IAS | INSTITUTE FOR ADVANCED STUDY

NetFlow: Troubleshooting Network & Security Problems with Flows

Presented by Christina Klam at NJEDge Conference 2016. 2016-11-18

NetFlow

- Developed and patented at Cisco® Systems in 1996
- NetFlow is now the primary network accounting technology in the industry
- Answers questions regarding IP traffic: who, what, where, when, and how
- Provides a detailed view of network behavior
- Insight into the network without minimizing the need for DPI (Deep Packet Inspection)

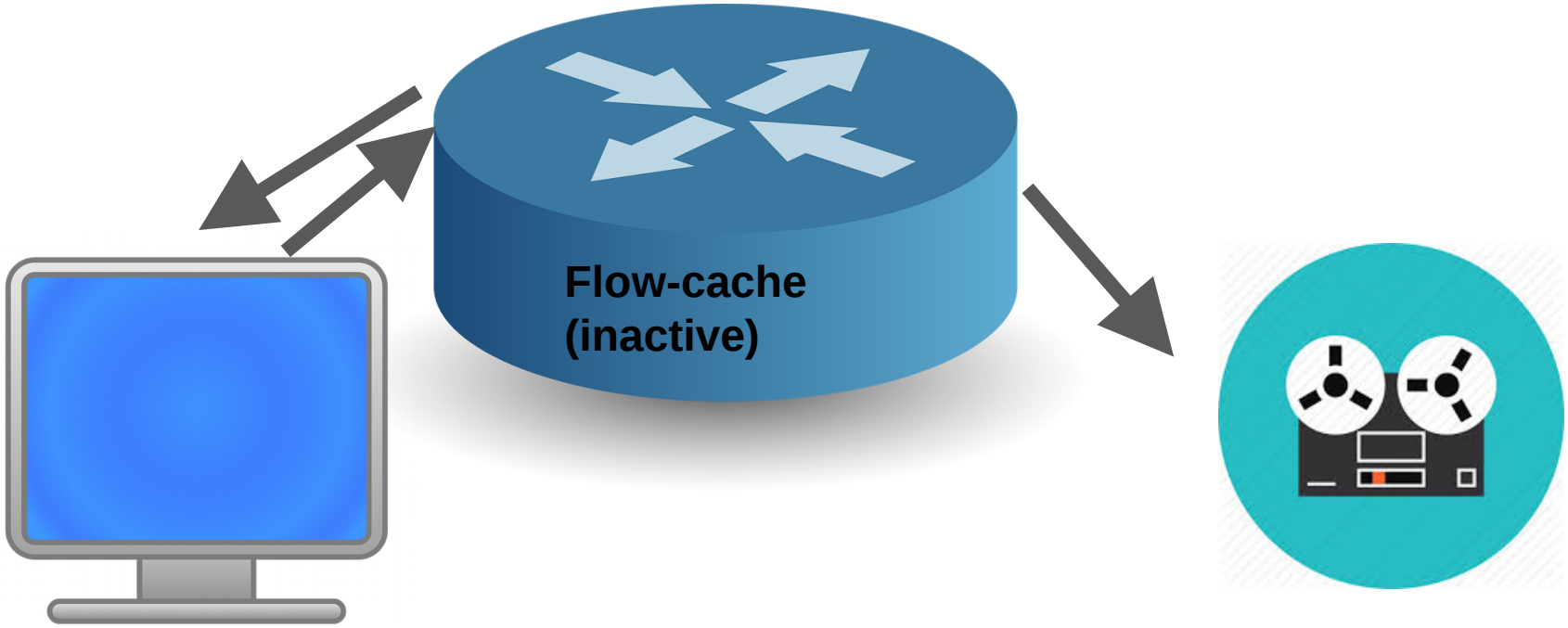
NetFlow

De-facto term although flow data comes in other forms:

- Juniper® (Jflow)
- 3Com/HP® , Dell® , and Netgear® (s-flow)
- Huawei® (NetStream)
- Alcatel-Lucent® (Cflow)
- Ericsson® (Rflow)

IAS | INSTITUTE FOR ADVANCED STUDY

Flow Record Creation



IAS | INSTITUTE FOR ADVANCED STUDY

Flow Record Creation

If only INACTIVE flows are sent

AND

Active Flow-cache default timeout = 30 min

Does this mean you have to wait 30 minutes to see traffic from an active connection???

IAS | INSTITUTE FOR ADVANCED STUDY

Flow Record Creation

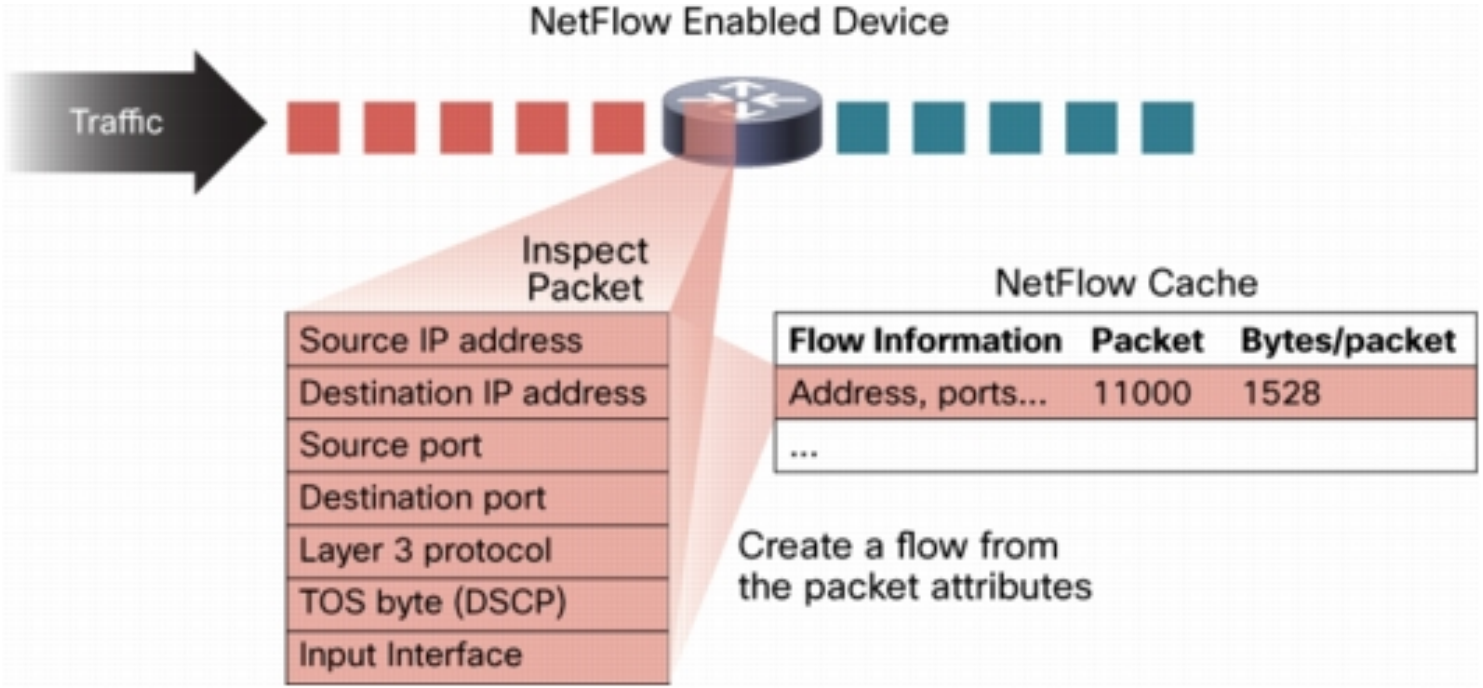
Change the timeout value to 1 minute (v5) or 1 second (v9+)

ip flow-cache timeout active 1

***** If this is a busy router, change it to something less frequent.

NetFlow Version	Comments
1	Original
5	Standard and most common
7	Specific to Cisco Catalyst 6500 and 7600 Series Switches Similar to Version 5, but does not include AS, interface, TCP Flag & TOS information
8	Choice of eleven aggregation schemes Reduces resource usage
9	Flexible, extensible file export format to enable easier support of additional fields & technologies; coming out now MPLS, Multicast, & BGP Next Hop

