

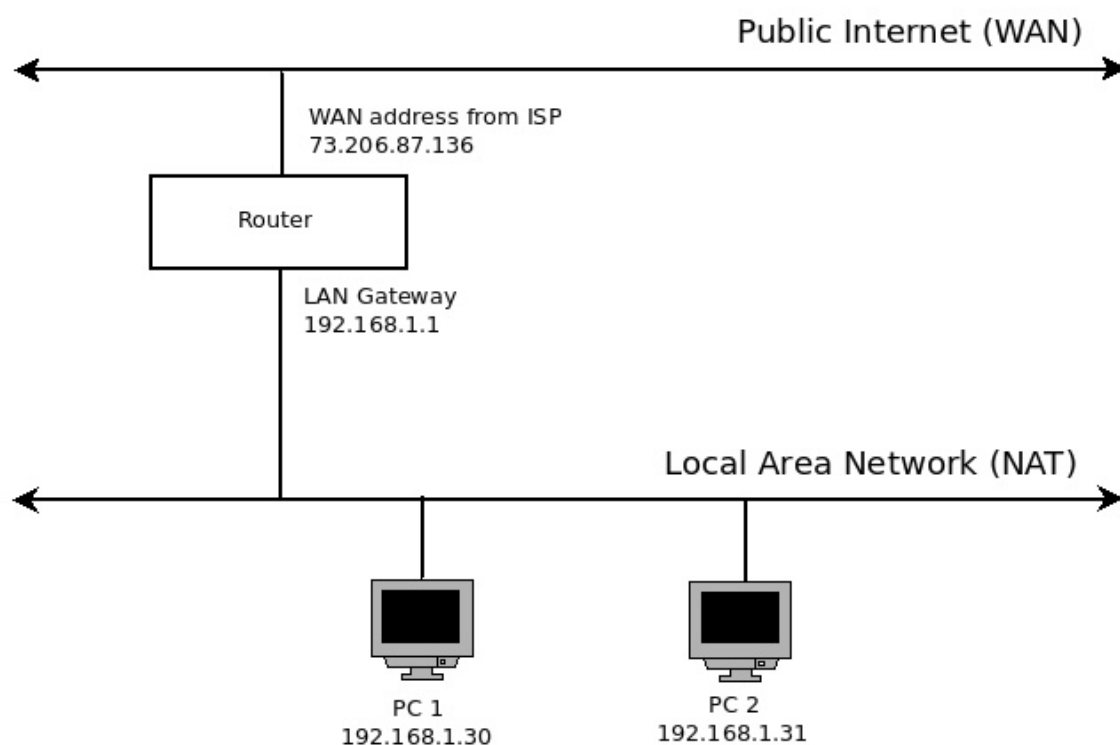
Scotti-BYTE Enterprise Consulting Services

The Joys of IPv6 (Part 2)

In my first blog about IPv6, we learned about the format of IPV6 packets and that IPv6 has no need for a private address range like IPv4 uses on most home networks to implement Network Address Translation (NAT).

One key home networking idea has always been that your Internet Service Provider (ISP) grants you one Wide Area Network (WAN) address and all of your systems live behind your router on a private NAT address range. Here is an example.

