Nexus Validation Test Phase 3.1

Network Hardware and Software Version Details

DC1 Image Versions

	Model No.	NVT 3.1
N7K	**N7K-SUP1**	6.2(8)a
N5K	**N5K-C5548UP-SUP**	5.2.1.N1.4
N3048	**N3K-C3048TP-1GE-SUP**	5.0.3.U5.1b
C6K	**VS-SUP2T-10G**	150-1.SY3
	VS-S720-10G	122-33.SXJ4
	WS-SUP720	122-33.SXJ4
	WS-SUP32-GE	122-33.SXJ
C4K	**WS-X45-SUP7-E**	03.03.02.SG.151-1.SG2
	WS-C4948	150-2.SG6-6.9
UCS	**UCS-5108**	N/A
	UCS-B200-M2	2.1(2a)*
	UCS-B22-M3	2.1(2a)*
	UCS-2208XP-FEX	2.1(2a)*
	UCS-6296UP-FI	2.1(2a)*

DC2 Image Versions

	Model No.	NVT 3.1
N7K	**N7K-SUP2E**	6.2(8)a
N7700	**N77-SUP2E**	6.2(8)a
N6000	**N6K-C6001-64P-SUP**	7.0(3)N1(0.31)
N5K	**N5K-C5548P -SUP**	5.2.1.N1.4
	N5K-C5548UP-SUP	5.2.1.N1.4
N3548	**N3K-C3548P-10G-SUP**	5.0.3.A1.2
C6K	**VS-SUP2T-10G**	150-1.SY3
	VS-S720-10G	122-33.SXJ4
	WS-SUP720	122-33.SXJ4
C4K	**WS-X45-SUP7-E**	03.03.02.SG.151-1.SG2
	WS-C4948	150-2.SG6-6.9
UCS	**UCS-5108**	2.1(2a)*
	UCS-B200-M2	2.1(2a)*
	UCS-B22-M3	2.1(2a)*
	UCS-2208XP-FEX	2.1(2a)*
	UCS-6296UP-FI	2.1(2a)*

Introduction

This is an addendum to NVT testbeds: DC1 (N7K sup1) and DC2 (N7K sup2). N7K's are running 6.2(8)a releases.
Please see below for test results and caveats found during 6.2(8)a NVT testing.

Caveats for NVT 3.1

Assigned/New	→	*Still working on fixes and may be seen in CCO image*
Unreproducible	→	*Not seen in CCO image, may be have fixed by other code fixes.*
Verified/Resolved	→	*Fixed in CCO image*
Closed	→	*System limitation and behavior will remain the same*

CSCun66981
Symptom: N7700: F2 module fails to come up after loading 6.2(8).
Conditions: When N7700 with F2 modules is loaded with 6.2(8), the F2 module keeps reloading and fails to come online. 'aclqos' cores are also seen on the switch for this F2 module
Workaround: None
Severity: Severe
Status: Verified
Platform Seen: N7700
Resolved Releases: 6.2(8)a
Applicable Releases: NA

CSCun11692
Symptom: pfstat: pfstat_restore_debug(529) errors seen on system switchover with 6.2(8). There is no service impact caused by the messages.
Conditions: When a system switchover is done, below errors are seen on 6.2(8):
N7K %$ VDC-1 %$ 12 17:11:59 %KERN-2-SYSTEM_MSG: [6330.639402] Switchover started by redundancy driver - kernel
N7K %$ VDC-1 %$ %SYSMGR-2-HASWITCHOVER_PRE_START: This supervisor is becoming active (pre-start phase).
N7K %$ VDC-1 %$ %SYSMGR-2-HASWITCHOVER_START: Supervisor 6 is becoming active.
N7K %$ VDC-2 %$ pfstat: pfstat_restore_debug(518): (Error) no such pss key
N7K %$ VDC-2 %$ pfstat: Error unable to restore debug pss
Workaround: None

Severity: Moderate
Status: Resolved
Platform Seen: N7000
Resolved Releases: 6.2(8)a
Applicable Releases: NA

CSCum54359
Symptom: 'aclqos' cores seen when N7000 is loaded with 6.2(8).
Conditions: N7000 had 'aclqos' cores on all modules when loaded with 6.2(8), previously running 6.2(2a) cco image.
Workaround: None
Severity: Severe
Status: Verified
Platform Seen: N7000
Resolved Releases: 6.2(8)a
Applicable Releases: NA

CSCum55746
Symptom: M2 module failed to come up when loaded with 6.2(8)
Conditions: On loading N7000 with 6.2(8) image, M2 modules in the switch remain in 'failure' state and do not come up. 'eltmc' core is seen on these modules.
Workaround: None
Severity: Severe
Status: Verified
Platform Seen: N7000
Resolved Releases: 6.2(8)a
Applicable Releases: NA

CSCuo36637
Symptom: Multicast routes get deleted on primary vpc-peer after ISSU from 6.2(6) to 6.2(8), hence causing traffic loss
Conditions: The multicast packet loss issue is seen during ISSU when following conditions are met:
1) ISSU from 6.1(X), 6.2(2), 6.2(2a), 6.2(6), 6.2(6a) to 6.2(8)
2) An F2 line card is shared between two VDC's

3) One vdc has VPC config and the other vdc has 'VPC+ and fabricpath' config for same vlans
Workaround: None
Severity: Severe
Status: Verified
Platform Seen: N7000
Resolved Releases: 6.2(8)a
Applicable Releases: NA

CSCum86523
Symptom: M1 module fails with ‘isis-301’ core after ISSU from 6.1(4) to 6.2(8) on N7000 sup-1 causing traffic losses.
Conditions: Issuing “install all kickstart <628_kickstart_image> system <628_system_image>” on N7000 with sup-1 and M1 modules will cause traffic loss. The M1 modules remain in failed state once ISSU completes. ‘isis-301’ cores are seen for M1 modules.
Workaround: None
Severity: Severe
Status: Verified
Platform Seen: N7000
Resolved Releases: 6.2(8)a
Applicable Releases: NA

CSCum86511
Symptom: M1 module fails with ‘ipfib’ core after ISSU from 6.1(4) to 6.2(8) on N7000 sup-1 causing traffic loss
Conditions: Issuing “install all kickstart <628_kickstart_image> system <628_system_image>” on N7000 with sup-1 and M1 modules will cause traffic loss. The M1 modules remain in failed state once ISSU completes. ‘ipfib’ cores are seen for M1 modules.
Workaround: None
Severity: Severe
Status: Verified
Platform Seen: N7000
Resolved Releases: 6.2(8)a
Applicable Releases: NA

CSCuo23173
Symptom: ‘l3vm’ core while making "vrf management" as "address-family ipv4 unicast"

Conditions: A core is triggered by performing the following steps on N7K running 6.2(8) image:
PE1(config)# vrf context management
PE1(config-vrf)# address-family ipv4 unicast
2014 Apr 10 16:29:08 PE1 %SYSMGR-2-SERVICE_CRASHED: Service "l3vm" (PID 9342) hasn't caught signal 11 (core will be saved).
Workaround: 'address-family ipv4 unicast' is unsupported command in vrf context, however 'l3vm' crash issue has been resolved.
Severity: Moderate
Status: Resolved
Platform Seen: N7000
Resolved Releases: 6.2(8)a
Applicable Releases: NA

CSCuo57841
Symptom: IP adjacencies are not installed for directly attached hosts on N7K running 6.2(8).
Conditions: With PVLAN configuration on N7k F2 module, IP routed traffic will be dropped in some of the ports.
Workaround: Delete and add the PVLAN configuration
Severity: Severe
Status: Resolved
Platform Seen: N7000
Resolved Releases: 6.2(8)a
Applicable Releases: NA

CSCuo63409
Symptom: When "fabricpath mode transit" is configured on N7K fabricpath spine, traffic outage would be observed as a result with drop occurring at the transit spine.
Conditions: This issue is more likely to occur in a scaled testbed, with more number of vlans, SVIs or L2 multicast group entries. Reload or vdc restart can also trigger the same on a scale bed.
Workaround: As a workaround, when transit mode is configured on the spine remove the rest of the vlan's from the node and then reload.
Severity: Severe
Status: Resolved
Platform Seen: N7000
Resolved Releases: 6.2(10), 7.1(0)
Applicable Releases: 6.2(8)a

CSCul44598
Symptom: Intermittent multicast traffic loss on common intermediate router when some receiver DR's are configured with SPT threshold infinity and others are configured as default.
Conditions: This issue is seen when the receiver DR with SPT threshold infinity and the receiver DR with default SPT threshold, have a common intermediate router which is in the shared tree path for both and also in the (S, G, R) prune path from the receiver with default SPT threshold while it sends joins to the source tree.
Workaround: Ensure that the same SPT threshold is configured on all receiver DR's.
Severity: Severe
Status: Verified
Platform Seen: N7000
Resolved Releases: 6.2(8)a
Applicable Releases: 6.2(6), 6.2(6a)

CSCuh58228
Symptom: ISSD from 6.2(8) to 6.2(6) on N7000 fails with STP core. Some of the VDC's restart and modules do not downgrade to 6.2(6). There will be impact on the traffic as switch reloads.
Conditions: 'install all kickstart <626_kickstart_image> system <626_system_image>' on N7000 running 6.2(8) image, can cause STP crash and VDC's to restart during the 'system switchover'. This issue is not frequently reproducible.
Workaround: The switch reloads when ISSD fails. If it doesn't, then reloading the switch will resolve the issue.
Severity: Severe
Status: Verified
Platform Seen: N7000
Resolved Releases: 6.2(8)a
Applicable Releases: 6.2(6)

CSCun64129
Symptom: M2 module fails with 'val_usd' core on ISSD from 6.2(8) to 6.2(2a) cco image. There will be a service impact as module does not come up.
Conditions: On ISSD from 6.2(8) to 6.2(2a) cco image the M2 module fails after system switchover, with a 'val_usd' core and remains in 'powered_down' state after ISSD completes.
Workaround: Reload the switch to bring up M2 module
Severity: Severe
Status: Unreproducible
Platform Seen: N7000

Resolved Releases: NA
Applicable Releases: 6.2(8)a

CSCui02797
Symptom: When trying to show a specific prefix-list the entire prefix-list configuration is shown:

```
Nexus# show ip prefix-list TEST
ip prefix-list Lisa-A: 10 entries
  seq 300 permit 10.46.1.0/24
  seq 400 permit 10.47.1.0/24
ip prefix-list List-B: 4 entries
  seq 100 permit 10.25.0.0/16 le 32
  seq 200 permit 10.26.0.0/16 le 32
  seq 300 permit 172.132.132.100/32
  seq 400 permit 172.132.132.200/32
ip prefix-list TEST: 6 entries
  seq 100 permit 10.25.0.0/16 le 32
  seq 200 permit 10.26.0.0/16 le 32
  seq 300 permit 10.20.20.205/32
  seq 400 permit 10.20.20.206/32
  seq 500 permit 10.21.21.205/32
  seq 600 permit 10.21.21.206/32
```

Conditions: Issuing "show ip prefix-list" with a specific prefix-list name
Workaround: None
Severity: Cosmetic
Status: New
Platform Seen: N7000
Resolved Releases: NA
Applicable Releases: 6.2(8)a, 6.2(6), 6.2(6a), 6.2(2), 6.2(2a)

CSCun71884
Symptom: 'sh (non-sysmgr)' crashed on N7000 after switchover with 6.2(8)
Conditions: On N7000/N7700 with type sup-2 running 6.2.8, if a system switchover is done, ‘sh (non-sysmgr)’ core is seen. The core is intermittently seen.

Workaround: ‘ssh’ connections will be lost. Workaround is to re-connect to the switch.
Severity: Severe
Status: Resolved
Platform Seen: N7000/N7700
Resolved Releases: 7.1(0)
Applicable Releases: 6.2(8)a, 6.2(6), 6.2(6a), 6.2(2), 6.2(2a)

CSCuo57183
Symptom: 'vsh (non-sysmgr)' crashed on N7000 after 8-10 hours of continuous ‘ssh’ to the switch.
Conditions: On N7000 with type sup-2E running 6.2.8, a continuous ‘ssh’ is done to connect to the switch, ‘vsh’ cores are seen.
Workaround: ‘ssh’ connections will be lost. Workaround is to re-connect to the switch.
Severity: Severe
Status: Assigned
Platform Seen: N7000
Resolved Releases: NA
Applicable Releases: 6.2(8)a

CSCun11736
Symptom: STP-2-SET_PORT_STATE_FAIL messages are seen on system switchover with 6.2(8).
Conditions: On N7K running version 6.2(8), when a system switchover is done, below pixm error messages are seen:
N7K %$ VDC-2 %$ %STP-2-SET_PORT_STATE_FAIL: Port state change req to PIXM failed, status = 0x801c0071 [No route to host] vdc 2, tree id 0, num ports 7, ports state BLK, opcode MTS_OPC_PIXM_SET_MULT_CBL_VLAN_BM_FOR_MULT_PORTS, msg id (1980289), rr_token 0x1E3781
N7K %$ VDC-2 %$ %STP-2-VPC_PEER_LINK_INCONSIST_BLOCK: vPC peer-link detected BPDU receive timeout blocking port-channel6 VLAN0013.
These syslogs after switchover on the SUP that is going down is expected and there is no functional impact.
Workaround: None
Severity: Severe
Status: Closed – Expected Behavior
Platform Seen: N7000
Resolved Releases: NA
Applicable Releases: 6.2(8)a

CSCup29872

Symptom: EPLD release notes do not show correct version information

Conditions: In http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/epld/epld_rn_62.html, Table 3 describes the EPLD versions for each module that were bundled with each EPLD image. The versions numbers in the table are sometimes not correct.