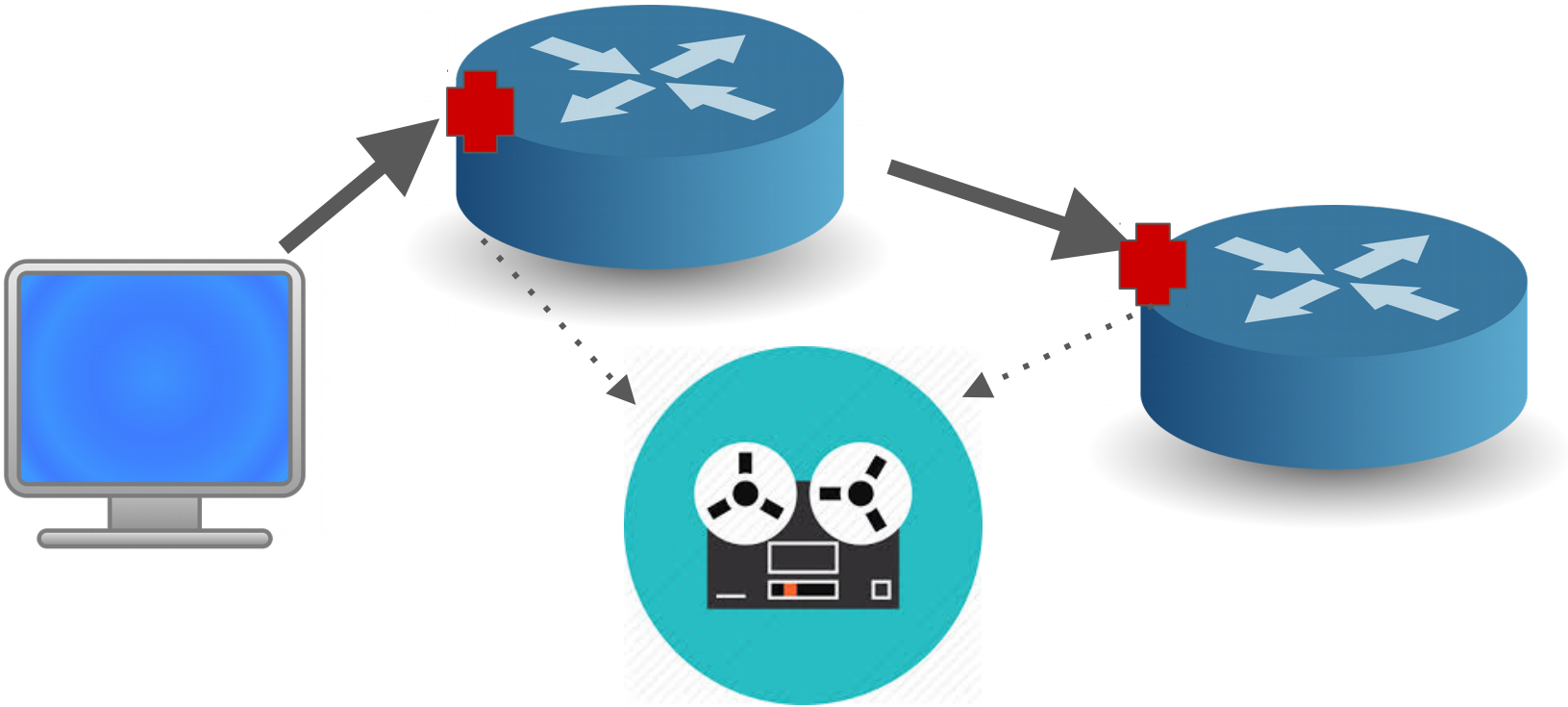
Version 5



Static set of fields or tuples

IAS | INSTITUTE FOR ADVANCED STUDY

Version 5: Ingress Only



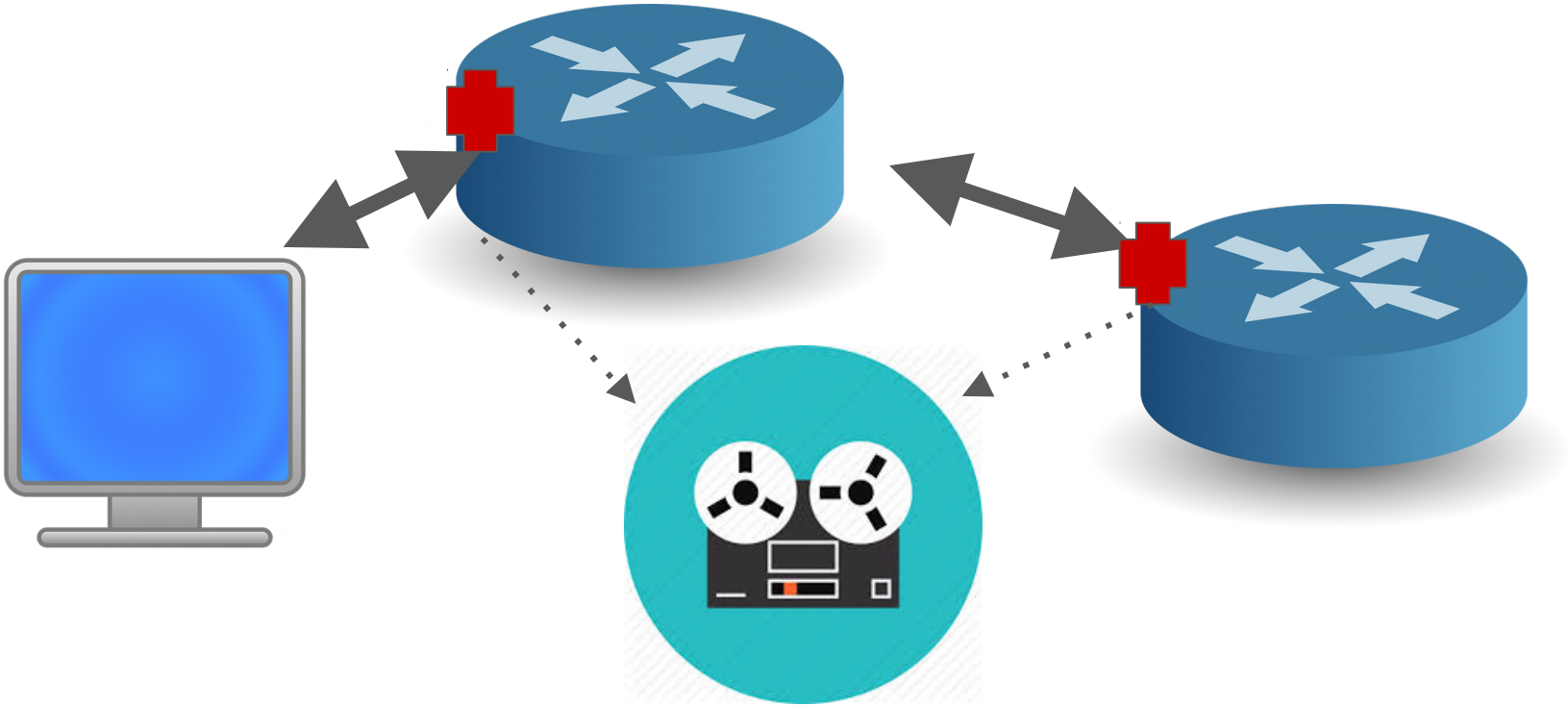
Version 9

- Version 5 fields + ...
- Up to a total of 128 fields
  - Type of service (ToS)
  - Packet and byte counts
  - Start and end timestamps
  - Layer 2: VLANs, mac addresses
  - Application
  - Routing information (MPLS, next-hop address, source autonomous system (AS) number, destination AS number, source prefix mask, destination prefix mask)

Dynamic set of fields

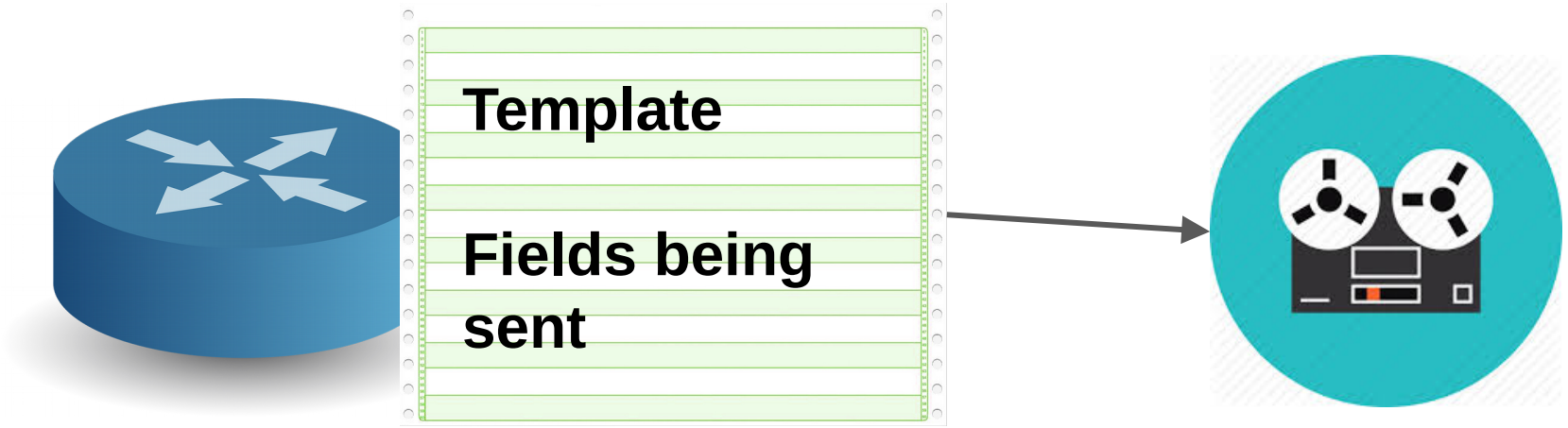
IAS | INSTITUTE FOR ADVANCED STUDY

Version 9: Ingress & Egress



IAS | INSTITUTE FOR ADVANCED STUDY

Version 9



Dynamic set of fields

f-r1-4500x-vss#sh flow exporter templates
Flow Exporter Scrutinizer:
  Client: Flow Monitor IPV4-FLOW
  Exporter Format: IPFIX (Version 10)
  Template ID   : 256
  Source ID   : 22
  Record Size   : 38
  Template layout

Field	ID	Ent.ID	Offset	Size
ipv4 source address	8		0	4
ipv4 destination address	12		4	4
transport source-port	7		8	2
transport destination-port	11		10	2
