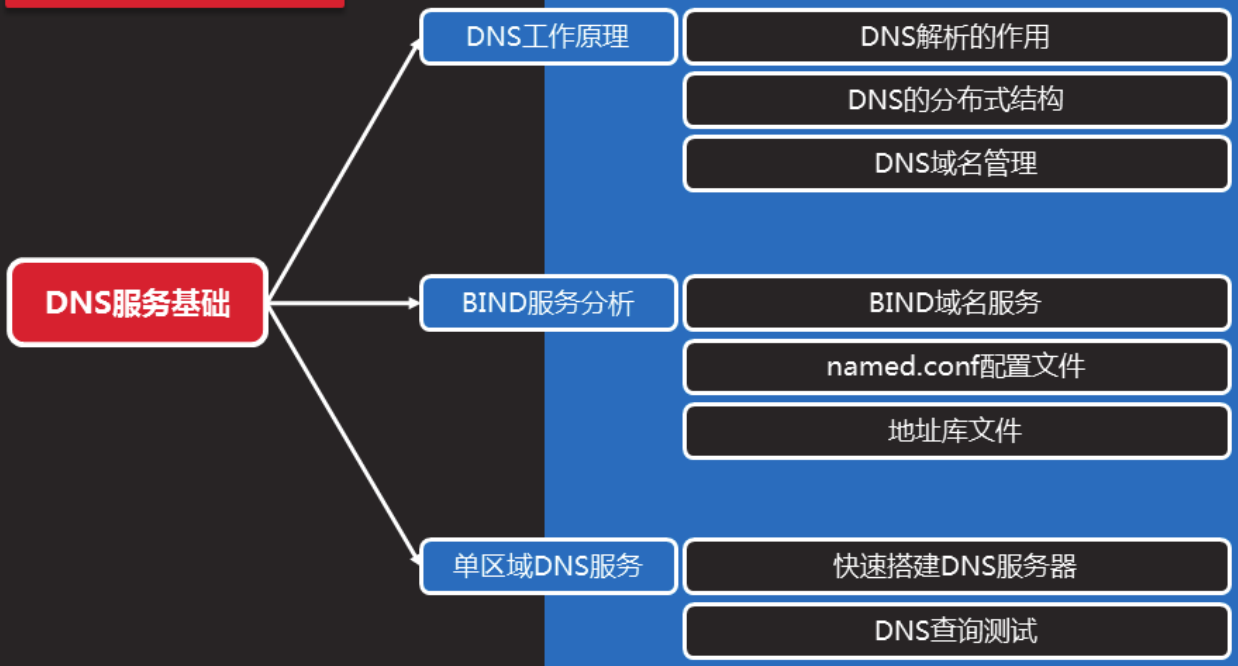
SERVICES DAY02

内容

上午	09:00 ~ 09:30	作业讲解和回顾
	09:30 ~ 10:20	DNS服务基础
	10:30 ~ 11:20	
	11:30 ~ 12:00	特殊解析
下午	14:00 ~ 14:50	DNS子域授权
	15:00 ~ 15:50	
	16:10 ~ 17:00	缓存DNS
	17:10 ~ 18:00	总结和答疑

DNS服务基础



DNS工作原理

DNS解析的作用

知识讲解

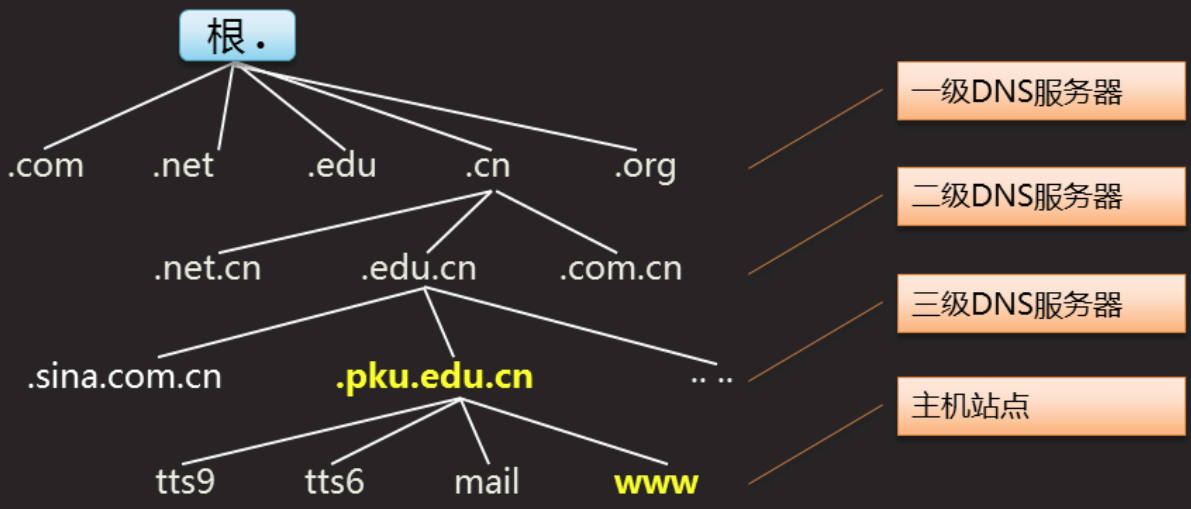
- 为什么需要DNS系统
  - www.baidu.com 与 119.75.217.56，哪个更好记？
  - 互联网中的114查号台/导航员
- DNS服务器的功能
  - 正向解析：根据注册的域名查找其对应的IP地址
  - 反向解析：根据IP地址查找对应的注册域名，不常用

