目 录

1 域名解析

1.1 域名解析简介

DNS（Domain Name System，域名系统）是一种用于 TCP/IP 应用程序的分布式数据库，提供域名与 IP 地址之间的转换。通过域名系统，用户进行某些应用时，可以直接使用便于记忆的、有意义的域名，而由网络中的域名解析服务器将域名解析为正确的 IP 地址。

域名解析分为静态域名解析和动态域名解析，二者可以配合使用。在解析域名时，首先采用静态域名解析（查找静态域名解析表），如果静态域名解析不成功，再采用动态域名解析。由于动态域名解析需要域名服务器（DNS server）的配合，会花费一定的时间，因而可以将一些常用的域名放入静态域名解析表中，这样可以大大提高域名解析效率。

1.1.1 静态域名解析

静态域名解析就是手工建立域名和 IP 地址之间的对应关系。当用户使用域名进行某些应用（如 telnet 应用）时，系统查找静态域名解析表，从中获取指定域名对应的 IP 地址。

1.1.2 动态域名解析

1. 解析过程

动态域名解析通过向域名服务器查询域名和 IP 地址之间的对应关系来实现将域名解析为 IP 地址。动态域名解析过程如下：

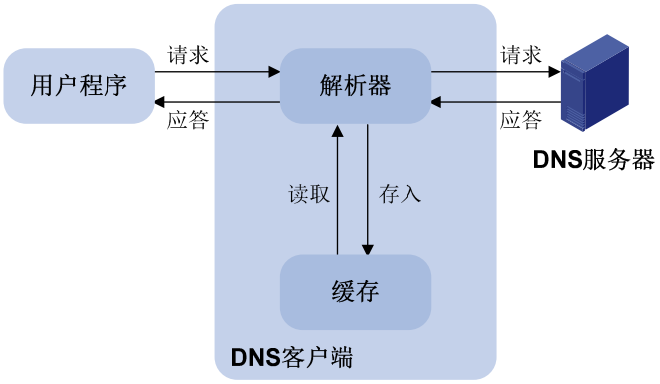
(1) 当用户使用域名进行某些应用时，用户程序首先向 DNS 客户端中的解析器发出请求。

(2) DNS 客户端收到请求后，首先查询本地的域名缓存。如果存在已解析成功的映射项，就将域名对应的 IP 地址返回给用户程序；如果未发现所要查找的映射项，就向域名服务器发送查询请求。

(3) 域名服务器首先从自己的数据库中查找域名对应的 IP 地址。如果判断该域名不属于本域范围，就将请求交给其他域名服务器处理，直到完成解析，并将解析的结果返回给 DNS 客户端。

(4) DNS 客户端收到域名服务器的响应报文后，将解析结果返回用户程序。

图1-1 动态域名解析



用户程序、DNS客户端及域名服务器的关系如 图 1-1 所示，其中解析器和缓存构成DNS客户端。用户程序、DNS客户端在同一台设备上，而DNS客户端和域名服务器一般分布在两台设备上。

动态域名解析支持缓存功能。每次动态解析成功的域名与 IP 地址的映射均存放在 DNS 客户端的动态域名缓存区中，当下一次查询相同域名的时候，就可以直接从缓存区中读取，不用再向域名服务器进行请求。缓存区中的映射在一段时间后会老化而被删除，以保证及时从域名服务器得到最新的内容。老化时间由域名服务器设置，DNS 客户端从域名服务器的应答报文中获得老化时间。

2. 域名后缀列表功能

动态域名解析支持域名后缀列表功能。用户可以预先设置一些域名后缀，在域名解析的时候，用户只需要输入域名的部分字段，系统会自动将输入的域名加上不同的后缀进行解析。例如，用户想查询域名 aabbcc.com，那么可以先在后缀列表中配置 com，然后输入 aabbcc 进行查询，系统会自动将输入的域名与后缀连接成 aabbcc.com 进行查询。

使用域名后缀的时候，根据用户输入域名方式的不同，查询方式分成以下几种情况：

- 如果用户输入的域名中没有“.”，比如 aabbcc，系统认为这是一个主机名，会首先加上域名后缀进行查询，如果所有加后缀的域名查询都失败，将使用最初输入的域名（如 aabbcc）进行查询。
- 如果用户输入的域名中间有“.”，比如 www.aabbcc，系统直接用它进行查询，如果查询失败，再依次加上各个域名后缀进行查询。
- 如果用户输入的域名最后有“.”，比如 aabbcc.com.，表示不需要进行域名后缀添加，系统直接用输入的域名进行查询，不论成功与否都直接返回结果。就是说，如果用户输入的字符中最后一个字符为“.”，就只根据用户输入的字符进行查找，而不会去匹配用户预先设置的域名后缀，因此最后这个“.”，也被称为查找终止符。带有查询终止符的域名，称为 FQDN（Fully Qualified Domain Name，完全合格域名）。

目前，设备支持静态域名解析和动态域名解析的 DNS 客户端功能。

说明

如果域名服务器上配置了域名的别名，设备也可以通过别名来解析主机的 IP 地址。

1.1.3 DNS代理

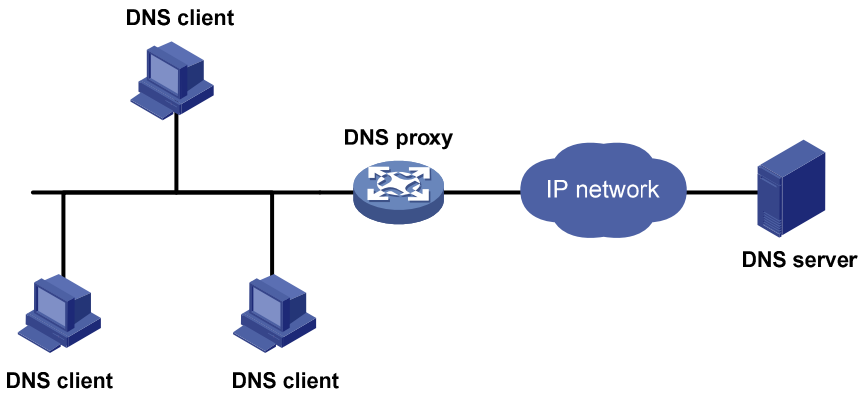
1. DNS代理简介

DNS 代理（DNS proxy）用来在 DNS client 和 DNS server 之间转发 DNS 请求和应答报文。局域网内的 DNS client 把 DNS proxy 当作 DNS server，将 DNS 请求报文发送给 DNS proxy。DNS proxy 将该请求报文转发到真正的 DNS server，并将 DNS server 的应答报文返回给 DNS client，从而实现域名解析。

使用 DNS proxy 功能后，当 DNS server 的地址发生变化时，只需改变 DNS proxy 上的配置，无需改变局域网内每个 DNS client 的配置，从而简化了网络管理。

DNS proxy的典型应用环境如 图 1-2 所示。

图1-2 DNS 代理典型组网应用



2. DNS代理的工作机制

DNS 代理的工作过程如下：

(1) DNS client 把 DNS proxy 当作 DNS server，将 DNS 请求报文发送给 DNS proxy，即请求报文的目的地址为 DNS proxy 的 IP 地址。

(2) DNS proxy 收到请求报文后，首先查找本地的静态域名解析表和动态域名解析缓存表，如果存在请求的信息，则 DNS proxy 直接通过 DNS 应答报文将域名解析结果返回给 DNS client。

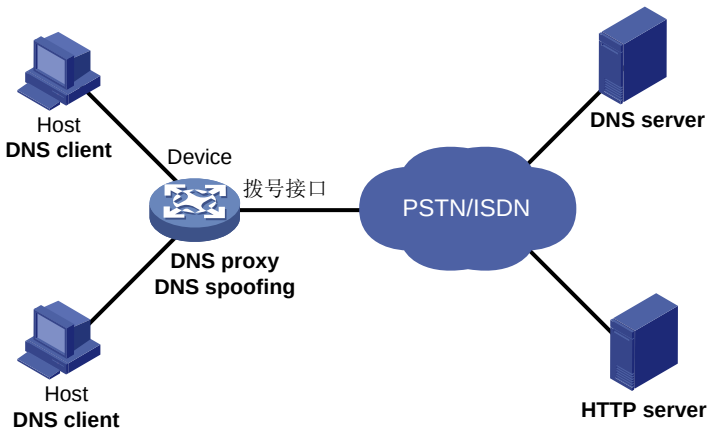
(3) 如果不存在请求的信息，则 DNS proxy 将报文转发给 DNS server，通过 DNS server 进行域名解析。

