The Ensemble Network Controller (ENC) is a service aware network controller and management system. ENC is equipped with a powerful web-based graphical user interface as well as open northbound APIs.

As such, ENC supports three deployment models:
- A stand-alone service management system
- A network controller and service management system integrated into higher level management and provisioning systems
- A complete NFV management and orchestration (MANO) system when integrated with Ensemble Service Orchestrator and cloud controller

With native support for all Overture network elements, ENC is extensible to support third-party network elements. ENC automates device detection, fault management and performance monitoring. By presenting a complete network picture, CSPs can focus on adding new services and virtualized network functions without compromising existing network operations.

Overture’s Ensemble OSA™ is the industry’s first open architecture for software-defined services at the metro service edge. Within this domain, Ensemble OSA is a complete and open platform for service automation and network functions virtualization (NFV).

Comprising three logical layers and a number of independent components interconnected with open APIs, Ensemble OSA is designed to easily integrate into the architecture and workflow of any communication service provider (CSP) environment.

The orchestration and control layer includes three components – Ensemble Service Orchestrator (ESO), OpenStack Cloud Controller and Ensemble Network Controller (ENC) – that may be used together or independently based on a CSP’s needs.
Ensemble Network Controller

**NETWORK MANAGEMENT**

ENC brings the entire network into a single, simplified view. Every layer, service, network element and connection is managed from graphical, template-driven interfaces that present a deep and complete picture. APIs connect northbound interfaces so no device or service is left out. Users can setup automation rules based on specific criteria including software updates, performance monitoring and fault management to reduce errors and streamline maintenance. A complete, accurate view of the network frees operators up to focus on provisioning, service creation and service orchestration.

The level of service awareness visible through the ENC significantly reduces the time it takes to turn-up new revenue-generating services.

**SERVICE CREATION AND MANAGEMENT**

CSPs can accelerate service creation when they know where – and what – services are efficiently running on the network. ENC allows network operators to poll all elements, then correlate each device’s location with the services it’s running. The result is an unmatched level of service awareness.

With resources properly identified, CSPs can create and activate new services quickly and without interruption across their complex, multi-vendor landscape. Network operators can define E-line or E-LAN services on single network devices or across multiple locations through enhanced MEF templates. Services can be created in minutes, not in weeks or months.

**PERFORMANCE MONITORING**

ENC presents a complete view into the network health by gathering interface-level performance data at regular intervals. Service level performance is assured through a comprehensive set of Ethernet service-level SLA management tools, leveraging CE2.0 constructs. Archived on a server for easy access, users can graphically see statistics versus time to correlate anomalies or errors to customer issues. ENC also makes it easy to perform service activation testing to ensure that the network is provisioned to support the committed SLA.

**FAULT MANAGEMENT**

ENC elevates network management by reporting faults from each device or service throughout the network. Customized alarm filters and escalation policies help your people work smarter and faster, not harder. And, this helps CSPs intercept failures prior to customer calls about a service outage.

ENC can forward traps from network devices to northbound surveillance systems and filter unwanted tracks based on a fault source or persistence time. All fault events and alarms, including filtered child views, are documented in customizable reports. The ENC simplifies operations and reduces upstream monitoring costs.
### Ensemble Network Controller

#### SNAPSHOT
- Accelerate service creation, activation and assurance
- Automatically correlate services with hardware and location for complete service awareness
- Use simple, graphical templates to turn-up services in minutes, not in weeks or months
- Easily integrate using open northbound APIs
- Reduce OpEx by simplifying network management and enabling software upgrades network wide on existing elements
- Bring your entire network – hardware, locations and services – into a single pane of glass
- Integrate with Ensemble Service Orchestrator (ESO) and Cloud Controller for a complete NFV MANO
- Scales to tens of thousands of network elements

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>BENEFIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service-level Configuration and Visibility</td>
<td>From a single pane of glass, the CSP can create, activate and assure CE2.0 services. Service and network performance and faults can be correlated for complete visibility into the customer experience.</td>
</tr>
<tr>
<td>Open northbound APIs</td>
<td>Easily integrate into higher level management, OSS and BSS systems and third party network elements.</td>
</tr>
<tr>
<td>Graphical interface</td>
<td>ENC’s question-and-answer format feeds extremely simple graphical interfaces. Users can click a map to see device alarms, chassis configuration or to telnet into the local device OS. ENC templates reduce human errors and improper configuration changes to services and specific elements.</td>
</tr>
<tr>
<td>Complete device detection</td>
<td>ENC performs background scans across the entire network automatically detecting and adding new devices to the inventory using SNMP. It controls discovery on devices or entire subnets based on flexible user criteria and domain grouping at specifically defined intervals. ENC discovers chassis, cards and even services, regardless of the method used to provision them to a device. All inventory views can be shared, via post analysis tools, as CSV files.</td>
</tr>
<tr>
<td>Configuration management</td>
<td>ENC provides tools that capture every alert from every network device when configuration changes are made. This is particularly important when so many services are running at the metro service edge. ENC allows users to automatically save a date-stamped configuration of each network device to a specific FTP server. If the device fails, users can quickly identify needed steps to get it up and running. This greatly minimizes replacing the device and restoring configuration.</td>
</tr>
<tr>
<td>Network KPIs</td>
<td>ENC’s easy-to-read network summaries show an “at-a-glance” view of network availability and fault resolution statistics. Users can set thresholds for alerts based on user-defined criteria and access reports that show fault history by severity, type and those that generate the highest number of alarms.</td>
</tr>
</tbody>
</table>
TECHNICAL SPECIFICATIONS

SYSTEM REQUIREMENTS

RECOMMENDED MINIMUM SERVER HARDWARE
- Dual Intel XEON E5520 2.26GHz quad core processor, supporting 16 threads
- 65 GB RAM
- Tereebyte HD

SERVER SOFTWARE
- MySQL 5.x database
- Red Hat 6.5/6.6 or CentOS 6.6

DISCOVER
- Auto discover SNMP-based over IP address range
- Discovery over multiple networks
- Export discovered inventory to csv files

FAULT MANAGEMENT
- Alarm summary view
- Customized alarm views and filters
- Alarm annotations and pickup status

SOFTWARE MANAGEMENT
- Flexible queries to isolate target devices for upgrade
- Select single device, subset of devices or all for upgrade
- Manage device active and backup images
- Software repository on local or remote FTP server

CONFIGURATION MANAGEMENT
- Configuration stored on local or remote FTP server
- Archive on command or on scheduled basis
- Support for active and startup configurations

USER SECURITY MANAGEMENT
- Accounts and passwords can be time limited
- Group based permissions or direct assignment
- Audit logs of all access requests and responses

NORTHBOUND SNMP TRAP FORWARDING
- Definable trap list
- Reliable trap forwarding feature captures missed traps from device

SUPPORTED NETWORK ELEMENTS
- Overture 6500 Multiservice Aggregator
- Overture 6100 Multiservice Aggregator
- Overture 1400 Multiservice EAD
- Overture 65 EoF EAD
- Overture 400 EoC EAD
- Overture 4000 EoC Aggregator
- Overture 500 EoTDM EAD
- Extensible to 3rd party network elements