2016

EPIC COMMON

COMMON APPLICATION REQUIREMENTS

Table of Contents

Change Tracking

Version	Date	Contact	Description
.01	2016-08-25	BM2535@att.com	Initial Draft

Introduction

As a Service provider, we need to align on a set of tools, security and development practices across the planned access technologies. This document will cover include items that are applicable to all EPICs, however the individual EPICs may supersede individual requirements. The EPICs will need to track which version of the COMMON requirements document that is targeted for the sprint. If a COMMON requirement cannot be met as part of the sprint it shall be referenced in the backlog.

Assumptions

- These requirements pertain to all EPICs

Acceptance Criteria

- Acceptance shall be part of the individual EPICs meeting the provided requirements.
- Meet the defined test plan developed. To be delivered 4Q2016

1.1 - General Requirements

1.1.1 - General Requirements

Requirement ID	Requirement Description 1.1.1 – General Requirements	RFP Requirement ID
1.1.1.1	Shall be based on the current standard of Ubuntu Linux 14.04.4 LTS	A 390
1.1.1.2	Shall not require kernel modifications	
1.1.1.3	Shall not impede capabilities of the underlying operating system	
1.1.1.4	Shall be operable in a KVM (Ubuntu 14.04.4 LTS Host) or Docker Container	A 410
1.1.1.5	Shall operate on non-vendor specific x86 hardware	
1.1.1.6	Shall keep up-to-date and readily available records of system releases including all fixes/changes, and document such in the Software Release Notes.	
1.1.1.7	Shall provide Release Notes prior to or at the time of product delivery to AT&T. At a minimum, the Release Notes shall contain the following: • The version number for each item delivered and controlled under configuration management; • A listing of all 3rd Party Software, including any patches necessary to run the application under test; • A listing and description of the features and functions added with this release; • A listing and description of the known non-conformances and troubles, including previously known defects that remain open; • A listing and description of the non-conformances that have been resolved in this release; • A listing and description of all precautions and/or warnings related to this release.	
1.1.1.8	Prior to delivery, a Requirements Traceability Matrix shall be completed by demonstrating that each requirement is met in the delivered product. The test results shall provide reference to the appropriate notes in the Software Release Notes document (SRN) accompanying the delivery to the Companies for those specific systems under test.	
1.1.1.9	All documents supplied (Release Notes, Test Plans, Test Results, etc.) shall be under version control.	
1.1.1.10	Revisions of software shall be backward compatible with the previous versions. This shall include the ability of the software to maintain provisioning information that is on the system, including both existing and pre-provisioned services.	

1.1.2 – IPv4 and IPv6 Dual Stack Requirements

User Story Requirement ID	Requirement Description 1.1.2 – IPv4 and IPV6 Dual Stack Requirements	RFP Requirement ID
1.1.2.1	Shall support requirements defined in RFC 2460, "Internet Protocol, Version 6 (IPv6) Specification.	L 3180
1.1.2.2	Shall support requirements defined in RFC 4443, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification."	L 3190
1.1.2.3	Shall support requirements defined in RFC 2464, "Transmission of IPv6 Packets over Ethernet Networks."	L 3200
1.1.2.4	Shall support requirements defined in RFC 2474, "Definition of the Differentiated Services Field (DS Field) in the IPv6 Headers."	L 3210
1.1.2.5	Shall support IPv6 based data services.	L 3230
1.1.2.6	Shall support IPv4 and IPv6 simultaneously without performance degradation.	L 3150
1.1.2.7	Support for IPv6 debugging/troubleshooting tools e.g., IPv6 ping, IPv6 traceroute	E 270

1.1.3 - VNF Guidelines

Guideline ID	Guideline Description 1.1.3 – VNF Guidelines	RFP Requirement ID
1.1.3.1	Shall support SFTP as both a client and a server	V 145
1.1.3.2	Virtualized Software Based Applications/Services Applications and services shall be comprised of software components which are encapsulated within a virtualized machine(s) and abstracted from the physical hardware	V 400
1.1.3.3	Open Platform Key functions are programmable via open APIs, which align to Industry/AT&T API Standards and supported by an open and extensible information/data model.	V 440
1.1.3.4	Supplier Agnostic Components should follow industry standards and/or be open-source so that they can be easily exchanged or replaced.	V 450
1.1.3.5	Execution Location Agnostic Highly location agnostic - Able to run on any AIC infrastructure regardless of location, which allows for placement that meets performance requirements	V 460
1.1.3.6	Virtual Functions must be agnostic to the details of the AIC platform (e.g. hardware, Host OS, Hypervisor) and must run on a shared standard AIC cloud with acknowledgement to the paradigm that the AT&T AIC platform will continue to rapidly evolve and the underlying components to the platform will change regularly.	V 600
1.1.3.7	Decomposition of network functions must be supported	V 620
1.1.3.8	Open and standard APIs must be supported. Independent interfaces should be implemented in all possible cases.	V 720
1.1.3.9	Software must run on virtual machines (VMs) or software containers, and must be able to run on the same physical host where one or more other VMs are running.	V 830
1.1.3.10	Software must run in a multi-tenant cloud environment.	V 840
1.1.3.11	Solution must support at least (1) vNIC per virtual network (max of (8) vNICs) .	V 850
1.1.3.12	Solution must support the ability for the AIC cloud to assign fixed IP addresses. Also, the solution must support the ability to procure IP addresses from AT&T systems and provision them dynamically. IP address assignment and management shall use OpenStack supported mechanisms. Dynamic IP assignment via DHCP shall be supported.	V 860
1.1.3.13	In general, the VF solution shall not require the Virtual Function's VMs to use a dynamic routing protocol for interacting with the networking infrastructure.	V 870
1.1.3.14	VF solution shall not require OpenStack's lP anti-spoofing protection to be disabled.	V 880
1.1.3.15	The solution shall not require PXE boot of certain VMs in a VF cluster from a specific 'boot' VM in that cluster.	V 890
1.1.3.16	The solution should maintain a clear distinction between the Overlay/Guest function (VMs, VFs) and the Underlay function (AIC Network Infrastructure).	V 900
1.1.3.17	VFs must operate effectively with networking access via the AIC Overlay Network. To meet near term performance needs, VFs may optionally operate using SR-IOV under exception, with the expectation that VFs will be enhanced to operate with AIC Overlay Network (AT&T's preferred operating mode) and still meet performance needs. VFs will be considered on a case by case to use	V 910

Guideline ID	Guideline Description 1.1.3 – VNF Guidelines	RFP Requirement ID
	SR-IOV for network I/O.	
1.1.3.18	VF's that support packet processing are encouraged to utilize Data Plane Development Kit (DPDK). Vendors will have to account for additional resources required for the overhead of DPDK polling.	V 920
1.1.3.19	Must collaborate with AT&T on the use of a standard naming convention and data model for common data elements (e.g. telephone numbers).	V 930
1.1.3.20	Shall be working toward CNCF certification (cncf.io) which encompasses an open container format and runtime (opencontainer.org), container packaging, and microservice orientation.	V 940
1.1.3.21	Databases holding highly-scalable or geo-redundant data, in general, should be decoupled from network functions and should use virtualized scalable open source database software that can meet the performance/latency requirements of the service.	V 1000
1.1.3.22	VFs should maintain long-lived session data (e.g. registration state, stable call state/incall dialog) separately from the call processing logic.	V 1070
1.1.3.23	A failure of a VF VM should not terminate stable sessions.	V 1080
1.1.3.24	Decompose if the functions have significantly different scaling characteristics (e.g. signaling versus media functions, control versus data plane functions, etc.)	V 1200
1.1.3.25	Where applies decomposition should enable customizing a specific aspect of the network function on instantiations (e.g. the interworking function may need to be customized specific to each carrier interconnect instantiation)	V 1210
1.1.3.26	Decomposition shall enable instantiating only the functionality that is needed for the service (e.g. if transcoding is not needed, it should not be instantiated)	V 1220
1.1.3.27	Shall be explicit in code dependencies and relationship with other libraries and services.	V 1310
1.1.3.28	Configuration Parameters - YANG Model for VF parameters shall be provided	V 1350
1.1.3.29	Configuration Agent - NETCONF over SSH shall be provided	V 1360
1.1.3.30	Configuration/Notification Protocol - NETCONF/YANG RFC list should be supported, other options based on HTTP and/or NETCONF CLI with common scripting options (e.g. Python, Chef, etc.) are being evaluated.	V 1370
1.1.3.31	Network Model to define the network configuration for the VF, including integration with physical network functions (PNFs).	V 1480
1.1.3.32	Shall allow changes to VF configuration without the need to bounce the VM container.	V 1640
1.1.3.33	The End User database must be virtualized	V 1050
1.1.3.34	Any End User database holding highly-scalable or geo-redundant data must meet all the n+k geo-redundancy requirements.	V 1060
1.1.3.35	Must support evolution to an AT&T subscriber database for end user data, with application server VFs supporting a standard agreed to interface to this AT&T database. AT&T will work with vendors to ensure that the technology selected for the AT&T database would meet the performance requirements for the VFs.	V 1090
1.1.3.36	The registration state should be decoupled from the application server VF.	V 1100
1.1.3.37	The VFs should support storing the registration state of an End User in a cache and an external geo-redundant state database.	V 1110
1.1.3.38	Shall support evolution to an AT&T database and support a standard agreed to	V 1130

Guideline ID	Guideline Description 1.1.3 – VNF Guidelines	RFP Requirement ID
	interface to the AT&T specified state database (when defined) to store long-lived state.	
1.1.3.39	The solution must support the ability for AT&T to instantiate the VFs for 1 customer or multiple customers where applicable.	V 1660
1.1.3.40	Long-lived state and end user (/subscriber/customer) data should be decoupled from processing logic.	V 640
1.1.3.41	Shall allow subscriber provisioning directly to the VF (an EMS should not be required).	V 1670
1.1.3.42	Shall ensure that once a VF is instantiated using AT&T's orchestration function, subsequent configuration changes shall not require an EMS.	V 1680
1.1.3.43	End user/subscriber data must be decoupled from VFs.	V 1010
1.1.3.44	The solution must support the ability for AT&T to instantiate and customize via parameters one or multiple decomposed VFs on a per-service basis.	V 1650
1.1.3.45	It should be possible to get specific information concerning how to operate the VF from the VF in the execution environment including hostname, configuration, and operational limits.	V 1880

1.1.4 –Domain 2.0 Guidelines

Guideline ID	Guideline Description 1.1.4 – Domain 2.0 Guidelines	RFP Requirement ID
1.1.4.1	Applications and services shall be contain open services utilizing industry standard protocols	D 400
1.1.4.2	All network control and management capabilities shall be managed through NETCONF protocol	D 401
1.1.4.3	Key functions shall be exposed via open APIs, which align to industry and AT&T API Standards and supported by an open and extensible information/data model.	D 410
1.1.4.4	Programmability - Applications/Services and application/service components should be programmable by ATT&T and users including the ability to program via policy and rules to eliminate/minimize the need for per service developments.	D 420
1.1.4.5	VNFs should follow the emerging ETSI NFV ISG Framework	D 510
1.1.4.6	Applications shall be execution location agnostic	D 600

1.2 - FCAPS Reference

As a Service Provider, we want to develop the NETCONF/YANG interface, used for command control/management of OLT/ONT equipment, to provide standard FCAPS functions, so that the ONOS SDN solution can be production ready and deployed into the production market.

Assumptions

Applies to hardware platform as well as software platform (IE: de-bugging etc.)

Acceptance Criteria

This NETCONF (open interface) should support the Faults, Configuration, Accounting, Performance, and Security Management functions (FCAPS), but not limited to, the items listed below:

- Fault: Event trigger via (DCAE) Data Collection Analytics, autonomous events
- Configuration: Backup/restore, reboot/restart, multiple network segments, port configurations
- Accounting: State changes, port availability, active available inventory, usage state
- Performance: PON statistics, counters
- Security management functions for OLT chassis (pizza box, mOLT hosted in HES) PON and ONTs, security logging, fault trigger logging
- Meet the defined test plan developed. To be delivered 4Q2016

1.2.0 – General FCAPS Reference

Reference ID	Reference Description 1.2.0 – General FCAPS Reference	RFP Requirement ID
1.2.0.1	The hardware will provide the ability to see the transmit power reading from the ONT back to the PON via the SDN Controller. Accuracy shall be +/- 0.5dB.	**N 180**
1.2.0.2	The SDN Controller will report on hardware - hard failure. NOTE: Hardware will reboot in an effort to recover from the failure.: Controller will also report on Failed recover	**N 200**
1.2.0.3	Any condition deemed to be a hardware failure, or out of tolerance conditions will be stored in an area of hardware Flash memory. Information stored in flash can be accessed by the SDN Controller/NAL	**N 210**
1.2.0.4	Hardware will support IEEE 802.1D learning and bridging of MAC packets between the hardware data port(s) and XGEM Port-IDs.	**N 610**
1.2.0.5	The Hardware optical transmitter will be internally monitored to detect conditions relevant to the transmitter's life-span (e.g., a bias current measurement) and generate corresponding alarms.	**N 1130**
1.2.0.6	The hardware will support Connectivity Fault Management (CFM) per IEEE 802.1ag. Any exception shall be explicitly noted.	**N 2400, M 6011, M 6071**
1.2.0.7	Shall support the configuration of all CFM functions for MEPs and MIPs.	**N 2410**
1.2.0.8	Shall support the configuration of MEPS/MIPS to move between links in a link aggregation group during link failure.	**N 2420**
1.2.0.9	Shall support ability to administratively turn MIPs and MEPs on/off.	**N 2430**
1.2.0.10	The hardware will support eight Maintenance Domain (MD) levels.	**N 2440**
1.2.0.11	The hardware will support combination of MEP and MIP to be configured simultaneously across different MD levels	**N 2450**
1.2.0.12	Shall support ability to configure MEPs and MIPs to generate CFM PDUs at any priority level.	**N 2460**
1.2.0.13	Shall support (via NETCONF) the configuration and monitoring IEEE 802.1ag CFM OAM and to allow reporting of status and AIS alarms to the SDN Controller.	**N 2500**

Reference ID	Reference Description 1.2.0 – General FCAPS Reference	RFP Requirement ID
1.2.0.14	The hardware will raise an alarm upon Ethernet link failure detection to notify the SDN Controller/NAL of failure occurrence	**N 2680**
1.2.0.15	All device Management functions, configuration, measurements and events will be exposed via a NETCONF interface.	**M 80**
1.2.0.16	All Network Device logging should be provided to the vOLT hardware abstraction layer.	**M 120**
1.2.0.17	All device information shall be aggregated and provided to the DCAE infrastructure.	**M 131**
1.2.0.18	Management functions shall be configurable to communicate in-band and/or out-of-band (Ethernet) communication links, at the option of the service provider.	**M 300**
1.2.0.19	Shall support reporting/alarming of NE watchdog function to assess the performance of non-volatile memory (e.g. Flash, NVRAM…) in the "Common Processor Boards" of the NE. It shall report degraded performance, such as excessive write/erase cycle time, of the FLASH memory.	**M 711**
1.2.0.20	Shall support reporting/alarming of NE watchdog function to verify the compatibility of software and configuration between all the I/O, line, network, and processor modules of the NE. The watchdog function shall be triggered into action upon the resetting of any component modules of the NE.	**M 721**
1.2.0.21	Shall support reporting/alarming of temperature sensor in the event that the hardware exceeds its normal temperature operating range on the per port level basis.	**M 741**
1.2.0.22	Shall support analyzing a self-audit at a configurable frequency (defaulted to every 15 minutes) to validate current (standing) alarms.	**M 791**
1.2.0.23	Shall support configuring the frequency of a self-audit	**M 792**
1.2.0.24	Shall support the collection of information of the Network Device power units, circuits, feeders, and fuses and report associated alarms.	**M 951**
1.2.0.25	Shall support the collection of an alarm when the equipment's Central Processing Unit (CPU) utilization reaches a predefined threshold.	**M 961**
1.2.0.26	Shall support the collection of hardware alerts when the hardware optical facility bit error rate exceeds the acceptable threshold crossing level (i.e. 10-10).	**M 971**
1.2.0.27	Shall support IEEE 802.3ah Link OAM, including both active and passive modes.	**M 6001**
1.2.0.28	Shall support end-to-end IP ping: GWR to ONT, GWR to ETH card, ETH card to ONT.	**M 6031**
1.2.0.29	Shall support a network interface and ICMP ping.	**M 6041**
1.2.0.30	Shall support Two-Way Active Measurement Protocol (TWAMP), per IETF RFC 5357.	**M 6051**
1.2.0.31	Shall support management VLAN for inband management of Network Device with minimum bandwidth guarantees.	**M 6061**
1.2.0.32	Ethernet Link OAM - full support for Ethernet Link OAM (IEEE 802.3ah, standard) for all Ethernet ports of the PON system.	**M 6081**
1.2.0.33	Reporting, logging and alerting of the vOLT control application shall be managed by the SDN controller	**V 500**
1.2.0.34	All logging elements shall be made to the syslog	**V 182**
1.2.0.35	Syslog settings will be manageable through SSH.	**V 185**
1.2.0.36	Syslog will be retrievable through SSH and NETCONF interface.	**V 186**
1.2.0.37	Device change log should include date, time, initiating user, initiating interface, element being changed, previous value, new value, and response/error code.	**V 187**
1.2.0.38	The Network Device will suppress redundant alarm reporting. In other words, the Network Device shall not provide autonomous alarm reports to the Controller and syslog for subsequent detection of a failure condition that has already been	**V 188**

