White Paper

TropOS Mesh OS: Foundation of the ABB Wireless mesh network architecture

TropOS broadband wireless mesh networks from ABB provide a reliable, secure, scalable, high performance communications platform upon which customers operate one or many mission critical applications. Customers use their TropOS broadband mesh networks to communicate with mobile workers and thousands of automation devices in the field and in large industrial facilities. TropOS high performance networks have successfully been deployed by customers for over a decade in markets such as utilities, oil and gas production, mining, industrial facilities and smart cities.

TropOS networks are constructed using fixed and nomadic TropOS wireless broadband mesh routers and MicrOS client nodes. TropOS mesh routers combine the industry's most sophisticated mesh networking intelligence, designed from the ground up to optimize throughput in a dynamic, large-scale networks, with purpose-built hardware that is ruggedized and weatherized to withstand extreme environmental conditions. Each router includes one or more open-standards-based 802.11a/b/g/n radios optimized for outdoor use. Fixed and nomadic routers can be mixed on a single network to create a mesh with dynamic coverage areas. Each broadband mesh router provides wireless connectivity to standard 802.11a/b/g/n clients and extends the coverage area of the network without the need for communications cabling.

A TropOS network is organized into nodes, gateways and clients. TropOS broadband mesh routers can be configured as either nodes or gateways. Gateways are attached to a wired network connection which injects capacity into the wireless network. Nodes operate completely wirelessly, sending and receiving packets to clients as well as forwarding them to other mesh routers.

All 802.11 end-devices, whether those employed for machine-to-machine (M2M) application or by workers using laptops or tablets for human-machine interfaces (HMIs) as well as for intranet/Internet access, are defined as clients. Clients can access the network through any TropOS mesh router.

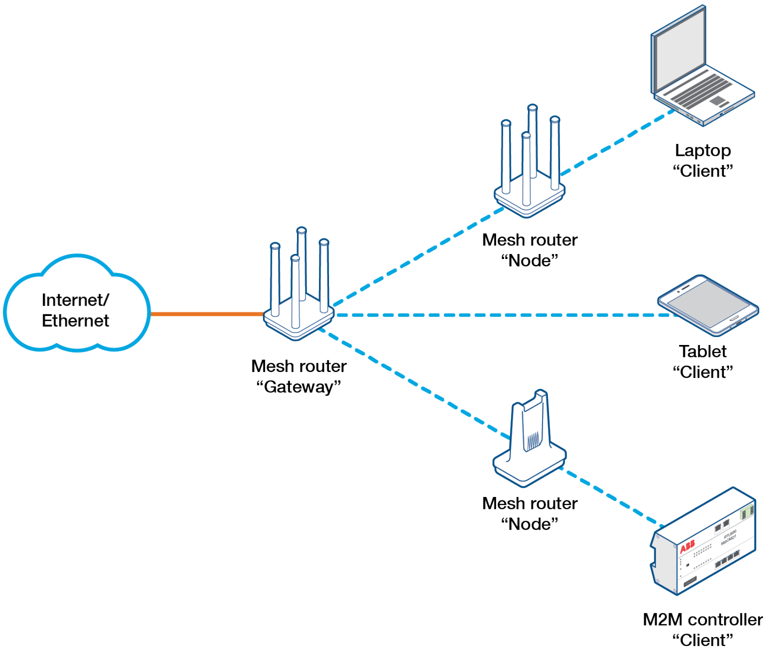

Figure 1 Tropos Mesh Network Elements

Each TropOS wireless mesh router includes all of the robust features of TropOS Mesh OS. TropOS Mesh OS is the foundation of the distributed, controller-free TropOS mesh network architecture. A common software platform that runs on each router across the network, TropOS Mesh OS leverages the router's on-board intelligence to monitor and maximize performance and reliability.

TropOS Mesh OS Explained

TropOS Mesh OS is not a separate product. Rather, it is a common software operating system that runs on each TropOS broadband mesh router in the network. TropOS Mesh OS leverages each router's on-board intelligence to minimize network congestion and adapt on a real-time, packet-by-packet basis. This distributed approach optimizes performance and throughput by minimizing control traffic, delivers a highly scalable solution, and provides high levels of network availability.

TropOS Mesh OS is the key to delivering high throughput, scalability and reliability. It is the industry's only mesh routing software that dynamically selects end-to-end paths through the mesh based on maximizing client-server throughput and minimizing latency.

TropOS Mesh OS can be best understood by examining the operation and interaction of its components, as is done in following sections of this white paper.

Predictive Wireless Routing Protocol (PWRP)

The patented Predictive Wireless Routing Protocol (PWRP) continually analyzes the quality of active and inactive mesh links to dynamically configure the ideal combination of paths to optimize network performance.

