Optimum Retiaculum

By James Keller

Background:

This document was made to aid in CyberPatriot but also to be your one stop reference for the best cisco notes ever made. In this document I would like to thank my previous training leads (especially Aidan Brehm, Joe O'Neill, and Nick Jacob). I would also like to thank those who went through Cisco training with me my first three years (Henry Craig, Andrew Alonsozana, and John Villianueva).

The Story Begins:

Enter the CLI and start by typing:
Router(config)#en
Router(config)#conf t
"en" stands for enable and "conf t" stands for configure terminal

This will put you in router config mode, there are also sub config modes and one of the most important, Privileged Exec Mode.

Most router wide commands will be in either User or Privileged EXEC Mode so to bypass having to go from Router config mode you can put "do" in front of your EXEC mode commands.

When starting an image it is best to see the devices starting configuration, to do this use the command
Router(config)# do show run

To save your configuration you can use the command
Router(config)#copy run start
Router(config)#write memory
You can also do:
Router(config)#copy running-config startup-config

The "exit" command will take you back one layer in the device so if you are configuring the terminal it will put you back in Privileged EXEC Mode

Basic Configuration Commands

Changing Hostname
Router(config)#hostname [hostname]

Difference between secret and password
When using a command to configure a password you have two options “password” and “secret”, unless told otherwise you should always use “secret” because it encrypts the password while “password” just displays it in plain text

Configuring a Privileged EXEC Password
Router(config)#enable secret/password [password]

Lines
Lines on cisco devices are physical ports on the router (serial) or virtual (VTY), which you have on a device.

Configuring a Console Password
Router(config) line console 0
Router(config-line)#password/secret [password]
Router(config-line)#login
Router(config-line)#exit

Type of Login
When logging into a router with a remote connection like ssh or telnet, you have two options for login. The command “login” will force you to login with only a password and “login local” will force you to login with a username AND a password.

Configuring SSH
Router(config)#ip domain-name [domain name, if none use cisco.com]
Router(config)#crypto key generate rsa
How many bits in the modulus [512]:
For above message, type 1024 as it is the default for SSH
Router(config)#username [username] password/secret [password]
Sometimes they ask for SSH version 2, to configure this type
Router(config)#ip ssh version 2
SSH configurations will have you apply it on certain VTY lines
Router(config)#line vty [first vty line] [second vty line]
Router(config-line)#transport input ssh
Router(config-line)#login
OR
Router(config-line)#login local

Enabling Encryption Service for Passwords
Router(config)#service password-encryption

Configuring a Banner
Router(config)#banner [login/motd] [message]

Remote Access Failed Logins
Router(config)#login block-for [seconds] attempts [failed attempts] within [seconds]

Setting EXEC Timeout
Router(config)#line vty [First line] [Second Line]
Router(config-line)#exec-tiemeout [Timeout in seconds]

Password Minimum Length
Router(config)service passwords min-length [Minimum Length]

Configuring Interfaces

Types of interfaces
INterfaces are ports on devices and can be virtual. Some examples of this are FastEthernet, GigabitEthernet, VLANs, and sub-interfaces. Most interfaces are in the format Gig0/1, with the letters and numbers changing to match different interfaces.

Accessing Normal Interfaces
Router(config)#int [interface identifier]
Accessing VLANs as an interface
Router(config)#int vlan [vlan number]
Accessing a Range of Interfaces
router(config)# int range [start identifier]-[end identifier]

Turning a Port or Off
Router(config-if)#shutdown
OR
Router(config-if)#no shutdown

Types of ports
The three port types are access, trunk, and dynamic. Access ports are ports where you connect an end device, trunk ports are ports that you connect network devices to (switches and routers) and dynamic ports can switch between the two but are very insecure. (never keep a port as dynamic). Access ports can only support one VLAN while trunk ports can support many.

