IP FABRIC
NETWORK INFRASTRUCTURE INTELLIGENCE

NETWORK ANALYSIS REPORT

As of 2019-07-22 08:35

For more information please visit www.ipfabric.io

If you have more questions, please reach us at sales@ipfabric.io

Free 30-day trial. Easy 10 minutes implementation. Let us know if you want to test IP Fabric platform in your network!

CONTENTS

EXECUTIVE SUMMARY

This report contains network analysis results of 573 devices between 2019-07-22 08:26 and 2019-07-22 08:35. Detailed snapshots of network protocols and technologies and their operational state were compared and analyzed for risk, compliance and security issues. Issues within individual categories are prioritized based on business impact.

Risk impact for each issue is calculated based on the risk severity, the number of affected users, and the amount of affected traffic. Severity of each issue is evaluated within context of the overall communication path and the role of the affected technology in the network topology.

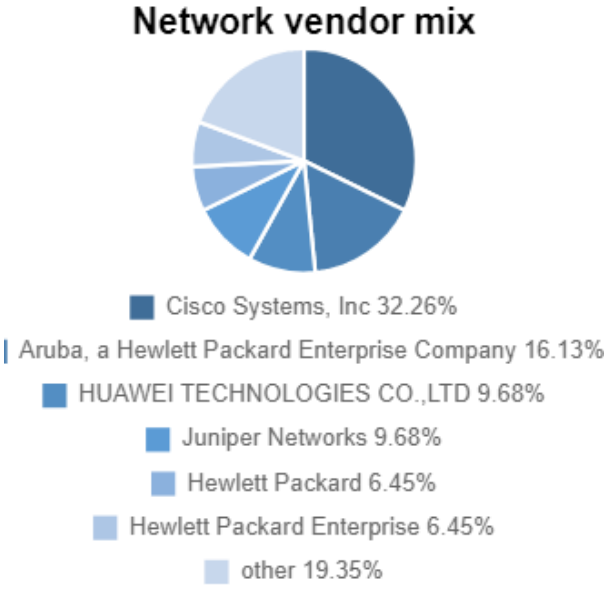
NETWORK OVERVIEW

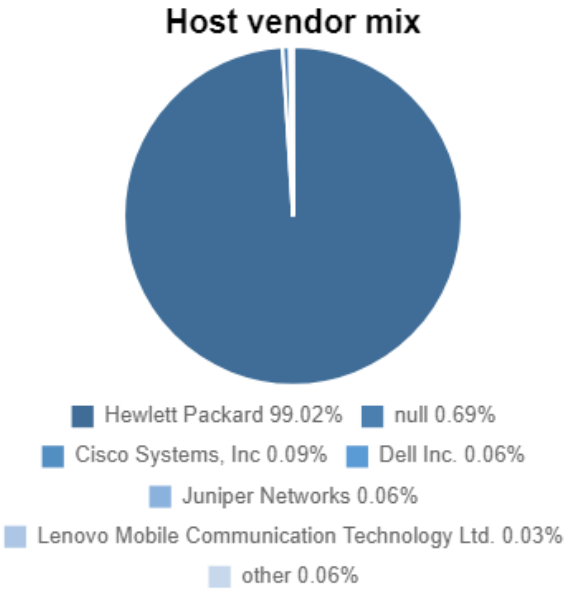
Network infrastructure state snapshot between 2019-07-22 08:26 and 2019-07-22 08:35 of 573 devices were used as a basis for the analysis.

Devices	573
Users	3478
Edge interfaces	537
Active interfaces	4909
Total interfaces	6642

Table 1 : Network Overview

VENDOR MIX OVERVIEW





DEFINED NETWORK VERIFICATION CHECKS

ENDPOINTS

Endpoints (total)

The total number of detected MAC addresses.

3478	The total number of detected MAC addresses.

Endpoints Resolution

Verifies if the IP address is present for each MAC addresses information.

3478	The total number of MAC addresses that have assigned IP Address information.

IP Phones (total)

All discovered IP phones.

3	All discovered IP phones.

ENVIRONMENT

Power-Supply State

Verifies the operational state of power-supply modules.

13	Power-supplies that are in healthy state (ok, good, normal, online).
11	Power-supplies that are neither in expected healthy state nor in the fail state.

Fan Module State

Verifies the operational state of fan modules.

23	Fan modules that are in healthy state (ok, good, normal, running successfully).
9	Fan modules that are neither in expected healthy state nor in the fail state.
1	Fan modules that are in faulty state (fail, fault).

Module State

Verifies the operational state of other discovered modules.

3	Modules that are in healthy state (powered-up).
1	Modules that are in faulty state (err).

PoE Interface State

Detects operational state of interfaces that are capable of distributing power over Ethernet (PoE).

10	Interfaces that are distributing power over ethernet and are operational (ON).
14	Interfaces that are capable of distributing power over ethernet and are not operational (OFF).

Stack Port State

Verifies the operational state of all discovered stack interfaces.

2	Stack interfaces that are operational, 'OK' detected status.
2	Stack interfaces that are not operational, 'DOWN' detected status.

FIRST HOP REDUNDANCY PROTOCOL (FHRP)

FHRP Virtual IPs (total)

All detected First Hop Redundancy Protocol (FHRP) virtual IP Addresses.

357	All detected FHRP Virtual IPs.

Gateway Redundancy

Verifies number of gateways for each discovered IP subnet.

211	IP subnets with more than one gateway with at least one user/endpoint.
91	IP subnets with only one gateway with at least one user/endpoint.

Virtual Gateways Consistency

Verifies gateways with virtual gateways alignment combined with the number of detected endpoints for each subnet.

261	IP subnets with two or more gateways and one virtual gateway with active endpoints or IP subnets with no active endpoints.
1055	IP subnets with zero virtual gateways or IP subnets with one physical gateway with less than 20 active endpoints.
15	IP subnets with two or more virtual gateways or IP subnets with no virtual gateway with more than 20 active endpoints.

FHRP Active Group Priority

Verifies the priority value for active First Hop Redundancy Protocol (FHRP) groups.

597	Active FHRP groups with priority value greater than 100.
126	Active FHRP groups with priority value of 100 (default) or lower.

FHRP Interfaces (total)

All detected First Hop Redundancy Protocol (FHRP) interfaces.

723	All detected First Hop Redundancy Protocol interfaces.

FHRP Group Members

Verifies number of members of First Hop Redundancy Protocol groups.

242	FHRP groups with expected number of members.
115	FHRP groups with unexpected number of members.

STP Root And FHRP Active Mismatch

Identifies active First Hop Redundancy Protocol (FHRP) gateways that are not aligned with the Spanning-Tree Protocol (STP) Root bridge.

7	Active FHRP gateways that are not aligned with the Spanning-Tree Protocol Root bridge.

IP ADDRESSING COMPLIANCE

Managed Networks (total)

Managed networks discovered by the platform.

1335	Unique managed networks discovered by the platform.

Managed IP Addresses (total)

Total number of managed IP addresses.

3057	Total number of managed IP addresses.

Managed IP Address DNS Consistency

Identifies IP addresses without matched Domain Name System (DNS) record.

14	Network devices with matching hostname with DNS and also the A/CNAME record.
3039	Network devices with no matching hostname with DNS or the A/CNAME record.
4	Network devices with no matching hostname with DNS and no matching A/CNAME record.

Duplicate IP Addresses

Identifies duplicated IP Addresses across the whole network, regardless of the VRF.

14	Duplicate IP addresses with 2 occurrences.
9	Duplicate IP addresses with more than 2 occurrences.

MAC Address Source

Identifies Media Access Control (MAC) address source.

29551	Media Access Control records with an expected dynamic sources (learn, dynamic, evpn, d, dl, dlr).
72	Media Access Control records from unexpected source.

Proxy ARP

Identifies Address Resolution Protocol (ARP) records which do not match IP network on an interface, resulting in Proxy ARP entries, potentially signifying network mask misconfiguration.

10231	Address Resolution Protocol records without Proxy ARP detected.
10	Address Resolution Protocol records with Proxy ARP detected.

INTERFACES

Interfaces (total)

The total number of discovered interfaces.

6642	The total number of discovered interfaces.

Interface Operational State

Verifies the administrative and operational state of the interfaces.

