CCNA GROUP 2 ASSIGNMENT

EIGRP ROUTING PROTOCOL

Daheeye University Multi-Campus Network

Theory • Enterprise Design • Full Configuration • Verification • Troubleshooting • Live Demo

Prepared for: CCNA Dynamic Routing Protocols Assignment
Autonomous System: 100 | Platform: Cisco Packet Tracer

FROM ZERO TO HERO

Presentation + Lab Guide

ASSIGNMENT ROADMAP

How this presentation earns the marks

Every assignment item is mapped to a slide and a live verification step.

Theory & Technical Content

EIGRP operation, packets, metric, DUAL purpose, FD/RD/FC, load balancing.

2 marks

Network Design

Four campuses, VLAN segmentation, redundant WAN paths, addressing and naming.

1 mark

Configuration Accuracy

Basic security, VTP, EtherChannel, ROAS, EIGRP, servers, SSH/Telnet.

5 marks

Live Demonstration

Neighbors, learned routes, websites, equal/unequal load balancing, failover.

5 marks

Verification & Troubleshooting

Show commands plus one intentional routing fault and recovery.

2 marks

Teamwork & Delivery

Clear roles, timed demo runbook, presenter notes and professional design.

3 marks

Source: Instructor assignment, pp. 1–7

Project scenario

A realistic enterprise story makes the topology easier to explain and remember.

Business case

Daheeye University operates four campuses: HQ, Borama, Burco and Berbera. Each campus has Admin, Faculty, Students, Servers and Network Management users. The campuses must communicate dynamically, survive a WAN link failure and allow users to open websites hosted at remote campuses.

Primary goal

Provide end-to-end Layer 2, Layer 3 and Application Layer connectivity.

Routing goal

Use EIGRP AS 100 for fast convergence and multiple-path routing.

Security goal

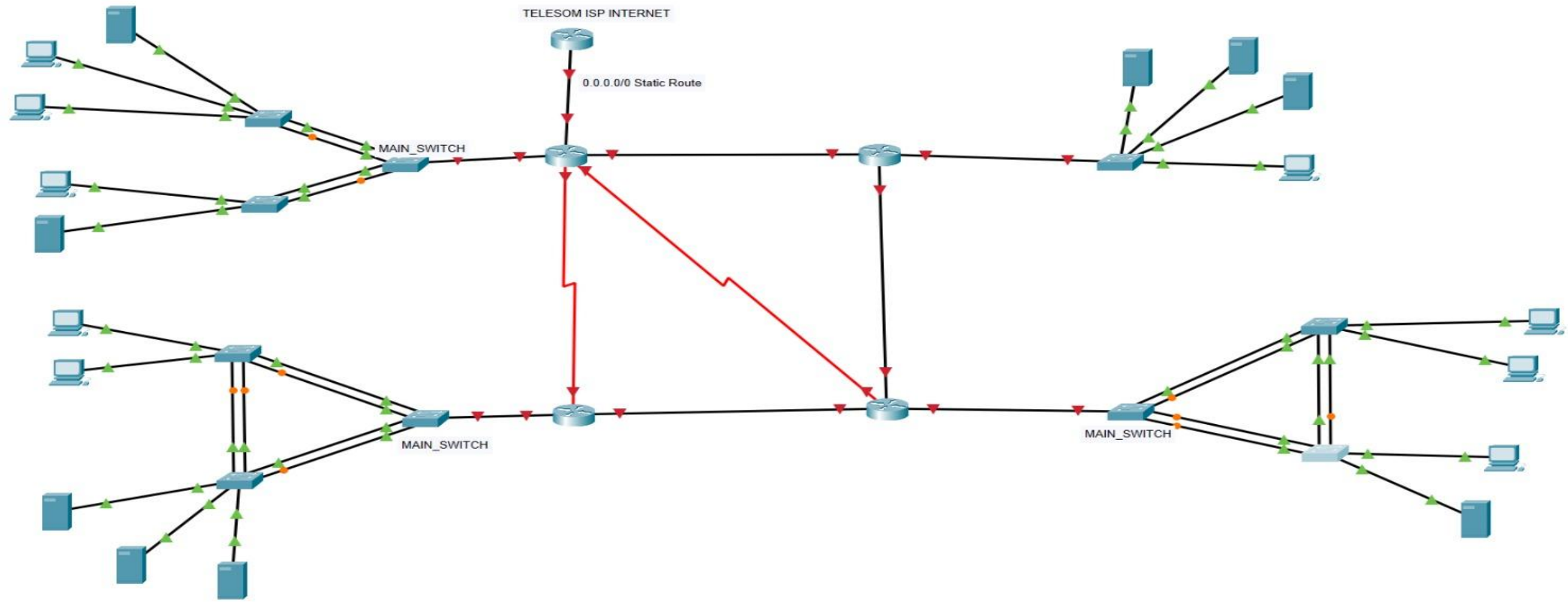
Secure devices with enable secret, local users, console control and SSH.

Bonus goal

Redundancy, default route to ISP, DHCP, Rapid-PVST and clean documentation.

Instructor’s minimum topology

We keep the original four-router redundant design and standardize the campus LANs.



4 enterprise routers | Redundant WAN paths | ISP default route | Multiple campus LANs | Servers at every site

Design enhancements

Small additions improve professionalism without making the lab unmanageable.

1	**Standard campus block**	Every site uses the same VLAN IDs and a unique 10.x.0.0/16 site block.
2	**Two-switch campus model**	Core switch + access switch allow VTP and mandatory Layer 2 EtherChannel.
3	**Router-on-a-Stick**	Each router performs inter-VLAN routing over an 802.1Q trunk.
4	**Redundant EIGRP WAN**	Ring plus HQ–Berbera diagonal provides equal-cost paths and failover.
5	**Server VLAN**	Each site hosts an HTTP server reachable locally and remotely.
6	**Operations & security**	Management VLAN, SSH, local users, interface descriptions, CDP and LLDP.

Naming convention

Consistent names make configuration, verification and troubleshooting easier.

