Network Analysis Report

Fri Jan 14 14:43:28 2022

Table of content

1. Network Analysis Report Summary

This report analyses 472 devices based on the IP Fabric system's snapshot data; the system compiled the snapshot on Thu Jan 13 21:00:01 2022. Various detailed network protocols and technology parameters were compared and analyzed for risk, compliance, and potential security risks-issues divided into multiple categories or groups.

System Hostname	ipfabric.ipf.ipfabric.io
System Version	4.2.0
Snapshots available	25
Snapshot ID:	ed9e7801-e973-4268-8b1d-1f58f8e2c1dc
Number of devices	472
Number of hosts	1271
Number of interfaces	6029
Number of active ints	3886
Number of edge ints	249
Detected Port-Channels	70
Detected unique VLAN IDs	201
Detected unique VRF names	83
Number of IPSec Tunnels	18
Number of IPSec Gateways	15
Routing protocols	['BGP', 'OSPF', 'OSPFV3', 'ISIS']

1.1 Network Overview

Fundamental facts about the network infrastructure based on the snapshot created between Thu Jan 13 21:00:01 2022 and Thu Jan 13 21:18:41 2022

1.2 Vendor Mix Overview

Vendor	#Families	#Platforms	#Models	#Devices Total
arista	1	1	1	3
checkpoint	1	1	1	1
cisco	5	9	8	417
dell	1	1	1	1
extreme	2	3	3	3
f5	1	1	1	1
fortinet	1	1	1	7
hp	5	9	9	15
juniper	1	4	2	20
mikrotik	1	2	2	3
riverbed	1	1	1	1

1.3 Management protocols summary

Network management protocols are responsible for collecting and organizing information about managed devices on IP networks and changing device behavior. Due to their nature, they form a critical part for network infrastructure management and therefore is essential to understand how they are implemented and what management systems are used to operate the network.

Following tables represents all detected management servers for supported management protocols.

AAA Servers (server - count [share])
10.0.10.10 - 417 [93.4978%], 10.50.9.140 - 6 [1.3453%], 10.0.10.17 - 5 [1.1211%], 1.2.3.4 - 3 [0.6726%], 11.12.13.14 - 2 [0.4484%], 10.50.9.142 - 2 [0.4484%], 10.50.9.141 - 2 [0.4484%], 5.6.7.8 - 1 [0.2242%], 25.26.27.28 - 1 [0.2242%], 21.22.23.24 - 1 [0.2242%], 19.18.17.16 - 1 [0.2242%], 15.16.17.18 - 1 [0.2242%], 11.22.33.44 - 1 [0.2242%], 10.0.9.100 - 1 [0.2242%], 1.11.111.1 - 1 [0.2242%]

NTP Servers (server - count [share])
10.0.10.10 - 383 [86.0674%], 10.0.20.10 - 38 [8.5393%], ntp2.fortiguard.com - 4 [0.8989%], ntp1.fortiguard.com - 4 [0.8989%], 1.1.1.1 - 4 [0.8989%], 10.0.10.15 - 2 [0.4494%], 69.94.125.29 - 1 [0.2247%], 66.187.233.4 - 1 [0.2247%], 63.240.161.99 - 1 [0.2247%], 209.104.4.231 - 1 [0.2247%], 208.70.196.25 - 1 [0.2247%], 195.113.144.238 - 1 [0.2247%], 195.113.144.201 - 1 [0.2247%], 10.9.8.7 - 1 [0.2247%], 10.10.10.10 - 1 [0.2247%], 10.0.10.11 - 1 [0.2247%]

SNMP Trap Hosts (server - count [share])
192.168.12.12 - 5 [21.7391%], 10.0.10.26 - 3 [13.0435%], 192.168.125.13 - 2 [8.6957%], 192.168.12.14 - 2 [8.6957%], fe::12:1 - 1 [4.3478%], 192.168.15.16 - 1 [4.3478%], 192.168.15.15 - 1 [4.3478%], 192.168.125.12 - 1 [4.3478%], 192.168.11.162 - 1 [4.3478%], 192.168.10.13 - 1 [4.3478%], 192.168.10.12 - 1 [4.3478%], 192.168.10.11 - 1 [4.3478%], 192.168.10.10 - 1 [4.3478%], 162.168.15.15 - 1 [4.3478%], 10.0.9.14 - 1 [4.3478%]

Syslog Servers (server - count [share])
10.0.10.10 - 367 [84.5622%], 10.0.20.10 - 38 [8.7558%], 10.0.10.15 - 8 [1.8433%], 10.0.9.50 - 5 [1.1521%], 10.10.10.10 - 3 [0.6912%], 10.0.10.16 - 3 [0.6912%], 10.0.32.133 - 2 [0.4608%], 10.0.9.43 - 1 [0.2304%], 10.0.9.37 - 1 [0.2304%], 10.0.32.132 - 1 [0.2304%], 10.0.32.131 - 1 [0.2304%], 10.0.10.20 - 1 [0.2304%], 1.2.3.4 - 1 [0.2304%], 1.1.1.3 - 1 [0.2304%], 1.1.1.2 - 1 [0.2304%]

Netflow Collectors (collector - count [share])
10.0.9.54 - 5 [71.4286%], 10.20.30.40 - 1 [14.2857%], 10.0.9.55 - 1 [14.2857%]

sFlow Collectors (collector - count [share])
10.0.9.54 - 5 [100.0%]

Telnet enabled devices total
399

2. Defined Intent-Based Rules
Widget - First Hop Redundancy Protocol (FHRP)

Gateway Redundancy

Verifies number of gateways for each discovered IP subnet.

