**DYMEC 3170XR**

**Industrial Managed Ethernet Router User Manual**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**



|  |
| --- |
| Firmware Version 1.1.14User’s ManualVersion 1.0Compliant: For Military contract that require the continuous monitoring and protection of industrial control systems (ICS) Networks Operating / monitoring the operating utilities such as Water, Sewer, Electrical, Security, Video, Building Controls, Street and Intelligent Transportation Systems (ITS).**Uses: Cyber-Lock, IP Device Binding, Cyber-Secure Video, Clean Code Technology, & Secure Console / Chassis (Patent Pending)****Meets NSA Guidelines for Secure Network Endpoints** |

**COPYRIGHT NOTICE**

Copyright © 2018 DYMEC, LLC.All rights reserved.

No part of this publication may be reproduced in any form without the prior written consent of DYMEC, LLC.

**TRADEMARKS**

**DYMEC & 3170** are registered trademarks of K-USA, LLC

All other trademarks belong to their respective owners.

**REGULATORY COMPLIANCE STATEMENT**

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specifications section for more details.

**WARRANTY**

DYMEC warrants that all DYMEC products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). DYMEC will repair or replace products found by DYMEC to be defective within this warranty period, with shipment expenses apportioned by DYMEC and the distributor. This warranty does not cover product modifications or repairs done by persons other than DYMEC approved personnel, and this warranty does not apply to DYMEC products that are misused, abused, improperly installed, or damaged by accidents.

Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

**DISCLAIMER**

Information in this publication is intended to be accurate. DYMEC shall not be responsible for its use or infringements on third-parties because of its use. There may occasionally be unintentional errors on this publication. DYMEC reserves the right to revise the contents of this publication without notice.

**CONTACT INFORMATION**

DYMEC, LLC

Kansas City, MO 64014

Telephone: (816) 988-7861

Website: www.DYMEC.com

Technical Support

E-mail: Sales@DYMEC.com

Sales Contact

E-mail: sales@DYMEC.com

support@DYMEC.com

Content

VLAN IP4

Static Route5

GRE Tunnel7

IPSec11

OSPFv216

# VLAN IP

We usually configure VLANs to divide broadcast domains in the Local Area Network (LAN). To communicate with others in another VLAN, we need the device to support inter-VLAN routing. Users can use VLANs to create Layer 3 interfaces by assigning IP address in different subnets to the VLAN. Before configuring any kind of routing protocols, users have to make sure the VLAN IP Address is configured.

Configure VLAN IP Address

* **Configure VLAN IP Address** (VLAN Mode)

**Cmd:** ip address [IP\_ADDR] [NETMASK]

* **Display VLAN IP Address** (VLAN Mode)

**Cmd:** show ip address

* **Remove VLAN IP Address** (VLAN Mode)

**Cmd:** no ip address

* **Display All Configured VLAN IP Address** (Config Mode)

**Cmd:** show vlan ip table

# Static Route

 **Static Routing** is the most basic routing method for IT networking. Users have to manually-configure the routing entries into a routing table. **Static Route** is fixed and unchanged, even if the Network is changed. **Static Route** is best configured as a gateway of last resort. The Network administrator has full and complete control over static routing’s behavior. The network design engineer must have enough background knowledge to handle its complexities and nuances.

Configuring A Static Route

 All the following commands are under **config mode**

* **Add Static Route**

**Cmd:** ip route [IP\_ADDR] [NETMASK:0-32] [NEXT\_HOP]

* **Display Static Route**

**Cmd:** show ip route static

* **Delete Static Route**

**Cmd:** no ip route [IP\_ADDR] [NETMASK:0-32]

Static Route Example

In the following diagram, we are going to configure a topology with Static Route for the network. Note that there are 3 networks in this drawing – each with its own color.