PWRP streamlines deployments and preserves performance by dynamically configuring and optimizing mesh connections. It improves overall throughput by selecting optimal routing paths while enhancing network resiliency by providing graceful rerouting of traffic in the event of RF interference, backhaul failures, or other disruptions in the wireless mesh. PWPR supports standard Wi-Fi client mobility without the need for special client hardware, software, or network reconfigurations, although mobility reliability and performance is enhanced when TropOS mobile mesh routers are employed. Because PWRP is a lightweight protocol, it enables the network to be scaled to thousands of nodes covering the largest geographical areas in the industry.

PWRP: Auto-Discovery

Using PWRP, TropOS mesh routers automatically discover one another and self-organize into a seamlessly interconnected wireless mesh network. Upon deployment, the routers automatically discover one another. Each mesh router determines the presence of both clients and other mesh routers. Once a mesh router has identified the existence of other like devices, it builds a table of neighboring devices and the corresponding paths through the network that each neighbor provides. The mesh router then identifies the optimal path to send data across the network, to a wired gateway. Optimal paths are chosen on the basis of throughput, packet success, signal-to-noise ratios, and other key criteria.

Figure 2 below shows how PWRP creates a mesh network.

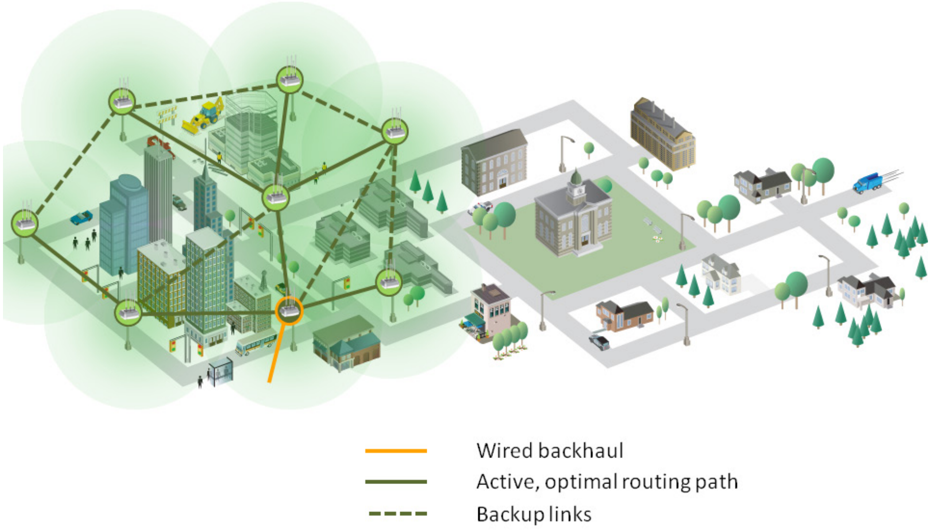

Figure 2 Mesh Routers Self-Organize into a Totally Wireless Network

As new mesh routers are added to the network, they participate in the auto-discovery process, and self-organize to become part of the network. Figure 3 shows how other routers immediately join the network.

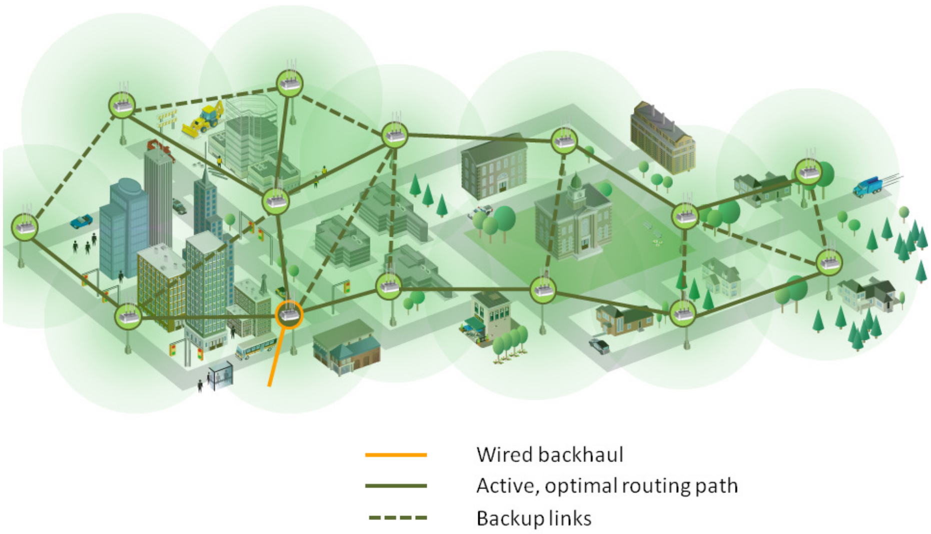

Figure 3 Additional Mesh Routers Immediately Join the Network

A TropOS network can operate with only one wired gateway, although multiple wired backhaul connections are typically deployed to ensure redundancy and to provide increased network bandwidth to meet performance and reliability requirements.

PWRP: Predictive Path Optimization

PWRP selects the optimal communication paths from each router to a wired gateway. These paths are based on various metrics designed to optimize the overall end-to-end quality of the wireless path, not just distance vectors.

