networktest

Juniper / Cisco Interoperability Tests

August 2014

Executive Summary

Juniper Networks commissioned Network Test to assess interoperability, with an emphasis on data center connectivity, between Juniper and Cisco switches. From Juniper, the devices tested included the EX9200, QFX5100, and EX4300 switches and MX80 router; from Cisco, the devices tested were the Nexus 7010 and Catalyst 3850 switches, the Cisco 5508 Wi-Fi controller, and Cisco 3602 and 3702 Wi-Fi access points. **In every test case where Juniper and Cisco switches supported the same protocol, all switches correctly forwarded traffic.**

These results demonstrate that users don't need to be locked into a single-vendor solution. Juniper devices fully supported all the open networking standards described here, and interoperated with Cisco gear even in cases where Cisco-proprietary protocols were involved.

In this evaluation, Network Test validated the interoperability of 18 protocols. The following table summarizes results of interoperability testing.

Juniper / Cisco Protocol Interoperability					
	Juniper Virtual Chassis Fabric (Juniper QFX5100, Juniper EX4300)	**Juniper Virtual Chassis (2 Juniper EX9208)**		**Juniper Virtual Chassis Fabric (Juniper QFX5100, Juniper EX4300)**	**Juniper Virtual Chassis (2 Juniper EX9208)**
CDP passthrough			**Real-Time Performance Monitoring**		
Cisco Catalyst 3850	✓	✓	Cisco Catalyst 3850	Not tested*	Not tested*
Cisco Nexus 7010	✓	✓	Cisco Nexus 7010	✓	✓
GRE tunneling			**Redundant Trunk Groups**		
Cisco Catalyst 3850	✓	✓	Cisco Catalyst 3850	✓	Not tested*
Cisco Nexus 7010	✓	✓	Cisco Nexus 7010	✓	Not tested*
Jumbo frame handling			**Remote performance monitoring**		
Cisco Catalyst 3850	✓	✓	Cisco Catalyst 3850	✓	✓
Cisco Nexus 7010	✓	✓	Cisco Nexus 7010	✓	✓
Layer-3 VPNs using BGP			**Spanning tree protocol**		
Cisco Catalyst 3850	✓	✓	Cisco Catalyst 3850	✓**	✓
Cisco Nexus 7010	✓	✓	Cisco Nexus 7010	✓**	✓
Link aggregation and MC-LAG			**VLAN trunking**		
Cisco Catalyst 3850	✓	✓	Cisco Catalyst 3850	✓	✓
Cisco Nexus 7010	✓	✓	Cisco Nexus 7010	✓	✓
LLDP			**VRRP**		
Cisco Catalyst 3850	✓	✓	Cisco Catalyst 3850	Not tested*	Not tested*
Cisco Nexus 7010	✓	✓	Cisco Nexus 7010	✓	✓
Multicast switching and routing			**Wi-Fi passthrough**		
Cisco Catalyst 3850	✓	✓	Cisco Catalyst 3850	✓***	✓
Cisco Nexus 7010	✓	✓	Cisco Nexus 7010	✓***	✓

* Cases noted as "not tested" refer to situations where either the Juniper or Cisco software image tested did not support a given protocol. Details for each protocol are given later in this document. Appendix B lists software versions tested for each switch.

** The Juniper EX4300 and Juniper QFX5100 both support all permutations of spanning tree tested. At testing time, the Juniper EX4300 did not support spanning tree when it is part of a Virtual Chassis Fabric. Network Test evaluated spanning tree on the Juniper EX4300 in standalone mode.

*** Tested with the Juniper EX4300; at test time, the Juniper QFX5100 did not support power over Ethernet.

Methodology and Results

Network Test used a Spirent TestCenter traffic generator/analyzer to verify that Juniper and Cisco switches would exchange traffic over a variety of layer-2 and layer-3 protocols. The switches were interconnected with a mix of gigabit Ethernet and 10-gigabit Ethernet links, as shown in Figure 1.

Except where noted, the Juniper switches used virtual interconnect methods to create a single logical switch from multiple physical devices. Two Juniper EX9200 switches formed a single Virtual Chassis. Two Juniper QFX5100 and one Juniper EX4300 switches formed a single Virtual Chassis Fabric. In both cases, the combined devices used a single configuration file and appeared as one device to the rest of the network. Wherever possible, Network Test used both QFX5100 and EX4300 ports when the Virtual Chassis Fabric was part of a given test.

