

Brocade Vyatta Network OS IPv6 Support Configuration Guide, 5.2R1

Supporting Brocade 5600 vRouter, VNF Platform, and Distributed
Services Platform

© 2016, Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, and MyBrocade are registered trademarks of Brocade Communications Systems, Inc., in the United States and in other countries. Other brands, product names, or service names mentioned of Brocade Communications Systems, Inc. are listed at www.brocade.com/en/legal/brocade-Legal-intellectual-property/brocade-legal-trademarks.html. Other marks may belong to third parties.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein or the computer programs that accompany it.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

Contents

Preface	5
Document conventions.....	5
Notes, cautions, and warnings.....	5
Text formatting conventions.....	5
Command syntax conventions.....	6
Brocade resources.....	6
Document feedback.....	6
Contacting Brocade Technical Support.....	7
Brocade customers.....	7
Brocade OEM customers.....	7
About This Guide	9
IPv6 Support Overview	11
IPv6 background.....	11
Supported standards.....	11
IPv6 addressing.....	12
Special addresses.....	13
IPv6 autoconfiguration.....	13
IPv6 forwarding.....	13
IPv6 neighbor discovery.....	14
Commands for IPv6.....	14
IPv6 Configuration Examples	15
Configure an IPv6 address on an interface.....	15
Verify IPv6 support.....	16
Display the IPv6 routing table.....	17
Confirm connectivity.....	17
Display IPv6 Neighbor Discovery (ND) cache.....	17
Clear ND cache.....	18
List of Acronyms	19

Preface

- Document conventions..... 5
- Brocade resources..... 6
- Document feedback..... 6
- Contacting Brocade Technical Support..... 7

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE

A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION

An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.



CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.



DANGER

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used to highlight specific words or phrases.

Format	Description
bold text	Identifies command names. Identifies keywords and operands. Identifies the names of GUI elements. Identifies text to enter in the GUI.
<i>italic text</i>	Identifies emphasis. Identifies variables. Identifies document titles.
Courier font	Identifies CLI output. Identifies command syntax examples.

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
<i>italic text</i>	Identifies a variable.
value	In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, --show WWN.
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ x y z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options. In Fibre Channel products, square brackets may be used instead for this purpose.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member[member...]</i> .
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Brocade resources

Visit the Brocade website to locate related documentation for your product and additional Brocade resources.

White papers, data sheets, and the most recent versions of Brocade software and hardware manuals are available at www.brocade.com.

Product documentation for all supported releases is available to registered users at MyBrocade.

Click the **Support** tab and select **Document Library** to access documentation on MyBrocade or www.brocade.com. You can locate documentation by product or by operating system.

Release notes are bundled with software downloads on MyBrocade. Links to software downloads are available on the MyBrocade landing page and in the Document Library.

Document feedback

Quality is our first concern at Brocade, and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. You can provide feedback in two ways:

- Through the online feedback form in the HTML documents posted on www.brocade.com
- By sending your feedback to documentation@brocade.com

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online, by telephone, or by e-mail. Brocade OEM customers should contact their OEM/solution provider.

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to www.brocade.com and select **Support**.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone	E-mail
<p>Preferred method of contact for non-urgent issues:</p> <ul style="list-style-type: none"> Case management through the MyBrocade portal. Quick Access links to Knowledge Base, Community, Document Library, Software Downloads and Licensing tools 	<p>Required for Sev 1-Critical and Sev 2-High issues:</p> <ul style="list-style-type: none"> Continental US: 1-800-752-8061 Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33) Toll-free numbers are available in many countries. For areas unable to access a toll-free number: +1-408-333-6061 	<p>support@brocade.com</p> <p>Please include:</p> <ul style="list-style-type: none"> Problem summary Serial number Installation details Environment description

Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/solution provider, contact your OEM/solution provider for all of your product support needs.

- OEM/solution providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/solution provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/solution provider.

About This Guide

This guide describes IPv6 support on Brocade products that run on the Brocade Vyatta Network OS (referred to as a virtual router, vRouter, or router in the guide).