The quality of a wireless link depends on several factors, including the distance between the transmitter and receiver, the radio transparency of any obstructions between them, interference from other radios and multi-path effects.

The optimal path is determined from a variety of link quality criteria available to each mesh router, as well as the cumulative effects of each subsequent link in the path.

By ensuring that only the highest quality links are selected, high performance is maintained across the entire path. The end result is a connection that experiences minimal packet loss, ensuring optimal performance in the wireless environment.

Unlike the TropOS system, traditional routing methods cannot discriminate among paths with varying latency and packet loss characteristics. Instead, typical solutions choose the path with the fewest hops between the source and the destination (i.e., the shortest path).

In wireless environments, the shortest path sometimes exhibits poorer performance than longer, alternate paths based on high quality links. As a result, traditional routing approaches frequently lead to sub-optimal path selections, resulting in poor end-to-end throughput. The TropOS system is intelligent enough to make those determinations and identify the path that will offer the best possible performance.

The TropOS approach to determining the optimal path via predictive path optimization is illustrated in Figure 4 below.

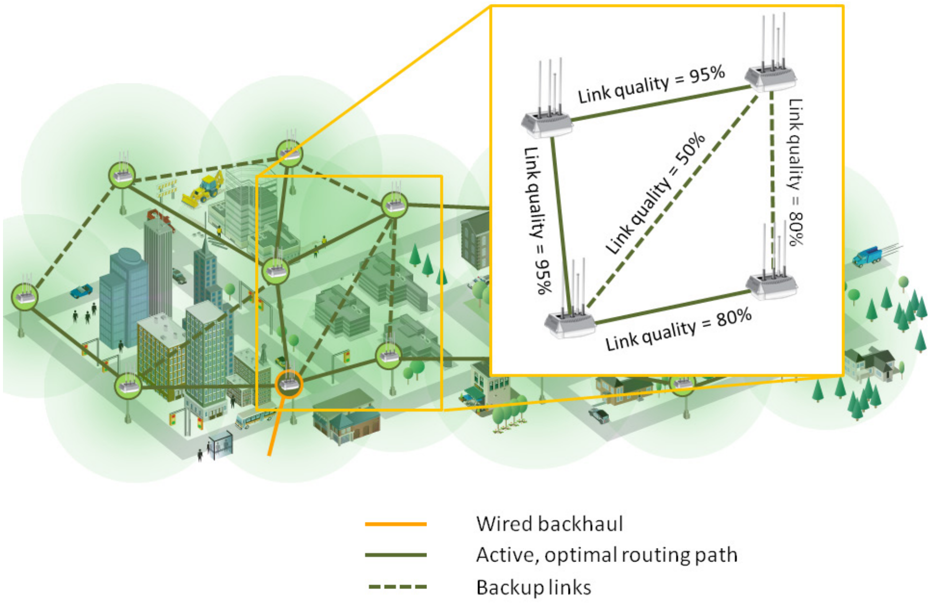

Figure 4 Optimal Path Selection

In this example, TropOS Mesh OS would select the green path, which is the path with highest overall path quality. Note that this is not the shortest path, but rather the path that has the highest end-to-end quality, as measured by packet loss, throughput and other measures.

Introducing the variable of path quality raises additional challenges. Because the wireless environment is inherently dynamic, the quality of any given link (and correspondingly, any path that utilizes that link) varies over time. The TropOS path selection algorithms intelligently refine path selection on an ongoing basis to adapt to these changes. As a result, PWRP with predictive path optimization ensures rapid response to significant environment changes and delivers high throughput over the entire network.

PWRP: Adaptive Clustering

ABB designed PWRP to be fully scalable from both a coverage and capacity perspective. Adding network capacity is as easy as connecting a backhaul link to any mesh router on the network. The newly wired mesh router then becomes a wired gateway on the network. The TropOS network seamlessly incorporates new gateways, automatically partitioning the network into clusters to intelligently distribute the additional capacity.

This adaptive clustering technique allows network owners to incrementally scale network capacity in direct response to changing usage needs and traffic patterns.

Importantly, network managers are not required to modify any existing network settings or topologies – network reconfiguration is seamless and automatic. The effect of automatic reconfiguration when adding backhaul capacity is shown below in Figure 5.

