

WOLEX / NETWORK FIELD REFERENCE

Cisco switches | Troubleshooting

Catalyst / IOS XE 17.x | Revision 1.0 | Reviewed 2026-10-10

IOS XE EXEC commands. Feature support and interface names vary. IOS XR, NX-OS and Meraki are outside this sheet.

Read-only inspection unless labeled otherwise. Replace every example address, interface and <PLACEHOLDER>. Confirm syntax with device help for your release.

Port down or intermittent

Read-only inspection

```
show interfaces status
show interfaces GigabitEthernet1/0/1
```

Inspect: Compare link state, speed/duplex and rising error counters. A single cumulative CRC count does not prove an active fault.

Next: Take two timestamped samples; inspect both ends and the physical path before changing speed or bouncing the port.

Interface is an example; replace it. Cable diagnostics can affect service and are not part of this read-only block.

Link up, wrong VLAN or no gateway

Read-only inspection

```
show interfaces GigabitEthernet1/0/1 switchport
show interfaces trunk
```

Inspect: Compare access/native VLAN and allowed/active VLANs along the uplink path.

Next: Check the same VLAN at the far end, then its gateway and the endpoint IP settings.

Do not assume trunk means every VLAN is forwarded.

Redundant link not forwarding

Read-only inspection

```
show spanning-tree vlan 30
show etherchannel summary
```

Inspect: Identify the root, forwarding/blocking roles and bundled versus individual members.

Next: Check VLAN and LACP settings on the peer; determine whether STP blocking is expected.

VLAN 30 is illustrative. Do not disable STP or force channel mode to hide a mismatch.

WOLEX / NETWORK FIELD REFERENCE

Cisco switches | Deployment

Catalyst / IOS XE 17.x | Revision 1.0 | Reviewed 2026-10-10

IOS XE EXEC commands. Feature support and interface names vary. IOS XR, NX-OS and Meraki are outside this sheet.

Cutover acceptance

Read-only inspection

```
show interfaces status
show interfaces trunk
show etherchannel summary
```

Inspect: Compare uplink state, VLAN carriage and bundle members with the saved baseline.

Next: Test management from a separate path and one real application per affected VLAN before saving the accepted running configuration.

Pre-stage interface mapping, console access and a tested backup/recovery method. A syntax-valid configuration is not proof of working service.

Change acceptance checklist

Before: approved scope, baseline, compatible software/optics, protected backup, console access and recovery owner.

After: compare links, VLANs, peers and routes; test management from a separate path, real application traffic, intended denies and redundancy. Record evidence and time.

Close: save or confirm the accepted configuration, update documentation and retain the reviewed recovery path.

Vendor references

[Cisco Catalyst port status](#)[Cisco IOS XE switching command reference](#)[Cisco configuration replacement](#)

Not executed on customer equipment. Documentation-reviewed examples; platform features and syntax vary. No login, config upload or device connection.

Live reference: wolex.net/tools/network-cheat-sheets/

Deployment and migration help from Wolex | [Network security review](#)

WOLEX / NETWORK FIELD REFERENCE

Cisco routers | Troubleshooting

IOS XE 17.x / IPv4 | Revision 1.0 | Reviewed 2026-10-10

Default IPv4 routing context. For VRFs, use the matching VRF-aware command syntax; a default-table result does not describe every tenant.

Read-only inspection unless labeled otherwise. Replace every example address, interface and <PLACEHOLDER>. Confirm syntax with device help for your release.

Destination unreachable

Read-only inspection

```
show ip route 192.0.2.10
show ip cef 192.0.2.10
```

Inspect: Compare the selected route with the forwarding entry, resolved next hop and outgoing interface.

Next: Verify next-hop reachability and the destination-side return route in the same routing context.

192.0.2.10 is a documentation address; replace it. CEF output alone does not prove hardware forwarding or firewall permission.

BGP established, missing reachability

Read-only inspection

```
show ip bgp summary
show ip bgp 192.0.2.0
```

Inspect: Distinguish neighbor state from received prefixes and selected paths. A numeric prefix count indicates an established session.

