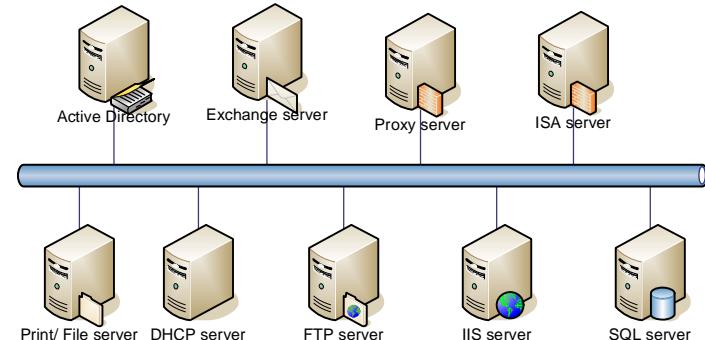


# Quản trị mạng Linux

## Mục tiêu khóa học



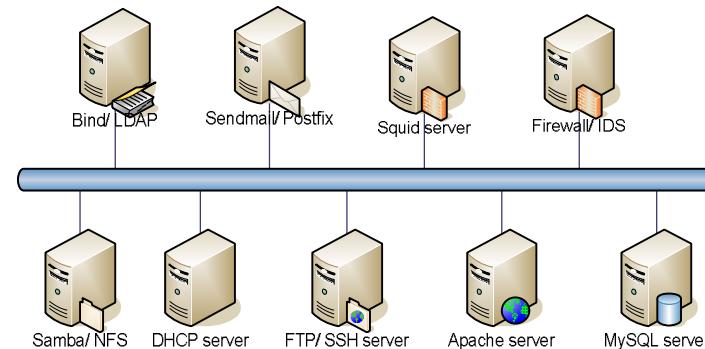
An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Mục tiêu khóa học (tt)

- Sử dụng máy tính Linux đáp ứng các yêu cầu chức năng như máy tính Windows.
- Thay thế mô hình mạng các server Windows bằng mô hình mạng các server Linux.
- Các server Linux đáp ứng đủ vai trò như server Windows, có khả năng quản lý tốt, chịu lỗi tốt.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Mục tiêu khóa học (tt)



An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Nội dung khóa học

### ◎ Installing Linux as a Server

- Technical Summary of Linux Distributions
- Installing Linux in a Server Configuration
- Installing Software

An Ninh Mạng ATHENA, www.athena.com.vn

## Nội dung khóa học (tt)

### ◎ Single host Administration

- Managing User
- The Command Line
- Booting and shutting down
- File Systems
- Core System Services
- Compiling the Linux Kernel

An Ninh Mạng ATHENA, www.athena.com.vn

## Nội dung khóa học (tt)

### ◎ Intranet services

- Networking Fundamentals
- DHCP server
- Samba/ NFS server
- NIS
- LDAP

An Ninh Mạng ATHENA, www.athena.com.vn

## Nội dung khóa học (tt)

### ◎ Internet services

- FPT/ SSH server
- DNS server
- Web server/ Database server
- Proxy server
- Mail server
- Firewall server
- IDS

An Ninh Mạng ATHENA, www.athena.com.vn

## Hỏi & Đáp



An Ninh Mạng ATHENA, www.athena.com.vn



## Technical summary of Linux Distributions

## Nội dung

- Phần mềm mã nguồn mở và GNU General Public License.
- Lịch sử phát triển của Linux
- Đặc điểm của hệ điều hành Linux.
- Khác biệt giữa hệ điều hành Linux và Windows.
- Lợi ích và hạn chế của hệ điều hành Linux.
- Các phiên bản Linux chính.

An Ninh Mạng ATHENA, www.athena.com.vn

## Mã nguồn mở và GPL

- GNU GPL: GNU General Public License.
- Mọi người đều có thể có source code của mã nguồn mở, chỉnh sửa, biên dịch theo ý riêng.
- Mã nguồn mở đã chỉnh sửa có thể dùng cho mục đích riêng hoặc công khai. Nếu công khai phải cung cấp đầy đủ source code.
- Linux là hệ điều hành mã nguồn mở, được phân phối theo quy định của GNU GPL.

An Ninh Mạng ATHENA, www.athena.com.vn

## Mã nguồn mở và GPL (tt)

- Có thể tính phí khi phân phối một sản phẩm có nguồn gốc là mã nguồn mở.
- Tuy nhiên, khi phân phối phải kèm theo source code.
- Khi người sử dụng đã có một phần mềm mã nguồn mở, họ được tự do chỉnh sửa, chia sẻ, phân phối lại...

An Ninh Mạng ATHENA, www.athena.com.vn

## Lịch sử Linux

- Linux được Linus Torvalds viết năm 1991.
- Được cộng đồng Internet đón nhận.
- Nhiều người tình nguyện tham gia phát triển Linux.
- Hệ điều hành Linux gồm:
  - Linux kernel.
  - Những ứng dụng và tiện ích GNU.
  - Những ứng dụng khác.

An Ninh Mạng ATHENA, www.athena.com.vn

## Đặc điểm của Linux

- Hardware:
  - Chạy trên nhiều platform, Alpha, AMD, Intel, MIPS, PowerPC, Sparc...
- Software:
  - <http://www.freshmeat.net>
  - <http://www.linuxberg.com>
  - <http://www.rpmfind.net/linux/RPM/>
- Document:
  - <http://www.tldp.org/>

An Ninh Mạng ATHENA, www.athena.com.vn

## Đặc điểm của Linux

- Giao diện đồ họa:
  - Hỗ trợ GNOME, KDE,...
  - Linux không yêu cầu giao diện đồ họa.
- Ngôn ngữ lập trình: C, C++, FORTRAN, Java, Perl, Python, PHP...
- Dễ dàng quản lý từ xa:
  - Dễ dàng remote từ xa bằng commandline hoặc GUI.
- Tính ổn định cao: Linux có thể chạy nhiều năm, không cần reboot.

An Ninh Mạng ATHENA, www.athena.com.vn

## Linux và Windows

- Windows là hệ điều hành được thiết kế cho single users.
- Unix là hệ điều hành được kế cho multi users. Nhiều người cùng chạy một chương trình trên một máy tính vào cùng một thời điểm.
- Từ Windows 95, đã hỗ trợ multi user. Tuy nhiên, Unix đã hỗ trợ multi user từ 1969.

An Ninh Mạng ATHENA, www.athena.com.vn

## Linux và Windows (tt)

- Sự tách biệt giữa GUI và Kernel:
  - GUI là thành phần chiếm nhiều memory nhất, và rất phức tạp, dễ bị lỗi nhất.
  - Với Windows, GUI và kernel là không thể tách rời => tiện lợi cho người dùng.
  - Với Linux, GUI tách biệt với kernel. Người sử dụng có thể sử dụng GUI hay không, hoặc sử dụng những GUI khác nhau => cho phép tùy biến, phù hợp với server, vốn không cần GUI, tiết kiệm được memory, và ít bị lỗi.

An Ninh Mạng ATHENA, www.athena.com.vn

## Linux và Windows (tt)

- Tất cả những cấu hình của Windows được lưu trong registry. Khi muốn chỉnh sửa rất phức tạp. Thường phải có phần mềm third-party.
- Cấu hình của Linux là file text, vì vậy dễ dàng chỉnh sửa theo ý muốn. Có thể xóa bỏ hoàn toàn những cấu hình cũ khi không cần  
=> không có một chuẩn cấu hình. Mỗi dịch vụ định nghĩa một chuẩn cấu hình riêng.

An Ninh Mạng ATHENA, www.athena.com.vn

## Lợi ích & hạn chế của Linux

- Tính ổn định cao và hầu như không có virus.
- Nhiều ý kiến cho rằng ai cũng có thể kiểm soát source code khiến nó không an toàn.
- Tuy nhiên, bí mật không phải là an toàn.
- Code của linux được hàng ngàn programer kiểm tra.
- Nếu có bug, dễ dàng được tìm thấy hơn mã nguồn đóng.

An Ninh Mạng ATHENA, www.athena.com.vn

## Lợi Ích & hạn chế của Linux (tt)

- Khó sử dụng cho người mới bắt đầu.
- Không có hỗ trợ, không có document đầy đủ.
- Bug vẫn tồn tại.
- Khi phát sinh lỗi, không phải ai cũng có khả năng hiểu lỗi.

An Ninh Mạng ATHENA, www.athena.com.vn

## Các phiên bản Linux

- Debian GNU/Linux
  - <http://www.debian.org>
- MandrakeSoft
  - <http://www.linux-mandrake.com>
- Red Hat
  - <http://www.redhat.com>
- Slackware Linux
  - <http://www.slackware.com>
- SuSE
  - <http://www.suse.com>
- TurboLinux
  - <http://www.turboLinux.com>

An Ninh Mạng ATHENA, www.athena.com.vn

## Hỏi & Đáp



An Ninh Mạng ATHENA, www.athena.com.vn



## Installing Linux in a Server Configuration

## Nội dung

- Tóm tắt các bước cài đặt.
- Kiểm tra sự hỗ trợ phần cứng.
- Cấu hình mạng.
- Linux file system.
- Linux boot loader.
- Các mode hoạt động của Linux.

An Ninh Mạng ATHENA, www.athena.com.vn

## Các bước cài đặt

- Chọn lựa kiểu cài đặt:
  - Từ CD local.
  - Qua môi trường mạng.
  - Từ một volume trên network server.
  - Dùng CD shared từ máy tính khác
  - Qua FTP, HTTP.

An Ninh Mạng ATHENA, www.athena.com.vn

## Các bước cài đặt (tt)

- Kiểm tra sự hỗ trợ phần cứng.
- Phân chia partition:
  - Phân chia tự động hoặc theo định dạng riêng.
  - Bắt buộc phải có phân vùng / và /swap.
  - Chia các phân vùng còn lại theo nhu cầu.
- Cấu hình mạng.
- Chọn lựa software để cài đặt.
- Chọn lựa boot loader.
- Tiến hành cài đặt.

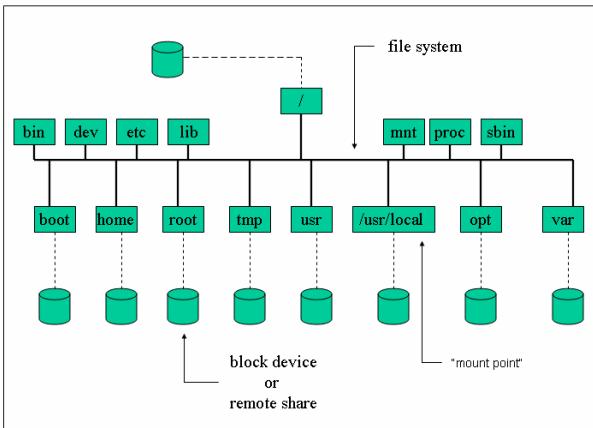
An Ninh Mạng ATHENA, www.athena.com.vn

## Hỗ trợ phần cứng

- Kiểm tra sự hỗ trợ phần cứng.
  - <http://hardware.redhat.com/hcl>.
- Hầu hết các distribution của Linux tự nhận diện cấu hình phần cứng như: PCMCIA, CD-ROM, Hard drive, Laptop issues, Memory, NIC, Modem, Mouse, SCSI adaptor...
- Cần chú ý đến những thiết bị phần cứng đặc biệt, mới.

An Ninh Mạng ATHENA, www.athena.com.vn

## Linux file system



An Ninh Mạng ATHENA, www.athena.com.vn

## Linux file systems (tt)

- Mặc định, các phân vùng được mount trên phân vùng /
- /swap: virtual memory.
- /bin: lệnh quan trọng.
- /boot: file cấu hình boot loader.
- /dev: file devices.
- /etc: file cấu hình.
- /home: dữ liệu của users.
- /lib: file thư viện quan trọng, và kernel module.

An Ninh Mạng ATHENA, www.athena.com.vn

## Cấu hình mạng

- Thiết lập các thông số cấu hình mạng cho server:
  - IP Address
  - Netmask
  - Gateway IP Address
  - Nameserver IP Address
  - Domain name
  - Hostname

An Ninh Mạng ATHENA, www.athena.com.vn

## Linux boot loader

- Boot loader
  - LILO
  - GRUB
- Boot loader cho phép chọn hệ điều hành nào để boot.
- Tại boot loader, có thể can thiệp bằng command để thay đổi các tham số boot.

An Ninh Mạng ATHENA, www.athena.com.vn

## Linux boot loader (tt)

```
○ File grub.conf
boot=/dev/sda
default=0
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title Linux Fedora (2.6.5-1.358smp)
    root (hd0,0)
    kernel /vmlinuz-2.6.5-1.358smp ro root=LABEL=/ rhgb quiet
    initrd /initrd-2.6.5-1.358smp.img
title Windows 2000
    rootnoverify (hd0,0)
    chainloader +1
```

An Ninh Mạng ATHENA, www.athena.com.vn

## Mode hoạt động của Linux

- Linux có các mode hoạt động sau:
  - 0: shutdown.
  - 1: single mode.
  - 2: multi user without networking.
  - 3: multi user with networking.
  - 4: unused.
  - 5: graphic.
  - 6: reboot.

An Ninh Mạng ATHENA, www.athena.com.vn

## Hỏi & Đáp



An Ninh Mạng ATHENA, www.athena.com.vn



## Installing software

## Nội dung

- Add/ Remove Program.
- Redhat Package Manager (RPM).
- Cài đặt bằng lệnh rpm.
- Cài đặt bằng source.
- Giới thiệu một số ứng dụng.

An Ninh Mạng ATHENA, www.athena.com.vn

## Add/ Remove Program

- Cài đặt bằng công cụ graphic add/ remove program của Linux giải quyết được các vấn đề sau:
  - thao tác đơn giản, dễ thực hiện.
  - tự động cài các gói phụ thuộc.
  - dễ quản lý.

An Ninh Mạng ATHENA, www.athena.com.vn

## Redhat Package Manager

- Được phát triển đầu tiên bởi Redhat, sau đó được các phiên bản linux khác sử dụng rộng rãi: Fedora, Mandrake, SuSe
- Gói rpm có dạng:



- Cài đặt bằng lệnh rpm.
- Đây là kiểu cài đặt phổ biến nhất của linux.
- Dễ cài đặt, dễ remove.

An Ninh Mạng ATHENA, www.athena.com.vn

## Lệnh rpm

- Cài đặt một package:
  - rpm -i package.rpm
- Update một package:
  - rpm -U package.rpm
- Gỡ bỏ một package:
  - rpm -e package.rpm
- Một số option khác sử dụng trong cài đặt:
  - --nodeps: cho phép cài đặt, bỏ qua các gói phụ thuộc.
  - --force: bắt buộc upgrade, bỏ qua conflicts.
  - --test: không cài đặt, upgrade, chỉ test.
  - --requires: liệt kê các gói phụ thuộc.

An Ninh Mạng ATHENA, www.athena.com.vn

## Lệnh rpm (tt)

- ◎ Các option truy vấn: kết hợp với option -q
  - -a: hiển thị danh sách các package đã cài đặt.
  - -f <file\_name>: hiển thị package sở hữu <file\_name>.
  - -p <package\_name>: hiển thị thông tin của package\_name. (package\_name chưa được cài đặt).
  - -i <package\_name>: hiển thị thông tin của package.
  - -l <package\_name>: hiển thị file chứa trong package\_name.

An Ninh Mạng ATHENA, www.athena.com.vn

## Lệnh rpm (tt)

```
[root@centos-1 ~]# rpm -qi openssh-server-4.3p2-16.el5
Name        : openssh-server                         Relocations: (not relocatable)
Version     : 4.3p2                                     Vendor: CentOS
Release    : 16.el5                                    Build Date: Thu 22 Mar 2007 03:49:25 AM ICT
Install Date: Sat 19 Jan 2008 10:48:27 PM ICT       Build Host: builder4.centos.org
Group      : System Environment/Daemons           Source RPM: openssh-4.3p2-16.el5.src.rpm
Size       : 457225                                    License: BSD
Signature   : DSA/SHA1, Wed 04 Apr 2007 07:26:48 AM ICT, Key ID a8a447dce8562897
URL        : http://www.openssh.com/portable.html
Summary    : The OpenSSH server daemon
Description :
OpenSSH is a free version of SSH (Secure SHell), a program for logging
into and executing commands on a remote machine. This package contains
the secure shell daemon (sshd). The sshd daemon allows SSH clients to
securely connect to your SSH server. You also need to have the openssh
package installed.
```

An Ninh Mạng ATHENA, www.athena.com.vn

## Lệnh rpm (tt)

```
[root@centos-1 ~]# rpm -ql openssh-server-4.3p2-16.el5 | more
/etc/pam.d/sshd
/etc/rc.d/init.d/sshd
/etc/ssh
/etc/ssh/sshd_config
/usr/libexec/openssh/sftp-server
/usr/sbin/sshd
/usr/share/man/man5/sshd_config.5.gz
/usr/share/man/man8/sftp-server.8.gz
/usr/share/man/man8/sshd.8.gz
/var/empty/sshd
/var/empty/sshd/etc
[root@centos-1 ~]# rpm -qf /etc/pam.d/sshd
openssh-server-4.3p2-16.el5
```

An Ninh Mạng ATHENA, www.athena.com.vn

## Cài đặt bằng source

- ◎ Tương thích với mọi phiên bản Linux.
- ◎ Được đóng gói sử dụng kiểu GNU Zip (.gz) hoặc BZip2 (bz2).
  - <filename>.tar.gz or <filename>.tar.bz2
- ◎ Giải nén bằng lệnh:
  - tar xvzf <filename>.tar.gz
  - tar xvjf <filename>.tar.bz2
- ◎ Đọc file INSTALL hoặc README để có những chỉ dẫn riêng biệt của gói cài đặt.

