Contents

DNS commands 1

display dns domain 1
display dns host 1
display dns server 3
display ipv6 dns server 4
dns domain 5
dns dscp 5
dns proxy enable 6
dns server 6
dns source-interface 7
dns spoofing 8
dns trust-interface 9
ip host 10
ipv6 dns dscp 10
ipv6 dns server 11
ipv6 dns spoofing 12
ipv6 host 13
reset dns host 14

DDNS commands 15

ddns apply policy 15
ddns dscp 16
ddns policy 16
display ddns policy 17
interval 18
method 19
password 20
ssl-client-policy 21
url 22
username 24

DNS commands

display dns domain

Use **display dns domain** to display the domain name suffixes.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

dynamic: Displays the domain name suffixes dynamically obtained through DHCP or other protocols. If you do not specify this keyword, the command displays the statically configured and dynamically obtained domain name suffixes.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. To display domain name suffixes on the public network, do not use this option.

Examples

Display domain name suffixes on the public network.

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

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

Table 1 Command output

Field	Description
No.	Sequence number.
Type	Domain name suffix type: • **S**—A statically configured domain name suffix. • **D**—A domain name suffix dynamically obtained through DHCP or other protocols.
Domain suffix	Domain name suffixes.

Related commands

dns domain

display dns host

Use **display dns host** to display information about domain name-to-IP address mappings.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip: Specifies type A queries. A type A query resolves a domain name to the mapped IPv4 address.

ipv6: Specifies type AAAA queries. A type AAAA query resolves a domain name to the mapped IPv6 address.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. To display domain name-to-IP address mappings for the public network, do not use this option.

Usage guidelines

If you do not specify the **ip** or **ipv6** keyword, this command displays domain name-to-IP address mappings of all query types.

Examples

Display domain name-to-IP address mappings of all query types.

```
<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
```

Table 2 Command output

Field	Description
No.	Sequence number.
Host name	Domain name.
Type	Domain name-to-IP address mapping type: • **S**—A static mapping configured by the **ip host** or **ipv6 host** command. • **D**—A mapping dynamically obtained through dynamic domain name resolution.
TTL	Time in seconds that a mapping can be stored in the cache. For a static mapping, a hyphen (-) is displayed.
Query type	Query type, **type A** or **type AAAA**.

Field	Description
IP addresses	Replied IP address: • For type A query, the replied IP address is an IPv4 address. • For type AAAA query, the replied IP address is an IPv6 address.

Related commands

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

display dns server

Use **display dns server** to display IPv4 DNS server information.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

dynamic: Displays IPv4 DNS server information dynamically obtained through DHCP or other protocols. If you do not specify this keyword, the command displays statically configured and dynamically obtained IPv4 DNS server addresses.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. To display IPv4 DNS server information for the public network, do not use this option.

Examples

Display IPv4 DNS server information about the public network.

```
<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
```

Table 3 Command output

Field	Description
No.	Sequence number.
Type	DNS server type: • **S**—A manually configured DNS server. • **D**—DNS server information dynamically obtained through DHCP or other protocols.

Field	Description
IP address	IPv4 address of the DNS server.

Related commands

dns server

display ipv6 dns server

Use **display ipv6 dns server** to display IPv6 DNS server information.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

dynamic: Displays IPv6 DNS server information dynamically obtained through DHCP or other protocols. If you do not specify this keyword, the command displays the statically configured and dynamically obtained IPv6 DNS server information.

vpn-instance *vpn-instance-name* : Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. To display IPv6 DNS server information for the public network, do not use this option.

Examples

Display IPv6 DNS server information about the public network.

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

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

Table 4 Command output

Field	Description
No.	Sequence number.
Type	DNS server type: • **S**—A manually configured DNS server. • **D**—DNS server information dynamically obtained through DHCP or other protocols.
IPv6 address	IPv6 address of the DNS server.
Outgoing Interface	Output interface.

Related commands

ipv6 dns server

dns domain

Use **dns domain** to configure a domain name suffix.

Use **undo dns domain** to delete the specified domain name suffix.

Syntax

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

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

Default

No domain name suffix is configured. Only the provided domain name is resolved.

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a domain name suffix. It is a dot-separated, case-insensitive string that can include letters, digits, hyphens (-), underscores (_), and dots (.), for example, aabbcc.com. The domain name suffix can include at most 253 characters, and each separated string includes no more than 63 characters.

vpn-instance *vpn-instance-name*: Specifies the name of a VPN instance, a case-sensitive string of 1 to 31 characters. To specify a domain name suffix on the public network, do not use this option.

