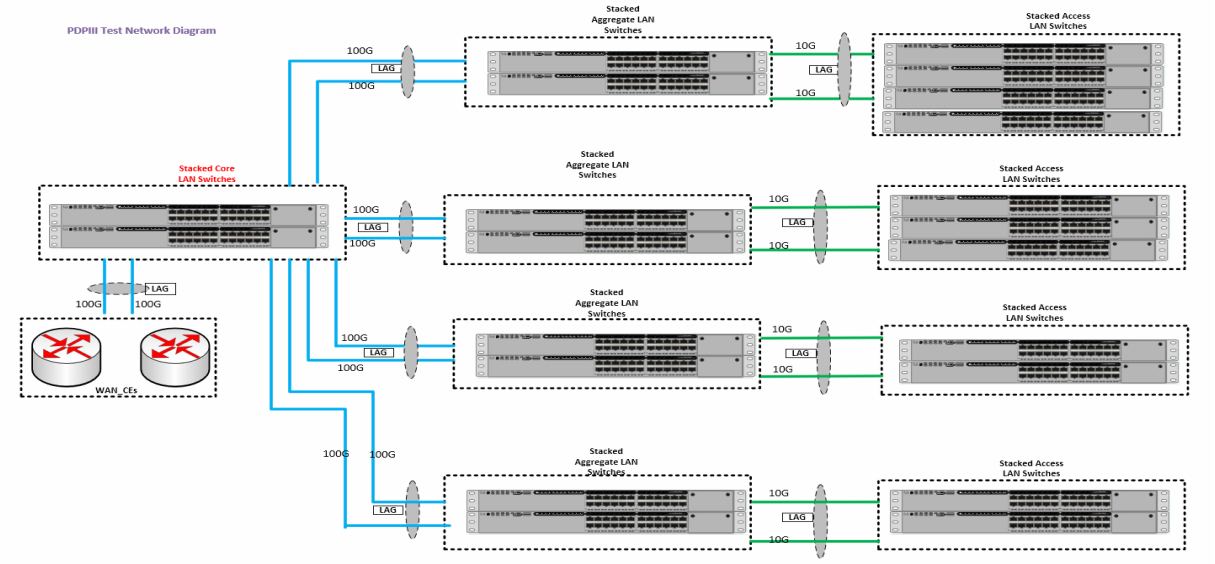
Annex D - Integration Test Plan

All tests will be performed on-site in the National Capital Region using production configurations, except where noted. The vendor will, with Shared Services Canada (SSC) support, connect two Cores, two Distribution and three Access switches based on the diagram below. SSC will provide appropriate configuration guidance as currently in production for SSC to aid in testing.

Software configurations put in place for testing can not be removed from the building either in paper or electronic forms. If the switches using during testing are not left as part of the initial equipment delivery, assuming a successful outcome, then configurations must be reset to factory default before leaving the lab.

Minimum Test Bed Equipment Requirements	**Quantity**
Switch Configuration - L3 Core	2
Switch Configuration - Distribution	2
Switch Configuration - Multigigabit Access	4
Switch Configuration - Gigabit Access	2
Supplemental Stacking Cable for Item 3 and 4 - 1 Meter	2
10GBASE-LR Transceiver	8
10GBASE-SR Transceiver	8
100GBASE-SR-BiDi Transceiver	8

Plus all stacking cables, power cords, fans and power supplies required to meet Annex C requirements.



Test 1 **Automation of LAN (Access, Agggregate and L3 core)**

Vendor must demostrate Zero-Touch Provisioning (ZTP), configuration push, configuration changes, license renewal, and Operating software upgrade, and In Service Upgrade wihtout any service interruption.

Test 2 **Vendor must demonstrate resiliency (Access, Agggregate and L3 core)**

A device is plugged on the access switch on a given vlan emulating a user, also another device is plugged in on the core, both devices must be on the same network using same Vlan ID. A continous ping is initiated between the core device and the user device. Vendor will have to power off the stack unit carrying the ICMP traffic and demostrate that traffic is recovered with no packet loss or no more than 3 packet loss.

Test 3 **Packets sourced from Inband Management interface within an VRF on L3 core switch**

Vendor must demostrate that management traffic is able to be sourced from an inband management interface within a VRF on the core router. Management traffic such as NTP, Syslog, SNMPv3, SSH, TACaCS+

Test 4 **Vendor must demonstrate 802.1x (NAC on Access switches only, support EAP-TLS and MAC bypass)**

Vendor must demonstrate 802.1x functionality and interoperability with Aruba Clearpass solution.

