Basic Router/Switch IOS commands:

Interface Configuration:

Router(config)#default int range fa 0/0 - 1 !(to clear all int config back to default)!(space b/w fa and -)
Router(config)#default int range fa 0/0 – 1, fa 0/4 - 5
Router(config)#int fa 0/0
Router(config-if)#mac-address 0000.1111.1111 !(hard code a mac address for ease of use)
Router(config-if)#ip address 192.168.1.1 255.255.255.0

Basic switch/router setup commands:

SW#setup
Switch(config)# hostname SW1
SW1(config)# enable secret cisco !(MD5 hash)
SW1(config)# enable password notcisco !(Clear text)
SW1(config)# line con 0
SW1(config-line)# password cisco
SW1(config-line)# login
SW1(config)# line vty 0 4
SW1(config-line)# password cisco
SW1(config-line)# login
SW1(config)# service password-encryption !(to encrypt all the password in the config)
SW1(config)# banner motd $
-=-
UNAUTHORIZED ACCESS IS PROHIBITED
-=-
$
SW1(config)# interface vlan 1
SW1(config-if)# ip address 172.16.1.11 255.255.255.0 !(or DHCP)
SW1(config-if)# no shutdown
SW1(config)# ip default-gateway 172.16.1.1
SW1# copy running-config startup-config
SW1# wr
SW1(config)# no ip domain-lookup
SW1(config)# line vty 0 4
SW1(config-line)# exec-timeout 0 0
SW1(config-line)# logging synchronous

Description, mdix speed and duplex:

SW1(config)# interface fastEthernet 0/1
SW1(config-if)# description LINK TO INTERNET ROUTER
SW1(config-if)# speed 100 !(Options: 10, 100, auto)
SW1(config)# interface range fastEthernet 0/5 - 10
SW1(config-if-range)# duplex full !(options: half, full, auto)
SW1(config-if)# mdix auto
SW1(config-if)# no mdix auto

Using ACL with a debug command for tshoot:

R#access-list 1 permit host 10.0.0.2
R#debug ip packet 1 detail

Configuring switch/router to use SSH:

SW1(config)# ip domain-name example.com
SW1(config)# username admin password cisco
SW1(config)# crypto key generate rsa
How many bits in the modulus [512]: 1024

SW1(config)# ip ssh version 2
SW1(config)# line vty 0 4
SW1(config-line)# login local
SW1(config-line)# transport input telnet ssh

Password recovery:

(0x2142: skip startup config / 0x2102: normal boot process)

1. Press Ctrl+Break while router is powering up for router to go into ROMmon.
2. rommon 1>confreg 0x2142 and rommon 1>reset
3. no to the initial setup script
4. R1#copy start run
5. R1(config)#enable secret cisco
6. R1(config)#config-register 0x2102 !(default is 0x2102 i.e. reads the startup config from nvram)
7. R1#copy run start

To boot your router from the flash device:

R1(config)#boot system flash c3640-i-mz.120-7.T.bin

To boot the system from the TFTP server:

R1(config)#boot system tftp://192.168.1.1/IOS/3640/c3640-is-mz.120-7.T.bin

CCP (Cisco Configuration Professional) pre-config:

R6(config)#ip http server
R6(config)#ip http secure-server
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R6(config)#ip http authentication local
R6(config)#username user1 privilege 15 password cisco
R6(config)#interface fastEthernet 0/0
R6(config-if)#ip address 20.0.0.1 255.0.0.0
R6(config-if)#no shutdown

Resetting switch config (Factory Default):

Reset Catalyst Switches Running CatOS:

Cat5k> (enable) clear config all

Reset Catalyst Switches Running Cisco IOS Software:

Cat2950# write erase
Erasing the nvram filesystem will remove all files! Continue? [confirm]y[OK]
Erase of nvram: complete
Cat2950# reload

Reset VLAN Information:

Cat2950# delete flash:vlan.dat
Cat2950# reload

Backup and restore:

!(Flash(IOS)/RAM(Running config)/NVRAM(Startup config)/HTTP/FTP/TFTP)

Backup IOS from the flash:

Router#copy flash tftp:
Source filename []? c1841-advipservicesk9-mz.124-15.T1.bin
Address or name of remote host []? 192.168.2.2
Destination filename [c1841-advipservicesk9-mz.124-15.T1.bin]?
Writing c1841-advipservicesk9-mz.124-15.T1.bin...!!!!!!!!!!!!!!!!!!!!!!!!![OK - 33591768 bytes]
33591768 bytes copied in 0.554 secs (6366420 bytes/sec)

Restoring the IOS from ROMmon:

!(if IOS is corrupted and the router goes to ROMmon)
rommon 1 > IP_ADDRESS=192.168.2.1
rommon 2 > IP_SUBNET_MASK=255.255.255.0

rommon 3 > DEFAULT_GATEWAY=192.168.2.2
rommon 4 > TFTP_SERVER=192.168.2.2
rommon 5 > TFTP_FILE=c1841-advipservicesk9-mz.124-15.T1.bin
rommon 6 > TFTP_CHACKSUM=0
rommon 7 > tftpdnld
!(yes to continue)
rommon 10 > reset

Backup Running or Startup config to tftp:
R1#copy run start
R1#copy startup-config tftp
Address or name of remote host []? 1.0.0.2
Destination filename [R1-confg]? R1-config
Writing startup-config...!!
[OK - 552 bytes]
552 bytes copied in 0.001 secs (552000 bytes/sec)

