

|  |
| --- |
| REPORT TITLE  2018 |
|  |
| August 8  COMPANY NAME  Authored by: Your Name |



# CCNA

Juniper devices:

Switching Devices:

EX series: EX2200, EX2200-C, EX3300, EX4200, EX4300, EX4500, EX4600, EX6200, EX8200

Support voice, video, data

8 QoS queues /switch ports

Virtual chassis technology

QFX series:

High performance switches

Designed for enterprise, SP & DCs

Virtual chassis technology

Combine switches into on to provide one high performance switch

Routing Devices:

MX Series VMX(virtual), MXS-20, MX-10/20/2020

Edge routers designed for service providers Enterprise network

PTX series PTX 1000/3000/5000

Package transport routers, core routers designed for high volume of traffic

ACX series ACX 1000/2000/4000/5000/5048/5096

Temperature harden devices, designed for mobile backhaul, service provider network

E series E120/320/ERX1410/ERX1440

Broad band service routers, ideal for internet based services IPTV, VOIP

T series T640/1600/4000

Multi chassis core routers high powerful. Contains TX matrix can connect up to 4 T640, TX Metrix plus 4xT4000 or 8xT1600

M series M7i/10i/m120/m320

Multiservice edge routers combined capabilities of IP and MPLS

Security devices

VSRX

SRX100,110

SRX210,220,240

SRX300,550,650

SRX1400,1500

SRX3400,3600

SRX5400,5600, 5800

SRX UTM (unified threat management)