Configuring a port type
Router(config-if)#switchport mode [access/trunk]

Assigning an IP address on an interface
Router(config)#int [identifier]
Router(config-if)#ip [address] [subnet]

Configuring Port Security
Router/Switch(config)#int [identifier]
Router/Switch(config-if)#switchport port-security
Port Security Options
After enabling port security there are other options you can assign
To log MAC addresses
Router(config-if)#switchport port-security mac-address sticky
To add a maximum number of MAC addresses
Router(config-if)#switchport port-security maximum [max number of MAC addresses]
To configure the result if the max amount of MAC addresses is reached
Router(config-if)#switchport port-security violation [shutdown/restrict/protect]

Subinterfaces
Interfaces can have subinterfaces which are exactly what they seem, divisions of interfaces. You can configure these just like normal with the “interface” command. Subinterfaces are in this format: Gig0/1.99. In this example the “99” is the VLAN ID for the subinterface. You cannot assign IP addresses to them without encapsulating them. You encapsulate them with this command.
Switch(config)#interface [Subinterface Identifier]
Switch(config-subif)#encapsulation dot1q [VLAN ID]
If the VLAN ID is the Native VLAN you do this command instead
Switch(config-subif)#encapsulation dot1q [VLAN ID] native

VLANs

VLANs are divisions of LANs on a switch who cannot talk to each other and are only available on Switches. They are used for security purposes to keep different parts of a network divided. There are two ways to configure VLANs, you can configure it as an interface with
Router(config)#int vlan [VLAN ID]
Or you can configure it as a normal VLAN
Router(config)#vlan [VLAN ID]

Naming VLANs
Switch(config)#vlan [VLAN ID]
Switch(config-vlan)#name [VLAN Name]

Assigning a VLAN to an Access Port(s)
Switch(config)#int {range} [Interface Identifiers(s)]
Switch(config-if)#switchport mode access
Switch(config-if)switchport access vlan [VLAN ID]

Assigning a VLAN to a Trunk Port
Switch(config)#int {range} [Interface Identifiers]
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan [VLAN #],[VLAN#],[VLAN#]

Assigning a Native VLAN to a Port
Switch(config)#int {range} [Interface Identifier(s)]
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan [VLAN ID]

Spanning Tree

What is Spanning Tree?
Spanning tree is a protocol for switches that prevents loops, if you have three switches in a triangular formation the data can end up looping around all three causing the network to slow down and information to not be delivered. For spanning tree, there are root bridges, root ports, designated ports, and blocked ports. The Root bridge will be the switch where all data will be sent so the switches can figure out the best place to send the data. The root switch is decided first by looking at which switch has the lowest Bridge ID #, if two switches have the same Bridge ID # the lowest MAC Address is used as a tie breaker.

Spanning Tree Mode
Switch(config)#spanning-tree mode rapid-pvst

Identifying Root Bridge
Switch(config)#spanning-tree vlan [VLAN-ID] root primary/secondary

STP Priority
Switch(config)#spanning-tree vlan 1 priority [increments of 4096]

STP Port Priority
Switch(config)#int [interface identifier]
Switch(config-if)#spanning-tree vlan [VLAN-ID] port-priority [increments of 16]

PortFast and BPDU Guard (only configure if told so)
Switch(config)#int [interface identifier]
Switch(config-if)#spanning-tree portfast

- Enables ends ports as soon as an intermediary device connects to them

Switch(config-if)#spanning-tree bpduguard enable

- Shuts down if a BPDU (switch info) is received

Switch(config)#spanning-tree portfast default

- Enables BPDU guard for all access ports on a switch

Switch(config)#spanning-tree portfast bpduguard default

Inter-VLAN Routing

If a trunk port on a switch is connected to a router, you will need to make sub-interfaces for each VLAN coming from the switch. You do this by dividing a port into its VLAN ID's. For example, if you have g0/0 and had VLANs 10 and 20, it would be separated into g0/0.10 and g0/0.20. To add an IP address to a subinterface you have to encapsulate it.

