EA-05-01-S
State CIO Adopted: June 24, 2024
TSB Approved: June 24, 2024
Sunset Review: June 24, 2024

Replaces:
N/A

WaTech
Washington Technology Solutions

STANDARD FOR IMPLEMENTATION OF IPV6

See Also:
RCW 43.105.054 OCIO Governance
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (22) "State agency"

1. **Agencies must acquire their IPv6 address block allocations from WaTech. See Enterprise Service: IP Address Management Standard.**

    a. Each Agency is allocated a /36 prefix.

    b. WaTech will not support Network Address Translation Prefix Translation (NAT-PT), NAT64, NAT 4 to 6 for customers for WAN transport and connectivity service. Agencies may utilize these options for LAN connections under their own agency's support.

    c. Agencies must use nibble boundaries to maintain summarization for routing purposes. See Table 1 Nibble Boundaries.

    d. WaTech will designate link-local addresses on customer handoff links for ease of identification and troubleshooting.

    e. K-20 organizations are exempt from this standard as per RCW 43.41.391.

2. **Agencies must apply static addressing to all authentication servers.**

    a. Servers and storage need to have static IPv6 addresses assigned to ensure functionality and availability. If servers are not manually configured with an IPv6 address, a new IPv6 address is autoconfigured whenever a Network Interface Card (NIC) is replaced.

    b. Give servers statically assigned prefixes.

3. **Agencies must ensure that address schemes:**

    a. Map to the agency's network topology.

    b. Meet current agency requirements as well as state policy and standard requirements.

    c. If a link-local address is manually configured it must be in an easily readable

format. This will make verifying or troubleshooting routes easier.

4. **Agencies must use a hierarchical addressing plan:**

    a. Agencies can use nibble boundaries on internal LANs with a prefix greater than a /48. See Table 1 Nibble Boundaries. See Network Address Allocation Examples below.

    b. Agencies must plan for their summarization based off the /48 VRF or edge device connection. See RFC 6177: IPv6 Address Assignment to End Sites (rfc-editor.org)

5. **Tunnels need appropriate security protocols in place. See NIST 800-119 Guidelines for the Secure Deployment of IPv6. Agencies must consider the following items for tunneling into an internal agency LAN (see IPv6 Guidelines.)**

6. **Agencies must implement a deny all or allow by exception IPv6 ruleset. See the Firewall Standard and NIST 800-119 Guidelines for the Secure Implementation of IPv6.**

7. **Agencies must apply current network security standards and polices with the implementation of IPv6 (see NIST 800-53).**

    a. Network device management security must include:

        i. Apply Access Control Lists (ACLs) to Virtual Teletype (VTY) lines.

        ii. Apply ACLs to Simple Network Management Protocol (SNMP) communities/groups.

        iii. Configure Internet Control Message Protocol (ICMP) error message rate limiting on routers.

    b. Routing security must:

        i. Ensure access control lists permit router advertisement (RA) and router solicitation (RS) traffic.

        ii. Manually assign the link-local addresses.

    c. WaTech will suppress router advertisements, unreachable, and redirects on the network edges and where appropriate.

        i. Agencies may suppress unreachable within their internal networks, including all networks behind the agency's firewalls.

    d. Filter internal-use addresses at the agency border.

e. For end user devices, use dynamic host configuration protocol addressing (IPV6 DHCP). Agencies may not use SLAAC.

f. WaTech will not support transition mechanisms on WaTech equipment, including:

   i. ISATAP.

   ii. NAT64 (/96).

   iii. Teredo.

g. All IPv6 interface gateways must be a /64 industry standard.

8. **Agencies will maintain the following nibble boundaries as this will help prevent unintentional overlapping of addresses between subnets (See Table 1 Nibble Boundaries):**

   a. Interfaces.

   b. Sites.

   c. Agencies will start with a /48 prefix on edge routing devices connecting to the state core networks. Aligns with RFCs and industry standards.

REFERENCES

1. RCW 43.41.391 K-20 network.
2. Enterprise Service: IP Address Management Standard
3. RFC 6177: IPv6 Address Assignment to End Sites (rfc-editor.org)
4. NIST SP 800-119, Guidelines for the Secure Deployment of IPv6 | CSRC (nist.gov)
5. Definition of Terms Used in WaTech Policies and Reports.
6. Table 1 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
11. NIST Cybersecurity Framework Mapping:
    - Identify.Governance-1 (ID.GV-1): Organizational information security policy is established and communicated.
    - Identify.Supply Chain-3 (ID.SC-3): Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.

