网络核心服务 Mate-CNS 系列产品介绍

DDI，即 DNS，DHCP & IP Address Management（IPAM）的缩写。它最初来自 Gartner2009 年的一次报告，当时，Gartner 开始重新强调“核心网络服务”的重要性。更在这份报告中首 次提出 DDI 这个名词，以及 DDI 市场的概念。

DNS 和 DHCP 能被称为核心网络服务(Core Network Service，简称 CNS)，其重要性不言而喻。当 DNS 不能连接，就没法访问网站了；若 DHCP 发生故障，那么连网络都无法接入，更谈不上上网了。由此可见，DNS 与 DHCP 都是非常关键的，而这两者的结合点就是 IP，因此业内通常将 DNS、DHCP 及 IPAM 统筹考虑。

起初在规划信息化建设与网络安全的时候，内网桌面管理、行为审计与网络边界安全都 会做的非常的完善，而恰恰在 IP 地址层面的管理是微乎其微的，直至现在依然没有摆脱手动管理的传统方式，地址冲突/欺骗、非法接入等事件层出不穷。

随着“云时代”与 BYOD 时代的到来，企业激增的网络办公需求以及业务系统的丰富，让不少企业开始重新审视原有的网络布局，以确保维持企业网络安全、稳定、可靠的运行状态。在企业信息化系统建设和实施中，企业核心网络服务（Core Network Services，CNS，既保障网络运行的 DHCP、DNS、IPAM 三项关键服务）的简单、可靠、稳定及高可用性，实现 IP 地址自动化分配管理审计及访客 IP 授权控制，对用户来说极为重要。CNS 是所有基于 IP 的应用程序的运行基础，直接关系到企业业务应用的稳定运行和安全通讯，是企业 IT 管理最核心的

部分。

CNS 产品关注基础网络安全，保障业务稳定运行

IP 地址和域名的合理规划是网络设计中的重要一环，对数据网络就尤为重要。IP 地址规划的好坏，不仅影响到网络路由协议算法的效率、网络性能、网络的管理、网络扩展，还 直接影响到网络应用的进一步发展。集中的自动化 IP 地址分配与回收提供高可靠稳定的 DNS 域名解析。

- 保障 IP 地址分配的稳定可靠
- 避免 IP 地址冲突/欺骗的现象
- DNS/DHCP/NTP 网络服务的冗余备份
- IPv4/IPv6 地址体系平滑迁移

CNS 产品关注 IP 分配授权控制，保障 IP/MAC 的安全审计

IP 地址管理规划审计是信息化运行成功的关键因素。IP 地址是计算机网络能够保持高效运行的关键。如果 IP 地管理不当，很容易影响网络正常业务的开展。同时，有效地、全面的 IP 地址管理审计也是加强管理，追查网上犯罪等危害国家安全行为的有效手段。

- 无需安装客户端的 IP 准入机制
- MAC 地址黑白名单，控制非法 IP 接入
- 无线 BYOD 终端类型自动识别，支持 DHCP 指纹
- 防止私接路由器、交换机
- 实名制动态 IP 地址分配审计
- 访客 IP 地址动态授权控制

BYOD 突显 IP 地址自动化管理的重要性

随着 BYOD 的模式逐渐为企业所接受，公司员工携带的移动设备皆必须提供可连网服务， 如此之下，一名员工可能同时在使用 IP 语音（VoIP）电话、智能手机、笔记型电脑等设备， 每一个连网设备都需要配置一个 IP 地址。如果仍沿用以往管理 IP 模式，每当有新地址和新 网络被分配或修改时，IT 管理者以手动维护，实际上就已经常发生资料无法及时更新，或人工输入错误等状况，更何况是 IP 配置数量超过以往 2 至 3 倍的 BYOD 时代，这种效率低 与容易出错的管理模式，便显得左支右绌。

CNS 产品内嵌的高性能 DHCP 服务具有接入授权控制功能，实现了网络边界准入和 BYOD 设备指纹识别，既允许已授权设备才可以获取到合法的 IP 地址，这种方式能够对局域网实 现了比较好的控制，在网络与用户设备的交界处进行控制，限制非法用户对网络资源的使用。

