IP range blocks training

Martin Rulsch
martin.rulsch@wikipedia.de

plwiki peer support for administrators
31 January

Martin Rulsch

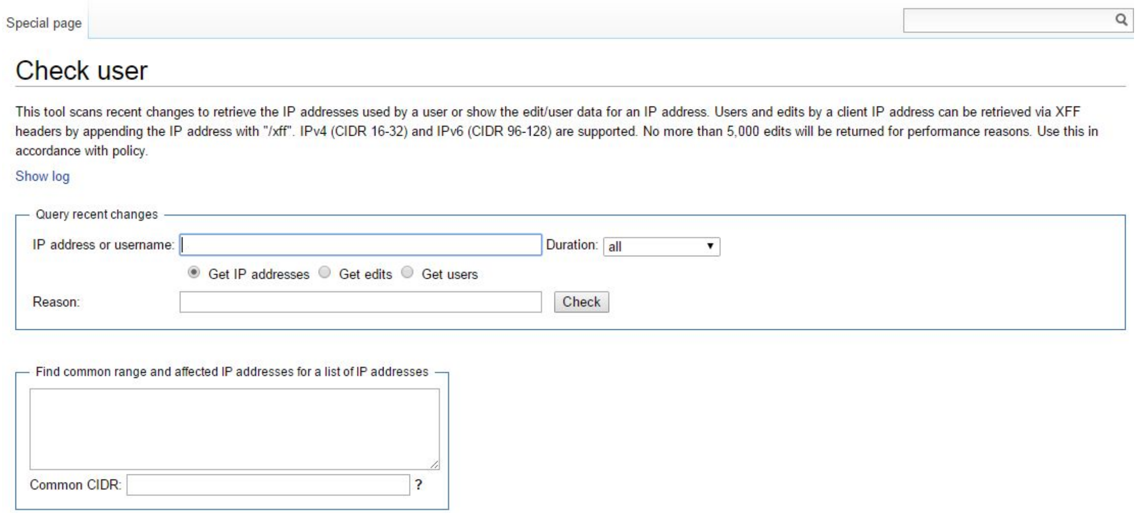
- active in Wikimedia projects since 2005
- photographer, admin, author, organizer, mentor, software developer and lecturer
- Wikimedia Steward since 2007
- Wikimedia Deutschland: board 2011–13, employee since 2015
- Classical philologist (M.A. 2014)

License: Sandro Halank (WMDE), 2019-09-04 Martin Rulsch by Sandro Halank (WMDE), crop by Martin Rulsch, CC BY-SA 4.0

Context

Context within Wikimedia projects

- simple vandalism, be it local or global, is often caused by IP addresses which can be seen in diffs, history, talk pages, etc. – handled by either admins or stewards
- trolling, sock puppetry, manipulations are often caused by registered users
- the IP address is logged in the background for every action of a registered account
- under some conditions, local checkusers have the right to investigate the underlying IP addresses



Special page

Check user

This tool scans recent changes to retrieve the IP addresses used by a user or show the edit/user data for an IP address. Users and edits by a client IP address can be retrieved via XFF headers by appending the IP address with "/xff". IPv4 (CIDR 16-32) and IPv6 (CIDR 96-128) are supported. No more than 5,000 edits will be returned for performance reasons. Use this in accordance with policy.

Show log

Query recent changes

IP address or username: Duration: all

● Get IP addresses ○ Get edits ○ Get users

Reason: Check

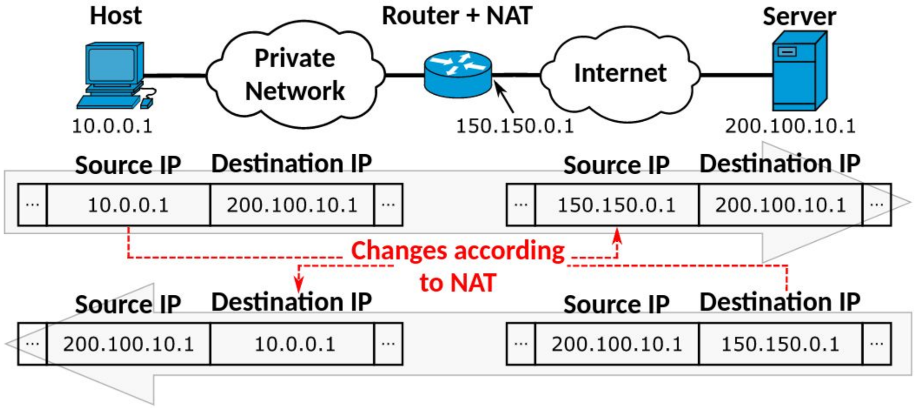
Find common range and affected IP addresses for a list of IP addresses

Common CIDR: ?

License: Los Vegas, Tool of CheckUser, CC BY-SA 3.0

IP address in general

- numerical label such as 192.0.2.1 that is connected to a computer network that uses the Internet Protocol for communication (individual users, websites, etc.)
- 2 main functions: network interface identification, location addressing
- IP address space is managed by Internet service providers (ISPs)



License: Michel Bakni, NAT Concept-en, CC BY-SA 4.0

IP types: standard

- static IP address: permanent number for one network section (government, school, university, office, individual, ...); several static IP addresses can create one entity within one range (e.g., several IPs for one ministry)
- dynamic IP address: selection range of numbers within a network section which changes randomly, when resetting the router, etc. (mostly individuals) – gets reassigned to the next customer

IP types: modulation

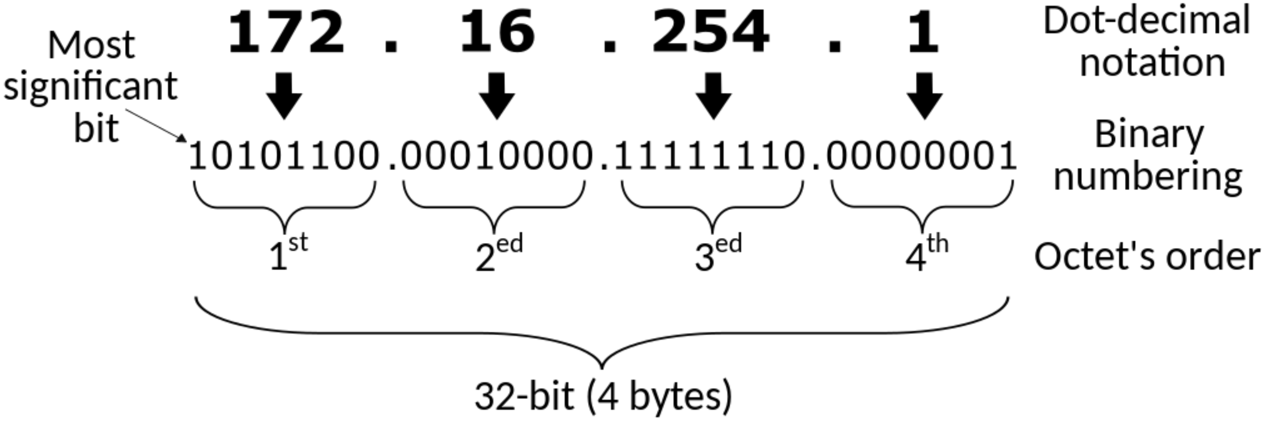
- instead of using the IP address which is connected to your computer, it is possible to use a middleman system in between
  - for the good: getting access to tools which are connected to your work computer, hiding from surveillance, data protection, etc.
  - for the worse: doing illegal things, etc.
- sometimes in use without own knowledge: Apple iCloud, Opera in private mode, AOL, etc. – providers often knows the original address
- different types like open proxy, Virtual Private Network, Tor, etc.
- the use is forbidden by global policy m:NOP

Read more (English)

- Diff blog post about open proxies

IPv4

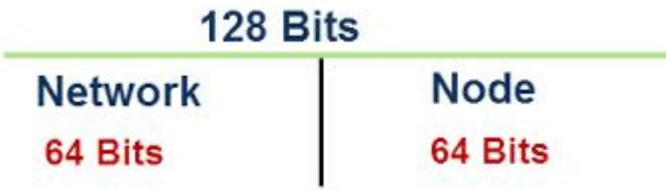
- numerical composed of **4** segments, divided by a dot
- each segment is composed of octets which can either be 0 or 1 = **8 bit** (= 2^8 variations possible = 256) → decimal notation 0–255
- 4 bytes



License: Michel Bakni, IPv4 address structure and writing systems-en, CC BY-SA 4.0