Restore config from tftp to Running or Startup config:
!(when you do it to running config it merges so better do it to startup config and reload)
Router#copy tftp running-config
Address or name of remote host []? 1.0.0.2
Source filename []? R1-config
Destination filename [running-config]?
Accessing tftp://1.0.0.2/R1-config....
Loading R1-config from 1.0.0.2: !
[OK - 552 bytes]
552 bytes copied in 3.003 secs (183 bytes/sec)

Static and Default Routes:
Static Route:
R(config)#ip route <destination network> <subnet-mask> <next hop address>
Headquarters(config)#ip route 2.2.2.0 255.255.255.0 192.168.12.2
Default Route:
R(config)#ip route 0.0.0.0 0.0.0.0 <next hop address>
Headquarters(config)#ip route 0.0.0.0 0.0.0.0 1.2.3.1

Port-Security:
SW(config)#interface fa0/1
SW(config-if)#switchport mode access !(works only on access ports not on dynamic interfaces)
!(it can be configured on a trunk port, but not a good idea as the max MACs need to be set)

SW(config-if)#switchport port-security !(turn ON port security)
SW(config-if)#switchport port-security violation shutdown !(options: shutdown | protect | restrict)!(default is shutdown)
SW(config-if)#switchport port-security maximum 1 !(allows max 1 MAC address on the port)!(default max is 1)
!(you might need max 2 MAC allowed if PC connected to Iphone and Iphone connected to switch)
SW(config-if)#switchport port-security mac-address aaaa.bbbb.cccc !(can hard code the allowed MAC)
OR
SW(config-if)#switchport port-security mac-address sticky !(or to get the MACs the switch sees instead of manually adding them, based on max MACs value set)

To bring the port manually up when it is in err-disable state, otherwise it will stay in it forever:
SW(config)#interface fa0/1
SW(config-if)#shutdown
SW(config-if)#no shutdown
To automatically bring the port up when it is in err-disable state:
SW(config)#errdisable recovery cause psecure-violation !(only when port security violation occurs)
SW(config)#interface fa0/1
SW(config-if)#switchport port-security aging time 10 !(in mins)!(default is 5 mins)

VLANs:

VLAN Creation:
!(this creates mac-address-table and stp instance straight away)
Switch(config)# vlan 100
Switch(config-vlan)# name Engineering
!(This method is the only way to configure extended range VLANs as opposed to database mode)
!(Normal VLAN 1-1005. Extended VLAN(1006-4094) transparent mode or V3.Internal 1002-1005)
VLAN database mode (is being deprecated):
Switch#vlan database
Switch(vlan)#vlan 4 name sales
Switch(vlan)#apply
Switch(vlan)#exit
Access Port Configuration (Assigning a port to an access VLAN):
Switch(config-if)# switchport mode access !(can belong only to one VLAN. Will not send DTP)
!(It is good security measure to disable DTP/trunk negotiation on unused ports)
Switch(config-if)# switchport access vlan 100
Switch(config-if)# switchport voice vlan 150 !(options: vlan-id | dot1p | untagged | none)
!(You can configure the switch port, which is connected to an IP Phone, to use one VLAN for voice traffic and another VLAN for data traffic originating from a device that is connected to the access port of the IP Phone)
Trunk (tagged) Port Configuration:
!(Trunk port can be connected to a server, switch or a router)
Switch(config-if)# switchport trunk encapsulation dot1q !(do this first before making it a trunk)
OR
Switch(config-if)# switchport trunk encapsulation isl !(not all switches support this anymore)
Switch(config-if)# switchport mode trunk !(transmits DTP messages as courtesy)
Switch(config-if)# switchport nonegotiate !(will not send DTP messages even it is a trunk port)
Switch(config-if)# switchport trunk native vlan 10
!(it is a good security measure to change the native vlan to something other than VLAN 1)
Allowed VLANs on the trunk:
Switch(config-if)# switchport trunk allowed vlan 10,20-30 !(these are the only allowed. Careful!)
Switch(config-if)#switchport trunk allowed vlan remove 1- 4094
Switch(config-if)#switchport trunk allowed vlan add 1-50 !(adds to the previous ones)
Switch(config-if)#switchport trunk allowed vlan none
Switch(config-if)#switchport trunk allowed vlan all !(default so won't see in show run)
Trunk Negotiation (DTP Negotiation):
1. dynamic auto and dynamic desirable.
Switch(config-if)#switchport mode dynamic auto
OR
Switch(config-if)#switchport mode dynamic desirable

VTP:

Switch(config)# vtp mode server !(options: server | client | transparent)
Switch(config)# vtp domain CBTNuggets
Switch(config)# vtp password MyPassword !(must be the same on all the switches)
Switch(config)# vtp v2-mode !(options: 1 | 2 | 3)
OR
Switch(config)# vtp version 2 !(options: 1 | 2 | 3) !(must be the same on all the switches)
VTP version3:
Switch(config)#vtp domain CBT
Switch(config)# vtp mode server
Switch(config)#vtp version 3
Switch(config)#vtp primary !(this will be the only one to make changes and advertise)
Switch(config)#vtp password cisco hidden !(hashed password, more like service password)
Switch(config)#vtp password <32 chars length hash> secret
VTP Pruning (Dynamic Pruning) (VLAN 2 - 1001 prune eligible):
Switch(config)# vtp pruning !(send VTP prune message and not VTP Join message)
Switch(config-if)#switchport trunk pruning vlan remove 4,20-30 !(Removes VLANs 4 and 20-30)
Switch(config-if)#switchport trunk pruning vlan except 40-50 !(All VLANs are added to the pruning list except for 40-50)

