Key Definitions:

- **Split Horizon –** *The split horizon feature prevents a route learned on one interface from being advertised back out of that same interface.*
- **Poison Reverse –** *The Poison Reverse feature causes a route received on one interface to be advertised back out of that same interface with a metric considered to be infinite.*
- **Non-Broadcast Multiaccess (NBMA) –** *A network medium that doesn't use broadcasts, or subsequently multicasts, for identifying neighbors or performing other group communication/negotiation tasks. ATM and Frame Relay are examples of NBMA networks.*
- **Asymmetric Routing –** *A routing situation that causes traffic for an endpoint to be sent out through a certain route, but received to that endpoint on a different route.*
- **Maximum Segment Size (MSS) –** *The amount of data that can be contained in a single TCP segment; dependent on the current TCP window size.*
- **IPsec –** A security technology that offers the features of confidentiality, integrity, authentication, and anti-replay.
- **Internet Key Exchange (IKE) –** IPSec's primary negotiation means, IKE consists of Phase 1 (ISAKMP session, parameters exchanged, common session key used) and Phase 2 (encryption established, individual session keys used).

GRE Tunnel Commands

- **GRE Tunnel Setup Steps:**
  - interface tunnel 1 *(global config command that creates virtual tunnel interface 1)*
  - ip address 10.250.24.1 255.255.255.252 *(interface config command that assigns the 10.250.24.1/30 IP address to our tunnel)*
  - tunnel source Serial0/0 *(tunnel interface command that sets the tunnel's interface to be Serial0/0 – can also be used with an IP address)*
  - tunnel destination 10.250.24.2 *(tunnel interface command that specifies the destination IP address the tunnel should connect to)*

Misc 'Show' Commands:

- show ip nhrp *(exec command that displays current NHRP-discovered peers and status)*
- show crypto ipsec sa *(exec command that shows all established IPsec tunnels and their connection parameters)*

IPv6 Address Assignment Table for Global Unicast

Method	**Dynamic or Static**	**Prefix and Length Learned From**	**Host Learned From**	**Default Router Learned From**	**DNS Addresses Learned From**
Stateful DHCP	Dynamic	DHCP Server	DHCP Server	Router, using NDP	(Stateful) DHCP Server
Stateless Autoconfig	Dynamic	Router, using NDP	Derived from MAC	Router, using NDP	Stateless DHCP
Static Configuration	Static	Local config	Local config	Router, using NDP	Stateless DHCP
Static Config with EUI-64	Static	Local config	Derived from MAC	Router, using NDP	Stateless DHCP

IPv6 Client Address Prefixes:

- **2 or 3 –** Global unicast, unicast packets sent throughout the entire internet.
- **FD –** Unique local, unicast packets inside an organization.
- **FE8 –** Link-local, addresses used for packets sent in the local subnet.

Common IPv6 Multicast Addresses:

- **FF02::1 –** All IPv6 nodes on this link
- **FF02::2 –** All IPv6 routers on this link
- **FF02::5, FF02::6 –** OSPF messages
- **FF02::9 –** RIP messages
- **FF02::A –** EIGRP messages
- **FF02::1:2 –** DHCP relay agents
- **FF05::1:3 –** DHCP servers (site scope)
- **FF05::101 –** All NTP servers (site scope)

A solicited node multicast address (what Neighbor Discovery Protocol uses as a substitute for IPv4's ARP) is formed by taking FF02::1:FF00:0/104, then adding the final 24 bits of the host's self-assigned (link-local) IPv6 address to it.

IPv6 Addressing Commands:

- ipv6 unicast-routing *(global config command that enables the routing of IPv6 unicast traffic)*
- ipv6 cef *(global config command that enables Cisco Express Forwarding, or CEF, for IPv6)*
- ipv6 flowset *(global config command that configures flow-label marking in 1280-byte or larger packets sent from the router)*
- ipv6 address 2001::8452/64 *(interface command to statically configure the IPv6 address as 2001:8452/64)*
- ipv6 address 2001:4361::/64 eui64 *(interface command to configure that EUI-64 address on prefix 2001:4361::)*
- ipv6 address autoconfig *(interface command to tell the router to assign an IP address via stateless autoconfiguration)*
- ipv6 address dhcp *(interface command to tell the router to use stateful DHCP to find an address)*
- ipv6 unnumbered Serial0/0 *(interface command to have this interface use the same IPv6 unicast address as the Serial0/0 interface)*
- ipv6 enable *(interface command to enable IPv6, but results in only a link-local address)*
- ipv6 address FE80:4001::1 link-local *(interface command that overrides the auto link-local address with FE80:4001::1)*
- ipv6 address 2001:4361::1/64 anycast *(interface command that specifies the 2001:4361::1 address as an anycast address)*
- show ipv6 interface Serial0/0 *(exec command that shows the IPv6 parameters for the Serial0/0 interface)*
- show ipv6 neighbors *(exec command that displays all IPv6 neighbors, or in short, the IPv6 neighbor discovery table)*
- show ipv6 router *(exec command that shows the default router discovered through either RA/RS or a variant of IPv6 autoconfig)*

