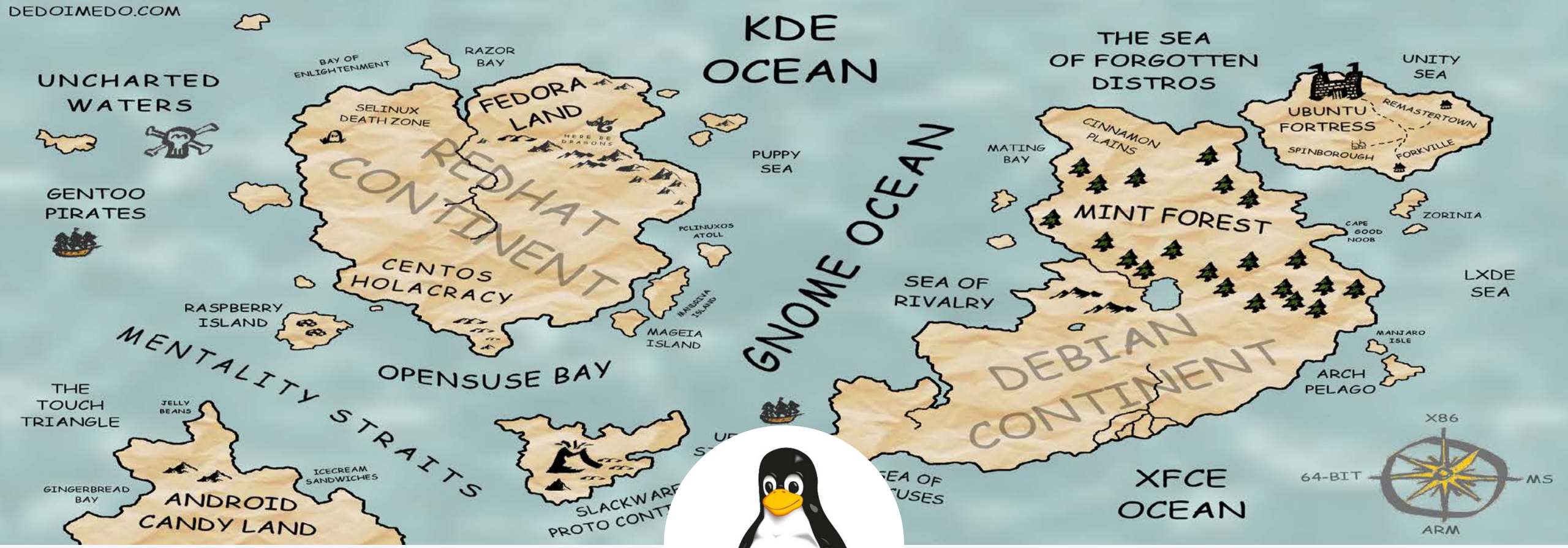


使用BIND提供域名解析服务

任课教师：刘遄 www.LinuxProbe.com

课程概述

01 **DNS域名解析服务**
DNS Domain Name Resolution Service

02 **安装bind服务程序**
Install bind service program

03 **部署从服务器**
Deploy Slave Server

04 **安全的加密传输**
Secure Encrypted Transmission

05 **部署缓存服务器**
Deploy Cache Server

06 **分离解析技术**
Separation And Analysis Technology

前言

01

DNS域名解析服务的原理以及作用，域名查询功能中正向解析与反向解析的作用，通过实验的方式演示了如何在DNS主服务器上部署正、反解析工作模式，以便让大家深刻体会到DNS域名查询的便利以及强大。

02

如何部署DNS从服务器以及DNS缓存服务器来提升用户的域名查询体验，如何使用chroot牢笼机制插件来保障bind服务程序的可靠性，如何在主服务器与从服务器之间部署TSIG密钥加密功能，进一步保障迭代查询中数据的安全性。从实战层面讲解了DNS分离解析技术，让来自不同国家、不同地区的用户都能获得最优的网站访问体验。

