Huawei Router configuration:

Console configuration <Huawei>system-view [Huawei]sysname rt1 [rt1]user-interface console 0 [rt1-ui-console0]set authentication password cipher alamin [rt1-ui-console0]display this [rt1-ui-console0]quit	To enter system view Set sysname To enter console mode # Set console password
Telnet configuration [rt1]user-interface vty 0 4 [rt1-ui-vty0-4]authentication-mode password [rt1-ui-vty0-4]set authentication password cipher alamin [rt1-ui-vty0-4]quit	** TELNet is not Secure so use SSH. Same as describe in switch section.
Set Interface IP Address & Description [rt1]interface Ethernet0/0/0 [rt1-Ethernet0/0/0]description Connect_to_Routr_2 [rt1-Ethernet0/0/0]ip address 10.0.12.1 24 [rt1-Ethernet0/0/1]quit **Optional: Set multiple ip address to an interface** [rt1-Ethernet0/0/0]ip address 192.168.0.1 24 sub	
Static route & Default route [rt1]ip route-static 10.0.23.0 255.255.255.0 10.0.12.2 description routes_for_23_block [rt2]ip route-static 0.0.0.0 0.0.0.0 10.0.31.1	ip route-static ip-address {mask | mask-length} {nexthop-address | interface-type interface-number [nexthop-address]} [preference preference]
Backup route/ Floating route ip route-static 10.0.23.0 24 10.0.31.1 preference 80 description Backup_static route [rt2]ip route-static 0.0.0.0 0.0.0.0 10.0.12.1 preference 90	Preference is like Administrative distance. Higher the preference value, lower the preference. Default preference for static route in huawei is 60 Backup static route for default route.
Check & verification [rt2] display ip routing-table	

OSPF Configuration	
ospf [process-id | router-id router-id] [rt1]ospf 1 router-id 1.1.1.1 [rt1-ospf-1]area 0 [rt1-ospf-1-area-0.0.0.0]network 10.0.0.0 0.0.0.255 [rt1-ospf-1-area-0.0.0.0]network 1.1.1.1 0.0.0.0 [rt1-ospf-1-area-0.0.0.0]display this [rt1-ospf-1]area 1 [rt1-ospf-1-area-0.0.0.1]network 10.0.1.0 0.0.0.255 [rt1-ospf-1-area-0.0.0.1]display this [rt1-ospf-1-area-0.0.0.1]quit	To enter OSPF router configuration mode Set ospf process id and router ID Set area parameter Specify the area for interfaces on a network segment
OSPF Check and Verification [rt1]display ip routing-table [rt1]display ip routing-table protocol ospf [rt1]display ospf peer [rt1]display ospf lsdb summary [rt1]display ospf lsdb [rt1]display ospf routing [rt1]display ospf 1 routing	
Optional [rt1-GigabitEthernet0/0/0]ospf cost 100 [rt1-GigabitEthernet0/0/0]ospf authentication-mode simple plain alamin	Set OSPF cost, By default cost of an interface is calculated as 10^8/BW bps Set OSPF Packet Header Authentication Interface Authentication
[rt1-GigabitEthernet0/0/0]ospf network-type p2p	
ospf Stub Area configuration: [rt1]ospf [rt1-ospf-1]area 1 [rt1-ospf-1-area-0.0.0.1]stub [rt1-ospf-1-area-0.0.0.1]stub no-summary [rt1-ospf-1-area-0.0.0.1]quit	To set stub area To set area 1 as a totally stub area
NSSA area Configuration [rt2]ospf [rt2-ospf-1]area 1 [rt2-ospf-1-area-0.0.0.2]nssa [rt2-ospf-1-area-0.0.0.2]nssa no-summary	To set NSSA Area Totally NSSA Area
Import External route ip route-static 192.168.1.0 255.255.255.0 NULL 0 [rt1-ospf-1]import-route static	Considering router1 has static route Import static route to OSPF
Import default route [rt1]ip route-static 0.0.0.0 0.0.0.0 NULL 0 [rt1]ospf 1 [rt1-ospf-1]default-route-advertise [rt1-ospf-1]default-route-advertise always	If static default route not exist.
Check & Verification [rt1]display ospf lsdb ase 0.0.0.0	

