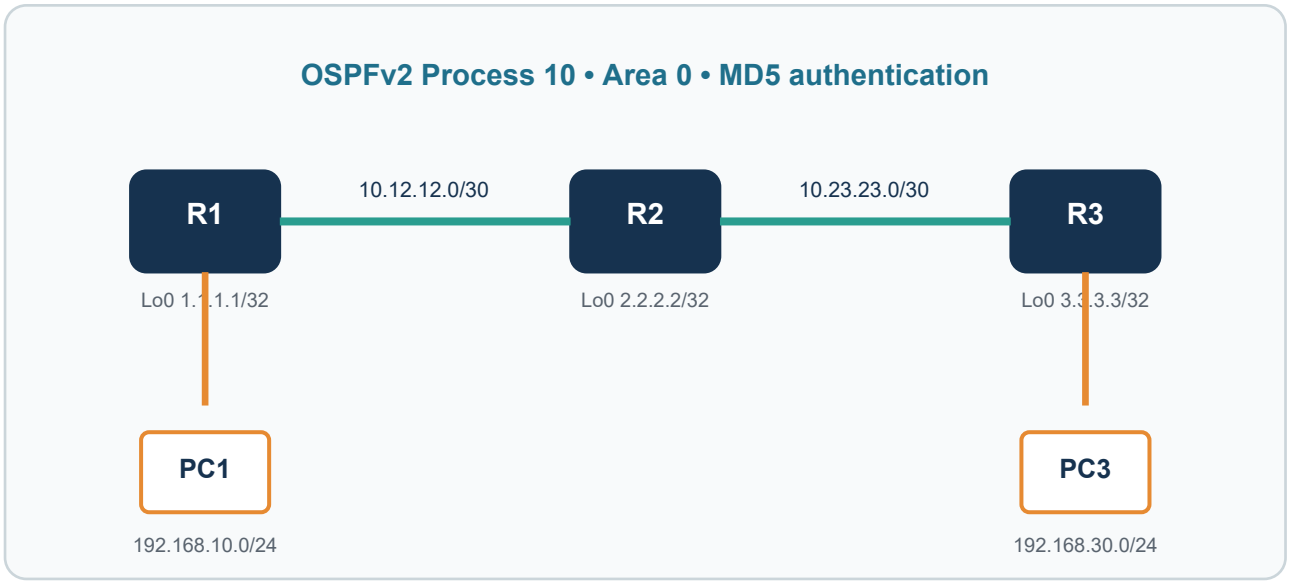
CCNP ENARSI

Lab 01

OSPFv2 Adjacency, Authentication & Evidence



Production-ready guided workbook

Build authenticated OSPFv2 adjacencies across a three-router enterprise path, prove route exchange with control-plane evidence, and validate end-to-end forwarding between two branch clients.

Blueprint	Level	Estimated time	Validated platform
1.10.a, 1.10.b	Intermediate	120–150 minutes	EVE-NG + approved IOL L3 + VPCS

1. Lab Overview

This lab is the first ENARSI routing exercise. It deliberately separates three questions that engineers must answer during an outage: Is the physical/IP path healthy? Did OSPF form the expected neighbor relationship? Did the resulting routes produce the required forwarding behavior? The configuration is small enough to inspect line by line, but its verification method is the same method used on larger production networks.

You will configure OSPFv2 process 10 in area 0, select stable router IDs, suppress unnecessary Hellos on user-facing LANs, use point-to-point OSPF network behavior on routed transit links, protect neighbor formation with MD5 message-digest authentication, and validate both routing tables and client traffic.

Why this matters

• A route in the configuration is not evidence that it is active. You must verify the neighbor, LSDB-derived route, next hop, and forwarding result.

• Authentication mismatches frequently look like ordinary neighbor failures. A disciplined engineer checks interface state, IP reachability, OSPF parameters, and authentication in a fixed order.

• Passive interfaces reduce unnecessary protocol exposure while still allowing their connected networks to be advertised.

• Router IDs are operational identifiers. Stable, intentional IDs make monitoring and incident correlation easier.

2. Learning Objectives

• Explain the OSPF neighbor prerequisites used in this topology.

• Configure interface-based OSPFv2 activation in area 0.

• Configure stable router IDs and understand when they take effect.

• Apply and verify area-level message-digest authentication and matching interface keys.

• Use passive-interface default safely while enabling Hellos only on transit links.

• Verify FULL adjacencies, OSPF routes, next hops, and end-to-end client reachability.

• Recognize symptoms of an authentication mismatch or an accidentally passive transit interface.

3. Enterprise Scenario

Northstar Manufacturing has opened two routed branches. R1 serves Branch 1, R3 serves Branch 3, and R2 is the regional transit router. Static routes were acceptable during staging, but operations now requires dynamic reachability and consistent neighbor authentication. The security baseline also requires that routing Hellos never be sent toward user LANs.

Your change is successful only when the two expected neighbors are FULL, each edge router learns the remote branch LAN as an OSPF intra-area route, and PC1 can reach PC3 without any static route.

4. Required Prior Knowledge

• IPv4 addressing and /30 versus /24 subnet boundaries.

• Cisco IOS interface configuration and the meaning of up/up.

• Connected and local routes in the IPv4 routing table.