Network – 192.168.10.x (Magenta)

Network – 192.168.11.x (Brown)

Network – 192.168.10.x (Green)



* **Configurations for RA**

|  |  |
| --- | --- |
| **Command** | **Description** |
| Switch> enable | Enter “Privileged mode” |
| Switch# configure terminal | Enter “Configuration mode” |
| Switch(config)# vlan 1 | Enter “VLAN mode” for VLAN 1 |
| Switch(config-vlan1)# ip address 192.168.11.182 255.255.255.0 | Configure IP Address to “192.168.11.182” for VLAN 1 |
| Switch(config-vlan1)# vlan 2 | Enter “VLAN mode” for VLAN 2 |
| Switch(config-vlan2)# ip address 192.168.12.182 255.255.255.0 | Configure IP Address to “192.168.12.182” for VLAN 2 |
| Switch(config-vlan2)# member tag 11 | Add Lan11 to VLAN 2 with tagged |
| Switch(config-vlan2)# exit | Exit “VLAN mode”, back to “Configuration mode” |
| Switch(config)# ip route 192.168.10.0 24 192.168.12.166 | Configure static router for subnet 192.168.10.0/24.The next hop is 192.168.12.166 |

* **Configurations for RB**

|  |  |
| --- | --- |
| **Command** | **Description** |
| Switch> enable | Enter “Privileged mode” |
| Switch# configure terminal | Enter “Configuration mode” |
| Switch(config)# vlan 1 | Enter “VLAN mode” for VLAN 1 |
| Switch(config-vlan1)# ip address 192.168.10.166 255.255.255.0 | Configure IP Address to “192.168.10.166” for VLAN 1 |
| Switch(config-vlan1)# vlan 2 | Enter “VLAN mode” for VLAN 2 |
| Switch(config-vlan2)# ip address 192.168.12.166 255.255.255.0 | Configure IP Address to “192.168.12.166” for VLAN 2 |
| Switch(config-vlan2)# member tag 8 | Add Lan8 to VLAN 2 with tagged |
| Switch(config-vlan2)# exit | Exit “VLAN mode”, back to “Configuration mode” |
| Switch(config)# ip route 192.168.11.0 24 192.168.12.182 | Configure static router for subnet 192.168.11.0/24.The next hop is 192.168.12.182 |

# GRE Tunnel

 **GRE** implies **Generic Routing Encapsulation**. It is a communication protocol that used to build up a direct point-to-point connection between network devices. **GRE Tunnel** is a virtual point-to-point link between two networks. And **GRE** can encapsulate a wide variety of network protocols inside the tunnel over an Internet Protocol Network. **GRE Tunnel** provides higher security than normal Network environment and it is also a niche to connect two detached subnetworks.

Configure GRE Tunnel

 All the following commands are under **config mode**

* **Configure GRE Tunnel Source & Destination**

**Cmd:** tunnel gre [1-4] src-dest [SOURCE\_IP\_ADDR] [DESTINATION\_IP\_ADDR]

* **Display GRE Tunnel Source & Destination**

**Cmd:** show tunnel gre [1-4] src-dest

* **Remove GRE Tunnel Source & Destination**

**Cmd:** no tunnel gre [1-4] src-dest

* **Configure GRE Tunnel Private IP Address**

**Cmd:** tunnel gre [1-4] ip address [IP\_ADDR] [NETMASK]

* **Display GRE Tunnel Private IP Address**

**Cmd:** show tunnel gre [1-4] ip address

* **Remove GRE Tunnel Private IP Address**

**Cmd:** no tunnel gre [1-4] ip address

* **Enable/Disable GRE Tunnel**

**Cmd:** tunnel gre [1-4] operation [enable | disable]

* **Display GRE Tunnel State**

**Cmd:** show tunnel gre [1-4] operation

GRE Tunnel Example

 In the following diagram, we are going to configure a topology with Static Route and GRE Tunnel for the system.