6624	Interfaces that are either administratively down or operating normally.
18	Interfaces with administrative state 'UP' and operational state is 'DOWN'.

Interface Duplex

Verifies duplex information on interfaces with the operational Link-Layer state (UP).

1536	Interfaces with the Link-Layer state 'UP' and 'FULL' duplex detected.
3124	Interfaces with the Link-Layer state 'UP' and no duplex detected.
255	Interfaces with the Link-Layer state 'UP' and duplex other than 'FULL' detected.

Interface Description

Detects if there's any description configured on discovered interfaces.

1658	Interfaces with configured description.
4984	Interfaces without configured description.

Maximum Transmission Unit (MTU)

Detects Maximum Transmission Unit (MTU) consistency on transit links across the network infrastructure.

1735	Transit links with consistent MTUs detected.
52	Transit links with missing MTU detected on either side.
8	Transit links with inconsistent MTUs detected.

Edge Port Security

Verifies the security method applied to edge interfaces.

537	Edge switching interfaces with security method other than 802.1X applied.

Edge-Ports with Multiple Neighbors

Detects non-trunk edge-ports with multiple learned mac-addresses.

461	Non-trunk edge-ports with two or less mac-addresses detected.
3	Non-trunk edge-ports with more than 100 mac-addresses detected.

Switchport Modes

Detects switchport modes for Spanning-Tree Protocol (STP) enabled interfaces.

2162	Interfaces with detected mode 'TRUNK' or 'ACCESS'.

55	Interfaces with detected modes other than 'TRUNK' or 'ACCESS'.

INVENTORY

Managed Network Devices (total)

Managed network infrastructure devices (including APs).

573	Total number of managed network infrastructure devices, including lightweight access points.

Device Uptime

Device uptime verification. Verifies that device continuous running time is within the expected thresholds.

570	Devices with uptime longer than 1 week and less than 3 years
2	Devices with uptime less than one week
1	Devices with uptime less than one day

Device Reload Reason

Device reload reason verification

569	Reload occurred more than 3 months ago
4	Reload reason contains failure and occurred in the past 1 week or a failure that was not due to power issues in the past 3 months

Device Memory Usage (%)

Memory utilization verification according to thresholds.

546	Devices memory utilization below 50%.
16	Device memory utilization between 50% and 70%.
4	Device memory utilization between 70% and 85%.
7	Device memory utilization greater than 85%

Software Configuration Register

Boot configuration register verification.

16	Devices with present configuration register other than 0x0
489	Devices with configuration register value equal to 0x0. The device will not load an OS or Configuration after reboot.

Modules (total)

Detected network device modules.

185	Detected network device modules.

End of Sale

End of Life verification. Lists part numbers which are no longer available to be ordered through the vendor's point-of-sale mechanisms.

15	Part numbers that have passed the End of Sale date.

End of Maintenance

Detects infrastructure devices that are no longer maintained by the vendor.

5	Part numbers which have announced End of Support date or equivalent, but have yet to pass it.
10	Part numbers which have announced End of Maintenance date or equivalent which has passed

End of Support

End of Life verification compares part numbers against vendor End of Life announcements, and reports part numbers which are no longer supported by the vendor, or are planned not to be supported in the future.

5	Part numbers which have announced End of Support date or equivalent, but have yet to pass it.
10	Part numbers which have announced End of Support date or equivalent which has passed

MANAGEMENT CONSISTENCY

AAA Authentication Method

Verifies the type of Authentication, authorization and accounting (AAA) Primary Authentication Method.

1034	Records with any type of Authentication method except 'none' or 'unspecified'.
502	Records with the type of Authentication method 'none' or 'unspecified'.

AAA Authorization Method

Verifies the type of Authentication, authorization and accounting (AAA) Primary Authorization Method.

517	Records with any type of Authorization method except 'none' or 'unspecified'.
8	Records with the type of Authorization method 'none' or 'unspecified'.

AAA Accounting Method

Verifies the type of Authentication, authorization and accounting (AAA) Primary Accounting Method.

508	Records with any type of Accounting method except 'none' or 'unspecified'.
3	Records with the type of Accounting method 'none' or 'unspecified'.

AAA Authentication Type

Verifies Authentication, authorization and accounting (AAA) Authentication for AAA lines.

1042	Lines with default AAA authentication method.
4	Lines with local authentication method, signifying the use of username and password configured locally on the device.
1	Lines with line authentication, signifying password configured directly on the line.
1	Lines with no authentication method, allowing unauthenticated access.

Devices with Telnet Access (total)

Detects network devices that allow access via Telnet.

505	

NTP Configured Sources

Verifies the number of configured Network Time Protocol (NTP) sources for each network device.

12	Network devices with 2 or 3 configured NTP sources.
525	Network devices with only 1 or more than 3 configured NTP sources.
32	Network devices with 0 configured NTP sources.

NTP Reachable Sources

Verifies reachable Network Time Protocol (NTP) sources with comparison to configured sources.

515	Network devices with equal number of configured sources and reachable sources.
9	Network devices with at least 1 configured source and 1 reachable source.
32	Network devices with no configured source and no reachable source.
13	Network devices with at least 1 configured source and no reachable source.

NTP Stratum Level

Verifies the value of Network Time Protocol (NTP) Stratum.

526	NTP sources with Stratum value lower than 4.
21	Unsynchronized NTP sources with Stratum value 16.

NTP Time Offset

Verifies the Time Offset (ms) value for Network Time Protocol (NTP) sources.

560	NTP sources with Time Offset less than 100ms.
6	NTP sources with Time Offset more above 1000ms.

NTP Network Round-Trip Time

Verifies the Round Trip Time (RTT) value for Network Time Protocol (NTP) sources.

559	NTP sources with Round Trip Time lower than 50ms.
4	NTP sources with Round Trip Time value within 50-100ms.
3	NTP sources with Round Trip Time value within 100-500ms.

Remote System Logging Destination Port

Verifies destination port configured for remote Syslog server for destination hosts.

532	Destination syslog hosts with destination port 514.
2	Destination syslog hosts with destination port other than 514 and not within the well-known network port range.
6	Destination syslog hosts with destination port other than 514 and within the well-known port range.

Remote System Logging Severity

Verifies remote system logging severity for network devices.

538	Devices with remote syslog server configuration that do not have 'DEBUG' enabled.
2	Devices with remote syslog server configuration that have 'DEBUG' enabled.

Local System Logging Severity

Verifies local system logging severity for network devices.

26	Devices with local syslog server configuration that do not have 'DEBUG' enabled.

SNMP Community Name

Verifies Simple Network Management Protocol (SNMP) communities configuration for network devices.

44	SNMP communities that have not been left with default name.
8	SNMP communities that are left with default name 'PUBLIC' or 'PRIVATE'.

SNMP Configuration Compliance

Verifies Simple Network Management Protocol (SNMP) configuration for network devices.

9	Devices with at least one configured SNMP user and with at least one configured SNMP community.
11	Devices with at least one configured SNMP user or with at least one configured SNMP community.
549	Devices with no SNMP user and no SNMP community configured.

Saved Config Consistency

Verifies saved configuration consistency for network devices.

569	Devices where check was not performed if the configuration was saved

Device Logging Configuration

Verifies Syslog server configuration for network devices.

516	Network devices with at least one remote and one local logging configured.
12	Network devices with no remote but at least one local logging configured.
41	Network devices with no remote and no local logging configured.

NEIGHBORSHIP COMPLIANCE

Duplex Mismatch or Missing

Detects mismatched or missing duplex information.

120	Links with missing duplex information.
22	Links with mismatched duplex.

Trunk Allowed VLAN Mismatch

Verifies allowed VLAN consistency at each end of the trunk link.

193	Trunk links with unequal number of allowed VLANs detected at each end.

Port-Channel Members State

Verifies membership state of aggregated interfaces across the network infrastructure.

69	Aggregated interfaces with healthy membership status 'UP', 'Collecting Distributing, '(P)', '(A)' or 'SELECTED'.
3	Aggregated interfaces with other than expected membership status.

STP Neighborship Expected State

Verifies Spanning-Tree Protocol (STP) port states between two neighbors on a shared link.

8320	Spanning-Tree neighbors with expected port role states on each side of a shared link (designated-alternate, root-designated).
2	Spanning-Tree neighbors with other than expected port role states on each side of shared link.

