



RAJANT



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.



THE NETWORK OF THINGS



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



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

Problems To Solve



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



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



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



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



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



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



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

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.



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



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 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

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.

View Mesh BreadCrumb Help

- Filter Ctrl+F
- BreadCrumb Table Columns
- Topology Layouts
- BreadCrumb Table
- Topology View
- Alerts
- Tasks
- Details
- Peers
- Clients
- BC | Connectors
- BCAPI Explorer
- Live Trace
- Live Statistics
- Event Log
- Management Overhead
- WiFi Clients
- RiSMs**
 - Apply Layout
 - Save Layout as...
 - Switch Profile
 - Remove Profile

Create RiSM Enclave

RiSM Enclave Configuration

Save Reset Cancel

Type filter text

- General
- Keys
- RiSM Devices

General

- Enclave Name
- Description
- Enclave password
- Input Side MTU: 1460
- Enable RiSM status LEDs:

RiSMs

RiSM Enclaves

| Name | Status | Current Key Sta |
|--------------|--------|-----------------|
| rajantrajant | Locked | Current |

RiSM Devices

| Name | Model | Serial | Enclave |
|-----------|-----------|--------|--------------|
| RiSM-1028 | RISM-1SPF | 1028 | rajantrajant |
| RiSM-1034 | RISM-1SPF | 1034 | rajantrajant |

Initialize RiSM Devices

Discovered RiSMs

Below are the RiSMs found on the mesh that currently do not have keys. Click on the check box to select it. After you click Save, you will see your selected RiSM(s) added to the Security Module Device List table. After you save the configuration, BCC will attempt to initialize those RiSM(s) to the enclave.

| To Add | RiSM Serial | BreadCrumb Serial | BreadCrumb Name |
|--------------------------|-------------|-------------------|--------------------------|
| <input type="checkbox"/> | 1028 | FE1-2255B-85994 | irisRism-FE1-2255B-85994 |

Select All Deselect All

Manual Initialization

Below you can manually enter RiSMs to be initialized into the enclave. The Initialization IP Address is either the RiSM's default IPv4 address or its link-local IPv6 address. After you click Save, you will see your entered RiSM(s) added to the Security Module Device List table. After you save the configuration, BCC will attempt to initialize those RiSM(s) to the enclave.

| RiSM Serial | Initialization IP Address |
|-------------|---------------------------|
|-------------|---------------------------|

