2015

Chris Hildebrandt
@childebrandt42

CISCO 640-911 EXAM STUDY GUIDE

This study guide is meant to assist you with your prep work for the Cisco 640-911 exam

Table of Contents

Introduction

I made the decision to make an effort to put together an exam study guide for the Cisco CCNA-DC 640-911 test. I am putting this out hoping one person finds some use of this document, or at least a good laugh. This is not meant to be an "Official Study Guide." This is merely a collection of my notes that I found valid for the Exam. I highly recommend that you read through the documentation, and the exam outline, books, and check out the Cisco learning site. I did purchase a book by Wendell Odom and Chad Hintz Titled CCNA Data Center DCICN 640-911 Official Cert Guide, and was an amazing help through the study process. I am putting an effort to make this as detailed as time permits me to do. So use at your own risk and remember this is not meant to be the sole study method. It is meant to be a guide to help you determine your weak spots, and also help me remember stuff for my own exam.

If there are any questions or concerns feel free comment on my blog post or to reach out to me on twitter and I will do my best to address the issue.

Section 1 – Describe how a Network works

Overview

Section one focuses around some of the different types of network devices, the different topology's used for networks, and the OSI model. This section makes up 15% of the material for the Exam according to Cisco.

Section 1 is made up of the following Objectives and Sub-Objectives.

Objective 1.1 Describe the purpose and function of various networks

Sub-Objective 1.1.a Interpret a network topologies

Sub-Objective 1.1.b Define physical network topologies

Objective 1.2 Select the components required to meet a network specification

Sub-Objective 1.2.a Switches

Objective 1.3 Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network

Sub-Objective 1.3.a IP

Sub-Objective 1.3.b TCP

Sub-Objective 1.3.c UDP

Objective 1.4 Describe the purpose and basic operation of the protocols in the OSI and TCP

Sub-Objective 1.4.a TCP/IP

Sub-Objective 1.4.b OSI Layers

Objective 1.1 Describe the purpose and function of various networks

I guess the first place to start is with a question. What is a network? The Wikipedia definition is "a group or system of interconnected people or things." In the computer world I think its best put as a group of connected devices like; computers, printers, servers, phones, and so on. And, this can be as small as two devices and scaled up to your imagination.

Network Types

The Local Area Network (LAN)

Really this is as it sounds. A Local Area Network is a network that spans; a location, a single building, a department, a home office.

LAN's are made up of Endpoint devices, Switches, and Routers.

LANs could be physically wired networks or wireless networks or both.

The Wide Area Network (WAN)

The Wide Area Network is kind of a difficult thing to define. The simplest way that I have ever heard it defined is "A network that spans a large geographical area." The biggest and most well-known example would be the "Internet."

A WAN is made up of Routers, Switches, and Public links.

Key differences between the LAN and WAN

- WAN is made to span geographical locations and LAN is made to span a single location.
- WAN is usually slower due to the distance it has to travel.
- WAN usually requires a router at both ends of the link.

WAN is normally leased lines. What is meant by that? You do not own your WAN lines you lease them from an ISP. Leased lines are much different from the LAN works we deal with day to day. A leased line could actually be a direct connection from one site to another. But it's extremely unlikely, in today's world. It's more likely that to get from site A it may take two or more router hops on three different cables to get to site B or more. That is a more common configuration. Really we do not need to know what goes on at the carrier level. But, anything that is installed in your building you need to know. This is what is known as CPE or Customer Premises Equipment. Today CPE includes a router but before there used to be a router and CSU/DSU. The Channel Service Unit/Data Service Unit was a separate piece of hardware but now it's built into most of the routers. Carrier signal is usually sent over two pairs.

Data Link over leased lines.

High-Level Data Link Control – HDLC – is a light load protocol. It's a simple point-to-point leased line.

When a packet is sent it has an address field but it's just an implied address because it only has one place to go.

HDLC today is an ISO standard but Cisco has a proprietary HDLC It adds the Type field. It is lacking in the ISO standard. This allows routers to see they type of packet that is stored in the data field.

Typical routing uses HDLC.

Office1PC1 sends an IP packet to Office2PC2.

Packet leaves PC1 but is encapsulated in an Ethernet frame with a destination of Office1's router. Office1 then de-encapsulates the IP packet and encapsulates into a HDLC frame and forwards it to office2's router. Office2's router de-encapsulates the IP packet and then encapsulates the packet into an Ethernet frame with PC2's MAC as the destination and forwards it to PC2.

Transporting Ethernet over a WAN, this is also known as EoMPLS or Ethernet over Multi-Protocol Label Switching or (MPLS). This gives the WAN the ability to use the Ethernet protocol to pass traffic over the WAN, making things more efficient. EoMPLS acts like an Ethernet link between site A's router and Site B's router.

The internet….The internet is really just a really large WAN. The internet is literally made up of everyone's data. And can be shared with everyone that has access. The internet core is made up of ISP's, as a whole they are the internet core. There are a few ways to get to the internet. And some new ways are popping up all the time. What are covered in the test are just Leased Lines, DSL and Cable

DSL or Digital Subscriber Line is a short high speed link WANS between Telco customer and an ISP. Usually these are less than 10 miles in length. DSL operates over the home TELCO service. It will share the same wire as your existing telephone. But will require a filter for your phone to cut out the noise that is generated by the DSL. DSL is also asymmetric, meaning upload speeds are slower than download speeds.

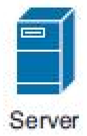
Cable Internet is internet over your coax for your cable TV. It also works asymmetrically. Cable and DSL compete in the same market place. But cable tends to be faster speeds than DSL but DSL tends to be cheaper.

Common Network Components

There are many different network pieces, and quite frankly, there are too many to list so I am just going to cover a hand full.

- Servers
- Repeater
- Hub
- Router
- Switch
- Bridge
- Firewall
- Storage Area Network (SAN)

Server



Servers are really defined as a running instance of an application capable of accepting requests from the client and giving responses accordingly. But we tend to encapsulate the physical hardware around this term also. So in today's lighter sense of the word "Server" is more a powerful computer designed to run a piece of serving software on it.

Servers are further more broke down into types. (Not necessary to memorize these)

- Application Server
- Catalog Server
- Communication Server
- Compute Server
- Database Server
- Fax Server
- File Server
- Game Server
- Home Server
- Mail Server
- Mobile Server
- Name Server
- Print Server
- Proxy Server
- Sound Server
- Stand-Alone Server
- Webserver

Repeaters

A repeater is what it sounds like. It gets information from one port reads it, generates a clean strong signal, and then transmits the information out the other port. The purpose of the repeater was to extend the cable due to attenuation. Repeaters are a Layer 1 device on the OSI model, also they are a single broadcast domain, and single collision domain.

Hub

An Ethernet Hub is "a device for connecting multiple Ethernet devices together and making them act as a single network segment. You don't usually see these anymore. But I wanted to make sure I at least mentioned what it was. A hub is known as a "Dumb Switch" when a packet comes in one port it gets rebroadcast out all other ports on the hub at the same time. A hub is also known as a multiport repeater. A hub also operates at half duplex. This means that the hub at any given time can only send or receive on that port at a time. It forwards traffic based on destination IP. Keep note that a Hub is a single broadcast domain, single collision domain, and also a hub is a layer one device on the OSI model.

Router

Router

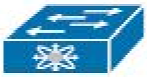
A router is a networking device that forwards data packets between computer networks. A router is what you use to connect two networks together and enable you to route traffic between the two. A router is a layer 3 device on the OSI model.

Switch

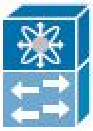
A network switch “is a computer networking device that connects devices together on a computer network, by using a form of packet switching to forward data to the destination device. A network switch is considered more advanced than a (repeater) hub because a switch will only forward a message to one or multiple devices that need to receive it, rather than broadcasting the same message out of each of its ports.” A switch has multi-broadcast domain, Also a switch operates as a layer 2 on the OSI model. There are some layer 3 switches that do some limited routing. A switch contains a MAC address table this allows the switch to learn the devices attached to it. This allows it to send the traffic to only who it’s intended for. A switch is a vast improvement over the Hub because of the ability to use full duplex ports that allow you to send and receive at the same time. Also, a switch is a Single broadcast domain with multiple Collison domains.

Layer 2 Switch

Layer 3 Switch



Nexus Switch



Nexus 7000 Switch

Bridge

A bridge is a device which connects two parts of a network together at the data link layer or layer 2. A bridge can split a hub network into collision domains. Frames from one side cannot collide with frames sent from the other side. Bridges are designed to Join or extend LAN segments. Bridges can regenerate signals, reduce collisions, learn and filter traffic massed on MAC address. A bridge can only operate at Half-Duplex.

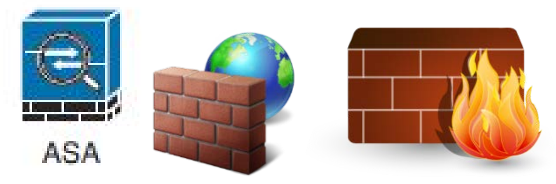
When the bridge receives traffic that is unknown its floods frames and sends traffic out all ports except the port it was received on. A network works similar to network switches, but the traffic is managed differently. A bridge learns MAC address and does not blindly forward frames. A bridge also uses CSMA/CD to handle avoid and handle collisions. A bridge forwards traffic based on destination MAC addresses.

Comparing Bridges and Switches

Bridges	**Switches**
Operated at Layer 2	Operated at Layer 2
Maintain MAC Tables	Maintain MAC Tables
Limited Features	Many Features
Half-Duplex only	Full-Duplex only
Switch in software	Switch in hardware
Slower Speeds (Normally 10 MBps)	Faster Speeds (Up to 1 Gbps)

Firewall

A firewall is a network security device that controls traffic in and out based on the rules that are set in the firewall. A firewall is meant to be a barrier between a trusted secure internal network and any other networks. The firewall is a span of a few layers of the OSI model. Its spans Layer 2, Layer 3, and Layer 4, and some even span Layer 5 for virus scanning. A firewall can be used to do routing also.



A firewall is commonly displayed as a brick wall that may or not be on fire. So I wanted to show Cisco's preferred icon and the common ones you see in the work space.

Storage Area Network (SAN)

A SAN is out of scope on the test but I have been lead to believe there is reference to this in the exam. A Storage Area Network is not really a network device, it's a network made up with Fiber Channel Switches. A Fiber Channel Switch does not run Ethernet, its runs Fiber Channel Protocol (FCP). FCP is a way to make a server think it's writing to local discs when it's not.

Sub-Objective 1.1.a Interpret a network diagram

Interpreting a network diagram is really covered all the way through this document. As you look through the types of networks you will see examples of network diagrams.

Network Architecture

Networking was designed so we could share information, how the information is shared relates to how the type of architecture. There are two main types that I am going to cover: Peer-to-Peer and Client/Server networks.

Peer-to-Peer Networks

Peer-to-Peer networks are computers connected to each other with no ventral authority. All the computers are peers, and in the view of security and authority they are all equal. For each file request, the computer asking for the file asks for permission from the computer holding the file. These networks are quite common today in the Windows, Mac, and or Unix networks. The most common use would be home workgroups.

Client/Server Networks

Client/Server networks are quite different compared to peer-to-peer networks. There is a single server that is the authorities master for the network. The central authoritative server manages the whole network. When a computer wants to request a file the request goes to the authoritative server, gets validated, and then directed to the content it was requesting.

Sub-Objective 1.1.b Define Physical Network Topologies

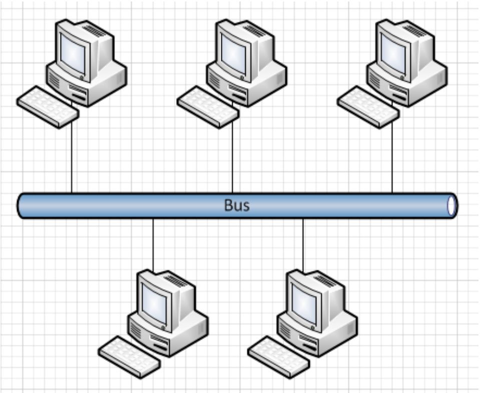
A physical network topology is in simple since a map of the network. There are physical and logical topologies; they are both very different. The major differences between the two are that physical topology gives you the lay of the network; whereas, the logical topology shows how things move through the network. A network map is more like a road atlas of your network.

There are a basically four main types of network topologies that you many run into:

- Bus
- Ring
- Star
- Tree

Then there are four that are really a mixture of topology types.

- Mesh
- Point-to-Point
- Point-to-Multipoint
- Hybrid

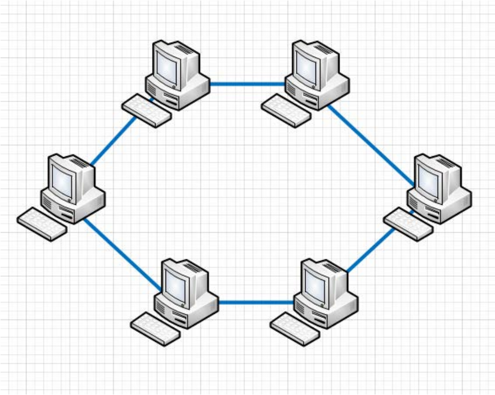


Bus Topology

A bus network is a shared cable medium.

