一、内网基础知识

1、内网概述

内网也指局域网(Local Area Network，LAN)是指在某一区域内由多台计算机互联成的计算机组，一般是方圆几千米以内。局域网可以实现文件管理、应用软件共享、打印机共享、工作组内的日程安排、电子邮件和传真通信服务等功能。

内网是封闭的，它可以由办公室内的两台计算机组成，也可以由一个公司内的上千台计算机组成。例如：银行、学校、企业工厂、政府机关、网吧、单位办公网等都属于此类。

在研究内网的时候，经常会听说一些例如"工作组"、"域"、"域控制器(DC)"、“父域”、“子域”、“域树”、“域森林”和“活动目录(AD)”、“DMZ”、“域内权限”等专有名词。那么它们到底指的是什么？又有何区别呢？这就是本节所要讲解的内容。

2、工作组(Work Group)

在一个大的单位内，可能有成百上千台电脑互相连接组成局域网，它们都会列在“网络(网上邻居)”内，如果这些电脑不分组，可想而知有多么混乱，要找一台电脑很困难。为了解决这一问题，就有了“工作组”这个概念，将不同的电脑一般按功能(或部门)分别列入不同的工作组中。

例如：技术部的计算机都列入“技术部”工作组中、行政部的计算机都列入“行政部”工作组中。要访问某个部门的资源，就在“网络”里找到那个部门的工作组名，双击就可以看到那个部门的所有计算机了。相比不分组的情况就有序很多了，尤其是对于大型局域网来说。

(1)、加入/创建工作组的方法

鼠标右键桌面上的“此电脑”，在弹出的菜单中选择“属性”，点击“重命名这台电脑”，点击“更改”，在“计算机名”一栏中输入想好的计算机名称，在“工作组”一栏中输入想加入的工作组名称。

如果输入的工作组名称网络中没有，那么相当于新建了一个工作组，当前暂时只有你自己的计算机在组内。单击“确定”按钮后，Windows 提示需要重新启动，重新启动之后，再进入“网络”就可以看到你所加入的工作组成员了。

(2)、退出工作组

只需要将工作组名称改动即可。不过在网上别人依然可以访问你的共享资源。你也可以随便加入同一网络上的任何其它工作组。“工作组”就像一个可以自由进入和退出的“社团”，方便同一组的计算机互相访问。

工作组并不存在真正的集中管理作用，工作组里的所有计算机都是对等的，没有服务器和客户机之分。

3、域(Domain)

域(Domain)：一个有安全边界的计算机集合(安全边界：在两个域中，一个域中的用户无法访问另一个域中的资源)，可以简单的把域理解成升级版的“工作组”，相比工作组而言，它有一个更加严格的安全管理控制机制，如果你想访问域内的资源，必须拥有一个合法的身份登录到该域中，而你对该域内的资源拥有什么样的权限，需要取决于你在该域中的用户身份。

(1)、域控制器(Domain Controller，DC)

域控制器(Domain Controller，简写为 DC)是一个域中的一台类似管理服务器的计算机，相当于单位的门卫一样，它负责每一台联入的计算机和用户的验证工作，域内计算机如果想互相访问首先都要经过它的审核。

(2)、域的分类

单域
父域、子域
域树(tree)
域森林(forest)
DNS 域名服务器

(3)、单域

在一般的具有固定地理位置的小公司里，建立一个域就可以满足所需。

一般在一个域内要建立至少两个域服务器，一个作为 DC，一个作为备份 DC。如果没有第二个备份 DC，那么一旦 DC 瘫痪，则域内的其他用户就不能登录该域，因为活动目录的数据库(包括用户的账号信息)是存储在 DC 中的。而有一台备份域控制器(BDC)，则至少该域还能正常使用，期间把瘫痪的 DC 恢复即可。