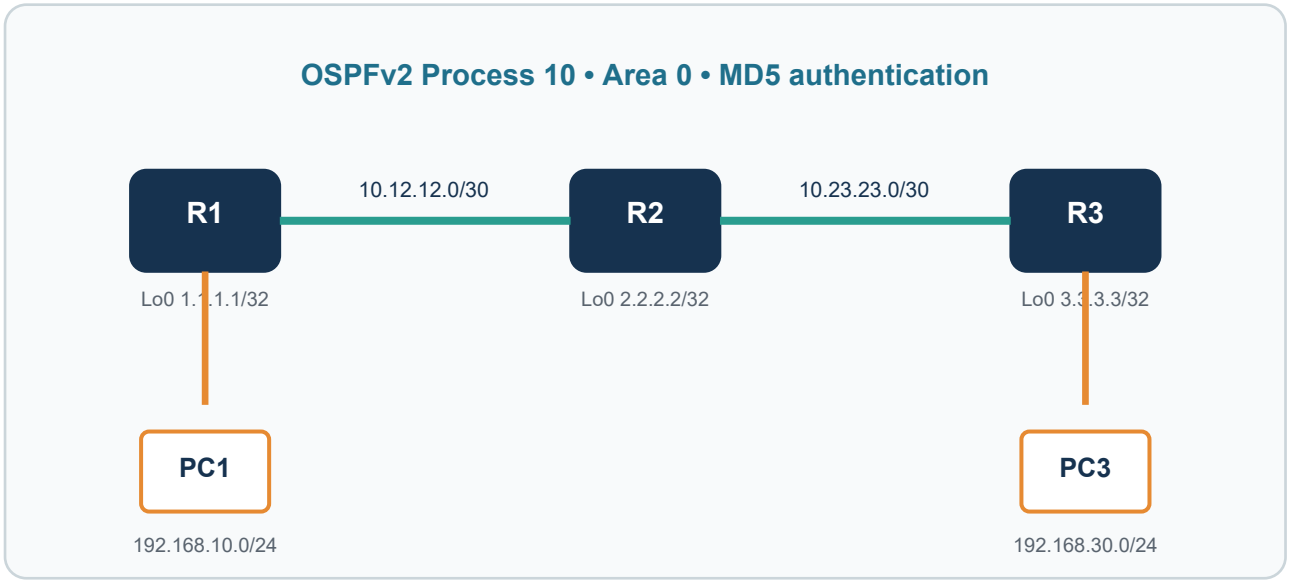
• Basic use of ping, show commands, and configuration modes.

• The purpose of an IGP and the difference between control-plane adjacency and data-plane forwarding.

Prerequisite refresher

A directly connected ping proves Layer 1–3 reachability on one link; it does not prove OSPF compatibility. OSPF neighbors must agree on key parameters, including area, network type, Hello/Dead timers, authentication type and key. After a FULL adjacency forms, LSAs are exchanged and SPF selects routes. End-to-end ping then proves that the installed routes and return path work together.

5. Topology



R1 and R3 are branch routers. R2 is a transit router and therefore must form two independent OSPF adjacencies. PC1 and PC3 are data-plane test points; they do not run OSPF.

6. Node Connection Table

Link	Endpoint A	Endpoint B	Purpose
1	R1 Ethernet0/0	R2 Ethernet0/0	R1–R2 routed transit
2	R2 Ethernet0/1	R3 Ethernet0/0	R2–R3 routed transit
3	R1 Ethernet0/1	PC1 eth0	Branch 1 user LAN
4	R3 Ethernet0/1	PC3 eth0	Branch 3 user LAN

7. IP Addressing Table

Node	Interface	IPv4 address	Role
R1	Loopback0	1.1.1.1/32	OSPF router ID source
R1	Ethernet0/0	10.12.12.1/30	Transit to R2
R1	Ethernet0/1	192.168.10.1/24	PC1 gateway
R2	Loopback0	2.2.2.2/32	OSPF router ID source
R2	Ethernet0/0	10.12.12.2/30	Transit to R1
R2	Ethernet0/1	10.23.23.1/30	Transit to R3
R3	Loopback0	3.3.3.3/32	OSPF router ID source
R3	Ethernet0/0	10.23.23.2/30	Transit to R2
R3	Ethernet0/1	192.168.30.1/24	PC3 gateway
PC1	eth0	192.168.10.10/24	Gateway 192.168.10.1
PC3	eth0	192.168.30.10/24	Gateway 192.168.30.1

8. Starting State

Three UNLs share the identical topology. RAW starts without addressing or OSPF; follow every build step. SAVE-IP-CONFIGURATION contains device names, loopbacks, interface descriptions and IPv4/VPCS addressing only; verify the baseline and start Phase B. SAVE-CONFIG contains the fully completed healthy OSPF configuration and named clients; after boot, wait 45 seconds for convergence and proceed directly to sections 12-14. No configuration entry is required for that final version. On RAW, answer no to the initial configuration dialog and accept termination of autoinstall.

CLI annotations: GREEN - expected healthy result; YELLOW - warning or interpretation required; RED - fault or failed requirement. Colors are workbook annotations, not native CLI colors. Variable timers and ages may differ. Yellow/red items include a one-line reason.