* **Configurations for RA**

|  |  |
| --- | --- |
| **Command** | **Description** |
| Switch> enable | Enter “Privileged mode” |
| Switch# configure terminal | Enter “Configuration mode” |
| Switch(config)# vlan 1 | Enter “VLAN mode” for VLAN 1 |
| Switch(config-vlan1)# ip address 192.168.11.182 255.255.255.0 | Configure IP Address to “192.168.11.182” for VLAN 1 |
| Switch(config-vlan1)# vlan 6 | Enter “VLAN mode” for VLAN 6 |
| Switch(config-vlan6)# ip address 192.168.6.182 255.255.255.0 | Configure IP Address to “192.168.6.182” for VLAN 6 |
| Switch(config-vlan6)# member tag 11 | Add Lan11 to VLAN6 with tagged |
| Switch(config-vlan6)# exit | Exit “VLAN mode”, back to “Configuration mode” |
| Switch(config)# tunnel gre 1 src-dest 192.168.6.182 192.168.7.166 | Configure GRE Tunnel’s local and remote IP.First parameter is “Local”, second one is “Remote” |
| Switch(config)# tunnel gre 1 ip address 172.1.1.1 30 | Configure GRE Tunnel’s private IP Address |
| Switch(config)# tunnel gre 1 operation enable | Enable GRE Tunnel 1 |
| Switch(config)# ip route 192.168.10.0 24 172.1.1.2 | Configure static router for subnet 192.168.10.0/24.The next hop is 172.1.1.2 |
| Switch(config)# ip route 192.168.7.0 24 192.168.6.108 | Configure static router for subnet 192.168.7.0/24.The next hop is 192.168.6.108 |

* **Configurations for RB**

|  |  |
| --- | --- |
| **Command** | **Description** |
| Switch> enable | Enter “Privileged mode” |
| Switch# configure terminal | Enter “Configuration mode” |
| Switch(config)# vlan 1 | Enter “VLAN mode” for VLAN 1 |
| Switch(config-vlan1)# ip address 192.168.10.166 255.255.255.0 | Configure IP Address to “192.168.10.166” for VLAN 1 |
| Switch(config-vlan1)# vlan 7 | Enter “VLAN mode” for VLAN 7 |
| Switch(config-vlan7)# ip address 192.168.7.166 255.255.255.0 | Configure IP Address to “192.168.7.166” for VLAN 7 |
| Switch(config-vlan7)# member tag 8 | Add Lan8 to VLAN 7 with tagged |
| Switch(config-vlan7)# exit | Exit “VLAN mode”, back to “Configuration mode” |
| Switch(config)# tunnel gre 1 src-dest 192.168.7.166 192.168.6.182 | Configure GRE Tunnel’s local and remote IP.First parameter is “Local”, second one is “Remote” |
| Switch(config)# tunnel gre 1 ip address 172.1.1.2 30 | Configure GRE Tunnel’s private IP Address |
| Switch(config)# tunnel gre 1 operation enable | Enable GRE Tunnel 1 |
| Switch(config)# ip route 192.168.11.0 24 172.1.1.1 | Configure static router for subnet 192.168.11.0/24.The next hop is 172.1.1.1 |
| Switch(config)# ip route 192.168.6.0 24 192.168.7.108 | Configure static router for subnet 192.168.6.0/24.The next hop is 192.168.7.108 |

* **Configurations for RC**

|  |  |
| --- | --- |
| **Command** | **Description** |
| Switch> enable | Enter “Privileged mode” |
| Switch# configure terminal | Enter “Configuration mode” |
| Switch(config)# vlan 1 | Enter “VLAN mode” for VLAN 1 |
| Switch(config-vlan1)# ip address 192.168.3.108 255.255.255.0 | Configure IP Address to “192.168.3.108” for VLAN 1 |
| Switch(config-vlan1)# vlan 6 | Enter “VLAN mode” for VLAN 6 |
| Switch(config-vlan6)# ip address 192.168.6.108 255.255.255.0 | Configure IP Address to “192.168.6.108” for VLAN 6 |
| Switch(config-vlan6)# member tag 8 | Add Lan8 to VLAN6 with tagged |
| Switch(config-vlan6)# vlan 7 | Enter “VLAN mode” for VLAN 7 |
| Switch(config-vlan7)# ip address 192.168.7.108 255.255.255.0 | Configure IP Address to “192.168.7.108” for VLAN 7 |
| Switch(config-vlan7)# member tag 4 | Add Lan4 to VLAN 7 with tagged |
| Switch(config-vlan7)# exit | Exit “VLAN mode”, back to “Configuration mode” |

# IPSec

 **Internet Protocol Security (IPsec)** is a secure Networks protocol for the Internet protocols. It offers the security on the IP Layer to protect the communication data of entire Internet. IPSec provides authentication and confidentiality methods. The authentication function is used to ensure the identities of each other by exchanging host keys and it can prevent the transmitting data from tampering. The other function confidentiality is to encrypt the data of packets to avoid snooping during transmission.