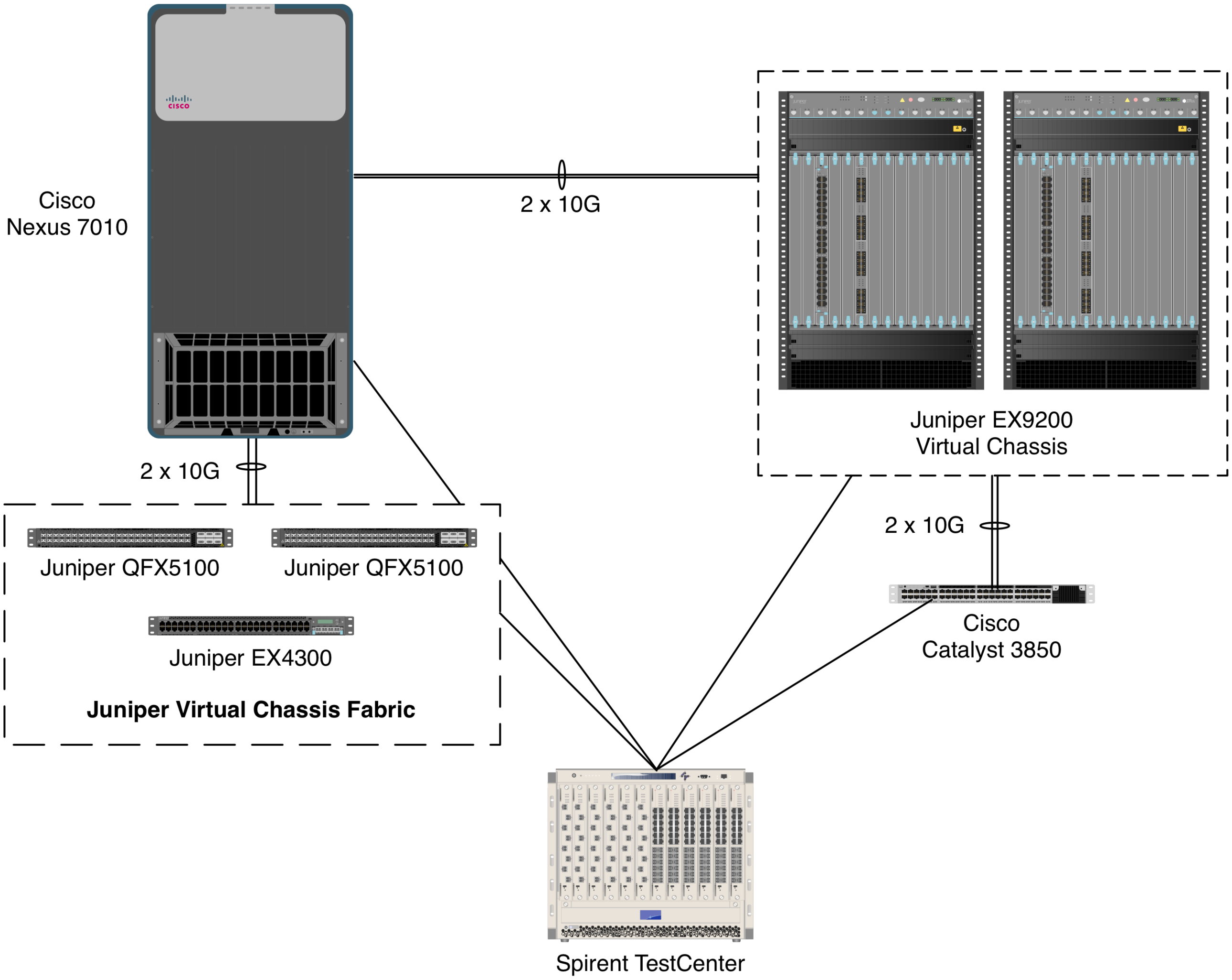

Figure 1: Juniper / Cisco interoperability test bed

Cisco Discovery Protocol (CDP) Passthrough

The proprietary Cisco Discovery Protocol (CDP) allows sharing of information, such as IP address, model number and power requirements, among connected Cisco devices. Network Test verified the ability of the Juniper EX4300, Juniper QFX5100 and Juniper EX9200 switches to "pass through" CDP data between two connected Cisco devices.

Engineers validated transport of this information by enabling CDP on two Cisco devices and verifying via the Cisco switches' command-line interfaces (CLIs) that they could identify one another after passing packets through an intermediate Juniper switch.

CDP uses IP multicast, and this required disabling of IGMP snooping on the Juniper switches to ensure forwarding of all multicast traffic. With IGMP snooping disabled, all Juniper switches successfully "passed through" CDP messages between pairs of Cisco switches.

