Infoblox
CONTROL YOUR NETWORK

Use Case: Network Issues

Use Case | October, 2013

Monitoring, detection, and reporting of network issues

Overview

Network Automation issue monitoring, detection, and report allows you to be proactive in resolving problems on your network. Being reactive to an issue costs more time and money than being proactive to an issue.

Current Situation

If you had no network management system, you would be notified of a network problem by a user. Now you are in reactive network troubleshooting mode. First, you would have to track down the source of the problem and then fix it. If you had a NMS, it would report issues based upon SNMP traps. Not all issues are reported via SNMP traps.

Infoblox Network Automation Solution

Network Automation not only looks at SNMP traps to generate issues, but also examines the configuration files of discovered devices to uncover potential problems. This examination would be done on a four hour basis until the issue was addressed or suppressed. The system classifies issues in three severity levels:

- Errors are important issues that may affect the smooth operation of the network. Generally, such issues are clear signs that something is wrong.
- Warnings are intermediate level issues that should be addressed after the errors have been corrected. A warning may not be a real problem, depending on the design and operation of the network.
- Info issues are provided for information, and typically alert you to minor things that may or may not indicate a problem.

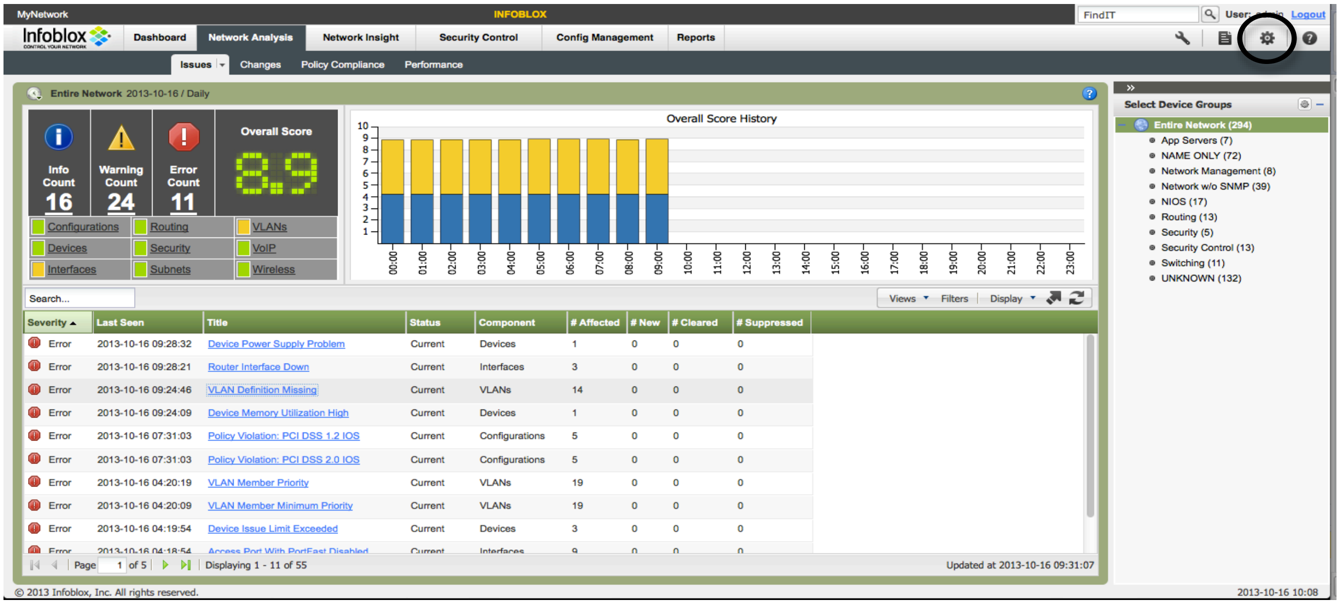
They can range from a port going down, device misconfiguration, HSRP problems, to an entire device going down. See appendix A for the list of issues. Issues are listed on the front screen, on the device viewer, or in a report.

Use Case

In a large enterprise or service provider environment, it is a best practice to assign each network engineer and/or network operator to a specific portion of the network. In a large organization, everybody does not need to see every issue with every device. Most likely, the network support staff are grouped by function, devices, and/or region. This allows the appropriate staff to address issues within their work responsibilities. Here are the steps:

Use Case: Network Issues

Use Case | October, 2013



🟩 Configurations	🟩 Routing	🟨 VLANs
🟩 Devices	🟩 Security	🟩 VoIP
🟨 Interfaces	🟩 Subnets	🟩 Wireless

