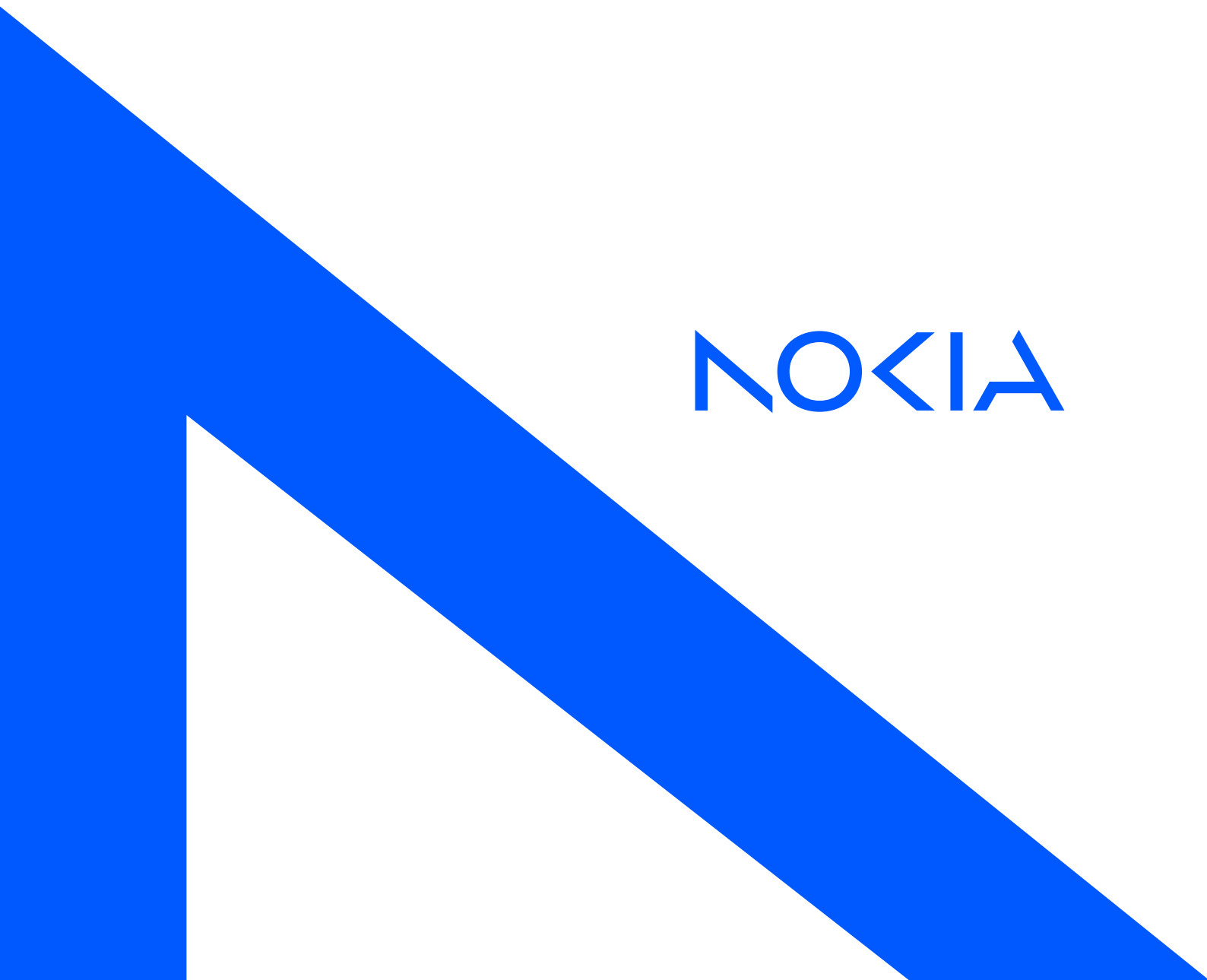
Security for microwave links

Risks and mitigations for point-to-point microwave

Application note



Abstract

Over many decades, point-to-point microwave radio has proven to be a secure mechanism for transmitting sensitive voice, video, and data communications. It is a leading solution for backhaul of cellular traffic worldwide, and it is a trusted technology for the hundreds of thousands of networks supporting mission-critical communications for power utilities, military operations, public safety, first responders, and homeland security agencies. In this paper, recommendations are made for the security capabilities of wireless point-to-point microwave communications. In addition, the paper highlights flexible security design combined with the inherent security capabilities of the Nokia 9500 Microwave Packet Radio (MPR).