(4) DNS proxy 收到 DNS server 的应答报文后，记录域名解析的结果，并将报文转发给 DNS client。DNS client 利用域名解析的结果进行相应的处理。

只有 DNS proxy 上存在域名服务器地址，并存在到达域名服务器的路由，DNS proxy 才会向 DNS server 发送域名解析请求。

1.1.4 DNS spoofing

图1-3 DNS spoofing 典型应用场景



DNS spoofing（DNS欺骗）主要应用于 图 1-3 所示的拨号网络。在该网络中：

- Device 通过拨号接口连接到 PSTN/ISDN 等拨号网络。只有存在通过拨号接口转发的报文时，才会触发拨号接口建立连接。
- Device 作为 DNS proxy。在 Host 上将 Device 指定为 DNS 服务器；拨号接口建立连接后，Device 通过 DHCP 等方式动态获取 DNS 服务器地址。

Device 上未开启 DNS spoofing 功能时，Device 接收到 Host 发送的域名解析请求报文后，如果不存在对应的域名解析表项，则需要向 DNS server 发送域名解析请求。但是，由于此时拨号接口尚未建立连接，Device 上不存在 DNS server 地址，Device 不会向 DNS server 发送域名解析请求，也不会应答 DNS client 的请求。从而导致域名解析失败，且没有流量触发拨号接口建立连接。

DNS spoofing 功能可以解决上述问题。使能 DNS spoofing 功能后，即便 Device 上不存在 DNS server 地址或到达 DNS server 的路由，Device 也会利用指定的 IP 地址作为域名解析结果，应答 DNS client 的域名解析请求。DNS client 后续发送的报文可以用来触发拨号接口建立连接。

图 1-3 所示网络中，Host访问HTTP server的报文处理流程为：

(1) Host 通过域名访问 HTTP server 时，首先向 Device 发送域名解析请求，将 HTTP server 的域名解析为 IP 地址。

(2) Device 接收到域名解析请求后，如果拨号接口尚未建立连接，Device 上不存在 DNS server 地址，或者设备上配置的 DNS server 地址均不可达，则 Device 利用 DNS spoofing 中指定的 IP 地址作为域名解析结果，应答 DNS client 的域名解析请求。该域名解析应答的老化时间为 0。并且，应答的 IP 地址满足如下条件：Device 上存在到达该 IP 地址的路由，且路由的出接口为拨号接口。

(3) Host 接收到 Device 的应答报文后，向应答的 IP 地址发送 HTTP 请求。

(4) Device 通过拨号接口转发 HTTP 请求时，触发拨号接口建立连接，并通过 DHCP 等方式动态获取 DNS server 的地址。

(5) 域名解析应答老化后，Host 再次发送域名解析请求。

(6) 之后，Device的处理过程与DNS proxy工作过程相同，请参见“1.1.3 2. DNS代理的工作机制”。

(7) Host 获取到正确的 HTTP server 地址后，可以正常访问 HTTP server。

说明

由于 DNS spoofing 功能指定的 IP 地址并不是待解析域名对应的 IP 地址，为了防止 DNS client 上保存错误的域名解析表项，该 IP 地址对应域名解析应答的老化时间为 0。

1.2 域名解析配置任务简介

表1-1 域名解析配置任务简介

配置任务	说明	详细配置
配置IPv4 DNS client	二者必选其一	1.3
配置IPv6 DNS client		1.4
配置DNS proxy	可选	1.5
配置DNS spoofing	可选	1.6
配置监视指定出接口的网络制式	可选	1.7
配置DNS报文的源端口	可选	1.8
配置DNS信任接口	可选	1.9
配置DNS/IPv6 DNS报文的DSCP优先级	可选	1.10

1.3 配置IPv4 DNS client

1.3.1 配置静态域名解析

配置静态域名解析就是通过配置使主机名与 IPv4 地址相互对应。当使用 Telnet 等应用时，可以直接使用主机名，由系统解析为 IPv4 地址。

在配置静态域名解析时，需要注意：

- 在公网或单个 VPN 实例内，一个主机名只能对应一个 IPv4 地址。重复配置时，新的配置会覆盖原有配置。
- 公网或单个 VPN 实例内最多可以配置 1024 个主机名和 IPv4 地址的对应关系。可以同时在公网和 VPN 实例内配置主机名和 IPv4 地址的对应关系。

表1-2 配置静态域名解析

操作	命令	说明
进入系统视图	**system-view**	-
配置主机名和对应的IPv4地址	**ip host** *host-name ip-address* [**vpn-instance** *vpn-instance-name*]	缺省情况下，不存在主机名及IPv4地址的对应关系

1.3.2 配置动态域名解析

1. 功能简介

如果用户要使用动态域名解析功能，则需要配置域名服务器的地址，这样才能将请求报文发送到正确的服务器进行解析。

用户还可以配置域名后缀，以便实现只输入域名的部分字段，而由系统自动加上预先设置的后缀进行解析。

2. 配置限制和指导

- 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。
- 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 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。
- 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。
- 查询主机名对应的IPv4地址时，优先向域名服务器的IPv4地址发送查询请求。如果查询失败，则再向域名服务器的 IPv6 地址发送查询请求。
- 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，失败后再根据优先级从高到低的次序向其他域名服务器发送查询请求。公网或单个 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。
- 添加域名后缀的优先级顺序为：先配置的域名后缀优先级高于后配置的域名后缀；设备上手工配置的域名后缀优先级高于通过 DHCP 等方式动态获取的域名后缀。设备首先添加优先级最高的域名后缀，查询失败后再根据优先级从高到低的次序添加其他域名后缀。

3. 配置步骤

表1-3 配置动态域名解析

操作		命令	说明
进入系统视图		**system-view**	-
（可选）配置域名后缀		**dns domain** *domain-name* [**vpn-instance** *vpn-instance-name*]	缺省情况下，未配置域名后缀，即只根据用户输入的域名信息进行解析
系统视图下配置域名服务器的IPv4地址		**dns server** *ip-address* [**vpn-instance** *vpn-instance-name*]	三者至少选其一 缺省情况下，未配置域名服务器的地址
接口视图下配置域名服务器的IPv4地址	进入接口视图	**Interface** *interface-type interface-number*	
	配置域名服务器的IPv4地址	**dns server** *ip-address* [**vpn-instance** *vpn-instance-name*]	
配置域名服务器的IPv6地址		**ipv6 dns server** *ipv6-address* [*interface-type interface-number*] [**vpn-instance** *vpn-instance-name*]	

1.4 配置IPv6 DNS client

1.4.1 配置静态域名解析

配置静态域名解析就是通过配置使主机名与 IPv6 地址相互对应。当使用 Telnet 等应用时，可以直接使用主机名，由系统解析为 IPv6 地址。

在配置静态域名解析时，需要注意：

- 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。重复配置时，新的配置会覆盖原有配置。
- 公网或单个 VPN 内最多可配置 1024 个主机名与 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。

表1-4 配置静态域名解析

操作	命令	说明
进入系统视图	**system-view**	-
配置主机名和对应的IPv6地址	**ipv6 host** *host-name ipv6-address* [**vpn-instance** *vpn-instance-name*]	缺省情况下，不存在主机名及IPv6地址的对应关系

1.4.2 配置动态域名解析

1. 功能简介

如果用户要使用动态域名解析功能，则需要配置域名服务器的地址，这样才能将查询请求报文发送到正确的服务器进行解析。

用户还可以配置域名后缀，以便实现只输入域名的部分字段，而由系统自动加上预先设置的后缀进行解析。

2. 配置限制和指导

- 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 IPv4 地址。可同时在公网和 VPN 实例内配置域名服务器 IPv4 地址。
- 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 IPv6 地址。可同时在公网和 VPN 实例内配置域名服务器 IPv6 地址。
- 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。
- 查询主机名对应的IPv6地址时，优先向域名服务器的IPv6地址发送查询请求。如果查询失败，则再向域名服务器的 IPv4 地址发送查询请求。
- 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。

- 公网或单个 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
- 添加域名后缀的优先级顺序为：先配置的域名后缀优先级高于后配置的域名后缀；设备上手工配置的域名后缀优先级高于通过 DHCP 等方式动态获取的域名后缀。设备首先添加优先级最高的域名后缀，查询失败后再依次添加其他域名后缀。

