COMPOSE

ekinops
Empowering Networks

DATASHEET

OneOS6

Operating System for Physical CPEs and VNFs

OneOS6 is the next-generation software for the Ekinops' ONE products. Its modern architecture separates and distributes management, control and data planes in processes running in parallel. As a result, OneOS6 delivers market-leading packet switching throughput and latencies with an entirely software-based technology.

The management plane relies on a unified object-based framework using the Yang modelling language. The framework is a future-proof design to ease future integration within SDN orchestration systems. In addition to this breakthrough technology, OneOS6 management interfaces are aimed at providing a smooth migration for OneOS5 customers. This datasheet includes the data, voice and management features of OneOS6.10.

Interface Characteristics

The definition of an "interface" on equipment entirely depends on the configuration of the unit and can correspond to the following:

- A physical interface, e.g. an Ethernet interface, an EFM interface, a DSL interface, etc.
- A VLAN
- A Tunnel
- An PPP dialer interface
- A virtual Ethernet

Every interface above supports all IP and Bridge services and can provide its IP address for management services. It can also include voice interfaces to connect on-premise legacy devices:

- An analog interface: FXS, FXO
- A digital interface: PRI, BRI

WAN Protocols

PPP& PPPoE

- PPP (RFC1661, 1662)
- Link Control Protocols BCP (RFC3518) and IPCP (RFC 1332, 3242)
- Authentication protocols PAP (RFC1334) and CHAP (RFC1994), unidirectional and bidirectional
- PPPoE (RFC2516)
- PPPoE with VLANs, ATM and Ethernet traffic

EFM

- Ethernet in the First Mile (IEEE 802.3)
- Over the available media (DSL, Fiber)

ATM

- PVCs with VCI/VPI configuration
- CBR, UBR a VBR QoS
- AAL5 multiprotocol (RFC2684)
- VC based multiprotocol: IPoA (RFC1577), PPPoA (RFC2364), IPoPPPoEoA
- ATM OAM

LAG/LACP

- Link Aggregation (LAG/LACP) according to IEEE 802.1ax (formerly 802.3ad)

Ethernet OAM

- Link OAM IEEE802.3ah: discovery and remote loopback
- Ethernet OAM 802.1ag & Y.1731: CC, LB, LT, AIS, RDI, DL, LM, SLM

IP Services

The IP router complies with the router requirements from RFC1812 and supports the routing of standard IP packets (RFC791) between the different interfaces on the device. Common router features for IPv4 and IPv6 are:

- ARP and proxy ARP
- Static IP address assignment
- Path MTU discovery
- Loopback interfaces
- Configurable MTU
- Equal Cost Multi-Path Routing (ECMP): load sharing over routes with equal cost and distance
- ECMP Least Load First *
- ICMPv4 and ICMPv6 (RFC4443) error management

IPv4 Specific Services

- Variable Length Subnet Mask (VLSM - RFC1878) (IPv4)
- Classless Inter-Domain Routing (CIDR)
- TCP Maximum Segment Size (MSS) Clamping
- IP helper address
- BootP (RFC951) & DHCP server (RFC2131, 3132) with static or dynamic address assignment
- DHCP relay agent
- Static IP & PPP IPCP address assignment
- BootP & DHCP client
- DHCP options for server and client side
- Secondary IP addresses
- DNS client and proxy, DynDNS

Operating System for pCPEs and VNFs

IPv6 Specific Services

- DHCPv6 stateless (RFC3736) and stateful (RFC3315) server
- DHCPv6 relay agent
- DHCPv6 stateless and stateful client
- DHCPv6 prefix delegation
- DNSv6 client and proxy
- Use of prefix name

IPv4 Network Address Translation

- Compliant with RFC 3022
- NAT mode for one-to-one private to public IP address translation
- PAT mode for many-to-one private to public IP address translation (also called port mapping, single address NAT or NAPT)
- NAT/PAT configurable on any interface (the interface with the public address(es)
- Twice NAT
- Static NAPT on port range
- TCP/UDP server load balancing
- Easy NAT: self learning of overloaded IP address
- Selective NAT (translate only traffic matching access lists) and NAT bypass (translate all except traffic matching ACL)
- Application Layer Gateway (ALG), FTP, SIP, NetBIOS, GRE
- Session limiting, Denial of Service protection

