EA-02-03-01-G
State CIO Adopted: October 6, 2023
Sunset Review: October 6, 2026

Replaces:
N/A

Washington Technology Solutions

IPV6 IMPLEMENTATION GUIDELINES

See Also:
RCW 43.105.054 OCIO Governance
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (22) "State agency"
American Registry for Internet Numbers
RFC Filtering
RFC Basic IPV6 Transition Mechanisms
RFC Unique Local IPv6 Unicast Addresses

1. **Agencies should apply static addressing to servers and storage to ensure functionality and availability.**

    a. If servers are not manually configured with an Internet Protocol version 6 (IPv6) address, a new IPv6 address should be autoconfigured whenever a Network Interface Controller (NIC) card is replaced.

    b. Keep the following tips in mind when you create addresses for servers:

        i. Give servers meaningful and stable interface identifications (interface IDs).

        ii. One strategy is to use a sequential numbering scheme for interface IDs.

2. **Agencies should Plan IPv6 addressing as follows:**

    a. Plan for addressing based on the total number of sites, not the end number of devices.

    b. The end user device is no longer a factor when planning the address scheme.

    c. Reserve a block for infrastructure, such as internal routing interface addressing, and static addresses for administration servers and devices.

    d. Lay out each subnet prefix of equal size within each level of the hierarchy.

    e. Begin tracking and planning for the upgrade/replacement of devices that are not IPv6 capable.

3. **Address Schemes Guidelines. See Subnet Calculator and/or Test my ipv6 Subnet Calculator.**

    a. IPV6 uses hexadecimal numbering. See Hexidecimal_Binary_Chart

    b. Map to network topology.

    c. Meet current requirements under IPV6 Policy.

    d. Manually configure link-local addresses in an easily readable format. This will make verifying or troubleshooting routes easier.

    a. Ensure schemas align with nibble boundaries as much as possible. See Table_1_Nibble_Boundaries and associated examples:
        i. Network_Allocation_Example_48_52_60
        ii. Network_Allocation_Example_36_56_64
        iii. Network_Allocation_Example_36_48_56
        iv. Network_Allocation_Example_36_44_56

4. **Security considerations for Tunneling on an Internal Agency Local Area Network (LAN):**

    i. Tunnel endpoints.

    ii. Inspection.

    iii. Access control.

    iv. Termination.

    v. Tunnels shall be treated as external links with the appropriate security protocols in place. See NIST 800-119 Guidelines for the Secure Deployment of IPV6.

5. **Agencies should update the following network services to support IPv6:**

    i. Domain Naming Service (DNS) Records-

        i. PRIMARY Records

            A. A- IPv4

            B. AAAA- IPv6

            C. PTR= Pointer Records

            D. CNAME- Canonical Name Records

E. NS- Name Server

F. MX – Mail Exchange records, add IPv6 addressing to the mail server.

b. Records to inspect for IPv6 compatibility.

c. NIS- Name Information Server

i. NFS- Name File Server

ii. NTP- Network Time Protocol Server

iii. WEB- Server

iv. Linux and Bind Services

v. Note: LDAP supports IPv6 without requiring additional configuration changes.

6. Agencies should validate IPv6 capability:

a. Validate that devices (current and future) can support IPv6 routing protocol of choice for both hardware/software and operating system (OS).

b. Agencies shall ensure the current IOS is IPv6 compatible.

c. Ensure that current or future model and version type are compatible, as a model may be compatible while select versions are not.

d. Verify which hardware on the network can be upgraded to IPv6 and any other device. For Example:

i. Routers.

ii. Switches.

iii. Servers.

7. Agencies should assess IPv6 for the agency environment:

a. An IPv6 plan should be built for each key technology pillar (or silo) within an agency. Agencies are responsible for and assessing the impact of anycasting to:

i. **Network** – Routers, switches, wireless, load balancing, DHCP, DNS, IPAM, Internet peering, routing policies.

ii. **Security** – Firewalls, IDS/IPS, logging, identity management.

iii. **Systems and Virtualization** – Host servers, applications, guest OS's, DNS, DHCP, IPAM, logging, identity management, client OS's.

iv. **Storage** – SAN, file protocols, file services, backup, and recovery.

v. **Database** – SQL, big data, or other data analysis processes.

vi. **Line of business applications** – CRM, Human Resources, Financials, or any customer applications developed by the agency itself.

8. **SLAAC (Stateless Address Auto-Configuration) will not be used on the State Core Networks.**

   i. If an agency implements SLAAC internally on their LAN, then the entire LAN must be 100% IPv6.

   ii. For stateless configuration to work properly, the advertised prefix length in an RA message must always be 64 bits.