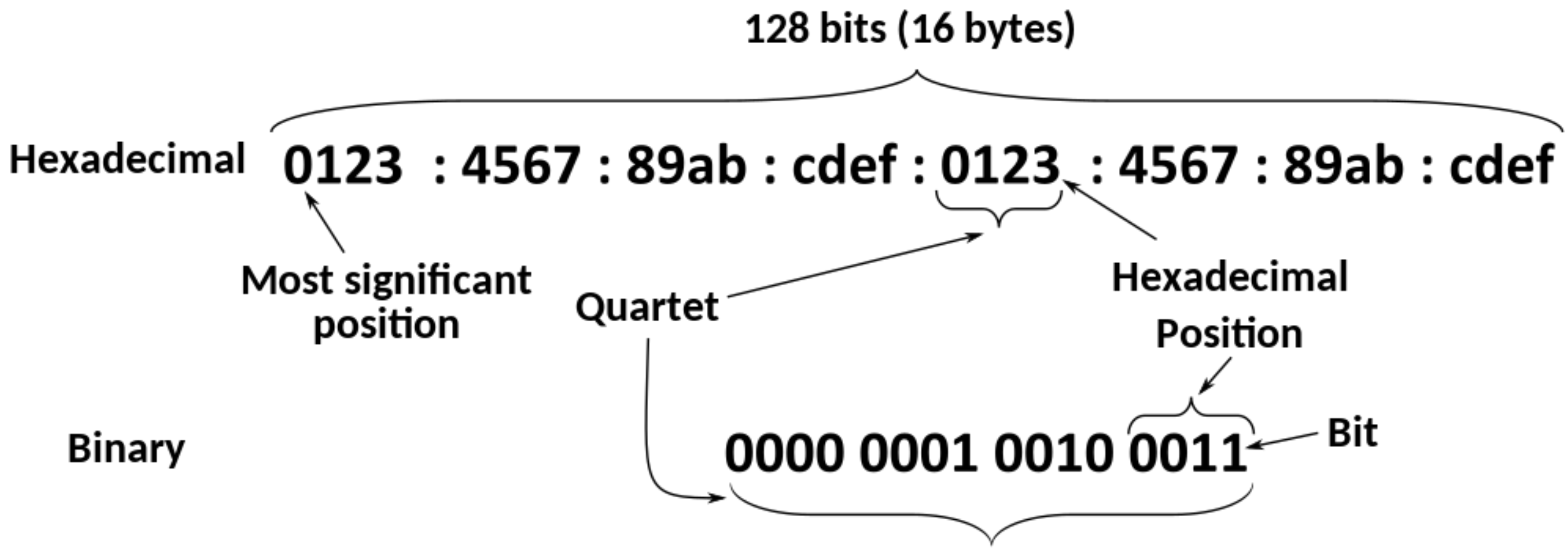
IPv6

- number of possible IP v4 is limited: $2^{31} – 1$ = 2 147 483 647
- numerical composed of **8** segments, divided by a dot
- each segment is composed of hexadecimalets which can either be 0 or 1 = **16 bit** (= 2^{16} variations possible = 65 536) → decimal notation 0–65 535 = hexadecimal 0–ffff; starting 0 can be omitted
- 128 bit = 3.4×10^{38} total addresses
  - ⇒ more static IP addresses possible → less data protection because everybody is unique ⇒ more use of modulations
  - easier composition of the address



IPv6 Address Network and Node

IPv6



License: Michel Bakni, IPv6 address terminology-en, CC BY-SA 4.0

⇒ consequences: due to the almost unlimited number of IP addresses, the ranges for individuals can be much higher → more difficult

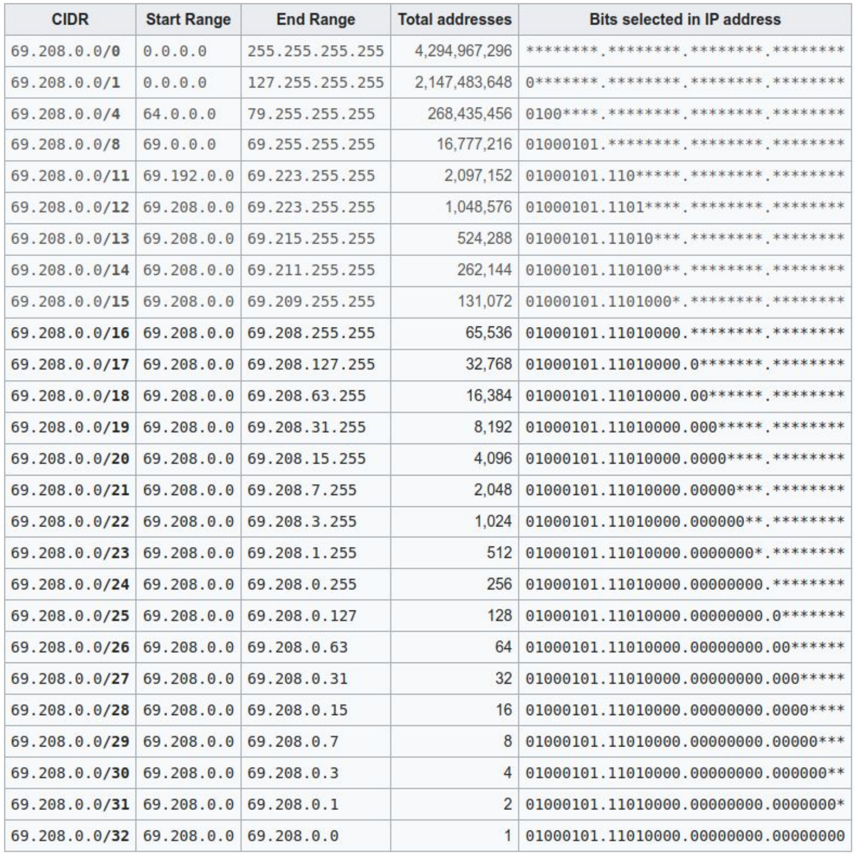
What is an IP range?

- dynamic IP addresses are not randomly assigned
- the provider hands out an IP address from within a range which they have got for that region, bureau complex, etc.
- the ranges are different for IPv4 and IPv6 because of the different size, notation and composition of the number
- a range is noted with a slash / and a decimal number for the amount of bits which are stable (≠ dynamic)
- blocking an IP range can cause serious damage to innocent people in the same range, please check their contributions and help local users with IP block exemptions if need be

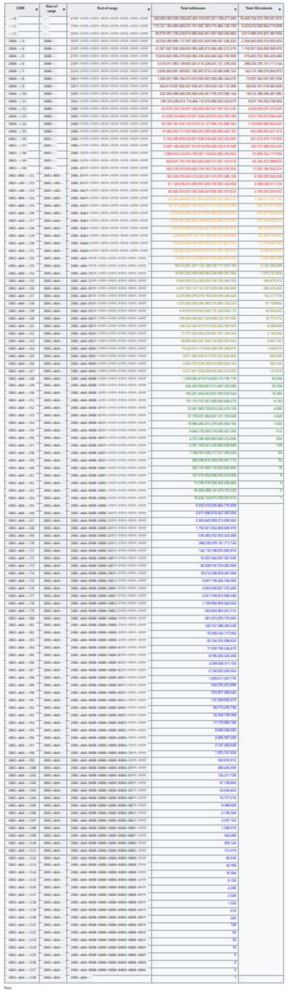
Range calculation

IP ranges in Wikimedia projects

- it’s all complicated
- IPv6 makes it even more complicated with hexadecimals, longer numbers, etc.
- it is possible to calculate it manually but that won’t be explained here