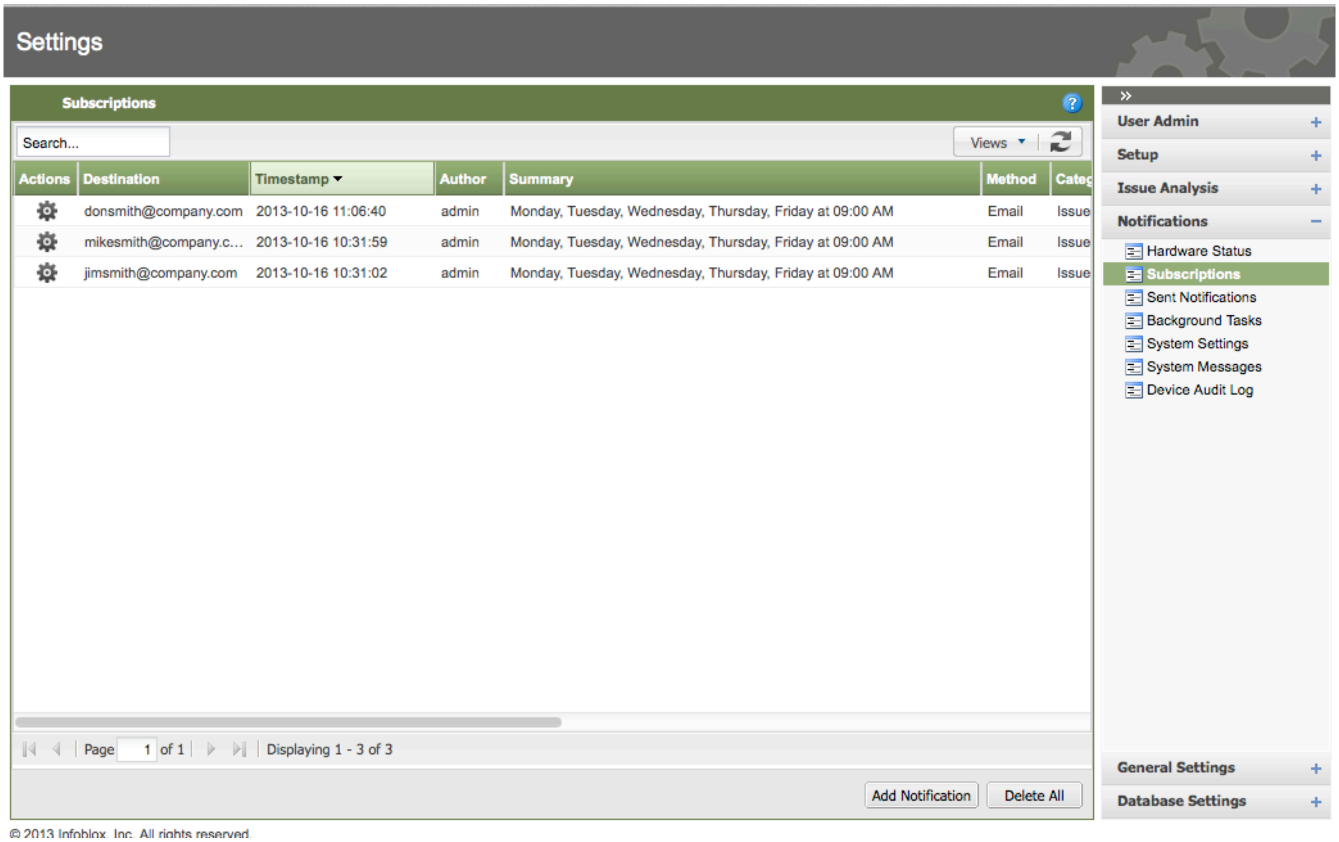
Severity ▲	Last Seen	Title	Status	Component	# Affected	# New	# Cleared	# Suppressed
Error	2013-10-16 09:28:32	Device Power Supply Problem	Current	Devices	1	0	0	0
Error	2013-10-16 09:28:21	Router Interface Down	Current	Interfaces	3	0	0	0
Error	2013-10-16 09:24:46	VLAN Definition Missing	Current	VLANs	14	0	0	0
Error	2013-10-16 09:24:09	Device Memory Utilization High	Current	Devices	1	0	0	0
Error	2013-10-16 07:31:03	Policy Violation: PCI DSS 1.2 IOS	Current	Configurations	5	0	0	0
Error	2013-10-16 07:31:03	Policy Violation: PCI DSS 2.0 IOS	Current	Configurations	5	0	0	0
Error	2013-10-16 04:20:19	VLAN Member Priority	Current	VLANs	19	0	0	0
Error	2013-10-16 04:20:09	VLAN Member Minimum Priority	Current	VLANs	19	0	0	0
Error	2013-10-16 04:19:54	Device Issue Limit Exceeded	Current	Devices	3	0	0	0
Error	2013-10-16 04:18:54	Access Port With PortFast Disabled	Current	Interfaces	9	0	0	0

Page 1 of 5 | Displaying 1 - 11 of 55 — Updated at 2013-10-16 09:31:07

- Entire Network (294)
  - App Servers (7)
  - NAME ONLY (72)
  - Network Management (8)
  - Network w/o SNMP (39)
  - NIOS (17)
  - Routing (13)
  - Security (5)
  - Security Control (13)
  - Switching (11)
  - UNKNOWN (132)

© 2013 Infoblox, Inc. All rights reserved. 2013-10-16 10:08

1. Log into Network Automation.
2. In the upper right corner of the screen, click on the settings button which is highlighted in the circle.

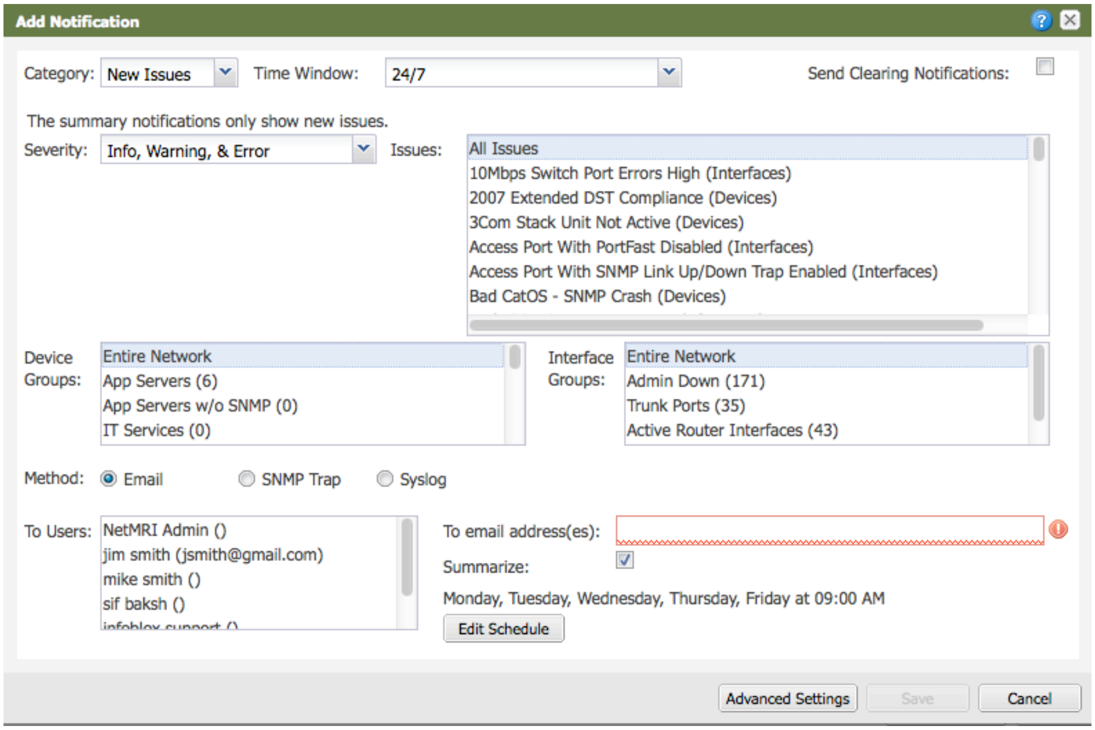


Actions	Destination	Timestamp ▾	Author	Summary	Method	Categ
⚙	donsmith@company.com	2013-10-16 11:06:40	admin	Monday, Tuesday, Wednesday, Thursday, Friday at 09:00 AM	Email	Issue
⚙	mikesmith@company.c...	2013-10-16 10:31:59	admin	Monday, Tuesday, Wednesday, Thursday, Friday at 09:00 AM	Email	Issue
⚙	jimsmith@company.com	2013-10-16 10:31:02	admin	Monday, Tuesday, Wednesday, Thursday, Friday at 09:00 AM	Email	Issue

Page 1 of 1 | Displaying 1 - 3 of 3

© 2013 Infoblox, Inc. All rights reserved.

