

# SOI Asia Server Installation

0011

Patcharee Basu(YOO)<yoo@soi.ne.jp>

SOI Asia Workshop 2004

ITB, Indonesia

AIT, Thailand

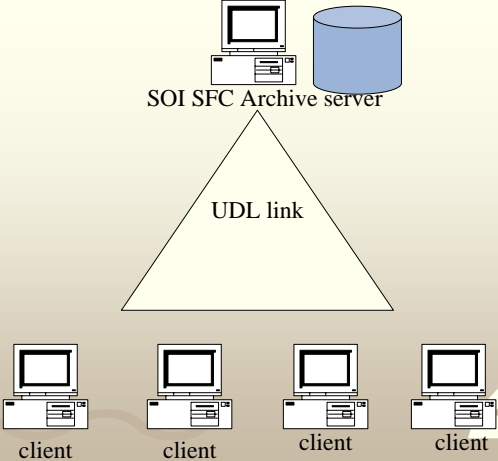
# Server Purposes

0011

- Basic Internet Services
  - DHCP,DNS,FTP,WWW,SMTP, Web cache
- SOI Asia Archive Lecture Mirror
  - WWW,Real Server, MTM<Multicast Tree Mirroring>

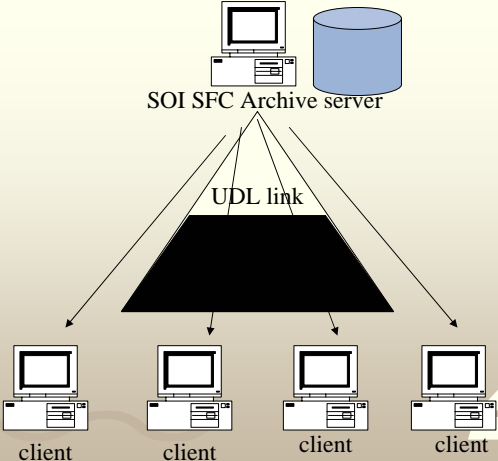
# Lecture Mirroring

0011

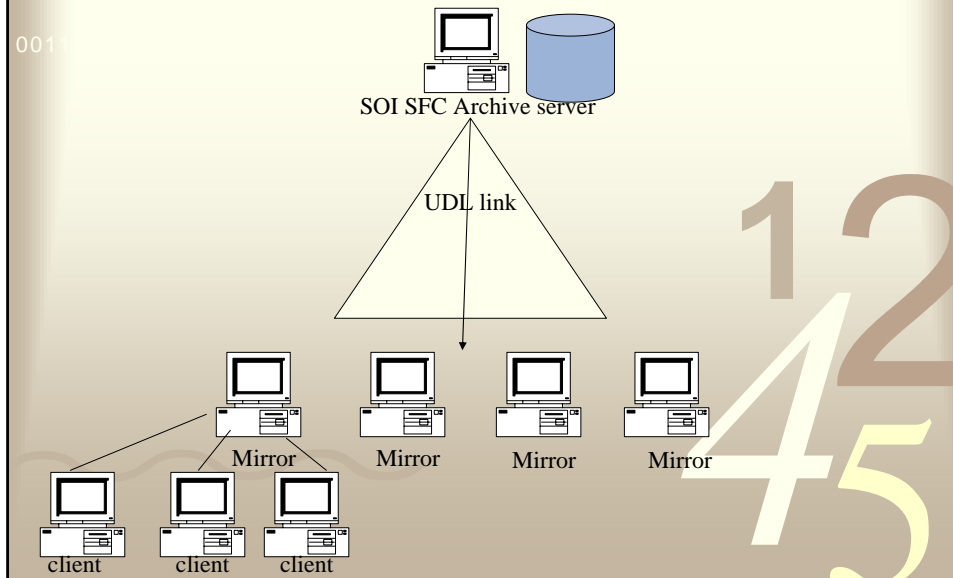


# Lecture Mirroring

0011



## Lecture Mirroring



## Operating System

- 0011
- Fedora Core 1
    - <http://fedora.redhat.com/>
    - Red-Hat-sponsored and community-supported open source project.
- The background features a large, stylized number '4' and '5' in yellow and brown, and the binary code '0011' in the top left corner.

