CCNA Cheat Sheet
Internetworking Essentials

Internetwork Training

OSI Model vs. TCP/IP Model

OSI Reference Model

Application - Identifying and establishing the availability of intended communication partner and whether there are sufficient resources

Presentation - Data translation, encryption, code formatting

Session - Setting up, managing and tearing down sessions. Keeps application's data separate

Protocol Data Units (PDUs)

Segment: **Transport** - Provides end-to-end transport services - establishes logical connections between hosts. Connection-oriented or connectionless data transfer.

packet: **Network** - Manages logical addressing and path determination

frame: **Data Link** - Provides physical transmission of data, handles error notification, flow control and network topology. Split into two sub layers (LLC and MAC)

bits: **Physical** - Specifies electrical, mechanical, procedural and functional requirements for activating, maintaining and deactivating a physical link.

TCP/IP Model Protocol Suite

Process/Application layer
FTP - TCP file transfer service – port 20-21
Telnet - Terminal emulation program – port 23
TFTP - UDP file transfer – port 69
SMTP - Send email service – port 25
DHCP – Assigns IP addresses to hosts – ports 67 and 68
DNS – Resolves FQDNs to IP addresses – port 53

Host-to-Host layer
TCP - Connection-oriented protocol, provides reliable connections (acknowledgments, flow control, windowing)
UDP - Connectionless protocol, low overhead but unreliable

Internet layer
IP - connectionless protocol, provides network addressing and routing
ARP - finds MAC addresses from known IPs
RARP - finds IPs from known MAC addresses
ICMP - provides diagnostics, used by ping and traceroute

Network Access

General Troubleshooting

Troubleshooting Steps

1. Ping 127.0.0.1 (Loopback)
2. Ping default gateway
3. Ping remote device

Cisco Ping & Response Codes

Router> ping 172.15.9.1

!	Success
.	Timed out waiting for reply
U	Destination unreachable
|	Ping process interrupted
?	Unknown packet type
C	Congestion-experienced
&	Time to live exceeded

Windows DOS Troubleshooting Commands

- ping 127.0.0.1
- tracert
- ipconfig/all
- arp -a

Cisco Trace Command & Responses

Router> traceroute 172.15.9.1

*****	Timed out
!H	Router received packet but did not forward it
N	Network unreachable
P	Protocol unreachable
U	Port unreachable

IP Classes

Class Ranges

Class A - 1-126 - network.node.node.node
Class B - 128-191 - network.network.node.node
Class C - 192-223 - network.network.network.node

Private Address Ranges

Class A - 10.0.0.0 - 10.255.255.255
Class B - 172.16.0.0 - 172.31.255.255
Class C - 192.168.0.0 - 192.168.255.255

CIDR Notation (Classless Inter-Domain Routing)

255.0.0.0	/8
255.128.0.0	/9
255.192.0.0	/10
255.224.0.0	/11
255.240.0.0	/12
255.248.0.0	/13
255.252.0.0	/14
255.254.0.0	/15
255.255.0.0	/16
255.255.128.0	/17
255.255.192.0	/18
255.255.224.0	/19
255.255.240.0	/20
255.255.248.0	/21
255.255.252.0	/22
255.255.254.0	/23
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30

Cisco 3-Layer Hierarchical Model

Core - *Backbone*, common to all users, needs to be as fast as possible and fault tolerant, avoid ACL, VLAN trunking and packet filtering here.
Distribution - *Routing* - provides access control policies, filtering, WAN access and VLAN trunking
Access - *Switching* - User and workgroup access, segmentation

Patch Cable Types

Straight-through - Connect PC to hub or switch (router to switch or hub)
Crossover - Connect hub to hub/ switch to switch/PC to PC
Rolled - Console connection for PC to router

Half Duplex Ethernet shares a collision domain resulting in lower throughput than **Full Duplex Ethernet** which requires a point-to-point link between two compatible nodes

Causes of LAN congestion - Broadcast storms, too many hosts with a broadcast domain, multicasting, low bandwidth, bottlenecks

Collision domain - Switches/bridges breakup collision domains, hubs extend them

Broadcast domains - Routers and VLANs breakup broadcast domains

Network Devices

Physical Layer (Layer 1) Devices
These devices extend collision domains, increase traffic problems and reduce network bandwidth.

