

# Infrastructure

## Static IP Pool Setup on AT&T Fiber NVG

The image below shows how to setup a static IP pool on an AT&T Fiber device, such as an Arris NVG599.

Device	Broadband	Local Network	Voice	Firewall	Diagnostics
Status	Configure	Wi-Fi	MAC Filtering	Wi-Fi Scan	Subnets & DHCP

### Subnets & DHCP

*Making a change to some pulldowns on this page will automatically change the context below it, enabling you to fill only the appropriate fields for the change you have made.  
\* all IP addresses and netmasks must be in IPv4 format nnn.nnn.nnn.nnn*

#### Private LAN Subnet

Device IPv4 Address:

Subnet Mask:

#### DHCP Server

DHCP Server Enable:

DHCPv4 Start Address:

DHCPv4 End Address:

DHCP Lease: Days:  Hours:  Minutes:  Seconds:   
e.g. 01:00:00:00

#### Public Subnet

Public Subnet Mode:

Allow Inbound Traffic:

Public Gateway Address:

Public Subnet Mask:

DHCPv4 Start Address:

DHCPv4 End Address:

Primary DHCP Pool: ☐ Private ☒ Public

#### Cascaded Router

Cascaded Router Enable:

### Help

DHCP server functionality enables the device to assign a "private" IP address and other parameters that allow network communication to your LAN devices. This feature simplifies network administration because the device maintains a list of IP address assignments.

**Device IPv4 Address:** Specifies the LAN IPv4 address of the device itself.

**Subnet Mask:** Specifies the common Class C subnet.

**DHCP Server Enable:** Specifies if the device will hand out leases to LAN-side clients.

**DHCPv4 Start Address:** Specifies the first address in the DHCP address range. You can reserve a sequence of up to 253 IP addresses within a subnet, beginning with the specified address, for dynamic assignment.

**DHCPv4 End Address:** Specifies the last address in the DHCP address range.

**DHCP Lease:** Specifies the default length for DHCP leases issued by the device. Enter lease time in dd:hh:mm:ss format.

**Public Subnet Mode:** Using a public subnet means that IP addresses assigned to LAN clients will be public addresses.

**Allow Inbound Traffic:** When enabled, connections to LAN-side devices are allowed to be initiated from the WAN side. This opens the LAN devices on the Public Subnet to potentially malicious traffic, so care should be taken to ensure the LAN-side devices are properly protected. (Firewall-enabled)

**Public Gateway Address:** The IP address of the public subnet.

Unique solution ID: #1009

Author: n/a

Last update: 2021-01-31 17:09