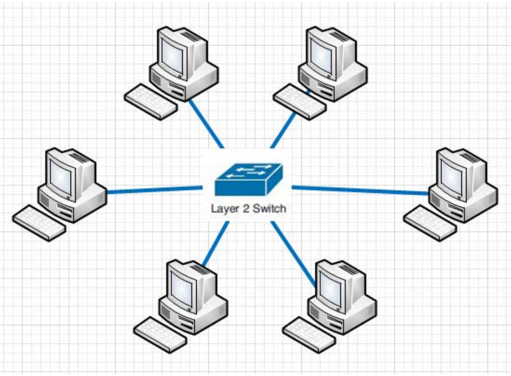
Key Features

- Loss of single client or node does not affect others
- A cut in the bus cable results in a loss of the network
- Terminator at the end of the cable to prevent signal bounce back
- Collisions are common, only one client can send or receive at a time



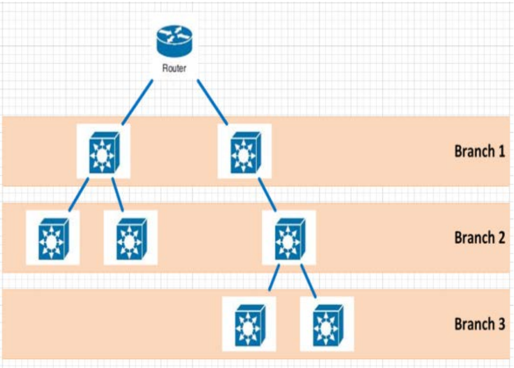
Ring Topology

A ring network is a client dependent network. Each client is connected to two other clients. Fiber Distributed Data Interface (FDDI) is one big use case for a Ring network. The traffic from the most common ring only goes one way. If the ring is broken in the single direction ring the network is down. There are some that had counter-rotating or what they call dual ring designed. Dual ring designs will allow traffic to go both ways. And if the dual ring is broken it will create what is known as a “C Ring.”



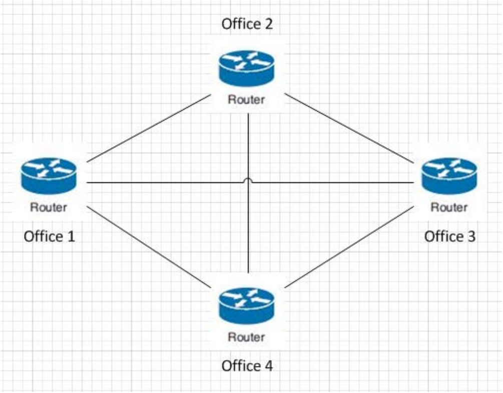
Star Topology and Extended Start Topology

Star networks are extremely common in today’s networks. Each client is connected to a central switch. When a client fails it does not affect the network. But when the central switch fails it causes the whole network to fail. Star networks can avoid this issue but using a pair of central switches, creating redundancy. Extended Star networks are nothing more than adding more switches of the central switch. Both forms are extremely common today.



Tree Topology

A tree network is a common network that you see today. There are a lot of company’s out there today with these types of networks. They work great in small companies because they have a scale limit. The traffic has to go up to the root router to be routed anywhere and if the right side wants to talk to the left side.

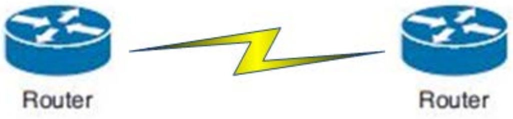


Mesh Topology

A mesh topology is set into two different types.

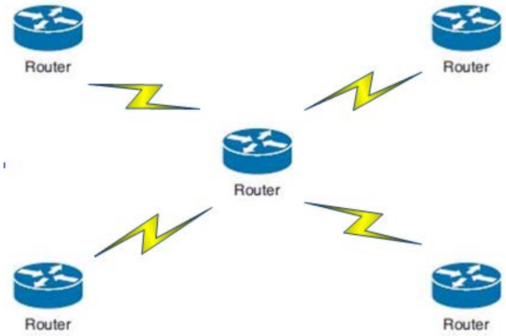
- Partially connected where each node is connected by two links.
- Fully connected mesh where all nodes are connected to each other.

Both of these are very expensive to implement. The number of connections grows exponentially. Not really used any more.



Point-to-Point

A point to point network is more of a WAN network. It's normally used to connect two offices together.



Point-to-Multipoint

A Point-to-Multipoint network is also known as a hub and spoke network. A hub and spoke network has a center point and is connected to each spoke by one link. It looks like an old wagon wheel. They are common in frame relay and T-1 networks. But they have a major drawback. If the hub fails the whole network goes down, but if you lose a spoke it does not affect the network.

Hybrid

A hybrid topology is really the mixture of various topologies. This is the most common configuration in the world today. In most cases it's a mixed topology of Star, tree, and partial mesh. Those are the most common. And it would be really odd to see Bus or Ring in a modern network unless you have some legacy system that you have not managed to get thrown out.

Network Connectors and Cables

Common LAN cable Speeds, Types, length

Ethernet Cable Type	Cable Speed	Media	MAX Cable Length	Connector
10BASE-T	10Mbps	CAT3 or better (2-Pair)	100m	RJ11, RJ12, RJ45
100BASE-T	100Mbps	CAT5-UTP (2-Pair)	100m	RJ11, RJ12, RJ45
1000BASE-T	1000Mbps	CAT5e/6-UDP (4-Pair)	100m	RJ11, RJ12, RJ45
1000BASE-LX or SX	1000Mbps	Multimode Fiber	550m	ST, SC, LC
1000BASE-LX	1000Mbps	Single-Mode Fiber	5km	ST, SC, LC
10GBASE-T	10Gbps	CAT6a-UTP	100m	RJ45
Less used or Outdated Types				
Thicknet 10BASE-5	10Mbps	RG-8	500m	BNC, N, TNC, UHF
Thinnet 10BASE-2	10Mbps	CATV coax	185m	BNC, N, TNC, UHF

BASE-T = Twisted Pairs

BASE-LX = Long Wave Length Fiber

BASE-SX = Short Wave Length Fiber

Connectors

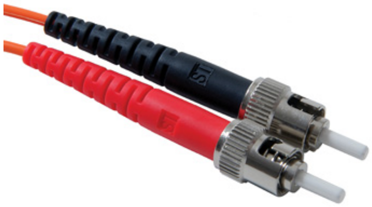
RJ45 – Used with Copper Cables, 8 Pin

RJ11 – Used with Copper Cables (Common with Telephones), 2, 4, or 6 Pin

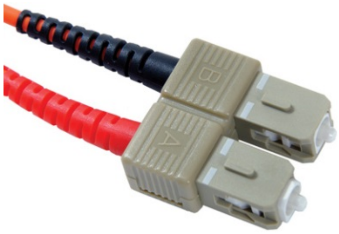
SFP – Small Form-Factor Pluggable used by Fiber Cables or Ethernet port converters.

GBIC – Gigabit Interface Converter, another name for SFP

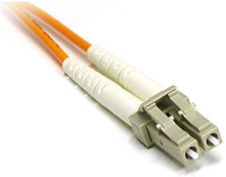
ST – Straight Tip connector for fiber multimode cable



SC – Subscriber Connector for fiber multimode cable

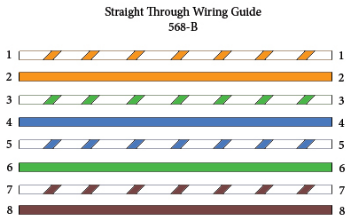


LC – Lucent Connector for fiber (Most Common Connector)

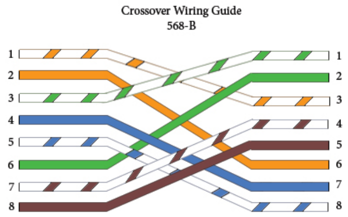


Common Ethernet Cables

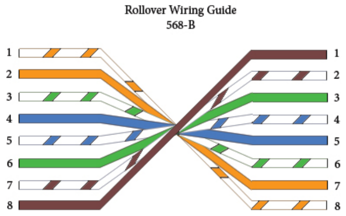
Straight-Through Cable – Cables are made so the pins match on each side



Crossover Cable – Pins are crossed from one side to the other. 1>3,2>6,3>1,4>7,5>8,6>3,7>4,8>5



Rollover Cable – Pins are exact opposite on the other end of the cable 1>8,2>7,3>6,4>5,5>4,6>3,7>2,8>1



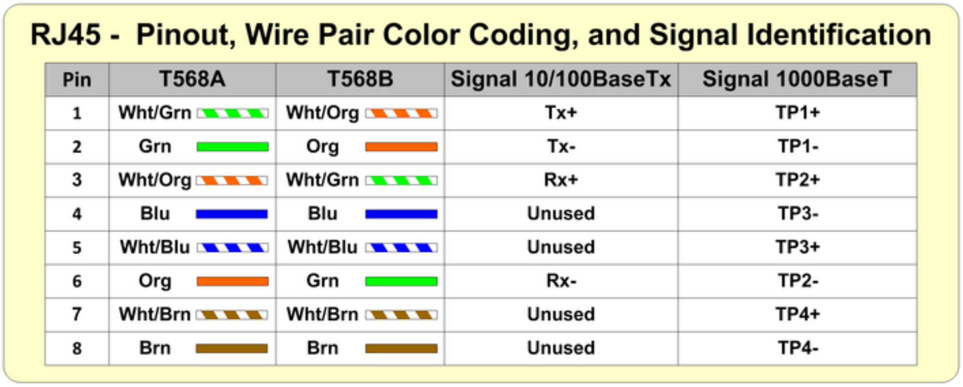
Cable to Device Matrix

	Hub	Switch	Router	Workstation
Hub	Crossover	Crossover	Straight	Straight
Switch	Crossover	Crossover	Straight	Straight
Router	Straight	Straight	Crossover	Crossover
Workstation	Straight	Straight	Crossover	Crossover

Wiring Standards

For some reason someone thought it was a great reason to create two wiring standards. Why? I really don’t know, I just want to hit they guy that did some days when contractors do one standard and other does it a different way.

There are two types T568A and T568B. T568B is the most common found around.



RJ45 - Pinout, Wire Pair Color Coding, and Signal Identification

Pin	T568A	T568B	Signal 10/100BaseTx	Signal 1000BaseT
1	Wht/Grn	Wht/Org	Tx+	TP1+
2	Grn	Org	Tx-	TP1-
3	Wht/Org	Wht/Grn	Rx+	TP2+
4	Blu	Blu	Unused	TP3-
5	Wht/Blu	Wht/Blu	Unused	TP3+
6	Org	Grn	Rx-	TP2-
7	Wht/Brn	Wht/Brn	Unused	TP4+
8	Brn	Brn	Unused	TP4-

Objective 1.2 Select the components required to meet a network specification

Coming up with a set list of how to make sure things meet network specifications is really hard for me, it’s one of those answers that just depends. I hate it when I hear that answer but as you spend more time in technology you hear it more often and you kind of get nulled to the word. Every network is completely different and there for every case is different.

Best ways to decide on what gear to get.

- A good solid education on what each product you are looking at does and what its purpose is.
- Learn the pros and cons of each piece. Get to know the limitation, and performance of each piece.
- Understand the features of each device, match them to your company’s requirements, and needs.
- And, usually the deal breaker in most cases is budget.

Sub-Objective 1.2.a Switches

Switches

We covered switches of a few pages ago in light detail. So to save you time and me time I am not going to copy and paste that info in here. But I did want to give the definition again.

A network switch "is a computer networking device that connects devices together on a computer network, by using a form of packet switching to forward data to the destination device."

A switch has two BIOS loaded to it. They are Golden BIOS and the Upgradable BIOS

Golden BIOS – is non-upgradable bios. It's the master bios that the switch is shipped with. You cannot change this BIOS nor do you want to. If you mess something up in the switch you can always revert back to this version. You can force boot to the Golden BIOS by pressing (Ctrl-Shift-6) during boot.

Upgradeable BIOS – This is the BIOS you use when operating the switch. This BIOS you can upgrade with Cisco code patches, or software upgrades.

Switch Start up Process

When the BIOS are loaded they preform system health checks on the switch. Then the BIOS loads the Loader service. The Loader loads the Kickstart image to the RAM. Once the image is loaded into the RAM it starts the Kickstart image.

Nexus has two different images. One is the Kickstart image, and the other is the system image. They both have to be the same on the same version. The System image is what the switch actually runs.

Once the Kickstart has loaded it takes over the process. The kickstart image is in charge of loading the kernel (Yes it's Linux), and drivers, and then the system image.

The next step is to load the Configuration.

The switch configuration is saved in NVRAM (Non-Volatile RAM), NVRAM is extremely fast so the configuration can be loaded very quickly. Also, NVRAM is not whipped when power is removed or the switch is restarted.

The running configuration is loaded in RAM. So if you do not run "copy run start" once you make changes and the switch reboots your changes are lost.

Also, if you mess up the configuration or just want to start fresh you can enter the command "write erase" this will start the switch as if it just came out of the box.

If you would like to reboot the switch you will need to use the "reload" command.

This is the Startup of a switch. Pretty simple right? I think this is something most of us will have to take some time to memorize.

