RiSM

Rajant In-line Security Module

January 24, 2024

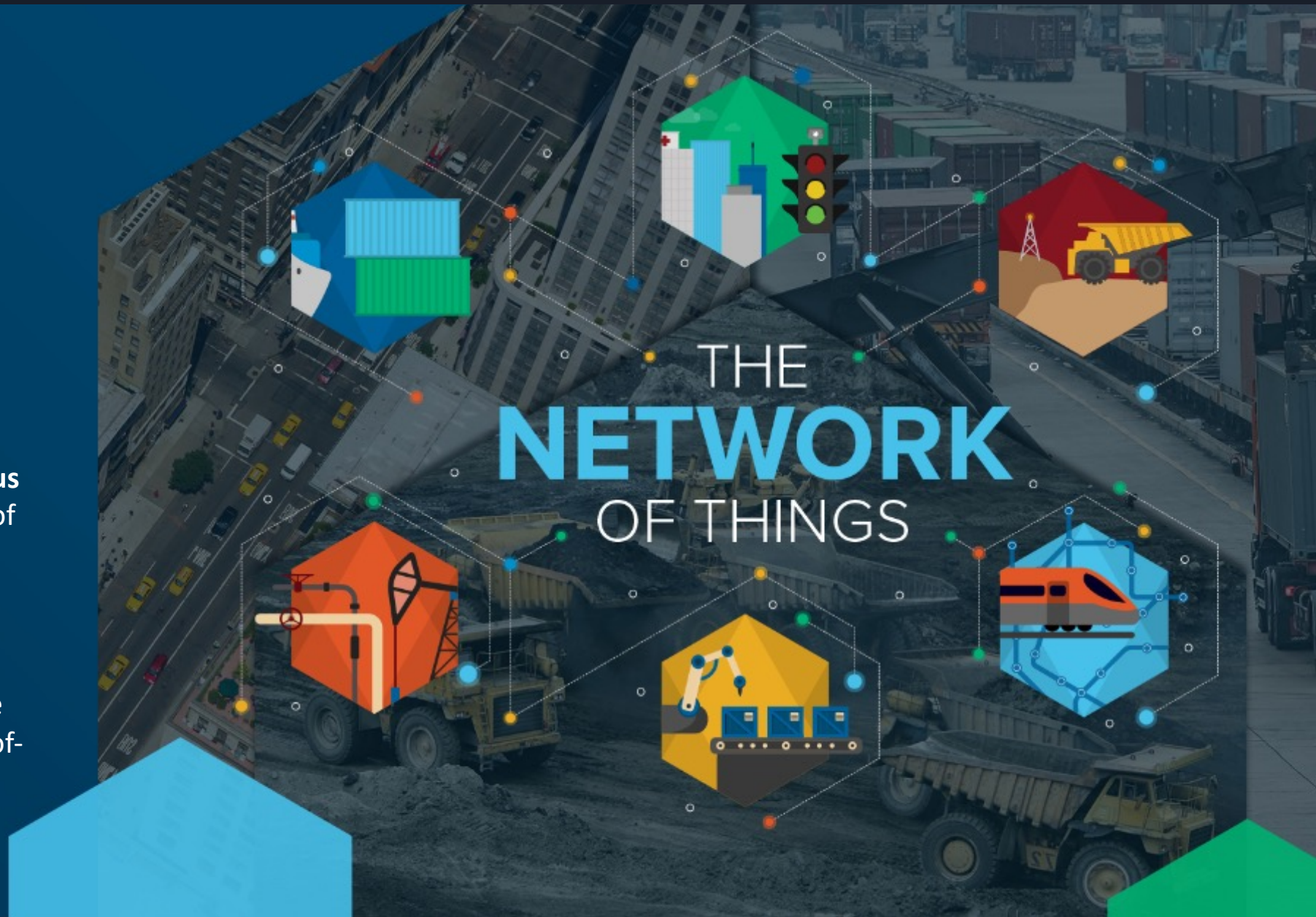
Who is Rajant? We Make Wi-Fi and LTE Work Better.