IPv6 Support Overview

- IPv6 background..... 11
- Supported standards..... 11
- IPv6 addressing..... 12
- Special addresses..... 13
- IPv6 autoconfiguration..... 13
- IPv6 forwarding..... 13
- IPv6 neighbor discovery..... 14
- Commands for IPv6..... 14

IPv6 background

There are two versions of the Internet Protocol (IP) in use today. Version 4 (IPv4) is the version most commonly in use. However, there are issues with IPv4, and the Internet Engineering Task Force (IETF) has designated Version 6 (IPv6) to succeed IPv4 as the next-generation protocol for use on the Internet.

IPv6 has a number of advantages over IPv4. The following are four important ones:

- **Large address space**

An IPv4 address consists of four bytes (32 bits). IPv6 addresses consist of 16 bytes (128 bits). The increase from 32 to 128 bits results in a huge increase in the number of available addresses: 79 billion billion billion times the addresses available in the IPv4—this is about 10³⁸ addresses, or 10³⁰ addresses for each person on the planet.

The expanded address space means that IPv6 does not face the address exhaustion problems predicted imminently for IPv4. Furthermore, the availability for so many addresses means that private address spaces are not required, and that address shortage work-arounds such as Network Address Translation (NAT) can be eliminated. With no private addresses, there need be no hidden networks or hosts, and all devices can be globally reachable. A larger address space also means that features such as multihoming and aggregation are easier to implement.

- **Support for mobile devices**

A special protocol, Mobile IP, is required to support mobility. Mobile IP is not automatic in IPv4, and there are several challenges involved in implementing Mobile IP on IPv4 networks. In contrast, Mobile IP was designed into IPv6 from its inception, and is a mandatory feature in a standards-compliant IPv6 protocol stack.

- **Flexibility**

IPv6 includes multiple levels of hierarchy in the address space. This allows for hierarchical allocation of addressing and more efficient route aggregation. It also permits new kinds of addresses not possible in IPv4, such as link- and site-scoped addressing.

- **Security**

Because devices can be globally reachable, end-to-end security can be employed, which is not possible on an internetwork with hidden networks and hosts.

Supported standards

The Brocade vRouter implementation of IPv6 complies with the following standards:

- RFC 2460: *Internet Protocol, version 6 (IPv6) Specification*
- RFC 4443: *Internet Control Message Protocol (ICMPv6) for the Internet protocol version 6 (IPv6)*

IPv6 addressing

IP addresses generally take the following form:

```
x:x:x:x:x:x:x
```

where *x* is a 16-bit hexadecimal number; for example:

```
2001:0DB8:0000:0000:51DA:27C0:E4C2:0124
```

Addresses are case-insensitive; for example, the following is equivalent to the example given above:

```
2001:0db8:0000:0000:51da:27c0:e4c2:0124
```

Leading zeros are optional; for example, the following is a valid IPv6 address:

```
2001:DB8:0:0:51DA:27C0:E4C2:124
```

IPv6 addresses often contain many bytes with a value of zero. Successive fields of zeros can be represented by replacing them with a double colon, as in the following:

```
2001:DB8::51DA:27C0:E4C2:124
```

Similarly the following:

```
2001:DB8::124
```

is equivalent to the following:

```
2001:DB8:0:0:0:0:0:0124
```

and this:

```
0:0:0:0:0:0:0:1
```

is equivalent to this:

```
::1
```

The replacement by the double colon may be made only once within an address, as using the double colon more than once can result in ambiguity. For example, the following:

```
2001:DB8::27C0::0124
```

is ambiguous between these three addresses:

```
2001:0DB8:0000:27C0:0000:0000:0000:0124
2001:0DB8:0000:0000:27C0:0000:0000:0124
2001:0DB8:0000:0000:0000:27C0:0000:0124
```