DNS的分布式结构

Tedu.cn 达内教育

知识讲解

- 大型、分布式的互联网DNS解析库



DNS的分布式结构（续1）

Tedu.cn 达内教育

知识讲解

- Full Qualified Domain Name，完全合格主机名
  - = 站点名.域名后缀
  - = 站点名. .. .. .二级域.一级域

比如，www.pku.edu.cn

- 常见的顶级/一级域名
  - 国家/地区域：.cn、.us、.kr、.hk、.tw、.. ..
  - 组织域：.com、.net、.edu、.org、.gov、.mil、.. ..

DNS域名管理

知识讲解

- IANA，互联网数字分配机构
  - Internet Assigned Numbers Authority，
  - 整个域名系统的最高权威机构
  - 主管DNS根、.int、.arpa等国际化域名资源
- CNNIC，中国互联网络信息中心
  - China Internet Network Information Center
  - 主管国家顶级域 .cn

DNS域名管理（续1）

知识讲解

- 域名代理/注册/购买服务商
  - 新网，http://www.xinnet.com
  - 万网，http://www.net.cn
  - 中国互联，http://hulian.top
  - .. ..

管理申请的域名

BIND服务分析

BIND域名服务

知识讲解

- BIND（Berkeley Internet Name Daemon）
  - 伯克利 Internet 域名服务
  - 官方站点：https://www.isc.org/

```
[root@svr7 ~]# yum  -y  install  bind-chroot  bind
[root@svr7 ~]# rpm  -qa  bind*
bind-9.9.4-29.el7.x86_64                  //域名服务包
bind-chroot-9.9.4-29.el7.x86_64           //提供虚拟根支持
.. ..
```

BIND域名服务（续1）

知识讲解

- BIND服务器端程序
  - 主要执行程序：/usr/sbin/named
  - 系统服务：named
  - 默认端口：TCP/UDP 53
  - 运行时的虚拟根环境：/var/named/chroot/
- 主配置文件：/etc/named.conf
- 地址库文件：/var/named/.. ..

named.conf配置文件

知识讲解

- 全局配置部分
  - 设置监听地址/端口、地址库存放位置等

```
options {
    listen-on port 53 { 192.168.4.7; };          //监听地址和端口
    directory   "/var/named";                    //地址文件的默认位置
    allow-query   { any; };                      //允许任何客户机查询
     .. ..
    //listen-on-v6 port 53 { ::1; };
    //Include   "/etc/named.rfc1912.zones";      //可载入其他配置
};
```

清理冗余配置，三种注释方法：

#	注释一整行或行内的部分文字
//	注释一整行或行内的部分文字
/* */	可注释连续的多行文字

named.conf配置文件（续1）

Tedu.cn 达内教育

知识讲解

- 区域配置部分
  - 定义DNS区域、类型、地址文件路径等
  - 关键词 IN 表示 Internet，可省略

```
zone "tedu.cn" IN {                    //定义正向区域
    type  master;                      //区域类型为主DNS
    file  "tedu.cn.zone";              //地址库文件
};
```

named.conf配置文件（续2）

Tedu.cn 达内教育

知识讲解

- 检查配置语法
  - 格式：named-checkconf [配置文件]

```
[root@svr7 ~]# named-checkconf  /etc/named.conf
etc/named.conf:3: expected quoted string near "

[root@svr7 ~]# vim  etc/named.conf
.. ..                                  //修正错误
[root@svr7 ~]# named-checkconf  /etc/named.conf
[root@svr7 ~]#                         //无错误，无输出
```

地址库文件

知识讲解

- 全局TTL配置项及SOA记录
  - $TTL（Time To Live，生存时间）
  - SOA（Start Of Authority，授权信息开始）
  - 分号“;”开始的部分表示注释

```
@ IN SOA 区域名. 区域管理邮箱.（
    .. ..
）
```

在当前文件内，本区域名可简写为 @

地址库文件（续1）

知识讲解

- NS，域名服务器（Name Server）记录
- A，地址（Address）记录，仅用于正向解析区域

```
@       IN  NS  ns.tedu.cn.
ns      IN  A   192.168.4.7
svr7    IN  A   192.168.4.7
www     IN  A   192.168.4.100
pc207   IN  A   192.168.4.207
```

地址库文件（续2）

- 检查配置语法
  - 格式：named-checkzone 区域名 配置文件

知识讲解

```
[root@svr7 ~]# cd /var/named/
[root@svr7 named]# named-checkzone tedu.cn tedu.cn.zone
zone tedu.cn/IN: loaded serial 2013090901
OK                                          //检查未发现问题
```