Configure IPSec

 All the following commands are under **config mode**

* **Set IP Address for Local IPSec Interface**

**Cmd:** Ipsec left address [IP\_ADDR]

* **Display IP Address for Local IPSec Interface**

**Cmd:** show ipsec left address

* **Remove IP Address for Local IPSec Interface**

**Cmd:** no ipsec left address

* **Generate Hostkey for Local IPSec Interface**

**Cmd:** ipsec left hostkey

* **Display Hostkey for Local IPSec Interface**

**Cmd:** show ipsec left hostkey

* **Remove Hostkey for Local IPSec Interface**

**Cmd:** no ipsec left hostkey

* **Set IP Address for Remote IPSec Interface**

**Cmd:** ipsec right address [IP\_ADDR]

* **Display IP Address for Remote IPSec Interface**

**Cmd:** show ipsec right address

* **Remove IP Address for Remote IPSec Interface**

**Cmd:** no ipsec right address

* **Configure Hostkey for Remote IPSec Interface**

**Cmd:** ipsec right hostkey [KEY\_PATH]

**Note:** The right hostkey must be saved in the USB

* **Display Hostkey for Remote IPSec Interface**

**Cmd:** show ipsec right hostkey

* **Remove Hostkey for Remote IPSec Interface**

**Cmd:** no ipsec right hostkey

* **Set Key Life Timer**

**Cmd:** ipsec keylife [60-86400secs]

* **Display Key Life Timer**

**Cmd:** show ipsec keylife

* **Remove Key Life Timer**

**Cmd:** no ipsec keylife

* **Enable IPSec Protocol**

**Cmd:** ipsec enable

* **Disable IPSec Protocol**

**Cmd:** no ipsec

* **Display IPSec Protocol State**

**Cmd:** show ipsec state

IPSec Example

 In the following diagram, we are going to configure a topology with Static Route, GRE Tunnel, and IPSec for the system.



* **Configurations for RA**

|  |  |
| --- | --- |
| **Command** | **Description** |
| Switch> enable | Enter “Privileged mode” |
| Switch# configure terminal | Enter “Configuration mode” |
| Switch(config)# vlan 1 | Enter “VLAN mode” for VLAN 1 |
| Switch(config-vlan1)# ip address 192.168.11.182 255.255.255.0 | Configure IP Address to “192.168.11.182” for VLAN 1 |
| Switch(config-vlan1)# vlan 6 | Enter “VLAN mode” for VLAN 6 |
| Switch(config-vlan6)# ip address 192.168.6.182 255.255.255.0 | Configure IP Address to “192.168.6.182” for VLAN 6 |
| Switch(config-vlan6)# member tag 11 | Add Lan11 to VLAN6 with tagged |
| Switch(config-vlan6)# exit | Exit “VLAN mode”, back to “Configuration mode” |
| Switch(config)# tunnel gre 1 src-dest 192.168.6.182 192.168.7.166 | Configure GRE Tunnel’s local and remote IP.First parameter is “Local”, second one is “Remote” |
| Switch(config)# tunnel gre 1 ip address 172.1.1.1 30 | Configure GRE Tunnel’s private IP Address |
| Switch(config)# tunnel gre 1 operation enable | Enable GRE Tunnel 1 |
| Switch(config)# ip route 192.168.10.0 24 172.1.1.2 | Configure static router for subnet 192.168.10.0/24.The next hop is 172.1.1.2 |
| Switch(config)# ip route 192.168.7.0 24 192.168.6.108 | Configure static router for subnet 192.168.7.0/24.The next hop is 192.168.6.108 |
| Switch(config)# ipsec left address 192.168.6.182 | Configure IPSec local IP address to 192.168.6.182 |
| Switch(config)# ipsec left hostkey | Generate IPSec local hostkey |