|  |
| --- |
| **Configuring the Hostname and password in Cisco:** Cisco interface  (Executive mode) 🡪en(privilege executive mode) 🡪 conf t (global config mode) 🡪 hostname <name of device>  en 🡪 conf t 🡪 enable password <password that you want to keep>  you can see the password by show running-config (privilege executive mode) |
| To store password in encrypted format: en 🡪 conf t 🡪 service password-encryption  if you are in global config and want to get something in privilege executive mode  use :do <command>  to disable encryption  en 🡪 conf t 🡪 no service password-encryption  disables future password encrypted not current on  To set up the console port:  en 🡪 conf t 🡪 line console <number on which pc is connected to>  password <password that you want to keep>  login  end  you can use cdp to detect any problem  Hostname and password configuration in Juniper:  To show the configuration  Configure🡪show  Configure🡪Edit system  -Show | match host-name  -Set host-name <host name that you want to keep>  -Commit  Set system root-authentication plain-text-password  <Set password>  <Set password>  commit |
| **Cisco CDP**En🡪Show cdp neighbors Serial communication has 2 port dce-data communication equipment & dte- data terminal equipment dce provide clock signal  To find out type  En🡪 show controllers serial 0  To set clock rate of serial communication  en 🡪 conf t 🡪 int serial 0  clock rate <clock rate you want>  to configure the ip address  en 🡪 conf t 🡪 int serial 0  ip address <ip address> <subnet> **To Save configuration into Cisco device:** Copy running-config startup-config  Enter, Enter **To Save configuration into Juniper device:** To save the current configuration without the text configuration:  host1#copy running-configuration system2.cnf  To save the current configuration and add the text configuration to the file in compressed format:  host1#copy running-configuration system2.cnf include-text-config  Save all outstanding (unsaved) configuration changes to NVS.  host1#copy running-configuration startup-configuration |
| **Configure VLAN in Cisco Devices:** After configuration of IP address in the PC/ End devices  PC 1 and 3 in vlan 1  PC 2 and 4 in vlan 2  To select range of ports:  interface range Fa0/4 – 8  Inside switch:  en 🡪 conf t 🡪 int f0/2  switchport mode access  switchport access vlan 1 Int f0/3 switchport mode access  switchport access vlan 2  en 🡪 conf t 🡪 Int f0/1  Switchport mode trunk  Reflect on all the switches |
| Do reflect this changes in all the switches  Why we cant ping between pc 2 and pc 4🡪 due to native vlan1- the f0/1 of both switch are assigned to native vlan only traffic from vlan 1 can pass    Native vlan 🡪 vlan 1 is considered as native vlan all untagged vlan packets are assume to be a native vlan packet.  To enable vlan 2 we need to configure the port connecting switch with each other as trunk ports.  en 🡪 conf t 🡪 Int f0/1  Switchport mode trunk  Reflect on all the switches  There are different types of encapsulation present in the switching devices. Encapsulation: ISL cisco proprietary & dot1Q – Open standards.  The switches such as 3560 24 PS supports 2 types of encapsulations  Therefore, to configure the trunk mode in these switches differs.  You just need to configure trunk port in the following way instead of pervious to achive the result.  En🡪 conf t 🡪 int f0/1  Switchport trunk encapsulation dot1q  Switchport mode trunk **Configure VLAN in Juniper Devices:** edit  Show vlans  Edit vlans  Set vlan1 vlan-id 1  Set vlan2 vlan-id 2  Show  Top  Edit interfaces  Edit ge-0/0/2 unit 0 ethernet-switching  Set port-mode access  Set vlan member vlan1  Up 3  Edit ge-0/0/3 unit 0 ethernet-switching  Set port-mode access  Set vlan member vlan1  Up 3  Edit ge-0/0/1 unit 0 ethernet-switching  Set port-mode trunk  Set vlan member vlan1  Set vlan member vlan2  <set all the vlans that you want the switch to flow the packets>  show  Up 3  Top  Commit  Exit  Show vlans  For dot1q  Set interface ge-0/1/0 unit 0 family ethernet-switching port-mode trunk  Set interface ge-0/1/0 unit 0 family ethernet-switching vlan members 1 2  #Set vlans v100 vlan-id 100  #Set vlans v100 l3-interface vlan.100  #Set interface ge-0/1/0 unit 100 family inet address 20.0.0.2/24  If you are configuring the cisco and juniper then use following set of commands  Juniper  Set interface ge-0/1/0 unit 0 family ethernet-switching port-mode trunk  Set interface ge-0/1/0 unit 0 family ethernet-switching vlan members 1 2  Cisco  Int f0/1  Switchport trunk allowed vlan 1,2  Switchport mode trunk  Configure Cisco switch and router for inter-vlan routing:  Do all configuration same as intra vlan routing at router and the switch connecting router do this:  Router:  En🡪conf t🡪int g0/0  No shutdown  Int g0/0.<vlan id 1>  Encapsulation dot1q <vlan id 1>  Ip address <gateway ip address of vlan id 1>  Int g0/0.<vlan id 2>  Encapsulation dot1q <vlan id 2>  Ip address <gateway ip address of vlan id 2>  Connecting Switch:  En🡪conf t🡪Int g0/1  Switchport mode trunk  Connecting Switch:  En🡪conf t🡪Int g0/1  Switchport mode trunk  Troubleshooting of above problem:   1. Confirm the problem:   The 2 vlan pc could not be able to communicate in between  The R1 enables the communication between the two vlans  On switch  Show ip interface brief  Show run  Show interfaces trunk -NP  Check PC default gateway:  Ipconfig /all-- NP  On Router:  Show ip interface brief  Show interface g0/0.13 check vlan id = 13 – yes, NP  Show interface g0/0.24 check vlan id = 14 –No, P  Change vlan id to 24  Conf t🡪 int g0/0.24  Encapsulation dot1q 24  Test vlan pc with ping  Configure Juniper switch and router for inter-vlan routing:  Do all configuration same as intra vlan routing at router and the switch connecting router do this:  Router: VSRX  Set interfaces ge-0/0/1 vlan-tagging  Set interfaces ge-0/0/1 unit 10 vlan-id 10  Set interfaces ge-0/0/1 unit 10 family inet address 192.168.10.1/24  Set interfaces ge-0/0/1 unit 20 vlan-id 20  Set interfaces ge-0/0/1 unit 20 family inet address 192.168.20.1/24  Commit and-quit  Show configuration interfaces | display set  Switch side  Edit interface ge-0/1/0  Set interface ge-0/1/0 unit 0 family ethernet-switching port-mode trunk  Set interface ge-0/1/0 unit 0 family ethernet-switching vlan members 10 20  ### |
| How to set username and password to device with local device database  En🡪 conf t 🡪 username <name of user> password <password of user>  Line console 0  Login local  User name is note case sensitive  Password is case sensitive  To set console banner and login banner  Conf t 🡪banner motd ‘message you want to set’  Banner login ‘message you want to set’ |
| Configure basic DHCP: configure router to switch interface with ip address  And loopback address router is your dhcp server and DNS server  En🡪conf t 🡪 ip dhcp excluded-address <ip from> <ip to>  Ip dhcp pool <pool name>  Network <Network IP to use dhcp on> <subnetmask>  To know the neighbor details  Sh cdp neighbours details  Sh cdp entry <neighboring device name>  To know device details  Sh version |
| Default-router <default gateway IP>  Dns-server <dns ip address>  Do sh Ip dhcp binding 🡪 to see the ipadress associated with the mac |
| CDP displays the directly connected neighbors to the devices  Sh cdp neighbours  To change the clock rate of cdp use  En🡪 conf t 🡪 int <interface>  Clock rate <clock>  To see the cdp activation  Sh cdp int  To enable cdp  Cdp run  To disable  No cdp run  To configure in certain interfaces  Int range <startingint – Endingint >  Int range f0/1 - 10  No cdp run  Loop back interfaces:  Loopback interfaces are logical interfaces  Used for testing, never goes down  Loop back interfaces are on different networks  Int loopback <loopback no> |
