Routing & GRE Tunnel Playbook

# 1. Routing & GRE Tunnel – Playbook

## Step 1: Configure WAN Interfaces

- Assign public IPs to HQ-RTR and BR-RTR on their WAN-facing Gigabit ports toward ISP-RTR.  
- ISP-RTR gets the first usable address in each /30, HQ-RTR/BR-RTR take the second.  
- Verify with 'ping' between HQ and ISP, and BR and ISP.

## Step 2: Build the GRE Tunnel

On HQ-RTR:  
interface Tunnel0  
 ip address 192.168.98.1 255.255.255.252  
 tunnel source fa0/1  
 tunnel destination 198.51.100.2  
 no shutdown  
  
On BR-RTR:  
interface Tunnel0  
 ip address 192.168.98.2 255.255.255.252  
 tunnel source fa0/1  
 tunnel destination 203.0.113.2  
 no shutdown  
  
Verify with 'ping 192.168.98.1' from BR and 'ping 192.168.98.2' from HQ.

## Step 3: Enable OSPF

Enable OSPF on both routers over Tunnel0 only:  
router ospf 1  
 router-id <unique-ID>  
 passive-interface default  
 no passive-interface Tunnel0  
 network 192.168.98.0 0.0.0.3 area 0  
  
Verify with 'show ip ospf neighbor' (HQ and BR should show FULL adjacency).

## Step 4: Advertise Internal VLANs

Add VLAN subnets to OSPF so HQ and BR learn each other's networks:  
network 192.168.99.0 0.0.0.127 area 0  
  
Confirm with 'show ip route ospf'.

# 2. Explanation

The WAN interfaces simulate the 'Internet' using test networks, but since private VLAN subnets cannot be routed directly across them, a GRE tunnel is built between HQ and BR. GRE encapsulates the private traffic inside routable packets, creating a virtual point-to-point link between the two routers.  
  
OSPF is then enabled across the tunnel, dynamically exchanging routes so each site knows how to reach the other’s VLANs. This avoids static routes and scales better. Making all other interfaces passive keeps routing updates off LAN-facing links.  
  
The result: HQ and Branch VLANs can communicate securely through the tunnel, with OSPF handling route discovery and the GRE tunnel simulating a WAN overlay.