DCYK IPv6 手册

目录

修订记录

本文档修订内容列表.

修订	修订说明
Rev 01	初始发布

IPv6 支持

IPv6 协议是下一代大规模 IP 网络，它支持 128 位长的地址。这允许 2 个可能的地址（而不是 2 个可能的 IPv4 地址）。

通常，在 IPv6 主机上分配的 IP 地址由 64 位子网标识符和 64 位接口标识符组成。IPv6 地址表示为八个冒号分隔的字段，每个字段最多四个十六进制数字。以下是 IPv6 地址的示例：

2001:0000:0eab:DEAD:0000:00A0:ABCD:004E

使用 symbol 是一种特殊语法，可用于压缩一组或多组零或压缩地址中的前导或尾随零。这在一个地址中只能出现一次。

例如，地址，

2001：0000：0dea：C1AB：0000：00D0：ABCD：004E 也可以表示为：

2001:0:eab:DEAD:0:A0:ABCD:4E – leading zeros can be omitted

2001:0:0eab:dead:0:a0:abcd:4e – not case sensitive

2001:0:0eab:dead::a0:abcd:4e - valid

2001::eab:dead::a0:abcd:4e - invalid

IPv6 使用“/”表示法来描述网络掩码中位的 no：，类似于 IPv4。

2001:eab::1/128 – single Host

2001:eab::/64 – network

原生 IPv6 支持

神州云科 OS 现在提供原生 IPv6 支持，允许企业使用移动导体和托管设备部署纯 IPv6 无线网络。在本机 IPv6 部署中，受管设备上运行的所有应用程序和进程都支持 IPv6 地址，以便在移动导体和受管设备之间实现无缝通信。本机 IPv6 部署适用于 Mobility Conductor 和托管设备之间的以下场景：

- 如果移动导体和受管设备都配置为纯 IPv6 部署（未配置 IPv4 地址），则 AP 仅在受管设备上提供有效的 IPv6 地址。
- 如果 Mobility Conductor 和受管设备都配置为纯 IPv6 部署（受管设备配置为双堆栈部署，但 Mobility Conductor 配置时没有 IPv4 地址），则无论群集如何，AP 都会以 IPv4 或 IPv6 地址在受管设备上启动。

本机 IPv6 部署会影响以下组件:

- VLAN 接口 — VLAN 接口上的 IPv4 地址现在对于移动导线和受管设备是可选的。因此，根据部署类型，您可以配置 IPv4 地址、IPv6 地址或两者的组合。
- Conductor IP 地址 — 配置 IPv6 地址时，不强制配置 Mobility Conductor 或受管设备的 IPv4 地址。现在，当在 Mobility Conductor 上配置 IPv6 地址时，您可以删除 Mobility Conductor 的 IPv4 地址。此外，当受管设备使用 VPNC 连接到移动导体时，VPNC 上的 IPv4 地址在导体 IP 配置期间是可选的。
- VRRP IP 地址 — 在第 2 层冗余场景中，不强制配置 VRRP 的 IPv4 地址。
- LMS IP 地址 — AMON 源中的 LMS IP 地址现在填充了 IPv4 和 IPv6 地址，具体取决于 Mobility Conductor 和受管设备上 IPv4 或 IPv6 地址的类型和可用性。本机 IPv6 部署还决定了用于传输 AMON 消息的 PAPI 传输和隧道的类型。
- 通过 DHCP 的 ZTP — 在本机 IPv6 部署中，受管设备还通过 DHCP 选项 17 和选项 16 字段获取 IPv6 地址，以便在 ZTP 期间查找移动导体。因此，DHCP 选项 17 字段中不需要移动导体的 IPv4 地址。
- 设置对话框 - 完整设置对话框现在提供仅配置 IPv4、IPv6 或两者组合的灵活性。如果使用 IPv6 地址终止 IPsec 隧道，则不再强制要求在设置对话框的 Mobility Conductor IP 配置中配置 IPv4 地址。

提示:不建议在本机 IPv6 部署中使用小型设置对话框。

提示:在本机 IPv6 部署中，最初启动运行 神州云科 OS 8.7.1.2 或更早映像的 AP 大约需要 30 分钟。对于运行 神州云科 OS 8.7.1.3 或更高版本映像的 AP，最初启动 AP 大约需要 17 分钟。

