The SIP School

Course Objectives

This course will take delegates through the basics of SIP into some very technical areas and is suited to people who will be installing and supporting SIP solutions of all kinds. It is also of value for people who need to have a good understanding to help them sell SIP Solutions and Services along with planning their implementations.

Being a modular training course, delegates can work through all modules or simply choose the module they really need. If delegates are new to SIP, they can start at the center of the circle and work their way outwards.

Each module has it's own ‘mini’ quiz at the end to help delegates ‘gauge’ how well they are doing and the ‘Final’ SSCA™ accreditation test is available from the SIP School Login Page.

The Modules are as follows with detailed descriptions further in this document:

- Core SIP
- SIP Trunking
- SIP-T and the PSTN
- Firewalls, NAT and Session Border Controllers
- SIP Security
- SIP and Voice over IP
- SIP and Unified Communications
- ENUM and DNS
- Testing and Troubleshooting

Total Running time for this course (including time taken to work on all the labs) is approximately 14 ½ hours from the start to finish. This does not include study time for the SSCA™ or the taking of the SSCA™ final test itself.
Core SIP

Module times
- Running time = 63 minutes
- Quizzes = 7 minutes
- Total = 70 minutes

SIP (The Session Initiation Protocol) is described in this module along with the many other Components and Services that will be encountered on a SIP based network

Topics:

- SIP - Who benefits?
- SIP – The Session Initiation Protocol
- SIP 'Official Summary'
- Based on HTML
- Where does SIP fit in?
- SIP Clients and Servers
- SIP User Agents
- Simple Call Session Setup
- SIP System Architecture
- The URI - Unique Resource Identifier
- SIP Addressing
- SIP Addressing Examples
- SIP Servers and Operation Registration
- Re-Registration
- SIP Proxy servers and why we need them
- SIP Server – Proxy Mode
- SIP Server – Re-Direct Mode
- Proxy Server 'State' types
- Location Services Registration
- Re-Registration
- DHCP and SIP
- SIP Proxy – Trapezoid Model
- SIP Server in Proxy Mode
- SIP Server in Proxy Redirect Mode
- Stateful and Stateless Proxies
- Location Server
- Location Server – Components
- Location Server – Information
- Sources
- Location Server – Example
- SIP Messaging
- Request Methods
- Response Codes
- SIP Headers
- INVITE – Example
- RESPONSE – Example
- SIP Request Methods
- SIP Response Codes
- SIP Headers
- SIP HEADER - INVITE
- SIP HEADER - 200 Response
- SDP – The Session Description Protocol
- SDP in a SIP Message
- An SDP Example
- Extending SDP
- Changing Session Parameters
- Call Hold example
- Multiple ‘m’ lines
- SDP – The Session Description Protocol
- SDP Component in a SIP Message
- SDP Example
- Extending SDP
- Changing Session Parameters
- SIP Call Forking - Sequential
- Call Forward - No Answer
- Call Forward to Voicemail
- More Proxy Server details
- Headers
- Record-Route Defined
- Record Route Example
- How do we keep track?
- Call leg and Call ID
- Tag and Branch ID
- More on Proxies and SIP Routing
- VIA Headers
- Record-Route and Route Session Policies
- MIME
- Multiple MIME parts
- SIP and the PSTN
- SIP to PSTN Call Flow
- SIP to PSTN Detail
- SIP Codes and the PSTN
- SIP and B2BUA
- B2BUA - Back to Back User Agent
- B2BUA Example
- B2BUA Benefits and Features
- Request for Comments
- New RFCs
- SIPIT
- The Call Process
SIP Trunks

Module times
- Running time = 36 minutes
- Quizzes = 7 minutes
- Lab – ‘Setting up SIP Trunks’ – approx 120 minutes
- Total = 163 minutes

This module teaches the theory of connecting a SIP based PBX to the PSTN and it is the foundation of vendor specific Trunking modules.

