STRATUM

STRATUM Switch

User's Guide

Version 0.4.3 | August 2026

Native Layer-2 switching for STRATUM virtual datacenters, test bays, distributed labs, and external network integration.

Document scope

This guide documents the STRATUM Switch v0.4.3 behavior, CLI, runtime architecture, configuration model, diagnostics, and management interface supplied with the current STRATUM integration.

About This Guide

STRATUM Switch is STRATUM's native lightweight Layer-2 switch runtime. It is designed to be placed directly on a STRATUM canvas and used like a managed Ethernet switch without requiring a network operating system image, a virtual machine, a container, or a virtual disk.

This guide is intended for STRATUM administrators, lab designers, network engineers, test engineers, and operators who need to configure virtual switching, VLAN trunks, Q-in-Q provider bridging, topology protection, aggregation, packet observation, fault injection, or distributed test-bay connectivity.

> **VERSION SCOPE:** The examples and command reference are based on STRATUM Switch v0.4.3 and runtime schema 3. Behavior can change in later releases; use show version on a running node when validating a deployed environment.

Conventions

Notation	Meaning
STRATUM-SW1#	Privileged EXEC prompt.
STRATUM-SW1(config)#	Global configuration prompt.
STRATUM-SW1(config-if)#	Single-interface configuration prompt.
STRATUM-SW1(config-if-range)#	Interface-range configuration prompt.
STRATUM-SW1(config-vlan)#	VLAN configuration prompt.
<value>	Required value in syntax descriptions.
[value]	Optional value or clause.
Ethernet0/1	Typical STRATUM Switch interface name.

Contents

1. Product Overview 5

2. Architecture and Network Model 6

3. Deploying and Accessing STRATUM Switch 7

4. CLI Fundamentals 8

5. Baseline Configuration and Verification 9

6. VLANs and Access Ports 10

7. IEEE 802.1Q Trunking 11

8. IEEE 802.1ad / Q-in-Q Provider Bridging 12

9. MAC Learning and the Forwarding Database 14

10. Rapid Spanning Tree 15

11. Link Aggregation and LACP 16

12. LLDP and Topology Discovery 17

13. IGMP and MLD Snooping 18

14. Private VLANs and Protected Ports 19

15. Port Security, Storm Control, and Err-Disable 20

16. SPAN and Packet Capture 21

17. Fault Injection and Network Impairment 22

18. Distributed Execution, VXLAN, and External Networks 23

19. STRATUM-Native Diagnostics 24

20. Configuration Management and Recovery 25

21. Operational Design Patterns 26

22. Troubleshooting 28

23. Security and Qualification Boundaries 29

Appendix A. Complete CLI Command Reference 30

Appendix B. Runtime JSON Reference 37

Appendix C. Control API Reference 39

Appendix D. Defaults and Limits 40

Appendix E. Glossary 41

1. Product Overview

STRATUM Switch provides an Ethernet switching plane that is native to STRATUM. Each switch instance is a small C11 process with TAP-backed ports. It participates in the same STRATUM mission canvas and network attachment model used by other runtimes, while retaining a switch-oriented CLI and management surface.

- **Lightweight runtime.** One process can expose up to 256 Ethernet ports using a single epoll event loop.
- **Managed Layer 2.** Access ports, 802.1Q trunks, native VLANs, VLAN-aware MAC learning, static MAC entries, RSTP, LACP, LLDP, multicast snooping, private VLANs, SPAN, packet capture, and security controls are implemented directly in the switch.
- **Provider bridging.** v0.4.3 adds true IEEE 802.1ad Q-in-Q behavior using an outer 0x88a8 S-tag while preserving an optional customer 0x8100 C-tag.
- **Distributed by STRATUM.** When a logical vdatacenter network spans workers, STRATUM can build a stable-VNI VXLAN substrate below the switch.
- **Test-lab instrumentation.** Per-port impairment, forced link state, Ethernet test frames, PCAP capture, counters, topology validation, and tech-support output are built in.

1.1 What STRATUM Switch does not replace

STRATUM Switch is intentionally a Layer-2 switch. It does not become a router, DHCP server, NAT gateway, firewall, or customer-configurable VXLAN control plane merely because it is connected to those services. Routing, addressing, DHCP, NAT, and firewall behavior are supplied by attached virtual appliances, STRATUM network objects, or upstream infrastructure.

> **Q-IN-Q BOUNDARY:** Q-in-Q provider bridging does not imply Layer-2 protocol tunneling. Transparent tunneling of customer STP/BPDU/CDP-style control protocols is a separate feature and is not part of v0.4.3. Contact us if you need this feature.

2. Architecture and Network Model

The most important architectural distinction is between the switch dataplane and the network substrate that connects a STRATUM logical network across a host or across workers. VLAN and Q-in-Q decisions occur in the STRATUM Switch process. Distributed VXLAN, bridge creation, and worker placement are performed by STRATUM's runtime integration.

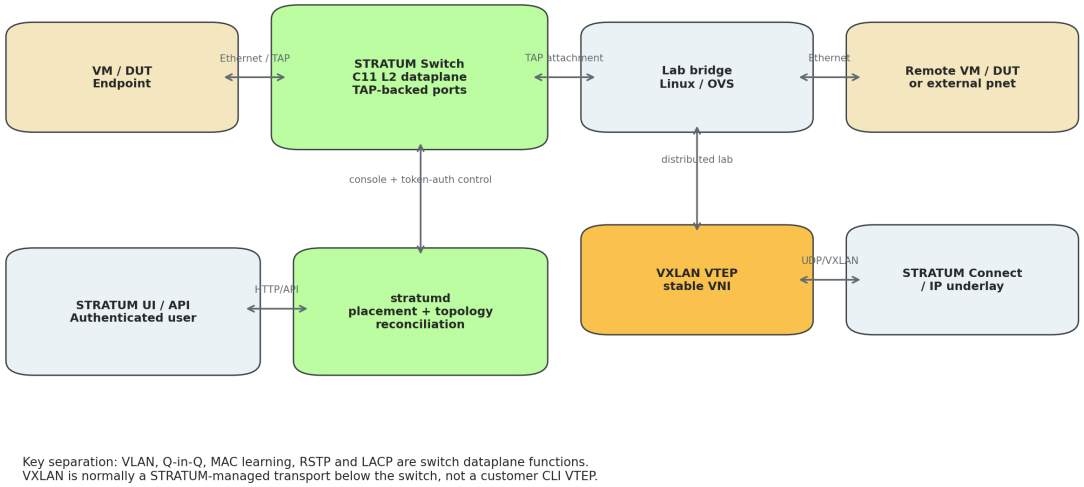

Figure 1. STRATUM Switch dataplane, management plane, and distributed transport.

2.1 Port and attachment model

Every Ethernet interface is backed by a TAP device created or prepared by STRATUM. The runtime JSON associates the interface with its TAP name, logical network identity, bridge, external-network flag, and peer/topology metadata. The switch itself reads and writes Ethernet frames through these TAP file descriptors.

- **Local lab network.** A TAP attaches to an existing Linux or Open vSwitch bridge representing the STRATUM logical network.
- **Distributed vdatacenter network.** The STRATUM worker prepares the lab bridge and, when configured, a stable-VNI VXLAN interface that extends the logical network to other workers.
- **External network.** For pnetN (physical network), natN, cloud, or another external network type, STRATUM validates the already-present external bridge. The switch remains Layer 2.

2.2 Forwarding pipeline

1. Validate the ingress port state and parse Ethernet/VLAN headers.
2. Consume local control protocols such as LLDP, RSTP, and LACP as appropriate.
3. Classify the ingress frame into an access VLAN, 802.1Q trunk VLAN, Q-in-Q service VLAN, or private-VLAN service context.
4. Apply multicast snooping, port security, MAC learning, and storm-control policy.
5. Look up the destination MAC or flood broadcast, multicast, and unknown-unicast traffic as required.
6. Apply private-VLAN/protected-port policy, spanning-tree state, channel selection, and multicast egress filtering.
7. Rewrite the egress tag presentation for access, 802.1Q trunk, Q-in-Q edge, or 802.1ad provider trunk ports, then transmit.