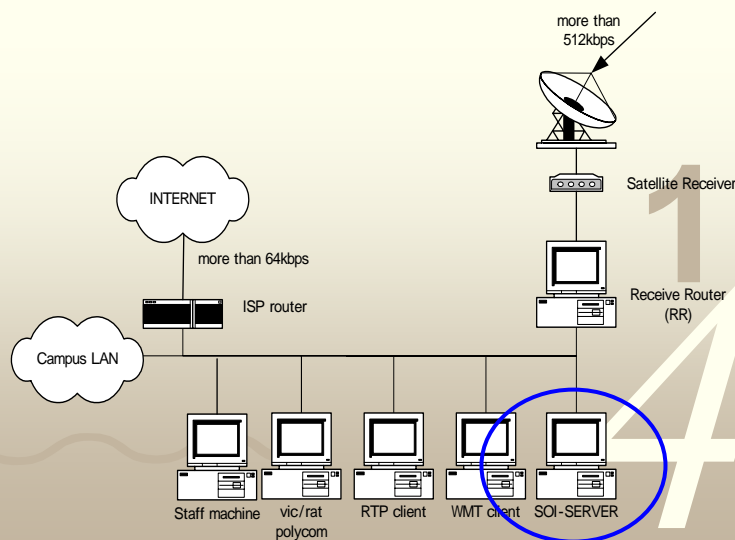
# STEP 1 Fedora Core1 Installation

0011

12  
45

## SOI Asia network topology

0011



# IP/Hostname Convention

- IP Assignment

Example, Given 202.249.26.0/255.255.255.248

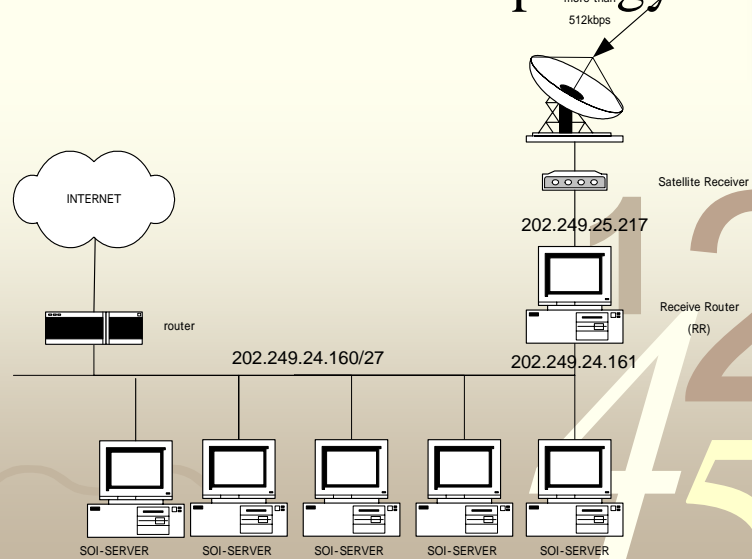
- RR = first IP number <202.249.26.1>
- SOI server = second IP number <202.249.26.2>
- Realtime lecture machines = other remaining IPs

- Hostname

<sitename>-soi.ai3.net

- example, sfc-soi.ai3.net

# Classroom network topology



# Classroom Network Configuration

## General Network Configuration

Subnet : 202.249.24.160/255.255.255.224  
RR : 202.249.24.161  
DNS : 202.249.24.18

## IP for SOI servers

## Note

- Mapping IP address written in text book to the classroom network

	Textbook	Classroom
Subnet	202.249.26.0	202.249.24.160
Netmask	255.255.255.248	255.255.255.224
RR	202.249.26.1	202.249.24.161
SOI server	202.249.26.2	Your machine IP
DNS	202.249.24.18	202.249.24.18

# Fedora Installation

0011

- For disk partitioning part, do not follow the textbook.

12  
45

## STEP 2 Explanation

0011

12  
45

## STEP 2

0011

- Test network reachability
- Turn off unused services  
chkconfig service\_name <on,off>
- Limit access to your SOI server  
/etc/hosts.allow  
/etc/hosts.deny
- Configuration for private IP <SKIP>

1 2  
4 5

## STEP 3 Explanation

0011

1 2  
4 5

## STEP 3

0011

- Existing Kernel does not support full functionalities of IPv6
- Abazh<UNIBRAW> helps make a custom kernel
  - Fedora kernel + USAGI <Linux IPv6 patch>

1 2  
4 5

## STEP 4 Explanation

0011

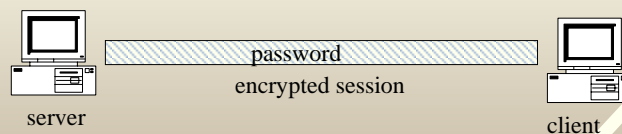
1 2  
4 5

## Security for Remote Login

- TELNET
  - Plain text password, unencrypted session
  - Do not use
- SSH
  - Encrypted session
  - 2 authentication options
    - Password Authentication
    - Key authentication<Recommended>

## SSH Password Authentication

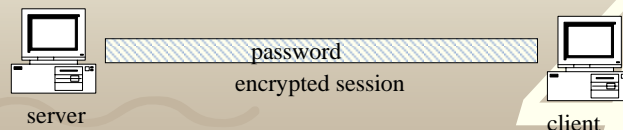
- Encrypted session
- Password is sent on the network



## SSH Password Authentication

0011

- If the server is hacked, intruder knows user's password
- It can use this password to break in other machines
- Even worse, if it gets root password



## SSH Key Authentication

0011

- Encrypted Session
- Password is not sent on the network
- User has a pair of keys
  - Public key : distribute to others
  - Private key: keep secretly
- Point
  - A message encrypted with public key can be decrypted only by private key.

## SSH Key Authentication

0011

1. Server has public key
2. Client has private key
3. Server random a message “hello” and encrypted with the public key
4. Server sends the encrypted message to client
5. Client decrypts it with private key and get “hello”
6. Client sends “hello” back to server
7. Server knows that this is the correct user



Neither password nor key is sent on the network !!

## SSH Operation

0011

1. Always upgrade Openssh/Openssl packages on your server to the most up-to-date version.
2. configuration
  - No Password authentication
  - No Root Login
  - No Empty password

Follow (STEP 4) instructions

## STEP 5 Explanation

0011

1 2  
4 5

### Package/Distribution Management

0011

- Packages/Distribution are changing with time
  - Old packages have security vulnerability
  - Old packages have less functionalities
- Big jobs for Administrator to keep system up-to-date

1 2  
4 5

# Package/Distribution Management

0011

## Repository Server

- Keeps up-to-date packages for public access
  - Index of packages <package list>
  - Packages
- Fedora repository server

## Fedora Machine

- Automatic package management programs
  - apt-get : used in SOI Asia
  - yum : you may want to try ☺

# APT-GET

0011

- Specify Source with specified for mat

/etc/apt/sources.list : input manually

/etc/apt/sources.list.d/mirror-select.list : input automatically

- Operations

apt-get update : Download package lists.

apt-get upgrade : Update all packages currently installed on your server

apt-get install <package(s)> : install/upgrade specific packages and its dependencies

apt-get mirror-select : Choose repositories and mirrors for use with apt

apt-cache search <word> : Search all known packages entries for *word*.

apt-cache show <package> : Show basic information about a package.