Creating SubInterfaces and Assigning IPs
Router(config)#int [interface identifier]
Router(config-subif)#encapsulation dot1q [VLAN ID]
Router(config-subif)#ip address [IP address] [Subnet Mask]

Native Subinterface
Router(config-subif)#encapsulation dot1q [VLAN ID] native

Static Routes

A static route sends traffic bound for one address to a different one (not a hard concept). Think of it like trying to take a road to school but the road is closed so you are redirected to a different way. A common use for a static route is a default route, this says that if a router doesn't know where to send traffic it will send it to another router who might know where the destination is.

Creating a Static Route
Router(config)#ip route [Destination IP] [Destination Subnet Mask] [Next Hop Address]

Creating a Default Route
Router(config)#ip route 0.0.0.0 0.0.0.0 [Next Hop Address to Default Gateway]

OSPF

OSPF is a routing protocol that sends routing updates between routers and creates a map of the network. OSPF does this by having a process ID, each router has a Router ID and you configure every network connected to the router. You also configure passive interfaces to ports that connect to things like the internet or switches so you aren't sending updates to devices who can't use them. It can also work with other routing protocols but only do that if told so. OSPF uses cost to determine the fastest way to the destination.

Setting IDs
Router(config)router ospf [Process ID]
Router(config-router)router-id [Router ID]

Adding Network and Creating Passive Interfaces
Router(config-router)#network [Network ID] [Wildcard Bits] area [Area ID]
Router(config-router)#passive-interface [Interface ID]

Enabling OSPF with Other Protocols (Only if they say)
Router(config)#redistribute [Routing Protocol]

Configuring Cost
Router(config-router)#auto-cost reference bandwidth [Megabits per second]
OR
Router(config)#int [Interface ID]
Router(config-if)#ip ospf cost [Cost Number]

Configuring Hello and Dead Timers
Router(config)#int [Interface ID]
Router(config-if)#ip ospf hello-interval [Time in seconds]
Router(config-if)#ip ospf dead-interval [Time in Seconds]

RIP Routing

RIP routing is an outdated protocol with two versions but Patriot still uses it and you should still learn it. RIP uses a distance vector algorithm to decide which way to send a packet to its destination. Each router has a routing table which is a list of all the destinations a router knows how to reach. It broadcasts its routing table to other routers every 30 seconds.

Configuring RIP
Router(config)#router rip

Router(config-router)#version 2

Auto-Summary
Router(config-router)#no auto-summary

- Only if directions tell you to disable the summarizations of networks

Adding Networks
Router(config-router)#network [Network ID]

Redistributing Routes
If no distance is given use the command
Router(config-router)#redistribute [Routing Protocol]
If distance is given, use this command:
Router(config-router)#redistribute [Routing Protocol] metric [Distance]

Passive Interfaces
Router(config)#passive-interface [Interface Identifier]

EIGRP

EIGRP (Enhanced Interior Gateway Routing Protocol) is a routing protocol used by routers to exchange routing information in a network. It is a Cisco proprietary protocol and is used mostly in Cisco networks. EIGRP uses a complex algorithm to calculate the best route for data to travel from one network to another. This allows it to choose the most efficient route based on factors such as network congestion, link speed, and the number of hops required to reach the destination. EIGRP is a popular choice for large enterprise networks because of its ability to quickly converge on a new network topology and its efficient use of network bandwidth.

Configuring EIGRP on a Router
Router(config)#do show ip route connected
Router(config)#router eigrp [EIGRP Autonomous Number]
Router(config-router)#network [All networks given by first command]
Router(config-router)#no auto-summary

Access Control Lists (ACLs)

Access Control Lists (ACLs) are one of the hardest topics to first understand in Cisco Networking, they permit or deny certain traffic through interfaces on routers. There are two types of ACLs, extended and standard. Standard ACLs are numbers 1-99 and extended are 100-199. Standard ACLs only have a source address and are applied closest to the destination. Extended ACLs have a source and a destination address and are applied closest to the source, extended ACLs also have implicit deny statements at

the end of them. At the end of a standard ACL you are using to filter traffic you might need to add a deny any statement.

