V-OLT XGS PHASE-3 EVALUATION TEST PLAN

Lab Entry Requirements and Insight for Suppliers Participating in the Virtualized XGS-PON Evaluations

Edition 3.1
May 16, 2017

Information herein is a "Contribution" submitted under ONOS Agreement between AT&T Services, Inc. and Open Networking Laboratory dated 1/16/14

Document Contributors

Authors	
Reviewers	TBD

Document Change Log

Revision	Date	Author	Change

Contents

Table of Figures

1 Introduction

The evaluation methodology employed for the XGS project approximates an agile process. As such, while this document attempts to be as exhaustive as possible, users of this document should understand that just like the XGS project itself, this is a living document and hence, will be revised as needed to include updated and new information, as that information becomes available.

Phases of the XGS-PON vOLT Evaluation:

- Phase-1: Self-contained POD configuration with no connections to Lab Network
- Phase-2: Integrate POD at network layer with network representative of production network
- **Phase-3: Dry run for field trial / PoC, with POD software installed on Lab's production grade compute**
- Phase-4: Field trial in carrier's production environment with live (friendly) traffic

This document describes the plan for the Phase-3 Evaluation, including lab entrance requirements and expectations, durations, network topologies, logistics, etc. While this document is intended to be comprehensive, it does not preclude or invalidate other documents and documentation sources. All current and potential issues and road blocks shall also be disclosed in advance of the Evaluation, during the bi-weekly sync-up meeting between carrier's XGS-PON team and Supplier participant.

High-level test outlines are also included in this document to provide the evaluation participants the guidance of the level of the evaluation to be expected during the lab evaluation.

1.1 What's New/Changed in Phase-3

The following is a not quite exhaustive summary of new and changed items in Phase-3:

- Migration from POD to carrier grade Compute (and other) supporting infrastructure
- The SSM template has been updated. The revised template can be found in Appendix A.
- All equipment must be DC powered for user in the Central Office environment
- Timing, Chronological – New dates for Phase-3 Evaluations and the Trial
- Hardware - Must be production deployable
- Scalability – Initial Outlook and Verification Plan
- TR-69 RG Management Transport – RGs must be manageable via Client Management System
- Alarm and Condition Configuration and Reporting – Must be configurable
- Production security requirements
- Distribution Images – SSM and repositories must be cached
- Restartable in Isolation - All subsystems need to be restartable without Internet access
- Production Images – Lab verified images need to be captured for replication & deployment
- Privileged Command Segregation – All privileged command usage must be identified
- Registration Method – Phase-3 will utilize pre-assigned ONU serial numbers and ONU_IDs
- Backup and Restore – System configuration shall be transferable to a removable medium
- ONU/ODN Topology – The Phase-3 Evaluation shall utilize 9 Supplier provided ONUs

- OLT/ONU Interoperability – Demonstrate ONUs are able to work on all vOLT MA Hardware
- Least Privilege Principle – Shall be applied
- User Accounts – Application level accounts and such, need to be formalized
- ONU Pre-provisioning – Is now required
- Persistent storage of provisioning – Must be maintained indefinitely
- OpenOMCI – A stretch goal in Phase-3 and forthcoming requirement
- Checklist / SoC – This required submission is a convenient way to track Phase-3 requirements
- System-Level Configuration – Furnished to allow advance configuration by the Supplier
- User and Service-Level Configuration – Furnished to allow advance configuration by the Supplier
- Performance Management – Some level of PMs need to start being provided by the vOLT Solution
- Software/firmware upgrade strategy and capability – Including patches
- Compute Solution and Software Installation - Carrier to Supply Compute
- Supplier Technical Support and Escalation Strategy – Record in Appendix D
- Provisioning Strategy – Solution provisioning will be provided in advance
- CO Deployment Requirements – NEBS, etc. are Required
- Roles and Responsibilities – Who's supplying what, who's doing what, etc.

1.2 From Phase-2

- HW venders who are currently using Broadcom Maple B0 eval box or FPGA based solution must provide the near deployable product based on OCP submission of the XGS-PON Soc specification before the conclusion of Phase 3 of PoC testing.
- The goal is to have ONOS/VOLTHA as the XGS-PON vOLT software for carrier implementation.

The following is a brief summary of the 4 phases of the XGS-PON vOLT Evaluation, the first 3 of which have or will, be performed in DVL's Austin Lab.

1.3 Phase-1 Summary

The Phase-1 Evaluation provided an initial assessment of the state of the hardware and software components of the vOLT application. Suppliers submitted self-contained solutions where the data sources, such as IPTV video streams, were originated in components included with the system under evaluation.

Focus was on the ability to range ONUs on the PON, PON through-put and PON optical performance.

Management functions (i.e. FCAPS) were not evaluated.

1.4 Phase-2 Summary

The Phase-2 Evaluation provided an initial assessment of the ability to integrate the vOLT Solution with Carrier's High-Speed Internet Access (HSIA), IPTV video service, RG CPE and low-level OSS infrastructure (e.g., RADIUS and DHCP).

Focus was predominantly on ability to interconnect and interoperate with carrier's Lab infrastructure.

For Phase 2 testing, it is to verify that the XGS-PON vOLT/ONT software and hardware will successfully pass the production High-Speed Internet traffic, IPTV Multicast with functioning IGMP Join/Leave to approved RG and STB. cVoIP support will also be verified when time allowed.

