White Paper

Securing modern wireless IP communication networks from ABB Wireless

Modern wireless IP communication networks are being used increasingly in a wide variety of industrial applications by utilities, oil and gas companies, mining companies and others. Each industrial application presents its own, unique communication network security requirements.

To benefit network owners and operators, ABB Wireless has used its fifteen-plus years of experience in deploying more than 1,000 customer networks to develop the technology and techniques necessary to meet the security requirements of multi-use wireless communication networks. ABB Wireless' vast experience implementing communication networks for a wide array of industrial applications and verticals uniquely positions the organization to meet these diverse security needs.

It would be challenging enough to meet each of these security requirements if only one industrial application used each network. However, modern wireless IP communication networks deliver the greatest return on investment (ROI) when multiple applications and classes of users share the same physical network infrastructure. As a result, deployment of multi-use industrial communication networks is becoming commonplace.

Multi-use networks complicate the security picture by necessitating that the security requirements of all applications and classes of users be satisfied simultaneously. While there may be commonality of some requirements, the security needs of some applications and user groups may be mutually exclusive. For example, both the basic (e.g., use of WPA2 and SSID suppression) and advanced (e.g., use of VPNs and filters/firewalls that permit only VPN traffic to traverse the network) techniques that can be used to secure a SCADA network cannot be used by communication networks for contractor and guest connectivity that depend on the ability of any standard 802.11 client to easily access the network.

This paper enables network administrators, network architects and CIOs to understand the multi-layer, defense-in-depth security approach that ABB Wireless has used successfully to secure hundreds of wireless IP communication networks.

A multi-layer, defense-in-depth approach to wireless network security

ABB Wireless has used its unparalleled experience in deploying field area wireless IP communication networks to develop a multi-layer approach that achieves robust network security by leveraging time-tested and industry-proven techniques.

The task of securing wireless networks can be divided into five challenges:

1. Network access control
2. Network resource protection
3. End-point, including wireless client, protection
4. Secure end-to-end data traffic transmission
5. Secure network configuration, operation and management

ABB Wireless security elements incorporate and extend industry best practices for securing wireless networks, resources and data. We implement only security algorithms that have been industry-proven and verified, and that have been shown to be appropriate for field area wireless IP communication networks.

The principles used to craft our security approach include:

- Multi-layer – Utilize multiple security mechanisms at several network layers, employing defense-in-depth to provide high levels of protection.
- Time-tested and proven – Utilize well-known security techniques that have undergone extensive scrutiny by the security community and can offer users a strong degree of confidence in their implementation.
- Open, standards-based – Integrate open, standard elements so that a wide variety of economical clients and end-devices can securely attach to the network.
- Upgradeable – Incorporate upgradeability into products so that future security threats can be countered quickly and new security standards and innovations integrated via new software loads.
- Flexible – Accommodate the security requirements of the different applications and user communities sharing the network such that ROI can be maximized.

Each of the advanced security techniques employed in the ABB Wireless security model satisfies these design criteria. Techniques, protocols and algorithms such as traffic filtering, WPA2, EAP, RADIUS, AES, HTTPS, and VPNs have been employed for many years in a wide variety of Internet applications. Leveraging the higher-layer intelligence of our products, ABB Wireless combines the best Internet and wireless security techniques to offer a robust and multi-layered security framework. No other wireless networking product combines all these elements to offer the highest levels of protection.

In the following sections, we outline how the ABB Wireless security features operate to secure the wireless communication network for even the most stringent operator requirements.

1. Network access control

Wireless network security begins with prohibiting access by unauthorized wireless devices while ensuring that authorized clients can connect reliably. ABB Wireless products support a wide variety of network access control mechanisms that can be tailored to meet a broad range of access control requirements.

Wi-Fi Protected Access 2 (WPA2) authentication (TropOS and MicrOS product line)

WPA2 is the Wi-Fi Alliance's latest security standard. It defines both authentication and encryption mechanisms, providing an interoperable implementation of the IEEE's 802.11i security standard.

WPA2 uses port-based access control built on IEEE 802.1x. The TropOS and MicrOS product lines support 802.1x authentication using the Extensible Authentication Protocol (EAP) and RADIUS. EAP supports multiple methods including PEAP, EAP-TLS and EAP-TTLS. Additionally, authentication and access control can be based on the use of Pre-Shared Keys (PSK).