Switch Diagnostics

Most of the time there is not much to troubleshoot on a switch physically. Most of the time you just need to check to see if the power cables are inserted, or if the power supplies are pulled out and need reseated. On the bigger switches make sure the line card is inserted completely. But that is really it. There are times you may need to go deeper. There is a program that is called GOLD.

GOLD – Generic Online Diagnostics. This is a diagnostic program that you can run while the switch is in production. GOLD is made up of several tests:

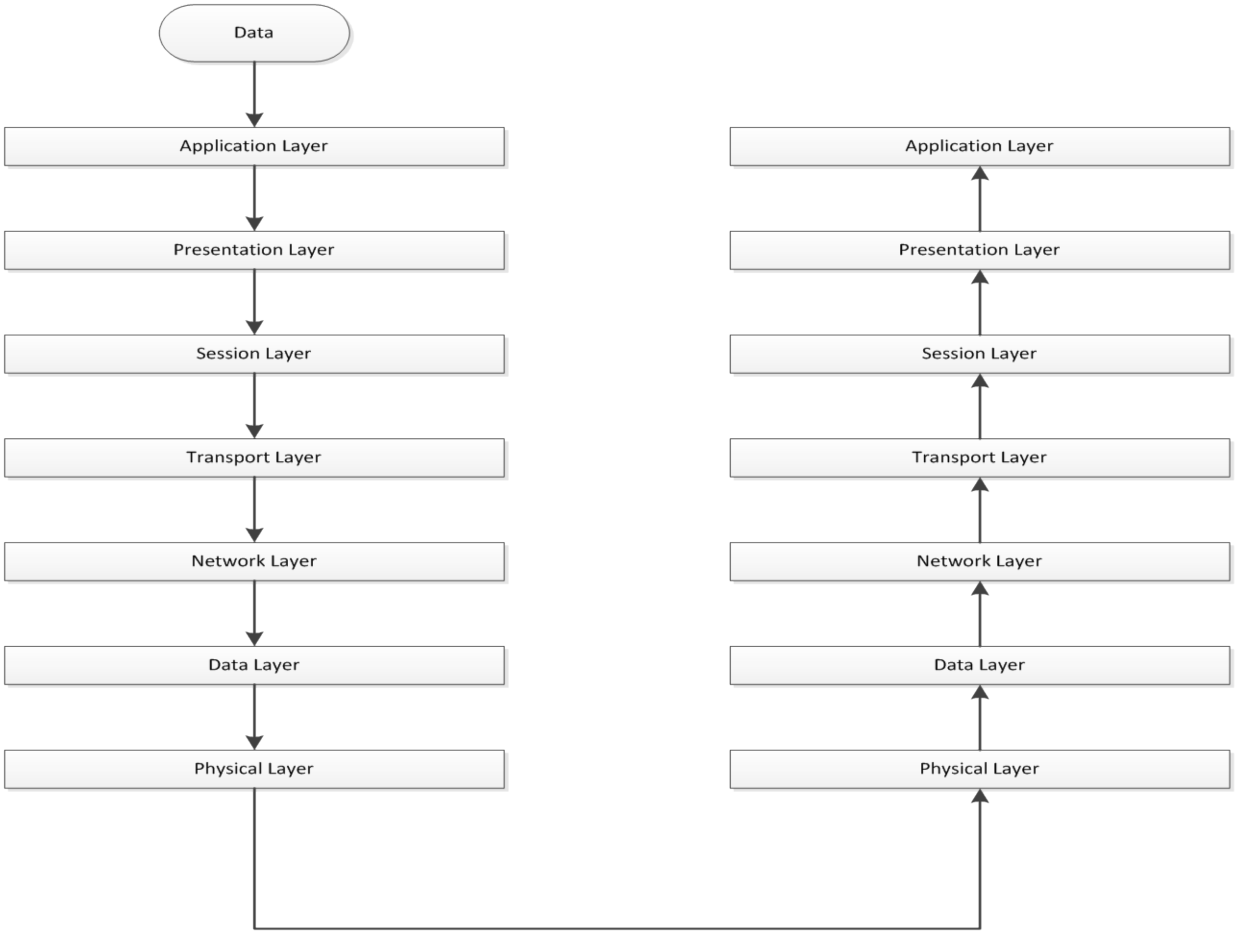
- Boot up Diagnostics
- Runtime Diagnostics
- Health Monitoring
- On-Demand Diagnostics
- High Availability
- Virtualization Support (VDC)

Objective 1.3 Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network

When the network devices were invented, there were no standards. None of the vendors would talk to each other. So if you wanted to change brands you needed to rip and replace all the network equipment.

This topic is a little out of order and should be along with the OSI model. So here we go we will explain the way data flows through the network and then in a couple of pages you will make it to the OSI model in more detail.

Here is the flow chart of data.



As traffic moves down the OSI model it adds information to the data packet. This is called encapsulation. This repeats down the OSI model. And as traffic moves up the OSI Model it strips off the Headers this is called De-encapsulation. See example below.

Application						Application Header	Data	
Presentation					Presentation Header	Application Header	Data	
Session				Session Header	Presentation Header	Application Header	Data	
Transport			Transport Header	Session Header	Presentation Header	Application Header	Data	
Network		Network Header	Transport Header	Session Header	Presentation Header	Application Header	Data	
Data Link	Data Link Header	Network Header	Transport Header	Session Header	Presentation Header	Application Header	Data	Data Link Trailer
Physical	Bits							

Great site for this: http://blog.pluralsight.com/networking-basics-tcp-udp-tcpip-osi-models

Sub-objective 1.3.a IP

IP – Internet Protocol. Internet Protocol is the main communications protocol we use for relaying datagrams across network boundaries. IP is the protocol of the Network Layer. IP identifies any host or router that connects to a TCP/IP network. The internet protocol is known as a connectionless and this really means that this is best effort on its own since it relies on the transport layer to get its reliability. One big part of IP is IP addressing. An IP address is made of a 32 bit address. It is made up of 4 octets; for example 192.168.56.123. This is also known as dotted decimal number. IP addresses are based on a hierarchy system. A portion of the IP address represents the network you are on and the other portion represents the host.

Public and private networks also use a thing called DHCP or Dynamic Host Configuration Protocol. DHCP allows networks to auto assign IP addresses.

DHCP is a 4 step process:

- Discover - Host sends a Discover Message (Requesting an address)
- Offer - The DHCP host will send an Offer Message
- Request - Host will send a request for the address
- Acknowledgment - Last the DHCP host will send an acknowledgment message.

This can be remembered as D.O.R.A.

DNS – Domain Name System is the way you map a name to an IP address; for example www.google.com may translate to 7.7.7.7.

IP has some great tools to view IP information and to troubleshoot in a command prompt inside the windows system.

ipconfig – Will show network information

Ipconfig /all – will show detailed network information

Ipconfig /release – will release your DHCP address

Ipconfig /renew – will renew your DHCP address

Arp –d will flush your local ARP table

"Ping" is also a great tool. Packet Internet Grouper is what it's called. (I did not know that one) Ping is a great way to check to see if an IP address is working, or you can even use it in combination with DNS to look up website address.

"Tracert" is also a great tool. Trace Route is a tool that allows you to see the router hops as the traffic moves through the network and the internet.

Sub-objective 1.3.b TCP

TCP – Transmission Control Protocol. TCP protocol is what we use most often when we surf the web. TCP is a reliable protocol. In TCP the packet is guaranteed, it's a connection oriented protocol. It's kind of like mailing a letter but instead of using the normal mail where it might get lost, you make this a certified letter. This will guarantee your letter or in our case packet will arrive at its destination and in turn you are notified that it arrived at its destination. TCP uses what they call a 3 way hand shake. A host will send a packet to a different host. Inside the header will be a SYN flag setting. The receiving host will get this packet and will send a packet back called SYN ACK and then the requesting host will send an ACK back to the destination host. TCP utilizes flow control. When the destination buffer cannot handle the whole stream it can send a not ready message, and the sender will pause. TCP also uses a sliding window concept. This lowers the overhead to use this protocol. TCP also allows for Session multiplexing. Session Multiplexing is a way to combine several message streams or sessions onto a logical link.

Sub-objective 1.3.c UDP

UDP – User Datagram Protocol. Some people also refer to this as Unreliable Datagram Protocol. UDP data is a stateless connection. The packets are sent in a continuous stream with no return acknowledgement. UDP is like the regular mail service; you put your letter in an envelope put a stamp on it and drop it in the mailbox. You don't care if it makes it there, you just care it's out of your hands now. The UDP protocol does not care if there are dropped or lost packets. It just keeps streaming the packets. The UDP protocol is most common in video and audio streaming, because you do not want to pause the stream and wait on the packet to be resent every time there is a lost packet. Also very low overhead. UDP also allows for Session multiplexing.

Objective 1.4 Describe the purpose and basic operation of the protocols in the OSI and TCP

Well Known Port Mappings (Ports 1 – 1023) Regulated Port Numbers

Ports ranging from 1024 – 49151 called Registered Port numbers.

Ports ranging from 49152 – 63535 are dynamically assigned port numbers.

Protocols used in the OSI and TCP model (Not all)

TLA or FLA	Full Name	Port	TCP or UDP	Description
FTP	File Transfer Protocol	20 and 21	TCP	File Transfer Protocol
SSH	Secure Shell	22	TCP	Encrypted remote management
Telnet	Telnet	23	TCP	Unencrypted remote management
SMTP	Simple Mail Transfer Protocol	25	TCP	Email message transfer
DNS	Domain Name Resolution	53	TCP & UDP	Resolves domain names
DHCP	Dynamic Host Configuration Protocol	67 and 68	UDP	IP address assignment
TFTP	Trivial File Transfer Protocol	69	UDP	Base version of FTP
HTTP	Hyper-Text Transfer Protocol	80	TCP	WWW
POP3	Post Office Protocol	110	TCP	Email Access
SNMP	Simple Network Management Protocol	161	UDP	Network management and device monitoring
HTTPS	Hyper-Text Transfer Protocol Secured	443	TCP	Secure WWW

Sub-objective 1.4.a TCP/IP

TCP/IP Model

In the 1980's there was no such thing as the TCP/IP model. Really there were a few companies that had created their own model for each company. In the late 80's the DOD (Department of Defense) model sprouted up. This is what is known as the TCP/IP model.

TCP/IP Model Original and Revised

TCP/IP Original	TCP/IP Updated
Application	Application
Transport	Transport
Internet	Network
Link	Data link Physical

Don't think because you hear more about the OSI model that you do not need to know the TCP/IP model. You are wrong. The TCP/IP model is so engrained in what we use day to day it's not going away for some time. Actually I think the OSI model is dying off.

Each layer of this is described in detail blow in the OSI mode description.

TCP/IP to OSI comparison

TCP/IP Model		OSI Model
Application	The OSI model split the Application layer into 3 Layers.	Application
		Presentation
		Session
Transport		Transport
Internet	OSI changed the name to Network from Internet	Network
Network Access	OSI split the Network access layer out to Data Link and Physical.	Data Link
		Physical

Sub-objective 1.4.b OSI Layers

OSI Model

The OSI model is a scary subject for most people. I know the first time that I ever heard of it I was completely confused. The OSI model was brought forth to break the complex network down into simplified chunks. The other reason the OSI model was created was to create a standard for networking so all manufactures would work with each other. Over my years I have always wondered why you would ever spend the time to learn about the OSI model. I never could figure out why I needed to know this. After some time I found out. I had an issue with a network, and knowing the OSI model helped me troubleshoot the issue. But the most important reason to learn it now is to pass this Cisco CCNA-DC 640-911 exam.

Layer Name	Layer Number	Devices	Purpose
Application	Layer 7		Protocols for applications to work
Presentation	Layer 6		Formatting of the information
Session	Layer 5		Creating and managing sessions
Transport	Layer 4		Decides if traffic is TCP or UDP
Network	Layer 3	Router's, Some Switches	IP addresses
Data Link	Layer 2	Switch's, Bridge's	Error Discovery and Correction, MAC Address's, Token Ring Media Access Control
Physical	Layer 1	Cable's, Hub's, Repeater	Network Connections

There are two ways to help you learn this model faster. You can memorize this with a sentence "**A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing". This way is to learn from the top down. The one that was the best for me to learn was "**P**lease **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way", this method goes from the bottom up.

The OSI model is split into the upper section, Layer 5 to Layer 7, and the lower, Layer 1 to Layer 4. The lower layer is where most problems take place. In the Internet Protocol Suite Application Layer this includes Layer 5 and Layer 6 of the OSI model. And in the Internet Protocol Suite Network Access Layer includes Layers 1 and 2 of the OSI model. The layers in the OSI model are unaware of each other.

PDU – is the information that moves down the network with the User Data and the Control Information (Headers and Trailers)

Sliding Windows – Is when host A sends 2 packets to host B. Host B acknowledges. Then host A sends 3 packets, and host B acknowledges. This will continue until the packets cannot be handled and it will step down the window. Sending so many chunks of traffic at once and only waiting on one acknowledgment speeds up the transmitting of data.

SYN – Synchronization Request

SYN ACT – Synchronization Acknowledgement

ACK - Acknowledgement

RTP – Real-Time Transport Protocol, it is also sometimes known as RTTP. But most people drop the first T. RTP is extensively used in the communication and entertainment systems that involve streaming media like video, phone, and video teleconferencing. This is used in UDP to make streaming media reliable.

