

华域智能 DDIC-DNS 系统技术白皮书

摘要

该文档简要阐述了深圳华域通信技术有限公司 (Huau Communication technology Co., Ltd.) 的荣誉产品华域智能 DDIC-DNS 系统产品技术特点、功能特点和技术背景，欢迎垂询。

深圳华域通信技术有限公司
Huau Communication technology Co., Ltd.

版权信息

版权所有(C) 2010-2016 深圳华域通信技术有限公司(Huau Communication technology Co., Ltd.), 保留所有权利

文档保证声明

非经本公司书面许可, 任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部, 并不得以任何形式传播。

注意

由于产品版本升级或其它原因, 本文档内容会不定期进行更新。除非另有约定, 本文档仅作为使用指导, 本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

联系方式

公司地址: 深圳市福田区福田街道深南中路福田大厦东部 18 楼

电话: 400-6996-601

服务邮箱: service@huautech.com

公司网站: www.huautech.com

目录

版权信息.....	2
文档保证声明.....	2
注意	2
联系方式.....	2
公司简介.....	4
产品介绍.....	4
2.1. 基本背景.....	4
2.2. 产品目标与特性.....	5
2.2.1. 安全方面.....	5
2.2.2. 高可靠性.....	5
2.2.3. 可扩展性.....	5
2.2.4. 模块化管理.....	5
2.2.5. 易用性.....	5
2.2.6. 通用性.....	6
2.3. 特色功能介绍.....	7
2.3.1. 分线路智能解析.....	7
2.3.2. 域名管理系统.....	7
2.3.3. 资源负载调度.....	7
2.3.4. 解析过滤.....	7
2.3.5. 区域响应.....	8
2.3.6. 域名探针.....	8
2.3.7. 域名纠错.....	8
2.3.8. DNS-64.....	8
2.3.9. HTTP-DNS	9
2.3.10. 解析限速.....	9
2.3.11. 存根区.....	9
2.3.12. 热备、集群负载.....	9
2.3.13. 链路保护.....	9
2.3.14. 日志功能.....	10
2.4. 系统部署.....	11
2.4.1. 主辅模式.....	11
2.4.2. 热备模式.....	11
2.4.3. 群集模式.....	12
2.4.4. Anycast 集中管理	12

公司简介

深圳华域通信技术有限公司是一家专注于域名系统、网络应用优化的高科技互联网公司。公司研发团队紧贴用户实际需求，立足“开放、创新、安全”的产品理念，立志为用户打造更加科学、高效、便捷、安全的网络优化解决方案。

产品介绍

2.1. 基本背景

互联网的飞速发展使人们的生活方式、信息获取途径都发生着巨大的变化，其提供的方便而广泛的互连必将对未来社会生活的各个方面带来影响。然而互联网是由成千上万个网络组成的，其中又包括公用网络和私有网络。随着规模的不断扩大，互联网也变得越来越错综复杂。当更多的用户可以通过各种不同的途径和方式接入到互联网的同时，其自身也正一步步的走向无序和不可预知。无整体规划和设计、网络拓补结构不清晰、可靠性能的缺乏、安全性问题是困扰核心网络服务（CNS）管理效率的重要因素。

网际互连问题是指当不同的网络运营商网络进行对等互连时，由于竞争等经济原因造成互连点的链路拥塞。而中国有多家 ISP 运营商，他们之间相互访问的宽瓶颈问题，由于不同运营商网络之间的互连需要较大的投入，但是又没有明显的经济效益产生，所以通常网络运营商都不会主动去解决这个瓶颈。

企业成长的同时，IP 地址空间的规模和复杂性不断增加，规划、分配及追查记录变得越来越困难。实际上，管理 IP 地址对许多企业来说都是愈发严峻的挑战。若使用电子表格软件的简单解决方案，或互联网开源软件等传统方式来管理 IP 地址，则根本无法提供符合目前状况所需的进阶特性，来支持企业的需求。

由于 IPv4 地址已经用罄，IPv6 是解决 IP 地址不足的方案。然而，由于 IPv6 是一个全新的技术与规格，地址高达 128bit，已经是人力所无法记忆及管理的。在网络核心服务的管理方面面临这巨大的挑战。

