Product Details

Description

Cisco 2504 Wireless Controller, belongs to Cisco 2500 Series Wireless Controllers. The Cisco 2500 Series Wireless Controllers are designed for small to midsize network. It scales to 75 access points and 1000 client devices. It also offers highly secure wireless guest access. With integrated Cisco CleanAir technology, this controller runs a self healing, self optimizing network. It is an ideal choice for small networks and branch offie, the 2500 series wireless controller will grow with your business.

The Cisco 2504 Wireless Controller supports Cisco Application Visibility and Control (AVC), the technology that includes Cisco's Network-Based Application Recognition 2 (NBAR-2) engine. N-BAR-2 does deep packet inspection (DPI) to classify applications and tie into quality of service (QoS) to either drop or mark the traffic, thereby prioritizing business-critical applications in the network. Cisco AVC uses NetFlow Version 9 to export the flows to Cisco Prime™ Infrastructure or a third-party NetFlow Collector. The Cisco 2504 Wireless Controller also supports Bonjour Services Directory, which enables Bonjour (Apple) Services to be advertised and utilized in a separate Layer 3 network. Wireless Policy engine is a wireless profiler and policy feature on the Cisco 2500 Series Wireless Controller that enables profiling of wireless devices and enforcement of policies such as VLAN assignment, QoS, ACL, and time-of-day-based access.

Features

Features	Benefits

Scalability	• Support up to 75 Access Points • Support up to 1000 Client
Ease of Deployment	For quick and easy deployment Access Points can be connected directly to 2504 Wireless LAN Controller via two PoE (Power over Ethernet) port
High Performance	Wired-network speed and nonblocking performance for 802.11n and 802.11ac networks. Supports up to 1 Gbps throughput
RF Management	Provides both real-time and historical information about RF interference impacting network performance across controllers, via systemwide Cisco CleanAir Technology integration
Comprehensive End to End Security	Offers CAPWAP-compliant Datagram Transport Layer Security (DTLS) encryption to help ensure full-line-rate encryption between access points and controllers across remote WAN/LAN links
End to end Voice	• Supports Unified Communications for improved collaboration through messaging, presence, and conferencing • Supports all Cisco Unified Wireless IP Phones for cost-effective, real-time voice services
High Performance Video	Integrates Cisco VideoStream technology as part of the Cisco medianet framework to optimize the delivery of video applications across the WLAN
PCI Integration	Part of Payment Card Industry (PCI) certified architecture, and are well-suited for retail customers who deploy transactional data applications such as scanners and kiosks

Office Extend	• Supports corporate wireless service for mobile and remote workers with secure wired tunnels to the Cisco Aironet® 600, 1130, 1140 or 3500 Series Access Points • Extends the corporate network to remote locations with minimal setup and maintenance requirements • Improves productivity and collaboration at remote site locations • Separate service set identifier (SSID) tunnels allow both corporate and personal Internet access • Reduced carbon dioxide emissions from a decrease in commuting • Higher employee job satisfaction from ability to work at home • Improves business resiliency by providing continuous, secure connectivity in the event of disasters, pandemics, or inclement weather
Enterprise	• Allows access points to dynamically establish wireless connections without the need for a physical connection to the wired network • Available on select Cisco Aironet access points, Enterprise Wireless Mesh is ideal for warehouses, manufacturing floors, shopping centers, and any other location where extending a wired connection may prove difficult or aesthetically unappealing
Enviromentally Responsible	Organizations may choose to turn off access point radios to reduce power consumption during off-peak hours

Mobility Security and Management for IPv6 & Dual-Stack Clients	• Secure, reliable wireless connectivity and consistent end-user experience • Increased network availability by proactive blocking of known threats • Equips administrators for IPv6 troubleshooting, planning, client traceability from a common wired and wireless management system
Guest Anchor and Wired Guest Access	• Supports up to 15 guest anchor Ethernet over IP (EoIP) tunnels forpath isolation of guest traffic from enterprise data traffic • Extends the guest access services to the wired clients on par with other WLAN Controllers

Specification

Maximum Throughput	1Gbps
Link Aggregation Group (LAG)	Yes
Form Factor	Desktop
Flexconnect + mesh	Yes
Max WLANs	16
Maximum access point	75
Interfaces or network I/O	Four 1GE

Access Control Lists	Yes
Radio Resource Management (RRM)	Yes
Bonjour Gateway	Yes
Max Power Consumption	80W
Mesh	Yes
Cisco VideoStream	Yes
Office Extend	Yes
Rendundant Power	No
Guest Services (Wireless)	Yes
Minimum Access Points	5
Maximum RF Tag Support	500
QoS	Yes
Application Visibility and Control	Yes
HA with Client SSO	No - only N+ 1HA
Guest Services (Wired)	Yes
Max Access Points per Group	25
Datagram Transport Layter Security (DTLS)	Yes