DNS域名解析服务

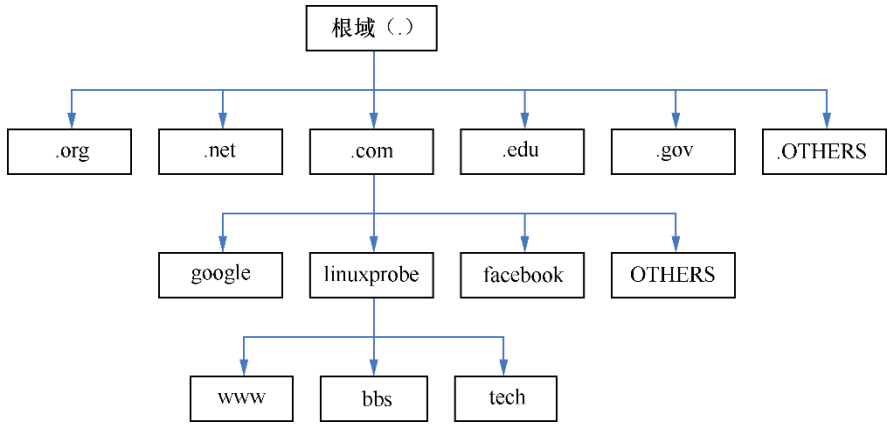
DNS Domain Name Resolution Service

DNS域名解析服务

域名系统

为了降低用户访问网络资源的门槛，域名系统（Domain Name System，DNS）技术应运而生。这是一项用于管理和解析域名与IP地址对应关系的技术。

鉴于互联网中的域名和IP地址对应关系数据库太过庞大，DNS域名解析服务采用了类似目录树的层次结构来记录域名与IP地址之间的对应关系，从而形成了一个分布式的数据库系统。



DNS域名解析服务采用的目录树层次结构

域名后缀

域名后缀一般分为国际域名和国内域名。原则上来讲，域名后缀都有严格的定义，但在实际使用时可以不必严格遵守。

1. .com（商业组织）
2. .org（非营利组织）
3. .gov（政府部门）
4. .net（网络服务商）
5. .edu（教育机构）
6. .pub（公共大众）
7. .cn（中国国家顶级域名）
8. ……

服务器

主服务器

在特定区域内具有唯一性，负责维护该区域内的域名与IP地址之间的对应关系。

从服务器

从主服务器中获得域名与IP地址的对应关系并进行维护，以防主服务器宕机等情况。

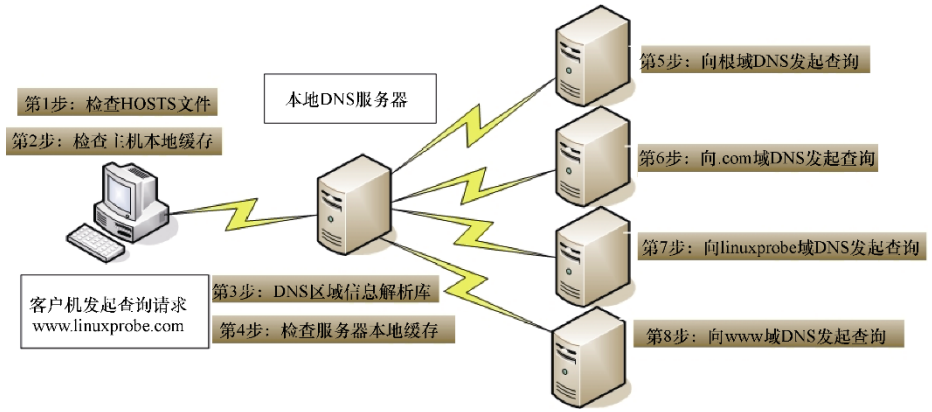
缓存服务器

通过向其他域名解析服务器查询获得域名与IP地址的对应关系，并将经常查询的域名信息保存到服务器本地，以此来提高重复查询时的效率。

DNS域名解析服务

DNS域名解析服务

DNS域名解析服务采用分布式的数据结构来存放海量的“区域数据”信息，在执行用户发起的域名查询请求时，具有递归查询和迭代查询两种方式。**递归查询**，是指DNS服务器在收到用户发起的请求时，必须向用户返回一个准确的查询结果。**迭代查询**，是指DNS服务器在收到用户发起的请求时，并不直接回复查询结果，而是告诉另一台DNS服务器的地址，用户再向这台DNS服务器提交请求，这样依次反复，直到返回查询结果。