CIDR	Start Range	End Range	Total addresses	Bits selected in IP address
69.208.0.0/0	0.0.0.0	255.255.255.255	4,294,967,296	********.********.********.********
69.208.0.0/1	0.0.0.0	127.255.255.255	2,147,483,648	0*******.********.********.********
69.208.0.0/4	64.0.0.0	79.255.255.255	268,435,456	0100****.********.********.********
69.208.0.0/8	69.0.0.0	69.255.255.255	16,777,216	01000101.********.********.********
69.208.0.0/11	69.192.0.0	69.223.255.255	2,097,152	01000101.110*****.********.********
69.208.0.0/12	69.208.0.0	69.223.255.255	1,048,576	01000101.1101****.********.********
69.208.0.0/13	69.208.0.0	69.215.255.255	524,288	01000101.11010***.********.********
69.208.0.0/14	69.208.0.0	69.211.255.255	262,144	01000101.110100**.********.********
69.208.0.0/15	69.208.0.0	69.209.255.255	131,072	01000101.1101000*.********.********
69.208.0.0/16	69.208.0.0	69.208.255.255	65,536	01000101.11010000.********.********
69.208.0.0/17	69.208.0.0	69.208.127.255	32,768	01000101.11010000.0*******.********
69.208.0.0/18	69.208.0.0	69.208.63.255	16,384	01000101.11010000.00******.********
69.208.0.0/19	69.208.0.0	69.208.31.255	8,192	01000101.11010000.000*****.********
69.208.0.0/20	69.208.0.0	69.208.15.255	4,096	01000101.11010000.0000****.********
69.208.0.0/21	69.208.0.0	69.208.7.255	2,048	01000101.11010000.00000***.********
69.208.0.0/22	69.208.0.0	69.208.3.255	1,024	01000101.11010000.000000**.********
69.208.0.0/23	69.208.0.0	69.208.1.255	512	01000101.11010000.0000000*.********
69.208.0.0/24	69.208.0.0	69.208.0.255	256	01000101.11010000.00000000.********
69.208.0.0/25	69.208.0.0	69.208.0.127	128	01000101.11010000.00000000.0*******
69.208.0.0/26	69.208.0.0	69.208.0.63	64	01000101.11010000.00000000.00******
69.208.0.0/27	69.208.0.0	69.208.0.31	32	01000101.11010000.00000000.000*****
69.208.0.0/28	69.208.0.0	69.208.0.15	16	01000101.11010000.00000000.0000****
69.208.0.0/29	69.208.0.0	69.208.0.7	8	01000101.11010000.00000000.00000***
69.208.0.0/30	69.208.0.0	69.208.0.3	4	01000101.11010000.00000000.000000**
69.208.0.0/31	69.208.0.0	69.208.0.1	2	01000101.11010000.00000000.0000000*
69.208.0.0/32	69.208.0.0	69.208.0.0	1	01000101.11010000.00000000.00000000



Basic knowledge I

- basic knowledge for interpreting the results from the tools
- if you have more than one IP address at hand, check only the parts of the IP if they are the same
  - IPv4: first two of the four segments, **87.174**.128.0
  - IPv6: first three of the eight segments, **2003:C1:23C0:**0:0:0:0:0 (this can also be abbreviated to 2003:C1:23C0::)
- if not the same, they are likely from two different networks and you don’t need to open a tool
- sometimes a person gets dynamic IPs from two different networks from their provider, then you have to check both

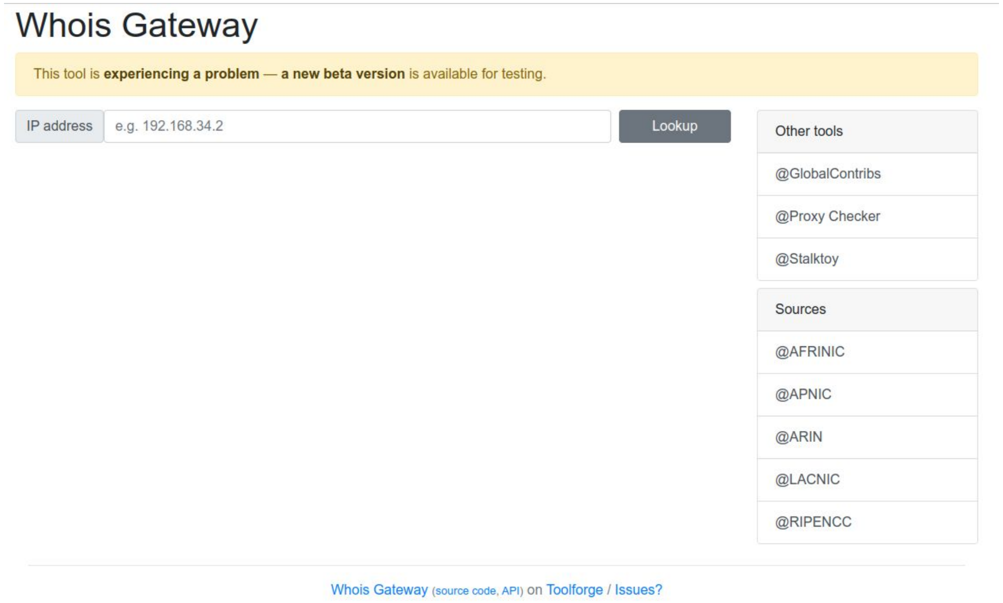
Basic knowledge II

- regular ranges on Wikimedia projects are:
  - IPv4: /32 up to /16
  - IPv6: /128 up to /19
- admins can only block these IP ranges, not larger ones → if you have larger ranges like IPv4 with /15, you have to split them into smaller parts (not easy, ask an expert! or go “trial and error” in the tools)
- IPv6 /64 equals one individual access which allows dynamic change , see also this help page

Tools

Whois

- one of the countless tools for checking the backgrounds behind an IP address – this one is hosted on Toolforge: https://whois.toolforge.org/ (without geolocation)
- often, such tools are linked at the bottom of Special:Contributions



Whois Gateway

This tool is **experiencing a problem** — **a new beta version** is available for testing.

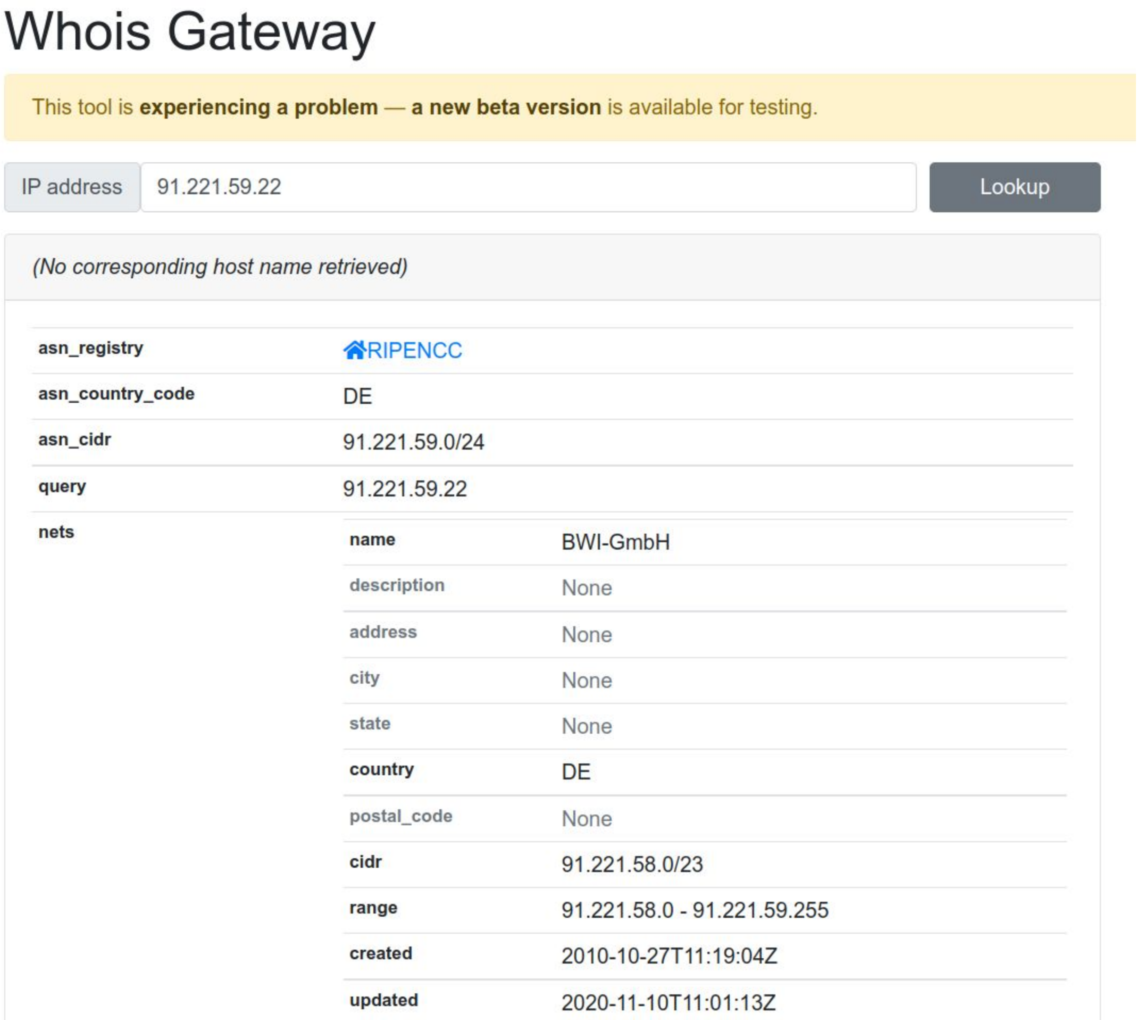
IP address | e.g. 192.168.34.2 | Lookup

Other tools
- @GlobalContribs
- @Proxy Checker
- @Stalktoy

Sources
- @AFRINIC
- @APNIC
- @ARIN
- @LACNIC
- @RIPENCC

Whois Gateway (source code, API) on Toolforge / Issues?