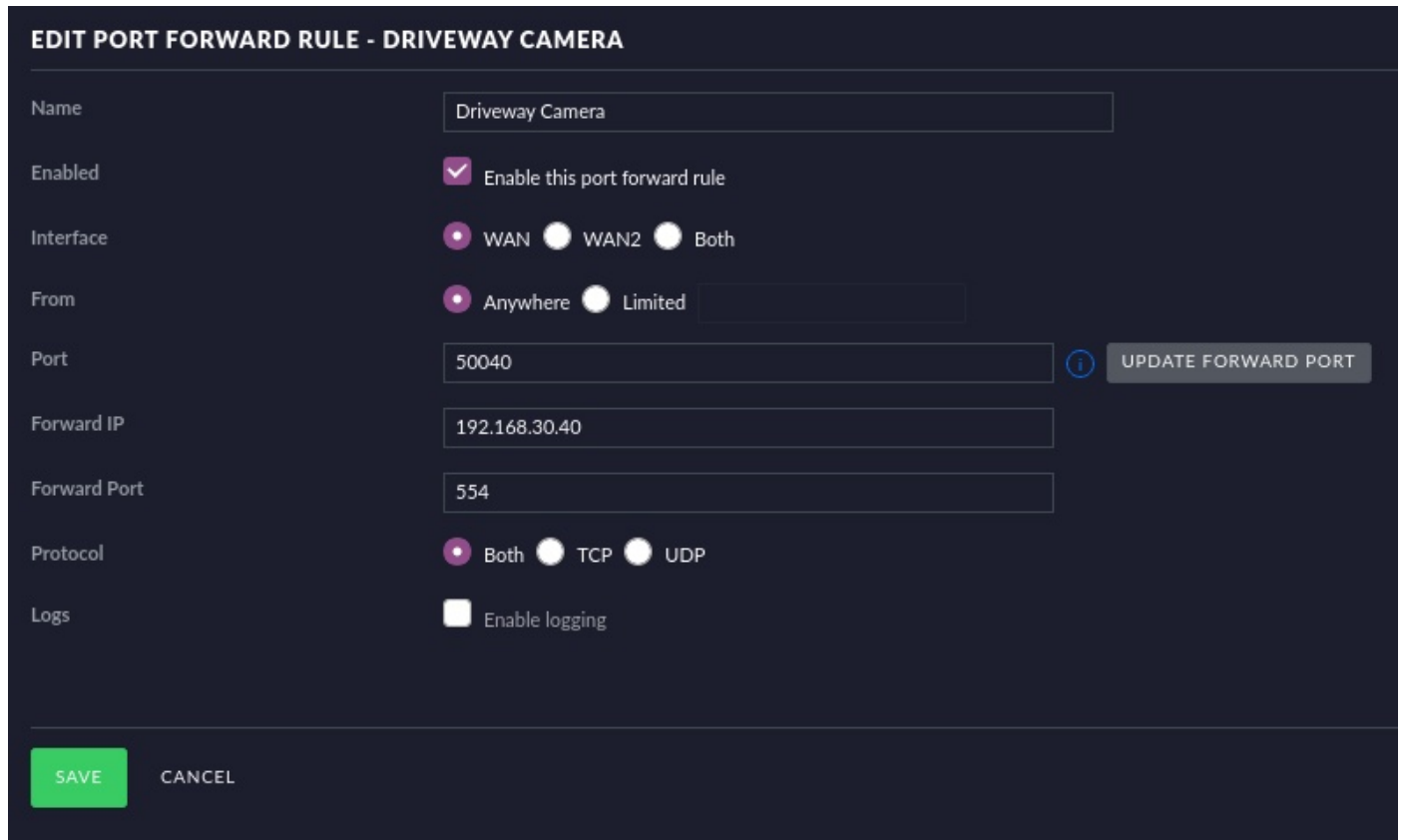
Simple IPv4 Home Network



This arrangement works just fine for putting multiple systems on a private network. When PC 1 goes to a website, the 192.168.1.30 address is encapsulated in the outbound packet which is identified by the 73.206.87.136 WAN address. When the website returns its information to 73.206.87.136, the router sees the encapsulated address 192.168.1.30 for PC 1 is where the data should be sent.

This works fine when the main purpose of the network is to communicate outward. However, if the purpose is to have a server (perhaps PC 2) where a user from outside the network initiates a connection, this is where things get more complicated.

