Payload Types At Different OSI Layers:

- Layer 2 - Frame
- Layer 3 - Packet
- Layer 4 - Datagram

Default Cisco Terminal Options:

- 9600 bits/second
- No hardware flow control
- 8-bit ASCII
- No parity
- 1 stop bit

Setting Console/VTY Password:

- line console 0 *(switches you to console port config)*
- line vty 0 4 *(switches you to VTY port config)*
- login *(forces you to use credentials for future console port access)*
- password cisco *(changes the console password to 'cisco')*

General Cisco Commands:

- hostname CalebRouter *(sets the hostname of the device to 'CalebRouter')*
- exit (*moves back to the next higher mode in the command line)*
- end *(immediately return to enable mode from any of the configuration submodes)*
- Ctrl + Z *(this key combination does the same thing as the 'end' command*)
- no debug all *(disables all currently-enabled logs)*
- undebug all *(" ")*
- reload *(reboots the Cisco device)*
- copy running-config startup-config *(copies the active configuration to the configuration stored in NVRAM)*
- copy startup-config running-config *(copies the stored config in NVRAM to the active config in RAM)*
- write erase *(deletes the startup configuration stored in NVRAM)*
- erase startup-config *(" ")*
- erase nvram: *(" ")*
- quit *(disconnects you from the current CLI session as long as you're in EXEC mode)*
- enable *(switches the connected session from user mode to EXEC mode)*
- disable *(switches the connected session from EXEC mode to user mode)*
- configure terminal *(switches the connected session from EXEC mode to configuration mode)*
- username caleb secret Awesome *(creates the user 'Caleb' and sets his encrypted password to 'Awesome')*
- enable secret Awesome *(specifies the encrypted EXEC mode password for the switch to be 'Awesome')*
- history size 30 *(tells the command history buffer to contain the last 30 commands entered)*
- logging synchronous *(tells the device to only show log messages when you're finished typing a command, and not during a command being typed)*
- logging console *(tells the device to show log message entries on the console; can be turned off by preceding with 'no')*
- exec-timeout 15 0 *(sets the timeout for VTY sessions to be 15 minutes and 0 seconds)*
- terminal history size 50 *(changes the history buffer size to 50, but only for the current user)*

General Cisco 'Show' Commands:

- show running-config *(displays the contents of the configuration stored in RAM)*
- show startup-config *(displays the contents of the configuration stored in NVRAM)*
- show interfaces status *(displays basic status information about each interface in an easy-to-read format)*
- show dhcp lease *(lists any information regarding the addresses the device acquired as a DHCP client)*
- show crypto key mypubkey rsa *(lists the public and shared key generated by the device during SSH setup)*
- show ip ssh *(shows status information regarding the SSH server)*
- show ssh *(shows current connection information for active SSH sessions)*
- show interface vlan 5 *(shows detailed information about the VLAN 5 interface)*
- show ip default-gateway *(shows the currently-configured default gateway for the device)*
- show history *(lists the commands that are currently in the history buffer)*
- show ip interface brief *(shows a limited line item-style readout of interface status and configuration)*
- show protocols *(lists global information about protocols used on interfaces)*
- show controllers Serial0/0/0 *(shows controller circuit information for Serial interfaces)*

MAC Address Table Commands:

- show mac address-table *(shows all MAC address table entries of all types)*
- show mac address-table dynamic *(shows all dynamically-learned MAC address table entries)*
- show mac address-table dynamic vlan 2 *(shows all dynamically-learned MAC address table entries in VLAN 2)*
- show mac address-table dynamic address 01:02:03:04:05:06 *(shows the dynamically-learned MAC address table entries for this address)*
- show mac address-table dynamic Fa0/1 *(shows all dynamically-learned MAC addresses on the Fa0/1 interface)*
- show mac address-table aging-time *(shows the global as well as per-VLAN aging timeout for table entries)*
- clear mac address-table dynamic *(clears all dynamically-learned entries out of the MAC address table)*
- show mac address-table secure Fa0/1 *(shows port security-learned MAC addresses for the Fa0/1 interface)*
- show mac address-table static Fa0/1 *(shows MAC addresses statically added for the Fa0/1 interface)*

