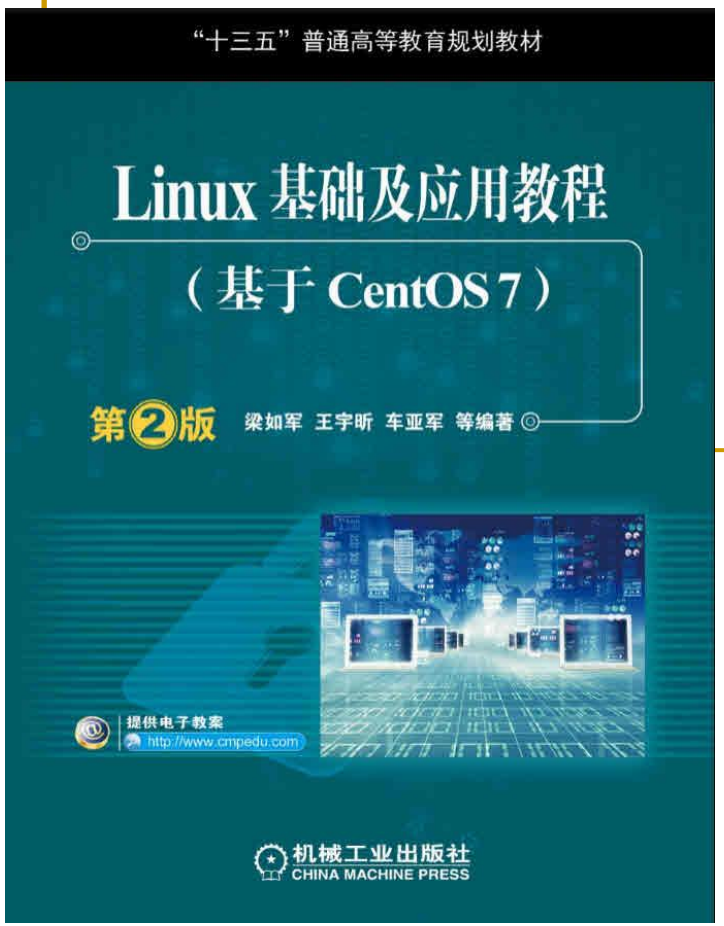


第11章 DHCP和DNS服务

主讲人： 梁如军

2015-05-05

本章内容要点

- DHCP协议
- DHCP服务
- DNS的相关概念
- DNS服务工作原理
- BIND的安装和启动
- BIND的配置语法
- 配置常用的域名服务器
- BIND的测试及工具
- DNS客户端的配置

梁如军（linuxbooks@126.com）

本章学习目标

- 熟悉DHCP协议、掌握DHCP工作过程
- 学会配置DHCP服务器及中继代理
- 了解大型网络中DHCP服务部署
- 理解DNS的相关概念和工作原理
- 熟悉DNS查询方式和域名解析过程
- 掌握BIND的安装、启动和配置语法
- 掌握常用域名服务配置
- 掌握BIND的测试工具的使用

梁如军（linuxbooks@126.com）

DHCP服务

梁如军（linuxbooks@126.com）

DHCP的概念和工作过程

- 为主机或设备分配IP地址的方法
- DHCP 协议简介
- DHCP的运行机制
- DHCP的相关概念
- DHCP的工作过程

梁如军（linuxbooks@126.com）

DHCP简介

- **DHCP**（Dynamic Host Configuration Protocol）动态主机配置协议是TCP / IP协议簇中的一种
- DHCP 是由因特网工程任务组（IETF）设计的，详尽的协议内容参考 **RFC2131** 和 **RFC1541**
- DHCP 协议主要是用来自动为局域网中的客户机器分配 TCP/IP 信息的网络协议，并完成每台客户机的 TCP/IP 协议配置
  - TCP/IP 信息包括 IP地址、子网掩码、网关，以及DNS服务器等。
- DHCP 的前身是 BOOTP（引导协议），DHCP 可以说是 BOOTP 的增强版本

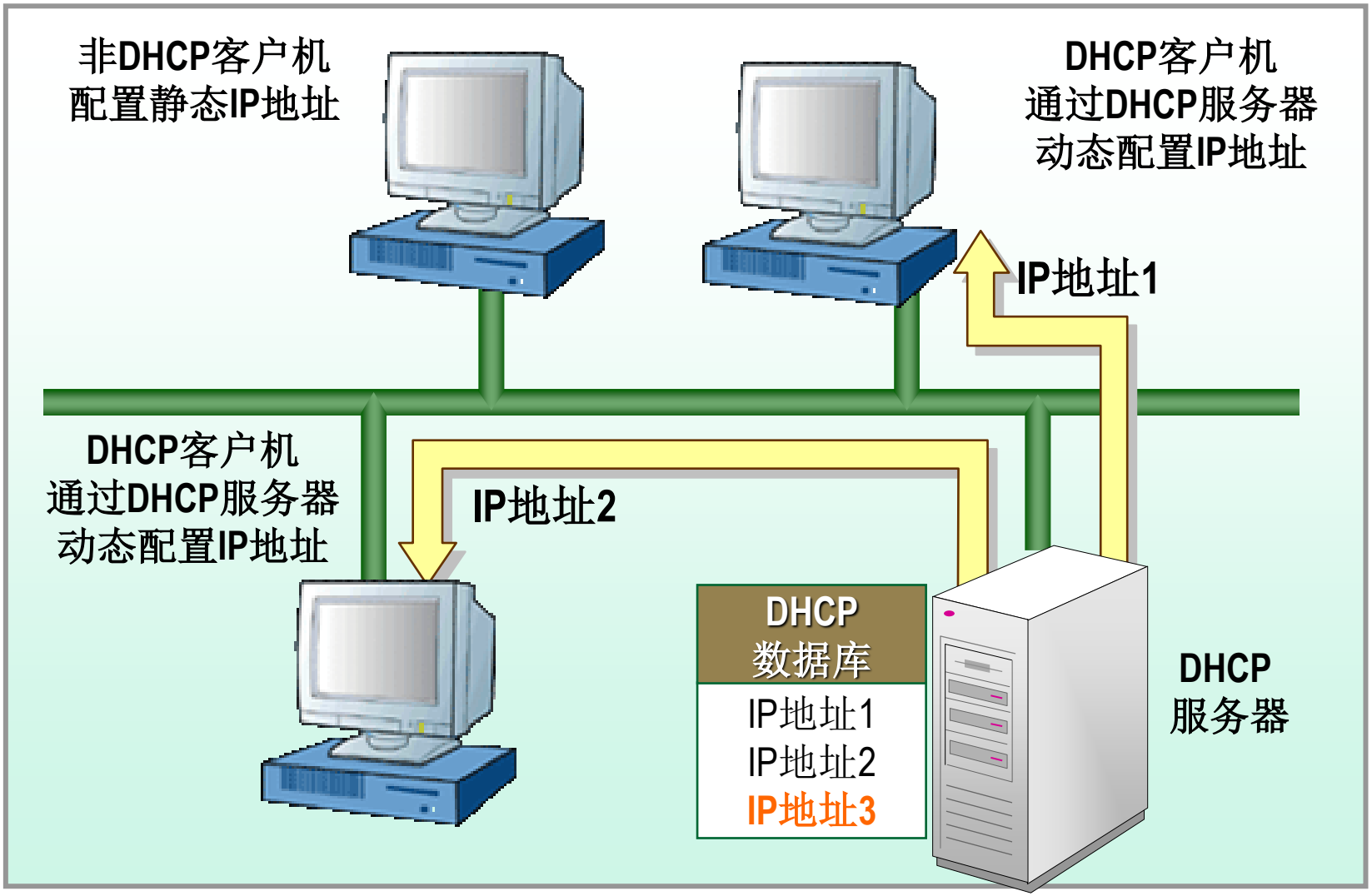
梁如军（linuxbooks@126.com）

使用DHCP的优点

- 减少管理员的工作量
- 避免IP冲突
- 减少收入错误的可能
- 能方便地更改网络的IP网段
- 移动计算机后不用重新配置网络信息
- 提高IP地址的利用率

梁如军（linuxbooks@126.com）

DHCP的运行机制



梁如军（linuxbooks@126.com）

DHCP的相关概念（1）

- DHCP客户
  - 是指一台通过DHCP服务器来获得网络配置参数的主机，通常是不同的客户机或工作站。
- DHCP服务器
  - 是指提供网络配置参数给DHCP客户的主机。
- DHCP中继代理
  - 是指在DHCP服务器和DHCP客户之间转发DHCP消息的主机或路由器。若要使用DHCP服务器支持跨越多重路由的子网，则路由器可能需要硬件升级。路由器必须支持RFC1533、RFC1534、RFC1541和RFC1542。

梁如军（linuxbooks@126.com）

DHCP的相关概念（2）

- 作用域
  - 是指一个网络中的所有可分配的 IP 地址的连续范围。作用域主要用来定义网络中单一的物理子网的 IP 地址范围。作用域是服务器用来管理分配给网络客户的 IP 地址的主要手段。
- 超级作用域
  - 是指一组作用域的集合，它用来实现同一个物理子网中包含多个逻辑 IP 子网的情况。在超级作用域中只包含一个成员作用域或子作用域的列表。然而超级作用域并不用于设置具体的范围。子作用域的各种属性需要单独设置。