3. Click on Notifications -> Subscriptions.
4. Click on the Add Notification button to assign network support staff to specific or groups of issues.



Add Notification

Category: New Issues
Time Window: 24/7
Send Clearing Notifications: □

The summary notifications only show new issues.

Severity: Info, Warning, & Error

Issues:
All Issues
10Mbps Switch Port Errors High (Interfaces)
2007 Extended DST Compliance (Devices)
3Com Stack Unit Not Active (Devices)
Access Port With PortFast Disabled (Interfaces)
Access Port With SNMP Link Up/Down Trap Enabled (Interfaces)
Bad CatOS - SNMP Crash (Devices)

Device Groups:
Entire Network
App Servers (6)
App Servers w/o SNMP (0)
IT Services (0)

Interface Groups:
Entire Network
Admin Down (171)
Trunk Ports (35)
Active Router Interfaces (43)

Method: ● Email ○ SNMP Trap ○ Syslog

To Users:
NetMRI Admin ()
jim smith (jsmith@gmail.com)
mike smith ()
sif baksh ()
infoblox support ()

To email address(es):

Summarize: ☑

Monday, Tuesday, Wednesday, Thursday, Friday at 09:00 AM

5. Select a category. They are:
   - New Issues-notify when an issue occurs
   - Change-notify when a device configuration changes and device status changes
   - Job-notify when a job completes and job approval status
   - System Alert-notify when the Network Automation appliance has a maintenance event, software updates, reboots, and general appliance errors.
6. Select the time window. This setting determines when an issue notification is sent. The choices are:
   - 24/7
   - Work Hours (M-F 8am-6pm)
   - Off Hours (M-F 6pm-8am, Sat, Sun)
   - First Shift (M-F 12am-8am)
   - Second Shift (M-F 8am-4pm)
   - Third Shift (M-F 4pm-12am)
   - Weekends (Sat/Sun)
7. Select the Severity. This setting determines the level of severity of the issues sent to the user. The choices are:
   - Info, Warning, & Error
   - Warning and Error
   - Error
8. Select the Issue(s) to be sent to the user. You can select one or more issues to be sent.
9. Select the device groups and interface groups.
10. Enter the email address of the user that will receive the alerts.
11. Optionally, edit the schedule to control the days that the issue notifications are sent.
12. Click save to save the subscription.

After this configuration is done, the selected network engineers or selected network operators will get notifications of types of issues and at the times that they are on shift.

Appendix A

Configuration Related

Config Activity (Error)

Lists all devices found to have a large amount of configuration activities in the prior 24-hour period. The default threshold is 6 configuration activities. This issue is only relevant for Cisco devices that the system is NOT successfully retrieving configuration files for and relies on the Cisco ccmHistory SNMP variables. For Cisco devices that the system is successfully retrieving configuration files for the Config Difference Issue will fire instead.

Config Activity (Warning)

Lists all devices found to have a higher than normal amount of configuration activities in the prior 24-hour period. The default threshold is 3-5 configuration activities. This issue is only relevant for Cisco Devices that the system is NOT successfully retrieving configuration files for and relies on the Cisco ccmHistory SNMP variables. For Cisco devices that the system is successfully retrieving configuration files for the Config Difference Issue will fire instead.

Config Activity (Info)

Lists all devices found to have configuration activities in the prior 24-hour period. The default threshold is 1-2 configuration activities.

This issue is only relevant for Cisco Devices that the system is NOT successfully retrieving configuration files for and relies on the Cisco ccmHistory SNMP variables. For Cisco devices that the system is successfully retrieving configuration files for the Config Difference Issue will fire instead

Config Bad Password (Warning)

The following devices have either weak or unknown Telnet or SSH passwords or have no enable password. Weak passwords represent a security problem and unknown passwords prevent configuration file processing for those devices.

Config Collection Disabled (Info)

The following devices currently have config file collection disabled, because both the Telnet and SSH collectors are disabled for these devices. When config file collection is disabled for a device, no config files will be gathered from the device, and therefore, no config file analysis will be performed. To enable config file collection for a device group, go to Settings -> Setup -> Collectors and Groups -> Groups -> Device Groups. To enable config file collection for all devices, go to Settings -> Setup -> Collectors and Groups -> Global.

Config Difference (Error)

This issue lists all devices for which configuration collection is enabled for which 6 or more differences were found between the previously collected configuration and the current configuration or 6 or more differences exist between the running and saved configurations.

Config Difference (Warning)

This issue lists all devices for which configuration collection is enabled for which 3 or more differences were found between the previously collected configuration and the current configuration or 3 or more differences exist between the running and saved configurations.

Config Difference (Info)

This issue lists all devices for which configuration collection is enabled for which a difference was found between the previously collected configuration and the current configuration or a difference exists between the running and saved configurations.

Config Policy Failure (Error)

The following devices experienced one or more configuration policy failures during a 24 hour period. Please see the Details page for more information

Config Retrieval Error (Error)

The following devices experienced one or more config file retrieval errors during a 24-hour period. Please see the Device Viewer Config Errors page for details on why the config file retrieval failed.

Config Running Not Saved (Info)

Lists all routers and switches that have running configurations that have been changed, but that have not been saved to NVRAM. If such a device reboots, the current configuration will be lost, possibly including changes that were assumed to be permanent. This issue only relevant for Cisco Devices that the system is NOT successfully retrieving configuration files for and relies on the Cisco ccmHistory SNMP variables or if config files are being collected. Those config files indicate that there is a difference between the running and saved config. Devices which ARE successfully have successfully retrieved configs and indicate a difference between the running and saved configs will also generate this issue.

Configuration Command Script Failure (Error)

The following devices experienced one or more configuration command script failures in the prior 24-hour period.

Vendor Defaults Found (Warning)

This issue is raised when a device configured with vendor default passwords is found. Depending on the schedule this may be during the previous day or previous week. A standard network attack method is to use these usernames/passwords to gain entry to your network device. They should be changed to a more secure (non-vendor) username/password. For SNMP community strings and telnet line passwords, there are no usernames used. Since username is not appropriate for telnet line passwords and SNMP community strings, the usernames will be blank. For security reasons, the passwords are not shown here. To see the full list of default username/password credentials found, log in with SysAdmin privilege and go to Reports - Change and Config - Default Credentials Report.

