NIH Network Device Standard

Purpose: This standard establishes minimum requirements for network devices (e.g. switches or routers) that interoperate with the NIH enterprise network (NIHnet). Compliance with this standard is required to ensure the interoperability, performance, reliability and security of NIHnet. Adherence to this standard will enable more rapid enterprise-wide adoption of current and future networking and security capabilities.

Scope: This standard applies to all network devices that comprise or interoperate with NIHnet (wired, wireless, and VPN).

Standard: Network devices interoperating with NIHnet must satisfy the following requirements:

1. **Connection speeds:** device supports 1 Gigabit, 10 Gigabit, 40 Gigabit, and/or 100 Gigabit (or higher) Ethernet connectivity.
2. **Device Management:** device supports encrypted channels (e.g. HTTPS, SSH) for device management.
3. **Dual-homed:** device supports a minimum of two (2) uplink connections to the NIH network.
4. **Fiber optic connections:** device supports both single-mode fiber optic and multi-mode fiber optic connections to the NIH enterprise network.
5. **Internet Protocols:** device supports both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6).
6. **Network Access Control (NAC):** device supports the following protocols and capabilities needed for enterprise NAC:

    a. 802.1X -- IEEE 802.1X authentication and accounting via remote RADIUS servers to authenticate and log devices connecting or disconnecting to switch ports.
    b. 802.1X RFC 3580 -- dynamic VLAN assignments using the 802.1X RFC3580 standard to support NAC enforcement by assigning the guest or blacklist VLANs for unauthorized devices.
    c. 802.1X RFC 3576/5176 -- remote RADIUS disconnection as part of the 3576 and 5176 standards required to perform authorization changes to a currently connected device.
    d. 802.1X MAC Authentication Bypass -- authenticate a device based on its MAC address for devices that cannot support other NAC authentication methods.
    e. 802.1X Multiple Authentication -- authenticate multiple devices per switch port, required to support devices such as virtual machines on a host computer.
    f. 802.1X Open Authentication -- ability to place a port in an authenticated state whenever a device is connected which is required so that NAC can operate in a 'read-only' monitoring mode and the switch can fail open and continue to provide access in case of NAC system failure.
    g. IP Tracking -- ability to identify the IP address of connected devices for the NAC system to properly identify the IP address and hostname of connected devices.
    h. MAC Move -- ability to permit authenticated hosts to move between multiple NAC-enabled ports, required to provide access to a device if the switch failed to delete the original authentication session at the time the device disconnected.

i. Simple Network Management Protocol (SNMP) -- ability to support SNMP v3, or SNMP v1 or v2 with access control lists (ACLs) if SNMP v3 is not supported. This is required for the NAC system to perform enforcement actions such as manually assigning a device to a blacklist or forcing a disconnection.

7. **Network Time Protocol (NTP):** device uses NTP for clock synchronization within 10 milliseconds of Coordinated Universal Time (UTC).
8. **Port-channel:** device supports the bundling of multiple links to form a port-channel for layer-2 connections or independent layer-3 connections. This includes support of link aggregation required to interoperate with NIHnet.
9. **Quality of Service (QoS):** device can classify and give precedence to priority network traffic such as Voice-over-IP (VOIP).
10. **Routing Protocols:** device, for layer-3 connections, supports the following routing protocols:
    a. Border Gateway Protocol (BGP) version 2 or 3, including support for:
       - Anti-Spoofing of Network routes
       - Minimum of 2 BGP peer points
       - Default Route Originated to IC
       - IPv4 and IPv6 route exchange
       - Encryption of BGP route exchange

    b. Static Routing, including support for:
       - Anti-Spoofing of Network routes
       - Minimum of 2 Static Route peer points

    Note: Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) routing protocols are not supported on the NIH backbone, but may be used on an IC's internal network.
11. **Security:** device is configured and maintained in accordance with all applicable Federal, HHS and NIH security policies and practices (e.g., currently supported by the vendor, at current patch level, etc.).
12. **Spanning Tree Protocol (STP) controls:** device, for layer-2 connections, supports the following STP controls:
    a. Root Guard – controls which of the device's ports may use as a network root bridge.
    b. BPDU Guard – ensures bridge protocol data unit (BPDU) packets, used to dynamically control network topology, are only received from authorized ports (e.g., not access ports connected to end-user devices).
    c. BPDU Filter – controls which of the device's ports may both send and receive BPDU packets.
    d. Rapid-PVST – allows for faster Spanning-Tree calculations and convergence in response to layer-2 network topology changes.
    e. Storm Control – device prevents the excessive proliferation of broadcast, multicast, and unknown unicast packets.