SSH Setup Steps:

- Make sure that you've already got a local username/password combo created.
- ip domain-name *huggenberger.local* (*this appends this DNS suffix to all this device's connections*)
- crypto key generate rsa 2048 (*creates an RSA key pair for a modulus size of 2048)*
- ip ssh version 2 (*enables SSHv2, which is much more secure than v1*)
- Use the '*transport input ssh'* command on a VTY line to force incoming connections to only use SSH.

IPv4 Addressing:

- interface vlan 1 *(changes the configuration scope to the VLAN 1 interface)*
- ip address 192.168.100.10 255.255.255.0 *(statically configures the specified address on a defined interface)*
- ip address dhcp *(dynamically configures a DHCP address on the defined interface)*
- ip default-gateway 216.229.20.1 *(configures the device's default gateway address to be 216.229.20.1)*
- ip name-server 216.229.25.5 216.229.25.25 *(specifies two DNS servers for the switch to use for name lookups)*

Interface Commands:

- interface GigabitEthernet 0/1 *(selects the GigabitEthernet 0/1 interface to enter config mode for)*
- interface range GigabitEthernet 0/1 – 5 *(configures the range of ports all at once from 0/1 through 0/5)*
- shutdown *(administratively sets an interface's status to 'down'; can be reverted by preceding with 'no')*
- speed 100 *(sets an Ethernet interface's speed to 100Mb)*
- duplex half *(sets the duplex function of an Ethernet interface to 'half')*
- bandwidth 1000 *(sets the interface speed that the router considers it to operate at, but doesn't change the actual interface speed; used for things like routing metric calculation)*
- clock rate 64000 *(sets the clocking rate on serial interfaces in terms of bits per second; 64000 in this case)*
- description WiFiAccessPoint37 *(sets the interface's readable description to 'WiFiAccessPoint37')*
- show interface Fa0/1 status *(shows line item-style status information for the Fa0/1 interface)*
- show interface description *(shows a line-item style readout of all the interface descriptions)*

Port Security Commands:

- switchport mode access *(manually sets the defined port to be an access port)*
- switchport port-security mac-address 01:02:03:04:05:06 *(configures the specified MAC address as the only allowed MAC address on this interface)*
- switchport port-security mac-address sticky *(adds the first MAC address detected in the ARP table for this interface to be the only allowed MAC address for it)*
- switchport port-security maximum 5 *(sets the maximum number of allowed MAC addresses on this interface to '5')*
- switchport port-security violation shutdown *(changes the violation action to shutting down a port for breaking port security rules)*
- show port-security interface Fa0/1 *(shows related port security information for the Fa0/1 interface)*
- show port-security *(lists one line per interface showing the port security settings for them)*

VLAN & Trunking Commands:

- vlan 3 *(creates VLAN 3 if it doesn't already exist, and puts you into configuration mode for it)*
- name *(used within a VLAN's configuration mode to declare a readable name for it)*
- shutdown *(used within a VLAN's configuration mode to administratively turn it off without removing it)*
- shutdown vlan 3 *(global-level command to turn VLAN 3 off without removing it)*
- vtp mode transparent *(global-level command that sets the VTP mode to transparent)*
- switchport access vlan 5 *(interface-level command to set a port's access VLAN to 5)*
- switchport trunk encapsulation dot1q *(specifies a trunk's encapsulation protocol to the DOT1Q standard)*
- switchport trunk native vlan 4 *(sets the default untagged VLAN on the defined interface to '4')*
- switchport nonegotiate *(interface-level command that tells the port to never negotiate to be a trunk port)*
- switchport voice vlan 10 *(interface-level command that defines the voice VLAN used, and subsequently to use DOT1Q encapsulation for packets in that VLAN for the port)*
- switchport trunk allowed vlan 1,2,5 *(tells the trunk port in question to only allow VLANS 1, 2, and 5)*
- show interface Fa0/1 switchport *(shows switchport VLAN-related information and state for Fa0/1)*
- show interface Fa0/1 trunk *(shows information about operational trunks on interface Fa0/1)*
- show vlan brief *(shows limited VLAN information about VLANs on this device)*
- show vlan id 5 *(shows detailed information about VLAN 5)*
- show vlan *(shows detailed information about all VLANs, including connected ports, for this device)*
- show vtp status *(lists VTP configuration and status information)*