新一代网络核心服务自动化开通平台（Mate-CNS）采用软硬件一体的解决方案，依托专 用的网络硬件平台，配以自主研发的操作系统，保证系统可靠、安全、稳定的运行。分别 适用于运营商、政府、军队、能源、金融、教育、大中小型企业等各类用户。

Mate-CNS 系统功能

1. 自动化的 IP 地址管理设备部署完毕后，企业网络终端设备将摒弃传统的手工设置固 定 IP 地址的方式，全部采用自动获取 IP 地址的方式；可让管理员有效管理子网（含有线子 网及无线子网），并能实现 IP 地址的有效分配、追踪、回收、审计以达到对网络可视性管理的目的；

2. 为了使企业现有的上网行为管理设备能管理到具体的终端设备，IP 地址管理

设备要 能基于终端设备的 MAC 地址实现固定 IP 地址的推送，保证所有终端设备即使采用 DHCP 获取 IP 地址也能获取到固定的 IP 地址，从而实现对所有终端设备的有效管理；

3. 替代传统的利用 Windows 或 Linux、交换设备或者路由设备实现简单 DHCP Server 自动分发 IP 地址的状态，实现基于 DHCP+的 IP 分发策略。传统的利用交换设备或者路由设备实现 DHCP 功能时，不但功能有限且可极大的占用相关网络设备的 CPU 资源，从而降低 网络设备转发数据的效率。保障 IP 地址分配的稳定可靠，避免 IP 地址冲突/欺骗的现象的 发生；

4. 采用传统 Windows DNS 或采用服务器在上面自行安装 BIND 软件完成的域名解析服务，不能适应现代的网络社会的需要，采用新一代硬件化的智能 DNS 设备，以加强企业网基本 DNS 服务，提高网络基础服务的可靠性和安全性；

5. 实时地址数据分析。当前企业采用手工 Excel 表格进行 IP 地址的管理，这种管理方式维护量巨大，且极易造成数据不一致、不准确的情况发生。因此要求 IP 地址管理设备必须能实现自动报表的功能，将网管人员从繁重的 Excel 表格中解脱出来，去更高效的从事其他工作；

6. 企业目前有将近 65%的员工已经使用自有设备（BYOD：自携带设备）访问与工作相 关的数据。为了实现有效、可控的 IP 管理，要求 IP 地址管理设备要能根据系统指纹

（Fingerprints）识别不同的终端类型（比如：苹果、安卓、手持终端、路由器、WINXP、 WIN7 等）并为不同的终端分配不同的 IP 地址段，实现对当前多种终端的有效管理。从而在 企业中实现真正的 BYOD 应用，保证企业资源被安全、可控的访

问；

7. 可通过系统指纹认证，系统唯一指纹验证，精细到不同的操作系统版本，实现自动 识别、隔离私设路由/交换设备，达到网络可视化管理的目的；

8. 实现防止手动私改和私设 IP/MAC 地址的目的。自动化 IP 管理设备，要能实现对全网的统一的 IP/MAC 管理。当有终端私设 IP/MAC 或手改 IP/MAC 时，自动化管理设备可与公司现有交换机实现联动，通过交换机上 DAI（动态 ARP 检测）功能和 IP Source Guard(IPSG) 功能，阻止这些非法终端上网，从而阻止手改 IP 和私设 IP 的问题；

9. 需实现非法设备(IP/MAC)接入的检测。部署了自动化 IP 管理设备后，要求可以对企业的全网络进行检测。一旦有任何非授权设备接入，会将此设备隔离在隔离网段中，同时将设备的 IP/MAC 和其他相关信息与注册的合法设备的 MAC 信息进行比较，从而防止非法设备接入办公内网；

10. 支持 IPv6 地址的分配与管理。自动 IP 地址管理设备支持 IPv6 地址的自动分发与管理（DHCPv6）。将考虑 IPv4 至 IPv6 地址的迁移，需通过 IP 地址管理设备来实现顺滑、平稳的过渡。

Mate-CNS 系统优势

No IP, No Network, No Business，IP 通信是保证业务稳定运行的关键。新一代网络核心服 务自动化管理支撑平台提供面向业务服务的 IPv4/IPv6 地址管理、分配和安全接入, 提供可扩展的技术框架，从而保证网络更稳定的运行。