For example, for Supervisor 2 and 2E for Nexus 70xx switches, the table shows that the newest EPLD was most recently released as:

-Power Manager: 2.005 @6.1(5)

-IO: 1.013 @6.1(2)

But the EPLD image that was shipped with 6.2.8 shows that the latest are:

-Power Manager SPI: 37.000

-IO SPI: 1.013

-Power Manager: 37.0000

-IO: 1.013

Workaround: None

Severity: Severe

Status: Assigned

Platform Seen: N7000

Resolved Releases: NA

Applicable Releases: 6.2(8)a

CSCuo79063

Symptom: N7K M2 module hardware FIB install times are much slower than C6K.

Conditions: Route convergence time is slower on scaled setup for N7K with M2 modules, as compared to Cat6k devices. The HW install time on N7K is measured by "show forwarding ipv4 route summary" displaying the correct # of routes.

Workaround: NA

Severity: Moderate

Status: Assigned

Platform Seen: N7000

Resolved Releases: NA

Applicable Releases: 6.2(8)a

CSCuo80937

Symptom: If there is any topology change after upgrade to 6.2.(6), 6.2.(6a) or 6.2.(8), then after approximately 90 days of active supervisor uptime, STP TC BPDUs are sent out every 2 seconds for a long period of time.

Conditions: Nexus 7000 or 7700 running 6.2(6), 6.2.(6a), or 6.2(8)

Workaround: In order to circumvent this issue until an upgrade to fixed code can be performed, execute the appropriate workaround depending on whether you have a dual-supervisor or single-supervisor configuration before each 90 days of Active supervisor uptime.

For dual-supervisor setups:

1. Reload the standby supervisor using cli "reload module x" where x is standby supervisor slot number.
2. Use the 'show module' command to confirm that the standby supervisor is up and in the ha-standby mode.
3. Use the system 'switchover command' to switch to the standby supervisor.

For single-supervisor setups:

1. Upgrade to 6.2.6b or 6.2.8a, depending on your business requirements.
2. Reload the switch.

Severity: Severe

Status: Verified

Platform Seen: N7000, N7700

Resolved Releases: 6.2(8)a, 6.2(6)b

Applicable Releases: 6.2(6), 6.2(6)a

DC1 and DC2 results

	Folders	Verification	Total # of test cases	Total # of Pass	Total # of Pass w/Exception	Total # of Fail	Total # of Iteration	Defect(s)
1	**NVT 3.1**		2060	2048	3	9	3878	
1.3	**DC2**		1389	1378	3	8	2414	
1.3.1	Core to Distribution Setup		2	2	0	0	10	
1.3.1.1	Setup interfaces from Core to Distribution blocks		2	2	0	0	10	
		Verify SSH works through the management network on a dedicated vrf						
		Verify startup and running config						
		Verify TB, error, crash						
		Verify any core dumps						
		Verify RSA key does not change on device						
		Verify ssh on device is functional						
		Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers						
		Verify NTP/PTP and Time Zone : ntp.interop.cisco.com						
		Verify Syslog to syslog.interop.cisco.com						
		Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10						
		Verify DNS search list: interop.cisco.com, cisco.com						
		Verify CMP port connections to the management network.						
		Verify CDP neighbors						
		Verify SNMP agent (read community): public + interop; (private community): private + cisco						
		Verify SNMP traps to monitor network events						

		Verify UDLD neighbors and UDLD aggressive mode						
		Verify LACP for link aggregation						
		Verify BFD peering for all possible clients with default protocol timers for the clients						
		Verify SSO/NSF and GR						
		Verify CoPP function						
		Verify CoPP counters						
		Verify hardware rate limiter						
		Verify SPAN ensuring cross-module SPAN.						
		Configure Authentication for: OSPF/OSPFv3, HSRP/HSRPv6, MSDP, Layer 2 ISIS (FabricPath, OTV)						
		Verify DHCP IP helper and primary/backup server						
		Verify interfaces in error						
		OSPF: Verify OSPFv2/OSPFv3 peering.						
		PIM: Verify PIM peering.						
		MSDP: Verify MSDP peering and SA-cache						
		Verify that there are no dead flows						
1.3.2	Distribution to Core Setup		10	8	2	0	49	
1.3.2.1	Setup interfaces from Distribution N7K-201 to the core switches		10	8	2	0	49	CSCui02797
		Verify SSH works through the management network on a dedicated vrf						
		Verify startup and running config						
		Verify TB, error, crash						
		Verify any core dumps						
		Verify RSA key does not change on device						
		Verify ssh on device is functional						

		Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers						
		Verify NTP/PTP and Time Zone : ntp.interop.cisco.com						
		Verify Syslog to syslog.interop.cisco.com						
		Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10						
		Verify DNS search list: interop.cisco.com, cisco.com						
		Verify CMP port connections to the management network.						
		Verify CDP neighbors						
		Verify SNMP agent (read community): public + interop; (private community): private + cisco						
		Verify SNMP traps to monitor network events						
		Verify UDLD neighbors and UDLD aggressive mode						
		Verify LACP for link aggregation						
		Verify BFD peering for all possible clients with default protocol timers for the clients						
		Verify SSO/NSF and GR						
		Verify CoPP function						
		Verify CoPP counters						
		Verify hardware rate limiter						
		Verify SPAN ensuring cross-module SPAN.						
		Configure Authentication for: OSPF/OSPFv3, HSRP/HSRPv6, MSDP, Layer 2 ISIS (FabricPath, OTV)						
		Verify DHCP IP helper and primary/backup server						
		Verify interfaces in error						
		OSPF: Verify OSPFv2/OSPFv3 peering.						
		PIM: Verify PIM peering.						

		OTV: Verify OTV ISIS adjacencies are properly established and OTV routing table. Verify the primary AS is being used. On the primary AS, verify all edge devices show up in the unicast replication list						
		Verify that there are no dead flows						
		Verify error vlans						
		Verify frames delta does not increase.						
1.3.3	ToR to Distribution Setup		19	19	0	0	41	
1.3.3.1	Setup interfaces from ToR N5k vPC Switch to N7K-201		4	4	0	0	10	
		Verify SSH works through the management network on a dedicated vrf						
		Verify startup and running config						
		Verify TB, error, crash						
		Verify any core dumps						
		Verify RSA key does not change on device						
		Verify ssh on device is functional						
		Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers						
		Verify NTP/PTP and Time Zone : ntp.interop.cisco.com						
		Verify Syslog to syslog.interop.cisco.com						
		Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10						
		Verify DNS search list: interop.cisco.com, cisco.com						
		Verify CMP port connections to the management network.						
		Verify CDP neighbors						
		Verify SNMP agent (read community): public + interop; (private community): private + cisco						
		Verify SNMP traps to monitor network events						
		Verify UDLD neighbors and UDLD aggressive mode						

		Verify LACP for link aggregation						
		Verify BFD peering for all possible clients with default protocol timers for the clients						
		Verify SSO/NSF and GR						
		Verify CoPP function						
		Verify CoPP counters						
		Verify hardware rate limiter						
		Verify SPAN ensuring cross-module SPAN.						
		Verify DHCP IP helper and primary/backup server						
		Verify interfaces in error						
		vPC: Verify vPC peer status and consistency parameters. Check MAC/ARP/ND/igmp snooping synchronization.						
		IGMP/MLD Snooping: Verify IGMP/MLD Snooping						
		STP: Verify RSTP parameters and port status.						
		VACL, PACL: Verify that all the policies are properly programmed in hardware.						
		Verify that there are no dead flows						
1.3.3.2	Setup vPC interface from ToR Layer 2 Switch to N7K-201		2	2	0	0	4	
		Verify SSH works through the management network on a dedicated vrf						
		Verify startup and running config						
		Verify TB, error, crash						
		Verify any core dumps						
		Verify RSA key does not change on device						
		Verify ssh on device is functional						
		Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers						

		Verify NTP/PTP and Time Zone : ntp.interop.cisco.com						
		Verify Syslog to syslog.interop.cisco.com						
		Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10						
		Verify DNS search list: interop.cisco.com, cisco.com						
		Verify CMP port connections to the management network.						
		Verify CDP neighbors						
		Verify SNMP agent (read community): public + interop; (private community): private + cisco						
		Verify SNMP traps to monitor network events						
		Verify UDLD neighbors and UDLD aggressive mode						
		Verify LACP for link aggregation						
		Verify BFD peering for all possible clients with default protocol timers for the clients						
		Verify SSO/NSF and GR						
		Verify CoPP function						
		Verify CoPP counters						
		Verify hardware rate limiter						
		Verify SPAN ensuring cross-module SPAN.						
		Configure Authentication for: OSPF/OSPFv3, HSRP/HSRPv6, MSDP, Layer 2 ISIS (FabricPath, OTV)						
		Verify DHCP IP helper and primary/backup server						
		Verify interfaces in error						
		STP: Verify RSTP parameters and port status.						
		IGMP/MLD Snooping: Verify IGMP/MLD Snooping						
		VACL, PACL: Verify that all the policies are properly programmed in hardware.						

		Verify that there are no dead flows						
1.3.3.3	Setup vPC interface from ToR Layer 2 Switch to N7K-202		3	3	0	0	6	
		Verify SSH works through the management network on a dedicated vrf						
		Verify startup and running config						
		Verify TB, error, crash						
		Verify any core dumps						
		Verify RSA key does not change on device						
		Verify ssh on device is functional						
		Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers						
		Verify NTP/PTP and Time Zone : ntp.interop.cisco.com						
		Verify Syslog to syslog.interop.cisco.com						
		Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10						
		Verify DNS search list: interop.cisco.com, cisco.com						
		Verify CMP port connections to the management network.						
		Verify CDP neighbors						
		Verify SNMP agent (read community): public + interop; (private community): private + cisco						
		Verify SNMP traps to monitor network events						
		Verify UDLD neighbors and UDLD aggressive mode						
		Verify LACP for link aggregation						
		Verify BFD peering for all possible clients with default protocol timers for the clients						
		Verify SSO/NSF and GR						
		Verify CoPP function						

		Verify CoPP counters						
		Verify hardware rate limiter						
		Verify SPAN ensuring cross-module SPAN.						
		Configure Authentication for: OSPF/OSPFv3, HSRP/HSRPv6, MSDP, Layer 2 ISIS (FabricPath, OTV)						
		Verify DHCP IP helper and primary/backup server						
		Verify interfaces in error						
		STP: Verify RSTP parameters and port status.						
		IGMP/MLD Snooping: Verify IGMP/MLD Snooping						
		VACL, PACL: Verify that all the policies are properly programmed in hardware.						
		Verify that there are no dead flows						
1.3.3.4	Setup interfaces from ToR N3k Layer 3 to N7K-202		1	1	0	0	3	
		Verify SSH works through the management network on a dedicated vrf						
		Verify startup and running config						
		Verify TB, error, crash						
		Verify any core dumps						
		Verify RSA key does not change on device						
		Verify ssh on device is functional						
		Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers						
		Verify NTP/PTP and Time Zone : ntp.interop.cisco.com						
		Verify Syslog to syslog.interop.cisco.com						
		Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10						
		Verify DNS search list: interop.cisco.com, cisco.com						

		Verify CMP port connections to the management network.						
		Verify CDP neighbors						
		Verify SNMP agent (read community): public + interop; (private community): private + cisco						
		Verify SNMP traps to monitor network events						
		Verify UDLD neighbors and UDLD aggressive mode						
		Verify LACP for link aggregation						
		Verify BFD peering for all possible clients with default protocol timers for the clients						
		Verify SSO/NSF and GR						
		Verify CoPP function						
		Verify CoPP counters						
		Verify hardware rate limiter						
		Verify SPAN ensuring cross-module SPAN.						
		Configure Authentication for: OSPF/OSPFv3, HSRP/HSRPv6, MSDP, Layer 2 ISIS (FabricPath, OTV)						
		Verify DHCP IP helper and primary/backup server						
		Verify interfaces in error						
		OSPF: Verify OSPFv2/OSPFv3 peering.						
		PIM: Verify PIM peering.						
		IGMP/MLD Snooping: Verify IGMP/MLD Snooping						
		ARP & MAC / ND: Verify ARP and MAC addresses are properly learnt across all the forwarding engines.						
		ACL, VACL, PACL: Verify that all the policies are properly programmed in hardware.						
		QoS: Verify QoS marking.						
		DHCP Relay Agent: Verify DHCP relay functionality.						

