Netopty

SYNTHETIC DEMONSTRATION — SAMPLE REPORT

TECHNICAL NETWORK AS-BUILT

RTG-HQ

Riverside Technology Group

Technical Network As-Built and Engineering Assessment

Site	RTG-HQ
Organisation	Riverside Technology Group
Document	Technical Network As-Built and Engineering Assessment
Version	1.0 (generated)
Report date	06 November 2026
Data collected	Live collection 20 Oct 2026; oldest source support schedule 19 Oct 2026; 1 undated (all dates: Purpose and scope / evidence register)
Prepared by	Network Engineering
Review status	Not reviewed: generated from collected data
Classification	Public sample — synthetic data, fictional organisation

Contents

Document control 4
1 Executive summary 6
1.1 Site at a glance 6
1.2 Key risks and next actions 7
1.3 Site architecture overview 9
2 Hardware 10
2.1 Switches 10
2.2 Switch stacks 12
2.3 Firewalls 12
2.4 Power and environment 13
2.5 PoE budget 14
2.6 Optics 14
2.7 Software lifecycle 15
2.8 Vulnerability correlation 16
2.9 Support contracts 17
3 Connectivity 19
3.1 WAN services 19
3.2 WAN hand-off 19
3.3 Infrastructure links 20
3.4 Port-channels and LAGs 21
3.5 Firewall ports 22
3.6 Endpoints per switch 22
3.7 Port capacity 23
3.8 Physical topology 24
3.9 Engineering connectivity 26
3.10 Interface inventory 31
3.11 Interface operational health 32
4 Layer 2 33
4.1 VLANs 33
4.2 VTP 33
4.3 Spanning tree 34
4.4 Fabric Connect 37
4.5 Switching topology 38
5 Layer 3 41
5.1 Switch Layer 3 interfaces 41
5.2 Firewall interfaces 42
5.3 Firewall zones 43
5.4 Firewall routing 44
5.5 Default gateways and static routes 44
5.6 DHCP and DNS relay 44
5.7 Gateway redundancy (VRRP/HSRP) 45
5.8 Routing adjacencies 45
5.9 Routing peerings 46
5.10 Subnets 47
5.11 Layer 3 view: routing summary 48
5.12 Layer 3 view: site prefixes 48
5.13 Routing topology 50
6 Management and security 53
6.1 Management services 53
6.2 Configuration backups 54
6.3 Management access 55
6.4 Authentication servers 56
6.5 SNMP management and traps 56
6.6 Service map: NTP servers 57
6.7 Service map: DNS servers 58
6.8 Service map: Syslog and log forwarding 58
6.9 Service map: SNMP trap receivers 59
6.10 Service map: access and addressing 60
6.11 Interface access lists 61

6.12 Quality of service 61
6.13 Edge port protection 61
6.14 Firewall policy and services 62
6.15 Firewall licences 62
6.16 High availability 62
6.17 Baseline compliance 63
7 Collection coverage and scope 64
7.1 Devices collected 64
7.2 Assumptions and exclusions 65
7.3 Methodology and limitations 65
8 Dependencies and readiness 66
8.1 Switch dependencies 66
8.2 Aggregation points 67
8.3 Firewall high availability and WAN 67
8.4 Readiness assessment 68
8.5 Assessment scope and limits 69
9 Findings register 70
9.1 Findings and recommendations 70
9.2 Change-control planning 82
9.3 Findings no longer raised 84
10 Changes since previous collection 85
10.1 Summary 85
10.2 Changes 85
Appendix A Optics 87
Appendix B Access points 89
Appendix C Collection status 90
Appendix D Evidence register 92

Figures

Figure 1 – Site architecture overview 9
Figure 2 – Physical topology 24
Figure 3 – Engineering connectivity 26
Figure 4 – Engineering connectivity: c9500-hq-c01 27
Figure 5 – Engineering connectivity: c9500-hq-c02 28
Figure 6 – Engineering connectivity: c9300-hq-c03 29
Figure 7 – Engineering connectivity: c9300-hq-c04 30
Figure 8 – Switching topology 38
Figure 9 – Switching topology (part 2 of 2, left to right) 39
Figure 10 – Firewall zones 43
Figure 11 – Routing peerings 46
Figure 12 – Subnets 47
Figure 13 – Routing topology 50
Figure 14 – Routing topology (part 2 of 2, left to right) 51
Figure 15 – Service map: NTP servers 57
Figure 16 – Service map: DNS servers 58
Figure 17 – Service map: Syslog and log forwarding 58
Figure 18 – Service map: SNMP trap receivers 59
Figure 19 – Service map: access and addressing 60

Document control

Report metadata

What this document is built from. Documents with the same evidence snapshot rest on the same collected data; a different snapshot means a different collection. The review status of this document is recorded beside it (<report>_review.json), not in the PDF.

Item	Value
Customer / site	Riverside Technology Group / RTG-HQ
Evidence snapshot	8e957703443f
Evidence collected	19 Oct 2026 - 20 Oct 2026
Document generated	2026-11-06T00:18:54
Collection profile	Full engineering assessment
Edition	full (findings included)
Report schema / generator	netopty-asbuilt/2 / Netopty as-built (version not recorded)
Evidence manifest	sha256:992f7368b92b00bb (58 files)
Collection	regeneration 20261105T131839Z-1cc5ac (offline regeneration from saved evidence; no new collection)
Evidence package	Riverside Technology Group [RTG]/RTG-HQ
Evidence age	newest 16 day(s), oldest 17 day(s) when generated
Regenerated	yes, from saved evidence

Review and approval

Generated documents are drafts. Engineer review and approval for customer delivery are recorded with the report (its review record), tied to this exact file and its evidence; regenerating the report or changing the evidence voids them.

Role	Name	Signature	Date
Prepared by			
Reviewed by			
Approved by			

Sources

Source
REGENERATED OFFLINE from saved evidence: Regenerated offline from saved evidence; NetBox, devices and Panorama were not contacted. Inventory coverage is relative to the devices in the saved collection.
REGENERATED OFFLINE from saved evidence: NetBox prefixes and the per-switch VLAN summary are not part of the saved evidence; those sections are empty in this regeneration
Devices: evidence originally acquired by live collection over SSH (CDP/LLDP, show commands); no device was contacted for this document
Inventory and prefixes: NetBox, as saved with the evidence (not queried for this document)
WAN services: WAN provider service export (where supplied)
Support contracts: RTG_support_schedule_20261019.xlsx
Security settings: latest configuration backups (dates under Configuration backups in section 6)

1 Executive summary

1.1 Site at a glance

20 Switches	**22** Switch units	**2** Firewalls collected	**14** VLANs
24 APs on collected switches	**217** Connected endpoints	**6** WAN circuits	**2** High-severity findings

Firewalls collected: firewalls whose own output is in this collection (security devices only seen as a neighbour are listed below, not counted). Access points and endpoints: devices found on switch ports through CDP/LLDP and the collected tables; devices that announce nothing are not counted. Access points on a network this collection did not read (a wireless system reached through a firewall or a switch that was not collected) are not seen: 0 means none was found on the collected switches, not that the site has no wireless.

Infrastructure overview

Item	Detail
Core switching	c9300-hq-c03 (C9300-24UX, 1 unit(s)); c9300-hq-c04 (C9300-24UX, 1 unit(s)); c9500-hq-c01 (C9500-24Y4C, 1 unit(s)); c9500-hq-c02 (C9500-24Y4C, 1 unit(s))
Firewalls	pa3410-hq-f01 (PA-3410, 11.1.4-h7); pa3410-hq-f02 (PA-3410, 11.1.4-h7)
WAN services	Business Internet 1000 Mbps (primary); Business Internet 1000 Mbps (secondary); Ethernet Private Line HQ - North (VLAN 901); Ethernet Private Line HQ - South (VLAN 902); Dark fibre HQ - DC1 (path A); Dark fibre HQ - DC1 (path B)

Hardware health. Conditions the devices themselves reported in this collection (power supplies, fans, temperature); detail by stack member and slot is in Power and environment.

Device	Reported condition
c9300-hq-a03	Power supply PSU 1B (member 1, slot B): fault (Bad)

Documentation confidence

How complete the collected evidence is. Each measure has its own denominator; per-device detail is in the collection status appendix.

Measure	Value	Definition
Reference data	software lifecycle: available (5 vendor files); end-of-life: eol_models.csv (7 model patterns)	Locally maintained data the lifecycle and end-of-life assessments rest on. Missing data means those assessments were not made, not that nothing was found.
Collection profile	Full engineering assessment	What this collection asked for. A capability outside the profile is 'Not requested', not a gap; evidence for it found anyway (e.g. an earlier backup) is still used.
Inventory coverage (saved collection)	22 of 22	Devices in the saved collection that were collected. NetBox was not consulted for this offline regeneration, so devices it lists but the saved collection never reached are not counted.
Collection attempts	22 of 22	Devices in the saved collection a collection was attempted for (NetBox was not consulted for this offline regeneration).

Measure	Value	Definition
Reachability	22 of 22	Devices a collection was attempted for (active in NetBox, platform supported) that answered.
Authentication	22 of 22	Reachable devices that accepted the login.
Collection completeness	22 of 22 devices complete in every capability; 284 of 284 capabilities	Collected devices with every capability the profile asked for, and that applies, Complete; and those capabilities over every collected device (see the collection status appendix). A device that answered is not counted complete by answering.
Evidence completeness	60 of 60 complete; 59 of 60 dated	Evidence records this document rests on: how many are complete, and how many carry the time they were collected (an undated record cannot be tied to the snapshot).
Report readiness	Draft until validated and reviewed	Decided after generation, not by collection: the report validation record and the engineer review record beside the report (<report>_validation.json, <report>_review.json). A generated document is a draft until an engineer reviews it.
Infrastructure outside NetBox	6 (c4451-hq-r01, c4451-hq-r02, c9300-nth-c01, vsp5520-sth-c01, vsp7520-dc1-c01, vsp7520-dc1-c02)	Switches, firewalls and routers that collected devices report over CDP/LLDP but NetBox does not list.
Discovery completeness	Unknown	Only NetBox devices and their CDP/LLDP neighbours are seen; devices that announce nothing and are not in NetBox cannot be ruled out.

1.2 Key risks and next actions

The highest-severity findings that rest on confirmed or high-confidence evidence, what still needs verifying, what this assessment could not establish, and the recommended next actions. Every finding, with its evidence, is in the findings register of the technical as-built (section 9).

Principal risks

Severity	ID	Risk	Confidence	Next step
HIGH	F-HW-ACBCB3	Power, fan or temperature faults: c9300-hq-a03 power supply PSU 1B (member 1, slot B: Bad). Why it matters: The device runs without its power or cooling redundancy; a further failure can stop it.	Confirmed	Routine controlled change
HIGH	F-SUP-982735	Support has ended (21 Aug 2026) for c9300-hq-a05 (1 serials), although the schedule still lists them as live devices. Why it matters: Without a support contract, hardware replacement and vendor cases are not available when a fault occurs.	High confidence	Investigation
MEDIUM	F-SEC-13E8DF	Access ports have no BPDU guard on vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11, vsp5420-hq-a12, vsp5420-hq-a13, vsp5420-hq-a14, vsp5420-hq-a15, vsp5420-hq-a16. Why it matters: A switch plugged into an access port can join the spanning tree and move the root or cause a loop.	Confirmed	Potentially disruptive change

Severity	ID	Risk	Confidence	Next step
MEDIUM	F-SUP-F35F2E	Hardware whose serials are not on the support schedule (RTG_support_schedule_20261019.xlsx), which does list other equipment of the same manufacturer: c9300-hq-a06. Why it matters: These devices may have no support contract, so a failure may have no replacement path.	High confidence	Investigation

Assessment summary

Item	Detail
Findings	12 in total: 2 high, 2 medium, 5 low, 3 info
Interface health	no interface concerns (413 interfaces)
Dependencies	0 of 16 switches have a single uplink; c9500-hq-c01 carries 2 devices alone
Project readiness	5 confirmed facts, 0 suspected issues, 4 unknowns, 0 design decisions (section 8.4)

Assessment limitations

Item	Detail
Baseline compliance	no approved baseline supplied: differences are inconsistencies, not deviations
Vulnerabilities	not assessed: no local advisory data supplied
Evidence age	regenerated from saved evidence: it describes the network as it was when the evidence was collected (dates in the document control)
Not in scope	structured cabling and patching, wireless controller and SSID configuration, servers and applications, firewall rule content (section 7)

Recommended next actions

#	Action
1	Review the 4 key risks above against the intended design (F-HW-ACBCB3, F-SUP-982735, F-SEC-13E8DF, F-SUP-F35F2E).

1.3 Site architecture overview

The site's structure at a glance: which device each switch and firewall takes its uplink from, from the evidence in this collection.

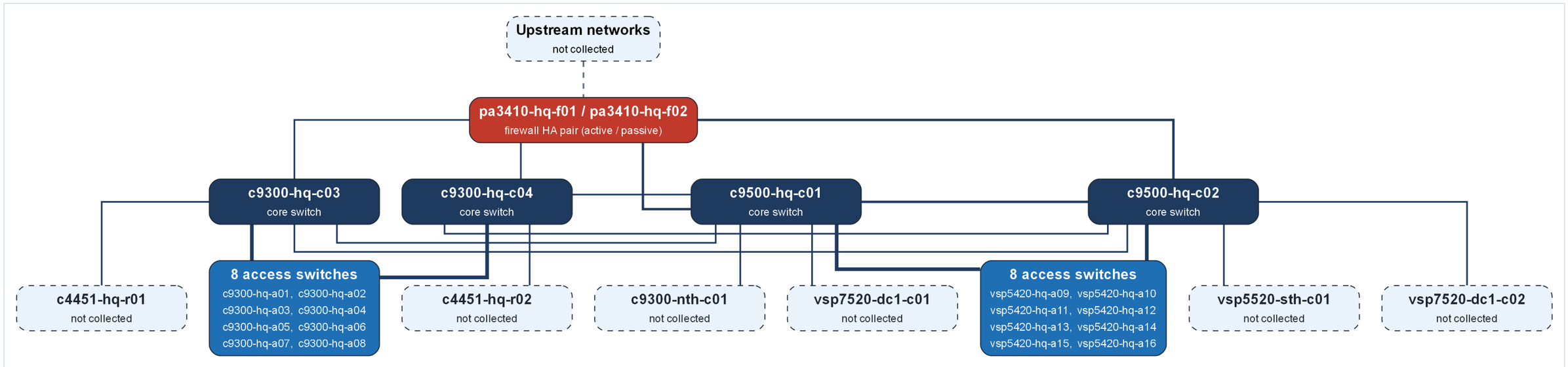


Figure 1 – Site Architecture Overview, RTG-HQ (evidence snapshot 8e957703443f)

Each box is a device, stack, HA pair or fabric pair, placed below the device it takes its uplink from; a box with two lines above it is dual-homed. Lines are the connections the evidence shows (solid: reported by the devices, thicker for more links; dashed orange: inferred; dashed grey: routes or routing peers that lead outside the collected devices). Dashed boxes were not collected. Ports and individual links are in the engineering connectivity diagrams. Upstream: OSPF 10.255.1.2: FULL/BDR; OSPF 10.255.2.2: FULL/BDR; default route via 198.51.100.1. 8 access switches with the same upstream connections are one box: c9300-hq-a01, c9300-hq-a02, c9300-hq-a03, c9300-hq-a04, c9300-hq-a05, c9300-hq-a06, c9300-hq-a07, c9300-hq-a08. 8 access switches with the same upstream connections are one box: vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11, vsp5420-hq-a12, vsp5420-hq-a13, vsp5420-hq-a14, vsp5420-hq-a15, vsp5420-hq-a16. Connected to more than one upstream device (drawn under each): 8 access switches, 8 access switches.

2 Hardware

2.1 Switches

One row per switch or stack, from each switch's version and inventory output collected on 20 Oct 2026. Highlighted models are on the end-of-life list (eol_models.csv), which records no verified source: highlighting is provisional (see Software lifecycle).

Hostname	Location	Manufacturer	Model	Members	Serial Numbers	Software
c9500-hq-c01	RTG-HQ | Building A Level 1 Comms Room | 1 Riverside Way, Riverton	Cisco	C9500-24Y4C	1	SYNF2CA86B6	17.9.5
c9500-hq-c02	RTG-HQ | Building A Level 1 Comms Room | 1 Riverside Way, Riverton	Cisco	C9500-24Y4C	1	SYN4C454DF4	17.9.5
c9300-hq-c03	RTG-HQ | Building A Level 1 Comms Room | 1 Riverside Way, Riverton	Cisco	C9300-24UX	1	SYN35EF3C11	17.9.5
c9300-hq-c04	RTG-HQ | Building A Level 1 Comms Room | 1 Riverside Way, Riverton	Cisco	C9300-24UX	1	SYN61BA24BA	17.9.5
c9300-hq-a01	RTG-HQ | Building A Level 1 Comms Room | 1 Riverside Way, Riverton	Cisco	C9300-48P	2	SYNBED7B6D4, SYNBC2A5F04	17.9.5
c9300-hq-a02	RTG-HQ | Building A Level 1 Comms Room | 1 Riverside Way, Riverton	Cisco	C9300-48P	2	SYNAA1B4C01, SYND5649154	17.9.5
c9300-hq-a03	RTG-HQ | Building A Level 1 Comms Room | 1 Riverside Way, Riverton	Cisco	C9300-48P	1	SYN65691562	17.9.5
c9300-hq-a04	RTG-HQ | Building A Level 2 Comms Room | 1 Riverside Way, Riverton	Cisco	C9300-48P	1	SYNA1DC348A	17.9.5
c9300-hq-a05	RTG-HQ | Building A Level 2 Comms Room | 1 Riverside Way, Riverton	Cisco	C9300-48P	1	SYNB8588C49	17.9.5
c9300-hq-a06	RTG-HQ | Building A Level 2 Comms Room | 1 Riverside Way, Riverton	Cisco	C9300-48P	1	SYN012CF92F	17.9.5

Hostname	Location	Manufacturer	Model	Members	Serial Numbers	Software
c9300-hq-a07	RTG-HQ | Building A Level 3 Comms Room | 1 Riverside Way, Riverton	Cisco	C9300-48P	1	SYND958E333	17.9.5
c9300-hq-a08	RTG-HQ | Building A Level 3 Comms Room | 1 Riverside Way, Riverton	Cisco	C9300-48P	1	SYN83AC15F7	17.9.5
vsp5420-hq-a09	RTG-HQ | Building B Ground Floor Comms Room | 1 Riverside Way, Riverton	Extreme Networks	5420M-48W-4YE-FabricEngine	1	SYNC9F04C91	9.0.6.0
vsp5420-hq-a10	RTG-HQ | Building B Ground Floor Comms Room | 1 Riverside Way, Riverton	Extreme Networks	5420M-48W-4YE-FabricEngine	1	SYN83978195	9.0.6.0
vsp5420-hq-a11	RTG-HQ | Building B Ground Floor Comms Room | 1 Riverside Way, Riverton	Extreme Networks	5420M-48W-4YE-FabricEngine	1	SYN0E24C00E	9.0.6.0
vsp5420-hq-a12	RTG-HQ | Building B Ground Floor Comms Room | 1 Riverside Way, Riverton	Extreme Networks	5420M-48W-4YE-FabricEngine	1	SYNA2207E31	9.0.6.0
vsp5420-hq-a13	RTG-HQ | Building B Ground Floor Comms Room | 1 Riverside Way, Riverton	Extreme Networks	5420M-48W-4YE-FabricEngine	1	SYN56CD105F	9.0.6.0
vsp5420-hq-a14	RTG-HQ | Building B Ground Floor Comms Room | 1 Riverside Way, Riverton	Extreme Networks	5420M-48W-4YE-FabricEngine	1	SYN51F8F1C3	9.0.6.0
vsp5420-hq-a15	RTG-HQ | Building B Ground Floor Comms Room | 1 Riverside Way, Riverton	Extreme Networks	5420M-48W-4YE-FabricEngine	1	SYN29F47270	9.0.6.0
vsp5420-hq-a16	RTG-HQ | Building B Ground Floor Comms Room | 1 Riverside Way, Riverton	Extreme Networks	5420M-48W-4YE-FabricEngine	1	SYN9A6EC4BF	9.0.6.0

2.2 Switch stacks

Members of each switch stack, with their role, stack priority, model and serial number.

Stack	Member	Role	State	Priority	Model	Serial
c9500-hq-c01	1	Active	Ready	15	C9500-24Y4C	SYNF2CA86B6
c9500-hq-c02	1	Active	Ready	15	C9500-24Y4C	SYN4C454DF4
c9300-hq-c03	1	Active	Ready	15	C9300-24UX	SYN35EF3C11
c9300-hq-c04	1	Active	Ready	15	C9300-24UX	SYN61BA24BA
c9300-hq-a01	1	Active	Ready	15	C9300-48P	SYNBED7B6D4
c9300-hq-a01	2	Standby	Ready	14	C9300-48P	SYNBC2A5F04
c9300-hq-a02	1	Active	Ready	15	C9300-48P	SYNAA1B4C01
c9300-hq-a02	2	Standby	Ready	14	C9300-48P	SYND5649154
c9300-hq-a03	1	Active	Ready	15	C9300-48P	SYN65691562
c9300-hq-a04	1	Active	Ready	15	C9300-48P	SYNA1DC348A
c9300-hq-a05	1	Active	Ready	15	C9300-48P	SYNB8588C49
c9300-hq-a06	1	Active	Ready	15	C9300-48P	SYN012CF92F
c9300-hq-a07	1	Active	Ready	15	C9300-48P	SYND958E333
c9300-hq-a08	1	Active	Ready	15	C9300-48P	SYN83AC15F7
vsp5420-hq-a09	1	Active	Ready	15	5420M-48W-4YE-FabricEngine	SYNC9F04C91
vsp5420-hq-a10	1	Active	Ready	15	5420M-48W-4YE-FabricEngine	SYN83978195
vsp5420-hq-a11	1	Active	Ready	15	5420M-48W-4YE-FabricEngine	SYN0E24C00E
vsp5420-hq-a12	1	Active	Ready	15	5420M-48W-4YE-FabricEngine	SYNA2207E31
vsp5420-hq-a13	1	Active	Ready	15	5420M-48W-4YE-FabricEngine	SYN56CD105F
vsp5420-hq-a14	1	Active	Ready	15	5420M-48W-4YE-FabricEngine	SYN51F8F1C3
vsp5420-hq-a15	1	Active	Ready	15	5420M-48W-4YE-FabricEngine	SYN29F47270
vsp5420-hq-a16	1	Active	Ready	15	5420M-48W-4YE-FabricEngine	SYN9A6EC4BF

2.3 Firewalls

From each firewall's system information. Highlighted models are on the end-of-life list, which records no verified source: highlighting is provisional (see Software lifecycle).

Hostname	Manufacturer	Model	Software	Serial	Management IP	HA state
pa3410-hq-f01	Palo Alto Networks	PA-3410	11.1.4-h7	SYND10738E0	10.10.210.251	active
pa3410-hq-f02	Palo Alto Networks	PA-3410	11.1.4-h7	SYNED55B269	10.10.210.252	passive

2.4 Power and environment

Power supplies, fans and temperature sensors as each device reports them, one count per state. "Not reported by platform": the device has no such sensor in its output (the PA-400 series firewalls report thermal only; a fanless switch reports no fans); "not collected": its output was not read; "not installed": an empty supply slot; "down, no module identified": the slot reports down and no module identity could be read (empty or unreadable -- not an installed supply reporting a failure); "no reading": a sensor without a value. Temperatures are judged against each sensor's own warning and critical thresholds. Scope says which stack members a reading covers -- a 3750/2960 stack reports every member's power supply but its fan and temperature for the stack master only; newer stacks name the member on each reading. Highlighted rows have a reported condition.

Device	Power supplies	Fans	Temperature	Scope
c9500-hq-c01	2 OK	3 OK	1 OK	-
c9500-hq-c02	2 OK	3 OK	1 OK	-
c9300-hq-c03	2 OK	3 OK	1 OK	-
c9300-hq-c04	2 OK	3 OK	1 OK	-
c9300-hq-a01	4 OK	6 OK	2 OK	power: members 1, 2; fans: members 1, 2; temperature: members 1, 2
c9300-hq-a02	4 OK	6 OK	2 OK	power: members 1, 2; fans: members 1, 2; temperature: members 1, 2
c9300-hq-a03	1 OK, 1 fault	3 OK	1 OK	-
c9300-hq-a04	2 OK	3 OK	1 OK	-
c9300-hq-a05	2 OK	3 OK	1 OK	-
c9300-hq-a06	2 OK	3 OK	1 OK	-
c9300-hq-a07	2 OK	3 OK	1 OK	-
c9300-hq-a08	2 OK	3 OK	1 OK	-
vsp5420-hq-a09	2 OK	4 OK	3 OK	-
vsp5420-hq-a10	2 OK	4 OK	3 OK	-
vsp5420-hq-a11	2 OK	4 OK	3 OK	-
vsp5420-hq-a12	2 OK	4 OK	3 OK	-
vsp5420-hq-a13	2 OK	4 OK	3 OK	-
vsp5420-hq-a14	2 OK	4 OK	3 OK	-
vsp5420-hq-a15	2 OK	4 OK	3 OK	-
vsp5420-hq-a16	2 OK	4 OK	3 OK	-
pa3410-hq-f01	2 OK	2 OK	1 OK	-
pa3410-hq-f02	2 OK	2 OK	1 OK	-

Readings that are not OK, by stack member and slot, in the device's own words. Highlighted rows are conditions; the others (empty slots, sensors without a reading) are listed for completeness.

Device	Component	Where	State	Device reports	Source
c9300-hq-a03	Power supply PSU 1B	member 1, slot B	Fault	1B PWR-C1-715WAC SYN93F7AA8B Bad Bad Bad 715	show env all

2.5 PoE budget

Power over Ethernet available and in use per switch. Highlighted switches are at 80% or more.

Switch	Available (W)	Used (W)	Used
c9500-hq-c01	740	0	0%
c9500-hq-c02	740	0	0%
c9300-hq-c03	740	0	0%
c9300-hq-c04	740	0	0%
c9300-hq-a01	1480	220	15%
c9300-hq-a02	1480	220	15%
c9300-hq-a03	740	151	20%
c9300-hq-a04	740	151	20%
c9300-hq-a05	740	151	20%
c9300-hq-a06	740	151	20%
c9300-hq-a07	740	151	20%
c9300-hq-a08	740	151	20%
vsp5420-hq-a09	740	28	4%
vsp5420-hq-a10	740	28	4%
vsp5420-hq-a11	740	28	4%
vsp5420-hq-a12	740	28	4%
vsp5420-hq-a13	740	28	4%
vsp5420-hq-a14	740	28	4%
vsp5420-hq-a15	740	28	4%
vsp5420-hq-a16	740	28	4%

2.6 Optics

Pluggable optics by type, from the port status audit. Each one is listed with its switch and port in Appendix A.

Optic	Installed	In use
SFP-25GBase-SR	24	24
SFP-10GBase-SR	20	20
10GbSR	16	16
QSFP-100G-SR4	4	4
QSFP-100G-LR4	2	2
SFP-25GBase-LR	2	2

2.7 Software lifecycle

Running software against lifecycle reference data. For hardware with a last software train, the suggested release is that train and support follows the hardware. Highlighted rows are past end of support or behind their hardware's final train. Reference: Verified means a vendor source checked within the data's age limit; Unverified statuses are shown for planning only, pending verification of the data (software_audit/lifecycle_data/cisco.json records no source, retrieval or verification date; software_audit/lifecycle_data/extreme.json records no source, retrieval or verification date; software_audit/lifecycle_data/paloalto.json records no source, retrieval or verification date).