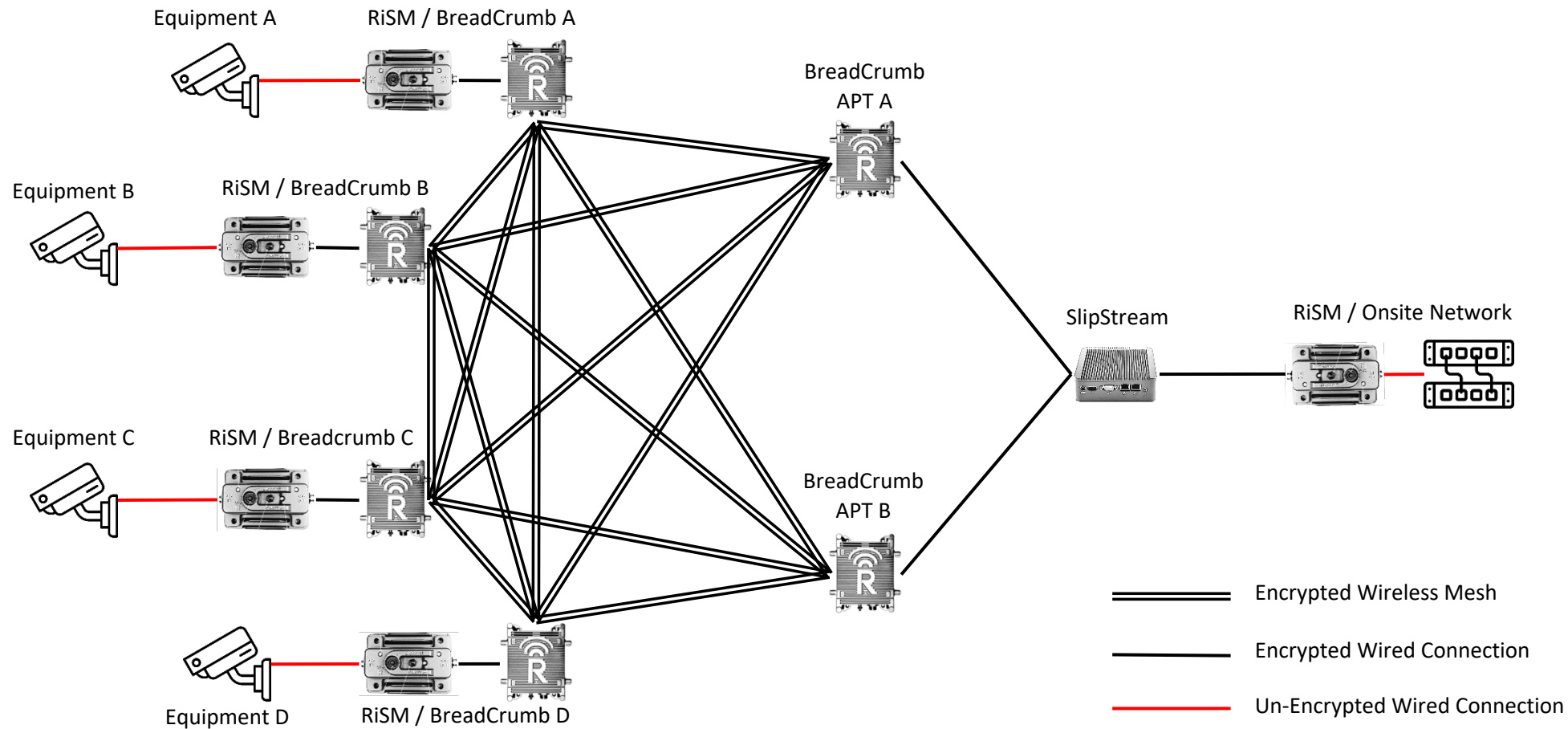
RiSM Enclave Unlock

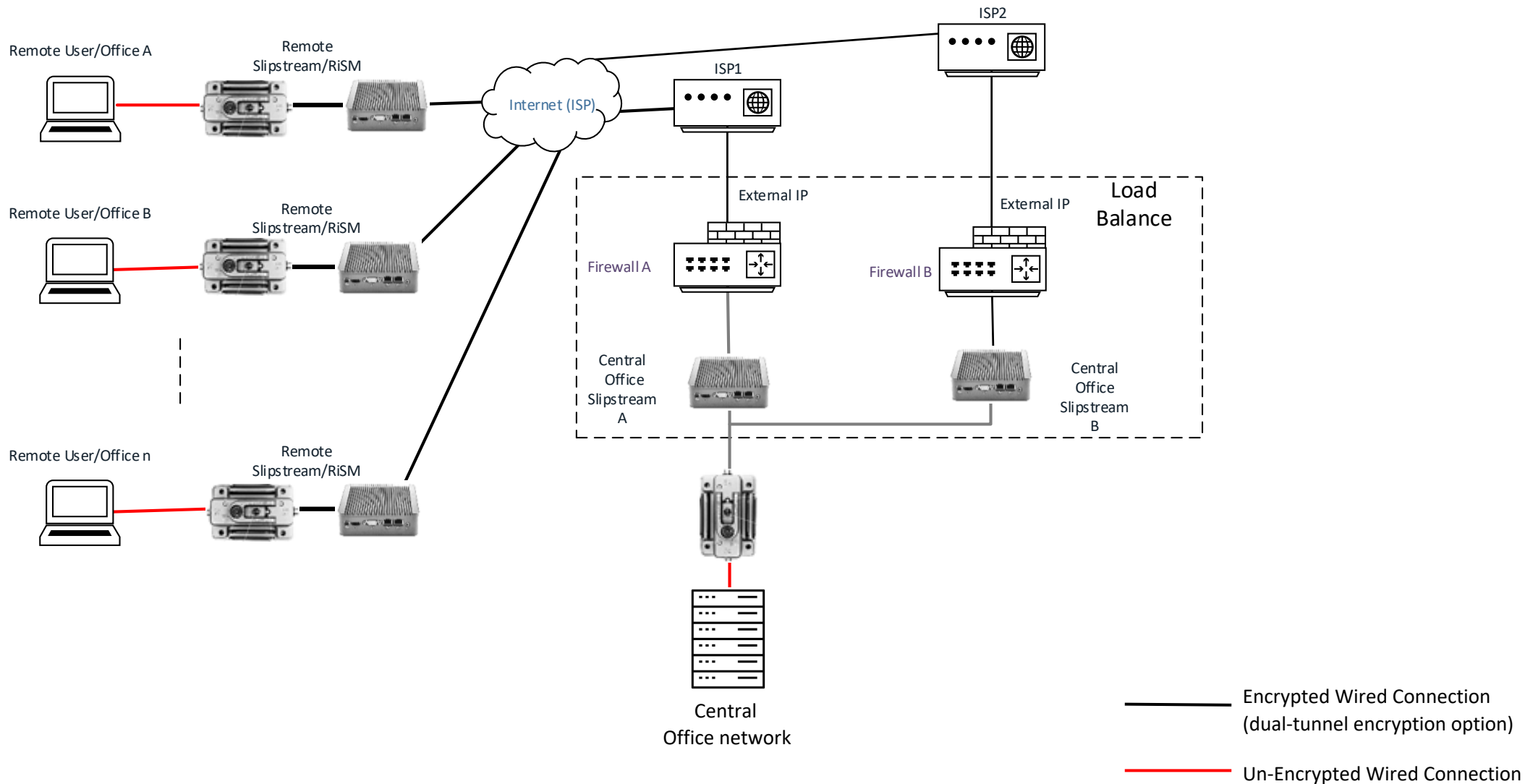
RiSM Devices

