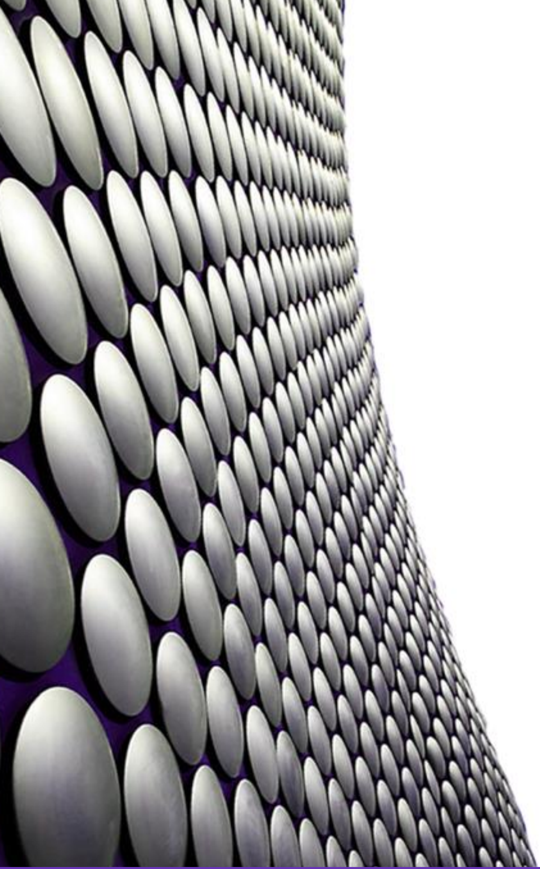


orchid link

Session Border Controller

Technical Data Sheet

Build Your Own SBC

One Platform – Any Use Case

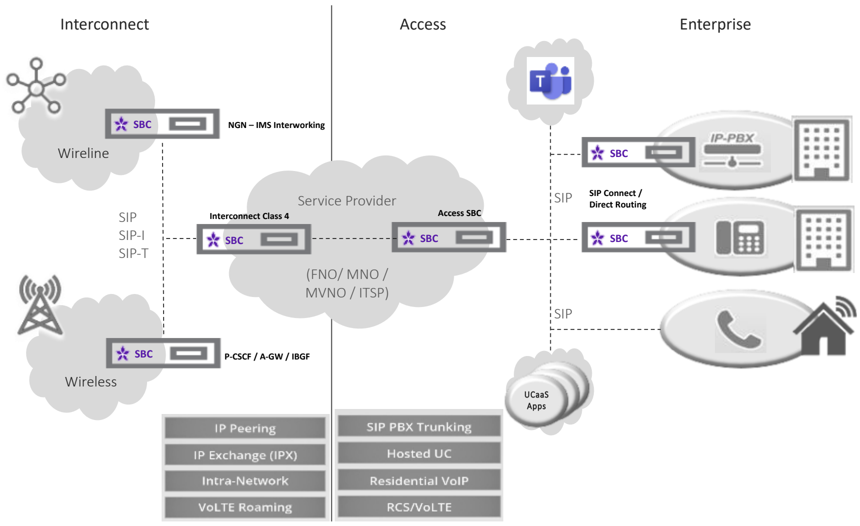
Cataleya's Orchid Link is a fully-featured, all-in-one Session Border Controller for those seeking to deploy outstanding technology in a simplified and cost effective manner.

The software-based platform enables you to build a reliable voice network on COTS servers, and supports a variety of deployments on bare-metal and virtualized environments, including NFV. This also allows for unlimited scalabilty across various deployment sizes. Thanks to the versatility of Orchid Link, it can be deployed across a wide variety of business use cases and networks be it Access or Interconnect function, deployed in NGN or IMS networks, Enterprise / Retail or Wholesale Service Provider use cases.

Rich features and reliable performance aside, you will benefit from the deep analytics and powerful diagnostics tools that is built into the SBC, giving you more control over your SLAs. A powerful & programmable Policy Engine ensures that your interworking & interoperability concerns are elegantly addressed.   A Building-Blocks based Service Management framework facilitates rapid building of new services, and gives you the edge with short time-to-market for rolling out new features to your customers. Our SBC Platform addresses all aspects of SIP based voice requirements and offers an easy-to use web portal for your team to manage the daily operation or fully integrate to your existing OSS and BSS systems via our rich set of APIs.