STP/CDP Neighbor Information Mismatch

Detects mismatch between Spanning-Tree Protocol (STP) and Cisco Discovery Protocol (CDP) or Link-Layer Discovery Protocol (LLDP) information.

14	Network devices with mismatched information between Spanning-Tree Protocol (STP) and discovery protocols (CDP/LLDP).

CDP/LLDP unidirectional

Detects unidirectional Cisco Discovery Protocol (CDP) or Link-Layer Discovery Protocol (LLDP) sessions.

23	Unidirectional CDP or LLDP sessions.

CDP/LLDP Neighbor State

Detects managed and unmanaged Cisco Discovery Protocol (CDP) or Link-Layer Discovery Protocol (LLDP) neighbors.

1474	Managed CDP or LLDP neighbors.
30	Unmanaged CDP or LLDP neighbors.

OSPF Neighbor State

Verifies operational state for detected Open Shortest Path First (OSPF) neighbors.

1640	OSPF neighbors with healthy state (FULL, 2WAY, ATTEMPT).
50	OSPF neighbors with transitive state (EXCHANGE, EXSTART, INIT, LOADING).
20	OSPF neighbors that are currently down.

OSPF Cost Consistency

Detects Open Shortest First Path (OSPF) sessions with mismatched or maximized cost values.

1278	OSPF sessions with equal local and neighbor cost.
2	OSPF sessions with maximized local and neighbor cost (65535).
430	OSPF sessions with unequal local and neighbor cost.

OSPF Interface Neighbors

Verifies the number of Open Shortest Path First (OSPF) sessions for OSPF enabled interfaces.

1169	OSPF enabled interfaces with one or more neighbors detected.
769	OSPF enabled interfaces with zero neighbors detected.

OSPFv3 Neighbor State

Verifies operational state for detected Open Shortest Path First version 3 (OSPFv3) neighbors.

60	OSPFv3 neighbors with healthy state (FULL, 2WAY, ATTEMPT).

OSPFv3 Cost Consistency

Detects Open Shortest First Path version 3 (OSPFv3) sessions with mismatched or maximized cost values.

50	OSPFv3 sessions with equal local and neighbor cost.
10	OSPFv3 sessions with unequal local and neighbor cost.

OSPFv3 Interface Neighbors

Verifies the number of Open Shortest Path First version 3 (OSPFv3) sessions for OSPFv3 enabled interfaces.

57	OSPFv3 enabled interfaces with one or more neighbors detected.
9	OSPFv3 enabled interfaces with zero neighbors detected.

EIGRP Interface Neighbors

Verifies number of Enhanced Interior Gateway Routing Protocol (EIGRP) sessions for OSPF interfaces.

42	EIGRP interfaces with one or more neighbors detected.
31	EIGRP interfaces with zero neighbors detected.

BGP Neighbor State

Verifies operational state for detected Border Gateway Protocol (BGP) sessions.

171	BGP sessions in ESTABLISHED state.
15	BGP sessions in a transitive state (OPENSENT, OPENCONFIRM, IDLE, CONNECT).
8	BGP sessions in ACTIVE state.

BGP Received Prefixes

Verifies the number of received prefixes from configured or established Border Gateway Protocol (BGP) neighbors.

140	Established BGP sessions with one or more received prefixes.
21	Non-established BGP sessions with no received prefixes.
33	Established BGP sessions with no received prefixes.

IS-IS Interface Neighbors

Verifies the number of Intermediate System to Intermediate System (IS-IS) neighbors for IS-IS enabled interfaces.

33	IS-IS enabled interfaces with one or more neighbors detected.
15	IS-IS enabled interfaces with zero neighbors detected.

RIP Interface Neighbors

Verifies number of Routing Information Protocol (RIP) neighbors for RIP enabled interfaces.

6	RIP interfaces with one or more neighbors detected.
46	RIP interfaces with zero neighbors detected.

LDP Interface Neighbors

Verifies the number of Label Distribution Protocol (LDP) neighbors for LDP enabled interfaces.

37	LDP enabled interfaces with one or more neighbors detected.
15	LDP enabled interfaces with zero neighbors detected.

OPERATING SYSTEM (OS)

Operating System Version (%)

Verifies operating system consistency for discovered vendors, families and platforms.

45	Platforms with the same operating system, that is installed on more than 30% of the platform.
2	Platforms with the same operating system, that is installed within 30% and 20% of the platform.
2	Platforms with the same operating system, that is installed within 20% and 10% of the platform.
6	Platforms with the same operating system, that is installed on less than 10% of the platform.

Devices with Unique OS

Detects operating system dispersion across discovered platforms.

49	Network devices with non-unique installed operating system.
6	Network devices with unique installed operating system.

Devices with Unique Platform

Detects network devices with unique platforms.

27	Network devices with non-unique platform.

28	Network devices with unique platform.

PERFORMANCE

Transfer Rates (inbound)

Verifies impact value for inbound transfer data rates on interfaces.

4251	Interfaces with 'Inbound Loss Impact' value equal to zero.
9	Interfaces with 'Inbound Loss Impact' value between 1 and 5.

Transfer Rates (outbound)

Verifies impact value for outbound transfer data rates on interfaces.

4240	Interfaces with 'Outbound Loss Impact' value equal to zero.
18	Interfaces with 'Outbound Loss Impact' value between 1 and 5.
2	Interfaces with 'Outbound Loss Impact' value between 5 and 10.

Transfer Rates (bidirectional)

Verifies impact value for bidirectional transfer data rates on interfaces.

4234	Interfaces with 'Bidirectional Loss Impact' value equal to zero.
24	Interfaces with 'Bidirectional Loss Impact' value between 1 and 5.
2	Interfaces with 'Bidirectional Loss Impact' value between 5 and 10.

Transfer Rates (device-inbound)

Verifies impact value for inbound transfer data rates per network device.

564	Devices with 'Inbound Loss Impact' value equal to zero.
8	Devices with 'Inbound Loss Impact' value between 1 and 5.

Transfer Rates (device-outbound)

Verifies impact value for outbound transfer data rates per network device.

552	Devices with 'Outbound Loss Impact' value equal to zero.
18	Devices with 'Outbound Loss Impact' value between 1 and 5.
2	Devices with 'Outbound Loss Impact' value between 5 and 10.

Transfer Rates (device-bidirectional)

Verifies impact value for bidirectional transfer data rates per network device.

548	Devices with 'Bidirectional Loss Impact' value equal to zero.
22	Devices with 'Bidirectional Loss Impact' value between 1 and 5.
2	Devices with 'Bidirectional Loss Impact' value between 5 and 10.

Input errors impact

Verifies impact value for input errors on individual interfaces.

4253	Interfaces with 'Input Errors Impact' value equal to zero.
3	Interfaces with 'Input Errors Impact' value between 1 and 5.

Output errors impact

Verifies impact value for output errors on individual interfaces.

4256	Interfaces where 'Output Errors Impact' value equal to zero.

Error Rates (bidirectional)

Verifies impact value for bidirectional errors on individual interfaces.

4253	Interfaces with 'Bidirectional Errors Impact' value equal to zero.
3	Interfaces with 'Bidirectional Errors Impact' value between 1 and 5.

Device input errors impact

Verifies impact value for input errors per network device.

569	Devices with 'Input Errors Impact' value equal to zero.
3	Devices with 'Input Errors Impact' value between 1 and 5.

Device output errors impact

Verifies impact value for output errors per network device.

572	Devices with 'Output Errors Impact' value equal to zero.

Error Rates (device-bidirectional)

Verifies impact value for bidirectional errors on individual interfaces.

569	Interfaces with 'Bidirectional Errors Impact' value equal to zero.
3	Interfaces with 'Bidirectional Errors Impact' value between 1 and 5.

Input drops impact

Verifies impact value for input drops on individual interfaces.

4250	Interfaces with 'Input Drops Impact' value equal to zero.
6	Interfaces with 'Input Drops Impact' value between 1 and 5.

Output drops impact

Verifies impact value for output drops on individual interfaces.

4236	Interfaces with 'Output Drops Impact' value equal to zero.
18	Interfaces with 'Output Drops Impact' value between 1 and 5.
2	Interfaces with 'Output Drops Impact' value between 5 and 10.

