IOS Commands

Privileged Mode

enable - get to privileged mode
disable - get to user mode
enable password <password_here> - sets privileged mode password
enable secret <password_here> - sets encrypted privileged mode password

Setting Passwords

enable secret <password_here> - set encrypted password for privilegedaccess
enable password <password_here> - set password for privileged access (used when there is no enable secret and when using older software)

Set password for console access:

```
  (config)#line console 0
  (config-line)#login
  (config-line)#password <password_here>
```

Set password for virtual terminal (telnet) access (password must be set to access router through telnet)**:**

```
   (config)#line vty 0 4
   (config-line)#login
   (config-line)#password <password_here>
```

Set password for auxiliary (modem) access:

```
   (config)#line aux 0
   (config-line)#login
   (config-line)#password <password_here>
```

Configuring the Router

sh running-config - details the running configuration file (RAM)
sh startup-config - displays the configuration stored in NVRAM
setup - Will start the the automatic setup; the same as when you first boot the router
config t - use to execute configuration commands from the terminal
config mem - executes configuration commands stored in NVRAM; copies startup-config to running-config
config net - used to retrieve configuration info from a TFTP server
copy running-config startup-config - copies saved config in running config (RAM) to NVRAM or "write memory" for IOS under ver.11
copy startup-config running-config - copies from non-volatile (NVRAM) to current running config (RAM)
boot system flash <filename_here> - tells router which IOS file in flash to boot from
boot system tftp - tells router which IOS file on the tftp server to boot from
boot system rom - tell router to boot from ROM at next boot
copy flash tftp - Copies flash to tftp server
copy tftp flash - Restores flash from tftp server
copy run tftp - Copies the current running-config to tftp server
copy tftp run - Restores the running-config from tftp server

General Commands

no shutdown - (enables the interface)
reload - restarts the router
sh ver - Cisco IOS version, uptime of router, how the router started, where system was loaded from,

the interfaces the POST found, and the configuration register
sh clock - shows date and time on router
sh history - shows the history of your commands
sh debug - shows all debugging that is currently enabled
no debug all - turns off all debugging
sh users - shows users connected to router
sh protocols - shows which protocols are configured
banner motd # Your_message # - Set/change banner
hostname <router_name_here> - use to configure the hostname of the router
clear counters - clear interface counters

Processes & Statistics
sh processes - shows active processes running on router
sh process cpu - shows cpu statistics
sh mem - shows memory statistics
sh flash - describes the flash memory and displays the size of files and the amount of free flash memory
sh buffers - displays statistics for router buffer pools; shows the size of the Small, Middle, Big, Very Big, Large and Huge Buffers
sh stacks - shows reason for last reboot, monitors the stack use of processes and interrupts routines

CDP Commands (Cisco Discovery Protocol uses layer 2 multicast over a SNAP-capable link to send data):
sh cdp neighbor - shows directly connected neighbors
sh cdp int - shows which interfaces are running CDP
sh cdp int eth 0/0 - show CDP info for specific interface
sh cdp entry <cdp_neighbor_here> - shows CDP neighbor detail
cdp timer 120 - change how often CDP info is sent (default cdp timer is 60)
cp holdtime 240 - how long to wait before removing a CDP neighbor (default CDP holdtime is 180)
sh cdp run - shows if CDP turned on
no cdp run - turns off CDP for entire router (global config)
no cdp enable - turns off CDP on specific interface

Miscellaneous Commands
sh controller t1 - shows status of T1 lines
sh controller serial 1 - use to determine if DCE or DTE device
(config-if)#clock rate 6400 - set clock on DCE (bits per second)
(config-if)#bandwidth 64 - set bandwidth (kilobits)