One SBC – Any use case

Orchid Link can be deployed as an Access and Interconnect SBC at the same time. A comprehensive feature set makes Orchid an ideal choice for different use cases like Enterprise SIP trunking service, Unified Communications as a Service (UCaaS), Service Providers and Enterprises using Microsoft Teams Direct Routing, Voice Wholesale, International Gateways, Domestic Interconnect Exchanges, Clearing Houses, IMS networks for VoLTE, and VoWiFi, NGN networks for TDM to IP conversion, and many more. All these functions are built on top of a wide range of platform functions like Policy Engine, rich Service Analytics, handy Diagnostic tools, and a Border Control function that secures service provider networks against security threats and attacks.



Access

- UCaaS / Hosted PBX
- SIP Trunk to MS-Teams
- WebRTC
- VoLTE / VoWiFi - IMS P-CSCF / A-GW
- Cloud Communication
- WebVoice APIs for Call Center Applications

Security

Security is the prime function of a Session Border Controller. Attacks to a VoIP network can happen anywhere from within the underlying network, transport protocols, VoIP devices, applications, underlying operating systems, and more. Orchid Link's security infrastructure ensures that system resources are always available for traffic from legitimate sources while blocking or mitigating attacks from rogue sources. Security features are built into each layer to thwart threats and protect against attacks. Orchid employs a Service Aware Firewall that runs on specialized & dedicated network processes that provides protection against L3 / L4 attacks. A SIP Application Gateway screens the traffic for malformed or malicious SIP messages. Features like TLS can be used for enhanced protection of SIP signaling.

NETWORK LAYER
- Service aware firewall with ACLs and L3, L4 protection measures
- Packet rate policing to mitigate DoS attacks
- Dynamic pinholes for RTP flows

SIGNALING LAYER
- Malicious/malformed SIP message handling
- SIP message flood handling
- TLS for SIP signaling
- ACL, Blacklist, GreyList, Trust Level
- Control Plane Policing
- SIP Protocol Validation

MEDIA LAYER
- Media delay detection
- Media inactivity detection
- Media encryption with SRTP
- RTP Policing

SESSION LAYER
- Dynamic black listing
- B2BUA provides topology hiding
- Allow sessions from configured endpoints
- Machine-learning fraud detection

MANAGEMENT LAYER
- Secured using TLS (HTTPS) with self signed certificates
- Advanced role based user management and authentication
- User action audit

There are protection mechansims in place to detect Media delays and inactivity, and a possibility to encrypt Media packets with SRTP. The Session Layer provides mechansims like topology hiding, and Call Admission Control to ensure controlled traffic flow to the SBC, and has means to dynamically blacklist erring interconnects.

Service Analytics

Providers of wholesale voice, IPX, Interconnect carrier, and ITSP services face several challenges such as lack of visibility, adapting to changes in the network and traffic, predictability and consistency in delivering real time voice, video, and multimedia services over IP networks. Orchid Platform Analytics and QoS feature provides necessary functionality and tools to address the issues prevalent in IP networks. Orchid's Service Analytics ensures that our customers get rich insights into both the Operations and Business aspects of their deployments from deep data analysis on signaling and media packets. It also provides comprehensive reporting to help the customers get complete visibility of their network and service.

Orchid's Analytics provides the following:

- 360 degree real time insights in to all aspects of the service and network
- Proactive SLA monitoring, alerting
- Intelligent session steering (self-healing) and SLA enforcements
- Trending and service consistency measurement
- QoS and QoE dashboards

