DDANEP CCNA

Enterprise HQ-Branch Lab

As-Built Configuration, Validation and Troubleshooting Record

CLASSIFICATION	TIER 3 - Integrated multi-domain practical lab
PLATFORM	Cisco Packet Tracer
AUTHOR	David Dela Nuwordu
AS-BUILT DATE	13 October 2026
STATUS	Operational and evidence-validated

Publication-safe edition: authentication secrets and password hashes are intentionally excluded.

1. Document control and executive summary

Purpose	Record the final implemented state, validation evidence and troubleshooting lessons for a multi-site CCNA enterprise lab.
Scope	HQ campus switching and routing, branch router-on-a-stick, ISP/public server, OSPF, DHCP relay, PAT, ACLs, SSH and port security.

Executive summary

The completed lab joins an HQ campus, a branch LAN and a simulated ISP. The HQ multilayer switch provides inter-VLAN routing, the edge router originates the OSPF default route and performs PAT, and the branch uses router-on-a-stick. A central DHCP/DNS service supports both sites through DHCP relay. Security controls include guest isolation, SSH-only management, sticky port security, BPDU Guard on endpoint ports, an unused-port parking VLAN and a black-hole native VLAN.

> **Acceptance outcome: end-to-end routing, DHCP relay, DNS, HTTP, OSPF default-route propagation, PAT, guest policy and access-port security were demonstrated with command output and endpoint tests.**

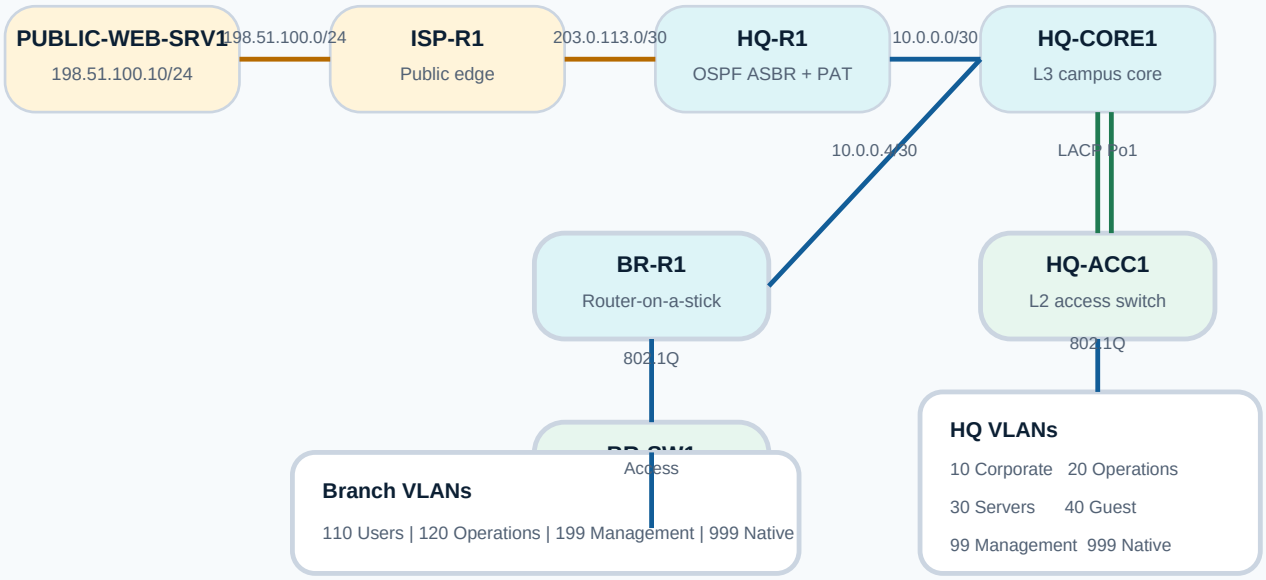
Tier classification

Tier 3 is appropriate because the exercise integrates multiple devices and technology domains, requires dependency-aware troubleshooting, and validates business-style policy rather than a single command objective.