Reference data status: 0 of 22 rows rest on a verified vendor source; 22 rest on unverified reference data. Their statuses and dates are indicative, for planning only, and are not authoritative until verified.

Device	Software	Status	End of support	Suggested release	Reference
c9500-hq-c01	17.9.5	Supported (unverified)	2028-06-30	-	Unverified
c9500-hq-c02	17.9.5	Supported (unverified)	2028-06-30	-	Unverified
c9300-hq-c03	17.9.5	Supported (unverified)	2028-06-30	-	Unverified
c9300-hq-c04	17.9.5	Supported (unverified)	2028-06-30	-	Unverified
c9300-hq-a01	17.9.5	Supported (unverified)	2028-06-30	-	Unverified
c9300-hq-a02	17.9.5	Supported (unverified)	2028-06-30	-	Unverified
c9300-hq-a03	17.9.5	Supported (unverified)	2028-06-30	-	Unverified
c9300-hq-a04	17.9.5	Supported (unverified)	2028-06-30	-	Unverified
c9300-hq-a05	17.9.5	Supported (unverified)	2028-06-30	-	Unverified
c9300-hq-a06	17.9.5	Supported (unverified)	2028-06-30	-	Unverified
c9300-hq-a07	17.9.5	Supported (unverified)	2028-06-30	-	Unverified
c9300-hq-a08	17.9.5	Supported (unverified)	2028-06-30	-	Unverified
vsp5420-hq-a09	9.0.6.0	Supported (unverified)	2028-12-31	9.1	Unverified
vsp5420-hq-a10	9.0.6.0	Supported (unverified)	2028-12-31	9.1	Unverified
vsp5420-hq-a11	9.0.6.0	Supported (unverified)	2028-12-31	9.1	Unverified
vsp5420-hq-a12	9.0.6.0	Supported (unverified)	2028-12-31	9.1	Unverified
vsp5420-hq-a13	9.0.6.0	Supported (unverified)	2028-12-31	9.1	Unverified
vsp5420-hq-a14	9.0.6.0	Supported (unverified)	2028-12-31	9.1	Unverified
vsp5420-hq-a15	9.0.6.0	Supported (unverified)	2028-12-31	9.1	Unverified
vsp5420-hq-a16	9.0.6.0	Supported (unverified)	2028-12-31	9.1	Unverified
pa3410-hq-f01	11.1.4-h7	Supported (unverified)	2028-12-31	-	Unverified
pa3410-hq-f02	11.1.4-h7	Supported (unverified)	2028-12-31	-	Unverified

2.8 Vulnerability correlation

Not performed: no local advisory data was supplied (ASBUILT_ADVISORIES). The as-built does not query vulnerability databases or upload inventory; software lifecycle statuses above come from vendor lifecycle data only.

2.9 Support contracts

Every collected device and stack member against the customer's support schedule (RTG_support_schedule_20261019.xlsx, which holds records for Cisco, Extreme Networks, Palo Alto Networks), matched by serial number. Covered: a record with a future end date. Expired: its end date has passed. Expiry not provided: a record whose end date the schedule leaves blank ("Not provided in source"). No matching record: the schedule lists this manufacturer but not this serial. Vendor not in schedule: the schedule holds no records of this manufacturer; that is not evidence that support is absent, and another source is needed. Expired rows are red, unmatched amber.

Manufacturer	Assets	Covered	Expired	No matching record
Cisco	14	12	1	1
Extreme Networks	8	8	0	0
Palo Alto Networks	2	2	0	0

Device	Member	Manufacturer	Model	Serial	Coverage	SLA	Starts	Ends
c9500-hq-c01	1	Cisco	C9500-24Y4C	SYNF2CA86B6	Covered	24x7x4	01 Jul 2025	30 Jun 2027
c9500-hq-c02	1	Cisco	C9500-24Y4C	SYN4C454DF4	Covered	24x7x4	01 Jul 2025	30 Jun 2027
c9300-hq-c03	1	Cisco	C9300-24UX	SYN35EF3C11	Covered	24x7x4	01 Jul 2025	30 Jun 2027
c9300-hq-c04	1	Cisco	C9300-24UX	SYN61BA24BA	Covered	24x7x4	01 Jul 2025	30 Jun 2027
c9300-hq-a01	1	Cisco	C9300-48P	SYNBED7B6D4	Covered	8x5xNBD	01 Jul 2025	30 Jun 2027
c9300-hq-a01	2	Cisco	C9300-48P	SYNBC2A5F04	Covered	8x5xNBD	01 Jul 2025	30 Jun 2027
c9300-hq-a02	1	Cisco	C9300-48P	SYNAA1B4C01	Covered	8x5xNBD	01 Jul 2025	30 Jun 2027
c9300-hq-a02	2	Cisco	C9300-48P	SYND5649154	Covered	8x5xNBD	01 Jul 2025	30 Jun 2027
c9300-hq-a03	1	Cisco	C9300-48P	SYN65691562	Covered	8x5xNBD	01 Jul 2025	30 Jun 2027
c9300-hq-a04	1	Cisco	C9300-48P	SYNA1DC348A	Covered	8x5xNBD	01 Jul 2025	30 Jun 2027
c9300-hq-a05	1	Cisco	C9300-48P	SYNB8588C49	Expired	8x5xNBD	22 Aug 2023	21 Aug 2026
c9300-hq-a06	1	Cisco	C9300-48P	SYN012CF92F	No matching record	-	-	-
c9300-hq-a07	1	Cisco	C9300-48P	SYND958E333	Covered	8x5xNBD	01 Jul 2025	30 Jun 2027
c9300-hq-a08	1	Cisco	C9300-48P	SYN83AC15F7	Covered	8x5xNBD	01 Jul 2025	30 Jun 2027

Device	Member	Manufacturer	Model	Serial	Coverage	SLA	Starts	Ends
vsp5420-hq-a09	1	Extreme Networks	5420M-48W-4YE-FabricEngine	SYNC9F04C91	Covered	8x5xNBD	01 Jul 2025	30 Jun 2027
vsp5420-hq-a10	1	Extreme Networks	5420M-48W-4YE-FabricEngine	SYN83978195	Covered	8x5xNBD	01 Jul 2025	30 Jun 2027
vsp5420-hq-a11	1	Extreme Networks	5420M-48W-4YE-FabricEngine	SYN0E24C00E	Covered	8x5xNBD	01 Jul 2025	30 Jun 2027
vsp5420-hq-a12	1	Extreme Networks	5420M-48W-4YE-FabricEngine	SYNA2207E31	Covered	8x5xNBD	01 Jul 2025	30 Jun 2027
vsp5420-hq-a13	1	Extreme Networks	5420M-48W-4YE-FabricEngine	SYN56CD105F	Covered	8x5xNBD	01 Jul 2025	30 Jun 2027
vsp5420-hq-a14	1	Extreme Networks	5420M-48W-4YE-FabricEngine	SYN51F8F1C3	Covered	8x5xNBD	01 Jul 2025	30 Jun 2027
vsp5420-hq-a15	1	Extreme Networks	5420M-48W-4YE-FabricEngine	SYN29F47270	Covered	8x5xNBD	01 Jul 2025	30 Jun 2027
vsp5420-hq-a16	1	Extreme Networks	5420M-48W-4YE-FabricEngine	SYN9A6EC4BF	Covered	8x5xNBD	01 Jul 2025	30 Jun 2027
pa3410-hq-f01	-	Palo Alto Networks	PA-3410	SYND10738E0	Covered	24x7x4	01 Jul 2025	30 Jun 2027
pa3410-hq-f02	-	Palo Alto Networks	PA-3410	SYNED55B269	Covered	24x7x4	01 Jul 2025	30 Jun 2027

3 Connectivity

3.1 WAN services

From the WAN provider's service export.

Service	Type	Status	Circuit ID
Business Internet 1000 Mbps (primary)	Internet	Active	SYN-INT-HQ-0001
Business Internet 1000 Mbps (secondary)	Internet	Active	SYN-INT-HQ-0002
IP address block 198.51.100.0/29	Addressing	Active	SYN-IPB-HQ-0001
Ethernet Private Line HQ - North (VLAN 901)	EPL	Active	SYN-EPL-0901
Ethernet Private Line HQ - South (VLAN 902)	EPL	Active	SYN-EPL-0902
Dark fibre HQ - DC1 (path A)	Dark fibre	Active	SYN-DF-0001
Dark fibre HQ - DC1 (path B)	Dark fibre	Active	SYN-DF-0002

3.2 WAN hand-off

Where the site meets its WAN: the firewall interfaces in WAN zones or facing a BGP peer, with the peering, and below how each firewall's default route is known. An established BGP session is not evidence of a learned default: a learned default is reported only from the firewall's routing table (show routing route destination 0.0.0.0/0); without the table, a default that is not configured statically is reported as not established, not as absent. A passive HA unit runs no dynamic routing, so an idle BGP session there is expected.

Firewall	Interface	Zone	Local IP	WAN peer	Protocol	Peer state	Default route
pa3410-hq-f01	ethernet1/1	untrust	198.51.100.2/29	-	-	-	static via 198.51.100.1
pa3410-hq-f02	ethernet1/1	untrust	198.51.100.2/29	-	-	-	static via 198.51.100.1

Firewall	HA state	Virtual router	Default route	Next hop	Interface	Evidence
pa3410-hq-f01	active	default	static (active in the routing table)	198.51.100.1	ethernet1/1	show routing route destination 0.0.0.0/0: 0.0.0.0/0 via 198.51.100.1 flags A S
pa3410-hq-f02	passive	default	static (active in the routing table)	198.51.100.1	ethernet1/1	show routing route destination 0.0.0.0/0: 0.0.0.0/0 via 198.51.100.1 flags A S; passive HA unit: the route is held, traffic is forwarded by the active unit

3.3 Infrastructure links

Links between switches, firewalls and other network devices, from CDP and LLDP; links to firewalls from the switches' MAC tables and LAG names, and, where nothing else showed it, from hostname unit numbers (marked "inferred from hostnames"). A LAG is shown with its member ports in brackets; "or" means the bundle is split across switches and neither LLDP nor LACP reported which member is on this one. HA links between firewalls are inferred from the addresses on their HA ports. Highlighted rows are a switch connected to itself. Every connection, endpoints included, is in the network mapping workbook.

Hostname	Interface	Neighbour	Neighbour Port	Media
c9500-hq-c01	Hu1/0/25	vsp7520-dc1-c01	1/49	Fibre (SM)
c9500-hq-c01	Hu1/0/27	c9500-hq-c02	Hu1/0/27	Fibre (MM)
c9500-hq-c01	Hu1/0/28	c9500-hq-c02	Hu1/0/28	Fibre (MM)
c9500-hq-c01	Twe1/0/13	c9300-nth-c01	Te1/1/4	Fibre (SM)
c9500-hq-c01	Twe1/0/21	pa3410-hq-f01	ethernet1/5	Fibre (MM)
c9500-hq-c01	Twe1/0/22	pa3410-hq-f01	ethernet1/6	Fibre (MM)
c9500-hq-c02	Hu1/0/25	vsp7520-dc1-c02	1/49	Fibre (SM)
c9500-hq-c02	Twe1/0/13	vsp5520-sth-c01	2/1	Fibre (SM)
c9500-hq-c02	Twe1/0/21	pa3410-hq-f02	ethernet1/5	Fibre (MM)
c9500-hq-c02	Twe1/0/22	pa3410-hq-f02	ethernet1/6	Fibre (MM)
c9300-hq-c03	Te1/0/23	c4451-hq-r01	Gi0/0/1	Copper
c9300-hq-c03	Te1/0/24	pa3410-hq-f01	ethernet1/1	Copper
c9300-hq-c03	Te1/1/1	c9500-hq-c01	Twe1/0/1	Fibre (MM)
c9300-hq-c03	Te1/1/2	c9500-hq-c02	Twe1/0/1	Fibre (MM)
c9300-hq-c04	Te1/0/23	c4451-hq-r02	Gi0/0/1	Copper
c9300-hq-c04	Te1/0/24	pa3410-hq-f02	ethernet1/1	Copper
c9300-hq-c04	Te1/1/1	c9500-hq-c01	Twe1/0/2	Fibre (MM)
c9300-hq-c04	Te1/1/2	c9500-hq-c02	Twe1/0/2	Fibre (MM)
c9300-hq-a01	Te1/1/1	c9300-hq-c03	Te1/0/1	Fibre (MM)
c9300-hq-a01	Te2/1/1	c9300-hq-c04	Te1/0/1	Fibre (MM)
c9300-hq-a02	Te1/1/1	c9300-hq-c03	Te1/0/2	Fibre (MM)
c9300-hq-a02	Te2/1/1	c9300-hq-c04	Te1/0/2	Fibre (MM)
c9300-hq-a03	Te1/1/1	c9300-hq-c03	Te1/0/3	Fibre (MM)
c9300-hq-a03	Te1/1/2	c9300-hq-c04	Te1/0/3	Fibre (MM)
c9300-hq-a04	Te1/1/1	c9300-hq-c03	Te1/0/4	Fibre (MM)
c9300-hq-a04	Te1/1/2	c9300-hq-c04	Te1/0/4	Fibre (MM)
c9300-hq-a05	Te1/1/1	c9300-hq-c03	Te1/0/5	Fibre (MM)
c9300-hq-a05	Te1/1/2	c9300-hq-c04	Te1/0/5	Fibre (MM)
c9300-hq-a06	Te1/1/1	c9300-hq-c03	Te1/0/6	Fibre (MM)
c9300-hq-a06	Te1/1/2	c9300-hq-c04	Te1/0/6	Fibre (MM)

Hostname	Interface	Neighbour	Neighbour Port	Media
c9300-hq-a07	Te1/1/1	c9300-hq-c03	Te1/0/7	Fibre (MM)
c9300-hq-a07	Te1/1/2	c9300-hq-c04	Te1/0/7	Fibre (MM)
c9300-hq-a08	Te1/1/1	c9300-hq-c03	Te1/0/8	Fibre (MM)
c9300-hq-a08	Te1/1/2	c9300-hq-c04	Te1/0/8	Fibre (MM)
vsp5420-hq-a09	1/49	c9500-hq-c01	Twe1/0/3	Fibre (MM)
vsp5420-hq-a09	1/50	c9500-hq-c02	Twe1/0/3	Fibre (MM)
vsp5420-hq-a10	1/49	c9500-hq-c01	Twe1/0/4	Fibre (MM)
vsp5420-hq-a10	1/50	c9500-hq-c02	Twe1/0/4	Fibre (MM)
vsp5420-hq-a11	1/49	c9500-hq-c01	Twe1/0/5	Fibre (MM)
vsp5420-hq-a11	1/50	c9500-hq-c02	Twe1/0/5	Fibre (MM)
vsp5420-hq-a12	1/49	c9500-hq-c01	Twe1/0/6	Fibre (MM)
vsp5420-hq-a12	1/50	c9500-hq-c02	Twe1/0/6	Fibre (MM)
vsp5420-hq-a13	1/49	c9500-hq-c01	Twe1/0/7	Fibre (MM)
vsp5420-hq-a13	1/50	c9500-hq-c02	Twe1/0/7	Fibre (MM)
vsp5420-hq-a14	1/49	c9500-hq-c01	Twe1/0/8	Fibre (MM)
vsp5420-hq-a14	1/50	c9500-hq-c02	Twe1/0/8	Fibre (MM)
vsp5420-hq-a15	1/49	c9500-hq-c01	Twe1/0/9	Fibre (MM)
vsp5420-hq-a15	1/50	c9500-hq-c02	Twe1/0/9	Fibre (MM)
vsp5420-hq-a16	1/49	c9500-hq-c01	Twe1/0/10	Fibre (MM)
vsp5420-hq-a16	1/50	c9500-hq-c02	Twe1/0/10	Fibre (MM)
pa3410-hq-f01	ethernet1/7 (HA1)	pa3410-hq-f02	ethernet1/7 (HA1)	Copper
pa3410-hq-f01	ethernet1/8 (HA2)	pa3410-hq-f02	ethernet1/8 (HA2)	Copper

3.4 Port-channels and LAGs

Link aggregation on each device: Cisco port-channels, Extreme MLTs (SMLT where split across a core pair; the vIST joins the pair), Junos and Palo Alto ae interfaces. Protocol is LACP, PAgP or Static (no negotiation, so a miscabled member is not detected); mode is the LACP mode (active sends LACPDUs, passive only answers; at least one end must be active). VOSS MLTs and firewall aggregates are from the devices' own command output, the rest from the newest configuration backup. A row naming several devices lists the same bundle configured separately on each device (one bundle per device, not one bundle spanning them); a multi-chassis bundle is shown only where the evidence identifies one (SMLT and its vIST). Members up is each member's link state from the device's own port counters: a member that is down or not present leaves the bundle on fewer cables than it is configured for. Highlighted rows are static, down, have one member, or have a member that is not up; "bundle down, members running unbundled" is a bundle whose members have links but did not form it.

Device	LAG	Name	Members	Members up	Protocol	Mode
c9500-hq-c01, c9500-hq-c02	Port-channel1	-	Hu1/0/27, Hu1/0/28	2 of 2	LACP	active
c9500-hq-c01, c9500-hq-c02	Port-channel21	-	Twe1/0/21, Twe1/0/22	2 of 2	LACP	active
pa3410-hq-f01, pa3410-hq-f02	ae1	-	ethernet1/5, ethernet1/6	-	-	-

3.5 Firewall ports

Physical ports and aggregates on each firewall and what they are used for. Ports set to type HA carry the HA control and data links between the pair; they connect firewall to firewall, so no switch reports them. Highlighted rows are down on one unit, or used differently on pa3410-hq-f01 and pa3410-hq-f02.

Port	Role	pa3410-hq-f01 link	pa3410-hq-f02 link
ethernet1/1	Layer 3, zone untrust	up, 1000/full, 198.51.100.2/29	up, 1000/full, 198.51.100.2/29
ethernet1/5	ae1 member	up, 10000/full	up, 10000/full
ethernet1/6	ae1 member	up, 10000/full	up, 10000/full
ethernet1/7	HA1 link	up, 1000/full	up, 1000/full
ethernet1/8	HA2 link	up, 1000/full	up, 1000/full

3.6 Endpoints per switch

Devices that announce themselves over CDP or LLDP on each switch's access ports (IP phones, access points, some printers and servers). PCs and most other devices do not, so these are not the number of devices connected; a switch with none is left out. "MAC only" devices gave no name.

Switch	Access Points	Named Devices	MAC Only	Total
c9300-hq-c03	0	1	0	1
c9300-hq-a01	2	30	0	32
c9300-hq-a02	2	30	0	32
c9300-hq-a03	2	18	0	20
c9300-hq-a04	2	19	0	21
c9300-hq-a05	2	18	0	20
c9300-hq-a06	2	18	0	20
c9300-hq-a07	2	19	0	21
c9300-hq-a08	2	19	0	21
vsp5420-hq-a09	1	3	0	4
vsp5420-hq-a10	1	2	0	3
vsp5420-hq-a11	1	3	0	4
vsp5420-hq-a12	1	3	0	4
vsp5420-hq-a13	1	2	0	3
vsp5420-hq-a14	1	2	0	3
vsp5420-hq-a15	1	3	0	4
vsp5420-hq-a16	1	3	0	4
Total	**24**	**193**	**0**	**217**

3.7 Port capacity

Ports on each switch from the port status audit: connected now, free (enabled but not connected) and administratively disabled. Every port is listed in the port status workbook in the site's audits folder (port_status_audit_output_RTG-HQ.xlsx).

Switch	Ports	Connected	Free	Disabled	Used
c9500-hq-c01	16	16	0	0	100%
c9500-hq-c02	16	16	0	0	100%
c9300-hq-c03	26	13	13	0	50%
c9300-hq-c04	26	12	14	0	46%
c9300-hq-a01	98	34	64	0	35%
c9300-hq-a02	98	34	64	0	35%
c9300-hq-a03	50	22	28	0	44%
c9300-hq-a04	50	23	27	0	46%
c9300-hq-a05	50	22	28	0	44%
c9300-hq-a06	50	22	28	0	44%
c9300-hq-a07	50	23	27	0	46%
c9300-hq-a08	50	23	27	0	46%
vsp5420-hq-a09	52	16	36	0	31%
vsp5420-hq-a10	52	15	37	0	29%
vsp5420-hq-a11	52	16	36	0	31%
vsp5420-hq-a12	52	16	36	0	31%
vsp5420-hq-a13	52	15	37	0	29%
vsp5420-hq-a14	52	15	37	0	29%
vsp5420-hq-a15	52	16	36	0	31%
vsp5420-hq-a16	52	16	36	0	31%
Total	**996**	**385**	**611**	**0**	**39%**

3.8 Physical topology

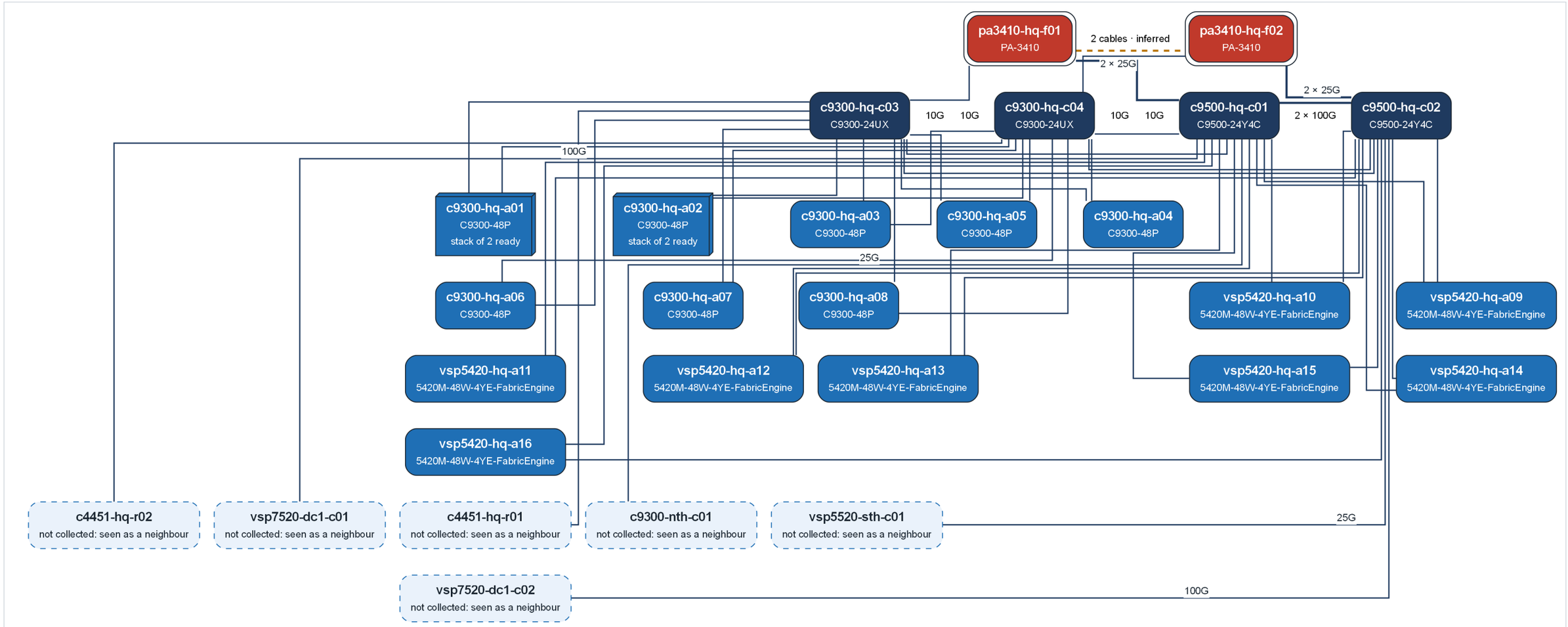


Figure 2 – L1 Physical Topology, RTG-HQ (evidence snapshot 8e957703443f). Dark lines without a label: 10G (36 links)

Switches, stacks, firewalls and the cables between them, from the CDP/LLDP neighbour tables, interface configuration and stack membership in this collection. Solid lines: links a device reported; dashed: inferred (no device reported it); thick lines are the member cables of a LAG, named on the line; a stack is one box with its members. What the evidence does not show is listed on the diagram, not drawn. Scalable copy with its own legend: l1_physical_topology.svg in the report's diagrams folder.

On the figure	Means
Solid dark line	cable(s) between the pair reported by CDP/LLDP; thicker for more cables; label: cable count, speed, LAG
Dashed orange line	inferred link (HA addressing, MAC table): no device reported it
Double line	LAG drawn as one line: its member ports are known but which cable joins which pair of ports is not (or the members were not collected)
Red line	a port reported with two different neighbours (both kept)
3-D box	switch stack: one logical switch; ready and provisioned members stated
Dashed box	device seen only as a neighbour; not collected
Box colour	role: firewall red, core navy, access blue
Unlabelled line	the label most lines of that kind share, stated once in the caption
Tag [1]	a label with no clear room beside its line: its text is in the caption and link notes

Link notes (labels stated once, and the text of tagged labels such as [1])

- Dark lines without a label: 10G (36 links).

Limitations of the evidence for this figure

- Known only from neighbours (not collected): c4451-hq-r01, c4451-hq-r02, c9300-nth-c01, vsp5520-sth-c01, vsp7520-dc1-c01, vsp7520-dc1-c02.

3.9 Engineering connectivity

Every infrastructure link in this collection (52), drawn once, with its upstream device (5 pages; devices with few links share a page, one frame each). Each row of a box is a port; a line joins the two ends of a cable (solid: reported by CDP/LLDP; dashed orange: inferred). Speed and LAG are beside the upstream port; dashed boxes were not collected. CDP/LLDP show the logical neighbour, not the cable path through patch panels.