IP Filtering and Firewall

- Firewall is based on advanced access-list functions
- Firewall policies attached to interface inbound/outbound direction
- Access lists can be attached to internal server applications (SSH, telnet...)
- IP extended access lists filter on the following parameters:
  - Source IP address range
  - Destination IP address range
  - Type Of Service (TOS) value range (8 bits in the IP header, also called DSCP bits)
  - IP protocol
  - Source port range for UDP / TCP packets
  - Destination port range for UDP / TCP packets
- Stateful inspection firewall
  - TCP, FTP
  - Half open session management
  - Rule logging
  - Detection of malicious IP
- Reflexive filters
- Reverse path check
- Zone-based Firewall *
- DDoS protection
- NAT64 and NAT46

IP Routing

This section applies to both IPv4 and IPv6 routing unless explicitly mentioned. Some protocols obiously apply only to either IPv4 or IPv6.

Several routing protocols are available. The routes are selected in the Routing Information Base by discriminating metric and administrative distance of every route. The following routing features are available:

Static Routes

Routing is based on static routing entries in the routing table. Alternate routing is possible through the use of different administrative distance for different routes to the same destination.

Route Tracking

A performance measurement probe can be associated with a route. If the probe considers that certain performance objectives are not met, the associated static route is disabled.

Virtual Routing and Forwarding (VRF)

Virtual routing and forwarding or VRF allows a single router to use multiple routing tables. The main benefit is enhanced VPN support. Multiple customers can now be connected to a single device without address collisions, as they each have a separate routing table assigned to them.

Network paths can be segmented without using multiple devices. Traffic is automatically segregated, i.e. prevented from being forwarded outside a specific VRF path, and traffic that should remain outside the VRF path is also kept out. As a result, VRF increases network security and may eliminate the need for encryption and authentication. For specific conditions, route leakage between different VRFs can be achieved through the use of VASI interfaces.

Policy-based Routing

Normal routing is based on the destination IP address. Policy based routing offers the possibility to define different routing entries based on additional higher layer information. Traffic is routed to a certain interface or gateway based on one or more of the following parameters:

- Source and destination IP address range
- Type Of Service (TOS) value range (8 bits in the IP header, also called DSCP bits)
- IP protocol
- Source and destination port range for UDP / TCP packets

RIP

- RIPv1 (RFC1058) & RIPv2 (RFC2453) for IPv4
- RIPnG (RFC2080) for IPv6
- Split horizon and selective router updates per interface
- RIP2 authentication with MD5 hashing or clear text
- Triggered RIP for ISDN interfaces
- Route Distribution list (prefix-list, ACL)
- Redistribution of routes: default, static, connected, BGP, OSPF
- Route redistribution filtering with route maps
- Validation of update source can be de-activated

OSPF

- OSPFv2 (RFC2328) for IPv4
- OSPFv3 (RFC2740) for IPv6
- Route summarization and route suppression through range definitions on areas
- OSPFv2 encryption through simple password or MD5 encryption chains
- OSPFv3 authentication/confidentiality (RFC4552)
- Stub areas, OSPF NSSA (RFC 3101)
- Virtual links

Operating System for pCPEs and VNFs

- Opaque LSAs (RFC2370)
- Cost tuning
- RFC1583 compatibility option
- MTU check override
- Overflow management
- Redistribution of routes: default, static, connected, RIP, BGP
- Route redistribution filtering with route maps

BGP4

- Border Gateway Protocol version 4 (RFC1771)
- Interior and exterior BGP (iBGP & eBGP)
- Authentication (RFC2385)
- Multipath load sharing
- eBGP multi-hop
- Peer groups
- iBGP configurable source address
- Tuning of BGP routing criteria
- Redistribution of routes: default, static, connected, RIP and OSPF
- Routing filtering on ingress and egress
- Route filtering with ACL, AS path filters with regular expressions, route maps with community lists, AS paths, local preference settings
- Allow AS Loops
- Backdoor routes
- AS confederations (RFC3065)
- Route reflectors (RFC2796, 4456)
- Flap dampening (RFC2439)
- BGP capacities advertisement (RFC3392)
- BGP graceful reset (RFC4724)