Static Route and RoaS Commands:

- interface Fa0/0.5 *(creates a subinterface on Fa0/0 to be used in RoaS setups)*
- encapsulation dot1q 10 native *(VLAN interface-level command to specify encapsulation or native VLAN status)*
- sdm prefer lanbase-routing *(enables Layer 3 routing on an older Cisco switch if it supports this)*
- ip routing *(enables Layer 3 routing on newer Cisco routers and switches)*
- ip route 192.168.100.0 255.255.255.0 192.168.99.1 *(creates a static route to the 192.168.100.0/24 subnet through 192.168.99.1)*
- ip route 192.168.100.0 255.255.255.0 192.168.99.1 permanent *(creates a static route to the 192.168.100.0/24 subnet through 192.168.99.1 that persists even if 192.168.99.1 isn't reachable)*
- ip route 192.168.100.0 255.255.255.0 192.168.99.1 100 *(creates a static route to the 192.168.100.0/24 subnet through 192.168.99.1 with a cost of 100)*
- show ip route *(lists the router's entire routing table)*
- show ip route static *(lists the router's routing table for routes that were statically added)*
- show arp *(shows the IPv4 ARP table for the router)*
- show ip arp *(" ")*
- clear ip arp 192.168.100.1 *(removes the 192.168.100.1 bonding from the ARP table)*

Setting up a Layer 3 Switch for inter-VLAN routing:

- Enable support for IP routing. (*sdm prefer lanbase-routing*)
- Enable IP routing. (*ip routing*)
- Create VLAN interfaces for each VLAN to be routed. (*interface VLAN 10)*
- Configure an appropriate IP address and mask for each VLAN interface. (*ip address 10.0.0.1 255.0.0.0)*
- Turn the VLAN interface on. (*no shutdown*)

RIPv2 Routing Commands

- router rip *(global command that enters RIP configuration mode)*
- network 192.168.100.0 *(RIP subcommand that enables RIP on all interfaces within the 192.168.100.0 classful network)*
- version 2 *(RIP subcommand that enables version 2 of RIP)*
- passive-interface Fa0/1 *(RIP subcommand that tells RIP to no longer advertise updates on the Fa0/1 interface)*
- passive-interface default *(RIP subcommand that changes the RIP default to make all RIP-enabled interfaces passive)*
- auto-summary *(RIP subcommand that enables the auto summarization feature of RIP; can be reverted by preceding with 'no')*
- maximum-paths 10 *(RIP subcommand that changes the default number of hops before routes are discarded)*
- default-information originate *(RIP subcommand that allows the advertisement of the default route)*
- show ip route rip *(shows all the routes the router has learned via RIP)*
- show ip rip database *(shows a line item-style listing of router adjacencies via RIP)*
- show ip route 192.168.100.1 *(shows routing information specific to the route the 192.168.100.1 address is located on)*

DHCP Server Commands:

- ip dhcp pool IP_Pool *(creates a DHCP pool under the name 'IP_Pool')*
- ip dhcp excluded-address 192.168.100.100 192.168.100.150 *(DHCP pool subcommand that creates an address exclusion from .100 to .150)*
- network 192.168.100.0/24 *(DHCP pool subcommand that enables DHCP on the specified subnets/interfaces)*
- default-router 192.168.100.1 *(DHCP pool subcommand that defines the default gateway for address leases)*
- dns-server 216.229.25.25 216.229.0.25 *(DHCP pool subcommand that specifies the DNS servers to be used in DHCP leases given)*
- lease 1 0 0 *(DHCP pool subcommand that sets the lease time as 1 day, 0 hours, and 0 minutes)*
- ip helper-address 192.168.101.1 *(interface subcommand that tells the router to forward DHCP broadcasts on that interface to 192.168.101.1)*
- show ip dhcp binding *(lists the currently-leased addresses on the DHCP server)*
- show ip dhcp pool IP_Pool *(lists the full range of IPs for the 'IP_Pool' DHCP pool, as well as usage statistics)*
- show ip dhcp server statistics *(lists statistics about requests served by the DHCP server)*
- show ip dhcp conflict *(lists IP addresses that the DHCP server found were already in use when a lease attempt was made)*
- clear ip dhcp conflict *(removes all entries from the conflicting DHCP lease table)*

Standard ACL Commands:

- access-list 1 remark "This is for router security on VLAN 5" *(access list command that leaves a remark)*
- access-list 1 deny 192.168.100.0 0.0.0.255 *(denies traffic from 192.168.100.0/24)*
- ip access-group 1 in *(interface-level command that bounds access-list 1 to this interface's rules)*
- show access-list 1 *(shows the details of access-list 1)*
- show ip access-list 1 *(shows the IP-related details of access-list 1)*
- ip access-list standard Self_Deny *(creates a standard ACL with the name Self_Deny)*

Extended ACL Commands:

- access-list 100 deny tcp 192.168.102.0 0.0.0.255 192.168.101.0 0.0.0.255 eq 80 *(creates a rule to deny TCP HTTP traffic from 192.168.102.0/24 to 192.168.101.0/24)*
- access-list 101 permit ip any any *(global whitelist ACL entry)*
- ip access-group 1 in *(interface-level command that bounds access-list 1 to this interface's rules)*
- ip access-list extended Self_Deny *(creates an extended ACL with the name Self_Deny)*
- deny tcp 192.168.105.0 0.0.0.127 192.168.104.0 0.0.0.63 eq 443 *(ACL subcommand that denies TCP HTTPS traffic from 192.168.105.0/25 to 192.168.104.0/26)*
- remark "Test ACL" *(ACL subcommand that creates a remark)*

NAT Setup Commands:

- ip nat inside *(interface subcommand to tell NAT that this is the LAN-side point for NAT)*
- ip nat outside *(interface subcommand to tell NAT that this is the WAN-side point for NAT)*
- ip nat inside source list 100 interface Gi0/1 pool Default_IPs *(specifies the inside NAT side, bonds ACL 100 to the interface for translations, and uses pool name "Default_IPs")*
- ip nat inside source interface Gi0/1 pool Inside_IPs overload *(specifies the inside NAT side, uses pool name "Inside_IPs", and uses overloaded PAT)*
- ip nat pool Inside_IPs 216.229.11.19 216.229.11.20 netmask 255.255.255.248 *(global command to define a pool of NAT addresses)*
- ip nat inside source 192.168.100.1 216.229.11.19 *(global command that lists the inside and outside addresses for NAT translation, respsectively)*
- show ip nat statistics *(lists NAT counters as well as basic configuration information)*
- show ip nat translations *(displays the current NAT table)*
- clear ip nat translation inside 216.229.20.1 192.168.100.1 *(clears the 216.229.20.1 translation from the dynamic NAT table)*
- debug ip nat *(turns on console logging for NAT-related log messages)*

IPv6 Address Types:

- 0:0:0:0:0:0:0:0 This is the equivalent of 0.0.0.0 in IPv4
- 0:0:0:0:0:0:0:1 This is the equivalent of IPv4's loopback address (127.0.0.1)
- 0:0:0:0:172:16:100:1 How an IPv4 address would be written in a mixed IP environment (IPv4 & IPv6)
- 2000::/3 The global unicast address range
- FC00::/7 The unique local unicast range *(the RFC specifies FD00::/8 as well)*
- FE80::/10 The link-local unicast range
- FF00::/8 The multicast range
- 3FFF:FFFF::/32 Reserved for examples and documentation
- 2001:0DB8::/32 Also reserved for examples and documentation
- 2002::/16 Used with the 6-to-4 tunneling protocol

IPv6 addresses use the first 23 bits for the Internet Registry, 9 bits for the ISP Prefix, 16 bits for the company, 16 bits for the subnet, and the remaining 64 bits for the host interface ID. In that order.