An Ninh Mạng ATHENA, www.athena.com.vn

## Cài đặt bằng source (tt)

- Sau khi giải nén, chuyển đến thư mục của gói source:
  - cd <extracted\_dir\_name>
- Chạy script configure, cần đọc file README, INSTALL để có những option cần thiết:
  - ./configure
- Build gói source bằng lệnh make:
  - make
- Cài đặt gói source:
  - make install

An Ninh Mạng ATHENA, www.athena.com.vn

## Cài đặt bằng source (tt)

- Khi có thay đổi trong source, cần biên dịch, cài đặt lại.
- Sau khi cài đặt xong, để gỡ bỏ gói source, dùng những lệnh sau:
  - make clean
  - make distclean
- Nếu cần thiết xóa bỏ luôn thư mục source cài đặt:
  - rm -rf <extracted\_dir\_name>

An Ninh Mạng ATHENA, www.athena.com.vn

## Một số ứng dụng

- Một số ứng dụng cơ bản cần cho thao tác văn phòng trên linux:
  - open office
  - unikey
  - acrobat reader
  - chm reader

An Ninh Mạng ATHENA, www.athena.com.vn

## Hỏi & Đáp



An Ninh Mạng ATHENA, www.athena.com.vn

## Managing Users

### Nội dung

- Những thông tin định nghĩa users
- Công cụ quản lý users.
- Users và cấp quyền users.
- Định nghĩa cấu hình mặc định cho người dùng.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

### Định nghĩa Users

- Users được định nghĩa trong một hệ thống để xác định “ai? được quyền dùng cái gì?” trong hệ thống đó.
- Với Linux, mỗi user có một định danh duy nhất, gọi là UID (User ID).
  - 0 – 99: user có quyền quản trị.
  - > 99: user khác.  $\geq 500$ : không phải user hệ thống.
  - => **UID có khả năng sử dụng lại???**
- Mỗi user thuộc ít nhất một group. Mỗi group cũng có một định danh duy nhất là GID.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

### Định nghĩa Users (tt)

- Mỗi users cần có những thông tin: tên user, UID, tên group, GID, home directory...
- Windows quản lý thông tin bằng LDAP, Kerberos. Linux quản lý thông tin bằng file text.
- Có thể chỉnh sửa thông tin của users bằng công cụ, hoặc sửa trực tiếp bằng text file.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Định nghĩa Users (tt)

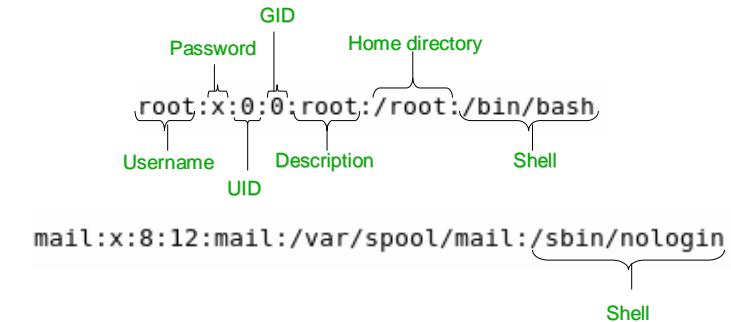
### ◎ Những file định nghĩa thông tin users:

- /etc/passwd: chứa thông tin user login, password mã hóa, UID, GID, home directory, và login shell. Mỗi dòng là thông tin của một user.
- /etc/shadow: chứa thông tin password mã hóa, thời gian sử dụng password, thời gian phải thay đổi password...
- /etc/group: chứa thông tin group.

An Ninh Mạng ATHENA, www.athena.com.vn

## Định nghĩa Users (tt)

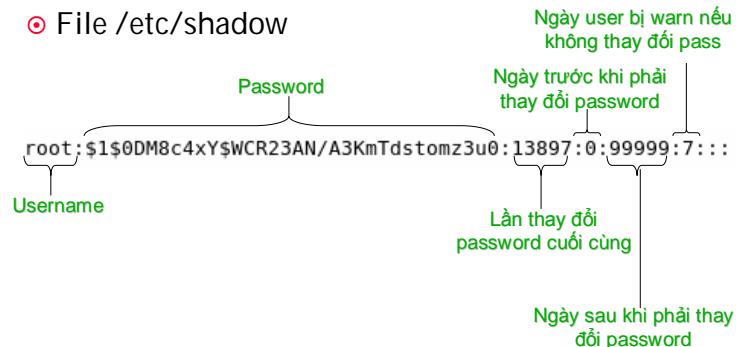
### ◎ File /etc/passwd



An Ninh Mạng ATHENA, www.athena.com.vn

## Định nghĩa Users (tt)

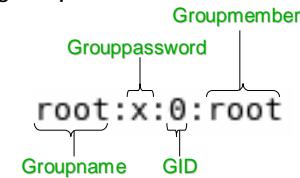
### ◎ File /etc/shadow



An Ninh Mạng ATHENA, www.athena.com.vn

## Định nghĩa Users (tt)

### ◎ File /etc/group



An Ninh Mạng ATHENA, www.athena.com.vn

## Công cụ quản lý Users

- Quản lý bằng command line
  - useradd: tạo user.
  - usermod: chỉnh sửa thông tin user.
  - userdel: xóa user.
  - groupadd: tạo group.
  - groupdel: xóa group.
  - groupmod: chỉnh sửa thông tin group.
- Quản lý bằng giao diện đồ họa

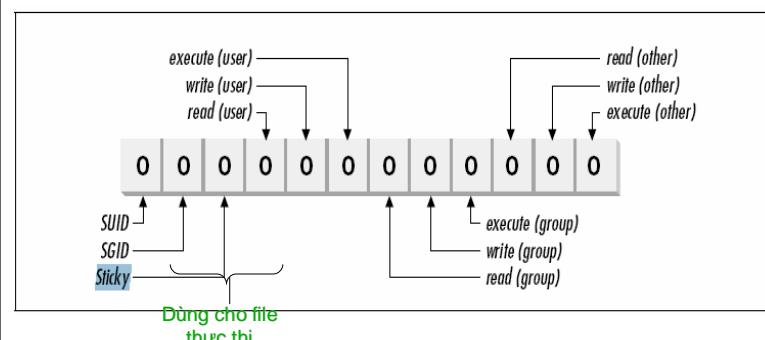
An Ninh Mạng ATHENA, www.athena.com.vn

## Cấp quyền Users

- Quyền trong linux được phân chia như sau:
  - Quyền đọc: r (read).
  - Quyền ghi: w (write).
  - Quyền thực thi: x (execute).
- Mỗi file trong linux được gán quyền theo ba lớp user sau:
  - owner
  - group
  - everyone (other)

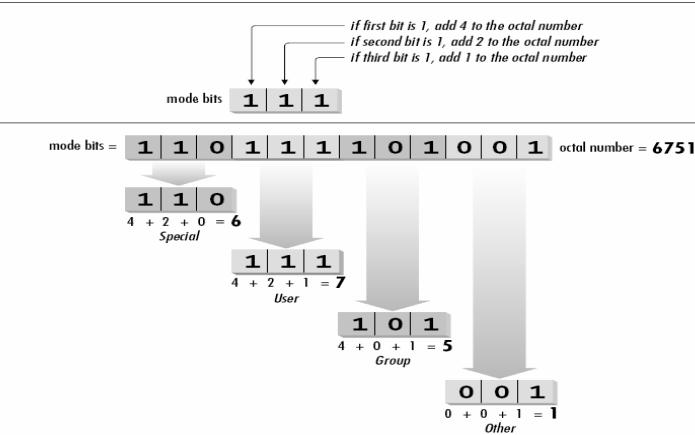
An Ninh Mạng ATHENA, www.athena.com.vn

## Cấp quyền users (tt)



An Ninh Mạng ATHENA, www.athena.com.vn

## Cấp quyền users (tt)



An Ninh Mạng ATHENA, www.athena.com.vn

## Cấp quyền users (tt)

- ◎ SetUID: program nào được set SUID, khi thực thi sẽ được sở hữu bởi owner của program đó, bất kể user nào gọi thực thi program này.
- ◎ SetGID: hiện thực như SUID, nhưng áp dụng cho file group owner.
- ◎ Sticky bit: chỉ cho phép owner, hoặc root được quyền delete file.

An Ninh Mạng ATHENA, www.athena.com.vn

## Cấu hình mặc định

- ◎ Khi dùng lệnh useradd không có option kèm theo để tạo user, các thuộc tính của user sẽ được tạo theo các cấu hình mặc định.
- ◎ Những file định nghĩa cấu hình mặc định:
  - /etc/default/useradd
  - /etc/skel
  - /etc/login.defs
- ◎ Nếu muốn thay đổi cấu hình mặc định, thay đổi trực tiếp trong những file này.

An Ninh Mạng ATHENA, www.athena.com.vn

## Cấu hình mặc định (tt)

- ◎ /etc/default/useradd: những giá trị mặc định cho việc tạo account.
- ◎ /etc/skel: thư mục chứa nội dung mặc định sẽ tạo trong home directory của users.
- ◎ /etc/login.defs: những cấu hình mặc định cho shadow password.

An Ninh Mạng ATHENA, www.athena.com.vn

## Hỏi & Đáp



An Ninh Mạng ATHENA, www.athena.com.vn

## The Command Line

## The Command Line

- Giới thiệu dòng lệnh
- Cú pháp dòng lệnh
- Một số lệnh thông dụng
- Chuyển hướng dòng lệnh
  - redirection
  - pipe
- Background jobs

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Giới thiệu dòng lệnh

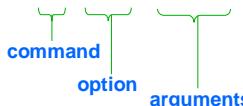
- Dòng lệnh là thế mạnh của hệ điều hành Unix và Linux.
- Với hệ điều hành Unix và Linux, các thao tác đồ họa không thể đáp ứng đủ công việc cần thiết. Dòng lệnh là công cụ hữu hiệu nhất.
- Dòng lệnh trong Unix và Linux là “case sensitive”.
- Để biết cách sử dụng dòng lệnh, gọi lệnh man.
  - Vd: *man ls*

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Cú pháp dòng lệnh

- Cú pháp của một dòng lệnh gồm có ba thành phần:

*<command> [option] [arguments]*

  - command: hệ thống sẽ làm gì?
  - option: hệ thống sẽ làm gì?
  - arguments: hệ thống sẽ thực thi lệnh ở đâu?
- *ls -al /root*: *liệt kê nội dung của thư mục root (bao gồm cả file ẩn)*.  


An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

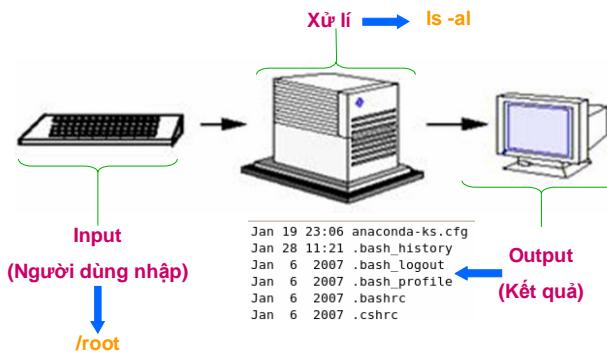
## Lệnh thông dụng

- Lệnh su và sudo.
- Lệnh gán biến môi trường.
- Lệnh tạo, xóa, sửa, copy file , thư mục.
  - mkdir, cp, mv, rmdir, ln
  - cat, vi, rm
- Lệnh cấp quyền trên file, thư mục.
  - chown, chgrp, chmod
- Lệnh tìm kiếm
  - find, locate
- Lệnh xem kích thước thư mục, phân vùng.
  - df, du
- Lệnh quản lý tiến trình, tình trạng hệ thống.
  - ps, top, kill

An Ninh Mạng ATHENA, www.athena.com.vn

## Chuyển hướng dòng lệnh

- Phân tích lệnh `ls -al /root`



An Ninh Mạng ATHENA, www.athena.com.vn

## Chuyển hướng dòng lệnh

- Redirection: có hai loại redirection:
  - redirect input
    - `command < filename`
    - Tạo file /tmp/in.txt có nội dung /root
    - Sử dụng lệnh: `ls -al /tmp/in.txt`
  - redirect output
    - `command > output`
    - `command >> output`
    - Sử dụng lệnh: `ls -al /root > /tmp/out.txt`

An Ninh Mạng ATHENA, www.athena.com.vn

## Chuyển hướng dòng lệnh (tt)

- Pipe: là khái niệm đưa output của lệnh này thành input của lệnh kia.
  - `command1 | command2`
  - `ls -al /root | more`

An Ninh Mạng ATHENA, www.athena.com.vn

## Background jobs

- ◎ Thông thường, lệnh chạy ở mode foreground, đưa kết quả output ra màn hình (có thể chuyên hướng đưa kết quả output vào file).
- ◎ Nếu một lệnh chạy 1h ở mode foreground, thì lệnh sẽ chiếm luôn BASH shell đó => người dùng phải mở một shell khác để làm việc.
- ◎ Có thể start lệnh chạy mode background, nếu cần thiết thì đưa kết quả output vào file và người dùng vẫn có thể làm việc với BASH shell đó bình thường.

An Ninh Mạng ATHENA, www.athena.com.vn

## Background jobs (tt)

- ◎ Lệnh chạy ở background gọi là **JOB**.
- ◎ Start lệnh ở background:
  - command &
- ◎ Một số lệnh kiểm soát **jobs**.

Command	Value
jobs	Display which jobs are currently running.
fg %n	Place a job in the foreground.
bg %n	Place a job in the background.
kill %n	Abort the specified background job. The job ID must be specified.
Ctrl-c	Abort the foreground job.
Ctrl-z	Suspend the foreground job.

An Ninh Mạng ATHENA, www.athena.com.vn

## Hỏi & Đáp



An Ninh Mạng ATHENA, www.athena.com.vn



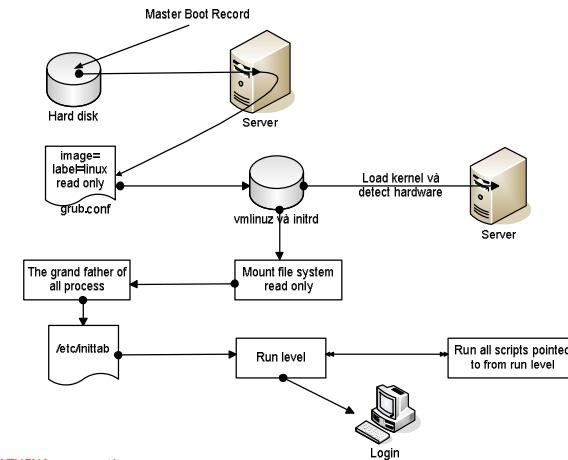
**Booting and  
shutting down**

## Nội dung (tt)

- Quá trình boot Linux
- Boot loader (boot manager)
  - Boot loader GRUB
  - Boot loader LILO
- Kernel image và initrd
- Tiến trình init và file inittab
- Tiến trình rc.sysinit
- /etc/rc.d/rc script
- Quá trình shutdown Linux

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Quá trình boot linux



An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Quá trình boot Linux

- BIOS/ POST
- MBR (lilo hoặc grub): cho phép lựa chọn hệ điều hành boot.
- Kernel + initrd: load kernel và detect hardware.
- Mount root file system (read only)
- /sbin/init: tiến trình cha của mọi tiến trình.
- /etc/inittab: quyết định run level và gọi start các dịch vụ cần thiết của run level đó.
- Hiển thị đồ họa nếu ở runlevel 5.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Boot loader

- Boot loader hay còn gọi là boot manager cho phép quản lý nhiều hệ điều hành, chọn boot vào hệ điều hành nào.
- Hai boot loader phổ biến của Linux:
  - LILO (Linux LOader)
  - GRUB (GRand Unified Boot loader)
- Khi thay đổi file cấu hình, GRUB tự động nhận biết, LILO thì phải dùng lệnh /sbin/lilo để update cấu hình.
- Ngày nay, GRUB là boot loader mặc định của đại đa số các hệ điều hành Linux.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Boot loader GRUB

- File cấu hình grub.conf:

```
default=0  
timeout=10  
splashimage=(hd0,0)/grub/splash.xpm.gz  
hiddenmenu  
title Linux Fedora (2.6.5-1.358smp)  
root (hd0,0) → Đĩa đầu tiên, partition đầu tiên  
kernel /vmlinuz-2.6.5-1.358smp ro root=LABEL=/ rhgb quiet  
initrd /initrd-2.6.5-1.358smp.img  
title Windows server 20003  
rootnoverify (hd0,1)  
chainloader +1
```

An Ninh Mạng ATHENA, www.athena.com.vn

## Boot loader GRUB (tt)

- Cách phân biệt partition trong boot loader GRUB khác với cách thông thường của Linux.
- GRUB không phân biệt IDE, và SCSI. đĩa cứng được hiểu là: hd%d.
- %d: là số nguyên, bắt đầu từ zero để chỉ partition đầu tiên.
- LILO có cách hiểu thông thường như Linux: hdXY, sdXY.

An Ninh Mạng ATHENA, www.athena.com.vn

## Boot loader GRUB (tt)

- Một số lệnh của grub: sử dụng trong mode grub, hoặc trong file grub.conf

GRUB Command	Description
kernel	Points to the kernel file used to boot the system and any options to pass to the loaded kernel.
root	Mounts the specified device and partition as GRUB's root partition.
default	Sets the default boot entry, which is used if the time-out time is reached. The number refers to a title command, with 0 pointing to the first title in the configuration file, 1 pointing to the second title command, and so on.
fallback	Defines the title entry to use if the initial boot attempt fails.
hiddenmenu	Hides the GRUB menu. If the user does not unhide the menu by pressing the ESC key at startup, the time-out time will elapse and the default entry will be loaded.
password	Requires that the user know the password (which is MD5-encrypted in this file) to edit the boot loader configuration.
timeout	Sets the time limit after which GRUB will automatically load the default entry.
splashimage	Points to the image presented when GRUB starts.
title	Provides a name for a group of configuration commands. This name is displayed on GRUB's boot menu.
initrd	Points to the initial RAM disk used during booting.

