JUNIPER NETWORKS | Engineering Simplicity

Junos® OS

Standards Reference

Published
2024-12-19

JUNOS

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos® OS Standards Reference

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

Use this guide to identify the standards substantially supported by Junos OS.

1

PART

Overview

CHAPTER 1

Accessing Standards Documents

IN THIS CHAPTER

Accessing Standards Documents on the Internet

The following information about the location of standards on the Internet is accurate as of March 2018. It is subject to change and is provided only as a courtesy to the reader.

Information about accessing MIBs is provided in the entry for each MIB.

- ANSI standards are published by the American National Standards Institute. You can search for specific standards at http://webstore.ansi.org/.
- FRF (Frame Relay Forum) standards are published by the Broadband Forum. They can be accessed at https://www.broadband-forum.org/component/sppagebuilder/?view=page&id=185.
- GR (Generic Requirements) standards are published by Ericsson (Telcordia is now part of Ericcson). Information about them can be accessed by clicking the “Documents” link at http://telecom-info.telcordia.com/site-cgi/ido/.
- IEEE standards are published by the Institute of Electrical and Electronics Engineers. They can be accessed at http://ieeexplore.ieee.org/browse/standards/get-program/page/.
- ISO/IEC standards are published by the International Organization for Standardization/International Electrotechnical Commission. They can be accessed at https://www.iso.org/isoiec-27001-information-security.html.
- INCITS standards are published by the InterNational Committee for Information Technology Standards. They can be accessed at http://www.incits.org/standards-information/.
- Internet drafts are published by the Internet Engineering Task Force (IETF). They can be accessed at https://www.ietf.org/standards/ids/ .
- ITU–T Recommendations are published by the International Telecommunication Union. They can be accessed at http://www.itu.int/rec/T-REC.

NOTE: Junos OS supports ITU-T Y.1731 (year 2006 version) that defines Ethernet service OAM features for fault monitoring, diagnostics, and performance monitoring.

- RFCs are published by the IETF. They can be accessed at https://www.ietf.org/standards/rfcs/.

2

PART

Supported Standards

CHAPTER 2

Chassis and System Standards

IN THIS CHAPTER

Supported BFD Standards

Junos OS substantially supports the following standards for Bidirectional Forwarding Detection (BFD).

- RFC 5880, *Bidirectional Forwarding Detection*. (Partial support—Echo and Demand mode is not supported).
- RFC 5881, *Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6* (Fully compliant).
- RFC 5882, *Generic Application of Bidirectional Forwarding Detection (BFD).*
- RFC 5883, *Bidirectional Forwarding Detection (BFD)* (Fully compliant).
- RFC 5884, *Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)*. (Partial support—Packets from egress to ingress come with singlehop port and while sending packets, the router alert option is used setting TTL to 1).
- RFC 5885, *Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)*. (Fully compliant)
- RFC 7130, *Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces, also called micro-BFD for sub-second failure detection*

Supported BOOTP and DHCP Standards

The Junos operating system (Junos OS) substantially supports the following RFCs, which define standards for the bootstrap protocol (BOOTP) and the Dynamic Host Control Protocol (DHCP).

- RFC 951, *BOOTSTRAP PROTOCOL (BOOTP)*
- RFC 1001, *PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: CONCEPTS AND METHODS*
- RFC 1002, *PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: DETAILED SPECIFICATIONS*
- RFC 1035, *DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION*
- RFC 1534, *Interoperation Between DHCP and BOOTP*
- RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*
- RFC 1700, *ASSIGNED NUMBERS*
- RFC 2131, *Dynamic Host Configuration Protocol*

  DHCP over virtual LAN (VLAN)-tagged interfaces is not supported.
- RFC 2132, *DHCP Options and BOOTP Vendor Extensions*
- RFC 3046, *DHCP Relay Agent Information Option*
- RFC 3118, *Authentication for DHCP Messages*

  Only Section 4, “Configuration token,” is supported.
- RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
- RFC 3397, *Dynamic Host Configuration Protocol (DHCP) Domain Search Option*
- RFC 3633, *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*
- RFC 3925, *Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)*
- RFC 4649, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option*

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported Mobile IP Standards

Junos OS supports only static configuration of home agent addresses and IP tunnels; dynamic configuration is not supported. Junos OS does not support the Mobile IP foreign agent, accounting, QoS, policy, data path, or logical interfaces per mobile node (for a mobile subscriber).

Junos OS substantially supports the following RFCs, which define standards for Mobile IP.

- RFC 2794, *Mobile IP Network Access Identifier Extension for IPv4*
- RFC 3024, *Reverse Tunneling for Mobile IP, revised*
- RFC 3344, *IP Mobility Support for IPv4*

  Only the Mobile IP home agent is supported.
- RFC 3543, *Registration Revocation in Mobile IPv4*
- RFC 4433, *Mobile IPv4 Dynamic Home Agent (HA) Assignment*

The following RFC does not define a standard, but provides information about Mobile IP. The IETF classifies it as "Informational."

- RFC 2977, *Mobile IP Authentication, Authorization, and Accounting Requirements*

  Accounting is not supported.

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported Network Management Standards

Junos OS supports the majority of network management features defined in the following standards documents.

- Extended Security Options (ESO) Consortium, *ESO Consortium MIB*.

  As of February 2011, the text of this MIB is accessible at http://www.snmp.com/eso/esoConsortiumMIB.txt.
- Institute of Electrical and Electronics Engineers (IEEE) Standard 802.3ad, *Aggregation of Multiple Link Segments* (published as Clause 43 in Section 3 of the 802.3 specification)

Only the following MIB objects are supported:

- `dot3adAggPortDebugActorChangeCount`
- `dot3adAggPortDebugActorSyncTransitionCount`
- `dot3adAggPortDebugMuxState`
- `dot3adAggPortDebugPartnerChangeCount`
- `dot3adAggPortDebugPartnerSyncTransitionCount`
- `dot3adAggPortDebugRxState`
- `dot3adAggPortListTable`
- `dot3adAggPortStatsTable`
- `dot3adAggPortTable`
- `dot3adAggTable`
- `dot3adTablesLastChanged`

- Integrated Local Management Interface (ILMI) MIB in the *Integrated Local Management Interface (ILMI) Specification, Version 4.0*.

  This document is accessible at https://www.broadband-forum.org/component/sppagebuilder/?view=page&id=185 under ATM Forum Technical Specifications.

  Only the `atmfMYIPNmAddress` and `atmfPortMyIfname` objects are supported.

- Internet Assigned Numbers Authority (IANA), *IANAiftype Textual Convention MIB* (referenced by RFC 2863, *The Interfaces Group MIB*)

  As of February 2011, the text of this MIB is accessible at http://www.iana.org/assignments/ianaiftype-mib.

- RFC 1122, *Requirements for Internet Hosts -- Communication Layers*
- RFC 1155, *Structure and Identification of Management Information for TCP/IP-based Internets*
- RFC 1156, *Management Information Base for Network Management of TCP/IP-based internets*
- RFC 1157, *A Simple Network Management Protocol (SNMP)*
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*

  Only the following MIB objects are supported:

  - `isisAdjIPAddr`

- isisAreaAddr
- isisCirc
- isisCircLevel
- isisIPRA
- isisISAdj
- isisISAdjAreaAddr
- isisISAdjProtSupp
- isisMANAreaAddr
- isisPacketCount
- isisRa
- isisSysProtSupp
- isisSummAddr
- isisSystem

- RFC 1212, *Concise MIB Definitions*
- RFC 1213, *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*

  Only the following features are supported:

  - Junos OS-specific secured access list
  - Primary configuration keywords
  - MIB II and its SNMP version 2 derivatives, including the following:
    - Interface management
    - IP (except for the ipRouteTable object, which has been replaced by the inetCidrRouteTable object, [RFC 4292, *IP Forwarding MIB*])
    - SNMP management
    - Statistics counters
  - Reconfigurations upon receipt of the SIGHUP signal
  - SNMP version 1 Get and GetNext requests and version 2 GetBulk requests

- RFC 1215, *A Convention for Defining Traps for use with the SNMP*

  Only MIB II SNMP version 1 traps and version 2 notifications are supported.

- RFC 1406, *Definitions of Managed Objects for the DS1 and E1 Interface Types* (obsoleted by RFC 2495)

  The T1 MIB is supported.

- RFC 1407, *Definitions of Managed Objects for the DS3/E3 Interface Type* (obsoleted by RFC 2496)

  The T3 MIB is supported.

- RFC 1471, *The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol*

- RFC 1472, *The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol*

- RFC 1473, *The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol*

- RFC 1657, *Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2*

  The `bgpBackwardTransition` and `bgpEstablished` notifications are not supported.

- RFC 1695, *Definitions of Managed Objects for ATM Management Version 8.0 Using SMIv2* (obsoleted by RFC 2515)

- RFC 1724, *RIP Version 2 MIB Extension*

- RFC 1850, *OSPF Version 2 Management Information Base*

  The following features are not supported:

  - Host Table
  - `ospfLsdbApproachingOverflow` trap
  - `ospfLsdbOverflow` trap
  - `ospfOriginateLSA` trap
  - `ospfOriginateNewLsas` MIB object
  - `ospfRxNewLsas` MIB object

- RFC 1901, *Introduction to Community-based SNMPv2.*

- RFC 1905, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)* (obsoleted by RFC 3416)
- RFC 1907, *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)* (obsoleted by RFC 3418)
- RFC 2011, *SNMPv2 Management Information Base for the Internet Protocol using SMIv2*
- RFC 2012, *SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2*
- RFC 2013, *SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2*
- RFC 2024, *Definitions of Managed Objects for Data Link Switching using SMIv2*
- RFC 2068, *Hypertext Transfer Protocol -- HTTP/1.1*
- RFC 2096, *IP Forwarding Table MIB*

  The `ipCidrRouteTable` object is extended to include the tunnel name when the next hop is through an RSVP-signaled label-switched path (LSP).

  NOTE: RFC 2096 has been replaced by RFC 4292. However, Junos OS currently supports both RFC 2096 and RFC 4292.

- RFC 2115, *Management Information Base for Frame Relay DTEs Using SMIv2*

  Only the `frDlcmiTable` object is supported.

- RFC 2233, *The Interfaces Group MIB using SMIv2* (obsoleted by RFC 2863)
- RFC 2287, *Definitions of System-Level Managed Objects for Applications*

  Only the following MIB objects are supported:

  - `sysApplElmtRunTable`
  - `sysApplInstallElmtTable`
  - `sysApplInstallPkgTable`
  - `sysApplMapTable`

- RFC 2465, *Management Information Base for IP Version 6: Textual Conventions and General Group*

  IP version 6 (IPv6) and Internet Control Message Protocol version 6 (ICMPv6) statistics are not supported.

- RFC 2466, *Management Information Base for IP Version 6: ICMPv6 Group*
- RFC 2495, *Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types*

  The following MIB objects are not supported:

  - `dsx1FarEndConfigTable`
  - `dsx1FarEndCurrentTable`
  - `dsx1FarEndIntervalTable`
  - `dsx1FarEndTotalTable`
  - `dsx1FracTable`
- RFC 2496, *Definitions of Managed Objects for the DS3/E3 Interface Type*

  The following MIB objects are not supported:

  - `dsx3FarEndConfigTable`
  - `dsx3FarEndCurrentTable`
  - `dsx3FarEndIntervalTable`
  - `dsx3FarEndTotalTable`
  - `dsx3FracTable`
- RFC 2515, *Definitions of Managed Objects for ATM Management*

  The following MIB objects are not supported:

  - `aal5VccTable`
  - `atmVcCrossConnectTable`
  - `atmVpCrossConnectTable`
- RFC 2558, *Definitions of Managed Objects for the SONET/SDH Interface Type* (obsoleted by RFC 3592)
- RFC 2570, *Introduction to Version 3 of the Internet-standard Network Management Framework*

  RFC 2571, *An Architecture for Describing SNMP Management Frameworks*

  Only read-only access is supported.
- RFC 2572, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* (obsoleted by RFC 3412)

Only read-only access is supported.

- RFC 2578, *Structure of Management Information Version 2 (SMIv2)*
- RFC 2579, *Textual Conventions for SMIv2*
- RFC 2580, *Conformance Statements for SMIv2*
- RFC 2662, *Definitions of Managed Objects for the ADSL Lines*
- RFC 2665, *Definitions of Managed Objects for the Ethernet-like Interface Types*
- RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol*

  The following features are not supported:

  - Row creation
  - `Set` operation
  - `vrrpStatsPacketLengthErrors` MIB object
- RFC 2790, *Host Resources MIB*

  Only the following MIB objects are supported:

  - `hrStorageTable` object. The file systems `/`, `/config`, `/var`, and `/tmp` always return the same index number. When SNMP restarts, the index numbers for the remaining file systems might change.
  - Objects in the `hrSystem` group.
  - Objects in the `hrSWInstalled` group.
- RFC 2819, *Remote Network Monitoring Management Information Base*

  Only the following MIB objects are supported:

  - `alarmTable`
  - `etherStatsTable` object for Ethernet interfaces
  - `eventTable`
  - `logTable`
- RFC 2863, *The Interfaces Group MIB*
- RFC 2864, *The Inverted Stack Table Extension to the Interfaces Group MIB*
- RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*

Only the following MIB objects are supported:

- `pingCtlTable`
- `pingMaxConcurrentRequests`
- `pingProbeHistoryTable`
- `pingResultsTable`
- `traceRouteCtlTable`
- `traceRouteHopsTable`
- `traceRouteProbeHistoryTable`
- `traceRouteResultsTable`

- RFC 2932, *IPv4 Multicast Routing MIB*
- RFC 2981, *Event MIB*
- RFC 3014, *Notification Log MIB*
- RFC 3019, *IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol*
- RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*
- RFC 3412, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*
- RFC 3413, *Simple Network Management Protocol (SNMP) Applications*

  The proxy MIB is not supported.
- RFC 3414, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*
- RFC 3415, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*
- RFC 3416, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*
- RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP)*
- RFC 3418, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*

- RFC 3498, *Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures*

  Support is implemented under the Juniper Networks Enterprise branch.

- RFC 3592, *Definitions of Managed Objects for the Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) Interface Type*

- RFC 3635, *Definitions of Managed Objects for the Ethernet-like Interface Types*

  Supports all objects, except `dot3StatsRateControlAbility` and `dot3StatsRateControlStatus` in `dot3StatsEntry` table.

  > **NOTE**: The values of the following objects in `dot3HCStatsEntry` table will be always zero for both 32-bit counters and 64-bit counters:
  >
  > - `dot3HCStatsSymbolErrors`
  > - `dotHCStatsInternalMacTransmitErrors`

- RFC 3811, *Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management*

- RFC 3812, *Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)*

  Only read-only access is supported, and the following features and MIB objects are not supported:

  - MPLS tunnels as interfaces
  - `mplsTunnelCRLDPResTable` object
  - `mplsTunnelPerfTable` object
  - The following objects in the `TunnelResource` table:
    - `mplsTunnelResourceExBurstSize`
    - `mplsTunnelResourceMaxBurstSize`
    - `mplsTunnelResourceMeanBurstSize`
    - `mplsTunnelResourceMeanRate`
    - `mplsTunnelResourceWeight`

  The `mplsTunnelCHopTable` object is supported on ingress routers only.

