

OSPF Configuration

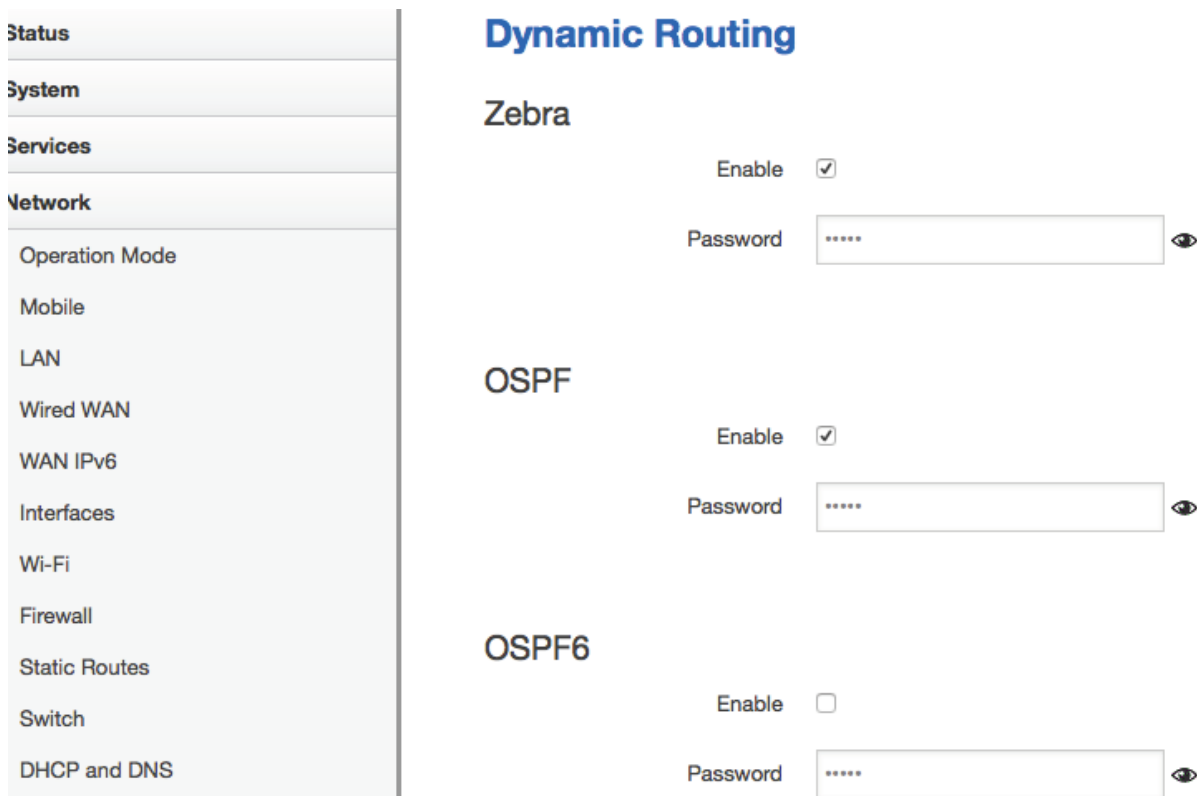
Network topology:

Router A: Lan subnet 192.168.2.0/24, WAN ip address: 192.168.1.118

Router B: Lan subnet 192.168.3.0/24, WAN ip address: 192.168.1.138

Router C: Lan subnet 192.168.1.0/24, Router A and Router B's WAN ports connect to Router C.

1. Enable OSPF on Router A. Open page Network→Dynamic Routing, check enable of zebra, and enable OSPF also, then click button “Save & Apply”



Status
System
Services
Network
Operation Mode
Mobile
LAN
Wired WAN
WAN IPv6
Interfaces
Wi-Fi
Firewall
Static Routes
Switch
DHCP and DNS

Dynamic Routing

Zebra

Enable

Password

OSPF

Enable

Password

OSPF6

Enable

Password

2. Config firewall. Open page Network→Firewall → Traffic Rules.

General Settings Port Forwards Traffic Rules Source NAT DMZ Security

Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts.