Next: Check address family and import/export policy; confirm that the selected prefix is actually installed in the IP routing table.

A healthy TCP/BGP session does not guarantee the needed prefix is accepted or advertised.

One source works, another fails

Read-only inspection

```
show ip cef exact-route 198.51.100.10 192.0.2.10
```

Inspect: Identify the forwarding choice for this source/destination pair.

Next: Compare source networks, routing context, ACL/NAT policy and return path; reproduce the failing application tuple.

Documentation addresses; replace both. Policy-based routing can alter the path. This is not a complete PBR or security-policy evaluation.

WOLEX / NETWORK FIELD REFERENCE

Cisco routers | Deployment

IOS XE 17.x / IPv4 | Revision 1.0 | Reviewed 2026-10-10

Default IPv4 routing context. For VRFs, use the matching VRF-aware command syntax; a default-table result does not describe every tenant.

Route-change acceptance

Read-only inspection

```
show ip route 192.0.2.10
show ip cef 192.0.2.10
show ip bgp summary
```

Inspect: Compare next hop, forwarding choice and expected peers with the pre-change baseline.**Next:** Verify application traffic from affected source networks; use the reviewed recovery plan if acceptance fails. Save only the accepted configuration.

IOS XE changes normally affect running state immediately. Configuration replacement needs a compatible full backup and platform-specific preparation; do not paste a generic rollback command.

Change acceptance checklist

Before: approved scope, baseline, compatible software/optics, protected backup, console access and recovery owner.**After:** compare links, VLANs, peers and routes; test management from a separate path, real application traffic, intended denies and redundancy. Record evidence and time.**Close:** save or confirm the accepted configuration, update documentation and retain the reviewed recovery path.

Vendor references

[Cisco IP route reference](#)[Cisco CEF reference](#)[Cisco IOS XE BGP reference](#)[Cisco configuration replacement](#)

Not executed on customer equipment. Documentation-reviewed examples; platform features and syntax vary. No login, config upload or device connection.

Live reference: wlex.net/tools/network-cheat-sheets/Deployment and migration help from Wolex | [Network security review](#)

WOLEX / NETWORK FIELD REFERENCE

Juniper switches | Troubleshooting

EX / QFX, Junos OS | Revision 1.0 | Reviewed 2026-10-10

Operational mode unless stated. Confirm ELS versus non-ELS configuration syntax. Virtual Chassis checks apply only to supported VC deployments.

Read-only inspection unless labeled otherwise. Replace every example address, interface and <PLACEHOLDER>. Confirm syntax with device help for your release.

Physical link or logical unit down

Read-only inspection

```
show interfaces terse
show interfaces ge-0/0/1 extensive
```

Inspect: Separate physical Admin/Link state from logical-unit protocol state; compare error-counter deltas.

Next: Inspect the peer and cabling, then verify whether the required logical unit exists and is configured for the intended service.

Replace ge-0/0/1 with the actual member/port. A physical up state does not prove VLAN or L3 reachability.

Client MAC missing or on wrong path

Read-only inspection

```
show ethernet-switching table
show vlans
```

Inspect: Check VLAN membership and where the client MAC is learned.

Next: Generate controlled client traffic; follow the MAC along each hop and then check the gateway ARP/route.

Use EX/QFX switching syntax. MX bridge-domain tables and ELS/non-ELS configuration stanzas differ.

Aggregation or VC member missing

Read-only inspection

```
show lacp interfaces
show virtual-chassis status
show virtual-chassis vc-port all-members
```

Inspect: Check LACP participation, expected member roles and VCP links.

Next: Compare serial/member mapping and peer state with the design; inspect links before attempting a membership change.

Run VC commands only on a supported Virtual Chassis. Stack changes can affect management and transit traffic.

WOLEX / NETWORK FIELD REFERENCE

Juniper switches | Deployment

EX / QFX, Junos OS | Revision 1.0 | Reviewed 2026-10-10

Operational mode unless stated. Confirm ELS versus non-ELS configuration syntax. Virtual Chassis checks apply only to supported VC deployments.