2.2. 产品目标与特性

华域智能 DDIC-DNS 系统立足于满足目前的企业网络核心服务管理需求，同时对满足未来的新技术、新需求挑战，进行了前瞻性的设计和技术创新。系统汇集了 DNS 基本模块、安全模块、分析模块，实现多重服务的统一管理。可极大改善企业网络中 DNS 系统的易用性、安全性、扩展性，同时可减少高达 50% 以上的管理投入和运营支出。具体特性包括：

2.2.1. 安全性

华域智能 DDIC-DNS 系统从底层系统核心、安全模块和硬件兼容性等各个层次进行了精心的设计和优化，提供运营商级的 DNS 服务，为企业构建安全的 DNS 架构。

2.2.2. 高可靠性

具有更高的容错能力，支持多机负载以及热备功能，保证 7x24 小时不间断提供服务。

2.2.3. 可扩展性

随着基于 IP 的新业务（云计算、虚拟化等）的增长和 IPv6 的应用普及，跨多业务的需求越来越多，产品实施开放性原则，方便与其他不同厂商的网络设备进行联动，各种协议和接口均符合国际标准。

2.2.4. 模块化管理

华域智能 DDIC-DNS 系统，单台设备即可满足中小型企业单位的需求。面对大型企业，可以通过独有的集群以及模块化方案，满足跨地域、复杂网络环境下的统一部署、集中管理需求。

2.2.5. 易用性

系统采用统一的 GUI 配置界面，同时每项配置均有内容提示，使得操作简单易上手。同时我们提供全面的产品文档和全方位的技术支持服务，以协助管理员对系统进行实施与维

护。

2.2.6. 通用性

符合国际标准：RFC-1034、RFC-1035、RFC-1123、RFC-1886、RFC-2136、RFC-2181、RFC-2308、RFC-2535、RFC-2671、RFC-2782、RFC-2930、RFC-3645、RFC-3646

2.3. 特色功能介绍

华域智能 DDIC-DNS 系统可同时支持权威解析服务和递归解析服务功能。既可以承担公司域名的对外发布功能，也可以支持解析外部域名，并可针对在多运营商出口环境下内网访问公网资源的优化。以下为华域 DDIC-DNS 系统的优势功能：

2.3.1. 分线路智能解析

为解决国际线路以及国内运营商之间的网际互连问题，华域智能 DNS 系统可根据来访 IP，智能返回一个和用户在同一运营商或地区的镜像 IP 供其进行访问，避免用户走不同运营商之间的接口而导致的瓶颈问题。设备内置包括国内四大运营商（电信、联通、移动、教育）、国内 30 个省级行政区域、国际 252 个国家，共计 286 条内置线路，供用户自行选用。

2.3.2. 域名管理系统

华域智能 DDIC-DNS 系统提供专业而的域名管理功能。通过域名管理功能，可以让域名管理员轻松的配置和管理正解域名和反解地址。支持多种常用记录类型：A、A6、AAAA、CNAME、MX、NS、PTR、TXT、HINFO、SRV、NAPTR 等。

2.3.3. 资源负载调度

华域智能 DDIC-DNS 系统支持针对不同资源类别进行分类解析，配合出口目的路由功能实现资源负载均衡的功能（可根据时间段、出口负载状况调度）。使用华域智能 DNS 系统的资源负载调度功能，不会产生跨运营商访问目的资源的路由代价，所以可达到更高的出访效率、且可有效避免出口拥堵状况的发生。

2.3.4. 解析过滤

在整个 DNS 解析架构中缓存污染、缓存投毒、DNS 劫持已经成为最让管理员头疼的事情。为了有效预防此类攻击对最终用户带来损失，华域智能 DNS 系统可对响应结果进行过滤剔除，来增加 DNS 设备的安全系数。主要应用场景：权威域名堡垒 DNS 设备、已知上层 DNS 遭污染修正。