Topics:
- A Basic Overview
- Benefits of SIP Trunking
- SIP Trunking – more depth
- SIP Trunking in the Network
- SIP Trunk Capabilities
- SIP Trunking Network Examples
- SIP Peering
- Peering problems?
- Least Cost routing (LCR)
- Disaster Recovery
- SIP PBX Requirements
- Enterprise PSTN Identities
- P-Preferred and P-Asserted
- Call Progress Tones
- Trunking ‘Variations’
- Single Site, TDM PBX
- Single Site, No ‘Forklift’
- Single Site, Converged
- Converged – SIP/IP PBX
- Multiple Site, ‘Converged’
- Media Gateways
- SIP PBX to Non-SIP PBX
- SIP PBX to Non-SIP PBX, Call
- Flow
- SIP Trunks Performance
- The ADSL issue
- Codecs, Voice and Data
- Symmetric DSL (SDSL)
- Bandwidth Calculator
- Testing your link
- Configuration
- Security and SIP Trunks
- SIP Trunk Security - Overview
- Session Border Controllers
- Setting up a SIP Trunk
- Add a VoIP Provider
- Provider SIP Servers
- Authentication
- Stun and the Firewall test
- Add a Dialling Rule
- Trunk setup complete
- Registration Trace
- Call out Trace
- Next Generation Networks
- An Example – British Telecom
- Troubleshooting and Interops
- SIP Trunks and Common Problems
- The SIP Forum
- SIPit
- SIPit Results
- SIP Connect Document
- Choosing an ITSP
- ITSP Offerings
### SIP-T and the PSTN

Module times
- Running time = 25 minutes
- Quizzes = 7 minutes
- Total = 32 minutes

SIP Networks will of course have to allow connections to and from the PSTN. This module works through SIP and PSTN connectivity.

Topics:
- SIP to PSTN Overview
- SIP to PSTN Call Flow
- SIP to PSTN Detail
- PSTN to SIP Call Flow
- SIP to PSTN Call Failure
- SIP to PSTN Call trace
- Early Media
- Early Media - SIP to PSTN Call Gateways
- Early Offer / Delayed Offer
- Default Gateway?
- Gateway Location and Routing with TRIP
- TRIP Example
- SIP-T and PSTN Bridging
- SIP-T
- ISUP, ISDN and SIP
- ISUP and SIP Messages
- ISDN User Part (ISUP) to SIP Codes
- PSTN to PSTN via SIP
- ISUP Encapsulation
- ISUP Encapsulation / SDP Addressing Notes
- SIP and DTMF
- DTMF - Quick Re-Cap
- What is DTMF?
- DTMF Transport methods
- DTMF ‘Inband’
- RFC 2833 ‘Trace’ example

### Firewalls, NAT and Session Border Controllers

Module times
- Running time = 24 minutes
- Quizzes = 7 minutes
- Total = 31 minutes

Inevitably, all IP traffic comes across a Firewall / NAT device and in the case of SIP they can stop the flow of SIP message. This module looks at the problems and the solutions including Session border controllers.

Topics:
- Firewalls
  - What does a Firewall do?
  - Are Firewalls effective?
  - What is NAT?
  - NAT Request
  - NAT Response
  - Multiple NATs
  - The NAT Problem
  - Types of NAT
  - NAT – Full Cone
  - NAT – Restricted Cone
  - NAT – Port Restricted Cone
  - NAT – Symmetric
  - The NAPT or (PAT) Problem
- Problems with NAT, Firewalls and SIP
- The Solutions
- STUN (Simple Traversal of UDP)
- STUN (Simple Traversal of UDP)
- STUN and rport
- Problems with STUN
- TURN (Traversal Using Relay NAT)
- Interactive Connectivity
- Establishment (ICE)
- How ICE works – Simplified!
- More on ICE
- Universal Plug and Play
- (UPnP)
- The RTP Problem
- The Firewall Problem
- Solving the RTP Problem
- Symmetric RTP
- Media Proxy
- Application Level Gateway
- SIP Aware Firewalls - Incoming
- SIP Aware Firewalls - Outgoing
- Session Border Controllers
- SBC for the Enterprise
- SBC for the ITSP
- Enterprise SBC – in Action!
SIP Security

Module times
- Running time = 35 minutes
- Quizzes = 7 minutes
- Lab – ‘Various’ ~ approx 120 minutes
- Total = 162 minutes

SIP Security is a complex issue and this modules covers many SIP Security problems along with possible solutions

Topics:

Authentication and Authorization
- SSL and TLS
- SIP and TLS
- TLS Thoughts
- Attacks and Responses
- Phishing and SIP exploit
- RFC 4475

SIP Proxy Authentication
- SIP and TLS
- SSL and SIP in Action
- Try for Yourself
- Types of Attack on a VoIP/SIP

401 and 407 Authorization
- SIPS and SIP Addressing
- Network
- Responses and Protection
- TLS v SSL

SIP Authorization
- Setting SRTP on SIP Devices
- SRTP and SRTCP
- Response Identity – A Problem!

