Technical Guide

Domain Name System (DNS) for AlliedWare Plus™ Switches

Feature Overview and Configuration Guide

Introduction

The **Domain Name System** allows you to access remote systems by entering human-readable device host names rather than IP addresses. DNS works by creating a mapping between a domain name, such as “www.alliedtelesis.com”, and its IP address. These mappings are held on DNS servers. DNS translates meaningful domain names into IP addresses for networking equipment to locate and address these devices. The benefits of DNS are that domain names:

- can map to a new IP address if the host’s IP address changes
- are easier to remember than an IP address
- allow organizations to use a domain name hierarchy that is independent of any IP address assignment

AlliedWare Plus™ has the ability to resolve IP addresses associated with domain names for internally generated commands (DNS Client) as well as providing the DNS information to connected hosts (via DNS Relay and DHCP Server). The DNS Client is enabled automatically when at least one DNS server is configured on the device. This client allows you to use domain names instead of IP addresses when using commands on your device, like ping, SSH, and copy.

The DNS Relay provides the presence of a local virtual DNS server which can service DNS lookup requests sent to it from local hosts. The DHCP Server can be configured to provide DNS information to DHCP clients during the lease process.

Products and software version that apply to this guide

This guide applies to AlliedWare Plus™ switches that support DNS and are running version **5.4.4** or later. To see whether your product supports DNS, see the following documents:

- The product’s Datasheet
- The product’s Command Reference

These documents are available from the above links on our website at alliedtelesis.com.

In order to access DNS features from the Device GUI, we recommend that you have version 2.16.0 or later installed on your device.

For information about DNS on AlliedWare Plus AR-Series Firewalls, see Domain Name System (DNS) for AlliedWare Plus AR-Series Firewalls.

Contents

Domain Name System (DNS)

Domain name parts

Domain names are made up of a hierarchy of two or more name segments. Each segment is separated by a period. The format of domain names is the same as the host portion of a URL (Uniform Resource Locator). The first segment from the left is unique to the host, with each following segment mapping the host in the domain name hierarchy. The segment on the far right is a top-level domain name shared by many hosts.

Server hierarchy

A network of domain name servers maintains the mappings between domain names and their IP addresses. This network operates in a hierarchy that is similar to the structure of the domain names. When a local DNS server cannot resolve your request it sends the request to a higher level DNS server.

For example, to access the site “alliedtelesis.com”, your PC sends a DNS inquiry to its local DNS server asking for the IP address matching alliedtelesis.com. If this address is already locally cached (following its recent use), the DNS server returns the IP address that matches alliedtelesis.com. If the DNS server does not have this address cached, it forwards the request upwards through the hierarchy of DNS servers until a DNS server can resolve the mapping. This means an often-used domain name is resolved quickly, while an uncommon or nonexistent domain may take longer to resolve or fail.

As well as the hierarchy of domain name servers accessible through the Internet, you can operate your own DNS server to map to private IP addresses within your network.

The DHCP server IP address can be either statically defined, or can be dynamically assigned via DHCPv4 option 6 using the **ip name-server** command and DHCP option 15 using the **ip domain-name** command if the DHCP client is configured.

Setting a preference between static or dynamic DNS servers

From release 5.4.9-0.1 onwards, it is possible to set a preference between using statically configured DNS servers or dynamically learned DNS servers.

The command **ip name-server preferred-order [*dynamic*|*static*]** can be used to choose which DNS server set to use first. Select either the **dynamic** or **static** parameter.

By default, the dynamic learned DNS servers are used first. For example, if you want to change the preference to use static servers first, use the command, **ip name-server preferred-order static**.

DNS client

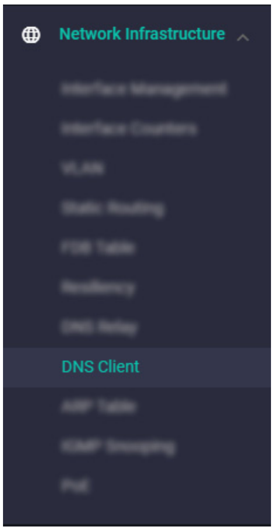
Your AlliedWare Plus device has a DNS Client that is enabled automatically when you configure a name server address on your device. This client allows you to use domain names instead of IP addresses when configuring some features on your device.