Whois



Whois Gateway

This tool is **experiencing a problem** — **a new beta version** is available for testing.

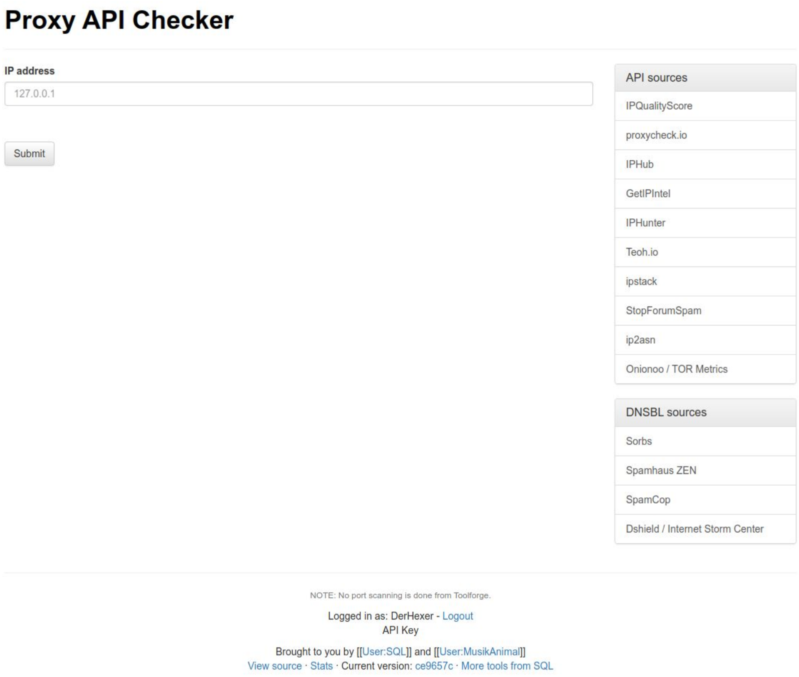
IP address: 91.221.59.22

(No corresponding host name retrieved)

asn_registry	🏠RIPENCC	
asn_country_code	DE	
asn_cidr	91.221.59.0/24	
query	91.221.59.22	
nets	**name**	BWI-GmbH
	description	None
	address	None
	city	None
	state	None
	country	DE
	postal_code	None
	cidr	91.221.58.0/23
	range	91.221.58.0 - 91.221.59.255
	created	2010-10-27T11:19:04Z
	updated	2020-11-10T11:01:13Z

IP proxy check

- in case you have to check if an IP address is an open proxy, you can use a tool like Proxy API Checker on Toolforge: https://ipcheck.toolforge.org/ (only available to active community members through OAuth)
- results can be confusing – check with the countless other tools or search for the IP address itself whether it's on abuse lists
- more or less only these open ports can be abused when surfing: 80, 8080, 3126, 3127
- if in doubt, ask an expert



Proxy API Checker

IP address

127.0.0.1

API sources

IPQualityScore

proxycheck.io

IPHub

GetIPIntel

IPHunter

Teoh.io

ipstack

StopForumSpam

ip2asn

Onionoo / TOR Metrics

DNSBL sources

Sorbs

Spamhaus ZEN

SpamCop

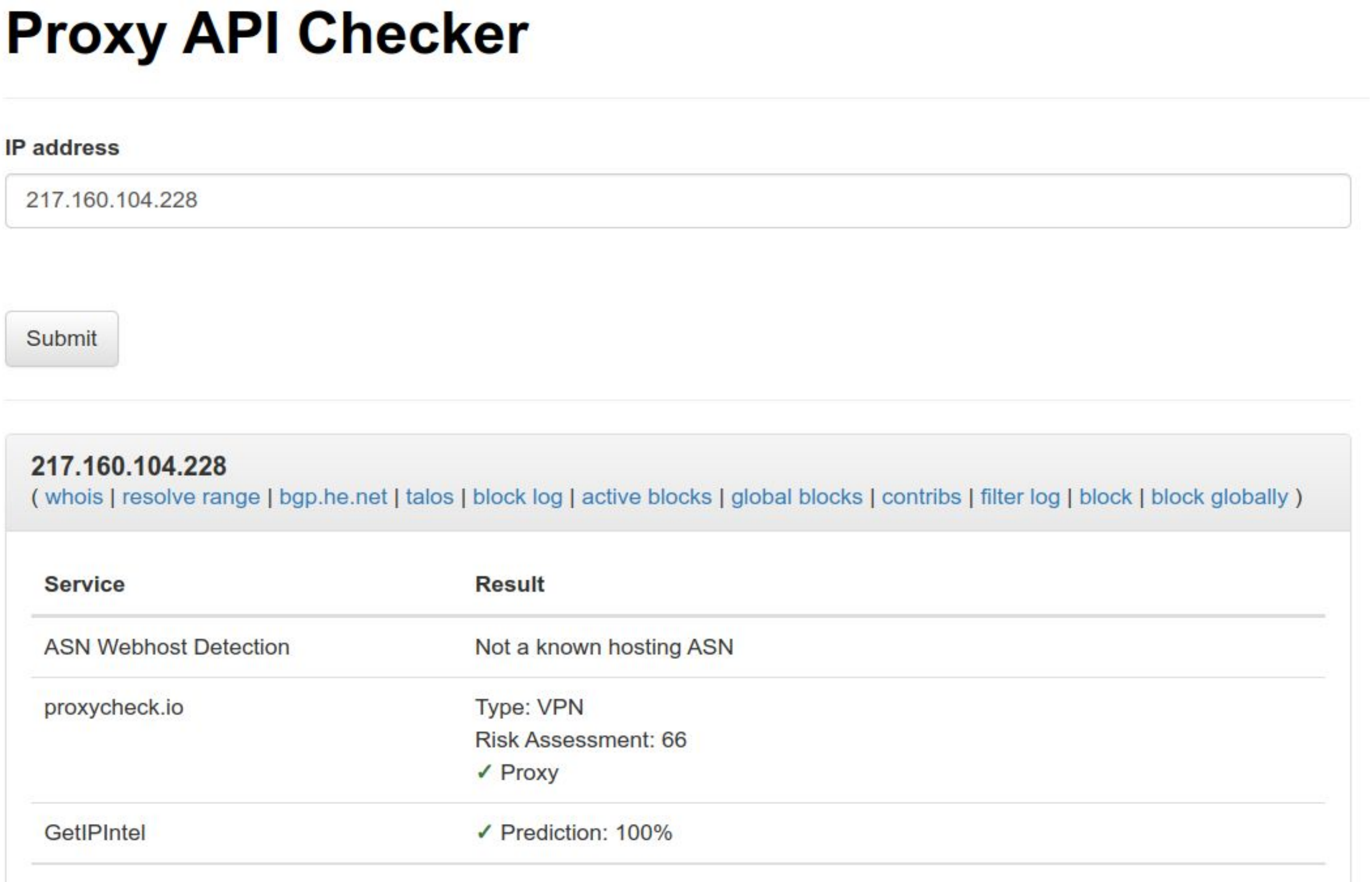
Dshield / Internet Storm Center

NOTE: No port scanning is done from Toolforge.

Logged in as: DerHexer - Logout
API Key

Brought to you by [[User:SQL]] and [[User:MusikAnimal]]
View source · Stats · Current version: ce9657c · More tools from SQL

IP proxy check



Proxy API Checker

IP address

217.160.104.228

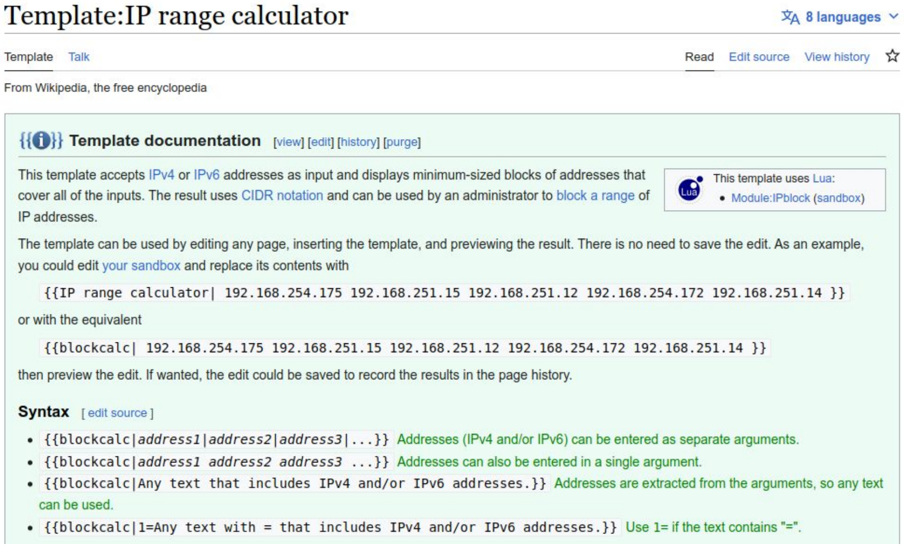
217.160.104.228

(whois | resolve range | bgp.he.net | talos | block log | active blocks | global blocks | contribs | filter log | block | block globally)

