

# Wireless Controllers

High-performance, Enterprise-class WLAN Controllers



Scalable to over 1000 Access Points per wireless controller with unified management of 802.11n and 802.11a/b/g Access Points

Seamless roaming with centralized and distributed forwarding

Integrated wireless IPS to proactively protect against security threats

High-availability architecture for real-time voice/video/data applications

Centralized visibility and control to unify wired and wireless role-based access

## Product Overview

The award-winning Enterasys Wireless Controller family provides a scalable range of solutions that are ideal for managed WLAN deployments supporting demanding voice/video/data applications. Our Wireless Controllers are simple to deploy and manage, yet provide advanced functionality to allow organizations to define how wireless voice/video/data traffic is processed without architectural constraints and in accordance with the business needs.

The Enterasys Wireless Controller portfolio includes:

- The **C20/C20N** supporting up to 64 Access Points (APs)
- The **C2400** supporting up to 400 APs
- The **C4110** supporting up to 500 APs
- The **C5110** supporting up to 1050 APs

The C20, C2400, C4110 and C5110 are housed in rugged, modular enclosures while the C20N is a plug-in module for the Enterasys N-Series LAN switch.

Enterasys Wireless Controllers provide role-based management for users, devices, and applications with individualized services including Quality of Service (QoS), call admission control, secure access policies, network access control (NAC), captive portals, rate limiting, multicast, filtering, and traffic forwarding. These services are enabled by the unique and flexible Enterasys Wireless Virtual Network Service (VNS) architecture and easily provisioned and managed by an intuitive web interface.

Each controller supports mixed mode deployments of 802.11n and 802.11a/b/g APs along with the ability to seamlessly roam between wireless controllers and access points, providing scalability and ease of deployment. For large deployments, Enterasys Wireless further simplifies the management of thousands of APs by creating mobility zones that extend the VNS properties across multiple wireless controllers. Mobility zones maintain the VNS definitions and the individual policies throughout the entire mobility zone, ensuring that policies follow the user regardless of physical location.

Enterasys Wireless provides an easy, low cost way to deploy 802.11n solutions, delivering cost-effective pricing, wired/wireless integration, and low TCO while openly supporting a broad range of mobile voice, video, and location-based applications to drive enterprise productivity and reduce the overall cost of mobility. With the ability to deliver both centralized and distributed traffic forwarding by application, Enterasys Wireless Controllers enable a flexible, cost-effective path to deploying 802.11n for the enterprise. Backed by industry-leading global support and services, Enterasys Wireless solutions enable customers to leverage existing investments and avoid forklift upgrades.

## Benefits

### Business Alignment

- Support for demanding voice/video/data applications to enhance mobile worker productivity and convenience
- Role-based grouping of users, devices, and applications to deliver priority, QoS, and security in accordance with business needs
- Integrated management, security, and QoS features reduce operating cost and ensure a consistent user experience regardless of location
- Key element of mobility solutions that enable VoWLAN and dual-mode devices

### Operational Efficiency

- Centralized visibility and control to simplify management, accelerate problem resolution, optimize network utilization, and automate response to wireless threats
- Integrated wired and wireless management, and role-based access control greatly reduce administration time and effort
- Adaptive architecture reduces complexity and optimizes information flow for each application

### Security

- Authentication and authorization functions include role-based access control using 802.1X, MAC authentication, and captive portal
- Standards-based encryption (WEP, TKIP, WPA, WPA2, WPA-PSK, WPA2-PSK, and AES)
- External captive portal allows full customization for guest access
- Integrated wired and wireless intrusion prevention
- Denial of Service (DoS) protection for management, control, and data traffic

### Support and Service

- Industry-leading customer satisfaction and first call resolution rates
- Personalized services, including site surveys, network design, installation, and training

**There is nothing more important than our customers.**

---

## Virtual Network Service (VNS) - An Adaptive WLAN Architecture

Most WLAN solutions force network administrators to choose between a centralized or distributed architecture. A significant advantage of Enterasys Wireless Controllers is that they can support both deployment models simultaneously, offering significant flexibility benefits over other solutions. Network administrators can select how traffic will be handled on a per-SSID basis, without any restrictions, so that the wireless LAN infrastructure can adapt to business requirements and applications.