DHCP Server configuration	
DHCP Global Address Pool-based service model configuration	
ip pool ip-pool-name	Command Syntax.
[rt1]ip pool depertment_tech	Create POOL
[rt1-ip-pool-depertment_tech]quit	
[rt1]ip pool depertment_tech	Enter the specific pool
[rt1-ip-pool-depertment_tech]network 192.168.1.0 mask 255.255.255.0	Set network
[rt1-ip-pool-depertment_tech]gateway-list 192.168.1.1	Set gateway list
[rt1-ip-pool-depertment_tech]lease day 1 hour 2	Set lease time
[rt1-ip-pool-depertment_tech]dns-list 8.8.8.8	Set DNS list
[rt1-ip-pool-depertment_tech]excluded-ip-address 192.168.1.200 192.168.1.254	Set excluded ip list start IP and End IP
[rt1-ip-pool-depertment_tech]quit	
Interface Configuration:	
[rt1]dhcp enable	Enable DHCP
[rt1]interface Ethernet 0/0/0	Enter the interface
[rt1-Ethernet0/0/0]ip address 192.168.1.1 24	Set IP address (Gateway address)
[rt1-Ethernet0/0/0]dhcp select global	Set global address pool-based model
[rt1-Ethernet0/0/0]quit	
DHCP Relay agent configuration	
[rt3]interface Ethernet 0/0/0	Enter the interface mode.
[rt3-Ethernet0/0/0]ip address 172.16.1.1 24	Set IP address
[rt3-Ethernet0/0/0]dhcp select relay	Set DHCP relay
[rt3-Ethernet0/0/0]dhcp relay server-ip 192.168.1.1	Set DHCP server IP, Where DHCP pool has already been created.
[rt3-Ethernet0/0/0]quit	
DHCP Check & Verification: [rt1]display ip pool name depertment_tech used	To check IP those are already being used.

ACL & NAT	
The range of possible ACL numbers is different depending on ACL type: • Basic—2000 to 2999 • Advanced—3000 to 3999 • Layer-2—4000 to 4999 • User-defined—5000 to 5999	
Basic ACL rule [rule-id] {deny|permit} [source{source-address source-wildcard|any}|fragment|logging|time-range time-name] [rt1]acl 2000 [rt1-acl-basic-2100]description DENY_Network_1 [rt1-acl-basic-2000]rule deny source 192.168.1.100 0.0.0.0 [rt1-acl-basic-2000]quit [rt1]interface GigabitEthernet 0/0/0 [rt1-GigabitEthernet0/0/0]traffic-filter inbound acl 2000 **Check** [rt1]display acl 2000	

Advance ACL
`rule [rule-id] {deny|permit} ip [destination {destination-address destinationwildcard|any}] [source {source-address source-wildcard|any}]`
 	
`[sw1]acl name block_net`
`[sw1-acl-adv-block_net]rule 0 permit ip destination 192.168.100.100 0.0.0.0 source 172.16.100.100 0.0.0.0`
`[sw1-acl-adv-block_net]quit`
Interface configuration
`[sw1]interface GigabitEthernet 0/0/2`
`[sw1-GigabitEthernet0/0/2]traffic-filter inbound acl name block_net`
`[sw1-GigabitEthernet0/0/2]quits`
Check ACL
`[sw1]display acl name block_net`	

**** For Telnet Security**
`[rt1]user-interface vty 0 4`
`[rt1-ui-vty0-4]acl 2000 inbound`
`[rt1-ui-vty0-4]quit`	

Static NAT:
`[Router] interface gigabitethernet 2/0/0`
`[Router-GigabitEthernet2/0/0] nat static global 202.10.1.3 inside 192.168.0.2`
`[Router-GigabitEthernet2/0/0] quit`	

Dynamic NAT
`[Huawei-Router] acl number 2222`
`[Huawei-Router-acl-basic-2222] rule 5 permit source 10.10.10.0 0.0.0.255`
`[Huawei-Router-acl-basic-2222] quit`
	LAN Interface IP Block

`[Huawei-Router]nat address-group 1 200.200.200.5 200.200.200.10`	WAN IP range
`[Huawei-Router-GigabitEthernet0/0/1]nat outbound 2222 address-group 1 no-pat` • In Cisco we use, “overload” command for PAT. If you do not use this keyword then, it is becoming pure Dynamic NAT. This is reverse in Huawei. Ref: 3	at the WAN Interface

