通过上面的案例，我们发现：目前国内信息化项目此起彼伏，而企业内部网络的安全规划则是我们的重中之重。

而我们却习惯性的认为安全就要靠防火墙，安全就要靠杀毒软件。殊不知这些都是解决表面问题的手段。

一个真正意义上安全的网络首先是需要一个安全强壮的网络拓扑结构，其次是基于强壮骨架之上的服务。而我们所面对的安全问题从应用层去解决的方法其实就在我们所熟知的micsoft产品中---windows域。

在基于域环境的计算机管理手段中策略正式我们强行管理企业内部网络的钢铁法则。域环境之所以强大，之所以安全也正是域的管理模式是基于法则的。

一个社会之所以安定，是要一部不断健全的法律来支持的。而我们windows域环境正是以这样的结构和方式去对域中的计算机、帐户等资源进行统一集中管理的。今天抛砖引玉，以这样的方案提出了域的概念，而对域更深层次的理解以及更详细的应用，请见下篇：《深入理解域概念之开国篇》

要创建windows域，就要弄明白什么是windows域，windows域可以解决什么问题。要弄明白什么是windows域，就要先来一起回顾一下工作组：

首先,工作组中,每一台计算机都独立维护自己的资源,不能集中管理所有网络资源

其次,每一台计算机都在本地存储用户的帐户

第三,一个账户只能登陆到一台计算机

第四,工作组中计算机都是平等的,对于其他计算机来说即是服务器,也是客户机

第五,工作组的网络规模一般少于10台计算机.

成都有条很有名的步行街，里面有个派出所，早期的时候8台计算机，工作组管理模式。网络配置很轻松,几乎不用管理.哪台机器有问题就去哪来机器上解决.工作强度也不是很大. 不到3个月时间.随着信息化的深入,公司的计算机台数增加到了50台.网管员采用同样的管理方式. 每天都很忙碌,从早上到公司到晚上离开,一直在解决网络中用户的计算机故障问题,病毒\IE首页篡改\甚至出现了公司内部恶意攻击的事件,经常晚上加班,通宵达旦的工作.但问题总是解决不了。

一个月后,他被辞退了。

为什么会这样呢?有没有更简单方便的管理方式呢?

下面我们来看这么个例子:

如果我们把工作组看成是原始社会,各服务器(人)各自为政

再想想刚刚的例子,小张公司的8台电脑最开始都是各自为政的,

所以就不存在管理的概念,

小张只能充当一个哪里出问题就去哪解决的故障排除机器般的被动角色.

那么在网络日益应用广泛,结构越来越复杂的今天,我们可不可以,让我们的计算机网络世界也进化一下呢?

比如在计算机中通过网络成立一个国家,在公司的一定范围内实现集中管理,中央集权!!

(微软替我们想到了这一点,也做到了这一点,从微软的NT时代就提出的域的概念,演化到现在也就是我们的单域环境.)

一个国家可以管理的范围只在一个国家内(适合一些规模小,地域范围跨度小的公司),想做更复杂范围更广阔的管理,需要什么样的体制呢?

感谢地球,因为我们有联合国,欧盟.

实现多个基本管理范围(国家,域)的联合管理.减少这些基本管理范围内的重复管理工作.

方便相互之间资源调用。(也就是现在域森林多域的网络环境为当今的跨地域性企业提供了高效适合管理的网络管理方式.)

那么我们继续刚刚的例子,来看看活动目录域的定义：

首先谁能加入联合国(活动目录中能放哪些对象)

其次共同遵守的设定和规则(通用性设定)

第三不干涉别国内政(各域数据原则上由该数据所在的域进行管理)

我们何以把活动目录当作一个联合国,其中包括了所有的成员国信息,大家遵守统一的规则,每个成员国各自管理自己的国家。

那么每个成员国以及每个国家中的人(域和域中的计算机)如何去其他国家呢,走什么样的路线呢?国家与国家之间又怎样联系彼此呢?

DNS这个具有全球定位系统服务的管理机构,也就是我们的联合国管理委员会,帮助我们解决了这个问题。

准确的定位各个国家的位置,并为各个国民提供了方便的查询服务.

我们想要去某个国家,想在某个国家内享受一个国民的基本权利,比如取得这个国家提供的最低生活保证金(访问域中的网络资源:如共享文件,打印),就连想要加入某个国家国籍(加入域)都必须通过DNS这个机构为我们指引。

有的人容易把域林域树子域的概念搞混

那么在这里提出来再解释一下：

结构关系:域林和树可以看成我们的联合国和成员国(国家内的省,省内的县市,县市内的村子) 这种管理结构关系

称呼名词:而子域这个名称是相对的,可以看作一个相对某个成员国中的某一个省或者相对某个省的某一个县。

这里有牵扯到一个名词:DC(域控制器)

我们可以把它看成一个国家的首都(也就是一台物理服务器上安装了AD活动目录).

我们的所有的国民的户籍信息都存储在这里。

通过上面的几个案例我们清楚的认识到：

**将网络中多台计算机逻辑上组织到一起，进行集中管理，这种区别于工作组的逻辑环境叫做域，这个核心管理单元（域）可以帮助我们组织与存储资源（包括物理、逻辑资源）。而这个核心管理单元的实现手段就是活动目录（AD）。**

下面我们来看看活动目录(AD)的安装步骤，及注意事项：

1、运行中输入：dcpromo

2、是否创建新域（如果当前网络环境中没有域，那么我们创建的就是整个森林的第一棵树，日后他可能发展成为森林。）

3、新域的DNS全名（全名要符合DNS的命名规范）

4、新域的NetBIOS名（用来使win98或者只能使用netbios服务的操作系统加入域）

5、数据库和日志文件文件夹（建议部署到非系统安装盘下。）

6、共享的系统卷（sysvol存放组策略的共享卷）

7、DNS注册诊断（AD需要DNS的支持，这里检测当前环境有没有DNS，没有就在本机安装）

8、域兼容性（域的功能级别：2000纯模式、2000混合模式【默认】、2003纯模式）

9、还原模式密码（DC中另一个administrator的密码，不记载在AD中。）

从安装步骤中我们可以看出AD活动目录要是想要正常工作，那么就必须依靠DNS的支持，而DNS在域中的作用则是：

**1、域名的命名采用DNS标准**

•**办公网络与Internet集成**

**2、定位DC**

•**1）客户机发送DNS查询请求给DNS服务器**

•**2）DNS服务器查询匹配的SRV资源记录**

•**3）DNS服务器返回相关DC的IP地址列表给客户机**

•**4）客户机联系到DC**

•**5）DC响应客户机的请求**

**域的DNS区域维护**

**\*SRV资源记录可以定位DC**

我们在活动目录管理的时候，遇到的很大一部分问题都是由DNS引起的，那么除了DNS我们还会遇到什么样的问题，请见下篇《常见故障排除案例分析之加入域》