NOTE: The branch used by the proprietary LDP MIB (`ldpmib.mib`) conflicts with RFC 3812. `ldpmib.mib` has been deprecated and replaced by `jnx-mpls-ldp.mib`.

- RFC 3813, *Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)*

  Only read-only access is supported, and the following MIB objects are not supported:

  - `mplsInSegmentMapTable`
  - `mplsInSegmentPerfTable`
  - `mplsInterfacePerfTable`
  - `mplsOutSegmentPerfTable`
  - `mplsXCDown`
  - `mplsXCUp`

- RFC 3815, *Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)*

  Only the following MIB objects are supported:

  - `mplsLdpLsrID`
  - `mplsLdpSesPeerAddrTable`

- RFC 3826, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*

- RFC 4001, *Textual Conventions for Internet Network Addresses*

- RFC 4087, *IP Tunnel MIB*

  Supports MIB objects with `MAX-ACCESS` of read-only in the following tables:

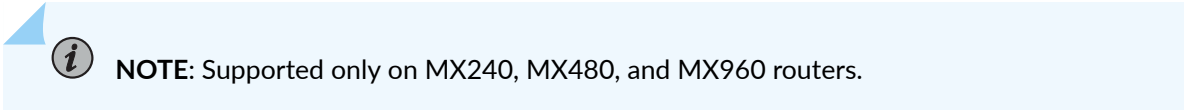
  - `tunnelIfTable`
  - `tunnelInetConfigTable`

- RFC 4133, *Entity MIB*

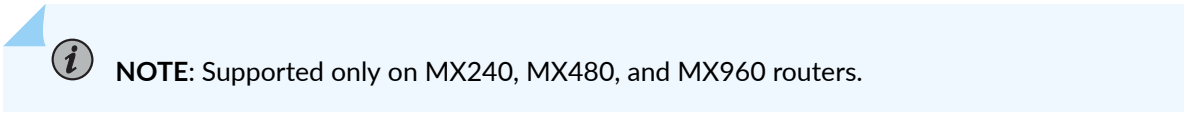
  Supports tables and objects except:

  - `entityLogicalGroup` table
  - `entPhysicalMfgDate` and `entPhysicalUris` objects in `entityPhysical2Group` table

- entLPMappingTable and entPhysicalContainsTable in entityMappingGroup table
- entityNotoficationsGroup table



- RFC 4188, *Definitions of Managed Objects for Bridges*
- RFC 4268, *Entity State MIB*



- RFC 4292, *IP Forwarding MIB*

  Supports the following table and associated MIB objects:

  - inetCidrRouteTable
  - inetCidrRouteNumber
  - inetCidrRouteDiscards

- RFC 4382, *MPLS/BGP Layer 3 Virtual Private Network (VPN) MIB*

  Supports the following scalar objects and tables:

  - mplsL3VpnConfiguredVrfs
  - mplsL3VpnActiveVrfs
  - mplsL3VpnConnectedInterfaces
  - mplsL3VpnNotificationEnable
  - mplsL3VpnVrfConfMaxPossRts
  - mplsL3VpnVrfConfRteMxThrshTime
  - mplsL3VpnIllLblRcvThrsh
  - mplsL3VpnVrfTable
  - mplsL3VpnVrfPerfTable
  - mplsL3VpnVrfRteTable
  - mplsVpnVrfRTTable

- Internet draft draft-ietf-bfd-mib-02.txt, *Bidirectional Forwarding Detection Management Information Base*

  Only read-only access is supported, and the `bfdSessDown` and `bfdSessUp` traps are supported. Objects in the `bfdSessMapTable` and `bfdSessPerfTable` tables are not supported. The MIB that supports this draft is `mib-jnx-bfd-exp.txt` under the Juniper Networks Enterprise `jnxExperiment` branch.

- RFC 4273, *Definitions of Managed Objects for the Fourth Version of Border Gateway Protocol (BGP-4), Second Version*

  Only the following MIB objects are supported:

  - `jnxBgpM2PrefixInPrefixes`
  - `jnxBgpM2PrefixInPrefixesAccepted`
  - `jnxBgpM2PrefixInPrefixesRejected`

- RFC 4444, *Management Information Base for Intermediate System to Intermediate System (IS-IS)*

  Only the following tables are supported:

  - `isisISAdjAreaAddrTable`
  - `isisISAdjIPAddrTable`
  - `isisISAdjProtSuppTable`
  - `isisISAdjTable`

- RFC 4741, *NETCONF Configuration Protocol* (RFC 4741 is obsoleted by RFC 6241)
- RFC 4742, *Using the NETCONF Configuration Protocol over Secure Shell (SSH)* (RFC 4742 is obsoleted by RFC 6242)
- RFC 5424, *The Syslog Protocol*
- RFC 5601, *Pseudowire (PW) Management Information Base (MIB)*
- RFC 5603, *Ethernet Pseudowire (PW) Management Information Base (MIB)*
- Internet draft draft-ietf-msdp-mib-08.txt, *Multicast Source Discovery protocol MIB*

  The following MIB objects are not supported:

  - `msdpBackwardTransition`
  - `msdpEstablished`
  - `msdpRequestsTable`

- RFC 6020, *YANG - A data modeling language for NETCONF*
- RFC 6241, *Network Configuration Protocol (NETCONF)* (RFC 6241 obsoletes RFC 4741)

  The following features are not supported:

  - Advertisement of NETCONF 1.1 capabilities during session establishment
  - `:confirmed-commit:1.1` capability, which includes the `<cancel-commit>` operation and the `<persist>` and `<persist-id>` parameters for the `<commit>` operation
- RFC 6242, *Using the NETCONF Protocol over Secure Shell (SSH)* (RFC 6242 obsoletes RFC 4742)
- RFC 6527, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol Version 3 (VRRPv3)*

  The following features are not supported:

  - Row creation
  - `Set` operation
  - `vrrpv3StatisticsPacketLengthErrors` MIB object
  - `vrrpv3StatisticsRowDiscontinuityTime` MIB object
- RFC 7589, *Using the NETCONF Protocol over Transport Layer Security (TLS) with Mutual X.509 Authentication*
- RFC 8071, *NETCONF Call Home and RESTCONF Call Home*

  Only NETCONF Call Home over SSH is supported.
- Internet draft draft-ietf-ospf-ospfv3-mib-11.txt, *Management Information Base for OSPFv3*

  Only read-only access is supported, and only for the `ospfv3NbrTable` table. The MIB that supports this draft is `mib-jnx-ospfv3mib.txt` under the Juniper Networks Enterprise `jnxExperiment` branch; MIB object names are prefixed with `jnx` (for example, `jnxOspfv3NbrAddressType`).
- Internet draft draft-reeder-snmpv3-usm-3desede-00.txt, *Extension to the User-Based Security Model (USM) to Support Triple-DES EDE in "Outside" CBC Mode*

The following RFCs do not define standards, but provide information about network management. The IETF classifies them variously as "Best Current Practice," "Experimental" or "Informational."

- RFC 1901, *Introduction to Community-based SNMPv2*
- RFC 2330, *Framework for IP Performance Metrics*
- RFC 2934, *Protocol Independent Multicast MIB for IPv4*

- RFC 3410, *Introduction and Applicability Statements for Internet Standard Management Framework*
- RFC 3584, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*
- RFC 5601, *PW-FRAME-MIB*

  Supported on MX Series routers with MPC/MIC interfaces that use the ATM MIC with SFP.
- RFC 5603, *PWE3 MIB*

  Supported on MX Series routers with MPC/MIC interfaces that use the ATM MIC with SFP.
- Internet draft draft-ietf-l3vpn-mvpn-mib-03.txt, *MPLS/BGP Layer 3 VPN Multicast Management Information Base*

  Implemented under the Juniper Networks enterprise branch [`jnxExperiment`]. OID for `jnxMvpnExperiment` is `.1.3.6.1.4.1.2636.5.12`. This includes `jnxMvpnNotifications` traps.

RELATED DOCUMENTATION

Network Management and Monitoring Guide

Accessing Standards Documents on the Internet | 2

Supported Port Extension Standards

Junos OS substantially supports Institute of Electrical and Electronics Engineers (IEEE) Standard 802.1BR, *Standard for Local and Metropolitan Area Networks - Virtual Bridged Local Area Networks - Bridge Port Extension*.

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported RADIUS and TACACS+ Standards for User Authentication

For validation of the identity of users who attempt to access a router, Junos OS supports RADIUS authentication, TACACS+ authentication, and authentication by means of Junos OS user accounts

configured on the router. Junos OS supports the configuration of Juniper Networks-specific RADIUS and TACACS+ attributes, and the creation of template accounts.

All users who can log in to the router must already be assigned to a Junos OS login class. A *login class* defines its members' access privileges during a login session, the commands they can and cannot issue, the configuration statements they can and cannot view or change, and the idle time before a member's login session is terminated.

Junos OS substantially supports the following RFCs, which define standards for RADIUS and TACACS+.

- RFC 1492, *An Access Control Protocol, Sometimes Called TACACS*
- RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*
- RFC 3162, *RADIUS and IPv6*
- RFC 4818, *RADIUS Delegated-IPv6-Prefix Attribute*

The following Internet drafts do not define standards, but provide information about RADIUS. The IETF classifies them as "Informational."

- RFC 2866, *RADIUS Accounting*
- RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*
- RFC 2869, *RADIUS Extensions*
- RFC 4679, *DSL Forum Vendor-Specific RADIUS Attributes*
- RFC 5176, *Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*

RELATED DOCUMENTATION

Supported System Access Standards | 21

Accessing Standards Documents on the Internet | 2

Supported System Access Standards

Junos OS substantially supports the following protocols and applications for remote access to devices: telnet, FTP, rlogin, and finger.

Junos OS substantially supports RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*.

For jurisdictions without limits on dataplane encryption, that version of Junos OS substantially supports the following RFCs, which define standards for technologies used with Secure Sockets Layer (SSL).

- RFC 1319, *The MD2 Message-Digest Algorithm*
- RFC 1321, *The MD5 Message-Digest Algorithm*
- RFC 2246, *The TLS Protocol Version 1.0*
- RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

Junos OS substantially supports the following RFCs and standards that apply to the SSH protocol. These are used for control plane administration on devices running Junos OS either directly using the CLI or in conjunction with NETCONF:

- RFC 4250, *The Secure Shell (SSH) Protocol Assigned Numbers*

  You can find the assigned SSH numbers at https://www.iana.org/assignments/ssh-parameters/ssh-parameters.xhtml.

- RFC 4251, *The Secure Shell (SSH) Protocol Architecture*
- RFC 4252, *The Secure Shell (SSH) Authentication Protocol*
- RFC 4253, *The Secure Shell (SSH) Transport Layer Protocol*
- RFC 4254, *The Secure Shell (SSH) Connection Protocol*
- RFC 4256, *Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)*

  Also known as “keyboard-interactive” authentication.

- RFC 4335, *The Secure Shell (SSH) Session Channel Break Extension*
- RFC 4344, *The Secure Shell (SSH) Transport Layer Encryption Modes*

  The following encryption methods are supported:

  - aes128-ctr
  - aes192-ctr
  - aes256-ctr

- RFC 4419, *Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol*
- RFC 4432, *RSA Key Exchange for the Secure Shell (SSH) Transport Layer Protocol*
- RFC 4819, *Secure Shell Public Key Subsystem*

Junos OS supports SSH file transfer protocol (SFTP).

- RFC 5656, *Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer*

  The following Elliptic Curves are supported:

  - nistp256
  - nistp384
  - nistp521

  The following public keys are supported:

  - ecdsa-sha2-nistp256
  - ecdsa-sha2-nistp384
  - ecdsa-sha2-nistp521

- RFC 6668, *SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol*

  The hmac-sha2-256 and hmac-sha2-512 integrity algorithms are supported.

- RFC 8270, *Increase the Secure Shell Minimum Recommended Diffie-Hellman Modulus Size to 2048 Bits*

- OpenSSH per the *openssh-portable/PROTOCOL*.

  For more information about OpenSSH, see https://github.com/openssh/openssh-portable/blob/master/PROTOCOL.

The following RFCs provide information about TFTP, which Junos OS supports as a remote access protocol. The IETF does not include the RFCs in its Standards track, instead assigning them status "Unknown (Legacy Stream.)"

- RFC 783, *THE TFTP PROTOCOL (REVISION 2)*
- RFC 906, *Bootstrap Loading using TFTP*

The following RFCs provide information about Transport Layer Security (TLS) protocol, which Junos OS supports to enable client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

- RFC 4346, *The Transport Layer Security (TLS) Protocol Version 1.1*
- RFC 5346, *The Transport Layer Security (TLS) Protocol Version 1.2*
- RFC 8446, *The Transport Layer Security (TLS) Protocol Version 1.3*

RELATED DOCUMENTATION

Supported RADIUS and TACACS+ Standards for User Authentication | 20

Accessing Standards Documents on the Internet | 2

Supported Time Synchronization Standard

Junos OS and Junos Evolved OS substantially support:

- RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*.
- RFC 2030, *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI*, does not define a standard, but provides information about time synchronization technology. The IETF classifies it as "Informational.". In CLI operational mode, you can set the current date and time on the router manually or from an NTP server.
- RFC 8915, *Network Time Security for the Network Time Protocol*.
- MX Series routers with the Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP, Junos OS substantially supports RFC 4553, *Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)*

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

CHAPTER 3

Interface Standards

IN THIS CHAPTER

Supported ATM Interface Standards

Junos OS substantially supports the following standards for Asynchronous Transfer Mode (ATM) interfaces.

- International Telecommunication Union–Telecommunication Standardization (ITU–T) Recommendation I.432.3, *B-ISDN user-network interface - Physical layer specification: 1544 kbit/s and 2048 kbit/s operation*
- RFC 1483, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*

  Only routed protocol data units (PDUs) are supported.
- RFC 2225, *Classical IP and ARP over ATM*

  Only responses are supported.
- RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*

  Only routed PDUs and Ethernet bridged PDUs are supported.
- RFC 4717, *Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks*

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported Ethernet Interface Standards

Junos OS substantially supports the following standards for Ethernet interfaces.

