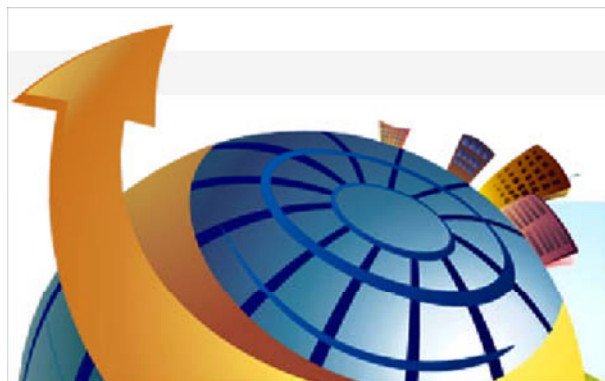


[首页](#) | [网站地图](#)[日文](#) | [繁体中文](#) | [简体中文](#) | [English](#)**JFT**[首页](#) | [最新消息](#) | [产品](#) | [支援](#) | [关于我们](#)

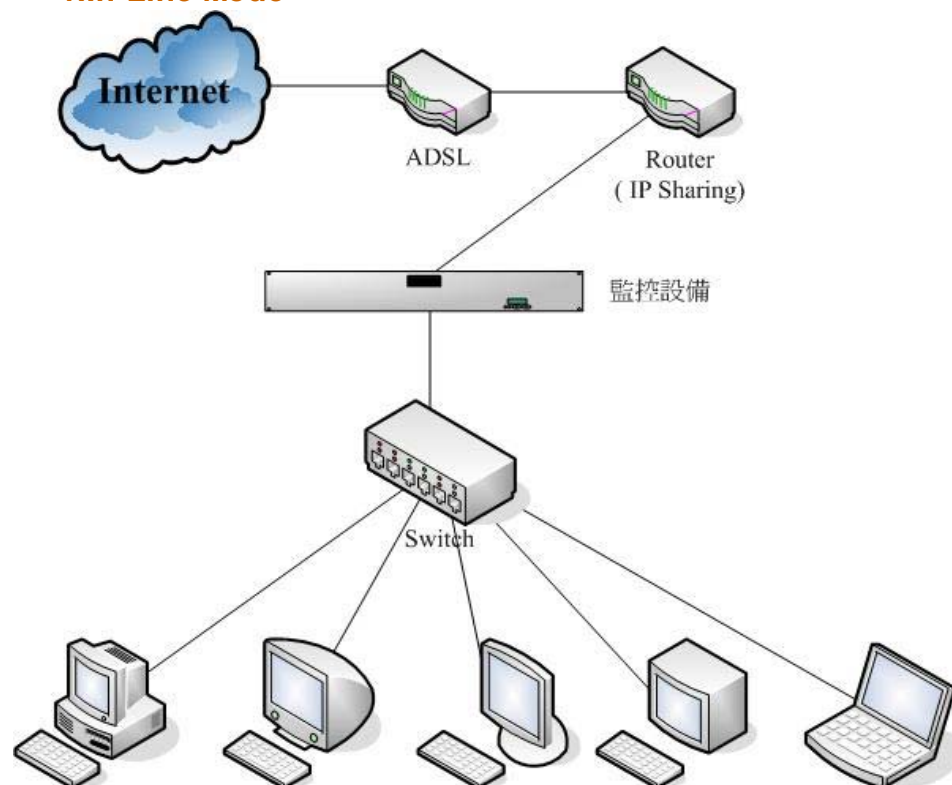
 **销售专线**
138-098-288-26

MISKeeper 支援[使用说明](#)[安装说明](#)[资料下载](#)[维护说明](#)[软件维护条约](#)[硬件维护条约](#)[客户服务](#)[问与答](#)**技术文章**[IM 侧录模式 \(上\)](#)[IM 侧录模式 \(下\)](#)

实时通讯软件控管模式解说(上)

目前市面上少数产品可以提供给企业主针对内部员工上网行为管理,包含实时通讯软件的内容与使用控管,其中有各产品的管控模式与各 IM 实时通讯软件的特性,这里先对部分规格做解说,各 MIS 或管理者就可以知道该产品架构是否适用贵单位网络系统.一般来说网络监控产品分为以下几种模式,我以简单的网络架构图示说明,其中若贵单位具有负载平衡设备,VPN 线路,不同子网段切割,的状况就不是那么单纯,总之先了解各模式的含义后,若网络架构较为复杂,我们可以再进行分析使用何种模式较为恰当.