## STEP 5

0011

```
# cd /usr/local/src
# rpm -ivh apt-0.5.15cnc6-0.fdr.11.2.i386.rpm
# vi /etc/apt/sources.list
rpm http://202.249.24.190/fedora fedora/1/i386 os updates
rpm-src http://202.249.24.190/fedora fedora/1/i386 os updates
# apt-get update
# apt-get upgrade
```

## STEP 6 Explanation

0011

## SSH Generating key pairs

Procedure to allow a user to do a remote login

- User create a key pair
- User sends the public key to servers' administrator
- Administrator put the public key to /home/user/.ssh/authorized\_key
- Administrator informs user that you can login
- User can login server successfully

## SSH Key Authentication Procedure

Generating Key pair

<http://sfc-cpu.ai3.net/~kotaro/ai3/soi-asia/20040510/>

I have prepared a public key for testing

<http://202.249.24.190/fedora/identity.pub>

TA verifies by using following information to login

private key: <http://202.249.24.190/fedora/identity>

passphrase: soiasia

Follow instructions on STEP6 to add a user for your TA

## Services Installation

- DNS
- SMTP
- DHCP
- File Transfer Service using SSH
- WWW
- Web cache

## STEP 1 Explanation

# DNS

0011

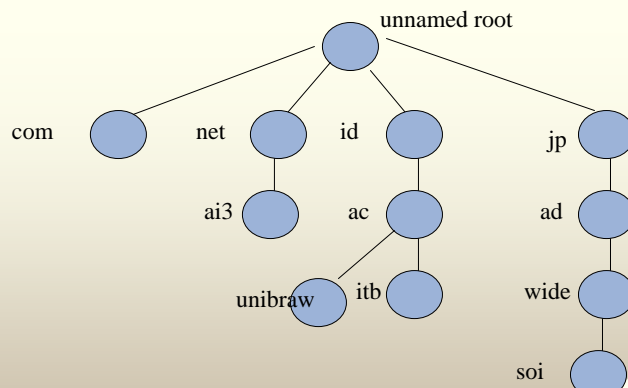
## DNS - Domain Name System

- A system to translates domain names into IP addresses
- Domain name(Alphabetic) is easier to remember than IP(32 bits)



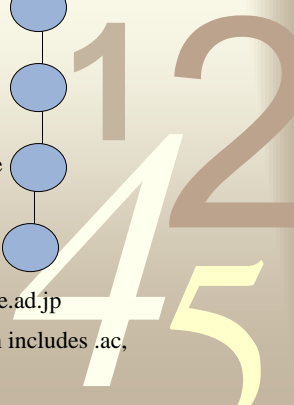
## DNS Name Space

0011

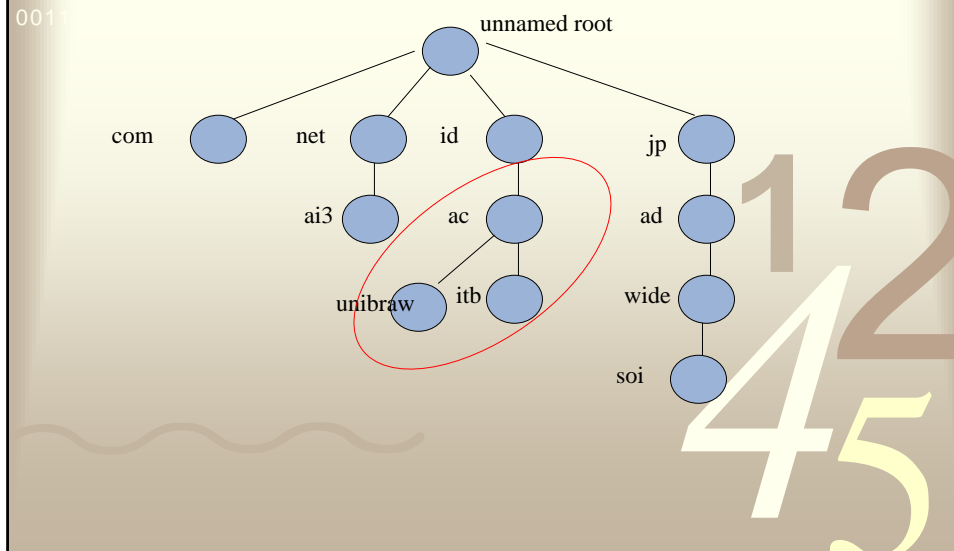


Domain name is read from the node itself upto the root : soi.wide.ad.jp

Domain is everything(every names) below that node: .ac domain includes .ac, .unibraw.ac, .itb.ac



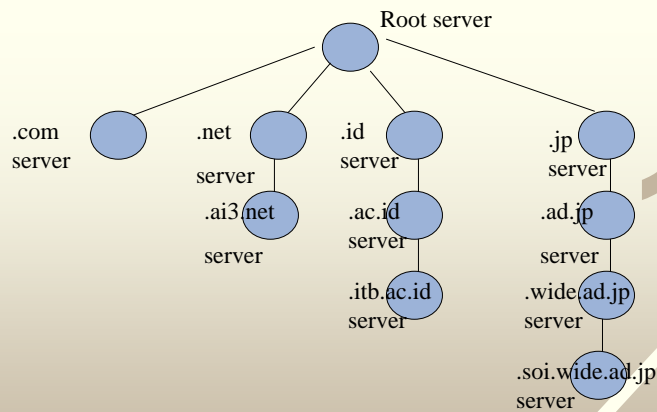
# Domain



# Delegation

- ICANN < Internet Corporation For Assigned Names and Numbers> takes care assignment of top level domain name.
- A delegate is chosen to take care of a domain name.
- Delegate can create subdomains to group hosts
- Delegate of a domain can give responsibility for managing a subdomain to someone else
- The parent domain retains links to the delegated subdomain