BGP - Border Gateway Protocol will rely on TCP. BGP is designed to exchange routing and reachability information between autonomous systems on the internet.

There are a few Protocols that do not rely on TCP or UDP. They have their own protocol. A couple of these protocols are EIGRP and OSPF.

Below is a chart showing what Data and Headers are called at each step in the OSI model

Layer	What the Data and Headers is called
Application	Data
Presentation	Data
Session	Data
Transport	Segment
Network	Packet
Data Link	Frame
Physical	Bits

Section 2 Configure, Verify and Troubleshoot a Switch with VLAN's and inter-switch communications using Nexus

Overview

This section is made up with all things about switching. This section will also require you to get to know the Nexus OS and IOS a bit. You will need to be able to Create, Verify and Troubleshoot basic switching concepts. This section makes up 21% of the material for the Exam according to Cisco. Beings this is 21% of your exam. I highly recommend you get into a lab of some sort. There are some great labs on Cisco's website. (NOTE THE ADDRESS). There are some other simulators out there (LIST THE LOCATIONS)

For Common Switch commands please look at the "Nexus Command Reference" at the end of this guide.

Section 2 is made up of the following Objectives and Sub-Objectives.

Objective 2.1 Explain the technology and media access control method for Ethernet

Sub-Objective 2.1.a IEEE 802 protocols

Sub-Objective 2.1.b CSMA/CD

Objective 2.2 Explain basic switching concepts and the operation of Cisco Switches

Sub-Objective 2.2.a Layer 2 Addressing

Sub-Objective 2.2.b MAC table

Sub-Objective 2.2.c Flooding

Objective 2.3 Describe and configure enhanced switching technologies

Sub-Objective 2.3.a VTP

Sub-Objective 2.3.b VLAN

Sub-Objective 2.3.c 802.1q

Sub-Objective 2.3.d STP

Nexus

Before we get too far into this I want to explain a bit about the Nexus OS. NX-OS or known as Nexus was designed by Cisco to offer a high performance, highly reliable OS for switches. It was built off a Linux platform. Right now it runs on both MDS and Nexus switch lines. Nexus by default has two user roles, one Admin, and one Operator.

Some of the key features of the Nexus OS are:

Intelligent Traffic Director (ITD) – It's a hardware based Layer 4 load-balancing, traffic steering and clustering

NX Port ID Virtualization (NPIV) – It enables multiple Fiber Channel node port ID's to share the same single physical port.

Unidirectional Link Detection (UDLD) – is a monitoring service that uses the Data link protocol to detect configurations of cables and unidirectional links. UDLD is a layer 2 process.

Nexus uses three key core infrastructure services that provide HA functionality:

System Manager

Persistent Storage Service (PSS)

Message and Transaction Service (MTS)

There are 5 key security features in the Nexus OS:

Cisco TrustSec – A built in hardware and software feature that provides admission control, Security group based policies, and link-layer cryptography.

Integrated Security Features – Protects the network from DoS attacks, network host spoofing and snooping of data and voice traffic.

IEE 802.1x – Uses this for authentication

Port Access Control Lists (PACLs), Router ACLs (RACLs), VLAN ACLs (VACLs), Role-Based Access Control (RBAC) – All for Securing privileges and providing flexibility in protecting information.

Control Plane Protection (CoPP) – Provides broad and granular controls over traffic that reaches the supervisor.

Objective 2.1 Explain the technology and media access control method for Ethernet

Media access control is way to allow computers to transmit signals over network cabling, while ensuring that only one computer transmits at a time. If two computers simultaneously place signals on the wire, a collision can occur and data might be corrupted unless a method is used to resolve the collision gracefully. Media access control methods act like traffic lights by permitting the smooth flow of traffic on a network, and they prevent or deal with collisions. Media access control methods are implemented at the data link layer of the Open Systems Interconnection (OSI) reference model.

Four main media access control methods are used in networking:

- Carrier Sense Multiple Access with Collision Detection (CSMA/CD), which is used in Ethernet networking
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), which is used in AppleTalk networking
- Token passing, which is used in Token Ring and Fiber Distributed Data Interface (FDDI) networking
- Demand priority, which is used in 100BaseVG networking

Sub-Objective 2.1.a IEEE 802. Protocols

IEEE 802 refers to a family of Institute of Electrical and Electronics Engineers (IEEE) standards that deal with Local Area Networks (LAN). The services specifically covered in this map are the lower two layers. Layer 1 the Physical layer and Layer 2 the Data Link layer. IEEE 802 splits the Data Link Layer into two sub-layers named Logical Link Control (LLC) and Media Access Control (MAC).

Data Link Layer

LLC Sublayer

MAC Sublayer

Physical Layer

LLC Sublayer "provides multiplexing mechanisms that make it possible for several network protocols to coexist within a multipoint network and to be transported over the same network medium."

The IEEE has done an amazing job creating some standards that only help us the end user. This is what allows us to purchase any brand network equipment knowing it will work with the others as long as they tend to the IEEE standards.

They have managed to standardize many things from the network traffic, the devices used in that traffic, Cable, connectors and many more things.

IEEE 802.2

I felt the need to cover this a little more in detail as I have seen some things in there that I have never seen before.

IEEE 802.2 is the standard that defines Logical Link Control (LLC) as the upper portion of the Data Link Layer of the OSI model. LLC is a software component that provides uniform interface to the user of the data link service (Common users Network Layer).

LLC offers three types of services

- Acknowledged connectionless mode services (Optional)
- Connection mode services (Optional)
- Unacknowledged Connection mode services (Mandatory)

LLC uses the service of MAC on Ethernet, Token Ring, FDDI, 802.11, etc.

IEEE 802.2 has sublayers that are known as LLC Protocol Data Unit (PDU) and additional info is added to by the sublayer to a LLC Header. LLC Header consist of DSAP (Destination Service Access Point), SSAP (Source Service Access Point), and the Control field.

DSAP and SSAP are both 8 bit fields and The control field is 8 or 16 bits. Then there can be a variation of the LLC Protocol called Subnetwork Access protocol (SNAP) extension which allows using EtherType values to specify the protocol being transported.

Both LLC and SNAP look like the following

802.2 LLC Header			Info
DSAP Address	SSAP Address	Control	
8 Bits	8 Bits	8 or 16 Bits	In 8 bit Increments

802.2 LLC Header			SNAP Extension		Upper Layer Data
DSAP Address	SSAP Address	Control	OUI	Protocol ID	
8 Bits	8 Bits	8 or 16 Bits	24 Bits	16 Bits	In 8 bit Increments

Ethernet Data-Link Protocols

IEEE standardized the Ethernet Protocol. In doing so they moved from the old DIX Ethernet framing to a two header standard, to add in the MAC and LLC sub layers.

IEEE Ethernet

802.3 Header	802.2 Header	Data	802.3 Trailer

DIX Ethernet

Ethernet Header	Data	Ethernet Trailer

One of the biggest changes made was defining a Ethernet Data Field. IEEE created the Destination Service Access Point (DSAP) field. This was created for the role of a Protocol Type field.

Fast forward a few years and IEEE changed their minds again. They decided that the original DIX frame type would work best with some minor modifications. It looks extremely similar just with some name changes. They combined the first 8 bits of the 802.3 header from 7 bits of Preamble and 1 bit SFD to just be an 8 bit Preamble.

IEEE 802 Standards

802.1	Bridging and Management
802.2	Logical Link Control
802.3	Ethernet CSMA/CD access Method
802.4	Token Passing Bus Access Method
802.5	Token Ring Access Method
802.6	Distributed Queue Dual Bus Access Method
802.7	Broadband LAN
802.8	Fiber Optic
802.9	Integrated Services LAN
802.10	Security
802.11	Wireless LAN
802.12	Demand Priority Access
802.14	Medium Access Control
802.15	Wireless Personal Area Networks
802.16	Broadband Wireless Metro Area Networks
802.17	Resilient Packet Ring

IEEE Physical Layer Standards for network speeds

IEEE Standard	Name	Informal Name	Speed	Cabling Type	Year
802.3i	10Base-T	Ethernet	10 Mbps	UTP	1990
802.3u	100Base-T	Fast Ethernet	100Mbps	UTP	1995
802.3z	1000Base-X	Gigabit Ethernet or GigE	1000Mbps	Fiber	1992
802.3.ab	1000Base-T	Gigabit Ethernet or GigE	1000Mbps	UTP	1999
802.3.ae	10Gbase-X	10 GigE	10 Gbps	UTP	2002
802.3.ba	40Gbase-X	40 GigE	40 Gbps	Fiber	2010
802.3.ba	100Gbase-X	100 GigE	100 Gbps	Fiber	2010

IEEE Wireless standards

Protocol	Maximum Data Transfer Speed	Frequency	Highest order Modulation	Channel Bandwidth	Antenna Configuration	Year Introduced
802.11a	54 Mbps	5 GHz	64 QAM	20 MHz	1x1 SISO	1999
802.11b	11 Mbps	2.4 GHz	11 CCK	20 MHz	1x1 SISO	1999
802.11g	54 Mbps	2.4 GHz	64 QAM	20 MHz	1x1 SISO	2003
802.11n	65 to 600 Mbps	2.4 or 5 GHz	64 QAM	20 & 40 MHz	Up to 4x4 MIMO	2009
802.11ac	78 Mbps to 3.2 Gbps	5 GHz	256 QAM	20, 40 , 80, and 160 MHz	Up to 8x8 MIMO	2012

Sub-objective 2.1.b CSMA/CD

Carrier Sense Multiple Access / Collision Detection or CSMA/CD, This is a set of rules that determine how network devices respond when two devices attempt to use data channel simultaneously (This is called a Collision). Standard networks use CSMA/CD to physically monitor the traffic the line, if no transmissions are taking place the station can transmit, if two stations attempt to transmit simultaneously, this can cause a collision, and will be detected by all participating stations. After a random time the stations that collided will attempt to transmit again. If a collision happens again, the time intervals are increased step by step. CSMA/CD is common in a Bus network design.

CSMA/CD was standardized in the IEEE 802.3.

Objective 2.2 Explain the basic switching concepts and the operation of Cisco switches

We have covered many parts of switching through this document. In this section we are going to step into some of the basic concepts and further on we will jump into some of the more in-depth sections. Switches are specially designed pieces of networking genius. I mean we all remember the Hub and Hub Twists and loved them so much, but when the switch came along and became affordable we all jumped ship quick. Switches have some very important key jobs that make it a switch.

Address learning – when a switch is first powered on it has no idea of what or who is plugged into it. Once the switch starts passing traffic the switch learns the locations of its connected devices. It starts the collection of MAC address and stores them in what is known as a MAC address table.

Forwarding and filtering decisions – When traffic is sent to a specific port that is located in the switches MAC table it will only send that traffic to that port of the destination address. Filtering is extremely efficient and leads to extremely fast switches.

Loop Avoidance – Loops are what they sound like. We create these knowingly for redundancy. But this can cause major problems if left alone. One of these problems is a broadcast storm; basically where a single piece of broadcast traffic keeps getting circled through the loop and using all the bandwidth of the switch. This has been known to bring a network to its knees and completely stop traffic just because of one loop. Switches have some built in loop avoidance known as Spanning Tree Protocol or STP.

Sub-objective 2.2.a Layer 2 addressing

Layer 2 addressing is a unique identification number for each device. This is known as a Media Access Control or MAC. A MAC address is like a serial number for each device connected to the network. A MAC is assigned to anything with a network interface. It could be any of the following:

- Ethernet
- Wireless
- Bluetooth
- IEEE 802.5 networks
- Fiber Distributed Data Interface (FDDI)
- Asynchronous Transfer Mode (ATM)
- Fiber Channel and Serial Attached SCSI (Part of the World Wide Name)

A MAC is made up with a 12 digit hexadecimal number 48 bits in length. There are a lot of people out there that refer to them as hardware or physical addresses. Traditionally the MAC addresses are written in two ways either with "-"or ":" separating the octets.

Example

00-50-56-C0-00-08

Or

00:50:56:C0:00:08

The first half of the MAC address or the first 3 octets, "00-50-56" is manufacturer assigned. Each manufacturer is assigned a set of MAC address prefixes by the Internet Standards Body. In my case the prefix MAC of "00-50-56" is a VMware address. The second half is a number assigned to the adapter by the manufacturer, typically the Serial Number of the interface, so the last half of mine is "C0-00-08" and this would be the Serial Number of my adapter.

Why the need for the MAC? If you look at the OSI model the MAC sits in the layer 2 or the Data Link Layer. The MAC address really is used for supporting the hardware implementation of the network stack. Also it is a constant number that does not change. In most cases it's actually "burned" into the hardware and you cannot change it. In some cases there are soft MAC addresses; like mine is from a VMware Workstation machine.

MAC addresses work together with IP addresses in helping to identify your network device; both of these addresses are stored in tables known as Address Resolution Protocol or ARP tables. This is a map between IP addresses and MAC addresses.

Sub-objective 2.2.b MAC Table

MAC tables – A MAC table is nothing more than a table that stores MAC addresses. When a switch receives traffic it gathers the port and MAC off of the traffic and stores it in the MAC address table. This allows the switch to create a street map of the switch.

CAM tables – Content Addressable Memory. This is where the MAC address is located. It's not really used in the switches today. But the term has stuck around.