Validate a switch cutover

Read-only inspection

```
show interfaces terse
show ethernet-switching table
show lacp interfaces
```

Inspect: Compare ports, VLAN learning and expected aggregate participation against the baseline.

Next: Use the Junos change sequence below; test management and affected applications before confirming the timed commit.

Pre-check EX model, release, ELS syntax, member IDs and optics. Do not assume EX3300 configuration stanzas can be copied unchanged to every EX3400 release.

Change acceptance checklist

Before: approved scope, baseline, compatible software/optics, protected backup, console access and recovery owner.

After: compare links, VLANs, peers and routes; test management from a separate path, real application traffic, intended denies and redundancy. Record evidence and time.

Close: save or confirm the accepted configuration, update documentation and retain the reviewed recovery path.

Junos controlled change sequence - changes device state

```
show | compare
commit check
commit confirmed 5 comment "CHG-123 validation window"
run show system commit
commit comment "CHG-123 validated"
```

Configuration mode, after staging only your approved change. Run commit check BEFORE the timed commit; on Junos it can confirm an already-pending confirmed commit. The final commit is issued only after acceptance. Replace CHG-123; track the timer. If validation fails, follow the tested rollback plan or allow the timer to expire. Rollback loads a candidate and requires a commit to activate; choose the correct revision rather than assuming rollback 1 is always your intended state.

Vendor references

[Junos interface status](#)[Junos operational command reference](#)[Junos ELS MAC table](#)[Junos LACP reference](#)[Juniper Virtual Chassis guide](#)[Junos commit and confirmed rollback](#)[Junos configuration management](#)

Not executed on customer equipment. Documentation-reviewed examples; platform features and syntax vary. No login, config upload or device connection.

Live reference: wolex.net/tools/network-cheat-sheets/

Deployment and migration help from Wolex | [Network security review](#)

WOLEX / NETWORK FIELD REFERENCE

Juniper routers | Troubleshooting

MX / ACX, Junos OS | Revision 1.0 | Reviewed 2026-10-10

IPv4 inet.0 examples. Check the correct routing-instance table. This is not an SRX flow-security or Junos OS Evolved configuration guide.

Read-only inspection unless labeled otherwise. Replace every example address, interface and <PLACEHOLDER>. Confirm syntax with device help for your release.

Prefix absent, hidden or inactive

Read-only inspection

```
show route 192.0.2.0/24 detail
show route forwarding-table destination 192.0.2.10
```

Inspect: Separate route selection from the forwarding-table entry and next-hop resolution.

Next: Check the correct routing instance, preference/policy and next-hop reachability; verify a route for the return source.

Examples target inet.0. A route in another table does not automatically provide reachability here.

BGP peer healthy, prefix not passing

Read-only inspection

```
show bgp summary
show route advertising-protocol bgp 198.51.100.1
show route receive-protocol bgp 198.51.100.1
```

Inspect: Compare session state with advertisements and received paths for the actual neighbor.

Next: Inspect policy and active-route eligibility, then test the destination from the actual source network.

Replace the neighbor. Received-route display is not proof that the route is active or forwarded.

Path healthy at IP, application still fails

Read-only inspection

```
show interfaces terse
show interfaces xe-0/0/0 extensive
```

Inspect: Compare interface state, MTU and counter changes on the suspected path.

Next: Test return routing and application-size behavior; for MPLS/VPN environments verify labels and service tables using the release-specific guide.

A small ping can work while larger packets fail. This sheet does not prescribe a universal MTU.

WOLEX / NETWORK FIELD REFERENCE

Juniper routers | Deployment

MX / ACX, Junos OS | Revision 1.0 | Reviewed 2026-10-10

IPv4 inet.0 examples. Check the correct routing-instance table. This is not an SRX flow-security or Junos OS Evolved configuration guide.

Validate a routed migration

Read-only inspection

```
show route 192.0.2.0/24 detail
show bgp summary
show route forwarding-table destination 192.0.2.10
```

Inspect: Compare route activity, peers and next hops against the pre-change baseline.