(4)、父域和子域

出于管理及其他一些需求，需要在一个域中划分出多个域，被划分的域称为**父域**，划分出来的各分部域称为该域的**子域**。

比如一个大公司的各部分位于不同的地理位置，这种情况下就可以把不同位置的部门分别放到不同的子域，然后部门通过自己的域来管理相应的资源，并且每个子域都能拥有自己的安全策略。

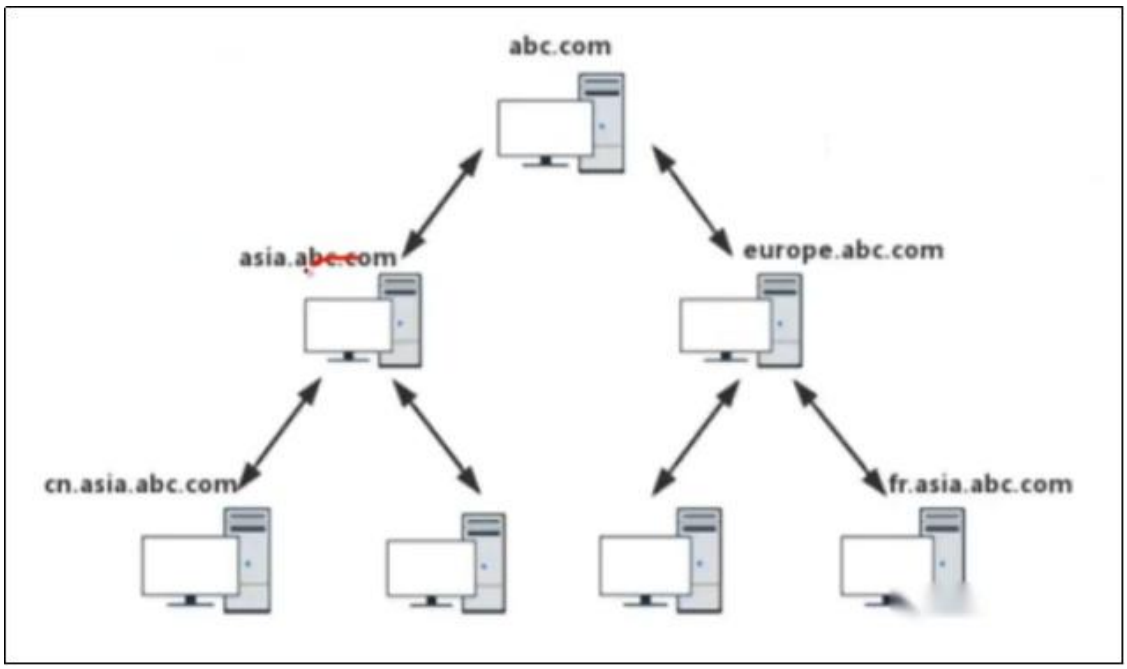
从域名看，子域是整个域名中的一个段。各子域之间使用"."来分割，一个"."就代表域名的一个层级。

(5)、域树

域树：若干个域通过建立信任关系组成的集合。一个域管理员只能管理本域的内部，不能访问或者管理其他的域，两个域之间相互访问则需要建立信任关系(Trust Relation)

