TECHNOLOGY BRIEF

APCON
Solutions for Networks

COLLECT UNSAMPLED NETFLOW TRAFFIC FROM MULTIPLE DEVICES

NetFlow Solutions using the IntellaView Platform

When you are responsible for monitoring and security appliances, you need clear data visibility for analysis of network traffic to protect against dangerous or unwanted flows. NetFlow helps to understand the context of network conversations by identifying flows or strings of related network packets. The data collection process for NetFlow generation is delivered using advanced traffic management for ultra-high-speed networks.

APCON's latest hardware solutions are capable of aggregating large volumes of network traffic. The IntellaView platform monitors high-speed 100G data flows and is an ideal, scalable source of NetFlow records for analyzing and reporting traffic statistics according to your network needs.

CHALLENGES

ADVANCED PACKET PROCESSING TO FEED COLLECTION TOOLS

A common challenge for data centers is collecting the full flow of unsampled traffic from all the devices on the network, but lacking the tools to accomplish it. APCON provides network solutions to collect flows from routers in various parts of the network and feed this data to both a network and a security solution.

Unfortunately, many routers cannot handle the unsampled data flows; consequently, these projects often stall. APCON IntellaView series switches, shown below, can collect this traffic and convert it to flows without conducting any sampling.

Figure 1 | APCON's IntellaView Hardware Products (Switch sizes: 9RU, 5RU, 3RU, EdgeSwitch)

THE SMART SOLUTION

COLLECT NETFLOW TRAFFIC WITH THE INTELLAVIEW PLATFORM

APCON solutions can convert packets to NetFlow records and deliver the information to any collector solution in your environment. APCON IntellaView aggregates the packets coming off the wire from various parts of your network to an aggregation blade within a chassis. The traffic is then sent to service engines on an IntellaView HyperEngine blade in the same chassis where it converts the packets to NetFlow version 5, 9, or IPFIX. The IntellaView HyperEngine blade has six service engines and processes 100Gbps of traffic per engine, in addition to other advanced services.

To assist in tracking the flow of data, APCON can also make use of an iFindex value (interface index value). Customers need to be able to identify where in their network the traffic flow is originating. The iFindex is a unique identifying value associated with a physical or logical interface and represents the actual port receiving traffic from the network. This persistent interface index number is inserted into the flow records.

Let's view some examples of how you can replicate this when using a network packet broker aggregating traffic from multiple parts of the network.

EXAMPLES

CUSTOMER NETWORK TRAFFIC OPTIONS

Using iFindex

You can use the device (router) iFindex number per collector connection using the interface ID configuration setting up the NetFlow generation on the HyperEngine.

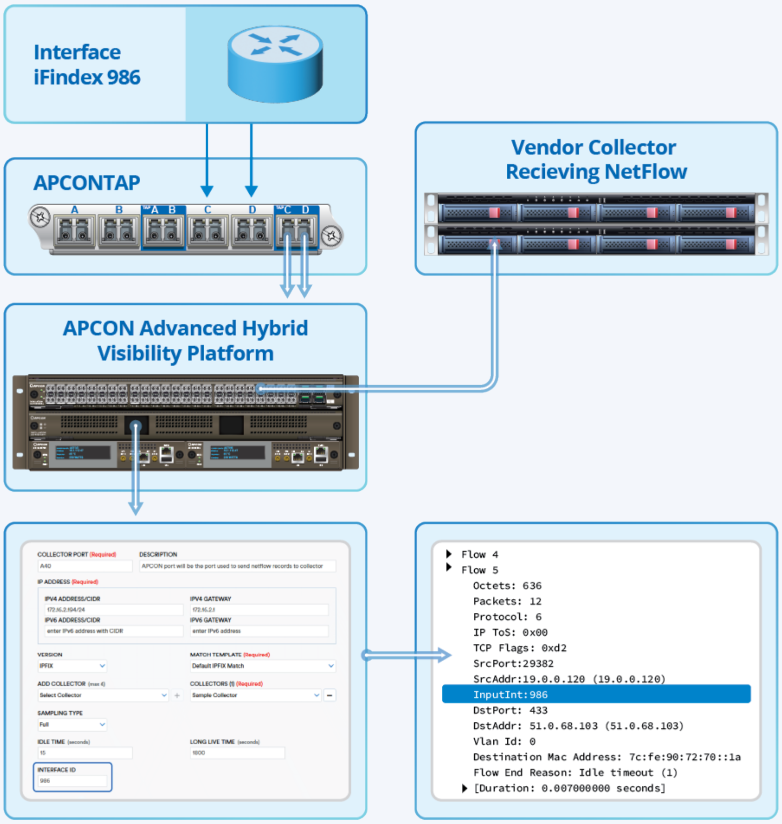
In Figure 2, the traffic is tapped from the router into an APCON aggregation blade. The router iFindex number is 986. You then configure the iFindex number 986 in the Interface ID box found on the HyperEngine NetFlow generation page. Once saved, the traffic will flow to the HyperEngine blade and convert to flows with the flow interface section of the records shown in a trace file. APCON will then send the traffic to a vendor collector where the data can be added to their internal records/reports.