Bidirectional Forwardin Detection (BFD)

- BFD neighbor binding with static (VRF) routes
- Multihop BFD (RFC5883)
- Synchronous and asynchronous modes

VRRP

- Virtual Router Redundancy Protocol in accordance with RFC 3768
- Multiple VRRP instances
- Priority adjusted based on critical interface status or route presence monitoring

Multicast Routing

- IGMPv1/v2/v3 for IPv4 (Internet Group Management Protocol, RFC 2236, RFC4604)
- MLDv1/v2 for IPv6 (Multicast Listener Discovery, RFC3810, RFC4604)
- Static multicast routes
- PIM-SM (Protocol Independent Multicast – Sparse Mode) version 2 (RFC2362, RFC4601, RFC7761)

Bridging and VLANs

Bridging

- Multiple configurable bridge groups
- Configurable MAC learning
- MAC relearning options
- Policy based bridging
- MAC address filtering and Access lists (ACL)
- Layer 2 access lists (ACL) filter on source & destination MAC addresses, Ethernet type, VLAN ID and number of VLAN tags, TPID, COS & DEI bits
- Can be combined with IP access lists
- ACLs are attached to an interface in inbound or outbound direction
- Configurable private interfaces
- Broadcast, Multicast and unknown Unicast bandwidth control
- Bridge Virtual Interfaces (BVI) link the Bridge with the IP router
- Spanning Tree Protocols STP (802.1d), RSTP (802.1w) and MSTP (802.1s)
- BPDU filtering and guard
- IGMPv2 snooping
- LLDPv2 - IEEE802.1ab

VLANs

- 802.1q/p
- Single and double VLAN tagging/untagging on interfaces
- Configurable TPID & COS at VLAN tagging
- QinQ and 802.1ad

Tunneling and VPNs

Tunneling

- Generic Routing Encapsulation (GRE, RFC1701, RFC2784)
- IPv4/v6 GRE with IPv4, IPv6 and Ethernet payloads
- 6in4 tunnels (Dual Stack over IPv4 GRE tunnel)
- isatap tunnel (IPv6 over IPv4 GRE)
- Layer 2 Tunneling Protocol: L2TPv2 (RFC2661) & L2TPv3 (RFC4719) *
- IPv4 L2TPv2 with IPv4 payload
- IPv4/v6 L2TPv3 with IPv4, Ethernet and VLAN payloads
- IPv4 in IPv4 tunnels
- Next Hop Resolution Protocol (NHRP) client and server (RFC2332) **

IP Security (IPsec)

- Compliant with RFC4301 and succeeding
- IPsec transport mode for IPv4, GRE and L2TP (RFC3193)
- IPsec tunnel mode for any IPv4/IPv6 combination
- Authentication Header (AH - RFC4302)
- Encapsulation Security Payload (ESP - RFC4303)
- Use of crypto maps with ACL & SA traffic selectors (aka proxy-id) with IKEv1
- Use of IPsec profiles with IKEv1 & IKEv2
- IKEv1 (RFC2412) main (RFC2367) and agressive modes
- IKEv2 (RFC4307, RFC7296)
- IKEv2 fragmentation (RFC7383)
- Encryption algorithms AES-CBC (RFC3602), AES-GCM (RFC4106, product dependent), 3DES, DES
- Hash algorithms SHA-2, SHA-1, MD5
- IKE authentication with pre-shared keys and RSA certificates (X.509)
- Dead Peer Detection (DPD, RFC3706)
- NAT Traversal (NAT-T, RFC3947, RFC3715, RFC3948)
- Reverse Route Injection (RRI) with IKEv1
- Easy VPN client with X-AUTH, MODE-CFG
- Easy VPN server with X-AUTH, MODE-CFG support *
- Dynamic Virtual Tunnel Interfaces *
- IPsec Group Mode **
- IKE with redundant peers

Operating System for pCPEs and VNFs

Quality of Service (QoS)

Quality of Service (QoS) can be enabled on any input and output logical interface. At the input it is possible to classify packets and mark them with DSCP/precedence value and apply policing. At the output, the same processing is possible as well as traffic shaping and congestion avoidance.