单区域DNS服务

快速搭建DNS服务器

Tedu.cn 达内教育

知识讲解

- 基本思路
  1. 安装 bind、bind-chroot 包
  2.1 建立主配置文件 /etc/named.conf
  2.2 建立地址库文件 /var/named/.. ..
  3. 启动 named 服务

DNS查询测试

Tedu.cn 达内教育

知识讲解

- 为客户机设置默认使用的DNS

```
[root@pc207 ~]# vim  /etc/resolv.conf
nameserver 192.168.4.7
```

- 使用 host 测试命令，指定DNS地址
  - host 查询目标 [DNS服务器地址]

```
[root@pc207 ~]# host  www.tedu.cn
www.tedu.cn has address 192.168.4.100
```

案例1：搭建单区域DNS服务器

课堂练习

1. 提供以下正向记录的解析
   - svr7.tedu.cn ---> 192.168.4.7
   - pc207.tedu.cn ---> 192.168.4.207
   - www.tedu.cn ---> 192.168.4.100
2. 在客户机上验证查询结果

特殊解析

地址记录应用

DNS轮询

知识讲解

- 基于DNS的站点负载均衡
  - 一个域名 ---> 多个不同IP地址
  - 每个IP提供镜像服务内容

```
[root@svr7 ~]# vim  /var/named/tedu.cn.zone
.. ..
www     IN      A       192.168.4.100
www     IN      A       192.168.4.110
www     IN      A       192.168.4.120
```

//正向区域文件

泛域名解析

知识讲解

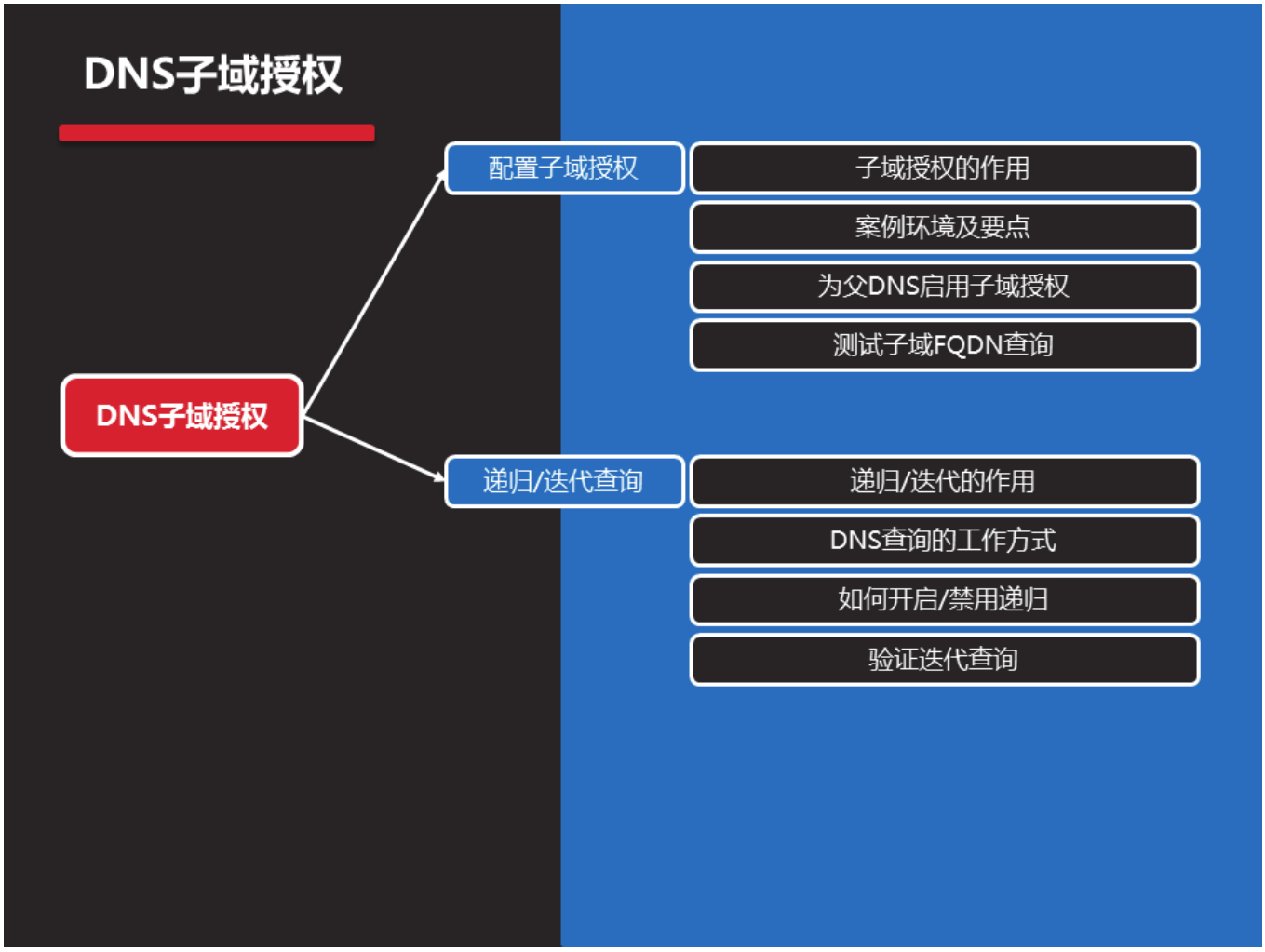
- 匹配本域内未定义的任何主机地址
  - 直接以 * 条目匹配
  - 一般只用在正向区域文件中

```
[root@svr7 ~]# vim  /var/named/tedu.cn.zone
.. ..
*                IN     A      192.168.4.100          //正向区域文件
                                                      //最后一条记录
```