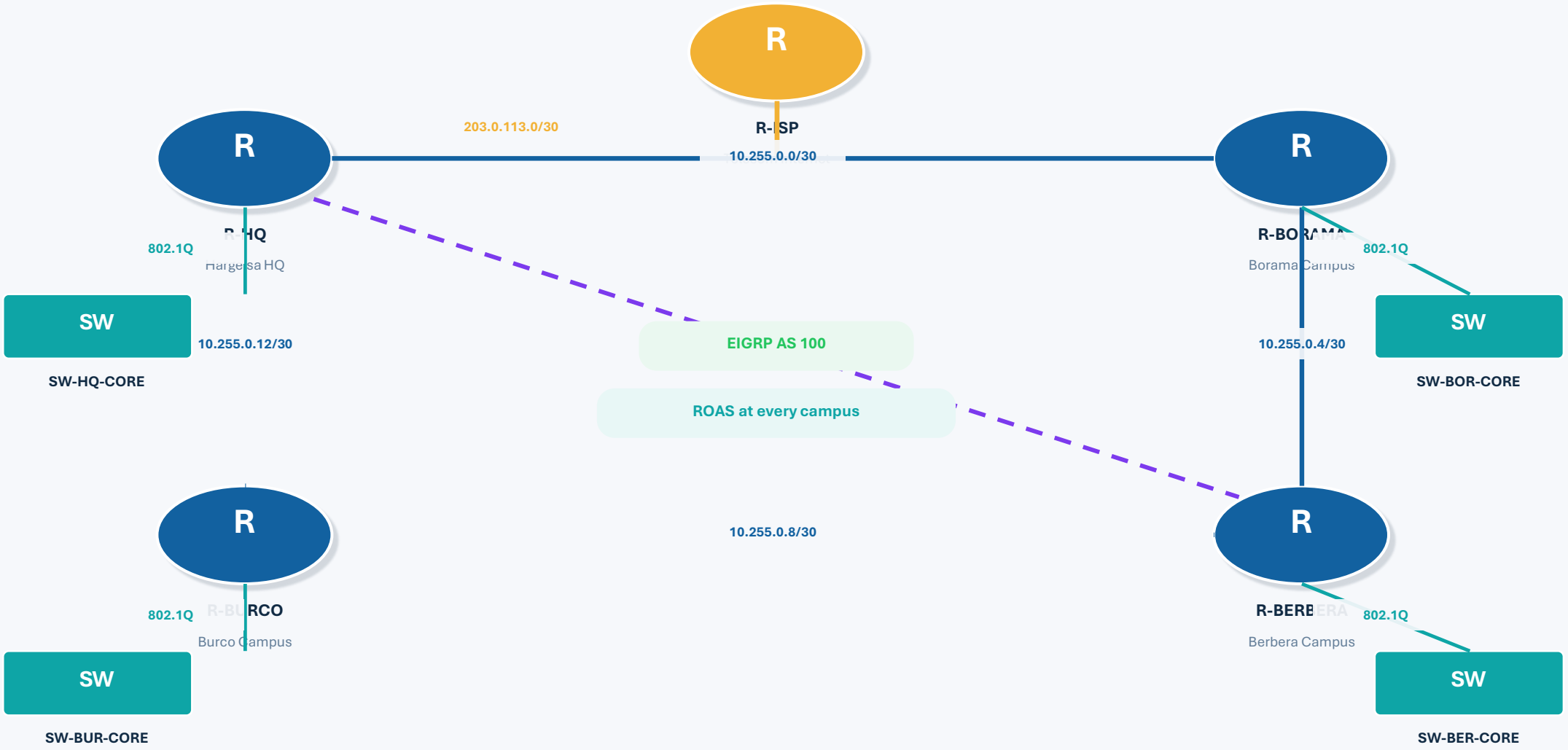
Device role	HQ	Borama	Burco	Berbera
Router	R-HQ	R-BORAMA	R-BURCO	R-BERBERA
Core switch	SW-HQ-CORE	SW-BOR-CORE	SW-BUR-CORE	SW-BER-CORE
Access switch	SW-HQ-ACC1	SW-BOR-ACC1	SW-BUR-ACC1	SW-BER-ACC1
HTTP server	SRV-HQ-WEB	SRV-BOR-WEB	SRV-BUR-WEB	SRV-BER-WEB
Loopback / Router ID	1.1.1.1	2.2.2.2	3.3.3.3	4.4.4.4

Naming rule

ROLE–SITE–FUNCTION. Example: SW-HQ-CORE immediately tells the engineer what the device is, where it is and what it does.

Final logical topology

Four routed campuses, local VLANs, an ISP edge and multiple EIGRP paths.



IP addressing strategy

Hierarchical addressing keeps the design scalable and easy to summarize.

Campus blocks

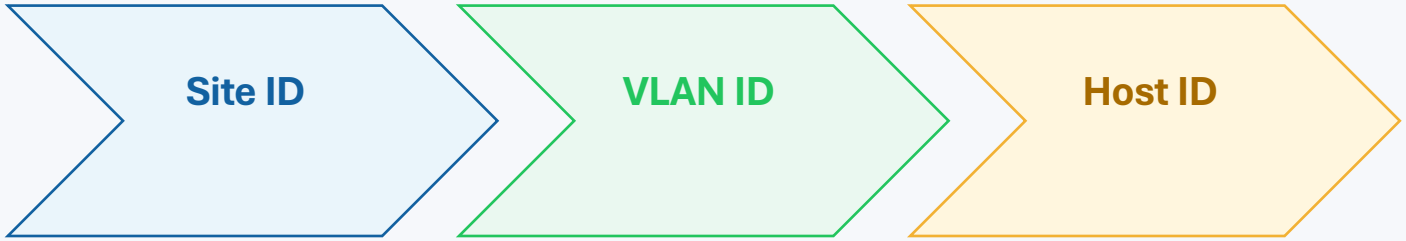
HQ: 10.10.0.0/16
Borama: 10.20.0.0/16
Burco: 10.30.0.0/16
Berbera: 10.40.0.0/16

WAN block

Enterprise point-to-point links use 10.255.0.0/27 divided into /30 subnets.

ISP block

HQ–ISP: 203.0.113.0/30
Internet server: 198.51.100.0/24



Example: 10.20.30.25 = Borama campus, Student VLAN 30, host 25

IP PLAN

WAN addressing table

All point-to-point links use /30 to conserve addresses.