Interconnect

VoLTE peering | IMS IBCF / TrGW | International Gateways

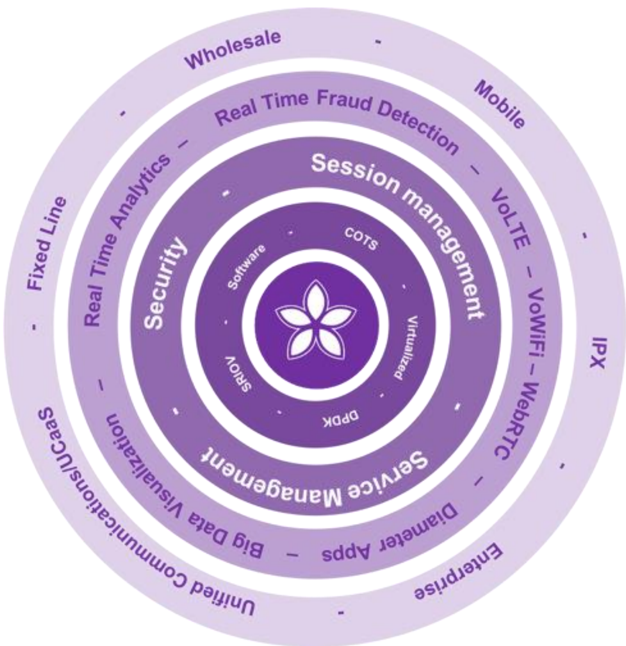
IMS-NGN interworking | Wholesale

Carrier-grade performance and scale on COTS

Cataleya's Orchid SBC is designed to keep network transformation, open source innovation and multi-vendor environment at the forefront. The SBC can be deployed on commercial (COTS) hardware servers for higher density centralized models or a virtualized instance which fits into different orchestration models for elastic scalability and flexibility in distributed models. Orchid is designed to run on cloud with high performance networking capabilities, real-time applications such as voice and video demands high performance network I/O capabilities:

- higher packets-per-second processing
- lower latency and jitter

Orchid achieves these with the use of intel 82599 vIF and AWS ENA drivers that use the SR-IOV technique to virtualize the network interface. Along with DPDK FastPath, these provide Orchid high throughput, low latency and jitter, thereby increasing the session capacity while ensuring voice quality.



TECHNICAL SPECIFICATIONS

Media Support

- G.711, G.723.1, G.726, G.729.1, G.722, G.722.1, G.729 AB, AMR, SILK, Opus
- H.264, H.265, VP9
- T.38
- Narrowband and Wideband codecs
- Transcoding & Transrating
- Tonal conversion from in-band in the input to RTC2833 in the output
- RTP inactivity detection, RTCP report
- Media NAT

Total Visibility Package

- Near real-time and trending visibility into Media QoE
- R-factor, MOS scores – one way and two-way paths
- Periodic and on-demand MOS score calculations
- Security threats and mitigation reports – near real-time and trending
- System and application performance
- Network traffic in and out – packet types, rates, counts
- Session KPIs – ITU and I3
- SLA monitoring – near real-time and trending, accepted
- SLAs and current SLA adherence levels
- Big Data-based analytics for prediction models
- Business intelligence tools built-in for business/ operational insights

Security and Privacy

- Service aware firewall with ACLs and L3, L4 protection measures
- Packet rate policing to mitigate DoS attacks
- Dynamic pinholes for RTP flows
- Malicious/ malformed SIP message handling
- SIP message flood handling
- TLS for SIP signaling
- Media delay detection
- Media inactivity detection
- Secure RTP (SRTP) for media encryption
- Dynamic blacklisting
- B2BUA provides topology hiding
- Allow sessions only from configured IP address / subnets
- Management access secured using TLS (HTTPS) with self-signed certificates
- Advanced role-based user management and authentication
- User action audit

Interconnect SBC capabilities

- Carrier-grade, high-performance switching with rich service analytics & Fraud detection
- Software-based transcoding
- Flexible and efficient Routing Policies, including QoS-based routing
- Exhaustive & powerful rule-based framework for SIP Header & Call-flow repair
- Ability to define flexible Transparency profiles (per-trunk) to allow for controlled topology hiding
- IMS I-BCF, I-BGF
- Peering and protocol-interworking capabilities, supporting IMS/NGN, SIP-I/SIP-T, IPv4/v6
- Lawful Intercept (LI) support
- Flexible CDR customization and formatting
- Single and Central Management server managing / monitoring multiple sites and nodes
- Network-wide licensing for increased savings and improved license utilization