Reference ID	Reference Description 1.2.0 – General FCAPS Reference	RFP Requirement ID
	reported and not cleared.	
1.2.0.39	Syslog purge events will log the time, date and user that performed the action.	**V 190**
1.2.0.40	Syslog will have capability for local log rolling and compression.	**V 191**
1.2.0.41	Syslog will have the ability to reference remote syslog collection systems.	**V 192**
1.2.0.42	All Measurement data shall be exposed via a NETCONF interface	**V 193**
1.2.0.43	All measures will be made available to an Apache Kafka UEB Interface, syslog and SFTP.	**V 194, M 1820**
1.2.0.44	Standardized mechanisms for Fault Configuration Accounting Performance and Security (FCAPS) functions must be supported by VFs.	**V 670**
1.2.0.45	Monitoring Agents - Agents embedded in the VF and/or that are external to the VF that consume telemetry messages, perform analytics, and publish events when some actions or lifecycle change is needed for the VF	**V 1390**
1.2.0.46	VF supports collection and analytics of the Lifecycle Events. Shall provide the information needed to implement the VF analytic signatures/events triggering changes that are required in the VF configuration topology	**V 1420**
1.2.0.47	Shall enable their VF products to provide the following data in real-time and near real-time to northbound AT&T systems via a standard agreed to interface: - Consistent alarm and event format in a defined standard - Faults - Events (i.e. host/customer configurations changes, prepaid service events) - Performance Management Data (i.e. Application KPIs) - Usage data (i.e. CDR data, VF performance data) - On demand access to additional detailed tracing and trouble-shooting data. - Note: The VF must provide the data in a timely manner (e.g. real-time streaming). The need for timeliness also implies the need for direct access to the information (e.g. no vendor-provided EMS function is envisioned in the architecture)	**V 1810**
1.2.0.48	Fault and performance data must be passed directly from the VFs to the AT&T collectors through standardized interfaces provided by the vendor (an EMS must not be required).	**V 1820**
1.2.0.49	Enable VFs to provide logging/audit trail capabilities according to AT&T standards. - Ensure that logging issues such as saturation of logging queues shall not impact the performance of resources.	**V 1830**
1.2.0.50	AT&T intends to minimize or eliminate the need for passive probe-based monitoring at various points in the network. In order to realize this goal, the VF should provide enhanced instrumentation that allows AT&T to build or procure applications providing detailed view into the VF and network behavior (e.g. Session Analysis, DPI analysis). Vendors shall enable their VFs to: - Provide detailed records (flow records, session records, transaction records, etc.) at configurable intervals. - Provide access to the control-plane message stream processed by the VF. - Provide on-demand access to the User plane stream (that is configurable in a flexible manner – for specific set of International Mobile Subscriber Identity (IMSIs), IPs, time interval etc.) - Include configurable instrumentation (not requiring a development cycle) to accommodate fast operational turnaround.	**V 1840**
1.2.0.51	Need to provide visibility into VF performance and fault at VFC (VF component is the smallest granularity of functions in our architecture) level to allow ECOMP to proactively monitor and manage network conditions at its source.	**V 1850**

Reference ID	Reference Description 1.2.0 – General FCAPS Reference	RFP Requirement ID
1.2.0.52	AT&T standard tools should be able to monitor VF components.	**V 1860**
1.2.0.53	All VF components should be monitored locally and restarted automatically when a failure occurs. - Automatic restart - Bridge and Roll (instantiate a new VF instance retaining the original VF's content & context)	**V 1870**
1.2.0.54	The VF may provide the ability to control workload within a VM/container.	**V 1890**
1.2.0.55	Will have a pluggable interface for health check and management of workloads.	**V 1900**

1.2.1 – Fault Reference

As a Service Provider, we want to develop the NETCONF/YANG interface, used for command control/management of OLT/ONT equipment, to provide standard fault reporting functions, so that the ONOS SDN solution can be production ready and deployed into the production market

Assumptions

Applies to hardware platform as well as software platform (IE. de-bugging etc.)

Acceptance Criteria

- This NETCONF (open interface) should support the Faults.
- Fault: Event trigger via (DCAE) Data Collection Analytics, autonomous events
- Meet the defined test plan developed. To be delivered 4Q2016

Reference ID	Reference Description 1.2.1 – Fault Reference	RFP Requirement ID
1.2.1.1	Hardware shall forward all alarm information northbound to the SDN system.	**G 650**
1.2.1.2	In the event the link between the SDN and the hardware is down, the hardware shall retain all alarm information, including the original timestamps, until the link is re-established and then forward the stored information to the SDN.	**G 660**
1.2.1.3	The hardware shall perform a self-audit at a configurable frequency (defaulted to every 15 minutes) to validate current alarms.	**G 670**
1.2.1.4	ONT/ONU miscellaneous alarm inputs attributes should be user defined and provisioned on a per ONT/ONU basis, by assigning one of several environmental alarm profiles, or by individually provisioning each ONT/ONU alarms. In terms of alarms, assignable attributes should include the ntcncde, almtype, and almmsg.	**G 680**
1.2.1.5	System shall provide critical, major and minor severity alarms, as well as “informational” alerts.	**G 690**
1.2.1.6	A complete failure of the power system controller for remote alarm transmitting/reporting units, if used, shall be reported to the relevant management system.	**G 700**
1.2.1.7	A failure within the power system controller to remote alarm transmitting/ reporting units, if used, shall not result in any false signaling or inaccuracies in alarm information that could result in service interruptions.	**G 710**
1.2.1.8	Hardware shall support monitoring of the physical layer to indicate change in link status. Status should be "In-Service" or "Out-of-Service" for each ONT served by the OLT and shall be made available by the OLT upon request.	**G 1170**
1.2.1.9	All PON optical transmitters and receivers used shall be internally monitored to raise relevant alarms. These Alarms shall be provided to the vOLT and presented on the SDN Controller.	**L 630**
1.2.1.10	Hardware should trigger the appropriate alarms for Loss of Continuity.	**L 2650**
1.2.1.11	Hardware shall generate IEEE 802.1ag Connectivity Fault Management (CFM) OAM related statistics that are retrievable from the SDN. The required statistics are: received, relayed, generated OAM packets and byte counts per interface, dropped OAM packets and byte counts with cause code.	**L 2670**
1.2.1.12	Hardware shall not provide autonomous alarm reports to the SDN for subsequent detection of a trouble that has already been reported. If the trouble is cleared, the clearing of the trouble shall be reported to the SDN.	**L 3720**
1.2.1.13	During the software update process if a service impacting call is received, a human readable error will be returned to the vOLT requiring the port to be disabled prior to updates.	**M 230**
1.2.1.14	Alarms, diagnostic commands, and status information will be provided to the Abstraction layer	**M 511**

Reference ID	Reference Description 1.2.1 – Fault Reference	RFP Requirement ID
1.2.1.15	Shall maintain active monitoring on hardware and software during normal operation and report failed checks through syslog and the vOLT	**M 561**
1.2.1.16	Upon trouble detection, the Network Device shall initiate automatic recovery where possible. Switchover to protect facility/link is allowed during the recovery. Notification of event should occur through syslog and vOLT	**M 570**
1.2.1.17	The use of specialized manual fault-finding techniques or tools to diagnose faults in the Network Device shall not be required.	**M 690**
1.2.1.18	Shall provide a mechanism to capture and store failure/fault data at a "debug" or vendor developer level of detail. SFTP transfer to the target system. The intent is for the Network Device vendor to supply detailed data for root cause failure analysis.	**M 701**
1.2.1.19	Shall support reporting/alarming of Fan shelf failure situations: either one fan fail, more than one fan fails, fan speed is below normal, or airflow is below normal.	**M 751**
1.2.1.20	Shall support detection of troubles (hardware, software, performance degradation, loss of synchronization, etc.) and autonomously report alarms and conditions	**M 771**
1.2.1.21	Shall report an alarm clear messages when the corresponding alarm condition clears.	**M 781**
1.2.1.22	Support alarms from the Network Device	**M 801**
1.2.1.23	The Network Device Alarms will include an operator defined Terminal Identifier of up to 20-characters, alarm type, alarm priority (Critical, Major, Minor), a service affecting or non-service affecting (SA/NSA) indicator, and a character text alarm description.	**M 821**
1.2.1.24	The Network Device alarms will be configurable as critical, major, minor, not reported, and not alarmed. Network Device alarm levels shall be configurable per port, per module, and/or per NE.	**M 831**
1.2.1.25	Shall have the capability to prevent alarm storms.	**M 841**
1.2.1.26	Shall support providing an alarm profile as a method of configuring alarm severity assignments on a "per Network Device", logical port and physical port.	**M 851**
1.2.1.27	The Network Device shall report alarms to the vOLT and syslog (configurable for one, the other or both) via both the in-band and out-of-band management communication links.	**M 880**
1.2.1.28	No Network Device reset or rebooting shall be required to clear any alarm condition.	**M 890**
1.2.1.29	Shall suppress alarms on pre-provisioned equipment and ports until the correct hardware and a valid transmission signal is subsequently established. Once these conditions are met, the Network Device will change the operational state of the component or facility to "In Service" and enable alarm reporting.	**M 901**
1.2.1.30	Shall suppress redundant alarm reporting for subsequent detection of a failure condition that has already been reported and not cleared.	**M 911**
1.2.1.31	Shall support the collection of data related to loss of signal from the ONT.	**M 981**
1.2.1.32	Shall support the collection of detailed information of the discrete system components to sufficiently identify the hardware in a failure condition.	**M 991**
1.2.1.33	There shall be an admin state for the PAE associated with each port, when the NE is enabled for 802.1X.	**V 1570**
1.2.1.34	The PAE admin state for the port shall be enabled or disabled.	**V 1580**
1.2.1.35	NE Information Models and Schemas: Information models and Schemas, that are **not currently** supported in YANG, shall be published and maintained from release to release for all information exported from all NE interfaces, including all fault, performance, traffic, inventory, topology, configuration, syslog and policy data.	**E 1030**

Reference ID	Reference Description 1.2.1 – Fault Reference	RFP Requirement ID
	This requirement applies to all modes of export – standardized interfaces (e.g., SNMP) as well as craft interfaces (e.g., command line interfaces or other vendor-specific interfaces). These schemas shall be exportable from the NE for compilation on an AT&T OSS.	
1.2.1.36	Network Element will support a unique, configurable, source address for router-originated messages, preferably the loopback address. Such messages include SNMP Traps, Log messages, Authentication requests, DNS queries.	**E 1040**
1.2.1.37	Network Element will support the following Network Management protocol interfaces to north bound Controllers and other OSSs: NETCONF [IETF RFC 6241]; Flow Monitoring [RFC 3954]; SNMP [various RFCs]; SYSLOG [RFC 5424]; [TOR-only] OpenFlow Configuration and Management Protocol (OF-Config); and [TOR-only] OpenFlow (1.0 and 1.3) 2.X RESTConf [IETF RFC draft-bierman-netconf-restconf-xx].	**E 1050**
1.2.1.38	Network Element will support environmental status monitoring that includes power, voltage, current, and temperature. The NE shall generate an alarm in case environmental exception conditions are detected.	**E 1340**
1.2.1.39	Network Element will support monitoring of all hardware components. The Network Element will generate an alarm in case an operational failure is detected in a hardware component.	**E 1360**
1.2.1.40	Provide list of all hardware components monitored and corresponding alarms generated.	**E 1370**
1.2.1.41	Network Element will monitor all of its software processes and components. The NE shall generate an alarm in case a failure is detected in a software component.	**E 1389**
1.2.1.42	Network Element will be able to generate an alarm when loss of a redundant hardware component occurs, such as loss of a redundant power supply, redundant fan.	**E 1400**
1.2.1.43	Network Element will support actions to be taken based on the IEEE 802.3ah alarming.	**E 1520**
1.2.1.44	Network Element will support 802.3ah alarms per standard and provide sufficient error information, e.g., NE, interface	**E 1530**
1.2.1.45	Network Element will support 802.3ah troubleshooting commands.	**E 1540**
1.2.1.46	Network Element will notify the NMS when a link degrades beyond a configurable BER (Bit Error Rate) threshold.	**E 1550**
1.2.1.47	Correspondingly, notify when degrade condition is cleared.	**E 1560**
1.2.1.48	Network Element will notify the NMS and take a link down at local end when link fails beyond a (separate) configurable BER threshold.	**E 1580**
1.2.1.49	Network Element will notify and bring a link up when a link fail condition is cleared.	**E 1610**
1.2.1.50	Network Element will notify the remote end when the link clears via standards-based OAM protocol.	**E 1620**
1.2.1.51	All notifications should follow current AT&T NM design for the product (e.g., via SNMP Trap, via Syslog).	**E 1670**
1.2.1.52	Network Element will support LACP alarms per standard and provide sufficient error information as well as topology information, e.g., Network Element, interface.	**E 1700**
1.2.1.53	No silent failures: There shall be no silent failures, which according to Telcordia TR-NWT-000418 are any equipment or software failures that result in a loss of service, a loss of protection, or a loss of platform management and control functions without an audible alarm and/or remote signaling to initiate corrective action. Compliance with this requirement shall be demonstrated through a design review,	**E 1970**

Reference ID	Reference Description 1.2.1 – Fault Reference	RFP Requirement ID
	a review of the reliability block diagram, and the analyses of expected failures for the platform. CRITICAL NOTE: AT&T recognizes that it may be impossible to meet this requirement in its entirety, but AT&T does expect the vendor to fully document any and all potential silent failures and the probability of occurrence for each. AT&T is particularly concerned about traffic black holes resulting from silent failures. The vendor shall state whether the silent failures could result in a traffic black hole.	

1.2.2 – Configuration Reference

As a Service Provider, we want to develop the NETCONF/YANG interface, used for command control/management of OLT/ONT equipment, to provide standard Configuration functions, so that the ONOS SDN solution can be production ready and deployed into the production market.

Assumptions

Applies to hardware platform as well as software platform

Acceptance Criteria

- This NETCONF (open interface) should support the Configuration functions
- Configuration: Backup/restore, reboot/restart, multiple network segments, port configurations
- Meet the defined test plan developed. To be delivered 4Q2016

Reference ID	Reference Description 1.2.2 – Configuration Reference	RFP Requirement ID
1.2.2.1	The PON system shall support the use of third party optics for both uplinks and PON ports. The use of software keys or any other method that prevents the PON system from fully functioning with third party optics is prohibited.	**G 20**
1.2.2.2	The PON system shall be fully compliant with ITU-T G.989.x and ITU-T G.9807.1 specifications.	**G 30**
1.2.2.3	The PON system shall fully comply with GR-909-CORE.	**G 40**
1.2.2.4	The PON system shall fully comply with IEEE 802.1F, "Common Definitions and Procedures for IEEE 802 Management Information".	**G 50**
1.2.2.5	The design of the network element shall allow for fiber connectors and fiber routing and should not result in fiber bends or stress on the fiber connectors when the network element shelf doors are opened or closed, or the network element plug-ins are inserted or removed.	**G 60**
1.2.2.6	All network elements (including all equipment units and assemblies) shall be marked with model and/or part numbers, month and year of manufacture, and serial numbers.	**G 70**
1.2.2.7	The PON system shall meet the equipment coding requirements of Telcordia Technologies' GR-485-CORE, "Common Language® Equipment Coding Processes and Guidelines".	**G 80**
1.2.2.8	The PON system shall support enabling or disabling downstream AES encryption for each channel identified by Port_ID. The default shall be enabled (note: the default does not apply to multicast Port_ID).	**G 110**
1.2.2.9	The PON system shall support at least 128 ONTs per PON.	**G 120**
1.2.2.10	The PON system shall be capable of providing symmetric bandwidth allocation.	**G 150**
1.2.2.11	Proposed system shall operate with multiple TWDM channels with both of line rates of 9.95328 Gbps downstream and 9.95328 Gbps upstream in a TWDM PON over a single fiber.	**G 200**
1.2.2.12	The System, including components, circuit packs and software, shall be under configuration management, such that each configurable item has an assigned version number (or CLEI codes for hardware and software release number) that can be used for tracking purposes.	**G 260**
1.2.2.13	Shall provide configuration information specific to the system under test, or for deployment, including NE/SDN configuration (with appropriate release levels, 3rd Party Software, Patch Releases), server platform, database release, open systems and interface feature sets.	**G 270**
1.2.2.14	The OLT shall provide a mechanism to map the service class of a XGEM Port-ID to the Ethernet priority bits in the corresponding VLAN tag, and vice versa.	**L 970**

