

NacTrack How To Guide

Operational answers, step by step, captured from a live install.

15 entries · generated 2026-08-02

Contents

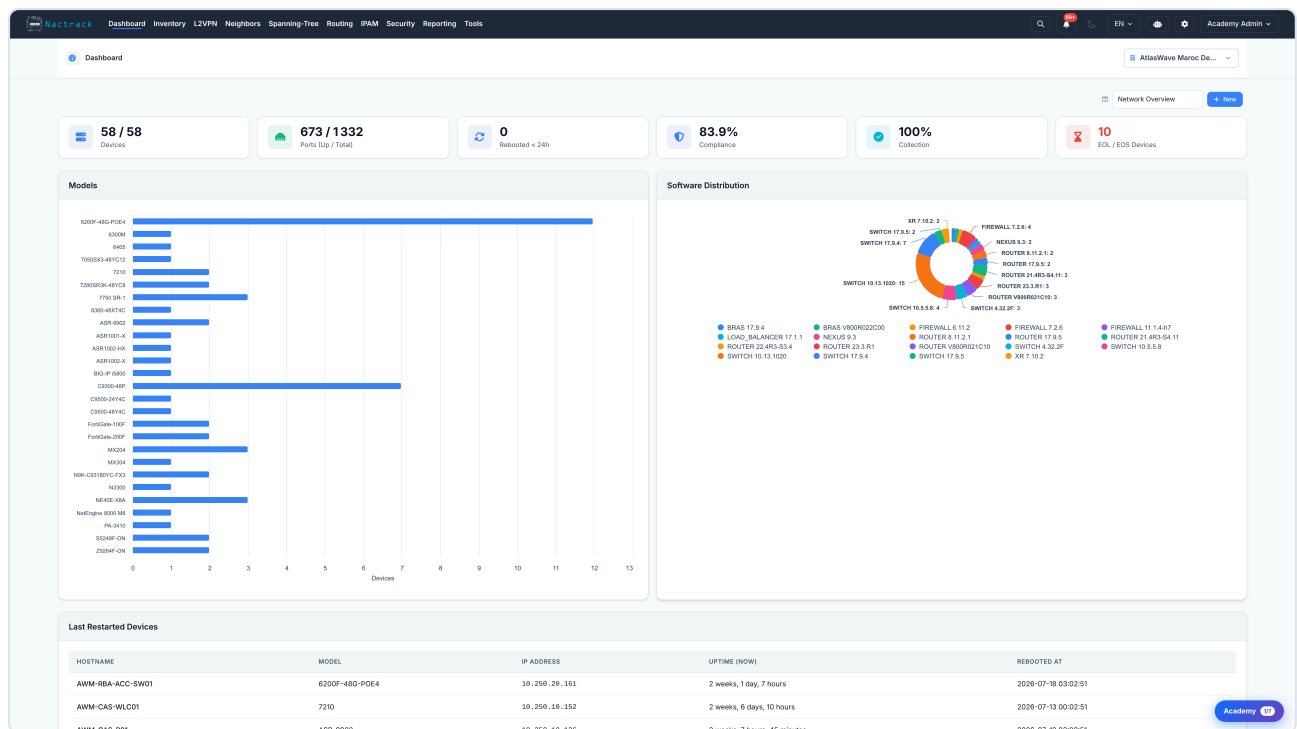
1. FIND IT · ENDPOINTS
How to find which switch and port a MAC address is on
2. FIND IT · ENDPOINTS
How to find where an IP address lives on the network
3. FIND IT · ENDPOINTS
How to search with a partial MAC address to find every device from one manufacturer
4. FIND IT · ENDPOINTS
How to tell whether an IP belongs to a user device or to network equipment
5. FIND IT · VLANS AND LAYER 2
How to find every port carrying a VLAN
6. FIND IT · VLANS AND LAYER 2
How to see which VLANs a trunk allows
7. UNDERSTAND IT · SECURITY POSTURE
How to see which ports are configured for 802.1X
8. UNDERSTAND IT · SECURITY POSTURE
How to check whether a device still allows Telnet
9. UNDERSTAND IT · SECURITY POSTURE
How to find devices using default or version 1 and 2c SNMP communities
10. UNDERSTAND IT · SECURITY POSTURE
How to read a device's management access posture
11. UNDERSTAND IT · SPANNING TREE
How to find which switch is root bridge for each VLAN
12. UNDERSTAND IT · SPANNING TREE
How to find which ports spanning tree is blocking
13. UNDERSTAND IT · SPANNING TREE
How to check whether BPDU Guard is enabled on edge ports
14. UNDERSTAND IT · VLANS AND LAYER 2
How to tell whether a VLAN still has any ports on a switch
15. DIAGNOSE IT · CHANGE AND FAILURE
How to find out what changed on the network between two collections

How to find which switch and port a MAC address is on

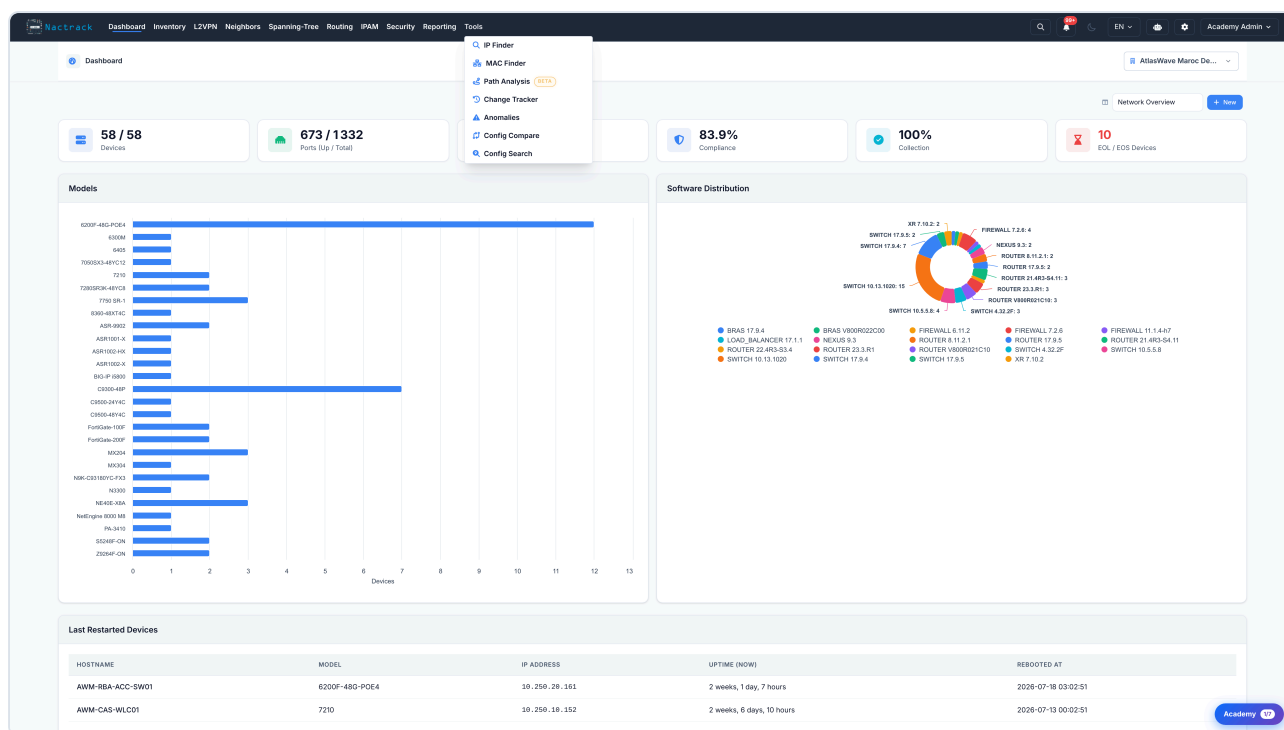
A user reports a problem and all you have is a MAC address. MAC Finder searches every MAC table collected across the estate at once and tells you the device, the interface and the VLAN it was learned on. It reads the last collection, not the live switch, so the answer is as recent as your last collect round.

Requires: module: core, permission: use_troubleshooting

- 1 We start on the NacTrack dashboard, with the latest collection already loaded. Locating an endpoint is a troubleshooting task, so everything we need sits in one menu.



- 2 Open the Tools menu in the top navigation bar. This is where NacTrack keeps the tools that answer a question about one specific thing, rather than showing you a whole inventory.



- 3 Choose MAC Finder. The page opens empty, with a single search box: it holds no list of its own and searches only what you ask it for. Everything it returns comes from the MAC tables collected from your switches.

The screenshot shows the NacTrack MAC Finder tool interface. It features a search box labeled 'MAC Address / IP Address' with a dropdown menu showing 'aa:bb:cc:dd:ee:ff / aa:bb:cc:dd:ee:ff / 10.0.0.1'. Below the search box are 'Find' and 'Reset' buttons. A note indicates 'Wildcards supported, e.g. aa:bb*, 10.0.0.*, aa:bb:cc*'. The interface is clean and minimalist, designed for quick searches.

- 4 Type the MAC address you are looking for. Colon, dot and dash formats are all accepted, so you can paste it exactly as your ticket has it, without reformatting.

The search box on this page is not the one in the top navigation bar, which searches IP addresses.

The screenshot shows the NacTrack MAC Finder tool interface with the MAC address '3c:97:0e:68:41:41' entered into the search box. The 'Find' and 'Reset' buttons are still visible. The interface remains consistent with the previous screenshot, showing the search box and the note about wildcard support.

- 5 Click Find. Every switch that learned this address answers at once. Read the row left to right: the address, the IP behind it, the VLAN, the interface, the device holding that interface, the VRF, and how long ago it was seen.

The screenshot shows the Nactrack MAC Finder interface. The search bar contains the MAC address 3c:97:0e:68:41:41. Below the search bar, it indicates "14 results found". The results are displayed in a table with columns: MAC ADDRESS, IP ADDRESS, VLAN, INTERFACE, DEVICE, TYPE, VRF, AGE, and COLLECTED. The table shows 14 rows of data, including MAC addresses, IP addresses, VLANs, interfaces, devices, types, VRFs, ages, and collection times.

MAC ADDRESS	IP ADDRESS	VLAN	INTERFACE	DEVICE	TYPE	VRF	AGE	COLLECTED
3c:97:0e:68:41:41	10.188.0.103	100	Gi1/0/4	AWM-CAS-DC-SP01	Dynamic	VRF-DC-SHARED	50	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.188.0.103	100	Gi1/0/4	AWM-CAS-DC-SP03	Dynamic	VRF-DC-SHARED	50	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.188.0.103	100	ethernet1/10	AWM-CAS-DC-LF04	Dynamic	VRF-DC-SHARED	50	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.188.0.103	100	Gi1/0/4	AWM-CAS-ACC-SW02	Dynamic	VRF-DC-SHARED	50	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.188.0.103	100	Gi1/0/4	AWM-RBA-CORE-SW01	Dynamic	VRF-DC-SHARED	50	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.188.0.103	100	Gi1/0/4	AWM-RBA-AGG-SW01	Dynamic	VRF-DC-SHARED	50	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.188.0.103	100	Gi1/0/4	AWM-MRT-ACC-SW02	Dynamic	VRF-DC-SHARED	50	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.188.0.103	100	Gi1/0/4	AWM-TNG-ACC-SW02	Dynamic	VRF-DC-SHARED	50	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.188.0.103	100	Gi1/0/4	AWM-FES-ACC-SW02	Dynamic	VRF-DC-SHARED	50	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.188.0.103	100	Gi1/0/4	AWM-HGA-ACC-SW02	Dynamic	VRF-DC-SHARED	50	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.188.0.103	-	Vlan100	AWM-CAS-DC-LF01	Arp	VRF-DC-SHARED	229	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.188.0.103	-	Vlan100	AWM-CAS-DC-LF02	Arp	VRF-DC-SHARED	91	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.188.0.103	-	Vlan100	AWM-CAS-DC-LF03	Arp	VRF-DC-SHARED	197	2026-07-31T14:02:51
3c:97:0e:68:41:41	10.188.0.103	-	Vlan100	AWM-CAS-DC-LF04	Arp	VRF-DC-SHARED	50	2026-07-31T14:02:51

WORTH KNOWING

One MAC normally returns several rows. Every switch on the path learned it, so uplinks appear alongside the access port. The access port is the one where the interface is not a trunk toward another switch.

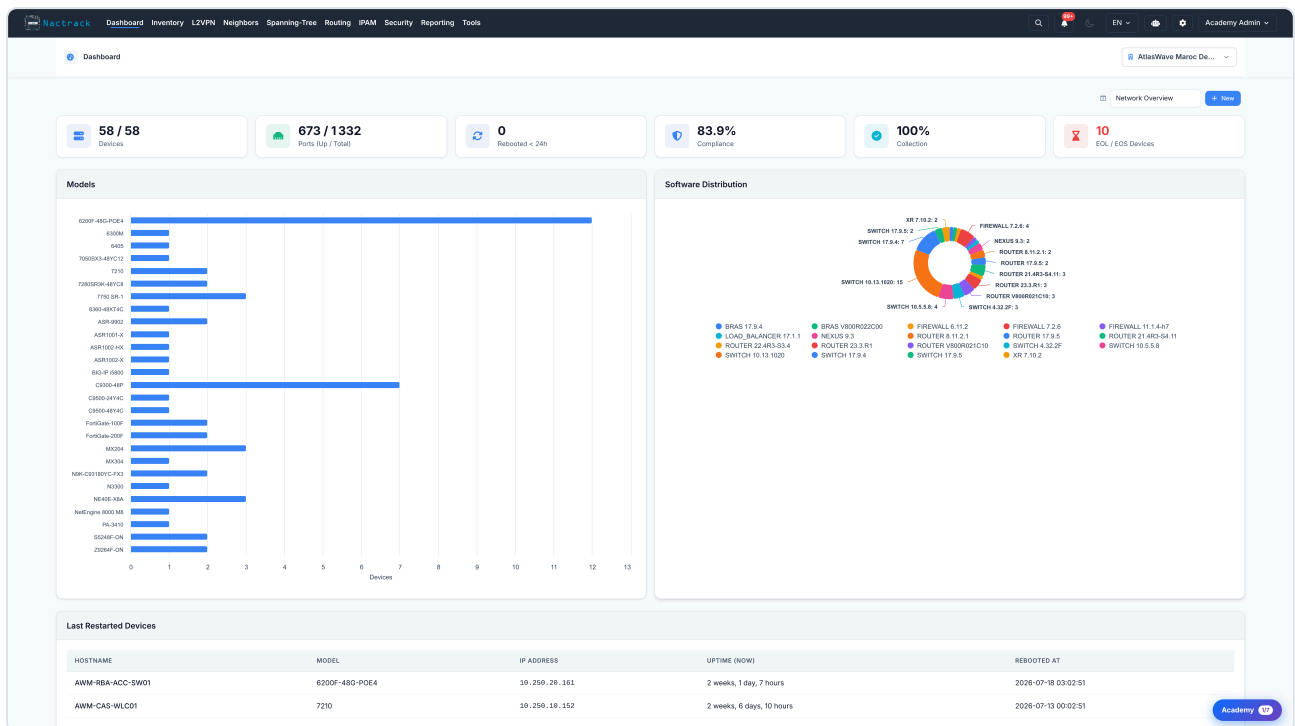
The IP column is filled in only when the same address was also seen in an ARP table. An empty IP means the endpoint is layer 2 only, or no router in the path has ARPed it.

How to find where an IP address lives on the network

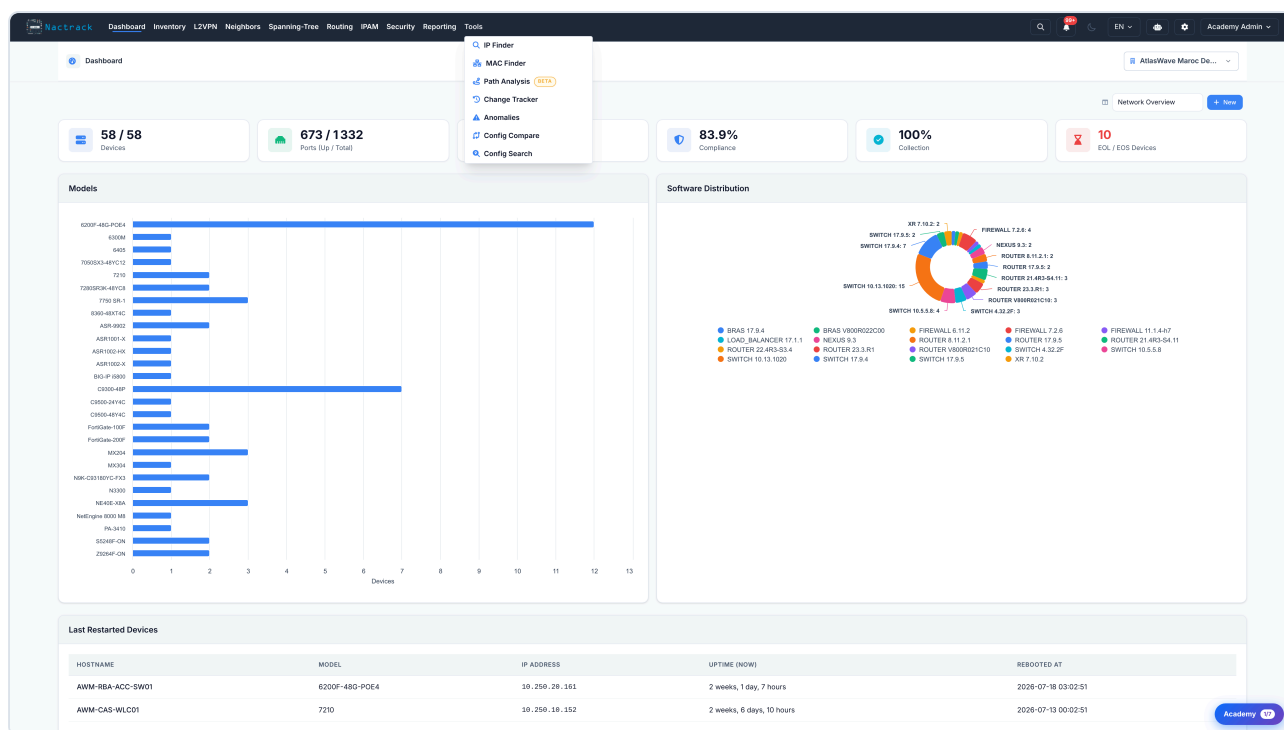
You have an IP and need to know which device holds it and behind which interface. IP Finder searches every source NacTrack collected - ARP tables, the inventory and the neighbour tables - and groups the answer by where it was found, so you can tell an endpoint apart from a device management address at a glance.

Requires: module: core, permission: use_troubleshooting

- 1 Again we begin on the dashboard, with the last collection loaded. Finding an address is a lookup, not a report, so we go to the same troubleshooting menu.



- 2 Open the Tools menu. IP Finder sits at the top of the list, just above MAC Finder: the two are companions, one starting from an address and the other from a hardware identifier.



- 3 Choose IP Finder. Like MAC Finder it opens with a single field and no list of its own, and it accepts either one host address or a whole subnet in CIDR notation.

The screenshot shows the IP Finder tool interface. It has a search bar with the text '192.0.2.7 or 198.51.100.0/24' and a dropdown menu. Below the search bar are 'Find' and 'Reset' buttons.

- 4 Type the address you are looking for.

The screenshot shows the IP Finder tool interface with the address '10.100.0.103' entered in the search bar. The 'Find' and 'Reset' buttons are still visible.

- 5 Click Find. The block is headed by the source that matched, here the ARP table, and every row names the device that holds the entry, the interface, the VRF and the MAC address sitting behind that IP.

The screenshot shows the Nactrack IP Finder interface. At the top, there's a navigation bar with links like Dashboard, Inventory, L2VPN, Neighbors, Spanning-Tree, Routing, IPAM, Security, Reporting, and Tools. A search bar at the top right contains the IP address 10.100.0.103. Below the navigation bar, the IP Finder section is active, showing a search for IP/Subnet 10.100.0.103. A 'Find' button is visible. Below the search bar, the results are displayed under the heading 'ARP Table (4)'. The table lists four entries, each representing a device's ARP table entry for the specified IP.