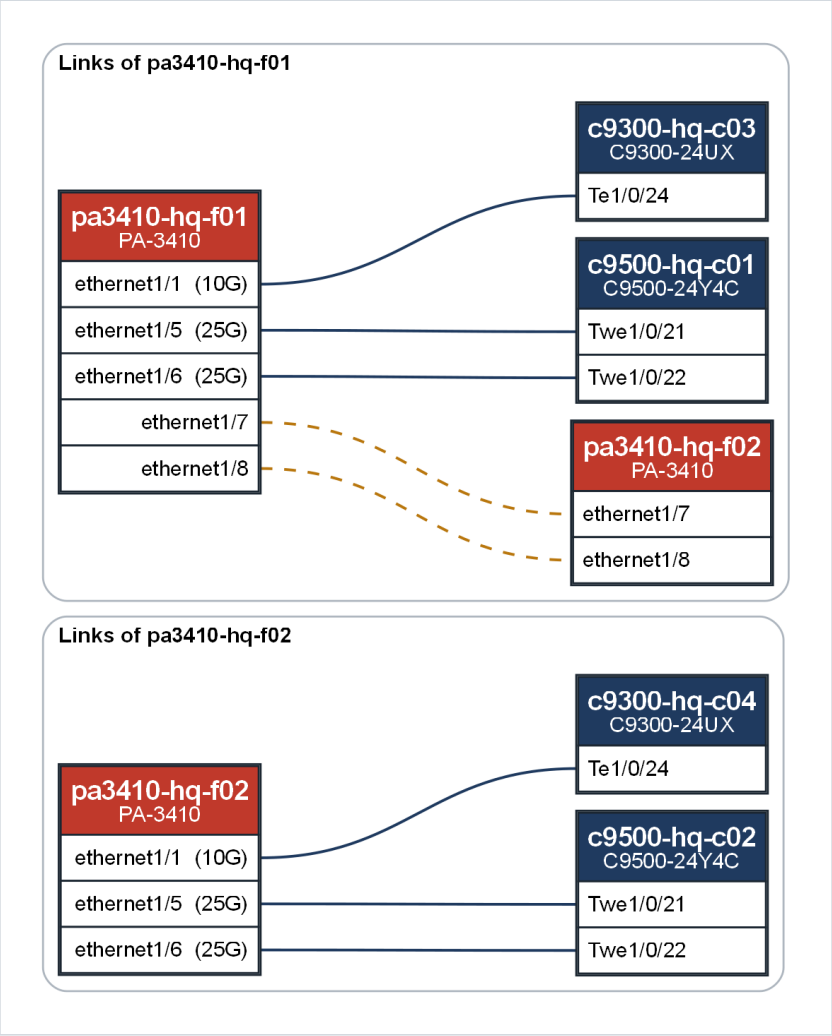


Figure 3 – Engineering Connectivity, page 1 of 5: links of pa3410-hq-f01 and pa3410-hq-f02 (8), RTG-HQ, evidence snapshot 8e957703443f

Engineering connectivity: c9500-hq-c01

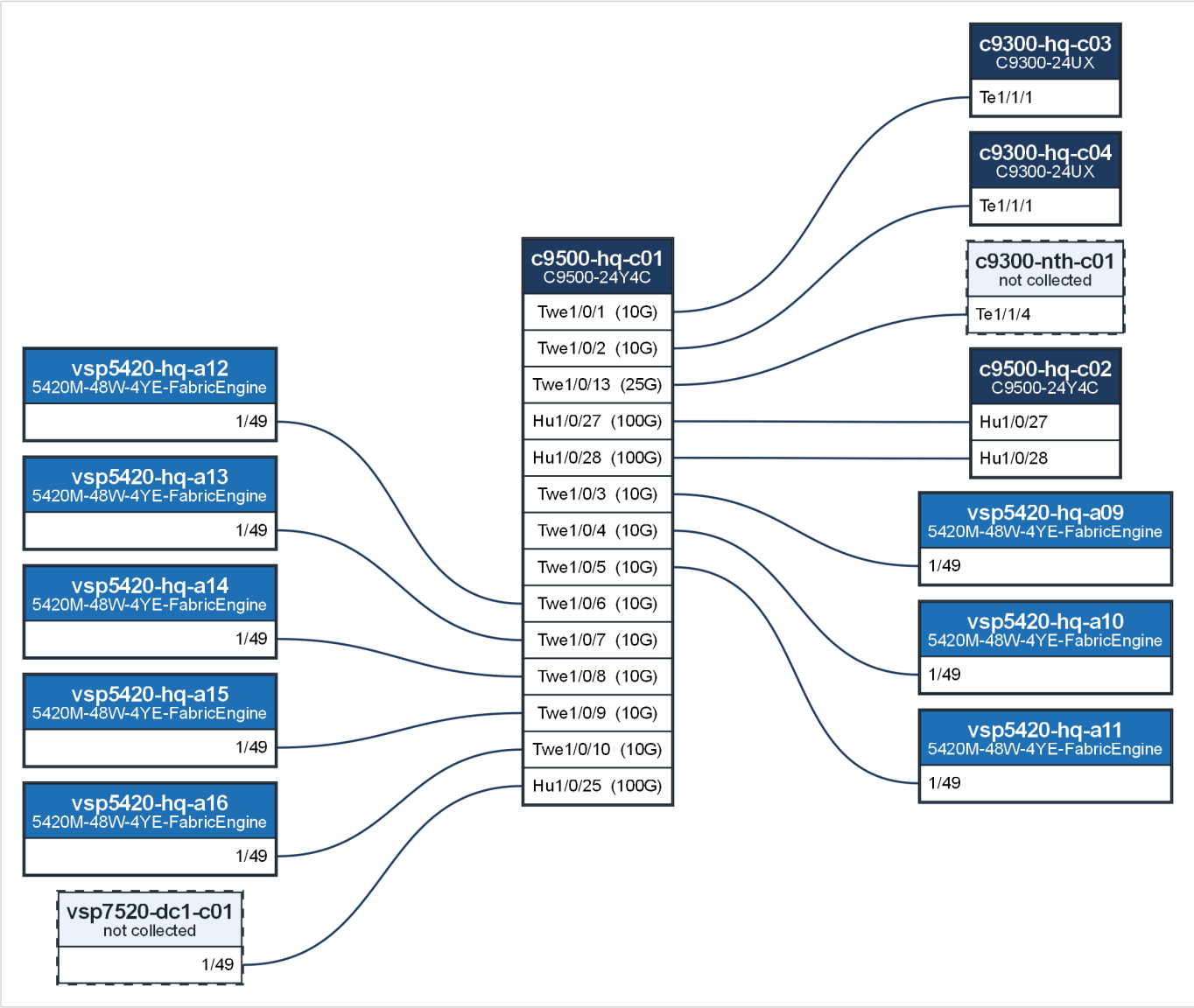


Figure 4 – Engineering Connectivity, page 2 of 5: links of c9500-hq-c01 (14), RTG-HQ, evidence snapshot 8e957703443f

Engineering connectivity: c9500-hq-c02

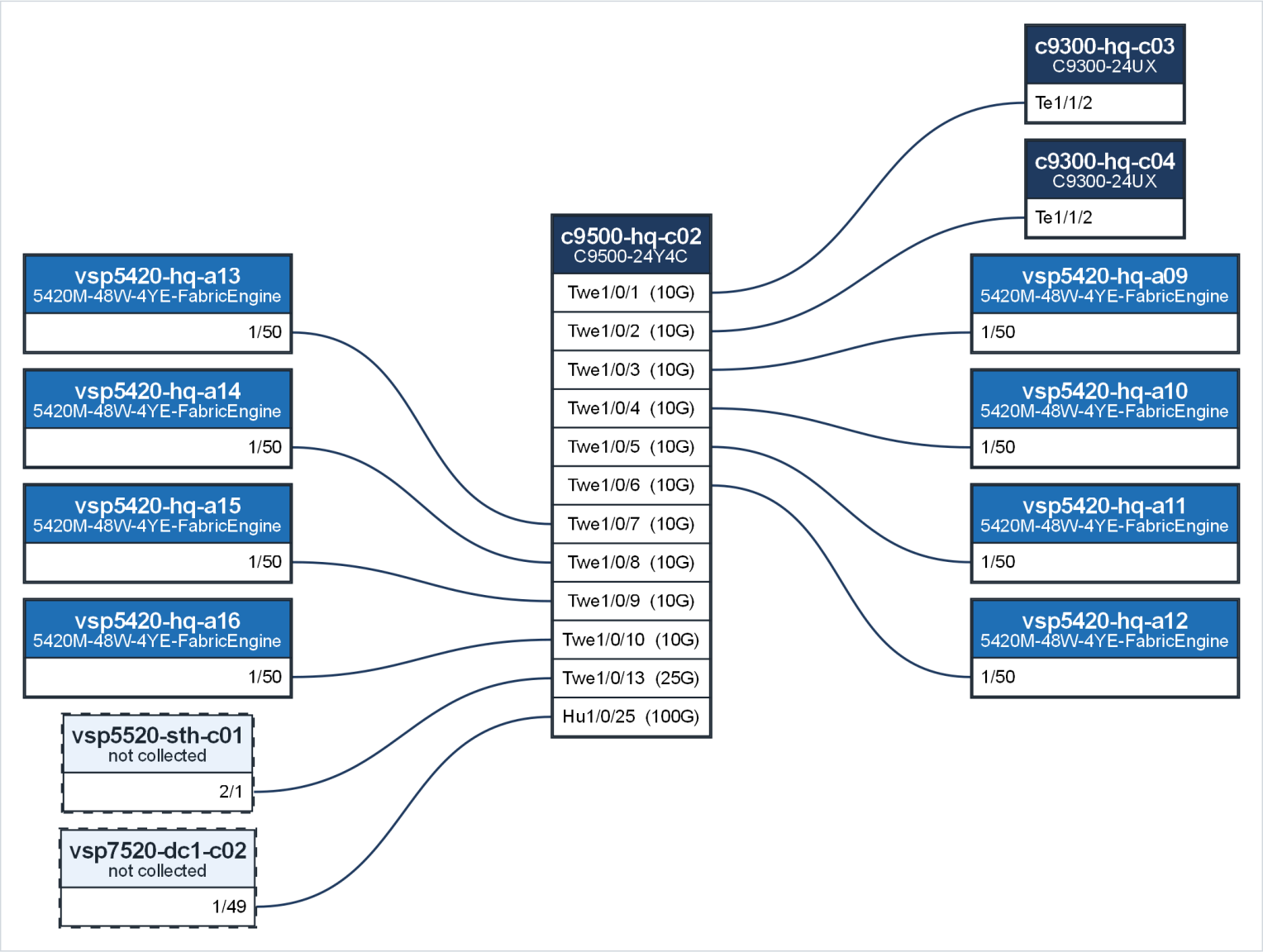


Figure 5 – Engineering Connectivity, page 3 of 5: links of c9500-hq-c02 (12), RTG-HQ, evidence snapshot 8e957703443f

Engineering connectivity: c9300-hq-c03

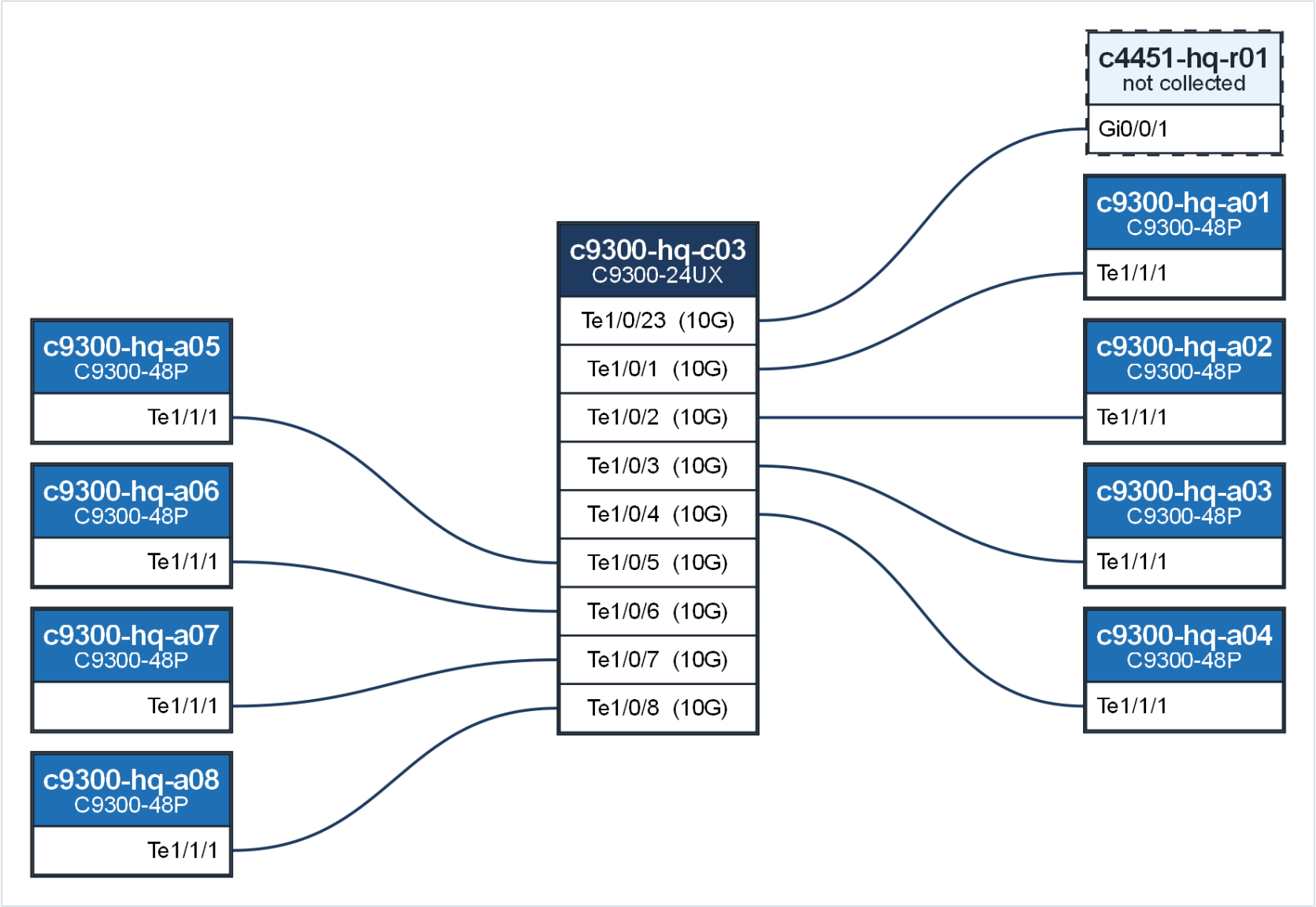


Figure 6 – Engineering Connectivity, page 4 of 5: links of c9300-hq-c03 (9), RTG-HQ, evidence snapshot 8e957703443f

Engineering connectivity: c9300-hq-c04

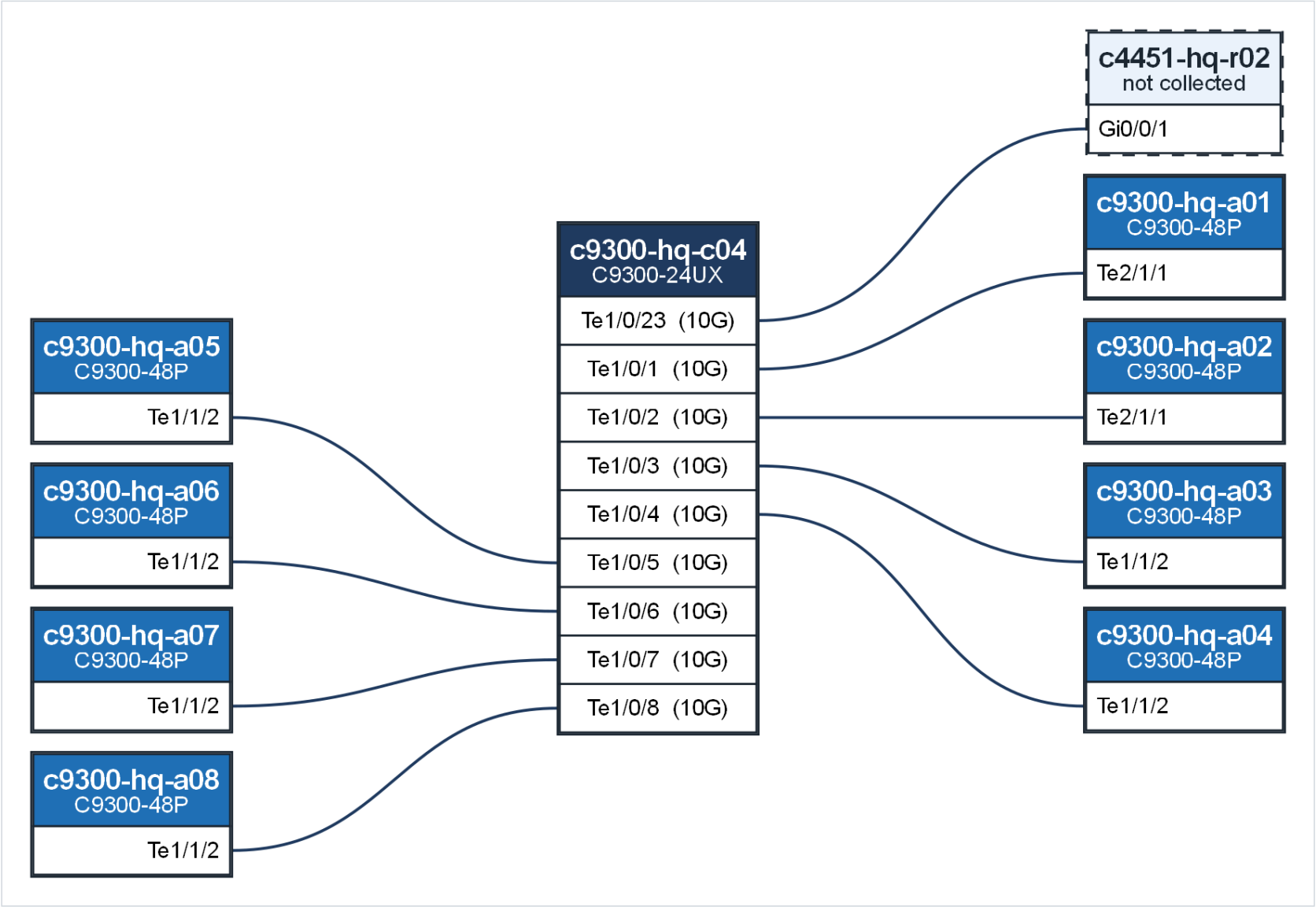


Figure 7 – Engineering Connectivity, page 5 of 5: links of c9300-hq-c04 (9), RTG-HQ, evidence snapshot 8e957703443f

3.10 Interface inventory

Interfaces identified per device and how many of them carry each attribute: operational state and speed (from the device's own 'show interfaces' or the port status audit), configuration -- mode, VLANs, port-channel -- (from the configuration backup or the port status audit), and description. Sources names where the records come from. Every interface with all its values is in the interface inventory export (interfaces_RTG-HQ.csv, interfaces_RTG-HQ.xlsx, in this report's derived folder): "(not collected)" there means no source provided the value; "-" means collected and empty. Errors/discards are cumulative counters (Interface operational health); MAC counts and last change are not collected by this collection.

Device	Interfaces	With state	With configuration	With description	Up	Sources
c9500-hq-c01	30	28	30	16	16	configuration backup, port status audit
c9500-hq-c02	30	28	30	16	16	configuration backup, port status audit
c9300-hq-c03	32	32	32	13	13	configuration backup, port status audit
c9300-hq-c04	32	32	32	12	12	configuration backup, port status audit
c9300-hq-a01	112	112	112	34	34	configuration backup, port status audit
c9300-hq-a02	112	112	112	34	34	configuration backup, port status audit
c9300-hq-a03	56	56	56	22	22	configuration backup, port status audit
c9300-hq-a04	56	56	56	23	23	configuration backup, port status audit
c9300-hq-a05	56	56	56	22	22	configuration backup, port status audit
c9300-hq-a06	56	56	56	22	22	configuration backup, port status audit
c9300-hq-a07	56	56	56	23	23	configuration backup, port status audit
c9300-hq-a08	56	56	56	23	23	configuration backup, port status audit
vsp5420-hq-a09	52	52	52	16	16	configuration backup, port status audit
vsp5420-hq-a10	52	52	52	15	15	configuration backup, port status audit
vsp5420-hq-a11	52	52	52	16	16	configuration backup, port status audit
vsp5420-hq-a12	52	52	52	16	16	configuration backup, port status audit
vsp5420-hq-a13	52	52	52	15	15	configuration backup, port status audit
vsp5420-hq-a14	52	52	52	15	15	configuration backup, port status audit

Device	Interfaces	With state	With configuration	With description	Up	Sources
vsp5420-hq-a15	52	52	52	16	16	configuration backup, port status audit
vsp5420-hq-a16	52	52	52	16	16	configuration backup, port status audit
pa3410-hq-f01	5	5	5	2	5	firewall show interface all
pa3410-hq-f02	5	5	5	2	5	firewall show interface all

3.11 Interface operational health

Interface counters from the switches (Cisco show interfaces; EXOS show ports rxerrors / txerrors / statistics; VOSS show interfaces ... error / statistics). Counters are cumulative since the last clear or reboot, so a count on its own is historical: rates and "increasing" need two samples, and a reboot, cleared counters or a counter that went down voids the comparison. Utilisation comes only from a rate (the switch's 5-minute average, or bytes between two samples), never from byte totals. Thresholds: errors increasing at 10/h (and 10+ errors), utilisation 80%, historical errors above 1e-05 of packets.

413 interfaces (385 ports and port-channels, as in the interface inventory, plus 28 VLAN interfaces) on 20 devices (compared with the previous collection of 2026-07-20 10:40): 413 healthy.

Raw counters for every interface are in the interface health export (interface_health_<site>.csv).

4 Layer 2

4.1 VLANs

VLANs defined on the switches (reserved 1002-1005 omitted).

VLAN	Name	VLAN	Name
1	default	80	SECURITY-SYSTEMS
10	NETWORK-MGMT	110	DMZ
20	CORP-USERS	900	FW-TRANSIT
30	VOICE	901	EPL-NORTH
50	WLAN-CORP	902	EPL-SOUTH
60	WLAN-GUEST	903	DCI-TRANSIT
70	PRINTERS	999	WAN-EDGE

4.2 VTP

VTP mode and domain on the Cisco switches. Servers are highlighted.

Hostname	VTP Mode	VTP Domain
c9500-hq-c01	Transparent	RTG
c9500-hq-c02	Transparent	RTG
c9300-hq-c03	Transparent	RTG
c9300-hq-c04	Transparent	RTG
c9300-hq-a01	Transparent	RTG
c9300-hq-a02	Transparent	RTG
c9300-hq-a03	Transparent	RTG
c9300-hq-a04	Transparent	RTG
c9300-hq-a05	Transparent	RTG
c9300-hq-a06	Transparent	RTG
c9300-hq-a07	Transparent	RTG
c9300-hq-a08	Transparent	RTG

4.3 Spanning tree

Spanning-tree mode and the VLANs each switch is root for, from show spanning-tree summary. Highlighted rows are switches other than the core acting as root. Fabric Connect switches are each the root of their own spanning-tree domain by design (IS-IS/SPBM joins them) and are not highlighted.

Hostname	Mode	Root bridge for VLANs
c9500-hq-c01	rapid-pvst	1, 10, 20, 30, 50, 60, 70, 80, 110, 900-903, 999
c9500-hq-c02	rapid-pvst	none
c9300-hq-c03	rapid-pvst	none
c9300-hq-c04	rapid-pvst	none
c9300-hq-a01	rapid-pvst	none
c9300-hq-a02	rapid-pvst	none
c9300-hq-a03	rapid-pvst	none
c9300-hq-a04	rapid-pvst	none
c9300-hq-a05	rapid-pvst	none
c9300-hq-a06	rapid-pvst	none
c9300-hq-a07	rapid-pvst	none
c9300-hq-a08	rapid-pvst	none
vsp5420-hq-a09	MSTP	none
vsp5420-hq-a10	MSTP	none
vsp5420-hq-a11	MSTP	none
vsp5420-hq-a12	MSTP	none
vsp5420-hq-a13	MSTP	none
vsp5420-hq-a14	MSTP	none
vsp5420-hq-a15	MSTP	none
vsp5420-hq-a16	MSTP	none

Spanning-tree evidence per switch, from show spanning-tree root / bridge / blockedports (Cisco), show stpd detail / ports (EXOS) and show spanning-tree mstp|rstp status / port role (VOSS). "Root for" lists the VLANs or instances where the switch reports itself as root. Statuses other than collected are stated, not omitted: not supported means the switch did not recognise the commands; not applicable marks a Fabric Connect switch, where IS-IS/SPBM rather than spanning tree prevents loops between fabric switches.

Device	Status	Protocol	Priority	Root for	Root port	Root cost	Blocked ports	Note
c9500-hq-c01	collected	rapid-pvst	-	1, 10, 20, 30, 50, 60, 70, 80, 110, 900-903, 999	-	-	-	root per VLAN only (bridge IDs and port roles not in this collection)
c9500-hq-c02	collected	rapid-pvst	-	-	HundredGigE1/0/27	2	-	root per VLAN only (bridge IDs and port roles not in this collection)
c9300-hq-c03	collected	rapid-pvst	-	-	TenGigabitEthernet1/1/1	2	-	root per VLAN only (bridge IDs and port roles not in this collection)
c9300-hq-c04	collected	rapid-pvst	-	-	TenGigabitEthernet1/1/1	2	-	root per VLAN only (bridge IDs and port roles not in this collection)
c9300-hq-a01	collected	rapid-pvst	-	-	TenGigabitEthernet1/1/1	4	-	root per VLAN only (bridge IDs and port roles not in this collection)
c9300-hq-a02	collected	rapid-pvst	-	-	TenGigabitEthernet1/1/1	4	-	root per VLAN only (bridge IDs and port roles not in this collection)
c9300-hq-a03	collected	rapid-pvst	-	-	TenGigabitEthernet1/1/1	4	-	root per VLAN only (bridge IDs and port roles not in this collection)
c9300-hq-a04	collected	rapid-pvst	-	-	TenGigabitEthernet1/1/1	4	-	root per VLAN only (bridge IDs and port roles not in this collection)
c9300-hq-a05	collected	rapid-pvst	-	-	TenGigabitEthernet1/1/1	4	-	root per VLAN only (bridge IDs and port roles not in this collection)
c9300-hq-a06	collected	rapid-pvst	-	-	TenGigabitEthernet1/1/1	4	-	root per VLAN only (bridge IDs and port roles not in this collection)

Device	Status	Protocol	Priority	Root for	Root port	Root cost	Blocked ports	Note
c9300-hq-a07	collected	rapid-pvst	-	-	TenGigabitEthernet1/1/1	4	-	root per VLAN only (bridge IDs and port roles not in this collection)
c9300-hq-a08	collected	rapid-pvst	-	-	TenGigabitEthernet1/1/1	4	-	root per VLAN only (bridge IDs and port roles not in this collection)
vsp5420-hq-a09	collected	MSTP	32768	-	1/49	2000	1	Fabric Connect switch: spanning tree is not the loop prevention on fabric links
vsp5420-hq-a10	collected	MSTP	32768	-	1/49	2000	1	Fabric Connect switch: spanning tree is not the loop prevention on fabric links
vsp5420-hq-a11	collected	MSTP	32768	-	1/49	2000	1	Fabric Connect switch: spanning tree is not the loop prevention on fabric links
vsp5420-hq-a12	collected	MSTP	32768	-	1/49	2000	1	Fabric Connect switch: spanning tree is not the loop prevention on fabric links
vsp5420-hq-a13	collected	MSTP	32768	-	1/49	2000	1	Fabric Connect switch: spanning tree is not the loop prevention on fabric links
vsp5420-hq-a14	collected	MSTP	32768	-	1/49	2000	1	Fabric Connect switch: spanning tree is not the loop prevention on fabric links

Device	Status	Protocol	Priority	Root for	Root port	Root cost	Blocked ports	Note
vsp5420-hq-a15	collected	MSTP	32768	-	1/49	2000	1	Fabric Connect switch: spanning tree is not the loop prevention on fabric links
vsp5420-hq-a16	collected	MSTP	32768	-	1/49	2000	1	Fabric Connect switch: spanning tree is not the loop prevention on fabric links

Root bridges, identified by matching each root bridge MAC with the bridge IDs the switches report for themselves (a root no collected switch owns is shown as outside the collected devices, not guessed). Highlighted: a root outside the collected devices -- the switches that see it take their spanning-tree topology from a bridge this collection did not read, through the root port shown.