- *Transceivers* – Connect one media type to another e.g. Fiber to copper
- *Repeaters* – Used to extend the reach of a network segment
- *Hubs* – These are multiport repeaters. Used to share a single network segment with many devices. Only one device can transmit at any one time

Data Link Layer (Layer 2) Devices
Filter traffic on the LAN by MAC (hardware) address. They break up collision domains, increase available bandwidth to devices and reduce LAN traffic problems.

- *Bridges* – Connect two network segments together and filter data between them
- *Switches* – These work like multiport bridges. Each connected device can transmit simultaneously unlike hubs
- *Network Interface Cards (NICs)* – Allow a device to connect to the network. Contains a unique 48-bit MAC address.
- *Access Points* – These allow devices to connect to the network wirelessly

Network Layer (Layer 3) Devices
Route traffic between networks by logical network addresses. They use path determination to select the best route to a destination. They break up collision domains and broadcast domains.

- *Routers* – Connect different networks to one another and make routing decisions based on one or more metrics to decide the best path

Network Media (Cabling)

Coaxial Cable

10Base5 (Thicknet) – Original Ethernet cabling media. Up to 500m per segment. Highly resistant to EMI. Uses physical and logical bus topology with clients connecting using *vampire* clasps. Data transmission up to 10Mbps. Now obsolete.
10Base2 (Thinnet) – Replaced Thicknet because it was lighter and thinner and easier to work with. Up to 185m per segment. Uses physical and logical bus topology with clients attaching using BNC and T connectors. Data transmission up to 10Mbps. Now obsolete.

Twisted Pair Cable

10BaseT – Uses two-pair unshielded twisted-pair (UTP) wiring. Up to 100m per segment. Uses RJ45 connectors. Physical star with logical bus topology. Use EIA/TIA category 3 cable. Data transmission up to 10Mbps.
100BaseTX – Uses two-pair UTP wiring. Up to 100m per segment. Uses RJ45 MII connectors. Physical star with logical bus topology. Use EIA/TIA category 5, 6 or 7 cable. Data transmission up to 100Mbps
1000BaseT – Uses four-pair UTP wiring. Up to 100m per segment. Use EIA/TIA category 5 or 5e cable. Data transmission up to 1000Mbps
1000BaseCX – Uses copper twisted-pair (twinax). Maximum length 25m.

Optical Fiber

100BaseFX – Uses 62.5/125-micron multimode fiber. Maximum length 412m. Uses ST or SC connectors.
1000BaseSX – Uses 62.5/50-micron multimode fiber. Maximum length 220m – 550m.
1000BaseLX – Uses 9-micron single-mode fiber. Maximum length between 3 - 10km.

Physical Network Topologies

Bus Topology

- All devices on a single wire (coaxial)
- A cable fault can bring network down

Ring Topology

- All devices connect to each other in a circle
- A cable fault can bring network down
- Can be configured with a second ring for redundancy
- Difficult to expand network

Star Topology

- Most common physical topology
- All devices connect to a central hub/switch
- Cable faults don't bring the whole network down
- Easily expandable
- Requires more cabling than bus or ring
- Hub/switch is a central point of failure

Mesh Topology

- Every device is directly connected to every other device
- Complete redundancy
- Uses the most cable compared to other topologies
- Expanding the network can be problematic

Logical Topologies

Bus (broadcast) logical topology

- Most commonly used logical topology
- Broadcasts data to all nodes on the network
- Contention-based

Token (ring) logical topology

- A token is passed from one device to the next
- Devices can only transmit when they have the token
- Each device checks the token to see if the data inside is for them
- Slower than logical bus topology
- No longer used

LAN Standards

802.3 (Ethernet)
- Physical bus/star, logical bus
- Coaxial or twisted pair
- 10 Mbps

802.3u (Fast Ethernet)
- Physical star, logical bus
- Twisted pair
- 100 Mbps

802.3ab (Gigabit Ethernet)
- Physical star, logical bus
- Twisted pair
- 1000 Mbps (250 Mbps per pair)

802.3z (Gigabit Ethernet)
- Physical star, logical bus
- Twisted pair, optical fiber, or twinax
- 1000 Mbps