Private, secure peer to peer wireless network technology for mission critical industries.

BANDWIDTH
High Speed & Low Latency

MOBILITY / RESILIENCY
Seamless and Instantaneous Joining, Leaving & Moving of Network Assets

SMART
Higher Performance from Greater Scale. Mitigate the affects of range, Non-Line-of-Sight and Network Traffic.



Key Differentiators

Fully Mobile

- Extend your network past the limitations of fixed infrastructure
- Create an instantaneous network
- Machine-to-Machine communication enables network resiliency

Multi-radio, Multi-frequency

- RX and TX simultaneously eliminates throughput loss and latency stacking multiple hops
- Enables much higher aggregated capacity
- Mitigates interference

Ease of Deployment

- Same network?
- Same frequency?
- It connects!

Cyber Security

- Mission-critical security via Chandler, Arizona's crypto team

Layer-2

- Integrates seamlessly within a Layer-3 network
- Limits latency to milliseconds versus tens of milliseconds

3 R's

- Resiliency
- Reliability
- Redundancy

Vertical Markets – Air, Land, & Sea


DEFENSE


OPEN PIT MINING


UNDERGROUND MINING


OIL & GAS


PETROCHEMICAL


PORTS


RAIL


PUBLIC SAFETY


DRONES & ROBOTS


WAREHOUSE AUTOMATION


UTILITIES


HEALTHCARE


HEAVY CONSTRUCTION


AGRICULTURE


AIRPORTS


ACTION SPORTS


THEME PARKS


ENTERTAINMENT

Rajant In-line Security Module (RiSM)

Problems To Solve

Federal Agencies: All agencies using cryptographic security systems to protect information in network-based systems

Utilities, Telcos, & Transportation: Need to comply with new federal requirements for securing critical infrastructure

Public Safety & Smart City Infrastructure: Making improvements to infrastructure security (some with federal BEAD funds)

Remote Offices: Need improved security and better network access above what they get with a traditional VPN tunnel (eg. multi-tunnel)

Banking: Need to comply with Sarbanes Oxley Act of 2002 that mandates data be encrypted with 256-bit AES

Health Industry: Need to setup and maintain a complex set of controls for HIPAA compliance (FIPS)

Network Designers: Have the burden to validate the encryption security on their own, proving HIGH ASSURANCE of their security

Rajant In-line Security Module (RiSM)

Value delivered

- **RiSM** allows users to meet the latest NIST standards for encryption (FIPS 140-3) & device protection in a package that is more affordable than other hardware alternatives.
- **High Assurance = Lower Risk:** Protecting data with RiSM is beneficial in limiting access to cryptography keys to just Crypto Officers & reduces the risk of compromised data from a security hack or key compromise, the cost of which is invaluable.
- **Simplicity:** RiSM is easier to setup than any other HSM solution and more reliable than software solutions that require a multi-tunnel approach.

Rajant In-line Security Module (RiSM)

The RiSM

- High-speed Hardware Security Module (HSM)
  - Performs Layer-2 packet Encryption/Decryption
  - High Assurance device that protects cryptographic keys, algorithms, credentials, & operational firmware
- NIST FIPS 140-3 Level 2 Certification
- Based on Rajant's Wolverine Cryptographic Module Architecture
  - Designed to meet US Government needs, but now available to commercial customers (EAR exportable)
- High-Throughput: 500 Mbps & Low Latency: 12uS
- Military Strength 256 AES-GCM encryption/decryption
- Power Over Ethernet (PoE): device power & pass-through PoE for downstream devices
- BCC: Integrated RiSM management to deploy Secure Enclaves
- Ruggedized Design

Rajant In-line Security Module (RiSM)

Why Use FIPS Verified Devices?