| Port security:  Configured on switch interfaces and controls which mac address are allowed on which interfaces.  To see the mac address tables  Sh mac address-table  Port security is only configured on the access port not on the trunk port  The port security cant take the dynamic port you have to explicitly mention the post as access port  En🡪 conf t 🡪  switchport mode access  Interface range f0/2 - 3  switch port-security  switchport port-security mac-address <mac address>  or  switchport port-security mac sticky  switchport port-security violation shutdown  to see port security  do show port security  what if the port security violated 3 action it can take   1. Protect : drop packet for mac address that are not allowed on the port. No shut down of interface , doesn’t display any message don’t increase the violation count the swich keeps. 2. Restrict. Dorp packet, display message on switch and increase the violation count on the switch. 3. Shutdown. Put interface into shutdown error disabled state increase violation count   Default is shutdown  To set it use :  switchport port-security violation shutdown  to see the mac address of secure port  sh port-security address  Configure VTY line for Telenet and SSH:  VTY line Telenet: Virtual teletype  The devices are connected to Management PC via regular ethernet port. It use vty lines in network devices for connection.  On switch:  En🡪 conf t🡪 int vlan 1 🡪 ip address <management ip you want to put > <subnet>🡪 no shut  On router:  En🡪 conf t🡪 int <interface connecting device> 🡪 ip address <management ip you want to put > <subnet>🡪 no shut  On all devices:  Username <user> password <pass>  Line vty 0 15  Login local  Transport input telenet  Pc telenet <management ip of device >  Configure VTY line for SSH:  VTY line ssh: secure shell  The devices are connected to Management PC via regular ethernet port. It use vty lines in network devices for connection.  On switch:  En🡪 conf t🡪 int vlan 1 🡪 ip address <management ip you want to put > <subnet>🡪 no shut  On router:  En🡪 conf t🡪 int <interface connecting device> 🡪 ip address <management ip you want to put > <subnet>🡪 no shut  On all devices:  Username <user> password <pass>  Ip domain-name <domainname.com>  Crypto key generate rsa  1024 <select size of key>  Line vty 0 15  Login local  Transport input ssh  Exec-timeout <select inactivity time to logout>  Exit  Ip ssh version 2  Don’t forget to put the ip of the management pc in same subnet  Pc ssh -l <username> <management ip of device >  Routing:  Static routing:  Once Ips are configured  En🡪 conf t 🡪 ip route <ip of the network not connected directly to the router> <its subnet> <ip of opposite routers interface ip address/ or you can give exit interface >  To see the routing table  Sh ip route  C means connected network  L refers as local address of router  S for staic route  Configure same on opposite router  To set floating backup static route:  En🡪 conf t 🡪 ip route <ip of the network not connected directly to the router> <its subnet> <ip of opposite routers interface ip address/ or you can give exit interface > <AD 1 higher than the current dynamic routing AD>  Dynamic routing protocol:  RIP:  Router rip  Network <interfaces of network connecting other routers>  Network <router connecting lower networks>  ACL:  Standard ACL controls the traffic based on source address where as the extended ACL controls the traffic based on source and destination address.  Number or name and standard or extended.  1-99 for standard access list  Number standard access list:  ACL must be configured closed to the destination  Access-list <number> <action> <network> <network wildcard>  Access-list 1 permit 192.168.1.0 0.0.0.255  This mean only allow 192.168.1.0 traffic and deny all other  Everything doesn’t apply will be denied  After configuring the access list you need to apply it.  Applying ACL to interface:  Get into interface  Int g0/1  Ip access-group 1 out  Ip access-group <access-list number> <in/out>  To deny certain host:  Access-list 1 deny host 192.168.2.4  Access-list 1 permit any  Int g0/2  Ip access-group 1 out  The access list check hierarchical conditions if 1 one doesn’t satisfied then. It will go for next condition.  Extended ACL:  To allow certain host to access certain host:  Access-list <100-199> permit ip host <source host ip> host <destination host ip>  Access-list <100-199> deny ip any host <destination host ip>  R1(config)#access-list 100 permit ip host 192.168.1.3 host 192.168.3.3  R1(config)#access-list 100 deny ip any host 192.168.3.3  To allow certain network to access certain hosts:  Access-list <100-199> permit ip host <source network ip> <network wild card> host <destination host ip>  Access-list <100-199> deny ip any host <destination host ip>  R1(config)#access-list 100 permit ip 192.168.2.0 0.0.0.255 host 192.168.3.4  R1(config)#access-list 100 deny ip any host 192.168.3.4  Applying to the interface:  R1(config)#int gigabitEthernet 0/0  R1(config-if)#ip access-group 100 out  To configure named access lists:  Ip access list standard <name of accesslist>  Deny 192.168.2.0 0.0.0.255  Permit any  Exit  Interface <interface where you want to block traffic form ip>  Ip access-group <accesslist name> out  NTP: Cisco devices has hardware calender built in to look  Sh clock  Sh clock detail  Configuration of timing done in global config mode  Clock timezone <timezone shortform> <hrs offset> <min offset>  Come back in privilege mode and configure the clock  Clock set <hh mm ss> <Month date year>  Sh clock detail  To set is as NTP configure it as master to configure and syc with all devices for client configure it as server  Master device:  Ntp master <authoritative you want lower is more autority>  Client devices  Global config mode  Clock timezone <timezone shortform> <hrs offset> <min offset>  Ntp server <ip address of link where ntp master is set>  To check NTP  Sh ntp associates  sh ntp associations  for indirect devices:  Clock timezone <timezone shortform> <hrs offset> <min offset>  Ntp server <ip address of link where ntp intermediate device is set>  Setting up NTP with authentication: clock set 08:43:00 Apr 06 2020  Conf t  clock timezone MDT -4  ntp authenticate  ntp authentication-key 1 md5 cisco1  ntp authentication-key 2 md5 cisco2  R1(config)#ntp trusted-key 1  R1(config)#ntp trusted-key 2  Other devices:  Clock timezone EDT -4  Ntp authenticate  Ntp authentication-key 1 md5 cisco1  Ntp trusted-key 1  Ntp server 12.0.0.1 key 1  Sh ntp associations  LLDP (Link layer discovery protocol)  Conf t 🡪 no cdp run 🡪 lldp run (on all the devices)  Sh lldp  Sh lldp neighbors  sh lldp neighbors detail  to remove lldp  in the interface:  no lldp receive  no lldp transmit    Setting UP DHCP:# to do this you need to config router with their interface address and routing protocol:  En🡪conf t  ip dhcp pool <name of pool>  network <network address of pool> <subnet>  network 10.0.0.0 255.255.255.0  default-router <default router ip>  dns-server <DNS server ip>  ip dhcp excluded-address <ip of excluded address> <ip of excluded address>  other routers config in same router:  ip dhcp pool <name of pool>  network <network address of pool> <subnet>  network 20.0.0.0 255.255.255.0  default-router <default router ip>  dns-server <DNS server ip>  ip dhcp excluded-address <ip of excluded address> <ip of excluded address>  Link between the routers:  ip dhcp pool <name of pool>  network <network address of pool> <subnet>  network 192.168.12.0 255.255.255.0  int ge <interface to other router>  ip address <ip of connecting interface>  ip address 192.168.12.1 255.255.255.0  In other router on the connecting interface: # to get ip to connecting interface on other router  R2(config)#int gigabitEthernet 0/0  R2(config-if)#ip address dhcp  Interaface ge <interface connecting subnet where dhcp needs to be relayed>  Ip helper-address <ip of dhcp router interface connecting relay router>  Int ge 0/1  ip helper-address 192.168.12.1  DNS server:  Router\_1(config)#ip dhcp excluded-address 192.168.1.1  Router\_1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10  Router\_1(config)#ip dhc  Router\_1(config)#ip dhcp p  Router\_1(config)#ip dhcp pool  Router\_1(config)#ip dhcp pool pool  Router\_1(config)#ip dhcp pool pool1  Router\_1(config)#ip dhcp pool pool1  Router\_1(dhcp-config)#de  Router\_1(dhcp-config)#default-router 192.168.1.1  Router\_1(dhcp-config)#dh  Router\_1(dhcp-config)#dn  Router\_1(dhcp-config)#dns-server 20.0.0.100  Go in service in select DNS add the A record with name and ip address and you are good to go.  