Xirrus ArrayOS

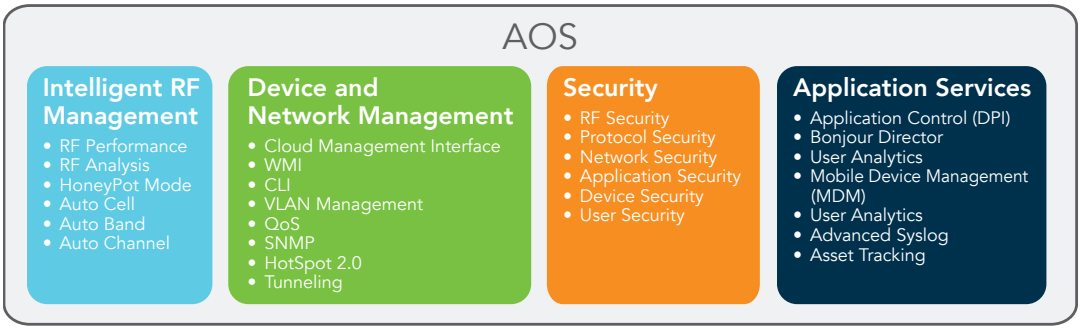
DATASHEET

Overview

Xirrus ArrayOS (AOS) is the software that powers Xirrus APs and Arrays. AOS is a unified software stack that runs on all Xirrus wireless platforms (XR family of products) and provides the functionality associated with the operation and management of the APs and Arrays. ArrayOS includes the operating system, Wi-Fi drivers, and software to interact with peripheral devices and management systems.

At a Glance

AOS provides functionality in four main categories – intelligent RF management, device and network management, security and application services.



- 802.11a/b/g/n/ac Wi-Fi support
- Automatic RF optimization
- Integrates directly with Active Directory
- ACExpress™ technology for superior client performance
- Multi-layered security
- Integrated user and location analytics
- Northbound API for Application and Service integration

Benefits

Simplified Deployment

AOS automates RF optimization with Auto Cell, Auto Band and Auto Channel features. AOS dynamically sets radio power levels to minimize interference and compensate for coverage gaps caused by system interruptions or AP/Array failures. Auto Channel mitigates channel interference while Auto Band move clients to the appropriate band based on their capabilities.

Application Visibility and Control

Gain comprehensive visibility into applications used on the wireless network. AOS can block/throttle/allow, apply QoS, and manage 1,300+ applications using Layer 7 Deep Packet Inspection (DPI) and other contextual application detection techniques. Schedule policies by application categories or individual applications for specific days and time.

Robust Security

AOS integrates comprehensive security with a multi-tiered approach. It supports standards based encryptions and authentication methods along with RF, protocol, network, device, user and application security features.

Enhanced performance with ACExpress

Xirrus' ACExpress™ mitigates the performance impact of combining slower and faster clients on the same radio. When multiple radios are available, AOS automatically load balances and segregates clients by band/mode/speed on different radios to maximize throughput.

Deliver New Services

Easily integrate with best-in-class 3rd party applications to enable business processes or new revenue streams with services such as location analytics, user analytics, multi-vendor management and monetization applications. AOS supports a RESTful JSON API for integration with other systems and services.

Future-Proof with lower TCO

AOS enables mixing of modular radios supporting different technologies. This functionality allows IT organizations to lower the TCO by using the modular Arrays with radios supporting newer standards without replacing the entire platform.

XIRRUS® High Performance Wireless Networks

Optrics Engineering

INTELLIGENT RF FEATURES	
RF Performance	• WDS (Wireless Distribution System) for point-to-point communication • Wireless Mode per IAP • Auto Cell Technology • Sharp Cell Technology • Wireless Data Rate Optimization • Wireless Traffic Shaping • Wireless Voice Call Admission Control • Fast Layer 2 and 3 Roaming • Standby Mode
RF Security	The RF security subsystem consists of the following sub-features: • Wireless IDS/ IPS (Intrusion Detection/ Prevention System) • Wireless Stateful Firewall • User Group Policies • Authenticated Guest Access Gateway • NAC Integration
RF Analysis	Xirrus RAM consists of the following sub-features: • RF Analysis: Spectrum analyzer leverages the threat sensor radio for RF Analysis (view of channel utilization, interference and errors) • Packet Analysis: A packet capture tool that provides filterable views of traffic passing through the wired and wireless interfaces of the AP/Array. • Failure Recovery: Self-test and self-healing mechanism ensures continuous system operation. • Network Tools: Ping, RADIUS ping, traceroute • Netflow support
Honeypot Mode	Honeypot Mode support in AOS helps increase available wireless device density through management of spurious association traffic.