- High assurance by design
- Design is independently evaluated
- Confirmed to standard, no programming shortcuts, no back doors
- Certified & not just compliant
- Protected against hacking with backdoor patches, bootloader access, or crypto algorithm modifications

NIST
National Institute of Standards and Technology

NIST FIPS 140-3

Defines four increasing, qualitative levels of security:
Level 1: Production-grade equipment and externally tested algorithms

Level 2: Physical tamper-evidence and role-based authentication.

Level 3:

- Physical tamper-resistance & identity-based authentication
- Private keys can only enter or leave in encrypted form
- Environmental failure protection, or EFP

Level 4: Tamper-active, erasing the contents if it detects environmental attack with multi-factor authentication

Rajant In-line Security Module (RiSM)

Should I use a Hardware Security Module (HSM) instead of software?

What is your CPU load when encryption is on?

Network Security Assurance

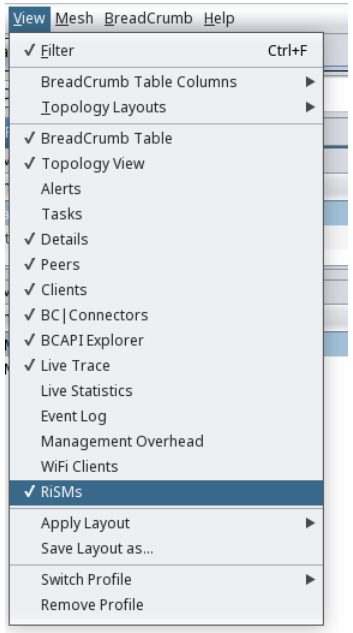
Cryptographic keys for encryption, decryption, & digital signing are some of your company's most precious assets! Where is yours stored?

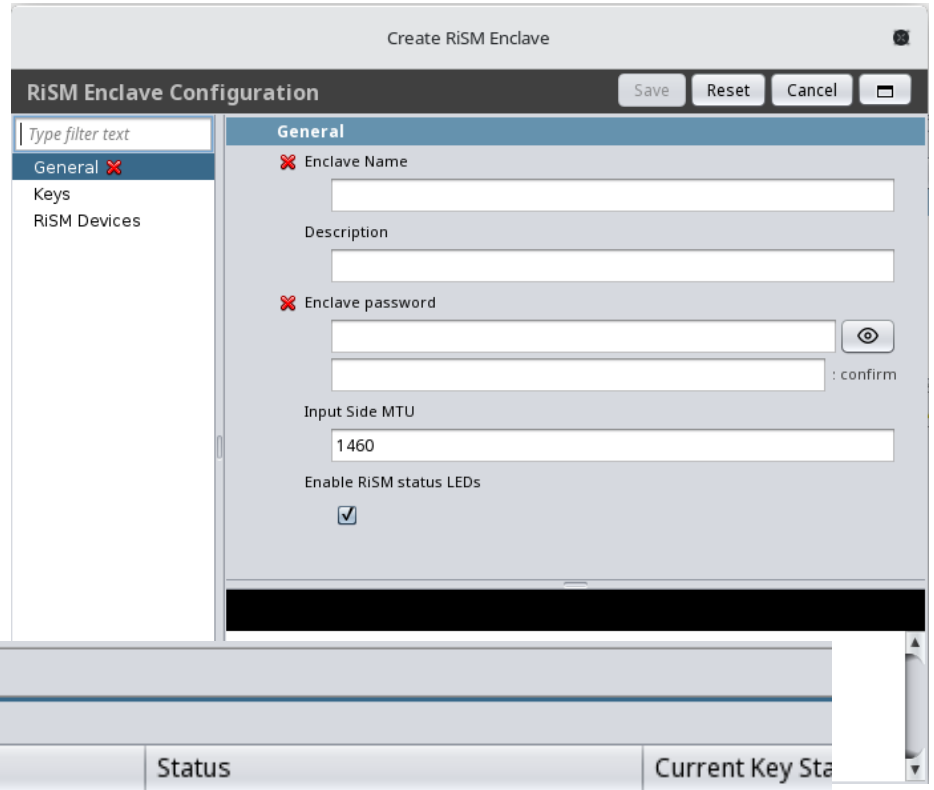
With a HSM, your CPU & network will run at full speed while HSM handles all the load of encryption & decryption.