PROXY Authentication
- Secure RTP (SRTP)
- Secure RTP (SRTP) - Example
- Rogue SIP Proxy
- More Examples

SSL with MD5 Cracked !
- MD5 v SHA
- Caller Identity
- Try for yourself!

Encryption
- Setting SRTP on SIP Devices
- SRTP and SRTCP

Why Encrypt SIP?
- Secure RTP (SRTP) - Example
- Cain

Certificates and HTTPS
- MD5 v SHA
- S/MIME and SIP
- nmap

Certificate Authorities
- Caller Identity
- MIME and ISUP
- NIST Recommendations

Certificate Example
- Setting SRTP on SIP Devices
- Enhancing SIP Trunk Security

Self-Signed Certificates
- Secure RTP (SRTP) - Example
- Alternatives - IPSec, ZRTP

Format type
- SRTP and SRTCP
- Cain

Securing SIP and VoIP
- MD5 v SHA
- S/MIME and SIP
- nmap

S/MIME and ISUP
- SELIR Trunking and Security
- NIST Recommendations

DTLS/SRTP
- Enhancing SIP Trunk Security
- Alternatives - IPSec, ZRTP
### SIP and VoIP

**Module times**
- Running time = 34 minutes
- Quizzes = 7 minutes
- Total = 41 minutes

This module is a refresher module on the basics of **Voice over IP** and also focuses on components that are important to a SIP based Network

**Topics:**

<table>
<thead>
<tr>
<th>What is VoIP?</th>
<th>Delivery Information</th>
<th>802.1P - L2 Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is Voice over IP?</td>
<td>RTP Encapsulation</td>
<td>TOS and DiffServe</td>
</tr>
<tr>
<td>VoIP – ‘A Basic Call’</td>
<td>RTP Header Trace</td>
<td>Layer 3 Classification</td>
</tr>
<tr>
<td>VoIP and TCP / UDP</td>
<td>Real Time Control Protocol</td>
<td>Codecs and Bandwidth</td>
</tr>
<tr>
<td>VoIP over the Internet</td>
<td>RTP-XR (Extended Reports)</td>
<td>Symmetric DSL (SDSL)</td>
</tr>
<tr>
<td>Branch to Branch VoIP</td>
<td>RTP / RTCP and UDP Ports</td>
<td>Testing your link</td>
</tr>
<tr>
<td>IP PBX</td>
<td>Quality of Service</td>
<td>SIP, SDP and VoIP</td>
</tr>
<tr>
<td>Voice Sampling and Codecs</td>
<td>QoS Issues</td>
<td>SIP in the TCP/IP Model</td>
</tr>
<tr>
<td>Encoding</td>
<td>Measuring Delay</td>
<td>SIP and SDP Messages</td>
</tr>
<tr>
<td>Codecs for Voice</td>
<td>Jitter and Packet Loss</td>
<td>SIP and SDP Codec mapping</td>
</tr>
<tr>
<td>MOS – Mean Opinion scores</td>
<td>General VoIP Acceptance Criteria</td>
<td>Where does SIP fit in?</td>
</tr>
<tr>
<td>The Real Time Protocol (RTP)</td>
<td>QoS on the Network</td>
<td>SIP, SDP and VoIP INVITE</td>
</tr>
<tr>
<td>Payload Type Identification</td>
<td>802.1Q – VLANs</td>
<td>Audio and Video in the SDP body</td>
</tr>
<tr>
<td>Sequence Numbering</td>
<td>802.1Q/P Tagging</td>
<td></td>
</tr>
<tr>
<td>Timestamps</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Testing and Troubleshooting

Module times
- Running time = 29 minutes
- Quizzes = 7 minutes
- Lab – ‘Various’ ~ approx 240 minutes
- Total = 276 minutes

Learn how to Monitor and Test SIP devices and services using Wireshark. This tool enables delegates to analyze call control messages to establish where a fault may lie in your SIP infrastructure. Full examples are provided and delegates are encouraged to follow the exercises to try for themselves.