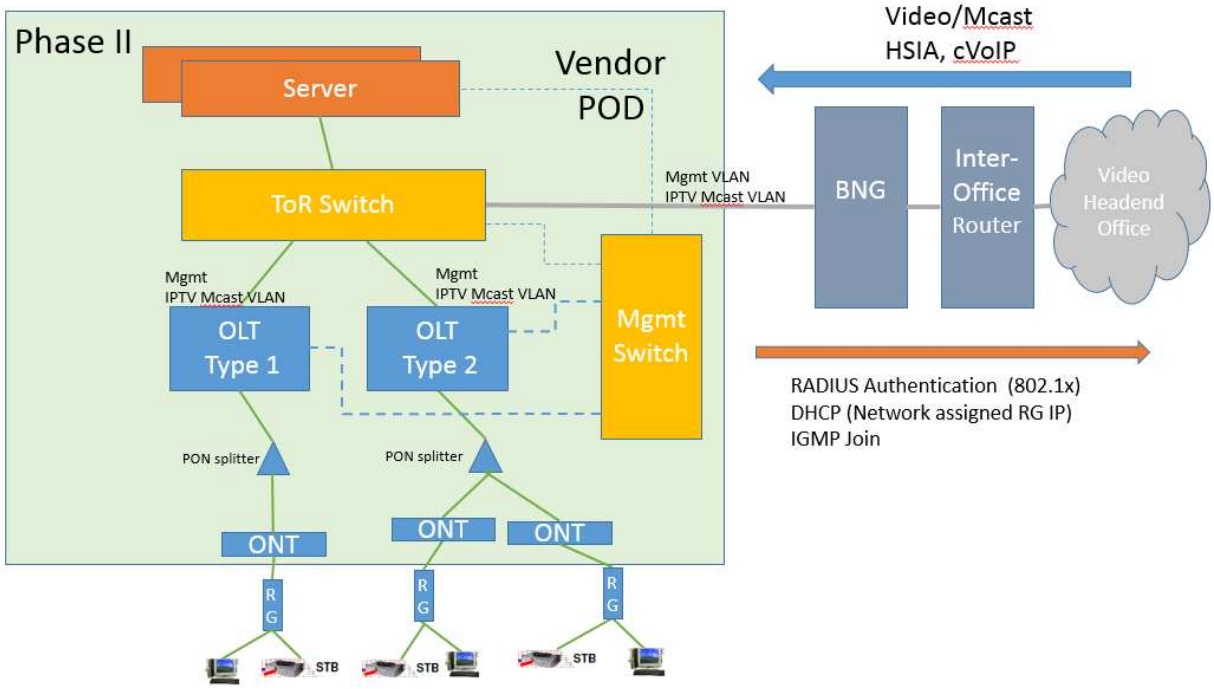


Figure 1: High Level Topology of the POD Layout and Network Connection

The OLT Whitebox may be connected to BNG directly as one of the options for Phase 2 and Phase 3.

1.5 Phase-3 Overview

As previously stated, Phase-3 is the "dress rehearsal" for the actual PoC, which will be a trial performed in the field, connected to the production network and using live traffic, albeit with "friendlies".

Phase-3 and Phase-4 are interrelated in that the requirements are ostensibly the same, where Phase-3 is intended to validate the functionality and Phase-4 is intended to demonstrate it in practice, in the field.

Please note, Phase-3 is critical path to Phase-4; even though Ph-3 will be in a lab, deficiencies at Ph-3 that would critically impact Production will have to be mitigated before proceeding to Ph-4. In other words, if something doesn't work in the lab, we don't want to have to fix it in the field.

High-level Objectives

- Demonstrate solution is can go to the field for trial
- Familiarize TAC w/ Trial Solution

All field trial requirements apply to the lab in Phase-3, so as to validate all functionality in advance of bringing a Solution to the field.

Synopsis of Phase-3 Services to be delivered

Turn up small quantity of XGS-PON-based Multi-gigabit (XGig) service trial subscribers with:

- XGig HSIA
- U-verse video
- cVoIP voice service (potentially)
- ~~POTS voice service~~

on an XGS platform for a finite span of time, in-region, in a realistic operations environment that closely models the demands of the production environment

Timing, Chronological: Phase-3 lab testing will be performed <fill in dates here>. The field trial is targeted for <fill in month or quarter here>.

Given the compressed schedule and nature of the project, certain high-level requirements are not expected, such as flow-through provisioning for OSS/BSS integration. However, more general requirements, such as NEBS-3 are an intrinsic part of deploying equipment in a CO, and cannot be avoided.

In lieu of flow-through provisioning, the provisioning strategy is to provide datafill to Suppliers in advance. This information will be provided in Appendix B and in Appendix C. Suppliers will use this information to configure their Solution.

Phase-3 requirements must be met for a solution to successfully complete Phase-3. In order for a solution to enter Phase-4, it must first successfully complete Phase-3.

2 Prerequisites for Evaluation

The following sections describe the minimum requirements to start Phase-3 evaluation. The intent behind this requirements is to help ensure the PoC turn-up goes as smoothly as possible, and since Phase-3 involves live traffic, that once the PoC begins it will be maintainable and manageable.

2.1 Lab Entrance Requirements

The following items must be provided at last 1 week in advance of the start of the trial. This is to allow sufficient time for review of the material by the Lab Engineering staff.

- <list here>
- Minimum required h/w quantity
- As suggested, two (2) PON hardware variants should be employed (4 in total)
- Documentation and Manuals
    - Scalability Strategy and Plan (does not have to be implemented; just want to know the plans to support scalability, and to test it)
    - The SSM template has been updated. The supplier shall provide their updated SSM. The revised template can be found in Appendix A.

  The supplier shall continue provide the following documentation prior to the day of assigned lab evaluation starting date.

    - *Updated POD topology and connection detailed diagram, if any changes from previous setup*
    - *Vendor internal test cases, test scripts and test reports*
    - *CLI Command guides and Configuration Guides*
    - *Product manuals and User Guides*
    - Scalability – Initial Outlook and Verification Document

  The Supplier shall describe initial assessments of their Solution's scalability, including system maximums in both dimensions and throughput, as well as their plan and methodology to test and certify their Solution for its scalability targets.

- Hardware
    - Migration from POD to carrier grade compute (and other) supporting infrastructure

      Phase 3 Lab evaluation will decompose the vendor provided POD used for Phase 1 & 2 testing. The Lab host will supply bare metal Compute resources, and a connection to BNG.

      The supplier shall provide the XGS-PON OLT hardware with two or more OLT hardware variants, as specifically communicated separately from this Test Plan document.