Next: Use the Junos change sequence below, then verify source-specific application traffic and the reverse path before confirming.

On dual Routing Engines, use the platform-reviewed synchronization method. Do not commit independently on a backup RE as a generic recovery step.

Change acceptance checklist

Before: approved scope, baseline, compatible software/optics, protected backup, console access and recovery owner.

After: compare links, VLANs, peers and routes; test management from a separate path, real application traffic, intended denies and redundancy. Record evidence and time.

Close: save or confirm the accepted configuration, update documentation and retain the reviewed recovery path.

Junos controlled change sequence - changes device state

```
show | compare
commit check
commit confirmed 5 comment "CHG-123 validation window"
run show system commit
commit comment "CHG-123 validated"
```

Configuration mode, after staging only your approved change. Run commit check BEFORE the timed commit; on Junos it can confirm an already-pending confirmed commit. The final commit is issued only after acceptance. Replace CHG-123; track the timer. If validation fails, follow the tested rollback plan or allow the timer to expire. Rollback loads a candidate and requires a commit to activate; choose the correct revision rather than assuming rollback 1 is always your intended state.

Vendor references

[Juniper BGP troubleshooting](#)[Junos interface status](#)[Junos operational command reference](#)[Junos commit and confirmed rollback](#)[Junos configuration management](#)

Not executed on customer equipment. Documentation-reviewed examples; platform features and syntax vary. No login, config upload or device connection.

Live reference: wolex.net/tools/network-cheat-sheets/Deployment and migration help from Wolex | [Network security review](#)

WOLEX / NETWORK FIELD REFERENCE

Palo Alto firewalls | Troubleshooting

PAN-OS 11.2 / NGFW | Revision 1.0 | Reviewed 2026-10-10

Operational mode examples; select the correct vsys and virtual router. Legacy routing-engine commands are not interchangeable with Advanced Routing Engine commands. Panorama push scope also matters.

Read-only inspection unless labeled otherwise. Replace every example address, interface and <PLACEHOLDER>. Confirm syntax with device help for your release.

Find the real application session

Read-only inspection

```
show session all filter source 198.51.100.10 destination 192.0.2.10
show session id <SESSION_ID>
```

Inspect: Inspect both flow directions, rule, zones, application, translations and byte counters.

Next: Compare the original and translated tuple with traffic logs and the return route during a fresh, controlled attempt.

Replace the addresses and session ID. No matching session is not by itself proof of a firewall deny.

Which security rule would match?

Read-only inspection

```
test security-policy-match from <SOURCE_ZONE> to <DEST_ZONE> source 198.51.100.10 destination
192.0.2.10 destination-port 443 protocol 6
```

Inspect: Compare the matched rule with the intended zones, addresses, protocol and port.

Next: Add the actual application/user context where needed; validate the real session and traffic log after a controlled attempt.

Policy simulation is not end-to-end traffic proof. NAT, PBF, App-ID, User-ID, decryption and existing sessions can change what you observe.

VPN up, no useful traffic

Read-only inspection

```
show vpn ike-sa
show vpn ipsec-sa
show vpn flow
```

Inspect: Separate IKE state, IPsec state and traffic/counter movement.

Next: Verify selectors/proxy IDs, tunnel routing, policy/NAT and return routes; test the actual application from both sides.

An established tunnel does not prove that a subnet or application is permitted through it.

Confirm the selected route

Read-only inspection

```
test routing fib-lookup ip 192.0.2.10 virtual-router <VR_NAME>
```

Inspect: Identify the route/egress selected by the specified legacy virtual router.

Next: Check PBF and session egress, then the reverse path. For Advanced Routing Engine deployments use its logical-router command reference.

Use the correct vsys/VR. The legacy and advanced routing command sets differ.

WOLEX / NETWORK FIELD REFERENCE

Palo Alto firewalls | Deployment

PAN-OS 11.2 / NGFW | Revision 1.0 | Reviewed 2026-10-10

Operational mode examples; select the correct vsys and virtual router. Legacy routing-engine commands are not interchangeable with Advanced Routing Engine commands. Panorama push scope also matters.