Device Related

3Com Stack Unit Not Active (Warning)

The following 3Com stack units were found to be inactive.

Bare Metal Device Found (Info)

The devices shown have been discovered with the sysName autoconfig. These devices may be provisioned if a triggered job for this issue is approved.

CDP Neighbor Changed (Warning)

The following devices had a CDP neighbor change with a network device during the previous 24-hour period.

CDP Neighbor Changed (Info)

The following devices had a CDP neighbor change with a non-network device during the previous 24-hour period.

Cisco Buffer Misses High (Error)

The following devices experienced a buffer miss every 10 seconds over 24 hours.

Cisco Buffer Misses High (Warning)

The following devices experienced a buffer miss every 100 seconds over 24 hours.

Cisco Buffer Misses High (Info)

The following devices experienced a buffer miss every 400 seconds over 24 hours.

Cisco No Buffer Memory (Error)

The following devices have buffer create failures. Buffer create failures are typically caused by a lack of free memory. The default threshold is 1 buffer failure but may be different depending on device group settings.

Device CPU Utilization High (Error)

The following devices have a high CPU utilization. The default threshold is 80% utilization but may be different depending on device group settings.

Device CPU Utilization High (Warning)

The following devices have a high CPU utilization. The default threshold is 60% utilization but may be different depending on device group settings.

Device Disk Utilization High (Error)

The following disk partitions have a high utilization. The default threshold is 90% utilization but may be different depending on device group settings.

Device Disk Utilization High (Warning)

The following disk partitions have a high utilization. The default threshold is 75% utilization but may be different depending on device group settings

Device DNS and SNMP sysName Mismatch (Info)

This issue is raised for devices where the configured SNMP sysName on the device doesn't resolve in DNS to an IP address configured on the device

Device Fan Problem (Error)

This device has generated a fan failure. The fan being monitored has failed.

Device Fan Problem (Warning)

This device has generated a fan warning. The fan being monitored is not functioning properly.

Device Free Memory Low (Error)

The following devices have a low amount of free memory. The default threshold is 4KB but may be different depending on device group settings. A low memory condition could indicate a memory leak or some other problem that may lead to a device reboot.

Device Identity Change (Info)

The following devices experienced at least one sysName and sysDescr change.

Device Issue Limit Exceeded (Error)

The following devices have an excessive number of open issues. A device is included in this list if it has more than 2 open issues with a severity level of Error or more than 5 open issues with a severity level of Warning or more than 10 open issues of any severity.

Device Memory Utilization High (Error)

This issue is raised when the 5-minute memory utilization of a device exceeds thresholds. The default threshold is 80% but may be different depending on device group settings.

Device Memory Utilization High (Warning)

This issue is raised when the 5-minute memory utilization of a device exceeds thresholds. The default threshold is 60% but may be different depending on device group settings.

Device Memory Utilization Increasing (Error)

The following devices have experienced a significant free memory decrease in the prior 24-hours. This could indicate a memory leak that may lead to a device reboot or crash. The default value is a 20% decrease but may be different depending on device group settings.

Device Memory Utilization Increasing (Warning)

The following devices have experienced a large free memory decrease in the prior 24-hours. This could indicate a memory leak that may lead to a device reboot or crash. The default value is a 10% decrease but may be different depending on device group settings.

Device Memory Utilization Increasing (Info)

The following devices have experienced a minor free memory decrease in the prior 24-hours. This could indicate a memory leak that may lead to a device reboot or crash. The default value is a 4% decrease but may be different depending on device group settings.

Device OS Version Change (Info)

The following devices are now running a version of operating system different than what it was previously in the prior 24-hour period.

Device Partially Supported (Info)

The following devices were found by the system that support SNMP data collection. However these devices may not be fully supported by the system. If you wish to see these devices supported by the system for data collection, please contact support with these issue details.

Device Power Supply Problem (Error)

This device has generated a power supply failure. The status of a power supply is outside the normal operating range and a system shutdown is imminent. For devices that report only the power supply state, this issue is triggered when a power supply has failed.

Device Power Supply Problem (Warning)

This device has generated a power supply warning. The status of the power supply being monitored is outside the normal operating range. For devices that report only the power supply state, then the power supply state of the entity being monitored is not functioning properly.

Device Recently Restarted (Info)

The following devices have restarted in the past 24 hours

Device Restarted Multiple Times (Warning)

The following devices have restarted multiple times in the previous 24-hour analysis period. The default threshold is 2 reboots but may be different depending on device group settings.

Device Temperature Problem (Error)

This device has generated a temperature warning. The temperature of the monitored entity is outside the normal operating range and a system shutdown is imminent. For devices that report only the temperature sensor state, then the temperature state of the entity being monitored has failed.

Device Temperature Problem (Warning)

This device has generated a temperature warning. The temperature of the monitored entity is outside the normal operating range. For devices that report only the temperature sensor state, then the temperature state of the entity being monitored is not functioning properly.

Device Voltage Problem (Error)

This device has generated a voltage failure. The voltage is outside the normal range of operation and a system shutdown is imminent. For devices that report only state, this issue is triggered for devices where the state of the entity being monitored has failed.

Device Voltage Problem (Warning)

This device has generated a voltage warning. The voltage is outside the normal range of operation. For devices that report only voltage sensor state, this issue is triggered for devices where the state of the entity being monitored is not functioning properly.

Down Device (Info)

The following devices are not reachable from the system and may be down.

Event Analysis Degraded Mode (Error)

Due to repeated volume license violations, the Event Analysis Module has stopped logging syslog messages and SNMP traps. More detailed information is available within the Event Analysis Module web interface.

Event Analysis Disk Space Check (Error)

The Event Analysis Module disk filesystem is over 80% utilization, and may indicate more disk space is needed.

Event Analysis Disk Space Check (Warning)

The Event Analysis Module disk filesystem is over 60% utilization, and may indicate more disk space is needed.

Event Analysis Disk Space Check (Info)

The Event Analysis Module disk filesystem is over 50% utilization, and may indicate more disk space is needed.

Event Analysis License Exceeded (Warning)

The Event Analysis Module Daily Volume Limit has been exceeded within the past 30 days. A portion of daily event traffic may be discarded unless volume is decreased or license limit is increased.