通过网络核心服务的自动化和统一化管理来控制网络运营成本，体现在以下几个方面：

- 统一化管理，减少运营操作成本
- 提高效率和生产力，减少技术支援成本
- 简化和自动化现有基于手工管理的流程
- 实时监视地址分配、审计和统计分析
- 提高 DNS 域名解析的高可靠、高稳定性
- 严格、周密的 IP/MAC 地址安全审计跟踪
- 简化故障 IP 地址的诊断、定位和排除
- MAC 地址授权接入，防止未知设备接入网络造成安全威胁
- 避免IP 冲突和用户私自安装DHCP 导致IP 地址混乱

网络核心服务 CNS 产品应用

1、替换采用Excel 表格或手工管理IP 地址空间的方式

2、替换原有路由器/防火墙自带的DHCP 服务

3、替换原有核心交换机自带的DHCP 服务

4、替换原有服务器（Windows DNS/Linux Bind 等）的DNS/DHCP 服务

5、提升IP 地址安全审计，满足等级保护与塞班斯法案的要求

6、实现IPv6 平滑迁移，满足IPv4/IPv6 双栈管理及域名解析

7、实现 DHCP、DNS 服务的高可用（DHCP 服务可实现双机同时接管全部地址池空间）

Mate-CNS 产品型号规格（硬件版本）

	MATE-CNS 1000	MATE-CNS 2000	MATE-CNS 4000	MATE-CNS 8000
DNS 查询/秒	3000-6000	6,000 - 12,000	12,000 - 36,000	>=36,000
DHCP 租约/秒	25 - 75	25 - 75	75 - 175	225
设备尺寸	1U	1U	2U	2U
电源模块	单电源	单电源	冗余电源	冗余电源
内存	2G	>=4G	>=8G	>=16G
存储介质	>=500G	>=500G	>=2TB	>=2TB

Mate-CNS 产品型号规格（虚拟化版本）

虚拟化版本功能与硬件版本功能完全相同，目前支持 VMware ESXi v5.5、v6.0；Citrix XenServer v6.0、v6.5 平台部署，根据 License 授权

	MATE-vCNS 1000	MATE-vCNS 4000	MATE-vCNS 8000
DNS 查询/秒	3000-6000	12,000 - 36,000	>=36,000
DHCP 租约/秒	25 - 75	75 - 175	225

Mate-CNS 产品功能指标

	指标要求
	固定业务接口， 6 个 10/100/1000M RJ45 网络接口
	管理接口，1×RJ45 管理接口，1×Pin Header
	温度，0℃~45℃（工作）-40℃~70℃（存储）
	湿度，5~95% RH，不凝结
性能和容量	采用专用硬件平台，采用多核处理器
	采用专用的、经过加固的操作系统
	采用专用的内置的、不需维护的数据库，保证数据存储的有效性
	支持双机备份技术，实现多重冗余，支持active-standby 模式