For other devices where ip is manually configured can see the default gateway and DNS  Ip default-gatway <default gateway of network >  Ip name-server <dns ip address>  STATIC NAT:  Interface <inside interface of inside network>  Ip nat inside  Interface <outside interface connecting internet>  Ip nat outside  Router-1(config)#ip nat inside source static 192.168.1.11 1.2.3.11  ip nat inside source static <inside host ip address translated ip address>  Router-1(config)#ip nat inside source static 192.168.1.12 1.2.3.12  ip nat inside source static <inside host ip address translated ip address>  show ip nat translation  show ip nat statistics  show ip route  Dynamic ACL:  Interface <inside interface of inside network>  Ip nat inside  Interface <outside interface connecting internet>  Ip nat outside  access-list 1 permit <inside network ip address > <widecard bit>  Router-1(config)#access-list 1 permit 192.168.1.0 0.0.0.255  ip nat pool <pool name > <starting ip of the range of global ip used in nat> <ending ip of the range of global ip used in nat> <netmask>  Router-1(config)#ip nat pool pool1 1.2.3.10 1.2.3.20 netmask 255.255.255.0  ip nat inside source list <access list number> pool <pool name>  Router-1(config)#ip nat inside source list 1 pool pool1  Sh ip nat translations  Clear ip nat translations  |||Static NAT 1 to 1 translation  Dynamic NAT Many to Many translations  PAT is Many to 1 traslation. Uses layer 4 port number|||  PAT:  Interface <inside interface of inside network>  Ip nat inside  Interface <outside interface connecting internet>  Ip nat outside  access-list 1 permit <inside network ip address > <widecard bit>  Router-1(config)#access-list 1 permit 192.168.1.0 0.0.0.255  ip nat inside source list 1 interface <outside interface of the device where the nat will be used> overload  ip nat inside source list 1 interface s0/3/0 overload  Syslog:  Indicate status of device including port down or problem.  Configure device to display the message real time on cli  Stored in ram or server.  There are 8 levels of severity 0 = emergency, 7 = debug  As you restart the link you will get:  %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to down  Router-1(config-if)#no shutdown  Router-1(config-if)#  %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up  %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up  Now these message on the cli show the level 5 which is informational  To get the logs with timestamps  service timestamps log datetime msec  syslog messages are not displayed default on vty lines.  To enable:  Router-1#terminal monitor  Syncronus login – syslog appeat in typing ios rewrite the command  Line con 0  Logging synchronous  Line vty 0 15  Logging synchronous  To store the logs in ram  To see the logging  Sh logging  To enable  Router-1(config)#logging buffered  To increase buffer size  Router-1(config)#logging buffered 8192  To get the log in server:  Logging <ip address of server>  Logging host <ip address of server>  Router-1(config)#logging host 192.168.1.4  See in services in syslog  Password recovery, configuration backup, IOS upgrade:  To recover the forgotten password from the device:  Restart device physically and press control + break  rommon 1 > confreg 0x2142  rommon 2 > reset  en  Router#copy startup-config running-config  Reset password  Enable secret <new pass>  Router(config)#config-register 0x2102  TFTP back up  Router-1#copy startup-config tftp  Address or name of remote host []? 192.168.1.3  Upgrading the IOS image:  To check version:  Sh version  Router-1#copy tftp flash  Address or name of remote host []? 192.168.1.3  Source filename []? c2900-universalk9-mz.SPA.155-3.M4a.bin  Destination filename [c2900-universalk9-mz.SPA.155-3.M4a.bin]?  33591768 bytes copied in 1.816 secs (1942178 bytes/sec)  Router-1#sh flash:  System flash directory:  File Length Name/status  3 33591768 c2900-universalk9-mz.SPA.151-4.M4.bin  4 33591768 c2900-universalk9-mz.SPA.155-3.M4a.bin  [67439355 bytes used, 188304645 available, 255744000 total]  249856K bytes of processor board System flash (Read/Write)  Router-1#delete flash:c2900-universalk9-mz.SPA.151-4.M4.bin  Delete filename [c2900-universalk9-mz.SPA.151-4.M4.bin]?  Delete flash:/c2900-universalk9-mz.SPA.151-4.M4.bin? [confirm]  Router-1#sh flash  IPv6 Configuration:  Router-0(config)#ipv6 unicast-routing  Router-0(config)#interface gigabitEthernet 0/0  Router-0(config-if)#ipv6 address 2001:db8:123:123::1/64  Router-0(config)#interface gigabitEthernet 0/1  Router-0(config-if)#ipv6 address 2001:db8:1:1::1/64  Router-0(config)#do sh ipv6 int br  There are address that are configured and other addresses are link local addresses automatically generated on ipv6 interfaces. These addresses are never routed used in local link. In fe80/10 range.  On other routers:  Configure the inner links connecting end devices. The router links will be configured using slack.  Router-1(config)#ipv6 unicast-routing  Router-1(config)#int gigabitEthernet 0/1  Router-1(config-if)#ipv6 add  Router-1(config-if)#ipv6 address 2001:db8:2:2:::1/64  % Incomplete command.  Router-1(config-if)#ipv6 address 2001:db8:2:2::1/64  Router-1(config-if)#no shut  Router-1(config-if)#no shutdown  Stateless address auto config  It gives ipv6 address to router connecting other routers  It uses ndp  It will take the prefix and uses its own mac to generate address.  Router-2(config)#interface gigabitEthernet 0/0  Router-2(config-if)#no sh  Router-2(config-if)#no shutdown  Router-2(config-if)#  %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up  %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up  Router-2(config-if)#  Router-2(config-if)#ipv6 add  Router-2(config-if)#ipv6 address au  Router-2(config-if)#ipv6 address autoconfig  Static router config:  Router-0(config)#ipv6 route 2001:DB8:3:3::1/64 2001:DB8:123:123:201:63FF:FE26:A001  Router-0(config)#ipv6 rout  Router-0(config)#ipv6 route 2001:DB8:2:2::1/64 2001:DB8:123:123:201:42FF:FE9E:4301  Router-1(config)#ipv6 route 2001:DB8:1:1::1/64 2001:DB8:123:123::1  Router-1(config)#  Router-1(config)#ipv6 route 2001:DB8:3:3::1/64 2001:DB8:123:123:201:63FF:FE26:A001  If any routing issue  Check the ip protocol  Sh ip protocols  If passive interface meaning the interface can listen to the advertisements but cant respond  Router rip  No passive-interface <interface that is passive>  Sh ip rip database  To check dhcp  Sh ip interface  Check for helper address  Ip helper-address <interface ip is coming from>  To check nat  Do sh ip nat translations  Do sh ip nat stat  Do sh run| inc ins  Do sh access-list  To check dns  In dhcp server  Do sh run  To check DTP:  do sh in g0/1 sw  Switch-1(config)#interface gigabitEthernet 0/1  On each interface disable DTP:  Switch-1(config-if)#switchport nonegotiate  Switch-1(config-if)#switchport mode trunk  Switch-1(config)#interface range f0/1 - 10  Switch-1(config-if-range)#switchport mode access  Switch-1(config-if-range)#switchport no  Switch-1(config-if-range)#switchport nonegotiate  Do in to all the switches….  