

TECHNICAL NOTE

DEPLOYING STRM IN AN IPV6 ENVIRONMENT

JANUARY 2009

STRM 2008.3 introduces support for deployment in IPv4, IPv6, or mixed environments. IPv4 and IPv6 addressing is supported for network connectivity and management of STRM software and appliances. When you install STRM, you are prompted to specify whether your Internet protocol is an IPv4 or IPv6 environment. If you are upgrading to STRM 2008.3, you will not be prompted to specify your Internet protocol. After the upgrade, however, you can change IP addressing using the `qchange_netsetup` command. For more information, see the *STRM Installation Guide*.

This document provides the following information:

- [Understanding IPv6](#)
- [IPv6 Configuration Considerations](#)
- [Known Limitations](#)

Understanding IPv6

IPv6 is an Internet protocol for packet-switched networks. IPv6 has a larger address space than IPv4, thus allowing flexibility in allocating addresses and routing traffic. Event and flow records contain normalized fields for IPv6 addresses. Also, Device Support Modules (DSMs) can parse IPv6 source and destination address from event payloads.

IPv6 Integration with STRM

The following STRM components support IPv6:

- [Flow Viewer](#)
- [Event Viewer](#)
- [Searching, Grouping, and Reporting on IPv6 Fields](#)
- [Custom Rules](#)
- [Deployment Editor](#)

Flow Viewer

Depending on your deployment, the Flow Viewer can display four IP address fields:

- Source IP Address
- Destination IP Address

- IPv6 Source Address
- IPv6 Destination Address

To save space and indexing in a native IPv4 or IPv6 source environment, additional IP address fields are not stored or displayed. In a mixed IPv4/IPv6 environment, a flow record contains both IPv4 and IPv6 addresses.

IPv6 addresses are supported for both packet data, including sFlow, and NetFlow V9 data. However, older versions of NetFlow may not support IPv6.

Event Viewer Depending on your deployment, the Event Viewer can display four IP address fields:

- Source IP Address
- Destination IP Address
- IPv6 Source Address
- IPv6 Destination Address

When an address does not exist, template-based records are used to avoid wasted space.

DSMs can parse IPv6 addresses from the event payload. If any DSM can not parse IPv6 addresses, a DSM Extension can parse the addresses.

**Searching, Grouping,
and Reporting on
IPv6 Fields**

In an IPv6 or mixed deployment, you can:

- Search events and flows using IPv6 parameters in the search criteria.
- Group and sort event and flow records based on IPv6 parameters.
- Base reports on data from IPv6-based searches.

Custom Rules

A custom rule has been added to support IPv6 addressing:

- SRC/DST IP = IPv6 Address
- IPv6-based building blocks have also been added for use in additional rules.

Deployment Editor

The Deployment Editor supports IPv6 addresses.

**IPv6 Configuration
Considerations**

When deploying STRM 2008.3 in an IPv6 or mixed environment, consider the following:

- In a non-IPv6 DNS environment, use the `/etc/hosts` parameter for address translation.
- Flow sources, such as NetFlow and sFlow, can be accepted from IPv4 and IPv6 addresses.

- Event sources, such as syslog and SNMP, can be accepted from IPv4 and IPv6 addresses.
- Disable superflows and flow bundling in an IPV6 environment. See *STRM Administration Guide*.
- STRM 2008.3 currently does not support adding an IPv4-only managed host to an IPv6/IPv4 mixed mode console.

To setup an IPv4-only managed host in a mixed mode system:

Step 1 Install your STRM Console as IPV6.

Step 2 On the Console, enter the following command:

```
opt/qradar/bin/setup_v6v4_console.sh
```

Step 3 To add an ipv4 managed host, enter the following command

```
/opt/qradar/bin/add_v6v4_host.sh
```

Step 4 Add the managed host through the interface.

Known Limitations

When STRM 2008.3 is deployed in an IPv6 environment, the following limitations are known:

- The network hierarchy is not updated to support IPv6. Some aspects of the STRM deployment, including surveillance, searching, and analysis, do not take advantage of the network hierarchy. For example, within the Event Viewer, you cannot search or aggregate events By Network.
- No IPv6-based Asset Profiles. Asset Profiles will only be created if STRM receives events, flows, and vulnerability data for IPv4 hosts.
- No host profile test in custom rules for IPv6 addresses
- No specialized indexing or optimization of IPv6 addresses
- No IPv6-based attackers and targets for offenses.

Copyright Notice

Copyright © 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Part Number 530-028626-01