- Institute of Electrical and Electronics Engineers (IEEE) Standard 802.1ag, *IEEE Standard for Local and metropolitan area networks—Virtual Bridged Local Area Networks, Amendment 5: Connectivity Fault Management*
- IEEE Standard 802.1ah, *IEEE Standard for Local and metropolitan area networks—Virtual Bridged Local Area Networks, Amendment 7: Provider Backbone Bridges*
- IEEE Standard 802.1Q, *IEEE Standard for Local and metropolitan area networks—Virtual Bridged Local Area Networks*
- IEEE Standard 802.1Qaz, *IEEE Standard for Local and Metropolitan Area Networks---Virtual Bridged Local Area Networks - Amendment: Enhanced Transmission Selection*
- IEEE Standard 802.1Qbb, *IEEE Standard for Local and Metropolitan Area Networks---Virtual Bridged Local Area Networks - Amendment: Priority-based Flow Control*
- IEEE Standard 802.1s, *IEEE Standard for Multiple Instances of Spanning Tree Protocol (MSTP)---Virtual Bridged Local Area Networks*
- IEEE Standard 802.3, *IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements, Part 3: Carrier sense multiple access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*
- IEEE Standard 802.3ab, *1000BASE-T* (published as Clause 40 in Section 3 of the 802.3 specification)
- IEEE Standard 802.3ad, *Aggregation of Multiple Link Segments* (published as Clause 43 in Section 3 of the 802.3 specification)
- IEEE Standard 802.3ae, *10-Gigabit Ethernet* (published as Clauses 44-53 in Section 4of the 802.3 specification)
- IEEE Standard 802.3ah, *Operations, Administration, and Maintenance (OAM)* (published as Clause 57 in Section 5 of the 802.3 specification)
- IEEE Standard 802.3z, *1000BASE-X* (published as Clauses 34-39, 41-42 in Section 3 of the 802.3 specification)

- InterNational Committee for Information Technology Standards (INCITS) T11, *Fibre Channel Interfaces*
- International Telecommunication Union–Telecommunication Standardization (ITU–T) Recommendation Y.1731, *OAM functions and mechanisms for Ethernet based networks*

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported Frame Relay Interface Standards

Junos OS substantially supports the following standards for Frame Relay interfaces.

- American National Standards Institute (ANSI), *Annex D, Additional Procedures for Permanent Virtual Connections (PVCs) Using Unnumbered Information Frames* to T1.617-1991, *Integrated Services Digital Network (ISDN)—Signaling Specification for Frame Relay Bearer Service for Digital Subscriber Signaling System Number 1 (DSS1)*
- Broadband Forum standard FRF.12, *Frame Relay Fragmentation Implementation Agreement*
- FRF.15, *End-to-End Multilink Frame Relay Implementation Agreement*
- FRF.16.1, *Multilink Frame Relay UNI/NNI Implementation Agreement*
- International Telecommunication Union–Telecommunication Standardization (ITU–T), *Annex A, Additional procedures for Permanent Virtual Connection (PVC) status management (using Unnumbered Information frames)* to Recommendation Q.933, *ISDN Digital Subscriber Signalling System No. 1 (DSS1) - Signalling specifications for frame mode switched and permanent virtual connection control and status monitoring*
- RFC 1973, *PPP in Frame Relay*
- RFC 2390, *Inverse Address Resolution Protocol*
- RFC 2427, *Multiprotocol Interconnect over Frame Relay* (obsoletes RFC 1490)
- RFC 2590, *Transmission of IPv6 Packets over Frame Relay Networks Specification*
- Internet draft draft-martini-frame-encap-mpls-01.txt, *Frame Relay Encapsulation over Pseudo-Wires* (expires December 2002)

  Translation of the command/response bit and sequence numbers and padding are not supported.

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported GRE and IP-IP Interface Standards

Junos OS substantially supports the following RFCs, which define standards for generic routing encapsulation (GRE) and IP-IP interfaces.

- RFC 2003, *IP Encapsulation within IP*
- RFC 2784, *Generic Routing Encapsulation (GRE)*
- RFC 2890, *Key and Sequence Number Extensions to GRE*

  The key field is supported, but the sequence number field is not.

The following RFCs do not define standards, but provide information about GRE, IP-IP, and related technologies. The IETF classifies them as "Informational."

- RFC 1701, *Generic Routing Encapsulation (GRE)*
- RFC 1702, *Generic Routing Encapsulation over IPv4 networks*
- RFC 2547, *BGP/MPLS VPNs* (over GRE tunnels)

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported PPP Interface Standards

Junos OS substantially supports the following RFCs, which define standards for Point-to-Point Protocol (PPP) interfaces.

- RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*
- RFC 1334, *PPP Authentication Protocols*
- RFC 1661, *The Point-to-Point Protocol (PPP)*
- RFC 1662, *PPP in HDLC-like Framing*

- RFC 1989, *PPP Link Quality Monitoring*
- RFC 1990, *The PPP Multilink Protocol (MP)*
- RFC 2364, *PPP Over AAL5*
- RFC 2615, *PPP over SONET/SDH*
- RFC 2686, *The Multi-Class Extension to Multi-Link PPP*

  The following features are not supported:

  - Negotiation of address field compression and protocol field compression PPP NCP options; instead, a full 4-byte PPP header is always sent
  - Prefix elision
- RFC 3021, *Using 31-Bit Prefixes on IPv4 Point-to-Point Links*

The following RFCs do not define standards, but provide information about PPP. The IETF classifies them as "Informational."

- RFC 1877, *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*
- RFC 2153, *PPP Vendor Extensions*

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported SDH and SONET Interface Standards

Junos OS substantially supports the following standards for SDH and SONET interfaces.

- American National Standards Institute (ANSI) standard T1.105-2001, *Synchronous Optical Network (SONET) – Basic Description including Multiplex Structure, Rates, and Formats*
- ANSI standard T1.105.02-2001, *Synchronous Optical Network (SONET) – Payload Mappings*
- ANSI standard T1.105.06-2002, *Synchronous Optical Network (SONET): Physical Layer Specifications*
- GR-253-CORE (Telcordia Generic Requirements standard), *Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria* (replaces GR-1377-CORE, *SONET OC-192 Transport System Generic Criteria*)

- GR-499-CORE, *Transport Systems Generic Requirements (TSGR): Common Requirements*
- International Telecommunication Union–Telecommunication Standardization (ITU–T) Recommendation G.691, *Optical interfaces for single channel STM-64 and other SDH systems with optical amplifiers*
- ITU–T Recommendation G.707 (1996), *Network node interface for the synchronous digital hierarchy (SDH)*
- ITU–T Recommendation G.783 (1994), *Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks*
- ITU–T Recommendation G.813 (1996), *Timing characteristics of SDH equipment client clocks (SEC)*
- ITU–T Recommendation G.825 (1993), *The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)*
- ITU–T Recommendation G.826 (1999), *Error performance parameters and objectives for international, constant bit-rate digital paths at or above the primary rate*
- ITU–T Recommendation G.831 (1993), *Management capabilities of transport networks based on the synchronous digital hierarchy (SDH)*
- ITU–T Recommendation G.957 (1995), *Optical interfaces for equipments and systems relating to the synchronous digital hierarchy*
- ITU–T Recommendation G.958 (1994), *Digital line systems based on the synchronous digital hierarchy for use on optical fibre cables*
- ITU–T Recommendation I.432 (1993), *B-ISDN user-network interface – Physical layer specification*
- RFC 1619, *PPP over SONET/SDH*

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported Serial Interface Standards

Junos OS substantially supports the following standards for serial interfaces.

- International Telecommunication Union–Telecommunication Standardization (ITU–T) Recommendation V.35, *Data transmission at 48 kilobits per second using 60-108 kHz group band circuits*

- ITU–T Recommendation X.21 (1992), *Interface between Data Terminal Equipment and Data Circuit-terminating Equipment for synchronous operation on public data networks*

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported T3 Interface Standard

Junos OS substantially supports International Telecommunication Union–Telecommunication Standardization (ITU–T) Recommendation G.703, *Physical/electrical characteristics of hierarchical digital interfaces*.

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

CHAPTER 4

Layer 2 Standards

IN THIS CHAPTER

Supported Layer 2 Networking Standards

Junos OS substantially supports the following standards for Layer 2 networking.

- Institute of Electrical and Electronics Engineers (IEEE) Standard 802.1ab, *IEEE Standard for Local and metropolitan area networks—Station and Media Access Control Connectivity Discovery* (Link Layer Discovery Protocol (LLDP))
- IEEE Standard 802.1D, *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges*

  This document includes the standard for Rapid Spanning Tree Protocol (RSTP), which is often referred to as 802.1w. It also discusses Quality of Service (QoS) at the MAC level, often referred to as 802.1p.
- IEEE Standard 802.1X, *IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control*

  IEEE 802.1X Port-Based Network Access Control regulates access to the network, guarding against transmission and reception by unidentified or unauthorized parties, and consequent network disruption, theft of service, or data loss.

RELATED DOCUMENTATION

Supported L2TP Standards | 33

Supported VPWS Standards | 33

Supported Layer 2 VPN Standards | 34

Accessing Standards Documents on the Internet | 2

Supported L2TP Standards

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or Multiservices PICs or DPCs, Junos OS substantially supports the following RFC, which defines the standard for Layer 2 Tunneling Protocol (L2TP).

- RFC 2661, *Layer Two Tunneling Protocol "L2TP"*

The following RFC does not define a standard, but provides information about technology related to L2TP. The IETF classifies it as "Informational."

- RFC 2866, *RADIUS Accounting*

RELATED DOCUMENTATION

Services Interfaces Overview for Routing Devices

MX Series 5G Universal Routing Platform Interface Module Reference

Accessing Standards Documents on the Internet | 2

Supported VPWS Standards

Junos OS substantially supports the following RFCs, which define standards for VPWS and Layer 2 circuits.

- RFC 4447, *Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*

  Junos OS does not support Section 5.3, "The Generalized PWid FEC Element."

- RFC 4448, *Encapsulation Methods for Transport of Ethernet over MPLS Networks*
- RFC 6074, *Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)*
- RFC 6391, *Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network*

- RFC 6790, *The Use of Entropy Labels in MPLS Forwarding*

The following Internet drafts do not define standards, but provide information about Layer 2 technologies. The IETF classifies them as "Historic."

- Internet draft draft-martini-l2circuit-encap-mpls-11.txt, *Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*

  Junos OS differs from the Internet draft in the following ways:

  - A packet with a sequence number of 0 (zero) is treated as out of sequence.
  - Any packet that does not have the next incremental sequence number is considered out of sequence.
  - When out-of-sequence packets arrive, the expected sequence number for the neighbor is set to the sequence number in the Layer 2 circuit control word.

- Internet draft draft-martini-l2circuit-trans-mpls-19.txt, *Transport of Layer 2 Frames Over MPLS*

RELATED DOCUMENTATION

Supported Carrier-of-Carriers and Interprovider VPN Standards

Supported Layer 2 VPN Standards

Supported Layer 3 VPN Standards

Supported Multicast VPN Standards

Supported VPLS Standards

Accessing Standards Documents on the Internet

Supported Layer 2 VPN Standards

Junos OS substantially supports the following standards and Internet drafts, which define standards for Layer 2 virtual private networks (VPNs).

- RFC 7348, *Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks*
- Internet draft draft-kompella-l2vpn-vpls-multihoming, *Multi-homing in BGP-based Virtual Private LAN Service*
- Internet draft draft-kompella-ppvpn-l2vpn-03.txt, *Layer 2 VPNs Over Tunnels*

RELATED DOCUMENTATION

- *Supported Carrier-of-Carriers and Interprovider VPN Standards*
- *Supported VPWS Standards*
- *Supported Layer 3 VPN Standards*
- *Supported Multicast VPN Standards*
- *Supported VPLS Standards*
- Accessing Standards Documents on the Internet

Supported Security Standards

Junos OS substantially supports the following standard for security.

- IEEE Standard 802.1AE, *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security*

  This document will facilitate standard secure communication between two security devices through secure chassis cluster control and fabric ports.

  SRX340 and SRX345 supports only 802.1AE-2006 standard.

RELATED DOCUMENTATION

- Accessing Standards Documents on the Internet | 2

Supported VPWS Standards

Junos OS substantially supports the following RFCs, which define standards for VPWS and Layer 2 circuits.

- RFC 4447, *Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*

  Junos OS does not support Section 5.3, “The Generalized PWid FEC Element.”

- RFC 4448, *Encapsulation Methods for Transport of Ethernet over MPLS Networks*
- RFC 6074, *Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)*
- RFC 6391, *Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network*

- RFC 6790, *The Use of Entropy Labels in MPLS Forwarding*

The following Internet drafts do not define standards, but provide information about Layer 2 technologies. The IETF classifies them as “Historic.”

- Internet draft draft-martini-l2circuit-encap-mpls-11.txt, *Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*

  Junos OS differs from the Internet draft in the following ways:

  - A packet with a sequence number of 0 (zero) is treated as out of sequence.
  - Any packet that does not have the next incremental sequence number is considered out of sequence.
  - When out-of-sequence packets arrive, the expected sequence number for the neighbor is set to the sequence number in the Layer 2 circuit control word.

- Internet draft draft-martini-l2circuit-trans-mpls-19.txt, *Transport of Layer 2 Frames Over MPLS*

RELATED DOCUMENTATION

Supported Carrier-of-Carriers and Interprovider VPN Standards

Supported Layer 2 VPN Standards

Supported Layer 3 VPN Standards

Supported Multicast VPN Standards

Supported VPLS Standards

Accessing Standards Documents on the Internet

CHAPTER 5

MPLS Applications Standards

IN THIS CHAPTER

Supported GMPLS Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for Generalized MPLS (GMPLS).

- RFC 3471, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description*

  Only the following features are supported:

  - Bidirectional LSPs (upstream label only)
  - Control channel separation
  - Generalized label (suggested label only)
  - Generalized label request (bandwidth encoding only)

- RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions*

  Only Section 9, “Fault Handling,” is supported.

- RFC 4202, *Routing Extensions in Support of Generalized Multi-Protocol Label Switching*

  Only interface switching is supported.

- RFC 4206, *Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)*
- Internet draft draft-ietf-ccamp-gmpls-rsvp-te-ason-02.txt, *Generalized MPLS (GMPLS) RSVP-TE Signalling in support of Automatically Switched Optical Network (ASON)* (expires January 2005)
- Internet draft draft-ietf-ccamp-gmpls-sonet-sdh-08.txt, *Generalized Multi-Protocol Label Switching Extensions for SONET and SDH Control*

  Only S,U,K,L,M-format labels and SONET traffic parameters are supported.
- Internet draft draft-ietf-ccamp-lmp-10.txt, *Link Management Protocol (LMP)*
- Internet draft draft-ietf-ccamp-ospf-gmpls-extensions-12.txt, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching*

  The following sub-TLV types for the Link type, link, value (TLV) are not supported:

  - Link Local/Remote Identifiers (type 11)
  - Link Protection Type (type 14)
  - Shared Risk Link Group (SRLG) (type 16)

  The features described in Section 2 of the draft, “Implications on Graceful Restart,” are also not supported.

  The Interface Switching Capability Descriptor (type 15) sub-TLV type is implemented, but only for packet switching.
- Internet draft draft-ietf-mpls-bundle-04.txt, *Link Bundling in MPLS Traffic Engineering*

Supported LDP Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for LDP.

- RFC 3212, *Constraint-Based LSP Setup using LDP*
- RFC 3478, *Graceful Restart Mechanism for Label Distribution Protocol*
- RFC 7060, *Using LDP Multipoint Extensions on Targeted LDP Sessions*
- RFC 8661, *Segment Routing MPLS Interworking with LDP*
- RFC 8077, *Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*

- Internet draft draft-napierala-mpls-targeted-mldp-01.txt, *Using LDP Multipoint Extensions on Targeted LDP Sessions*

The following RFCs do not define standards, but provide information about LDP. The IETF classifies them as “Informational.”

