Disappearing Choice of Recursive DNS Services in Home Networks

Robert Edmonds (redmonds @ fastly.com)

The home network “gateway” device

Most home broadband Internet users use an access device supplied by their service provider. It typically integrates some or all of:

- Modem
- Router
- Ethernet switch
- Wi-Fi access point
- Analog telephone adapter

This means that the ISP is responsible for the WAN, LAN, and WLAN segments of the home user’s network!

The home network “gateway” device

Gateway manufacturers will be responsive to what features their customers want.

But:

The customer for an ISP-supplied gateway device is not the end user. **The customer is the ISP!**

The home network “gateway” device

Large ISPs who buy millions of units can dictate:

- Branding
- Features

Typical AT&T gateway used for GPON and VDSL2

Typical Comcast gateway used for DOCSIS 3.0

Devices connected to the home network

Almost every device on a home network:

- Needs DHCP for IP address configuration
- Uses a stub resolver and needs DHCP to advertise recursive DNS servers

Of course, there will be exceptions. This talk is not about exceptions.

DHCP servers in branded gateways

ISPs appear to have locked down the options end users can configure in their branded gateways.

The ability to configure custom recursive DNS servers is conspicuously **absent** (for a DNS-OARC audience, anyway) from branded gateways!

In some cases an OEM produces both branded and unbranded versions of the same model, and this ability is **present** on unbranded devices!

DHCP servers in branded gateways

A very reasonable inference would be that large ISPs have ***specifically required*** from OEMs that their gateways ***not*** expose the ability to configure an alternative recursive DNS service in the customer accessible management interface.

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	192.168.1.254
Subnet Mask	255.255.255.0

DHCP Server

DHCP Server Enable	On ▾
DHCPv4 Start Address	192.168.1.64
DHCPv4 End Address	192.168.1.253
DHCP Lease	**Days:** 1 : **Hours:** 0 : **Minutes:** 0 : **Seconds** 0 ***e.g. 01:00:00:00***

Configure IPv6 DHCP

Configure

Broadband Source Override Auto

Base MTU 1500

e.g. 1500

IPv6 MTU 1500

e.g. 1472

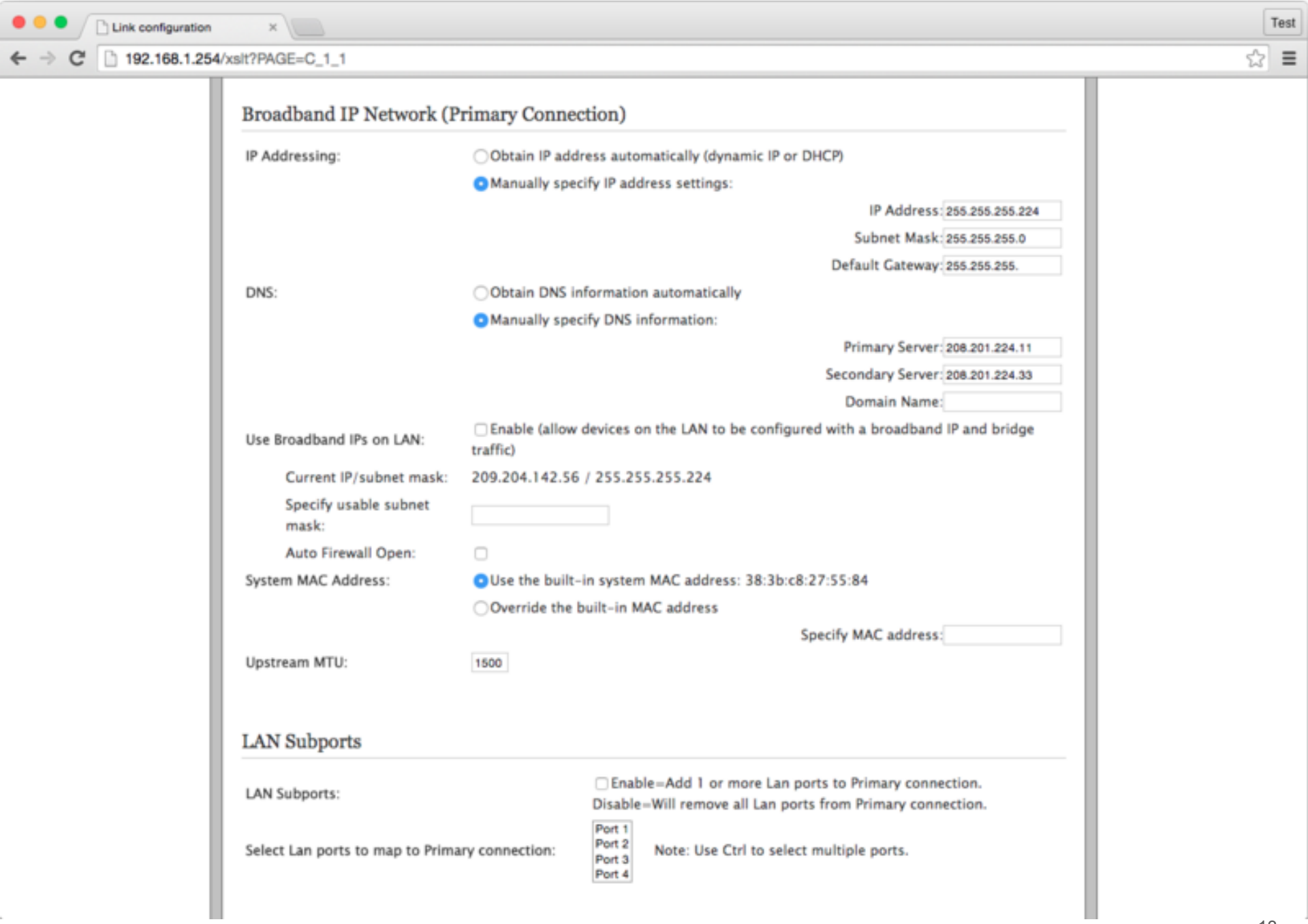
Save Cancel

Firewall Advanced

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.

Drop packets with invalid source or destination IP address	Off ▾
Protect against port scan	Off ▾
Drop packets with unknown ether types	Off ▾
Drop packets with invalid TCP flags	Off ▾
Drop incoming ICMP Echo requests to LAN	Off ▾
Drop incoming ICMP Echo requests to Device LAN Address	Off ▾
Drop incoming ICMP Echo requests to Device WAN Address	Off ▾
Suppress ICMP error responses	Off ▾
Flood Limit	Off ▾
Flood rate limit	4 *e.g. 4*
Flood burst limit	8 *e.g. 8*
Flood limit ICMP enable	On ▾
Flood limit UDP enable	On ▾
Flood limit TCP enable	On ▾
Flood limit TCP SYN-cookie	On ▾
Neighbor Discovery Attack protection	Off ▾
ESP Header Forwarding	On ▾
Authentication Header Forwarding	On ▾
Reflexive ACL	Off ▾
ESP ALG	Off ▾
SIP ALG	Off ▾

Save Cancel Restore Defaults


Link configuration
Test
192.168.1.254/xslt?PAGE=C_1_1
Broadband IP Network (Primary Connection)
IP Addressing:
Obtain IP address automatically (dynamic IP or DHCP)
Manually specify IP address settings:
IP Address: 255.255.255.224
Subnet Mask: 255.255.255.0
Default Gateway: 255.255.255.
DNS:
Obtain DNS information automatically
Manually specify DNS information:
Primary Server: 208.201.224.11
Secondary Server: 208.201.224.33
Domain Name:
Use Broadband IPs on LAN:
Enable (allow devices on the LAN to be configured with a broadband IP and bridge traffic)
Current IP/subnet mask: 209.204.142.56 / 255.255.255.224
Specify usable subnet mask:
Auto Firewall Open:
System MAC Address:
Use the built-in system MAC address: 38:3b:c8:27:55:84
Override the built-in MAC address
Specify MAC address:
Upstream MTU: 1500
LAN Subports
LAN Subports:
Enable=Add 1 or more Lan ports to Primary connection.
Disable=Will remove all Lan ports from Primary connection.
Select Lan ports to map to Primary connection:
Port 1
Port 2
Port 3
Port 4
Note: Use Ctrl to select multiple ports.

Special Case: AT&T U-Verse

Alexander Harrison
Updated 6 months ago

Follow

Unfortunately, due to the firmware restrictions that AT&T has placed upon UVERSE-enabled devices, it is not possible to change the DNS settings on these devices. This is a limitation due to ATT and unfortunately cannot be changed.

If you would like to use our services on a UVERSE-enabled connection then please configure your computers individually or configure a router that connects your UVERSE device and computers.

EG Connection Expert

11-22-2017 10:23 AM

Re: Quad 9 DNS service

The default DNS servers cannot be changed in the Comcast supplied gateway devices. They act as DNS forwarders / proxies. The DNS needs to be configured / changed in the individual network clients.

I am not a Comcast employee, I am a paying customer just like you!

I am an XFINITY Forum Expert and I am here to help. For information on the program click here.

We ask that you post publicly so people with similar questions may benefit from the conversation.

Was your question answered? Mark it as an accepted solution!

0 Kudos

15

Reply

Workarounds

Yes, there are workarounds, such as:

- Replacing the device entirely, if possible
- Placing a better device behind the ISP-supplied device

These require time and money and may result in a technically inferior solution (e.g., double NAT). Only motivated, technically adept customers will pursue workarounds.

End results

The vast majority of customers are unaware of DNS and the existence of alternative recursive DNS services.

A small group of customers aware of alternative recursive DNS servers but unable to perform workarounds are prevented from choosing an alternative service.

A tiny group of customers capable of and willing to perform workarounds are able to choose an alternative service.

Questions

Is this good/bad/…?

Why are (large) ISPs doing this?

Is there a legitimate customer support or security reason to prevent customers from choosing an alternative recursive DNS service?

If so, is there an alternative that accomplishes these goals while still allowing customers to choose alternatives?

Thanks!