updated April 2012

These notes cover the current 640-802 examination as the 'single exam option for CCNA' and the two stage examination track consisting of a basic 'ICND-1' examination (641-822) for CCENT certification and 'ICND-2' examination (640-816) to complete the CCNA certification using the kccvoip.net training.

The following notes may help narrow the study topics to the relevant areas. The 'Study Summary' for each section highlights the main items covered by the examination. *** This information is not supported or endorsed by Cisco Systems, Inc. *** please report any errors/comments.

NOTE the actual Vue/Pearson examinations DO NOT ALLOW you to go back and change or mark any questions, as many other demo and training examinations do. **AND** not all questions are multiple choice and may require you to fill in the blank, drag & drop responses, telnet simulation or input your response to a diagrammatic exhibit (for a demonstration see the Cisco CCNA simulation demo on CCO). The simulation questions will accept the usual abbreviated commands (sh = show, int = interface etc..) but will not allow many of the help commands as seen on the real hardware (?, show? etc.). Be prepared to configure an interface, setup a routing protocol and diagnose problems with interface and routing configuration without the use of the Cisco context help system found in the real routers and switches. Long gone are the protocols of Novell, IPX/SPX, Appletalk, and several items from LAN switching replaced by the requirements for increased depth of knowledge required on the OSI model, basic WiFi, some VPN, security, basic IP version 6 and updated WAN technologies etc.

see also CCNA example questions, IOS Configuration Examples, (links via kccommunications.com/public)

If you have study materials from the old 640-801 exam - Compare exam versions 640-801 to 640-802 (change over was November 6th 2007) you cheapskate ☺

The Vue / Pearson tests can be booked online via www.vue.com/cisco (since Cisco changed from Thomson/Prometric to Vue/Pearson there seems to be less testing centers available outside of the US, so check on their web site for centers and schedules in your area)

Cisco IOS Study Summary

The new examinations use a syllabus based upon extracts from **12.4 IOS** commands and basic knowledge of the current 'small enterprise' network devices including the 29xx Catalyst series switches, 26xx/18xx/28xx/29xx/39xx… 'standard G1 IOS' routers. The 2500 and 2600 are still excellent training routers and are available at very low cost, but any of the low end Cisco routers can be used provided they will run a full IOS. Any IOS version above 12.2 will provide 90% of the commands you need (SDM functionality and some of the manager commands will be missing). Any of the low end Catalyst switches can also be used to become familiar with the CCNA requirements for VLANs, VTP and trunking etc.

The following document is used as checklist within the KCC CCNA FastTrack Course;

- Switch and Router differences and connections via Console, Auxiliary and Telnet options (rollover cables, cross cables, serial setup etc.)
- Router configuration, (memory use and functions… RAM, FLASH, ROM, NVRAM)
- Router and Switch CLI (Command Line Interface) and exec mode basics for ;
    - key sequences for edit and recall etc. {lab #1}
    - basic boot system commands {lab #3}
    - file system commands and tftp functions [NOTE... the CCNA exam ignores the use of FTP for IOS file transfers on larger routers and states only tftp can be used for IOS file transfer] {lab #1}
    - system messages commands for logging etc. {lab #1}
    - interface configuration and monitoring {all labs}
    - CDP functions {all labs}
    - setup menu commands etc. {lab #1}
    - hostname, banner, prompts etc. {lab #1}

(lab numbers refer to the kccvoip.net training handout schedule)

BASIC IOS FUNCTIONS REQUIRED BY CCNA; (PRACTICE !)

FUNCTION	**COMMAND** (may be abbreviated to first few non-ambiguous characters of each command)
go into enable (privileged mode)	enable
exit from enable mode	disable
logoff (leave the router)	quit *or* exit *or* logoff
previous command from history	<up arrow> *or* <Ctrl-**P**>
next command from history	<down arrow> *or* <Ctrl-**N**>
move **f**orward one character	<right arrow> *or* <Ctrl-**F**>
move **b**ack one character	<left arrow> *or* <Ctrl-**B**>
auto completion of command	<tab>
break (default)	<shift-Ctrl-6> <x>
stop ping/trace	<shift-Ctrl-6>
refresh console line	<Ctrl-L>

BASIC IOS ADMIN FUNCTIONS REQUIRED BY CCNA;

(PRACTICE !)