Reference ID	Reference Description 1.2.2 – Configuration Reference	RFP Requirement ID
1.2.2.15	The OLT shall provide a mechanism to map the service class of a subscriber port to the Ethernet priority bits in the corresponding VLAN tag, and vice versa.	**L 1010**
1.2.2.16	The PON system elements shall be able to support configuration of buffer sizes/depth of all ingress and egress queues per CoS.	**L 1640**
1.2.2.17	For VoIP queues, the PON system elements shall support configurable priority queue sizes to support at least 9 Ethernet frames.	**L 1650**
1.2.2.18	For video queues, the PON system elements shall support configurable priority queue sizes to support at least 96 Ethernet frames.	**L 1660**
1.2.2.19	The Strict Priority (SP) queue should have an option to limit the PIR to a configurable value.	**L 1670**
1.2.2.20	The PON system elements shall support configurable re-marking of p-bits based on classified flow, i.e., marking based either on classifier output (no policer) or on policer output (classifier + policer).	**L 1680**
1.2.2.21	Utilize registration codes, that could be received at the OLT end, for newly installed, or replaced ONTs.	**N 1920**
1.2.2.22	OCP ONIE Kernel will run on network device	**M 31**
1.2.2.23	OCP ONIE model shall support provisioning of the Network device	**M 32**
1.2.2.24	ONIE should support configuration of network device in the vOLT and vOMCI	**M 33**
1.2.2.25	OCP ONIE platform shall utilize OpenSource Software	**M 34**
1.2.2.26	ONIE OCP shall support re-initialization of the network device in the event of a catastrophic failure	**M 211**
1.2.2.27	ONIE re-initialization will be able to be initiated from the vOLT, Local Craft and SSH.	**M 220**
1.2.2.28	Software shall support pre-provisioning of hardware where one or more plug-ins or components of the end-to-end PON customer are temporarily missing, mismatched, out of service, or yet to be equipped.	**M 271**
1.2.2.29	The Network Device shall be capable of synchronizing automatically the software and configuration between any of the I/O, line, network, and processor modules of the NE, if it founds them to be incompatible. The synchronization shall be based on a designated master (e.g. at the primary “common processor board”). The Operator shall be able to turn on/off this feature via vOLT, SSH or Craft interface. That is, any subtended systems, modules, ONT devices shall sync with the activated software and configuration on the active control card/module on the NE.	**M 350**
1.2.2.30	The PON system shall provide configuration data over a vOLT interface for all physical interfaces including inventory, virtual interfaces, OSI layer 3 and above protocols into which there is visibility.	**M 360**
1.2.2.31	When a plug-in is replaced, the software shall automatically upgrade the replacement plug-in’s according to its provisioned software version and overwrite provisioning data with then current provisioning data.	**M 551**
1.2.2.32	Shall include an option to enable or inhibit revertive automatic protection switching of protected transport facilities and timing supplies.	**M 621**
1.2.2.33	On command switch to protect upon request of the Craft Interface, vOLT and SSH, shall be supported for configurations having automatic restoration. On-command switching shall not cause error rates outside of service level parameters.	**M 630**
1.2.2.34	Shall allow backup, initialization, re-initialization, or restoration	**M 731**
1.2.2.35	Shall utilize the NETCONF protocol for configuration and management of the managed devices.	**M 1740**
1.2.2.36	Shall provide ability to utilize YANG data models to define communication to NE.	**M 1750**
1.2.2.37	The vOLT in ONOS shall allow provisioning the RADIUS servers to be behind	**V 1301**

Reference ID	Reference Description 1.2.2 – Configuration Reference	RFP Requirement ID
	reverse NAT translation. (This supports a specific customer configuration where server addresses are translated between the server and the OLT.)	
1.2.2.38	NE TID and port AID shall be used as object identifiers for the 802.1X instead of a port number.	**V 1560**
1.2.2.39	The value of the Agent Circuit ID shall be explicitly configurable, per individual access loop and logical port. When not explicitly configured, it shall be automatically generated using the default or flexible syntax described in following requirements.	**V 1640**
1.2.2.40	The value of Access-Node-Identifier shall be configurable per Network element, using an element management interface. The Access-Node-Identifier may be derived automatically from an already defined object ID (e.g., IP address of management interface).	**V 1650**
1.2.2.41	It shall be possible to override the default syntax of circuit ids, and let the operators configure a more flexible syntax for the Agent Circuit ID, with flexibility in the choice of elements used in the automated generation of circuit-IDs. Such syntax is unique per Network element. The flexible syntax shall allow the concatenation of 2 types of elements: • Strings of ASCII characters configured by the network operator. This will typically include characters used as separators between variable fields (usually # . , ; / or space). • Variable fields whose content is automatically generated by the OLT. Fields should include information which doesn't vary over time for a given access loop.	**V 1660**
1.2.2.42	Shall provide a capability to configure the addressing and access parameters to at least two (primary and secondary) external RFC 2685 compliant RADIUS servers.	**V 1670**
1.2.2.43	Shall provide a configuration to utilize an external RADIUS system first for user authentication, and then use the locally defined userIDs if the RADIUS servers is unavailable.	**V 1680**
1.2.2.44	System shall support time synchronization methods over SyncE, NTP, PTP, BITS or IEEE 1588 Timing	**A 600**
1.2.2.45	Shall provide time synchronization from multiple NTP based time sources	**A 610**
1.2.2.46	The solution should support configuration rollback.	**V 4270**
1.2.2.47	Support IEEE 802.3	**E 10**
1.2.2.48	Support IEEE 802.1p Traffic Class Expediting, 802.1v VLAN Classification	**E 20**
1.2.2.49	Support IEEE 802.1D MAC Bridges	**E 30**
1.2.2.50	Support IEEE 802.1q Virtual LAN	**E 40**
1.2.2.51	Support IEEE 802.1ad Q-in-Q Provider Bridges	**E 50**
1.2.2.53	Support for gratuitous ARP	**E 70**
1.2.2.54	Support VLAN tag push, pop, swap for both SVLAN and CVLAN.	**E 80**
1.2.2.55	Support 802.1q, outer SVLAN TPID=0x8100, inner CVLAN TPID=0x8100.	**E 90**
1.2.2.56	Support 802.1ad, outer SVLAN TPID=0x88a8, inner CVLAN TPID=0x8100.	**E 100**
1.2.2.57	Support 802.1q and transmitting and receiving up to 5 VLAN tags stacking TPID=0x8100	**E 110**
1.2.2.58	No restriction on use of tag values 1 - 4095 for SVLAN. Identify the restriction if any.	**E 120**
1.2.2.59	No restriction on use of tag values 1 - 4095 for CVLAN.	**E 130**
1.2.2.60	Support unnumbered interfaces	**E 170**
1.2.2.61	Support Inbound packet filtering based on: Source IP address; Destination IP address; Source port number or range; Destination port number or range and/or	**E 180**

Reference ID	Reference Description 1.2.2 – Configuration Reference	RFP Requirement ID
	protocol.	
1.2.2.62	Support Outbound packet filtering based on: Source IP address; Destination IP address; Source port number or range; Destination port number or range and/or protocol.	**E 190**
1.2.2.63	Support RFC 7130 BFD for LAG Interface to be run on each individual link within a link aggregation bundle, such that failure detection on a single member link causes that member to be removed from the bundle.	**E 210**
1.2.2.64	Support for jumbo frames, where a jumbo frame is ~ 9000 bytes in size. Please indicate the maximum jumbo frame size for each interface type, and indicate specifically what that number includes, i.e. IP datagram, L2 overhead, CRC/FCS, etc.	**E 220**
1.2.2.65	Support of 2-tuple per-flow load-balancing based on source IP address and destination IP address (either IPv4 or IPv6).	**E 230**
1.2.2.66	Support of 5-tuple per-flow load-balancing based on source IP address, destination IP address, (either IPv4 or IPv6), source port, destination port, and protocol.	**E 240**
1.2.2.67	Support IPv6 packet filtering based on ACL.	**E 260**
1.2.2.68	All QoS requirements apply to both IPv4, IPv6 and DS (Note any exception in the supplier response for each requirement).	**E 380**
1.2.2.69	Support Full DiffServ support, RFC 2597 and 3246.	**E 390**
1.2.2.70	Support a complete separation of EXP and TOS QoS as well as DSCP per physical interface. [Ability to assign EXP, TOS and DSCP to any queue].	**E 400**
1.2.2.71	Support a complete separation of EXP and TOS QoS as well as DSCP per logical (VLAN) interface. [Ability to assign EXP, TOS and DSCP to any queue].	**E 410**
1.2.2.72	Support TOS/DSCP/EXP to/from 802.1p translation - ability to map in either direction.	**E 420**
1.2.2.73	Support the ability to differentiate between classes with a weighted mechanism within queues. Also to schedule, drop, police and shape within these queues based upon that weighted factor.	**E 430**
1.2.2.74	Support a class based drop mechanism that uses configurable relative class weights within each queue, number of queues ranging from one to eight when using EXP and IP precedence values. The drop mechanism must be based on average queue depth with the ability to tune that.	**E 440**
1.2.2.75	Support traffic shaping parameters should be configurable as a percentage of interface bandwidth as well as an absolute rate.	**E 450**
1.2.2.76	Support Egress traffic shaping and ingress rate limiting shall be class-aware.	**E 460**
1.2.2.77	Support Policing per logical interface.	**E 470**
1.2.2.78	Support Marking per logical interface.	**E 480**
1.2.2.79	Support marking per packet based on IP header (v4 and v6).	**E 490**
1.2.2.80	Support Shaping per logical interface.	**E 500**
1.2.2.81	Support Full line forwarding at 64 byte packet sizes with QoS mechanism enabled.	**E 510**
1.2.2.82	Support classification based on any field in the IP header as well as physical or logical incoming interface.	**E 520**
1.2.2.83	Support policing based on any field in the IP header as well as physical or logical incoming interface.	**E 530**
1.2.2.84	Support egress policing based on any field in the IP header as well as physical or logical interface.	**E 540**
1.2.2.85	Support to assign queues to any of the possible 8 classes.	**E 550**
1.2.2.86	Support for WRED, Class-Based WFQ, LLQ mechanisms.	**E 560**

Reference ID	Reference Description 1.2.2 – Configuration Reference	RFP Requirement ID
1.2.2.87	Support two or more queuing priorities. Realtime and data priorities.	**E 570**
1.2.2.88	Support three or more queuing priorities. This would include a low latency or Realtime priority, a near Realtime priority and a data priority.	**E 580**
1.2.2.89	Support Policing, classifying queuing and scheduling should be effective on aggregate of IPv4 and IPv6 combined traffic.	**E 590**
1.2.2.90	Support Policing, classifying queuing and scheduling should be effective on aggregate of unicast (IPv4 and IPv6 combined) and multicast (IPv4 and IPv6 combined) traffic.	**E 600**
1.2.2.91	Support Hierarchical policing on ingress and egress.	**E 610**
1.2.2.92	Support Hierarchical queuing/scheduling/shaping on ingress and egress.	**E 620**
1.2.2.93	Support Hierarchical QoS, allowing multiple logical interfaces (but not the entire port) to be combined under a single shaper/scheduler/policer policy structure.	**E 630**
1.2.2.94	Support of all QoS features on all logical interfaces configured. i.e. scale numbers should assume QoS on all interfaces.	**E 640**
1.2.2.95	Support flexibility to configure at a global, physical interface and logical interface levels is highly desired.	**E 650**
1.2.2.96	Support Ability to assign a class to any locally originated control traffic.	**E 660**
1.2.2.97	Ability to assign a class to locally originated control/NM traffic based on protocol.	**E 670**
1.2.2.98	Support IGMPv2 & IGMPv3.	**E 680**
1.2.2.99	Support at least 4 and at most 8 10GE interfaces. Each interface can be configured as either an uplink or a downlink,	**E 690**
1.2.2.100	Please indicate your Support for Ethernet Link Aggregation (LAG 802.3ad) for 10GEinterfaces. Indicate the maximum number of member links that can be supported on your platform per physical interface type.	**E 720**
1.2.2.101	Please indicate your Support for Ethernet Link Aggregation Control Protocol (LACP) for 10GEinterfaces. Indicate the LACP implementation, active-active, active-standby, etc.	**E 730**
1.2.2.102	Addition or deletion or failure or recovery of members to existing LAG shall be hitless (<50 milliseconds loss).	**E 740**
1.2.2.103	Support IGMP proxy.	**E 750**
1.2.2.104	Support OpenFlow 1.3 or greater.	**E 770**
1.2.2.105	Ability to configure OpenFlow flows via CLI or NETCONF.	**E 780**
1.2.2.106	Ability to directly manipulate the FIB using an external controller.	**E 790**
1.2.2.107	Ability to program forwarding plane using OpenFlow 1.3 or greater to a SDN controller.	**E 800**
1.2.2.108	The full capabilities of each pluggable must be addressable independently of the rest of the switch via a standards based API.	**E 830**
1.2.2.109	In-Band management Access via any active WAN or LAN Interface shall be configurable. Access list controls must be supported to restrict such in-band access. This connection should provide fully functional access to the NEs CLI interface.	**E 1090**
1.2.2.110	The NE shall support five or more simultaneous remote sessions to access the CLI, and this shall include in-band and out-of-band sessions.	**E 1110**
1.2.2.111	The NE shall support a smooth and easy way of clearing active and stuck VTY/vCP connections.	**E 1120**
1.2.2.112	The NE shall support remote access session inactivity Time-outs – timeout values shall be configurable.	**E 1130**
1.2.2.113	Multiple debug/log levels shall be supported. Syslog messages should be grouped	**E 1310**

Reference ID	Reference Description 1.2.2 – Configuration Reference	RFP Requirement ID
	by level. The ability to turn on syslog by level should be supported.	
1.2.2.114	The capability to activate and de-active (i.e., shutdown) syslog event logging through the command line interface shall be supported.	**E 1320**
1.2.2.115	Configuration of syslog parameters shall be supported through the command line interface. At least the following parameters must be configurable: Remote syslog server IP address (syslog messages are sent to the remote syslog server); Size of internal log buffer; and Source IP address of syslog messages tied to loopback of NE.	**E 1330**
1.2.2.116	Time of action should be configurable; with a sub-second initial value.	**E 1480**
1.2.2.117	Restoring link back into service should include a configurable dampening option to mitigate impact of flapping links.	**E 1490**
1.2.2.118	Notify remote end when link taken down via standards-based OAM protocol.	**E 1590**
1.2.2.119	Time of action should be configurable, with a sub-second initial value.	**E 1600**
1.2.2.120	Implement a configurable link dampening method to mitigate impact of flapping links.	**E 1630**

1.2.3 – Accounting Reference

As a Service Provider, we want to develop the NETCONF/YANG interface, used for command control/management of OLT/ONT equipment, to provide standard Accounting functions.

Assumptions

Applies to hardware platform as well as software platform

Acceptance Criteria

- This NETCONF (open interface) should support Accounting
- Accounting: State changes, port availability, active available inventory, usage state
- Meet the defined test plan developed. To be delivered 4Q2016

Reference ID	Reference Description 1.2.3 – Accounting Reference	RFP Requirement ID
1.2.3.1	Changes to the network device shall be captured on the Access Network Abstraction Layer and provided to the DCAE platform	**M 251**
1.2.3.2	The software shall report a successful or unsuccessful attempt to restore of the network device configuration data and to re-initialization after restore.	**M 311**
1.2.3.3	Shall report a successful restoration or unsuccessful attempt-at-restoration; for example, protection switching on “Common Hardware,” facilities, etc.	**M 591, M 601**
1.2.3.4	Shall be capable of reporting autonomous state changes. For example, a state change notification would result when the operational state of a piece of equipment changes from “in-service” to “out-of-service”.	**M 661**
1.2.3.5	Shall detect and report a successful ONT restoration to the vOLT.	**M 671**
1.2.3.6	Shall support the collection of optical basic band receive power level values	**M 1001**
1.2.3.7	Shall support Reporting, accounting and stats collection	**V 490**
1.2.3.8	System and application will log changes. Provide a service that reports the old & new values for a defined time period.	**A 90**
1.2.3.9	End user data should be cached for fast retrieval of data	**V 1030**
1.2.3.10	Do you support MAC-Layer Accounting?	**E 280**
1.2.3.11	The NE platform shall support a bulk statistics mechanism that allows users to configure a specific set of managed objects (i.e., SNMP MIB counters), for which its instance value is generated and made available at a specific time interval. Describe your mechanism, its intervals and is methods of making the resulting data available to other systems (e.g., SFTP).	**E 1710**
1.2.3.12	The aggregation interval for statistics generation shall be configurable (5 minutes, 15 minutes, 60 minutes, etc.). Describe your capabilities.	**E 1720**
1.2.3.13	Describe your bulk statistics file storage limitations and whether any such limit is configurable. Also describe how the NE handles statistics file roll-overs when such limits are exceeded.	**E 1730**
1.2.3.14	Data storage to support northbound system restoration. One hour’s worth of measurements shall be stored in the NE. Describe your capabilities and support for northbound system restoration.	**E 1740**
1.2.3.15	Ethernet statistics support for NE interfaces: Ethernet Frame count at each port; incoming and outgoing; Byte count at each Ethernet port: incoming and outgoing; Errored frames received at each Ethernet port: aggregate, as well as per error type (such as CRC); Frames dropped at each port (due to congestion); incoming and outgoing.	**E 1750**
1.2.3.16	Packet statistics support per interface. All statistics below shall be available on all NE interfaces per: CoS, orig/dest IP address, and AS; Packets / octets transmitted	**E 1760**

Reference ID	Reference Description 1.2.3 – Accounting Reference	RFP Requirement ID
	and received; Packets / octets discarded; and Packet length statistics.	
1.2.3.17	Describe how the Ethernet and Packet statistics are made available.	**E 1770**
1.2.3.18	Separate statistics for each direction's traffic on bi-directional resources. On all NE interfaces, all measurements of bi-directional resources, such as interfaces, shall include separate counts for each direction of transport	**E 1820**
1.2.3.19	Event driven data collection: Describe the ability of the platform to perform event driven date collection. Event driven data collection shall mean that all data (logs/traces) of events shall be automatically captured and archived for small duration events. The data stored for these events shall present a timeline view of activity that occurred on the platform for each protocol, in the control plane, in the forwarding plane and in the hardware. The duration for the data driven events shall be configurable by the operator.	**E 2120**
1.2.3.20	Subsystem/process logging: Describe the ability of the platform to perform subsystem/process logging. Subsystem/process logging shall mean that all subsystem/process failures log appropriate error messages. Writing a trace entry is not sufficient.	**E 2130**

1.2.4 – Performance Reference

As a Service Provider, we want to develop the NETCONF/YANG interface, used for command control/management of OLT/ONT equipment, to provide standard Performance Reporting

Assumptions

Applies to hardware platform as well as software platform (IE. de-bugging etc.)