Cisco Compatible Extensions Call Admission Control (CAC)/WI-FI Multimedia (WMM)	Yes
HA with AP SSO	No- only N+1HA
Bi Directional Rate Limiting	Yes
Max VLANs	16
Redundant fans	Built in Fan
Integrated Wireless Policy Engine	Yes
Maximum Client Support	1000
Central Mode (Formerly Local Mode)	Yes
Max Number of access point groups	30
Mobility	L2 & L3
FlexConnect	Yes

Technical Specification

Item	Specification

Wireless Standards	IEEE 802.11a, 802.11ac, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11k, 802.11n, 802.11r, 802.11u, 802.11w, 802.11ac
Wired/ Switching/ Routing	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX specification, 1000BASE-T, and IEEE 802.1Q VLAN tagging
Data Request for Comments(RFCs)	• RFC 768 UDP • RFC 791 IP • RFC 2460 IPv6 (passthrough bridging mode only) • RFC 792 ICMP • RFC 793 TCP • RFC 826 ARP • RFC 1122 Requirements for Internet Hosts • RFC 1519 CIDR • RFC 1542 BOOTP • RFC 2131 DHCP • RFC 5415 CAPWAP Protocol Specification
	• Wi-Fi Protected Access (WPA) • IEEE 802.11i (WPA2, RSN) • RFC 1321 MD5 Message-Digest Algorithm • RFC 1851 The ESP Triple DES Transform • RFC 2104 HMAC: Keyed Hashing for Message Authentication • RFC 2246 TLS Protocol Version 1.0

Security Standards	• RFC 2401 Security Architecture for the Internet Protocol • RFC 2403 HMAC-MD5-96 within ESP and AH • RFC 2404 HMAC-SHA-1-96 within ESP and AH • RFC 2405 ESP DES-CBC Cipher Algorithm with Explicit IV • RFC 2406 IP Encapsulating Security Payload (ESP) • RFC 2407 Interpretation for ISAKMP • RFC 2408 ISAKMP • RFC 2409 IKE • RFC 2451 ESP CBC-Mode Cipher Algorithms • RFC 3280 Internet X.509 PKI Certificate and CRL Profile • RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPsec • RFC 3686 Using AES Counter Mode with IPsec ESP • RFC 4347 Datagram Transport Layer Security • RFC 4346 TLS Protocol Version 1.1

Encryption	• WEP and Temporal Key Integrity Protocol-Message Integrity Check (TKIP-MIC): RC4 40, 104 and 128 bits (both static and shared keys) • Advanced Encryption Standard (AES): CBC, CCM, Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) • DES: DES-CBC, 3DES • Secure Sockets Layer (SSL) and Transport Layer Security (TLS): RC4 128-bit and RSA 1024- and 2048-bit • DTLS: AES-CBC
Authentication, Authorization, and Accounting (AAA)	• 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 RADIUS Tunnel Accounting • RFC 3576 Dynamic Authorization Extensions to RADIUS • RFC 3579 RADIUS Support for EAP • RFC 3580 IEEE 802.1X RADIUS Guidelines • RFC 3748 Extensible Authentication Protocol • Web-based authentication • TACACS support for management users
	SNMP v1, v2c, v3

Management	RFC 854 Telnet RFC 1155 Management Information for TCP/IP-Based Internets RFC 1156 MIB RFC 1157 SNMP RFC 1213 SNMP MIB II RFC 1350 TFTP RFC 1643 Ethernet MIB RFC 2030 SNTP RFC 2616 HTTP RFC 2665 Ethernet-Like Interface types MIB RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual Extensions RFC 2819 RMON MIB RFC 2863 Interfaces Group MIB RFC 3164 Syslog RFC 3414 User-Based Security Model (USM) for SNMPv3 RFC 3418 MIB for SNMP RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs

	Cisco private MIBs
Management Interfaces	• Designed for use with Cisco Wireless Control System • Web-based: HTTP/HTTPS individual device manager • Command-line interface: Telnet, SSH, serial port
Interfaces and indicators	• Console port: RJ-45 connector • Network: Four 1 Gbps Ethernet (RJ-45) • LED indicators: Link Activity (each 1 Gigabit Ethernet port), Power, Status, Alarm
Physical and Environmental	Temperature: • Operating: 32 to 104 °F (0 to 40°C) • Storage: -13 to 158°F (-25 to 70°C Humidity: • Operating humidity: 10 to 95 percent, noncondensing • Storage humidity: Up to 95 percent Power adapter: Input power: 100 to 240 VAC; 50/60 Hz Heat dissipation: 72 BTU/hour
Regulatory Compliance	Safety: ● UL 60950-1, 2nd Edition ● EN 60950:2005 EMI and susceptibility (Class B): ● U.S.: FCC Part 15.107 and 15.109 ● Canada: ICES-003 ● Japan: VCCI ● Europe: EN 55022, EN 55024