REFERENCES:

1. Subnet Calculator.
2. Test my ipv6 Subnet Calculator.
3. Hexidecimal_Binary_Chart.
4. NIST 800-119 Guidelines for the Secure Deployment of IPv6.
   a. Para. 3.7.3.3 IPv6-Specific DNS Security Recommendations.
   b. Para 6.4 Dual Stack Ipv4/IPv6 Environments.
   c. Para 6.5.1 General Security Considerations for Tunneling.
5. Statewide Migration to IPv6.
6. Table 1 Information System (Nibble) Boundaries.
7. Network_Allocation_Example_48_52_60.
8. Network_Allocation_Example_36_56_64.
9. Network_Allocation_Example_36_48_56.
10. Network_Allocation_Example_36_44_56.

Table 1: Information System (Nibble) Boundaries, with prefix notations (these are not CIDRs notations):

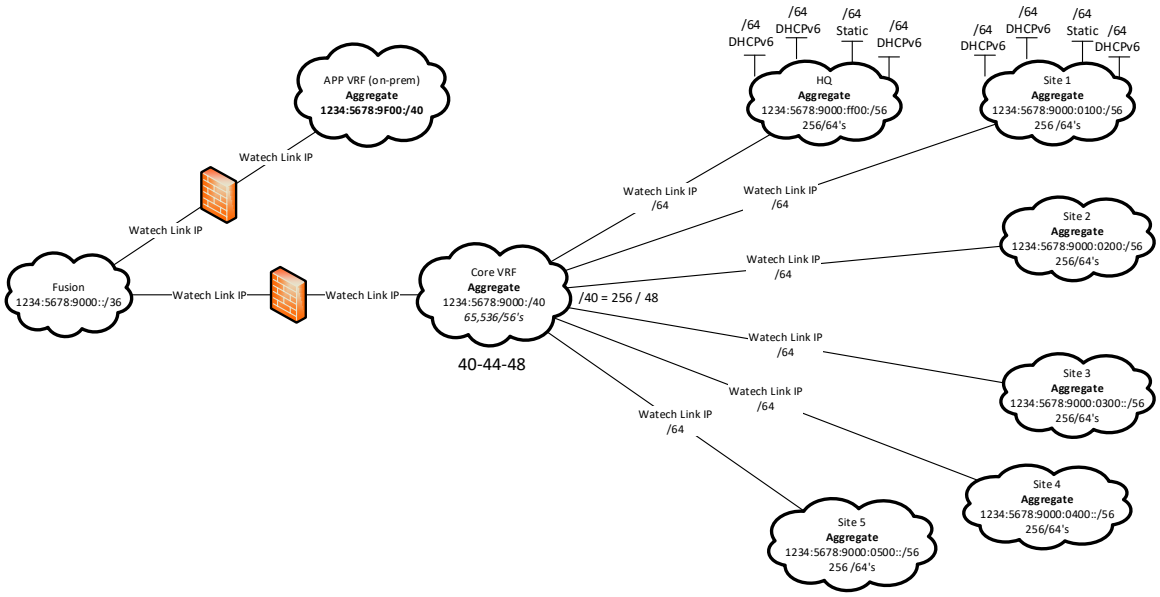
/36 includes **16- /40** 256 /44 4,096 /48 65,536 /52 1,048,576 /56 16,777,216 /60 268,435,456 /64	**/40** includes 16 - /44's 256 /48's 4,096 /52's 65,536 /56's 1,048,576 /60's 16,777,216 /64's	**/44** includes 16 - /48's 256 - /52's 4,096 /56's 65,536 /60's 1,048,576 /64	**/48** includes 16 - /52's 256 - /56's 4,096 /60's 65,536 /64
/52 includes 16 - /56's 256 - /60's 4,096 /64's	**/56** includes 16 - /60's 256 - /64's	**/60** includes 16 - /64's	/64 includes 1- /64 = (18,446,744,073,709,551,616 host addresses)

