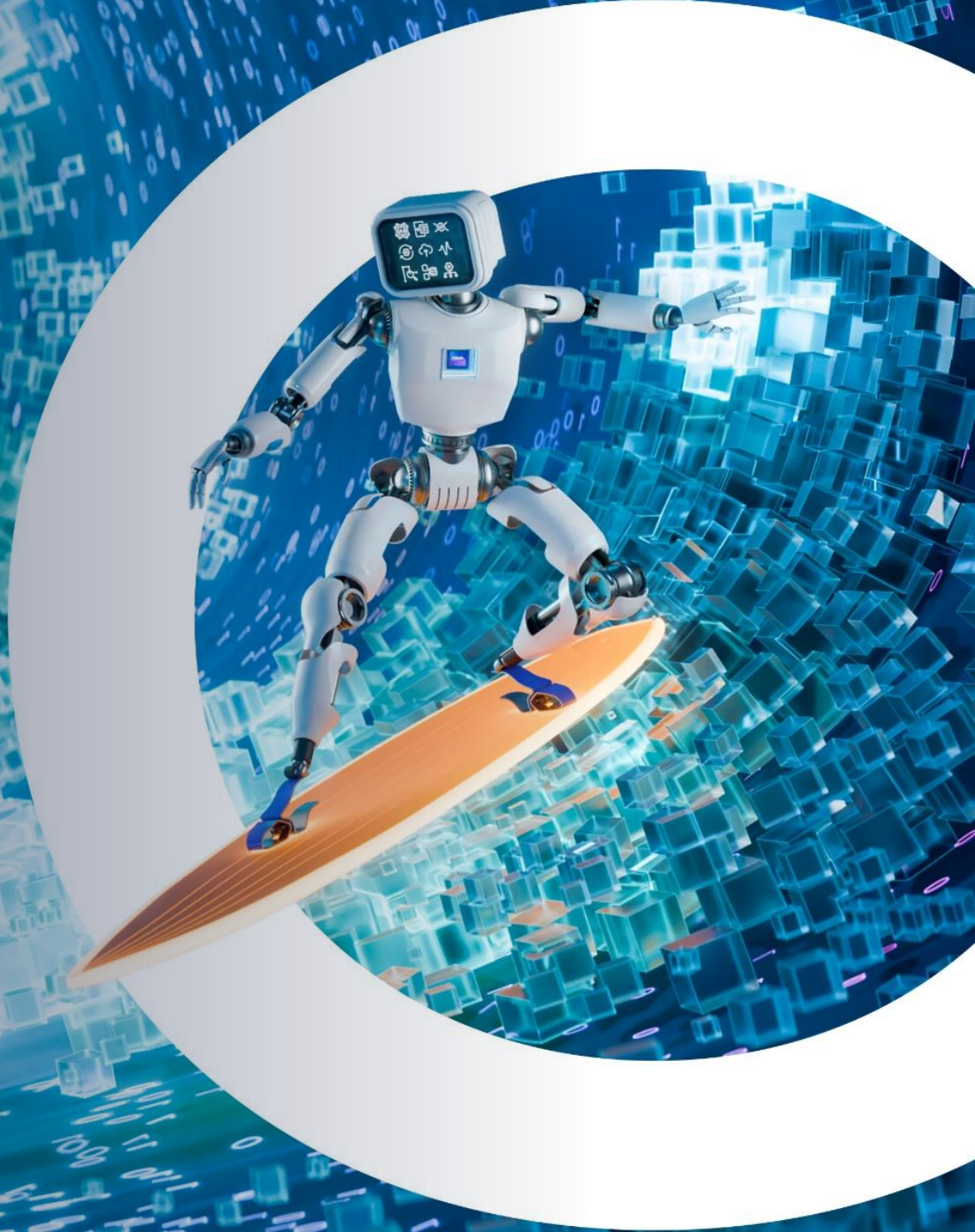
# Trends in DCI Interconnection and security