DEVICE AND NETWORK MANAGEMENT FEATURES	
Cloud Management Interface	Xirrus Management System-Cloud enables full monitoring and management of the Xirrus wireless network remotely via a web based application with graphical map views.
Web Management Interface (WMI)	The WMI provides the following set of functionality through its user interface: • Array Status and Configuration • Network Status and Configuration • RF Monitoring • Station Information • Statistics Data • Application Control • System Logging • IDS Event Logging
Command Line Interface (CLI)	AOS allows a Secure Shell (SSH) connection to the Array, using a standard SSH utility, such as puTTY. The CLI provides a rich set of commands to configure, manage Xirrus wireless network.
SNMP	AOS includes support for SNMP v1, v2 and v3.
Tunneling	AOS includes support for both GRE (General Routing Encapsulation) and VTun (Virtual Tunnels over TCP/IP networks).

APPLICATION AND ACCESS MANAGEMENT FEATURES	
Hotspot 2.0	AOS is HotSpot 2.0 (Passpoint) Certified.
Mobile Device Management (MDM) with Airwatch	AOS enables Mobile Device Management (MDM) through interfaces with Airwatch, verifies enrollment and compliance status of devices as they connect to MDM enabled SSIDs. Note that only Android and iOS devices are supported by Airwatch at the moment.
Euclid Analytics Integration	AOS includes integration with Euclid Analytics – which allows for the use of Xirrus Arrays in place of Euclid hardware sensors to feed location data to the Euclid servers. In addition to the Euclid format, from AOS 6.6 onwards there is support for being able to export station location data in a "generic" format.
RESTful/JSON API support	AOS supports the Representation State Transfer (REST) architecture for distributed systems on the World Wide Web. The media type supported is JavaScript Object Notation (JSON).
Advanced Syslogging with Splunk	AOS generates syslog messages in Splunk format, which helps you use Splunk for diagnosing network issues.
Asset Tracking with Ekahau	AOS processes Ekahau Blink-Mode packets to enable you to deploy Ekahau's location tracking system for tracking assets, using your wireless network.
Application Control	Gain visibility and manage applications using Layer 7 Deep Packet Inspection (DPI) techniques including: • Surgical Pattern Matching • Deep Protocol Dissection • Semantic and Conversational Awareness • Behavioral Analysis • Flow Registration and Association Applications are classified into 15 different subcategories: Collaboration, Games, Remote Access, VPN, Database, Mail, Networking, Monitoring, Social, Web, File Transfer, Messaging, Proxy, Streaming and Xirrus.
Bonjour Director	Discover Apple devices such as iPads and printers enabled with Airprint on different local networks. Bonjour Director filters and forwards specific mDNS traffic between VLANS to allow Apple clients to access resources across the entire network.

Technical Specifications

FEATURE	SPECIFICATIONS	
RF Management	In-band per radio Spectrum Analysis Dynamic channel configuration Dynamic cell size configuration Wired and wireless packet captures (including 802.11 headers) Radio assurance for radio self test and healing RF monitor 2.4 & 5.0GHz Honeypot Control – Increase available 2.4 and 5GHz wireless device density through management of spurious 2.4 & 5.0GHz association traffic Ultra Low Power Mode – Maximize wireless channel re-use and increase wireless device density through tight power controls	
Wireless Protocols	IEEE 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11n, 802.11ac, limited 802.11k support (limited to only 2 of 34 parameters – Bit-1 "Neighbor Report" and Bit-16 "Channel Report")	
Wired Protocols	IEEE 802.3 10-BASE-T, IEEE 802.3u 100BASE-TX, 1000BASE-T, IEEE 802.3ab 1000BASE-T IEEE 802.1q – VLAN Tagging IEEE 802.1d – Spanning Tree IEEE 802.1p – Layer 2 Traffic Prioritization IPv6 Control – Increase wireless device density through control of unnecessary IPv6 traffic on IPv4-only networks	
RFC Support	RFC 768 UDP RFC 791 IP RFC 2460 IPV6 (Bridging only) RFC 792 ICMP RFC 793 TCP	RFC 826 ARP RFC 1122 Requirements for internet hosts – communication layers RFC 1542 BOOTP RFC 2131 DHCP