BGP Routing	
Basic BGP Configuration	
[rt1]bgp 64512	
[rt1-bgp]peer 10.0.2.2 as-number 64512	Set peer AS number
[rt1-bgp]peer 10.0.2.2 connect-interface LoopBack 0	Remote interface
[rt1-bgp] [rt1-bgp]network 10.1.1.1 255.255.255.0	To advertise Network.
[rt1-bgp]peer 10.0.14.2 ip-prefix pref_detail_control export	To filter the route.
[rt1-bgp]quit	Exit form BGP configuration mode.
[rt1]ip ip-prefix pref_detail_control index 10 permit 10.1.1.1 32 less-equal 32	To make Prefix list.
[rt2-bgp]display bgp routing-table	To check BGP.

BGP Configuration Flowchart:

- Start a BGP Process.
- Configure a BGP Peer.
- Configure BGP to import Routes.
- Configure BGP Attribute.
- Configure BGP Advertisement-Control. /BGP Filter.
- Check & Verify BGP Configuration.

Start BGP Process <rt8>system-view [rt8]bgp 200 [rt8-bgp]router-id 8.8.8.8	The system view is displayed. A BGP process is enabled. (Optional) Configuring or changing the router ID of BGP results in the reset of the BGP peer relationship between routers
Configuring a BGP Peer. [rt8-bgp]peer 192.168.0.1 as-number 100	Set Peer IP address and Peer AS-Number.
[rt8-bgp]peer 192.168.0.1 description BGP_with_R7	(Optional)Set Description
[rt8-bgp]peer 192.168.0.1 ebgp-max-hop 2	EBGP .There must be a directly connected physical link between EBGP peers. If this requirement is not met, you can use the peer ebgp-max-hop command to configure EBGP peers to establish TCP connections through multiple hops.
[rt8-bgp]peer 192.168.0.1 connect-interface GigabitEthernet 0/0/0	(Optional). To increase the stability and reliability of BGP connections, we can configure the local interface as the loopback interface for BGP connections.
Check & Verification. [rt8]display bgp peer [rt8]display bgp peer verbose [rt8]display bgp peer 192.168.0.1 log-info	

Configuring BGP Import route:

BGP itself cannot discover routes

BGP routes are imported in either of the following modes:

- The **import** command imports routes based on protocol types, such as RIP routes, OSPF routes, Intermediate System to Intermediate System (IS-IS) routes, static routes, or direct routes.
- The **network** command imports a route with the specified prefix and mask to the BGP routing table, which is more precise than the previous mode.

`[rt8-bgp]import-route ospf 1 med 1`
`[rt8-bgp]import-route static`
`[rt8-bgp]default-route imported`
	import-route *protocol* [*process-id*] [**med** *med* | **route-policy** *route-policyname*]
	Import route from other protocols.
	(Optional). To import default route

`[rt8-bgp]network 192.168.0.0 24`	**network** *ipv4-address* [*mask* | *mask-length*] [**route-policy** *route-policyname*] BGP is configured to import local routes

Configuring BGP Route Attributes

- Configuring route attributes can change route selection results.
  BGP has many route attributes. You can change route selection results by configuring attributes for routes.

BGP priority

Setting the BGP priority can control route selection between BGP routes and routes of other routing protocols.

Preferred values

After preferred values are set for BGP routes, the route with the greatest value is preferred when multiple routes to the same destination exist in the BGP routing table.

Local_Pref

The Local_Pref attribute has the same function as the preferred value of a route. If both of them are configured for a BGP route, the preferred value takes precedence over the Local_Pref attribute.

MED

The MED attribute is used to determine the optimal route for traffic that enters an AS. The route with the smallest MED value is selected as the optimal route if the other attributes of the routes are the same.

Next_Hop

BGP route selection can be controlled by changing Next_Hop attributes for routes.

AS_Path

The AS_Path attribute is used to prevent rooting loops and control route selection.

Setting the BGP Priority:
Syntax: **preference** { *external internal local* | **route-policy** *route-policy-name* }
`[rt8-bgp]preference 5 2 1`
	By default, the priority of EBGP external routes, IBGP internal routes, and BGP local routes is 255.
	5 is EBGP preference value, 2 for IBGP,1 for locally generated route.

