali Signature (LMS) code to OQS
- LMS alg testing available in Automated Cryptographic Validation Protocol (ACVP)
- OQS joins Linux Foundation

2024
- NIST approves 3 PQC algorithms, ML-KEM testing available on ACVP prod servers
- Cisco joins NCCoE Interop workstream
- CiscoSSH Interop testing completed

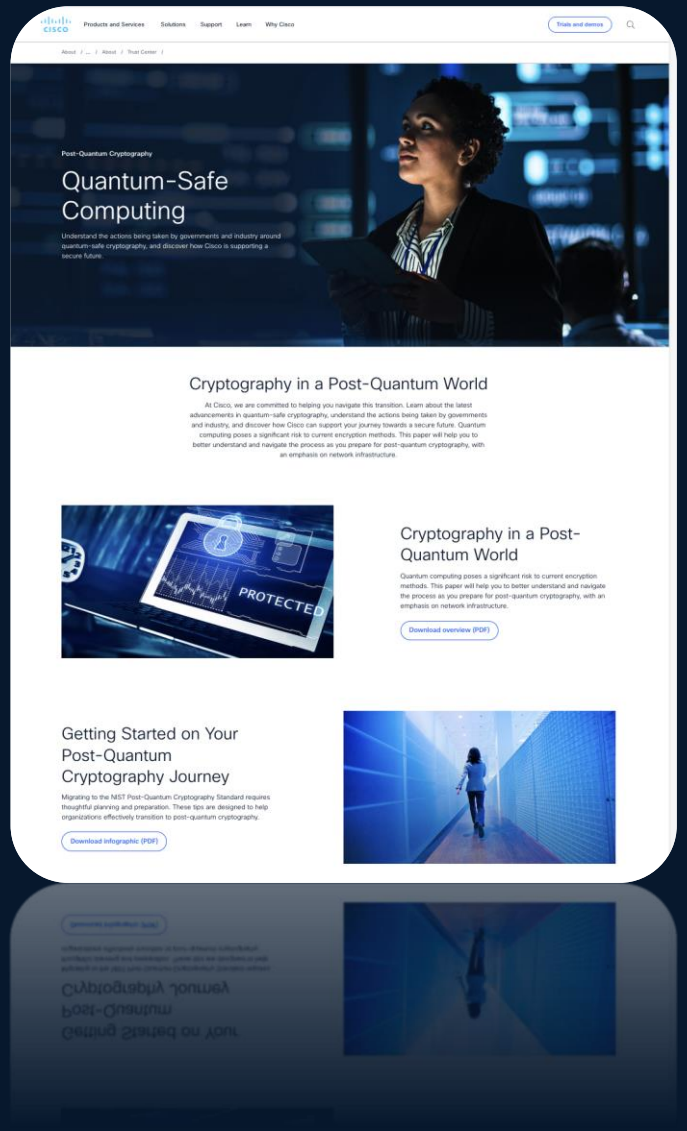
2025
- Cisco ranked among top contributors to Linux Foundation
- First Cisco product shipped with LMS for 1st stage HW secure boot

2026+
- PQCA/OQS/OpenSSL deployment/adoption
- OpenSSL Business Advisory & PQC FIPS discussions
- Additional IETF protocol standards finalized
- Certification requirements updated to include PQC
- NIST's competitions for other algorithms

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Next Steps



- Visit https://www.cisco.com/go/pqc
- Check the latest blog posts

  https://blogs.cisco.com/networking/safeguard-your-wan-from-quantum-computing-threats
- Check- BRKENT-2055: Making Your WAN Quantum-Safe with IOS XE: Everything You Need to Know

© 2026 Cisco and/or its affiliates. All rights reserved.

Complete your session surveys



Complete your surveys in the Cisco Events App.



Complete a minimum of 4 session surveys and the overall event survey to receive a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

© 2025 Cisco and/or its affiliates. All rights reserved.

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Engineer meeting

Visit the Technical Solutions Clinics to discuss your technical questions



Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at CiscoLive.com/On-Demand

© 2025 Cisco and/or its affiliates. All rights reserved.

Thank you




CISCO