Ribbon IP Wave Portfolio Security Capabilities

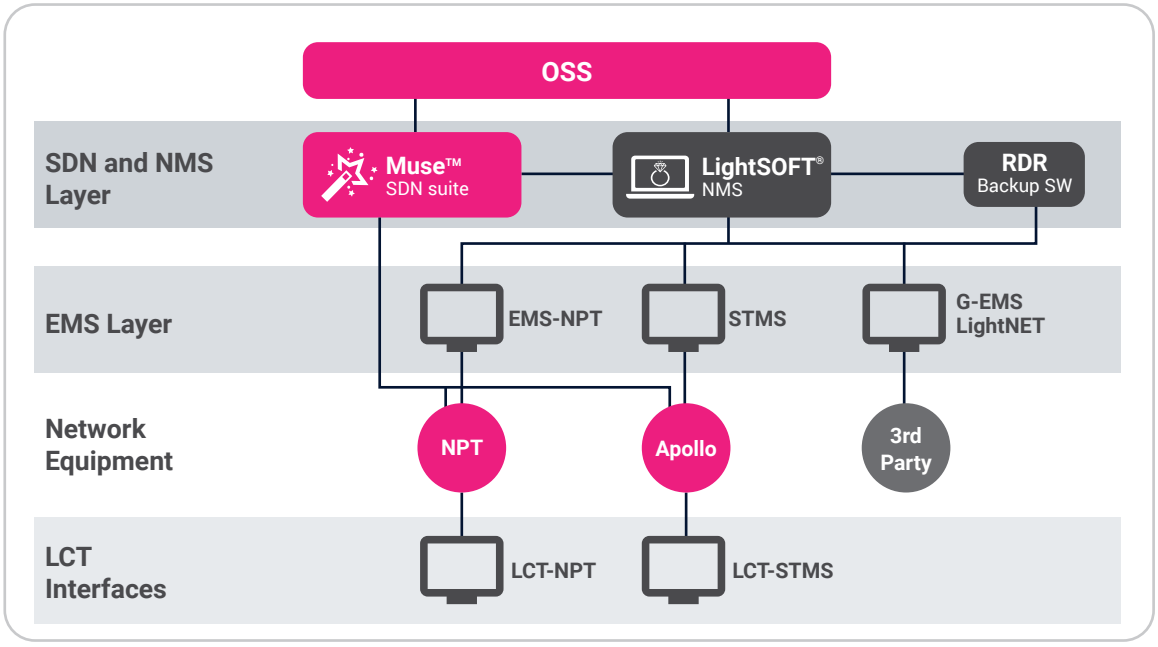
Total Protection From the Network Up

IP and optical networks are configurable with a few button clicks. Without proper protection, it can be just as easy to misconfigure or bring the network down, whether inadvertently or maliciously. To ensure that this does not occur, IP Wave is architected with multiple layers of comprehensive security throughout, from network and element management systems through to the network equipment itself. Role based-access control (RBAC) extends to operations personnel as well as end-customers using customer network management (CNM) portals. Transport Layer Security (TLS) secures all intersystem links, and the underlying operating systems are hardened. In addition, IP Wave networking products offer advanced security features, like encryption or network slicing, which the operator can use for internal purposes or offer to end-customers as a service.

User Security

Platform Security

Network Security



COMMON CRITERIA CERTIFIED EAL2

ribbon

IP Wave Security Approach

The IP Wave comprises of NPT for IP routing and packet transport and Apollo for optical networking, integrated domain control of NPT and Apollo is provided by either Muse or LightSOFT®. User and platform security protects against erroneous or malicious use of networking or management capabilities. At the same time, NPT and Apollo deliver their own value-added networking security features. This brochure highlights major aspects of the comprehensive IP Wave approach.

User Security

User security ensures that only authorized operations users can access the IP Wave management and control systems and regulates their capabilities. Notable features include:

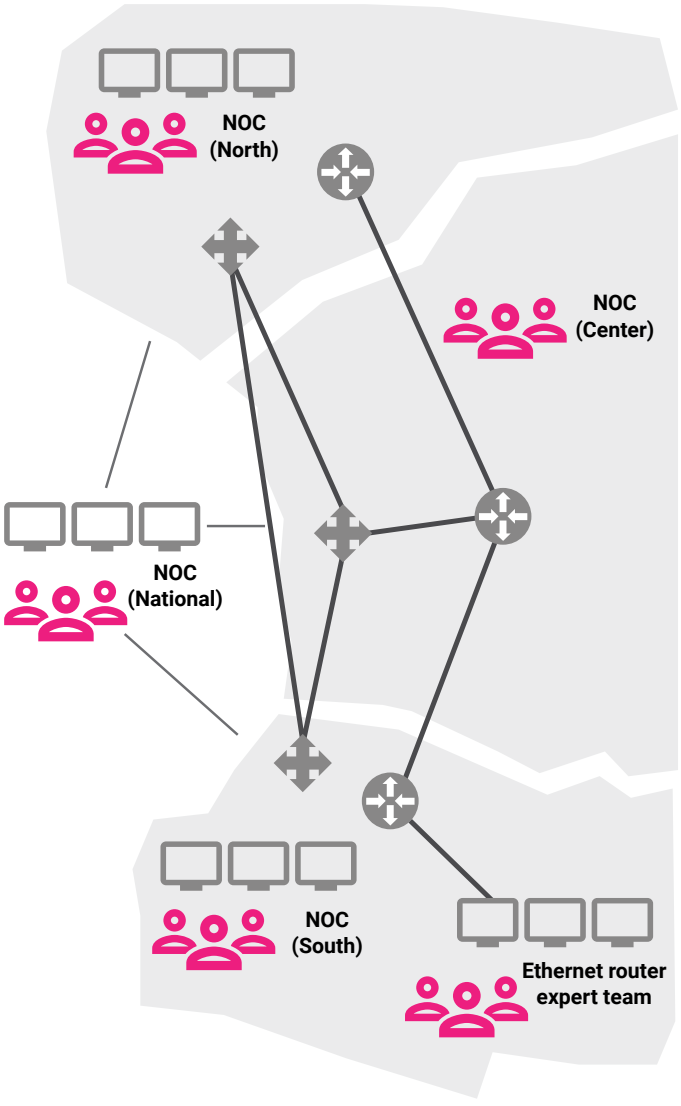
Authorization and authentication – Centrally-administered RADIUS, TACACS+, Kerberoso Land DAP based applications safeguard user access.

Two-factor authentication option – A combination of password knowledge and physical possession of a smart card significantly increases access security.

User profile management – Role-based access control (RBAC) manages the span of network domains that users can access and the range of functional control capabilities that they can exercise within those domains. Customizable prebuilt profiles for major operational categories, such as configuration, provisioning, and maintenance facilitate the creation and management of profiles for individual users or user groups.

Enhanced security – Additional controls provide added security, beyond access authorization and profiles. These include items, such as login attempt monitoring and lockouts, activity filtering, activity monitoring and logging, and file and mail restrictions.

Customer network management – Application of all the above controls to end-customers enables them to manage their transport services or subnetworks through a CNM portal. Customers gain the satisfaction of controlling their domains directly, while the network operator has the assurance that this control is isolated from interfering with other resources.



Platform Security

Platform security operates at a system level that is independent of users. It hardens communication links and underlying operation systems against improper use or hacking and ensures data integrity. Notable features include:

Secure communication links – Transport Layer Security (TLS) cryptographic protocols protect all intersystem links in the the IP Wave ecosystem, ensuring privacy between the communicating entities. This includes links among Muse, LightSOFT, networking equipment, and remote databases. Additional capabilities are IP port blocking and special authorizations for remote sessions.

Hardened operating systems – All OSs of Muse, LightSOFT, and NPT and Apollo EMSs have been hardened to protect against misuse through a range of methods. These include disabling unnecessary system services, added levels of user authorizations, and special measures like firewalls, IP Tunneling, VPNs, RAS, and NAT.

Database security – Access to management and control databases is secured, locally and remotely, via credentials that restrict access to specified application and operating system domains. For added security, aliasing is available, which hides database connection string details from data-source definitions.

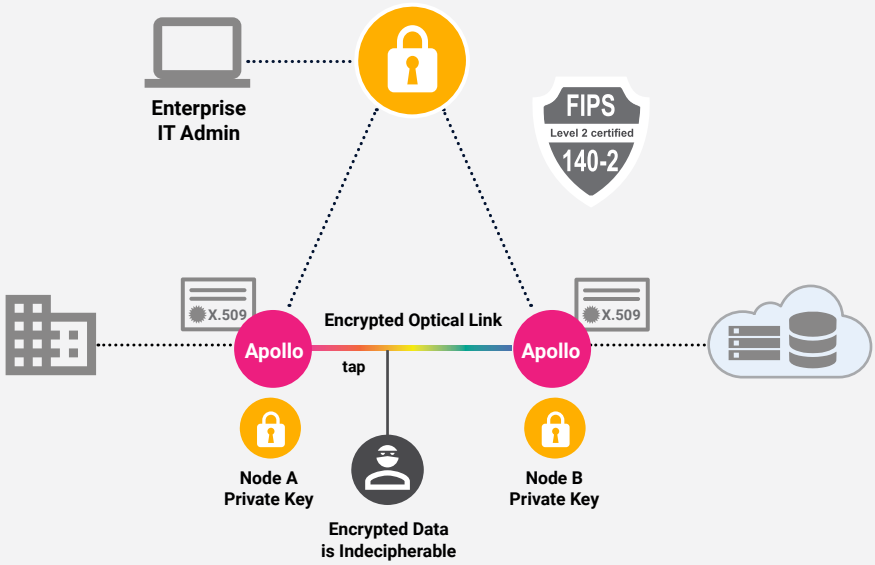
Geographic redundancy – Remote Database Replication (RDR), a field-proven flexible redundancy mechanism, provides full network management backup capabilities for disaster recovery. It is configurable for a wide variety of topologies for different geographic infrastructure distribution, security needs, and available budgets for standby mirror hardware.