Note that WPA2 authentication cannot be used in contractor and guest access networks where the network operator wants new users to be able to register via the wireless network.

MAC address Access Control Lists (ACLs) (TropOS, MicrOS, ArcheOS and TeleOS product lines)

MAC address Access Control Lists (ACLs) provide additional protection when used in conjunction with other Layer 2 security mechanisms.

ABB wireless products support the creation and administration of ACLs based on client MAC addresses. These ACLs can be whitelists and/or blacklists.

Creating a MAC address whitelist will allow only specific client MAC addresses to connect to the wireless network. Client MAC addresses not on the whitelist will not be able to connect to the network.
A MAC address blacklist will deny specific client MAC addresses the ability to connect to the wireless network. When a blacklist is employed, only client MAC addresses not on the blacklist have the ability to connect to the wireless network.

MAC address whitelists and blacklists can be created and administered from the SuprOS communication network management system. SuprOS centrally manages whitelists and blacklists and provisions them onto ABB Wireless products.

Because hackers can spoof the MAC address of a valid client, MAC address-based authentication can be only one element of a layered security architecture.

Note that MAC access control whitelists cannot be used in contractor and guest access networks where the network operator wants new users to be able to register via the wireless network.

MAC access control blacklists are suitable for all types of wireless IP communication networks.

SSID suppression (TropOS product line)
IEEE 802.11 access points typically broadcast their Service Set Identifier (SSID) (their network name) to allow client devices to discover the network. For networks where public access is desired, this is an essential function, altering potential users of the network's availability. However, for a private network, that is, one where access is limited to a specified set of users who already know of its existence, SSID broadcast is undesirable because it announces the network's availability to unauthorized persons.

TropOS mesh routers allow network administrators to optionally suppress SSID broadcasts. In a private network, this does not hamper user access because client devices can be configured to attach to the network even though the SSID is suppressed. Suppressing the SSID broadcasts means that unauthorized persons will not know the network is available unless they use sniffing tools.

SSID suppression has been shown to be vulnerable to passive attacks, and is therefore considered inadequate if used alone. However, it is useful as a deterrent because it prevents a casual hacker from quickly accessing the wireless network.

Note that SSID suppression cannot be used in contractor and guest access networks where the network operator wants new users to be able to register via the wireless network.

Per user group authentication policies using multiple VLANs and SSIDs (TropOS, MicrOS, ArcheOS and TeleOS product lines)
To provide operators the flexibility to accommodate multiple classes or groups of users with differing wireless settings and security needs, ABB Wireless products support multiple virtual LANs (VLANs) and SSIDs (TropOS mesh routers only) with per-VLAN security configuration support.

Using this functionality, a single physical infrastructure can be used to set up multiple virtual network infrastructures offering different authentication methods and policies for different user communities. Each VLAN acts as a separate virtual network that is segregated from the other VLANs through an amalgam of physical and network layer separation mechanisms, including distinct authentication profiles.

The use of VLANs is one of the most prevalent and industry-standard building blocks for secure multi-use modern wireless IP communication networks. As such, multiple VLAN support is required in all multi-use wireless IP networks.

Beyond security, multiple VLANs can also be used to ensure that high-priority users receive access precedence and reserved bandwidth.

IP address, protocol and TCP/UDP port filtering for access control (TropOS, MicrOS, ArcheOS and TeleOS product lines)
Packet filtering firewalls have long been used in conventional wired network security architectures. ABB Wireless has extended the concept to modern wireless IP communication networks with packet filtering capabilities that enhance wireless network security.

ABB Wireless products can filter traffic at the edge of the wireless network using filters based on IP source and destination addresses, protocol and TCP/UDP port. For instance, if wireless access is permitted only for a specific set of clients for web browsing and e-mail, only traffic matching that profile will be forwarded by ABB Wireless products. That is, only traffic from defined IP addresses or subnets destined to defined TCP ports (TCP port 80 for HTTP, port 110 for POP3, in our example) will be forwarded. This means that access can be controlled by application and by protocol, as well as by client. These policies are enforced at the edge of the wireless network.

