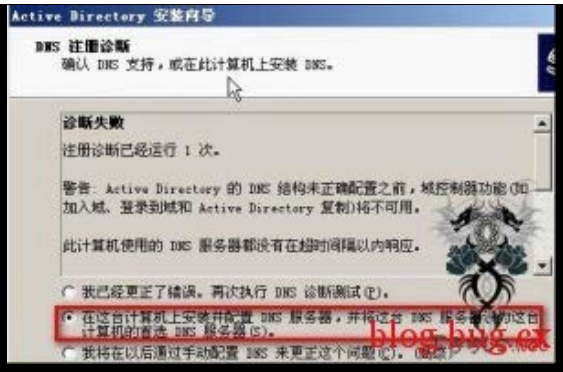
关于域控的经验分享
----答IT民工问
1如何寻找域控？
方法一 ipconfig /all 找到

域名就是openlab.cn
nslookup openlab.cn 就可以列出所有的域控制器IP

方法二 登录域控制器-->用户和计算机 （需要管理员权限）

可以看到所有域控的计算机名。
方法三 脚本
★
```
set obj=GetObject("LDAP://rootDSE")
wscript.echo obj.servername
```
★
后缀保存为vbs。
方法四 注释
在域内的任意一台机器上执行net view /domain
Server Name Remark
\\2109-DA3773A363 Domain Controller
\\XIN-5EE4B4EE10B SH Domain Controller
这个方法全凭运气，管理员要是懒得话，谁也没办法。
注意:
1在3389登录一个IP时候，有"选择到"这个选项，域控的下拉列表中只有域名，而普通的机器有computer name（this computer）这一选项。可以利用这一点来判断是否是域控。
2大多数域，DNS服务器和DC很有可能是同一台机器，找到了DNS就找到了域控。



（安装域控的时候，默认把第一台当做DNS服务器。）
3如果一个域中含有子域，那么上述所有的方法中会连子域的域控列出来。这对寻找主域控是不利的。
解决办法使用ping -a IP 得到两台主机的主机名。

比较两个主机名可以得出 192.168.200.102是子域。