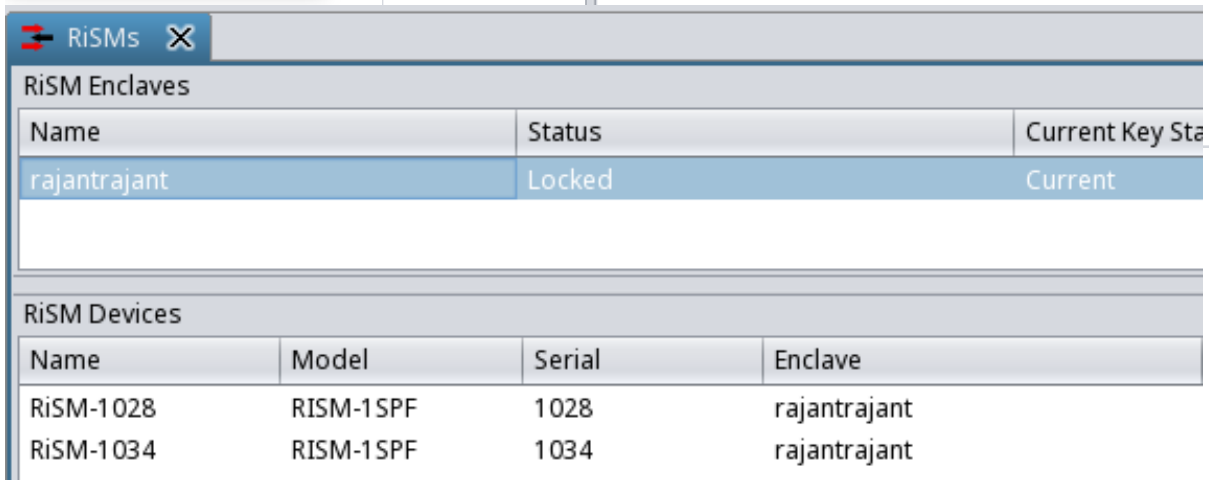
Cryptography protects your data. HSMs protect your cryptography and ensures only authorized traffic is allowed to enter the network.

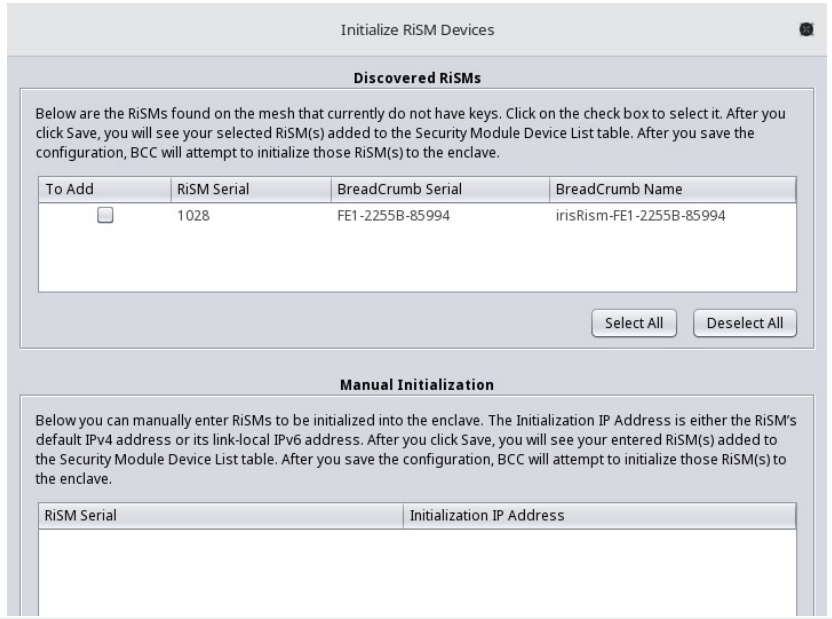
Keys are securely stored in the HSM and managed remotely with just a Crypto Officer.

