

Chương 7.

Mạng và Dịch Vụ Mạng

7.1. Tiến trình quản lý dịch vụ mạng-xinetd

- Red Hat Linux sử dụng **xinetd** (Extended Internet Services Deamon) để quản lý nhiều dịch vụ mạng phổ biến như FTP, IMAP, POP, telnet...
- **xinetd** duy trì các tài nguyên hệ thống, cung cấp chức năng quản lý truy cập và có thể sử dụng khởi động các dịch vụ theo mục đích đặc biệt nào đó.

- Các chức năng quản lý truy cập của **xinetd** bao gồm quản lý máy truy nhập, thời gian truy nhập, tốc độ và tài nguyên kết nối...
- Tập tin cấu hình của **xinetd** là **/etc/xinetd.conf**. Tập tin này là cha của tất cả các tập tin cấu hình của các dịch vụ được điều khiển bởi **xinetd**. Nó xác định các dịch vụ khác nhau cần phải kích hoạt khi được yêu cầu cùng với các lựa chọn và cơ chế bảo mật của dịch vụ.

- Theo mặc định **/etc/xinetd.conf** có chứa các thiết lập cấu hình cơ bản áp dụng cho mọi dịch vụ.
- Cấu hình riêng cho mỗi dịch vụ được đặt trong tập tin cấu hình tương ứng trong thư mục **/etc/xinetd.d/**.
- Những tập tin trong thư mục này sẽ được đọc mỗi khi **xinetd** khởi động. Tên các tập tin trong thư mục này trùng với tên dịch vụ được điều khiển bởi **xinetd**.

- Để bật hay tắt một dịch vụ do **xinetd** quản lý, ta cần sửa tập tin cấu hình của nó trong thư mục **/etc/xinetd.d/**.
 - Nếu thuộc tính **disable** được gán bằng **yes**, dịch vụ sẽ bị tắt.
 - Nếu thuộc tính **disable** được gán bằng **no**, dịch vụ được bật.
- Sau khi thay đổi trạng thái bật/tắt của một dịch vụ ta cần phải thực hiện khởi động lại **xinetd** để cho sự thay đổi có hiệu lực.
- Để bật/tắt hay khởi động lại **xinetd**, ta sử dụng script khởi động lại trong thư mục **/etc/rc.d/init.d/xinetd** **start | stop | restart**

7.2. Các tập tin cấu hình mạng cơ bản

- Các hệ thống Linux được thiết kế làm việc trong môi trường mạng sử dụng họ giao thức TCP/IP.
- Cấu hình một mạng TCP/IP trên Linux được thực hiện bằng cách sử dụng một tập hợp các tập tin cấu hình mạng nằm trong thư mục **/etc** và **/etc/sysconfig/**.
- Những tập tin cấu hình này xác định các thông tin về mạng như **tên máy**, **tên miền**, **địa chỉ IP**... Các tập tin cấu hình mạng cơ bản của Linux như sau:

- **/etc/hosts**

Tập tin này giúp thực hiện phân giải tên máy, khi không thể phân giải tên bằng bất cứ cách nào khác. Nó có thể sử dụng để phân giải tên máy trong trường hợp mạng không có máy chủ DNS. Tập tin này nên chứa một dòng thực hiện phân giải tên **localhost.localdomain** ứng với địa chỉ IP của giao tiếp mạng loopback (127.0.0.1)

- **/etc/resolv.conf**

Tập tin này xác định địa chỉ IP của máy chủ DNS

- **/etc/sysconfig/network**

Chứa các khai báo hệ thống về cấu hình mạng được sử dụng trong tiến trình khởi động. Những khai báo này bao gồm thông tin định tuyến, tên máy, gateway...

- **/etc/sysconfig/network-scripts/ifcfg-interface**

Chứa các tập tin script khởi động các giao tiếp mạng. Mỗi giao tiếp mạng có một cấu hình tương ứng.

7.3. Cấu hình mạng

Sau khi đã có sự thay đổi về cấu hình mạng, ta cần thông báo lại cho nhân hệ điều hành biết về các thay đổi này bằng cách thi hành script sau

/etc/rc.d/init.d/network stop| start |restart

7.3.1. Tên máy

- **Lệnh hostname**

Xem và đặt tên máy

- **Cú pháp:**

hostname [tên máy]

- Muốn lưu lại tên máy khi restart hệ thống hay dịch vụ mạng thì ta thêm dòng **hostname= tên máy** vào file **/etc/sysconfig/network**

7.3.2. Cấu hình giao tiếp mạng- Lệnh **ifconfig**

Sử dụng để nhận diện và cấu hình các thiết bị mạng trên Linux

- Tên giao tiếp mạng của Linux được định nghĩa bên trong nhân hệ điều hành chứ không phải được quản lý thông qua một tập tin thiết bị (trong /dev/). Tên của một số giao tiếp mạng như sau:
- **lo**: Đây là giao tiếp mạng loopback được sử dụng với mục đích kiểm tra
- **eth0, eth1, eth2....**: Được sử dụng cho các card mạng Ethernet, tên này thông thường phụ thuộc vào thứ tự của thiết bị được cấu hình. Ví dụ: card đầu tiên là **eth0**...