Traffic Rules

Name	Match	Action	Enabled
Allow-All-LAN-Ports	Any traffic From <i>any host</i> in <i>wan</i> To <i>any host</i> , ports <i>1-65535</i> in <i>lan</i>	Accept forward	<input type="checkbox"/>
Allow-DHCP-Renew	IPv4-UDP From <i>any host</i> in <i>wan</i> To <i>any router IP</i> at port <i>68</i> on <i>this device</i>	Accept input	<input checked="" type="checkbox"/>
Allow-Ping-WAN	IPv4-ICMP with type <i>echo-request</i> From <i>any host</i> in <i>wan</i> To <i>any router IP</i> on <i>this device</i>	Accept input	<input checked="" type="checkbox"/>
Allow-IGMP	IPv4-IGMP From <i>any host</i> in <i>wan</i> To <i>any router IP</i> on <i>this device</i>	Accept input	<input checked="" type="checkbox"/>

3. Scroll down,, input name (OSPF) at section “Open ports on router” , then click button “Add”.

Allow-ICMPv6-Forward IPv6-ICMP with types *echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type*
From *any host* in *wan*
To *any host* in *any zone*

Accept forward and limit to 1000 pkts. per second

Open ports on router:

Name	Protocol	External port
<input type="text" value="OSPF"/>	<input type="text" value="TCP+UDP"/>	<input type="text"/>

4. At the rule page, select “Protocol” to “—custom --”, then input “ospf”. Click button “Save & Apply”

Firewall - Traffic Rules - OSPF

This page allows you to change advanced properties of the traffic rule entry, such as matched source and

Rule is enabled




Name

Restrict to address family

Protocol

Match ICMP type

Source zone

- Any zone
- lan: lan: 
- openvpn: (empty)
- vpnzone: (empty)
- wan: wan:  wan6:  ifmobile: (empty)

5. telnet to router to config OSPF, the telnet port for OSPF is 2604

```
root@TR-1815-LTE:~# telnet localhost 2604
```

```
Entering character mode  
Escape character is '^]'.  
  
Hello, this is Quagga (version 0.99.22.4).  
Copyright 1996-2005 Kunihiro Ishiguro, et al.
```

```
User Access Verification
```

```
Password:  
TR-1815-LTE>  
TR-1815-LTE> en  
TR-1815-LTE> enable  
TR-1815-LTE#  
TR-1815-LTE# con term  
TR-1815-LTE(config)#  
TR-1815-LTE(config)# router ospf  
TR-1815-LTE(config-router)#  
TR-1815-LTE(config-router)# route  
TR-1815-LTE(config-router)# router-id 192.168.1.118  
TR-1815-LTE(config-router)#  
TR-1815-LTE(config-router)# network 192.168.1.0/24 area 1  
TR-1815-LTE(config-router)#  
TR-1815-LTE(config-router)# network 192.168.2.0/24 area 1  
TR-1815-LTE(config-router)#  
TR-1815-LTE(config-router)# write file  
Configuration saved to /etc/quagga/ospfd.conf  
TR-1815-LTE(config-router)#  
TR-1815-LTE(config-router)# q  
TR-1815-LTE(config)#  
TR-1815-LTE(config)# q  
TR-1815-LTE#  
TR-1815-LTE# q
```

```
Connection closed by foreign host
```