案例2：特殊DNS解析

课堂练习

1. 为站点 www.tedu.cn 提供DNS轮询解析
   - 192.168.4.100、192.168.4.110、192.168.4.120
2. 配置泛域名解析实现以下解析记录
   - 任意名称.tedu.cn ---> 119.75.217.56

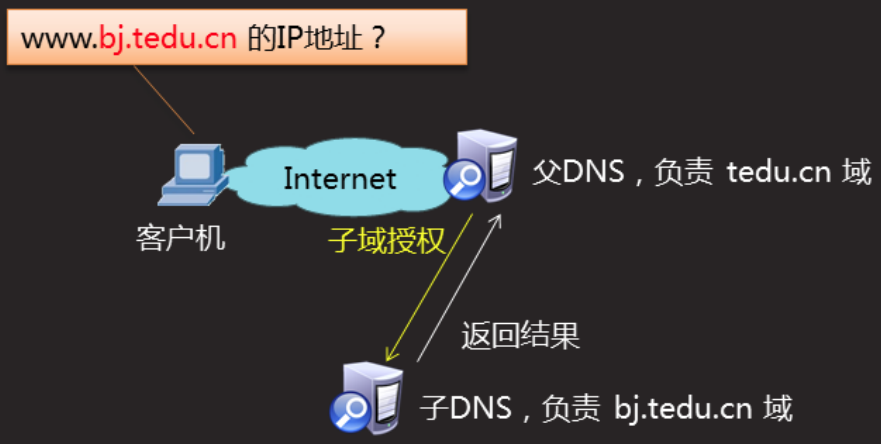

DNS子域授权
DNS子域授权
配置子域授权
子域授权的作用
案例环境及要点
为父DNS启用子域授权
测试子域FQDN查询
递归/迭代查询
递归/迭代的作用
DNS查询的工作方式
如何开启/禁用递归
验证迭代查询


Tedu.cn
达内教育
配置子域授权

子域授权的作用

知识讲解

- 适用于同一个DNS组织
  - 父/子域的解析工作由不同的DNS服务器负责
  - 父DNS服务器应该有为子域迭代的能力



案例环境及要点

知识讲解

- 子DNS：pc207.bj.tedu.cn 192.168.4.207
  - 负责 bj.tedu.cn 域的解析
- 父DNS：svr7.tedu.cn 192.168.4.7
  - 负责 tedu.cn 域的解析
  - 当客户机向父DNS查询 www.bj.tedu.cn 时，授权给子DNS处理，获得反馈结果后发给客户机

案例环境及要点（续1）

知识讲解

- 基本配置步骤
  - 1. 配置父DNS（www.tedu.cn --> 192.168.4.100）
  - 2. 配置子DNS（www.bj.tedu.cn --> 1.2.3.4）
  - 3. 在父DNS中，添加子域授权配置

    子域域名.　　IN　NS　　子DNS的FQDN.

    子DNS的FQDN.　IN　A　　子DNS的IP地址
  - 4. 测试子域FQDN查询

为父DNS启用子域授权

知识讲解

- 修改父域的地址库文件
  - 添加到子域的NS记录
  - 确保有可用的子DNS服务器的A记录

```
[root@svr7 ~]# vim  /var/named/tedu.cn.zone
.. ..
bj.tedu.cn.              IN    NS        pc207.bj.tedu.cn.
pc207.bj.tedu.cn.        IN     A        192.168.4.207

[root@svr7 ~]# systemctl  restart  named
```

测试子域FQDN查询

Tedu.cn 达内教育

知识讲解

- 向父DNS可查询子域中的站点

```
[root@svr7 ~]# host  www.bj.tedu.cn  192.168.4.7
www.bj.tedu.cn  has address 1.2.3.4
```

