目 录

1 域名解析

1.1 域名解析配置命令

1.1.1 display dns domain

display dns domain 命令用来显示域名后缀信息。

【命令】

display dns domain [**dynamic**] [**vpn-instance** *vpn-instance-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

dynamic：显示通过 DHCP 等协议动态获得的域名后缀信息。如果未指定本参数，则显示静态配置和动态获得的域名后缀信息。

vpn-instance *vpn-instance-name*：显示指定 VPN 内的域名后缀信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则显示公网的域名后缀信息。

【举例】

显示公网静态配置和动态获得的域名后缀信息。

```
<Sysname> display dns domain
Type:
  D: Dynamic    S: Static

No.    Type   Domain suffix
1      S      com
2      D      net
```

表1-1 display dns domain 命令显示信息描述表

字段	描述
No.	序号
Type	域名后缀类型： • S：表示静态配置的域名后缀 • D：表示通过 DHCP 等协议动态获得的域名后缀
Domain suffix	域名后缀

【相关命令】

- **dns domain**

1.1.2 display dns host

display dns host 命令用来显示域名解析信息。

【命令】

display dns host [**ip** | **ipv6**] [**vpn-instance** *vpn-instance-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

ip：显示 A 类查询的信息。A 类查询用来解析域名对应的 IPv4 地址。

ipv6：显示 AAAA 类查询的信息。AAAA 类查询用来解析域名对应的 IPv6 地址。

vpn-instance *vpn-instance-name*：显示指定 VPN 的域名解析信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则显示公网的域名解析信息。

【使用指导】

如果未指定 **ip** 和 **ipv6** 参数，则显示所有查询类型的域名解析信息。

【举例】

显示所有查询类型的域名解析信息。

```
<Sysname> display dns host
Type:
  D: Dynamic    S: Static

Total number: 3
No.  Host name         Type  TTL        Query type   IP addresses
1    sample.com        D     3132       A            192.168.10.1
                                                     192.168.10.2
                                                     192.168.10.3
2    zig.sample.com    S     -          A            192.168.1.1
3    sample.net        S     -          AAAA         FE80::4904:4448
```

表1-2 display dns host 命令显示信息描述表

字段	描述
No.	序号
Host name	查询名称

字段	描述
Type	域名解析信息的类型： • S：表示静态配置的域名解析信息，即通过 **ip host** 或 **ipv6 host** 命令配置的主机名及其对应的主机 IPv4/IPv6 地址 • D：表示通过动态域名解析获得的域名解析信息
TTL	域名解析信息的剩余有效时间，单位为秒 静态信息的TTL值显示为“-”
Query type	查询类型，取值包括A和AAAA
IP addresses	主机名对应的IP地址 • 对于 A 类查询类型，为 IPv4 地址 • 对于 AAAA 类查询类型，为 IPv6 地址

【相关命令】

- **reset dns host**
- **ip host**
- **ipv6 host**

1.1.3 display dns server

display dns server 命令用来显示域名服务器的 IPv4 地址信息。

【命令】

display dns server [**dynamic**] [**vpn-instance** *vpn-instance-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

dynamic：显示通过 DHCP 等协议动态获得的域名服务器 IPv4 地址信息。如果未指定本参数，则显示静态配置和动态获得的域名服务器 IPv4 地址信息。

vpn-instance *vpn-instance-name*：显示指定 VPN 内的域名服务器 IPv4 地址信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则显示公网的域名服务器 IPv4 地址信息。

【举例】

显示公网的域名服务器 IPv4 地址信息。

```
<Sysname> display dns server
Type:
  D: Dynamic    S: Static
```

```
No. Type  IP address
1   S     202.114.0.124
2   S     169.254.65.125
```

表1-3 display dns server 命令显示信息描述表

字段	描述
No.	域名服务器的序号，系统自动给所配置的服务器编号，从1开始
Type	域名服务器类型 • S 表示静态指定的域名服务器信息 • D 表示通过 DHCP 等协议动态获得的域名服务器信息
IP address	域名服务器的IPv4地址

【相关命令】

- **dns server**

1.1.4 display ipv6 dns server

display ipv6 dns server 命令用来显示域名服务器的 IPv6 地址信息。

【命令】

display ipv6 dns server [**dynamic**] [**vpn-instance** *vpn-instance-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

dynamic：显示通过 DHCP 等协议动态获得的域名服务器 IPv6 地址信息。如果未指定本参数，则显示静态配置和动态获得的域名服务器 IPv6 地址信息。

vpn-instance *vpn-instance-name*：显示指定 VPN 内的域名服务器 IPv6 地址信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则显示公网的域名服务器 IPv6 地址信息。

【举例】

显示公网域名服务器的 IPv6 地址信息。

```
<Sysname> display ipv6 dns server
Type:
  D: Dynamic    S: Static

No. Type  IPv6 address                            Outgoing Interface
1   S     2::2
```

表1-4 display ipv6 dns server 命令显示信息描述表

字段	描述
No.	域名服务器的序号
Type	域名服务器类型 • S 表示静态指定的域名服务器信息 • D 表示通过 DHCP 等协议动态获得的域名服务器信息
IPv6 address	域名服务器的IPv6地址
Outgoing Interface	出接口名