2.3 Management plane

Operators normally use the STRATUM console presented for the switch node.

3. Deploying and Accessing STRATUM Switch

3.1 STRATUM node defaults

The supplied STRATUM node definition is an eight-port switch template. Administrators can adjust the number of Ethernet ports and selected runtime defaults before deployment.

Node setting	Default / behavior
Ethernet Ports	8 by default; effective runtime supports up to 256 per switch.
MTU	1500 in the supplied node template; runtime/manual invocation can use other values.
MAC Aging Time	300 seconds.
Per-Port Queue Bytes	4,194,304 bytes (4 MiB) in the STRATUM integration.
LLDP	Enabled by default.
Rapid Spanning Tree	Enabled by default.
IGMP Snooping	Enabled by default.
MLD Snooping	Enabled by default.

3.2 Starting a switch

When a STRATUM Switch node is started, STRATUM prepares its workspace, management token, runtime JSON, Ethernet TAPs, network attachments, and console/control endpoints. In a distributed deployment, STRATUM submits a low-memory one-CPU Slurm job to the selected worker, then prepares local bridges and VXLANs before launching the switch process.

3.3 Console access

The node console is a TCP/Telnet-style terminal. Depending on the node/template attributes, STRATUM Switch can require a configured console username and/or secret. The CLI supports multiple concurrent read-only sessions, with one exclusive configuration lock.

> **CONCURRENCY:** Up to eight CLI sessions are supported. Only the session holding the configuration lock can enter configuration mode; operational show commands remain available to other sessions.

4. CLI Fundamentals

4.1 Modes and prompts

Mode	Use
Privileged EXEC	Operational commands, show/clear/test/capture, checkpoints, write/copy, diagnostics.
Global configuration	System-wide settings, VLAN creation, interface selection, monitoring sessions, static MAC entries.
Interface configuration	Access/trunk/Q-in-Q/PVLAN, RSTP edge/guards, LACP, security, storm control, impairment.
Interface-range configuration	Applies a supported interface command to every selected port.
VLAN configuration	VLAN name and private-VLAN type/association.

```
STRATUM-SW1# configure terminal
STRATUM-SW1(config)# interface Ethernet0/1
STRATUM-SW1(config-if)# exit
STRATUM-SW1(config)# vlan 20
STRATUM-SW1(config-vlan)# end
STRATUM-SW1#
```

4.2 Help, completion, abbreviations, and editing

- **Context help.** Press ? to display commands relevant to the current CLI mode.
- **Tab completion.** TAB completes supported top-level command patterns or displays multiple matches.
- **Unambiguous abbreviations.** Common tokens can be shortened; for example sh int stat canonicalizes to show interfaces status.
- **History.** Up/Down arrows navigate up to 32 stored commands.
- **Editing.** Left/Right arrows, Ctrl-A, Ctrl-E, Ctrl-U, Ctrl-W, Ctrl-C, Backspace, and Delete-compatible backspace are supported.
- **Paging.** terminal length controls --More-- output; Space advances a page, Enter advances one line, and q exits paging.

4.3 Output filters and redirection

```
show running-config | include spanning-tree
show running-config | exclude shutdown
show running-config | begin interface Ethernet0/8
show running-config | section Ethernet0/8
show interfaces | count
show tech-support | redirect tech-support.txt
```

include, exclude, begin, section, and count are simple text filters. redirect writes the command output to a path relative to the switch workspace; absolute paths and parent-directory traversal are rejected.

4.4 Running operational commands from configuration mode

```
STRATUM-SW1(config-if)# do show interfaces Ethernet0/1
STRATUM-SW1(config-if)# do show mac address-table
```

5. Baseline Configuration and Verification

A new switch starts with VLAN 1 active, interfaces in access mode on VLAN 1, LLDP/RSTP/IGMP/MLD enabled by the standard STRATUM integration, MAC learning enabled, and no storm-control or impairment thresholds.

5.1 Set identity and basic timers

```
configure terminal
hostname TEST-BAY-SW1
mac address-table aging-time 300
lldp run
spanning-tree mode rapid
ip igmp snooping
ipv6 mld snooping
end
write memory
```

5.2 Verify the node before changing it

```
show version
show system
show interfaces status
show vlan brief
show spanning-tree
show stratum runtime
show stratum validation
```

5.3 Reset an interface to defaults

```
configure terminal
default interface Ethernet0/4

# or a range
default interface range Ethernet0/1-8
end
```

SAFETY: default interface removes the switch-level configuration on the selected port, clears learned entries associated with the port, and restores access VLAN 1, ordinary 802.1Q encapsulation, standard RSTP cost, and default security/impairment state.

6. VLANs and Access Ports

6.1 Create and name VLANs

```
configure terminal
vlan 10
 name MANAGEMENT
 exit
vlan 20
 name SERVERS
 exit
vlan 30
 name TEST-CLIENTS
 exit
end
```

VLAN IDs 1 through 4094 are valid. VLAN 1 is created by default. A VLAN can also become active implicitly when it is referenced by an access port, trunk list, native VLAN, Q-in-Q service VLAN, static MAC entry, or private-VLAN mapping.

6.2 Configure access ports

```
configure terminal
interface Ethernet0/1
 description Application Server
 switchport mode access
 switchport access vlan 20
 spanning-tree portfast
 no shutdown
exit
interface Ethernet0/2
 description Test Client
 switchport mode access
 switchport access vlan 30
 spanning-tree portfast
 no shutdown
end
```

Access ports accept untagged ingress Ethernet frames. Tagged ingress frames are rejected and counted as invalid-VLAN drops. Frames leaving an access port are emitted without an 802.1Q tag.

6.3 Configure many access ports

```
configure terminal
interface range Ethernet0/1-8,Ethernet0/12
 description COMPUTE-NODES
 switchport mode access
 switchport access vlan 20
 spanning-tree portfast
 switchport port-security
 no shutdown
end
```

6.4 Verify VLAN membership

```
show vlan brief
show vlan id 20
show interfaces switchport
show interfaces switchport Ethernet0/1
show mac address-table vlan 20
```

7. IEEE 802.1Q Trunking

An ordinary trunk carries one or more 802.1Q VLANs. The native VLAN is the untagged VLAN for the trunk; all other allowed VLANs are emitted with a 0x8100 tag. On ingress, an untagged frame is classified into the native VLAN and a tagged frame is classified by its 802.1Q VLAN ID.

7.1 Basic trunk

```
configure terminal
interface Ethernet0/24
 description TEST-BAY-UPLINK
 switchport mode trunk
 switchport trunk native vlan 10
 switchport trunk allowed vlan 10,20,30
 no shutdown
end

show interfaces trunk
```

7.2 Modify the allowed VLAN set

```
configure terminal
interface Ethernet0/24
 switchport trunk allowed vlan add 40-49
 switchport trunk allowed vlan remove 20
 switchport trunk allowed vlan except 100-199
end
```

The allowed-VLAN parser accepts comma-separated VLANs and ranges. The keywords all and none are supported for replacement. add preserves the current list and enables additional VLANs; remove subtracts VLANs; except begins with all VLANs allowed and removes the specified set.

7.3 Native VLAN behavior

The native VLAN is meaningful only for ordinary dot1q trunks. Setting the native VLAN also marks that VLAN as allowed. A provider dot1ad trunk does not use a native VLAN because the outer service tag is mandatory.

7.4 Test-bay example

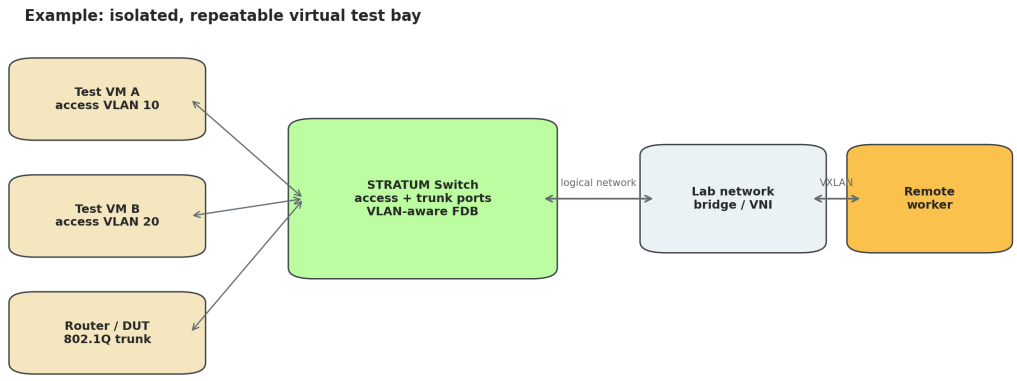

Figure 2. A trunk-capable virtual test bay can span a STRATUM distributed logical network.