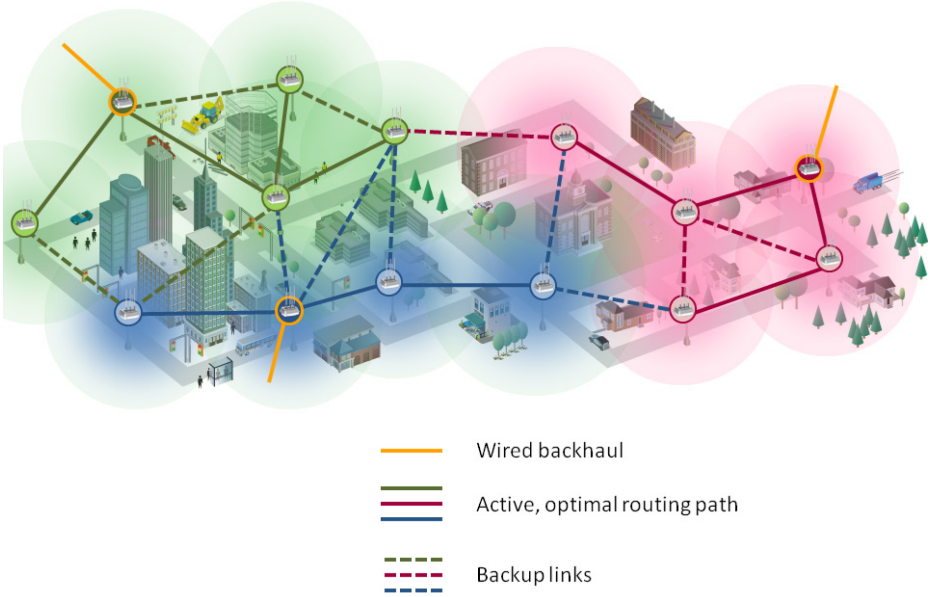

Figure 5 Automatic Reconfiguration with Added Backhaul Capacity

Two additional wired gateways have been added to the network. The other mesh routers automatically identify the wired gateways and reconfigure their wireless backhaul paths to take advantage of the additional connections. In the process, the mesh routers add alternate paths to their routing tables, enabling fail-over protection in the event of a wired outage.

PWRP: Self-Healing

PWRP provides several levels of fail-over protection. For example, if a link between active nodes becomes disrupted, the mesh routers identify the problem and automatically switch to an alternative path, effectively routing round the disruption. The following diagrams illustrate the effect.

In Figure 6 a link is lost due to interference. As shown in Figure 7, the optimal solution is to assign the affected node from the green cluster to the blue cluster. TropOS Mesh OS reclusters the network automatically.