BC Commander With RiSM

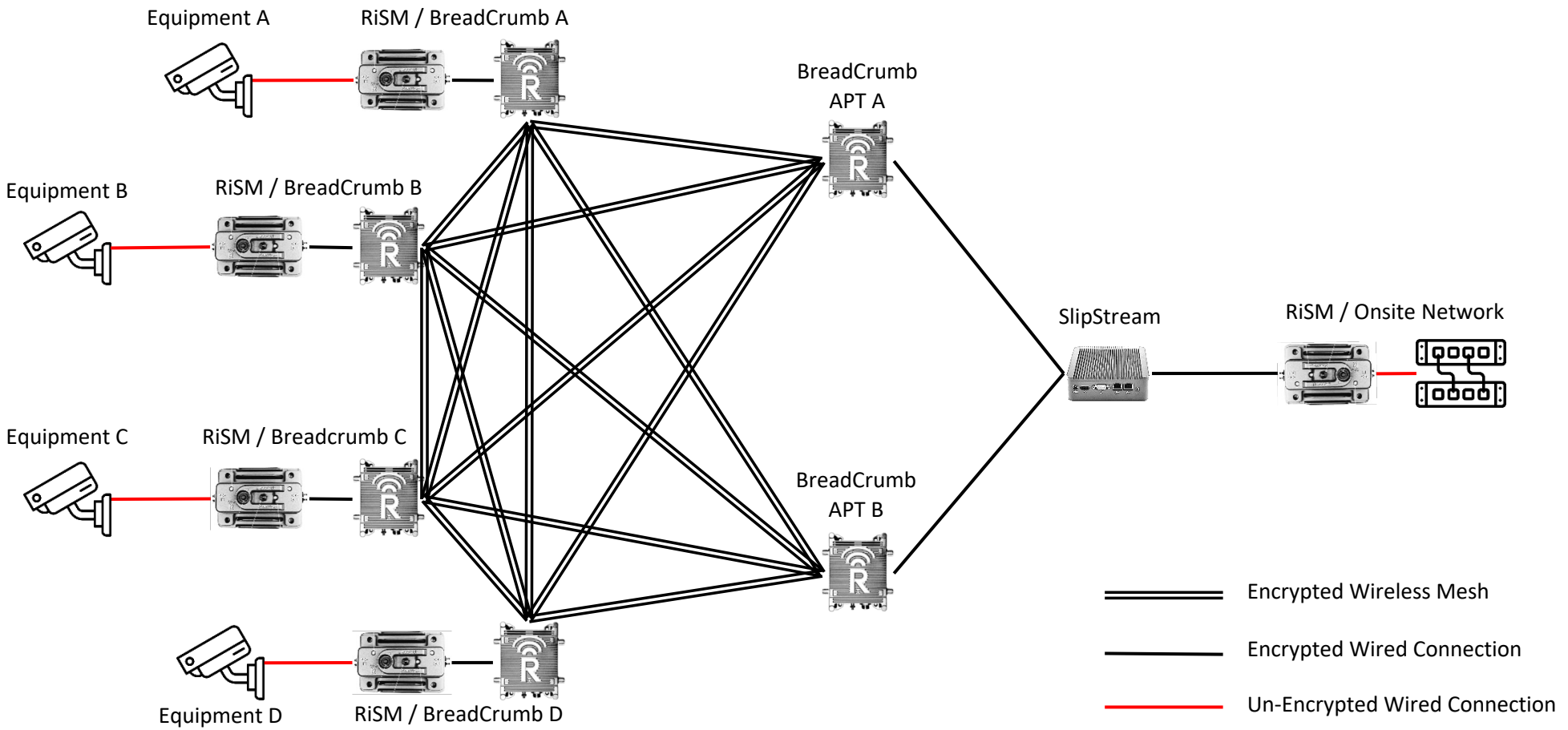