Contents

Section	Topic
2	Logical topology and design intent
3	Addressing and VLAN plan
4	Layer 2 implementation
5	Layer 3 and OSPF
6	IP services and Internet edge
7	Security controls
8	Troubleshooting record
9	Acceptance tests
10	Operations runbook and known variances
11	CCNA exam review

2. Logical topology and design intent



All routed internal links participate in OSPF area 0; the ISP remains outside OSPF.

Device	Role	Primary responsibility
HQ-CORE1	Layer 3 campus core	SVIs, inter-VLAN routing, OSPF, guest ACL, DHCP relay
HQ-ACC1	HQ access switch	Endpoint VLANs, LACP, trunking, sticky port security
HQ-R1	Enterprise edge	OSPF ASBR, static default route, PAT to ISP
BR-R1	Branch router	Router-on-a-stick, DHCP relay, OSPF
BR-SW1	Branch access switch	Branch VLAN access, trunking, sticky port security
ISP-R1	Simulated ISP	Public transit and connected public server network

Design intent

- Keep the ISP outside the internal OSPF domain.
- Advertise one default route from HQ-R1 to the entire enterprise.
- Use PAT so all internal clients share 203.0.113.1 for public access.
- Centralize DHCP and DNS at 192.168.30.10 while relaying requests across routed boundaries.
- Isolate guest clients from private networks while allowing defined infrastructure services and public access.

3. Addressing and VLAN plan

Node	Interface	IPv4	Purpose
HQ-CORE1	Gi0/1	10.0.0.1/30	Routed link to HQ-R1
HQ-CORE1	Vlan10	192.168.10.1/24	Corporate gateway
HQ-CORE1	Vlan20	192.168.20.1/24	Operations gateway
HQ-CORE1	Vlan30	192.168.30.1/24	Server gateway
HQ-CORE1	Vlan40	192.168.40.1/24	Guest gateway and ACL ingress
HQ-CORE1	Vlan99	192.168.99.1/24	HQ management gateway
HQ-ACC1	Vlan99	192.168.99.11/24	Switch management
HQ-R1	Gi0/0	203.0.113.1/30	ISP link and PAT outside
HQ-R1	Gi0/1	10.0.0.2/30	HQ-CORE1 and NAT inside
HQ-R1	Gi0/2	10.0.0.5/30	BR-R1 and NAT inside
ISP-R1	Gi0/0	203.0.113.2/30	Enterprise-facing ISP link
ISP-R1	Gi0/1	198.51.100.1/24	Public server gateway
BR-R1	Gi0/1.110	192.168.110.1/24	Branch users gateway
BR-R1	Gi0/1.120	192.168.120.1/24	Branch operations gateway
BR-R1	Gi0/1.199	192.168.199.1/24	Branch management gateway
BR-R1	Gi0/2	10.0.0.6/30	HQ-R1 routed link
BR-SW1	Vlan199	192.168.199.11/24	Switch management
HQ-INFRA-SRV1	Fa0	192.168.30.10/24	DHCP and DNS
PUBLIC-WEB-SRV1	Fa0	198.51.100.10/24	Public HTTP service

3. Addressing and VLAN plan (continued)

VLAN catalogue

VLAN	Name	Site	Subnet / treatment
10	CORPORATE	HQ	192.168.10.0/24
20	OPERATIONS	HQ	192.168.20.0/24
30	SERVERS	HQ	192.168.30.0/24
40	GUEST	HQ	192.168.40.0/24
99	MANAGEMENT	HQ	192.168.99.0/24
110	BR-USERS	Branch	192.168.110.0/24
120	BR-OPERATIONS	Branch	192.168.120.0/24
199	BR-MANAGEMENT	Branch	192.168.199.0/24
998	UNUSED-PORTS	Both	No routed service
999	NATIVE-BLACKHOLE	Both	No routed service

4. Layer 2 implementation

HQ EtherChannel and trunk

HQ-CORE1 and HQ-ACC1 use LACP Port-channel1 across Fa0/23 and Fa0/24. The core is active and the access switch is passive. The bundle operates as a Layer 2 trunk with native VLAN 999 and allowed VLANs 10,20,30,40,99,999.

```
HQ-ACC1# show etherchannel summary
1 Po1(SU) LACP Fa0/23(P) Fa0/24(P)

Native VLAN: 999
Allowed: 10,20,30,40,99,999
```

Branch trunk

BR-SW1 Gi0/1 is a static 802.1Q trunk to BR-R1. It carries VLANs 110,120,199,999, uses VLAN999 as the native black-hole VLAN, and disables DTP negotiation.