Gonzalo Sosa
Optical Business Development Manager
Nokia

Tical 2025 – Costa Rica
November 2025

# Key applications putting pressure on the metro-access optical network


## Cloud IT

Cloudifying operations

## AI

Massive DCI and distributed DC build out

## Mobile

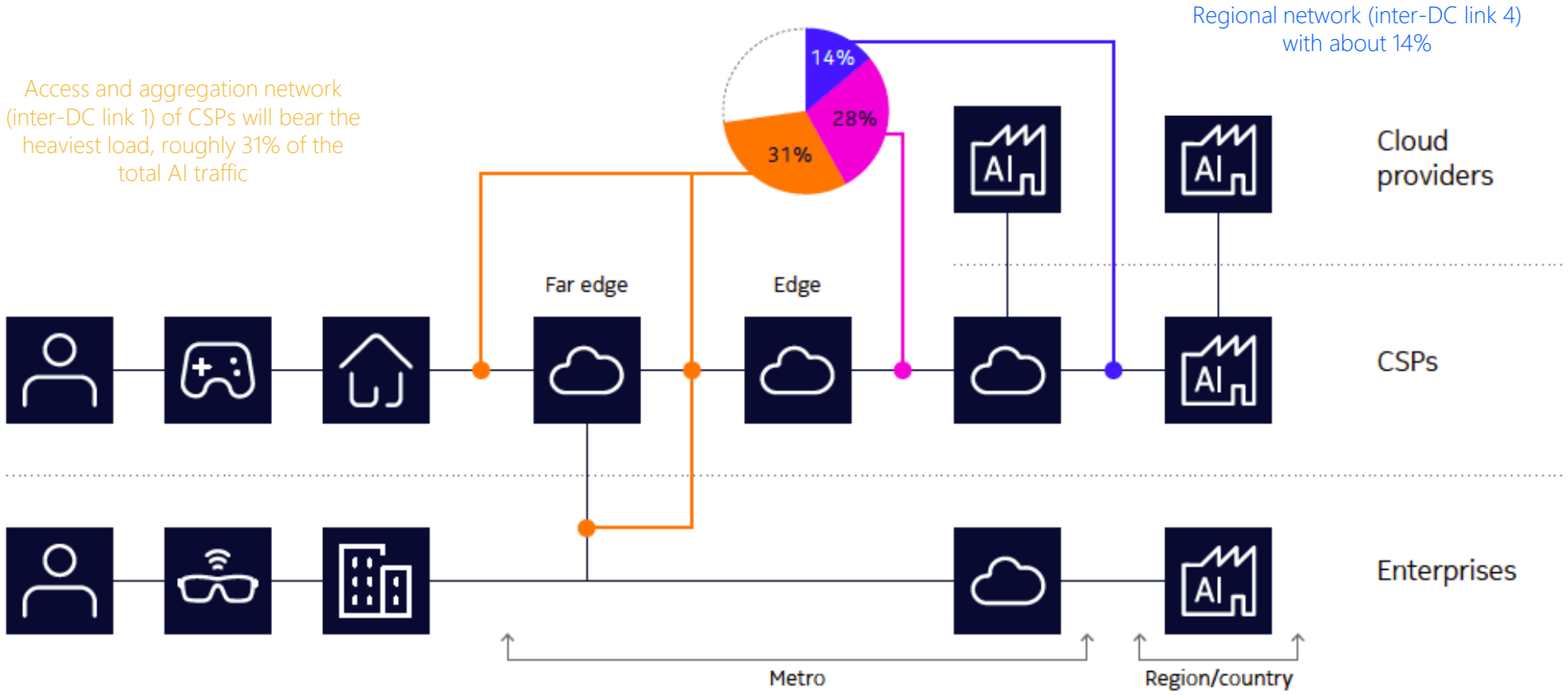
5G deployments, preparing for 6G

## Video

Ever more content

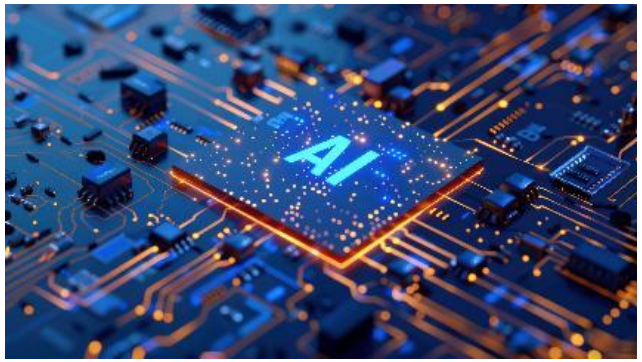
# AI traffic demands major network capacity expansion

## AI traffic over inter-data center links



# Data center connectivity challenges in the AI era

## Bandwidth




**100%**

AI-related bandwidth CAGR

AI accelerating bandwidth growth

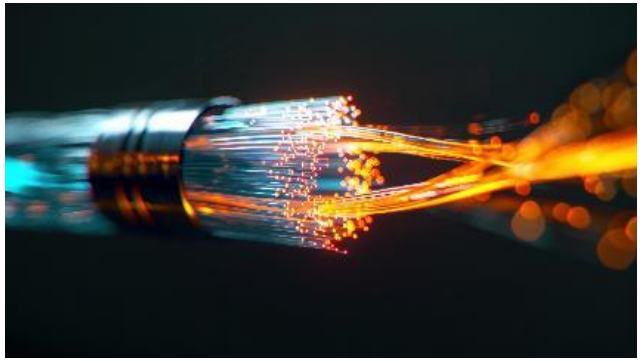
## Data centers

**27%**

Data center capacity CAGR

Driven by demand, power, space

## Line systems



**2x**

OLS requirements by 2027

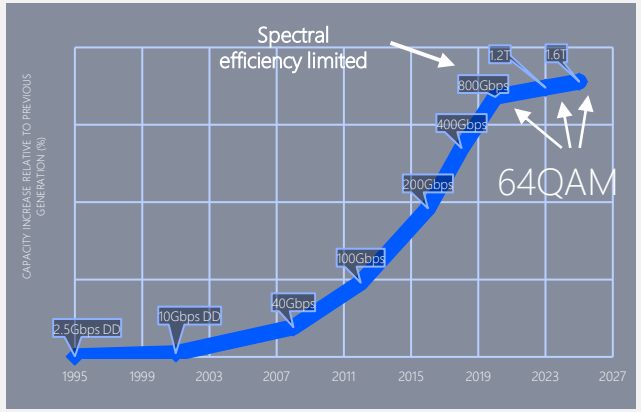
Fiber capacity exhaust fueling innovations