IPv6 addresses that are extensions of IPv4 addresses can be written in a mixed notation, where the rightmost four bytes of the IPv6 address are replaced with the four decimal octets of the IPv4 address. In mixed notation, the four hexadecimal bytes are separated by colons and the four decimal octets are separated by dots, as in the following example:

```
2001:db8:0:1::192.168.100.51
```

which is equivalent to

```
2001:db8:0:1::c0a8:6433
```

Special addresses

Like IPv4, IPv6 has some special addresses, which are used by convention for special functions. For unicast addresses, these include the following:

- The unspecified address. This address is used as a placeholder when no address is available (for example, in an initial DHCP address), or to stand for “any” address. In IPv6, the unspecified address can be represented as either of the following:

```
0:0:0:0:0:0:0:0
::
```

- The localhost (loopback) interface. The loopback interface is a software interface that represents the local device itself. In IPv4, the address 127.0.0.1 is used by convention for the loopback interface. In IPv6, the loopback interface can be represented by either of the following:

```
0:0:0:0:0:0:0:1
::1
```

The IPv6 address architecture is quite rich, and includes types of addressing unavailable in IPv4, such as unicast and multicast scoped addresses, aggregatable global addresses, and anycast addresses. Multicast broadcast addresses do not exist in IPv6. For more information about the IPv6 address architecture, consult RFC 4291, *IP Version 6 Addressing Architecture*.

IPv6 autoconfiguration

IPv6 supports two mechanisms for automatically configuring devices with IP addresses: stateful and stateless. Both are supported in the Brocade 5600 vRouter.

In stateful configuration, addressing and service information is distributed by a protocol (DHCPv6) in the same way that the Dynamic Host Configuration Protocol (DHCP) distributes information for IPv4. This information is “stateful” in that both the DHCP server and the DHCP client must maintain the addressing and service information.

Stateless configuration uses the Stateless Address Autoconfiguration (SLAAC) protocol, which is a component of the larger Neighbor Discovery (ND) protocol. SLAAC has a host component and a router component.

In the host component of SLAAC, the IPv6 system constructs its own unicast global address from the system’s network prefix together with its Ethernet media access control (MAC) address. The device proposes this address to the network, without requiring approval from a server such as a DHCP server. The combination of network prefix and MAC address is assumed to be unique. Stateless autoconfiguration is performed by default by most IPv6 systems, including the Brocade vRouter.

In the router component of SLAAC, routers respond to Router Solicitation (RS) packets from hosts with network prefix information in the form of Router Advertisement (RA) packet. Hosts receive these advertisements and use them to form globally unique IPv6 addresses. The RS and RA packets also provide the router discovery function, allowing hosts to locate routers that are configured to serve as default routers. The Brocade vRouter fully supports router-side SLAAC and router discovery, including all required configurable parameters.

The ND protocol and the router discovery function are specified in RFC 4861. IPv6 Stateless Address Autoconfiguration is described in RFC 4862.

IPv6 forwarding

On the Brocade vRouter, IPv6 forwarding is enabled by default. If you want to disable IPv6 forwarding, use the following command in configuration mode: **set system ipv6 disable-forwarding**. This command is described in *Brocade Vyatta Network OS Basic System Configuration Guide*.

IPv6 neighbor discovery

IPv6 Neighbor Discovery (ND) provides a layer 3 to layer 2 address resolution mechanism for IPv6 similar to the way that Address Resolution Protocol (ARP) provides for layer 3 to layer 2 address resolution for IPv4.

ND resolution is carried out in both the data plane and the control plane; however, it is primarily carried out in the data plane. Note that ND caches in the control plane and data plane are no longer synchronized because entries in the two caches are managed independently. The data plane cache contains entries for both forwarded and locally terminated traffic. The control plane maintains cache entries only for destinations with which the local stack of the control plane communicates.

The advantages of implementing the ND protocol in the data plane are as follows:

- Avoids bandwidth issues in deployments with distributed data planes, because ND resolution can be performed locally rather than on a centralized controller.
- Improves performance because ND does not need to send all ND packets to the control plane.
- Protects against scanning DOS attacks due to resolution throttling.