Setting the Preferred value for peer: **Syntax**: **peer** { *group-name* | *ipv4-address* } **preferred-value** *value* `[rt8-bgp]peer 192.168.0.1 preferred-value 1`	Set the peer preferred-value. By default, the original preferred value of a route learned from a peer is 0

Set local_pref: **Syntax: default local-preference** *local-preference* [rt8-bgp]default local-preference 105	The Local_Pref attribute is used to determine the optimal route for the traffic that leaves an AS. By default, the local preference of BGP is 100.
Configuring MED Syntax: **default med** *med* [rt8-bgp]default med 120 [rt8-bgp]compare-different-as-med	After the MED attributes of routes are set, an EBGP peer selects the route with the smallest MED value for the traffic that enters an AS if the other attributes of the routes are the same. The **default med** command is valid only for routes imported using the **import-route** command and BGP summarized routes on the local device. The MED values of routes from different ASs are compared. By default, the BGP device compares the MED values of only routes from different peers in the same AS
Setting Next_hop Syntax: **peer** { *ipv4-address* | *group-name* } **next-hop-local** [rt8-bgp]peer 192.168.0.1 next-hop-local	By default, a device does not change the next hop address of a route learned from an EBGP peer before forwarding the route to IBGP peers. The next hop address of a route advertised by an EBGP peer to this device is the address of the EBGP peer. It relates to ASBR.
Setting AS_Path Syntax: **peer** { *ipv4-address* | *group-name* } **allow-as-loop** [*number*] [rt8-bgp]peer 192.168.0.1 allow-as-loop	In most cases, a BGP router checks the AS_Path attribute of a route received from a peer. If the local AS number is carried by the route, the BGP router discards this route to avoid routing loops.
Setting Community Attribute: peer { ipv4-address | group-name } advertise-community peer { ipv4-address | group-name } advertise-ext-community peer { ipv4-address | group-name } route-policy route-policy-name export [rt8-bgp]peer 192.168.0.1 advertise-community	BGP is configured to advertise the standard community attribute to a peer or a peer group. By default, the community attribute is not advertised to any peer or peer group. So we neet to set route policy.

BGP Filter:

There are usually a large number of routes in a BGP routing table.
BGP can filter routes to be advertised to a specific peer or peer group.
ACL, IP-Prefix,AS_Path,Community, Extcommunity, Route-Policy

Set ACL: [rt7]acl 2000 rule 0 permit source 172.16.0.192 0.0.0.64 [rt7-acl-basic-2000]quit [rt7-bgp] bgp 100 [rt7-bgp]peer 192.168.0.2 filter-policy 2000 export	Set Basic ACL Filter Using ACL
IP-Prefix: Syntax: **ip ip-prefix** *ip-prefix-name* [**index** *index-number*] { **permit** | **deny** } *ipaddress mask-length* [**greater-equal** *greater-equal-value*] [**less-equal** *less-equal-value*] [rt7]ip ip-prefix outgoing_traffic_1 index 1 permit 172.16.0.192 26 less-equal 26 [rt7-bgp] bgp 100 [rt7-bgp]peer 192.168.0.2 ip-prefix outgoing_traffic-1 export	Set IP-Prefix list
AS-Path filter Syntax: **ip as-path-filter** { *as-path-filter-number* | *as-path-filter-name* }{ **permit** | **deny** } *regular-expression* [rt7]ip as-path-filter as_1 permit 6551* [rt7]bgp 100 [rt7-bgp]peer 192.168.0.2 as-path-filter as_1 export	AS path configuration Filter using AS
Community filter [RouterA] route-policy comm_policy permit node 10 [RouterA-route-policy] apply community no-export [RouterA-route-policy] quit [RouterA] bgp 10 [RouterA-bgp] ipv4-family unicast [RouterA-bgp-af-ipv4] peer 200.1.2.2 route-policy comm_policy export [RouterA-bgp-af-ipv4] peer 200.1.2.2 advertise-community	BGP communities allow routers to tag routes with an indicator (the community) and allow other routers to make decisions based on that tag. Communities are not restricted to one network or one autonomous system, and they have no physical boundaries
Route Policy: route-policy route-policy-name { permit | deny } node node [rt7]route-policy policy_1 permit node 15	

[rt7-route-policy]if-match ip-prefix outgoing_traffic_1 [rt7-route-policy]apply as-path 300 additive	