Development security – Ribbon employs a secure Software Development Life Cycle process. This includes automatic static security code analysis on all Ribbon and 3rd-party software. It also analyzes and manages possible security vulnerabilities of open-source components.

Networking Security

IP Wave offers networking products offer advanced security features that network operators can use for internal purposes or provide to end-customers as a service.

Layer 1 Optical Encryption (L1OE) – The only way to protect against fiber tapping is by encrypting the optical bit stream. Apollo L1 Optical Encryption provides AES256 encryption and is fully FIPS104-2 Level 2 certified. Encryption can be applied selectively at a per-service level, or to an entire wavelength, without adding any delay to the bit stream. Apollo can also extend key administration to Enterprise IT to apply to their optical services or links without telco involvement.



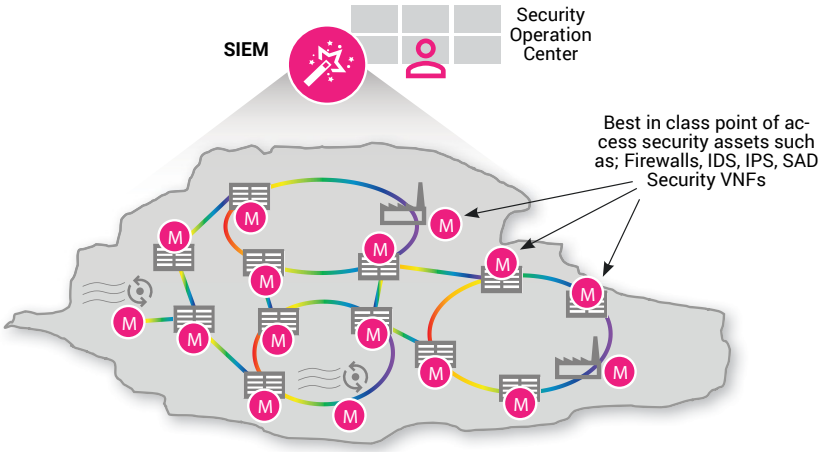
IP Routing and Packet Transport Network Security — NPT provides multiple mechanisms to protect the integrity of the IP routing and the transported packets

- **Access Control Lists (ACL)** protect routers by specifying permissions, such as a list of restricted IP addresses from which the user can access a specific device, or a list of IP addresses that the user is allowed to access within the network.
- **Layer 2 MACsec encryption** provides data origin authentication, data confidentiality, and data integrity for secure transport of media access control services among business locations over the public WAN.
- **VPN security** protects users from attacks or loss of data privacy through comprehensive filtering and segregation. The contents of packets classified to a specific VPN are not visible to other VPNs, providing sniffing or snooping protection.
- **Port-based Network Access Control (PNAC)** authenticates devices, wishing to attach to a LAN or WLAN.
- **Broadcast Storm Control** halts extremely heavy levels of incoming broadcast traffic, typically encountered under DoS attacks, giving network operators an opportunity to pinpoint and resolve the source of the problem.
- **Dynamic ARP inspection** protects against Address Resolution Protocol (ARP) spoofing and certain man-in-the-middle attacks, by intercepting and discarding ARP packets with invalid IP-to-MAC address bindings.

Security Isolation through Network Slicing — Muse manages hard and soft slicing technologies within NPT and Apollo, including FlexE, VPNs, and ODUflex. These are used to create virtual subnetworks dedicated to customer segments or service classes with a high degree of isolation from intrusion and other network traffic. Network slicing is particularly important to support performance guarantees for the different 5G service types, such as ultra-reliable low-latency communications.

Comprehensive Security Ecosystem — By supplementing the IP Wave security features with best-in-class security capabilities such as SIEMS, IDS, IPS, SCADA anomaly detection, Ribbon builds comprehensive, tailored, end-to end security ecosystems specifically matched to the business and operational needs of our customers.

Ribbon's approach to total protection of its product portfolio, supplemented by best-in-class industrial leading security assets, provides network operators with peace of mind that their networks are protected against inadvertent user errors and malicious attack.



About Ribbon

Ribbon Communications (Nasdaq: RBBN) delivers communications software, IP and optical networking solutions to service providers, enterprises and critical infrastructure sectors globally. We engage deeply with our customers, helping them modernize their networks for improved competitive positioning and business outcomes in today's smart, always-on and data-hungry world. Our innovative, end-to-end solutions portfolio delivers unparalleled scale, performance, and agility, including core to edge software-centric solutions, cloud-native offers, leading-edge security and analytics tools, along with IP and optical networking solutions for 5G. We maintain a keen focus on our commitments to Environmental, Social and Governance (ESG) matters, offering an annual Sustainability Report to our stakeholders. To learn more about Ribbon visit rbbn.com.

Contact Us Contact us to learn more about Ribbon solutions.