InterVLAN Routing (Router-on-a-stick) (each sub-interface share the same mac address):
Switch(config)#int fa0/3
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20
R1(config)#interface fastEthernet 0/0
R1(config-if)#no shutdown
R1(config)#interface fastEthernet 0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 192.168.10.254 255.255.255.0
R1(config)#interface fastEthernet 0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 192.168.20.254 255.255.255.0

SVI(Switch Virtual Interface)/Inter-VLAN Routing/L3 Switching/MultiLayer Switch Config:
!(SVI (Using MultiLayer Switch for routing) (each SVI interface has different a mac address))
!(Logical layer3 VLAN interface (Switch routing capabilities. Config SVI for each VLAN and put an IP address on it, used by computers as their default gateway))
Switch(config)#ip routing
Switch(config)#int vlan 10
Switch(config-if)#no shut
Switch(config-if)#ip address 192.168.10.254 255.255.255.0
Switch(config)#int vlan 20
Switch(config-if)#no shut
Switch(config-if)#ip address 192.168.20.254 255.255.255.0

PPP(Point to Point Protocol) and HDLC (High-Level Data Link Control):
R1(config)#interface serial 0/0
R1(config-if)#encapsulation ppp !(options: ppp | hdlc)
!(same config on the other end)
R1(config)#interface serial 0/0
R1(config-if)#ip address 192.168.12.1 255.255.255.0
R1(config-if)#clock rate 64000 !(ISP DCE side)

R1(config-if)#no shut
!(same and opposite IP config on the other end)
R1(config)#username Skull password MYSECRET
!(same and opposite config on the other end)
R1(config)#interface serial 0/0
R1(config-if)#ppp authentication chap

CDP (Cisco Discovery Protocol)/LLDP (Link Local Discover Protocol):
!(CDP is enabled by default on cisco devices, but LLDP is not)
R(config)#cdp run
R(config)#cdp timer 5 !(5 secs instead of default 60 secs)
R(config)#cdp holdtime 35 !(35 secs instead of default 180 secs)
R(config)#no cdp run
R(config-if)#cdp enable
R(config-if)#no cdp run !(turn it off on ports it is not needed | security measure)
!(lldp has same commands as cdp, just use lldp instead of cdp in the same commands)
R(config)#lldp run
R(config-if)#lldp receive !(receive only)
R(config-if)#lldp transmit !(transmit only)
R(config-if)#no lldp receive
R(config-if)#no lldp transmit

STP:
!(STP(802.1d)/PVST+/RSTP(802.1w)/RPVST/MST)
!([BPDU:BridgePriority(32768)+MAC])
!(STP: RootPorts->DesignatedPorts->BlockingPorts)
!(All RootBridgePorts are DP and One DP per link)
!(ElectRoot->RootPorts(LowestCost/LowestBrdigeID/LowestPortNumber)->BlockTheRest)
!(Costs: 100Mbps=19/1Gbps=4/10Gbps=2)
!(STP Timers:Block20sec/Listen15sec/Learn15sec/Forward)
!(RSTP: RootPorts->DesignatedPorts->AlternatePorts)
Change BPDU default timers:
SwitchA(config)#spanning-tree vlan 10 hello-time 1 !(1sec/default 2sec)
SwitchB(config)#spanning-tree vlan 20 max-age 6 !(6sec/default 20sec)
SwitchC(config)#spanning-tree vlan 30 forward-time 4 !(4sec/default 15sec)
Change Root bridge:
SwitchA(config)#spanning-tree vlan 1 root primary !(hard code a root bridge)
!(This is a macro that looks at the current priority of the root bridge and changes your running-config to lower your own priority. Based on VLAN number)
OR
SwitchA(config)#spanning-tree vlan 1 priority 4096 !(hard code priority. multiple of 4096)
Change Root Port/Non-Designated Port:
SwitchB(config)#interface fa0/14
SwitchB(config-if)#spanning-tree cost 500
!(can be used to change the cost of root port to get a different root port chosen)
OR
SwitchA(config)#interface fa0/14
SwitchA(config-if)#spanning-tree port-priority 16
!(can be used to change the port priority to get a different root port chosen)
PortFast:
!(To avoid spanning tree calculations and disable STP for connections to PCs)

SwitchB(config)interface fa0/2
SwitchB(config-if)#spanning-tree portfast !(configured on access ports)
SwitchB(config)#spanning-tree portfast default !(can be enabled globally for all access mode ports)
Enable Rapid-PVST:
SwitchA(config)#spanning-tree mode rapid-pvst !(to enable rapid spanning-tree protocol)

ACLs:

Standard Access List:
!(Standard Access List close to the destination are best)
R1(config)#access-list 1 permit 10.0.0.0 0.255.255.255
R1(config)#access-list 1 deny host 10.0.0.1 log
R1(config)#access-list 1 permit any any !(don't forget this as there is a default deny at the end)
Extended Access list:
!(Extended Access lists closer to the source are best)
R1(config)#access-list 101 permit tcp 10.0.0.0 0.255.255.255 187.100.1.6 0.0.0.0 eq 20
!(187.100.1.6 0.0.0.0 is the same as host 187.100.1.6)
R1(config)#access-list 101 deny tcp any eq 22 host 10.0.0.1 range 22 23
R1(config)#access-list 101 permit ip any any dscp cs2
Apply this ACL to an interface:
R1(config)#interface Fa0/1
R1(config-if)#ip access-group 1 out
OR
R1(config)#interface Fa0/0
R1(config-if)#ip access-group 1 in
Named ACLs:
R(config)#ip access-list extended MyACL
R(config-ext-nacl)#100 permit ip host 1.1.1.1 any
Edit and Insert Lines in ACLs:
R(config)#ip access-list extended MyACL
R(config-ext-nacl)#no 500
R(config-ext-nacl)#500 permit ip any host 5.5.5.5
R(config-ext-nacl)#510 permit ip any host 6.6.6.6
Time-based ACLs:
R(config)#time-range TR_WORKDAYS
R(config-time-range)#periodic weekdays 08:00 to 19:00
!(Don't configure NTP unless mentioned in the LAB)
R(config)#ip access-list extended 100
R(config-ext-nacl)#27 permit tcp any any eq www time-range TR_WORKDAYS
Block pings with acls:
access-list 100 deny icmp any any echo
access-list 100 deny icmp any any echo-reply
access-list 100 permit ip any any
OR
access-list 101 deny icmp host 192.168.1.51 host 192.168.1.34 echo
access-list 100 permit ip any any
ACL log keyword:
R1(config)# ip access-list extended Block_SSH
R1(config-ext-nacl)# no 10
R1(config-ext-nacl)# 10 deny tcp any any eq 22 log

NAT:

Define the traffic to match:

R(config)#access-list 10 permit 10.0.0.0 0.0.255.255 !(ACL to match)
Static NAT: (Note: two way NAT. Just like a port-forward so be careful)
R(config)#ip nat inside source static 10.0.0.19 192.0.2.1
OR
R(config)#ip nat outside source static 192.0.2.1 10.0.0.19
R(config)#ip nat inside source static tcp 10.0.0.3 80 192.0.2.1 80
R(config)#ip nat inside source static tcp 10.0.0.3 443 192.0.2.1 443
Dynamic NAT:
R(config)#ip nat pool MyPool 192.0.2.1 192.0.2.254 prefix-length 24 !(Public IP pools)
R(config)#ip nat inside source list 10 pool MyPool !(actual NAT rule)
R(config)#ip nat inside source static 10.0.0.42 192.0.2.42 !(can be combined with static)
PAT:
R(config)#ip nat inside source static tcp 10.0.0.3 80 192.0.2.1 80
R(config)#ip nat inside source static tcp 10.0.0.3 443 192.0.2.1 443
R(config)#ip nat inside source static tcp 10.0.0.10 3389 192.0.2.1 3389
R(config)#ip nat inside source static tcp 10.0.0.11 3389 192.0.2.1 3390
R(config)#ip nat inside source list 10 pool MyPool overload
OR
R(config)#ip nat inside source list 10 interface FastEthernet 0/0 overload
Identify interfaces: (Note: should be the last step, especially in a production network)
R(config)#int fa0/0
R(config-if)#ip address dhcp !(ISP assigned IP for external interface)
R(config-if)#ip nat outside
R(config)#int fa0/1
R(config-if)#ip address 192.168.1.1
R(config-if)#ip nat nat inside

Syslog (splunk/kiwi)(port udp 514):
Router(config)#ntp server pool.ntp.org
Router(config)#no service timestamps !(you can disable timestamps and use sequence numbers)
Router(config)#service sequence-numbers
Router(config)#logging console errors !(severity level 3 and lower)
!(This logging information is saved in the RAM of your device. Once you reboot it you will lose this logging history)
Router(config)#terminal monitor !(if you want to see syslog messages on vty sessiosn when your on vty)
Router(config)#logging buffered 4096 !(buffer size in bytes)
Router(config)#logging 192.168.1.100 !(all logging sent to the syslog server except level 7)
Router(config)#logging trap 7 !(this will sent also the debug info to the syslog server)

R1(config)# logging host 192.168.1.25
R1(config)# logging source-interface Loopback0
R1(config)# logging trap notifications
R1(config)# no logging console

NTP:
Clock commands:
R1# clock set 14:12:00 10 feb 2005
R1(config)# clock timezone ARIZONA -7
R1# show clock
NTP config:
R1(config)# ntp server 1.gr.pool.ntp.org

Use the router as an NTP server:
R1(config)# ntp master

SNMP:
Router(config)#snmp-server community MY_STRING ro 10 !(options: ro | rw)
Router(config)#access-list 10 permit host 192.168.1.2
Router(config)#snmp-server location Amsterdam
Router(config)#snmp-server contact info@gns3vault.com

Netflow:
Router(config)#interface fastEthernet 0/0 !(the direction to monitor)
Router(config-if)#ip flow ingress
Router(config-if)#ip flow egress
Router(config)#ip flow-export version 9 !(netflow version)
Router(config)#ip flow-export destination 192.168.1.2 100 !(netflow collector)