【相关命令】

- **ipv6 dns server**

1.1.5 dns domain

dns domain 命令用来添加域名后缀。

undo dns domain 命令用来删除指定的域名后缀。

【命令】

dns domain *domain-name* [**vpn-instance** *vpn-instance-name*]

undo dns domain *domain-name* [**vpn-instance** *vpn-instance-name*]

【缺省情况】

未配置域名后缀，即只根据用户输入的域名信息进行解析。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

domain-name：域名后缀，由“.”分隔的字符串组成（如 aabbcc.com），每个字符串的长度不超过 63 个字符，包括“.”在内的总长度不超过 253 个字符。不区分大小写，字符串中可以包含字母、数字、“-”、“_”或“.”。

vpn-instance *vpn-instance-name*：为指定 VPN 添加或删除域名后缀。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示为公网添加或删除域名后缀。

【使用指导】

域名解析时，用户只需要输入域名的部分字段，系统会按照域名后缀配置的先后顺序，依次将输入的域名加上不同的域名后缀进行解析。

本命令配置的域名后缀同时用于 IPv4 域名解析和 IPv6 域名解析。

公网或每个 VPN 实例内最多可以配置 16 个域名后缀。可同时在公网和 VPN 实例内配置域名后缀。

【举例】

为公网添加一个域名后缀 com。

```
<Sysname> system-view
[Sysname] dns domain com
```

【相关命令】

- **display dns domain**

1.1.6 dns dscp

dns dscp 命令用来配置发送 DNS 报文的 DSCP 优先级。

undo dns dscp 命令用来恢复缺省情况。

【命令】

dns dscp *dscp-value*

undo dns dscp

【缺省情况】

发送 DNS 报文的 DSCP 优先级为 0。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

dscp-value：DNS 报文的 DSCP 优先级，取值范围为 0～63。

【使用指导】

DSCP 优先级用来体现报文自身的优先等级，决定报文传输的优先程度。配置的 DSCP 优先级的取值越大，报文的优先级越高。

通过本命令可以指定 DNS 客户端或 DNS proxy 发送的 DNS 报文中携带的 DSCP 优先级的取值。

【举例】

配置发送的 DNS 报文的 DSCP 优先级为 30。

```
<Sysname> system-view
[Sysname] dns dscp 30
```

1.1.7 dns proxy enable

dns proxy enable 命令用来开启 DNS proxy 功能。

undo dns proxy enable 命令用来关闭 DNS proxy 功能。

【命令】

dns proxy enable

undo dns proxy enable

【缺省情况】

DNS proxy 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

本命令的配置同时用于 IPv4 域名解析和 IPv6 域名解析。

【举例】

开启 DNS proxy 功能。

```
<Sysname> system-view
[Sysname] dns proxy enable
```

1.1.8 dns server

dns server 命令用来配置域名服务器的 IPv4 地址。

undo dns server 命令用来删除域名服务器的 IPv4 地址。

【命令】

dns server *ip-address* [**vpn-instance** *vpn-instance-name*]

undo dns server [*ip-address*] [**vpn-instance** *vpn-instance-name*]

【缺省情况】

未配置域名服务器的 IPv4 地址。

【视图】

系统视图

接口视图

【缺省用户角色】

network-admin

【参数】

ip-address：域名服务器的 IPv4 地址。

vpn-instance *vpn-instance-name*：为指定 VPN 配置或删除域名服务器的 IPv4 地址。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示为公网配置或删除域名服务器的 IPv4 地址。

【使用指导】

在系统视图下，公网或单个 VPN 实例内最多可以配置 6 个域名服务器的 IPv4 地址。可同时在公网和 VPN 实例内配置域名服务器的 IPv4 地址。

在接口视图下，公网或单个 VPN 实例内最多可以配置 6 个域名服务器的 IPv4 地址。可同时在公网和 VPN 实例内配置域名服务器的 IPv4 地址。

域名服务器的优先级顺序为：系统视图下配置的域名服务器优先级高于接口视图下配置的域名服务器；先配置的域名服务器优先级高于后配置的域名服务器；设备上手工配置的域名服务器优先级高于通过 DHCP 等方式动态获取的域名服务器。设备首先向优先级最高的域名服务器发送查询请求，失败后再依次向其他域名服务器发送查询请求。

执行 **undo dns server** 命令时如果未指定 *ip-address* 参数，则删除公网或指定 VPN 实例中的所有域名服务器 IPv4 地址。

【举例】

配置域名服务器的 IPv4 地址为 172.16.1.1。

```
<Sysname> system-view
[Sysname] dns server 172.16.1.1
```