案例3：配置DNS子域授权

Tedu.cn 达内教育

课堂练习

实现向父DNS可查询子域的主机名

1）构建父DNS（tedu.cn）服务器
2）构建子DNS（bj.tedu.cn）服务器
3）在父DNS上配置子域授权
4）测试子域授权查询

Tedu.cn 达内教育

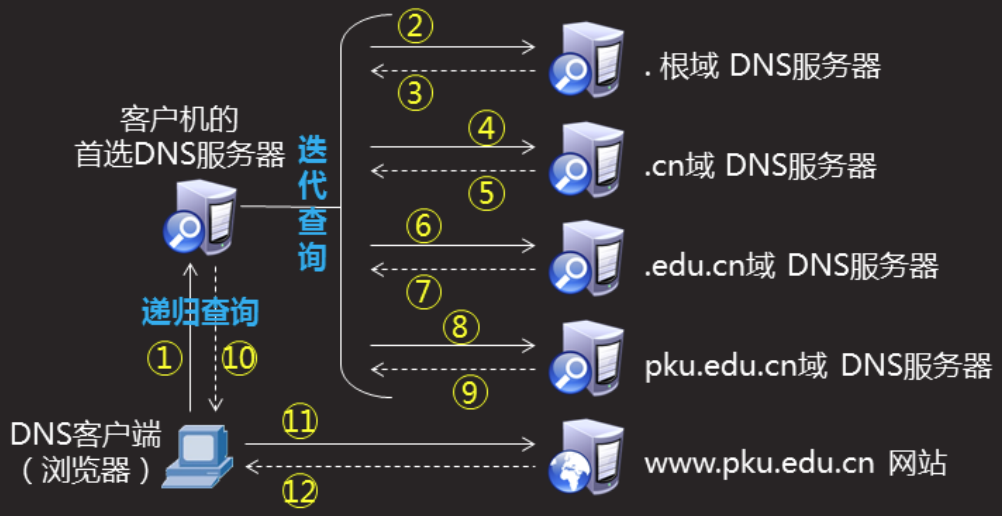
递归/迭代查询

Tedu.cn 达内教育

DNS查询的工作方式

- 如何获取解析结果？

知识讲解



如何开启/禁用递归

知识讲解

- 递归查询是默认开启的
  - 也可以设置 recursion yes; 来明确启用
- 若要禁止递归
  - 需要设置 recursion no;

```
[root@svr7 ~]# vim /etc/named.conf
options {
        directory "/var/named";
        recursion no;                                    //禁用递归
};
.. ..
```