DESIGN PATTERN: Use access ports for ordinary endpoints and a trunk port for a virtual router, firewall, network appliance, nested system, or physical uplink that needs to see multiple VLANs.

8. IEEE 802.1ad / Q-in-Q Provider Bridging

v0.4.3 implements true provider bridging with a 0x88a8 outer S-tag. A customer-facing Q-in-Q edge port maps all accepted customer traffic into a configured service VLAN while preserving an optional customer 0x8100 C-tag. A provider trunk switches and learns on the service VLAN and adds or removes the S-tag as traffic crosses the provider boundary.

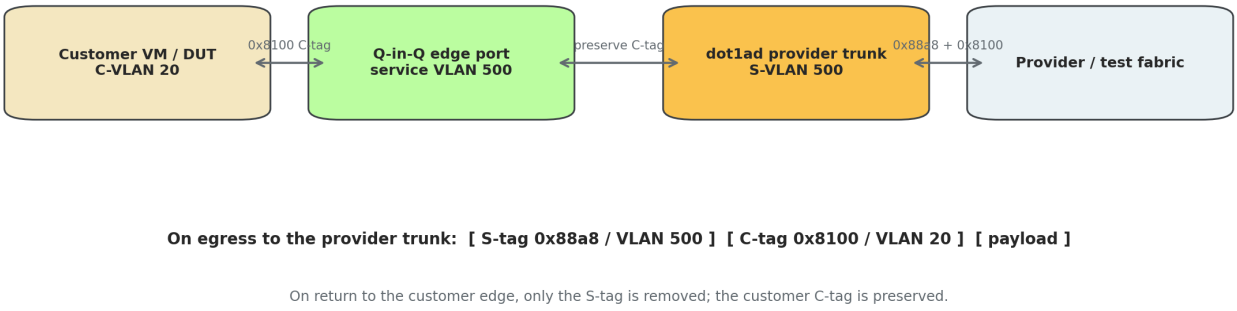

Figure 3. Q-in-Q customer edge and provider trunk tag behavior.

8.1 Configure the customer edge

```
configure terminal
interface Ethernet0/1
 description CUSTOMER-TEST-BAY
 switchport mode qinq
 switchport qinq service vlan 500
 no shutdown
end
```

switchport mode dot1q-tunnel is accepted as an alias for switchport mode qinq. The corresponding dot1q-tunnel service VLAN form is also accepted.

8.2 Configure the provider trunk

```
configure terminal
interface Ethernet0/24
 description PROVIDER-DOT1AD
 switchport mode trunk
 switchport trunk encapsulation dot1ad
 switchport trunk allowed vlan 500,501
 no shutdown
end
```

8.3 Ingress validation and safety

- **Q-in-Q edge.** Accepts an untagged customer frame or one 0x8100 customer tag. A customer-injected 0x88a8 S-tag or already stacked customer frame is rejected.
- **dot1ad provider trunk.** Requires an explicit 0x88a8 S-tag on ingress. Untagged traffic and a bare 0x8100 C-tag are rejected.
- **Service VLAN filtering.** The provider S-VLAN must be present in the trunk's allowed VLAN set.
- **No native service VLAN.** dot1ad trunks always emit the S-tag and do not treat any service VLAN as untagged.

8.4 Return to ordinary trunking

```
configure terminal
interface Ethernet0/24
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 10
end
```

INTEROPERABILITY BOUNDARY: The frame parser recognizes up to two VLAN headers (802.1Q and/or 802.1ad). The Q-in-Q customer edge intentionally accepts at most one customer 0x8100 tag. This is provider bridging, not arbitrary multi-level VLAN stacking.

9. MAC Learning and the Forwarding Database

The forwarding database is VLAN-aware. Source MAC addresses are learned against the effective service VLAN, and destination lookup uses the same VLAN context. Dynamic entries age according to the configured MAC aging timer; static entries persist in the running configuration.

9.1 View the FDB

```
show mac address-table
show mac address-table summary
show mac address-table dynamic
show mac address-table static
show mac address-table vlan 20
show mac address-table interface Ethernet0/5
show mac address-table address 52:54:00:12:34:56
```

9.2 Static MAC entries

```
configure terminal
mac address-table static 52:54:00:12:34:56 vlan 20 interface Ethernet0/5
end

configure terminal
no mac address-table static 52:54:00:12:34:56 vlan 20
end
```

9.3 Disable learning on a port

```
configure terminal
interface Ethernet0/5
 mac-learning disable
end
```

Disabling MAC learning removes dynamic entries currently associated with the port. Static entries are not removed by that action.

9.4 Clear dynamic learning

```
clear mac address-table dynamic
```

10. Rapid Spanning Tree

STRATUM Switch implements a single common-instance rapid spanning tree. It protects Layer-2 topologies from loops and exposes familiar edge and guard controls. It is not a per-VLAN PVST/RPVST or MST implementation in v0.4.3.

10.1 Enable or disable RSTP

```
configure terminal
spanning-tree mode rapid
end

# Disable globally
configure terminal
no spanning-tree
end
```

10.2 Edge ports and guards

```
configure terminal
interface Ethernet0/1
 spanning-tree portfast
 spanning-tree bpduguard enable
exit
interface Ethernet0/24
 spanning-tree guard root
 spanning-tree cost 10000
end
```

PortFast marks an endpoint-facing interface as an edge port. BPDU Guard can err-disable a protected edge port if a BPDU is received. Root Guard and Loop Guard mark a port inconsistent when the corresponding protection condition is detected. Root Guard and Loop Guard are mutually exclusive on a port.

10.3 Operational views

```
show spanning-tree
show spanning-tree detail
show spanning-tree blockedports
show spanning-tree inconsistentports
show spanning-tree interface Ethernet0/24
```

RECOVERY: If BPDU Guard err-disables a port, use clear errdisable interface <port> for manual recovery or enable timed recovery with errdisable recovery cause bpduguard.

11. Link Aggregation and LACP

STRATUM Switch supports up to 64 port-channel groups. A member can use static aggregation (mode on) or IEEE LACP in active or passive mode. Egress selection uses flow hashing, and flooding is de-duplicated so a flooded frame is sent once per channel rather than once per physical member.

11.1 Static EtherChannel

```
configure terminal
interface range Ethernet0/21-22
 channel-group 10 mode on
end
```

11.2 LACP

```
configure terminal
interface Ethernet0/21
 channel-group 10 mode active
exit
interface Ethernet0/22
 channel-group 10 mode active
end
```

11.3 Remove a member

```
configure terminal
interface Ethernet0/22
 no channel-group
end
```

11.4 Verify aggregation

```
show etherchannel summary
show etherchannel load-balance
show lacp neighbor
show lacp internal
show lacp counters
show lacp system-id
```

12. LLDP and Topology Discovery

LLDP is enabled by default in the supplied STRATUM template. The switch transmits and receives LLDP, ages neighbors, reports remote chassis/port/system information, and exposes topology metadata used by STRATUM diagnostics.

```
show lldp neighbors
show lldp neighbors detail
show lldp traffic
show lldp interface Ethernet0/4
```

12.1 Global control

```
configure terminal
lldp run
end

configure terminal
no lldp run
end
```

The default LLDP interval is 30 seconds and hold time is 120 seconds in v0.4.3.