在接口 GigabitEthernet2/1/1 配置域名服务器的 IPv4 地址为 172.16.1.1。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/1/1
[Sysname-GigabitEthernet2/1/1] dns server 172.16.1.1
```

【相关命令】

- **display dns server**

1.1.9 dns source-interface

dns source-interface 命令用来指定 DNS 报文的源接口。

undo dns source-interface 命令用来恢复缺省情况。

【命令】

dns source-interface *interface-type interface-number* [**vpn-instance** *vpn-instance-name*]

undo dns source-interface *interface-type interface-number* [**vpn-instance** *vpn-instance-name*]

【缺省情况】

设备根据 DNS server 的地址，通过路由表查找报文的出接口，并将该出接口的主 IP 地址作为发送到该服务器的 DNS 查询报文的源地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interface-type interface-number：源接口的接口类型和接口编号。

vpn-instance *vpn-instance-name*：为指定 VPN 配置 DNS 报文的源接口。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示为公网配置 DNS 报文的源接口。

【使用指导】

通过本命令指定 DNS 报文的源接口后，系统将选择指定接口的主 IPv4 地址或根据 RFC 3484 中定义的规则选择指定接口的某个 IPv6 地址，作为 DNS 查询报文的源地址。

本命令的配置同时用于 IPv4 域名解析和 IPv6 域名解析。

公网或每个 VPN 实例内只能配置 1 个源接口。多次执行本命令，最后一次执行的命令生效。可同时在公网和 VPN 实例配置源接口。

无论配置的源接口是否属于指定的 VPN，该配置都会生效。不建议将不属于 VPN 的接口配置为该 VPN 的源接口。

【举例】

指定公网 DNS 报文的源接口为 GigabitEthernet2/1/1。

```
<Sysname> system-view
[Sysname] dns source-interface gigabitethernet 2/1/1
```

1.1.10 dns spoofing

dns spoofing 命令用来开启 DNS spoofing 功能，并指定应答的 IPv4 地址。

undo dns spoofing 命令关闭 DNS spoofing 功能。

【命令】

dns spoofing *ip-address* [**vpn-instance** *vpn-instance-name*]

undo dns spoofing *ip-address* [**vpn-instance** *vpn-instance-name*]

【缺省情况】

DNS spoofing 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ip-address：用来欺骗性应答域名解析请求的 IPv4 地址。

vpn-instance *vpn-instance-name*：为指定 VPN 配置 DNS spoofing 功能。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示为公网配置 DNS spoofing 功能。

【使用指导】

配置 DNS spoofing 前，需要先开启 DNS proxy 功能。

开启 DNS spoofing 功能后，如果设备上未配置域名服务器地址或不存在到达域名服务器的路由，则会利用配置的应答 IP 地址作为域名解析结果，欺骗性地应答 A 类域名解析请求。

公网或每个 VPN 内只能配置 1 个 DNS spoofing 应答的 IPv4 地址。多次执行本命令，最后一次执行的命令生效。可同时在公网和 VPN 实例内配置 DNS spoofing 功能。

【举例】

开启公网的 DNS spoofing 功能，并指定应答的 IPv4 地址为 1.1.1.1。

```
<Sysname> system-view
[Sysname] dns proxy enable
[Sysname] dns spoofing 1.1.1.1
```

【相关命令】

- **dns proxy enable**

1.1.11 dns spoofing track

dns spoofing track 命令用来配置监视指定出接口的网络制式。

undo dns spoofing track 命令用来恢复缺省情况。

【命令】

dns spoofing track controller *interface-type interface-number*

undo dns spoofing track

【缺省情况】

未配置监视指定出接口的网络制式。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

controller *interface-type interface-number*：指定被监视的出接口，*interface-type interface-number* 表示接口类型和接口编号。

【使用指导】

配置监视指定出接口的网络制式时，需要先开启 DNS spoofing 或 IPv6 DNS spoofing 功能。

多次执行本命令，最后一次执行的命令生效。

【举例】

配置监视指定出接口 Cellular0/1 的网络制式，并配置欺骗应答的 IP 地址为 192.168.1.10。

```
<Sysname> system-view
[Sysname] dns proxy enable
[Sysname] dns spoofing 192.168.1.10
[Sysname] dns spoofing track controller cellular 0/1
```

【相关命令】

- **dns spoofing**
- **ipv6 dns spoofing**

1.1.12 dns trust-interface

dns trust-interface 命令用来指定 DNS 信任接口。

undo dns trust-interface 命令用来删除指定的 DNS 信任接口。

【命令】

dns trust-interface *interface-type interface-number*

undo dns trust-interface [*interface-type interface-number*]

【缺省情况】

未指定任何接口为信任接口。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interface-type interface-number：DNS 信任接口的接口类型和接口编号。

【使用指导】

缺省情况下，任意接口通过 DHCP 等协议动态获得的域名后缀和域名服务器信息都将作为有效信息，用于域名解析。如果网络攻击者通过 DHCP 服务器为设备分配错误的域名后缀和域名服务器地址，则会导致设备域名解析失败，或解析到错误的结果。通过本配置指定信任接口后，域名解析时只采用信任接口动态获得的域名后缀和域名服务器信息，非信任接口获得的信息不能用于域名解析，从而在一定程度上避免这类攻击。

本命令同时用于 IPv4 域名解析和 IPv6 域名解析。

设备最多可以配置 128 个信任接口。

执行 **undo dns trust-interface** 命令时，如果未指定任何接口，则删除所有的 DNS 信任接口，恢复到缺省情况。

【举例】

指定接口 GigabitEthernet2/1/1 为 DNS 信任接口。