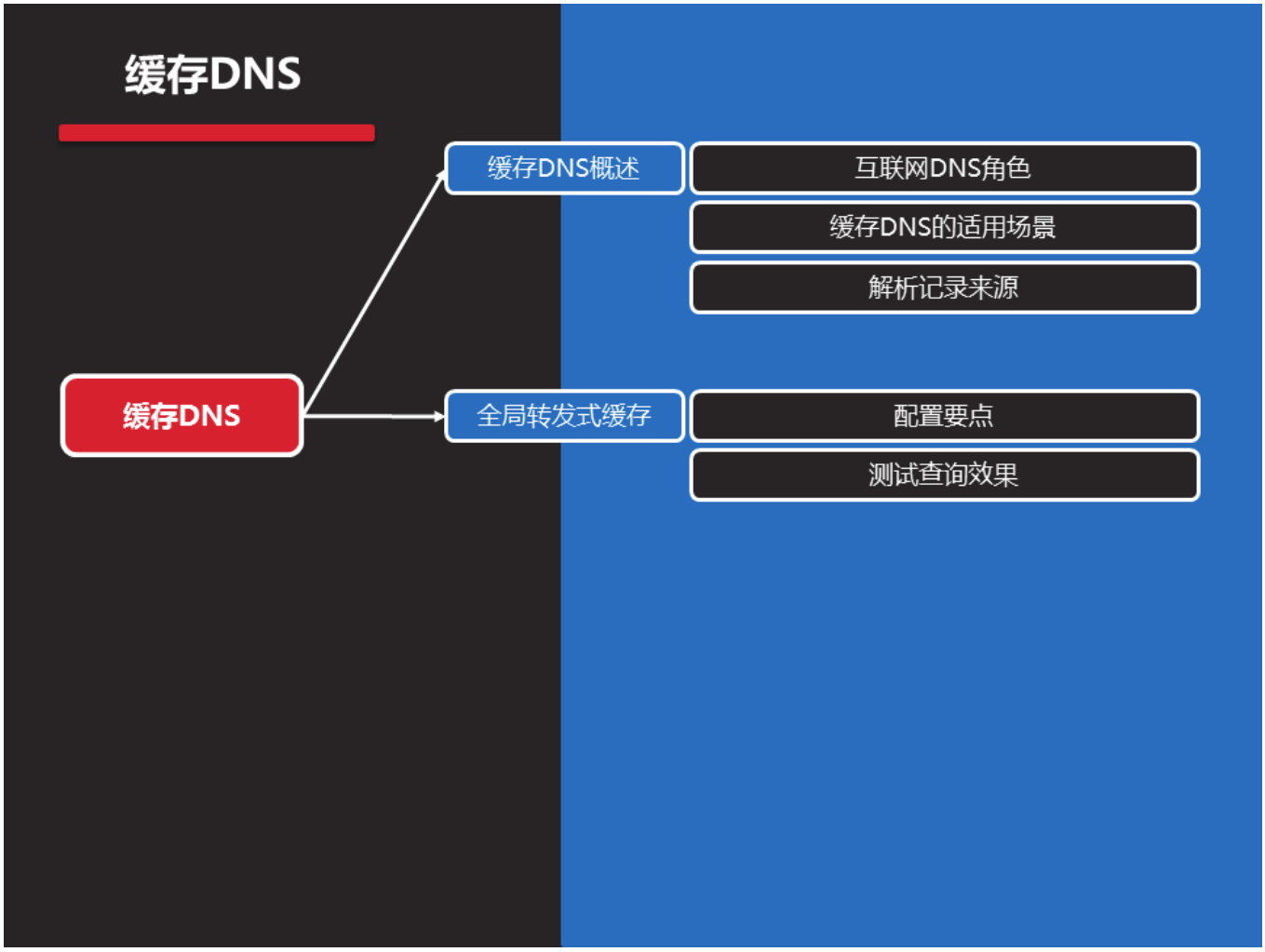
验证迭代查询

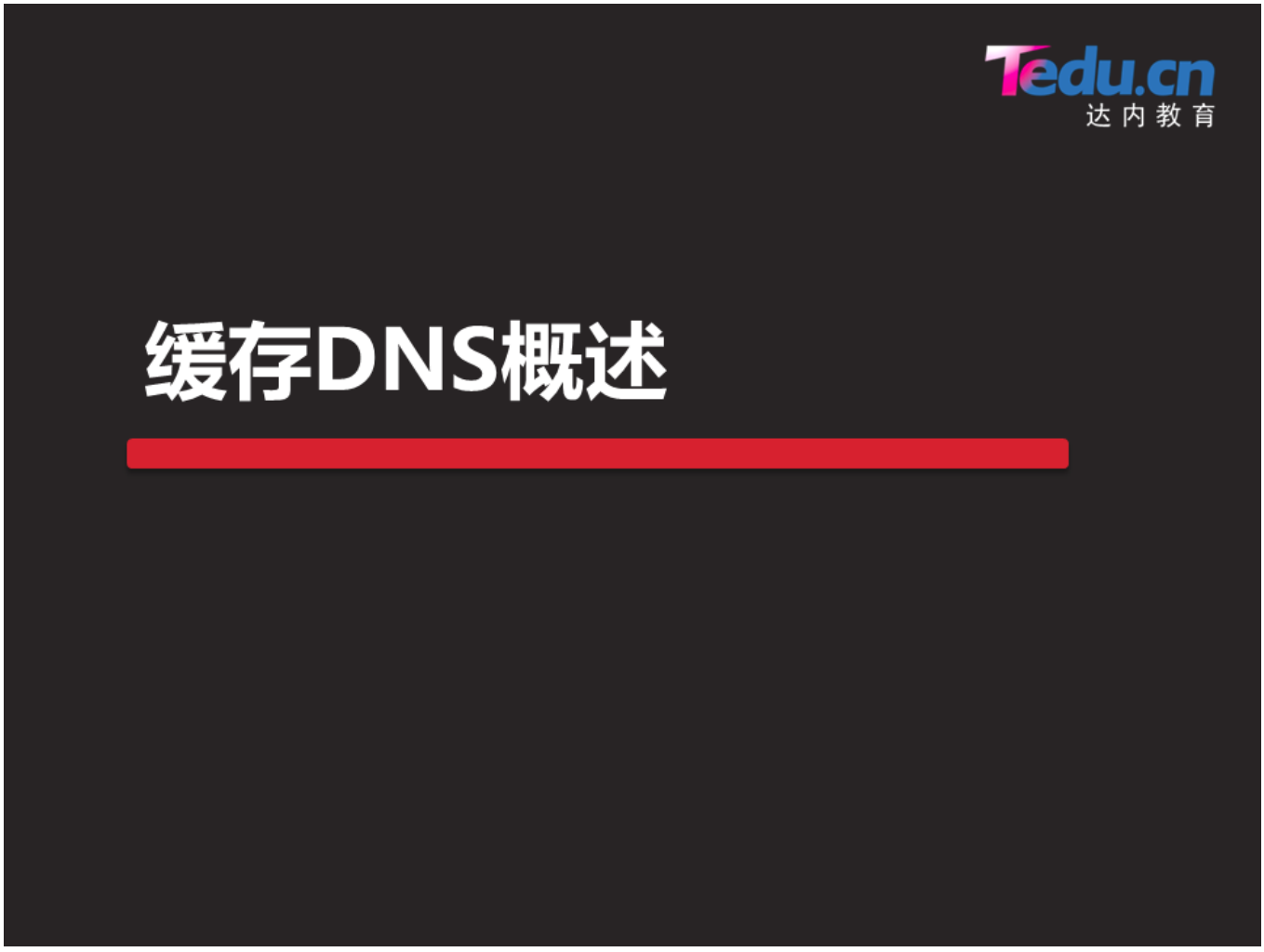
知识讲解

- dig命令，更专业的DNS测试工具
  - 由软件包 bind-utils 提供
  - 格式： dig @DNS服务器 目标地址

```
[root@svr7 ~]# dig @192.168.4.7 www.bj.tedu.cn
.. ..
;; AUTHORITY SECTION:
bj.tedu.cn.        86400   IN      NS      pc207.bj.tedu.cn.

;; ADDITIONAL SECTION:
pc207.bj.tedu.cn.    86400   IN      A       192.168.4.207
.. ..
```