FUNCTION	**COMMAND** (may be abbreviated to first few non-ambiguous characters of each command)
enter terminal configuration mode (from the enable mode)	*Router* # configure terminal
exit terminal configuration mode	*Router (config)*# <Ctrl-Z> *or* exit (each level of context)
drop back one level of context within config	*Router (config-int)*# exit *Router (config)*#
copy config from tftp server to RAM	*Router* # copy tftp running-config
save/copy running-config (RAM) to NVRAM	*Router* # write memory *or* copy running-config startup-config
copy file from tftp server to flash memory	*Router* # copy tftp flash
copy file from flash to tftp server	*Router* # copy flash tftp
delete start-up (NVRAM) configuration	*Router* # write erase *or* erase startup-config
view IOS version information	*Router* > show version
view current configuration (RAM)	*Router* # show running-config *or* write terminal
view saved (startup) configuration	*Router* # show config *or* show startup-config
view basic files system (flash)	*Router* # show flash (or dir)

view router utilization	*Router* # show processes
disable CDP for entire router	*Router (config)* # no cdp run
disable CDP on an interface	*Router (config-int)* # no cdp enable
show interfaces and ip addressing	*Router* > show ip interface brief
show routing table	*Router* > show ip route
show routing protocols for ip	*Router* # show ip protocol
show ip arp table	*Router* # show ip arp

NOTE:CCNA makes use of 'standard catalyst' 29xx switches and 'standard G1 IOS' routers (26xx,18xx,28xx,29xx,39xx,72xx etc)

Get plenty of practice configuring routers and switches doing the basic interface addressing, basic routing, trunks, vlans etc.. you will need to configure a simulated network in the exam.

see also IOS Configuration Examples, configuration register settings for password recovery

OSI Reference Model Study Summary

- OSI Reference model & examples (table below)
- Connectionless and connection oriented protocols
- Data Link protocol functions (Arbitration, Addressing, Error Detection & Types)
- Layer 3 protocol address structures (IP, OSI), network/host field sizes
- Frames, Packets and Segments (layer 2,3 & 4)
- Flow control methods (buffering, congestion avoidance and windowing)
- MAC address functions (NIC, LAA, Unicast, Multicast, Broadcast)

NETWORK LAYER UTILITIES;

REMEMBER

ARP Address Resolution Protocol will resolve a mac address from a given ip address. A device may send an ARP broadcast to ask every station on it's network for the mac address of a given IP address. **REMEMBER HOW** the ip address and mask dictate if the device should send traffic to it's local network or to it's gateway.

DNS Domain Name System will resolve domain names to IP addresses. So a device looking for cisco.com will request a domain lookup from it's DNS server to be able to send traffic to the IP address of cisco.com (and then using ARP to resolve the IP address of cisco.com to a mac address in order to send it's traffic)

DHCP Dynamic Host Configuration Protocol can be used to supply IP addresses to any device either via static configuration (mapped to mac address) or via a pool of addresses. DHCP can also provide much more information to the end device such as multiple DNS server addresses and TFTP server addresses etc.

OSI MODEL AND EXAMPLES;

OSI Layer Name	Description	Example
Application layer 7	Application / user interface (including user authentication etc)	Telnet, HTTP, FTP, SMTP, SNMP, VoIP, POP3, FTP
Presentation layer 6	Data translation /presentation / encryption	JPEG, EBCDIC, ASCII, GIF, MPEG, MIDI, Encryption....
Session layer 5	Session control, allocation/tracking	op systems, SQL, NetBIOS, DECnet
Transport layer 4	Multiplexing /control, Data delivery using flow control and error recovery & segmentation etc	TCP, UDP, SPX
Network layer 3	logical addressing and path determination (routing)	IP, IPX, AppleTalk, X.25
Data Link layer 2	frame construction, mac addressing, error detection using frame check sequence (switching)	802.2/802.3, VTP, HDLC, ATM, PPP, Frame Relay, Ethernet, CDP.....
Physical layer 1	Electrical connections & signals… physical media	Cables specifications; RJ45, V.35, EIA232, Ethernet

THERE ARE **ALWAYS SEVERAL** QUESTIONS ON THE OSI MODEL !!

TCP/IP Layer Name	Description	Example
Application	Application / user interface / Presentation and session control) maps to Layers 5, 6 & 7 of OSI	Telnet, HTTP, FTP, SMTP, SNMP, VoIP, POP3, FTP
Transport	Multiplexing /control, Data delivery using flow control and error recovery etc .. maps to Layer 4 of OSI	TCP, UDP
Internet	logical addressing and path determination maps to layer 3 of OSI	IP
Network Access	Maps to Layer 1 & 2 of OSI model = mac protocols & physical media etc	802.2/802.3, PPP, Frame Relay, Ethernet, CDP.....