An Ninh Mạng ATHENA, www.athena.com.vn

## Boot loader LILO

- File cấu hình lilo.conf:

```
boot=/dev/hda  
prompt  
timeout=10  
image=/boot/vmlinuz-2.6.5-1.358smp  
label=Linux Fedora (2.6.5-1.358smp)  
root=/dev/hda1 → Đĩa IDE đầu tiên, partition đầu tiên  
read-only  
other = /dev/hda2  
label=Windows server 2003  
table=/dev/hda
```

An Ninh Mạng ATHENA, www.athena.com.vn

## Boot loader LILO (tt)

- Để cài đặt LILO làm boot loader, dùng lệnh:
  - /sbin/lilo – yêu cầu phải có file lilo.conf
- Gỡ bỏ boot loader LILO, dùng lệnh:
  - /sbin/lilo –u
- Tìm hiểu lệnh lilo:
  - man lilo
- Tìm hiểu file cấu hình boot loader lilo:
  - man lilo.conf

An Ninh Mạng ATHENA, www.athena.com.vn

## Kernel image và initrd

- Kernel image là hình ảnh nhỏ nhất của kernel được nén thành file vmlinuz-version.tar.gz.
- Kernel image chứa những thành phần quan trọng cần thiết đầu tiên để boot máy tính.
- initrd – initial ram disk: được sử dụng để detect phần cứng và load driver.
- Đồng thời mount file systems dưới dạng read only để tiến hành kiểm tra.

An Ninh Mạng ATHENA, www.athena.com.vn

## Tiến trình init và file inittab

- Tiến trình init là cha của mọi tiến trình.
- Tiến trình init sẽ tìm đọc file /etc/inittab để quyết định runlevel nào sẽ được boot.
- Mỗi dòng trong /etc/inittab có dạng như sau:

– id: runlevels:action:process

  
id:5:initdefault: Nếu không định nghĩa, sẽ boot vào runlevel nào???  
si::sysinit:/etc/rc.d/rc.sysinit  
l5:5:wait:/etc/rc.d/rc 5

An Ninh Mạng ATHENA, www.athena.com.vn

## Tiến trình init ...(tt)

Values for action Field in /etc/inittab File	Description
respawn	The process will be restarted whenever it terminates.
<b>wait</b>	The process will be started once when the runlevel is entered, and init will wait for its completion.
once	The process will be started once when the runlevel is entered; however, init won't wait for termination of the process before possibly executing additional programs to be run at that particular runlevel.
boot	The process will be executed at system boot. The runlevels field is ignored in this case.
bootwait	The process will be executed at system boot, and init will wait for completion of the boot before advancing to the next process to be run.
ondemand	The process will be executed when a specific runlevel request occurs. (These runlevels are a, b, and c.) No change in runlevel occurs.
<b>initdefault</b>	Specifies the default runlevel for init on startup. If no default is specified, the user is prompted for a runlevel on console.
<b>sysinit</b>	The process will be executed during system boot, before any of the boot or bootwait entries.
powerwait	If init receives a signal from another process that there are problems with the power, this process will be run. Before continuing, init will wait for this process to finish.
powerfail	Same as powerwait, except that init will not wait for the process to finish.

An Ninh Mạng ATHENA, www.athena.com.vn

## Tiến trình rc.sysinit

- Tiến trình rc.sysinit thực thi những nhiệm vụ sau:
  - thiết lập hostname của máy tính và detect môi trường network.
  - Mount /proc file system.
  - Thiết lập các tham số của kernel.
  - Thiết lập giờ hệ thống, fonts.
  - Khởi tạo phân vùng swap.
  - Check file system và mount lại ở mode read-write.
  - Load những module cần thiết.

An Ninh Mạng ATHENA, www.athena.com.vn

## /etc/rc.d/rc script

- Thực thi tất cả script liên quan đến run level đó.
- Vd: nếu runlevel là 5, sẽ gọi thực thi các script trong /etc/rc.d/rc5.d
- Các script này là file symbolic link, link đến các script thật sự, thường chứa trong /etc/init.d

```
S80sendmail -> ../init.d/sendmail  
└── start  
K15httpd -> ../init.d/httpd  
└── stop
```

An Ninh Mạng ATHENA, www.athena.com.vn

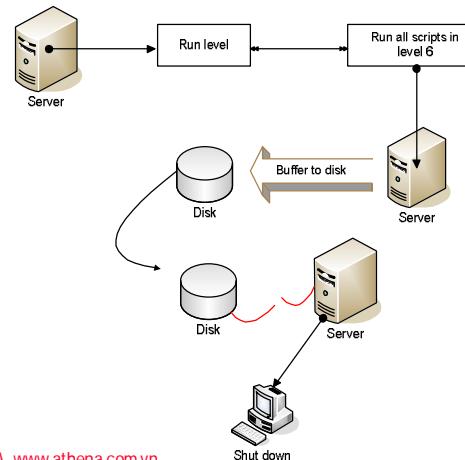
## /etc/rc.d/rc script (tt)

K02avahi-dnsconfd	K74ncsd	S10restorecond	S44acpid
K02dhcdbd	K74ntpd	S11audited	S500plip
K02NetworkManager	K85mdmpd	S12syslog	S55cups
K02NetworkManagerDispatcher	K88wpa_supplicant	S13irqbalance	S55sshd
K02oddjobd	K89dund	S13mcstrans	S80sendmail
K05commanc	K89netplugd	S13portmap	S85gpm
K05aslaudhd	K89pand	S14nfsllock	S90crond
K10psacct	K89rdisc	S15mdmonitor	S90xfs
K15httpd	K91capl	S18pcidmapd	S95anacron
K20nfs	S00microcode_ctl	S19rpcssd	S95atd
K241rda	S04readahead_early	S22messagebus	S96readahead_later
K30spamassassin	S05kudzu	S25bluetooth	S97yum-updatesd
K35vncserver	S06cpuspeed	S25nets	S98avahi-daemon
K35winbind	S08ip6tables	S25pcscd	S98haldaemon
K50lmasm	S08iptables	S26apmd	S99firstboot
K69rpvcsvcssd	S09isdn	S26hidd	S99local
K73ypbind	S10network	S28autofs	S99smartd

- Những script có bắt đầu bằng S, hệ thống sẽ gọi chạy lệnh: /etc/rc.d/init.d<command> start.
- Những script bắt đầu bằng K, hệ thống sẽ gọi chạy lệnh: /etc/rc.d/init.d<command> stop.

An Ninh Mạng ATHENA, www.athena.com.vn

## Quá trình shut down linux



An Ninh Mạng ATHENA, www.athena.com.vn

## Hỏi & Đáp



An Ninh Mạng ATHENA, www.athena.com.vn



## File systems

## Nội dung

- Disk và partition.
- Khái niệm File Systems.
- Quản lý File Systems.
  - mount và umount.
  - Lệnh fsck.
- Logical Volume Management.

An Ninh Mạng ATHENA, www.athena.com.vn

## Disk và partition

- Mọi đĩa cứng (disk) đều cần được phân chia partition.
- Mỗi partition được xem như một phân vùng độc lập. Khi dữ liệu đầy, partition này không thể "overflow" (lấn chiếm) kích thước của partition khác.
- Có thể cài các hệ điều hành khác nhau lên các partition khác nhau.
- Sau đó, dùng một trình quản lý boot loader để quản lý quá trình boot.

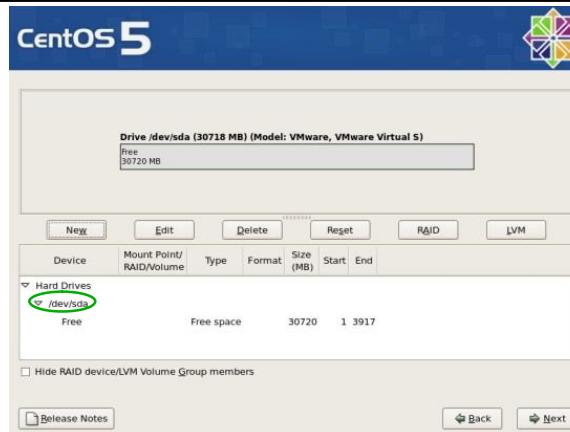
An Ninh Mạng ATHENA, www.athena.com.vn

## Disk và partition (tt)

- Những ổ đĩa IDE sẽ có tên là hdX.
  - X có giá trị từ [a-z] đại diện cho một ổ đĩa vật lý. *Vd: hda, hdb...*
- Khi được chia partition, partition sẽ có dạng: hdXY
  - X là kí tự ổ đĩa.
  - Y là số thứ tự.
  - *Vd: hda1, hda2, hdb1, hdb2...*
- CDROM cũng được hiểu như một ổ đĩa IDE.
- Ổ đĩa SCSI sẽ có tên là sdX

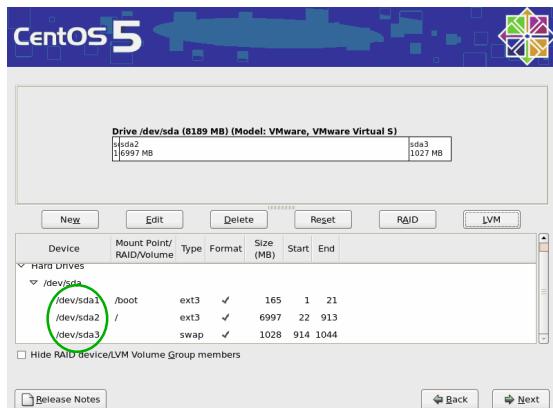
An Ninh Mạng ATHENA, www.athena.com.vn

## Disk và partition (tt)



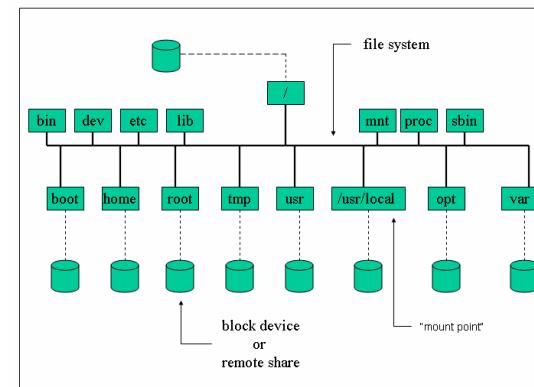
An Ninh Mạng ATHENA, www.athena.com.vn

## Disk và partition (tt)



An Ninh Mạng ATHENA, www.athena.com.vn

## Khái niệm File systems



An Ninh Mạng ATHENA, www.athena.com.vn

## Khái niệm File Systems (tt)

- ◎ Mặc định, các phân vùng được mount trên phân vùng /
- ◎ /swap: virtual memory.
- ◎ /bin: lệnh quan trọng.
- ◎ /boot: file cấu hình boot loader.
- ◎ /dev: file devices.
- ◎ /etc: file cấu hình.
- ◎ /home: dữ liệu của users.
- ◎ /lib: file thư viện quan trọng, và kernel module.

An Ninh Mạng ATHENA, www.athena.com.vn

## Quản lý File Systems

- ◎ Partition, ổ đĩa CD-ROM, floppy, usb... cần được mount, nhờ thẻ nội dung của nó mới có thể đọc được.
- ◎ Mount là biến một partition, một thiết bị (CD-ROM, USB...) thành một thư mục trên cây thư mục. Thư mục này được gọi là **mount-point**.
- ◎ Xem nội dung của partition vừa được mount bằng xem nội dung của thư mục mount-point.

An Ninh Mạng ATHENA, www.athena.com.vn

## Quản lý File Systems (tt)

- ◎ Tạo một thư mục /mnt/cdrom. Thư mục này dùng làm mount-point cho ổ đĩa CD-ROM

```
[root@testsrv ~]# mount /dev/cdrom /mnt/cdrom
mount: block device /dev/cdrom is write-protected, mounting read-only

[root@testsrv ~]# ls -l /mnt/cdrom
total 1105
dr-xr-xr-x 1 root root 51200 Apr 11 2007 CentOS
-r-xr-xr-x 1 root root 212 Mar 30 2007 EULA
-r-xr-xr-x 1 root root 18009 Mar 10 2007 GPL
-r-xr-xr-x 1 root root 4222 Sep 12 00:20 huongdan-guide.txt
dr-xr-xr-x 1 root root 2048 Apr 11 2007 images
dr-xr-xr-x 1 root root 2048 Apr 11 2007 isolinux
dr-xr-xr-x 1 root root 2048 Apr 11 2007 NOTES
```

An Ninh Mạng ATHENA, www.athena.com.vn

## Quản lý File Systems (tt)

- ◎ Nếu thư mục mount point đã có dữ liệu trước.

```
[root@centos-1 ~]# ls -al /mnt/cdrom/
total 20
drwxr-xr-x 3 root root 4096 Jan 26 21:28 .
drwxr-xr-x 3 root root 4096 Jan 26 21:28 ..
drwxr-xr-x 2 root root 4096 Jan 26 21:28 test
-rw-r--r-- 1 root root 63 Jan 26 21:28 testfile
```

- ◎ Mount một partition vào thư mục mount point.
- ◎ Xem nội dung của thư mục mount point.
  - Có những file trước đó không???
- ◎ Umount CD-ROM ra khỏi mount point
  - Những file trước đó có bị mất không???

An Ninh Mạng ATHENA, www.athena.com.vn

## Quản lý File Systems (tt)

- Mỗi partition đều phải được mount để sử dụng  
=> những partition hệ thống được mount lúc nào => `/etc/fstab`

```
LABEL=/          /          ext3 defaults    1 1
devpts          /dev/pts   devpts gid=5,mode=620 0 0
tmpfs           /dev/shm   tmpfs  defaults    0 0
proc             /proc      proc   defaults    0 0
sysfs           /sys       sysfs  defaults    0 0
LABEL=SWAP-sda2 swap       swap   defaults    0 0
```

An Ninh Mạng ATHENA, www.athena.com.vn

## Quản lý File Systems (tt)

- Lệnh fdisk: xem, tạo, xóa partition.

```
[root@testsrv ~]# fdisk -l
Disk /dev/sda: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

Device Boot Start End Blocks Id System
/dev/sda1 *      1  21 168651  83 Linux
/dev/sda2          22  913 7164990  83 Linux
/dev/sda3          914 1044 1052257+ 82 Linux swap / Solaris
```

- Lệnh fsck: chẩn đoán và sửa lỗi file systems.

```
[root@testsrv ~]# fsck -a /dev/sda4
fsck 1.39 (29-May-2006)
/dev/sda4 is mounted.
```

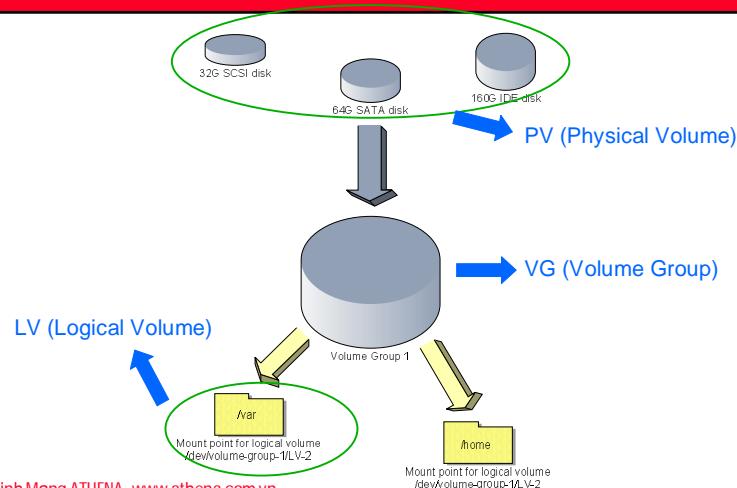
WARNING!!! Running e2fsck on a mounted filesystem may cause SEVERE filesystem damage.

Do you really want to continue (y/n)? yes

```
/dev/sda4: clean, 11/128520 files, 26763/514080 blocks
```

An Ninh Mạng ATHENA, www.athena.com.vn

## Logical Volume Management



An Ninh Mạng ATHENA, www.athena.com.vn

## Logical Volume Management (tt)

- Linh hoạt trong việc phân chia partition.
- Dễ dàng mở rộng kích thước của volume.
- Để mở rộng dung lượng lưu trữ dữ liệu, đơn giản chỉ cần thêm đĩa mới vào.

An Ninh Mạng ATHENA, www.athena.com.vn

## Logical Volume Management (tt)

- ◎ **pvcreate**: khởi tạo những physical volume để sử dụng trong môi trường LVM. Physical volume có thể là đĩa cứng, thiết bị lưu trữ khác, hoặc partition...
- ◎ **pvdisplay**: hiển thị thông tin của physical volume.
- ◎ **vgcreate**: khởi tạo một volume group từ những physical devices đã được khởi tạo bằng pvcreate.
- ◎ **vgextend**: thêm physical volume vào volume group.
- ◎ **vgdisplay**: xem thông tin của volume group
- ◎ **lvcreate**: tạo logical volume từ volume group.
- ◎ **lvdisplay**: xem thông tin của logical volume.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Hỏi & Đáp



An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Core System Services



## Nội dung

- ◎ Service syslogd
- ◎ Service crond
- ◎ Service xinetd

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Service syslogd

- Người quản trị có nhu cầu thường xuyên theo dõi các sự kiện xảy ra trong hệ thống.
- Khi có sự cố, người quản trị có nhu cầu tìm lại các sự kiện xảy ra trước thời điểm đó trong hệ thống.
- Một hệ thống luôn có nhu cầu cần lưu log.
- Có thể lưu log cục bộ, hoặc lưu log tập trung.