HOSTNAME	IP ADDRESS	MAC ADDRESS	INTERFACE	VRF	DETAILS
AWM-CAS-DC-LF01	10.100.0.103	3c:97:0e:68:41:41	Vlan100	VRF-DC-SHARED	dynamic Age: 229
AWM-CAS-DC-LF02	10.100.0.103	3c:97:0e:68:41:41	Vlan100	VRF-DC-SHARED	dynamic Age: 81
AWM-CAS-DC-LF03	10.100.0.103	3c:97:0e:68:41:41	Vlan100	VRF-DC-SHARED	dynamic Age: 197
AWM-CAS-DC-LF04	10.100.0.103	3c:97:0e:68:41:41	Vlan100	VRF-DC-SHARED	dynamic Age: 50

WORTH KNOWING

Several devices normally answer for the same endpoint IP. Each is a router or switched virtual interface that has the address in its own ARP table; they are not duplicates.

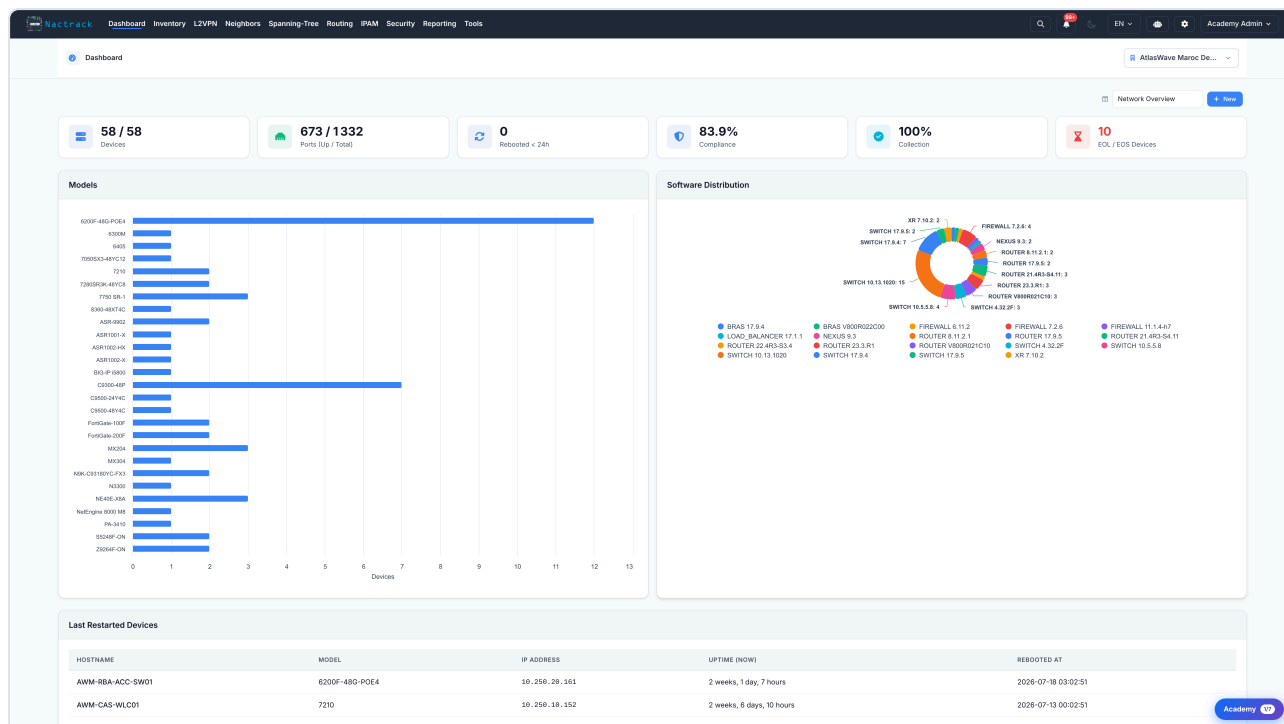
The answer is only as fresh as the last collection. An ARP entry that has since aged out on the device will still be shown until the next collect round.

How to search with a partial MAC address to find every device from one manufacturer

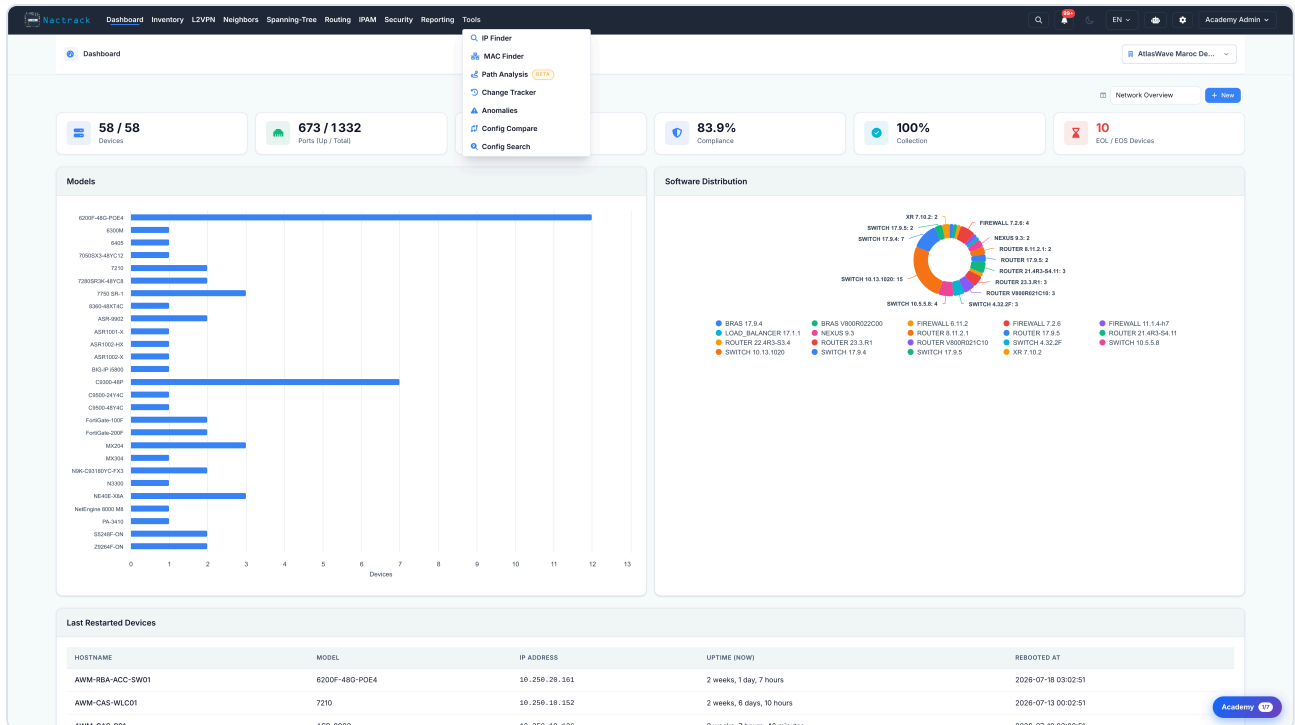
The first three bytes of a MAC address identify the manufacturer. Searching on that prefix with a wildcard turns MAC Finder into an inventory of everything from one vendor that is plugged into your network - useful when a firmware advisory or a recall names a manufacturer rather than a list of serial numbers.

Requires: module: core, permission: use_troubleshooting

- 1 We are on the dashboard once more. This time we are not chasing one endpoint but asking a question about a whole population of them, and the same tool answers both.



2 Open the Tools menu again.



3 Choose MAC Finder. Notice the hint under the field: wildcards are supported. That single line is what turns a lookup tool into a survey tool.

The screenshot shows the 'Tools > MAC Finder' interface. It features a text input field for 'MAC Address / IP Address' with the placeholder text 'aa:bb:cc:dd:ee:ff / aa:bb:cc:dd:ee:ff / 10.0.0.1'. Below the field, a hint states 'Wildcards supported, e.g. aa:bb:*, 10.0.0.*, aa:bb:cc:*'. There are 'Find' and 'Reset' buttons.

4 Type the manufacturer prefix followed by a star. Three bytes is the usual length of a vendor prefix, but any partial address works.

The screenshot shows the 'Tools > MAC Finder' interface with the text '00:1c:b3*' entered into the 'MAC Address / IP Address' field. The hint 'Wildcards supported, e.g. aa:bb:*, 10.0.0.*, aa:bb:cc:*' is still visible. The 'Find' and 'Reset' buttons are present.

- 5 Click Find. Every endpoint whose address starts with that prefix comes back, across every switch and every site, each with the port it is connected to. What was one answer is now a population you can count.

The screenshot shows the Nactrack MAC Finder tool interface. At the top, there's a navigation bar with tabs like Dashboard, Inventory, L2VPN, Neighbors, Spanning-Tree, Routing, IPAM, Security, and Reporting. Below this, the 'Tools' dropdown is open, and 'MAC Finder' is selected. The search bar contains the MAC address '00:1c:b3:07:7b:29'. Below the search bar, there are buttons for 'Find' and 'Reset'. The results section shows '120 results found'. There are tabs for 'CSV' and 'Excel'. A 'Show 50 entries' dropdown is visible. The main table displays the search results with columns: MAC ADDRESS, IP ADDRESS, VLAN, INTERFACE, DEVICE, TYPE, VRF, AGE, and COLLECTED. The table contains 20 rows of data, showing various network devices and interfaces associated with the searched MAC address. The 'DEVICE' column includes names like 'AWM-CAS-CORE-SW01', 'AWM-CAS-AGG-SW02', 'AWM-RBA-ACC-SW01', etc. The 'TYPE' column shows 'Dynamic' for most entries. The 'VRF' column shows 'VRF-DC-SHARED' for many entries. The 'AGE' column shows values like 142, 27, 121, 4, and 142. The 'COLLECTED' column shows timestamps like '2026-07-31T14:02:51'.

MAC ADDRESS	IP ADDRESS	VLAN	INTERFACE	DEVICE	TYPE	VRF	AGE	COLLECTED
00:1c:b3:07:7b:29	-	10	Gi1/0/1	AWM-CAS-CORE-SW01	Dynamic	-	-	2026-07-31T14:02:51
00:1c:b3:07:7b:29	-	10	Gi1/0/1	AWM-CAS-AGG-SW02	Dynamic	-	-	2026-07-31T14:02:51
00:1c:b3:07:7b:29	-	10	Gi1/0/1	AWM-RBA-ACC-SW01	Dynamic	-	-	2026-07-31T14:02:51
00:1c:b3:07:7b:29	-	10	Gi1/0/1	AWM-RMA-ACC-SW01	Dynamic	-	-	2026-07-31T14:02:51
00:1c:b3:07:7b:29	-	10	Gi1/0/1	AWM-TNG-AGG-SW01	Dynamic	-	-	2026-07-31T14:02:51
00:1c:b3:07:7b:29	-	10	Gi1/0/1	AWM-FES-AGG-SW01	Dynamic	-	-	2026-07-31T14:02:51
00:1c:b3:07:7b:29	-	10	Gi1/0/1	AWM-AGA-AGG-SW01	Dynamic	-	-	2026-07-31T14:02:51
00:1c:b3:07:7b:29	-	10	Gi1/0/1	AWM-OLD-AGG-SW01	Dynamic	-	-	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	100	Gi1/0/4	AWM-CAS-CORE-SW02	Dynamic	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	100	ethernet1/10	AWM-CAS-DC-LF01	Dynamic	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	100	ethernet1/1	AWM-CAS-DC-LF02	Dynamic	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	100	ethernet1/1	AWM-CAS-DC-LF04	Dynamic	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	100	Gi1/0/4	AWM-CAS-ACC-SW01	Dynamic	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	100	Gi1/0/4	AWM-RBA-ACC-SW02	Dynamic	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	100	Gi1/0/4	AWM-MRT-ACC-SW01	Dynamic	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	100	Gi1/0/4	AWM-TNG-ACC-SW01	Dynamic	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	100	Gi1/0/4	AWM-FES-ACC-SW01	Dynamic	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	100	Gi1/0/4	AWM-AGA-ACC-SW01	Dynamic	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	-	Vlan100	AWM-CAS-DC-LF01	Arp	VRF-DC-SHARED	27	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	-	Vlan100	AWM-CAS-DC-LF02	Arp	VRF-DC-SHARED	121	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	-	Vlan100	AWM-CAS-DC-LF03	Arp	VRF-DC-SHARED	4	2026-07-31T14:02:51
00:1c:b3:08:96:1a	19.100.8.108	-	Vlan100	AWM-CAS-DC-LF04	Arp	VRF-DC-SHARED	142	2026-07-31T14:02:51
00:1c:b3:25:38:53	-	20	Gi1/0/2	AWM-CAS-DC-SF02	Dynamic	-	-	2026-07-31T14:02:51
00:1c:b3:25:38:53	-	20	Gi1/0/2	AWM-CAS-DC-SF04	Dynamic	-	-	2026-07-31T14:02:51

WORTH KNOWING

A manufacturer prefix is not proof of a device type. It tells you who made the network chip, which on a virtualised host is the hypervisor vendor rather than the machine's.

Results are capped for display. Narrow the prefix, or filter by device, if the list is longer than the page shows.

- 4 The block is headed ARP Table. NacTrack knows this address only because routers resolved it, which means it is something connected to the network rather than part of it.

The screenshot shows the NacTrack IP Finder tool. The search bar contains '10.100.0.103'. Below the search bar, the 'ARP Table' is displayed with 4 entries. The table has columns: HOSTNAME, IP ADDRESS, MAC ADDRESS, INTERFACE, VRF, and DETAILS.

HOSTNAME	IP ADDRESS	MAC ADDRESS	INTERFACE	VRF	DETAILS
AWM-CAS-DC-LF01	10.100.0.103	3c:97:0e:68:41:41	Vlan100	VRF-DC-SHARED	dynamic Age: 229
AWM-CAS-DC-LF02	10.100.0.103	3c:97:0e:68:41:41	Vlan100	VRF-DC-SHARED	dynamic Age: 81
AWM-CAS-DC-LF03	10.100.0.103	3c:97:0e:68:41:41	Vlan100	VRF-DC-SHARED	dynamic Age: 197
AWM-CAS-DC-LF04	10.100.0.103	3c:97:0e:68:41:41	Vlan100	VRF-DC-SHARED	dynamic Age: 50

- 5 Now clear the field and search a device management address instead.
- 6 The heading has changed to Inventory, and a second block has appeared for the LLDP neighbour that sees this address. Same search box, same syntax, and the answer tells you what kind of thing you found.

The screenshot shows the NacTrack IP Finder tool. The search bar contains '10.250.10.124'. Below the search bar, the 'Ports' section is displayed with 1 entry. The table has columns: HOSTNAME, INTERFACE, DESCRIPTION, IP ADDRESS, PREFIX, VRF, VLAN, MODE, STATUS, SPEED, DUPLEX, BUNDLE ID, and BUNDLE MODE.

HOSTNAME	INTERFACE	DESCRIPTION	IP ADDRESS	PREFIX	VRF	VLAN	MODE	STATUS	SPEED	DUPLEX	BUNDLE ID	BUNDLE MODE
AWM-CAS-RR01	DiagbleEthernet0/0/0	Management	10.250.10.124		default	-		UP	10000	full		

WORTH KNOWING

The sections that appear depend entirely on what was collected. An endpoint that no router has ARPed since the last collection will not appear at all, even though it is connected.

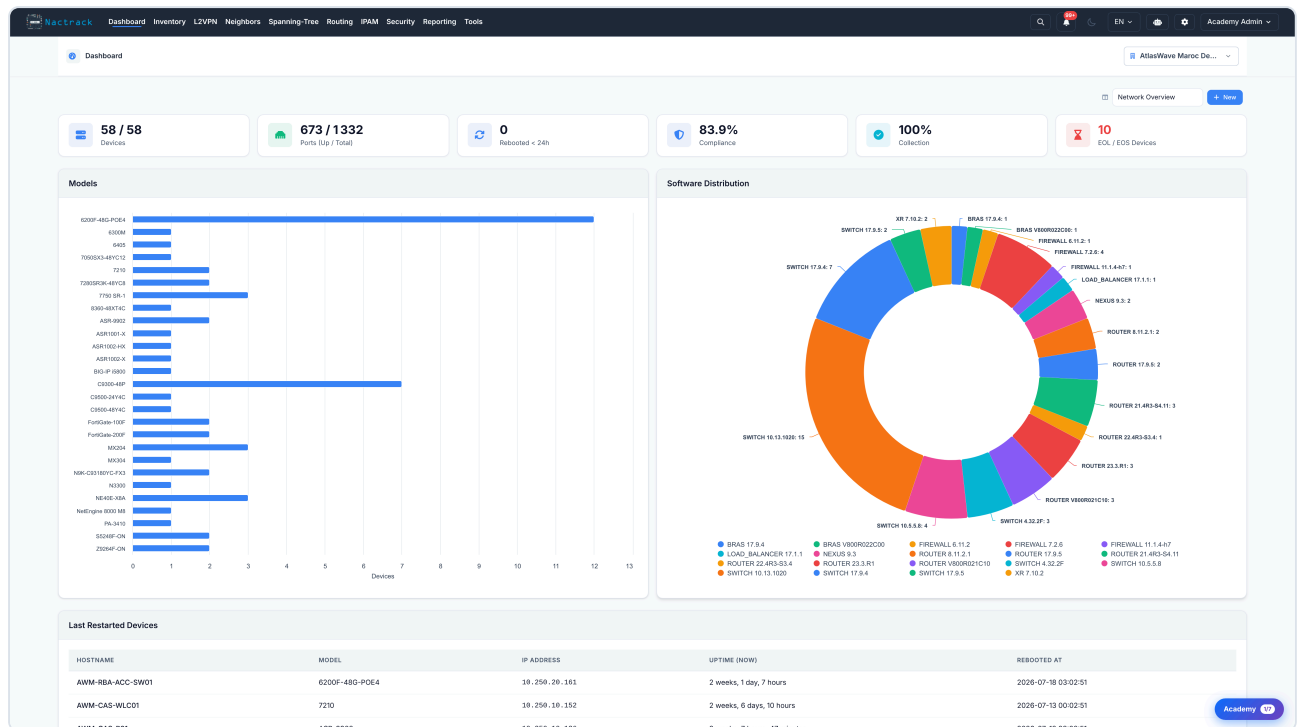
An address can legitimately appear under several sources at once. That is confirmation, not a conflict.

How to find every port carrying a VLAN

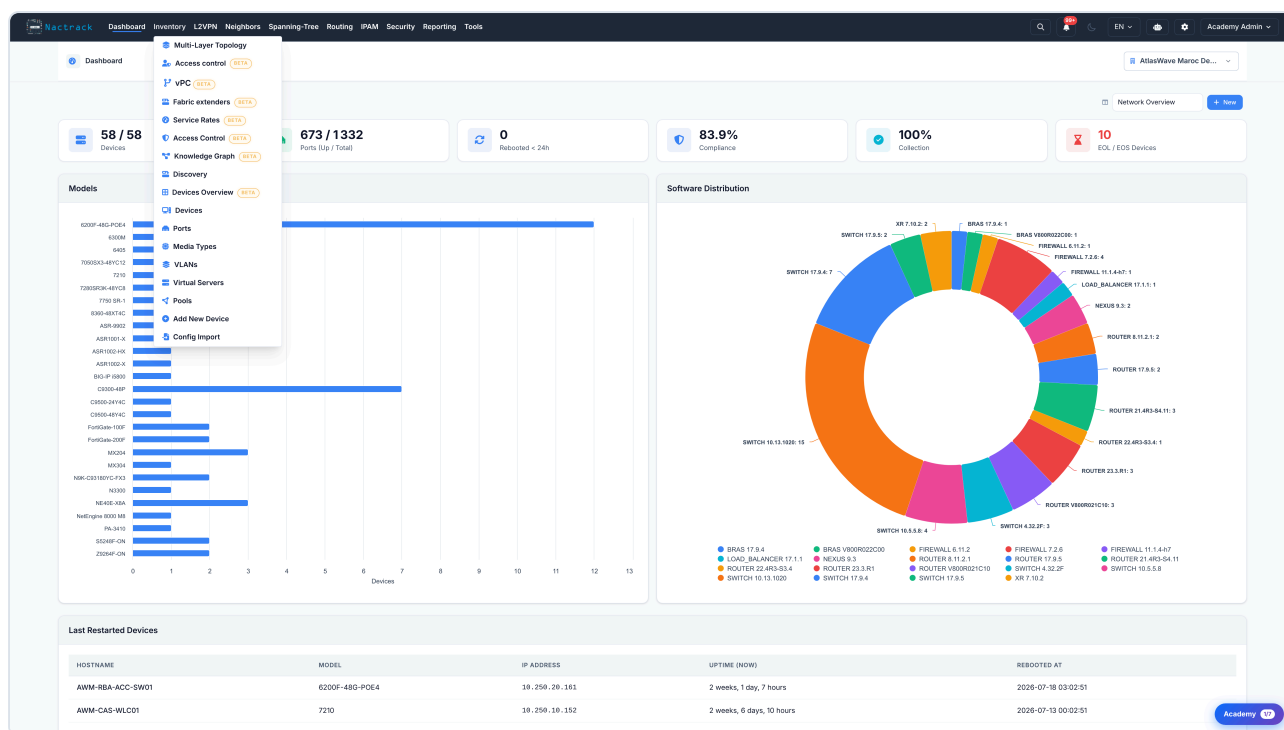
Before you change or retire a VLAN you need to know what is actually using it. The VLAN inventory lists every VLAN found on every switch, with the ports assigned to it, so one page answers the question across the whole estate instead of one switch at a time.