RAW — first boot response

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Would you like to terminate autoinstall? [yes]: yes
```

Item	RAW	save-ip-configuration	save-config
Topology	Present	Identical	Identical
Device names / IPs	Unconfigured	Present	Present
VPCS names / gateway	Unconfigured	Present	Present
OSPF / authentication	Absent	Absent	Complete / healthy
Learner action	Build from scratch	Build OSPF	Verify / ping only

9. Technical Deep Dive

9.1 Neighbor formation is a compatibility test

OSPF sends Hello packets on participating interfaces. A received Hello is not enough to create a FULL adjacency: the neighbors compare critical parameters. In this lab the physical link, subnet, area 0 assignment, point-to-point network type, Hello/Dead intervals, and message-digest authentication must align. When one item differs, the diagnostic task is to identify the first failed prerequisite instead of repeatedly clearing the process.

On a point-to-point OSPF network there is no DR/BDR election. Each transit link has only two routers, so point-to-point behavior is operationally clear and converges without a designated-router role. Broadcast behavior and DR/BDR are studied in Lab 02.

9.2 Router ID and process behavior

The router ID is a 32-bit identifier, written like an IPv4 address, that identifies the OSPF speaker in LSAs and neighbor output. Configuring it explicitly under the process removes ambiguity. A router ID is selected when the process starts; changing it later normally requires restarting the OSPF process or reloading. In a planned build, configure it before neighbors form.

9.3 Passive-interface default

OSPF must advertise the branch LANs, but no OSPF router exists on those LANs. The safe operational pattern is passive-interface default, followed by no passive-interface only on approved router-to-router links. A passive interface still contributes its connected subnet to OSPF when the interface itself is enabled for the process; it simply stops sending Hellos and cannot form a neighbor.

9.4 Authentication scope and key placement

The area command enables message-digest authentication for OSPF interfaces in area 0. Each participating transit interface then needs a matching key ID and secret. Both ends must use the same authentication mode, key ID, and key value. The key protects OSPF packets; it does not encrypt user traffic. In production, secrets should follow the organization’s key lifecycle and should not be exposed in validation reports.

9.5 Evidence chain

A professional validation chain moves from local state to end-to-end behavior: interface up/up → directly connected ping → OSPF interface parameters → FULL neighbor → OSPF-learned prefix → recursive next-hop resolution → client ping in both directions. Each step rules out a class of causes. This is also a strong interview answer because it explains how you know the network works, not just which commands you typed.

10. Phase A — Baseline Addressing (RAW only)

On save-ip-configuration, verify this phase and continue to Phase B. On save-config, skip configuration and go directly to final verification. On RAW, apply the baseline below; these commands establish local addressing without solving OSPF.

Configure R1 baseline

R1 needs a stable loopback, one /30 transit address, and the Branch 1 default gateway. Interface descriptions make later troubleshooting faster.

R1 — baseline configuration

```
enable
conf t
hostname R1
no ip domain lookup
interface Loopback0
description OSPF_ROUTER_ID
ip address 1.1.1.1 255.255.255.255
no shutdown
interface Ethernet0/0
description TO_R2
ip address 10.12.12.1 255.255.255.252
no shutdown
interface Ethernet0/1
description BRANCH1_LAN
ip address 192.168.10.1 255.255.255.0
no shutdown
end
```

Configure R2 baseline

R2 is the transit router. Both /30 links must be reachable before OSPF is introduced.

R2 — baseline configuration

```
enable
conf t
hostname R2
no ip domain lookup
interface Loopback0
description OSPF_ROUTER_ID
ip address 2.2.2.2 255.255.255.255
no shutdown
interface Ethernet0/0
description TO_R1
ip address 10.12.12.2 255.255.255.252
no shutdown
interface Ethernet0/1
description TO_R3
ip address 10.23.23.1 255.255.255.252
no shutdown
end
```

Configure R3 baseline

R3 mirrors the edge role of R1 for Branch 3.

R3 — baseline configuration

```
enable
conf t
hostname R3
no ip domain lookup
interface Loopback0
description OSPF_ROUTER_ID
ip address 3.3.3.3 255.255.255.255
no shutdown
interface Ethernet0/0
description TO_R2
ip address 10.23.23.2 255.255.255.252
no shutdown
interface Ethernet0/1
description BRANCH3_LAN
ip address 192.168.30.1 255.255.255.0
no shutdown
end
```

Configure the clients

The VPCS commands define each client address, prefix, and default gateway. The gateway is required for destinations outside the local /24.

VPCS — client addressing

```
VPCS> set pcname PC1
PC1> ip 192.168.10.10 192.168.10.1 24
PC1> save

VPCS> set pcname PC3
PC3> ip 192.168.30.10 192.168.30.1 24
PC3> save
```

Immediate baseline verification

Verify every router interface is up/up, then test only directly connected peers. PC1-to-PC3 is expected to fail at this stage because no route to the remote branch exists.

Baseline verification

```
R1# show ip interface brief
R1# ping 10.12.12.2
R2# ping 10.23.23.2
PC1> ping 192.168.10.1
PC3> ping 192.168.30.1
PC1> ping 192.168.30.10
```

Expected result: all local and directly connected tests succeed; the final remote-branch ping fails. That failure is correct evidence of the unsolved starting state. The first local probe may precede ARP resolution; repeat local pings and require five replies before continuing.

Actual CLI output - R1

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            10.12.12.1      YES manual up                    up
Ethernet0/1            192.168.10.1    YES manual up                    up
Ethernet0/2            unassigned      YES unset  administratively down down
Ethernet0/3            unassigned      YES unset  administratively down down
Loopback0              1.1.1.1         YES manual up                    up
```

Actual CLI output - R1

```
R1# ping 10.12.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.12.12.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

WARNING - Some initial probes were lost; repeat the test and require the subsequent five replies before continuing.

Actual CLI output - R1

```
R1# ping 10.12.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.12.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Actual CLI output - R2

```
R2# ping 10.23.23.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.23.23.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

WARNING - Some initial probes were lost; repeat the test and require the subsequent five replies before continuing.

Actual CLI output - R2

