

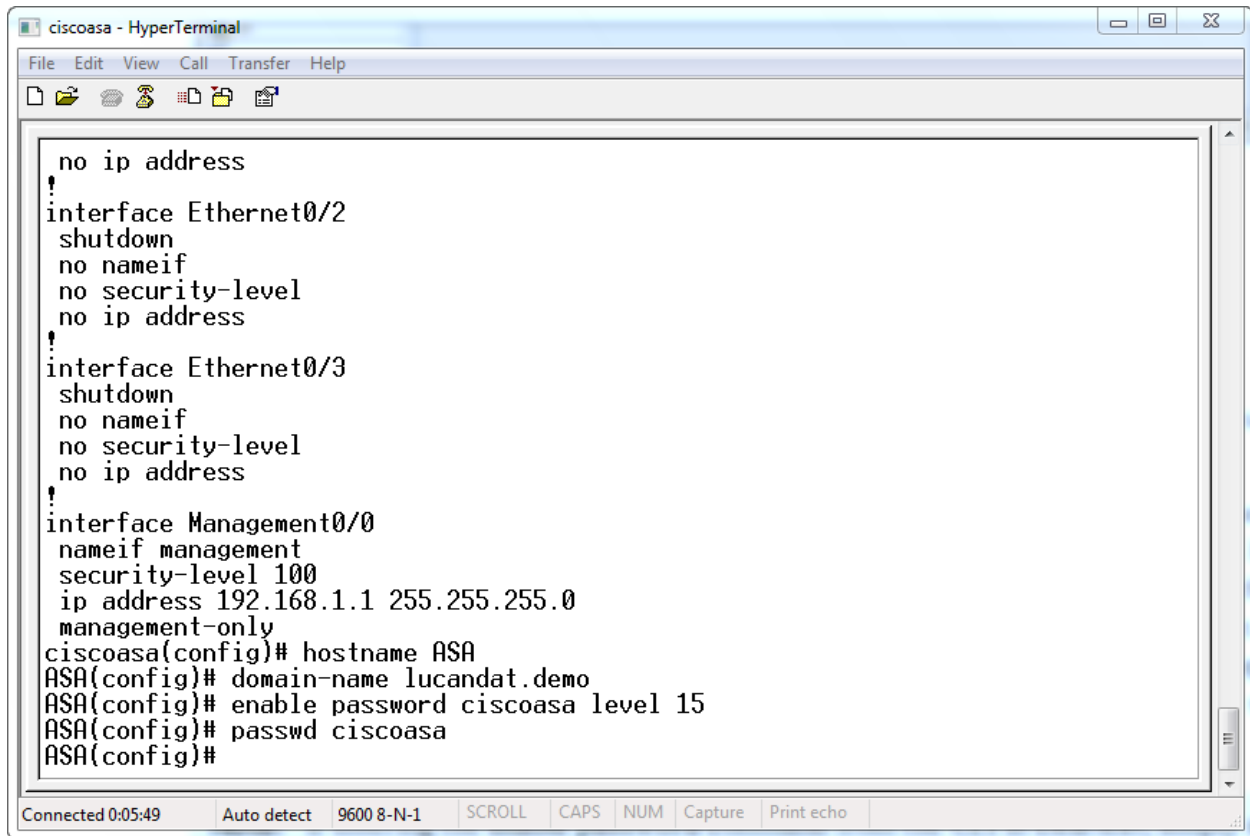
Cấu hình cơ bản với ASDM

The screenshot displays the Cisco ASDM 7.1 for ASA configuration interface. The window title is "Cisco ASDM 7.1 for ASA - 192.168.1.1". The main menu includes File, View, Tools, Wizards, Window, and Help. The left sidebar shows the "Device Setup" tree with options: Startup Wizard, Interfaces, Routing, Device Name/Password (selected), and System Time. Below the tree is a navigation pane with icons for Device Setup, Firewall, Remote Access VPN, Site-to-Site VPN, IPS, and Device Management. The main content area is titled "Configuration > Device Setup > Device Name/Password" and contains the following fields:

- Hostname and Domain Name:**
 - Hostname: ASA
 - Domain Name: lucandat.demo
- Enable Password:**
 - Change the privileged mode password.
 - Old Password: [masked]
 - New Password: [masked]
 - Confirm New Password: [masked]
- Telnet Password:**
 - Change the password to access the console of the security appliance.
 - Old Password: [masked]
 - New Password: [masked]
 - Confirm New Password: [masked]

At the bottom of the configuration area are "Apply" and "Reset" buttons. The status bar at the bottom left shows "Configuration changes saved successfully." and the bottom right shows the user "", page number "15", and a timestamp "1/1/03 1:01:07 AM UTC".

cấu hình với CLI



The image shows a HyperTerminal window titled "ciscoasa - HyperTerminal". The window contains a list of configuration commands for a Cisco ASA device. The commands are as follows:

```
no ip address
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
ciscoasa(config)# hostname ASA
ASA(config)# domain-name lucandat.demo
ASA(config)# enable password ciscoasa level 15
ASA(config)# passwd ciscoasa
ASA(config)#
```

At the bottom of the window, there is a status bar with the following information: "Connected 0:05:49", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

Kiểm tra hostname và domain name với ASDMS

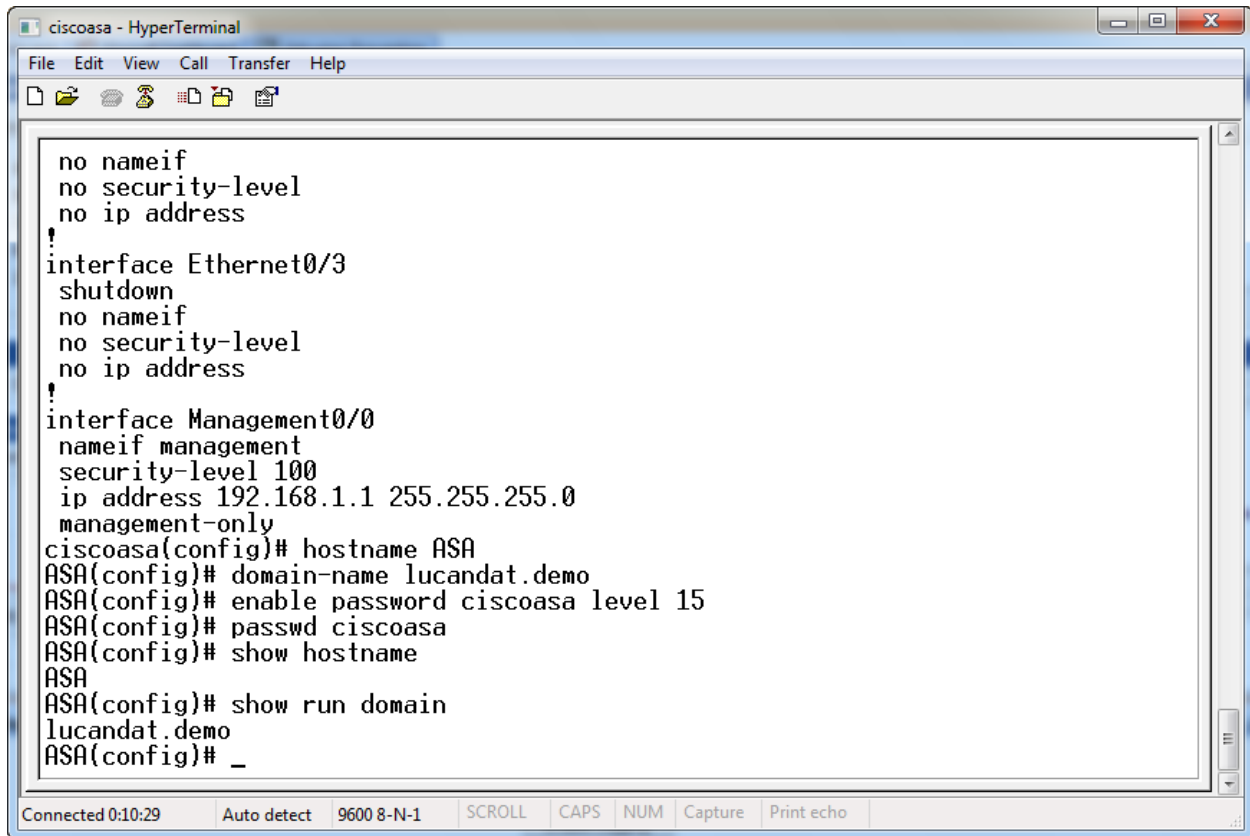
The screenshot displays the Cisco ASDM 7.1 for ASA - 192.168.1.1 interface. The main content area is divided into several sections:

- Device Information:** Shows general and license details. Host Name: **ASA.lucandat.demo**. ASA Version: **8.2(2)**. ASDM Version: **7.1(3)**. Firewall Mode: **Routed**. Total Flash: **256 MB**. Device Uptime: **0d 1h 11m 37s**. Device Type: **ASA 5510, SSM-10**. Context Mode: **Single**. Total Memory: **256 MB**.
- Interface Status:** A table showing interface details for the 'management' interface.

Interface	IP Address/Mask	Line	Link	Kbps
management	192.168.1.1/24	+	up	5
- VPN Sessions:** Shows 0 IPsec, 0 Clientless SSL VPN, and 0 AnyConnect Client sessions.
- System Resources Status:** Includes CPU Usage (percent) and Memory Usage (MB) graphs. CPU usage is currently at 0%.
- Traffic Status:** Shows Connections Per Second Usage and 'management' Interface Traffic Usage (Kbps) graphs.
- Latest ASDM Syslog Messages:** A message indicating that ASDM logging is disabled, with an 'Enable Logging' button.

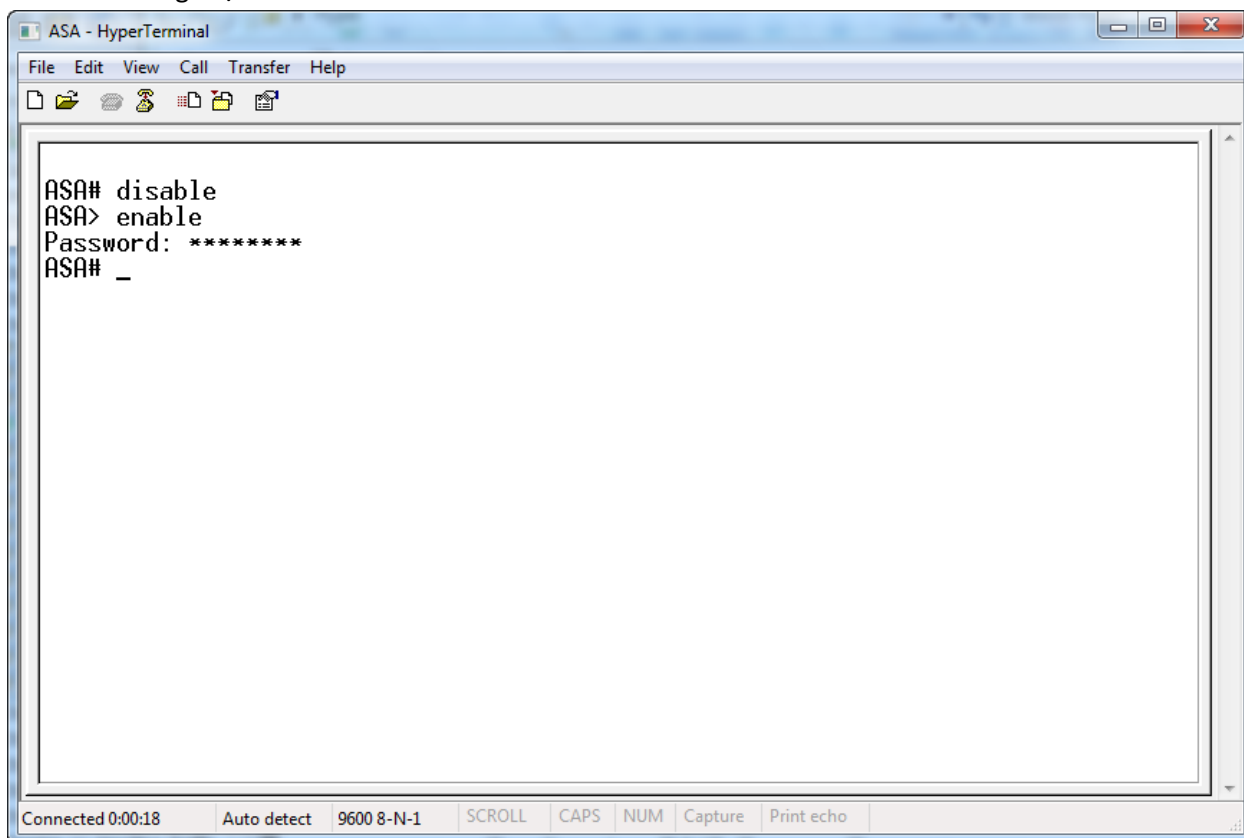
The bottom status bar shows the user is logged in as '<admin>' with 15 sessions, and the time is 1/1/03 1:12:37 AM UTC.