从 神州云科 OS 8.7.0.0 开始，您可以在设备和组级别删除控制器 IPv4 地址，同时使用 no controller-ip 命令从纯 IPv4 或双栈部署迁移到本机 IPv6 部署。

以下更改是作为 no controller-ip 命令：

1.在以下情况下，您可以删除控制器 IPv4 地址：

- 当有效的控制器 IPv6 地址在同一设备或组级别可用时。
- 当控制器上有一个 IPv4 地址可用时。

2.当有多个 IPv4 地址可用时，您无法删除控制器 IPv4 地址。因此，您必须确保只有控制器 IPv4 及其接口地址是迁移过程中要删除的最后剩余 IPv4 实体。根据具体情况，发出 no controller-ip 命令时，CLI 中会显示以下错误之一：

Controller IPv4 cannot be removed. Please configure controller-ipv6 on some

other valid vlan or the loopback

Controller IPv4 cannot be removed. Multiple v4 addresses exist on the

controller"

3.尝试删除控制器 IPv4 地址时，会发出以下命令，自动删除相应 VLAN 或环回接口上最后剩余的 IPv4 地址：

- 对于 VLAN 接口：

interface vlan <id> no ip address

- 对于环回接口：

interface loopback no ip address

4.验证代码阻止了删除最后剩余 IPv4 地址的尝试，并在 CLI 中显示以下错误消息：

Controller IPv4 configured with this address. Execute <no controller-ip> command

to auto-delete the interface address.

支持的应用程序

神州云科 OS 支持以下应用程序或方案的本机 IPv6 部署：

- Mobility Conductors 和托管设备中的应用程序，这些应用程序直接连接或通过 IPv6 网

络中的 VPNC 连接。

- 在 IPv6 网络中连接的初级和次级移动导体中的应用程序。
- 集群部署中的远程 AP 内部 IP 池。
- 配置了 IPv6 地址的 RADIUS 服务器的 ClearPass Policy Manager 可下载用户角色。
- 通过以下标准协议与服务器通信:
  - NTP
  - SNMP
  - SCP
  - FTP
  - TFTP
  - RADIUS
- 在 ARM 配置文件中配置 ClientMatch。
- 配置 upgrademgr 进程在 Mobility Conductors 和受管设备之间。
- AirMatch 中的计划部署。
- WebCC 功能，用于从云服务下载用于 Web 分类的数据库。

要记住的要点

- 以下应用或方案目前不支持本机 IPv6 部署:
  - Airgroup
  - UCC
  - 激活 ZTP 或允许列表下载
  - 用于动态路由 的 OSPF
- 终止 VIA 连接的受管设备
- 使用 DHCP 和 VLAN 池配置将 IP 地址分配给受管设备
- 使用 IPv6 帮助程序地址的 DHCP 中继。
- 以下 WAN 上行链路功能:

- 动态路径选择
- IP 健康检查
- 上行链路负载均衡
- 广域网优化
- Cellular

- 通过以下标准协议与服务器通信:
  - Kerberos
  - NTLM
  - WISPr
  - LDAP
  - Dynamic DNS
  - 证书注册的 EST

有关在双栈和本机 IPv6 网络中部署 神州云科 Mobility Conductor 和托管设备的更多信息，请参阅 神州云科 OS 8.x IPv6 部署指南。

启用 IPv6

在使用任何 IPv6 功能之前，必须在受管设备上启用 IPv6 选项。您可以使用该命令在受管设备上启用 IPv6 数据包或防火墙处理。默认情况下，IPv6 选项处于禁用状态。

以下过程介绍如何启用 IPv6 选项:

1.在 Mobility Conductor 节点层次结构，导航到配置 > 服务>防火墙 tab.