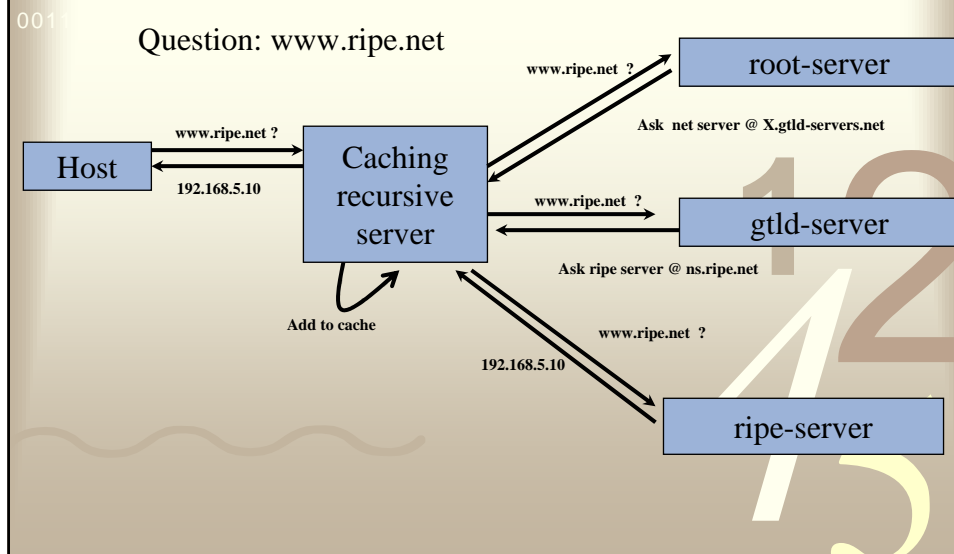
## DNS Authoritative Servers



## DNS Server

- 0011
- Name servers answer 'DNS' questions.
  - UDP Port 53
  - Two main types of DNS server
    - Authoritative server
      - Take care of a domain
        1. Keep records of Name -> IP
        2. Keep links to servers of subdomains
    - (Caching) recursive server
      - Do not have a domain
      - Do the name resolve
- 1 2  
4 5

## Resolving process



## SOI Asia DNS

- 0011
- Caching Only Name Server
  - Bind 9
  - Chrooted
    - improve security
    - Limit directory access to the daemonIt sees `</var/named/chroot >` as `</>`

## SOI Asia DNS

0011

### Configuration

- Work only for our clients

```
options {  
  allow-query { 202.249.24.160/27; localhost; };  
  allow-recursion { 202.249.24.160/27; localhost; };  
  allow-transfer { none;};  
};
```

- Follow instructions

## Command

0011

1. `service service_name <start, stop, restart>`

Turn on/Turn off or restart the service\_name

2. `chkconfig service_name <on, off>`

Turn on/off the service at system bootup

## STEP 2 Explanation

0011

1 2  
4 5

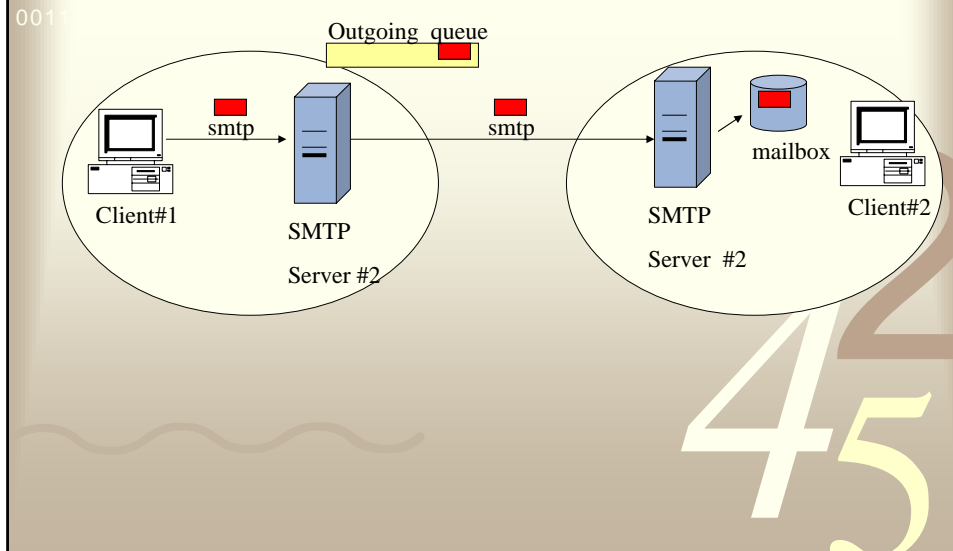
## SMTP

0011

- Simple Mail Transfer Protocol
- sending e-mail messages between two end systems
- client-server architecture
- Server: TCP port 25

1 2  
4 5

# SMTP



# SOI Asia SMTP

- 0011
- Postfix (default is sendmail)
    - Easier configuration
  - Chrooted
  - Follow the instructions
- The background features a large, faint watermark of the numbers '12' and '45'.

