2016

EPIC 3

SDN CONTROL

SAURAV DAS

Table of Contents

Introduction

As a service provider, access technologies require a secure, scalable and resilient controller platform. These platforms will have the ability to control various subscriber based service flows running on a variety of network access technologies. When we define SDN controller behavior, we take the following points into consideration:

- Configure, control and manage the resources (infrastructure), services (network, subscribers and application) and state
- Closed loop control to maintain capabilities
- Uses platform services to implement, manage and modify controlled objects
- Responsible for the management, deployment, operation and coordination of L4-7 Services to ensure and maintain end-to-end performance objectives

Assumptions

- Instantiation, management, and control of VFs and PNFs within its scope
- Performs elastic capacity management of the resources within its scope
- Coordinates controllers to set up Service Chains
- Responds to exceptions within its scope
- Validates service before launching
- Runs a local, closed control loop that consists of Analytics, Policy and Orchestration
  - The scope of the control loop is restricted to resources under its control
- Shall meet requirements provided in the EPIC_COMMON.docx

Acceptance Criteria

- Meet the defined test plan developed. To be delivered 4Q2016

3.0.1 – General SDN Requirements

Requirement ID	Requirement Description 3.0.1 – General SDN Requirements	RFP Requirement ID
3.0.1.1	All Services, device configurations, hardware abstraction and Openflow applications (flowlets) should be specified in declarative YANG data model.	M 1700
3.0.1.2	A REST interface will be provided from OSS, BSS, Infrastructure Control and Orchestration.	M 1720
3.0.1.3	Shall operate in a hierarchical fashion capable of having parents and children controllers	
3.0.1.4	Shall use standard protocols to interface between controllers. This will require collaboration with the standards organizations	
3.0.1.5	Shall be able to operate as a child or a parent SDN Controller	
3.0.1.6	Neutron will be utilized for configuring controller and virtual switch flows.	M 1730
3.0.1.7	Shall utilize OpenFlow 1.3 or greater for flow control of the control plane.	M 1760
3.0.1.8	Any custom adapters provided will be OpenSource and contributed to the core project.	M 1770
3.0.1.9	SDN interface shall support initiating test and displaying readable results.	M 1810
3.0.1.10	Collaborate with AT&T to standardize the intent API framework	
3.0.1.11	Shall support a YANG (1.0 & 1.1) modeled NETCONF interface to network devices.	

Requirement ID	Requirement Description 3.0.1 – General SDN Requirements	RFP Requirement ID
3.0.1.12	Shall provide an interface to initiate and test calls shall be provided as part of the controller. (e.g.. yangui)	A 1150, M 1690
3.0.1.13	Shall support all IPv6 features in without any performance degradation.	V 200
3.0.1.14	Shall support Ipv4 and IPv6 simultaneously without performance degradation.	V 210
3.0.1.15	Shall support Ipv4 and IPv6 dual-stack operations.	V 220
3.0.1.16	Shall support requirements defined in RFC 2460, "Internet Protocol, Version 6 (IPv6) Specification.	V 230
3.0.1.17	Shall support requirements defined in RFC 2463, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification."	V 240
3.0.1.18	Shall support requirements defined in RFC 2464, "Transmission of IPv6 Packets over Ethernet Networks."	V 250
3.0.1.19	Shall support requirements defined in RFC 2474, "Definition of the Differentiated Services Field (DS Field) in the IPv6 Headers."	V 260
3.0.1.20	Shall support operation as a cluster	
3.0.1.21	Shall support migration of devices between cluster members	
3.0.1.22	Shall provide migration service of devices between clusters	
3.0.1.23	Shall provide ability to mix versions of SDN controllers in a cluster	
3.0.1.24	Shall provide subscriber automated migration services between controllers in a cluster. This includes migrating to a new version.	
3.0.1.25	Shall provide subscriber automated migration services between controllers in different clusters	
3.0.1.26	The ability to reuse VFs must be supported to enable AT&T to rapidly create services by chaining the VFs based on service needs.	V 630
3.0.1.27	Shall provide an Apache Kafka data publishing interface	

User Story 3.1: SDN Controller API for OpenDayLight

As a service provider, the environment will contain various SDN controllers and will evolve over time. It is critical that the ONOS platform can interface with other SDN controllers currently running on OpenDayLight.