Link	Network	Side A	Side B
R-HQ ↔ R-BORAMA	10.255.0.0/30	HQ 10.255.0.1	Borama 10.255.0.2
R-BORAMA ↔ R-BERBERA	10.255.0.4/30	Borama 10.255.0.5	Berbera 10.255.0.6
R-BERBERA ↔ R-BURCO	10.255.0.8/30	Berbera 10.255.0.9	Burco 10.255.0.10
R-BURCO ↔ R-HQ	10.255.0.12/30	Burco 10.255.0.13	HQ 10.255.0.14
R-HQ ↔ R-BERBERA	10.255.0.16/30	HQ 10.255.0.17	Berbera 10.255.0.18
R-ISP ↔ R-HQ	203.0.113.0/30	ISP 203.0.113.1	HQ 203.0.113.2

/30 reminder

Network + 2 usable host addresses + broadcast. Perfect for a traditional point-to-point link.

IP PLAN

VLAN and LAN addressing table

The same VLAN IDs are reused at every campus; only the site octet changes.

VLAN	Name	HQ	Borama	Burco	Berbera
10	ADMIN	10.10.10.0/24	10.20.10.0/24	10.30.10.0/24	10.40.10.0/24
20	FACULTY	10.10.20.0/24	10.20.20.0/24	10.30.20.0/24	10.40.20.0/24
30	STUDENTS	10.10.30.0/24	10.20.30.0/24	10.30.30.0/24	10.40.30.0/24
40	SERVERS	10.10.40.0/24	10.20.40.0/24	10.30.40.0/24	10.40.40.0/24
99	MGMT	10.10.99.0/24	10.20.99.0/24	10.30.99.0/24	10.40.99.0/24
999	NATIVE-BLACKHOLE	No Layer 3 gateway	No Layer 3 gateway	No Layer 3 gateway	No Layer 3 gateway

Gateway = .1

Core switch = .2

Access switch = .3

Web server = .10

DHCP clients = .21–.200

Subnetting rationale

The design balances simplicity, scalability and address efficiency.

Why /24 for VLANs?

- Up to 254 hosts per department
- Simple default mask
- Easy troubleshooting
- Enough room for growth
- Clear one-VLAN-one-subnet rule

Why /30 for WAN?

- Exactly two usable addresses
- Minimal waste
- Clear point-to-point boundaries
- Easy route verification
- Matches the assignment’s subnetting requirement

Why /16 site blocks?

- Each campus can grow
- Predictable hierarchy
- Easier documentation
- Supports future summarization
- Site can be recognized from the second octet

02

EIGRP Theory

Understand what the protocol does before typing the commands.

Theory → Design → Configuration → Verification → Live Demonstration

What is EIGRP?

Enhanced Interior Gateway Routing Protocol is a dynamic IGP used inside one autonomous system.



Dynamic

Learns and adapts routes automatically when the network changes.

Interior Gateway Protocol

Designed for routing within an organization’s autonomous system.

Fast convergence

DUAL helps select loop-free paths and quickly use a feasible backup.

Efficient updates

Uses neighbor relationships and sends incremental updates when routes change.

Cisco: Understand and Use EIGRP

Why is EIGRP called a “hybrid” protocol?

A useful classroom label—technically it is commonly described as an advanced distance-vector IGP.

Distance-vector behavior

- Exchanges route information with directly connected neighbors
- Selects paths using a calculated distance/metric
- Does not flood a complete link-state database like OSPF

Advanced features

- Neighbor table
- Topology table
- Reliable transport for selected packets
- Incremental updates
- Feasible successor backup routes

Best wording in class

“EIGRP is an advanced distance-vector protocol often called hybrid because it combines neighbor-based route exchange with fast-convergence and topology-tracking features.”

The three EIGRP data structures

Each table answers a different operational question.

1

Neighbor Table

Who are my EIGRP neighbors?

`show ip eigrp neighbors`

2

Topology Table

What paths do I know?

`show ip eigrp topology`

3

Routing Table

Which best paths will forward traffic?

`show ip route eigrp`

Basic EIGRP operation

From Hello packets to a usable route in seven clear steps.



1 Hello

Routers discover neighbors on a common network.

2 Adjacency

Matching neighbors form an EIGRP relationship.

3 Exchange

Initial routing information is exchanged reliably.

4 Topology

All learned paths are stored in the topology table.

5 DUAL

Successor and possible feasible successor are selected.

6 Install

The successor route enters the IP routing table.

7 Change

Incremental Update—or Query/Reply—handles a topology change.

Key point

EIGRP does not send the full routing table periodically. After the initial exchange, it sends bounded, incremental updates when something changes.

Cisco: EIGRP neighbor discovery and maintenance

EIGRP packet types

Five core packet types support discovery, learning and convergence.

	Purpose	Delivery	Reliability
HELLO	**Discover and maintain neighbors**	Usually multicast	No acknowledgement
UPDATE	**Send routing information**	Multicast or unicast	Reliable / acknowledged
QUERY	**Ask neighbors for another path**	Multicast or unicast	Reliable / acknowledged
REPLY	**Answer an EIGRP query**	Unicast	Reliable / acknowledged
ACK	**Confirm reliable delivery**	Unicast	Hello packet with no data

DUAL: purpose and key terms

The assignment requires the purpose—not the internal mathematics—of DUAL.

DUAL purpose

Select loop-free routes, keep a safe backup when possible and converge quickly after a failure.

Successor

The best next hop to the destination. This route is installed in the routing table.

Feasible Successor

A loop-free backup path that satisfies the Feasibility Condition.

Feasible Distance (FD)

The local router’s best known total metric to the destination.