Find Traffic Origination Port

When you want to use the APCON iVif number to represent the iFindex value in flow records, the tools can be configured appropriately to interpret that data.

The network has many direct SPAN links coming into the APCON aggregation blade and APCON is tasked with providing a value to represent them in the NetFlow records. APCON can do this by using the iVif value representing each port. You can then view the value in the flow reports where it will appear as an iFindex number.

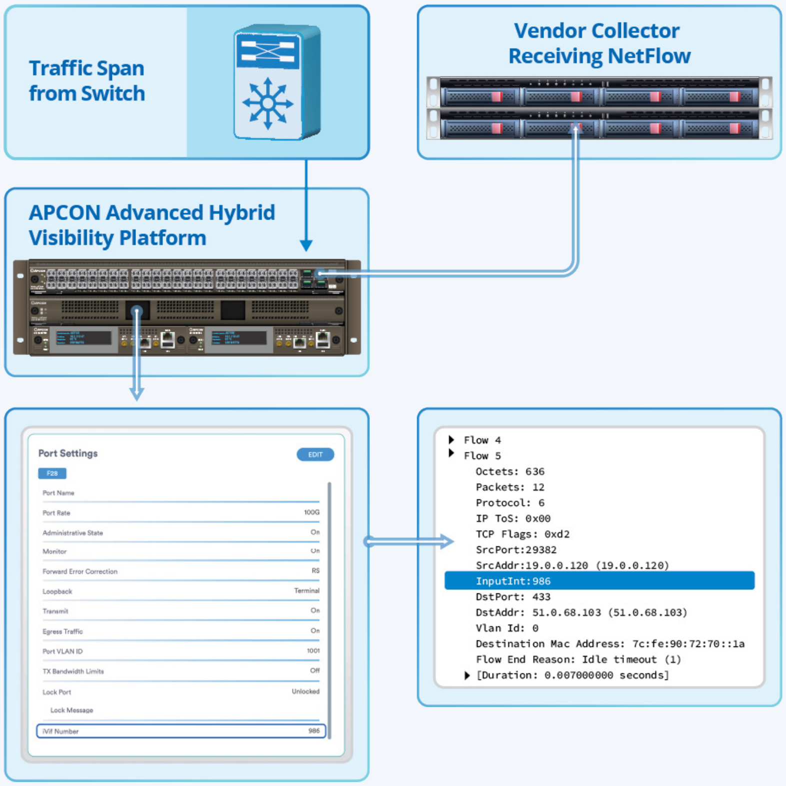
While investigating network or security issues, users can note the iFindex value in their NetFlow report, log in to APCON IntellaView, launch the bulk view page and see which port has the value in the iVif Number section for Port Settings. In this example, the capture trace file shows flow records and reflects the port interface ID shown under InputInt (Figure 3).