Filtering is suitable for all types of wireless IP communication networks. However, care must be taken when configuring the filters to ensure that legitimate users and applications are not prevented from accessing the network.

Virtual Private Networks (VPNs) combined with filtering for access control (TropOS, MicrOS, ArcheOS and TeleOS product lines)

To provide the highest levels of security, ABB Wireless recommends the use of industry-tested virtual private networks (VPNs). While the main function of a VPN is to provide secure end-to-end data transmission (see below), VPNs also play a role in network access control. When a VPN is used, only clients with the appropriate VPN software or hardware/software and valid login credentials can access the network, especially when combined with intelligent traffic filtering that permits only VPN traffic to traverse the network.

Note that traffic filtering as a means of requiring VPN use cannot be employed in contractor and guest access networks where the network operator wants new users to be able to register via the wireless network.

.

2. Network resource protection

Because wireless networks provide access to shared network resources (e.g., servers, databases) and the network itself is a shared resource, wireless network deployments must protect network resources from malicious wireless users and others who would seek to do harm. ABB Wireless networks accomplish this through a combination of physical deterrents as well as address, protocol and port filtering, alone and in conjunction with VPNs.

Physical deterrents (TropOS product line)

TropOS mesh routers are equipped with indicators that provide evidence of tampering if any occurs. Further, a variety of software alarms sent to the SuprOS communication network management system can alert network operators if any physical tampering takes place. TropOS mesh routers also include protections such as an encrypted file-system to guard and protect sensitive stored data.

Address, protocol and TCP port filtering for network resource protection (TropOS, MicrOS, ArcheOS and TeleOS product lines)

In addition to playing a role in network access control, packet filtering on ABB Wireless products also plays a part in protecting shared assets.

Returning to our previous example, destination IP address filtering can be configured on ABB Wireless products, in addition to IP source address and TCP port filtering. In this manner, authorized clients can not only be limited to web browsing and e-mail but also limited to connecting to specific web and e-mail servers. Crafting filters that disallow traffic to unprotected/unauthorized wired or wireless hosts helps protect those assets. Again, the policies will be enforced at the edge of the wireless network.
These measures are suitable for all types of wireless IP communication networks but must be carefully implemented.

Detection and notification of DoS attacks and jamming (TropOS and MicrOS product lines)

With 15 years of experience implementing large-scale, outdoor wireless networks, ABB Wireless has gained the expertise to recognize the signatures of denial of service (DoS) attacks and jamming. Based on this experience, ABB Wireless engineers have implemented, in TropOS Mesh OS and the embedded MicrOS operating firmware, heuristics to detect DoS attacks and jamming. DoS attacks are detected by observing inbound data traffic patterns while jamming is detected by observing RF characteristics.

When the embedded operating firmware determines that the criteria for a DoS attack or jamming are met, it notifies the SuprOS communication network management system. In turn, SuprOS can be configured to alert the network administrators so they can investigate and take corrective action.

.

VPNs combined with filtering for network resource protection (TropOS, MicrOS, ArcheOS and TeleOS product lines)

VPNs and the filtering capabilities of ABB Wireless products can help protect shared assets. Configuring filters that block all traffic except VPN traffic will prevent unauthorized traffic from reaching shared assets.

Again, traffic filtering as a means of requiring VPN use cannot be employed in contractor and guest access networks where the network operator wants new users to be able to register via the wireless network.

Use of embedded web servers with SSL (TropOS, MicrOS, ArcheOS and TeleOS product lines)

Many network infrastructure devices, including all ABB Wireless products contain embedded Web servers for device configuration and monitoring. To ensure maximum security, these Web servers should be configured to always employ Secure Sockets Layer (SSL), aka, HTTPS.

3. End-point, including wireless client, protection

Wireless clients must be protected both for their own sake and to prevent a permitted client from being used for network access by an unauthorized client. This is especially important because wireless clients are not limited to human-operated devices such as laptops and PDAs – they also include automated end-points such as utility automated metering infrastructure concentrators, SCADA endpoints, PLCs, RTUs and surveillance cameras.