- Software
    1. *Supplier shall provide detailed on software stack and software delivery mechanism.*

    2. *Software Requirement, but not limited to*
        - *OS: Ubuntu 14.04.4 LTS*
        - *Hypervisor: KVM*
        - *Docker*
        - *Infrastructure controller and Orchestrator for Hypervisor and/or Docker*
        - *SDN Controller (ONOS)*
        - *VOLTHA with current code release 1.0*

2.2 Support Infrastructure

The XGS trial will be monitored 24 hours a day by Operations organizations. Therefore suppliers need to demonstrate the ability to provide escalation support for Operations, to assist in the recovery of an emergencies, such as a system outage or degradation.

Support Infrastructure includes not only a designated support group, but also the following items:

- Business Hours Contact List
- Emergency Escalation Plan, including key contacts and reach numbers
- Remote Access Plan; Lab staff will work with Suppliers on this item
- Committed Response Time(s), based on situation impact
- Agreed Resolution Flow, Including Updates on Hot Issues

Suppliers should outline which of the Supplier's organization(s) will be providing technical support 24/7, where to contact them and how to request support.

Suppliers should also outline their customer escalation plan, including names and contacts for each level in the plan.

This information should be entered in the Support Contact and Escalation Template provided in Appendix D.

3 Network Integration and Element Requirements

Unlike the previous evaluation phases which integrated solely with lab infrastructure, Phase-3 will integrate with the live Production network and therefore have to meet many of the production requirements.

A checklist / form shall be submitted as a statement-of-compliance (SoC), but can also be used as a high-level checklist to help ensure critical requirements are being addressed.

The SoC should be completed and submitted at least 1 week prior to lab entry.

3.1 Equipment and Other Material

3.1.1 Roles and Responsibilities

Who's supplying what, who's doing what, etc.

Suppliers should assume the lab will provide:

- Compute
- BNG
- RGs
- STBs
- -48V DC power

Suppliers should provide all addition material required.

If there are any questions in this area, please address them to the contacts provided in Appendix E.

3.1.2 vOLT MA Hardware

Duplicated components are required.

The physical Media Adaptation (MA), xPON terminating hardware, shall be provided in pairs for Phase-3. In other words, for every variant of hardware used in the Evaluation, 2 physical, identical units, shall be provided.

For multi-port units, a quantity of 4 XGS-PON terminating transceivers shall be supplied for the primary unit. The secondary until does not require its own optics.

In the case of vOLT MA hardware with atomic granularity (i.e. single-port), a quantity of 4 XGS-PON terminating units shall be supplied. No secondary units need be supplied for atomic hardware.

The general intent in the secondary unit is to provide a warm spare for the primary. This ensures that in a worst-case scenario, there will be no lead time to obtain an additional unit. The intent is also to provide a reference unit for comparison, for the cases where the hardware is suspect, but not proven as a factor.

During the trial, the secondary until shall be cabled, energized, loaded and registered, such that the PON and NNI fibers (or DAC) can be swung over to it, and it can be immediately restored to service. This exercise shall specifically be performed during Phase-3 testing.

Specifics regarding the hardware, embedded software and driver/adapters for Broadcom-based Solutions will be provided in a separate communication, and the requirements stipulated in that communication are incorporated by reference into this Test Plan.

3.1.3 ONU / ODN Test Bed Hardware and Design

The Phase-3 Evaluation requires the Supplier to provide 9 ONUs for testing, and the other supporting items described below, and otherwise required to operate the ONUs with the OLTs in various permutations (e.g., splitters, fibers, power supplies, etc.).

The system provided by the Supplier for the Phase-3 Evaluation shall include 9 ONUs, configured as 3 groups of 3 ONUs. Each group of 3 ONUs shall be coupled to the first 3 ports of an 8 (or more) port splitter. Each of the 3 splitters, plus a fourth splitter of 8 or more ports, shall be coupled to various terminations during evaluation.

The intent of this ODN configuration is to allow as many as 9 ONUs to be coupled to a single PON, or as few as 3 ONUs to be coupled to as many as 3 PONs. Other permutations may be utilized, as situations warrant.

The following diagram depicts the ODU/ONU testbed topology.