- RFC 3215, *LDP State Machine*
- RFC 5036, *LDP Specification*

  For the following features described in the indicated sections of the RFC, Junos OS supports one of the possible modes but not the others:

  - Label distribution control (section 2.6.1): Ordered mode is supported, but not Independent mode.
  - Label retention (section 2.6.2): Liberal mode is supported, but not Conservative mode.
  - Label advertisement (section 2.6.3): Both Downstream Unsolicited mode and Downstream on Demand mode are supported.
- RFC 5283, *LDP Extension for Inter-Area Label Switched Paths (LSPs)*
- RFC 5443, *LDP IGP Synchronization*
- RFC 5561, *LDP Capabilities*
- RFC 6512, *Using Multipoint LDP When the Backbone Has No Route to the Root*

  Only the Recursive Opaque Value is supported.
- RFC 6826, *Multipoint LDP In-Band Signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*

  Junos OS support limited to point-to-multipoint extensions for LDP.

Supported MPLS Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for MPLS and traffic engineering.

- RFC 2858, *Multiprotocol Extensions for BGP-4*
- RFC 3031, *Multiprotocol Label Switching Architecture*
- RFC 3032, *MPLS Label Stack Encoding*
- RFC 3140, *Per Hop Behavior Identification Codes*

- RFC 3270, *Multi-Protocol Label Switching (MPLS) Support of Differentiated Services*

  Only E-LSPs are supported.

- RFC 3443, *Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks*
- RFC 3478, *Graceful Restart Mechanism for Label Distribution Protocol*
- RFC 3906, *Calculating Interior Gateway Protocol (IGP) Routes Over Traffic Engineering Tunnels*
- RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*

  Node protection in facility backup is not supported.

- RFC 4124, *Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering*
- RFC 4182, *Removing a Restriction on the use of MPLS Explicit NULL*
- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*
- RFC 4385, *Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN*.

  Supported on MX Series routers with the Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP.

- RFC 4875, *Extensions to RSVP-TE for Point-to-Multipoint TE LSPs*
- RFC 4950, *ICMP Extensions for Multiprotocol Label Switching*
- RFC 5317, *Joint Working Team (JWT) Report on MPLS Architectural Considerations for a Transport Profile*
- RFC 5586, *MPLS Generic Associated Channel*
- RFC 5654, *Requirements of an MPLS Transport Profile*

  The following capabilities are supported in the Junos OS implementation of MPLS Transport Profile (MPLS-TP):

  - MPLS-TP OAM can send and receive packets with GAL and G-Ach, without IP encapsulation.
  - Two unidirectional RSVP LSPs between a pair of routers can be associated with each other to create an associated bidirectional LSP for binding a path for the GAL and G-Ach OAM messages. A single Bidirectional Forwarding Detection (BFD) session is established for the associated bidirectional LSP.

- RFC 5712, *MPLS Traffic Engineering Soft Preemption*

- RFC 5718, *An In-Band Data Communication Network For the MPLS Transport Profile*
- RFC 5860, *Requirements for Operations, Administration, and Maintenance (OAM) in MPLS Transport Networks*
- RFC 5884, *Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)*
- RFC 5921, *A Framework for MPLS in Transport Networks*
- RFC 5950, *Network Management Framework for MPLS-based Transport Networks*
- RFC 5951, *Network Management Requirements for MPLS-based Transport Networks*
- RFC 5960, *MPLS Transport Profile Data Plane Architecture*
- RFC 6215, *MPLS Transport Profile User-to-Network and Network-to-Network Interfaces*
- RFC 6291, *Guidelines for the Use of the "OAM" Acronym in the IETF*.
- RFC 6370, *MPLS Transport Profile (MPLS-TP) Identifiers*
- RFC 6371, *Operations, Administration, and Maintenance Framework for MPLS-Based Transport Networks*.
- RFC 6372, *MPLS Transport Profile (MPLS-TP) Survivability Framework*
- RFC 6373, *MPLS-TP Control Plane Framework*
- RFC 6388, *Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*

  Only Point-to-Multipoint LSPs are supported.
- RFC 6424, *Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels*
- RFC 6425, *Detecting Data-Plane Failures in Point-to-Multipoint MPLS - Extensions to LSP Ping*
- RFC 6426, *MPLS On-Demand Connectivity Verification and Route Tracing*
- RFC 6428, *Proactive Connectivity Verification, Continuity Check, and Remote Defect Indication for the MPLS Transport Profile*
- RFC 6510, *Resource Reservation Protocol (RSVP) Message Formats for Label Switched Path (LSP) Attributes Objects*
- RFC 6790, *The Use of Entropy Labels in MPLS Forwarding*
- RFC 7746, *Label Switched Path (LSP) Self-Ping*

- Internet draft draft-ietf-mpls-rsvp-te-no-php-oob-mapping-01.txt, *Non PHP behavior and Out-of-Band Mapping for RSVP-TE LSPs*

The following RFCs and Internet drafts do not define standards, but provide information about MPLS, traffic engineering, and related technologies. The IETF classifies them variously as "Experimental," "Historic," or "Informational."

- RFC 2547, *BGP/MPLS VPNs*
- RFC 2702, *Requirements for Traffic Engineering Over MPLS*
- RFC 2917, *A Core MPLS IP VPN Architecture*
- RFC 3063, *MPLS Loop Prevention Mechanism*
- RFC 3208, *PGM Reliable Transport Protocol Specification*

  Only the network element is supported.
- RFC 3469, *Framework for Multi-Protocol Label Switching (MPLS)-based Recovery*
- RFC 3564, *Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering*
- RFC 4125, *Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*
- RFC 4127, *Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*
- Internet draft draft-martini-l2circuit-encap-mpls-11.txt, *Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*

  Junos OS differs from the Internet draft in the following ways:

  - A packet with a sequence number of 0 is treated as out of sequence.
  - Any packet that does not have the next incremental sequence number is considered out of sequence.
  - When out-of-sequence packets arrive, the expected sequence number for the neighbor is set to the sequence number in the Layer 2 circuit control word.
- Internet draft draft-martini-l2circuit-trans-mpls-19.txt, *Transport of Layer 2 Frames Over MPLS*
- RFC 4875, *Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs) (Support one path per S2L mode of signaling)*

Supported PCEP Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for PCEP.

- RFC 5440, *Path Computation Element (PCE) Communication Protocol (PCEP)—Stateful PCE*
- RFC 8231, *Path Computation Element Communication Protocol (PCEP)—Extensions for Stateful PCE*
- RFC 8281, *Path Computation Element Communication Protocol (PCEP)—Extensions PCE-Initiated LSP Setup in a Stateful PCE Model*
- Internet draft-ietf-pce-stateful-pce-07.txt, *PCEP Extensions for Stateful PCE*
- Internet draft-crabbe-pce-pce-initiated-lsp-03.txt, *PCEP Extensions for PCE-initiated LSP Setup in a Stateful PCE Model*
- Internet draft-ietf-pce-segment-routing-06.txt, *PCEP Extensions for Segment Routing*
- Internet draft-ietf-pce-stateful-pce-p2mp-02.txt, *Path Computation Element (PCE) Protocol Extensions for Stateful PCE usage for Point-to-Multipoint Traffic Engineering Label Switched Paths*
- Internet draft draft-cbrt-pce-stateful-local-protection-01, *PCEP Extensions for RSVP-TE Local-Protection with PCE-Stateful* (excluding support for bypass LSP mapping)
- Internet draft draft-ietf-pce-pcep-flowspec-05, *PCEP Extension for Flow Specification*

  The current implementation of this feature does not implement the following sections of the draft:

  - Section 3.1.2—Advertising PCE capabilties in IGP
  - Section 3.2—PCReq and PCRep message
  - Section 7—Most of the flow specifications, except route distinguisher and IPv4 Multicast Flow specifications, are not supported.

Supported RSVP Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for RSVP.

- RFC 2205, *Resource ReSerVation Protocol (RSVP)—Version 1 Functional Specification*
- RFC 2210, *The Use of RSVP with IETF Integrated Services*
- RFC 2211, *Specification of the Controlled-Load Network Element Service*

- RFC 2212, *Specification of Guaranteed Quality of Service*
- RFC 2215, *General Characterization Parameters for Integrated Service Network Elements*
- RFC 2745, *RSVP Diagnostic Messages*
- RFC 2747, *RSVP Cryptographic Authentication* (updated by RFC 3097)
- RFC 2750, *RSVP Extensions for Policy Control* (RFC is not supported. Fully compliant with devices that support this RFC).
- RFC 2961, *RSVP Refresh Overhead Reduction Extensions*
- RFC 3097, *RSVP Cryptographic Authentication—Updated Message Type Value*
- RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels*

  The Null Service Object for maximum transmission unit (MTU) signaling in RSVP is not supported.
- RFC 3210, *Applicability Statement for Extensions to RSVP for LSP-Tunnels*
- RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions*

  Only Section 9, "Fault Handling," is supported.
- RFC 3477, *Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)*
- RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*
- RFC 4203, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*

  (OSPF extensions can carry traffic engineering information over unnumbered links.)
- RFC 4558, *Node-ID Based Resource Reservation Protocol (RSVP) Hello: A Clarification Statement*
- RFC 4561, *Definition of a Record Route Object (RRO) Node-Id Sub-Object*

  The RRO node ID subobject is for use in inter-AS link and node protection configurations.
- RFC 4875, *Extensions to RSVP-TE for Point-to-Multipoint TE LSPs*
- RFC 5151, *Inter-Domain MPLS and GMPLS Traffic Engineering -- Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions*
- RFC 5420, *Encoding of Attributes for MPLS LSP Establishment Using Resource Reservation Protocol Traffic Engineering (RSVP-TE)*

Only the LSP_ATTRIBUTES object is supported.

- RFC 6437, *IPv6 Flow Label Specification*
- RFC 6510, *Resource Reservation Protocol (RSVP) Message Formats for Label Switched Path (LSP) Attributes Objects*
- RFC 7570, *Label Switched Path (LSP) Attribute in the Explicit Route Object (ERO)*
- RFC 8370, *Techniques to Improve the Scalability of RSVP-TE Deployments*
- RFC 8577, *Signaling RSVP-TE Tunnels on a Shared MPLS Forwarding Plane*
- RFC 8796, *RSVP-TE Summary Fast Reroute Extensions for Label Switched Path (LSP) Tunnels*
- draft-ietf-mpls-ri-rsvp-frr-05, *Refresh Interval Independent FRR Facility Protection*

The following RFCs do not define standards, but provide information about RSVP and related technologies. The IETF classifies them variously as “Experimental” or “Informational.”

- RFC 2209, *Resource ReSerVation Protocol (RSVP)—Version 1 Message Processing Rules*
- RFC 2216, *Network Element Service Specification Template*
- RFC 4125, *Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*
- RFC 4127, *Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*
- RFC 8577, *Signaling RSVP-TE Tunnels on a Shared MPLS Forwarding Plane (Fully compliant)*

CHAPTER 6

Open Standards

IN THIS CHAPTER

Supported Open Standards

Junos OS substantially supports the following open standards:

- *OpenFlow Switch Specification, Version 1.0.0*

  For a detailed list of supported messages and fields, match conditions, wild cards, flow actions, statistics, and features, see *OpenFlow v1.0 Compliance Matrix for Devices Running Junos OS*.

  The Junos OS implementation of OpenFlow v1.0 differs from the specification in the following ways:

  (The sections of the OpenFlow specification are indicated in the parentheses.)

  - Junos OS supports only the following flow action types (section 5.2.4):
    - OFPAT_OUTPUT—supports OFPP_NORMAL, OFPP_FLOOD, OFPP_ALL, and OFPP_CONTROLLER for normal flow actions, and OFPP_FLOOD and OFPP_ALL for Send Packet flow actions.
    - OFPAT_SET_VLAN_VID—support varies by platform.
    - OFPAT_STRIP_VLAN—support varies by platform
  - Flow priority is supported according to OpenFlow Switch Specification v1.3.0 in which there is no prioritization of exact match entries over wildcard entries.
  - Emergency mode as defined in OpenFlow v1.0 is not supported. If the controller connection is lost and cannot be reestablished, the switch maintains all flow states in the control and data planes.

  The following features are not supported:

  - Encryption through TLS connection (section 4.4)

- 802.1D Spanning Tree Protocol (sections 4.5 and 5.2.1)
- OFPP_LOCAL virtual port (section 5.2.1)
- Physical port features OFPPF_PAUSE and OFPPF_PAUSE_ASYM (section 5.2.1)
- Queue structures and queue configuration messages (section 5.2.2 and 5.3.4)
- Flow action types: OFPAT_SET_VLAN_PCP, OFPAT_SET_DL_SRC/DST, OFPAT_SET_NW_SRC/DST/TOS, OFPAT_SET_TP_SRC/DST and OFPAT_ENQUEUE (section 5.2.4)
- buffer_id for Modify Flow Entry Message, Send Packet Message, and Packet-In Message (sections 5.3.3, 5.3.6, and 5.4.1)
- Port Modification Message (section 5.3.3)
- Vendor Statistics (section 5.3.5)
- Vendor message (section 5.5.4)

- *OpenFlow Switch Specification, Version 1.3.1*

  For a detailed list of supported messages and fields, port structure flags and numbering, match conditions, flow actions, multipart messages, flow instructions, and group types, see *OpenFlow v1.3.1 Compliance Matrix for Devices Running Junos OS*.

  The Junos OS implementation of OpenFlow v1.3.1 differs from the specification in the following ways:

  (The sections of the OpenFlow specification are indicated in the parentheses.)

  - Junos OS supports only the following flow action types (section 5.12):
    - OFPAT_SET_VLAN_VID
    - OFPAT_POP_VLAN
    - OFPAT_GROUP
  - Junos OS supports only the following group types (section 5.6.1):
    - OFPGT_ALL
    - OFPGT_INDIRECT
  - Junos OS supports only one flow instruction per flow entry. Further, only the following flow instructions (section A.2.4) are supported:
    - OFPIT_WRITE_ACTIONS

    - OFPIT_APPLY_ACTIONS

- For OFPT_SET_CONFIG (section A.3.2), Junos OS supports only the OFPC_FRAG_NORMAL configuration flag, and the OFPCML_NO_BUFFER setting for the miss_send_len field.
- On MX Series routers, Junos OS supports only the following IPv6-related match conditions (A.2.3.7):
    - OFPXMT_OFB_IPV6_SRC
    - OFPXMT_OFB_IPV6_DST

The following features are not supported:

- Multiple flow tables (section 5)
- Table metadata (section 2)
- Action sets (section 5.10)
- Meter (section 5.7)
- MPLS fields (section 5.12.1)
- MPLS actions (section 5.10 and 5.12)
- Encryption through TLS connection (section 6.3.3)
- Per-port queues (section A.2.2)
- Auxiliary connections (section 6.3.5)
- Multiple virtual switches (section A.3.1)
- IPv6-related set-field actions (5.12)

RELATED DOCUMENTATION

OpenFlow v1.0 Compliance Matrix for Devices Running Junos OS

OpenFlow v1.0 Compliance Matrix for QFX5100 and EX4600 Switches

OpenFlow v1.3.1 Compliance Matrix for Devices Running Junos OS

Understanding OpenFlow Operation and Forwarding Actions on Devices Running Junos OS

CHAPTER 7

Packet Processing Standards

IN THIS CHAPTER

Supported CoS Standards

Junos OS substantially supports the following standards for class of service (CoS).