A switch learns MAC addresses in a simple way. It listens to the incoming frames and stores the address and what port it came in on. The switch keeps an "Inactivity Timer" for the address entries. When a switch receives a new frame from a MAC that it has in its table it resets the clock to 0. The timer counts upwards and it knows the lowest is the newest and the largest is the oldest. When the MAC table's space fills it purges the oldest first.

Sub-Objective 2.2.c Flooding

Flooding is a way of a switch to find unknown destinations. When a switch gets traffic going to a destination it is not aware of it sends a unicast flood of traffic to all ports except the source port. This is not a broadcast.

A broadcast is where the source wants to send the info out to all ports.

Objective 2.3 Describe and configure enhanced switching technologies

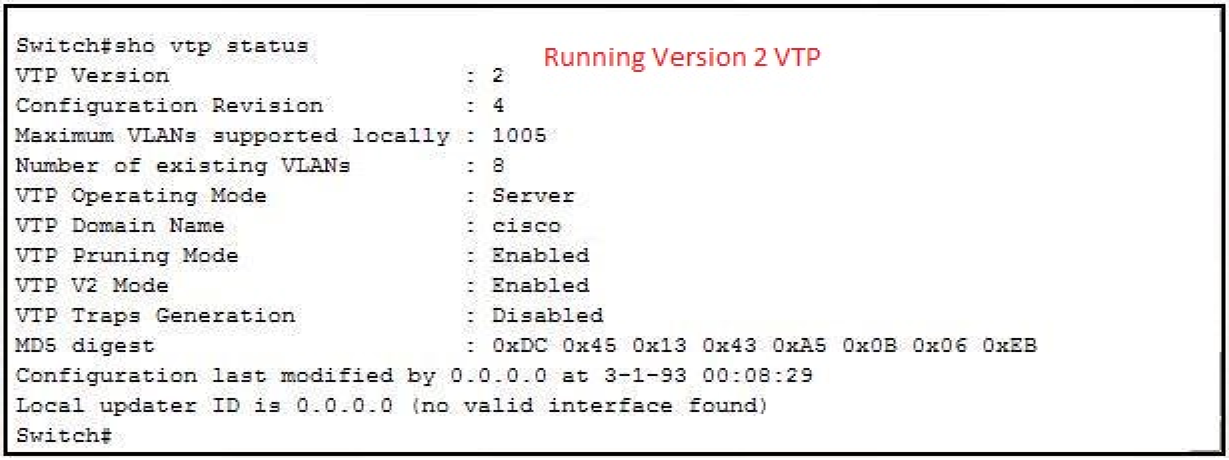
There are a series of enhanced features that are included in Cisco switches. VLAN Trucking Protocol (VTP) in short is really just management for VLAN across multiple switches. VLAN's are Virtual Local Area Networks, 802.1q Trunks, are the ports between two switches to send multiple VLAN's across one link. And then we have Spanning Tree Protocol (STP), which in simple terms is loop avoidance.

Sub-objective 2.3.a VTP

What is VTP? VTP stands for VLAN Trucking Protocol. Think of this more as a management for VLAN across multiple devices. You can use VTP to populate VLAN set up in one switch to other switches. When it propagates this information it uses the Trunk networks. So, if there is no trunk setup between two switches the VTP will fail. VTP is made as a Server / Client configuration. There is also an option to set a VTP configuration on a switch as "Transparent." When a switch is set as transparent it will forward VTP requests but the switch will hold its own VLAN database.

The VTP database is based on revision numbers. When a VTP server makes a change it changes the VLAN database. It increments the configuration revision number by 1 and then this propagates to all the clients participating in the VTP. On a Nexus switch VLAN 1 is used for VTP advertisements.

By default VTP is enabled. But the domain is set to NULL. Once you change the domain from NULL to a domain it will start propagating the VLAN database. Good word of thumb is to set a VTP password to keep unwanted switches from automatically joining the VTP domain. It will create some extra work because you will have to go to every switch and enter the VTP password but this will save you some headaches later.



```
Switch#sho vtp status
VTP Version                     : 2
Configuration Revision          : 4
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 8
VTP Operating Mode              : Server
VTP Domain Name                 : cisco
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xDC 0x45 0x13 0x43 0xA5 0x0B 0x06 0xEB
Configuration last modified by 0.0.0.0 at 3-1-93 00:08:29
Local updater ID is 0.0.0.0 (no valid interface found)
Switch#
```

Running Version 2 VTP

One feature that makes VTP nice is VTP Pruning. VTP Pruning is a way of cutting down on network traffic. If a switch only handles one VLAN the other switches will not send any traffic to it that does not match that VLAN. (FYI this can be done without VTP, you just need to change the allowed VLAN's to a Switchport)

Setting UP VTP domain requires you to turn on the feature in NEX-OS, because the feature is not enabled by default. To setup a VTP domain use the following commands.

feature vtp	– turns on VTP
show vtp status	– shows VTP status
vtp domain (Whatever you want)	– sets the domain.
vtp password (your password)	– sets the VTP password
vtp version 2	– enables VTP version 2

Setting up a VTP client

You must first setup up trunk port between the VTP server and the client switch.

feature vtp	– turns on VTP
vtp mode client	– sets VTP mode to client
vtp domain (Whatever you want)	– sets the domain.
vtp password (your password)	– sets the VTP password
vtp version 2	– enables VTP version 2

If you want to turn on VTP Pruning it has to be turned on at the server with the following commands:

vtp pruning   This turns on VTP pruning for the entire VTP domain.

Resetting VTP revision number is pretty easy. You can reset the number by simply renaming the VTP domain.

vtp domain (What you want to rename it to)   – This will reset the configuration counter to 0.

Sub-objective 2.3.b VLAN

VLAN – Stands for Virtual Local Area Network.

What is the real purpose of VLANs? Really this is meant to cut down on broadcast domains. It also cuts down hardware costs of physically splitting up the network.

By default VLAN 1 is enabled on most switches. This is the default VLAN for most traffic out of the box. To limit the broadcast domains and to segment up the traffic in your network most company's break up their network up into different VLANs. One key feature that must be in place in order for VLAN traffic to be passed is that the Route Processor (Layer 3 device like a Router or a Layer 3 switch) has to be present in the network for the traffic to move. In a Nexus OS switch VLAN 1 is used for Cisco Discovery Protocol (CDP) and Advertising VTP. Also Vlan1 defines a broadcast domain and cannot be deleted.

Commands to create a VLAN
vlan 10 - This creates the VLAN 10
name (Whatever name) - This names the vlan (This is common practice but does not need to be done)

To enable multiple VLAN's at a time.
vlan 10, 20, 30, 40-100 - This will create vlans 10, 20, 30, 40 through 100 all from one line.

show what vlans and setup
show vlan brief

There are two major different VLAN ports: Access Port and a Trunk Port

Access Port is typically one VLAN is assigned to a port. The switchport assigns the VLAN tag the traffic as it leaves the switchport. Most of the time the server is unaware that it is using VLAN tagging, then when the entering the switchport the VLAN tag is removed before it reaches the client.

Configure an interface to be a switchport access port.
switchport - to verify you are dealing with a switchport.
switchport mode access - Changes the port to a Access port
switchport access vlan 51 - Adds VLAN 51 to the allowed VLAN on the switch port.
show vlan brief - To show you added the VLAN to the port.
or
show interface ethernet ??/?? switchport - this will show the status of switchport on that interface.

Add a series of ports to a VLAN.
interface ethernet 3/3,e3/4,e3/5-22 - This will select the group of ports 3,4,5 through 22.
Then you can just add them to the switchport access and assign the VLAN like above. If done correctly when you hit enter after this command it should say (Config-if-range)

Trunk Port is typically carrying all VLAN's. Usually used between two switches or between a switch and hypervisor. The trunk port has a native VLAN. As a default standard VLAN 1 is the default VLAN port. It passes untagged packets for the native VLAN. It addresses

Configure an interface to be a switchport trunk port.
switchport - to verify you are dealing with a switchport.
switchport mode trunk - Changes the port to a trunk port
switchport trunk allow vlan 51 - Adds VLAN 51 to the allowed VLAN on the switch port.
Switchport trunk native vlan 2 - Sets native VLAN for trunk to VLAN 2
show vlan brief - To show you added the VLAN to the port.
or
show interface Ethernet ??/?? switchport - this will show the status of switchport on that interface.

Add a series of ports to a VLAN.
interface ethernet 3/3,e3/4,e3/5-22 - This will select the group of ports 3,4,5 through 22. Then you can just add them to the switchport trunk and assign the VLAN like above. If done correctly when you hit enter after this command it should say (Config-if-range)

SVI (Switch Virtual Interface)

SVI provides Layer 3 processing of VLAN packets for all switch ports assigned to that VLAN. SVI to VLAN are a 1 to 1 ratio.

Turning of SVI

feature SVI - Turns on the SVI feature set

interface vlan? - Enters VLAN(?) global configuration mode

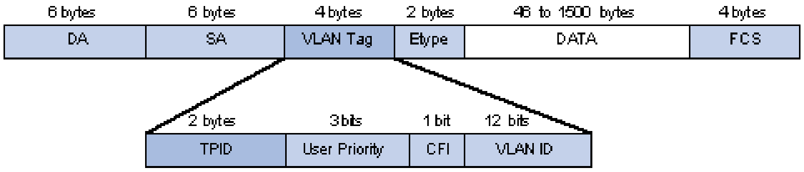
ip address (ip and subnet) - Assigns an Address and Subnet to VLAN?

ip name-server (ip address of name server) - Optional adds a DNS server

no shutdown - Makes sure the interface is not shutdown.

Sub-objective 2.3.c 802.1q

802.1q is a standard. Set forth by the IEEE. This standard was created to make a standard around VLANs on Ethernet network.



Total number of VLAN’s is 4096, 0 through 4095. The Nexus OS reserves 3968 – 4094. Why are we only allowed to use 4096 VLANS that is pretty simple math, we are only allowed to use 12 bits and each bit is either on or off. So you take 2 ^12 and you get 4096.

Sub-objective 2.3.d STP

STP – Spanning Tree Protocol

STP is built for loop avoidance. Its sole purpose in life is to disable the loops you build for redundancy in your network. The IEEE 802.1D is the standards for this protocol. STP is a layer 2 Protocol. Personally I think STP is quite a complex nightmare.

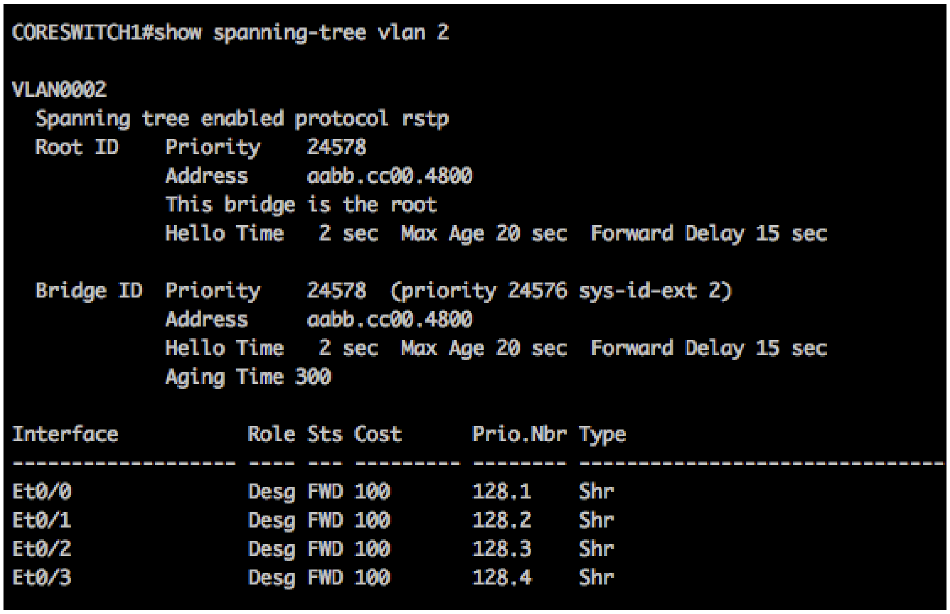
Determining a Root Bridge – This is determined by the lowest bridge ID.

How to get the Bridge ID: Are the addition of the MAC address and the Priority value of the switch.

The default Priority value is 32768 (increments of 4096)

Lower Priority value = higher priority

There are ways to guarantee who will win the Root Bridge the common way is to change the priority value. (Most of the time the root bridge is the oldest switch) so most people like to pick the newer switch.



```
CORESWITCH1#show spanning-tree vlan 2

VLAN0002
  Spanning tree enabled protocol rstp
  Root ID    Priority    24578
             Address     aabb.cc00.4800
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24578  (priority 24576 sys-id-ext 2)
             Address     aabb.cc00.4800
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Et0/0               Desg FWD 100       128.1    Shr
Et0/1               Desg FWD 100       128.2    Shr
Et0/2               Desg FWD 100       128.3    Shr
Et0/3               Desg FWD 100       128.4    Shr
```

show Spanning-tree - Shows the spanning tree info.

Section 3 Implement an IP addressing Scheme and IP service to Meet Network Requirements in a Medium-Size Enterprise Branch Office Network using Nexus

Overview

Through this section we are going to cover IPv4 and IPv6 addressing, subnetting, and also Number conversions.