3. 配置步骤

表1-5 配置动态域名解析

操作		命令	说明
进入系统视图		**system-view**	-
（可选）配置域名后缀		**dns domain** *domain-name* [**vpn-instance** *vpn-instance-name*]	缺省情况下，未配置域名后缀，即只根据用户输入的域名信息进行解析
系统视图下配置域名服务器的IPv4地址		**dns server** *ip-address* [**vpn-instance** *vpn-instance-name*]	三者至少选其一 缺省情况下，未配置域名服务器的地址
接口视图下配置域名服务器的IPv4地址	进入接口视图	**Interface** *interface-type interface-number*	
	配置域名服务器的IPv4地址	**dns server** *ip-address* [**vpn-instance** *vpn-instance-name*]	
配置域名服务器的IPv6地址		**ipv6 dns server** *ipv6-address* [*interface-type interface-number*] [**vpn-instance** *vpn-instance-name*]	

1.5 配置DNS proxy

可以指定多个 DNS server。DNS proxy 接收到客户端的查询请求后，首先向优先级最高的 DNS server 转发查询请求，失败后再依次向其他 DNS server 转发查询请求。

无论 DNS proxy 接收到的查询请求是来自 IPv4 客户端还是来自 IPv6 客户端，DNS proxy 都会按照优先级顺序向域名服务器的 IPv4 地址和 IPv6 地址转发查询请求。如果查询请求是 IPv4 报文，则优先向域名服务器的 IPv4 地址转发查询请求。如果查询请求是 IPv6 报文，则优先向域名服务器的 IPv6 地址转发查询请求。

表1-6 配置 DNS proxy

操作		命令	说明
进入系统视图		**system-view**	-
开启DNS proxy功能		**dns proxy enable**	缺省情况下，DNS proxy功能处于开启状态
系统视图下配置域名服务器的IPv4地址		**dns server** *ip-address* [**vpn-instance** *vpn-instance-name*]	三者至少选其一 缺省情况下，未配置域名服务器的地址
接口视图下配置域名服务器的IPv4地址	进入接口视图	**Interface** *interface-type interface-number*	
	配置域名服务器的IPv4地址	**dns server** *ip-address* [**vpn-instance** *vpn-instance-name*]	

操作	命令	说明
配置域名服务器的IPv6地址	**ipv6 dns server** *ipv6-address* [*interface-type interface-number*] [**vpn-instance** *vpn-instance-name*]	

1.6 配置DNS spoofing

1. 配置准备

只有在以下条件均满足的情况下，DNS spoofing 功能才会生效：

- 设备上启用了 DNS proxy 功能
- 设备上未指定域名服务器地址或不存在到达域名服务器的路由

因此，配置 DNS spoofing 前，需要先启用 DNS proxy 功能。

配置 DNS spoofing 功能时，需要注意：

- 公网或单个 VPN 实例内只能配置 1 个 DNS spoofing 应答的 IPv4 地址和 1 个 DNS spoofing 应答的 IPv6 地址。重复配置时，新的配置会覆盖原有配置。
- 可同时在公网和 VPN 实例内配置 DNS spoofing 功能。
- DNS spoofing 功能生效时，即使设备上配置了静态域名解析，也会使用 DNS spoofing 指定的 IP 地址来应答 DNS 请求。

2. 配置步骤

表1-7 配置 DNS spoofing

操作		命令	说明
进入系统视图		**system-view**	-
启用DNS proxy功能		**dns proxy enable**	缺省情况下，DNS proxy功能处于开启状态
开启DNS Snooping功能，并指定DNS spoofing应答地址	指定DNS spoofing应答的IPv4地址	**dns spoofing** *ip-address* [**vpn-instance** *vpn-instance-name*]	二者至少选其一 缺省情况下，未开启DNS Snooping功能
	指定DNS spoofing应答的IPv6地址	**ipv6 dns spoofing** *ipv6-address* [**vpn-instance** *vpn-instance-name*]	

1.7 配置监视指定出接口的网络制式

对于某些特殊组网，如果设备已经具有到达 DNS 服务器的路由，用户可以通过本配置来监视该路由对应的 Cellular 类型出接口的网络制式：

- 如果 Cellular 口的网络制式为 2G，由于出口带宽较小，因此设备不希望用户通过该接口访问 DNS 服务器，这时利用配置的应答 IPv4/IPv6 地址作为域名解析结果，对用户进行 DNS spoofing 欺骗代答；

- 如果 Cellular 口的网络制式为 3G/4G，由于出口带宽较大，因此设备不需要进行 DNS spoofing 欺骗代答，用户可以访问到 DNS 服务器。

表1-8 配置监视指定出接口的网路制式

操作		命令	说明
进入系统视图		**system-view**	-
启用DNS proxy功能		**dns proxy enable**	缺省情况下，DNS proxy功能处于开启状态
开启DNS Snooping功能，并指定DNS spoofing应答地址	指定DNS spoofing应答的IPv4地址	**dns spoofing** *ip-address* [**vpn-instance** *vpn-instance-name*]	二者至少选其一 缺省情况下，未开启DNS Snooping功能 该地址建议配置为本设备的私网地址
	指定DNS spoofing应答的IPv6地址	**ipv6 dns spoofing** *ipv6-address* [**vpn-instance** *vpn-instance-name*]	

1.8 配置DNS报文的源接口

提示

无论配置的源接口是否属于指定的 VPN，该配置都会生效。不建议为 VPN 配置不属于该 VPN 的接口作为源接口。否则，设备会使用不属于该 VPN 的地址作为 DNS 报文源地址，导致无法收到 DNS 应答。

缺省情况下，设备根据域名服务器的地址，通过路由表查找请求报文的出接口，并将该出接口的主 IP 地址作为发送到该服务器的 DNS 请求报文的源地址。根据域名服务器的地址不同，发送报文的源地址可能会发生变化。在某些特殊的组网环境中，域名服务器只应答来自特定源地址的 DNS 请求报文。这种情况下，必须指定 DNS 报文的源接口。如果为设备配置了 DNS 报文的源接口，则设备在发送 DNS 报文时，将固定使用该接口的主 IP 地址作为报文的源地址。

发送 IPv4 DNS 报文时，将使用源接口的主 IPv4 地址作为 DNS 报文的源地址。发送 IPv6 DNS 报文时，将根据 RFC 3484 中定义的规则从源接口上选择 IPv6 地址作为 DNS 报文的源地址。如果源接口上未配置对应的地址，则将导致报文发送失败。

公网或单个 VPN 实例内只能配置 1 个源接口。重复配置时，新的配置会覆盖原有配置。可同时在公网和 VPN 实例内配置源接口。

表1-9 配置 DNS 报文的源接口

操作	命令	说明
进入系统视图	**system-view**	-
指定DNS报文的源接口	**dns source-interface** *interface-type interface-number* [**vpn-instance** *vpn-instance-name*]	缺省情况下，未指定DNS报文的源接口

1.9 配置DNS信任接口

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。

表1-10 配置 DNS 信任接口

操作	命令	说明
进入系统视图	**system-view**	-
指定DNS信任接口	**dns trust-interface** *interface-type interface-number*	缺省情况下，未指定任何接口为信任接口

说明

设备最多可以配置 128 个 DNS 信任接口。

1.10 配置DNS报文的DSCP优先级

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。通过本配置可以指定设备发送的 DNS 报文的 DSCP 优先级。

本命令的配置同时用于 DNS 客户端和 DNS proxy。

表1-11 配置 DNS 报文的 DSCP 优先级

操作	命令	说明
进入系统视图	**system-view**	-
配置DNS报文的DSCP优先级	**dns dscp** *dscp-value*	缺省情况下，DNS报文的DSCP优先级为0，IPv6 DNS报文的DSCP优先级为0
配置IPv6 DNS报文的DSCP优先级	**ipv6 dns dscp** *dscp-value*	

1.11 域名解析显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示域名解析配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可以清除动态域名缓存信息。

表1-12 域名解析显示和维护

操作	命令
显示域名解析表信息	**display dns host** [**ip** | **ipv6**] [**vpn-instance** *vpn-instance-name*]
显示域名服务器的IPv4地址信息	**display dns server** [**dynamic**] [**vpn-instance** *vpn-instance-name*]
显示域名服务器的IPv6地址信息	**display ipv6 dns server** [**dynamic**] [**vpn-instance** *vpn-instance-name*]
显示域名后缀信息	**display dns domain** [**dynamic**] [**vpn-instance** *vpn-instance-name*]
清除动态域名解析缓存信息	**reset dns host** [**ip** | **ipv6**] [**vpn-instance** *vpn-instance-name*]