802.4 (Token Bus)
- Physical bus, logical ring
- Coaxial
- 4 Mbps

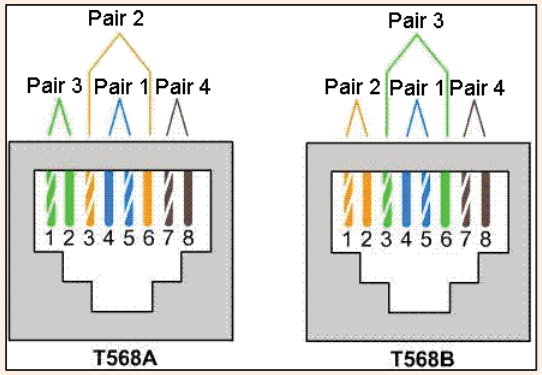
802.5 (Token Ring)
- Physical ring, logical ring
- Twisted pair
- 4 or 16 Mbps

EIA/TIA 568A and 568B Standards

Straight-through cable - Use 568B pinouts on both ends of a cable
Crossover cable – Use 568A on one end and 568B on the other end of a cable

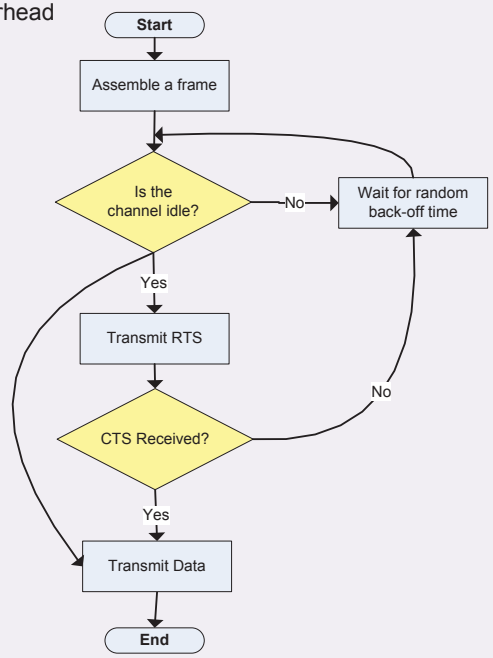
Remembering colours for 568B:
*"**O**nly **G**ood **B**oys **G**et **B**rownies"*
Orange, **G**reen, **B**lue, **G**reen, **B**rown

568A pinouts reverse the orange and green pair.



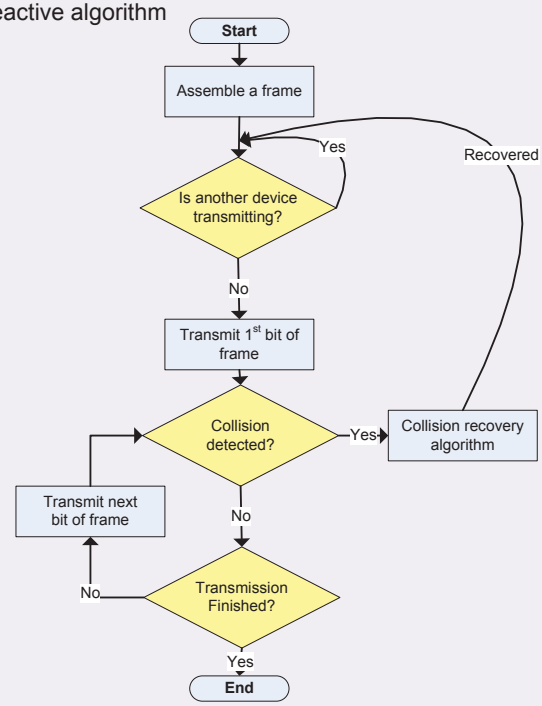
Carrier Sense Multiple Access Collision Avoidance (CSMA/CA)

- Used in wireless networking
- Proactive algorithm
- High overhead



Carrier Sense Multiple Access Collision Detection (CSMA/CD)

- Used in wired Ethernet networks
- Reactive algorithm



www.InternetworkTraining.com

Switch Modes

Cut through – Forwards the frame straight after the destination address has been read. Very fast, but can forward frames with errors.