Multiple VLANs plus WPA2 for end-point protection (TropOS, MicrOS, ArcheOS and TeleOS product lines)

Segregating different groups of users onto different VLANs protects end-points because only members of a given group can send traffic directly to other members of that group. For 802.11 wireless networks, this protection can be strengthened by requiring that WPA2 authentication be used to access the group's VLAN.

While multiple VLANs can be used in all wireless IP communication networks, WPA2 cannot be used in contractor and guest access networks where the network operator wants new users to be able to register via the wireless network.

Evil twin detection (TropOS product line)

Evil twin is a term used to describe an access point or wireless router that is configured with the same SSID as a wireless IP broadband mesh network but that is not actually a part of that network.

The intent behind an evil twin is not always malicious – for example, an enterprise may set up an evil twin to prevent their employees from connecting their work computers to a nearby wireless mesh network. However, such an evil twin can have the unintended but undesirable effect of denying access to user of the wireless IP broadband mesh network.

In other instances, evil twins are just that – evil, used for nefarious purposes such as harvesting passwords and other confidential information.

No matter why an evil twin is present, it is essential for network security that the network operator knows of its existence so that appropriate action can be taken. Tropos Mesh OS supports configurable evil twin detection, enabling mitigation of evil twin threats. The presence of an evil twin is reported by the SuprOS communication network management system.

Evil twin detection is required in all wireless IP broadband mesh networks.

Address filtering to block peer-to-peer traffic flows (TropOS, MicrOS, ArcheOS and TeleOS product lines)
In the same manner that filtering can be used to protect shared network resources, it can also be used to protect network clients. In particular, IP destination address filtering on ABB Wireless products can be used to prohibit clients from sending traffic to other clients.
This type of filtering is suitable for all types of wireless IP communication networks. Note, however, that it may disable some peer-to-peer applications where both peers connect to the wireless network.

VPNs combined with filtering (TropOS, MicrOS, ArcheOS and TeleOS product lines)
As described previously, TropOS mesh routers can be configured to permit only VPN traffic to enter the network and to force that traffic to go only to specified VPN servers on the wired network. A by-product of this configuration is to protect wireless clients because no traffic can be sent directly to them from the wireless network.

Use of embedded web servers with SSL (TropOS, MicrOS, ArcheOS and TeleOS product lines)
While beyond the scope of security provided by ABB Wireless products, it is important to note that many wireless end-points that are not human-operated devices (e.g., utility AMI concentrators, SCADA endpoints, PLCs, RTUs and surveillance cameras) contain embedded Web servers. To ensure maximum security, these Web servers should be configured to always employ Secure Sockets Layer (SSL), aka, HTTPS.

4. Secure end-to-end transmission

Whenever possible, wireless network traffic must be shielded from eavesdroppers using a strong encryption algorithm.

WPA2 encryption for client-to-mesh router links (TropOS product line)
In addition to providing access control via standardized authentication mechanisms, WPA2 also defines encryption between the client and the access point or mesh router using AES or TKIP ciphers. These provide for dynamic per-user encryption keys that are derived per-session as part of a key negotiation process. Tropos mesh routers support both TKIP and AES ciphers.

WPA2 is necessary but not sufficient to ensure secure end-to-end transmission. In addition to encryption of traffic between clients and the network, encryption of traffic within the network is also required (see below.) WPA2 cannot be employed in contractor and guest access networks where the network operator wants new users to be able to register via the wireless network.

SSL (TropOS, MicrOS, ArcheOS and TeleOS product lines)
As noted above, WPA2 cannot be used in contractor and guest access networks where the network operator wants new users to be able to register via the wireless network. As a result, users must take care to ensure that SSL is used to secure their transmissions when they send sensitive information over the Web. Use of SSL is indicated by the appearance of https:// (as opposed to http://) at the beginning of the address line in the user's Web browser.

Use of SSL to secure transmission of sensitive information on the Web is recommended at all times.

AES encryption for wireless network links (TropOS, MicrOS, ArcheOS and TeleOS product lines)
AES-encrypted wireless network links contribute to secure data transmission. ABB Wireless uses AES to encrypt all data traffic through the network, across multiple hops, until the traffic reaches a wired network (see figure 1). AES is recommended by the United States National Institute of Standards and Technology (NIST) as the most robust private key encryption technique.

