# Conditional Protocol Slicing

Many network monitoring tools are only interested in the layer 2, possibly layer 3, possibly layer 4, maybe part of the payload and information in an IP packet and either are not allowed to store, or have no interest in, the actual packet's content beyond that. Despite that, these tools still have to manage the entire packet for every flow that is received, which places an unnecessary load on the tool and traffic backhaul, in turn requiring sufficient processing resources, transport pipes, and NICs to handle the volume of data.

## Conditional Slicing

Typical application examples include:

- Security monitoring, where court orders may authorize monitoring of certain information such as originating IP address or URL but not the actual content of the traffic
- Voice over IP (VoIP) monitoring where the UDP and RTP header information is used to estimate voice quality but the actual RTP payload (encoded voice) is not required

Because deploying many monitoring tools with heavyweight processing resources and many interfaces tends to be costly, it is more cost-effective to make use of packet flow switches that have the ability to strip off the data, not required by the monitoring tools, before the flows or packets are forwarded to the tools.

Packet slicing is a traffic grooming technique traditionally done in a network analyzer at the monitoring infrastructure layer. It defines and discards part of a packet from the copy of traffic that had been sent to that analyzer, thereby allowing it to process and store more data of interest. It also dramatically reduces the amount of monitoring traffic that needs to be sent back to the monitoring applications.

In many cases, not all traffic either needs or is wanted to be sliced, and so the packet slicing should only be performed based on certain conditions, e.g. specific packet type and content.

## Slice Closer to the Network

Conditional protocol slicing (vSlice) supported by NETSCOUT nGenius® Packet Flow Switches (PFS) extends the capability of packet slicing manifold by allowing users to perform packet slicing at the traffic capture layer, anywhere in a network. Unlike competitive technologies, vSlice performs conditional packet slicing, which enables users to set slice points at different offsets for each packet, specify the types of traffic to be sliced, such as HTTP and the VoIP protocols RTP and RTCP, and only slice packets that contain specific content.

Conditional protocol slicing enables packet slicing to occur at the point of traffic capture, instead of at each analytical tool. As a result, conditional slicing can be used to ensure uniform and consistent packet slicing at one or many network segments. One or more instances of conditional slicing can extend the coverage of multiple analytical tools.

## Greater Security

By acting at the point of capture, conditional slicing permits the removal of end-user identifying information at the beginning of the traffic capture process, reducing the risk of a privacy breach. Conditional protocol slicing helps ensure compliance with regulations mandating privacy best practices, such as the Payment Card Industry Data Security Standard (PCI DSS), which requires limiting access to cardholder information to on a need-to-know basis.

## Conditional Protocol Slicing

Conditional protocol slicing can be applied on multiple ports of an nGenius PFS device, independent of other settings such as port mapping. Conditional slicing is available at 1, 10, and 40 GigE speeds, and on copper as well as fiber media.

The conditional slicing feature is available on nGenius PFS models 2204, 4204, and 6010, and provides the ability to conduct conditional slicing of the packets, from a user-defined point, such that only the content of each packet required is retained in the monitoring traffic that is sent to the tools.

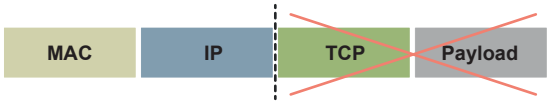


**Figure 1: IP Slicing Example.**


**Figure 2: RTP Slicing Example.**

The packet to be selected for slicing is determined by a filter expression. The point at which the slicing occurs is determined by an anchor point and offset value. Up to eight different combinations of filter and slicing point can be used per port. After stripping or slicing, the CRC is recalculated for each packet.

## Advantages

Competitive offerings of slicing do not contain the conditional element as a part of their slicing, but rather rely on a combination of pre- or forwarding filters and then fixed offset slicing. The two main disadvantages of this approach are:

- While the initial filtering helps to separate out the traffic to be sliced, it also removes other traffic from being sent to the tool
  - Conditional slicing employs filter expressions as part of its method for determining which traffic packets to slice. This is completely separate to any actual traffic filtering, which can be employed in combination with conditional slicing
- By utilizing a fixed offset, slicing will always be conducted at the same numerical byte position in the packet
  - The user-definable anchor points and offsets enable slicing to be conducted at the desired point in a packet, even if that point varies in terms of its numerical byte position in each packet. Up to eight different combinations of filters and slicing points can be defined per port

NETSCOUT

**Americas East**
310 Littleton Road
Westford, MA 01886-4105
Phone: 978-614-4000
Toll Free: 800-357-7666

**Americas West**
178 E. Tasman Drive
San Jose, CA 95134
Phone: 408-571-5000

**Asia Pacific**
17F/B
No. 167 Tun Hwa N. Road
Taipei 105, Taiwan
Phone: +886 2 2717 1999

**Europe**
One Canada Square
29th floor, Canary Wharf
London E14 5DY, United Kingdom
Phone: +44 207 712 1672

NETSCOUT offers sales, support, and services in over 32 countries.

**For more information, please visit www.netscout.com or contact NETSCOUT at 800-309-4804 or +1 978-614-4000**