

FUNDAMENTALS | REV 2.0 | REVIEWED 2026-10-10

IPv4 subnetting & address planning

01 / Quick reference and concepts

Calculate boundaries, size a subnet and identify address-plan mistakes before touching a device.

IPv4 CIDR. Host counts below assume ordinary broadcast subnets except the explicitly labeled /31 and /32 cases.



Worked example: 192.0.2.77/27 belongs to 192.0.2.64/27. Usable ordinary host addresses are .65 through .94.

Prefix	Mask	Addresses	Ordinary hosts
/24	255.255.255.0	256	254
/25	255.255.255.128	128	126
/26	255.255.255.192	64	62
/27	255.255.255.224	32	30
/28	255.255.255.240	16	14
/29	255.255.255.248	8	6
/30	255.255.255.252	4	2
/31	255.255.255.254	2	2 on P2P
/32	255.255.255.255	1	Single address

What to understand first

- Address count is $2^{(32 - \text{prefix length})}$. For ordinary broadcast subnets, subtract the network and broadcast addresses. /31 point-to-point links and /32 host routes have different semantics.
- Find the boundary by applying the mask to the address. In the changing octet, block size is 256 minus the mask value. Round down to a multiple of that size; carry across octets when required.
- Use variable-length subnetting by allocating the largest requirements first. Include growth, infrastructure and reserved addresses; track every allocation to prevent overlap.
- A summary must cover the intended component networks and be aligned to its prefix boundary. A larger summary can accidentally attract traffic for space you do not own.

FUNDAMENTALS | REV 2.0 | REVIEWED 2026-10-10

IPv4 subnetting & address planning

02 / Commands and worked example

Replace documentation addresses, example interfaces and every <PLACEHOLDER>. Check command help for your model/release and routing context. Examples are documentation-reviewed, not executed on customer equipment.

Cisco IOS XE

Read-only EXEC

```
show ip interface brief
show ip route 192.0.2.77
show ip arp
```

Inspect: Compare the actual mask, selected route and next-hop resolution. A default route can hide a missing more-specific route.

Junos

Read-only operational

```
show interfaces terse
show route 192.0.2.77 detail
show arp no-resolve
```

Inspect: Confirm the correct routing-instance table and interface address. A neighbor entry does not prove an application is reachable.

Worked boundary calculation

Illustrative teaching example, not captured device output.

```
Address: 192.0.2.77/27
Mask:    255.255.255.224
Block:   32 addresses
Network: 192.0.2.64
Hosts:   192.0.2.65 - 192.0.2.94
Bcast:   192.0.2.95
```

- 77 falls between the aligned boundaries 64 and 96. The last address before 96 is the broadcast address.
- A gateway chosen as .65 leaves 29 other ordinary host addresses; reservations reduce the usable pool further.

FUNDAMENTALS | REV 2.0 | REVIEWED 2026-10-10

IPv4 subnetting & address planning

03 / Troubleshooting and acceptance

1. Write the client address, mask and gateway exactly as configured; compare them with IPAM rather than trusting a diagram.
2. Calculate the client and gateway subnet boundaries independently. Check duplicate addresses and DHCP scope options.
3. If the destination is on-link, inspect ARP and VLAN carriage. If off-link, inspect gateway reachability and routing.
4. Check the return route from the destination context. Overlapping private networks can make VPN routing ambiguous.
5. Validate the real application from the affected client after correcting the address plan.

Common mistakes

- Applying the $2^n - 2$ rule to a /31 point-to-point link.
- Choosing a broadcast address as a host or assuming the first address is always the gateway.
- Treating a successful gateway ping as proof of correct DHCP, DNS or return routing.

Acceptance checks

- No overlapping allocations; gateway and client masks agree.
- DHCP exclusions, static reservations and documentation match.
- Forward and reverse application paths pass from each affected subnet.

Primary references

[Cisco IPv4 addressing](#)[RFC 3021: IPv4 /31 point-to-point links](#)

Original Wolex diagrams, scenarios and troubleshooting sequences. Vendor names identify platform scope; no affiliation is implied.

[Read the full web guide and supporting references](#)[Deployment and migration help](#) | [Network security review from Wolex](#)

FUNDAMENTALS | REV 2.0 | REVIEWED 2026-10-10

IPv6 addressing & neighbor discovery

01 / Quick reference and concepts

Read IPv6 prefixes and troubleshoot link-local neighbors, router advertisements and dual-stack failures.

IPv6 unicast and Neighbor Discovery. CLI examples target IOS XE and Junos operational modes; routing-instance and platform options vary.



Neighbor Discovery resolves local neighbors. Router advertisements can supply the default router; a DHCPv6 lease alone does not prove one exists.

Item	Meaning	Example / note
Global unicast	Globally scoped address	2001:db8::/32 is documentation only
Link-local	Valid on the local link	fe80::/10; identify the interface
Loopback	This host	::1/128
Unspecified	No assigned address	::/128
Multicast	Group delivery	ff00::/8; no IPv6 broadcast
LAN prefix	Common SLAAC design	/64; not every link must be /64

What to understand first

- IPv6 has 128 bits, usually written as eight hexadecimal groups. Leading zeros may be omitted; one run of zero groups can be compressed with ::. Canonical text uses lowercase and the longest eligible run.
- The prefix length identifies network bits. A /48 allocation contains 65,536 /64 prefixes. 2001:db8:1200:30::/64 and 2001:db8:1200:31::/64 are separate LANs.
- ICMPv6 supports Neighbor Discovery and path-MTU feedback. IPv4-style blanket ICMP blocking can break IPv6 even when addresses and routes look correct.
- Duplicate Address Detection, neighbor reachability, RA flags and address lifetimes are separate checks. Dual-stack applications may choose IPv6 even while IPv4 tests pass.

FUNDAMENTALS | REV 2.0 | REVIEWED 2026-10-10

IPv6 addressing & neighbor discovery

02 / Commands and worked example

Replace documentation addresses, example interfaces and every <PLACEHOLDER>. Check command help for your model/release and routing context. Examples are documentation-reviewed, not executed on customer equipment.

Cisco IOS XE

Read-only EXEC

```
show ipv6 interface brief
show ipv6 neighbors
show ipv6 route
```

Inspect: Check address state, neighbor status and default route; inspect the specific interface for RA settings.