1.12 IPv4域名解析典型配置举例

1.12.1 静态域名解析配置举例

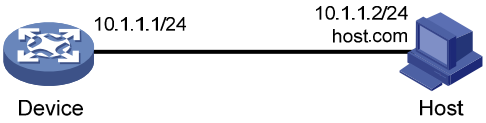
1. 组网需求

为了避免记忆复杂的 IP 地址，Device 希望通过便于记忆的主机名访问某一主机。在 Device 上手工配置 IP 地址对应的主机名，利用静态域名解析功能，就可以实现通过主机名访问该主机。

在本例中，Device 访问的主机 IP 地址为 10.1.1.2，主机名为 host.com。

2. 组网图

图1-4 静态域名解析配置组网图



3. 配置步骤

配置主机名 host.com 对应的 IP 地址为 10.1.1.2。

```
<Sysname> system-view
[Sysname] ip host host.com 10.1.1.2
```

执行 **ping host.com** 命令，Device 通过静态域名解析可以解析到 host.com 对应的 IP 地址为 10.1.1.2。

```
[Sysname] ping host.com
Ping host.com (10.1.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 10.1.1.2: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=4 ttl=255 time=2.000 ms
```

```
--- Ping statistics for host.com ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.200/2.000/0.400 ms
```

1.12.2 动态域名解析配置举例

1. 组网需求

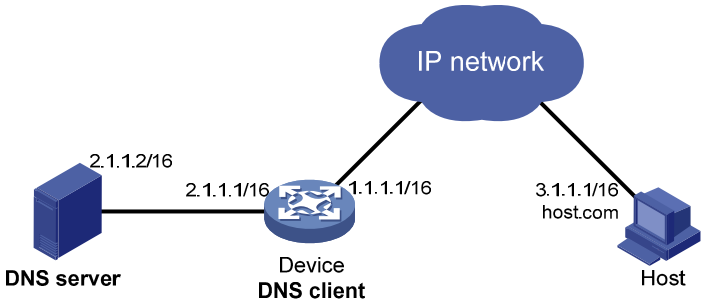
为了避免记忆复杂的 IP 地址，Device 希望通过便于记忆的域名访问某一主机。如果网络中存在域名服务器，则可以利用动态域名解析功能，实现通过域名访问主机。

在本例中：

- 域名服务器的 IP 地址是 2.1.1.2/16，域名服务器上存在 com 域，且 com 域中包含域名“host”和 IP 地址 3.1.1.1/16 的对应关系。
- Device 作为 DNS 客户端，使用动态域名解析功能，将域名解析为 IP 地址。
- Device 上配置域名后缀 com，以便简化访问主机时输入的域名，例如通过输入 host 即可访问域名为 host.com、IP 地址为 3.1.1.1/16 的主机 Host。

2. 组网图

图1-5 动态域名解析组网图



3. 配置步骤

说明

- 在开始下面的配置之前，假设设备与主机之间的路由可达，设备和主机都已经配置完毕，接口IP地址如 图 1-5 所示。
- 不同域名服务器的配置方法不同，下面仅以 Windows Server 2008 R2 为例，说明域名服务器的配置方法。

(1) 配置域名服务器

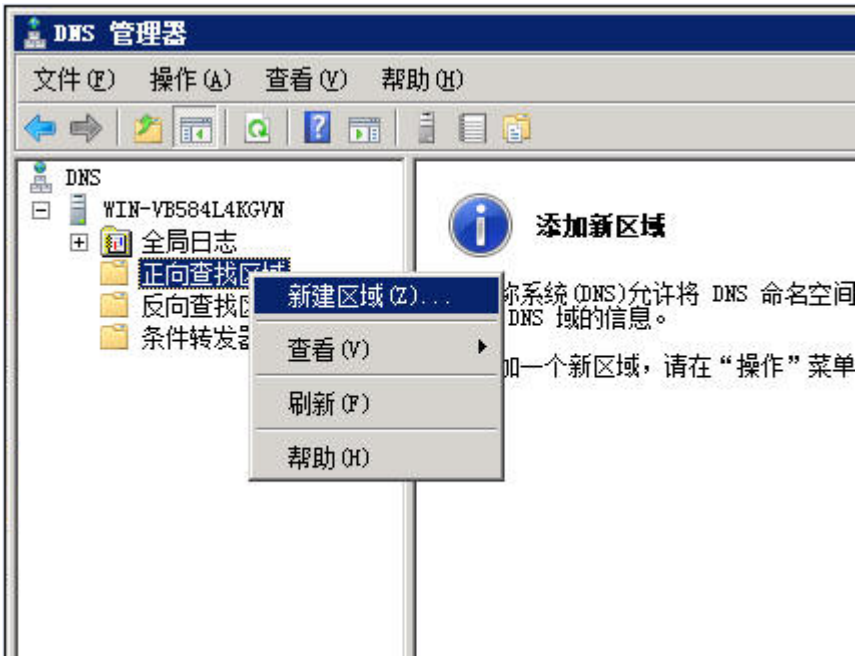
进入域名服务器配置界面。

在开始菜单中，选择[程序/管理工具/DNS]。

创建区域 com。

如 图 1-6 所示，右键点击[正向查找区域]，选择[新建区域]，按照提示创建新的区域com。

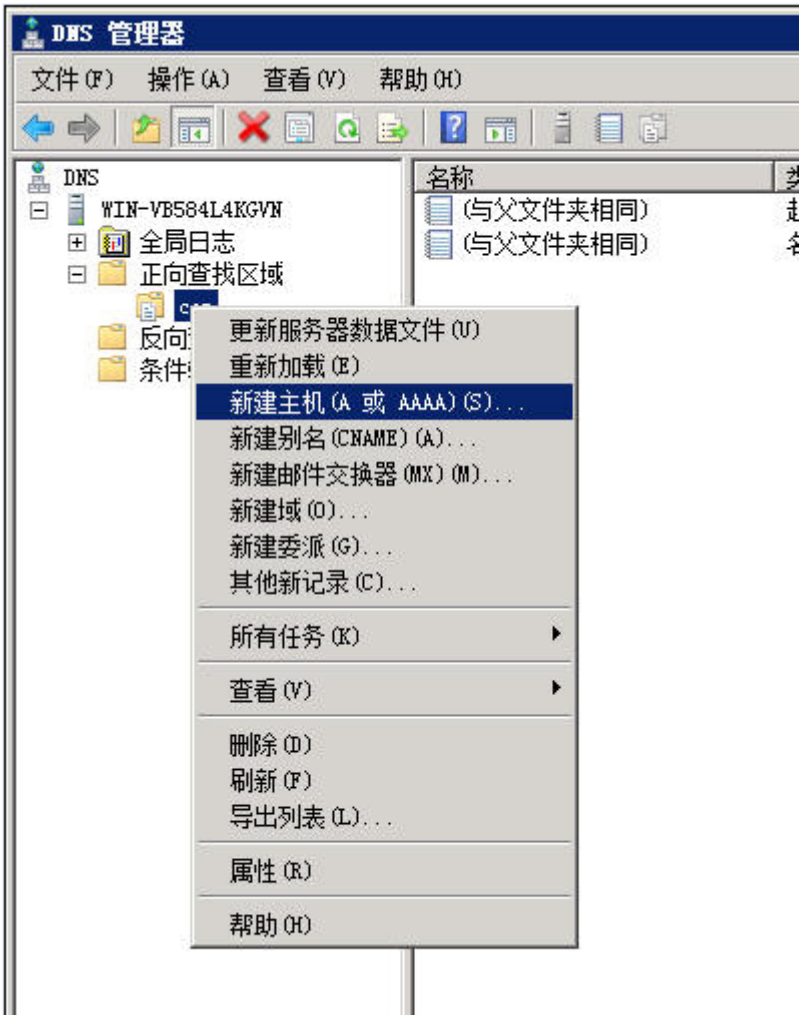
图1-6 创建区域



添加域名和 IP 地址的映射。

如 图 1-7 所示，右键点击区域[com]。

图1-7 新建主机



选择[新建主机]，弹出如 图 1-8 的对话框。按照 图 1-8 输入域名host和IP地址 3.1.1.1。单击<添加主机>可完成操作。

图1-8 添加域名和 IP 地址的映射

(2) 配置 DNS 客户端 Device

```
<Sysname> system-view
```

配置域名服务器的 IP 地址为 2.1.1.2。

```
[Sysname] dns server 2.1.1.2
```

配置域名后缀 com。

```
[Sysname] dns domain com
```

4. 验证配置

在设备上执行 **ping host** 命令，可以 ping 通主机，且对应的目的地址为 3.1.1.1。

```
[Sysname] ping host
Ping host.com (3.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 3.1.1.1: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=4 ttl=255 time=2.000 ms

--- Ping statistics for host ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.200/2.000/0.400 ms
```