Requires: module: inventory, permission: view_inventory

- 1 We start on the dashboard. A VLAN question is an inventory question, not a troubleshooting one, so this time we go to a different menu.



- 2 Open the Inventory menu. This is where NacTrack keeps what it found rather than what you asked about: devices, ports, VLANs, and the rest of the collected estate.

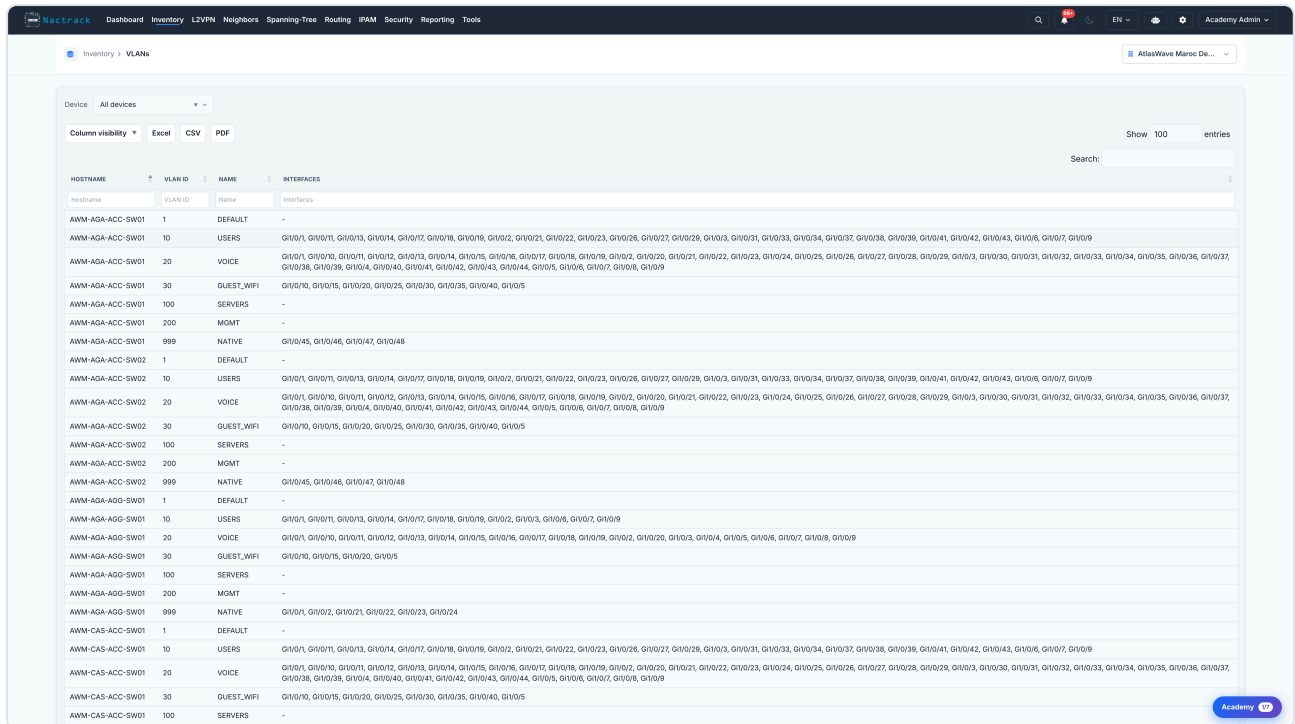


- 3 Choose VLANs. Every row is one VLAN on one switch, so the same VLAN id appears once per device that carries it. The Interfaces column is the answer to our question: the ports on that switch assigned to that VLAN.

The screenshot displays the NacTrack Inventory VLANs table. The table has the following columns: Hostname, VLAN ID, Name, and Interfaces. The data is as follows:

Hostname	VLAN ID	Name	Interfaces
AWM-AGA-ACC-SW01	1	DEFAULT	-
AWM-AGA-ACC-SW01	10	USERS	G1/0/1, G1/0/11, G1/0/13, G1/0/14, G1/0/17, G1/0/18, G1/0/19, G1/0/21, G1/0/22, G1/0/23, G1/0/26, G1/0/27, G1/0/28, G1/0/31, G1/0/33, G1/0/34, G1/0/37, G1/0/38, G1/0/39, G1/0/41, G1/0/42, G1/0/43, G1/0/46, G1/0/7, G1/0/9
AWM-AGA-ACC-SW01	20	VOICE	G1/0/1, G1/0/11, G1/0/12, G1/0/13, G1/0/14, G1/0/15, G1/0/16, G1/0/17, G1/0/18, G1/0/19, G1/0/21, G1/0/22, G1/0/23, G1/0/24, G1/0/25, G1/0/26, G1/0/27, G1/0/28, G1/0/29, G1/0/30, G1/0/31, G1/0/32, G1/0/33, G1/0/34, G1/0/35, G1/0/36, G1/0/37, G1/0/38, G1/0/39, G1/0/40, G1/0/41, G1/0/42, G1/0/43, G1/0/44, G1/0/45, G1/0/46, G1/0/7, G1/0/8, G1/0/9
AWM-AGA-ACC-SW01	30	GUEST_WIFI	G1/0/10, G1/0/15, G1/0/20, G1/0/25, G1/0/30, G1/0/35, G1/0/40, G1/0/5
AWM-AGA-ACC-SW01	100	SERVERS	-
AWM-AGA-ACC-SW01	200	MGMT	-
AWM-AGA-ACC-SW01	999	NATIVE	G1/0/45, G1/0/46, G1/0/47, G1/0/48
AWM-AGA-ACC-SW02	1	DEFAULT	-
AWM-AGA-ACC-SW02	10	USERS	G1/0/1, G1/0/11, G1/0/13, G1/0/14, G1/0/17, G1/0/18, G1/0/19, G1/0/21, G1/0/22, G1/0/23, G1/0/26, G1/0/27, G1/0/28, G1/0/31, G1/0/33, G1/0/34, G1/0/37, G1/0/38, G1/0/39, G1/0/41, G1/0/42, G1/0/43, G1/0/46, G1/0/7, G1/0/9
AWM-AGA-ACC-SW02	20	VOICE	G1/0/1, G1/0/11, G1/0/12, G1/0/13, G1/0/14, G1/0/15, G1/0/16, G1/0/17, G1/0/18, G1/0/19, G1/0/21, G1/0/22, G1/0/23, G1/0/24, G1/0/25, G1/0/26, G1/0/27, G1/0/28, G1/0/29, G1/0/30, G1/0/31, G1/0/32, G1/0/33, G1/0/34, G1/0/35, G1/0/36, G1/0/37, G1/0/38, G1/0/39, G1/0/40, G1/0/41, G1/0/42, G1/0/43, G1/0/44, G1/0/45, G1/0/46, G1/0/7, G1/0/8, G1/0/9
AWM-AGA-ACC-SW02	30	GUEST_WIFI	G1/0/10, G1/0/15, G1/0/20, G1/0/25, G1/0/30, G1/0/35, G1/0/40, G1/0/5
AWM-AGA-ACC-SW02	100	SERVERS	-
AWM-AGA-ACC-SW02	200	MGMT	-
AWM-AGA-ACC-SW02	999	NATIVE	G1/0/45, G1/0/46, G1/0/47, G1/0/48
AWM-AGA-ACC-SW01	1	DEFAULT	-
AWM-AGA-ACC-SW01	10	USERS	G1/0/1, G1/0/11, G1/0/13, G1/0/14, G1/0/17, G1/0/18, G1/0/19, G1/0/21, G1/0/22, G1/0/23, G1/0/26, G1/0/27, G1/0/28, G1/0/31, G1/0/33, G1/0/34, G1/0/37, G1/0/38, G1/0/39, G1/0/41, G1/0/42, G1/0/43, G1/0/46, G1/0/7, G1/0/9
AWM-AGA-ACC-SW01	20	VOICE	G1/0/1, G1/0/11, G1/0/12, G1/0/13, G1/0/14, G1/0/15, G1/0/16, G1/0/17, G1/0/18, G1/0/19, G1/0/21, G1/0/22, G1/0/23, G1/0/24, G1/0/25, G1/0/26, G1/0/27, G1/0/28, G1/0/29, G1/0/30, G1/0/31, G1/0/32, G1/0/33, G1/0/34, G1/0/35, G1/0/36, G1/0/37, G1/0/38, G1/0/39, G1/0/40, G1/0/41, G1/0/42, G1/0/43, G1/0/44, G1/0/45, G1/0/46, G1/0/7, G1/0/8, G1/0/9
AWM-AGA-ACC-SW01	30	GUEST_WIFI	G1/0/10, G1/0/15, G1/0/20, G1/0/25, G1/0/30, G1/0/35, G1/0/40, G1/0/5
AWM-AGA-ACC-SW01	100	SERVERS	-
AWM-AGA-ACC-SW01	200	MGMT	-
AWM-AGA-ACC-SW01	999	NATIVE	G1/0/1, G1/0/21, G1/0/22, G1/0/23, G1/0/24
AWM-AGA-ACC-SW01	1	DEFAULT	-
AWM-AGA-ACC-SW01	10	USERS	G1/0/1, G1/0/11, G1/0/13, G1/0/14, G1/0/17, G1/0/18, G1/0/19, G1/0/21, G1/0/22, G1/0/23, G1/0/26, G1/0/27, G1/0/28, G1/0/31, G1/0/33, G1/0/34, G1/0/37, G1/0/38, G1/0/39, G1/0/41, G1/0/42, G1/0/43, G1/0/46, G1/0/7, G1/0/9
AWM-AGA-ACC-SW01	20	VOICE	G1/0/1, G1/0/11, G1/0/12, G1/0/13, G1/0/14, G1/0/15, G1/0/16, G1/0/17, G1/0/18, G1/0/19, G1/0/21, G1/0/22, G1/0/23, G1/0/24, G1/0/25, G1/0/26, G1/0/27, G1/0/28, G1/0/29, G1/0/30, G1/0/31, G1/0/32, G1/0/33, G1/0/34, G1/0/35, G1/0/36, G1/0/37, G1/0/38, G1/0/39, G1/0/40, G1/0/41, G1/0/42, G1/0/43, G1/0/44, G1/0/45, G1/0/46, G1/0/7, G1/0/8, G1/0/9
AWM-AGA-ACC-SW01	30	GUEST_WIFI	G1/0/10, G1/0/15, G1/0/20, G1/0/25, G1/0/30, G1/0/35, G1/0/40, G1/0/5
AWM-AGA-ACC-SW01	100	SERVERS	-

- 4 Read a single row left to right: the switch, the VLAN id, the name the switch gives it, and the ports carrying it. A VLAN that is defined but has no ports assigned shows a dash, which is worth noticing before you assume it is in use.



The screenshot shows the Hactrack web interface, specifically the 'Inventory > VLANs' section. The table displays VLAN configurations for various switches, including AWM-AGA-ACC-SW01, AWM-AGA-ACC-SW02, AWM-AGA-ACC-SW03, AWM-AGA-ACC-SW04, AWM-AGA-ACC-SW05, AWM-AGA-ACC-SW06, AWM-AGA-ACC-SW07, AWM-AGA-ACC-SW08, AWM-AGA-ACC-SW09, AWM-AGA-ACC-SW10, AWM-AGA-ACC-SW11, AWM-AGA-ACC-SW12, AWM-AGA-ACC-SW13, AWM-AGA-ACC-SW14, AWM-AGA-ACC-SW15, AWM-AGA-ACC-SW16, AWM-AGA-ACC-SW17, AWM-AGA-ACC-SW18, AWM-AGA-ACC-SW19, AWM-AGA-ACC-SW20, AWM-AGA-ACC-SW21, AWM-AGA-ACC-SW22, AWM-AGA-ACC-SW23, AWM-AGA-ACC-SW24, AWM-AGA-ACC-SW25, AWM-AGA-ACC-SW26, AWM-AGA-ACC-SW27, AWM-AGA-ACC-SW28, AWM-AGA-ACC-SW29, AWM-AGA-ACC-SW30, AWM-AGA-ACC-SW31, AWM-AGA-ACC-SW32, AWM-AGA-ACC-SW33, AWM-AGA-ACC-SW34, AWM-AGA-ACC-SW35, AWM-AGA-ACC-SW36, AWM-AGA-ACC-SW37, AWM-AGA-ACC-SW38, AWM-AGA-ACC-SW39, AWM-AGA-ACC-SW40, AWM-AGA-ACC-SW41, AWM-AGA-ACC-SW42, AWM-AGA-ACC-SW43, AWM-AGA-ACC-SW44, AWM-AGA-ACC-SW45, AWM-AGA-ACC-SW46, AWM-AGA-ACC-SW47, AWM-AGA-ACC-SW48, AWM-AGA-ACC-SW49, AWM-AGA-ACC-SW50, AWM-AGA-ACC-SW51, AWM-AGA-ACC-SW52, AWM-AGA-ACC-SW53, AWM-AGA-ACC-SW54, AWM-AGA-ACC-SW55, AWM-AGA-ACC-SW56, AWM-AGA-ACC-SW57, AWM-AGA-ACC-SW58, AWM-AGA-ACC-SW59, AWM-AGA-ACC-SW60, AWM-AGA-ACC-SW61, AWM-AGA-ACC-SW62, AWM-AGA-ACC-SW63, AWM-AGA-ACC-SW64, AWM-AGA-ACC-SW65, AWM-AGA-ACC-SW66, AWM-AGA-ACC-SW67, AWM-AGA-ACC-SW68, AWM-AGA-ACC-SW69, AWM-AGA-ACC-SW70, AWM-AGA-ACC-SW71, AWM-AGA-ACC-SW72, AWM-AGA-ACC-SW73, AWM-AGA-ACC-SW74, AWM-AGA-ACC-SW75, AWM-AGA-ACC-SW76, AWM-AGA-ACC-SW77, AWM-AGA-ACC-SW78, AWM-AGA-ACC-SW79, AWM-AGA-ACC-SW80, AWM-AGA-ACC-SW81, AWM-AGA-ACC-SW82, AWM-AGA-ACC-SW83, AWM-AGA-ACC-SW84, AWM-AGA-ACC-SW85, AWM-AGA-ACC-SW86, AWM-AGA-ACC-SW87, AWM-AGA-ACC-SW88, AWM-AGA-ACC-SW89, AWM-AGA-ACC-SW90, AWM-AGA-ACC-SW91, AWM-AGA-ACC-SW92, AWM-AGA-ACC-SW93, AWM-AGA-ACC-SW94, AWM-AGA-ACC-SW95, AWM-AGA-ACC-SW96, AWM-AGA-ACC-SW97, AWM-AGA-ACC-SW98, AWM-AGA-ACC-SW99, AWM-AGA-ACC-SW100.

