

分布式机构网络的基本网络服务

每个网络都由一组核心网络服务支持，这组服务为所有的设备和应用提供可靠性、可用性、安全以及操作效率。这组核心服务包括名称、地址分配、认证、文件发布以及日志记录服务等。当今的机构需要一种基础结构，以便在整个机构中集成、分配并且管理这些核心网络服务。

在分布式机构环境下使用设备来发布核心网络服务



该网络服务套件在所有Infoblox设备平台上都是可用的。

大部分机构采用了传统的服务器和操作系统，并在其上使用一系列专门的软件应用来布署诸如DNS、DHCP、RADIUS以及TFTP的核心网络服务。这些服务提供了可用性、安全性、可控性以及发展性，但是由于对这些提供的功能不断提出新的要求，所以上述方法不再被人们采纳。因此，采用设备发送这些服务已经为业界推荐的最佳选择，因为设备固有的可靠性、可管理性、可扩展性、及安全性比通用服务器上软件的特性更出色。在分布式环境中，需要把设备连接在一起以提供集中化控制，保证数据正确性，提供不间断服务发送并且保证便捷的灾难恢复。

该网络服务套件包含在Infoblox设备中，这些设备使用安全的Infoblox NIOS™ 操作系统和集成的 bloxSDB™ 数据库，可提供完整的核心网络服务。该网络服务套件还包含了 Infoblox 网格模块，此模块将分布式设备连接为统一的网格，这些网格提供了无法超越的管理性、控制性、可见性、以及服务恢复性。Infoblox 网格在整个机构内部建立了一个基础，便于机构发送高可用性、安全以及易于管理的网络服务，这个基础包括：

网络服务套件优势

- 对所有网络服务进行集成化管理，包括 DNS、DHCP、RADIUS、TFTP/HTTP、NTP以及Syslog。
- 对于本地设备发送核心网络服务有集中化的管理
- 使用bloxHA™和bloxSYNC™技术进行快速网络故障切换和数据库同步功能，具有高可用性
- 一键式软件升级功能让新特性的添加变得容易，同时保证了安全
- 无论在何处工作，或者经过何种防火墙，使用基于SSL的VPN可以进行安全的管理

- Protocols (DNS, DHCP, RADIUS, TFTP, NTP, 等。)
- 数据 (IP地址、MAC地址、用户保密凭证、域名、处理日志等。)
- 文件 (策略、设备配置文件、可执行程序、证书撤销列表等。)

Infoblox网格既具有强大的不间断的本地服务发送功能，又具有集中化的管理与控制的优势。它们提供了下一代的核心基础结构，能够支持所有的网络和应用。

网络服务套件的特性及优点

Infoblox网络服务套件提供了所有网络和应用所需的基本服务，并且允许机构通过网络布署这些服务以提高可靠性、可用性以及安全性，同时降低运行成本。网络服务套件内的服务包括：

- 域名系统（DNS）提供名称服务；
- 动态主机配置协议（DHCP）提供地址分配服务；
- IP 地址管理提供网络可见性和网络控制服务；
- 认证服务（RADIUS）；
- 普通文件传输协议（TFTP）提供的配置服务；
- 通过HTTP配置服务；
- 网络时间协议（NTP）提供时间同步服务
- Syslog 提供的日志服务

该网络服务套件还包括Infoblox的专利申请技术，此项技术可以将分布的设备连接为一个统一的网格。对于同一网格中的Infoblox设备，其内嵌的数据库能够智能地连接在一起，因此可以共享实时的主机名称、IP地址租赁、用户证书以及其它网络数据。Infoblox网格在各个设备之间使用了安全通信技术，并采用完善的数据库技术来保证数据完整性。这样可以保证网格中的所有设备都能获得正确的数据，并且在出现大范围设备故障和广域网失效的情况下，网格仍能提供服务而不出现数据丢失和损毁。Infoblox的网格技术支持智能数据复制以减少网格的带宽，并确保每个位置都部署“大小合适”的设备。

更多优势

高可用性服务高可用性（HA）服务是由 bloxHA™ 技术—此技术采用业界标准的虚拟路由冗余协议（VRRP）完成5秒内的网络故障恢复—和 bloxSYNC™ 技术支持实现，确保实时数据库同步而不会出现数据丢失和数据重复。