RIPng Commands:

- **Enabling RIPng Steps:**
  - ipv6 unicast-routing *(global config command that enables IPv6 unicast routing)*
  - ipv6 router rip RIP_Name *(global config command that enables RIPng under the process name 'RIP_NAME', which must be unique per router)*
  - Enable IPv6 on an interface by either configuring an IPv6 address manually, or using the 'ipv6 enable' command mentioned prior.
  - ipv6 rip RIP_Name enable *(interface command that enables RIP on an interface with the 'RIP_Name' process)*
- **RIPng Show Commands:**

  - show ipv6 route rip *(shows all RIPng-learned routes in the routing table)*
  - show ipv6 rip *(shows RIPng timers as well as other information)*
  - show ipv6 rip next-hops *(shows a list of RIPng routing information sources*
  - show ipv6 protocols *(displays, among other things, the interfaces upon which RIPng is enabled)*

EIGRP Commands:

- show ip eigrp interfaces *(lists the working interfaces on which EIGRP is enabled)*
- show ip protocols *(shows the contents of the network configuration commands for each routing process, a list of neighbor IP addresses, and any passive interfaces for routing processes)*
- show ip eigrp neighbors *(lists known neighbors, but does not list neighbors for which some mismatches parameter is preventing a bond from forming)*
- show ip eigrp topology *(lists all successor and feasible successor routes, but does not list all topology details)*
- ip hello-interval eigrp 10 5 *(interface command that manually sets the hello interval on EIGRP ASN '10' to 5 seconds for the interface's connections)*
- ip hold-time eigrp 10 15 *(interface command that manually sets the hold interval on EIGRP ASN '10' to 15 seconds for the interface's connections)*
- show ip eigrp interfaces detail Serial0/0 *(among a plethora of other things, lists the hello and hold timers for the Serial0/0 interface)*
- passive-interface Serial0/0 *(EIGRP configuration command that specifies the Serial0/0 interface as passive)*
- neighbor 10.10.10.1 Serial0/0 *(EIGRP configuration command that manually states '10.10.10.1' as an EIGRP neighbor on interface Serial0/0)*
- metric weights 0 1 0 1 1 0 *(EIGRP configuration command in which the first number sets the ToS for EIGRP, which must always be '0', with the subsequent five numbers being the K-value references)*
- eigrp router-id 192.168.255.1 *(EIGRP configuration command that statically sets the EIGRP router ID to '192.168.255.1')*
- show ip eigrp topology 10.0.0.0/24 *(shows only the part of the EIGRP topology table that has 10.0.0.0/24)*
- ip split-horizon eigrp 10 *(interface command that re-enabled split horizon for EIGRP ASN '10')*
- ip bandwidth-percent eigrp 10 75 Serial0/0 *(global command that statically sets the percentage of bandwidth that EIGRP traffic will consume on the Serial 0/0 interface to 75% of its total bandwidth capacity)*
- delay 20000 *(interface command that sets the reference delay for EIGRP on this interface to 20,000 tens of microseconds)*
- offset-list 10 in 5 Serial0/0 *(EIGRP configuration command that tells the Serial0/0 interface to check incoming EIGRP learned networks against ACL '10', and if they match inbound, add '5' to both the calculated cost as well as the metric)*
- maximum-paths 6 *(EIGRP configuration command that sets the maximum number of feasible routes to load balance over to '6')*
- variance 2 *(EIGRP configuration command that sets the variance multiplier for unequal cost load balancing to '2')*
- show ip eigrp topology all-links *(lists all possible EIGRP routes, including those that are neither successors or feasible successors)*
- timers active-time 5 *(EIGRP configuration command that statically sets the time that a routing update can be stuck in an 'Active' state to 10 minutes)*
- distribute-list 5 out Serial0/0 *(EIGRP configuration command that filters routing updates outbound on Serial0/0 based on access list '5')*
- distribute-list 5 out *(similar to the previous command, but applied globally, not for a single interface)*
- ip prefix-list ROUTE_OUT permit 10.0.0.0/8 ge 16 le 28 *(global configuration command that creates IP prefix list 'ROUTE_OUT', that permits routes within 10.0.0.0/8 as long as they have a subnet mask between /16 and /28)*
- distribute-list prefix ROUTE_OUT *(similar to the aforementioned distribute-list commands, but applies the 'ROUTE_OUT' prefix list as created prior)*
- ip summary-address eigrp 10 10.0.0.0 255.255.0.0 *(global configuration command that creates an EIGRP summary route of 10.0.0.0/16 for ASN '10')*

The ‘network’ command for EIGRP overrides an interface configured with the ‘passive interface’ command, even though the Cisco IOS will let you have both commands in place at the same time.