Kiểm tra hostname và domain name với CLI



```
ciscoasa - HyperTerminal
File Edit View Call Transfer Help
no nameif
no security-level
no ip address
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
nameif management
security-level 100
ip address 192.168.1.1 255.255.255.0
management-only
ciscoasa(config)# hostname ASA
ASA(config)# domain-name lucandat.demo
ASA(config)# enable password ciscoasa level 15
ASA(config)# passwd ciscoasa
ASA(config)# show hostname
ASA
ASA(config)# show run domain
lucandat.demo
ASA(config)# _
Connected 0:10:29 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

Kiểm tra chứng thực với CLI



The image shows a HyperTerminal window titled "ASA - HyperTerminal". The window contains a menu bar with "File", "Edit", "View", "Call", "Transfer", and "Help". Below the menu bar is a toolbar with icons for file operations. The main terminal area displays the following text:

```
ASA# disable
ASA> enable
Password: *****
ASA# _
```

At the bottom of the window, there is a status bar with the following information: "Connected 0:00:18", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

Kích hoạt DNS Client trên cổng inside

The screenshot shows the Cisco ASDM 7.1 for ASA configuration interface. The breadcrumb path is Configuration > Device Management > DNS > DNS Client. The main configuration area is titled "Specify how to resolve DNS requests." and includes the following sections:

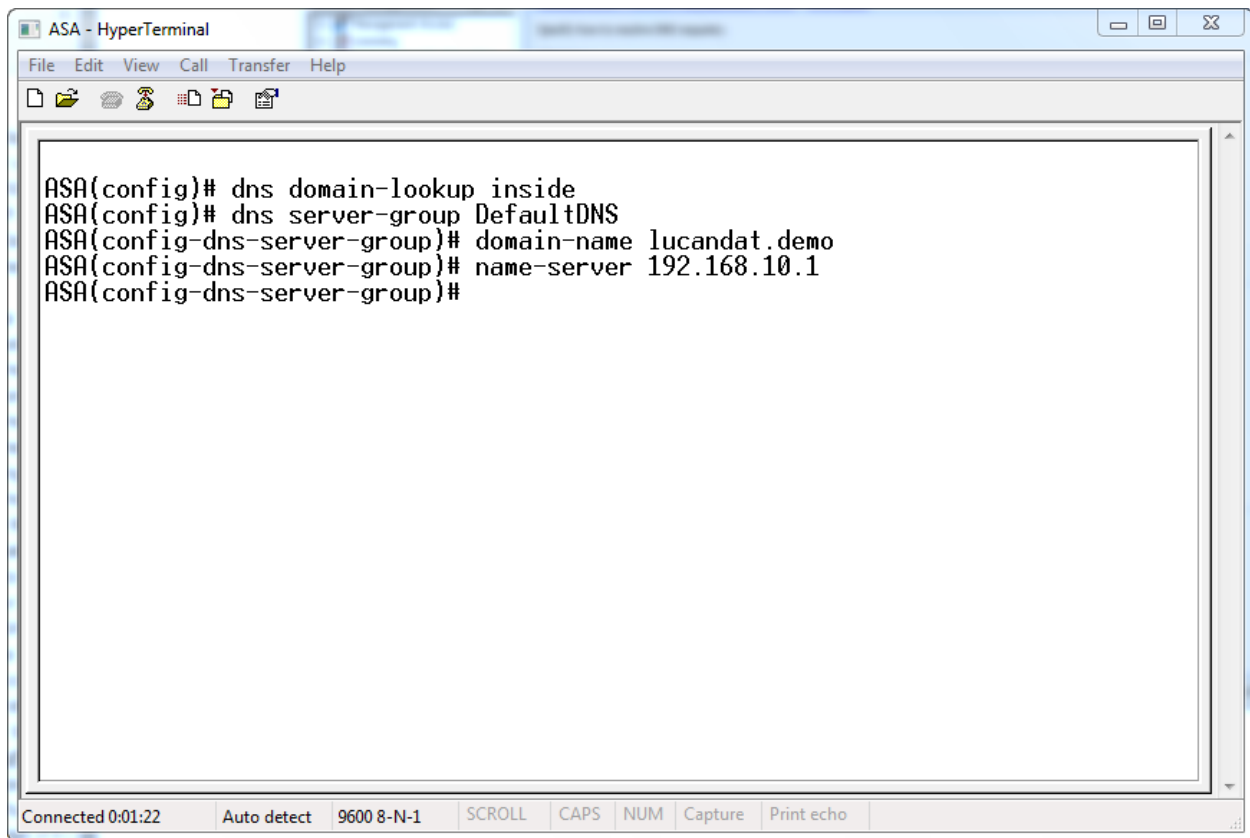
- DNS Setup:** Radio buttons for "Configure one DNS server group" (selected) and "Configure multiple DNS server groups".
 - Primary DNS Server: 192.168.10.1
 - Secondary Servers: (empty text box)
 - Domain Name: lucandat.demo
- DNS Lookup:** A note states "To configure DNS, enable DNS lookup on at least one interface." Below this is a table:

Interface	DNS Enabled
inside	True
management	False
outside	False

- DNS Guard:** A note states "This function enforces one DNS response per query. If DNS inspection is configured, this option is ignored on that interface." Below this is a checkbox for "Enable DNS Guard on all interfaces." which is currently unchecked.

At the bottom of the configuration area are "Apply" and "Reset" buttons. A status bar at the very bottom of the window displays "Configuration changes saved successfully.", the user role "<admin>", the page number "15", and the timestamp "1/1/03 1:22:17 AM UTC".

Cấu hình DNS với CLI



The image shows a HyperTerminal window titled "ASA - HyperTerminal". The window contains a terminal session with the following commands and prompts:

```
ASA(config)# dns domain-lookup inside
ASA(config)# dns server-group DefaultDNS
ASA(config-dns-server-group)# domain-name lucandat.demo
ASA(config-dns-server-group)# name-server 192.168.10.1
ASA(config-dns-server-group)#
```

The terminal window also displays a status bar at the bottom with the following information: "Connected 0:01:22", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

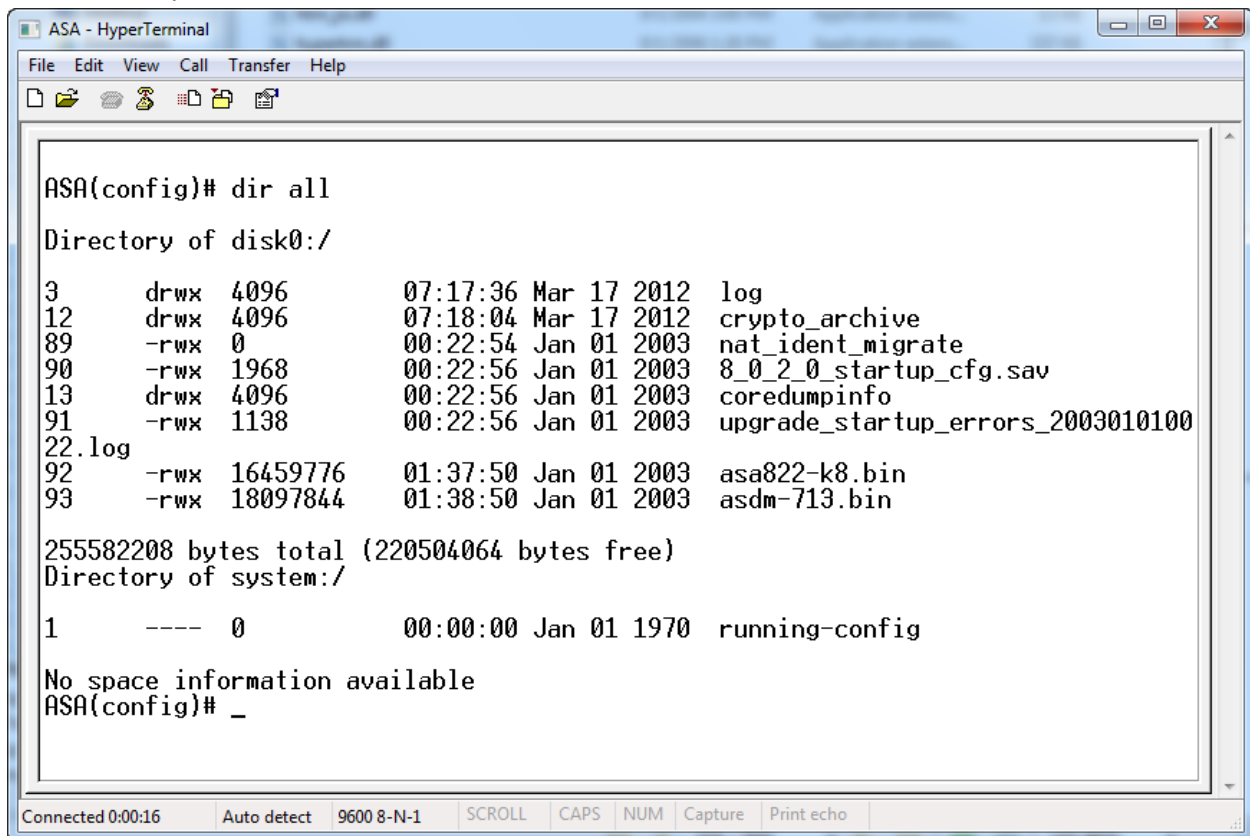
Kiểm tra các tập tin hệ thống với ASDM

The screenshot displays the Cisco ASDM 7.1 interface for ASA 192.168.1.1. The 'File Management' window is open, showing the file system structure of the 'disk0' device. The left pane shows the folder hierarchy, and the right pane shows a table of files and folders. The 'asdm-713.bin' file is highlighted, indicating it is the selected ASDM image.

Flash Space:
Total: 255,582,208 bytes
Available: 220,504,064 bytes

FileName	Size (bytes)	Date Modified	Status
coredumpinfo		01/01/03 00:22:56	
crypto_archive		03/17/12 07:18:04	
log		03/17/12 07:17:36	
8_0_2_0_startup_cfg.sav	1,968	01/01/03 00:22:56	
asa822-k8.bin	16,459,776	01/01/03 01:37:50	
asdm-713.bin	18,097,844	01/01/03 01:38:50	ASDM image
nat_ident_migrate	0	01/01/03 00:22:54	
upgrade_startup_errors_...	1,138	01/01/03 00:22:56	

Kiểm tra file system với CLI



```
ASA - HyperTerminal
File Edit View Call Transfer Help
ASA(config)# dir all
Directory of disk0:/
3      drwx  4096      07:17:36 Mar 17 2012  log
12     drwx  4096      07:18:04 Mar 17 2012  crypto_archive
89     -rwx   0          00:22:54 Jan 01 2003  nat_ident_migrate
90     -rwx  1968      00:22:56 Jan 01 2003  8_0_2_0_startup_cfg.sav
13     drwx  4096      00:22:56 Jan 01 2003  coredumpinfo
91     -rwx  1138      00:22:56 Jan 01 2003  upgrade_startup_errors_2003010100
22.log
92     -rwx 16459776   01:37:50 Jan 01 2003  asa822-k8.bin
93     -rwx 18097844   01:38:50 Jan 01 2003  asdm-713.bin