Commands for IPv6

In addition to the general IPv6 information found in this document, information specific to major functions of the Brocade vRouter are found within the applicable documents for that function; for example, the following:

- Commands for enabling and disabling IPv6 on the system are located in *Brocade Vyatta Network OS Basic System Configuration Guide*.
- Commands for configuring IPv6 on a given interface are located in the guide that describes the interface. For example, commands for configuring IPv6 on an Ethernet interface are located in *Brocade Vyatta Network OS LAN Interfaces Configuration Guide*.
- Static IPv6 routing information can be found in *Brocade Vyatta Network OS Basic Routing Configuration Guide*.
- RIPng-related dynamic IPv6 routing information can be found in *Brocade Vyatta Network OS RIPng Configuration Guide*.
- BGP-related dynamic IPv6 routing information can be found in *Brocade Vyatta Network OS BGP Configuration Guide*.
- DHCPv6-related information can be found in *Brocade Vyatta Network OS Services Configuration Guide* as well as *Brocade Vyatta Network OS LAN Interfaces Configuration Guide*.
- Tunneling IPv6 over IPv4 is discussed in *Brocade Vyatta Network OS Tunnels Configuration Guide*.
- Multicast routing for IPv6 is discussed in *Brocade Vyatta Network OS IGMP and MLD Configuration Guide*.

IPv6 Configuration Examples

- Configure an IPv6 address on an interface.....15
- Verify IPv6 support.....16
- Display the IPv6 routing table.....17
- Confirm connectivity.....17
- Display IPv6 Neighbor Discovery (ND) cache.....17
- Clear ND cache.....18

Configure an IPv6 address on an interface

Figure 1 shows a simple network with two IPv6 nodes.

FIGURE 1 IPv6 address on an interface



IPv6 addresses are configured on data-plane interfaces in the same way that IPv4 addresses are. To configure dp0p1p3 on R1, perform the following steps in configuration mode.

TABLE 1 Add an IPv6 address to dp0p1p3 on R1

Step	Command
Add the IPv6 address to the dp0p1p3 interface.	<pre>vyatta@R1# set interfaces dataplane dp0p1p3 address 2001:db8:2::1/64</pre>
Commit the change.	<pre>vyatta@R1# commit</pre>
Verify the configuration.	<pre>vyatta@R1# show interfaces dataplane dp0p1p3 duplex auto hw-id b6:71:6b:8a:c9:3c mtu 1500 speed auto</pre>
Change to operational mode.	<pre>vyatta@R1# exit exit vyatta@R1:~\$</pre>
Show the status of the interfaces on R1.	<pre>vyatta@R1:~\$ show interfaces Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down Interface IP Address S/L Description dp0p1p1 - u/u dp0p1p2 - u/u dp0p1p3 2001:DB8:2::1/64 u/u dp0p1p4 - u/u</pre>

TABLE 1 Add an IPv6 address to dp0p1p3 on R1 (continued)

Step	Command
	<pre>lo 127.0.0.1/8 u/u lo ::1/128 u/u</pre>

To configure dp0p1p1 on R2, perform the following steps in configuration mode.

TABLE 2 Add an IPv6 address to dp0p1p1 on R2

Step	Command
Add the IPv6 address to the dp0p1p1 interface.	<pre>vyatta@R2# set interfaces dataplane dp0p1p1 address 2001:db8:2::2/64</pre>
Commit the change.	<pre>vyatta@R2# commit</pre>
Verify the configuration.	<pre>vyatta@R2# show interfaces dataplane dp0p1p1 address 2001:db8:2::2/64 duplex auto hw-id 3a:26:db:4d:63:a2 speed auto</pre>
Change to operational mode.	<pre>vyatta@R2# exit exit vyatta@R2:~\$</pre>
Show the status of the interfaces on R2.	<pre>vyatta@R2:~\$ show interfaces Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down Interface IP Address S/L Description dp0p1p1 2001:DB8:2::2/64 u/u dp0p1p2 - u/u dp0p1p3 - u/u lo 127.0.0.1/8 u/u lo ::1/128 u/u</pre>

Verify IPv6 support

A simple step to verify that IPv6 support is available is to configure the loopback interface with an IPv6 address and then ping it. To verify IPv6 support, perform the following step in operational mode.