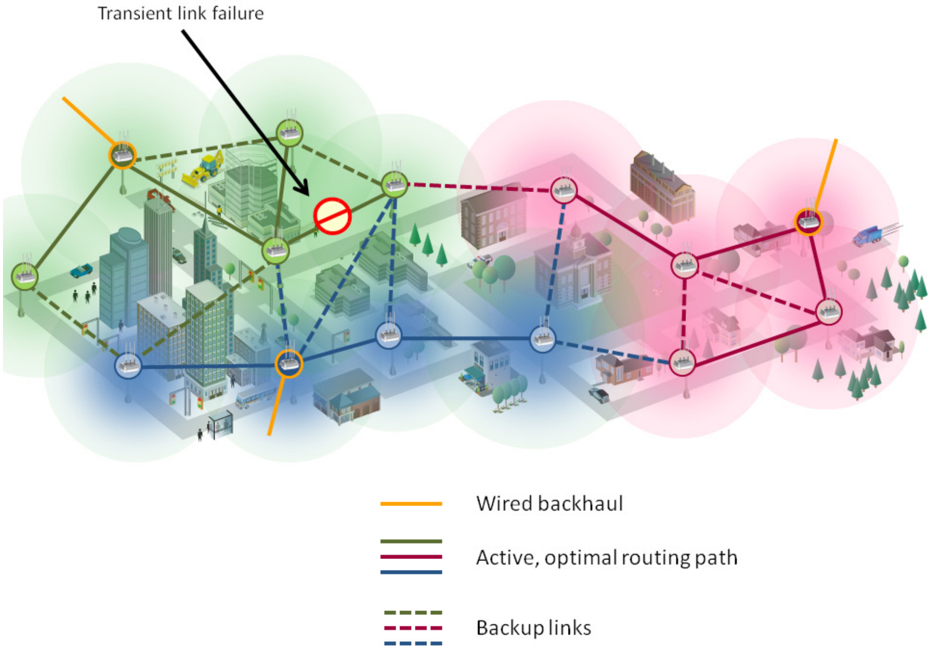

Figure 6 Interference Causes Transient Link Failure

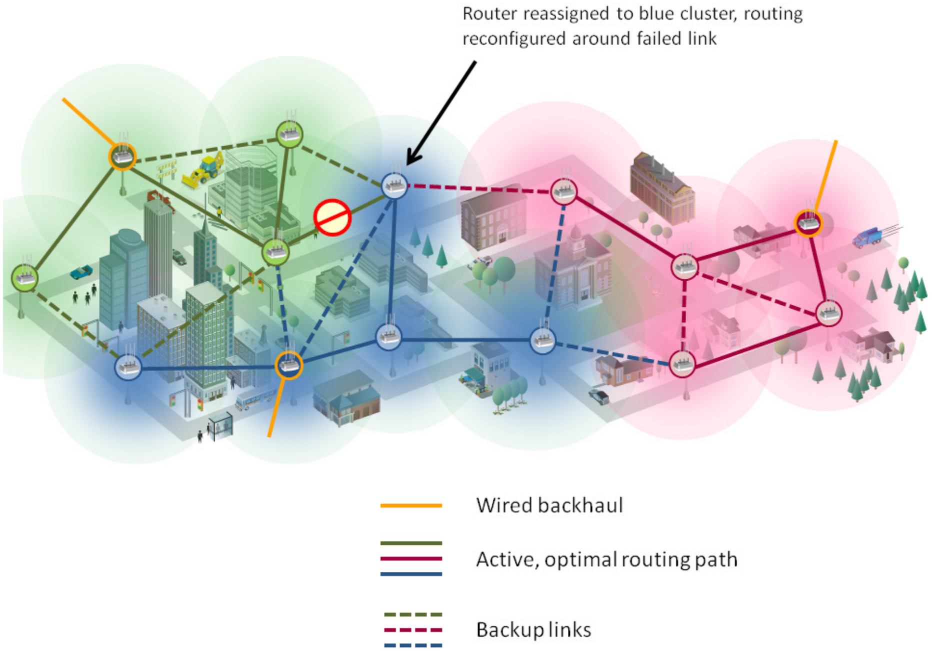
Router reassigned to blue cluster, routing reconfigured around failed link
Wired backhaul
Active, optimal routing path
Backup links

Figure 7 Network Reconfigures to Route Around Failure

The following diagrams illustrate what happens in the case of an outage on a backhaul connection. Figure 8 shows the backhaul failure condition while Figure 9 shows the automatic network reconfiguration in response to the outage.