255582208 bytes total (220504064 bytes free)
Directory of system:/
1      ----  0          00:00:00 Jan 01 1970  running-config

No space information available
ASA(config)# _
Connected 0:00:16  Auto detect  9600 8-N-1  SCROLL  CAPS  NUM  Capture  Print echo
```

Kiểm tra thứ tự boot order của IOS

The screenshot shows the Cisco ASDM 7.1 for ASA configuration interface. The breadcrumb navigation path is Configuration > Device Management > System Image/Configuration > Boot Image/Configuration. The main content area displays the Boot Configuration section, which includes a table for boot images and fields for configuration file paths.

Boot Configuration

Configure boot images from an external TFTP server and flash file system. Up to four images can be configured for the boot system. Only one TFTP boot image can be configured. The TFTP boot image, if configured, must be the first image in the list.

Boot Order	Boot Image Location
1	disk0:/asa822-k8.bin

Buttons: Add, Edit, Delete, Move Up, Move Down

Boot Configuration File Path: Browse Flash...

ASDM Image Configuration

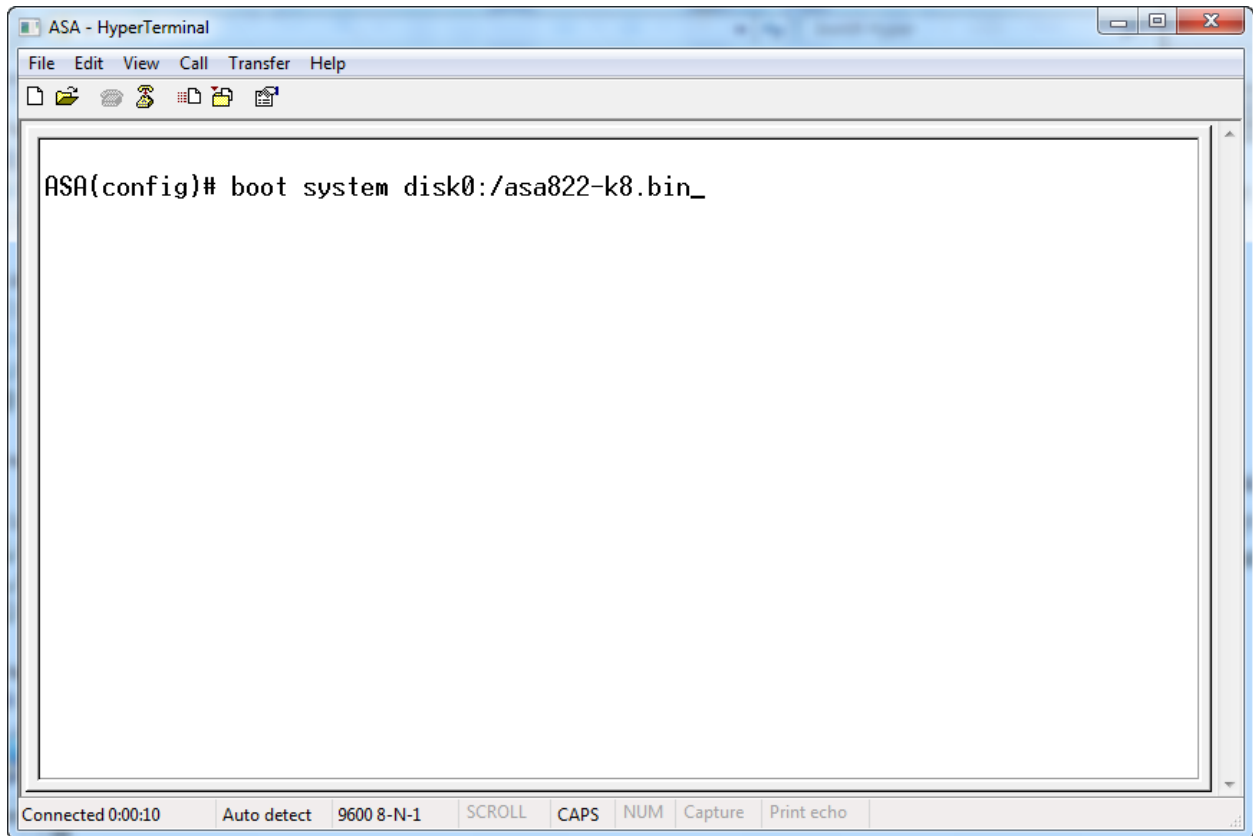
ASDM Image File Path: Browse Flash...

Buttons: Apply, Reset

Device configuration loaded successfully.

System tray: <admin> 15 1/1/03 1:40:07 AM UTC

Khai báo IOS sẽ boot khi khởi động ASA với CLI



Cập nhật ASDM

The screenshot displays the Cisco ASDM 7.1 for ASA interface. The main window is titled "Cisco ASDM 7.1 for ASA - 192.168.1.1". The navigation pane on the left shows the "Device Management" tree with "Boot Image/Configuration" selected. The main content area is titled "Configuration > Device Management > System Image/Configuration > Boot Image/Configuration".

The "Boot Configuration" section contains the following text: "Configure boot images from an external TFTP server and flash file system. Up to four images can be configured for the boot system. Only one TFTP boot image can be configured. The TFTP boot image, if configured, must be the first image in the list."

Boot Order	Boot Image Location
1	disk0:/asa822-k8.bin

An "Upgrade Software" dialog box is open in the foreground. It contains the following fields and buttons:

- Image to Upload: ASDM
- Local File Path: D:\Software hv\ASA\asdm-649.bin
- Flash File System Path: disk0:/asdm-649.bin
- Buttons: Upload Image, Close, Help, Browse Local Files..., Browse Flash...

At the bottom of the main window, there are "Apply" and "Reset" buttons. The status bar at the bottom shows "Device configuration loaded successfully.", "<admin> 15", and the time "1/1/03 1:44:07 AM UTC".

Kiểm tra active-key và cập nhật key với ASDM

Cisco ASDM 7.1 for ASA - 192.168.1.1

Configuration > Device Management > Licensing > Activation Key

Permanent Activation Key

Serial No.: JMX1237L19A
Permanent Activation Key: 0x7524c555 0xe0005cc2 0x391268ec 0xc8c85458 0xc00fda9b

New Activation Key

Configure a new activation key for the device. It will take effect after the next reload.

New Activation Key:

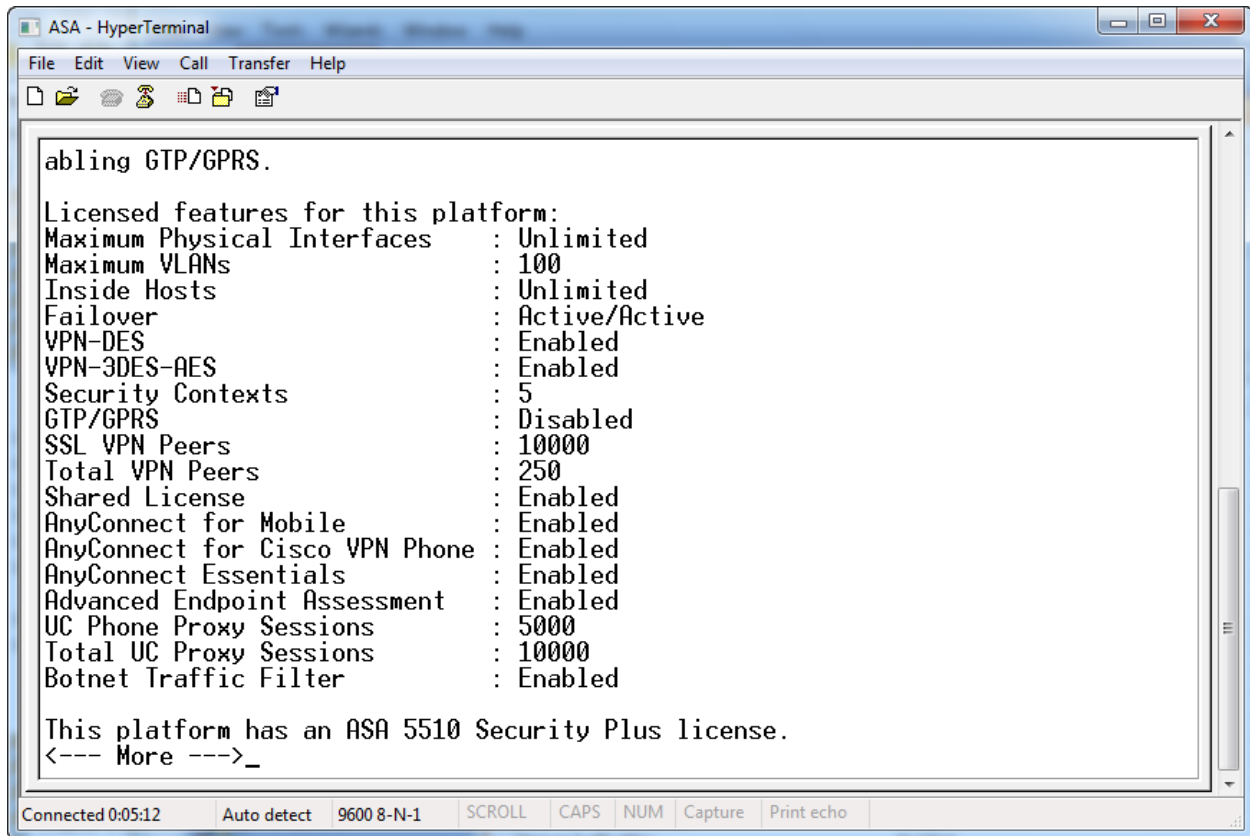
Effective Running Licenses

License Feature	License Value	License Duration
Device license	Security Plus	
Maximum Physical Interfaces	Unlimited	
Maximum VLANs	100	
Inside Hosts	Unlimited	
Falover	Active/Active	
VPN-DES	Enabled	
VPN-3DES-AES	Enabled	
Security Contexts	5	
GTP/GPRS	Disabled	
SSL VPN Peers	10000	
Total VPN Peers	250	
Shared License	Enabled	
AnyConnect for Mobile	Enabled	
AnyConnect for Cisco VPN Phone	Enabled	
AnyConnect Essentials	Enabled	
Advanced Endpoint Assessment	Enabled	
UC Phone Proxy Sessions	5000	
Total UC Proxy Sessions	10000	
Botnet Traffic Filter	Enabled	

Update Activation Key

<admin> 15 1/1/03 1:48:37 AM UTC

Kiểm tra và cập nhập active-key với CLI



```
ASA - HyperTerminal
File Edit View Call Transfer Help
[Icons]