Generic Routing Encapsulation (GRE) Tunneling

Network Test validated the ability of all Juniper and Cisco switches to pass traffic through GRE tunnels. In all cases, test traffic and tunnel endpoints used different sets of IP addresses.

To validate interoperability, engineers configured GRE tunnels between all devices on the test bed: a Virtual Chassis Fabric (encompassing two Juniper QFX5100s and one Juniper EX4300); the Cisco Nexus 7010; a Virtual Chassis (encompassing two Juniper EX9208s); and a Cisco Catalyst 3850. Then Spirent TestCenter offered IP traffic to access devices using IP networks different than those defined by the GRE tunnel endpoints.

The Juniper and Cisco devices delivered all traffic through the GRE tunnels without loss. A check of each switch's command-line interface (CLI) also verified that GRE tunnels were up throughout this test.

Jumbo Frame Handling

To validate the ability of Juniper and Cisco switches to exchange jumbo Ethernet frames – those larger than the standard maximum of 1,518 bytes – Network Test conducted jumbo tests in both switching and routing modes.

For the switching and routing tests, Spirent TestCenter offered 9,152-byte jumbo Ethernet frames in a bidirectional pattern between Juniper and Cisco switches[1]. For all switch pairs, all devices correctly forwarded jumbo traffic without loss.

Layer-3 Virtual Private Networks (L3 VPNs)

Network Test verified the ability of Juniper and Cisco core switches to set up a VPN tunnel across an MPLS backbone network using the Border Gateway Protocol (BGP), and to forward traffic through that tunnel.

To validate L3 VPN service, engineers configured the Juniper Virtual Chassis (with two EX9208s) and Cisco Nexus 7010 to act as MPLS provider edge (PE) devices. An intermediate Juniper MX80 router acted as an MPLS provider (P) device. At the edges of the network, engineers configured the Juniper

[1] Juniper EX9200 switches support a maximum Ethernet frame length of 9,192 bytes. The maximum length in Virtual Chassis mode is 9,152 bytes to account for a 40-byte internal header. Virtual Chassis Fabric devices (both EX4300 and QFX5100) support a maximum Ethernet frame length of 9,216 bytes.

Virtual Channel Fabric (two Juniper QFX5100s and one Juniper EX4300) and Cisco Catalyst 3850 to act as MPLS customer edge (CE) devices.

Using BGP to carry VPN parameters, the Juniper and Cisco core devices correctly established a tunnel and forwarded traffic across the MPLS backbone. No MPLS awareness was needed on the part of the CE devices.

Link Aggregation

Network Test evaluated the bundling of multiple physical ports into one logical port using the IEEE 802.3ad link aggregation protocol, and assessed the dynamic management of ports within a link aggregation group (LAG) using the Link Aggregation Control Protocol (LACP).

Engineers configured two-port LAGs between all Juniper and Cisco switches using 10-gigabit Ethernet links. These included the Juniper EX9200 (in a Virtual Chassis); the Juniper QFX5100 and Juniper EX4300 (in a Virtual Chassis Fabric); the Cisco Nexus 7010; and Cisco Catalyst 3850. A Spirent TestCenter offered traffic across the test bed, forcing packets to traverse each LAG. In all cases, the Juniper and Cisco switches correctly forwarded traffic.

To assess LACP, Network Test removed and then re-added ports (members) from the LAG to verify that both Juniper and Cisco switches would correctly reconfigure the LAG. A query of LACP status on the command-line interface (CLIs) of each switch during each step showed the switches dynamically reconfigured the LAG as ports were removed or added.

Link Layer Discovery Protocol (LLDP)

LLDP, based on the IEEE 802.1AB specification, is a standards-based method of exchanging device capabilities. Network Test verified LLDP interoperability between all permutations of Juniper and Cisco switches.

To validate interoperability, engineers enabled LLDP on each device and then asked each switch to show information about its neighbors. In all cases, the Juniper and Cisco devices correctly supplied information about attached switches and interfaces.

Multi-Channel Link Aggregation Groups (MC-LAG)

With MC-LAG, one access switch can set up a link aggregation group with ports in two core switches, enhancing reliability. Network Test verified the ability of Juniper core switches to establish an MC-LAG with a Cisco access switch, and to continue forwarding traffic in the event of a LAG interface link failure.

To validate MC-LAG behavior, engineers configured a two-port MC-LAG between two Juniper EX9208 core switches and one Cisco Catalyst 3850 access switch. Network Test used Spirent TestCenter to offer traffic across the LAG. Engineers then disabled one interface in the LAG, forcing traffic to be forwarded over the other MC-LAG member.