IP Commands
Configure IP on an interface:
int serial 0
ip address 157.89.1.3 255.255.0.0
int eth 0
ip address 2008.1.1.4 255.255.255.0
Other IP Commands:
sh ip route - view ip routing table
ip route <remote_network> <mask> <default_gateway> [administrative_distance] - configure a static IP route
ip route 0.0.0.0 0.0.0.0 <gateway_of_last_resort> - sets default gateway

ip classless - use with static routing to allow packets destined for unrecognized subnets to use the best possible route

sh arp - view arp cache; shows MAC address of connected routers

ip address 2.2.2.2 255.255.255.0 secondary - configure a 2nd ip address on an interface

sh ip protocol

IPX Commands

Enable IPX on router:

ipx routing

Configure IPX + IPX-RIP on an int:

int ser 0
ipx network 4A

Other Commands:

sh ipx route - shows IPX routing table
sh ipx int e0 - shows ipx address on int
sh ipx servers - shows SAP table
sh ipx traffic - view traffic statistics
debug ipx routing activity - debugs IPS RIP packets
debug ipx sap - debugs SAP packets

Routing Protocols

Configure RIP:

router rip
network 157.89.0.0
network 208.1.1.0

Other RIP Commands:

debug ip rip - view RIP debugging info

Configure IGRP:

router IGRP 200
network 157.89.0.0
network 208.1.1.0

Other IGRP Commands:

debug ip igrp events - view IGRP debugging info
debug ip igrp transactions - view IGRP debugging info

Access Lists (see notes below for details)

sh ip int ser 0 - use to view which IP access lists are applies to which int
sh ipx int ser 0 - use to view which IPX access lists are applies to which int
sh appletalk int ser 0 - use to view which AppleTalk access lists are applies to which int

View access lists:

sh access-lists
sh ip access-lists
sh ipx access-lists
sh appletalk access-lists

Apply standard IP access list to int eth 0:

access-list 1 deny 200.1.1.0 0.0.0.255
access-list 1 permit any
int eth 0
ip access-group 1 in

Apply Extended IP access list to int eth 0:

```
    access-list 100 deny tcp host 1.1.1.1 host 2.2.2.2 eq 23
    access-list 100 deny tcp 3.3.3.0 0.0.0.255 any eq 80
    int eth 0
    ip access-group 100 out
```

Apply Standard IPX access list to int eth 0:

```
    access-list 800 deny 7a 8000
    access-list 800 permit -1
    int eth 0
    ipx access-group 800 out
```

Apply Standard IPX access list to int eth 0:

```
    access-list 900 deny sap any 3378 -1
    access-list 900 permit sap any all -1
    int eth 0
    ipx access-group 900 out
```

Wan Configurations (see notes below for more details)

PPP Configuration

encapsulation ppp
ppp authentication <chap_or_pap_here>
ppp chap hostname <routername_here>
ppp pap sent-username <username_here>
sh int ser 0 - use to view encapsulation on the interface

Frame-Relay Configuration

encapsulation frame-relay ietf - use IETF when setting up a frame-relay network between a Cisco router and a non-Cisco router
frame-relay lmi-type ansi - LMI types are Cisco, ANSI, Q933A; Cisco is the default; LMI type is auto-sensed in IOS v11.2 and up
frame-relay map ip 3.3.3.3 100 broadcast - if inverse ARP won't work, map Other IP to Your DLCI # (local)
keepalive 10 - use to set keepalive
sh int ser 0 - use to show DLCI, LMI, and encapsulation info
sh frame-relay pvc - shows the configured DLCI's; shows PVC traffic stats
sh frame-relay map - shows route maps
sh frame-relay lmi - shows LMI info

Keyboard Shortcuts

CTRL-P - show previous command
CTRL-N - show next command
SHIFT-CTRL-6 - Break

Notes

Static and Dynamic Routing

Static Routing - manually assigned by the Admin user entering the routes (**Routed Protocols** - IP, IPX and AppleTalk)
Dynamic Routing - generated/determined by a Routing Protocol (Routing Protocols - RIP I, RIP II,

IGRP, EIGRP, OSPF, NLSP, RTMP)

Dynamic

1) With Dynamic Routing, routers pass information between each other so that routing tables are regularly maintained.
2) The routers then determine the correct paths packets should take to reach their destinations.
3) Information is passed only between routers.
4) A routing domain is called an Autonomous System, as it is a portion of the Internetwork under common admin authority.
5) Consists of routers that share information over the same protocol. Can be split into routing areas.