An Ninh Mạng ATHENA, www.athena.com.vn

## Service syslogd (tt)

- Log trong hệ thống được syslog phân loại như sau:
  - facility: cho biết ứng dụng nào phát sinh ra log.
    - syslog định nghĩa các facility có sẵn: authpriv, cron, daemon, kern, lpr, mail, mark, news, syslog, user, uucp .
    - syslog dành facility từ local0 -> local7 cho người dùng định nghĩa.
  - level: mức độ nghiêm trọng của log.
    - debug < info < notice < warn < err < crit, alert < emerg
  - action: log sẽ được xử lý như thế nào? Lưu hay không, lưu ở đâu?

An Ninh Mạng ATHENA, www.athena.com.vn

## Service syslogd (tt)

- File cấu hình của syslog:
  - /etc/syslog.conf:
    - file cấu hình chính của service syslogd.
    - Kiểm soát việc record log nào được ghi, và ghi vào đâu?
  - /etc/sysconfig/syslog:
    - định nghĩa mode hoạt động của service syslogd.
    - Lưu log cục bộ, hay lưu log vào remote server?

An Ninh Mạng ATHENA, www.athena.com.vn

## Service syslogd (tt)

```
# Don't log private authentication messages!
*.info:mail.none:authpriv.none:cron.none                                /var/log/messages
# The authpriv file has restricted access.
authpriv.">*
```

/var/log/secure

```
# Log all the mail messages in one place.
mail.*                                                               /var/log/maillog
```

/var/log/cron

```
# Log cron stuff
cron.*
```

\*

```
# Everybody gets emergency messages
*.emerg
```

/var/log/spooler

```
# Save news errors of level crit and higher in a special file.
uucp.news:crit
```

/var/log/spooler

```
# Save root messages also to boot.log
local7.*
```

/var/log/boot.log

```
graph TD
    facility((facility)) --> m1["*.info:mail.none:authpriv.none:cron.none"]
    facility --> m2["# The authpriv file has restricted access.  
authpriv.*"]
    facility --> m3["# Log all the mail messages in one place.  
mail.*"]
    facility --> m4["# Log cron stuff  
cron.*"]
    facility --> m5["# Everybody gets emergency messages  
*.emerg"]
    facility --> m6["# Save news errors of level crit and higher in a special file.  
uucp.news:crit"]
    facility --> m7["# Save root messages also to boot.log  
local7.*"]
    level((level)) --> m1
    level --> m2
    level --> m3
    level --> m4
    level --> m5
    level --> m6
    level --> m7
    action((action)) --> m1
    action --> m2
    action --> m3
    action --> m4
    action --> m5
    action --> m6
    action --> m7
```

An Ninh Mạng ATHENA, www.athena.com.vn

## Service syslogd (tt)

- Log trong hệ thống được lưu liên tục sẽ quá nhiều log. Có những log quá cũ, không cần thiết nữa.
- Cần có một tiến trình cắt log hàng ngày, cắt theo theo kích thước do người dùng định nghĩa, để dọn dẹp bớt log cũ.
- Tiến trình thực hiện việc cắt log: logrotate.
  - /etc/logrotate.conf: định nghĩa các option dùng chung cho việc cắt log.
  - Những dịch vụ cắt log theo kiểu thông thường có thể định nghĩa trực tiếp trong file logrotate.conf
  - /etc/logrotate.d/: mỗi dịch vụ có thể định nghĩa một file riêng, để cắt log theo yêu cầu, phù hợp với dịch vụ đó.

An Ninh Mạng ATHENA, www.athena.com.vn

## Service syslogd (tt)

- File /etc/logrotate.conf

```
# global options
# rotate log files weekly
weekly
# keep 4 weeks worth of backlogs
rotate 4
# send errors to root
errors root
# create new (empty) log files after rotating old ones
create
# compress log files
compress
# specific files
/var/log/wtmp (
    monthly
    create 0664 root utmp
    rotate 1
)
○ File /etc/logrotate.d/radiusd
/data/radius/log/radius.log {
    rotate 10
    size=30M
}
```

An Ninh Mạng ATHENA, www.athena.com.vn

## Service crond

- Các dịch vụ cần chạy định kì, chạy vào một thời điểm nào đó cụ thể trong ngày -> cần các thao tác lập lịch.
- Service crond là service định kì gọi thực thi các tác vụ được định nghĩa sẵn.
- Chạy trực tiếp bằng lệnh crontab.
- Chạy bằng service crond, với file cấu hình là /etc/crontab

An Ninh Mạng ATHENA, www.athena.com.vn

## Service crond

- File /etc/crontab có cấu trúc như sau:
  - minute hour day month dayofweek command
  - minute: có giá trị từ 0-59.
  - hour: có giá trị từ 0-23
  - day of month: có giá trị từ 0-31
  - month: có giá trị từ 1-12
  - day of week: có giá trị từ 0-6
  - command: như command thực thi ở BASH shell.
  - trường nào có dấu “\*”: mọi lúc.
  - trường nào có dấu “/\*”: mỗi lúc.

An Ninh Mạng ATHENA, www.athena.com.vn

## Service crond

- Những dòng định nghĩa sau có ý nghĩa như thế nào???

- 0 1 \* \* \* command;
- 0 11,15 \* \* command;
- 0 11-15 \* \* command;
- 0 1 \*/5 \* \* command;

An Ninh Mạng ATHENA, www.athena.com.vn

## Service xinetd

- Mỗi dịch vụ đều lắng nghe, nhận request từ client. Có nhiều dịch vụ không có request thường xuyên, vẫn lắng nghe => tốn tài nguyên.
- xinetd - the extended Internet services daemon.
- xinetd quản lý chung các dịch vụ. xinetd sẽ lắng nghe tất cả các request gửi đến các dịch vụ mà nó phục vụ.
- Khi cần dịch vụ nào, xinetd mới khởi tạo dịch vụ đó, và forward request cho dịch vụ.
- Các dịch vụ chỉ cần nhận request từ xinetd, không nhận trực tiếp từ client.
- Các dịch vụ được xinetd bảo vệ kiểm tra trước khi nhận request.

An Ninh Mạng ATHENA, www.athena.com.vn

## Service xinetd (tt)

- Cấu hình xinetd:

- /etc/xinetd.conf: định nghĩa một số option chung cho các dịch vụ sử dụng xinetd.

```
defaults
{
    instances          = 60
    log_type          = SYSLOG authpriv
    log_on_success    = HOST PID
    log_on_failure    = HOST
    cps               = 25 30
```

- /etc/xinetd.d/\*, mỗi dịch vụ có một file cấu hình, định nghĩa cụ thể cấu hình của dịch vụ đó khi sử dụng xinetd.

An Ninh Mạng ATHENA, www.athena.com.vn

## Service xinetd (tt)

- File /etc/xinetd.d/krb5-telnet

```
service telnet
{
    flags             = REUSE
    socket_type      = stream
    wait              = no
    user              = root
    server            = /usr/kerberos/sbin/telnetd
    log_on_failure    += USERID
    disable           = yes
}
```

An Ninh Mạng ATHENA, www.athena.com.vn

## Service xinetd (tt)

- Trước khi cho phép xử lý request, xinetd có thể kiểm tra sự hợp lệ của IP request bằng những file sau:

- /etc/hosts.allow: những host trong file này được chấp nhận.  
ALL : 192.168.1.1  
ALL : 172.16.10.3  
ALL : 10.0.0.5
- /etc/hosts.deny: những host trong file này bị discard request.  
ALL: 192.168.4.3  
ALL: 10.0.0.10
- Câu hình như thế nào, để deny tất cả, chỉ chấp nhận những host trong hosts.allow???

An Ninh Mạng ATHENA, www.athena.com.vn

## Hỏi & Đáp



An Ninh Mạng ATHENA, www.athena.com.vn

## Compiling The Linux kernel



## Nội dung

- Kernel version.
- Kernel modules.
- Compiling kernel.

An Ninh Mạng ATHENA, www.athena.com.vn

## Kernel version

- Version của kernel có format như sau:
  - linux-major.minor.patchlevel
    - Vd: linux-2.6.18.8
  - major: version chính của kernel
  - minor: những thay đổi quan trọng của version.
    - số chẵn: version này đã được kiểm tra và công bố sử dụng. 2.4, 2.6...
    - số lẻ: version này dùng cho mục đích thử nghiệm. Các kernel developer thường sử dụng.
  - patchlevel: dùng để vá lỗi.

An Ninh Mạng ATHENA, www.athena.com.vn

## Kernel version (tt)

- Để xác định kernel version, dùng lệnh:
  - uname -a
  - uname -r

```
[root@centos-1 ~]# uname -r  
2.6.18-8.el5  
[root@centos-1 ~]# uname -a  
Linux centos-1 2.6.18-8.el5 #1 SMP Thu Mar 15 19:57:35 EDT 2007 i686 i686 i386 GNU/Linux
```

- Kernel mặc định đã được dịch với các module cần thiết, khi có nhu cầu có thể tiến hành dịch lại kernel => **có một hệ điều hành mới.**

An Ninh Mạng ATHENA, www.athena.com.vn

## Kernel modules

- Kernel thường được biên dịch với các module cần thiết nhất.
- Các module ít sử dụng có thể được insert vào kernel khi cần thiết.
- Các module của kernel là một file object, nằm trong thư mục  
*/lib/modules/kernel-version/kernel.*

An Ninh Mạng ATHENA, www.athena.com.vn

## Kernel modules (tt)

- Một số kernel modules:
  - block: module cho những thiết bị phần cứng đặc biệt: RAID controller, IDE tape drivers.
  - cdrom: module cho CDROM.
  - fs: module cho file systems.
  - ipv4: module cần thiết cho việc hoạt động với TCP/IP networking.
  - net: module cho network interface.
  - scsi: module cho SCSI controller.
  - video: module cho video adapter.
  - misc: các module không thuộc các module kể trên.

An Ninh Mạng ATHENA, www.athena.com.vn

## Kernel modules (tt)

- Lệnh lsmod: liệt kê những module đang được kernel hỗ trợ.
- Lệnh insmod: thêm một module vào kernel.
- Lệnh rmmod: xóa bỏ một module ra khỏi kernel.
- Lệnh modinfo: xem thông tin một module.
- File modules.dep: liệt kê mối quan hệ phụ thuộc giữa các module.

An Ninh Mạng ATHENA, www.athena.com.vn

## Compiling kernel

- Download source kernel từ:
  - kernel.org
- Để biên dịch được kernel, cần cài đặt bộ C compiler.
- Các lệnh để biên dịch:
  - make mrproper
  - make config, hoặc make menuconfig, make xconfig, hoặc make oldconfig.
  - Sau khi tạo file config xong, có thể edit trong makefile, và thực hiện tiếp các lệnh sau.

An Ninh Mạng ATHENA, www.athena.com.vn

## Compiling kernel (tt)

- Các lệnh để biên dịch kernel:
  - make dep
  - make clean
  - make bzImage
  - make modules
  - make modules\_install

An Ninh Mạng ATHENA, www.athena.com.vn

## Compiling kernel (tt)

- Các lệnh để biên dịch kernel:
  - make dep: những file source C sẽ được kiểm tra các mối quan hệ phụ thuộc.
  - make clean: remove những output file cũ có thể đã tồn tại trong source.
  - make bzImage: tạo một file kernel image.
  - make modules: biên dịch những driver thiết bị, và những module đã chọn lựa để biên dịch.
  - make modules\_install: tất cả những modules đã được biên dịch sẽ được cài đặt vào thư mục /lib/modules/kernel-version.

An Ninh Mạng ATHENA, www.athena.com.vn

## Compiling kernel (tt)

- Sau khi biên dịch kernel hoàn tất, tạo ra một kernel image và một initrd mới.
- Khởi động lại máy, boot loader sẽ nhận thêm một hệ điều hành mới.
- File system của hệ điều hành mới cũng là file system của hệ điều hành cũ.
- Hệ điều hành mới chỉ khác hệ điều hành cũ các modules được biên dịch trong kernel.

An Ninh Mạng ATHENA, www.athena.com.vn

## Hỏi & Đáp



An Ninh Mạng ATHENA, www.athena.com.vn



# Networking Fundamentals

## Nội dung

- Các file cấu hình
  - /etc/hosts
  - /etc/network
  - /etc/sysconfig/network-scripts/ifcfg-eth[n]
  - /etc/resolv.conf
  - /etc/services
- Các lệnh cấu hình, debug thông tin
  - ifconfig, ifup, ifdown
  - route
  - traceroute, netstat, tcpdump

An Ninh Mạng ATHENA, www.athena.com.vn

## File /etc/hosts

- ⦿ Là bản map giữa địa chỉ IP và tên máy tính trong network.
- ⦿ Tương tự file lmhosts của Windows.
- ⦿ Cú pháp của file:
  - IP address<Tab>Fully.Qualified.Name<space>[host\_alias]\*
  - 192.168.1.10                   centos-1.nhatnghe.com                   centos-1
- ⦿ Các ứng dụng trước tiên sẽ sử dụng file này khi cần truy vấn một máy tính bằng tên.

An Ninh Mạng ATHENA, www.athena.com.vn

## File /etc/sysconfig/network

- ⦿ File /etc/sysconfig/network định nghĩa các cấu hình network cơ bản cho máy tính.

The diagram illustrates the configuration of the /etc/sysconfig/network file. It shows the following mappings:

- `NETWORKING=yes` ← enable network
- `NETWORKING_IPV6=yes` ← enable network IPv6
- `HOSTNAME=centos-1` ← tên máy tính (Machine Name)
- `GATEWAY=192.168.2.1`

Annotations in orange explain the logic:

- A green circle highlights the `HOSTNAME` entry, with an arrow pointing to it labeled "so sánh với giá trị trong /etc/hosts" (Compare with value in /etc/hosts).
- An arrow points from the `GATEWAY` entry to the text "default gateway của máy tính" (Default gateway of the machine).

An Ninh Mạng ATHENA, www.athena.com.vn

## File ifcfg-eth[n]

- ⦿ Mỗi card mạng có một file cấu hình `/etc/sysconfig/network-scripts/ifcfg-eth[n]`.
- ⦿ n: có giá trị bắt đầu từ 1.
- ⦿ Card loopback có file cấu hình `ifcfg-lo`

The diagram illustrates the configuration of the ifcfg-eth[n] file. It shows the following mappings:

- `DEVICE=eth0` ← tên card mạng (Name of network card)
- `BOOTPROTO=static` ← gán IP tĩnh, hoặc DHCP (Assign static IP, or DHCP)
- `BROADCAST=192.168.2.255`
- `HWADDR=00:0C:29:48:C0:AE`
- `IPADDR=192.168.2.4`
- `IPV6ADDR=`
- `IPV6PREFIX=`
- `NETMASK=255.255.255.255`
- `NETWORK=192.168.2.0`
- `ONBOOT=yes` ← active khi boot. (Active at boot)

An Ninh Mạng ATHENA, www.athena.com.vn

## File /etc/resolv.conf

- ⦿ File /etc/resolv.conf dùng để định nghĩa name server mà máy tính sẽ sử dụng để thực hiện các truy vấn phân giải tên miền.
- ⦿ Một số cú pháp thông dụng:
  - domain: DNS domain của máy tính.
  - nameserver: IP hoặc tên của name server mà máy tính sẽ sử dụng. Có tối đa 3 giá trị.
  - search:

An Ninh Mạng ATHENA, www.athena.com.vn

## File /etc/services

- File /etc/services gồm một danh sách network port và các service sử dụng những port này.
- Khi định nghĩa một service mới, người quản trị phải định nghĩa một cặp service name và port number vào file /etc/services.

```
http      80/tcp    www www-http  # WorldWideWeb HTTP
http      80/udp    www www-http  # HyperText Transfer Protocol
```

- Port 0 – 1024: là những port đã được dành riêng.
- Port > 1024: port được định nghĩa thêm vào tùy theo nhu cầu của ứng dụng.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Lệnh ifconfig, ifup, ifdown

- Lệnh ifconfig dùng để cấu hình địa chỉ IP, netmask, địa chỉ broadcast và các tham số cấu hình khác.
  - ifconfig eth0 192.168.1.10 netmask 255.255.255.0
  - man ifconfig.
- Lệnh ifconfig cấu hình cho từng card mạng (từng interface).
- Các tham số cấu hình của lệnh ifconfig có ý nghĩa như file /etc/sysconfig/network-scripts/ifcfg-eth[n].
- Lệnh ifup dùng để enable một interface.
- Lệnh ifdown dùng để disable một interface.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Lệnh route

- Lệnh route dùng để hiển thị, chỉnh sửa, quản lý bảng routing table.
- Lệnh route cho phép định nghĩa các static route theo ý của người quản trị.
- Static route là những routing ít thay đổi, không phải cập nhật thường xuyên, được định nghĩa vì một mục đích nào đó.
- Lệnh route cũng cho phép người quản trị điều chỉnh default gateway theo ý muốn.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Lệnh traceroute, netstat, tcpdump

- Lệnh traceroute: để theo dõi đường đi của gói tin trong hệ thống mạng. Lệnh traceroute thường dùng để debug, xác định vì sao gói tin không di chuyển đến một network khác.
- Lệnh netstat: để liệt kê các port đang lắng nghe, các kết nối đang mở đến máy tính, và tình trạng của các kết nối này.
- Lệnh tcpdump: để bắt gói tin di chuyển trong network. Có thể lưu lại thành file, dùng ethereal để phân tích gói tin, xác định loại traffic, hoặc tìm kiếm các dấu hiệu mong muốn.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Hỏi & Đáp



An Ninh Mạng ATHENA, www.athena.com.vn



## DHCP Server

## Nội dung

- Giới thiệu dịch vụ DHCP
  - chức năng
  - gói cài đặt.
- File cấu hình
  - /etc/dhcpd.conf.
  - /var/lib/dhcpd/dhcpd.leases.
- Lệnh dhclient

An Ninh Mạng ATHENA, www.athena.com.vn

## Giới thiệu dịch vụ DHCP

- DHCP là dịch vụ cung cấp địa chỉ IP động cho các máy tính trong hệ thống.
- DHCP cũng cung cấp động các tham số khác: DNS, gateway..., cấp IP tĩnh.
- DHCP được cài đặt bằng hai gói:
  - dhcp-[version].rpm.
  - dhcp-devel-[version].rpm.
  - Hoặc cài đặt từ gói source.
- File cấu hình chính:
  - /etc/dhcpd.conf.