Usage guidelines

A domain name suffix applies to both IPv4 DNS and IPv6 DNS.

You can specify the following:

- Domain name suffixes for the public network and up to 1024 VPNs.
- A maximum of 16 domain name suffixes for the public network or each VPN.

For domain name resolution, the resolver automatically uses the suffix list to supply the missing part of an incomplete name entered by a user.

Examples

Configure the domain name suffix **com** for the public network.

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

Related commands

display dns domain

dns dscp

Use **dns dscp** to set the DSCP value for DNS packets sent by a DNS client or DNS proxy.

Use **undo dns dscp** to restore the default.

Syntax

dns dscp *dscp-value*

undo dns dscp

Default

The DSCP value in DNS packets is 0.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Sets the DSCP value for outgoing DNS packets, in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value for outgoing DNS packets to 30.

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

dns proxy enable

Use **dns proxy enable** to enable DNS proxy.

Use **undo dns proxy enable** to restore the default.

Syntax

dns proxy enable

undo dns proxy enable

Default

DNS proxy is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This configuration applies to both IPv4 DNS and IPv6 DNS.

Examples

Enable DNS proxy.

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

dns server

Use **dns server** to specify the IPv4 address of a DNS server.

Use **undo dns server** to remove the specified IPv4 address of a DNS server. If you do not specify an IPv4 address, the **undo dns server** command removes all DNS server IPv4 addresses on the public network or the specified VPN.

Syntax

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

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

Default

No DNS server is specified.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies an IPv4 address of a DNS server.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. To specify an IPv4 address on the public network, do not use this option.

Usage guidelines

The device sends DNS query request to the DNS servers in the order their IPv4 addresses are specified.

You can specify the following:

- DNS server IPv4 addresses for the public network and up to 1024 VPNs.
- A maximum of six DNS server IPv4 addresses for the public network or each VPN.

Examples

Specify the IPv4 address of a DNS server as 172.16.1.1.

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

Related commands

display dns server

dns source-interface

Use **dns source-interface** to specify the source interface for DNS packets.

Use **undo dns source-interface** to restore the default.

Syntax

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*]

Default

No source interface for DNS packets is specified. The device uses the primary IP address of the output interface of the matching route as the source IP address for a DNS request.

Views

System view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. To specify a source interface on the public network, do not use this option.

Usage guidelines

This configuration applies to both IPv4 and IPv6.

- In IPv4 DNS, the device uses the primary IPv4 address of the specified source interface as the source IP address of DNS query.
- In IPv6 DNS, the device follows the procedure defined in RFC 3484 to select an IPv6 address of the source interface as the source IP address for DNS query.

If you use the command multiple times, the most recent configuration takes effect.

You can specify the following:

- Source interfaces for the public network and a maximum of 1024 VPNs.
- Only one source interface for the public network or each VPN.

Make sure the specified interface is on the VPN specified by the **vpn-instance** *vpn-instance-name* option.

Examples

Specify VLAN-interface 2 as the source interface for DNS packets on the public network.

```
<Sysname> system-view
[Sysname] dns source-interface vlan-interface 2
```

dns spoofing

Use **dns spoofing** to enable DNS spoofing and specify the IPv4 address to spoof DNS query requests.

Use **undo dns spoofing** to disable DNS spoofing.

Syntax

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

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

Default

DNS spoofing is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IPv4 address used to spoof name query requests.

vpn-instance *vpn-instance-name*: Specifies the name of a VPN instance, a case-sensitive string of 1 to 31 characters. To enable DNS spoofing on the public network, do not use this option.

Usage guidelines

Use the **dns spoofing** command together with the **dns proxy enable** command. DNS spoofing enables the DNS proxy to send a spoofed reply with a configured IP address even if it cannot reach the DNS server because no dial-up connection is available. Without DNS spoofing, the proxy does

not answer or forward a DNS request if it cannot find a local matching DNS entry or reach the DNS server.

You can configure DNS spoofing for the public network and a maximum of 1024 VPNs. You can specify only one replied IPv4 address on the DNS spoofing device for the public network or each VPN.

If you use the command multiple times, the most recent configuration takes effect.

Examples

Enable DNS spoofing on the public network and specify the IPv4 address 1.1.1.1 to spoof DNS requests.