梁如军（linuxbooks@126.com）

DHCP的相关概念（3）

- 排除范围
  - 是指作用域内从 DHCP 服务中排除的有限IP地址序列。排除范围确保在这些范围内的任何地址都不由 DHCP 服务器分配给 DHCP 客户机。
- 地址池
  - 定义DHCP 作用域并应用排除范围之后，剩余的地址在作用域内形成可用地址池。地址池内的地址由DHCP服务器在网络上动态指派给DHCP客户机。
- 保留
  - 指通过 DHCP 服务器的永久地址租约指派。保留确保了子网上指定的硬件设备始终可使用相同的 IP 地址。

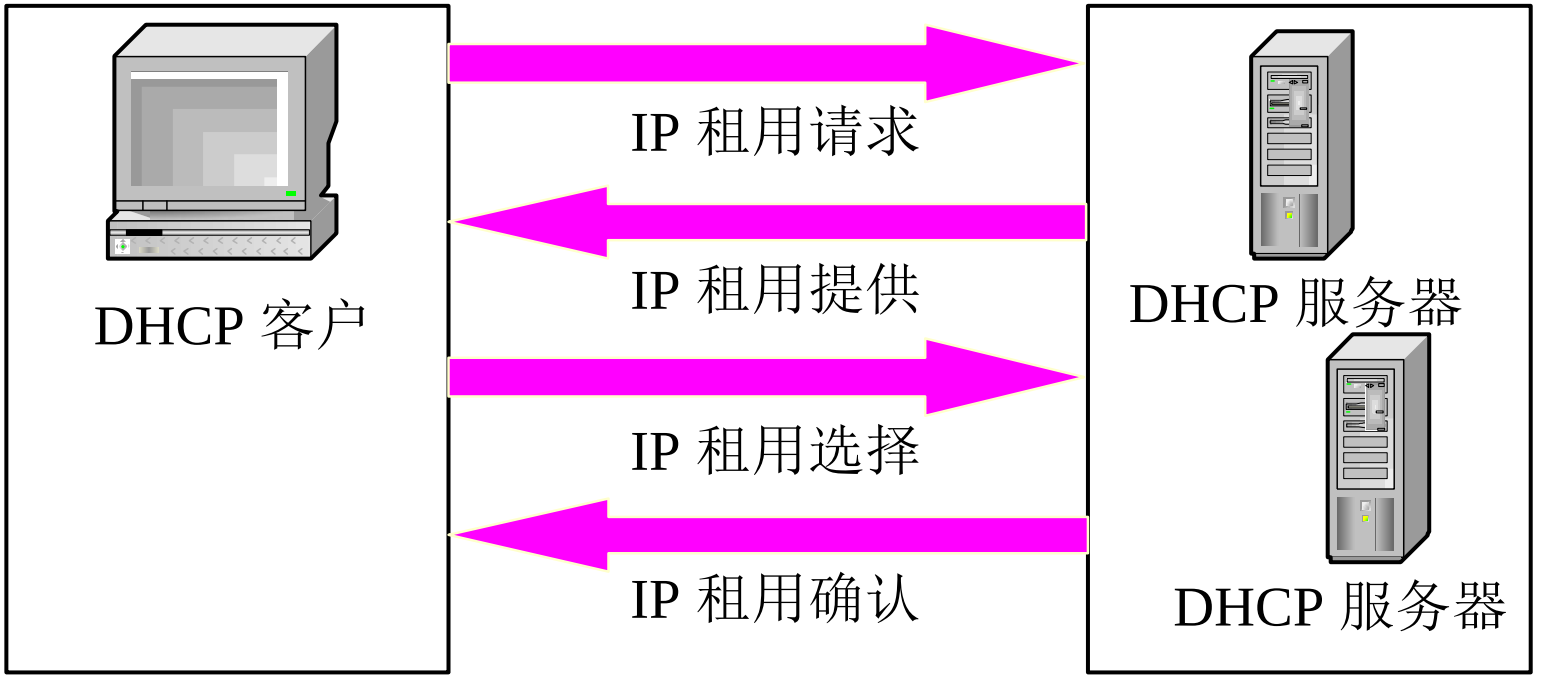
梁如军（linuxbooks@126.com）

DHCP的相关概念（4）

- 租用
  - 是指DHCP客户从DHCP服务器上获得并临时占用某IP地址的过程。
- 租约
  - 是指客户机可使用的被DHCP服务器指派的IP地址的时间长度，在这个时间范围内客户机可以使用所获得的IP 地址。
  - 当客户机获得 IP 地址时租约被激活。在租约过期之前，客户机一般需要通过服务器更新其地址租约。当租约期满或在服务器上删除时租约停止。租约期限决定租约何时期满以及客户需要用服务器更新它的次数。