2.3.5. 区域响应

一个 DNS 请求的响应一般会包含多个资源记录值，它们形成了一个资源记录值集。DNS 设备通常是按照轮询的方式将结果返回到客户端。客户端解析器应适当重新对资源记录进行排序，即优先使用本地网络中的资源记录值，然后才使用其他资源记录值。然而不是所有的客户端解析器都可以完成这项工作。华域智能 DNS 系统可以基于客户端的地址，直接在服务器上对返回结果进行进一步优化排序（根据客户端所属网段、地区、自定义等返回相应记录），而完全不需要客户端解析器重新进行排序，保证最优解析结果。主要应用场景为：跨区域网站建设、地区 BGP 选路、CDN 全局调度等。

2.3.6. 域名探针

随着运营商带宽资费的降低，企业出口带宽资源已经不是网络的瓶颈，使用户享受到更优化的网络环境已经成为企业网络管理的重点。华域智能 DNS 系统内置域名探针功能，可探测到所访问资源在各个运营商内 CDN 镜像的速度，从而给出更优化的访问线路。

2.3.7. 域名纠错

当客户端输入错误的域名时，浏览器往往弹出“无法显示网页”的提示，系统 DNS 模块内置域名纠错功能，通过分析 DNS 应答报文并构造应答报文返回客户端。将浏览器重定向到提示页面上，为用户提供更多帮助，也为牵引网络流量、开展网络增值服务创造条件。同时在一定程度上能有效防止黑客采用 nxdomain 攻击行为攻击 DNS 设备。

2.3.8. DNS-64

为配合企业无缝向 IPv6 方向过渡，同时实现 IPv6 与 IPv4 之间的网络地址与协议转换技术。IETF 重新设计了一项新的解决方案：NAT64 与 DNS64 技术。华域 DNS64 可配合 NAT64 工作，将 DNS 查询信息中的 A 记录（IPv4 地址）合成到 AAAA 记录（IPv6 地址）中，返回合成的 AAAA 记录给用户给 IPv6 侧用户。

2.3.9. HTTP-DNS

HTTP-DNS 是一种移动解析服务的专用名称。用户可使用 HTTP 协议向 DNS 设备的 80 端口发起查询请求,代替传统的 DNS 协议向 DNS 服务器的 53 端口进行请求,绕开了 Local DNS、DNS 协议重定向等,从而避免了查询域名被劫持问题。

2.3.10. 解析限速

DDOS 攻击一直以来都是对 DNS 设备威胁最大的一种攻击方式,设备内置解析限速设置,可有效减少攻击流量,来缓解 DNS 设备遭受 DDOS 攻击。

2.3.11. 存根区

存根区只包含用于标识一个区对应的权威服务器的记录,通常包括 SOA, NS 和 A 记录。当域名服务器收到对存根区中数据的查询请求时,可以使用存根区中的信息定位正确的权威服务器进行查询,从而消除了每次查询都需要从根服务器开始的查找代价。

2.3.12. 热备、集群负载

华域智能 DDIC-DNS 系统支持双机热备(可热备加负载)、集群负载均衡功能(最小可支持双设备集群),支持常见的集群调度模式:RR、WRR、LC、WLC、LBLC、LBLCR、DH、SH、SED、NQ。通过这些功能,可最大化的提高 DNS 服务的可用性,充分发挥硬件性能,降低 IT 运营成本。