VTP config:  On each interface disable DTP:  Switch-1(config-if)#switchport nonegotiate  Switch-1(config-if)#switchport mode trunk  VTP config:  Switch-2(config)#vtp mode transparent  Switch-2(config)#vtp domain cisco  Switch-2(config)#vtp version 2  Switch-2(config)#vlan 40  Switch-2(config-vlan)#name accounting  ON switch 1:  Switch-1(config)#vtp domain cisco  Switch-1(config)#vtp version 2  Switch-1(config)#vtp mode server  Switch-1(config)#vlan 10  Switch-1(config-vlan)#name HR  Switch-1(config)#vlan 20  Switch-1(config-vlan)#name sales  Switch-1(config)#vlan 30  Switch-1(config-vlan)#name engineering  On swich 3:  Switch-3(config)#int range fastEthernet 0/2-3  Switch-3(config-if-range)#switchport mode access  Switch-3(config-if-range)#switchport access vlan 30  Switch-3(config)#int fastEthernet 0/1  Switch-3(config-if)#switchport mode access  Switch-3(config-if)#switchport access vlan 10  Switch-3(config-if)#exit  Switch-3(config)#int fastEthernet 0/4  Switch-3(config-if)#switchport mode access  Switch-3(config-if)#switchport access vlan 20  Switch-3(config-if)#switchport nonegotiate  Switch-2(config)#int range f0/1 -2  Switch-2(config-if-range)#switchport mode access  Switch-2(config-if-range)#switchport access vlan 40  Switch-2(config-if-range)#switchport nonegotiate  Switch-2(config-if-range)#exit  Switch-1(config)#int range fa 0/1-2  Switch-1(config-if-range)#switchport mode access  Switch-1(config-if-range)#switchport access vlan 10  Switch-1(config-if-range)#switchport nonegotiate  Switch-1(config-if-range)#exit  Switch-1(config)#int fa 0/3  Switch-1(config-if)#switchport mode access  Switch-1(config-if)#switchport access vlan 20  Switch-1(config-if)#switchport nonegotiate  Switch-1(config-if)#exit  On the trunk port:  Switch-1(config)#int gigabitEthernet 0/2  Switch-1(config-if)#switchport trunk allowed vlan 1,10,20  TO verify:  Switch-1(config-if)#do sh int trunk  On switch 2:  Switch-2(config)#int range gigabitEthernet 0/1 - 2  Switch-2(config-if-range)#switchport trunk allowed vlan 1,10,20  On switch 3:  Switch-3(config)#int gigabitEthernet 0/1  Switch-3(config-if)#switchport trunk allowed vlan 1,10,20  Do sh vtp status  Do sh vlan br  Sh spanning-tree  Ether channel:  Layer 2 ether channel switch1 and switch 2:  PAGP  Switch1:  Requirements:  All ports must have same config duplex, speed native vlan and allowed vlan and same trunk and access ports  En🡪conft🡪  Channel-group 1 mode desirable  Do show eth sum  Int po1  Switchport mode trunk  Switch 2:  En🡪conft🡪  Channel-group 1 mode desirable  Do show eth sum  Int po1  Switchport trunk encapsulation dot1q  Switchport mode trunk  Layer 3 ether channel:  Ip routing  Int range g0/1-2  No switchport  channel-group 1 mode on  int po1  ip address 23.0.0.1 255.255.255.0  Switch 3  Ip routing  Int range g0/1-2  No switchport  channel-group 1 mode on  int po1  ip address 23.0.0.1 255.255.255.0  Now use LACP:  int range fastEthernet 0/1-4  channel-group 2 mode active  switchport trunk encapsulation dot1q  switchport mode trunk  Switch 4:  int range fastEthernet 0/1-4  channel-group 2 mode active  switchport trunk encapsulation dot1q  switchport mode trunk  Troubleshooting:  Sh eth sum  Sh int f0/4  To change speed  Int f0/4  Speed 100  Sh Ip int g0/2  Inter-VLAN routing:  Using SVI  To make switch as router  En🡪conf t 🡪Ip routing  Int g0/1  Switchport access vlan 10  Int g0/2  Switchport access vlan 20  Int vlan 10  Ip address 10.0.1.1 255.255.255.0  No shutdown  Int vlan 20  Ip address 10.0.2.1 255.255.255.0  No shutdown  Do sh vlan br  OSPF:  Single area OSPF  Router-1:  Router ospf <pid>  All the instance you will use single ospf instance on a router .  You can create sepeater pid which will create separate database.  The pid is locally significant they can be different in router and still they can be neighbors.  Router ospf 1  Advertise network  It will look for the interfaces within the range stated in the network command and advertises the network prefix on those interfaces. Doesn’t necessarily advertise the exact network in network command  Network <ip of network> <wild card mask> area <area no>  Even if you enter incorrect wild card the network takes correct subnet mask bits.  Router-1(config-router)#network 12.0.0.0 0.0.0.255 area 0  Router-1(config-router)#network 12.0.0.0 0.0.0.255 area 0  Router-1(config-router)#network 14.0.0.0 0.0.0.255 area 0  Router-1(config-router)#network 1.1.1.1 0.0.0.0 area 0  Router2:  Router ospf 2  To configure network into all interfaces  Network 0.0.0.0 255.255.255.255 area 0  Router-1(config)#router ospf 2  Router-1(config-router)#network 12.0.0.0 0.0.0.255 area 0  Router-1(config-router)#network 23.0.0.0 0.0.0.255 area 0  Router-1(config-router)#network 2.2.2.2 0.0.0.0 area 0  Router-3:  Router ospf 3  Network 0.0.0.0 255.255.255.255 area 0  Router-4:  Router ospf 4  Network 0.0.0.0 255.255.255.255 area 0  Don’t use this short cut to realtime router as it applies ospf to all the ports.  To check the neighbor relation  Do sh ip ospf neighbor  Do sh ip route  To disable the advertisement on loopback  Passive-interface l0  To calculate cost the the bandwith is devided by the reference bandwidth  The reference bandwidth by default is 100MBPS fast ethernet bandwidth is 100MBPS.  Therefore the metric is 1 for fast ethernet  The lowest possible metric is 1.  For Gigabit 1000 MBPS  100M/1000M= 0.1  Therefore GE and FA has same metric by default  10GE and 100GE is same  To change reference bandwidth  Auto-cost reference-bandwidth 10000  To raise the cost of certain route  Int g0/0  Ip ospf cost 10000  OSPF multi area:  Router0:  Router opsf 1  Network 0.0.0.0 255.255.255.255 area 1  Passive-interface l0  Auto-cost reference-bandwidth 10000  Router1:  Router opsf 1  Network 0.0.0.0 255.255.255.255 area 1  Passive-interface l0  Auto-cost reference-bandwidth 10000  Router2:  Router opsf 1  Network 0.0.0.0 255.255.255.255 area 1  Passive-interface l0  Auto-cost reference-bandwidth 10000  Router4:  Router opsf 1  Network 0.0.0.0 255.255.255.255 area 0  Passive-interface l0  Auto-cost reference-bandwidth 10000  Router7:  Router opsf 1  Network 0.0.0.0 255.255.255.255 area 2  Passive-interface l0  Auto-cost reference-bandwidth 10000  Router6:  Router opsf 1  Network 0.0.0.0 255.255.255.255 area 2  Passive-interface l0  Auto-cost reference-bandwidth 10000  Router8:  Router opsf 1  Network 0.0.0.0 255.255.255.255 area 2  Passive-interface l0  Auto-cost reference-bandwidth 10000  Router3:  Router opsf 1  Network 12.1.0.2 0.0.0.255 area 1  Network 12.2.1.1 0.0.0.255 area 0  Network 4.4.4.4 0.0.0.255 area 0  Passive-interface l0  Auto-cost reference-bandwidth 10000  Router(config-router)#area 0 range 12.0.0.0 255.0.0.0  Router5:  Router opsf 1  Network 12.2.2.2 0.0.0.255 area 0  Network 6.6.6.6 0.0.0.255 area 0  Network 12.3.0.1 0.0.0.255 area 2  Passive-interface l0  Auto-cost reference-bandwidth 10000  Router(config-router)#area 0 range 12.0.0.0 255.0.0.0  OSPF troubleshooting  Sh ip ospf neigh  Sh ip protocols  Router1:  Router ospf 1  Network 1.1.1.1 0.0.0.0 area 1  Passive interface l0  Router4:  Sh ip ospf neigh  Router ospf 1  No passive interface g0/0  Router 2:  Sh ip ospf neigh  Sh ip protocol  Sh ip interface br  Sh run  Conf t  Int f0/2  No shutdown  Router 3:  Sh ip ospf neigh  Sh ip protocol  Router ospf 1  Network 10.23.0.0 0.0.0.255 area 0  No area 2 range 10.0.0.0 255.0.0.0  Area 0 range 10.0.0.0 255.0.0.0  Do sh run  Router ospf 1  Area 0 range  Router5:  Sh ip ospf neigh  Sh ip route  IPV6 ospf mutiarea setup:  Internet:  Router(config-if)#ipv6 address 2001:DB8:1:1::1/64  Router(config-if)#no shut  Router 0:  Router(config)#ipv6 unicast-routing  Router(config)#ipv6 router ospf 1  Now ospf process is created  To activate on int g0/0 and g0/1  Router 0:  Router(config-rtr)#int g0/0  Router(config-if)#ipv6 ospf 1 area 1  Router(config-if)#int g0/1  Router(config-if)#ipv6 ospf 1 area 1  Router 2  Router(config-if)#ipv6 unicast-routing  Router(config)#interface gigabitEthernet 0/1  Router(config-if)#ipv6 ospf 1 area 1  Router 1:  Router(config)#ipv6 unicast-routing  Router(config)#interface gigabitEthernet 0/1  Router(config)#interface gigabitEthernet 0/1  Router(config-if)#ipv6 ospf 1 area 0  Router(config-if)#interface gigabitEthernet 0/0  Router(config-if)#ipv6 ospf 1 area 1  Router 3:  Router(config)#ipv6 unicast-routing  Router(config)#interface gigabitEthernet 0/1  Router(config-if)#ipv6 ospf 1 area 0  Router(config-if)#interface gigabitEthernet 0/0  Router(config-if)#ipv6 ospf 1 area 2  Router 4:  Router(config)#ipv6 unicast-routing  Router(config-if)#interface gigabitEthernet 0/0  Router(config-if)#ipv6 ospf 1 area 2  Sh ipv6 protocol  Sh ipv6 ospf  Sh ipv6 ospf neigh  The Router 0 is connected to internet in order to make it as default route and advertise.  