Enterprise Secure Wi-Fi Mobility and Roaming Solutions Training Course

21 - 25 Dec 2026

Berlin

5800 € (Per Person)

Ref: #NO7240_119595

Course Introduction / Overview:

In today's hyper-connected enterprise environment, the demand for seamless and secure wireless mobility is no longer a luxury but a core operational necessity. This course provides a comprehensive exploration of the architectures and protocols that underpin modern, secure Wi-Fi roaming. We will move beyond basic configurations to delve into the intricate mechanics of how devices maintain persistent, secure connections while moving across complex corporate networks. Drawing upon foundational principles outlined by experts like Matthew S. Gast in his seminal work, "802.11 Wireless Networks: The Definitive Guide," this program dissects critical technologies such as 802.1X authentication, WPA3 Enterprise, and the fast transition mechanisms of 802.11r. Participants will gain a deep architectural understanding, enabling them to design, implement, and troubleshoot robust mobility solutions that support everything from corporate laptops to BYOD and IoT devices. BIG BEN Training Center has designed this curriculum to empower IT professionals with the strategic knowledge needed to build resilient wireless infrastructures that balance stringent security requirements with the high-performance user experience expected in the modern digital workplace. This training is your blueprint for mastering secure wireless mobility from the ground up.

Target Audience / This training course is suitable for:

- Network Engineers and Administrators.
- Wireless Network Specialists.
- IT Security Professionals and Analysts.
- Solutions Architects and Network Designers.
- IT Managers and Team Leaders.
- Systems Engineers responsible for infrastructure.
- Technical Support Engineers specializing in networking.
- Infrastructure Project Managers.

Target Sectors and Industries:

- Corporate and Enterprise a.
- Healthcare and Medical Facilities.
- Higher Education and School Districts.
- Retail and E-commerce Logistics.
- Hospitality and Public Venues.
- Manufacturing and Industrial Operations.
- Financial Services and Banking.
- Government and Public Sector Agencies.
- Telecommunications Service Providers.

Target Organizations Departments:

- Information Technology Department.
- Network Operations Center (NOC).
- Information Security (InfoSec) and Cybersecurity.
- Infrastructure and Operations Management.
- Technical Services and Support.
- Research and Development (R&D).
- Enterprise Architecture.

Course Offerings:

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

- Design and deploy robust enterprise-grade secure Wi-Fi roaming architectures.
- Implement and manage 802.1X/EAP authentication using RADIUS servers.
- Master the configuration and benefits of WPA3 Enterprise security protocols.
- Leverage 802.11r, 802.11k, and 802.11v to enable fast and seamless client roaming.
- Architect secure guest and BYOD access solutions without compromising the core network.
- Troubleshoot complex roaming and connectivity issues using protocol analysis.
- Integrate wireless networks with Network Access Control (NAC) solutions.
- Develop comprehensive security policies for corporate wireless environments.
- Optimize RF environments to enhance mobility performance and reliability.
- Evaluate and select appropriate wireless hardware and software for specific mobility needs.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, interactive, and directly applicable to real-world challenges. This course moves beyond theoretical lectures to foster a deep, practical understanding of secure Wi-Fi mobility. A significant portion of the training is dedicated to hands-on lab simulations and configuration exercises that mirror complex enterprise environments. Participants will engage in collaborative problem-solving sessions, analyzing case studies of successful and failed roaming implementations to learn critical design principles. Our expert instructors facilitate dynamic group discussions on topics like developing BYOD policies and integrating NAC solutions, encouraging the exchange of diverse perspectives and experiences. The learning process is reinforced through a continuous feedback loop, where participants present their design solutions and receive constructive critiques. This blend of expert instruction, practical application, and peer-to-peer collaboration ensures that attendees not only learn the "how" but also master the "why" behind secure wireless architectures, leaving them fully equipped to implement effective solutions within their own organizations.

Course Agenda (Course Units):

Unit One: Foundations of Enterprise Wireless Security and Mobility

- Introduction to enterprise WLAN concepts.
- Deep dive into the 802.11 standards family (Wi-Fi 5, Wi-Fi 6/6E).
- Understanding the vulnerabilities of legacy Wi-Fi security (WEP, WPA).
- Comprehensive overview of WPA2 and WPA3 Enterprise security.
- The role of encryption and integrity protocols (TKIP, CCMP, GCMP).
- Fundamentals of RF behavior and its impact on mobility.
- Identifying common wireless security threats and attack vectors.

Unit Two: Mastering 802.1X and EAP Authentication

- The core components of the 802.1X framework (Supplicant, Authenticator, Authentication Server).
- Detailed exploration of Extensible Authentication Protocol (EAP) types (EAP-TLS, EAP-PEAP, EAP-TTLS).
- Configuring and managing RADIUS servers for enterprise authentication.
- Public Key Infrastructure (PKI) and certificate management for wireless clients.
- Implementing certificate-based authentication for maximum security.
- Troubleshooting common 802.1X and EAP authentication failures.
- Integrating directory services (e.g., Active Directory) with RADIUS.

Unit Three: Architecting for Seamless Roaming

- Understanding the client roaming decision process.
- Contrasting Layer 2 and Layer 3 roaming mechanisms.
- Implementing Fast BSS Transition (FT) with 802.11r.
- Utilizing 802.11k for radio resource measurement and neighbor reports.
- Leveraging 802.11v for BSS Transition Management and network optimization.
- Designing controller-based and controller-less roaming architectures.
- Analyzing inter-controller and inter-subnet roaming scenarios.

Unit Four: Advanced Security and Specialized Access Solutions

- Implementing Wireless Intrusion Prevention and Detection Systems (WIPS/WIDS).
- Designing secure and isolated guest Wi-Fi access portals.
- Developing and enforcing Bring Your Own Device (BYOD) security policies.
- Integrating Network Access Control (NAC) for posture assessment and dynamic policy enforcement.
- Understanding and deploying Pass point (Hotspot 2.0) for automatic and secure network access.
- Strategies for securing connections for Internet of Things (IoT) devices.
- Segmenting wireless traffic using VLANs and firewall policies.

Unit Five: Performance Tuning, Troubleshooting, and Optimization

- Conducting wireless site surveys for optimal AP placement and roaming.
- Using spectrum analyzers to identify and mitigate RF interference.
- Capturing and analyzing wireless frames to troubleshoot roaming issues.
- Monitoring key performance indicators (KPIs) for wireless mobility.
- Optimizing roaming thresholds and RF parameters for high-density environments.
- Real-world case studies of enterprise Wi-Fi deployments.
- Final project: Designing a comprehensive secure mobility solution for a sample organization.

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:

As IoT and BYOD proliferation continues to blur network perimeters, how must traditional roaming authentication models evolve to maintain a zero-trust security posture without compromising user experience?

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

This course distinguishes itself by focusing on the vendor-agnostic architectural principles that govern all robust, secure wireless networks, rather than concentrating on the specific command-line interface of a single manufacturer. While many training programs teach you how to configure a device, this curriculum teaches you how to design a resilient and secure system. We emphasize the "why" behind the protocols, ensuring participants understand the intricate interactions between 802.1X, EAP types, and fast roaming amendments like 802.11r. This foundational knowledge empowers professionals to make informed design decisions that are not locked into one ecosystem. Furthermore, the course content places a unique emphasis on the intersection of security, performance, and user experience, treating them as interconnected pillars of a successful mobility strategy. By integrating case studies of complex, real-world deployments and dedicating significant time to advanced troubleshooting methodologies using protocol analysis, the course provides a level of strategic insight that is rare in the industry, preparing participants to architect solutions rather than simply manage existing ones.