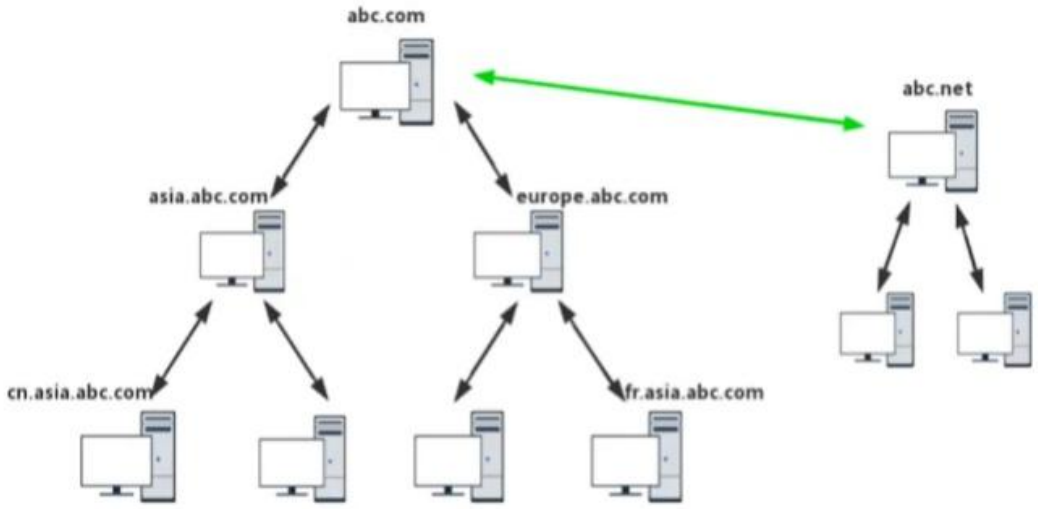
信任关系是连接在域和域之间的桥梁。域树内的父域和子域之间不但可以按需要相互进行管理，还可以跨网分配文件和打印机等设备资源，使不同的域之间实现网络资源的共享与管理，以及相互通信和数据传输。

在一个域树中，父域可以包含很多子域，子域是相对父域来说的，指域名中的每一个段。子域只能使用父域作为域名的后缀，也就是说在一个域树中，域的名字是连续的。



(6)、域林

域林：若干个域树通过建立信任关系组成的集合。可以通过域树之间建立的信任关系来管理和使用整个域森林中的资源，从而又保持了原有域自身原有的特性。



(7)、域名服务器(Domain Name Server)

DNS 域名服务器是进行域名(Domain Name)和与之相对应的 IP 地址(IP Address)转换的服务器。

域树中的域的名字和 DNS 域的名字非常相似，实际上域的名字就是 DNS 域的名字，因为域中的计算机使用 DNS 来定位域控制器和服务器以及其他计算机、网络服务等。

一般情况下，我们在内网渗透时就通过寻找 DNS 服务器来定位域控制器，因为通常 DNS 服务器和域控制器会处在同一台机器上。

(8)、Ntds.dit 文件

`Ntds.dit` 文件是域环境的域控制器上保存的一个二进制文件，最主要的活动目录数据库，其文件路径为域控制器的`%SystemRoot%\ntds\ntds.dit`。`Ntds.dit` 文件中包括但不限于有关域用户、用户密码的哈希散列值、用户组、组成员身份和组策略信息。`Ntds.dit` 文件使用存储在系统 SYSTEM 文件的密钥对这些 hash 值进行加密。

而在非域环境即工作组环境中，用户的登录凭据等信息存储在本地 SAM 中。

4、活动目录(Active Directory，AD)

活动目录(Active Directory)是安装在域控制器上，为整个域环境提供集中式目录管理服务的组件。活动目录存储了有关域环境中各种对象的信息，如域、用户、用户组、计算机、组织单位、共享信息、安全策略等。目录数据存储在域控制器的 `ntds.dit` 文件中，活动目录提供了以下功能。

计算机集中管理：集中管理所有加入域的服务器及客户端计算机，统一下发组策略。
用户集中管理：集中管理域用户、组织通讯录、用户组、对用户进行统一的身份认证、资

源授权等。
资源集中管理：集中管理域中的打印机，文件共享服务等网络资源。
环境集中管理：集中的配置域中计算机的工作环境，如统一计算机桌面、统一网络连接配置，统一计算机安全配置等。
应用集中管理：对域中的计算机统一推送软件，安全补丁，防病毒系统，安装网络打印机等。

(1)、逻辑结构

在活动目录中，管理员可以完全忽略被管理对象的具体地理位置，而将这些对象按照一定的方式放置在不同的容器中。由于这种组织对象的做法不考虑被管理对象的具体地理位置，这种组织框架称为“逻辑结构”。