DHCP:
R1(config)# service dhcp
R1(config)# ip dhcp pool NET-POOL
R1(dhcp-config)# network 192.168.1.0 255.255.255.0 !(you can use prefix notation with it)
R1(dhcp-config)# default-router 192.168.1.1
R1(dhcp-config)# dns-server 8.8.8.8 8.8.4.4
R1(dhcp-config)# domain-name company1.com
R1(dhcp-config)# lease 9 !(9 days/default is 1 day)
OR
R1(dhcp-config)# lease 0 4 30 !(set the lease time for 4 hours and 30 minutes)
R1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.5
R1(config)# ip dhcp excluded-address 192.168.1.10
Cisco DHCP Option 150 Configuration:
R1(config)# ip dhcp pool NET-POOL
R1(dhcp-config)# option 150 ip 10.10.22.99 10.10.22.100 !(Configure 2 IPs)

DHCP Snooping and DAI (Dynamic ARP Inspection):
SwitchA(config)#ip dhcp snooping !(enable globally)
SwitchA(config)#no ip dhcp snooping information option
!(By default the switch will add option 82 to the DHCP discover message before passing it along to the DHCP server. Some DHCP servers don't like this and will drop the packet. If you client doesn't get an IP address anymore after enabling DHCP snooping globally you should use the above command)
SwitchA(config)#ip dhcp snooping vlan 1 !(select vlan for which you want dhcp snooping)
!(dhcp snooping needs to be enabled for dynamic arp inspection)
SwitchA(config)#ip arp inspection vlan 1 !(DAI needs to be enabled per VLAN)
SwitchA(config)#interface fa0/2
SwitchA(config-if)#ip dhcp snooping trust !(this will be connected to the actual DHCP server)
SwitchA(config)#interface fa0/1
SwitchA(config-if)#ip dhcp snooping limit rate 10 !(10 packets per sec)
!(ideal to rate limit all the ports for DHCP packets except the DHCP server interface)
SwitchA(config)#interface fa0/1
SwitchA(config-if)#ip arp inspection limit rate 10

RIP:

!(Distance Vector(DV): 1. Max Distance (16 hops)/2.RoutePoison/3.TriggeredUpdates/4.SplitHorizon/5.HoldDownTimers)
R1(config)#router rip
R1(config-router)#network 192.168.12.0 !(network command tells what network to advertise and what interfaces to send advertisements out)
R1(config-router)#network 172.16.1.0
R1(config-router)#version 2
R1(config-router)#no auto-summary
R2(config)#router rip
R2(config-router)#network 192.168.12.0
R2(config-router)#network 192.168.23.0
R2(config-router)#version 2
R2(config-router)#no auto-summary
R3(config)#router rip
R3(config-router)#network 172.16.0.0
R3(config-router)#network 192.168.23.0
R3(config-router)#version 2
R3(config-router)#no auto-summary

FHRP (First Hop Redundancy Protocols):

!(Virtual IP and Virtual MAC)

HSRP(Hot Standby Routing Protocol):

!(Hello 3sec/Hold 10sec)
!(Active-Standby)
SwitchA(config)#interface fa0/17 !(internal interface)
SwitchA(config-if)#no switchport
SwitchA(config-if)#ip address 192.168.1.1 255.255.255.0
SwitchA(config)#interface fa0/19 !(external interface)
SwitchA(config-if)#no switchport
SwitchA(config-if)#ip address 192.168.14.1 255.255.255.0
SwitchA(config)#ip routing
SwitchA(config)#ip route 0.0.0.0 0.0.0.0 192.168.14.4
SwitchA(config)#interface fa0/17
SwitchA(config-if)#standby 1 ip 192.168.1.3 !(create a standby group and assign an IP)
!(Same and opposite config on SwitchB)
!(PC is configured with a default gateway of 192.168.1.3 i.e. Virtual Gateway's IP)
!(HSRPv1 uses the 0000.0c07.acXX MAC address where XX is the HSRP group number e.g. 0000.0c07.ac01 for group 1)(HSRPv2 uses 0000.0C9F.FXXX MAC)
!(By default the switch with the highest priority will become the active HSRP device. If the priority is the same then the highest IP address)
SwitchA(config)#interface fa0/17
SwitchA(config-if)#standby 1 priority 150 !(default priority is 100)
SwitchA(config-if)#standby 1 preempt !(could become active if router goes down & then up)
SwitchA(config-if)#standby 1 preempt delay minimum 60
OR
SwitchA(config-if)#standby 1 preempt delay reload 60 !(If a router reboots it might need some time to “converge”)
SwitchA(config-if)#standby 1 mac-address 0000.1111.5555 !(instead of using default hsrp MAC)
SwitchA(config-if)#standby 1 version 2 !(version must be same on both devices)
SwitchA(config-if)#standby 1 name my-hsrp-name !(name of the group for ease)
SwitchA(config-if)#standby 1 authentication md5 key-string md5pass !(prevent rogue hsrp router)

!(can also use a key chain the same way you would use in eigrp or anywhere else)
SwitchA(config-if)#standby 1 timers msec 100 msec 300 !(default hello 3 secs & hold 10 secs)

Interface tracking (object tracking):

1. Select an interface to track and if it fails decrease the priority so that another device can become the active router. Tracking checks the line protocol status, but can also be configured to check if the route exists or with SLA probes.

