Homework 2
Network Flow Analysis

Slides Credit: 14740 and 14825

What is a Flow?

- A unidirectional stream of packets between a source and destination
- 7 fields
  - Source IP address
  - Destination IP address
  - Layer 3 protocol type
  - Type of Service
  - Source port number
  - Destination port number
  - Input logical interface

Flow Record

- A data structure describing the flow
- Includes byte and packet counts per flow
- Also TCP flags, timestamps of first/last packets, etc

Unidirectional Vs. Bidirectional Flow

Unidirectional Flow

sTime	Proto	SrcAddr Sport	Dstaddr Dport	Pkts	Byte	State
13:50:01.9744	tcp	192.168.141.128.34430	192.168.141.129.80	6	524	SPAF-
13:50:02.2037	tcp	192.168.141.129.80	192.168.141.128.34430	5	686	S-AF-

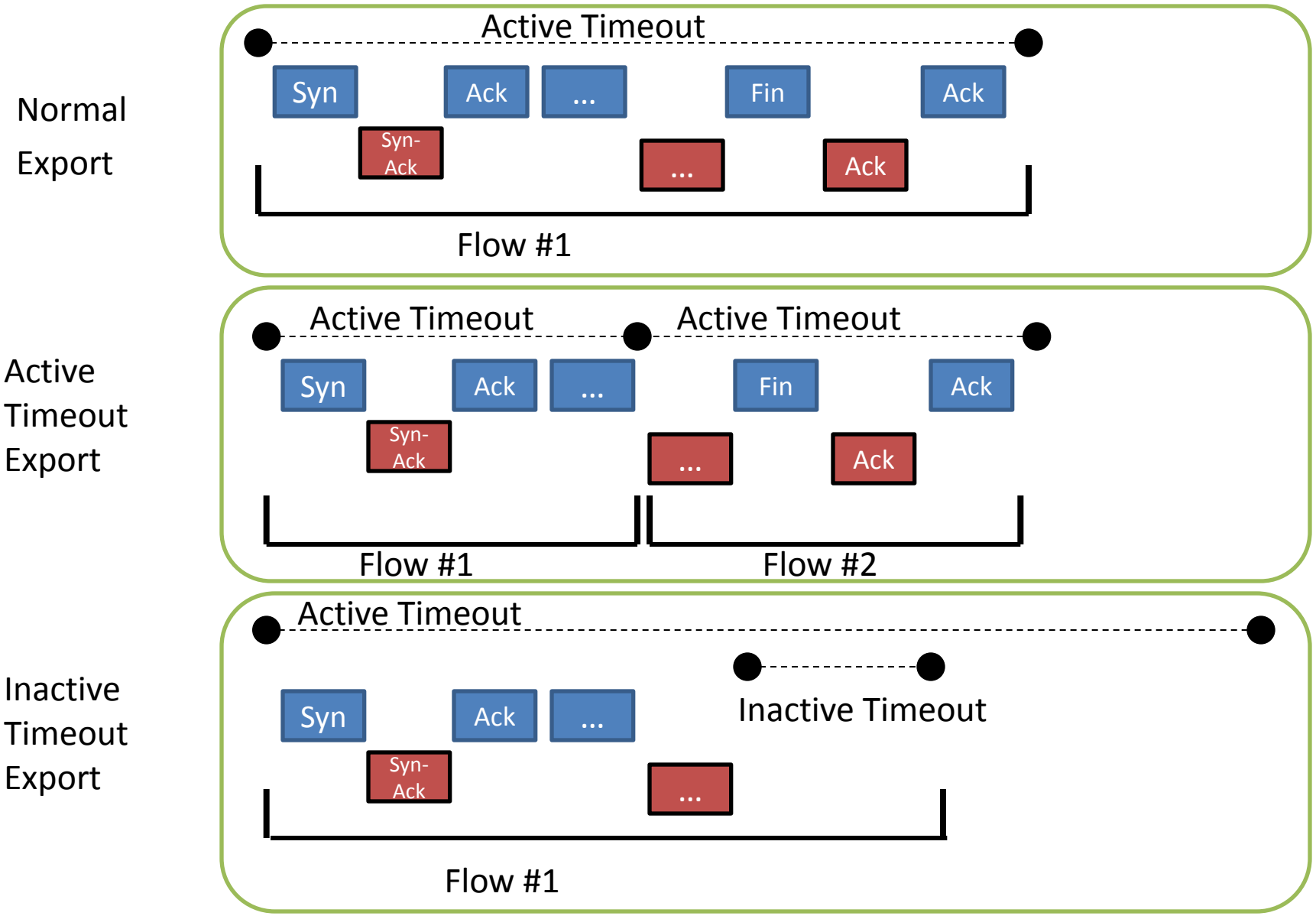
Bidirectional Flow

sTime	Proto	SrcAddr Sport	Dir	DstAddr Dport	Srcpkts	Dstpkts	Srcbytes	Dstbytes	State
13:50:01.9744	tcp	192.168.141.128.34430	->	192.168.141.129.80	6	5	524	686	SPAF_SAF

Flow Generation

- A new flow is initiated on first instance of the 5-tuple:
  - Protocol
  - Source and destination IP
  - Source and destination Port
- Flows are terminated (exported) upon
  - TCP: Fin or RST packet
  - Active timeout
  - Inactive timeout

Flow Generation



Argus

- A bidirectional flow meter and associated analysis tools
- Originally developed in 1993 at CERT

http://www.qosient.com/argus

ra

NAME

```
ra – read argus (8) data.
```

SYNOPSIS

```
ra [raoptions] [- filter-expression]
```

- Reads and filters argus data
- Output either to stdout or to another file
- Filter criteria is derived from tcpdump with adaptation to flow semantics and flow-derived record types
- Additional reading
  - `man ra`

ra - Demo

- Simple output
- Show headers
- Name, port and protocol resolution
- Adding and removing column headers
- Filter examples

racount

NAME

```
racount – count things from argus data.
```

SYNOPSIS

```
racount –r argus-file [ra options]
```

- Prints out various counts from the data file

racount - Demo

- Stats without filter.
