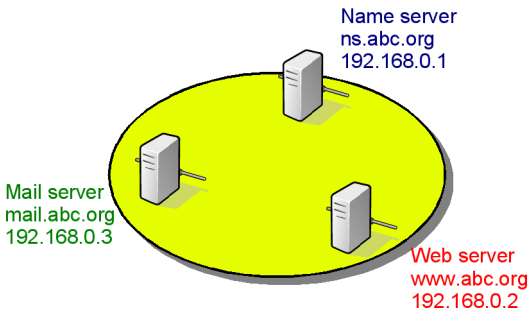
Network Services

Name Server

- The ISC's BIND is the most popular name server software.
- Package name is `bind9`
  - Default configuration allows bind to operate as a local name server.
- The service name is `bind9`.
  - Try to start it, and test :)
- To set up an authoritative name server:
  - Configure a zone in `/etc/bind/named.conf.local`
  - Write a zone file, put it in `/etc/bind/master/`

(cont.)

- The abc.org



(cont.)

- Add a new zone:

```
zone “abc.org” {
  type master;
  file “/etc/bind/master/abc.org”;
  allow-update { none; };
};
```

- Create `/etc/bind/master` directory

(cont.)

- A zone file - `/etc/bind/master/abc.org`

```
$TTL 2H
@     IN  SOA  ns.abc.org. root.abc.org. (
                2006022501 ; serial
                8H         ; refresh
                2H         ; retry
                1D         ; expire
                1H)        ; min TTL
      NS       ns.abc.org.
      MX  10   mail.abc.org.
ns    A        192.168.0.1
www   A        192.168.0.2
mail  A        192.168.0.3
```


(cont.)

- Check the configuration and zone file

```
# named-checkconf
# named-checkzone
```

- Restart `named` or reload the configuration file

```
# /etc/init.d/bind9 restart
```

or

```
# rndc reload
```

- Now test the `abc.org` domain

```
# dig abc.org
# dig www.abc.org
```

- Try to change and update the domain

DHCP Server

- Dynamic Host Configuration Protocol is used to automatically configure basic networking for clients
  - IP addresss and netmask
  - Gateway
  - DNS servers
  - WINS, etc. etc.
- We'll use the popular ISC DHCP3 server.
- The package and service name is `dhcp3-server`.
- Edit `/etc/default/dhcp3-server`
  `INTERFACES="<iface>"`

(cont.)

- Edit `/etc/dhcp3/dhcpd.conf`, comment default options and lease, then add

```
subnet 192.168.0.0 netmask 255.255.255.0 {
  range 192.168.0.128 192.168.0.250;
  option domain-name-servers 192.168.0.1;
  option domain-name "abc.org";
  option routers 192.168.0.254;
  option broadcast-address 192.168.0.255;
  default-lease-time 3600;
  max-lease-time 7200;
}
```


Mail Server

- sendmail is very popular and is installed by default. It is very powerful, and flexible. You may go with sendmail. But,
  - The configuration file is human-unreadable.
    - Not so good for novice administrators.
  - Serious security vulnerabilities, so far, every 6 months.
- The alternative is Postfix.
  - Fast, small, easy
- Just install `postfix`
  - Choose “internet site” configuration.
  - Set mail name (the address after @ sign)

(cont.)

- You may want to revisit the config file at `/etc/postfix/main.cf`.
  ```
  myhostname = <hostname>
  mydestination = <hostname or domain>
  inet_interface = all
  mynetworks = <network address>
  ```
- The service name is `postfix`.

Web Server

- Apache HTTPD server is the most popular HTTP server.
- The package is `apache2`
- The config file is `/etc/apache2/*.conf`.
- The (default) web page configuration is `/etc/apache2/site-available/default`
  - See the `DocumentRoot`.
- The service name is `apache2`.
  - Start it and try to access your web server.
    - Install `elinks` to access your web on the console.
  - Now you can write your own web pages.

PHP and MySQL

- There are many packages to be installed, but, thanks to the APT, we can just install
  - `libapache2-mod-php5`
  - `php5-mysql` or `php5-mysqli`
- The configuration file is at `/etc/php5/apache2/php.ini`.
- Try to restart `apache2` and access the web page.
  - Now, write a piece of PHP code in your web page.