Sources: Meta at ECOC 2024, Goldman Sachs, OMDIA and Nokia, respectively

# Optical technology trends

## Shannon's limit

Capacity per fiber flattening

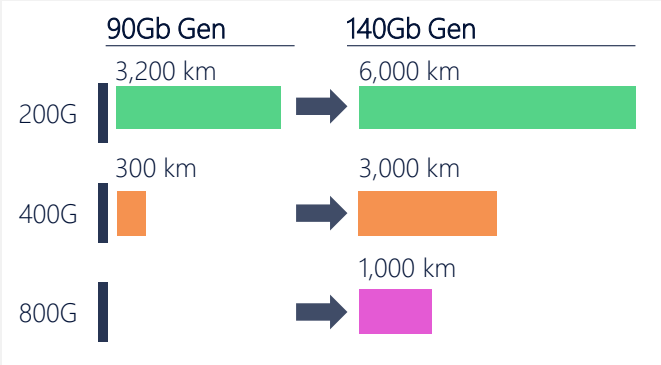



Need for multi-fiber strategies

## Pluggable evolution

Form factor

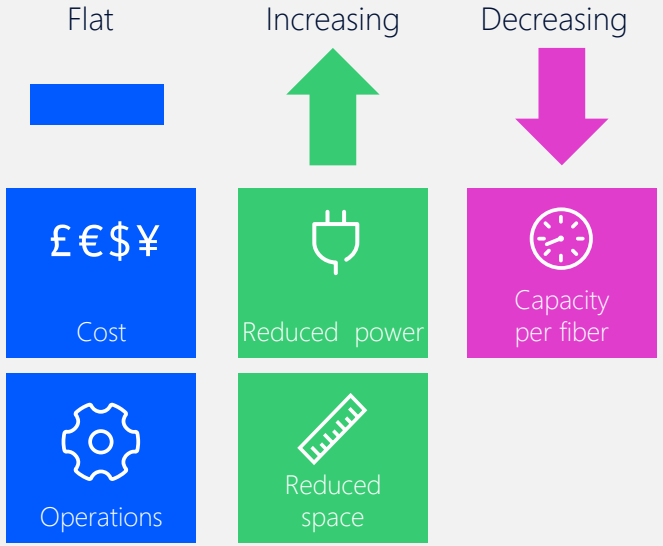

Performance




Smaller with greater reach enabling more applications

## Shifting priorities

Different applications have different priorities



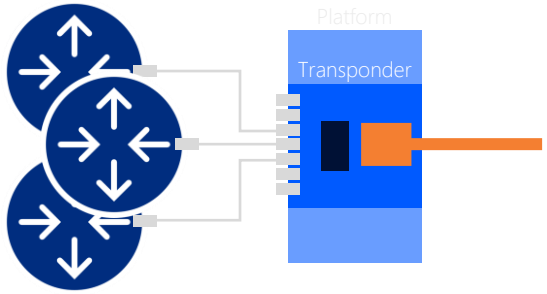

Increasing desire to leverage the benefits of coherent pluggables

# Management and operations impact

## An uphill climb

# Current deployment models

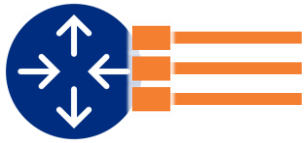
## Embedded Transponder




- Maximum fiber capacity
- Multiple client-side aggregation
- Operational domain separation
  - Lawful intercept, SLA boundaries, Commercial demarcation, Streaming telemetry, etc.
- Full suite of optical capabilities
  - Grooming, hair pining, alarm isolation & correlation, optical protection

- Higher power consumption
- Larger footprint
- Higher CapEx

## IPoDWDM

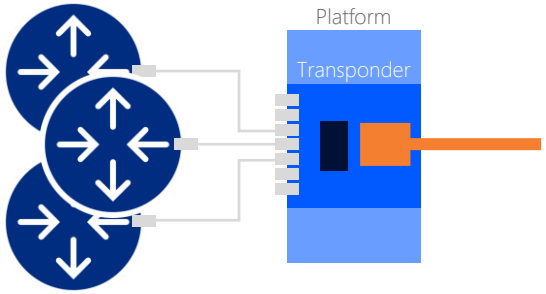


- Lower power
- Lower CapEx
- Smaller footprint
- Optical interoperability

- Operational complexity
  - Management, Certification, compatibility, different OSs, etc.
- Limited to router port speed
- Longer links cause port capacity loss
- Loss of key optical capabilities
- Reduced capacity per fiber