A centralized architecture requires all traffic to be backhauled to a centralized controller. With the higher data rates of 802.11n APs, traffic loads on the wired network can be much greater than those created by legacy 802.11a/b/g APs. Depending on the size of the WLAN deployment and how much data is forwarded to the centralized controller, significant congestion may result.

A fully distributed deployment eliminates backhauling traffic to a wireless controller but increases the processing complexity for real-time mobile applications that require seamless cross-subnet roaming (e.g. VoWLAN). This can force IT managers to either create a large broadcast domain or apply many VLANs.

Enterasys Wireless Virtual Network Services control traffic flow by allowing traffic to be backhauled to a wireless controller or switched locally at the AP on a per SSID basis. With local switching, the AP is still managed centrally by the wireless controller, but data is not backhauled to the wireless controller. This improves responsiveness and ensures that traffic does not unnecessarily traverse costly WANs or contribute to bottlenecks at aggregating switches. A VNS also provides role-based policies providing security, NAC, mobility, and QoS priority that can be implemented on a per user and per application basis.

## Integrated Management and Control across Wireless and Wired Networks

### Web-based Centralized Management via Wireless Assistant

The Wireless Assistant provides network administrators with a centralized web-based interface designed to easily manage both infrastructure and services. Hosted on the wireless controller, this interface allows network administrators to separately configure, enable, or disable each AP or group of APs. The wireless controller consolidates data received from across the network to provide meaningful statistics in easy-to-read reports. Additionally, a number of standards-based management tools are available to facilitate integration of the WLAN infrastructure with enterprise management applications. For large networks with multiple wireless controllers the optional Enterasys Wireless Management Suite (WMS) can be used to collect and manage data for a centralized view of the entire WLAN.

### Multi-Controller Management

Enterasys Wireless Management Suite provides centralized management for the Enterasys Wireless portfolio, consolidating management information from across the entire WLAN for a global network perspective. The solution is enhanced by the addition of the WMS Intrusion Prevention System (WIPS) option which provides sophisticated wireless intrusion prevention and location assessment capabilities. Wired and wireless network integration is further enhanced by the visibility of all the wireless elements through the Enterasys Network Management Suite (NMS). Integration between NMS and the Enterasys Wireless portfolio provides end-to-end visibility of wireless Access Points, Controllers, and wireless clients from the NMS Console. The integration delivers improved network management efficiency and wired/wireless infrastructure topology mapping and visibility for network administrators. Further integration with NMS Inventory Manager effectively centralizes distribution of software and tracking of configuration changes.

### Integrated Security

Wireless Management Suite WIPS enhances security with embedded wireless intrusion prevention and location-based services. When deployed in conjunction with the Enterasys Intrusion Prevention System (IPS), full packet inspection, adaptive signature pattern matching, protocol analysis, and behavioral anomaly detection are delivered for both wired and wireless users. Further, Enterasys Network Access Control (NAC) identity-based policy privileges are unified across the wired and wireless infrastructure to deliver role-based access control – regardless of connectivity method. The NAC policies ensure only the right users have access to the right information, from the right place, at the right time. Third party authentication systems can also be integrated with the use of the External Captive Portal interface.

## High Performance & High Availability

Enterasys Wireless delivers the perfect combination of high-performance and high-availability demanded by today's wireless applications. By combining unique voice optimization features and the latest in industry standards, Enterasys Wireless provides enterprise grade reliability for all users.

### High Scalability

The Enterasys Wireless portfolio supports from a single AP to 1,000+ APs per wireless controller, providing linear scalability from small to large wireless deployments. In addition, wireless controllers can be networked to scale beyond the limits of a single controller or availability pair to offer a multi-wireless controller mobility zone. Mobility zones enable seamless roaming across a large number of wireless controllers while still delivering real-time session-availability services without requiring the purchase of additional AP licenses for redundancy.