Device	VLAN ID	Name	Interfaces
AWM-AGA-ACC-SW01	1	DEFAULT	-
AWM-AGA-ACC-SW01	10	USERS	Gi1/0/1, Gi1/0/11, Gi1/0/13, Gi1/0/14, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/2, Gi1/0/21, Gi1/0/22, Gi1/0/23, Gi1/0/26, Gi1/0/27, Gi1/0/29, Gi1/0/3, Gi1/0/31, Gi1/0/33, Gi1/0/34, Gi1/0/37, Gi1/0/38, Gi1/0/39, Gi1/0/41, Gi1/0/42, Gi1/0/43, Gi1/0/46, Gi1/0/7, Gi1/0/9
AWM-AGA-ACC-SW01	20	VOICE	Gi1/0/1, Gi1/0/10, Gi1/0/11, Gi1/0/12, Gi1/0/13, Gi1/0/14, Gi1/0/15, Gi1/0/16, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/2, Gi1/0/20, Gi1/0/21, Gi1/0/22, Gi1/0/23, Gi1/0/24, Gi1/0/25, Gi1/0/26, Gi1/0/27, Gi1/0/28, Gi1/0/29, Gi1/0/3, Gi1/0/30, Gi1/0/31, Gi1/0/32, Gi1/0/33, Gi1/0/34, Gi1/0/35, Gi1/0/36, Gi1/0/37, Gi1/0/38, Gi1/0/39, Gi1/0/4, Gi1/0/40, Gi1/0/43, Gi1/0/45, Gi1/0/46, Gi1/0/47, Gi1/0/8, Gi1/0/9
AWM-AGA-ACC-SW01	30	GUEST_WIFI	Gi1/0/10, Gi1/0/15, Gi1/0/20, Gi1/0/25, Gi1/0/30, Gi1/0/35, Gi1/0/40, Gi1/0/5
AWM-AGA-ACC-SW01	100	SERVERS	-
AWM-AGA-ACC-SW01	200	MGMT	-
AWM-AGA-ACC-SW01	999	NATIVE	Gi1/0/45, Gi1/0/46, Gi1/0/47, Gi1/0/48
AWM-AGA-ACC-SW02	1	DEFAULT	-
AWM-AGA-ACC-SW02	10	USERS	Gi1/0/1, Gi1/0/11, Gi1/0/13, Gi1/0/14, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/2, Gi1/0/21, Gi1/0/22, Gi1/0/23, Gi1/0/26, Gi1/0/27, Gi1/0/29, Gi1/0/3, Gi1/0/31, Gi1/0/33, Gi1/0/34, Gi1/0/37, Gi1/0/38, Gi1/0/39, Gi1/0/41, Gi1/0/42, Gi1/0/43, Gi1/0/46, Gi1/0/7, Gi1/0/9
AWM-AGA-ACC-SW02	20	VOICE	Gi1/0/1, Gi1/0/10, Gi1/0/11, Gi1/0/12, Gi1/0/13, Gi1/0/14, Gi1/0/15, Gi1/0/16, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/2, Gi1/0/20, Gi1/0/21, Gi1/0/22, Gi1/0/23, Gi1/0/24, Gi1/0/25, Gi1/0/26, Gi1/0/27, Gi1/0/28, Gi1/0/29, Gi1/0/3, Gi1/0/30, Gi1/0/31, Gi1/0/32, Gi1/0/33, Gi1/0/34, Gi1/0/35, Gi1/0/36, Gi1/0/37, Gi1/0/38, Gi1/0/39, Gi1/0/4, Gi1/0/40, Gi1/0/43, Gi1/0/45, Gi1/0/46, Gi1/0/47, Gi1/0/8, Gi1/0/9
AWM-AGA-ACC-SW02	30	GUEST_WIFI	Gi1/0/10, Gi1/0/15, Gi1/0/20, Gi1/0/25, Gi1/0/30, Gi1/0/35, Gi1/0/40, Gi1/0/5
AWM-AGA-ACC-SW02	100	SERVERS	-
AWM-AGA-ACC-SW02	200	MGMT	-
AWM-AGA-ACC-SW02	999	NATIVE	Gi1/0/45, Gi1/0/46, Gi1/0/47, Gi1/0/48
AWM-AGA-ACC-SW03	1	DEFAULT	-
AWM-AGA-ACC-SW03	10	USERS	Gi1/0/1, Gi1/0/11, Gi1/0/13, Gi1/0/14, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/2, Gi1/0/3, Gi1/0/6, Gi1/0/7, Gi1/0/9
AWM-AGA-ACC-SW03	20	VOICE	Gi1/0/1, Gi1/0/10, Gi1/0/11, Gi1/0/12, Gi1/0/13, Gi1/0/14, Gi1/0/15, Gi1/0/16, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/2, Gi1/0/20, Gi1/0/3, Gi1/0/4, Gi1/0/5, Gi1/0/6, Gi1/0/7, Gi1/0/8, Gi1/0/9
AWM-AGA-ACC-SW03	30	GUEST_WIFI	Gi1/0/10, Gi1/0/15, Gi1/0/20, Gi1/0/5
AWM-AGA-ACC-SW03	100	SERVERS	-
AWM-AGA-ACC-SW03	200	MGMT	-
AWM-AGA-ACC-SW03	999	NATIVE	Gi1/0/1, Gi1/0/2, Gi1/0/21, Gi1/0/22, Gi1/0/23, Gi1/0/24
AWM-AGA-ACC-SW04	1	DEFAULT	-
AWM-AGA-ACC-SW04	10	USERS	Gi1/0/1, Gi1/0/11, Gi1/0/13, Gi1/0/14, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/2, Gi1/0/21, Gi1/0/22, Gi1/0/23, Gi1/0/26, Gi1/0/27, Gi1/0/29, Gi1/0/3, Gi1/0/31, Gi1/0/33, Gi1/0/34, Gi1/0/37, Gi1/0/38, Gi1/0/39, Gi1/0/41, Gi1/0/42, Gi1/0/43, Gi1/0/46, Gi1/0/7, Gi1/0/9
AWM-AGA-ACC-SW04	20	VOICE	Gi1/0/1, Gi1/0/10, Gi1/0/11, Gi1/0/12, Gi1/0/13, Gi1/0/14, Gi1/0/15, Gi1/0/16, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/2, Gi1/0/20, Gi1/0/21, Gi1/0/22, Gi1/0/23, Gi1/0/24, Gi1/0/25, Gi1/0/26, Gi1/0/27, Gi1/0/28, Gi1/0/29, Gi1/0/3, Gi1/0/30, Gi1/0/31, Gi1/0/32, Gi1/0/33, Gi1/0/34, Gi1/0/35, Gi1/0/36, Gi1/0/37, Gi1/0/38, Gi1/0/39, Gi1/0/4, Gi1/0/40, Gi1/0/43, Gi1/0/45, Gi1/0/46, Gi1/0/47, Gi1/0/8, Gi1/0/9
AWM-AGA-ACC-SW04	30	GUEST_WIFI	Gi1/0/10, Gi1/0/15, Gi1/0/20, Gi1/0/25, Gi1/0/30, Gi1/0/35, Gi1/0/40, Gi1/0/5
AWM-AGA-ACC-SW04	100	SERVERS	-
AWM-AGA-ACC-SW05	1	DEFAULT	-
AWM-AGA-ACC-SW05	10	USERS	Gi1/0/1, Gi1/0/11, Gi1/0/13, Gi1/0/14, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/2, Gi1/0/3, Gi1/0/6, Gi1/0/7, Gi1/0/9
AWM-AGA-ACC-SW05	20	VOICE	Gi1/0/1, Gi1/0/10, Gi1/0/11, Gi1/0/12, Gi1/0/13, Gi1/0/14, Gi1/0/15, Gi1/0/16, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/2, Gi1/0/20, Gi1/0/3, Gi1/0/4, Gi1/0/5, Gi1/0/6, Gi1/0/7, Gi1/0/8, Gi1/0/9
AWM-AGA-ACC-SW05	30	GUEST_WIFI	Gi1/0/10, Gi1/0/15, Gi1/0/20, Gi1/0/5
AWM-AGA-ACC-SW05	100	SERVERS	-
AWM-AGA-ACC-SW05	200	MGMT	-
AWM-AGA-ACC-SW05	999	NATIVE	Gi1/0/1, Gi1/0/2, Gi1/0/21, Gi1/0/22, Gi1/0/23, Gi1/0/24
AWM-AGA-ACC-SW06	1	DEFAULT	-
AWM-AGA-ACC-SW06	10	USERS	Gi1/0/1, Gi1/0/11, Gi1/0/13, Gi1/0/14, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/2, Gi1/0/21, Gi1/0/22, Gi1/0/23, Gi1/0/26, Gi1/0/27, Gi1/0/29, Gi1/0/3, Gi1/0/31, Gi1/0/33, Gi1/0/34, Gi1/0/37, Gi1/0/38, Gi1/0/39, Gi1/0/41, Gi1/0/42, Gi1/0/43, Gi1/0/46, Gi1/0/7, Gi1/0/9
AWM-AGA-ACC-SW06	20	VOICE	Gi1/0/1, Gi1/0/10, Gi1/0/11, Gi1/0/12, Gi1/0/13, Gi1/0/14, Gi1/0/15, Gi1/0/16, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/2, Gi1/0/20, Gi1/0/21, Gi1/0/22, Gi1/0/23, Gi1/0/24, Gi1/0/25, Gi1/0/26, Gi1/0/27, Gi1/0/28, Gi1/0/29, Gi1/0/3, Gi1/0/30, Gi1/0/31, Gi1/0/32, Gi1/0/33, Gi1/0/34, Gi1/0/35, Gi1/0/36, Gi1/0/37, Gi1/0/38, Gi1/0/39, Gi1/0/4, Gi1/0/40, Gi1/0/43, Gi1/0/45, Gi1/0/46, Gi1/0/47, Gi1/0/8, Gi1/0/9
AWM-AGA-ACC-SW06	30	GUEST_WIFI	Gi1/0/10, Gi1/0/15, Gi1/0/20, Gi1/0/25, Gi1/0/30, Gi1/0/35, Gi1/0/40, Gi1/0/5
AWM-AGA-ACC-SW06	100	SERVERS	-

WORTH KNOWING

The Interfaces column is built from access, voice and native VLAN assignments only. It does NOT read the trunk allowed-VLAN list, so a VLAN carried across an uplink does not appear here. To see that, look at the Allowed VLANs column on the Ports page.

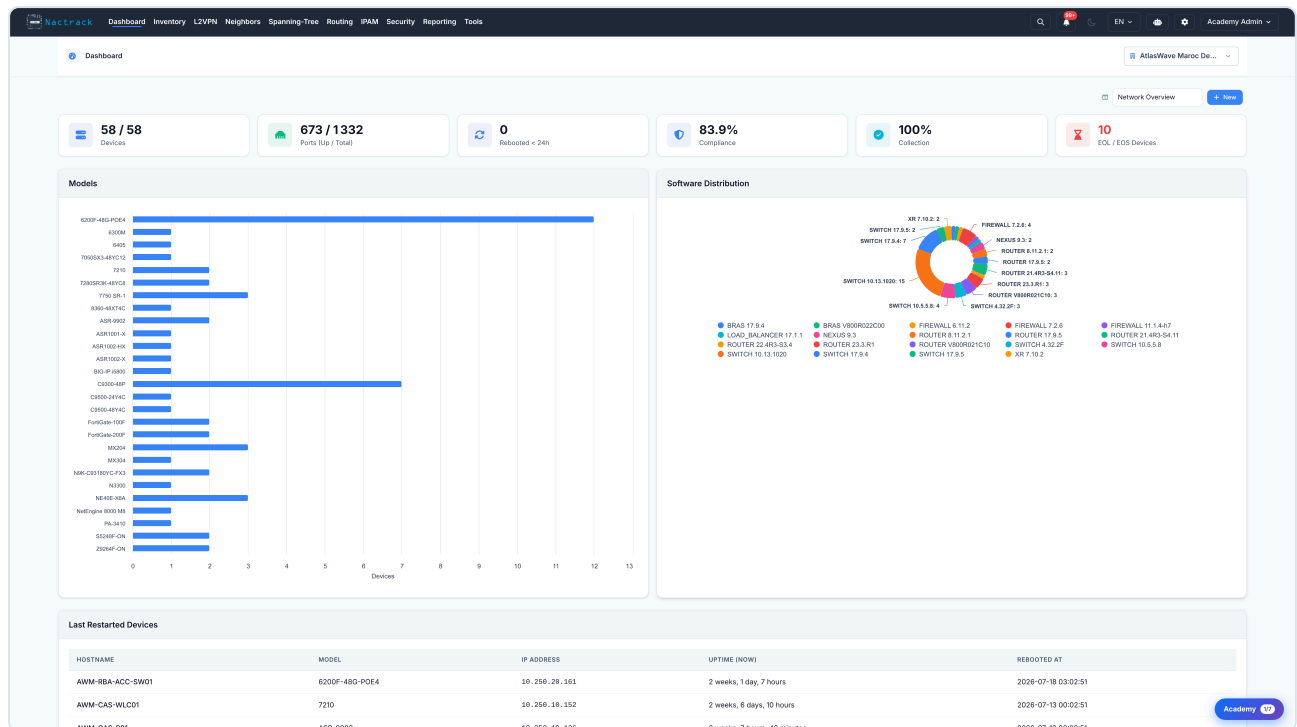
The same VLAN id on two switches is not necessarily the same layer 2 domain. It is the same domain only if a path carries it between them.

How to see which VLANs a trunk allows

A VLAN reaches a remote switch only if every trunk along the way allows it, so when a VLAN is missing at one site the allowed list is the first thing to check. The Ports inventory shows the allowed VLANs and the native VLAN for every trunk in the estate, side by side.

Requires: module: inventory, permission: view_inventory

- 1 From the dashboard again. Trunk configuration is collected interface state, so it lives under Inventory with the rest of the port data.



- 2 Open Inventory and choose Ports. Every physical and logical interface NacTrack collected is here, one row each, which is why the table is wide: it carries the VLAN, speed, duplex, media and VRF for each one.

Nactrack Dashboard Inventory L2VPN Neighbors Spanning-Tree Routing IPAM Security Reporting Tools

Inventory > Ports

AtlasWave Maroc De... ▾

Device: All devices ▾ Only physical ports

Column visibility ▾ Excel CSV PDF

Show 100 entries

Search:

HOSTNAME	NAME	DESCRIPTION	IP ADDRESS	ACCESS VLAN	VOICE VLAN	NATIVE VLAN	ALLOWED VLANS	MODE	STATUS	BUNDLE ID	BUNDLE MODE	MEDIA TYPE	VRF	SPEED	DUPLEX	INTERFACE TYPE	CONFIG	24h TREND
Hostname	Name	Description	IP Address	Access VLAN	Voice VLAN	Native VLAN	Allowed VLANs	Mode	Status	Bundle ID	Bundle Mode	Media Type	VRF	Speed	Duplex	Interface Type	Con	24h T
AWM-AGA-ACC-SW01	G1/0/1	Aggrdr user access port 01	unassigned	10	20	-	-	access	UP			1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/10	Aggrdr user access port 10	unassigned	30	20	-	-	access	UP			1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/11	Aggrdr user access port 11	unassigned	10	20	-	-	access	UP			1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/12	Aggrdr user access port 12	unassigned	20		-	-	access	UP			1000BASE-T	default	1000		physical	View config	
AWM-AGA-ACC-SW01	G1/0/13	Aggrdr user access port 13	unassigned	10	20	-	-	access	UP			1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/14	Aggrdr user access port 14	unassigned	10	20	-	-	access	UP			1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/15	Aggrdr user access port 15	unassigned	30	20	-	-	access	UP			1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/16	Aggrdr user access port 16	unassigned	20		-	-	access	UP			1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/17	Aggrdr user access port 17	unassigned	10	20	-	-	access	UP			1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/18	Aggrdr user access port 18	unassigned	10	20	-	-	access	UP			1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/19	Aggrdr user access port 19	unassigned	10	20	-	-	access	UP			1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/2	Aggrdr user access port 02	unassigned	10	20	-	-	access	UP			1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/20	Aggrdr user access port 20	unassigned	30	20	-	-	access	UP			1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/21	Aggrdr user access port 21	unassigned	10	20	-	-	access	UP			1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/22	Aggrdr user access port 22	unassigned	10	20	-	-	access	UP			1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/23	Aggrdr user access port 23	unassigned	10	20	-	-	access	UP			1000BASE-T	default	1000	full	physical	View config	
AWM-AGA-ACC-SW01	G1/0/24	Aggrdr user access port 24	unassigned	20		-	-	access	UP			1000BASE-T	default	1000	full	physical	View config	

Academy 92

- 3 Four columns answer the VLAN question. Access VLAN and Voice VLAN apply to access ports. Native VLAN and Allowed VLANs apply to trunks: the allowed list is exactly what the trunk will carry, and anything absent from it is silently dropped at that hop.

Device		All devices	☒ Only physical ports															
Column visibility		Excel	CSV	PDF														
		Show 100 entries																
Hostname		Name	Description	IP Address	Access VLAN	Voice VLAN	Native VLAN	Allowed VLANs	Mode	Status	Bundle ID	Bundle Mode	Media Type	VRF	Speed	Duplex	Interface Type	Config
Hostname		Name	Description	IP Address	Access VLAN	Voice VLAN	Native VLAN	Allowed VLANs	Mode	Status	Bundle ID	Bundle Mode	Media Type	VRF	Speed	Duplex	Interface Type	Con
AWM-AGA-ACC-SW01	G1/0/1	Aggrdr user access port 01	unassigned	10	20	-	-	-	access	UP	-	-	1000BASE-T	default	1000	full	physical	View config
	G1/0/10	Aggrdr user access port 10	unassigned	30	20	-	-	-	access	UP	-	-	1000BASE-T	default	1000	full	physical	View config
	G1/0/11	Aggrdr user access port 11	unassigned	10	20	-	-	-	access	UP	-	-	1000BASE-T	default	1000	full	physical	View config
	G1/0/12	Aggrdr user access port 12	unassigned	20	-	-	-	-	access	UP	-	-	1000BASE-T	default	1000	full	physical	View config
	G1/0/13	Aggrdr user access port 13	unassigned	10	20	-	-	-	access	UP	-	-	1000BASE-T	default	1000	full	physical	View config
	G1/0/14	Aggrdr user access port 14	unassigned	10	20	-	-	-	access	UP	-	-	1000BASE-T	default	1000	full	physical	View config
	G1/0/15	Aggrdr user access port 15	unassigned	30	20	-	-	-	access	UP	-	-	1000BASE-T	default	1000	full	physical	View config
	G1/0/16	Aggrdr user access port 16	unassigned	20	-	-	-	-	access	UP	-	-	1000BASE-T	default	1000	full	physical	View config
	G1/0/17	Aggrdr user access port 17	unassigned	10	20	-	-	-	access	UP	-	-	1000BASE-T	default	1000	full	physical	View config
	G1/0/18	Aggrdr user access port 18	unassigned	10	20	-	-	-	access	UP	-	-	1000BASE-T	default	1000	full	physical	View config
	G1/0/19	Aggrdr user access port 19	unassigned	10	20	-	-	-	access	UP	-	-	1000BASE-T	default	1000	full	physical	View config
	G1/0/2	Aggrdr user access port 02	unassigned	10	20	-	-	-	access	UP	-	-	1000BASE-T	default	1000	full	physical	View config
	G1/0/20	Aggrdr user access port 20	unassigned	30	20	-	-	-	access	UP	-	-	1000BASE-T	default	1000	full	physical	View config
	G1/0/21	Aggrdr user access port 21	unassigned	10	20	-	-	-	access	UP	-	-	1000BASE-T	default	1000	full	physical	View config
	G1/0/22	Aggrdr user access port 22	unassigned	10	20	-	-	-	access	UP	-	-	1000BASE-T	default	1000	full	physical	View config
	G1/0/23	Aggrdr user access port 23	unassigned	10	20	-	-	-	access	UP	-	-	1000BASE-T	default	1000	full	physical	View config
	G1/0/24	Aggrdr user access port 24	unassigned	20	-	-	-	-	access	UP	-	-	1000BASE-T	default	1000	full	physical	View config

WORTH KNOWING

A VLAN present in the allowed list is not necessarily defined on the switch. The allowed list is configuration text; it can name a VLAN that was never created, and the trunk will still carry nothing for it.

Nothing here counts the VLANs on a trunk or ranks trunks by how many they carry. The allowed list is shown as it was configured, and you read it yourself.

How to see which ports are configured for 802.1X

802.1X decides whether a device plugged into a wall socket is allowed onto the network at all. NacTrack reads that configuration back off the switches, so you can see where port authentication was actually deployed rather than where it was meant to be. The gap between the two is usually the point: an access switch installed after the rollout, or a floor that was skipped, keeps its ports open to anyone with a cable.

Requires: module: beta_testing, permission: view_inventory, data: has_dot1x, vendors: Cisco access switches; the fields come from interface configuration **+ beta_testing**

- 1 Port security sits under Inventory, next to the interface views, because what it reports is interface configuration rather than a security product of its own.
- 2 Choose Access control. The page lists only the ports that carry an 802.1X configuration, so its length is itself the answer to how far the rollout got.
- 3 Every row is one authenticated port. The first column names the switch, so reading down it tells you which switches took part and, just as usefully, which never appear at all.

DEVICES	INTERFACE	DESCRIPTION	PORT CONTROL	HOST MODE	MAB	PORT-SECURITY	DATA VLAN
AWM-CAS-ACC-SW01	611/6/1	Casablanca user access port 01	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/38	Casablanca user access port 10	auto	multi-domain	-	-	30
AWM-CAS-ACC-SW01	611/6/31	Casablanca user access port 11	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/32	Casablanca user access port 12	auto	multi-domain	BYPASS	-	20
AWM-CAS-ACC-SW01	611/6/33	Casablanca user access port 13	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/34	Casablanca user access port 14	auto	multi-domain	BYPASS	Enabled (max 2)	10
AWM-CAS-ACC-SW01	611/6/35	Casablanca user access port 15	auto	multi-domain	BYPASS	-	30
AWM-CAS-ACC-SW01	611/6/36	Casablanca user access port 16	auto	multi-domain	-	-	20
AWM-CAS-ACC-SW01	611/6/37	Casablanca user access port 17	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/38	Casablanca user access port 18	auto	multi-domain	BYPASS	-	10
AWM-CAS-ACC-SW01	611/6/39	Casablanca user access port 19	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/2	Casablanca user access port 02	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/28	Casablanca user access port 20	auto	multi-domain	-	-	30
AWM-CAS-ACC-SW01	611/6/21	Casablanca user access port 21	auto	multi-domain	BYPASS	Enabled (max 2)	10
AWM-CAS-ACC-SW01	611/6/22	Casablanca user access port 22	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/23	Casablanca user access port 23	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/24	Casablanca user access port 24	auto	multi-domain	BYPASS	-	20
AWM-CAS-ACC-SW01	611/6/3	Casablanca user access port 03	auto	multi-domain	BYPASS	-	10
AWM-CAS-ACC-SW01	611/6/4	Casablanca user access port 04	auto	multi-domain	-	-	20
AWM-CAS-ACC-SW01	611/6/5	Casablanca user access port 05	auto	multi-domain	-	-	30
AWM-CAS-ACC-SW01	611/6/6	Casablanca user access port 06	auto	multi-domain	BYPASS	-	10
AWM-CAS-ACC-SW01	611/6/7	Casablanca user access port 07	auto	multi-domain	BYPASS	Enabled (max 2)	10
AWM-CAS-ACC-SW01	611/6/8	Casablanca user access port 08	auto	multi-domain	-	-	20
AWM-CAS-ACC-SW01	611/6/9	Casablanca user access port 09	auto	multi-domain	BYPASS	-	10
AWM-CAS-ACC-SW02	611/6/1	Casablanca user access port 01	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW02	611/6/38	Casablanca user access port 10	auto	multi-domain	-	-	30
AWM-CAS-ACC-SW02	611/6/31	Casablanca user access port 11	auto	multi-domain	-	-	10

- 4 Two columns carry the meaning. Port Control set to auto is the one that enforces: the port stays shut until the connected device authenticates. Host Mode says how many devices may share the socket, and multi-domain is the usual choice for a desk, allowing one computer alongside one IP phone.