AES encrypted mesh links should be used in all types of wireless IP communication networks.

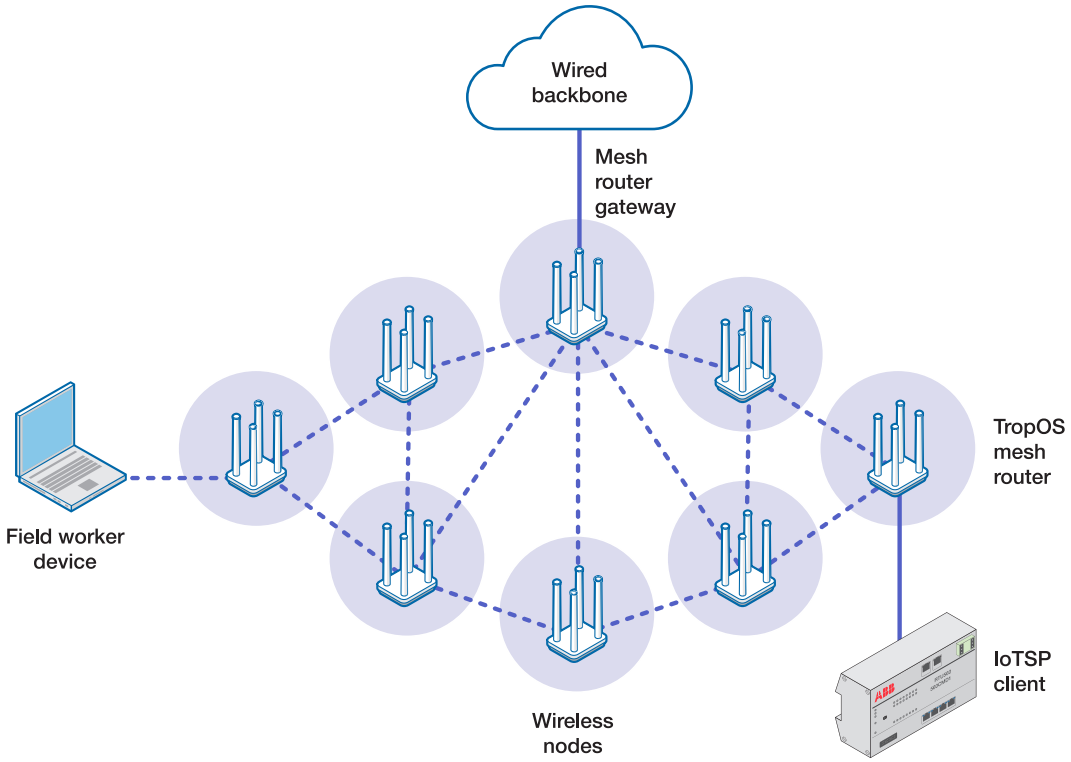

Figure 1: Basic TropOS Network Architecture

Multiple VLAN support for secure transmission (TropOS, MicrOS, ArcheOS and TeleOS product lines)

All ABB Wireless products support multiple VLANs with per-VLAN security configuration. Using this functionality, a single physical infrastructure can support different user communities with the traffic for each user community effectively segregated from that of all other user communities.

Multiple VLAN support is required in all multi-use wireless IP networks.

VPNs (TropOS, MicrOS, ArcheOS and TeleOS product lines)

To provide the highest levels of security, ABB Wireless recommends and uses industry-tested virtual private networks (VPNs). VPNs are very challenging or impossible to overcome even when attacked by serious and sophisticated adversaries. In fact, the use of a VPN alone may be the simplest way to meet many security requirements in a wireless network.

Building on the lower layer methods we've already discussed, ABB Wireless products combine unique VPN compatibility and traffic filtering with industry-leading VPNs.
As enterprises began allowing employees to connect to internal networks via the Internet, VPNs were developed in response to the security threats posed by malicious hackers attempting to gain access to internal network resources. Connections from the Internet to the internal network are encrypted by the VPN once the user requesting the connection authenticates successfully. Other incoming connections are disallowed. Driven by the increasing popularity of remote corporate access over Internet links, VPNs have rapidly matured.