13. IGMP and MLD Snooping

IPv4 IGMP and IPv6 MLD snooping constrain multicast flooding by learning multicast group membership. This is a Layer-2 optimization; it does not provide multicast routing.

```
show ip igmp snooping
show ip igmp snooping groups
show ip igmp snooping statistics
show ip igmp snooping mrouter
show ip igmp snooping vlan 20

show ipv6 mld snooping
show ipv6 mld snooping groups
show ipv6 mld snooping statistics
show ipv6 mld snooping mrouter
```

13.1 Enable or disable snooping

```
configure terminal
ip igmp snooping
ipv6 mld snooping
end

# Disable either family independently
configure terminal
no ip igmp snooping
no ipv6 mld snooping
end
```

13.2 Clear learned multicast state

```
clear multicast
```

The implementation maintains up to 256 multicast group records. Membership aging is 260 seconds and multicast-router aging is 255 seconds in v0.4.3.

14. Private VLANs and Protected Ports

Private VLANs provide finer isolation than ordinary VLANs while preserving a shared primary service context. STRATUM Switch supports primary, isolated, and community VLAN types, host ports, and promiscuous ports. Protected ports provide a simpler local isolation mechanism.

14.1 Define a private-VLAN domain

```
configure terminal
vlan 100
 name PVLAN-PRIMARY
 private-vlan primary
 exit
vlan 101
 name PVLAN-ISOLATED
 private-vlan isolated
 private-vlan primary 100
 exit
vlan 102
 name PVLAN-COMMUNITY
 private-vlan community
 private-vlan primary 100
 exit
end
```

14.2 Host and promiscuous ports

```
configure terminal
interface Ethernet0/1
 switchport mode private-vlan host
 switchport private-vlan host-association 100 101
exit
interface Ethernet0/2
 switchport mode private-vlan host
 switchport private-vlan host-association 100 102
exit
interface Ethernet0/24
 switchport mode private-vlan promiscuous
 switchport private-vlan mapping 100
end
```

Isolated hosts cannot forward directly to other private-VLAN host ports. Community hosts can communicate with hosts in the same community secondary VLAN. Host ports can communicate through a promiscuous port associated with the same primary VLAN.

14.3 Protected ports

```
configure terminal
interface range Ethernet0/5-8
 switchport protected
end
```

Two protected ports do not forward Layer-2 traffic directly to each other. They can still communicate with an eligible unprotected port. Use no switchport protected to remove the restriction.

```
show private-vlan
show private-vlan interface Ethernet0/1
```

15. Port Security, Storm Control, and Err-Disable

15.1 Port security

Port security limits the number of source MAC addresses accepted on an interface. Sticky learning can promote accepted learned addresses to static FDB entries. Violation handling can silently protect, count/restrict, or err-disable the port.

```
configure terminal
interface Ethernet0/4
 switchport port-security
 switchport port-security maximum 4
 switchport port-security mac-address sticky
 switchport port-security violation shutdown
end
```

```
show port-security
show port-security interface Ethernet0/4
```

Violation mode	Behavior
protect	Drop violating source traffic without err-disabling the port.
restrict	Drop and count violations while keeping the port forwarding for permitted MAC addresses.
shutdown	Drop the violation and place the port into err-disabled state.

15.2 Storm control

Storm-control thresholds are packets per one-second window. A value of zero disables the corresponding threshold.

```
configure terminal
interface Ethernet0/4
 storm-control broadcast 1000
 storm-control multicast 5000
 storm-control unknown-unicast 2000
end
```

15.3 Err-disable and recovery

```
configure terminal
errdisable recovery cause bpduguard
errdisable recovery cause port-security
errdisable recovery interval 300
end

show errdisable recovery
show interfaces status err-disabled
clear errdisable interface Ethernet0/4
```

The recovery interval accepts 30 through 86400 seconds. Automatic recovery can be enabled independently for BPDU Guard and port-security causes. Manual clear is available at any time.

16. SPAN and Packet Capture

16.1 SPAN to another switch port

Up to four mirror sessions are supported. A session can have multiple RX, TX, or bidirectional source ports. A port destination is monitor-only by default, preventing it from participating in normal forwarding unless the forwarding keyword is explicitly used.

```
configure terminal
monitor session 1 source interface Ethernet0/3 both
monitor session 1 source interface Ethernet0/4 rx
monitor session 1 destination interface Ethernet0/8
end

show monitor session
```

16.2 SPAN directly to PCAP

```
configure terminal
monitor session 2 source interface Ethernet0/3 both
monitor session 2 destination pcap /stratum/tmp/<workspace>/span-2.pcap
end
```

Direct PCAP SPAN uses the switch's safe PCAP rotation defaults. Remove an entire session with no monitor session <id>.

16.3 Per-port capture

```
capture interface Ethernet0/4 both max-size 500MB rotate 5 duration 300 ether-host 52:54:00:12:34:56
show capture detail
no capture interface Ethernet0/4
```

Per-port capture defaults to 500 MiB per file with five rotations. max-size accepts bytes or K/KB, M/MB, and G/GB suffixes. duration is seconds; zero means no duration limit. If no file path is specified, the capture is placed in the switch workspace as capture-port-<id>.pcap.

> **STORAGE CONTROL:** Capture rotation and duration should be chosen conservatively on shared STRATUM storage. Capture files can be large and are intentionally treated as workspace artifacts.

17. Fault Injection and Network Impairment

STRATUM Switch includes deterministic lab-oriented tools for simulating link failures and degraded Ethernet conditions. These controls are intended for test and resilience workflows rather than production traffic shaping.

17.1 Link state simulation

```
test interface Ethernet0/4 link down
test interface Ethernet0/4 link up
test interface Ethernet0/4 link flap count 5 interval 2
```

17.2 Per-port impairment

```
configure terminal
interface Ethernet0/4
 impairment delay 25
 impairment jitter 5
 impairment loss 10000
 impairment duplicate 1000
 impairment reorder 5000
 impairment corrupt 100
 impairment rate 100000000
end

show impairment interface Ethernet0/4
```

PROBABILITY UNITS: loss, duplicate, reorder, and corrupt are parts per million (ppm). For example, 10000 = 1%, 1000 = 0.1%, and 100 = 0.01%. delay and jitter are milliseconds; rate is bits per second.

17.3 Clear impairment

```
clear impairment interface Ethernet0/4

# or from interface configuration
configure terminal
interface Ethernet0/4
 no impairment
end
```

17.4 Inject STRATUM test frames

```
test ethernet interface Ethernet0/4 destination ff:ff:ff:ff:ff:ff vlan 20 count 10
```

Generated test frames use STRATUM-reserved experimental EtherType 0x88B5. The command is useful for validating a path, VLAN presentation, capture, or counter behavior without depending on a guest workload.

18. Distributed Execution, VXLAN, and External Networks

STRATUM Switch can run on the controller or on a selected worker. In distributed execution, STRATUM's switch-specific Slurm launcher prepares the Ethernet substrate before starting the native switch process. This design keeps customer switching behavior independent from the transport used to span a logical STRATUM network.

18.1 Stable-VNI VXLAN

For an ordinary non-external lab bridge, the runtime integration derives a stable VNI from the logical bridge name when VXLAN is enabled. The worker creates or reuses vxlan<VNI>, attaches it to the lab bridge, sets the effective link MTU, and then launches STRATUM Switch. The default VXLAN destination port is UDP 4789.

- **With STRATUM Network Fabric.** The VTEP binds to the STRATUM fabric IP/interface, uses the fabric peer list for flood destinations, and respects the fabric payload MTU.
- **Without required fabric mode.** The launcher can use a multicast VXLAN group on the selected VXLAN device.
- **Inside the switch.** The STRATUM Switch process still sees Ethernet on its TAP. It does not need to parse the transport VXLAN header.

18.2 Customer VXLAN inside a test bay

A VM or virtual network appliance can itself generate or terminate UDP/VXLAN traffic. In that case, VXLAN is simply payload from the STRATUM Switch point of view. The switch forwards the outer Ethernet/IP/UDP frames according to its Layer-2 policy, while the guest device remains the VTEP under test.

18.3 External bridge-backed networks

External networks such as pnetN, natN, or cloud-backed objects are treated differently from ordinary lab bridges. STRATUM validates that the resolved external Linux or OVS bridge already exists on the selected worker and is usable. It does not create a parallel stable-VNI overlay for that external attachment.