Drop Rates (bidirectional)

Verifies impact value for bidirectional drops on individual interfaces.

4233	Interfaces with 'Bidirectional Drops Impact' value equal to zero.
21	Interfaces with 'Bidirectional Drops Impact' value between 1 and 5.
2	Interfaces with 'Bidirectional Drops Impact' value between 5 and 10.

Device input drops impact

Verifies impact value for input drops per network device.

567	Devices with Input Drops Impact' value equal to zero.
5	Devices with 'Input Drops Impact' value between 1 and 5.

Device output drops impact

Verifies impact value for output drops per network device.

552	Devices with 'Output Drops Impact' value equal to zero.
18	Devices with 'Output Drops Impact' value between 1 and 5.
2	Devices with 'Output Drops Impact' value between 5 and 10.

Drop Rates (device-bidirectional)

Verifies impact value for bidirectional drops per network device.

550	Devices with 'Bidirectional Drops Impact' value equal to zero.
20	Devices with 'Bidirectional Drops Impact' value between 1 and 5.
2	Devices with 'Bidirectional Drops Impact' value between 5 and 10.

Access Point - Radio Signal Impact

Verifies the impact value for each access point (AP).

1	Access points zero impact value.
3	Access points with the impact value within 1 and 6.

Access Point - Connected Clients

Verifies the number of clients for each access point (AP) against predefined thresholds.

4	Access points with less than 50 clients connected.

Wireless Client - RSSI

Verifies the average Signal Strength (dBm) value for each connected client.

1	Connected clients with Signal Strength (dBm) greater than -60.

Path Performance Impact

Verifies the impact value for each network path.

4232	Network paths with no impact.
20	Network paths with the impact value between 1 and 9.

QoS EF Class Drops

QoS Expedited Forwarding classes are usually carrying critical traffic where drops are highly unwanted and can cause service degradation, signifying under-provisioning or other issues. Verification detects the drop rate within the Expedited Forwarding classes.

47	Classes carrying Expedited Forwarding traffic with drop rate equal to 0

Path Capacity Impact

Verifies the impact value for each network path capacity.

4234	Network paths with no impact.
18	Network paths with the impact value between 1 and 9.

Wireless Client - SNR

Verifies the average Signal to Noise Ratio (SNR) value for each connected client.

1	Connected clients with SNR greater than 25.

Port-Channel Output Balancing Variance

Verifies output balancing variance for aggregated interfaces.

46	Aggregated interfaces with output balancing variance lower than 500.
26	Aggregated interfaces with output balancing variance higher than 500 and Rate below 30Mbps.

Port-Channel Input Balancing Variance

Verifies input balancing variance value for aggregated interfaces.

54	Aggregated interfaces with input balancing variance lower than 500.
17	Aggregated interfaces with input balancing variance higher than 500 and Rate below 30Mbps.

QUALITY OF SERVICE (QOS)

Shaping Queues Child Policy

Verifies the presence of child policy for shaping queues.

47	Shaping queues with child policy configured.
37	Shaping queues without any child policy configured.

QoS EF Class Drops

QoS Expedited Forwarding classes are usually carrying critical traffic where drops are highly unwanted and can cause service degradation, signifying under-provisioning or other issues. Verification detects the drop rate within the Expedited Forwarding classes.

47	Classes carrying Expedited Forwarding traffic with drop rate equal to 0

QoS Priority Queue Drops

Detects drops on Quality of Service (QoS) Priority classes operating in the network.

47	QoS priority classes without any drops detected.

Queue Limit Size (packets)

Detects queue-limit size (packets) for each class within configured QoS policies.

178	QoS class with queue-limit size that is below 64 packets.
47	QoS classes with queue-limit size between 64 and 256 packets.

SPANNING-TREE PROTOCOL (STP)

STP Virtual Port Status

Verifies the status of Spanning-Tree Protocol virtual ports.

15545	STP virtual ports with healthy status (Forwarding, Blocking, Disabled, Disarding).
1	STP virtual ports with unexpected status.
17	STP virtual ports with non-healthy or transit status (Broken, Learn, Listen).

Switchport VLANs Without STP

Detects network devices with VLANs where no Spanning-Tree Protocol (STP) is being detected.

9	Network devices with VLANs where no Spanning-Tree Protocol (STP) is being detected.

STP Loops

Detects Spanning-Tree Protocol (STP) loops within switching topologies across the whole network.

8320	Spanning-Tree relationships with no loops detected.
2	Spanning-Tree relationships with loop detected.

STP Ports with Multiple Neighbors

Identifies network devices with Spanning-Tree Protocol (STP) ports with more than one neighbor attached.

21	Network ports using Spanning-Tree Protocol (STP) with more than one STP neighbor.

Multiple STP Links Between Two Devices

Detects multiple separate Spanning-Tree Protocol (STP) links between network devices.

12	Network devices with multiple shared Spanning-Tree Protocol links.

STABILITY

Device Uptime

Device uptime verification. Verifies that device continuous running time is within the expected thresholds.

570	Devices with uptime longer than 1 week and less than 3 years
2	Devices with uptime less than one week
1	Devices with uptime less than one day

Device Reload Reason

Device reload reason verification

569	Reload occurred more than 3 months ago
4	Reload reason contains failure and occurred in the past 1 week or a failure that was not due to power issues in the past 3 months

OSPF Session Age

Verifies Open Shortest Path First (OSPF) session age time against predefined compliance thresholds.

1534	OSPF sessions with uptime between one month and one week.
58	OSPF sessions with uptime between one week and one day.
103	OSPF sessions with uptime less than 24 hours.

OSPFv3 Session Age

Verifies Open Shortest Path First version 3 (OSPF) session age time against predefined compliance thresholds.

60	OSPFv3 sessions with uptime between one month and one week.

EIGRP Session Age

Verifies Enhanced Interior Gateway Routing Protocol (EIGRP) session age time against predefined compliance thresholds.

60	EIGRP sessions with uptime between one month and one week.

IS-IS Session Age

Verifies Intermediate System to Intermediate System (IS-IS) session age time against predefined compliance thresholds.

38	IS-IS sessions with uptime between one month and one week.
6	IS-IS sessions with uptime between one week and one day.
10	IS-IS sessions with uptime less than 24 hours.

BGP Session Age

Verifies Border Gateway Protocol (BGP) session age time against predefined compliance thresholds.

164	BGP sessions with uptime between one month and one week.
7	BGP sessions with uptime between one week and one day.
23	BGP sessions with uptime less than 24 hours.

LDP Session Age

Verifies Label Distribution Protocol (LDP) session age time against predefined compliance thresholds.

40	LDP sessions with uptime between one month and one week.

ENGINEERING SUMMARY

Engineering summary presents technical information about causes of issues currently affecting the network, and the best practice compliance notes that help with network operations.

INVENTORY

Inventory represents information about pieces of hardware or software and their associated detail for all of the 573 analyzed network infrastructure devices.

TRANSMISSION

Network infrastructure performance is derived from its ultimate goal to deliver a packet from source to destination in a sufficiently short amount of time. The key performance indicators of loss and delay are universally used by all IP consumers and dependent technologies. Transmission analysis focuses on packet loss at every point in the network to create a complete view of the network performance issues caused by network not being able to deliver a packet.

INTERFACE ERRORS

Interface errors represent packet loss occurring due to transmission faults.

INPUT INTERFACE ERRORS

Input interface errors signify the number of packets that had to be discarded because the packet could not be read. Input errors are caused by poor quality of physical wiring, ruptured cables, dirty connectors, network hardware faults, or other physical issues. Because input errors are closely associated with the physical layer they are often referred to as hard errors.

Issue impact: ★★★

Cost of remediation: ★★☆

The following table represents interfaces with the highest impact to user productivity due to input errors.

Hostname	Interface	Impact	Errors/second	In Errors %
L68AC25	Et0/1	1	0.06	0.4779 %

HWLAB-C3750-STACK	Gi1/0/21	5	1.362	3.2542 %
HWLAB-C871	Fa1	5	2.189	4.7662 %

Table 2: Interfaces with the highest productivity impact due to Input Interface Errors

REMEDIATION OF INPUT INTERFACE ERRORS

Check for physical cable damage. Ensure that proper category of cable is used and that connectors are correctly crimped and firmly plugged in. A patch panel, cable plant, media converter, or a circuit connected to the interface may be faulty.