1.12.3 DNS proxy典型配置举例

1. 组网需求

某局域网内拥有多台设备，每台设备上都指定了域名服务器的 IP 地址，以便直接通过域名访问外部网络。当域名服务器的 IP 地址发生变化时，网络管理员需要更改局域网内所有设备上配置的域名服务器 IP 地址，工作量将会非常巨大。

通过 DNS proxy 功能，可以大大减少网络管理员的工作量。当域名服务器 IP 地址改变时，只需更改 DNS proxy 上的配置，即可实现局域网内设备通过新的域名服务器解析域名。

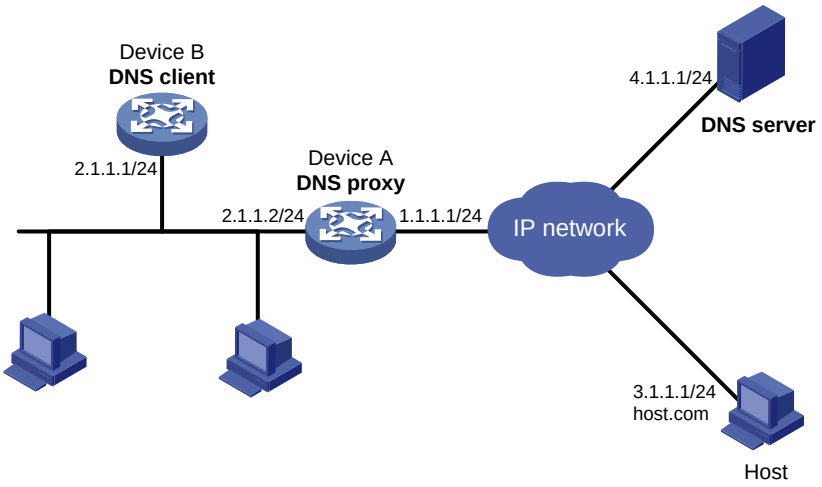
在本例中，具体配置步骤为：

(1) 局域网中的某台设备 Device A 配置为 DNS proxy，DNS proxy 上指定域名服务器 IP 地址为真正的域名服务器的地址 4.1.1.1。

(2) 局域网中的其他设备（如 Device B）上，域名服务器的 IP 地址配置为 DNS proxy 的地址，域名解析报文将通过 DNS proxy 转发给真正的域名服务器。

2. 组网图

图1-9 DNS proxy 组网图



3. 配置步骤

说明

在开始下面的配置之前，假设设备与域名服务器、主机之间的路由可达，并已按照 图 1-9 配置各接口的IP地址。

(1) 配置域名服务器

不同的域名服务器的配置方法不同。Windows Server 2008 R2 作为域名服务器时，配置方法请参见“1.12.2 动态域名解析配置举例”。

(2) 配置 DNS 代理 Device A

配置域名服务器的 IP 地址为 4.1.1.1。

```
<DeviceA> system-view
```

```
[DeviceA] dns server 4.1.1.1
```

开启 DNS proxy 功能。

```
[DeviceA] dns proxy enable
```

(3)　配置 DNS 客户端 Device B

```
<DeviceB> system-view
```

配置域名服务器的 IP 地址为 2.1.1.2。

```
[DeviceB] dns server 2.1.1.2
```

4. 验证配置

在 Device B 上执行 **ping host.com** 命令，可以 ping 通主机，且对应的目的地址为 3.1.1.1。

```
[DeviceB] ping host.com
Ping host.com (3.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 3.1.1.1: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=4 ttl=255 time=2.000 ms

--- Ping statistics for host.com ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.200/2.000/0.400 ms
```

1.13 IPv6域名解析典型配置举例

1.13.1 静态域名解析配置举例

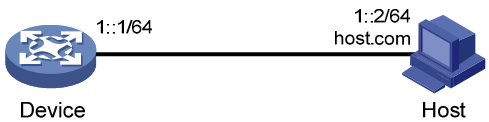
1. 组网需求

为了避免记忆复杂的 IPv6 地址，Device 希望通过便于记忆的主机名访问某一主机。在 Device 上手工配置 IPv6 地址对应的主机名，利用静态域名解析功能，就可以实现通过主机名访问该主机。

在本例中，Device 访问的主机 IPv6 地址为 1::2，主机名为 host.com。

2. 组网图

图1-10 静态域名解析配置组网图



3. 配置步骤

配置主机名 host.com 对应的 IPv6 地址为 1::2。

```
<Sysname> system-view
[Sysname] ipv6 host host.com 1::2
```

执行 **ping ipv6 host.com** 命令，Device 通过静态域名解析可以解析到 host.com 对应的 IPv6 地址为 1::2。

```
[Sysname] ping ipv6 host.com
```

```
Ping6(56 data bytes) 1::1 --> 1::2, press CTRL_C to break
56 bytes from 1::2, icmp_seq=0 hlim=128 time=1.000 ms
56 bytes from 1::2, icmp_seq=1 hlim=128 time=0.000 ms
56 bytes from 1::2, icmp_seq=2 hlim=128 time=1.000 ms
56 bytes from 1::2, icmp_seq=3 hlim=128 time=1.000 ms
56 bytes from 1::2, icmp_seq=4 hlim=128 time=0.000 ms

--- Ping6 statistics for host.com ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.600/1.000/0.490 ms
```

1.13.2 动态域名解析配置举例

1. 组网需求

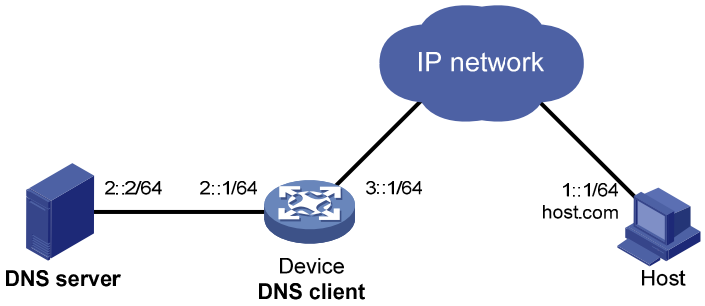
为了避免记忆复杂的 IPv6 地址，Device 希望通过便于记忆的域名访问某一主机。如果网络中存在域名服务器，则可以利用动态域名解析功能，实现通过域名访问主机。

在本例中：

- 域名服务器的 IPv6 地址是 2::2/64，域名服务器上存在 com 域，且 com 域中包含域名“host”和 IPv6 地址 1::1/64 的对应关系。
- Device 作为 DNS 客户端，使用动态域名解析功能，将域名解析为 IPv6 地址。
- Device 上配置域名后缀 com，以便简化访问主机时输入的域名，例如通过输入 host 即可访问域名为 host.com、IPv6 地址为 1::1/64 的主机 Host。

2. 组网图

图1-11 动态域名解析组网图



3. 配置步骤

说明

- 在开始下面的配置之前，假设设备与主机之间的路由可达，设备和主机都已经配置完毕，接口 IPv6 地址如 图 1-11 所示。
- 不同域名服务器的配置方法不同，下面仅以 Windows Server 2008 R2 为例，说明域名服务器的配置方法。配置之前，需确保 DNS 服务器支持 IPv6 DNS 功能，以便处理 IPv6 域名解析报文；且 DNS 服务器的接口可以转发 IPv6 报文。