Acceptance Criteria

- This NETCONF (open interface) should support Performance data collection.
- Performance: PON statistics, counters
- Meet the defined test plan developed. To be delivered 4Q2016

Reference ID	Reference Description 1.2.4 – Performance Reference	RFP Requirement ID
1.2.4.1	Provide detailed summary describing the system bottleneck and capacity limitation of the proposed PON platform. Also please provide the deployment model which can maximize the utilization of the proposed platform.	**G 160**
1.2.4.2	The PON system shall support standard performance monitoring through Ethernet OA&M at all Ethernet interfaces.	**G 1180**
1.2.4.3	The PON system shall support monitoring of the implemented and visible protocol layers above the Ethernet framing, such as IGMP snooping/proxy performance, DHCP option 82 imposition performance (RFC 3046), EAP over RADIUS, and voice performance.	**G 1190**
1.2.4.4	The PON system shall support Ethernet performance monitoring by CoS and by VLAN including untagged and null tagged frames.	**G 1200**
1.2.4.5	The PON system shall measure frame throughput rate and bandwidth utilization transmit/receive average and peak; by type of frame (unicast, multicast, broadcast), and by size of frame.	**G 1210**
1.2.4.6	The PON system shall measure average and maximum latency and jitter and frame discards resulting from policy settings.	**G 1220**
1.2.4.7	The PON system shall measure frame discards resulting from errors by type of error.	**G 1230**
1.2.4.8	Support for subscriber based traffic management	**V 510**
1.2.4.9	Retrieving End User data from the database must meet all the existing performance requirements of a service.	**V 1020**
1.2.4.10	Mechanisms to prioritize packets/traffic should be supported.	**V 2710**
1.2.4.11	Specify any performance variations, including but not limited to delay, throughput, CPU utilization, etc. from no load to full load	**E 290**
1.2.4.12	Indicate the throughput when forwarding the following packet sizes, specifically: 100% - 64 byte; 100% - 512 byte; 100% - 1500 byte; Imix (Provide Imix packet profile used).	**E 300**
1.2.4.13	Note any cases where forwarding is not possible (e.g. enablement of a certain feature, oversubscribed ports, etc.)	**E 310**
1.2.4.14	Indicate any packet forwarding implications of small packets with micro-flows, i.e. large volumes of traffic using a small set of source/destination IP addresses	**E 320**
1.2.4.15	Specify the bottlenecks or hard limits, if any, in the control plane.	**E 330**
1.2.4.16	Specify impacts on the performance with various levels of logging turned on and or external data polling.	**E 340**
1.2.4.17	Specify whether or not Packet re-ordering occur on the platform with or without load	**E 350**

Reference ID	Reference Description 1.2.4 – Performance Reference	RFP Requirement ID
1.2.4.18	Identify causes or configurations that will result in intensive CPU consumption.	**E 360**
1.2.4.19	Describe any impacts like delay or jitter on the data traffic resulting from any variations of the control traffic on the platform.	**E 370**
1.2.4.20	The NE shall support monitoring of utilization of expendable NE system resources such as CPU, Memory, Disk, RAM, NVRAM etc.	**E 1410**
1.2.4.21	The solution should provide a list of all expendable resources monitored and corresponding alarms and stats generated.	**E 1420**
1.2.4.22	The NE shall support the Link Fault Management (LFM/802.3ah) specification in IEEE 802.3-2008 Section 5 (aka “EFM OAM” or Ethernet in the First Mile OAM).	**E 1470**
1.2.4.23	For parallel interfaces configured in a LAG, fault and performance management for each lane should be supported.	**E 1510**
1.2.4.24	The NE shall be able to detect BER on 10GbE.	**E 1570**
1.2.4.25	All parameters useful in assessing BER (e.g., PCS Errors, FCS Errors, Optical Power levels) should be reportable via CLI.	**E 1640**
1.2.4.26	Extensions for localized product enhancements to estimate BER more accurately should be provided to AT&T for review, assuming they do not impact inter-vendor operation.	**E 1690**
1.2.4.27	Collaboration with AT&T D2 performance management systems.	**E 1780**
1.2.4.28	Describe your collaboration, if any, with network management software for the purpose analyzing the measurements.	**E 1790**
1.2.4.29	Support polling access from multiple performance management systems.	**E 1800**
1.2.4.30	Describe how multiple performance management systems will be allowed to simultaneously poll a single NE. Describe any limits on the number allowed.	**E 1810**

1.2.5 – Security Reference

As a Service Provider, we want to develop the NETCONF/YANG interface, used for command control/management of OLT/ONT equipment, to provide standard Security Management functions, so that the ONOS SDN solution can be production ready and deployed into the production market

Assumptions

Applies to hardware platform as well as software platform

Acceptance Criteria

- This NETCONF (open interface) should support the Security Management functions
- Security management functions for OLT chassis (pizza box, mOLT hosted in HES) PON and ONTs, security logging, fault trigger logging
- Meet the defined test plan developed. To be delivered 4Q2016

Reference ID	Reference Description 1.2.5 – Security Reference	RFP Requirement ID
1.2.5.1	Management platform must support security containment and recovery as defined in GR-3025-CORE, Issue 1, 07/2001.	**G 1240**
1.2.5.2	If SNMP is employed the data confidentiality shall be based on SNMPv3 usage of the encryption algorithm DES when SDN or OSS type applications are used.	**G 1250**
1.2.5.3	Shall include an option to inhibit (lock out) automatic switching of "Common Hardware" and transport facilities.	**M 611**
1.2.5.4	Authenticator Port Access Entity (PAE) shale be utilized.	**V 1310**
1.2.5.5	The Authenticator PAE shall implement the Authenticator state machines as defined in 802.1x.	**V 1320**
1.2.5.6	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.	**V 1330**
1.2.5.7	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.)	**V 1340**
1.2.5.8	The specific case of the supplicant using EAP-TLS with bi-directional authentication shall be verified.	**V 1350**
1.2.5.9	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.	**V 1360**
1.2.5.10	When a subscriber port is authenticated, packets from the subscriber that do not contain the source MAC of the RG, which was authenticated, shall not be forwarded to the network. (This behavior is beyond what is specified in 802.1X. The standard allows all traffic on a port once it is authenticated.)	**V 1370**
1.2.5.11	The current 802.1X state of a port shall be available on the vOLT's SDN GUI and SDN NBI.	**V 1380**
1.2.5.12	The AAA shall support simultaneous authentication on all user ports.	**V 1390**
1.2.5.13	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.	**V 1400**

Reference ID	Reference Description 1.2.5 – Security Reference	RFP Requirement ID
1.2.5.14	For Ethernet lines, a link shall be considered established when the link operational status is enabled.	**V 1410**
1.2.5.15	The PAE shall allow the supplicant to initiate an authentication sequence at any time with an EAPOL-Start message.	**V 1420**
1.2.5.16	When the PAE receives an EAPOL-Start message, the PAE shall return an EAP-Request/Identity message.	**V 1430**
1.2.5.17	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.	**V 1440**
1.2.5.18	If a port is not authorized when the EAPOL-Start message is received by the PAE, the port shall remain in the not authorized state until the authentication process succeeds.	**V 1450**
1.2.5.19	The AAA 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.	**V 1460**
1.2.5.20	Attribute definitions from RFC 2869 and RFC 2865 shall be used.	**V 1470**
1.2.5.21	The NAS-IP-Address in the RADIUS request shall be the management IP address of the OLT, which sends and receives RADIUS messages.	**V 1480**
1.2.5.22	The Calling-Station-ID in the RADIUS request shall be the Ethernet MAC address of the 802.1X supplicant.	**V 1490**
1.2.5.23	The NAS-Identifier in the RADIUS request shall be the TID of the OLT requesting authentication of the port to the RADIUS server.	**V 1500**
1.2.5.24	The EAP-Message in the RADIUS request shall be an encapsulation of the EAP message received from the supplicant.	**V 1510**
1.2.5.25	The NAS-Port-Id in the RADIUS request shall contain the port hardware address.	**V 1520**
1.2.5.26	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 identifier).	**V 1530**
1.2.5.27	The AAA shall send RADIUS requests to UDP port 1812 of the RADIUS server.	**V 1540**
1.2.5.28	When the PAE admin state is disabled, there shall be no 802.1X processing on the port.	**V 1600**
1.2.5.29	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.	**V 1610**
1.2.5.30	Each PAE shall support an authenticator configuration managed object.	**V 1620**
1.2.5.31	The vOLT shall support the IEEE 802.1X standards.	**V 1630**
1.2.5.32	All VNF functions shall be hardened to meet AT&T Security Requirements (Req will be reviewed with CSO during contract negotiations)	**V 143**
1.2.5.33	Linux distribution will support pluggable authentication models (e.g. PAM, LDAP, RSA)	**V 157**

Reference ID	Reference Description 1.2.5 – Security Reference	RFP Requirement ID
1.2.5.34	Log files shall not store passwords, hashes or credentials	**V 183**
1.2.5.35	Availability and Security Requirement Availability and Security Requirements are well articulated and evidenced through architectural approaches utilized.	**V 510**
1.2.5.36	VF vendors should support the new security solutions to mitigate new and additional threats introduced by virtualization. VF vendors should be able to embed their security solutions in the Domain 2.0 deployment.	**V 2800**
1.2.5.37	VF vendors must evolve their current security controls and adopt new security controls to protect against new and evolving threats in the virtual environment accordingly as per AT&T's security framework and guidelines.	**V 2810**
1.2.5.38	VF vendors should continue to support basic security features that are currently available in a non-virtualized deployment	**V 2820**
1.2.5.39	VFs running on an AT&T standard image will have standard AT&T security and OS agents/tools protecting the application and OS. AT&T security and OS agents/tools or other mitigating controls must be deployed on VFs running on vendor provided guest OS's.	**V 2830**
1.2.5.40	VF vendors should work with AT&T CS0 to conduct security Proof of Concepts to drive security design and requirements through industry forums.	**V 2840**
1.2.5.41	Domain 2.0 security vendors should implement Security Function Virtualization (SFV) by leveraging SDN and NFV technologies (virtual Firewalls, virtual IDS/IPS, vDDOS etc.).	**V 2850**
1.2.5.42	Domain 2.0 Security vendors should integrate their solution with AT&T's Domain 2.0 Security Framework and concepts to provide a robust security design and architecture (open platform, API-based solution, etc.).	**V 2860**
1.2.5.43	VF vendors should ensure that their Identity and Access Management (IdAM) solutions and controls can integrate with AT&T's centralized IdAM system in a virtual environment.	**V 2870**
1.2.5.44	AT&T IdAM solutions will authenticate users for access to VM operating systems using centralized operating system authentication	**V 2880**
1.2.5.45	AT&T IdAM solutions will apply authorization workflow approvals and authorization provisioning for the VM operating system hosting the VF.	**V 2890**
1.2.5.46	AT&T IdAM solutions will authenticate a user and either authorize at the centralized IdAM level, e.g., RBAC, OAuth 2.0, ABAC, or provide user identity data to local VF solution authorization mechanisms, e.g., RBAC.	**V 2900**
1.2.5.47	AT&T IdAM solution and VF solutions must mutually authenticate and communicate over an encrypted channel	**V 2910**
1.2.5.48	VF vendors should be able to provide security controls for Enhanced Control, Orchestration, Management and Policy (ECOMP) functions to protect the infrastructure and services.	**V 2920**
1.2.5.49	VF vendors must provide security monitoring and analytics platforms that can be adaptive to the virtual environment (i.e. elastic and on-demand security monitoring, etc.).	**V 2930**
1.2.5.50	VF vendors must adhere to the security requirements as described in AT&T Security Policy and Requirements (ASPR).ASPR requirements can be reviewed with the AT&T sponsor through a separate procedure which will need to be followed at a later stage.	**V 2940**
1.2.5.51	VF vendors should be able to provide solutions that can take into account the security policy and requirements for the virtual environment and address compliance, privacy, and regulatory implications (ASPR, CALEA, E911, etc.).	**V 2950**
1.2.5.52	VF vendors should be able to provide security tools that can implement Trusted	**V 2960**

Reference ID	Reference Description 1.2.5 – Security Reference	RFP Requirement ID
	Software Lifecycle including development, testing, and configuration controls. This tool-based code validation process will ensure vulnerability free software.	
1.2.5.53	VF vendors should leverage security integration in Domain 2.0 to offer scalable Security as a Service to Enterprise and Consumers. These apply to the security pillars that are part of Domain 2.0 framework.	**V 2970**
1.2.5.54	VF vendors must incorporate Supplier Information Security Requirements (SISR) into the product.	**V 2980**
1.2.5.55	VF vendors must adhere to CSO's existing security guidelines for Network to ensure audit compliance as per Network Security Control Framework	**V 2990**
1.2.5.56	Security solutions associated with the VFs must ensure that user access control is implemented for the new virtualized elements (integrate with security access management systems).	**V 3000**
1.2.5.57	Vendor solutions must implement user-IDs and passwords to uniquely identify the user/application (Authentication) for the new virtualized elements.	**V 3010**
1.2.5.58	VF Vendor solutions should implement 3-Factor Authentication for users/applications accessing from outside the VPN (e.g. user/application on a mobile device trying to access internal AT&T services should authenticate as follows: 1st factor = Software token on device (RSA SecureID); 2nd factor = User Name+Password; 3rd factor = Fingerprint or Voice-Print via device).	**V 3020**
1.2.5.59	Encryption of data elements (password) must be implemented for user/application access authentication for the new virtualized elements.	**V 3030**
1.2.5.60	VF vendors should implement roles to permit/limit the user/application to performing specific activities (least-privilege/Authorization) for the new virtualized elements.	**V 3040, V 3070**
1.2.5.61	VF vendors should implement logging for a historical view of "who did what" (Accounting) for the new virtualized elements.	**V 3050, V 3080**
1.2.5.62	VF vendors should implement Access Control List (restricting access to certain ports or applications) for the network VFs.	**V 3060, V 3090**
1.2.5.63	VF vendors should implement L3 VPNs to segregate traffic by application (dropping packets not belonging to the VPN) (i.e. AVPN, IPSec VPN for Internet routes).	**V 3100**
1.2.5.64	VF vendors must implement security event/KPI reporting and audit logging for the new virtualized elements.	**V 3110**
1.2.5.65	VF vendors must ensure the software vulnerability management process is used to test the new virtualized elements.	**V 3120**
1.2.5.66	Application VF vendors (e.g., vSGW, vPGW, vRouter, vBNG) should continue to support basic security features such as eNodeb authentication to avoid false handover, PGW's packet filtering feature to support QoS, ability to mitigate rogue IP address assignment, and policy enforcement functions to detect speed and session policy violation.	**V 3130**
1.2.5.67	VF vendors should ensure that these can integrate and intenNork with strong VM quarantine/isolation capabilities that are available as part of AIC infrastructure.	**V 3140**
1.2.5.68	VF vendors should ensure that their products can adapt, integrate and interoperate with various access control mechanisms for the hypervisor.	**V 3150**
1.2.5.69	VF (Security) vendors should ensure that the product has the ability to detect unauthorized access to hypervisor and log failed access attempts.	**V 3160**
1.2.5.70	VF vendors should ensure it can interwork with Hypervisor Introspection function	**V 3170**
1.2.5.71	VF vendors should support virtual trusted platform module, hypervisor security testing and scanning	**V 3180**
1.2.5.72	VF vendors should ensure that it can interwork with the orchestration function to provide security policies for instantiation, management and validation	**V 3190**

Reference ID	Reference Description 1.2.5 – Security Reference	RFP Requirement ID
1.2.5.73	VF vendors should ensure that these can interwork with the orchestration functions to provide a mechanism for automated/frequent system configuration auditing.	**V 3200**
1.2.5.74	Application VF vendors (e.g., vEPC) should continue to support basic security features such as ciphering, integrity protection for NAS signaling, RRC signaling and user plane traffic.	**V 3210**
1.2.5.75	Application VF vendors must continue to provide protection to the visibility of the UE's permanent user identity (IMSI)	**V 3220**
1.2.5.76	Application VF vendors (e.g., vUSP/vIMS) must provide hardening features to pass security vulnerability scans.	**V 3230**
1.2.5.77	The VF vendors must subject the product to security testing such as flooding attacks, general malware attacks, protocol attacks, DDOS attacks.	**V 3240**
1.2.5.78	VF vendors should ensure that third-party security functions (e.g. Virtual IDS/IPS) can leverage vendor's product's alert capabilities (e.g. syslog, SNMP alerts, etc.) to detect security events.	**V 3250**
1.2.5.79	VF vendors should ensure that security functions (e.g., IPS, IDS, DDoS, Firewall, etc.) can potentially be embedded into vendor product and integrate.	**V 3260**
1.2.5.80	VF security vendors should ensure that dynamic service chaining of virtual security functions can be made possible using API, controller and orchestration functions.	**V 3270**
1.2.5.81	Ensure that VF vendor's product can communicate with SDN Controller over SSL or equivalent secure protocol.	**V 3280**
1.2.5.82	Ensure that VF vendor interoperate with (SDN Controller) so that it can dynamically modify the firewall rules, ACL rules, QoS rules, virtual routing & forwarding rules.	**V 3290**
1.2.5.83	Ensure that VF vendor can communicate with DCAE (Data Collection, Analytics and Events) and respective SDN Controller to provide real-time analytics for DDoS detection and mitigation.	**V 3300**
1.2.5.84	Ensure that VF vendor's product is compatible with OpenStack security standards such as keystone	**V 3310**
1.2.5.85	Ensure that the VF vendor's product has support for both North Bound and South Bound APIs.	**V 3320**
1.2.5.86	VF vendors must ensure that its product follows the orchestration security policies for instantiation, management and validation.	**V 3330**
1.2.5.87	VF vendors must ensure that it can interwork with orchestration functions to validate instantiation of VMs.	**V 3340**
1.2.5.88	VF vendors must ensure that it can interwork with the orchestration for automated/frequent system configuration auditing.	**V 3350**
1.2.5.89	Security VF vendor solutions should be able to monitor VMs and patching of OS and appropriate applications.	**V 3360**
1.2.5.90	Security VF vendor solutions should implement logging and monitoring of hypervisor activities, scanning of hypervisors.	**V 3370**
1.2.5.91	Security vendors should ensure hardening of hypervisors and all images, access control for administrative access to hypervisor.	**V 3380**
1.2.5.92	Monitoring in virtualized environment may add additional complexities based on the type of deployment and types of interfaces interconnecting the VFs. Security VF vendors should explore additional methodologies such as API-based monitoring to take care of security analytics in those situations where interfaces are either not exposed or they use proprietary interfaces and internal data structure.	**V 3390**