Access edge controls

Control	As-built implementation
Endpoint mode	Static access VLAN assignments
Loop protection	PortFast and BPDU Guard on endpoint-facing ports
Identity binding	Sticky MAC learning, maximum 1 secure MAC
Violation response	Restrict - drops violating traffic without shutting the port
Unused ports	VLAN998, descriptive label, administratively shut down
Native VLAN	VLAN999, no routed service

Verified state: HQ Po1(SU), both members in (P), HQ Fa0/1-6 and branch Fa0/1-3 Secure-up with one sticky MAC each and zero violations.

5. Layer 3 routing and OSPF

Device	Router ID	Adjacency links	Advertised networks	Default role
HQ-CORE1	1.1.1.1	Gi0/1	HQ VLANs and 10.0.0.0/30	Learns O*E2 default
HQ-R1	2.2.2.2	Gi0/1, Gi0/2	10.0.0.0/30 and 10.0.0.4/30	Originates default
BR-R1	3.3.3.3	Gi0/2	Branch VLANs and 10.0.0.4/30	Learns O*E2 default

Default-route design

```
HQ-R1
ip route 0.0.0.0 0.0.0.0 203.0.113.2
router ospf 10
default-information originate

HQ-CORE1 learned: O*E2 0.0.0.0/0 via 10.0.0.2
BR-R1 learned: O*E2 0.0.0.0/0 via 10.0.0.5
```

The ISP link is deliberately excluded from OSPF. During the audit, a stale default route and default-information command were removed from HQ-CORE1 so that HQ-R1 remains the sole default-route originator.

> **OSPF acceptance evidence: HQ-R1 and BR-R1 reached FULL adjacency, internal routes populated both directions, and the Type-5 default LSA was advertised only by router ID 2.2.2.2.**

6. IP services and Internet edge

DHCP and DNS

Pool	Start address	Gateway	DNS
CORPORATE	192.168.10.100	192.168.10.1	192.168.30.10
OPERATIONS	192.168.20.100	192.168.20.1	192.168.30.10
GUEST	192.168.40.100	192.168.40.1	192.168.30.10
BR-USERS-110	192.168.110.100	192.168.110.1	192.168.30.10
BR-OPS-120	192.168.120.100	192.168.120.1	192.168.30.10

DHCP relay is configured on the routed client gateways. VLAN30 hosts the server directly, while management VLANs use static addressing. DNS resolution to the campus service was verified.

PAT implementation

```
access-list 1 permit 192.168.0.0 0.0.255.255
interface Gi0/0
ip nat outside
interface Gi0/1
ip nat inside
interface Gi0/2
ip nat inside
ip nat inside source list 1 interface Gi0/0 overload
```

Inside local	Inside global	Outside global	Observed use
192.168.120.100	203.0.113.1:1024	198.51.100.10:80	Branch HTTP
192.168.10.100	203.0.113.1:1025	198.51.100.10:80	HQ HTTP

PAT evidence: active TCP translations, ACL 1 match counters, NAT hits, successful ICMP and HTTP from HQ, branch and guest clients.