- IEEE Standard 802.1D, *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges*

  This document discusses Quality of Service (QoS) at the MAC level, often referred to as 802.1p.

- RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
- RFC 2597, *Assured Forwarding PHB Group*
- RFC 2598, *An Expedited Forwarding PHB*
- RFC 3246, *An Expedited Forwarding PHB (Per-Hop Behaviour)*
- RFC: 3270, *Multi-Protocol Label Switching (MPLS) Support of Differentiated Services*

The following RFCs do not define standards, but provide information about CoS and related technologies. The IETF classifies them as “Informational.”

- RFC 2475, *An Architecture for Differentiated Services*
- RFC 2697, *A Single Rate Three Color Marker*
- RFC 2698, *A Two Rate Three Color Marker*
- RFC 2983, *Differentiated Services and Tunnels*

- RFC 3140, *Per Hop Behavior Identification Codes*
- RFC 3246, *An Expedited Forwarding PHB (Per-Hop Behavior)*
- RFC 3260, *New Terminology and Clarifications for Diffserv*

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported Packet Filtering Standards

Junos OS provides a packet filtering language that enables you to control the flow of packets being forwarded to a network destination, as well as packets destined for and sent by the router. It substantially supports the following RFCs, which define standards for packet filtering.

- RFC 792, *INTERNET CONTROL MESSAGE PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*
- RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
- RFC 2597, *Assured Forwarding PHB Group*
- RFC 2598, *An Expedited Forwarding PHB*
- RFC 3246, *An Expedited Forwarding PHB (Per-Hop Behavior)*
- RFC 4291, *IP Version 6 Addressing Architecture*
- RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
- RFC 8200, *Internet Protocol, Version 6 (IPv6) Specification*

The following RFCs do not define standards, but provide information about packet filtering and related technologies. The IETF classifies them as “Informational.”

- RFC 2267, *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*
- RFC 2475, *An Architecture for Differentiated Services*
- RFC 2983, *Differentiated Services and Tunnels*
- RFC 3260, *New Terminology and Clarifications for Diffserv*

RELATED DOCUMENTATION

- Routing Policies, Firewall Filters, and Traffic Policers User Guide
- Accessing Standards Documents on the Internet | 2

Supported Policing Standard

Junos OS supports policing, or rate limiting, to limit the amount of traffic that passes through an interface. For information about rate limiting, see RFC 2698, *A Two Rate Three Color Marker*.

The Junos OS implementation of policing uses a token-bucket algorithm and supports the following features:

- Adaptive shaping for Frame Relay traffic
- Virtual channels

RELATED DOCUMENTATION

- Accessing Standards Documents on the Internet | 2

CHAPTER 8

Routing Protocol Standards

IN THIS CHAPTER

Supported Standards for BGP

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for IP version 4 (IPv4) BGP.

For a list of supported IP version 6 (IPv6) BGP standards, see *Supported IPv6 Standards*.

Junos OS BGP supports authentication for protocol exchanges (MD5 authentication).

- RFC 1745, *BGP4/IDRP for IP—OSPF Interaction*
- RFC 1772, *Application of the Border Gateway Protocol in the Internet*
- RFC 1997, *BGP Communities Attribute*
- RFC 2283, *Multiprotocol Extensions for BGP-4*
- RFC 2385, *Protection of BGP Sessions via the TCP MD5 Signature Option*

- RFC 2439, *BGP Route Flap Damping*
- RFC 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*
- RFC 2796, *BGP Route Reflection – An Alternative to Full Mesh IBGP*
- RFC 2858, *Multiprotocol Extensions for BGP-4*
- RFC 2918, *Route Refresh Capability for BGP-4*
- RFC 3065, *Autonomous System Confederations for BGP*
- RFC 3107, *Carrying Label Information in BGP-4*
- RFC 3345, *Border Gateway Protocol (BGP) Persistent Route Oscillation Condition*
- RFC 3392, *Capabilities Advertisement with BGP-4*
- RFC 4271, *A Border Gateway Protocol 4 (BGP-4)*
- RFC 4273, *Definitions of Managed Objects for BGP-4*
- RFC 4360, *BGP Extended Communities Attribute*
- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4456, *BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)*
- RFC 4486, *Subcodes for BGP Cease Notification Message*
- RFC 4576, *Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4659, *BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*
- RFC 4632, *Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan*
- RFC 4684, *Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*
- RFC 4724, *Graceful Restart Mechanism for BGP*
- RFC 4760, *Multiprotocol Extensions for BGP-4*
- RFC 4781, *Graceful Restart Mechanism for BGP with MPLS*
- RFC 4798, *Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*

  Option 4b (eBGP redistribution of labeled IPv6 routes from AS to neighboring AS) is not supported.

- RFC 4893, *BGP Support for Four-octet AS Number Space*
- RFC 5004, *Avoid BGP Best Path Transitions from One External to Another*
- RFC 5065, *Autonomous System Confederations for BGP*
- RFC 5082, *The Generalized TTL Security Mechanism (GTSM)*
- RFC 5291, *Outbound Route Filtering Capability for BGP-4 (partial support)*
- RFC 5292, *Address-Prefix-Based Outbound Route Filter for BGP-4 (partial support)*

  Devices running Junos OS can receive prefix-based ORF messages.
- RFC 5396, *Textual Representation of Autonomous System (AS) Numbers*
- RFC 5492, *Capabilities Advertisement with BGP-4*
- RFC 5512, *The BGP Encapsulation Subsequent Address Family Identifier (SAFI) and the BGP Tunnel Encapsulation Attribute*
- RFC 5549, *Advertising IPv4 Network Layer Reachability Information with an IPv6 Next Hop*
- RFC 5575, *Dissemination of flow specification rules*. Covers RFC 8955 and RFC 8956.

  RFC-8955 - Provides a Border Gateway Protocol Network Layer Reachability Information (BGP NLRI) encoding format that can be used to distribute (intra-domain and inter-domain) traffic flow specifications for IPv4 unicast and IPv4 BGP/MPLS VPN services.

  RFC8956 - Provides a Border Gateway Protocol (BGP) extension for the propagation of traffic flow specifications for the purpose of rate limiting or filtering IPv6 protocol data packets.
- RFC 5668, *4-Octet AS Specific BGP Extended Community*
- RFC 5701, *IPv6 Address Specific BGP Extended Community Attribute*
- RFC 5925, *The TCP Authentication Option*
- RFC 6286, *Autonomous-System-Wide Unique BGP Identifier for BGP-4- fully compliant*
- RFC 6368, *Internal BGP as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 6774, *Distribution of Diverse BGP Paths*
- RFC 6793, *BGP Support for Four-Octet Autonomous System (AS) Number Space*
- RFC 6810, *The Resource Public Key Infrastructure (RPKI) to Router Protocol*
- RFC 6811, *BGP Prefix Origin Validation*

- RFC 6996, *Autonomous System (AS) Reservation for Private Use*
- RFC 7300, *Reservation of Last Autonomous System (AS) Numbers*
- RFC 7311, *The Accumulated IGP Metric Attribute for BGP*
- RFC 7404, *Using Only Link-Local Addressing inside an IPv6 Network*
- RFC 7432, *BGP MPLS-Based Ethernet VPN (eVPN)*
- RFC 7606, *Revised Error Handling for BGP UPDATE Messages*
- RFC 7611, *BGP ACCEPT_OWN Community Attribute*

  We support the RFC by enabling Juniper routers to accept routes received from a route reflector with the `accept-own` community value.

- RFC 7752, *North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP*
- RFC 7854, *BGP Monitoring Protocol (BMP)*
- RFC 7911, *Advertisement of Multiple Paths in BGP*
- RFC 8097, *BGP Prefix Origin Validation State Extended Community*
- RFC 8210, *The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 1*
- RFC 8212, *Default External BGP (EBGP) Route Propagation Behavior without Policies- fully compliant*

  Exceptions:

  The behaviors in RFC 8212 are not implemented by default in order to avoid disruption of existing customer configuration. The default behavior is still kept to accept and advertise all routes with regard to EBGP peers.

- RFC 8277, *Using BGP to Bind MPLS Labels to Address Prefixes*
- RFC 8326, *Graceful BGP session Shutdown*
- RFC 8481, *Clarifications to BGP Origin Validation Based on Resource Public Key Infrastructure (RPKI)*
- RFC 8538, *Notification Message Support for BGP Graceful Restart*
- RFC 8571, *BGP - Link State (BGP-LS) Advertisement of IGP Traffic Engineering Performance Metric Extensions*
- RFC 8584, *Framework for Ethernet VPN Designated Forwarder Election Extensibility*

- RFC 8642, *Policy Behavior for Well-Known BGP Communities*
- RFC 8669, *Segment Routing Prefix Segment Identifier Extensions for BGP*
- RFC 8810, *Revision to Capability Codes Registration Procedures*
- RFC 8814 *Signaling Maximum SID Depth (MSD) Using the Border Gateway Protocol - Link State (partial support)*
- RFC 8950, *Advertising IPv4 Network Layer Reachability Information (NLRI) with an IPv6 Next Hop*
- RFC 8955
- RFC 8956
- RFC 9003, *Extended BGP Administrative Shutdown Communication*
- RFC 9012, *The BGP Tunnel Encapsulation Attribute*
- RFC 9029, *Updates to the Allocation Policy for the Border Gateway Protocol - Link State (BGP-LS) Parameters Registries*
- RFC 9069, *Support for Local RIB in the BGP Monitoring Protocol (BMP)*
- RFC 9085, *Border Gateway Protocol - Link State (BGP-LS) Extensions for Segment Routing*
- RFC 9117, *Revised Validation procedure for Dissemination of BGP Flow Specifications. This enables the Flow Specifications to be originated within the same autonomous system as the BGP peer performing the validation.*
- RFC 9384, *A BGP Cease NOTIFICATION Subcode for Bidirectional Forwarding Detection (BFD)*
- Internet draft draft-idr-rfc8203bis-00, *BGP Administrative Shutdown Communication* (expires October 2018)
- Internet draft draft-ietf-grow-bmp-adj-rib-out-01, *Support for Adj-RIB-Out in BGP Monitoring Protocol (BMP)* (expires September 3, 2018)
- Internet draft draft-ietf-idr-aigp-06, *The Accumulated IGP Metric Attribute for BGP* (expires December 2011)
- Internet draft draft-ietf-idr-as0-06, *Codification of AS 0 processing* (expires February 2013)
- Internet draft draft-ietf-idr-link-bandwidth-06.txt, *BGP Link Bandwidth Extended Community* (expires July 2013)
- Internet draft draft-ietf-sidr-origin-validation-signaling-00, *BGP Prefix Origin Validation State Extended Community (partial support)* (expires May 2011)

The extended community (origin validation state) is supported in Junos OS routing policy. The specified change in the route selection procedure is not supported.

- Internet draft draft-kato-bgp-ipv6-link-local-00.txt, *BGP4+ Peering Using IPv6 Link-local Address*

The following RFCs and Internet draft do not define standards, but provide information about BGP and related technologies. The IETF classifies them variously as "Experimental" or "Informational."

- RFC 1965, *Autonomous System Confederations for BGP*
- RFC 1966, *BGP Route Reflection—An alternative to full mesh IBGP*
- RFC 2270, *Using a Dedicated AS for Sites Homed to a Single Provider*
- RFC 3345, *Border Gateway Protocol (BGP) Persistent Route Oscillation Condition*
- RFC 3562, *Key Management Considerations for the TCP MD5 Signature Option*
- Internet draft draft-ietf-ngtrans-bgp-tunnel-04.txt, *Connecting IPv6 Islands across IPv4 Clouds with BGP* (expires July 2002)

RELATED DOCUMENTATION

Supported IPv6 Standards

Accessing Standards Documents on the Internet | 2

Supported ES-IS Standards

Junos OS substantially supports the following standards for End System–to–Intermediate System (ES-IS).

- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) standard 8473, *Information technology — Protocol for providing the connectionless-mode network service*
- ISO/IEC standard 9542, *Information processing systems — Telecommunications and information exchange between systems — End system to Intermediate system routeing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473)*

RELATED DOCUMENTATION

Supported Standards for IS-IS | 70

Supported ICMP Router Discovery and IPv6 Neighbor Discovery Standards

Junos OS substantially supports the following RFCs, which define standards for the Internet Control Message Protocol (ICMP for IP version 4 [IPv4]) and neighbor discovery (for IP version 6 [IPv6]).

- RFC 1256, *ICMP Router Discovery Messages*
- RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)*
- RFC 2463, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
- RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
-
- RFC 4862, *IPv6 Stateless Address Autoconfiguration*
- RFC 8335, *PROBE: A Utility for Probing Interfaces*

Supported IP Multicast Protocol Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for IP multicast protocols, including the Distance Vector Multicast Routing Protocol (DVMRP), Internet Group Management Protocol (IGMP), Multicast Listener Discovery (MLD), Multicast Source Discovery Protocol (MSDP), Pragmatic General Multicast (PGM), Protocol Independent Multicast (PIM), Session Announcement Protocol (SAP), and Session Description Protocol (SDP).

- RFC 1112, *Host Extensions for IP Multicasting* (defines IGMP Version 1)
- RFC 2236, *Internet Group Management Protocol, Version 2*
- RFC 2327, *SDP: Session Description Protocol*
- RFC 2710, *Multicast Listener Discovery (MLD) for IPv6*
- RFC 2858, *Multiprotocol Extensions for BGP-4*

- RFC 3031, *Multiprotocol Label Switching Architecture*
- RFC 3376, *Internet Group Management Protocol, Version 3*
- RFC 3956, *Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*
- RFC 3590, *Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*
- RFC 7761, *Protocol Independent Multicast – Sparse Mode (PIM-SM): Protocol Specification*
- RFC 4604, *Using IGMPv3 and MLDv2 for Source-Specific Multicast*
- RFC 4607, *Source-Specific Multicast for IP*
- RFC 4610, *Anycast-RP Using Protocol Independent Multicast (PIM)*
- RFC 5015, *Bidirectional Protocol Independent Multicast (BIDIR-PIM)*
- RFC 5059, *Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*

  The scoping mechanism is not supported.

- RFC 5384, *The Protocol Independent Multicast (PIM) Join Attribute Format*
- RFC 5496, *The Reverse Path Forwarding (RPF) Vector TLV*

  Starting in Release 17.3R1, Junos OS provides support for Protocol Independent Multicast (PIM) resolve type-length-value (TLV) for multicast in seamless MPLS. This support allows PIM in environments where the core routers do not maintain external routes.