ip tos	5		12	1
ip protocol	4		13	1
interface input snmp	10		14	4
interface output snmp	14		18	4
counter bytes long	1		22	8
counter packets long	2		30	8

Client: Option options application-name
  Exporter Format: NetFlow Version 9
  Template ID   : 258
  Source ID   : 22
  Record Size   : 87
  Template layout

Field	Type	Offset	Size
v9-scope system	1	0	4
application id	95	4	4
application name	96	8	24
application description	94	32	55

IPFIX: Vendor Templates

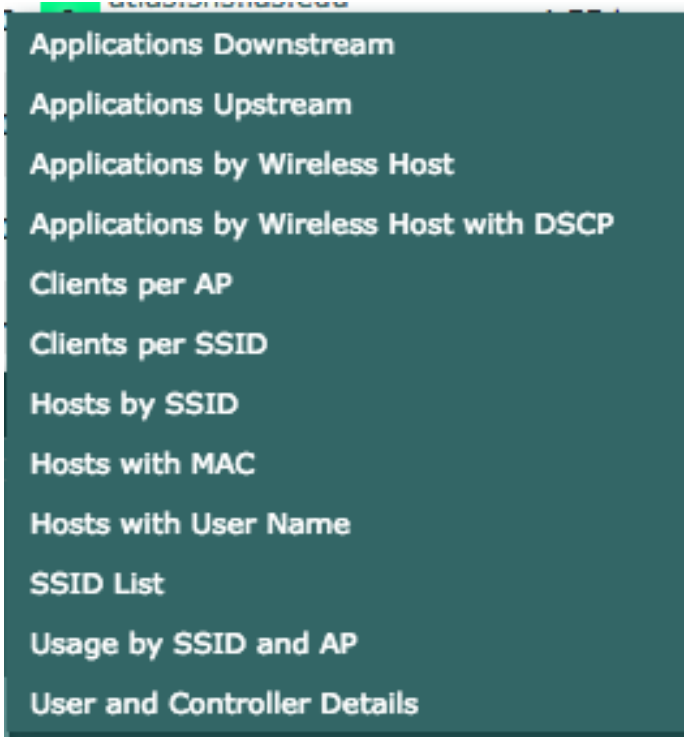
- **Not flow technology.**
- **IANA standard for both sflow and netflow flow technology.**
- Allows for variable length fields that can be used for URLs, messages, etc.
- Like with flexible v9, the templates allows for specifying just the information you need.
  - Templates are sent by router every 20 packets
  - Templates explains the info being sent

If Netflow and SNMP had a baby

- Push technology like snmptrap and syslog
- Allows for unique elements across vendors.
- Each vendor has an unique enterprise number -- usually same used in SNMP.
- Like SNMP MIBS without the need for compiling and uses less bandwidth.