Reference ID	Reference Description 1.2.5 – Security Reference	RFP Requirement ID
1.2.5.93	VFs must support security monitoring/detection/analytics/reporting capabilities.	**V 3400**
1.2.5.94	Ensure that VF's APIs/integration capabilities can support other threat management systems.	**V 3410**
1.2.5.95	Ensure that security VF can correlate control plane data and user plane data to provide subscriber identifying information (e.g. IMSI, IMEI etc.).	**V 3420**
1.2.5.96	Ensure this product can provide network forensics that are equal to or better than what we have in place today.	**V 3430**
1.2.5.97	Ensure VF vendors have support for network element fault management (monitoring, alarming, ticketing, reporting, dashboards, NOC, analysis, resolution, tier 1/2/3).	**V 3440**
1.2.5.98	Ensure the VF vendors support software vulnerability management process such as authentication, encryption (e.g., SSH), traffic separation (dropping packets not belonging to vOA&M-VPN), For example, software patching process needs to have an authentication mechanism in place in order to avoid the rogue patching.	**V 3450**
1.2.5.99	Ensure that the VF vendors support access control list for vOA&M services by restricting to certain ports or applications.	**V 3460**
1.2.5.100	For a VF vendor's product with multiple interfaces, all OA&M services and applications (SNMP, SSH, HTTPS, etc.) shall be bound to the OA&M interface only. Ensure that this relationship is verified each time the Network Element (NE) is patched, upgraded, rebooted, etc.	**V 3470**
1.2.5.101	The vendor solution should ensure that the network/routing configuration will be verified at each initialization, reboot, patch or other OS modification.	**V 3480**
1.2.5.102	VF vendors should ensure that OA&M access applications and protocols must be encrypted or use natively encrypted protocols (ex. SSH, https, etc.).	**V 3490**
1.2.5.103	Any use of Active Directory for OAM purposes must be reviewed and approved by AT&T CSO during design.	**V 3500**
1.2.5.104	Use of Active Directory or similar families of services for OA&M may trigger additional requirements.	**V 3510**
1.2.5.105	All data used to provide the Domain 2.0 infrastructure and all data transmitted, stored and operated on by Domain 2.0 services must be classified according to AT&T Security Policy and Requirements.	**V 3520**
1.2.5.106	The VF vendors must enforce the principle of least privilege at all times. This includes during both administrative activities and service execution.	**V 3530**
1.2.5.107	VF vendors must ensure that all data in the Domain 2.0 environment is accessed, stored and transmitted in compliance with the following ASPR policies: User Authentication for Systems and Applications, Storage of Electronic Data, and Transmission of Electronic Data.	**V 3540**
1.2.5.108	VF vendors should implement data leakage protection (DLP) services.	**V 3550**
1.2.5.109	VF vendors must ensure that access control is implemented for all Domain 2.0APIs. All APIs must integrate with AT&T access control technologies in compliance with the security requirements dictated by the sensitivity of the data and functionality accessible through the API.	**V 3560**
1.2.5.110	All VF APIs should validate input and return consistent error messages when presented with unexpected input. The error messages must not provide information that can be used to help an attacker.	**V 3570**
1.2.5.111	The API security environment must provide measures to ensure availability and to prevent both volumetric and non-volumetric Denial of Service attacks.	**V 3580**
1.2.5.112	All VF APIs must ensure confidentiality of the data.	**V 3590**
1.2.5.113	All VF APIs must implement logging and monitoring that is compliant with ASPR.	**V 3600**

Reference ID	Reference Description 1.2.5 – Security Reference	RFP Requirement ID
1.2.5.114	All Domain 2.0 APIs must be developed in compliance with ASPR policies on Service Realization, Application/System Development and Application Security.	**V 3610**
1.2.5.115	The VF vendors should adhere to the policy that would not cause the instantiation to be out of compliance with relevant security standards (e.g., ASPR, legal, regulatory, HIPAA, PCI, etc.) for all valid specific data inputs to an instantiation.	**V 3620**
1.2.5.116	The solution should support the ability to work with aliases (e.g. gateways, proxies) to protect and encapsulate resources.	**V 3630**
1.2.5.117	VF shall support access over SSH	**V 4330**
1.2.5.118	VF shall support shared key authentication model	**V 4340**
1.2.5.119	Shall review AT&T ASPR guidelines to ensure solution documented configurations meet or exceed ASPR standards as they apply.	**A 750**
1.2.5.120	Any ASPR exception should be reported with a Risk assessment	**A 760**
1.2.5.121	Support for tunneling protocols such as: IPSEC and GRE	**E 200**
1.2.5.122	The NE shall support limiting remote access by source IP address.	**E 1100**
1.2.5.123	The NE shall support a configurable number of maximum allowable remote sessions	**E 1140**
1.2.5.124	The NE shall support remote access via SSH.	**E 1150**
1.2.5.125	Support SNMP version 2 and 3 authentication, encryption, and packet filtering for access control.	**E 2330**
1.2.5.126	Support SSH version 2 for VTY access, packet filter to SSH for access control; filter has to checked before a TCP port is open; limit the number of concurrent SSH sessions and the number of SSH session attempts (per unit time).	**E 2340**
1.2.5.127	Support encrypted file transfer.	**E 2350**
1.2.5.128	Ability to disable any/unused ports. All ports should be disabled by default. Support the capability to disable all unneeded physical ports (e.g., console, auxiliary, craft).	**E 2360**
1.2.5.129	The command line interface must support following capabilities: Login with user ID. Where user ID can be six characters long, with the first character being a letter, and the remaining characters being alphanumeric; Authentication via password.	**E 2370**
1.2.5.130	A failed login attempt must not identify the reason for the failure to the user, only that the login was incorrect. After a maximum of six (6) consecutive unsuccessful attempts to login, the User's ID must be automatically disabled and further login attempts must be denied.	**E 2380**
1.2.5.131	Multiple access levels with command filtering at least the following two user access levels: Read-only access; and Read-write access.	**E 2390**
1.2.5.132	Support TACACS+ with minimum 4 servers for redundancy, a time out value for each server.	**E 2400**
1.2.5.133	Enforce the following minimum requirements with respect to local passwords: Passwords must be at least six (6) characters in length, must include characters from at least two (2) of these groupings: alpha, numeric, and special characters; and Passwords must not be the same as the user id with which they are associated.	**E 2410**
1.2.5.134	Support an AT&T-defined warning notice to be issued during the logon sequence. The warning notice should remain displayed until positive action by the user is taken to acknowledge the message.	**E 2420**
1.2.5.135	Support as an NTP client to use one or more NTP servers. This synchronized clock must be the basis of all times reported in syslog and TACACS+ messages.	**E 2440**
1.2.5.136	Log(s) must be automatically updated by at least the following system events: Successful and unsuccessful login attempts; Successful and unsuccessful attempts	**E 2440**

Reference ID	Reference Description 1.2.5 – Security Reference	RFP Requirement ID
	to switch to another entity's account or assume another entity's privileges (where applicable); logoffs; user attempts to access files or resources outside their privilege level; user access to all privileged files and/or processes, network element configuration changes; changes to system hardware and software; all security related changes including adding users; failures for computer, program, communications and operations; starting and stopping of logging.	
1.2.5.137	Log must contain at minimum the following fields: event type; date/time; protocol; service or program used for access; success/failure; Login ID only if the Login ID is defined on the network element; otherwise, the field must contain 'unknown', in order to protect passwords accidentally entered at the Login ID prompt from appearing in the security audit log.	**E 2450**
1.2.5.138	Logs must never contain an authentication credential, e.g., password, even if encrypted.	**E 2460**
1.2.5.139	When the log storage medium is filled to capacity, new events must continue to be logged and only log entries associated with oldest events removed.	**E 2470**
1.2.5.140	Support Telcordia GR-815-CORE. Generic Requirements for Network Element/Network System (NE/NS) Security	**E 2480**
1.2.5.141	Comply with the final version of T1M1.5/2003-007R5 ANSI "Baseline Security Requirements for the Management Plane".	**E 2490**
1.2.5.142	The device must support methods to protect against the following scenarios as discussed in RFC 4665: Service Requirements for Layer 2 Provider-Provisioned Virtual Private Networks: protocol attacks; resource utilization; unauthorized access; tampering with signaling; tampering with data forwarding.	**E 2500**
1.2.5.143	Ability to disable gratuitous ARP processing.	**E 2510**
1.2.5.144	Ability to defend against ARP table flooding.	**E 2520**
1.2.5.145	Support MAC addresses filtering.	**E 2530**
1.2.5.146	The device must be able to filter/block/log traffic based on any field or combination of fields of a packet header.	**E 2540**
1.2.5.147	Support packet filtering with rate limiting based on bytes, packets, or both on inbound and outbound IPv4 and IPv6 traffic on a logical interface. Within a packet filter it must be possible to specify source/ destination IP address/prefix, source/destination port number or range, TTL (Hop Limit for IPv6) value, protocol, IPv4 fragment, IPv4 option, IPv6 Next Header value, TCP flags (including syn, ack, rst and fin) and/or ICMP/ICMPv6 message type and code. It must be possible to count and log the packets matching each term of a packet filter.	**E 2550**
1.2.5.148	Ability to turn off directed broadcasting.	**E 2560**
1.2.5.149	Ability to disable forwarding fragmented packets.	**E 2570**
1.2.5.150	Ability to control protocol access directed to the device (e.g., SNMP, HTTP, ICMP, etc.)	**E 2580**
1.2.5.151	Ability to control, disable, and rate limit specific control protocols like ICMP.	**E 2590**
1.2.5.152	Ability to withstand UDP/TCP probes from scanning tools across all interface types.	**E 2600**
1.2.5.153	Ability to control protocol access directed to the device (e.g., SNMP, HTTP, ICMP, etc.).	**E 2610**
1.2.5.154	Ability to rate limit control traffic (e.g., ICMP) punted to control plane against Distributed Denial of Service (DDOS) attacks.	**E 2620**
1.2.5.155	Specify mechanisms available to protect route processor (or CPU) from DDoS attacks.	**E 2630**
1.2.5.156	Describe your policies and processes regarding correcting, and disseminating alerts	**E 2640**

Reference ID	Reference Description 1.2.5 – Security Reference	RFP Requirement ID
	or advisories pertaining to, any security flaws discovered in this network element.	
1.2.5.157	Management platform must support security containment and recovery as defined in GR-3025-CORE, Issue 1, 07/2001.	**G 1240**
1.2.5.158	System documentation shall specify UDP and TCP ports used on the network side of the OLT to support this feature. (This requirement is to facilitate configuration of firewalls that may be between the OLT and RADIUS server.)	**V 1550**
1.2.5.159	The PON system shall have the capability of preventing subscriber data from passing between other subscribers on the system.	**G 170**
1.2.5.160	The PON system shall support intelligent cross connection between Ethernet interfaces and subscriber data flows.	**G 180**

1.3 - Resiliency, Reliability and Scalability Requirements

As a Service provider, we need to define the resiliency, reliability and scalability architecture of a SDN OLT/ONT solution, so that we can properly plan a production deployment of an SDN OLT/ONT solution.

This will require the following

- Proper resource planning/sizing of virtual machines/containers up to and including testing/validating results.
- The ability to achieve 99.99% availability (Service /Application)
- Clustering (in local data center) and/or diverse instantiation (in multiple data centers) architectures to be defined/tested/validated

Assumptions

- Simply clustering an application might not provide 99.99% service availability due to datacenter reliability.
- Common requirements are met that are provided in EPIC_COMMON.docx

Acceptance Criteria

This will require the following

- Proper resource planning/sizing of virtual machines/containers up to and including testing/validating results.
- The ability to achieve 99.99% availability (Service /Application)
- Clustering (in local data center) and/or diverse instantiation (in multiple data centers) architectures to be defined/tested/validated
- Meet the defined test plan developed. To be delivered 4Q2016

1.3.1 – General Requirements

Requirement ID	Requirement Description 1.3.1 – General Requirements	RFP Requirement ID
1.3.1.1	Installation or removal of any protected hardware of the Network Device shall not impact the functionality of any other Network Device hardware nor system data collection or alarm reporting	
1.3.1.2	Any trouble condition shall not cause the Network Device or any Network Device network resource to get hung and required hard rest of the hung objects.	M 650
1.3.1.3	The Network Device shall continue to function when it loses management communications with the vOLT.	M 680
1.3.1.4	Shall support the association with multiple DHCP servers for failover operation or support a single load balanced address	V 1221
1.3.1.5	Controller architecture shall be scalable.	D 910
1.3.1.6	All virtualized services will operate in a clustered mode.	V 140
1.3.1.7	All services are able to automatically failover to another member of the cluster without impacting the subscriber services.	V 141, V 150
1.3.1.8	Decoupled Applications/Services Applications and services are decoupled from the underlying infrastructure and network. They must be designed with cloud-based scaling and reliability techniques.	V 410
1.3.1.9	The VF design must use cloud-based paradigms to enable standardization of technology, scalability and reliability.	V 610
1.3.1.10	Geo-resiliency and the ability to deploy with local and geo-redundancy should be supported for VFs.	V 650
1.3.1.11	The VF design should meet the resiliency, availability, and performance (e.g.	V 680, V 690

Requirement ID	Requirement Description 1.3.1 – General Requirements	RFP Requirement ID
	real-time response) requirements of the service	
1.3.1.12	Depending on its size and VF requirements for local vs cross-site access, End user data should be replicated to all geo-resilient sites or just to a subset of them. In either case, end user data should be reachable to VFs at all geo-resilient sites.	V 1040
1.3.1.13	If a site or a VF pool at a site fails, the registration state of End Users registered at that site should be available to the VF pool(s) at the geo-resilient sites. (Note: The End users should not have to re-register in this case and should be able to make calls without the need for re-registration).	V 1120
1.3.1.14	The end-to-end service reliability and availability in a virtualized network will greatly depend on the ability to monitor and manage the behavior of Virtual Functions in near real-time rather than relying on reliability and availability of network elements. The ECOMP platform must be able to monitor performance of VFs using the capabilities provided by these resources to pro-actively predict potential issues and resolve them automatically by taking appropriate actions such as restart of the resources or providing additional capacity. The vendor should provide a rich set of monitoring and alerting capabilities for its VFs to facilitate near real-time monitoring and proactive problem resolution.	V 1800
1.3.1.15	The solution must support the ability for AT&T's process (controller) to dynamically add or remove VFC instances to/from a VFC pool (horizontal scaling).	V 2200
1.3.1.16	Scaling should be accomplished by adding or removing instances of a VFC (horizontal scaling), however we recognize that in some circumstances a VFC may need to add or remove resources to an existing instance (vertical scaling). AT&T's direction is to only support horizontal scaling.	V 2210
1.3.1.17	The solution must support deployment of clusters in resource pools where the pool only contains active VFCs. - There must be a query mechanism to list the current members of the resource pool - AT&T manages the resource pool	V 2220
1.3.1.18	Shall provide the limits and restrictions on pool growth given AT&T's stated SLO's.	V 2230
1.3.1.19	Shall support Admission Control features so that excessive traffic does not bring down the entire VF. The VF should notify AIC when this maximum threshold is crossed.	V 2250
1.3.1.20	Resource pools containing VFC instances should support a load balancing mechanism in addition to the discovery mechanism.	V 2260
1.3.1.21	Any VFC instance within the pool shall be able to deliver any and all functionality that the pool provides. The pool member should be transparent to the client. Upstream and downstream clients should only recognize the function being performed, not the member performing it.	V 2270
1.3.1.22	Must provide the following information such that AT&T can determine when to instantiate/terminate a VFC instance. - Engineering rules per VFC instance and runtime levels in a VF pool - Relevant performance usage information - KPI information for capacity, performance and fault management	V 2280