67	IP subnets with more than one gateway with at least one user/endpoint.
41	IP subnets with only one gateway with at least one user/endpoint.

FHRP Master Inconsistency

Highlights group with no master, or more than one.

176	FHRP group with one master
0	Default
2	FHRP master appear more than once
14	No master detected

FHRP Active Group Priority

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

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

FHRP Group Members

Verifies number of members of First Hop Redundancy Protocol groups.

152	FHRP groups with expected number of members.
40	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.

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

Virtual Gateways Consistency

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

163	IP subnets with two or more gateways and one virtual gateway with active endpoints or IP subnets with no active endpoints.
1079	IP subnets with zero virtual gateways or IP subnets with one physical gateway with less than

	20 active endpoints.
3	IP subnets with two or more virtual gateways or IP subnets with no virtual gateway with more than 20 active endpoints.

Widget - Quality of Service (QoS)

Queue Limit Size (packets)

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

103	QoS class with queue-limit size that is below 64 packets.
29	QoS classes with queue-limit size between 64 and 256 packets.
0	QoS classes with queue-limit size greater than 256 packets.

Shaping Queues Child Policy

Verifies the presence of child policy for shaping queues.

29	Shaping queues with child policy configured.
16	Shaping queues without any child policy configured.

QoS Random And Tail Drops

Verifies the number of Random drop packets and Tail drop packets for each Quality of Services (QoS) class.

0	QoS classes with no detected Random or Tail Drop packets.
0	QoS classes with Random Drops detected but with no Tail Drops detected.
0	QoS classes with Random and Tail Drops detected.
0	QoS classes with more than 10000 Random Drops and more than 1000 Tail Drops detected.

QoS Priority Queue Drops

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

29	QoS priority classes without any drops detected.
0	QoS priority classes with drops detected.

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.

29	Classes carrying Expedited Forwarding traffic with drop rate equal to 0
0	Classes carrying Expedited Forwarding traffic with drop rate greater than 0

Widget - Spanning-Tree Protocol (STP)

STP Virtual Port Status

Verifies the status of Spanning-Tree Protocol virtual ports.

9509	STP virtual ports with healthy status (Forwarding, Blocking, Disabled, Disarding).
95	STP virtual ports with unexpected status.
0	STP virtual ports with non-healthy or transit status (Broken, Learn, Listen).
0	STP virtual ports with non-healthy Discard status while in Designated state.

VLAN Names

Verification of VLAN Name configuration.

3352	VLANS with detected Name or Description.
15	VLANS without any detected Name or Description.

Switchport VLANs Without STP

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

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

VLAN status verification

Verification of VLAN active status on network devices with one or more VLANs configured.

2541	Active VLANs
736	System VLANs
10	Inactive VLANs

STP Ports with Multiple Neighbors

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

0	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.

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

SPT mode PVST or disabled

Display the list of hosts configured with PVST mode or where spanning tree is disabled.

7	STP disabled
8	SPT in PVST mode

STP Loops

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

6623	Spanning-Tree relationships with no loops detected.
0	Spanning-Tree relationships with loop detected.

Widget - Interfaces

Error-Disabled Interfaces (total)

Error disabled Interfaces.

0	Detected error-disabled Interfaces.

Edge-Ports with Multiple Neighbors

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

181	Non-trunk edge-ports with two or less mac-addresses detected.
0	Non-trunk edge-ports with 3-20 mac-addresses detected.
0	Non-trunk edge-ports with 20-100 mac-addresses detected.
0	Non-trunk edge-ports with more than 100 mac-addresses detected.

Interface Duplex

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

1091	Interfaces with the Link-Layer state 'UP' and 'FULL' duplex detected.
2660	Interfaces with the Link-Layer state 'UP' and no duplex detected.
135	Interfaces with the Link-Layer state 'UP' and duplex other than 'FULL' detected.

Edge Port Security

Verifies the security method applied to edge interfaces.

0	Edge switching interfaces with security method 802.1X applied.
0	Edge switching interfaces with 'unknown' security method.
249	Edge switching interfaces with security method other than 802.1X applied.

Interface Description

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

1330	Interfaces with configured description.
4699	Interfaces without configured description.

Maximum Transmission Unit (MTU)

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

1042	Transit links with consistent MTUs detected.
29	Transit links with missing MTU detected on either side.
8	Transit links with inconsistent MTUs detected.