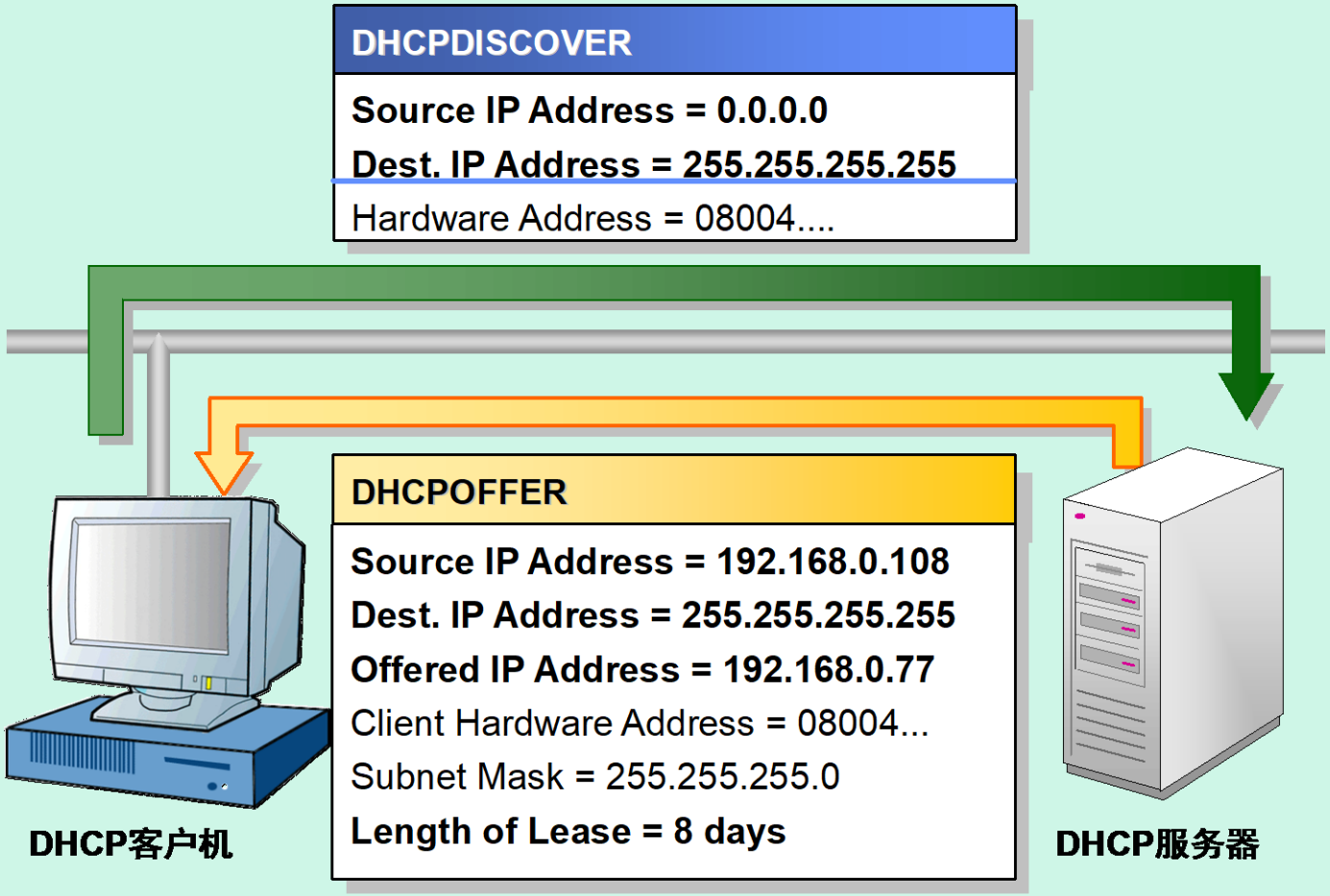
梁如军（linuxbooks@126.com）

DHCP的工作过程
——DHCP客户端首次登录网络



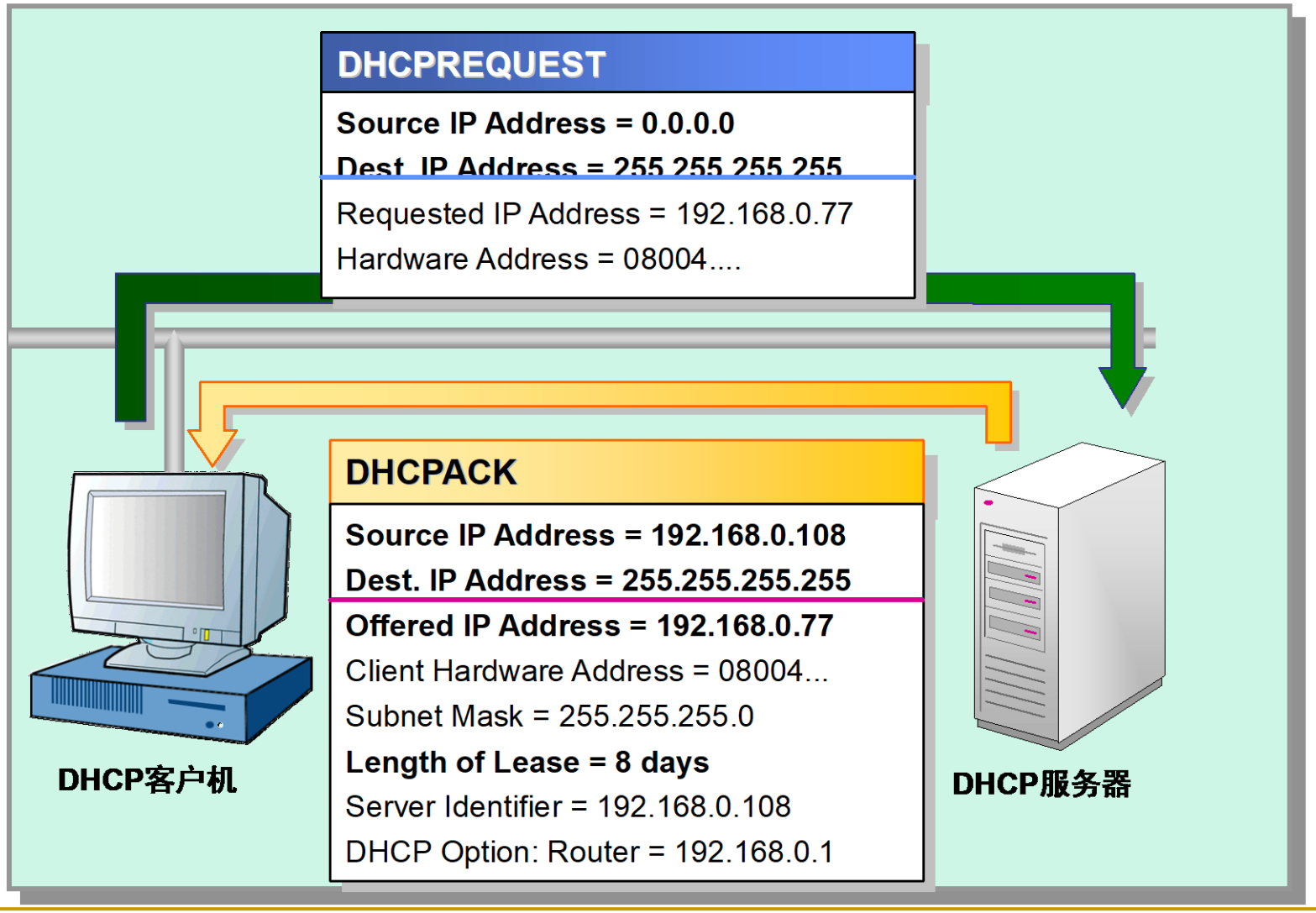
梁如军（linuxbooks@126.com）

IP租用请求和提供



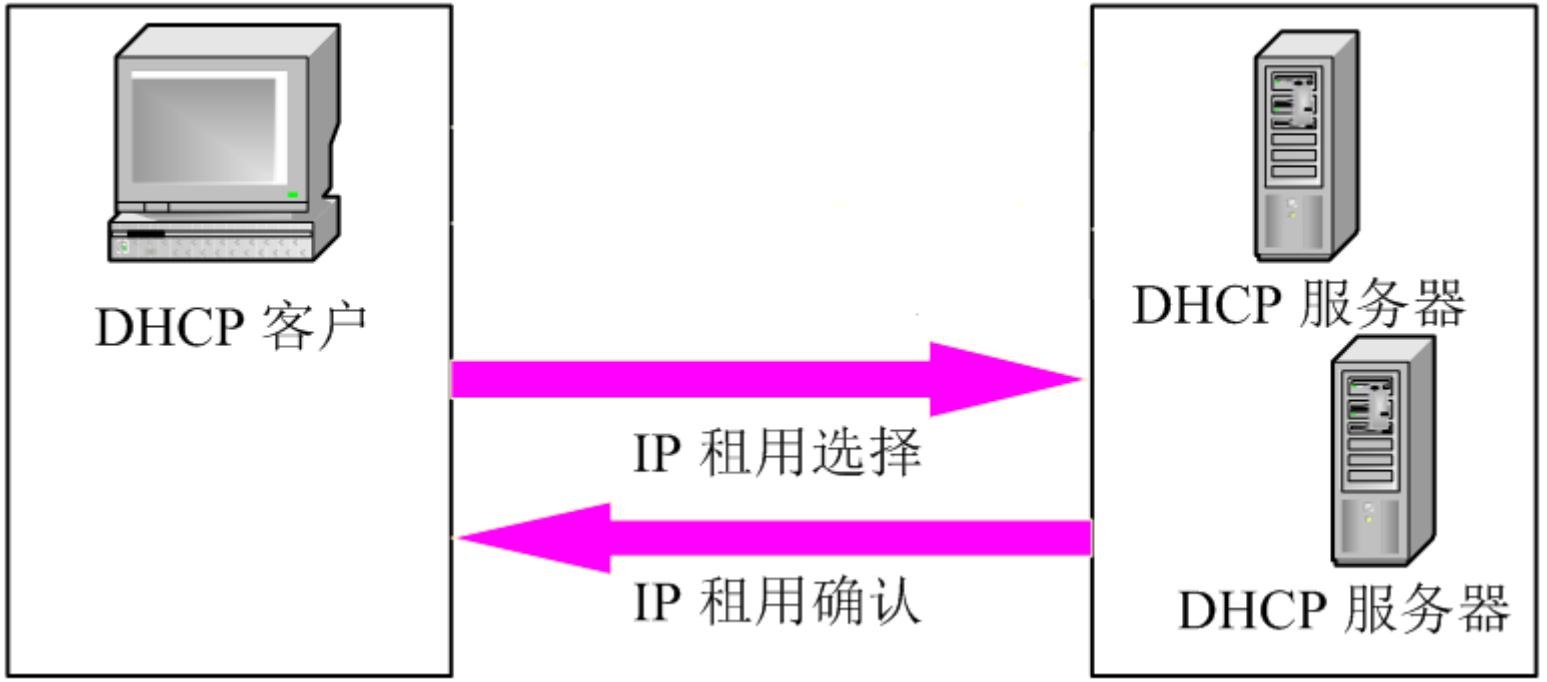
梁如军（linuxbooks@126.com）

IP选择和确认



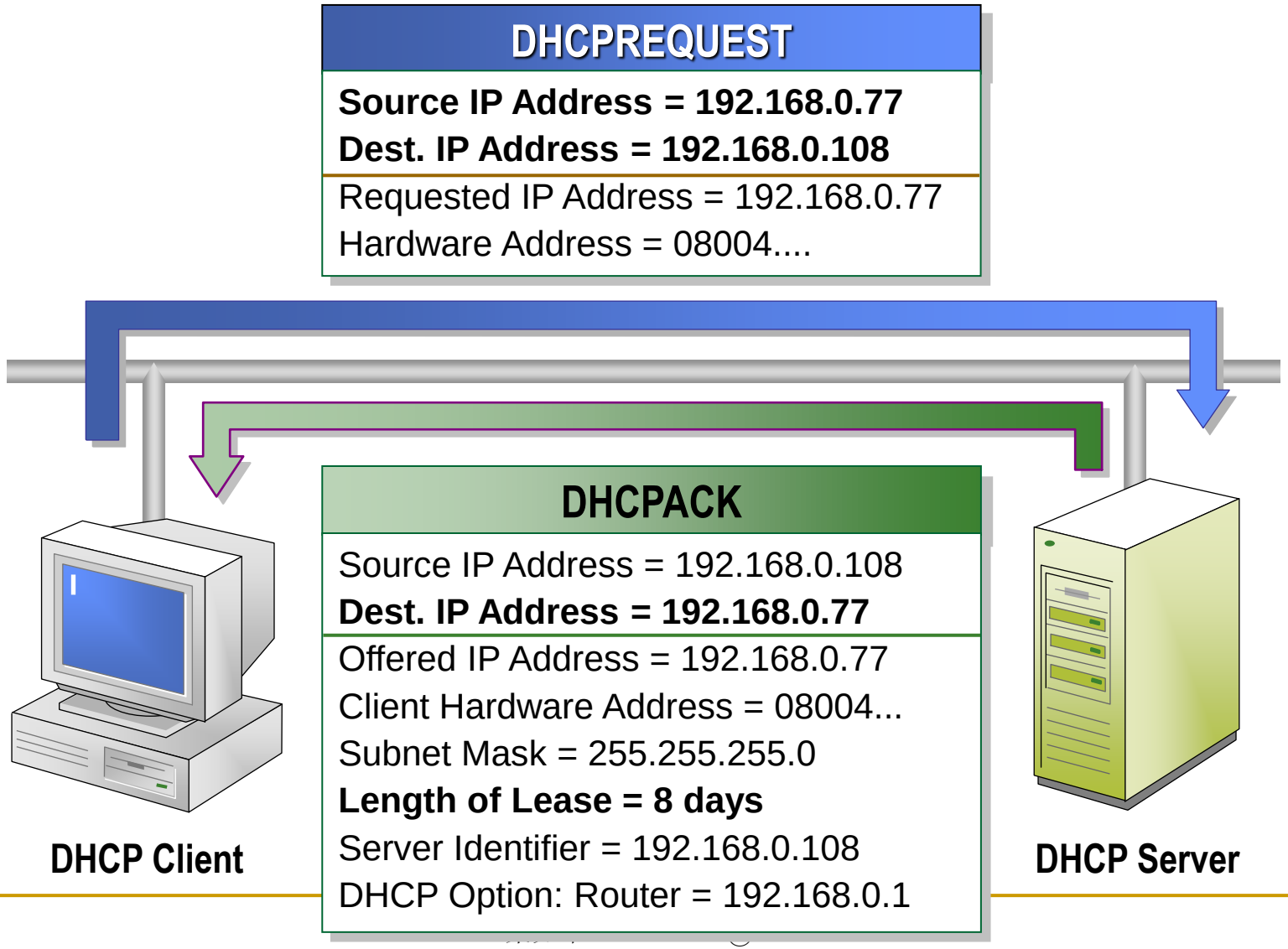
梁如军（linuxbooks@126.com）

DHCP的工作过程
——DHCP 租约的更新过程



梁如军（linuxbooks@126.com）

DHCP的续约确认



DHCP 租约的更新

- 自动更新租约
  - 客户租约期限已过去50%，自动尝试更新租约
  - 当期限过去87.5% 发出广播再次更新租约
  - 若租约已经到期(100%)，客户机必须立即停止使用当前的IP地址。然后DHCP客户机开始新的DHCP租约过程，尝试租用新的IP地址
- 手工更新租约
  - Windows： **ipconfig /renew** 和 **/release**
  - Linux：dhclient -r <interface>

梁如军（linuxbooks@126.com）

CentOS 7下的DHCP服务

- 安装和启动
- 配置文件语法
- DHCP服务配置举例
- 大型网络的DHCP部署

梁如军（linuxbooks@126.com）

DHCP 服务概览

- 软件包：dhcp
- 服务类型：由Systemd启动的守护进程
- 配置单元：/usr/lib/systemd/system/dhcpd.service
- 守护进程：/usr/sbin/dhcpd
- 端口：67（bootps）、68（bootpc）
- 配置文件：/etc/dhcpd.conf、/var/lib/dhcpd/dhcpd.leases
- 相关软件包：dhclient

梁如军（linuxbooks@126.com）

DHCP的安装和启动

- 安装

  # yum install dhcp

- 配置文件
  - /etc/dhcpd.conf （默认不存在）
  - /usr/share/doc/dhcp-*/dhcpd.conf.example （模板）
- 检查语法

  # dhcpd -t

- 启动

  # systemctl enable dhcpd.service

  # systemctl start dhcpd.service

梁如军（linuxbooks@126.com）

DHCP服务的配置文件语法

- DHCP服务的配置文件中的三类陈述
  - 声明：描述网络的布局，描述客户，提供客户的地址，或把一组参数应用到一组声明中。
  - 参数：表明如何执行任务，是否要执行任务，或将哪些网络配置选项发送给客户。
  - 选项：配置DHCP的可选参数，以option关键字开头。

梁如军（linuxbooks@126.com）

DHCP配置文件中的声明

- **shared-network**：用于告知DHCP服务器某些IP子网其实是共享同一个物理网络。
- **subnet**：用于提供足够的信息来阐明一个IP地址是否属于该子网。
- **range**：对于任何一个需要动态分配IP地址的subnet语句里，至少要有一个range语句，用于说明要分配的IP地址范围。
- **host**：为特定的DHCP客户机提供IP网络参数。
- **group**：为一组参数提供声明。

梁如军（linuxbooks@126.com）

DHCP配置文件中的参数

- **ddns-update-style**：配置DHCP-DNS 互动更新模式
- **default-lease-time**：指定默认地址租期
- **max-lease-time**：指定最长的地址租期
- **hardware**：指定硬件接口类型及硬件地址
- **fixed-address**：为DHCP客户指定IP地址
- **filename**：指定启动时载入的初始启动文件
- **next-server**：指定初始启动文件存放的主机

梁如军（linuxbooks@126.com）

DHCP配置文件中的选项

- **domain-name**：为客户指明DNS名字
- **domain-name-servers**：为客户指明DNS服务器的IP地址
- **host-name**：为客户指定主机名
- **time-offset**：为客户设置与格林威治时间的偏移时间（秒）
- **ntp-servers**：为客户设置网络时间服务器的IP地址
- **routers**：为客户设置默认网关
- **subnet-mask**：为客户设置子网掩码
- **broadcast-address**：为客户设置广播地址