集成化的、零管理的数据库该网络服务套件在集成的 bloxSDB™ 数据库中存储了所有的 DNS、DHCP 以及认证数据，此数据库内建于所有Infoblox设备上的 Infoblox NIOS™ 软件中。bloxSDB数据库使用非常复杂的技术在网格实时发布数据，具有的关键优势包括集中化管理、不间断服务发送、实时监控和报表、以及内置的灾难恢复功能。



该网络服务套件包含了Infoblox网络管理器。

便于使用的网络用户界面：该网络服务套件包含了Infoblox网络管理器，使该套件能够在安装有Windows XP或者Linux操作系统的个人计算机上运行。网络管理以流水线的方式管理复杂的、重复性的管理操作，因此管理员可以把精力集中于数据和服务而不是设备和协议。这样就减少了管理时间并消除了很多常见的数据项错误。

精细化的，基于角色的管理管理员可以委派其他管理员来管理特定的区域、网络、和设备，管理员还可以为被委派的其他管理员创建“只读”资料。这将允许公司向不同部门的员工下发管理授权，只把部分网络资源授予他们。

加固的安全性：Infoblox NIOS软件具有强化的安全性，能经得住政府和军事部门对安全扫描和入侵要求的考验。DNS、DHCP以及认证服务能够被轻松升级，保证最大限度地减少安全威胁。发现新变化时，底层的Infoblox NIOS软件可在简单的操作下在几分钟内进行升级。入侵这样的系统要比入侵有漏洞的通用操作系统困难很多。所有的数据发布和管理通信都是安全的，因为采用了安全套接层（SSL）——加密VPN，防止管理漏洞。

核心网络方案的不间断体系结构

Infoblox网络服务设备具有的特定功能可以服务于关键网络应用：

802.1X 和网络访问控制（NAC）的基础

与网络服务套件配合使用的RADIUS认证服务使用802.1x认证协议，为已分布式的网络提供了独具特性的解决方案。此外，Infoblox NAC Foundation 模块—包含在 Infoblox NIOS软件中—可以对 Infoblox 的DHCP 服务进行智能的、基于策略的控制，例如为采用不同厂商的组件而形成的NAC方案建立基础。它还提供了基本的NAC功能，例如访客接入和网络隔离。NAC Foundation 模块—内含一个强制网页门户，便于用户和访客注册—可以和第三方认证系统以及端点策略评估系统相交互，而且具备内置的策略引擎。它与 Infoblox NIOS 软件的其它模块完整集成，同时兼容 Infoblox 的网格技术。得益于自己的网格技术，它具有集中管理的特性和高可用的故障恢复特性。

为语音IP服务的网络服务

网络服务套件所具有的特性为语音IP应用提供了易于管理的、高可用性的解决方案：

高可用性的DHCP

Infoblox支持业界标准的DHCP故障恢复，在分布式的广域网范围有效。另外，用于热备份的Infoblox设备可以方便的设置为“HA模式”，提供快速故障恢复和实时数据库同步功能，无需为IP地址分配浪费时间。这保证了IP电话一直能够收到IP地址并且连入网络。

内置的TFTP

IP电话要求周期性的固件和配置文件更新，通过TFTP或者HTTP服务实现。该网络服务套件得益于网格技术，能够通过分布式的、集中管理的TFTP/HTTP配置服务来管理IP电话。只需一次操作就可以把固件和配置文件上传到网格管理中心并自动传送给网络中的各个设备和应用。在思科环境中，Infoblox网络连接器让固件和配置文件在思科呼叫管理器和网格主控之间进行自动同步。这样极大地减少了管理IP电话固件的时间，并且确保了所有设备都有正确的软件和配置。

为 Microsoft Active Directory（AD）提供可靠 DNS 架构

Infoblox 是 Microsoft 公司的认证伙伴，通过专有的支持，Infoblox DNSone 套件可以方便地集成到 Microsoft AD 环境。这样可以确保企业的关键DNS服务无论是在 Microsoft 还是非 Microsoft 环境下都是可用的和安全的。

为无线网络提供的可靠DHCP和RADIUS服务

要提供安全的、可靠的无线网络接入就需要对底层的DHCP和RADIUS服务提出要求。保证无线网络安全的工业标准是802.1x认证协议，此协议在用户每次试图访问无线网络时使用RADIUS协议与认证服务器进行通信。此外，当移动设备在建筑物或校园内移动时，每当它们连接不同的接入点，就可能需要一个新的IP地址。Infoblox的bloxHA 以及网格技术提供了可靠的DHCP和RADIUS服务以保证无线网络一直是可用的和安全的。

IP地址管理 (IPAM)