(1)　配置域名服务器

进入域名服务器配置界面。

在开始菜单中，选择[程序/管理工具/DNS]。

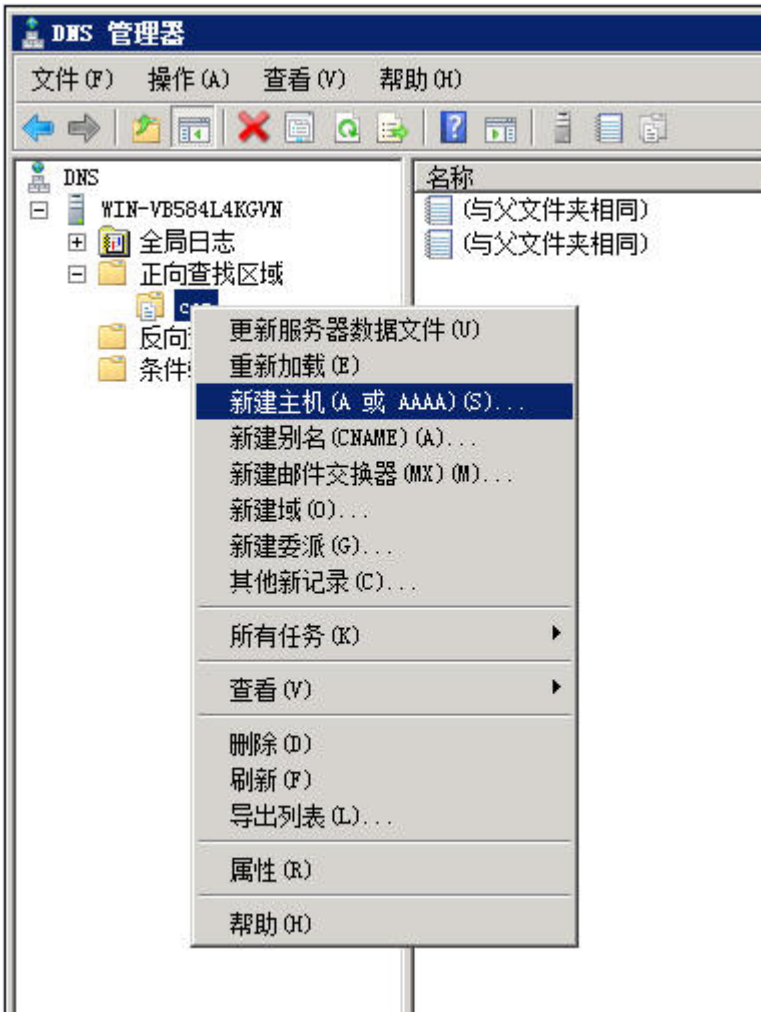
创建区域 com。

如 图 1-12 所示，右键点击[正向查找区域]，选择[新建区域]，按照提示创建新的区域com。

图1-12 创建区域

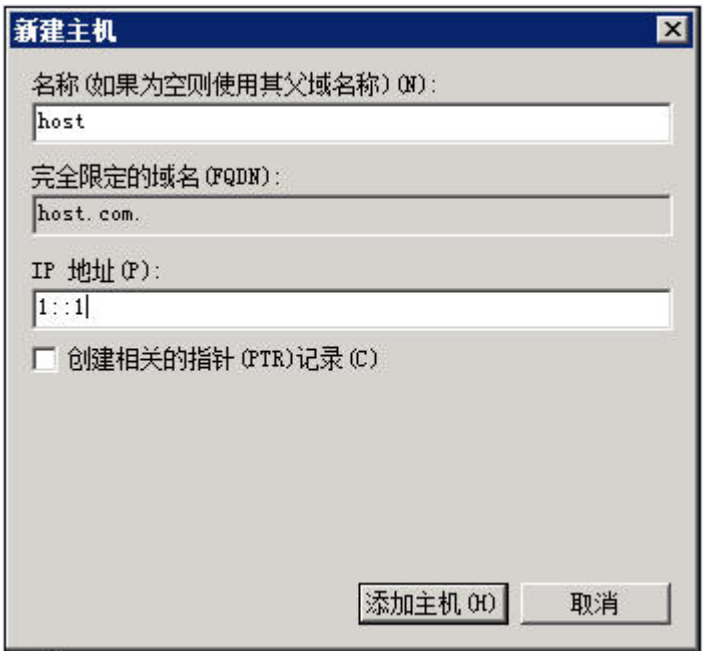
如 图 1-13 所示，右键点击区域[com]。

图1-13 新建主机



选择[新建主机]，弹出如 图 1-14 的对话框，输入域名和IPv6 地址 1::1。单击<添加主机>可完成操作。

图1-14 添加域名和 IPv6 地址的映射



(2) 配置 DNS 客户端 Device

配置域名服务器的 IPv6 地址为 2::2。

```
<Device> system-view
[Device] ipv6 dns server 2::2
```

配置域名后缀 com。

```
[Device] dns domain com
```

4. 验证配置

在设备上执行 **ping ipv6 host** 命令，可以 ping 通主机，且对应的目的地址为 1::1。

```
[Device] ping ipv6 host
Ping6(56 data bytes) 3::1 --> 1::1, press CTRL_C to break
56 bytes from 1::1, icmp_seq=0 hlim=128 time=1.000 ms
56 bytes from 1::1, icmp_seq=1 hlim=128 time=0.000 ms
56 bytes from 1::1, icmp_seq=2 hlim=128 time=1.000 ms
56 bytes from 1::1, icmp_seq=3 hlim=128 time=1.000 ms
56 bytes from 1::1, icmp_seq=4 hlim=128 time=0.000 ms

--- Ping6 statistics for host ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.600/1.000/0.490 ms
```

1.13.3 DNS proxy典型配置举例

1. 组网需求

某局域网内拥有多台设备，每台设备上都指定了域名服务器的 IPv6 地址，以便直接通过域名访问外部网络。当域名服务器的 IPv6 地址发生变化时，网络管理员需要更改局域网内所有设备上配置的域名服务器 IPv6 地址，工作量将会非常巨大。

通过 DNS proxy 功能，可以大大减少网络管理员的工作量。当域名服务器 IPv6 地址改变时，只需更改 DNS proxy 上的配置，即可实现局域网内设备通过新的域名服务器解析域名。

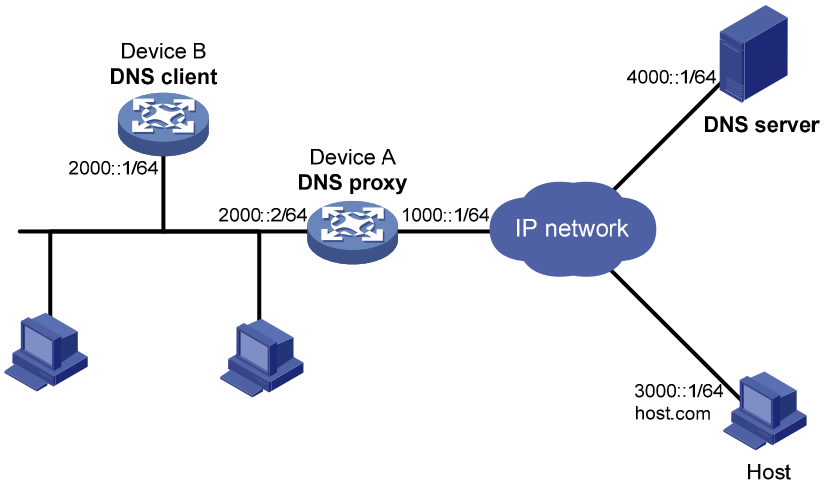
在本例中，具体配置步骤为：

(1) 局域网中的某台设备 Device A 配置为 DNS proxy，DNS proxy 上指定域名服务器 IPv6 地址为真正的域名服务器的地址 4000::1

(2) 局域网中的其他设备（如 Device B）上，域名服务器的 IPv6 地址配置为 DNS proxy 的地址，域名解析报文将通过 DNS proxy 转发给真正的域名服务器。

2. 组网图

图1-15 DNS proxy 组网图



3. 配置步骤

说明

在开始下面的配置之前，假设设备与域名服务器、主机之间的路由可达，并已按照 图 1-9 配置各接口的IPv6 地址。

(1) 配置域名服务器

不同的域名服务器的配置方法不同。Windows Server 2008 R2 作为域名服务器时，配置方法请参见“1.13.2 动态域名解析配置举例”。

(2) 配置 DNS 代理 Device A

配置域名服务器的 IPv6 地址为 4000::1。

```
<DeviceA> system-view
```

```
[DeviceA] ipv6 dns server 4000::1
```

开启 DNS proxy 功能。

```
[DeviceA] dns proxy enable
```

(3)　配置 DNS 客户端 Device B

配置域名服务器的 IPv6 地址为 2000::2。

```
<DeviceB> system-view
[DeviceB] ipv6 dns server 2000::2
```

4. 验证配置

在 Device B 上执行 **ping host.com** 命令，可以 ping 通主机，且对应的目的地址为 3000::1。

```
[DeviceB] ping host.com
Ping6(56 data bytes) 2000::1 --> 3000::1, press CTRL_C to break
56 bytes from 3000::1, icmp_seq=0 hlim=128 time=1.000 ms
56 bytes from 3000::1, icmp_seq=1 hlim=128 time=0.000 ms
56 bytes from 3000::1, icmp_seq=2 hlim=128 time=1.000 ms
56 bytes from 3000::1, icmp_seq=3 hlim=128 time=1.000 ms
56 bytes from 3000::1, icmp_seq=4 hlim=128 time=0.000 ms

--- Ping6 statistics for host com ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.600/1.000/0.490 ms
```