Root bridge	Bridge MAC	VLANs / instances	Seen by (root port)
c9500-hq-c01	02:72:74:e1:a8:65	1, 10, 20, 30, 50, 60, 70, 80, 110, 900-903, 999, CIST	c9300-hq-a01 (TenGigabitEthernet1/1/1), c9300-hq-a02 (TenGigabitEthernet1/1/1), c9300-hq-a03 (TenGigabitEthernet1/1/1), c9300-hq-a04 (TenGigabitEthernet1/1/1), c9300-hq-a05 (TenGigabitEthernet1/1/1), c9300-hq-a06 (TenGigabitEthernet1/1/1), c9300-hq-a07 (TenGigabitEthernet1/1/1), c9300-hq-a08 (TenGigabitEthernet1/1/1), c9300-hq-c03 (TenGigabitEthernet1/1/1), c9300-hq-c04 (TenGigabitEthernet1/1/1), c9500-hq-c02 (HundredGigE1/0/27), vsp5420-hq-a09 (1/49), vsp5420-hq-a10 (1/49), vsp5420-hq-a11 (1/49), vsp5420-hq-a12 (1/49), vsp5420-hq-a13 (1/49), vsp5420-hq-a14 (1/49), vsp5420-hq-a15 (1/49), vsp5420-hq-a16 (1/49)

4.4 Fabric Connect

Shortest Path Bridging on the Extreme Fabric Engine switches: each switch's nickname, its IS-IS adjacencies (fabric links), the switches on the other end of them (from the cabling, not the name each one announces) and the services (I-SIDs) it carries. Highlighted rows have an adjacency that is not up.

Switch	Nickname	B-VLANs	IS-IS adjacencies	Neighbours	I-SIDs
vsp5420-hq-a09	0.0a.13	4051,4052	-	-	-
vsp5420-hq-a10	0.0a.14	4051,4052	-	-	-
vsp5420-hq-a11	0.0a.15	4051,4052	-	-	-
vsp5420-hq-a12	0.0a.16	4051,4052	-	-	-
vsp5420-hq-a13	0.0a.17	4051,4052	-	-	-
vsp5420-hq-a14	0.0a.18	4051,4052	-	-	-
vsp5420-hq-a15	0.0a.19	4051,4052	-	-	-
vsp5420-hq-a16	0.0a.1a	4051,4052	-	-	-

4.5 Switching topology

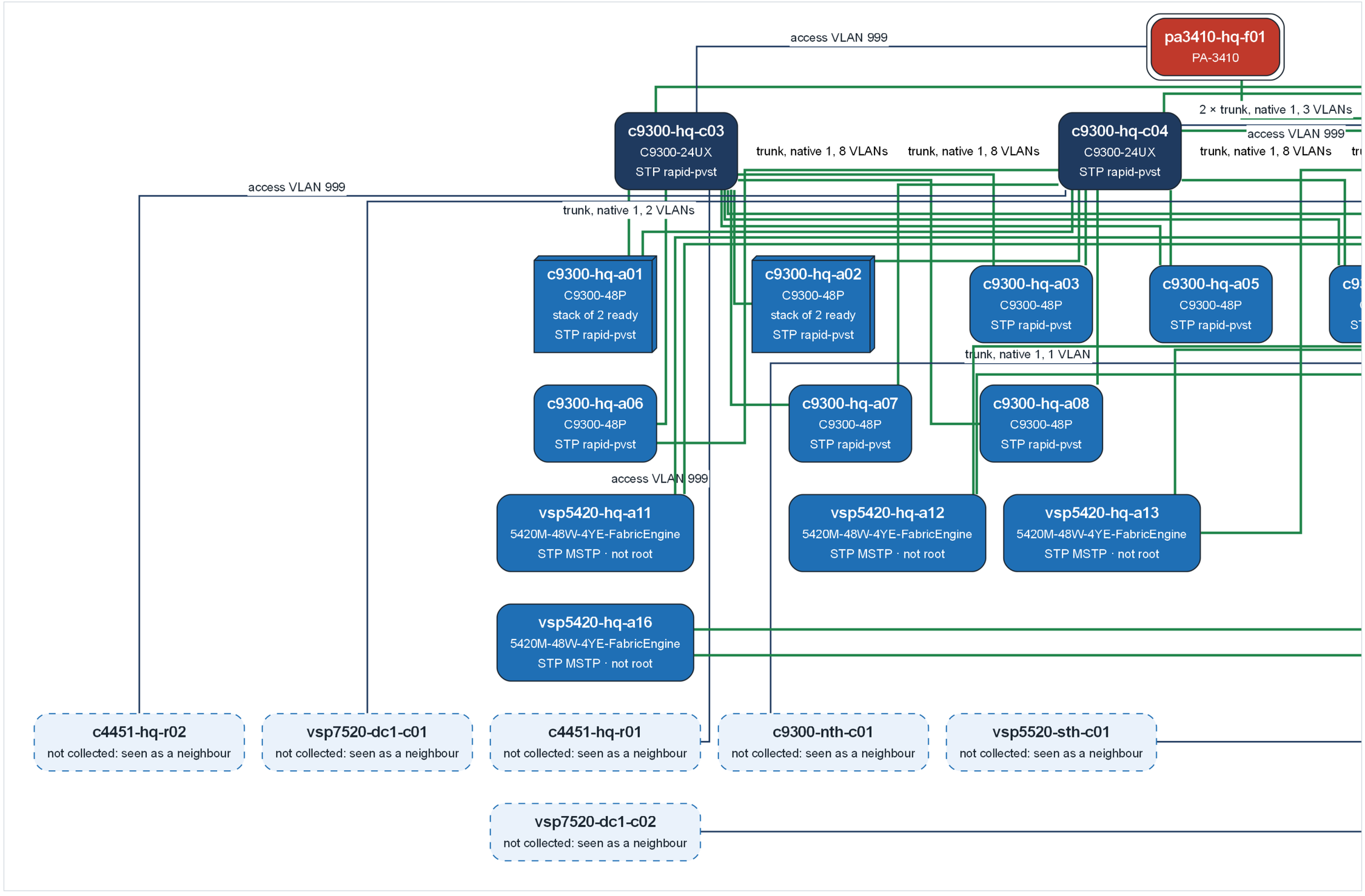


Figure 8 – L2 Switching Topology, RTG-HQ (evidence snapshot 8e957703443f). Green lines without a label: trunk, native 1, 7 VLANs (32 links) (part 1 of 2, left to right)

Switching topology (part 2 of 2, left to right)

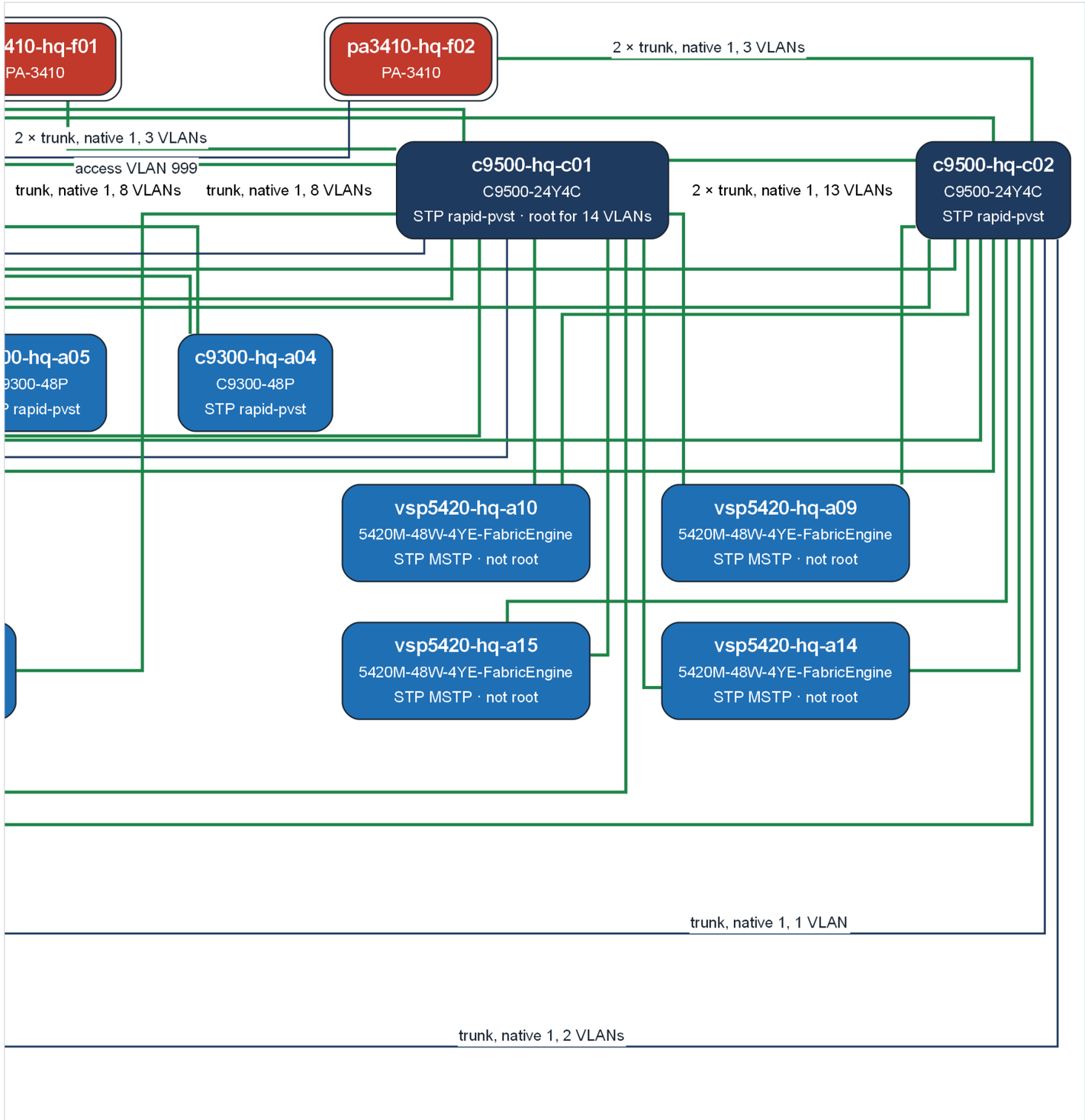


Figure 9 – L2 Switching Topology, RTG-HQ (evidence snapshot 8e957703443f). Green lines without a label: trunk, native 1, 7 VLANs (32 links) (part 2 of 2, left to right)

The links between switches and firewalls with each end's switchport mode as its configuration backup shows it (trunk native and allowed VLANs, or access VLAN), and each switch's spanning-tree mode and root VLANs from the audit. Trunk membership is never inferred from matching VLAN numbers; a port with no configuration is shown as not collected. Access ports to endpoints are left out. Scalable copy with its own legend: l2_switching_topology.svg in the report's diagrams folder.

On the figure	Means
Thick green line	trunk at the switch end(s); labelled with the native VLAN and how many VLANs are allowed where the configuration was collected (unlabelled: port status only)
Solid dark line	access or mixed modes, as each end is configured
Grey line, no label	no configuration or port status for the switch end(s): mode not collected
Dashed orange line	link inferred, not reported
Purple line	Fabric Connect IS-IS adjacency the switches reported (dotted: not up)
Box text	spanning-tree mode and how many VLANs (or which instance) the switch is root for; 'STP not collected' where neither the audit nor the spanning-tree output returned it
Caption: lines without a label	where the caption says so, unlabelled lines of that kind carry the label stated there (most of them share it)
Tag [1]	a label with no clear room beside its line: its text is in the caption and link notes

Link notes (labels stated once, and the text of tagged labels such as [1])

• Green lines without a label: trunk, native 1, 7 VLANs (32 links).

Limitations of the evidence for this figure

• Known only from neighbours (not collected): c4451-hq-r01, c4451-hq-r02, c9300-nth-c01, vsp5520-sth-c01, vsp7520-dc1-c01, vsp7520-dc1-c02.

• 6 link ends have neither configuration nor port status (mostly devices not collected): their mode is not collected and not assumed (grey, unlabelled lines).

5 Layer 3

5.1 Switch Layer 3 interfaces

Addressed interfaces on each switch.

Switch	Interface	IP Address
c9500-hq-c01	Vlan10	10.10.210.2
	Vlan20	10.10.20.2
	Vlan30	10.10.30.2
	Vlan50	10.10.50.2
	Vlan70	10.10.70.2
	Vlan80	10.10.80.2
	Vlan900	10.10.250.2
	Vlan901	10.255.1.1
	Vlan903	10.255.3.2
c9500-hq-c02	Vlan10	10.10.210.3
	Vlan20	10.10.20.3
	Vlan30	10.10.30.3
	Vlan50	10.10.50.3
	Vlan70	10.10.70.3
	Vlan80	10.10.80.3
	Vlan900	10.10.250.3
	Vlan902	10.255.2.1
	Vlan903	10.255.3.3
c9300-hq-c03	Vlan10	10.10.210.4
c9300-hq-c04	Vlan10	10.10.210.5
c9300-hq-a01	Vlan10	10.10.210.11
c9300-hq-a02	Vlan10	10.10.210.12
c9300-hq-a03	Vlan10	10.10.210.13
c9300-hq-a04	Vlan10	10.10.210.14
c9300-hq-a05	Vlan10	10.10.210.15
c9300-hq-a06	Vlan10	10.10.210.16
c9300-hq-a07	Vlan10	10.10.210.17
c9300-hq-a08	Vlan10	10.10.210.18
vsp5420-hq-a09	Vlan10	10.10.210.19
vsp5420-hq-a10	Vlan10	10.10.210.20
vsp5420-hq-a11	Vlan10	10.10.210.21

Switch	Interface	IP Address
vsp5420-hq-a12	Vlan10	10.10.210.22
vsp5420-hq-a13	Vlan10	10.10.210.23
vsp5420-hq-a14	Vlan10	10.10.210.24
vsp5420-hq-a15	Vlan10	10.10.210.25
vsp5420-hq-a16	Vlan10	10.10.210.26

5.2 Firewall interfaces

Logical interfaces from each firewall's interface table. Shown side by side for the HA pair; highlighted rows differ between pa3410-hq-f01 and pa3410-hq-f02 or have a VLAN tag that does not match the sub-interface number. Zone names are truncated by the firewall's own output.

Interface	Zone	Tag	pa3410-hq-f01 IP	pa3410-hq-f02 IP	Forwarding
ae1.60	guest	60	10.10.60.1/24	10.10.60.1/24	vr:default
ae1.110	dmz	110	10.10.110.1/24	10.10.110.1/24	vr:default
ae1.900	trust	900	10.10.250.4/29	10.10.250.4/29	vr:default
ethernet1/1	untrust	0	198.51.100.2/29	198.51.100.2/29	vr:default

5.3 Firewall zones

Security zones on each firewall and the interfaces in them.



Figure 10 – Firewall zones and interfaces, RTG-HQ

5.4 Firewall routing

Routing summary from each firewall. A BGP session that is not established is highlighted, except on a passive HA unit, which runs no dynamic routing.

Firewall	Item	Detail
pa3410-hq-f01	Routes (all address families)	8
	Virtual router default	4 interfaces: ae1.60, ae1.110, ae1.900, ethernet1/1
pa3410-hq-f02	Routes (all address families)	8
	Virtual router default	4 interfaces: ae1.60, ae1.110, ae1.900, ethernet1/1

5.5 Default gateways and static routes

Gateways and static routes configured on the switches and firewalls (dynamic routes are summarised above).

Device	Route	Next hop	Interface
c9300-hq-c03	default gateway	10.10.210.1	-
c9300-hq-c04	default gateway	10.10.210.1	-
c9300-hq-a01	default gateway	10.10.210.1	-
c9300-hq-a02	default gateway	10.10.210.1	-
c9300-hq-a03	default gateway	10.10.210.1	-
c9300-hq-a04	default gateway	10.10.210.1	-
c9300-hq-a05	default gateway	10.10.210.1	-
c9300-hq-a06	default gateway	10.10.210.1	-
c9300-hq-a07	default gateway	10.10.210.1	-
c9300-hq-a08	default gateway	10.10.210.1	-
pa3410-hq-f01 and pa3410-hq-f02	0.0.0.0/0	198.51.100.1	ethernet1/1

5.6 DHCP and DNS relay

Interfaces that forward DHCP requests to a server on another subnet (Cisco ip helper-address, VOSS dhcp-relay, Junos dhcp-relay, Palo Alto DHCP relay), read from each device's newest configuration backup. Highlighted interfaces are shut down. No DNS relay or proxy is configured on any switch or firewall (Cisco ip dns server, Palo Alto DNS proxy, Junos DNS proxy).

Device	Interface	VLAN	Address	Relays DHCP to	State
c9500-hq-c01	Vlan20	20	10.10.20.2/24	10.21.100.61	up
c9500-hq-c01	Vlan50	50	10.10.50.2/24	10.21.100.61	up
c9500-hq-c02	Vlan20	20	10.10.20.3/24	10.21.100.61	up
c9500-hq-c02	Vlan50	50	10.10.50.3/24	10.21.100.61	up

5.7 Gateway redundancy (VRRP/HSRP)

First-hop redundancy groups on the routed interfaces: the virtual gateway address the hosts use, each router's priority (the highest is active) and whether it takes the role back when it recovers (preempt); a value the configuration does not set is the protocol's default (priority 100). The peer is the other device holding the same group and address. Highlighted groups have no peer in the backups or are not enabled. Subnets routed by the firewalls fail over with the firewall HA pair instead.

Device	Interface	VLAN	Address	Protocol	Virtual IP	Priority	Preempt	Peer
c9500-hq-c01	Vlan10	10	10.10.210.2/24	HSRP 10	10.10.210.1	110	yes	c9500-hq-c02
c9500-hq-c01	Vlan20	20	10.10.20.2/24	HSRP 20	10.10.20.1	110	yes	c9500-hq-c02
c9500-hq-c01	Vlan30	30	10.10.30.2/24	HSRP 30	10.10.30.1	110	yes	c9500-hq-c02
c9500-hq-c01	Vlan50	50	10.10.50.2/24	HSRP 50	10.10.50.1	110	yes	c9500-hq-c02
c9500-hq-c01	Vlan70	70	10.10.70.2/24	HSRP 70	10.10.70.1	110	yes	c9500-hq-c02
c9500-hq-c01	Vlan80	80	10.10.80.2/24	HSRP 80	10.10.80.1	110	yes	c9500-hq-c02
c9500-hq-c01	Vlan900	900	10.10.250.2/29	HSRP 135	10.10.250.1	110	yes	c9500-hq-c02
c9500-hq-c02	Vlan10	10	10.10.210.3/24	HSRP 10	10.10.210.1	100	yes	c9500-hq-c01
c9500-hq-c02	Vlan20	20	10.10.20.3/24	HSRP 20	10.10.20.1	100	yes	c9500-hq-c01
c9500-hq-c02	Vlan30	30	10.10.30.3/24	HSRP 30	10.10.30.1	100	yes	c9500-hq-c01
c9500-hq-c02	Vlan50	50	10.10.50.3/24	HSRP 50	10.10.50.1	100	yes	c9500-hq-c01
c9500-hq-c02	Vlan70	70	10.10.70.3/24	HSRP 70	10.10.70.1	100	yes	c9500-hq-c01
c9500-hq-c02	Vlan80	80	10.10.80.3/24	HSRP 80	10.10.80.1	100	yes	c9500-hq-c01
c9500-hq-c02	Vlan900	900	10.10.250.3/29	HSRP 135	10.10.250.1	100	yes	c9500-hq-c01

5.8 Routing adjacencies

BGP, OSPF, EIGRP and RIP neighbours of every switch and firewall, with the AS or area and the session state. A neighbour on the site is named; anything else is an external peer. Highlighted sessions are not established (a passive HA unit's idle BGP session is expected and not highlighted).

Device	Protocol	Neighbour	Neighbour device	AS / area	State
c9500-hq-c01	OSPF	10.255.1.2		-	FULL/BDR
c9500-hq-c01	OSPF	10.10.250.3	c9500-hq-c02	-	FULL/BDR
c9500-hq-c02	OSPF	10.255.2.2		-	FULL/BDR
c9500-hq-c02	OSPF	10.10.250.2	c9500-hq-c01	-	FULL/BDR

5.9 Routing peerings

Each line is a routing adjacency, coloured by protocol and labelled with its AS or area and state. Site devices are grouped by their BGP AS; external peers by theirs.

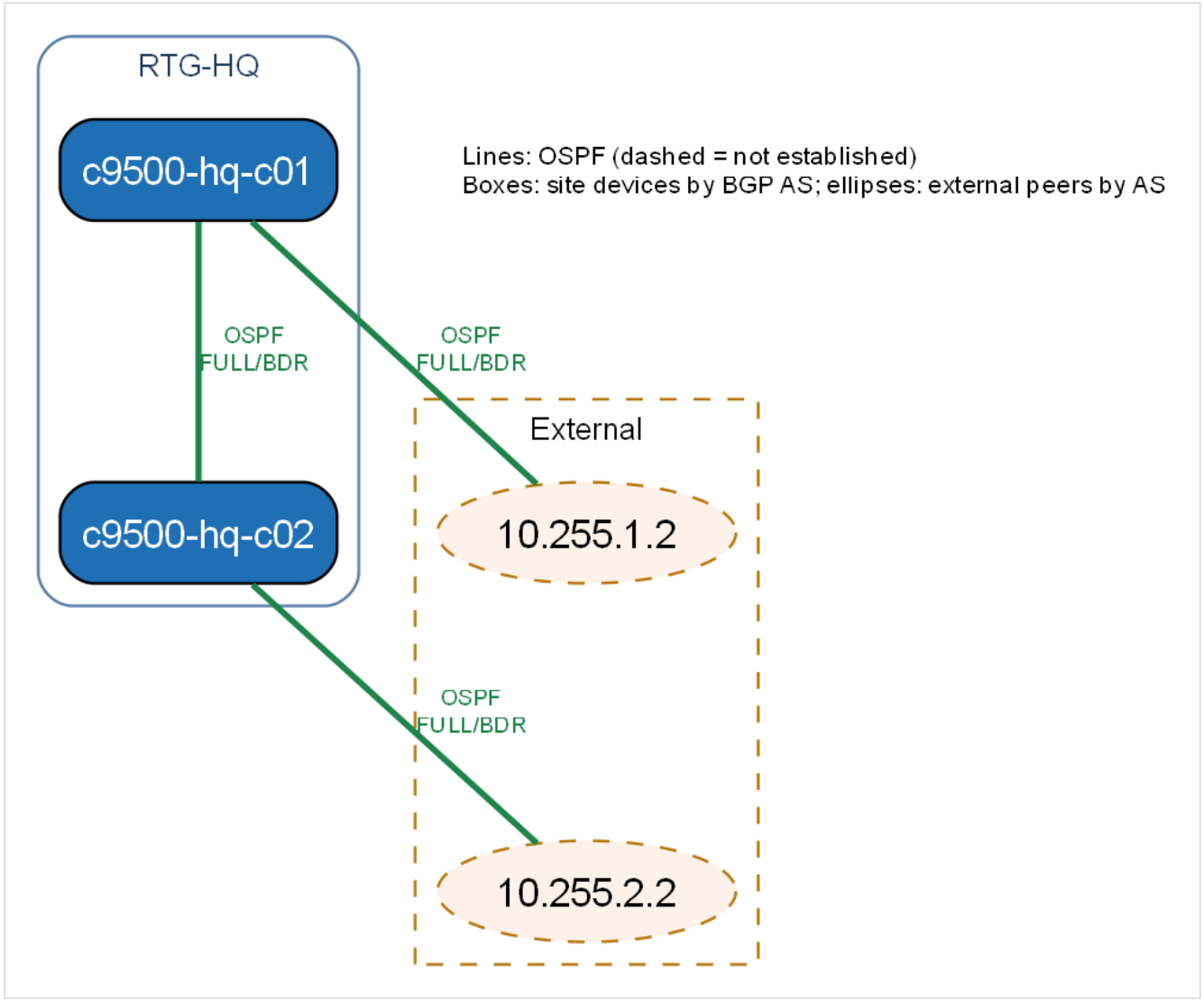


Figure 11 – Routing peerings by protocol, AS and area, RTG-HQ

5.10 Subnets

Every subnet with an interface on a switch or firewall, and the interface and host address on it. An HA pair holding the same subnets is drawn once.

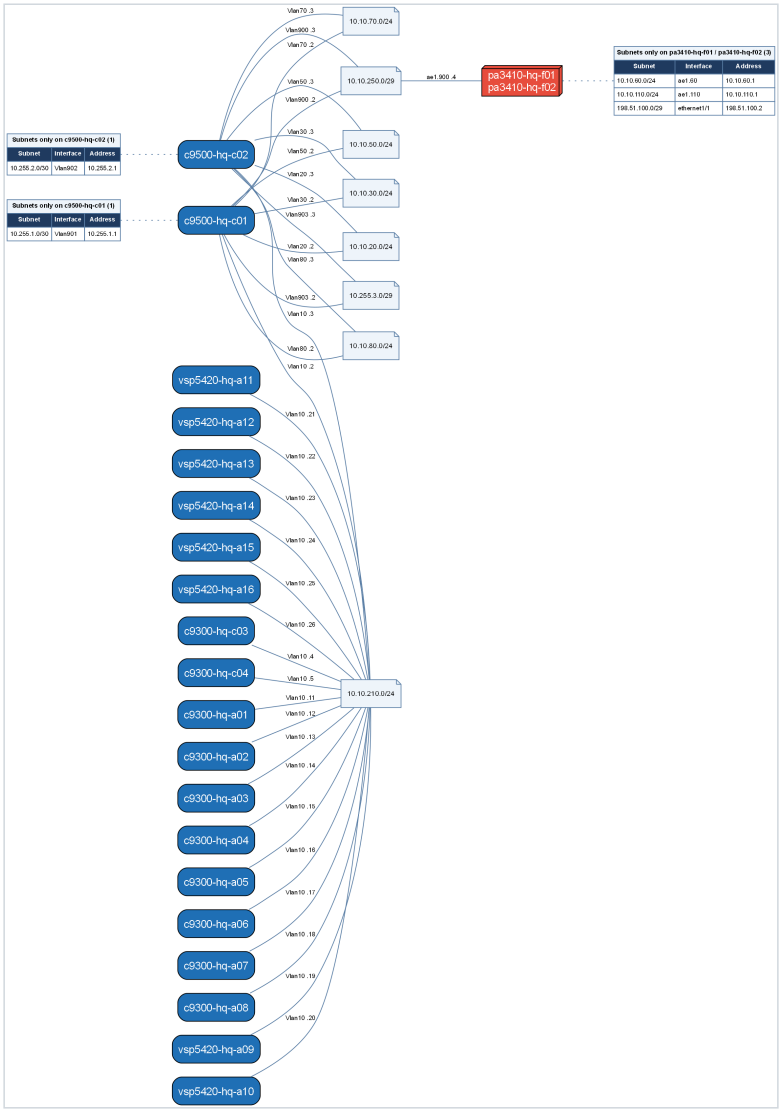


Figure 12 – Routed interfaces and subnets, RTG-HQ

5.11 Layer 3 view: routing summary

Each routing device as the site map's Layer 3 view summarises it: its routes by source, its addressed (Layer 3) interfaces and its BGP peers.