向DNS服务器发起域名查询请求的流程

13台根DNS服务器的具体信息

名称	管理单位	地理位置	IP地址
A	INTERNIC.NET	美国弗吉尼亚州	198.41.0.4
B	美国信息科学研究所	美国加利弗尼亚州	128.9.0.107
C	PSINet公司	美国弗吉尼亚州	192.33.4.12
D	马里兰大学	美国马里兰州	128.8.10.90
E	美国航空航天管理局	美国加利弗尼亚州	192.203.230.10
F	因特网软件联盟	美国加利弗尼亚州	192.5.5.241
G	美国国防部网络信息中心	美国弗吉尼亚州	192.112.36.4
H	美国陆军研究所	美国马里兰州	128.63.2.53
I	Autonomica公司	瑞典斯德哥尔摩	192.36.148.17
J	VeriSign公司	美国弗吉尼亚州	192.58.128.30
K	RIPE NCC	英国伦敦	193.0.14.129
L	IANA	美国弗吉尼亚州	199.7.83.42
M	WIDE Project	日本东京	202.12.27.33

注：这里提到的13台根域服务器并非真的只有13台服务器，没有哪台服务器能独立承受住如此大的请求量，这是技术圈习惯的叫法而已。实际上用于根域名的服务器总共有504台，它们从A到M进行了排序，并共用13个IP地址，以此进行负载均衡，以抵抗分布式拒绝服务（DDoS）攻击。

安装bind服务程序

Install bind service program

安装bind服务程序

bind服务程序

BIND（Berkeley Internet Name Domain，伯克利因特网名称域）服务是全球范围内使用最广泛、最安全可靠且高效的域名解析服务程序。

chroot扩展包

在生产环境中安装部署bind服务程序时加上chroot（俗称牢笼机制）扩展包，以便有效地限制bind服务程序仅能对自身的配置文件进行操作，以确保整个服务器的安全。

bind服务程序的配置

要想为用户提供健全的DNS查询服务，要在本地保存相关的域名数据库，而如果把所有域名和IP地址的对应关系都写入到某个配置文件中，估计要有上千万条的参数，这样既不利于程序的执行效率，也不方便日后的修改和维护。

3个关键文件

主配置文件

（/etc/named.conf），只有59行，而且在去除注释信息和空行之后，实际有效的参数仅有30行左右，这些参数用来定义bind服务程序的运行。

区域配置文件

（ /etc/named.rfc1912.zones），用来保存域名和IP地址对应关系的所在位置。类似于图书的目录，对应着每个域和相应IP地址所在的具体位置，当需要查看或修改时，可根据这个位置找到相关文件。

数据配置文件目录

（/var/named），该目录用来保存域名和IP地址真实对应关系的数据配置文件。

解析参数

```
zone “linuxprobe.com” IN{
    type master;
    file “linuxprobe.com.zone”;
    allow-update  {none; };
};
```

服务类型

域名与 IP 地址解析规则保存的文件位置

允许哪些客户机动态更新解析信息

正向解析参数

```
zone “10.168.192.in-addr.arpa” IN{
    type master;
    file “192.168.10.arpa”;
};
```

表示192.168.10.0/24 网段的反向解析区域

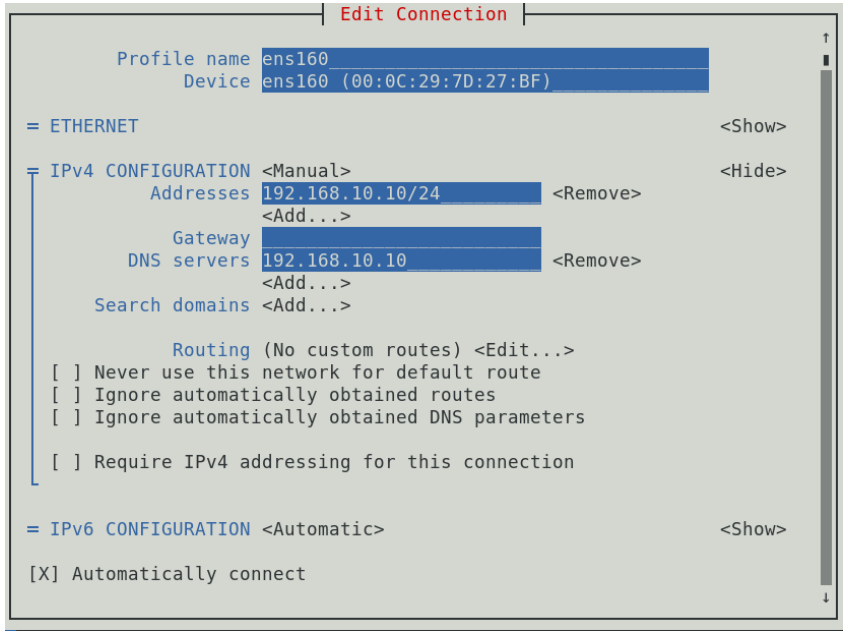
反向解析参数

正向解析实验

正向解析

在DNS域名解析服务中，正向解析是指根据域名（主机名）查找到对应的IP地址。当用户输入了一个域名后，bind服务程序会自动进行查找，并将匹配到的IP地址返给用户。这也是最常用的DNS工作模式。