Reported Distance (RD)

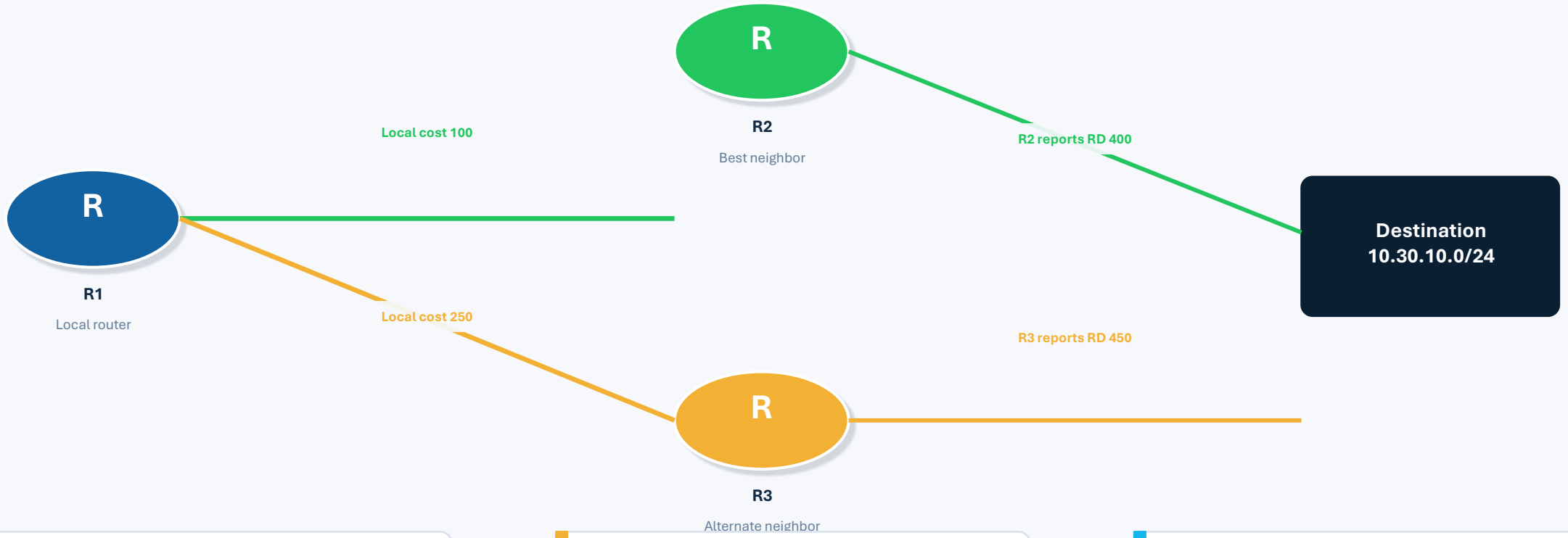
The metric a neighbor reports from itself to the destination.

Feasibility Condition

A candidate is loop-free when RD < current successor FD.

FD, RD and Feasibility Condition—simple example

A numerical example makes the backup-route decision easy to defend.



Successor FD

100 + 400 = 500

Alternate total metric

250 + 450 = 700

FC test

RD 450 < FD 500 ✓

EIGRP composite metric

By default, path selection mainly uses minimum bandwidth and cumulative delay.

Default classic metric = 256 × [(10^7 ÷ minimum bandwidth in kbps) + sum of delay in tens of µs]

Bandwidth

The lowest-bandwidth link along the entire path.

Delay

The sum of interface delays along the path.

Reliability

Available in the composite metric, but K4/K5 are 0 by default.

Load

Available, but K2 is 0 by default.

MTU

Carried in EIGRP information but not used in the default path calculation.

Cisco EIGRP metric guide: default K1=1, K3=1; others 0

Administrative Distance and route identification

AD answers: “Which routing source should I trust?”

Route source	Administrative Distance	Routing-table code
Connected	0	C
Static	1	S
EIGRP summary	5	D (summary)
EIGRP internal	90	D
OSPF	110	O
RIP	120	R
EIGRP external	170	D EX

What you will see

D 10.30.10.0/24 [90/xxxxx] via 10.255.0.x

Read the brackets

[90 / metric] = [Administrative Distance / EIGRP composite metric]

Exam tip

Lower AD is preferred between different routing sources.

Equal-cost and unequal-cost load balancing

EIGRP can install multiple loop-free paths; variance controls unequal-cost eligibility.

Equal-cost load balancing

- Multiple paths have the same EIGRP metric
- Enabled by default
- maximum-paths controls how many routes can be installed
- Our demo: Borama → Burco through HQ and Berbera

Unequal-cost load balancing

- Paths have different metrics
- Alternate must be a feasible successor
- variance multiplier expands the acceptable metric range
- Our demo: increase delay on one Borama WAN link, then configure variance 2

variance n condition Alternate metric < Successor metric × n AND alternate satisfies the Feasibility Condition

Cisco: Unequal Cost Path Load Balancing (Variance)

Advantages, limitations and enterprise use cases

A balanced explanation is stronger than saying only “EIGRP is fast.”

Advantages

- Fast convergence
- Feasible-successor backup
- Incremental updates
- Supports VLSM/CIDR
- Equal and unequal load balancing
- Scales well in controlled enterprise networks

Limitations

- Less common than OSPF in multivendor designs
- Metric and variance can be misunderstood
- Poor design can expand query scope
- Not an Internet exterior routing protocol
- Classic-mode lab syntax differs from named mode

Use cases

- Cisco-heavy enterprise WAN
- Campus-to-campus routing
- Branch networks requiring fast failover
- Networks needing unequal-cost multipath
- Training labs for dynamic routing and convergence

03

Packet Tracer Build

Build Layer 1 and Layer 2 correctly before enabling EIGRP.

Theory → Design → Configuration → Verification → Live Demonstration

Hardware placement and cabling

Use a build that has enough routed interfaces for the five WAN links.

Recommended devices

- 5 × Cisco 2911 routers
- HWIC-2T modules as needed
- 8 × Cisco 2960 switches
- PCs/laptops for each VLAN
- 5 HTTP servers (4 campus + 1 Internet test server)

Cable types

- Serial DCE/DTE: router-to-router WAN
- Copper straight-through: router-to-switch and host-to-switch
- Two parallel copper links: core-to-access EtherChannel
- Set clock rate only on the DCE end

Before cabling

1. Power off router
2. Insert HWIC-2T module
3. Power on
4. Connect and label every link
5. Record which side is DCE
6. Save the .pkt file with version numbers

Build order—do not skip ahead

A disciplined order prevents hidden Layer 1 or Layer 2 faults from looking like EIGRP problems.

1 Place & cable

Devices, modules, labels and interface plan.

2 Basic config

Hostnames, passwords, local user, SSH and descriptions.