Interface iFindex 986
APCONTAP
A
B
A B
C
D
C D
Vendor Collector Recieving NetFlow
APCON Advanced Hybrid Visibility Platform

COLLECTOR PORT (Required): A40
DESCRIPTION: APCON port will be the port used to send netflow records to collector
IP ADDRESS (Required)
IPV4 ADDRESS/CIDR: 172.16.2.194/24
IPV4 GATEWAY: 172.16.2.1
IPV6 ADDRESS/CIDR: enter IPv6 address with CIDR
IPV6 GATEWAY: enter IPv6 address
VERSION: IPFIX
MATCH TEMPLATE (Required): Default IPFIX Match
ADD COLLECTOR (max 4): Select Collector
COLLECTORS (1) (Required): Sample Collector
SAMPLING TYPE: Full
IDLE TIME (seconds): 15
LONG LIVE TIME (seconds): 1800
INTERFACE ID: 986

```
▶ Flow 4
▶ Flow 5
    Octets: 636
    Packets: 12
    Protocol: 6
    IP ToS: 0x00
    TCP Flags: 0xd2
    SrcPort:29382
    SrcAddr:19.0.0.120 (19.0.0.120)
    InputInt:986
    DstPort: 433
    DstAddr: 51.0.68.103 (51.0.68.103)
    Vlan Id: 0
    Destination Mac Address: 7c:fe:90:72:70::1a
    Flow End Reason: Idle timeout (1)
  ▶ [Duration: 0.007000000 seconds]
```

Figure 2 | Traffic tapped to APCON


Traffic Span from Switch
Vendor Collector Receiving NetFlow
APCON Advanced Hybrid Visibility Platform

Port Settings
EDIT
F28

Port Name	
Port Rate	100G
Administrative State	On
Monitor	On
Forward Error Correction	RS
Loopback	Terminal
Transmit	On
Egress Traffic	On
Port VLAN ID	1001
TX Bandwidth Limits	Off
Lock Port	Unlocked
Lock Message	
iVif Number	986

```
▶ Flow 4
▶ Flow 5
    Octets: 636
    Packets: 12
    Protocol: 6
    IP ToS: 0x00
    TCP Flags: 0xd2
    SrcPort:29382
    SrcAddr:19.0.0.120 (19.0.0.120)
    InputInt:986
    DstPort: 433
    DstAddr: 51.0.68.103 (51.0.68.103)
    Vlan Id: 0
    Destination Mac Address: 7c:fe:90:72:70::1a
    Flow End Reason: Idle timeout (1)
  ▶ [Duration: 0.007000000 seconds]
```

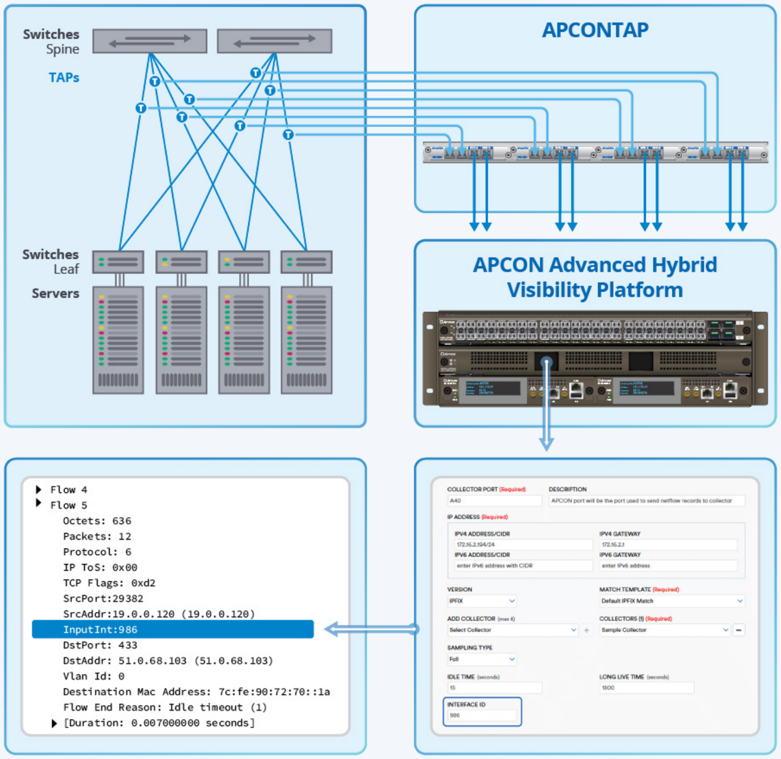
Figure 3 | APCON receives SPAN traffic aggregated to a blade where the port's iVif ID will be used.

