pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Network Router and Switch Requirements

ITP Number GEN-NET002B	**Effective Date** September 22, 2006
Category Network	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** October 2019

1. Purpose

The purpose of router and switch technologies is to protect the confidentiality of information, safeguard the integrity of information, establish common equipment platforms/standards, and ensure access to information.

2. Required Features

- Provide a modular, standard 19-inch rack mountable design
- Co-exist with IPv4 for conversion to IPv6
- Support VOIP and QOS. New deployments must implement QOS.
- Support IPv6
- Provide port mirroring
- Provide an out-of-band port management option. Must comply with all applicable regulatory requirements. (ex: Multi-Factor Authentication)
- Enable wire-speed performance for current services
- Support port channeling
- Support access control lists
- Support the ability to turn off telnet access
- Provide the ability to support Power over Ethernet for Intermediate Distribution Frame (IDF) implementations
- Support current SNMP version(s) v2 and v3:
  - SNMP support shall include the standard Internet MIB-II current and back level
  - SNMP read-only and read-write access shall be independently configurable, including separate community strings and separate access lists (or equivalent) for restricting access by IP address
- Provide the ability to disable web-based or GUI configuration features. If web-based interfaces are enabled, provide for HTTPS-only access using a TLS version that adheres to ITP-SEC031 *Encryption Standards for Data in Transit*.
- Provide the ability to display accurate octet and packet counters per interface, viewable from the CLI and from SNMP
- Support encrypted, secure in-band management access using current SSH version
- Allow, via optional configuration parameters, centralized in-band login management for operators and administrator using either TACACS or RADIUS
- Provide the ability to interface with Radius security
- Support import and export of full configuration in readable ASCII text format
- Support password recovery procedures for any configurable password on routers and switches

3. Evaluation Considerations

When evaluating router and switch technology, agencies are to consider the following criteria during their selection process:

- Support for the Commonwealth's Identity Management solution and common security architecture
- Robustness and usability of monitoring and reporting capabilities.
- Total cost of ownership. Including but not limited to:

  - Management costs
  - Support and licensing costs
  - Sparing strategies within and across agencies with a goal to standardize and leverage across the commonwealth
- Robustness and usability of tool and utility administration
- Robustness and usability of user role, privilege and access control administration
- Degree of support for advanced multicast and unicast management
- Performance and throughput capabilities of the device

4. Supported Protocols

- Full TCP/IP Suite
- 3DES – Data Encryption Standard using three different keys
- 802.1Q VLAN
- 802.1X
- 802.1P (QOS)
- 802.3 1000 Base-TX (Gigabit Ethernet)
- ATM – Asynchronous Transfer Mode
- ARP - Address Resolution Protocol
- BGP – Border Gateway Protocol
- CDP - Cisco Discovery Protocol
- CHAP - Challenge Handshake Authentication Protocol
- DHCP Relay – Dynamic Host Configuration Protocol / Relay
- DHCP Server – Dynamic Host Configuration Protocol / Server
- EIGRP - Enhance Interior Gateway Routing Protocol
- Ethernet LAN
- GRE – Generic Routing Encapsulation Protocol
- HDLC - High-Level Data Link Control
- HSRP – Hot Stand-by Router Protocol
- ICMP -Internet Control Message Protocol
- IGMP - Multicast Internet Group Management Protocol
- IKE – Internet Key Exchange
- IPSec – Internet Protocol Security
- IPSec VPN – Internet Protocol Security – Virtual Private Network
- IS-IS – Link State Routing Protocol Classless Routing Protocol Intermediate System to Intermediate System
- L2F - Layer 2 Forwarding Protocol
- L2TP – Layer 2 VPN Layer 2 Tunneling Protocol
- LAPB - Link Access Procedure Balanced
- LLDP-MED Link Layer Discovery Protocol Media Endpoint Discovery
- LLDP - Link Layer Discover Protocol
- MGCP - Media Gateway Control Protocol Megaco (H.248)
- MLPPP – Multi-Link Point-to Point Protocol
- MPLS – Multi-Protocol Label Switching
- Multicast PIM-DM – Protocol Independent Multicast – Dense Mode
- Multicast PIM-SM – Protocol Independent Multicast – Sparse Mode (RFC 2362)
- NAT/PAT - Network Address Translation/Port Address Translation support
- NFS Network File System
- NTP – Network Time Protocol (Refer to ITP-NET017 *Network Timing Protocol* for detailed guidance)

- OSPF – Open Shortest Path First
- PAP - Password Authentication Protocol
- PPP - Point to Point Connections
- PPTP - Point to Point Tunneling Protocol
- PVlan – Cisco implementation of Private Virtual Lan
- RARP Reverse Address Resolution Protocol
- Rem Br (STP over PPP)
- RTP - Real-time Transport Protocol
- RVP – A Presence and Instant Messaging Protocol
- SDP - Session Description Protocol
- SIP - Session Initiated Protocol
- SMB - Server Message Block
- STP - Spanning Tree Protocol
- STUN – Session Traversal Utilities for NAT
- SSH – Secure Shell
- Static Routing
- SCCP - Skinny Client Control Protocol
- TCP -Transmission control Protocol
- UDP – User Datagram Protocol
- WCCP - Web Cache Communication Protocol
- UDP - User Datagram Protocol
- VRRP – Virtual Router Redundancy Protocol
- VTP - VLAN Trunking Protocol

5. Related ITPs/Other References

Definitions of associated terms of this policy are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/Glossary.aspx

Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx

- Management Directive 205.34 *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- ITP-NET002 *Network Router and Switch Technology Standards*
- ITP-NET017 *Network Timing Protocol*
- ITP-SEC031 *Encryption Standards for Data in Transit*

6. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

7. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov for Commonwealth personnel and on the Office of Administration public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx. Questions regarding this publication are to be directed to RA-ITCentral@pa.gov.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision
Original	09/22/2006	Base Document
Revision	12/20/2010	ITP Refresh
Revision	10/31/2018	ITP Reformat Shortened policy title name Updated Required Features Updated Evaluation Considerations Updated Supported Protocols