HP Buffer Misses High (Error)

The following HP ProCurve switches have experienced a buffer miss every 10 seconds over a 24-hour period.

HP Buffer Misses High (Warning)

The following HP ProCurve switches have experienced a buffer miss every 100 seconds over a 24-hour period.

HP Buffer Misses High (Info)

The following HP ProCurve switches have experienced a buffer miss every 400 seconds over a 24-hour period.

HP Corrupted Buffer Deletes High (Warning)

The following devices experienced a large number of corrupted message or packet buffer deletions during the prior 24-hour period. The default value is 10 but may be different depending on device group settings.

Management IP Not Reachable (Info)

The following devices are no longer responding to SNMP requests on the management IP address chosen for the device. The system has found an alternate IP address for the device and will continue to use it until the management IP address becomes accessible or it determines that a new IP address is to be used. If you believe that the system chose the wrong management IP to begin with you may suppress this instance of the issue.

New Device Found (Info)

The following new devices were found in the network in the prior 24-hour period.

New Non-Network Device Found (Info)

The following new non-network devices were found in the network in the prior 24-hour period.

New Wireless AP Device Found (Info)

The following new wireless AP devices were found in the network in the prior 24-hour period.

Rogue DHCP Server Cannot Be Isolated (Error)

The devices shown are running DHCP but are not sanctioned DHCP servers according to NIOS and are not found in the DHCP server exception list named TAE Allowed DHCP Servers which cannot be isolated.

Rogue DHCP Server Detected (Warning)

The devices shown are running DHCP but are not sanctioned DHCP servers according to NIOS and are not found in the DHCP server exception list named TAE Allowed DHCP Servers.

Rogue DHCP Server Located (Error)

The devices shown are running DHCP but are not sanctioned DHCP servers according to NIOS and are not found in the DHCP server exception list named TAE Allowed DHCP Servers. The location of the devices are known to the system for isolation.

Router With No ARP or Routing Tables (Warning)

The following routers do not allow SNMP collection of ARP or routing tables. Not providing ARP information limits the ability of the system to discover devices on the network. Not providing routing information will prevent the system from performing any routing analysis.

Router With No Loopback Address (Info)

The following routers do not have a loopback address configured.

SNMP Access Lost (Warning)

The following devices had known SNMP community strings but are no longer responding to SNMP queries. If the SNMP community string is no longer correct, go to the Settings display for the device and update the SNMP community string.

SNMP Collection Disabled (Info)

The following devices currently have SNMP data collection disabled. When SNMP data collection is disabled for a device no data can be gathered to perform analysis for that device and possibly part of the network where it lives. To enable SNMP data collection for the device click on the device from the list below, and go to the Settings menu option in the Device Viewer. From there, SNMP data collection can be re-enabled.

Switch With No Forwarding Tables (Warning)

The following switches do not allow SNMP collection of forward table data. Not providing forwarding data limits the ability of the system to discover devices on the network and perform analysis.

Routing Related

BGP Neighbor Changes High (Warning)

The following devices experienced one or more neighbor changes with a neighboring BGP router in the prior 24-hour period. The default value is 1 change but may be different depending on device group settings.

Device No Route (Error)

The following routers experienced a large number of 'no routes' in the prior 24-hour period. The default value is 5000 'no routes' but may be different depending on device group settings. The 'no route' counter is incremented whenever the router receives a packet that cannot be forwarded for any reason. One reason is that no system replied to an ARP request by the router. Ping sweeps of sparsely populated subnets will generate large numbers of 'no routes'. Such ping sweeps may be due to network discovery processes and may be due to worms or viruses on the network. Another reason is that the packet contained a destination address that didn't correspond to any route in the routing table. An example is an application that is using an invalid IP address, either hard coded into the application or obtained from an out of date DNS entry. A network analyzer is typically required to troubleshoot such problems.

Device No Route (Warning)

The following routers experienced a large number of 'no routes' in the prior 24-hour period. The default value is 750 'no routes' but may be different depending on device group settings. The 'no route' counter is incremented whenever the router receives a packet that cannot be forwarded for any reason. One reason is that no system replied to an ARP request by the router. Ping sweeps of sparsely populated subnets will generate large numbers of 'no routes'. Such ping sweeps may be due to network discovery processes and may be due to worms or viruses on the network. Another reason is that the packet contained a destination address that didn't correspond to any route in the routing table. An example is an application that is using an invalid IP address, either hard coded into the application or obtained from an out of date DNS entry. A network analyzer is typically required to troubleshoot such problems.

Device Routing Table Changed (Warning)

The following devices have had routing table changes during the analysis period. By default, host routes are excluded from this issue.

EIGRP Neighbor Changes High (Warning)

The following devices experienced one or more neighbor changes with a neighboring EIGRP router in the prior 24-hour period. The default value is 1 but may be different depending on device group settings.

HSRP In Initial State (Warning)

The following routers have HSRP groups in an `initial' state. Each HSRP group configured on the router is shown with the virtual IP address of the group in the initial state. When a HSRP group is in the `initial' state, the router is not ready to participate in HSRP. This could be because an interface is down or because a group has not been assigned an IP address. This problem can also result as an incomplete configuration of HSRP on an interface. The output of ‘show standby' will not show any HSRP groups in initial state. Use ‘show standby init' to see groups in initial state. HSRP in initial state may be caused by at least two things: A partial configuration statement, similar to 'ip standbypriority 110'. Note that if there is no group number, it defaults to group 0. If there's a group number and no IP address, the group will exist and the address will be 0.0.0.0. Check the configuration for incomplete HSRP configuration statements. A router that is not configured with HSRP may show a standby group that is being advertised by a neighboring router (depends on the IOS version).

ICMP Destination Unreachables Sent (Warning)

The following devices sent a large number of ICMP destination unreachable messages in the prior 24-hour period. The default value is 100 but may be different depending on device group settings. Large numbers of

ICMP destination unreachable messages, especially when seen on a large number of routers, indicate that a network scan may be taking place.

ICMP Redirects High (Info)

The following devices have experienced a high number of ICMP redirect messages in the prior 24-hour period. The default value is 500 but may be different depending on device group settings. ICMP redirects are used to communicate to a device, errors encountered while routing packets and to exercise control on traffic. Large numbers of ICMP redirects could indicate that a host is configured with an incorrect default gateway or improper routing is occurring.

IP Routing Discards (Error)

The following devices experienced a large number of IP routing discards during the prior 24 hours. The default value is 50 but may be different depending on device group settings. IP routing discards are the number of routing entries which where chosen to be discarded even though they are valid. A possible reason for IP routing discards could be to free buffer space to make room for other routing entries.