> **PHYSICAL TRUNKS:** To carry an 802.1Q or 802.1ad trunk to physical infrastructure, the entire path from the STRATUM Switch TAP through the host bridge/OVS and physical NIC must preserve the required Ethernet tags. Validate the host and physical-switch configuration end to end.

18.4 Live topology synchronization

When a mission canvas link or network attachment changes, STRATUM sends a one-shot token-authenticated set_port_attachment command only to the affected running switch port. The switch reconciles the TAP's actual Linux/OVS bridge master, updates topology metadata, and clears dynamic FDB entries learned on that port. There is no inventory polling loop.

19. STRATUM-Native Diagnostics

The native diagnostic commands combine switch state with the runtime metadata supplied by STRATUM. They are especially useful when the Ethernet switch configuration looks correct but the worker attachment, VXLAN substrate, bridge membership, MTU, or topology does not.

```
show stratum runtime
show stratum fabric
show stratum topology
show stratum validation
show stratum vxlan
diagnose topology
diagnose fabric
trace mac 52:54:00:12:34:56
show tech-support
```

19.1 Validation categories

Local validation can report evidence for native-VLAN/allowed-VLAN inconsistencies, MTU mismatches, aggregation/channel concerns, spanning-tree guard states, VXLAN/backend attachment issues, external bridge problems, and monitor-destination inconsistencies. Graph-wide path correlation remains a controller-level concern rather than an inference made by the switch process itself.

19.2 Interface topology view

```
show interface Ethernet0/4 topology
show interfaces descriptions
show lldp neighbors detail
```

Interface telemetry distinguishes the bridge configured by STRATUM from the actual kernel/OVS master. The management API exposes bridge, bridge_actual, and bridge_attached so missing or stale attachments can be diagnosed explicitly.

19.3 Tech-support collection

```
terminal length 0
show tech-support | redirect tech-support.txt
```

show tech-support includes version/runtime data, STRATUM fabric and validation state, interface status and errors, VLANs, private VLANs, FDB, RSTP, LACP, LLDP, multicast state, SPAN/capture, port security, err-disable, impairments, running configuration, and recent events.

20. Configuration Management and Recovery

20.1 Running and startup configuration

```
show running-config
show startup-config
write memory
copy running-config startup-config
copy startup-config running-config
erase startup-config
```

Startup configuration is written through a temporary file, fsync, and atomic rename behind the scenes of STRATUM. The previous startup configuration is retained as startup-config.prev.

20.2 Configuration diff and history

```
show configuration diff startup-config running-config
show configuration changes
show configuration history
```

20.3 Named checkpoints and rollback

```
checkpoint before-trunk-change
show checkpoints

configure terminal
interface Ethernet0/24
 switchport trunk allowed vlan 10,30
end

show configuration changes
rollback checkpoint before-trunk-change
```

20.4 Confirmed rollback

Entering configuration mode automatically captures a hidden rollback point. commit confirmed starts a timer of 10 through 3600 seconds. If commit is not issued before the timer expires, the switch reloads the configuration captured when configuration mode was entered.

```
configure terminal
interface Ethernet0/24
 switchport trunk allowed vlan 10,30
end
commit confirmed 120

# Verify reachability and policy, then:
commit
```

REMOTE CHANGES: Use commit confirmed before changing a trunk, security policy, or attachment that could cut off management reachability.

21. Operational Design Patterns

21.1 Virtual test bay with a DUT trunk

Use access ports for ordinary endpoint VMs and a trunk toward the device under test. This reproduces a familiar physical test-bay pattern while allowing the entire bay to remain a versioned STRATUM topology.

```
configure terminal
vlan 10
 name MGMT
 exit
vlan 20
 name USERS
 exit
vlan 30
 name SERVICES
 exit
interface Ethernet0/1
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
exit
interface Ethernet0/2
 switchport mode access
 switchport access vlan 20
 spanning-tree portfast
exit
interface Ethernet0/10
 description DUT-TRUNK
 switchport mode trunk
 switchport trunk native vlan 10
 switchport trunk allowed vlan 10,20,30
end
```

21.2 Provider-bridged tenant/test-bay handoff

Use a Q-in-Q edge port when the attached customer/test appliance controls its own C-VLAN IDs but the provider/test fabric needs a distinct service VLAN namespace.

```
configure terminal
interface Ethernet0/1
 switchport mode qinq
 switchport qinq service vlan 700
exit
interface Ethernet0/24
 switchport mode trunk
 switchport trunk encapsulation dot1ad
 switchport trunk allowed vlan 700
end
```

21.3 Capture before changing a path

```
checkpoint before-change
capture interface Ethernet0/24 both duration 120
show interfaces counters errors
show stratum validation
# perform the change
show capture detail
```

21.4 Resilience test

```
configure terminal
interface Ethernet0/4
 impairment delay 75
 impairment jitter 20
 impairment loss 25000
end

test interface Ethernet0/4 link flap count 3 interval 5
```

22. Troubleshooting

Symptom	Recommended checks
Port shows down or not-forwarding	Check show interfaces status, administrative shutdown, forced link state, err-disable, monitor-destination status, and spanning-tree state. Use show spanning-tree interface <port> and show impairment interface <port>.
Access-port traffic is dropped	An access port rejects tagged ingress traffic. Confirm switchport mode access and verify the endpoint is sending untagged Ethernet.
Trunk VLAN does not pass	Check show interfaces trunk, allowed VLAN membership, native VLAN agreement, active VLAN state, and the upstream device configuration.
dot1ad provider trunk drops traffic	A dot1ad provider trunk requires a 0x88a8 S-tag. Untagged traffic and a bare 0x8100 C-tag are intentionally rejected.
Q-in-Q customer edge drops traffic	The edge accepts untagged or one 0x8100 C-tag. Customer S-tags or already stacked frames are rejected.
MAC never appears in FDB	Check mac-learning disable, port-security, VLAN classification, port state, and show interfaces counters errors.
Port is err-disabled	Use show errdisable recovery and show port-security interface <port>. Clear manually or enable the correct recovery cause.
Multicast floods unexpectedly	Confirm IGMP/MLD snooping is enabled and verify learned groups. Clear multicast state if testing changed topology abruptly.
Distributed path fails across workers	Use show stratum fabric, show stratum validation, worker runtime logs, bridge attachment telemetry, and verify the STRATUM fabric/VXLAN substrate.
External pnet trunk loses tags	Validate the host Linux/OVS bridge, physical NIC, NIC offload/driver assumptions, and physical switch trunk. STRATUM Switch cannot preserve tags if an upstream/downstream component strips them.
Console change cut connectivity	Use commit confirmed for risky changes. If the timer is still active, allow automatic rollback; otherwise rollback a named checkpoint or reload startup-config.

22.1 First-response command set

```
show version
show interfaces status
show interfaces counters errors
show interfaces trunk
show mac address-table summary
show spanning-tree detail
show lldp neighbors detail
show stratum runtime
show stratum validation
show logging
show tech-support | redirect tech-support.txt
```

23. Security and Qualification Boundaries

23.1 Management security

STRATUM creates management.token from 32 bytes of cryptographic randomness and stores it mode 0600. Console authentication can be configured per node/template; the current release compares the configured secret directly, so the vdatacenter definition must be protected accordingly.

23.2 Runtime privilege boundary

The switch opens TAP devices supplied by STRATUM and runs with the privileges of the configured STRATUM runtime user. The current security documentation recommends Linux capability reduction, seccomp, and no_new_privs before treating the process as a hard security enforcement boundary.

23.3 Qualification boundary

The v0.4.3 source is designed to pass strict GCC/Clang builds, static-PIE compilation, unit/protocol tests, and Address/UndefinedBehavior sanitizers. Those tests do not replace real multi-worker STRATUM/VXLAN qualification, physical-uplink interoperability, throughput benchmarking, fuzzing, long-duration soak, or production network certification.

> **POSITIONING:** Treat STRATUM Switch as a STRATUM-native lab and virtual-datacenter switching runtime. Qualify the exact external hardware, hypervisor, worker, MTU, and physical network path used in a production or mission environment.