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

Related commands

dns proxy enable

dns trust-interface

Use **dns trust-interface** to specify the DNS trusted interface.

Use **undo dns trust-interface** to remove the specified DNS trusted interface. If you do not specify an interface, the **undo dns trust-interface** command removes all DNS trusted interfaces.

Syntax

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

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

Default

No trusted interface is specified.

Views

System view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

By default, an interface obtains DNS suffix and DNS server information from DHCP. A network attacker might act as the DHCP server to assign a wrong DNS suffix and DNS server address to the device. As a result, the device fails to obtain the resolved IP address or might get the wrong IP address. With the DNS trusted interface specified, the device only uses the DNS suffix and DNS server information obtained through the trusted interface to avoid attack.

This configuration is applicable to both IPv4 and IPv6.

You can configure up to 128 DNS trusted interfaces on the device.

Examples

Specify VLAN-interface 2 as the DNS trusted interface.

```
<Sysname> system-view
[Sysname] dns trust-interface vlan-interface 2
```

ip host

Use **ip host** to create a host name-to-IPv4 address mapping.

Use **undo ip host** to remove a mapping.

Syntax

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

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

Default

No mappings are created.

Views

System view

Predefined user roles

network-admin

Parameters

host-name: Specifies a host name, a case-insensitive string of 1 to 253 characters. It can include letters, digits, hyphens (-), underscores (_), and dots (.).

ip-address: Specifies the IPv4 address of the host.

vpn-instance *vpn-instance-name*: Specifies the name of a VPN instance, a case-sensitive string of 1 to 31 characters. To specify a host name-to-IP address mapping on the public network, do not specify this option.

Usage guidelines

You can configure the following:

- Host name-to-IPv4 address mappings for the public network and up to 1024 VPNs.
- A maximum of 1024 host name-to-IPv4 address mappings for the public network or each VPN.

On the public network or a VPN, each host name maps only to one IPv4 address. If you use the command multiple times, the most recent configuration takes effect.

Do not use the **ping** command parameter **ip**, **-a**, **-c**, **-f**, **-h**, **-i**, **-m**, **-n**, **-p**, **-q**, **-r**, **-s**, **-t**, **-tos**, **-v**, or **-vpn-instance** as the host name. For more information about the **ping** command parameters, see *Network Management and Monitoring Command Reference*.

Examples

Map IPv4 address 10.110.0.1 to host name **aaa** on the public network.

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

Related commands

display dns host

ipv6 dns dscp

Use **ipv6 dns dscp** to set the DSCP value for IPv6 DNS packets sent by an IPv6 DNS client or DNS proxy.

Use **undo ipv6 dns dscp** to restore the default.

Syntax

ipv6 dns dscp *dscp-value*

undo ipv6 dns dscp

Default

The DSCP value for IPv6 DNS packets is 0.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Sets the DSCP value for outgoing IPv6 DNS packets, in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value for outgoing IPv6 DNS packets to 30.

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

ipv6 dns server

Use **ipv6 dns server** to specify the IPv6 address of a DNS server.

Use **undo ipv6 dns server** to remove the specified DNS server IPv6 address. If you do not specify an IPv6 address, the **undo ipv6 dns server** command removes all DNS server IPv6 addresses on the public network or the specified VPN.

Syntax

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*]

Default

No DNS server IPv6 address is specified.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of a DNS server.

interface-type interface-number: Specifies the output interface by its type and number. If you do not specify an interface, the device forwards DNS packets out of the output interface of the matching route. You must specify the output interface when the IPv6 address of the DNS server is a link-local address.

vpn-instance *vpn-instance-name*: Specifies the name of a VPN instance, a case-sensitive string of 1 to 31 characters. To specify a DNS server IPv6 address on the public network, do not use this option.

Usage guidelines

For dynamic DNS, the device sends DNS query request to the IPv6 DNS servers in the order their IPv6 addresses are specified.

You can specify the following:

- DNS server IPv6 addresses for the public network and up to 1024 VPNs.
- A maximum of six DNS server IPv6 addresses for the public network or each VPN.

Examples

Specify the DNS server IPv6 address as 2002::1 for the public network.

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

Related commands

display ipv6 dns server

ipv6 dns spoofing

Use **ipv6 dns spoofing** to enable DNS spoofing and specify the translated IPv6 address.