To ensure that there is no issue with the local interface, use a known good interface.

In case remote device is outside of administrative domain, a temporary managed device may be inserted near the remote end to monitor for any cable faults and ensure that errors are not caused by the local interface.

Circuit may be tested by soft or hard loops, or by conducting end-to-end circuit test in cooperation with the carrier. A remote interface may be faulty or run improper drivers.

For copper cabling, use built in TDR to identify cable faults and too long links. TDR test causes a port outage up to several seconds, but may cause lasting ripple due to convergence events reacting at the port-down event.

For optical cabling, attenuation or dirt may be at fault. Loops, ODR tests, or cleaning of the connectors may help to determine or resolve the issue.

OUTPUT INTERFACE ERRORS

Output interface errors are caused by local controller or interface failures, such as local encapsulation failures, local hardware failures, and misconfiguration of interface or controller, resulting in failure to properly transmit a packet. Most output errors are avoidable and should be fixed.

No output errors were present during the analysis interval on any of the 4909 interfaces.

INTERFACE DROPS

Interface drops represent packets loss occurring due to buffer overflow. Interface drops are the most frequent cause of the packet loss in the network, signifying capacity issues.

INPUT INTERFACE DROPS

Input interface drops represent packet loss caused by input buffer overflow. Input drops result from inability of the platform to process incoming traffic fast enough due to system resource exhaustion, such as insufficient forwarding capacity, or head-of-line blocking on

the internal forwarding path. In cut-through systems, and systems with fabric supporting backpressure, input drops can be caused by the overutilized output port.

Issue impact: ★★★

Cost of remediation: ★★☆

The following table represents interfaces causing the highest impact to user productivity.

Hostname	Interface	Impact	In Drops/sec	In Drops %
HWLAB-ARUBA-AP-135-2	Br0	3	0.1	10.8225 %
aruba-ap-135-1	Br0	3	0.1	10.7181 %
HWLAB-ARUBA-AP-125	Br0	3	0.1	11.5473 %
HWLAB-FW-PA4020	Et1/2	4	0.496	49.9496 %
L1FW4	Et1/1	1	0.035	6.9721 %
HWLAB-FW-PA4020	Et1/1	4	0.496	42.3932 %

Table 3: Interfaces with the highest productivity impact due to Input Drops

REMEDIATION OF INPUT INTERFACE DROPS

Verify platform for system, line card, and fabric aggregation overutilization. In case system forwarding capacity, limit is reached, such as in the case of software platforms, consider switching to more efficient forwarding lookup methods, limiting the use of resource-heavy features, or upgrading the platform. In case line card or fabric aggregation limits are being reached, consider moving the function to a different port connected to a less utilized ASIC or line card. In case of cut-through systems and buffer backpressure propagation, verify output port utilization and path MTU.

OUTPUT INTERFACE DROPS

Output interface drops represent packet loss caused by output buffer overflow. Output drops are one of the most prevalent reasons for packet loss in IP networks, and usually signifies path overutilization.

Issue impact: ★★★

Cost of remediation: ★★☆

Proper network planning and statistical sharing of network capacity can significantly reduce the chance of microbursts saturating output buffer, however with increasing bandwidth demands it is a continuous endeavor.

The following table represents interfaces causing the highest impact to user productivity.

Hostname	Interface	Impact	Out Drops/sec	Out Drops %
L51EXR1	Et0/0	6	5.426	6.9903 %
L62EXR2	Et0/2	1	0.102	0.5499 %
L66EXR1	Et0/0	1	0.041	0.8989 %
L34CSR9	Gi2	5	1.576	13.1872 %
L49EXR2	Et0/0	1	0.069	0.4597 %
L68CSR8	Gi1	2	0.133	2.175 %
L68CSR7	Gi1	2	0.13	1.3625 %
L49EXR1	Et0/0	2	0.172	1.0395 %
L34CSR10	Gi2	3	0.215	3.9442 %
HWLAB-ARUBA-AP-135-2	Br0	1	0.017	43.5897 %
aruba-ap-135-1	Br0	1	0.017	43.5897 %
HWLAB-ARUBA-AP-125	Br0	1	0.017	43.5897 %
L31EXR2	Et0/0	3	0.733	0.2419 %
L38EXR2	Et0/0	2	0.168	0.8326 %
L31EXR1	Et0/0	2	0.649	0.2158 %
L66EXR2	Et0/0	2	0.128	1.6008 %
L38EXR1	Et0/0	1	0.092	0.4554 %
L36EXR2	Et0/0	4	0.862	1.7231 %
L45EXR2	Et0/0	3	0.193	1.5424 %
HWLAB-C871	Vl999	6	3.59	7.989 %

Table 4: Interfaces with the highest productivity impact due to Output Interface Drops

REMEDIATION OF OUTPUT INTERFACE DROPS

Output drops are directly addressed by capacity management, whether by strategically shifting traffic patterns to accommodate optimal cost parameters, distributing traffic over multiple links to gradually increase capacity, or upgrading hardware or circuits. Because drops will always be present, congestion management covering buffer segmentation and queue scheduling can reliably ensure that when drops have to occur, they will impact the less preferred traffic first.

DUPLEX MISMATCH

Most network equipment supports and prefers full duplex setting. There are few exceptions when half duplex operation is necessary, and in such a case all sides must be set for consistently half-duplex operation. Most frequent cause of half-duplex state is due to poor compatibility in historical Ethernet standard implementations, or from legacy configuration.

Issue impact: ★★☆

Cost of remediation: ★★☆

Duplex directly impacts both performance and capacity. Performance is further impacted due to wait times before sending traffic, imposed by the mandatory minimum interval

dictated by CSMA/CD. Duplex issues cause packet loss due to alignment errors, input errors due to overvoltage that scrambles encoding on the link, and other collision induced performance degradation, worsened by often inconsistent duplex state of direct neighbors.

The following table represents enabled Interfaces with duplex mismatch.

Local Hostname	Local Interface	Local Duplex	Remote Duplex	Remote Hostname	Remote Interface
HWLAB-FW-CPUTM1	Internal	N/A	full	HWLAB-C3750-STACK	Gi1/0/3
L43FWR3	Et0/2	N/A	full	L43AC5	Et0/1
L43FWR3	Et0/3	N/A	full	L43AC5	Et0/3
L43FWR3	Et1/0	N/A	full	L43AC5	Et1/1
L43FWR3	Et1/1	N/A	full	L43AC5	Et1/3
L71R4	Et0/3	N/A	full	L71FW5	port1
L72R8	Et0/1	N/A	half	L72AC24	Et0/2
L39AC101	Et0/1	half	N/A	L39EXR1	Et0/2
L66AC22	Et0/2	auto	full	L66JR6	em5

Table 5: Interfaces with mismatched duplex

ERR-DISABLED

There should be no interfaces disabled due to error. Interfaces are disabled due to violation of operational parameter, and should be self-healed by the automatic recovery timers, or recovered manually, ensuring that the violation will not occur in the future.

No interfaces have been disabled due to error events.

PHYSICAL STABILITY

Risk at physical layer affect base device operations, such as unexpected device reloads, announced end of life milestones affecting ability to procure vendor support, or disabled interfaces due to a detected error event.

UNEXPECTED RELOADS

The reason of the device operational state should be an expected event, such as device power event, reload command, or an upgrade.

Issue impact: ★★☆

Cost of remediation: ★★★

The following devices have rebooted due to unexpected reason. Unexpected reloads can be caused by software or hardware issue, repair of which is covered by the warranty or service contract.

Hostname	Uptime	Reload reason
L67JR6	2 weeks, 4 days, 22 hours, 59 minutes	0x10:misc hardware reason
L67JR5	1 week, 4 days, 22 hours, 9 minutes	0x10:misc hardware reason
L66JR6	1 week, 3 days, 8 hours, 38 minutes	0x10:misc hardware reason
L66JR5	1 week, 2 days, 19 hours, 46 minutes	0x10:misc hardware reason

Table 6: Unexpected Reloads

CONFIGURATION REGISTER

Configuration register instructs the system how to behave during boot, and can modify operational low-level system parameters.