TABLE 3 Confirm IPv6 support

Step	Command
Ping the loopback interface.	<pre>vyatta@R1:~\$ ping ::1 PING ::1(::1) 56 data bytes 64 bytes from ::1: icmp_seq=1 ttl=64 time=2.13 ms 64 bytes from ::1: icmp_seq=2 ttl=64 time=0.086 ms ^C --- ::1 ping statistics --- 2 packets transmitted, 2 received, 0% packet loss, time 1006ms rtt min/avg/max/mdev = 0.086/1.112/2.138/1.026 ms</pre>

Display the IPv6 routing table

When an IPv6 address is added to an interface, a connected network for it appears in the routing table. To display the routing table, perform the following step in operational mode.

TABLE 4 Display the IPv6 routing table

Step	Command
Show the routing table.	<pre>vyatta@R1:~\$ show ipv6 route IPv6 Routing Table Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2, I - IS-IS, B - BGP > - selected route, * - FIB route, p - stale info Timers: Uptime C>* ::1/128 is directly connected, lo C>* 2001:db8:2::/64 is directly connected, dp0p1p3 C * fe80::/64 is directly connected, dp0p1p3 C * fe80::/64 is directly connected, dp0p1p2 C>* fe80::/64 is directly connected, dp0p1p1 K>* ff00::/8 is directly connected, dp0p1p3</pre>

Confirm connectivity

To confirm that R1 and R2 can communicate, use the **ping** command. To confirm connectivity, perform the following step in operational mode.

TABLE 5 Confirm connectivity between R1 and R2

Step	Command
Ping R2 from R1.	<pre>vyatta@R1:~\$ ping 2001:db8:2::2 PING 2001:db8:2::2(2001:db8:2::2) 56 data bytes 64 bytes from 2001:db8:2::2: icmp_seq=1 ttl=64 time=6.52 ms 64 bytes from 2001:db8:2::2: icmp_seq=2 ttl=64 time=0.333 ms ^C --- 2001:db8:2::2 ping statistics --- 2 packets transmitted, 2 received, 0% packet loss, time 1013ms rtt min/avg/max/mdev = 0.333/3.427/6.522/3.095 ms</pre>

Display IPv6 Neighbor Discovery (ND) cache

To display a list of neighbors in the Neighbor Discovery (ND) caches in both the data plane and the controller, use the **show ipv6 neighbors** command. To display the ND cache in the data plane only use the **show ipv6 neighbors**. Perform the following step in operational mode.

TABLE 6 Display the ND cache

Step	Command
Display the list of known neighbors in both the data	<pre>vyatta@R1:~\$ show ipv6 neighbors</pre>

TABLE 6 Display the ND cache (continued)

Step	Command
plane and the controller.	<pre>IPv6 Address HW address Dataplane Controller Device 2001:db8:2::2 52:54:0:9b:6a:3f VALID [REACHABLE] VALID [REACHABLE] dp0p1p3 fe80::20c:29ff:fe4e:fc6 52:54:0:9b:6a:3f VALID [DELAY] VALID [REACHABLE] dp0p1p3</pre>
Display the list of known neighbors only in the data plane.	<pre>vyatta@R1:~\$ show dataplane nd IPv6 Address HW address Flags State Device 2001:db8:2::2 52:54:0:9b:6a:3f VALID REACHABLE dp0p1p3 fe80::20c:29ff:fe4e:fc6 52:54:0:9b:6a:3f VALID DELAY dp0p1p3</pre>

Clear ND cache

To clear the Neighbor Discovery (ND) cache, use the **reset ipv6 neighbors** command. To clear the ND cache on interface dp0p1p3, perform the following step in operational mode.