		BOOTP Relay Agent: Verify BOOTP relay functionality.						
		Verify that there are no dead flows						
1.3.3.5	Setup interfaces from ToR N5k FabricPath to the N7K-202		8	8	0	0	16	
		Verify SSH works through the management network on a dedicated vrf						
		Verify startup and running config						
		Verify TB, error, crash						
		Verify any core dumps						
		Verify RSA key does not change on device						
		Verify ssh on device is functional						
		Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers						
		Verify NTP/PTP and Time Zone : ntp.interop.cisco.com						
		Verify Syslog to syslog.interop.cisco.com						
		Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10						
		Verify DNS search list: interop.cisco.com, cisco.com						
		Verify CMP port connections to the management network.						
		Verify CDP neighbors						
		Verify SNMP agent (read community): public + interop; (private community): private + cisco						
		Verify SNMP traps to monitor network events						
		Verify UDLD neighbors and UDLD aggressive mode						
		Verify LACP for link aggregation						
		Verify BFD peering for all possible clients with default protocol timers for the clients						
		Verify SSO/NSF and GR						

		Verify CoPP function						
		Verify CoPP counters						
		Verify hardware rate limiter						
		Verify SPAN ensuring cross-module SPAN.						
		Configure Authentication for: OSPF/OSPFv3, HSRP/HSRPv6, MSDP, Layer 2 ISIS (FabricPath, OTV)						
		Verify DHCP IP helper and primary/backup server						
		Verify interfaces in error						
		FabricPath: Verify FabricPath route and mac-table are built as expected. Verify IS-IS database. Verify multi-destination trees for broadcast and multicast. Verify fabricpath load-balance works as expe						
		FHRP: Verify FHRP MAC address is programmed in the mac table						
		IGMP/MLD Snooping: Verify IGMP/MLD Snooping						
		STP: Verify RSTP parameters and port status.						
		VACL, PACL: Verify that all the policies are properly programmed in hardware.						
1.3.3.6	Setup interfaces from ToR N3k Layer 3 to C6KE8-104		1	1	0	0	2	
1.3.4	L2 Link Failure/Recovery		156	156	0	0	377	
1.3.4.1	vPC leg failure/recovery between Distribution and ToR devices		36	36	0	0	91	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						

		The maximum traffic disruption for unicast will be half for both upstream and downstream traffic.						
		The maximum traffic loss for multicast upstream will be half and for downstream will be either 100% disrupted or no loss depending on which vPC leg is shut.						
		Multicast forwarder should not change.						
		Verify that there is no protocol flapping.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify mac move and any missing mac address.						
		Verify mac table is empty after link shut.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
		Verify traffic drop based on interface counters.						
		Verify that no flooding happens after traffic convergence.						
		Verify STP port states after link disruption are in the expected forwarding mode. Verify that the STP root does not change.						
		Verify mac addresses are not learned via vPC Peer-Link before primary link shut						
		Verify 30 sec Load Interval Input and output rate of the interfaces to be greater than user Specified rate,Before Shut.						
		Verify CDP is enabled globally						
		Verify LLDP is enabled globally.						
		Verify cdp status are appropriate before failure						
		verify lldp status are appropriate before Failure						
		Verify IGMP is enabled globally						
		Verify traffic drop by checking Rx rate in all ixia ports after Shut						
		Verify flooding by checking Rx rate in all ixia ports after Shut						

		Verify 30 sec Load Interval Input and output rate of the interfaces to be greater than user Specified rate,After Shut.						
		Verify mac addresses are removed from the link after link shut						
		Verify mac addresses are moved from primary link to vPc peer-link after primary link is shut						
		Verify cdp peer entries are lost for affected links						
		Verify cdp entries does not lose peer information for unaffected links						
		Verify lldp peer entries are lost for affected links						
		Verify lldp entries does not lose peer information for unaffected links						
		verify ARP entries after link shut are same as before link shut						
		verify IGMP group membership after link shut is same as before link shut						
		Verify all DHCP Relay entries are same after link shut						
		Verify traffic drop by checking Rx rate in all ixia ports after No Shut						
		Verify flooding by checking Rx rate in all ixia ports after No Shut						
		Verify 30 sec Load Interval Input and output rate of the interfaces to be greater than user Specified rate,After No Shut.						
		Verify there are no missing MAC addresses after no shut						
		Verify vPc Peer-Link no longer has MAC addresses from initial capture of the primary link						
		Verify that cdp entries after No Shut are same as entries taken before						
		Verify that lldp entries after No Shut are same as entries taken before						
		Verify all IGMP snooping entries after link no shut are same as before the link shut						
		verify ARP entries after link no shut are same as before link shut						
		verify IGMP group membership after link no shut is same as before link shut						
		Verify all DHCP Relay entries are same after link no shut						
		Verify VPC information after link no shut is same as before link shut						

		Verify frames delta does not increase before link shut						
		Verify error vlans						
		Verify mac sync for VPC setup (Compare mac entries are same in both VPC peers before shut)						
		Verify that the STP state of all Vlans are in same state that of corresponding STP interface (RSTP) before shut						
		Verify if the STP interfaces are in FWD state (MST) before shut						
		Verify all IGMP snooping entries are same after link shut (vpc link)						
		Verify that SVIs static MAC entries remains same as Before Links Shut						
		Verify frames delta does not increase after link no shut						
		Verify that the STP state of all Vlans are in same state that of corresponding STP interface (RSTP) after no shut						
		Verify if the STP interfaces are in FWD state (MST) after no shut						
		Verify that SVIs static MAC entries after Links No Shut remains same as Before Links Shut						
1.3.4.2	vPC peer-link failure/recovery between Distribution vPC peer switches		4	4	0	0	14	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify that the operational secondary vPC peer will bring down the vPC member ports.						
		Verify that secondary peer will suspend the vpc vlan svi’s.						
		Verify that on recovery, the original states will be re-established.						
		Verify frames delta does not increase.						

		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
1.3.4.3	vPC peer-link member failure/recovery between Distribution vPC peer switches		8	8	0	0	30	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify that the operational secondary vPC peer will bring down the vPC member ports.						
		Verify that secondary peer will suspend the vpc vlan svi's.						
		Verify that on recovery, the original states will be re-established.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
1.3.4.5	L2 port-channel member failure/recovery between Distribution and ToR devices		72	72	0	0	178	
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						

		Verify port-channel load balancing and rbh assignment						
		Verify that IGMP/MLD membership is not affected.						
		The maximum traffic disruption for unicast should be in sub-second range for both upstream and downstream traffic.						
		The maximum traffic loss for member failure multicast will be proportionate to number of members failed						
		Multicast DR should not change.						
		Verify that there is no protocol flapping.						
1.3.4.6	L2 Port-channel Failure/Recovery between Distribution and ToR devices		12	12	0	0	12	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify FHRP peers status does not change. Verify FHRP MAC in ARP/ND table. Verify FHRP MAC address is programmed as a router/static MAC on the active switch and a dynamic entry on the standby switch.						
		Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link.						
		Verify the L2 forwarding table should remove entries of the affected link at the access switch and re-learnt correctly on the alternative link.						
		Verify that MAC's for SVI's are programmed as router/static entries on the switches where they are configured and learned as dynamic entries on the L2 peers.						
		Verify that the L2 forwarding entries on all switches for nodes connected to the access layer are associated with the corresponding STP forwarding ports.						
		Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines.						

		Verify IGMP/MLD snooping entries are deleted for the affected link for non-vpc setup.and re-learnt correctly on the alternative link after query from the IGMP snooping router.						
		Verify that IGMP/MLD membership is not affected on the routers.						
		Verify ACL TCAM is programmed correctly to share for ACL's and features that allow for sharing and verify ACL's are not sharing when not expected.						
		Verify SPAN is mirroring packets correctly.						
		Verify isolated vlans remain to have complete separation from other ports within the same PVLAN but not from the promiscuous ports using proxy-arp.						
		DHCP relay configured on the aggregation switches should remain unaffected.						
		Verify that secondary addresses provide the same capability and services to nodes through DHCP relay, FHRP services, ARP, proxy arp and IGMP.						
		Verify that IPv6 global HSRP is functional.						
		Verify that packets only traverse the fabric for known unicast/multicast destinations and flood through the fabric for unknown unicast, multicast when IGMP snooping is disabled, and broadcast.						
		All unicast and multicast traffic should re-converge with minimal packet loss.						
		Verify SNMP traps are sent to SNMP collector						
		Verify traffic destined for CoPP classes is policed as expected.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify mac move and any missing mac address.						
		Verify mac table is empty after link shut.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
		Verify traffic drop based on interface counters.						

		Verify that no flooding happens after traffic convergence.						
		Verify STP port states after link disruption are in the expected forwarding mode. Verify that the STP root does not change.						
1.3.4.7	vPC peer-link failure/recovery between ToR vPC peer switches		8	8	0	0	20	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify that the operational secondary vPC peer will bring down the vPC member ports.						
		Verify that secondary peer will suspend the vpc vlan svi's.						
		Verify that on recovery, the original states will be re-established.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
1.3.4.8	vPC peer-link member failure/recovery between ToR vPC peer switches		16	16	0	0	32	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						

		Verify any core dumps						
		Verify that the operational secondary vPC peer will bring down the vPC member ports.						
		Verify that secondary peer will suspend the vpc vlan svi's.						
		Verify that on recovery, the original states will be re-established.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
1.3.5	L3 Link Failure/Recovery		386	386	0	0	648	
1.3.5.1	L3 port-channel Failure/Recovery between Core and Distribution Layers		104	104	0	0	211	
		Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines.						
		Verify SPAN is mirroring packets correctly.						
		Verify OTV traffic reconverges and optimize OSPF as needed.						
		Verify SNMP traps are sent to SNMP collector.						
		All unicast and multicast traffic should re-converge with proportionate packet loss.						
		Verify traffic destined for CoPP classes is policed as expected.						
		Verify OSPF interface status for the affected links.						
		Verify OSPF neighbor changes and authentication.						
		Verify OSPF DB/Topology consistency.						
		Verify OSPF routes and forwarding table consistency..						
		Verify OSPF multi-path load-balancing.						
		Verify HW and SW entries are properly programmed and synchronized.						

		Verify PIM neighbor status.						
		Verify PIM both multipath and non-multipath functionalities.						
		Verify AutoRP mapping.						
		Verify static RP mapping as the backup of auto RP.						
		Verify MSDP neighbors and SA cache consistency.						
		Verify multicast HW and SW entries are properly programmed and synchronized.						
		On the multicast LHR, verify (*,G) and (S,G) creation based on SPT-threshold settings.						
		Verify PIM source register and register stop.						
		Verify BFD peer detection and client notifications.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link.						
		Verify the L2 forwarding table should remove entries of the affected link.						
1.3.5.2	L3 port-channel member failure/recovery		128	128	0	0	294	

		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify port-channel load balancing and rbh assignment						
		Verify traffic switches to high Bandwidth port-channels for both unicast and multicast when member failure and traffic will switch back when member recovers.						
		Verify LACP rebundle for port-channel after member recover.						
		The traffic should be able to re-converge within acceptable time.						
		Verify the convergence pattern is as expected.						
		Verify the route tables for both unicast and multicast are updated correctly.						
		Verify the hardware entries, LC programming, fabric programming, outgoing interface, forwarding engine entries, for both unicast and multicast are updated correctly.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
1.3.5.3	L3 member link Failure/Recovery between Core and Distribution Layers		130	130	0	0	119	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						

		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify port-channel load balancing and rbh assignment						
		Verify traffic switches to high Bandwidth port-channels for both unicast and multicast when member failure and traffic will switch back when member recovers.						
		Verify LACP rebundle for port-channel after member recover.						
		The traffic should be able to re-converge within acceptable time.						
		Verify the convergence pattern is as expected.						
		Verify the route tables for both unicast and multicast are updated correctly.						
		Verify the hardware entries, LC programming, fabric programming, outgoing interface, forwarding engine entries, for both unicast and multicast are updated correctly.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
1.3.5.4	L3 Port-channel Failure/Recovery between Distribution and ToR N3K Layer 3		24	24	0	0	24	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						

		Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link.						
		Verify the L2 forwarding table should remove entries of the affected link.						
		Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines.						
		Verify SPAN is mirroring packets correctly.						
		Verify OTV traffic reconverges and optimize OSPF as needed.						
		Verify SNMP traps are sent to SNMP collector.						
		All unicast and multicast traffic should re-converge with proportionate packet loss.						
		Verify traffic destined for CoPP classes is policed as expected.						
		Verify OSPF interface status for the affected links.						
		Verify OSPF neighbor changes and authentication.						
		Verify OSPF DB/Topology consistency.						
		Verify OSPF routes and forwarding table consistency..						
		Verify OSPF multi-path load-balancing.						
		Verify HW and SW entries are properly programmed and synchronized.						
		Verify PIM neighbor status.						
		Verify PIM both multipath and non-multipath functionalities.						
		Verify AutoRP mapping.						
		Verify static RP mapping as the backup of auto RP.						
		Verify MSDP neighbors and SA cache consistency.						
		Verify multicast HW and SW entries are properly programmed and synchronized.						
		On the multicast LHR, verify (*,G) and (S,G) creation based on SPT-threshold settings.						
		Verify PIM source register and register stop.						

		Verify BFD peer detection and client notifications.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
1.3.6	FabricPath - Link Failure/Recovery		744	744	0	0	1132	
1.3.6.1	Fabricpath - Core Link member failure/recovery		576	576	0	0	722	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify port-channel load balancing and RBH assignment.						
		Verify IS-IS database, topology and route distribution for metric change.						
		Verify that IGMP/MLD membership is not affected.						
		Verify that IGMP snooping entries change based on multi-destination tree topology change.						
		The maximum traffic disruption for unicast/multicast should be in sub-second range for both upstream and downstream traffic.						
		Multicast DR should not change.						
		Verify that there is no protocol flapping.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						

		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
1.3.6.2	FabricPath - Core Link Failure/Recovery		144	144	0	0	362	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify FabricPath route and mac-table are built as expected.						
		Verify IS-IS database, topology and route distribution.						
		Verify multi-destination trees for broadcast and multicast.						
		Verify fabricpath load-balance works as expected.						
		Verify FHRP peers status does not change.						
		Verify FHRP MAC in ARP/ND table.						
		Verify FHRP MAC address is programmed as a router/static MAC on the active switch and a dynamic entry on the standby switch.						
		Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link.						
		Verify SNMP traps are sent to SNMP collector.						
		Verify that MAC's for SVI's are programmed as router/static entries on the switches where they are configured and learned as dynamic entries on the L2 peers.						
		On the aggregation switches, verify that the ARP/ND are programmed as adjacencies for L3 next hop forwarding.						
		Verify that no flooding happens after traffic convergence.						

		Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines.						
		Verify IGMP/MLD snooping entries are deleted for the affected link and re-learnt correctly on the alternative link after query from the IGMP snooping router.						
		Verify that IGMP/MLD membership is not affected on the routers.						
		Verify SPAN is mirroring packets correctly.						
		DHCP relay configured on the aggregation switches should remain unaffected.						
		Verify that secondary addresses provide the same capability and services to nodes through DHCP relay, FHRP services, ARP, proxy arp and IGMP.						
		Verify that IPv6 global HSRP is functional.						
		Verify that packets only traverse the fabric for known unicast/multicast destinations and flood through the fabric for unknown unicast, multicast when IGMP snooping is disabled, and broadcast.						
		All unicast and multicast traffic should re-converge with minimal packet loss.						
		Verify traffic destined for CoPP classes is policed as expected.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
1.3.6.3	Fabricpath - vPC+ peer-link failure/recovery (spine/leaf)		8	8	0	0	16	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						

		Verify any core dumps						
		Verify that the operational secondary vPC+ peer will bring down the vPC+ member ports.						
		Verify that secondary peer will not suspend the vPC+ vlan SVI's if "dual-active exclude vlans" is configured						
		Verify on recovery that the operational secondary vPC+ peer will bring up the vPC+ member ports after the configured "delay restore" timer						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
1.3.6.4	Fabricpath - vPC+ peer-link member failure/recovery (spine/leaf)		16	16	0	0	32	
1.3.7	Supervisor and Fabric HA		4	3	1	0	30	
1.3.7.1	Supervisor HA on the edge/core layer		2	2	0	0	4	CSCun71884, CSCun11736, CSCun11692
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Compare startup/running configuration on Active Sup and Standby Sup before and after SSO.						
		Verify BGP neighbors status and authentication.						
		Verify BGP table and routing table consistency in accordance to the NEXT-HOP attribute settings.						
		Verify proper BGP policy routing and filtering based on prefix, AS-PATH, LOCAL_PREFERENCE attributes.						

		Verify the conditional injection of the default route from BGP into the IGP.						
		Verify BGP recursive lookup scenario.						
		Verify BGP reconvergence (control-plane & data-plane).						
		Verify OSPF interface status.						
		Verify OSPF neighbor changes and authentication.						
		Verify OSPF DB/Topology consistency.						
		Verify OSPF routes and forwarding table consistency..						
		Verify HW and SW entries are properly programmed and synchronized after SSO.						
		Verify PIM neighbor status.						
		Verify static RP mapping as the backup of auto RP.						
		Verify MSDP neighbors and SA cache consistency.						
		Verify multicast HW and SW entries are properly programmed and synchronized after SSO.						
		Verify BFD peer should not flap during and after SSO.						
		No traffic loss is expected.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
1.3.7.2	Supervisor HA on the Distribution layer		2	1	1	0	26	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						

		Verify interfaces in error						
		Verify any core dumps						
		Compare startup/running configuration on Active Sup and Standby Sup before and after SSO.						
		Verify STP port states during and after SSO.						
		Verify FHRP peers status during and after SSO.						
		Verify CDP/LLDP status after SSO.						
		Verify ARP/ND tables remain unaffected						
		Verify FHRP MAC in ARP/ND table.						
		Verify OTV ARP optimization/ARP caching works as expected after SSO.						
		Verify head-end replication for multicast traffic on unicast-only transport works as expected, check the data-group mapping table for receiver information.						
		Verify automated mapping of OTV sites multicast groups to transport multicast group.						
		Verify FHRP MAC address is programmed as a router/static MAC on the active switch and a dynamic entry on the standby switch.						
		Verify that MAC's for SVI's are programmed as router/static entries on the switches where they are configured and learned as dynamic entries on the L2 peers.						
		On the aggregation switches, verify that the ARP/ND are programmed as adjacencies for L3 next hop forwarding after SSO.						
		Verify IGMP snooping entries remain unaffected.						
		Verify that no flooding happens after traffic convergence.						
		Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines.						
		Verify SPAN is mirroring packets correctly during and after SSO.						
		Verify SNMP traps are sent to SNMP collector.						
		Verify traffic destined for CoPP classes is policed as expected.						
		Verify OSPF interface status.						

		Verify OSPF neighbor changes and authentication.						
		Verify OSPF DB/Topology consistency.						
		Verify OSPF routes and forwarding table consistency..						
		Verify HW and SW entries are properly programmed and synchronized after SSO.						
		Verify PIM neighbor status.						
		Verify static RP mapping as the backup of auto RP.						
		Verify MSDP neighbors and SA cache consistency.						
		Verify multicast HW and SW entries are properly programmed and synchronized after SSO.						
		Verify BFD peer should not flap during and after SSO.						
		Verify vPC peer status (role, peer link, keepalive link and consistency parameters) before and after SSO						
		No traffic loss is expected.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
1.3.8	Configuration Change		2	2	0	0	4	
1.3.8.1	Perform VPC Vlan add and delete		2	2	0	0	4	
		Verify STP port states after each change are in the expected forwarding mode.						
1.3.9	Linecard OIR/Reset		8	8	0	0	16	
1.3.9.1	L3 port-channel member failure/recovery, on OIR/reset line card		8	8	0	0	16	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						

		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify hitless operation for non-affected ports						
		Verify traffic load-balancing for distributed port-channels before and after OIR/reset						
		Verify BGP/ IGP/ PIM reconvergence (control-plane & data plane)						
		Verfiy BFD peer detection and client notifications						
		Verify LACP interoperability for distributed port-channels						
		Verify that CDP/LLDP does not lose peer information for non-affected line card. Verify that CDP/LLDP peer is removed for disrupted line cards.						
		Verify the L2 forwarding table should be re-learnt correctly after OIR/reset.						
		Verify that no flooding happens after traffic convergence.						
		Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines.						
		Verify SPAN is mirroring packets correctly.						
		Verify SNMP traps are sent to SNMP collector.						
		All unicast and multicast traffic should re-converge with minimal packet loss.						
		Verify traffic destined for CoPP classes is policed as expected.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
1.3.10	FabricPath - Linecard OIR/Reset		8	8	0	0	16	
1.3.10.1	OIR/reset line card on spine nodes		8	8	0	0	16	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						

		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify hitless operation for non-affected ports						
		Verify traffic load-balancing for distributed port-channels before and after OIR/reset						
		Verify BGP/ IGP/ PIM reconvergence (control-plane & data plane)						
		Verfiy BFD peer detection and client notifications						
		Verify LACP interoperability for distributed port-channels						
		Verify that CDP/LLDP does not lose peer information for non-affected line card. Verify that CDP/LLDP peer is removed for disrupted line cards.						
		Verify the L2 forwarding table should be re-learnt correctly after OIR/reset.						
		Verify that no flooding happens after traffic convergence.						
		Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines.						
		Verify SPAN is mirroring packets correctly.						
		Verify SNMP traps are sent to SNMP collector.						
		All unicast and multicast traffic should re-converge with minimal packet loss.						
		Verify traffic destined for CoPP classes is policed as expected.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
1.3.11	Reload and Power Cycle Switch		6	3	0	3	20	

1.3.11.1	Reload and Power Cycle Edge/Core Switch		6	3	0	3	20	CSCum54359, CSCum55746, CSCul44598
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify BGP neighbors status and authentication.						
		Verify BGP table and routing table consistency in accordance to the NEXT-HOP attribute settings.						
		Verify BGP multi-path load-balancing.						
		Verify proper BGP policy routing and filtering based on prefix, AS-PATH, LOCAL_PREFERENCE attributes.						
		Verify the conditional injection of the default route from BGP into the IGP.						
		Verify BGP recursive lookup scenario.						
		Verify BGP reconvergence (control-plane & data-plane).						
		Verify OSPF interface status for the affected links.						
		Verify OSPF neighbor changes and authentication.						
		Verify OSPF DB/Topology consistency.						
		Verify OSPF routes and forwarding table consistency..						
		Verify OSPF multi-path load-balancing.						
		Verify HW and SW entries are properly programmed and synchronized.						
		Verify PIM neighbor status.						
		Verify PIM both multipath and non-multipath functionalities.						

		Verify AutoRP mapping and boundaries.						
		Verify static RP mapping as the backup of auto RP.						
		Verify MSDP neighbors and SA cache consistency.						
		Verify multicast HW and SW entries are properly programmed and synchronized.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
1.3.12	FabricPath - Reload		4	3	0	1	10	
1.3.12.1	FabricPath - Spine Node failure/recovery		4	3	0	1	10	CSCun66981
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify Fabricpath multi-destination trees reconverge after root change on node failure.						
		Verify FabricPath route and mac-table are built as expected.						
		Verify IS-IS database, topology and route distribution.						
		Verify FHRP MAC address is programmed as a router/static MAC on the active switch and a dynamic entry on the standby switch.						
		Verify that MAC's for SVI's are programmed as router/static entries on the switches where they are configured and learned as dynamic entries on the L2 peers.						
		On the distribution switches, verify that the ARP/ND are programmed as adjacencies for L3 next hop forwarding.						
		Verify that no flooding happens after traffic convergence.						

		Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines on the other spine routers						
		Verify IGMP/MLD snooping entries are deleted for the affected link for non-vpc setup.and re-learnt correctly on the alternative link after query from the IGMP snooping router.						
		Verify that IGMP/MLD membership is not affected on the other spine routers.						
		Verify SPAN is mirroring packets correctly.						
		Verify SNMP traps are sent to SNMP collector.						
		DHCP relay configured on the aggregation switches should remain unaffected.						
		Verify that secondary addresses provide the same capability and services to nodes through DHCP relay, FHRP services, ARP, proxy arp and IGMP.						
		All unicast and multicast traffic should re-converge with minimal packet loss.						
		Verify traffic destined for CoPP classes is policed as expected.						
		Verify that the MAC table, FP ISIS route table, ARP/ND table, IP routing table, IGMP membership table, IGMP snooping table, Multicast routing table return to original state on recovery						
		Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines on recovery						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
1.3.13	ISSU/ISSD/Image Change		32	28	0	4	45	
1.3.13.1	6.2.x/6.2.8		32	28	0	4	45	CSCum86511, CSCun64129, CSCuo36637, CSCuh58228
		Verify if ISSU image compatibility for non-disruptive upgrade/downgrade						
		Verify ISSU/ISSD happens as expected. OSPF graceful restart, PIM triggered Joins should work as expected.						
		Compare startup/running configuration on Active Sup and Standby Sup before and after ISSU/ISSD.						
		Verify STP port states during and after ISSU/ISSD.						

		Verify FHRP peers status during and after ISSU/ISSD.						
		Verify CDP/LLDP status after ISSU/ISSD.						
		Verify FHRP MAC in ARP/ND table.						
		Verify FHRP MAC address is programmed as a router/static MAC on the active switch and a dynamic entry on the standby switch.						
		Verify that MAC's for SVI's are programmed as router/static entries on the switches where they are configured and learned as dynamic entries on the L2 peers.						
		On the distribution switches, verify that the ARP/ND are programmed as adjacencies for L3 next hop forwarding after ISSU/ISSD.						
		Verify that no flooding happens after traffic convergence.						
		Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines.						
		Verify SPAN is mirroring packets correctly during and after ISSU/ISSD.						
		Verify SNMP traps are sent to SNMP collector.						
		Verify traffic destined for CoPP classes is policed as expected.						
		Verify BGP neighbors status and authentication.						
		Verify BGP table and routing table consistency in accordance to the NEXT-HOP attribute settings.						
		Verify proper BGP policy routing and filtering based on prefix, AS-PATH, LOCAL_PREFERENCE attributes.						
		Verify the conditional injection of the default route from BGP into the IGP.						
		Verify BGP recursive lookup scenario.						
		Verify BGP reconvergence for control-plane.						
		Verify OSPF interface status.						
		Verify OSPF neighbor changes and authentication.						
		Verify OSPF DB/Topology consistency.						
		Verify OSPF routes and forwarding table consistency.						

