

**Information Technology Supporting Documentation
Commonwealth of Pennsylvania
Governor's Office of Administration/Office for Information Technology**

Document Number:	GEN-NET002B	
Document Title:	Network Router and Switch Hardware/Software Business Requirements	
Issued by:	Deputy Secretary for Information Technology	
Date Issued:	September 22, 2006	Date Revised: December 20, 2010
Domain:		
	Network	
Discipline:		
	Physical Network	
Technology Area:		
	Network Router and Switch Technology	
Referenced by:		
	ITP-NET002	
Revision History		
Date:	Description:	
12/20/2010	ITP Refresh	

Introduction:

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.

The requirements and standards listed in this General Information Document comply with the policies and standards established in ITP-NET002, *Network Router and Switch Technology Standards* and ITP-NET002A, *Network Router and Switch Technology - Product and Platform Standards*. In addition, the router and switch technologies adopted by the Commonwealth comply with IEEE 802.3 standards.

Required Features:

All Commonwealth router and switch technology implementations are required to support the following features:

- Provide a modular, standard 19-inch rack mountable design.
- Co-exist with IPv4 for conversion to IPv6.
- Support VOIP and QOS.
- Support IPv6.
- Provide port mirroring.
- Provide an out-of-band port management option.
- Enable wire-speed performance for current services.
- Contain integrated hardware-based encryption.
- Contain port channeling.
- Support access control lists.
- Support the ability to turn off telnet access.
- Provide the ability to support Power over Ethernet.
- Support current SNMP version:
 - 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.
- Support out-of-band serial RS-232C compatible access to the CLI; the serial port access shall be protected by a configurable password.
- 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.

- Contain inbuilt secure access features that support 128-bit SSL data encryption and secure remote access beyond the MAN using SSL VPN or IPSEC VPN.
- Provide the ability to interface with Radius security.
- Provide text-based CLI accessibility from terminal-emulation software operating on a wide variety of platforms (including UNIX, Macintosh, and Windows).
- Accommodate configuration can be uploaded/downloaded to and from an external ASCII file using standard Internet protocols.
- Support password recovery procedures for any configurable password on routers and switches.

Evaluation Considerations:

Additionally, 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.
- 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.

Supported Protocols:

Full TCP/IP Suite

3DES – Data Encryption Standard using three different keys

802.1Q VLAN

802.1X

802.1P (QOS)

802.3 100 Base-TX (Fast Ethernet - 2 port minimum)

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

DLSW – Data Link Switching (Cisco)

DDR – Dial-on-Demand Routing

EGP – Exterior Gateway Protocol

EIGRP - Enhance Interior Gateway Routing Protocol

Ethernet LAN

Frame Relay

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

IGRP – Interior Gateway Routing Protocol

IKE – Internet Key Exchange

IMA – Inverse Multiplexing over ATM

IPSec – Internet Protocol Security

IPSec VPN – Internet Protocol Security – Virtual Private Network

ISL Trunking encapsulation – Internet Switch Link (Cisco proprietary)/Trunking encapsulation

ISDN – Integrated Services Digital 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
NCP Netware Core Protocol
NFS Network File system
NTP – Network Time Protocol
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
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
VoATM – Voice over ATM
VoFR – Voice over Frame Relay
VRRP – Virtual Router Redundancy Protocol
VTP - VLAN Trunking Protocol