Irregular configuration register settings can significantly prolong recovery after a failure or a reboot, complicate management over console interface, or cause abnormal broadcast behavior.

Usual symptoms of suboptimal configuration register settings include device losing its configuration upon reboot or device not loading the system image, both of which require manual intervention via the console port.

Issue impact: ★☆☆

Cost of remediation: ★☆☆

Devices in the following list have configuration register other than the expected values 0x2102, 0x2101, or 0xF, and should be checked whether there is justified use-case.

Hostname	Configuration register
L36AC33	0x0
L1R13	0x0
L81R10	0x0
L81R6	0x0
L81R3	0x0
L81R8	0x0
L81R7	0x0

Table 7: Irregular configuration register

RECENT RELOADS

Devices should not be reloaded without purpose. Device with frequent reboots may have detrimental impact on the business.

Issue impact: ★★☆

Cost of remediation: ★★★

The following table lists the devices that have been operational for less than a month.

Hostname	Uptime	Reload Reason	Platform
HWLAB-FW-RBSH1	2 hours, 32 minutes, 31 seconds	N/A	riverbed
HWLAB-HPE1920	1 day, 19 hours, 34 minutes	N/A	hp
L1EOS2	6 days, 21 hours, 56 minutes	N/A	arista
L66JR5	1 week, 2 days, 19 hours, 46 minutes	0x10:misc hardware reason	juniper
L66JR6	1 week, 3 days, 8 hours, 38 minutes	0x10:misc hardware reason	juniper
L1EOS1	1 week, 3 days, 19 hours, 10 minutes	N/A	arista
L67JR5	1 week, 4 days, 22 hours, 9 minutes	0x10:misc hardware reason	juniper
HWLAB-FW-CPUTM1	1 week, 5 days, 18 hours, 10 minutes	N/A	checkpoint

Table 8: Devices operational for less than a month

END OF LIFE MILESTONES

Network infrastructure vendors use end of life milestones to communicate stage of the product lifecycle, allowing sufficient time to migrate to a next generation product.

Issue impact: ★☆☆

Cost of remediation: ★★★

Lifecycle extension beyond end of life defined by vendor is a viable strategy that delivers substantial benefits when risk is managed properly. With proper tools and procedures, network infrastructure equipment can efficiently serve long past official last day of life.

End of Life milestones were announced for the part numbers in the table below.

Hostname	P/N	End of Support
HWLAB-FW-C5510/admin	ASA-180W-PWR-AC	30.09.2018
HWLAB-FW-PA4020	PA-4020	30.04.2019
HWLAB-WLC-C4400	AIR-WLC4402-25-K9	30.06.2016
HWLAB-AP-1242AG	AIR-LAP1242AG-E-K9	31.07.2018
L1R11	CISCO7206VXR	30.09.2017
L1R11	MEM-I/O-FLD128M	30.09.2017
L1R11	NPE-400	08.09.2015
HWLAB-WLC-A620	620-4	01.10.2018
HWLAB-C3750-STACK	WS-C3750-24PS-S	31.07.2015
HWLAB-C3750-STACK	WS-C3750E-24TD-S	31.01.2018

Table 9: Announced End of Life milestones

LINK LAYER STABILITY

Link layer stability is calculated based on risk observed in the component link layer protocols.

DISCOVERY PROTOCOLS

This section covers state information from CDP and LLDP protocols.

UNMANAGED LINK NEIGHBORS

Link layer discovery protocols generously share management information without authentication by design, and should be within a single administrative domain. Running link layer discovery protocols such as CDP or LLDP between management domains poses a moderate security risk, and should not be used without consideration.

All of the CDP and LLDP neighbors are managed.

UNIDIRECTIONAL LINK NEIGHBORS

Link layer discovery protocols should be established bidirectionally between devices where enabled. Unidirectional neighborship points to consistency issues or misconfiguration.

Issue impact: ★☆☆

Cost of remediation: ★☆☆

The following table represents lists network devices which see a remote neighbor through a link layer discovery protocol without reciprocating visibility from the neighbor side.

Local Hostname	Local Interface	Remote IP	Remote Hostname
L71FW5	port4	10.71.109.103	L71R3
L71FW5	port1	10.71.209.104	L71R4
HWLAB-ARUBA-AP-135-2	Et0	192.168.103.1	HWLAB-C3750-STACK
L62SD25	Et0/0	10.62.26.109	L62R9
L1R12	Et2/6	10.241.12.9	L1R9
L62SD24	Et0/0	10.62.25.108	L62R8
L38AC7	Et0/1	10.38.109.105	L38R5
HWLAB-A2530	1	192.168.101.1	HWLAB-C3750-STACK
HWLAB-C3750-STACK	Gi1/0/17	192.168.127.100	HWLAB-FW-RBSH1
L35AC171	Et0/1	10.35.254.50	L35EXR13
L34AC25	Et0/1	10.34.91.103	L34R3
L47AC7	Et0/1	10.47.109.105	L47R5

Table 10: Unmanaged CDP and LLDP neighbors

AGGREGATION CHANNELS

This section covers state information about port-channels (or ether channels), which combine multiple physical links for load sharing and redundancy purposes.

CHANNEL MEMBERSHIP ANALYSIS

All of the member interfaces of each link aggregation channel should be either in up or down state, representing common operational behavior. When a dynamic aggregation protocol detects an operational issue, it suspends the member interface. Such interfaces should be addressed as a priority due to a potentially damaging behavior that can result from inconsistently configured channels.

Issue impact: ★★☆

Cost of remediation: ★☆☆

The following table presents channels with members in suspended, waiting, or individual states.

Hostname	Portchannel	Members in irregular state
HWLAB-JEX2200-SW1	ae0	ge-0/0/20(DOWN (DETACHED)), ge-0/0/21(DOWN (DETACHED))
HWLAB-SGE300	Po1	Gi2(NON-CANDIDATE), Gi1(ACTIVE)
HWLAB-WLC-A620	Po1	Fa1/7(DOWN)

Table 11: Irregular member state

CHANNEL BALANCING

Issue impact: ★☆☆

Cost of remediation: ★☆☆

The following table lists aggregation channels with unbalanced load distribution between individual members

Hostname	Interface	Balancing Ratios	Members
L48ACC135	Po28	99/0/0/0	Et2/0, Et2/1, Et2/2, Et2/3
L48SD5	Po29	95/1/1/3	Et3/0, Et3/1, Et3/2, Et3/3
L48ACC135	Po31	95/0/2/3	Et3/0, Et3/1, Et3/2, Et3/3
L36ACC134	Po20	93/0/4/2	Et0/0, Et0/1, Et0/2, Et0/3
L48SD4	Po34	93/0/0/6	Et4/0, Et4/1, Et4/2, Et4/3
L48SD4	Po26	93/0/0/6	Et3/0, Et3/1, Et3/2, Et3/3
L48SD4	Po25	93/0/0/6	Et2/0, Et2/1, Et2/2, Et2/3
L48SD5	Po27	91/2/2/5	Et0/0, Et0/1, Et0/2, Et0/3
L48SD5	Po32	90/3/2/5	Et4/0, Et4/1, Et4/2, Et4/3
L36AC10	Po20	97/1/1/1	Et0/0, Et0/1, Et0/2, Et0/3

Table 12: Uneven channel balancing

SPANNING TREE

Spanning tree protocol prevents loops and manages redundancy in a layer 2 network. Spanning tree instances and contiguous domains are analyzed for stability and consistency.

STP TOPOLOGY CHANGES

No topology convergence events have been observed during the analysis.

UNEXPECTED STP VIRTUAL PORT STATE

Virtual ports are ports in a particular VLAN. A single trunk will participate in multiple spanning tree instances, one for every VLAN allowed on the port, including native VLAN. Port status determines forwarding behavior. Broken virtual ports signify present inconsistency and are not forwarding.

