

State of Minnesota Guidelines IP Networking Guidelines

Timeline

These guidelines are for the 2012-03-30 edition of the standard, and are informative and not normative.

Overview

These guidelines address several aspects of IP Networking:

- IPv4 configuration requirements
- IPv6 configuration requirements
- User interface requirements for IP addresses
- Private and special networks
- Internal State network usage
- The IPv4 to IPv6 transition process

IPv4 Configuration Requirements

This section covers the specifics for supporting IPv4.

For usages that require configuring the network layer, support can be static or dynamic.

Static support requires manual configuration of the following:

- IP address
- Network information (as a bit-count number, subnet mask, or other mechanism)
- Default route
- Name server(s)

Dynamic support requires:

- Selection of DHCP
- Provision of, or arranging for, the provision of a suitable DHCP server

For other usages, support requires the ability to accept just a host name (either locally resolved or a fully qualified domain name resolved by the State's name servers), just an IP address, or either.

IPv6 Configuration Requirements

This section covers the specifics for supporting IPv6.

For usages that require configuration of the network layer, support can be static or dynamic.

Note that under IPv6 with a static configuration, most information is acquired dynamically during network interface initialization. Anyone configuring an IPv6 network segment should do so in consultation with MN.IT Services' Network Services recommendations.

Static IP addresses will normally only be assigned to specific published services. The IPv6 native address assignment mechanism will normally be used for client configuration.

Static support requires manual configuration of the following:

- IP address
- Network information as a bit-count number

Dynamic support requires:

- Selection of DHCP
- Provision of, or arranging for, the provision of a suitable DHCP server

For other usages, support requires the ability to accept just a host name (either locally-resolved or a fully-qualified domain name resolved by the State's name servers), just an IP address, or either.

User Interface Requirements for IP

This section covers requirements for user interfaces that provide user entry of IP address or host name information.

Fully Qualified Domain Name (FQDN) requirements:

- Allow 255 characters
- Display 40 or more (e.g., "...<input type="text" size="40" maxlength="255" ...>...")
- FQDNs associated with electronic mail addresses allow only the letters a-z and A-Z, the digits 0-9 and the characters "-", "_", and "." (this requirement applies to the host portion of the address to the right of the "@" symbol)
- FQDNs for other purposes should not be syntax-checked. Any input should be presumed valid by the user interface

IPv4 Address Requirements:

- The form is "#.#.#.#" where the "#" character refers to any string of 0, 1, or 2 digit characters forming a number in the range 0 to 255
- Entry of leading zero characters in each part of the address should be mildly discouraged as they can lead to ambiguities due to possible interpretation as octal
- Allow 15 characters
- Display 15
- Allow the digits 0-9 and the "." character

IPv4 Network Requirements:

- The form is a valid IPv4 address, a "/" character and a string of 1 or 2 digit characters forming a number in the range 0 to 32, inclusive
- Future applications should avoid using subnet masks for input, although they may display them
- Allow 18 characters
- Display 18
- Allow the digits 0-9 and the "." and "/" characters

IPv6 Address Requirements:

- The form is "#:#:#:#:#:#:#:#" where the "#" character refers to any string of 0, 1, 2, 3, or 4 hexadecimal digit characters forming a number in the range 0 to ffff hexadecimal (65,535 decimal)

- Two consecutive colons with no intervening hexadecimal digit characters are permitted once per IPv6 address
- The upper or lower case versions of the hexadecimal digits A to F should be treated identically
- Allow 39 characters
- Display 39
- Allow the digits 0-9, the letters a-f and A-F and the ":" character

IPv6 Network Requirements:

- The form is a valid IPv6 address, a "/" character and a string of 1, 2 or 3 digit characters forming a number in the range 0 to 128, inclusive
- Allow 43 characters
- Display 43 or more
- Allow the digits 0-9, the letters a-f and A-F and the ":" and "/" characters

IPv4/IPv6 Address Requirements (allow either):

- Allow entries that match either the IPv4 address or IPv6 address forms
- Allow 39 characters
- Display 39
- Allow the digits 0-9, the letters a-f and A-F and the "." and ":" characters
- Since the two forms use different syntax, it is possible to analyze the entry and reliably determine which form was entered

IPv4/IPv6 Network Requirements (allow either):

- Allow entries that match either the IPv4 network or IPv6 network forms
- Allow 43 characters
- Display 43
- Allow the digits 0-9, the letters a-f and A-F and the ".", ":" and "/" characters
- Since the two forms use different syntax, it is possible to analyze the entry and reliably determine which form was entered
- It is also possible to analyze the entry and determine whether an address or a network was entered

Private and Special Networks

This section lists the private and special network blocks assigned (they may or may not be in use). This document provides a summary list. See the referenced RFCs for details.

The networks are:

- 0.0.0.0/8 - Addresses in this block refer to source hosts on "this" network. [RFC1700, page 4].
- 10.0.0.0/8 - This block is set aside for use in private networks. Its intended use is documented in [RFC1918].
- 100.64.0.0/10 – This block is set aside for use by ISPs.
- 127.0.0.0/8 - This block is assigned for use as the Internet host loopback address. [RFC1700, page 5].
- 169.254.0.0/16 - This is the "link local" block. It is allocated for communication between hosts on a single link. Hosts obtain these addresses by auto-configuration, such as when a DHCP server may not be found.
- 172.16.0.0/12 - This block is set aside for use in private networks. Its intended use is documented in [RFC1918].