```
R2# ping 10.23.23.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.23.23.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Actual CLI output - PC1

```
PC1> show ip
NAME        : PC1[1]
IP/MASK     : 192.168.10.10/24
GATEWAY     : 192.168.10.1
MAC         : 00:50:79:66:68:04
LPORT       : 20000
RHOST:PORT  : 127.0.0.1:30000
MTU         : 1500
```

Actual CLI output - PC1

```
PC1> ping 192.168.10.1
192.168.10.1 icmp_seq=1 timeout
84 bytes from 192.168.10.1 icmp_seq=2 ttl=255 time=0.616 ms
84 bytes from 192.168.10.1 icmp_seq=3 ttl=255 time=1.466 ms
84 bytes from 192.168.10.1 icmp_seq=4 ttl=255 time=0.545 ms
84 bytes from 192.168.10.1 icmp_seq=5 ttl=255 time=2.377 ms
```

WARNING - Initial local probes may precede neighbor resolution; repeat and require five replies.

Actual CLI output - PC1

```
PC1> ping 192.168.30.10
*192.168.10.1 icmp_seq=1 ttl=255 time=1.620 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.10.1 icmp_seq=2 ttl=255 time=1.261 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.10.1 icmp_seq=3 ttl=255 time=0.587 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.10.1 icmp_seq=4 ttl=255 time=0.526 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.10.1 icmp_seq=5 ttl=255 time=0.532 ms (ICMP type:3, code:1, Destination host unreachable)
```

WARNING - Remote forwarding is intentionally unavailable because the routing exercise is not configured yet.

Actual CLI output - PC3

```
PC3> show ip
NAME        : PC3[1]
IP/MASK     : 192.168.30.10/24
GATEWAY     : 192.168.30.1
MAC         : 00:50:79:66:68:05
LPORT       : 20000
RHOST:PORT  : 127.0.0.1:30000
MTU         : 1500
```

Actual CLI output - PC3

```
PC3> ping 192.168.30.1
192.168.30.1 icmp_seq=1 timeout
84 bytes from 192.168.30.1 icmp_seq=2 ttl=255 time=0.555 ms
84 bytes from 192.168.30.1 icmp_seq=3 ttl=255 time=1.122 ms
84 bytes from 192.168.30.1 icmp_seq=4 ttl=255 time=1.507 ms
84 bytes from 192.168.30.1 icmp_seq=5 ttl=255 time=0.617 ms
```

WARNING - Initial local probes may precede neighbor resolution; repeat and require five replies.

11. Phase B — Build Authenticated OSPFv2

The process configuration establishes identity, a default passive posture, approved transit interfaces, and the area authentication mode. Interface commands then activate OSPF, select point-to-point behavior on the transit links, and apply the matching message-digest key.

Configure R1

R1 — OSPFv2 process 10

```
enable
conf t
router ospf 10
router-id 1.1.1.1
passive-interface default
no passive-interface Ethernet0/0
area 0 authentication message-digest
exit
interface Loopback0
ip ospf 10 area 0
interface Ethernet0/0
ip ospf network point-to-point
ip ospf message-digest-key 1 md5 ENARSI-LAB01
ip ospf 10 area 0
interface Ethernet0/1
ip ospf 10 area 0
end
```

Configure R2

R2 — OSPFv2 process 10

```
enable
conf t
router ospf 10
router-id 2.2.2.2
passive-interface default
no passive-interface Ethernet0/0
no passive-interface Ethernet0/1
area 0 authentication message-digest
exit
interface Loopback0
ip ospf 10 area 0
interface Ethernet0/0
ip ospf network point-to-point
ip ospf message-digest-key 1 md5 ENARSI-LAB01
ip ospf 10 area 0
interface Ethernet0/1
ip ospf network point-to-point
ip ospf message-digest-key 1 md5 ENARSI-LAB01
ip ospf 10 area 0
end
```

Configure R3

R3 — OSPFv2 process 10

```
enable
conf t
router ospf 10
router-id 3.3.3.3
passive-interface default
no passive-interface Ethernet0/0
area 0 authentication message-digest
exit
interface Loopback0
ip ospf 10 area 0
interface Ethernet0/0
ip ospf network point-to-point
ip ospf message-digest-key 1 md5 ENARSI-LAB01
ip ospf 10 area 0
interface Ethernet0/1
ip ospf 10 area 0
end
```

12. Immediate OSPF Verification

Start with the neighbor table. R1 and R3 should each see one FULL neighbor. R2 should see two. Because the transit links use point-to-point OSPF network behavior, the state is FULL/- rather than FULL/DR or FULL/BDR.

Neighbor verification

```
R1# show ip ospf neighbor
R2# show ip ospf neighbor
R3# show ip ospf neighbor
```

Actual CLI output - R1

```
R1# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           0   FULL/  -        00:00:34    10.12.12.2      Ethernet0/0
```

Actual CLI output - R2

```
R2# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           0   FULL/  -        00:00:33    10.23.23.2      Ethernet0/1
1.1.1.1           0   FULL/  -        00:00:37    10.12.12.1      Ethernet0/0
```

Actual CLI output - R3

```
R3# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           0   FULL/  -        00:00:38    10.23.23.1      Ethernet0/0
```

Verify interface-level facts

These commands confirm the area, process, network type, timers, cost, passive state, and authentication behavior on the actual interface.