7. Security controls

Guest policy

Function	Policy	Purpose
DHCP	Permit UDP bootpc to bootps	Client address assignment
DNS	Permit UDP/TCP to 192.168.30.10:53	Name resolution
Campus web	Permit TCP to 192.168.30.10:80/443	Approved service
Diagnostics	Permit ICMP echo to 192.168.30.10	Approved infrastructure test
Private networks	Deny 192.168.40.0/24 to 192.168.0.0/16	Guest isolation
Public access	Permit remaining IP traffic	Internet through PAT

```
Observed counters after tests
permit ICMP to 192.168.30.10: 4 matches
deny private destinations: 4 matches
permit public destinations: 17 matches
```

Management and access hardening

Control	Implementation
SSH	Version 2, local authentication, Telnet disabled
HQ management ACL	SSH sources restricted to VLAN20 and VLAN99 on HQ-CORE1 and HQ-ACC1
Port security	Sticky MAC, maximum 1, violation restrict
Unused interfaces	Moved to VLAN998 and administratively shut down
Native VLAN	VLAN999 black-hole treatment
Credentials	Excluded from this publication-safe document

8. Troubleshooting record

Symptom	Root cause	Corrective action	Evidence
No internal default route	HQ-R1 had not yet originated a default	Added ISP static default, then OSPF default-information originate	O*E2 installed at HQ-CORE1 and BR-R1
PAT failed for every endpoint	Gi0/0 was mistakenly classified as NAT inside	Removed inside role and applied ip nat outside	Outside Gi0/0; inside Gi0/1 and Gi0/2
HQ-R1 could reach ISP but not public server	Public server gateway was 192.51.100.1 instead of 198.51.100.1	Corrected the server default gateway	HQ-R1 and clients reached 198.51.100.10
Branch switch could not manage through expected SVI	Management address was initially placed under the wrong SVI	Moved management to VLAN199 and disabled VLAN999 SVI	Vlan199 192.168.199.11 up/up
Sticky address table initially empty	No source frames arrived after enabling sticky learning	Generated endpoint traffic	One SecureSticky MAC learned per access port
HQ core had stale Internet statements	Static default and default-originate were present on the wrong device	Removed both from HQ-CORE1	Only router ID 2.2.2.2 advertises the default
Guest policy verification	Need proof of both permit and deny behavior	Tested public, management and infrastructure destinations	ACL counters matched intended results

8. Troubleshooting record (continued)

> **Troubleshooting principle demonstrated: establish the failure boundary, verify the forwarding path in both directions, change one variable, and prove recovery with independent evidence.**

Operational lesson

A same-subnet ping can succeed even when a host has the wrong default gateway. The public server could reach ISP-R1 locally, but it could not return traffic to HQ until its gateway was corrected. This was the decisive clue in the Internet-path fault.

9. Acceptance tests

Test	Method	Acceptance evidence	Result
HQ EtherChannel	show etherchannel summary	Po1(SU), Fa0/23(P), Fa0/24(P)	PASS
HQ trunk	show interfaces trunk	Native 999; required VLANs forwarding	PASS
Branch trunk	show interfaces trunk	110,120,199,999 active and forwarding	PASS
HQ inter-VLAN	Endpoint pings	VLAN gateways and permitted VLANs reachable	PASS
Branch routing	Branch to 192.168.30.10	Replies received; TTL 125	PASS
OSPF	show ip ospf neighbor	FULL adjacency across both routed links	PASS
Default propagation	show ip route 0.0.0.0	O*E2 at core and branch	PASS
DHCP relay	Client DHCP request	Branch VLAN120 received 192.168.120.100	PASS
PAT	show ip nat translations	HQ and branch HTTP translations present	PASS
Public HTTP	Browser to 198.51.100.10	Page rendered from HQ, branch and guest	PASS
Guest isolation	Ping management destination	Rejected by 192.168.40.1; deny counter incremented	PASS
Guest exception	Ping 192.168.30.10	Replies received; permit counter incremented	PASS
Port security	show port-security	One sticky MAC per used port; zero violations	PASS

Overall acceptance status: PASS. The implemented forwarding, services and policy controls met the lab objectives at the time of final validation.

