

Course ID
UNIFIED
Course Duration
2-3 days

Course Title
**Unified Communications in Public Safety, Law Enforcement,
and Homeland Security**

**Related
Courses**

- Communications Assistance to Law Enforcement Act (CALEA): Technologies and Compliance for TDM and Packet Voice Services (CALEA, 2-3 days)
- Emerging Communications and Technologies in Public Safety, Law Enforcement and Homeland Security (EMERGE-LAW, 2-3 days)
- Security, Privacy and Information Integrity for Managers Executives and Policy Makers (SECURITY-EXEC, 2-3 days)
- IEEE 802.11 (WiFi) Wireless LAN Security (WIFISEC, 3 days)
- Architecture and Operation of Wireless Networks for Technical Investigators: From Their Analog Origins to the Emerging 3G Technologies (WIRELESS-TI, 4-5 days)
- IP, Location and Geo-Location Technologies for Law Enforcement, Intelligence and Public Safety (IPGEOLOC, 2-3 days)
- IP Security v2 (IPSec v2) Architecture and Protocols (IPSEC, 2-3 days)
- IP Security v3 (IPSec v3) Workshop (IPSECWS, 2-3 days)
- Principles of Network Security: CompTIA Security+ and US DoD Directive 8570.1 (NETSEC, 3-4 days)
- SIP Security: A Comprehensive Short Course (SIPSEC, 2 days)
- Session Initiation Protocol (SIP) Workshop (SIPWS, 2-3 days)
- VoIP Security (VOIPSEC, 2 days)
- Voice Communications and Technologies for 911 Call Takers, Supervisors and Trainers (VOICE-911, 2-3 days)
- VoIP for 911 Administrators, Managers, Directors and Regulators (VOIP-911, 2-3 days)
- 911 for IP Professionals (911-IP, 2-3 days)

Aimed At

Technical personnel in public safety, law enforcement, and homeland security arenas who need to undertake a comprehensive study of Unified Communications, from the high-level industry and architectural perspective to the low level protocols and internals.

Group Size

5-25

Prerequisites

A working knowledge of the IP suite, data, voice and video protocols, along with a basic understanding of the principles of Quality of Service/Experience (QoS and QoE) will help fully appreciate the material covered in this course. Those who lack some or all of these prerequisites will still benefit from the course, though they may not be able to finish the lab work during class.

**Course
In a Nutshell**

This intermediate-to-advanced course is intended to prepare an engineering audience for the sea change that is now occurring in communications. It provides the key knowledge and skills required to deal with the Unified Communications protocols, architectures, analysis and system testing, and to understand where Unified Communications -- as defined by multiple vendors -- fits into the overall public safety, law enforcement and homeland security capability, productivity and application set. Upon course completion, you will know everything needed to understand and deal with the next generation of applications as well as the network infrastructure required to support them. Highlights include:

- Brief high level overview of UC and Web 2.0 industry landscape
- Architectural overview of multiple vendors' Unified Communications architectures
- Protocol Workshop based upon a discovery learning approach
- Emphasis on productivity and impact of UC on operations environment
- Focus on Quality of Service (QoS) and Quality of Experience (QoE) issues
- Security, Certificate Authorities, Encryption and Key Management

Customize It!

Customize this course to your group's requirements at little-to-no added cost. We can teach distinct versions of this course tailored for audiences such as network planners, equipment/application designers, and less technical audiences such as managers, executives, business planners, sales/marketing specialists, and operations and support personnel. The specific topics discussed in the course, as well as the depth of treatment for each, can also be tailored to your need.

**Course
Outline**

Introduction: Multiple Views of Unified Communications

- Microsoft View
- Cisco View
- IBM View
- Nortel, Avaya and Alcatel-Lucent View
- Service Provider View
- UC vs Unified Messaging

Web 1.0 to Web 2.0

- The O'Reilly Factor
- Shifting Paradigms

Multimedia, Internet, Communications, Entertainment (MICE)

- MICE Overview
- Life beyond the Triple Play
- Infrastructure, QoS, and QoE
- Service Ubiquity
 - Broadband Wireless
 - Standards

- Platforms and Mobility
- Role of IMS

Unified Communications Architectures in Depth

- Microsoft
 - Solution Integration
 - Network Infrastructure
 - Security
 - Mobility
 - Network Management
 - Third-party Applications
- Cisco
 - Solution Integration
 - Network Infrastructure
 - Security
 - Mobility
 - Network Management
 - Third-party Applications
- Avaya
 - Solution Integration
 - Network Infrastructure
 - Security
 - Mobility
 - Network Management
 - Third-party Applications
- ShoreTel
 - Solution Integration
 - Network Infrastructure
 - Security
 - Mobility
 - Network Management
 - Third-party Applications
- Networx Universal UC Services
 - AT&T
 - UC Service Descriptions
 - Availability
 - QoS/QoE
 - Security
 - Service Level Agreements
 - Qwest
 - UC Service Descriptions
 - Availability
 - QoS/QoE
 - Security
 - Service Level Agreements
 - Verizon
 - UC Service Descriptions

- Availability
- QoS/QoE
- Security
- Service Level Agreements

Inside UC Part 1: Sessions

- Session Initiation Protocol (SIP)
 - SIP Protocol
 - SIP Call Flows
 - SIP Testing
 - SIP Security
- SIP SIMPLE
- Session Description Protocol (SDP)
 - SDP Format
 - SDP: Data Sessions
 - SDP: Voice Sessions/VoIP
 - SDP: Video Sessions
- RSVP
 - Call Admission Control
 - Quality of Service (QoS)
 - Quality of Experience (QoE)
- Location Tracking
 - Presence Applications/SIP Presence Engine (SPE)
 - User Location
 - Wireless
 - Wireline
 - Cisco Emergency Responder
- Session Border Controller (SBC)

Individual Lab Exercise and Group Debrief: SIP, SDP and RSVP Internals and Testing

Inside UC Part 2: Data

- HTTP/sHTTP
- HTML/XML
- FTP/TFTP

Inside UC Part 3: Voice

- SIP Voice
- SCCP/Cisco Skinny
- H.323
- MGCP

Inside UC Part 4: Video

- Videoconferencing Rooms
- Unified IP Phones
- Unified Video Advantage
- Multipoint/Multimedia Control Unit

- H.320 / H.323
- SCCP
- SIP

Inside UC Part 5: Rich Media Conferencing

- Integration
 - SMTP
 - Jabber
 - Outlook
- Web Conferencing
- TelePresence

Inside UC Part 6: Security

- Privacy and Security
- Certificates and Certificate Authorities
- Encryption
- Key Management, PKI, pKI
- SIP Proxy/Secure Authentication
- HTTP Digest Authentication
- Secure Real Time Protocol
- Cisco Remote Party ID (RPID)

Pulling it All Together

- UC and MICE

Individual Discovery Lab Exercise and Group Debrief: Unified Communications

Conclusion

How You Will Learn

- You will learn from an instructor who's well versed in a variety of current and emerging communications technologies and an expert on Unified Communications.
- Along with the lecture, we will use exercises, workshops, group debriefs, and discovery labs to enrich the instruction and drive home the important points.
- If you already know something about UC, we will build on that. We'll compare and contrast what's familiar with what's new, making the new ideas easier to learn as well as more relevant.
- If your background is less technical, we will use examples and analogies to simplify the complex subject matter.
- The Participant Handbook will provide you with a framework to which you can add the information and insight provided in real-time, turning it into a valuable reference resource you can take back to your job.