Enterasys Wireless provides true end-to-end Quality of Service (QoS) with each controller and AP supporting native IP prioritization (DiffServ, TOS, Precedence), Ethernet 802.1p, as well as 802.11e's WMM and TSPEC wireless QoS standards. Enterasys Wireless devices support distinct queues on all interfaces, whether wired or wireless.

When voice and data traffic are running on the same AP, voice traffic can be prioritized to ensure minimal delay and jitter for optimal voice quality. The wireless controllers are able to translate WMM prioritized traffic to existing QoS prioritization schemes on the wired network (TOS, DSCP, etc.).

### Fast and Secure Roaming for Seamless Voice and Data Mobility

Enterasys Wireless Controllers manage sessions centrally to ensure fast, secure, and seamless roaming as users and devices move throughout the radio coverage range of each AP. Seamless roaming greatly improves productivity by providing true mobility across the enterprise, all transparent to the user.

The Wireless Controllers use industry standards to deliver fast and secure roaming. 802.11i pre-authentication (Pre-Auth) ensures that the user is authenticated to adjacent APs before entering their coverage range, preserving voice calls as users move throughout the enterprise. Opportunistic Key Caching (OKC) is also a supported mechanism which greatly improves device roaming times.

### High Availability and Self-Healing

Redundant Enterasys Wireless Controllers can be deployed across the network and operate in failover or load sharing mode. Access points can be configured for fast-failover mode to allow configuration and service restoration (in tunnel mode) in less than two seconds, thus enabling user sessions to continue uninterrupted. When switching traffic locally, APs continue to provide service even when the link to the wireless controller is severed and can be configured to resume service should a power outage force them to restart.

Enterasys Wireless APs also feature Dynamic Radio Management, which enables the network to automatically adapt to changes in the RF environment or failure of any individual APs, ensuring availability and performance to users. Each wireless AP continuously monitors channel use, signal to noise ratio (SNR) for interference, and the receive power of neighboring APs (Enterasys or third party) to adjust their channel and transmit power.

### Enterasys RoamAbout Controller Investment Protection

Previous investments in the Enterasys RoamAbout® 8110 and 8210 wireless controllers can be leveraged through software upgrades that enable Enterasys Wireless operation.

## Enterasys Wireless Controllers



Supported Features	C20/C20N	C2400	C4110	C5110	CRBT8110	CRBT8210
Capacity						
Total APs supported per controller	64	400	500	1050	48	144
Total APs supported in standard mode	32	200	250	525	24	72
Additional APs supported in high-availability mode	32	200	250	525	24	72
Simultaneous users per controller	512	4096	4096	8192	480	1024
VNS segments per controller	8	64	64	128	8	16
Manageability						
Pre standard (CAPWAP)	✓	✓	✓	✓	✓	✓
Integrated VLAN-VNS	✓	✓	✓	✓	✓	✓
Auto-discovery of new APs	✓	✓	✓	✓	✓	✓
CDR/RADIUS accounting	✓	✓	✓	✓	✓	✓
Visibility through Enterasys NMS Console	✓	✓	✓	✓	✓	✓
Enterasys Wireless Management Suite integration	✓	✓	✓	✓	✓	✓
Integration with Enterasys NAC	✓	✓	✓	✓	✓	✓
Integration with Enterasys IPS and SIEM	✓	✓	✓	✓	✓	✓

## Enterasys Wireless Controllers (cont.)

Supported Features	C20/C20N	C2400	C4110	C5110	CRBT8110	CRBT8210
Performance and Availability						
Automatic failover to redundant controllers	√	√	√	√	√	√
Fast fail-over and Session Availability	√	√	√	√	√	√
Dynamic RF Management (DRM)	√	√	√	√	√	√
Support for intelligent traffic forwarding by user/application segment	√	√	√	√	√	√
Dual, hot swappable power supply		√	√	√		
Security						
Robust standards based security: 802.11i/WPA2, WPA, TKIP, WEP	√	√	√	√	√	√
802.1x Authentication: EAP-TLS, EAP-SIM, EAP-TTLS, PEAP, EAP-MD5, EAP-FAST	√	√	√	√	√	√
RADIUS Authentication and Accounting	√	√	√	√	√	√
Encryption Algorithms: AES (CCMP), RC4-40, 104, 128-bit (TKIP, WEP)	√	√	√	√	√	√
Captive Portal (URL Redirect) and Walled Garden (Unauthenticated access to URL)	√	√	√	√	√	√
Voice						
Voice-over-WLAN Optimization: 802.11e/WMM, U-APSD, TSPEC, CAC, QBSS	√	√	√	√	√	√
Wired-Wireless (DSCP/TOS-to-WMM) QoS Mapping	√	√	√	√	√	√
Roaming between IP subnets	√	√	√	√	√	√
Roaming between multiple controllers	√	√	√	√	√	√