An Ninh Mạng ATHENA, www.athena.com.vn

## File /etc/dhcpd.conf

```
subnet 192.168.36.0 netmask 255.255.255.0 {  
  
    # --- default gateway  
    option routers           192.168.36.254;  
    option subnet-mask        255.255.255.0;  
  
    option nis-domain         "nhatnghe.com";  
    option domain-name        "nhatnghe.com";  
    option domain-name-servers 192.168.36.1;  
  
    option time-offset        -18000; # Eastern Standard Time  
    range dynamic-bootp 192.168.36.233 192.168.36.240;  
    default-lease-time 21600;  
    max-lease-time 43200;  
  
    # we want the nameserver to appear at a fixed address  
    host ns {  
        next-server marvin.redhat.com;  
        hardware ethernet 12:34:56:78:AB:CD;  
        fixed-address 207.175.42.254;  
    }  
}
```

An Ninh Mạng ATHENA, www.athena.com.vn

## File dhcpcd.leases

- File dhcpcd.leases theo dõi tình trạng cấp phát IP động:

```
lease 192.168.36.240 {  
    starts 1 2008/02/04 23:39:12;  
    ends 2 2008/02/05 05:39:12;  
    binding state active;  
    next binding state free;  
    hardware ethernet 00:0c:29:7d:7d:b9;  
}  
lease 192.168.36.240 {  
    starts 1 2008/02/04 23:40:15;  
    ends 2 2008/02/05 05:40:15;  
    binding state active;  
    next binding state free;  
    hardware ethernet 00:0c:29:7d:7d:b9;  
}
```

An Ninh Mạng ATHENA, www.athena.com.vn

## Lệnh dhclient

- Có thẻ get IP động bằng cách điều chỉnh file:
  - /etc/sysconfig/network-scripts/ifcfg-eth[n]
  - BOOTPROTO=dhcp
- Lệnh dhclient: dùng để get IP động từ DHCP server.

An Ninh Mạng ATHENA, www.athena.com.vn

## Hỏi & Đáp



An Ninh Mạng ATHENA, www.athena.com.vn

## NFS & Samba server

### Nội dung

#### ○ NFS server

- Giới thiệu dịch vụ NFS.
- Cấu hình dịch vụ NFS.
- NFS security.

#### ○ Samba server

- Giới thiệu dịch vụ Samba.
- Cấu hình dịch vụ Samba.
- SWAT

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

### Giới thiệu dịch vụ NFS

- NFS – Network File System là dịch vụ chia sẻ file trong môi trường network giữa các server Linux.
- Dịch vụ NFS cho phép các NFS client mount một phân vùng của NFS server như phân vùng cục bộ của nó.
- Dịch vụ NFS không được security nhiều, vì vậy cần thiết phải tin tưởng các client được permit mount các phân vùng của NFS server.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

### Cấu hình NFS

#### ○ Các tiến trình của NFS server:

- portmap
- rpc.nfsd
- rpc.statd và rpc.lockd
- rpc.rpquotad: kiểm soát quota mà NFS users có thể sử dụng.
- rpc.mountd: kiểm soát quyền được mount partition của NFS users.

#### ○ File cấu hình của NFS server:

- /etc/exports

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Cấu hình NFS (tt)

### File /etc(exports:

- Cú pháp:

– /path/to/export  
    |  
    |  
    Thư mục chia sẻ

[host](options)  
    |  
    |  
    Host truy cập

Quyền truy cập

- Ví dụ:

– /mnt/cdrom (ro)  
– /tmp (rw)  
– /home 192.168.0.0/255.255.255.0(rw)

An Ninh Mạng ATHENA, www.athena.com.vn

## Cấu hình NFS (tt)

### Quyền truy cập có các giá trị sau:

- secure : Port từ client requests phải nhỏ hơn 1024
- ro : Read only
- rw : Read – write
- noaccess : Denied access
- root\_squash : Ngăn remote root users
- no\_root\_squash : Cho phép remote root users

### Hai cú pháp sau giống hay khác nhau:

- host (options)
- host(options)



An Ninh Mạng ATHENA, www.athena.com.vn

## Cấu hình NFS (tt)

### Lệnh của NFS client:

- mount: dùng để mount một phân vùng của NFS server thành phân vùng cục bộ. Có thể đưa vào file /etc/fstab để mount tự động lúc khởi động.
- nfsstat
- rpcinfo
- showmount: hiển thị thông tin client nào sử dụng phân vùng nào của NFS server.

An Ninh Mạng ATHENA, www.athena.com.vn

## NFS security

### Để đảm bảo NFS security, sử dụng dựa vào 2 file /etc/hosts.allow và /etc/hosts.deny.

#### File /etc/hosts.deny

- portmap,lockd,mountd,rquotad,statd: ALL

#### File /etc/hosts.allow

- portmap,lockd,mountd,rquotad,statd:  
192.168.0.0/255.255.0.0

An Ninh Mạng ATHENA, www.athena.com.vn

## Giới thiệu dịch vụ Samba

- Samba là dịch vụ chia sẻ file và dịch vụ in trong môi trường network giữa các máy tính Linux và máy tính Windows.
- Từ Linux:
  - Mount thư mục chia sẻ của Windows.
  - Truy cập máy in của Windows.
  - Chứng thực với các máy tính Windows.
- Từ Windows:
  - Thấy những thư mục chia sẻ của Linux.
  - Chứng thực với các máy tính Linux.
  - Truy cập máy in của Linux.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Giới thiệu dịch vụ Samba (tt)

- Dịch vụ Samba gồm những tiến trình sau:
  - Tiến trình smbd:
    - lắng nghe trên port 139, trực tiếp xử lý các request truy cập đến thư mục chia sẻ trên Linux.
    - Khi một client kết nối, smbd sẽ tạo ra một tiến trình mới, phục vụ cho kết nối này.
  - Tiến trình nmbd:
    - lắng nghe trên port 137, chịu trách nhiệm cung cấp tên NetBIOS của samba server cho các request kết nối.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Giới thiệu dịch vụ Samba (tt)

- Windows và Linux đều sử dụng mã hóa khi cần chứng thực users.
- Khi users cần chứng thực, password do user nhập vào sẽ được mã hóa, đem so sánh với password mã hóa đã được lưu sẵn. Nếu giống nhau thì chứng thực thành công.
- Kiểu mã hóa mà Windows và Linux sử dụng là khác nhau.
- Để một user trên windows chứng thực thành công trên linux, tạo lại user đó trên linux, dùng lệnh smbpasswd.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Cấu hình Samba

- Dịch vụ Samba có thể được cài đặt từ RPM:
  - samba-client-[version]
  - samba-common-[version]
  - samba-[version]
  - system-config-samba-[version]
- Hoặc có thể cài đặt dịch vụ Samba từ gói source.
- File cấu hình chính của dịch vụ Samba:
  - /etc/samba/smb.conf
  - Dùng lệnh testparm để test file cấu hình Samba.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Cấu hình Samba (tt)

- File cấu hình dịch vụ Samba có thể được chỉnh sửa trực tiếp, hoặc chỉnh sửa qua giao diện web sử dụng SWAT.
- Định nghĩa các option chung của Samba trong section [global]:

```
hosts allow = 192.168.36.  
security = user  
passdb backend = smbpasswd
```

- Những thư mục share của Samba được định nghĩa thành từng section.

An Ninh Mạng ATHENA, www.athena.com.vn

## Cấu hình Samba (tt)

- Thư mục share của Samba:

```
[share] ← đường dẫn để share  
comment = Share Folder  
path = /share ← tên thư mục thật sự  
public = yes  
writable = yes } ← gán quyền  
printable = no
```

An Ninh Mạng ATHENA, www.athena.com.vn

## SWAT

- SWAT là giao diện web-based cho phép chỉnh sửa các cấu hình của Samba trên giao diện web.
  - <http://localhost:901/>
- Lệnh của Samba client:
  - smbclient
  - smbmount

An Ninh Mạng ATHENA, www.athena.com.vn

## Hỏi & Đáp



An Ninh Mạng ATHENA, www.athena.com.vn



**PAM**

## Nội dung

- Pluggable Authentication Modules (PAM).
  - Giới thiệu
  - Cấu hình

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

### Pluggable Authentication Modules

- Mỗi ứng dụng có một kiểu xác thực => phức tạp hệ thống.
- Pluggable Authentication Modules – PAM: cung cấp một phương thức xác thực tập trung.
- Ứng dụng không trực tiếp xác thực, mà chuyển request cho PAM, yêu cầu xác thực.
- PAM làm việc và trả về kết quả xác thực cho ứng dụng.
- Ứng dụng quyết định cho phép user login hay không.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

### PAM (tt)

- Theo cách hiểu của Windows, PAM đóng vai trò như DLL đối với các ứng dụng khác.
- Theo cách hiểu của Linux, PAM là một thư viện.
- PAM cung cấp nhiều module xác thực /lib/security từ đơn giản đến phức tạp.
- Khi ứng dụng cần xác thực theo phương thức nào thì gọi phương thức đó của trong thư viện của PAM.
- Thông tin về các module xác thực của PAM:
  - man [pam\_module]

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## PAM (tt)

- /lib/security: những module xác thực của PAM.
- /etc/security: file cấu hình tương ứng của từng module xác thực của PAM.
- /etc/pam.d: file cấu hình của những ứng dụng sử dụng PAM xác thực.
  - => mỗi ứng dụng xác thực bằng PAM có một file cấu hình trong /etc/pam.d

An Ninh Mạng ATHENA, www.athena.com.vn

## PAM (tt)

- *module\_type control\_flag module\_path arguments*
- module\_type: nhận một trong 4 giá trị: auth, account, session, password.
- control\_flag: cấu hình cách xử lí của ứng dụng với kết quả xác thực do PAM trả về.
- module\_path: đường dẫn cụ thể của module xác thực.
- arguments: các tham số khác.

An Ninh Mạng ATHENA, www.athena.com.vn

## PAM (tt)

<b>module_type</b>	<b>Mô tả</b>
auth	Ứng dụng yêu cầu user phải nhập password.
account	Không thực hiện chứng thực, dựa vào các yếu tố khác để quyết định user có được login không: login từ đâu, vào giờ nào...
session	Chi định những thao tác cần thực hiện trước hoặc sau khi user login.
password	Cho phép user đổi password.

An Ninh Mạng ATHENA, www.athena.com.vn

## PAM (tt)

<b>control_flag</b>	<b>Mô tả</b>
required	Module phải chứng thực thành công, nếu không kết quả fail sẽ được gởi về.
requisite	Nếu module này fail, kết quả sẽ được trả về ngay lập tức, không sử dụng đến các module sau.
sufficient	Nếu module này thành công, và không có module required nào nữa, kết quả thành công sẽ được trả về.
optional	Cho phép tiếp tục kiểm tra module khác, dù module này bị fail.

An Ninh Mạng ATHENA, www.athena.com.vn

## PAM (tt)

argument	Mô tả
debug	Log lại thông tin debug
no_warn	Không gửi msg warning đến ứng dụng.
use_first_pass	Lưu lại password, để sử dụng cho lần xác thực sau.
try_first_pass	Giống option trên, tuy nhiên nếu password fail, yêu cầu user nhập lại.

An Ninh Mạng ATHENA, www.athena.com.vn

## PAM (tt)

```
auth      include      system-auth
account  required    pam_nologin.so
account  include      system-auth
password include    system-auth
# pam_selinux.so close should be the first session rule
session  required    pam_selinux.so close
session  include      system-auth
session  required    pam_loginuid.so
session  optional   pam_console.so
```

Dùng lệnh man [pam\_module] để tìm hiểu về từng module xác thực:

Vd: man pam\_nologin

An Ninh Mạng ATHENA, www.athena.com.vn

## Hỏi & Đáp



An Ninh Mạng ATHENA, www.athena.com.vn



NIS

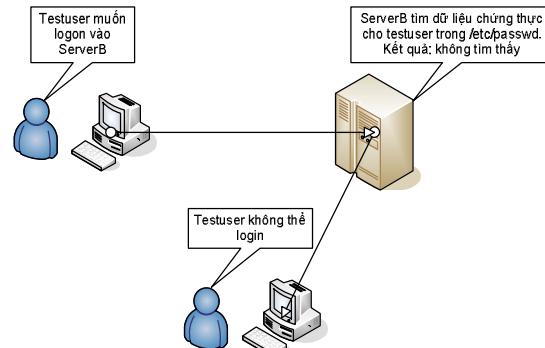
## Nội dung

- Giới thiệu NIS
- Cài đặt NIS
  - các daemon
  - file cấu hình
- NIS tools

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Giới thiệu NIS

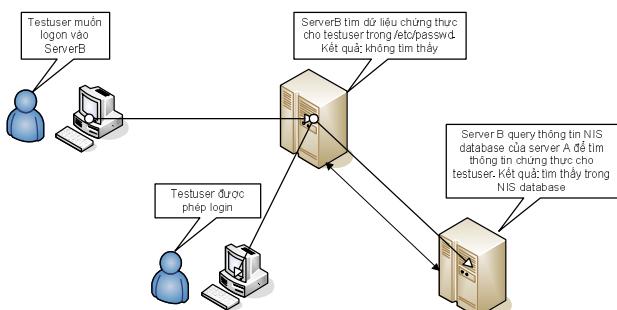
- Trước khi có NIS, việc chứng thực cho một user login vào hệ thống như sau:



An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Giới thiệu NIS (tt)

- Khi có NIS, việc chứng thực cho user login vào hệ thống có thể hiểu như sau:



An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Giới thiệu NIS (tt)

- NIS – Network Information Service là nơi lưu trữ dữ liệu tập trung để các client có thể truy vấn.
- Dữ liệu có thể lưu trữ trong NIS là những dữ liệu text.
  - /etc/passwd, /etc/hosts, /etc/services, /etc/protocol...
  - những dữ liệu text này cách nhau bằng "tab", và có ít nhất một cột có giá trị duy nhất trên mỗi dòng.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Cài đặt & cấu hình NIS

- NIS được cài đặt gói bằng gói rpm, hoặc source:
  - ypserv-[version].rpm
- NIS hoạt động theo mô hình client/server.
- Server có các daemon sau:
  - ypserv: lắng nghe truy vấn từ client, và trả lời cho những truy vấn này.
  - ypxfrd: transfer những thay đổi từ NIS master sang NIS slave.
- Daemon của client:
  - ypbnd: tìm kiếm NIS server để gửi truy vấn.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Cài đặt & cấu hình NIS (tt)

- Để NIS server có thể hoạt động được, đầu tiên cần khởi tạo dữ liệu cho NIS server bằng tiến trình ypinit.
- File /var/yp/Makefile: quyết định những dữ liệu nào NIS server sẽ hỗ trợ.
- Khi cần update dữ liệu của NIS server, sử dụng lệnh:
  - /var/yp/make

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## NIS tools

- Client có thể sử dụng những tools sau để truy vấn từ NIS server:
  - ypcat: dump nội dung một bảng map của NIS server.
    - ypcat passwd
  - ypwhich: cho biết NIS server nào đang phục vụ request
    - ypwhich
  - ypmatch: truy vấn dữ liệu bảng map của NIS match một từ khóa nào đó
    - ypmatch test passwd

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Hỏi & Đáp



An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## LDAP

### Nội dung

- Giới thiệu Network Directory
- Giới thiệu LDAP protocol
- Cấu trúc lưu trữ LDAP Directory
- Giới thiệu Openldap
  - server side daemon
  - client side command

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

### Network Directory

- Network directory là một cấu trúc dùng để tổ chức lưu trữ theo dạng phân cấp hình cây.
- Network directory được tổ chức để thuận tiện nhất cho việc đọc và tìm kiếm.
- Nếu ứng dụng cần nhiều thao tác insert, update thì không nên lưu trữ theo kiểu network directory.
- X.500 là một network directory.

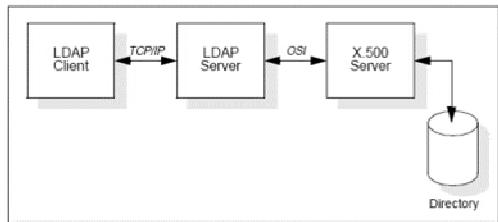
An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

### Giới thiệu LDAP protocol

- Để truy vấn network directory, người ta đã sử dụng giao thức DAP – Directory Access Protocol.
- Giao thức này quy định một tập lệnh giao tiếp giữa client và server lưu trữ (network directory) để truy vấn dữ liệu cần thiết.
- DAP hoạt động dựa trên giao thức OSI.
- LDAP – Lightweight Directory Access Protocol là giao thức ra đời để thay thế DAP.
- LDAP định nghĩa một tập lệnh giao tiếp giữa client/server dựa trên giao thức TCP để truy vấn dữ liệu directory.