- RFC 6513, *Multicast in MPLS/BGP IP VPNs*
- RFC 6514, *BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs*
- Internet draft draft-raggarwa-l3vpn-bgp-mvpn-extranet-08.txt, *Extranet in BGP Multicast VPN (MVPN)*
- Internet draft draft-rosen-l3vpn-spmsi-joins-mldp-03.txt, *MVPN: S-PMSI Join Extensions for mLDP-Created Tunnels*

The following RFCs and Internet drafts do not define standards, but provide information about multicast protocols and related technologies. The IETF classifies them variously as “Best Current Practice,” “Experimental,” or “Informational.”

- RFC 1075, *Distance Vector Multicast Routing Protocol*
- RFC 2362, *Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*
- RFC 2365, *Administratively Scoped IP Multicast*

- RFC 2547, *BGP/MPLS VPNs*
- RFC 2974, *Session Announcement Protocol*
- RFC 3208, *PGM Reliable Transport Protocol Specification*
- RFC 3446, *Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*
- RFC 3569, *An Overview of Source-Specific Multicast (SSM)*
- RFC 3618, *Multicast Source Discovery Protocol (MSDP)*
- RFC 3810, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*
- RFC 3973, *Protocol Independent Multicast – Dense Mode (PIM-DM): Protocol Specification (Revised)*
- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- Internet draft draft-ietf-idmr-dvmrp-v3-11.txt, *Distance Vector Multicast Routing Protocol*
- Internet draft draft-ietf-mboned-ssm232-08.txt, *Source-Specific Protocol Independent Multicast in 232/8*
- Internet draft draft-ietf-mmusic-sap-00.txt, *SAP: Session Announcement Protocol*
- Internet draft draft-rosen-vpn-mcast-07.txt, *Multicast in MPLS/BGP VPNs*

  Only section 7, “Data MDT: Optimizing flooding,” is supported.

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet

Supported IPv4, TCP, and UDP Standards

Junos OS substantially supports the following RFCs, which define standards for IP version 4 (IPv4), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP).

- RFC 768, *User Datagram Protocol*
- RFC 791, *INTERNET PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*

- RFC 792, *INTERNET CONTROL MESSAGE PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*
- RFC 793, *TRANSMISSION CONTROL PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*
- RFC 826, *Ethernet Address Resolution Protocol—or—Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*
- RFC 854, *TELNET PROTOCOL SPECIFICATION*
- RFC 855, *TELNET OPTION SPECIFICATIONS*
- RFC 856, *TELNET BINARY TRANSMISSION*

  To transmit using an 8-bit binary path, use the `telnet` *`host`* `8bit` command, where *host* is the name or address of the remote system.
- RFC 862, *Echo Protocol*
- RFC 863, *Discard Protocol*
- RFC 894, *A Standard for the Transmission of IP Datagrams over Ethernet Networks*
- RFC 896, *Congestion Control in IP/TCP Internetworks*
- RFC 903, *A Reverse Address Resolution Protocol*
- RFC 919, *BROADCASTING INTERNET DATAGRAMS*
- RFC 922, *BROADCASTING INTERNET DATAGRAMS IN THE PRESENCE OF SUBNETS*
- RFC 950, *Internet Standard Subnetting Procedure*
- RFC 959, *FILE TRANSFER PROTOCOL (FTP)*
- RFC 1027, *Using ARP to Implement Transparent Subnet Gateways*
- RFC 1042, *A Standard for the Transmission of IP Datagrams over IEEE 802 Networks*
- RFC 1157, A *Simple Network Management Protocol (SNMP)*
- RFC 1166, *INTERNET NUMBERS*
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*
- RFC 1256, *ICMP Router Discovery Messages*
- RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*

- RFC 1519, *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*
- RFC 1812, *Requirements for IP Version 4 Routers*
- RFC 2338, *Virtual Router Redundancy Protocol* (obsoleted by RFC 3768 in April 2004)
- RFC 2873, *TCP Processing of the IPv4 Precedence Field*
- RFC 3021, *Using 31-Bit Prefixes on IPv4 Point-to-Point Links*
- RFC 3246, *An Expedited Forwarding PHB (Per-Hop Behavior)*
- RFC 3768, *Virtual Router Redundancy Protocol (VRRP)*
- RFC 4884 *Extended ICMP to Support Multi-Part Messages*

  NOTE: In Junos OS, support not available for setting the length attribute.

- RFC 5798, *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6*
- RFC 5925, *The TCP Authentication Option*

  TCP-based features are fully supported. Master Key Tuple/ key management is Junos specific. The CLI/application uses Junos keychain infrastructure for MKT configuration.

- RFC 6527, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol Version 3 (VRRPv3)*

  The following features are not supported:

  - Row creation
  - `Set` operation
  - `vrrpv3StatisticsRowDiscontinuityTime` MIB object
  - `vrrpv3StatisticsPacketLengthErrors` MIB object

- RFC 8335, *PROBE: A Utility for Probing Interfaces*

The following RFCs do not define standards, but provide information about IP, TCP, UDP, and related technologies. The IETF classifies them as “Informational.”

- RFC 1878, *Variable Length Subnet Table For IPv4*
- RFC 1948, *Defending Against Sequence Number Attacks*

RELATED DOCUMENTATION

Supported IPv6 Standards | 63

Accessing Standards Documents on the Internet | 2

Supported IPv6 Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for IP version 6 (IPv6):

- RFC 1981, *Path MTU Discovery for IP version 6*
- RFC 2080, *RIPng for IPv6*
- RFC 2081, *RIPng Protocol Applicability Statement*
- RFC 2373, *IP Version 6 Addressing Architecture*
- RFC 2375, *Multicast Address Assignments*
- RFC 2461, *Neighbor Discovery for IP Version 6 (IPv6)*
- RFC 2462, *IPv6 Stateless Address Autoconfiguration*
- RFC 2463, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
- RFC 2464, *Transmission of IPv6 Packets over Ethernet Networks*
- RFC 2465, *Management Information Base for IP Version 6: Textual Conventions and General Group*

  IP version 6 (IPv6) and Internet Control Message Protocol version 6 (ICMPv6) statistics are not supported.
- RFC 2472, *IP Version 6 over PPP*
- RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
- RFC 2491, *IPv6 Over Non-Broadcast Multiple Access (NBMA) networks*
- RFC 2492, *IPv6 over ATM Networks*
- RFC 2526, *Reserved IPv6 Subnet Anycast Addresses*
- RFC 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*
- RFC 2578, *Structure of Management Information Version 2 (SMIv2)*

- RFC 2675, *IPv6 Jumbograms*
- RFC 2711, *IPv6 Router Alert Option*
- RFC 2767, *Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS)*
- RFC 2784, *Generic Routing Encapsulation*
- RFC 2878, *PPP Bridging Control Protocol (BCP)*
- RFC 3056, *Connection of IPv6 Domains via IPv4 Clouds.*
- RFC 3306, *Unicast-Prefix-based IPv6 Multicast Addresses*
- RFC 3307, *Allocation Guidelines for IPv6 Multicast Addresses*
- RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

  Address assignment is supported with IP version 4 (IPv4) but not IP version 6 (IPv6).
- RFC 3513, *Internet Protocol Version 6 (IPv6) Addressing Architecture*
- RFC 3515, *The Session Initiation Protocol (SIP) Refer Method*
- RFC 3590, *Source Address Selection for the Multicast Listener D* (Supported for SSM include mode only)
- RFC 3768, *Virtual Router Redundancy Protocol (VRRP)*
- RFC 3810, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*
- RFC 3879, *Deprecating Site Local Addresses*
- RFC 3971, *Secure Neighbor Discovery for IPv6* (No support for certification paths, anchored on trusted parties)
- RFC 3972, *Cryptographically Generated Addresses*
- RFC 4007, *IPv6 Scoped Address Architecture*
- RFC 4087, *IP Tunnel MIB*
- RFC 4193, *Unique Local IPv6 Unicast Addresses*
- RFC 4213, *Basic Transition Mechanisms for IPv6 Hosts and Routers*

  RFC 4213 supersedes RFC 2893, *Transition Mechanisms for IPv6 Hosts and Routers*.

NOTE: On EX Series switches, except for the EX9200 Series, only dual IP layer is supported. On EX9200 Series switches, both dual IP layer and configured tunneling of IPv6 over IPv4 are supported.

- RFC 4291, *IP Version 6 Addressing Architecture*
- RFC 4292, *IP Forwarding Table MIB*
- RFC 4293, *Management Information Base for the Internet Protocol (IP)*
- RFC 4294, *IPv6 Node Requirements* (Partial support)
- RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
- RFC 4552, *Authentication/Confidentiality for OSPFv3*
- RFC 4604, *Using Internet Group Management Protocol Version 3 (IGMPv3)*
- RFC 4659, *BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*
- RFC 4798, *Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*

  Option 4b (eBGP redistribution of labeled IPv6 routes from AS to neighboring AS) is not supported.
- RFC 4861 *Neighbor Discovery for IP Version 6 (IPv6)*
- RFC 4862, *IPv6 Stateless Address Autoconfiguration*
- RFC 4884, *Extended ICMP to Support Multi-Part Messages*
- RFC 4890, *Recommendations for Filtering ICMPv6 Messages in Firewalls*
- RFC 4942, *IPv6 Transition/Coexistence Security Considerations*
- RFC 5072, *IP Version 6 over PPP*
- RFC 5095, *Deprecation of Type 0 Routing Headers in IPv6*
- RFC 5308, *Routing IPv6 with IS-IS*
- RFC 5340, *OSPF for IPv6* (RFC 2740 is obsoleted by RFC 5340)
- RFC 5575, *Dissemination of Flow Specification Rules*
- RFC 5798, *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6*
- RFC 5905, *Network Time Protocol Version 4 (for IPv6)*

- RFC 5952, *A Recommendation for IPv6 Address Text Representation*
- RFC 6164, *Using 127-Bit IPv6 Prefixes on Inter-Router Links*
- RFC 6527, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol Version 3 (VRRPv3)*

  The following features are not supported:

  - Row creation
  - `Set` operation
  - `vrrpv3StatisticsPacketLengthErrors` MIB object
  - `vrrpv3StatisticsRowDiscontinuityTime` MIB object
- RFC 6583, *Operational Neighbor Discovery Problems*

  Only Prioritize NDP Activities, Tuning of the NDP Queue Rate Limit, and Queue Tuning are supported.
- RFC 6724, *Default Address Selection for Internet Protocol version 6 (IPv6)*
- RFC 8200, *Internet Protocol, Version 6 (IPv6) Specification*
- RFC 8201, *Path MTU Discovery for IP version 6*
- RFC 8335, *PROBE: A Utility for Probing Interfaces*
- Internet draft draft-ietf-l3vpn-bgp-ipv6-07.txt, *BGP-MPLS IP VPN extension for IPv6 VPN*
- Internet draft draft-ietf-lsr-flex-algo-20.txt, *IGP Flexible Algorithm* to allow IGPs to compute constraint-based paths over the network.
- Internet draft draft-ietf-idr-flow-spec-00.txt, *Dissemination of flow specification rules*
- Internet draft draft-ietf-softwire-dual-stack-lite-04.txt, *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*
- Internet draft draft-kato-bgp-ipv6-link-local-00.txt, *BGP4+ Peering Using IPv6 Link-local Address*

The following RFCs and Internet draft do not define standards, but provide information about IPv6 and related technologies. The IETF classifies them variously as “Experimental” or “Informational.”

- RFC 1901, *Introduction to Community-based SNMPv2*
- RFC 2081, *RIPng Protocol Applicability Statement*
- RFC 2767, *Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS)*

- RFC 3587, *IPv6 Global Unicast Address Format*
- Internet draft draft-ietf-ngtrans-bgp-tunnel-04.txt, *Connecting IPv6 Islands across IPv4 Clouds with BGP*

  Only MP-BGP over IP version 4 (IPv4) approach is supported.

RELATED DOCUMENTATION

Supported IPv4, TCP, and UDP Standards | 60

Accessing Standards Documents on the Internet | 2

Supported OSPF and OSPFv3 Standards

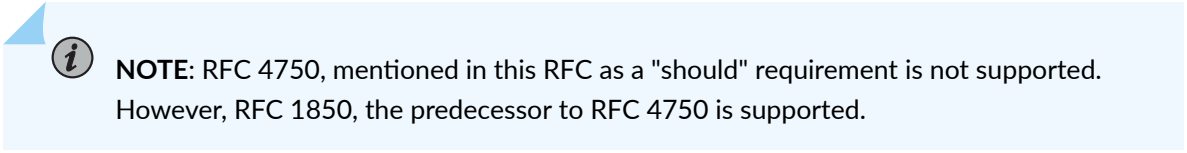
Junos OS substantially supports the following RFCs and Internet drafts, which define standards for OSPF and OSPF version 3 (OSPFv3).

- RFC 1583, *OSPF Version 2*
- RFC 1765, *OSPF Database Overflow*
- RFC 1793, *Extending OSPF to Support Demand Circuits*
- RFC 1850, *OSPF Version 2 Management Information Base*
- RFC 2154, *OSPF with Digital Signatures*
- RFC 2328, *OSPF Version 2*
- RFC 2370, *The OSPF Opaque LSA Option*

  Support is provided by the `update-threshold` configuration statement at the `[edit protocols rsvp interface interface-name ]` hierarchy level.
- RFC 3101, *The OSPF Not-So-Stubby Area (NSSA) Option*
- RFC 3623, *Graceful OSPF Restart*
- RFC 3630, *Traffic Engineering (TE) Extensions to OSPF Version 2*
- RFC 4136, *OSPF Refresh and Flooding Reduction in Stable Topologies*
- RFC 4203, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*

  Only interface switching is supported.

- RFC 4552, *Authentication/Confidentiality for OSPFv3*
- RFC 4576, *Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4577, *OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4811, *OSPF Out-of-Band Link State Database (LSDB) Resynchronization*
- RFC 4812, *OSPF Restart Signaling*
- RFC 4813, *OSPF Link-Local Signaling*
- RFC 4915, *Multi-Topology (MT) Routing in OSPF*
- RFC 5185, *OSPF Multi-Area Adjacency*
- RFC 5187, *OSPFv3 Graceful Restart*
- RFC 5250, *The OSPF Opaque LSA Option*

  NOTE: RFC 4750, mentioned in this RFC as a "should" requirement is not supported. However, RFC 1850, the predecessor to RFC 4750 is supported.

- RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates*
- RFC 5340, *OSPF for IPv6* (RFC 2740 is obsoleted by RFC 5340)
- RFC 5709, *OSPFv2 HMAC-SHA Cryptographic Authentication*
- RFC 5838, *Support of Address Families in OSPFv3*
- Internet draft draft-ietf-ospf-af-alt-10.txt, *Support of address families in OSPFv3*
- Internet draft draft-katz-ward-bfd-02.txt, *Bidirectional Forwarding Detection*

  Transmission of echo packets is not supported.