This section makes up 12% of the material for the Exam according to Cisco.

Section 3 is made up of the following Objectives and Sub-Objectives.

Objective 3.1 Describe the operation and benefits of using private and public IP addressing.

- **Sub-objective 3.1.a Classful IP address**
- **Sub-objective 3.1.b RFC 1918**
- **Sub-objective 3.1.c RFC4193**

Objective 3.2 Describe the difference between IPV4 and IPV6 addressing schemes

- **Sub-objective 3.2.a Comparative address space**
- **Sub-objective 3.2.b Host addressing**

Objective 3.1 Describe the operation and benefits of using private and public IP addressing.

Public IP addressing is nothing more than what is routable on the internet. Public IP addresses are handled by the Internet Service Providers ISP around the world. When you get internet services you get the option of receiving a set of public IP addresses. These are used for services facing the internet. Like your webpage, DNS server, VPN, or software for your business, and so on. These are addresses that anyone from the internet can reach.

Private IP addresses are what they sound like; they are Private internal IP addresses. IEEE set aside 3 ranges of addresses for use inside the firewall of your business or home. These addresses are not public facing nor are they routable on the internet. The networks are 10.0.0.0, 127.0.0.0, and the 192.168.0.0 networks. These 3 networks are not routable, and intended as internal networks for your Local Area Network (LAN). These make up your workstations, switches, servers, and so on. In order to share these IP addresses on the internet you need to use Network Address Translation (NAT)

Sub-objective 3.1.a Classful IP address

The IP addresses are broke up into classes. Classes A, B, C are the normal classes we see, then there are two others, Class D and E. Class D is for broadcasts, and Class E is for future use.

	Class A	Class B	Class C	Class D	Class E
First Octet Range	1-126	128-191	192-223	224-239	240-255
Valid Networks	1.0.0.0 – 126.0.0.0	128.0.0.0 – 191.255.0.0	192.0.0.0 – 223.255.255.0	224.0.0.0 – 239.255.255.0	240.0.0.0 – 255.255.255.0
Total Number of Networks	2^7 – 2 = 126	2^14 = 16,384	2^21 = 2,097,152	Not Defined	Not Defined
Hosts per network	2^24 – 2	2^16 -2	2^8 -2	Not Defined	Not Defined
Octets (bits) in network part	1 (8)	2 (16)	3 (24)	Not Defined	Not Defined
Octets bits per host part	3 (24)	2 (16)	1(8)	Not Defined	Not Defined
Default Mask	255.0.0.0	255.255.0.0	255.255.255.0	Not Defined	Not Defined
First Octet Bit Order	0	10	110	1110	1111
Unicast or Multicast	Unicast	Unicast	Unicast	Multicast	Experimental
Reserved or Private Networks	127.0.0.0 Loopback 10.0.0.0 Private Network	172.16.0.0 – 172.31.255.255 Private Network	192.168.0.0 – 192.168.255.255 Private Network	UNK	UNK

Each network has two reserved addresses to each one. The first reserved address would be the all zeros in the host bits, this is called a Network address. Example 10.0.0.0 for a class A address. The second one would be all ones in the host bits, this is called a Broadcast address. Example would be 10.255.255.255. These two addresses cannot be used for host addressing. There is a local broadcast address that is reserved and its address 255.255.255.255. Also the loop back address is reserved 127.0.0.0. Then there is a Microsoft reserved address called the Auto Configuration address. This is used with a DHCP address and it is given the address of 169.254.???.???

Subnets – Are a group of IP addresses in the same network, the grouping process is done by TCP/IP.

Subnet masks are a way to group together a set of networks. A subnet mask is a 32 bit number also. It's represented by a Dotted decimal also for example 255.255.255.0 or it also be represented a Prefix Notation for example /24. A Prefix notation number is the number of ones in the Subnet Mask This is also known as a CIDR notation.

IP and Subnet work like a mailing address. Using subnets this makes moving across the network a little less complex. Routers store the Subnets to keep them from having to store every single IP, which in turn uses less overhead in the router.

Sub-objective 3.1.b RFC 1918

RFC 1918 is nothing more than a definition of Private Networks - are networks that are set aside for companies and homes to use. These networks are not-routable on the internet. Private networks use something called NAT or Network Address Translation. When you are using Private Network addresses you need to translate these to Public IP addresses. Where do you get the public IP address? You get these from your Internet Service Provider or ISP. They will issue you or your company your Public IP addresses. NAT works when your PC wants to view a webpage. Your traffic goes to the router. Your router uses NAT to translate your IP address from a private address to a public address and then forwards the traffic to the webpage. This is done so that the webpage can send the traffic back. If it stayed a private address you would never receive the return traffic, because Private Networks are not routable from the internet.

Network Class	Private Networks	Number of Networks
A	10.0.0.0	1
B	172.16.0.0 – 172.31.0.0	16
C	192.168.0.0 – 192.168.255.0	256

Sub-objective 3.1.c RFC4193

RFC4193 refers to IPv6. Are you still there? Okay don't be scared, IPv6 is not that bad. Yes it's different but if you look at it it's something that we need. Well let's go into this.

As I am sure you have heard many times, we are running out of IP addresses out there in the public network. Right now with IPv4 we only have about 4 billion addresses. And with IPv6 there are 4 times the binary spaces.

IPv6 address is huge. They are 128 bits long. IPv6 is displayed similar to IPv4 except its 16 bits separated by a colon. One big difference is instead of being displayed in decimal IPv6 is displayed in Hexadecimal. This allows 16 different combinations instead of 10 for each digit.

Example

2001:db80:0000:0001:0203:ffff:fee1:2a73

IPv6 assigns its own address. Yes I know IPv4 does too with DHCP but IPv6 can do so much more. IPv6 address can be assigned 4 different ways.

Static Configuration – Meaning it was manually assigned.

Stateless Auto Address Configuration (SLAAC) – The network adapter assigned its own address by looking on the network to make sure it is not conflicting with anyone else.

Stateful DHCP IPv6 – Is like IPv4 DHCP with some differences.

Stateless DHCP – This is a combo of SLAAC and Stateful DHCP. The network adapter gives itself an IP address and then asks a DHCP server for option codes. These are like the Default gateway, Time server and stuff like that.

A records are no more in IPv6. They are now AAAA records.

To make some address easer to write, there are some abbreviations that can help you out. The first shortcut is you can remove the leading zeros. This can be done on any 4 character grouping; you can just not type the leading zeros.

2001:0000:0000:0001:0203:ffff:fee1:2a73

Example of removing the leading zeros

2001:0000:0000:1: 203:ffff:fee1:2a73

Then there is the ability of removing long strings of zeros with a double colon. ***You can only do this once in an address***

For example

2001:0000:0000: 1: 203:ffff:fee1:2a73

2001::1: 203:ffff:fee1:2a73

IPv6 loop back address.

This one is not like the IPv4 counterpart. IPv6 address is at the beginning of the network.

Loopback: 0000: 0000: 0000: 0000: 0000: 0000: 0000: 0001
Short hand covered before is ::1

IPv6 has great migration capabilities, IPv6 allows you to run IPv6 and IPv4 side by side. This makes migration a little less cumbersome. There are two common methods, Dual Stack and Tunneling IPv6 inside IPv4.

Objective 3.2 Describe the difference between IPv4 and IPv6 addressing schemes

There are many differences between IPv4 and IPv6 but for me the two biggest ones are the extremely long addresses, and how many address there are.

IPv4	IPv6
32 Bit address	128 Bit address
About 4 billion addresses	Over 340 undecillion addresses or 2 to 128th
IPv4 address are binary numbers represented dotted decimal	IPv6 addresses are binary numbers represented in hexadecimals
IPsec support is only optional	IPsec support is built in
Fragmentation is done by sender and forwarding routers	Fragmentation is done on by sender
No packet flow identification	Packet Flow Identification is available within the IPv6 header using Flow Label field
Checksum Field is available in IPv4 header	No checksum field in IPv6 header
Option fields are available in IPv4 header	No option fields, but IPv6 extension headers are available.
ARP is available to map IPv4 addresses or MAC addresses	ARP is replaced with a function of Neighbor Discovery Protocol NDP
IGMP is used to manage multicast group membership	IGMP is replaced with Multicast Listener Discovery MLD messages
Broadcast messages are available	Broadcast messages are not available. Instead a link-local scope “All Nodes” Multicast IPv6 address is used for broadcast similar functionality.
Manual configuration (static) if IPv4 address or DHCP is required to configure IPv4 addresses	Auto-Configuration of addresses is available
Has an “A” record for DNS	Has an “AAAA” record for DNS
Needs NAT to translate private address to public address	No need for NAT
Designed before the global internet	Designed with massive global scale in mind

Sub-objective 3.2.a Comparative address space

Really I am at a loss for what goes here. But this seemed like a fitting place to put this info. We are going to cover Conversions and subnetting.

Conversions

Number conversion is going to be something that you need to know quite well for the test. But there are some simple methods to doing this. First off when you go in for your test on your paper they give you this chart. Start from right to left. Write 2 to the power of 0 and do this all the way through 7. Why because you have only 8 bits for the octet in an IPv4 address. Then do the math, 2 to the 0 is 1, 2 to the 1 is 2 and so on. From the 1 power you can just double the number from there.

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Converting from this chart is the best way that I have ever tried.

Decimal to Binary - Find the binary value of 72.

This is done by simply taking the number of 72 and finding the highest number that will go into it. And put a "1" under it. Then subtract that number from 72, so in our case 72-64=8, so now we repeat the steps with the number 8, and you continue to repeat this process till you have a zero left. If you look below we have two ones. Then you fill in the blanks with Zero's and that is your decimal number.

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
	1			1			

1001000 is binary for 72

Binary to Decimal – find the value for 10110111

This is the simplest way to convert, it's just addition. Put the numbers in the chart from right to left. Like below. Then add all the numbers with the one below them.

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	1	0	1	1	1

128+32+16+4+2+1 = 183

Hex is a bit different. Hex is base 16. If you have a number in hex most of the time you will see "0x" in front of the number. This is to let you and anyone else reading it that it's a hex number. Example: 0x542 is a HEX number of 542. Below are the hex values.

DEC	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
HEX	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

Hex to Binary

Hex to binary is pretty simple once you get the method understood. In hex each character represents 4 bits. The number conversion is a little bit different than Decimal to hex, but the same concept. For each character you will use your chart, starting from right to left. We are going to convert 0x 542

	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
	128	64	32	16	8	4	2	1
2					0	0	1	0
4					0	1	0	0
5					0	1	0	1

Then you lay the numbers out in the same order.

0101 (5) 0100 (4) 0010 (2) so your answer is 010101000010 and that is the Binary for 0x 542

Hex to Dec

Hex to Dec is a little more complicated. There are two ways you can do this. If you convert the Hex number to Binary first then convert from Binary to Decimal. Or you can do it by the powers method. As you know Hex is base 16, and the way to do this is to take each character value times 16 to the power of its position in the hex number. For 0x 542 it would look like this.

2 = 2   2*16^0 = 2

4 = 4   4*16^1= 64

5 = 5   5*16^2= 1280

Then you add up the answers of the above equations.

2+64+1280=1346 is the Dec for the Hex number of 0x 542.

Dec to Hex

This one is a bit more complicated, even more so for people that hate division. We will use the same number as before 1346. In order for us to convert this we need to divide this number by 16.

1346/16= 84 with a remainder of 2

We convert the remainder to Hex. Then we divide the 84 by 16. We continue this process until we get to a digit less than or equal to 16.

84/16=5 with a remainder of 4

We convert the remainder to Hex. And then we do the same with the 5 because it is less than or equal to 16. Then you write your number out from right to left.

0x 542 = 1346 in Dec

There is also another way to do Decimal to Hex conversion, or Hex to Decimal. I wanted to keep this a bit separate. We used it in the Hex to Decimal conversion. Here is the formula:

Value * (Base ^ Position) + Value * (Base ^ Position) + and so on.

For 0x 542 it would be 5*(16^2) + 4*(16^1) + 2*(16^0)= 1346 in Dec

IPv4 Subnetting – This is splitting up networks into smaller networks. This is done by changing the subnet mask to break up the network. Why would we subnet, really it's as simple as to cut down broadcast domains, and to enable more networks to be used off a single large network like a Class A or Class B or even a Class C network.

The math to figure out how many host in each network is pretty simple. Equation:

2^(number of host bits) – 2 = number of host in the network. (Why the minus 2, that is because the first and last address are reserved.)

Example:

IP Network = 172.25.0.0

Math – 2^16(using 16 host bits) – 2 = 65534 hosts.

Another example is: 255.255.254.0 = 2^9 – 2 = 510 hosts. (We only have 9 host bits in the subnet mask.)

To figure out how many subnets can be created from a network the equation is very similar.

2^(home many network bits being added)

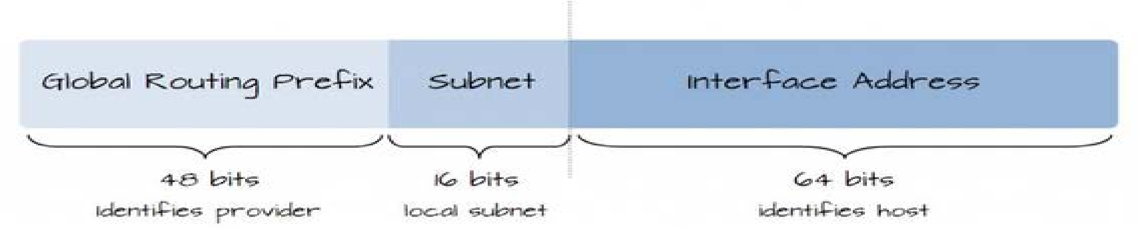
Example: 172.25.1.0 you would be using 8 network bits from the 1 value. So the math would look like 2^8 = 256 networks we could create.

