The Power of Decapsulation

By **Iain Kenney**, Senior Director and Head of Product Management

The days are getting a little colder even here in North Carolina. I am sure our message to our kids (and adults alike) is that layers are good, especially as it does get a little colder! "You can always take off the jacket when you get to school" etc.. etc.. 🙂

Well as a long-time networking guy, layers have always been important to me all year round. Those layers are a little different to the trousers, jumper, jacket layers that we recommend to our kids. They are more like MAC headers, IP headers, VLANs, QinQ and other specific protocols. These form layers in the packets that our software and devices depend upon for correct operation.

These layers/headers/encapsulations allow devices such as switches, routers, and more intelligent middle boxes and ultimately clients and servers to correctly process the packets to achieve the goals intended. Conversely these layers can be used to block malicious packets from getting to the client or server that they are trying to access/hack.

cPacket appliances, especially the Packet Broker (cVu NG) family have always sought to have a flexible scalable approach to packet processing. Normally sitting out-of-band to receive and forward packets to tools including Packet Capture (cStor S) these tools can sometimes and sometimes not handle the respective headers/tags/encapsulations that were replicated from the production network. Such as a tool which does not want all the VLAN tags but just the "original" VLAN tag coming from the network and not a tag which was added by the monitoring infrastructure etc. Similarly, when an ERSPAN packet is received by the Packet Broker it needs to be removed before being sent onto tools which don't understand or need (or care about!!) the ERSPAN headers etc.

Most recently the cPacket Packet Broker team has added support for TrustSec stripping. TrustSec is a suite of connected technologies described by Cisco as "… TrustSec builds secure networks by establishing domains of trusted network devices." [1] Clearly this can and should be an important protocol/approach for network security. However, once the packet is sent to the Packet Broker it is outside the scope of TrustSec and passing the Header isn't required so rather than confusing downstream tools customers can now enable TrustSec stripping and the headers will be removed.

(1) https://community.cisco.com/kxiwq67737/attachments/kxiwq67737/discussions-sd-access/2461/1/cisco_trustsec_overview.pdf

Other protocols can be handled in a similar way, including VXLAN and Geneve for public and private cloud deployments. Ultimately packets of any shape and size along with potentially multiple headers and tags can be processed before being sent to a set of tools which are not quite as flexible.

Having FPGAs on each port in the Packet Broker (cVu NG) family gives cPacket great flexibility to modify packets at line-rate enabling numerous features to be enabled without any impact to performance (or the cost of the device!). Any stripping features are selectively applied to only modify packets which have those specific protocols rather than "chopping" all packets unnecessarily. Additionally, the packets have their checksum recalculated so that any interconnected switches do not drop these modified packets!

cPacket products support a wide range of protocols which can be decapsulated or stripped. So, if you are a tools vendor who needs correctly formatted packets to be sent to your tool in the datacenter or in the public/private cloud or if you are an end user who would like to roll out additional tools or technologies which may need to be stripped by your monitoring infrastructure please reach out and cPacket would be happy to help.

About cPacket Networks

cPacket Networks de-risks IT I&O through network-aware service and security assurance across hybrid and multi-cloud environments. Our AIOps-ready Intelligent Observability Platform provides single-pane-of-glass analytics and deep network visibility required for complex IT environments enabling Fortune 500 organizations around the world to keep their business running. cPacket solutions are fully reliable, tightly integrated, and consistently simple. Our cutting-edge technology enables network, application, and security teams to proactively identify issues before negatively impacting the business. The result: increased service agility, enhanced experience assurance, and faster transactional velocity. Learn more at **cpacket.com**.

BL-111924