6. Enable OSPF and Zebra on Router B, and config traffic rules as same as Router A, then config OSPF:

Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

```
Password:
CM685V_W>
CM685V_W> en
CM685V_W#
CM685V_W# conf te
CM685V_W(config)#
CM685V_W(config)# router ospf
CM685V_W(config-router)#
CM685V_W(config-router)# router-id 192.168.1.138
CM685V_W(config-router)#
CM685V_W(config-router)# network 192.168.1.0/24
% Command incomplete.
CM685V_W(config-router)#
CM685V_W(config-router)# network 192.168.1.0/24 area 1
CM685V_W(config-router)#
CM685V_W(config-router)# network 192.168.3.0/24 area 1
CM685V_W(config-router)#
CM685V_W(config-router)# write file
Configuration saved to /etc/quagga/ospfd.conf
CM685V_W(config-router)#
CM685V_W(config-router)# q
CM685V_W(config)#
CM685V_W(config)# q
CM685V_W#
CM685V_W# q
```

Connection closed_by foreign host

7. check route in CLI.

```
Kernel IP routing table
Destination      Gateway         Genmask        Flags Metric Ref    Use Iface
default          192.168.1.1    0.0.0.0        UG    0      0      0 eth0.2
192.168.1.0     *              255.255.255.0  U     0      0      0 eth0.2
192.168.1.1     *              255.255.255.255 UH    0      0      0 eth0.2
192.168.2.0     *              255.255.255.0  U     0      0      0 br-lan
192.168.3.0     192.168.1.138 255.255.255.0  UG    20     0      0 eth0.2
root@TR-1815-LTE:~#
```

```

root@CM685V_W:~# route
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
default          192.168.1.1    0.0.0.0          UG    0     0     0 eth0.2
192.168.1.0     *               255.255.255.0   U     0     0     0 eth0.2
192.168.1.1     *               255.255.255.255 UH    0     0     0 eth0.2
192.168.2.0     192.168.1.118 255.255.255.0   UG    20    0     0 eth0.2
192.168.3.0     *               255.255.255.0   U     0     0     0 br-lan
root@CM685V W:~# █

```

8. check route on GUI.

Status

- Overview
- Network
- Firewall
- Routes
- System Log
- Kernel Log
- Reboot Log
- Realtime Graphs
- VPN

System

Services

Network

Logout

Routes

The following rules are currently active on this system.

ARP

IPv4-Address	MAC-Address	In
192.168.1.138	90:22:06:c0:04:00	et
192.168.1.1	90:22:06:80:53:69	et
192.168.2.100	3c:07:54:76:91:5e	br

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric
wan	0.0.0.0/0	192.168.1.1	0
wan	192.168.1.0/24		0
wan	192.168.1.1		0
lan	192.168.2.0/24		0
wan	192.168.3.0/24	192.168.1.138	20

Status
Overview
Network
Firewall
Routes
System Log
Kernel Log
Reboot Log
Realtime Graphs
VPN
System
Services
Network
Logout

Routes

The following rules are currently active on this system.

ARP

IPv4-Address	MAC-Address	In
192.168.1.1	90:22:06:80:53:69	et
192.168.1.118	90:22:06:c0:53:50	et

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric
wan	0.0.0.0/0	192.168.1.1	0
wan	192.168.1.0/24		0
wan	192.168.1.1		0
wan	192.168.2.0/24	192.168.1.118	20
lan	192.168.3.0/24		0

9. check ping and traceroute

```
dentydeMacBook-Pro-3:~ apple$ ping 192.168.3.1
PING 192.168.3.1 (192.168.3.1): 56 data bytes
64 bytes from 192.168.3.1: icmp_seq=0 ttl=63 time=1.472 ms
64 bytes from 192.168.3.1: icmp_seq=1 ttl=63 time=1.430 ms
^C
--- 192.168.3.1 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.430/1.451/1.472/0.021 ms
dentydeMacBook-Pro-3:~ apple$ traceroute 192.168.3.1
traceroute to 192.168.3.1 (192.168.3.1), 64 hops max, 52 byte packets
 1 tr-1815-lte (192.168.2.1)  1.389 ms  0.743 ms  0.675 ms
 2 192.168.3.1 (192.168.3.1)  1.437 ms  1.382 ms  1.308 ms
dentydeMacBook-Pro-3:~ apple$
```