Today, connecting wireless networks to an existing wireline network poses risks similar those encountered when first connecting to internal networks via the Internet. Because wireless signals propagate beyond the physical confines of the typical data network, wireless connections to the wired network also become a potential access method that can be exploited by malicious hackers.

Because of this threat, ABB Wireless strongly recommends using VPNs with wireless communication networks. VPNs (typically based on IPsec) are available from numerous vendors and offer proven implementations of network access control and secure data transmission. TropOS mesh routers support integrated IPsec VPNs to their wireless and wired interfaces and have demonstrated compatibility with a number of commercially available VPNs.

5. Secure configuration, operation and management

In addition to securing data transmission, it is also crucial to secure the configuration and management of the network infrastructure and safeguard its operation. Only authorized network operators must be able to alter the operation of network elements and the interaction of network infrastructure devices.

The techniques described below combine to enable secure configuration and management by preventing unauthorized access to, or monitoring of, the network's management and control traffic by malicious third-parties.

AES encryption for wireless mesh control and management traffic (TropOS product line)
In addition to the role AES encryption plays in securing data transmission, TropOS mesh networks from ABB Wireless also use AES to encrypt the Predictive Wireless Routing Protocol (PWRP™), the protocol used by TropOS mesh routers to transmit node identification and path selection information to each other, as well as management information sent wirelessly from nodes to their associated gateways. (See Figure 2.)

AES encrypted mesh links should be used in all types of wireless IP broadband mesh networks.

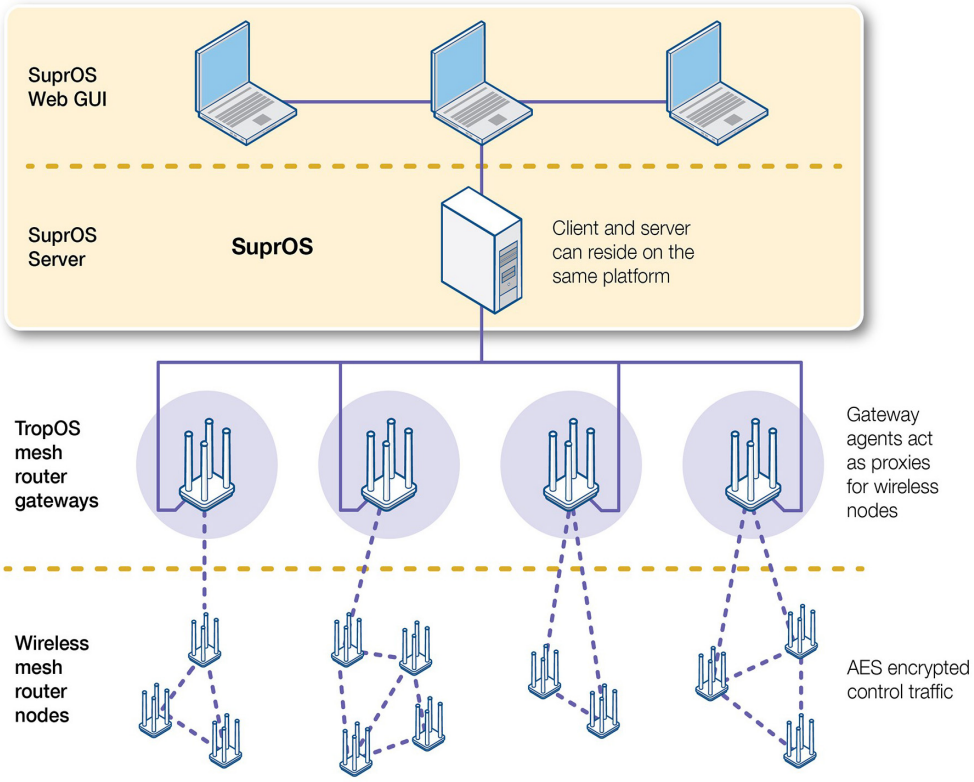

Figure 2: Secure configuration and management

No SuprOS access from wireless clients (TropOS, MicrOS, ArcheOS and TeleOS product lines)
SuprOS servers cannot be accessed via the wireless network. This prevents malicious wireless users from attempting to break into the SuprOS server.