Issue impact: ★★★

Cost of remediation: ★★☆

The following table represents broken STP ports

Hostname	VLAN	Port	Port Status	Port ID	Root ID
L1R12	Vl1	Et2/3	N/A	128.259	5000.0010.002f
L1EOS1	Vl126	Et1	learning	128.1	0000.0024.76c6
L1EOS1	Vl124	Et1	learning	128.1	0000.0024.76c6
L1EOS1	Vl123	Et1	learning	128.1	0000.0024.76c6
L1EOS1	Vl122	Et1	learning	128.1	0000.0024.76c6
L1EOS1	Vl121	Et1	learning	128.1	0000.0024.76c6
L1EOS1	Vl119	Et1	learning	128.1	0000.0024.76c6
L1EOS1	Vl118	Et1	learning	128.1	0000.0024.76c6
L1EOS1	Vl117	Et1	learning	128.1	0000.0024.76c6
L1EOS1	Vl116	Et1	learning	128.1	0000.0024.76c6
L1EOS1	Vl115	Et1	learning	128.1	0000.0024.76c6
L1EOS1	Vl113	Et1	learning	128.1	0000.0024.76c6
L1EOS1	Vl112	Et1	learning	128.1	0000.0024.76c6
L1EOS1	Vl111	Et1	learning	128.1	0000.0024.76c6
L1EOS1	Vl100	Et1	learning	128.1	0000.0024.76c6
L1EOS1	Vl12	Et1	learning	128.1	0000.0024.76c6
HWLAB-C3750-STACK	Vl1	Gi1/0/19	broken	128.19	4431.920b.8112
HWLAB-C3750-STACK	Vl101	Gi1/0/19	broken	128.19	0014.6a06.2180

Table 13: Unexpected STP Virtual Port State

NETWORK LAYER STABILITY

Network layer stability is calculated based on the routing and network layer protocol information and the number of users affected by each issue.

MANAGED DUPLICATE IP ADDRESSING

IP addresses should be unique throughout the network, except for highly specialized applications, such as geographical service distribution via anycast. Duplicate IPs usually signify a network fault, such as loss of keep alive link or misconfiguration, and can cause various degrees of issues from total loss of connectivity for a network segment to intermittent application reachability to complicating network infrastructure management.

Issue impact: ★☆☆

Cost of remediation: ★★☆

The following table presents duplicate active addresses in the network.

Duplicate IP	Number of occurrences	Devices with duplicate IPs
128.0.0.1	6	HWLAB-JEX2200-SW1(bme0.32768), L1R14(em1.0), L1R17(em1.0), L1R15(em1.0), L1R18(em1.0), L1R7(em1.0)
10.0.0.4	5	L1R14(em1.0), L1R17(em1.0), L1R15(em1.0), L1R18(em1.0), L1R7(em1.0)
128.0.0.4	5	L1R14(em1.0), L1R17(em1.0), L1R15(em1.0), L1R18(em1.0), L1R7(em1.0)
172.16.0.1	4	L67JR6(em1.0), L67JR5(em1.0), L66JR6(em1.0), L66JR5(em1.0)
10.77.220.1	4	L77R9-LEAF3(Vl220), L77R8-LEAF2(Vl220), L77R7-LEAF1(Vl220), L77R10-LEAF4(Vl220)
10.77.200.1	4	L77R9-LEAF3(Vl200), L77R8-LEAF2(Vl200), L77R7-LEAF1(Vl200), L77R10-LEAF4(Vl200)
10.0.0.6	3	L66JFW9(sp-0/0/0.16383), L66JFW10(sp-0/0/0.16383), L1R16(sp-0/0/0.16383)
192.168.127.1	3	L1EOS1(Vl127), HWLAB-C871(Vl127), HWLAB-C3750-STACK(Vl127)
128.0.0.6	3	L66JFW9(sp-0/0/0.16383), L66JFW10(sp-0/0/0.16383), L1R16(sp-0/0/0.16383)
192.168.127.254	2	HWLAB-WLC-A620(Vl127), L1EOS2(Vl127)
1.1.1.1	2	L1LB1(VLAN_GROUP1), L1FW4(vlan.100)
127.0.0.1	2	HWLAB-FW-CPUTM1(lo), L1fw8(lo)
10.77.100.1	2	L77R5-SPINE1(Lo1), L77R6-SPINE2(Lo1)
10.46.129.1	2	L46DR7(Et0/3.129), L46DR8(Et0/3.129)
10.46.128.1	2	L46DR7(Et0/3.128), L46DR8(Et0/3.128)
10.46.127.1	2	L46DR7(Et0/3.127), L46DR8(Et0/3.127)
10.46.126.1	2	L46DR7(Et0/3.126), L46DR8(Et0/3.126)
10.46.125.1	2	L46DR7(Et0/3.125), L46DR8(Et0/3.125)
10.46.124.1	2	L46DR7(Et0/3.124), L46DR8(Et0/3.124)
10.46.123.1	2	L46DR7(Et0/3.123), L46DR8(Et0/3.123)
10.46.122.1	2	L46DR7(Et0/3.122), L46DR8(Et0/3.122)
10.46.121.1	2	L46DR7(Et0/3.121), L46DR8(Et0/3.121)
10.46.120.1	2	L46DR7(Et0/3.120), L46DR8(Et0/3.120)

Table 14: Duplicate Managed IP Addresses

ROUTING STABILITY

Routed network stability is measured from the last convergence time of the network, and depends on how many users are located in that network, and in how many routing tables the network is present. Network instability adds to intermittent or prolonged outages for hosts and users.

OSPF STABILITY

Issue impact: ★☆☆

Cost of remediation: ★★☆

The following OSPF sessions have converged in the past month

Hostname	Interface Name	Area	Neighbor Address	Neighbor Hostname	Neighbor Interface	VRF	Session time
L47R5	Et0/3.115	0	10.47.115.106	L47R6	Et0/3.115	N/A	1 minute, 14 seconds
L34CSR10	Gi2.122	0	10.34.122.109	L34CSR9	Gi2.122	N/A	1 minute, 16 seconds
L47R5	Et0/3.116	0	10.47.116.106	L47R6	Et0/3.116	N/A	1 minute, 20 seconds
L47R5	Et0/3.110	0	10.47.110.106	L47R6	Et0/3.110	N/A	1 minute, 22 seconds
L34CSR10	Gi2.127	0	10.34.127.109	L34CSR9	Gi2.127	N/A	1 minute, 24 seconds
L68CSR10	Gi2.121	0	10.68.121.109	L68CSR9	Gi2.121	N/A	1 minute, 41 seconds
L68CSR10	Gi2.120	0	10.68.120.109	L68CSR9	Gi2.120	N/A	1 minute, 41 seconds
L1EOS3	Vl100	0.0.0.0	10.241.1.1	L1R1	Et0/2	default	22 hours, 14 minutes
L1EOS1	Vl100	0.0.0.0	10.241.1.2	L1R2	Et0/2	default	1 day, 1 hour
L1EOS2	Vl100	0.0.0.0	10.241.1.21	L1EOS1	Vl100	default	1 day, 1 hour, 26 minutes, 8 seconds
L47R5	Et0/3.114	0	10.47.114.106	L47R6	Et0/3.114	N/A	1 day, 2 hours
L47R6	Et0/3.114	0	10.47.114.105	L47R5	Et0/3.114	N/A	1 day, 2 hours
L38R5	Et0/3.114	0	10.38.114.106	L38R6	Et0/3.114	N/A	2 days, 11 hours
L38R6	Et0/3.114	0	10.38.114.105	L38R5	Et0/3.114	N/A	2 days, 11 hours
L34CSR9	Gi2.129	0	10.34.129.110	L34CSR10	Gi2.129	N/A	4 days, 3 hours
L34CSR10	Gi2.129	0	10.34.129.109	L34CSR9	Gi2.129	N/A	4 days, 3 hours
L1R1	Et0/2	0	10.241.1.21	L1EOS1	Vl100	N/A	4 days, 5 hours
L1R16	ge-0/0/2.0	0	10.241.1.21	L1EOS1	Vl100	master	4 days, 5 hours, 7 minutes, 32 seconds
L1SW1	Vl100	0	10.241.1.22	L1EOS2	Vl100	N/A	6 days, 21 hours
L1R3	Gi1	0	10.241.1.22	L1EOS2	Vl100	N/A	6 days, 21 hours
L1R1	Et0/2	0	10.241.1.23	L1EOS3	Vl100	N/A	6 days, 21 hours
L1XOS2	VLAN100	0.0.0.0	10.241.1.3	L1R3	Gi1	VR-Default	1 week, 3 days, 19 hours, 8 minutes, 35 seconds
L1XOS2	VLAN100	0.0.0.0	10.241.1.1	L1R1	Et0/2	VR-Default	1 week, 3 days, 19 hours, 8 minutes, 35 seconds
L1XOS2	VLAN100	0.0.0.0	10.241.1.16	L1R16	ge-0/0/2.0	VR-Default	1 week, 3 days, 19 hours, 8 minutes, 35 seconds
L1XOS2	VLAN100	0.0.0.0	10.241.1.104	L1FW1	Gi0/0	VR-Default	1 week, 3 days, 19 hours, 8 minutes, 35 seconds