		Verify HW and SW entries are properly programmed and synchronized after ISSU/ISSD.						
		Verify PIM neighbor status.						
		Verify static RP mapping as the backup of auto RP.						
		Verify MSDP neighbors and SA cache consistency.						
		Verify multicast HW and SW entries are properly programmed and synchronized after ISSU/ISSD.						
		Verify BFD peer should not flap during and after ISSU/ISSD.						
		No traffic loss is expected.						
		If ISSU is disruptive, verify that all unicast/multicast traffic reconverges.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
1.3.15	Clear IPv4/IPv6 Multicast Routes		8	8	0	0	16	
1.3.15.1	Clear Pim Routes		4	4	0	0	8	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		All multicast traffic should re-converge.						
		Verify periodic PIM joins are received and sent upstream after clearing.						
		Verify that the multicast hardware entries are properly removed and re-installed during the mroute flaps						

		Verify that CDP/LLDP does not lose peer information.						
		Verify that no flooding happens after traffic convergence.						
		Verify PIM neighbor status.						
		Verify PIM both multipath and non-multipath functionalities.						
		Verify AutoRP mapping.						
		On the multicast LHR, verify (*,G) and (S,G) creation based on SPT-threshold settings.						
		Verify PIM source register and register stop.						
		Verify IGMP/MLD snooping entries are deleted and re-learnt correctly after query from the IGMP snooping router.						
		Verify SPAN is mirroring packets correctly.						
		Verify SNMP traps are sent to SNMP collector.						
		Verify traffic destined for CoPP classes is policed as expected.						
		Verify the hardware entries, LC programming, fabric programming, outgoing interface, forwarding engine entries, for both unicast and multicast are updated correctly.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
1.3.15.2	Clear IPv4/IPv6 Multicast Routes		4	4	0	0	8	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						

		All multicast traffic should re-converge.						
		Verify periodic PIM joins are received and sent upstream after clearing.						
		Verify that the multicast hardware entries are properly removed and re-installed during the mroute flaps						
		Verify that CDP/LLDP does not lose peer information.						
		Verify that no flooding happens after traffic convergence.						
		Verify PIM neighbor status.						
		Verify PIM both multipath and non-multipath functionalities.						
		Verify AutoRP mapping.						
		On the multicast LHR, verify (*,G) and (S,G) creation based on SPT-threshold settings.						
		Verify PIM source register and register stop.						
		Verify IGMP/MLD snooping entries are deleted and re-learnt correctly after query from the IGMP snooping router.						
		Verify SPAN is mirroring packets correctly.						
		Verify SNMP traps are sent to SNMP collector.						
		Verify traffic destined for CoPP classes is policed as expected.						
		Verify the hardware entries, LC programming, fabric programming, outgoing interface, forwarding engine entries, for both unicast and multicast are updated correctly.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
1.4	**DC1**		671	670	0	1	1464	
1.4.1	Core to Distribution Setup		2	2	0	0	4	
1.4.1.1	Setup interfaces from Core to Distribution blocks		2	2	0	0	4	
		Verify SSH works through the management network on a dedicated vrf						

		Verify startup and running config						
		Verify TB, error, crash						
		Verify any core dumps						
		Verify RSA key does not change on device						
		Verify ssh on device is functional						
		Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers						
		Verify NTP/PTP and Time Zone : ntp.interop.cisco.com						
		Verify Syslog to syslog.interop.cisco.com						
		Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10						
		Verify DNS search list: interop.cisco.com, cisco.com						
		Verify CMP port connections to the management network.						
		Verify CDP neighbors						
		Verify SNMP agent (read community): public + interop; (private community): private + cisco						
		Verify SNMP traps to monitor network events						
		Verify UDLD neighbors and UDLD aggressive mode						
		Verify LACP for link aggregation						
		Verify BFD peering for all possible clients with default protocol timers for the clients						
		Verify CoPP function						
		Verify CoPP counters						
		Verify hardware rate limiter						
		Verify SPAN ensuring cross-module SPAN.						
		Configure Authentication for: OSPF/OSPFv3, HSRP/HSRPv6, MSDP, Layer 2 ISIS (FabricPath, OTV)						
		Verify DHCP IP helper and primary/backup server						

		Verify interfaces in error						
		OSPF: Verify OSPFv2/OSPFv3 peering.						
		PIM: Verify PIM peering.						
		MSDP: Verify MSDP peering and SA-cache						
		Verify that there are no dead flows						
		Verify SSO/NSF and GR						
1.4.2	Distribution to Core Setup		16	16	0	0	36	
1.4.2.1	Setup interfaces from Distribution N7K-101 to the core switches		4	4	0	0	24	
		Verify SSH works through the management network on a dedicated vrf						
		Verify startup and running config						
		Verify TB, error, crash						
		Verify any core dumps						
		Verify RSA key does not change on device						
		Verify ssh on device is functional						
		Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers						
		Verify NTP/PTP and Time Zone : ntp.interop.cisco.com						
		Verify Syslog to syslog.interop.cisco.com						
		Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10						
		Verify DNS search list: interop.cisco.com, cisco.com						
		Verify CMP port connections to the management network.						
		Verify CDP neighbors						
		Verify SNMP agent (read community): public + interop; (private community): private + cisco						
		Verify SNMP traps to monitor network events						

		Verify UDLD neighbors and UDLD aggressive mode						
		Verify LACP for link aggregation						
		Verify BFD peering for all possible clients with default protocol timers for the clients						
		Verify SSO/NSF and GR						
		Verify CoPP function						
		Verify CoPP counters						
		Verify hardware rate limiter						
		Verify SPAN ensuring cross-module SPAN.						
		Configure Authentication for: OSPF/OSPFv3, HSRP/HSRPv6, MSDP, Layer 2 ISIS (FabricPath, OTV)						
		Verify DHCP IP helper and primary/backup server						
		Verify interfaces in error						
		OSPF: Verify OSPFv2/OSPFv3 peering.						
		PIM: Verify PIM peering.						
		OTV: Verify OTV ISIS adjacencies are properly established and OTV routing table. Verify the primary AS is being used. On the primary AS, verify all edge devices show up in the unicast replication list						
		Verify that there are no dead flows						
1.4.2.2	Setup interfaces from Distribution N7K-102 to the core switches		4	4	0	0	4	
		Verify SSH works through the management network on a dedicated vrf						
		Verify startup and running config						
		Verify TB, error, crash						
		Verify any core dumps						
		Verify RSA key does not change on device						
		Verify ssh on device is functional						

		Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers						
		Verify NTP/PTP and Time Zone : ntp.interop.cisco.com						
		Verify Syslog to syslog.interop.cisco.com						
		Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10						
		Verify DNS search list: interop.cisco.com, cisco.com						
		Verify CMP port connections to the management network.						
		Verify CDP neighbors						
		Verify SNMP agent (read community): public + interop; (private community): private + cisco						
		Verify SNMP traps to monitor network events						
		Verify UDLD neighbors and UDLD aggressive mode						
		Verify LACP for link aggregation						
		Verify BFD peering for all possible clients with default protocol timers for the clients						
		Verify SSO/NSF and GR						
		Verify CoPP function						
		Verify CoPP counters						
		Verify hardware rate limiter						
		Verify SPAN ensuring cross-module SPAN.						
		Configure Authentication for: OSPF/OSPFv3, HSRP/HSRPv6, MSDP, Layer 2 ISIS (FabricPath, OTV)						
		Verify DHCP IP helper and primary/backup server						
		Verify interfaces in error						
		OSPF: Verify OSPFv2/OSPFv3 peering.						
		PIM: Verify PIM peering.						
		OTV: Verify OTV ISIS adjacencies are properly established and OTV						

		routing table. Verify the primary AS is being used. On the primary AS, verify all edge devices show up in the unicast replication list						
		Verify that there are no dead flows						
1.4.2.3	Setup interfaces from Distribution C6KE8 VSS to the core switches		1	1	0	0	1	
		Verify SSH works through the management network on a dedicated vrf						
		Verify startup and running config						
		Verify TB, error, crash						
		Verify any core dumps						
		Verify RSA key does not change on device						
		Verify ssh on device is functional						
		Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers						
		Verify NTP/PTP and Time Zone : ntp.interop.cisco.com						
		Verify Syslog to syslog.interop.cisco.com						
		Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10						
		Verify DNS search list: interop.cisco.com, cisco.com						
		Verify CMP port connections to the management network.						
		Verify CDP neighbors						
		Verify SNMP agent (read community): public + interop; (private community): private + cisco						
		Verify SNMP traps to monitor network events						
		Verify UDLD neighbors and UDLD aggressive mode						
		Verify LACP for link aggregation						
		Verify BFD peering for all possible clients with default protocol timers for the clients						
		Verify SSO/NSF and GR						

		Verify CoPP function						
		Verify CoPP counters						
		Verify hardware rate limiter						
		Verify SPAN ensuring cross-module SPAN.						
		Configure Authentication for: OSPF/OSPFv3, HSRP/HSRPv6, MSDP, Layer 2 ISIS (FabricPath, OTV)						
		Verify DHCP IP helper and primary/backup server						
		Verify interfaces in error						
		OSPF: Verify OSPFv2/OSPFv3 peering.						
		PIM: Verify PIM peering.						
		Verify that there are no dead flows						
1.4.2.4	Setup interfaces from Distribution C6KE8 to the core switches		2	2	0	0	2	
		Verify SSH works through the management network on a dedicated vrf						
		Verify startup and running config						
		Verify TB, error, crash						
		Verify any core dumps						
		Verify RSA key does not change on device						
		Verify ssh on device is functional						
		Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers						
		Verify NTP/PTP and Time Zone : ntp.interop.cisco.com						
		Verify Syslog to syslog.interop.cisco.com						
		Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10						
		Verify DNS search list: interop.cisco.com, cisco.com						
		Verify CMP port connections to the management network.						

		Verify CDP neighbors						
		Verify SNMP agent (read community): public + interop; (private community): private + cisco						
		Verify SNMP traps to monitor network events						
		Verify UDLD neighbors and UDLD aggressive mode						
		Verify LACP for link aggregation						
		Verify BFD peering for all possible clients with default protocol timers for the clients						
		Verify SSO/NSF and GR						
		Verify CoPP function						
		Verify CoPP counters						
		Verify hardware rate limiter						
		Verify SPAN ensuring cross-module SPAN.						
		Configure Authentication for: OSPF/OSPFv3, HSRP/HSRPv6, MSDP, Layer 2 ISIS (FabricPath, OTV)						
		Verify DHCP IP helper and primary/backup server						
		Verify interfaces in error						
		OSPF: Verify OSPFv2/OSPFv3 peering.						
		PIM: Verify PIM peering.						
		Verify that there are no dead flows						
1.4.2.5	Setup interfaces from Distribution C6KE7 VSS to the core switches		1	1	0	0	1	
		Verify SSH works through the management network on a dedicated vrf						
		Verify startup and running config						
		Verify TB, error, crash						
		Verify any core dumps						
		Verify RSA key does not change on device						

		Verify ssh on device is functional						
		Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers						
		Verify NTP/PTP and Time Zone : ntp.interop.cisco.com						
		Verify Syslog to syslog.interop.cisco.com						
		Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10						
		Verify DNS search list: interop.cisco.com, cisco.com						
		Verify CMP port connections to the management network.						
		Verify CDP neighbors						
		Verify SNMP agent (read community): public + interop; (private community): private + cisco						
		Verify SNMP traps to monitor network events						
		Verify UDLD neighbors and UDLD aggressive mode						
		Verify LACP for link aggregation						
		Verify BFD peering for all possible clients with default protocol timers for the clients						
		Verify SSO/NSF and GR						
		Verify CoPP function						
		Verify CoPP counters						
		Verify hardware rate limiter						
		Verify SPAN ensuring cross-module SPAN.						
		Configure Authentication for: OSPF/OSPFv3, HSRP/HSRPv6, MSDP, Layer 2 ISIS (FabricPath, OTV)						
		Verify DHCP IP helper and primary/backup server						
		Verify interfaces in error						
		OSPF: Verify OSPFv2/OSPFv3 peering.						
		PIM: Verify PIM peering.						

		Verify that there are no dead flows						
1.4.2.6	Setup interfaces from Distribution C6KE7 to the core switches		2	2	0	0	2	
		Verify SSH works through the management network on a dedicated vrf						
		Verify startup and running config						
		Verify TB, error, crash						
		Verify any core dumps						
		Verify RSA key does not change on device						
		Verify ssh on device is functional						
		Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers						
		Verify NTP/PTP and Time Zone : ntp.interop.cisco.com						
		Verify Syslog to syslog.interop.cisco.com						
		Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10						
		Verify DNS search list: interop.cisco.com, cisco.com						
		Verify CMP port connections to the management network.						
		Verify CDP neighbors						
		Verify SNMP agent (read community): public + interop; (private community): private + cisco						
		Verify SNMP traps to monitor network events						
		Verify UDLD neighbors and UDLD aggressive mode						
		Verify LACP for link aggregation						
		Verify BFD peering for all possible clients with default protocol timers for the clients						
		Verify SSO/NSF and GR						
		Verify CoPP function						

		Verify CoPP counters						
		Verify hardware rate limiter						
		Verify SPAN ensuring cross-module SPAN.						
		Configure Authentication for: OSPF/OSPFv3, HSRP/HSRPv6, MSDP, Layer 2 ISIS (FabricPath, OTV)						
		Verify DHCP IP helper and primary/backup server						
		Verify interfaces in error						
		OSPF: Verify OSPFv2/OSPFv3 peering.						
		PIM: Verify PIM peering.						
		Verify that there are no dead flows						
1.4.2.7	Setup interfaces from Distribution C4K to the core switches		2	2	0	0	2	
		Verify SSH works through the management network on a dedicated vrf						
		Verify startup and running config						
		Verify TB, error, crash						
		Verify any core dumps						
		Verify RSA key does not change on device						
		Verify ssh on device is functional						
		Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers						
		Verify NTP/PTP and Time Zone : ntp.interop.cisco.com						
		Verify Syslog to syslog.interop.cisco.com						
		Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10						
		Verify DNS search list: interop.cisco.com, cisco.com						
		Verify CMP port connections to the management network.						
		Verify CDP neighbors						