```
<Sysname> system-view
[Sysname] dns trust-interface gigabitethernet 2/1/1
```

1.1.13 ip host

ip host 命令用来配置主机名及其对应的主机 IPv4 地址。

undo ip host 命令用来删除主机名及其对应的主机 IPv4 地址。

【命令】

ip host *host-name ip-address* [**vpn-instance** *vpn-instance-name*]

undo ip host *host-name ip-address* [**vpn-instance** *vpn-instance-name*]

【缺省情况】

不存在主机名及 IPv4 地址的对应关系。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

host-name：主机名，为 1～253 个字符的字符串，不区分大小写，字符串中可以包含字母、数字、“-”、“_”和“.”。

ip-address：与主机名对应的 IPv4 地址。

vpn-instance *vpn-instance-name*：为指定 VPN 配置主机名和 IPv4 地址的对应关系。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示为公网配置主机名和 IPv4 地址的对应关系。

【使用指导】

公网或单个 VPN 内最多可以配置 1024 个主机名和 IPv4 地址的对应关系。可同时在公网和 VPN 实例内配置主机名和 IPv4 地址的对应关系。

在公网或单个 VPN 内，一个主机名只能对应一个 IPv4 地址。多次执行本命令，最后一次执行的命令生效。

ip、**-a**、**-c**、**-f**、**-h**、**-i**、**-m**、**-n**、**-p**、**-q**、**-r**、**-s**、**-t**、**-tos**、**-v** 和**-vpn-instance** 已被系统用作 **ping** 命令的参数关键字，在配置主机名时，请避免使用相同的字符串作为主机名。**ping** 命令支持的参数形式，请参考“网络管理和监控”中的“**ping**”命令。

【举例】

配置公网内主机名 aaa 对应的 IPv4 地址为 10.110.0.1。

```
<Sysname> system-view
[Sysname] ip host aaa 10.110.0.1
```

【相关命令】

- **display dns host**

1.1.14 ipv6 dns dscp

ipv6 dns dscp 命令用来配置发送 IPv6 DNS 报文的 DSCP 优先级。

undo ipv6 dns dscp 命令用来恢复缺省情况。

【命令】

ipv6 dns dscp *dscp-value*

undo ipv6 dns dscp

【缺省情况】

发送 IPv6 DNS 报文的 DSCP 优先级为 0。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

dscp-value：IPv6 DNS 报文的 DSCP 优先级，取值范围为 0～63。

【使用指导】

DSCP 优先级用来体现报文自身的优先等级，决定报文传输的优先程度。配置的 DSCP 优先级的取值越大，报文的优先级越高。

通过本命令可以指定 IPv6 DNS 客户端或 DNS proxy 发送的 IPv6 DNS 报文中携带的 DSCP 优先级的取值。

【举例】

配置发送的 IPv6 DNS 报文的 DSCP 优先级为 30。

```
<Sysname> system-view
[Sysname] ipv6 dns dscp 30
```

1.1.15 ipv6 dns server

ipv6 dns server 命令用来配置域名服务器的 IPv6 地址。

undo ipv6 dns server 命令用来删除域名服务器的 IPv6 地址。

【命令】

ipv6 dns server *ipv6-address* [*interface-type interface-number*] [**vpn-instance** *vpn-instance-name*]

undo ipv6 dns server [*ipv6-address* [*interface-type interface-number*]] [**vpn-instance** *vpn-instance-name*]

【缺省情况】

未配置域名服务器的 IPv6 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6-address：域名服务器的 IPv6 地址。

interface-type interface-number：指定报文的出接口的接口类型和接口编号。如果未指定本参数，则根据路由表查找报文的出接口。域名服务器的 IPv6 地址为链路本地地址时，必须指定本参数。域名服务器的 IPv6 地址为全球单播地址时，无法指定本参数。

vpn-instance *vpn-instance-name*：为指定 VPN 配置或删除域名服务器的 IPv6 地址。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示为公网配置或删除域名服务器的 IPv6 地址。

【使用指导】

在进行动态域名解析时，系统按照域名服务器 IPv6 地址配置的先后顺序，依次向各个域名服务器发送查询请求。

公网或单个 VPN 内最多可以配置 6 个域名服务器的 IPv6 地址。可同时在公网和 VPN 实例内配置域名服务器的 IPv6 地址。

执行 **undo ipv6 dns server** 命令时如果未指定 *ipv6-address* 参数，则删除公网或指定 VPN 中的所有域名服务器 IPv6 地址。

【举例】

配置公网内域名服务器的 IPv6 地址为 2002::1。