- Có hai chế độ hoạt động của chương trình **ifconfig**
 - Chế độ thông báo
 - Chế độ cấu hình
- **ifconfig [interface]**
 - Chế độ thông báo hiển thị các thông tin cấu hình của thiết bị mạng đã được cài đặt.
 - Nếu không có đối số kèm theo sẽ hiển thị thông tin tất cả các giao tiếp mạng đã được cấu hình.
- **Ví dụ: ifconfig eth1**

- **ifconfig interface [aftype] options| address**

- Chế độ cấu hình của **ifconfig** cho phép thiết lập, thay đổi các tham số cho các card mạng.

- Trong đó

- **interface** là card mạng cần cấu hình
- Sau **interface** có thể là họ địa chỉ **aftype** (address family) được sử dụng để hiển thị và giải mã tất cả các địa chỉ giao thức trong lệnh **ifconfig**.

- Ví dụ:

ifconfig eth1 192.168.1.10 netmask 255.255.255.240

- Họ địa chỉ mặc định là **inet** (TCP/IP), trong trường hợp sử dụng IPv6 thì họ địa chỉ là **inet6**. Đối số sau cùng là các options hay địa chỉ IP gán cho card mạng.

- **Các option:**

- **address**: Địa chỉ IP gán cho giao tiếp mạng. Nếu không khai báo subnetmask thì subnetmask mặc định của địa chỉ này được lấy theo lớp địa chỉ IP của thiết bị.

- **netmask mask**: Khai báo subnetmask là **mask** cho giao tiếp mạng

- **up**: Kích hoạt giao tiếp mạng interface

- **down**: Tắt giao tiếp mạng

- Ta có thể dùng lệnh **ifdown <interface>** hoặc **ifup <interface>** để **inactive** hoặc **active** một **interface**

7.3.3. Script khởi động giao tiếp mạng

Mỗi giao tiếp mạng trong hệ thống đều có một script tương ứng dùng để khởi động nó. Script này được đặt tên là **ifcfg-interfaceName** (**interfaceName** là tên giao tiếp của card mạng. Ví dụ: **ifcfg-eth0**) được đặt trong thư mục **/etc/sysconfig/network-scripts/**. Nội dung cơ bản của script này bao gồm các khai báo sau:

- **DEVICE=name**: tên giao tiếp mạng name
- **IPADDR=address**: IP gán cho giao tiếp
- **NETMASK=mask**: subnetmask của giao tiếp
- **GATEWAY=ip_address**: Địa chỉ IP của gateway mà card mạng kết nối tới.
- **ONBOOT=yes|no**: Nếu là **yes** thì các thông số cấu hình sẽ được gán cho card mạng mỗi khi hệ thống khởi động. Nếu là **no** thì ngược lại
- **BOOTPROTO=static|dhcp**: Nếu là **static** thì giao tiếp mạng sẽ nhận địa chỉ IP, netmask, và địa chỉ gateway được khai báo trong script này. Nếu là **dhcp** thì card mạng sẽ nhận các địa chỉ trên thông qua **DHCP server** và khi đó không cần phải khai báo các dòng **IPADDR**, **NETMASK** và **GATEWAY**

7.3.4. Khai báo nhiều IP cho một card mạng

- Trong một số trường hợp ta có thể muốn gán nhiều địa chỉ IP cho một card mạng. Việc này thường được gọi là alias (tên hiệu) cho giao tiếp mạng. Mỗi alias có thể xem như là một giao tiếp mạng độc lập
- Tên alias của một giao tiếp mạng được đặt theo quy định sau

InterfaceName : cloneName

- Trong đó **interfaceName** là tên của card mạng
- **cloneName** là các số nguyên bắt đầu từ 0 chỉ ra tên alias của card mạng.
- Ví dụ:
ifconfig eth1:1 192.168.1.5 up
ifconfig eth1:2 192.168.2.10 up

7.4. Định tuyến mạng- routing

- IP Routing là một cách thức mà theo đó một máy tính có thể kết nối tới nhiều mạng sẽ quyết định nơi mà nó chuyển các gói IP mà nó nhận được đến.
- Trên một mạng lớn, các gói dữ liệu được gửi đi từ máy tính này đến máy tính khác cho đến khi đến máy tính đích.
- Để xác định đường đi của gói trong mạng ta cần thiết lập lộ trình (route).
- Lộ trình có thể là động (dynamic routing) hoặc tĩnh (static routing)

- Đường dẫn tĩnh có nghĩa là sử dụng một bảng dẫn đường để xác định địa điểm gửi đi các gói tin.
- Để thiết lập đường dẫn tĩnh ta có thể sử dụng lệnh **route** hay khai báo trong tập tin script **/etc/sysconfig/static-routes**.
- Việc thực hiện dẫn đường rất quan trọng trong trường hợp máy tính có từ hai card mạng trở lên.
- Để xem bảng dẫn đường hiện hành, ta sử dụng lệnh **route** không có tham số kèm theo