缓存DNS
缓存DNS
缓存DNS概述
互联网DNS角色
缓存DNS的适用场景
解析记录来源
全局转发式缓存
配置要点
测试查询效果


Tedu.cn
达内教育
缓存DNS概述

互联网DNS角色

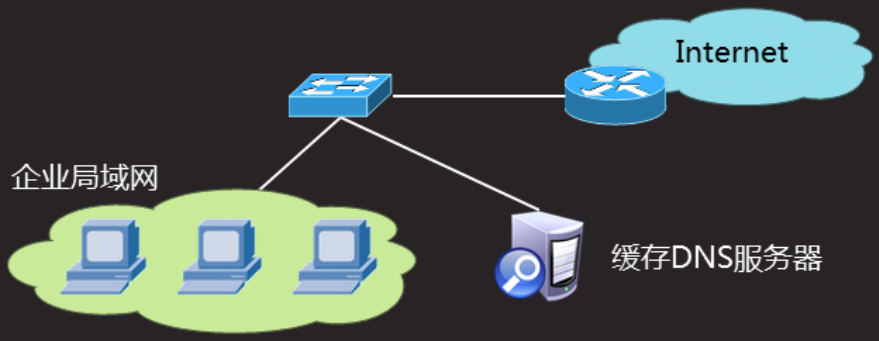
知识讲解

- 权威/官方DNS
  - 至少管理一个DNS区域，，需要IANA等官方机构授权
  - 典型应用：根域DNS、一级域DNS、.. ..
- 缓存DNS
  - 不需要管理任何DNS区域，但是能够替客户机查询，而且通过缓存、复用查询结果来加快速度
  - 典型应用：ISP服务商、企业局域网

缓存DNS的适用场景

知识讲解

- 主要适用环境
  - 互联网出口带宽较低的企业局域网络
  - ISP服务商的公共DNS服务器



解析记录来源

知识讲解

- 方式1：全局转发
  - 将请求转发给指定的公共DNS（其他缓存DNS），请求递归服务
- 方式2：根域迭代
  - 依次向根、一级、二级……域的DNS服务器迭代

全局转发式缓存

配置要点

知识讲解

- 基本配置步骤
  - 1. 建立 named.conf 主配置文件
    —— 设置 forwarders { 公共DNS; }; 转发器
  - 2. 启动named服务
  - 3. 验证缓存DNS服务器

配置要点（续1）

知识讲解

- 添加转发器，并启用named服务
  - 以转发至 202.106.0.20、8.8.8.8 为例
  - 前提条件：缓存DNS与上述DNS之间网络畅通

```
[root@pc207 ~]# vim  /etc/named.conf
options {
        directory  "/var/named";
        forwarders { 202.106.0.20; 8.8.8.8; };
};

[root@pc207 ~]# systemctl  restart  named
```

测试查询效果

Tedu.cn 达内教育

知识讲解

- 前提条件及效果
  - 只要 202.106.0.20、8.8.8.8 能提供的解析记录
  - 向本例中的缓存DNS一样可以查到

```
[root@pc207 ~]# host  www.baidu.com  192.168.4.207
Using domain server:
Name: 192.168.4.207
Address: 192.168.4.207#53
Aliases:

www.baidu.com is an alias for www.a.shifen.com.
www.a.shifen.com has address 111.13.100.92
www.a.shifen.com has address 111.13.100.91
```