Junos

Read-only operational

```
show interfaces terse
show ipv6 neighbors
show route table inet6.0
```

Inspect: inet6.0 is the default IPv6 table. Use the appropriate instance table for tenant traffic.

Illustrative dual-stack failure

Illustrative teaching example, not captured device output.

```
Client: 2001:db8:1200:30::25/64
Neighbor: fe80::1 on the client link
IPv4 application: works
IPv6 default route: absent
```

- The neighbor can resolve locally while the remote application still has no route. Check the RA/default-router path.
- These are teaching observations, not captured device output. Do not infer a default route from an assigned address.

FUNDAMENTALS | REV 2.0 | REVIEWED 2026-10-10

IPv6 addressing & neighbor discovery

03 / Troubleshooting and acceptance

1. Confirm whether the failing attempt used IPv4 or IPv6; check DNS A and AAAA answers.
2. Check address validity and DAD status, then the intended /64 and VLAN.
3. Inspect the link-local neighbor on the correct interface and whether an RA supplies a usable router.
4. Check the destination prefix and reverse route in the correct IPv6 table.
5. If small traffic works but transfers stall, review ICMPv6 Packet Too Big delivery and tunnel MTU.

Common mistakes

- Using multiple :: compressions in one address.
- Treating a link-local address as unique without its link/interface context.
- Assuming IPv4 firewall rules, DNS results or tests also validate IPv6.

Acceptance checks

- Both address families pass the intended application tests.
- ND/RA behavior matches design and unwanted RAs are controlled.
- Path-MTU feedback works and address lifetimes are documented.

Primary references

[RFC 4291: IPv6 addressing](#)[RFC 5952: IPv6 text representation](#)[RFC 4861: Neighbor Discovery](#)[Junos IPv6 neighbor inspection](#)

Original Wolex diagrams, scenarios and troubleshooting sequences. Vendor names identify platform scope; no affiliation is implied.

[Read the full web guide and supporting references](#)

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

SWITCHING | REV 2.0 | REVIEWED 2026-10-10

VLANs, trunks & MAC learning

01 / Quick reference and concepts

Follow one endpoint VLAN across access ports, trunks and the gateway without confusing link state with forwarding.

Cisco Catalyst IOS XE and Juniper EX/QFX. Junos configuration differs between ELS and non-ELS; this guide uses inspection commands.



Verify the same VLAN at every hop. A physical uplink can be up while VLAN 30 is absent or blocked.

Check	Access port	Trunk / uplink
VLAN identity	Assigned access VLAN	Allowed, active and forwarding VLAN
Tagging	Usually untagged endpoint	802.1Q; native handling must match
MAC learning	Client on expected port	Client follows expected uplink
Gateway	Client resolves its gateway	Gateway interface and return path

What to understand first

- A VLAN is a Layer 2 broadcast domain. Access and trunk describe interface behavior; routing between VLANs requires an L3 gateway and the relevant policy.
- A trunk has several distinct tests: negotiated/configured mode, VLAN permission, VLAN existence and spanning-tree forwarding. Passing the first does not prove the others.
- Native VLAN and untagged handling must match the design on both ends. Junos native-vlan-id and interface-mode placement depend on model and configuration style.
- MAC tables learn source addresses from traffic and age entries out. An absent MAC can mean an idle endpoint, wrong VLAN or missing frames, rather than a broken switch.

SWITCHING | REV 2.0 | REVIEWED 2026-10-10

VLANs, trunks & MAC learning

02 / Commands and worked example

Replace documentation addresses, example interfaces and every <PLACEHOLDER>. Check command help for your model/release and routing context. Examples are documentation-reviewed, not executed on customer equipment.

Cisco IOS XE

Read-only EXEC

```
show interfaces GigabitEthernet1/0/1 switchport
show interfaces trunk
show mac address-table vlan 30
show spanning-tree vlan 30
```

Inspect: Follow VLAN 30 through allowed, active and forwarding lists; trace the client MAC.

Junos EX/QFX

Read-only operational

```
show ethernet-switching interfaces
show vlans
show ethernet-switching table
show spanning-tree interface
```

Inspect: Compare VLAN membership, learned MAC location and STP state. Output details vary by release.

Illustrative trunk evidence

Illustrative teaching example, not captured device output.

```
Uplink state: up
Configured allowed VLANs: 10,20,30
Active VLANs:           10,20
Client VLAN:             30
```

- VLAN 30 is permitted but not active in this simplified example. Check VLAN existence and the intended configuration on both switches.
- Do not overwrite the whole allowed-VLAN list to repair one entry; review the approved change and existing traffic first.

SWITCHING | REV 2.0 | REVIEWED 2026-10-10

VLANs, trunks & MAC learning

03 / Troubleshooting and acceptance

1. Record endpoint MAC, VLAN, port and gateway; generate one controlled application attempt.
2. Verify access VLAN and physical errors at the endpoint port.
3. Follow the MAC and VLAN hop by hop, checking trunk permission and STP forwarding at both ends.
4. Once the gateway is reached, move to ARP, routing and firewall/session checks.
5. Retest another VLAN sharing the uplink to detect unintended impact.

Common mistakes

- Equating trunk status with carriage of every VLAN.
- Copying ELS stanzas directly into a non-ELS switch or vice versa.
- Changing native VLANs on one end or replacing an allowed list blindly.

Acceptance checks

- Expected VLANs traverse the uplink and unintended VLANs do not.
- MACs learn on the expected paths without unexplained movement.
- Gateway and real client applications pass on each affected VLAN.

Primary references

[Cisco IOS XE VLAN trunks](#)[Junos ELS MAC table](#)[Junos spanning-tree monitoring](#)

Original Wolex diagrams, scenarios and troubleshooting sequences. Vendor names identify platform scope; no affiliation is implied.

[Read the full web guide and supporting references](#)[Deployment and migration help](#) | [Network security review from Wolex](#)

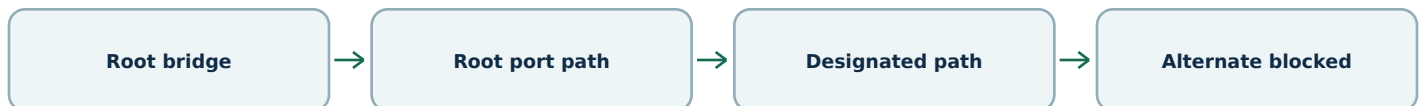
SWITCHING | REV 2.0 | REVIEWED 2026-10-10

STP, RSTP & MST field reference

01 / Quick reference and concepts

Interpret root election and port roles, distinguish expected blocking from a fault and check MST boundaries.