活动目录的逻辑结构就包括**组织单元(OU)、域(Domin)、域树(Tree)、域森林(Forest)**。

在域树内的所有域共享一个活动目录，这个活动目录内的数据分散地存储在各个域内，且每一个域只存储该域内的数据。

(2)、域控制器(DC)和活动目录(AD)的区别

如果网络规模较大，我们就会考虑把网络中的众多对象：计算机、用户、用户组、打印机、共享文件等，分门别类、井然有序地放在一个大仓库中，并做好检索信息，以利于查找、管理和使用这些对象(资源)。这个有层次结构的数据库，就是活动目录数据库，简称“AD”库。

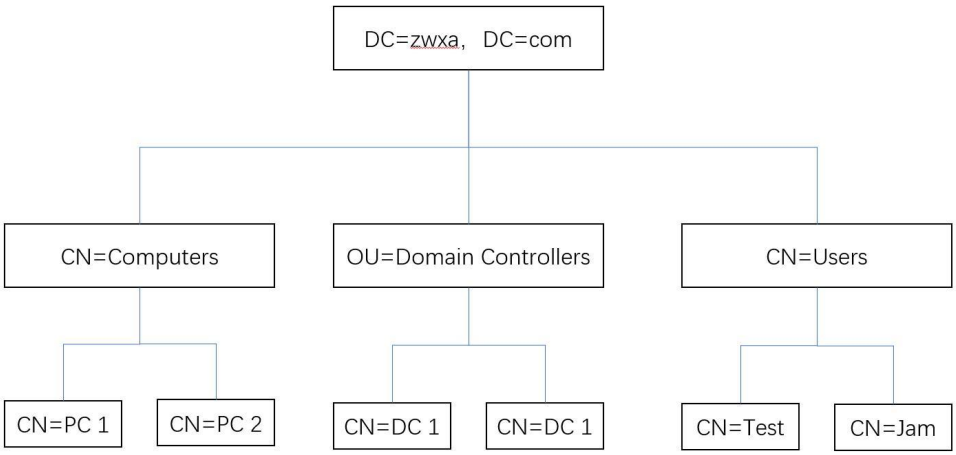
那么，我们应该把这个数据库放在哪台计算机上呢？我们把存放有活动目录数据库的计算机称为 DC。所以我们要实现域环境，其实就是要安装 AD，当内网中的一台计算机安装了 AD 后，它就变成了 DC。

(3)、目录服务和 LDAP

活动目录是一种目录服务数据库，区别于常见的关系型数据库。目录数据库实现的是目录服务，是一种可以帮助用户快速、准确地从目录中找到所需要信息地服务。目录数据库将所有数据组织成一个有层次地树状结构，其中地每个节点都是一个对象，有关这个对象地所有信息作为这个对象地属性被存储。用户可以根据对象名称去查找这个对象的所有有关信息。

LDAP(Lightweight Directory Access Protocol，轻量目录访问协议)是设用来访问目录服务数据库的一个协议。活动目录就是利用 LDAP 名称路径来描述对象在活动目录中的位置。

下图所示就是一个目录服务数据库，在整体上呈现一种极具层次的树状结构来组织数据。



(a)、目标树：在一个目录服务数据库中，整个目录信息集可以表示为一个目录信息树，树中的每个节点是一个条目。
(b)、条目：每个条目就是一条记录，每个条目有自己的唯一可区别的名称（CN）。比如图中的每个方框都是一条记录。
(c)、DN(Distinguished Name，绝对可辨识名称)：指向一个 LDAP 对象的完整路径。DN 由对象本体开始，向上延伸到域顶级的 DNS 命名空间。CN(Common Name，通用名),OU(Organizational Unit，组织单位),DC(Domain Component，域组件)。如上图中，CN=DC 1 的 DN 绝对可辨识名称为： CN=DC1,OU=Domain Controllers,DC=Zwxa,DC=com。其含义是 DC1 对象在 zwxa.com 域的 Domain Controllers 组织单元中，类似文件系统目录中的绝对路径，其中 CN=DC 1 代表这个主机的一个对象，OU=Domain Controllers 代表一个 Domain Controllers 组织单位。
(d)、RDN(Relative Distinguished Name，相对可辨识名称)：用于指向一个 LDAP 对象的相对路径，比如 CN=DC 1 条目的 RDN 就是 CN=DC 1
(e)、属性：用于描述数据库中每个条目的具体信息。