Device	Routes	Protocols	Connected	Static	BGP	OSPF	L3 interfaces	BGP peers
c9500-hq-c01	-	OSPF	-	-	-	not counted	9	-
c9500-hq-c02	-	OSPF	-	-	-	not counted	9	-
c9300-hq-c03	-	-	-	-	-	-	1	-
c9300-hq-c04	-	-	-	-	-	-	1	-
c9300-hq-a01	-	-	-	-	-	-	1	-
c9300-hq-a02	-	-	-	-	-	-	1	-
c9300-hq-a03	-	-	-	-	-	-	1	-
c9300-hq-a04	-	-	-	-	-	-	1	-
c9300-hq-a05	-	-	-	-	-	-	1	-
c9300-hq-a06	-	-	-	-	-	-	1	-
c9300-hq-a07	-	-	-	-	-	-	1	-
c9300-hq-a08	-	-	-	-	-	-	1	-
vsp5420-hq-a09	-	-	-	-	-	-	1	-
vsp5420-hq-a10	-	-	-	-	-	-	1	-
vsp5420-hq-a11	-	-	-	-	-	-	1	-
vsp5420-hq-a12	-	-	-	-	-	-	1	-
vsp5420-hq-a13	-	-	-	-	-	-	1	-
vsp5420-hq-a14	-	-	-	-	-	-	1	-
vsp5420-hq-a15	-	-	-	-	-	-	1	-
vsp5420-hq-a16	-	-	-	-	-	-	1	-
pa3410-hq-f01	-	static	-	-	-	-	4	-
pa3410-hq-f02	-	static	-	-	-	-	4	-

5.12 Layer 3 view: site prefixes

Every prefix with an address on a switch or firewall, its VLAN, and each device, interface and address on it. The maps that follow show, prefix by prefix, which devices and links carry it.

Prefix	VLAN	Devices, interfaces and addresses
10.10.20.0/24	20	c9500-hq-c01 Vlan20 10.10.20.2; c9500-hq-c02 Vlan20 10.10.20.3
10.10.30.0/24	30	c9500-hq-c01 Vlan30 10.10.30.2; c9500-hq-c02 Vlan30 10.10.30.3
10.10.50.0/24	50	c9500-hq-c01 Vlan50 10.10.50.2; c9500-hq-c02 Vlan50 10.10.50.3
10.10.60.0/24	60	pa3410-hq-f01 ae1.60 10.10.60.1; pa3410-hq-f02 ae1.60 10.10.60.1
10.10.70.0/24	70	c9500-hq-c01 Vlan70 10.10.70.2; c9500-hq-c02 Vlan70 10.10.70.3
10.10.80.0/24	80	c9500-hq-c01 Vlan80 10.10.80.2; c9500-hq-c02 Vlan80 10.10.80.3

Prefix	VLAN	Devices, interfaces and addresses
10.10.110.0/24	110	pa3410-hq-f01 ae1.110 10.10.110.1; pa3410-hq-f02 ae1.110 10.10.110.1
10.10.210.0/24	10	c9500-hq-c01 Vlan10 10.10.210.2; c9500-hq-c02 Vlan10 10.10.210.3; c9300-hq-c03 Vlan10 10.10.210.4; c9300-hq-c04 Vlan10 10.10.210.5; c9300-hq-a01 Vlan10 10.10.210.11; c9300-hq-a02 Vlan10 10.10.210.12; c9300-hq-a03 Vlan10 10.10.210.13; c9300-hq-a04 Vlan10 10.10.210.14; c9300-hq-a05 Vlan10 10.10.210.15; c9300-hq-a06 Vlan10 10.10.210.16; c9300-hq-a07 Vlan10 10.10.210.17; c9300-hq-a08 Vlan10 10.10.210.18; vsp5420-hq-a09 Vlan10 10.10.210.19; vsp5420-hq-a10 Vlan10 10.10.210.20; vsp5420-hq-a11 Vlan10 10.10.210.21; vsp5420-hq-a12 Vlan10 10.10.210.22; vsp5420-hq-a13 Vlan10 10.10.210.23; vsp5420-hq-a14 Vlan10 10.10.210.24; vsp5420-hq-a15 Vlan10 10.10.210.25; vsp5420-hq-a16 Vlan10 10.10.210.26
10.10.250.0/29	900	c9500-hq-c01 Vlan900 10.10.250.2; c9500-hq-c02 Vlan900 10.10.250.3; pa3410-hq-f01 ae1.900 10.10.250.4; pa3410-hq-f02 ae1.900 10.10.250.4
10.255.1.0/30	901	c9500-hq-c01 Vlan901 10.255.1.1
10.255.2.0/30	902	c9500-hq-c02 Vlan902 10.255.2.1
10.255.3.0/29	903	c9500-hq-c01 Vlan903 10.255.3.2; c9500-hq-c02 Vlan903 10.255.3.3
198.51.100.0/29	-	pa3410-hq-f01 ethernet1/1 198.51.100.2; pa3410-hq-f02 ethernet1/1 198.51.100.2

5.13 Routing topology

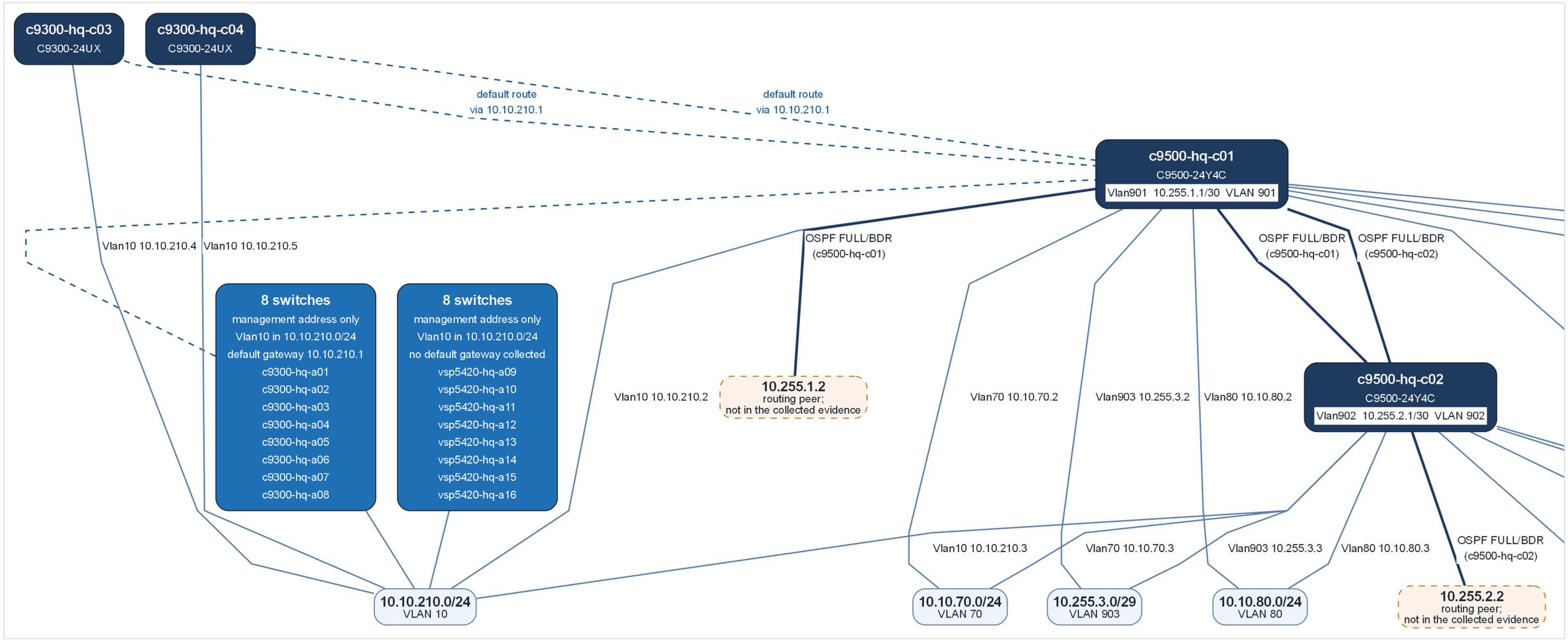


Figure 13 – L3 Routing Topology, RTG-HQ (evidence snapshot 8e957703443f) (part 1 of 2, left to right)

Routing topology (part 2 of 2, left to right)

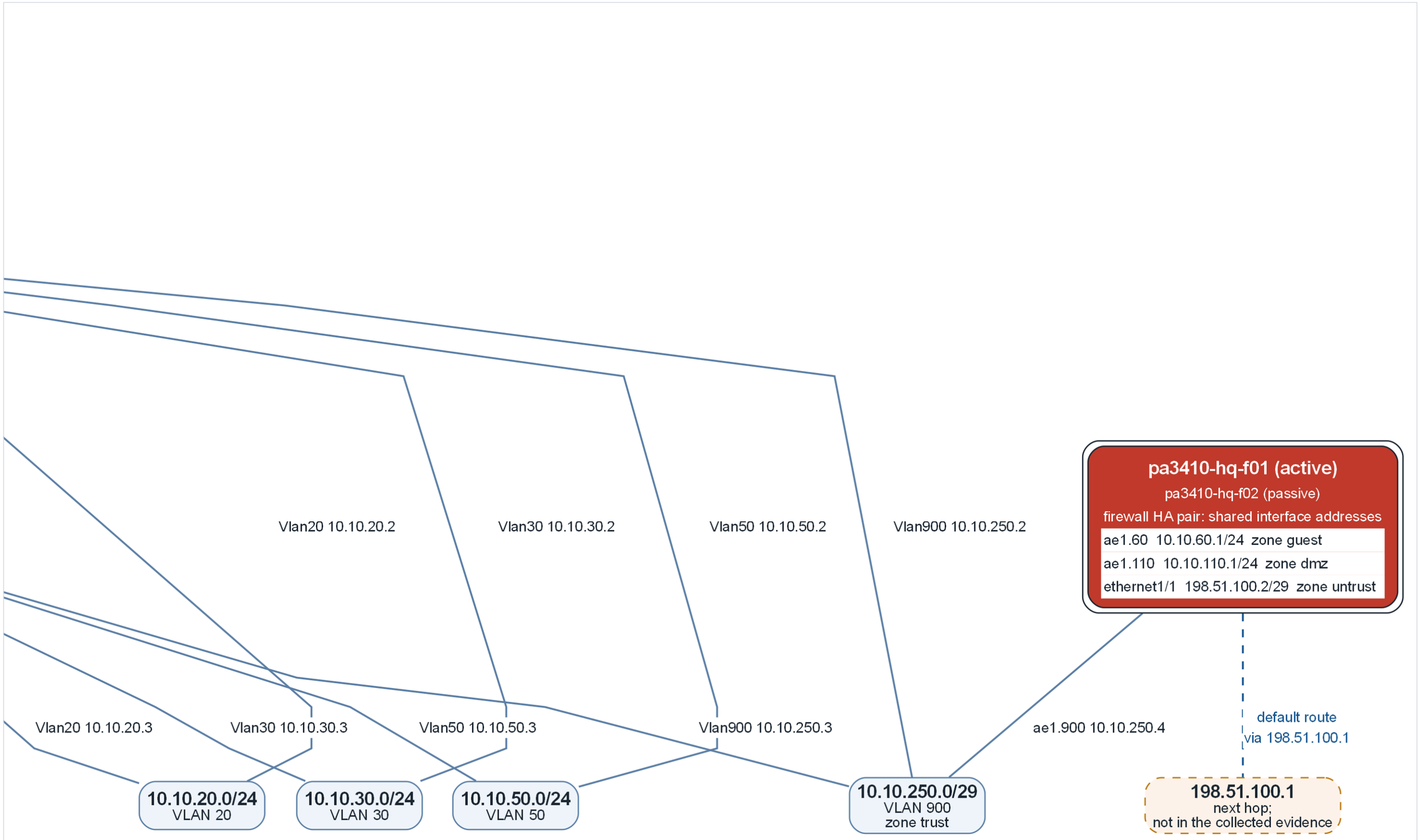


Figure 14 – L3 Routing Topology, RTG-HQ (evidence snapshot 8e957703443f) (part 2 of 2, left to right)

Layer 3 interfaces and the subnets they are directly connected to, default gateways and static routes drawn to the device that owns the next hop, and routing adjacencies only as the devices reported them (state shown). A next hop or peer that no collected device owns is shown as

unknown; no provider or destination is named that the evidence does not name. Switches with only a management address are grouped (named in the box). Scalable copy with its own legend: l3_routing_topology.svg in the report's diagrams folder.

On the figure	Means
Thin blue line	directly connected: the device has an address in that shared subnet
Dashed blue line	default or static route via a next hop, drawn to the device that owns it
Bold dark line	routing adjacency the device reported as up
Dotted dark line	routing peer reported but not established
White rows in a box	subnets only that device has an address in
Dashed box	an address no collected device owns (unknown; not named)
Grouped box	firewall HA pair with shared addresses, or switches with only a management address

Limitations of the evidence for this figure

- Some next hops belong to no collected device: shown as unknown next hops.

6 Management and security

6.1 Management services

Time, name resolution and logging on each switch, from the switch audit. Highlighted switches have a clock that is not synchronised.

Switch	NTP	DNS	Syslog	Clock
c9500-hq-c01	10.21.100.11, 10.21.100.12	10.21.100.53, 10.21.100.54	10.21.100.21, 10.21.100.22	synchronised
c9500-hq-c02	10.21.100.11, 10.21.100.12	10.21.100.53, 10.21.100.54	10.21.100.21, 10.21.100.22	synchronised
c9300-hq-c03	10.21.100.11, 10.21.100.12	10.21.100.53, 10.21.100.54	10.21.100.21, 10.21.100.22	synchronised
c9300-hq-c04	10.21.100.11, 10.21.100.12	10.21.100.53, 10.21.100.54	10.21.100.21, 10.21.100.22	synchronised
c9300-hq-a01	10.21.100.11, 10.21.100.12	10.21.100.53, 10.21.100.54	10.21.100.21, 10.21.100.22	synchronised
c9300-hq-a02	10.21.100.11, 10.21.100.12	10.21.100.53, 10.21.100.54	10.21.100.21, 10.21.100.22	synchronised
c9300-hq-a03	10.21.100.11, 10.21.100.12	10.21.100.53, 10.21.100.54	10.21.100.21, 10.21.100.22	synchronised
c9300-hq-a04	10.21.100.11, 10.21.100.12	10.21.100.53, 10.21.100.54	10.21.100.21, 10.21.100.22	synchronised
c9300-hq-a05	10.21.100.11, 10.21.100.12	10.21.100.53, 10.21.100.54	10.21.100.21, 10.21.100.22	synchronised
c9300-hq-a06	10.21.100.11, 10.21.100.12	10.21.100.53, 10.21.100.54	10.21.100.21, 10.21.100.22	synchronised
c9300-hq-a07	10.21.100.11, 10.21.100.12	10.21.100.53, 10.21.100.54	10.21.100.20	synchronised
c9300-hq-a08	10.21.100.11, 10.21.100.12	10.21.100.53, 10.21.100.54	10.21.100.20	synchronised
vsp5420-hq-a09	10.21.100.12	10.21.100.53, 10.21.100.54	10.21.100.22	synchronised
vsp5420-hq-a10	10.21.100.12	10.21.100.53, 10.21.100.54	10.21.100.22	synchronised
vsp5420-hq-a11	10.21.100.12	10.21.100.53, 10.21.100.54	10.21.100.22	synchronised
vsp5420-hq-a12	10.21.100.12	10.21.100.53, 10.21.100.54	10.21.100.22	synchronised
vsp5420-hq-a13	10.21.100.12	10.21.100.53, 10.21.100.54	10.21.100.22	synchronised
vsp5420-hq-a14	10.21.100.12	10.21.100.53, 10.21.100.54	10.21.100.22	synchronised
vsp5420-hq-a15	10.21.100.12	10.21.100.53, 10.21.100.54	10.21.100.22	synchronised
vsp5420-hq-a16	10.21.100.12	10.21.100.53, 10.21.100.54	10.21.100.22	synchronised

6.2 Configuration backups

The newest configuration backup of each device in the site's backups folder. A backup is complete when it runs through to the device's prompt after the configuration; an incomplete one cannot be used to restore the device. Red rows are incomplete; amber rows are more than 90 days old.

Device	Last backup	Age (days)	Complete	File
c9500-hq-c01	20 Oct 2026 02:00	16	yes	cisco\20261020_020000\c9500-hq-c01_backup_20261020_020000.txt
c9500-hq-c02	20 Oct 2026 02:00	16	yes	cisco\20261020_020000\c9500-hq-c02_backup_20261020_020000.txt
c9300-hq-c03	20 Oct 2026 02:00	16	yes	cisco\20261020_020000\c9300-hq-c03_backup_20261020_020000.txt
c9300-hq-c04	20 Oct 2026 02:00	16	yes	cisco\20261020_020000\c9300-hq-c04_backup_20261020_020000.txt
c9300-hq-a01	20 Oct 2026 02:00	16	yes	cisco\20261020_020000\c9300-hq-a01_backup_20261020_020000.txt
c9300-hq-a02	20 Oct 2026 02:00	16	yes	cisco\20261020_020000\c9300-hq-a02_backup_20261020_020000.txt
c9300-hq-a03	20 Oct 2026 02:00	16	yes	cisco\20261020_020000\c9300-hq-a03_backup_20261020_020000.txt
c9300-hq-a04	20 Oct 2026 02:00	16	yes	cisco\20261020_020000\c9300-hq-a04_backup_20261020_020000.txt
c9300-hq-a05	20 Oct 2026 02:00	16	yes	cisco\20261020_020000\c9300-hq-a05_backup_20261020_020000.txt
c9300-hq-a06	20 Oct 2026 02:00	16	yes	cisco\20261020_020000\c9300-hq-a06_backup_20261020_020000.txt
c9300-hq-a07	20 Oct 2026 02:00	16	yes	cisco\20261020_020000\c9300-hq-a07_backup_20261020_020000.txt
c9300-hq-a08	20 Oct 2026 02:00	16	yes	cisco\20261020_020000\c9300-hq-a08_backup_20261020_020000.txt
vsp5420-hq-a09	20 Oct 2026 02:00	16	yes	extreme\20261020_020000\vsp5420-hq-a09_extreme_backup_20261020_020000.txt
vsp5420-hq-a10	20 Oct 2026 02:00	16	yes	extreme\20261020_020000\vsp5420-hq-a10_extreme_backup_20261020_020000.txt
vsp5420-hq-a11	20 Oct 2026 02:00	16	yes	extreme\20261020_020000\vsp5420-hq-a11_extreme_backup_20261020_020000.txt
vsp5420-hq-a12	20 Oct 2026 02:00	16	yes	extreme\20261020_020000\vsp5420-hq-a12_extreme_backup_20261020_020000.txt
vsp5420-hq-a13	20 Oct 2026 02:00	16	yes	extreme\20261020_020000\vsp5420-hq-a13_extreme_backup_20261020_020000.txt
vsp5420-hq-a14	20 Oct 2026 02:00	16	yes	extreme\20261020_020000\vsp5420-hq-a14_extreme_backup_20261020_020000.txt
vsp5420-hq-a15	20 Oct 2026 02:00	16	yes	extreme\20261020_020000\vsp5420-hq-a15_extreme_backup_20261020_020000.txt

Device	Last backup	Age (days)	Complete	File
vsp5420-hq-a16	20 Oct 2026 02:00	16	yes	extreme\20261020_020000\vsp5420-hq-a16_extreme_backup_20261020_020000.txt
pa3410-hq-f01	20 Oct 2026 02:00	16	yes	palo\20261020_020000\pa3410-hq-f01_paloalto_backup_20261020_020000.txt
pa3410-hq-f02	20 Oct 2026 02:00	16	yes	palo\20261020_020000\pa3410-hq-f02_paloalto_backup_20261020_020000.txt

6.3 Management access

How each device can be managed, read from its latest configuration backup. Highlighted rows allow telnet or use a default SNMP community. Telnet is what the VTY lines permit, not evidence that Telnet sessions take place. SSH v2: Yes when the configuration sets version 2, or when this collection logged in over SSH (the collector uses SSH version 2 only); Not verified when the configuration does not set the version and no SSH login was made.

Device	Backup date	Telnet	HTTP management	SSH v2	SNMP	AAA	Login banner
c9500-hq-c01	20 Oct 2026	No	No	Yes	v3 only	TACACS/RADIUS	Yes
c9500-hq-c02	20 Oct 2026	No	No	Yes	v3 only	TACACS/RADIUS	Yes
c9300-hq-c03	20 Oct 2026	No	No	Yes	v3 only	TACACS/RADIUS	Yes
c9300-hq-c04	20 Oct 2026	No	No	Yes	v3 only	TACACS/RADIUS	Yes
c9300-hq-a01	20 Oct 2026	No	No	Yes	v3 only	TACACS/RADIUS	Yes
c9300-hq-a02	20 Oct 2026	No	No	Yes	v3 only	TACACS/RADIUS	Yes
c9300-hq-a03	20 Oct 2026	No	No	Yes	v3 only	TACACS/RADIUS	Yes
c9300-hq-a04	20 Oct 2026	No	No	Yes	v3 only	TACACS/RADIUS	Yes
c9300-hq-a05	20 Oct 2026	No	No	Yes	v3 only	TACACS/RADIUS	Yes
c9300-hq-a06	20 Oct 2026	No	No	Yes	v3 only	TACACS/RADIUS	Yes
c9300-hq-a07	20 Oct 2026	No	No	Yes	v3 only	TACACS/RADIUS	Yes
c9300-hq-a08	20 Oct 2026	No	No	Yes	v3 only	TACACS/RADIUS	Yes
vsp5420-hq-a09	20 Oct 2026	No	No	Yes	No	TACACS/RADIUS	No
vsp5420-hq-a10	20 Oct 2026	No	No	Yes	No	TACACS/RADIUS	No
vsp5420-hq-a11	20 Oct 2026	No	No	Yes	No	TACACS/RADIUS	No
vsp5420-hq-a12	20 Oct 2026	No	No	Yes	No	TACACS/RADIUS	No
vsp5420-hq-a13	20 Oct 2026	No	No	Yes	No	TACACS/RADIUS	No
vsp5420-hq-a14	20 Oct 2026	No	No	Yes	No	TACACS/RADIUS	No
vsp5420-hq-a15	20 Oct 2026	No	No	Yes	No	TACACS/RADIUS	No
vsp5420-hq-a16	20 Oct 2026	No	No	Yes	No	TACACS/RADIUS	No
pa3410-hq-f01	20 Oct 2026	No	No	Yes	No	TACACS/RADIUS	Yes
pa3410-hq-f02	20 Oct 2026	No	No	Yes	No	TACACS/RADIUS	Yes

6.4 Authentication servers

TACACS+, RADIUS and Kerberos servers each device uses, and what for (device logins, 802.1X, accounting), from the newest configuration backups; keys are not shown. Highlighted rows use a server group with no server configured, so every login falls back to local accounts. pa3410-hq-f01, pa3410-hq-f02 are not managed by Panorama; their own configuration backups configure authentication servers or SNMP on pa3410-hq-f01, pa3410-hq-f02 (see the Management access table).

Device	Protocol	Servers	Used for	Local fallback
c9300-hq-a01, c9300-hq-a02, c9300-hq-a03, c9300-hq-a04, c9300-hq-a05, c9300-hq-a06, c9300-hq-a07, c9300-hq-a08, c9300-hq-c03, c9300-hq-c04, c9500-hq-c01, c9500-hq-c02	TACACS+	10.21.100.41, 10.21.100.42	exec authorisation, login	yes
vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11, vsp5420-hq-a12, vsp5420-hq-a13, vsp5420-hq-a14, vsp5420-hq-a15, vsp5420-hq-a16	RADIUS	10.21.100.41	CLI login	yes

6.5 SNMP management and traps

How each device can be polled over SNMP (v2c communities by access, never their strings; v3 by security level) and where it sends traps, from the newest configuration backups. Highlighted rows allow v2c write access, have a v2c community no access list limits, or send no traps. pa3410-hq-f01, pa3410-hq-f02 are not managed by Panorama; their own configuration backups configure authentication servers or SNMP on pa3410-hq-f01, pa3410-hq-f02 (see the Management access table).

Device	SNMP access	Trap destinations	Trap source
c9300-hq-c03, c9300-hq-c04	v3 authPriv	10.21.100.31 (v3 priv), 10.21.100.32 (v2c)	Vlan10
c9300-hq-a01, c9300-hq-a02, c9300-hq-a03, c9300-hq-a04, c9300-hq-a05, c9300-hq-a06, c9300-hq-a07, c9300-hq-a08, c9500-hq-c01, c9500-hq-c02	v3 authPriv	10.21.100.31 (v3 priv)	Vlan10
vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11, vsp5420-hq-a12, vsp5420-hq-a13, vsp5420-hq-a14, vsp5420-hq-a15, vsp5420-hq-a16	v3 authPriv	10.21.100.31 (v3 authPriv)	-

6.6 Service map: NTP servers

Diagrams of the servers the site's devices depend on, read from the switch audit, the configuration backups and the firewalls. Devices that use exactly the same servers are drawn as one box; each service has its own colour. The time servers each device synchronises to.

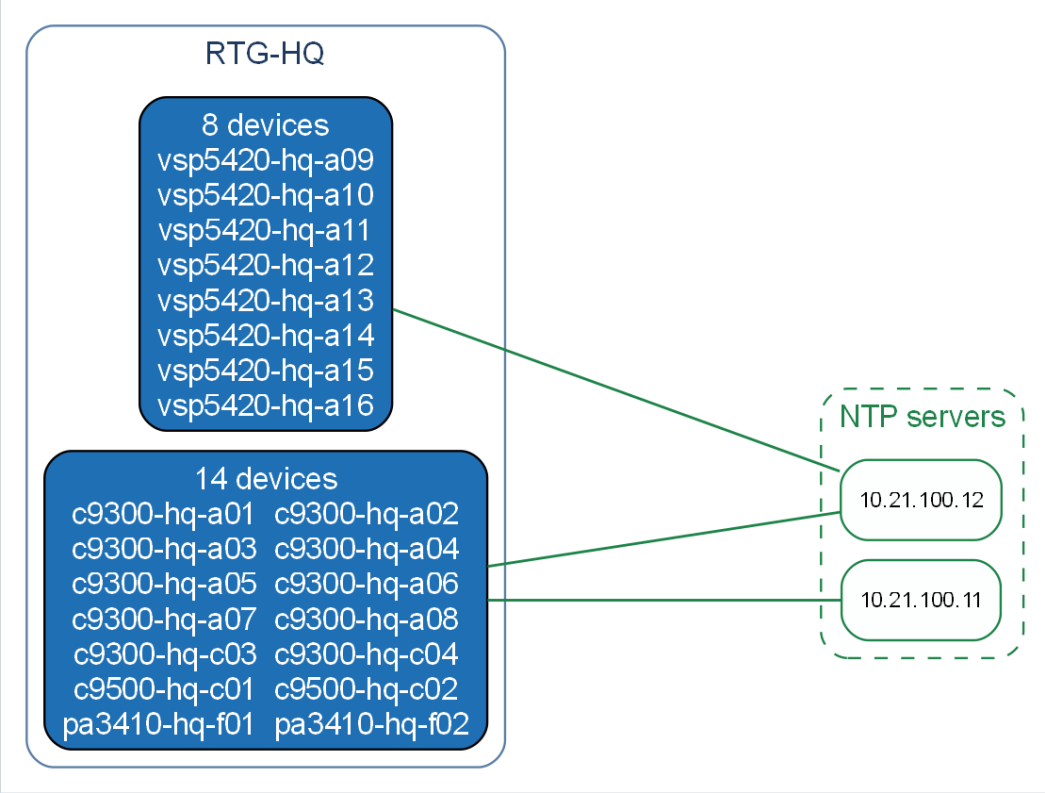


Figure 15 – Service map: NTP servers, RTG-HQ

6.7 Service map: DNS servers

The name servers each device resolves against.