## STEP 3 Explanation

0011

1 2  
4 5

## DHCP

0011

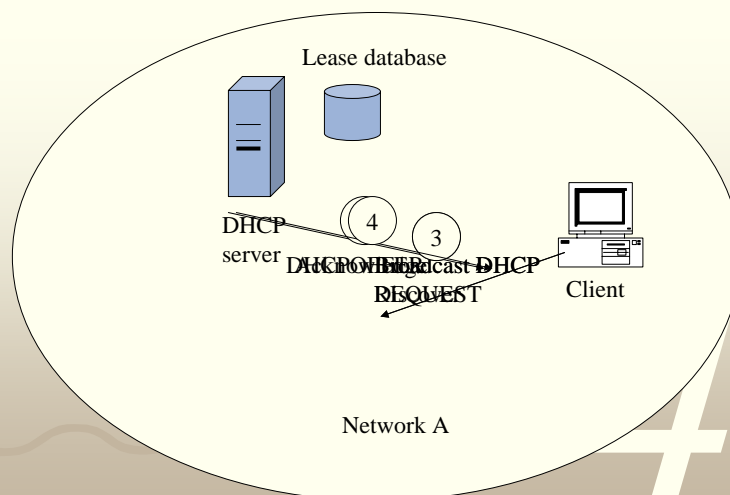
- **Dynamic Host Configuration Protocol**
  - enable individual computers on an IP network to extract their configurations from a server  
IP, netmask, domain, default route
- **Motivation**
  - reduce the work necessary to administer
  - Temporary clients shares limited number of IP addresses

1 2  
4 5

# DHCP

- DHCP server
  - Keep pool of IP address
  - When requested, lease a network configuration for a specific period<lease time>
  - Keep tracks of currently used IP
  - Network parameters are all set by administrator

## DHCP Lease Mechanism



## DHCP Lease Renewal

0011

Clients do renewal lease

- Every 50% of the lease time  
Attempt to renew the lease
- 50% or more passed  
Attempt to renew the lease
- At 87.5% - lease expires  
Do a new lease



## DHCP Configuration

0011

default-lease-time : lease time server gives to client

maximum-lease-time: limitation of client's lease time request

range : pool of IPs to be dynamically assign

others: network information

Follow instructions



## STEP 4 Explanation

0011

12  
45

## SCP

0011

- SCP <secure copy>
  - Includes in SSH suites
  - No additional Installation

12  
45



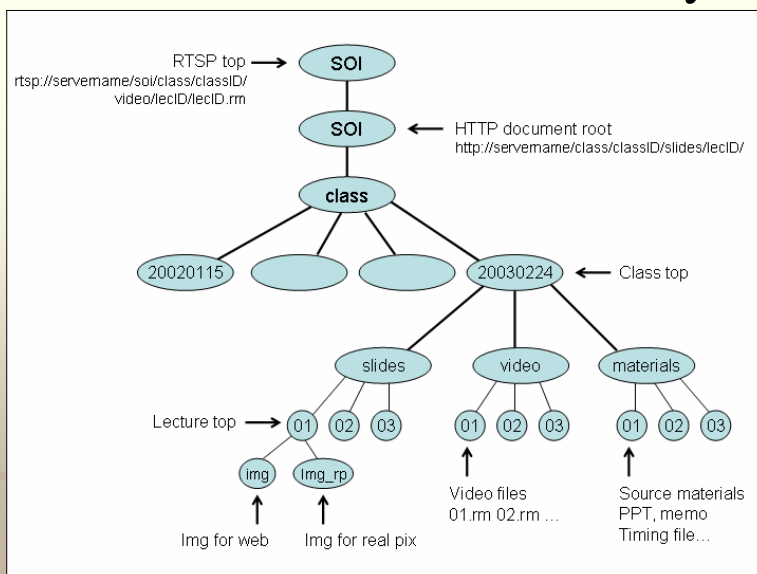
# STEP 5 Explanation

0011



## SOI Asia Archive Directory

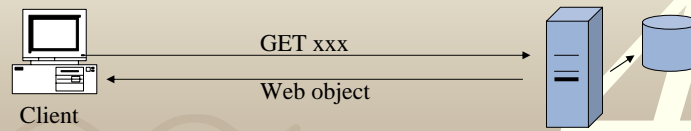
0011



## WWW Service

0011

- Apache
- HTTP protocol
- TCP port 80



## STEP 5

0011

- Create a HTTP root directory</soi/soi>
- Configure HTTPD to recognize the root directory
- Follow instructions

## STEP 6 Explanation

0011



## Web cache

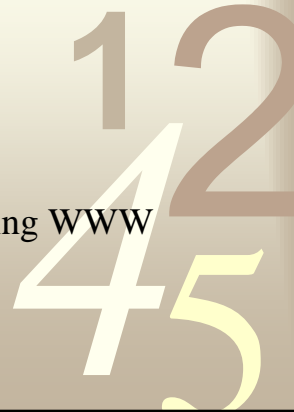
0011

### Motivation

- Rapid growth of WWW usage
- Limitation of bandwidth

### Concept

- Keeps web objects closer to users
- User shares same interests in accessing WWW
- Reduce bandwidth usage
- Improve access time