Layer 2 STP variants on Catalyst IOS XE and Junos. Per-VLAN, common-tree and MST interoperability must be designed explicitly.



This is a role-reading sequence, not a physical topology. Each non-root bridge selects a root port; alternate paths can be intentionally non-forwarding.

Item	Interpretation	Operational check
Root election	Lowest bridge ID wins	Priority plus system-ID extension / MAC
Root port	Best path toward root	Compare cost and tie-breakers
Designated	Selected port for segment	Normally forwards when converged
Alternate	Other path to root	Discarding can be healthy
RSTP states	Discarding / learning / forwarding	Role and state are different
Classic timers	Hello 2s / max age 20s / delay 15s	Defaults, not a convergence guarantee
MST region	Name, revision, VLAN mapping	Must agree for same region

What to understand first

- Root placement should follow the intended traffic design. An accidental low bridge priority can move the root and redirect traffic without a physical link failure.
- Classic STP uses blocking, listening, learning and forwarding states; RSTP combines non-forwarding states as discarding and uses rapid transition mechanisms where applicable.
- Edge/PortFast settings are for intended endpoint edges. BPDU Guard and root protection serve different purposes; investigate their trigger before restoring a port.
- MST maps VLANs into instances. A mismatch in name, revision or mapping creates a region boundary even when the cables and VLAN lists match.

SWITCHING | REV 2.0 | REVIEWED 2026-10-10

STP, RSTP & MST field reference

02 / Commands and worked example

Replace documentation addresses, example interfaces and every <PLACEHOLDER>. Check command help for your model/release and routing context. Examples are documentation-reviewed, not executed on customer equipment.

Cisco IOS XE

Read-only EXEC

```
show spanning-tree summary
show spanning-tree vlan 30
show spanning-tree inconsistentports
show spanning-tree mst configuration
```

Inspect: Check root identity, role/state, inconsistent ports and the actual MST mapping.

Junos

Read-only operational

```
show spanning-tree bridge
show spanning-tree interface
```

Inspect: Inspect root ID, root port, costs and role/state. Match the output to RSTP, MSTP or VSTP in use.

Illustrative role/state observations

Illustrative teaching example, not captured device output.

```
Root ID: distribution switch A
Uplink 1: Root / Forwarding
Uplink 2: Alternate / Discarding
Root changes during incident: 0
```

- A non-forwarding alternate can be correct loop prevention. Confirm the topology before trying to make both uplinks forward.
- If the expected root changes repeatedly, investigate BPDUs, link instability and unauthorized switches.

SWITCHING | REV 2.0 | REVIEWED 2026-10-10

STP, RSTP & MST field reference

03 / Troubleshooting and acceptance

1. Identify the intended and actual root for the affected VLAN/instance.
2. Compare roles and states on both ends of the suspected segment.
3. Review topology changes, error counters and protection-triggered ports with timestamps.
4. For MST, compare region parameters and VLAN-to-instance mappings exactly.
5. Use a planned redundancy test; verify reconvergence and application recovery before closing.

Common mistakes

- Disabling STP to make a blocked link pass traffic.
- Applying edge settings to an inter-switch link without the intended design.
- Assuming all vendors run an identical per-VLAN tree by default.

Acceptance checks

- Actual roots and region boundaries match the design.
- No unexplained inconsistent ports or sustained topology-change bursts.
- Approved link-failure test meets the application recovery target.

Primary references

[Cisco IOS XE spanning tree](#)[Junos spanning-tree monitoring](#)[Junos show spanning-tree bridge](#)

Original Wolex diagrams, scenarios and troubleshooting sequences. Vendor names identify platform scope; no affiliation is implied.

[Read the full web guide and supporting references](#)[Deployment and migration help](#) | [Network security review from Wolex](#)

SWITCHING | REV 2.0 | REVIEWED 2026-10-10

LACP & port-channel troubleshooting

01 / Quick reference and concepts

Check whether links are actually participating in a bundle and explain why a single flow does not use its total capacity.

IEEE LACP on Catalyst IOS XE and Junos ae interfaces. Static channels, multi-chassis features and vendor flags have separate semantics.



LACP decides participation. The forwarding hash chooses a member for a flow; two 10G members do not guarantee 20G for one transfer.

Item	Meaning	Check
Active / passive	At least one active peer initiates	Passive + passive does not initiate
Actor / partner	Local and peer negotiation state	Correct peer system and key
Collecting / distributing	Member eligible to receive/send	Not just physical link up
Logical interface	Port-channel or ae	VLANs, MTU and L3 config
Minimum links	Threshold for bundle operation	Design versus surviving members
Hashing	Flow-to-member selection	Distribution across multiple flows

What to understand first

- Treat the aggregate as one logical forwarding interface. Confirm member compatibility and the logical interface configuration rather than only comparing physical status.
- Negotiated LACP and a forced static channel are different mechanisms. Mixing them can leave individual links or create an unsafe forwarding topology.
- Cisco summary flags must be read against the legend in that output. Junos actor/partner state and collecting/distributing indicate negotiation and participation.
- A surviving member may satisfy link state but fail a capacity or minimum-links requirement. Monitor both health and the service acceptance threshold.

SWITCHING | REV 2.0 | REVIEWED 2026-10-10

LACP & port-channel troubleshooting

02 / Commands and worked example

Replace documentation addresses, example interfaces and every <PLACEHOLDER>. Check command help for your model/release and routing context. Examples are documentation-reviewed, not executed on customer equipment.

Cisco IOS XE

Read-only EXEC

```
show etherchannel summary
show lacp neighbor
show interfaces port-channel 1
show interfaces trunk
```

Inspect: Verify bundled member flags, the expected peer, logical errors and carried VLANs.

Junos

Read-only operational

```
show lacp interfaces
show interfaces ae0 extensive
show interfaces terse
```

Inspect: Check actor/partner synchronization and eligible members; compare ae0 counters with physical members.