Assumptions

- Existing SDN controller platform is currently an OpenDayLight Controller
- Shall meet requirements provided in the EPIC_COMMON.docx

Acceptance Criteria

- Ability to interact with OpenDayLight (Describe interact)
- Meet the defined test plan developed. To be delivered 4Q2016

Requirements

3.1.1 SDN Controller API for OpenDayLight

Requirement ID	Requirement Description 3.1.1 Management Requirements for SDN-U API	RFP Requirement ID
3.1.1.1	Shall operate in a hierarchical fashion capable of having parents and children controllers (e.g. OpenDayLight)	
3.1.1.2	Shall use standard protocols to interface between controllers. This will require collaboration with the standards organizations	
3.1.1.3	Shared Standard Controllers - Infrastructure and Network functions are controlled with shared AIC Infrastructure Controllers and Network Controllers. An Application function is controlled by an AIC Application Controller.	V 500
3.1.1.4	Shall provide YANG models and reference for OpenDayLight API	

User Story 3.2: vOLT Tenant Applications

As a service provider, it is the intent to disaggregate and virtualize components of the OLT platform and shift the control plane of the subscriber based services to the ONOS controller utilizing a vOLT control application to manage the 802.1x authentication, subscriber state management, VLAN assignments, ARP proxy services, DHCP services, DHCP Proxy and IGMP.

Assumptions

- Common requirements are met that are provided in EPIC_COMMON.docx

Acceptance Criteria

- Perform data and IPTV service meeting or exceeding what is currently provided from the ALU 7360 today
- Disaggregated vOLT functions providing Subscriber state management, VLAN assignments, ARP Proxy, DHCP Services, 802.1X and IGMP
- Meet the defined test plan developed. To be delivered 4Q2016

Requirements

3.2.1 OLT Requirements for SDN Control

Requirement ID	Requirement Description 3.2.1 – OLT requirements for SDN Control	RFP Requirement ID
3.2.1.1	During initial ONT turn up, the ONT shall be visible to the SDN per standard defined ONT turn-up procedure; shall be capable of being managed remotely by the SDN; shall have start up code capable of allowing the ONT to provide basic functions (to be specified) and support the software upgrade process; and shall notify the OLT or SDN that a startup code is present.	L 3950
3.2.1.2	The OLT or the SDN shall be capable of identifying that the ONT needs a software upgrade. A trap shall be created that identifies the ONT is currently on startup code.	L 3960
3.2.1.3	The software upgrade/transfer process shall be tracked by the SDN. This means that the operator shall be able to identify that the transfer has started, in-progress and that the transfer has completed. A trap (informational) should indicate that start up code was detected and transfer begun. The GUI should also give some sort of indication that an ONT upgrade is in progress.	L 3970
3.2.1.4	SDN interface must expose CRUD functions for both OLT and ONT management as defined by the YANG models.	M 1790
3.2.1.5	SDN GUI shall display status of both OLT and ONT devices.	M 1800
3.2.1.6	vOLT Control shall be able to operate independently of the ONOS controller.	
3.2.1.7	Shall function without the manipulation of the underlying network fabric	V 398
3.2.1.8	Shall provide support for the vBNG or Nokia/ALU 7450	V 399
3.2.1.9	Shall support the vendor specific/defined attribute of DHCP Option 82 in which the vendor and model of the OLT are each uniquely identified in separate attribute fields of Option 82.	V 1200
3.2.1.10	Shall inspect upstream and downstream DHCP packets, discover mapping of IP address to MAC address and populate its ARP table accordingly.	V 1210
3.2.1.11	Shall operate in a peallocation model or proxy to existing DHCP Infrastructure.	V 1220
3.2.1.12	Shall support configuration and management capabilities of the OLT through a NETCONF interface	