Tiered access rights and auditing for SuprOS (TropOS, MicrOS, ArcheOS and TeleOS product lines)

To provide both the flexibility and security required for effective and efficient network management and administration, SuprOS offers tiered access rights based on user type or function. Four levels of access have been defined for SuprOS – Root, Admin, Read/Write and Read-Only. Authorization can be done locally on the management system or remotely using RADIUS.

Further, all configuration changes made to and/or using SuprOS are logged, including time, date and user information. This provides an audit trail detailing who made what configuration change and when they were made.

Secure network infrastructure device configuration (TropOS, MicrOS, ArcheOS and TeleOS product lines)

In addition to configuration via SuprOS, ABB Wireless products can be configured and monitored by a Web-based configurator. All configurator traffic is protected with HTTPS (see Figure 3). Network administrators can securely monitor and configure individual network infrastructure devices from anywhere on the Internet. Login is provided by a certificate-based authentication scheme that can support up to 20 authorized users.

As with SuprOS, all changes made using the configurator are logged, providing an audit trail.

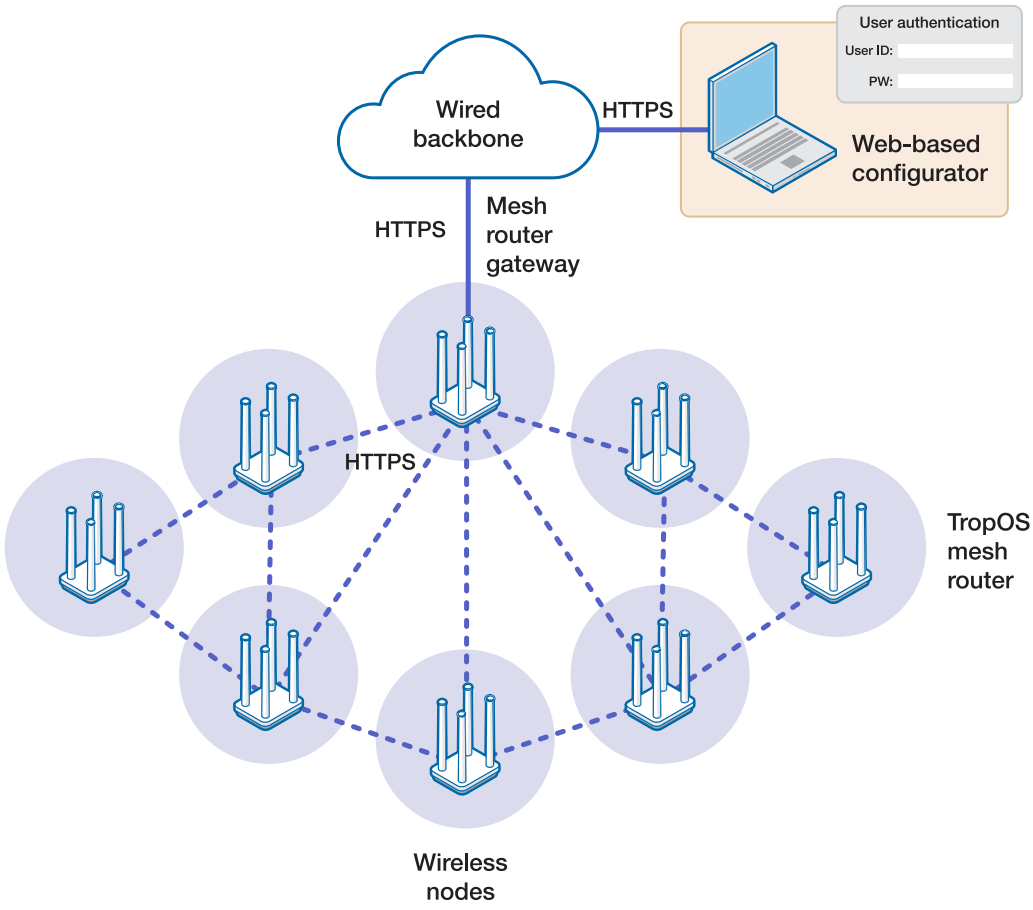

Figure 3: Secure web-based configuration

Field area and enterprise, wireless and wired

While there is some commonality between the basic security requirements for enterprise WLANs and field area wireless IP communication networks, there are also significant differences. Further, some techniques required for enterprise WLAN security are unnecessary or inappropriate for field area networks and vice versa.