OSPF interface evidence

```
R1# show ip ospf interface Ethernet0/0
R2# show ip ospf interface brief
R3# show ip ospf interface Ethernet0/0
```

Actual CLI output - R1

```
R1# show ip ospf interface Ethernet0/0
Ethernet0/0 is up, line protocol is up
  Internet Address 10.12.12.1/30, Interface ID 2, Area 0
  Process ID 10, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 10
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Cryptographic authentication enabled
    Youngest key id is 1
```

Actual CLI output - R2

```
R2# show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Lo0          10    0               2.2.2.2/32         1     LOOP  0/0
Et0/1        10    0               10.23.23.1/30      10    P2P   1/1
Et0/0        10    0               10.12.12.2/30      10    P2P   1/1
```

Actual CLI output - R2

```
R2# show ip ospf interface Ethernet0/1
Ethernet0/1 is up, line protocol is up
  Internet Address 10.23.23.1/30, Interface ID 3, Area 0
  Process ID 10, Router ID 2.2.2.2, Network Type POINT_TO_POINT, Cost: 10
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 3.3.3.3
  Cryptographic authentication enabled
    Youngest key id is 1
```

Actual CLI output - R3

```
R3# show ip ospf interface Ethernet0/0
Ethernet0/0 is up, line protocol is up
  Internet Address 10.23.23.2/30, Interface ID 2, Area 0
  Process ID 10, Router ID 3.3.3.3, Network Type POINT_TO_POINT, Cost: 10
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Cryptographic authentication enabled
    Youngest key id is 1
```

Read Area 0, Process ID 10, POINT_TO_POINT, Hello 10/Dead 40 and key ID 1. Cryptographic authentication enabled confirms the mode; successful FULL adjacency additionally proves peer compatibility. Selected interface lines are shown verbatim; unrelated platform details are omitted.

Verify routes

R1 must learn the Branch 3 LAN and R3 loopback through R2. R3 must learn the Branch 1 LAN and R1 loopback. The route code O denotes an intra-area OSPF route.

Route verification

```
R1# show ip route ospf
R1# show ip route 192.168.30.0
R3# show ip route ospf
R3# show ip route 192.168.10.0
```

Actual CLI output - R1

```
R1# show ip route ospf
Gateway of last resort is not set
      2.0.0.0/32 is subnetted, 1 subnets
O        2.2.2.2 [110/11] via 10.12.12.2, 00:00:48, Ethernet0/0
      3.0.0.0/32 is subnetted, 1 subnets
O        3.3.3.3 [110/21] via 10.12.12.2, 00:00:45, Ethernet0/0
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O        10.23.23.0/30 [110/20] via 10.12.12.2, 00:00:47, Ethernet0/0
O     192.168.30.0/24 [110/30] via 10.12.12.2, 00:00:45, Ethernet0/0
```

Actual CLI output - R1

```
R1# show ip route 192.168.30.0
Routing entry for 192.168.30.0/24
  Known via "ospf 10", distance 110, metric 30, type intra area
  Last update from 10.12.12.2 on Ethernet0/0, 00:00:45 ago
  Routing Descriptor Blocks:
  * 10.12.12.2, from 3.3.3.3, 00:00:45 ago, via Ethernet0/0
      Route metric is 30, traffic share count is 1
```

Actual CLI output - R3

```
R3# show ip route ospf
Gateway of last resort is not set
      1.0.0.0/32 is subnetted, 1 subnets
O        1.1.1.1 [110/21] via 10.23.23.1, 00:00:48, Ethernet0/0
      2.0.0.0/32 is subnetted, 1 subnets
O        2.2.2.2 [110/11] via 10.23.23.1, 00:00:48, Ethernet0/0
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O        10.12.12.0/30 [110/20] via 10.23.23.1, 00:00:48, Ethernet0/0
O     192.168.10.0/24 [110/30] via 10.23.23.1, 00:00:48, Ethernet0/0
```

Actual CLI output - R3

```
R3# show ip route 192.168.10.0
Routing entry for 192.168.10.0/24
  Known via "ospf 10", distance 110, metric 30, type intra area
  Last update from 10.23.23.1 on Ethernet0/0, 00:00:48 ago
  Routing Descriptor Blocks:
  * 10.23.23.1, from 1.1.1.1, 00:00:48 ago, via Ethernet0/0
      Route metric is 30, traffic share count is 1
```

Verify passive LAN behavior

The branch LANs must be advertised but must not send OSPF Hellos. The passive-interface display should include Ethernet0/1 on R1 and R3. No OSPF neighbor should appear on those interfaces.

Passive-interface verification

```
R1# show ip protocols
R3# show ip protocols
```

Actual CLI output - R1

```
R1# show ip protocols
Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Routing on Interfaces Configured Explicitly (Area 0):
    Loopback0
    Ethernet0/1
    Ethernet0/0
  Passive Interface(s):
    Ethernet0/1
    Ethernet0/2
    Ethernet0/3
    Loopback0
    SR0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      00:00:45
    2.2.2.2              110      00:00:47
  Distance: (default is 110)
```

WARNING - Passive suppresses Hellos; exclude every transit that must form a router adjacency.

Actual CLI output - R3

```
R3# show ip protocols
Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Routing on Interfaces Configured Explicitly (Area 0):
    Loopback0
    Ethernet0/1
    Ethernet0/0
  Passive Interface(s):
    Ethernet0/1
    Ethernet0/2
    Ethernet0/3
    Loopback0
    SR0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:00:47
    2.2.2.2              110      00:00:47
  Distance: (default is 110)
```

WARNING - Passive suppresses Hellos; exclude every transit that must form a router adjacency.