Topics:

Setting up a Test Environment  Wireshark Icons  Troubleshooting SIP Trunks
SIP Phones  Using Wireshark - Capturing  4xx — Client Failure Responses
Choosing a ‘Trial/Test’ ITSP  Using Wireshark – Simple Filters  5xx — Server Failure Responses
Download a Free Soft Phone  Using Wireshark – SIP Statistics  6xx — Global Failure Responses
Free ITSP Accounts  Using Wireshark – SIP ladders  More SIP Testing Tools
Configuring the Softphone  Using Wireshark – RTP Statistics  SIP Scenario
Even more SIP Softphones  Saving Captures  SIP Scan
The SIP Phones @ The SIP School  Where to Capture?  TestYourVoIP.com
Wireshark  Common Sip Problems  HoverIP
Load Wireshark  Will it ever work?  NSLookup
Network interface setup  What else can you do?  Using the NET to find answers
Wireshark - Basic Layout  Common SIP/VoIP Problems  The SIP Wiki

Common SIP/VoIP Problems
4xx — Client Failure Responses
5xx — Server Failure Responses
6xx — Global Failure Responses
More SIP Testing Tools
SIP Scenario
SIP Scan
TestYourVoIP.com
HoverIP
NSLookup
Using the NET to find answers
The SIP Wiki
SIP and Unified Communications

Module times
- Running time = 45 minutes
- Quizzes = 7 minutes
- Total = 52 minutes

SIP and Unified Communications shows you how SIP underpins all the elements of Unified Communications to realize efficiencies that a successful implementation promises to business.

Topics Include

- Communication Breakdown
- XML
- Why SIP?
- Centralized conferencing
- SIP Clients
- Tuples
- Centralized Signalling
- Example Presence doc with
- Tuples (using a Mobile Phone)
- Centralized Mixing (optional)
- Rich Presence
- Centralized Authentication
- The METHODS in Action
- B2BUA (Discussed in core module)
- PUBLISH STATE
- Conference Components
- PUBLISH and PIDF/XML body
- The Focus
- SUBSCRIBE METHOD
- More IMPP work
- 202 OK Response
- SIMPLE
- NOTIFY
- More IMPP and CPP
- MESSAGE
- The Background Stuff
- Add A Buddy/Subscribe
- The IMPP working group
- is-composing
- IMPP and CPP
- Alternative ‘Presence States’
- More IMPP work
- 2 Places at the same time
- SIMPLE
- Conferenceing
- How it all works
- What SIP does in Conferencing
- Presentity
- INITIATE a conference
- More than one Focus
- JOIN a conference
- Conference Setup
- LEAVE / EXIT a conference
- iscomposing in Conference
- INVITE other participants
- NOTIFY
- Conference Components
- REFER conference server to invite
- The Focus
- or others to join
- Conference Components
- EXPEL participants
- The Focus
- CONFIGURE the media stream
- The METHODS in Action
- CONTROL a conference
- Why SIP?
- SDP BODY OF INVITE
- Centralized conferencing
- IETF work and Conferencing
- SIMPLE and/or XMPP
- XMPP v SIP/SIMPLE
- Gateways
- What is XMPP?
- Federations
- What is Federation?
- Multiple Presence sources
- Super-Aggregation
- Inter-Domain Federation
- RFCs Galore

2 places at one time
Presentity and more!
A Basic SIP Subscription
Multiple Presence States
Presence and P2P
A Presence Network
Getting inside the SIP packets
2 places at one time
Presentity and more!
A Basic SIP Subscription
Multiple Presence States
Presence and P2P
A Presence Network
Get inside the SIP packets
The Packet Structure
PIDF Message Body
ENUM and DNS

Module times
- Running time = 20 minutes
- Quizzes = 7 minutes
- Lab – ‘Registering / Testing ENUM’ ~ approx 20 minutes
- Total = 47 minutes

ENUM (along with DNS) is developing into an essential protocol on SIP networks and its purpose is to assist in finding destination SIP devices from a single SIP address.

Topics:
- What is E.164?
- What is ENUM?
- Why ENUM?
- Call Routing and ENUM - Example
- Why are we using DNS?
- DNS and the Web
- The e164.arpa Domain
- Approved ENUM Delegations
- TIERS 0, 1, 2 and 3
- TIERS and Registrars
- DNS and AOR
- e164.arpa Domain in action
- Example - ENUM in the UK
- Address of Record
- Reseaux IP Europeens
- PSTN to SIP UA - Example
- The ENUM Query
- NAPTR Records
- DNS Response to an ENUM query
- Calls Flows
- PSTN to SIP UA – Example (2)
- IP to PSTN (Simplified)
- Different ‘Types’ of ENUM
- The Problems with ‘Public’ ENUM
- Example – ‘Private’ ENUM
- Example – ‘Operator’ ENUM
- A few providers
- SIP User agent and ENUM
- Register your number
- Testing ENUM
- How is ENUM moving forward?
- Useful Links