DNS client in the Device GUI

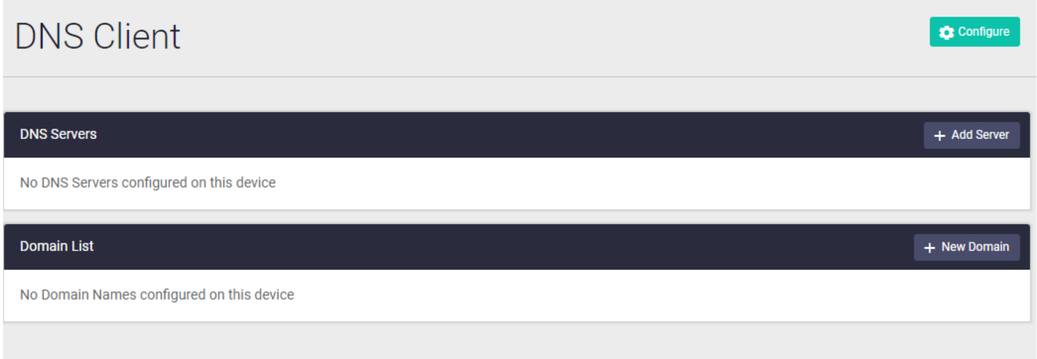
From Device GUI version 2.16.0 onwards, you can use the DNS Client page to:

- configure DNS clients,
- add servers to DNS clients, and
- add or remove domains from the domain list.

Use the left-hand menu to navigate to **Network Infrastructure** > **DNS Client**



The DNS Client page contains the Configure button, and DNS Servers and Domain List tables.



DNS Client

DNS Servers

No DNS Servers configured on this device

Domain List

No Domain Names configured on this device

Clicking on the **Configuration** button will open the Configure window, where you can configure **Domain Lookup via Relay**. Note that DNS Relay is disabled by default. For more information about DNS Relay, see "Enabling DNS Relay in the Device GUI" on page 8.

The **DNS Servers** table displays the servers that you configure for the client to contact. The DNS Servers table includes a source column, which is the source that it learns the server's IP from.

You can use the **Domain List** table to append domains to the DNS query. This is useful if your network has multiple domains, and you would like to simplify the administration. The domain list is ordered based on the order you enter the domains in. In other words, the first entry you create is queried first.

You may want to use the domain list to filter through specific domains, or top-level domains. For example:

- if you add a domain entry as ‘domain.com’, and then perform a DNS query for ‘site1’ it will check **site1.domain.com.**
- if you add a top-level domain entry as ‘.com’, and then you perform a DNS query for ‘site1’, it will check **site1.com**.

Click **+ New Domain** to add a new domain entry in the list.

DNS client commands

The following section shows you a variety of commands that you can use to set up DNS on your device.

Add DNS Server

To add a DNS server to the list of servers that the device sends DNS queries to, use the command:

```
awplus(config)# ip name-server <ip-addr>
```

The order that you enter the servers in, is the order in which they will be used.

Check list of servers

To check the list of servers that the device sends DNS queries to, use the command:

```
awplus# show ip name-server
```

Add default domain name

To add a default domain name used to append to DNS requests, use the command:

```
awplus(config)# ip domain-name <domain-name>
```

To check the domain name configured with this command, use the show command:

```
awplus# show ip domain-name
```

Matching hostnames to network

To use DNS to match hostnames to your internal network named “example.net”, use the command:

```
awplus(config)# ip domain-name example.net
```

Then, if you use the command **ping host2**, your device sends a DNS request for host2.example.net.

Domain List

Alternatively you can create a list of domain names that your device will try in turn by using the command:

```
awplus(config)# ip domain-list <domain-name>
```

For example, to use DNS to match incomplete hostnames to the top level domains “.com”, and “.net”, use the commands:

```
awplus(config)# ip domain-list .com
awplus(config)# ip domain-list .net
```

If you then use the command **ping alliedtelesis**, your device sends a DNS request for alliedtelesis.com and if no match was found your device would then try alliedtelesis.net.

Check domain list entries

To check the entries in the domain list, use the command:

```
awplus# show ip domain-list
```

Disable DNS client

To disable the DNS client on your device, use the command:

```
awplus(config)# no ip domain-lookup
```

Check DNS client status

To check the status of the DNS client on your device, and the configured servers and domain names, use the command:

```
awplus# show hosts
```

DNS Relay

Enabling DNS Relay on your device provides the capability for it to act as a local virtual DNS server. You device can then service DNS lookup requests sent to it from local hosts.

When your device receives a DNS query from a client, the device will attempt to match the request with entries in its cache. If the device does not have this address cached, it forwards the request upwards through the hierarchy of DNS servers for resolution.