Use **undo ipv6 dns spoofing** to disable DNS spoofing.

Syntax

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

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

Default

DNS spoofing is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address used to spoof name query requests.

vpn-instance *vpn-instance-name*: Specifies the name of a VPN instance, a case-sensitive string of 1 to 31 characters. To enable DNS spoofing on the public network, do not use this option.

Usage guidelines

Use the **ipv6 dns spoofing** command together with the **dns proxy enable** command.

DNS spoofing enables the DNS proxy on the device to send a spoofed reply with an IPv6 address in response to a type AAAA DNS request. Without DNS spoofing, the device does not forward or answer a request if no DNS server is specified or no DNS server is reachable.

You can configure DNS spoofing for the public network and a maximum of 1024 VPNs. You can specify only one replied IPv6 address for the public network or each VPN.

If you use the command multiple times, the most recent configuration takes effect.

Examples

Enable DNS spoofing on the public network and specify 2001::1 as the translated IPv6 address.

```
<Sysname> system-view
[Sysname] dns proxy enable
[Sysname] ipv6 dns spoofing 2001::1
```

Related commands

dns proxy enable

ipv6 host

Use **ipv6 host** to create a host name-to-IPv6 address mapping.

Use **undo ipv6 host** to remove a mapping.

Syntax

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

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

Default

No mappings are created.

Views

System view

Predefined user roles

network-admin

Parameters

host-name: Specifies a host name, a case-insensitive string of 1 to 253 characters. It can include letters, digits, hyphens (-), underscores (_), and dots (.).

ipv6-address: Specifies the IPv6 address of the host.

vpn-instance *vpn-instance-name*: Specifies the name of a VPN instance, a case-sensitive string of 1 to 31 characters. To create a host name-to-IPv6 address mapping on the public network, do not use this option.

Usage guidelines

You can configure the following:

- Host name-to-IPv6 address mappings for the public network and up to 1024 VPNs.
- A maximum of 1024 host name-to-IPv6 address mappings for the public network or each VPN.

For the public network or a VPN, each host name maps only to one IPv6 address. If you use the command multiple times, the most recent configuration takes effect.

Do not use the **ping ipv6** command parameter **-a**, **-c**, **-i**, **-m**, **-q**, **-s**, **-t**, **-tc**, **-v**, or **-vpn-instance** as the host name. For more information about the **ping ipv6** command parameters, see *Network Management and Monitoring Command Reference*.

Examples

Map IPv6 address 2001::1 to host name **aaa** on the public network.

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

Related commands

ip host

reset dns host

Use **reset dns host** to clear dynamic DNS entries.

Syntax

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

Views

User view

Predefined user roles

network-admin

Parameters

ip: Specifies type A queries. A type A query resolves a domain name to the mapped IPv4 address.

ipv6: Specifies type AAAA queries. A type AAAA query resolves a domain name to the mapped IPv6 address.

vpn-instance *vpn-instance-name*: Specifies the name of a VPN instance, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN, this command clears dynamic DNS entries for the public network.

Usage guidelines

If you do not specify the **ip** or **ipv6** keyword, the **reset dns host** command clears dynamic DNS entries of all query types.

Examples

Clear dynamic DNS entries of all query types for the public network.

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

Related commands

display dns host

DDNS commands

The term "interface" in this chapter refers to VLAN interfaces.

ddns apply policy

Use **ddns apply policy** to apply a DDNS policy to an interface to update the mapping between the FQDN and the primary IP address of the interface, and to enable DDNS update.

Use **undo ddns apply policy** to remove the application of a DDNS policy from an interface and to stop DDNS update.

Syntax

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

undo ddns apply policy *policy-name*

Default

No DDNS policy and FQDN for update are specified on the interface, and DDNS update is disabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies the DDNS policy name, a case-insensitive string of 1 to 32 characters.

fqdn *domain-name*: Specifies the FQDN to replace <h> in the URL for DDNS update. The *domain-name* argument specifies a case-insensitive string of 1 to 253 characters. It can include letters, digits, hyphens (-), underscores (_), and dots (.).

Usage guidelines

You can apply up to four DDNS policies to an interface.

If you use the **ddns apply policy** command multiple times with the same DDNS policy name but different FQDNs, both of the following occur:

- The most recent configuration takes effect.
- The device initiates a DDNS update request immediately.