REMEMBER;

CONNECTIONLESS TFTP, UDP, 802.3, 802.5.... (most layer 3)

CONNECTION ORIENTED (i.e. requires end to end communications) LLC2, 802.2, TCP/IP, SPX, X.25, Frame Relay, ATM, PPP, xDSL.....

'SAME-LAYER INTERACTION ON DIFFERENT COMPUTERS' = two computers using the same protocol to communicate

'ADJACENT-LAYER INTERACTION ON SAME COMPUTER' = a single computer making use of the protocol stack where one layer provides a service to an adjacent layer within the OSI model

Bridges/Switches, LAN Design Study Summary

- Protocol Type Fields and header formats – basic knowledge
- Ethernet Standards (mac specifications, **cable lengths & types**)

  KNOW the definitions of ; collision domain, broadcast domain and network segment !

- Spanning Tree basic functions (now including RSTP 802.1w and PVSTP) – no need to know the timing and protocol details, but **essential to know the port naming, election procedure, bridge ID and basic spanning tree functionality.**
- VLANs overview inter-vlan routing, collision domain / broadcast domain and segments
- **Trunking/Tagging Protocols & VTP basics** (VTP modes, tagging specifications ISL/802.1q)
- switching methods (see table below)
- Switch port security – know the methods and configuration commands

Switching Methods;

Store and Forward Switch port fully receives all bits in the frame before forwarding the frame. The switch checks the FCS in the Ethernet trailer before forwarding the frame.
Cut Through Switch performs an address lookup as soon as the destination field header has been received. The first bits in the frame can be sent out before the final bits of the incoming frame are received, therefore the FCS can not be checked.
Fragment Free Switch acts in the same way as cut through switching, but waits for 64 bytes to be received before forwarding to ensure collision errors did not occur. The FCS is not checked.

NOTE fortunately, the CCNA no longer requires knowledge of the 'odd' 1900 switches ☺

Catalyst 29xx and other low-end catalyst switches now tend to use a more 'standard' Cisco operating system (we no longer need the strange 1900). All have a separate VLAN-database configuration mode in addition to the 'config' mode and use an IOS format. {LAB #9} Larger switches such as Catalyst 6500 etc. use can CatOS or a Hybrid combination of IOS/CatOS on the switching processors and some have separate IOS on the layer-3 routing processors - fortunately, the CatOS is no longer required for CCNA .

IF you have access to high-end switches such as the 3560,3750… etc. turn off the layer-3 capabilities – the CCNA is not supposed to know about those features. For CCNA study use only layer-2 switching – turn them on again in the real-world and after you have passed the exam.

REMEMBER: VTP MODES on all Cisco Catalyst switches (flooded every 5mins & when ever there has been a change);

Function	Server	Client	Transparent
source VTP messages	yes	yes	no
listen to VTP messages	yes	yes	no
create/edit/delete VTP messages	yes	no	local
save VTP messages	yes	no	local

TRUNK/TAGGING DETAILS;

- **Cisco's ISL encapsulation (adds 26 bytes overhead) tagging** for VLAN identification for Fast Ethernet or Gigabit Ethernet links only - although now phased out in new switches
- **802.1Q is the IEEE standard** (subset of Cisco's ISL) for VLAN tagging **adds a 4 byte shim** (they will ask in the exam)
- 802.10 tagging on FDDI {history}

- LANE tagging on ATM {history}
- DISL is Cisco's first generation trunk establishment protocol
- DTP is Cisco's second generation of trunk establishment protocol
- VTP is Cisco's method for distribution of VLAN configuration information
- VTP pruning increases available bandwidth by restricting flooded traffic to contain only the required/configured VLANs for that trunk and not sending all available VLAN information

see also VLAN Overview

Network Protocols Study Summary

- TCP/IP (RFC 793, UDP, **port numbers and type numbers** (RFC 1700), DNS, ARP, ICMP)
- **IP Addressing and classes** (subnet masking before VLSM), default routes … **ESSENTIAL YOU CAN CALCULATE VLSM ADDRESSING FAST !!!!!**
- **Classful addressing and VLSM & CIDR** (basic knowledge)
- **Encapsulation in IP**
- **IP and MAC addressing flow**
- **DNS, DHCP and general WEB traffic flow**
- **NAT addressing terms** (very basic knowledge)
- **FTP TFTP (basic knowledge of commands and functions)**
- **IOS commands** (CCNA sub-set of commands – see below)
- **SSH** (know the steps to configure SSH on a switch and the principal of RSA public/private key exchange)
- **Basic Network Management functions** (SNMP version1 and version2)
- **KNOW CDP and what it can show, how it can help fault finding**

common IP configuration commands; (practice these commands !)