Peer links Status

Checks MLAG Peer Link status across the network infrastructure.

0	Peer Link status is UP
2	Role is not primary nor secondary
0	Peer Link status is not UP

Interface Operational State

Verifies the administrative and operational state of the interfaces.

5977	Interfaces that are either administratively down or operating normally.
52	Interfaces with administrative state 'UP' and operational state is 'DOWN'.

Switched Port Analyzer (SPAN) ports (total))

Detects Switched Port Analyzer (SPAN) feature on discovered interfaces.

0	Interfaces with detected Switched Port Analyzer (SPAN) feature.

Juniper Cluster Link Status

Verifies state of control and fabric links in the cluster.

0	Control or Fabric links that are UP.
0	Control or Fabric links that are not UP.

Widget - Management Consistency

DHCP Snooping Enabled VLANs

Verifies if there are any enabled VLANs when DHCP Snooping is enabled.

17	Represents devices with enabled DHCP Snooping on any number of VLANs
1	Represents devices with enabled DHCP Snooping with no enabled VLANs.

DHCP Snooping Trusted Port

Verifies if there are any trusted ports when DHCP Snooping is enabled.

18	Represents devices with enabled DHCP Snooping with available trusted port.
0	

Devices with Telnet Access (total)

Detects network devices that allow access via Telnet.

399	

SNMP Community & ACL

Verifies Simple Network Management Protocol (SNMP) communities and related Access-List (ACL) configuration.

4	SNMP Communities with configured ACL.
423	SNMP Communities without configured ACL.

Remote System Logging Destination Port

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

431	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.
1	Destination syslog hosts with destination port other than 514 and within the well-known port range.

AAA Authentication Type

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

411	Lines with default AAA authentication method.
3	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.

0	Lines with no authentication method, allowing unauthenticated access.

NTP Configured Sources

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

10	Network devices with 2 or 3 configured NTP sources.
418	Network devices with only 1 or more than 3 configured NTP sources.
44	Network devices with 0 configured NTP sources.

NTP Stratum Level

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

374	NTP sources with Stratum value lower than 4.
1	NTP sources with Stratum value 4 or 5.
0	NTP sources with Stratum between 5 and 16.
56	Unsynchronized NTP sources with Stratum value 16.

NTP Time Offset

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

443	NTP sources with Time Offset less than 100ms.
0	NTP sources with Time Offset more than 100ms and less 500ms.
0	NTP sources with Time Offset more than 500ms and less 1000ms.
2	NTP sources with Time Offset more above 1000ms.

AAA Accounting Method

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

376	Records with any type of Accounting method except 'none' or 'unspecified'.
2	Records with the type of Accounting method 'none' or 'unspecified'.

Device Logging Configuration

Verifies Syslog server configuration for network devices.

414	Network devices with at least one remote and one local logging configured.
24	Network devices with no remote but at least one local logging configured.
34	Network devices with no remote and no local logging configured.

NTP Reachable Sources

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

369	Network devices with equal number of configured sources and reachable sources.
5	Network devices with at least 1 configured source and 1 reachable source.
44	Network devices with no configured source and no reachable source.
54	Network devices with at least 1 configured source and no reachable source.

Remote System Logging Severity

Verifies remote system logging severity for network devices.

429	Devices with remote syslog server configuration that do not have 'DEBUG' enabled.
5	Devices with remote syslog server configuration that have 'DEBUG' enabled.

Saved Config Consistency

Verifies saved configuration consistency for network devices.

0	Network devices with saved running configuration
472	Devices where check was not performed if the configuration was saved
0	Network devices with unsaved configuration, having different running and startup configurations.

AAA Authentication Method

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

830	Records with any type of Authentication method except 'none' or 'unspecified'.
407	Records with the type of Authentication method 'none' or 'unspecified'.

DHCP Snooping Dropped Packets

Verifies the total number of dropped packets compared to total packets.

18	Represents devices with enabled DHCP Snooping without dropped packets detected.
0	Represents devices with enabled DHCP Snooping with dropped packets detected.

Local System Logging Severity

Verifies local system logging severity for network devices.

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

AAA Authorization Method

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

411	Records with any type of Authorization method except 'none' or 'unspecified'.
2	Records with the type of Authorization method 'none' or 'unspecified'.

SNMP Community Name

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

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

DHCP Binding session expiration

Verifies the expiration time for DHCP bindings. Most of the implementations try to renew a leased IP address after reaching half of the timeout.

0	Represents DHCP binding session with session expiration time greater than 300 seconds.
2	Represents DHCP binding session with session expiration time within 300 and 180 seconds, or unknown.
0	Represents DHCP binding session with session expiration time within 180 and 60 seconds.
0	Represents DHCP binding session with session expiration time less than 60 seconds.

NTP Network Round-Trip Time

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

443	NTP sources with Round Trip Time lower than 50ms.
0	NTP sources with Round Trip Time value within 50-100ms.
2	NTP sources with Round Trip Time value within 100-500ms.
0	NTP sources with Round Trip Time value above 500ms.