Contents

Overview

This document provides information regarding the security capabilities of wireless point-to-point microwave communications, along with recommendations on using these capabilities. The topic of wireless network security is quite broad and depends on the wireless technology used, plus the security requirements of the organization. Potential threats to wireless network security can take the form of eavesdropping, unauthorized access, signal interference, or creating a signal disruption. Preventive measures should be taken to minimize these risks based on the technology deployed. Point-to-point microwave transmission is highly secure, due to the characteristics of its propagation and equipment design, but organizations should develop a robust network-based security policy that includes this technology and enforce it.

A security policy is an organization's foundation for designing, implementing, and maintaining properly secured technologies. The policy should address the design and operation of the technical infrastructure and the behavior of users. Devices should be configured to comply with policies, such as disabling unneeded services and altering default configurations.

Wireless LANs vs. Point-to-Point microwave links

Wireless LAN (WLAN) systems

Wireless LAN (WLAN) systems, such as those based on IEEE 802.1x standards like 802.11 (Wi-Fi®) and 802.16 (WiMAX), operate in a point-to-multipoint (P2MP) or mesh fashion. One or more access points (AP) function as hubs, which transmit and receive in all directions or in wide sector-based coverage to communicate with multiple standards-based devices from multiple manufacturers in proximity to the AP. Since each device is inherently able to talk to any other device, encryption technology, such as Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA or WPA2), is employed to prevent eavesdropping and unauthorized access to the signals and information being transmitted. Encryption is enabled by simple provisioning of each AP and device. Over the years, these devices have been the target of many well documented methods of intercepting and decrypting their signals. There are even commercial devices built for the purpose of testing the vulnerability of these types of systems. Therefore securing these types of networks has become a continuous task.

Point-to-Point microwave links

In contrast, Point-to-Point (P2P) microwave links are designed to communicate exclusively between two radio transceivers from a single manufacturer. The radio equipment at each end has no provision for transmitting to or receiving from a device other than the far-end radio. Because they communicate only to the far-end antenna, the antennas are also narrow beam and highly directional. Therefore, the potential threats to microwave links and the corresponding measures to enable secure transmissions over these links are much different than for P2MP systems. An attacker will encounter significant challenges to actually detect and receive the microwave signals, face difficulties in intercepting message traffic, and will ultimately find it impractical to penetrate any network through a microwave link.

Vulnerabilities and threats for P2P systems

This section describes vulnerabilities in P2P systems, threats to these systems, and some countermeasures to mitigate those threats. As discussed earlier, P2P systems are susceptible to specific threats as well as threats common to all wireless technologies. Organizations should mitigate threats and vulnerabilities by implementing a combination of management, operational, and technical countermeasures.

The vulnerabilities specific to P2P systems are far fewer than for other wireless technologies. P2P network threats focus on compromising the radio links between nodes. P2P systems pose a greater challenge to attack than P2MP or mesh systems, because an adversary would have to physically locate equipment between the transmitting nodes to compromise the confidentiality or integrity of the wireless link. The security mechanisms available in these systems address some, but not all, of the shortcomings. Many of the recommended mitigations are procedural or address the network architecture more holistically. The following sections discuss several major vulnerabilities and threats.

Lack of radio-to-radio authentication: eavesdropping

Eavesdropping occurs when the attacker uses a traffic analyzer or “sniffer” within the signal on a P2P link. Eavesdropping mitigation relies heavily on technical controls that protect the confidentiality and integrity of communications. The attacker wants to monitor management message traffic to identify encryption ciphers, determine the footprint of the network, or conduct traffic analysis to gain network intelligence or information that will allow network penetration. Lack of mutual authentication between radios on a P2P link may allow a rogue radio to impersonate a legitimate radio, thereby rendering the far end unable to verify the authenticity of protocol messages received from the originating radio. A successful attack would enable a rogue radio operator to take complete control of all traffic over the link, including capture of authentication credentials. Such an attack would also enable access to other parts of a network. This vulnerability is mitigated by using link identifiers between radios on the P2P link. Once set, the far-end value and near-end value must match for the radio link to lock up, or the link will drop.