13. **Syslog:** device supports syslog protocol to send event messages to a logging server.
14. **Virtual local-area network (VLAN):** device supports layer-2 VLANs and has IEEE.802.1Q capability to support multiple VLAN connections.
15. **Virtual Routing and Forwarding (VRF):** device supports VFR to enable internal network segmentation in conjunction with the NIH Network's Multiprotocol Label Switching (MPLS) backbone.
16. **Wireless Network:** security implementation requirements are outlined in Appendix A.

Compliance

All new network devices must immediately comply this standard. Existing (legacy) devices must be upgraded (or replaced) to comply with this standard within three (3) years of the standard's approval date noted below.

Where deviations from this standard are necessary, requests for exceptions should be submitted to nihciocommunications@nih.gov, and will be evaluated by the NIH Chief Information Officer (CIO). A waiver request must include a business case for the exception that specifies how the enforcement of this standard would restrict the mission of NIH and the specific compensating controls that will be implemented.

Approved

Andrea T. Norris -S

Digitally signed by Andrea T. Norris -S
Date: 2018.10.23 10:24:44 -04'00'

Andrea T. Norris
NIH Chief Information Officer

Appendix A: NIH Wireless Network Implementation Requirements

Definitions:

a. **General NIH Users:** NIH staff members that use the NIH Virtual Private Network (VPN) or 802.1X solution.
b. **Guests:** Users of the NIH Guest Network, which provides internet access but no access to the NIH network except for NIH public websites.
c. **Hand-Held Users:** Users with hand-held devices that need wireless access, but don't require VPN or web authentication, i.e., need a point-to-point connection to communicate with the mobile device server.
d. **Wireless Enabled Devices:** Devices that require wireless access to function (typically need limited access to communicate with a management or monitoring server).

1. **Compartmentalization:** Wireless networks and subnets (Internet Protocol [IP] addresses) must be segregated to allow application of appropriate authentication, intrusion detection, and incident response methods necessary to identify and differentiate a wireless event from a wired event.

   a. **All Wireless Local Area Network (WLAN)** IP ranges must be segregated from the rest of NIH network.
   b. **WLANs** must be segregated via a separate physical network or a Virtual Local Area Network (VLAN) that contains all wireless access points for any specific network or subnet and no other enterprise resources. This is referred to as a **Wireless DMZ (WDMZ)**.
   c. WDMZs shall be isolated with a firewall or appropriate router configuration to establish an intermediate network.
   d. A unique IP range dedicated to the intermediate network shall be assigned to support wireless user IP addresses when connecting to the WDMZ.
   e. The NIH network shall be isolated from wireless guest users, and Internet access for guest users will be implemented outside of the NIH network perimeter.
   f. **Wireless Intrusion Detection System (IDS)** sensors shall be installed at sensitive network areas.
   g. Ad hoc connections between endpoint wireless devices without a centralized infrastructure are prohibited.

2. **Encryption:** Both the wireless network infrastructure and NIH-managed mobile devices shall support end-to-end encryption sufficient to meet the following conditions:

   a. The NIH VPN or WPA2 shall provide a level of encryption sufficient to meet NIST SP 800-48, Guide to Securing Legacy IEEE 802.11 Wireless Networks (as amended) and multi-vendor interoperability requirements.
   b. Only encryption methods that are compliant with the FIPS 140-2 shall be used, e.g., Advanced Encryption Standard (AES) or Triple-Data Encryption Standard (3DES). In user and routing areas, where known sensitive data transmission occurs, appropriate encryption algorithms shall be employed.
   c. No encryption level is required for wireless guest internet access only.
   d. The use of pre-shared keys is permitted for devices that cannot support user authentication.

3. **Access Control:**

   a. All NIH WLANs, except Wireless Guest Internet access, must provide an authentication mechanism referenced to a central credential authority such as Active Directory. This must be done through the NIH VPN solution or 802.1X.
   b. Wireless administrators will ensure that all vendor default usernames and passwords are removed from access point devices.

4. **Network Management:**

   a. The NIH Center for Information Technology will manage all NIH WLAN infrastructure equipment.
   b. The NIH wireless network infrastructure will be maintained under a documented configuration management program.
   c. Access points will be installed in a safe, adequately monitored location to prevent unauthorized access and physical tampering. These devices will not be placed in easily accessible public locations.