* **Configurations for RB**

|  |  |
| --- | --- |
| **Command** | **Description** |
| Switch> enable | Enter “Privileged mode” |
| Switch# configure terminal | Enter “Configuration mode” |
| Switch(config)# vlan 1 | Enter “VLAN mode” for VLAN 1 |
| Switch(config-vlan1)# ip address 192.168.10.166 255.255.255.0 | Configure IP Address to “192.168.10.166” for VLAN 1 |
| Switch(config-vlan1)# vlan 7 | Enter “VLAN mode” for VLAN 7 |
| Switch(config-vlan7)# ip address 192.168.7.166 255.255.255.0 | Configure IP Address to “192.168.7.166” for VLAN 7 |
| Switch(config-vlan7)# member tag 8 | Add Lan8 to VLAN 7 with tagged |
| Switch(config-vlan7)# exit | Exit “VLAN mode”, back to “Configuration mode” |
| Switch(config)# tunnel gre 1 src-dest 192.168.7.166 192.168.6.182 | Configure GRE Tunnel’s local and remote IP.First parameter is “Local”, second one is “Remote” |
| Switch(config)# tunnel gre 1 ip address 172.1.1.2 30 | Configure GRE Tunnel’s private IP Address |
| Switch(config)# tunnel gre 1 operation enable | Enable GRE Tunnel 1 |
| Switch(config)# ip route 192.168.11.0 24 172.1.1.1 | Configure static router for subnet 192.168.11.0/24.The next hop is 172.1.1.1 |
| Switch(config)# ip route 192.168.6.0 24 192.168.7.108 | Configure static router for subnet 192.168.6.0/24.The next hop is 192.168.7.108 |
| Switch(config)# ipsec left address 192.168. 7.166 | Configure IPSec local IP address to 192.168. 7.166 |
| Switch(config)# ipsec left hostkey | Generate IPSec local hostkey |
| Switch(config)# ipsec right address 192.168. 6.182 | Configure IPSec remote IP address to 192.168. 6.182 |
| Switch(config)# ipsec right hostkey key.txt | Configure IPSec remote hostkeyUsers have to save the key in a text file in the USB |
| Switch(config)# ipsec enable | Enable IPSec protocol |
| Switch(config)# show ipsec state | Display IPSec state |

* **Configurations for RC**

|  |  |
| --- | --- |
| **Command** | **Description** |
| Switch> enable | Enter “Privileged mode” |
| Switch# configure terminal | Enter “Configuration mode” |
| Switch(config)# vlan 1 | Enter “VLAN mode” for VLAN 1 |
| Switch(config-vlan1)# ip address 192.168.3.108 255.255.255.0 | Configure IP Address to “192.168.3.108” for VLAN 1 |
| Switch(config-vlan1)# vlan 6 | Enter “VLAN mode” for VLAN 6 |
| Switch(config-vlan6)# ip address 192.168.6.108 255.255.255.0 | Configure IP Address to “192.168.6.108” for VLAN 6 |
| Switch(config-vlan6)# member tag 8 | Add Lan8 to VLAN6 with tagged |
| Switch(config-vlan6)# vlan 7 | Enter “VLAN mode” for VLAN 7 |
| Switch(config-vlan7)# ip address 192.168.7.108 255.255.255.0 | Configure IP Address to “192.168.7.108” for VLAN 7 |
| Switch(config-vlan7)# member tag 4 | Add Lan4 to VLAN 7 with tagged |
| Switch(config-vlan7)# exit | Exit “VLAN mode”, back to “Configuration mode” |

# OSPFv2

 **Open Shortest Path First (OSPF)** is one of several **dynamic routing protocols** and OSPFv2 is for **IPv4** Networks. **OSPF** is the most widely used **interior Gateway Protocol (IGP)** and it is designed for medium-and-large-scale enterprise networks. **OSPF** nodes exchange neighbors’ information via Link-State information and calculate the shortest path with their Cost to transmit packets. **OSPF** is operating under a hierarchical system and divide the system to several Areas by different Area IDs. OSPF nodes only exchange information with the nodes in the same Area.