Unencrypted management messages

Management messages that are not encrypted are susceptible to eavesdropping attacks. In many cases, encryption is not applied to these messages to increase the efficiency of network operations. The best mitigation is to encrypt the management and control between the network management system (NMS) and the radios. Simple Network Management Protocol Version 3 (SNMPv3) is recommended for all management traffic between the P2P radios and the NMS because it solves the risk of unencrypted management traffic. This protocol includes the following important security features:

- Confidentiality – Encryption of packets to prevent sniffing by an unauthorized source
- Integrity check – Message integrity to ensure that a packet has not been tampered with in transit, including an optional packet replay protection mechanism
- Authentication – Verification that the message is from a valid source

Use of electromagnetic spectrum as a disruption: radio frequency (RF) jamming

Using RF to communicate inherently enables execution of a denial of service (DoS) attack by introducing a powerful RF source intended to overwhelm system radio spectrum. This vulnerability is associated with all wireless technologies. The only defenses are either to locate and remove the source of RF interference or to change frequencies. This type of attack is not common, but one recommended method for mitigating a determined attack is to plan for out-of-band communications.

Man in the middle

These attacks occur when a device is inserted to appear as a legitimate radio repeater to both ends of a P2P link simultaneously. This can allow the attacker to act as a pass-through for all communications and to inject malicious traffic into the communications stream. An attacker would perform a man-in-the-middle attack by exploiting unprotected management messages during the initial network entry process. This can be effective because management messages that control how the link communicates are not protected. The mitigation combines link identification that is hard to duplicate with encryption of the control traffic for the radio. This risk is discussed in more detail in the “Man in the middle attack is improbable” section.

Physical access

Often, the most cost-effective mechanism for gaining access to the physical network is through unsecured ports, management interfaces, and cabling. In many cases, the physical cable between the radio and antenna—or between the radio and an adjacent network device—can be tapped or compromised, which allows eavesdropping when the attacker uses a traffic analyzer or “sniffer.” Mitigating this risk may be as simple as ensuring that only authorized personnel have access to microwave equipment. Physical security includes measures such as physical access control systems, personnel security and identification, and external boundary protection.

Challenging to detect

In contrast to P2MP systems, P2P microwave transmits a highly directional radio signal between antennas over a line-of-sight path. The highly directional nature of P2P microwave inherently makes detection and reception of the radio signal very difficult. If attackers wished to operate from a location far from either end of the path, they would have to raise an antenna for everyone to see, in order to get within the stronger beam width of the signal. Or they would need to move near one of the radio sites in the hope of snagging the much weaker signals off a side lobe. In either scenario, maintaining a covert operation would be a challenge.

For example, consider the radio beam available to the attacker. The angle of radio beam spread is inversely proportional to the size of the antenna and the frequency used. The approximate formula for the half-power beam width of microwave signals using parabolic antennas is:

$\phi \approx 70/(d \bullet f)$

In this formula, d is in feet and f is in gigahertz. So, for a given frequency and antenna size, the width of the microwave beam is simply a function of the distance traveled:

$BW = \text{distance} \bullet \sin(\phi)$

For short-haul transmission, the antenna sizes may be small, yet higher frequencies are often used. Antenna size and frequency balance to create beam-width angles that are similar to long-haul transmission, which uses larger antennas and lower frequencies. For instance, an 18-GHz radio with a 2-foot antenna and a 6-GHz radio with a 6-foot antenna both have beam widths of 1.94°.

In the first case, if attackers were around 1000 feet from the transmitter (less than ¼ mile) and raised an antenna into the signal path, they would have a target only several feet in diameter to enable reception. In the second case, an attacker would need to be directly next to the transmitting antenna on the tower to capture side lobe signals.

Difficult to intercept

Even if an attacker could establish a covert location to detect and receive signals from a microwave link, actually decoding the radio signal into a recognizable data stream would be extremely difficult. Each microwave radio vendor uses unique modulation and data-framing techniques along with data scrambling. The attacker would have to purchase exactly the same radio model that is operating over the link, somehow tune it to the specific radio frequency used on that path, and get the intercepting antenna to be within the beam width of the transmitting antenna (and risk being exposed and caught).

Today's radios are provisioned with an identification code (link identifier) to allow communication only with its paired unit at the far end of the path. Therefore, an attacker can only capture the raw transmitted signals and cannot access the network from within the link. Once the attacker has the raw signal data, it would be unreadable. So he would also need equipment to demodulate the signal at the same rate the current signal is configured to use—and to demultiplex the desired traffic from the radio's payload. This equipment has to match the payload type, which could be channel banks, T1/T3 multiplexers, SONET multiplexer, video codec and/or packet-based sniffer for switch and router traffic.