SNMP Configuration Compliance

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

6	Devices with at least one configured SNMP user and with at least one configured SNMP community.
314	Devices with at least one configured SNMP user or with at least one configured SNMP community.
152	Devices with no SNMP user and no SNMP community configured.

Widget - Security

IPSec Tunnel Encryption

The verification of the encryption strength of IPSec tunnels.

8	IPSec tunnels with secure/strong encryption algorithms.
1	IPSec tunnels with insecure/weak encryption algorithm.

IPSec Gateway Encryption

The verification of the encryption strength of IPSec gateways.

11	IPSec gateways with secure/strong encryption algorithms.
1	IPSec gateways with insecure/weak encryption algorithm.

IPSec Tunnel Status

The overall status of the IPSec tunnels.

9	IPSec tunnels that are in UP status.
9	IPSec tunnels that are in DOWN status.

DMVPN Tunnel State

Verifies the operational state of Dynamic Multipoint VPN (DMVPN) tunnels.

4	DMVPN tunnels that are in the 'UP' state.
0	DMVPN tunnels that are in other than the 'UP' state.

IPSec Tunnel Authentication

The verification of authentication of IPSec tunnels.

5	IPSec tunnels with strong authentication
3	IPSec tunnels with weak authentication

Edge Port Security

Verifies the security method applied to edge interfaces.

0	Edge switching interfaces with security method 802.1X applied.
0	Edge switching interfaces with 'unknown' security method.
249	Edge switching interfaces with security method other than 802.1X applied.

IPSec Gateway Authentication

The verification of authentication of IPSec gateways.

11	IPSec gateways with strong authentication
1	IPSec gateways with weak authentication

IPSec Gateway Status

The overall status of the IPSec gateways.

12	IPSec gateways that are in UP status.
3	IPSec gateways that are in DOWN status.

Widget - Endpoints

IP Phone - Connected MACs

Verifies the number of Media Access Control (MAC) addresses detected behind each IP phone, signifying users connected to the phone.

0	IP phones with a single MAC address connected behind the phone.
0	IP phones with multiple MAC addresses connected behind the phone.

Endpoints Resolution

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

1271	The total number of MAC addresses that have assigned IP Address information.
0	The total number of MAC addresses that have not assigned any IP Address information.

Widget - Stability

BGP Session Age

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

185	BGP sessions with uptime greater than one month.
6	BGP sessions with uptime between one month and one week.
9	BGP sessions with uptime between one week and one day.
33	BGP sessions with uptime less than 24 hours.

DMVPN Tunnel State

Verifies the operational state of Dynamic Multipoint VPN (DMVPN) tunnels.

4	DMVPN tunnels that are in the 'UP' state.
0	DMVPN tunnels that are in other than the 'UP' state.

PIM Session Age

Verifies Protocol Independent Multicast (PIM) session age time against predefined compliance thresholds.

23	PIM sessions with uptime greater than one month.
0	PIM sessions with uptime between one month and one week.
0	PIM sessions with uptime between one week and one day.
0	PIM sessions with uptime less than 24 hours.

IS-IS Session Age

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

27	IS-IS sessions with uptime greater than one month.
0	IS-IS sessions with uptime between one month and one week.
0	IS-IS sessions with uptime between one week and one day.
0	IS-IS sessions with uptime less than 24 hours.

EIGRP Session Age

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

14	EIGRP sessions with uptime greater than one month.
0	EIGRP sessions with uptime between one month and one week.
0	EIGRP sessions with uptime between one week and one day.

0	EIGRP sessions with uptime less than 24 hours.

Device Reload Reason

Device reload reason verification

436	Reload occurred more than 3 months ago
1	Reload reason contains failure and occurred in the past 3 months
0	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
0	Reload reason contains failure that was not due to a power issue or miscellaneous reason and occurred within the past 24 hours

Recent Route Convergence

Detects recent route convergence.

4292	Routes with acceptable convergence.
29	With more than 30% of route occurrences that converged between past 4 hours to 24 hours.
4	With more than 30% of route occurrences that converged between past 15 mins to 4 hours.
1	With more than 30% of route occurrences that converged in the past 15 mins.

LDP Session Age

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

136	LDP sessions with uptime greater than one month.
0	LDP sessions with uptime between one month and one week.
0	LDP sessions with uptime between one week and one day.
0	LDP 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.

8	OSPFv3 sessions with uptime greater than one month.
16	OSPFv3 sessions with uptime between one month and one week.
0	OSPFv3 sessions with uptime between one week and one day.
0	OSPFv3 sessions with uptime less than 24 hours.

Device Uptime

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

469	Devices with uptime longer than 1 week and less than 3 years
0	Devices running for more than 3 years
2	Devices with uptime less than one week
1	Devices with uptime less than one day

Stack Members Uptime

Device uptime verification. Verifies that the stack member's continuous running time is within the expected thresholds.

2	Stack member with uptime longer than 1 week and less than 3 years
0	Stack members running for more than 3 years
0	Stack member with uptime less than one week
0	Stack members with uptime less than one day

SDWAN Sites Uptime

SDWAN Site uptime verification.