Configuring OSPFv2

 All the following commands are under **Config Mode**

* **Configure OSPF Router ID**

**Cmd:** router ospf router-id [ROUTER\_ID]

* **Display OSPF Router ID**

**Cmd:** show router ospf router-id

* **Clear OSPF Router ID**

**Cmd:** no router ospf router-id

* **Configure OSPF Network**

**Cmd:** router ospf network [IP\_ADDR] [NETMASK:0-32] [AREA\_ID]

* **Display OSPF Network**

**Cmd:** show router ospf network

* **Remove OSPF Network Rule for Specific Subnet**

**Cmd:** no router ospf network [IP\_ADDR] [NETMASK:0-32]

* **Enable OSPF Authentication with Text on Specific Area**

**Cmd:** router ospf authentication area [AREA\_ID]

* **Enable OSPF Authentication with MD5 on Specific Area**

**Cmd:** router ospf authentication message-digest area [AREA\_ID]

* **Display OSPF Authentication State**

**Cmd:** show router ospf authentication

* **Disable OSPF Authentication on Specific Area**

**Cmd:** no router ospf authentication area [AREA\_ID]

* **Display OSPF Operation Status**

**Cmd:** show router ospf

* **Display OSPF Neighbors’ Status**

**Cmd:** show router ospf neighbor

All the following commands are under **VLAN Mode**

* **Configure OSPF Hello Interval**

**Cmd:** ip ospf hello-interval [1-65535]

The default OSPF Hello Interval is **10** seconds.

* **Display OSPF Hello Interval**

**Cmd:** show ip ospf hello-interval

* **Clear OSPF Hello Interval**

**Cmd:** no ip ospf hello-interval

* **Configure OSPF Dead Interval**

**Cmd:** ip ospf dead-interval [1-65535]

The default OSPF Dead Interval is **4 times** hello interval.

* **Display OSPF Dead Interval**

**Cmd:** show ip ospf dead-interval

* **Clear OSPF Dead Interval**

**Cmd:** no ip ospf dead-interval

* **Enable OSPF Authentication with Text on Specific VLAN**

**Cmd:** ip ospf authentication

* **Enable OSPF Authentication with MD5 on Specific VLAN**

**Cmd:** ip ospf authentication message-digest

* **Display OSPF Authentication State**

**Cmd:** show ip ospf authentication

* **Disable OSPF Authentication on Specific VLAN**

**Cmd:** no ip ospf authentication

* **Configure OSPF Authentication Password**

**Cmd:** ip ospf authentication-key [PASSWD]

* **Display OSPF Authentication Password**

**Cmd:** show ip ospf authentication-key

* **Clear OSPF Authentication Password**

**Cmd:** no ip ospf authentication-key

* **Configure OSPF MD5 Authentication Password**

**Cmd:** ip ospf message-digest-key [KEY\_ID] md5 [PASSWD]

* **Display OSPF MD5 Authentication Password**

**Cmd:** show ip ospf message-digest-key

* **Clear OSPF MD5 Authentication Password**

**Cmd:** no ip ospf message-digest-key [KEY\_ID]

OSPFv2 Example

 In the following diagram, we are going to configure a topology with Dynamic Routing – OSPFv2 for the system. Use the following commands to check the link state after configurations are completed:

* + show router ospf
	+ show router ospf neighbor
	+ show ip route



*\*Simulation Internet by through RC.\**

* **Configurations for RA**

|  |  |
| --- | --- |
| **Command** | **Description** |
| Switch> enable | Enter “Privileged mode” |
| Switch# configure terminal | Enter “Configuration mode” |
| Switch(config)# vlan 1 | Enter “VLAN mode” for VLAN 1 |
| Switch(config-vlan1)# ip address 192.168.11.182 255.255.255.0 | Configure IP Address to “192.168.11.182” for VLAN 1 |
| Switch(config-vlan1)# vlan 6 | Enter “VLAN mode” for VLAN 6 |
| Switch(config-vlan6)# ip address 192.168.6.182 255.255.255.0 | Configure IP Address to “192.168.6.182” for VLAN 6 |
| Switch(config-vlan6)# member tag 4 | Add Lan4 to VLAN6 with tagged |
| Switch(config-vlan6)# exit | Exit “VLAN mode”, back to “Configuration mode” |
| Switch(config)# router ospf router-id 0.0.0.1 | Configure OSPF router id to 0.0.0.1 |
| Switch(config)# router ospf network 192.168.11.0 24 0 | Configure subnet 192.168.11.0/24 to join OSPF network area 0 |
| Switch(config)# router ospf network 192.168.6.0 24 0 | Configure subnet 192.168.6.0/24 to join OSPF network area 0 |

* **Configurations for RB**

|  |  |
| --- | --- |
| **Command** | **Description** |
| Switch> enable | Enter “Privileged mode” |
| Switch# configure terminal | Enter “Configuration mode” |
| Switch(config)# vlan 1 | Enter “VLAN mode” for VLAN 1 |
| Switch(config-vlan1)# ip address 192.168.10.166 255.255.255.0 | Configure IP Address to “192.168.10.166” for VLAN 1 |
| Switch(config-vlan1)# vlan 7 | Enter “VLAN mode” for VLAN 7 |
| Switch(config-vlan7)# ip address 192.168.7.166 255.255.255.0 | Configure IP Address to “192.168.7.166” for VLAN 7 |
| Switch(config-vlan7)# member tag 6 | Add Lan6 to VLAN 7 with tagged |
| Switch(config-vlan7)# exit | Exit “VLAN mode”, back to “Configuration mode” |
| Switch(config)# router ospf router-id 0.0.0.2 | Configure OSPF router id to 0.0.0.2 |
| Switch(config)# router ospf network 192.168.10.0 24 0 | Configure subnet 192.168.10.0/24 to join OSPF network area 0 |
| Switch(config)# router ospf network 192.168.7.0 24 0 | Configure subnet 192.168.7.0/24 to join OSPF network area 0 |

* **Configurations for RC**

|  |  |
| --- | --- |
| **Command** | **Description** |
| Switch> enable | Enter “Privileged mode” |
| Switch# configure terminal | Enter “Configuration mode” |
| Switch(config)# vlan 1 | Enter “VLAN mode” for VLAN 1 |
| Switch(config-vlan1)# ip address 192.168.3.108 255.255.255.0 | Configure IP Address to “192.168.3.108” for VLAN 1 |
| Switch(config-vlan1)# vlan 6 | Enter “VLAN mode” for VLAN 6 |
| Switch(config-vlan6)# ip address 192.168.6.108 255.255.255.0 | Configure IP Address to “192.168.6.108” for VLAN 6 |
| Switch(config-vlan6)# member tag 8 | Add Lan8 to VLAN6 with tagged |
| Switch(config-vlan6)# vlan 7 | Enter “VLAN mode” for VLAN 7 |
| Switch(config-vlan7)# ip address 192.168.7.108 255.255.255.0 | Configure IP Address to “192.168.7.108” for VLAN 7 |
| Switch(config-vlan7)# member tag 4 | Add Lan4 to VLAN 7 with tagged |
| Switch(config-vlan7)# exit | Exit “VLAN mode”, back to “Configuration mode” |
| Switch(config)# router ospf router-id 0.0.0.3 | Configure OSPF router id to 0.0.0.3 |
| Switch(config)# router ospf network 192.168.6.0 24 0 | Configure subnet 192.168.6.0/24 to join OSPF network area 0 |
| Switch(config)# router ospf network 192.168.7.0 24 0 | Configure subnet 192.168.7.0/24 to join OSPF network area 0 |