You will need to know the above for the test. But in the real world you would be using a subnet calculator like the one on cisco.com https://www.cisco.com/cgi-bin/Support/IpSubnet/subnets.pl There are many other subnet calculators out there. And there are many calculators for your phone or tablet. But you cannot use these on the test so you need to learn how to do it the old fashion way.

IPv6 Subnetting

IPv6 address is made up with different segments.

The first 48 bits is made up of Global unicast, the second 16 bits is the subnet, and then the last 64 is the interface id or host.



Global Routing Prefix – This is designated by the Internet Service Provider (ISP)

Subnet – This is the local subnet

Interface Address (Host) – These are the host address bits.

Sub-objective 3.2.b Host addressing

I think we covered most of this in the past couple of segments but we are going to go into more detail of the ways IPv6 and IPv4 networks get their addresses.

DHCP IPv4 – Dynamic Host Configuration Protocol or DHCP is a way that a network device can receive a network address automatically. DHCP requires some configuration before it can work. You need a DHCP server in your network. This can be done with many devices but the most common in the corporate network is a DHCP server. This server can serve address in three different ways either by Dynamic Allocation, Automatic Allocation, or Static Allocation.

- Dynamic Allocation – An administrator reserves a range of IP for the server to assign to the clients. And when a client requests an address it hands one of the reserved addresses out.
- Automatic Allocation – The DHCP permanently assigns the IP address to the client. The DHCP server keeps a table of who has what IP address.
- Static Allocation – The DHCP server allocates an IP address to requesting client from a preset address mapped by the clients MAC address.

Static Configuration – Meaning it was manually assigned. This is just as it sounds when you setup the network card you manually assign the IPv6 address. This is normally done by the IT department for Routers, switches, and so on.

Stateless Auto Address Configuration (SLAAC) – SLAAC is a two-step process. The host learns what the subnet prefix is from the router from the NDP then the host calculates the interface ID and generates the IP address. EUI-64 rules.

Stateful DHCP IPv6 – Is like IPv4 DHCP with some differences. One big difference is that DHCPv6 updates the protocol messages to use IPv6 packets. DHCPv6 also uses solicit, advertise, request, and reply messages instead of using DORA.

Stateless DHCP – This is a combo of SLAAC and Stateful DHCP. The network adapter gives its self an IP address and then asks a DHCP server for option codes. These are like the Default gateway, Time server and stuff like that.

Section 4 Configure, Verify, and Troubleshoot Basic Router Operation and Routing on Cisco Devices using Nexus

Overview

This section is over half the exam. So if it was me I would spend the most time in this area. And from what I hear you need to pay extra attention to RIP. Routing is a big subject in general, and it's a fairly complex subject. This section is going to cover the Layer 3 features of a Nexus switch. This section makes up 52% of the material for the Exam according to Cisco. Please make sure to get out there and practice some on a Nexus OS.

Section 4 is made up of the following Objectives and Sub-Objectives.

Objective 4.1 Describe and configure basic routing concepts

Sub-objective 4.1.a Packet forwarding

Sub-objective 4.1.b Router look-up process (exec mode, exec commands, configuration mode)

Objective 4.2 Describe the operation of Cisco Routers

Sub-objective 4.2.a Router boot-up process

Sub-objective 4.2.b POST

Sub-objective 4.2.c Router components

Objective 4.1 Describe and configure basic routing concepts

Routing is nothing more than routing traffic based on a routing table. The routing table is built from different types of entries. One could be direct attached, meaning that it's attached to one of the routers interfaces. In another you can manually assign a Static entry. Dynamic could be another through different routing protocols like RIP, OSPF, and EIGRP. And lastly the router can learn a default route; this route can be learned dynamically or statically.

Sub-objective 4.1.a Packet forwarding

IP routing – The process of forwarding IP packets. This delivers the packets across the entire TCP/IP networks from the place the original packet builder to the destination device.

The forwarding process can be explained in 5 steps

1. Each data-link frame, the router chooses to process the frame based on the following.
   a. No errors in the frame.
   b. The frames destination is in the routers address table.
2. If the router chooses to process the frame, the router de-encapsulates the packet from within the frame.
3. Time to make the routing decision. Compare the packets destination IP address to the routing table; find the route that matches the destination address. The router then places the frame to the appropriate route.
4. Next step is to encapsulate the packet into a data-link frame appropriate for the interface it's leaving on.
5. Transmit the frame on the outbound interface of its choosing that matched the IP route.

There are a few different protocol methods that can be used for this, Distance Vector, Link State, or even a Hybrid.

Distance Vector Protocols, Is based on a router knowing the direction a subnet is located in and also a distance value for that subnet.

RIP – Routing Information Protocol. RIP measures distance (called a Metric) by hop counts. One of the bad things about this is that you start Routing by Rumor. Routing by Rumor is basing the location of a subnet on something it's not for sure the location. This can cause routing loops. RIP does have a maximum hop metric of 16 but 16 is considered an infinite distance and the route is considered unreachable, so in reality the max hop is 15, this limits the size, and is not really designed for the networks of today. Each RIP router transmits full routing updates every 30 seconds by default. RIP comes in two versions RIP v1 and RIP v2. RIP v1 is class less, and RIP v2 is class full.

Configuring rip commands

feature rip - Turns on the RIP feature

router rip (name) - This turns on the RIP and names the tag

To turn on RIP for an interface (Go under the interface and enter the following)

ip router rip (Name from above)

Link State Protocols

OSPF – Open Shortest Path First. OSPF bases its metric by default on the link bandwidth; this allows OSPF to make better route decisions than you can with hop counts. OSPF is a layer 2 protocol. OSPF uses a hello protocol to find its neighbors, and to make sure they are still there; this allows them to see link state. OSPF exchanges topology data with the routers it's directly connected to from its routes. The router chooses the best route to the subnet and adds it to its routing table.

EIGRP – Enhanced Interior Gateway Routing Protocol is more of a hybrid, it uses both link state features and distance vector features. EIGRP does not rely on the shortest path. It in turns relies on something known as the Defusing Update Algorithm (D.U.A.L). For a router that knows of two different ways to a destination, it can mark one as the best known path and enter it into the routing table. Then on the second route it can mark it as a feasible successor route, this is in place so if something happens to the best route its replace with the feasible path.

feature eigrp

router eigrp (anonymous system number)

To enable on a port (Go under the port)

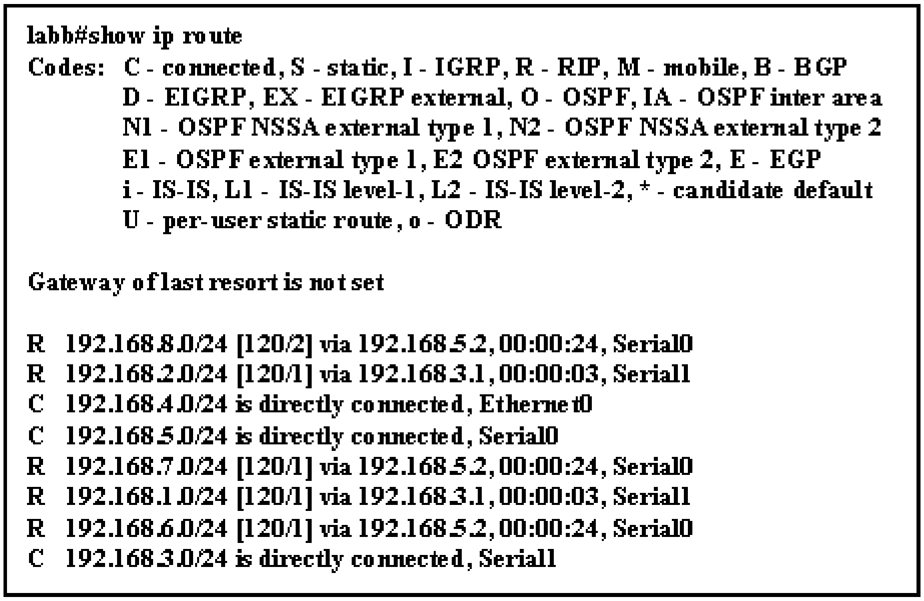
ip router eigrp (anonymous system number)

BGP – Border Gateway Protocol, This protocol is an external protocol. BGP is designed to advertise prefix from organization to organization.

Sub-objective 4.1.b Router look-up process (exec mode, exec commands, configuration mode)

Router look-up process

If you run the command of “show ip route” this will display something like this:



```
labb#show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
        U - per-user static route, o - ODR

Gateway of last resort is not set

R  192.168.8.0/24 [120/2] via 192.168.5.2, 00:00:24, Serial0
R  192.168.2.0/24 [120/1] via 192.168.3.1, 00:00:03, Serial1
C  192.168.4.0/24 is directly connected, Ethernet0
C  192.168.5.0/24 is directly connected, Serial0
R  192.168.7.0/24 [120/1] via 192.168.5.2, 00:00:24, Serial0
R  192.168.1.0/24 [120/1] via 192.168.3.1, 00:00:03, Serial1
R  192.168.6.0/24 [120/1] via 192.168.5.2, 00:00:24, Serial0
C  192.168.3.0/24 is directly connected, Serial1
```

If you notice at the top of the output screen it shows the Codes. These correspond to the letters on the lower left side of the routes. For example all the routes that are shown with the letter “C” those are directly connected to the router, if one of them was labeled with an “S” that would mean it’s a Static route.

There are two types of routes used.

Level 1 Routes

Default Route – Default route is an address of 0.0.0.0, this is the default route for the network.

Supernet Route – Network address with a mask less than the classful mask.

Network Route – has a subnet mask equal to the classful mask. A network route can be a parent route.

Ultimate Route – ultimate route either contains the next-hop IPv4 address or an exit interface. Directly connected, dynamically learned, and local routes are ultimate addresses.

Parent Route – is a network route that does not obtain a next-hop IP address or an exit interface. A parent route is reliant on a Level 2 Child route.

Level 2 Routes

Child Route – Is a route that is a subnet of a classful network address. Child routes are also part of a parent route. If a child route is removed so is the parent route. Level 2 child routes are also considered an ultimate route because it contains the next-hop IP address and/or an exit interface.

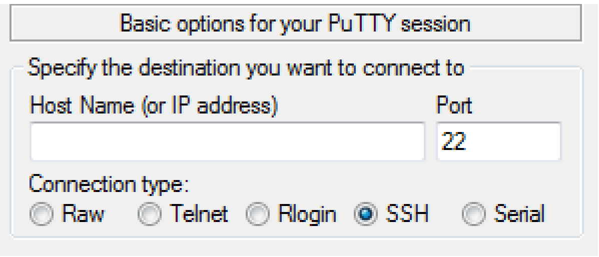
Exec Mode Commands

There are 3 ways to access a router. This can be done with Console, Telnet, and SSH.

Setting up a Terminal Emulator

One thing you will need is a terminal emulator to do configuration changes to the switch. I prefer a program called "Putty" it's simple and it works. But there are many other options out there, but I think putty is kind of the de facto standard.

On the main screen of the Putty session there is the option to change how you will be connecting.



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address)

Port: 22

Connection type:

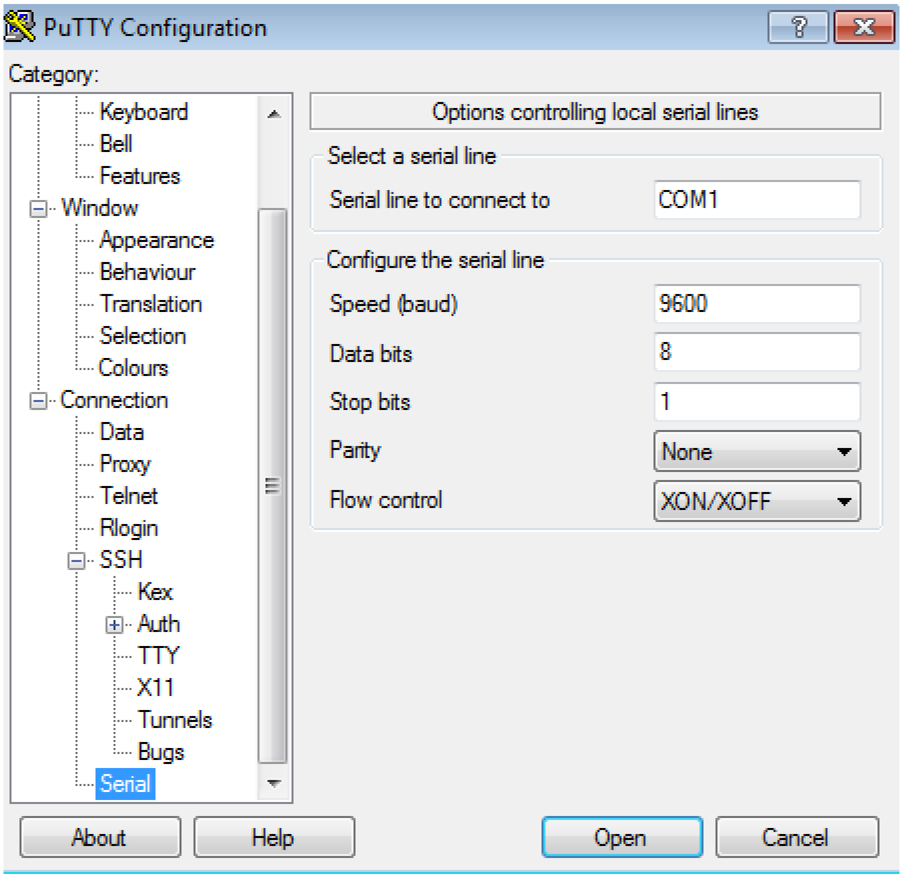
○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

This will allow you to switch between Serial Console, Telnet and SSH.