SwitchA(config)#interface fa0/17 !(internal interface)
SwitchA(config-if)#standby 1 preempt !(preemption is imp otherwise tracking is useless)
SwitchB(config)#interface fa0/19 !(internal interface)
SwitchB(config-if)#standby 1 preempt !(preemption is imp otherwise tracking is useless)
SwitchA(config-if)#standby 1 track fastEthernet 0/19 !(external interface)
SwitchA(config)#interface fa0/19
SwitchA(config-if)#shutdown
!(Verify)
SwitchA#show standby | include Priority
Priority 140 (configured 150) !(by default decrements the priority by 10)
SwitchA(config)#interface fa0/17
SwitchA(config-if)#standby 1 track fastEthernet 0/19 60
OR
SwitchA(config-if)#standby 1 track 1 decrement 60
!(If the links goes down again the priority will become 90 reducing it by 60 so the other device with default priority 100 will then become active)
!(Interface tracking will only check the state of any interface not if anything fails upstream)

IP SLA with object tracking:

!(IP SLA can be used for many things. One of them is to generate a ping to a destination every X seconds and we can combine this with object tracking)
SwitchA(config)#interface fa0/17
SwitchA(config-if)#no standby 1 track fastEthernet 0/19 60
SwitchA(config)#ip sla 1
SwitchA(config-ip-sla)#icmp-echo 192.168.14.4
SwitchA(config)#ip sla schedule 1 start-time now life forever
SwitchA(config)#track 1 rtr 1 reachability
SwitchA(config)#interface fa0/19
SwitchA(config-if)#standby 1 track 1 decrement 60
!(Test)
RouterA(config)#interface fa0/13
RouterA(config-if)#shutdown

VRRP (Virtual Router Redundancy Protocol):

!(Hello 1sec/Hold 3sec)
!(Master-Backup)
1. Exactly same config as HSRP except we use vrrp instead of standby
2. VRRP uses the 0000.5e00.01XX MAC address where XX is the VRRP group number.
3. VRRP can have the same IP as that of the real interface as opposed to HSRP. The device that has got the real IP as the virtual IP becomes the master, priority is not looked at then because the priority of the master is set to the highest value of 255.

GLBP (Gateway Load Balancing Protocol):

!(Hello 3sec/Hold 10sec)
!(Active-Active Load Balancing)
!(AVG(Active Virtual Gateway)(Manager: Generates MACs for AVFs) and AVF(Active Virtual Forwarder))
R1(config)#interface fa1/0
R1(config-if)#glbp 1 ip 192.168.1.3

R1(config-if)#glbp 1 preempt
R1(config-if)#glbp 1 authentication md5 key-string mypass
!(Same and opposite config on SwitchB)
R1(config-if)#glbp 1 priority 150
!(The virtual MAC address that GLBP uses is 0007.b400.XXYY (where X = GLBP group number and Y = AVF number))

GLBP interface tracking:

!(Interface tracking works differently for GLBP compared to HSRP or VRRP. It has a weighting mechanism whic is used to determine if a device can be AVF or not)
SwitchB#show glbp | include Weighting
Weighting 100 (default 100)
SwitchB(config)#track 16 interface fastEthernet 0/16 line-protocol
SwitchB(config)#track 17 interface fastEthernet 0/17 line-protocol
SwitchB(config)#interface fa0/19
SwitchB(config-if)#glbp 1 weighting track 16 decrement 20
SwitchB(config-if)#glbp 1 weighting track 17 decrement 20
SwitchB(config-if)#glbp 1 weighting 100 lower 70 upper 90
!(Verify)
SwitchB#show glbp | include Weighting
Weighting 100 (configured 100), thresholds: lower 70, upper 90
!(Test and verify)
!(Now shutdown int fa0/16)
!(Weighting 80 (configured 100), thresholds: lower 70, upper 90)
!(Now shutdown int fa0/17)
!(Weighting 60, low (configured 100), thresholds: lower 70, upper 90)
!(Now 'no shutdown' int fa0/16
!(Weighting 80, low (configured 100), thresholds: lower 70, upper 90)
!(Now 'no shutdown' int fa0/17)
!(Weighting 100, low (configured 100), thresholds: lower 70, upper 90)

GLBP weighted Load-Balancing:

!(default I round-robin. If you have a beefier router you can use weighted load-balancing)
!(configured on AVG)
SwitchB(config)#interface fa0/19
SwitchB(config-if)#glbp 1 load-balancing weighted
SwitchB(config-if)#glbp 1 weighting 200 !(this switch will have double the traffic going through)

EIGRP:

!(BackupRoutes(FastConvergence/DUAL)/FelxibleSummrization/UnequalCostLB)
!(NeighbourTable(OnlyNeighbours)/TopologyTable(LearnedFromneighbours)/RoutingTable(Best))
(FeasibleDistance(HowFarFromYou)/AdvertisedDistance(HowFarFromNeighbour)/Successor(RoutingTable)/FeasibleSuccessor(TopologyTable)/ActiveRoute(ActivelySearching)/PassiveRoute)
!(To be a Feasible Successor, the AD must be less than the FD of the Successor)
!(Hello/Update/Query/Reply/Ack)
!(Bandwidth (k1) and Delay (k3) by default/MTU/Load/Reliability)
Metric = bandwidth (slowest link) + delay (sum of delays)
1. Bandwidth: [10^7 / minimum bandwidth in the path] * 256.
2. Delay: sums of delays in the path multiplied by 256 (in tens of microseconds).
So the formula looks like:
Metric = (10^7 / minimum bandwidth) * 256 + (sum of delays) * 256