- Stats with filter.

racluster

NAME

racluster – aggregate the records based on specific flow key criteria.

SYNOPSIS

racluster [-m agr(s)] [raoptions]

- Aggregates all records matching a key.

racluster – Demo

- Show unique fields: SIP, DIP, ports
  - Find number of unique fields: | wc -l
- Aggregate by field:
  - Bytes per port

Note: To cluster on port, you also need to include protocol.

rabins

NAME

`rabins – split argus data to bins`

SYNOPSIS

`rabins –M splitmode [splitmode options] [raoptions]`

- Aggregates data to a set of bins, or slots
- Mainly used to aggregate data on a time series
- Note: Pipe to it using from other commands using `[-w - ]`
- Note: Use `[–m srcid]` to aggregate by argus source identifier

rabins - Demo

- Split data into time slots
  - Days
  - Hours
  - Minutes

rasort

NAME

`rasort- sort argus data`

SYNOPSIS

```
rasort [-M sortmode] [-m sort fields]
[raoptions]
```

- Sorts the records based on the specified criteria
- Note: Pipe to it using from other commands using [`-w -`]
- Tip: show Top-N using unix `head` command.

rasort - Demo

- Show top-10 destination ports by bytes.

Backup

ra-demo:

ra -r sotm27.arg

ra -r sotm27.arg –L0

ra -r sotm27.arg –L0 –n

ra -r sotm27.arg –L0 –nn

ra -r sotm27.arg –L0 –nnn

ra -r sotm27.arg –L0 –nn -s stime proto saddr dir daddr pkts state

ra -r sotm27.arg –L0 –nn -s –state +state:8

ra –r sotm27.arg –L0 –nn – ip and src host 219.118.31.42

Backup (2)

- Racount-demo

racount -r sotm27.arg

racount -r sotm27.arg - host 219.118.31.42

Backup(3)

- Racluster-demo

```
# racluster -r sotm27.arg -m saddr -s saddr -L0 -
   nn - dst host 172.16.134.191
# | wc -l
# racluster -r sotm27.arg -m saddr -s saddr
   sbytes -L0 -nn - dst host 172.16.134.191
```

Backup (4)

- Rabins – demo

```
# ra -r sotm27.arg -w - | rabins -M time 6h -m
   srcid -L0 -s stime bytes
```

1 day, 12 hour, 1 min?

Backup (5)

- Rasort- demo

racluster -r sotm27.arg -m proto dport -w - - dst host 172.16.134.191 | rasort -L0 -m bytes -s proto dport bytes