Classification Criteria

- Access-lists
- Input interface
- Application
- RTP
- DSCP / precedence
- 802.1p tag
- Virtual QoS group

Marking

- DSCP / precedence
- 802.1p tag
- Virtual QoS group
- Reflexive DSCP marking

Traffic Conditioning (Policing)

- Per traffic class, Committed Information Rate (CIR), Peak Information Rate (PIR) and Burst Size are configurable
- CIR/PIR absolute and relative (as percentage of interface rate) values
- Forward, mark and drop actions on conform / exceed / violate conditions

Traffic Shaping

- CIR & remaining bandwidth distribution configurable
- Low latency Queuing (LLQ) with absolute priority for real-time classes. Maximum latency configurable
- Weighted Fair Queuing (WFQ)
- Configurable queue size
- RED & WRED congestion avoidance, based on DSCP, precedence, COS; ECN
- Hierarchical queuing
- Host-based Weighted Fair Queuing *

DiffServ

- DiffServ is a specific QoS use case for IP traffic (RFC2474, 2475, 3168, 3260) with traffic classification based on TOS values
- DiffServ Assured Forwarding (AF - RFC2597)
- DiffServ Expedited Forwarding (EF - RFC2598)

Application Aware Traffic Steering

- Deep Packet Inspection (DPI) for UDP/TCP protocols
- NetFlow v9 for export traffic flow info
- Traffic Identification and Classification (TIC) based on external database **
- Application aware traffic policing and shaping
- For IPv4/v6 traffic

Service Level Agreements (SLA)

Performance probing is an application to measure network performance. It helps to monitor the health of your network.

- IP SLA based on ICMP & UDP echo, any UDP port packets
- Initiator and Responder sides
- TWAMP & TWAMP light (RFC5357) initiator* and responder
- Measurement of roundtrip delay, one way jitter and loss
- History filtering and storage

Voice

Analog Interface Features

- Incoming / outgoing calls
- FXS Line Voltage Drop
- Direct call (automatic call after off-hook)
- Fully configurable ringing & tones
- FSK/DTMF caller-id presentation on POTS terminal interface
- FXO Loop-back & ground-start
- FXO far end disconnect supervision
- Line Hunting, Local port switching
- Services: Hold, Retrieve, Brokering, Call Transfer, 3-PTY

ISDN Interface Features

- Incoming / outgoing calls
- PRI VN4/6, ETSI, NI2, 5ESS, DMS100
- BRI NT (Network) / TE (Terminal)
- Force ISDN layer-2 activity
- ISDN Permanent layer-2 & layer-1
- ISDN channel specialization
- Line Hunting, Local port switching
- Services: Hold, Retrieve, Suspend, Resume, Restart, Call Transfer, 3-way Conference
- ISDN header insertion / suppression
- ISDN PRI with CNAME

SIP

- Geo-localization: NAPTR, DNS-A, DNS-SRV
- SIP 2.0 over UDP/TCP/TLS and RTP/SRTP
- Support of VRF & VLAN
- DSCP marking
- SIP Registration (basic, 3GPP method) for Trunking and Hosted solutions
- SIP Authentication
- DTMF in-band (RFC 2833) and out-band (SIP INFO)
- SIP call routing based on Request URI, P-Called-Party-ID and To fields
- Join an External Conference Bridge
- Join an External Voice-mail
- Configurable SIP timers
- Allow discard of 3XX message
- Support of Trunk Group as per RFC 4904
- Support of SIP User Agent header
- Support for SIP multi-trunks with different IP addresses, ports & settings
- SIP Session Timer according to RFC4028
- Emergency calls
- SIP NAT ALG (UDP and TCP)
- SIP redundancy, survivability & fail-over
- SIP monitoring via OPTIONS method
- Automatic call disconnection on no RTP flows
- Configurable automatic device reboot on SIP NOTIFY reception

Session Border Controler (SBC)*

- SIP proxy for both Centrex (hosted) & B2BUA solutions
- Registration: Two-step & transparent
- Certified Microsoft Teams Direct Routing
- SIP Server Registration
- Local SIP Authentication (401/407)
- Basic calls, Hold, Retrieve, Suspend, Resume, Call Forward, Call Transfer, Message Waiting Indication
- SIP Message Interception for Centrex solution