Review and validate a firewall change

Read-only inspection

```
show config diff
show jobs all
show high-availability state
```

Inspect: Review candidate/running differences, commit job outcome and HA state.

Next: Validate and review scope before commit; after commit, check logs and new sessions for intended allows and intended denies. For Panorama, verify the push job and target device.

Export a protected configuration backup and document the recovery procedure first. A successful commit does not prove that the application works. These commands do not perform a commit or HA failover.

Change acceptance checklist

Before: approved scope, baseline, compatible software/optics, protected backup, console access and recovery owner.

After: compare links, VLANs, peers and routes; test management from a separate path, real application traffic, intended denies and redundancy. Record evidence and time.

Close: save or confirm the accepted configuration, update documentation and retain the reviewed recovery path.

Vendor references

[PAN-OS session interpretation](#)[PAN-OS policy tests](#)[PAN-OS networking reference](#)[PAN-OS 11.2 operational CLI](#)

Not executed on customer equipment. Documentation-reviewed examples; platform features and syntax vary. No login, config upload or device connection.

Live reference: wlex.net/tools/network-cheat-sheets/

Deployment and migration help from Wolex | [Network security review](#)

WOLEX / NETWORK FIELD REFERENCE

Cross-vendor field checks | Troubleshooting

Application flow / deployment | Revision 1.0 | Reviewed 2026-10-10

Engineer-authored workflow. Record exact endpoints, protocol, ports, time and routing context; verify every direction independently.

Read-only inspection unless labeled otherwise. Replace every example address, interface and <PLACEHOLDER>. Confirm syntax with device help for your release.

Trace a failed application flow

Read-only inspection

Inspect: Write source, destination, TCP/UDP port, time, source VLAN/VRF and expected path. Separate DNS resolution from reachability.

Next: Check link -> VLAN/MAC -> gateway/ARP -> route -> policy/NAT -> session -> reverse path. Keep the failing tuple unchanged between tests.

Engineer-authored method. Do not substitute a device management ping for the affected client application test.

Small ping works, transfer stalls

Workflow / scoped active test

Inspect: Compare packet sizes, path MTU, tunnel overhead and whether required ICMP feedback is permitted.

Next: Use a scoped, rate-limited size test in both directions with platform-appropriate DF options; correlate counters or an approved filtered capture.

Active probes generate traffic. Do not guess a universal MTU or enable an unrestricted production capture.

Build a useful escalation handoff

Read-only inspection

Inspect: Collect model/release, timestamp/timzone, topology, affected tuple, counter deltas and relevant sanitized outputs.

Next: State what works, what fails, the last change and which hop is supported by evidence. Record the owner and next validation step.

Remove secrets and unnecessary customer identifiers. Full support bundles can be large and sensitive; gather deliberately.

WOLEX / NETWORK FIELD REFERENCE

Cross-vendor field checks | Deployment

Application flow / deployment | Revision 1.0 | Reviewed 2026-10-10

Engineer-authored workflow. Record exact endpoints, protocol, ports, time and routing context; verify every direction independently.

Before / during / after deployment

Change planning

Inspect: Before: record ports, optics, VLANs, peers, routes, management path, version compatibility and an approved backup. Define acceptance and rollback triggers.

Next: During: make one reviewed change, track timing and preserve console access. **After:** test management plus real services, intended denies, redundancy and monitoring; compare with baseline.

Close only after acceptance, saved/confirmed configuration and updated documentation. A reachable CLI is not full deployment acceptance.

Change acceptance checklist

Before: approved scope, baseline, compatible software/optics, protected backup, console access and recovery owner.

After: compare links, VLANs, peers and routes; test management from a separate path, real application traffic, intended denies and redundancy. Record evidence and time.

Close: save or confirm the accepted configuration, update documentation and retain the reviewed recovery path.

Not executed on customer equipment. Documentation-reviewed examples; platform features and syntax vary. No login, config upload or device connection.

Live reference: wolex.net/tools/network-cheat-sheets/

Deployment and migration help from Wolex | [Network security review](#)