The Nokia 9500 Microwave Packet Radio (MPR) is a carrier-class packet microwave radio, based on patented technology that allows the transport of Ethernet and TDM traffic and the distribution of a physical Layer 1 synchronization signal over packetized wireless links. These patented technologies start in the base level of the radio framing, continue into the next layer of the modulation schemes, and finally extend into the Ethernet frames and sequencing. This complex set of interacting technologies allows the Nokia 9500 MPR to perform flawlessly under many different conditions—and also renders any intercepted signals undecipherable.

Low probability to penetrate

Unauthorized access

It is an extreme proposition to place an illegal transceiver in line with a microwave radio beam to intercept just half of a radio transmission (that is, one direction only). But is it possible to actually "hack into" the link to penetrate the microwave operator's network? In brief, it is highly improbable, and the reason has nothing to do with encryption. As discussed earlier, the two radios communicate with each other exclusively in a full duplex link. Each radio is always locked onto the signal transmitted from the far end. Attempting to infiltrate the link by transmitting another signal into either receiver will create interference and jam the radio transmission—creating an alarm notification at the receiver and dropping the link.

Man in the middle attack is improbable

In this scenario, an attacker must gain a position between the two ends of the radio link, establish independent connections with each end, continue to relay information between them, and make them believe they are talking directly with each other over a private connection. Once this middle repeater has infiltrated the microwave link, it could operate at the traffic layer to intercept messages and inject new ones. This approach has two key problems. First, to transmit into both of the end radios, the attacker must totally block the intended signal from reaching the far end. Otherwise it will create the same jamming or interference issue described previously and take down the link. The physical size of a screen or panel used to block the radio signal would be an obvious sign of nefarious activity. The second problem has to do with the network emulation required at the midpoint. This middle radio needs to simultaneously function as a radio repeater while not appearing as an addressable device. This contradiction in networking requirements will generate alarms in the management system and the microwave nodes—and block the flow of traffic.

Countermeasures

This section summarizes many of the countermeasures already discussed that may be used to reduce or mitigate the risks inherent in P2P radio links. These countermeasures do not guarantee security and cannot prevent all possible attacks. The optimum security design is a dynamic balance between the level of threat risk and the cost of countermeasures. Organizations should implement countermeasures commensurate with their acceptable level of risk. The management, operational, and technical countermeasures described in the following sections take an approach similar to that of the National Institute of Standards and Technology (NIST).[1]

Management countermeasures

Management countermeasures generally address any problem related to risk, system planning, or security assessment by an organization's management. Organizations should develop a wireless security policy that addresses P2P radio links. This security policy will be the foundation for designing, implementing, and maintaining properly secured P2P links. A P2P microwave policy should address the design and operation of the technical infrastructure and the behavior of users. Policy considerations should include the following:

1 The National Institute of Standards and Technology (NIST) webpage is http://csrc.nist.gov/publications/PubsSPs.html Recommended best practices were adopted from the Special Publication 800 series documents of general interest to the information security community, including several on wireless security. The Special Publication 800 series was established in 1990 to provide a separate identity for information technology security publications.

1. Roles and responsibilities

- Which users or groups of users are authorized to use the microwave
- Which office or officer provides the strategic oversight and planning for all microwave technology programs
- Which parties are authorized and responsible for installing and configuring microwave equipment
- Which individual or entity tracks the progress of microwave security standards, features, threats, and vulnerabilities to help ensure continued secure implementation of P2P microwave
- Which individual or entity is responsible for incorporating microwave technology risk into the organization's risk management framework

2. Microwave infrastructure

- Physical security requirements for microwave assets
- The use of standards-based microwave system technologies
- Types of information permitted over the microwave system, including acceptable use guidelines
- How microwave transmissions should be protected, including requirements for the use of encryption and for cryptographic key management
- A mitigation plan or transition plan for legacy or microwave systems that are not compliant with the organization's adopted security standards
- Inventory of microwave and other dependent devices

3. Microwave security assessments

- Frequency and scope of security assessments
- Standardized approach to vulnerability assessment, risk statements, risk levels, and corrective actions

Operational countermeasures

Operational countermeasures include controls that are executed by people, such as personnel security, physical environment protection, configuration management, security awareness and training, and incident response. These controls are documented in a system security plan (SSP) which should be maintained by all parties involved with microwave operations. SSPs are living documents that provide an overview of the security requirements of a system and describe the controls in place to meet those requirements. This includes all system hardware and software, policies, roles and responsibilities, and other documentation materials. Documentation itself is a security control,
as it formalizes security and operational procedures to a given system.