Policy, Routing and Service Core

- Call Admission Control at Node, Partition, & Trunk level
- Policy -based rules engine – intelligent decision tree
- Exhaustive parameters analysis and manipulations – Digits, URI, SIP IEs
- Protocol parameter-based call routing
- Custom and derived parameter-based routing
- Support for directories/route lists
- Real-time QoS based routing
- LCR based routing
- Interface with external SIP 3xx redirection servers
- Pre-paid billing systems integration either through Diameter, JSON or REST API

Diagnostic Tools

- SDR Viewer (Call / Media / Routing information on each completed call)
- QoS Analysis (Media Stream statistics, R-Factor and MOS Scores, Call Quality Degradation reason and ranking)
- Active Calls / Registrations Monitoring
- Test Call feature
- Proactive "Always-On" SIP Protocol tracing
- Criteria Based call tracing across all the nodes in the network

Protocols supported

- IPv4, IPv6, IPSEC
- TCP, UDP, TLS, RTP, RTCP, SRTP
- SIP, SIP-I, SIP-T
- DNS, ENUM
- SNMP, NTP
- SSH, sFTP
- Diameter, RADIUS
- HTTP / REST, JSON, SOAP, XML, RPC

TECHNICAL SPECIFICATIONS – Contd…

Access Capabilities	• SIP signaling and media NAPT – topology hiding and Media anti-tromboning • Software-based transcoding • Registration Caching, with prevention of Registration storms and Call Admission Control • Proactive QoS monitoring and alerting for SIP trunks • WebRTC gateway with SIP over WebSocks & DTLS • IETF SIPREC SIP recording interface to call recording systems • SIP Connect 1.0 support: Services-related SIP message handling to facilitate IPPBX features • Extendable service framework to support authentication-based interop using XML/RPC, RADIUS, Diameter, etc. • DTMF, Fax • IPSEC for signaling encryption and Mobile authentication, IMS-AKA support • IMS P-CSCF, AGW • Multi-tenancy: Ability to create logical SBC partitions as virtual SBCs (Independent SBC partition per enterprise) • MS-Teams Direct Routing support with certification from Microsoft • WebVoice Service APIs including Text-to-Speech function to play bulk announcements • Lawful Intercept (LI) support
Network Interfaces	• Management Interfaces (HTTP / REST, SFTP, SSH, SNMP) • HA Interface (towards the HA peer) • Traffic Interfaces (up to 4 x 1GE / 10GE ports) • VLAN tagging • Separated Data Plane with dedicated processors
Bare-metal Deployment	• COTS Servers: Dell, SuperMicro, and HP servers • 1,000 – 70,000 Concurrent calls • 100 – 2000 CPS • 500 – 10,000 SRTP Sessions • 10,000 – 200,000 Registered Endpoints • Minimum 6 Core CPU / 32 GB RAM / 250 GB SSD • Additional (up to 4 ports) 1G / 10G Traffic NICs (according to required capacity) that supports DPDK packages
VM Deployment	• KVM, VMware - Minimum 4 CPUs, 16 GB RAM, 200 GB Storage • AWS – Minimum c4.large, 4 CPUs, 7.5GB RAM • Up to 10,000 concurrent SIP sessions per instance • Up to 200 SIP sessions / Calls per second (CPS) per instance • Up to 10,000 RTP/RTCP media flows, and TLS SIP sessions per instance • Up to 3,000 SRTP sessions per instance • Up to 64,000 registrations, and 2,000 registrations per second per instance
Billing	• CDR/MDR generation with standard and custom – fields for calls and media related information • XML based CDR field selection, ordering and format • Selection to comply with the back end – billing mediation system • Over 300 columns of call and network quality evaluation for each call – highly customizable
Management System	• Alarms – standard and user defined • SNMP based trap generation • Intuitive configuration management • Web-based near real-time analytics and reports • Real-time call tracing (signaling and media) and monitoring • Role-based user access • Software upgrades and version management • NTP support • Backup and restore • Central Management of multiple nodes across the network (CMS) • Separated FCAPS and Analytics (CMS-Plus) for managing more nodes, and longer retention of Billing and Analytics Records

For more information, contact us at **info@cataleya.com**

Update Apr 2021

cataleya

Redefining flexibility