Technical Specifications	C20	C20N	C2400	C4110	C5110
Dimensions					
Length	33.9 cm (13.4 in)	18.54 cm (7.3 in)	33 cm (13.0 in) with module levers	66.04 cm (26 in)	77.2 cm (30.4 in)
Width	43.6 cm (17.2 in)	27.05 cm (10.65 in)	44 cm (17.3 in)	42.63 cm (16.78 in)	42.6 cm (16.7 in)
Height	6.6 cm (2.7 in) – 1.5U	4.57 cm (1.8 in)	11.1 cm (4.4 in) - 2.5U	4.26 cm (1.67 in) – 1U	4.26 cm (1.67 in) – 1U
Weight	7.3 kg (16 lbs.)	N/A	9.4 kg (21 lbs.)	13.45 kg (29.66 lbs.)	17.7 kg (35.8 lbs.)
Environmental					
Operating Temperature	0° C to 40° C (32° F to 104° F)	+5° to 40° C (41° F to 104° F) (maximum change not to exceed 10° C)	0° C to 40° C (32° F to 104° F)	10° C to 35° C (50° F to 95° F)	10° C to 35° C (50° F to 95° F)
Storage Temperature	-40° C to 70° C (-40° F to 158° F)	-10° to +73° C (14° F to 164° F) (ambient)	-40° C to 70° C (-40° F to 158° F)	-40° C to 65° C (-40° F to 149° F)	-40° C to 65° C (-40° F to 149° F)
Humidity	10% to 95%, non-condensing	10% to 90%, non-condensing	10% to 95%, non-condensing	20% to 80%, non-condensing	5% to 95%, non-condensing
Mounting					
19" Rack Mountable	1.5U configuration to fit standard 19" rack (mounting ears provided)	Fits in rack mountable N-Series	2.5U configuration to fit standard 19" rack (mounting ears provided)	1U configuration to fit standard 19" rack	1U configuration to fit standard 19" rack
Front and Rear Mount	I/O cabling at front of unit; power cabling and power switch at the rear	I/O cabling and power cabling at front of unit	I/O cabling at front of unit; power cabling and power switch at the rear	I/O cabling and power cabling at back of unit; power switch at the front	I/O cabling and power cabling at back of unit; power switch at the front