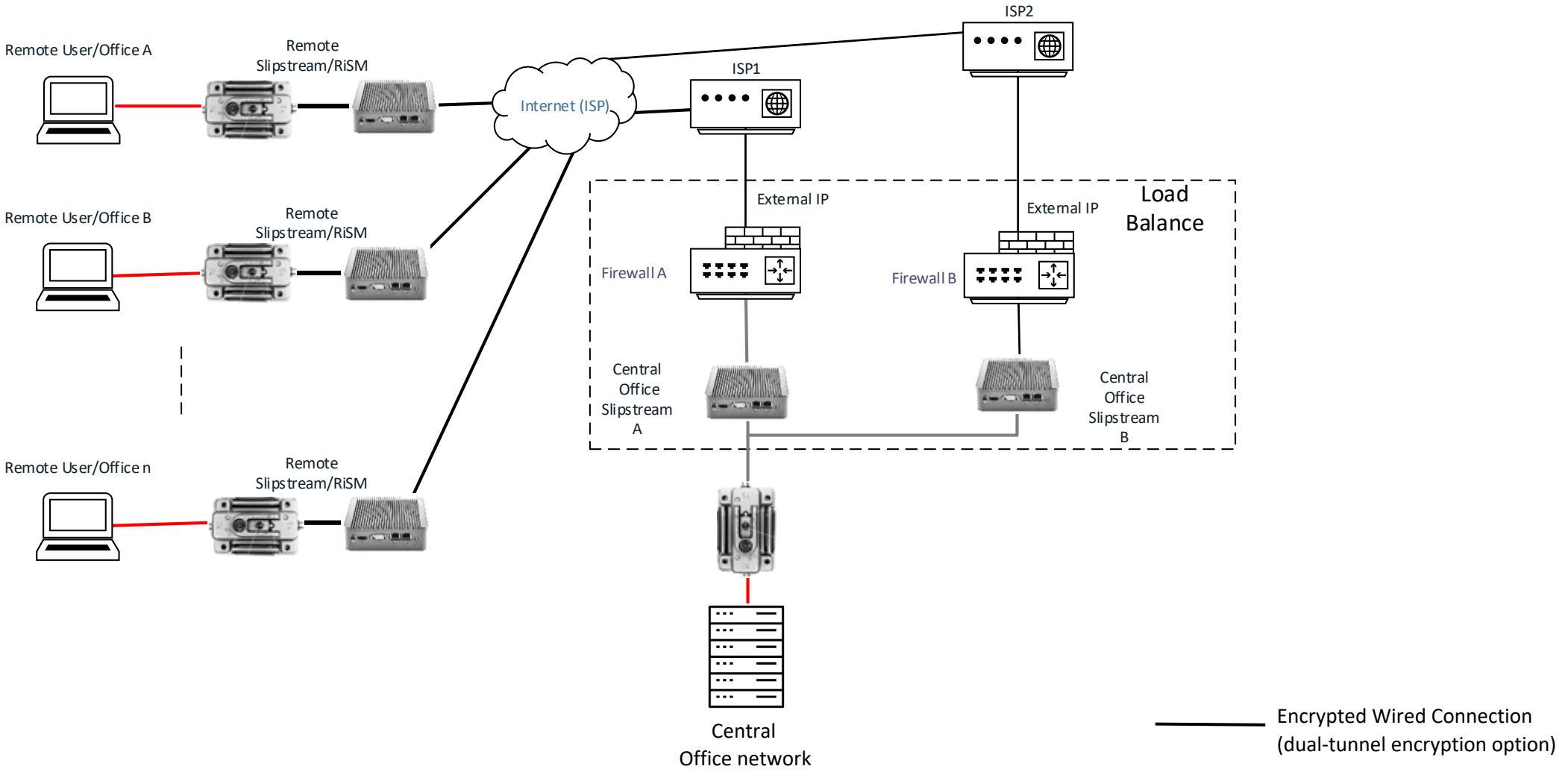




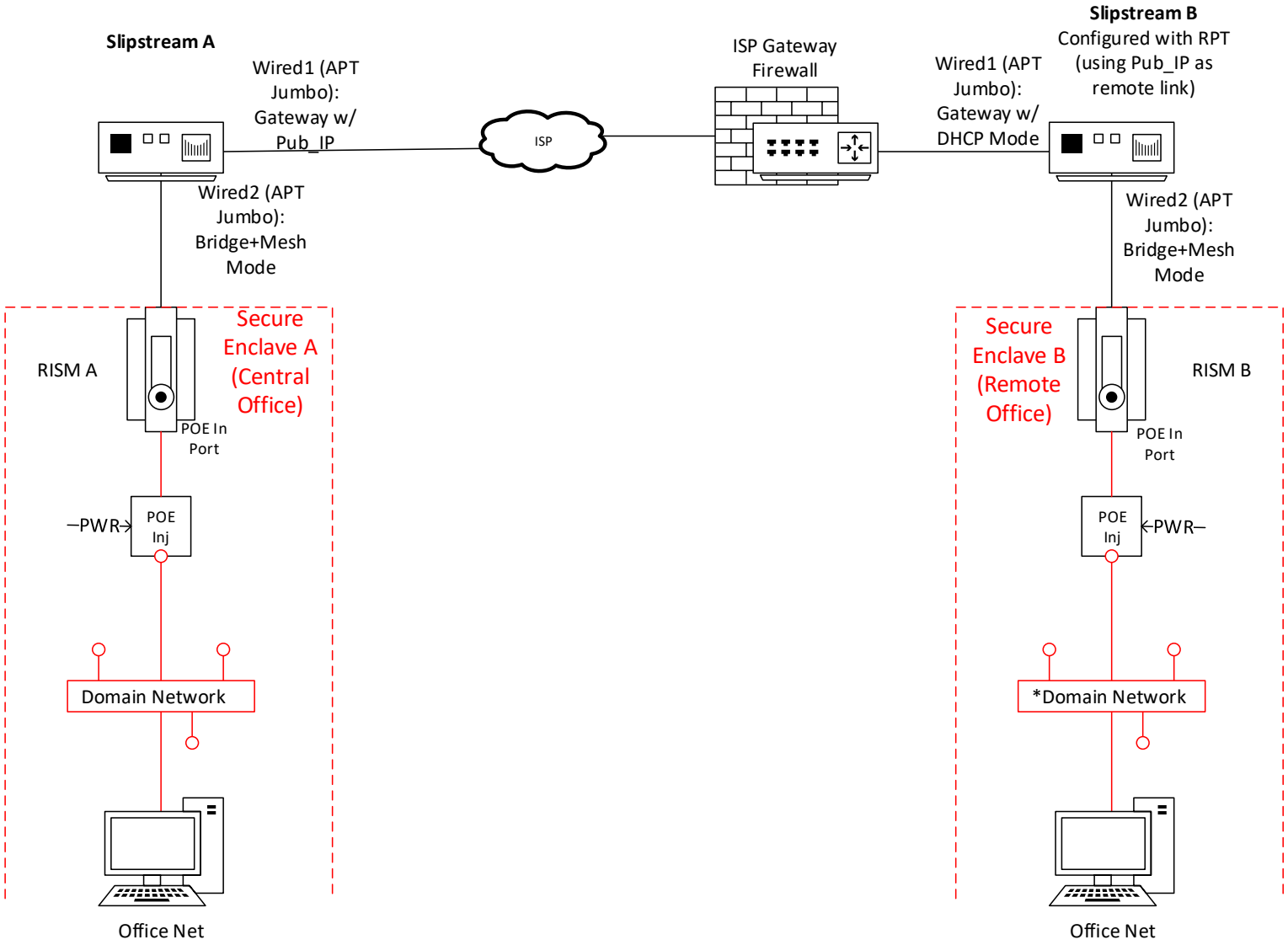
