Remote Packet Capture
<draft-bullard-pcap-00.txt>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026 [1].

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet- Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

1 Copyright Notice

Copyright (C) The Internet Society (2000). All Rights Reserved.

2 Abstract

This memo describes a set of recommendations for remote packet capture. The approach is designed to address deployment, performance and privacy issues that limit the usefulness of existing packet capture technology.
Overview

Packet capture is a fundamental mechanism in Internet network management and is used in support of a wide range of network operational functions, such as fault detection, protocol functional assurance, performance analysis, and security assessment. The IETF has specified technology for remote packet capture in RMON, STD-59[2], and working groups, such as RMON and IPPM, continue to describe various aspects of packet capture technology in RMON2, RFC-2021[3], SMON, RFC-2613[4], and IPPM, RFC-2330[5].

With new network paradigms and new network analytic requirements, existing packet capture technology is finding its limits, and vendors are generating proprietary mechanisms to overcome these hurdles. To address the issue of proprietary remote packet capture mechanisms in the switched network environment, the SMON MIB introduced the concept of an extended data source mechanism. This facility is designed to support vendors supplied "Copy Port" functions, and does not address the general issue of proprietary remote packet capture.

This proposal recommends specification of a remote packet capture source facility that can act as a reliable external packet capture point in Internet networks. Designed to support a number of existing applications, such as RMON and RTFM, a remote packet capture facility should also enable new applications, such as those emerging from the IPPM and TE WGAs.

This proposal recommends that new remote packet capture mechanisms support full wire speed packet header capture, with wireline...
timestamping, and in-band transport of the captured data to overcome the perceived limitations of existing technology.

5 Remote Packet Capture Requirements/Goals

5.1 High Performance Packet Capture

A remote packet capture source facility should perform at a level that assures comprehensive packet capture at full duplex line rate, without packet loss. If packet loss does occur, the condition should be detectable and possibly quantifiable.

Existing RMON packet capture technology cannot support sustained packet capture at existing link speeds, primarily due to local storage requirements. Port mirroring, or port copy, based packet capture technology, can perform full packet capture at wireline rates, but these mechanisms have inherent congestion problems when mirroring full duplex interfaces, and congestion related packet loss is not detectable or reportable.

5.2 Distributed Monitoring Applications

A remote packet capture facility should provide reliable packet capture in asymmetric network architectures. Remote capture facilities should also support distributed monitoring applications, such as those where the same packet must be monitored at multiple points along its path.

Both of these situations require multiple remote capture points with packet event correlation handled by a mediation device. Remote packet strategies should support this type of application.

5.3 Support Remote Captured Packet Storage

One of the primary performance limitations in existing remote packet capture technology is the architectural requirement for local storage of captured packets. Because of the need to support very high-speed packet capture, any new remote packet strategy should support remote capture storage.

5.4 Wireline Packet Timestamping

In order to perform time dependant analysis of network events, accurate time reporting is critical. All packet capture technology should support/conform to the wireline timestamp guidelines as described in the IPPM WG's Framework document, RFC-2330.

5.5 Privacy Threat Issues

Packet capture can pose a threat to individual privacy as it can be used to support unauthorized disclosure. In order to address this important issue, new packet capture technology must adopt strategies
that help to minimize these threats when packet capture is used to support authorized tasks.

5.5.1 Content Separation

Network management functions, such as RMON, must inspect some aspect of network datagram content in order to perform the designed function. If a particular network management function is an authorized function, then the minimum set of packet data required to support the authorized function will represent authorized data. All other packet contents can be referred to as unauthorized data content.

Current packet capture technology does not support the separation of authorized data from unauthorized data, and as a result, current technology can pose a threat to privacy even when used to support authorized functions.

A primary requirement of future packet capture technology should be that the facility support selective capture of authorized information.

5.5.2 Captured Content Protection

Captured packet contents MUST be protected from unauthorized modification and/or disclosure.

Integrity protection for captured packet contents is very important not only because network management decisions and actions will be made based on captured packet contents, but because fraudulent packet capture data can have significant impacts on individual privacy.

5.6 Partial Packet Capture

Remote packet capture facilities should provide selective length packet capture. Applications may require full packet capture of a subset of network traffic, such as ICMP packets, but require only partial packet contents for other network traffic.

A few examples would be Layer 2 header content capture to support the RMON Ethernet History function, or simple MPLS tag capture to support emerging TE performance measurements.

6 Recommendations

6.1 Packet Header Capture

In order to support performance, security and application specific issues in remote packet capture, this proposal recommends that remote packet capture technology support packet capture on protocol header boundaries.
If a network management function has authority to access IP header content information from packets of interest, such as the information needed to compile a RMON HostTopN list, the remote packet data source that is supplying the information needed for this function should be designed to provide only the IP header from packets of interest.

This approach will significantly reduce the captured packet load, and limit the capture to the minimum set of information required of the application.

And because there are hardware packet classifiers that are currently available that can make header boundary determinations at wireline speeds, this approach can be implemented as an integrated mechanism in high performance equipment.

6.2 Captured Packet Encapsulation Header

To support distributed packet capture, partial packet capture, and wireline timestamping, this proposal recommends pre-pending captured packets with a captured packet header.

```
+-----------------+-----------------+-----------------+-----------------+
| Source Identifier | ifIndex          | Interface Type  |
| +-----------------+-----------------+-----------------+-----------------+-----------------+-----------------+-----------------+-----------------+
| Status           | Length           | Status           | Length           | Status           | Length           | Status           | Length           |
| +-----------------+-----------------+-----------------+-----------------+-----------------+-----------------+-----------------+-----------------+
| Sequence Number  | Time Stamp (sec) | Time Stamp (nsec) | Captured Packet Data |
+-----------------+-----------------+-----------------+-----------------+
```

Draft PCAP Header Format

Bullard Informational-Expires May 2001

Remote Packet Capture November, 2000

6.3 In-Band Captured Packet Transport

In order to support high-speed integrated implementations, as well as to meet the requirement to support remote captured packet storage and security protection for captured packets, this proposal recommends In-Band transport of captured packets.

By pre-pending an IP header, whether the captured datagrams are targeted for an integrated packet capture application, or to a truly
remote network monitoring application, a remote packet capture facility can now route captured packets, and provide wireline protections through IP Sec.

In-Band transport may require fragmentation when supporting large packet capture sizes.

7 Security Considerations

Protection against known security threats such as unauthorized access, modification or disclosure of remotely captured packet content can be accomplished using existing IETF specified technology, particularly SNMPv3 and IPsec.

Threats against captured packet data while resident in a persistent store is beyond the scope of this document.

8 References

1 Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.


9 Acknowledgments

10 Author’s Addresses

Carter Bullard
QoSient, LLC.
300 E. 56th Street, Suite 17A
New York, New York 10022-1439
Phone: +1 212 813 9426
Email: carter@qosient.com