# Expanding deployment models

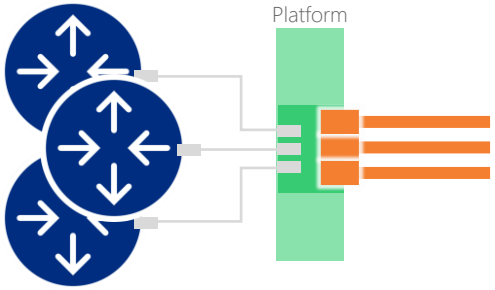
## Embedded Transponder




- Maximum fiber capacity
- Multiple client-side aggregation
- Operational domain separation
  - Lawful intercept, SLA boundaries, Commercial demarcation, Streaming telemetry, etc.
- Full suite of optical capabilities
  - Grooming, hair pining, alarm isolation & correlation, optical protection

- Higher power consumption
- Larger footprint

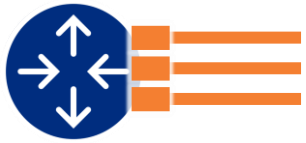
## Thin Transponder




- Lower power
- Lower CapEx
- Smaller footprint
- Optical interoperability
- Multiple client-side aggregation
- Operational domain separation
- Numerous optical capabilities
  - Aggregation, alarm isolation & correlation, optical protection

- Reduced capacity per fiber
- Limited client service grooming

## IPoDWDM

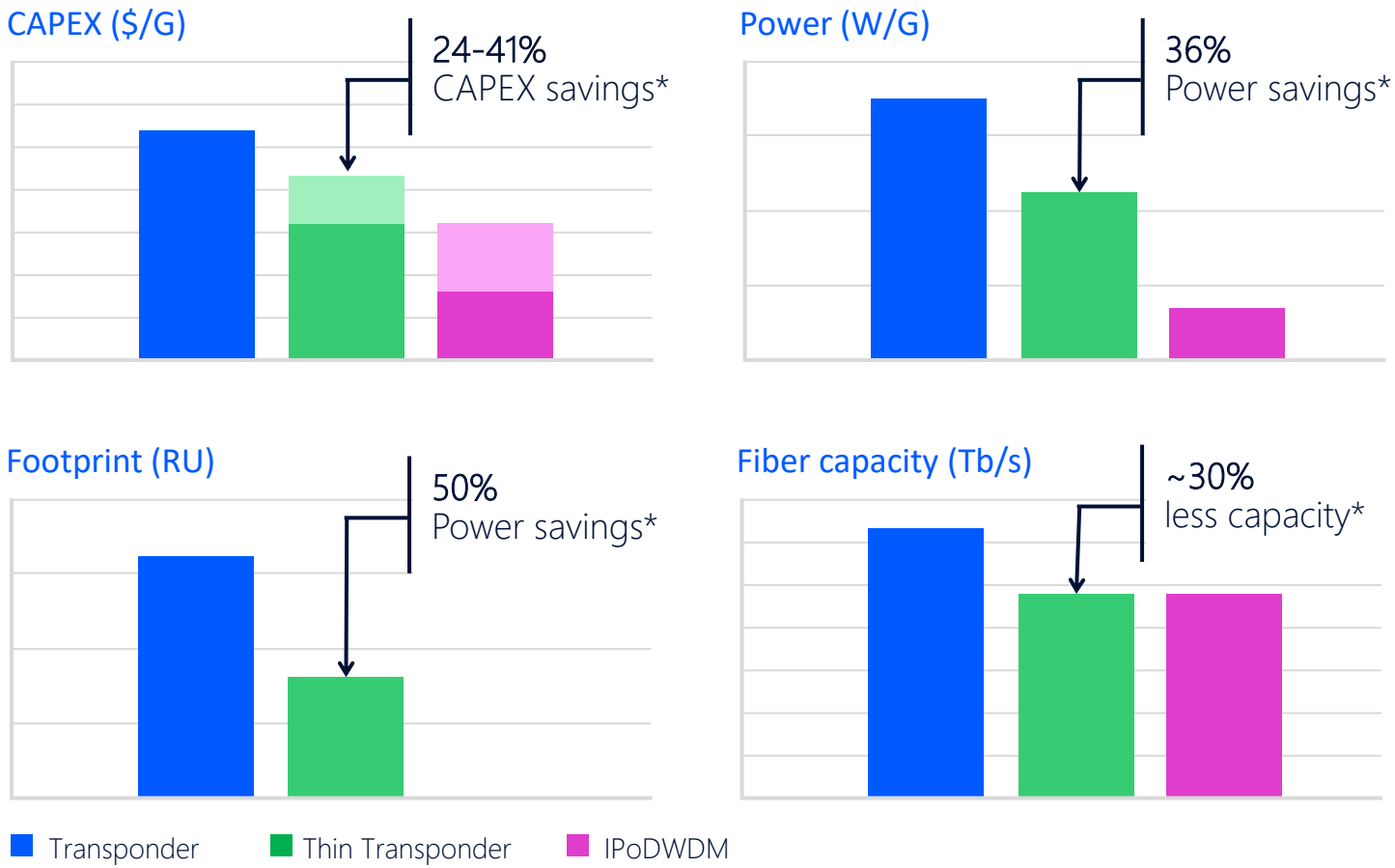


- Lower power
- Lower CapEx
- Smaller footprint
- Optical interoperability

- Operational complexity
  - Management, Certification, compatibility, different OSs, etc.
- Limited to router port speed
- Longer links cause port capacity loss
- Loss of key optical capabilities
- Reduced capacity per fiber