You can calculate the IPv6 EUI-64 address by leaving the 64 network bits of the IP address as-is, and using the MAC address of the device to make the last 64. You insert "*FFFE*" into the center of the MAC address, and then invert the 7th bit from the left of the front of the MAC address

IPv6 Addressing Commands:

- ipv6 address *2001:cd:81:511:FF:FA6:61:1/64* (*configures this IP address on an interface*)
- ipv6 address 2001:cd:81:511::/64 eui-64 (*tells the interface to calculate a EUI address within this network*)
- ipv6 enable (*required to make a router pass IPv6 traffic through packet routing*)
- ipv6 address autoconfig (*tells an interface to create its own EUI-64 address based off a RA it receives*)
- ipv6 address autoconfig default (*autoconfigures a default route from a RA that's received*)
- show ipv6 interface *FastEthernet 0/1* (*shows IPv6 details for this interface*)
- ipv6 unicast-routing (*enables IPv6 globally on a router*)
- show ipv6 route (*lists the IPv6 routing table*)
- show ipv6 interface brief (*shows brief IPv6 interface status*)
- ipv6 address dhcp (*tells an interface to get it's IPv6 address through DHCP*)
- ipv6 dhcp relay destination 2001:DB8:1111:3::8 (*configures IPv6 DHCP relay*)
- ipv6 route *2001:DB8:1111:2::/64 2001:DB8:1111:4::2* (*configures a static IPv6 route*)
- ipv6 route ::/0 2001:DB8:1111:4::2 *(configures the IPv6 default route)*
- ipv6 router ospf 1 (*configures OSPFv3 using process ID '1'*)
- ipv6 ospf 1 area 0 (*used on an interface, adds OSPFv3 routing to process '1'*)
- router-id 1.1.1.1 (*this same command enables OSPFv3 router ID '1.1.1.1', just as in OSPFv2*)
- show ipv6 ospf interface brief (*shows brief details about all active OSPF interfaces*)
- show ipv6 protocols (*shows all IPv6 protocols running on the router at present*)
- show ipv6 ospf neighbor (*shows all ND OSPF routing neighbors in the same OSPF area*)
- show ipv6 ospf database (*self-explanatory*)
- traceroute6 *(test IPv6 routes using the IPv6 version of traceroute)*

Default Routing Protocol Administrative Distances:

- Connected 0
- Static 1
- BGP (external) 20
- EIGRP (internal) 90
- IGRP 100
- OSPF 110
- IS-IS 115
- RIP 120
- EIGRP (external) 170
- BGP (internal) 200
- Unusable 255

NTP & Time Commands:

- ntp server 192.168.0.1 version 4 (*configures NTP server functionality to lean on this IP address*)
- show ntp status (*shows the NTP client status*)
- show ntp associations (*shows which NTP peers are using the NTP relay at the moment*)
- ntp master (*turns on the integrated NTP server on a router*)
- ntp master 3 *(turns on the integrated NTP server on a router and sets it's stratum level to 3)*
- ntp source 192.168.55.1 *(sets the NTP client to using 192.168.55.1 as its time source)*
- clock timezone CST -6 *(tells the Cisco device to use CST time, -6 below GMT)*
- clock summertime CDT recurring *(tells the Cisco device to configure daylight savings time automatically)*
- show clock *(lists the current date and time, per the local device)*

Logging Commands:

- logging console *(enables logging to the console for debug/info messages)*
- logging monitor *(enables logging to VTY sessions for debug/info messages)*
- logging buffered *(enables logging to an internal buffer)*
- logging host 192.168.55.1 *(enables logging to the syslog server with IP address 192.168.55.1)*
- logging console 5 *(sets the log message level to 5 for console output)*
- logging monitor 5 *(" ")*
- logging buffered 5 *(" ")*
- logging trap 5 *(sets the logging level for SNMP traps sent to the syslog server)*
- service sequence-numbers *(changes the default logging method of timestamping to using sequence numbers instead)*
- show logging *(shows the current logging configuration)*
- terminal monitor *(toggles the receipt of log messages on VTY sessions on or off per user, not globally)*

Licensing Commands:

- show license *(displays the licensed features running in your IOS, line item-style)*
- show license feature *(more specific variant of the command mentioned prior)*
- show license udi *(displays the UDI of the Cisco device)*
- license install http://license.cisco.com/config/key/123456.bin *(installs the license located at the link specified)*
- license boot module c2900 technology-package securityk9 *(adds the 'securityk9' right-to-use license to the device)*

CDP/LLDP Commands:

- show cdp neighbors (*shows neighboring CDP devices)*
- show cdp neighbors detail (*shows detailed information about neighboring CDP devices, including IP address*)
- show cdp interface (*shows whether CDP is enabled on each interface*)
- show cdp entry Cisco2960S *(displays CDP information for the neighboring device named 'Cisco2960S')*
- show cdp *(shows whether the CDP protocol is enabled globally and what timers are set to)*
- show cdp traffic *(shows global statistics for CDP and number of packets sent)*
- show lldp neighbors (*shows neighboring LLDP devices)*
- show lldp neighbors detail (*shows detailed information about neighboring LLDP devices, including IP address*)
- show lldp interface (*shows whether LLDP is enabled on each interface*)
- show lldp entry Cisco2960S *(displays LLDP information for the neighboring device named 'Cisco2960S')*
- show lldp *(shows whether the LLDP protocol is enabled globally and what timers are set to)*
- show lldp traffic *(shows global statistics for LLDP and number of packets sent)*
- no cdp enable *(interface-level command that turns off CDP for a specific interface*)
- cdp run *(global command that enables or disables CDP across the entire device)*
- lldp run *(global command that enables or disables LLDP across the entire device)*
- lldp transmit *(interface-level command that enables or disables the transmission of LLDP messages)*
- lldp receive *(interface-level command that enables or disables the reception of LLDP messages)*

Filesystem & Boot Management Commands:

- config-register 0x2102 *(sets the config register variable to the password recovery setting)*
- boot system usbflash:/c2960_universalk9_12.2.5.bin *(tells the system to boot from the file specified)*
- boot system tftp c2960_universalk9_12.2.5.bin 192.168.105.1 *(tells the system to boot from the file specified on TFTP server 192.168.105.1)*
- boot system flash flash:/c2960_universalk9_12.2.5.bin *(tells the system to boot from the file specified in flash)*
- archive *(global command that moves the user into archive mode)*
- write-memory *(archive mode command that causes the config to be archived every time it is saved to startup-config)*
- time-period 1440 *(archive mode commandspecifies the time in minutes to automatically back up the config to archive, 1440 in this case)*
- path tftp://192.168.100.1/Cisco2960/ *(archive mode command that specifies the path, in either FTP or TFTP, that the configs are saved to)*
- ip ftp username cisco *(global command that specifies the FTP username for the archive storage)*
- ip ftp password cisco *(global command that specifies the FTP password for the archive storage)*
- reload *(reboots the Cisco device)*
- copy flash:/Cisco.bin flash:/Cisco.bkp *(copy command that functions the same as in Linux)*
- show flash *(displays the contents of the flash filesystem)*
- setup *(enters the initial Cisco setup mode)*
- dir flash:/ *(dir command that functions the same as in Windows)*
- archive config *(manually forces the router to make an archive right now)*
- verify /md5 flash:/Cisco.bin $1$5inasf51db35sdb8a35 *(verifies the file specified against the MD5 hash declared)*