- Protect.Identity Management and Access Control-1 (PR.AC-1): Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.
- Protect.Identity Management and Access Control-3 (PR.AC-3): Remote access is managed.
- Protect.Identity Management and Access Control-5 (PR.AC-5): Network integrity is protected, incorporating network segregation where appropriate.
- Protect.Information Processes and Procedures-1 (PR.IP-1): A baseline configuration of information technology/industrial control systems is created and maintained.
- Protect.Information Processes and Procedures-3 (PR.IP-3): Configuration change control processes are in place.
- Detect.Anomolies and Events-1 (DE.AE-1): A baseline of network operations and expected data flows for users and systems is established and managed.

CONTACT INFORMATION

- For questions about this policy, please contact the WaTech Policy Mailbox.
- For technical assistance, please submit a service ticket.

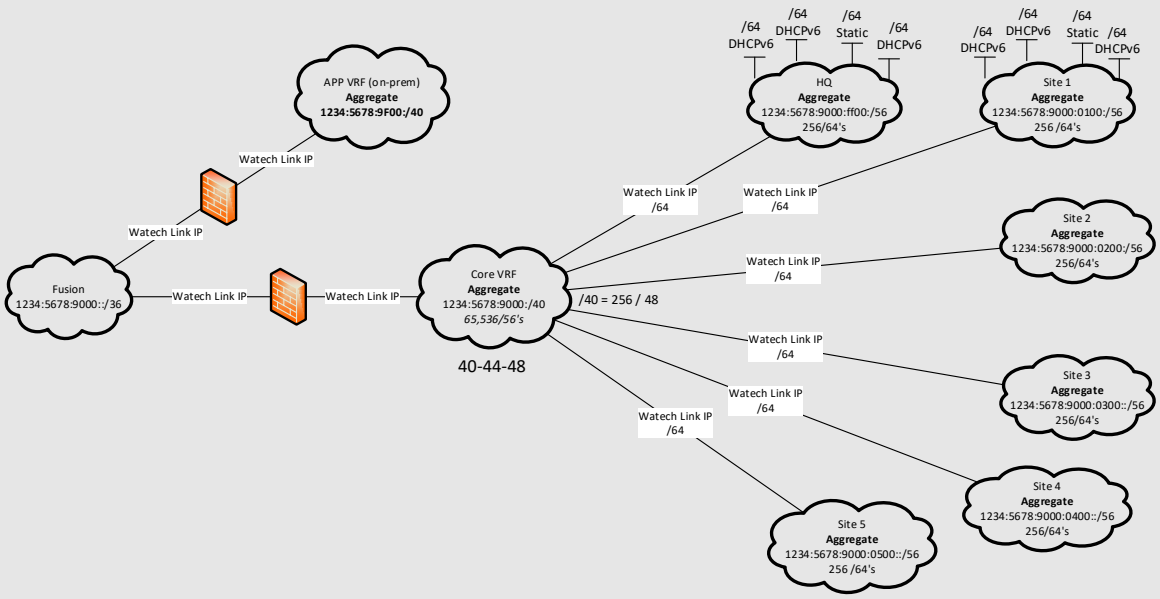
Table 1 Nibble Boundaries

/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)