An EIGRP stub router is a router that should not forward traffic between two remote EIGRP-learned subnets. They’re specifically designed to be used on the “spoke” side of hub and spoke networks.

EIGRP Message Types:

- Hello
- Update (Contains the topology information, prefixes, lengths, metric components, and nonmetric items such as MTU and hop count.)
- Query
- Reply
- ACK (Acknowledgment, contains the receipt for the Update message.)

EIGRP Stub Router Commands:

- eigrp stub *(EIGRP configuration command that designates the router as an EIGRP stub router, with the default options of ‘connected’ and ‘summary’)*
- eigrp stub connected *(EIGRP configuration command that sets the router as an EIGRP stub with the ‘connected’ option, which will only advertise routes designated in network commands)*
- eigrp stub summary *(EIGRP configuration command that sets the router as an EIGRP stub with the ‘summary’ option, which will advertise auto-summarized or statically-configured summary routes)*
- eigrp stub static *(EIGRP configuration command that sets the router as an EIGRP stub with the ‘static’ option, which will advertise static routes assuming that the redistribute static command is configured)*
- eigrp stub leak-map EIGRP_BLOCK *(EIGRP configuration command that sets the router as an EIGRP stub with the ‘leak-map’ option, which will filter advertised routes specified by the ‘EIGRP_BLOCK’ leak map)*
- eigrp stub redistributed *(EIGRP configuration command that sets the router as an EIGRP stub with the ‘redistributed’ option, which will advertise redistributed routes assuming that redistribution is configured)*
- eigrp stub receive-only *EIGRP configuration command that sets the router as an EIGRP stub with the ‘receive-only’ option, which will not advertise any routes)*

Route Map Sample Setup Commands:

- route-map TEST deny 5
  - match ip address prefix-list DATA
- route-map TEST deny 10
  - match ip address prefix-list VOICE
- route-map TEST permit 15
- ip prefix-list DATA permit 10.10.10.0/24

- ip prefix-list VOICE permit 10.10.20.0/24

General Routing Commands:

- ip default-network 192.168.100.0 *(global configuration command that injects 192.168.100.0 into the routing protocols as a candidate default route)*

EIGRPv6 Setup Command Steps:

- ipv6 unicast-routing *(enables IPv6 routing unicast routing capability on the router)*
- ipv6 router eigrp 100 *(creates the EIGRPv6 routing process using ASN '100')*
- Enable IPv6 on an interface by either configuring an IPv6 address manually, or using the 'ipv6 enable' command.
- ipv6 eigrp 100 *(interface command to bind this interface to EIGRPv6 ASN '100')*
- no shutdown *(EIGRP configuration command that enables the process as it's disabled by default)*
- router-id 192.168.100.1 *(EIGRP configuration command that manually specifies the router's ID as '192.168.100.1')*

EIGRPv6 Commands:

- show ipv6 route eigrp *(displays all routes in the routing table that originated via EIGRPv6)*
- show ipv6 protocols *(shows EIGRPv6 interfaces, metric weights, variance, redistribution, maximum paths, and administrative distance)*
- show ipv6 eigrp neighbors *(displays EIGRPv6 neighbor information)*
- show ipv6 eigrp interfaces detail *(displays, among other information, interface-specific hello and hold timers)*
- show ipv6 eigrp topology *(displays the EIGRPv6 database in its entirety)*
- show ipv6 eigrp topology all-links *(displays the entire EIGRPv6 database, including inactive EIGRPv6 neighbor connections and routes)*
- debug ipv6 eigrp notifications *(shows you what updates are sent and received for EIGRPv6)*

Named EIGRPv6 & Related Commands:

- router eigrp PRIMARY_EIGRP *(global configuration command that creates a new EIGRP named virtual instance called 'PRIMARY_EIGRP')*
- address-family ipv6 autonomous-system 100 *(EIGRP configuration command that creates a new IPv6 address set under ASN '100')*
- network 2001:4567::/64 *(address-family command that specifies the IPv6 subnet 2001:4567::/64 network to be used)*
- eigrp stub *(address-family command that declares the related address group to identify as an EIGRP stub)*
- metric 0 1 0 1 0 0 *(address-family command that sets the EIGRP ToS and K-values for the related address family entry)*
- eigrp router-id 192.168.100.1 *(address-family command that sets the EIGRP router ID for this address family to '192.168.100.1')*
- af-interface Serial0/0 *(enters interface address-family configuration mode, and allows you to enter a series of subcommands to configure certain options, such as authentication, bandwidth-percent, hello-interval, hold-time, passive-interface, and split-horizon)*
- topology base *(address-family command to enter topology mode, which allows you to enter a series of options including auto-summary, maximum-paths, redistribute, and variance)*