IPFIX

IPFIX Templates: AVC & NBAR



	Application
1	ssl (Type: 13 ID: 453)
2	youtube (Type: 13 ID: 82)
3	video-over-http (Type: 13 ID:...
4	binary-over-http (Type: 13 ID...
5	secure-http (Type: 3 ID: 443)
6	internet-video-streaming (Typ...
7	http (Type: 3 ID: 80)
8	dns (Type: 3 ID: 53)
9	unknown (Type: 13 ID: 1)
10	rtsp (Type: 3 ID: 554)

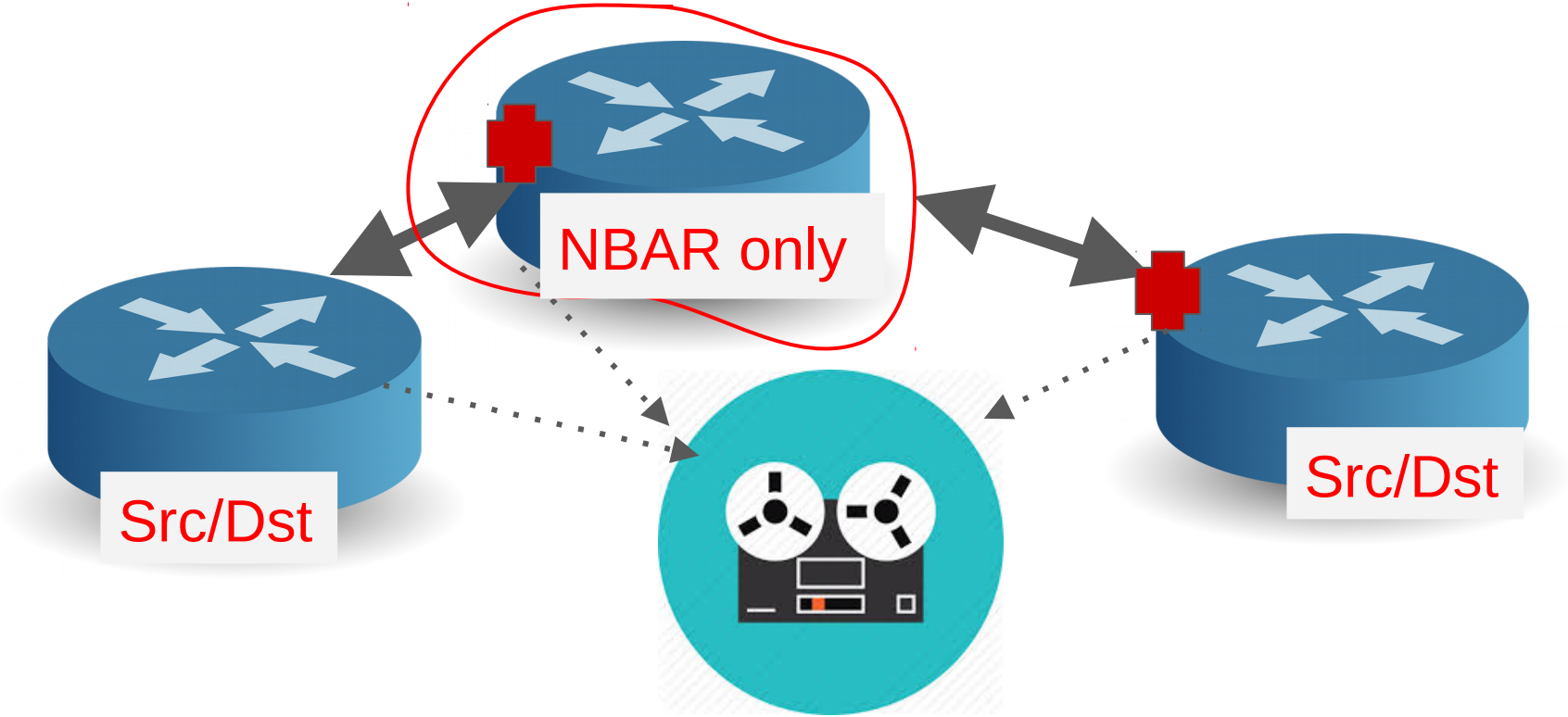
Resource Impact

- As most vendors are moving v9 & IPFIX to silicon, there is a much smaler hit to the CPU.
  - For vendors who do the flow via software, they may be sticking with sFlow

- Exporting NBAR instead of source and destination can reduce the number of flows as well. With NBAR alone, you lose the source and destination if the flow is not also coming from somewhere else.

IAS | INSTITUTE FOR ADVANCED STUDY

NBAR only Topology



IAS | INSTITUTE FOR ADVANCED STUDY

3 Ingredients for Configuration

Record

Export

Monitor

IAS | INSTITUTE FOR ADVANCED STUDY

Flow Record: Layer3+

match ipv4 source address
match ipv4 destination address
match ip protocol
match ip tos
match transport source-port
match transport destination-port
match interface input
match interface output
match flow direction
collect routing source as
collect routing destination as
collect routing next-hop address ipv4
collect transport tcp flags
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last

Flow Record: Layer 2

- Source and destination MAC addresses
- Source VLAN ID
- EtherType from the Ethernet frame

Apply to INGRESS interfaces:

1. Switch ports in access mode
2. Switch ports in trunk mode
3. Layer 2 port channels

Cannot be applied to VLANs, egress interfaces, or Layer 3 interfaces such as VLAN interfaces.

Flow Export

- Netflow Version {5,9,IPFIX}
- IP of the collector
- Protocol (UDP or SCTP)
- Port Number
- Source interface
- DSCP

Flow Export

Cisco and others tend to use UDP: NetFlow is UDP port 2055, but other ports like 9555 or 9995, 9025, and 9026 can also be used. UDP port 4739 is the default port used by IPFIX.

SCTP

IPFIX prefers Stream Control Transmission Protocol (SCTP) as its transport protocol.

SCTP vs TCP vs UDP

Services/Features	SCTP	TCP	UDP
Connection-oriented	yes	yes	no
Full duplex	yes	yes	yes
Reliable data transfer	yes	yes	no
Partial-reliable data transfer	optional	no	no
Ordered data delivery	yes	yes	no
Unordered data delivery	yes	no	yes
Flow control	yes	yes	no
Congestion control	yes	yes	no
ECN capable	yes	yes	no
Selective ACKs	yes	optional	no
Preservation of message boundaries	yes	no	yes
Path MTU discovery	yes	yes	no
Application PDU fragmentation	yes	yes	no
Application PDU bundling	yes	yes	no
Multistreaming	yes	no	no
Multihoming	yes	no	no
Protection against SYN flooding attacks	yes	no	n/a
Allows half-closed connections	no	yes	n/a
Reachability check	yes	yes	no
Psuedo-header for checksum	no (uses vtags)	yes	yes
Time wait state	for vtags	for 4-tuple	n/a

IAS | INSTITUTE FOR ADVANCED STUDY

SCTP is a transport level protocol. "...[i]t is message-oriented like UDP and ensures reliable, in-sequence transport of messages with congestion control like TCP; it differs from these in providing multi-homing and redundant paths to increase resilience and reliability."