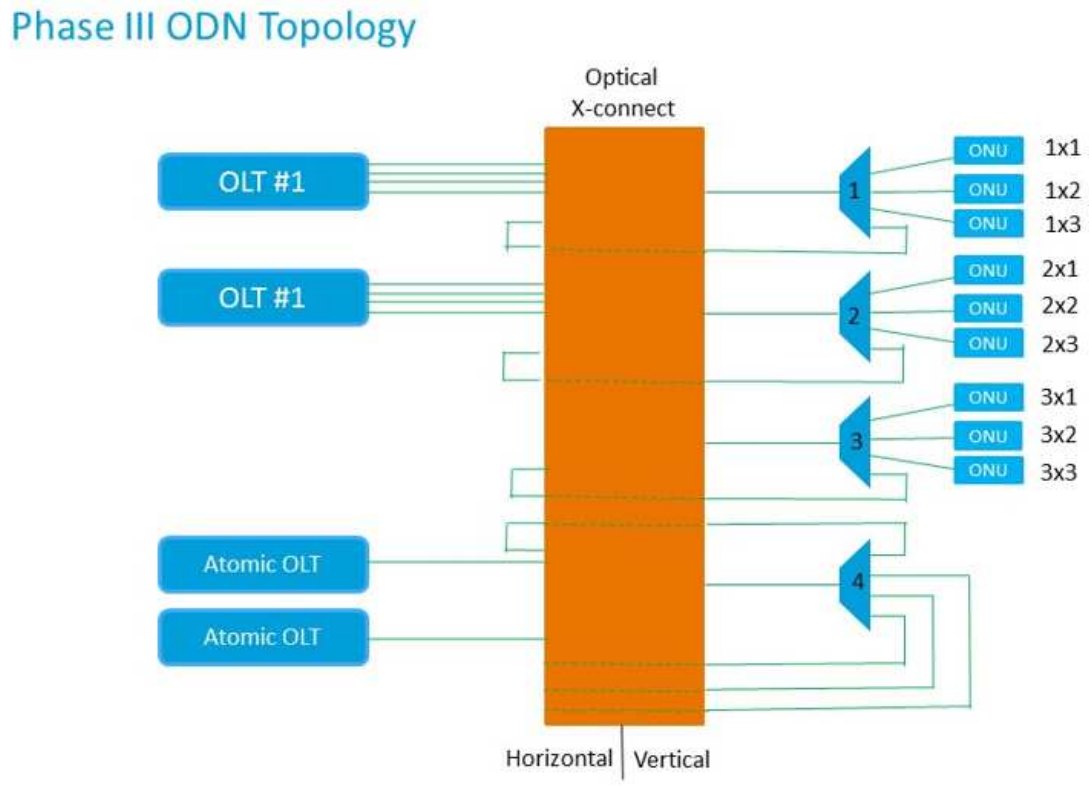


Figure 2: ODN/ONU Testbed Design

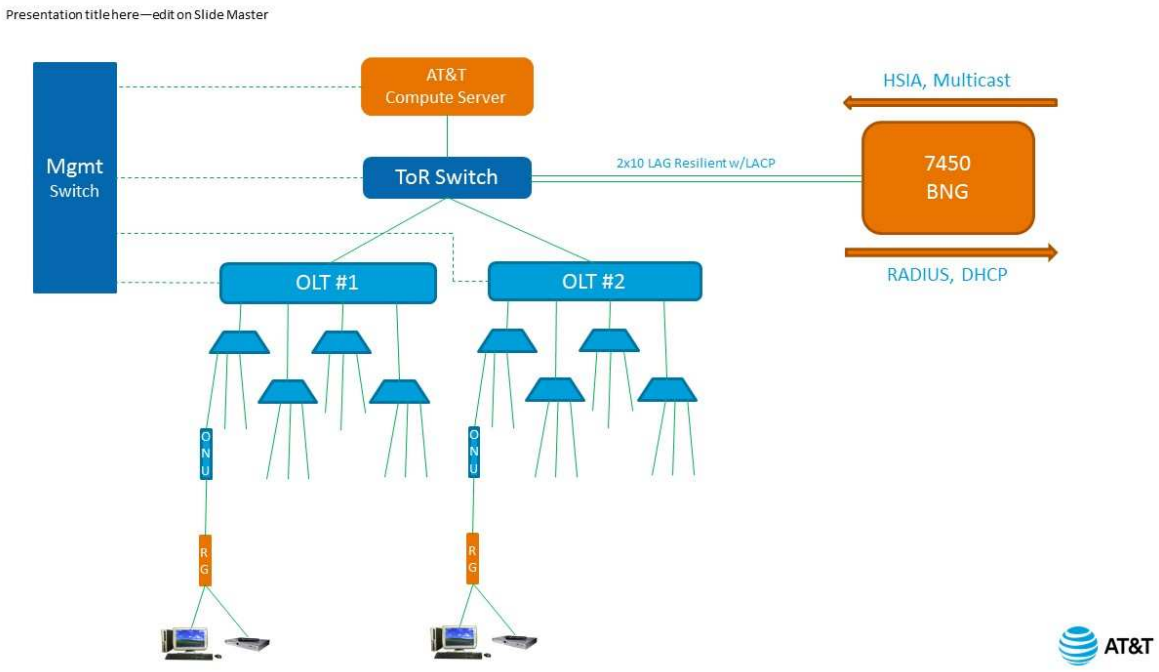
3.2 Physical and Logical Interface Requirements

<Diagrams and connections here>

3.2.1 XGS vOLT High-Level Design

The following diagram depicts the high-level topology for the Phase-3 XGS Evaluation:

Figure 3: XGS vOLT High-Level Design



Note, the ODU/ONUs depicted are for reference only. Refer to the ODN/ONU Access Section for detailed information relating to that area.

<Descriptive text here>

3.2.2 TR-69 RG Management Transport

RGs must be manageable via Client Management System (CMS).

The vOLT Solution shall transport TR-69 to allow remote management of the RGs. This should not introduce any new requirements on the Solution, but was not validated in previous phases.

3.2.3 OLT/ONU Interoperability

Stretch Goal: Demonstrate ONUs are able to work on all vOLT MA Hardware variants

All ONU variants included in Phase-3, should be tested against all OLT variants included in Phase-3, and determine if they "work". Working is defined as, they range, activate, can be provisioned with HSIA and other Services, and those Services are fully usable by subscribers, as the Services are intended to be used.

For clarification, in the case of IGMP, *working* constitutes being able to tune a STB to a channel and watch it for any arbitrary length of time. The following provides some examples to illustrate:

- Can tune to a channel and see 10 seconds of video, then freeze // Not Working
- Can tune to a channel and see 300 seconds of video, then freeze // Not Working
- Can tune to a channel and as long as you change channels every few minutes, can watch video // Not Working
- Can tune to a channel, and watch it for as long as you want (20 mins or more) // Working

3.3 Cloud/Compute Environment

The Lab will provide the Compute component for Phase-3. These will consist of some incarnation of x86 servers, suitable for use in the CO environment. It is host's intent to perform the install on these servers, as well.

The specific server to be used in the trial has not been finalized at this time, but the key things to know for Phase-3 is carrier's intends to supply them, and that Lab engineer's intends to install the Supplier software, with Supplier support. Lastly, that they will be modern x86-based servers, and that there isn't a significant amount of variance from server to server, irrespective of the specific make and model,

If your software has any dependencies on particular server hardware, please identify those requirements as quickly as possible and provide to the lab.

Please provide your software's minimum x86 physical requirements, as well. This should include minimum amount of RAM, number of cores, amount of disk space, etc.

The intent is to provide servers that are single-socket.

<Diagrams and connections here>

3.4 CO Deployment Requirements

As Phase-3 is a dry run for the trial, it will apply the same physical requirements as will the trial. The carrier is working to identify the specific, applicable requirements, and will supply them as soon as they are finalized.

One significant requirement that is well known is that all equipment will need to be DC powered, and operate from a nominal Office battery supply of -48V DC. Equipment should be capable of operating for an indefinite period of time at up to -56 volts (aka high-float), and down to -42V (aka low-voltage disconnect or trip).

Trip is not guaranteed at -42V, so if Supplier equipment is receiving battery voltage outside of its permissible operating range, it should shut itself down and should ensure it prevents damage. While the chances of experiencing a low voltage scenario of extremely small, it may be seen in the event of a commercial power failure, and if for some reason backup generators are not present or fail and the batteries run down.