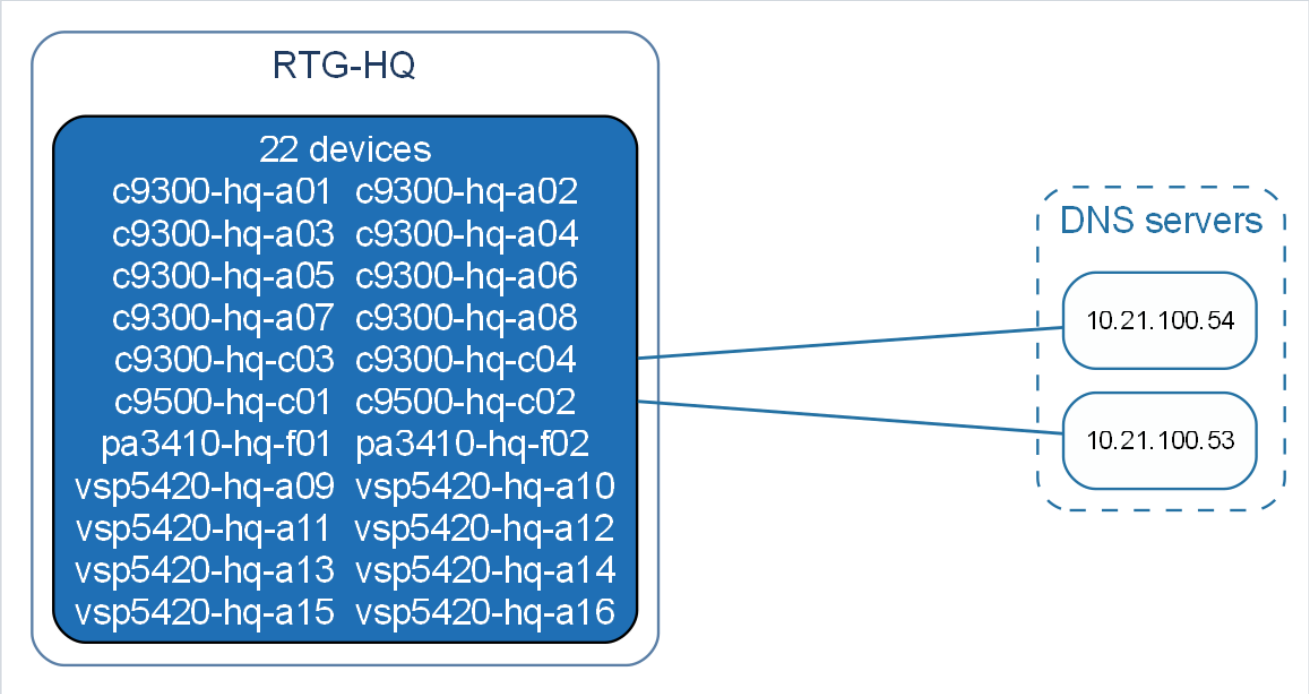


Figure 16 – Service map: DNS servers, RTG-HQ

6.8 Service map: Syslog and log forwarding

Where each device sends its logs: switches by syslog, firewalls by log forwarding.

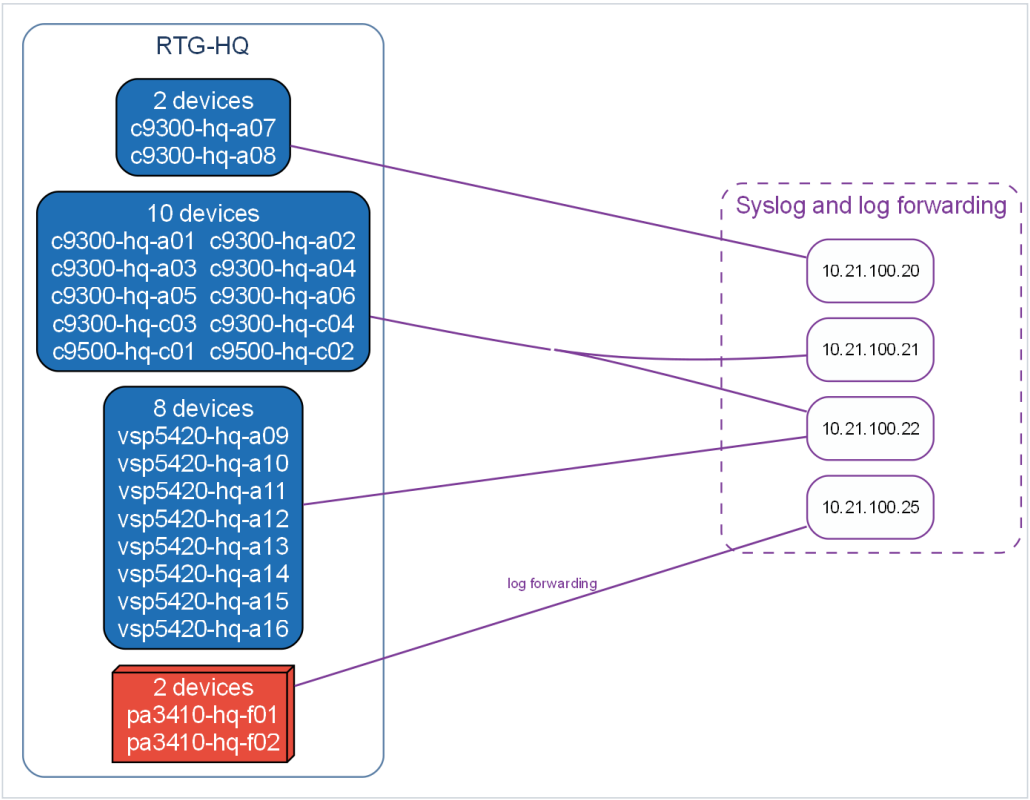


Figure 17 – Service map: Syslog and log forwarding, RTG-HQ

6.9 Service map: SNMP trap receivers

Where each device sends SNMP traps; lines show the SNMP version and security level.

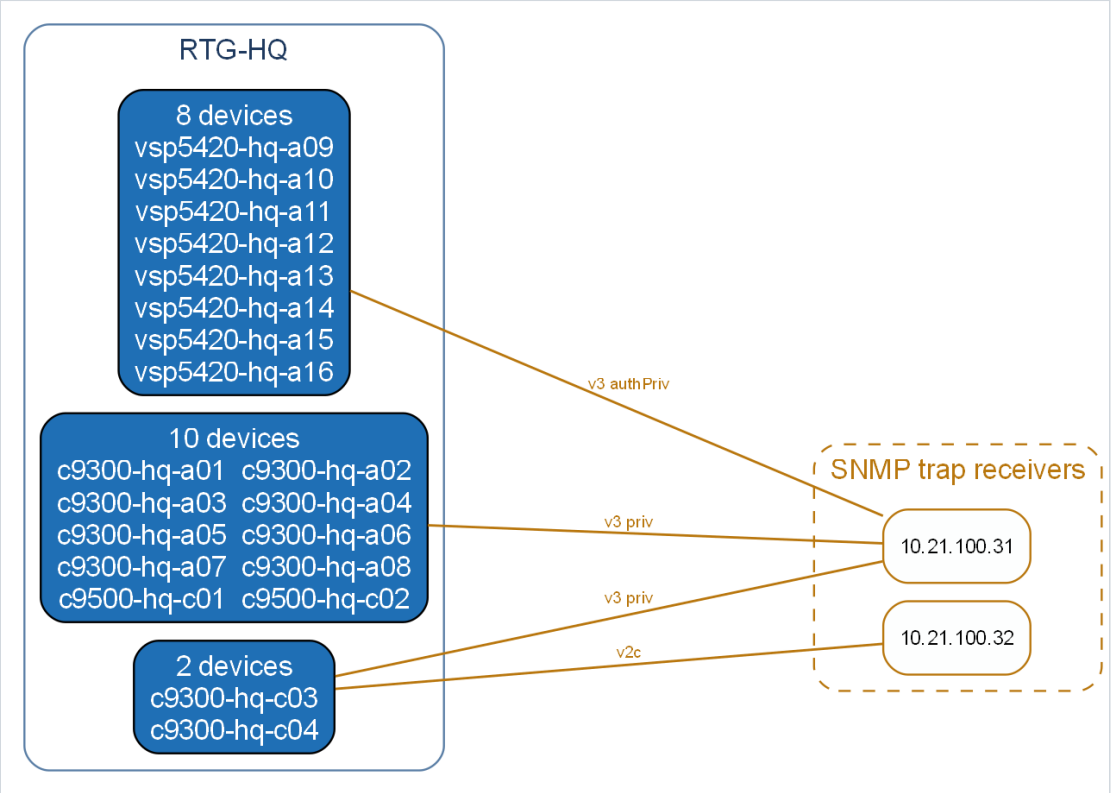


Figure 18 – Service map: SNMP trap receivers, RTG-HQ

6.10 Service map: access and addressing

The TACACS+, RADIUS and Kerberos servers each device uses; lines show what for. The DHCP servers the routed interfaces relay to; lines show the VLANs relayed.

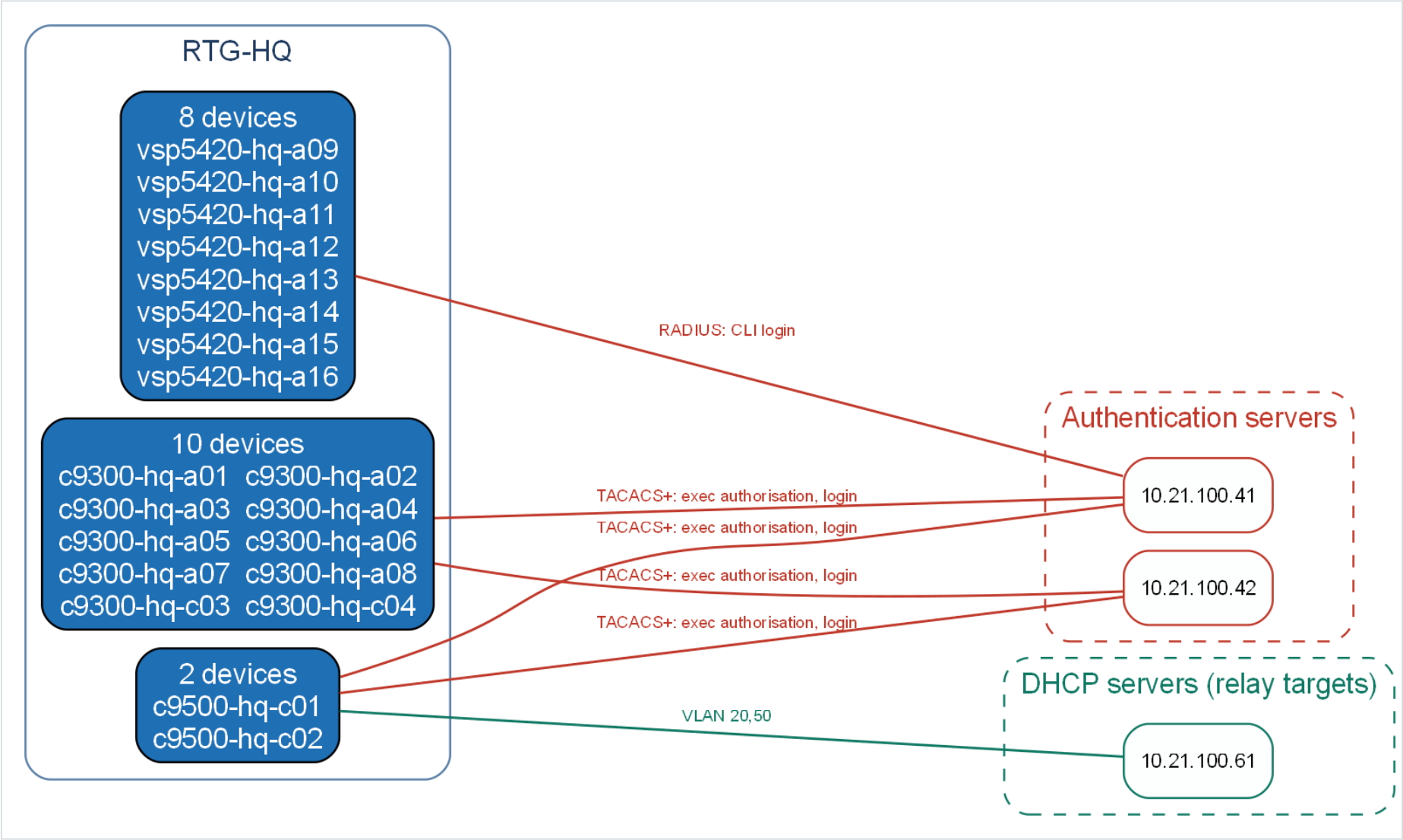


Figure 19 – Service map: access and addressing, RTG-HQ

6.11 Interface access lists

No access list is applied to any switch interface or management line in the configuration backups; traffic between subnets is filtered only by the firewalls.

6.12 Quality of service

How each switch classifies and queues traffic: whether QoS is enabled (Catalyst "mls qos", or MQC policy-maps on IOS-XE), AutoQoS, the number of global queue, threshold and CoS/DSCP map settings, ports with a voice VLAN, and control-plane policing. Highlighted switches carry voice VLAN ports with QoS off, so voice is queued like any other traffic. With QoS off, no voice VLAN ports and no control-plane policing (left out of the table): c9500-hq-c01, c9500-hq-c02, c9300-hq-c03, c9300-hq-c04, vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11, vsp5420-hq-a12, vsp5420-hq-a13, vsp5420-hq-a14, vsp5420-hq-a15, vsp5420-hq-a16.

Device	QoS	AutoQoS	Queue and map settings	Voice ports	Control-plane policing
c9300-hq-a01	off	no	0	26	no
c9300-hq-a02	off	no	0	26	no
c9300-hq-a03	off	no	0	15	no
c9300-hq-a04	off	no	0	15	no
c9300-hq-a05	off	no	0	15	no
c9300-hq-a06	off	no	0	15	no
c9300-hq-a07	off	no	0	15	no
c9300-hq-a08	off	no	0	15	no

6.13 Edge port protection

Protection on access ports: BPDU guard, storm control and 802.1X or port security (ports protected / access ports), read from the latest configuration backup ("-" where that backup is incomplete), and unused ports left enabled: ports enabled with nothing connected at collection time, from the port status audit (empty optic slots not counted).

Device	BPDU guard	Storm control	802.1X / port security	Unused ports left up
c9500-hq-c01	Global	-	-	-
c9500-hq-c02	Global	-	-	-
c9300-hq-c03	Global	0/3 access ports	0/3 access ports	13
c9300-hq-c04	Global	0/2 access ports	0/2 access ports	14
c9300-hq-a01	Global	0/32 access ports	0/32 access ports	64
c9300-hq-a02	Global	0/32 access ports	0/32 access ports	64
c9300-hq-a03	Global	0/20 access ports	0/20 access ports	28
c9300-hq-a04	Global	0/21 access ports	0/21 access ports	27
c9300-hq-a05	Global	0/20 access ports	0/20 access ports	28
c9300-hq-a06	Global	0/20 access ports	0/20 access ports	28
c9300-hq-a07	Global	0/21 access ports	0/21 access ports	27
c9300-hq-a08	Global	0/21 access ports	0/21 access ports	27
vsp5420-hq-a09	No	No	No	34

Device	BPDU guard	Storm control	802.1X / port security	Unused ports left up
vsp5420-hq-a10	No	No	No	35
vsp5420-hq-a11	No	No	No	34
vsp5420-hq-a12	No	No	No	34
vsp5420-hq-a13	No	No	No	35
vsp5420-hq-a14	No	No	No	35
vsp5420-hq-a15	No	No	No	34
vsp5420-hq-a16	No	No	No	34

6.14 Firewall policy and services

Rule counts from the running policy, VPN tunnels and log forwarding on each firewall. "-" means the firewall did not return the list, for example because a commit was in progress.

Firewall	Security rules	NAT rules	VPN tunnels	Log forwarding
pa3410-hq-f01	3	2	none	connected (10.21.100.25)
pa3410-hq-f02	3	2	none	connected (10.21.100.25)

6.15 Firewall licences

Licences and subscriptions. Highlighted rows have expired.

Firewall	Licence	Expires	Expired
pa3410-hq-f01	Threat Prevention	01 Oct 2027	no
pa3410-hq-f01	Advanced URL Filtering	01 Oct 2027	no
pa3410-hq-f02	Threat Prevention	01 Oct 2027	no
pa3410-hq-f02	Advanced URL Filtering	01 Oct 2027	no

6.16 High availability

Each unit's HA state, election settings and versions. Peers must run the same software and content to fail over cleanly.

Firewall	State	Priority	Preemptive	Software	App/threat content	Peer versions match
pa3410-hq-f01	active	100	no	11.1.4-h7	8925-9201	yes
pa3410-hq-f02	passive	110	no	11.1.4-h7	8925-9201	yes

6.17 Baseline compliance

No approved configuration baseline was supplied (ASBUILT_BASELINE), so differences between devices are reported as inconsistencies requiring review, not as deviations.

7 Collection coverage and scope

7.1 Devices collected

Every device NetBox lists at the site (the list saved with the evidence), and whether this document was able to collect from it. Highlighted devices are not described anywhere in the document.

Device	Manufacturer	Type	Status	Note
c9500-hq-c01	Cisco		Collected	
c9500-hq-c02	Cisco		Collected	
c9300-hq-c03	Cisco		Collected	
c9300-hq-c04	Cisco		Collected	
c9300-hq-a01	Cisco		Collected	
c9300-hq-a02	Cisco		Collected	
c9300-hq-a03	Cisco		Collected	
c9300-hq-a04	Cisco		Collected	
c9300-hq-a05	Cisco		Collected	
c9300-hq-a06	Cisco		Collected	
c9300-hq-a07	Cisco		Collected	
c9300-hq-a08	Cisco		Collected	
vsp5420-hq-a09	Extreme Networks		Collected	
vsp5420-hq-a10	Extreme Networks		Collected	
vsp5420-hq-a11	Extreme Networks		Collected	
vsp5420-hq-a12	Extreme Networks		Collected	
vsp5420-hq-a13	Extreme Networks		Collected	
vsp5420-hq-a14	Extreme Networks		Collected	
vsp5420-hq-a15	Extreme Networks		Collected	
vsp5420-hq-a16	Extreme Networks		Collected	
pa3410-hq-f01	Palo Alto Networks	PA-3410	Collected	
pa3410-hq-f02	Palo Alto Networks	PA-3410	Collected	

7.2 Assumptions and exclusions

Item
Regenerated from previously saved evidence: no network devices or external systems were contacted for this document. It describes the network as it was when the evidence was collected (dates in the document control and the evidence register).
Devices are those recorded in NetBox for the site with status Active; anything not in NetBox is only described where a neighbouring device reported it (CDP/LLDP).
Security settings are read from the newest configuration backup of each device, which may be older than the collection (dates under Configuration backups in section 6).
Not covered: structured cabling and patching, wireless controller and SSID configuration, servers and applications, firewall rule content (counts only), and devices that could not be logged in to.
Endpoint counts include only devices that announce themselves over CDP or LLDP.

7.3 Methodology and limitations

Area	How it was assessed / what it cannot show
Collection	Evidence acquisition: read-only show commands and API reads over the sessions the original collection opened; no configuration was changed. Report generation: regenerated from that saved evidence, with no device or external system contacted. Each value's source and date are in the evidence register (appendix).
Findings	Raised by rules from the collected data, each with a stable ID, confidence and basis. A finding is resolved only when a later collection re-assessed it; incomplete collection is never read as absence.
Baselines	No approved baseline: differences between devices are inconsistencies, not deviations.
Interface health	Counters from 20 devices; rates only between two samples, utilisation only from rates.
Spanning tree	Observed root placement and evidence only; whether it is correct depends on the intended design, which the collected data does not show.
Vulnerabilities	Not performed: no local advisory data supplied; nothing was looked up online.
Dependencies	From CDP/LLDP adjacency; physical redundancy is not proven resilience (no failover tested).
Not assessed	Utilisation trends over time, optical levels, wireless controllers, firewall rule content, cabling and patching, and devices that could not be logged in to.

8 Dependencies and readiness

8.1 Switch dependencies

How each switch reaches the core, from the CDP/LLDP neighbour tables. A port-channel and its member links count as one bundle. "Single points of failure" are devices, stack members or links whose loss alone cuts the switch off from the core. Two physical paths are physical redundancy only: failover was not tested, so it is not proven resilience.

Device	Upstream	Links	Bundling	Classification	Single points of failure	Endpoints
c9300-hq-a01	c9300-hq-c03 Te1/0/1; c9300-hq-c04 Te1/0/1	2	none	Dual-homed (two upstream devices)	none	32
c9300-hq-a02	c9300-hq-c03 Te1/0/2; c9300-hq-c04 Te1/0/2	2	none	Dual-homed (two upstream devices)	none	32
c9300-hq-a03	c9300-hq-c03 Te1/0/3; c9300-hq-c04 Te1/0/3	2	none	Dual-homed (two upstream devices)	none	20
c9300-hq-a04	c9300-hq-c03 Te1/0/4; c9300-hq-c04 Te1/0/4	2	none	Dual-homed (two upstream devices)	none	21
c9300-hq-a05	c9300-hq-c03 Te1/0/5; c9300-hq-c04 Te1/0/5	2	none	Dual-homed (two upstream devices)	none	20
c9300-hq-a06	c9300-hq-c03 Te1/0/6; c9300-hq-c04 Te1/0/6	2	none	Dual-homed (two upstream devices)	none	20
c9300-hq-a07	c9300-hq-c03 Te1/0/7; c9300-hq-c04 Te1/0/7	2	none	Dual-homed (two upstream devices)	none	21
c9300-hq-a08	c9300-hq-c03 Te1/0/8; c9300-hq-c04 Te1/0/8	2	none	Dual-homed (two upstream devices)	none	21
vsp5420-hq-a09	c9500-hq-c01 Twe1/0/3; c9500-hq-c02 Twe1/0/3	2	none	Dual-homed (two upstream devices)	none	4
vsp5420-hq-a10	c9500-hq-c01 Twe1/0/4; c9500-hq-c02 Twe1/0/4	2	none	Dual-homed (two upstream devices)	none	3
vsp5420-hq-a11	c9500-hq-c01 Twe1/0/5; c9500-hq-c02 Twe1/0/5	2	none	Dual-homed (two upstream devices)	none	4
vsp5420-hq-a12	c9500-hq-c01 Twe1/0/6; c9500-hq-c02 Twe1/0/6	2	none	Dual-homed (two upstream devices)	none	4
vsp5420-hq-a13	c9500-hq-c01 Twe1/0/7; c9500-hq-c02 Twe1/0/7	2	none	Dual-homed (two upstream devices)	none	3

Device	Upstream	Links	Bundling	Classification	Single points of failure	Endpoints
vsp5420-hq-a14	c9500-hq-c01 Twe1/0/8; c9500-hq-c02 Twe1/0/8	2	none	Dual-homed (two upstream devices)	none	3
vsp5420-hq-a15	c9500-hq-c01 Twe1/0/9; c9500-hq-c02 Twe1/0/9	2	none	Dual-homed (two upstream devices)	none	4
vsp5420-hq-a16	c9500-hq-c01 Twe1/0/10; c9500-hq-c02 Twe1/0/10	2	none	Dual-homed (two upstream devices)	none	4

8.2 Aggregation points

Devices and core stack members that a group of switches depends on alone, with the endpoints discovered behind them (CDP/LLDP; endpoints that announce nothing are not counted).

Aggregation point	Devices depending on it alone	Endpoints behind them	Devices
c9500-hq-c01	2	0	c9300-nth-c01, vsp7520-dc1-c01
c9500-hq-c02	2	0	vsp5520-sth-c01, vsp7520-dc1-c02
c9300-hq-c03	1	0	c4451-hq-r01
c9300-hq-c04	1	0	c4451-hq-r02

8.3 Firewall high availability and WAN

HA state as the firewalls reported it, and the switch ports each firewall attaches to.

Firewall	HA	Peer	Config sync	HA links	Attaches to
pa3410-hq-f01	Active-Passive active	passive	synchronized	HA1, HA2	c9300-hq-c03 Te1/0/24, reported by both ends; c9500-hq-c01 Twe1/0/21, reported by both ends; c9500-hq-c01 Twe1/0/22, reported by both ends
pa3410-hq-f02	Active-Passive passive	active	synchronized	HA1, HA2	c9300-hq-c04 Te1/0/24, reported by both ends; c9500-hq-c02 Twe1/0/21, reported by both ends; c9500-hq-c02 Twe1/0/22, reported by both ends

Service	Circuit	Status
Business Internet 1000 Mbps (primary)	SYN-INT-HQ-0001	Active
Business Internet 1000 Mbps (secondary)	SYN-INT-HQ-0002	Active
Ethernet Private Line HQ - North (VLAN 901)	SYN-EPL-0901	Active
Ethernet Private Line HQ - South (VLAN 902)	SYN-EPL-0902	Active
Dark fibre HQ - DC1 (path A)	SYN-DF-0001	Active
Dark fibre HQ - DC1 (path B)	SYN-DF-0002	Active

More than one WAN service is physical redundancy only: path diversity and failover between them are not visible to the collection.

8.4 Readiness assessment

What a change or refresh project at the site can rely on. There is deliberately no score: each item states what it rests on.

Confirmed	Evidence
16 switches reach the core; 0 by a single uplink, 0 by a port-channel, 0 by parallel unbundled links, 16 dual-homed.	CDP/LLDP neighbour tables (Infrastructure links, section 3)
c9500-hq-c01 alone carries 2 devices (0 discovered endpoints).	uplink ports and stack member numbering
pa3410-hq-f01: HA Active-Passive active, peer passive, configuration synchronized; attaches to c9300-hq-c03 Te1/0/24, reported by both ends; c9500-hq-c01 Twe1/0/21, reported by both ends; c9500-hq-c01 Twe1/0/22, reported by both ends.	firewall HA state (show high-availability)
pa3410-hq-f02: HA Active-Passive passive, peer active, configuration synchronized; attaches to c9300-hq-c04 Te1/0/24, reported by both ends; c9500-hq-c02 Twe1/0/21, reported by both ends; c9500-hq-c02 Twe1/0/22, reported by both ends.	firewall HA state (show high-availability)
6 WAN services recorded: Business Internet 1000 Mbps (primary); Business Internet 1000 Mbps (secondary); Ethernet Private Line HQ - North (VLAN 901); Ethernet Private Line HQ - South (VLAN 902); Dark fibre HQ - DC1 (path A); Dark fibre HQ - DC1 (path B).	WAN provider service export

Unknown	Evidence
WAN path diversity: whether the WAN services share a building entry, duct or carrier path, and how traffic fails over between them, is not visible to the collection.	-
Devices seen only as neighbours (not collected): c4451-hq-r01, c4451-hq-r02, c9300-nth-c01, vsp5520-sth-c01, vsp7520-dc1-c01, vsp7520-dc1-c02. Their redundancy and role are not assessed.	CDP/LLDP
Failover behaviour: no failover test was performed; physical redundancy is not proven resilience.	-
Interface error counters were collected at one point in time (Interface operational health, section 3); sustained utilisation and per-link power redundancy are not collected.	-

Actions	Evidence
Plan a controlled failover test (uplink, core member, firewall HA) in a change window before relying on the physical redundancy shown.	-
F-HW-ACBCB3: Check and replace the failed unit; the device is still running but without its redundancy.	Potentially undesirable configuration
F-SUP-982735: Renew support for these serials or confirm they moved to another contract; parts and TAC cases depend on it.	Requires engineering investigation

8.5 Assessment scope and limits

What this assessment covered, and what the collected data cannot show.