Vendor must demonstrate that the access switch must be able to parse and process the following RADIUS attributes that it receives from the RADIUS response (ACCEPT, DROP, REJECT):

- Attribute 81: Tunnel-Private-Group-Id as defined in RFC2868. Switch must be able to set VLAN based on numeric VLAN ID (example VLAN '63') or VLAN tag (example VLAN 'Corporate') .
- Attribute 92: NAS-Filter-Rule as defined in RFC4849 and/or Attribute 11 Filter-id. If using attribute 92 the switch must set an ACL based on string value sent from RADIUS server attribute. If using Attribute 11 filter-id, the ACL must be pre-configured on the switch and activated on the port if the ACL name is passed by RADIUS 11 response.
- Dot.1x port must support VoIP to ensure a phone set is dynamically put on a given Vlan as well as the same dot1x port is able to support a device plugged in series with the VoIP phone and the device is also dynamically put on a different vlan than the phone set.

Test 5 **Vendor must demonstrate traffic isolation (L3 Core)**

Test performed offline with full stage 1 interim build (L3 cores)

Virtual route forwarding (VRF) must be configured on the core, and a VLAN added with a non-OZ address. If needed a port can be brougt up to bring p the VLAN or it can be pinned up manually if the feature is available. Traffic from the OZ network must not be able to reach the VRF carried traffic. Success will be indicated by traffic isolation between zones(as indicated by ping), failure will be indicated as successful vlan traversal regardless of the VRF.

Test 6 **Vendor must demonstrate TACACS+ User Authentication, Authorization, and Accounting - Access**

Test performed online with SSC Cisco cores.

Testing must demonstrate successful user access for RW and RO access via supplied Active Directory credentials

Testing must demonstrate that RW and RO levels as assigned in AD are passed to the switch limiting or allowing access to elevated privilege commands. elevated priveledge commands will be determined during assessment, but generally include the ability to modifiy and permanantly commit any significant non-transitive config elements.

Testing must demonstrate the logging of SSH/Telnet sessions (when a user attempts or successfully logs in to the switch) to the TACACS+ server as well as the logging of what commands are executed and from which user account they were executed (also to the TACACS+ server)

Failure is indicated by the switches not being able to be accessed via TACACS+, no user level separation is possible ie only RW, or that those priveldge levels are not respected by the switch. ie RO users granted elevated privledges. Failure is also indicated by an inability to log SSH/Telnet sessions or commands via TACACS+ accounting.

Test 7 **Vendor must demonstrate compatibilty with VoIP phone system - Access**

Testing must demonstrate the successful negotitian of POE and commnuication of LLDP-MED to place the phone in the correct voice VLAN. Config guidance by SSC will be provided to adapt to vendor config statements. Successfull testing will be indicated by an online VOIP handset. Failure will be indicated by no POE delivery or failure to detect correct voice VLAN via LLDP-MED

Test 8 **Vendor must demonstrate MACsec using a 256bit key between access, aggregation and core switches**

MACsec must be configured between access, aggreggation and core switches. Connectivity between switches is done over a lag with a minimum of two ports per LAG. Traffic should be pushed at full line rate. Port mirroring must be enabled to capture such traffic and confirm traffic is encrypted. While traffic is traversing, a port within the lag should be disconnected and confirm traffic continues to traverse over the existing link with no packet loss or maximum of 5 packet loss.

Test 9 **Vendor must demonstrate adding a port to the LAG without any impact to existing traffic**

While traffic is flowing over the existing lag, vendor must add another port to the lag and demonstrate existing traffic continues to flow with no interruption and zero packet loss

Test 10 **Vendor must demonstrate adding and removing power supply to a switch with in the stack does not impact traffic flow**

While traffic is flowing between core-aggreggate and access, vendor must remove one power supply from a switch within the stack and demonstrate that the traffic is not impacted. Second portion is to demonstrate the vendor adding a powersupply to a switch within the stack and ensuring traffic is not impacted as well.

Test 11 **Vendor must demonstrate RadSec functionality using TLS based certficate and integration with Aruba Clearpass**

The switch and RADIUS server will be configured to communicate over RADSec using TLS based certificate. The RADIUS server will have all other methods disabled. Ensure communication between LAN switches and radius (Clearpass) are established and stable. Repeat test case # 4.

Test 11 **Vendor must demonstrate gigabit and multigigabit access switch stacking**

Using stacking cables, the vendor must demonstrate the successufl creation of a stack of access switches that consists of two multigigabit sand one gigabit swtich.