The relevant Telcordia GRs and TP documents should be consulted regarding DC powered equipment in the Central Office, and supersede any information provided herein.

<Power, thermal (dissipation), physical, airflow, TP-762123456, etc. here; references in Appendix F>

3.5 Security Requirements

3.5.1 Security Policy Requirement (SPR) Compliance

Servers connected to any Production Network(s) must comply with operators' requirements, and are regularly audited. Security Policy Requirement (SPR) primarily applies to 3 major areas:

1) Server attack surface area
2) Server resident agents
3) Supplier process

A server's attack surface area includes, but is not limited to, such things as open ports, use of unencrypted protocols, processes, groups, files, users, etc. and their associated privilege levels, etc. Servers are routinely scanned for vulnerably that are identifiable from an external vantage point, and without credentials. For example, an open telnet port, or an interface advertising its application and release level.

Resident agents are supplied by Security Office (SO) and must be installed on machines connected to the network. These agents report vulnerabilities from an internal vantage point.

Supplier Process proactively addresses security vulnerabilities by ensuring best-practices are employed during the development and support phases of a product's life cycle. This includes a wide range of areas, such as not implementing backdoors, not having hard-coded passwords, etc.

This Test Plan incorporates SPR by reference.

3.5.2 Privileged Command Segregation

Privileged commands used for installation need to be isolated and run manually. All privileged commands for maintenance need to be de-escalated. All privileged commands invoked during startup shall be removed; any use of suid needs to be documented and approved.

Commands, including anything that executes with elevated privileges, are generally employed in 3 different categories of activities:

- Installation
- Instantiation
- Maintenance

Installation: All commands invoked during installation should be segregated from all other installation commands, scripts, activities, etc., and should be identified and documented, such that they can be invoked manually by the deployment installation responsible party. Scripts should NOT run with elevated

privileges, and commands requiring elevated privileges should be minimized. During software installation, these specific commands will be invoked and tracked through sudo. Sudo'ing to a shell is not permissible.

Instantiation: The vOLT application, inclusive of all subsystems required to provide full Solution functionality, shall be automatically instantiated. In the event of the untimely death of any of these processes/subsystems, the Solution shall automatically re-spawn the failed component. When these processes are spawned or re-spawned, they shall operate with user-level privileges, in their own or an appropriate group. Any components that require elevated privileges for normal operation shall be clearly identified and provided with a detailed explanation, which will be considered for approval by the appropriate SMEs. No executables shall have their suid attribute set, without appropriate approval. In short, nothing should require elevated privileges for normal operation.

Maintenance: Any vOLT Solution-specific user commands or tools that require elevated privileges, shall be identified and documented. Ideally, there shouldn't be any. Note: This is not intended to include general OS commands that require elevated privileges (e.g., ifconfig, ifup, ifdown, etc.).

<Table of commands, scripts, etc., requiring elevated privileges>

3.5.3 Least Privilege Principle

Users, programs, processes, groups, files, etc. shall be assigned the minimum privilege levels required to perform their assigned function.

Sudoers list command entries shall be provided for functions (i.e. users) requiring elevated privileges.

3.5.4 User Account Formalization

User account names, group names and file ownership shall be formalized and reasoning for any elevated privileges (e.g., sudoers list entry) documented.

3.6 Provisioning

3.6.1 System-Level Configuration

The System-Level Configuration form is provided in Appendix B to specify global parameters which must be configured by the Supplier on the vOLT Solution. Note, this form does not address user/ONU-specific configuration.

3.6.2 User and Service-Level Configuration

The User and Service-Level Configuration form is provided in Appendix C to specify per-user parameters which must be configured by the Supplier on the vOLT Solution. Note, this form does not address System-Level configuration.

3.6.3 ONU Pre-Provisioning

As described in Section 3.7.6 PON Registration Method, support for (pre-)provisioning of ONUs, their serial numbers and ONU_IDs (and configuration), is required. While the term pre-provisioning implies provisioning of an ONU which is not physically connected to the PON and powered at the time of provisioning, it is effectively the same as an ONU that was previously connected to the PON and provisioned, yet at some time subsequent to that, has been disconnected from the PON, from power, or both, and may at any moment be reconnected (i.e. may range).

3.6.4 Persistent Storage of Provisioning

Persistent storage of provisioning must be maintained indefinitely.

In the event of any category of restart, of any vOLT Solution subsystem, including hardware, software and NFVI, up to and including complete power cycle of entire network, the Solution shall be restartable and retain the exact configuration it had prior to the restart(s).

The recorded configuration shall always be manipulated such that its integrity is ensured, even in the event of a disruption that interrupts a write access to the non-volatile medium.

Under no circumstances shall the vOLT Solution fail to recover from any type of restart, induced for any type of reason, autonomously. Recover is defined as resuming to provide its intended, configured Service(s).

3.7 General Requirements

3.7.1 Software Distribution Media/Images

All software identified in the SSM and repositories must be cached.

The vOLT Control Plane may have limited, or no access whatsoever to the public Internet. As such, all software identified in the SSM, as well as all repositories required to support the identified software, must be included in the distribution image(s) provided by Suppliers, identified in the distribution media's manifest, and furnished with cryptographic hashes to detect corruption and/or tampering.

The manifest should be signed.

3.7.2 Software Images for the Production Network

Lab verified images need to be captured for replication & deployment during Phase-4 and must be under strict version control.

As the XGS Solution moves closer to production, stricter controls will required to prevent regressions. Recognizing an agile process adds a lot of value by speeding delivery, once a Solution is delivered and in Production, agile process must be controlled to ensure it doesn't undo its value.

When a Solution is accepted into the lab for Phase-3, its composition must exactly match the SSM. **Strict version control will be adhered to from that point forward**, and all changes must be reported and documented.

A Solution exiting the lab for Phase-3 and approved for Phase-4, must be imaged. **At the point the image is taken, all further changes are to be locked out.** This will ensure what is deployed in the field is the same as what is in the lab, is the same as what is in the Support lab, etc. In the event of a critical defect, given the appropriate approval, a patch can be introduced into the SSM, to resolve the issue.

3.7.3 Restartable in Isolation

All subsystems must be restartable without Internet access.