Distance Vector and Link-State Routing

Routing Protocols

I) Interior (within an autonomous system - AS - group of routers under the same administrative authority)

a) Distance Vector - understands the direction and distance to any network connection on the internetwork. Knows how many hops (the metric) to get there. All routers w/in the internetwork listen for messages from other routers, which are sent every 30 to 90 seconds. They pass their entire routing tables. Uses hop count for measurement. 1) Used in smaller networks that are have fewer than 100 routers. 2) Easy to configure and use. 3) As routers increase in number, you need to consider CPU utilization, convergence time, and bandwidth utilization. 4) Convergence is due to routing updates at set intervals. 5) When a router recognizes a change it updates the routing table and sends the whole table to all of its neighbors.

1) RIP - 15 hop count max
2) IGRP - 255 hop count max, uses reliability factor (255 optimal), and bandwidth
3) RTMP

b) Link State - understands the entire network, and does not use secondhand information. Routers exchange LSP?s (hello packets). Each router builds a topographical view of the network, then uses SPF (shortest path first) algorithm to determine the best route. Changes in topology can be sent out immediately, so convergence can be quicker. Uses Bandwidth, congestion for measurement; Dijkstra's algorithm;

1) Maintains Topology Database. 2) Routers have formal neighbor relationship. 3) Exchanges LSA (Link State Advertisement) or hello packets with directly connected interfaces. 4) These are exchanged at short intervals (typically 10 sec). 5) Only new info is exchanged. 6) Scales well, however link?state protocols are more complex. 7) Requires more processing power, memory, and bandwidth.

1) OSPF - decisions based on cost of route (metric limit of 65,535)
2) EIGRP - hybrid protocol (both Distance-Vector and Link State), Cisco proprietary
3) NLSP
4) IS-IS

II) Exterior

1) EGP (Exterior Gateway Protocol)

2) BGP (Border Gateway Protocol)

Routing Protocols used for each Routed Protocol
IP - RIP, IGRP, OSPF, IS-IS, EIGRP
IPX - IPX RIP, NLSP, EIGRP
AppleTalk - RTMP, AURP, EIGRP

Problems with Routing Protocols
1) Routing Loops - occur when routing tables are not updated fast enough when one of the networks becomes unreachable. Due to the slow convergence (updates of routing table between all routers), some routers will end up with incorrect routing table and will broadcast that routing table to other routers. This incorrect routing tables will cause packets to travel repeatedly in circles.
2) Counting to infinity - occurs when packets end up in a routing loop; hop count increases with every pass through a router on the network

Solutions to Problems with Routing Protocols
1) Define the maximum number of hops - When the number of hops reaches this predefined value, the distance is considered infinite, thus the network is considered unreachable. This does stop routing loops, but only limit the time that packet can travel inside the loop.
2) Split horizon - The packets can not be sent back to the same interface that they originally came from. During the updates, one router does not send updates to the router that it received the information from.
3) Route poisoning - The router sets the cost/distance of routes that are unreachable to infinity. Used with hold-down timers
4) Triggered updates - The router sends updates of the routing table as soon as it detects changes in the network. Does not wait for the prescribed time to expire.
5) Hold-Downs - After the router detects unreachable network, the routers waits for a specified time before announcing that a network is unreachable. The router will also wait for a period of time before it updates its routing table after it detects that another router came online (Router keeps an entry for the network possibly down state, allowing time for other routers to re-compute for this topology change). Hold-downs can only partially prevent counting to infinity problem. Prevents routes from changing too rapidly in order to determine if a link has really failed, or is back up

Encapsulation Types

	Encapsulation
802.2	sap
802.3	novell-ether
Ethernet II	arpa (Internet Standard)
Snap	snap

Wan Service Providers
1) Customer premises equipment (CPE) - Devices physically located at subscriber?s location; examples: CSU/DSU, modem, wiring on the customer's location
2) Demarcation (or demarc) - The place where the CPE ends and the local loop portion of the service

begins. (Usually in the "phone closet").
3) Local loop - Cabling from the demarc into the WAN service provider?s central office; wiring from customer's location to the nearest CO
4) Central Office switch (CO) - Switching facility that provides the nearest point of presence for the provider?s WAN service; location of telephone company's equipment where the phone line connects to the high speed line (trunk); Regional Telco Office where the local loop terminates (the Telco location nearest you)
5) Toll network - The switches and facilities, (trunks), inside the WAN provider?s "cloud."