0	Sites with uptime longer than 1 week and less than 3 years
0	Sites running for more than 1 year
0	Sites with uptime less than one week
0	Sites with uptime less than one day

OSPF Session Age

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

830	OSPF sessions with uptime greater than one month.
26	OSPF sessions with uptime between one month and one week.
5	OSPF sessions with uptime between one week and one day.
66	OSPF sessions with uptime less than 24 hours.

Widget - IP Addressing compliance

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.

5500	Address Resolution Protocol records without Proxy ARP detected.
11	Address Resolution Protocol records with Proxy ARP detected.

Managed IP Address DNS Consistency

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

2371	Network devices with matching hostname with DNS and also the A/CNAME record.
6	Network devices with no matching hostname with DNS or the A/CNAME record.
5	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.

11	Duplicate IP addresses with 2 occurrences.
6	Duplicate IP addresses with more than 2 occurrences.

MAC Address Source

Identifies Media Access Control (MAC) address source.

13776	Media Access Control records with an expected dynamic sources (learn, dynamic, evpn, d, dl, dlr).
37	Media Access Control records from unexpected source.
36	Media Access Control records with source 'static' or 'self'.

Widget - Performance

Output drops impact

Verifies impact value for output drops on individual interfaces.

3327	Interfaces with 'Output Drops Impact' value equal to zero.
4	Interfaces with 'Output Drops Impact' value between 1 and 5.
3	Interfaces with 'Output Drops Impact' value between 5 and 10.
0	Interfaces with 'Output Drops Impact' value greater than 10.

Transfer Rates (inbound)

Verifies impact value for inbound transfer data rates on interfaces.

3424	Interfaces with 'Inbound Loss Impact' value equal to zero.
15	Interfaces with 'Inbound Loss Impact' value between 1 and 5.
0	Interfaces with 'Inbound Loss Impact' value between 5 and 10.
0	Interfaces with 'Inbound Loss Impact' value greater than 10.

Transfer Rates (device-outbound)

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

462	Devices with 'Outbound Loss Impact' value equal to zero.
4	Devices with 'Outbound Loss Impact' value between 1 and 5.
4	Devices with 'Outbound Loss Impact' value between 5 and 10.
0	Devices with 'Outbound Loss Impact' value greater than 10.

Transfer Rates (outbound)

Verifies impact value for outbound transfer data rates on interfaces.

3429	Interfaces with 'Outbound Loss Impact' value equal to zero.
6	Interfaces with 'Outbound Loss Impact' value between 1 and 5.
4	Interfaces with 'Outbound Loss Impact' value between 5 and 10.
0	Interfaces with 'Outbound Loss Impact' value greater than 10.

Output errors impact

Verifies impact value for output errors on individual interfaces.

3331	Interfaces where 'Output Errors Impact' value equal to zero.
2	Interfaces with 'Output Errors Impact' value between 1 and 5.
1	Interfaces with 'Output Errors Impact' value between 5 and 10.
0	Interfaces with 'Output Errors Impact' value greater than 10.

Drop Rates (device-bidirectional)

Verifies impact value for bidirectional drops per network device.

462	Devices with 'Bidirectional Drops Impact' value equal to zero.
5	Devices with 'Bidirectional Drops Impact' value between 1 and 5.
3	Devices with 'Bidirectional Drops Impact' value between 5 and 10.
0	Devices with 'Bidirectional Drops Impact' value greater than 10.

Error Rates (device-bidirectional)

Verifies impact value for bidirectional errors on individual interfaces.

459	Interfaces with 'Bidirectional Errors Impact' value equal to zero.
10	Interfaces with 'Bidirectional Errors Impact' value between 1 and 5.
1	Interfaces with 'Bidirectional Errors Impact' value between 5 and 10.
0	Interfaces with 'Bidirectional Errors Impact' value greater than 10.

MRoute RPF Errors

Detecting Reverse Path Forwarding errors increase between two latest snapshots.

12	MRoutes without any detected errors per seconds compared to previous discovery records.
4	MRoutes with detected errors per seconds compared to previous discovery records.

Device output errors impact

Verifies impact value for output errors per network device.

469	Devices with 'Output Errors Impact' value equal to zero.
0	Devices with 'Output Errors Impact' value between 1 and 5.
1	Devices with 'Output Errors Impact' value between 5 and 10.
0	Devices with 'Output Errors Impact' value greater than 10.

Device output drops impact

Verifies impact value for output drops per network device.

463	Devices with 'Output Drops Impact' value equal to zero.
4	Devices with 'Output Drops Impact' value between 1 and 5.
3	Devices with 'Output Drops Impact' value between 5 and 10.
0	Devices with 'Output Drops Impact' value greater than 10.

Access Point - Signal-to-Noise Ratio (SNR)

Verifies the average Signal To Noise Ratio (SNR) value for each access point (AP).