	设备集成 DNS、DHCP、NTP、DHCP 指纹识别功能、IP 授权接入控制、IP 地址 管理审计功能
	联动交换机的DHCP SNOOPING 和DAI 功能，可以预防IP 地址冲突、ARP 病毒
管理功能	用户界面支持中文，并具有纠错功能
	支持系统的软件升级功能
	支持将外部数据方便的导入，支持.xls 和.xlsx 格式
	支持将数据库内容实时备份和定时备份
	支持将设备的日志文件方便的导出
	支持数据列定制导出，支持.xls 和.xlsx 格式
	设备必须支持SNMPv1、v2c、v3
	设备必须支持Web 远程管理
	设备支持Telnet 或ssh
DNS 服务	标准 DNS 服务：系统必须支持标准的 DNS 服务
	反向DNS 解析：支持反向DNS 解析功能
	DNS 委派：支持区域委派功能，将某个域或子域解析权委派到其他 DNS 服务器
	DNS 记录：支持基于RFC 标准的DNS 记录类型: 如A、AAAA、CNAME、MX、PTR、SRV 等
	支持DNS 主从备份机制，支持DNS 转发
	支持 DNS 参数定义（如allow-transfer、allow-recursion、allow-query、allow-notify、acl 等参数）
	支持泛域名解析，支持DNS 轮询，实现DNS 负载均衡
	支持IPv6，DNS 解析服务支持IPv6
	支持中文域名，DNS 解析服务支持中文域名记录
	支持域名智能解析，DNS 服务器对于外部 INTERNET 访问本地站点时候，可以针对不同的用户解析到不同的 IP 地址（如来自网通的访问者，则解析到网通 的镜像服务器等）
	内置防DOS 攻击模块,可防止服务器自身的安全
DHCP 服务	RFCs 支持：RFC2131、RFC2132、RFC2241、RFC2242、RFC2485、RFC2610、RFC2937、RFC3361、RFC3397、RFC3442、RFC958、RFC1157、RFC3942、RFC3315、RFC3319、 RFC3646、RFC3898、RFC4075、RFC4242、RFC4280、RFC4291、RFC4704
	CIDR（无类域间路由）支持
	基于IP/MAC 地址的静态绑定（IP 保留地址分配）

	实现地址的动态分配和回收
	支持业界标准的DHCP Failover
	支持DHCP Option 60/Option 82
	支持DHCP 系统指纹（Fingerprints）
	高级DHCP 选项编辑器，支持厂商自定义Option
	支持所有ISC 预定义的 DHCP option 空间（如Option 1 到Option 125）和客户化的DHCP Option 空间（如Option 126 到Option 254）
IPv6 支持	支持创建/64 到/128 网络
	支持创建DHCPv6 地址分配池
	支持DHCPv6 保留地址分配，支持DUID 绑定
	支持DHCPv6 客户端参数设定
	支持无状态地址信息刷新时间设定
	支持DHCPv6 有状态地址分配
	支持IPv4、IPv6 双栈地址管理
IP 地址管理和审计	中央数据集中的IP 管理控制台
	支持交换机自定义脚本配置功能，实现与交换机之间自动和交互式任务进行通信，提供快速开通配置交换机等功能
	支持对IP 地址进行逻辑分组管理
	实时显示分配地址的状态和续租信息
	实名制地址分配、回收和历史数据的审计分析
	支持 DHCP 系统指纹技术，支持 BYOD（BringYourOwnDevice），自动识别智能 手机、平板电脑等的系统指纹
	确保数据完整性（没有数据丢失、损毁或延迟）
	系统必须记录DHCP 地址分配的记录数据，并能够方便地查找定位
	支持数据完整性检查，数据核查机制可以在系统部署前进行数据检查，提前发现系统配置的问题
	生成DHCP 的IP 地址时不占用存储空间，只有确认分配时才占用数据库存储
	支持 MAC 地址黑白名单，可以只对已授权 MAC 的设备分配 IP 地址。向 MAC 动态授权列表内临时添加新的记录，不需要重启 DHCPv4 服务进程
	灵活的MAC 地址永久授权，及MAC 地址活跃度分析
	支持动态解除已临时授权的MAC 地址
访客IP 授权控制	允许访客临时分配IP 地址
	访客分配地址使用期限设定

	手动/定期解除已授权地址
	基于Portal 的访客信息的录入和自动授权
	与LDAP/RADIUS 等认证服务器帐户进行验证
	实名制访客IP 地址审计
	支持访客可允许注册设备数量的灵活自定义
IP 地址调和	系统允许定义地址核查策略，用于定期比较物理网络和本系统内的地址变更
	支持待清除核查状态，此状态表明此IP 地址长时间没有被使用
	支持未知 IP 核查状态，此状态表明此 IP 由于各种原因没有被记录在系统中，如非法接入、手动私设地址等
	支持不匹配 IP 地址核查状态，此状态表明此 IP 地址所对应的 MAC 地址信息修改或随意更换了连接端口，如地址欺骗、移动办公等
	支持设备端口/MAC 扫描，自动发现 IP 设备和交换机端口的对应关系，自动发现和显示 VLAN 信息，显示交换机端口的详细信息，包括端口速率，端口状态， 端口信息描述等信息