show ip protocol	view routing protocols in use for ip
show controller {serial | ethernet | ...}	view controller for interface (check cable type etc)
show debug	view current debug setting
show version	view config register, device spec and current IOS etc
ip address ip-address mask {secondary}	configure an IP address on to an interface
debug ip packet	diagnose & view all IP packets
ip domain-lookup	configure use of dns

ip netmask-format {*bitcount* | *decimal* | *hexadecimal}*	format configuration for interface address view
show ip arp {mac}	view IP arp table
ip host *name {tcp-port-number} address1 address2...*	configuration of host table
ip route *prefix mask {next hop | output interface}*	configure static route
ip name-server *server address1 {server address2...}*	configure name server(s) for DNS
no ip domain-lookup	switch OFF DNS lookups from this device for management (default is ON)
show clock	view date and time setting
clock set {HH:MM:SS DD MMM YYYY}	set date and time for this device
show ip interface *{brief}*	view IP interface details
show ip route {*subnet}* {protocol}	view IP routing table

see also IOS Configuration Examples, well known tcp port numbers, NAT & PAT

WiFI – CCNA NEED TO KNOW;

WiFi WLAN Mode	Description	Cisco exam 'phrase'
Ad hoc (peer to peer)	Two devices communicate directly without the use of an AP	Independent Basic Service Set **(IBSS)**
Infrastructure mode	Single AP – single LAN	Basic Service Set **(BSS)**
Infrastructure mode with more than one AP	Multiple AP – one wireless LAN allowing roaming	Extended Service Set **(ESS)**
IEEE STANDARD	Description	Channels available
802.11a (OFDM)	54Mbps using 5GHz	12 non-overlapping
802.11b (DSSS)	11Mbps using 2.4GHz	3 non-overlapping
802.11g (OFDM)	54Mbps using 2.4GHz	3 non-overlapping

REMEMBER - WiFi is effected by metal filing cabinets, DECT wireless telephones and building structures. (270 to 300 feet line of sight range)

SECURITY STANDARD	Description	Encryption Level
WEP	Static key, weak authentication, no user authentication	weak
Cisco proprietary	Dynamic key, Device authentication, 802.1x user authentication support	TKIP good
WPA (WiFi Protected Access)	Static & Dynamic key, Device authentication, 802.1 x user authenticationsupport	TKIP good
802.11i (WPA2)	As above	AES excellent

ROUTING Study Summary

- **Know the functions and basic differences** between RIP 1, RIP2, IGRP, EIGRP and OSPF - which are distance vector, classful/VLSM, link state….
- **Know the defaults** for the various routing protocols (hello times, split horizon, poison reverse, admin-distance, metric types) – sequences for failed routes etc…
- **Comparison of routing protocols** optimization (brief overview)
- **very brief** knowledge of BGP - see table below
- **Tunneling** (basic knowledge - GRE, IPv4 & IPv6)
- basic router IOS commands for **configure and manage** the routing protocols (be able to configure and troubleshoot)
- NOTE – CCNA level **ignores** the use of 31 bit masks
- NO NEED FOR detailed IPv6 routing knowledge, just basic IPv6 addressing