OSPF Commands:

- router ospf 1 *(global configuration command to create OSPF process ID '1')*

- network 192.168.100.0 0.0.0.255 area 0 *(OSPF configuration command that adds 192.168.100.0/24 into distribution in AS ‘0’)*
- show ip ospf interface brief *(lists the interfaces on which OSPF is enabled based on network commands, and omits passive interface)*
- show ip protocols *(lists the contents of the configuration commands for each routing process and all enabled but passive interfaces)*
- show ip ospf neighbors *(lists known neighbors as well as neighbor state; does not list neighbors with mismatched parameters)*
- show ip ospf database *(lists all LSAs for all connected areas)*
- ip ospf 1 area 10 *(interface command that adds the affected interface to OSPF area 10 for OSPF process ‘1’)*
- passive-interface Serial0/0 *(OSPF command that declares interface Serial0/0 as passive)*
- ip ospf hello-interval 15 *(interface command that manually sets the OSPF hello interface to 15 seconds)*
- show ip ospf interface Serial0/0 *(displays OSPF interface statistics, including timers)*
- router-id 1.1.1.1 *(OSPF command that statically sets the router ID to ‘1.1.1.1’)*
- ip ospf network non-broadcast *(interface command that manually sets the OSPF detection type to NMA)*
- neighbor 10.10.10.1 *(OSPF command that manually sets a neighbor relationship with ’10.10.10.1’)*
- area 5 virtual-link 192.168.1.1 *(establishes an OSPF virtual link over AS ‘5’ to the router with an ID of ‘192.168.1.1’)*
- show ip ospf virtual-links *(displays OSPF virtual link information, including cost and adjacency status)*
- show ip ospf database router 192.168.1.1 *(displays detailed information for the OSPF database entry for 192.168.1.1’s Type 1 LSA, including connected networks and if they’re stubs or conventional networks)*
- show ip ospf database network 192.168.1.1 *(displays detailed information for the OSPF database entry for the 192.168.1.1 DR’s Type 2 LSA)*
- ip ospf priority 50 *(interface command that sets the OSPF router’s DR election priority to ‘50’)*
- show ip ospf database summary 192.168.100.0 *(displays information regarding the Type 3 Summary LSA that contains 192.168.100.0)*
- max-lsa 10 *(OSPF command that limits the amount of LSAs the router can learn from neighbors)*
- auto-cost reference-bandwidth 1000 *(OSPF command that changes the OSPF reference bandwidth to 1000 from the default)*
- ip ospf cost 10 *(interface command that manually sets the OSPF link cost to ’10’)*
- area 10 filter-list prefix DATA in *(OSPF command that filters prefixes from the ‘DATA’ prefix list inbound into OSPF area ‘10’)*
- ip prefix-list FILTER seq 5 deny 192.168.1.0/24 *(global command that creates the ‘FILTER’ prefix list and blocks 192.168.1.0/24 using it)*
- distribute-list prefix FILTER in *(OSPF command that takes the ‘FILTER’ prefix list mentioned prior, and applies it to LSDB distribution)*
- area 50 range 10.10.10.0 255.255.255.0 50 *(OSPF command that creates a summary for 10.10.10.0/24 in area 50, and gives it a cost of ‘50’)*
- area 10 range 0.0.0.0 0.0.0.0 *(OSPF command that advertises a default route as originating from area 10)*
- default-information originate *(OSPF command that will allow the advertisement of default routes without other explicit commands)*
- area 50 stub *(OSPF command that designates area 50 as a stub; must be entered on all routes in this area for it to take effect)*
- area 50 stub no-summary *(OSPF command that designates area 50 as totally stubby; must be entered on all ABRs for this area)*
- area 50 default-cost 10 *(OSPF command that sets the default route cost for area 50 to ‘10’)*
- show ip ospf database database-summary *(only lists summary information for different areas in the OSPF database)*
- area 50 nssa no-summary *(OSPF command that designates area 50 as a Totally NSSA)*
- area 50 nssa default-information originate *(OSPF command that designates area 50 as a NSSA)*
- show ip ospf database external 192.168.0.0 *(displays the external entry in the OSPF database for 192.168.0.0)*

- show ip ospf database asbr-summary *(displays only the sections of the OSPF database that deal with Type 4 ASBR summary LSAs)*
- show ip ospf border-routers *(displays only the ABRs and ASBRs in the OSPF database)*

OSPF LSA Types:

1. **Router LSA** – Each router creates its own Type 1 LSA to represent itself for each area to which it connects. The LSDB for one area contains one Type 1 LSA per router per area, listing the RID and all interface IP addresses on that router that are in that area. Represents stub networks as well.
2. **Network LSA –** One per transit network. Created by the DR on the subnet, and represents the subnet and the router interfaces connected to the subnet.
3. **Net Summary LSA –** Created by ABRs to represent subnets listed in one area's Type 1 and 2 LSAs when being advertised into another area. Defines the links (subnets) in the origin area, and cost, but no topology data.
4. **ASBR Summary LSA –** Like a Type 3 LSA, except it advertises a host route used to reach an ASBR.
5. **AS External LSA –** Created by ASBRs for external routes injected into OSPF.
6. **Group Membership LSA –** Defined for MOSPF; not supported by the Cisco IOS.
7. **NSSA External LSA –** Created by ASBRs inside an NSSA area, instead of a Type 5 LSA.
8. **Link LSA –** Type 8 LSAs only exit on a local link, where they are used by a router to advertise the router's link-local address to all other routers on the same link. Additionally, the Type 8 LSA provides to routers on that link a listing of all IPv6 addresses associated with the link.
9. **Intra-Area Prefix LSA –** Can send information about IPv6 networks (including stub networks) attached to a router (similar to the Type 1 LSA for IPv4 networks). Additionally, a Type 9 LSA can send information about transit IPv6 network segments within an area (similar to the Type 2 LSA for IPv4 networks).
10. **Opaque LSA –** Used as generic LSAs to allow easy future extension of OSPF. For example, Type 10 has been adapted for MPLS traffic engineering.
11. " "

OSPF Stub/NSSA Capability Matrix

Area Type	**ABRs Flood Type 5 External LSAs into the Area?**	**ABRs Flood Type 3 Summary LSAs into the Area?**	**Allows Redistribution of External LSAs into the Stubby Area?**
Stub	No	Yes	No
Totally stubby	No	No	No
NSSA	No	Yes	Yes
Totally NSSA	No	No	Yes

OSPFv3 Commands:

- ipv6 unicast-routing *(global command that enables IPv6 routing capabilities)*
- ipv6 router ospf 1 *(global command that starts OSPFv3 on the router under process ID '1')*
- router-id 192.1.1.1 *(OSPFv3 command that manually sets the router's ID to '192.1.1.1')*
- ipv6 ospf 1 area 5 *(interface command that adds the interface into OSPFv3's process 1, in area '5')*
- passive-interface Serial0/0 *(OSPFv3 command that designates Serial0/0 as a passive interface if needed)*
- show ipv6 ospf neighbor *(displays neighbor partnership information for OSPFv3)*
- ipv6 ospf neighbor FE80:4567::1 *(interface command that manually specifies an OSPFv3 neighbor of FE80:4567::1)*

- address-family ipv6 unicast *(OSPFv3 command that creates an address family set of rules for IPv6)*
- ospfv3 1 ipv6 area 0 *(interface command that adds the interface into OSPFv3 process '1' and area 0)*
- area 5 stub no-summary *(address family command that creates a totally NSSA on an address family)*
- show ospfv3 neighbor *(displays OSPFv3 neighbor adjacency information)*
- show ospfv3 interface brief *(displays OSPFv3 interface information including IPv4/IPv6, and adjacency status)*
- show ospfv3 database *(displays the OSPFv3 link-state database)*

Route Redistribution Commands:

- redistribute ospf 5 *(EIGRP/BGP command that allows distribution of OSPF AS 5 routes in the current routing protocol)*
- redistribute eigrp 5 *(OSPF/BGP command that allows distribution of EIGRP AS 5 classful routes in the current routing protocol)*
- redistribute connected *(routing command that allows distribution of connected routes in the current routing protocol)*
- redistribute ospf 5 route-map DATA *(EIGRP/BGP command that redistributes routes in OSPF AS 5 after filtering them through the 'DATA' route map)*
- redistribute eigrp 5 subnets *(OSPF/BGP command that allows distribution of EIGRP AS 5 classless routes in the current routing protocol)*
- redistribute eigrp 10 metric-type 1 *(OSPF command that distributes EIGRP AS 10 into OSPF, but does so as an E1 external)*
- redistribute eigrp 5 metric 5 *(OSPF command that redistributes routes in EIGRP AS 5 into OSPF with a metric of 5)*

With external routes, E1 routes include both the outside cost as well as internal cost (cost on the remote ASN as well as the local one), whereas E2 routes only include the outside cost (cost on the remote ASN).