正向解析技术示意图



配置网卡DNS参数信息

正向解析实验

第1步

编辑区域配置文件。该文件中默认已经有了一些无关紧要的解析参数，旨在让用户有一个参考。

第2步

编辑数据配置文件。可以从/var/named目录中复制一份正向解析的模板文件（named.localhost），然后把域名和IP地址的对应数据填写数据配置文件中并保存。

第3步

检验解析结果。为了检验解析结果，一定要先把Linux系统网卡中的DNS地址参数修改成本机IP地址，这样就可以使用由本机提供的DNS查询服务了。

正向解析实验

$TTL 1D	**#生存周期为1天**				
@	IN SOA	linuxprobe.com.	root.linuxprobe.com.	{	
#授权信息开始:		#DNS区域的地址	#域名管理员的邮箱(不要用@符号)		
0;serial					#更新序列号
1D;refresh					#更新时间
1H;retry					#重试延时
1W;expire					#失效时间
3H);minimum					#无效解析记录的缓存时间
NS		ns.linuxprobe.com.	#域名服务器记录		
ns	IN A	192.168.10.10	#地址记录（ns.linuxprobe.com.）		
www	IN A	192.168.10.10	#地址记录（www.linuxprobe.com.）		

域名解析记录类型

记录类型	作用
A	将域名指向一个IPv4地址
CNAME	将域名指向另外一个域名
AAAA	将域名指向一个IPv6地址
NS	将子域名指定由其他DNS服务器解析
MX	将域名指向邮件服务器地址
SRV	记录提供特定的服务的服务器
TXT	文本内容一般为512字节，常作为反垃圾邮件的SPF（Sender Policy Framework，发送方策略框架）记录
CAA	CA证书颁发机构授权校验
显性URL	将域名重定向到另外一个地址
隐性URL	与显性URL类似，但是会隐藏真实目标地址

反向解析实验

正向解析

在DNS域名解析服务中，反向解析的作用是将用户提交的IP地址解析为对应的域名信息，它一般用于对某个IP地址上绑定的所有域名进行整体屏蔽，屏蔽由某些域名发送的垃圾邮件。它也可以针对某个IP地址进行反向解析，大致判断出有多少个网站运行在上面。

反向解析技术示意图

```
10 IN       PTR       www.linuxprobe.com.
20 IN       PTR       bbs.linuxprobe.com.
```

在 192.168.10.in-addr.arpa 反向区域数据文件中，则对应为 192.168.10.20 的 IP 地址

反向解析文件中IP地址参数规范

反向解析实验

第1步

编辑区域配置文件。在编辑该文件时，除了不要写错格式之外，还需要记住此处定义的数据配置文件名称，因为一会儿还需要在/var/named目录中建立与其对应的同名文件。

第2步

编辑数据配置文件。首先从/var/named目录中复制一份反向解析的模板文件（named.loopback），然后把下面的参数填写到文件中。

第3步

检验解析结果。在前面的正向解析实验中，已经把系统网卡中的DNS地址参数修改成了本机IP地址，因此可以直接使用nslookup命令来检验解析结果，仅需输入IP地址即可查询到对应的域名信息。

反向解析实验

$TTL 1D				
@	IN SOA	Linuxprobe.com.	Root.linuxprobe.com .	(
				0;serial
				1D;refresh
				1H;retry
				1W;expire
				3H);minimum
	NS	ns.linuxprobe.com.		
ns	A	192.168.10.10		
10	PTR	ns.linuxprobe.com.	#PTR为指针记录，仅用于反向解析	
10	PTR	www.linuxprobe.com.		
20	PTR	bbs.linuxprobe.com.		