Check the OSPF passive list includes Loopback0 and Ethernet0/1 on each branch router; Ethernet0/0 must be absent. The unrelated application routing-protocol section is omitted from the excerpts.

13. End-to-End Validation

Control-plane success is necessary but not sufficient. Test traffic from each client so the forward route, reverse route, router interfaces, and default gateways are all exercised.

Client forwarding tests

```
PC1> ping 192.168.30.10
PC1> trace 192.168.30.10
PC3> ping 192.168.10.10
PC3> trace 192.168.10.10
```

Actual CLI output - PC1

```
PC1> show ip
NAME        : PC1[1]
IP/MASK     : 192.168.10.10/24
GATEWAY     : 192.168.10.1
MAC         : 00:50:79:66:68:04
LPORT       : 20000
RHOST:PORT  : 127.0.0.1:30000
MTU         : 1500
```

Actual CLI output - PC1

```
PC1> ping 192.168.30.10
84 bytes from 192.168.30.10 icmp_seq=1 ttl=61 time=1.392 ms
84 bytes from 192.168.30.10 icmp_seq=2 ttl=61 time=2.834 ms
84 bytes from 192.168.30.10 icmp_seq=3 ttl=61 time=1.631 ms
84 bytes from 192.168.30.10 icmp_seq=4 ttl=61 time=1.572 ms
84 bytes from 192.168.30.10 icmp_seq=5 ttl=61 time=1.303 ms
```

Actual CLI output - PC1

```
PC1> ping 192.168.30.10
84 bytes from 192.168.30.10 icmp_seq=1 ttl=61 time=3.280 ms
84 bytes from 192.168.30.10 icmp_seq=2 ttl=61 time=1.347 ms
84 bytes from 192.168.30.10 icmp_seq=3 ttl=61 time=1.044 ms
84 bytes from 192.168.30.10 icmp_seq=4 ttl=61 time=1.146 ms
84 bytes from 192.168.30.10 icmp_seq=5 ttl=61 time=1.794 ms
```

Actual CLI output - PC1

```
PC1> trace 192.168.30.10
trace to 192.168.30.10, 8 hops max, press Ctrl+C to stop
 1   192.168.10.1   0.553 ms  0.594 ms  0.936 ms
 2   10.12.12.2   1.181 ms  0.971 ms  2.731 ms
 3   10.23.23.2   3.106 ms  1.181 ms  0.990 ms
 4   *192.168.30.10   1.513 ms (ICMP type:3, code:3, Destination port unreachable)
```

WARNING - VPCS replies with UDP port-unreachable at the destination; this normally ends the trace.

Actual CLI output - PC3

```
PC3> show ip
NAME        : PC3[1]
IP/MASK     : 192.168.30.10/24
GATEWAY     : 192.168.30.1
MAC         : 00:50:79:66:68:05
LPORT       : 20000
RHOST:PORT  : 127.0.0.1:30000
MTU         : 1500
```

Actual CLI output - PC3

```
PC3> ping 192.168.10.10
84 bytes from 192.168.10.10 icmp_seq=1 ttl=61 time=1.304 ms
84 bytes from 192.168.10.10 icmp_seq=2 ttl=61 time=1.987 ms
84 bytes from 192.168.10.10 icmp_seq=3 ttl=61 time=2.549 ms
84 bytes from 192.168.10.10 icmp_seq=4 ttl=61 time=3.303 ms
84 bytes from 192.168.10.10 icmp_seq=5 ttl=61 time=2.095 ms
```

Actual CLI output - PC3

```
PC3> ping 192.168.10.10
84 bytes from 192.168.10.10 icmp_seq=1 ttl=61 time=3.551 ms
84 bytes from 192.168.10.10 icmp_seq=2 ttl=61 time=1.487 ms
84 bytes from 192.168.10.10 icmp_seq=3 ttl=61 time=1.824 ms
84 bytes from 192.168.10.10 icmp_seq=4 ttl=61 time=1.704 ms
84 bytes from 192.168.10.10 icmp_seq=5 ttl=61 time=1.513 ms
```

Actual CLI output - PC3

```
PC3> trace 192.168.10.10
trace to 192.168.10.10, 8 hops max, press Ctrl+C to stop
 1   192.168.30.1   1.080 ms  0.506 ms  0.487 ms
 2   10.23.23.1   0.980 ms  0.789 ms  0.636 ms
 3   10.12.12.1   1.154 ms  1.176 ms  1.641 ms
 4   *192.168.10.10   1.575 ms (ICMP type:3, code:3, Destination port unreachable)
```

WARNING - VPCS replies with UDP port-unreachable at the destination; this normally ends the trace.

Compare NAME, IP/MASK and GATEWAY with the addressing table. Require five replies in each direction. In the UDP trace, the final VPCS port-unreachable reply identifies arrival at the endpoint; it is not a failed ping.

Save only after validation

Saving before validation can preserve a faulty state. When every checklist item passes, save each router and each VPCS configuration.

Persist the verified state

```
R1# write memory
R2# write memory
R3# write memory
PC1> save
PC3> save
```

Actual CLI output - R1

```
R1# write memory
Building configuration...
[OK]
```

Actual CLI output - R2

```
R2# write memory
Building configuration...
[OK]
```

Actual CLI output - R3

```
R3# write memory
Building configuration...
[OK]
```

Actual CLI output - PC1

```
PC1> save
Saving startup configuration to startup.vpc
.  done
```

Actual CLI output - PC3

```
PC3> save
Saving startup configuration to startup.vpc
.  done
```

14. Expected Final State

• R1–R2 and R2–R3 OSPF neighbors are FULL/-.