梁如军（linuxbooks@126.com）

基本DHCP服务器配置举例——/etc/dhcpd.conf


```
ddns-update-style none;
ignore client-updates;
default-lease-time   18000;
max-lease-time       36000;
subnet 192.168.0.0 netmask 255.255.255.0 {
        option routers                  192.168.0.1;
        option subnet-mask              255.255.255.0;
        option domain-name              "ls-al.me";
        option domain-name-servers      192.168.0.252,192.168.0.1;
        range 192.168.1.100 192.168.1.200;
        class "pxeclients" {
            match if substring(option vendor-class-identifier, 0 , 9) = "PXEClient";
            next-server 192.168.0.252;
            filename "linux-install/pxelinux.0";
        }
        host centos2 {
           hardware ethernet 00:A0:78:8E:9E:AA;
           fixed-address 192.168.0.250;
        }
}
```

大型网络的DHCP部署

- 在有多个网络接口的服务器上实现DHCP多作用域管理
- 使用DHCP超级作用域实现多作用域管理
- 设置DHCP中继代理

梁如军（linuxbooks@126.com）

设置DHCP中继代理（1）

- 在中继代理上安装包含dhcrelay的dhcp软件包

  # yum install dhcp

- 开启内核路由转发

  # echo "net.ipv4.ip_forward=1" >> /etc/sysctl.conf

  # sysctl -p

梁如军（linuxbooks@126.com）

设置DHCP中继代理（2）

- 配置自定义的 dhcrealy.service单元配置文件

 # cp /usr/lib/systemd/system/dhcrelay.service /etc/systemd/system/

 # vi /etc/systemd/system/dhcrelay.service

将配置行ExecStart=/usr/sbin/dhcrelay -d --no-pid

修改为如下行（指定网络接口和上游DHCP服务器）

ExecStart=/usr/sbin/dhcrelay -d --no-pid –i eno16777736 192.168.0.254

 # systemctl daemon-reload

- 启动DHCP中继代理

 # systemctl enable dhcrealy.service

 # systemctl start dhcrealy.service

梁如军（linuxbooks@126.com）

DHCP客户端配置

- Windows的DHCP客户端配置
- Linux的DHCP客户端配置

梁如军（linuxbooks@126.com）

DNS相关概念

梁如军（linuxbooks@126.com）

IP地址和主机名转换的方法

- Host表
  - 是简单的文本文件（/etc/hosts文件），其中存放了主机名和IP地址的映射表，它通过在该文件中搜索来匹配主机名和IP地址。
- NIS（Network Information System）
  - 是由Sun Microsystems开发的，它将主机表用作NIS主机数据库，从它这里，客户机可以得到他们所需的主机表信息。
- DNS（Domain Name Server）
  - 是一种新的主机名和IP地址的转换机制，它使用一种分层的**分布式数据库**来处理Internet上的成千上万个主机和IP地址的转换。

梁如军（linuxbooks@126.com）

DNS简介

- DNS（Domain Name Service，域名系统）是一个分布式数据库系统，其作用将域名解析成IP地址。
- 域名系统允许用户使用友好的名字而不是难以记忆的数字——IP地址来访问Internet上的主机。
- DNS是基于客户 / 服务器模型设计的。
- DNS协议
  - RFC1034 — DNS 概念和工具
  - RFC1035 — DNS 实现及其DNS 的基本协议