# Thin layer transponder

- Embedded provides highest spectral efficiency and longest reach
- Pluggables reduce rack space, even when regeneration is needed
- Thin transponders gives an intermediate solution, specially when the operators have separate domains.

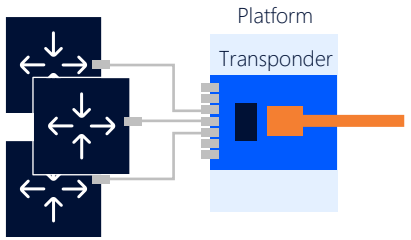



*Reflects ICP volume and scale

Analysis performed on fully-filled fiber over 1,000 km

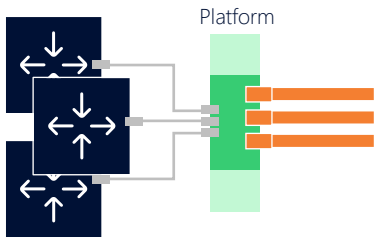
# Expanding deployment models

## Embedded transponder




- When fiber is scarce
- Over long-haul/subsea applications
- When different services must be supported
- When advanced traffic functions are required (grooming, protection, etc.

## Thin transponder




- When a low variety of services must be supported
- When space and power are limited
- When some traffic functions are required (virtual bandwidth, etc.)
- When increasing the reliability of IP traffic is required
- When IP and optical divisions are separate and demarcation requirements

## IPoDWDM

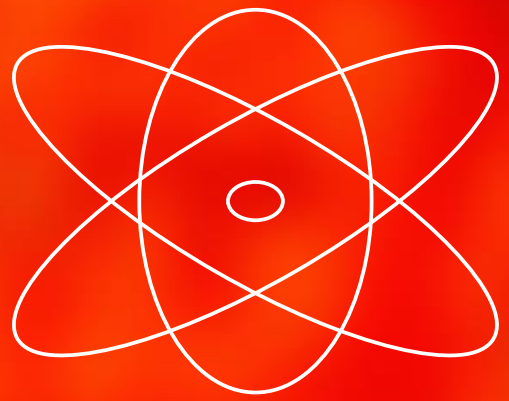
- When space, power and CAPEX are driving factors
- When traffic is only IP/Ethernet

# Quantum Safe Networks with 1830SMS

Traditional cryptography is vulnerable to quantum computers

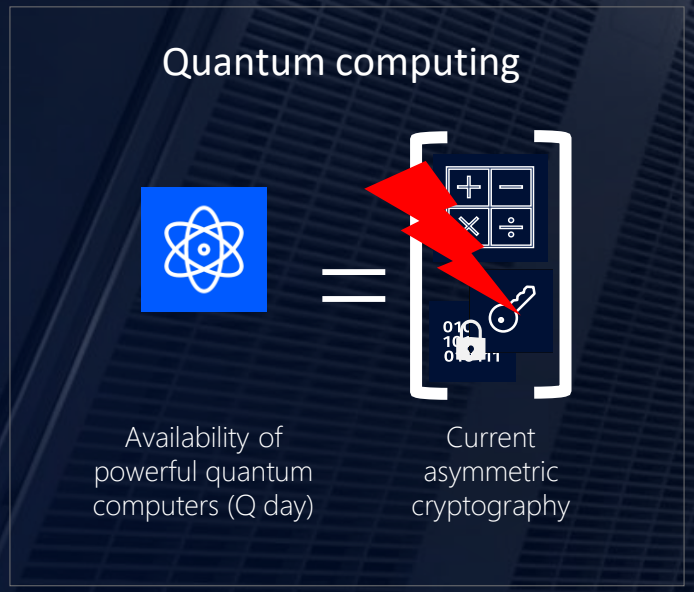
Quantum-resistant cryptographic algorithms are needed

We must ensure robust security to cope with evolving threats



# The ICT industry is facing a significant migration in cryptography

# Quantum computing breaks our decades-long asymmetric cryptography frameworks




Intercept data now and store it

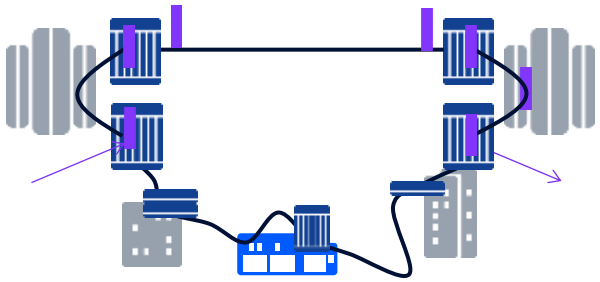
Decrypt it once a quantum computer is available