EIGRP Config:

R1(config)#router eigrp 1 !(1 is AS number)
R1(config-router)#no auto-summary

R1(config-router)#network 1.1.1.0 0.0.0.255
R1(config-router)#network 192.168.12.0
R1(config-router)#exit
R2(config)#router eigrp 1
R2(config-router)#no auto-summary
R2(config-router)#network 2.2.2.0 0.0.0.255
R2(config-router)#network 192.168.12.0

Named EIGRP:

!(Since IOS 15, EIGRP has a new method of configuration called named EIGRP)
R1(config)#router eigrp MY_NAME
R1(config-router)#address-family ipv4 autonomous-system 12
R1(config-router-af)#network 192.168.12.0
R1(config-router-af)#af-interface FastEthernet 0/0

EIGRP Authentication:

R1(config)#key chain MYCHAIN
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string BANANA
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip authentication mode eigrp 1 md5
R1(config-if)#ip authentication key-chain eigrp 1 MYCHAIN

EtherChannel:

!(PagP Modes: On/Desirable/Auto/Off)
!(LACP Modes: On/Active/Passive/Off)

EtherChannel L2 Configuration:

SwitchA(config)#default int range fa0/13 - 14
SwitchA(config)#int range fa0/13 – 14
SwitchA(config-if)#shut
SwitchA(config-if)#channel-group 1 mode desirable !(options(LACP/PAgp): active/desirable,passive/auto, on)
SwitchA(config-if)#no shut
SwitchA(config)#interface port-channel 1
SwitchA(config-if)#switchport trunk encapsulation dot1q
SwitchA(config-if)#switchport mode trunk
!(same config when using LACP except for modes are different)

EtherChannel L3 Configuration:

SW1(config)# interface port-channel 1
SW1(config-if)# no switchport
SW1(config-if)# ip address 172.16.1.11 255.255.255.0
SW1(config)# deafult int range fastethernet0/1 - 2
SW1(config)# int range fastethernet0/1 – 2
SW1(config-if-range)# no switchport
SW1(config-if-range)# no ip address
SW1(config-if-range)# channel-group 1 mode desirable
!(same an opposite config on SW2)

OSPF:

Configuration:

R1(config)#router ospf 1
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0

Protected Ports (Private VLAN Edge):

!(We can ensure ComputerA and ComputerB are unable to communicate with each other by using protected ports. By default all switch ports are unprotected)
!(If someone takes over your ComputerB (Web Server) you can reduce the attack surface by preventing them from connecting to other servers (ComputerA) in your network)
SwitchA(config)#interface fa0/1
SwitchA(config-if)#switchport protected
SwitchA(config)#interface fa0/3
SwitchA(config-if)#switchport protected
!(Test using simple pings)
Protected port <--> Unprotected = working
Protected port <--> Protected port = not working

Private VLANs:
!((Creates a VLAN within a VLAN)(Reduces attack vector))
1. Community VLAN: All ports within the community VLAN are able to communicate with each other and the promiscuous port.
2. Isolated VLAN: All ports within the isolated VLAN are unable to communicate with each other but they can communicate with the promiscuous port.
SwitchA(config)#vtp mode transparent !(Private VLANs work only on vtp transparent mode)
!(vtp version3 can automatically propagate private vlan information across switches)

SwitchA(config)#vlan 501 !(community (secondary) vlan)
SwitchA(config-vlan)#private-vlan community

SwitchA(config)#vlan 502 !(isolated (secondary) vlan)
SwitchA(config-vlan)#private-vlan isolated

SwitchA(config-vlan)#vlan 500 !(primary vlan)
SwitchA(config-vlan)#private-vlan primary
SwitchA(config-vlan)#private-vlan association add 501,502

SwitchA(config)#interface range fa0/1 – 2 !(community (secondary) vlan ports)
SwitchA(config-if-range)#switchport mode private-vlan host
SwitchA(config-if-range)#switchport private-vlan host-association 500 501

SwitchA(config)#interface range fa0/3 – 4 !(isolated (secondary) vlan ports)
SwitchA(config-if-range)#switchport mode private-vlan host
SwitchA(config-if-range)#switchport private-vlan host-association 500 502

SwitchA(config)#interface fa0/24 !(promiscuous port)
SwitchA(config-if)#switchport mode private-vlan promiscuous
SwitchA(config-if)#switchport private-vlan mapping 500 501-502
!(Can be an SVI port: S(config)#int vlan 500 and S(config-if)#private-vlan mapping 501,300)

CCNA Voice:
Voice port config on the Switch:
Switch(config)#int range fa0/1-4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 50
Switch(config-if-range)#switchport voice vlan 10

CME/CUCME (Cisco Unified Call Manager Express)/CIPC(Cisco IP Communicator)(Soft IP

Phone):
1. telephony-service is a global configuration place telephony services.
2. ephones manages the phones.
3. ephone-dn manages the ephone numbers.
4. dial-peers manages the phone directory (route plan).