0	Access points with average SNR greater than 25 for APs with at least one client.
0	Access points with average SNR within 25 and 15 for APs with at least one client.
0	Access points with average SNR within 15 and 10 for APs with at least one client.
0	Access points with average SNR lower than 10 for APs with at least one client.

Error Rates (bidirectional)

Verifies impact value for bidirectional errors on individual interfaces.

3316	Interfaces with 'Bidirectional Errors Impact' value equal to zero.
17	Interfaces with 'Bidirectional Errors Impact' value between 1 and 5.
1	Interfaces with 'Bidirectional Errors Impact' value between 5 and 10.
0	Interfaces with 'Bidirectional Errors Impact' value greater than 10.

Wireless Client - RSSI

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

0	Connected clients with Signal Strength (dBm) greater than -60.
0	Connected clients with Signal Strength (dBm) within -60 and -67.
0	Connected clients with Signal Strength (dBm) within -67 and -80.
0	Connected clients with Signal Strength (dBm) lower than -80.

Drop Rates (bidirectional)

Verifies impact value for bidirectional drops on individual interfaces.

3326	Interfaces with 'Bidirectional Drops Impact' value equal to zero.
5	Interfaces with 'Bidirectional Drops Impact' value between 1 and 5.
3	Interfaces with 'Bidirectional Drops Impact' value between 5 and 10.
0	Interfaces with 'Bidirectional Drops Impact' value greater than 10.

Wireless Client - SNR

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

0	Connected clients with SNR greater than 25.
0	Connected clients with SNR within 25 and 15.
0	Connected clients with SNR within 15 and 10.
0	Connected clients with SNR lower than 10.

End-to-End Path Flooding

Verifies whether End-to-End paths have MAC flooding.

0	End-to-End paths without any MAC flooding detected.
0	End-to-End paths with MAC flooding detected.

Access Point - Radio Signal Impact

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

0	Access points zero impact value.
0	Access points with the impact value within 1 and 6.
0	Access points with the impact value within 6 and 10.
0	Access points with the impact value greater than 10.

End-to-End Path Verification

Verifies End-to-End path's result against the predefined expected state.

0	End-to-End path verifications that are in an expected state (OK or FAIL)
0	End-to-End path verifications that are in the 'ERROR' state.
0	End-to-End path verifications that are not in an expected state (OK or FAIL)

Input errors impact

Verifies impact value for input errors on individual interfaces.

3319	Interfaces with 'Input Errors Impact' value equal to zero.
15	Interfaces with 'Input Errors Impact' value between 1 and 5.
0	Interfaces with 'Input Errors Impact' value between 5 and 10.
0	Interfaces with 'Input Errors Impact' value greater than 10.

Input drops impact

Verifies impact value for input drops on individual interfaces.

3333	Interfaces with 'Input Drops Impact' value equal to zero.
1	Interfaces with 'Input Drops Impact' value between 1 and 5.
0	Interfaces with 'Input Drops Impact' value between 5 and 10.
0	Interfaces with 'Input Drops Impact' value greater than 10.

Transfer Rates (device-inbound)

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

460	Devices with 'Inbound Loss Impact' value equal to zero.
10	Devices with 'Inbound Loss Impact' value between 1 and 5.
0	Devices with 'Inbound Loss Impact' value between 5 and 10.
0	Devices with 'Inbound Loss Impact' value greater than 10.

Device input errors impact

Verifies impact value for input errors per network device.

460	Devices with 'Input Errors Impact' value equal to zero.
10	Devices with 'Input Errors Impact' value between 1 and 5.
0	Devices with 'Input Errors Impact' value between 5 and 10.
0	Devices with 'Input Errors Impact' value greater than 10.

Port-Channel Output Balancing Variance

Verifies output balancing variance for aggregated interfaces.

57	Aggregated interfaces with output balancing variance lower than 500.
13	Aggregated interfaces with output balancing variance higher than 500 and Rate below 30Mbps.
0	Aggregated interfaces with output balancing variance higher than 500 and Rate above 30Mbps.
0	Aggregated interfaces with output balancing variance greater than 500 and Rate above 1000Mbps.

Transfer Rates (bidirectional)

Verifies impact value for bidirectional transfer data rates on interfaces.

3416	Interfaces with 'Bidirectional Loss Impact' value equal to zero.
19	Interfaces with 'Bidirectional Loss Impact' value between 1 and 5.
4	Interfaces with 'Bidirectional Loss Impact' value between 5 and 10.
0	Interfaces with 'Bidirectional Loss Impact' value greater than 10.

Device input drops impact

Verifies impact value for input drops per network device.

469	Devices with Input Drops Impact' value equal to zero.
1	Devices with 'Input Drops Impact' value between 1 and 5.
0	Devices with 'Input Drops Impact' value between 5 and 10.
0	Devices with 'Input Drops Impact' value greater than 10.

Port-Channel Input Balancing Variance

Verifies input balancing variance value for aggregated interfaces.

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

0	Aggregated interfaces with input balancing variance higher than 500 and Rate above 30Mbps.
0	Aggregated interfaces with input balancing variance greater than 500 and Rate above 1000Mbps.