Ipv6 routes # ip address of opposite side router internet.  Router(config)#ipv6 route ::/0 2001:DB8:01:01::1  Router(config)#ipv6 router ospf 1  Router(config-rtr)#default-information originate  Sh ipv6 routes  EIGRP: Enhanced version of IGRP. Form cisco proprietary now moved to open standard  However in multi vendor environment mostly ospf is used.  Router eigrp <Autonomous system number>  Router eigrp 100  The eigrp number has to be same for the all router  If AS number is not same the router will ne become neighbor with other router  Troubleshooting look for AS number  Network <ip address> <wild card mask>  Router 0  Router(config)#router eigrp 100  Router(config-router)#networ  Router(config-router)#network 10.12.0.0 0.0.0.255  Router(config-router)#network 10.23.0.0 0.0.0.255  Router(config-router)#network 1.1.1.1 0.0.0.  Router 1  Router eigrp 100  Router(config-router)#network 10.12.0.0 0.0.0.255  Router(config-router)#network 10.14.0.0 0.0.0.255  Router(config-router)#network 2.2.2.2 0.0.0.0  Router(config-router)#passive-interface l0  Router(config-router)#no auto-summary  Router 2  Router(config)#router eigrp 100  Router(config-router)#network 10.23.0.0 0.0.0.255  Router(config-router)#network 10.34.0.0 0.0.0.255  Router(config-router)#network 10.35.0.0 0.0.0.255  Router(config-router)#network 3.3.3.3  Router 3  Router(config)#router eigrp 100  Router(config-router)#network 10.14.0.0 0.0.0.255  Router(config-router)#network 10.34.0.0 0.0.0.255  Router(config-router)#network 4.4.4.4 0.0.0.0  Router(config-router)#passive-interface l0  Router(config-router)#no auto-summary  Router 4  Router(config)#router eigrp 100  Router(config-router)#network 10.35.0.0 0.0.0.255  Router(config-router)#network 5.5.5.5 0.0.0.0  Router(config-router)#passive-interface l0  Router(config-router)#no auto-summary  Sh ip route  OSPF can do same cost load balancing  Where as eigrp can do unequal cost load balancing  To enable router to load balance between links  If enter 2 the load balance happen upto double the fisable distance  With out fisable successor eigrp can do load balancing  Router(config-router)#variance 2  Router(config-router)#  %DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.12.0.1 (GigabitEthernet0/1) is up: new adjacency  %DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.14.0.1 (GigabitEthernet0/0) is up: new adjacency  Manual summary:  To configure summary route  Interface G0/0  Router(config-if)#ip summary-address eigrp 100 10.0.0.0 255.0.0.0  Eigrp troubleshooting:  Sh ip eigrp neighbours  Process no is 10  This process no is AS  It should use AS no 100  Sh run  Reconfigure eigrp with AS no 100  Sh ip protocols  Sh ip int br  Reconfigure loopback interface  Remove passive interface of physical link  Remove 10 network  Eigrp network command is default to /8 network  Sh run  Other interface for sum  Reconfigure the summary route  IPV6 EIGRP:  Router 1:  Router(config)#ipv6 unicast-routing  Router(config)#ipv6 router eigrp 100  Router(config-rtr)#passive-interface g0/2  Router(config-rtr)#int g0/0  Router(config-if)#ipv6 eigrp 100  Router(config-if)#int g0/1  Router(config-if)#ipv6 eigrp 100  Router(config-if)#int g0/2  Router(config-if)#ipv6 eigrp 100  Router(config-if)#ipv6 router eigrp 100  Router(config-rtr)#no shutdown  Router 2:  Router(config)#ipv6 unicast-routing  Router(config)#interface g0/0  Router(config-if)#ipv6 eigrp 100  Router(config-if)#interface g0/1  Router(config-if)#ipv6 eigrp 100  Router(config-if)#ipv6 router eigrp 100  Router(config-rtr)#no shutdown  Router 3:  Router(config)#ipv6 unicast-routing  Router(config)#interface gigabitEthernet 0/0  Router(config-if)#ipv6 eigrp 100  Router(config-if)#interface gigabitEthernet 0/1  Router(config-if)#ipv6 eigrp 100  Router(config-rtr)#no shutdown  Router 4:  Router(config)#ipv6 unicast-routing  Router(config)#interface gigabitEthernet 0/0  Router(config-if)#ipv6 eigrp 100  Router(config-if)#interface gigabitEthernet 0/1  Router(config-if)#ipv6 eigrp 100  Router(config-rtr)#no shutdown  Router 5:  Router(config)#ipv6 unicast-routing  Router(config)#interface gigabitEthernet 0/0  Router(config-if)#ipv6 eigrp 100  Router(config-if)#interface gigabitEthernet 0/1  Router(config-if)#ipv6 eigrp 100  Router(config-rtr)#no shutdown  TO set default routes:  Int g0/0  Ipv6 summary-address eigrp 100 ::/0  Int g0/1  Ipv6 summary-address eigrp 100 ::/0  PPP: Point to point protocol  Layer 2 protocol used over serial WAN  On cisco router the default layer 2 encapsulation is cisco hdlc  PPP provides secure security through autnetication functionality.  PPP with 2 different authentication  Hdlc static password for authentication  Chap chllenge handshake authentication protocol  Setting up VPC:    Nexus 9000 switches  Configuration is a four step process   1. Enable features 2. Keep-Alive link 3. vPC Domain 4. Peer-Link 5. Member ports 6. Orphan ports   Switch\_1# conf t 🡪 feature vpc 🡪 feature lacp 🡪 interface mgmt 0  Ip address <ip address of management interface/vlan subnet>  Ip address 10.244.102.1/30  No shut  Ping 10.244.102.2/30 vrf management  Exit  Vpc domain 10  Role priority 10  Peer-keepalive destination 10.244.102.2 source 10.244.102.1 vrf management  Show vpc brief  Interface eth 1/53-54  Description \*\*vPC Peer-Link\*\*  Channel-group 15 mode active  No shut  Int port-channel 15  Description \*\*vPC Peer-Link\*\*  No shut  Switchport  Switchport mode trunk  Int eth 1/20  Channel-group 20 mode active  No shut  Interface port-channel 20  Switchport  Vpc 20  Sh vpc brief  Interface eth 1/11  No shut  Switch  Show vpc orphan-ports  Switch\_2# conf t 🡪 feature vpc 🡪 feature lacp 🡪 interface mgmt 0  Ip address <ip address of management interface/vlan subnet>  Ip address 10.244.102.2/30  No shut  Ping 10.244.102.1/30 vrf management  Exit  Vpc domain 10  Role priority 20  Peer-keepalive destination 10.244.102.1 source 10.244.102.2 vrf management  Interface eth 1/53-54  Description \*\*vPC Peer-Link\*\*  Channel-group 15 mode active  No shut  Int port-channel 15  Description \*\*vPC Peer-Link\*\*  No shut  Switchport  Switchport mode trunk  Sh vpc brief  Routing over VPC  s  Setting up Basic BGP internal and external:  En🡪 conf t🡪 no ip domain-lookup  Hostname <router name >  Alias exec s show ip int br  Line con 0  No exec-timeout  Logging synchronous  Int <interface on which you want to configure your bgp>  Ip address <ip address you want to provide for the interface> <subnet mask>  No shutdown  Configure it ip address on both side such that you can ping using both the routers  En🡪 conf t🡪  Router bgp <own AS number of router>  Neighbor <ip address of other routers interface> remote-as <for i bgp own AS no for ebgp other routers AS>  Same config on other router |
|  |
| Follow above procedure on all the routers  Now the OSPF is configured & you can able to ping the neighboring routes  Configuring MPLS: This config assign mpls label to packet dynamically to ip address.  En🡪 conf t  Mpls ip  Mpls label range 100 150  Interface g<interface>  Mpls ip  For static binding:  En🡪 conf t🡪  Mpls label range <> static <range of label for static label assignment>  Mpls static binding ipv4 <ip address > <subnet> <label to bind from static range>  Debug :  Show mpls label range  Show mpls static binding ipv4  Show mpls forwarding table  Sh mpls static crossconnect  At PE configure static at P configure dynamic |

