Advanced Enterprise Wireless LAN Design and Security Training Course



26 - 30 Oct 2026

Boston

7500 € (Per Person)

Ref: #TEL4459_146488

Course Introduction / Overview:

In today's hyper-connected business environment, a robust and secure wireless network is no longer a convenience but the foundational backbone of enterprise operations. This course provides a comprehensive exploration of designing, implementing, and securing modern enterprise Wireless LANs (WLANs). We move beyond basic configurations to delve into the complex architectural decisions that ensure scalability, high performance, and ironclad security. As detailed by experts like Matthew S. Gast in works such as "802.11ac: A Survival Guide," the nuances of RF behavior and security protocols are critical for success. This program, offered by BIG BEN Training Center, addresses the entire lifecycle of an enterprise WLAN, from initial radio frequency (RF) planning and site surveying to deploying advanced security mechanisms like WPA3-Enterprise and Network Access Control (NAC). Participants will gain the strategic insights needed to build resilient wireless infrastructures that can securely support high-density environments, Bring Your Own Device (BYOD) policies, and the proliferation of Internet of Things (IoT) devices, ensuring the network is an enabler of business innovation rather than a point of vulnerability. This training course is meticulously structured to transform participants into proficient architects of enterprise-grade wireless solutions.

Target Audience / This training course is suitable for:

- Network Engineers and Administrators.
- IT Security Specialists and Analysts.
- Wireless Network Architects.
- IT Managers and Team Leaders.
- Solutions Architects and Pre-Sales Engineers.
- Infrastructure Project Managers.
- Systems Engineers responsible for network infrastructure.
- IT professionals seeking to specialize in wireless networking.

Target Sectors and Industries:

- Technology and Telecommunications.
- Financial Services and Banking.
- Healthcare and Medical Facilities.
- Higher Education and K-12 School Districts.
- Retail and E-commerce.
- Manufacturing and Industrial Operations.
- Hospitality and Large Public Venues.
- Government Agencies and Public Sector Organizations.

Target Organizations Departments:

- Information Technology (IT) Department.
- Network Operations Center (NOC).
- Information Security (InfoSec) Department.
- Infrastructure and Operations.
- Technical Support and Help Desk.
- Research and Development (R&D).
- Corporate Real Estate and Facilities Management.

Course Offerings:

By the end of this course, the participants will have able to:

- Design scalable and high-density enterprise WLAN architectures based on business requirements.
- Conduct comprehensive RF site surveys for optimal access point placement and coverage.
- Implement robust wireless security using WPA3, 802.1X, and EAP protocols.
- Configure and manage Network Access Control (NAC) for secure device onboarding.
- Develop and enforce effective security policies for BYOD and corporate-owned devices.
- Integrate and secure IoT devices on the enterprise wireless network.
- Troubleshoot complex connectivity, performance, and security issues in a WLAN environment.
- Perform capacity planning to ensure the network meets current and future demands.
- Analyze wireless traffic and identify potential security threats using modern tools.
- Evaluate and select appropriate WLAN hardware and management platforms.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive, ensuring participants can translate theoretical knowledge into real-world skills. This course moves beyond traditional lectures by integrating a dynamic blend of expert-led instruction, in-depth case study analyses of complex enterprise deployments, and collaborative group workshops. Participants will engage in design simulations where they architect WLAN solutions for various business scenarios, from a high-density corporate campus to a secure healthcare facility. These activities are structured to foster critical thinking and problem-solving skills. Interactive sessions encourage open dialogue, allowing participants to share their unique challenges and learn from the collective experience in the room. Our instructors facilitate these discussions, providing targeted feedback and expert insights. The curriculum emphasizes a vendor-agnostic approach, focusing on the underlying principles of RF design, security architecture, and troubleshooting that are applicable across all major technology platforms. This hands-on, collaborative approach ensures a deep and lasting understanding of the subject matter, empowering participants to confidently design and secure enterprise wireless networks.

Course Agenda (Course Units):

Unit One: Foundations of Modern Enterprise WLANs

- Introduction to enterprise wireless networking standards (802.11ac, 802.11ax - Wi-Fi 6/6E).
- Understanding radio frequency (RF) fundamentals and characteristics.
- Key components of a WLAN architecture: Access Points, Controllers, and Cloud Management.
- Exploring different WLAN architectures: autonomous, controller-based, and cloud-managed.
- The role of antennas and understanding antenna selection criteria.
- Fundamentals of spectrum analysis and identifying sources of interference.
- Regulatory domains and their impact on channel and power selection.

Unit Two: Advanced RF Design and Site Surveying

- The complete site survey lifecycle: planning, execution, and analysis.
- Predictive modeling and design techniques using planning tools.
- Conducting active and passive on-site surveys for data, voice, and location services.
- Capacity planning for high-density user environments.
- Advanced channel planning and co-channel interference mitigation strategies.
- Designing for challenging RF environments like warehouses and hospitals.
- Validating post-deployment network performance against design requirements.

Unit Three: Core Principles of Wireless LAN Security

- An overview of the modern wireless threat landscape.
- Deep dive into WPA3 security enhancements (Personal and Enterprise).
- Implementing robust authentication with 802.1X and Extensible Authentication Protocol (EAP).
- Configuring and managing RADIUS servers for centralized authentication.
- The role of digital certificates and Public Key Infrastructure (PKI) in wireless security.
- Understanding and implementing secure Fast Roaming technologies.
- Securing wireless network management interfaces and protocols.

Unit Four: Implementing Secure Network Access and Segmentation

- Introduction to Network Access Control (NAC) concepts and architecture.
- Developing a comprehensive Bring Your Own Device (BYOD) security policy.
- Implementing secure guest access solutions with captive portals.
- Techniques for device profiling, posture assessment, and onboarding automation.
- Using dynamic VLANs and access control lists for network segmentation.
- Strategies for securing headless devices like IoT sensors and printers.
- Integrating the WLAN with enterprise identity management systems.

Unit Five: WLAN Management, Troubleshooting, and Optimization

- Implementing a Wireless Intrusion Prevention System (WIPS) for threat detection.
- Best practices for monitoring WLAN health and performance.
- Utilizing protocol and spectrum analyzers for advanced troubleshooting.
- Diagnosing and resolving common client connectivity and performance issues.
- Optimizing WLAN performance through RF resource management (RRM).
- Techniques for auditing wireless network security and configuration.
- Preparing for the future: an overview of emerging wireless technologies like Wi-Fi 7.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

How will the convergence of 5G and Wi-Fi 6/7 redefine the concept of the enterprise campus network, and what new security paradigms will be required to manage this unified wireless fabric?

What unique qualities does this course offer compared to other courses?

This training course distinguishes itself by focusing on vendor-agnostic architectural principles rather than vendor-specific product training. While many courses teach how to configure a particular brand of equipment, our program teaches the fundamental 'why' behind strategic design and security decisions, empowering participants to build optimal solutions regardless of the hardware. The curriculum is built upon a foundation of real-world case studies, challenging participants to solve complex problems drawn from actual enterprise deployments in sectors like healthcare, finance, and large public venues. We emphasize a holistic security posture, moving beyond simple WPA2/3 passwords to cover the entire secure access lifecycle, including 802.1X, NAC, device profiling, and micro-segmentation for IoT. Furthermore, the course content is forward-looking, preparing attendees not only for today's challenges with Wi-Fi 6E but also for the emerging integration of technologies like 5G and the demands of next-generation applications. The interactive methodology ensures that participants learn not just from the instructor, but from the diverse experiences of their peers, creating a rich, collaborative learning environment that fosters deep conceptual understanding and practical mastery.