

### Login Enhancements

Command	Function
<code>login block-for 120 attempts 3 within 30</code>	blocks login attempts for 120 secs if 3 fail within 30 secs ( <code>login local</code> must be configured)
<code>login quiet-mode access-class [acl-name   acl-number]</code>	maps to an ACL so only authorized hosts can attempt to login
<code>login delay seconds</code>	wait-time between login attempts
<code>login on-success log</code>	records successful logins
<code>login on-failure log</code>	records failed login attempts

> Login enhancements don't apply to console connections  
> `login block-for` must be configured before any others

### Role-Based CLI Views

Command	Mode	Function
<code>aaa new-model</code>	global	enables AAA
<code>parser view view-name</code>	global	creates a new view (must be in root view)
<code>secret password</code>	view	assigns view password (required)
<code>commands parser-mode [include exclude] [command interface]</code>	view	assigns command or interface to view
<code>enable view view-name</code>	priv. EXEC	enters view (enable secret for root password)
<code>parser view view-name superview</code>	global	creates a new superview
<code>secret password</code>	superview	assigns superview password (required)
<code>view view-name</code>	superview	assigns existing view to superview

### IPsec VPNs (Site-to-Site)

	Command	Mode
<b>----- Phase 1 -----</b>		
<code>cry is en</code>	<code>crypto isakmp enable</code>	global
<code>cry is pol 10</code>	<code>crypto isakmp policy 10</code>	global
<code>h sha</code>	<code>hash sha</code>	(config-isakmp)
<code>a p (auth pre)</code>	<code>authentication pre-share</code>	(-isakmp)
<code>g 14</code>	<code>group [DH group #]</code>	(-isakmp)
<code>l 3600</code>	<code>lifetime [secs]</code>	(-isakmp)
<code>enc a 256</code>	<code>encryption aes 256</code>	(-isakmp)
<code>cry is key vpnpass add 10.2.2.2</code>	<code>crypto isakmp key [key] address [peer IP]</code>	global
<b>----- Phase 2 -----</b>		
<code>cry ip t VPN-SET esp-a 256 esp-sha-</code>	<code>crypto ipsec transform-set [tag] [encry.] [bits] [hash]</code>	global



### IPsec VPNs (Site-to-Site) (cont)

<code>cry ip s l s</code>	<code>crypto ipsec security-association lifetime seconds 1800</code>	global
<code>cry map CMAP 10 ipsec-i</code>	<code>crypto map [name] [seq #] ipsec-isakmp</code>	global
<code>m add 101</code>	<code>match address 101</code>	(-crypto-map)
<code>s pe 10.2.2.2</code>	<code>set peer [peer IP]</code>	(-crypto-map)
<code>s pfs group14</code>	<code>set pfs [group#]</code>	(-crypto-map)
<code>s t VPN-SET</code>	<code>set transform-set [tag]</code>	(-crypto-map)
<code>s s li s 900</code>	<code>set security-association lifetime seconds [secs]</code>	(-crypto-map)
<code>desc [text]</code>	<code>description [text]</code>	(-crypto-map)
<code>cry m CMAP</code>	<code>crypto map [name]</code>	interface

### Line Config Mode

Command	Line	Function
<code>no exec</code>	any unused	disables EXEC mode for the line (outgoing connections only)
<code>login local</code>	all	forces username/password authentication from local database
<code>logging synchronous</code>	all	prevents logging from interrupting commands
<code>exec-timeout 5 0</code>	all	logs out after 5 mins inactive

### Informational/Show Commands

Short Command	Full Command	What It Displays
<code>sh login</code>	<code>show login</code>	configured login settings
<code>sh login f</code>	<code>show login failures</code>	details about login failures (src IP, count, time/date, etc)
<code>sh cry key mypubkey r</code>	<code>show crypto key mypubkey rsa</code>	current RSA keys
<code>sh ip ssh</code>	<code>show ip ssh</code>	SSH configuration
<code>sh ssh</code>	<code>show ssh</code>	current SSH connections
<code>sh p v a</code>	<code>show parser view all</code>	summary of all configured views (asterisk indicates superview)
<code>sh sec b</code>	<code>show secure bootset</code>	verification of the archive
<code>sh logg</code>	<code>show logging</code>	logging configuration & buffered syslog messages
<code>sh us</code>	<code>show users</code>	users connected to the device
<code>sh cr is po</code>	<code>show crypto isakmp policy</code>	ISAKMP policy configuration
<code>sh cr ip sa</code>	<code>show crypto ipsec sa</code>	IPsec security association
<code>sh cr map</code>	<code>show crypto map</code>	crypto map configuration



### Logging & Monitoring

Command	Mode	Function
<code>service timestamps log datetime msec</code>	global	enables timestamps service
<code>logging host ip-address</code>	global	specifies syslog server
<code>logging trap level</code>	global	sets log severity level
<code>logging source-interface ip-address</code>	global	identifies the device sending the log info
<code>logging on</code>	global	turns on logging

### Secure Bootset

Command	Mode	Function
<code>secure boot-image</code>	global	secures IOS image & enables Cisco IOS image resilience
<code>secure boot-config</code>	global	takes snapshot of running-config to save in persistent storage
<b>--- To Restore Secure Configuration ---</b>		
<code>reload-&gt; ROMmon mode</code>		
<code>dir</code>	ROMmon	lists contents of device where secure bootset is stored
<code>boot flash:filename</code>	ROMmon	boots route with secure IOS image
<code>secure boot-config restore flash:filename</code>	global	restores secure config

### SSH Configuration

Command	Function
<code>user Bob algorithm-type scrypt secret password</code>	creates user in local database
<code>ip domain-name span.com</code>	sets network domain name
<code>crypto key zeroize rsa</code>	removes any existing RSA key pairs
<code>cry key gen rsa gen mod 1024</code>	creates RSA encryption key (max: 4096 bits)
<code>transport input ssh</code>	enables SSH (line config, vty)
<code>ip ssh time-out seconds</code>	sets SSH timeout length
<code>ip ssh authentication-retries 2</code>	sets number of login attempts before user is disconnected
<code>ip ssh version 2</code>	sets SSH version to v2

### Miscellaneous Configurations

Command	Function
<code>license boot module c1900 technology-package securityk9</code>	<i>Adds security package to 1941 routers!</i>
<code>no service password-recovery</code>	prevents an attacker from recovering the router password