梁如军（linuxbooks@126.com）

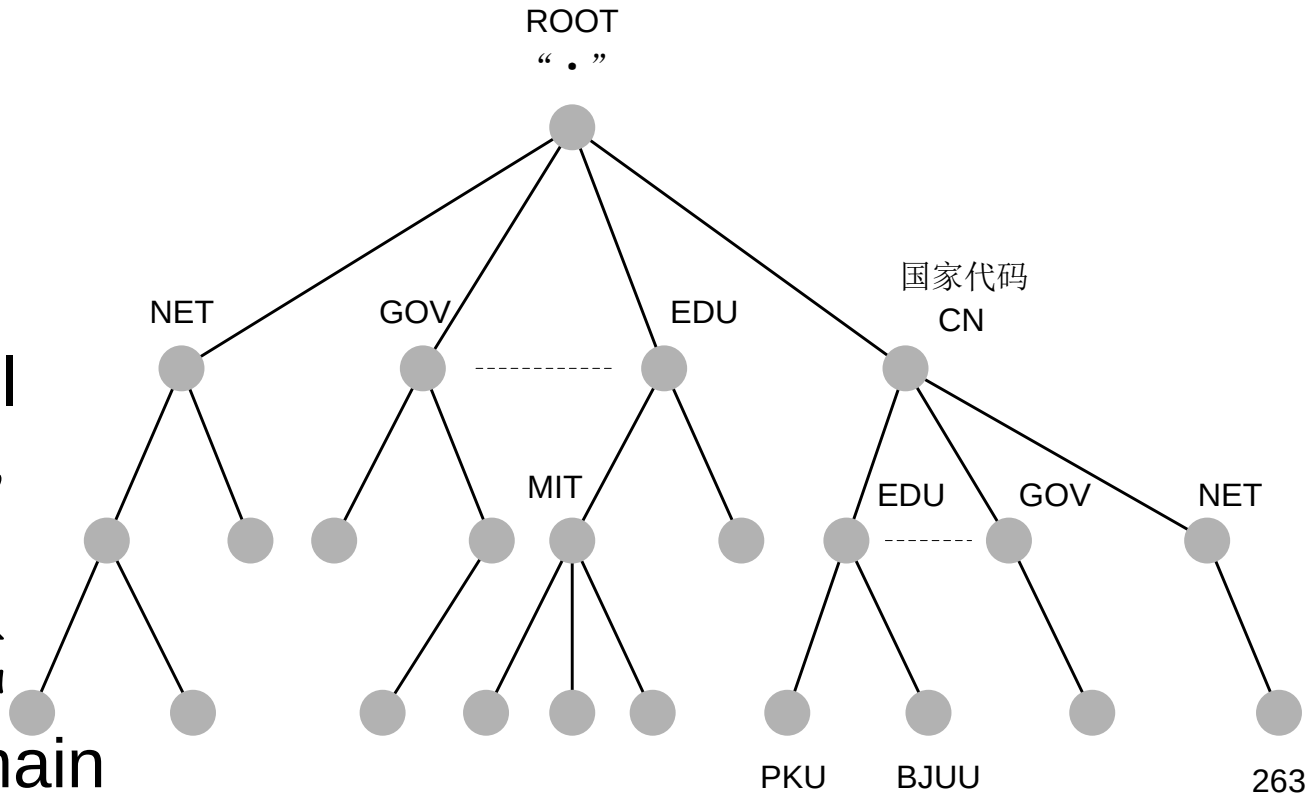
DNS系统的组成

- 域名空间
  - 标识一组主机并提供它们的有关信息的树结构的详细说明
- 域名服务器
  - 保持和维护域名空间中数据的程序
- Stub解析器
  - 解析器是简单的程序或子程序库，它从服务器中提取信息以响应对域名空间中主机的查询，用于DNS客户

梁如军（linuxbooks@126.com）

域名空间的分层结构（正向）

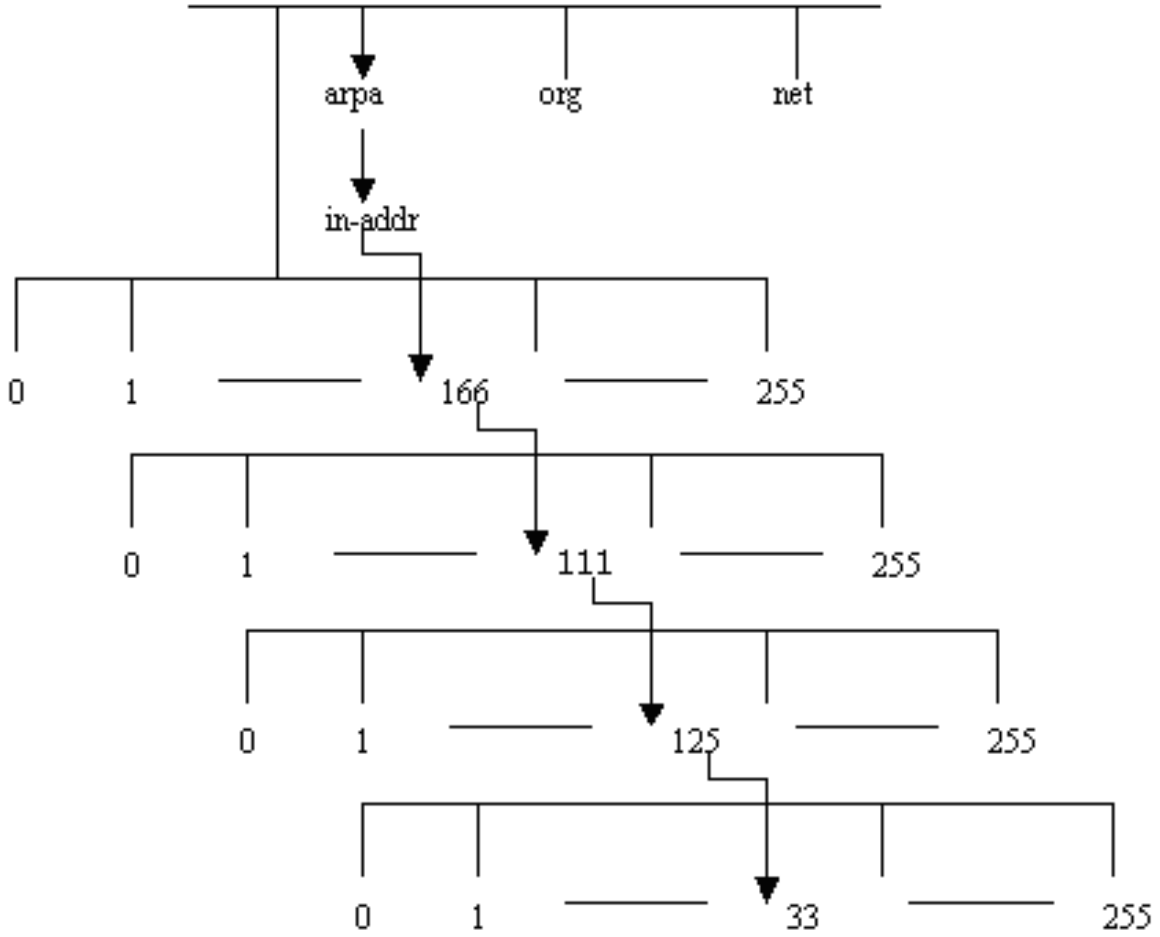
- 根域
  - Root Domain
- 顶级域
  - top-level domain，TLD
- 各级子域
  - Subdomain



梁如军（linuxbooks@126.com）

域名空间的分层结构（反向）

- 反向域（in-addr.arpa）



梁如军（linuxbooks@126.com）

DNS服务器类型——权威性服务器

- **主域名服务器**（Primary Name Server）
  - 是区数据的最根本的来源，是从本地硬盘文件中读取域的数据的，它是所有辅域名服务器进行域传输的源。
- **辅域名服务器**（Secondary Name Server）
  - 通过“区传输（zone transfer）”从主服务器复制区数据，辅域名服务器可以提供必需的冗余服务。所有的辅域名服务器都应该写在这个域的NS 记录中。
- **残根域名服务器**（Stub Name Server）
  - 与辅域名服务器类似，但只复制 NS 记录而不复制主机数据。
- **秘密域名服务器**（Stealth Name Server）
  - 并没有列在这个域的NS 记录里，仅对于知道其 IP 地址的人可见。

梁如军（linuxbooks@126.com）

DNS服务器类型——非权威性服务器

- 惟高速缓存服务器（Caching-only Server）
  - 从一个“根线索文件”加载一些根服务器的地址，并缓存这些由根服务器解析的结果并不断累计。
  - 可以将它收到的信息存储下来，并再将其提供给其它的用户进行查询，直到这些信息过期。
  - 配置中没有任何本地的授权域的配置信息。
- 转发服务器（Forwarding Server）
  - 代替众多客户执行查询并创建一个大的缓存。

梁如军（linuxbooks@126.com）

使用多种类型的DNS域名服务器

- 所有的服务器均设置高速缓冲服务器来提供名字的解答
- 一些域的主服务器可以是另外一些域的辅助域名服务器
- 一个域只能创建一个主域名服务器，另外至少应该创建二个辅助域名服务器
- 在网络上设置高速缓冲服务器可以减少主服务器和辅助域名服务器的装载量，以此来减少网络传输
- 转发服务器一般用于用户不希望站点内的服务器直接和外部服务器通讯的情况