部署从服务器

Deploy Slave Server

部署从服务器

主机名称	操作系统	IP地址
主服务器	RHEL 8	192.168.10.10
从服务器	RHEL 8	192.168.10.20

主服务器与从服务器分别使用的操作系统与IP地址信息

部署从服务器

第1步

在主服务器的区域配置文件中允许该从服务器的更新请求，即修改allow-update {允许更新区域信息的主机地址;};参数，然后重启主服务器的DNS服务程序。

第2步

在主服务器上配置防火墙放行规则，让DNS协议流量可以被顺利传递。

第3步

在从服务器上安装bind-chroot软件包（输出信息省略）。修改配置文件，让从服务器也能够对外提供DNS服务，并且测试其与主服务器的网络连通性。

部署从服务器

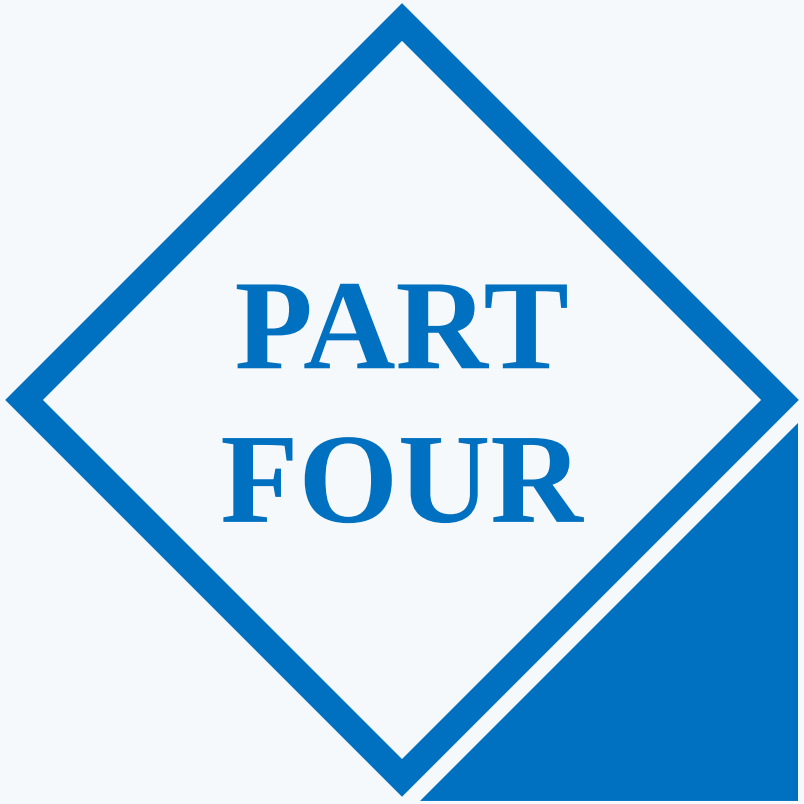
第4步

在从服务器中填写主服务器的IP地址与要抓取的区域信息，然后重启服务。注意此时的服务类型应该是slave（从），而不再是master（主）。masters参数后面应该为主服务器的IP地址，而且file参数后面定义的是同步数据配置文件后要保存到的位置，稍后可以在该目录内看到同步的文件。

注：这里的masters参数比正常的主服务类型master多了个字母s，表示可以有多个主服务器。请大家小心，不要漏掉哦。

第5步

检验解析结果。当从服务器的DNS服务程序在重启后，一般就已经自动从主服务器上同步了数据配置文件，而且该文件默认会放置在区域配置文件中所定义的目录位置中。



安全的加密传输

Secure Encrypted Transmission

安全的加密传输

安全的加密传输

- ✓ 互联网中的绝大多数DNS服务器（超过95%）都是基于BIND域名解析服务搭建的，而bind服务程序为了提供安全的解析服务，已经对TSIG（见RFC 2845）加密机制提供了支持。
- ✓ TSIG主要是利用了密码编码的方式来保护区域信息的传输（Zone Transfer），即TSIG加密机制保证了DNS服务器之间传输域名区域信息的安全性。

参数	作用
-a	指定加密算法，包括RSA MD5（RSA）、RSA SHA1、DSA、NSEC3RSASHA1、NSEC3DSA等
-b	密钥长度（HMAC-MD5的密钥长度在1～512位之间）
-n	密钥的类型（HOST表示与主机相关）

dnssec-keygen命令的常用参数

安全的加密传输

第1步

在主服务器中生成密钥。dnssec-keygen命令用于生成安全的DNS服务密钥，其格式为“dnssec-keygen [参数]”。

第2步

在主服务器中创建密钥验证文件。进入bind服务程序用于保存配置文件的目录，把刚刚生成的密钥名称、加密算法和私钥加密字符串按照下面的格式写入tansfer.key传输配置文件中。