TABLE 7 Clear the ND cache

Step	Command
Clear the list of known neighbors on dp0p1p3.	<pre>vyatta@R1:~\$ reset ipv6 neighbors interface dp0p1p3</pre>

List of Acronyms

Acronym	Description
ACL	access control list
ADSL	Asymmetric Digital Subscriber Line
AH	Authentication Header
AMI	Amazon Machine Image
API	Application Programming Interface
AS	autonomous system
ARP	Address Resolution Protocol
AWS	Amazon Web Services
BGP	Border Gateway Protocol
BIOS	Basic Input Output System
BPDU	Bridge Protocol Data Unit
CA	certificate authority
CCMP	AES in counter mode with CBC-MAC
CHAP	Challenge Handshake Authentication Protocol
CLI	command-line interface
DDNS	dynamic DNS
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DLCI	data-link connection identifier
DMI	desktop management interface
DMVPN	dynamic multipoint VPN
DMZ	demilitarized zone
DN	distinguished name
DNS	Domain Name System
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
eBGP	external BGP
EBS	Amazon Elastic Block Storage
EC2	Amazon Elastic Compute Cloud
EGP	Exterior Gateway Protocol
ECMP	equal-cost multipath
ESP	Encapsulating Security Payload
FIB	Forwarding Information Base
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HDLC	High-Level Data Link Control
I/O	Input/Output
ICMP	Internet Control Message Protocol

Acronym	Description
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IPS	Intrusion Protection System
IKE	Internet Key Exchange
IP	Internet Protocol
IPOA	IP over ATM
IPsec	IP Security
IPv4	IP Version 4
IPv6	IP Version 6
ISAKMP	Internet Security Association and Key Management Protocol
ISM	Internet Standard Multicast
ISP	Internet Service Provider
KVM	Kernel-Based Virtual Machine
L2TP	Layer 2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAN	local area network
LDAP	Lightweight Directory Access Protocol
LLDP	Link Layer Discovery Protocol
MAC	medium access control
mGRE	multipoint GRE
MIB	Management Information Base
MLD	Multicast Listener Discovery
MLPPP	multilink PPP
MRRU	maximum received reconstructed unit
MTU	maximum transmission unit
NAT	Network Address Translation
NBMA	Non-Broadcast Multi-Access
ND	Neighbor Discovery
NHRP	Next Hop Resolution Protocol
NIC	network interface card
NTP	Network Time Protocol
OSPF	Open Shortest Path First
OSPFv2	OSPF Version 2
OSPFv3	OSPF Version 3
PAM	Pluggable Authentication Module
PAP	Password Authentication Protocol
PAT	Port Address Translation
PCI	peripheral component interconnect
PIM	Protocol Independent Multicast
PIM-DM	PIM Dense Mode

Acronym	Description
PIM-SM	PIM Sparse Mode
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PTMU	Path Maximum Transfer Unit
PVC	permanent virtual circuit
QoS	quality of service
RADIUS	Remote Authentication Dial-In User Service
RHEL	Red Hat Enterprise Linux
RIB	Routing Information Base
RIP	Routing Information Protocol
RIPng	RIP next generation
RP	Rendezvous Point
RPF	Reverse Path Forwarding
RSA	Rivest, Shamir, and Adleman
Rx	receive
S3	Amazon Simple Storage Service
SLAAC	Stateless Address Auto-Configuration
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SONET	Synchronous Optical Network
SPT	Shortest Path Tree
SSH	Secure Shell
SSID	Service Set Identifier
SSM	Source-Specific Multicast
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus
TBF	Token Bucket Filter
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
ToS	Type of Service
TSS	TCP Maximum Segment Size
Tx	transmit
UDP	User Datagram Protocol
VHD	virtual hard disk
vif	virtual interface
VLAN	virtual LAN
VPC	Amazon virtual private cloud
VPN	virtual private network
VRRP	Virtual Router Redundancy Protocol

Acronym	Description
WAN	wide area network
WAP	wireless access point
WPA	Wired Protected Access