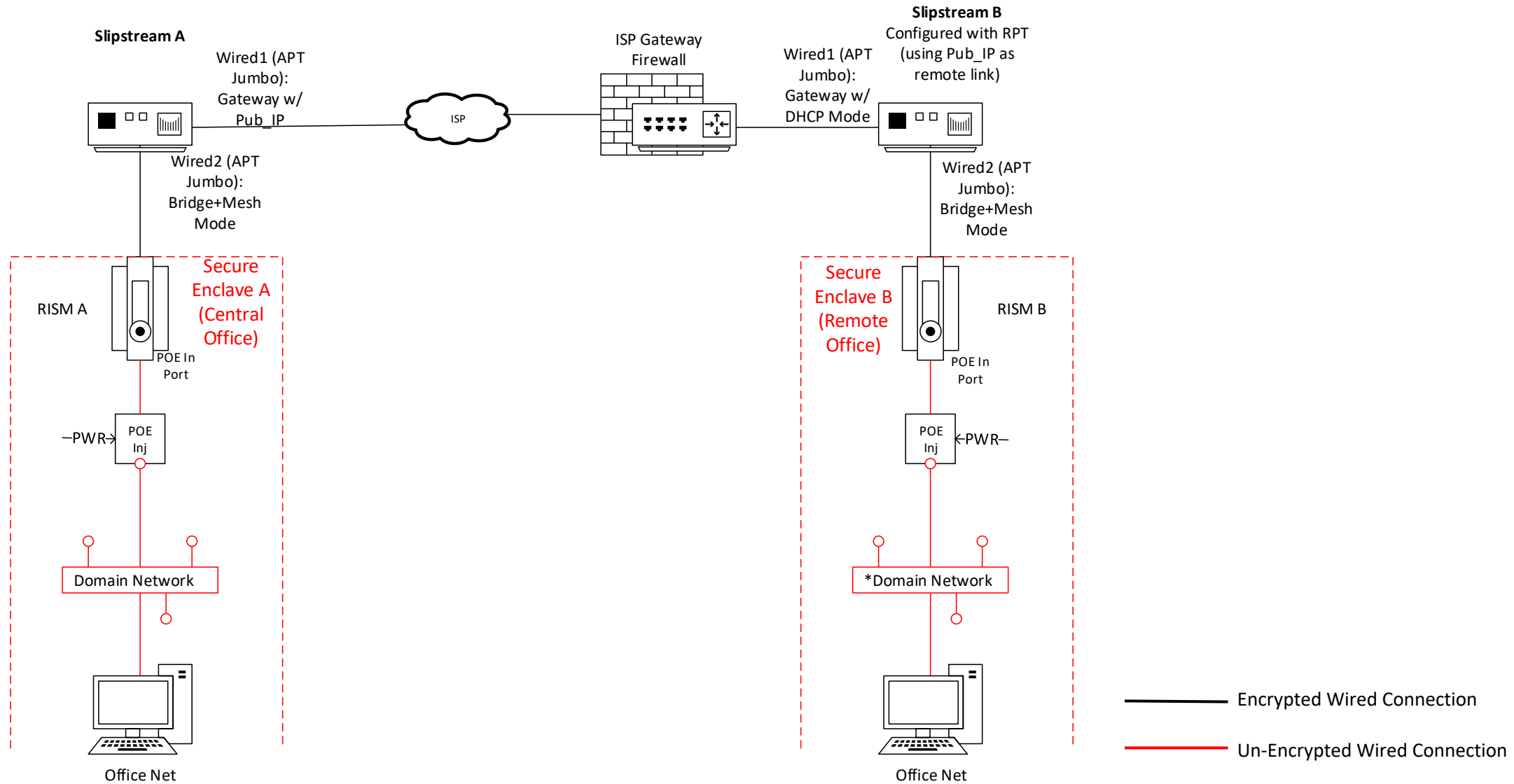
Performing RiSM Communication Check

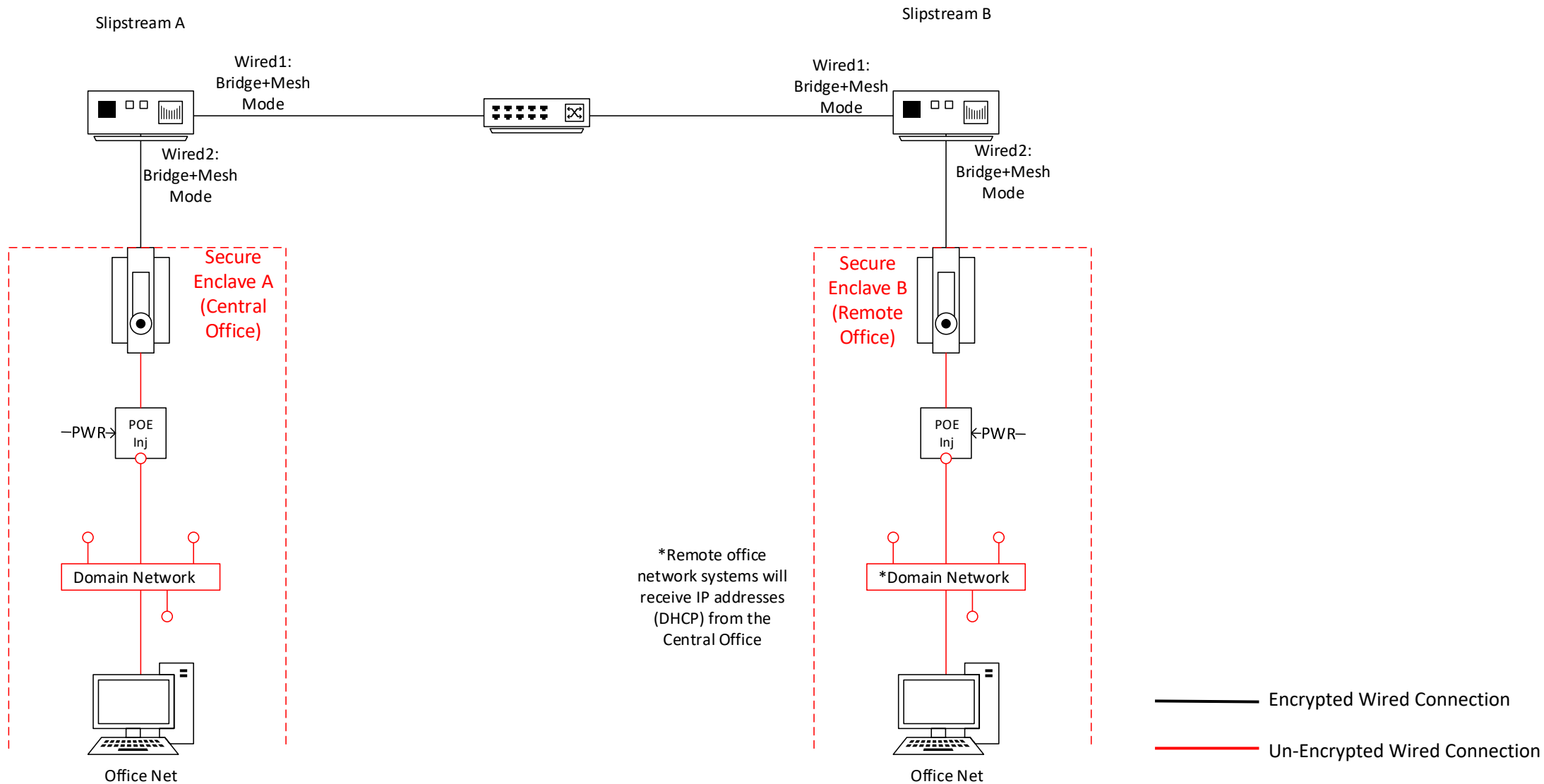
| RiSM | Progress |
|------|----------|
| 1028 | Complete |
| 1034 | Complete |

Close









 RAJANT



Thank you!