See also the CCNA Routing Reminder guide

CCNA required details **(in RED);**

PROTOCOL	RIP 1	RIP 2	IGRP	EIGRP	OSPF	BGP
TYPE	DISTANCE VECTOR	DISTANCE VECTOR	DISTANCE VECTOR	BALANCED HYBRID/DV	LINK STATE	PATH VECTOR/DV
LOOP PREVENTION	HOLDDOWN, SPLIT HORIZ	HOLDDOWN, SPLIT HORIZ	HOLDDOWN, SPLIT HORIZ/DUAL	DUAL/FEASABLE SUCCESSOR ..	DIJHSTRA SPF ALGORITHUM + TOPOLOGY DATABASE	AS PATH
VLSM SUPPORT	NO	YES	NO	YES	YES	YES
ADMIN DIS	120	120	100	summary=5 internal=90 external=170	110	internal=200 external =20
UPDATE	30 sec	30 sec	90 sec	triggered	triggered and 30mins	config
METRIC	hops	hops	BW + DELAY	BW + DELAY	cost	med, local pref, weight, AS-Path .... etc. LOTS !
HOLDDOWN	180 sec	180 sec	280 sec	3 x hello	(max age = 1 hour)	config
FLASH UPDATES	NO	NO	YES	YES	YES	YES
HELLO	NO	NO	5 to 60 sec	5 to 60 sec	10 to 30 sec	keepalive
INFINITY	16 hops	16 hops	4M (+255 hops)	64M (+255 hops)	64k	config
AUTO SUMMARY	FIXED	FIXED	FIXED	default = auto	default = no auto	config
CONNECTION	broadcast UDP port 520	multicast 224.0.0.9 UDP port 520	broadcast IP protocol #9	multicast 224.0.0.10 (IP protocol #88)	multicast 224.0.0.5/6 (IP protocol #89)	TCP 179
RFC	1058	1723		Cisco	1247, 1583	1771
MAX PATHS	1-16 (default = 4)equal costs only1-16 (default = 4)	1-16 (default = 4)equal costs only1-16 (default = 4)	1-16 (default = 4) load balancing over non-equal paths also using VARIANCE 1-16 (default=4)	1-16 (default = 4) load balancing over non-equal paths also using VARIANCE1-16 (default=4)	1-16 (default = 4)equal costs only1-16 (default = 4)	config
AUTHENTICATION	NO	YES	NO	YES	YES	YES

REMEMBER:

- STATIC ROUTES have admin **distance of 1** by default
- FLOATING STATIC ROUTES are configured to have an admin distance just above dynamic routing protocol admin-distance-value in use to make them less desirable than a dynamically available route and therefore available as a backup route
- CONNECTED ROUTES have admin **distance of 0**
- It is worth remembering the main values (in RED) from the above table

PRACTICE SUB-NET CALCULATIONS !!! There are **ALWAYS several questions** involving sub-net masks, gateway and addressing where you have to calculate the network, sub-net and quantity of addresses available within the sub-net etc…

WAN Protocols,

- Point to Point leased lines, cabling standards, interface standards (V.35,RS232,X.21), line speeds….DS0=64kbps, DS1=1.544Mbps=T1 (24 x DS0), DS3=44.736Mbps=T3, J1=E1=2.048Mbps (32 x DS0), E3=34.064Mbps,
- PPP (authentication, Multilink, multi-protocol, error detection) WAN
- **Very brief** overview of , xDSL, dialup and cable modems etc.
- Frame Relay Terms & Concepts (DLCI, LAPF, RFC 1490/2427) LMI functions and encapsulation types (FECN, BECN)
- HDLC (Cisco default) remember Cisco protocol type field

PPP NOTES TO REMEMBER;

PPP was designed for multiprotocol interoperablity and provides several features in addition to synchronization and framing

Function LCP feature description		
Multilink Support	multilink ppp	allows load balancing over multiple lines (bundles)
error detection	LQM (Link Quality Monitoring)	PPP can take a link out of circuit based upon the percentage of errors detected. LQM provides error percentages based upon lost packets over packets sent (in both directions)
Looped Link Detection	magic numbers	each end of the link sends 'magic numbers' and can recognize it's own magic

		number should the link be looped
Authentication	PAP and CHAP	Password Authentication Protocol (clear text) and Challenge Handshake Authentication (MD5 encrypted)
Compression	STAC ,Predictor and MPPC	three compression options

Summary of **access lists** required by CCNA;

Command Configuration & use	
access-list {**1-99**} {permit | deny} *source-address* {*source mask*}	global command for **STANDARD NUMBERED IP** ACCESS LIST
access-list {**100-199**} {permit | deny} *protocol source-address* {*source mask*} {options} *destination-address* {*destination mask*} {options}	global command for **EXTENDED NUMBERED IP** ACCESS LIST
access-list {200 - 299} {permit | deny}	protocol type access lists
ip access-group {*number* | *name*} in | out	interface sub-command to **activate ip list on interface**
ip access-list {standard | extended} *name* global command for **named access-lists**	show access-list {*list-number}* view all (or selected) access lists and hits
show {*ip* | *ipx* | *appletalk*} access-list	view single protocol access lists

Type of Access List Matching functions available	
IP STANDARD ACCESS LISTS (1 - 99)	Source IP address or portions of source address
IP EXTENDED ACCESS LISTS (100 - 199)	as above plus; destination IP address, portion of destination address, protocol type (TCP, UDP, ICMP etc..), source port, destination port, established (checks only first time), IP TOS, IP precedence