Flow Monitor

Flow Monitor

Examples of some Neflow **collectors**

- Plixar Scrutinizer
- NFSEN
- NTOP
- Cisco Stealthwatch
- CFLOW
- PRTG
- Arbor Peakflow

IAS | INSTITUTE FOR ADVANCED STUDY

Flow Monitor

Criteria for selecting a netflow **collectors**

- Can it read the v9/ipfix templates?
- Can it read NBAR?
- Cost
- Ease of searching and reporting

IAS | INSTITUTE FOR ADVANCED STUDY

Apply it to an interface

IF YOU WALK ON SNOW YOU CANNOT HIDE YOUR FOOTPRINTS

GEORGE HERBERT

PICTUREQUOTES.com

IAS | INSTITUTE FOR ADVANCED STUDY

Netflow Give OSI Layer Visibility

Layer 1: Interface and Traffic flow by bit/bytes/packets

Layer 2: MAC Address

Layer 3: Source & Destination IP

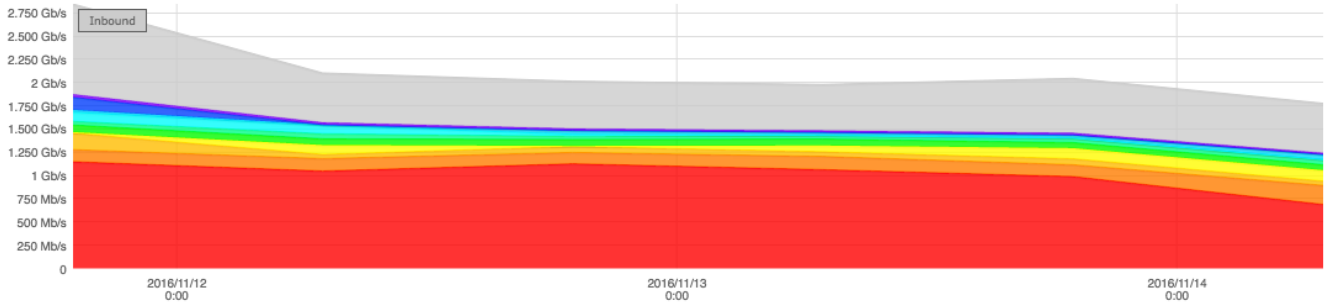
Layer 4 & 5: Protocol (TCP, UDP, ICMP) & Port Number

Layer 6 & 7: NBAR/Application/URLs

Netflow: Top Destinations

IAS | INSTITUTE FOR ADVANCED STUDY

Source » Hosts From **2016-11-11 7:00** to **2016-11-14 7:00** in auto (12h) intervals



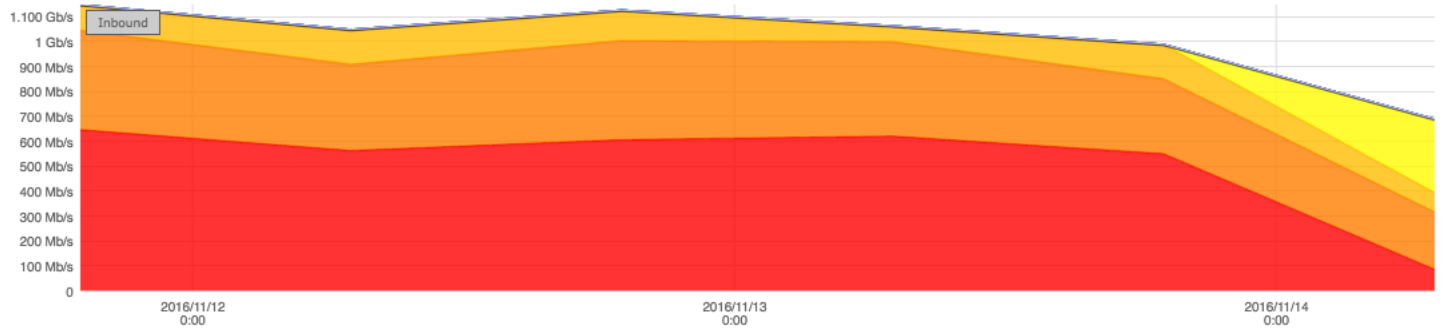
Inbound Results

	Source	Percent	Bits
1	cistern.vmnfs.itg.ias.edu	47.55 %	1.012 Gb/s
2	fas-svm2.vmnfs.sns.ias.edu	6.73 %	143.260 Mb/s
3	fas-svm1.ias.edu	3.49 %	74.318 Mb/s
4	oceanvhb.vmnfs.itg.ias.edu	3.24 %	68.911 Mb/s
5	wlc1.net.ias.edu	3.18 %	67.714 Mb/s
6	fas-svm2.ias.edu	2.10 %	44.637 Mb/s
7	vs1.vmft.sns.ias.edu	1.60 %	34.096 Mb/s
8	fas-svm2.sv.sns.ias.edu	1.56 %	33.226 Mb/s
9	fas-node1-rep.sv.sns.ias.edu	1.07 %	22.747 Mb/s
10	130.156.252.210	1.05 %	22.428 Mb/s
Other			604.805 Mb/s
Total*			2.128 Gb/s

Netflow: What is cistern doing?

IAS INSTITUTE FOR ADVANCED STUDY

Top » Applications Defined From **2016-11-11 7:00** to **2016-11-14 7:00** in auto (12h) intervals ?



Inbound Results

	Application	Percent	Bits
1	compaq-evm (619 - TCP)	50.68 %	512.744 Mb/s
2	fcp-udp (810 - TCP)	33.85 %	342.475 Mb/s
3	nfs (2049 - TCP)	10.61 %	107.305 Mb/s
4	mcns-sec (638 - TCP)	4.85 %	49.066 Mb/s
5	maitrd (997 - TCP)	0.00 %	29.464 kb/s
6	rushd (696 - TCP)	0.00 %	21.651 kb/s
7	ris-cm (748 - TCP)	0.00 %	18.513 kb/s
8	cadlock (770 - TCP)	0.00 %	9.919 kb/s
9	entrust-kmsh (709 - TCP)	0.00 %	8.771 kb/s
10	flexlm (744 - TCP)	0.00 %	8.615 kb/s
Other			233.294 b/s
Total*			1.012 Gb/s