When acting as a DNS Relay**,** the device will relay (pass on) the requests to an external, or upstream, DNS server. The relaying of DNS queries is useful if a network administrator wishes to easily change to using a different DNS server.

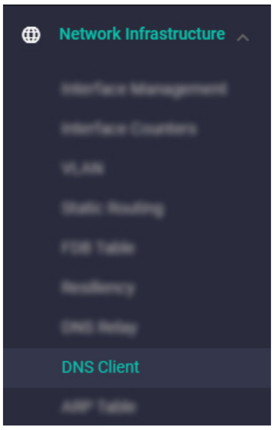
You may wish to configure only the gateway device with the actual DNS address(es), and then configure all the other devices to send their DNS requests to that gateway device. This would mean that, when changing to a different DNS server, you only need to update the DNS address(es) in one place, on the gateway device. This is far more convenient than having to update DNS addresses in all the individual hosts in the network.

DNS Relay requires that IP domain lookup is enabled. To see how to enable IP domain lookup from the CLI, see "DNS Relay commands" on page 9.

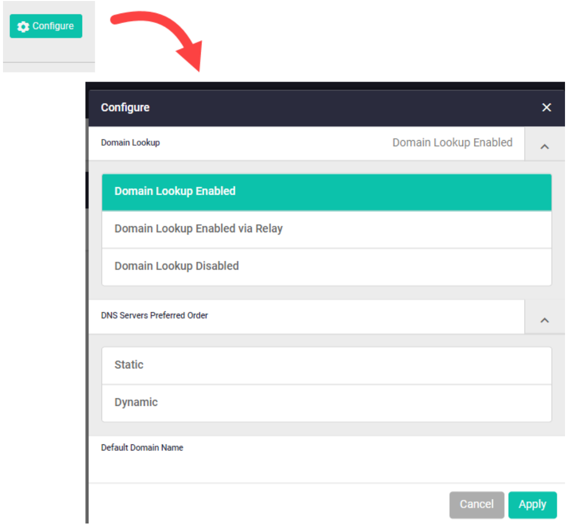
Enabling DNS Relay in the Device GUI

To enable **DNS Relay** from the Device GUI, also known as **Domain Lookup Enabled via Relay,** you must have Device GUI version 2.16.0 or later installed on your device.

Use the left-hand menu to navigate to **Network Infrastructure** > **DNS Client**



Click on the **Configure** button on the DNS Client page to open the Domain Lookup settings:



Domain Lookup: Domain Lookup Enabled

- Domain Lookup Enabled
- Domain Lookup Enabled via Relay
- Domain Lookup Disabled

DNS Servers Preferred Order

- Static
- Dynamic

Default Domain Name

Toggle the Domain Lookup dropdown, and select **Domain Lookup Enabled via Relay** to enable DNS Relay. You can also select a specific order that you would prefer the relay to occur in.

Enabling IP Name Server for DNS Relay

DNS Relay uses the DNS server list configured by the **ip name-server** command to forward DNS query packets. To enable DNS Relay you need to configure the list of servers that the device sends DNS queries to and then enable DNS forwarding, as shown in the following example for a DNS server with an IPv4 address:

```
awplus# configure terminal
awplus(config)# ip name-server 192.168.1.1
awplus(config)# ip name-server 192.168.1.2
awplus(config)# ip dns forwarding
```

DNS Relay requires that IP domain lookup is enabled.

IP domain lookup is enabled by default, but if it has been disabled, you can re-enable it by using the command:

```
awplus(config)# ip domain-lookup
```

Note: Both IPv4 and IPv6 support DNS record types. IPv4 and IPv6 are supported in DNS name-to-address and DNS address-to-name lookup processes. Specifying a name server and enabling DNS forwarding maps both IPv4 and IPv6 addresses.

IPv6 addresses

You can configure DNS Relay to use IPv6 addresses using the same commands used to configure DNS Relay to use IPv4 addresses, as shown in the following example:

```
awplus# configure terminal
awplus(config)# ip name-server 2001:0db8:010d::1
awplus(config)# ip name-server 2001:0db8:010d::2
awplus(config)# ip dns forwarding
```

DNS Relay commands

You can then configure DNS Relay behavior with the following commands:

To set the number of times a device will retry to forward DNS queries, use the command:

```
awplus(config)# ip dns forwarding retry <0-100>
```

To set the number of seconds to wait for a response, use the command:

```
awplus(config)# ip dns forwarding timeout <0-3600>
```

To set the DNS forwarding dead-time period in seconds, use the command:

```
awplus(config)# ip dns forwarding dead-time <60-43200>
```

At the dead-time period set, the device stops sending requests to an unresponsive server.