5、安全域的划分

划分安全域的目的是将一组安全等级相同的计算机划入同一个网段内，这一网段内的计算机拥有相同的网络边界，在网络边界上采用防火墙部署来实现对其他安全域的 NACL(网络访问控制策略)，允许哪些 IP 访问此域、不允许哪些 IP 访问此域；允许此域访问哪些 IP/网段、不允许访问哪些 IP/网段。使得其风险最小化，当发生攻击时可以将威胁最大化的隔离，减少对域内计算机的影响。

6、DMZ

DMZ 称为“隔离区”，也称“非军事化区”。是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。

这个缓冲区位于企业内部网络和外部网络之间的小网络区域内，在这个小网络区域内可以放置一些必须公开的服务器设置，如企业 Web 服务器、FTP 服务器和论坛等。

另一方面，通过这样一个 DMZ 区域，更加有效地保护了内部网络，因为这种网络部署，比起一般的防火墙方案，对攻击者来说又多了一道关卡。

(1)、DMZ 的屏障功能

a、内网可以访问外网
内网的用户需要自由地访问外网。在这一策略中，防火墙需要执行 NAT。

b、内网可以访问 DMZ
此策略使内网用户可以使用或者管理 DMZ 中的服务器。

c、外网不能访问内网
防火墙的基本策略，内网中存放的是公司内部数据，显然这些数据不允许外网的用户进行访问。如果要访问，就要通过 VPN 方式来进行。

d、外网可以访问 DMZ
DMZ 中的服务器需要为外界提供服务，所以外网必须可以访问 DMZ。同时，外网访问 DMZ 需要由防火墙完成对外地址到服务器实际地址的转换。

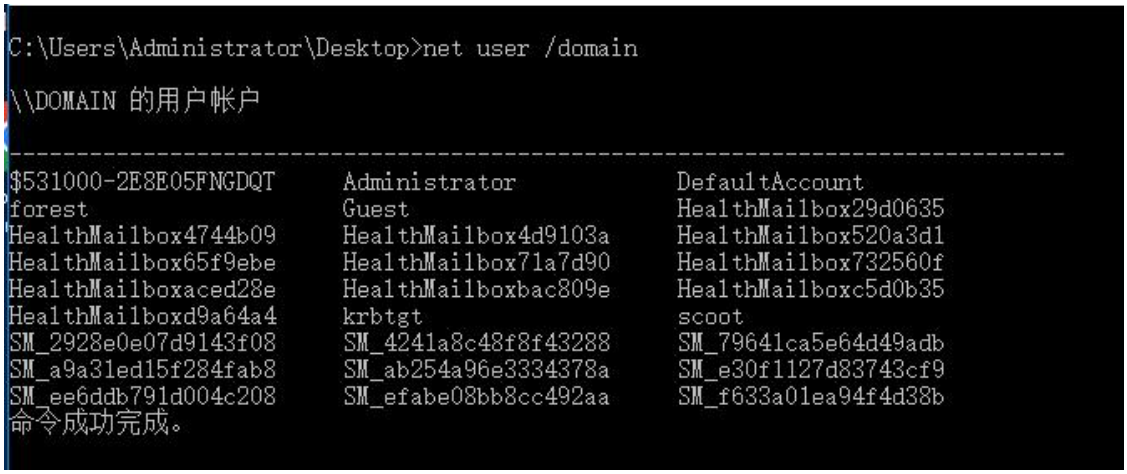
e、DMZ 不能访问内网
如不执行此策略，则当入侵者攻陷 DMZ 时，内网网络将不会受保护。