Reporting


BYOD
BRING YOUR OWN DEVICE


amazonmusic

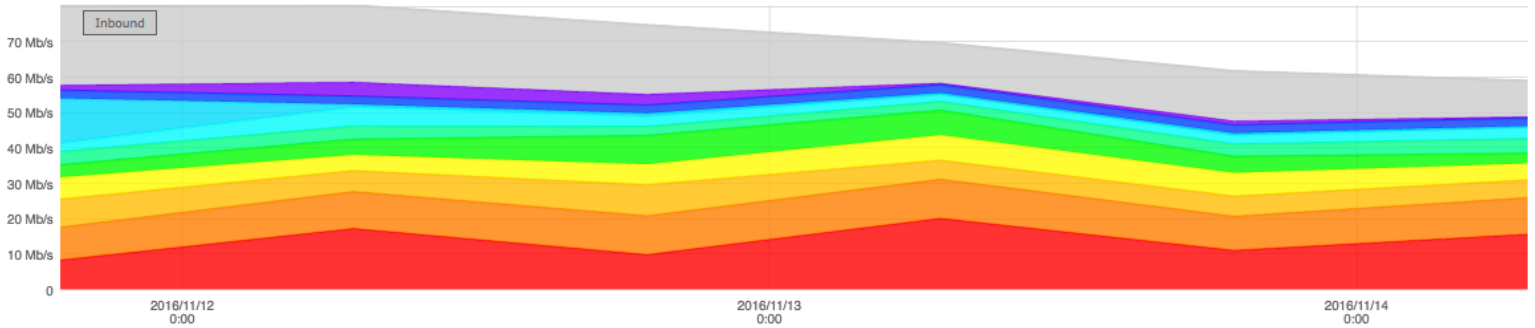

AWS


skype™


amazon
instant video

Netflow: Top Applications

IAS | INSTITUTE FOR ADVANCED STUDY

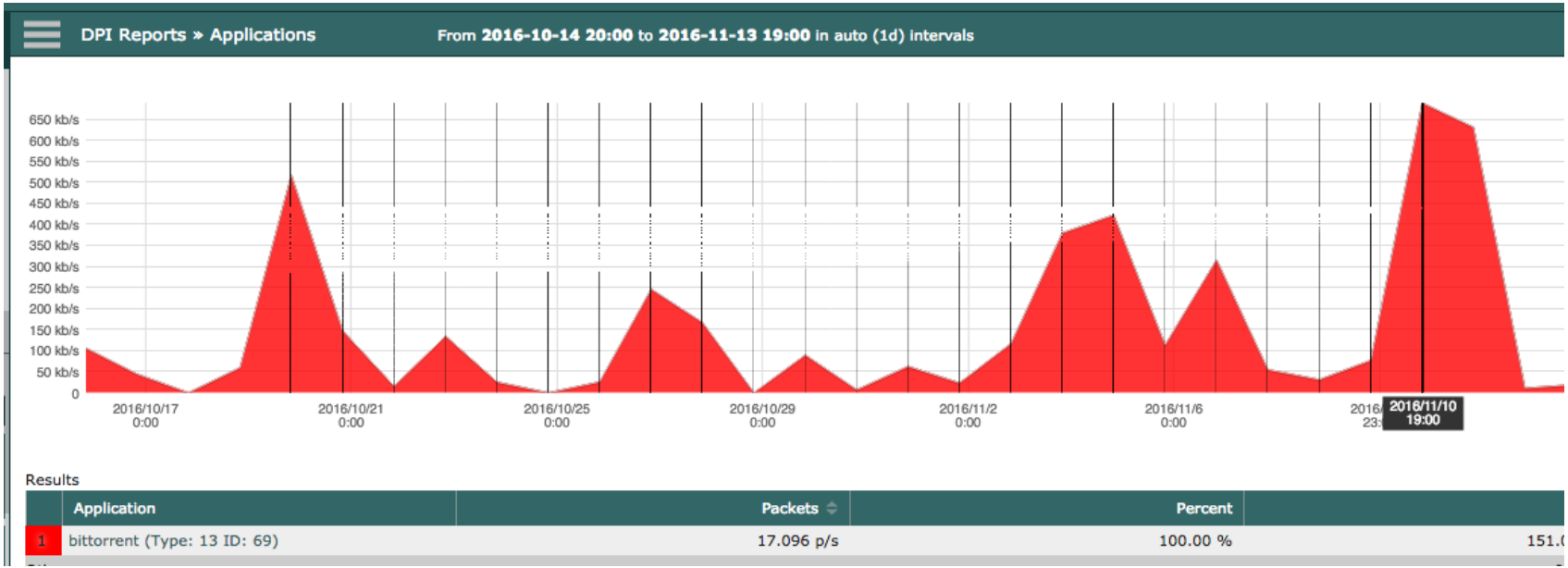


Results

	Application	Packets	Percent	Bits
1	ssl (Type: 13 ID: 453)	1.863 kp/s	19.36 %	13.763 Mb/s
2	youtube (Type: 13 ID: 82)	1.053 kp/s	14.51 %	10.315 Mb/s
3	video-over-http (Type: 13 ID: 432)	734.980 p/s	9.14 %	6.495 Mb/s
4	binary-over-http (Type: 13 ID: 431)	611.090 p/s	7.99 %	5.682 Mb/s
5	internet-video-streaming (Type: 13 ID: 574)	589.179 p/s	7.29 %	5.185 Mb/s
6	secure-http (Type: 3 ID: 443)	380.841 p/s	4.71 %	3.346 Mb/s
7	http (Type: 3 ID: 80)	402.197 p/s	4.38 %	3.116 Mb/s
8	dropbox (Type: 3 ID: 17500)	322.881 p/s	3.50 %	2.486 Mb/s
9	rtsp (Type: 3 ID: 554)	374.105 p/s	3.30 %	2.343 Mb/s
10	dns (Type: 3 ID: 53)	252.387 p/s	2.44 %	1.734 Mb/s

Netflow: Patterns

IAS | INSTITUTE FOR ADVANCED STUDY

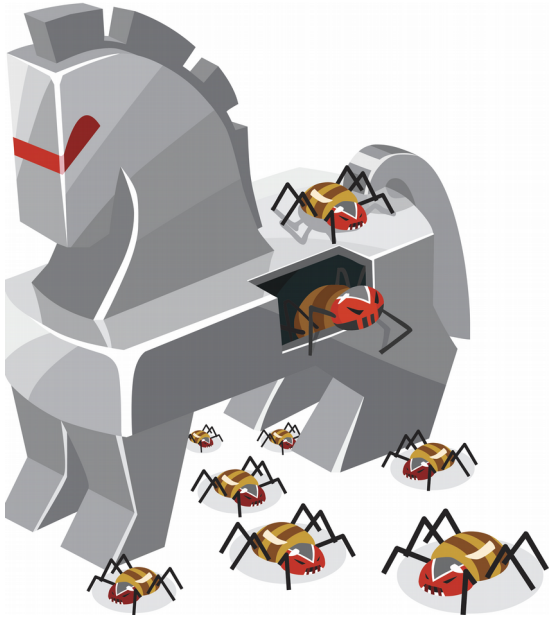


Voice and Video Traffic Monitoring and Reporting

Rich media traffic monitoring must go beyond traditional usage metrics. Excessive jitter or packet loss are often telltale signs of a voice and video issue, but where on the network was the problem introduced? Where did the DSCP value change and why wasn't the traffic prioritized correctly? Voice and video traffic monitoring often needs to be done campus-wide and, ideally, when quality of service slips, thresholds are breached, notifications are triggered, and if configured, traffic is rerouted. Does your company have the solution to investigate and accurately report on all of this recorded information on an end-to-end or hop-by-hop basis?