• All OSPF-enabled interfaces belong to process 10 and area 0.

• Transit interfaces use point-to-point OSPF network behavior.

• Area 0 message-digest authentication is active with matching key ID 1 on each transit link.

• Branch LAN interfaces are passive but their /24 prefixes are advertised.

• R1 and R3 install the remote branch /24 as an OSPF intra-area route.

• PC1 and PC3 reach each other in both directions.

15. Common Failures and Diagnostic Reasoning

These are guided diagnostic cases, not a separate Incident workbook. They have been tested during production validation and restored before release.

Symptom	Likely cause	Evidence	Minimal correction
Neighbor remains DOWN/INIT	Interface or Hello path problem	Interface state, direct ping, debug Hello	Restore link/IP and confirm multicast reception
Authentication errors; no FULL state	Mode, key ID, or key mismatch	OSPF interface auth details and logs	Match area mode and interface key on both ends
No neighbor on an up/up transit	Transit accidentally passive	show ip protocols	no passive-interface on the approved transit
Neighbor FULL but branch route absent	LAN not activated in OSPF	show ip ospf interface and LSDB/route	Enable OSPF on the LAN interface; keep it passive
Route present but client ping fails	Gateway, host address, ACL, or return path	VPCS show ip, router route/ARP	Correct the failed data-plane prerequisite

Authentication mismatch workflow

If R2–R3 fails while R1–R2 remains healthy, scope the fault to the R2–R3 link. Confirm direct ping, compare show ip ospf interface output, check the area authentication mode, and compare the configured key ID/value. Restore only the mismatched key; do not rebuild the whole process.

Focused evidence collection

```
R2# show ip ospf neighbor
R2# show ip ospf interface Ethernet0/1
R2# show running-config interface Ethernet0/1
R3# show ip ospf interface Ethernet0/0
R3# show running-config interface Ethernet0/0
```

Actual controlled validation case: only R3's transit key was deliberately changed. The snapshots below show the resulting symptom; the production build uses the matching key and must remain healthy.

Actual CLI output - R2

```
R2# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           0   FULL/  -        00:00:39    10.12.12.1      Ethernet0/0
```

Actual CLI output - R2

```
R2# show ip ospf interface Ethernet0/1
Ethernet0/1 is up, line protocol is up
  Internet Address 10.23.23.1/30, Interface ID 3, Area 0
  Process ID 10, Router ID 2.2.2.2, Network Type POINT_TO_POINT, Cost: 10
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Neighbor Count is 0, Adjacent neighbor count is 0
  Cryptographic authentication enabled
    Youngest key id is 1
```

ERROR - The deliberately introduced fault prevents the required full adjacency on this transit.

Actual CLI output - R2

```
R2# show running-config interface Ethernet0/1
Building configuration...
Current configuration : 185 bytes
!
interface Ethernet0/1
 description TO_R3
 ip address 10.23.23.1 255.255.255.252
 ip ospf message-digest-key 1 md5 ENARSI-LAB01
 ip ospf network point-to-point
 ip ospf 10 area 0
end
```

Actual CLI output - R2

```
R2# show ip route 192.168.30.0
% Network not in table
```

ERROR - The deliberately mismatched OSPF key prevents the R2-R3 adjacency and remote route.

Actual CLI output - R3

```
R3# show ip ospf neighbor
```

Actual CLI output - R3

```
R3# show ip ospf interface Ethernet0/0
Ethernet0/0 is up, line protocol is up
  Internet Address 10.23.23.2/30, Interface ID 2, Area 0
  Process ID 10, Router ID 3.3.3.3, Network Type POINT_TO_POINT, Cost: 10
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Neighbor Count is 0, Adjacent neighbor count is 0
  Cryptographic authentication enabled
    Youngest key id is 1
```

ERROR - The deliberately introduced fault prevents the required full adjacency on this transit.

Actual CLI output - R3

```
R3# show running-config interface Ethernet0/0
Building configuration...
Current configuration : 184 bytes
!
interface Ethernet0/0
 description TO_R2
 ip address 10.23.23.2 255.255.255.252
 ip ospf message-digest-key 1 md5 WRONG-LAB01
 ip ospf network point-to-point
 ip ospf 10 area 0
end
```

ERROR - This intentionally wrong key differs from the R2 key and prevents authenticated adjacency.

Actual CLI output - R3

```
R3# show ip route 192.168.30.0
Routing entry for 192.168.30.0/24, 2 known subnets
  Attached (2 connections)
  Variably subnetted with 2 masks
C        192.168.30.0/24 is directly connected, Ethernet0/1
L        192.168.30.1/32 is directly connected, Ethernet0/1
```

Recovery: restore the matching key on R3 Ethernet0/0, wait 45 seconds, and verify both neighbors and the remote branch route.

Actual CLI output - R2

```
R2# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           0   FULL/  -        00:00:33    10.23.23.2      Ethernet0/1
1.1.1.1           0   FULL/  -        00:00:31    10.12.12.1      Ethernet0/0
```

Actual CLI output - R2

```
R2# show ip route 192.168.30.0
Routing entry for 192.168.30.0/24
  Known via "ospf 10", distance 110, metric 20, type intra area
  Last update from 10.23.23.2 on Ethernet0/1, 00:00:44 ago
  Routing Descriptor Blocks:
  * 10.23.23.2, from 3.3.3.3, 00:00:44 ago, via Ethernet0/1
      Route metric is 20, traffic share count is 1
```

Accidentally passive transit workflow

A passive transit interface sends no Hello packets. The interface can remain up/up and the subnet can remain in the LSDB, so physical checks alone will not find the cause. Use show ip protocols to inspect the passive list, then remove only the unintended passive setting.