IP地址是最为重要的资源之一，它在任何网络中都需要被管理。对于哪个IP地址正在被使用、在何时它们被分配、它们被分配给哪个设备以及谁在使用它们等信息而言，对其直接访问的能力在消除冲突以及减少网络中断是至关重要的，它保证了网络安全、发现并处理网络问题并且保证了对规则的遵守。

Infoblox IP 地址管理功能使客户能够在企业范围管理DNS和地址数据，进行统一的管理和监控，同时提供适当的集中化审计和报表功能。Infoblox IPAM 模块，与网络服务套件中的 DNS 以及 DHCP 模块相结合，是世界上第一个把内建IPAM和DNS以及DHCP进行集成的设备解决方案。

数据表

RADIUS 技术规范

| | |
|------|--|
| 协议引擎 | 自由远程身份验证拨号用户服务 1.1.3 |
| 认证方法 | <ul style="list-style-type: none"> • PAP – 密码认证协议 • CHAP, MS-CHAP 和 MS-CHAPv2 – 挑战认证握手协议 • EAP – 为使用802.1x协议，基于端口的鉴定提供的“可扩展鉴定协议” EAP-TLS, EAP-MSCHAPv2, EAP-GTC • PEAP – 为802.1x基于端口的鉴定提供的“保护可扩展鉴定协议”， PEAP/EAP-GTC, PEAP/ EAP-MSCHAPv2 (这些鉴定方法由Windows客户端提供原生日本地支持) • EAP/TLS – “可扩展鉴定协议，传输层安全”，提供双向鉴定，需要客户端证书 • EAP-TTLS/EAP-PAP, EAP-TTLS/EAP-CHAP, EAP-TTLS/EAP-MS-CHAP, EAP-TTLS/EAP-MS-CHAPv2, EAP-TTLS/EAP-MSCHAPv2, EAP-TTLS/EAP-GTC |

DNS 技术规范

| | |
|---------|---|
| RFCs支持的 | 1034和1035 动态升级, RFC 2136 增量区域数据传输, RFC 1995 区域变化通知, RFC 1996 密钥事务鉴定 (TSIG), RFC 2845 Classless IN-ADDR.ARPA delegation, RFC 2317 |
| 协议引擎 | BIND 9.3.4 |
| 更多功能 | <ul style="list-style-type: none"> • 使用TSIG进行安全的DNS升级 • 秘密传送 • Microsoft Active Directory 支持 • Infoblox视图 • 为查询、区域传送、以及动态升级建立基于IP地址的访问列表 • 区域导入工具 • 可自定义的TTL设置 |

DHCP 技术规范

| | |
|---------|--|
| RFCs支持的 | RFCs 3046, 2131 和 1531 BOOTP, RFCs 1534 和 2132 |
| 协议引擎 | DHCPD 3.0.1 |
| 更多功能 | <ul style="list-style-type: none"> • VLSM (可变长子网掩码) 支持 • CIDR (无类域间路由) 支持 • 段内多子网 (supernetting) • 基于MAC地址的“静态租赁” (手动分配) • 基于MAC地址的过滤 • 地址分配前可用性检查 • DHCP中继代理 / Option 82支持 • 租期发布时, 安全的DHCP-DNS集成升级 • 高级DHCP选项编辑器 • Windows, Unix和MAC OS兼容 • 外部系统日志服务器支持 |

部件编号

| | |
|--------------------------------|----------------|
| 带有NSS套件的 Infoblox-250设备, 100授权 | IB-250-100-NSS |
| 带有NSS套件的 Infoblox-250设备, 300授权 | IB-250-300-NSS |
| 带有NSS套件的 Infoblox-550 设备 | IB-550-NSS |
| 带有NSS套件的 Infoblox-1050 设备 | IB-1050-NSS |
| 带有NSS套件的 Infoblox-1550 设备 | IB-1550-NSS |
| 带有NSS套件的 Infoblox-1552 设备 | IB-1552-NSS |
| 带有NSS套件的 Infoblox-2000 设备 | IB-2000-NSS |

Infoblox 产品质保与服务声明

标准的硬件质保期为一年。系统软件的质保期为90天，软件符合声明规范。可选的、扩展硬件和软件质保声明的服务产品也是可获得的。推荐使用可选产品，以确保设备得到最新的软件功能升级，从而保证系统的安全性和可用性。Infoblox同时提供专业的服务和培训课程。此文档内容若有变更，恕不另行通知。Infoblox有限公司不在此文档中的错误负责。