Standard ACLs

Creating the ACL
Router(config)#ip access-list standard [1-99 or Name]

Creating a Standard ACL statement
Router(config-std-nacl)#[permit/deny] [host/Network address/any]

- Host:
    - Router(config-std-nacl)#permit/deny host [IP Address]
- Network Address: [Network ID]
    - Router(config-std-nacl)#permit/deny [Network ID] [Wildcard Bits]
- Any:
    - Router(config-std-nacl)#permit/deny any

Extended ACLs

Creating the ACL
Router(config)#ip access-list extended [100-199 or Name]

Creating an Extended ACL statement
Router(config-exd-nacl)#permit/deny [Protocol] [Source Address] [Source Wildcard] [any/host Destination IP/Destination address & Destination Wildcard]

- If protocol is anything but IP and you need to permit a certain protocol like SSH or NTP, use command
- Router(config-exd-nacl)#permit/deny [Protocol] [Source Address] [Source Wildcard] [any/host Destination IP/Destination address & Destination Wildcard] eq [Port Number]

Application of ACLs
Router(config)#interface [Interface Identifier]
Router(config-if)#ip access-group [ACL Number/ACL Name] [In or Out]
Router(config)#line vty [Start VTY Line] [End VTY Line]
Router(config-line)#access-class [Name or Number] [In or Out]

Network Address Translation (NAT)

NAT stands for Network Address Translation and is a method used by network routers to translate a public IP address to a private IP address and vice versa. This is done to hide

the internal network structure and IP address of the devices on the network. NAT can be either static or dynamic and you must make an ACL for dynamic NAT.

Configuring and Applying Static NAT
Router(config)#ip nat inside source static [Local IP Address] [Global IP Address]
Router(config)#int [Interface Identifier]
Router(config-if)#ip nat [inside or outside]

Configuring and Applying Dynamic NAT
Router(config)#ip nat pool [Pool Name] [Start IP Address] [End IP Address]
Router(config)#ip nat inside source list [ACL Number] pool [Pool Name]
Router(config)#int [Interface Identifier]
Router(config-if)#ip nat [Inside or Outside]

Port Address Translation (PAT)

PAT, or Port Address Translation, is a networking technology that allows multiple devices on a local network to share a single public IP address. This is commonly used in home networks where there are multiple devices (e.g. computers, smartphones, tablets) that need to access the internet, but the internet service provider only provides a single public IP address.

Configuring PAT with an Address Pool
Router(config)#ip nat pool [Pool Name] [Start IP Address] [End IP Address]
Router(config)#ip nat inside source list [ACL Number] pool [Pool Name] overload
Router(config)#int [Interface Identifier]
Router(config-if)#ip nat [Inside or Outside]

Configuring PAT for a Single Address
Router(config)#ip nat inside source list [ACL number] interface [Interface Type] [Interface Number] overload
Router(config)#int [Interface Identifier]
Router(config-if)#ip nat [inside or outside]

Dynamic Host Configuration Protocol (DHCP)

DHCP, or Dynamic Host Configuration Protocol, is a networking protocol that is used to automatically assign IP addresses to devices on a network. When a device connects to a network that uses DHCP, the device sends a broadcast request for an IP address. The

DHCP server, which is typically a router or other network device, responds with an available IP address that the device can use. This allows the device to communicate with other devices on the network and access the internet, without the need for manual configuration of IP addresses. DHCP only works on one LAN so you use DHCP relays to connect LANs together.

Turning On DHCP
Router(config)#service dhcp

Excluding Addresses
Router(config)#ip dhcp excluded-address [First IP Address] [Last IP Address]

- If you are only to exclude one address, the IP you are excluding is both the first IP and the last IP (Andrew)

IPv4

Configure Basic DHCP Server
Router(config)#ip dhcp pool [Pool-Name]
Router(dhcp-config)#network [Network Address] [Subnet Mask]
Router(dhcp-config)#default-router [Default Gateway]
Router(dhcp-config)#dns-server [DNS Address]
Router(dhcp-config)#domain-name [example.com]

Adding a DHCP Relay
Router(config-if)#ip helper-address [DHCP Address]

Letting DHCP Assign Interface IP Addresses
Router(config)#int [Interface Identifier]
Router(config)#ip address dhcp