In both the forwarding and failover test cases, the Juniper-Cisco MC-LAG correctly forwarded traffic without loss. Notably, this test required no MC-LAG awareness on the part of the Cisco access switch.

Multicast Routing and Switching

Network Test validated the ability of Juniper and Cisco devices to share information about multicast routing topology and to correctly forward multicast traffic.

Multicast testing involved purely routed and purely switched IP multicast scenarios. In the routing scenario, Network Test configured Juniper and Cisco devices to run Protocol Independent Multicast-Sparse Mode (PIM-SM) and Open Shortest Path First (OSPF) to carry multicast and unicast routing information, respectively. In the switching scenario, both Juniper and Cisco devices used Internet Group Multicast Protocol snooping (IGMP snooping) to forward traffic to multicast subscribers.

For both routing and switching test, Spirent TestCenter transmitted traffic to 10 multicast groups into the Cisco Nexus 7010, and emulated multicast subscribers to all 10 groups on Juniper Virtual Chassis Fabric devices. One additional monitor port was set up on Spirent TestCenter to verify the Juniper Virtual Chassis Fabric device did not flood frames to a non-subscriber port. Network Test then repeated both tests with the Juniper EX9200 Virtual Chassis in the core and the Cisco Catalyst 3850 as the access switch.

In both routed and switched scenarios, the Juniper and Cisco devices correctly delivered multicast traffic to subscribers, and did not flood traffic to non-subscribers. The switching tests used IGMPv3 – the most recent version of the multicast distribution protocol – and in all cases the Juniper switches correctly joined groups and forwarded multicast traffic only to the appropriate destinations.

Redundant Trunk Group (RTG)

Juniper's Redundant Trunk Group (RTG) feature allows definition of primary and secondary VLAN trunk ports between switches, and redirects traffic across a secondary trunk if the primary fails. RTG provides an alternative to spanning tree for redundancy. Juniper asked Network Test to validate that RTG would operate between Juniper and Cisco switches with no additional configuration needed on Cisco switches with additional trunk ports.

To assess RTG interoperability, Network Test and Juniper engineers set up three Juniper and Cisco switches in a ring topology and configured RTG on the Virtual Chassis Fabric (Juniper QFX5100 and Juniper EX4300). Aside from defining VLAN trunk ports on the Cisco switches (Catalyst 3850 and Nexus 7010), no additional configuration was needed on the Cisco switches.

Network Test first verified connectivity by generating traffic between random switch pairs using Spirent TestCenter; traffic was observed only on the primary trunk link and not the backup. Then, after administratively disabling the primary trunk port on the Juniper Virtual Chassis Fabric, Network Test verified that the switches continued to forward traffic via the secondary trunk port, which took over the primary role. Thus, RTG was fully interoperable between the Juniper Virtual Chassis Fabric and the Cisco Catalyst 3850 and Nexus 7010. Network Test did not evaluate RTG with the Juniper EX9200, since this feature was not supported in the software image tested on that platform.

Remote Performance Monitoring (RPM)

Juniper's Remote Performance Monitoring (RPM) feature can perform health checks on attached network devices and servers using ICMP, TCP, and UDP probes and requests. Network Test validated RPM interoperability by configuring Juniper core and access switches to monitor roundtrip times to and from Cisco Catalyst core and access devices.

Using RPM with ICMP probes, both the Virtual Chassis (two Juniper EX9208s) and the Virtual Chassis Fabric (two Juniper QFX5100s and one Juniper EX4300) monitored round-trip times to and from the Cisco Nexus 7000 and Cisco Catalyst 3850 as expected.

Spanning Tree Protocol (STP)

Network Test assessed spanning tree with three variations of the widely used loop prevention and redundancy protocol:

1. RSTP (Juniper) / Rapid PVST+ (Cisco)
2. MSTP (Juniper and Cisco, using the 802.1s specification)
3. VSTP (Juniper) / Rapid PVST+ (Cisco)

Each test involved one core and two access switches. Network Test evaluated this configuration twice, Juniper and Cisco devices playing both core and access roles. At the time of testing, Virtual Chassis software images for the Juniper EX9208 did not support spanning tree; instead, Network Test used a standalone Juniper EX9204 for the these tests.

For each protocol variation, Network Test used two criteria to assess interoperability. First, engineers verified spanning tree's loop prevention capabilities by determining that traffic was received only from ports in forwarding state. Second, upon failure of a link Network Test verified that spanning tree correctly redirected traffic onto backup paths that previously had been in blocking state.