Physical security is fundamental to ensuring that only authorized personnel have access to microwave equipment. Physical security includes measures such as physical access control systems, personnel security and identification, and external boundary protection. Microwave system administrators and users should receive training to address the specific challenges and threats to wireless technologies. While it is difficult to prevent all unauthorized users from attempting to access a microwave system, the use of additional security mechanisms may help prevent theft, alteration, or misuse of microwave components.

The Nokia 9500 MPR customers have the capability to add an optional intrusion device to prevent cards to be easily tampered with per FIPS suggestions. Additionally all outdoor radio units have tamper detection devices so customers can see if someone has tried to tamper with the outdoor radio unit.

P2P microwave technologies operate on licensed or unlicensed RF spectrum. The spectrum used most often includes licensed P2P frequencies assigned by the country-based regulatory authority. (The US body is the FCC.) But microwave solutions are also viable across several unlicensed spectrum ranges. Organizations should understand the implications of spectrum allocation as it impacts system availability. Due to the proliferation of unlicensed wireless technologies, interference may become an implementation obstacle when operating in unlicensed spectrum. Regardless of which spectrum frequency is used, organizations should use counter-interference technologies in addition to site surveys to ensure system availability.

Prior to deployment, site surveys construct the foundation for a microwave system's design to ensure system availability. Long-distance radio transmissions should be tailored and optimized for RF obstacles and interference sources. Site survey tools include terrain maps, global positioning systems, RF propagation models, spectrum analyzers, packet analyzers, and other tools that can provide a more thorough understanding of the environment's RF landscape. A site survey requires specialized skills, and it is typically provided as part of the overall vendor solution. Organizations should, at a minimum, involve themselves in the site survey process and document its findings in the system security plan (SSP).

As with all wireless technologies, operational countermeasures may not provide protection against general wireless threats, such as DoS, eavesdropping, and man in the middle. However, operational controls rely upon both management and technical controls and often require highly specialized expertise.

Technical countermeasures

These countermeasures are system safeguards implemented with technology, such as management systems, authentication, access control, auditing, and communication protection. Technical countermeasures are typically designed into microwave systems before implementation and vary widely among vendors. Before implementing a microwave system, an organization should consult vendors to gain a better understanding of potential system reconfiguration constraints and the need for compensating controls to address technical security needs that an individual product may not address.

Confidentiality and integrity protection

P2P microwave links broadcast data over a large geographic area, which is usually outside the organization's physical control. Organizations must rely on link-level protection to provide confidentiality and integrity protection for its wireless links. Many organizations that need to protect the confidentiality of their data communications are required to use corporate-approved encryption algorithms. This can be accomplished in one of two ways. The first method uses equipment-based encryption implemented directly in the vendor's hardware or software. The second encrypts the data through a separate encryption technology, such as encryption overlay solutions to protect OSI data link or network layer data communications. Data link encryption overlay solutions provide encryption, including packet headers and trailers, for all data traffic taking place at the OSI network layer, or they can supply group-based encryption for specific applications while allowing other traffic to remain unencrypted. Network layer encryption solutions provide encryption for the data portion of the network layer, including all upper-layer data. Encryption overlay solutions require an encryption appliance behind the P2P radio and a corresponding termination point on the end-user device.

A virtual private network (VPN) offers another method of providing confidentiality and integrity protection. A VPN is a virtual network that creates a secure tunnel between devices, which provides a secure communications channel for data and IP information. VPNs are often used to facilitate the secure transfer of sensitive data across shared and untrusted networks. VPNs are a mature technology, and a variety of VPN technologies exist, such as IP/MPLS which allows for Layer 2 or Layer 3 VPNs. IPsec, PPTP, and Secure Sockets Layer (SSL) are other examples of VPN technologies. VPN services are independent of OSI data link

layer protocols, and they are recommended for use as an overall end-to-end data service technology to simplify network design and architecture.