Requirement ID	Requirement Description 3.2.1 – OLT requirements for SDN Control	RFP Requirement ID
3.2.1.13	The PAE admin state for a port shall be provisionable via the SDN GUI and SDN controller northbound interface (NBI).	V 1590
3.2.1.14	Shall support ICMPv6 as defined in RFC4443.	V 270
3.2.1.15	The OLT shall support IPv6 based data services.	V 280
3.2.1.16	DHCP snooping function, if used on the OLT, shall support DHCP v6.	V 290
3.2.1.17	All data service functionality supported as part of IP v4 implementation shall be supported for IPv6 based data service.	V 300
3.2.1.18	OLT shall support IPv6 multicast based on RFC 3810 and RFC 4604.	V 310
3.2.1.19	All the IPTV functionality shall be supported for IPv4 and IPv6 based Multicast	V 320
3.2.1.20	Support referencing 3rd party BNG services either the ALU 7450 or vBNG	A 130
3.2.1.21	Shall provide a mechanism to register Multicast streams either directly to network devices or to SDN controllers. Shall support multiple methods of modification REST, RESTCONF and NETCONF	V 1100
3.2.1.22	Shall allow provisioning the RADIUS servers to be behind reverse NAT translation. (This supports a specific customer configuration where server addresses are translated between the server and the OLT.)	L 2710
3.2.1.23	Shall support Authenticator Port Access Entity (PAE).	L 2720
3.2.1.24	The Authenticator PAE shall implement the Authenticator state machines as defined in 802.1x.	L 2730
3.2.1.25	The PAE shall forward all EAPOL messages received from the supplicant except EAPOL-Start, EAPOL-Logoff and EAP-Request/Identity to the RADIUS server in the EAP-Message attribute of the RADIUS message.	L 2740
3.2.1.26	The PAE shall forward messages in the EAP-Message attribute of a RADIUS response as an EAPOL message to the supplicant. (The above requirements allow the supplicant and RADUIS server to use any authentication protocol they both understand.)	L 2750
3.2.1.27	The specific case of the supplicant using EAP-TLS with bi-directional authentication shall be verified.	L 2760
3.2.1.28	When a subscriber port is configured for 802.1X and the port is not in an enabled and authenticated state, no packets shall be exchanged between the subscriber port and the subscriber's network VLAN.	L 2770
3.2.1.29	The current 802.1X state of a port shall be available on the OLT's SDN GUI and SDN controller northbound interface (NBI).	L 2770
3.2.1.30	Shall support simultaneous authentication on all user ports.	L 2800
3.2.1.31	The PAE shall generate an EAP Request Identity message toward the subscriber when all of the following occur: • The port has a connection to the WAN • The port has 802.1x enabled • The port is in Admin enabled state • The port has a link established • The port is not authenticated.	L 2810
3.2.1.32	The PAE shall allow the supplicant to initiate an authentication sequence at any time with an EAPOL-Start message.	L 2830
3.2.1.33	When the PAE receives an EAPOL-Start message, the PAE shall return an EAP-Request/Identity message.	L 2840
3.2.1.34	If a port is authorized when the EAPOL-Start message is received by the PAE, the port shall remain authorized until the authentication process fails.	L 2850
3.2.1.35	If a port is not authorized when the EAPOL-Start message is received by the	L 2860