- RFC 6549, *OSPFv2 Multi-Instance Extensions*
- RFC 8665, *OSPF Extensions for Segment Routing*
- Internet draft draft-ietf-lsr-flex-algo-07.txt, *IGP Flexible Algorithm*

The following RFCs do not define standards, but provide information about OSPF and related technologies. The IETF classifies them as “Informational.”

- RFC 3137, *OSPF Stub Router Advertisement*
- RFC 3509, *Alternative Implementations of OSPF Area Border Routers*
- RFC 5309, *Point-to-Point Operation over LAN in Link State Routing Protocols*
- RFC 8920, *OSPF Application-Specific Link Attributes*
- RFC 8920, *OSPFv2 Prefix/Link Attribute Advertisement*

RELATED DOCUMENTATION

Supported IPv6 Standards

Accessing Standards Documents on the Internet

Supported Standards for RIFT

Junos OS substantially supports the following Internet drafts for Routing in Fat Tree (RIFT) protocol.

- draft draft-ietf-rift-rift-09, *RIFT: Routing in Fat Trees*

RELATED DOCUMENTATION

Supported Standards for IS-IS | 70

Supported RIP and RIPng Standards

Junos OS substantially supports the following RFCs, which define standards for RIP (for IP version 4 [IPv4]) and RIP next generation (RIPng, for IP version 6 [IPv6]).

Junos OS supports authentication for all RIP protocol exchanges (MD5 or simple authentication).

- RFC 1058, *Routing Information Protocol*
- RFC 2080, *RIPng for IPv6*
- RFC 2082, *RIP-2 MD5 Authentication*

  Multiple keys using distinct key IDs are not supported.

- RFC 2453, *RIP Version 2*

The following RFC does not define a standard, but provides information about RIPng. The IETF classifies it as “Informational.”

- RFC 2081, *RIPng Protocol Applicability Statement*

RELATED DOCUMENTATION

Supported IPv4, TCP, and UDP Standards

Supported IPv6 Standards

Accessing Standards Documents on the Internet

Supported Standards for IS-IS

Junos OS substantially supports the following standards for IS-IS.

- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 8473, *Information technology — Protocol for providing the connectionless-mode network service*
- ISO 9542, *End System to Intermediate System Routing Exchange Protocol for Use in Conjunction with the Protocol for the Provision of the Connectionless-mode Network Service*
- ISO/IEC 10589, *Information technology — Telecommunications and information exchange between systems — Intermediate System to Intermediate System intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)*
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*
- RFC 5120, *M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)*
- RFC 5130, *A Policy Control Mechanism in IS-IS Using Administrative Tags*
- RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates*
- RFC 5301, *Dynamic Hostname Exchange Mechanism for IS-IS*
- RFC 5302, *Domain-Wide Prefix Distribution with Two-Level IS-IS*
- RFC 5303, *Three-Way Handshake for IS-IS Point-to-Point Adjacencies*
- RFC 5304, *IS-IS Cryptographic Authentication*

- RFC 5305, *IS-IS Extensions for Traffic Engineering*
- RFC 5306, *Restart Signaling for IS-IS*
- RFC 5307, *IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*
- RFC 5308, *Routing IPv6 with IS-IS*
- RFC 5310, *IS-IS Generic Cryptographic Authentication*
- RFC 5880, *Bidirectional Forwarding Detection (BFD)*
- RFC 6119, *IPv6 Traffic Engineering in IS-IS*
- RFC 6232, *Purge Originator Identification TLV for IS-IS*
- RFC 6233, *IS-IS Registry Extension for Purges*
- RFC 7775, *IS-IS Route Preference for Extended IP and IPv6 Reachability*
- RFC 7794, *IS-IS Prefix Attributes for Extended IPv4 and IPv6 Reachability*
- RFC 7981, *IS-IS Extensions for Advertising Router Information*
- RFC 8202, *IS-IS Multi-Instance*
- RFC 8518, *Selection of Loop-Free Alternates for Multi-Homed Prefixes*
- RFC 8570, *IS-IS Traffic Engineering (TE) Metric Extensions*
- RFC 8667, *IS-IS Extensions for Segment Routing*
- RFC 8706, *Restart Signaling for IS-IS*
- RFC 8919, *IS-IS Application-Specific Link Attributes*
- RFC 9350 *IGP Flexible Algorithm* (Partial support)
- RFC 9352, *IS-IS Extensions to Support Segment Routing over the IPv6 Data Plane*

The following RFCs do not define standards, but provide information about IS-IS and related technologies. The IETF classifies them as “Informational.”

- RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*
- RFC 2973, *IS-IS Mesh Groups*
- RFC 3277, *Intermediate System to Intermediate System (IS-IS) Transient Blackhole Avoidance*
- RFC 3358, *Optional Checksums in Intermediate System to Intermediate System (ISIS)*

- RFC 3359, *Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System*
- RFC 3373, *Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies*
- RFC 3567, *Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication*
- RFC 3719, *Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS)*
- RFC 3787, *Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS)*
- RFC 3847, *Restart Signaling for Intermediate System to Intermediate System (IS-IS)*
- RFC 5309, *Point-to-Point Operation over LAN in Link State Routing Protocols*
- RFC 6151, *updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms*
- Internet draft draft-ietf-isis-wg-255adj-02.txt, *Maintaining more than 255 circuits in IS-IS*
- Internet draft draft-przygienda-flood-reflector-00, *Flood Reflectors*
- Internet draft draft-przygienda-lsr-flood-reflection-01, *IS-IS Flood Reflection*

RELATED DOCUMENTATION

IS-IS Overview

Supported ES-IS Standards | 57

Accessing Standards Documents on the Internet | 2

Supported Standards for Segment Routing

Junos OS substantially supports the following RFCs and Internet drafts for Segment Routing.

- draft-agrawal-spring-srv6-mpls-interworking-06, *SRv6 and MPLS interworking*

  Supports service interworking.

- draft-ali-spring-sr-traffic-accounting, *SR traffic matrix accounting (Partial support)*

  Supports counter only.

- draft-bashandy-rtgwg-segment-routing-ti-lfa, *Topology Independent Fast Reroute using Segment Routing*
- draft-bashandy-rtgwg-segment-routing-uloop, *Microloop Avoidance using Segment Routing*
- draft-barth-pce-segment-routing-policy-cp-05, *PCEP extension to support Segment Routing Policy Candidate Paths*
- draft-filsfils-rtgwg-segment-routing-use-cases-02, *Segment Routing Use Cases*
- draft-filsfils-spring-sr-policy-considerations-05, *SR Policy Implementation and Deployment Considerations*
- draft-filsfils-spring-sr-traffic-counters, *SR traffic counters*
- draft-ginsberg-isis-prefix-attributes, *IS-IS Prefix Attributes for Extended IPv4 and IPv6 Reachability (Partial support)*
- draft-ietf-bess-srv6-services-07, *SRv6 BGP based Overlay Services*
- draft-ietf-idr-bgp-prefix-sid, *Advertise BGP segment for a BGP Prefix*
- draft-ietf-idr-bgpls-segment-routing-epe, *BGP-LS extensions for Egress peer traffic engineering using SR*
- draft-ietf-idr-segment-routing-te-policy, *Advertise SR-TE policies via BGP*
- draft-ietf-idr-segment-routing-te-policy-09, *Advertising Segment Routing Policies in BGP*
- draft-ietf-lsr-flex-algo-11.txt, *IGP Flexible Algorithm (Partial support)*

  Supports IS-IS only.
- draft-ietf-lsr-isis-srv6-extensions, *IS-IS Extensions to Support Segment Routing over IPv6 Dataplane*
- draft-ietf-ospf-segment-routing-extensions, *OSPF extensions to distribute SR segments*
- draft-ietf-pce-segment-routing, *PCE extensions to setup a SR-TE path from the controller (south bound)*
- draft-ietf-isis-segment-routing-extensions, *ISIS extensions to distribute SR segments*
- draft-ietf-rtgwg-segment-routing-ti-lfa-04, *Topology Independent Fast Reroute using Segment Routing*
- draft-ietf-spring-conflict-resolution, *Segment Routing MPLS Conflict Resolution*
- draft-ietf-spring-ipv6-use-cases, *Use Cases for IPv6 Source Packet Routing in Networking (Partial support)*

- draft-ietf-spring-resiliency-use-cases, *Resiliency use cases in SPRING networks*
- draft-ietf-spring-segment-routing-msdc, *BGP-Prefix Segment in Large Scale data centers (Partial support)*
- draft-ietf-spring-segment-routing-central-epe, *SR Centralized BGP Egress Peer Engineering*
- draft-ietf-spring-segment-routing-mpls, *Segment Routing details with MPLS forwarding*
- draft-ietf-spring-segment-routing-policy, *SR policy for TE (Partial support)*
- draft-ietf-spring-segment-routing-policy-07.txt, *Segment Routing Policy Architecture*
- draft-kaliraj-idr-bgp-classful-transport-planes-12, *BGP Classful Transport Planes*
- RFC 4971, *Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information (Partial support)*

  Supports counter only.
- RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates*
- RFC 7471, *OSPF Traffic Engineering (TE) Metric Extensions*
- RFC 7490, *Remote Loop-Free Alternate (LFA) Fast Reroute (FRR)*
- RFC 7684, *OSPFv2 Prefix/Link Attribute Advertisement*
- RFC 7752, *North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP*
- RFC 7855, *Source Packet Routing in Networking (SPRING) Problem Statement and Requirements*
- RFC 8102, *Remote-LFA Node Protection and Manageability*
- RFC 8277, *Using BGP to Bind MPLS Labels to Address Prefixes*
- RFC 8287, *LSP Ping/Traceroute for Segment Routing*
- RFC 8402, *Segment Routing Architecture (Partial support)*
- RFC 8403, *A Scalable and Topology-Aware MPLS Data-Plane Monitoring System*
- RFC 8426, *RSVP-SR coexistence*
- RFC 8570, *IS-IS Traffic Engineering (TE) Metric Extensions (Partial support)*

  Supports link delay related parameters.
- RFC 8571, *BGP - Link State (BGP-LS) Advertisement of IGP Traffic Engineering Performance Metric Extensions*

- RFC 8604, *Interconnecting Millions of Endpoints with Segment Routing*
- RFC 8660, *Segment Routing with the MPLS Data Plane*
- RFC 8661, *Segment Routing MPLS Interworking with LDP*
- RFC 8663, *MPLS Segment Routing over IP (Partial support)*
- RFC 8665, *OSPF Extensions for Segment Routing*
- RFC 8690, *Clarification of Segment ID Sub-TLV Length for RFC 8287*
- draft-xu-mpls-sr-over-ip, *MPLS Segment Routing over IP (Partial support)*
- RFC 8919, *IS-IS Application-Specific Link Attributes (Partial support)*
- RFC 8986, *Segment Routing over IPv6 (SRv6) Network Programming*
- RFC 9085, *Border Gateway Protocol - Link State (BGP-LS) Extensions for Segment Routing*
- RFC 9086, *Border Gateway Protocol - Link State (BGP-LS) Extensions for Segment Routing BGP Egress Peer Engineering*
- RFC 9256, *Segment Routing Policy Architecture*

The following RFCs do not define standards, but provide information about Segment Routing and related technologies. The IETF classifies them variously as “Experimental” or “Informational.”

- RFC 6571, *Loop-Free Alternate (LFA) Applicability in Service Provider (SP) Networks*
- RFC 9087, *Segment Routing Centralized BGP Egress Peer Engineering*

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

CHAPTER 9

Services PIC and DPC Standards

IN THIS CHAPTER

Supported DTCP Standard

Junos OS substantially supports Internet draft draft-cavuto-dtcp-03.txt, *DTCP: Dynamic Tasking Control Protocol*.

RELATED DOCUMENTATION

Accessing Standards Documents on the Internet | 2

Supported Flow Monitoring and Discard Accounting Standards

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions), Monitoring Services PICs, or Dense Port Concentrators (DPCs), Junos OS substantially supports the standards for cflowd version 5 and version 8 formats that are maintained by CAIDA and accessible at http://www.caida.org.

RFC 3954, *Cisco Systems NetFlow Services Export Version 9* does not define a standard but provides information about flow monitoring. The IETF classifies it as “Informational.”

Internet draft *draft-kumar-ippm-ifa-02.txt, Inband Flow Analyzer* does not define standards but provides information about Inband Flow Analyzer (IFA). You use this feature to record flow-specific information from an end station or switches across a network.

On MX Series routers, Junos OS partially supports the following RFCs:

- RFC 5101, *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information*
- RFC 5102, *Information Model for IP Flow Information Export*

RELATED DOCUMENTATION

Services Interfaces Overview for Routing Devices

MX Series 5G Universal Routing Platform Interface Module Reference

Accessing Standards Documents on the Internet | 2

Supported IPsec and IKE Standards

On routers equipped with one or more MS-MPCs, MS-MICs, or DPCs, the Canada and U.S. version of Junos OS substantially supports the following RFCs, which define standards for IP Security (IPsec) and Internet Key Exchange (IKE).

- RFC 2085, *HMAC-MD5 IP Authentication with Replay Prevention*
- RFC 2401, *Security Architecture for the Internet Protocol* (obsoleted by RFC 4301)
- RFC 2402, *IP Authentication Header* (obsoleted by RFC 4302)
- RFC 2403, *The Use of HMAC-MD5-96 within ESP and AH*
- RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH* (obsoleted by RFC 4305)
- RFC 2405, *The ESP DES-CBC Cipher Algorithm With Explicit IV*
- RFC 2406, *IP Encapsulating Security Payload (ESP)* (obsoleted by RFC 4303 and RFC 4305)
- RFC 2407, *The Internet IP Security Domain of Interpretation for ISAKMP* (obsoleted by RFC 4306)
- RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)* (obsoleted by RFC 4306)

- RFC 2409, *The Internet Key Exchange (IKE)* (obsoleted by RFC 4306)
- RFC 2410, *The NULL Encryption Algorithm and Its Use With IPsec*
- RFC 2451, *The ESP CBC-Mode Cipher Algorithms*
- RFC 2560, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*
- RFC 3193, *Securing L2TP using IPsec*
- RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*
- RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*
- RFC 3948, *UDP Encapsulation of IPsec ESP Packets*
- RFC 4106, *The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)*
- RFC 4210, *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*
- RFC 4211, *Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)*
- RFC 4301, *Security Architecture for the Internet Protocol*
- RFC 4302, *IP Authentication Header*
- RFC 4303, *IP Encapsulating Security Payload (ESP)*
- RFC 4305, *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*
- RFC 4306, *Internet Key Exchange (IKEv2) Protocol*
- RFC 4307, *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*
- RFC 4308, *Cryptographic Suites for IPsec*

  Only Suite VPN-A is supported in Junos OS.
- RFC 4754, *IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)*
- RFC 4835, *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*
- RFC 5996, *Internet Key Exchange Protocol Version 2 (IKEv2)* (obsoleted by RFC 7296)
- RFC 7296, *Internet Key Exchange Protocol Version 2 (IKEv2)*

- RFC 7427, *Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)*
- RFC 7634, *ChaCha20, Poly1305, and Their Use in the Internet Key Exchange Protocol (IKE) and IPsec*
- RFC 8200, *Internet Protocol, Version 6 (IPv6) Specification*

Junos OS partially supports the following RFCs for IPsec and IKE:

- RFC 3526, *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*
- RFC 5114, *Additional Diffie-Hellman Groups for Use with IETF Standards*
- RFC 5903, *Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2*

The following RFCs and Internet draft do not define standards, but provide information about IPsec, IKE, and related technologies. The IETF classifies them as "Informational."

- RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*
- RFC 2412, *The OAKLEY Key Determination Protocol*
- RFC 3706, *A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers*
- Internet draft draft-eastlake-sha2-02.txt, *US Secure Hash Algorithms (SHA and HMAC-SHA)* (expires July 2006)

RELATED DOCUMENTATION

Services Interfaces Overview for Routing Devices

MX Series 5G Universal Routing Platform Interface Module Reference

Accessing Standards Documents on the Internet

Supported L2TP Standards

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or Multiservices PICs or DPCs, Junos OS substantially supports the following RFC, which defines the standard for Layer 2 Tunneling Protocol (L2TP).

- RFC 2661, *Layer Two Tunneling Protocol "L2TP"*

The following RFC does not define a standard, but provides information about technology related to L2TP. The IETF classifies it as "Informational."

- RFC 2866, *RADIUS Accounting*

RELATED DOCUMENTATION

Services Interfaces Overview for Routing Devices

MX Series 5G Universal Routing Platform Interface Module Reference

Accessing Standards Documents on the Internet | 2

Supported Link Services Standards

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or DPCs, Junos OS substantially supports the following RFCs, which define standards for link services.

- RFC 1990, *The PPP Multilink Protocol (MP)*
- RFC 2364, *PPP Over AAL5*
- RFC 2686, *The Multi-Class Extension to Multi-Link PPP*

  The following features are not supported:

  - Negotiation of address field compression and protocol field compression PPP NCP options; instead, a full 4-byte PPP header is always sent
  - Prefix elision

RELATED DOCUMENTATION

Services Interfaces Overview for Routing Devices

MX Series 5G Universal Routing Platform Interface Module Reference

Accessing Standards Documents on the Internet | 2

Supported NAT and SIP Standards

The Junos OS substantially supports the following Network Address Translation (NAT) and Session Initiaion Protocol (SIP) standards. NAT supports SIP dialogs and UDP/IP version 4 (IPv4) transport of SIP messages.

NOTE: This is applied to Junos routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions), Multiservices PICs or DPCs, and services cards (SPC) of a security device (i.e. SRX).

Junos OS substantially supports the following RFC and Internet draft.

- RFC 3261, *SIP: Session Initiation Protocol*
- Internet draft draft-mrw-behave-nat66-01.txt, *IPv6-to-IPv6 Network Address Translation (NAT66)*

The following RFCs do not define standards, but provide information about NAT. The IETF classifies them variously as “Best Current Practice,” “Historic,” or “Informational.”

- RFC 1631, *The IP Network Address Translator (NAT)*
- RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*
- RFC 2766, *Network Address Translation - Protocol Translation (NAT-PT)*
- RFC 2993, *Architectural Implications of NAT*
- RFC 3022, *Traditional IP Network Address Translator (Traditional NAT)*
- RFC 4787, *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*
- RFC 5382, *NAT Behavioral Requirements for TCP*
- RFC 5508, *NAT Behavioral Requirements for ICMP*

RELATED DOCUMENTATION

Services Interfaces Overview for Routing Devices

MX Series 5G Universal Routing Platform Interface Module Reference

Accessing Standards Documents on the Internet | 2

Supported RPM, TWAMP, STAMP, and Benchmarking Test Standards

IN THIS SECTION

Real-Time Performance Monitoring (RPM) Standard

On routers and switches equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or DPCs, Junos OS substantially supports the Juniper-proprietary feature known as real-time performance monitoring (RPM), and provides MIB support with extensions in substantial support of RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*. Junos OS Evolved supports Packet-Forwarding-Engine-based or Routing-Engine-based RPM, and provides MIB support with extensions in substantial support of RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*.

Two-Way Active Measurement Protocol (TWAMP) and Simple Two-Way Active Measurement Protocol (STAMP) Standards

The Two-Way Active Management Protocol (TWAMP), described in RFC 5357 *Two-Way Active Measurement Protocol* , is an extension of the One-Way Active Management Protocol (OWAMP) that supplies two-way or round-trip measurements instead of unidirectional capabilities. Both Junos OS and Junos OS Evolved support RFC 5357, including Appendix I, which documents a simpler operational mode known as TWAMP Light. The Simple Two-Way Active Measurement Protocol (STAMP) is defined in RFC 8762 *Simple Two-Way Active Measurement Protocol* . RFC 8762 standardizes and extends this TWAMP Light operational mode. Junos OS Evolved supports RFC 8762.

Benchmarking Test Standard

RFC 2544 defines a series of tests that can be used to describe the performance characteristics of a network-interconnecting device, such as a router, and outlines specific formats to report the results of the tests. These tests can be used to benchmark interconnected network devices and devise a guideline or a measurement pattern to analyze the health and efficiency of the network devices. These tests are the standard benchmarking tests for Ethernet networks and are known as RFC 2544-based

benchmarking tests. Junos OS and Junos OS Evolved support RFC 2544, *Benchmarking Methodology for Network Interconnect Devices*.

RELATED DOCUMENTATION

- **Understanding Using Probes for Real-Time Performance Monitoring on M, T, ACX, MX, and PTX Series Routers, EX and QFX Switches**
- Services Interfaces Overview for Routing Devices
- MX Series 5G Universal Routing Platform Interface Module Reference
- Accessing Standards Documents on the Internet | 2

Supported Voice Services Standards

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or DPCs, Junos OS substantially supports the following RFCs, which define standards for technologies used with voice services.

- RFC 2508, *Compressing IP/UDP/RTP Headers for Low-Speed Serial Links*
- RFC 2509, *IP Header Compression over PPP*

RELATED DOCUMENTATION

- Services Interfaces Overview for Routing Devices
- MX Series 5G Universal Routing Platform Interface Module Reference

CHAPTER 10

VPLS and VPN Standards

IN THIS CHAPTER

Supported Carrier-of-Carriers and Interprovider VPN Standards

Junos OS substantially supports the following RFCs, which define standards for carrier-of-carriers and interprovider virtual private networks (VPNs).

- RFC 3107, *Carrying Label Information in BGP-4*
- RFC 3916, *Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)*

  Supported on MX Series routers with the Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP.
- RFC 3985, *Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture*

  Supported on MX Series routers with the Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP.
- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 6368, *Internal BGP as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*

RELATED DOCUMENTATION

- *Supported VPWS Standards*
- *Supported Layer 2 VPN Standards*
- *Supported Layer 3 VPN Standards*
- *Supported Multicast VPN Standards*
- *Supported VPLS Standards*
- Supported Standards for BGP
- Accessing Standards Documents on the Internet

Supported EVPN Standards

RFCs and Internet drafts that define standards for EVPNs:

- RFC 3704, *Ingress Filtering for Multihomed Networks*
- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4761, *Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*
- RFC 7209, *Requirements for Ethernet VPN (EVPN)*
- RFC 7432, *BGP MPLS-Based Ethernet VPN*

  The following features are not supported:

  - Automatic derivation of Ethernet segment (ES) values. Only static ES configurations are supported.
  - Host proxy ARP.
- RFC 7623, *Provider Backbone Bridging Combined with Ethernet VPN (PBB-EVPN)*
- RFC 8214, *Virtual Private Wire Service Support in Ethernet VPN*
- RFC 8317, *Ethernet-Tree (E-Tree) Support in Ethernet VPN (EVPN) and Provider Backbone Bridging EVPN (PBB-EVPN)*
- RFC 8365, *A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN)*
- RFC 8560, *Seamless Integration of Ethernet VPN (EVPN) with Virtual Private LAN Service (VPLS) and Their Provider Backbone Bridge (PBB) Equivalents*
- RFC 8667, *IS-IS Extensions for Segment Routing*

- RFC 9047, *Propagation of ARP/ND Flags in an Ethernet Virtual Private Network (EVPN)*
- RFC 9135, *Integrated Routing and Bridging in Ethernet VPN (EVPN)*
- RFC 9136, *IP Prefix Advertisement in Ethernet VPN (EVPN)*
- RFC 9161, *Operational Aspects of Proxy-ARP/ND in Ethernet Virtual Private Networks*
- RFC 9251, *Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Proxies for Ethernet VPN (EVPN)*
- Internet draft draft-ietf-bess-evpn-oam-req-frmwk, *EVPN Operations, Administration and Maintenance Requirements and Framework*
- Internet draft draft-ietf-bess-evpn-optimized-ir, *Optimized Ingress Replication solution for EVPN*
- Internet draft draft-ietf-bess-evpn-pref-df, *Preference-based EVPN DF Election*
- Internet draft draft-ietf-bess-evpn-virtual-eth-segment, *EVPN Virtual Ethernet Segment*
- Internet draft draft-ietf-bess-evpn-vpws-fxc, *EVPN VPWS Flexible Cross-Connect Service*
- Internet draft draft-ietf-bess-evpn-yang, *Yang Data Model for EVPN*
- Internet draft draft-ietf-spring-segment-routing-13, *Segment Routing Architecture*
- Internet draft draft-ietf-spring-segment-routing-mpls-11, *Segment Routing with MPLS data plane*
- Internet draft draft-wsv-bess-extended-evpn-optimized-ir, *Extended Procedures for EVPN Optimized Ingress Replication*
- Internet draft draft-lin-bess-evpn-irb-mcast, *EVPN Optimized Inter-Subnet Multicast (OISM) Forwarding*

RELATED DOCUMENTATION

EVPN Overview

Accessing Standards Documents on the Internet

Supported VPWS Standards

Junos OS substantially supports the following RFCs, which define standards for VPWS and Layer 2 circuits.

- RFC 4447, *Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*

  Junos OS does not support Section 5.3, "The Generalized PWid FEC Element."

- RFC 4448, *Encapsulation Methods for Transport of Ethernet over MPLS Networks*
- RFC 6074, *Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)*
- RFC 6391, *Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network*
- RFC 6790, *The Use of Entropy Labels in MPLS Forwarding*

The following Internet drafts do not define standards, but provide information about Layer 2 technologies. The IETF classifies them as "Historic."

- Internet draft draft-martini-l2circuit-encap-mpls-11.txt, *Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*

  Junos OS differs from the Internet draft in the following ways:

  - A packet with a sequence number of 0 (zero) is treated as out of sequence.
  - Any packet that does not have the next incremental sequence number is considered out of sequence.
  - When out-of-sequence packets arrive, the expected sequence number for the neighbor is set to the sequence number in the Layer 2 circuit control word.

- Internet draft draft-martini-l2circuit-trans-mpls-19.txt, *Transport of Layer 2 Frames Over MPLS*

RELATED DOCUMENTATION

Supported Carrier-of-Carriers and Interprovider VPN Standards

Supported Layer 2 VPN Standards

Supported Layer 3 VPN Standards

Supported Multicast VPN Standards

Supported VPLS Standards

Accessing Standards Documents on the Internet

Supported Layer 2 VPN Standards

Junos OS substantially supports the following standards and Internet drafts, which define standards for Layer 2 virtual private networks (VPNs).

- RFC 7348, *Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks*
- Internet draft draft-kompella-l2vpn-vpls-multihoming, *Multi-homing in BGP-based Virtual Private LAN Service*
- Internet draft draft-kompella-ppvpn-l2vpn-03.txt, *Layer 2 VPNs Over Tunnels*

RELATED DOCUMENTATION

Supported Carrier-of-Carriers and Interprovider VPN Standards

Supported VPWS Standards

Supported Layer 3 VPN Standards

Supported Multicast VPN Standards

Supported VPLS Standards

Accessing Standards Documents on the Internet

Supported Layer 3 VPN Standards

Junos OS substantially supports the following RFCs, which define standards for Layer 3 virtual private networks (VPNs).

- RFC 2283, *Multiprotocol Extensions for BGP-4*
- RFC 2685, *Virtual Private Networks Identifier*
- RFC 2858, *Multiprotocol Extensions for BGP-4*
- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*

  The traceroute functionality is supported only on transit routers.
- RFC 4576, *Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4577, *OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4659, *BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*

- RFC 4684, *Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*

The following RFCs do not define a standard, but provide information about technology related to Layer 3 VPNs. The IETF classifies them as a "Best Current Practice" or "Informational."

- RFC 1918, *Address Allocation for Private Internets*
- RFC 2917, *A Core MPLS IP VPN Architecture*

RELATED DOCUMENTATION

Supported Carrier-of-Carriers and Interprovider VPN Standards

Supported VPWS Standards

Supported Layer 2 VPN Standards

Supported Multicast VPN Standards

Supported VPLS Standards

Supported MPLS Standards

Supported Standards for BGP

Accessing Standards Documents on the Internet

Supported Multicast VPN Standards

Junos OS substantially supports the following RFCs and Internet draft, which define standards for multicast virtual private networks (VPNs).

- RFC 6513, *Multicast in MPLS/BGP IP VPNs*
- RFC 6514, *BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs*
- RFC 6515, *IPv4 and IPv6 Infrastructure Addresses in BGP Updates for Multicast VPN*
- RFC 6625, *Wildcards in Multicast VPN Auto-Discovery Routes*
- Internet draft draft-morin-l3vpn-mvpn-fast-failover-06.txt, *Multicast VPN Fast Upstream Failover*
- Internet draft draft-raggarwa-l3vpn-bgp-mvpn-extranet-08.txt, *Extranet in BGP Multicast VPN (MVPN)*
- RFC 7900, *Extranet Multicast in BGP/IP MPLS VPNs (partial support)*
- RFC 8534, *Explicit Tracking with Wildcard Routes in Multicast VPN (partial support)*

- RFC 9081, *Interoperation between Multicast Virtual Private Network (MVPN) and Multicast Source Directory Protocol (MSDP) Source-Active Routes*

RELATED DOCUMENTATION

Supported Carrier-of-Carriers and Interprovider VPN Standards

Supported VPWS Standards

Supported Layer 2 VPN Standards

Supported Layer 3 VPN Standards

Supported VPLS Standards

Supported MPLS Standards

Supported Standards for BGP

Accessing Standards Documents on the Internet

Supported VPLS Standards

Junos OS substantially supports the following Internet RFCs and draft, which define standards for virtual private LAN service (VPLS).

- RFC 4761, *Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*
- RFC 4762, *Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*

  FEC 128, FEC 129, control bit `0`, the Ethernet pseudowire type `0x0005`, and the Ethernet tagged mode pseudowire type `0x0004` are supported.
- RFC 6391, *Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network*
- RFC 6790, *The Use of Entropy Labels in MPLS Forwarding*
- Internet draft draft-kompella-l2vpn-vpls-multihoming, *Multi-homing in BGP-based Virtual Private LAN Service*

RELATED DOCUMENTATION

Supported Carrier-of-Carriers and Interprovider VPN Standards

Supported VPWS Standards

Supported Layer 2 VPN Standards