Multiple Ports, Single Connection

When you want to aggregate multiple ports into a single connection so that they all have a single interface number using an APCON interface ID, our blades can do the job.

There can be many tapped interfaces on one switch linked to one interface ID represented as a group. In this case, since many of the interfaces are tapped in a leaf-spine design, you may want those interfaces represented as one interface ID on the APCON switch. Those who analyze NetFlow records in reports may find it easier to use one interface ID since having many interfaces to recall in a very large design will be problematic. If there is an issue with a specific switch, technicians can log in and investigate. Figure 4 shows an example of tapped interfaces coming into an APCON aggregation blade, the traffic then will pass through the IntellaView HyperEngine blade, and the interface ID will be inserted and shown in the trace file on the right.

When it comes to converting packets to flows, APCON provides innovative and refined ways to manage the delivery of NetFlow traffic to various tools. Whether you are monitoring or analyzing network, security, or application issues with flows, IntellaView acquires, converts, and delivers the flows to your collectors.



```
▸ Flow 4
▸ Flow 5
    Octets: 636
    Packets: 12
    Protocol: 6
    IP ToS: 0x00
    TCP Flags: 0xd2
    SrcPort:29382
    SrcAddr:19.0.0.120 (19.0.0.120)
    InputInt:986
    DstPort: 433
    DstAddr: 51.0.68.103 (51.0.68.103)
    Vlan Id: 0
    Destination Mac Address: 7c:fe:90:72:70::1a
    Flow End Reason: Idle timeout (1)
  ▸ [Duration: 0.007000000 seconds]
```

COLLECTOR PORT (Required): A40
DESCRIPTION: APCON port will be the port used to send netflow records to collector
IP ADDRESS (Required)
IPV4 ADDRESS/CIDR: 172.16.2.194/24
IPV4 GATEWAY: 172.16.2.1
IPV6 ADDRESS/CIDR: enter IPv6 address with CIDR
IPV6 GATEWAY: enter IPv6 address
VERSION: IPFIX
MATCH TEMPLATE (Required): Default IPFIX Match
ADD COLLECTOR (max 4): Select Collector +
COLLECTORS (1) (Required): Sample Collector −
SAMPLING TYPE: Full
IDLE TIME (seconds): 15
LONG LIVE TIME (seconds): 1800
INTERFACE ID: 986

Figure 4 | Configure Interface ID, then all interfaces will use the new interface ID number in flow records.

APCON SOLUTIONS

APCON leverages its proprietary IP and deep expertise to provide flexible, focused solutions across

- Government
- Healthcare
- Higher Education
- Financial Services
- Manufacturing
- Telecommunications

APCON solutions provide the flexibility and means to gain visibility to data more efficiently, resulting in savings across the board, including time, resources, and maintenance.

SERVICE AND SUPPORT

APCON's professional services team of certified engineers has years of experience optimizing network visibility strategies for businesses across the globe. In addition to providing installation assistance of existing analysis tools, this team proudly provides around-the-clock troubleshooting services and support.

ABOUT APCON

Since 1993, APCON has consistently delivered technology designed with unparalleled innovation, stability, and scalability to mid-sized and Fortune 1000 customers in over 40 countries.

Our products instill network and security professionals with the confidence that data is monitored, secured, and protected in both physical and virtual environments. APCON helps companies sustain maximum performance by empowering total network visibility.

APCON
Solutions for Networks

APCON, Inc. ▪ 9255 SW Pioneer Court, Wilsonville, Oregon 97070
+1 503–682–4050 ▪ 1–800–624–6808 ▪ @APCON ▪ company/APCON ▪ **apcon.com**