Harvest now and decrypt later (HNDL)

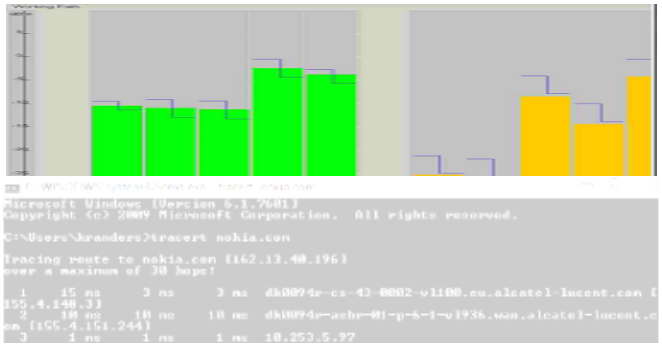
Zero-day vulnerability

# Security is more than just encryption

## Wavelength tracker – monitor optical link health

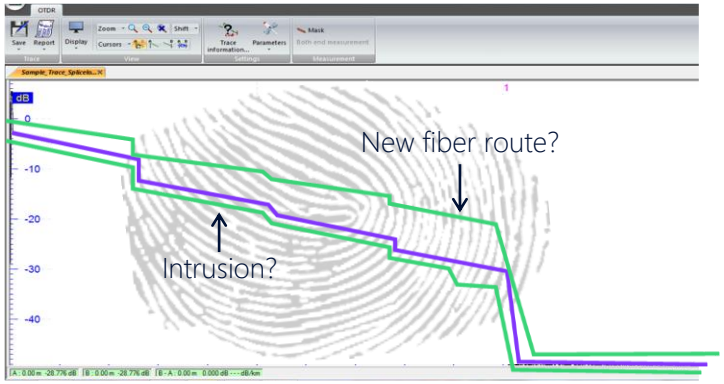


Allows wavelength tracking, power and fiber monitoring and reporting

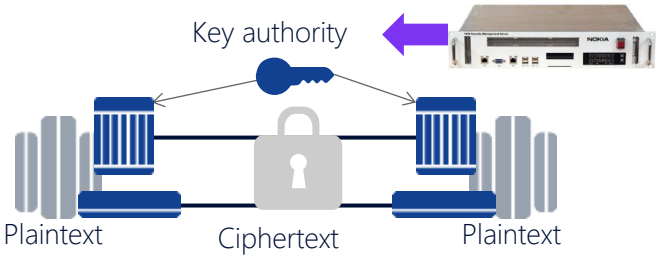


## OTDR – localize faults or taps immediately

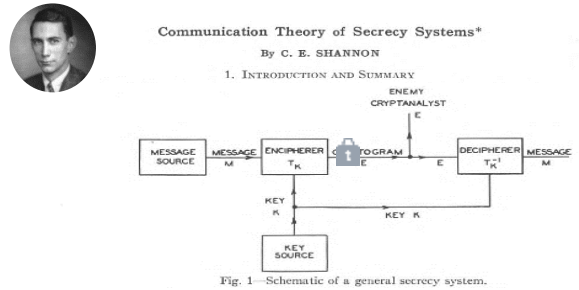
Detect and localize precisely any anomalies on fiber network