Requirement ID	Requirement Description 1.3.1 – General Requirements	RFP Requirement ID
1.3.1.23	FQDNs (and not IP address) must be supported by the solution for Service Chaining.	V 2290
1.3.1.24	Shall support the ability to scale down a VFC pool without jeopardizing active sessions. Ideally, an active session should not be tied to any particular VFC instance.	V 2300
1.3.1.25	Function-level horizontal scalability should be included in certification testing	V 4300
1.3.1.26	All applications shall be developed, architected or enhanced to support Geo-Redundant clustering	A 19
1.3.1.27	Upgrades shall not have a perceivable impact to the customer's service	A 430
1.3.1.28	Services shall be self-healing	A 610
1.3.1.29	All Subscribers services hosted in a cluster member shall be automatically moved over to an active cluster member in under 5 minutes in the event of a failure.	
1.3.1.30	A VF may consist of several components (VFC's). The performance and reliability requirements apply to all VFC's of a VF. In the description below VF stands for both the VF and its component VFCs.	**V 2500**
1.3.1.31	In the AIC and Domain 2.0 environment, large part of the solution relies upon software, both at the VF level as well as the AIC infrastructure level (OpenStack, virtual networking Open vSwitch, ECOMP, host servers, racks, overlay and underlay network components, etc.). The design of VF's (both the software module and its deployment in a distributed/ redundant architecture) should expect infrastructure and VF software failures.	**V 2510**
1.3.1.32	The design of the VF must leverage elasticity to provide service continuity	**V 2520**
1.3.1.33	The design of the VF must include failure monitoring, failure prevention, failure recovery and fault-tolerance to achieve service continuity.	**V 2530**
1.3.1.34	D2.0 services expect the same level of performance and resilience from VF based services comparable with physical network function based services they replace. Vendor solutions should provide specific deployment configuration (scale-out, scale-up, parameter tuning) to achieve such a parity.	**V 2540**
1.3.1.35	Vendors must provide performance metrics and reliability characteristics datasheets for each VF maintaining similar rigor as used for physical function counterparts.	**V 2550**
1.3.1.36	VF vendor must provide scalability model (for example, how performance changes as a function of workload/processing it can deliver, i.e., number of parallel users allowed, number of parallel VF instances, and concurrent transactions supported at peak).	**V 2560**
1.3.1.37	VF vendor must provide software resiliency limitations. For example, all layer redundancy, application resilient error handling, and system resource optimization.	**V 2570**
1.3.1.38	The solution must support the ability to instantiate and configure a VF such that it is ready to operate and accept traffic within specified time delay	**V 2580**
1.3.1.39	VF updates must not impact VF-dependent service continuity by expecting a service-level "planned downtime".	**V 2590**
1.3.1.40	Performance, reliability and availability of any VF should not be degraded as long as the resource requirements are satisfied by the AIC. Given an end-to-end service availability requirement, The solution must meet availability of the service.	**V 2600**
1.3.1.41	VF deployment models must support both local redundancy and geo-redundancy across multiple locations. The solution should support n+k (where n and k are	**V 2610**

Requirement ID	Requirement Description 1.3.1 – General Requirements	RFP Requirement ID
	specified by AT&T) to meet AT&T's need to deploy VFs in an n+k model without any restrictions.	
1.3.1.42	The vendor must design the VF with the service and engineering rules to meet Service Level Objectives (SLO's). This should include performance latency requirements and administrative functions such as sending log files and performance metrics.	**V 2620**
1.3.1.43	The software design of VF's should incorporate software resiliency principles as they map to standard physical network function methods (as appropriate) for fault tolerance, failure prevention, no single failure, service accessibility control, prioritization, and event-driven monitoring and management of known failure conditions.	**V 2630**
1.3.1.44	The VF software should be designed to be resilient to failures internal to the VF..	**V 2640**
1.3.1.45	Persistence of data in a resilient manner must be addressed for state data, messages and any other permanent data across both local instances of a VF and geo-located VFs.	**V 2650**
1.3.1.46	The vendor software should be designed and developed to utilize redundant pools of resources to achieve high availability. Examples are multiple thread pools, multiple connection pools.	**V 2660**
1.3.1.47	The solution should incorporate robust retry logic to address both downstream service errors and network transport errors. Retry times and intervals should be configurable by AT&T.	**V 2670**
1.3.1.48	The solution should be built to support requests/responses between VF from/to any location both within a Data Center or between Data Centers.	**V 2680**
1.3.1.49	The solution should support multiple version co-existence of VF and interfaces between VF.	**V 2690**
1.3.1.50	The solution should ensure that as instances are scaled up or down those instances can communicate appropriately when that instance is ready to process traffic or when traffic should no longer be routed to that instance.	**V 2700**

1.3.2 –Network Requirements

The requirements in this section are related to the network to ensure that we can support the same quality of service and Service Level Agreements (SLA) that are currently provided to the customers depending on the service that is purchased. The intent is to deploy and architecture that would be highly reliable with minimal customer impact when a failure occurs in the network. The scale in terms of the number of customers impacted during an outage has a direct correlation with the reliability and resiliency. During an outage situation, we have to ensure that we minimize the time required for the customer to come back up. This would imply that all customer policies and configurations would be required to be duplicated to the standby node and the VNF instance that is spawned at the same site or a different site. There are different options that need to be tested as listed below:

1. VNF deployed in one AIC node with dual LCP
    a. VNF deployed in active/active mode across the two LCP
    b. VNF deployed in active/standby mode across the two LCP (resources reserved in the standby LCP)
    c. VNF deployed in active/standby mode with minimal resources reserved in the standby LCP
2. VNF deployed in two AIC nodes with dual LCP
    a. VNF deployed in active/active mode across the two LCP
    b. VNF deployed in active/standby mode across the two LCP (resources reserved in the standby LCP)
    c. VNF deployed in active/standby mode with minimal resources reserved in the standby LCP

Assumptions

- The VNF will be deployed across a minimum of 2 AIC locations each having a minimum of 1 LCP
- The connectivity will be established to a pair of Leafs
- Authentication will not have to reestablished when a link goes down

Acceptance Criteria

- All tests should pass with the latency recorded in all instances and all services.
- The time taken to instantiate a VNF should be recorded as per the options listed above.
- The time taken to instantiate a VNF in the worst case scenario should not exceed 5 sec
- Meet the defined test plan developed. To be delivered 4Q2016

Requirement ID	Requirement Description 1.3.2 – Network Requirements	RFP Requirement ID
1.3.2.1	Failure of PON monitoring VNF will result in an instantiation of another VNF to monitor the OLT	**M 530**
1.3.2.2	The PON monitoring VNF should be instantiated in <5ms in an active mode on the dual LCP in the AIC node	**M 650**
1.3.2.3	Failure of NAL VNF will result in an instantiation of another VNF to support the OLT	
1.3.2.4	The NAL VNF should be instantiated in <5ms in an active mode on the dual LCP in the AIC node	
1.3.2.5	The new VNF should mimic all the configurations for all the customers on the old VNF.	
1.3.2.6	The new VNF should require new VLAN assignment	
1.3.2.7	The new VNF should not require authentication and DHCP assignment	
1.3.2.8	Failure of CvOLT (Control “Plane” Virtualized Optical Line Termination) VNF will result in an instantiation of another VNF to support the OLT	
1.3.2.9	The CvOLT VNF should be instantiated in <5ms in an active/active mode on the dual LCP in the AIC node	

1.4 - Security Requirements

As a Service Provider, we want to insure security measures, such as best practices as well as standards are considered in the development of an SDN OLT/ONT solution, so that this solution can be put into production.

The solution shall provide secured software download mechanism/channel from software repository to OLT hardware driver layer and ONT hardware driver layer.

The solution shall provide mechanism to prevent the subscribers from hacking into ONT from the CPE, such as Residential Gateway, and traverse into the OLT system and into the provider's SDN network.

Assumptions

A standard set of functions is identified and documented for this Standard OLT mode.

Acceptance Criteria

- Provided solution documented and address security standards as it relates to the following areas: Identification
    1. Authentication
    2. Encryption
    3. Access Control
    4. Confidentiality
    5. Security Alarms and Logs
    6. Vulnerability Management
    7. Incident Response
    8. System/Software Integrity
    9. Independent Security Audit.
    10. Standards Compliance *(applicable government and industry-mandated information security standards - not ASPR.)*
- Meet the defined test plan developed. To be delivered 4Q2016

1.4.1 – Definitions

Name	Definitions 1.4.1 - Definitions
"Demilitarized Zone" or "DMZ"	A network or sub-network that sits between a trusted internal network, such as a corporate private Local Area Network (LAN), and an untrusted external network, such as the Internet. A DMZ helps prevent outside users from gaining direct access to internal Information Resources. Inbound packets from the untrusted external network terminate within the DMZ and are not allowed to flow directly through to the trusted internal network. All inbound packets which flow to the trusted internal network originate within the DMZ.
"Information Resource(s)"	Systems, applications, websites, networks, network elements, and other computing and information storage devices, including Mobile and Portable Devices (as defined below) and In-Scope Information stored, transmitted, or processed with these resources.
"Mobile and Portable Devices"	Mobile and/or portable computers, devices, media and systems capable of being easily carried, moved, transported or conveyed that are used in connection with the Agreement. Examples of such devices include laptop computers, tablets, USB hard drives, USB memory sticks, Personal Digital Assistants (PDAs), and wireless phones, such as smartphones.
"Nonpublic Information Resources"	Those Information Resources used under the Agreement to which access is restricted and cannot be gained without proper authorization and identification.
"Sensitive Personal Information" or "SPI"	The data elements listed in the "Table of SPI Data Elements" located at the end of this appendix.
"Security Gateway"	A set of control mechanisms between two or more networks having different trust levels which filter and log traffic passing, or attempting to pass, between networks, and the associated administrative and management servers. Examples of Security Gateways include firewalls, firewall management servers, hop boxes, session border controllers, proxy servers, and intrusion prevention devices.
"Strong Authentication"	The use of authentication mechanisms and authentication methodologies stronger than the passwords required by the applicable requirements herein. Examples of Strong Authentication mechanisms and methodologies include digital certificates, two-factor authentication, and one-time passwords.
"Strong Encryption"	The use of encryption technologies with minimum key lengths of 128-bits for symmetric encryption and 1024-bits for asymmetric encryption whose strength provides reasonable assurance that it will protect the encrypted information from unauthorized access and is adequate to protect the confidentiality and privacy of the encrypted information, and which incorporates a documented policy for the management of the encryption keys and associated processes adequate to protect the confidentiality and privacy of the keys and passwords used as inputs to the encryption algorithm.

1.4.2 - Security Requirements

Requirement ID	Requirement Description 1.4.2 – Security Requirements
1.4.2.1	**Identification** The supplier shall provide a detailed assessment of all functional capabilities for positively and uniquely identifying users to its applications, networks and systems
1.4.2.2	**Authentication** The supplier shall provide a detailed assessment of all functional capabilities for enforcing authentication of users to its applications, networks and systems based on identification information. Based upon the sensitivity of applications, networks, systems and the information handled, the demonstration of multi-factor proof of authentication may be appropriate. The assessment should address any methods by which the supplier retains authentication permissions for remote emergency access to the device.
1.4.2.3	**Encryption** The supplier shall provide a detailed assessment of any encryption-based capabilities designed to improve the security of user or administrator remote access; sensitive information storage, transmission and transfer; system management and administration; and operational system control. The assessment should address key management and cryptographic strength of the designated utilities.
1.4.2.4	**Access Control** The supplier shall provide a detailed assessment of all functional access control capabilities for mediating access to its applications, networks and systems based on documented policy. The assessment should discuss how applications, systems and users gain access rights, including associated approval processes, all periodic access rights review processes and procedures, and how access rights are cancelled, modified or removed when no longer needed. The assessment should document how privileged, administrative and management rights are segregated from the rights of ordinary users, including how the rule of least privilege is implemented and managed. The assessment should address the flexibility and granularity with which policy rules might be enforced or changed during an emergency. It should also include any issues related to the integration and use of firewalls, intrusion detection/prevention systems, and related access filters.
1.4.2.5	**Confidentiality** The supplier shall provide a detailed assessment of all capabilities for ensuring the confidentiality of all personal and proprietary information on a need to know basis. The assessment should include policies and procedures for assuring information confidentiality as information flows between differing applications and systems, and when information is moved off-site to locations not managed or directly controlled by the supplier.
1.4.2.6	**Security Alarms and Logs** The supplier shall provide a detailed assessment of all real-time security alarming and logging capabilities embedded in its applications, networks and systems. The assessment should address real-time issues, as well as compatibility of generated data collection trails with commercial threat management tools.
1.4.2.7	**Vulnerability Management** The supplier shall provide a detailed assessment of how it deals in real-time with the discovery or announcement of vulnerabilities. The assessment should address timeliness issues, as well as customer notification and patch management processes. The assessment should also detail any past vulnerability experiences the supplier might have experienced in this area.
1.4.2.8	**Incident Response** The supplier shall provide a detailed assessment of its incident response capability. The assessment should explain how the supplier supports customer notification, as well as any process explanations that might detail any timelines, data flows, or reporting issues.

Requirement ID	Requirement Description 1.4.2 – Security Requirements
1.4.2.9	**System/Software Integrity** The supplier shall provide a detailed assessment of its processes for ensuring the integrity of its systems and software. Where appropriate, the assessment should document the policies and procedures for ensuring system and software integrity during development and deployment to production, including discussion of all implemented change management policies, processes and procedures. The assessment should include the details of how recurring administrative and operational responsibilities are implemented and controlled, and of how Trojan horse or malicious insertions are avoided during the development, deployment, and usage lifecycle. It should also provide evidence that integrity issues in its applications, networks and systems cannot be exploited to allow unauthorized access or to allow denial-of-service attacks to block access by authorized users.
1.4.2.10	**Independent Security Audit** The supplier shall provide a detailed statement of its willingness to submit to an independent security audit. The statement should include documentation of any previous or existing standards-based certifications and its willingness to provide access to previous audits that might be applicable to its applications, networks and systems.
1.4.2.11	**Physical Security** The supplier shall provide a detailed assessment of all functional capabilities to ensure the physical protection of shared assets by location in a controlled space such as mobile and portable devices and media. The assessment should address how monitoring and logging of access to the controlled space is achieved.
1.4.2.12	**Communications Security** The supplier shall provide a detailed assessment of all functional capabilities and controls for any logical access to non-public infrastructure.
1.4.2.13	**Business Continuity and Disaster Recovery** The supplier shall provide a detailed assessment of all documented policies and procedures to ensure application, network, system and information availability in the event of natural disasters and other unusual events, such as a terrorist attack.
1.4.2.14	**Standards Compliance** The supplier shall provide a detailed assessment of all policies and procedures to ensure compliance with any applicable government and industry-mandated information security standards.
1.4.2.15	**Risk Management and Acceptance** The supplier shall provide a detailed assessment of all documented policies and procedures to ensure risk is adequately managed, especially those risks resulting from non-compliance with documented policies, standards and procedures. This assessment should include discussion of the guidelines for assessing and categorizing risks, the conditions under which risk acceptance is warranted, and how risks are accepted, approved, and where warranted, eventually remediated.

1.4.3 – System Security Requirements

Requirement ID	Requirement Description 1.4.3 – System Security Requirements
1.4.3.1	Actively monitor industry resources (e.g., www.cert.org, pertinent software vendor mailing lists and websites, and information from subscriptions to automated notifications) for timely notification of all applicable security alerts that pertain to Supplier's Information Resources and promptly take action to address them. (Security Alerts)
1.4.3.2	Periodic scanning of Internet accessible and internal Information Resources with industry-standard security vulnerability scanning software to detect unremediated security vulnerabilities.
1.4.3.3	Deploy Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), or Intrusion Detection and Prevention Systems (IDP) in an active mode of operation that monitors all traffic entering and leaving Information Resources in conjunction with the Agreement.
1.4.3.4	Have and use a documented process to remediate security vulnerabilities in the Information Resources and apply appropriate security patches promptly based on potential risk that a given vulnerability is or can be exploited.
1.4.3.5	Assign security administration responsibilities for configuring host operating systems to specific individuals.
1.4.3.6	Ensure that all of Supplier's Information Resources are and remain 'hardened' including, but not limited to, removing or disabling unused networking and other computing services (e.g., finger, rlogin, ftp, simple Transmission Control Protocol/Internet Protocol (TCP/IP) services, etc.) and installing a system firewall, Transmission Control Protocol (TCP) wrappers or similar technology.
1.4.3.7	Change all default account names and/or default passwords.
1.4.3.8	Limit system administrator (also known as root, privileged, or super user) access to operating systems intended for use by multiple users only to individuals requiring such high-level access in the performance of their jobs.
1.4.3.9	Enforce the rule of least privilege by requiring application, database, network and system administrators to restrict access by users to only the commands, data and Information Resources necessary for them to perform authorized functions.

1.4.4 – Physical Security Requirements

Requirement ID	Requirement Description 1.4.4 – Physical Security Requirements
1.4.4.1	Ensure that all of Supplier's Information Resources intended for use by multiple users are located in secure physical facilities with access limited and restricted to authorized individuals only.
1.4.4.2	Monitor and record, for audit purposes, access to the physical facilities containing Information Resources intended for use by multiple users used in connection with Supplier's performance of its obligations under the Agreement.

1.4.5 – Network Security Requirements

Requirement ID	Requirement Description 1.4.5 – Network Security Requirements
1.4.5.1	When providing Internet accessible services have Denial of Service (DoS/DDoS) protection in place. In addition, protect In-Scope Information by the implementation of a network DMZ. Web servers shall reside in the DMZ. Information Resources storing In-Scope Information (such as application and database servers) shall reside in a trusted internal network.
1.4.5.2	Provide a high-level copy of their logical network diagram. The network diagram needs to provide details about placement of information resources and security devices such as (firewalls, servers, DMZ, IDS/IPS, DoS/DDoS, etc.) within the supplier's network.
1.4.5.3	Use Strong Encryption for the transfer of information outside of controlled networks or when transmitting In-Scope Information over any untrusted network.
1.4.5.4	Require Strong Authentication for any remote access use of Nonpublic Information Resources.

1.4.6 – Information Security Requirements

Requirement ID	Requirement Description 1.4.6 – Information Security Requirements
1.4.6.1	Isolate proprietary applications from any other customer's or Supplier's own applications and information either by (i) using physically separate servers or (ii) alternatively by using logical access controls where physical separation of servers is not implemented.
1.4.6.2	Have documented procedures for the secure backup, recovery and destruction of information.
1.4.6.3	Limit access to In-Scope Information only to authorized persons or systems.
1.4.6.4	Have a documented process and controls in place to detect and handle unauthorized attempts to access In-Scope Information.