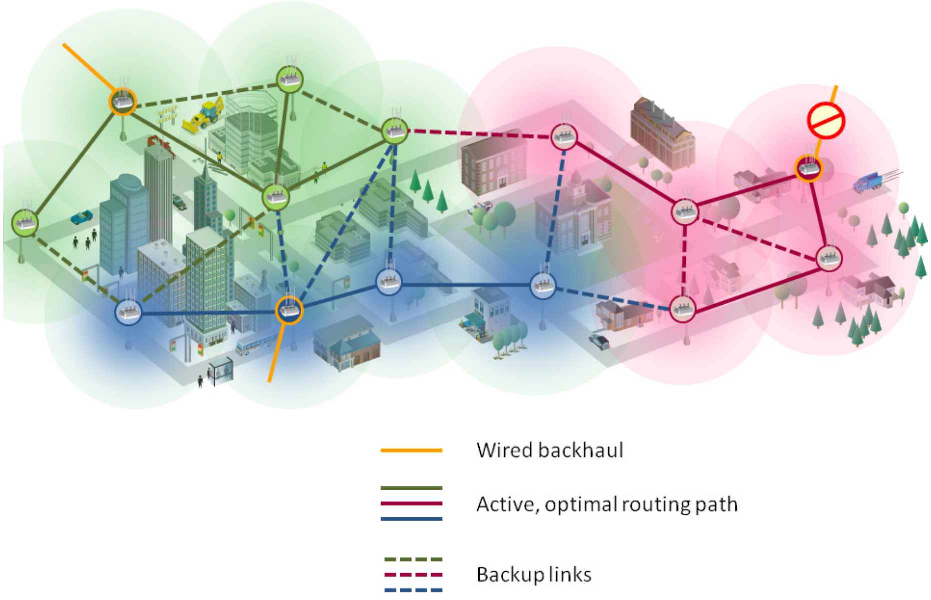

Figure 8 Backhaul Failure Threatens Entire Cluster

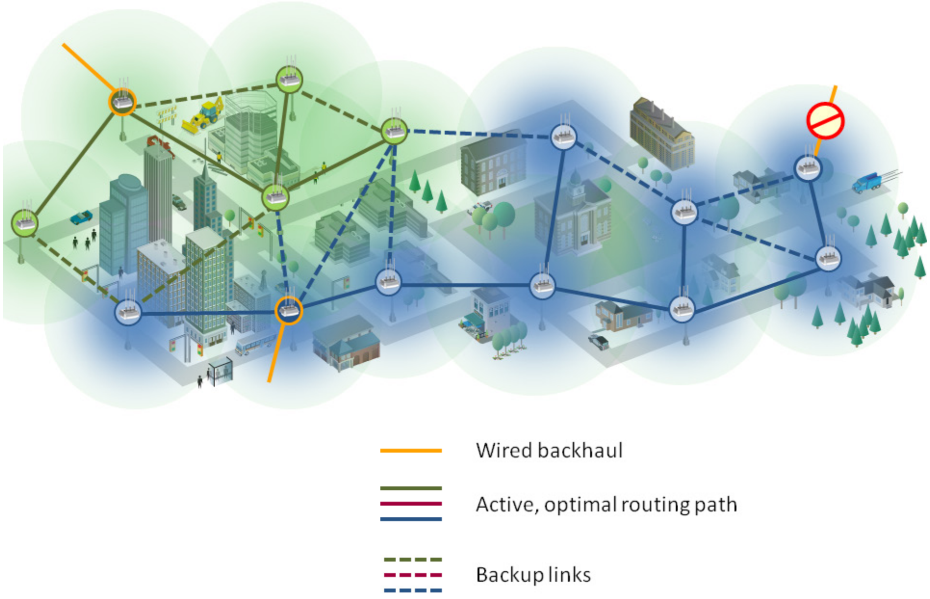

Figure 9 Automatic Reroute Around Failed Backhaul

In this case, the TropOS network adapts to the outage to ensure continued connectivity for all mesh routers. Individual mesh routers automatically detect the outage and the network reorganizes around the remaining backhaul points, as shown. Full service and connectivity is maintained. All TropOS network configurations are operationally redundant and self-healing. The redundancy operates in real time and is transparent to end-points.

PWRP: Multi-Radio/Multi-Mode Routing

TropOS Mesh OS dynamically chooses the optimal path to maximize network performance. In deployments using dual-radio TropOS mesh routers (e.g., the TropOS 6420 or TropOS 7320), TropOS Mesh OS in every router constantly scans the radio network and characterizes the performance of every link, whether active or unused, around it. TropOS Mesh OS can be configured to use 5 GHz links for inter-router connectivity when available and to fall back to 2.4 GHz inter-router links when the 5 GHz links perform sub-optimally. In this way, TropOS Mesh OS leverages the benefits of using additional spectrum to increase capacity while eliminating the pitfalls of the 5 GHz spectrum, which often only operates acceptably when line-of-sight is available between routers. An example is shown below in Figure 10.

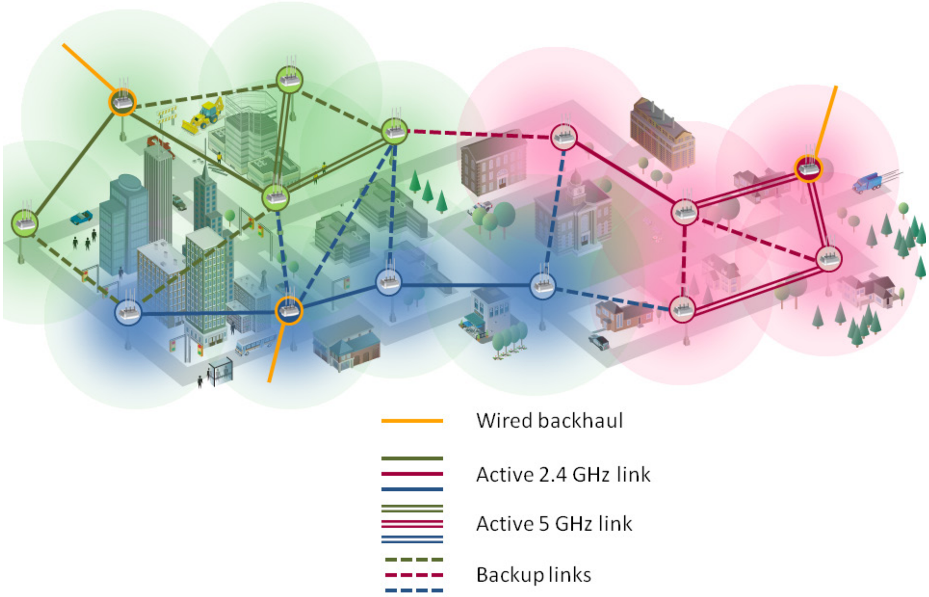

Figure 10 Multi-Radio, Multi-Mode Routing Makes Most Efficient Use of Spectrum

Scalability and capacity are less about the number of radios and more about spectral efficiency. TropOS Mesh OS makes the most efficient use of spectrum by constantly adapting to radio domain changes and by using the most optimal channel in the best available spectrum. Combining auto-channel and auto-band feature sets along with intelligent routing enhances network performance and capacity. Additionally, combining 2.4 GHz and 5 GHz in mesh paths provides incremental capacity while maintaining reliability and economical node density.

PowerCurve

A distributed algorithm that leverages PWRP, PowerCurve maximizes network performance and capacity by automatically optimizing power and rate parameters on a per-connection and per-packet basis. This advanced, distributed algorithm continually adjusts transmit power to maximize the number of wireless links that can operate concurrently. Unlike alternative approaches where transmit power is configured as a static setting, PowerCurve tightly couples power and bit rate control. This enables the router to make continuous and dynamic adjustments that can enhance throughput and provides better client connectivity and performance.

PowerCurve dynamically monitors and adjusts transmit power and rate on a per-packet, per-link basis, delivering maximum capacity possible given RF conditions. It enhances network reliability, capacity and scalability beyond the capabilities of static, controller-based architectures. Because of its dynamic nature, PowerCurve streamlines network planning, deployment and optimization.