Service	Result
ASN Webhost Detection	Not a known hosting ASN
proxycheck.io	Type: VPN Risk Assessment: 66 ✓ Proxy
GetIPIntel	✓ Prediction: 100%

Template

- some larger Wikipedias have templates which automatically calculate ranges when multiple IP addresses are entered
- English Wikipedia has [Template:IP range calculator]() which could be copied and adjusted to other wikis
- due to its subnet function, it can help you find smaller ranges to block (= less damage)



Template:IP range calculator

From Wikipedia, the free encyclopedia

Template documentation [view] [edit] [history] [purge]

This template uses Lua:
- Module:IPblock (sandbox)

This template accepts IPv4 or IPv6 addresses as input and displays minimum-sized blocks of addresses that cover all of the inputs. The result uses CIDR notation and can be used by an administrator to block a range of IP addresses.

The template can be used by editing any page, inserting the template, and previewing the result. There is no need to save the edit. As an example, you could edit your sandbox and replace its contents with

```
{{IP range calculator| 192.168.254.175 192.168.251.15 192.168.251.12 192.168.254.172 192.168.251.14 }}
```

or with the equivalent

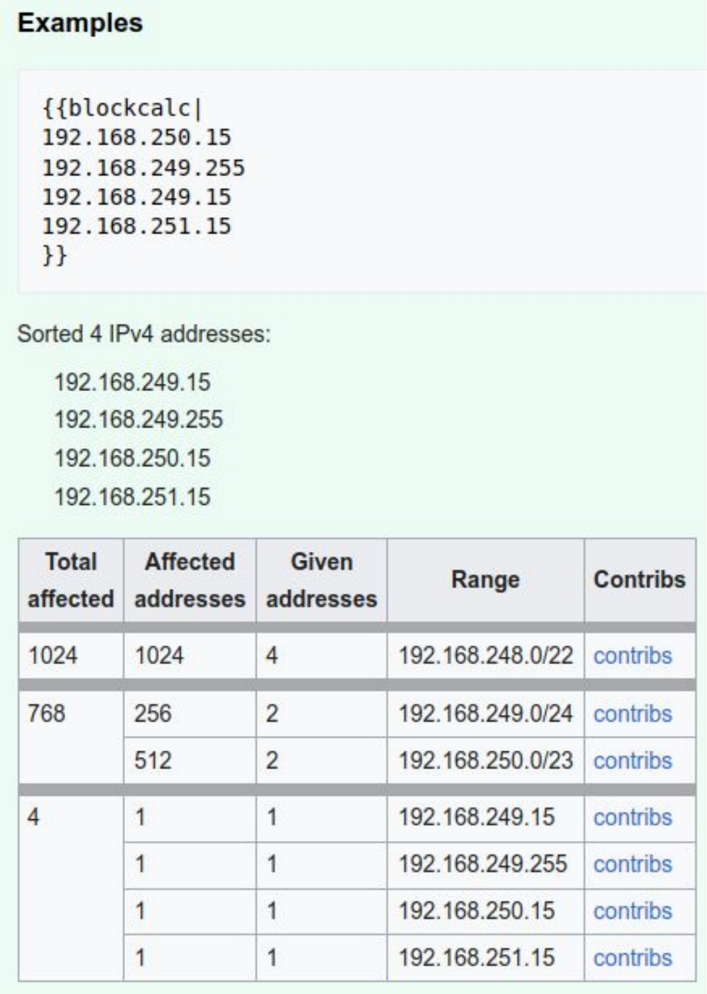
```
{{blockcalc| 192.168.254.175 192.168.251.15 192.168.251.12 192.168.254.172 192.168.251.14 }}
```

then preview the edit. If wanted, the edit could be saved to record the results in the page history.

Syntax [edit source]

- `{{blockcalc|address1|address2|address3|...}}` Addresses (IPv4 and/or IPv6) can be entered as separate arguments.
- `{{blockcalc|address1 address2 address3 ...}}` Addresses can also be entered in a single argument.
- `{{blockcalc|Any text that includes IPv4 and/or IPv6 addresses.}}` Addresses are extracted from the arguments, so any text can be used.
- `{{blockcalc|1=Any text with = that includes IPv4 and/or IPv6 addresses.}}` Use 1= if the text contains "=".

Template



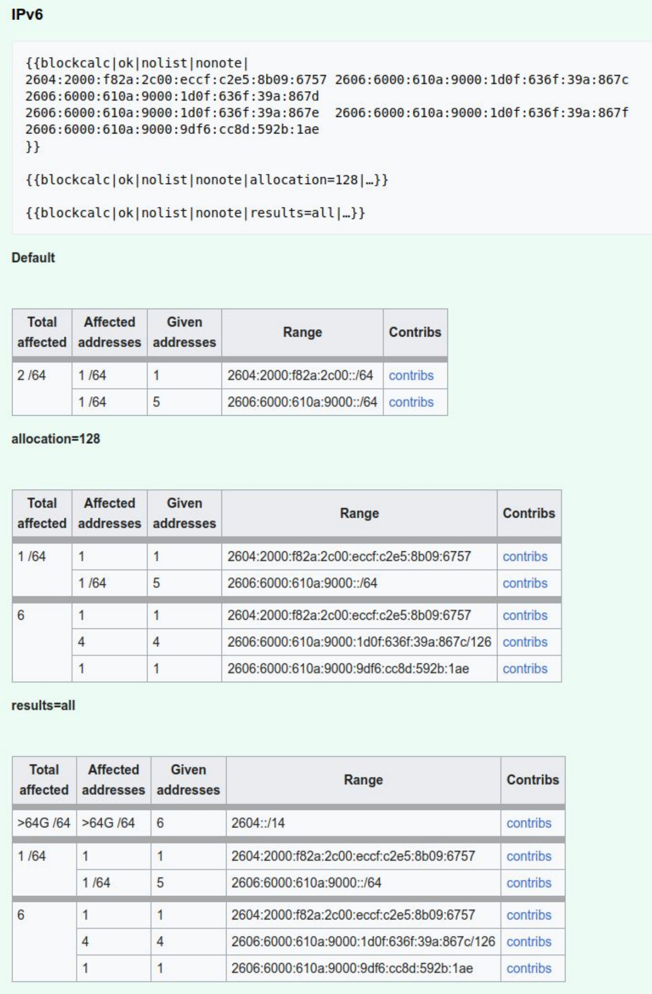
Examples

```
{{blockcalc|
192.168.250.15
192.168.249.255
192.168.249.15
192.168.251.15
}}
```

Sorted 4 IPv4 addresses:

192.168.249.15
192.168.249.255
192.168.250.15
192.168.251.15

Total affected	Affected addresses	Given addresses	Range	Contribs
1024	1024	4	192.168.248.0/22	contribs
768	256	2	192.168.249.0/24	contribs
	512	2	192.168.250.0/23	contribs
4	1	1	192.168.249.15	contribs
	1	1	192.168.249.255	contribs
	1	1	192.168.250.15	contribs
	1	1	192.168.251.15	contribs



IPv6

```
{{blockcalc|ok|nolist|nonote|
2604:2000:f82a:2c00:eccf:c2e5:8b09:6757 2606:6000:610a:9000:1d0f:636f:39a:867c
2606:6000:610a:9000:1d0f:636f:39a:867d
2606:6000:610a:9000:1d0f:636f:39a:867e  2606:6000:610a:9000:1d0f:636f:39a:867f
2606:6000:610a:9000:9df6:cc8d:592b:1ae
}}

{{blockcalc|ok|nolist|nonote|allocation=128|…}}

{{blockcalc|ok|nolist|nonote|results=all|…}}
```