- Để bổ sung thêm hay loại bỏ các mục từ trong bảng dẫn đường, ta sử dụng lệnh **route** với các tham số là **add** hay **del** theo cú pháp
route add [-net|-host] target [netmask Nm] [gw Gw]
route del [-net|-host] target [netmask Nm] [gw Gw]
- Trong đó:
 - **add**: Bổ sung thêm tuyến đường vào bảng
 - **del**: Xóa một tuyến đường ra khỏi bảng

- net**: Khai báo thiết lập đường đi cho một mạng
- host**: Khai báo thiết lập đường đi cho một máy tính.
- target**: Địa chỉ máy hay mạng cần thực hiện định tuyến.
- netmask Nm**: Khai báo subnetmask **Nm** của máy hay mạng (target) cần định tuyến
- gw Gw**: Khai báo địa chỉ **IP** hay tên **Gw** của gateway thực hiện xử lý các gói tin.
- **Ví dụ**
`route add -net 192.168.15.0 netmask 255.255.255.0 gw 192.168.125.1`

- Khi bổ sung thêm một mục từ vào bảng dẫn đường bằng lệnh **route** thì khi ta khởi động lại dịch vụ mạng, những mục từ mới thêm sẽ không tồn tại trong bảng dẫn đường.
- Để giải quyết vấn đề này, Linux cung cấp một script cho phép ta khai báo các mục từ tĩnh cho bảng dẫn đường.
- Script này được đặt tên là **/etc/sysconfig/static-routes**, mỗi dòng trong nó có chứa một khai báo tuyến đường tĩnh với định dạng sau:

device net network netmask gw Gateway

- Trong đó **device** là tên giao tiếp mạng mà các gói tin phải đi qua trước khi được chuyển đến mạng **network/netmask** thông qua máy **gateway**.

- Ví dụ

eth1 net 192.168.15.0 netmask 255.255.255.0 gw 192.168.3.1

7.5. Chuyển tiếp gói tin – ip forwarding

- Trong trường hợp hệ thống của ta có từ hai card mạng trở lên, ta cần phải bật chức năng chuyển tiếp gói tin để có thể được chuyển tiếp giữa các card mạng (mặc định hệ thống sẽ không bật chức năng này).
- Để thực hiện bật/tắt chuyển tiếp gói tin giữa các card mạng ta thực hiện một trong các cách sau:

- Thi hành lệnh để bật chức năng ngay lập tức
echo > 1 /proc/sys/net/ipv4/ip_forward
- Khai báo trong tập tin **/etc/sysctl.conf** mục từ sau (để được có hiệu lực mỗi khi khởi động máy lại)
net.ipv4.ip_forward = 1

7.6. Một số tiện ích theo dõi mạng

• Ping

- Là tiện ích theo dõi mạng phổ biến nhất.
- Giao thức mà lệnh ping sử dụng là ICMP.
- Lệnh ping cho phép kiểm tra kết nối mạng từ một máy tính đến máy tính nào đó trên mạng. Lệnh ping liên tục gửi các gói tin ICMP yêu cầu đến máy tính đích, máy tính đích sau khi nhận được yêu cầu sẽ gửi thông điệp trả lời.
- Trường hợp không có kết nối tới máy tính đích thì một thông điệp lỗi sẽ được trả về.

- Nguyên nhân lỗi của lệnh ping có thể do lỗi vật lý trên đường kết nối, lỗi do cấu hình mạng, do firewall và cũng có khi máy tính đích đang tắt.
- **Các cú pháp**
ping IP|hostname
ping 127.0.0.1| loopback| localhost
- **tracert**
 - Tương tự như lệnh **ping**, lệnh **tracert** cho phép kiểm tra đường kết nối tới một máy tính khác.
 - Tuy nhiên ngoài chức năng giống như ping, lệnh này còn cho ta biết được thông tin đường đi tới máy đích.

- Nó có thể được sử dụng để theo vết dây các mạng/hệ thống mà thông điệp của ta phải đi qua trước khi tới đích và qua đó cũng dễ dàng hơn trong việc nhận diện sự cố kết nối trên mạng.
- Kết quả của lệnh này sẽ liệt kê danh sách các gateway mà gói tin đi qua để tới được máy tính đích
- **Cú pháp**
tracert IP | hostname

- **netstat**

- Lệnh này là tiện ích cung cấp thông tin theo thời gian thực về trạng thái của các kết nối mạng, bảng định tuyến, cũng như thông số thống kê mạng.

- **Cú pháp**

netstat [options]

- Theo mặc định lệnh **netstat** sẽ hiển thị một danh sách các socket đang mở.

- **Các option**

- t: Hiển thị thông tin các kết nối TCP socket

- u: Hiển thị thông tin các kết nối UCP socket

- i: Hiển thị thông tin thống kê cho tất cả các giao tiếp mạng.

- a: Hiển thị thông tin các kết nối của tất cả các Internet socket.

- r: Hiển thị bảng định tuyến

- c: Thực hiện cập nhật liên tục trạng thái

- **who, w, finger**

Cung cấp thông tin về các người dùng đang đăng nhập hệ thống.