To set the interface to use for forwarding and receiving DNS queries, use the command:

```
awplus(config)# ip dns forwarding source-interface <interface-name>
```

To specify the DNS Relay name resolver cache size and lifetime, use the command:

```
awplus(config)# ip dns forwarding cache [size <0-1000>] [timeout <60-
3600>]
```

To remove entries from the DNS Relay name resolver cache, use the command:

```
awplus(config)# clear ip dns forwarding cache
```

Information which may be useful for troubleshooting DNS Relay is available using the DNS Relay debugging function. To enable DNS Relay debugging, use the command:

```
awplus# debug ip dns forwarding
```

To display the status of DNS Relay, use the command:

```
awplus# show ip dns forwarding
```

To display the status of DNS Relay name servers, use the command:

```
awplus# show ip dns forwarding server
```

To display the DNS Relay name resolver cache, use the command:

```
awplus# show ip dns forwarding cache
```

DNS operation with VRF-lite

From release 5.5.2-0.1 onwards, on devices that support VRF-lite, you can configure the DNS Client and DNS Relay functionality to be VRF aware.

In this mode the DNS Client will use name-servers configured for the VRF, and DNS Relay will forward DNS messages within specified VRF instances.

Configuring DNS operation with VRF-lite.

The **ip name-server [vrf <*name*>] <*ip-addr*>** command configures a name-server for the specified VRF. This command assigns the address of one or more name servers to a VRF table to be used for name and address resolution. If no VRF-lite instance (vrf<*name*>) is specified, the name-server is configured for the global VRF. A VRF specific name-cache is created within the DNS relay for every VRF instance that has a name-server configured.

A maximum of three name-servers may be defined for each VRF instance.

The configuration command, **ip dns forwarding**, will apply to all VRF instances configured on the device and not on a per VRF basis.

The configuration commands listed below apply to all VRF instances configured on the device and not on a per VRF basis. Timeouts are in seconds as per existing commands:

- `ip dns forwarding retry`
- `ip dns forwarding timeout`
- `ip dns forwarding dead-time`
- `ip dns forwarding source-interface`
- `ip dns forwarding cache`

The following **show** commands provide output information for the VRF instance specified. If a VRF instance is not specified, output is shown for all VRF instances, including the global instance and the output will be formatted in a way that distinguishes the information for each VRF.

- `show ip dns [vrf <name>|global] forwarding server`
- `show ip dns [vrf <name>|global] forwarding cache`
- `show ip name-server [vrf <name>|global]`

The DNS cache can also be cleared on a per VRF instance basis by using the **clear ip dns [vrf <*name*>|global] forwarding cache** command.

The DNS client can be made VRF-aware by forwarding all lookups to the DNS relay.

To configure the DNS client to be VRF-aware, use the commands:

Output

```
awplus# configure terminal
awplus(config)# ip domain-lookup via-relay
awplus(config)# ip dns forwarding
```

The following commands show how to configure a DNS relay name-server for both the specified VRF instance VRF red, and the global VRF instance.

To configure a DNS relay name-server for the VRF-lite instance red:

```
awplus# configure terminal
awplus(config)# ip name-server vrf red 192.168.0.1
awplus(config)# ip domain-lookup
```

To configure a DNS relay name-server for the global VRF instance:

```
awplus# configure terminal
awplus(config)# ip name-server 192.168.1.1
awplus(config)# ip domain-lookup
```

DNS name resolver caching

You can enable **DNS name resolver caching** on the DNS relay, which provides a lookup speed advantage, and avoids unnecessary repeated requests to external DNS servers.

When you enable DNS Relay name resolver cache, the device will maintain a cache of recently used mappings between domain names and IP addresses so that other identical requests can be responded to without further reference to an external, or upstream DNS server.

- The DNS cache has a limited size, and times out entries after a specified period of up to 60 minutes.
- DNS caching is disabled by default.

DHCP options

When your device is using its DHCP client for an interface, it can receive the following DHCP options from the DHCP server:

- Option 6 - a list of DNS servers. This list appends to the dynamic DNS server set on your device with the **ip name-server** command. If you want to change the preference to static, use the command **ip name-server preferred-order static**.
- Option 15 - a domain name used to resolve host names. This option replaces the domain name set with the **ip domain-name** command.

C613-22096-00 REV D

Allied Telesis NETWORK SMARTER

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com