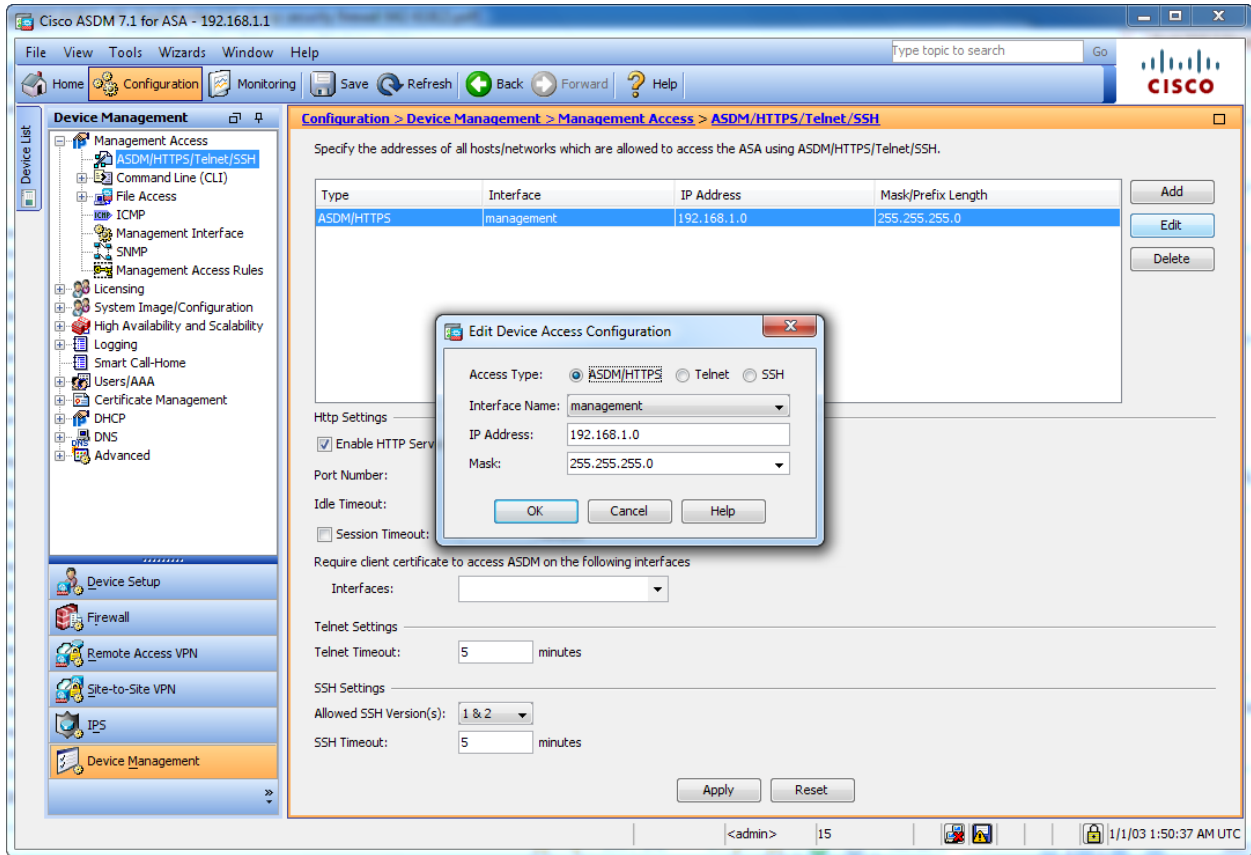
abling GTP/GPRS.

Licensed features for this platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs              : 100
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Enabled
Security Contexts          : 5
GTP/GPRS                    : Disabled
SSL VPN Peers               : 10000
Total VPN Peers             : 250
Shared License              : Enabled
AnyConnect for Mobile       : Enabled
AnyConnect for Cisco VPN Phone : Enabled
AnyConnect Essentials       : Enabled
Advanced Endpoint Assessment : Enabled
UC Phone Proxy Sessions     : 5000
Total UC Proxy Sessions     : 10000
Botnet Traffic Filter        : Enabled

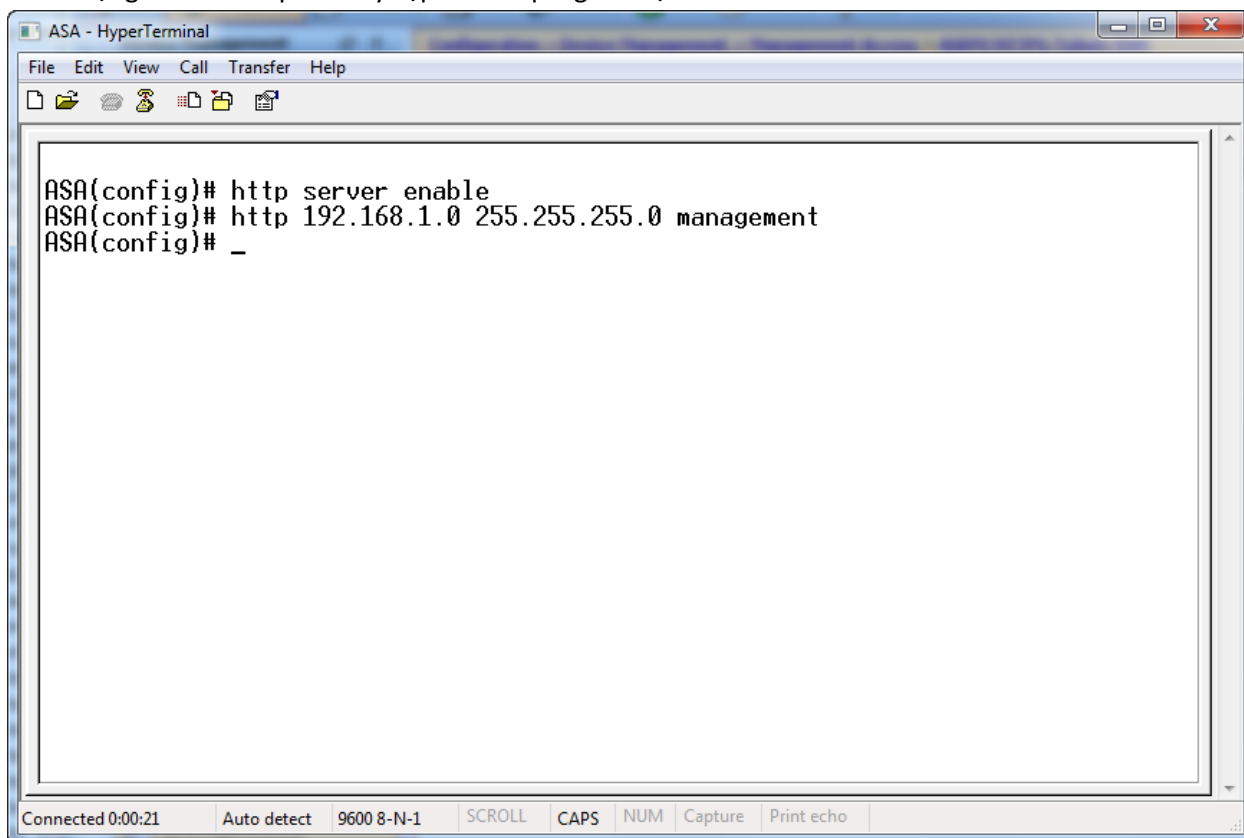
This platform has an ASA 5510 Security Plus license.
<--- More --->_

Connected 0:05:12  Auto detect  9600 8-N-1  SCROLL  CAPS  NUM  Capture  Print echo
```

Kích hoạt cho phép truy cập ASDM qua giao diện web giao thức https



Kích hoạt giao thức http để truy cập ASDM qua giao diện wweb

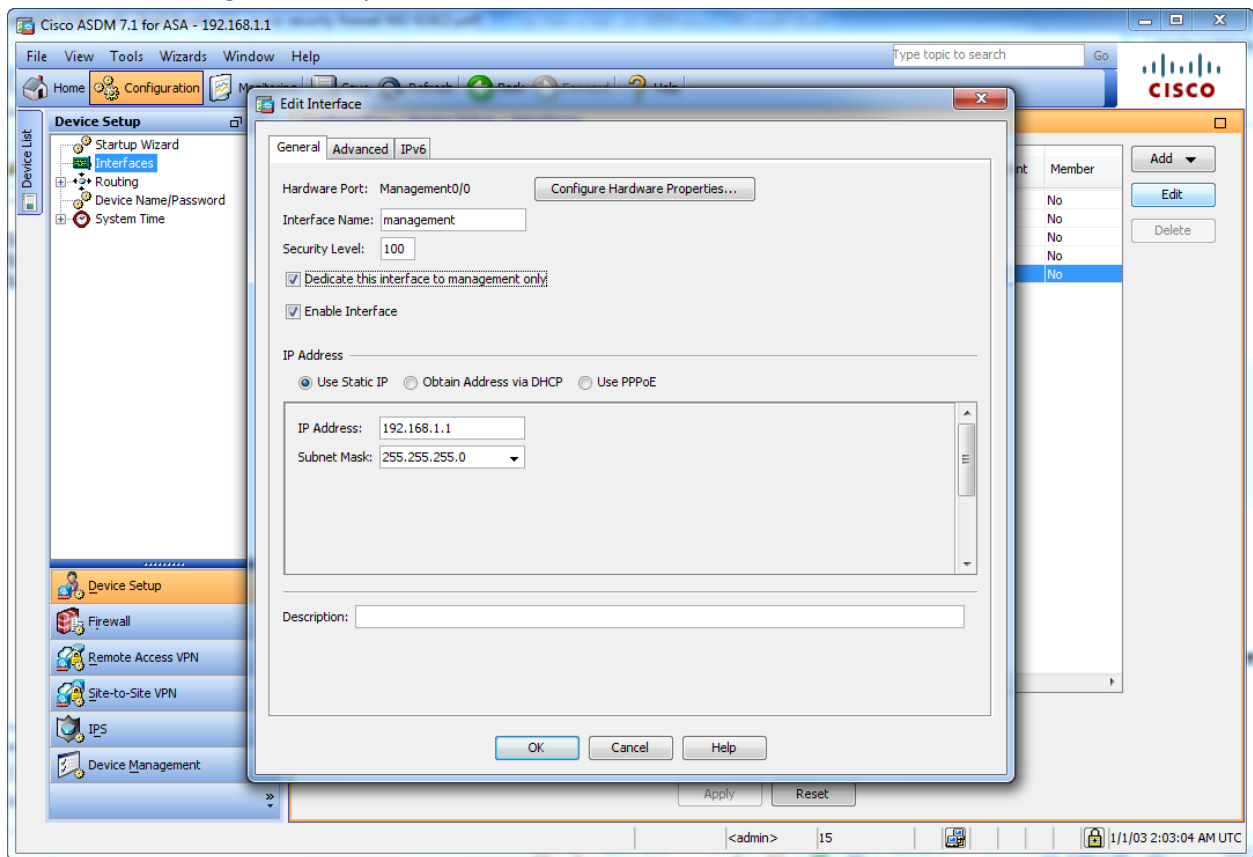


The image shows a HyperTerminal window titled "ASA - HyperTerminal". The window has a menu bar with "File", "Edit", "View", "Call", "Transfer", and "Help". Below the menu bar is a toolbar with icons for file operations. The main area of the window displays the following text:

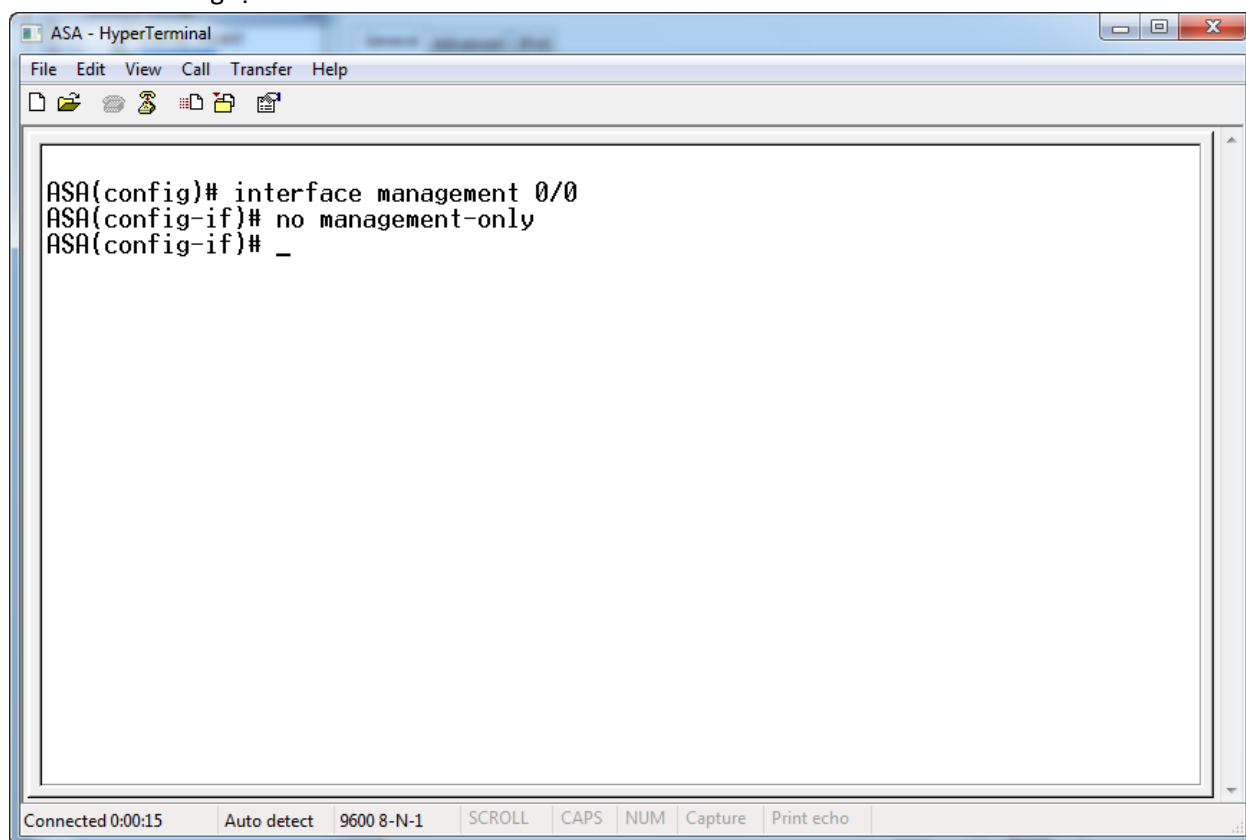
```
ASA(config)# http server enable
ASA(config)# http 192.168.1.0 255.255.255.0 management
ASA(config)# _
```

At the bottom of the window, there is a status bar with the following information: "Connected 0:00:21", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

Cấu hình no management-only trên ASDM



Cấu hình với dòng lệnh



The image shows a HyperTerminal window titled "ASA - HyperTerminal". The window contains a terminal session with the following commands and prompts:

```
ASA(config)# interface management 0/0
ASA(config-if)# no management-only
ASA(config-if)# _
```

The status bar at the bottom of the window displays the following information: "Connected 0:00:15", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

Cấu hình cho phép telnet

The screenshot displays the Cisco ASDM 7.1 for ASA configuration interface. The main window is titled "Cisco ASDM 7.1 for ASA - 192.168.1.1". The navigation pane on the left shows the "Device Management" tree, with "Management Access" expanded to "ASDM/HTTPS/Telnet/SSH". The main content area shows the "ASDM/HTTPS/Telnet/SSH" configuration page, which includes a table of access rules and various settings.

The table lists the current configuration for ASDM/HTTPS access:

Type	Interface	IP Address	Mask/Prefix Length
ASDM/HTTPS	management	192.168.1.0	255.255.255.0

An "Edit Device Access Configuration" dialog box is open, showing the configuration for a Telnet access rule. The "Access Type" is set to "Telnet". The "Interface Name" is "management", the "IP Address" is "192.168.1.0", and the "Mask" is "255.255.255.0".

The "Edit Device Access Configuration" dialog box contains the following fields:

- Access Type: ASDM/HTTPS Telnet SSH
- Interface Name: management
- IP Address: 192.168.1.0
- Mask: 255.255.255.0

Buttons: OK, Cancel, Help

The main configuration page also includes sections for "Http Settings", "Telnet Settings", and "SSH Settings".

Http Settings:

- Enable HTTP Service
- Port Number: []
- Idle Timeout: []
- Session Timeout: []

Require client certificate to access ASDM on the following interfaces:

Interfaces: []

Telnet Settings:

- Telnet Timeout: 5 minutes

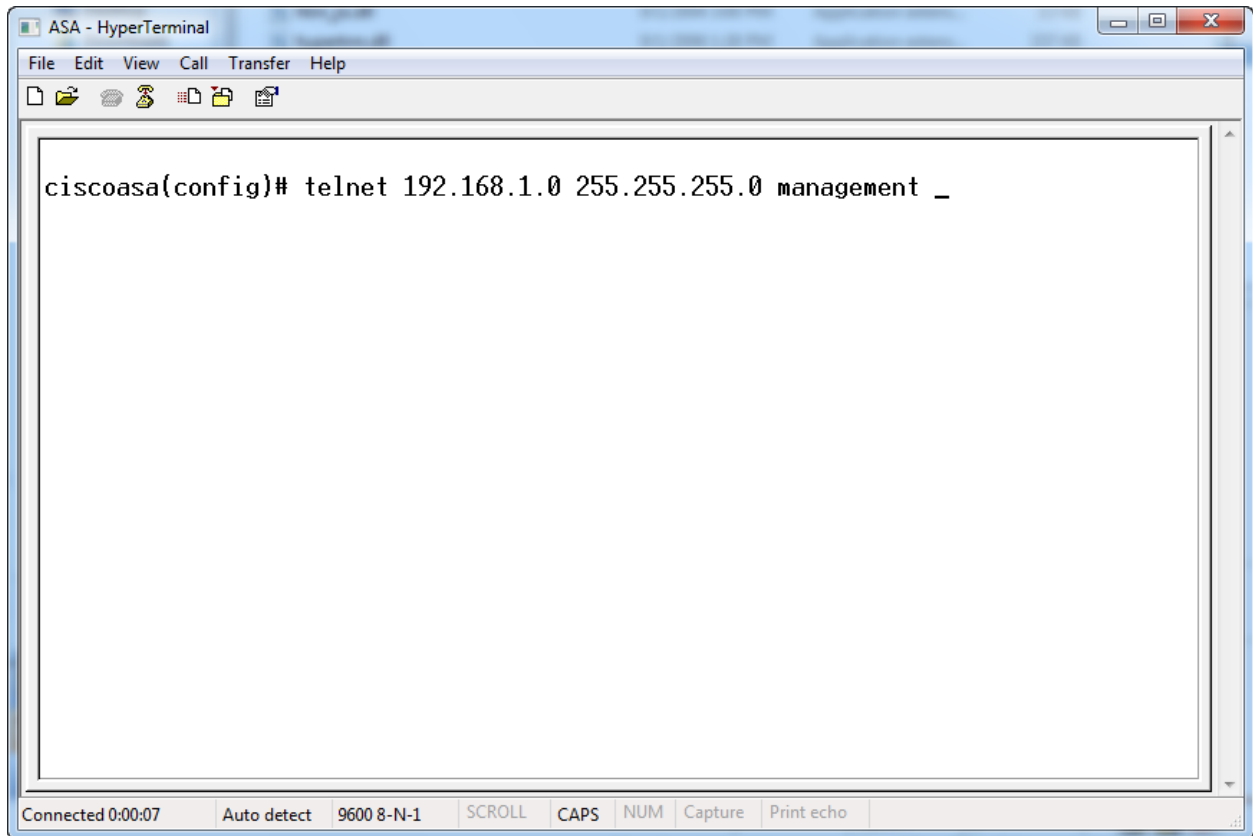
SSH Settings:

- Allowed SSH Version(s): 1 & 2
- SSH Timeout: 5 minutes

Buttons: Apply, Reset

System tray: <admin> 15 1/1/03 2:09:41 AM UTC

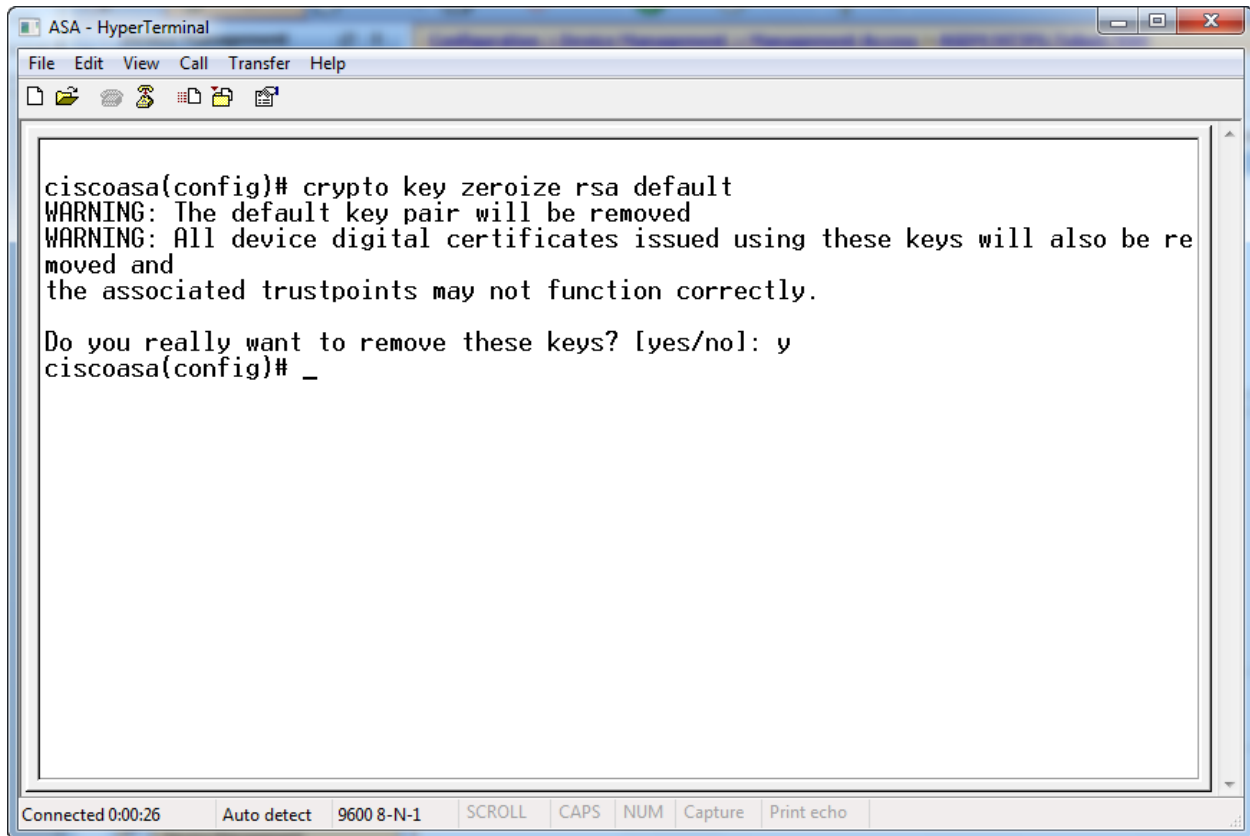
Cấu hình cho phép telnet với CLI



The image shows a HyperTerminal window titled "ASA - HyperTerminal". The window contains a menu bar with "File", "Edit", "View", "Call", "Transfer", and "Help". Below the menu bar is a toolbar with icons for file operations. The main text area displays the command: `ciscoasa(config)# telnet 192.168.1.0 255.255.255.0 management _`. At the bottom of the window, a status bar shows "Connected 0:00:07", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

