Now that IPv4 addresses have been depleted around the world, the need to move to IPv6 is becoming more and more real. Here are a few of the questions that need to be addressed prior to migration: What is in my network today? Which parts need to be upgraded first? Do existing network devices support IPv6? If not, can they be upgraded? What migration strategy should be used for addressing, tunneling, etc? How will existing legacy applications perform over IPv6? Will network capacity be adequate to support migration to IPv6? How will operational integrity and network security be ensured during the incremental migration?

In an effort to help Network Nebraska participant's preparedness, this document has been created. This document is aimed to address Campus/Entity readiness assessment, Network Nebraska Addressing Methodology and determine some best practices when deploying IPv6. Network Nebraska staff believe that now is the time to start assessing how your institution is positioned in regards to IPv6. We feel it is time to start to lab up some IPv6 networks, so that Network Nebraska as a whole is prepared for the transition to an IPv4/IPv6 world as that day is finally quickly approaching.

Readiness Assessment:

Technical staff should survey and catalogue all aspects of systems that may be impacted by IPv6 deployment. Should also identify stakeholders within organization that need to participate in readiness assessment.

Here are some possible examples:

Internal/external IPv6 address space
Development or updating of policies for the use of IPv6 on corporate networks
Internal/external IPv6 addressing schemes/plans
Internal/external DNS servers (including DHCP servers)
Authentication systems (such as Radius servers)
Use of peering, transit, relays, or tunnels for external connectivity
Management tools for network devices (routers, switches, etc.)
Physical hardware of network devices (routers, switches, etc.)
Service load balancers
Firewalls and VPN concentrators/clients
Storage systems
Video conferencing systems
VoIP systems
Client OS deployments
Server OS deployments
Corporate applications
Security policies and support in network devices & servers
Operations readiness including management systems, troubleshooting & monitoring tools, testing tools

Outsourced applications
Associated broadband CPE, such as cable modems, DSL modems, and router/wireless AP's
General staff readiness (level of knowledge/expertise)
Ensuring that all new network service providers the company contracts with provide documented support for IPv6
Identify embedded/hard-coded reliance on IPv4 connectivity and IPv4 addresses
Identify latency-sensitive or port-intensive applications that would be impacted by NAT implementation outside the entities control
Ensure appropriate handling of IPv6 addresses within logging, access control, and other relevant subsystems
Identification of IP-connected embedded devices or systems (microcontrollers, HVAC, etc.) not under the control or management of the technical staff/IT team
Future network hardware vendors provide documented support for IPv6
Future application platform vendors provide documented support for IPv6
Future software/Saabs/application vendors provide documented support for IPv6
Future vendors/providers be able to provide QA results for IPv6 support, as required/necessary

Time and Effort costs to consider:

Comprehensive Survey Development
Roadmap & Timeline Development
Process & Policy Development
Development effort for product/application/service, as relevant
Hardware/Software Testing
Required Upgrades & Enhancements
Training
Ongoing Measurement & Monitoring

Potential Network Nebraska Deployment Methodology:

What follows doesn't actually reflect the final plan as far as actual assignment details, but it should convey the general methodology.

What we ended up deciding was that is was more important to maintain sanity than to use every single address and maintain strict route aggregation internally. We aggregate it all at the internet egress to be responsible, but internally it's not going to make much difference to see 200 routes as opposed to 25, and if it means it's easier to follow then all the better. With that in mind here is what we came up with for CSN. We have left out a lot of the shortening to make it easier to follow.

We started at the highest order assignable 7 bits in the /32 allocation and broke up /37 blocks for organizational types. This gives CSN 32 Org Types. We considered adding geographic disparity to it as well, but scratched it because it just reduced the number of org types significantly for very little appreciable gain in aggregation.

2606:1c00:00xx::/37
2606:1c00:08xx::/37
2606:1c00:10xx::/37
2606:1c00:18xx::/37

....
.....
.....
2606:1c00:F8xx::/37

Each /37 gives me 2048 /48 blocks to hand out to entities under that org type. If we need more than 2048 blocks, we will add another /37 to that org type.

Each /48 contains 65536 /64 prefixes for use by that entity. We don't foresee even those largest entities needing more prefixes than that. One /64 contains billions of possible addresses and no one wants a layer 2 domain that large. :)

2606:1c00::/32 = CSN ARIN assignment

2606:1c00:00::/37 = CSN
2606:1c00:08::/37 = RESERVED
2606:1c00:10::/37 = State Colleges(?)
2606:1c00:18::/37 = K-12(?)
2606:1c00:20::/37 =?
etc.....

Under CSN we broke it up further as follows:

2606:1c00:0000::/48 =Network devices
2606:1c00:0000:0000::/64 = loopback addresses, /128 mask. Billions of them.....
2606:1c00:0000:0001::/64 - 2606:1c00:0000:FFFF::/64 = Network Links,
We assign these as /64's but use a /126 mask on Point to Point links (/127 is invalid due to interference with the subnet-router anycast address (some people use them though). I use ::1 and ::2 on PtP links. On non PtP links I use the /64 mask.

2606:1c00:0001::/48 =Management Subnets
2606:1c00:0002::/48 =Server Subnets
2606:1c00:0003::/48 =Desktop Subnets

Under each subnet, we'll embed the VLAN at the /64 level to make the individual subnet allocation, such as:

2606:1c00:0001:1625::/64 =VLAN 1625 and is used for a management network
2606:1c00:0003:0149::/64 =VLAN 0149 and is a Desktop subnet

Best Practices when deploying IPV6:

Karl Schlitt from CNS staff found a very good manual on best practices and deploying IPv6. We will attach that document with this document. Everyone should really take the time to look through the document. You can also goto http://ripe.net/training/material/IPv6-for-LIRs-Training-Course/IPv6_addr_plan4.pdf and download the manual.