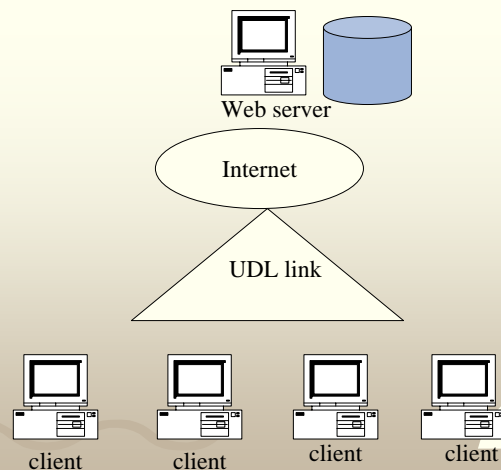
## Web cache mechanism

0011

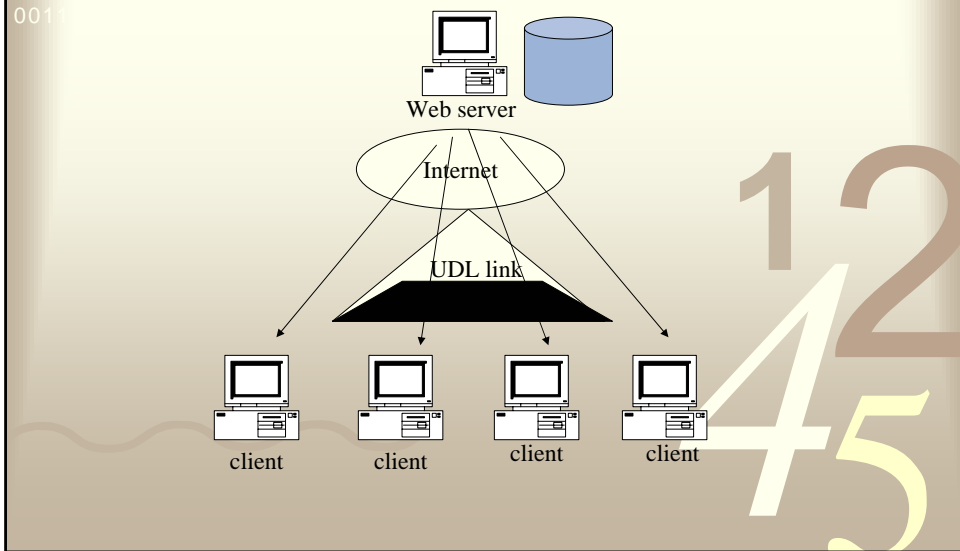
- Intermediate entity between HTTP client and HTTP server
- HTTP client sends HTTP request to a web cache instead of HTTP server
- Web cache checks if the required URL is in local storage or not
- If yes<cache hit>, send this local object to client
- If no<cache miss>, get object on HTTP server and keep it in local disk

## HTTP model

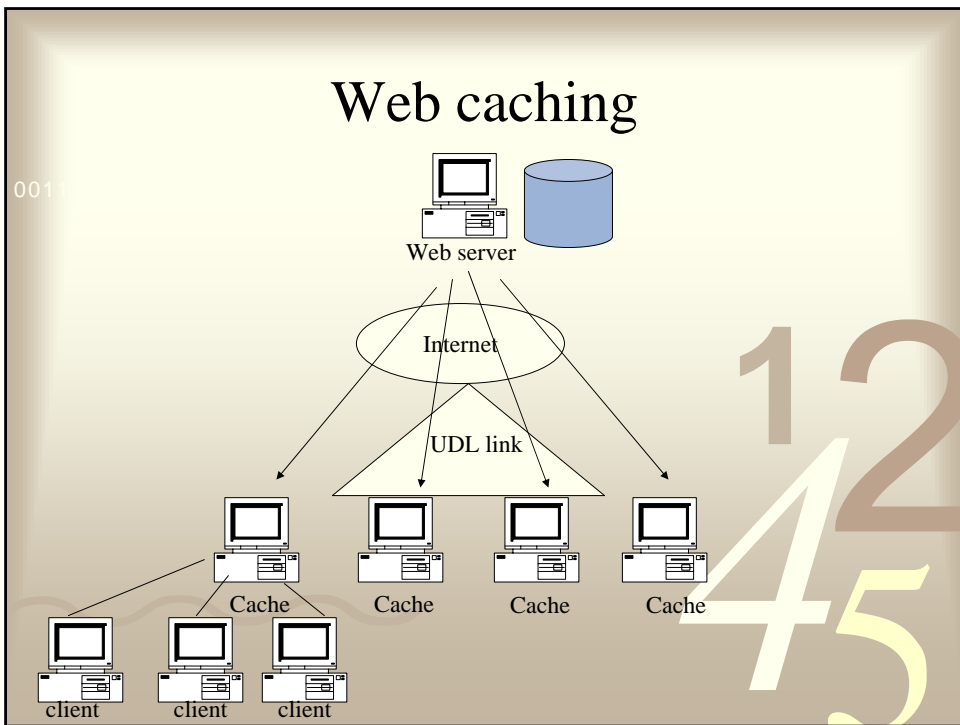
0011



# HTTP model



# Web caching



## Cache Peering

- Sharing content between caches
- ICP <Internet Cache Protocol>
  - Objects query between caches
  - Not object transfer
- 2 relationships
  - Parent
    - give local object or get from web server for child
  - Sibling
    - give local object but won't help get it from web server

## Cache Peering

### Parent-Child

- Parent to me is closed
- Parent to Internet is closer than I go to Internet
- Normally in hierarchy network

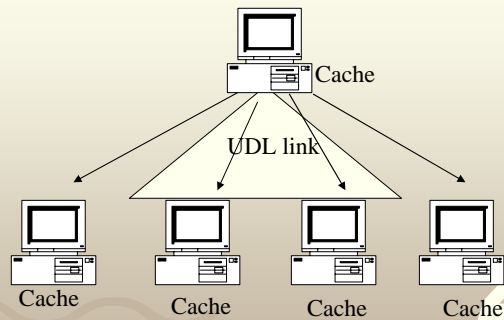
### Sibling

- Sibling to me is close
- Sibling to Internet is same or worse than I go by myself.