This was verified by results from Spirent TestCenter traffic generator/analyzer which showed that the switches move traffic onto ports in "forwarding" state and did not move traffic onto ports in "blocking" state. Engineers verified spanning tree convergence by disabling a forwarding-mode port, forcing another port formerly in blocking mode to become active and forward traffic. Spanning tree delivered loop-free operation and seamless failover in all three test cases.

Virtual Router Redundancy Protocol (VRRP)

Network Test verified the ability of Juniper and Cisco switches to use the IETF-standard virtual router redundancy protocol (VRRP). In the VRRP tests, a backup router took over after the failure of a primary router or link.

Testing involved running VRRP on both Juniper and Cisco products, configuring the switches as routers, and breaking a link to determine if failover worked. Both sets of Juniper/Cisco router pairs agreed on a virtual IP (VIP) address, as seen via their respective command-line interfaces (CLIs).

Initially, a Cisco device acted as master and a Juniper device as backup. Then Network Test configured the Juniper device to act as master by changing its priority to force VRRP failover. Again, the two sides agreed on VRRP settings.

The results demonstrate that upon failure of an active router or link, Juniper and Cisco devices will work cooperatively to reroute onto a backup link.

VRRP testing involved two sets of router pairs. The first setup involved the Juniper EX4300 and Juniper QFX5100 configured in a Virtual Chassis Fabric along with a Cisco Nexus 7010. The second set of tests involved a pair of Juniper EX9200 switches, in this case a Juniper EX9204 and Juniper EX9208, in standalone mode. The software image tested on the Cisco Catalyst 3850 did not support VRRP.

VLAN Trunking

Network Test evaluated interoperability of IEEE 802.1Q VLAN trunking in three ways: forwarding of allowed tagged traffic; forwarding of allowed untagged (native) traffic; and blocking of disallowed untagged traffic.

The Juniper and Cisco switches were configured with two tagged VLANs and one native VLAN, all of which should have passed across the trunk. In addition, Spirent TestCenter generated traffic from a fourth VLAN that was not allowed on the trunk. This last step was taken to determine if switch trunk ports would correctly block disallowed traffic.

In all tests, each pair of Juniper and Cisco switches correctly forwarded only the traffic intended to be forwarded, and did not carry traffic that was not intended to be forwarded.

Wi-Fi Passthrough

Enterprise-class Wi-Fi often depends on a central controller that configures and manages access points (APs) at multiple locations. Network Test validated the ability of Juniper core and access switches to “pass through” traffic between a Cisco Wi-Fi controller and Cisco APs.

To validate Wi-Fi passthrough capability, engineers constructed a test bed with a Cisco 5508 wireless controller and DHCP server attached to a Juniper EX9208 core switch. To represent the network’s access layer, engineers connected a Juniper EX4300 access switch to the EX9200 core switch, and in turn attached Cisco 3602 and 3702 APs to the EX4300. Both APs used Power over Ethernet (PoE) from the Juniper access switch.

Both Cisco APs correctly found the controller and obtained their configurations across the Juniper infrastructure. The Cisco controller verified that APs were attached, and that clients had associated to the APs. Also, the Cisco APs reported receiving 23 watts of power from the Juniper access switch, as required by the IEEE PoE+ specification.

Conclusion

Interoperability testing was successful in every case where both Juniper and Cisco devices supported a given protocol. As noted in the discussion of each the protocols, there were a few isolated cases whether a given Juniper or Cisco image did not support a given feature; no interoperability testing was attempted in these cases. Anytime a protocol was supported in both vendors’ devices, interoperability worked as expected. This provides assurance to network professionals considering design or deployment of networks comprised of a mix of Juniper and Cisco switches.

Appendix A: Software Versions Tested

This appendix lists the software versions tested on all Juniper and Cisco switches in this project.

Juniper EX4300 and QFX5100 (in Virtual Chassis Fabric): Junos 13.2-20140409_x_132_x51_vjunos.0
Juniper EX9208 (in Virtual Chassis): Junos 13.3R1.6
Juniper MX80: Junos 13.3R1.6
Cisco Catalyst 3850: IOS-XE 03.02.01.SE
Cisco Nexus 7010: NX-OS 6.1(4a)
Cisco 5508 controller: 7.6.110.0

Appendix B: Disclaimer

Network Test Inc. has made every attempt to ensure that all test procedures were conducted with the utmost precision and accuracy, but acknowledges that errors do occur. Network Test Inc. shall not be held liable for damages which may result for the use of information contained in this document.

TESTED WITH SPIRENT