## Key management – the key quality is vital to any encryption




Protect data with a strong quality key and symmetric distribution



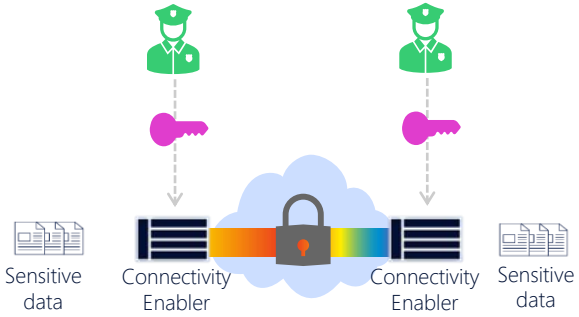

Quantum-Safe symmetric key distribution and generation

# Nokia QSN blueprints

## Adapting to each customer ecosystem

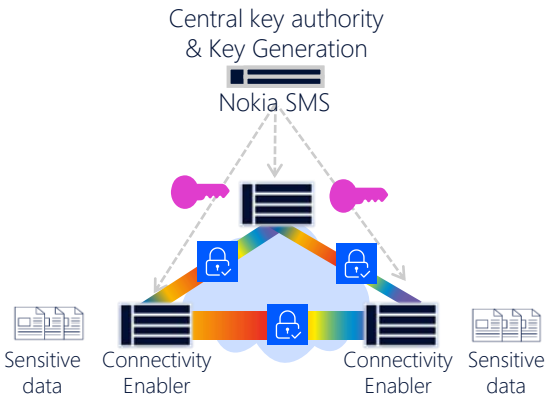
CP-RNG/Centralized

Q-RNG/QKD



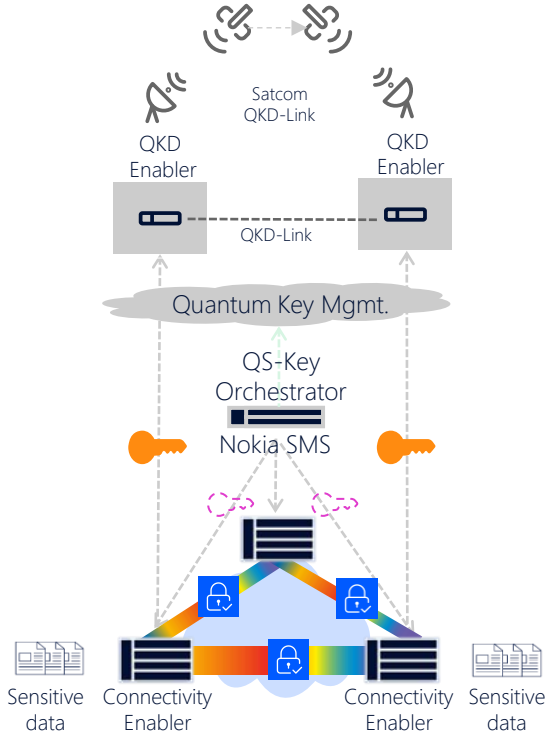

Pre-Shared 1

Quantum safe


Classic 2

Quantum safe




QKD hybrid blueprint 3

Quantum safe

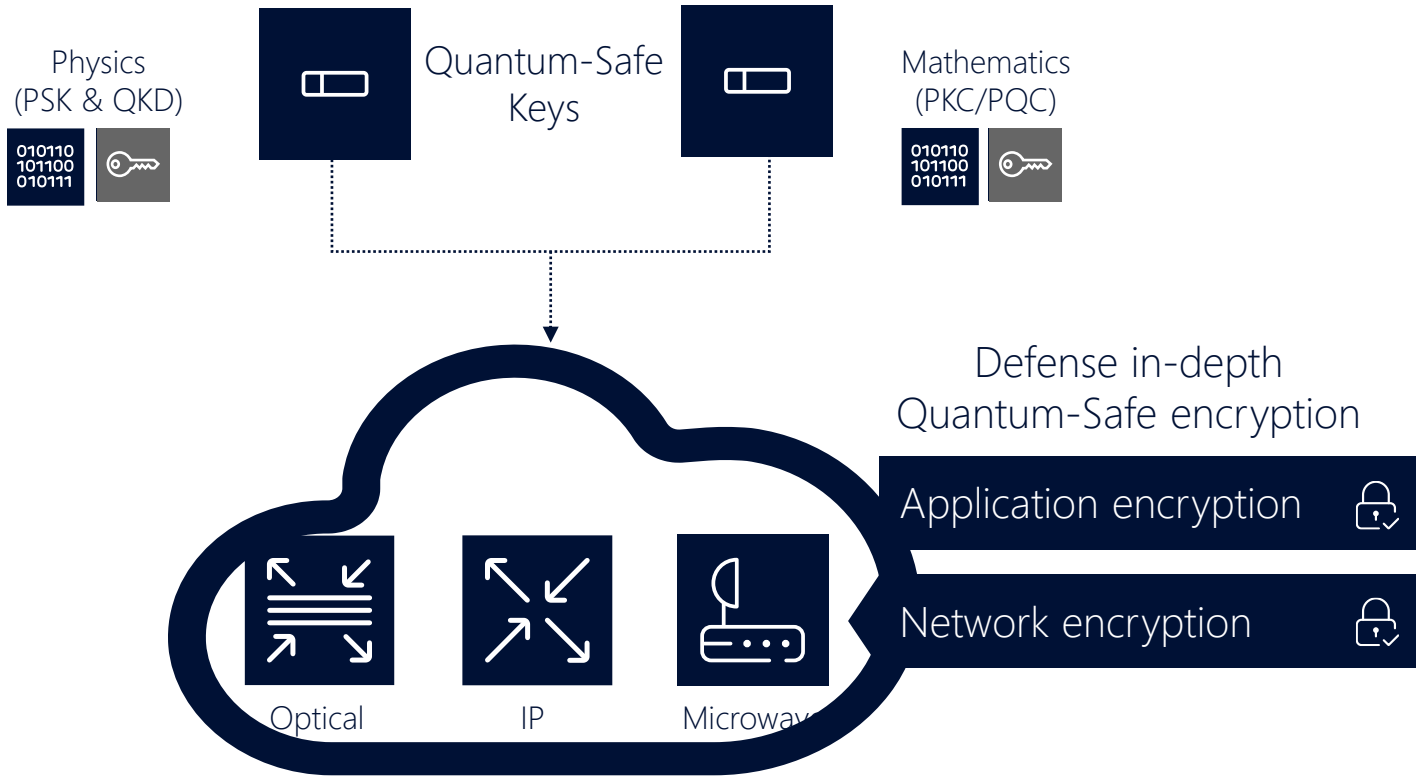
HNDL = harvest now decrypt later

CP-RNG = classic physic random number generator

Q-RNG = quantum random number generator

# Nokia's Quantum-Safe Networking and Transport

## 1830 Secure Management Server (SMS)




**Secure Key Management**

Secure out-of-band symmetrical pre-shared key distribution & rotation on certified secure hardware