1.14 常见配置错误举例

1.14.1 IPv4 域名解析常见配置错误举例

1. 现象描述

配置了动态域名解析，但不能根据域名解析到正确的 IP 地址。

2. 故障分析

DNS 客户端需要和域名服务器配合使用，才能根据域名解析到正确的 IP 地址。

3. 故障排除

- 执行命令 **display dns host ip**，检查动态域名缓存信息是否存在指定域名。
- 如果不存在要解析的域名，检查 DNS 客户端是否和域名服务器通信正常，域名服务器是否工作正常。
- 如果存在要解析的域名，但地址不对，则检查 DNS 客户端所配置的域名服务器的 IP 地址是否正确。
- 检查域名服务器所设置的域名和地址映射表是否正确。

1.14.2 IPv6 域名解析常见配置错误举例

1. 现象描述

配置了动态域名解析，但不能根据域名解析到正确的 IPv6 地址。

2. 故障分析

DNS 客户端需要和域名服务器配合使用，才能根据域名解析到正确的 IPv6 地址。

3. 故障排除

- 执行命令 **display dns host ipv6**，检查动态域名缓存信息是否存在指定域名。
- 如果不存在要解析的域名，检查 DNS 客户端是否和域名服务器通信正常，域名服务器是否工作正常。
- 如果存在要解析的域名，但地址不对，则检查 DNS 客户端所配置的域名服务器的 IPv6 地址是否正确。
- 检查域名服务器所设置的域名和地址映射表是否正确。

2 DDNS

设备各款型对于本节所描述的特性的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	DDNS	仅MSR810-LMS/810-LUS不支持
MSR2600-6-X1/2600-10-X1		支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		不支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3640/3660		支持
MSR5620/5660/5680		支持

型号	命令	描述
MSR810-W-WiNet/810-LM-WiNet	**DDNS**	支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	DDNS	支持
MSR810-W-LM-GL		支持
MSR830-6EI-GL		支持
MSR830-10EI-GL		支持
MSR830-6HI-GL		支持
MSR830-10HI-GL		支持

型号	特性	描述
MSR2600-6-X1-GL		支持
MSR3600-28-SI-GL		不支持

2.1 DDNS简介

2.1.1 概述

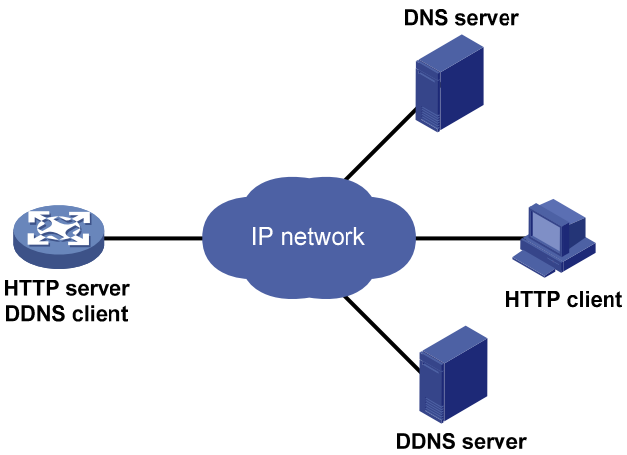
利用 DNS 可以将域名解析为 IP 地址，从而实现使用域名来访问网络中的节点。但是，DNS 仅仅提供了域名和 IP 地址之间的静态对应关系，当节点的 IP 地址发生变化时，DNS 无法动态地更新域名和 IP 地址的对应关系。此时，如果仍然使用域名访问该节点，通过域名解析得到的 IP 地址是错误的，从而导致访问失败。

DDNS（Dynamic Domain Name System，动态域名系统）用来动态更新 DNS 服务器上域名和 IP 地址之间的对应关系，保证通过域名解析到正确的 IP 地址。

目前，只有 IPv4 域名解析支持 DDNS，IPv6 域名解析不支持 DDNS，即只能通过 DDNS 动态更新域名和 IPv4 地址之间的对应关系。

2.1.2 DDNS典型组网应用

图2-1 DDNS 典型组网图



DDNS的典型组网环境如 图 2-1 所示，DDNS采用客户端/服务器模式：

- DDNS 客户端：IP 地址变化时，需要在 DNS 服务器上动态更新其域名和 IP 地址对应关系的设备。Internet 用户通常通过域名访问提供应用层服务的服务器，如 HTTP、FTP 服务器。为了保证 IP 地址变化时，仍然可以通过域名访问这些服务器，当服务器的 IP 地址发生变化时，服务器将作为 DDNS 客户端，向 DDNS 服务器发送更新域名和 IP 地址对应关系的 DDNS 更新请求。
- DDNS 服务器：负责通知 DNS 服务器动态更新域名和 IP 地址之间的对应关系。接收到 DDNS 客户端的更新请求后，DDNS 服务器通知 DNS 服务器重新建立 DDNS 客户端的域名和 IP 地

址之间的对应关系。从而保证即使 DDNS 客户端的 IP 地址改变，Internet 用户仍然可以通过同样的域名访问 DDNS 客户端。

说明

- 目前，DDNS 更新过程没有统一的标准，向不同的 DDNS 服务器请求更新的过程各不相同。
- 设备可以作为 DDNS 客户端，通过 www.3322.org、花生壳等 DDNS 服务器动态更新 DNS 服务器上域名和 IP 地址之间的对应关系。

2.2 设备作为DDNS客户端配置任务简介

表2-1 设备作为 DDNS 客户端配置任务简介

配置任务	说明	详细配置
配置DDNS策略	必选	2.3
在接口上应用DDNS策略	必选	2.4
配置DDNS报文的DSCP优先级	可选	2.5

2.3 配置DDNS策略

1. 功能简介

DDNS 策略是 DDNS 服务器的地址、端口号、登录用户名、密码、时间间隔、关联的 SSL 客户端策略和更新时间间隔等信息的集合。创建 DDNS 策略后，可以在不同的接口上应用相同的 DDNS 策略，从而简化 DDNS 的配置。

2. 配置限制和指导

设备向不同DDNS服务器请求更新的过程各不相同，因此，DDNS更新请求的URL地址的配置方式也存在差异，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>
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>

DDNS 服务器	DDNS 更新请求的 URL 地址格式
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

其中：

- 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。建议不要修改URL中的<h>和<a>，以免配置错误的FQDN和IP地址。应用DDNS策略的详细介绍，请参见“2.4 在接口上应用DDNS策略”。
- 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。

说明

FQDN 是节点在网络中的唯一标识，由主机名和域名组成，可被解析为 IP 地址。

3. 配置准备

登录 DDNS 服务提供商的网站，注册帐户，并为 DDNS 客户端申请域名。通过 DDNS 服务器更新域名和 IP 地址的对应关系时，DDNS 服务器将检查 DDNS 更新请求中的帐户信息是否正确、需要更新的域名是否属于该帐户。

4. 配置步骤

与 DHS 通信时，需要通过 **method** 命令指定 HTTP 使用 http-post 参数传输方式进行 DDNS 更新。

基于 HTTPS 与 DDNS 服务器通信时，需要通过 **ssl client policy** 命令指定与 DDNS 策略关联的 SSL 客户端策略，SSL 客户端策略的配置方法请参见“安全配置指导”中的“SSL”。

表2-3 配置 DDNS 策略

操作	命令	说明
进入系统视图	**system-view**	-
创建DDNS策略，并进入DDNS策略视图	**ddns policy** *policy-name*	缺省情况下，设备上不存在任何DDNS策略
指定DDNS更新请求的URL地址	**url** *request-url*	缺省情况下，未指定DDNS更新请求的URL地址
指定登录DDNS服务器的用户名	**username** *username*	缺省情况下，未指定登录DDNS服务器的用户名
指定登录DDNS服务器的的密码	**password** { **cipher** | **simple** } *string*	缺省情况下，未指定登录DDNS服务器的密码
（可选）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	**method** { **http-get** | **http-post** }	缺省情况下，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 本命令仅在基于HTTP或HTTPS与DDNS服务器通信时生效
（可选）指定与DDNS策略关联的SSL客户端策略	**ssl-client-policy** *policy-name*	缺省情况下，未指定与DDNS策略关联的SSL客户端策略 SSL客户端策略只对URL为HTTPS地址的DDNS更新请求有效
（可选）指定定时发起更新请求的时间间隔	**interval** *days* [*hours* [*minutes*]]	缺省情况下，定时发起DDNS更新请求的时间间隔是1小时

2.4 在接口上应用DDNS策略

在接口上应用 DDNS 策略，并指定需要更新的 FQDN 与 IP 地址对应关系后，DDNS 客户端才会向 DDNS 服务器发起更新域名和接口主 IP 地址对应关系的请求。