Default

Total affected	Affected addresses	Given addresses	Range	Contribs
2 /64	1 /64	1	2604:2000:f82a:2c00::/64	contribs
	1 /64	5	2606:6000:610a:9000::/64	contribs

allocation=128

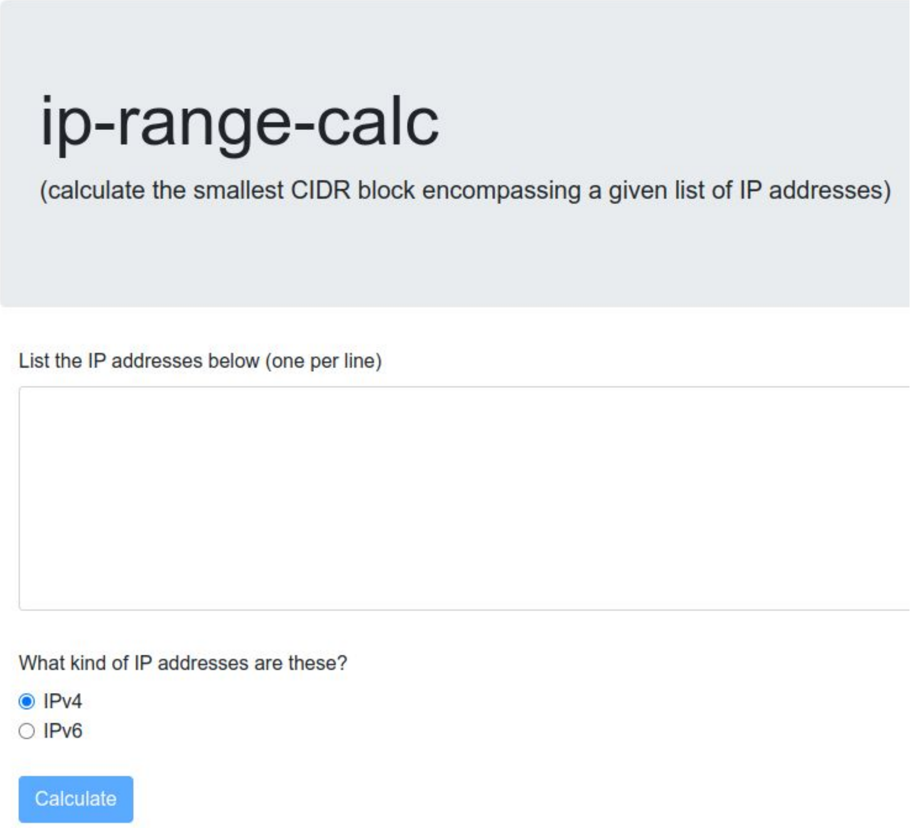
Total affected	Affected addresses	Given addresses	Range	Contribs
1 /64	1	1	2604:2000:f82a:2c00:eccf:c2e5:8b09:6757	contribs
	1 /64	5	2606:6000:610a:9000::/64	contribs
6	1	1	2604:2000:f82a:2c00:eccf:c2e5:8b09:6757	contribs
	4	4	2606:6000:610a:9000:1d0f:636f:39a:867c/126	contribs
	1	1	2606:6000:610a:9000:9df6:cc8d:592b:1ae	contribs

results=all

Total affected	Affected addresses	Given addresses	Range	Contribs
>64G /64	>64G /64	6	2604::/14	contribs
1 /64	1	1	2604:2000:f82a:2c00:eccf:c2e5:8b09:6757	contribs
	1 /64	5	2606:6000:610a:9000::/64	contribs
6	1	1	2604:2000:f82a:2c00:eccf:c2e5:8b09:6757	contribs
	4	4	2606:6000:610a:9000:1d0f:636f:39a:867c/126	contribs
	1	1	2606:6000:610a:9000:9df6:cc8d:592b:1ae	contribs

IP-range-calc

- there are countless IP range block tools, too – IP-range-calc is hosted on Toolforge: https://ftools.toolforge.org/general/ip-range-calc.html
- it calculates IPv4 and IPv6, most other tools can only do one of these
- it warns you if the range is too big for a block on Wikipedia



ip-range-calc

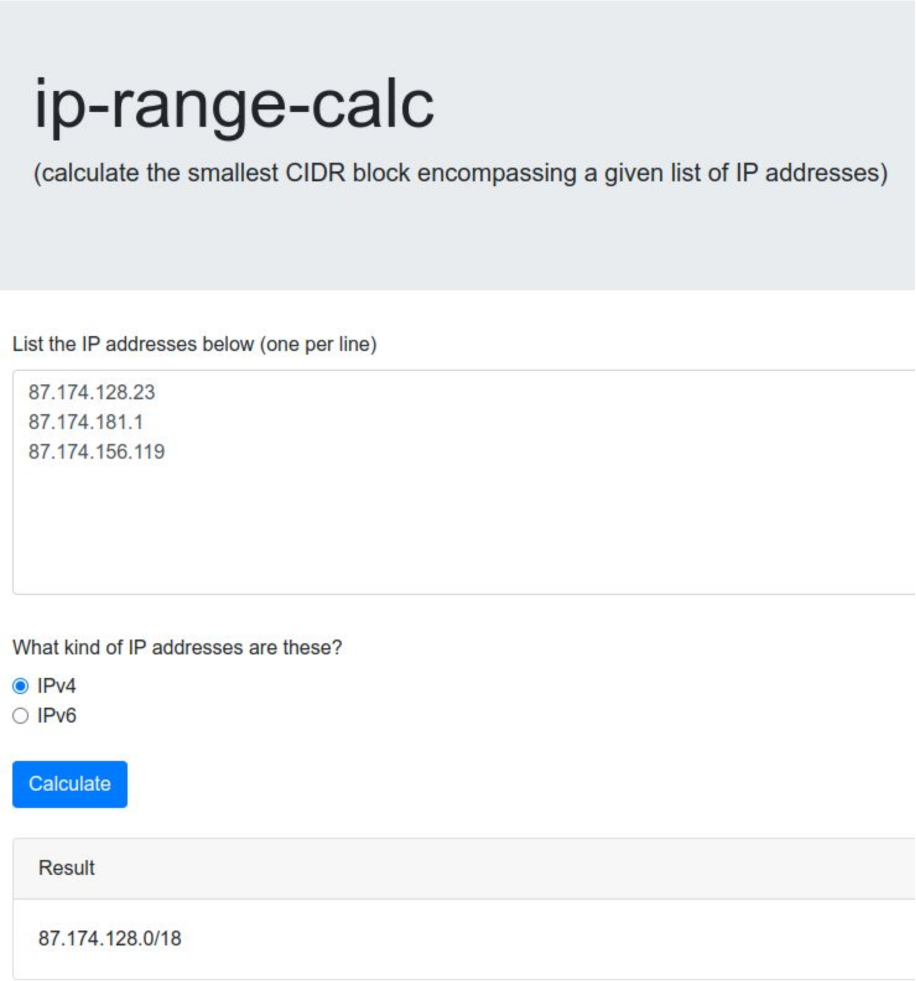
(calculate the smallest CIDR block encompassing a given list of IP addresses)

List the IP addresses below (one per line)

What kind of IP addresses are these?

● IPv4
○ IPv6

IP-range-calc



ip-range-calc

(calculate the smallest CIDR block encompassing a given list of IP addresses)

List the IP addresses below (one per line)

```
87.174.128.23
87.174.181.1
87.174.156.119
```

What kind of IP addresses are these?