2.展开全局设置列表。

3.点击启用 IPv6 复选框以启用 IPv6 选项。

4.点击提交。

5.点击挂起的更改。

6.在挂起的更改窗口中，选中该复选框，然后单击部署更改。

提示:对于 7000 系列和 7200 系列控制器，必须在全局级别启用或禁用 IPv6 选项后重新

启动控制器。此外，还建议在全局级别禁用 IPv6 选项之前删除与 IPv6 相关的参数。

提示:从 IPv4 迁移到双栈或纯 IPv6 部署时，必须先启用 IPv6 选项，然后重新启动控制器。控制器启动后，您可以配置与 IPv6 相关的参数。

启用对 Mobility Conductor 和 AP 的 IPv6 支持

此版本的 神州云科 OS 为 Mobility Conductor 和接入点提供 IPv6 支持。现在，您可以使用 IPv6 地址配置 Mobility Conductor 来管理受管设备和 AP。IPv4 和 IPv6 AP 都可以在 IPv6 托管设备上终止。当受管设备接口配置了 IPv6 地址时，您可以在网络中预配 IPv4 或 IPv6 AP。IPv6 AP 可以同时为 IPv4 和 IPv6 客户端提供服务。

从 神州云科 OS 8.4.0.0 开始，您可以在 AP MultiZone 配置文件的一个数据区域中配置 IPv4 和 IPv6 地址，也可以同时配置 IPv4 和 IPv6 地址。有关配置 AP MultiZone 配置文件的详细信息，请参阅第 464 页的配置 MultiZone。

提示:您必须在受管设备接口上手动配置 IPv6 地址才能启用 IPv6 支持。

您还可以使用以下命令查看受管设备上的 IPv6 统计信息:

- show datapath ip-reassembly ipv6 — View the IPv6 contents of the IP reassembly statistics table.
- show datapath route ipv6 — View datapath IPv6 routing table.
- show datapath route-cache ipv6 — View datapath IPv6 route cache.
- show datapath tunnel ipv6 — View the tcp tunnel table filtered on IPv6 entries.
- show datapath user ipv6 — View datapath IPv6 user statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users, and maximum link length.
- show datapath session ipv6 — View datapath IPv6 session entries and statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users, and maximum link length.
- show controller-ipv6 — View IPv6 address and VLAN interface ID of the managed device.

此外，您可以使用以下 show 命令查看受管设备上的 IPv6 AP 信息:

- show ap database
- show ap active
- show user
- show ap details ip6-addr
- show ap debug

下表列出了 IPv6 功能:

IPv6 AP 支持矩阵

特性	在 IPv6 AP 上受支持
Forward Mode - Tunnel	Yes
Forward Mode - Decrypt Tunnel	Yes
Forward Mode - Bridge	Yes
Forward Mode - Split Tunnel	Yes
AP Type - Campus AP	Yes
AP Type - Remote AP	Yes
AP Type - Mesh Node No	Yes
CPsec	Yes
Wired-AP or Secure-Jack	Yes
Fragmentation or Reassembly	Yes
MTU Discovery	Yes
Provisioning Through Static IPv6 Addresses	Yes
Provisioning Through IPv6 FQDNConductor Name	Yes
Provisioning from WebUI	Yes
Provisioning Through IPv6 FQDN	Yes
Provisioning Through DHCPv6 Option 52	Yes
AP Boot by Flash	Yes
AP Boot by TFTP	Yes

特性	在 IPv6 AP 上受支持
WMM QoS	Yes
AP Debug and Syslog	Yes
ARM & AM	Yes
WIDS	Yes
CLI Support for Users and Datapath	Yes
AP MultiZone Profile	Yes
Duplicate Address Detection (DAD)	Yes

配置组播侦听器发现

您可以使用 WebUI 或 CLI 在受管设备上启用 IPv6 组播监听，并配置 MLD 参数，如查询间隔、查询响应间隔、鲁棒性变量和 ssm-range。

源特定组播 （SSM） 支持仅从接收方请求的特定源地址发送组播数据包的传送。如果源和组与客户端订阅的源组对 （S，G） 匹配，则可以将组播流转发到客户端。

受管设备支持以下 IPv6 组播源过滤模式：

- 包含 - 在包含模式下，仅从源列表中列出的源地址启用发送到指定组播地址的数据包接收。默认 IPv6 SSM 地址范围为 FF3X：：4000：1－FF3X：：FFFF：FFFF，订阅 SSM 组的主机只能处于包含模式。
- 排除 — 在排除模式下，启用从所有源地址发送到特定组播地址的数据包的接收。如果客户端处于排除模式，则订阅将被视为 MLDv1 联接。