```
ciscoasa(config)# telnet 192.168.1.0 255.255.255.0 management _
```

Xoá key RSA mặc định



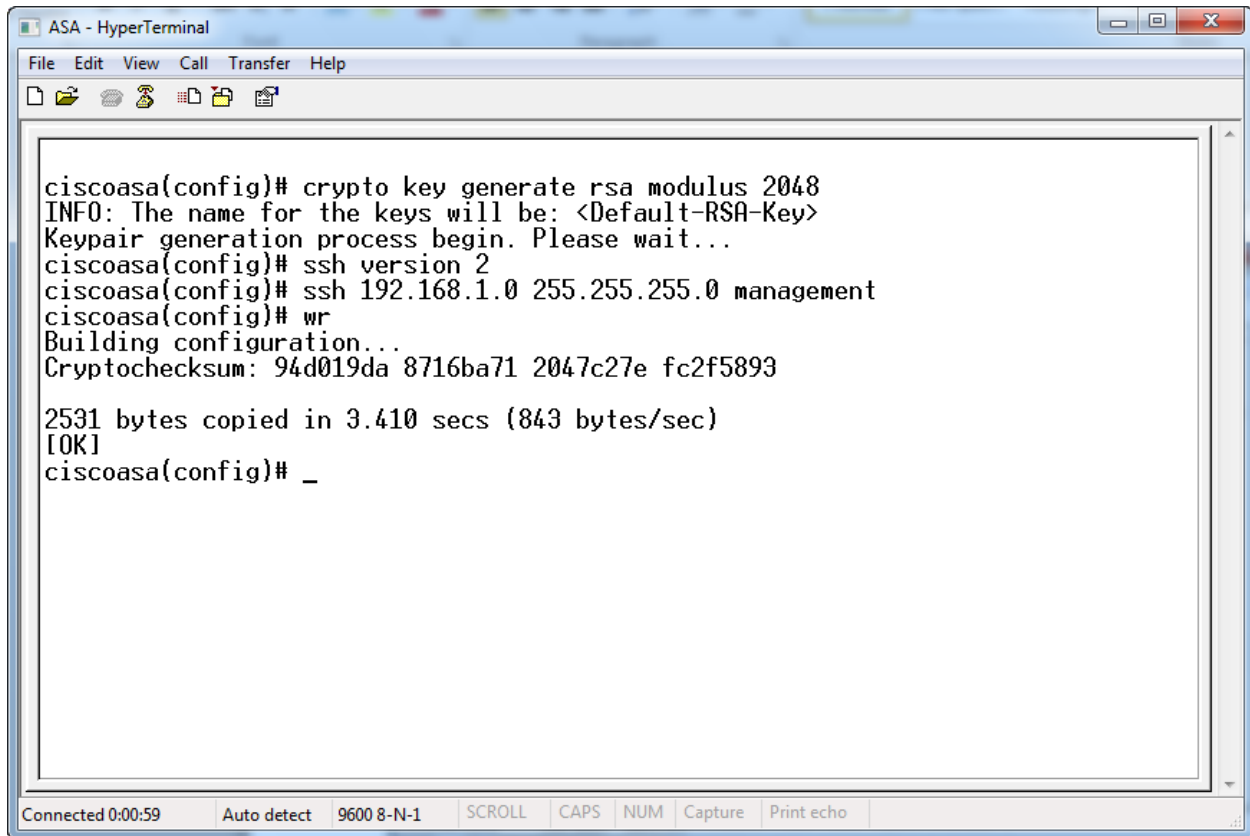
The screenshot shows a HyperTerminal window titled "ASA - HyperTerminal". The window contains a terminal session with the following text:

```
ciscoasa(config)# crypto key zeroize rsa default
WARNING: The default key pair will be removed
WARNING: All device digital certificates issued using these keys will also be removed and
the associated trustpoints may not function correctly.

Do you really want to remove these keys? [yes/no]: y
ciscoasa(config)# _
```

The status bar at the bottom of the window displays "Connected 0:00:26", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

Tạo key rsa mới



```
ASA - HyperTerminal
File Edit View Call Transfer Help
ciscoasa(config)# crypto key generate rsa modulus 2048
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
ciscoasa(config)# ssh version 2
ciscoasa(config)# ssh 192.168.1.0 255.255.255.0 management
ciscoasa(config)# wr
Building configuration...
Cryptochecksum: 94d019da 8716ba71 2047c27e fc2f5893

2531 bytes copied in 3.410 secs (843 bytes/sec)
[OK]
ciscoasa(config)# _

Connected 0:00:59  Auto detect  9600 8-N-1  SCROLL  CAPS  NUM  Capture  Print echo
```

Kích hoạt ssh

Cisco ASDM 7.1 for ASA - 192.168.1.1

Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH

Specify the addresses of all hosts/networks which are allowed to access the ASA using ASDM/HTTPS/Telnet/SSH.

Type	Interface	IP Address	Mask/Prefix Length
ASDM/HTTPS	management	192.168.1.0	255.255.255.0

Edit Device Access Configuration

Access Type: ASDM/HTTPS Telnet SSH

Interface Name: management

IP Address: 192.168.1.0

Mask: 255.255.255.0

Http Settings

Enable HTTP Service

Port Number:

Idle Timeout:

Session Timeout:

Require client certificate to access ASDM on the following interfaces

Interfaces:

Telnet Settings

Telnet Timeout: 5 minutes

SSH Settings

Allowed SSH Version(s): 1 & 2

SSH Timeout: 5 minutes

Apply Reset

<admin> 15 1/1/03 2:17:51 AM UTC

Tạo user cho phép truy cập ASDM

Cisco ASDM 7.1 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Configuration > Device Management > Users/AAA > User Accounts

Create entries in the ASA local user database.

Add User Account

Identity

VPN Policy

Username: lucandat

Password: *****

Confirm Password: *****

User authenticated using MSCHAP

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.
Note: All users have network access, regardless of these settings.

Full access(ASDM, SSH, Telnet and Console)
Privilege level is used with command authorization.
Privilege Level: 15

CLI login prompt for SSH, Telnet and console (no ASDM access)
This setting is effective only if "aaa authentication http console LOCAL" command is confi

No ASDM, SSH, Telnet or Console access
This setting is effective only if "aaa authentication http console LOCAL" and "aaa authori

Find: [] Next Previous

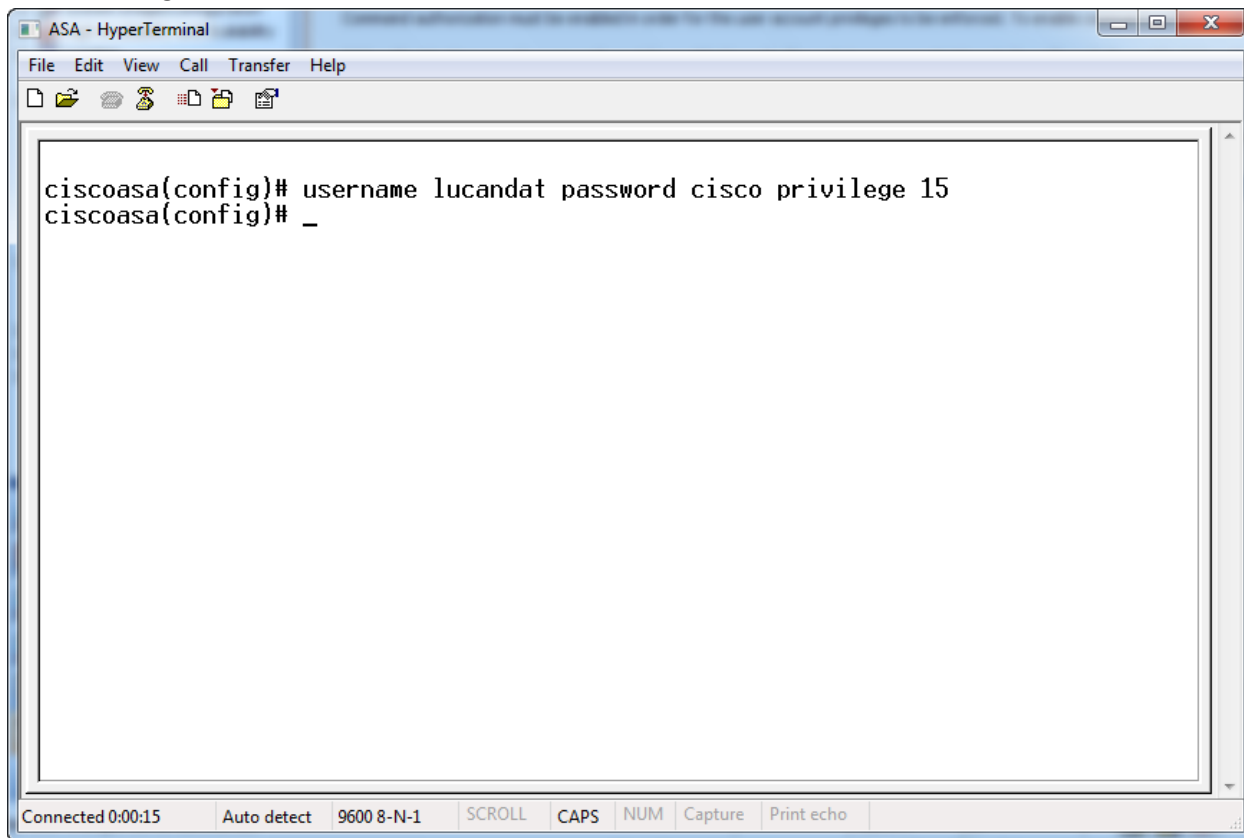
OK Cancel Help

Apply Reset

Configuration changes saved successfully.

<admin> 15 1/1/03 2:26:41 AM UTC

Tạo user bằng CLI



The image shows a HyperTerminal window titled "ASA - HyperTerminal". The window contains a terminal session with the following text:

```
ciscoasa(config)# username lucandat password cisco privilege 15  
ciscoasa(config)# _
```

The terminal window has a menu bar with "File", "Edit", "View", "Call", "Transfer", and "Help". Below the menu bar is a toolbar with icons for file operations. At the bottom of the window, there is a status bar with the following text: "Connected 0:00:15", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

Tạo AAA Server GROUP

The screenshot displays the Cisco ASDM 7.1 for ASA configuration interface. The main window shows the configuration path: Configuration > Device Management > Users/AAA > AAA Server Groups. A table lists the existing AAA Server Groups:

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	LOCAL				1

An "Add AAA Server Group" dialog box is open, with the following configuration:

- AAA Server Group: Tacacs
- Protocol: TACACS+
- Accounting Mode: Simultaneous Single
- Reactivation Mode: Depletion Timed
- Dead Time: 10 minutes
- Max Failed Attempts: 3

The dialog box has OK, Cancel, and Help buttons. The background configuration page includes a search bar, a "Find:" field, and a "Match Case" checkbox. The status bar at the bottom shows "Device configuration loaded successfully.", the user is logged in as "<admin>", and the time is 1/1/03 2:32:31 AM UTC.

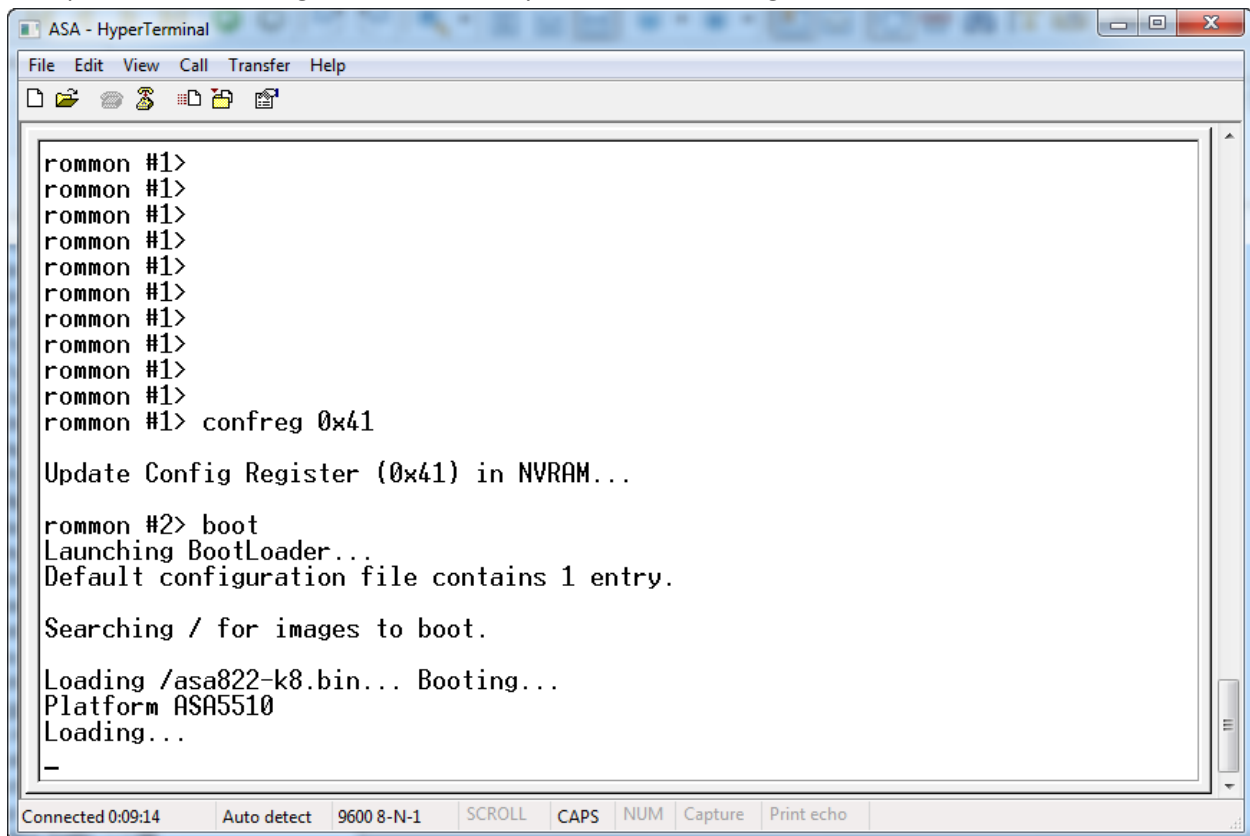
Chứng thực truy cập với tacacs

The screenshot displays the Cisco ASDM 7.1 for ASA configuration interface. The main window is titled "Configuration > Device Management > Users/AAA > AAA Access > Authentication". The left sidebar shows a tree view of configuration categories, with "Users/AAA" expanded to show "AAA Access". The main content area is divided into three tabs: "Authentication", "Authorization", and "Accounting". The "Authentication" tab is active, showing the following configuration options:

- Enable authentication for administrator access to the ASA. (checked)
- Require authentication to allow use of privileged mode commands:
 - Enable
 - Server Group: Tacacs
 - Use LOCAL when server group fails
- Require authentication for the following types of connections:
 - HTTP/ASDM: Server Group: Tacacs, Use LOCAL when server group fails
 - Serial: Server Group: Tacacs, Use LOCAL when server group fails
 - SSH: Server Group: Tacacs, Use LOCAL when server group fails
 - Telnet: Server Group: Tacacs, Use LOCAL when server group fails

At the bottom of the configuration area, there are "Apply" and "Reset" buttons. A status bar at the bottom of the window indicates "Configuration changes saved successfully." and shows the user as "<admin>" with a session ID of "15". The system time is "1/1/03 2:33:01 AM UTC".

Khôi phục mật khẩu bằng cách nhấn ESC hay Break khi khởi động ASA