Operating System for pCPEs and VNFs

- Media negotiation: End-to-end, Per-leg
- CDR generation per SIP leg
- Media transcoding: G.711 (a/μ law), G.729ab, G.722, AMR-WB(G.722.2), SILK, CES configurable
- DTMF/FAX transcoding
- Anti-tromboning feature
- Support for Video (H.262, H.263, H.264) codecs in transparency mode

Voice Security

- SIP Anti-Flooding Mechanism
- Topology hiding
- SIP message filtering
- Address translation
- SIP Lawful Interception (outbound proxy)
- SIP Lawful Interception (ACL)
- Traffic separation
- Hosted NAT transversal

Voice Routing

- Selection of voice processing
- Call routing, Pre and Post Routing
- Call backup
- Numbering plan management, Insertion & suppression of digits
- Call Admission and Control
- Gateway Intrusive mode
- Intrusive voice-port
- Dialer watch list
- Inline Test Calls
- Configurable Test Calls

VoIP Processing

- Voice compression: G.711 (a/μ law), G.729ab, G.722, AMR-WB(G.722.2), SILK, CES configurable
- Codecs with static & dynamic payload
- Packet length
- DTMF detection and generation
- Echo cancellation: G.165/168 compliant, non-linear processing
- Adaptive jitter, packet loss concealment
- Country specific tone generation and customization
- Silence suppression and comfort noise generation
- MOS scoring evaluations
- Fax pass-through, T.38 ECM & Modem over IP
- VAD/CNG

Voice Quality

- RTCP-XR report
- RTP extended statistics (loss, jitter, voice quality diagnostics)
- MOS-LQ / MOS-CQ calculation
- R factor display
- VQM (Voice Quality Monitoring) report
- Voice statistics

Voice Interoperability

- SIP Header Manipulation
  - SIP messages tuning
  - Update/Replace URI format in SIP header fields
- SIP Connect 1.1 / 2.0
- Interworking PSTN/SIP
  - COLP, COLR
  - CLIP, CLIR
  - MCID, SUB, MWI, UUS, CW
  - AOC TISPAN
  - SIP return-code & q850-cause conversion

Device Management & Monitoring

Management and Management Tools

- Industry-standard Command Line Interface (CLI)
- Local console
- SSHv2/telnet server with command line
- SSHv2 authentication with password (client), keys and certificates
- SSHv2/telnet client
- Embedded web server (HTTP(S), RFC2068)
- Customizable web GUI
- SNMPv1 (RFC1157), SNMPv2 (RFC3416-3418), SNMPv3 (RFC3413-3415)
- SNMP MIB2 (RFC1213), private MIBs
- SNMP standard traps (RFC1215)
- SNMP views & groups
- CWMP (TR-069) based provisioning and firmware update
- CWMP TLS support (HTTPS)
- TR-111: TR-069 pass-through behind NAT with STUN
- Zero Touch Provisioning (ZTP)
- DNS failover for CWMP, ZTP
- TFTP, FTP, SFTP, HTTP client for file transfer
- SCP, TFTP server for file transfer
- Syslog event logging (RFC3164)
- Mutual TLS certificate authentication for syslog, NetConf, Netflow, ZTP, web server, CWMP and SIP-TLS
- Simple network Time Protocol client (SNTP/NTP, RFC2030)
- SNTP/NTP server with configurable parent NTP server address (RFC5905/4330/2030)
- Ping (RFC792) and traceroute with extended options
- Protocol tracing
- Event and trace storage in local memory or file, forwarding to syslog server or console port
- Alarm framework
- Embedded Event Manager
- Object tracking
- Historical statistics (2h, 24h, 7 days) for interfaces
- Interface packet capturing and decoding
- NETCONF v1.1 and call home (without reverse SSH)
- NETCONF over SSHv2 and over mTLS
- Dual software image allows secure firmware upgrades
- Recovery of last working configuration