IP Routing Discards (Warning)

The following devices experienced a large number of IP routing discards during the prior 24 hours. The default value is 10 but may be different depending on device group settings. IP routing discards are the number of routing entries which where chosen to be discarded even though they are valid. A possible reason for IP routing discards could be to free buffer space to make room for other routing entries.

IP Routing Discards (Info)

The following devices experienced a large number of IP routing discards during the prior 24 hours. The default value is 1 but may be different depending on device group settings. IP routing discards are the number of routing entries which where chosen to be discarded even though they are valid. A possible reason for IP routing discards could be to free buffer space to make room for other routing entries.

Network Routing Table Changed (Warning)

A change in the global network routing summary has occurred. By default, host routes are excluded from this issue.

OSPF Area Not Connected to Backbone (Error)

The following list of OSPF Area's are not connected to the backbone. This is determined by not finding any router in an area also connected to area 0.

OSPF Authentication Disabled (Error)

The following routers have OSPF authentication disabled. Using OSPF authentication protects against unauthorized injection of packets or denial of service against a network running OSPF.

OSPF Neighbor Changes High (Warning)

The following devices are experiencing neighbor changes with a neighboring OSPF router. The default threshold is 1 change but may be different depending on device group settings. Regular neighbor changes imply that OSPF hello timers may not be matched or that some other mechanism is causing regular communications problems that affect OSPF's hello protocol. A single neighbor change that doesn't repeat periodically may be due to other factors such as switch maintenance or due to a network change made by a WAN carrier and may not be a concern.

OSPF Stability Problem (Error)

The following devices have calculated the intra-area route table a large number of times during the prior 24-hour period. The default value is 75 but may be different depending on device group settings.

OSPF Stability Problem (Warning)

The following devices have calculated the intra-area route table a large number of times during the prior 24-hour period. The default value is 60 but may be different depending on device group settings.

Possible Bad IPv4 Route (Error)

The following IPv4 routes have been found to have a network mask between 1 and 7 bits. This amount of aggregation may reflect an error or an attempt to interfere with proper routing, and may also impact the performance of some Cisco routers running CEF. Determine whether this route is legitimate, and if not identify and block the source.

Possible Routing Loop (Info)

The following devices have experienced a high number of Time Exceeded ICMP messages in the prior 24 hours. High numbers of Time Exceeded ICMP messages are caused by packets that are being discarded due to an expiring TTL. High use of traceroute or routing loops are the typical causes of large number of Time Exceeded ICMP messages.

QoS Queue Dropped Packets (Error)

The following device interfaces have dropped packets in a high priority queue.

QoS Queue Dropped Packets (Warning)

The following device interfaces have dropped packets in a mid-priority queue.

QoS Queue Dropped Packets (Info)

The following device interfaces have dropped packets in a low priority queue.

QoS Queue Without Any Hits (Info)

The following QoS queues have registered no hits in the prior 24-hour period. This could mean that traffic intended for the queue is hitting another queue or that a queue hasn't been assigned to an interface. The default time period is 24 hours but may be different depending on interface group settings.

Security Related

Device With Web Interface Open (Warning)

The following network devices were found to have an open web interface in the prior 24-hour period. These devices usually have some sort of administrative access to the device through the web interface. If the interface is not password protected or not protected with access lists or firewall rules, then unauthorized users may be able to access the administrative functions of the device.

Firewall Buffer Pool Utilization High (Error)

This issue is raised when a Cisco firewall reports a low percentage of current buffers are free which is an indication of high utilization. The default threshold is 20% but may be different depending on device group settings. Exhausting the buffer pool will cause the firewall to stop processing until buffers are returned to the buffer pool when a connection is terminated or is timed out. There are several buffer sizes and this issue reports on any of the buffer sizes that have high utilization.

Firewall Connection Count High (Error)

This issue is raised when a firewall connection count was greater than or equal to 80% of the maximum number of allowed connections during the analysis period. The actual threshold may be different depending on device group settings. The details display the current connection count percentage, the number of connections, maximum connections allowed according to the platform's license, and the maximum number of connections detected since the device booted at the last time.

Firewall Connection Count High (Warning)

This issue is raised when a firewall connection count was greater than or equal to 60% but less than 80% of the maximum number of allowed connections during the analysis period. The actual threshold may be different depending on device group settings. The details display the current connection count percentage, the number of connections, maximum connections allowed according to the platform's license, and the maximum number of connections detected since the device booted at the last time.

Firewall Connection Count High (Info)

This issue is raised when a firewall connection count was greater than or equal to 50% but less than 60% of the maximum number of allowed connections during the analysis period. The actual threshold may be different depending on device group settings. The details display the current connection count percentage, the number of connections, maximum connections allowed according to the platform's license, and the maximum number of connections detected since the device booted at the last time.

Firewall Redundancy Failure (Error)

This issue is raised when a redundant unit for a firewall has failed during the analysis period.

Unknown Community Strings (Warning)

The following devices could not be accessed because the SNMP community string is unknown. In such cases, you should enter the SNMP community string using the SNMP Collector menu option on the System Settings page so that the devices can be monitored properly.

Weak Community String (Warning)

The following devices were accessed using commonly known SNMP community strings. You should change these SNMP community strings to something less obvious or add them to the list of known community strings using the Setup -> SNMP Credentials menu option on the Settings page.

Security Control Related

Duplicate Object (Warning)

This issue is raised for IP addresses assigned to multiple named security control objects.

Duplicate Rule (Warning)

This issue is raised for rules with the same meaning (IP address and flow).

Duplicate Service (Warning)

This issue is raised for flows assigned to multiple named security control services.

Hidden Rule (Warning)

This issue is raised when a rule with a larger subnet/flow id defined before this one and then fully hide this rule.

Hidden Rule (Warning)

This issue is raised when a rule with a larger subnet/flow id defined before this one and then fully hide this rule.

Overlap Rule (Warning)

This issue is raised for security control rules which are overlapped partially by another rule placed before.

Subset Rule (Warning)

This issue is raised for rules which is a subset (IP addresses / flow) of another rule placed below and then hide it partially.

Unused Object (Warning)

This issue is raised for security control objects that are not referenced elsewhere in the device configuration.

Unused Rule (Warning)

This issue is raised for security control rules that have not been used within a 30-day period.

Unused RuleList (Warning)

This issue is raised for security control rule lists (ACL) that aren't used.