Appendix A. Complete CLI Command Reference

The following tables consolidate the v0.4.3 command surface implemented by the native CLI. Some commands have aliases; the canonical form is listed first, with important aliases noted in the description.

A.1 Privileged EXEC: system, configuration, and session

Command	Mode	Purpose / notes
`help / ?`	EXEC	Display summary help; pressing ? interactively provides context help.
`show version`	EXEC	Version, runtime schema, build timestamp.
`show system`	EXEC	PID, uptime, port count, FDB size, MAC moves, queue limit, control socket, events path. Aliases: show processes, show memory, show uptime.
`show users`	EXEC	Display connected CLI users/sessions.
`show configuration lock`	EXEC	Show whether configuration mode is locked and by which console file descriptor.
`configure terminal`	EXEC	Enter global configuration mode and capture the hidden configuration-entry rollback point.
`write memory`	EXEC	Atomically save running configuration as startup-config. Alias: copy running-config startup-config.
`copy startup-config running-config`	EXEC	Load startup configuration into the running switch.
`erase startup-config`	EXEC	Remove the startup-config file.
`show running-config`	EXEC	Display current running configuration.
`show startup-config`	EXEC	Display saved startup configuration.
`show configuration diff startup-config running-config`	EXEC	Show startup-to-running differences. Alias: show configuration changes.
`show configuration history`	EXEC	Display recent configuration-related event records.
`checkpoint <name>`	EXEC	Create a named running-configuration checkpoint.
`show checkpoints`	EXEC	List checkpoint files.
`rollback checkpoint <name>`	EXEC	Load a named checkpoint.
`commit confirmed <10-3600>`	EXEC	Start timed rollback to the configuration captured on entry to configuration mode.
`commit`	EXEC	Cancel a pending confirmed rollback and accept the current configuration.
`terminal length <n>`	EXEC	Set page length. 0 disables paging.
`terminal width <n>`	EXEC	Set terminal width metadata.
`enable`	EXEC	Accepted compatibility command; no mode change is required.
`exit / quit / logout`	EXEC	Close the CLI session.

A.2 Privileged EXEC: interface and VLAN views

Command	Mode	Purpose / notes
`show interfaces`	EXEC	Interface status summary. Aliases: show interfaces status, show interfaces brief.
`show interfaces counters`	EXEC	Interface packet/byte counters. Alias: show interfaces accounting.
`show interfaces counters errors`	EXEC	Runts, giants, VLAN, STP, PVLAN, multicast, port-security, and impairment drops.
`show interfaces trunk`	EXEC	Trunk encapsulation, native VLAN, state, and allowed VLAN list. Alias: show interfaces vlan membership.
`show interfaces descriptions`	EXEC	Interface descriptions/topology labels. Alias: show interfaces description.
`show interfaces switchport`	EXEC	Switchport mode and VLAN summary for all ports.
`show interfaces switchport <port>`	EXEC	Detailed switchport/interface view for one port.
`show interface <port>`	EXEC	Detailed single-interface status.
`show interface <port> queue`	EXEC	Output-queue bytes, limit, and drops.
`show interface <port> topology`	EXEC	Detailed interface plus STRATUM topology/attachment metadata.
`show interface <port> transceiver`	EXEC	Accepted detailed-interface alias; no physical optics model is implied.
`show interface <port> accounting`	EXEC	Accepted detailed-interface alias.
`show vlan`	EXEC	VLAN table. Alias: show vlan brief.
`show vlan id <1-4094>`	EXEC	Show one VLAN name and normal/private type.

A.3 Privileged EXEC: FDB, protocols, security, and observation

Command	Mode	Purpose / notes
`show mac address-table`	EXEC	Display FDB entries.
`show mac address-table summary`	EXEC	Dynamic/static/total counts and aging timer. Alias: ... count.
`show mac address-table dynamic`	EXEC	Dynamic entries only.
`show mac address-table static`	EXEC	Static entries only.
`show mac address-table vlan <id>`	EXEC	Entries for one VLAN.
`show mac address-table interface <port>`	EXEC	Entries learned/installed on one port.
`show mac address-table address <mac>`	EXEC	Entries matching one MAC.
`clear mac address-table dynamic`	EXEC	Flush dynamic FDB entries.
`show spanning-tree`	EXEC	RSTP bridge/root summary and per-port role/state. Aliases: summary, root.
`show spanning-tree detail`	EXEC	Detailed RSTP state and timers. Alias: statistics.
`show spanning-tree blockedports`	EXEC	Non-forwarding/inconsistent ports. Alias: inconsistentports.
`show spanning-tree interface <port>`	EXEC	Detailed RSTP view for one interface.

Command	Mode	Purpose / notes
`show etherchannel summary`	EXEC	Configured port channels and member state. Aliases: show port-channel, load-balance.
`show etherchannel <...>`	EXEC	Accepted channel-summary family.
`show lacp neighbor`	EXEC	LACP member/partner information. Aliases: internal, counters, system-id.
`show lldp neighbors`	EXEC	LLDP neighbor summary. Alias: show lldp.
`show lldp neighbors detail`	EXEC	Detailed LLDP neighbors. Alias: show lldp errors.
`show lldp traffic`	EXEC	LLDP traffic counters.
`show lldp interface <port>`	EXEC	Neighbor on one local port.
`show ip igmp snooping`	EXEC	IPv4 snooping summary. Aliases: statistics, mrouter.
`show ip igmp snooping groups`	EXEC	Learned IPv4 multicast groups.
`show ip igmp snooping vlan <id>`	EXEC	IPv4 multicast group table path scoped by command family.
`show ipv6 mld snooping`	EXEC	IPv6 snooping summary. Aliases: statistics, mrouter.
`show ipv6 mld snooping groups`	EXEC	Learned IPv6 multicast groups.
`clear multicast`	EXEC	Clear learned multicast state.
`show private-vlan`	EXEC	Private VLANs and private/protected port summary.
`show private-vlan interface <port>`	EXEC	Private-VLAN role and association for a port.
`show port-security`	EXEC	Configured secure ports and violation counts.
`show port-security interface <port>`	EXEC	Detailed port-security status.
`show errdisable recovery`	EXEC	Err-disabled ports and recovery policy. Alias: show interfaces status err-disabled.
`clear errdisable interface <port>`	EXEC	Manually recover an err-disabled port.
`show monitor session`	EXEC	Configured SPAN sessions.
`show capture`	EXEC	Active per-port captures. Alias: show capture detail.
`show logging`	EXEC	Display recent events.jsonl content (up to internal display cap).
`show logging last <N>`	EXEC	Read approximately N KiB from the end of the event file.
`clear counters`	EXEC	Clear interface counters.

A.4 Privileged EXEC: capture, tests, impairment, and STRATUM diagnostics

Command	Mode	Purpose / notes
`capture interface <port> [rx|tx|both] [max-size <size>] [rotate <N>] [duration <sec>] [ether-host <mac>] [file <path>]`	EXEC	Start per-port capture.
`no capture interface <port>`	EXEC	Stop capture. Alias: clear capture <port>.
`test interface <port> link up|down|flap [count <N> interval <sec>]`	EXEC	Force or flap simulated link state.
`test ethernet interface <port> destination <mac> [vlan <id>] [count <N>]`	EXEC	Send 0x88B5 STRATUM experimental test frames.

Command	Mode	Purpose / notes
`show impairment`	EXEC	Display impairment settings for all ports.
`show impairment interface <port>`	EXEC	Display impairment for one port.
`clear impairment interface <port>`	EXEC	Clear impairment settings.
`show stratum runtime`	EXEC	STRATUM runtime/worker metadata. Alias: show stratum worker.
`show stratum fabric`	EXEC	STRATUM network/fabric attachment view. Aliases: topology, endpoints, networks, vxlan.
`show stratum validation`	EXEC	Local topology/fabric validation. Aliases: diagnose topology, diagnose fabric.
`show stratum endpoint mac <mac>`	EXEC	Locate a MAC through the local FDB.
`trace mac <mac>`	EXEC	Trace/locate a MAC through local forwarding evidence.
`show tech-support`	EXEC	Aggregate comprehensive operational state.