Area	Assessed	Limits
Layer 1/2 dependency	uplinks, port-channels, stack members, single points of failure	from CDP/LLDP; a link neither end announces is not seen
Firewall HA	mode, state, config sync, HA links, attachment	failover not tested; path monitoring not assessed
WAN	WAN services and BGP peers when collected	carrier diversity and physical path are not visible to the collection
Routing	interfaces, static routes, adjacencies when collected	route convergence and failover are not assessed
Capacity	port counts and PoE budget (sections 2.5, 3.6)	link utilisation and errors are not collected

9 Findings register

9.1 Findings and recommendations

Raised automatically from the collected data. They are prompts for review: each should be confirmed against the intended design before any change is made. The summary lists every finding; the detail that follows gives each one in full, with the evidence records it rests on (linked to the evidence register appendix). IDs are stable between documents, and confidence is independent of severity. Confidence: Confirmed — the collected configuration or device output states it directly; High confidence — it rests on reference data or an interpretation of the data; Requires verification — it rests on an assumed platform default, on sources that disagree, or on no evidence record; Insufficient evidence — the data needed was not collected.

Summary of findings

Severity	ID	Affected	Finding	Confidence	Recommended action
HIGH	F-HW-ACBCB3	c9300-hq-a03	Power, fan or temperature faults: c9300-hq-a03 power supply PSU 1B (member 1, slot B: Bad).	Confirmed	Check and replace the failed unit; the device is still running but without its redundancy.
HIGH	F-SUP-982735	c9300-hq-a05	Support has ended (21 Aug 2026) for c9300-hq-a05 (1 serials), although the schedule still lists them as live devices.	High confidence	If verification confirms the condition is not intended: renew support for these serials or confirm they moved to another contract; parts and TAC cases depend on it.
MEDIUM	F-SEC-13E8DF	8 devices (vsp5420-hq-a09, vsp5420-hq-a10, …)	Access ports have no BPDU guard on vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11, vsp5420-hq-a12, vsp5420-hq-a13, vsp5420-hq-a14, vsp5420-hq-a15, vsp5420-hq-a16.	Confirmed	Enable BPDU guard on edge (access) ports, after confirming no switch is legitimately connected to them.
MEDIUM	F-SUP-F35F2E	c9300-hq-a06	Hardware whose serials are not on the support schedule (RTG_support_schedule_20261019.xlsx), which does list other equipment of the same manufacturer: c9300-hq-a06.	High confidence	Confirm whether the serials are under a support contract (the schedule may be incomplete), and add them to the schedule if they are.
LOW	F-MGT-79E9FF	8 devices (vsp5420-hq-a09, vsp5420-hq-a10, …)	NTP servers differ between switches: vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11, vsp5420-hq-a12, vsp5420-hq-a13, vsp5420-hq-a14, vsp5420-hq-a15, vsp5420-hq-a16 use something other than 10.21.100.11, 10.21.100.12 (the most common set, used by 12 of the 20 switches whose setting was read).	Confirmed	Confirm the approved NTP servers for the site (the most common set is not necessarily the right one) and align every switch to it, so each keeps time from the same sources.

Severity	ID	Affected	Finding	Confidence	Recommended action
LOW	F-MGT-8C2350	10 devices (c9300-hq-a07, c9300-hq-a08, …)	Syslog servers differ between switches: c9300-hq-a07, c9300-hq-a08, vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11, vsp5420-hq-a12, vsp5420-hq-a13, vsp5420-hq-a14 and 2 more use something other than 10.21.100.21, 10.21.100.22 (the most common set, used by 10 of the 20 switches whose setting was read).	Confirmed	Confirm the approved Syslog servers for the site (the most common set is not necessarily the right one) and align every switch to it, so each logs to the same collectors.
LOW	F-SEC-6DAA03	18 devices (c9300-hq-a01, c9300-hq-a02, …)	595 unused ports are left enabled (c9300-hq-c03, c9300-hq-c04, c9300-hq-a01, c9300-hq-a02, c9300-hq-a03, c9300-hq-a04, c9300-hq-a05, c9300-hq-a06 and 10 more).	High confidence	Confirm with the site which of these ports are genuinely unused: "not connected" is a moment in time, and ports used intermittently (mobile carts, docking stations, clinical equipment) look the same.
LOW	F-SEC-3E358B	12 devices (c9300-hq-a01, c9300-hq-a02, …)	Management (VTY) lines are not limited by an access list on c9500-hq-c01, c9500-hq-c02, c9300-hq-c03, c9300-hq-c04, c9300-hq-a01, c9300-hq-a02, c9300-hq-a03, c9300-hq-a04 and 4 more.	Confirmed	Apply an access-class to the VTY lines that permits only the management and jump-host subnets, so SSH to the switches is not reachable from user VLANs.
LOW	F-MGT-EA9BAB	c9300-hq-c03, c9300-hq-c04	SNMP trap destinations differ between devices: most send to 10.21.100.31; c9300-hq-c03, c9300-hq-c04 (10.21.100.31, 10.21.100.32).	Confirmed	Send traps from every device to the same monitoring servers, so faults on any of them raise an alert.
INFO	F-VLN-C65A38	VLANs	VLANs with no gateway on the firewall or a switch: 999 WAN-EDGE.	High confidence	Confirm these are meant to be layer 2 only, or routed by another device; otherwise devices on them cannot reach other subnets.
INFO	F-COV-5E913E	8 devices (c9300-hq-a01, c9300-hq-a02, …)	QoS was not assessed on c9300-hq-a01, c9300-hq-a02, c9300-hq-a03, c9300-hq-a04, c9300-hq-a05, c9300-hq-a06, c9300-hq-a07, c9300-hq-a08: their platform (ios-xe) does not use the classic-IOS QoS model this check reads (mls qos).	Confirmed	Review voice and QoS treatment on these switches against the site's QoS standard and the platform's own QoS model (on IOS-XE: the interface service policies and trust behaviour).
INFO	F-DHCP-725058	c9500-hq-c01, pa3410-hq-f01, pa3410-hq-f02	6 gateway interfaces have no DHCP relay: c9500-hq-c01 Vlan30 (10.10.30.0/24); pa3410-hq-f01 and pa3410-hq-f02 ae1.60 (10.10.60.0/24); c9500-hq-c01 Vlan70 (10.10.70.0/24); c9500-hq-c01 Vlan80 (10.10.80.0/24); pa3410-hq-f01 and pa3410-hq-f02 ae1.110 (10.10.110.0/24); c9500-hq-c01 Vlan10 (10.10.210.0/24).	High confidence	Confirm these subnets are statically addressed or have a DHCP server on the subnet; otherwise clients on them cannot get an address.

Detailed findings

F-HW-ACBCB3	Power, fan or temperature faults: c9300-hq-a03 power supply PSU 1B (member 1, slot B: Bad).	Evidence
Severity	High (Hardware)	
Confidence	Confirmed; Supported by linked evidence; Potentially undesirable configuration	
Affected infrastructure	All affected devices (1): c9300-hq-a03	
Observation	Power, fan or temperature faults: c9300-hq-a03 power supply PSU 1B (member 1, slot B: Bad).	
Why it matters	Availability: The device runs without its power or cooling redundancy; a further failure can stop it.	
Evidence	Live collection: show version / show inventory / show environment; end-of-life list (eol_models.csv); evidence dated 20 Oct 2026	E-LIVE-2FD4F E-AUDI-298B4 E-AUDI-5F9A2
Verify first	Confirm the fault on the device and the replacement part.	
Recommendation	Check and replace the failed unit; the device is still running but without its redundancy.	
Before any change	Verification complete; change approved under the site's normal process.	
Change planning	Routine controlled change	
Tracking	New since 2026-10-20; rule hardware.power-fan-or-temperature (ruleset 2026.10-AJ.1); snapshot 8e957703443f	

F-SUP-982735	Support has ended (21 Aug 2026) for c9300-hq-a05 (1 serials), although the schedule still lists them as live devices.	Evidence
Severity	High (Support)	
Confidence	High confidence; Supported by linked evidence; Requires engineering investigation	
Affected infrastructure	All affected devices (1): c9300-hq-a05	
Observation	Support has ended (21 Aug 2026) for c9300-hq-a05 (1 serials), although the schedule still lists them as live devices.	
Why it matters	Supportability: Without a support contract, hardware replacement and vendor cases are not available when a fault occurs.	
Evidence	Support schedule spreadsheet, matched by serial; rests on locally maintained reference data; evidence dated 19 Oct 2026 - 20 Oct 2026	E-AUDI-298B4 E-AUDI-5F9A2 E-SUPP-CDEF3
Verify first	Confirm the contract state in the contract system.	

F-SUP-982735	Support has ended (21 Aug 2026) for c9300-hq-a05 (1 serials), although the schedule still lists them as live devices.	Evidence
Recommendation	If verification confirms the condition is not intended: renew support for these serials or confirm they moved to another contract; parts and TAC cases depend on it. Check against a newer schedule than RTG_support_schedule_20261019.xlsx.	
Before any change	Complete the verification first; no change until then.	
Change planning	Investigation	
Tracking	New since 2026-10-20; rule support.support-has-ended-serials (ruleset 2026.10-AJ.1); snapshot 8e957703443f	

F-SEC-13E8DF	Access ports have no BPDU guard on vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11, vsp5420-hq-a12, vsp5420-hq-a13, vsp5420-hq-a14, vsp5420-hq-a15, vsp5420-hq-a16.	Evidence
Severity	Medium (Security)	
Confidence	Confirmed; Supported by linked evidence; Potentially undesirable configuration	
Affected infrastructure	All affected devices (8): vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11, vsp5420-hq-a12, vsp5420-hq-a13, vsp5420-hq-a14, vsp5420-hq-a15, vsp5420-hq-a16	
Observation	Access ports have no BPDU guard on vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11, vsp5420-hq-a12, vsp5420-hq-a13, vsp5420-hq-a14, vsp5420-hq-a15, vsp5420-hq-a16.	
Why it matters	Availability: A switch plugged into an access port can join the spanning tree and move the root or cause a loop.	
Evidence	Configuration backups (newest per device); evidence dated 20 Oct 2026	E-BACK-1251F E-BACK-C2556 E-BACK-83272 E-BACK-861DD E-BACK-B24A5 E-BACK-707AA E-BACK-7031E E-BACK-157CB
Verify first	Confirm no switch or bridge is legitimately connected to an edge port (BPDU guard disables it).	
Recommendation	Enable BPDU guard on edge (access) ports, after confirming no switch is legitimately connected to them. Commands are not given: they are written for Cisco ios/ios-xe, and the platform of vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11, vsp5420-hq-a12, vsp5420-hq-a13, vsp5420-hq-a14 and more is voss -- verify the equivalent for that platform. BPDU guard err-disables a port that receives a BPDU: confirm no switch is legitimately connected to an edge port first.	
Before any change	Verification complete; impact assessment, rollback plan and an approved change window.	
Change planning	Potentially disruptive change	

F-SEC-13E8DF	Access ports have no BPDU guard on vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11, vsp5420-hq-a12, vsp5420-hq-a13, vsp5420-hq-a14, vsp5420-hq-a15, vsp5420-hq-a16.	Evidence
Tracking	Open since 2026-07-20; rule security.access-ports-have-no (ruleset 2026.10-AJ.1); snapshot 8e957703443f	

F-SUP-F35F2E	Hardware whose serials are not on the support schedule (RTG_support_schedule_20261019.xlsx), which does list other equipment of the same manufacturer: c9300-hq-a06.	Evidence
Severity	Medium (Support)	
Confidence	High confidence; Supported by linked evidence; Requires engineering investigation	
Affected infrastructure	All affected devices (1): c9300-hq-a06	
Observation	Hardware whose serials are not on the support schedule (RTG_support_schedule_20261019.xlsx), which does list other equipment of the same manufacturer: c9300-hq-a06.	
Why it matters	Supportability: These devices may have no support contract, so a failure may have no replacement path.	
Evidence	Support schedule spreadsheet, matched by serial; rests on locally maintained reference data; evidence dated 19 Oct 2026 - 20 Oct 2026	E-AUDI-298B4 E-AUDI-5F9A2 E-SUPP-CDEF3
Verify first	Confirm the serials against the contract system.	
Recommendation	Confirm whether the serials are under a support contract (the schedule may be incomplete), and add them to the schedule if they are.	
Before any change	Complete the verification first; no change until then.	
Change planning	Investigation	
Tracking	New since 2026-10-20; rule support.hardware-support-schedule (ruleset 2026.10-AJ.1); snapshot 8e957703443f	

F-MGT-79E9FF	NTP servers differ between switches: vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11, vsp5420-hq-a12, vsp5420-hq-a13, vsp5420-hq-a14, vsp5420-hq-a15, vsp5420-hq-a16 use something other than 10.21.100.11, 10.21.100.12 (the most common set, used by 12 of the 20 switches whose setting was read).	Evidence
Severity	Low (Management)	
Confidence	Confirmed; Supported by linked evidence; Inconsistency requiring review	
Affected infrastructure	All affected devices (8): vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11, vsp5420-hq-a12, vsp5420-hq-a13, vsp5420-hq-a14, vsp5420-hq-a15, vsp5420-hq-a16	
Observation	NTP servers differ between switches: vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11, vsp5420-hq-a12, vsp5420-hq-a13, vsp5420-hq-a14, vsp5420-hq-a15, vsp5420-hq-a16 use something other than 10.21.100.11, 10.21.100.12 (the most common set, used by 12 of the 20 switches whose setting was read).	
Why it matters	Maintainability: Devices taking time from different sources can drift apart, so logs disagree.	
Evidence	Live collection: show ntp / show clock / running-config includes; configuration backups; evidence dated 20 Oct 2026	E-AUDI-298B4 E-AUDI-5F9A2 E-BACK-1251F E-BACK-C2556 E-BACK-83272 E-BACK-861DD E-BACK-B24A5 E-BACK-707AA +2 more
Verify first	Confirm the approved NTP servers.	
Recommendation	Confirm the approved NTP servers for the site (the most common set is not necessarily the right one) and align every switch to it, so each keeps time from the same sources.	
Before any change	Verification complete; change approved under the site's normal process.	
Change planning	Routine controlled change	
Tracking	Open since 2026-07-20; rule management.ntp-differs (ruleset 2026.10-AJ.1); snapshot 8e957703443f	

F-MGT-8C2350	Syslog servers differ between switches: c9300-hq-a07, c9300-hq-a08, vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11, vsp5420-hq-a12, vsp5420-hq-a13, vsp5420-hq-a14 and 2 more use something other than 10.21.100.21, 10.21.100.22 (the most common set, used by 10 of the 20 switches whose setting was read).	Evidence
Severity	Low (Management)	
Confidence	Confirmed; Supported by linked evidence; Inconsistency requiring review	
Affected infrastructure	All affected devices (10): c9300-hq-a07, c9300-hq-a08, vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11, vsp5420-hq-a12, vsp5420-hq-a13, vsp5420-hq-a14, vsp5420-hq-a15, vsp5420-hq-a16	
Observation	Syslog servers differ between switches: c9300-hq-a07, c9300-hq-a08, vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11, vsp5420-hq-a12, vsp5420-hq-a13, vsp5420-hq-a14 and 2 more use something other than 10.21.100.21, 10.21.100.22 (the most common set, used by 10 of the 20 switches whose setting was read).	
Why it matters	Security: Logs go to different collectors, leaving gaps in the central record during an investigation.	
Evidence	Live collection: show ntp / show clock / running-config includes; configuration backups; evidence dated 20 Oct 2026	E-AUDI-298B4 E-AUDI-5F9A2 E-BACK-AA467 E-BACK-D58CD E-BACK-1251F E-BACK-C2556 E-BACK-83272 E-BACK-861DD +4 more
Verify first	Confirm the approved syslog collectors.	
Recommendation	Confirm the approved Syslog servers for the site (the most common set is not necessarily the right one) and align every switch to it, so each logs to the same collectors.	
Before any change	Verification complete; change approved under the site's normal process.	
Change planning	Routine controlled change	
Tracking	Open since 2026-07-20; rule management.syslog-differs (ruleset 2026.10-AJ.1); snapshot 8e957703443f	

F-SEC-6DAA03	595 unused ports are left enabled (c9300-hq-c03, c9300-hq-c04, c9300-hq-a01, c9300-hq-a02, c9300-hq-a03, c9300-hq-a04, c9300-hq-a05, c9300-hq-a06 and 10 more).	Evidence
Severity	Low (Security)	
Confidence	High confidence; Supported by linked evidence; Potentially undesirable configuration	
Affected infrastructure	All affected devices (18): c9300-hq-a01, c9300-hq-a02, c9300-hq-a03, c9300-hq-a04, c9300-hq-a05, c9300-hq-a06, c9300-hq-a07, c9300-hq-a08, c9300-hq-c03, c9300-hq-c04, vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11, vsp5420-hq-a12, vsp5420-hq-a13, vsp5420-hq-a14, vsp5420-hq-a15, vsp5420-hq-a16	
Observation	595 unused ports are left enabled (c9300-hq-c03, c9300-hq-c04, c9300-hq-a01, c9300-hq-a02, c9300-hq-a03, c9300-hq-a04, c9300-hq-a05, c9300-hq-a06 and 10 more).	
Why it matters	Security: Anyone with physical access can connect a device to these ports.	
Evidence	Configuration backups (newest per device); an interpretation of the collected data; evidence dated 20 Oct 2026	E-BACK-90E1B E-BACK-8EAAA E-BACK-6C308 E-BACK-8DC5D E-BACK-F2146 E-BACK-8C13C E-BACK-AA467 E-BACK-D58CD +10 more
Verify first	Confirm with the site which ports are genuinely unused (check last input).	
Recommendation	Confirm with the site which of these ports are genuinely unused: "not connected" is a moment in time, and ports used intermittently (mobile carts, docking stations, clinical equipment) look the same. Check each port's last input or history first. Then shut the confirmed-unused ports, or put them in an unused VLAN, in a change window.	
Before any change	Verification complete; change approved under the site's normal process.	
Change planning	Routine controlled change	
Tracking	Open since 2026-07-20; rule security.unused-ports-left-enabled (ruleset 2026.10-AJ.1); snapshot 8e957703443f	

F-SEC-3E358B	Management (VTY) lines are not limited by an access list on c9500-hq-c01, c9500-hq-c02, c9300-hq-c03, c9300-hq-c04, c9300-hq-a01, c9300-hq-a02, c9300-hq-a03, c9300-hq-a04 and 4 more.	Evidence
Severity	Low (Security)	
Confidence	Confirmed; Supported by linked evidence; Potentially undesirable configuration	
Affected infrastructure	All affected devices (12): c9300-hq-a01, c9300-hq-a02, c9300-hq-a03, c9300-hq-a04, c9300-hq-a05, c9300-hq-a06, c9300-hq-a07, c9300-hq-a08, c9300-hq-c03, c9300-hq-c04, c9500-hq-c01, c9500-hq-c02	
Observation	Management (VTY) lines are not limited by an access list on c9500-hq-c01, c9500-hq-c02, c9300-hq-c03, c9300-hq-c04, c9300-hq-a01, c9300-hq-a02, c9300-hq-a03, c9300-hq-a04 and 4 more.	
Why it matters	Security: Management logins are reachable from any network that can route to the switch, including user VLANs.	
Evidence	Configuration backups (newest per device); evidence dated 20 Oct 2026	E-BACK-90E1B E-BACK-8EAAA E-BACK-6C308 E-BACK-8DC5D E-BACK-F2146 E-BACK-8C13C E-BACK-AA467 E-BACK-D58CD +4 more
Verify first	Test the access list from the jump host before saving; a wrong list locks out administrators.	
Recommendation	Apply an access-class to the VTY lines that permits only the management and jump-host subnets, so SSH to the switches is not reachable from user VLANs. (Commands are Cisco ios/ios-xe syntax, unvalidated: check the command reference; apply only through change control. A wrong access list locks out management: test from the jump host before saving.)	
Before any change	Verification complete; change approved under the site's normal process.	
Change planning	Routine controlled change	
Tracking	Open since 2026-07-20; rule security.management-vty-lines-limited (ruleset 2026.10-AJ.1); snapshot 8e957703443f	

F-MGT-EA9BAB	SNMP trap destinations differ between devices: most send to 10.21.100.31; c9300-hq-c03, c9300-hq-c04 (10.21.100.31, 10.21.100.32).	Evidence
Severity	Low (Management)	
Confidence	Confirmed; Supported by linked evidence; Inconsistency requiring review	
Affected infrastructure	All affected devices (2): c9300-hq-c03, c9300-hq-c04	
Observation	SNMP trap destinations differ between devices: most send to 10.21.100.31; c9300-hq-c03, c9300-hq-c04 (10.21.100.31, 10.21.100.32).	
Why it matters	Maintainability: Traps from some devices do not reach the monitoring system others use, so faults may go unnoticed.	
Evidence	Live collection: show ntp / show clock / running-config includes; configuration backups; evidence dated 20 Oct 2026	E-AUDI-298B4 E-AUDI-5F9A2 E-BACK-AB304 E-BACK-C7A10
Verify first	Confirm the approved trap receivers.	
Recommendation	Send traps from every device to the same monitoring servers, so faults on any of them raise an alert.	
Before any change	Verification complete; change approved under the site's normal process.	
Change planning	Routine controlled change	
Tracking	Open since 2026-07-20; rule management.snmp-trap-destinations-differ (ruleset 2026.10-AJ.1); snapshot 8e957703443f	

F-VLN-C65A38	VLANs with no gateway on the firewall or a switch: 999 WAN-EDGE.	Evidence
Severity	Info (VLANs)	
Confidence	High confidence; Supported by linked evidence; Requires engineering investigation	
Affected infrastructure	VLANs	
Observation	VLANs with no gateway on the firewall or a switch: 999 WAN-EDGE.	
Why it matters	Project readiness: If these VLANs are meant to be routed, hosts on them cannot reach other subnets; if they are layer 2 only, there is no impact.	

F-VLN-C65A38	VLANs with no gateway on the firewall or a switch: 999 WAN-EDGE.	Evidence
Evidence	Live collection: show vlan, show interfaces trunk; firewall subinterface tags; an interpretation of the collected data; evidence dated 20 Oct 2026	E-LIVE-3999A E-LIVE-99BB9 E-LIVE-2FD4F E-LIVE-34599 E-LIVE-0987D E-LIVE-A69B3 E-LIVE-30182 E-LIVE-7E9BA +25 more
Verify first	Confirm whether each VLAN is routed, and by which device.	
Recommendation	Confirm these are meant to be layer 2 only, or routed by another device; otherwise devices on them cannot reach other subnets.	
Before any change	Complete the verification first; no change until then.	
Change planning	Investigation	
Tracking	Open since 2026-07-20; rule vlans.vlans-no-gateway-firewall (ruleset 2026.10-AJ.1); snapshot 8e957703443f	

F-COV-5E913E	QoS was not assessed on c9300-hq-a01, c9300-hq-a02, c9300-hq-a03, c9300-hq-a04, c9300-hq-a05, c9300-hq-a06, c9300-hq-a07, c9300-hq-a08: their platform (ios-xe) does not use the classic-IOS QoS model this check reads (mls qos).	Evidence
Severity	Info (Coverage)	
Confidence	Confirmed; Supported by linked evidence; Missing information	
Affected infrastructure	All affected devices (8): c9300-hq-a01, c9300-hq-a02, c9300-hq-a03, c9300-hq-a04, c9300-hq-a05, c9300-hq-a06, c9300-hq-a07, c9300-hq-a08	
Observation	QoS was not assessed on c9300-hq-a01, c9300-hq-a02, c9300-hq-a03, c9300-hq-a04, c9300-hq-a05, c9300-hq-a06, c9300-hq-a07, c9300-hq-a08: their platform (ios-xe) does not use the classic-IOS QoS model this check reads (mls qos).	
Why it matters	Documentation accuracy: The document cannot state this for the devices concerned; anything that would rest on it is unknown, not absent.	
Evidence	Collection results against the NetBox inventory; evidence dated 20 Oct 2026 (1 source undated)	E-AUDI-298B4 E-AUDI-5F9A2 E-NETB-F1949
Verify first	Collect the missing data, then re-run.	

F-COV-5E913E	QoS was not assessed on c9300-hq-a01, c9300-hq-a02, c9300-hq-a03, c9300-hq-a04, c9300-hq-a05, c9300-hq-a06, c9300-hq-a07, c9300-hq-a08: their platform (ios-xe) does not use the classic-IOS QoS model this check reads (mls qos).	Evidence
Recommendation	Review voice and QoS treatment on these switches against the site's QoS standard and the platform's own QoS model (on IOS-XE: the interface service policies and trust behaviour).	
Before any change	Complete the verification first; no change until then.	
Change planning	Investigation	
Tracking	Open since 2026-07-20; rule coverage.qos-not-assessed-platform (ruleset 2026.10-AJ.1); snapshot 8e957703443f	

F-DHCP-725058	6 gateway interfaces have no DHCP relay: c9500-hq-c01 Vlan30 (10.10.30.0/24); pa3410-hq-f01 and pa3410-hq-f02 ae1.60 (10.10.60.0/24); c9500-hq-c01 Vlan70 (10.10.70.0/24); c9500-hq-c01 Vlan80 (10.10.80.0/24); pa3410-hq-f01 and pa3410-hq-f02 ae1.110 (10.10.110.0/24); c9500-hq-c01 Vlan10 (10.10.210.0/24).	Evidence
Severity	Info (DHCP)	
Confidence	High confidence; Supported by linked evidence; Inconsistency requiring review	
Affected infrastructure	All affected devices (3): c9500-hq-c01, pa3410-hq-f01, pa3410-hq-f02	
Observation	6 gateway interfaces have no DHCP relay: c9500-hq-c01 Vlan30 (10.10.30.0/24); pa3410-hq-f01 and pa3410-hq-f02 ae1.60 (10.10.60.0/24); c9500-hq-c01 Vlan70 (10.10.70.0/24); c9500-hq-c01 Vlan80 (10.10.80.0/24); pa3410-hq-f01 and pa3410-hq-f02 ae1.110 (10.10.110.0/24); c9500-hq-c01 Vlan10 (10.10.210.0/24).	
Why it matters	Availability: If clients on these subnets need DHCP, they cannot obtain an address.	
Evidence	Configuration backups (ip helper-address, dhcp-relay); an interpretation of the collected data; firewalls: their own configuration backups (pa3410-hq-f01, pa3410-hq-f02); evidence dated 20 Oct 2026	E-BACK-0BDA0 E-BACK-CF279 E-BACK-31954
Verify first	Confirm the subnets are statically addressed or served locally.	
Recommendation	Confirm these subnets are statically addressed or have a DHCP server on the subnet; otherwise clients on them cannot get an address.	
Before any change	Complete the verification first; no change until then.	
Change planning	Investigation	
Tracking	Open since 2026-07-20; rule dhcp.gateway-interfaces-have-no (ruleset 2026.10-AJ.1); snapshot 8e957703443f	

9.2 Change-control planning

Findings whose remedy is a configuration change or needs a security review, from the same finding records as above. Netopty makes no change and has no authority to make one: each item is a proposal for the site's change process, after the verification shown. Potentially disruptive changes need an impact assessment, a rollback plan and an approved window; an urgent security review calls for a prompt assessment, not an emergency change.