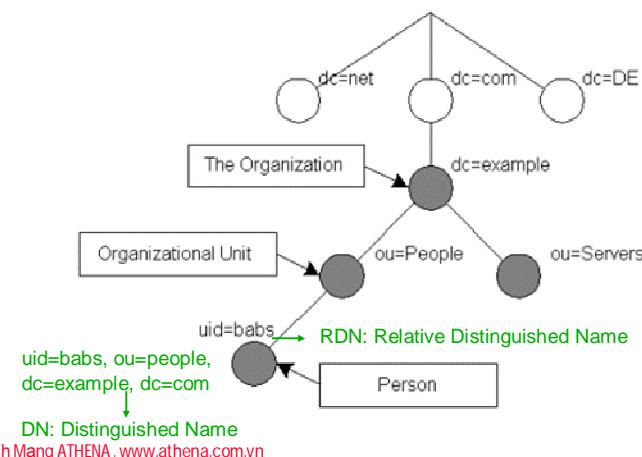
An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## LDAP protocol (tt)

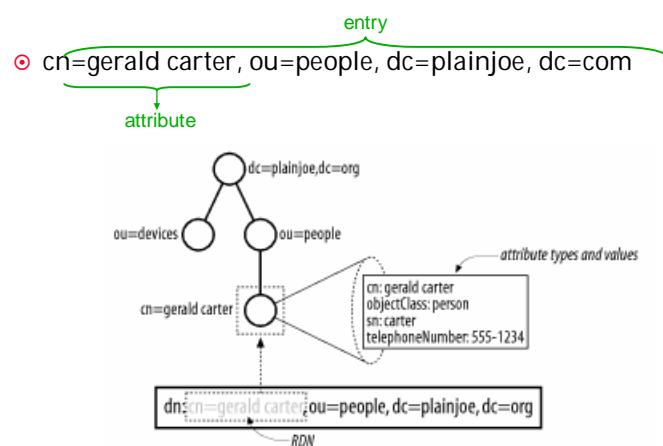


An Ninh Mạng ATHENA, www.athena.com.vn

## LDAP directory



## LDAP directory (tt)

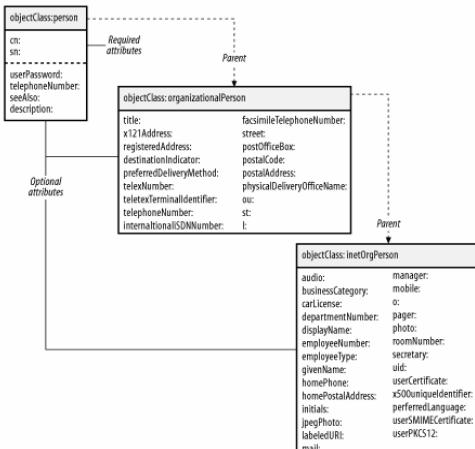


An Ninh Mạng ATHENA, www.athena.com.vn

- Những schema và objectclass thường được dùng đều đã được định nghĩa sẵn trong RFC.
- Khi muốn định nghĩa một cấu trúc cây thư mục, phân tích, quyết định cần những attribute nào, sau đó tìm những objectclass, schema có những attribute này.
- Từ đó, xây dựng nên cấu trúc cây thư mục.
- Nếu không có schema thỏa mãn yêu cầu, có thể định nghĩa schema, objectclass mới.

An Ninh Mạng ATHENA, www.athena.com.vn

## LDAP directory (tt)



An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## OPENLDAP (tt)

- Openldap là phần mềm mã nguồn mở, dùng để hiện thực LDAP chạy trên hệ điều hành Linux/ UNIX.
- Phía server gồm có hai dịch vụ chính:
  - slapd: standalone LDAP daemon. Daemon này lắng nghe các request truy vấn LDAP từ client, tiến hành truy vấn, và gửi câu trả lời.
  - slurpd: LDAP replication daemon. Daemon này dùng để đồng bộ những thay đổi từ LDAP master server sang LDAP slave server.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## OPENLDAP (tt)

- Để truy vấn LDAP, client dùng những lệnh sau:
  - ldapadd: thêm một entry mới.
  - ldapmodify: chỉnh sửa thông tin một entry.
  - ldapdelete: xóa một entry.
  - ldapmodrdn: chỉnh sửa RDN của entry.
  - ldapsearch: tìm kiếm thông tin entry.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Hỏi & Đáp



An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## FTP & SSH server

### Nội dung

#### ○ Dịch vụ FTP

- Giới thiệu dịch vụ FTP
- Cài đặt dịch vụ FTP
- Cấu hình dịch vụ FTP

#### ○ Dịch vụ SSH

- Giới thiệu dịch vụ SSH
- Cài đặt dịch vụ SSH
- Cấu hình dịch vụ SSH

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

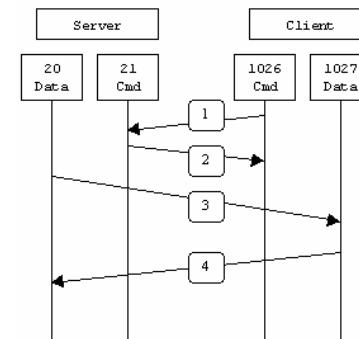
### Giới thiệu dịch vụ FTP

- Dịch vụ FTP là dịch vụ cung cấp cơ chế truyền, nhận file qua giao thức TCP/IP.
- Dịch vụ FTP hoạt động trên hai port:
  - Port 20: data port. Dữ liệu sẽ được truyền trên port này.
  - Port 21: control port. Port này dùng để trao đổi lệnh, reply giữa client và server.
- Dịch vụ FTP có hai mode hoạt động:
  - Active FTP.
  - Passive FTP.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

### Giới thiệu dịch vụ FTP (tt)

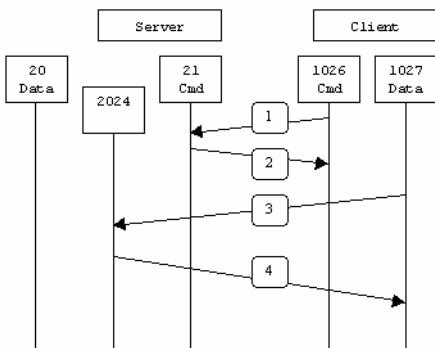
#### ○ Active FTP



An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Giới thiệu dịch vụ FTP (tt)

- Passive FTP



An Ninh Mạng ATHENA, www.athena.com.vn

## Cài đặt & cấu hình dịch vụ FTP

- Có nhiều gói để cài đặt dịch vụ FTP như: vsftpd, wuftpd, pureFTPD, proFTPD.
- Gói vsftpd được đánh giá là security tốt.
- Có thể cài đặt bằng RPM hoặc source.
- File cấu hình chính của gói vsftpd:
  - vsftpd.conf: kiểm soát hoạt động của dịch vụ FTP.
  - vsftpd.ftpusers: ds những users không được phép log vào FTP.
  - vsftpd.user\_list: tùy theo cấu hình file vsftpd.conf, dịch vụ FTP sẽ deny hoặc allow ds những users này.

An Ninh Mạng ATHENA, www.athena.com.vn

## Giới thiệu dịch vụ SSH

- Thẻ mạnh của hệ điều hành Linux là dòng lệnh.
- Dịch vụ SSH cho phép điều khiển một phiên làm việc từ xa bằng dòng lệnh.
- Dữ liệu, password truyền trong môi trường SSH là dữ liệu mã hóa.
- Vì tính an toàn dữ liệu, dịch vụ SSH được tin dùng hơn dịch vụ telnet.
- Dịch vụ SSH lắng nghe ở port 22.

An Ninh Mạng ATHENA, www.athena.com.vn

## Cài đặt dịch vụ SSH

- Mặc định dịch vụ SSH đã được cài đặt khi cài đặt máy tính.
- Hoặc có thể cài đặt dịch vụ SSH bằng gói:
  - openssh-[version].
- File cấu hình chính của dịch vụ SSH:
  - sshd\_config

An Ninh Mạng ATHENA, www.athena.com.vn

## Hỏi & Đáp



An Ninh Mạng ATHENA, www.athena.com.vn

## Nội dung

- Giới thiệu dịch vụ DNS.
- Hoạt động của dịch vụ DNS
  - Fully Qualified Domain Name (FQDN)
  - The in-addr.arpa Domain
  - Phân giải request DNS
  - Types of DNS server
- Cài đặt dịch vụ DNS
- Cấu hình dịch vụ DNS
- DNS tools

An Ninh Mạng ATHENA, www.athena.com.vn



## DNS server

## Giới thiệu dịch vụ DNS

- Để máy tính này có thể liên lạc với máy tính kia, cần phải biết địa chỉ IP.
- Người sử dụng khó khăn trong việc nhớ địa chỉ IP. Người sử dụng muốn liên lạc với máy tính khác trong mạng bằng tên máy tính.
- Cần có một bảng map giữa địa chỉ IP và tên máy tính.
- Với hệ thống mạng nhỏ, dùng file text để quản lý.
- Với mạng Internet, sử dụng dịch vụ DNS.

An Ninh Mạng ATHENA, www.athena.com.vn

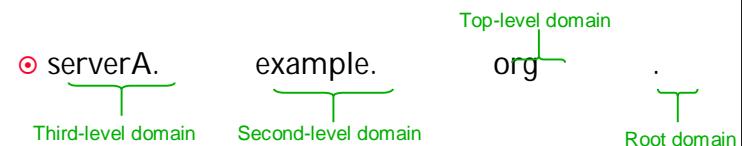
## Giới thiệu dịch vụ DNS

- Dịch vụ DNS – Domain Name Service là dịch vụ phân giải tên miền.
- Dịch vụ DNS sẽ ánh xạ từ tên miền sang địa chỉ IP.
- Dịch vụ DNS cho phép người dùng truy cập đến các máy tính khác bằng tên, không cần nhớ đến địa chỉ IP.
- Dịch vụ DNS được hiện thực bằng phần mềm Berkely Internet Name Domain system (BIND).

An Ninh Mạng ATHENA, www.athena.com.vn

## Fully Qualified Domain Name

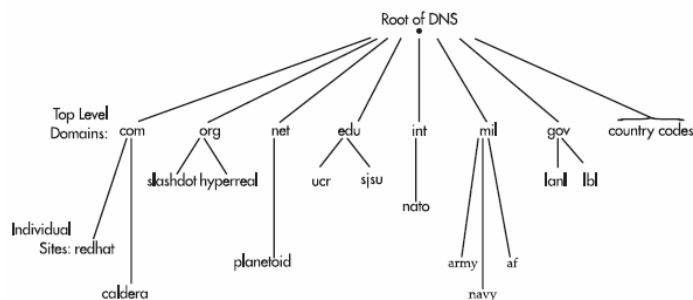
- Dịch vụ DNS quản lý tên miền bằng Fully Qualified Domain Name (FQDN).



- DNS quản lý tên miền theo cấu trúc cây.

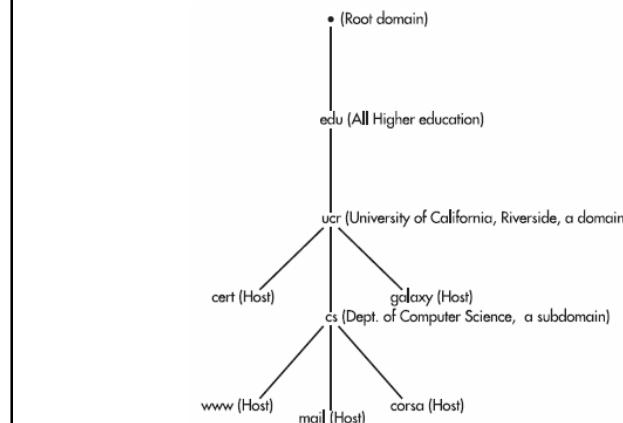
An Ninh Mạng ATHENA, www.athena.com.vn

## Fully Qualified Domain Name (tt)



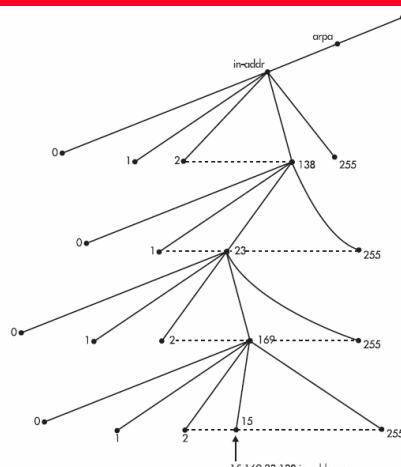
An Ninh Mạng ATHENA, www.athena.com.vn

## Fully Qualified Domain Name (tt)



An Ninh Mạng ATHENA, www.athena.com.vn

## The in-addr.arpa Domain (tt)



An Ninh Mạng ATHENA, www.athena.com.vn

## Phân giải request DNS

- request -> server DNS -> IP (a.b.c.d)
- domain name: tên miền do Athena quản lý.
- domain name: tên miền do VNNIC quản lý.
- domain name: tên miền quốc tế.
- request (domain name) -> server DNS -> IP (a.b.c.d)
- server DNS: DNS của Athena.
- server DNS: DNS của nhà cung cấp khác.

An Ninh Mạng ATHENA, www.athena.com.vn

## Phân giải request DNS (tt)

- Tên miền do Athena quản lý:
  - request -> Athena -> answer.
- domain name: tên miền do VNNIC quản lý.
  - request -> Athena -> VNNIC -> ISP -> answer.
- domain name: tên miền quốc tế.
  - request -> Athena -> Root servers -> DNS primary -> answer.

An Ninh Mạng ATHENA, www.athena.com.vn

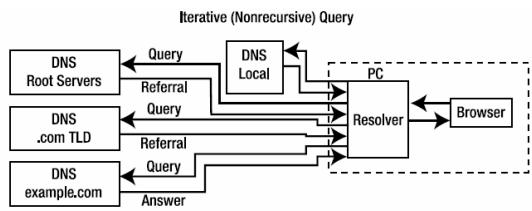
## Phân giải request DNS (tt)

- DNS Athena:
  - request -> Viettel -> answer.
- DNS của nhà cung cấp khác:
  - request -> DNS server -> answer.
  - request -> DNS server -> VNNIC -> Athena -> answer.

An Ninh Mạng ATHENA, www.athena.com.vn

## Phân giải request DNS (tt)

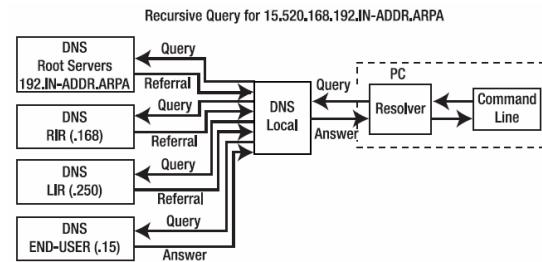
- Chi tiết xử lí request của DNS không hỗ trợ mode recursive:



An Ninh Mạng ATHENA, www.athena.com.vn

## Phân giải request DNS (tt)

- Chi tiết xử lí request của DNS hỗ trợ mode recursive:



An Ninh Mạng ATHENA, www.athena.com.vn

## Type of DNS server

- Primary DNS server
- Secondary DNS server
- Caching/ Forwarding DNS server

An Ninh Mạng ATHENA, www.athena.com.vn

## Cài đặt dịch vụ DNS

- Cài đặt dịch vụ DNS bằng các gói bind
  - bind-utils-[version]
  - bind-libs-[version]
  - bind-[version]
- File cấu hình chính của dịch vụ DNS:
  - named.conf

An Ninh Mạng ATHENA, www.athena.com.vn

## Cấu hình dịch vụ DNS (tt)

```
options
{
    query-source port 53;
    query-source-v6 port 53;
    directory      "/var/named"; // the default
    dump-file     "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    notify        yes;
};

zone "." in {
    type hint;
    file "named.root";
};

zone "nhatnghep.com" {
    type master;
    file "nhatnghep.com.db";
};
```

An Ninh Mạng ATHENA, www.athena.com.vn

} Option chung  
} Root servers  
} Định nghĩa domain

## Cấu hình dịch vụ DNS (tt)

- DNS hỗ trợ các bản ghi: SOA, NS, PTR, MX, A, CNAME.

	IN	SOA	ns.example.com. root.example.com. (
			1999080101 ; serial
			10800 ; refresh (3 hours)
			3600 ; retry (1 hour)
			604800 ; expire (17 days)
			86400 ) ; minimum (1 day)
	IN	NS	ns1.example.com.
	IN	NS	ns2.example.com.
	IN	MX	0 mail.example.com.
	IN	A	192.168.0.212
localhost	IN	A	127.0.0.1
www	IN	A	192.168.0.212
ns1	IN	A	192.168.0.10
ns2	IN	A	192.168.0.11
ftp	IN	CNAME	www
mail	IN	CNAME	www
irc	IN	CNAME	irc.example.net.

An Ninh Mạng ATHENA, www.athena.com.vn

## DNS tools

- Lệnh dig:
  - dig @nameserver domain
- Lệnh dnsquery:
  - dnsquery -n nameserver host
- Lệnh host:
  - host domain
- Lệnh nslookup:
  - nslookup record [server]
  - nslookup ipaddress

An Ninh Mạng ATHENA, www.athena.com.vn

## Hỏi & Đáp

An Ninh Mạng ATHENA, www.athena.com.vn



## Nội dung

- Giới thiệu dịch vụ Web.
- Giới thiệu Apache.
- Cài đặt Apache.
- Cấu hình Apache
- Access control
- Log Files
- Performance

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Giới thiệu dịch vụ Web

- World Wide Web (WWW) là một ứng dụng client-server dựa trên giao thức HTTP protocol.
- Web client (browsers) sẽ gửi request đến Web server sử dụng HTTP protocol.
- Web server nhận request, xử lý, và trả kết quả cho web client (browsers).
- HyperText Markup Language (HTML) là ngôn ngữ dùng để viết web.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Apache

- Nhiều phần mềm được sử dụng để hiện thực tính năng của web server: IIS, Apache...
- Apache là một phần mềm mã nguồn mở được sử dụng để làm web server phổ biến nhất trên Linux.
- Apache tương thích với hầu hết hệ điều hành UNIX, và cả Windows.
- Apache hoạt động linh hoạt, cho phép mở rộng nhiều tính năng, có thể biên dịch thêm nhiều module từ:
  - <http://modules.apache.org>

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Cài đặt Apache

- Có thể cài đặt Apache bằng gói rpm
  - httpd-[version].rpm
- Hoặc có thể cài đặt Apache bằng gói source
  - httpd-[version].tar.gz
- Khi cài đặt bằng gói source có thể chọn nhiều option để biên dịch Apache
  - --enable-proxy
  - --enable-ssl
  - --enable-rewrite
  - .....