Unused Service (Warning)

This issue is raised for security control objects that are not referenced elsewhere in the device configuration.

Useless Rule (Warning)

This issue is raised for security control rules which are useless - a same exact matching rule with opposite allow/deny is defined before this rule.

VLAN Related

VLAN Topology Change (Error)

The following VLAN devices had a small number of topology changes during prior 24-hour period. The default threshold is 200 changes but may be different depending on device group settings. When 802.1d STP is running, each topology change causes the switch forwarding table cache timer to be reduced to 15 seconds, resulting in increased unicast flooding as the cache is refreshed. The default cache timer is 5 minutes (300 seconds), causing a cache refresh 144 times a day. When 802.1w RSTP is running, the table is immediately flushed. Too many topology changes effectively reduces the cache timer and increases unicast flooding. If the ports causing these topology changes to occur are user end stations or ports for which a link going up or down isn't a significant event, they can be eliminated by enabling portfast.

VLAN Topology Change (Warning)

The following VLAN devices had a small number of topology changes during prior 24-hour period. The default threshold is 100 changes but may be different depending on device group settings. When 802.1d STP is running, each topology change causes the switch forwarding table cache timer to be reduced to 15 seconds, resulting in increased unicast flooding as the cache is refreshed. The default cache timer is 5 minutes (300 seconds), causing a cache refresh 144 times a day. When 802.1w RSTP is running, the table is immediately flushed. Too many topology changes effectively reduces the cache timer and increases unicast flooding. If the ports causing these topology changes to occur are user end stations or ports for which a link going up or down isn't a significant event, they can be eliminated by enabling portfast.

VLAN Topology Change (Info)

The following VLAN devices had a small number of topology changes during prior 24-hour period. The default threshold is 50 changes but may be different depending on device group settings. When 802.1d STP is running, each topology change causes the switch forwarding table cache timer to be reduced to 15 seconds, resulting in increased unicast flooding as the cache is refreshed. The default cache timer is 5 minutes (300 seconds), causing a cache refresh 144 times a day. When 802.1w RSTP is running, the table is immediately flushed. Too many topology changes effectively reduces the cache timer and increases unicast flooding. If the ports causing these topology changes to occur are user end stations or ports for which a link going up or down isn't a significant event, they can be eliminated by enabling portfast.

VLAN With No Active Ports (Warning)

The following VLANs were found on the listed devices and do not have any active ports in the VLAN. If the VLAN was learned from a trunk link, then it is a candidate for pruning. Otherwise it is an orphaned VLAN from a static configuration.

Wireless Related

Wireless AP Hot Standby Active (Error)

The following wireless access points running in hot standby became the active unit. Contact with the previous active unit was lost.

Wireless AP Hot Standby Ethernet Failure (Error)

The following wireless access points running in hot standby mode detected an Ethernet connectivity failure with the active unit but has not taken over the active role. Check connectivity between the standby and active units.

Wireless AP Hot Standby Radio Failure (Error)

The following wireless access points running in hot standby mode detected a radio connectivity failure with the active unit but has not taken over the active role. Check connectivity between the standby and active units.

Interfaces Related

10Mbps Switch Port Errors High (Error)

The following 10Mbps switch interfaces experienced a high packet volume where the error rate was greater than 1% of in either direction. The default trigger threshold is one million packets in the same direction as the error rate but may be different depending on interface group settings. 10Mbps ports typically operate in half duplex mode and some vendors count collisions as errors, causing a high number of errors to be reported. Since collisions trigger a retry by the Ethernet interface, the packet may actually make it to the destination without error. The Ethernet interface will retry the transmission up to 16 times before the packet is discarded. If the switch and attached device support 10Mbps/Full Duplex, then configuring this configuration will eliminate collisions.

10Mbps Switch Port Errors High (Warning)

The following 10Mbps switch interfaces experienced a high packet volume where the error rate was greater than 1% of in either direction. The default trigger threshold is 100,000 packets in the same direction as the error rate but may be different depending on interface group settings. 10Mbps ports typically operate in half duplex mode and some vendors count collisions as errors, causing a high number of errors to be reported. Since collisions trigger a retry by the Ethernet interface, the packet may actually make it to the destination without error. The Ethernet interface will retry the transmission up to 16 times before the packet is discarded. If the switch and attached device support 10Mbps/Full Duplex, then configuring this configuration will eliminate collisions.

10Mbps Switch Port Errors High (Info)

The following 10Mbps switch interfaces experienced a high packet volume where the error rate was greater than 1% of in either direction. The default trigger threshold is one packet in the same direction as the error rate but may be different depending on interface group settings. 10Mbps ports typically operate in half duplex mode and some vendors count collisions as errors, causing a high number of errors to be reported. Since collisions trigger a retry by the Ethernet interface, the packet may actually make it to the destination without error. The Ethernet interface will retry the transmission up to 16 times before the packet is discarded. If the switch and attached device support 10Mbps/Full Duplex, then configuring this configuration will eliminate collisions.

Access Port With PortFast Disabled (Error)

The following active switch access ports are not configured with the PortFast feature enabled. This will cause delays with the port becoming active as the port cycles through the listening and learning phases. The delay can also cause devices connected to the switch to give up trying to connect to a server (such as DHCP) before the switch even allows traffic to pass. In addition, each time a port becomes active and moves to the forwarding state the switch will propagate a topology change notification throughout the VLAN causing all MAC addresses to be aged from the switch after 15 seconds. With PortFast, the switch will not send out topology change notifications when the port becomes active.

Access Port With SNMP Link Up/Down Trap Enabled (Info)

The following active switch access ports are configured to raise a SNMP trap for each state change of the interface. On a user access port this could result in excessive notifications that are typically ignored.

Broken Switch Port (Warning)

The following switch ports are marked as broken as defined by application of the Spanning Tree Protocol.

Current Interface Utilization High (Warning)

The following router interfaces had a high utilization during the most recent polling cycle. The default threshold is 80% but may be different depending on device group settings.

Downstream Hub or Switch (Info)

The following non-trucking switch ports were found to have more than one direct neighbor on them during the analysis period.

EtherChannel On One Card (Warning)

The following interfaces are part of an EtherChannel group where all the links are defined to be on one card.

EtherChannel Unbalanced (Warning)

The following interfaces are part of an EtherChannel group where the lowest utilized link differs in utilization by more than 50% of the highest utilized link.

Incorrect Duplex Setting (Warning)

The following switch interfaces are operating with a duplex setting that is likely to be incorrect and should be validated.

