Ruby trunk - Feature #15734

Parsing of shorthand IPv4 addresses compatible with inet_aton

03/28/2019 05:50 PM - Envek (Andrey Novikov)

Status:	Open
Priority:	Normal
Assignee:	
Target version:	

Description

Hi Ruby team!

I've created pull request to ipaddr gem: https://github.com/ruby/ipaddr/pull/12
I want it to be merged and included to the version of gem that bundled in Ruby itself.

Many applications (like browsers, curl, and ping) and even Ruby's own Net::HTTP library accepts shorthand IPv4 addresses like 127.1 or 2130706433 that both stands for 127.0.0.1.

```
$ irb
irb(main):001:0> require 'net/http'
irb(main):002:0> Net::HTTP.get(URI.parse("http://127.1/")) # Success if you have web server runnin
g locally
=> "<!DOCTYPE html>\n<html>\n<head>\n<title>Welcome to nginx!</title>…"
```

But IPAddr can't accept such addresses, and it is really confusing:

```
irb(main):003:0> IPAddr.new("http://127.1/")
IPAddr::InvalidAddressError (invalid address: http://127.1/)
```

This pull request makes parsing IPv4 to match the behavior of most well-known applications despite that isn't a standardized extension, but there is an RFC draft: Textual Representation of IPv4 and IPv6 Addresses.

Moreover, that mismatch in behavior could cause security vulnerabilities in Ruby applications that use network, allow users to provide URLs to access (like “Upload picture from URL”), and have incorrectly configured URL filtering. A malicious user then could provide a link like http://2130706433/private_file which currently will not be recognized as loopback IP address but Net::HTTP.get will happily query local host's web server for the private_file. This called an SSRF attack. Actually, I created this pull request because our security auditors reported such vulnerability in one of our applications.
NOTE: There is **no** security flaw in ipaddr itself! It is just possible to get when you're developing an application.

See also:

- Discussion at Reddit: https://www.reddit.com/r/networking/comments/7cf0zp/documentation_of_the_behavior_of_shorthand_ipv4/
- inet_aton man page: https://linux.die.net/man/3/inet_aton