```
<Sysname> system-view
[Sysname] ipv6 dns server 2002::1
```

【相关命令】

- **display ipv6 dns server**

1.1.16 ipv6 dns spoofing

ipv6 dns spoofing 命令用来开启 DNS spoofing 功能，并指定应答的 IPv6 地址。

undo ipv6 dns spoofing 命令用来关闭 DNS spoofing 功能。

【命令】

ipv6 dns spoofing *ipv6-address* [**vpn-instance** *vpn-instance-name*]

undo ipv6 dns spoofing *ipv6-address* [**vpn-instance** *vpn-instance-name*]

【缺省情况】

DNS spoofing 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6-address：用来欺骗性应答域名解析请求的 IPv6 地址。

vpn-instance *vpn-instance-name*：为指定 VPN 配置 DNS spoofing 功能。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示为公网配置 DNS spoofing 功能。

【使用指导】

开启 DNS spoofing 功能后，如果设备上未配置域名服务器地址或不存在到达域名服务器的路由，则会利用配置的应答 IPv6 地址作为域名解析结果，欺骗性地应答 AAAA 类域名解析请求。当设备上存在可达的域名服务器时，设备将向该服务器发送域名解析请求，并将正确的解析结果返回给 DNS 客户端。

公网或每个 VPN 内只能配置 1 个 DNS spoofing 应答的 IPv6 地址。多次执行本命令，最后一次执行的命令生效。可同时在公网和 VPN 实例内配置 DNS spoofing 功能。

本命令必须和 **dns proxy enable** 命令一起使用。

【举例】

为公网开启 DNS spoofing 功能，并指定应答的 IPv6 地址为 2001::1。

```
<Sysname> system-view
[Sysname] dns proxy enable
```

```
[Sysname] ipv6 dns spoofing 2001::1
```

【相关命令】

- **dns proxy enable**

1.1.17 ipv6 host

ipv6 host 命令用来配置主机名及其对应的主机 IPv6 地址。

undo ipv6 host 命令用来删除主机名及其对应的主机 IPv6 地址。

【命令】

ipv6 host *host-name ipv6-address* [**vpn-instance** *vpn-instance-name*]

undo ipv6 host *host-name ipv6-address* [**vpn-instance** *vpn-instance-name*]

【缺省情况】

不存在主机名及 IPv6 地址的对应关系。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

host-name：主机名，为 1～253 个字符的字符串，不区分大小写，字符串中可以包含字母、数字、“-”、“_”和“.”。

ipv6-address：与主机名对应的 IPv6 地址。

vpn-instance *vpn-instance-name*：为指定 VPN 配置主机名和 IPv6 地址的对应关系。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示为公网配置主机名和 IPv6 地址的对应关系。

【使用指导】

公网或每个 VPN 内最多可以配置 1024 个主机名和 IPv6 地址的对应关系。可同时在公网和 VPN 实例内配置主机名和 IPv6 地址的对应关系。

在公网或同一个 VPN 实例内，一个主机名只能对应一个 IPv6 地址。多次执行本命令，最后一次执行的命令生效。

-a、**-c**、**-i**、**-m**、**-q**、**-s**、**-t**、**-tc**、**-v** 和**-vpn-instance** 已被系统用作 **ping ipv6** 命令的参数关键字，在配置主机名时，请避免使用相同的字符串作为主机名。**ping ipv6** 命令支持的参数形式，请参考“网络管理和监控”中的“**ping ipv6**”命令。

【举例】

配置公网内主机名 aaa 对应的 IPv6 地址为 2001::1。

```
<Sysname> system-view
[Sysname] ipv6 host aaa 2001::1
```

【相关命令】

- **ip host**

1.1.18 reset dns host

reset dns host 命令用来清除动态域名解析缓存信息。

【命令】

reset dns host [**ip** | **ipv6**] [**vpn-instance** *vpn-instance-name*]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

ip：清除 A 类查询的动态缓存信息。A 类查询用来解析域名对应的 IPv4 地址。

ipv6：清除 AAAA 类查询的动态缓存信息。AAAA 类查询用来解析域名对应的 IPv6 地址。

vpn-instance *vpn-instance-name*：清除指定 VPN 的动态域名解析缓存信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则清除公网的动态域名解析缓存信息。

【使用指导】

如果未指定 **ip** 和 **ipv6** 参数，则清除所有查询类型的动态域名解析缓存信息。

【举例】

清除公网所有查询类型的动态域名解析缓存信息。