		Verify SNMP agent (read community): public + interop; (private community): private + cisco						
		Verify SNMP traps to monitor network events						
		Verify UDLD neighbors and UDLD aggressive mode						
		Verify LACP for link aggregation						
		Verify BFD peering for all possible clients with default protocol timers for the clients						
		Verify SSO/NSF and GR						
		Verify CoPP function						
		Verify CoPP counters						
		Verify hardware rate limiter						
		Verify SPAN ensuring cross-module SPAN.						
		Configure Authentication for: OSPF/OSPFv3, HSRP/HSRPv6, MSDP, Layer 2 ISIS (FabricPath, OTV)						
		Verify DHCP IP helper and primary/backup server						
		Verify interfaces in error						
		OSPF: Verify OSPFv2/OSPFv3 peering.						
		PIM: Verify PIM peering.						
		Verify that there are no dead flows						
1.4.3	ToR to Distribution Setup		17	17	0	0	17	
1.4.3.1	Setup vPC interface from ToR Layer 2 Switch to N7k-101		2	2	0	0	2	
		Verify SSH works through the management network on a dedicated vrf						
		Verify startup and running config						
		Verify TB, error, crash						
		Verify any core dumps						
		Verify RSA key does not change on device						

		Verify ssh on device is functional						
		Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers						
		Verify NTP/PTP and Time Zone : ntp.interop.cisco.com						
		Verify Syslog to syslog.interop.cisco.com						
		Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10						
		Verify DNS search list: interop.cisco.com, cisco.com						
		Verify CMP port connections to the management network.						
		Verify CDP neighbors						
		Verify SNMP agent (read community): public + interop; (private community): private + cisco						
		Verify SNMP traps to monitor network events						
		Verify UDLD neighbors and UDLD aggressive mode						
		Verify LACP for link aggregation						
		Verify BFD peering for all possible clients with default protocol timers for the clients						
		Verify SSO/NSF and GR						
		Verify CoPP function						
		Verify CoPP counters						
		Verify hardware rate limiter						
		Verify SPAN ensuring cross-module SPAN.						
		Configure Authentication for: OSPF/OSPFv3, HSRP/HSRPv6, MSDP, Layer 2 ISIS (FabricPath, OTV)						
		Verify DHCP IP helper and primary/backup server						
		Verify interfaces in error						
		STP: Verify RSTP parameters and port status.						
		IGMP/MLD Snooping: Verify IGMP/MLD Snooping						

		VACL, PACL: Verify that all the policies are properly programmed in hardware.						
		Verify that there are no dead flows						
1.4.3.2	Setup vPC interface from ToR Layer 2 Switch to N7k-102		3	3	0	0	3	
		Verify SSH works through the management network on a dedicated vrf						
		Verify startup and running config						
		Verify TB, error, crash						
		Verify any core dumps						
		Verify RSA key does not change on device						
		Verify ssh on device is functional						
		Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers						
		Verify NTP/PTP and Time Zone : ntp.interop.cisco.com						
		Verify Syslog to syslog.interop.cisco.com						
		Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10						
		Verify DNS search list: interop.cisco.com, cisco.com						
		Verify CMP port connections to the management network.						
		Verify CDP neighbors						
		Verify SNMP agent (read community): public + interop; (private community): private + cisco						
		Verify SNMP traps to monitor network events						
		Verify UDLD neighbors and UDLD aggressive mode						
		Verify LACP for link aggregation						
		Verify BFD peering for all possible clients with default protocol timers for the clients						
		Verify SSO/NSF and GR						

		Verify CoPP function						
		Verify CoPP counters						
		Verify hardware rate limiter						
		Verify SPAN ensuring cross-module SPAN.						
		Configure Authentication for: OSPF/OSPFv3, HSRP/HSRPv6, MSDP, Layer 2 ISIS (FabricPath, OTV)						
		Verify DHCP IP helper and primary/backup server						
		Verify interfaces in error						
		STP: Verify RSTP parameters and port status.						
		IGMP/MLD Snooping: Verify IGMP/MLD Snooping						
		VACL, PACL: Verify that all the policies are properly programmed in hardware.						
		Verify that there are no dead flows						
1.4.3.3	Setup interfaces from ToR N3k Layer 3 to N7k-102		1	1	0	0	1	
		Verify SSH works through the management network on a dedicated vrf						
		Verify startup and running config						
		Verify TB, error, crash						
		Verify any core dumps						
		Verify RSA key does not change on device						
		Verify ssh on device is functional						
		Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers						
		Verify NTP/PTP and Time Zone : ntp.interop.cisco.com						
		Verify Syslog to syslog.interop.cisco.com						
		Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10						

		Verify DNS search list: interop.cisco.com, cisco.com						
		Verify CMP port connections to the management network.						
		Verify CDP neighbors						
		Verify SNMP agent (read community): public + interop; (private community): private + cisco						
		Verify SNMP traps to monitor network events						
		Verify UDLD neighbors and UDLD aggressive mode						
		Verify LACP for link aggregation						
		Verify BFD peering for all possible clients with default protocol timers for the clients						
		Verify SSO/NSF and GR						
		Verify CoPP function						
		Verify CoPP counters						
		Verify hardware rate limiter						
		Verify SPAN ensuring cross-module SPAN.						
		Configure Authentication for: OSPF/OSPFv3, HSRP/HSRPv6, MSDP, Layer 2 ISIS (FabricPath, OTV)						
		Verify DHCP IP helper and primary/backup server						
		Verify interfaces in error						
		OSPF: Verify OSPFv2/OSPFv3 peering.						
		PIM: Verify PIM peering.						
		IGMP/MLD Snooping: Verify IGMP/MLD Snooping						
		ARP & MAC / ND: Verify ARP and MAC addresses are properly learnt across all the forwarding engines.						
		ACL, VACL, PACL: Verify that all the policies are properly programmed in hardware.						
		QoS: Verify QoS marking.						
		DHCP Relay Agent: Verify DHCP relay functionality.						

		BOOTP Relay Agent: Verify BOOTP relay functionality.						
		Verify that there are no dead flows						
1.4.3.4	Setup interfaces from ToR N3k Layer 3 to C6KE8-104		1	1	0	0	1	
		Verify SSH works through the management network on a dedicated vrf						
		Verify startup and running config						
		Verify TB, error, crash						
		Verify any core dumps						
		Verify RSA key does not change on device						
		Verify ssh on device is functional						
		Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers						
		Verify NTP/PTP and Time Zone : ntp.interop.cisco.com						
		Verify Syslog to syslog.interop.cisco.com						
		Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10						
		Verify DNS search list: interop.cisco.com, cisco.com						
		Verify CMP port connections to the management network.						
		Verify CDP neighbors						
		Verify SNMP agent (read community): public + interop; (private community): private + cisco						
		Verify SNMP traps to monitor network events						
		Verify LACP for link aggregation						
		Verify BFD peering for all possible clients with default protocol timers for the clients						
		Verify SSO/NSF and GR						
		Verify CoPP function						

		Verify CoPP counters						
		Verify hardware rate limiter						
		Verify SPAN ensuring cross-module SPAN.						
		Configure Authentication for: OSPF/OSPFv3, HSRP/HSRPv6, MSDP, Layer 2 ISIS (FabricPath, OTV)						
		Verify interfaces in error						
		OSPF: Verify OSPFv2/OSPFv3 peering.						
		PIM: Verify PIM peering.						
		IGMP/MLD Snooping: Verify IGMP/MLD Snooping						
		ARP & MAC / ND: Verify ARP and MAC addresses are properly learnt across all the forwarding engines.						
		ACL, VACL, PACL: Verify that all the policies are properly programmed in hardware.						
		DHCP Relay Agent: Verify DHCP relay functionality.						
		BOOTP Relay Agent: Verify BOOTP relay functionality.						
		Verify that there are no dead flows						
		Verify UDLD neighbors and UDLD aggressive mode						
		Verify DHCP IP helper and primary/backup server						
		QoS: Verify QoS marking.						
1.4.3.5	Setup interfaces from ToR N5k vPC Switch to N7k-101		4	4	0	0	4	
		Verify SSH works through the management network on a dedicated vrf						
		Verify TB, error, crash						
		Verify any core dumps						
		Verify ssh on device is functional						
		Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers						

		Verify NTP/PTP and Time Zone : ntp.interop.cisco.com						
		Verify Syslog to syslog.interop.cisco.com						
		Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10						
		Verify DNS search list: interop.cisco.com, cisco.com						
		Verify CMP port connections to the management network.						
		Verify CDP neighbors						
		Verify SNMP agent (read community): public + interop; (private community): private + cisco						
		Verify SNMP traps to monitor network events						
		Verify UDLD neighbors and UDLD aggressive mode						
		Verify LACP for link aggregation						
		Verify BFD peering for all possible clients with default protocol timers for the clients						
		Verify SSO/NSF and GR						
		Verify CoPP function						
		Verify CoPP counters						
		Verify hardware rate limiter						
		Verify SPAN ensuring cross-module SPAN.						
		Configure Authentication for: OSPF/OSPFv3, HSRP/HSRPv6, MSDP, Layer 2 ISIS (FabricPath, OTV)						
		Verify DHCP IP helper and primary/backup server						
		Verify interfaces in error						
		vPC: Verify vPC peer status and consistency parameters. Check MAC/ARP/ND/igmp snooping synchronization.						
		IGMP/MLD Snooping: Verify IGMP/MLD Snooping						
		STP: Verify RSTP parameters and port status.						
		VACL, PACL: Verify that all the policies are properly programmed						

		in hardware.						
		Verify that there are no dead flows						
		Verify startup and running config						
		Verify RSA key does not change on device						
1.4.3.6	Setup interfaces from ToR N5k FabricPath to the N7k-102		6	6	0	0	6	
		Verify startup and running config						
		Verify any core dumps						
		Verify RSA key does not change on device						
		Verify ssh on device is functional						
		Verify Tacacs+ (tacacs.interop.cisco.com) and primary/backup servers						
		Verify NTP/PTP and Time Zone : ntp.interop.cisco.com						
		Verify DNS domain : interop.cisco.com and server : 172.28.92.9-10						
		Verify DNS search list: interop.cisco.com, cisco.com						
		Verify CMP port connections to the management network.						
		Verify CDP neighbors						
		Verify SNMP agent (read community): public + interop; (private community): private + cisco						
		Verify SNMP traps to monitor network events						
		Verify UDLD neighbors and UDLD aggressive mode						
		Verify LACP for link aggregation						
		Verify BFD peering for all possible clients with default protocol timers for the clients						
		Verify SSO/NSF and GR						
		Verify CoPP function						
		Verify CoPP counters						

		Verify hardware rate limiter						
		Verify SPAN ensuring cross-module SPAN.						
		Configure Authentication for: OSPF/OSPFv3, HSRP/HSRPv6, MSDP, Layer 2 ISIS (FabricPath, OTV)						
		Verify interfaces in error						
		FHRP: Verify FHRP MAC address is programmed in the mac table						
		STP: Verify RSTP parameters and port status.						
		VACL, PACL: Verify that all the policies are properly programmed in hardware.						
		Verify SSH works through the management network on a dedicated vrf						
		Verify TB, error, crash						
		Verify Syslog to syslog.interop.cisco.com						
		Verify DHCP IP helper and primary/backup server						
		FabricPath: Verify FabricPath route and mac-table are built as expected. Verify IS-IS database. Verify multi-destination trees for broadcast and multicast. Verify fabricpath load-balance works as expe						
		IGMP/MLD Snooping: Verify IGMP/MLD Snooping						
1.4.4	L2 Link Failure/Recovery		84	84	0	0	104	
1.4.4.1	vPC leg failure/recovery between Distribution and ToR devices		36	36	0	0	56	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						

		The maximum traffic disruption for unicast will be half for both upstream and downstream traffic.						
		The maximum traffic loss for multicast upstream will be half and for downstream will be either 100% disrupted or no loss depending on which vPC leg is shut.						
		Multicast forwarder should not change.						
		Verify that there is no protocol flapping.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify mac move and any missing mac address.						
		Verify mac table is empty after link shut.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
		Verify traffic drop based on interface counters.						
		Verify that no flooding happens after traffic convergence.						
		Verify STP port states after link disruption are in the expected forwarding mode. Verify that the STP root does not change.						
1.4.4.2	vPC peer-link failure/recovery between Distribution vPC peer switches		4	4	0	0	4	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		The maximum traffic disruption for unicast should be in sub-second range for both upstream and downstream traffic.						
		The maximum traffic loss for member failure multicast upstream will drop proportionate and for downstream will be either 50% disrupted or no loss depending on which vPC leg member is shut (assuming th						
		Multicast forwarder should not change.						

		Verify that there is no protocol flapping.						
		Verify port-channel load balancing and rbh assignment.						
		Verify that IGMP/MLD membership is not affected.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify that the operational secondary vPC peer will bring down the vPC member ports.						
		Verify that secondary peer will suspend the vpc vlan svi's.						
		Verify that on recovery, the original states will be re-established.						
1.4.4.3	vPC peer-link member failure/recovery between Distribution vPC peer switches		8	8	0	0	8	
		Verify that there are no dead flows						
		The maximum traffic disruption for unicast should be in sub-second range for both upstream and downstream traffic.						
		The maximum traffic loss for member failure multicast upstream will drop proportionate and for downstream will be either 50% disrupted or no loss depending on which vPC leg member is shut (assuming th						
		Multicast forwarder should not change.						
		Verify that there is no protocol flapping.						
		Verify port-channel load balancing and rbh assignment.						
		Verify that IGMP/MLD membership is not affected.						