Store and forward – Reads the entire frame prior to forwarding. Performs error an check, but adds latency to transmission. Most new switches use this mode because it can cater for hosts running at different speeds.

Fragment Free – Forwards the frame after reading the first 64 bytes to avoid forwarding frames with errors.

Catalyst Switch Boot Sequence + Operation

1.) POST (error indicated with amber SYST LED).
2.) Load IOS from Flash.
3.) Configuration file copied from NVRAM to RAM.
4.) Floods all frames it receives out all ports (CAM table empty).
5.) Begins to populate CAM table (port address table) as it learns which devices are attached to its ports.
6.) Before forwarding a frame it will check the CAM table, if an entry exists for the destination address it will forward the frame out of the port that the destination is connected. If no entry exists it will flood the frame out of all ports.
7.) Will always flood multicast and broadcast messages, unicast message are filtered.

www.InternetworkTraining.com

Internal Router Components

Bootstrap - stored in ROM - Brings up router on boot, loads IOS
POST - checks router hardware and interfaces on start-up
ROM monitor - Used for testing, troubleshooting
Mini-IOS - Small IOS in ROM, used for maintenance
RAM - Holds routing tables, running config, ARP cache
ROM - Holds POST, bootstrap and Mini-IOS
Flash - Stores IOS
NVRAM - Stores configuration and config register
Config register - Controls how router boots up

Router Boot Sequence

1.) POST
2.) Load IOS from Flash
3.) startup-config copied from NVRAM to RAM
(If no valid startup-config found it goes to setup mode)

Connecting to a Router via HyperTerminal

1.) Use a rollover cable from PC COM port to console port of router
2.) Start HyperTerminal
3.) Set bitrate to 9600 and flow control to None

Router EXEC Modes

Setup mode – Step-by-step configuration dialog
Router> - User EXEC mode for basic monitoring commands
Router# - Privileged EXEC mode, access to all other router commands
Router(config)# - Global configuration mode
Router(config-if)# - Interface configuration mode
Router(config-router)# - Routing engine configuration mode
Router(config-line)# - Line level (vty, tty, async) configuration mode

IP Routing

MAC addresses are only used on the local LAN. If a frame needs to pass through a router the frame (layer 2 PDU) will change but the packet (layer 3 PDU) is never changed throughout its journey. The frame carries the packet to either a host on the LAN or a routers interface only.

Routing vs. Routed Protocols

Routing Protocols learn about the internetwork in which they are connected and maintain a routing table to enable them to route packets.
Examples are RIP, OSPF, IGRP, EIGRP.

Routed Protocols are logical network addressing schemes used to transmit user data through an internetwork.
Examples are IP, IPv6.

Configuration Register Settings

0x2100 – Boot to ROM monitor mode
0x2102 (Default) – Loads Cisco IOS from Flash and config from NVRAM
0x2101 (0x101) – Loads IOS from ROM
0x2142 – Ignore NVRAM contents, used in Password recovery procedure. Router loads into setup mode

Changing and Verifying Configuration Register

Router(config)#config-register 0x2101 - Change Configuration Register
Router#show version – Displays basic system configuration including IOS version and config register

Restore/Backup/Upgrade a Cisco IOS Image

Router#copy flash tftp - Backup an IOS image to a TFTP server
Router#copy tftp flash – Upgrade or restore an IOS image from a TFTP server
Router#copy running-config startup-config – Save router configuration
Router#erase startup-config – Erase router configuration in NVRAM

Routing Protocols

Routing Protocol	RIP	RIPv2	IGRP	EIGRP	OSPF
Type	Distance Vector	Distance Vector	Distance Vector	Hybrid	Link State
Algorithm	Bellman-Ford	Bellman-Ford	Bellman-Ford	DUAL	Dijkstra
Admin Distance	120	120	100	90/170(external)	110
Metric	Hop Count	Hop Count	Bandwidth, delay (load, reliability)	Bandwidth, delay (load, reliability)	Bandwidth
Supported Routed Protocols	IP	IP	IP	IP, IPv6, IPX, AppleTalk	IP, IPv6
VLSM Support	NO	YES	NO	YES	YES
Classless/ Classful	Classful	Classless	Classful	Classless	Classless
Other	Broadcast updates every 30 secs	Multicast updates Every 30 secs	Cisco proprietary	Cisco proprietary	

Setting Hostname, Description & IP Address

Router#config terminal
Router(config)#hostname London
London(config)#banner motd #
Welcome to Router London
#
London(config)#int Ethernet 0
London(config-if)#ip address 1.1.1.1 255.255.0.0
London(config-if)#no shutdown
London(config-if)#description Accounts LAN

London#show int e0 – Shows whether the interface is shutdown, IP address, send/receive statistics, encapsulation, MAC address.