```
<Sysname> reset dns host
```

【相关命令】

- **display dns host**

2 DDNS

2.1 DDNS配置命令

2.1.1 ddns apply policy

ddns apply policy 命令用来在接口上应用指定的 DDNS 策略来更新指定的 FQDN 与 IP 地址的对应关系，并启动 DDNS 更新。

undo ddns apply policy 命令用来在接口上取消应用 DDNS 策略，停止 DDNS 更新。

【命令】

ddns apply policy *policy-name* [**fqdn** *domain-name*]

undo ddns apply policy *policy-name*

【缺省情况】

没有为接口指定任何 DDNS 策略和需要更新的 FQDN，且未启动 DDNS 更新。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

policy-name：DDNS 策略名称，为 1～32 个字符的字符串，不区分大小写。

fqdn *domain-name*：指定需要更新该 FQDN 与 IP 地址的对应关系，用于替换 DDNS 更新请求 URL 中的<h>。*domain-name* 为主机名，主机名，为 1～253 个字符的字符串，不区分大小写，字符串中可以包含字母、数字、“-”、“_”和“.”。

【使用指导】

一个接口上最多可以应用 4 个 DDNS 策略。

重复应用名称相同的 DDNS 策略，并指定不同的 FQDN 时，最后一次执行的命令生效，同时发起一次 DDNS 更新。

【举例】

在接口 GigabitEthernet2/1/1 下指定应用 DDNS 策略 steven_policy 来更新合格域名 www.whatever.com 与 IP 地址的对应关系，并启动 DDNS 更新功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 2/1/1
[Sysname-GigabitEthernet2/1/1] ddns apply policy steven_policy fqdn www.whatever.com
```

【相关命令】

- **ddns policy**
- **display ddns policy**

2.1.2 ddns dscp

ddns dscp 命令用来配置发送 DDNS 报文的 DSCP 优先级。

undo ddns dscp 命令用来恢复缺省情况。

【命令】

ddns dscp *dscp-value*

undo ddns dscp

【缺省情况】

配置发送 DDNS 报文的 DSCP 优先级为 0。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

dscp-value：DDNS 报文的 DSCP 优先级，取值范围为 0～63。

【使用指导】

DSCP 优先级用来体现报文自身的优先等级，决定报文传输的优先程度。配置的 DSCP 优先级的取值越大，报文的优先级越高。通过本命令可以指定发送的 DDNS 报文中携带的 DSCP 优先级的取值。

【举例】

配置发送的 DDNS 报文的 DSCP 优先级为 30。

```
<Sysname> system-view
[Sysname] ddns dscp 30
```

2.1.3 ddns policy

ddns policy 命令用来创建 DDNS 策略，并进入 DDNS 策略视图。如果指定的 DDNS 策略视图已存在，则直接进入 DDNS 策略视图。

undo ddns policy 命令用来删除 DDNS 策略。

【命令】

ddns policy *policy-name*

undo ddns policy *policy-name*

【缺省情况】

设备上不存在 DDNS 策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

policy-name：DDNS 策略名称，为 1～32 个字符的字符串，不区分大小写。

【使用指导】

设备上最多可以创建 16 个 DDNS 策略。

【举例】

创建名称为 steven_policy 的 DDNS 策略，并进入 DDNS 策略视图。

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
```

【相关命令】

- **display ddns policy**
- **ddns apply policy**

2.1.4 display ddns policy

display ddns policy 命令用来显示 DDNS 策略的信息。

【命令】

display ddns policy [*policy-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

policy-name：DDNS 策略名称，为 1～32 个字符的字符串，不区分大小写。如果未指定本参数，则显示所有 DDNS 策略的信息。

【举例】

显示名称为 steven_policy 的 DDNS 策略的信息。

```
<Sysname> display ddns policy steven_policy
DDNS policy: steven_policy
  URL              : http://members.3322.org/dyndns/update?
                     system=dyndns&hostname=<h>&myip=<a>
  Username         : steven
  Password         : ******
  Method           : GET
  SSL client policy:
  Interval         : 1 days 0 hours 1 minutes
```

显示所有 DDNS 策略的信息。

```
<Sysname> display ddns policy
DDNS policy: steven_policy
  URL              : http://members.3322.org/dyndns/update?system=
```

```
                    dyndns&hostname=<h>&myip=<a>
  Username          : steven
  Password          : ******
  Method            : GET
  SSL client policy:
  Interval          : 0 days 0 hours 30 minutes

DDNS policy: tom-policy
  URL               : http://members.3322.org/dyndns/update?system=
                      dyndns&hostname=<h>&myip=<a>
  Username          :
  Password          :
  Method            : GET
  SSL client policy:
  Interval          : 0 days 0 hours 15 minutes

DDNS policy: u-policy
  URL               : oray://phservice2.oray.net
  Username          : username
  Password          :
  Method            : -
  SSL client policy:
  Interval          : 0 days 0 hours 15 minutes
```

表2-1 display ddns policy 命令显示信息描述表

字段	描述
DDNS policy	DDNS策略名称
URL	DDNS更新请求的URL地址。未配置时显示为空
Username	登录DDNS服务器的用户名。未配置时显示为空
Password	登录DDNS服务器的密码。未配置时显示为空，有配置时显示为“******”
Method	采用HTTP或HTTPS报文发送DDNS更新请求时，使用的参数传输方式 取值包括： • GET：表示使用 HTTP 或 HTTPS 报文发送 DDNS 更新请求，且参数传输方式为 GET 方式 • POST：表示使用 HTTP 或 HTTPS 报文发送 DDNS 更新请求，且参数传输方式为 POST 方式
SSL client policy	关联的SSL客户端策略名称。未配置时显示为空
Interval	定时发起DDNS更新请求的时间间隔

【相关命令】

- **ddns policy**

2.1.5 interval

interval 命令用来指定定时发起更新请求的时间间隔。

undo interval 命令用来恢复缺省情况。

【命令】

interval *days* [*hours* [*minutes*]]

undo interval

【缺省情况】

定时发起 DDNS 更新请求的时间间隔是 1 小时。

【视图】

DDNS 策略视图

【缺省用户角色】

network-admin

【参数】

days：天，取值范围为 0～365。

hours：小时，取值范围为 0～23。

minutes：分钟，取值范围为 0～59。

【使用指导】

不论是否到达定时发起更新请求的时间，只要对应接口的主 IP 地址发生改变或接口的链路状态由 down 变为 up，都会立即发起更新请求。

如果配置时间间隔为 0，则不会定时发起更新，除非对应接口的 IP 地址发生改变或接口的链路状态由 down 变为 up。

多处执行本命令，最后一次执行的命令生效。如果 DDNS 策略已经应用到接口上，则立即触发一次 DDNS 更新，并以最后一次配置的时间间隔为更新周期。

【举例】

为 DDNS 策略 steven_policy 指定定时发起更新请求的时间间隔为 1 天零 1 分。

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
[Sysname-ddns-policy-steven_policy] interval 1 0 1
```