3 Layer 2

VLANs, VTP, trunks, access ports, EtherChannel.

4 Inter-VLAN

ROAS subinterfaces and gateway tests.

5 WAN Layer 3

/30 addresses, clock rate, no shutdown, direct pings.

6 EIGRP

AS 100, networks, router IDs and passive interfaces.

7 Applications

DHCP, HTTP servers and remote browsing.

8 Demo features

Load balancing, metric change, failover and troubleshooting.

Golden rule

Never troubleshoot EIGRP until interface status, IP addressing, masks and direct neighbor pings are correct.

CONFIGURATION

Step 1 — Basic router security configuration

Apply the same baseline to every router; change only the hostname.

R-HQ — baseline

```
enable
configure terminal
hostname R-HQ
no ip domain-lookup
enable secret Ccna@2026
service password-encryption
banner motd # AUTHORIZED ACCESS ONLY #
username admin privilege 15 secret Admin@123
ip domain-name daheeye.local
crypto key generate rsa modulus 1024
ip ssh version 2
line console 0
 password Console@123
 login
 logging synchronous
 exec-timeout 10 0
line vty 0 4
 login local
 transport input telnet ssh
 exec-timeout 10 0
end
copy running-config startup-config
```

Why both Telnet and SSH?

The assignment asks for both. We demonstrate Telnet, then explain that SSH is preferred because it encrypts credentials and traffic.

Interface descriptions

Every physical and logical interface will include a clear “description” command.

Verification

show running-config | section line
show ip ssh
show users

CONFIGURATION

Step 2 — Basic switch configuration

Secure management access before creating VLANs and trunks.

SW-HQ-CORE — baseline

```
enable
configure terminal
hostname SW-HQ-CORE
no ip domain-lookup
enable secret Ccna@2026
service password-encryption
username admin privilege 15 secret Admin@123
ip domain-name daheeye.local
crypto key generate rsa modulus 1024
ip ssh version 2
line console 0
 password Console@123
 login
 logging synchronous
line vty 0 15
 login local
 transport input telnet ssh
spanning-tree mode rapid-pvst
cdp run
lldp run
end
copy run start
```

Management comes later

The VLAN 99 SVI and default gateway are configured after VLAN propagation.

Rapid-PVST bonus

This is not mandatory, but it improves Layer 2 convergence and demonstrates enterprise design.

Discovery protocols

CDP is Cisco-proprietary; LLDP is the open IEEE standard.

CONFIGURATION

Step 3 — Create VLANs, access ports and trunks

The core switch is the local VTP server and owns the VLAN database.

SW-HQ-CORE — VLANs and router trunk

```
vtp domain DAHEEYE
vtp mode server
vtp version 2
vtp password Ccna2026

vlan 10
 name ADMIN
vlan 20
 name FACULTY
vlan 30
 name STUDENTS
vlan 40
 name SERVERS
vlan 99
 name MANAGEMENT
vlan 999
 name NATIVE-BLACKHOLE

interface g0/24
 description 802.1Q TRUNK TO R-HQ G0/0
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,30,40,99,999
 no shutdown
```

Access-port example

```
interface range f0/1-5
 description ADMIN USERS
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
 spanning-tree bpduguard enable

interface range f0/6-12
 description FACULTY USERS
 switchport mode access
 switchport access vlan 20
 spanning-tree portfast

interface range f0/13-20
 description STUDENT USERS
 switchport mode access
 switchport access vlan 30
 spanning-tree portfast

interface f0/21
 description CAMPUS WEB SERVER
 switchport mode access
 switchport access vlan 40
```

Step 4 — Configure and demonstrate VTP

VTP propagation occurs only inside a Layer 2 campus; it does not cross the routers.

VTP client

```
hostname SW-HQ-ACC1
vtp domain DAHEEYE
vtp mode client
vtp version 2
vtp password Ccna2026

! Do NOT create VLANs on the client
! Wait for the trunk/EtherChannel to come up

show vtp status
show vlan brief
```

Advantages

- Central VLAN creation
- Consistent names/IDs
- Less repetitive work

Limitations

- Revision mistakes can be dangerous
- Same domain/password required
- Layer 2 only

Use it when

A controlled campus has central switch management. Avoid careless VTP use in unmanaged or mixed environments.

Live proof

Create VLAN 50 temporarily on the VTP server → show it appears on the client → delete it after the demonstration.

CONFIGURATION

Step 5 — Build mandatory Layer 2 EtherChannel

Two physical trunks become one logical Port-Channel using LACP.

SW-HQ-CORE

```
! CORE SWITCH
interface range g0/1-2
 description LACP LINKS TO SW-HQ-ACC1
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,30,40,99,999
 channel-group 1 mode active
 no shutdown

interface port-channel 1
 description LACP PORT-CHANNEL TO SW-HQ-ACC1
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,30,40,99,999
```

show etherchannel summary

show interfaces trunk

SW-HQ-ACC1

```
! ACCESS SWITCH
interface range g0/1-2
 description LACP LINKS TO SW-HQ-CORE
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,30,40,99,999
 channel-group 1 mode passive
 no shutdown

interface port-channel 1
 description LACP PORT-CHANNEL TO SW-HQ-CORE
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,30,40,99,999
```

P = bundled in port-channel

CONFIGURATION

Step 6 — Configure Router-on-a-Stick

One physical router interface becomes the default gateway for multiple VLANs.

R-HQ — ROAS

```
interface g0/0
 description 802.1Q TRUNK TO SW-HQ-CORE G0/24
 no ip address
 no shutdown

interface g0/0.10
 description HQ ADMIN GATEWAY
 encapsulation dot1Q 10
 ip address 10.10.10.1 255.255.255.0

interface g0/0.20
 description HQ FACULTY GATEWAY
 encapsulation dot1Q 20
 ip address 10.10.20.1 255.255.255.0

interface g0/0.30
 description HQ STUDENTS GATEWAY
 encapsulation dot1Q 30
 ip address 10.10.30.1 255.255.255.0

interface g0/0.40
 description HQ SERVERS GATEWAY
 encapsulation dot1Q 40
 ip address 10.10.40.1 255.255.255.0

interface g0/0.99
 description HQ MANAGEMENT GATEWAY
 encapsulation dot1Q 99
 ip address 10.10.99.1 255.255.255.0

interface g0/0.999
 encapsulation dot1Q 999 native
```

Inter-VLAN test

Admin PC → ping 10.10.20.x Faculty PC

Trunk match

Router native VLAN 999 must match the switch native VLAN 999.