10. Operations runbook and known variances

Rapid verification sequence

Step	Domain	Primary checks
1	Physical and VLAN state	show ip interface brief; show interfaces status; show vlan brief
2	Trunks and bundles	show interfaces trunk; show etherchannel summary
3	Routing	show ip ospf neighbor; show ip route; show ip route 0.0.0.0
4	DHCP and DNS	ipconfig /all; ping 192.168.30.10; test configured hostname
5	Security policy	show access-lists GUEST-IN; show port-security; show port-security address
6	Internet edge	show ip nat translations; show ip nat statistics; browse 198.51.100.10

Known non-blocking variances

Item	Recorded status
Management identity	Packet Tracer authentication behavior led to retaining the known-working ddanep-admin account on selected devices. Standardization is deferred.
Domain names	hqcampus.local, ddanep.lab and ddanep.local remain mixed. Changing domain names can alter RSA key naming; treat as a controlled future change.
VTY source filtering	HQ-CORE1 and HQ-ACC1 use SSH source ACLs. Router and BR-SW1 source restrictions require an agreed management-source policy.
HQ LACP negotiation	The core members use forced 100/full while the access side operates automatically in Packet Tracer. Standardize both ends before physical deployment.
Router-facing branch trunk	PortFast and BPDU Guard are retained on BR-SW1 Gi0/1 as the current edge-trunk policy. Review before connecting any bridge-capable device.
Packet Tracer scope	Platform behavior and command support do not exactly reproduce every IOS release or physical interface negotiation behavior.

Backup and change control

- Save each validated device with copy running-config startup-config.
- Preserve a versioned Packet Tracer file before deliberate fault injection.
- Record each future change with objective, commands, validation and rollback.
- Never publish real credentials, password hashes, private keys or sensitive production addressing.

11. CCNA exam review

Blueprint relevance

Domain	Demonstrated skills
Network Fundamentals	IPv4 addressing, gateways, forwarding path and media state
Network Access	VLANs, trunks, native VLAN, EtherChannel, STP, PortFast and BPDU Guard
IP Connectivity	Inter-VLAN routing, OSPF neighbor formation, route selection and default routes
IP Services	DHCP relay, DNS, SSH and NAT/PAT
Security Fundamentals	ACL sequencing, guest isolation, port security and unused-port hardening

Tier 3 characteristics

- Multiple dependent technologies must work together before the business service succeeds.

- Troubleshooting crosses Layer 1 through Layer 7 evidence rather than relying on one show command.

- The candidate must distinguish control-plane, data-plane, policy and endpoint configuration faults.

- Success requires verification from devices and endpoints, including negative security tests.

Advantages and disadvantages

Perspective	Assessment
Advantages	High realism; strong troubleshooting practice; combines routing, switching, services and security; produces portfolio evidence.
Disadvantages	More dependencies; longer fault isolation; configuration drift is easier; Packet Tracer may simplify or omit IOS behavior.

Simulated exam questions

#	Question and choices	Answer
1	A branch client receives an address but cannot reach the public server. OSPF routes are present and HQ-R1 reaches ISP-R1. Which command gives the most direct evidence that PAT is occurring? A. show vlan brief B. show ip nat translations C. show spanning-tree D. show cdp neighbors	B
2	An ISP router can ping a directly connected public server, but HQ-R1 cannot. The server has the correct IP and mask. Which setting should be checked first? A. OSPF router ID B. LACP mode C. Server default gateway D. Port-security maximum	C
3	Which OSPF route should appear at BR-R1 after HQ-R1 originates its existing static default? A. C 0.0.0.0/0 B. O*E2 0.0.0.0/0 C. O IA 0.0.0.0/0 D. S 0.0.0.0/0	B
4	Why does a sticky port-security table remain empty immediately after configuration? A. Trunking is required B. The switch has not received a source frame C. BPDU Guard blocks learning D. The VLAN must be native	B
5	A guest ping to 192.168.99.11 receives an unreachable message from 192.168.40.1 and the ACL deny counter increases. What is the best conclusion? A. DNS failed B. PAT failed C. The inbound guest ACL is enforcing policy D. OSPF adjacency failed	C

Publication recommendation: publish the PDF on the portfolio site as the permanent case study and share a concise LinkedIn post that links to it. LinkedIn should present the outcome and lessons; the portfolio should preserve the full engineering evidence.