Perhaps a good example of this need is a camera on my network which requires connection initiated by a "cloud" based service such as Amazon. To achieve this in an IPv4 network, you enter a port forwarding rule on the router. On the Ubiquiti Unifi routers, a typical port forward rule looks like this:



The screenshot shows the configuration page for a port forwarding rule named "Driveway Camera". The settings are as follows:

- Name:** Driveway Camera
- Enabled:** Enable this port forward rule
- Interface:** WAN WAN2 Both
- From:** Anywhere Limited
- Port:** 50040 (with an "UPDATE FORWARD PORT" button)
- Forward IP:** 192.168.30.40
- Forward Port:** 554
- Protocol:** Both TCP UDP
- Logs:** Enable logging

At the bottom, there are "SAVE" and "CANCEL" buttons.

Notice that this rule says that if something from the outside requests connection to TCP or UDP port number 50040, then it will be routed to the device on the private LAN at 192.168.30.40 and will be routed to port 554. Port 554 is what cameras use for the Real Time Streaming Protocol (RTSP) and it uses port 554 by convention.

The problem with this arrangement is that since I have only one WAN address that my ISP grants me, in order to make port forward rules for many cameras, I need to use one unique port number on the outside for each camera on the inside, since each camera has a different private LAN address.

Port forward rules like this get converted to WAN IN interface router rules on a router. This works pretty well until you realize that having one WAN address from your ISP complicates things like offering multiple web servers that someone may connect to from the public Internet. Web server protocol for HTTP uses port 80 and HTTPS uses port 443.

This means that you need to use URL redirection at the Domain Name Server (DNS) level to provide a simple URL to end users in conjunction with port forwarding rules.

An example might be:

`https://www.mydomain.com/ ----> https://73.206.87.136:7000`

and the port forward rule for this would take port 7000 and forward the connection to a private address of 192.168.1.30:443 so that it goes to the right web server at the right port.

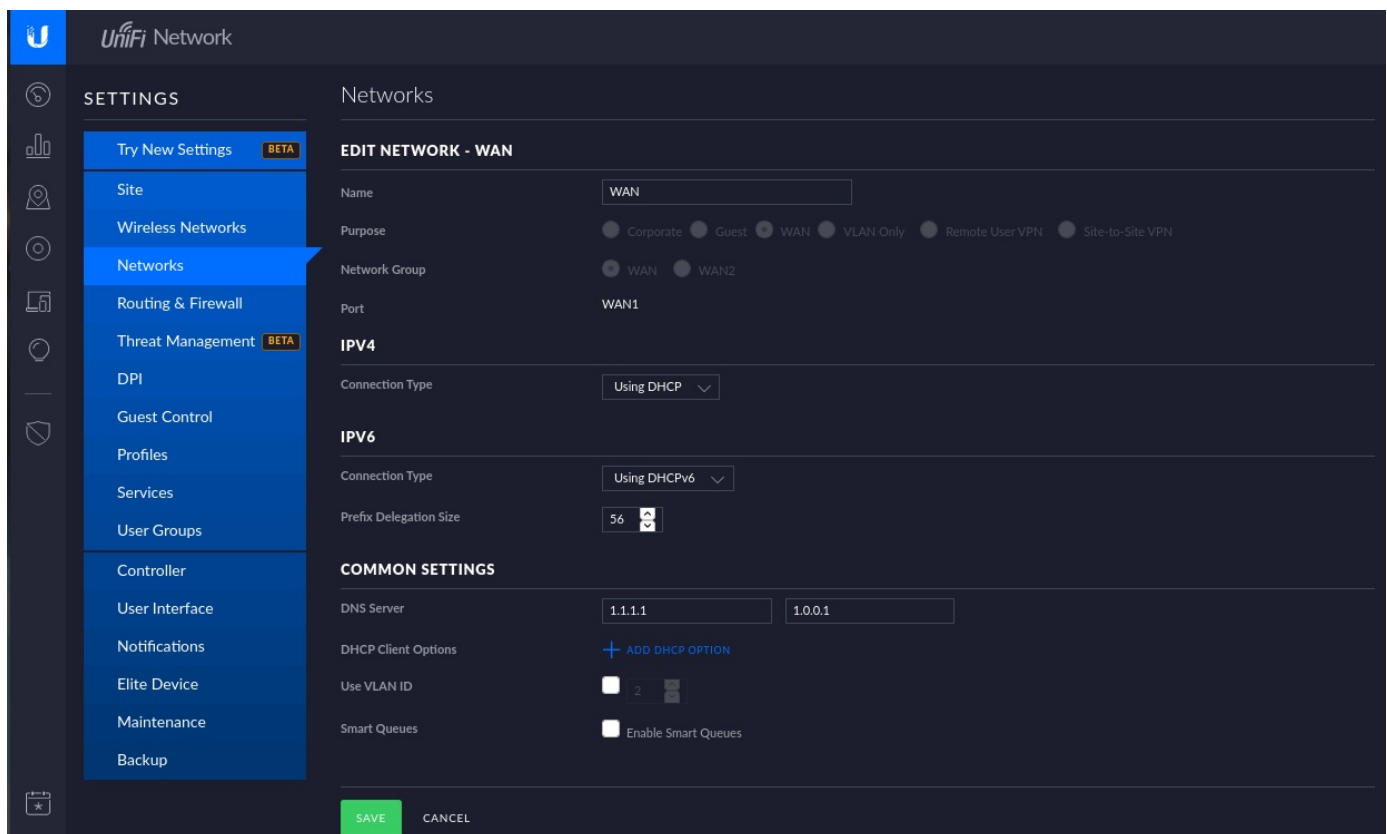
likewise, if you have a second web server:

`https://mysite2.mydomain.com/ ----> https://73.206.87.136:7001`

and the port forward rule for this would take port 7001 and forward the connection to a different private address of 192.168.1.31:443 so that it also makes a connection, but to a different server.

The URL redirection to the WAN address is messy and there are several security programs that flag or deny access to "redirections" like this.

With IPv6, instead of having only one WAN address granted to your router, you receive an IPv6 prefix delegation. This occurs at the router WAN Interface and looks like this on Unifi.



So, to turn on IPv6 for your WAN connection, you change the IPv6 connection type from "NONE" to using DHCPv6. The prefix delegation size can be as small as 1 and as large as 64. 64 means that you are asking for a pool of addresses that is 2^{64} number of nodes. Typically, most ISPs standardize on a prefix delegation size of 56 meaning that each ISP user can have 2^{56} unique IPv6 addresses at their disposal or 4,722,366,482,869,645,213,696 addresses. This may seem unbelievably huge and wasteful until you realize that the entire 128 bit IPv6 address range actually

makes that number look small. The total number of IPv6 addresses is:

340,282,366,920,938,463,463,374,607,431,768,211,456

The total number of IPv4 addresses is 2^{32} which is:

4,294,967,296

IPv6 has been around for 20 years now and operating systems like Windows, Mac OSX, Linux, IOS, and Android have had compatibility for IPv6 built in for most of that time. In addition to that, most ISPs have had IPv6 in operation for years. Almost all routers have IPv6 support.

The world is running out of IPv4 addresses. For now, most new public servers coming online have both IPv4 and IPv6 addresses. The two protocols are entirely different. One cannot talk to the other. For that reason, since most OS support both protocols, the tendency is to offer services on both interfaces.

This is coming to an end though. Once the IPv4 address pool is exhausted, new servers will come online with only IPv6. Similarly, since so much of the world runs on IPv4, you need to continue to run it on your network for the foreseeable future. There is no impact of running both IPv4 and IPv6 on your home network together. Eventually, everyone will move over to IPv6. How long this will take is very hard to say.

So, besides turning on IPv6 on your WAN connection as shown above, you need to enable IPv6 on your LAN network. In Unifi, this is done by going to settings, and editing your LAN network and then going to configure IPV6 Network. Simply change your IPv6 Interface type from "NONE" to "Prefix Delegation".