Repeat per site

Change only the site octet: 10.20, 10.30 or 10.40.

CONFIGURATION

Step 7 — Configure DHCP and campus web servers

DHCP is a bonus feature; servers use static addresses in VLAN 40.

R-HQ — DHCP example

```
ip dhcp excluded-address 10.10.10.1 10.10.10.20
ip dhcp excluded-address 10.10.20.1 10.10.20.20
ip dhcp excluded-address 10.10.30.1 10.10.30.20

ip dhcp pool HQ-ADMIN
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.1
 dns-server 8.8.8.8

ip dhcp pool HQ-FACULTY
 network 10.10.20.0 255.255.255.0
 default-router 10.10.20.1
 dns-server 8.8.8.8

ip dhcp pool HQ-STUDENTS
 network 10.10.30.0 255.255.255.0
 default-router 10.10.30.1
 dns-server 8.8.8.8
```

HQ web server

IP 10.10.40.10 /24
Gateway 10.10.40.1
HTTP service: ON

Remote sites

Borama 10.20.40.10
Burco 10.30.40.10
Berbera 10.40.40.10

Homepage text

“Welcome to Daheeye University — [Campus Name] Web Server”

CONFIGURATION

Step 8 — Configure WAN interfaces

Finish all /30 links and prove direct connectivity before EIGRP.

R-HQ — WAN interfaces

```
interface s0/0/0
 description WAN TO R-BORAMA S0/0/0
 ip address 10.255.0.1 255.255.255.252
 bandwidth 1544
 delay 2000
 clock rate 64000   ! DCE side only
 no shutdown

interface s0/0/1
 description WAN TO R-BURCO S0/0/1
 ip address 10.255.0.14 255.255.255.252
 bandwidth 1544
 delay 2000
 no shutdown

interface s0/1/0
 description REDUNDANT WAN TO R-BERBERA S0/1/0
 ip address 10.255.0.17 255.255.255.252
 bandwidth 1544
 delay 2000
 no shutdown

interface g0/1
 description INTERNET EDGE TO R-ISP
 ip address 203.0.113.2 255.255.255.252
 no shutdown
```

DCE check

show controllers serial 0/0/0

Interface check

show ip interface brief

Direct ping

ping every directly connected neighbor IP

04

EIGRP Configuration

Enable neighbor relationships, advertise networks and control update boundaries.

Theory → Design → Configuration → Verification → Live Demonstration

Step 9 — Configure EIGRP AS 100

Classic-mode syntax is chosen for maximum Cisco Packet Tracer compatibility.

R-HQ

```
interface loopback0
 description EIGRP ROUTER-ID
 ip address 1.1.1.1 255.255.255.255

router eigrp 100
 eigrp router-id 1.1.1.1
 no auto-summary
 passive-interface default
 no passive-interface s0/0/0
 no passive-interface s0/0/1
 no passive-interface s0/1/0
 network 1.1.1.1 0.0.0.0
 network 10.10.0.0 0.0.255.255
 network 10.255.0.0 0.0.0.31
 maximum-paths 4
```

Branch pattern

```
! R-BORAMA
router eigrp 100
 eigrp router-id 2.2.2.2
 no auto-summary
 passive-interface default
 no passive-interface s0/0/0
 no passive-interface s0/0/1
 network 2.2.2.2 0.0.0.0
 network 10.20.0.0 0.0.255.255
 network 10.255.0.0 0.0.0.31
 maximum-paths 4

! R-BURCO uses 3.3.3.3 and 10.30.0.0/16
! R-BERBERA uses 4.4.4.4 and 10.40.0.0/16
```

Step 10 — Propagate the ISP default route

Only R-HQ knows the ISP; branches learn a default route through EIGRP.

Default route and return path

```
! R-HQ
ip route 0.0.0.0 0.0.0.0 203.0.113.1

router eigrp 100
 default-metric 100000 100 255 1 1500
 redistribute static

! R-ISP return route
ip route 10.0.0.0 255.0.0.0 203.0.113.2
```

Expected branch route

D EX 0.0.0.0/0 [170/metric] via an EIGRP neighbor

Why external?

The route originated as a static route and was redistributed into EIGRP, so its AD is 170.

