



EC-Council Certified VoIP Professional

Course Description

VoIP refers to voice calls that are routed over online networks using the Internet Protocol--the IP that serves as the backbone of the Internet and is used to ferry e-mails, instant messages and Web pages to millions of PCs or cell phones. VoIP is a unique bundle of technologies that allows internet-ready devices to transmit voice and other multimedia data over the web instead of over the telephone network. This course covers Voice over IP technologies, concepts, threats and security issues.

Who Should Attend

The **ECVP certification** is intended for IT professionals who are responsible for designing and building Voice over IP networks.

Duration:

5 days (9:00 – 5:00)

Certification

The ECVP 312-78 exam will be conducted on the last day of training. Students need to pass the official Prometric exam to receive the **ECVP** certification.

Course Outline v2

Module 01: Introduction to VoIP

- What is VoIP?
- Why use IP for Voice?
- VoIP-Convergence of Technologies
- Basic VoIP Architecture
- Need of a Layered Architecture
- VoIP Layers
- TCP/IP Overview
 - Functions of TCP/IP Layers
- VoIP Layers Vs. TCP/IP Layers

- Public Switched Telephone Networking(PSTN)
- Circuit Switching Vs. Packet Switching
- Basic VoIP Features
- Benefits of VoIP
- Building The ROI Model
- Disadvantages of VoIP
- Future of VoIP
- Growth in VoIP Subscribers

Module 02: Analog to Digital Conversions

- Source:
 - A to D Conversion
 - Types of ADC's
 - Sigma Delta ADC
 - Successive Approximation ADC
 - Pipelined ADC
 - Flash ADC
 - Comparison of ADC's
 - Working of ADC's
 - Voice Compression
 - Encryption
 - Headers
- Destination
 - Sequencing
 - Decryption
 - Decompression
 - Digital to Analog Conversion

Module 03: Traditional Voice Telephony Principles

- Analog Signaling
- Types of Analog Signaling
 - Earth & Magnet (E&M) Signaling
 - Loop-Start
 - Ground-Start

- Dial-Pulse Signaling
- Dual Tone Multi-Frequency Signaling
- Analog Systems
- Analog Network Components
- Cabling
- Basic Telephone System Operation
- Plain Old Telephone Service (POTS)
- Direct Inward Dialing (DID)
- Digital Subscriber Line (DSL)
- Digital Loop Carrier (DLC)
- Passive Optical Network (PON)
- Dial Plans
- Four-Wire Circuit
- Time Division Multiplexing (TDM)
- Call Control Signaling
- Signaling System 7 (SS7)
 - Signaling Points
 - Signaling Links
 - SS7 Protocol Stack

Module 04: VoIP Devices and Cisco Components

- Basic VoIP Equipments
- VoIP Network Components
 - Analog Telephone Adaptor (ATA)
 - Media Gateway
 - Features of Media Gateway
 - Media Gateway Controller
 - Signaling Gateway
 - Call Manager
 - VoIP Switches
 - IP Phones
 - Private Branch eXchange (PBX)
 - PSTN Gateway

- Session Controller
- Modems
- VoIP Router
 - Cisco's VoIP Components
- Types of VoIP Ports
 - Foreign Exchange Station (FXS)
 - Foreign Exchange Office (FXO)
 - Earth & Magnet (E&M) Interface
- VNM/VIC
 - VNM Models: NM-1V
 - VNM Models: NM-2V
 - VNM Models: NM-HDV High-Density VNM
 - VIC Models: VIC-2E/M
 - VIC-2FXS
 - VIC-2FXO
 - VWIC-2MFT-T1
- Two-Port ISDN BRI Card
- Four-Port Analog DID/FXS VICs

Module 05: Configuring VoIP

- Prerequisites for VoIP Configuration
- Voice Port Cabling and Configuration
 - Port Numbering: 1700 Series
 - Port Numbering: Cisco 1760
 - Port Numbering: 2600 and 3600 Series
 - Port Numbering: MC3810 Series
 - Port Numbering: 7200 Series
 - Port Numbering: AS5300 Series
 - Port Numbering: AS5x00 Series
- Configuring Voice Ports
- Configuring FXO or FXS Voice Ports
- Configuring E&M Ports
- Configuring to adjust Parameters of E&M Ports

- Configuring DID Ports
- Connection Command
- Configuring Delay
 - Fine-Tuning FXS/FXO Ports
 - Fine-Tuning E&M Ports
 - Fine-Tuning DID Ports
 - Configuring POTS Dial Peers
 - Configuring Dial-Peer For VoIP
 - Configuring Dial-Peer For VoFR
 - Configuring Dial-Peer For VoATM
- Configuring Trunking
 - Supervisory Disconnect
 - Configuring a Supervisory Disconnect Voice Class
 - Configuring ISDN BRI Voice Ports
 - Configuring ISDN PRI Voice Ports
 - Configuring ISDN PRI Voice Ports with Q.931
 - Configuring QSIG
 - Configuring T-CCS
- Configuring H.323 Gateways
- Configuring H.323 Gatekeepers
 - H.323 ID Addresses
 - Zone Prefixes
 - Gatekeeper Zone Prefix
 - Technology Prefixes
 - IP Precedence
 - RTP Priority
 - Traffic Shaping
- Configuring cRTP
 - Enable cRTP on a Serial Interface
 - Enable cRTP with Frame Relay Encapsulation
 - Change the Number Of Header Compression Connections
 - Displaying Statistics

- Configuring Custom Queuing
- Enabling Custom Queuing
 - Applying Configuration to an Interface
 - Enabling Priority Queuing: Priority-List Command
 - Enabling Priority Queuing: Set Up Configuration
 - Configuring the Queue Limits
- Applying Priority List to an Interface
 - Verifying Priority Queuing: Show Interface Command
 - Verifying Priority Queuing: Show Queuing Priority Command
- Enabling Weighted Fair queuing
 - Verifying Weighted Fair Queuing: Show Interface Command
 - Verifying Weighted Fair Queuing: Show Queuing Command
- Configuring Class-Based Weighted Fair Queuing (CBWFQ)
 - Defining Class Maps
 - Creating Policies
 - Attaching Policies to Interfaces
 - Verifying CBWFQ: Show-Policy-Map Command
 - Verifying CBWFQ: Show-Policy-Map Interface Command
 - Configuring Packet Classification
 - IP Precedence
 - Verifying IP Precedence
 - Policy Routing
 - Verifying Policy Routing
- Configuring RSVP
 - Verifying RSVP
- Call Admission Control (CAC)
 - Verifying Call Admission Control
 - Configuring Priority Queuing with WFQ
 - Verifying Priority Queuing with WFQ
- Configuring Traffic Shaping
 - Verifying Traffic Shaping
- Configuring Congestion Avoidance with WRED

- Verifying WRED
- Configuring Link fragmentation and Interleaving
 - Verifying Link fragmentation and Interleaving
- Configuring a Single-Router VoIP Network
 - Reviewing the Design
 - Configuring the Router: Step by Step
 - Testing and Verification

Module 06: Implementation and Applications of VoIP

- VoIP Implementation Types
 - Phone to Phone Connection
 - Analog Telephone Adaptor (ATA) Setup
 - Phone to Phone Connection Using Gateway
 - Phone to Phone Connection Using Router
 - Computer to Computer Connection
 - Phone to Computer and Vice-Versa
- IP-Enabled PBX (Private Branch Exchange) Method
- IP Centric LAN Method
- Satellite VoIP
- Software Support for VoIP
- Applications of VoIP
 - What is Skype?
 - System Requirements
 - Getting Started with Skype
 - Skype is Safe
 - Features of Skype
- Skype for Windows
- Skype for Mac OSX
- Skype for LINUX
- Skype for Business
- Skype Web Toolbar
- Skype Email Toolbar
- Skype Office Toolbar

- Skype for Mobile

Module 07: Quality of Service (QoS) of VoIP

- Introduction to QoS
- Quality of Experience (QoE) Vs. QoS
- QoE for VoIP
- Why is QoS needed in IP Transmission?
- Why is QoS needed for VoIP Networks?
- Factors Affecting Quality of Voice in VoIP
- QoS Monitoring
 - Passive Monitoring
 - Active Monitoring
- QoS Protocols
 - RTP
 - RTCP
 - RSVP
- Multiprotocol Label Switching (MPLS)
- Integrated Services (IntServ)
- Differentiated Services (DiffServ)
- IntServ Vs. DiffServ

Module 08: H.323 Standards

- VoIP Standards
- What is the need for VoIP Protocols?
- Introduction to H.323
 - Network Components of H.323
 - Components of H.323
 - H.323 Protocols Suite
 - H.323 Protocol Stack
 - Control and Signaling in H.323
 - H.323 Advantages
 - Network Address Translation (NAT)
 - H.323 and NAT
- H.225

- H.225/Q.931 Call Signaling
- Q.931 Call Signaling Messages
- H.225/Q.931 Signaling
- H.225 Registration, Admission, Status (RAS)
- H.225/Q.931 RAS
- Key RAS Messages
- H.225 Protocol Structure
- H.225 Security Considerations
- H.235: Security and Encryption for H.323
- H.245 Call Control Messages
- H.245 Call Control
- H.245 Security Mechanism
- H.261 (Video Stream for Transport Using the Real-Time Transport)
- H.263 (Bitstream in the Real-Time Transport Protocol)
- DVB (Digital Video Broadcasting)
- H.450.1
- H.450.2
- H.450.3
- H.450.4
- H.450.5
- H.450.6
- H.450.7
- H.450.8
- T.38
- T.120
- T.121
- T.122
- T.124
- T.125
- T.126
- T.127

Module 09: SIP and Supporting Protocols

- Session Initiation Protocol (SIP)
 - Components of SIP
 - SIP Messages
 - Headers for SIP Entities
 - SIP Functions
 - SIP: Supported Protocols
 - Understanding SIP's Architecture
 - Registering with a SIP Registrar
 - Requests through Proxy Servers
 - Requests through Redirect Servers
 - Peer to Peer Architecture
 - Instant Messaging and SIMPLE
 - SIP security
 - H.323 Vs. SIP
- Session Description Protocol (SDP)
 - SDP Specifications
 - Security Issues
- Real-Time Transport Protocol (RTP)
- Real-Time Transport Control Protocol (RTCP)
- Real-Time Transport Streaming Protocol (RTSP)
- Simple Gateway Control Protocol (SGCP)
- Session Announcement Protocol (SAP)
- Skinny Client Control Protocol (SCCP)
- Security Implications for Skinny
- Dynamic Host Configuration Protocol (DHCP)
- Trivial File Transfer Protocol (TFTP)
- Hyper Text Transfer Protocol (HTTP)
- Skype Protocol
- Inter-Asterisk Exchange (IAX)
- Simple Network Management Protocol (SNMP)

Module 10: Megaco Protocol

- Media Gateway Control Protocol (MGCP)

- History of Megaco (H.248)
- Media Gateway Reference Architecture
- MGCP Connections
- Per-Call Requirements
- Megaco Vs. MGCP
- Megaco Protocol Design
- Megaco Commands
- Megaco Messaging Sequence
- Megaco Packages
- Megaco IP Phone Media Gateway
- Role of Call Processing Language
- Call Processing Language Characteristics
- Protocol Security

Module 11: Resource Reservation Protocol

- Resource Reservation Protocol (RSVP)
- RSVP Setup
- RSVP Message Structure
- RSVP Message
- RSVP Message Types
- RSVP Object Fields
- RSVP Object Classes
- RSVP Operation
- RSVP Data Payload
- RSVP Quality of Service
- RSVP Session Start-up
- RSVP Reservation Style
- RSVP Tunneling
- RSVP Traffic Control Module
- Security Implications

Module 12: Wireless VoIP

- Voice Over WLAN (VoWLAN)
 - VoWLAN Call Routing

- Characteristics of VoWLAN
- Limitations of VoWLAN
- Wireless VoIP
 - Wireless VoIP Deployment
 - Advantages of Wireless VoIP
 - Limitations of Wireless VoIP
 - Standards and Protocols
- Unlicensed Mobile Access (UMA)
- Wireless VoIP Gateway: AH1038
- Wireless VoIP Gateway: D-Link DVG-G1402S
- Wireless VoIP Gateway: Motorola HH1620 DSL
- Wireless IP Phone
- Wireless VoIP Phone: EZLoop
- Wireless VoIP Phone: P-2000W_V2
- Wireless VoIP Phone: Shenzhen WP10W-S
- Challenges to Build Successful Wireless VoIP Product
- Attacks on Wireless VoIP

Module 13: Encryption Techniques for VoIP

- Encryption
 - Why VoIP needs Encryption?
 - VoIP Encryption
 - How to Encrypt VoIP?
 - Pros & Cons of VoIP Encryption
 - Voice and Data Encryption Device (V/DED)
 - Speech Encryption
 - Media Encryption
 - Wireless Encryption
- IPSec and Role of IPSec in VoIP
 - Transport Mode
 - Tunnel Mode
- Solutions to VoIPSec Issues
 - IETF Encryption Solutions for VoIP

- Suites from the IETF
- S/MIME: Message Authentication
- Transport Layer Security (TLS)
- TLS: Key Exchange and Signaling Packet Security
- Secure Real-Time Transport Protocol (SRTP)
- SRTP: Voice/ Video Packet Security

Module 14: Troubleshooting VoIP Network

- Issues of Network Slow Down
- Troubleshooting Packet Loss
- Troubleshooting Jitter
- Troubleshooting Packetization Delay
- Troubleshooting Bandwidth Problems
- Troubleshooting Echo
- Troubleshooting Voice Quality on Voice Ports
- Troubleshooting Two-stage Dialing Failures
- Troubleshooting Socket Failures
- Troubleshooting Speech Recognition
- Troubleshooting Cabling
- Troubleshooting Private Branch Exchange (PBX) Problems
- Troubleshooting Central Office (CO) Problems
- Troubleshooting Trunk Signaling
- Troubleshooting Gateways and Gatekeepers
- Troubleshooting Dial Peers
- Troubleshooting Serial Interfaces
- Troubleshooting Frame Relay
- Troubleshooting FXS and FXO Voice Ports
- Troubleshooting E&M Voice Ports
- Troubleshooting Dial Plans
- Basic VoIP Issues and Solutions
- Troubleshooting RSVP
- Troubleshooting MGCP
- Troubleshooting RTP

- Troubleshooting RTSP

Module 15: VoIP Testing and Tools

- Test Strategy
- VoIP Network Component Testing
 - Gateway Testing
 - Gatekeeper Testing
 - IVR Testing
 - Billing and Prepaid Testing
 - NMS Testing
 - VoIP Test Suite
- MediaPro: VoIP and Video Analyzer
- 323Sim: H.323 Simulator
- Vulnerability Assessment
- Penetration and Vulnerability Testing
- VoIP Security Tools
- VoIP Sniffing Tools
 - Auth Tool
 - VoIPong
 - Vomit
 - PSIPDump
 - Netdude
 - Oreka
 - Wireshark
 - Web Interface for SIP Trace (WIST)
 - RTP Break
- VoIP Scanning and Enumeration Tools
 - SNScan
 - Netcat
 - Smap
 - SIPScan
 - SIPcrack
 - VoIPaudit

- iWAR
- SiVUS
- SCTPscan
- VoIP Packet Creation and Flooding Tools
 - Sipsak
 - SIPp
 - SIPNess Messenger
 - SIP Bomber
 - Spitter
 - Sip Send Fun
 - Scapy
- VoIP Fuzzing Tools
 - Ohrwurm
 - Fuzzy Packet
 - SIP Forum Test Framework (SFTF)
 - Asteroid
 - SIP-Proxy
- VoIP Signaling Manipulation Tools
 - RTP Tools
 - Tcpdump
 - Windump
 - Ethereal (Wireshark)
 - Softperfect Network Sniffer
 - Http Sniffer
 - Ether Detect Packet Sniffer
 - Iris Network Traffic Analyzer
 - SmartSniff
 - NetResident Tool
- VoIP Troubleshooting Tools
 - P.862
 - P.563
 - RTCP-RFC3550

- RTCP XR-RFC3611
- Packet Statistics
- Test Tools
- Traceroute
- VQmon
- Other VoIP Tools

Module 16: Threats to VoIP Communication Network

- VoIP is Prone to Numerous Threats
- VoIP Vulnerabilities
 - Denial of Service (DOS)
 - DoS Attack Scenarios
 - Eavesdropping
 - Packet Spoofing and Masquerading
 - Replay Attack
 - Call Redirection and Hijacking
 - ARP Spoofing
 - ARP Spoofing Attack Scenarios
 - Service Interception
 - H.323-Specific Attacks
 - SIP Security Vulnerabilities

Module 17: VoIP Security

- Why VoIP Security?
- Constituents of VoIP Security
- VoIP Myths and Realities
- Securing VoIP with DoS Attacks
- Securing against Replay Attack
- Securing ARP Caches against ARP Manipulation
- Securing H.235 Protocol
- Transport Layer Security (TLS)
- Skype Protocol Security
- IAX Protocol Security
- Security Implications for TFTP

- Security Implications for HTTP
- Security Implications for DHCP
- Security Policies and Processes
- Physical Security
 - Human Safeguard Recommendations
 - Environmental Safeguard Recommendations
- Network Intrusion Detection Systems
- Host-Based Intrusion Detection Systems
- Guidelines for Securing VoIP Network
- Best-Practice Approaches for Minimizing common VoIP Network Risks

Module 18: Logical Segregation of Network Traffic

- Logical Separation of Data
- Converged Network
- Virtual LANs (VLANs)
 - VLAN Security
 - VLANs and Softphones
- QoS and Traffic Shaping
- NAT and IP Addressing
 - How does NAT Work?
 - NAT: Modes of Operation
 - NAT and Encryption
- Authentication Header (AH)
 - AH: Transport and Tunnel Modes
- Encapsulation Security Payload (ESP)
 - ESP Header: Transport Mode and Tunnel Mode
- Firewalls
 - Deep packet Inspection (DPI)
 - Shallow packet Inspection
 - Stateful Inspection
 - Medium-Depth Packet Inspection
- VoIP-Aware Firewalls Issues
 - H.323 Firewalls Issues

- SIP Firewalls Issues
- Bypassing Firewalls and NAT
- Methods for Enabling SIP
- Access Control Lists

Module 19: Hardware and Software VoIP Vendors

- Alcatel
- Global Crossing
- Avaya
- Whaleback
- Nortel
- Norstar VoIP Gateway
- Polycom
- Packet8
- Vonexus
- Infotel
- Net 4 India
- Dialxia
- NGT
- Qwest
- Pingtel
- Cisco
- 3Com
- Vocalocity
- Motorola
- Nokia

Module 20: Regulatory Compliance of VoIP

- Regulatory Compliance
 - Sarbanes-Oxley Act (SOX)
 - Management Assessment of Internal Controls
 - SOX Compliance and Enforcement
 - Gramm-Leach-Bliley Act (GLBA)
 - Privacy Rule -Protection of Nonpublic Personal Information

- Risk Management Guidelines for VoIP Systems
- Development and Implementation of Information Security
- Health Insurance Portability and Accountability Act (HIPAA)
 - Security Standards for the Protection of PHI
 - Safeguards Standard for the Protection of PHI
 - Types of Safeguards
 - Administrative safeguards
 - Physical safeguards
 - Technical safeguards
- Communication Assistance for Law Enforcement ACT (CALEA)
 - Assistance Capability Requirements
 - Cooperation of Equipment Manufacturers and Providers of Telecommunic Support Services
 - Technical Requirements and Standards
 - Steps to Resolve CALEA
- Enhanced 911 and Related Regulations
 - E911 Regulatory Basics
- European Union (EU) Regulatory Framework
 - EU Regulatory Basics

Module 21: VoIP Hacking

- Types of VoIP Hacking
- Stages of VoIP Hacking:
 - Foot printing
 - Scanning
 - Enumeration
- Footprinting
 - Information Sources
 - Unearthing Information
 - Organizational Structure and Corporate Locations
 - Help Desk
 - Job Listings
 - Phone Numbers and Extensions

- VoIP Vendors
- Resumes
- WHOIS and DNS Analysis
- Steps to Perform Footprinting
- Scanning
 - Objectives of Scanning
 - Host/Device Discovery
 - ICMP Ping Sweeps
 - ARP Pings
 - TCP Ping Scans
 - SNMP Sweeps
 - Port Scanning and Service Discovery
 - TCP SYN Scan
 - UDP Scan
 - Host/Device Identification
- What is Enumeration?
 - Steps to Perform Enumeration
 - Banner Grabbing with Netcat
 - SIP User/Extension Enumeration
 - REGISTER Username Enumeration
 - INVITE Username Enumeration
 - OPTIONS Username Enumeration
 - Automated OPTIONS Scanning with sipsak
 - Automated REGISTER, INVITE and OPTIONS Scanning with SIPSCAN against server
 - Automated OPTIONS Scanning Using SIPSCAN against SIP Phones
 - Enumerating TFTP Servers
 - SNMP Enumeration
 - Enumerating VxWorks VoIP Devices
- Steps to Exploit the Network
 - DoS & DDoS Attacks
 - Flooding Attacks

- DNS Cache Poisoning
- Sniffing TFTP Configuration File Transfers
- Performing Number Harvesting and Call Pattern Tracking
- Call Eavesdropping
- Interception through VoIP Signaling Manipulation
- Man-In-The-Middle (MITM) Attack
- Application-Level Interception Techniques
 - How to Insert Rogue Application?
 - SIP Rogue Application
 - Listening to/Recording Calls
 - Replacing/Mixing Audio
 - Dropping Calls with a Rogue SIP Proxy
 - Randomly Redirect Calls with a Rogue SIP Proxy
 - Additional Attacks with a Rogue SIP Proxy
- What is Fuzzing?
 - Why Fuzzing?
 - Commercial VoIP Fuzzing tools
- Signaling and Media Manipulation
 - Registration Removal with erase_registrations Tool
 - Registration Addition with add_registrations Tool
- VoIP Phishing
- Covering Tracks

© 2007 EC-Council. All rights reserved.

This document is for informational purposes only. EC-Council MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUM
EC-Council logo is registered trademarks or trademarks of EC-Council in the United States and/or other countries.