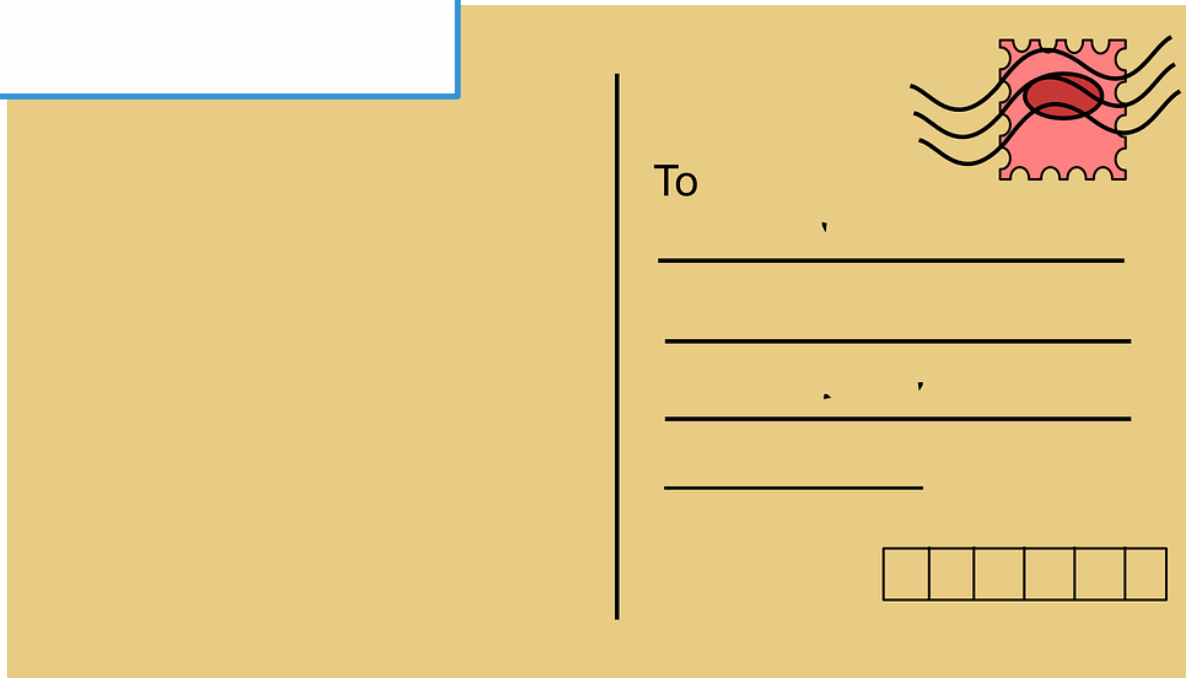
IAS | INSTITUTE FOR ADVANCED STUDY

Netflow Security



IAS | INSTITUTE FOR ADVANCED STUDY

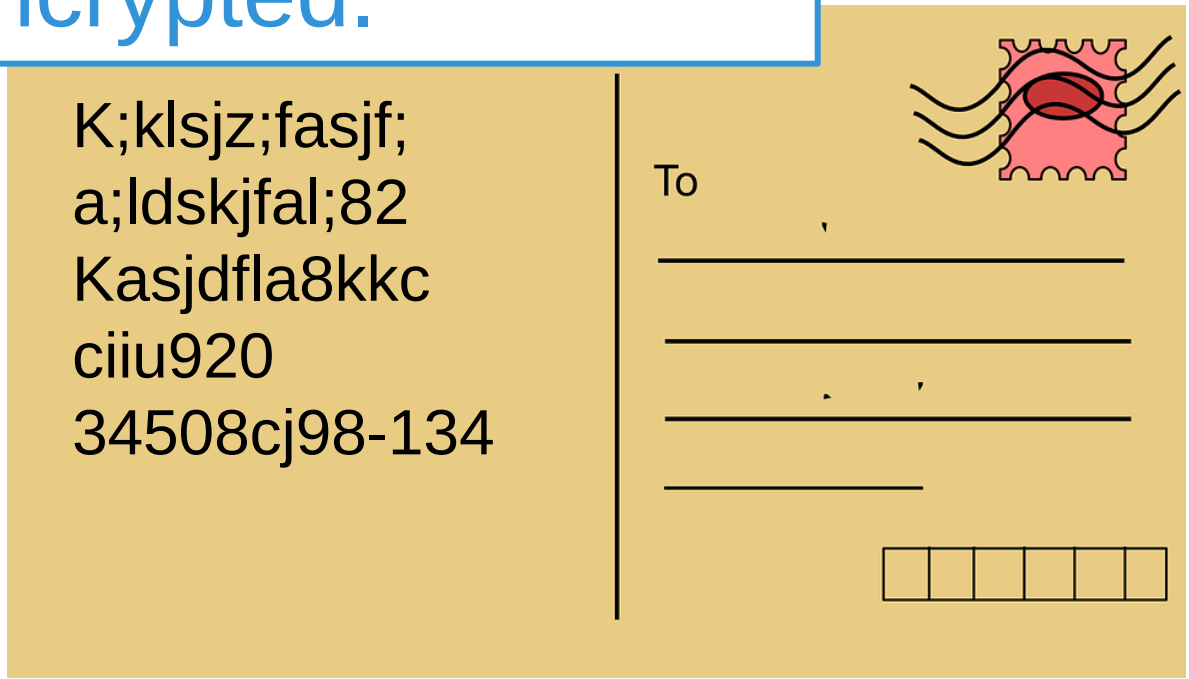
NetFlow cannot see **payloads**



IAS | INSTITUTE FOR ADVANCED STUDY

Neither will you DPI if the packet is encrypted.

Keeping netflows requires far less storage that your IDS.