Back to REFERENCES

Network Address Allocation Examples

EXAMPLE **EXAMPLE**

Example /36 Broken into /40 to /56 to /64 assigned to devices

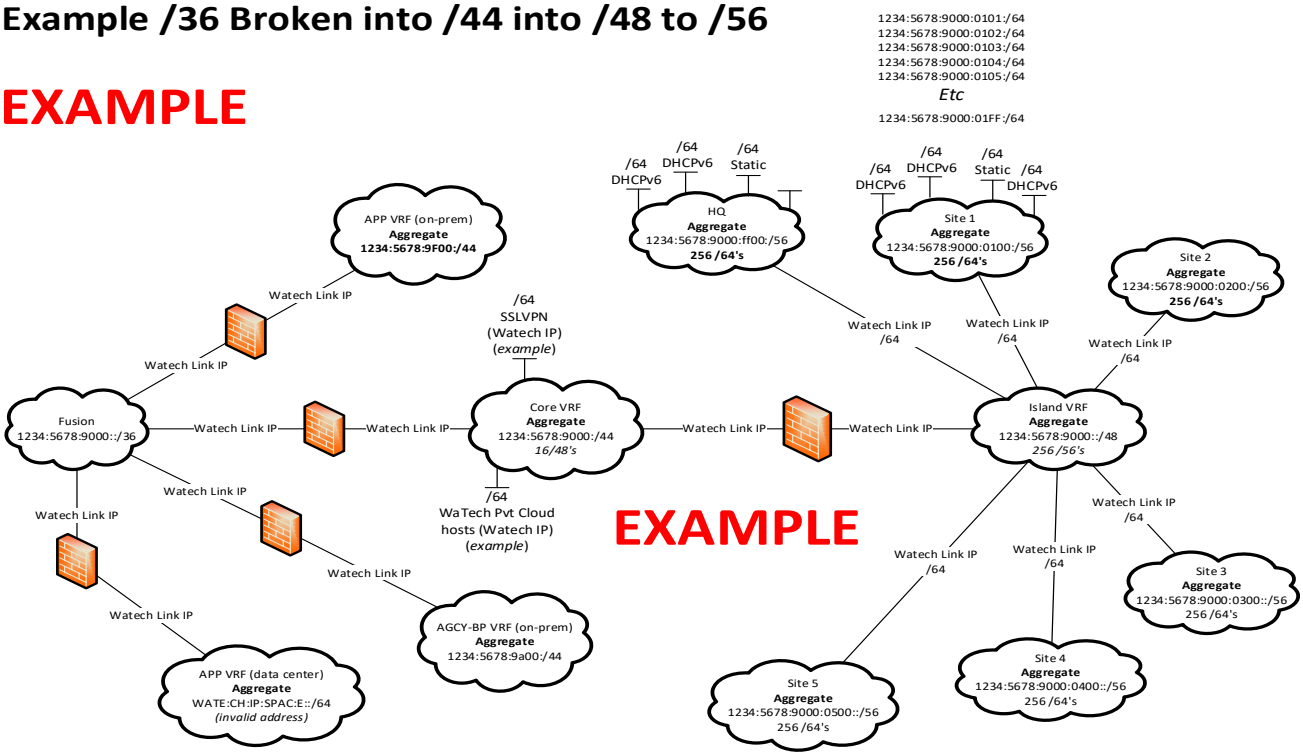


EXAMPLE **EXAMPLE**

[Back to REFERENCES]