MLD 侦听不会将 IPv6 请求节点组播地址或组添加到组播表中。请求节点组播地址是在本地链路（例如，以太网段或帧中继云）中有效的 IPv6 组播地址。每个 IPv6 主机每个接口至少有一个这样的地址。

请求节点组播地址在邻居发现协议中用于获取其他节点的第 2 层链路层地址。

筛选 IPv6 扩展标头

神州云科 OS 防火墙经过增强，可处理 IPv6 扩展标头以启用 IPv6 数据包过滤。您现在可以根据 EH 类型过滤传入的 IPv6 数据包。您可以使用 CLI 在默认 EH 中编辑数据包过滤器选项。默认 EH 别名允许所有 EH 类型。

以下 CLI 命令允许或拒绝与 EH 类型匹配的 IPv6 数据包。

((host) [md](config) #netexthdr default

(host) [md](config-exthdr) #eh <eh-type> permit | deny

以下 CLI 命令显示被拒绝的 EH 类型。

(host) [md](config-exthdr) #show netexthdr default

通过 IPv6 配置强制网络门户

现在，在强制网络门户上启用了 IPv6，以便在 神州云科 托管设备上进行用户身份验证。对于用户身份验证，请使用从受管设备启动的内部强制网络门户。已向 IPv6 强制网络门户会话 ACL 添加了一个新参数 captive：

(host) [md] (config)#ipv6 user alias controller 6 svc-https captive

提示:强制网络门户身份验证、页面自定义和其他属性与 IPv4 相同。

您可以使用 WebUI 或 CLI 配置基于 IPv6（类似于 IPv4）的强制网络门户。有关配置的详细信息，请参阅第 331 页的在基本操作系统中配置强制网络门户。

使用 IPv6 RA

神州云科 OS 使受管设备能够在 IPv6 网络中发送 RA。当您在主机上启用 ipv6 时，每个主机都会自动生成一个链路本地地址。链路本地地址允许主机在连接到同一链路的节点之间进行通信。

IPv6 无状态自动配置机制允许主机使用本地可用信息和路由器通告的信息的组合来生成自

己的地址。主机针对其在 IPv6 网络中的配置参数发送路由器请求组播请求。路由器请求的源地址可以是分配给发送接口的 IP 地址，也可以是未指定的地址（如果未分配给发送接口的地址）。

网络中的路由器以 RA 进行响应。RA 也可以定期发送。RA 包含第 3 层 IPv6 地址（IPv6 前缀）的网络部分。主机使用 RA 提供的 IPv6 前缀;它生成地址的通用唯一主机部分（接口标识符），并将两者组合在一起以派生完整的地址。要与默认路由器建立连续连接，主机将启动路由器的邻居可访问性状态机。

了解支持 IPv6 的身份验证和防火墙功能

本节介绍支持 IPv6 客户端的 神州云科 OS 功能。

了解身份验证

认证方式	IPv6 客户端的支持
802.1X	Yes
Stateful 802.1X	Yes
Local database	Yes
Captive Portal	Yes
VPN	Yes
xSec	No
MAC-based	Yes

为 IPv6 客户端配置 802.1X 身份验证的方式与为 IPv4 客户端配置配置的方式相同。有关在 Mobility Conductor 上配 置 802.1X 身份验证的详细信息，请参阅第 269 页的 802.1X 身份验证。

使用防火墙功能

如果在 Mobility Conductor 中安装了 PEFNG 许可证，则可以为 IPv6 客户端流量配置防

火墙功能。虽然这些防火墙功能 与 IPv4 客户端的防火墙功能相同，但您需要为 IPv6 流量显式配置它们。

提示:IPv6 流量不支持语音相关和 NAT 防火墙功能。

配置防火墙功能的方法如下:

1.在 Mobility Conductor 节点层次结构中，导航到“配置>服务>防火墙”选项卡。

2.展开 Global Setting 手风琴。

3. 在“IPv6”列下，输入以下内容:

a.输入“监视 ping 攻击”的值(每 30 秒)。

b.输入监控 IP 会话攻击的值(每 30 秒)。

c.输入“监视 TCP SYN 攻击速率(每 30 秒)”的值。

4. 点击提交。

5. 单击“挂起的更改”。

6. 在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

以下 CLI 命令配置防火墙功能:

```
(host) [mynode] (config)#ipv6 firew all attack-rate ping 15

(host) [mynode] (config)#ipv6 firewall attack-rate session 25

(host) [mynode] (config)#ipv6 firewall session-idle-timeout 60
```