Automatic Interference Avoidance

Designed to optimize performance in both single- and dual-radio networks, this distributed algorithm continually samples available channels to analyze link performance and interference trends. Channel decision logic is integrated into PWRP so that the quality of end-to-end paths on different RF channels across the network are assessed and the optimum path selected. In dual-radio routers, fine-grained channel allocations are implemented within individual clusters to dynamically optimize each cluster for client coverage and spatial reuse of spectrum. SmartChannel's network analysis is non-disruptive to user traffic and sessions. SmartChannel optimizes capacity and reliability by predicting and using the channels that are least likely to experience interference.

Adaptive Noise Immunity

Adaptive Noise Immunity (ANI) adjusts chip-level packet detection parameters in real time to minimize false detection events and maximize receiver sensitivity. Outdoor environments differ significantly from indoor environments in the variety and strength of interference sources, and dynamic detection parameter adjustment is critical to maintaining high performance. TropOS ANI algorithms have been developed through real-world testing and refined to perform in challenging interference environments where other devices stall, reset, or lose sensitivity.

Virtual Network Infrastructure

Different networked applications in the wireless world require virtual networks as robust as those found in the wired world. TropOS networks enable many different applications to use the same wireless broadband IP network and yet operate within their own private network, with its own address space, quality of service and security settings. The TropOS network architecture provides all the capabilities necessary to create a secure virtual network infrastructure. These capabilities include:

- Multiple ESSID support. TropOS broadband mesh networks support up to 16 ESSIDs and 40 VLAN tags. VLAN tags can be defined by IP address or ESSID.
- Different IP address spaces. Each application can have its own IP address space, DNS server, etc., allowing IP policies to be administered and enforced by the group responsible for that application.
- Different security settings. Each application can have its own security settings. See the section titled Multi-Layer Security for more details.
- Different quality of service settings. Each application can have its own quality of service settings. See the section titled Quality of Service for more details.
- All aspects of each virtual network can be centrally monitored and managed using TropOS Control. The network administrator can add or change any network setting to respond to increased security concerns, add new applications and more.

Quality of Service

TropOS networks support 802.11e, providing prioritization of data packets into four queues including a strict priority queue for voice applications. The system can classify and prioritize upstream traffic based on SSID and downstream traffic based on DSCP or 802.1p. It can reclassify traffic priorities received from clients; rewrite 802.1p bits; classify VoIP traffic using heuristics based on packet size/rates, ESSID, DSCP and destination subnet; reclassify packets which exceed packet rate and size expected for VoIP into lower priority queues; limit client airtime consumption and rate limit clients based on the amount of data transmitted. TropOS networks enforce QoS and rate-limiting policies at each wireless mesh router, ensuring that airtime is not wasted sending traffic through the mesh to a centralized controller only to have the controller drop the traffic. The network can also classify and prioritize traffic for downstream wired devices connected to a wired client interface on a TropOS mesh router.

TropOS mesh routers also support rate limiting to limit the bandwidth used by egregious clients and to provide service differentiation and fair access to the media. Rate limiting and service differentiation may be applied on a per SSID and per VLAN basis.

Multi-Layer Security

TropOS Mesh OS has been designed from the outset to deliver the same security options over the wireless network that is available over wired networks. The system provides a number of functions to monitor, report, and mitigate security threats to the network. The system includes a multi-layer, defense-in-depth security model with login reporting, evil twin monitoring, DoS identification, compliance reporting and mitigation. TropOS broadband mesh routers and MicrOS client nodes provide the technical controls required to achieve NERC CIP v5 compliance.

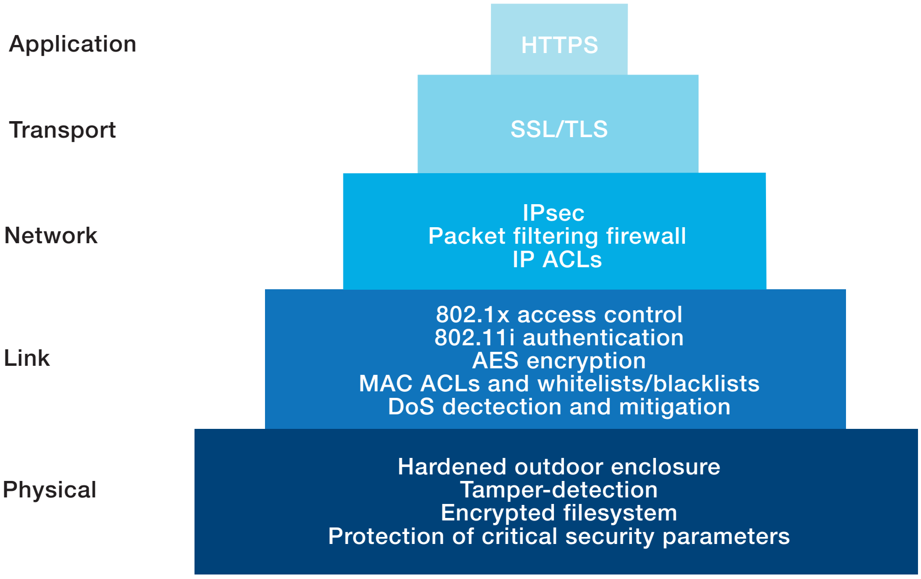
Application
HTTPS
Transport
SSL/TLS
Network
IPsec
Packet filtering firewall
IP ACLs
Link
802.1x access control
802.11i authentication
AES encryption
MAC ACLs and whitelists/blacklists
DoS dectection and mitigation
Physical
Hardened outdoor enclosure
Tamper-detection
Encrypted filesystem
Protection of critical security parameters