● IPv4
○ IPv6

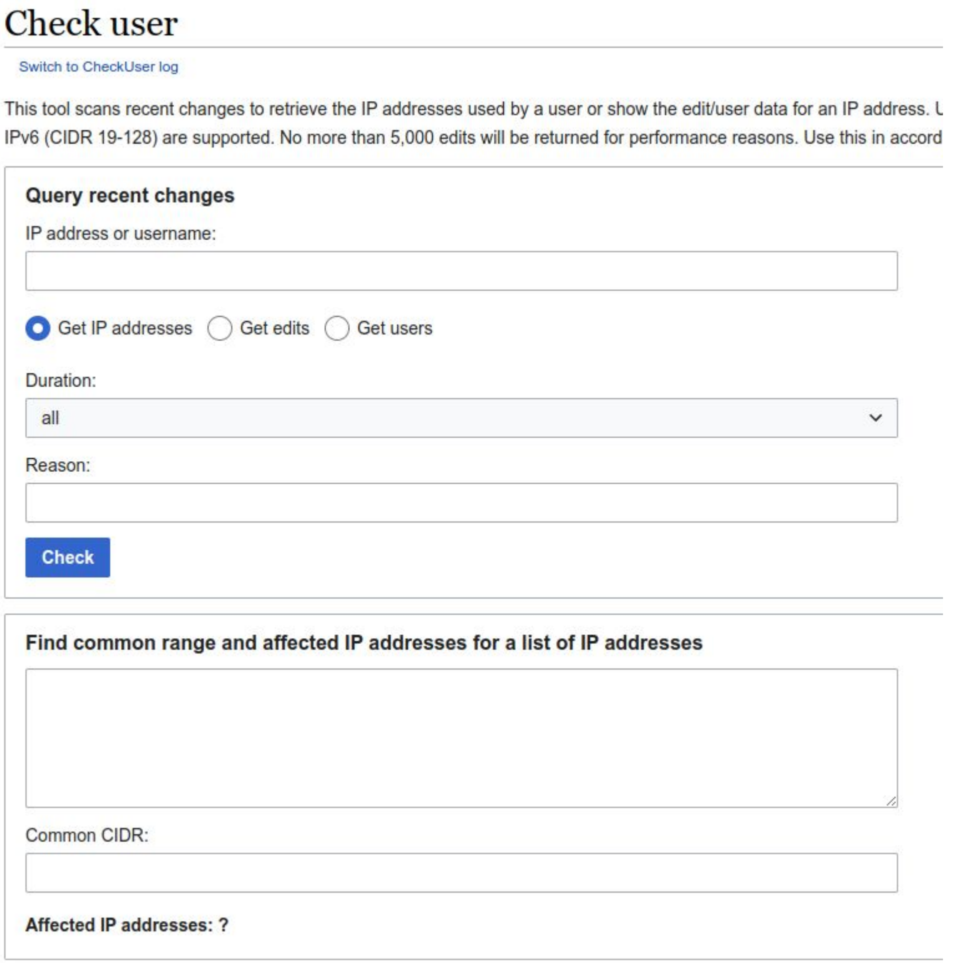
Result

87.174.128.0/18

Martin Rulsch, IP range blocks, plwiki admin training 2023

Checkuser tool

- people with access to the checkuser tool likely have noticed the form at the bottom of the page which also calculates IP ranges
- IPs can be copied from the CU result, ranges will be automatically calculated, including affected numbers



Check user

Switch to CheckUser log

This tool scans recent changes to retrieve the IP addresses used by a user or show the edit/user data for an IP address. U
IPv6 (CIDR 19-128) are supported. No more than 5,000 edits will be returned for performance reasons. Use this in accord

Query recent changes

IP address or username:

● Get IP addresses ○ Get edits ○ Get users

Duration: all

Reason:

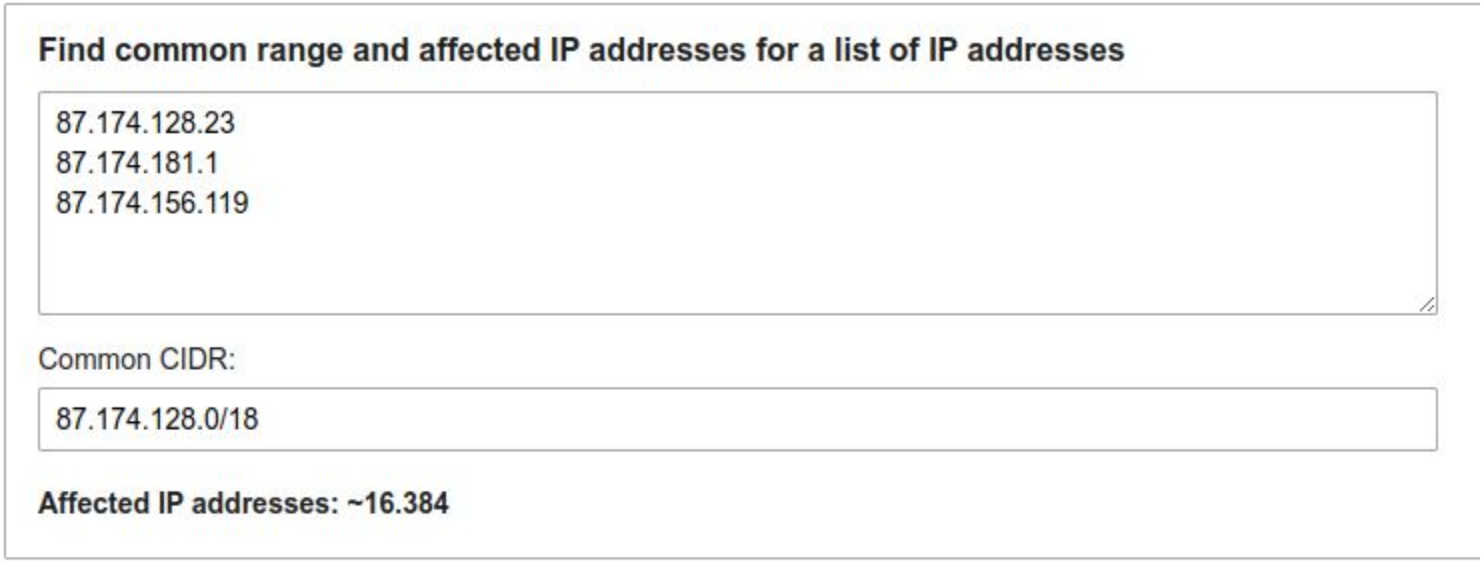
Check

Find common range and affected IP addresses for a list of IP addresses

Common CIDR:

Affected IP addresses: ?

Checkuser tool



Find common range and affected IP addresses for a list of IP addresses

```
87.174.128.23
87.174.181.1
87.174.156.119
```

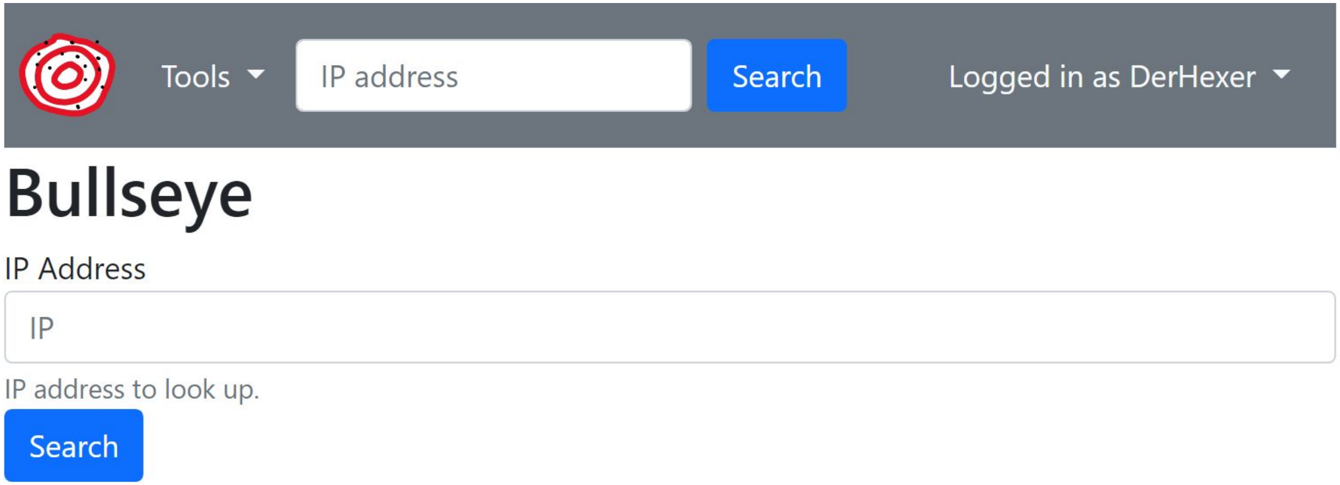
Common CIDR:

87.174.128.0/18

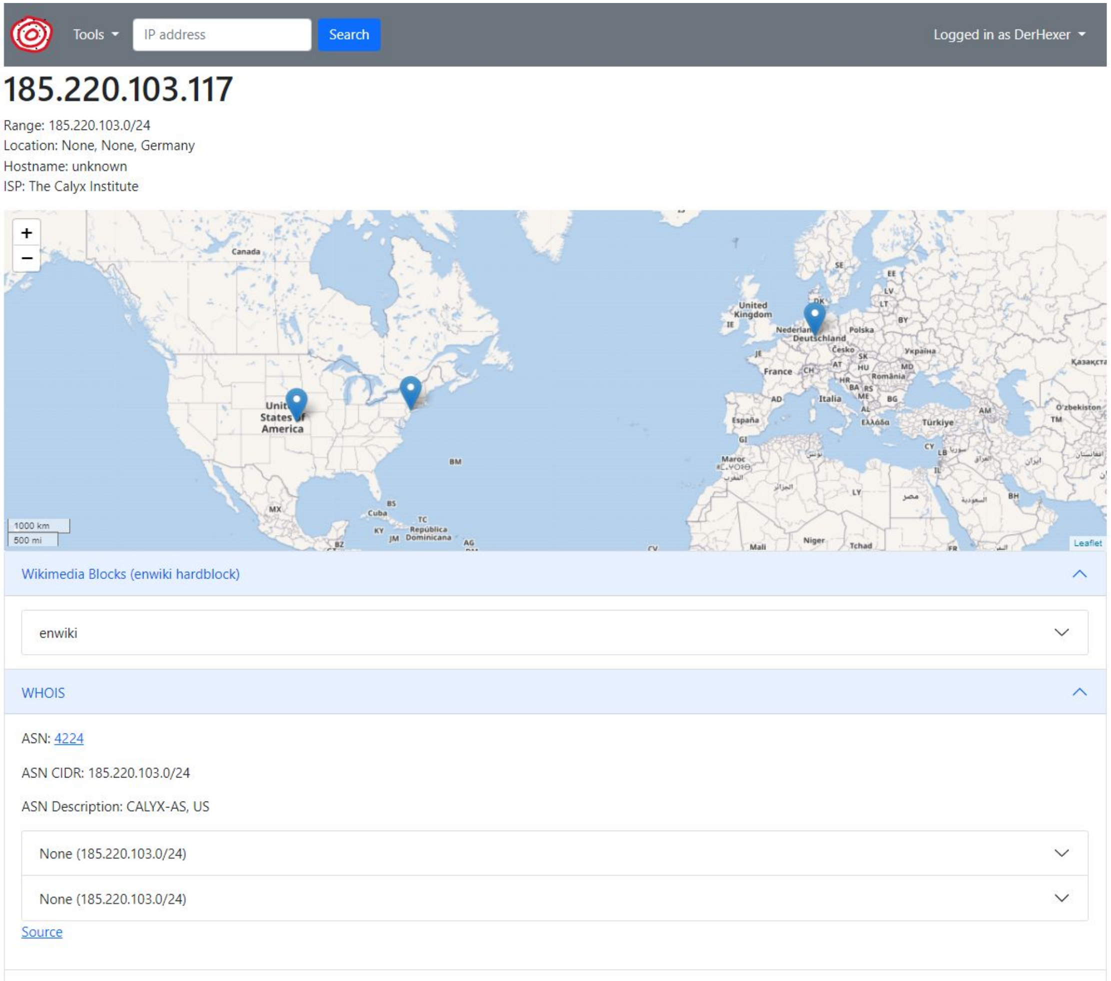
Affected IP addresses: ~16.384

One for all: Bullseye

- one tool combines many of these functions: IP data, geolocation, proxy check, wiki contributions, etc.; also available on Toolforge: https://bullseye.toolforge.org/ (only available to active community members through OAuth)



One for all: Bullseye



185.220.103.117

Range: 185.220.103.0/24
Location: None, None, Germany
Hostname: unknown
ISP: The Calyx Institute

Wikimedia Blocks (enwiki hardblock)

enwiki

WHOIS

ASN: 4224

ASN CIDR: 185.220.103.0/24

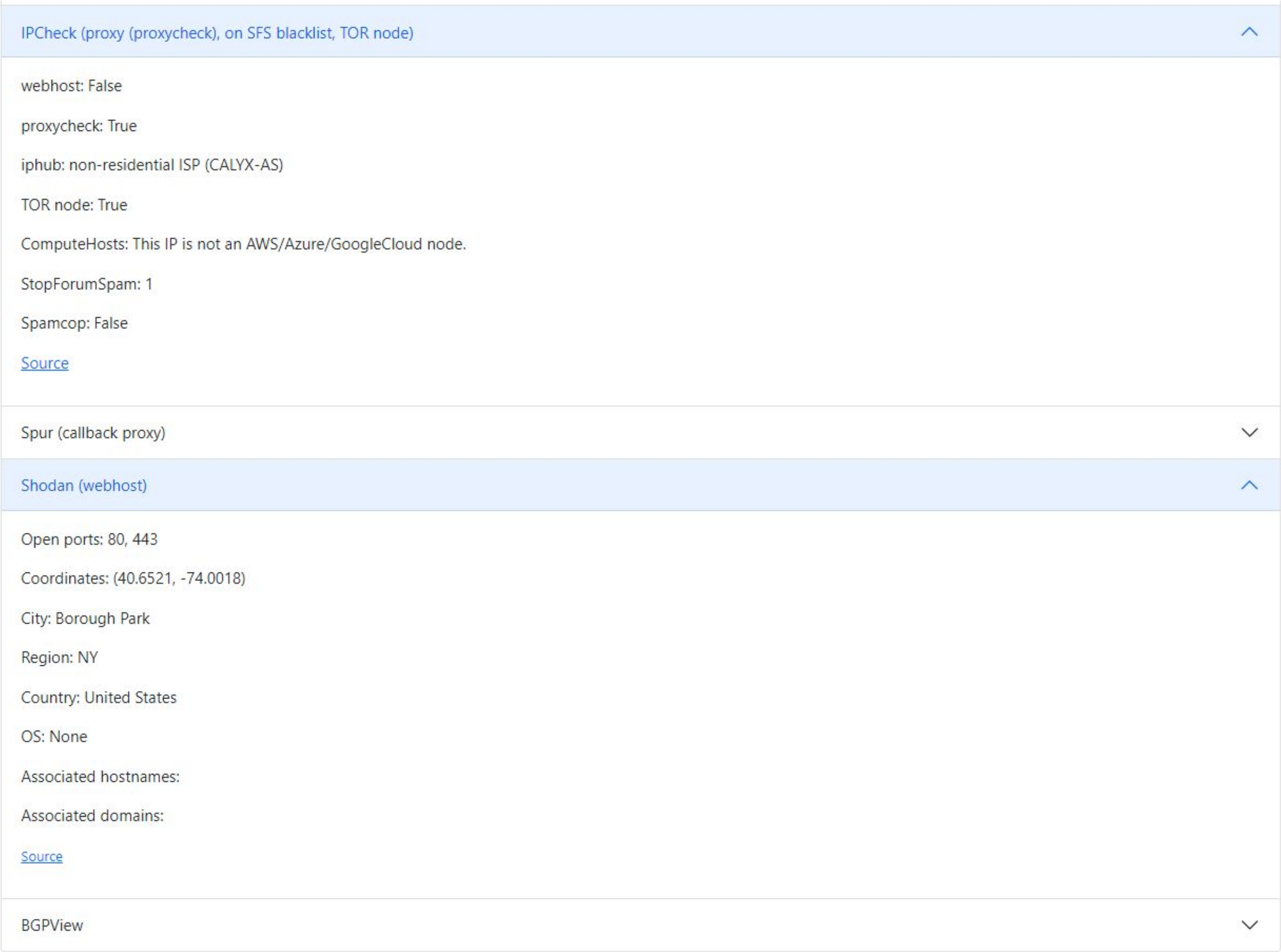
ASN Description: CALYX-AS, US

None (185.220.103.0/24)

None (185.220.103.0/24)

Source

One for all: Bullseye



IPCheck (proxy (proxycheck), on SFS blacklist, TOR node)

webhost: False

proxycheck: True

iphub: non-residential ISP (CALYX-AS)

TOR node: True

ComputeHosts: This IP is not an AWS/Azure/GoogleCloud node.

StopForumSpam: 1

Spamcop: False

Source

Spur (callback proxy)

Shodan (webhost)

Open ports: 80, 443

Coordinates: (40.6521, -74.0018)

City: Borough Park

Region: NY

Country: United States

OS: None

Associated hostnames:

Associated domains:

Source

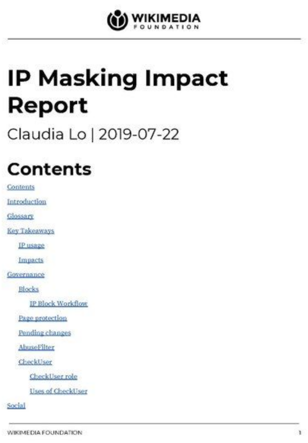
BGPView

Excursus

The Future: IP masking

- IP addresses are getting more and more considered as private data (esp. since the IPv6 introduction) as they can localize or even identify individuals through their computer networks
- some organizations help their users to hide their IP addresses (and sometimes user agents ~ computer data)
- instead, Wikimedia projects kept IP addresses of any kind in article histories, etc. – a complete removal would prevent anti-vandalism work

⇒ IP masking is planned → IPs only visible for people who need them (checkusers, admins, etc.), IP info will help reveal the IP address



WIKIMEDIA FOUNDATION

IP Masking Impact Report

Claudia Lo | 2019-07-22

Contents

WIKIMEDIA FOUNDATION 1

Questions?

Some help pages (English)

- mw:Range_blocks
- mw:Range_blocks/IPv6

IP range blocks training

Martin Rulsch
martin.rulsch@wikipedia.de

plwiki peer support for administrators
31 January