Technical Specifications	C20	C20N	C2400	C4110	C5110
Ports					
<b>Data Ports</b>	2 x 10/100/1000 Base-T	2x1 Gbps SFP DFE Uplink Ports, 2x1 Gbps Internal Ports (connecting the N-Series Wireless Controller Module to the DFE)	4 x 10/100/1000 Base-T	4 x 10/100/1000 Base-T	<ul style="list-style-type: none"> <li>• 2 x 10Gb Short Range Fiber Optic with LC Connectors</li> <li>• 1 x 10/100/1000 Base-T</li> </ul>
<b>Management Ports</b>	<ul style="list-style-type: none"> <li>• 1 x 10/100 Base-T</li> <li>• 1 x USB Port</li> <li>• Console Port DB9 Serial</li> </ul>	<ul style="list-style-type: none"> <li>• 1x 10/100/1000 Base-T</li> </ul>	<ul style="list-style-type: none"> <li>• 1 x 10/100 Base-T</li> <li>• Console Port DB9</li> </ul>	<ul style="list-style-type: none"> <li>• 1 x 10/100/1000 Base-T</li> <li>• 1 x USB Port</li> <li>• Console Port DB9</li> </ul>	<ul style="list-style-type: none"> <li>• 1 x 10/100/1000 Base-T</li> <li>• 4 x USB Ports available. Use one.</li> <li>• Console Port DB9</li> </ul>
Electrical					
<b>Power Rating</b>	<ul style="list-style-type: none"> <li>• Voltage: 90-264 VAC</li> <li>• Frequency: 47-63 Hz</li> <li>• Input Current: 4 A max.</li> </ul>	<ul style="list-style-type: none"> <li>• Voltage Range: 4.96 Amp at 115 V</li> </ul>	<ul style="list-style-type: none"> <li>• Voltage: 90-264 VAC</li> <li>• Frequency: 47-63 Hz</li> <li>• Power (max): 200 W</li> </ul>	<ul style="list-style-type: none"> <li>• Voltage: 110/240 VAC</li> <li>• Frequency: 50-60 Hz</li> <li>• Power (max): 400 W</li> </ul>	<ul style="list-style-type: none"> <li>• Voltage: 110/220 VAC</li> <li>• Frequency: 48-62 Hz</li> <li>• Power (max): 670 W</li> </ul>
Standards Compliance					
<b>Regulatory/Safety</b>	<ul style="list-style-type: none"> <li>• UL 60950-1</li> <li>• CSA 22.1 60950</li> <li>• EN 60950-1</li> <li>• IEC 60950-1</li> </ul>	<ul style="list-style-type: none"> <li>• UL 60950-1</li> <li>• CSA 22.1 60950</li> <li>• EN 60950-1</li> <li>• IEC 60950-1</li> </ul>	<ul style="list-style-type: none"> <li>• UL 60950-1</li> <li>• CSA 22.1 60950</li> <li>• EN 60950-1</li> <li>• IEC 60950-1</li> </ul>	<ul style="list-style-type: none"> <li>• UL 60950-1</li> <li>• CSA 22.1 60950</li> <li>• EN 60950-1</li> <li>• IEC 60950-1</li> </ul>	<ul style="list-style-type: none"> <li>• UL 60950-1</li> <li>• CSA 22.1 60950</li> <li>• EN 60950-1</li> <li>• IEC 60950-1</li> </ul>
<b>Emissions/Immunity</b>	<ul style="list-style-type: none"> <li>• FCC Part 15 (Class A)</li> <li>• ICES-003 (Class A)</li> <li>• AS/NZS CISPR 22 (Class A)</li> <li>• EN 55022 (Class A)</li> <li>• EN 55024</li> <li>• EN 61000-3-2</li> <li>• EN 61000-3-3</li> </ul>	<ul style="list-style-type: none"> <li>• FCC Part 15 (Class A)</li> <li>• ICES-003 (Class A)</li> <li>• BSMI</li> <li>• VCCI V-3</li> <li>• AS/NZS CISPR 22 (Class A)</li> <li>• EN 55022 (Class A)</li> <li>• EN 55024</li> <li>• EN 61000-3-2</li> <li>• EN 61000-3-3</li> </ul>	<ul style="list-style-type: none"> <li>• FCC Part 15 (Class A)</li> <li>• ICES-003 (Class A)</li> <li>• AS/NZS CISPR 22 (Class A)</li> <li>• EN 55022 (Class A)</li> <li>• EN 55024</li> <li>• EN 61000-3-2</li> <li>• EN 61000-3-3</li> </ul>	<ul style="list-style-type: none"> <li>• FCC Part 15 (Class A)</li> <li>• ICES-003 (Class A)</li> <li>• AS/NZS CISPR 22 (Class A)</li> <li>• EN 55022 (Class A)</li> <li>• EN 55024</li> <li>• EN 61000-3-2</li> <li>• EN 61000-3-3</li> </ul>	<ul style="list-style-type: none"> <li>• FCC Part 15 (Class A)</li> <li>• ICES-003 (Class A)</li> <li>• BSMI</li> <li>• VCCI V-3</li> <li>• AS/NZS CISPR 22 (Class A)</li> <li>• EN 55022 (Class A)</li> <li>• EN 55024</li> <li>• EN 61000-3-2</li> <li>• EN 61000-3-3</li> </ul>
<b>Networking</b>	<ul style="list-style-type: none"> <li>• SNMP v2c</li> <li>• Routing – OSPF v2</li> </ul>	<ul style="list-style-type: none"> <li>• SNMP v2c</li> <li>• Routing – OSPF v2</li> </ul>	<ul style="list-style-type: none"> <li>• SNMP v2c</li> <li>• Routing – OSPF v2</li> </ul>	<ul style="list-style-type: none"> <li>• SNMP v2c</li> <li>• Routing – OSPF v2</li> </ul>	<ul style="list-style-type: none"> <li>• SNMP v2c</li> <li>• Routing – OSPF v2</li> </ul>