Authentication and authorization

P2P radio nodes support an array of solutions that provide both device and user authentication. These authentication solutions can support the use of usernames and passwords, two-factor authentication methods, and so forth. Organizations should strongly consider centralized security solutions capable of supporting P2P nodes integrated with the rest of the network security policy, that is, TACACS+ or RADIUS. TACACS+ uses the Transmission Control Protocol (TCP), and RADIUS uses the User Datagram Protocol (UDP). Some network controllers recommend using TACACS+ because TCP is seen as a more reliable protocol. One additional difference is that RADIUS combines authentication and authorization in a user profile, while TACACS+ separates the two operations. Microwave solutions that cannot meet the criteria should employ a different means of authentication at a higher layer, such as encryption overlay or VPN.

Layer 1 encryption over microwave links

For specific domains such as Defense, Public Safety and Critical Infrastructure networks, where confidentiality and protection are of utmost importance, Nokia has developed a unified optical and microwave transport network performing symmetric Layer 1 encryption. The implementation relies on NIST's Advanced Encryption Standard (AES); it uses robust 256-bit AES keys to encrypt data flows and transport information securely.

The encryption capability is built into the Nokia 9500 MPR and introduces less than 1 microsecond delay into the over-the-air encrypted RF signal links. The encryption is performed on the microwave radio physical layer by the Microwave Packet Transceiver thus simplifying the encryption process. This common optical and microwave solution relies on a unique and highly secure hardware platform that manages the encryption keys of both Nokia 1830 PSS (Optical) and 9500 MPR systems.

The integrated Layer 1 highly secure optical and microwave transport network solution from Nokia complements existing encryption solutions according to the defense-in-depth principle. The solution complements other techniques used at higher layers like Ethernet/MAC security (MACsec), Layer 3/ IPSec and Network Group Encryption (NGE) by enabling a first line of defense, which increases security by ciphering full data flows (payload, headers, CRC, addresses MAC/IP). The system fits perfectly in use cases that need to secure high-capacity links without adding latency. Thus, the solution enables real-time communication for critical applications and synchronous replications to connect remote sites.

The Nokia multi-layered encryption solution covers multiple OSI layers with a set of network systems and was recognized by Frost & Sullivan with the "2015 New Product Innovation Award for North American Cyber Security Solutions for Utilities."

Read more on Nokia's unified, certified and secure transport networks for critical infrastructure providers: https://resources.nokia.com/asset/192614.

Summary

The most flexible security design combines the inherent security capabilities of the Nokia 9500 MPR platform with a sound security policy and security framework. For maximum security that cannot easily be circumvented, solutions can use individual link identifiers, secure protocols support such as SFTP, HTTPS, SSH, and SNMPV3 management traffic encryption and validation, and authentication and authorization mechanisms like TACACS+, with a flexible end-to-end group-based encryption overlay that is application- and service-based.

Over many decades, point-to-point microwave radio has proven to be a secure mechanism for transmitting sensitive voice, video, and data communications. It is the leading solution for backhaul of cellular traffic worldwide, and it is a trusted technology for the hundreds of thousands networks supporting mission-critical communications for power utilities, military operations, public safety, first responders, and homeland security agencies. Point-to-point microwave offers a cost-effective alternative to leased lines and wireline facilities, with high availability and flexible installation options. Nokia is the leading provider of microwave communications links in North America, as well as the worldwide leader for packet microwave. We invite you to enjoy the benefits of our secure wireless technology and the highest Quality of Service and security available.

Nokia is recognized as the industry leader for packet microwave. More than 350 operators around the globe have deployed the Nokia 9500 MPR to address mobile backhaul and enterprise applications.

Abbreviations

9500 MPR	Nokia 9500 Microwave Packet Radio
2G, 3G, 4G	Second Generation, Third Generation, Fourth Generation
AP	Access Point
IP	Internet Protocol
IPsec	Internet Protocol Security
LAN	Local Area Network
LTE	Long Term Evolution
NMS	Network Management System
P2P	Point-to-Point
P2MP	Point-to-Multipoint
QoS	Quality of Service
RF	Radio Frequency
WLAN	Wireless Local Area Network

Contacts

For more information about Nokia 9500 MPR solutions, please visit:
www.nokia.com or contact your Customer Team representative.

About Nokia

At Nokia, we create technology that helps the world act together.

As a trusted partner for critical networks, we are committed to innovation and technology leadership across mobile, fixed and cloud networks. We create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Adhering to the highest standards of integrity and security, we help build the capabilities needed for a more productive, sustainable and inclusive world.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: (February) CID157676