梁如军（linuxbooks@126.com）

DNS 区域（Zone）

CentOS
The Community ENTerprise Operating System

- 为了便于根据实际情况来分散域名管理工作的负荷，将DNS域名空间划分为区域来进行管理。
  - 区域是DNS服务器的管辖范围，是由单个域或由具有上下隶属关系的紧密相邻的多个子域组成的一个管理单位。
  - DNS服务器便是以区域为单位来管理域名空间的，而不是以域为单位。
- 一台DNS服务器可以管理一个或多个区域，而一个区域也可以有多台DNS服务器来管理。
  - DNS允许 DNS 名域空间分成几个区域（Zone），它存储着有关一个或多个 DNS 域的名称信息。
  - 在DNS服务器中必须先建立区域，再在区域中建立子域，以及在区域或子域中添加主机等各种记录。

梁如军（linuxbooks@126.com）

域的委托管理

- DNS服务的管理不是集中的，它的层次结构允许将整个管理任务分成多份，分别由每个子域自行进行管理，也就是说，DNS允许将子域授权给其他组织进行管理。
- 采用委托管理的优越性，主要表现在：
  - 工作负载分散。将DNS数据库分配到各个子域的域名服务器上，大幅度降低了上级或顶级域名服务器进行名字查询的负载。
  - 提高了域名服务器的响应速度。 负担共享使得查询的时间大幅度缩减。
  - 提高了网络带宽的利用率。由于数据库的分散性使得服务器与本地接近，减小了带宽资源的浪费。

域名注册

- 当我们的子网需要连接Internet并且需要由自己管理这个域时，就需要进行域名注册
- 选择域名时必须符合RCF 1123中的规定
- 获得域名和域名注册的信息并进行域名注册
  - 互联网络信息中心（NIC）：http://www.internic.net/
  - 中国互联网络信息中心（CNNIC）：http://www.cnnic.net/
- 域名传播
  - DNS服务器周期性地和其他DNS服务器上的各种数据库同步，并检查其他服务器上的新表项
  - 域名注册过程不是瞬时完成的，但是一个新域名大约会在3～4天内完成传播，能在世界各地获得相关信息

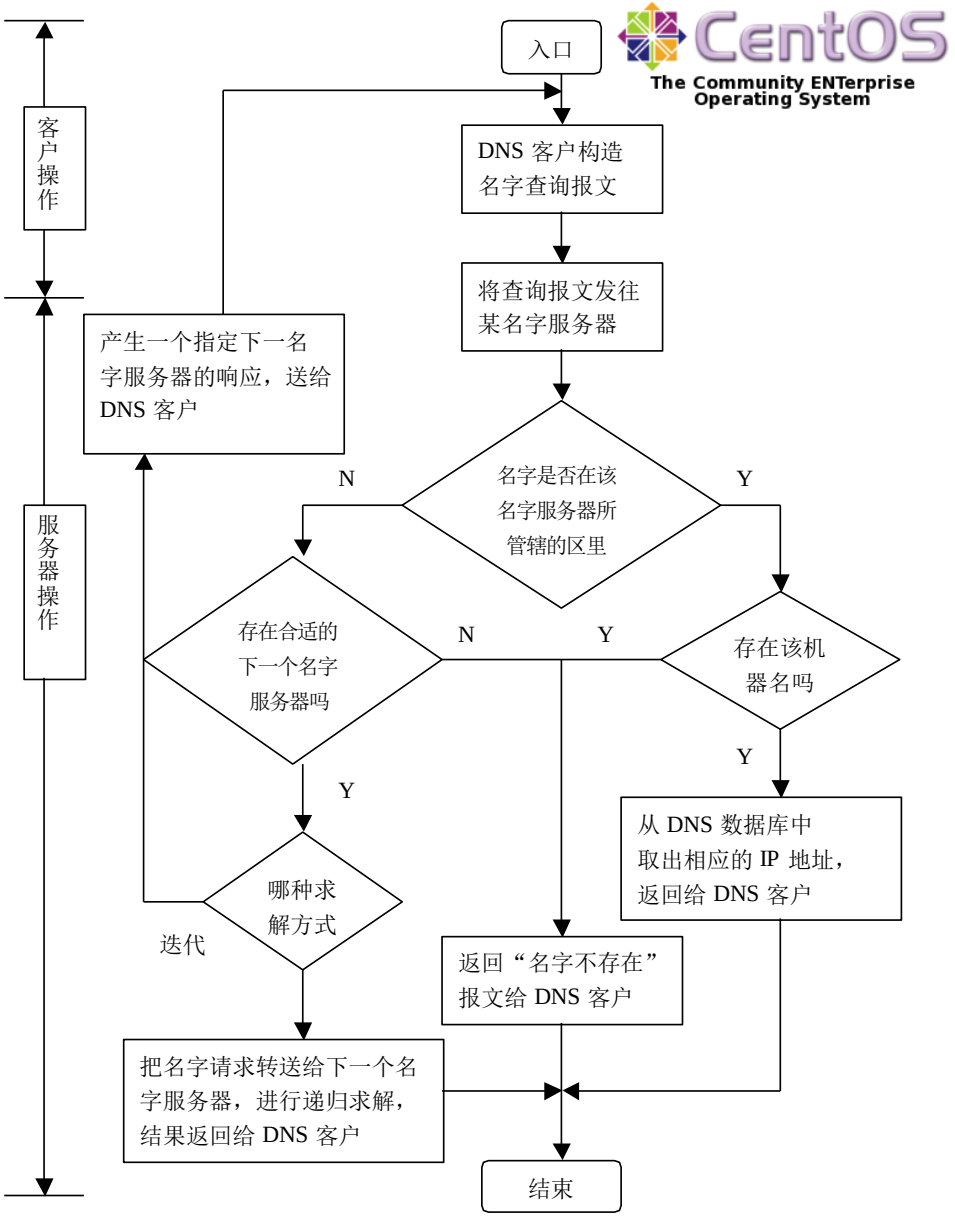
DNS查询模式

- 递归查询（Recursive Query） （给出最终结果）
  - 当收到DNS工作站的查询请求后，本地DNS服务器只会向DNS工作站返回两种信息：要么是在该DNS服务器上查到的结果、要么是查询失败。当本地名字服务器中找不到名字时，该DNS服务器绝对不会主动地告诉DNS工作站另外的DNS服务器的地址，而是由域名服务器系统自行完成名字和IP地址转换，即利用服务器上的软件来请求下一个服务器。如果其他名字服务器解析该查询失败，就由告知客户查询失败。
- 叠代查询（Iterative Query） （给出最佳结果）
  - 当收到DNS工作站的查询请求后，如果在DNS服务器中没有查到所需数据，该DNS服务器便会告诉DNS工作站另外一台DNS服务器的IP地址，然后，再由DNS工作站自行向此DNS服务器查询，依次类推一直到查到所需数据为止。如果到最后一台DNS服务器都没有查到所需数据，则通知DNS工作站查询失败。

梁如军（linuxbooks@126.com）

域名解析过程

- 一般而言，域名解析分为本域解析和跨域解析两种，当实施跨域解析时，
- 一般本地的域名服务器会直接向根域名服务器发出查询，这样的操作流程会保证比较高的查询效率。



梁如军（linuxbooks@126.com）

Stub 解析器

- 所有程序都可使用的通用解析程序库
  - 由 gethostbyname() 和其它 glibc 功能提供
  - 不具备更高性能的访问控制能力，例如签发或加密数据包
- 可以查询由 glibc 支持的任何名称服务
- 读取 /etc/nsswitch.conf 来决定查询名称服务的顺序
  - 默认配置： **hosts: files dns**
- NIS域名和DNS域名通常有所不同，这样会简化故障排除，避免名称冲突

梁如军（linuxbooks@126.com）

客户端解析程序（测试工具）

- DNS 特有的解析程序
  - dig
  - host
  - nslookup
- 读取的配置文件
  - 控制文件 **/etc/host.conf**
  - 配置文件 **/etc/resolv.conf**

梁如军（linuxbooks@126.com）

/etc/host.conf

- 常用选项
  - **Order** 指定使用不同的名字解析机制的顺序
    - **hosts**：试图通过查找本地/etc/hosts文件来解析名字
    - **bind**：使用DNS服务器来解析名字
    - **nis**：使用NIS服务来解析主机名字
  - **Alert**：以off和on为参数。若为on，则任何试图骗取IP地址的行为都通过syslog工具进行记录
  - **Nospoof**：若在反向解析找出与指定的地址匹配的主机名，则对返回的地址进行解析以确认它确实与您的查询地址相匹配。为了防止“骗取”IP地址，通过指定nospoof on来允许此功能

梁如军（linuxbooks@126.com）

/etc/host.conf 举例

```
order       bind  hosts
nospoof     on
alert       on
```

- 说明
  - order选项指明先使用DNS再使用Host表解析主机名
  - Nospoof选项表明要检查IP欺骗
  - Alert选项表明若检测出IP欺骗，则将警告信息进行记录