Verification

show ip route 0.0.0.0 | ping 198.51.100.10

VERIFICATION

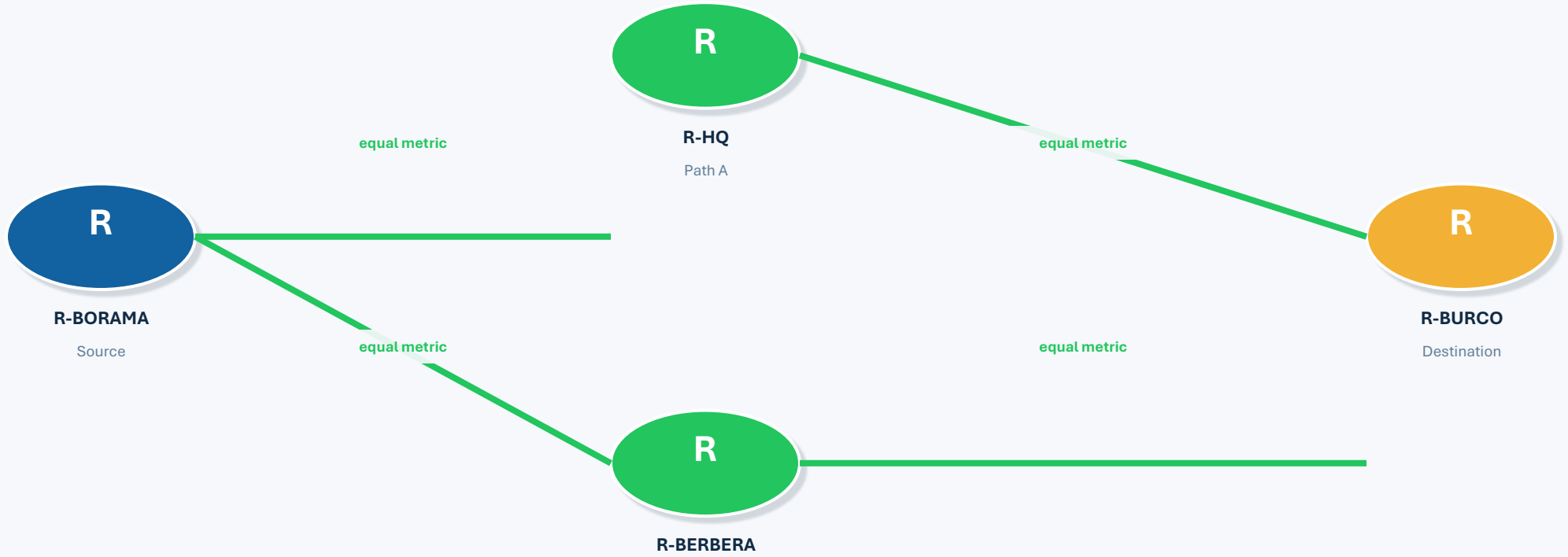
Step 11 — Verification command plan

Verify one layer at a time and save screenshots for the report.

Layer / feature	Command	What success looks like
Interfaces	show ip interface brief	Required ports are up/up
VLANs	show vlan brief	Correct access ports in each VLAN
Trunks	show interfaces trunk	Allowed/native VLANs match
VTP	show vtp status	Correct domain, mode and revision
EtherChannel	show etherchannel summary	Po1(SU), member ports show P
Neighbors	show ip eigrp neighbors	Expected WAN neighbors present
Topology	show ip eigrp topology	Successors and feasible successors
Routes	show ip route eigrp	Remote campus VLANs begin with D
Protocol	show ip protocols	AS 100, networks, passive interfaces
Discovery	show cdp neighbors / show lldp neighbors	Correct physical neighbor mapping

Live demo 1 — Equal-cost load balancing

Borama reaches Burco through two paths with the same EIGRP metric.



Expected proof

```
R-BORAMA# show ip route 10.30.10.0
D 10.30.10.0/24 [90/metric] via 10.255.0.1
                [90/metric] via 10.255.0.6
```

```
R-BORAMA# show ip eigrp topology
R-BORAMA# traceroute 10.30.10.10
```

Live demo 2 — Unequal-cost load balancing with variance

Make one path more expensive, confirm it is feasible, then install it with variance 2.

R-BORAMA — variance demo

```
! Step A — make path via HQ more expensive
R-BORAMA(config)# interface s0/0/0
R-BORAMA(config-if)# delay 4000

! Step B — inspect topology table
R-BORAMA# show ip eigrp topology

! Step C — allow unequal feasible path
R-BORAMA(config)# router eigrp 100
R-BORAMA(config-router)# variance 2
R-BORAMA(config-router)# maximum-paths 2
R-BORAMA(config-router)# traffic-share balanced

! Step D — prove both routes are installed
R-BORAMA# show ip route 10.30.10.0
```

Before variance

Only the lower-metric path is installed in the routing table.

Feasibility check

The alternate path must appear as a feasible successor; variance cannot use a non-feasible path.

After variance 2

Both loop-free paths appear with different metrics and traffic-share counts.

LIVE DEMONSTRATION

Live demo 3 — Link failure and route recovery

A continuous ping proves that EIGRP reconverges over the redundant path.

1. **Start continuous ping** — From a Borama PC: ping a Burco server repeatedly.
2. **Record current path** — Run tracert/traceroute and show the routing table.
3. **Fail one link** — shutdown R-BORAMA S0/0/0 (the HQ path).
4. **Observe convergence** — Neighbor disappears; route remains via Berbera.
5. **Restore link** — no shutdown and observe route recovery.

Failure commands

```
R-BORAMA(config)# interface s0/0/0
R-BORAMA(config-if)# shutdown
```

```
R-BORAMA# show ip eigrp neighbors
R-BORAMA# show ip route 10.30.40.0
R-BORAMA# traceroute 10.30.40.10

R-BORAMA(config-if)# no shutdown
```

Live demo 4 — Intentional routing fault and troubleshooting

Create a passive-interface error on both Burco WAN links, then solve it systematically.

Troubleshooting sequence

```
! CREATE THE PROBLEM
R-BURCO(config)# router eigrp 100
R-BURCO(config-router)# passive-interface s0/0/0
R-BURCO(config-router)# passive-interface s0/0/1

! SYMPTOMS
R-BURCO# show ip eigrp neighbors
R-BURCO# show ip route eigrp
R-BURCO# show ip protocols

! FIX
R-BURCO(config)# router eigrp 100
R-BURCO(config-router)# no passive-interface s0/0/0
R-BURCO(config-router)# no passive-interface s0/0/1

! VERIFY
R-BURCO# show ip eigrp neighbors
R-BURCO# show ip route eigrp
```

Symptom

Burco loses both EIGRP neighbors and remote routers lose Burco VLAN routes.

Diagnosis logic

Interfaces are up/up and direct pings work, so check EIGRP process settings and passive interfaces.

Proof of repair

Neighbors return, D routes reappear and remote HTTP access succeeds.

CDP, LLDP and remote management demonstration

Show both discovery protocols and prove secured management access.

CDP

Cisco Discovery Protocol
- Cisco proprietary
- Enabled by default on many Cisco devices
- Useful for Cisco device details

Commands:
show cdp neighbors
show cdp neighbors detail

LLDP

Link Layer Discovery Protocol
- Open IEEE standard
- Multi-vendor support
- Must often be enabled globally

Commands:
lldp run
show lldp neighbors detail

Remote access

From a management PC:

ssh -l admin 10.20.99.2
telnet 10.20.99.2

Explain: SSH encrypts the session; Telnet sends data in clear text.

Management SVI example

interface vlan 99 → ip address 10.10.99.2/24 → no shutdown → ip default-gateway 10.10.99.1

APPLICATION LAYER

Mandatory web server deployment

Prove complete Layer 2, Layer 3 and Application Layer connectivity.

1. Address

Set server IP, /24 mask and VLAN 40 gateway.