Examples

Apply the DDNS policy **steven_policy** to VLAN-interface 2 to update the domain name to IP address mapping for FQDN www.whatever.com and enable DDNS update.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ddns apply policy steven_policy fqdn www.whatever.com
```

Related commands

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

ddns dscp

Use **ddns dscp** to set the DSCP value for outgoing DDNS packets.

Use **undo ddns dscp** to restore the default.

Syntax

ddns dscp *dscp-value*

undo ddns dscp

Default

The DSCP value for outgoing DDNS packets is 0.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Sets the DSCP value for outgoing DDNS packets, in the range of 0 to 63.

Usage guidelines

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.

Examples

Set the DSCP value for outgoing DDNS packets to 30.

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

ddns policy

Use **ddns policy** to create a DDNS policy and enter its view.

Use **undo ddns policy** to delete a DDNS policy.

Syntax

ddns policy *policy-name*

undo ddns policy *policy-name*

Default

No DDNS policy is created.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies the DDNS policy name, a case-insensitive string of 1 to 32 characters.

Usage guidelines

You can create up to 16 DDNS policies on the device.

Examples

Create a DDNS policy **steven_policy** and enter its view.

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

Related commands

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

display ddns policy

Use **display ddns policy** to display information about DDNS policies.

Syntax

display ddns policy [*policy-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

policy-name: Specifies the DDNS policy name, a case-insensitive string of 1 to 32 characters. If you do not specify a DDNS policy, this command displays information about all DDNS policies.

Examples

Display information about the DDNS policy **steven_policy**.

```
<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
```

Display information about all DDNS policies.