DEVICES	INTERFACE	DESCRIPTION	PORT CONTROL	HOST MODE	MAB	PORT-SECURITY	DATA VLAN
AWM-CAS-ACC-SW01	611/6/1	Casablanca user access port 01	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/28	Casablanca user access port 10	auto	multi-domain	-	-	30
AWM-CAS-ACC-SW01	611/6/31	Casablanca user access port 11	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/32	Casablanca user access port 12	auto	multi-domain	BYPASS	-	20
AWM-CAS-ACC-SW01	611/6/33	Casablanca user access port 13	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/34	Casablanca user access port 14	auto	multi-domain	BYPASS	Enabled (max 2)	10
AWM-CAS-ACC-SW01	611/6/35	Casablanca user access port 15	auto	multi-domain	BYPASS	-	30
AWM-CAS-ACC-SW01	611/6/36	Casablanca user access port 16	auto	multi-domain	-	-	20
AWM-CAS-ACC-SW01	611/6/37	Casablanca user access port 17	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/38	Casablanca user access port 18	auto	multi-domain	BYPASS	-	10
AWM-CAS-ACC-SW01	611/6/39	Casablanca user access port 19	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/2	Casablanca user access port 02	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/28	Casablanca user access port 20	auto	multi-domain	-	-	30
AWM-CAS-ACC-SW01	611/6/21	Casablanca user access port 21	auto	multi-domain	BYPASS	Enabled (max 2)	10
AWM-CAS-ACC-SW01	611/6/22	Casablanca user access port 22	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/23	Casablanca user access port 23	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW01	611/6/24	Casablanca user access port 24	auto	multi-domain	BYPASS	-	20
AWM-CAS-ACC-SW01	611/6/3	Casablanca user access port 03	auto	multi-domain	BYPASS	-	10
AWM-CAS-ACC-SW01	611/6/4	Casablanca user access port 04	auto	multi-domain	-	-	20
AWM-CAS-ACC-SW01	611/6/5	Casablanca user access port 05	auto	multi-domain	-	-	30
AWM-CAS-ACC-SW01	611/6/6	Casablanca user access port 06	auto	multi-domain	BYPASS	-	10
AWM-CAS-ACC-SW01	611/6/7	Casablanca user access port 07	auto	multi-domain	BYPASS	Enabled (max 2)	10
AWM-CAS-ACC-SW01	611/6/8	Casablanca user access port 08	auto	multi-domain	-	-	20
AWM-CAS-ACC-SW01	611/6/9	Casablanca user access port 09	auto	multi-domain	BYPASS	-	10
AWM-CAS-ACC-SW02	611/6/1	Casablanca user access port 01	auto	multi-domain	-	-	10
AWM-CAS-ACC-SW02	611/6/38	Casablanca user access port 10	auto	multi-domain	-	-	30
AWM-CAS-ACC-SW02	611/6/31	Casablanca user access port 11	auto	multi-domain	-	-	10

WORTH KNOWING

This is configuration, not activity. A port shown as auto is set up to demand authentication; the page does not say whether anything authenticated on it, or whether a supplicant ever tried.

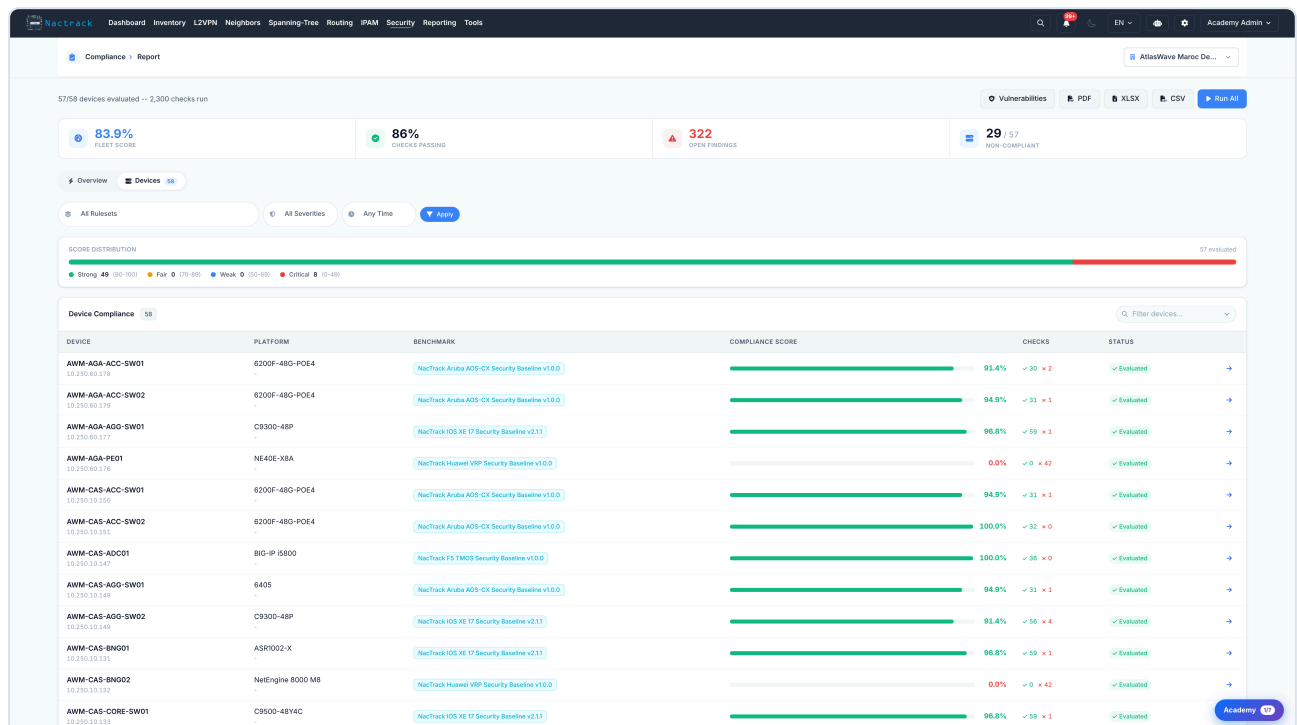
A switch that is missing from the list is not necessarily unprotected. It may be a core or aggregation switch with no user-facing ports, where 802.1X would have nothing to authenticate.

How to check whether a device still allows Telnet

Telnet carries passwords in clear text. Most networks turned it off years ago, which is exactly why the ones still answering on port 23 are easy to miss: they are usually not the devices anyone is worried about. NacTrack evaluates the collected configuration against a hardening benchmark for the platform, so the answer comes from what the device is actually running rather than from what the standard build was supposed to contain.

Requires: module: compliance, permission: view_audit, vendors: All benchmarked platforms; every shipped ruleset carries a Telnet check

- 1 Compliance lives under Security, alongside CVE exposure and lifecycle. All three answer the same kind of question: not what the network is doing, but what state you have left it in.
- 2 Choose Compliance. Every device that has been evaluated appears with the benchmark used for it, a score, and how many checks passed.
- 3 The report opens on its summary. The per-device table sits behind the Devices tab, which is where the detail you want lives.
- 4 A high score is not a clean bill of health. It is a weighted average, so a device can sit in the nineties while still failing one high-severity check. That is the case worth hunting for, because nobody looks twice at a device scoring ninety-five per cent.



- 5 Opening a device lists every check that was run against it. This aggregation switch scores almost ninety-five per cent, and one line is marked FAIL: the Telnet server is still enabled.

The screenshot shows the NacTrack interface for a compliance report. The top navigation bar includes Dashboard, Inventory, L2VPN, Neighbors, Spanning-Tree, Routing, IPAM, Security, Reporting, and Tools. The main header shows the device IP 10.250.10.148, Model 6405, and Benchmark NacTrack Aruba AOS-CX Security Baseline v1.0.0. Below the header is a table with columns: CODE, TITLE, SEVERITY, STATUS, EVIDENCE / DETAILS, RECOMMENDATION, FIX, and WAIVER. The table lists 12 checks, with the second row (NAC-ARU-1.2.telnet-disabled) marked as FAIL. The evidence for this failure is 'Clearnet Telnet server is enabled'. The recommendation is 'Disable the clearnet Telnet server; use SSH instead.' The fix is 'no telnet-server vrf default; no telnet-server vrf mgmt'. The waiver is 'Reason (accepted risk) dd/mm/yyyy'. The table also shows the severity (HIGH), weight (60), and profile (L1) for each check. At the bottom, there is a section for 'Recent Evaluation Jobs' and a 'PDF Report' button.

CODE	TITLE	SEVERITY	STATUS	EVIDENCE / DETAILS	RECOMMENDATION	FIX	WAIVER
NTC-ARU-1.1.ssh-server-vrf	Enable the SSH server on a VRF	HIGH Weight: 60 Profile: L1	PASS	ssh server vrf mgmt	Enable the SSH management server on a routing VRF.	-	-
NTC-ARU-1.2.telnet-disabled	Disable the Telnet server	HIGH Weight: 60 Profile: L1	FAIL	Clearnet Telnet server is enabled	Disable the clearnet Telnet server; use SSH instead.	no telnet-server vrf default; no telnet-server vrf mgmt	Reason (accepted risk) dd/mm/yyyy
NTC-ARU-1.3.https-server-vrf	Restrict the HTTPS/REST server to a VRF	MEDIUM Weight: 40 Profile: L2	PASS	https-server vrf mgmt	Expose the web/REST management interface only on a controlled VRF.	-	-
NTC-ARU-1.4.no-plaintext-http	Disable the plaintext HTTP server	HIGH Weight: 60 Profile: L1	PASS	-	Disable the plaintext HTTP server; use HTTPS only.	-	-
NTC-ARU-1.5.cli-session-timeout	Set CLI idle session timeout to 15 minutes or less	MEDIUM Weight: 40 Profile: L1	PASS	value=10.0	Time out idle management CLI sessions.	-	-
NTC-ARU-1.6.banner-motd	Configure a login banner (message of the day)	LOW Weight: 1 Profile: L1	PASS	banner motd	Display an authorized-use notice before login.	-	-
NTC-ARU-1.7.ssh-max-auth-attempts	Limit SSH authentication attempts	LOW Weight: 1 Profile: L2	PASS	value=3.0	Cap the number of SSH authentication attempts per connection.	-	-
NTC-ARU-1.8.mgmt-vrf-separation	Bind SSH management to a dedicated management VRF	MEDIUM Weight: 40 Profile: L2	PASS	ssh server vrf mgmt	Run management services on the dedicated mgmt VRF, separated from data VRFs.	-	-
NTC-ARU-2.1.aaa-login-remote	Authenticate management logins against remote AAA	HIGH Weight: 60 Profile: L1	PASS	aaa authentication login ssh group tacacs	Authenticate logins against a central AAA server, falling back to local.	-	-
NTC-ARU-2.2.tacacs-server	Configure a TACACS+ server	MEDIUM Weight: 40 Profile: L1	PASS	tacacs-server host 10.0.0.5	Configure a TACACS+ authentication server with an encrypted key.	-	-

- 6 The row carries more than a verdict. Evidence says what was found in the configuration, Recommendation says why it matters, and Fix gives the commands that would clear it. You can take that straight to a change request without opening the device.

This screenshot is identical to the one above, showing the NacTrack interface for a compliance report. The top navigation bar includes Dashboard, Inventory, L2VPN, Neighbors, Spanning-Tree, Routing, IPAM, Security, Reporting, and Tools. The main header shows the device IP 10.250.10.148, Model 6405, and Benchmark NacTrack Aruba AOS-CX Security Baseline v1.0.0. Below the header is a table with columns: CODE, TITLE, SEVERITY, STATUS, EVIDENCE / DETAILS, RECOMMENDATION, FIX, and WAIVER. The table lists 12 checks, with the second row (NAC-ARU-1.2.telnet-disabled) marked as FAIL. The evidence for this failure is 'Clearnet Telnet server is enabled'. The recommendation is 'Disable the clearnet Telnet server; use SSH instead.' The fix is 'no telnet-server vrf default; no telnet-server vrf mgmt'. The waiver is 'Reason (accepted risk) dd/mm/yyyy'. The table also shows the severity (HIGH), weight (60), and profile (L1) for each check. At the bottom, there is a section for 'Recent Evaluation Jobs' and a 'PDF Report' button.

CODE	TITLE	SEVERITY	STATUS	EVIDENCE / DETAILS	RECOMMENDATION	FIX	WAIVER
NTC-ARU-1.1.ssh-server-vrf	Enable the SSH server on a VRF	HIGH Weight: 60 Profile: L1	PASS	ssh server vrf mgmt	Enable the SSH management server on a routing VRF.	-	-
NTC-ARU-1.2.telnet-disabled	Disable the Telnet server	HIGH Weight: 60 Profile: L1	FAIL	Clearnet Telnet server is enabled	Disable the clearnet Telnet server; use SSH instead.	no telnet-server vrf default; no telnet-server vrf mgmt	Reason (accepted risk) dd/mm/yyyy
NTC-ARU-1.3.https-server-vrf	Restrict the HTTPS/REST server to a VRF	MEDIUM Weight: 40 Profile: L2	PASS	https-server vrf mgmt	Expose the web/REST management interface only on a controlled VRF.	-	-
NTC-ARU-1.4.no-plaintext-http	Disable the plaintext HTTP server	HIGH Weight: 60 Profile: L1	PASS	-	Disable the plaintext HTTP server; use HTTPS only.	-	-
NTC-ARU-1.5.cli-session-timeout	Set CLI idle session timeout to 15 minutes or less	MEDIUM Weight: 40 Profile: L1	PASS	value=10.0	Time out idle management CLI sessions.	-	-
NTC-ARU-1.6.banner-motd	Configure a login banner (message of the day)	LOW Weight: 1 Profile: L1	PASS	banner motd	Display an authorized-use notice before login.	-	-
NTC-ARU-1.7.ssh-max-auth-attempts	Limit SSH authentication attempts	LOW Weight: 1 Profile: L2	PASS	value=3.0	Cap the number of SSH authentication attempts per connection.	-	-
NTC-ARU-1.8.mgmt-vrf-separation	Bind SSH management to a dedicated management VRF	MEDIUM Weight: 40 Profile: L2	PASS	ssh server vrf mgmt	Run management services on the dedicated mgmt VRF, separated from data VRFs.	-	-
NTC-ARU-2.1.aaa-login-remote	Authenticate management logins against remote AAA	HIGH Weight: 60 Profile: L1	PASS	aaa authentication login ssh group tacacs	Authenticate logins against a central AAA server, falling back to local.	-	-
NTC-ARU-2.2.tacacs-server	Configure a TACACS+ server	MEDIUM Weight: 40 Profile: L1	PASS	tacacs-server host 10.0.0.5	Configure a TACACS+ authentication server with an encrypted key.	-	-

WORTH KNOWING

This reads configuration, not reachability. A device whose Telnet server is enabled may still be unreachable on port 23 because a firewall or a management ACL blocks it. The finding says the door is unlocked, not that anyone can walk to it.

The verdict is only as fresh as the last configuration collection. A device hardened this morning still reads as failing until it is collected and evaluated again.

How to find devices using default or version 1 and 2c SNMP communities

An SNMP community string is a password sent in clear text, and versions 1 and 2c have no other protection. Communities named public and private are worse still, because they are the first two anyone tries. This usually survives not through carelessness but through inheritance: a monitoring system needed read access years ago, the community was set fleet-wide, and nothing since has had a reason to revisit it.

Requires: module: compliance, permission: view_audit, vendors: All benchmarked platforms; the wording of the check differs by vendor

- 1 Open Security then Compliance. SNMP is judged by the same per-platform benchmark that covers Telnet and the rest of the management plane.
- 2 This spine switch fails two checks, and both are about SNMP. They are deliberately separate questions: one asks whether a default community name is in use, the other whether version 1 or 2c is enabled at all.

Dashboard

Inventory

L2VPN

Neighbors

Spanning-Tree

Routing

IPAM

Security

Reporting

Tools

Academy Admin

Compliance

AWM-CAS-DC-SP02

PDF Report

IP

10.250.10.136

Model

7280SR3K-48YC8

Benchmark

NacTrack Arista EOS Security Baseline v4.0.0

Column visibility

Excel

CSV

PDF

Show 10 entries

CODE	TITLE	SEVERITY	STATUS	EVIDENCE / DETAILS	RECOMMENDATION	FIX	WAIVER
NTC-EOS-11.api-tls	eAPI http-commands must use HTTPS/TLS	MEDIUM Weight: 40 Profile: L1	PASS	management api http-commands: protocol https	Serve eAPI over TLS only.	-	-
NTC-EOS-11.console-idle-timeout	Console session idle-timeout 1-15 minutes	MEDIUM Weight: 40 Profile: L1	PASS	management console: value=15.0	Bound idle console sessions.	-	-
NTC-EOS-11.http-disabled	Disable the cleartext HTTP management interface	HIGH Weight: 80 Profile: L1	PASS	no protocol http	Disable plaintext HTTP, keep HTTPS only.	-	-
NTC-EOS-11.login-banner	Present a login banner	LOW Weight: 1 Profile: L1	PASS	banner login	Display an authorized-use banner.	-	-
NTC-EOS-11.no-telnet	Disable the Telnet management server	HIGH Weight: 80 Profile: L1	PASS	no ip telnet server	Disable the cleartext Telnet server.	-	-
NTC-EOS-11.ssh-enabled	Enable the SSH management server	MEDIUM Weight: 40 Profile: L1	PASS	management ssh: no shutdown	Bring up the SSH management service.	-	-
NTC-EOS-11.ssh-idle-timeout	SSH session idle-timeout 1-15 minutes	MEDIUM Weight: 40 Profile: L1	PASS	management ssh: value=10.0	Bound idle SSH sessions.	-	-
NTC-EOS-12.aaa-auth-login	Configure AAA login authentication	HIGH Weight: 80 Profile: L1	PASS	aaa authentication login	Define a login authentication method.	-	-
NTC-EOS-12.aaa-login-remote-group	Login authentication uses a TACACS+/RADIUS group	MEDIUM Weight: 40 Profile: L1	PASS	aaa authentication login default group tacacs+	Authenticate against a central AAA server with local fallback.	-	-
NTC-EOS-12.aaa-root	aaa root protected by a secret	MEDIUM Weight: 40 Profile: L1	PASS	aaa root secret	Set a secret on the root account.	-	-

Showing 1 to 10 of 29 entries

Previous 1 2 3 Next

Recent Evaluation Jobs

No compliance jobs have been recorded yet.

Latest 0 entries

Academy 10

- 3 Each column has its own filter. Typing FAIL under Status reduces the table to what is actually wrong, which matters here because most of this device's checks pass and they would otherwise fill several pages before you reached the two that do not.

Compliance > AWM-CAS-DC-SP02

PDF Report

IP: 10.250.10.136 Model: 7280SR3K-4BYC8 Benchmark: NacTrack Arista EOS Security Baseline v4.0.0

Column visibility | Excel | CSV | PDF | Show 10 entries

CODE	TITLE	SEVERITY	STATUS	EVIDENCE / DETAILS	RECOMMENDATION	FIX	WAIVER
NTC-EOS-11.api-tls	eAPI http-commands must use HTTPS/TLS	MEDIUM Weight: 40 Profile: L1	PASS	management api http-commands: protocol https	Serve eAPI over TLS only.	-	-
NTC-EOS-11.console-idle-timeout	Console session idle-timeout 1-15 minutes	MEDIUM Weight: 40 Profile: L1	PASS	management console: value=15.0	Bound idle console sessions.	-	-
NTC-EOS-11.http-disabled	Disable the cleartext HTTP management interface	HIGH Weight: 80 Profile: L1	PASS	no protocol http	Disable plaintext HTTP, keep HTTPS only.	-	-
NTC-EOS-11.login-banner	Present a login banner	LOW Weight: 1 Profile: L1	PASS	banner login	Display an authorized-use banner.	-	-
NTC-EOS-11.no-telnet	Disable the Telnet management server	HIGH Weight: 80 Profile: L1	PASS	no ip telnet server	Disable the cleartext Telnet server.	-	-
NTC-EOS-11.ssh-enabled	Enable the SSH management server	MEDIUM Weight: 40 Profile: L1	PASS	management ssh: no shutdown	Bring up the SSH management service.	-	-
NTC-EOS-11.ssh-idle-timeout	SSH session idle-timeout 1-15 minutes	MEDIUM Weight: 40 Profile: L1	PASS	management ssh: value=10.0	Bound idle SSH sessions.	-	-
NTC-EOS-12.aaa-auth-login	Configure AAA login authentication	HIGH Weight: 80 Profile: L1	PASS	aaa authentication login	Define a login authentication method.	-	-
NTC-EOS-12.aaa-login-remote-group	Login authentication uses a TACACS+/RADIUS group	MEDIUM Weight: 40 Profile: L1	PASS	aaa authentication login default group=tacacs+	Authenticate against a central AAA server with local fallback.	-	-
NTC-EOS-12.aaa-root	aaa root protected by a secret	MEDIUM Weight: 40 Profile: L1	PASS	aaa root secret	Set a secret on the root account.	-	-

Showing 1 to 10 of 29 entries

Previous 1 2 3 Next

Recent Evaluation Jobs

No compliance jobs have been recorded yet.