DTE - the router side and receive clocking
DCE - the CSU/DSU side and provide clocking

WAN Devices
Routers - Offer both internetwork and WAN interface controls
ATM Switches - High-speed cell switching between both LANs and WANs
X.25 and Frame-Relay Switches - Connect private data over public circuits using digital signals
Modems - Connect private data over public telephone circuits using analog signals
CSU/DSU (Channel Service Units/Data Service Units) - Customer Premises Equipment (CPE) which is used to terminate a digital circuit at the customer site
Communication Servers - Dial in/out servers that allow dialing in from remote locations and attach to the LAN
Multiplexors - Device that allows more than one signal to be sent out simultaneously over one physical circuit

ISDN
ISDN BRI (Basic Rate Interface) - 2 64K B channels, plus 1 16K D channel
ISDN PRI (Primary Rate Interface) - 23 64K B channels, plus 1 64K D channel (North America & Japan), 30 64K B channels, plus 1 64K D channel (Europe & Australia)

Classful and Classless Protocols
Classful - summarizes routing info by major network numbers; ex. RIP, IGRP
Classless - BGP, OSPF
Administrative Distances for IP Routes

Administrative Distances are configured using ip route command:

Example: ip route 154.4.55.0 255.255.255.0 195.23.55.1 85 (where 85 is the administrative distance)

IP Route	**Administrative Distance**
Directly connected interface	0
Static route using connected interface	0
Static route using IP address	1
EIGRP summary route	5

External BGP route	20
Internal EIGRP route	90
IGRP route	100
OSPF route	110
IS-IS route	115
RIP route	120
EGP route	140
External EIGRP route	170
Internal BGP route	200
Route of unknown origin	255

Switching Terminology
Store-and-Forward ? copies entire frame into buffer, checks for CRC errors before forwarding. Higher latency.
Cut-Through ? reads only the destination address into buffer, and forwards immediately; Low latency; "wire-speed"
Fragment free ? modified form of cut-through; switch will read into the first 64 bytes before forwarding the frame. Collisions will usually occur within the first 64 bytes. (default for 1900 series).

Access Lists

1-99	IP Standard Access List
100-199	IP Extended Access List
200-299	Protocol Type-code Access List
300-399	DECnet Access List
600-699	Appletalk Access List
700-799	48-bit MAC Address Access List
800-899	IPX Standard Access List
900-999	IPX Extended Access List
1000-1099	IPX SAP Access List
1100-1199	Extended 48-bit MAC Address Access List

1200-1299	IPX Summary Address Access List

Access List	Filters	Wildcard Masks	
Standard IP	Source IP address field in the packet's IP header	To put simply, when the IP is broken down to binary, the 1's allow everything and the 0's must match exactly.	Wildcard mask 0.255.255.255= everything. 255
Extended IP	Source IP or Destination IP, or TCP or UDP Source or Destination Ports, or Protocol	Same as standard	The key word A HOST implies t
Standard IPX	Packets sent by clients and servers, and SAP updates sent by servers and routers	Configured as a hexadecimal number instead of binary	-1 means any ar
Extended IPX	Source Network or Node, or Destination Network or Node, or IPX Protocol, or IPX Socket, or SAP	Match multiple networks with one statement, again in hexadecimal	The most practi
SAP	Sent and received SAP traffic	N/A	Updates its own

Troubleshooting Tools:

Ping Results

!	success
,	timeout
U	destination unreachable
?	unknown packet type
&	TTL exceeded

Traceroute Results

!H	router rec'd, but didn't forward because of access-list
P	protocol unreachable
N	network unreachable
U	port unreachable

,	timeout

Accessing Router with Terminal Emulation

Using HyperTerminal on a Windows machine adjust the following settings:

VT100 Emulation
Connection Speed: 9600 Baud
Data Bits: 8
Parity: None
Stop Bits: 1
Flow Control: None

On a Linux machine you may use Seyon or Minicom (at least one should come with your distribution).

Router Startup Sequence

POST
Bootstrap program loaded from ROM
IOS is loaded from either flash (default), TFTP, or ROM
IOS image loaded into low-addressed memory; hardware and software is determined
Config file is load from NVRAM; if no configuration exists in NVRAM, the initial configuration dialog will begin