CONFIGURE IPV6 NETWORK ▾

IPv6 Interface Type None Static Prefix Delegation

IPv6 Prefix Delegation Interface WAN WAN 2

IPv6 RA Enable IPv6 Router Advertisement

IPv6 RA Priority High Medium Low

DHCPv6 Range -

DHCPv6/RDNSS DNS Control Auto Manual

That is all there is to it for the most part. The "RDNSS" is Neighbor Discovery Protocol and it is a protocol in IPv6 that is responsible for the configuration of local computers, domain servers and gateways used to communicate over IPv6.

Whenever you connect to a website from now on, your computer may use either IPv4 or IPv6, depending on the available connection. When you are on an IPv4 network LAN where the router WAN interface has been enabled for IPv6, but not the LAN, you will see your network interface reporting like the following.

```

enp4s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 172.16.1.225 netmask 255.255.0.0 broadcast 172.16.255.255
inet6 fe80::3ded:6c5b:a020:cedf prefixlen 64 scopeid 0x20<link>
ether b8:85:84:bc:00:cf txqueuelen 1000 (Ethernet)
RX packets 75584549 bytes 100629374334 (100.6 GB)
RX errors 0 dropped 8328 overruns 0 frame 0
TX packets 20721004 bytes 5514881595 (5.5 GB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 19

```

Although there is an entry above for IPv6, it begins with an FE80 which is a "Link Local" address and it is what the router uses to find your system and if you had IPv6 enabled on your LAN, it would be what one LAN based IPv6 system would use to talk to another IPv6 system on your LAN.

Once you enable IPv6 on your LAN segment as described above, those addresses will look like this:

```

enp4s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 172.16.1.225 netmask 255.255.0.0 broadcast 172.16.255.255
inet6 2601:2c4:8101:e0:3432:b054:773e:a148 prefixlen 64 scopeid 0x0<global>
inet6 fe80::3ded:6c5b:a020:cedf prefixlen 64 scopeid 0x20<link>
inet6 2601:2c4:8101:e0::3fa prefixlen 128 scopeid 0x0<global>
ether b8:85:84:bc:00:cf txqueuelen 1000 (Ethernet)
RX packets 75629875 bytes 100689019101 (100.6 GB)
RX errors 0 dropped 8333 overruns 0 frame 0
TX packets 20731567 bytes 5516235198 (5.5 GB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 19

```

As you can see, I have not only the internal FE80 LAN address, but I also have the Global 2601 address and the multicast/anycast IPv6 address. Every IPv6 receives a global address which allows that system to communicate on the Public Internet without any need for a private address range or "NAT". That being said, Link Local addresses still exist as mentioned above.

Since every system on the LAN already has a global address in IPv6, there is no reason for port forwarding rules which were designed for Network Address Translation (NAT). This does not mean that every system on the LAN is exposed to the Internet. The router is still a Firewall and so you must create a router firewall WAN IN rule to make a system accessible. These are located under settings, Routing & Firewall, Firewall, Rules IPv6:

The screenshot shows the UniFi Network settings interface. The 'FIREWALL' tab is active, and the 'Rules IPv6' sub-tab is selected. A table lists the following rules:

WAN IN	WAN OUT	WAN LOCAL	LAN IN	LAN OUT	LAN LOCAL	GUEST IN	GUEST OUT	GUEST LOCAL	
RULE INDEX	ENABLED	NAME	ACTION	PROTOCOL	SOURCE	DESTINATION	ACTIONS		
2500	✓	Allow Inbound to Jitsi	Accept	All		Groups: Jitsi Jitsi-ports	EDIT	DELETE	
3003	✓	allow established/related sessions	Accept	All			EDIT	DELETE	
3004	✓	drop invalid state	Drop	All			EDIT	DELETE	

At the bottom of the table, there is a '+ CREATE NEW RULE' button.