Figure 14 Tropos Multi-Layer Security Architecture

Authentication: TropOS Mesh OS supports Open, WPA-PSK, WPA-1x and WPA2 security mechanisms. TropOS supports WPA 802.1x authentication, using EAP-TLS/TTLS, SIM, PEAP, etc and has implemented a full RADIUS dictionary of standard and vendor specific AAA attributes.

- Networks that do not have a centralized authentication server can still take advantage of strong WPA authentication security by using the WPA pre-shared key (PSK) option. In the WPA-PSK approach, each network device that requires authentication is configured with the same password, or key. Clients access the network by presenting the password. As with RADIUS authentication, WPA-PSK uses EAP to send authentication messages.
- WPA2/WPA/802.1x and WPA-PSK are compatible with a variety of data encryption options. TropOS currently supports the Advanced Encryption Standard (AES) and Temporal Key Integrity Protocol (TKIP). The encryption method is determined by settings on the client station.
- TropOS wireless routers support the option of forgoing authentication and encryption entirely and thereby permitting any clients to access the network with no protection for data traffic. This option provides no protection for clients and should not be selected if network security is of concern.

Encryption: WPA/WPA2/802.1x and WPA-PSK are compatible with a variety of data encryption options. TropOS currently supports WEP, the Advanced Encryption Standard (AES) and Temporal Key Integrity Protocol (TKIP).

VPN support: TropOS supports VPN with IPsec/3DES.

TropOS has implemented a number of standard methodologies to identify, report, and mitigate security threats. DOS attacks are identified and reported by TropOS to the management system. The attacks are immediately mitigated using rate limiting and prevented by black listing the MAC of the attacker. Additionally TropOS networks identify other Layer 2 DoS attacks such as management frame flooding and MAC spoofing by constantly monitoring the network and reporting attacks to the management system.

“Rogue AP” is an enterprise term used to describe unauthorized access points (APs) that use a company Ethernet connection to provide wireless service to an area. Rogue APs are an issue in the enterprise since they may inadvertently pose a security risk to the corporate LAN. In large-scale environments, other APs are assumed to be present. TropOS security provisions as well as the proprietary handshake required to join the mesh, prevent unauthorized APs from joining a TropOS network. In this manner, the security of the infrastructure is protected.

“Evil twin” is a term used to denote an AP that picks up beacons from the legitimate network and transmits identical beacons trying to snare unwary clients. As long as wireless security is enabled, this type of attack cannot compromise the subscriber. TropOS detects the presence of evil twins by challenging non TropOS nodes with a request-response mechanism and, upon failure, reports them to the management system. No external equipment is needed.

TropOS provides Access Control Lists to create a list of clients, specified by MAC addresses to be explicitly permitted or denied to associate to the TropOS mesh. This provides an additional capability to control the network by denying access to blacklisted clients or limiting access to whitelisted clients.

The TropOS multi-layer security architecture prevents man in the middle and replay attacks through the use of AES encryption and 802.1x RADIUS Authentication to users and end-point devices like meters and data collectors. Because hackers can spoof the MAC address of a valid endpoint, MAC address based authentication, while an effective element in a layered security architecture, should not be the only authentication mechanism used. MAC address authentication should be supplemented with other networks such as virtual private networks (VPNs).

For more information regarding the TropOS multi-layer, defense-in-depth security architecture, see the ABB white paper Securing ABB Wireless IP Broadband Networks and the tech brief Bringing Enterprise-Class Security to IP-Based Field Area Communication Networks.

Summary

TropOS networks are based on a fully distributed mesh architecture. With no centralized controller, the architecture eliminates single-points-of-failure, performance bottlenecks and unnecessary network traffic.

With TropOS Mesh OS operating on each mesh router in the network, the TropOS mesh architecture's distributed intelligence dynamically selects the optimal end-to-end paths through the network by evaluating multiple RF links, channels and bands. TropOS Mesh OS also performs functions such as advanced RF resource management, VLAN enablement, and security and QoS policy enforcement. TropOS Mesh OS enables self-organizing networks, simplifying deployment of new networks and enabling ease in expanding existing ones. It is the key to delivering the superior capacity, resiliency, security and scalability that are the hallmarks of TropOS wireless mesh networks.

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