Illustrative bundle evidence

Illustrative teaching example, not captured device output.

```
Expected members: 2 x 10G
Member A: collecting / distributing
Member B: link up, not synchronized
Logical bundle: up on Member A
```

- Service may remain reachable while redundancy and capacity are degraded. Inspect partner state on Member B.
- This is a normalized teaching example; vendor output names and flags differ.

SWITCHING | REV 2.0 | REVIEWED 2026-10-10

LACP & port-channel troubleshooting

03 / Troubleshooting and acceptance

1. Check the actual cabling and peer system on every member.
2. Compare LACP mode, system/key information and compatible link settings at both ends.
3. Verify member participation, logical VLAN/L3 configuration and minimum-links behavior.
4. Compare timed error samples; run multiple representative flows for a capacity test.
5. Perform only an approved member-loss test and observe application continuity.

Common mistakes

- Forcing channel mode to conceal a negotiation mismatch.
- Expecting a single TCP flow to fill every member.
- Declaring success because the logical interface remains up with a missing member.

Acceptance checks

- All planned members participate with the correct peer.
- Logical VLANs, MTU and routing match the intended service.
- Member-loss behavior and available capacity meet acceptance criteria.

Primary references

[Cisco IOS XE EtherChannels](#)[Junos LACP inspection](#)[Cisco IOS XE VLAN trunks](#)

Original Wolex diagrams, scenarios and troubleshooting sequences. Vendor names identify platform scope; no affiliation is implied.

[Read the full web guide and supporting references](#)

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

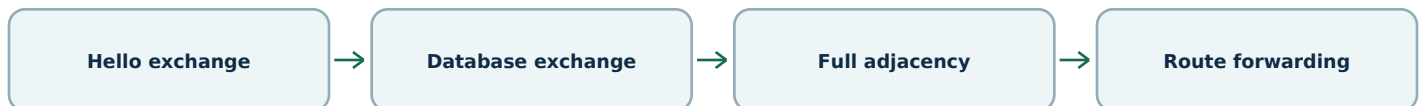
ROUTING | REV 2.0 | REVIEWED 2026-10-10

OSPF neighbors, routes & failure states

01 / Quick reference and concepts

Use neighbor state to narrow the fault, then verify the intended prefix reaches the routing and forwarding tables.

OSPFv2 IPv4 examples, Cisco IOS XE and Junos. OSPFv3, NBMA, virtual links and vendor-specific defaults need their own scope.



An adjacency becoming Full validates database synchronization with that neighbor; it does not prove an application path.

State / item	Meaning	First check
Down / Init	No usable bidirectional hello exchange	Link, area, timers, filtering
2-Way	Bidirectional hellos	Can be normal between DROTHERs
ExStart / Exchange	Database negotiation / exchange	MTU, IDs, packet loss
Loading	Missing LSAs being requested	Loss and retransmission evidence
Full	Database synchronization complete	Then inspect prefix and next hop
IP protocol 89	OSPF transport	Not TCP/UDP port 89
224.0.0.5 / .6	AllSPFRouters / AllDRouters	Link-local multicast roles

What to understand first

- Area, authentication, compatible hello/dead timers and link/network-type assumptions must agree where required. On ordinary broadcast links, DR/BDR behavior determines which pairs become fully adjacent.
- A persistent 2-Way state is not automatically a fault. Two DROTHER routers on a broadcast network normally do not form Full adjacency with each other.
- Persistent ExStart/Exchange can indicate an MTU mismatch or exchange problem. Compare interface MTU and database-description evidence instead of bypassing MTU checks immediately.
- OSPF cost influences path selection. An LSA in the database, an OSPF-selected route, an installed RIB entry and a resolved forwarding next hop are distinct evidence.

ROUTING | REV 2.0 | REVIEWED 2026-10-10

OSPF neighbors, routes & failure states

02 / Commands and worked example

Replace documentation addresses, example interfaces and every <PLACEHOLDER>. Check command help for your model/release and routing context. Examples are documentation-reviewed, not executed on customer equipment.

Cisco IOS XE

Read-only EXEC

```
show ip ospf neighbor
show ip ospf interface
show ip ospf database
show ip route 192.0.2.10
```

Inspect: Match neighbor state to link type, then check the destination route and outgoing path.

Junos

Read-only operational

```
show ospf neighbor
show ospf interface detail
show ospf database
show route 192.0.2.0/24 detail
```

Inspect: Use the correct routing instance and inspect protocol preference and resolved next hop.

Illustrative adjacency failure

Illustrative teaching example, not captured device output.

```
Peer state: ExStart for several minutes
Local interface MTU: 1500
Peer interface MTU: 9000
Affected link: routed Ethernet
```

- The mismatch is a strong lead, not the only possible cause. Confirm exchange evidence and the intended MTU end to end.
- An approved correction should align the design; do not blindly enable an MTU-ignore workaround.

ROUTING | REV 2.0 | REVIEWED 2026-10-10

OSPF neighbors, routes & failure states

03 / Troubleshooting and acceptance

1. Verify interface state, local/peer addresses and OSPF-enabled link context.
2. Compare area, authentication, timers, router IDs and network type.
3. Use the state table to inspect hello versus database exchange evidence.
4. For a missing prefix, follow database -> protocol route -> installed route -> forwarding entry.
5. Test the affected application and reverse path after convergence.

Common mistakes

- Treating every 2-Way neighbor as broken.
- Changing router IDs or restarting the process before collecting evidence.
- Using Full adjacency as the sole deployment acceptance test.

Acceptance checks

- Expected adjacencies match link type and remain stable.
- Required prefixes and next hops are installed in the correct table.
- Forward, reverse and planned failover application tests pass.

Primary references

[RFC 2328: OSPFv2](#)[Cisco OSPF ExStart / Exchange troubleshooting](#)[Junos OSPF verification and monitoring](#)

Original Wolex diagrams, scenarios and troubleshooting sequences. Vendor names identify platform scope; no affiliation is implied.

[Read the full web guide and supporting references](#)[Deployment and migration help | Network security review from Wolex](#)

ROUTING | REV 2.0 | REVIEWED 2026-10-10

BGP established, but no usable route

01 / Quick reference and concepts

Separate peer health, received paths, policy acceptance, best-path selection, installation and advertisement.

IPv4 BGP examples in IOS XE and Junos. Address-family, VRF, next-hop and release differences matter; this is not a universal best-path ordering chart.