Operating System for pCPEs and VNFs

Security

- The devices are password protected for access through the different maintenance and management tools. Each user can be given customized access-rights.
- One can enable/disable all management access to the device per interface
- Overall access for specific management tools can be prohibited (e.g. telnet, SSH, SNMP, HTTP ...)
- RADIUS (RFC2138/2139) for authentication
- TACACS+ (RFC1492) for authentication, authorization and accounting
- User access logging (successful and failed logins)
- User login blacklisting for telnet/SSH
- Certificate management (RFC4809) with trust-points: SCEP, Certificate import with HTTP, pkcs12 format support, CRL management, auto-enrollment
- Internet X.509 Public Key Infrastructure (PKI) (RFC5280)
- 802.1x authentication on Ethernet interfaces
- Secure software upgrade (optional)
- Trusted Platform Module (on selected hardware)

* *Subject to a separate license*
** *With SD-WAN license*

OneOS6 Products

Product	Product Type	Data support	Voice support
ONE421	Physical Router	Yes; ACS & SD-WAN licenses available	eSBC, license available
ONE521	Physical Router	Yes; ACS & SD-WAN licenses available	eSBC, license available
ONE526	Physical Router	Yes; ACS & SD-WAN licenses available	Voice; eSBC license available
ONE531	Physical Router	Yes; ACS & SD-WAN licenses available	eSBC, license available
ONE1526	Physical Router	Yes; ACS & SD-WAN licenses available	Voice; eSBC license available
ONE2501	Physical Router	Yes; throughput, ACS & SD-WAN licenses available	eSBC, license available
ONE2511	Physical Router	Yes; ACS & SD-WAN licenses available	eSBC, license available
ONE2515	Physical Router	Yes; throughput, ACS & SD-WAN licenses available	Voice; eSBC license available
ONE2520	Physical Router	Yes; ACS & SD-WAN licenses available	eSBC, license available
ONE2540	Physical Router	Yes; ACS & SD-WAN licenses available	eSBC, license available
ONE2560	Physical Router	Yes; ACS & SD-WAN licenses available	eSBC, license available
ONE2561	Physical Router	Yes; ACS & SD-WAN licenses available	eSBC, license available
ONE3540	Physical Router	Yes; throughput, ACS & SD-WAN licenses available	No
ONE-5G	Physical Router	Yes; ACS & SD-WAN licenses available	eSBC, license available
ONEVOIP16	Voice Gateway	No; no data licenses	Voice; eSBC license available
ONEVOIP30	Voice Gateway	No; no data licenses	Voice; eSBC license available
ONEVOIP120	Voice Gateway	No; no data licenses	Voice; eSBC license available
1647	EAD	Yes; routing, ACS & SD-WAN licenses available	No
1651	EAD	Yes	No
ONEv600	VNF	Yes; throughput, ACS & SD-WAN licenses available	No
ONEvSBC	VNF	No; no data licenses	eSBC license required
OneOS6-LIM	OVP	Yes; throughput, ACS & SD-WAN licenses available	No

About EKINOPS

Ekinops is a leading provider of open, trusted and innovative network connectivity solutions to service providers around the world. Our programmable and highly scalable solutions enable the fast, flexible, and cost-effective deployment of new services for both high-speed, high-capacity optical transport as well as virtualization-enabled managed enterprise services.

Our product portfolio consists of three highly complementary product and service sets: EKINOPS360, OneAccess and Compose.

- EKINOPS360 provides optical transport solutions for metro, regional and long-distance networks with WDM for high-capacity point-to-point, ring, and optical mesh architectures, and OTN for improved bandwidth utilization and efficient multi-service aggregation.
- OneAccess offers a wide choice of physical and virtualized deployment options for Layer 2 and Layer 3 access network functions.
- Compose supports service providers in making their networks software-defined with a variety of software management tools and services, including the scalable SD-WAN Xpress and SixSq Edge-to-Cloud solutions.

As service providers embrace SDN and NFV deployment models, Ekinops enables future-proofed deployment today, enabling operators to seamlessly migrate to an open, virtualized delivery model at a time of their choosing.

A global organization, Ekinops (EKI) - a public company traded on the Euronext Paris exchange operates on four continents.

EKINOPS360 Dynamic Optical Transport

COMPOSE

ONEACCESS Fast Network Virtualization

marketing@ekinops.com | www.ekinops.com