For example, the ability to detect and disable rogue access points (APs) is crucial for ensuring enterprise security. However, in field area deployments, it is expected that the wireless network and its users will be within range of possibly hundreds of access points belonging to other, perfectly legitimate networks. Any attempt to disable these access points would run afoul of regulations in most countries of the world, not to mention common courtesy and sense.

Another consideration is the fundamental architecture of the wireless network.
Most enterprise WLANs use a thin AP/central controller architecture. This makes sense because the only wireless hop is the one between the client and the AP and the WLAN controller can reside on the LAN switch that is required to connect the Ethernet links from the various APs.

In field area wireless communication networks, data may need to traverse several wireless links before arriving at a wired network. The bandwidth on wireless links is a precious commodity, one that must not be squandered. It makes no sense to force traffic to traverse wireless links to an expensive, failure-prone, centralized controller only to be dropped because of security concerns. To the contrary, a central controller architecture opens field area wireless networks to denial of service (DOS) attacks by failing to stop malicious packets at the network's edge.

Rather than a central controller architecture, it is crucial that field area wireless IP communication networks detect threats and enforce security policies at the edge of the wireless network. Doing so saves valuable airtime, increasing the usable capacity of the entire network.

When securing field area wireless networks, it is crucial to insure that the wired networks to which they connect are also secure. Only someone in the physical vicinity of a wireless network is a potential intruder – a population that generally numbers in the hundreds or, at worst, in the thousands. Contrast this to wired networks that connect to the Internet. Anyone with a computer and an Internet connection is a potential intruder – a population that numbers in the hundreds of millions!

For some applications such as mobile workforce access, there may be a temptation to adopt a brute force approach to this problem and physically separate the wired network that serves as the back-end for the wireless network from the wired network that connects to the Internet. This approach denies Internet access via the wireless network. While appealing, this approach significantly limits the utility of the wireless network. The best approach is not to disable Internet access but to provide solid security for the wired network and its connection to the Internet.

Summary

By leveraging the inherent intelligence of ABB Wireless products, modern wireless IP communication networks from ABB Wireless combine the most rigorous Internet security techniques to offer a robust and multi-layered security framework. This security framework can be configured to suit a broad range of access strategies, from the relatively unrestricted contractor and guest access with minimal deterrents the totally secure private network needed for mission-critical industrial applications. Moreover, with the multi-use capabilities of communication networks from ABB Wireless, these different applications and security requirements can be supported on a single physical network infrastructure, enhancing the return on the investment in the network.
Using ABB Wireless' multi-layer, defense-in-depth approach, network administrators have at least three tools they can use to secure each of the five main areas of concern in wireless networks. See Figure 3.

A final advantage of the ABB Wireless security approach is upgradeability.

New security threats are emerging constantly. ABB Wireless continually incorporates new techniques for combating threats into its mesh routers. Because ABB Wireless are very intelligent, and most security features are implemented in software, their security features can be enhanced with new releases of embedded operating software.

	Network Access Control	Network Resource Protection	End-Point Protection	Secure Data Transmission	Secure Configuration, Operation and Management
Physical Deterrents		✓			
WPA 2	✓		✓	✓	
MAC ACLs	✓				
SSID Suppression	✓				
Multiple SSID Support	✓				
Multiple VLAN Support	✓		✓	✓	
Address, Protocol and Port Filtering	✓	✓	✓		
VPNs				✓	
VPNs Combined with Filtering	✓	✓	✓		
Jamming detection and notification		✓			
DOS attack detection and notification		✓			
Evil Twin Detection			✓		
AES Encrypted Mesh Links				✓	✓
No Tropos Control Access from Wireless					✓
Tiered Access Rights					✓
Secure Configuration					✓
Auditing					✓

Figure 3: ABB Wireless Meeting the Security Challenge

For more information please contact:

ABB Wireless
3055 Orchard Drive
San Jose, CA 95134
Phone: +1 408.331.6800
E-Mail: wireless.sales@nam.abb.com

abb.tropos.com/unwired

1KHA - 001 406 - SEN - 1002- 12.2016