## SOI Asia Cache peering

0011

Parent cache: sfc-cache.ai3.net



## SOI Asia Cache peering

0011

### Advantages

- Sharing cache contents with other partners
- Good access time if hit
- Not so different access time if miss, because satellite delay is dominant
  - Hit : satellite delay
  - Miss : satellite delay + relative small Internet delay + small cache processing time
  - Not using : satellite delay + relative small Internet delay

## SOI Asia Cache peering

0011

### Disadvantages

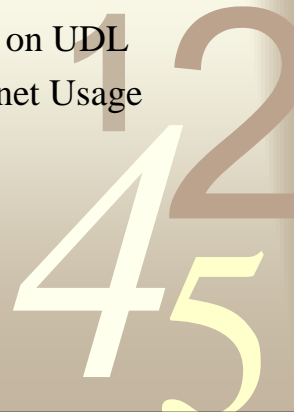
- Longer delay going to ID sites through UDL



## SOI Asia Cache Structure

0011

- Partner setups a web cache on SOI server
- Ask all HTTP clients to use web cache
- Together helps reduce bandwidth on UDL
- Parent Peering : depends on Internet Usage



## SOI Asia Web Cache

- Squid web cache software
- Configuration
  - Peer setting
  - Maximum web object size
  - Cache directory size
  - ftp\_user
  - Allow http access from local site only
  - Not allow ICP access
  - Information of cache manager

## Squid logfile

- All requests are logged in  
/var/log/squid/access.log
- Log rotation
  - backup current log file to new name  
<access.log.number>
  - empty current log

## SOI Asia

### Squid logfile management/analyze

- Rotate log every day at midnight
- Keep up to 10 logs
- Squid-graph script
  - Parsing access.log
  - Web/Image report of usage
  - Run every hour

## CRON

- Daemon to execute scheduled commands
- To edit schedule

```
#crontab -e
```
- Command format

```
Minute hour day month year command_to_be_execute
```
- Example

```
0 0 * * * /usr/sbin/squid -k rotate
1 * * * * /usr/local/src/squid-graph-3.1/bin/ squid-graph --
output-dir=/soi/soi/squid < /var/log/squid/access.log
```

## SOI Asia Archive Content(1)

- HTML pages
- Image files

## STEP 6

- Follow instructions to install squid and squid analyzer

## SOI Asia Archive Lecture Installation

0011

1 2  
4 5

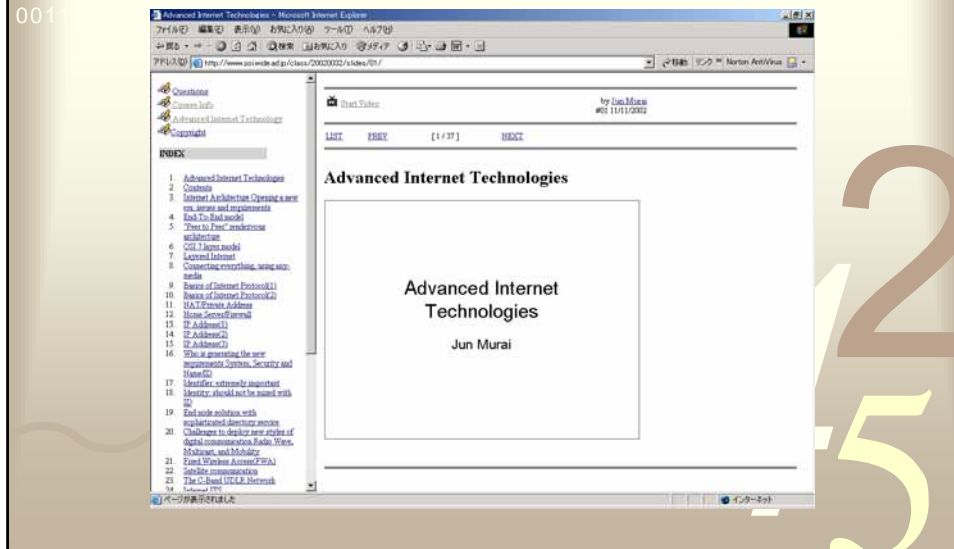
## SOI Asia Archive Content

0011

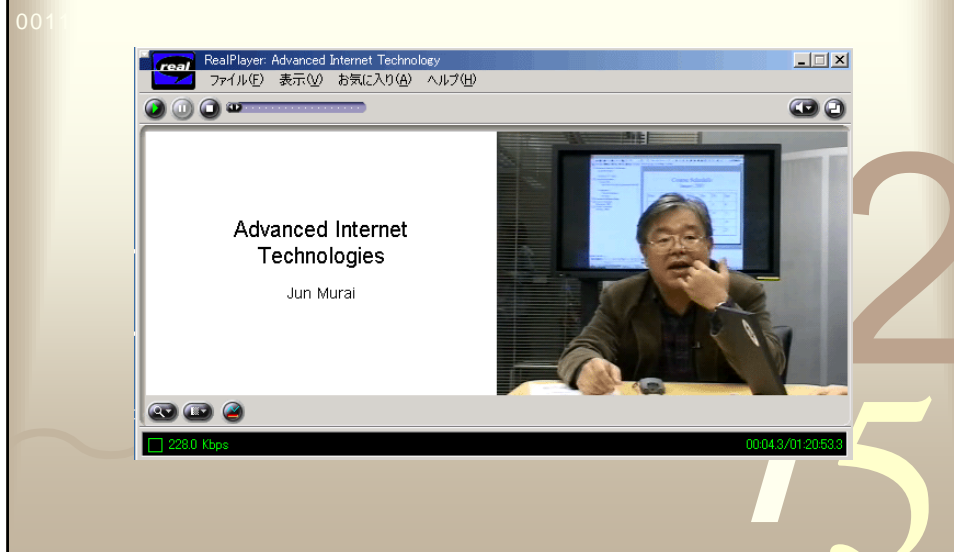
- (1) Web-style Presentation slides
- (2) Lecturer's video synchronized with slides