Network Address Allocation Examples

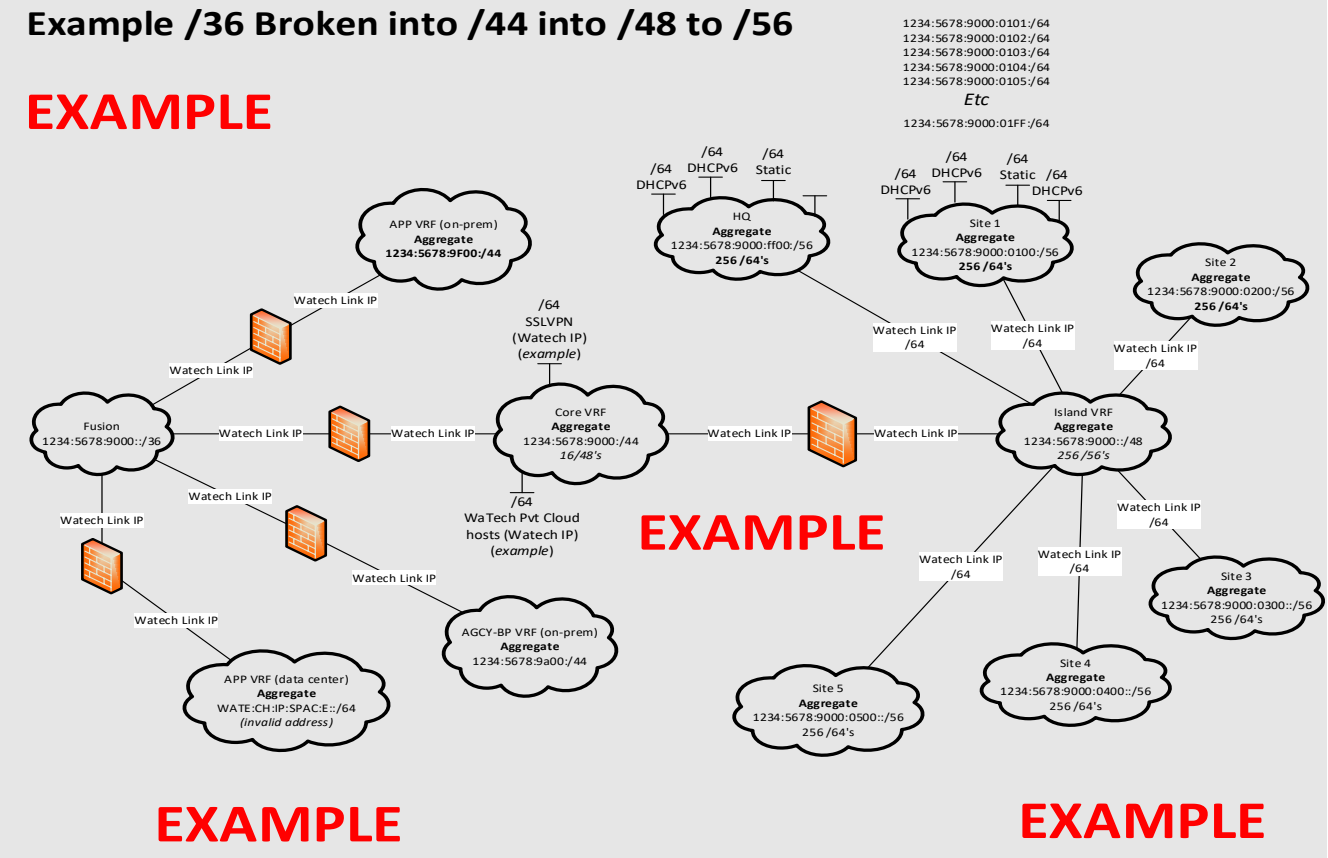
EXAMPLE EXAMPLE

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

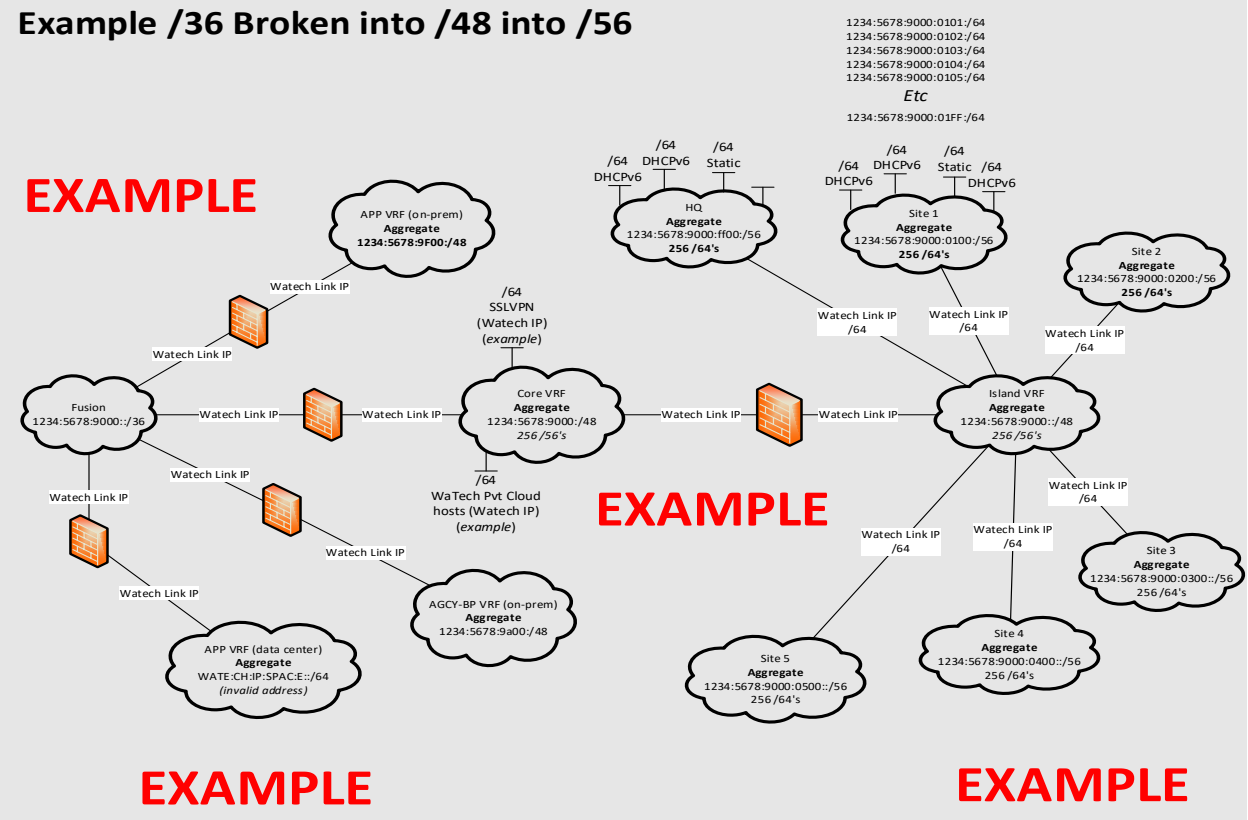