A.5 Global configuration commands

Command	Mode	Purpose / notes
`hostname <name>`	CONFIG	Set switch hostname/prompt.
`mac address-table aging-time <10-86400>`	CONFIG	Set dynamic FDB aging time in seconds.
`mac address-table static <mac> vlan <id> interface <port>`	CONFIG	Install a static FDB entry.
`no mac address-table static <mac> vlan <id>`	CONFIG	Remove matching static FDB entry.
`lldp run / no lldp run`	CONFIG	Enable/disable LLDP globally.
`spanning-tree mode rapid`	CONFIG	Enable common-instance RSTP.
`no spanning-tree`	CONFIG	Disable spanning tree globally.
`ip igmp snooping / no ip igmp snooping`	CONFIG	Enable/disable IPv4 multicast snooping.
`ipv6 mld snooping / no ipv6 mld snooping`	CONFIG	Enable/disable IPv6 multicast snooping.
`errdisable recovery cause bpduguard`	CONFIG	Enable automatic BPDU Guard recovery; no form disables.
`errdisable recovery cause port-security`	CONFIG	Enable automatic port-security recovery; no form disables.
`errdisable recovery interval <30-86400>`	CONFIG	Set automatic recovery interval in seconds.
`vlan <1-4094>`	CONFIG	Create/activate VLAN and enter VLAN mode.
`no vlan <2-4094>`	CONFIG	Remove VLAN definition.
`interface <port>`	CONFIG	Enter interface mode.
`interface range <range>`	CONFIG	Enter interface-range mode; e.g. Ethernet0/1-8,Ethernet0/12.
`default interface <port>`	CONFIG	Reset one interface to switch defaults.
`default interface range <range>`	CONFIG	Reset a set of interfaces.
`monitor session <id> source interface <port> [rx|tx|both]`	CONFIG	Add a SPAN source.
`monitor session <id> destination interface <port> [forwarding]`	CONFIG	Set port SPAN destination; monitor-only unless forwarding is specified.

Command	Mode	Purpose / notes
`monitor session <id> destination pcap <path>`	CONFIG	Set direct-PCAP SPAN destination.
`no monitor session <id>`	CONFIG	Remove a mirror session.
`do <EXEC-command>`	CONFIG	Run an operational command without leaving configuration mode.
`end`	CONFIG	Return to privileged EXEC.
`exit`	CONFIG	Leave current configuration level; from global mode, return to EXEC.

A.6 VLAN configuration commands

Command	Mode	Purpose / notes
`name <text>`	CONFIG-VLAN	Set VLAN display name.
`private-vlan primary`	CONFIG-VLAN	Mark VLAN as a primary private VLAN.
`private-vlan isolated`	CONFIG-VLAN	Mark VLAN as isolated secondary.
`private-vlan community`	CONFIG-VLAN	Mark VLAN as community secondary.
`private-vlan primary <id>`	CONFIG-VLAN	Associate an isolated/community secondary with its primary VLAN.
`exit`	CONFIG-VLAN	Return to global configuration.
`end`	CONFIG-VLAN	Return to EXEC.

A.7 Interface configuration: switching and topology

Command	Mode	Purpose / notes
`description <text>  /  no description`	CONFIG-IF	Set/remove interface description.
`switchport mode access`	CONFIG-IF	Untagged access port.
`switchport access vlan <1-4094>`	CONFIG-IF	Set access VLAN.
`switchport mode trunk`	CONFIG-IF	Enable trunk mode.
`switchport trunk native vlan <1-4094>`	CONFIG-IF	Set native VLAN for ordinary dot1q trunk.
`switchport trunk allowed vlan <list|all|none>`	CONFIG-IF	Replace allowed VLAN set.
`switchport trunk allowed vlan add <list>`	CONFIG-IF	Add VLANs/ranges.
`switchport trunk allowed vlan remove <list>`	CONFIG-IF	Remove VLANs/ranges.
`switchport trunk allowed vlan except <list>`	CONFIG-IF	Allow all except specified VLANs/ranges.
`switchport trunk encapsulation dot1q`	CONFIG-IF	Use ordinary 0x8100 trunk encapsulation.
`switchport trunk encapsulation dot1ad`	CONFIG-IF	Use 0x88a8 provider S-tags; requires S-tag on ingress.
`no switchport trunk encapsulation`	CONFIG-IF	Return trunk encapsulation to dot1q.
`switchport mode qinq`	CONFIG-IF	Customer-edge Q-in-Q mode. Alias: switchport mode dot1q-tunnel.
`switchport qinq service vlan <1-4094>`	CONFIG-IF	Set service S-VLAN for customer edge. dot1q-tunnel alias accepted.

Command	Mode	Purpose / notes
`switchport protected / no switchport protected`	CONFIG-IF	Enable/disable protected-port isolation.
`mac-learning disable / no mac-learning disable`	CONFIG-IF	Disable/enable dynamic MAC learning.
`shutdown / no shutdown`	CONFIG-IF	Administratively down/up; no shutdown also clears err-disable/guard inconsistent state.

A.8 Interface configuration: private VLAN, RSTP, aggregation, security, and impairment

Command	Mode	Purpose / notes
`switchport mode private-vlan host`	CONFIG-IF	Configure private-VLAN host role.
`switchport private-vlan host-association <primary> <secondary>`	CONFIG-IF	Associate host with primary/secondary PVLAN.
`switchport mode private-vlan promiscuous`	CONFIG-IF	Configure promiscuous PVLAN role.
`switchport private-vlan mapping <primary>`	CONFIG-IF	Associate promiscuous port with primary PVLAN.
`spanning-tree portfast / no spanning-tree portfast`	CONFIG-IF	Set/unset RSTP edge behavior.
`spanning-tree bpduguard enable / no spanning-tree bpduguard enable`	CONFIG-IF	Enable/disable BPDU Guard.
`spanning-tree guard root`	CONFIG-IF	Enable Root Guard and disable Loop Guard.
`spanning-tree guard loop`	CONFIG-IF	Enable Loop Guard and disable Root Guard.
`no spanning-tree guard`	CONFIG-IF	Remove root/loop guard and clear inconsistent state.
`spanning-tree cost <1-200000000>`	CONFIG-IF	Set RSTP path cost.
`channel-group <1-64> mode on|active|passive`	CONFIG-IF	Static or LACP channel membership.
`no channel-group`	CONFIG-IF	Remove port from channel.
`storm-control broadcast <0-100000000>`	CONFIG-IF	Broadcast packets-per-second threshold; 0 disables.
`storm-control multicast <0-100000000>`	CONFIG-IF	Multicast packets-per-second threshold; 0 disables.
`storm-control unknown-unicast <0-100000000>`	CONFIG-IF	Unknown-unicast packets-per-second threshold; 0 disables.
`no storm-control broadcast|multicast|unknown-unicast`	CONFIG-IF	Disable selected storm threshold.
`switchport port-security`	CONFIG-IF	Enable port security.
`no switchport port-security`	CONFIG-IF	Disable/reset port security.
`switchport port-security maximum <1-4096>`	CONFIG-IF	Maximum accepted source MAC addresses.
`switchport port-security mac-address sticky`	CONFIG-IF	Enable sticky learning and port security.
`no switchport port-security mac-address sticky`	CONFIG-IF	Disable sticky behavior.
`switchport port-security violation protect|restrict|shutdown`	CONFIG-IF	Set violation action and enable port security.
`impairment delay <0-3600000>`	CONFIG-IF	Delay in milliseconds.
`impairment jitter <0-3600000>`	CONFIG-IF	Jitter in milliseconds.

Command	Mode	Purpose / notes
`impairment loss <0-1000000>`	CONFIG-IF	Loss probability in ppm.
`impairment duplicate <0-1000000>`	CONFIG-IF	Duplicate probability in ppm.
`impairment reorder <0-1000000>`	CONFIG-IF	Reorder probability in ppm.
`impairment corrupt <0-1000000>`	CONFIG-IF	Corruption probability in ppm.
`impairment rate <bps>`	CONFIG-IF	Rate ceiling in bits per second; 0 disables.
`no impairment`	CONFIG-IF	Clear all configured impairment values.
`exit`	CONFIG-IF	Return to global configuration.
`end`	CONFIG-IF	Return to EXEC.

