Basic Router Operations	
To get to Priveledge mode	**enable**
To get to User mode	**disable**
To Exit router	**exit or logoff**
Previous Command	**up arrow or Ctrl-P**
Next Command	**down arrow or Ctrl-N**
Move forward one character	**right arror or Ctrl-F**
Move backward one character	**left arrow or Ctrl-B**
Break Key	**<shft>+<ctl>+6 'x'**
Auto complete command	**<tab>**
Viewing Router Information	
IOS version info	**show version**
Current config (RAM)	**show running-config**
Saved config (NVRAM)	**show startup-config**
IOS file and free space	**show flash**
Processor utilization	**show processes cpu**
Configuring the Router	
From the terminal session (keyboard) to running (RAM)	**configure terminal**
From tftp (file server) to running (RAM)	**copy tftp running-config**
From saved config (NVRAM) to running (RAM)	**copy startup-config running-config**
Upgrade the IOS from file server	**copy tftp flash**
Save backup copy of IOS to file server	**copy flash tftp**
Save your configuration (from RAM) to non-volatile (NVRAM)	**copy running-config startup-config**
Tell the router which IOS file in Flash to boot from	**boot system flash {filename}**
Tell the router which IOS file to request from TFTP (fallback)	**boot system tftp {filename}**
Passwords	
Set password for Console port	**line console 0** **login** **password cisco**
Set password for Telnet	**line vty 0 4** **login** **password sanjose**
Set password for Priveledge mode	**enable password cisco**
Set Encrypted password for Priveledge mode	**enable secret cisco**
Configuring a Serial Interface	
Is it DCE or DTE?	**show controller serial 1**
From global config	**interface serial 1**
Set clock rate on DCE	**clock rate 64000**
Set the bandwidth	**bandwidth 64**
Enable the interface	**no shutdown**
Check interface status	**show interface serial 1** **show ip interface brief**
Cisco Discovery Protocol	
See directly connect neighbors (add 'detail' for more info)	**show cdp neighbor**
See which inteface are running CDP	**show cdp interface**
See one neighbors detail	**show cdp entry P1R1**
Turn off CDP for whole router (from global config)	**no cdp run**
Turn off CDP on an interface	**no cdp enable**
Change how often you send CDP info	**cdp timer 120**
Change how long you will till you remove a CDP neighbor	**cdp holdtime 240**

TCP/IP	
Disable IP routing on the router (enabled by default)	**no ip routing**
To put an IP address on an interface	**interface serial 0** **ip address 157.89.1.3 255.255.0.0** **interface ethernet 0** **ip address 208.1.1.4 255.255.255.0**
Configure RIP	**router rip** **network 157.89.0.0** **network 208.1.1.0**
Configure IGRP	**router IGRP 200** **network 157.89.0.0** **network 208.1.1.0**
View IP routing table	**show ip route**
View RIP debug stuff	**debug ip rip**
View IGRP debug stuff	**debug ip igrp events** **debug ip igrp transactions**
IPX/SPX	
Enable IPX on the router (disabled by default)	**ipx routing**
Enable Load balancing	**ipx maximum-paths 6**
Interface Commands	
Enable IPX + IPX-RIP on an interface	**interface serial 0**
-- Default encapsulation	**ipx network 4A**
--- Defaults to novell-ether on ethernet, HDLC on serial	
**** TO FORCE ENCAPSULATION TYPE:	
-- 802.3 encapsulation = novell-ether	**ipx network 4A encap novell-ether**
-- 802.2 encapsulation = sap	**ipx network 4A encap sap**
-- Ethernet II encapsulation = arpa	**ipx network 4A encap arpa**
-- Snap Encapsulation = snap	**ipx network 4A encap snap**
IPX RIP routing is automatically enabled as soon as you put an IPX address on an interface	
Show Commands	
View IPX routinng table	**show ipx route**
View IPX address on an interface	**show ipx interface**
View SAP table	**show ipx servers**
View traffic statistics	**show ipx traffic**
Debug Commands	
Debug IPX RIP Packets	**debug ipx routing activity**
Debug SAP packets	**debug ipx sap**
Appletalk	
Enable appletalk on the router (disabled by default)	**appletalk routing**
Interface commands	
Specify routing protocol (default to RTMP) -- optional	**appletalk protocol eigrp** **appletalk protocol aurp**
Assign a cable range to an interface (required)	**appletalk cable-range 1000-1999**
Assign a zone to an interface (required)	**appletalk zone Workgroup1**
Put interface into discovery mode, it will find range & zone	**appletalk cable-range 0-0** or **appletalk discovery**
Show Commands	
View the appletalk address on an interface	**show appletalk interface serial 0**
View the appletalk routing table	**show appletalk routing**
View appletalk zones	**show appletalk zones**
Show Global appletalk settings	**show appletalk globals**
Debug Commands	
Watch real-time AppleTalk updates and status	**debug appletalk events**
View RTMP routing update packets	**debug appletalk routing**