RiSM in Rajant Network



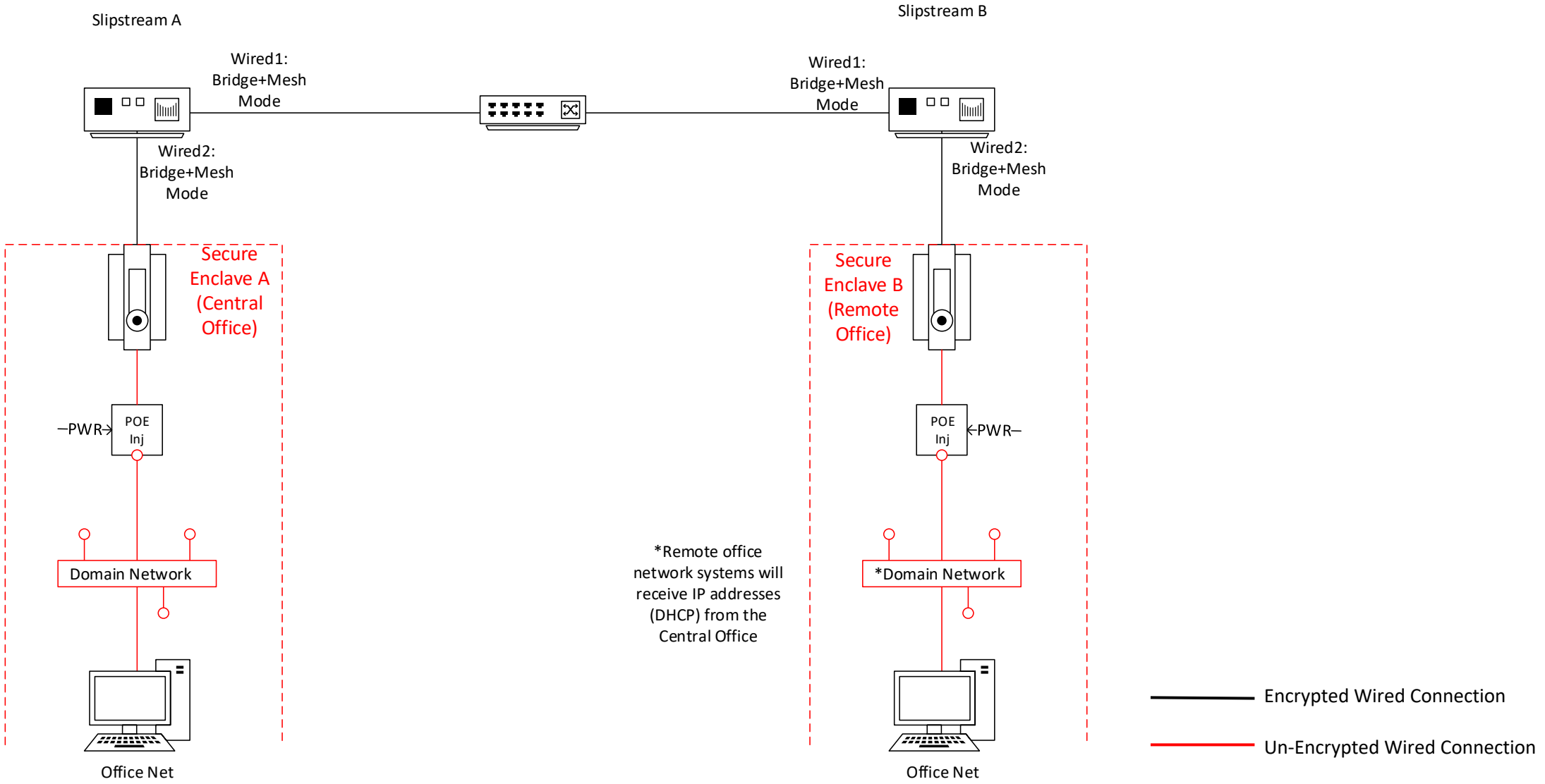
RiSM in Remote User Network



RiSM in Internet Network



RiSM in Internal WAN Network




RAJANT
thank you!