【相关命令】

- **display ddns policy**
- **ddns policy**

2.1.6 method

method 命令用来配置采用 HTTP 或 HTTPS 报文发送 DDNS 更新请求时使用的参数传输方式。

undo method 命令用来恢复缺省情况。

【命令】

method { **http-get** | **http-post** }

undo method

【缺省情况】

采用 HTTP 或 HTTPS 报文发送 DDNS 更新请求时使用的参数的传输方式为 http-get。

【视图】

DDNS 策略视图

【缺省用户角色】

network-admin

【参数】

http-get：参数的传输方式为 http-get。

http-post：参数的传输方式为 http-post。

【使用指导】

采用 HTTP 或 HTTPS 报文发送 DDNS 更新请求时，不同的 DDNS 服务器要求使用的参数传输方式可能不同。例如 DHS 服务器，需要使用 http-post 参数传输方式。通过本配置可以修改参数传输方式，以满足 DDNS 服务器的要求。

本命令仅在基于 HTTP 或 HTTPS 与 DDNS 服务器通信时生效。基于其他协议与 DDNS 服务器通信时，本命令不生效。

通过本命令修改 DDNS 策略的参数传输方式时，如果该 DDNS 策略已经应用到接口上，则立即触发一次 DDNS 更新。

【举例】

配置 DDNS 策略 steven_policy 采用 HTTP 或 HTTPS 报文发送 DDNS 更新请求时使用的参数传输方式为 http-post 方式。

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
[Sysname-ddns-policy-steven_policy] method http-post
```

【相关命令】

- **display ddns policy**
- **ddns policy**

2.1.7 password

password 命令用来指定登录 DDNS 服务器的密码。

undo password 命令用来恢复缺省情况。

【命令】

password { **cipher** | **simple** } *string*

undo password

【缺省情况】

未指定登录 DDNS 服务器的密码。

【视图】

DDNS 策略视图

【缺省用户角色】

network-admin

【参数】

cipher：表示以密文方式设置密码。

simple：表示以明文方式设置密码，该密码将以密文形式存储。

string：密码字符串，区分大小写。明文密码为 1～32 个字符的字符串，密文密码为 1～73 个字符的字符串。

【举例】

为 DDNS 策略 steven_policy 指定登录 DDNS 服务器的密码为 nevets。

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
[Sysname-ddns-policy-steven_policy] password simple nevets
```