Incorrect Serial Bandwidth Setting (Warning)

These Cisco serial interfaces were found to be running at more than 100% utilization, suggesting that their configured bandwidth is not the same as their operating bandwidth. The configured bandwidth setting is used by Cisco for a variety of routing and traffic shaping protocols and should be set to the correct bandwidth of the interface. Routing metric modifications to influence routing decisions should be done using the Delay metric for EIGRP or the Cost metric for OSPF.

Interface Broadcasts High (Error)

The follow router interfaces have a high broadcast packet rate of the packets sent or received. The default threshold is 50 packets per second but may be different depending on interface group settings.

Interface Broadcasts High (Warning)

The follow router interfaces have a high broadcast packet rate of the packets sent or received. The default threshold is 20 packets per second but may be different depending on interface group settings.

Interface Broadcasts High (Info)

The follow router interfaces have a high broadcast packet rate of the packets sent or received. The default threshold is 5 packets per second but may be different depending on interface group settings.

Interface Congested (Warning)

The following interfaces had a high discard rate of the total number of packets sent or received. The default threshold is 0.1% of the total number of packets sent or received but may be different depending on interface group settings.

Interface Errors High (Warning)

The following router interfaces currently have a high error rate during the most recent polling cycle. The default threshold is 0.00001% of the total number of packets sent or received but may be different depending on interface group settings.

Interface Non-Unicasts High (Warning)

The following router interfaces have a high non-unicast packet rate. The default threshold is 10% of the total number of packets sent or received, but may be different depending on interface group settings.

Interface Not Stable (Warning)

The following interfaces had a large number of operational state changes in the prior 24-hour period. The default threshold is 2 changes but may be different depending on interface group settings.

Interface Unexpected Utilization Change (Error)

For the following interfaces, the most average utilization calculated during the analysis period exceeds the 7-day running average utilization by more than 15%.

Interface Unexpected Utilization Change (Warning)

For the following interfaces, the most average utilization calculated during the analysis period exceeds the 7-day running average utilization by more than 8%.

Interface Utilization High (Warning)

The 95th percentile utilization metric for the following interfaces was greater than 40%. The 95th percentile utilization is determined by sampling the interface utilization every 10 minutes throughout the day. After the samples are sorted, the top 5% are thrown out and the highest remaining sample is used as the 95th percentile utilization value. Such calculations are typically used in Service Level Agreements (SLAs) for billing purposes.

Interface Utilization Low (Info)

The 95th percentile utilization metric for the following Serial interfaces was less than 1 percent. These interfaces may not be handling production traffic. The 95th percentile utilization is determined by sampling the interface utilization every 10 minutes throughout the day. After the samples are sorted, the top 5% are thrown out and the highest remaining sample is used as the 95th percentile utilization value. Such calculations are typically used in Service Level Agreements (SLAs) for billing purposes.

Invalid Admin / Oper State (Info)

The following interfaces have an administrative status of 'Up', and an operational status of 'Down'. The interface is either experiencing problems and should be 'Up'/'Up' or it should be configured to be 'Down'.

Port In Error Disable State (Error)

The following switch ports are in an errdisable state.

Router Interface Down (Error)

The following router interfaces have an administrative status of 'Up', and an operational status of 'Down'. The interface is either experiencing problems and should be 'Up'/'Up' or it should be configured to be 'Down'.

Switch Port Duplex Mismatch (Error)

The following 100Mbps switch interfaces experienced a high packet volume where the error rate was greater than 0.01% of in either direction. The default trigger threshold is one million packets in the same direction as the error rate but may be different depending on interface group settings. Such an error rate may indicate that the duplex setting for the interface does not match the other side of the link. FCS and alignment errors on a port usually means the port is configured for full duplex and the connected device is a repeater or half-duplex device.

Late collisions on the port usually indicate the port is configured for half-duplex and the attached device is full duplex. In addition to switch port duplex mismatch problems, errors may also be caused by bad cables, faulty switch ports, and other NIC issues.

Switch Port Duplex Mismatch (Warning)

The following 100Mbps switch interfaces experienced a high packet volume where the error rate was greater than 0.01% of in either direction. The default trigger threshold is one 100,000 packets in the same direction as the error rate but may be different depending on interface group settings. Such an error rate may indicate that the duplex setting for the interface does not match the other side of the link. FCS and alignment errors on a port usually means the port is configured for full duplex and the connected device is a repeater or half-duplex device. Late collisions on the port usually indicate the port is configured for half-duplex and the attached device is full duplex. In addition to switch port duplex mismatch problems, errors may also be caused by bad cables, faulty switch ports, and other NIC issues.

Switch Port Duplex Mismatch (Info)

This issue lists 100Mbps switch interfaces that experienced a an average error rate greater than 0.01% in either direction and the packet volume was greater than or equal to one packets per day but less than one million packets per day in the same direction. This may indicate that the duplex setting for the interface does not match the other side of the link. FCS and alignment errors on a port usually means the port is configured for full duplex and the connected device is a repeater or half-duplex device. Late collisions on the port usually indicate the port is configured for half-duplex and the attached device is full duplex. In addition to switch port duplex mismatch problems, errors may also be caused by bad cables, faulty switch ports, and other NIC issues.

Switch Port Failed Power-On Self Test (Warning)

The following switch ports have failed the power-on self test. For Cisco switches, this can be seen with the command show post.

Trunk Port With PortFast Enabled (Error)

The following active trunk ports are configured with the PortFast feature enabled. This feature should not be used on switch trunk ports because physical loops may result which can bring the network down.

Unidirectional Traffic Flow (Warning)

The following router interfaces processed packets in one direction, but not in the opposite direction.

VPN Tunnel MTU Mismatch (Error)

The following tunnels have MTU values that are not the same for all of the tunnel interfaces.

Interface VLAN Related

VLAN Definition Missing (Error)

The following ports were found to be assigned to a VLAN that doesn't exist on a device.

VLAN Trunk Port Down (Error)

The following VLAN trunk ports are down. In such cases, a VLAN may be partitioned, possibly resulting in traffic not reaching its intended destination or network redundancy may be compromised.

Interface Wireless Related

Wireless AP Broadcasting SSID (Warning)

The following wireless access point IEEE 802.11 interfaces were found to be announcing their own SSID making it easier for unauthorized users to access your network by being able to discover the wireless access point.
Wireless AP EAP Disabled (Warning)

The following wireless access point IEEE 802.11 interfaces were found to have EAP disabled. This means that the AP does not require user authentication for association. This weakens network security. Consider establishing authentication to increase security.