## Ordering Information

Part Number	Description
Controllers	
<b>WS-C20</b>	C20 WLAN controller. Manages 16 Access Points, expandable to 32 with 16 AP capacity upgrade (WS-C20XCAPUP16). Requires Reg Domain Key.
<b>WS-C20N-32</b>	C20N WLAN controller on N-Series DFE expansion cards. Manages 32 Access Points. Requires Reg Domain Key.
<b>WS-C2400</b>	C2400 WLAN controller. Manages 50 Access Points, expandable to 200 in 25 AP increments with 25 AP capacity upgrade (WS-CTLCAPUP25). Requires Reg Domain Key.
<b>WS-C4110</b>	C4110 WLAN controller. Manages 50 Access Points, expandable to 250 in 25 AP increments with 25 AP capacity upgrade (WS-CTLCAPUP25). Requires Reg Domain Key.
<b>WS-C5110-SR</b>	C5110 WLAN controller. Manages 150 Access Points, expandable to 525 in 25 AP increments with 25 AP capacity upgrade (WS-CTLCAPUP25). Requires Reg Domain Key.
Controller Options	
<b>WS-C20XCAPUP16</b>	C20 capacity upgrade. Increases capacity of WLAN controller from 16 to 32 access points.
<b>WS-CTLCAPUP25</b>	WLAN controller capacity upgrade. Increases capacity of WLAN controller by 25 access points - Note: Not for C20 or C20N.
<b>WS-EXTCP</b>	External Captive Portal for WLAN Controllers. Forces user authentication through customer's external captive portal.
<b>7S-MSM-PS-KIT</b>	WS-C20N External power supply required for all N-Series blades except the following: 7G4280-19, 7G4285-49, 7G4282-49, 4G4285-49, and 4G4282-49.
Activation Keys	
<b>WS-CTLREG6P-NAM</b>	V6 Regulatory Domain Key for North America. Enables WLAN controller and access points with appropriate wireless settings for region.
<b>WS-CTLREG6P-ROW</b>	V6 Regulatory Domain Key for Rest of World. Enables WLAN controller and access points with appropriate wireless settings for region.
<b>WS-CTLREG6P-TH</b>	V6 Regulatory Domain Key for Thailand. Enables WLAN controller and access points with appropriate wireless settings for region.
<b>WS-CTLREG6P-IL</b>	V6 Regulatory Domain Key for Israel. Enables WLAN controller and access points with appropriate wireless settings for region.

---

## Warranty

As a customer-centric company, Enterasys is committed to providing quality products and solutions. In the event that one of our products fails due to a defect, we have developed a comprehensive warranty that protects you and provides a simple way to get your products repaired or media replaced as soon as possible.

Enterasys Wireless Controllers come with a one year warranty against manufacturing defects. For full warranty terms and conditions please go to: [www.enterasys.com/support/warranty.aspx](http://www.enterasys.com/support/warranty.aspx).

## Service & Support

Enterasys Networks provides comprehensive service offerings that range from Professional Services to design, deploy and optimize customer networks, customized technical training, to service and support tailored to individual customer needs. Please contact your Enterasys account executive for more information about Enterasys Service and Support.

## Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at [enterasys.com](http://enterasys.com)



© 2009 Enterasys Networks, Inc. All rights reserved. Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications. Please visit <http://www.enterasys.com/company/trademarks.aspx> for trademark information.