案例4：搭建并测试缓存DNS

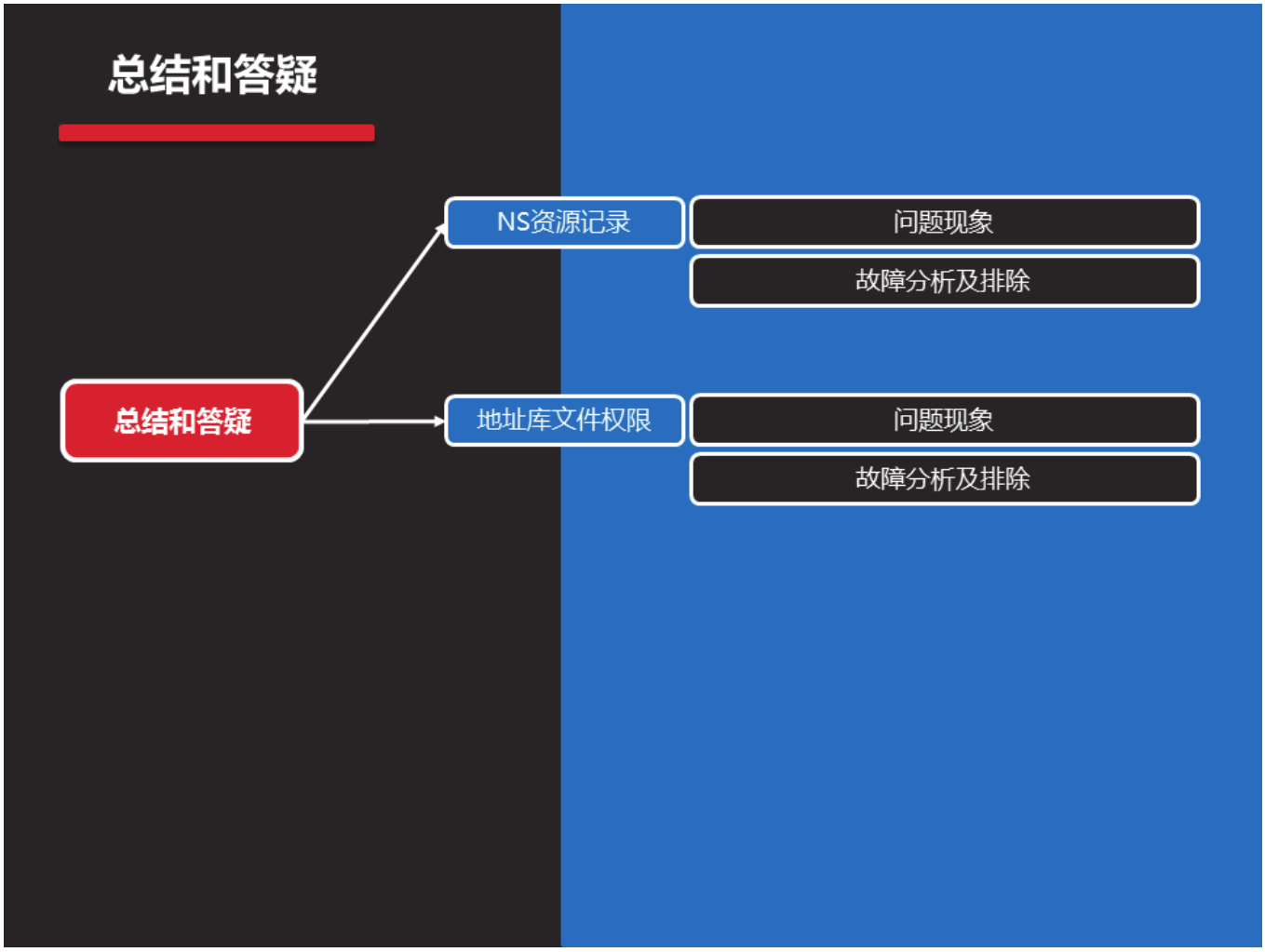
Tedu.cn 达内教育

课堂练习

准备一台桥接可上网的RHEL7虚拟机

1）安装 bind、bind-chroot 包

2）搭建并测试基于全局转发器的缓存DNS


总结和答疑
总结和答疑
NS资源记录
问题现象
故障分析及排除
地址库文件权限
问题现象
故障分析及排除


Tedu.cn
达内教育
NS资源记录

问题现象

知识讲解

- 启动named服务时失败
  - 报错：NS '.. ..' has no address records (A or .. ..)
  - 语法检查报同样的错误

```
[root@svr7 named]# service named start
启动 named：
Error in named configuration:
zone tedu.cn/IN: NS 'svr7.tedu.cn' has no address records (A or
AAAA)
zone tedu.cn/IN: not loaded due to errors.
_default/tedu.cn/IN: bad zone
                                                    [失败]
```

故障分析及排除

知识讲解

- 原因分析
  - NS记录用来标记本区域DNS服务器的地址（接收地址库更新通知）
  - 如果该地址正好隶属本区域，则需要增加相应A记录
- 解决办法
  - 指定 NS 记录时，同时设置配套的A记录即可

```
@       NS      svr7.tedu.cn.
svr7    A       192.168.4.7
```

地址库文件权限

问题现象

- 启动named服务成功，但host查询没有结果
  - 报错1：connection timed out ; no servers .. ..
  - 报错2：Host .. .. not found: 2(SERVFAIL) .. ..

知识讲解

```
[root@pc207 ~]# host  svr7.tedu.cn
;; connection timed out; trying next origin
;; connection timed out; no servers could be reached

[root@pc207 ~]# host svr7.tedu.cn  192.168.4.7
.. ..
Host svr7.tedu.cn.tarena.com not found: 2(SERVFAIL)
```

故障分析及排除

Tedu.cn 达内教育

知识讲解

- 原因分析
  - 问题1：客户机未正确指定DNS，无法查询
  - 问题2：DNS地址库中不包括要查询域名的A记录，或者named服务对地址库文件没有 r 权限
- 解决办法
  - 为客户机正确设置 /etc/resolv.conf 文件
  - 确认存在该站点记录，并调整地址库文件权限 644

```
[root@svr7 named]# ls  -lh  tedu.cn.zone
-rw-r-----. 1 root  named  162 3月  25 20:35 tedu.cn.zone
```