Table 15: Recently converged OSPF sessions

BGP STABILITY

Issue impact: ★☆☆

Cost of remediation: ★★☆

The following BGP sessions have converged in the past month

Hostname	Local AS	Neighbor Address	Neighbor Hostname	Neighbor Interface	Neighbor AS	State	Session time
L45R4	64545	10.45.255.111	L45XR11	Lo0	64545	idle	0 seconds
L1fw8	64580	10.241.255.16	L1R16	lo0.0	64580	established	0 seconds
L1fw8	64580	10.241.1.108	L1XOS1	VLAN100	459840747	established	0 seconds
HUA-AR1	65100	10.242.1.129	N/A	N/A	123456	connect	0 seconds
L45XR11	64545	10.45.255.104	L45R4	Lo0	64545	active	0 seconds
L45XR11	64545	10.10.45.112	L45XR12	Lo45	64545	idle	0 seconds
L45XR11	64545	10.10.45.112	L45XR12	Lo45	64545	idle	0 seconds
L45XR11	64545	10.10.45.112	L45XR12	Lo45	64545	idle	0 seconds

Table 16: Recently converged BGP sessions

EIGRP STABILITY

Issue impact: ★☆☆

Cost of remediation: ★★☆

The following EIGRP sessions have converged in the past month

Hostname	Local AS	Neighbor Address	Neighbor Hostname	Neighbor Interface	Neighbor AS	Session time
L1R11	50	10.251.10.12	L1R12	Et2/1.20	50	2 weeks, 1 day
L1R11	20	10.241.9.12	L1SW2	Gi1/0	20	2 weeks, 1 day
L1R11	20	10.241.8.12	L1R12	Et2/2	20	2 weeks, 1 day
L1R11	20	10.241.8.9	L1R9	Et0/1	20	2 weeks, 1 day
L1R11	20	10.241.10.12	L1R12	Et2/1.10	20	2 weeks, 1 day
L1R11	20	10.241.8.102	L1SW2	Vl200	20	2 weeks, 1 day
L1R11	20	10.241.13.10	L1R10	Fa1/0	20	2 weeks, 1 day
L1R11	20	10.241.9.10	L1R10	Fa0/1	20	2 weeks, 1 day
L1R11	20	10.241.8.10	L1R10	Fa0/0	20	2 weeks, 1 day
L1R9	20	10.241.8.11	L1R11	Fa0/0	20	2 weeks, 4 days

Table 17: Recently converged EIGRP sessions

IS-IS STABILITY

Issue impact: ★☆☆

Cost of remediation: ★★☆

The following IS-IS sessions have converged in the past month

Hostname	Interface	Neighbor Address	Neighbor Hostname	Neighbor Interface	Session time
L1EOS3	Vl100	10.241.1.4	L1R4	Gi1/0	0 seconds
L1EOS2	Vl100	10.241.1.9	L1R9	Et0/0	0 seconds
L1EOS2	Vl100	10.241.1.23	L1EOS3	Vl100	0 seconds
L1EOS2	Vl100	10.241.1.108	L1XOS1	VLAN100	0 seconds
L1EOS2	Vl100	10.241.1.4	L1R4	Gi1/0	0 seconds
L1EOS3	Vl100	10.241.1.9	L1R9	Et0/0	0 seconds
L1EOS3	Vl100	10.241.1.108	L1XOS1	VLAN100	0 seconds
L1EOS3	Vl100	10.241.1.22	L1EOS2	Vl100	0 seconds
L1R9	Et0/0	10.241.1.23	L1EOS3	Vl100	22 hours, 11 minutes, 31 seconds
L1R4	Gi1/0	10.241.1.23	L1EOS3	Vl100	22 hours, 11 minutes, 43 seconds
L1R9	Et0/0	10.241.1.108	L1XOS1	VLAN100	2 days, 18 hours
L1R4	Gi1/0	10.241.1.108	L1XOS1	VLAN100	2 days, 18 hours, 53 minutes, 25 seconds
L1R9	Et0/0	10.241.1.22	L1EOS2	Vl100	6 days, 21 hours
L1XOS1	VLAN100	10.241.1.23	L1EOS3	Vl100	6 days, 21 hours, 54 minutes
L1XOS1	VLAN100	10.241.1.22	L1EOS2	Vl100	6 days, 21 hours, 54 minutes
L1R4	Gi1/0	10.241.1.22	L1EOS2	Vl100	6 days, 21 hours, 55 minutes, 14 seconds
L1XOS3	VLAN100	10.241.1.108	L1XOS1	VLAN100	1 week, 14 hours, 10 minutes

Table 18: Recently converged IS-IS sessions

ACTIVE FHRP GATEWAYS WITH DEFAULT PRIORITY

Issue impact: ★☆☆

Cost of remediation: ★★☆

The following active gateways have default or smaller priority configured.

Hostname	Protocol	Group	Virtual IP	Interface	Priority
L35SD82	hsrp	180	10.35.180.1	Vl180	100
L35SD82	hsrp	181	10.35.181.1	Vl181	100
L35SD82	hsrp	182	10.35.182.1	Vl182	100
L35SD82	hsrp	183	10.35.183.1	Vl183	100
L35SD82	hsrp	184	10.35.184.1	Vl184	100
L35SD82	hsrp	185	10.35.185.1	Vl185	100
L35SD82	hsrp	186	10.35.186.1	Vl186	100
L35SD82	hsrp	187	10.35.187.1	Vl187	100
L35SD82	hsrp	188	10.35.188.1	Vl188	100
L35SD82	hsrp	189	10.35.189.1	Vl189	100
L36SD8	hsrp	120	10.36.120.1	Vl120	100
L36SD8	hsrp	121	10.36.121.1	Vl121	100
L36SD8	hsrp	122	10.36.122.1	Vl122	100

Table 19: Active gateways with default FHRP priority

MANAGEMENT

The following section covers analysis of management protocol access and parameters.

UNSYNCHRONIZED NTP

Issue impact: ★☆☆

Cost of remediation: ★★☆

The following table presents managed devices where NTP is not synchronized since none of the sources are eligible or sources are not configured.

Hostname	Configured Sources	Reachable Sources
L1R13	0	0
L1LB1	1	0
HWLAB-WLC-A620	0	0
HWLAB-JEX2200-SW1	0	0
HWLAB-SGE300	0	0
L77R11-LEAF5	0	0
L77R9-LEAF3	0	0
L77R12-LEAF6	0	0
L77R10-LEAF4	0	0
L68CSR8	0	0
L68CSR9	0	0
L68CSR7	0	0
L68CSR10	0	0
L67JR6	0	0
L67JR5	0	0
L66JFW9	0	0
L66JFW10	0	0

Table 207: Devices with not eligible NTP sources

TELNET PROTOCOL ACCESS

Issue impact: ★☆☆

Cost of remediation: ★★☆

The table presents managed devices where telnet protocol is enabled. Clear text management protocol is considered a security violation by many governmental and industrial regulations. While limited use of telnet can be acceptable under certain circumstances, such as restricted use only to specific management subnets, it is highly recommended to migrate to SSH protocol for management command line access

Hostname	Telnet access
L81EXR1	Enabled
L77R11-LEAF5	Enabled
L77R3-CORE1	Enabled
L77R4-CORE2	Enabled
L77R12-LEAF6	Enabled

L72R8	Enabled
L72R10	Enabled
L68R3	Enabled
L68R4	Enabled
L68EXR2	Enabled
L68EXR1	Enabled
L67R4	Enabled
L66R3	Enabled
L66R4	Enabled
L66EXR1	Enabled
L65EXR1	Enabled
L71EXR1	Enabled
L71FW9_root	Enabled
L71FW9_ipf	Enabled

Table 218: Devices with enabled TELNET access