MySQL Server

- To manipulate data in databases, you need to install the mysql server.
- Install `mysql-server-5.0`
- The service name is `mysql`.
  - Start and try to connect to the server.
    `# mysql -uroot`

Web Proxy Server

- Squid is a popular proxy server and web caching.
  - Many hardware-based proxy server is actually a computer with (a modified version of) squid.
- Just install `squid`
- The config file is `/etc/squid/squid.conf`.

```
visible_hostname <hostname>
acl our_networks src 192.168.0.0/24
http_access allow our_networks
```

- The service name is `squid`.
  - Try to access your proxy through the port 3128.
- May also change
  `http_port`

FTP Server

- The Very Secure FTP Daemon (vsftpd) is a good choice for anonymous FTP server.
  - Secure, lightweight, and very fast.
- The package and service name is `vsftpd`.
- The configuration file is /etc/vsftpd.conf
  - Just make sure that `anonymous_enable=YES`.
  - And do comment `local_enable=YES`.
- It's done !.

SMB/CIFS Server

- a.k.a. Windows Share
- The package is called `samba`.
- The service name is `samba`.
- To add/edit user:

```
# smbpasswd -a <username>
```

- To delete user:

```
# smbpasswd -x <username>
```

- The configuration file is `/etc/samba/smb.conf`.
  - Be careful, smb is quite complex.

(cont.)

- To share public directory for authenticated user

```
security = user
```

Then, add

```
[public]
path = /path/to/public/
public =yes
writable = no
force user = nobody
force group = nogroup
```

- To share the directory for all users, just change

```
security = share
```


(cont.)

- Let users access their home directory:

```
security = user
```

  - Then, uncomment `[homes]` section.
- You can also make it `writable`.

Secure Shell Server

- SSH obsoletes telnet, rsh, rcp, rlogin, ...
- Public key authentication
- Various algorithms for encryption
  - Blowfish, IDEA, 3DES, AES, ...
- X11 Forwarding
- TCP Redirection
- Install `openssh-server`

(cont.)

- Components:
  - `sshd` secure shell server
  - `ssh` secure shell client
  - `ssh-keygen` key generator
  - `ssh-agent/ssh-add` private-key agent
  - `scp` secure copy
  - `sftp` secure file transfer
- Try

```
ssh [user@]host [command [args]]
sftp [user@]host
scp /path/file [user@]host:[/path]
scp [user@]host:/path/file /path
```


Firewall

- `iptables` can be used to filter and manipulate packets based on rules.
  - This includes NAT.
- Table is a place to match packets
- Chain is a set of rules to match packets and send to specified target.
  - `FILTER` (default)
    - `INPUT, FORWARD, OUTPUT`
  - `NAT`
    - `PREROUTING, OUTPUT, POSTROUTING`
  - `MANGLE`
    - `INPUT, FORWARD, POSTROUTING`

(cont.)

- Target
  - `ACCEPT` accept matched packets
  - `DROP` drop matched packets
  - `LOG` syslog and continue
  - `REJECT` drop + error message
  - `DNAT` destination NAT
  - `SNAT` source NAT
  - `MASQUERADE` SNAT with the firewall's IP address

(cont.)

- Basic matching
  - Match source address
    `-s <IP address>`
  - Match destination address
    `-d <IP address>`
  - Protocol
    `-p <icmp | tcp | udp | all>`
- Extension
  - ICMP
    `--icmp-type <message type>`
  - TCP/UDP
    `--sport <port | start-port:end-port>`
    `--dport <port | start-port:end-port>`

(cont.)

- Set default policy
  `# iptables --policy <chain> <target>`
- Show current rules
  `# iptables -L`
- Add a new rule
  `# iptables -A <chain> <rule> -j <target>`
- Delete a rule
  `# iptables -A <chain> <rule> -j <target>`

(cont.)

- Example

```
# iptables --policy INPUT DROP
# iptables -A INPUT -s 192.168.0.0/24
   -j DROP
# iptables -A INPUT -i lo -j DROP
# iptables -A INPUT -s 10.0.0.0/8 -p udp
   -j DROP
```


(cont.)

- A simple NAT

```
# iptables -t NAT -A POSTROUTING -o eth0
   -j MASQUERADE
# echo 1 > /proc/sys/net/ipv4/ip_forward
# iptables -A INPUT -i eth0 -m state
   --state NEW,ESTABLISHED,INVALID -j DROP
# iptables -A FORWARD -i eth0 -m state
   --state NEW,ESTABLISHED,INVALID -j DROP
```