IPv6

Configure Basic DHCP Server
Router(config)#ipv6 dhcp pool [Pool Name]
Router(config-dhcpv6)#address prefix [IPv6 Network Identifier and Prefix]
Router(config-dhcpv6)#dns-server [DNS Server IP]
Router(config-dhcpv6)#domain-name [example.com]

Configure Stateless DHCPv6 on a Router
Router(config)#ipv6 unicast-routing
Router(config)#ipv6 dhcp pool [Pool Name]

Router(config-dhcpv6)#dns-server [DNS Server IP]
Router(config-dhcpv6)#domain-name [example.com]
Router(config)#interface [Interface Identifeir]
Router(config-if)#ipv6 dhcp server [Pool Name]
Router(config-if)#ipv6 client pd [Name]

Configuring a Router as a Stateless DHCPv6 Client
Router(config)#ipv6 enable
Router(config)#ipv6 address autoconfig

Configuring a Router as a Stateful DHCPv6 Client
Router(config)#ipv6 unicast-routing
Router(config)#ipv6 dhcp pool [Pool Name]
Router(config-dhcpv6)#address prefix [IPv6 Prefix and Length]
Router(config-dhcpv6)#dns-server [DNS IP Address]
Router(config-dhcpv6)#domain-name [example.com]
Router(config)#interface [Interface Identifier]
Router(config-if)#

- ipv6 enable
- ipv6 address autoconfig

Configure Stateful DHCPv6 on Router:

(Use information from the server)

-]
- interface [type] [number]
    - ipv6 dhcp server [pool-name]
    - ipv6nd managed-config-flag

Config Router as Stateful DHCPv6 Client:

- ipv6 enable
- ipv6 address dhcp

DHCPv6 Relay Agent:

- ipv6 dhcp relay destination [dhcp-address]

Network Time Protocol

NTP, or Network Time Protocol, is a networking protocol that is used to synchronize the clocks of devices on a network. It allows devices to obtain the current time from an NTP server (master), and to adjust their own clock so that it remains accurate. This is important for maintaining accurate timestamps for network events, and for ensuring that the clocks of different devices are synchronized. NTP can be synchronized with keys and passwords.

Configuring a NTP Server (Master)
Router(config)#ntp master

COnfiguring a NTP Client
Router(config)#ntp server [IP Address of Peer] key [Peer Key Number]

Enabling NTP Authentication
Router(config)#ntp authenticate
Router(config)#ntp authentication-key [Key Number] md5 [Authentication Key]
Router(config)#ntp trusted-key [Trusted Key Number]

Enabling NTP Calendar Updates
Router(config)#ntp update-calendar

Logging

In Cisco devices, logging refers to the process of recording events and information about the device's operation. This can include system messages, errors, alerts, and other information that can be useful for troubleshooting and monitoring the device's performance. Cisco devices can be configured to log this information to a variety of destinations, including local log files, syslog servers, and network management systems.

Turning Logging on and Setting a Syslog Server
Router(config)#logging on
Router(config)#logging host [Syslog Server IP Address]

Syslog Best Practice Configuration
Router(config)#logging trap debugging
Router(config)#logging userinfo
Router(config)#service timestamps log datetime msec

Logging Logins
Router(config)#login on-succcess log
Router(config)#login on-failure log

Etherchannel/LACP/PAGP

EtherChannel is a technology developed by Cisco that allows multiple physical Ethernet links to combine into a single logical link. This technology provides increased bandwidth and improved link redundancy. EtherChannel can be used with a variety of Cisco switches and other networking equipment, and it is a popular solution for creating high-performance, scalable network designs.

LACP, also known as Link Aggregation Control Protocol, is a networking protocol that is used to establish and maintain link aggregation groups (LAGs) between network devices. LACP allows network devices to negotiate automatic aggregation of multiple network links into a single logical link, providing increased bandwidth and improved link redundancy. LACP is supported by a variety of networking equipment, including Cisco switches, and it is often used in conjunction with EtherChannel to create high-performance, scalable network designs.