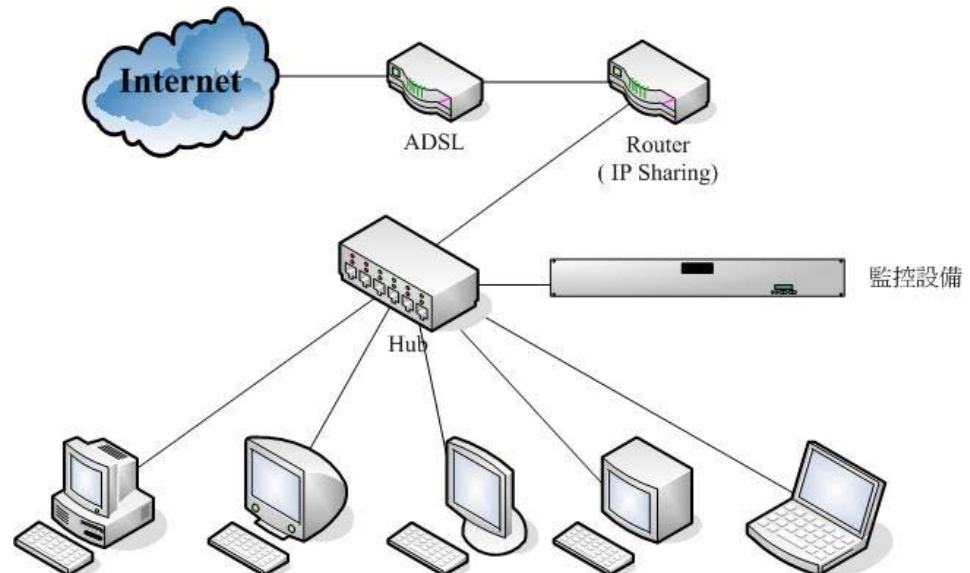
1. In-Line Mode



通常又会叫做 Gateway Mode 因为这种安装模式通常都会装在联外通路的主干上,类似匣道器的位置,所谓 In-Line Mode 顾名思义就是"在线里面"的模式,意思就是设备会成为线的一部分,这样的产品通常都会有 2 个以上的网络孔,一个是上行也就是连接对外通道,一个是下行也就是连接内

部欲控管的区域,这个模式跟匣道器最大的不同是在于,匣道器必须位于所有上网设备的头端,而**In-Line Mode**的控管设备并不负责封包导向,通常是负责纪录与拒绝的功能,所以其实你可以安装在网络的任何一个节点,不过只有其下的区域受到管控,这样的产品通常是透过封包解析与过滤的技术,将所有流过该线路的封包做检查,由于用户的网络封包多了一个节点,故在封包的导通速度上会受到一点影响,包含带宽与反应速度,而一般来说通常会需要使用这种模式的纪录与管控的应用大部分都是第七层的封包解析,也就是必须先解开封包最内层的数据,再针对该封包的特性判断为何种应用,再将其内容依照协议反向组合回人类可以阅读或操作的内容后纪录下来,由此可知此类型的产品模式需要非常大量的运算资源,尤其当你条件与反向协议(欲控管的应用)设定越多,机器的负载就越大,在一般的状况下,厂商都会提供该款设备所建议的控管人数或是封包透通量,但是,该类型的机器还会视应用协议的复杂程度而提高或降低处理器负载,所以实际测试厂商建议的型号是否适用贵单位的环境还是比较恰当的.通常使用这种模式最大的风险来自于,该产品若是出现不稳定或是当机的情况将会造成其下受控区域的网络断线,故若有不可承受断线风险的服务或是使用端,则要再三考虑,其次,由于系统负载并不是平均的出现(视用户使用状况),偶尔会出现封包阻塞的情形,也就是说,在观看某一网页时等待很久,正要放弃时突然页面上的所有图文件与资料同时出现,这就是可能因为该设备处理不及或是缓冲区满载所造成的现象.使用本模式通常是是需要控制的功能,**In-line mode**才能做到对封包舍弃或窜改(自己出现没有输入的数据在通讯软件上)的动作.

2.Sniffer Mode



又称为监听模式,也称做旁路模式也就是利用早期**Hub**(集线器)时代(目前大部分的设备都使用**Switch**也就是交换器了)特性,也就是说,以前的集线器内的封包是所有的**Port**都听得到的,也就是说如果你有一个**24Ports**的集线器在该集线器上的**10/100**带宽是共享的,因为每一个封包都会对每一个**Port**送出,利用这种特性将上行与下行的网络接上**Hub**再将测路设备也接在**Hub**上,该设备就可以对流经该线路的封包进行监听与测

录,如此就算该设备当机或损毁也不会影响封包的流通,降低设备对网络环境的冲击,设备的运作效能也不会影响网络的透通效率,不过,最大的缺点为该模式仅只能做到监听与测录的内容的需求,若是需要进行控管,由与设备对封包并没有主控权故无法对封包做拒绝,抛弃,或是窜改的动作.另外由于科技的进步,市面上所有的集线器都已经进化到交换器的程度了,而交换器的特性是内部具有比对回路,当与该Port的MAC相关之分组交换器才会对该Port进行封包传送,如此大大的提高该局域网络的分组交换效率,不过,也因为如此,透过交换器集中的网络要在其中进行监听是有困难的,因为设备并没有真正的跟使用者做沟通所以封包不一定会流向设备所在的Port,所以Hub的采购不易也是本模式的缺点,不过,以现在的高科技怎么可能做不到这么低的要求呢?故,再类似高贵的思科网络设备供货商所提供的部分高档Switch就具备了MirrorPort的功能,也就是可以透过设定将该Switch上的某 2 Port做Mirror的功能让该 2 Port做到类似像HUB的作用这样就可以解决封包监听的问题了,可是!!!那样的设备相对于目前一般的Switch来说价格会是10倍以上....欸.....划得来吗?另外偷偷透露,现在由于市面上的Switch价格都非常非常的流血,你觉得Switch会有封包判别再进行交换的功能....其实...严格来说可能Switch刚开机的时候会有啦!时间一久,由于分组交换的混乱与内部为了节省成本而缩小了CPU暂存表或是算法不够强,通常Switch就会变成Hub了...呵呵...不要说是我说的!

[首页](#) | [最新消息](#) | [产品](#) | [支援](#) | [关于我们](#)

JFETEK JAPAN © 2008 版权所有 | [隐私权政策](#) | [网站使用条款](#)