Inspect each stage separately. A route can be received but hidden, lose selection or fail next-hop resolution.

Stage	Question	Evidence
Transport	Can peers communicate?	TCP 179; source and peer context
Established	Is BGP exchanging messages?	State / uptime / prefix count
Received	Did this peer send the prefix?	Received route view / retention
Accepted	Did import policy allow it?	Policy and hidden/rejected reason
Selected	Is a usable path eligible?	Attributes and next-hop resolution
Installed	Did it reach RIB and FIB?	Route and forwarding entry
Advertised	Did export policy send it?	Neighbor-specific advertisement

What to understand first

- BGP uses TCP and a finite-state machine: Idle, Connect, Active, OpenSent, OpenConfirm and Established. Active means an attempt to establish transport, not a healthy forwarding session.
- Import/export policy is directional. A neighbor being established says nothing about whether the required prefix is permitted in the right address family.
- Best-path rules include attributes and implementation-specific behavior. Cisco weight is local to the device; LOCAL_PREF is normally carried within the AS. Neither replaces next-hop reachability.
- Received route visibility depends on retention and command semantics. Absence from one display can require checking policy, refresh capability and the sender before drawing conclusions.

ROUTING | REV 2.0 | REVIEWED 2026-10-10

BGP established, but no usable route

02 / Commands and worked example

Replace documentation addresses, example interfaces and every <PLACEHOLDER>. Check command help for your model/release and routing context. Examples are documentation-reviewed, not executed on customer equipment.

Cisco IOS XE

Read-only EXEC

```
show ip bgp summary
show ip bgp 192.0.2.0
show ip bgp neighbors 198.51.100.1 advertised-routes
show ip route 192.0.2.10
show ip cef 192.0.2.10
```

Inspect: Inspect the actual prefix, attributes and next hop; compare advertisement with installed forwarding.

Junos

Read-only operational

```
show bgp summary
show route receive-protocol bgp 198.51.100.1
show route 192.0.2.0/24 detail
show route advertising-protocol bgp 198.51.100.1
```

Inspect: Compare receipt, activity and export. Use hidden-route inspection and instance-specific tables when needed.

Illustrative missing-route evidence

Illustrative teaching example, not captured device output.

```
Neighbor: Established
Wanted prefix: 192.0.2.0/24 received
BGP next hop: 198.51.100.9
Route to next hop: missing
```

- Peer transport can work while the received path has an unresolved next hop. Check the intended underlay or next-hop policy.
- Changing LOCAL_PREF will not repair missing next-hop reachability. These observations are deliberately simplified.

ROUTING | REV 2.0 | REVIEWED 2026-10-10

BGP established, but no usable route

03 / Troubleshooting and acceptance

1. Confirm peer/source addresses, ASNs, TCP reachability and address family.
2. Ask whether the sender advertises the exact prefix, then inspect receipt at this peer.
3. Check import policy and next-hop resolution before debating path preference.
4. Compare selected BGP path with the RIB and FIB in the affected VRF/instance.
5. Inspect export to the next neighbor and test forward and reverse application traffic.

Common mistakes

- Resetting all peers to refresh one route without an approved plan.
- Confusing received, accepted and active routes.
- Assuming one vendor best-path list applies unchanged to another.

Acceptance checks

- Required prefixes are accepted, installed and exported as intended.
- Unwanted routes remain rejected; counters and policy evidence support it.
- Application paths and planned peer-loss behavior meet the target.

Primary references

[RFC 4271: BGP-4](#)[Cisco IOS XE BGP](#)[Junos BGP troubleshooting](#)

Original Wolex diagrams, scenarios and troubleshooting sequences. Vendor names identify platform scope; no affiliation is implied.

[Read the full web guide and supporting references](#)

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

SECURITY | REV 2.0 | REVIEWED 2026-10-10

NAT, zones & session troubleshooting

01 / Quick reference and concepts

Track the original and translated tuples and avoid the common destination-NAT address-versus-zone mistake.

PAN-OS 11.2 policy concepts and IOS XE inspection examples. Juniper SRX flow/NAT is outside the EX/MX command scope of this library.



Document both tuples and zones. A NAT translation changes addressing; it does not by itself authorize the application.

Item	Record	Why it matters
Original flow	Source / destination / ports	Rule match and original identity
Translated flow	Source / destination / ports	Server and return-path observations
NAT rule	Ordered first matching rule	Shadowed rules may never apply
Security rule	Addresses plus effective zones	Permission is a separate decision
Return path	Route back to translated source	Asymmetry can bypass session state

What to understand first

- Source NAT changes the source identity; destination NAT changes the destination. Port translation can change the transport tuple as well. Write the protocol and both ports, not just an IP pair.
- For PAN-OS destination NAT, NAT-rule destination-zone matching follows the original destination route lookup. Security policy uses original addresses with post-NAT zones.
- A first-match ordered NAT policy can select an unexpected earlier rule. Examine the actual session and applied translation instead of relying only on configuration intent.
- Existing sessions, policy-based forwarding and routing context can affect observations. A new controlled attempt gives clearer evidence after a reviewed change.

SECURITY | REV 2.0 | REVIEWED 2026-10-10

NAT, zones & session troubleshooting

02 / Commands and worked example

Replace documentation addresses, example interfaces and every <PLACEHOLDER>. Check command help for your model/release and routing context. Examples are documentation-reviewed, not executed on customer equipment.

PAN-OS

Read-only operational

```
show session all filter source 198.51.100.10 destination 203.0.113.20
show session id <SESSION_ID>
```

Inspect: Read original and translated flows, rule, zones, application and byte counters; select the correct vsys.

Cisco IOS XE

Read-only EXEC

```
show ip nat translations
show ip nat statistics
show ip route 192.0.2.20
```

Inspect: Compare translation entries and counters with intended interfaces and the server route. NAT feature support varies.

Illustrative inbound destination NAT

Illustrative teaching example, not captured device output.

```
Original: 198.51.100.10 -> 203.0.113.20:443
Translated: 198.51.100.10 -> 192.0.2.20:443
Original destination zone: untrust
Server destination zone: dmz
```

- In this simplified PAN-OS example, the NAT rule matches the original destination route zone; the security rule targets dmz with the original destination address.
- Server replies must follow a path that permits the firewall to apply the session translation. The documentation addresses are not deployment values.