Minimal recovery

```
R2# show ip protocols
R2# conf t
R2(config)# router ospf 10
R2(config-router)# no passive-interface Ethernet0/1
R2(config-router)# end
R2# show ip ospf neighbor
```

Actual controlled validation case: R2 Ethernet0/1 was made passive, then restored using the minimal recovery above.

Actual CLI output - R2

```
R2# show ip protocols
Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Routing on Interfaces Configured Explicitly (Area 0):
    Loopback0
    Ethernet0/1
    Ethernet0/0
  Passive Interface(s):
    Ethernet0/1
    Ethernet0/2
    Ethernet0/3
    Loopback0
    SR0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      00:01:34
    1.1.1.1              110      00:03:38
  Distance: (default is 110)
```

ERROR - R2 Ethernet0/1 is a router transit; making it passive suppresses the required OSPF Hellos.

WARNING - Passive suppresses Hellos; exclude every transit that must form a router adjacency.

Actual CLI output - R2

```
R2# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           0   FULL/  -        00:00:37    10.12.12.1      Ethernet0/0
```

Actual CLI output - R2

```
R2# show ip route 192.168.30.0
% Network not in table
```

ERROR - The deliberately passive R2-R3 transit suppresses Hellos and removes the remote route.

Actual CLI output - PC1

```
PC1> ping 192.168.30.10
*192.168.10.1 icmp_seq=1 ttl=255 time=0.561 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.10.1 icmp_seq=2 ttl=255 time=0.615 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.10.1 icmp_seq=3 ttl=255 time=0.787 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.10.1 icmp_seq=4 ttl=255 time=1.422 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.10.1 icmp_seq=5 ttl=255 time=0.753 ms (ICMP type:3, code:1, Destination host unreachable)
```

ERROR - The deliberately passive R2-R3 transit suppresses Hellos and removes the remote route.

Actual CLI output - R2

```
R2# show ip protocols
Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Routing on Interfaces Configured Explicitly (Area 0):
    Loopback0
    Ethernet0/1
    Ethernet0/0
  Passive Interface(s):
    Ethernet0/2
    Ethernet0/3
    Loopback0
    SR0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      00:00:45
    1.1.1.1              110      00:04:29
  Distance: (default is 110)
```

WARNING - Passive suppresses Hellos; exclude every transit that must form a router adjacency.

Actual CLI output - R2

```
R2# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           0   FULL/  -        00:00:36    10.23.23.2      Ethernet0/1
1.1.1.1           0   FULL/  -        00:00:33    10.12.12.1      Ethernet0/0
```

Actual CLI output - R2

```
R2# show ip route 192.168.30.0
Routing entry for 192.168.30.0/24
  Known via "ospf 10", distance 110, metric 20, type intra area
  Last update from 10.23.23.2 on Ethernet0/1, 00:00:45 ago
  Routing Descriptor Blocks:
  * 10.23.23.2, from 3.3.3.3, 00:00:45 ago, via Ethernet0/1
      Route metric is 20, traffic share count is 1
```

16. Final Validation Checklist

ID	Assertion	Required evidence	Result
V01	All required interfaces are up/up	show ip interface brief	PASS
V02	Direct transit pings succeed	R1↔R2 and R2↔R3 ping	PASS

ID	Assertion	Required evidence	Result
V03	R2 has two FULL/- neighbors	show ip ospf neighbor	PASS
V04	Message-digest auth is active	show ip ospf interface	PASS
V05	Only transit interfaces are non-passive	show ip protocols	PASS
V06	Remote /24 routes are OSPF intra-area	show ip route ospf	PASS
V07	PC1 reaches PC3 and reverse	VPCS ping	PASS
V08	Auth mismatch symptom/recovery verified	validation evidence	PASS
V09	Passive transit symptom/recovery verified	validation evidence	PASS
V10	Post-recovery regression passed	full checklist rerun	PASS

Release status: FINAL / LIVE VALIDATED — PASS

17. Key Takeaways

• A FULL neighbor is a result of compatible parameters, not merely an enabled routing process.

• Use a default-passive posture and explicitly approve only router-to-router adjacencies.

• Authentication protects OSPF packets; it does not encrypt application traffic.

• Verify in layers: interface → direct reachability → OSPF interface → neighbor → route → forwarding.

• A production change is complete only after failure recovery and regression checks also pass.

18. Validation Record

Tests validated RAW construction, the IP-only starting state and the complete save-config on EVE-NG 6.2.0-4 with the approved IOL L3 image and VPCS. Required FULL adjacencies, MD5 authentication, passive LAN policy, branch routes, explicit PC1/PC3 names, bidirectional five-reply pings, trace paths and both controlled fault/recovery cases passed. The complete save-config was independently cold-booted and verified without configuration entry. CLI excerpts are genuine output from their stated exercise stages.

Validated artifacts

Artifact	Contract
RAW UNL	Correct topology; no baseline or OSPF solution
save-ip-configuration UNL	Identical topology; named devices and addressing only; no OSPF solution
save-config UNL	Complete healthy configuration; independently cold-booted and verified without configuration entry
Workbook	RAW and IP-baseline workflows exercised; CLI excerpts are captured from their stated stage
Failure tests	Authentication mismatch and passive transit restored and regression-tested