梁如军（linuxbooks@126.com）

/etc/resolv.conf

- 常用选项
  - **nameserver**：列出域名服务器的IP地址
    - 最多可以出现三个 nameserver 指令
  - **domain**：定义默认的域名 (主机的本地域名)
  - **options**
    - **rotate**：打开客户端轮询查询选项。当nameserver中定义多个域名服务器时，进行轮询查询。
    - **nochecknames**：当需要使用带有下划线“_”的域名时，需设置该项。

梁如军（linuxbooks@126.com）

/etc/resolv.conf 举例

```
nameserver      127.0.0.1
nameserver      192.168.0.1
nameserver      192.168.1.254
domain          jamond.net
options          nochecknames   rotate
```

- 说明
  - 首先使用 nameserver 参数定义了三个名称服务器
  - Domain 参数定义了缺省域 jamond.net
  - Options 参数定义了不执行 RFC952 名字检测且执行查询轮询

梁如军（linuxbooks@126.com）

CENTOS 7下的DNS服务

梁如军（linuxbooks@126.com）

BIND简介

- Linux下架设DNS服务器通常是使用 BIND（Berkeley Internet Name Domain Service）程序来实现，是一款实现DNS服务器的开放源码软件
  - 在一个稳定可靠的体系上建构域名和IP地址关联
  - 对 DNS RFC 标准的参数实现
  - 可以在 chroot 环境下运行
- BIND是互联网上使用最广泛的DNS服务器
- 主页：http://www.isc.org/software/bind

DNS 服务概览

- 软件包：bind、bind-utils、bind-chroot
- 服务类型：由Systemd启动的守护进程
- 配置单元：
  - /usr/lib/systemd/system/named.service
- 守护进程：/usr/sbin/named, /usr/sbin/rndc
- 端口：53 (domain), 953(rndc)
- 配置文件：(chroot目录： /var/named/chroot/)
  - /etc/named.conf
  - /etc/rndc.key
  - /var/named/*

梁如军（linuxbooks@126.com）

与DNS服务相关的软件包

- **bind**：DNS服务器软件包。
- **bind-utils**：DNS测试工具，包括dig，host与nslookup等。
- **bind-chroot**：使BIND运行在指定的目录中的安全增强工具。

梁如军（linuxbooks@126.com）

BIND的安装和启动

- 安装

  # yum install bind bind-utils

- 启动

  # systemctl start named

  # systemctl enable named

- 查看域名服务器的运行状态

  # rndc status

梁如军（linuxbooks@126.com）

CentOS 7 中 BIND的默认配置

- 默认提供一个惟高速缓存服务器的配置

分类	文件	说明
配置文件	/etc/named.conf	主配置文件
	/etc/named.rfc1912.zones	被主配置文件包含的符合 rfc1912 区声明文件
密钥文件	/etc/rndc.key	被 rndc 使用的 key 文件。若没有 rndc.conf 文件（默认没有），rndc 命令将使用此文件中的 key
	/etc/named.root.key	包含根区的 DNSSEC key
	/etc/named.iscdlv.key	包含ISC DLV（dlv.isc.org）的DNSSEC key
区数据库文件	/var/named/named.ca	根服务器线索文件
	/var/named/named.localhost	localdomain 正向区数据库文件，用于将名字 localhost.localdomain 转换为本地回送 IPV4 地址 127.0.0.1
	/var/named/named.loopback	反向区数据库文件，用于将本地回送 IPV4 地址 127.0.0.1 转换为名字 localhost
	/var/named/named.empty	广播地址的反向区数据库文件

梁如军（linuxbooks@126.com）

BIND的配置语法

梁如军（linuxbooks@126.com）

/etc/named.conf 中常用的配置语句

- 定义客户端匹配列表名称——**acl**
  - 有四个无需定义即可使用的默认匹配列表名称
    - **any**（所有主机）
    - **none**（不匹配任何主机）
    - **localhost**（本地主机）
    - **localnets**（本地网络上的所有主机）
- 定义全局配置选项 ——**options**
- 定义区声明——**zone**
- 包含其他文件到本文件——**include**

/etc/named.conf ——全局配置选项（options）

```
options (
        配置子句;
        配置子句;
);
```

- 常用的配置子句
  - 定义服务器区配置文件的工作目录（**directory**）
  - 定义查询和传输的访问控制
    - 迭代: **allow-query { match-list; };**
    - 递归: **allow-recursion { match-list; };**
    - 传输: **allow-transfer { match-list; };**

梁如军（linuxbooks@126.com）

/etc/named.conf ——定义区声明（zone）

```
zone “zone-name” IN (
    type    子句;
    file    子句;
    其他子句;
);
```

- 常用的配置子句
  - 说明一个区的类型：
    - **type *master|hint|slave***
  - 说明本区的数据库文件位置：
    - **file “*filename*”**

梁如军（linuxbooks@126.com）

区数据库文件概述

- 区数文件通常也称（域名|区）数据库文件
- 区文件定义了一个区的所有域名信息
- 区文件的组成
  - **资源记录**（Resource Records，RR）
    - 每个区文件都是由 **SOA RR** 开始，随后应该包含 **NS** RR
    - 对于正向解析文件还包括 **A** RR, **MX** RR, **CNAME** RR 等
    - 而对于反向解析文件还包括 **PTR** RR 等
  - **区文件指令**
    - 简化区文件结构（ **$INCLUDE**、**$GENERATE** ）
    - 声明资源记录中使用的值（ **$ORIGIN**、**$TTL** ）

梁如军（linuxbooks@126.com）

区数据库文件——资源记录（RR）格式

[name]　[ttl]　IN　<type>　<rdata>

- name 字段
  - .：根域
  - @：默认域
    - 在 /etc/named.conf 的 zone 声明中指定
    - 可以在文件中使用$ORIGIN domain来说明默认域
  - 标准域名
    - 或是以“.”结束的完全域名
    - 或是一个相对域名
  - 空：使用前一个RR记录中的name字段值

梁如军（linuxbooks@126.com）

区数据库文件——资源记录（RR）格式（续）

[name]　　[ttl]　IN　　<type>　　<rdata>

- ttl字段
  - RR 的寿命字段
  - 定义该资源记录中的信息存放在高速缓存中的时间长度
  - 若本RR省略此字段
    - 使用由 $TTL区文件指令的生存周期值
    - 使用本区文件的 SOA RR中的最小ttl值
- 通常为了减少录入量，将 $TTL 86400 放在区块文件的第一行，可以省略每个RR的TTL

梁如军（linuxbooks@126.com）

区数据库文件
——资源记录（RR）格式（续2）

[name]　　[ttl]　IN　　<type>　　<rdata>

- type 字段
  - SOA(Start Of Authority)
  - A(Address)
  - CNAME(Canonical NAME)
  - MX(Mail eXchanger)
  - NS(Name Server)
  - PTR(domain name PoinTeR)
  - HINFO(Host INFOrmation)

梁如军（linuxbooks@126.com）

区数据库文件
——资源记录（RR）格式（续3）

[name]　　[ttl]　IN　　<type>　　<rdata>

- rdata字段
  - 指定与这个资源记录有关的数据
  - 数据字段的内容取决于类型字段
  - 以括号（）包含的多个值的 rdata 可以分写成多行，如 SOA RR

梁如军（linuxbooks@126.com）

区数据库文件
——SOA RR 的格式与说明

[name] [ttl] IN SOA Hostname Contact (
Serial：本区信息文件的版本号
Refresh：辅助域名服务器多长时间更新数据库
Retry：若辅助域名服务器更新数据失败，多长时间再试
Expire：若辅助域名服务器无法从主服务器上更新数据，原有的数据何时失效
Minimum：若资源记录栏未设定ttl，则以这里提供的时间为准 **)**

- **Hostname**：存放本资料的主机名字
- **Contact**：管理域的管理员的邮件地址，因为“@”在文件中有特殊含义，所以邮件地址abc@xyz.com写为abc.xyz.com

区数据库文件注意事项

- 应该为区文件选择一个能够反映管辖域的文件名
  - 如：example.com管辖域的文件为example.com.zone
- 一般无需从空文件开始创建区文件
  - 可以复制bind软件包安装的现有区文件或案例模板，然后修改
- 注释使用汇编语言模式（;）
- 若没有使用“点（.）”来终止域名，BIND 会在这个名称后补充管辖域（即认为相对域名）
- 修改了区文件后，不要忘记递增SOA RR的序列号码并重载 named 服务

梁如军（linuxbooks@126.com）

域名服务器的配置举例

梁如军（linuxbooks@126.com）

配置主域名服务器

- 编辑主配置文件 /etc/named.conf
  - 配置全局选项
  - 使用 include 包含配置文件

    include "/etc/named.rfc1912.zones";

    include "/etc/named.conf.zones";
- 编辑配置文件 /etc/named.conf.zones
  - 添加区声明
- 配置正向解析数据库文件
- 配置反向解析数据库文件