An Ninh Mạng ATHENA, www.athena.com.vn

## Cấu hình Apache

- File cấu hình của Apache: httpd.conf
- Cấu hình của Apache gồm ba phần chính:
  - Global section: những cấu hình trong section này apply cho tất cả host trên server.
  - Main section: apply cho những virtual host không có section riêng.
  - Virtual host section: mỗi virtual host có thể có một section riêng.

An Ninh Mạng ATHENA, www.athena.com.vn

## Cấu hình Apache (tt)

File cấu hình của Apache: httpd.conf – Global section:

```
ServerRoot "/etc/httpd" # Vị trí cài đặt Apache
Timeout 120 # Thời gian sống của một kết nối (giây)
KeepAlive On # Client gửi nhiều yêu cầu đến server qua 1 kết nối
MaxKeepAliveRequests 100 # Số request tối đa trên một kết nối
KeepAliveTimeout 15 # Thời gian timeout của một request
Listen 80 # Listen nghe trên port 80
User apache # User và Group để chạy httpd
Group apache
ServerAdmin root@localhost # Email của người quản trị
ServerName www.nhatnghe.lpti.com:80 # Khai báo địa chỉ URL
DocumentRoot "/var/www/html" # Thư mục gốc của web server
```

An Ninh Mạng ATHENA, www.athena.com.vn

## Cấu hình Apache (tt)

- Virtual host: có hai kiểu hiện thực name-based và IP-based.
- Với kiểu IP-based, mỗi virtual phải có một card mạng:

```
<VirtualHost 192.168.1.1>
DocumentRoot /opt/apache/www.example1.com
ServerName www.example1.com
</VirtualHost>

<VirtualHost 192.168.2.1>
DocumentRoot /opt/apache/www.example2.com
ServerName www.example2.com
</VirtualHost>
```

An Ninh Mạng ATHENA, www.athena.com.vn

## Cấu hình Apache (tt)

- Cấu hình Apache hỗ trợ Virtual host theo kiểu name-based

```
NameVirtualHost *:80
<VirtualHost *:80>
ServerName www.example1.com
ServerAlias example1.com
DocumentRoot /opt/apache/www.example1.com
</VirtualHost>

<VirtualHost *:80>
ServerName www.example2.com
ServerAlias example2.com
DocumentRoot /opt/apache/www.example2.com
</VirtualHost>
```

An Ninh Mạng ATHENA, www.athena.com.vn

## Access control

- Access control giúp kiểm tra user nào được phép truy cập trang web.
- User có thể truy cập trang web nào, không thể truy cập trang web nào.
- Có thể giới hạn truy cập qua dãy IP của user.
- Có thể giới hạn truy cập bằng cách chỉ chấp nhận những user đã được xác thực (valid user).

An Ninh Mạng ATHENA, www.athena.com.vn

## Access control (tt)

- Có thể giới hạn truy cập qua thông tin users. Những user được kiểm tra username/pass đúng mới được truy cập.

- Tạo username/pass:

```
# /opt/apache/bin/htpasswd -c /opt/apache/password.list demouser
New password:
Re-type new password:
Adding password for user demouser
```

- Giới hạn truy cập trong file httpd.conf

```
<Directory /opt/apache/www.example1.com/protected>
AuthName "Authorized Users Only"
AuthType Basic
AuthUserFile /opt/apache/password.list
require valid-user
</Directory>
```

An Ninh Mạng ATHENA, www.athena.com.vn

## Log Files

- access\_log – liệt kê từng request truy cập vào trang web.
- agent\_log – liệt kê những chương trình được web server gọi chạy. Log này là option, có thể chọn lúc biên dịch apache, hoặc cấu hình trực tiếp trong file cấu hình httpd.conf
- error\_log – Lỗi phát sinh trong quá trình chạy của web server.
- refer\_log – liệt kê những URL trước đó browser đã sử dụng. Log này cũng là option, có thể chọn trong khi biên dịch, khi cấu hình, hoặc có thể không cấu hình.

An Ninh Mạng ATHENA, www.athena.com.vn

## Performance

- Những option này được định nghĩa trong phần Global Section:
  - StartServers: số tiến trình con được sinh ra lúc đầu khi web server start.
  - MinSpareServers: số tiến trình con tối thiểu ở trạng thái idle, để chờ kết nối.
  - MaxSpareServers: số tiến trình con tối đa cho phép ở trạng thái idle, để chờ kết nối.
  - MaxClient: web server phục vụ tối đa cho bao nhiêu request đồng thời.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Hỏi & Đáp

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)



*Trung tâm Đào tạo Quản trị & An ninh mạng*

**ATHENA**

## Nội dung

- Giới thiệu Squid server
- Cấu hình Squid server
  - Option
  - Cấu hình ACL
- Squid Authentication

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Giới thiệu Squid server

- Squid là một caching proxy server. Squid server được đặt giữa Web client và Web server.
- Khi có request yêu cầu Web page, Squid sẽ kiểm tra, xác nhận tính hợp lệ của request dựa trên những policy đã được định nghĩa trong Squid.
- Sau đó, truy vấn Web page để trả về kết quả cho request. Nếu kết quả đã có trong cache của Squid, thì Squid trả kết quả về ngay cho request.

An Ninh Mạng ATHENA, www.athena.com.vn

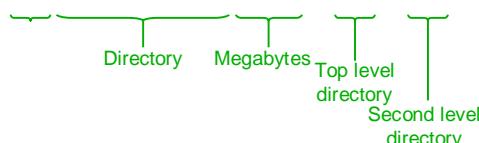
## Giới thiệu Squid server (tt)

- Squid server có thể được cài đặt bằng source hoặc bằng rpm.
- Squid server gồm những file sau trong hệ thống:
  - /etc/squid
  - /usr/lib/squid
  - /usr/sbin/squid
  - /var/log/squid

An Ninh Mạng ATHENA, www.athena.com.vn

## Cấu hình Squid server

- Một số option chính cấu hình Squid server:
  - http\_port: port Squid server lắng nghe request để phục vụ. Mặc định là port 3128.
  - cache\_dir: định nghĩa Squid server sẽ chứa cache ở đâu
    - cache\_dir storage\_type directory-name megabytes L1 L2 [options]
    - cache\_dir ufs /var/spool/squid 10000 16 256



An Ninh Mạng ATHENA, www.athena.com.vn

## Cấu hình Squid server (tt)

- cache\_mem: Squid server sẽ sử dụng bao nhiêu memory của RAM.
- cache\_access\_log: Squid server ghi nhận lại các request đã query Squid.
- acl: đây là phần phức tạp nhất của Squid server, cho phép người nào sẽ được truy cập Web, truy cập những trang nào.

```
acl intranet src 192.168.1.0/24  
http_access allow intranet  
http_access deny all
```

An Ninh Mạng ATHENA, www.athena.com.vn

## Cấu hình Squid server (tt)

- ⦿ Có thể dùng acl để giới hạn truy cập bằng nhiều cách:
  - Giới hạn truy cập theo thời gian.
  - Giới hạn truy cập theo IP.
  - Giới hạn truy cập theo port.
  - Giới hạn truy cập theo giao thức.
  - Giới hạn truy cập theo trang web.
  - Giới hạn file được phép download.
  - Giới hạn băng thông tối đa được sử dụng.

An Ninh Mạng ATHENA, www.athena.com.vn

## Cấu hình Squid server (tt)

```
http_port 192.168.1.1:3128          acl Safe_ports port 210
cache_mem 128M                      acl Safe_ports port 1025-65535
cache_access_log /var/log/squid/access.log  acl Safe_ports port 280
cache_dir ufs /var/spool/squid 1000 16 256  acl Safe_ports port 488
acl all src 0.0.0.0/0.0.0.0          acl Safe_ports port 591
acl manager proto cache_object      acl Safe_ports port 777
acl localhost src 127.0.0.1/255.255.255.255  acl CONNECT method CONNECT
acl to_localhost dst 127.0.0.0/8    http_access allow manager localhost
acl intranet src 192.168.1.0/24     http_access deny manager
acl SSL_ports port 443 563          http_access deny !Safe_ports
acl Safe_ports port 80              http_access deny CONNECT !SSL_ports
acl Safe_ports port 21              http_access allow localhost
acl Safe_ports port 443 563          http_access allow intranet
acl Safe_ports port 70              http_access deny all
```

An Ninh Mạng ATHENA, www.athena.com.vn

## Squid Authentication

- ⦿ Để sử dụng Squid, user phải có username/pass hợp lệ => Squid Authentication.
- ⦿ Để sử dụng tính năng Squid Authentication, cần biên dịch *ncsa\_auth* với Squid.
- ⦿ Tạo password cho user:

```
/opt/apache/bin/htpasswd -c /opt/squidusers.HTPASSWD demouser
```

- ⦿ Cấu hình Squid hỗ trợ tính năng Squid Authentication:

```
auth_param basic program /usr/sbin/ncsa_auth /opt/squidusers.HTPASSWD
acl passwd proxy_auth REQUIRED
http_access allow intranet passwd
```

An Ninh Mạng ATHENA, www.athena.com.vn

## Hỏi & Đáp

An Ninh Mạng ATHENA, www.athena.com.vn



## Nội dung

- Giới thiệu dịch vụ Mail
  - MUA – Mail User Agent.
  - MDA – Mail Delivery Agent.
  - MTA – Mail Transfer Agent.
  - Các protocol để transfer mail.
- Phân tích cách cấu hình MTA.
- Phân tích chính sách chống spam.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Giới thiệu dịch vụ Mail

- Dịch vụ Mail là dịch vụ quan trọng và cần thiết nhất đối với người sử dụng.
- Với người sử dụng, những lỗi thường gặp:
  - Gởi email, nhưng người nhận không nhận được, và người gửi cũng không nhận được msg báo lỗi.
  - Gởi email, nhưng > 1h, đến 1 ngày, người nhận mới nhận được email.
  - Thường xuyên phải nhận thư rác, thư quảng cáo...

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Giới thiệu dịch vụ Mail (tt)

- Để kiểm soát tốt dịch vụ Mail, người quản trị phải:
  - monitor tình trạng của email, đã được gởi đi chưa, gởi đến nơi chưa, đã được nhận về chưa, lý do vì sao không gởi được, không nhận được.
  - monitor được các kết nối gởi, nhận mail, nhiều hay ít, có bị nghẽn hay không?
  - kiểm soát được tình trạng gởi spam mail, virus mail...

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Giới thiệu dịch vụ Mail (tt)

- Quá trình gửi mail của người dùng như sau:
  - Người dùng cấu hình Outgoing, Incoming server trong chương trình soạn email. (Outlook, eudora, thunderbird...) → **MUA**
  - Dùng chương trình đó soạn email.
  - Người dùng send email. Server Outgoing nhận email → **MTA**
- Server Outgoing phân tích "To":address. Và liên lạc với server mail chịu trách nhiệm về rcpt này để gửi mail.  
→ **Remote MTA**

An Ninh Mạng ATHENA, www.athena.com.vn

## Giới thiệu dịch vụ Mail (tt)

- Quá trình liên lạc giữa các MTA như sau:
  - Sau khi phân tích "To":address, xác định rcpt cùng domain với sender, deliver local.  
→ **MTA**
  - Rcpt thuộc domain khác, outgoing sẽ dùng DNS để tìm bản ghi MX của mail server domain đó (remote MTA).
  - Outgoing sẽ liên lạc với remote MTA theo kết quả phân giải bản ghi MX của DNS.  
→ **SMTP**
  - Remote MTA sẽ chuyển email đến rcpt của họ.

An Ninh Mạng ATHENA, www.athena.com.vn

## Giới thiệu dịch vụ Mail (tt)

- User check email qua Incoming server. Incoming server thường là một server POP3 -> **MDA – Mail Delivery Agent**.
- Khi gửi mail trong cùng domain, server Outgoing (MTA) sẽ deliver mail cho server Incoming (MDA) bằng giao thức LMTP – Local Mail Transfer Protocol.
- Người sử dụng dùng giao thức POP hoặc IMAP kết nối với Incoming (MDA) để lấy mail về.

An Ninh Mạng ATHENA, www.athena.com.vn

## Giới thiệu dịch vụ Mail (tt)

- test@nhatnghe.com  
-> test1@yahoo.com
- Server outgoing Athena  
-> DNS -> Record MX ->  
Mail yahoo.
- outgoing → Mail yahoo  
-> test1@yahoo.com.
- test@nhatnghe.com  
-> test1@nhatnghe.com
- Server outgoing Athena  
-> Incoming Athena  
→ **LMTP**
- test1@nhatnghe.com -> checkmail bằng POP để nhận email từ Incoming.

An Ninh Mạng ATHENA, www.athena.com.vn

## Giới thiệu dịch vụ Mail (tt)

① [test1@yahoo.com](mailto:test1@yahoo.com)  
-> [test@nhatnghe.com](mailto:test@nhatnghe.com)

② Yahoo -> DNS ->  
Record MX -> Mail  
Athena.

③ Mail yahoo Mail  
Athena  
-> [test@nhatnghe.com](mailto:test@nhatnghe.com).

④ Mail Athena LMTP  
Incoming Athena để  
deliver mail cho  
[test@nhatnghe.com](mailto:test@nhatnghe.com)  
-> checkmail bằng POP để  
nhận email từ Incoming.

An Ninh Mạng ATHENA, www.athena.com.vn

## Giới thiệu dịch vụ Mail (tt)

① Các protocol sử dụng trong quá trình gửi nhận mail  
như sau:

- SMTP – Simple Mail Transfer Protocol: giao thức gửi nhận mail giữa các MTA.
- LMTP – Local Mail Transfer Protocol: giao thức deliver mail giữa MTA và MDA.
- POP – Post Office Protocol: giao thức lấy mail từ MDA về MUA.
- IMAP – Internet Mail Access Protocol: giao thức lấy mail từ MDA về MUA.

An Ninh Mạng ATHENA, www.athena.com.vn

## Giới thiệu dịch vụ Mail (tt)

- ① Các phần mềm dùng để đảm nhận chức năng MTA – Mail Transfer Agent:
  - Sendmail, Postfix, Qmail, Exim.
- ② Các phần mềm dùng để đảm nhận chức năng MDA – Mail Delivery Agent:
  - Procmail, Maildrop, Cyrus-IMAP, Courier IMAP.
- ③ Các phần mềm cho chức năng MUA – Mail User Agent:
  - Outlook, Thunderbird, Eudora.

An Ninh Mạng ATHENA, www.athena.com.vn

## Cấu hình MTA

- ① Khi cấu hình MTA, cần lưu ý những tính năng sau:
  - MTA yêu cầu user xác thực trước khi gửi mail => SMTP Authentication.
  - MTA xử lý mail cho những domain nào => relay domains.
  - MTA không chấp nhận kết nối từ những domain, IP nào.
  - MTA giới hạn số kết nối đồng thời từ một IP, số kết nối tối đa mà MTA có thể đảm nhận.
  - MTA giới hạn số rcpt tối đa có thể gửi đồng thời.
  - MTA giới hạn kích thước của msg.
  - Cách MTA xử lý hàng đợi mail: ở trong hàng đợi tối đa bao lâu, thời gian gửi warning cho người dùng, thời gian drop mail trong hàng đợi.
  - MTA sẽ chuyển mail cho server MDA nào.

An Ninh Mạng ATHENA, www.athena.com.vn

## Chính sách chống SPAM

- Chống SPAM cho mail có hai loại chính:
  - SPAM từ kết nối: chống SPAM bằng các chính sách kiểm tra kết nối gửi mail.
    - một IP liên tục mở nhiều kết nối -> hạn chế ngưỡng kết nối tối đa của một IP.
    - nhiều IP liên tục mở kết nối: kiểm tra reverse, dựa vào blacklist.
    - gửi liên tục nhiều email: dùng những phần mềm đánh giá nguồn gửi email.
  - Nội dung mail SPAM: chống SPAM bằng cách lọc nội dung email.
    - Nội dung email là nội dung quảng cáo
    - Email chứa virus nguy hiểm.
    - => dùng phần mềm lọc spam, virus.

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Hỏi & Đáp



An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)



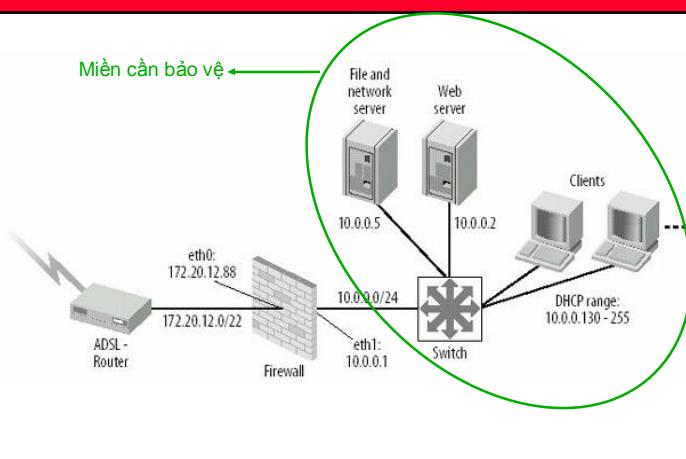
## Firewall

## Nội dung

- Giới thiệu iptables
  - Giới thiệu một mô hình mạng.
  - Phân tích traffic.
  - Áp dụng firewall.
- Mô hình xử lý logic của iptables
- Cú pháp iptables

An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Giới thiệu iptables



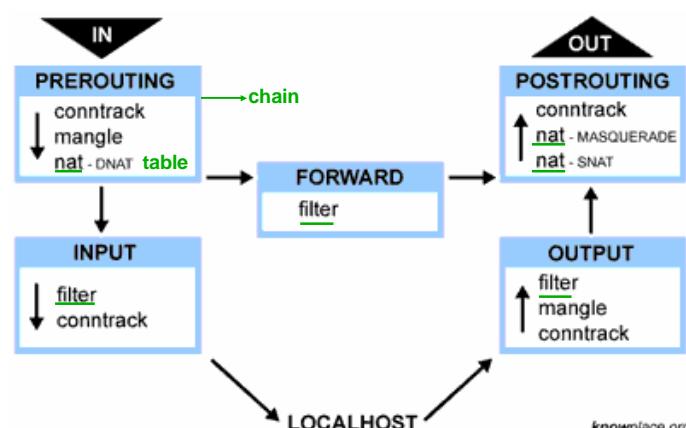
An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Giới thiệu iptables

- Cần quản lý những loại traffic sau:
  - Cho phép mọi traffic từ trong firewall (10.0.0.0/24) ra ngoài.
  - Cấm tất cả các traffic từ ngoài vào trong firewall, ngoại trừ những traffic sau:
    - TCP port 80, port 22, port 443 → filter
    - TCP port 80: forward đến web server.
    - TCP port 22: forward đến file server.
    - TCP port 443: forward đến file server.