- 192.0.2.0/24 - This block is assigned as "TEST-NET" for use in documentation and example code. It is often used in conjunction with domain names example.com or example.net in vendor and protocol documentation.
- 192.88.99.0/24 - This block is allocated for use as 6to4 relay anycast addresses, according to [RFC3068].
- 192.168.0.0/16 - This block is set aside for use in private networks. Its intended use is documented in [RFC1918].
- 198.18.0.0/15 - This block has been allocated for use in benchmark tests of network interconnect devices. Its use is documented in [RFC2544].
- 224.0.0.0/4 - This block, formerly known as the Class D address space, is allocated for use in IPv4 multicast address assignments. [RFC3171].
- 240.0.0.0/4 - This block, formerly known as the Class E address space, is reserved. [RFC1700, page 4]
- ::/8 – Reserved. [RFC1884]
- ::1/8 – Unassigned. [RFC1884]
- e800::/10 – Link local. [RFC1884]
- ec00::/10 – Site local. [RFC1884]
- ff00::/8 – Multicast. [RFC1884]

No addresses on any of the above networks may be used on the state's wide area network except as noted here.

Internal State Network Usage

The following blocks are set aside for use within an organization (which is to say, within that organization's VPN). They should never be used for communications between organizations. This definition corresponds to the RFC1918 usage.

- 10.0.0.0/11 (but see below)
- 192.168.0.0/16
- e800::/10
- ec00::/10

These blocks are set aside for use between organizations on the state's network, including the University of Minnesota network. Assignments are managed by MN.IT Services and addresses in the same range will not be assigned to more than one place on the network. Forward and reverse address assignments in these ranges may be entered into MN.IT Services' DNS servers, although responses may not be returned if the requestor is not on the state network.

- 10.1.128.0/17
- 10.32.0.0/11
- 10.64.0.0/10
- 10.128.0.0/9
- 100.64.0.0/10
- 172.16.0.0/16
- not needed in IPv6

For usages that require configuring the network layer, support can be static or dynamic.

The IPv4 to IPv6 transition process

Caution: this document presents a "best guess" process as of the time of writing. The actual process followed will differ from this envisioned process. All dates are the best available estimates as of the time of writing.

IPv4 Runout

The actual runout is a “soft” deadline composed of many smaller events.

The last open /8 block has already been allocated to a regional registry.

The regional registries have mostly issued their last sizable blocks (/16 or larger).

There currently are end users in other parts of the world that receive only IPv6 addresses.

For our purposes, the question is really when the first end user receives only an IPv6 address for a connection to us. We don't know when that will be. This date is unknown because of several factors:

- It is anticipated that a market for IPv4 to IPv6 gateway devices will exist and that devices will be created to meet that market. It is likely that these devices will perform adequately for many functions.
- It is also anticipated that the use of IPv4 NAT will be extended to prolong the life of existing IPv4 assignments.
- It is also anticipated that IP address pool allocations will be tightened and refined to prolong the life of existing IPv4 assignments.

For all of these reasons, it is unclear when state systems will have to support an IPv6-only end user.

Network Level Support

As of this writing:

- The Internet is mostly IPv4 (a few percent of traffic is IPv6).
- Internet2 supports both IPv4 and IPv6.
- Few Internet providers allow ordering of IPv6 service.
- Most major Internet sites support IPv6.
- Our existing network devices support IPv6 for customer data. Internal management is IPv4-only at this time. IPv6 support, while present, is not optimized to the same degree as IPv4.
- It is not clear how the widespread adoption of IPv6 would affect Internet global routing table size.

State Government Needs

The state's network has sufficient IPv4 address space available to meet the foreseen needs of its customers up to and beyond a 2015 planning horizon, absent any disruptive events.

Disruptive Events

It is possible that disruptive events may occur that will invalidate the above assumptions and estimates. Examples of such disruptive events are:

- New IPv4 applications that require on the order of 1 (or more) additional “real” IPv4 addresses per user. With 30,000 state employees (and many more state network users), such an expansion would use up all available supplies.
 - Note: two applications have already appeared:
 - VoIP telephony
 - possible statewide VPN services
 - We have been able to implement those applications using RFC 1918 addresses to avoid the problem.
- A new IPv6-only application may appear that is important for us to support.
- A federal government requirement to fully support IPv6.

Other disruptive events are possible.

Transition

The following transition is envisioned:

- External applications will be addressed first. They will be addressed in two phases:
 - Phase 1 is to require IPv6 support in all new or substantial upgrade to existing systems and software. We will provide adequate notice to vendors of this coming requirement.
 - Phase 2 is to actually configure the support, which may be some years after phase 1.
- Purely internal applications will be addressed later. They will be addressed in the same two phases, although phase 2 will happen considerably closer to phase 1 than with external applications.

For the purposes of this section, an external application is defined as one where either the source or destination of the traffic is not on the state's network, or is one that is accessed by someone who is not a state employee, contractor, consultant or agent. An internal application is one where both the source and destination of the traffic is on the state's network and is accessed by a state employee, contractor, consultant or agent. Note that this is a technology-centric definition and does not directly depend on the application's intended audience.

Some applications will remain internal indefinitely. Examples are the network device management infrastructure, computer room floor networks used for device control and similar closed systems.