BGP Check & Verification & reset/refresh	
[rt7]display bgp routing-table [rt7]display ip community-filter [rt7]display bgp routing-table as-path-filter as_1 [rt7]display bgp peer [rt7]display bgp network [rt7]display bgp peer verbose [rt7]display bgp routing-table different-origin-as [rt7]display acl 2000 [rt7]display route-policy policy_1 Refreshing BGP RoutesWhen BGP routing policy changes, it is required to re-compute associated routeinformation <rt7>refresh bgp all export After the user changes BGP policy or protocol configuration, they must cut off thecurrent connection so as to enable the new configuration. <rt7>reset bgp 192.168.0.2 flap-info <rt7>reset bgp all	Reset BGP-peer address Clear all connections of BGP

MPLS BGP VPN Basic Configuration:

The Multiprotocol Label Switching (MPLS) protocol is used on Internet Protocol (IP) backbone networks. MPLS uses connection-oriented label switching on connectionless IP networks

"Multiprotocol" in MPLS means that multiple network protocols are supported

MPLS is widely used for virtual private network (VPN), traffic engineering (TE), and quality of service (QoS)

LSR: network devices that swap MPLS labels and forward packets are label switching routers (LSRs), which form an MPLS domain LSRs that reside at the edge of the MPLS domain and connect to other networks are called label edge routers (LERs), and LSRs within the MPLS domain are core LSRs

A path along which IP packets are transmitted on an MPLS network is called a label switched path (LSP)

LDP
The Label Distribution Protocol (LDP) is designed for distributing labels. It sets up an LSP hop by hop according to Interior Gateway Protocol (IGP) and Border Gateway Protocol (BGP) routing information.

LDP
The Label Distribution Protocol (LDP) is designed for distributing labels. It sets up an LSP hop by hop according to Interior Gateway Protocol (IGP) and Border Gateway Protocol (BGP) routing information.

MP-BGP
MP-BGP is an extension to BGP and allocates labels to MPLS VPN routes and inter-AS VPN routes.

MPLS labels are distributed from downstream LSRs to upstream LSRs.

MPLS Forwarding Process:
Label operations involved in MPLS packet forwarding include push, swap, and pop

CE(Customer edge): A device that is deployed at the edge of a customer.
PE(Provider edge): A device at the edge of a carrier network, directly connected to a CE device.
P(Provider): It is a backbone device on carrier network.

RD (Route Distinguisher): An RD is a VPN route identifier consisting of eight bytes. On the same PE device, the RD for each VPN must be unique.

- To solve conflict routes during route advertisement RD is used.

VRF(Virtual Routing and Forwarding) is used when you want separation in routing table with the router.

- To solve local route conflict. [ref 6]

Why BGP is widely used for MPLS VPN.

- BGP is the unique routing protocol that supports a large number of VPN routes.
- BGP packets use TLV structure , which facilitates expansion.
- BGP can transmit any additional information attached to route information as optional attributes to BGP neighbors.

MPLS Configuration	
MPLS Configuration: [rt2]mpls lsr-id 2.2.2.2 [rt2]mpls [rt2-mpls]lsp-trigger all [rt2-mpls]quit	Specify LSR(Label Switched Router) identifier Configure LSP trigger policy
MPLS interface configuration: [rt2]mpls ldp [rt2-mpls-ldp]quit [rt2-GigabitEthernet0/0/1]mpls [rt2-GigabitEthernet0/0/1]mpls ldp [rt2-GigabitEthernet0/0/1]quit	Specify MPLS(Multiprotocol Label Switching)configurationinformation to set Label Distribution Protocol(LDP)
MPLS VPN configure: [rt2]ip vpn-instance vpn1 [rt2-vpn-instance-vpn1]route-distinguisher 100:1 [rt2-vpn-instance-vpn1-afipv4]vpn-target 100:1 both [rt2-vpn-instance-vpn1-afipv4]quit [rt2-vpn-instance-vpn1]quit **Bind Interfaces to VPN-Instances** [rt2-GigabitEthernet0/0/0]ip binding vpn-instance vpn1 [rt2-GigabitEthernet0/0/0] ip address 10.1.1.1 255.255.255.0	To set VPN instance name Set route distinguisher (RD) of current IPv4-family for VPN instance Set VPN-Target for current VPN instance, Both means import & export CE interface of PE router, After this command we need to configure ip address Set IP Address
configure MP-BGP [rt2]bgp 100 [rt2-bgp]ipv4-family vpnv4 [rt2-bgp-af-vpnv4]peer 3.3.3.3 enable [rt2-bgp-af-vpnv4]quit [rt2-bgp]ipv4-family vpn-instance vpn1 [rt2-bgp-vpn1]peer 10.1.1.2 as-number 64520 [rt2-bgp-vpn1]import-route direct [rt2-bgp-vpn1]quit	Specify VPNv4 address family BGP peer PE to P/PE to PE BGP for CE to PE BGP PE to CE Import route Exit
[rt2-bgp]display bgp vpnv4 vpn-instance vpn1 peer [rt2-bgp]display bgp vpnv4 all peer [rt2-bgp]display ip routing-table vpn-instance vpn1	[rt1]ping -a 100.0.0.1 100.0.1.1 [rt1]tracert -a 100.0.0.1 100.0.1.1 Ping for CE to CE.