SECURITY | REV 2.0 | REVIEWED 2026-10-10

NAT, zones & session troubleshooting

03 / Troubleshooting and acceptance

1. Capture the original tuple, time and ingress zone of one failing attempt.
2. Identify the first matching NAT rule and inspect the resulting session translation.
3. Check security policy with original addresses and the effective destination zone.
4. Verify server reachability and return routing for the translated source.
5. Compare both flow directions and new-session logs after the approved correction.

Common mistakes

- Assuming NAT implies an allow rule.
- Using the private server address where a PAN-OS security rule requires the original destination.
- Clearing all production sessions to test a single changed flow.

Acceptance checks

- The intended rule and translation match a fresh session.
- Forward and reverse counters move for the real application.
- Adjacent applications and intended denies remain correct.

Primary references

[PAN-OS destination NAT example](#)[PAN-OS NAT rules](#)[PAN-OS session interpretation](#)[Cisco IOS XE NAT monitoring](#)

Original Wolex diagrams, scenarios and troubleshooting sequences. Vendor names identify platform scope; no affiliation is implied.

[Read the full web guide and supporting references](#)[Deployment and migration help](#) | [Network security review from Wolex](#)

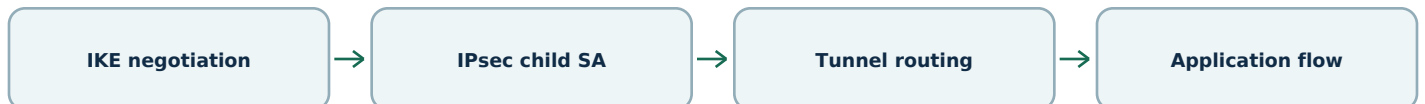
SECURITY | REV 2.0 | REVIEWED 2026-10-10

IPsec VPN: up, but traffic fails

01 / Quick reference and concepts

Separate IKE negotiation, IPsec selectors and real encrypted application traffic.

Route-based site-to-site VPN troubleshooting, PAN-OS inspection and cross-vendor workflow. IKEv1/IKEv2 and peer implementations differ.



A healthy IKE SA proves negotiation at one layer. Verify the child SA, selectors and traffic through the intended tunnel.

Layer	Inspect	Typical lead
Peer transport	Reachability / UDP 500 and 4500	NAT traversal / filtering
IKE	Identity, proposal, authentication	Mismatch or failed authentication
IPsec child SA	Transforms and traffic selectors	Proxy IDs / subnet mismatch
Routing	Destination through tunnel	Wrong VR or missing route
Policy / NAT	Intended flow permitted	Unexpected translation / deny
Traffic	Counters in both directions	Return routing / MTU / peer issue

What to understand first

- IKE establishes authenticated keying state. IPsec SAs protect selected traffic; an established IKE SA alone does not prove a useful child SA exists.
- IKEv1 proxy IDs and IKEv2 traffic selectors describe protected traffic, with negotiation differences between versions and peers. Compare local and remote definitions from both viewpoints.
- NAT traversal commonly carries IPsec over UDP 4500. Without NAT traversal, ESP uses IP protocol 50, not TCP/UDP port 50. Confirm the negotiated mode before checking filters.
- Tunnel-interface state, route selection, security policy and reverse path are independent. Overlapping networks or extra encapsulation can create failures despite healthy negotiation.

SECURITY | REV 2.0 | REVIEWED 2026-10-10

IPsec VPN: up, but traffic fails

02 / Commands and worked example

Replace documentation addresses, example interfaces and every <PLACEHOLDER>. Check command help for your model/release and routing context. Examples are documentation-reviewed, not executed on customer equipment.

PAN-OS

Read-only operational

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

Inspect: Compare gateway/tunnel identity, SA state and counter changes during one controlled attempt.

PAN-OS session inspection

Read-only operational

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

Inspect: Check actual zones, rule, tunnel egress and translations. Use the correct vsys and routing engine context.

Illustrative one-direction VPN traffic

Illustrative teaching example, not captured device output.

```
IKE SA: established
IPsec SA: installed
During client attempt:
  Local encrypted packets: increasing
  Local decrypted packets: unchanged
```

- This narrows the investigation toward the remote path or missing return traffic; it does not prove the peer is at fault.
- Correlate peer counters, selectors, remote policy and application replies with the same timestamp and tuple.

SECURITY | REV 2.0 | REVIEWED 2026-10-10

IPsec VPN: up, but traffic fails

03 / Troubleshooting and acceptance

1. Identify the exact client/server subnets, application tuple and peer/tunnel names.
2. Check peer transport and IKE state without restarting negotiations.
3. Compare child-SA selectors and proposals at both ends.
4. Verify tunnel route, policy/NAT and return route for that flow.
5. Compare timed encrypted/decrypted counters; if transfers stall, investigate MTU and permitted ICMP feedback.

Common mistakes

- Treating a green tunnel indicator as end-to-end success.
- Bouncing every tunnel before collecting failure evidence.
- Opening ESP by port number or assuming all traffic uses NAT traversal.

Acceptance checks

- Required subnets and applications pass in both directions.
- Counters and session evidence identify the intended tunnel.
- Rekey, recovery and MTU behavior satisfy the approved acceptance plan.

Primary references

[PAN-OS networking CLI](#)[PAN-OS configuration tests](#)[PAN-OS session interpretation](#)[RFC 7296: IKEv2 and traffic selectors](#)[RFC 3948: UDP encapsulation of IPsec ESP](#)

Original Wolex diagrams, scenarios and troubleshooting sequences. Vendor names identify platform scope; no affiliation is implied.

[Read the full web guide and supporting references](#)

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

PACKET ANALYSIS | REV 2.0 | REVIEWED 2026-10-10

Wireshark filters by troubleshooting task

01 / Quick reference and concepts

Find the conversation, inspect handshake failures and use TCP analysis flags as leads rather than verdicts.

Wireshark display filters for captured traffic. Capture filters use a different language; field availability depends on installed Wireshark version.



A capture shows what reached the observation point. Missing packets may reflect capture loss, asymmetric paths or a filter, rather than network loss.