2.3.13. 链路保护

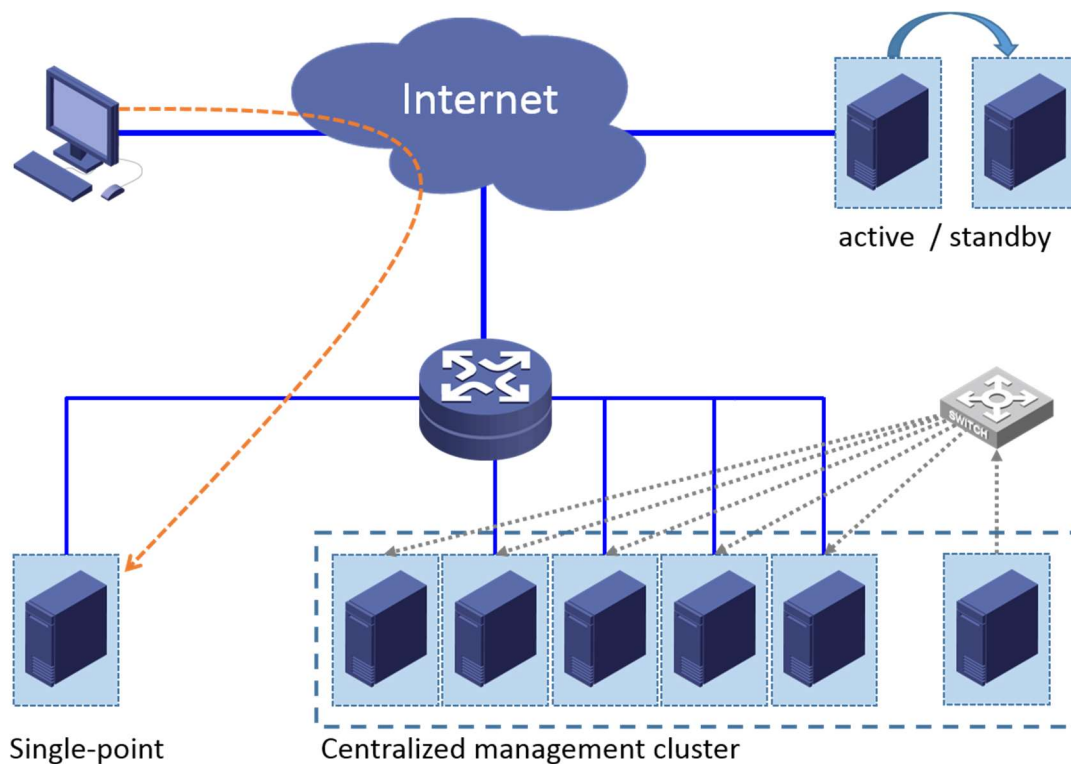
随着网络发展,企业出口多线路(ISP 线路)的网络环境已经非常普及,现实环境中经常会出现某条线路因为种种原因断线的情况,一旦出现故障,在此线路发布的各种对内、对外服务必将中断。华域智能 DNS 系统支持出口故障屏蔽,当某条出口链路故障时,设备可自动将流量迁移至其他出口,最大化保障各项业务的正常运行。

2.3.14. 日志功能

华域智能 DNS 系统提供丰富的日志和系统运行状态实时监控功能，如：DNS 解析日志（包括 QPS、Top 域名、Top IP、解析记录统计、解析异常）、安全日志、系统日志、操作日志和登录日志，并支持本地和远程存储。通过日志可以全面评估当前系统的运行状态以及快速进行故障定位。

2.4. 系统部署

华域智能 DNS 系统支持灵活的部署方式。可以根据不同需求进行各种方式部署。整体部署方式图如下：



2.4.1. 主辅模式

为更好的保证域名解析服务，通常网络中都会配置两台或两台以上的 DNS 做主辅域名服务器，所有数据均采用自动同步方式保证服务一致性。此种模式为传统部署模式，业务的冗余主要依靠客户端的解析器和浏览器针对失效 IP 的剔除方式来完成。

2.4.2. 热备模式

DNS 设备承担着核心网络服务的职能，业务的稳定性、可用性，非常重要。当网络中的设备出现故障后，需要高效恢复业务。通过热备技术，当网络中的一台设备故障时，业务会自动切换到另外一台备份机。另外，结合主辅模式可有效完成多台设备之间的数据同步。

注：传统热备模式处于备机模式的设备完全不会进行业务处理，华域智能 DNS 系统在热备模式下备机可与主机同时平均分配解析负载。

2.4.3. 群集模式

在大型和超大型网络中，主辅模式和主备模式已经不能灵活、稳定的对外提供业务。这时通常会采用集群模式将多台设备集中起来一起提供服务，来获得更高的计算速度。而在客户端看来就像是只有一个服务器。

2.4.4. Anycast 集中管理

对于面向全国用户的运营商，因为地域性、制度性、冗余性等关系，通常会采用 Anycast 技术来部署 DNS 设备，这时针对 DNS 策略的集中下发工作将变得非常繁琐，对策略的统一性也是一种考验。集中管理模式：中央管理器可将指定的多台 DNS 设备通过网络集中、统一的进行管理。所有策略均可自动下发到各设备，集中或分级进行维护。