Latest 0 entries

Academy

- 4 The table filters as you type. A moment later only the failing rows remain.
- 5 The distinction matters when you come to fix it. Renaming a community answers the first check and leaves the second failing, because the traffic is still unauthenticated and unencrypted. Only moving to version 3 clears both.

Compliance > AWM-CAS-DC-SP02

PDF Report

IP: 10.250.10.136 Model: 7280SR3K-4BYC8 Benchmark: NacTrack Arista EOS Security Baseline v4.0.0

Column visibility | Excel | CSV | PDF | Show 10 entries

CODE	TITLE	SEVERITY	STATUS	EVIDENCE / DETAILS	RECOMMENDATION	FIX	WAIVER
NTC-EOS-13.no-default-community	No default SNMP community (public/private)	HIGH Weight: 80 Profile: L1	FAIL	Queryable SNMP community present	Remove default communities.	configure no snmp-server community public no snmp-server community private end	Reason (accepted risk) dt/mn/yyyy Value
NTC-EOS-13.no-v1v2-community	No SNMP v1/v2c communities (v3 only)	MEDIUM Weight: 40 Profile: L2	FAIL	SNMP v1v2c community configured	Drop all communities and use SNMPv3.	configure no snmp-server community v1v2c end	Reason (accepted risk) dt/mn/yyyy Value

Showing 1 to 2 of 2 entries (Filtered from 29 total entries)

Previous 1 Next

Recent Evaluation Jobs

No compliance jobs have been recorded yet.

Latest 0 entries

WORTH KNOWING

A device with no SNMP configured at all passes both checks. Passing therefore means "not exposed this way", not "monitored securely" - the benchmark cannot tell an intentionally hardened device from one nobody ever set up.

Community strings are credentials. NacTrack reports that a weak one exists and does not print its value in the evidence, so the report can be shared without leaking what it found.

How to read a device's management access posture

Management exposure is not one setting. It is the sum of which services answer, whether they are encrypted, whether they are confined to a management VRF, whether logging in is authenticated centrally, and whether an idle session ever closes. Read individually those checks look like housekeeping. Read together for one device they describe how someone would get in, and that is the reading worth learning.

Requires: module: compliance, permission: view_audit, vendors: All benchmarked platforms; check names and counts differ by vendor

- 1 Open Security then Compliance, and sort by score. The lowest scores are where the management plane was never hardened at all, rather than where a single control drifted.
- 2 This one fails every check that was run against it. That pattern is characteristic: it is not a device that drifted, it is a device that was never brought onto the standard build in the first place.

The screenshot shows the NetTrack Security Compliance interface. The top navigation bar includes links for Dashboard, Inventory, L2VPN, Neighbors, Spanning-Tree, Routing, IPAM, Security, Reporting, and Tools. The main header displays the device IP (10.250.10.132), name (NetEngine 8000 MB), and benchmark (NacTrack Huawei VRP Security Baseline v1.0.0). Below this, there are tabs for Column visibility, Excel, CSV, and PDF. A search bar is located on the right. The main table lists 10 failed checks, each with a code, title, severity, status, evidence, recommendation, and fix. The status for all checks is 'FAIL'. The severity ranges from MEDIUM to HIGH. The evidence column shows the specific configuration or command that failed. The recommendation column provides guidance on how to resolve the issue. The fix column shows the correct configuration or command. The table is sorted by score, with the lowest scores (most failures) at the top.

CODE	TITLE	SEVERITY	STATUS	EVIDENCE / DETAILS	RECOMMENDATION	FIX	WAIVER
NTC-HW-1.1.local-user-has-hashed-password	Use irreversible-cipher for local-user passwords	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system view local-user <user> password irreversible-cipher <strong password> return	Reason (accepted risk) Waive dd/mm/yyyy
NTC-HW-1.1.local-user-ssh-service	Local user's allowed only required service types including SSH	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system view local-user <user> service-type ssh return	Reason (accepted risk) Waive dd/mm/yyyy
NTC-HW-1.1.telnet-enable	Enable SSH server (stelnet)	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system view stelnet server enable return	Reason (accepted risk) Waive dd/mm/yyyy
NTC-HW-1.1.telnet-disable	Disable telnet server	HIGH Weight: 60 Profile: L2	FAIL	configuration must be removed	-	system view undo telnet server enable return	Reason (accepted risk) Waive dd/mm/yyyy
NTC-HW-1.1.vty-aaa	Use AAA authentication on VTY	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system view user interface vty 0 4 authentication-mode aaa return	Reason (accepted risk) Waive dd/mm/yyyy
NTC-HW-1.1.vty-ssh-only	Restrict VTY protocol to SSH	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system view user interface vty 0 4 protocol inbound ssh return	Reason (accepted risk) Waive dd/mm/yyyy
NTC-HW-1.2.aaa-enable	Enable AAA framework	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system view aaa return	Reason (accepted risk) Waive dd/mm/yyyy
NTC-HW-1.2.domain-default-admin	Configure default admin domain	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present	-	system view default-domain authentication-scheme <scheme> authorization-scheme <scheme> accounting-scheme <scheme> return	Reason (accepted risk) Waive dd/mm/yyyy
NTC-HW-1.2.radius-or-lacpss-template	Configure centralized AAA server template	HIGH Weight: 60 Profile: L2	FAIL	required configuration not present	-	system view radius server template <name> return	Reason (accepted risk) Waive dd/mm/yyyy
NTC-HW-1.3.no-snmp-community	Disable SNMP community strings	HIGH Weight: 60 Profile: L2	FAIL	configuration must be removed	-	system view undo snmp-agent community read <community> undo snmp-agent community write <community> return	Reason (accepted risk) Waive dd/mm/yyyy

Showing 1 to 10 of 42 entries

- 3 Note which way this check points. It does not say a service should be turned off; it says the SSH server should be enabled and is not. Combine that with the Telnet server being active and you have the whole story: the only way onto this device is the unencrypted one.

CODE	TITLE	SEVERITY	STATUS	EVIDENCE / DETAILS	RECOMMENDATION	FIX	WAVES
NTC-HW-1.1.local-user-hash-password	Use irreversible-cipher for local-user passwords	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present		system-view local-user <user> password irreversible-cipher <strong password> return	Reason (accepted risk) Waive
NTC-HW-1.1.local-user-ssh-service	Local users allowed only required service types including SSH	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present		system-view local-user <user> service-type ssh return	Reason (accepted risk) Waive
NTC-HW-1.1.telnet-enable	Enable SSH server (stelnet)	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present		system-view stelnet server enable return	Reason (accepted risk) Waive
NTC-HW-1.1.telnet-disable	Disable telnet server	HIGH Weight: 60 Profile: L2	FAIL	configuration must be removed		system-view undo telnet server enable return	Reason (accepted risk) Waive
NTC-HW-1.1.vty-aaa	Use AAA authentication on VTY	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present		system-view user-interface vty 0 4 authentication-mode aaa return	Reason (accepted risk) Waive
NTC-HW-1.1.vty-ssh-only	Restrict VTY protocol to SSH	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present		system-view user-interface vty 0 4 protocol inbound ssh return	Reason (accepted risk) Waive
NTC-HW-1.2.aaa-enable	Enable AAA framework	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present		system-view aaa return	Reason (accepted risk) Waive
NTC-HW-1.2.domain-default-admin	Configure default admin domain	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present		system-view domain default-admin authentication-scheme <scheme> authorization-scheme <scheme> accounting-scheme <scheme> return	Reason (accepted risk) Waive
NTC-HW-1.2.radius-or-tacacs-template	Configure centralized AAA server template	HIGH Weight: 60 Profile: L2	FAIL	required configuration not present		system-view radius-server template <name> return	Reason (accepted risk) Waive
NTC-HW-1.3.no-snmp-community	Disable SNMP community strings	HIGH Weight: 60 Profile: L2	FAIL	configuration must be removed		system-view undo snmp-agent community read <community> undo snmp-agent community write <community> return	Reason (accepted risk) Waive

- 4 The terminal lines confirm it. This check wants the VTY sessions restricted to SSH alone, and it is failing, so the lines accept whatever the device offers. Three findings that each look minor on their own have now described a complete path in.

CODE	TITLE	SEVERITY	STATUS	EVIDENCE / DETAILS	RECOMMENDATION	FIX	WAVES
NTC-HW-1.1.local-user-hash-password	Use irreversible-cipher for local-user passwords	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present		system-view local-user <user> password irreversible-cipher <strong password> return	Reason (accepted risk) Waive
NTC-HW-1.1.local-user-ssh-service	Local users allowed only required service types including SSH	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present		system-view local-user <user> service-type ssh return	Reason (accepted risk) Waive
NTC-HW-1.1.telnet-enable	Enable SSH server (stelnet)	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present		system-view stelnet server enable return	Reason (accepted risk) Waive
NTC-HW-1.1.telnet-disable	Disable telnet server	HIGH Weight: 60 Profile: L2	FAIL	configuration must be removed		system-view undo telnet server enable return	Reason (accepted risk) Waive
NTC-HW-1.1.vty-aaa	Use AAA authentication on VTY	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present		system-view user-interface vty 0 4 authentication-mode aaa return	Reason (accepted risk) Waive
NTC-HW-1.1.vty-ssh-only	Restrict VTY protocol to SSH	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present		system-view user-interface vty 0 4 protocol inbound ssh return	Reason (accepted risk) Waive
NTC-HW-1.2.aaa-enable	Enable AAA framework	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present		system-view aaa return	Reason (accepted risk) Waive
NTC-HW-1.2.domain-default-admin	Configure default admin domain	MEDIUM Weight: 40 Profile: L1	FAIL	required configuration not present		system-view domain default-admin authentication-scheme <scheme> authorization-scheme <scheme> accounting-scheme <scheme> return	Reason (accepted risk) Waive
NTC-HW-1.2.radius-or-tacacs-template	Configure centralized AAA server template	HIGH Weight: 60 Profile: L2	FAIL	required configuration not present		system-view radius-server template <name> return	Reason (accepted risk) Waive
NTC-HW-1.3.no-snmp-community	Disable SNMP community strings	HIGH Weight: 60 Profile: L2	FAIL	configuration must be removed		system-view undo snmp-agent community read <community> undo snmp-agent community write <community> return	Reason (accepted risk) Waive

WORTH KNOWING

A benchmark is a shipped opinion about a platform, not your organisation's policy. A device that deliberately runs a service your standard permits will still be reported as failing until the check is waived.

Check counts are not comparable between vendors. One platform's benchmark may run thirty checks and another sixty, so a lower score does not automatically mean a worse device - compare a device against its own platform's baseline.

Requires: module: stp, permission: view_stp, vendors: Cisco and Huawei switches only

- [Dashboard](#)
[Inventory](#)
[L2VPN](#)
[Neighbors](#)
[Spanning-Tree](#)
[Routing](#)
[IPAM](#)
[Security](#)
[Reporting](#)
[Tools](#)

[Home](#)
[EN](#)
[ES](#)
[FR](#)
[DE](#)
[IT](#)
[PT](#)
[RU](#)
[CN](#)
[JP](#)
[KR](#)
[IN](#)
[TH](#)
[VN](#)
[PH](#)
[ID](#)
[MY](#)
[SG](#)
[AU](#)
[NZ](#)
[CA](#)
[US](#)
[MX](#)
[BR](#)
[AR](#)
[CL](#)
[CO](#)
[PE](#)
[VE](#)
[EC](#)
[GY](#)
[SR](#)
[TT](#)
[JM](#)
[CU](#)
[DO](#)
[PR](#)
[VI](#)
[AI](#)
[AG](#)
[BS](#)
[BB](#)
[BZ](#)
[JM](#)
[DO](#)
[PR](#)
[VI](#)
[AI](#)
[AG](#)
[BS](#)
[BB](#)
[BZ](#)

[Academy Admin](#)

Dashboard

AtlasWave Maroc De...

Network Overview

New

58 / 58

Devices

673 / 1332

Ports Up / Total

0

Rebooted < 24h

83.9%

Compliance

100%

Collection

10

EOL / EOS Devices

Models

Model	Count
6200F-480-POE4	12
6300M	1
6405	1
7000S-43-48YC-12	1
7210	2
7200S-20F-48YC-12	1
7730 SR-1	3
EX300-800T-AC	1
ASR-9902	2
ASR1001-X	1
ASR1001-AC	1
ASR1002-X	1
BQ-IP-6800	1
CR300-48P	7
CR300-24Y-AC	1
CR300-48Y-AC	1
FortiGate-100F	2
FortiGate-200F	3
MX204	1
MX204	1
NBR-C33-80T-CP-3	2
N3000	1
NE-45E-35A	3
NetEngine 8000 M8	1
PL-3410	1
SD-WAN-ON	2
Zte60F-ON	2

Software Distribution

Software Version	Count
BRAS 17.9.4	1
LOAD_BALANCER 17.1.1	1
ROUTER 22-48G-33.4	1
SWITCH 16.13.1020	1
VR800R22C00	1
ROUTER 23.3.R1	1
ROUTER 17.8.4	1
FIREWALL 6.11.2	1
ROUTER 6.11.2.1	1
ROUTER V800R22C10	1
SWITCH 17.8.5	1
FIREWALL 7.2.6	1
ROUTER 17.8.5	1
SWITCH 4.32.2P	1
XR 7.10.2	1
FIREWALL 11.1.4-7	1
ROUTER 21.48G-54.11	1
SWITCH 10.5.8	1

Last Restarted Devices

HOSTNAME	MODEL	IP ADDRESS	UPTIME (NOW)	REBOOTED AT
AWM-RBA-ACC-SW01	6200F-480-POE4	10.256.29.161	2 weeks, 1 day, 7 hours	2026-07-18 03:02:51
AWM-CAS-WLC01	7210	10.256.19.152	2 weeks, 6 days, 10 hours	2026-07-13 00:02:51

- 2 Open Spanning-Tree and choose STP Listing. The upper table is one row per switch per VLAN: Bridge ID is that switch's own identity, and Root Bridge is the switch it currently believes is root. Both are shown as address plus hostname, so you never have to translate a MAC.

Spanning-Tree > STP Listing

6 STP Domains, 0 Root Bridges, 168 Active Ports (54% of total), 0 Standby Ports (0 redundancy)

Devices: AWM-AGA-ACC-SW01
Role: Unknown
Captured At: 2026-07-31T14:02:51.000Z
STP Instances: 6

STP Glossary

STP Instances

HOSTNAME	STP INSTANCES	MODE	VLAN	BRIDGE ID	ROOT BRIDGE	ROOT?	BRIDGE PRIORITY	ROOT PRIORITY	CHANGES	LAST CHANGE	HELLO	MAX AGE	FORWARD DELAY	HOLD	CAPTURED AT
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0001	rapid-pvst	1	12:86:63:15:1b:19 Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32769 (Low)	24577	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0010	rapid-pvst	10	12:86:63:15:1b:19 Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32778 (Low)	24586	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0020	rapid-pvst	20	12:86:63:15:1b:19 Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32769 (Low)	24596	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0030	rapid-pvst	30	12:86:63:15:1b:19 Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32768 (Low)	24606	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0100	rapid-pvst	100	12:86:63:15:1b:19 Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32668 (Low)	24676	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0200	rapid-pvst	200	12:86:63:15:1b:19 Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32668 (Low)	24776	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00

Showing 1 to 6 of 6 entries

STP Ports

With 'All', this table shows one STP row per interface and per VLAN/instance, so the same physical interface can appear many times.

HOSTNAME	STP INSTANCES	INTERFACE	ROLE	STATE	COST	PRIORITY	DESIGNATED BRIDGE	DESIGNATED ROOT	S-VLAN	C-VLAN	MODE	STATUS	CAPTURED AT
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0001	Gi0/0/1	Designated	Forwarding	4	128	12:86:63:15:1b:19 Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	10	20	access	up	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0001	Gi0/0/2	Designated	Forwarding	4	128	12:86:63:15:1b:19 Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	10	20	access	up	2026-07-31T14:02:51+00:00

- 3 Read down the Root Bridge column. Every VLAN on a healthy campus should point at the same aggregation switch, and Root Priority tells you whether that was configured on purpose or won by accident on a tie-breaking address.

Spanning-Tree > STP Listing

6 STP Domains, 0 Root Bridges, 168 Active Ports (54% of total), 0 Standby Ports (0 redundancy)

Devices: AWM-AGA-ACC-SW01
Role: Unknown
Captured At: 2026-07-31T14:02:51.000Z
STP Instances: 6

STP Glossary

STP Instances

HOSTNAME	STP INSTANCES	MODE	VLAN	BRIDGE ID	ROOT BRIDGE	ROOT?	BRIDGE PRIORITY	ROOT PRIORITY	CHANGES	LAST CHANGE	HELLO	MAX AGE	FORWARD DELAY	HOLD	CAPTURED AT
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0001	rapid-pvst	1	12:86:63:15:1b:19 Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32769 (Low)	24577	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0010	rapid-pvst	10	12:86:63:15:1b:19 Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32778 (Low)	24586	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0020	rapid-pvst	20	12:86:63:15:1b:19 Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32769 (Low)	24596	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0030	rapid-pvst	30	12:86:63:15:1b:19 Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32768 (Low)	24606	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0100	rapid-pvst	100	12:86:63:15:1b:19 Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32668 (Low)	24676	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0200	rapid-pvst	200	12:86:63:15:1b:19 Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	-	32668 (Low)	24776	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00

Showing 1 to 6 of 6 entries

STP Ports

With 'All', this table shows one STP row per interface and per VLAN/instance, so the same physical interface can appear many times.

HOSTNAME	STP INSTANCES	INTERFACE	ROLE	STATE	COST	PRIORITY	DESIGNATED BRIDGE	DESIGNATED ROOT	S-VLAN	C-VLAN	MODE	STATUS	CAPTURED AT
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0001	Gi0/0/1	Designated	Forwarding	4	128	12:86:63:15:1b:19 Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	10	20	access	up	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0001	Gi0/0/2	Designated	Forwarding	4	128	12:86:63:15:1b:19 Q AWM-AGA-ACC-SW01	16:c7:c5:98:e3:95 Q AWM-AGA-AGG-SW01	10	20	access	up	2026-07-31T14:02:51+00:00

WORTH KNOWING

A priority left at the default means the root was decided by the lowest MAC address, not by design. It will move the day that switch is replaced.

Spanning tree is collected from Cisco and Huawei switches only, and is stripped from routers. An Aruba or Dell access layer will not appear here even though it is running spanning tree.

How to find which ports spanning tree is blocking

A blocking port is not a fault. It is spanning tree doing its job, holding a redundant link in reserve so the network has no loop. What matters is whether the ports it chose to block are the ones you would have chosen, because a link blocked at the wrong end sends traffic the long way round every day without anyone noticing.

Requires: module: stp, permission: view_stp, vendors: Cisco and Huawei switches only

- 1
- Open Spanning-Tree then STP Listing. The lower table is the one we want: every port taking part in spanning tree, on every switch, with the role it was given and the state it settled into.