第3步

开启并加载bind服务的密钥验证功能。首先需要在主服务器的主配置文件中加载密钥验证文件，然后进行设置，使得只允许带有master-slave密钥认证的DNS服务器同步数据配置文件。

安全的加密传输

第4步

配置从服务器，使其支持密钥验证。配置DNS需要在bind服务程序的配置文件目录中创建密钥认证文件，并设置相应的权限，然后设置该文件的一个硬链接，并指向/etc目录。

第5步

开启并加载从服务器的密钥验证功能。这一步的操作步骤也同样是在主配置文件中加载密钥认证文件，然后按照指定的格式写上主服务器的IP地址和密钥名称。

第6步

DNS从服务器同步域名区域数据。现在，两台服务器的bind服务程序都已经配置妥当，并匹配到了相同的密钥认证文件。

第7步

再次进行解析验证。功能正常。请大家注意观察，是由192.168.10.20从服务器进行解析的。

部署缓存服务器

Deploy Cache Server

部署缓存服务器

第1步

配置系统的双网卡参数。为了更加贴近真实的网络环境，实现外网查询功能，我们需要在缓存服务器中再添加一块网卡，并按照信息配置出两台Linux虚拟机系统。

第2步

还需要在虚拟机软件中将新添加的网卡设置为“桥接模式”。然后设置成与物理设备相同的网络参数。

第3步

在bind服务程序的主配置文件中添加缓存转发参数。在大约第20行处添加一行参数“forwarders { 上级DNS服务器地址; };”，上级DNS服务器地址指的是获取数据配置文件的服务器。

第4步

重启DNS服务，验证成果。把客户端主机的DNS服务器地址参数修改为DNS缓存服务器的IP地址192.168.10.10。

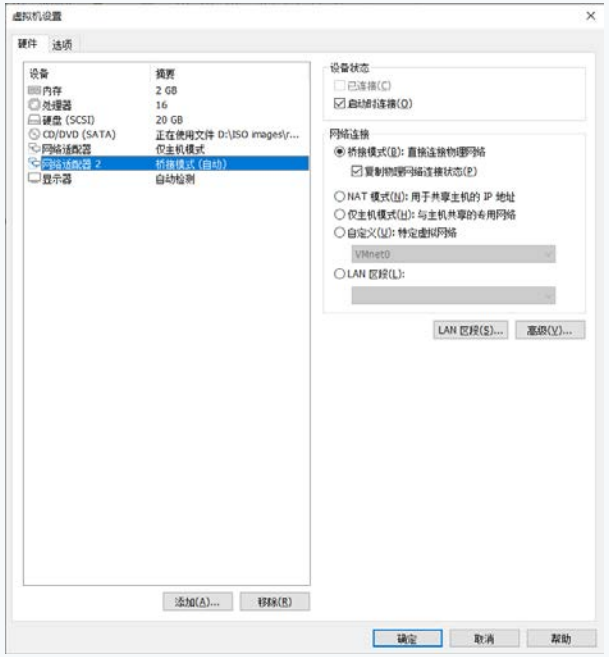
部署缓存服务器

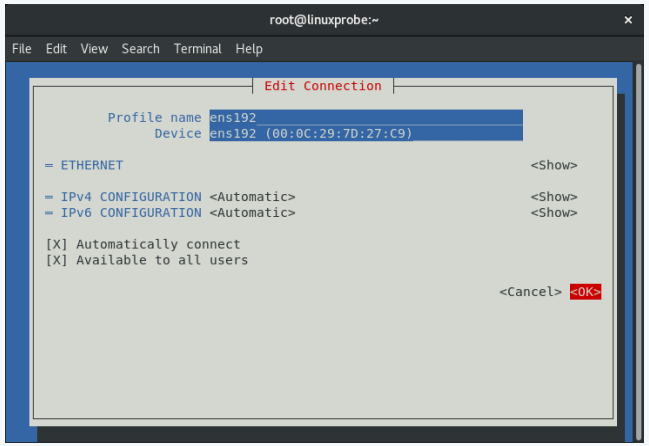
主机名称	操作系统	IP地址
缓存服务器	RHEL 8	网卡（外网）：根据物理设备的网络参数进行配置（通过DHCP或手动方式指定IP地址与网关等信息） 网卡（内网）：192.168.10.10
客户端	RHEL 8	192.168.10.20