Switching, CEF, and PBR Commands

- no ip route-cache *(interface command to manually enable process-based switching on your switch port)*
- ip route-cache *(interface command to manually enable fast switching on your switch port)*
- ip cef *(global command to enable CEF on the switch as a whole)*
- ip route-cache cef *(interface command to enable CEF on a single interface, if already globally allowed)*
- show ip cef *(displays a router's FIB table contents)*
- show adjacency *(displays basic information about FIB table adjacencies)*
- show adjacency detail *(displays more details about the FIB table adjacencies)*
- show ip interface Serial0/0 *(among other things, will show you the packet switching type allowed on the Serial0/0 interface)*
- set ip next-hop 192.168.1.1 *(route map command that statically forces 192.168.1.1 to be used as the next hop if the route map's criteria is triggered)*
- set ip default next-hop 192.168.1.1 *(same as the previous command, except PBR will first attempt to route based off the routing table)*
- set interface Serial0/0 *(route map command that will attempt to send the packet out the Serial0/0 interface; multiple interfaces can be specified here)*
- ip policy route-map FILTER *(interface policy command that binds the 'FILTER' route map to the interface)*
- show ip policy *(displays all interfaces and active policies bound to them)*
- show route-map *(displays basic route-map information for route maps that are actively being used)*
- debug ip policy *(shows transactional packet information for PBR-related packets)*
- set ip precedence *(route map command that manually sets the IPP value)*

- set ip tos 5   *(route map command that explicitly sets the Type of Server value to ‘5’)*

IP SLA Setup Commands

- The following is an IP SLA process setup that sends ICMP echos to 192.168.1.1 every 60 seconds, using source address 192.168.2.1, starting the operation immediately and running it indefinitely.
  - ip sla 10
  - icmp-echo 192.168.1.1 source-ip 192.168.2.1
  - frequency 60
  - exit
  - ip sla schedule 10 start-time now life forever

IP SLA Commands:

- show ip sla configuration   *(shows IP SLA configuration entries and status)*
- show ip sla statistics 10   *(shows stats for IP SLA entry number ‘10’)*
- track 1 ip sla 10 state   *(global command that creates track object numbered as ‘1’, and uses it to keep track of the state of IP SLA entry number ‘10’)*
- delay up 60 down 60   *(track command that sets the delay necessary between trigger conditions as 60 seconds)*
- ip route 192.168.0.0 255.255.255.0 192.168.1.1 track 1   *(creates an IP route that will only work if track condition ‘1’ is met)*
- show track   *(shows the configuration and status of all track objects)*
- set ip next-hop verify-availability 192.168.1.1 1 track 1   *(route map command that uses a combination of PBR and track object ‘1’ status to enable its criteria-based filtering)*

VRF Commands:

- ip vrf DATA   *(global command that creates a VRF called ‘DATA’ and enters configuration mode for it)*
- ip vrf forwarding DATA   *(interface command that adds the interface into the ‘DATA’ VRF forwarding group)*
- router ospf 1 vrf DATA   *(global command that binds OSPF process ‘1’ to the VRF ‘DATA’ forwarding group)*
- show ip vrf   *(shows all the VRFs currently configured on the router)*
- show ip route vrf DATA   *(shows all the routers in the DATA VRF’s routing table section)*
- ping vrf DATA 192.168.1.1   *(demonstrates usage of the PING command when pinging within a VRF)*

BGP ASN Spaces:

- 0 – Reserved
- 1 through 64,495 – Assignable by IANA for public use
- 64,496 through 64,511 – Reserved for use in documentation
- 64,512 through 65,534 – Private use
- 65,535 – Reserved

Advanced DHCP & NAT Commands:

- no ip dhcp client request *(interface command that prevents the interface, if set to DHCP, from adding a default route gained through that DHCP lease)*
- ip nat enable *(interface command that enables NAT Virtual Interface features)*
- ip nat inside source list 1 interface Serial0/0 overload *(global command that, coupled with NVI, enables PAT using ACL '1' on interface Serial0/0)*

BGP Commands:

- router bgp 10 *(global command that creates a process for BGP AS 10, and enters the configuration mode for it)*
- neighbor 192.168.1.1 remote-as 10 *(specifies 192.168.1.1 as a BGP neighbor in AS 10, which can make it either iBGP or eBGP depending on what AS the router this command is entered on has)*
- bgp router-id 192.1.1.1 *(BGP command that manually sets the BGP router ID to 192.1.1.1)*
- neighbor 192.168.1.1 update-source Loopback0 *(BGP command that sets the originating IP address for the 192.168.1.1 neighborship to be Loopback0's IP address instead of that of the physical interface the connection will go out)*
- neighbor 192.168.1.1 ebgp-multihop 10 *(BGP command that sets the 192.168.1.1 neighborship to allow a maximum of 10 hops, instead of the default of '1')*
- show ip bgp summary *(displays summary information for BGP neighbor and process status)*
- show ip bgp neighbors *(displays more complex information about BGP neighbor configuration)*
- show ip bgp neighbors 1.1.1.1 *(same as the previous command, but only lists information for the '1.1.1.1' neighborship)*
- neighbor 192.1.1.1 shutdown *(BGP command that turns off the neighborship for 192.1.1.1 by turning it to 'Idle' status)*
- debug ip bgp *(displays packet debug information for BGP)*
- show ip bgp *(only displays the BGP routes learned and pathing information, but not status)*
- show ip bgp neighbors 192.1.1.1 received-routes *(displays routes received from 192.1.1.1 prior to applying inbound route filters)*
- show ip bgp neighbors 192.1.1.1 routes *(same as the previous command, but displays routes post-filters)*
- show ip bgp neighbors 192.1.1.1 advertised-routes *(lists routes advertised to 192.1.1.1 after applying filters)*
- network 192.168.0.0 mask 255.255.255.0 *(BGP command that advertises 192.168.0.0/24 to any neighbors)*
- auto-summary *(BGP command that changes the default of no auto summarization to using auto summarization)*
- redistribute ospf 5 route-map FILTER *(BGP command that redistributes OSPF's AS '5' routes after running them through the 'FILTER' route map)*
- aggregate-address 192.168.0.0 255.255.192.0 summary-only *(BGP commands that creates a manual summary route for 192.168.0.0/18)*
- neighbor 192.1.1.1 next-hop-self *(advertises to neighbor 192.1.1.1 more than 1 hop away, but allows the BGP peer that ultimately does the direct relay to 192.1.1.1 to advertise the neighborship as coming from its own IP, making multi-hop reachability issues less severe)*
- synchronization *(BGP command that allows redistribution of eBGP routes into an IGP, including iBGP – is disabled by default)*
- neighbor 192.1.1.1 prefix-list FILTER in *(BGP command that applies the FILTER prefix list to routes learned by 192.1.1.1)*
- neighbor 192.1.1.1 route-map FILTER in *BGP command that applies the FILTER route map to routes learned by 192.1.1.1)*
- clear ip bgp 192.1.1.1 *(global command that performs a hard reset on the BGP neighborship with 192.1.1.1)*
- clear ip bgp 192.1.1.1 out *(global command that hard resets all routes shared with 192.1.1.1)*
- clear ip bgp 192.1.1.1 soft in *(global command that soft resets all routes received inbound from 192.1.1.1)*
- neighbor 192.1.1.1 weight 50 *(BGP command to add a weight of '50' to all routes learned from 192.1.1.1)*

- set weight 50 *(route map command that allows you to manually set a BGP weight of 50 for inbound routes)*
- set local-preference 150 *(route map command that sets the local preference of affected routes to ‘150’)*
- show ip bgp rib-failures *(displays all RIB table next-hop losses in the routing determination process)*
- set as-path prepend 10 10 *(route map command that prepends AS ‘10’ twice onto routes to increase the virtual hop count)*
- set metric 10 *(route map command that sets the MED value to ‘10’)*

BGP Attributes & Values

Processing Priority	**Name**	**Description**
0	Next hop	Is the next hop reachable?
1	Weight	Cisco-proprietary; bigger is better.
2	Local Preference	Bigger is better.
3	Locally-injected routes	Preferred over iBGP or eBGP-learned routes.
4	AS Path Length	Smaller is better.
5	Origin	I is preferred over E. E is preferred over unknown.
6	MED	Smaller is better.
7	Neighbor type	eBGP is preferred over iBGP.
8	IGP Metric to Next Hop	Smaller is better.

Advanced IPv6 Commands

- ipv6 traffic-filter FILTER out *(interface command that bind the ‘FILTER’ IPv6 ACL to outbound traffic)*
- set ipv5 next-hop 2001:4567::1 *(route map command that manually sets the PBR next hop to 2001:4567::1)*
- address-family ipv6 *(MP-BGP command that enters config mode for the IPv6 side of the protocol)*
- network 2001:4567::/64 *(IPv6 address family command that adds the 2001:4567::/64 to be shared among MP-BGP peers)*
- neighbor 192.1.1.1 activate *(IPv6 address family command that turns up the neighborship for the MP-BGP peer with router ID ‘192.1.1.1’)*
- show bgp ipv6 unicast *(displays next-hop networks known to MP-BGP and how to reach them)*
- show bgp ipv6 unicast summary *(same as the previous command, but briefer)*

Advanced ACL & Security Commands:

- time-range DAY *(global command that creates a time range called ‘DAY’, and enters configuration mode for it)*
- periodic weekdays 8:00 to 17:00 *(time range command that declares the time range parameters to be weekdays from 8AM to 5PM)*
- absolute start 08:00 1 June 2018 end 17:00 31 July 2018 *(time range command that declares an absolute time range from the start of the business day on June 1st, through to EoB on July 31st in 2018)*
- access-list FILTER time-range DAY *(global command that applies the ‘DAY’ time range we created earlier to the ‘FILTER’ access list)*
- ip verify unicast source reachable-via rx *(interface command that enables uRPF in strict mode; CEF must be enabled for this command to work)*
- ip verify unicast source reachable-via any *(same as the previous command, but in loose mode)*
- ip verify unicast source reachable-via rx allow-default *(same as the first ‘rx’ command, but allows a default route to be used for return traffic)*

AAA Commands:

- aaa new-model *(global command that enables AAA authentication)*
- aaa authentication login AUTH group tacacs+ local *(global command that specifies AAA to use the 'AUTH' group for login, attempt to use TACACS+ first, and should that fail, use a local login)*
- username Caleb secret IsAwesome! *(global command to create the 'Caleb' user, and set his encrypted password to 'IsAwesome!')*
- tacacs server CISCO-DEFAULT *(global command to specify a TACACS server under the name 'CISCO-DEFAULT')*
- address ipv4 192.168.1.1 *(tacacs server command that specifies the server IPv4 address of '192.168.1.1')*
- key cisco *(tacacs server command that specifies the authentication key for TACACS+ to be 'cisco')*
- login authentication CISCO-AUTH *(vty command that specifies the authentication methods to be the 'AUTH' group we created prior)*

SNMP Commands:

- snmp-server community PASSWORD ro 10 *(global command that specifies the read-only password for SNMP as 'PASSWORD', and binds ACL 10 to this access)*
- snmp-server community SECRET rw 10 *(global command similar to the first, but for the read-write SNMP access)*

NTP Commands:

- ntp authentication-key KEY md5 81naslfjna *(global command that specifies the 'KEY' string with the MD5 hash listed for authentication to NTP)*
- ntp authenticate *(global command that tells the local Cisco NTP server to authenticate client requests)*
- ntp trusted-key KEY *(global command that tells the local Cisco NTP server to use the 'KEY' key string to authenticate client requests)*
- ntp master 4 *(global command that tells the local Cisco NTP server to assign itself a stratum level number of '4')*
- ntp server 192.168.1.1 key KEY *(global command that tells the Cisco NTP client to authenticate against 192.168.1.1 for NTP, and use the 'KEY' string)*
- show ntp status *(displays the NTP status, and servers used)*
- show ntp associations detail *(shows more details information for NTP, including keys, status, and stratum)*

Frame Relay Commands:

- encapsulation frame-relay *(interface command that specifies the frame-relay encapsulation method)*
- frame-relay map ip 192.168.1.1 104 *(interface command that manually specifies the mapped next hop to IP 192.168.1.1, with a DLCI of '104')*
- frame-relay map bridge 104 *(interface command that manually maps the point-to-point link as a DLCI bridge to DLCI '104')*
- frame-relay lmi-type cisco *(interface command that manually sets the LMI type to Cisco's, although this has been the default since IOS 12.2)*
- keepalive 10 *(interface command that manually sets the LMI keepalive interval to 10 seconds)*
- frame-relay svc *(interface command that enables Frame Relay Switched Virtual Circuit support)*
- map-group DEFAULT *(interface command that assigns the DEFAULT Frame Relay map group to the interface)*

OSPF Neighbor States/Order

1. **Down –** No information has been received on the segment.
2. **Init –** The interface has detected a Hello packet coming from a neighbor, but bidirectional communication has not yet been established.
3. **2-Way –** There is bidirectional communication with a neighbor. DR and BDR election would now take place, if necessary. Routers decide whether to proceed in building an adjacency.
4. **ExStart –** Routers are trying to establish the initial sequence number that is going to be used to exchange information packets. One router becomes the master, with the other becoming the slave.
5. **Exchange –** Routers will describe their entire LSDB by sending DBD packets. Includes all LSAs that describe Networks.
6. **Loading –** Routers are finalizing the information exchange. LSRs have been completed.
7. **Full –** Adjacency is complete, with all routers having similar LSDBs.

BGP Neighbor States/Order

1. **Idle –** Listens for peer connections.
2. **Connect –** Waits for successful TCP negotiation with peer. Attempts to send Open message and transition to OpenSet.
3. **Active –** If TCP negotiation fails, router ends up in Active state. Will re-attempt, and eventually transition back to Idle if unsuccessful.
4. **OpenSent –** Open messages are exchange between peers. Validity is checked. If successful, keepalives are started.
5. **OpenConfirm –** Router waits for a keepalive from its peer. Doesn’t usually stay in this state for very long.
6. **Established –** Routers have successfully peered, and Updates are exchanged. If there are errors during updates, both routers transition back to the Idle state.