PAGP, also known as Port Aggregation Protocol, is a Cisco-proprietary networking protocol that is used to establish and maintain link aggregation groups (LAGs) between network devices. PAGP allows network devices to negotiate automatic aggregation of multiple network links into a single logical link, providing increased bandwidth and improved link redundancy. PAGP is supported by a variety of Cisco switches and other networking equipment, and it is often used in conjunction with EtherChannel to create high-performance, scalable network designs. Unlike LACP, which is an industry-standard protocol, PAGP is a proprietary Cisco technology.

To Bind Ports Together for Etherchannel
Switch(config)#int range [Start port]-[end port]
Switch(config-if-range)#channel-group [Channel Group Number] mode [mode]
Switch(config-if-range)#exit
Switch(config)#interface port-channel [group number]
Switch(config-if)#switchport mode trunk
Switch(configif)#switchport trunk allowed vlan [#1,#2,#3]

Etherchannel/LACP/PAGP Modes
Active - enable LACP unconditionally
Auto - enable PAGP only if a PAGP device is detected
Desirable - enable PAGP unconditionally
On - enable etherchannel only
Passive - enable LACP only if a LACP device is detected

AAA

AAA stands for "Authentication, Authorization, and Accounting." In Cisco systems, AAA is a framework for controlling access to network resources by providing authentication, authorization, and accounting services. This allows administrators to manage user access to the network and track user activities, helping to improve security and ensure that network resources are used properly.

To Create an AAA Model
Router(config)#aaa new-model

Authentication

Setting up AAA Authentication
Router(config)#aaa authentication login [Default or List Name] [Method(s)]
Router(config)#aaa authentication [default or list-name] local-case
Router(config)#aaa local authentication attempts max-fail [number of unsuccessful attempts]

Applying to a VTY Line
Router(config)#line vty [First line] [Last line]
Router(config-line)#login authentication [Method]

AAA Authentication Methods
Default - default method list - automatically applied to all interfaces except those with other method lists applied
Enable - uses enable password
Local - uses local username database
Local-case - Uses case sensitive local username database
None - No authentication
Group radius - uses the list of all RADIUS servers for authentication
Group tacacs+ - uses the list of all TACACS+ servers for authentication
Group [Group Name] - uses a subset of RADIUS or TACAS+ servers for authentication as defined by the “aaa group server radius” or “aaa group server tacacs+” command

Authorization

Setting up AAA Authorization

Router(config)#aaa authorization exec [default | exec | commands *level*] [default | *list-name*] [method(s)]

List of AAA Authorization Methods
Cache - use cached group
Group - use server-group
If-authenticated - succeed if user has authenticated
Krb5-instance - use kerberos instance privilege maps
Local - use local database
None - no authorization (always succeeds)

Accounting

AAA accounting uses triggers, these triggers specify what actions cause accounting records to be updated, a list of triggers follows:

AAA Triggers
Start-stop - send a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process
Stop-only - sends a stop accounting record for all cases including authentication failures
None - disables accounting method lists available

Setting up AAA Accounting
Router(config)aaa accounting [network | exec | connection] [default | list-name] [start-stop | stop-only | none] [broadcast] [method(s)]

VPN

A VPN, or Virtual Private Network, is a technology that allows users to securely access a private network and share data remotely through public networks. In Cisco systems, a VPN is typically used to provide secure remote access to an organization's network. VPNs use encryption to protect the data transmitted between the user's device and the VPN server, ensuring that the data remains confidential and cannot be intercepted by unauthorized parties. VPNs can be used to access corporate networks, enable remote workers to securely connect to the company's network, and allow users to securely access resources on the internet.

A remote-access VPN is created when VPN information is not statically set up, but instead allows for dynamically changing connection information, which can be enabled and disabled when needed.

A site-to-site VPN is created when devices on both sides of the VPN connection are aware of the VPN configuration in advance. The VPN remains static, and internal hosts have no knowledge that a VPN exists.