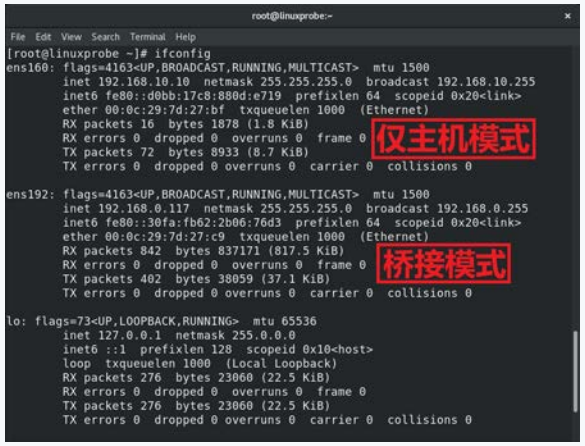
用于配置Linux虚拟机系统所需的参数信息

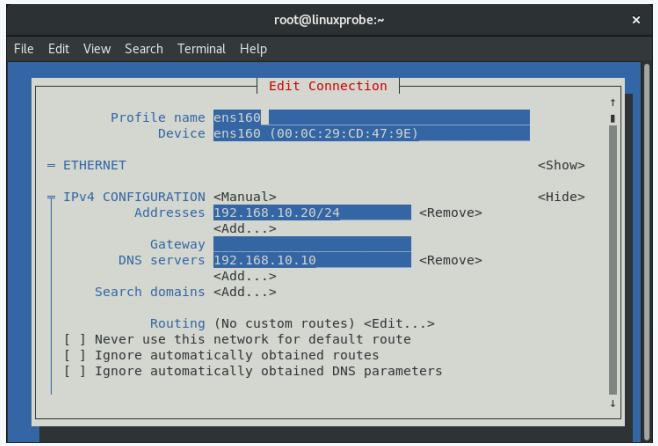
缓存服务器实验环境拓扑

部署缓存服务器









新添加一块桥接网卡 → 以DHCP方式获取网络参数 → 查看网卡的工作状态 → 设置客户端主机的DNS服务器地址参数

PART
SIX

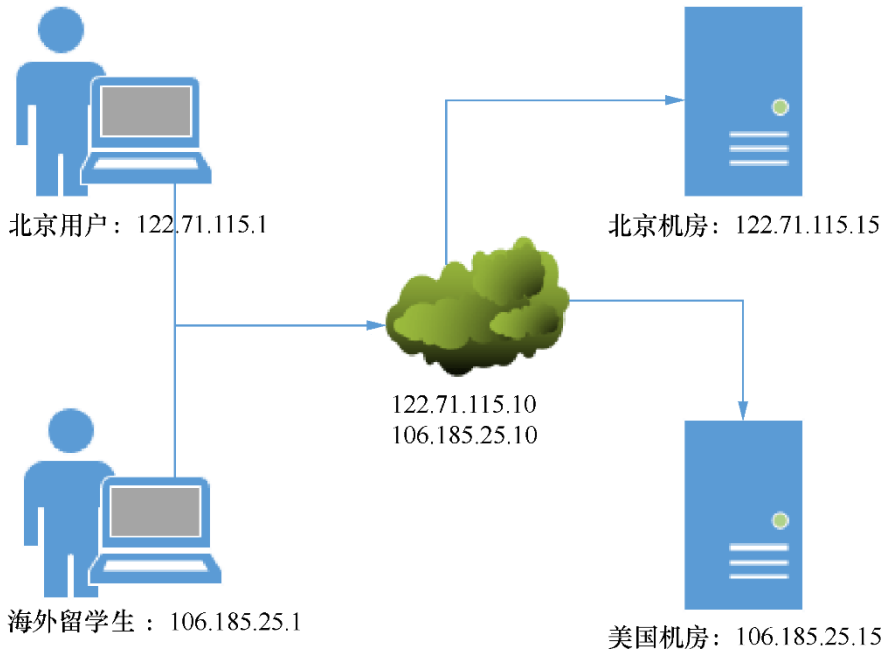
分离解析技术

Separation And Analysis Technology

分离解析技术

主机名称	操作系统	IP地址
DNS服务器	RHEL 8	北京网络：122.71.115.10 美国网络：106.185.25.10
北京用户	Windows 10	122.71.115.1
海外用户	Windows 10	106.185.25.1