```
ASA - HyperTerminal
File Edit View Call Transfer Help
rommon #1>
rommon #1>
rommon #1>
rommon #1>
rommon #1>
rommon #1>
rommon #1>
rommon #1>
rommon #1>
rommon #1>
rommon #1>
rommon #1>
rommon #1> confreg 0x41

Update Config Register (0x41) in NVRAM...

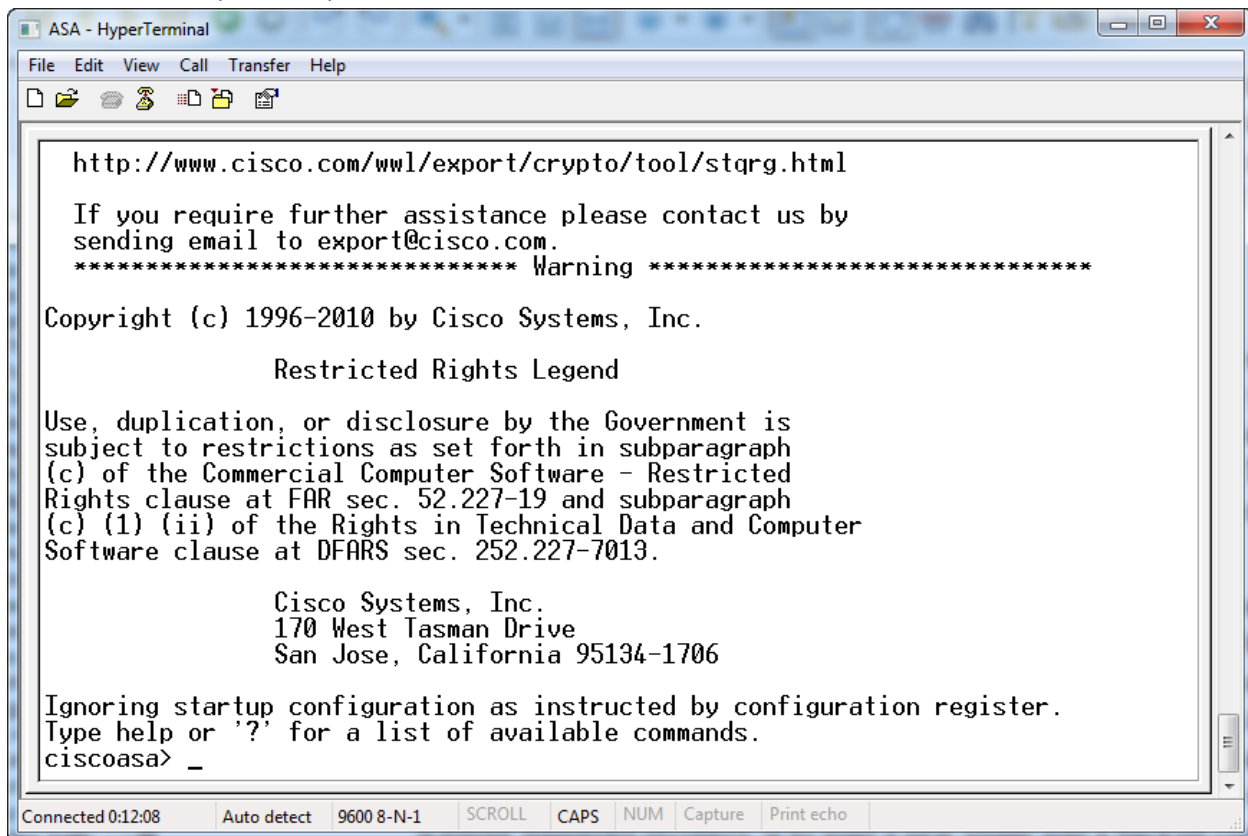
rommon #2> boot
Launching BootLoader...
Default configuration file contains 1 entry.

Searching / for images to boot.

Loading /asa822-k8.bin... Booting...
Platform ASA5510
Loading...
_

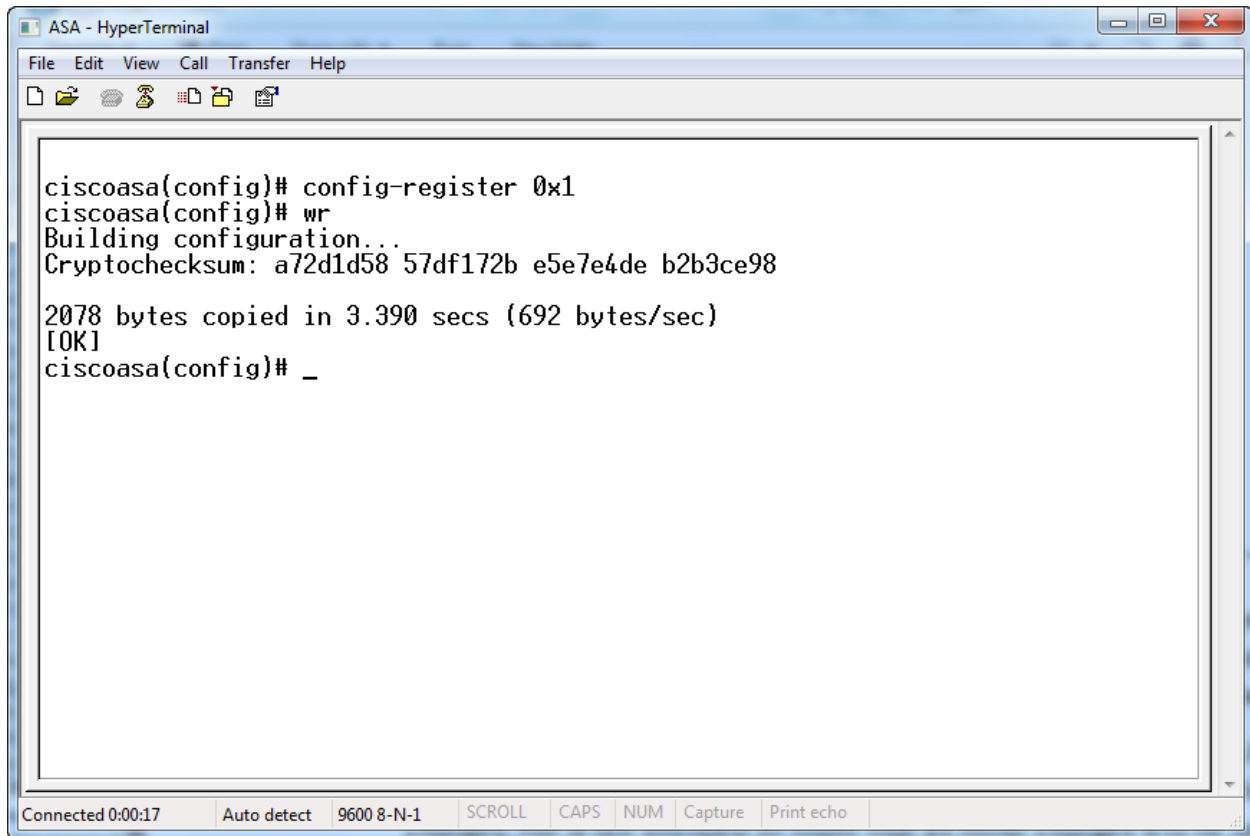
Connected 0:09:14 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