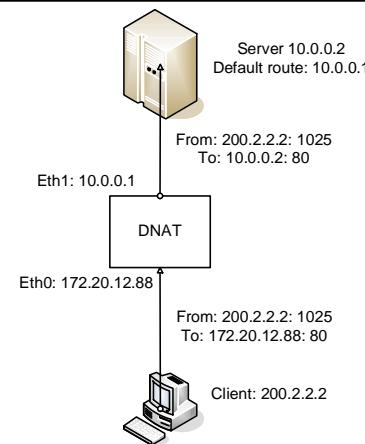
An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Mô hình logic iptables



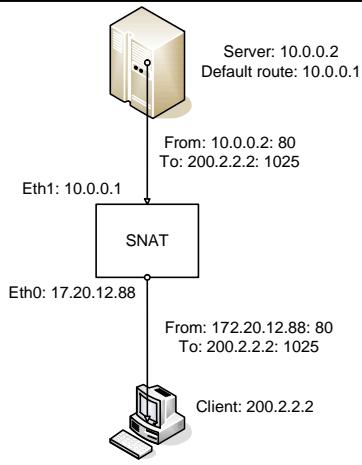
An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Mô hình logic iptables



An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Mô hình logic iptables



An Ninh Mạng ATHENA, www.athena.com.vn

## Cú pháp iptables

- iptables –t table –A chain [match] [target]
  - table: filter (default), nat, mangle
  - -A chain: thêm một rule mới.
  - -D chain: xóa một rule.
  - -I chain number: chèn một rule vào dòng [number].
  - -R chain number: thay thế một rule ở dòng [number].
  - -L chain: xem các rule đã có.
  - -F chain: xóa mọi rule hiện có.
  - -N chain: định nghĩa một chain mới.
  - -E [old\_chain] [new\_chain]: đổi tên chain (chỉ có thể thay đổi với những chain do người dùng tạo ra).

An Ninh Mạng ATHENA, www.athena.com.vn

## Cú pháp iptables (tt)

- iptables –A INPUT –p tcp –dport 22 –j ACCEPT
  - ACCEPT: cho phép gói tin đi qua.
  - DROP: vứt bỏ gói tin.
  - QUEUE: chuyển gói tin vào hàng đợi queue.
  - RETURN: trả về cho chain cấp trên hoặc default policy.
  - LOG: ghi lại thông tin packet trong system log
    - --log-level
    - --log-prefix
    - --log-tcp-sequence
    - --log-tcp-options
    - --log-ip-options

An Ninh Mạng ATHENA, www.athena.com.vn

## Cú pháp iptables – TARGET

- REJECT:
  - drop gói tin, đồng thời gửi gói tin ICMP trả lời về cho người gửi. Nếu đã gửi quá nhiều lần, sẽ không gửi nữa.
  - --reject-with type: gửi ICMP với type chỉ định.
    - icmp-net-unreachable
    - icmp-host-unreachable
    - icmp-port-unreachable
    - icmp-proto-unreachable

An Ninh Mạng ATHENA, www.athena.com.vn

## TARGET (tt)

- ◎ SNAT: chỉ có thể sử dụng trong table nat trong chain POSTROUTING
  - --to-source address[-address][:port-port]
  - -j SNAT --to-source 172.20.12.88
- ◎ DNAT: chỉ có thể sử dụng trong table nat trong chain PREROUTING
  - --to-destination address[-address][:port-port]
  - -j DNAT --to-destination 10.0.0.2:80
- ◎ MASQUERADE: là một dạng đặc biệt của SNAT.
- ◎ REDIRECT: chuyển hướng của gói tin tới một port khác trên máy local.
  - -j REDIRECT --to-ports 80

An Ninh Mạng ATHENA, www.athena.com.vn

## Match

- ◎ -p [!] name: chọn những packet dựa trên protocol. Protocol có thể là tên hoặc port tương ứng trong file /etc/protocols.
- ◎ -s [!] address[/mask]: chọn những packet dựa trên địa chỉ nguồn. Address có thể là hostname hoặc địa chỉ IP.
- ◎ -d [!] address[/mask]: cũng giống trường hợp trên nhưng là địa chỉ đích của packet.

An Ninh Mạng ATHENA, www.athena.com.vn

## Match (tt)

- ◎ -i name: chọn packet được nhận từ interface name (input).
- ◎ -o name: chọn những packet được gửi từ interface name (output).
- ◎ [!] -f: chọn những gói tin bị phân mảnh (từ mảnh vụn thứ hai).

An Ninh Mạng ATHENA, www.athena.com.vn

## Match (tt)

- ◎ --sport [!] [port][:port]: chọn những packet có port nguồn xác định như trên
- ◎ --dport [!] [port][:port]: chọn những packet có port đích xác định như trên.
- ◎ `iptables -A INPUT -p tcp -s 10.1.1.0/24 -i eth0 -d 192.168.1.1 --dport 80 -j ACCEPT`

An Ninh Mạng ATHENA, www.athena.com.vn

## Match icmp & mac (tt)

- Đổi với icmp (sử dụng -p icmp)
  - --icmp-type [!] type: chọn những packet icmp thuộc kiểu type. Type có thể chỉ định bằng số hoặc tên (iptables -p icmp -h)
- Đổi với mac (sử dụng -m)
  - --mac-source [!] address: chọn những packet có địa chỉ MAC nguồn là address. Address viết dưới dạng 00:60:08:91:CC:B7

An Ninh Mạng ATHENA, www.athena.com.vn

## Match limit (tt)

- Đổi với limit (sử dụng -m)
  - --limit rate: giới hạn tần suất của packet, được chỉ định bằng 1 con số và đằng sau là /second, /minute, /hour, /day. Default là 3/hour.
  - --limit-burst [number]: xác định số lượng packet tối đa được chấp nhận. Default là 5.

An Ninh Mạng ATHENA, www.athena.com.vn

## Match state (tt)

- Module state cho phép nhận biết và chọn các packet dựa trên trạng thái kết nối của các packet đó. Iptables là stateful.
  - --state states: chọn gói tin có trạng thái là 1 trong các trạng thái được liệt kê ở states
  - Các trạng thái của một kết nối là: INVALID, ESTABLISHED, NEW, RELATED

An Ninh Mạng ATHENA, www.athena.com.vn

## Hỏi & Đáp



An Ninh Mạng ATHENA, www.athena.com.vn

## IDS server

## Nội dung

- Giới thiệu Snort
  - Sniffer mode
  - Packet Logger mode
  - Network Instruction Detection System (NIDS)
  - Inline mode
- Cài đặt, cấu hình Snort
  - Preprocessor
  - Output modules
- Cấu trúc luật của Snort
  - Rule header
  - Rule option

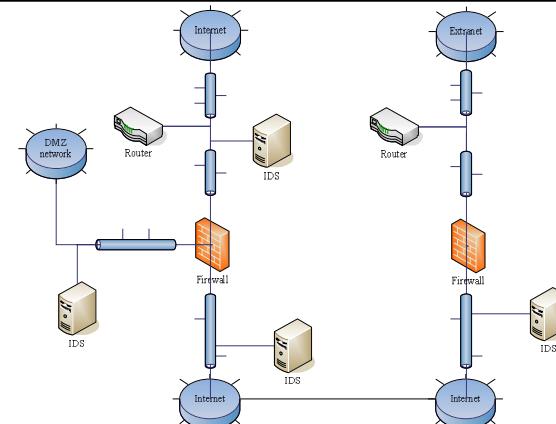
An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Giới thiệu Snort

- Snort là một phần mềm mã nguồn mở có khả năng phát hiện, chống sự xâm nhập trái phép.
- Snort hoạt động như một phần mềm đứng giữa sự giao tiếp của hai máy tính. Các packet trước khi được gửi đến máy tính đích sẽ được snort kiểm tra, thẩm định.
- Snort có thể phát hiện nhiều loại xâm nhập như: buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts...

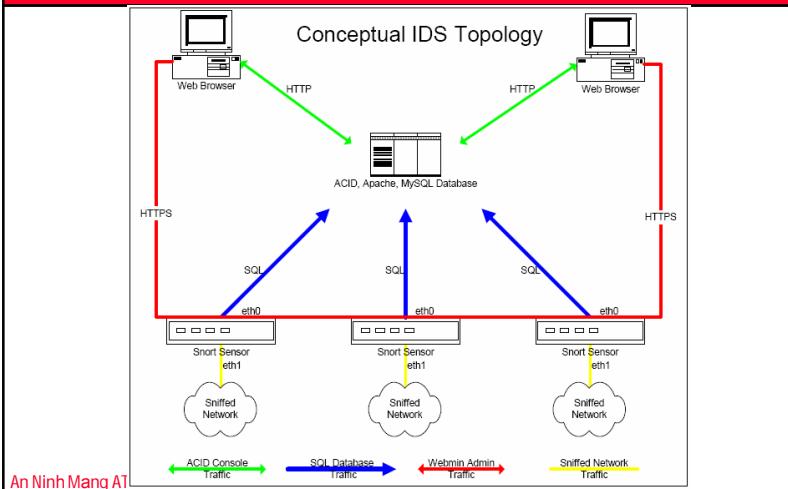
An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Giới thiệu Snort (tt)



An Ninh Mạng ATHENA, [www.athena.com.vn](http://www.athena.com.vn)

## Giới thiệu Snort (tt)



## Sniffer Mode

- Hiển thị thông tin header của packet:
  - snort -v
- Hiển thị thông tin ứng dụng đang phát sinh packet:
  - snort -v -d
- Header của tầng datalink:
  - snort -vde
  - snort -v -d -e

An Ninh Mạng ATHENA, www.athena.com.vn

## Packet Logger Mode

- Lưu thông tin xuống file:
  - snort –dev –l [filename]
- Lưu thông tin ở dạng binary:
  - snort –l [filename] -b
- Đọc ngược thông tin từ file binary:
  - snort –dv –r [filename]
  - snort –dv –r [filename] icmp

An Ninh Mạng ATHENA, www.athena.com.vn

## Network Instruction Detection System

- Mode hoạt động phức tạp nhất, nhiều option nhất.
- Bắt buộc phải chỉ ra file luật dùng để hoạt động (option -c)
  - snort –u snort –g snort –D –c /etc/snort
- Mặc định của mode này là cảnh báo full alert và log lại packet theo dạng ASCII.

An Ninh Mạng ATHENA, www.athena.com.vn

## Inline Mode

- Biên dịch hỗ trợ inline mode:
  - ./configure –enable-inline
- Có 3 loại luật được sử dụng ở mode inline:
  - **drop**: iptables sẽ bỏ qua packet và log lại sự kiện này.
  - **reject**: iptables sẽ bỏ qua packet, log lại sự kiện, và thông báo đến máy tính rằng packet này sẽ không đến nơi.
  - **sdrop**: iptables sẽ bỏ qua packet, không thông báo đến máy đích và cũng không log lại sự kiện.
- **snort\_inline -QDc ..etc/drop.conf -I /var/log/snort**

An Ninh Mạng ATHENA, www.athena.com.vn

## Cài đặt

- ./configure
- make
- make install
- Để hoạt động ở mode NIDS cần có tập luật: snortrules.tar.gz.
- tar -xzvf snortrules.tar.gz -C /etc/snort
- Sửa file /etc/snort/snort.conf

An Ninh Mạng ATHENA, www.athena.com.vn

## Cấu hình Snort

- *var HOME\_NET*: định nghĩa mạng cần bảo vệ.
- *var EXTERNAL\_NET*: định nghĩa mạng bên ngoài.
- *var DNS\_SERVERS*: định nghĩa các server DNS cần bảo vệ.
- *var SMTP\_SERVERS*: định nghĩa các server SMTP cần bảo vệ.
- *portvar HTTP\_PORTS* : định nghĩa port của ứng dụng.

An Ninh Mạng ATHENA, www.athena.com.vn

## Cấu hình Snort (tt)

- **preprocessor**: kiểm tra packet ngay sau khi packet được giải mã. Preprocessor được thực hiện trước tất cả các luật tìm kiếm, phát hiện khác.
  - **preprocessor <name>:<option>**
- **output module**: linh hoạt trong việc định dạng thông báo đến người sử dụng
  - **output <name>:<options>**

An Ninh Mạng ATHENA, www.athena.com.vn

## Cấu hình Snort (tt)

- Preprocessor:
  - stream4 -> replace bằng stream5
  - sfPortscan
  - Performance Monitor
  - ftp\_telnet
- Output modules:
  - alert\_syslog
  - alert\_fast
  - alert\_full
  - log\_tcpdump
  - alert\_csv

An Ninh Mạng ATHENA, www.athena.com.vn

## Cấu trúc luật Snort

- Rule header: rule action, protocol, địa chỉ IP nguồn và địa chỉ IP đích, port nguồn và port đích .
- Rule option: thông điệp cảnh báo, phần thông tin để xác định packet nào sẽ bị giữ lại.
- **alert tcp any any -> any any  
(content:"|00 01 86 a5|"; msg: "mountd  
access");**
  - Rule action
  - Protocol

An Ninh Mạng ATHENA, www.athena.com.vn

## Rule action

- Rule action:
  - **alert**: cảnh báo và ghi lại packet.
  - **log**: ghi lại packet.
  - **pass**: bỏ qua packet.
  - **active**: cảnh báo và gọi thực thi một rule khác.
  - **dynamic**: ở trạng thái idle cho đến khi được một rule khác được kích hoạt.
  - **drop**: cho phép iptables bỏ qua packet này và log lại packet bị bỏ qua.
  - **reject**: cho phép iptables bỏ qua packet này, log lại packet, đồng thời gửi thông báo từ chối đến máy nguồn.
  - **sdrop**: cho phép iptables bỏ qua packet này nhưng không log lại packet, cũng không thông báo đến máy nguồn.

An Ninh Mạng ATHENA, www.athena.com.vn

## Rule action (tt)

- Định nghĩa rule type riêng phù hợp với mục đích:

```
ruletype redalert
{
    type alert
    output alert_syslog: LOG_AUTH
    LOG_ALERT
    output database: log, mysql, user=snort
    dbname=snort host=localhost.
}
```

An Ninh Mạng ATHENA, www.athena.com.vn

## Rule option

- ◎ **meta-data**: cung cấp thông tin về rule nhưng không gây ra bất cứ ảnh hưởng nào đến quá trình phát hiện packet.
- ◎ **payload**: tìm kiếm thông tin trong phần payload của packet.
- ◎ **non-payload**: tìm kiếm thông tin trong phần non-payload của packet.
- ◎ **post-detection**: xảy ra sau khi một rule được kích hoạt.

An Ninh Mạng ATHENA, www.athena.com.vn

## Meta data

- ◎ **msg**: "<message text>";
- ◎ **reference**: <id system>, <id>;
- ◎ **sid**: <snort rules id>;
- ◎ **classtype**: <classname>;

Kiểu tấn công	Mô tả	Độ ưu tiên
attempted-admin	Có gắng chiếm quyền admin	Cao
attempted-user	Có gắng chiếm quyền user	Cao
successful-admin	Đã chiếm thành công quyền của admin	Cao
attempted-dos	Có gắng tấn công theo kiểu từ chối dịch vụ	Vừa
icmp-event	Sự kiện ICMP	Thấp

- ◎ **priority**: <priority integer>

An Ninh Mạng ATHENA, www.athena.com.vn

## Payload

- ◎ **content**: [!] "<context string>";
- ◎ **nocase**;
- ◎ **rawbytes**;
- ◎ **depth**: <number>;
- ◎ **offset**: <number>;
- ◎ **distance**: <byte count>;
- ◎ **uricontent**: [!]<context string>;
- ◎ **isdataat**: <int>;
- ◎ **byte\_test**: <bytes to convert>, [!] <operator>, <value>, <offset> [,relative] [,endian] [,<number type>, string];
- ◎ **byte jump**

An Ninh Mạng ATHENA, www.athena.com.vn

## Non Payload

- ◎ **ttl**: time to live.
- ◎ **tos**: type of service.
- ◎ **dsize**: kiểm tra non-payload có lớn hơn một kích thước xác định không.
- ◎ **flag**: kiểm tra TCP flag bits (F: FIN, S: SYN, R: RST, A: ACK).
- ◎ **flow**: xác định chiều của kết nối.
- ◎ **window**: kiểm tra tcp window size.

An Ninh Mạng ATHENA, www.athena.com.vn

## Post detection

- **logto**: kiểm tra log lại sự kiện vào file.
  - `logto: "filename";`
- **session**: sử dụng để lấy sự kiện từ một TCP session.
  - `session: [printable|all];`
- **resp, react**.

An Ninh Mạng ATHENA, www.athena.com.vn

## Hỏi & Đáp



An Ninh Mạng ATHENA, www.athena.com.vn