Requirement ID	Requirement Description 3.2.1 – OLT requirements for SDN Control	RFP Requirement ID
	PAE, the port shall remain in the not authorized state until the authentication process succeeds.	
3.2.1.36	Shall send RADIUS requests to UDP port 1812 of the RADIUS server.	L 2950
3.2.1.37	Shall populate the following attributes in RADIUS messages sent to the network: • User-name – This is the MAC address of the RG. • NAS-IP-Address – This is the management IP address of the OLT, which exchanges messages with the RADIUS server. • Calling-Station-ID – This is the MAC address of the RG being authenticated. • NAS-Identifier – This is the TID of the OLT • EAP-Message – This is an encapsulation of the EAP message exchanged between the Supplicant in the RG and the PAE in the OLT. • NAS-Port-ID – This is the AID of the physical port on the network being authenticated. • Vendor-Specific – This specifies the vendor id and model id of the OLT in different sub-attributes.	L 2870
3.2.1.38	Attribute definitions from RFC 2869 and RFC 2865 shall be used.	L 2880
3.2.1.39	The NAS-IP-Address in the RADIUS request shall be the management IP address of the OLT, which sends and receives RADIUS messages.	L 2890
3.2.1.40	The Calling-Station-ID in the RADIUS request shall be the Ethernet MAC address of the 802.1X supplicant.	L 2900
3.2.1.41	The NAS-Identifier in the RADIUS request shall be the TID of the OLT requesting authentication of the port to the RADIUS server.	L 2910
3.2.1.42	The EAP-Message in the RADIUS request shall be an encapsulation of the EAP message received from the supplicant.	L 2920
3.2.1.43	The NAS-Port-Id in the RADIUS request shall contain the port hardware address.	L 2930
3.2.1.44	The NAS-Port-Id in the RADIUS request shall have the same format as the circuit-id added by the OLT layer 2 DHCP relay agent in the Option 82 Agent Circuit-id field. It shall contains the same AID, but with no TID (node identifie8r).	L 2940
3.2.1.45	Shall provide a list of used TCP and UDP ports	
3.2.1.46	NE TID and port AID shall be used as object identifiers for the 802.1X MIBs instead of a port number.	L 2970
3.2.1.47	There shall be an admin state for the PAE associated with each port, when the NE is enabled for 802.1X.	L 2980
3.2.1.48	The PAE admin state for the port shall be enabled or disabled.	L 2990
3.2.1.49	The PAE admin state for a port shall be provisionable via the SDN GUI and SDN controller northbound interface (NBI).	L 3000
3.2.1.50	When the PAE admin state is disabled, there shall be no 802.1X processing on the port.	L 3010
3.2.1.51	Each NE shall have a SystemAuthControl attribute with a value of enabled or disabled, which shall enable or disable 802.1X processing for the entire OLT.	L 3020
3.2.1.52	When a system or NE is migrated from a version that does not support 802.1X to a version that does support 802.1X, the value for SystemAuthControl for all of the affected NEs shall be disabled.	L 3030
3.2.1.53	Each PAE shall support an authenticator configuration managed object.	L 3040
3.2.1.54	Shall support replicating 2048 active, simultaneous and unique IGMP-	L 1890

Requirement ID	Requirement Description 3.2.1 – OLT requirements for SDN Control	RFP Requirement ID
	controlled multicast groups at a minimum.	
3.2.1.55	Shall support the identification and processing of user-initiated IGMP messages.	L 2030
3.2.1.56	Shall support matching groups conveyed by IGMP messages to the list of groups corresponding to a multicast VLAN associated with this port. When there is no match, the IGMP message shall be either forwarded as regular user data or dropped. This behavior shall be configurable. When there is a match, the IGMP message shall be forwarded within a multicast VLAN, and enter the IGMP snooping function.	L 2060
3.2.1.57	IGMP v2/v3 snooping and proxy functions shall support the capability to snoop the multicast source IP address and destination IP group address in IGMP packets and to set the corresponding MAC group address filters.	L 2120
3.2.1.58	IGMP v2/v3 snooping and proxy functions shall be able to dynamically create and delete MAC-level Group Filter entries, enabling in turn, selective multicast forwarding from network-facing VLANs to user-facing ports.	L 2130