Technical Specifications Continued

Authentication	IEEE 802.1x RFC 2548 Microsoft vendor-specific RADIUS attributes RFC 2716 PPP EAP-TLS RFC 2865 RADIUS Authentication RFC 2866 RADIUS Accounting RFC 2867 Tunnel Accounting RFC 2869 RADIUS Extensions RFC 3576 Dynamic Authorizations extensions to RADIUS RFC 3579 RADIUS Support for EAP RFC 3748 EAP-PEAP RFC 5216 EAP-TLS	RFC 5281 EAP-TTLS RFC 2284 EAP-GTC RFC 4186 EAP-SIM RFC 4187 EAP-AKA RFC 3748 Leap Pass through RFC 3748 Extensible Authentication Protocol RFC5176 Dynamic Authorization extensions to RADIUS Web Page Authentication • WPR, Landing Page, Redirect • Support for Internal WPR, Landing Page and Authentication • Support for External WPR, Landing Page and Authentication • WPR Whitelist – ability to exclude certain sites from WPR
Carrier Applications	Passpoint Certification	
Management Protocols and Standards	SNMP v1 SNMPv2c as per RFCs 1901, 2580 SNMPv3 as per RFC 3410-3415 RFC 854 Telnet RFC 1155 Management Information for TCP/IP Based Internets RFC 1156 MIB RFC 1157 SNMP RFC 1212 Concise MIB Definitions RFC 1213 SNMP MIB II RFC 1215 A Convention for Defining Traps for use with the SNMP RFC 1350 TFTP RFC 1643 Ethernet MIB RFC 2030 Simple Network Time Protocol SNTP RFC 2578 Structure of Management Information Version 2 (SMIv2) RFC 2579 Textual Conventions for SMIv2 RFC 2616 HTTP 1.1 RFC 2665 Definitions of Managed Objects for the Ethernet Like Interface Types	RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions RFC 2819 Remote Network Monitoring Management Information Base RFC 2863 The Interface Group MIB RFC 3164 BSD Syslog Protocol and support for Station URL Syslog RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) RFC 3416 Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) RFC 3417 Transport Mappings for the Simple Network Management Protocol (SNMP) RFC 3418 Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) RFC 3636 Definitions of Managed Objects for IEEE Xirrus Private MIBs Integration with Splunk for accurate search and analysis of intra-organizational IT events Netflow Export v9 and IPFIX compatibility allows for IP traffic statistics collection

Ordering Information

PART NUMBER	DESCRIPTION
Software Licenses	
AOS-APPCON	ArrayOS Application Control license for 1 radio. Available on XR APs/Arrays only.
AOS-11AC	ArrayOS 802.11ac license enabling 802.11ac functionality on 1 radio. Available on XR 802.11ac AP/Arrays only.

Support & Maintenance

Xirrus is committed to the success of our customers and provides warranties and support options to best fit your needs. For further information on the Xirrus hardware warranties, software support and premium support offerings visit:

http://www.xirrus.com/support/

About Xirrus

To organizations who depend on wireless access to transform their business, Xirrus is the wireless network solution provider that provides the world's most powerful, scalable, and trusted solutions. Through product invention and system design, commitment to customer success, and the industry's best price performance, Xirrus gives you confidence that your wireless network performs under even the most demanding circumstances. Xirrus is a privately held company headquartered in Thousand Oaks, CA.

XIRRUS®
High Performance Wireless Networks

Optrics Engineering

Optrics Inc. a Xirrus Partner
6810 - 104 Street, Edmonton, AB T6H 2L6 Canada
Direct Dial: 780.430.6240
Toll Free (CDA): 1.877.463.7638
Toll Free (USA): 1.877.386.3763
Fax: 780.432.5630

To learn more visit:
Optrics.com/Xirrus or
email info@Optrics.com