**Data Path Encryption**

Highest possible encryption available today AES256

**Certifications**

Certified security from ANSSI, NIST, Common Criteria and FIPS 140-2/3

Safeguard your network's sensitive data and mission-critical services

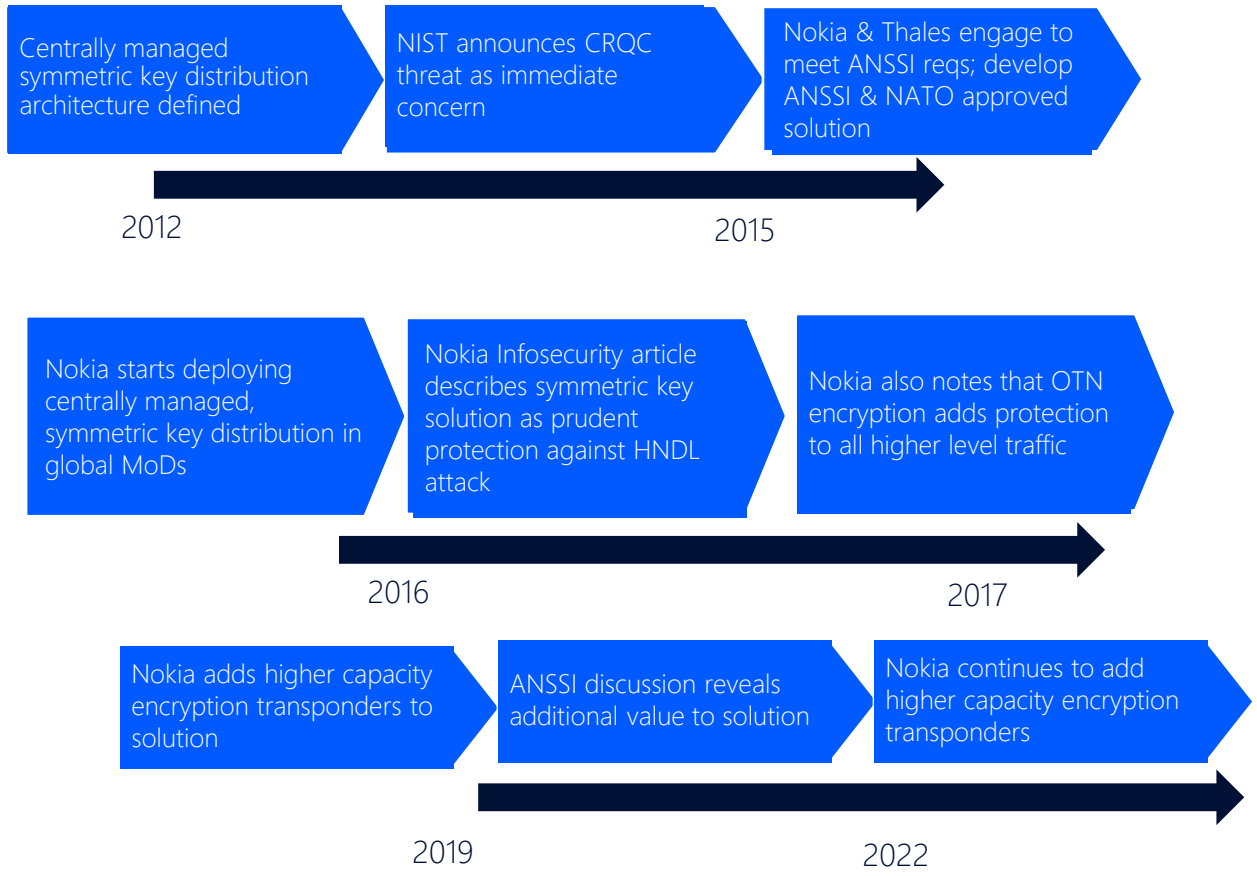
# Nokia 1830 Security Management Server (SMS)

## Quantum-key generation & distribution hybrid (classic)

Nokia 1830 SMS


- Centralized, symmetric key distribution
- Embedded cryptographic System-On-Chip
- Ensures key quality and strength
- Offloads intensive cryptographic processing
- SW integrity validation (Digital signature PP CWA 14167-2 compliant)
- CC EAL4+, ANSSI QR including EU and NATO restricted certs
- FIPS 140-2 Level 1 Software for Hardened Server

Over 10 years of quantum-safe development




NOKIA