Access-Lists

All Access-List numbered ranges (some not covered in ICRC)	
<1-99>	**IP standard access list**
<100-199>	**IP extended access list**
<200-299>	**Protocol type-code access list**
<300-399>	**DECnet access list**
<400-499>	**XNS standard access list**
<500-599>	**XNS extended 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**
View Which Access-lists are applied to which interface	**show ip interface serial 0** **show ipx interface serial 0** **show appletalk interface serial 0**
View the access-lists	**show access-lists** **show ip access-lists** **show ipx access-lists** **show appletalk access-lists**

Access-Lists, IP Standard = 1-99, filter on Source address

Goal- stop subnet 200.1.1.0 255.255.255.0 from sending packets into ethernet 0	
A. Deny the subnet	**access-list 1 deny 200.1.1.0 0.0.0.255**
B. Implicit deny all, so must permit others	**access-list 1 permit any**
C. Doesn't do anything until we bind it to an interface	**interface ethernet 0** **ip access-group 1 in**

Access-Lists, IP Extended = 100-199, filter on Source + Dest, Port, etc…

Goal - stop host 1.1.1.1 from telneting out e0 going to host 2.2.2.2 and stop subnet 3.3.3.0 from web surfing anywhere	
A. Remember access-list # source destination options	**access-list 100 deny tcp host 1.1.1.1 host 2.2.2.2 eq 23**
B. Stop that web surfing	**access-list 100 deny tcp 3.3.3.0 0.0.0.255 any eq 80**
C. Implicit deny, allow all others	**access-list 100 permit ip any any**
D. Doesn't do anythin, until you bind it to an interface	**interface ethernet 0** **ip access-group 100 out**

Named IP/IPX Access-Lists

Allows editing of lines instead of deleting entire list supports standard and extended (Named IP requires 11.2 or later) (Named IPX requires 11.3 or later)	**ip access-list standard cool_list** **deny 1.1.1.1** **permit any** **interface ethernet 0** **ip access-group cool_list in**

Access-Lists, IPX Standard = 800-899, filter Source & Dest

Stop network 7A from getting to network 8000	**access-list 800 deny 7a 8000**
Implicit deny all, allow all other networks	**access-list 800 permit -1**
Doesn't do anything until you bind it to an interface	**interface ethernet 0** **ipx access-group 800 out**

Access-Lists, IPX Extended = 900-999, filter on Source & Dest + Socket, etc…

Stop SAPs on socket 3378 from all networks to all networks	**access-list 900 deny sap any 3378 -1**
Implicit deny all, allow all other SAPs	**access-list 900 permit sap any all -1**
Doesn't do anything until you bind it to an interface	**interface ethernet 0** **ipx access-group 900 out**

Access-Lists, IPX SAP Filters = 1000-1099, filter on Source, Port, Service Name

Stop SAPs from server 1 from coming in Ethernet 0	**access-list 1000 deny 7A.0000.0000.0001 4**
Permit all others	**access-list 1000 permit -1**
Bind it to an itnerface	**interface ethernet 0**
Stop it coming in	**ipx input-sap-filter 1000**
Or stop it going out	**ipx output-sap-filter 1000**

Access-Lists, Appletalk = 600-699, filter on Cable-Range & Zone

Deny cable range 1000-1999	**access-list 600 deny cable-range 1000-1099**
Permt all other cable ranges	**access-list 600 permit other-access**
Deny the zone Workgroup1	**access-list 600 deny zone Workgroup1**
Permit all other zones	**access-list 600 permit additional-zones**
Bind it to an interface	**interface ethernet 0** **appletalk access-group 600**