ID	Scope	Recommended action	Class	Verify first	Change window
F-SEC-13E8DF	8 devices: vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11 and 5 more	Enable BPDU guard on edge ports, after confirming no switch is legitimately connected to them. (full recommendation in the findings register)	Potentially disruptive change	Confirm no switch or bridge is legitimately connected to an edge port (BPDU guard disables it).	Approved window, impact assessment, rollback plan
F-HW-ACBCB3	c9300-hq-a03	Check and replace the failed unit; the device is still running but without its redundancy.	Routine controlled change	Confirm the fault on the device and the replacement part.	Normal change approval
F-MGT-79E9FF	8 devices: vsp5420-hq-a09, vsp5420-hq-a10, vsp5420-hq-a11 and 5 more	Confirm the approved NTP servers for the site and align every switch to it, so each keeps time from the same sources. (full recommendation in the findings register)	Routine controlled change	Confirm the approved NTP servers.	Normal change approval
F-MGT-8C2350	10 devices: c9300-hq-a07, c9300-hq-a08, vsp5420-hq-a09 and 7 more	Confirm the approved Syslog servers for the site and align every switch to it, so each logs to the same collectors. (full recommendation in the findings register)	Routine controlled change	Confirm the approved syslog collectors.	Normal change approval
F-MGT-EA9BAB	c9300-hq-c03, c9300-hq-c04	Send traps from every device to the same monitoring servers, so faults on any of them raise an alert.	Routine controlled change	Confirm the approved trap receivers.	Normal change approval

ID	Scope	Recommended action	Class	Verify first	Change window
F-SEC-3E358B	12 devices: c9300-hq-a01, c9300-hq-a02, c9300-hq-a03 and 9 more	Apply an access-class to the VTY lines that permits only the management and jump-host subnets, so SSH to the switches is not reachable from user VLANs. (full recommendation in the findings register)	Routine controlled change	Test the access list from the jump host before saving; a wrong list locks out administrators.	Normal change approval
F-SEC-6DAA03	18 devices: c9300-hq-a01, c9300-hq-a02, c9300-hq-a03 and 15 more	Confirm with the site which of these ports are genuinely unused: "not connected" is a moment in time, and ports used intermittently look the same. (full recommendation in the findings register)	Routine controlled change	Confirm with the site which ports are genuinely unused (check last input).	Normal change approval

9.3 Findings no longer raised

Raised in an earlier document for this site but not by this collection. "Not re-assessed" means this collection did not fully cover the devices and data the finding rests on, so it may still apply.

ID	Area	Finding	Last detected	Status
F-SEC-AED915	Security	Plain HTTP management is enabled on c9300-hq-c03, c9300-hq-c04.	2026-07-20 10:40	Resolved

10 Changes since previous collection

10.1 Summary

Compared with the snapshot generated 2026-07-20 10:40:00 (its evidence collected 20 Jul 2026 - 20 Oct 2026 (1 sources undated)) (snapshot_20260720_104000.json). Ordering, formatting and timestamps do not count as changes. "Indeterminate" means one of the two collections did not fully cover the object, so it may or may not have changed; nothing is reported removed on that basis.

Category	added	removed	modified	renamed	resolved	indeterminate
finding	3	0	0	0	1	0
interface	0	0	3	0	0	0
software	0	0	2	0	0	0

10.2 Changes

Observed changes, most significant first.

Significance	Category	Object	Change	Previous	Current	Confidence
Medium	finding	F-HW-ACBCB3	added		Power, fan or temperature faults: c9300-hq-a03 power supply PSU 1B (member 1, slot B: Bad).	Confirmed
Medium	finding	F-SUP-982735	added		Support has ended (21 Aug 2026) for c9300-hq-a05 (1 serials), although the schedule still lists them as live devices.	High confidence
Medium	finding	F-SUP-F35F2E	added		Hardware whose serials are not on the support schedule (RTG_support_schedule_20261019.xlsx), which does list other equipment of the same manufacturer: c9300-hq-	High confidence
Medium	software	c9500-hq-c01	modified	17.9.4a	17.9.5	Confirmed
Medium	software	c9500-hq-c02	modified	17.9.4a	17.9.5	Confirmed
Low	finding	F-SEC-AED915	resolved	Plain HTTP management is enabled on c9300-hq-c03, c9300-hq-c04.		High confidence
Low	interface	c9300-hq-a03|Gi1/0/40	modified	description MFP Level 2 copy room hq-prn-01	description printer hq-prn-01	Confirmed
Low	interface	c9300-hq-a04|Gi1/0/45	modified	access_vlan 20; voice_vlan 30	access_vlan 80; voice_vlan -	Confirmed

Significance	Category	Object	Change	Previous	Current	Confidence
Low	interface	vsp5420-hq-a16|1/40	modified	access_vlan 1; description -; neighbour -; oper down; speed 0	access_vlan 10; description AP hq-blb-ap24; neighbour hq-blb-ap24; oper up; speed 1000	Confirmed

Appendix A Optics

Switch	Port	Optic	Status
c9500-hq-c01	Hu1/0/25	QSFP-100G-LR4	connected
c9500-hq-c01	Hu1/0/27	QSFP-100G-SR4	connected
c9500-hq-c01	Hu1/0/28	QSFP-100G-SR4	connected
c9500-hq-c01	Twe1/0/1	SFP-25GBase-SR	connected
c9500-hq-c01	Twe1/0/10	SFP-25GBase-SR	connected
c9500-hq-c01	Twe1/0/13	SFP-25GBase-LR	connected
c9500-hq-c01	Twe1/0/2	SFP-25GBase-SR	connected
c9500-hq-c01	Twe1/0/21	SFP-25GBase-SR	connected
c9500-hq-c01	Twe1/0/22	SFP-25GBase-SR	connected
c9500-hq-c01	Twe1/0/3	SFP-25GBase-SR	connected
c9500-hq-c01	Twe1/0/4	SFP-25GBase-SR	connected
c9500-hq-c01	Twe1/0/5	SFP-25GBase-SR	connected
c9500-hq-c01	Twe1/0/6	SFP-25GBase-SR	connected
c9500-hq-c01	Twe1/0/7	SFP-25GBase-SR	connected
c9500-hq-c01	Twe1/0/8	SFP-25GBase-SR	connected
c9500-hq-c01	Twe1/0/9	SFP-25GBase-SR	connected
c9500-hq-c02	Hu1/0/25	QSFP-100G-LR4	connected
c9500-hq-c02	Hu1/0/27	QSFP-100G-SR4	connected
c9500-hq-c02	Hu1/0/28	QSFP-100G-SR4	connected
c9500-hq-c02	Twe1/0/1	SFP-25GBase-SR	connected
c9500-hq-c02	Twe1/0/10	SFP-25GBase-SR	connected
c9500-hq-c02	Twe1/0/13	SFP-25GBase-LR	connected
c9500-hq-c02	Twe1/0/2	SFP-25GBase-SR	connected
c9500-hq-c02	Twe1/0/21	SFP-25GBase-SR	connected
c9500-hq-c02	Twe1/0/22	SFP-25GBase-SR	connected
c9500-hq-c02	Twe1/0/3	SFP-25GBase-SR	connected
c9500-hq-c02	Twe1/0/4	SFP-25GBase-SR	connected
c9500-hq-c02	Twe1/0/5	SFP-25GBase-SR	connected
c9500-hq-c02	Twe1/0/6	SFP-25GBase-SR	connected
c9500-hq-c02	Twe1/0/7	SFP-25GBase-SR	connected
c9500-hq-c02	Twe1/0/8	SFP-25GBase-SR	connected
c9500-hq-c02	Twe1/0/9	SFP-25GBase-SR	connected
c9300-hq-c03	Te1/1/1	SFP-10GBase-SR	connected

Switch	Port	Optic	Status
c9300-hq-c03	Te1/1/2	SFP-10GBase-SR	connected
c9300-hq-c04	Te1/1/1	SFP-10GBase-SR	connected
c9300-hq-c04	Te1/1/2	SFP-10GBase-SR	connected
c9300-hq-a01	Te1/1/1	SFP-10GBase-SR	connected
c9300-hq-a01	Te2/1/1	SFP-10GBase-SR	connected
c9300-hq-a02	Te1/1/1	SFP-10GBase-SR	connected
c9300-hq-a02	Te2/1/1	SFP-10GBase-SR	connected
c9300-hq-a03	Te1/1/1	SFP-10GBase-SR	connected
c9300-hq-a03	Te1/1/2	SFP-10GBase-SR	connected
c9300-hq-a04	Te1/1/1	SFP-10GBase-SR	connected
c9300-hq-a04	Te1/1/2	SFP-10GBase-SR	connected
c9300-hq-a05	Te1/1/1	SFP-10GBase-SR	connected
c9300-hq-a05	Te1/1/2	SFP-10GBase-SR	connected
c9300-hq-a06	Te1/1/1	SFP-10GBase-SR	connected
c9300-hq-a06	Te1/1/2	SFP-10GBase-SR	connected
c9300-hq-a07	Te1/1/1	SFP-10GBase-SR	connected
c9300-hq-a07	Te1/1/2	SFP-10GBase-SR	connected
c9300-hq-a08	Te1/1/1	SFP-10GBase-SR	connected
c9300-hq-a08	Te1/1/2	SFP-10GBase-SR	connected
vsp5420-hq-a09	1/49	10GbSR	upup
vsp5420-hq-a09	1/50	10GbSR	upup
vsp5420-hq-a10	1/49	10GbSR	upup
vsp5420-hq-a10	1/50	10GbSR	upup
vsp5420-hq-a11	1/49	10GbSR	upup
vsp5420-hq-a11	1/50	10GbSR	upup
vsp5420-hq-a12	1/49	10GbSR	upup
vsp5420-hq-a12	1/50	10GbSR	upup
vsp5420-hq-a13	1/49	10GbSR	upup
vsp5420-hq-a13	1/50	10GbSR	upup
vsp5420-hq-a14	1/49	10GbSR	upup
vsp5420-hq-a14	1/50	10GbSR	upup
vsp5420-hq-a15	1/49	10GbSR	upup
vsp5420-hq-a15	1/50	10GbSR	upup
vsp5420-hq-a16	1/49	10GbSR	upup
vsp5420-hq-a16	1/50	10GbSR	upup

Appendix B Access points

Access points found on the switch ports (the access point audit and LLDP). The vendor is what the access point reports over LLDP/CDP, or the registered owner of its own MAC address; one marked * is inferred less directly, from the MACs on its switch port or its mgt0 port name.

Access point	Vendor	Model	Switch	Port	PoE (W)
hq-bla-ap01	Cisco	cisco C9120AXI-Z	c9300-hq-a01	Gi1/0/1	15.4
hq-bla-ap02	Cisco	cisco C9120AXI-Z	c9300-hq-a01	Gi1/0/2	15.4
hq-bla-ap03	Cisco	cisco C9120AXI-Z	c9300-hq-a02	Gi1/0/1	15.4
hq-bla-ap04	Cisco	cisco C9120AXI-Z	c9300-hq-a02	Gi1/0/2	15.4
hq-bla-ap05	Cisco	cisco C9120AXI-Z	c9300-hq-a03	Gi1/0/1	15.4
hq-bla-ap06	Cisco	cisco C9120AXI-Z	c9300-hq-a03	Gi1/0/2	15.4
hq-bla-ap07	Cisco	cisco C9120AXI-Z	c9300-hq-a04	Gi1/0/1	15.4
hq-bla-ap08	Cisco	cisco C9120AXI-Z	c9300-hq-a04	Gi1/0/2	15.4
hq-bla-ap09	Cisco	cisco C9120AXI-Z	c9300-hq-a05	Gi1/0/1	15.4
hq-bla-ap10	Cisco	cisco C9120AXI-Z	c9300-hq-a05	Gi1/0/2	15.4
hq-bla-ap11	Cisco	cisco C9120AXI-Z	c9300-hq-a06	Gi1/0/1	15.4
hq-bla-ap12	Cisco	cisco C9120AXI-Z	c9300-hq-a06	Gi1/0/2	15.4
hq-bla-ap13	Cisco	cisco C9120AXI-Z	c9300-hq-a07	Gi1/0/1	15.4
hq-bla-ap14	Cisco	cisco C9120AXI-Z	c9300-hq-a07	Gi1/0/2	15.4
hq-bla-ap15	Cisco	cisco C9120AXI-Z	c9300-hq-a08	Gi1/0/1	15.4
hq-bla-ap16	Cisco	cisco C9120AXI-Z	c9300-hq-a08	Gi1/0/2	15.4
hq-blb-ap17	Extreme Networks	ExtremeWireless AP5050U	vsp5420-hq-a09	1/40	15.4
hq-blb-ap18	Extreme Networks	ExtremeWireless AP5050U	vsp5420-hq-a10	1/40	15.4
hq-blb-ap19	Extreme Networks	ExtremeWireless AP5050U	vsp5420-hq-a11	1/40	15.4
hq-blb-ap20	Extreme Networks	ExtremeWireless AP5050U	vsp5420-hq-a12	1/40	15.4
hq-blb-ap21	Extreme Networks	ExtremeWireless AP5050U	vsp5420-hq-a13	1/40	15.4
hq-blb-ap22	Extreme Networks	ExtremeWireless AP5050U	vsp5420-hq-a14	1/40	15.4
hq-blb-ap23	Extreme Networks	ExtremeWireless AP5050U	vsp5420-hq-a15	1/40	15.4
hq-blb-ap24	Extreme Networks	ExtremeWireless AP5050U	vsp5420-hq-a16	1/40	15.4

Appendix C Collection status

Per device and capability, what this collection actually parsed: C complete, P partial, F failed, U unsupported, NT not attempted, NR not requested by the collection profile, - not applicable, ? unknown (not collected, or collected without a usable result). A device that answered is not complete by answering; "?" is missing data, not a negative result. Capabilities: Inv inventory, Id identity, HW hardware, Intf interfaces, VLAN vlans, STP spanning tree, Topo topology, L3 layer 3, Rte routing, FW firewall config, Mgmt management, Sec security, Bkp config backup, Env environment.

Device	Inv	Id	HW	Intf	VLAN	STP	Topo	L3	Rte	FW	Mgmt	Sec	Bkp	Env
c9500-hq-c01	C	C	C	C	C	C	C	C	C	-	C	C	C	C
c9500-hq-c02	C	C	C	C	C	C	C	C	C	-	C	C	C	C
c9300-hq-c03	C	C	C	C	C	C	C	C	C	-	C	C	C	C
c9300-hq-c04	C	C	C	C	C	C	C	C	C	-	C	C	C	C
c9300-hq-a01	C	C	C	C	C	C	C	C	C	-	C	C	C	C
c9300-hq-a02	C	C	C	C	C	C	C	C	C	-	C	C	C	C
c9300-hq-a03	C	C	C	C	C	C	C	C	C	-	C	C	C	C
c9300-hq-a04	C	C	C	C	C	C	C	C	C	-	C	C	C	C
c9300-hq-a05	C	C	C	C	C	C	C	C	C	-	C	C	C	C
c9300-hq-a06	C	C	C	C	C	C	C	C	C	-	C	C	C	C
c9300-hq-a07	C	C	C	C	C	C	C	C	C	-	C	C	C	C
c9300-hq-a08	C	C	C	C	C	C	C	C	C	-	C	C	C	C
vsp5420-hq-a09	C	C	C	C	C	C	C	C	C	-	C	C	C	C
vsp5420-hq-a10	C	C	C	C	C	C	C	C	C	-	C	C	C	C
vsp5420-hq-a11	C	C	C	C	C	C	C	C	C	-	C	C	C	C
vsp5420-hq-a12	C	C	C	C	C	C	C	C	C	-	C	C	C	C
vsp5420-hq-a13	C	C	C	C	C	C	C	C	C	-	C	C	C	C
vsp5420-hq-a14	C	C	C	C	C	C	C	C	C	-	C	C	C	C

Device	Inv	Id	HW	Intf	VLAN	STP	Topo	L3	Rte	FW	Mgmt	Sec	Bkp	Env
vsp5420-hq-a15	C	C	C	C	C	C	C	C	C	-	C	C	C	C
vsp5420-hq-a16	C	C	C	C	C	C	C	C	C	-	C	C	C	C
pa3410-hq-f01	C	C	C	C	-	-	C	C	C	C	C	C	C	C
pa3410-hq-f02	C	C	C	C	-	-	C	C	C	C	C	C	C	C

Appendix D Evidence register

The evidence the findings rest on, referenced by ID from each finding. Each record gives the item's place in the evidence package (relative to the artifact store, so the document carries no workstation paths); command output and configurations are not reproduced here. Collected is when the data was collected, as far as its source records it (the time source is given in brackets; unknown when not recorded); Age is days from then to when this document ingested it.

ID	Source	Device	Method	Collected	Age	Status	Reference
E-AUDI-298B4	Live collection: switch audit workbook	(site)	show version, show inventory, show vlan, show spanning-tree summary, show ntp, show logging	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/audits/cisco_switch_audit_output_RTG-HQ.xlsx
E-AUDI-5F9A2	Live collection: switch audit workbook	(site)	show version, show inventory, show vlan, show spanning-tree summary, show ntp, show logging	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/audits/extreme_switch_audit_output_RTG-HQ.xlsx
E-BACK-0BDA0	Configuration backup	c9500-hq-c01	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/cisco/20261020_020000/c9500-hq-c01_backup_20261020_020000.txt
E-BACK-2421C	Configuration backup	c9500-hq-c02	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/cisco/20261020_020000/c9500-hq-c02_backup_20261020_020000.txt
E-BACK-AB304	Configuration backup	c9300-hq-c03	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/cisco/20261020_020000/c9300-hq-c03_backup_20261020_020000.txt
E-BACK-C7A10	Configuration backup	c9300-hq-c04	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/cisco/20261020_020000/c9300-hq-c04_backup_20261020_020000.txt
E-BACK-90E1B	Configuration backup	c9300-hq-a01	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/cisco/20261020_020000/c9300-hq-a01_backup_20261020_020000.txt

ID	Source	Device	Method	Collected	Age	Status	Reference
E-BACK-8EAAA	Configuration backup	c9300-hq-a02	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/cisco/20261020_020000/c9300-hq-a02_backup_20261020_020000.txt
E-BACK-6C308	Configuration backup	c9300-hq-a03	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/cisco/20261020_020000/c9300-hq-a03_backup_20261020_020000.txt
E-BACK-8DC5D	Configuration backup	c9300-hq-a04	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/cisco/20261020_020000/c9300-hq-a04_backup_20261020_020000.txt
E-BACK-F2146	Configuration backup	c9300-hq-a05	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/cisco/20261020_020000/c9300-hq-a05_backup_20261020_020000.txt
E-BACK-8C13C	Configuration backup	c9300-hq-a06	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/cisco/20261020_020000/c9300-hq-a06_backup_20261020_020000.txt
E-BACK-AA467	Configuration backup	c9300-hq-a07	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/cisco/20261020_020000/c9300-hq-a07_backup_20261020_020000.txt
E-BACK-D58CD	Configuration backup	c9300-hq-a08	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/cisco/20261020_020000/c9300-hq-a08_backup_20261020_020000.txt
E-BACK-1251F	Configuration backup	vsp5420-hq-a09	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/extreme/20261020_020000/vsp5420-hq-a09_extreme_backup_20261020_020000.txt

ID	Source	Device	Method	Collected	Age	Status	Reference
E-BACK-C2556	Configuration backup	vsp5420-hq-a10	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/extreme/20261020_020000/vsp5420-hq-a10_extreme_backup_20261020_020000.txt
E-BACK-83272	Configuration backup	vsp5420-hq-a11	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/extreme/20261020_020000/vsp5420-hq-a11_extreme_backup_20261020_020000.txt
E-BACK-861DD	Configuration backup	vsp5420-hq-a12	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/extreme/20261020_020000/vsp5420-hq-a12_extreme_backup_20261020_020000.txt
E-BACK-B24A5	Configuration backup	vsp5420-hq-a13	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/extreme/20261020_020000/vsp5420-hq-a13_extreme_backup_20261020_020000.txt
E-BACK-707AA	Configuration backup	vsp5420-hq-a14	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/extreme/20261020_020000/vsp5420-hq-a14_extreme_backup_20261020_020000.txt
E-BACK-7031E	Configuration backup	vsp5420-hq-a15	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/extreme/20261020_020000/vsp5420-hq-a15_extreme_backup_20261020_020000.txt
E-BACK-157CB	Configuration backup	vsp5420-hq-a16	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/extreme/20261020_020000/vsp5420-hq-a16_extreme_backup_20261020_020000.txt
E-BACK-CF279	Configuration backup	pa3410-hq-f01	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/palo/20261020_020000/pa3410-hq-f01_paloalto_backup_20261020_020000.txt

ID	Source	Device	Method	Collected	Age	Status	Reference
E-BACK-31954	Configuration backup	pa3410-hq-f02	configuration backup	20 Oct 2026 02:00 (backup file name)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/backups/palo/20261020_020000/pa3410-hq-f02_paloalto_backup_20261020_020000.txt
E-LIFE-DECEB	Vendor lifecycle data	(site)	vendor lifecycle data	20 Oct 2026 02:00 (file modified)	16	Complete	software_audit/lifecycle_data
E-LIVE-9A070	Live collection (SSH)	c9500-hq-c01	show version | include uptime; show environment all (+6 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/cisco_raw_c9500-hq-c01.txt
E-LIVE-4D93E	Live collection (SSH)	c9500-hq-c02	show version | include uptime; show environment all (+6 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/cisco_raw_c9500-hq-c02.txt
E-LIVE-5A805	Live collection (SSH)	c9300-hq-c03	show version | include uptime; show environment all (+6 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/cisco_raw_c9300-hq-c03.txt
E-LIVE-7EBA0	Live collection (SSH)	c9300-hq-c04	show version | include uptime; show environment all (+6 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/cisco_raw_c9300-hq-c04.txt
E-LIVE-3999A	Live collection (SSH)	c9300-hq-a01	show version | include uptime; show environment all (+6 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/cisco_raw_c9300-hq-a01.txt
E-LIVE-99BB9	Live collection (SSH)	c9300-hq-a02	show version | include uptime; show environment all (+6 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/cisco_raw_c9300-hq-a02.txt
E-LIVE-2FD4F	Live collection (SSH)	c9300-hq-a03	show version | include uptime; show environment all (+6 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/cisco_raw_c9300-hq-a03.txt
E-LIVE-34599	Live collection (SSH)	c9300-hq-a04	show version | include uptime; show environment all (+6 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/cisco_raw_c9300-hq-a04.txt

ID	Source	Device	Method	Collected	Age	Status	Reference
E-LIVE-0987D	Live collection (SSH)	c9300-hq-a05	show version | include uptime; show environment all (+6 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/cisco_raw_c9300-hq-a05.txt
E-LIVE-A69B3	Live collection (SSH)	c9300-hq-a06	show version | include uptime; show environment all (+6 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/cisco_raw_c9300-hq-a06.txt
E-LIVE-30182	Live collection (SSH)	c9300-hq-a07	show version | include uptime; show environment all (+6 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/cisco_raw_c9300-hq-a07.txt
E-LIVE-7E9BA	Live collection (SSH)	c9300-hq-a08	show version | include uptime; show environment all (+6 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/cisco_raw_c9300-hq-a08.txt
E-LIVE-26704	Live collection (SSH)	vsp5420-hq-a09	lldp_detail_out; port_state_out (+5 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/extreme_l3_raw_vsp5420-hq-a09.txt
E-LIVE-50132	Live collection (SSH)	vsp5420-hq-a09	show spanning-tree mstp status; show spanning-tree mstp port role (+2 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/extreme_asbuilt_raw_vsp5420-hq-a09.txt
E-LIVE-A0CE1	Live collection (SSH)	vsp5420-hq-a10	lldp_detail_out; port_state_out (+5 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/extreme_l3_raw_vsp5420-hq-a10.txt
E-LIVE-E7A02	Live collection (SSH)	vsp5420-hq-a10	show spanning-tree mstp status; show spanning-tree mstp port role (+2 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/extreme_asbuilt_raw_vsp5420-hq-a10.txt
E-LIVE-BDFB0	Live collection (SSH)	vsp5420-hq-a11	lldp_detail_out; port_state_out (+5 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/extreme_l3_raw_vsp5420-hq-a11.txt
E-LIVE-AC153	Live collection (SSH)	vsp5420-hq-a11	show spanning-tree mstp status; show spanning-tree mstp port role (+2 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/extreme_asbuilt_raw_vsp5420-hq-a11.txt

ID	Source	Device	Method	Collected	Age	Status	Reference
E-LIVE-1E5EC	Live collection (SSH)	vsp5420-hq-a12	lldp_detail_out; port_state_out (+5 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/extreme_l3_raw_vsp5420-hq-a12.txt
E-LIVE-4CF12	Live collection (SSH)	vsp5420-hq-a12	show spanning-tree mstp status; show spanning-tree mstp port role (+2 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/extreme_asbuilt_raw_vsp5420-hq-a12.txt
E-LIVE-6A189	Live collection (SSH)	vsp5420-hq-a13	lldp_detail_out; port_state_out (+5 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/extreme_l3_raw_vsp5420-hq-a13.txt
E-LIVE-BD4B6	Live collection (SSH)	vsp5420-hq-a13	show spanning-tree mstp status; show spanning-tree mstp port role (+2 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/extreme_asbuilt_raw_vsp5420-hq-a13.txt
E-LIVE-47F45	Live collection (SSH)	vsp5420-hq-a14	lldp_detail_out; port_state_out (+5 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/extreme_l3_raw_vsp5420-hq-a14.txt
E-LIVE-FEB24	Live collection (SSH)	vsp5420-hq-a14	show spanning-tree mstp status; show spanning-tree mstp port role (+2 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/extreme_asbuilt_raw_vsp5420-hq-a14.txt
E-LIVE-B73FF	Live collection (SSH)	vsp5420-hq-a15	lldp_detail_out; port_state_out (+5 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/extreme_l3_raw_vsp5420-hq-a15.txt
E-LIVE-EA82A	Live collection (SSH)	vsp5420-hq-a15	show spanning-tree mstp status; show spanning-tree mstp port role (+2 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/extreme_asbuilt_raw_vsp5420-hq-a15.txt
E-LIVE-C8C03	Live collection (SSH)	vsp5420-hq-a16	lldp_detail_out; port_state_out (+5 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/extreme_l3_raw_vsp5420-hq-a16.txt
E-LIVE-416C2	Live collection (SSH)	vsp5420-hq-a16	show spanning-tree mstp status; show spanning-tree mstp port role (+2 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/extreme_asbuilt_raw_vsp5420-hq-a16.txt

ID	Source	Device	Method	Collected	Age	Status	Reference
E-LIVE-87C99	Live collection (SSH)	pa3410-hq-f01	show system info; show interface all (+11 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/palo_raw_pa3410-hq-f01.txt
E-LIVE-3552E	Live collection (SSH)	pa3410-hq-f02	show system info; show interface all (+11 more commands)	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/raw/palo_raw_pa3410-hq-f02.txt
E-MAPP-E33D6	Live collection: CDP/LLDP mapping workbook	(site)	show cdp/lldp neighbors detail, LACP/MLT	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/discovery/network_mapping_output_RTG-HQ.xlsx
E-NETB-F1949	NetBox	(site)	NetBox API: devices, prefixes, circuits, site	unknown (not recorded)		Complete	NetBox
E-PORT-974DE	Live collection: port status workbook	(site)	show interfaces status	20 Oct 2026 10:15 (file modified)	16	Complete	Riverside Technology Group [RTG]/RTG-HQ/audits/port_status_audit_output_RTG-HQ.xlsx
E-SUPP-CDEF3	Support schedule	(site)	support schedule matched by serial	19 Oct 2026 16:30 (file modified)	17	Complete	Riverside Technology Group [RTG]/_supplemental/RTG_support_schedule_20261019.xlsx
E-WAN-F2274	WAN provider export	(site)	WAN provider portal export	19 Oct 2026 16:30 (file modified)	17	Complete	Riverside Technology Group [RTG]/_supplemental/RTG_wan_services_export_20261019.csv