f、DMZ 不能访问外网
此策略也存在例外，比如：在 DMZ 中放置邮件服务器时，就需要访问外网，否则将不能正常工作。

7、*域用户与机器用户*

(1)、域用户

域用户，就是域环境中的用户，在域控制器中被创建，并且其所有信息都保存在活动目录中。域用户账户位于域全局组的 Domain Users 中，而计算机本地用户账户位于本地 User 组中。当计算机加入域时，全局组 Domain Users 会被添加到计算机本地的 Users 组中。因此，域用户可以在域的任何一台计算机上登录。执行以下命令:net user /domain 可以查看域中的所有域用户。



(2)、机器用户

机器用户是一种特殊的域用户。查询活动目录时随便选中 Domain Computer 组的一台机器账户，查看其 objectClass 属性便可以发现该对象是 Computer 类的示例，并且 Computer 是 user 的子类，说明域用户有的属性，机器用户都有。

在域环境中，计算机上的本地用户 SYSTEM 对于域中的机器账户，在域中的用户名就是机器名+$。net group "domain computers" /domain 可以查看域中所有的机器用户。

8、域用户组的分类和权限

在域环境中，为了方便对用户权限进行管理，需要将具有相同权限的用户划为一组。这样，只要对这个用户组赋予一定的权限，那么该组内的用户就获得了相同的权限。

(1)、组的用途

组(Group)是用户账户的集合，按照用途，可以分为通讯组和安全组。

通讯组就是一个通信群组。例如，把某部门的所有员工拉进同一个通讯组，当给这个通讯组发信息时，组内的所有用户都能收到。

安全组则是用户权限的集合。例如，管理员在日常的网络管理中，不必向每个用户账户都设置单独的访问权限，只需要创建一个组，对这个组赋予特权，再将需要该特权的用户拉进这个组即可。

(2)、安全组权限

根据组的作用范围，安全组可以分为域本地组、通用组和全局组。这里的作用范围指的是组在域树或域林中应用的范围。域本地组：来自全林用于本域。全局组：来自本域作用于全林。通用组：来自全林用于全林

域本地组：作用与本域，主要用于访问同一个域中的资源。域本地组只能够访问本域中的资源

全局组：单域用户访问多域资源(必须是同一个域里面的用户)。只能在创建该全局组的域上进行添加用户和全局组，可以在域林中的任何域中指派权限，全局组可以嵌套在其他组中。

通用组：通用组成员来自域林中任何域中的用户账户、全局组和其他的通用组，可以在该域林中的任何域中指派权限，可以嵌套于其他域组中。非常适于域林中的跨域访问。

9、Kerberos 认证协议

(1)、相关名词

域控制器（Domain Controller，DC）：在域中至少有一台服务器负责每一台联入网络的电脑和用户的验证工作，相当于一个单位的门卫一样。

密钥分发中心（Key Distribution Center，KDC）：KDC 维护着域中所有安全主体（Security Principal）账户信息数据库，负责管理票据、认证票据、分发票据。

帐户数据库（Account Database，AD）：一个类似于 Windows 本机 SAM 的数据库，存储了域内所有网络对象的凭证，也存储所有 Client 的白名单，在白名单中的 Client 才可以申请到 TGT。