```
<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
```

Table 5 Command output

Field	Description
DDNS policy	DDNS policy name.
URL	URL address for a DDNS update request. This field is blank if no URL address is configured.
Username	Username to be included in the URL address for DDNS update requests. This field is blank if no username is configured.
Password	Password to be included in the URL address for DDNS update requests. This field is blank if no password is configured and displays ********** if a password is configured.
Method	Parameter transmission method used to send HTTP/HTTPS-based DDNS update requests. Method types include GET and POST.
SSL client policy	Name of the associated SSL client policy. This field is blank if no SSL client policy is associated.
Interval	Interval for sending DDNS update requests.

Related commands

ddns policy

interval

Use **interval** to specify the interval for sending DDNS update requests after DDNS update is enabled.

Use **undo interval** to restore the default value.

Syntax

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

undo interval

Default

The DDNS update request interval is one hour.

Views

DDNS policy view

Predefined user roles

network-admin

Parameters

days: Days in the range of 0 to 365.

hours: Hours in the range of 0 to 23.

minutes: Minutes in the range of 0 to 59.

Usage guidelines

A DDNS update request is initiated immediately after the primary IP address of the interface changes or the link state of the interface changes from down to up.

If you set the interval to 0, the device does not periodically initiate any DDNS update request. However, it initiates a DDNS update request in either of the following situations:

- When the primary IP address of the interface changes.
- When the link state of the interface changes from down to up.

If you use the **interval** command multiple times with different time intervals, the most recent configuration takes effect. If you change the interval for an applied DDNS policy, the device immediately initiates a DDNS update request and sets the interval as the update interval.

Examples

Set the interval for sending DDNS update requests to one day and one minute for the DDNS policy **steven_policy**.

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

Related commands

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

method

Use **method** to specify the parameter transmission method for sending DDNS update requests to HTTP/HTTPS-based DDNS servers.

Use **undo method** to restore the default.

Syntax

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

undo method

Default

The method **http-get** applies.

Views

DDNS policy view

Predefined user roles

network-admin

Parameters

http-get: Uses the get operation.

http-post: Uses the post operation.

Usage guidelines

This command applies to DDNS updates in HTTP/HTTPS. If the DDNS server uses HTTP or HTTPS service, choose a parameter transmission method compatible with the DDNS server. For example, a DHS server supports the **http-post** method.

If the DDNS policy has been applied to an interface, a DDNS update is sent immediately after the parameter transmission is changed.

Examples

Specify the parameter transmission method as **http-post** for DDNS update request for DDNS policy **steven_policy**.

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

Related commands

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

password

Use **password** to specify the password to be included in the URL address for DDNS update requests.

Use **undo password** to remove the password.

Syntax

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

undo password

Default

No password is specified for the URL address.

Views

DDNS policy view

Predefined user roles

network-admin

Parameters

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies a case-sensitive password string. If **simple** is specified, it must be a string of 1 to 32 characters. If **cipher** is specified, it must be a string of 1 to 73 characters.

Usage guidelines

For security purposes, all passwords, including passwords configured in plain text, are saved in ciphertext.

Examples

Specify the login password as **nevets** to be included in the URL address for update requests of DDNS policy **steven_policy**.

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

Related commands

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

ssl-client-policy

Use **ssl-client-policy** to associate an SSL client policy with a DDNS policy.

Use **undo ssl-client-policy** to cancel the association of an SSL client policy with a DDNS policy.

Syntax

ssl-client-policy *policy-name*

undo ssl-client-policy

Default

No SSL client policy is associated with any DDNS policy.

Views

DDNS policy view

Predefined user roles

network-admin

Parameters

policy-name: Specifies the SSL client policy name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

The SSL client policy is effective only for HTTPS-based DDNS update requests.

If you use the **ssl-client-policy** command multiple times with different SSL client policies, the most recent configuration takes effect.

Examples

Associate the SSL client policy **ssl_policy** with the DDNS policy **steven_policy**.

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

Related commands

- **ddns policy**
- **display ddns policy**
- **ssl-client-policy** (*Security Command Reference*)

url

Use **url** to specify the URL address for DDNS update requests.

Use **undo url** to delete the URL address.

Syntax

url *request-url*

undo url

Default

No URL address is specified for DDNS update requests.

Views

DDNS policy view

Predefined user roles

network-admin

Parameters

request-url: Specifies the URL address, a case-sensitive string of 1 to 240 characters.

Usage guidelines

The URL addresses configured for update requests vary by DDNS server. Common DDNS server URL address format are shown in Table 6.

Table 6 Common URL addresses for DDNS update request

DDNS server	URL addresses for DDNS update requests
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>
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*
PeanutHull	oray://phservice2.oray.net

Do not include the username or password in the URL address. To configure the username and password, use the **username** command and the **password** command.

HP and GNUDIP are common DDNS update protocols. The *server-name* parameter is the domain name or IP address of the service provider's server using one of the update protocols.

The URL address for an update request can start with:

- **http://**—The HTTP-based DDNS server.
- **https://**—The HTTPS-based DDNS server.
- **ods://**—The TCP-based ODS server.
- **gnudip://**—The TCP-based GNUDIP server.
- **oray://**—The TCP-based DDNS server.

The domain names of DDNS servers are members.3322.org and phservice2.oray.net. The domain names of PeanutHull DDNS servers can be phservice2.oray.net, phddns60.oray.net, client.oray.net, ph031.oray.net, and so on. Determine the domain name in the URL according to the actual situation.

The port number in the URL address is optional. If you do not specify a port number, the default port number is used. HTTP uses port 80, HTTPS uses port 443, and the PeanutHull server uses port 6060.

The system automatically performs the following tasks:

- Fills <h> with the FQDN that is specified when the DDNS policy is applied to an interface.
- Fills <a> with the primary IP address of the interface to which the DDNS policy is applied.

You can also manually specify an FQDN and an IP address in <h> and <a>, respectively. In this case, the FQDN that is specified when the DDNS policy is applied to an interface will not take effect. As a best practice, do not manually change the <h> and <a> because your configuration might be incorrect.

You cannot specify an FQDN and IP address in the URL address for contacting the PeanutHull server. Alternatively, you can specify an FQDN when applying the DDNS policy to an interface. The system automatically uses the primary IP address of the interface to which the DDNS policy is applied as the IP address for DDNS update.

To avoid misinterpretation, do not include colons (:), at signs (@), and question marks (?) in your login ID or password, even if you can do so.

If you use the **url** command multiple times with different URL addresses, the most recent configuration takes effect.

Examples

Specify the URL address for DDNS policy **steven_policy** with login ID **steven** and password **nevets**. The device contacts www.3322.org for DDNS update.

```
<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>
```

Related commands

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

username

Use **username** to specify the username to be included in the URL address for DDNS update requests.

Use **undo username** to remove the username.

Syntax

username *username*

undo username

Default

No username is specified for the URL address.

Views

DDNS policy view

Predefined user roles

network-admin

Parameters

username: Specifies the username, a case-sensitive string of 1 to 32 characters.

Examples

Specify the username as **steven** to be included in the URL address for update requests of DDNS policy **steven_policy**.

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

Related commands

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