Spanning-Tree > STP Listing

6 STP Domains

0 Root Bridges

168 Active Ports
58% of total

0 Standby Ports
0 redundancy

Devices: AWM-AGA-ACC-SW01

VLAN / Instance: All

Devices: AWM-AGA-ACC-SW01 10.250.60.178

Role: Unknown

STP Ports: 288

Captured At: 2026-07-31T14:02:51.000Z

STP Instances: 6

STP Glossary

STP Instances

Showing 1 to 6 of 6 entries

Previous 1 Next

HOSTNAME	STP INSTANCES	MODE	VLAN	BRIDGE ID	ROOT BRIDGE	ROOT?	BRIDGE PRIORITY	ROOT PRIORITY	CHANGES	LAST CHANGE	HELLO	MAX AGE	FORWARD DELAY	HOLD	CAPTURED AT
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0001	rapid-pvst	1	12:80:63:53:db:54 AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 AWM-AGA-AGG-SW01	-	32768 (Low)	24872	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0010	rapid-pvst	10	12:80:63:53:db:54 AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 AWM-AGA-AGG-SW01	-	32768 (Low)	24866	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0020	rapid-pvst	20	12:80:63:53:db:54 AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 AWM-AGA-AGG-SW01	-	32768 (Low)	24866	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0030	rapid-pvst	30	12:80:63:53:db:54 AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 AWM-AGA-AGG-SW01	-	32768 (Low)	24866	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0100	rapid-pvst	100	12:80:63:53:db:54 AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 AWM-AGA-AGG-SW01	-	32768 (Low)	24876	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0200	rapid-pvst	200	12:80:63:53:db:54 AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 AWM-AGA-AGG-SW01	-	32768 (Low)	24776	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00

STP Ports

With 'All', this table shows one STP row per interface and per VLAN/instance, so the same physical interface can appear many times.

Showing 1 to 2 of 2 entries

Previous 1 Next

HOSTNAME	STP INSTANCES	INTERFACE	ROLE	STATE	COST	PRIORITY	DESIGNATED BRIDGE	DESIGNATED ROOT	S-VLAN	C-VLAN	MODE	STATUS	CAPTURED AT
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0001	Gi0/0/1	Designated	Forwarding	4	128	12:80:63:53:db:54 AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 AWM-AGA-AGG-SW01	10	20	access	up	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01 10.250.60.178	VLAN0001	Gi0/0/2	Designated	Forwarding	4	128	12:80:63:53:db:54 AWM-AGA-ACC-SW01	86:c7:c5:98:e3:95 AWM-AGA-AGG-SW01	10	20	access	up	2026-07-31T14:02:51+00:00

- 2 Two columns carry the answer. Role is the job spanning tree gave the port, and State is what it is actually doing. A port with role Alternate and state Blocking is a healthy standby: it has a path to the root but a better one exists, so it waits.

The screenshot displays the Nactrack Spinning Tree STP Listing page. At the top, there are summary cards for STP Domains (6), Root Bridges (0), Active Ports (168), and Standby Ports (0). Below these, the 'STP Instances' table is shown, listing various VLANs and their configurations. The table includes columns for Hostname, STP Instances, Mode, VLAN, Bridge ID, Root Bridge, Root Priority, Bridge Priority, Root Priority, Changes, Last Change, Hello, Max Age, Forward Delay, Hold, and Captured At. The 'STP Ports' table is also visible, showing the status of individual ports, including their roles and states.

HOSTNAME	STP INSTANCES	MODE	VLAN	BRIDGE ID	ROOT BRIDGE	ROOT PRIORITY	BRIDGE PRIORITY	ROOT PRIORITY	CHANGES	LAST CHANGE	HELLO	MAX AGE	FORWARD DELAY	HOLD	CAPTURED AT
AWM-AGA-ACC-SW01	VLAN0001	rapid-pvst	1	12:8d:63:15:db:1a	16:c7:c5:98:43:91	-	32769 (Low)	24577	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01	VLAN0010	rapid-pvst	10	12:8d:63:15:db:1a	16:c7:c5:98:43:91	-	32778 (Low)	24586	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01	VLAN0020	rapid-pvst	20	12:8d:63:15:db:1a	16:c7:c5:98:43:91	-	32788 (Low)	24596	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01	VLAN0030	rapid-pvst	30	12:8d:63:15:db:1a	16:c7:c5:98:43:91	-	32798 (Low)	24606	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01	VLAN0100	rapid-pvst	100	12:8d:63:15:db:1a	16:c7:c5:98:43:91	-	32808 (Low)	24616	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01	VLAN0200	rapid-pvst	200	12:8d:63:15:db:1a	16:c7:c5:98:43:91	-	32818 (Low)	24716	0	2026-07-31T14:02:51+00:00	2	20	15	1	2026-07-31T14:02:51+00:00

HOSTNAME	STP INSTANCES	INTERFACE	ROLE	STATE	COST	PRIORITY	DESIGNATED BRIDGE	DESIGNATED ROOT	S-VLAN	C-VLAN	MODE	STATUS	CAPTURED AT
AWM-AGA-ACC-SW01	VLAN0001	G1/0/1	Designated	Forwarding	4	128	12:8d:63:15:db:1a	16:c7:c5:98:43:91	10	20	access	up	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01	VLAN0001	G1/0/2	Designated	Forwarding	4	128	12:8d:63:15:db:1a	16:c7:c5:98:43:91	10	20	access	up	2026-07-31T14:02:51+00:00

WORTH KNOWING

Most ports on an access switch read Disabled rather than Forwarding or Blocking. That is not spanning tree rejecting them; it is simply that nothing is plugged in.

This is the state at the last collection, not a live feed. A port that has since converged differently will still read as it did when it was collected.

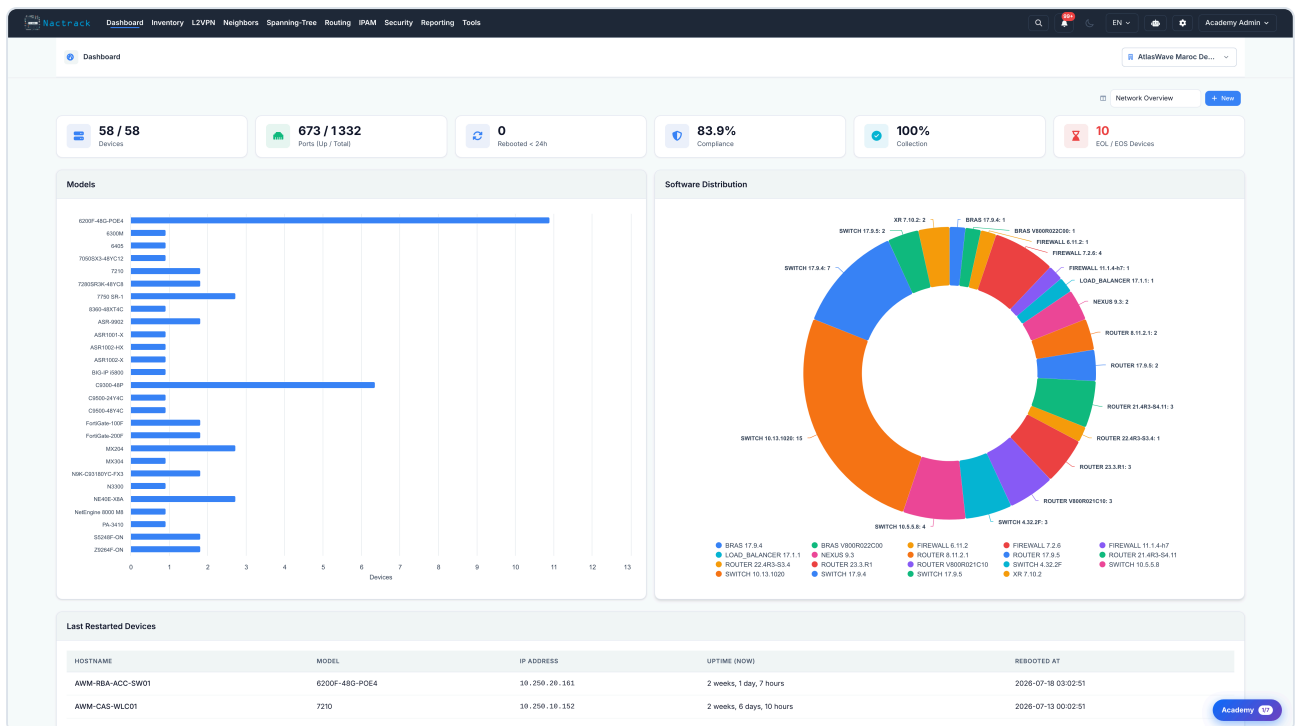
How to check whether BPDU Guard is enabled on edge ports

BPDU Guard shuts a port down the moment a switch appears where only endpoints should be, which is what stops someone plugging a desk switch into a wall socket and rearranging your spanning tree.

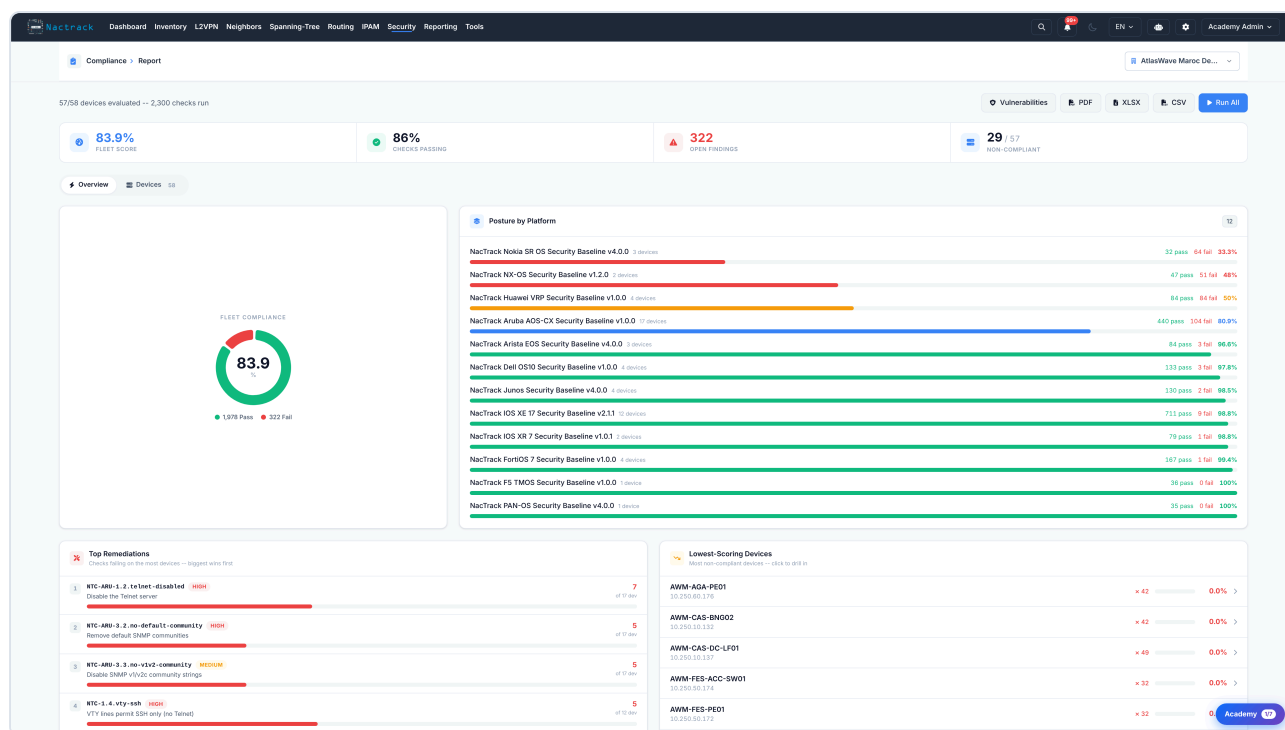
NacTrack does not read it from live state; it checks the running configuration against a benchmark rule, so the question is answered on the Compliance page rather than the STP one.

Requires: module: compliance, permission: view_audit, vendors: Aruba AOS-CX, Cisco NX-OS and Dell OS10 only

- 1 From the dashboard. This is a configuration question rather than a live-state one, so it lives under Security with the rest of the compliance work.



- 2 Open Security and choose Compliance. It opens on Overview, which is the fleet summary: the posture across every device, not the detail of any one of them.

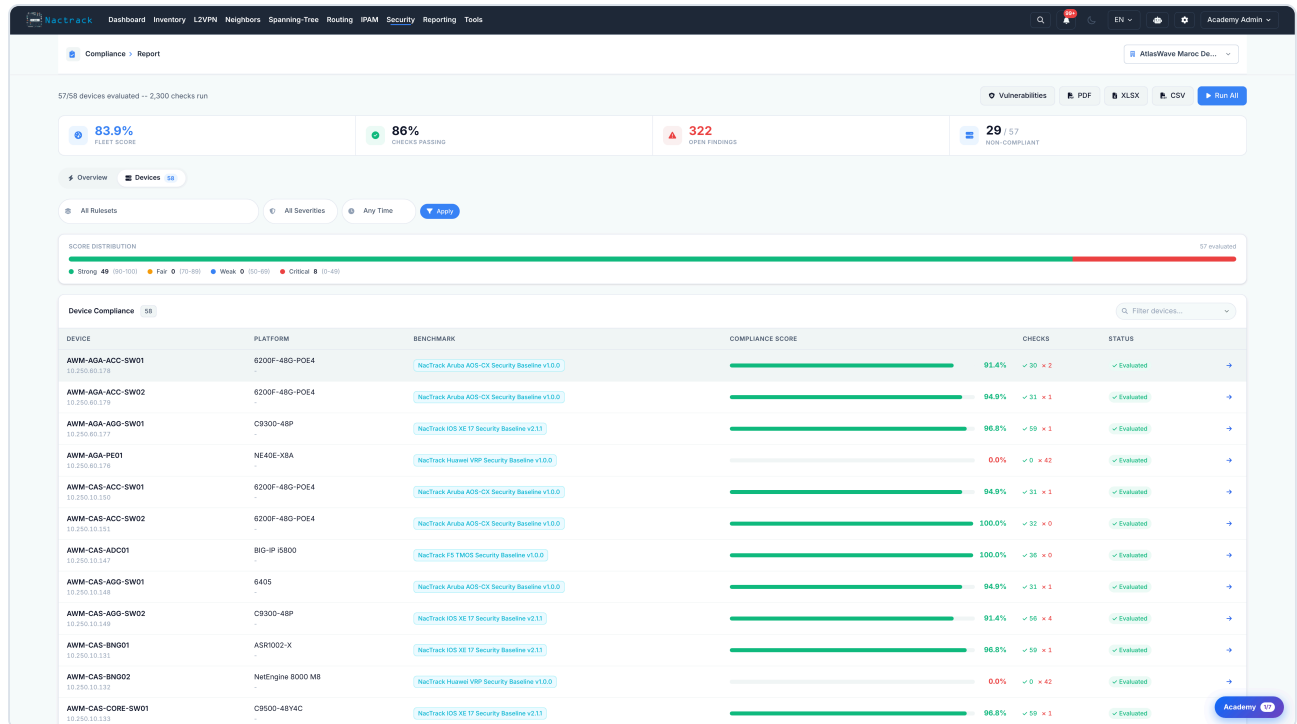


- 3 Switch to the Devices tab. Now every evaluated device is listed with its score and the number of checks that ran against it. The count beside the tab name tells you how many before you click.

The screenshot displays the NacTrack Compliance Devices page. The 'Devices' tab is selected, showing a 'Device Compliance' section with a search bar and a table of devices. The table includes columns for Device, Platform, Benchmark, Compliance Score, Checks, and Status. The 'Score Distribution' bar shows a range from 'Strong' to 'Critical'. The 'Device Compliance' section shows a list of devices with their scores and check counts.

Device	Platform	Benchmark	Compliance Score	Checks	Status
AWM-AGA-ACC-SW01	6200F-480-POE4	NacTrack Aruba AOS-CX Security Baseline v1.0.0	91.4%	30 x 2	Evaluated
AWM-AGA-ACC-SW02	6200F-480-POE4	NacTrack Aruba AOS-CX Security Baseline v1.0.0	94.9%	31 x 1	Evaluated
AWM-AGA-ACC-SW01	CR300-48P	NacTrack IOS XE 17 Security Baseline v2.1.1	96.8%	59 x 1	Evaluated
AWM-AGA-PE01	NE40E-X8A	NacTrack Huawei VRP Security Baseline v1.0.0	0.0%	0 x 42	Evaluated
AWM-CAS-ACC-SW01	6200F-480-POE4	NacTrack Aruba AOS-CX Security Baseline v1.0.0	94.9%	31 x 1	Evaluated
AWM-CAS-ACC-SW02	6200F-480-POE4	NacTrack Aruba AOS-CX Security Baseline v1.0.0	100.0%	32 x 0	Evaluated
AWM-CAS-ACC01	BIG-IP i5800	NacTrack FS TMOS Security Baseline v1.0.0	100.0%	36 x 0	Evaluated
AWM-CAS-ACC-SW01	6405	NacTrack Aruba AOS-CX Security Baseline v1.0.0	94.9%	31 x 1	Evaluated
AWM-CAS-ACC-SW02	CR300-48P	NacTrack IOS XE 17 Security Baseline v2.1.1	91.4%	56 x 4	Evaluated
AWM-CAS-BNG01	ASR1002-X	NacTrack IOS XE 17 Security Baseline v2.1.1	96.8%	59 x 1	Evaluated
AWM-CAS-BNG02	NetEngine 8000 MB	NacTrack Huawei VRP Security Baseline v1.0.0	0.0%	0 x 42	Evaluated
AWM-CAS-CORE-SW01	CR500-48Y4C	NacTrack IOS XE 17 Security Baseline v2.1.1	96.8%	59 x 1	Evaluated

- 4 Open a device to see its individual checks. The BPDU Guard rule appears by name among them, passed or failed, with the configuration line that decided it. That line is the evidence you would take to a change request.



WORTH KNOWING

Only three rules cover BPDU Guard, one each for Aruba AOS-CX, Cisco NX-OS and Dell OS10. A Cisco IOS or IOS-XE access switch is not checked for it at all, so a passing score does not mean the whole edge is protected.

Compliance reads configuration text. It can tell you the command is present; it cannot tell you the port ever actually blocked anything.

Root Guard is a different feature and NacTrack does not check it anywhere. Do not read a BPDU Guard pass as covering it.

Requires: module: inventory, permission: view_inventory

- | | | | | | | | | | | |
|--|-----------|-----------|-------|-----------|---------------|---------|------|----------|-----------|-------|
| | Dashboard | Inventory | L2VPN | Neighbors | Spanning-Tree | Routing | IPAM | Security | Reporting | Tools |
|--|-----------|-----------|-------|-----------|---------------|---------|------|----------|-----------|-------|

Inventory > VLANs
AtlasWave Maroc De...