A.9 Output pipeline

Command	Mode	Purpose / notes
`<command> | include <text>`	EXEC	Emit only lines containing text.
`<command> | exclude <text>`	EXEC	Emit lines not containing text.
`<command> | begin <text>`	EXEC	Start output at the first matching line.
`<command> | section <text>`	EXEC	Emit a matching configuration-style section until the next non-indented top-level line.
`<command> | count`	EXEC	Return the number of lines in command output.
`<command> | redirect <relative-path>`	EXEC	Write unfiltered command output under the switch workspace.

Appendix B. Runtime JSON Reference

Runtime schema 3 is generated by STRATUM for normal operation. Administrators typically configure node/template options in STRATUM rather than editing runtime JSON directly.

Field	Meaning
schema	Runtime schema; v0.4.3 uses 3.
name	Initial switch hostname.
node_id	STRATUM node identifier.
session_id	STRATUM session/lab identifier.
worker_host	Assigned worker hostname for distributed execution.
state_dir	Switch workspace containing configuration, events, token, sockets, captures, and markers.
listen	Console bind address.
console_port	Telnet-style CLI TCP port; 0 disables in manual mode.
control_socket	Unix JSON control socket path.
control_listen	TCP control bind address.
control_port	Secondary management/control TCP port.
management_token	Random token required for distributed TCP control.
console_auth	Whether console credentials are required.
console_username	Optional console username.
console_secret	Optional console secret.
events_file	JSONL event path.
mtu	Node link MTU exposed to the switch; distributed fabric may lower the effective link MTU.
mac_age	Dynamic MAC aging time.
queue_limit	Per-port output queue limit in bytes.
lldp	Enable LLDP.
rstp	Enable RSTP.
igmp_snooping	Enable IGMP snooping.
mld_snooping	Enable MLD snooping.
ports[]	Array of TAP-backed port records.

B.1 Port object fields

Field	Meaning
id	Zero-based runtime port identifier.
name	CLI name such as Ethernet0/1.
tap	Worker/controller TAP device name.

Field	Meaning
network_id	STRATUM logical network identifier.
network_name	STRATUM logical network display name.
network_type	bridge, pnetN, natN, cloud, or another resolved network type.
bridge	Expected Linux/OVS bridge.
external_network	True when attachment is an externally managed network type.
peer_node_id	Connected peer node identifier when known.
peer_node	Connected peer name when known.
peer_interface	Connected peer interface identifier/name.
peer_label	Topology/endpoint label or description.


```
{
  "schema": 3,
  "name": "ACCESS-SW1",
  "state_dir": "/stratum/tmp/example-switch",
  "console_port": 20008,
  "control_socket": "/stratum/tmp/example-switch/switch.sock",
  "control_port": 20009,
  "mtu": 8950,
  "mac_age": 300,
  "queue_limit": 4194304,
  "lldp": true,
  "rstp": true,
  "igmp_snooping": true,
  "mld_snooping": true,
  "ports": [
    {"id":0,"name":"Ethernet0/1","tap":"v00100100800","bridge":"vnet001001047"}
  ]
}
```

Appendix C. Control API Reference

command	Purpose
`get_status`	Switch status summary.
`get_interfaces`	Detailed interfaces including topology/backend, VLAN/PVLAN, Q-in-Q, trunk encapsulation/TPID, RSTP/LACP, err-disable, security, impairment, counters, and capture quotas.
`get_vlans`	VLAN inventory.
`get_fdb`	Forwarding database.
`get_stp`	RSTP state.
`get_channels`	Port-channel/LACP state.
`get_multicast`	IGMP/MLD learned state.
`get_mirrors`	SPAN/mirror state.
`get_running_config`	Rendered running configuration.
`clear_fdb`	Clear dynamic FDB state.
`clear_counters`	Clear interface counters.
`clear_multicast`	Clear multicast state.
`start_capture`	Start a safe per-port capture.
`stop_capture`	Stop a per-port capture.
`watch`	Stream events over the JSON connection.
`set_port_attachment`	STRATUM-internal live attachment reconciliation; not a direct browser command.

C.1 Capture request example

```
{
  "command":"start_capture",
  "interface":"Ethernet0/1",
  "direction":"both",
  "path":"/shared/workspace/capture.pcap",
  "max_bytes":524288000,
  "rotate":5,
  "duration":300,
  "filter_mac":"52:54:00:12:34:56"
}
```

C.2 Live attachment reconciliation

set_port_attachment is used by STRATUM when a running switch port is reconnected on the STRATUM mission canvas. The switch compares the requested bridge with the TAP's actual Linux/OVS master, moves the TAP only when necessary, updates in-memory topology metadata, and clears dynamic FDB entries learned on the port. If the requested bridge is absent, the operation fails without detaching the current working bridge.

Appendix D. Defaults and Limits

Parameter	v0.4.3 value
Version	0.4.3
Runtime schema	3
Maximum ports	256
Maximum Ethernet frame buffer	65,536 bytes
VLAN ID range	1-4094
FDB hash buckets	4096; entry capacity is memory-limited
Default MAC aging	300 seconds
Manual-process default MTU	9000 bytes
Supplied STRATUM template MTU	1500 bytes
Manual-process default queue limit	1 MiB per port
STRATUM integration queue default	4 MiB per port
Maximum CLI sessions	8
Maximum JSON control clients	16
CLI history	32 commands
Maximum mirror sessions	4
Maximum port channels	64
Maximum multicast group records	256
LLDP interval / holdtime	30 / 120 seconds
RSTP default bridge priority	32768
RSTP hello / max-age / forward-delay	2 / 20 / 15 seconds
Multicast membership age	260 seconds
Multicast-router age	255 seconds
Default capture max size	500 MiB per file
Default capture rotations	5
Err-disable default recovery interval	300 seconds
Confirmed rollback timer	10-3600 seconds
Impairment probability scale	0-1,000,000 ppm
802.1Q TPID	0x8100
802.1ad TPID	0x88A8
Test-frame EtherType	0x88B5
Default VXLAN UDP destination port	4789 (STRATUM distributed launcher)

Appendix F. Glossary

Term	Definition
Access port	A switch port that maps untagged Ethernet frames to one VLAN and emits frames untagged.
Bridge	A Linux or Open vSwitch Layer-2 object used by STRATUM to attach TAPs to a logical network.
C-tag	Customer 802.1Q tag, normally TPID 0x8100, preserved inside a Q-in-Q service frame.
DUT	Device under test; often a VM or virtual network appliance in a STRATUM test bay.
FDB	Forwarding database that maps VLAN/MAC pairs to switch ports.
LLDP	Link Layer Discovery Protocol.
MLD	Multicast Listener Discovery for IPv6.
Native VLAN	The untagged VLAN on an ordinary 802.1Q trunk.
pnet	STRATUM external physical-network object backed by an existing host bridge/uplink.
Port channel	A logical aggregation of multiple physical/virtual switch ports.
PVLAN	Private VLAN, providing primary/secondary isolation semantics.
Q-in-Q	Provider bridging that adds an outer service VLAN tag around customer Ethernet/VLAN traffic.
RSTP	Rapid Spanning Tree Protocol, used to avoid Layer-2 loops.
S-tag	Provider service tag, TPID 0x88a8 in STRATUM Switch dot1ad mode.
SPAN	Port mirroring for traffic observation or packet capture.
TAP	Linux virtual network interface presented as a file descriptor to a userspace process.
Trunk	A port carrying multiple VLANs, normally using 802.1Q tags.
VNI	VXLAN Network Identifier used by STRATUM's distributed logical-network substrate.
VTEP	VXLAN tunnel endpoint. In STRATUM's distributed substrate, the worker kernel normally provides the VTEP.
VXLAN	Layer-2-over-UDP overlay used by STRATUM to extend ordinary logical networks across workers when enabled.

END OF GUIDE