EXAMPLE EXAMPLE

[Back to REFERENCES]

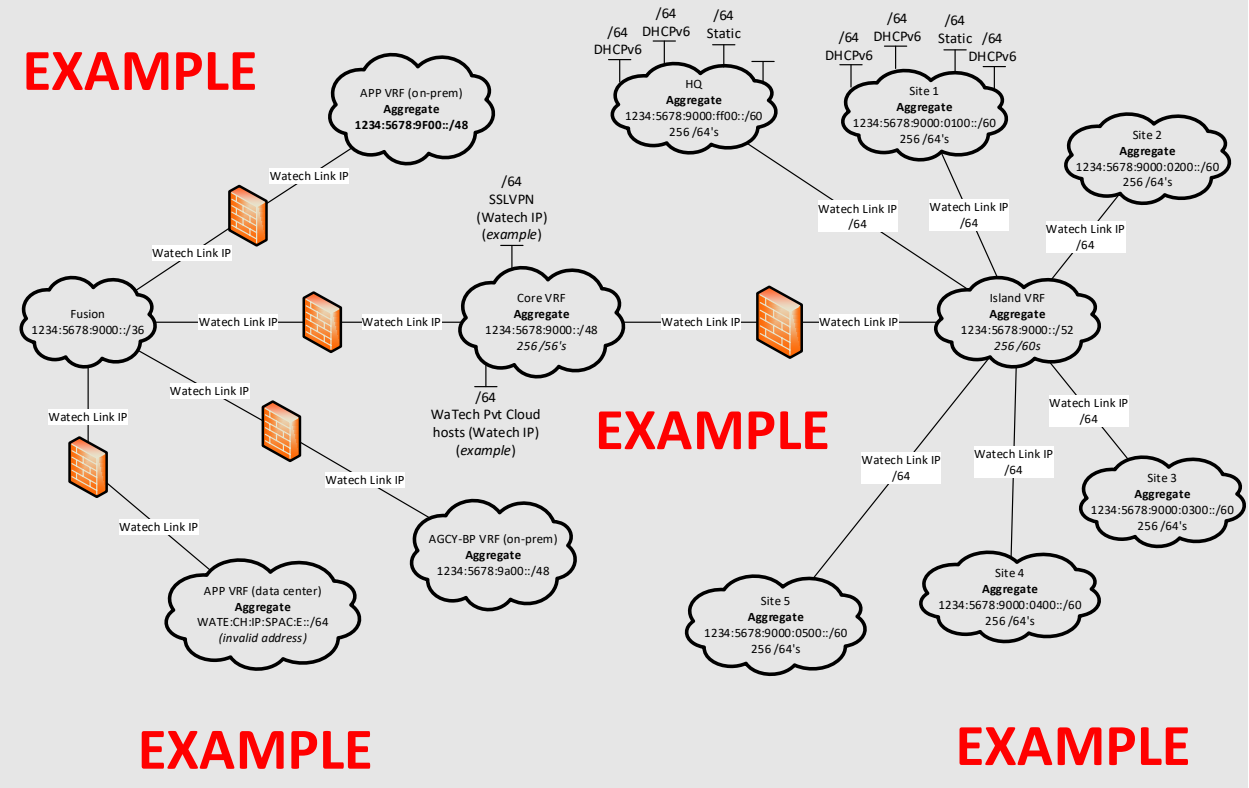


[Back to REFERENCES]



[Back to REFERENCES]

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



[Back to REFERENCES]