不同主机的操作系统与IP地址情况



DNS分离解析技术

分离解析技术

第1步

修改bind服务程序的主配置文件，把第11行的监听端口与第19行的允许查询主机修改为any。由于配置的DNS分离解析功能与DNS根服务器配置参数有冲突，所以需要把第52～55行的根域信息删除。

第2步

编辑区域配置文件。把区域配置文件中原有的数据清空，然后按照以下格式写入参数。

第3步

建立数据配置文件。分别通过模板文件创建出两份不同名称的区域数据文件，其名称应与上面区域配置文件中的参数相对应。

第4步

重新启动named服务程序，验证结果。将客户端主机（Windows系统或Linux系统均可）的IP地址分别设置为122.71.115.1与106.185.25.1，将DNS地址分别设置为服务器主机的两个IP地址。

分离解析技术

$TTL 1D	#生存周期为1天				
@	IN SOA	linuxprobe.com.	root.linuxprobe.com.	(	
	#授权信息开始:	#DNS区域的地址	#域名管理员的邮箱(不要用@符号)		
				0;serial	#更新序列号
				1D;refresh	#更新时间
				1H;retry	#重试延时
				1W;expire	#失效时间
				3H);minimum	#无效解析记录的缓存时间
	NS	ns.linuxprobe.com.		#域名服务器记录	
ns	IN A	122.71.115.10		#地址记录(ns.linuxprobe.com.)	
www	IN A	122.71.115.15		#地址记录(www.linuxprobe.com.)	

分离解析技术

$TTL 1D	#生存周期为1天				
@	IN SOA	linuxprobe.com.	root.linuxprobe.com.	(	
	#授权信息开始:	#DNS区域的地址	#域名管理员的邮箱(不要用@符号)		
				0;serial	#更新序列号
				1D;refresh	#更新时间
				1H;retry	#重试延时
				1W;expire	#失效时间
				3H);minimum	#无效解析记录的缓存时间
	NS	ns.linuxprobe.com.		#域名服务器记录	
ns	IN A	106.185.25.10		#地址记录(ns.linuxprobe.com.)	
www	IN A	106.185.25.15		#地址记录(www.linuxprobe.com.)	

分离解析技术

模拟中国用户的域名解析操作

模拟美国用户的域名解析

复习题

✓ **1．DNS技术提供的3种类型的服务器分别是什么?**

答：DNS主服务器、DNS从服务器与DNS缓存服务器。

✓ **2．DNS服务器之间传输区域数据文件时，使用的是递归查询还是迭代查询?**

答：DNS服务器之间是迭代查询，用户与DNS服务器之间是递归查询。

✓ **3．在Linux系统中使用bind服务程序部署DNS服务时，为什么推荐安装chroot插件?**

答：能有效地限制bind服务程序仅能对自身的配置文件进行操作，以确保整个服务器的安全。

✓ **4．在DNS服务中，正向解析和反向解析的作用是什么?**

答：正向解析是将指定的域名转换为IP地址，而反向解析则是将IP地址转换为域名。正向解析模式更为常用。

✓ **5．是否可以限制使用DNS域名解析服务的主机？如何限制?**

答：是的，修改主配置文件中第17行的allow-query参数即可。

复习题

✓ **6． 部署DNS从服务器的作用是什么?**

答：部署从服务器不仅可以减轻主服务器的负载压力，还可以提升用户的查询效率。

✓ **7． 当用户与DNS服务器之间传输数据配置文件时，是否可以使用TSIG加密机制来确保文件内容不被篡改?**

答：不能，TSIG加密机制保障的是DNS服务器与DNS服务器之间迭代查询的安全。

✓ **8．部署DNS缓存服务器的作用是什么?**

答：DNS缓存服务器把用户经常使用到的域名与IP地址的解析记录保存在主机本地，从而提升下次解析的效率。一般用于经常访问某些固定站点而且对这些网站的访问速度有较高要求的企业内网中，但实际的应用并不广泛。

✓ **9． DNS分离解析技术的作用是什么?**

答：可以让位于不同地理范围内的用户通过访问相同的网址，从不同的服务器获取到相同的数据，以提升访问效率。

祝同学们学习顺利，爱上Linux系统。