Access Point - Connected Clients

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

0	Access points with less than 50 clients connected.
0	Access points with within 50 and 80 clients connected.
0	Access points with within 80 and 100 clients connected.
0	Access points with more than 100 clients connected.

Transfer Rates (device-bidirectional)

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

454	Devices with 'Bidirectional Loss Impact' value equal to zero.
12	Devices with 'Bidirectional Loss Impact' value between 1 and 5.
4	Devices with 'Bidirectional Loss Impact' value between 5 and 10.
0	Devices with 'Bidirectional Loss Impact' value greater than 10.

MRoute Other Errors

Detecting Other errors increase between two latest snapshots.

9	MRoutes without any detected errors per seconds compared to previous discovery records. (TTL, Empty OIL, Encap, Other)
0	MRoutes with detected errors per seconds compared to previous discovery records. (TTL, Empty OIL, Encap, Other)

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.

29	Classes carrying Expedited Forwarding traffic with drop rate equal to 0
0	Classes carrying Expedited Forwarding traffic with drop rate greater than 0

Widget - Operating System (OS)

Operating System Version (%)

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

35	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.
7	Platforms with the same operating system, that is installed within 20% and 10% of the platform.
4	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.

40	Network devices with non-unique installed operating system.
8	Network devices with unique installed operating system.

Devices with Unique Platform

Detects network devices with unique platforms.

27	Network devices with non-unique platform.
21	Network devices with unique platform.

Widget - Inventory

End of Support Detail

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.

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

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.

0	Part numbers that have not passed the End of Sale date.
12	Part numbers that have passed the End of Sale date.

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.

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

Device Reload Reason

Device reload reason verification

436	Reload occurred more than 3 months ago
1	Reload reason contains failure and occurred in the past 3 months
0	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
0	Reload reason contains failure that was not due to a power issue or miscellaneous reason and occurred within the past 24 hours

SFP Modules (total)

Detected small form-factor pluggable (SFP) modules.

0	Detected small form-factor pluggable (SFP) modules.

End of Sale Detail

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

0	Part numbers that have not passed the End of Sale date.
17	Part numbers that have passed the End of Sale date.

End of Maintenance

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

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

Software Configuration Register

Boot configuration register verification.

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

Device Memory Usage (%)

Memory utilization verification according to thresholds.

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

End of Maintenance Detail

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

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

Device Uptime

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

469	Devices with uptime longer than 1 week and less than 3 years
0	Devices running for more than 3 years
2	Devices with uptime less than one week
1	Devices with uptime less than one day

Stack Members Uptime

Device uptime verification. Verifies that the stack member's continuous running time is within the expected thresholds.

2	Stack member with uptime longer than 1 week and less than 3 years
0	Stack members running for more than 3 years
0	Stack member with uptime less than one week
0	Stack members with uptime less than one day

Widget - Neighborship compliance

CDP/LLDP unidirectional

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

9	Unidirectional CDP or LLDP sessions.

BGP Neighbor State

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

206	BGP sessions in ESTABLISHED state.
0	BGP sessions in other than expected state.
8	BGP sessions in a transitive state (OPENSENT, OPENCONFIRM, IDLE, CONNECT).
19	BGP sessions in ACTIVE state.

STP Neighborship Expected State

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

6623	Spanning-Tree neighbors with expected port role states on each side of a shared link (designated-alternate, root-designated).
0	Spanning-Tree neighbors with other than expected port role states on each side of shared link.

Trunk Allowed VLAN Mismatch

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

0	Trunk links with equal number of allowed VLANs detected at each end.
40	Trunk links with unequal number of allowed VLANs detected at each end.

LDP Interface Neighbors

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

131	LDP enabled interfaces with one or more neighbors detected.
14	LDP enabled interfaces with zero neighbors detected.

Port-Channel Members State

Verifies membership state of aggregated interfaces across the network infrastructure.

39	Aggregated interfaces with healthy membership status 'UP', 'Collecting Distributing, '(P)', '(A)' or 'SELECTED'.
24	Aggregated interfaces with other than expected membership status.
7	Aggregated interfaces with membership status '(S)', '(F)', or '(I)'.

BGP Received Prefixes

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

198	Established BGP sessions with one or more received prefixes.
24	Non-established BGP sessions with no received prefixes.
11	Established BGP sessions with no received prefixes.

OSPF Neighbor State

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

904	OSPF neighbors with healthy state (FULL, 2WAY, ATTEMPT).
0	OSPF neighbors with other than expected state.
13	OSPF neighbors with transitive state (EXCHANGE, EXSTART, INIT, LOADING).
10	OSPF neighbors that are currently down.

OSPF Cost Consistency

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

594	OSPF sessions with equal local and neighbor cost.
0	OSPF sessions with maximized local and neighbor cost (65535).
333	OSPF sessions with unequal local and neighbor cost.