PPP layer 2 protocol often used over serial WAN. On CISCO router the default layer 2 encapsulation is CISCO HDLC. However, PPP provides secure security through authentication functionality. PAP static password to authenticate the connection. CHAP challenge handshake authentication protocol. Which uses the dynamic randomly generated string. Provide greater security than PAP

R1 – R1se PAP

R1(config)#username Packet password Tracer

R1(config)#username cisco password ccna

R1#sh int S2/0

R1(config-if)#ppp authentication pap

R1(config-if)#ppp pap sent-username cisco password ccna

R1se:

R1SE(config)#username cisco password ccna

R1SE(config)#int serial 2/0

R1SE(config-if)#encapsulation ppp

R1SE(config-if)#ppp authentication pap

R1SE(config-if)#ppp pap sent-username cisco password ccna

R1SE(config-if)#do sh ip int br

R2 – R2se CHAP

Username of other router.

R2(config)#username R2SE password CCNA

R2(config)#int serial 2/0

R2(config-if)#encapsulation ppp

R2(config-if)#ppp authentication chap

R2(config-if)#no shutdown

R2SE:

Router(config)#hostname R2SE pass

R2SE(config)#username R2 password CCNA

R2SE(config)#int serial 2/0

R2SE(config-if)#encapsulation ppp

R2SE(config-if)#ppp authentication chap

R2SE(config-if)#no shut

Sh int s0/0

Sh run

Password not set

Ppp pap sent-username cisco password CCNA

Authentication check

Do sh ip int br

Check hostname in chap as we use username of other router

Multilink PPP:

PAP on R1 to spr1

Chap on R2 to SPR 2

Conf t

Username Packet passward Tracer

Interface multilink 1

Ppp multilink

Ppp multilink group 1

Ppp authentication pap

Ppp pap sent-username cisco password CCNA

Ip address 100.0.0.2 255.255.255.254

Do sh run int multi 1

Int s1/0

Encapsulation ppp

Ppp multilink group 1

No shut

Int s1/1

Encapsulation ppp

Ppp multilink group 1

Show ppp all

Show ppp multilink

Ip route 0.0.0.0 0.0.0.0 100.0.0.1

Do sh ip route

R2:

Conf t

Username SPR2 password CCNA

Interface multilink 1

Ppp multilink

Ppp multilink group 1

Ppp authentication chap

Ip address 200.0.0.2 255.255.255.254

Do sh run int multi 1

Int s1/0

Encapsulation ppp

Ppp multilink group 1

No shut

Int s1/1

Encapsulation ppp

Ppp multilink group 1

Show ppp all

Show ppp multilink

Configure static default routes no router

Ip route 0.0.0.0 0.0.0.0 200.0.0.1

Do s hip route

PPPOE:

PPP authentication over ethernet frames.

Conf t

Username packet password Tracer

Interface dialer 1

Mtu 1492

Encapsulation ppp

Ip address negotiated

Ppp authentication pap

Ppp pap sent-username Cisco password CCNA

Dialer pool 1

Do sh run int dialer 1

Int g0/0

Pppoe client dail-pool-number 1

No shut

Sh ip int br

Dialer provides layer 3 information and virtual access provides layer 2 info

Ip route 0.0.0.0 0.0.0.0 100.0.0.1

Conf t

Username SPR2 password CCNA

Interface dialer 1

Mtu 1492

Encapsulation ppp

Ip address negotiated

Ppp authentication chap

Dialer pool 1

Do sh run int dialer 1

Int g0/0

Pppoe client dail-pool-number 1

No shut

Sh ip int br

Dialer provides layer 3 information and virtual access provides layer 2 info

Sh int dailer 1

Ip route 0.0.0.0 0.0.0.0 200.0.0.1

GRE tunnel:

R1(config)#int t0

R1(config-if)#ip add 192.168.1.1 255.255.255.252

R1(config-if)#tunnel source serial 0

R1(config-if)#tunnel destination 200.0.0.2

R1(config-if)#exit

R1(config)#ip route 0.0.0.0 0.0.0.0 100.0.0.1

Router(config)#hostname R2

R2(config-if)#ip address 192.168.1.2 255.255.255.252

R2(config-if)#tunnel source serial 0

R2(config-if)#tunnel destination 100.0.0.2

R2(config-if)#exit

R2(config)#ip route 0.0.0.0 0.0.0.0 200.0.0.1

R1#sh int tunnel 0

R1(config)#router eigrp 100

R1(config-router)#network 10.0.1.0 0.0.0.255

R1(config-router)#network 192.168.1.0 0.0.0.3

R2(config)#router eigrp 100

R2(config-router)#netwok

R2(config-router)#netwo

R2(config-router)#network 10.0.2.0 0.0.0.255

R2(config-router)#network 192.168.1.0 0.0.0.3

R2(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 192.168.1.1 (Tunnel0) is up: new adjacency

R2(config-router)#do sh ip route

GRE troubleshooting

Sh ip int br

Temp disable recursive routing

Sh int tunnel 0

Check source and destn address

Sh ip protocols

Change the ip to tunnel ip in protocol

Tunnel source is inside interface

Check the underlaying static route

BGP configuration :

IGP OSPF configuration:

Router0:

router ospf 1

log-adjacency-changes

network 0.0.0.0 255.255.255.255 area 0

Router 1:

router ospf 1

log-adjacency-changes

network 0.0.0.0 255.255.255.255 area 0

Router 2:

router ospf 1

log-adjacency-changes

passive-interface GigabitEthernet0/0

network 0.0.0.0 255.255.255.255 area 0

default-information originate

EGP:

router bgp 65000

bgp log-neighbor-changes

no synchronization

neighbor 100.0.0.1 remote-as 65001

network 1.1.1.1 mask 255.255.255.255

network 2.2.2.2 mask 255.255.255.255

network 3.3.3.3 mask 255.255.255.255

network 10.0.0.0 mask 255.255.0.0

network 100.0.0.0 mask 255.255.255.252

redistribute ospf 1 match external 1 external 2

ip route 0.0.0.0 0.0.0.0 100.0.0.1

ip route 10.0.0.0 255.255.0.0 Null0

Router 3:

router bgp 65001

bgp log-neighbor-changes

no synchronization

neighbor 100.0.0.2 remote-as 65000

neighbor 111.0.0.1 remote-as 65002

network 4.4.4.4 mask 255.255.255.255

network 111.0.0.0 mask 255.255.255.0

network 1.1.1.1 mask 255.255.255.255

network 2.2.2.2 mask 255.255.255.255

network 3.3.3.3 mask 255.255.255.255

network 100.0.0.0 mask 255.255.255.252

network 10.0.0.0 mask 255.255.0.0

network 112.0.0.0 mask 255.255.255.0

network 200.0.0.1 mask 255.255.255.255

Router 5:

router bgp 65002

bgp log-neighbor-changes

no synchronization

neighbor 111.0.0.2 remote-as 65001

neighbor 112.0.0.2 remote-as 65003

network 200.0.0.1 mask 255.255.255.255

network 100.0.0.0 mask 255.255.255.252

network 1.1.1.1 mask 255.255.255.255

network 2.2.2.2 mask 255.255.255.255

network 3.3.3.3 mask 255.255.255.255

network 10.0.0.0 mask 255.255.0.0

network 111.0.0.0 mask 255.255.255.0

network 112.0.0.0 mask 255.255.255.0

Internet:

router bgp 65003

bgp log-neighbor-changes

no synchronization

neighbor 112.0.0.1 remote-as 65002

network 130.0.2.0 mask 255.255.255.0

network 220.0.0.0

network 15.0.0.0

network 67.56.22.0 mask 255.255.255.0

network 112.0.0.0 mask 255.255.255.0

BGP troubleshooting:

Sh ip bgp summary

Sh ip bgp neighbor

Sh ip route

Sh ip bgp

HRSP:

Internet:

interface GigabitEthernet0/0/0

ip address 17.0.0.1 255.255.255.0

no shut

interface GigabitEthernet0/1/0

ip address 18.0.0.1 255.255.255.0

no shut

router bgp 65001

bgp log-neighbor-changes

no synchronization

neighbor 17.0.0.2 remote-as 65000

neighbor 18.0.0.2 remote-as 65000

network 15.0.0.0 mask 255.255.255.0

Router1:

interface GigabitEthernet0/0

ip address 12.0.0.1 255.255.255.252

interface GigabitEthernet0/1

ip address 10.10.10.2 255.255.255.0

interface GigabitEthernet0/2

ip address 10.20.20.3 255.255.255.0

interface GigabitEthernet0/0/0

ip address 17.0.0.2 255.255.255.0

router ospf 1

log-adjacency-changes

passive-interface GigabitEthernet0/0/0

network 0.0.0.0 255.255.255.255 area 0

router bgp 65000

bgp log-neighbor-changes

no synchronization

neighbor 17.0.0.1 remote-as 65001

network 17.0.0.0 mask 255.255.255.0

network 12.0.0.0 mask 255.255.255.252

network 10.10.10.0 mask 255.255.255.0

network 10.20.20.0 mask 255.255.255.0

ip route 0.0.0.0 0.0.0.0 17.0.0.1

standby version 2

standby 10 ip 10.10.10.1

standby 10 priority 110

standby 10 preempt

Router 2:

interface GigabitEthernet0/0

ip address 12.0.0.2 255.255.255.252

interface GigabitEthernet0/1

ip address 10.20.20.2 255.255.255.0

interface GigabitEthernet0/2

ip address 10.10.10.3 255.255.255.0

standby version 2

standby 10 ip 10.10.10.1

interface GigabitEthernet0/0/0

ip address 18.0.0.2 255.255.255.0

router ospf 1

log-adjacency-changes

passive-interface GigabitEthernet0/0/0

network 0.0.0.0 255.255.255.255 area 0

router bgp 65000

bgp log-neighbor-changes

no synchronization

neighbor 18.0.0.1 remote-as 65001

network 18.0.0.0 mask 255.255.255.0

network 12.0.0.0 mask 255.255.255.252

network 10.10.10.0 mask 255.255.255.0

network 10.20.20.0 mask 255.255.255.0

ip route 0.0.0.0 0.0.0.0 18.0.0.1

standby version 2

standby 10 ip 10.10.10.1

Switch 1:

interface FastEthernet0/1

switchport access vlan 10

switchport mode access

interface FastEthernet0/2

switchport access vlan 10

switchport mode access

Switch 2:

interface FastEthernet0/1

switchport access vlan 20

switchport mode access

interface FastEthernet0/2

switchport access vlan 20

switchport mode access

HRSP troubleshooting:

Duplicate address:

Sh standby <interface>

Sh standby g0/1

Check the standby version

Traceroute

Check preempt

ACL IPv4 and IPv6:

Deny host PC4 to access 10.4.4.100 server

R2(config)#access-list 1 deny host 10.2.2.12

R2(config)#access-list 1 permit any

R2(config-if)#ip access-group 1 out

Deny host PC5 to access 2001:DB8:22:22::/64

IPv6 only support named ACLs.

R1(config)#ipv6 access-list G0/2\_IN

R1(config-ipv6-acl)#deny ipv6 host 2001:DB8:3:3::11 2001:DB8:22:22::/64

R1(config-ipv6-acl)#permit ipv6 any any

R1(config-ipv6-acl)#int g0/2

R1(config-if)#ipv6 traffic-filter G0/2\_IN in

Deny PC3 communication with PC1:

R1(config)#ip access-list extended G0/1\_IN

R1(config-ext-nacl)#deny ip host 10.2.2.11 host 10.1.1.11

R1(config-ext-nacl)#permit ip any any

R1(config-ext-nacl)#int g0/1

R1(config-if)#ip access-group G0/1\_IN in

PC6 to telnet to R2:

R2(config)#ipv6 access-list TELNET

R2(config-ipv6-acl)#permit tcp host 2001:db8:3:3::12 any eq telnet

R2(config-ipv6-acl)#line vty 0 15

R2(config-line)#ipv6 access-class TELNET in

Troubleshooting:

Sh access-list <ACL no>

Check order of the statements

Sh ipv6 int g0/2

Sh run

SPAN:

Switch port analyzer:

Copies traffic from interface and send to another interface leads to monitoring server to analyze.

Switch 1 monitor G0/1 traffic

SW1(config)#monitor session 1 source interface g0/1 both

SW1(config)#monitor session 1 destination interface g0/2

IP SLA:

Service level agreement:

Ip sla 1

Icmp-echo 12.0.0.2

Icmp-echo <other side router>

Frequency 5

Exit

Ip-sla schedule 1 start-time now life forever

Ip-sla schedule 1 start-time <time> life <life time you want to send the ping>

Sh ip sla configuration

Sh ip sla statistics