Giao diện sau khi phục hồi password



```
ASA - HyperTerminal
File Edit View Call Transfer Help
http://www.cisco.com/wvl/export/crypto/tool/stgrg.html
If you require further assistance please contact us by
sending email to export@cisco.com.
***** Warning *****
Copyright (c) 1996-2010 by Cisco Systems, Inc.
Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
Ignoring startup configuration as instructed by configuration register.
Type help or '?' for a list of available commands.
ciscoasa> _
Connected 0:12:08 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

Cấu hình cho phép lần sau khởi động bình thường



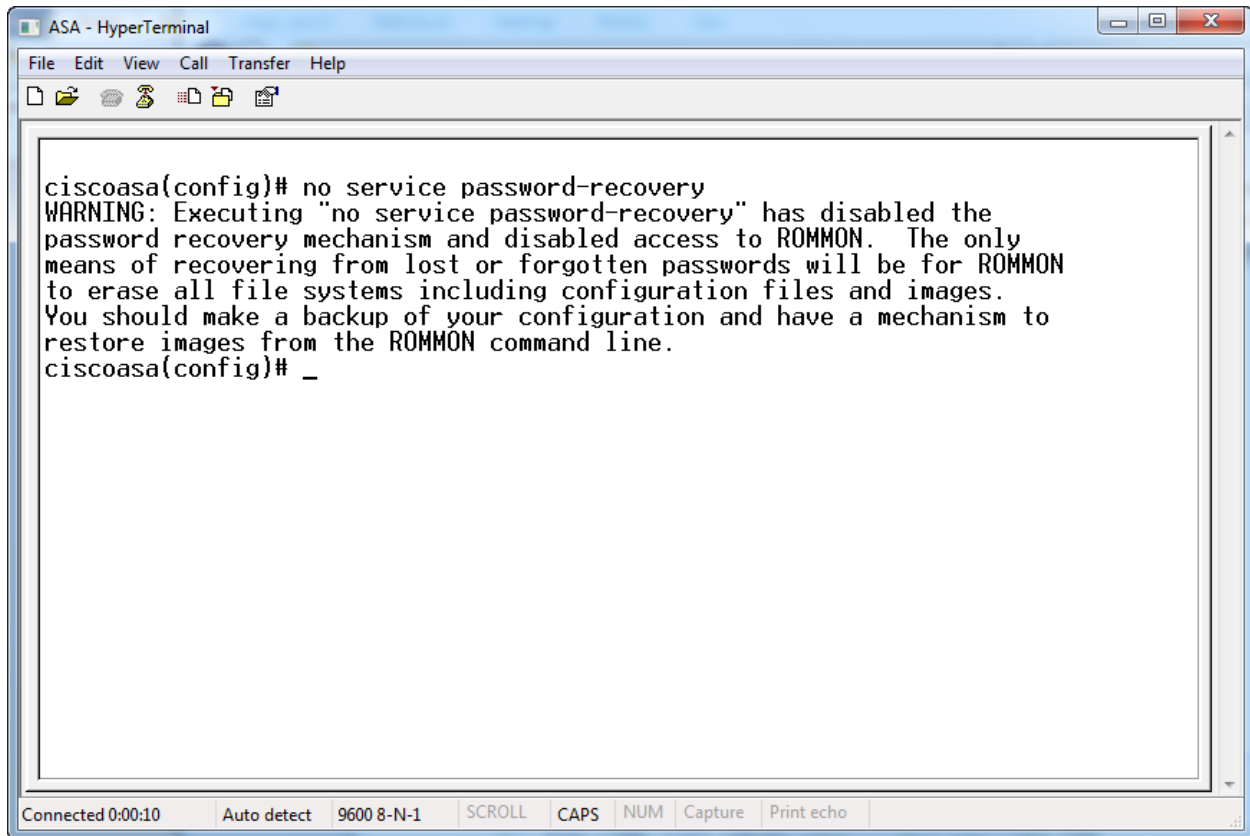
```
ASA - HyperTerminal
File Edit View Call Transfer Help
[Icons]

ciscoasa(config)# config-register 0x1
ciscoasa(config)# wr
Building configuration...
Cryptochecksum: a72d1d58 57df172b e5e7e4de b2b3ce98

2078 bytes copied in 3.390 secs (692 bytes/sec)
[OK]
ciscoasa(config)# _

Connected 0:00:17  Auto detect  9600 8-N-1  SCROLL  CAPS  NUM  Capture  Print echo
```

Cấu hình ngăn chặn service password-recovery



```
ASA - HyperTerminal
File Edit View Call Transfer Help
[Icons]

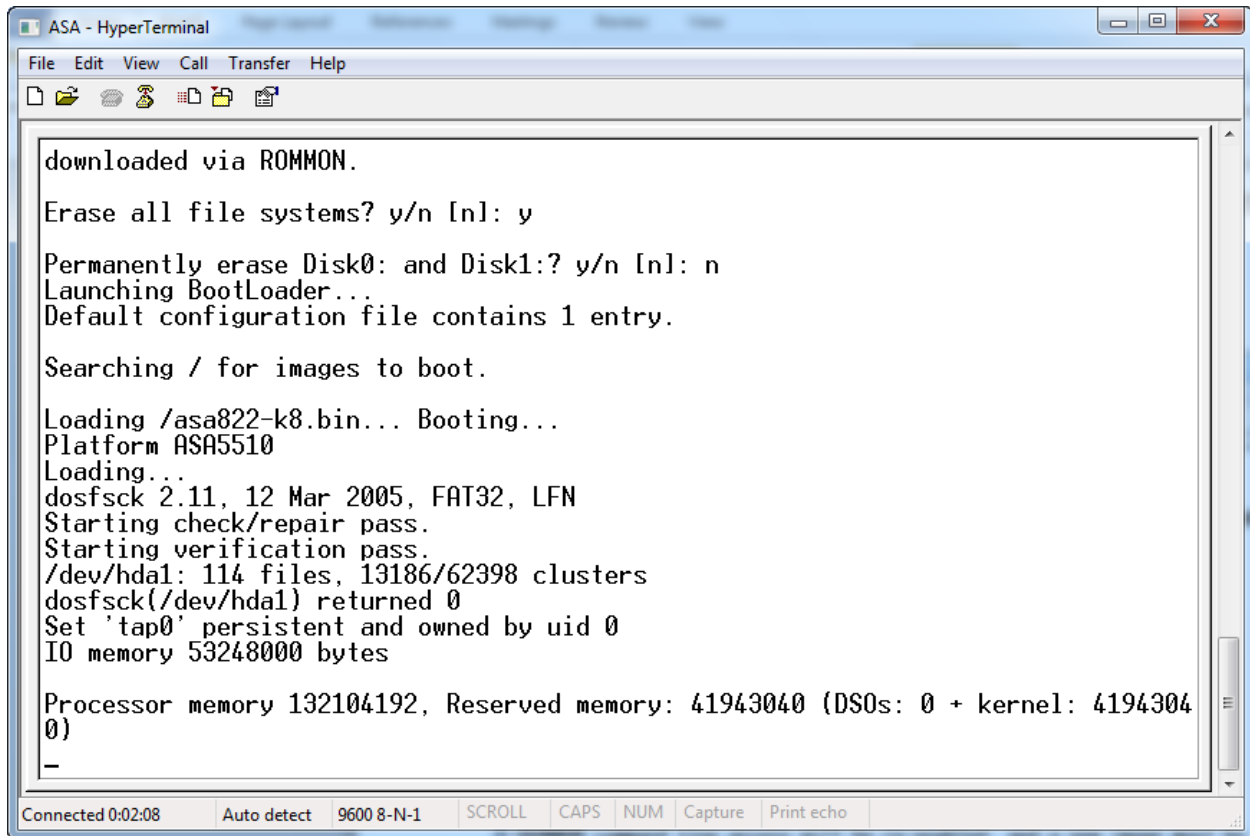
ciscoasa(config)# no service password-recovery
WARNING: Executing "no service password-recovery" has disabled the
password recovery mechanism and disabled access to ROMMON. The only
means of recovering from lost or forgotten passwords will be for ROMMON
to erase all file systems including configuration files and images.
You should make a backup of your configuration and have a mechanism to
restore images from the ROMMON command line.
ciscoasa(config)# _

Connected 0:00:10  Auto detect  9600 8-N-1  SCROLL  CAPS  NUM  Capture  Print echo
```

Sau khi cấu hình no service password-recovery, ASA bắt buộc user phải xoá tất cả cấu hình.

```
ASA - HyperTerminal
File Edit View Call Transfer Help
Launch BIOS Extension to setup ROMMON
Cisco Systems ROMMON Version (1.0(11)4) #0: Fri Mar 21 17:35:35 PDT 2008
Platform ASA5510
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.
Management0/0
Link is UP
MAC Address: 0021.d8cb.e342
WARNING: Password recovery and ROMMON command line access has been
disabled by your security policy. Choosing YES below will cause ALL
configurations, passwords, images, and files systems to be erased.
ROMMON command line access will be re-enabled, and a new image must be
downloaded via ROMMON.
Erase all file systems? y/n [n]: _
Connected 0:01:21 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

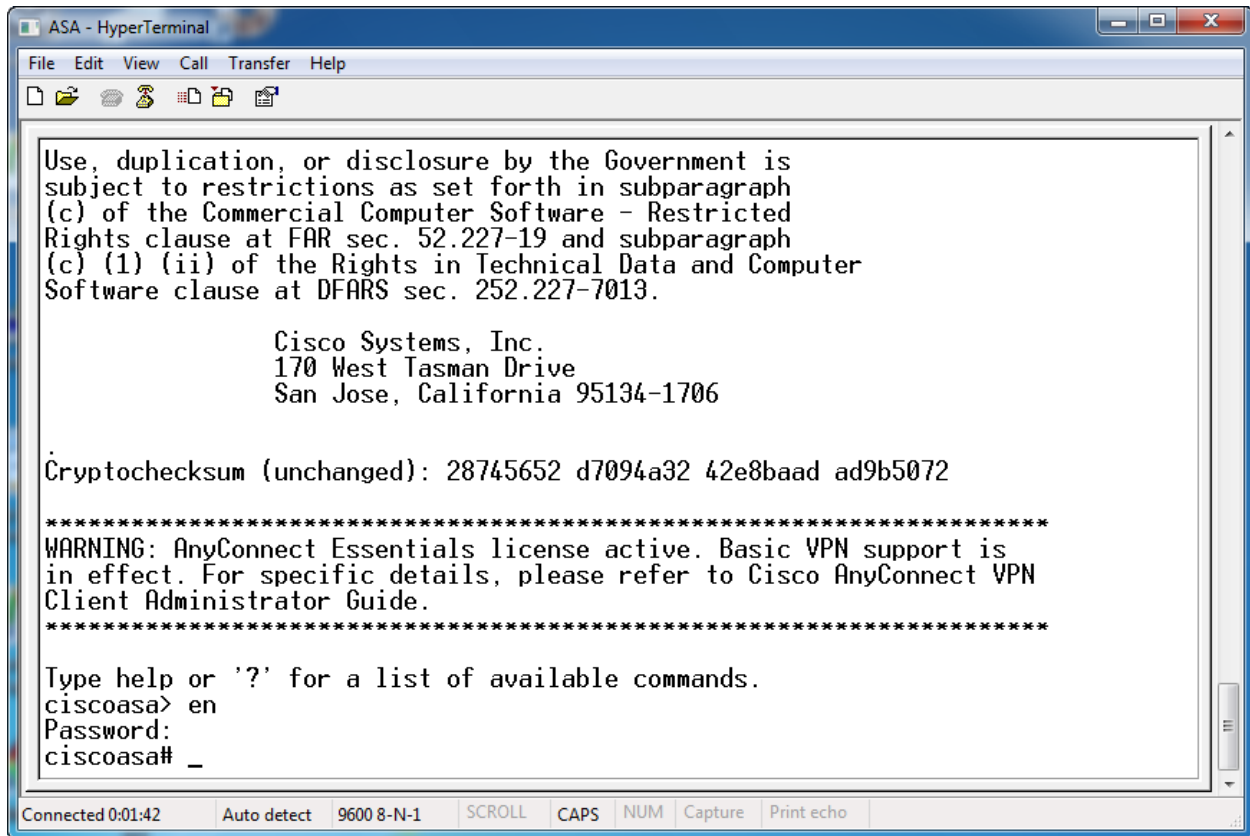

ASA khởi động lại



```
ASA - HyperTerminal
File Edit View Call Transfer Help
downloaded via ROMMON.
Erase all file systems? y/n [n]: y
Permanently erase Disk0: and Disk1:? y/n [n]: n
Launching BootLoader...
Default configuration file contains 1 entry.
Searching / for images to boot.
Loading /asa822-k8.bin... Booting...
Platform ASA5510
Loading...
dosfsck 2.11, 12 Mar 2005, FAT32, LFN
Starting check/repair pass.
Starting verification pass.
/dev/hda1: 114 files, 13186/62398 clusters
dosfsck(/dev/hda1) returned 0
Set 'tap0' persistent and owned by uid 0
IO memory 53248000 bytes

Processor memory 132104192, Reserved memory: 41943040 (DS0s: 0 + kernel: 41943040)
-
Connected 0:02:08 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

ASA sau khi boot xong sẽ trở lại giao diện cấu hình mặc định không có password



```
ASA - HyperTerminal
File Edit View Call Transfer Help
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cryptochecksum (unchanged): 28745652 d7094a32 42e8baad ad9b5072

*****
WARNING: AnyConnect Essentials license active. Basic VPN support is
in effect. For specific details, please refer to Cisco AnyConnect VPN
Client Administrator Guide.
*****

Type help or '?' for a list of available commands.
ciscoasa> en
Password:
ciscoasa# _

Connected 0:01:42 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```