		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
1.4.4.6	L2 port-channel Failure/Recovery between Distribution and ToR devices		12	12	0	0	12	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify FHRP peers status does not change. Verify FHRP MAC in ARP/ND table. Verify FHRP MAC address is programmed as a router/static MAC on the active switch and a dynamic entry on the standby switch.						
		Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link.						
		Verify the L2 forwarding table should remove entries of the affected link at the access switch and re-learnt correctly on the alternative link.						
		Verify that MAC's for SVI's are programmed as router/static entries on the switches where they are configured and learned as dynamic entries on the L2 peers.						
		Verify that the L2 forwarding entries on all switches for nodes connected to the access layer are associated with the corresponding STP forwarding ports.						
		Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines.						

		Verify that IGMP/MLD membership is not affected on the routers.						
		Verify SPAN is mirroring packets correctly.						
		Verify isolated vlans remain to have complete separation from other ports within the same PVLAN but not from the promiscuous ports using proxy-arp.						
		DHCP relay configured on the aggregation switches should remain unaffected.						
		Verify that IPv6 global HSRP is functional.						
		Verify that packets only traverse the fabric for known unicast/multicast destinations and flood through the fabric for unknown unicast, multicast when IGMP snooping is disabled, and broadcast.						
		Verify SNMP traps are sent to SNMP collector						
		Verify frames delta does not increase.						
		Verify packet loss duration is within expected range.						
		Verify mac move and any missing mac address.						
		Verify mac table is empty after link shut.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
		Verify traffic drop based on interface counters.						
		Verify that no flooding happens after traffic convergence.						
		Verify STP port states after link disruption are in the expected forwarding mode. Verify that the STP root does not change.						
		Verify IGMP/MLD snooping entries are deleted for the affected link for non-vpc setup.and re-learnt correctly on the alternative link after query from the IGMP snooping router.						
		Verify ACL TCAM is programmed correctly to share for ACL's and features that allow for sharing and verify ACL's are not sharing when not expected.						
		Verify that secondary addresses provide the same capability and services to nodes through DHCP relay, FHRP services, ARP, proxy arp and IGMP.						
		All unicast and multicast traffic should re-converge with minimal packet loss.						

		Verify traffic destined for CoPP classes is policed as expected.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
1.4.4.7	vPC peer-link failure/recovery between ToR vPC peer switches		8	8	0	0	8	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		The maximum traffic disruption for unicast should be in sub-second range for both upstream and downstream traffic.						
		The maximum traffic loss for member failure multicast upstream will drop proportionate and for downstream will be either 50% disrupted or no loss depending on which vPC leg member is shut (assuming th						
		Multicast forwarder should not change.						
		Verify that there is no protocol flapping.						
		Verify port-channel load balancing and rbh assignment.						
		Verify that IGMP/MLD membership is not affected.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify that the operational secondary vPC peer will bring down the vPC member ports.						
		Verify that secondary peer will suspend the vpc vlan svi’s.						

		Verify that on recovery, the original states will be re-established.						
1.4.4.8	vPC peer-link member failure/recovery between ToR vPC peer switches		16	16	0	0	16	
		Verify that there are no dead flows						
		The maximum traffic disruption for unicast should be in sub-second range for both upstream and downstream traffic.						
		The maximum traffic loss for member failure multicast upstream will drop proportionate and for downstream will be either 50% disrupted or no loss depending on which vPC leg member is shut (assuming th						
		Multicast forwarder should not change.						
		Verify that there is no protocol flapping.						
		Verify port-channel load balancing and rbh assignment.						
		Verify that IGMP/MLD membership is not affected.						
		Verify frames delta does not increase.						
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
1.4.5	L3 Link Failure/Recovery		264	264	0	0	751	
1.4.5.1	L3 port-channel Failure/Recovery between Core and Distribution Layers		80	80	0	0	493	
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						

		Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link.						
		Verify the L2 forwarding table should remove entries of the affected link.						
		Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines.						
		Verify SPAN is mirroring packets correctly.						
		Verify OTV traffic reconverges and optimize OSPF as needed.						
		Verify SNMP traps are sent to SNMP collector.						
		All unicast and multicast traffic should re-converge with proportionate packet loss.						
		Verify traffic destined for CoPP classes is policed as expected.						
		Verify OSPF interface status for the affected links.						
		Verify OSPF neighbor changes and authentication.						
		Verify OSPF DB/Topology consistency.						
		Verify OSPF routes and forwarding table consistency..						
		Verify OSPF multi-path load-balancing.						
		Verify HW and SW entries are properly programmed and synchronized.						
		Verify PIM neighbor status.						
		Verify PIM both multipath and non-multipath functionalities.						
		Verify AutoRP mapping.						
		Verify static RP mapping as the backup of auto RP.						
		Verify MSDP neighbors and SA cache consistency.						
		Verify multicast HW and SW entries are properly programmed and synchronized.						
		On the multicast LHR, verify (*,G) and (S,G) creation based on SPT-threshold settings.						
		Verify PIM source register and register stop.						

		Verify BFD peer detection and client notifications.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
1.4.5.2	L3 port-channel member failure/recovery		110	110	0	0	110	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify port-channel load balancing and rbh assignment						
		Verify traffic switches to high Bandwidth port-channels for both unicast and multicast when member failure and traffic will switch back when member recovers.						
		Verify LACP rebundle for port-channel after member recover.						
		The traffic should be able to re-converge within acceptable time.						
		Verify the convergence pattern is as expected.						
		Verify the route tables for both unicast and multicast are updated correctly.						
		Verify the hardware entries, LC programming, fabric programming, outgoing interface, forwarding engine entries, for both unicast and multicast are updated correctly.						

		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
1.4.5.3	L3 member link Failure/Recovery between Core and Distribution Layers		38	38	0	0	112	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify port-channel load balancing and rbh assignment						
		Verify traffic switches to high Bandwidth port-channels for both unicast and multicast when member failure and traffic will switch back when member recovers.						
		Verify LACP rebundle for port-channel after member recover.						
		The traffic should be able to re-converge within acceptable time.						
		Verify the convergence pattern is as expected.						
		Verify the route tables for both unicast and multicast are updated correctly.						
		Verify the hardware entries, LC programming, fabric programming, outgoing interface, forwarding engine entries, for both unicast and multicast are updated correctly.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						

		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
1.4.5.4	L3 Port-channel Failure/Recovery between Distribution and ToR N3K Layer 3		20	20	0	0	20	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link.						
		Verify the L2 forwarding table should remove entries of the affected link.						
		Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines.						
		Verify SPAN is mirroring packets correctly.						
		Verify OTV traffic reconverges and optimize OSPF as needed.						
		Verify SNMP traps are sent to SNMP collector.						
		All unicast and multicast traffic should re-converge with proportionate packet loss.						
		Verify traffic destined for CoPP classes is policed as expected.						
		Verify OSPF interface status for the affected links.						
		Verify OSPF neighbor changes and authentication.						
		Verify OSPF DB/Topology consistency.						
		Verify OSPF routes and forwarding table consistency..						
		Verify OSPF multi-path load-balancing.						
		Verify HW and SW entries are properly programmed and synchronized.						

		Verify PIM neighbor status.						
		Verify PIM both multipath and non-multipath functionalities.						
		Verify AutoRP mapping.						
		Verify static RP mapping as the backup of auto RP.						
		Verify MSDP neighbors and SA cache consistency.						
		Verify multicast HW and SW entries are properly programmed and synchronized.						
		On the multicast LHR, verify (*,G) and (S,G) creation based on SPT-threshold settings.						
		Verify PIM source register and register stop.						
		Verify BFD peer detection and client notifications.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
1.4.5.5	L3 Port-channel member Failure/Recovery between Distribution and ToR N3K Layer 3		16	16	0	0	16	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify port-channel load balancing and rbh assignment						
		Verify traffic switches to high Bandwidth port-channels for both unicast and multicast when member failure and traffic will switch						

		back when member recovers.						
		Verify LACP rebundle for port-channel after member recover.						
		The traffic should be able to re-converge within acceptable time.						
		Verify the convergence pattern is as expected.						
		Verify the route tables for both unicast and multicast are updated correctly.						
		Verify the hardware entries, LC programming, fabric programming, outgoing interface, forwarding engine entries, for both unicast and multicast are updated correctly.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
1.4.6	FabricPath - Link Failure/Recovery		218	218	0	0	478	
1.4.6.1	FabricPath - Core Link Failure/Recovery		84	84	0	0	234	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify FabricPath route and mac-table are built as expected.						
		Verify IS-IS database, topology and route distribution.						
		Verify multi-destination trees for broadcast and multicast.						
		Verify fabricpath load-balance works as expected.						

		Verify FHRP peers status does not change.						
		Verify FHRP MAC in ARP/ND table.						
		Verify FHRP MAC address is programmed as a router/static MAC on the active switch and a dynamic entry on the standby switch.						
		Verify that CDP/LLDP does not lose peer information for non-affected links. Verify that CDP/LLDP peer is removed for disrupted link.						
		Verify SNMP traps are sent to SNMP collector.						
		Verify that MAC's for SVI's are programmed as router/static entries on the switches where they are configured and learned as dynamic entries on the L2 peers.						
		On the aggregation switches, verify that the ARP/ND are programmed as adjacencies for L3 next hop forwarding.						
		Verify that no flooding happens after traffic convergence.						
		Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines.						
		Verify IGMP/MLD snooping entries are deleted for the affected link and re-learnt correctly on the alternative link after query from the IGMP snooping router.						
		Verify that IGMP/MLD membership is not affected on the routers.						
		Verify SPAN is mirroring packets correctly.						
		DHCP relay configured on the aggregation switches should remain unaffected.						
		Verify that secondary addresses provide the same capability and services to nodes through DHCP relay, FHRP services, ARP, proxy arp and IGMP.						
		Verify that IPv6 global HSRP is functional.						
		Verify that packets only traverse the fabric for known unicast/multicast destinations and flood through the fabric for unknown unicast, multicast when IGMP snooping is disabled, and broadcast.						
		All unicast and multicast traffic should re-converge with minimal packet loss.						
		Verify traffic destined for CoPP classes is policed as expected.						
		Verify frames delta does not increase.						

		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
1.4.6.2	Fabricpath - Core Link member failure/recovery		110	110	0	0	200	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify port-channel load balancing and RBH assignment.						
		Verify IS-IS database, topology and route distribution for metric change.						
		Verify that IGMP/MLD membership is not affected.						
		Verify that IGMP snooping entries change based on multi-destination tree topology change.						
		The maximum traffic disruption for unicast/multicast should be in sub-second range for both upstream and downstream traffic.						
		Multicast DR should not change.						
		Verify that there is no protocol flapping.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
1.4.6.3	Fabricpath - vPC+ peer-link failure/recovery (spine/leaf)		8	8	0	0	24	

		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify that the operational secondary vPC+ peer will bring down the vPC+ member ports.						
		Verify that secondary peer will not suspend the vPC+ vlan SVI's if "dual-active exclude vlans" is configured						
		Verify on recovery that the operational secondary vPC+ peer will bring up the vPC+ member ports after the configured "delay restore" timer						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
1.4.6.4	Fabricpath - vPC+ peer-link member failure/recovery (spine/leaf)		16	16	0	0	16	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		The maximum traffic disruption for unicast should be in sub-second range for both upstream and downstream traffic.						

		The maximum traffic loss for member failure multicast upstream will drop proportionate and for downstream will be either 50% disrupted or no loss depending on which vPC+ leg member is shut (assuming t						
		Multicast forwarder should not change.						
		Verify that there is no protocol flapping.						
		Verify port-channel load balancing and rbh assignment.						
		Verify that IGMP/MLD membership is not affected.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify interface status is UP/DOWN state after linkNoShut/linkShut respectively.						
1.4.7	Supervisor and Fabric HA		4	4	0	0	4	
1.4.7.1	Supervisor HA on the edge/core layer		2	2	0	0	2	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Compare startup/running configuration on Active Sup and Standby Sup before and after SSO.						
		Verify BGP neighbors status and authentication.						
		Verify BGP table and routing table consistency in accordance to the NEXT-HOP attribute settings.						
		Verify proper BGP policy routing and filtering based on prefix, AS-PATH, LOCAL_PREFERENCE attributes.						

		Verify the conditional injection of the default route from BGP into the IGP.						
		Verify BGP recursive lookup scenario.						
		Verify BGP reconvergence (control-plane & data-plane).						
		Verify OSPF neighbor changes and authentication.						
		Verify OSPF DB/Topology consistency.						
		Verify OSPF routes and forwarding table consistency..						
		Verify HW and SW entries are properly programmed and synchronized after SSO.						
		Verify PIM neighbor status.						
		Verify static RP mapping as the backup of auto RP.						
		Verify MSDP neighbors and SA cache consistency.						
		Verify multicast HW and SW entries are properly programmed and synchronized after SSO.						
		Verify BFD peer should not flap during and after SSO.						
		No traffic loss is expected.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
		Verify OSPF interface status.						
1.4.7.2	Supervisor HA on the Distribution layer		2	2	0	0	2	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						

		Verify interfaces in error						
		Verify any core dumps						
		Compare startup/running configuration on Active Sup and Standby Sup before and after SSO.						
		Verify STP port states during and after SSO.						
		Verify FHRP peers status during and after SSO.						
		Verify CDP/LLDP status after SSO.						
		Verify ARP/ND tables remain unaffected						
		Verify FHRP MAC in ARP/ND table.						
		Verify OTV ARP optimization/ARP caching works as expected after SSO.						
		Verify head-end replication for multicast traffic on unicast-only transport works as expected, check the data-group mapping table for receiver information.						
		Verify automated mapping of OTV sites multicast groups to transport multicast group.						
		Verify FHRP MAC address is programmed as a router/static MAC on the active switch and a dynamic entry on the standby switch.						
		Verify that MAC's for SVI's are programmed as router/static entries on the switches where they are configured and learned as dynamic entries on the L2 peers.						
		On the aggregation switches, verify that the ARP/ND are programmed as adjacencies for L3 next hop forwarding after SSO.						
		Verify IGMP snooping entries remain unaffected.						
		Verify that no flooding happens after traffic convergence.						
		Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines.						
		Verify SPAN is mirroring packets correctly during and after SSO.						
		Verify SNMP traps are sent to SNMP collector.						
		Verify traffic destined for CoPP classes is policed as expected.						
		Verify OSPF interface status.						