Device: All devices

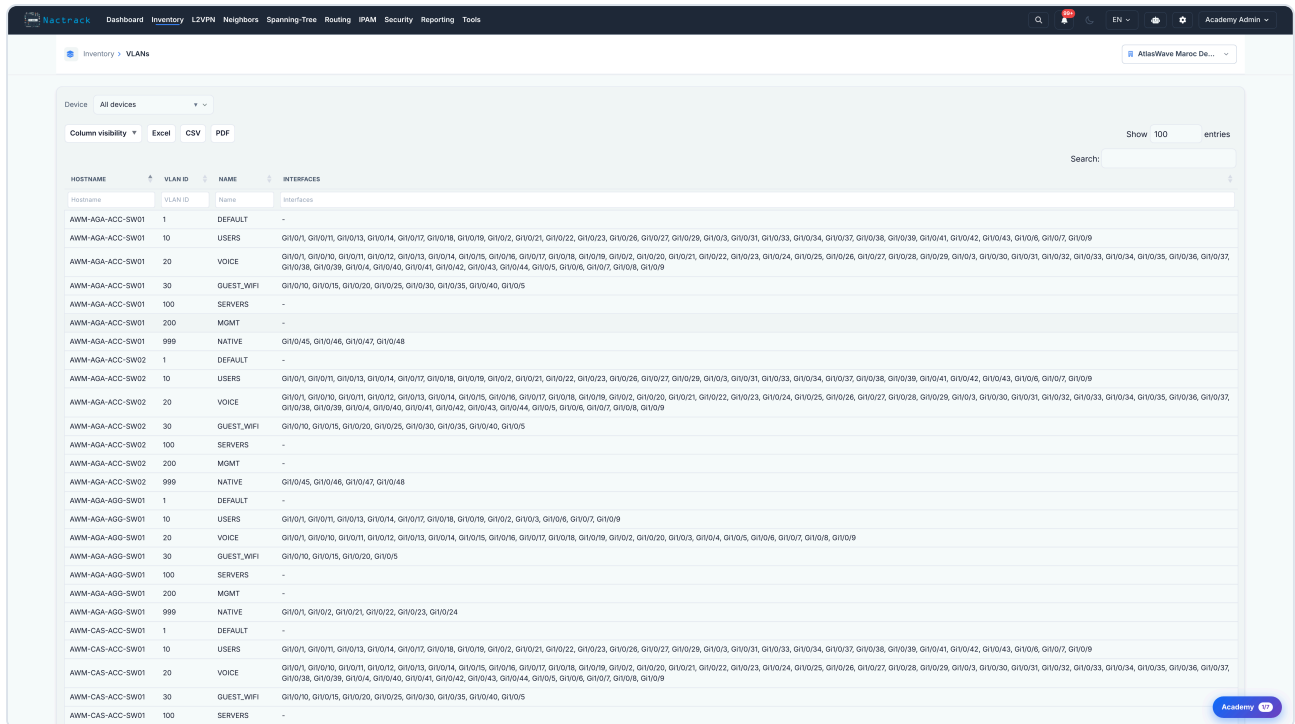
Column visibility: Excel CSV PDF

Show 100 entries

Search:

HOSTNAME	VLAN ID	NAME	INTERFACES
Hostname	VLAN ID	Name	Interfaces
AWM-AGA-ACC-SW01	1	DEFAULT	-
AWM-AGA-ACC-SW01	10	USERS	G1/0/1, G1/0/11, G1/0/13, G1/0/14, G1/0/17, G1/0/18, G1/0/19, G1/0/21, G1/0/22, G1/0/23, G1/0/26, G1/0/27, G1/0/28, G1/0/3, G1/0/31, G1/0/33, G1/0/34, G1/0/37, G1/0/38, G1/0/39, G1/0/41, G1/0/42, G1/0/43, G1/0/8, G1/0/7, G1/0/9
AWM-AGA-ACC-SW01	20	VOICE	G1/0/1, G1/0/10, G1/0/11, G1/0/12, G1/0/13, G1/0/14, G1/0/15, G1/0/16, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/28, G1/0/21, G1/0/22, G1/0/23, G1/0/24, G1/0/25, G1/0/26, G1/0/27, G1/0/28, G1/0/29, G1/0/3, G1/0/30, G1/0/31, G1/0/32, G1/0/33, G1/0/34, G1/0/35, G1/0/36, G1/0/37, G1/0/38, G1/0/39, G1/0/4, G1/0/40, G1/0/41, G1/0/42, G1/0/43, G1/0/44, G1/0/45, G1/0/6, G1/0/7, G1/0/8, G1/0/9
AWM-AGA-ACC-SW01	30	GUEST_WIFI	G1/0/10, G1/0/15, G1/0/20, G1/0/25, G1/0/30, G1/0/35, G1/0/40, G1/0/5
AWM-AGA-ACC-SW01	100	SERVICES	-
AWM-AGA-ACC-SW01	200	MGMT	-
AWM-AGA-ACC-SW01	999	NATIVE	G1/0/45, G1/0/46, G1/0/47, G1/0/48
AWM-AGA-ACC-SW02	1	DEFAULT	-
AWM-AGA-ACC-SW02	10	USERS	G1/0/1, G1/0/11, G1/0/13, G1/0/14, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/21, G1/0/22, G1/0/23, G1/0/26, G1/0/27, G1/0/28, G1/0/3, G1/0/31, G1/0/33, G1/0/34, G1/0/37, G1/0/38, G1/0/39, G1/0/41, G1/0/42, G1/0/43, G1/0/8, G1/0/7, G1/0/9
AWM-AGA-ACC-SW02	20	VOICE	G1/0/1, G1/0/10, G1/0/11, G1/0/12, G1/0/13, G1/0/14, G1/0/15, G1/0/16, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/28, G1/0/21, G1/0/22, G1/0/23, G1/0/24, G1/0/25, G1/0/26, G1/0/27, G1/0/28, G1/0/29, G1/0/3, G1/0/30, G1/0/31, G1/0/32, G1/0/33, G1/0/34, G1/0/35, G1/0/36, G1/0/37, G1/0/38, G1/0/39, G1/0/4, G1/0/40, G1/0/41, G1/0/42, G1/0/43, G1/0/44, G1/0/45, G1/0/6, G1/0/7, G1/0/8, G1/0/9
AWM-AGA-ACC-SW02	30	GUEST_WIFI	G1/0/10, G1/0/15, G1/0/20, G1/0/25, G1/0/30, G1/0/35, G1/0/40, G1/0/5
AWM-AGA-ACC-SW02	100	SERVICES	-
AWM-AGA-ACC-SW02	200	MGMT	-
AWM-AGA-ACC-SW02	999	NATIVE	G1/0/45, G1/0/46, G1/0/47, G1/0/48
AWM-AGA-AGG-SW01	1	DEFAULT	-
AWM-AGA-AGG-SW01	10	USERS	G1/0/1, G1/0/11, G1/0/13, G1/0/14, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/3, G1/0/6, G1/0/7, G1/0/9
AWM-AGA-AGG-SW01	20	VOICE	G1/0/1, G1/0/10, G1/0/11, G1/0/12, G1/0/13, G1/0/14, G1/0/15, G1/0/16, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/28, G1/0/3, G1/0/4, G1/0/5, G1/0/6, G1/0/7, G1/0/8, G1/0/9
AWM-AGA-AGG-SW01	30	GUEST_WIFI	G1/0/10, G1/0/15, G1/0/20, G1/0/5
AWM-AGA-AGG-SW01	100	SERVICES	-
AWM-AGA-AGG-SW01	200	MGMT	-
AWM-AGA-AGG-SW01	999	NATIVE	G1/0/1, G1/0/2, G1/0/21, G1/0/22, G1/0/23, G1/0/24
AWM-CAS-ACC-SW01	1	DEFAULT	-
AWM-CAS-ACC-SW01	10	USERS	G1/0/1, G1/0/11, G1/0/13, G1/0/14, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/21, G1/0/22, G1/0/23, G1/0/26, G1/0/27, G1/0/28, G1/0/3, G1/0/31, G1/0/33, G1/0/34, G1/0/37, G1/0/38, G1/0/39, G1/0/41, G1/0/42, G1/0/43, G1/0/8, G1/0/7, G1/0/9
AWM-CAS-ACC-SW01	20	VOICE	G1/0/1, G1/0/10, G1/0/11, G1/0/12, G1/0/13, G1/0/14, G1/0/15, G1/0/16, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/28, G1/0/21, G1/0/22, G1/0/23, G1/0/24, G1/0/25, G1/0/26, G1/0/27, G1/0/28, G1/0/29, G1/0/3, G1/0/30, G1/0/31, G1/0/32, G1/0/33, G1/0/34, G1/0/35, G1/0/36, G1/0/37, G1/0/38, G1/0/39, G1/0/4, G1/0/40, G1/0/41, G1/0/42, G1/0/43, G1/0/44, G1/0/45, G1/0/6, G1/0/7, G1/0/8, G1/0/9
AWM-CAS-ACC-SW01	30	GUEST_WIFI	G1/0/10, G1/0/15, G1/0/20, G1/0/25, G1/0/30, G1/0/35, G1/0/40, G1/0/5
AWM-CAS-ACC-SW01	100	SERVICES	-

- 2 Scan the Interfaces column. A dash means the VLAN is defined on that switch but no access, voice or native port is assigned to it. On this access switch the users and voice VLANs are populated while the servers and management VLANs are not, which is what you would expect at the edge.



The screenshot shows the Nactrack web interface with the 'Inventory > VLANs' page selected. The table displays VLAN configurations for various switches, including AWM-AGA-ACC-SW01, AWM-AGA-ACC-SW02, AWM-AGA-AGG-SW01, and AWM-CAS-ACC-SW01. Each row lists the device, VLAN ID, name, and the interfaces assigned to that VLAN. A search bar is visible at the top right of the table area.

HOSTNAME	VLAN ID	NAME	INTERFACES
AWM-AGA-ACC-SW01	1	DEFAULT	-
AWM-AGA-ACC-SW01	10	USERS	G1/0/1, G1/0/11, G1/0/13, G1/0/14, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/21, G1/0/22, G1/0/23, G1/0/26, G1/0/27, G1/0/29, G1/0/3, G1/0/31, G1/0/33, G1/0/34, G1/0/37, G1/0/38, G1/0/39, G1/0/41, G1/0/42, G1/0/43, G1/0/6, G1/0/7, G1/0/9
AWM-AGA-ACC-SW01	20	VOICE	G1/0/1, G1/0/10, G1/0/11, G1/0/12, G1/0/13, G1/0/14, G1/0/15, G1/0/16, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/20, G1/0/21, G1/0/22, G1/0/23, G1/0/24, G1/0/25, G1/0/26, G1/0/27, G1/0/28, G1/0/29, G1/0/3, G1/0/30, G1/0/31, G1/0/32, G1/0/33, G1/0/34, G1/0/35, G1/0/36, G1/0/37, G1/0/38, G1/0/39, G1/0/4, G1/0/40, G1/0/43, G1/0/44, G1/0/45, G1/0/5, G1/0/6, G1/0/7, G1/0/8, G1/0/9
AWM-AGA-ACC-SW01	30	GUEST_WIFI	G1/0/10, G1/0/15, G1/0/20, G1/0/25, G1/0/30, G1/0/35, G1/0/40, G1/0/5
AWM-AGA-ACC-SW01	100	SERVERS	-
AWM-AGA-ACC-SW01	200	MGMT	-
AWM-AGA-ACC-SW01	999	NATIVE	G1/0/45, G1/0/46, G1/0/47, G1/0/48
AWM-AGA-ACC-SW02	1	DEFAULT	-
AWM-AGA-ACC-SW02	10	USERS	G1/0/1, G1/0/11, G1/0/13, G1/0/14, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/21, G1/0/22, G1/0/23, G1/0/26, G1/0/27, G1/0/29, G1/0/3, G1/0/31, G1/0/33, G1/0/34, G1/0/37, G1/0/38, G1/0/39, G1/0/41, G1/0/42, G1/0/43, G1/0/6, G1/0/7, G1/0/9
AWM-AGA-ACC-SW02	20	VOICE	G1/0/1, G1/0/10, G1/0/11, G1/0/12, G1/0/13, G1/0/14, G1/0/15, G1/0/16, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/20, G1/0/21, G1/0/22, G1/0/23, G1/0/24, G1/0/25, G1/0/26, G1/0/27, G1/0/28, G1/0/29, G1/0/3, G1/0/30, G1/0/31, G1/0/32, G1/0/33, G1/0/34, G1/0/35, G1/0/36, G1/0/37, G1/0/38, G1/0/39, G1/0/4, G1/0/40, G1/0/43, G1/0/44, G1/0/45, G1/0/5, G1/0/6, G1/0/7, G1/0/8, G1/0/9
AWM-AGA-ACC-SW02	30	GUEST_WIFI	G1/0/10, G1/0/15, G1/0/20, G1/0/25, G1/0/30, G1/0/35, G1/0/40, G1/0/5
AWM-AGA-ACC-SW02	100	SERVERS	-
AWM-AGA-ACC-SW02	200	MGMT	-
AWM-AGA-ACC-SW02	999	NATIVE	G1/0/45, G1/0/46, G1/0/47, G1/0/48
AWM-AGA-AGG-SW01	1	DEFAULT	-
AWM-AGA-AGG-SW01	10	USERS	G1/0/1, G1/0/11, G1/0/13, G1/0/14, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/3, G1/0/6, G1/0/7, G1/0/9
AWM-AGA-AGG-SW01	20	VOICE	G1/0/1, G1/0/10, G1/0/11, G1/0/12, G1/0/13, G1/0/14, G1/0/15, G1/0/16, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/20, G1/0/3, G1/0/4, G1/0/5, G1/0/6, G1/0/7, G1/0/8, G1/0/9
AWM-AGA-AGG-SW01	30	GUEST_WIFI	G1/0/10, G1/0/15, G1/0/20, G1/0/5
AWM-AGA-AGG-SW01	100	SERVERS	-
AWM-AGA-AGG-SW01	200	MGMT	-
AWM-AGA-AGG-SW01	999	NATIVE	G1/0/1, G1/0/2, G1/0/21, G1/0/22, G1/0/23, G1/0/24
AWM-CAS-ACC-SW01	1	DEFAULT	-
AWM-CAS-ACC-SW01	10	USERS	G1/0/1, G1/0/11, G1/0/13, G1/0/14, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/21, G1/0/22, G1/0/23, G1/0/26, G1/0/27, G1/0/29, G1/0/3, G1/0/31, G1/0/33, G1/0/34, G1/0/37, G1/0/38, G1/0/39, G1/0/41, G1/0/42, G1/0/43, G1/0/6, G1/0/7, G1/0/9
AWM-CAS-ACC-SW01	20	VOICE	G1/0/1, G1/0/10, G1/0/11, G1/0/12, G1/0/13, G1/0/14, G1/0/15, G1/0/16, G1/0/17, G1/0/18, G1/0/19, G1/0/2, G1/0/20, G1/0/21, G1/0/22, G1/0/23, G1/0/24, G1/0/25, G1/0/26, G1/0/27, G1/0/28, G1/0/29, G1/0/3, G1/0/30, G1/0/31, G1/0/32, G1/0/33, G1/0/34, G1/0/35, G1/0/36, G1/0/37, G1/0/38, G1/0/39, G1/0/4, G1/0/40, G1/0/43, G1/0/44, G1/0/45, G1/0/5, G1/0/6, G1/0/7, G1/0/8, G1/0/9
AWM-CAS-ACC-SW01	30	GUEST_WIFI	G1/0/10, G1/0/15, G1/0/20, G1/0/25, G1/0/30, G1/0/35, G1/0/40, G1/0/5
AWM-CAS-ACC-SW01	100	SERVERS	-

WORTH KNOWING

A dash does not mean the VLAN is unused. It means no ACCESS port on this switch is in it. The VLAN may still be carried across the switch's trunks for other devices, and removing it would break them.

There is no fleet-wide "unused VLANs" report, and no filter for empty ones. This is a reading of a list, one switch at a time, which is why it belongs to the understanding tier rather than the lookup tier.

How to find out what changed on the network between two collections

Most outages follow a change, and the hard part is rarely the fix. It is establishing what moved and on which device, at a point where nobody is volunteering that they touched anything. NacTrack compares each device's configuration against its previous collection and records what was added, removed and modified, so the question stops being who changed something and becomes which of these changes could produce the symptom.

Requires: module: core, permission: use_troubleshooting, vendors: All collected platforms; the comparison is on configuration text

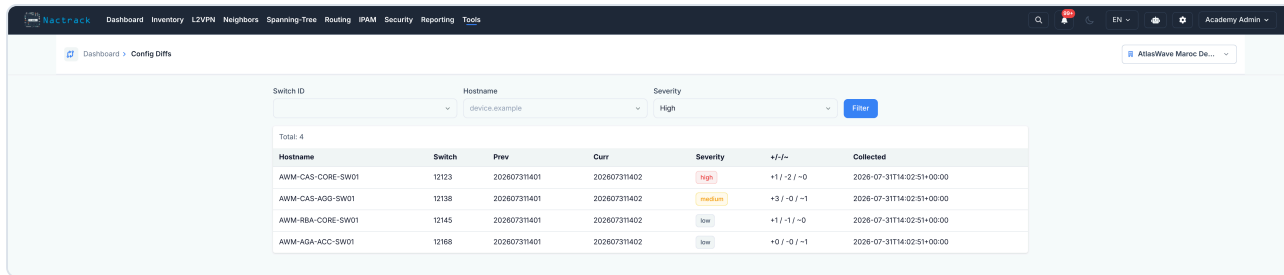
- 1 Change tracking sits with the troubleshooting tools rather than with inventory, because it is something you reach for with a symptom already in hand.
- 2 Each row is one device whose configuration differs from its previous collection. Prev and Curr identify the two collections being compared, and the three counts say how many lines were added, removed and modified. A change with removals is worth more attention than one that only adds, because removing a line is how something stops working.

Hostname	Switch	Prev	Curr	Severity	+/-	Collected
AWM-CAS-CORE-SW01	12123	202607311401	202607311402	High	+1 / -2 / -0	2026-07-31T14:02:51+00:00
AWM-CAS-AGG-SW01	12138	202607311401	202607311402	Medium	+3 / -0 / -1	2026-07-31T14:02:51+00:00
AWM-RBA-CORE-SW01	12145	202607311401	202607311402	Low	+1 / -1 / -0	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01	12168	202607311401	202607311402	Low	+0 / -0 / -1	2026-07-31T14:02:51+00:00

- 3 Severity is NacTrack's judgement of what was touched, not of how many lines moved. The high-severity row here removed two lines and added one, while a low-severity row further down modified a line and nothing else. Fewer lines, more consequence.

Hostname	Switch	Prev	Curr	Severity	+/-	Collected
AWM-CAS-CORE-SW01	12123	202607311401	202607311402	High	+1 / -2 / -0	2026-07-31T14:02:51+00:00
AWM-CAS-AGG-SW01	12138	202607311401	202607311402	Medium	+3 / -0 / -1	2026-07-31T14:02:51+00:00
AWM-RBA-CORE-SW01	12145	202607311401	202607311402	Low	+1 / -1 / -0	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01	12168	202607311401	202607311402	Low	+0 / -0 / -1	2026-07-31T14:02:51+00:00

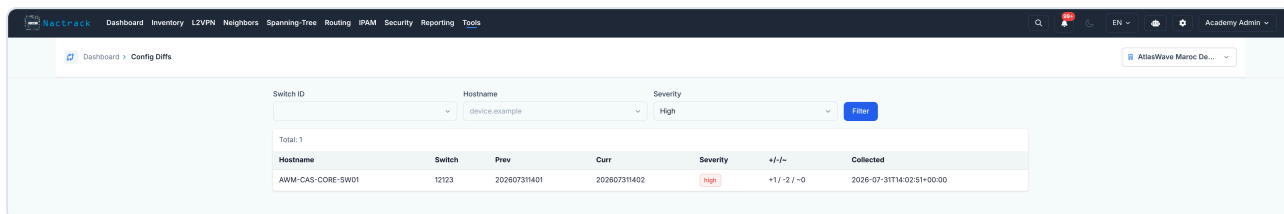
- 4 With a symptom and a time window, filter to the severity worth reading first. On a real estate this list is hundreds of rows a week, and starting from the high-severity ones is what makes it a diagnosis rather than a reading exercise.



The screenshot shows the Nactrack dashboard with the 'Config Diffs' section. The filters are set to 'Switch ID' (empty), 'Hostname' (device.example), and 'Severity' (High). The table shows 4 total results.

Hostname	Switch	Prev	Curr	Severity	+/-	Collected
AWM-CAS-CORE-SW01	12123	202607311401	202607311402	High	+1 / -2 / -0	2026-07-31T14:02:51+00:00
AWM-CAS-AGG-SW01	12138	202607311401	202607311402	Medium	+3 / -0 / -1	2026-07-31T14:02:51+00:00
AWM-RBA-CORE-SW01	12145	202607311401	202607311402	Low	+1 / -1 / -0	2026-07-31T14:02:51+00:00
AWM-AGA-ACC-SW01	12168	202607311401	202607311402	Low	+0 / -0 / -1	2026-07-31T14:02:51+00:00

- 5 One device remains. That is the candidate: a core switch that lost two configuration lines between two collections on the same day. From here the device page gives you its neighbours, its interfaces and its compliance state, which is where the diagnosis continues.



The screenshot shows the Nactrack dashboard with the 'Config Diffs' section. The filters are set to 'Switch ID' (empty), 'Hostname' (device.example), and 'Severity' (High). The table shows 1 total result.

Hostname	Switch	Prev	Curr	Severity	+/-	Collected
AWM-CAS-CORE-SW01	12123	202607311401	202607311402	High	+1 / -2 / -0	2026-07-31T14:02:51+00:00

WORTH KNOWING

This compares collections, not moments. Two changes made between the same pair of collections appear as one combined difference, and a change made and reverted before the next collection leaves no trace at all.

A change appearing here is not proof of a fault, and its absence is not proof of innocence. Plenty of outages come from something outside the configuration entirely - a failed optic, a neighbour's change, an expired certificate.

Severity is assigned from what kind of configuration changed, so it reflects blast radius rather than intent. A deliberate, approved change to a routing statement still reads as high.