1. 配置准备

- 配置该接口的主 IP 地址，使之与 DDNS 服务器路由可达。
- 配置IPv4 静态或动态域名解析功能，以便将DDNS服务器的域名解析为IP地址。域名解析功能的配置方法请参见“1.3 配置IPv4 DNS client”。

2. 配置步骤

表2-4 配置接口应用 DDNS 策略

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入接口视图	**interface** *interface-type interface-number*	-
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	**ddns apply policy** *policy-name* [**fqdn** *domain-name*]	除花生壳DDNS服务器外，其他的DDNS服务器均需要指定更新的FQDN，否则会导致DDNS更新失败 缺省情况下，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

说明

对于花生壳 DDNS 服务器，如果未指定更新的 FQDN，则 DDNS 服务器将更新 DDNS 客户端的帐户对应的所有域名；如果指定了更新的 FQDN，则 DDNS 服务器只更新指定的 FQDN。

2.5 配置DDNS报文的DSCP优先级

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。通过本配置可以指定 DDNS 服务器发送的 DDNS 报文的 DSCP 优先级。

表2-5 配置 DDNS 报文的 DSCP 优先级

操作	命令	说明
进入系统视图	**system-view**	-
配置DDNS报文的DSCP优先级	**ddns dscp** *dscp-value*	缺省情况下，DDNS报文的DSCP优先级为0

2.6 DDNS显示和维护

在完成上述配置后，在任意视图下执行 **display ddns policy** 命令可以显示 DDNS 策略的配置情况，通过查看显示信息验证配置的效果。

表2-6 DDNS 显示和维护

操作	命令
显示DDNS策略的配置情况	**display ddns policy** [*policy-name*]

2.7 DDNS典型配置举例

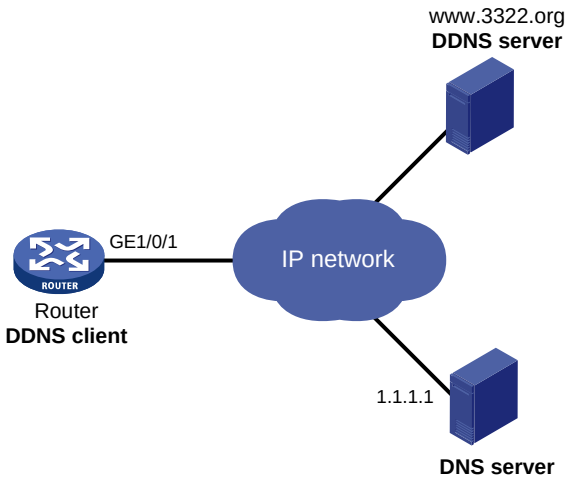
2.7.1 与www.3322.org互通的配置举例

1. 组网需求

- Router 为 Internet 上的用户提供 Web 服务，使用的域名为 whatever.3322.org。
- Router 通过 DHCP 获得 IP 地址，为保证 Router 的 IP 地址变化后，Internet 上的用户仍然可以利用域名 whatever.3322.org 访问 Router，Router 通过 www.3322.org 提供的 DDNS 服务及时通知 DNS 服务器更新域名和 IP 地址的对应关系。
- DNS 服务器的 IP 地址为 1.1.1.1。Router 通过该 DNS 服务器将 DDNS 服务器的域名 www.3322.org 解析为 IP 地址。

2. 组网图

图2-2 与 www.3322.org 互通配置举例组网图



3. 配置步骤

说明

配置之前，请登录 http://www.3322.org 注册帐户(本配置举例以帐户名 steven，密码 nevets 为例)。配置 DDNS 策略来更新指定的 FQDN whatever.3322.org 和 IP 地址的对应关系，并保证各个设备之间的路由可达。

创建名称为 3322.org 的 DDNS 策略，并进入 DDNS 策略视图。

```
<Router> system-view
[Router] ddns policy 3322.org
```

为 DDNS 策略 3322.org 指定 DDNS 更新请求的 URL 地址，登录用户名为 steven，密码为明文字段 nevets。

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

```
[Router-ddns-policy-3322.org] password simple nevets
```

为 DDNS 策略 3322.org 指定定时发起更新请求的时间间隔为 15 分钟。

```
[Router-ddns-policy-3322.org] interval 0 0 15
[Router-ddns-policy-3322.org] quit
```

配置 DNS 服务器的 IP 地址为 1.1.1.1。

```
[Router] dns server 1.1.1.1
```

在 GigabitEthernet1/0/1 接口下指定应用 DDNS 策略 3322.org，更新域名 whatever.3322.org 与接口主 IP 地址的对应关系，并启动 DDNS 更新功能。

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ddns apply policy 3322.org fqdn whatever.3322.org
```

配置完成后，Router 的接口 IP 地址变化时，它将通过 DDNS 服务提供商 www.3322.org 通知 DNS 服务器建立域名 whatever.3322.org 和新的 IP 地址的对应关系，从而保证 Internet 上的用户可以通过域名 whatever.3322.org 解析到最新的 IP 地址，访问 Router 提供的 Web 服务。

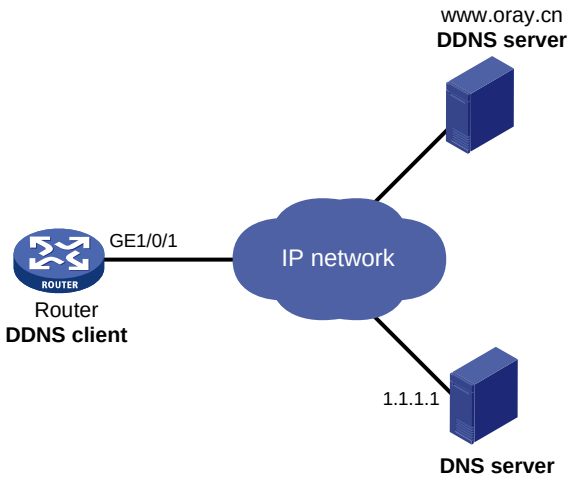
2.7.2 与花生壳DDNS服务器互通的配置举例

1. 组网需求

- Router 为 Internet 上的用户提供 Web 服务，使用的域名为 whatever.gicp.cn。
- Router 通过 DHCP 获得 IP 地址，为保证 Router 的 IP 地址变化后，Internet 上的用户仍然可以利用域名 whatever.gicp.cn 访问 Router，Router 通过花生壳提供的 DDNS 服务及时通知 DNS 服务器更新域名和 IP 地址的对应关系。
- DNS 服务器的 IP 地址为 1.1.1.1。Router 通过该 DNS 服务器将花生壳 DDNS 服务器的域名解析为 IP 地址。

2. 组网图

图2-3 与花生壳 DDNS 服务器互通配置举例组网图



3. 配置步骤

说明

配置之前，请登录 http://www.oray.cn 注册帐户（本配置举例以用户名 steven，密码 nevets 为例）。配置 DDNS 策略来更新指定的 FQDN whatever.gicp.cn 和 IP 地址的对应关系，并保证各个设备之间的路由可达。

创建名称为 oray.cn 的 DDNS 策略，并进入 DDNS 策略视图。

```
<Router> system-view
[Router] ddns policy oray.cn
```

为 DDNS 策略 oray.cn 指定 DDNS 更新请求的 URL 地址，登录用户名为 steven，密码为明文字段 nevets。

```
[Router-ddns-policy-oray.cn] url oray://phservice2.oray.net
[Router-ddns-policy-oray.cn] username steven
[Router-ddns-policy-oray.cn] password simple nevets
```

为 DDNS 策略 oray.cn 指定定时发起更新请求的时间间隔为 12 分钟。

```
[Router-ddns-policy-oray.cn] interval 0 0 12
[Router-ddns-policy-oray.cn] quit
```

配置 DNS 服务器的 IP 地址为 1.1.1.1。

```
[Router] dns server 1.1.1.1
```

在 GigabitEthernet1/0/1 接口下指定应用 DDNS 策略 oray.cn，更新域名 whatever.gicp.cn 与接口主 IP 地址的对应关系，并启动 DDNS 更新功能。

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ddns apply policy oray.cn fqdn whatever.gicp.cn
```

配置完成后，Router 的接口 IP 地址变化时，它将通过花生壳 DDNS 服务器通知 DNS 服务器建立域名 whatever.gicp.cn 和新的 IP 地址的对应关系，从而保证 Internet 上的用户可以通过域名 whatever.gicp.cn 解析到最新的 IP 地址，访问 Router 提供的 Web 服务。