了解防火墙策略

确定客户端网络权限的用户角色由一个或多个防火墙策略定义。防火墙策略由规则组成，这些规则定义特定流量的来源 目标和服务类型，以及是否希望受管设备允许或拒绝与规则匹配的流量。

您可以为 IPv4 流量或 IPv6 流量配置防火墙策略，并将 IPv4 和 IPv6 防火墙策略应用于同一用户角色。例如，如果您的 员工同时使用 IPv4 和 IPv6 客户端，则可以配置 IPv4 和 IPv6 防火墙策略，并将它们都应用于“员工”用户角色。

以下示例创建一个策略 ipv6-web-only， 该策略仅允许 IPv6 客户端进行 Web(HTTP 和

HTTPS) 访问，并将该策略分配 给用户角色 “web-guest”。

提示:用户角色 web-guest 可以同时包含 IPv6 和 IPv4 策略，但此示例仅显示 IPv6 策略的配置。

创建 IPv6 防火墙策略

以下过程介绍如何创建 IPv6 防火墙策略。

1.在“托管网络”节点层次结构中，导航到“配置”>“角色和策略”>“策略”选项卡。

2. 单击“+”创建新策略。

3. 输入 ipv6-web-only 作为策略名称。

4. 若要配置防火墙策略，请选择“会话”作为“策略类型”。

5. 点击提交。

6. 选择 ipv6-only 策略。

7. 单击“策略>ipv6-only web-rules”表中的“+”。

8. 在“规则类型”字段中选择“访问控制”选项，然后单击“确定”。

9. 从 IP 版本下拉列表中选择 IPv6。

10. 从“源”下拉列表中选择“网络”,然后输入以下值:

    a.对于 IPv6 地址，输入 2002:d81f:f9f0:1000::。

    b.对于 IPv6 网络掩码，输入 64 作为前缀长度。

    c.对于“服务/应用”,请从下拉列表中选择“服务”。 d.d.对于“服务别名”,从下拉列表中选择“svc-http”。

11. 点击提交。

12. 单击 ipv6-web-only 规则表>+策略，添加允许 HTTPS 流量的规则。

13. 在“规则类型”字段中选择“访问控制”选项，然后单击“确定”。

    a.在“IP 版本”列下，选择“IPv6”。

    b.从“源”下拉列表中选择“网络”。

    c.对于 IP，输入 2002:d81f:f9f0:1000::。

    d.对于“网络掩码”,输入 64 作为前缀长度。

e.在“服务/应用”下，从下拉列表中选择“服务”。 f.从滚动列表中选择 svc-https。

14. 点击提交。

提示:可以使用为每个规则提供的向上和向下箭头按钮对规则进行重新排序。

15. 单击“挂起的更改”。

16. 在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

以下 CLI 命令创建 IPv6 防火墙策略。

```
(host) [md] (config)#ip access-list session ipv6-web-only

(host) [md] (config-submode)#ipv6 network 2002:d81f:f9f0:1000::/64 any svc-http permit

(host) [md] (config-submode)#ipv6 network 2002:d81f:f9f0:1000::/64 any svc-https permit
```

将 IPv6 策略分配给用户角色

以下过程介绍如何分配 IPv6 策 略

1.在“托管网络”节点层次结构中，导航到“配置”>“角色和策略” >“角色”选项卡。

2.单击“+”创建新的用户角色。

3.在名称字段中输入 web-guest。

4.单击“提交”。

5.选择 web-guest 角色。

6.单击“显示高级视图”。

7.单击 Web 访客表>“角色”中的+。

8.在“新建策略”弹出窗口中选择“添加现有会话策略”选项。

9.从“策略名称”下拉列表中选择策略。

10.单击“提交”。

11.单击挂起的更改。

12.在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

以下 CLI 命令将 IPv6 策略分配给用户角色。

```
(host) [md] (config)#user-role web-guest

(host) [md] (config-submode)#access-list session ipv6-web-only position 1
```