2. Connect

Place the switch port in VLAN 40.

3. Enable HTTP

Server → Services → HTTP → On.

4. Edit homepage

Add campus name and project title to index.html.

5. Local test

Open the website from a PC in the same campus.

6. Remote test

Open the site from PCs in two different campuses.

Browser targets

http://10.10.40.10 | http://10.20.40.10 | http://10.30.40.10 | http://10.40.40.10

DELIVERY

Live demonstration runbook

A rehearsed 8–10 minute sequence prevents confusion during assessment.

Time	Presenter action	Command / proof
0:00–0:45	Introduce project and topology	Point to sites, VLANs and redundant WAN
0:45–1:45	Prove Layer 2	show vlan brief; show interfaces trunk; show etherchannel summary
1:45–2:45	Prove EIGRP neighbors	show ip eigrp neighbors on HQ and one branch
2:45–3:45	Prove learned routes	show ip route eigrp; show ip protocols
3:45–4:45	Open remote website	Browser from Borama PC to Burco server
4:45–5:45	Equal-cost paths	show route to Burco from Borama
5:45–7:00	Unequal-cost variance	delay change → topology → variance 2 → route table
7:00–8:15	Link failure and recovery	shutdown/no shutdown + continuous ping
8:15–9:30	Troubleshoot passive-interface fault	show commands → fix → verify
9:30–10:00	Close and summarize	Benefits, limitations and key learning

QUALITY ASSURANCE

Bonus features and final grading checklist

Use the extras only after all mandatory items work reliably.

- Professional enterprise naming and hierarchical addressing
- Redundant ring plus diagonal WAN path
- DHCP for user VLANs
- Rapid-PVST and BPDU Guard
- Native black-hole VLAN 999
- Default route propagation to ISP
- Interface descriptions on every link
- Versioned Packet Tracer files and screenshots

Mandatory first

Basic config, addressing, VLANs, VTP, L2 EtherChannel, CDP/LLDP, Telnet/SSH, EIGRP, verification, troubleshooting and web servers.

Configuration accuracy

Use the full configuration pack, then verify line by line with show commands.

Presentation quality

Use diagrams, avoid reading code word-for-word, and explain why each command exists.

Final action

Save: running-config, startup-config, .pkt, PPTX and screenshots.

CLOSING

Conclusion

The project demonstrates an end-to-end enterprise network, not only an EIGRP command.

EIGRP AS 100

Layer 2

VLANs • VTP • trunks • LACP EtherChannel

Layer 3

ROAS • /30 WANs • EIGRP • default route

Application

DHCP • local and remote HTTP websites

Operations

SSH • Telnet • CDP • LLDP • verification

Resilience

Equal/unequal paths • link failure • recovery

Troubleshooting

Intentional fault • diagnosis • proof of repair

Thank you — Questions?

Appendix A — R-HQ command map

Use the separate configuration pack for the complete copy/paste-ready configuration.

R-HQ build checklist

```
1. Basic security and SSH
2. Loopback0: 1.1.1.1/32
3. G0/0.10, .20, .30, .40, .99, .999 (ROAS)
4. G0/1: 203.0.113.2/30 to ISP
5. S0/0/0: 10.255.0.1/30 to Borama
6. S0/0/1: 10.255.0.14/30 to Burco
7. S0/1/0: 10.255.0.17/30 to Berbera
8. DHCP pools for VLANs 10, 20 and 30
9. Static default route to 203.0.113.1
10. EIGRP AS 100 + passive-interface default
11. Redistribute static with default metric
12. Save and verify
```

R-HQ verification

```
show ip interface brief
show interfaces description
show ip dhcp binding
show ip eigrp neighbors
show ip eigrp topology
show ip route eigrp
show ip route 0.0.0.0
show ip protocols
show cdp neighbors detail
show lldp neighbors detail
show running-config | section router eigrp
```

Appendix B — Branch substitutions

The branch configurations are identical in structure; only site-specific values change.

Item	Borama	Burco	Berbera
Router ID	2.2.2.2	3.3.3.3	4.4.4.4
Site block	10.20.0.0/16	10.30.0.0/16	10.40.0.0/16
VLAN gateways	10.20.VLAN.1	10.30.VLAN.1	10.40.VLAN.1
Core switch MGMT	10.20.99.2	10.30.99.2	10.40.99.2
Access switch MGMT	10.20.99.3	10.30.99.3	10.40.99.3
Web server	10.20.40.10	10.30.40.10	10.40.40.10
EIGRP WAN interfaces	S0/0/0, S0/0/1	S0/0/0, S0/0/1	S0/0/0, S0/0/1, S0/1/0

Rule

Do not change AS 100, VLAN IDs, native VLAN 999 or VTP domain/password.

Appendix C — Switch verification and common fixes

Use symptoms to identify the correct configuration layer.

Symptom	Likely cause	Command / fix
VLAN missing on client	VTP domain/password/mode or trunk down	show vtp status; verify trunk; match credentials
EtherChannel suspended	Port settings do not match	show etherchannel summary; match speed/trunk/native/allowed
PC cannot reach gateway	Wrong access VLAN or trunk/subinterface issue	show vlan brief; show interfaces trunk; check dot1Q tag
Switch cannot be SSH’d remotely	SVI down or default gateway missing	show ip int brief; ip default-gateway SITE.99.1
Native VLAN warning	Native VLAN mismatch	Set VLAN 999 on both ends
Remote campus unreachable	EIGRP neighbor/advertisement problem	show ip eigrp neighbors; show ip protocols; show route

REFERENCES

1. CCNA Group Assignment – Dynamic Routing Protocols. Instructor-provided PDF, pp. 1–7.

2. Cisco. IP Routing Configuration Guide, Cisco IOS XE 17.x — EIGRP.

3. Cisco. Understand and Use the Enhanced Interior Gateway Routing Protocol.

4. Cisco. How Does Unequal Cost Path Load Balancing (Variance) Work in EIGRP?

5. Cisco. EIGRP Command Reference — variance, metric weights and topology output.

6. Cisco. Configuring EIGRP — equal and unequal cost load balancing.

7. Cisco Packet Tracer command behavior may vary by router model and IOS image; verify syntax in the selected device.

End of deck