The vOLT Control Plane may have limited, or no access whatsoever to the public Internet. As such, all system components must be restartable at the lowest/most severe level of initialization (e.g. power cycle), in an isolated or captive environment. Therefore, all dependencies for restart must be resident and available.

3.7.4 Alarm and Condition Configuration and Reporting

The Alarm and Condition configuration and reporting of the OLT/ONT must be configurable. This includes the configuration of alarm severity, alarm suppression, alarm acknowledgment and alarm clearing.

3.7.5 Backup and Restore

System configuration shall be transferable to a detachable physical medium, such as a thumb drive or offsite ftp server, in the form of a file. A system running on the same release as that which created the backup, shall be capable of ingesting the file and adjusting itself accordingly (aka restoring), such that its configuration exactly matches that of the system that originally generated the backup.

3.7.6 PON Registration Method

Phase-3 will utilize Registration Method A <confirm>

A form will be provided in Appendix C which specifies the provisioning of the ONUs for Phase-3. A field is provided in each tuple for the Supplier to populate the ONU serial number corresponding to each ONU_ID. The vOLT shall bind each ONU_ID to the physical ONU and its intended datafill via its serial number.

When an ONU ranges that has been assigned a serial number matching one specified in the table, it shall be assigned the corresponding ONU_ID and configured appropriately.

The Solution shall be configurable to allow (or deny) "auto-registration", whereby an ONU that ranges but does not present a known serial number, shall be assigned an available ONU_ID and provided a default configuration. It is envisioned that auto-registration would only be used in the lab, to assist with initial turn-up of a node.

Request for, and qualification of, a "PLOAM Password" or Registration ID by the vOLT is not currently required by the Phase-3 use-cases.

3.7.7 Software/Firmware Upgrade Strategy and Capability

A strategy and capability to perform in-service software and firmware upgrades, including patches, must be provided.

Persistent configuration present at the time of an upgrade must remain intact following the upgrade. In the event an upgrade or patch alters the configuration data schema, mechanized reformat procs must accompany the new software to facilitate conversion of the database to the schema utilized by the new software.

Any upgrade process/scripts must, as a first step, perform a full backup and record the state of all equipment in inventory, as well as all standing alarms.

3.7.8 High-Availability

Suppliers' vOLT Solution must provide a High-Availability platform, where no single point of failure can result in a system outage or degradation, unless the single point of failure is imposed by the hardware and it is not technically feasible to provide redundancy in that hardware. Similarly, all software is to be redundant and offer the ability to switch to switch-over to the redundant instance in 50ms or less, with the exception of certain software instantiated on embedded hardware, that cannot be duplicated (e.g., the OS).

The HA strategy will be refined over time, and Suppliers are encouraged to propose HA Solutions for the platform.

3.8 Commissioning Requirements

This section is intended to describe the procedure and criteria for determining that a new deployment of equipment and software have been properly installed, and are fully functional.

3.9 OpenOMCI Interoperability

Compatibility with OpenOMCI is included as a stretch goal and a foreshadowing.

Ideally, the variant of OMCI utilized by the vOLT Solution should be OpenOMCI. This will become a requirement at some point in the future.

3.10 Software Version Control

As discussed above in the Software Images Section, deployment candidate software entering the lab, and software approved for deployment by the lab, both need to be under strict software version control, with appropriate collections of modules being issued a “build” number (or equivalent), that identifies the content of the “build”.

How build numbers are assigned, and what constitutes a build for any given subsystem is still under deliberation. Suppliers are encouraged to propose solutions for software versioning in this Application.

4 Phase-3 Test Coverage

The purpose of this section is to provide insight into the areas the carrier intends to exercise and evaluate during Phase-3. This list is intended to be extensive, but not exhaustive, so testing will be performed in other areas as well. As this Evaluation has not reached Production-level testing, detailed TCs have not been defined yet.

4.1 Configuration

- Pre-provision a new ONT from Netconf and/or vOLT CLI
- Provision services (uni and multi-cast)
- Provision services automatically
- Delete ONT and services
- Provision LAG group

4.2 Scalability

- Provision multiple ONTs on a PON – Verify ONOS is capable of processing multiple EAP, DHCP and IGMP proxy/snooping functions.
- Establish 4-6 simultaneous streams per ONT – Verify no packet loss
    - At least 32 ONTs on the same PON (Applicable to Ph3/Ph4 - TBD)
    - We want to see when all ONTs/RGs come to service if ONOS can handle storm of EAP/DHCP request

4.3 Resiliency

- Verify vOLT instantiation can be regenerated from a complete deletion situation (Legacy database backup/restore test case).
- Reboot vOLT – verify forwarding table resiliency
- Remove connectivity between vOLT and ONOS – ensure configurations and services are restored
    - Leaf switch reboot, ONOS/VOLT reboot/restart/disconnect when service is running, observe service backup

- Test Equipment/Traffic generator sends unknown unicast to test ONOS server process of flash of traffic
- FIT – Fault Insertion Tests

4.4 QoS / Service-Level Items

- Provision multiple ONTs on a PON – Verify T-CONT (CBR, ABR functions), p-bit processes and service profiles are properly managed by queues when congested.
- Verify maximum throughput capability of data service – 1G and 10G
- QoS testing – Test VLAN priority tagging. Saturate an ONT with traffic of different priorities and confirm they are discarded accordingly
- Perform standard frame size tests (64, 128, 256, 512, 1025, etc.)
- ONT/OLT need to do traffic shaping

4.5 Performance Monitoring

- Verify PON bandwidth utilization status – verify ability to see available bandwidth.
- Verify ONT optical power levels and distance from OLT can be seen.
- Verify ability to query inventory of how man ONT/RGs are in service.
- Verify ability to acquire RG authentication status.
- Verify ability to query CPU, I/O and memory status.
- Verify ability to query NNI utilization.

4.6 Facility Management

- Verify system's ability to detect new ONTs and see ONTs ranged (not activated).
- Verify system's ability to detect IS and OOS ONT service states.
- Verify ability to console/login to OLT HW for status check.