Create all the phone numbers:

```
Router(config)#ephone-dn 20 dual-line    !(could be single line or dual line)
Router(config-ephone-dn)#number 5308 secondary 8675308
Router(config)#ephone-dn 30 dual-line
Router(config-ephone-dn)#number 5309 secondary 8675309
```

Creating an actual phone and associate the number:

```
Router(config) # ephone 20
Router(config-ephone)# mac-address AAAA.BBBB.CCCC
Router(config-ephone)# type 7960 addon 1 7914
Router(config-ephone)# button 1:20 2:30 !(assocaiate button to the ephone-dn)
Router(config-ephone)#restart !(quick restart of the phone after button command)
Router(config-ephone)#reset !(takes longer)
```

sh run | s ephone

CME CCP Config:
1. Enable CME (Configure>Unified Communications>Unified Communications Features)
2. Global Telephony Services (Configure>Unified Communications>Telephony Settings)
3. Create a phone (Configure>Unified Communications>Users, Phones, Extension>Phones)
4. Create an Extension (Configure>Unified Communications>Users, Phones, Extension>Extensions)
5. Create a user and link (Configure>Unified Communications>Users, Phones, Extension>users(User and Phone/Extension tabs))

Converting Spoken Voice to Bits:
1. take samples of the analog signal
2. calculate a number representing each sample (aka Quantization)
3. Convert that number to binary (PCM (Pulse Code Modulation))
4. Compress the signal (optional)

Nyquist: 4000 is highest frequency so double is 8000 (so 8000 samples per second)

CODEC:
G.711(64Kbps) or G.729(8Kbps) or ILBC(15.2kbps)
VAD (Voice Activity Detection)
Audio codec is a computer program implementing an algorithm that compresses and decompresses digital audio data according to a given audio file or streaming media audio coding format. The objective of the algorithm is to represent the high-fidelity audio signal with minimum number of bits while retaining the quality. This can effectively reduce the storage space and the bandwidth required for transmission of the stored audio file.

Dial-peers (pots or voip):

```
Gateway(config)#dial-peer voice 10 pots
Gateway(config-dial-peer)#destinatio-pattern 3301
Gateway(config-dial-peer)#port 1/0/0   !(FXS)
Gateway(config)#dial-peer voice 20 pots
Gateway(config-dialpeer)#destinatio-pattern 3302
Gateway(config-dialpeer)#port 1/0/1   !(FXS)
```

CME_Voice(config)#dial-peer voice 330 voip
CME_Voice(config-dial-peer)#destinatio-pattern 330.
CME_Voice(config-dial-peer)#session target ipv4:10.1.1.2

Gateway(config)#dial-peer voice 10 voip
Gateway(config-dial-peer)#destinatio-pattern 10..
Gateway(config-dial-peer)#session target ipv4:10.1.1.1

sh voice port summary
sh voice call summary
sh dial-peer voice summary
debug voip dialpeer

Setting up CUCM (Cisco Unified Communications Manager)/UCM (Unified Communication Manager i.e. Call Manager):

!(Cisco Unified Communications Manager provides services such as session management, voice, video, messaging, mobility, and web conferencing)

Device Pool:

1. (System>Device Pool) (you need to configure the rest before creating device pool)
2. (System>Cisco Unified CM Group)
3. (System>Date/Time)
4. (System>Region) (usually g.711 is used within the same region and g.729 between regions over the WAN)(so create codec relationships between regions)
5. (System>SRST) Cisco Unified Survivable Remote Site Telephony (SRST)

Adding Phones to CUCM:

1. Device>Phone
2. Type>Protocol(SIP/SCCP):

Configure MAC address, device pool, phone button template and device security profile etc.
Then configure the line of the phone with a number (Directory number config).
[You can auto register System> Cisco Unified CM (select the CM and then auto registration config)
(System>Enterprise Parameters)
(Device>Device defaults)]

User Management:

User management>End User (local database)
(also associate the user to the device)(users can even manage their own phone)

AD connection (LDAP(LightWeight Directory Access Protocol)):

(System>LDAP)
CiscoDir service needs to be active
1. enable LDAP sync (MS AD and sAMAccountName)
2. set LDAP directory
(Use the domain admin user e.g. admin@home.local)
(LDAP query: ou=CCMEndUsers,dc=home,dc=local)
(also set sync timer)
3. set LDAP auth
(Use the domain admin user e.g. admin@home.local)
(LDAP query: ou=CCMEndUsers,dc=home,dc=local)
(AD IP)
!(User management>end user (users will be imported))

UCCX (Unified Contact Center Express):

Cisco Unified Contact Center is part of the Cisco Unified Communications application suite, which

delivers intelligent call routing, network-to-desktop computer telephony integration (CTI), and multichannel contact management to contact center agents over an IP network.

CUPS (Cisco Unified Presence Server):

Unified communications (UC) is a marketing buzzword describing the integration of real-time enterprise communication services such as instant messaging (chat), presence information, voice (including IP telephony), mobility features (including extension mobility and single number reach), audio, web & video conferencing, fixed-mobile convergence (FMC), desktop sharing, data sharing (including web connected electronic interactive whiteboards), call control and speech recognition with non-real-time communication services such as unified messaging (integrated voicemail, e-mail, SMS and fax). UC is not necessarily a single product, but a set of products that provides a consistent unified user interface and user experience across multiple devices and media types.

CUPC (Cisco Unified Personal Communicator):

Cisco Jabber is a unified communications application for PC, Mac, tablet and smartphone. Cisco Jabber client applications provide presence, instant messaging, voice and video, voice messaging, desktop sharing and conferencing capabilities.

Cisco Unity:

Cisco voice mail server (integaretes with Exchange server)

Basic ASA Commands:

IPSec VPN ASA:

IPv6: