

Questions, Issues,
Concerns, Suggestions
Welcome at any time
Even Now

Sun City Computer Club

Windows SIG

February 27, 2018

- Safer not Safe
- E-postcard not e-mail
- ADMINISTRATOR
- Passphrases not passwords
- Radio not wireless

Vocabulary



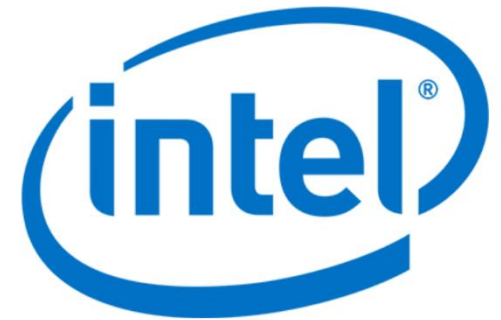


Urgent Microsoft Windows update

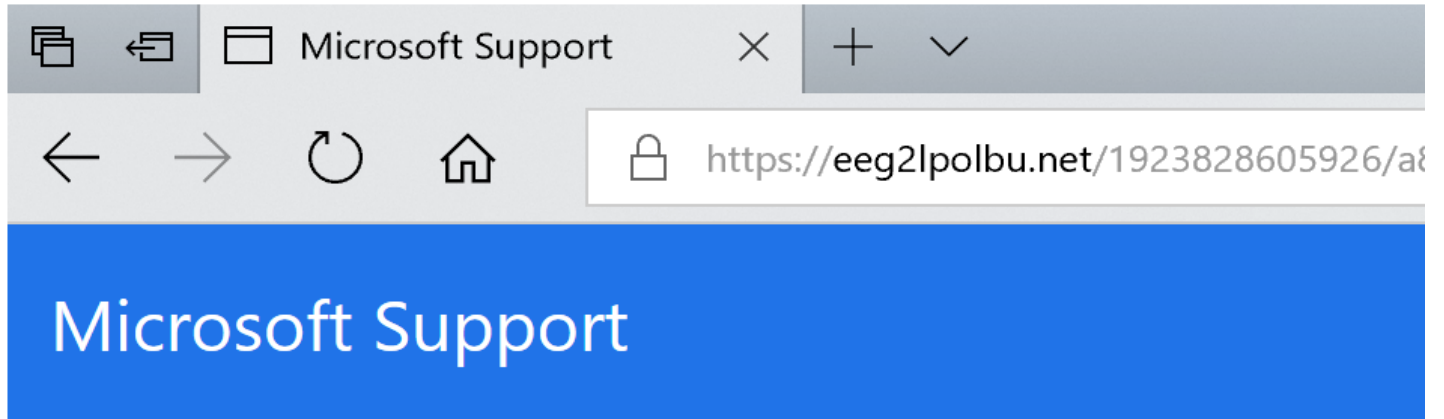
Download Now



Microsoft

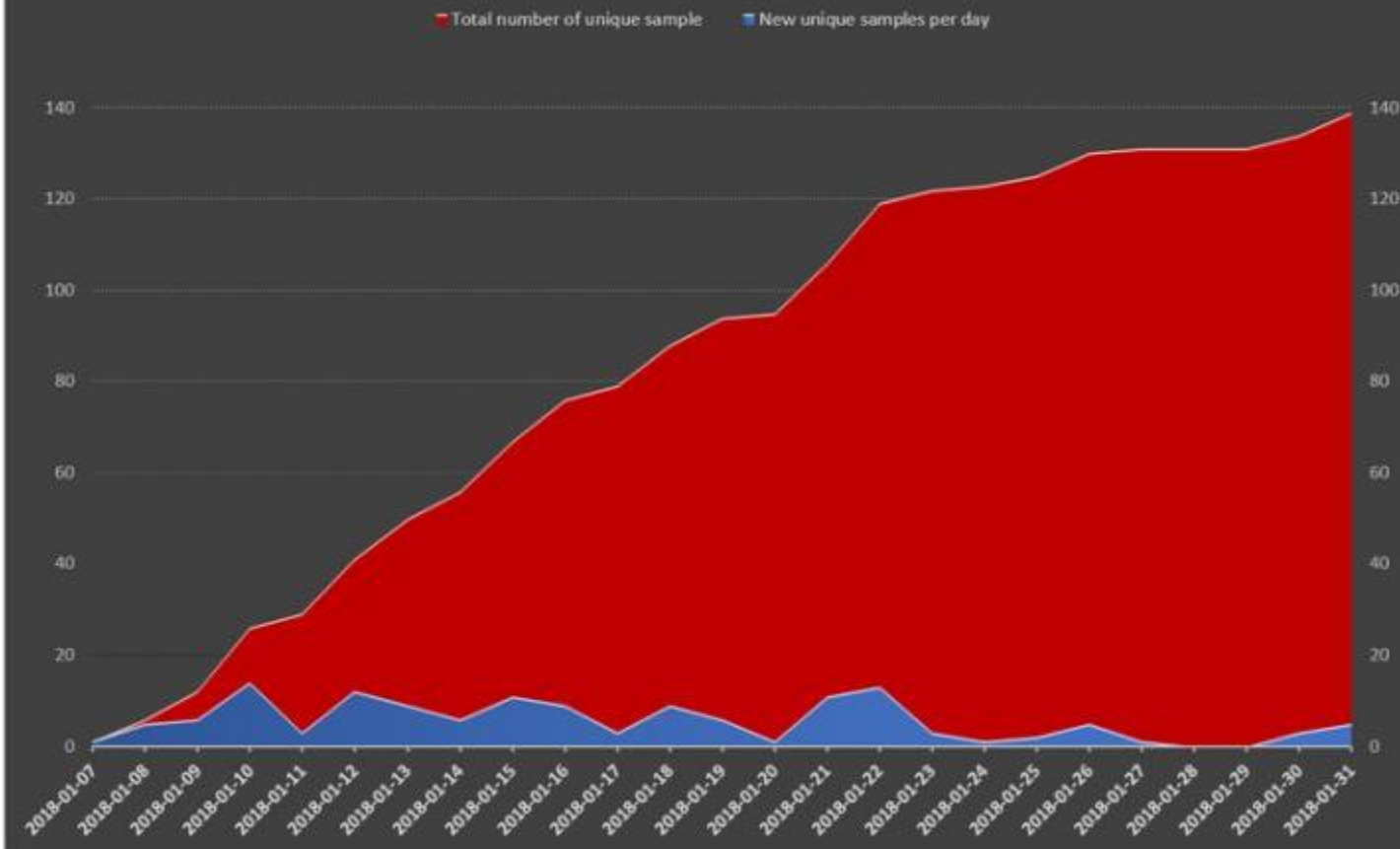


Microsoft 2018



Urgent M

Number of Spectre/Meltdown-related Samples in AV-TEST's Database



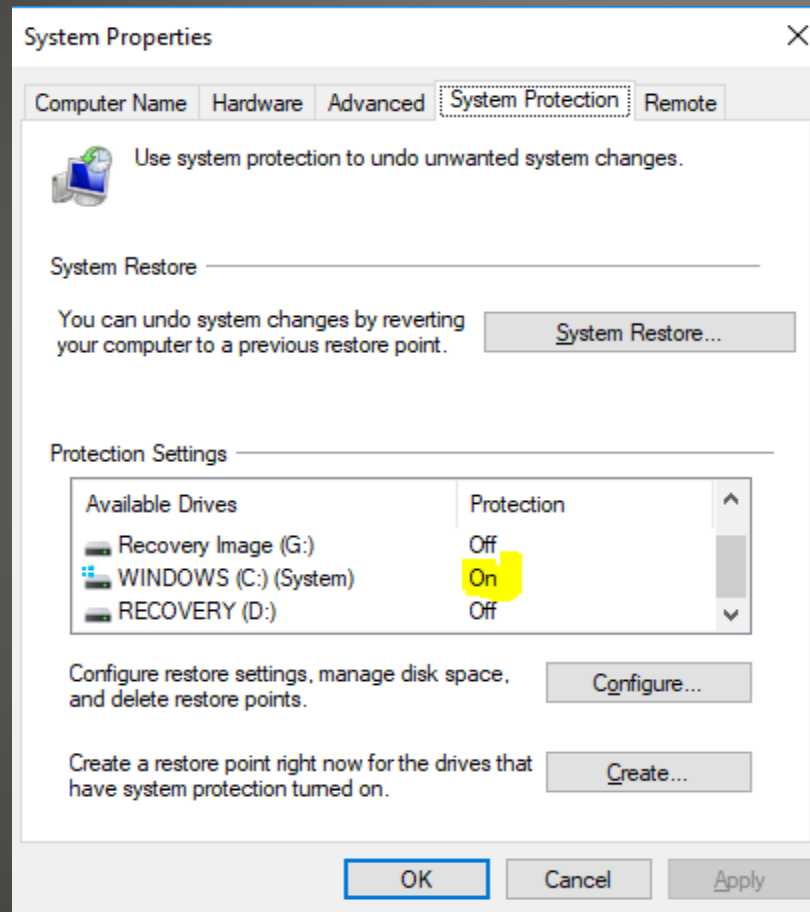
- 15 Windows patches instances January
Not 15 patches 15 Patch instances
Patches to patches, revoke patches,
Windows 7 SP1 patch,
- My experience
Cheap monitors (60 Hz refresh)
Surface detachable keyboard
USB internal HUB
Measurable performance decrease
- Your experience?

Current Topics

- Restore point
- Security suite(s)
- Machine BIOS, firmware, microcode
- Browser updates
 - Strict Site Isolation
- Edge getting pushy?
 - Settings>Personalization>Lock Screen
- Skype

Windows Associated

- Got protection?



Restore point

- <http://sctxwindows.com/>



Notes from previous sessions

- Name resolution

Own name, Hosts file, NetBIOS, DNS

C:**Windows**\System32\drivers\etc**hosts file**

- Domain Name System

Distributed, hierarchical, caching database

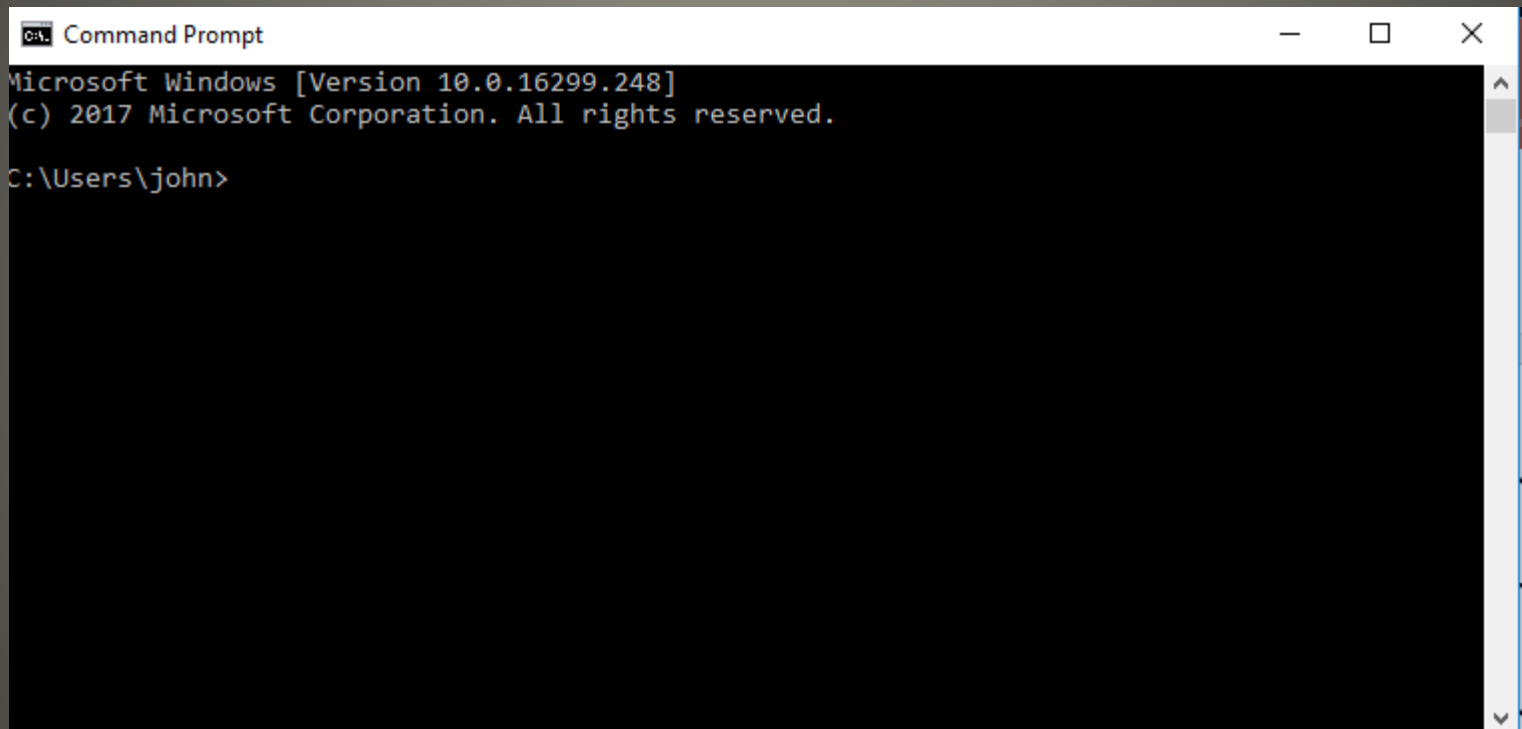
No authentication

- BGP

routing, No authentication

Journey to the Web site

- CMD in Windows Search Box

A screenshot of the Windows Command Prompt window. The title bar reads "Command Prompt". The window content shows the following text: "Microsoft Windows [Version 10.0.16299.248]" followed by "(c) 2017 Microsoft Corporation. All rights reserved." and the command prompt "C:\Users\john>". The window has standard Windows window controls (minimize, maximize, close) in the top right corner.

```
CA: Command Prompt
Microsoft Windows [Version 10.0.16299.248]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\john>
```

Command Prompt Window (Windows)

nslookup

- C:\Users\john>nslookup
161.170.244.20
- Server: Nonya
- Address: 192.168.1.1

- Name: www-origin.walmart.com
- Address: 161.170.244.20

hosts file

```
# Copyright (c) 1993-2009 Microsoft Corp.  
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.  
# This file contains the mappings of IP addresses to host names. Each  
# entry should be kept on an individual line. The IP address should  
# be placed in the first column followed by the corresponding host name  
161.170.244.20    Walmart.com
```

```
C:\Users\john>nslookup walmart.com  
Server: Nonya  
Address: 192.168.1.1
```

```
Non-authoritative answer:  
Name:    walmart.com  
Addresses: 161.170.248.20  
          161.170.244.20  
127.0.0.1    playboy.com
```

Command Prompt

```
C:\Users\john>nslookup nyt.com
```

```
Server:  ppoli
```

```
Address: 192.168.1.1
```

```
Non-authoritative answer:
```

```
Name:    nyt.com
```

```
Addresses: 151.101.193.164
```

```
           151.101.129.164
```

```
           151.101.65.164
```

```
           151.101.1.164
```

```
C:\Users\john>netstat -an | find ":443" | find "151.101."
```

```
TCP    192.168.1.170:63949    151.101.1.164:443      ESTABLISHED
```

```
TCP    192.168.1.170:63951    151.101.5.164:443      ESTABLISHED
```

```
TCP    192.168.1.170:63994    151.101.5.7:443        ESTABLISHED
```

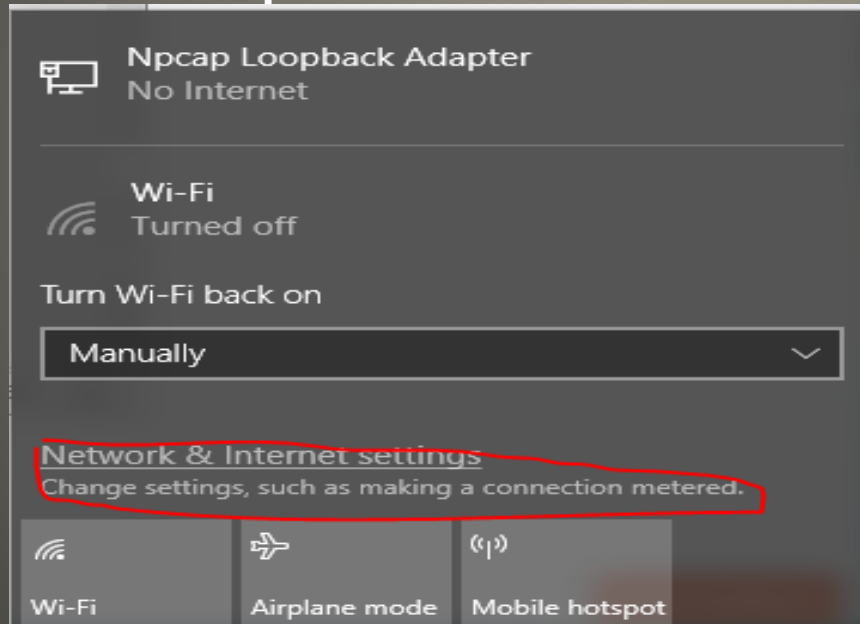
```
C:\Users\john>
```

Check an Open WEB site

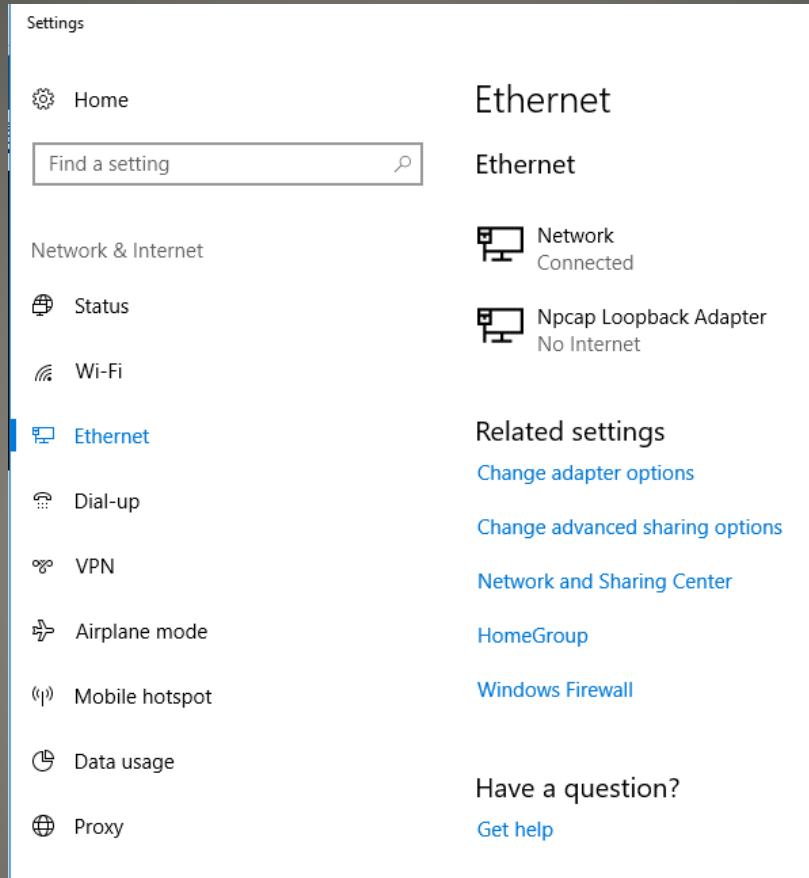
DNS Dynamic Name Service

- Easily fooled
- Cache poisoning
- Uses DNS server specified by client
- Domain squatting
- Akamai

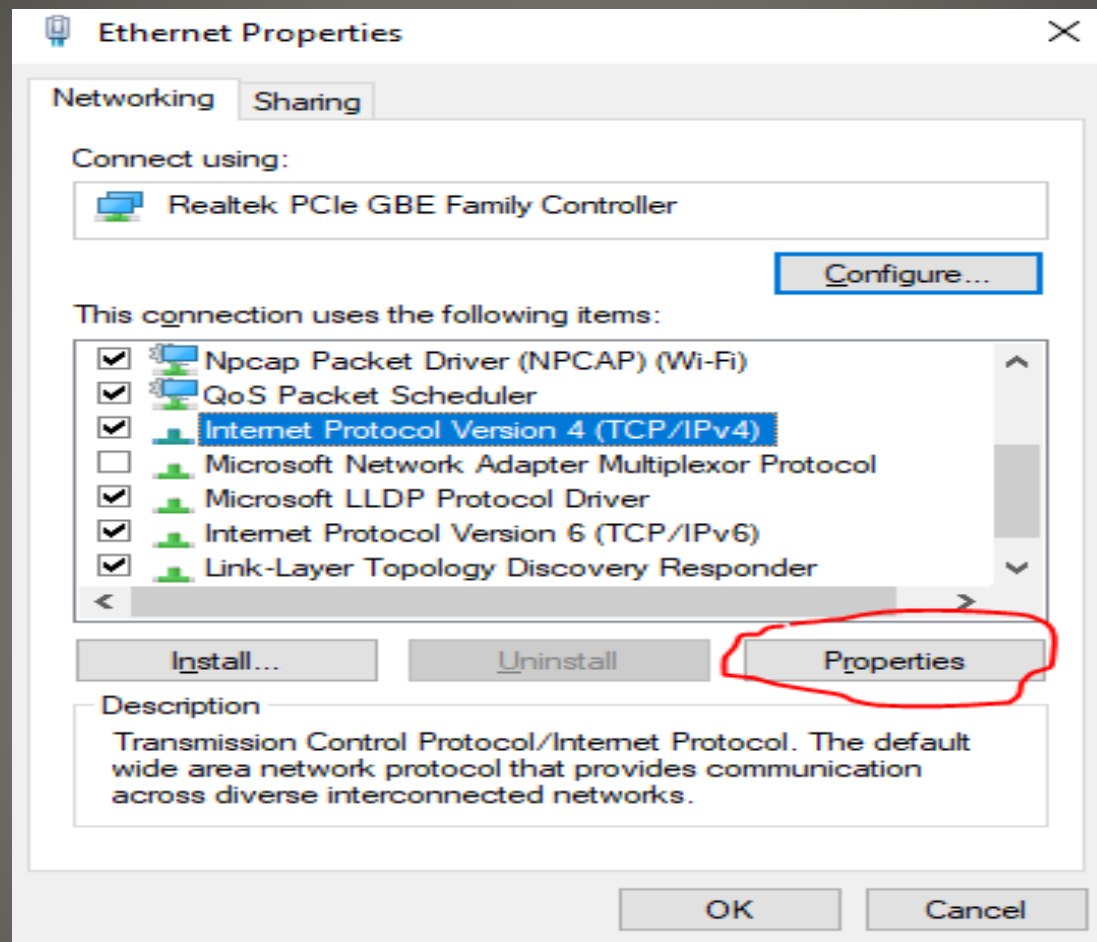
- Global Cyber Alliance
Better Performance
Less tracking
Some protections



Quad 9s



Ethernet or WiFi



Adapter settings IPv4 Properties

Internet Protocol Version 4 (TCP/IPv4) Properties

General Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☒ Obtain an IP address automatically

☐ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

☐ Validate settings upon exit

Advanced...

OK Cancel

Advanced TCP/IP Settings

IP Settings DNS WINS

DNS server addresses, in order of use:

↑

↓

Add... Edit... Remove

The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:

☒ Append primary and connection specific DNS suffixes

☒ Append parent suffixes of the primary DNS suffix

☐ Append these DNS suffixes (in order):

↑

↓

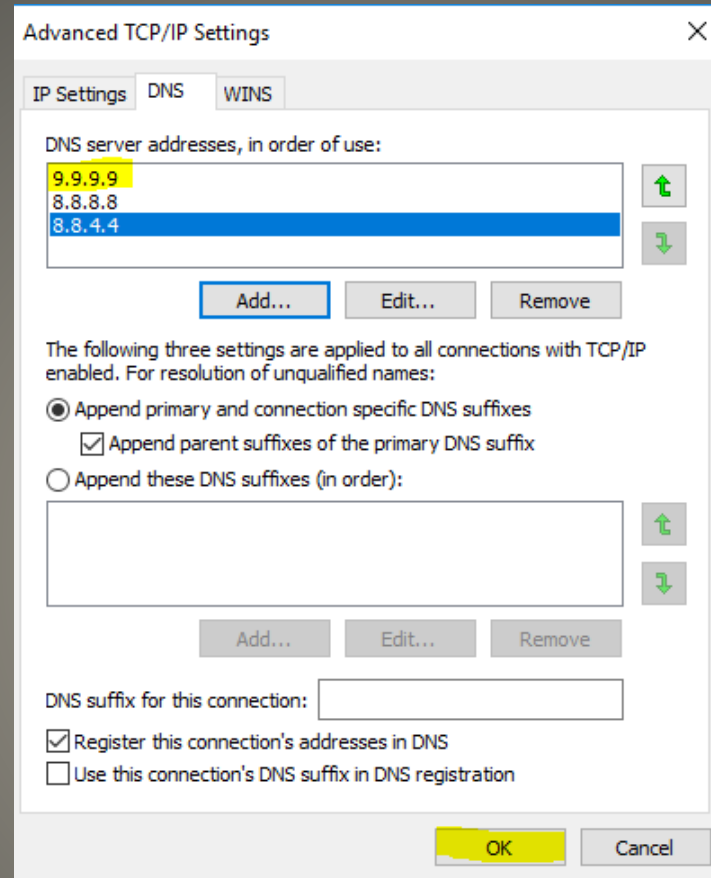
Add... Edit... Remove

DNS suffix for this connection:

☒ Register this connection's addresses in DNS

☐ Use this connection's DNS suffix in DNS registration

OK Cancel



Reboot/restart for full effect

• Questions, suggestions, comments?

- Chicken Little
- Tortoise and hare
- Each of us safer, all of us safer

- Vlan separation Guest access WEB
- Firewall UPnP
- Bandwidth
- Data Cap
- Proprietary
- Voice commands
- Heat Power
- Firmware
- Updates
- Update Security

Cutting the Cord