4.7 Alarms, States, Conditions

4.7.1 Retrieve Provisioned PON Parameters

- IS, OOS (both state and configured)
- vOLT instance association
- BER time measurement period that determines SD condition
- BER threshold used to establish SD condition
- BER threshold used to establish SF condition
- FEC enabled/disabled
- Distance of closest ONT
- Maximum differential logical reach on PON
- Rogue ONT test
- Upstream traffic threshold
- Downstream traffic threshold
- PON label/description
- Multicast encryption enabled/disabled

4.7.2 Retrieve operational PON parameters

- Ranged ONT numbers/identifiers
- IGMP – number of queries, drops, etc. and associated addresses.
- BEC DS
- BEC US
- ONT ranging condition

4.7.3 Retrieve Provisioned ONT Parameters

- IS, OOS (both state and configured)
- Ethernet Interface (UNI) – link configuration (i.e. 1000BTFULLDPLX), link state (UP/DOWN)

- 802.1x authentication – auto/forcedauth/forcedunauth, server timeout, supplicant timeout, maximum requests, reauthorization enable/disable, reauthorization timeout
- PAE port enable/disable
- Battery backup (present/not present)
- BER accumulation interval
- NTP information
- Description
- Part number
- Serial number
- Location Identifier
- Planned SW version
- FEC (enabled/disabled)
- Power shedding profile
- Optical measurements (RSSI)
- Active SW
- Passive SW
- Vendor ID
- Number of slots
- Number of T-CONTS
- Number of traffic schedulers
- Number of priority queues
- Upstream policing (on/off)
- AES (enable/disable)
- VoIP service creation
- CVLAN translation mode
- Bridge mapping mode
- IP Host capability
- DSCP to PBIT functionality (ONT or OLT)
- Data Dump Information (enabled, date, time)

4.7.4 Retrieve Operational ONT Parameters

- PLOAM status (Loss of signal, loss of acknowledgement, loss of GEM channel delineation, Physical Equipment Error, Start-up failure, Signal degrade, ONT disabled, Inactive, Loss of Frame, Signal Fail, Dying Gasp, Deactivation Failure, Loss of PLOAM, Window drift, Remote Defect Indicator, Loss of Key Sync, Differential Reach Exceeded)
- Distance (estimation) between OLT and ONT
- 802.1x – Report both PAE (initialized, disconnected, connecting, authenticating, authenticated, aborting, held, forced (auth and unauth) and backend (request, response, success, fail, timeout, held, initialize) states. Counters for each of these should be available.

4.7.5 Retrieve ONT optical parameters

- ONT TX and RCV levels (and associated TCAs for High and Low alarms)
- OLT RCV level
- Temperature
- Voltage
- Laser bias current
- These parameters should be able to be logged for historical data pulls

4.7.6 Retrieve Alarms

- On all provisioned equipment (vOLT, ONOS, vOLTHA, NNIs, LAGs, PONs, ONTs, UNIs, HSIA Services, POTS/VoIP services, configured VLANs, PMAAs)
- Severity level indication (Critical, Major, Minor…depending on service affecting)

4.7.7 Retrieve System CPU Utilization

- Current and average system load (Device, VOLTHA, ONOS, etc.)

4.7.8 Retrieve RADIUS Information

- Domain IS, OOS
- Domain Policy
- Auth Server IS, OOS
- Auth Server IP:port
- Auth Server retry, timeout parameters

4.7.9 Retrieve Equipment

- Current provisioned equipment
- IS, OOS

4.8 Interoperability

- Operate as many different (foreign) ONUs on as many different OLTs as is practical

    - Compute Portability – Validate the Solution does not have any dependencies on particular types of hardware, and/or document any dependencies identified.
    - Interoperability with CPE equipment (make and model number to be provided by the carrier)

4.9 Operational/Support/Debug Tools

- ONT self-test functionality
- Edit an ONT IS/OOS
- Assign/Unassign Serial numbers to ONTs
- Delete ONTs
- Download/Activate Software and retrieve active SW version

- LED Status Indicator accuracy and usability

4.10 Layer-1 Compliance

- Verify Industry Standards Compliance
    - G.989, G.989.1, G.989.2, G.989.3
    - G.988 – ONU Management and Control Interface (OMCI)
    - BBF TR-156
    - BBF TR-247 ONU Conformance Test
- Establish communication/range between the OLTs and ONT
- Optical Loss/Budget Testing – Test ONT's ability to operate throughout its "window"

4.11 Functional Testing

- RADIUS for RG/Subscriber authentication (802.1x Authentication against Lab's production grade standard RADIUS with lab provided RGs is required)
- DCHP
- Multicast (4 and 6 simultaneous streams of HD with ICC support)
- ONT remote reboot. Remote enable OLT/ONT

4.12 Integration-Level Items

- Verify OLT system is inventoried/recognized by ONOS
- Verify OLT is capable of being managed by ONOS
    - Capable of "on demand" management task recognition (i.e. reboot, profile change, RSSI, inventory query response, debug, etc.)
    - Demonstration of the alarm/event configuration capability, including configuring alarm severity, alarm suppression, alarm acknowledge and clearing with vOLT software.
        - Review the current supported alarm/event list.
    - Demonstration of OLT software download capability

    - At the minimal, provide the proposal about how to utilize the vOLT SW component to upgrade the OLT/ONT SW.
    - What interface and application in VOLTHA framework will provide this functionality?

- Verify PON operations act such that the behavior and operation of new ONTs is not disruptive and transparent/contiguous with that of currently deployed units. Examples include: Software downloads to ONT groups.
- Verify vOLT is not disruptive with existing QoS policies/implementations and allows for transparent application of current service configurations. Queuing structures and other QoS configurations should allow for seamless service provisioning and QoS execution. (Perhaps future test?)

4.13 Security

- Security Policy Requirement (SPR)
- userid/passwd for sub-components

4.14 NEBS / Physical / Environmental

- See above for requirements (still being finalized)

4.15 Creation and Validation of Deployable Software Images

Installation images in the form of tar or equivalent shall be created and validated during Phase-3.

A final approved monolithic production software stack shall be imaged and hashed during Phase-3. Also during Phase-3, at least 1 system shall be built from the installation image, and validated to be fully functional.