参见教材的配置步骤

梁如军（linuxbooks@126.com）

主域名服务器配置技巧

- 简单负载均衡
  - 为同一个主机名设置多个IP地址
- 泛域名的解析
  - 将一个域名下的所有主机、子域都被解析到同一个IP地址上
  - 加入一条以“*”为name字段的A资源记录
- 直接解析域名
  - 为域名本身设置A资源记录
  - 使 http://example.com 的访问成为可能

梁如军（linuxbooks@126.com）

配置辅助域名服务器

- 不能在同一台计算机上同时配置同一个域的主域名服务器和辅助域名服务器。
- 主配置文件与主域名服务器的配置一致
- 修改 /etc/named.conf.zones 添加区声明
  - **type slave;**
  - **file "slaves/example.com.hosts"**
  - **masters { 192.168.0.252 ; };**

参见教材的配置步骤

梁如军（linuxbooks@126.com）

域名转发器配置选项

- forwarders
  - 指定要把查询请求转发到的远程域名服务器的IP

    forwarders { ip_addr [port ip_port] ; [ip_addr [port ip_port] ; ...] }
  - 例如

    forwarders {202.106.196.115; 202.106.0.20; };
- forward
  - 设置域名转发的工作方法
  - **forward only**：使用forwarders DNS服务器做域名解析，如果查询不到则返回DNS客户端查询失败
  - **forward first**：优先使用forwarders DNS服务器做域名解析，如果查询不到再使用本地DNS服务器做域名解析

梁如军（linuxbooks@126.com）

域名转发器种类

- 全局转发器

```
options {
        recursion yes;
        forwarder { 202.106.196.115;  202.106.0.20; };
        forward only;
        ......
};
```

- 区转发器

```
zone “mytest.com” IN {
        type forward;
        forwarders { 192.168.10.5;  };
        ......
};
```


梁如军（linuxbooks@126.com）

配置区域委派

- 配置步骤
  - 在父服务器中，添加一个NS记录
  - 在父服务器中，添加一个A记录来完成授权
  - 在子服务器中，创建包含子域数据的区块文件
- 粘合记录
  - 如果子服务器的规范名称位于它管理的子域中，A记录就被称为“粘合（glue）”记录

梁如军（linuxbooks@126.com）

DNS测试及工具

梁如军（linuxbooks@126.com）

DNS测试

- 准备
  - 配置好客户配置文件 **/etc/resolv.conf**
  - 启动服务：**service named restart**
- 工具
  - 熟练地使用**dig**、**host**或**nslookup**中的任意一个校验DNS服务器配置
  - 在另外一个 shell 中运行 **tail -f /var/log/messages**
- 排错
  - 在编辑了配置文件后总是应该运行

    # service named configtest
    - configtest 会运行两个语法检查工具

梁如军（linuxbooks@126.com）

单独运行两个语法检查工具

- 主配置文件检查
  - **named-checkconf -t ROOTDIR /path/to/named.conf**
  - 默认检查 /etc/named.conf 文件
  - 示例：

    named-checkconf

    named-checkconf -t /var/named/chroot
- 区文件检查
  - **named-checkzone origin /path/to/zonefile**
  - 示例：

    named-checkzone ls-al.me /var/named/ls-al.me.zone

    named-checkzone ls-al.me
    /var/named/chroot/var/named/ls-al.me.zone

梁如军（linuxbooks@126.com）

域名测试程序—— dig

- 正向查询： **dig centos.org**
- 反向查询： **dig -x 72.232.194.162**
- SOA查询：**dig -t soa centos.org**
- 邮件交换器查询：

  dig -t mx centos.org
- 查询一切：

  dig -t axfr ls.me. @192.168.0.252
- 跟踪DNS查询：

  dig +trace centos.org

域名测试程序—— host

- 正向查询：**host centos.org**
- 反向查询：**host 72.232.194.162**
- SOA查询：**host -t soa centos.org**
- MX查询：**host -t mx centos.org**
- NS迭代查询：**host -rt ns centos.org**
- NS查询：**host -t ns ls-al.me**
- 查询一切：**host -a ls-al.me**

梁如军（linuxbooks@126.com）

配置访问控制

梁如军（linuxbooks@126.com）

地址匹配列表（ match-list ）

- 使用分号间隔的IP地址列表
  - 可以与基于主机的访问控制安全性指令共同使用
- 格式
  - IP地址：192.168.0.1
  - 网络地址：192.168.0.
  - CIDR：192.168.0/24
  - 使用叹号（！）来代表相反的结果
- 按顺序检查匹配列表，找到第一个匹配后就停止
- 示例：

{ 192.168.0.1; 192.168.0.; !192.168.1.0/24; };

梁如军（linuxbooks@126.com）

访问控制列表（ACL）

- 访问控制列表（ACL）就是一个被命名的地址匹配列表
- 一般可以用来代替匹配列表（允许嵌套！）
- 使用访问控制列表可以使配置简单而清晰，一次定义之后可以在多处使用
- 定义ACL的最好位置
  - /etc/named.conf 文件的开始处，

    include "/etc/named.conf.acls";
  - 使用用户自己定义的访问控制列表必须在使用之前定义
  - acl 是 named.conf 中的顶级语句，不能将其嵌入其他的语句

梁如军（linuxbooks@126.com）

Acl语句举例

```
acl "trusted"       { 192.168.1.21; };
acl "classroom"     { 192.168.0.0/24; trusted; };
acl "cracker"       { 192.168.1.0/24; };
acl "mymasters"     { 192.168.0.254; };
acl "myaddresses" { 127.0.0.1; 192.168.0.1; };
acl bogusnets {
    0.0.0.0/8;  1.0.0.0/8;  2.0.0.0/8;
    169.254.0.0/16;    192.0.2.0/24;
    224.0.0.0/3;       10.0.0.0/8;
    172.16.0.0/12;     192.168.0.0/16;
};
```

可以使用 ACL的配置语句

- 绑定服务接口
  - **listen-on port 53 { match-list; };**
  - **listen-on-v6 port 53 { match-list; };**
- 允许查询、传输、递归、动态更新
  - **allow-query { match-list; };**
  - **allow-transfer { match-list; };**
  - **allow-recursion { match-list; };**
  - **allow-update { match-list; };**
- 阻止查询
  - **blackhole { match-list; };**

梁如军（linuxbooks@126.com）

ACL 使用举例

- 限制查询、传输、递归
- 防止欺骗和拒绝服务攻击

梁如军（linuxbooks@126.com）

分离式（SPLIT）DNS 配置

梁如军（linuxbooks@126.com）

分离式 DNS 简介

- 可以让不同网络访问相同域名时解析到不同的 IP 地址
- 适用于
  - 对内外网用户指定不同的资源记录，或对内网用户提供更多的资源记录
  - 可以在内网使用 RFC 1918 中定义的私有地址，而在外网上使用公网地址
  - 分别对电信、网通的用户指定不同的资源记录

梁如军（linuxbooks@126.com）

View 语句

```
view  view_name {
    match-clients { address_match_list };
    [ view_option; ...]
    zone_statement; ...
};
```

- **match-clients** 子句非常重要，它用于指定谁能看到本 view，列表中可以使用由 acl 语句定义的 aclname。
- 可以在 view 语句中使用一些选项，详细信息请参考 named.conf 的手册页
- zone_statement 子句指定在当前 view 中可见的区声明

梁如军（linuxbooks@126.com）

View 语句注意事项

- 如果在配置文件中使用了 view 语句，则所有的 zone 语句都必须在 view 中出现。
- 对同一个 zone 而言，配置内网的 view 应该置于外网的 view 之前。

梁如军（linuxbooks@126.com）

分离式 DNS 配置举例

- 本例给出一个使用分离式 DNS 的小型公司 sinoesl.com 的配置。做如下要求：
  - 公网上 DNS 的服务器的 IP 分别为 1.2.3.4 和 5.6.7.8
  - 公司的本地私网使用 192.168.0/24 私网地址，192.168.0.200 作为内部主 DNS；
  - 无论内外网，将 sinoesl.com 和 www.sinoesl.com 都解析到公网地址

本章思考题

- 简述DHCP的工作过程。
- 简述如何在大型网络中部署DHCP服务。
- 简述自动安装服务器所需的组件。
- 简述DNS系统的组成、DNS服务器的类型。
- 简述DNS的查询模式、DNS解析过程。
- 什么是域名转发？
- 简述BIND的配置文件族。
- 简述资源记录的类型。

梁如军（linuxbooks@126.com）

本章实验

- 学会配置单作用域的DHCP服务器。
- 学会配置DHCP中继代理。
- 学会配置主域名服务器。
- 学会配置辅助域名服务器。
- 学会配置域名转发。

进一步学习

- 学习DHCP超级作用域的配置。
- 学习在DHCP服务器配置中使用类（class）以区分不同的客户类型。
- 学习配置DNS的区域委派。
- 学习配置Split DNS。
- 学习将BIND 运行在chroot jail 环境下的配置方法。
- 学习 BIND 的基于公钥技术的签名技术。
- 学习dnsmasq的安装和配置。
- 学习使用Cobbler（https://fedorahosted.org/cobbler/）

梁如军（linuxbooks@126.com）