1.4.7 – Identification and Authentication Security Requirements

Requirement ID	Requirement Description 1.4.7 – Identification and Authentication Security Requirements
1.4.7.1	Assign unique User IDs to individual users.
1.4.7.2	Have and use a documented User ID lifecycle management process including, but not limited to, procedures for approved account creation, timely account removal, and account modification for all Information Resources and across all environments. Such process shall include review of access privileges and account validity to be performed at least annually.
1.4.7.3	Limit failed login attempts to no more than six (6) successive attempts and lock the user account upon reaching that limit. Access to the user account can be reactivated subsequently through a manual process requiring verification of the user's identity or, where such capability exists, can be automatically reactivated after at least three (3) minutes from the last failed login attempt.
1.4.7.4	Terminate interactive sessions, or activate a secure, locking screensaver requiring authentication, after a period of inactivity not to exceed fifteen (15) minutes.
1.4.7.5	a. Use an authentication method based on the sensitivity of In-Scope Information. Whenever authentication credentials are stored, Supplier shall protect them using Strong Encryption. b. When passwords are used, they shall be complex and shall at least meet the following password construction requirements: • Be a minimum of eight (8) characters in length. • Include 3 of the 4 following types of characters: upper-case alphabetic, lower-case alphabetic, numeric, and special. • Not be the same as the UserID with which they are associated. • Not contain repeating or sequential characters or numbers. c. Require password expiration at regular intervals not to exceed ninety (90) days.
1.4.7.6	When providing users with a new or reset UserID, password or other authentication credentials, use a secure method to provide this information.

1.4.8 – Warning Notice Security Requirements

Requirement ID	Requirement Description 1.4.8 – Warning Notice Security Requirements
1.4.8.1	For Information Resource(s) that require authentication allow access to In-Scope Information display a warning notice on login screens/pages that indicate the following: • The service is restricted to authorized users • Unauthorized access is a violation of the law • This service may be monitored for administrative and security reasons • By proceeding the user consents to this monitoring

1.4.9 – Software and Data Integrity Security Requirements

Requirement ID	Requirement Description 1.4.9 – Software and Data Integrity Security Requirements
1.4.9.1	In environments where antivirus software is commercially available and to the extent practicable, have current antivirus software installed and running to scan for and promptly remove or quarantine viruses and other malware.
1.4.9.2	Separate non-production Information Resources from production Information Resources.
1.4.9.3	Have a documented change control process including back-out procedures for all production environments.
1.4.9.4	For applications which utilize a database that allows modifications to In-Scope Information and which support transaction logging, have database transaction logging features enabled and retain database transaction logs for a minimum of six (6) months.
1.4.9.5	• For all software developed under the Agreement, review such software to find and remediate security vulnerabilities prior to initial deployment and upon any modifications and updates. This review and remediation process must include source code vulnerability scanning where such tools are commercially available. • Where technically feasible, for all software used, furnished and/or supported under the Agreement, review such software to find and remediate security vulnerabilities prior to initial deployment and upon any modifications and updates.
1.4.9.6	Perform quality assurance testing for the security components (e.g., testing of identification, authentication and authorization functions), as well as any other activity designed to validate the security architecture, during initial implementation and upon any modifications and updates.

1.4.10 – Monitoring and Auditing Controls Security Requirements

Requirement ID	Requirement Description 1.4.10 – Monitoring and Auditing Controls Security Requirements
1.4.10.1	Restrict access to security logs to authorized individuals, and protect security logs from unauthorized modification.
1.4.10.2	Review, on no less than a weekly basis, all anomalies from security and security-related audit logs and document and resolve all logged security problems in a timely manner.

1.4.11 – Reporting Violations Security Requirements

Requirement ID	Requirement Description 1.4.11 – Reporting Violations Security Requirements
1.4.11.1	Have and use a documented procedure to be followed in the event of an actual or suspected attack upon, intrusion upon, unauthorized access to, loss of, or other security breach involving Supplier's Information Resources

1.4.12 – Mobile and Portable Device Security Requirements

Requirement ID	Requirement Description 1.4.11 – Reporting Violations Security Requirements
1.4.12.1	Use Strong Encryption to protect all of In-Scope Information stored on Mobile and Portable Devices.
1.4.12.2	Use Strong Encryption to protect all of In-Scope Information transmitted using or remotely accessed by network-aware Mobile and Portable Devices.
1.4.12.3	Have documented policies, procedures and standards in place which ensure that any Mobile and Portable Devices used to access and/or store In-Scope Information: a. Are in the physical possession of authorized individuals; b. Are physically secured when not in the physical possession of authorized individuals; or c. Have any In-Scope Information stored on them promptly and securely deleted when they are not in the physical possession of authorized individuals nor physically secured.
1.4.12.4	Prior to allowing access to In-Scope Information stored on or through the use of Mobile and Portable Devices, Supplier shall have and use a process to ensure that: a. The user is authorized for such access; and b. The identity of the user has been authenticated.
1.4.12.5	Implement a policy that prohibits: a. The use of any Supplier-issued Mobile and Portable Devices to access and/or store In-Scope Information unless the device is administered and/or managed by Supplier, and b. The use of any non-Supplier issued Mobile and Portable Devices to access and/or store In-Scope Information, as in cases where Supplier has a "Bring Your Own Devices" (BYOD) program, unless adequately segregated and protected such as by a Supplier administered and/or managed secure container-based solution.

1.4.13 – Security Gateways Security Requirements

Requirement ID	Requirement Description 1.4.12 – Security Gateways Security Requirements
1.4.13.1	Require Strong Authentication for administrative and/or management access to Security Gateways, including, but not limited to, any access for the purpose of reviewing log files.
1.4.13.2	Have and use documented controls, policies, processes and procedures to ensure that unauthorized users do not have administrative and/or management access to Security Gateways, and that user authorization levels to administer and manage Security Gateways are appropriate.
1.4.13.3	At least annually, ensure that each rule was properly authorized and is traceable to a specific business request, that all rule sets end with a "DENY ALL" statement.
1.4.13.4	Use monitoring tools to ensure that all aspects of Security Gateways (e.g., hardware, firmware, and software) are operational at all times. Ensure that all non-operational Security Gateways are configured to deny all access.

1.4.14 – Wireless Networking Security Requirements

Requirement ID	Requirement Description 1.4.14 – Wireless Networking Security Requirements
1.4.14.1	When using radio frequency (RF) based wireless networking, ensure that all of In-Scope Information transmitted is protected by the use of appropriate encryption technologies sufficient to protect the confidentiality of In-Scope Information; provided, however, that in any event such encryption shall use no less than key lengths of 256-bits for symmetric encryption and 256-bits for asymmetric encryption. The use of RF-based wireless headsets, keyboards, microphones, and pointing devices, such as mice, touch pads, and digital drawing tablets, is excluded from this requirement.
1.4.14.2	Regardless of whether radio frequency (RF) based wireless networking technologies are in use by the Supplier, perform scans at least quarterly to detect unauthorized wireless networks and promptly take appropriate action to eliminate them.

1.4.15 –Connectivity Security Requirements

Requirement ID	Requirement Description 1.4.15 – Connectivity Security Requirements
1.4.15.1	If the agreed upon connectivity methodology requires that Supplier implement a Security Gateway, maintain logs of all sessions using such Security Gateway. Such session logs must include sufficiently detailed information to assist with a security incident or a forensic investigation (e.g. identification of the end user or application accessing the system). Such session logs must include origination IP address, destination IP address, ports/service protocols used and duration of access. Such session logs must be retained for a minimum of six (6) months.

1.4.16 –Protection of SPI Security Requirements

Requirement ID	Requirement Description 1.4.16 – Protection of SPI Security Requirements
1.4.16.1	Use Strong Encryption to protect SPI when transmitted over any network.
1.4.16.2	Use Strong Encryption to protect SPI when stored.

1.4.17 – Table of SPI Data Elements

Data elements in the following table are classified as Sensitive Personal Information (SPI) when they apply to an employee, contractor, customer or supplier, except where explicitly stated otherwise and must be treated as such when used in their entirety, unless explicitly stated in the following table. This is true for all data formats including scanned images, PDFs, JPGs, etc

Data Element	Description
Driver's License Number	
Nationally-Issued Identification Number	Includes visa and/or passport values and non-U.S. identification numbers. Excludes U.S. SSN which is a separate data element.
State or Province-Issued Identification Number	Other than Driver's License Number which is a separate data element.
Social Security Number (SSN) **Applies to U.S.[1] only.**	Includes U.S. Social Security Number, and U.S. Taxpayer ID when it is the U.S. Social Security Number of an individual.
Credit Card Number	Primary Account Number (PAN) for all types of credit or debit cards - corporate, personal, etc.
Bank Account Number	Includes all types of bank accounts (savings, checking, etc.), both personal and business in an individual's name. Excludes bank routing number.
Customer Authentication Credentials **Applies to Customers only.**	Values used by customers to authenticate and permit access to: the customers' non-public personal information, including Customer Proprietary Network Information (CPNI) and Sensitive Personal Information (SPI), or an application enabling the customer to subscribe to, or unsubscribe from, services, or a service the customer is subscribed to For example: PINs, Passwords or Passcodes. Excludes Card Security Codes.
Customer Authentication Credential Hints **Applies to Customers only.**	Answers to questions used to retrieve customer authentication credentials, for example mother's maiden name.
Location-Based Information (LBI)	Information that identifies the current or past location of a specific individuals' mobile device. This element contains two factors both of which must be present and able to be associated with each other: 1. a mobile device's location (a map address, or latitude and longitude together with altitude where known) derived from the device's network connectivity and/or positioning system (e.g., GPS), rather than as a result of user action (e.g., email, SMS), and 2. an individual's identity derived from a unique identifier assigned to that mobile device such as customer name, MSISDN, IMSI, IMEI or ICCID.
Date of Birth (DOB)	Full and complete DOB, i.e., including Month, Day and Year. Excludes partial DOB where only Month and Day are used without Year.
Biometric Data	Measures of human physical and behavioral characteristics used for authentication purposes, for example fingerprint, voiceprint, retina or iris image. Excludes templates that contain discrete data points derived from Biometric Data that do not hold the complete biometric image, where the

Data Element	Description
	template cannot be reverse engineered back to the original biometric image.
Criminal History **Applies to *non-U.S.*[2] *only*.**	Information about an individual's criminal history, e.g., criminal check portion of a background check.
Racial or Ethnic Origin **Applies to *non-U.S.*[2] *only*.**	Data specifying and/or confirming an individual's racial or ethnic origin.
Trade Union Membership **Applies to *non-U.S.*[2] *only***	Data specifying and/or confirming an individual is a member of a trade union outside of the U.S.
Information Related to an Individual's Political Affiliation, Religious Belief, or Sexual Orientation **Applies to *non-U.S.*[2] *only*.**	Data specifying and/or confirming an individual's political affiliation, religious or similar beliefs, or sexual life or orientation.
Protected Health Information (PHI) **Applies to U.S.[1] only.**	Includes any health information that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individuals that includes information about: the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual
Medical and Health Information **Applies to *non-U.S.*[2] *only*.**	Information concerning physical or mental health or condition. Includes disability information.

1.5 – ECOMP Information

Enhanced Control, Orchestration, Management, and Policy (ECOMP). The ECOMP framework is the part of the larger Domain 2.0 (D2) ecosystem that is responsible for the efficient control, operation and management of D2 capabilities and functions. It specifies standardized abstractions and interfaces that enable efficient interoperation of the D2 ecosystem.

ECOMP encompasses the instantiation and life cycle management of Virtual Functions (VF) and the cloud platform the VFs reside on – hypervisor, container or bare metal based. We view ECOMP as a more comprehensive solution to what the standards and even open source communities have stitched together.

Assumptions

ECOMP is critical in achieving AT&T's D2 imperatives: increase the value of our network to customers by rapidly on-boarding of new services (created by AT&T or 3rd parties), reduce CapEx and OpEx, and provide Operations efficiencies. The goal of ECOMP is to support full automation in this new paradigm and reduce dependencies on our Legacy Operations Support Systems (OSS).

The ECOMP Platform enables product/service independent capabilities for design, creation and lifecycle management. There are many requirements that must be met by ECOMP to support the D2/ECOMP vision. Of those many requirements, some are key in supporting the following foundational principles:

- The architecture will be metadata-driven and
- policy-driven to ensure flexible ways in which capabilities are used and delivered
- The architecture shall enable sourcing best-in-class components
- Common capabilities are 'developed' once and 'used' many times
- Core capabilities shall support many AT&T Services
- The architecture shall support elastic scaling as needs grow or shrink

1.5.1 – ECOMP General Reference

Reference ID	Reference Description 1.5.1 – ECOMP General Reference	RFP Requirement ID
1.5.1.1	Services shall use Master Service Orchestrator (MSO)	**D 610**
1.5.1.2	Services shall use Service Design and Creation (SD&C)	**D 620**
1.5.1.3	Services shall use Active & Available Inventory (A&AI)	**D 630**
1.5.1.4	Services shall use Data Collection, Analytics and Events (DCAE)	**D 640**
1.5.1.5	Services shall use AT&T Policy system	**D 650**
1.5.1.6	Infrastructure and Network functions shall support control utilizing available/planned shared D2.0 Network Controllers which will use common D2.0 architecture and design templates.	**D 900**
1.5.1.7	VF shall operate as a VM utilizing KVM	**V 148**
1.5.1.8	VF can operate as a Docker container, however the system shall be self-managing	**V 149**
1.5.1.9	Shared Standard ECOMP (Enhanced Control, Orchestration, Management and Policy) services should use ECOMP components including: Master Services Orchestrator (MSO), AT&T Service Design and Creation (ASDC), Active & Available Inventory (A&AI), Data Collection, Analytics and Events (DCAE) and Policy	**V 470**
1.5.1.10	AT&T provided common platform solutions (e.g. cloud-based load-balancers, databases, resiliency solutions, etc.) instead of vendor-proprietary solutions should be supported where possible.	**V 660**

Reference ID	Reference Description 1.5.1 – ECOMP General Reference	RFP Requirement ID
1.5.1.11	Transition to a cloud-based design should be transparent to the end user.	**V 700**
1.5.1.12	VFs must be able to be instantiated and controlled via AT&T provided ECOMP functions. AVF or its component should not interact directly with the OpenStack infrastructure.	**V 710**
1.5.1.13	VFs should run without modifications on AT&T standard guest OS images. Provided guest OS images will be supported with restrictions.	**V 730**
1.5.1.14	The VF package provided must contain the information required by AT&T to instantiate and manage the VF. The set of reusable VFs forms the basis of AT&T's VF catalog that is exposed to service designers via AT&T's service design and creation environment. The VF software lifecycle should be fully automated and allow A&TT to instantiate and use the software on demand.	**V 1430**
1.5.1.15	Test Definitions/Scripts that define how to test the VF and can include all types of testing (functional, performance, load, etc.).	**V 1470**
1.5.1.16	The VF compatibility with AIC and ECOMP must be validated via the Domain 2.0 Incubation and Certification Environment (ICE) initiative using reference and comparable deployments of AIC & ECOMP. Please do note that the validation criteria will evolve over time and will be published in an upcoming reference document. D2 ICE will not certify the specific function of a VF; rather, ICE will focus on validating VF compatibility with AIC and ECOMP. Please submit a request via http://d2ice.att.io or send an email to d2ice@att.com to begin the process.	**V 4000**
1.5.1.17	The software should store all persistent data (logs, CDRs, etc.) in persistent cloud storage Note 1: Persistent data may be stored in a database or as files or object stores. Note 2: Running VMs will not be backed up in AIC. Bringing a VM back up with the configuration required will be accomplished by using appropriate snapshot images or using persistent storage.	**V 4010**
1.5.1.18	The software should have an automated upgrade path for an existing install. This includes OS level security patches on image based solutions.	**V 4020**
1.5.1.19	The software should have an automated downgrade path for an existing install. This includes OS level security patches on image based solutions.	**V 4030**
1.5.1.20	The software must utilize standard AT&T host naming conventions to ensure support teams can easily identify components by name and that all hosts in the solution can be inventoried in all AT&T standard systems.	**V 4040**
1.5.1.21	The software must install on non-root file systems, unless software is specifically included with the operating system distribution of the guest image.	**V 4050**
1.5.1.22	All alerts and error codes that are emitted to AT&T alerting infrastructure must be fully documented. The documentation must include a unique identification string for the specific VF, a description of the problem that caused the error, and steps or procedures to perform Root Cause Analysis and resolve the issue	**V 4060**
1.5.1.23	Supplier will be expected to provide engineering guidelines, capacity & overload test results and dimensioning information as part of the specific service projects.	**V 4070**
1.5.1.24	The solution should provide an automated test suite to validate every new version of the software on the target environment(s) with AT&T tooling. This validation should be run on all new instances to validate proper functionality prior to being put into use.	**V 4080**
1.5.1.25	VFs should provide access to various Test functions that allow AT&T systems to test various aspects of the VF function and behavior. The tests should be of sufficient granularity to independently test various representative VF use cases throughout its lifecycle. AT&T might choose to invoke these tests either on a scheduled basis or on demand to support various operations functions including test, turn-up and troubleshooting.	**V 4090**