身份验证服务（Authentication Service，AS）：用于生成 TGT 的服务。

票据发放服务（Ticket Granting Service，TGS）：用于生成某个服务的 ticket

票据许可票据（Ticket Granting Ticket，TGT）：可以理解为入场券，通过入场券能够获得票据，是一种临时凭证的存在。

票据（Ticket）：网络对象互相访问的凭证。

Master Key：长期密钥（被 Hash 加密的用户密钥），这里指 NTLM Hash，简单理解就是 Windows 加密过的密码口令。

Session Key ：短期会话密钥。

krbtgt 账户：每个域控制器都有一个 krbtgt 的用户账户，是 KDC 的服务账户，用来创建票据授予服务(TGS)加密的密钥。

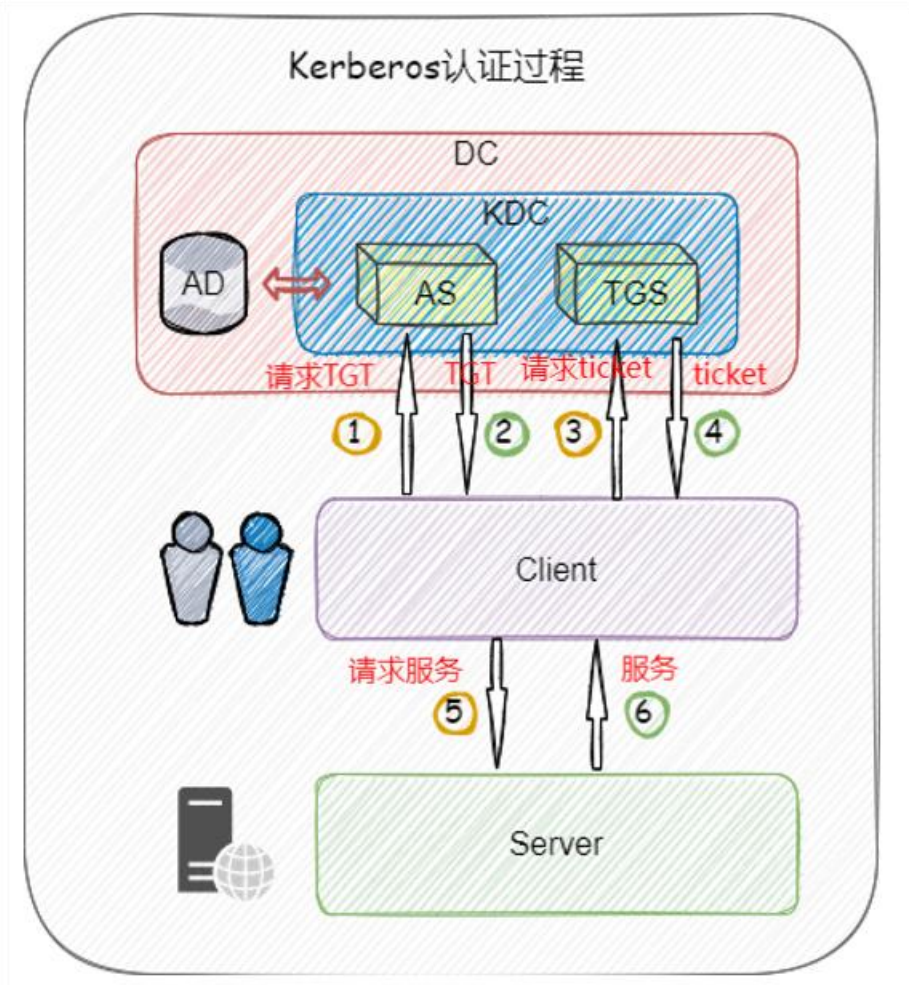
(2)、Kerberos 中的角色

Client：客户端

Server：需要访问的服务

KDC (DC)：认证服务器，一般为域控制器（DC）

(3)、认证过程



1）Client 向 KDC（认证服务器）的 AS（身份验证服务）服务发送请求，希望获取访问 Server 的权限。 KDC 收到请求后，通过在帐户数据库 AD 中存储的黑名单和 白名单来区分 Client 是否可信。确认成功后，AS 返回 TGT（票据许可票据）给 Client。

2）Client 得到了 TGT 后，继续向 KDC 的 TGS（票据发放服务）服务发送请求，希望获取访问 Server 的权限。KDC 通过客户端请求信息中的 TGT 判断客户端是否拥有权限，确认成功返回访问 Server 的权限 ticket。

3）Client 得到 ticket 后，Client 与 Server 二者进行相互验证，成功后，Client 就可以访问 Server 的资源。