OSPFv3 Neighbor State

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

24	OSPFv3 neighbors with healthy state (FULL, 2WAY, ATTEMPT).
0	OSPFv3 neighbors with other than expected state.
0	OSPFv3 neighbors with transitive state (EXCHANGE, EXSTART, INIT, LOADING).
0	OSPFv3 neighbors that are currently down.

OSPFv3 Cost Consistency

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

4	OSPFv3 sessions with equal local and neighbor cost.
0	OSPFv3 sessions with maximized local and neighbor cost (65535).
20	OSPFv3 sessions with unequal local and neighbor cost.

OSPF Interface Neighbors

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

793	OSPF enabled interfaces with one or more neighbors detected.
603	OSPF enabled interfaces with zero neighbors detected.

RIP Interface Neighbors

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

0	RIP interfaces with one or more neighbors detected.
19	RIP interfaces with zero neighbors detected.

IS-IS Interface Neighbors

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

26	IS-IS enabled interfaces with one or more neighbors detected.
20	IS-IS enabled interfaces with zero neighbors detected.

PIM Interfaces Neighbors

Verifies the number of Protocol Independent Multicast (PIM) sessions for PIM enabled interfaces.

23	PIM enabled interfaces with one or more neighbors detected.
21	PIM enabled interfaces with zero neighbors detected.

CDP/LLDP Neighbor State

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

1035	Managed CDP or LLDP neighbors.
190	Unmanaged CDP or LLDP neighbors.

Duplex Mismatch or Missing

Detects mismatched or missing duplex information.

113	Links with missing duplex information.
4	Links with mismatched duplex.

Unmanaged Neighbors

Verifies protocol type for the unmanaged neighbor.

113	Unmanaged neighbors detected with BGP protocol.
31	
551	Unmanaged neighbors detected with interior gateway protocols.

169	Unmanaged neighbors detected with discovery protocols.

Discovery Protocol Loops

Detects discovery protocol loops.

1225	Discovery protocol neighbors with no loop detected.
0	Local Hostname equals the Remote Neighbor column.
0	Local Hostname and Interfaces match remote Neighbor and Interface.

OSPFv3 Interface Neighbors

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

24	OSPFv3 enabled interfaces with one or more neighbors detected.
14	OSPFv3 enabled interfaces with zero neighbors detected.

STP/CDP Neighbor Information Mismatch

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

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

EIGRP Interface Neighbors

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

14	EIGRP interfaces with one or more neighbors detected.
15	EIGRP interfaces with zero neighbors detected.

Widget - Environment

Stack Port State

Verifies the operational state of all discovered stack interfaces.

2	Stack interfaces that are operational, 'OK' detected status.
0	Represents stack interfaces with other than 'OK' or 'DOWN' detected operational status.
2	Stack interfaces that are not operational, 'DOWN' detected status.

Module State

Verifies the operational state of other discovered modules.

0	Modules that are in healthy state (powered-up).
0	Modules that are neither in expected healthy state nor in the fail state.
0	Modules that are in faulty state (err).

Power-Supply State

Verifies the operational state of power-supply modules.

15	Power-supplies that are in healthy state (ok, good, normal, online).
10	Power-supplies that are neither in expected healthy state nor in the fail state.
0	Power-supplies that are not in healthy state (fail, fault, present).

PoE Module Watts Used (%)

Verifies the Watts Used (%) per hardware module.

1	Watts used per hardware module is below 60% of its capacity.
0	Watts used per hardware module is above 60% of its capacity.
0	Watts used per hardware module is above 80% of its capacity.
0	Watts used per hardware module is above 95% of its capacity.

Power-Supply Fan State

Verifies the operational state of power-supply fan modules.

0	Power-supply fans that are in healthy state (ok, good, normal, running successfully).
8	Power-supply fans that are neither in expected healthy state nor in the fail state.
0	Power-supply fans that are not in healthy state (fail, fault).

Fan Module State

Verifies the operational state of fan modules.

16	Fan modules that are in healthy state (ok, good, normal, running successfully).
2	Fan modules that are neither in expected healthy state nor in the fail state.
0	Fan modules that are in faulty state (fail, fault).

PoE Interface State

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

7	Interfaces that are distributing power over ethernet and are operational (ON).
17	Interfaces that are capable of distributing power over ethernet and are not operational (OFF).
0	Interfaces that are capable of distributing power over ethernet and have faulty operational status (FAULT, ERROR).

Widget - MPLS Pseudo-wires

PTMP VPLS State

Verifies the Virtual Private LAN Service (VPLS) circuit state.

12	VPLS circuit's state is UP
2	VPLS circuit's state is DOWN

All Pseudowires state

Verifies the all pseudowire circuit's state.

23	Pseudowire state is UP
8	Pseudowire state is DOWN

PTP VPWS State

Verifies the virtual private wire service (VPWS) circuit state

9	VPWS circuit's state is UP
5	VPWS circuit's state is DOWN

CCC state

Verifies the Circuit Cross-Connect (CCC) circuit state.

2	CCC circuit's state is UP
1	CCC circuit's state is UP