Reference ID	Reference Description 1.5.1 – ECOMP General Reference	RFP Requirement ID
1.5.1.26	The software must comply with AT&T's TSS (Technology Strategy and Standards). Any exceptions must be documented and approved for use by each application absorbing the software or the exception must be brought forward as a new TSS standard.	**V 4100**
1.5.1.27	The deployment packages should support multiple versions so that AT&T operations can deploy multiple packages simultaneously	**V 4110**
1.5.1.28	The solution must support a mechanism for AT&T Operations to audit configuration parameters of their VFs	**V 4120**
1.5.1.29	The deployment packages should support environment variable localization with allowance for pre, post JVM args, so that any new JVM args can be managed as a deployment time configuration.	**V 4130**
1.5.1.30	The solution should support the ability to do rolling deployments of components across instances within a site/cluster and across sites/clusters, so that deployments can be accomplished without incurring any downtime to business traffic.	**V 4140**
1.5.1.31	The solution should be delivered completely packaged as one deployable image to speed up deployment time. The image should not require any additional software to be installed on top of the provided image (e.g. minor application releases).	**V 4150**
1.5.1.32	The software must function on AT&T provided infrastructure, including AT&T provided hypervisor, guest OS, and guest OS release certified by AT&T (Note: when the guest OS is packaged with the application, an AT&T certified OS must be used).	**V 4160**
1.5.1.33	The solution must be built on top of an AT&T standard image. Suppliers may not modify the OS (e.g. kernel customization) or make use of proprietary system calls. Performance modifications must not impact AT&T's ability to conduct bulk OS patching. AT&T Admins must maintain ability to manage, support, patch, migrate, and evolve guest OS versions based on the AT&T OS Lifecycle Management policy. Vendor provided guest OS images will be supported with restrictions.	**V 4170**
1.5.1.34	The solution must NOT require privileged user permissions (i.e. root permissions) for installation so ATT Operations can install the product components as a non-root, mechanized-ID (mech-ID) or vtier userID or an application (non-login) user ID	**V 4180**
1.5.1.35	Application should support at least 2 privileged groups - Read-Only (RO) and Read-Write (RW), privileges must not be set locally on VF	**V 4190**
1.5.1.36	The solution must not require privileged user permissions (i.e. root permissions) to run, so that the processes can be run/managed under non-privileged mechanized-ID or application IDs.	**V 4200**
1.5.1.37	All third-party product installations (such as Apache, MySQL, others) should be separated from The software installation so that ATT Operations can install the third-party product components using standard deployment procedures and provide the location of the third party component (such as JAVE_HOME, MySQL-HOME, DB-URL, etc.) to the application.	**V 4210**
1.5.1.38	The solution must use an "installation-root-dir" like environment localization variable/value, so that the software can be installed in an operations user provided install locations and not a hard-coded location/mount point for application component installation location.	**V 4220**
1.5.1.39	The solution should handle a unique transaction ID to be passed from client/consumer of services to enable audit logging to help with transaction traceability and troubleshooting purposes across products and services.	**V 4230**
1.5.1.40	The solution should have dependency analysis built into the deployment package so that it will be easy to detect dependency issues or incompatibilities before deployment into a specific environment.	**V 4240**

Reference ID	Reference Description 1.5.1 – ECOMP General Reference	RFP Requirement ID
1.5.1.41	Must clearly document the solution's versioning scheme so that ATT Operations can plan for the capacity required for support multi-version support.	**V 4250**
1.5.1.42	The solution should not have flash-cut deployments. New versions should be backward compatible or old versions should be available some period of time to allow for client/consumers to migrate to the new version.	**V 4260**
1.5.1.43	The solution should support configuration lock to avoid another process instance trying to update concurrently while a process is updating the configuration.	**V 4280**
1.5.1.44	The solution should have self-healing capabilities where able. The solution should support full automation.	**V 4290**
1.5.1.45	The solution should provide command line interface (CLI) where possible for troubleshooting purposes.	**V 4310**
1.5.1.46	Multiple versions (at least n/n+1) of the same VF should be able to exist at the same time and interoperate to enable software upgrades.	**V 4320**
1.5.1.47	Shall provide Images based on AT&T target implementation (Currently KVM running host/tenant Ubuntu 14.04.4 LTS, Transitioning to Ubuntu 16.04 LTS in 2017)	**A 22**

1.5.2 – Orchestration Reference

In general, Orchestration can be viewed as the definition and execution of workflows or processes to manage the completion of a task. With respect to D2, "Orchestration" is defined as: "The automated implementation of logical and physical resources responsive to a customer or on-demand request to create, modify or remove network and/or service resources. The implementation is automated through the use of service models and policies." Although the orchestration workflow represents a step-by-step process for the delivery or update of D2 services, it also includes logic for gathering of related data and associated policies that may change or redirect the flow of activities along the process.

Assumptions

The following Principles and Objectives pertain to the use of orchestration in the end-to-end Domain 2.0 Architecture:

- Enable/facilitate the dynamic and flexible orchestration of services and the resources that support them.
- Provide automation between OSS/BSS functionality and the ordering, provisioning and operations of virtual function capabilities and dependent physical function capabilities.
- Provide an automation platform that enables dynamic and policy-driven process changes without the need for a 'traditional' IT development project to effect change.
- Consume event-based interfaces to quickly capture and react to Domain 2.0 events.
- Adhere to a common security model across all orchestration processes and interfaces.
- Design orchestration components for extensibility to enable consistent and efficient growth of D2 service/resource types and instances with no or minimal need for re-coding or re-tooling.
- Abstract and encapsulate functionality in modules with clear interfaces in a way that supports evolution of the components.
- Adopt open standards where applicable and appropriate based on scope and levels of industry adoption.
- Design with the expectation of real-time/on-demand or near real-time service execution for both requested and scheduled actions.
- Design for reusability of Orchestration Software components and orchestration process definitions such that processes that span multiple service instantiation and management are defined once and re-used to the degree that reuse is feasible.
- Orchestration Process Design should be easily understandable and readable, be represented by a graphical user interface and be easily modifiable by individuals without software programming knowledge.

Reference ID	Reference Description 1.5.2 – Orchestration Reference	RFP Requirement ID
1.5.2.1	The OLT shall support sub-second failover protection on link in LAG group.	**L 170**
1.5.2.2	The Orchestration platform must support a transaction engine that handles transactions from the operations at the service layer to the actual deployment of configuration changes in the network and or OLT.	**M 1630**
1.5.2.3	The Orchestration platform must support the implementation of network applications and services on a wide variety of networking devices, as well as OLT.	**M 1640**
1.5.2.4	The Orchestration platform must provide a specification of how a network service shall be applied to the network infrastructure (OLT).	**M 1650**
1.5.2.5	The Orchestration platform must support an entire service life-cycle including creating, modifying and deleting service instances.	**M 1660**
1.5.2.6	The Orchestration platform must apply all service changes towards the network as an atomic change-set, using distributed transactions, ensuring that the OLT is always in a consistent state and can automatically recover from failed	**M 1670**

Reference ID	Reference Description 1.5.2 – Orchestration Reference	RFP Requirement ID
	configuration changes.	
1.5.2.7	The Orchestration platform must maintain an accurate and synchronized copy of the network configuration state. Orchestration and management systems can be kept in sync with the network in real-time using the publish-subscribe APIs.	**M 1680**
1.5.2.8	Infrastructure Control will be based on OpenStack from Mirantis.	**M 1840**
1.5.2.9	Keystone will be utilized for key storage and retrieval.	**M 1850**
1.5.2.10	OpenStack Nova will be utilized for configuration and deployment of KVM.	**M 1860**
1.5.2.11	OpenStack Heat will be utilized for configuring the network on the ONOS, OVS, and OpenDayLight.	**M 1870**
1.5.2.12	Images will be stored in OpenStack Glace.	**M 1890**
1.5.2.13	Provide instantiation flows required to implement customer services including templates of the commands and profiles.	**M 1930**
1.5.2.14	Shall provide NBI of REST over HTTPS.	**M 1940**
1.5.2.15	Provided software components shall operate over standard well documented protocols that can interoperate with software component from other suppliers. This applies to both OpenSourced and licensed software	**A 10**
1.5.2.16	Network device will run the OCP ONIE Kernel	**A 500**
1.5.2.17	All NE will automatically locate the NOS installer, download, install and boot to the target NOS	**A 510**
1.5.2.18	Network device should support reinitialization in the event of a catastrophic failure following the ONIE OCP initialization process.	**A 520**
1.5.2.19	ONIE reinitialization will be able to be initiated from the Local Craft and SSH.	**A 530**
1.5.2.20	Components should run in an OpenStack environment	**D 520**
1.5.2.21	Applications, Networks and Infrastructure shall support a design for deterministic closed loop control and automation	**D 800**
1.5.2.22	Implementation shall utilize available/planned common control and orchestration architecture/platform, with architecture which allows migration to target.	**D 810**
1.5.2.23	Comprehensive Automation Applications, Networks and Infrastructure should be designed with deterministic closed loop control and automation	**V 490**
1.5.2.24	Shall provide the ability for automated onboarding of VFs using standards and processes defined by AT&T. AT&T's standards are based on applicable Open source models and industry standards and will be provided in On-Boarding & Running Virtual Function in an ECOMP Framework reference document. A centralized team engagement process or manual installs are not acceptable.	**V 1320**
1.5.2.25	Orchestration Templates - HEAT Orchestration Templates (HOT) shall be provided	**V 1330**
1.5.2.26	TOSCA Models shall be provided	**V 1340**
1.5.2.27	VF Definition – captures key attributes of the VF, such as VF type, KPIs, KQIs, necessary data collection (e.g. for billing attributes), and parameters needed for activation and monitoring.	**V 1440**
1.5.2.28	Descriptions of the configurable parameters and allowable values that drive the VF behavior. Configuration information should be separated out by: − Static/default parameters − Configurable parameters that may need to be modified for VF instantiation on a per service basis − Environment specific configurable parameters (e.g. IP address) − Policy levers/parameters and associated behavior	**V 1450**
1.5.2.29	Well defined scripts to specify the execution process for instantiation, change,	**V 1460**

Reference ID	Reference Description 1.5.2 – Orchestration Reference	RFP Requirement ID
	decommissioning, and auto-recovery of a resource instance.	
1.5.2.30	It is extremely important for AT&T to be able to automatically manage VF life-cycle to fully realize benefits of Network Function Virtualization. AT&T will rely on ECOMP Orchestration to address various VF life-cycle aspects such as Instantiation and configuration, elastic scaling, automatic recovery from resource failures, resource allocation, etc. It is therefore imperative to provide VFs that are equipped with well-defined capabilities that comply with AT&T orchestration standards to allow automatic management of these resources when deploying AT&T services.	**V 1600**
1.5.2.31	Standardized APIs to allow fully automated VM instantiation and configuration of the VF by ECOMP.	**V 1610**
1.5.2.32	Shall provide HEAT templates base on AT&T target implementation of OpenStack (Currently Mirantis OpenStack 7.0)	**A 23**
1.5.2.33	Provide TOSCA models and related scripts for instantiating sub-system components	**A 370**
1.5.2.34	Collaborate with AT&T AIC organization in the development of TOSCA Models	**A 591**

1.5.3 – Policy Reference

Policy is inherently applicable to very broad use in a multiplicity of areas, and purposes. Over time, types of Policy and accepted uses may grow in both number and scope, both within the currently envisioned ECOMP scopes and purposes, as well as beyond these.

Assumptions

- Policy is useful and needed/critical for a variety of important reasons, and the types and scale of Policy uses will expand over time.
- Policy will provide advantages but adds complexity, which must be managed via Framework mechanisms and automation. Policy should do no harm.
- The D2.0 Policy Framework must be unified and integrated, enabling reuse and helping to avoid the risk of possible conflicts. It should not simply emerge ad hoc as disparate islands.
- Policies should be created and validated centrally, then distributed to points of use prior to use.
- Policy should support many owners, each owning and administering their respective policy scopes/content sets. Policies should be easy to create and modify, but appropriately governed.
- Policy should support continual adjustment for discovery, learning, and activation / adjustment / refinement of policies by the various owners / stakeholders (e.g., Operations, CSO, NP&E, etc.)
- It is assumed that DCAE functionality will provide sufficient monitoring of policy influenced behaviors, performance, exceptions, etc. such that policies can be updated as needed.
- Policy will often consider current conditions or state as part of a conditional Policy decision process, so each policy must have access to the information required in its decision process.
- Policy decisions / evaluations will usually be made where (at least the majority of) the required decision information is available. If not, current information required for a policy evaluation must be obtained from a source that has that current information

Reference ID	Reference Description 1.5.3 – Policy Reference	RFP Requirement ID
1.5.3.1	Policy enforcement points - Points in the VF logic where some external control (e.g. turning on a virtual probe or changing an optimization algorithm) is possible either by a real-time change via the configuration agent or use of ECOMP Policy API	**V 1410**
1.5.3.2	Collaborate with AT&T in the development and definition of the alarm thresholds for all hardware and software components of the architecture	**A 24**

1.5.4 – Data Collection, Analytics and Events (DCAE) Reference

The primary purpose of DCAE is the collection, distribution, storage & analysis of data from the managed environment. The results of the analysis performed by the DCAE applications are used in a variety of ways, including enabling:

- Closed-loop response to anomalous network or service conditions by working with Policy & Orchestration subsystems
- Dynamic scaling up and scaling down of virtual network applications, functions, and NFVI resources to ensure optimal use of shared resources
- Operational surveillance of network and service conditions and impacts e.g. capacity, traffic, congestion etc.
- Other functions like real-time billing.

DCAE also provides the infrastructure for collection of autonomous events (e.g. faults, thresholds, state changes including creations and deletions, both from the network as well as various applications that publish events of interest) and making them available to subscribing applications.

Assumptions

- Gather key data and events from a dynamic multi-vendor network,
- Compute various analytics, and
- Enable a set of responses with appropriate actions based on any observed anomalies or defined behaviors.

Dependencies

Data Bus (DMaaP) (Kafka)

A DCAE instance depends on the ability to move data among its internal subcomponents. When required, the DCAE also needs the ability to move data to other external ECOMP components, Big Data applications, etc. This is the driving factor behind the decision to implement both an internal and external data bus.

- The internal data bus must be co-located with the DCAE instance to support low-latency applications. It should be a trusted transport mechanism to ensure data security and delivery assurance and among the DCAE subcomponents, and must support both message-based and file-based data.
- The external data bus must be globally accessible by all ECOMP components. It too should be a trusted transport mechanism to ensure data security and delivery assurance among the various ECOMP components, and must support both message-based and file-based data.

Reference ID	Reference Description 1.5.4 – Data Collection, Analytics and Events (DCAE) Reference	RFP Requirement ID
1.5.4.1	Proposed OLT system shall support measurements of downstream wavelengths transmit power level through SDN and report the power level in dBm unit and the associated wavelength as well.	**L 570**
1.5.4.2	Received optical power level measurements from each ONT shall be measured at the OLT and correspondingly sent to the SDN System. (Power level shall be stated in dBm Units and the associated wavelengths as well).	**L 580**
1.5.4.3	OLT shall generate OAM related statistics that are retrievable from the SDN. The required statistics are: received, relayed, generated OAM packets and byte counts per interface, dropped OAM packets and byte counts with cause code.	**L 2680**
1.5.4.4	Will provide data feeds to Apache Kafka UEB.	**M 1880**
1.5.4.5	Will have capabilities for gzip compression. Included gzip shall support STDIO compression	**V 155**
1.5.4.6	Telemetry Interfaces - Description of the interfaces and messages published to	**V 1380**

Reference ID	Reference Description 1.5.4 – Data Collection, Analytics and Events (DCAE) Reference	RFP Requirement ID
	syslog, messages queue, time series DB, etc.	
1.5.4.7	Shall collaborate with AT&T in the definition and configuration of the local log collection, compression, limits and retention	**A 25**
1.5.4.8	Log configurations to send performance measures to Apache Kafka UEB every 15 min	**A 450**
1.5.4.9	Event configurations to send critical events to Apache Kafka UEB immediately	**A 460**
1.5.4.10	Event configurations to send critical events to SDN controller via NETCONF	**A 470**
1.5.4.11	Provide documentation that details per subscriber data estimates itemized based on the individual sub-system component as inputs to system modelling. Information will need to be revised for updates and additions.	**A 480**
1.5.4.12	Data publisher shall be encrypted over SSL	**HA 510**

1.5.5 – Inventory Reference

Active and Available Inventory provides real-time views of the Domain 2.0 (D2) services and resources. A&AI stores inventory items and a graph of relationships between those items. New items and new types of items will be incorporated dynamically, and with zero touch where possible.

Active and Available Inventory (A&AI) is the component within the ECOMP Execution Environment that provides real-time views of D2 inventory and relationships across resources and services. The views provided by A&AI relate data managed by ECOMP and network applications to form a view of inventory across these applications enabling insights regarding the services and resources used to compose products. A&AI not only forms an inventory of services, and resources, it also maintains up-to-date views of the relationships between these inventory items across their instances and lifecycles. To deliver the vision of the dynamism of D2, A&AI will manage these multi-dimensional relationships in a resilient and automated fashion.

Assumptions

- Delivers basic information about any object (e.g. NE) with ability to retrieve detailed attributes from golden sources.
- Produces accurate and timely views of resource and service inventory.
- Maintains relationships between D2 inventory and other key entities (e.g. location) including Legacy inventory that supports D2.
- Holds historical inventory about recent changes to inventory items, relationship or states within a configurable window of time.
- Reflects state of inventory within ECOMP: active (assigned), available (ready for assignment) and not available (not operational).
  Supplies data for rendering topological relationships such as end to end services chains and service to resource dependency graphs

Acceptance Criteria

Controllers (Infrastructure, Network, Service/Application) interaction with* Active and Available Inventory (*A&AI)

- Controllers will notify A&AI as they make changes in the network cloud, keeping A&AI informed of the resources under their control. These notifications will be done by event publishing.
- Meet the defined test plan developed. To be delivered 4Q2016

Since the controllers are the 'golden' source of resource data and A&AI only has select data, A&AI might query a controller to get additional details when required.

Reference ID	Reference Description 1.5.5 – Inventory Reference	RFP Requirement ID
1.5.5.1	System shall provide details of physical hardware details and topology to centralized inventory system (A&AI)	
1.5.5.2	Shall provide configuration details to centralized Inventory system (A&AI)	
1.5.5.3	Shall provide software inventory details to data collection system (DCAE)	
1.5.5.4	Shall provide firmware versions of all devices to the inventory system (A&AI) and data collection system (DCAE)	
1.5.5.5	Shall provide inventory changes to the centralized inventory system (A&AI) and provide logging notification to the data collection system (DCAE)	

References

There are no sources in the current document.