IPsec is a Site to Site VPN protocol

Configure ISAKMP using HAGLE:

1. Hash (Integrity of Data)
2. Authentication (Digital Certificates or Pre Shared Keys
3. Group (DH group: Allows secret keys to be generated by peers to encrypt and decrypt data)
4. Lifetime (Default 1 day)
5. Encryption

Commands
Step 1:
Define traffic with ACL and make sure to permit the IPsec protocol traffic
Router(config)#permit udp eq isakmp
Router(config)#permit esp
Router(config)#permit ahp
Step 2:
Configure ISAKMP Policy with priority 1 using the SA parameters (HAGLE)
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#hash sha
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 24
Router(config-isakmp)#lifetime 3600
Router(config-isakmp)#encryption aes 256
May have to use crypto isakmp enable or license boot module c1900 technology-package securityk9 to turn on isakmp
Step 3:
Configure Transform Set
Router(config)#crypto ipsec transform-set [router hostname 1]-[router hostname 2] esp-aes esp-sha-hmac
Step 4:
Configure Crypto Map
Router(config)#crypto map [name] 10 ipsec-isakmp
Router(config-crypto-map)#match address 102
Router(config-crypto-map)#set transform-set [router hostname 1]-[router hostname 2]
Router(config-crypto-map)#set peer [peer address]
Router(config-crypto-map)#set pfs group24
Router(config-crypto-map)#set security-association lifetime seconds 900
Apply the map to an interface
Router(config-crypto-map)#interface [identifier]
Router(config-if)#crypto map [name]

ASA

ASAs do not have traditional interfaces, they have an inside, outside, and a DMZ. You must assign these to VLANs to configure them. Most ASA traffic flows from a higher security level to a lower level, however you can write ACL exceptions. ASAs also use Objects, objects are reusable components that can take the place of ip addresses, services, names, and so on.

Configuring ASA Interfaces
ASA(config)#int vlan [vlan identifier]
ASA(config-if)#nameif [inside | outside | DMZ]
ASA(config-if)#ip address [ip] [subnet]
ASA(config-if)#security-level [0-100]

COnfiguring NAT on an ASA
ASA(config)#object network [Object Name/ID]
ASA(config-network-object)#description [Description]
ASA(config-network-object)#host [IP Address]
ASA(config-network-object)#subnet [Network Address] [Subnet Mask]
ASA(config-network-object)#nat ([internal IF Name),[external if name]) [Nat Type]
ASA(config-network-object)#nat ([internal IF Name),[external if name]) dynamic [interface]
nat ([internal IF Name),[external if name]) static [Mapped IP Address]

Configuring SSH on ASA
ASA(config)#crypto key generate rsa modulus
ASA(config)#ssh [IP Address of HOst or Network] [Netmask][Origin interface]
ASA(config)#ssh timeout [Timeout in minutes]

Troubleshooting Commands

All in privileged EXEC mode, or put “do” in front of the command in config mode

General

Router#show run
Router#show ip route connected
Use “CTRL + SHIFT + 6” to cancel translating
To delete a configuration put “no” in front of the command that made it

VLANs

Switch#show vlan
Switch#show vlan brief
Switch#show vlan id [VLAN ID]
Switch#show vlan name [VLAN Name]

Spanning Tree

Switch#show spanning-tree
Switch#show spanning-tree vlan
Switch#show spanning-tree summary
Switch#show spanning-tree interface
Switch#show spanning-tree active
Switch#show spanning-tree detail

Static Routes

Router#show ip route
Router#show ip route summary
Router#show ip route static

OSPF

Router#show ip route ospf
Router#show ip route ospf [Process ID]

RIP

Router#show ip route rip

EIGRP

Router#show ip eigrp
Router#show ip eigrp neighbors
Router#show ip eigrp interfaces
Router#show ip eigrp topology
Router#show ip route eigrp

ACLs

Router#show access-lists [ACL Number or ACL Name]

NAT and PAT

Router#show ip nat translations

Router#clear ip nat translations
Router#show ip nat statistics

DHCP

Router#show ip dhcp pool
Router#show ip dhcp conflict
Router#show ip dhcp relay

NTP

Router#show ntp status
Router#show clock

AAA

Router#show aaa authentication

Index