1 2  
4 5

## SOI Asia Archive Content(1)



## SOI Asia Archive Content(2)

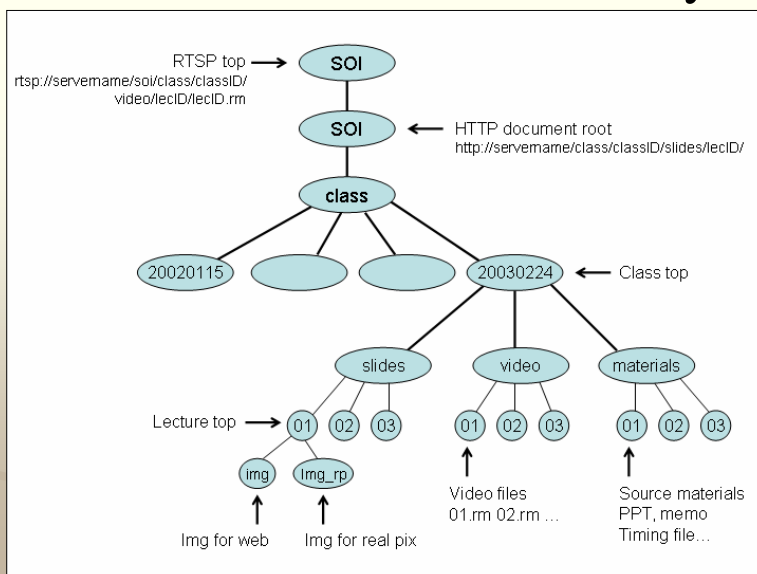


# SOI Asia Archive Content

- HTML pages
- Image files
- Real video
- Synchronizing script



# SOI Asia Archive Directory



## Real Streaming Server

### Installation Steps

1. Get a free license from Real networks  
/usr/local/src/rmsserver.lic
2. Install the program

#chkconfig rmsserver on

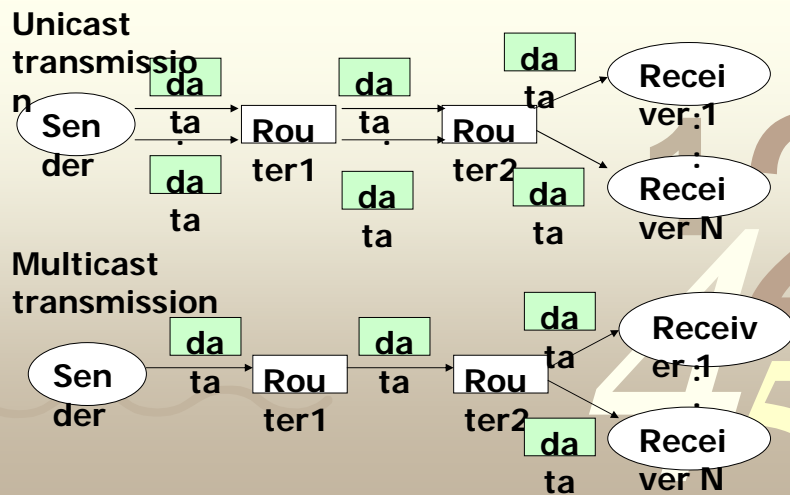
## Multicast Tree Mirroring(MTM)

- Developed by SOI Asia project
- Distribution of a directory tree or a file
- SOI master mirror - > partners' mirrors
- Reliable Multicast Transport Protocol<RMUS from AIT>
- Command execution at remote host
- Sync by checking modified time
- IPv6 in the future

# MTM

- Class materials distribution
  - PPT, PDF, PS, WORD
- Archive lecture distribution
  - HTML pages, images, video

# Multicast



## Multicast

0011

- Bandwidth Optimization
- Based on UDP
- Unreliable



## MTM Sender

0011

### Stateful entity

- given list of receivers ,a directory root and a command to be executed at the end of transfer.
  - create a job file
- ```
File1 rcv1[status],rcv2[status],rcv3[status]
File2 rcv1[status],rcv2[status],rcv3[status]
File3 rcv1[status],rcv2[status],rcv3[status]
```
- Trace the job file and send each file to all receivers
  - Write status of receiving into job file
  - Repeat transmission until finish
  - Execute a command at receiver'
  - Tell a receiver to write a complete transfer in a log file



## MTM Receiver

0011

### Stateless entity

- Receive a file if it is a more up-to-date file
- File timestamp/mode is the same as sender machine
- Execute command on sender's order
- Write a log file on sender's order

1 2  
4 5

## MTM Installation

0011

- Follow instructions

1 2  
4 5

## MTM Configuration

- MTM\_MULTICAST\_ADDRESS=224.224.224.1
- MTM\_MULTICAST\_PORT=49999
- CMD\_RUN\_PASSWORD=SOI-seCREt
- RUN\_DIR=/usr/local/mtm/run/
- LOG\_DIR=/usr/local/mtm/log/
- TMP\_DIR=/tmp/mtm

- Everyone tells me the IP address of server
- Wait until all are ready to receive
- I will send a html page and a video file

## **SOI Asia procedure to receive class materials and archive lectures of a course**

0011

## **Archive Courses 2004**

0011

- I) **Advanced Internet Technology-II: Internet  
Operation , Sep - Dec, 2004**  
size : 6 G
- II) **Advanced Topics for Fisheries and Marine  
Science III , Sep - Oct, 2004**  
size : 7 G
- III) **Tohoku University Biotechnology Lecture  
Series I , Jan - Mar, 2005**  
size : 8 G