In my exmple below, I have a Jitsi server running on an LXC container on my VLAN 80 network where I have enabled IPv6. This is the inbound IPv6 router rule:

The screenshot shows the UniFi Network interface for editing a rule. The left sidebar is set to 'Routing & Firewall'. The main panel is titled 'EDIT RULE - ALLOW INBOUND TO JITSi'. The rule name is 'Allow Inbound to Jitsi' and it is enabled. The rule is applied 'Before predefined rules' and the action is 'Accept'. The IPv6 Protocol is set to 'All'. Under the 'ADVANCED' section, logging is disabled, and states are set to 'New', 'Established', 'Invalid', and 'Related'. Under the 'SOURCE' section, the IPv6 Address Group is 'Any' and the Port Group is 'Any'. Under the 'DESTINATION' section, the IPv6 Address Group is 'Jitsi' and the Port Group is 'Jitsi-ports'.

Since I want my Jitsi server to be publically available, the source address and port group are left at "any". The destination address group is my Jitsi server and the destination port group are the TCP or UDP ports that Jitsi needs to access on the server.

Here is the address group. I got the address from an ifconfig in an ssh session to the server.

The screenshot shows the Mikrotik WinBox interface for editing a Firewall Group named 'JITSI'. The 'FIREWALL' tab is active, and the 'Groups' sub-tab is selected. The configuration is as follows:

- Name:** Jitsi
- Type:** Address IPv6 (selected)
- Address:** 2601:2c4:8101:e1:216:3eff:fe7a:881a

Buttons for 'SAVE' and 'CANCEL' are visible at the bottom left.

Here is the port group. These are the ports needed for the application.

The screenshot shows the Mikrotik WinBox interface for editing a Firewall Group named 'JITSI-PORTS'. The 'FIREWALL' tab is active, and the 'Groups' sub-tab is selected. The configuration is as follows:

- Name:** Jitsi-ports
- Type:** Port (selected)
- Port:** 10000, 443, 4443, 80

Buttons for 'SAVE' and 'CANCEL' are visible at the bottom left.

Unlike port forwarding, there is no requirement for address redirection at the DNS Server since every IPv6 system has its own global address that is reachable from the Internet. Therefore, unique DNS names can be granted for each system without the constraint of the router being the only device with an address.

There is no reason why you cannot have IPv4 port forwarding rules to the same system which you have an IPv6 WAN IN router rule for since as mentioned earlier, every system is running a dual protocol stack with IPv4 and IPv6. The advantage to running IPv6 is the simplicity of straight-forward WAN access and no redirection. In addition, IPv6 is not broadcast based like IPv4 and so there may be less network traffic as you increase your IPv6 usage and decrease your IPv4 reliance.

Admittedly, most of the world is still IPv4, but being prepared and understanding IPv6 now is an asset with no downsides.

From a Ubiquiti Unifi perspective, the Unifi Client listing screen lists systems by name, Mac address, and IPv4 address. There is no option to customize the display to list IPv6 addresses. I think this would be very helpful.

I can also see now why Ubiquiti did not bother to implement a local LAN DNS capability in Unifi. Although dnsmasq is a great combination DHCP and DNS caching utility, in IPv4, DNS was significant for Internet usability because people found it difficult to remember 12-digit IP addresses. With the transition to IPv6, DNS becomes critical, because no-one can remember a 128-bit hexadecimal address. As the Internet shifts from IPv4 to IPv6, hostnames stay the same. A user will continue requesting the same website, unaware that behind the scenes that site may or may not have transitioned to a 128-bit IPv6 address. I can only think that Ubiquiti is planning for IPv6 DNS.

So, right now, most websites have both an IPv4 A record and an IPv6 AAAA record. That's where the dual protocol comes in. The IPv4 clients connect to the server using the IPv4 stack and the IPv6 clients connect to the server using the IPv6 stack. There is no crossover or compatibility mode. That is the key reason why they tell IPv6 adopters to run both IPv4 and IPv6 on their network at the same time. Also, if a site were IPv6 only, and your home network is not configured for IPv6, that site would be unreachable. IPv6 has a lot of great capability and is faster with less overhead, however, IPv4 is still needed for a huge number of legacy connections and will be for years. New sites, will increasingly require IPv6.

I predict a huge wave of demand for consultants who understand how to configure a local LAN for IPv6 and can configure the security for IPv6 firewalls.