Task	Display filter	Interpretation
One IPv4 host	<code>ip.addr == 192.0.2.10</code>	Either direction
One IPv6 host	<code>ipv6.addr == 2001:db8::10</code>	Either direction
HTTPS TCP traffic	<code>tcp.port == 443</code>	Does not prove HTTP or decryption
Initial SYN	<code>tcp.flags.syn == 1 && tcp.flags.ack == 0</code>	Connection attempts
Reset	<code>tcp.flags.reset == 1</code>	Inspect sender and timing
DNS query	<code>dns.flags.response == 0</code>	Only decoded DNS
DNS errors	<code>dns.flags.response == 1 && dns.flags.rcode != 0</code>	Error response; inspect code
Retransmission lead	<code>tcp.analysis.retransmission</code>	Analyzer heuristic
Single stream	<code>tcp.stream == 7</code>	Index belongs to this capture

What to understand first

- Display filters select packets already in the capture. They do not reduce the original capture file. Use a capture filter only when its narrower acquisition scope is deliberate.
- Boolean fields must be compared to their value when checking a flag. `tcp.flags.syn` tests field presence; `tcp.flags.syn == 1` checks whether SYN is set.
- TCP analysis marks are derived from observed sequence and timing. Missing capture packets, offload and out-of-order arrival can affect conclusions.
- DNS and HTTP filters only work when those protocols are decoded and visible. Encrypted DNS, TLS and QUIC cannot be interpreted as cleartext by merely choosing a port.

PACKET ANALYSIS | REV 2.0 | REVIEWED 2026-10-10

Wireshark filters by troubleshooting task

02 / Commands and worked example

Replace documentation addresses, example interfaces and every <PLACEHOLDER>. Check command help for your model/release and routing context. Examples are documentation-reviewed, not executed on customer equipment.

Wireshark display bar

Read-only analysis filters

```
ip.addr == 192.0.2.10 && tcp.port == 443
tcp.flags.syn == 1 && tcp.flags.ack == 0
tcp.analysis.retransmission || tcp.analysis.fast_retransmission
```

Inspect: Select the failing tuple first, then inspect sequence, acknowledgment and timing in the full stream.

Conversation triage

Read-only analysis filters

```
dns.flags.response == 1 && dns.flags.rcode != 0
tcp.flags.reset == 1
tcp.analysis.zero_window
```

Inspect: An error, reset or zero window needs source identity and surrounding packets to explain it.

Illustrative handshake timeline

Illustrative teaching example, not captured device output.

```
0.000s Client -> Server: SYN
1.000s Client -> Server: SYN retransmission
3.000s Client -> Server: SYN retransmission
No SYN-ACK observed at this capture point
```

- This shows no observed response here. Check capture completeness, server-side receipt and the return path.
- A second authorized capture near the server can distinguish a missing request from a missing reply.

PACKET ANALYSIS | REV 2.0 | REVIEWED 2026-10-10

Wireshark filters by troubleshooting task

03 / Troubleshooting and acceptance

1. Record capture point, interfaces, clock accuracy, tuple and any acquisition filter.
2. Select the conversation and inspect SYN/SYN-ACK/ACK or the applicable UDP exchange.
3. Follow the stream and compare failures with a successful attempt under similar conditions.
4. Correlate retransmissions, resets, windows and response times with endpoint and network logs.
5. Preserve the original capture; share only the authorized minimum with a clear conclusion and its limits.

Common mistakes

- Pasting a display filter into a capture-filter field.
- Calling every retransmission flag proof of a bad network.
- Inferring no DNS activity from absent cleartext DNS while encrypted DNS is used.

Acceptance checks

- Capture includes the relevant directions and interval.
- Analysis identifies observations separately from hypotheses.
- A repeated application test confirms the corrected behavior.

Primary references

[Wireshark display-filter expressions](#)[Wireshark TCP field reference](#)[Wireshark documentation](#)

Original Wolex diagrams, scenarios and troubleshooting sequences. Vendor names identify platform scope; no affiliation is implied.

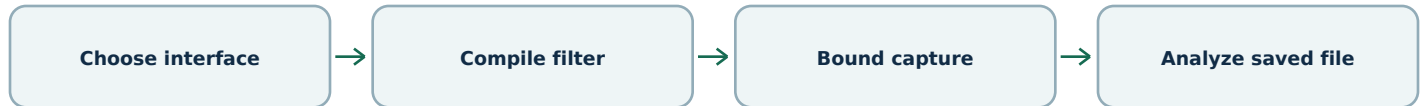
[Read the full web guide and supporting references](#)[Deployment and migration help](#) | [Network security review from Wolex](#)

PACKET ANALYSIS | REV 2.0 | REVIEWED 2026-10-10

tcpdump & capture-filter quick reference

01 / Quick reference and concepts

Capture a bounded, targeted conversation and read a saved trace without unnecessary name lookups. tcpdump/libpcap on an authorized Unix-like host. Interface names, privileges, link-layer types and available options vary.



Confirm interface and filter before capture. Packet count is not a wall-clock timeout; stop the capture at the end of the approved test window.

Option / filter	Purpose	Watch for
-D	List capture interfaces	Names vary by host
-nn	Keep numeric addresses and ports	Avoid lookup side effects
-i eth0	Choose interface	Example name; replace it
-c 200	Stop after 200 matched packets	Can wait indefinitely on quiet flow
-s 128	Limit bytes kept per packet	May truncate useful headers
-w flow.pcap	Write raw capture	May include sensitive content
-r flow.pcap	Read saved capture	No new network capture
host / port / net	libpcap acquisition filter	Different from Wireshark syntax

What to understand first

- A capture filter runs during acquisition or reading; it can exclude packets permanently from the saved capture. Use parentheses and quote the expression to avoid shell interpretation.
- Choose a snap length sufficient for the question. Header-limited capture reduces exposure but can lose encapsulated headers; -s 0 keeps full packets and may collect payloads.
- Packet-count bounds do not stop a quiet capture on elapsed time. Plan an explicit operator stop or use an approved OS timeout mechanism with compatible syntax.
- Capture-drop counters describe the collection path, not necessarily loss on the network. VLAN tags, tunnels and offload can change what a capture point sees.

PACKET ANALYSIS | REV 2.0 | REVIEWED 2026-10-10

tcpdump & capture-filter quick reference

02 / Commands and worked example

Replace documentation addresses, example interfaces and every <PLACEHOLDER>. Check command help for your model/release and routing context. Examples are documentation-reviewed, not executed on customer equipment.