PPP

Interface commands	
Enable PPP on the interface	**encapsulation ppp**
Enable authentication (chap or pap)	**ppp authentication chap**
specify chap hostname (defaults to router name)	**ppp chap hostname MyRouter**
Specify chap password (defaults to enable password)	**ppp chap password Clearwater**
Specify pap username	**ppp pap sent-username ArnoldZiffle**
Global Commands	
Create a username and password for logging in	**username OtherRouter password Skywalker**
Show Commands	
See encapsulation, open LCP's and more	**show interface serial 0**
Debug Commands	
View the authentication process	**debug ppp authentication**

X.25

Interface commands	
Enable X.25 on an interface and specify encap type	**encapsulation x25 ietf**
Specify YOUR Local x121 address	**x25 address 301222333444**
Map the OTHER IP to OTHER x121 address (global)	
Enable broadcasts for RIP & such	**x25 map ip 200.1.1.1 301999888777 broadcast**
OPTIONAL Interface commands	
Adjust Incoming Packet Size, must match on both sides	**x25 ips 512**
Adjust Outgoing Packet Size, must match on both sides	**x25 ops 512**
Adjust Incoming Windows Size, must match on both sides	**x25 win 7**
Adjust Outgoing Window Size, must match on both sides	**x25 wout 7**
Show Commands	
View Encapsulation, LAPB Status, & more	**show interface serial 0**
Back-to-Back x25 routers (for lab testing)	
Note, x25 does not care about which ONE router has DCE cable	
Enable X.25 on interface and specify encap type + ONE side is DCE	**encapsulation x25 dce ietf**
Set DCE-side to transmit clocking frequency in Kbits/Sec	**clockrate 9600**

Frame-Relay

Interface commands	
Enable Frame-Relay on an interface and specify encap type	**encapsulation frame-relay ietf**
Specify LMI Type (11.2+ will autosense LMI type)	**frame-relay lmi-type ansi**
If Inverse ARP won't work, Map OTHER IP to YOUR DLCI # (local)	**frame-relay map ip 3.3.3.3 100 broadcast**
Can also allow broadcast and specify encap type	
Define local DLCI (in LMI not working)	**frame-relay local-dlci 100**
Adjust keepalive period	**keepalive 10**
Show Commands	
View DLCI & LMI Info	**show interface serial 0**
View PVC traffic statistics	**show frame-relay pvc**
View Route Maps (static or dynamic)	**show frame-relay map**
View LMI info	**show frame-relay lmi**
Back-to-Back frame-relay routers (for lab testing)	
Note, must match DCE-side router commands with DCE cable	
Enable Frame-Relay switching on DCE-side router	**frame-relay switching**
Tell DCE-side to support DCE frame-relay functions on what interface	**frame-relay intf-type dce**
Tell DCE-side which interface & DLCI to switch current interface to	**frame-relay route {dlci} interface {int} {dlci}**
Set DCE-side to transmit clocking frequency in Kbits/Sec	**clockrate 64000**

Config-Reg

RXBOOT (diagnostics mode, use 'b' to continue booting)	**config-reg 0x2000**
Boot to ROM, use NVRAM (upgrade flash in run-from-flash routers)	**config-reg 0x2101**
Boot to ROM, skip NVRAM (disaster recovery)	**config-reg 0x2141**
Boot to Flash, use NVRAM (normal operation)	**config-reg 0x2102**
Boot to Flash, skip NVRAM (password recovery)	**config-reg 0x2142**

Auto-Install

Router broadcasts to get its own TCP/IP address using	**BOOTP**
Router broadcasts again to locate the file server IP address using	**TFTP**
Router attempts TFTP to get the IP-to-Hostname mapping file	**network-confg**
If above fails, fallback to 8.3 DOS compatible filename convention	**cisconet.cfg**
Router attempts TFTP to get its specific Hostname running-config	**{Hostname}-confg**
If above fails, fallback to 8.3 DOS compatible filename convention	**{Hostname}.cfg**

Note: {Hostname} is determined by parsing network-confg file and checking all Hostnames listed against own IP address

Password Recovery

Step 1, halt router bootup on console port (requires physical access)	**CTRL-BREAK**
Step 2, enter RXBOOT command to set config-reg bits & stop NVRAM	**o/r 0x2142**
Step 3, bypassing NVRAM startup allows Enable mode without pwd	**enable**
Step 4, once in Enable mode, copy NVRAM startup to RAM	**copy startup-config running-config**
Step 5, change Enable and all other passwords as desired	**enable password whatever**
Step 6, save RAM back into NVRAM, but now with new password	**copy running-config startup-config**
Step 7, change config-reg bits back, so router boots normally	**config-reg 0x2102**