Example /36 Broken into /44 into /48 to /56

EXAMPLE



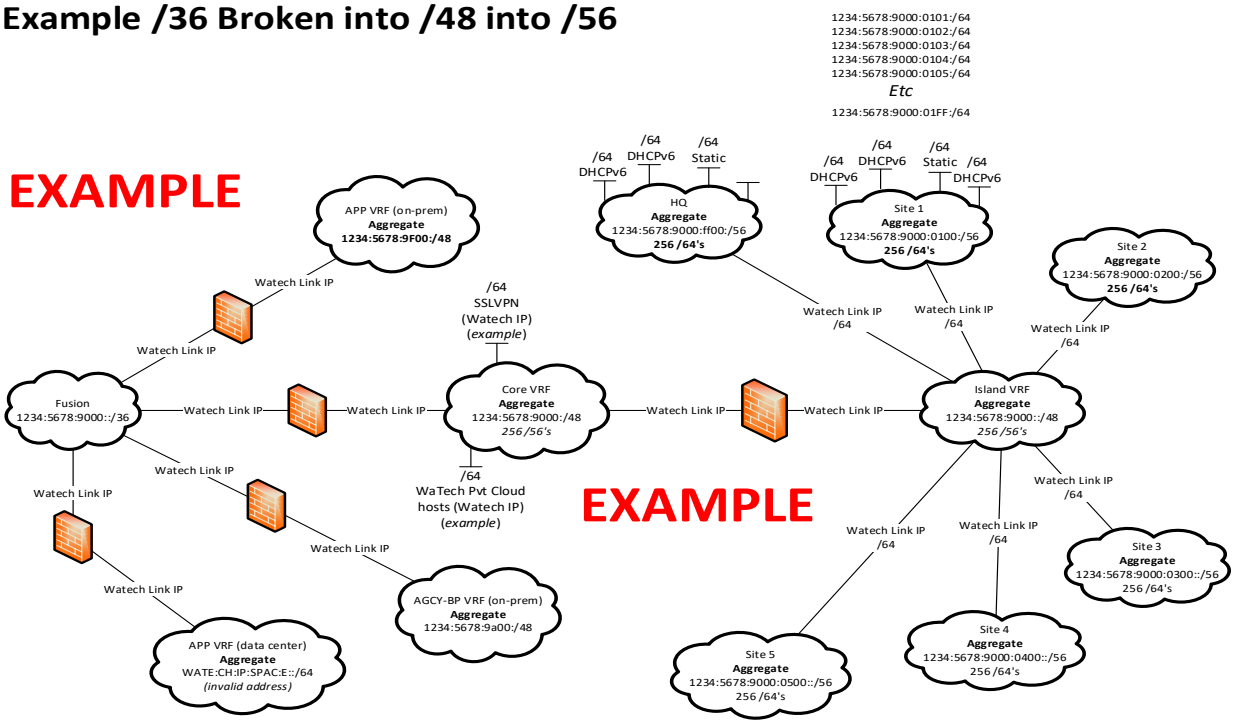
EXAMPLE

EXAMPLE

EXAMPLE

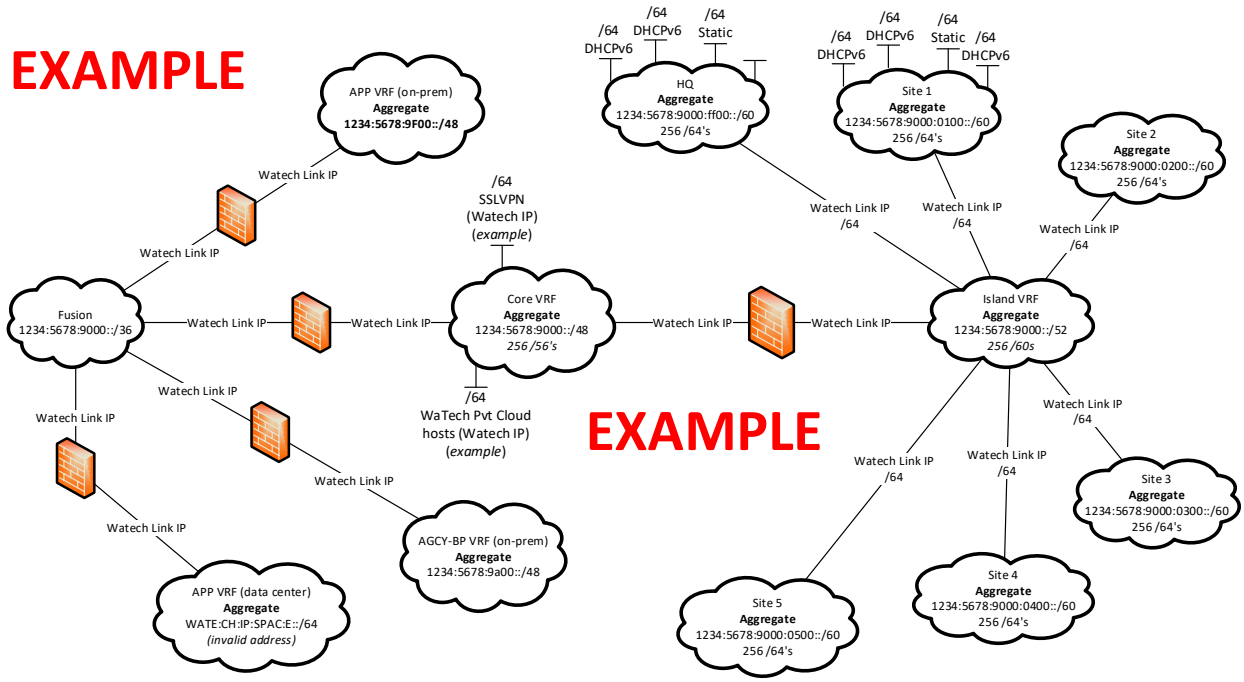
[Back to REFERENCES]

Example /36 Broken into /48 into /56



[Back to REFERENCES]

Example /36 Broken into /48 into /52 into /60 for site's



[Back to REFERENCES]

Hexidecimal/Binary Chart

Decimal	Hex	Binary
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Back to REFERENCES