		Verify OSPF neighbor changes and authentication.						
		Verify OSPF DB/Topology consistency.						
		Verify OSPF routes and forwarding table consistency..						
		Verify HW and SW entries are properly programmed and synchronized after SSO.						
		Verify PIM neighbor status.						
		Verify static RP mapping as the backup of auto RP.						
		Verify MSDP neighbors and SA cache consistency.						
		Verify multicast HW and SW entries are properly programmed and synchronized after SSO.						
		Verify BFD peer should not flap during and after SSO.						
		Verify vPC peer status (role, peer link, keepalive link and consistency parameters) before and after SSO						
		No traffic loss is expected.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
1.4.9	Linecard OIR/Reset		16	16	0	0	20	
1.4.9.1	L3 port-channel member failure/recovery, on OIR/reset line card		12	12	0	0	16	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						

		Verify hitless operation for non-affected ports						
		Verify traffic load-balancing for distributed port-channels before and after OIR/reset						
		Verify BGP/ IGP/ PIM reconvergence (control-plane & data plane)						
		Verfiy BFD peer detection and client notifications						
		Verify LACP interoperability for distributed port-channels						
		Verify that CDP/LLDP does not lose peer information for non-affected line card. Verify that CDP/LLDP peer is removed for disrupted line cards.						
		Verify the L2 forwarding table should be re-learnt correctly after OIR/reset.						
		Verify that no flooding happens after traffic convergence.						
		Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines.						
		Verify SPAN is mirroring packets correctly.						
		Verify SNMP traps are sent to SNMP collector.						
		All unicast and multicast traffic should re-converge with minimal packet loss.						
		Verify traffic destined for CoPP classes is policed as expected.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
1.4.9.2	vPC leg failure/recovery, on OIR/reset line card		4	4	0	0	4	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						

		Verify any core dumps						
		The maximum traffic disruption for unicast will be half for both upstream and downstream traffic.						
		The maximum traffic loss for multicast upstream will be half and for downstream will be either 100% disrupted or no loss depending on which vPC leg is shut.						
		Multicast forwarder should not change.						
		Verify that there is no protocol flapping.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
1.4.10	FabricPath - Linecard OIR/Reset		4	4	0	0	4	
1.4.10.1	OIR/reset line card on spine nodes		4	4	0	0	4	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify hitless operation for non-affected ports						
		Verify traffic load-balancing for distributed port-channels before and after OIR/reset						
		Verify BGP/ IGP/ PIM reconvergence (control-plane & data plane)						
		Verfiy BFD peer detection and client notifications						
		Verify LACP interoperability for distributed port-channels						
		Verify that CDP/LLDP does not lose peer information for non-affected line card. Verify that CDP/LLDP peer is removed for						

		disrupted line cards.						
		Verify the L2 forwarding table should be re-learnt correctly after OIR/reset.						
		Verify that no flooding happens after traffic convergence.						
		Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines.						
		Verify SPAN is mirroring packets correctly.						
		Verify SNMP traps are sent to SNMP collector.						
		All unicast and multicast traffic should re-converge with minimal packet loss.						
		Verify traffic destined for CoPP classes is policed as expected.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
1.4.11	Reload and Power Cycle Switch		6	6	0	0	6	
1.4.11.1	Reload and Power Cycle Edge/Core Switch		6	6	0	0	6	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify BGP neighbors status and authentication.						
		Verify BGP table and routing table consistency in accordance to the NEXT-HOP attribute settings.						
		Verify BGP multi-path load-balancing.						
		Verify proper BGP policy routing and filtering based on prefix, AS-PATH, LOCAL_PREFERENCE attributes.						

		Verify the conditional injection of the default route from BGP into the IGP.						
		Verify BGP recursive lookup scenario.						
		Verify BGP reconvergence (control-plane & data-plane).						
		Verify OSPF interface status for the affected links.						
		Verify OSPF neighbor changes and authentication.						
		Verify OSPF DB/Topology consistency.						
		Verify OSPF routes and forwarding table consistency..						
		Verify OSPF multi-path load-balancing.						
		Verify HW and SW entries are properly programmed and synchronized.						
		Verify PIM neighbor status.						
		Verify PIM both multipath and non-multipath functionalities.						
		Verify AutoRP mapping and boundaries.						
		Verify static RP mapping as the backup of auto RP.						
		Verify MSDP neighbors and SA cache consistency.						
		Verify multicast HW and SW entries are properly programmed and synchronized.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
1.4.12	FabricPath - Reload		4	4	0	0	4	
1.4.12.1	FabricPath - Spine Node failure/recovery		4	4	0	0	4	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						

		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		Verify Fabricpath multi-destination trees reconverge after root change on node failure.						
		Verify FabricPath route and mac-table are built as expected.						
		Verify IS-IS database, topology and route distribution.						
		Verify FHRP MAC address is programmed as a router/static MAC on the active switch and a dynamic entry on the standby switch.						
		Verify that MAC's for SVI's are programmed as router/static entries on the switches where they are configured and learned as dynamic entries on the L2 peers.						
		On the distribution switches, verify that the ARP/ND are programmed as adjacencies for L3 next hop forwarding.						
		Verify that no flooding happens after traffic convergence.						
		Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines on the other spine routers						
		Verify IGMP/MLD snooping entries are deleted for the affected link for non-vpc setup.and re-learnt correctly on the alternative link after query from the IGMP snooping router.						
		Verify that IGMP/MLD membership is not affected on the other spine routers.						
		Verify SPAN is mirroring packets correctly.						
		Verify SNMP traps are sent to SNMP collector.						
		DHCP relay configured on the aggregation switches should remain unaffected.						
		Verify that secondary addresses provide the same capability and services to nodes through DHCP relay, FHRP services, ARP, proxy arp and IGMP.						
		All unicast and multicast traffic should re-converge with minimal packet loss.						
		Verify traffic destined for CoPP classes is policed as expected.						

		Verify that the MAC table, FP ISIS route table, ARP/ND table, IP routing table, IGMP membership table, IGMP snooping table, Multicast routing table return to original state on recovery						
		Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines on recovery						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
1.4.13	ISSU/ISSD		4	3	0	1	4	
1.4.13.1	6.1.x/6.2.8		4	3	0	1	4	CSCum86523, CSCum86511
		Verify if ISSU image compatibility for non-disruptive upgrade/downgrade						
		Verify ISSU/ISSD happens as expected. OSPF graceful restart, PIM triggered Joins should work as expected.						
		Compare startup/running configuration on Active Sup and Standby Sup before and after ISSU/ISSD.						
		Verify STP port states during and after ISSU/ISSD.						
		Verify FHRP peers status during and after ISSU/ISSD.						
		Verify CDP/LLDP status after ISSU/ISSD.						
		Verify FHRP MAC in ARP/ND table.						
		Verify FHRP MAC address is programmed as a router/static MAC on the active switch and a dynamic entry on the standby switch.						
		Verify that MAC's for SVI's are programmed as router/static entries on the switches where they are configured and learned as dynamic entries on the L2 peers.						
		On the distribution switches, verify that the ARP/ND are programmed as adjacencies for L3 next hop forwarding after ISSU/ISSD.						
		Verify that no flooding happens after traffic convergence.						
		Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines.						
		Verify SPAN is mirroring packets correctly during and after ISSU/ISSD.						
		Verify SNMP traps are sent to SNMP collector.						

		Verify traffic destined for CoPP classes is policed as expected.						
		Verify BGP neighbors status and authentication.						
		Verify BGP table and routing table consistency in accordance to the NEXT-HOP attribute settings.						
		Verify proper BGP policy routing and filtering based on prefix, AS-PATH, LOCAL_PREFERENCE attributes.						
		Verify the conditional injection of the default route from BGP into the IGP.						
		Verify BGP recursive lookup scenario.						
		Verify BGP reconvergence for control-plane.						
		Verify OSPF interface status.						
		Verify OSPF neighbor changes and authentication.						
		Verify OSPF DB/Topology consistency.						
		Verify OSPF routes and forwarding table consistency.						
		Verify HW and SW entries are properly programmed and synchronized after ISSU/ISSD.						
		Verify PIM neighbor status.						
		Verify static RP mapping as the backup of auto RP.						
		Verify MSDP neighbors and SA cache consistency.						
		Verify multicast HW and SW entries are properly programmed and synchronized after ISSU/ISSD.						
		Verify BFD peer should not flap during and after ISSU/ISSD.						
		No traffic loss is expected.						
		If ISSU is disruptive, verify that all unicast/multicast traffic reconverges.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						

		Verify packet loss duration is within expected range.						
1.4.14	Clear OSPF Neighbors/Process/Routes		16	16	0	0	16	
1.4.14.1	Clear OSPF Neighbors/Process/Routes		16	16	0	0	16	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		All unicast and multicast traffic should re-converge.						
		Verify OSPF IPv4/IPv6 neighbors will restart and come back correctly.						
		Verify that the hardware entries are properly removed and re-installed during the neighbor/process flapping.						
		Verify that CDP/LLDP does not lose peer information.						
		Verify that no flooding happens after traffic convergence.						
		Verify the L2/L3 forwarding entries are synchronized among the hardware forwarding engines.						
		Verify SPAN is mirroring packets correctly.						
		Verify SNMP traps are sent to SNMP collector.						
		Verify traffic destined for CoPP classes is policed as expected.						
		Verify OSPF neighbor changes and authentication.						
		Verify OSPF DB/Topology consistency.						

		Verify OSPF routes and forwarding table consistency.						
		Verify OSPF multi-path load-balancing.						
		Verify HW and SW entries are properly programmed and synchronized.						
		Verify multicast HW and SW entries are properly programmed and synchronized.						
		Verify BFD peer detection and client notifications.						
		Verify the route tables for both unicast and multicast are updated correctly.						
		Verify the hardware entries, LC programming, fabric programming, outgoing interface, forwarding engine entries, for both unicast and multicast are updated correctly.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
1.4.15	Clear IPv4/IPv6 Multicast Routes		16	16	0	0	16	
1.4.15.1	Clear Pim Routes		8	8	0	0	8	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		All multicast traffic should re-converge.						
		Verify periodic PIM joins are received and sent upstream after clearing.						
		Verify that the multicast hardware entries are properly removed and re-installed during the mroute flaps						
		Verify that CDP/LLDP does not lose peer information.						

		Verify that no flooding happens after traffic convergence.						
		Verify PIM neighbor status.						
		Verify PIM both multipath and non-multipath functionalities.						
		Verify AutoRP mapping.						
		On the multicast LHR, verify (*,G) and (S,G) creation based on SPT-threshold settings.						
		Verify PIM source register and register stop.						
		Verify IGMP/MLD snooping entries are deleted and re-learnt correctly after query from the IGMP snooping router.						
		Verify SPAN is mirroring packets correctly.						
		Verify SNMP traps are sent to SNMP collector.						
		Verify traffic destined for CoPP classes is policed as expected.						
		Verify the hardware entries, LC programming, fabric programming, outgoing interface, forwarding engine entries, for both unicast and multicast are updated correctly.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						
1.4.15.2	Clear IPv4/IPv6 Multicast Routes		8	8	0	0	8	
		Verify that MEM and CPU Usage for Supervisors and line cards are comparable to previous releases.						
		Verify that all unicast/multicast traffic convergence is comparable to previous releases.						
		Verify that there are no dead flows						
		Verify TB, error, crash						
		Verify interfaces in error						
		Verify any core dumps						
		All multicast traffic should re-converge.						

		Verify periodic PIM joins are received and sent upstream after clearing.						
		Verify that the multicast hardware entries are properly removed and re-installed during the mroute flaps						
		Verify that CDP/LLDP does not lose peer information.						
		Verify that no flooding happens after traffic convergence.						
		Verify PIM neighbor status.						
		Verify PIM both multipath and non-multipath functionalities.						
		Verify AutoRP mapping.						
		On the multicast LHR, verify (*,G) and (S,G) creation based on SPT-threshold settings.						
		Verify PIM source register and register stop.						
		Verify IGMP/MLD snooping entries are deleted and re-learnt correctly after query from the IGMP snooping router.						
		Verify SPAN is mirroring packets correctly.						
		Verify SNMP traps are sent to SNMP collector.						
		Verify traffic destined for CoPP classes is policed as expected.						
		Verify the hardware entries, LC programming, fabric programming, outgoing interface, forwarding engine entries, for both unicast and multicast are updated correctly.						
		Verify frames delta does not increase.						
		Verify rx rate for all ixia ports are as expected (compared to baseline).						
		Verify packet loss duration is within expected range.						