IOS Keyboard Shortcuts

Up Arrow Displays your previous commands. (history)
TAB Key Completes a partially typed CLI commands.
CTRL+Z Takes you back to Privileged EXEC Mode.
CTRL+A Places the cursor at the beginning of a line.
CTRL+E Places the cursor at the end of a line.
CTRL+R Redisplays the current command line.
CTRL+W Erases a word (behind the cursor).
CTRL+U Erases an entire line.

Setting Passwords

Privileged Passwords

Router(config)#enable password nik – set unencrypted password, viewable in config file

Router(config)#enable secret nik – set encrypted password (overrides enable password)

Telnet Passwords

Router(config)#line vty 0 4
Router(config-line)#password nik
Router(config-line)#login

Console Password

Router(config)#line console 0
Router(config-line)# password nik
Router(config-line)# login

www.InternetworkTraining.com
Free Cisco CCNA Practice Tests

Configuring/Verifying OSPF

Configure OSPF with a process ID, other routers do not need to be configured with the same process ID. It is used to name the instance of the OSPF database on the router.
An OSPF area is a group of contiguous routers and networks.

Router#config t
Router(config)#router ospf 20
Router(config-router)#network 192.168.9.0 0.0.0.255 area 0

show ip ospf - Displays OSPF info for all OSPF processes running on the router

show ip ospf database - Displays info on the number of OSPF routers in the autonomous system

show ip ospf neighbor - Displays OSPF neighbours including info regarding their state

show ip ospf interface - Displays OSFP interface info

Configuring/Verifying EIGRP

Configure EIGRP with autonomous system (AS) number.
If you want routers running EIGRP to share routes they must use the same autonomous system number.

Router#config terminal
Router(config)#router eigrp 15
Router(config-router)#network 10.0.0.0

show ip route eigrp - Displays EIGRP entries from the routing table

show ip eigrp neighbors - Displays all EIGRP neighbours

show ip eigrp topology -Displays contents of the EIGRP topology table

debug ip eigrp notification - Displays EIGRP changes and updates as they occur

debug eigrp packet - Displays 'Hello' packets sent/received between neighbouring routers

Configuring/Verifying RIP

Router#config terminal
Router(config)#router rip
Router(config-router)#network 10.0.0.0

show ip route - displays the routers routing table

Router#show ip route

```
     10.0.0.0/24 is subnetted, 7 subnets
S    10.1.11.0 [150/0] via 10.1.4.1
C    10.1.9.0 is directly connected, Serial0/0/1
C    10.1.8.0 is directly connected, Serial0/0/0
C    10.1.4.0 is directly connected, Ethernet0
C    10.1.5.0 is directly connected, Ethernet1
R    10.1.3.0 [120/1] via 10.1.4.1, 00:00:03, Serial0/2/0
R    10.1.2.0 [120/1] via 10.1.4.1, 00:00:03, Serial0/2/0
```

Codes:
I - IGRP derived, R - RIP derived, O - OSPF derived, C - connected, S - static, D - EIGRP, * - candidate default route

debug ip rip - displays routing updates as they are sent and received

Troubleshooting Interface Problems

Serial0/0 is up, line protocol is up - The interface is functioning correctly.

Serial0/0 is down, line protocol is down - This message usually represents a physical interface problem. The cable may be disconnected. This can also occur if this interface is connected to another router whose interface has been shutdown.

Serial0/0 is up, line protocol is down - The Physical layer connectivity is not the issue. The line protocol being down is either a clocking issue (keepalives) or a mismatch of the frame types being used on connected devices.

Serial0/0 is administratively down, line protocol is down - The interface has been manually shutdown using the shutdown command.