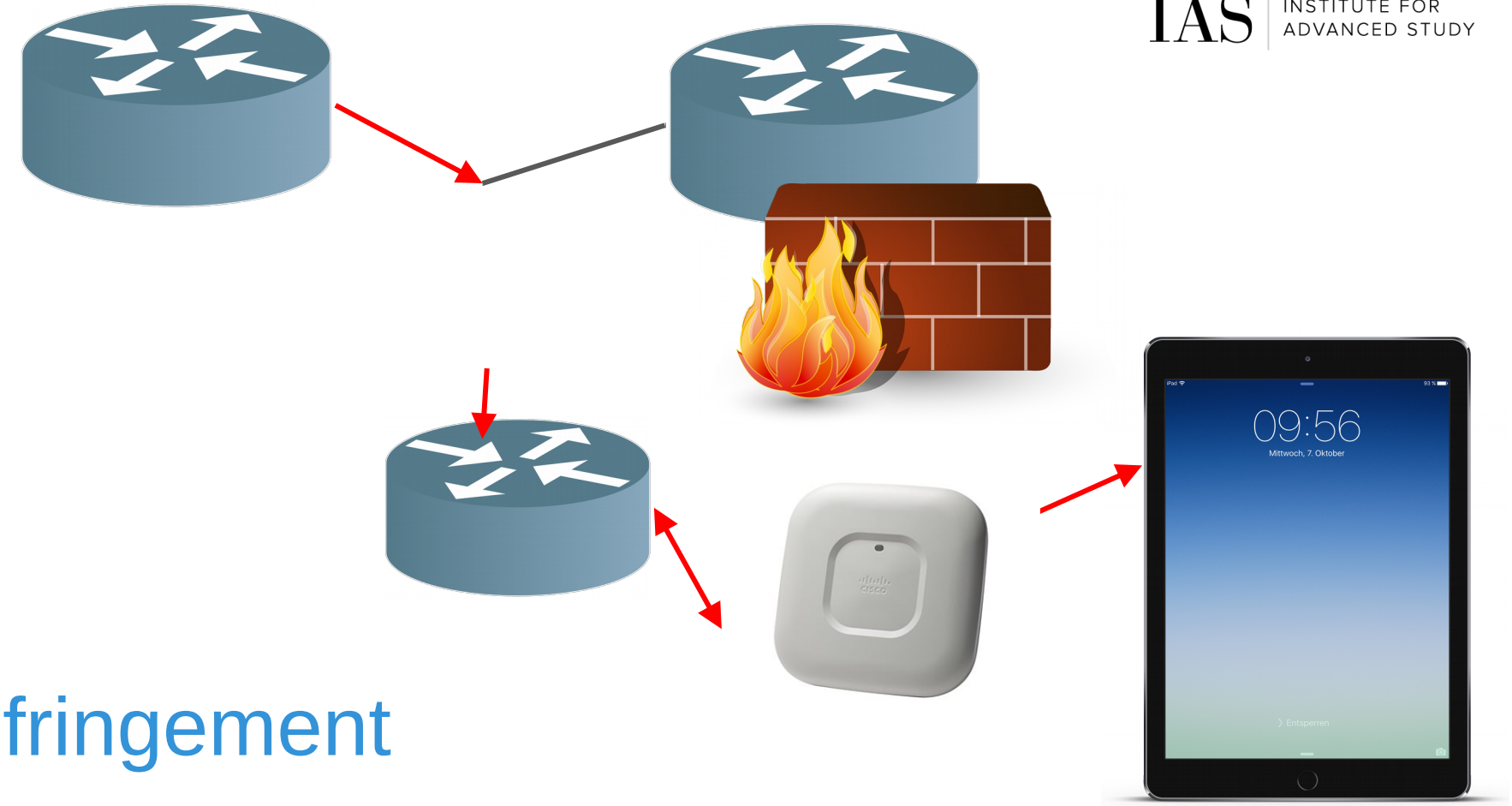
Compliance

- Recognize unauthorized host access
- Detect malicious and suspicious network activity
- Leverage third-party integrations for threat mitigation to remediate security policy violations
- **HIPPA, RIAA**
- Continuously monitor hosts and network activity to identify intrusions
- Conduct forensic analysis for security incidents: Who, what, when, how long

---------- Infringement Details ----------
Title: Last Week Tonight with John Oliver
Timestamp: 2016-11-07T23:07:29Z
IP Address: 192.16.204.250
Port: 23945
Type: BitTorrent
Torrent Hash: 2b9b91ca32f082e3f7d6c7af60e8a51d0eb9a465
Filename:
Last.Week.Tonight.With.John.Oliver.S03E29.HDTV.x264-BATV[ettv]
Filesize: 309 MB
- ----------

Diagnosing Compliance: RIAA

IAS | INSTITUTE FOR ADVANCED STUDY



Infringement

Compliance

- Recognize unauthorized host access
- Detect malicious and suspicious network activity
- Leverage third-party integrations for threat mitigation to remediate security policy violations
- HIPPA, RIAA
- Continuously monitor hosts and network activity to identify intrusions
- **Conduct forensic analysis for security incidents: Who, what, when, how long**

Diagnosing Vectors of Infection

IAS | INSTITUTE FOR ADVANCED STUDY

What is the malware doing?

Diagnosing Vectors of Infection

IAS | INSTITUTE FOR ADVANCED STUDY

What is the malware doing?

Who else has it?

Diagnosing Vectors of Infection

IAS | INSTITUTE FOR ADVANCED STUDY

What is the malware doing?

Who else has it?

How long has it been active on the network?

Diagnosing Vectors of Infection

IAS | INSTITUTE FOR ADVANCED STUDY

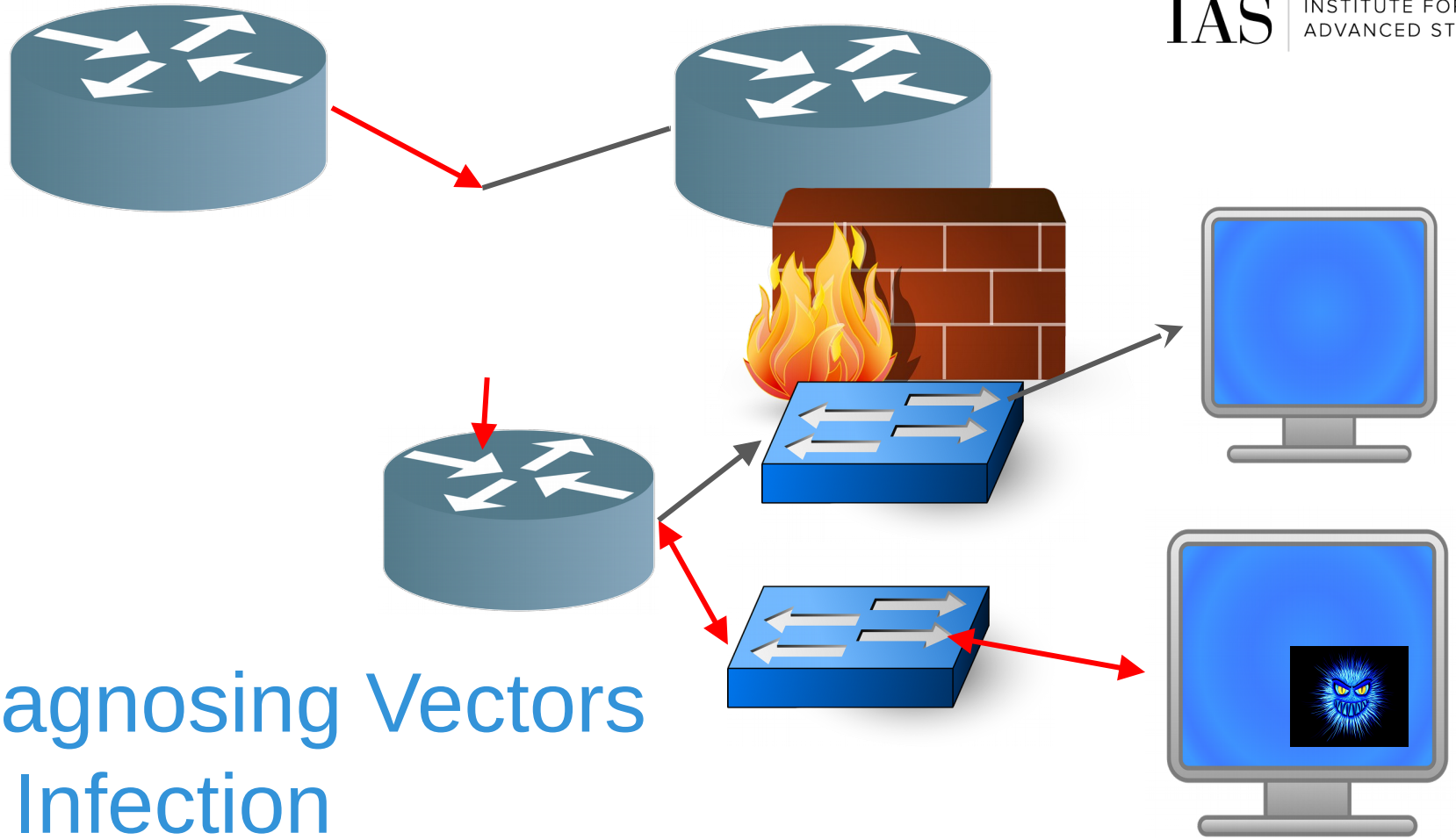
What is the malware doing?

Who else has it?

How long has it been active on the network?

What is the malware pattern?

IAS | INSTITUTE FOR ADVANCED STUDY



Diagnosing Vectors of Infection

IAS | INSTITUTE FOR ADVANCED STUDY

Questions?

How is netflow being used at your institution?

Presented by Christina Klam at NJEDge Conference 2016. 2016-11-18

IAS | INSTITUTE FOR ADVANCED STUDY

NetFlow: Troubleshooting Network & Security Problems with Flows

Presented by Christina Klam at NJEDge Conference 2016. 2016-11-18