There are some default connection settings you may want to verify if you have connection issues. Cisco requires some parameters for the serial connection to work.

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

This is what the settings look like in putty. These settings are set by default and I have not found may reason to change them.



Options controlling local serial lines

Select a serial line

Serial line to connect to: COM1

Configure the serial line

Speed (baud): 9600

Data bits: 8

Stop bits: 1

Parity: None

Flow control: XON/XOFF

Console – Console connection is nothing more than connecting a physical connection to the device (This case a router) to a PC. There are two way to do this. The older cisco gear had a RJ-45 port labeled console. It was blue and required you to use a roll over cable and a RJ-45 on one end and a serial connector on the other end. Now a lot of the newer switches and routers are shipping with a Mini-USB connector so you can connect up a Mini-USB to standard USB between the router and your computer. (Must download Cisco console drivers)

Telnet – Telnet is a network protocol used to provide bidirectional text orientated communication. By default on a Nexus OS telnet is disabled by default. It is not a very secure method of configuring a switch or a router. It passes the traffic unencrypted, this includes sending the username and password in clear text.

SSH – SSH is more secure version of Telnet. It establishes a secure data connection with both devices. SSH for the most part operates just like Telnet just secure. Also by default, SSH is enabled on the Nexus OS.

VRF – Virtual Routing and Forwarding interface. Nexus switches use these by default for the purpose of separating management traffic between the servers and the rest of the network. By default Nexus places management interfaces into the management VRF and places all other interfaces in the default VRF.

For Common Router commands please look at the "Nexus Command Reference" at the end of this guide.

Objective 4.2 Describe the operation of Cisco Routers

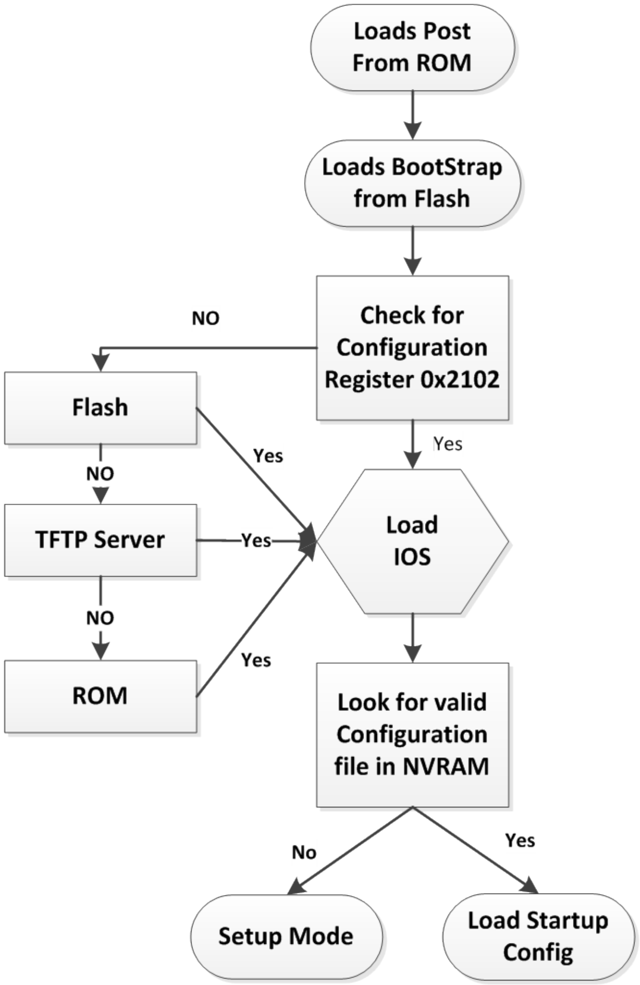
Cisco routers are designed to forward IP packets across the TCP/IP networks. They enable the ability to forward traffic between networks, inside and out. The routing process relies on network layer logic on routers and hosts.

5 step Routing Process
Decide whether to process the incoming frame
De-encapsulate the IP packet
Choosing Where to Forward the Packet
Encapsulating the Packet in a New Frame
Transmitting the Frame

Sub-objective 4.2.a Router boot-up process

Major phases of router boot-up process

- Test router hardware
    - Power-On Self-Test (POST)
    - Execute bootstrap loader
- Locate and Load Cisco IOS Software
    - Locate IOS
    - Load IOS
- Located and load startup configuration file or enter setup mode.
    - Bootstrap program looks for configuration file


Loads Post From ROM
Loads BootStrap from Flash
Check for Configuration Register 0x2102
NO
Yes
Flash
Yes
NO
TFTP Server
Yes
NO
ROM
Yes
Load IOS
Look for valid Configuration file in NVRAM
No
Yes
Setup Mode
Load Startup Config

You can also do the “show version” command to view information about the router during the boot process. Information like:

- Platform model number
- Image name and IOS version
- Bootstrap version stored in ROM
- Image file name & where it was loaded from
- Number and type of interfaces
- Amount of NVRAM
- Amount of Flash
- Configuration register

Output is in this format:

```
Cisco IOS Software, <platform> Software (<image-id>), Version <software-version>,
<software-type>
Technical Support: http://www.cisco.com/techsupport
Copyright (c) <date-range> by Cisco Systems, Inc.
Compiled <day> <date> <time> by <compiler-id>

ROM: System Bootstrap, Version <software-version>,  <software-type>
BOOTLDR: <platform> Software (image-id), Version <software-version>,  <software-type>

<router-name> uptime is <w> weeks, <d> days, <h> hours, <m> minutes
System returned to ROM by reload at <time> <day> <date>
System image file is "<filesystem-location>/<software-image-name>"
Last reload reason: <reload-reason>

Cisco <platform-processor-type> processor (revision <processor-revision-id>) with
<free-DRAM-memory>K/<packet-memory>K bytes of memory.
Processor board ID <ID-number>
<CPU-type> CPU at <clock-speed>MHz, Implementation <number>, Rev <Revision-number>,
<kilobytes-Processor-Cache-Memory>KB <cache-Level> Cache
```

Sub-objective 4.2.b POST

I am kind of stuck on this part. I cannot find a single document that goes into detail on the POST process.

POST is nothing more than a diagnostic program that runs to check the hardware on the router.

So really that is the limit of what I can find.

Sub-objective 4.2.c Router components

Major parts to the Router boot-up Process

- CPU – Executes the operating system instructions
- Random Access Memory (RAM) – Contains the running copy of the configuration file. Stores the routing table. The contents of RAM are flushed upon power off or a reboot.
- Read-Only memory (ROM) – Holds diagnostic software used when the router is powered up. The ROM also stores the routers bootstrap program.
- Non-volatile RAM (NVRAM) – Stores startup configuration. This may include IP addresses (Routing protocol, Hostname of the router)
- Flash memory – Contains the operating system (Cisco IOS)
- Interfaces – There are multiple physical interfaces that are used to connect network. I.E Ethernet, Fast Ethernet, Serial, DSL, ISDN, and Cable.

Reference Materials

Along with this Study guide I have found a chart that is extremely easy to memorize how to write it. I have created a Subnet and Number Conversion Chart. If you memorize how to write this out before the test you can enter the testing area and write it out before you begin the test and the paper they provide you with at the testing facility. So making the testing parts of Subnetting and number conversions simple as checking the chart. For me it something that helped my Dyslexic mind work through the subnet piece.

Also included below is a common Nexus Routing commands reference guide. I just made this to make it easy for me to remember the commands beings I don't have access to a nexus switch all day other than the simulator. Todd Lammle and John Schwarz made an amazing Nexus 7k simulator, download it and spend some time with it to learn the commands. Download link.

And the last piece I made a set of flash cards (You can laugh if you want but they work for Me.) to help me to get through most of this and learn what I though was important, or difficult for me to remember. I tried to break them up into sections so you can print off what ones you want. The big one for me was the OSI model. I think I spent the most time memorizing what each layer did and the protocols. I guess I better include my directions for them. Basically what I did was create an Excel worksheet that has 3 cards per page. Fold the page in half lengthwise and then I used a glue stick and glued the two half together then cut the card out.

One last thing, that I cannot stress enough is that you WILL want to go over the Nexus sales manuals.

Keyboard Shortcuts in the Nexus OS

Cursor Movement Shortcuts

Ctrl + A	Move cursor to the beginning of the line
Ctrl + E	Move cursor to the end of the line
Ctrl + F	Move cursor forward one character
Ctrl + B	Move cursor backward
Esc + F	Moves forward one word
Esc + B	Moves backwards one word
Ctrl + P	Previous command
Ctrl + N	Next command

Editing Shortcuts

Ctrl + W	Delete the word to the left of the cursor
Ctrl + U	Delete the whole line
Ctrl + T	Swap or transpose the current character with the one before it
Ctrl + K	Erase characters from the cursor to end of the line
Ctrl + X	Erase characters from the cursor to the beginning of the line
Esc + D	Delete from Cursor to end of word
Delete	Removes the character to the right of the cursor
Backspace	Removes the character to the left of the cursor

Up Arrow	Allows you to scroll forward through previous commands
Down Arrow	Allows you to scroll backwards through previous commands

Functional Shortcuts

Ctrl + L	Reprint the line
Ctrl + R	Refresh
Tab	Command autocomplete
Ctrl + C	Exit, Exit from config mode
Ctrl + Z	Apply the command line and exit from config mode

Less Common Shortcuts

Esc + C	Makes the letter at the cursor Uppercase
Esc + L	Makes the letter at the cursor lowercase
Esc + U	Makes letters from the point of the cursor to the end uppercase

Using the Delete Buffer

Deleted buffer is created from Ctrl + K, Ctrl + U, Ctrl + X	
Ctrl + Y	Paste the most recent entry in the deleted buffer
Esc + Y	Paste the Previous entry in the history buffer

Nexus Command Reference

This is not meant to be a complete guide to all the commands. This list is just what I could think of at the time and what I thought was important for the exam. There are thousands more commands and there is no sense in rewriting what Cisco has done for you. At the end there is the Official Command of this. Also there is a great reference guide here.

conf t or configure terminal- configuration terminal this is used to turn on configuration mode.

hostname - sets the host name of the device

feature ? – turn on a feature on the Nexus OS

no feature ? – disables a feature

show feature – displays all features and the state.

show version – shows OS version

show inventory – shows list of modules installed show interface ?? – shows the details on interface

show mac address-table – show mac address table

show license usage

show running-config – shows running config

feature SVI – turns on SVI

no switchport - To make a Nexus port a Routed port.

switchport – To turn a routed port into a switched port.

write erase boot – Erases the boot have to use “Reload” after command to get the Nexus switch to reload the default boot file

reload – forces the switch to reboot and reload the boot file.

reset – resets the nexus switch

shutdown – shuts down the nexus switch

vlan <???> - create vlan

no vlan <???> - delete vlan

feature vtp – turns on VTP

show vtp status – shows VTP status

vtp domain “name” – sets vtp domain to “name”

vtp mode client – sets VTP to client mode

vtp password “yourpassword” – sets the password to the vtp domain

vtp version 2 – enables vtp version 2

vtp pruning – turns on vtp pruning for the entire domain

NEXUS Official from Cisco Command Guides

Nexus 3000 Command Guides

http://www.cisco.com/c/en/us/support/switches/nexus-3000-series-switches/products-command-reference-list.html

Nexus 4000 Command Guides

http://www.cisco.com/c/en/us/support/switches/nexus-4000-series-switches/products-command-reference-list.html

Nexus 5000 Command Guides

http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-command-reference-list.html

Nexus 6000 Command Guides

http://www.cisco.com/c/en/us/support/switches/nexus-6000-series-switches/products-command-reference-list.html

Nexus 7000 Command Guides

http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-command-reference-list.html

Nexus 9000 Command Guides

http://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-command-reference-list.html

Conclusion

This has been a fun learning experience for me, and hopefully you. I have tried to give you the key points that I needed for this test. I tried to get as much information as I could into this without making it a book. This I just meant to be a study guide not the only method of studying, this just to help you cover the key points of the Exam outline.

This process took me through a massive amount of documentation, videos, and books. I want to reach out and say thank you to Wendell and Chad for creating a great book. It was very detailed and helped me through this. Also there is a wealth of information out there on the internet.

Also as a reference most of the Images in this were found on Google searches, so I can’t take credit for most of them. This Study guide is a mass collection of stuff found on the internet that I felt was useful in my study attempt.