CONCEPT

Enterprise VoIP and IP Telephony Course: SIP, QoS, IP PBX and Unified Communications



Enterprise VoIP and IP Telephony Course: SIP, QoS, IP PBX and Unified Communications

Introduction:

Enterprise VoIP and IP telephony, covering SIP, QoS, IP PBX and unified communications, is a 1-week course for network engineers, unified communications administrators and telephony support staff, ending with an Enterprise VoIP Deployment and Security Checklist. Many organisations move from legacy telephone systems to IP telephony and SIP trunks without voice-ready networks or security controls, and then face poor call quality, outages and toll fraud. Nominees already support networks or telephone systems, and teaching is hands-on in a lab with IP PBX, softphones and packet captures. CoreConcept Training Center delivers this enterprise VoIP course.

Course Objectives:

- Explain how SIP signalling, RTP media and codecs work together to set up, carry and end an enterprise call
- Configure an IP PBX with extensions, dial plans, call routing, voicemail and softphone and desk-phone endpoints
- Design and apply QoS for voice using DSCP marking, queuing and bandwidth calculations per codec
- Connect the IP PBX to a SIP trunk through a session border controller with secure signalling and media
- Diagnose call setup failures, one-way audio, echo and jitter using SIP traces, RTP statistics and MOS
- Produce an Enterprise VoIP Deployment and Security Checklist for a new site or migration

Target Audience:

- Network engineers responsible for LAN and WAN readiness for voice and video traffic
- Unified communications administrators responsible for IP PBX and call manager configuration
- Telephony support staff responsible for handsets, softphones and user call problems
- IT security staff responsible for protecting voice systems against fraud and attack
- Infrastructure project staff responsible for migrating sites from legacy telephone systems

Course Outline:

Day 1: VoIP Foundations and Enterprise Telephony Architecture

- Legacy TDM Telephony Compared With IP Telephony Architecture
- SIP RFC 3261 Messages, Methods and Response Codes
- RTP RFC 3550 Media Streams and RTCP Reports
- G.711, G.729, G.722 and Opus Codec Selection
- Enterprise Voice Readiness Assessment of Existing Networks

Day 2: SIP Call Flows, IP PBX and Unified Communications

- SIP Registration, Call Setup and Teardown Flow Analysis
- SDP Offer and Answer Codec Negotiation in Calls
- IP PBX Extensions, Dial Plans and Call Routing Rules
- Unified Communications Presence, Video and Softphone Integration
- Voicemail, Hunt Groups and Call Queue Configuration

Day 3: Voice QoS, SIP Trunking and Network Design

- DSCP Expedited Forwarding Marking and Voice VLAN Design
- Bandwidth Calculation per Codec, Packetisation and Overhead
- Queuing and Policing Policies for Voice and Video
- SIP Trunk Provisioning and Number Routing to Carriers
- Session Border Controller Placement, NAT Traversal and Interworking

Day 4: VoIP Security, Voice Quality and Troubleshooting

- Toll Fraud Patterns and Call-Pattern Monitoring Controls
- SIP Scanning, Registration Attacks and Rate Limiting Defences
- SRTP RFC 3711 and TLS Signalling Encryption Setup
- ITU-T G.107 E-Model and MOS Voice Quality Scoring
- Wireshark SIP Trace and RTP Jitter Diagnosis Procedure

Day 5: Lab Build and the Deployment Checklist

- Lab Build of an IP PBX With SIP Trunk
- QoS Policy Test Under Simulated Network Congestion
- Fault-Finding Lab on One-Way Audio and Failed Calls
- Security Hardening Review Against the Checklist Controls
- Enterprise VoIP Deployment and Security Checklist Completion

Skills You Will Gain:

- SIP Call Flow Analysis
- IP PBX Configuration
- Codec Selection
- Voice QoS Design
- SIP Trunk Integration
- Session Border Controller Configuration
- VoIP Fraud Prevention
- Voice Quality Troubleshooting

Why Attend This Course:

- Deliver an Enterprise VoIP Deployment and Security Checklist with a tested configuration record to the IT infrastructure manager and the security team
- Decide which codecs, QoS policies and trunk designs suit each site before a migration starts
- Avoid toll fraud losses, dropped calls and poor voice quality caused by unprepared networks and open SIP services
- Guide colleagues through SIP trace reading and the fault-finding steps practised in the lab

Conclusion:

Back at work, the participant gives the Enterprise VoIP Deployment and Security Checklist to the IT infrastructure manager, the security team and the project lead for the next site or migration. They use it to approve network readiness, choose codecs and trunk designs and confirm security controls before calls go live. After the first site cutover, the team should review call quality scores, failed-call records and fraud alerts against the checklist and update any control that did not hold.

Frequently Asked Questions FAQ:

What should participants know before an enterprise VoIP and IP telephony course?

Participants should understand IP addressing, VLANs and basic routing, and have supported a network or telephone system. Bringing a current dial plan, network diagram or recent call-quality complaint helps them apply the lab work to their own organisation.

How does an enterprise VoIP and IP telephony course differ from a service-provider voice core course?

This course covers voice inside an organisation: IP PBX, handsets, softphones, unified communications, SIP trunks and edge security. Service-provider courses cover carrier voice cores, mobile voice and interconnection between operators, which this course does not teach.

Why does enterprise VoIP and IP telephony need QoS on the network?

Voice packets must arrive quickly and evenly. Without marking and queuing, file transfers and video can delay or drop them, causing choppy audio, echo and dropped calls even when total bandwidth looks sufficient.

What do participants take back from the enterprise VoIP and IP telephony course?

Participants take back an Enterprise VoIP Deployment and Security Checklist, a tested IP PBX and SIP trunk configuration record, a QoS policy template and a fault-finding procedure for common call problems.