GRE Tunnel

```
system-view
[Huawei-Router1] interface Tunnel 1/1/1
[Huawei-Router1-Tunnel1/1/1] ip address 10.0.0.1 24
[Huawei-Router1-Tunnel1/1/1] tunnel-protocol gre
[Huawei-Router1-Tunnel1/1/1] source 100.100.100.1 24
[Huawei-Router1-Tunnel1/1/1] destination 200.200.200.1 24
[Huawei-Router1-Tunnel1/1/1] quit
```

configure Router 2. We will configure the same things in Router 2, only the IP addresses will change.

```
system-view
[Huawei-Router2] interface Tunnel 1/1/1
[Huawei-Router2-Tunnel1/1/1] ip address 10.0.0.2 24
[Huawei-Router2-Tunnel1/1/1] tunnel-protocol gre
[Huawei-Router2-Tunnel1/1/1] source 200.200.200.1 24
[Huawei-Router2-Tunnel1/1/1] destination 100.100.100.1 24
[Huawei-Router2-Tunnel1/1/1] quit
```

Static Routes

After Tunnel configuration, we need to tell the routes of indirectly connected networks to the routers. Here, we will do it with Static Routes.

```
[Huawei-Router1] ip route-static 172.16.2.0 24 Tunnel 1/1/1
[Huawei-Router2] ip route-static 172.16.1.0 24 Tunnel 1/1/1
```

Verification

To verify Hawei GRE Tunnel, we can use “display interface Tunnel” and “display ip routing-table“

```
[Huawei-Router1] display interface Tunnel
```

SNMP Configuration

```
[rt1]snmp-agent
[rt1]snmp-agent sys-info contact admin:101928
[rt1]snmp-agent sys-info location bangladesh
[rt1]snmp-agent sys-info version v3
[rt1]snmp-agent trap source GigabitEthernet 0/0/0
[rt1]snmp-agent trap enable
```

`[rt1]snmp-agent target-host trap address udp-domain 192.168.1.1 source GigabitEthernet 0/0/0 udp-port 162 public-net  params securityname 1`
 	
`[rt1]snmp-agent local-engineid 982AF097DE8`
`[rt1]snmp-agent community read monitor_read_only`
`[rt1]snmp-agent community write monitor_read_write`
 	
`[rt1]display snmp-agent  community`
`[rt1]display snmp-agent sys-info`
 	
REF: 13
	Set local engine ID hexadecimal ID it is

References:

1. HCNA Networking Study Guide(2016), Huawei Technologies Co., Ltd.
2. S2750&S5700&S6700 Series Ethernet Switches V200R005C00 Typical Configuration Examples
3. [ref 3] https://ipcisco.com/nat-configuration-on-huawei-routers/
4. HUAWEI NetEngine80E/40E Router V600R001C00 Configuration Guide - IP Routing
5. HUAWEI NetEngine80E/40E Router V600R001C00 Configuration Guide - MPLS
6. [ref 6] https://community.cisco.com/t5/routing/why-we-use-vrf-and-tell-me-for-how-many-purpose-it-use-please/td-p/2161205

**Software : eNSP V100R002C00B500

Md. Al-amin.
mdalaminbangladesh@gmail.com