【相关命令】

- **display ddns policy**
- **ddns policy**
- **url**
- **username**

2.1.8 ssl-client-policy

ssl-client-policy 命令用来指定与 DDNS 策略关联的 SSL 客户端策略。

undo ssl-client-policy 命令用来恢复缺省情况。

【命令】

ssl-client-policy *policy-name*

undo ssl-client-policy

【缺省情况】

未指定与 DDNS 策略关联的 SSL 客户端策略。

【视图】

DDNS 策略视图

【缺省用户角色】

network-admin

【参数】

policy-name：SSL 客户端策略名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

SSL 客户端策略只对 URL 为 HTTPS 地址的 DDNS 更新请求有效。

多次执行本命令，为同一个 DDNS 策略关联不同的 SSL 客户端策略时，DDNS 策略将只与最后配置的 SSL 客户端策略关联。

【举例】

将 SSL 客户端策略 ssl_policy 与 DDNS 策略 steven_policy 关联。

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
[Sysname-ddns-policy-steven_policy] ssl-client-policy ssl_policy
```

【相关命令】

- **ddns policy**
- **display ddns policy**
- **ssl-client-policy**（安全命令参考/SSL）

2.1.9 url

url 命令用来指定 DDNS 更新请求的 URL 地址。

undo url 命令用来恢复缺省情况。

【命令】

url *request-url*

undo url

【缺省情况】

未指定 DDNS 更新请求的 URL 地址。

【视图】

DDNS 策略视图

【缺省用户角色】

network-admin

【参数】

request-url：DDNS 更新请求的 URL 地址，为 1～240 个字符的字符串，区分大小写。

【使用指导】

不同DDNS服务器的请求更新URL地址有所不同。常见的DDNS服务器URL地址格式如 表 2-2所示。

表2-2 常见的 DDNS 更新请求 URL 地址格式列表

DDNS 服务器	DDNS 更新请求的 URL 地址格式
www.3322.org	http://members.3322.org/dyndns/update?system=dyndns&hostname=<h>&myip=<a>
DYNDNS	http://members.dyndns.org/nic/update?system=dyndns&hostname=<h>&myip=<a>
DYNS	http://www.dyns.cx/postscript.php?host=<h>&ip=<a>
ZONEEDIT	http://dynamic.zoneedit.com/auth/dynamic.html?host=<h>&dnsto=<a>
TZO	http://cgi.tzo.com/webclient/signedon.html?TZOName=<h>IPAddress=<a>

DDNS 服务器	DDNS 更新请求的 URL 地址格式
EASYDNS	http://members.easydns.com/dyn/ez-ipupdate.php?action=edit&myip=<a>&host_id=<h>
HEIPV6TB	http://dyn.dns.he.net/nic/update?hostname=<h>&myip=<a>
CHANGE-IP	http://nic.changeip.com/nic/update?hostname=<h>&offline=1
NO-IP	http://dynupdate.no-ip.com/nic/update?hostname=<h>&myip=<a>
DHS	http://members.dhs.org/nic/hosts?domain=dyn.dhs.org&hostname=<h>&hostscmd=edit&hostscmdstage=2&type=1&ip=<a>
HP	https://*server-name*/nic/update?group=*group-name*&myip=<a>
ODS	ods://update.ods.org
GNUDIP	gnudip://*server-name*
花生壳	oray://phservice2.oray.net

URL 地址中不支持携带用户名和密码，配置用户名和密码请配合 **username** 和 **password** 命令使用，请根据实际情况修改。

HP 和 GNUDIP 是通用的 DDNS 更新协议，*server-name* 是使用对应 DDNS 更新协议的服务提供商的服务器域名或地址。

DDNS 更新请求的 URL 地址可以以“http://”开头，表示基于 HTTP 与 DDNS 服务器通信；以“https://”开头，表示基于 HTTPS 与 DDNS 服务器通信；以“ods://”开头，表示基于 TCP 与 ODS 服务器通信；以“gnudip://”开头，表示基于 TCP 与 GNUDIP 服务器通信；以“oray://”开头，表示基于 TCP 与花生壳 DDNS 服务器通信。

members.3322.org 和 phservice2.oray.net 是服务提供商提供 DDNS 服务的域名。花生壳提供 DDNS 服务的域名可能是 phservice2.oray.net、phddns60.oray.net、client.oray.net 和 ph031.oray.net 等，请根据实际情况修改域名。

URL 地址中的端口号是可选项，如果不包含端口号则使用缺省端口号：HTTP 是 80，HTTPS 是 443，花生壳 DDNS 服务器是 6060。

<h>由系统根据接口上应用 DDNS 策略时指定的 FQDN 自动填写，<a>由系统根据应用 DDNS 策略的接口的主 IP 地址自动填写，用户可以不更改 URL 中的<h>和<a>。用户也可以手工输入需要更新的 FQDN 和 IP 地址，代替 URL 中的<h>和<a>，此时，应用 DDNS 策略时指定的 FQDN 将不会生效。为了避免配置错误，建议用户不要修改 URL 中的<h>和<a>。

花生壳 DDNS 服务器的 URL 地址中不能指定用于更新的 FQDN 和 IP 地址。用户可在接口上应用 DDNS 策略时指定 FQDN；用于更新的 IP 地址是应用 DDNS 策略的接口的主 IP 地址。

为避免歧义，请尽量不要在 DDNS 服务器上申请含有“:”、“@”或“?”字符的用户名和密码。

多次执行本命令，最后一次执行的命令生效。

【举例】

为 DDNS 策略 steven_policy 指定 DDNS 更新请求的 URL 地址。DDNS 服务提供商为 www.3322.org。

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
```

```
[Sysname-ddns-policy-steven_policy] url
http://members.3322.org/dyndns/update?system=dyndns&hostname=<h>&myip=<a>
```

【相关命令】

- **display ddns policy**
- **ddns policy**
- **password**
- **username**

2.1.10 username

username 命令用来指定登录 DDNS 服务器的用户名。

undo username 命令用来恢复缺省情况。

【命令】

username *username*

undo username

【缺省情况】

未指定登录 DDNS 服务器的用户名。

【视图】

DDNS 策略视图

【缺省用户角色】

network-admin

【参数】

username：登录 DDNS 服务器的用户名，为 1～32 个字符的字符串，区分大小写。

【举例】

为 DDNS 策略 steven_policy 指定登录 DDNS 服务器的用户名为 steven。

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
[Sysname-ddns-policy-steven_policy] username steven
```

【相关命令】

- **display ddns policy**
- **ddns policy**
- **password**
- **url**