Interface and filter preparation

Read-only listing / compile check

```
tcpdump -D  
tcpdump -i eth0 -d 'host 192.0.2.10 and tcp port 443'
```

Inspect: Listing and compiled-filter inspection do not save a trace. Confirm the chosen interface and intended match.

Targeted capture

Starts capture and writes a file

```
tcpdump -i eth0 -nn -s 128 -c 200 -w flow.pcap 'host 192.0.2.10 and tcp port 443'
```

Inspect: Use only authorized scope and required privileges. Stop when the test window ends; 128 bytes may be insufficient for encapsulated traffic.

Saved-file review

Reads existing file

```
tcpdump -nn -r flow.pcap 'tcp port 443'
```

Inspect: Read the saved flow numerically. Existing payload content remains in the file regardless of this display.

Capture filters versus display filters

Illustrative teaching example, not captured device output.

```
libpcap: host 192.0.2.10 and tcp port 443  
Wireshark: ip.addr == 192.0.2.10 && tcp.port == 443
```

- The two expressions target a similar IPv4 conversation but belong to different filter languages.
- Check matching packets against the capture link type; nested encapsulation can require additional filter treatment.

PACKET ANALYSIS | REV 2.0 | REVIEWED 2026-10-10

tcpdump & capture-filter quick reference

03 / Troubleshooting and acceptance

1. State the observation point, authorized endpoints, transport and time window.
2. Select the real interface and validate the filter syntax before collection.
3. Start the bounded capture, reproduce one attempt and stop deliberately.
4. Review both directions and collection-drop counters before inferring network loss.
5. Protect the trace and retain only the evidence needed for the troubleshooting question.

Common mistakes

- Using an unbounded full-payload capture as the default.
- Assuming -c provides a time limit or -nn hides captured data.
- Missing the flow because the chosen interface sees a translated or encapsulated tuple.

Acceptance checks

- Capture scope and duration match the approved test.
- Relevant headers and both directions are available.
- Trace storage and the escalation handoff preserve confidentiality.

Primary references

[tcpdump project manual source](#)

[libpcap filter manual source](#)

[Wireshark display-filter expressions](#)

Original Wolex diagrams, scenarios and troubleshooting sequences. Vendor names identify platform scope; no affiliation is implied.

[Read the full web guide and supporting references](#)

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

DEPLOYMENT | REV 2.0 | REVIEWED 2026-10-10

Network deployment & rollback acceptance

01 / Quick reference and concepts

Define what working means before the cutover, preserve a recovery path and close with evidence rather than a reachable CLI.

Engineer-authored change workflow for switches, routers and firewalls. Example checks are read-only; the Junos commit sequence explicitly changes device state.



Choose acceptance and rollback triggers before activation. Keep console/out-of-band access and assign the person who makes the recovery decision.

Stage	Record / test	Decision
Before	Ports, VLANs, routes, peers, HA, versions	Compatible and recoverable?
Activation	Approved scope and start time	Access and timer preserved?
Acceptance	Real flows, intended denies, redundancy	All agreed criteria pass?
Recovery	Known-good state and owner	Trigger reached or timer near expiry?
Closure	Save / confirm, monitor, document	Evidence and ownership complete?

What to understand first

- A backup is only useful if it is compatible, accessible and recoverable with the available access path. Record credentials through the approved secret-management process, not in the worksheet.
- Baseline the affected service and nearby dependencies. Include management, DNS, DHCP, routing, VPNs and monitoring where they are in scope.
- Acceptance needs source-specific application tests and intended denies. A successful commit, link-up state or management ping is evidence of only part of the change.
- Recovery differs by platform: IOS XE often applies running changes immediately; Junos candidate/confirmed commits have a timer; PAN-OS commit and Panorama push jobs have distinct target scope.

DEPLOYMENT | REV 2.0 | REVIEWED 2026-10-10

Network deployment & rollback acceptance

02 / Commands and worked example

Replace documentation addresses, example interfaces and every <PLACEHOLDER>. Check command help for your model/release and routing context. Examples are documentation-reviewed, not executed on customer equipment.

Cisco IOS XE

Read-only EXEC

```
show interfaces status
show interfaces trunk
show ip route 192.0.2.10
show ip bgp summary
```

Inspect: Choose only commands supported by this device and relevant to the approved change; compare with baseline.

Junos

Read-only operational

```
show interfaces terse
show route 192.0.2.0/24 detail
show system commit
```

Inspect: Verify the correct instance and confirmed-commit timing; keep an independent management path.

PAN-OS

Read-only operational

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

Inspect: Review scope and job outcome. A Panorama push must be checked on the intended target devices.

Junos configuration-mode sequence - changes device state

Illustrative teaching example, not captured device output.

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

- Stage only the approved candidate. Run commit check before the timed commit; it can confirm an already-pending confirmed commit.
- Issue the final commit only after acceptance. Track the timer. Rollback loads a candidate and requires a commit; choose the correct revision.

DEPLOYMENT | REV 2.0 | REVIEWED 2026-10-10

Network deployment & rollback acceptance

03 / Troubleshooting and acceptance

1. Record current topology and a timestamped baseline; verify compatibility and the recovery method.
2. Assign change, test and recovery owners with an agreed deadline and stop conditions.
3. Make the reviewed change while preserving console/out-of-band access and any confirmed-commit timer.
4. Test management, actual allowed flows, intended denies and approved redundancy behavior.
5. If acceptance fails, follow the reviewed recovery decision; otherwise save/confirm, monitor and update documentation.

Common mistakes

- Starting without a working independent access path.
- Using a generic rollback command without knowing its state and revision.
- Confirming the change before application tests finish.

Acceptance checks

- Every agreed test has an owner, timestamp and result.
- Accepted configuration is saved/confirmed and monitoring is clean.
- Recovery records and as-built documentation are complete.

Primary references

[Junos commit and confirmed rollback](#)[Cisco configuration replacement](#)[PAN-OS networking CLI](#)

Original Wolex diagrams, scenarios and troubleshooting sequences. Vendor names identify platform scope; no affiliation is implied.

[Read the full web guide and supporting references](#)[Deployment and migration help](#) | [Network security review from Wolex](#)

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: wolex.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/timezone, 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](#)