Appendix A Solution-Set Matrix

Please complete the Solution-Set Matrix in the attached Excel file. An image is presented below for quick reference. **Data must be populated in the Excel version**.

XGS_Phase-3_SSM

This file is embedded as an attachment to this PDF. To access the SSM, click the "paperclip" to the left, which will expose the attached file. Then, simply double-click on the file itself.

Remember to ensure the value you populate in the "Diagram Key" field in the SSM template accurately corresponds to the object annotations in your architecture diagram.

Figure 4: SSM Sample Image

Supplier Instructions: Populate the fields corresponding to your solution's unit-level BoM and version control (wild cards are ok for specifying point releases, build numbers

Values populated are for example; delete sample data and replace with data reflecting proposed solution

Category	Diagram Key	Subsystem (Examples)	Supplier	Quantity	Model No.	HW Revision	HW Status	Firmware Rls	Firmware Status	Comments
Hardware	OLTMA1	XGS-PON OLT								
Hardware	OLTMA2	XGS-PON OLT								
Hardware	ONU1	XGS-PON ONT								
Hardware	ONU2	XGS-PON ONT								
Hardware	SRVR1	Compute Server #1								
Hardware	TOR1	ToR Switch								
Hardware	SW1	Management Switch								
Hardware	XYZ1	Supplier h/w x, y, z								
Hardware	XYZ2	Supplier h/w x, y, z								
Hardware	XYZ3	Supplier h/w x, y, z								
Software	VOLTHA1	VOLTHA								
Software	SDNC1	SDN-Controller								
Software	D1	Docker								
Software		vOLT App								
Software		Hypervisor								
Software		NFVI/VIM/MANO/etc.								
Software		RADIUS								
Software		DHCP								
Software		DNS								
Software		Supplier app/program/module								
Software		Supplier app/program/module								
Hardware		BNG								
Hardware		RG								
Hardware		STB								
Hardware		Splitters								

Total Estimated Value:

Appendix B System-Level Provisioning

The vOLT Solution will be provisioned with the following datafill for Phase-3 testing, upon delivery to the site.

Appendix C ONU and Service Provisioning

The vOLT Solution will be provisioned with the following ONU/UNI-specific datafill for Phase-3 testing, upon delivery to the site.

<INSERT TABLE HERE>

Appendix D Supplier Support Contacts and Escalation

Support Infrastructure includes not only a designated support group, but also the following items:

- Business Hours Contact List
- Emergency Escalation Plan, including key contacts and reach numbers
- Remote Access Plan; Operator will work with Suppliers on this item
- Committed Response Time(s), based on situation impact
- Agreed Resolution Flow, Including Daily Updates on Hot Issues

Please complete and submit the Support Contacts and Escalation template

<SUPPLIER INSERT TABLE OR DOCUMENT HERE>

Appendix E XGS PoC Phase-3 Support Contacts

Appendix F References

Appendix G Glossary of Terms and Initialisms

ABR	Available Bit Rate
AC	Alternating Current
AES	Advanced Encryption Standard
SPR	Security Policy and Requirements
BBF	BroadBand Forum
BEC	Bit Error Count
BER	Bit Error Rate
BNG	Broadband Network Gateway
BSS	Business Support System
CBR	Committed Bit Rate
CLI	Command Line Interface
CMS	C.. Management System
CO	Central Office
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CSO	Chief Security Office
CVID	Customer VLAN IDentifier
CVLAN	Customer VLAN
cVoIP	Consumer VoIP
DAC	Direct Attach Cable
DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DS	DownStream
DSCP	DiffServ Code Point
DVL	Design Validation Lab
EAP	Extensible Authentication Protocol
EAPoL	EAP Over LAN
FCAPS	Fault, Configuration, Accounting, Performance, Security
FEC	Forward Error Correction
FIT	Fault Insertion Test
GEM	GPON Encapsulation Method
GR	Generic Requirements
HA	High Availability
HD	High Definition [video]
HSIA	High Speed Internet Access
HW	HardWare
I/O	Input/Output
ICC	Instant Channel Change
IGMP	Internet Group Management Protocol
IPTV	Internet Protocol TeleVision

IS	InService
iV	Intra-SDN Reference Point V (SDN Equivalent to TR-156 V)
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LED	Light Emitting Diode
LVL	Lightspeed Validation Lab
MAC	Media Access Control
MVT	Multi-Vendor Test
NEBS	Network Equipment Building System
NFVI	Network Function Virtualization Infrastructure
NNI	Network-Network Interface
NTP	Network Time Protocool
OCP	Open Compute Project
ODN	Optical Distribution Network
OLT	Optical Line Terminal
OMCI	Optical network unit Management and Control Interface
ONOS	Open Network Operating System
ONT	Optical Network Terminal
ONU	Optical Network Unit
OOMCI	OpenOMCI
OOS	Out Of Service
OS	Operating System
OSS	Operations Support System
PAE	Port Authentication Entity
PLOAM	Physical Layer Operations, Administration and Maintenance
PM	Performance Management
PMAA	Persistent Management Agent Aggregator
PoC	Proof of Concept
PON	Passive Optical Network
POTS	Plain Old Telephone Service
QoS	Quality of Service
RADIUS	Remote Access Dial In xx Server
RCV	ReCeiVe
RG	Residential Gateway
RSSI	Received Signal Strength Indication
SD	Signal Degrade
SDN	Software Defined Network
SF	Signal Fail
SME	Subject Matter Expert
SoC	Statement of Compliance
SoC	System on Chip
SSM	Solution Set Matrix
STB	Set Top Box

STC	Spirent Test Center
suid	Set User ID
SVID	Service VLAN IDentifier
SW	Software
TC	Test Case
TCA	Threshold Crossing Alarm
T-CONT	Traffic CONTainer
TX	Transmit
UNI	User-Network Interface
US	UpStream
VID	VLAN IDentifier
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
vOLT	virtual OLT
vOLT MA	vOLT Media Adaptation Hardware
VOLTHA	Virtual OLT Hardware Abstraction
VSA	Vendor Specific Attribute
XGig	Multi-Gigabit
XGS	10 Gigabit Symmetrical

v.20170502