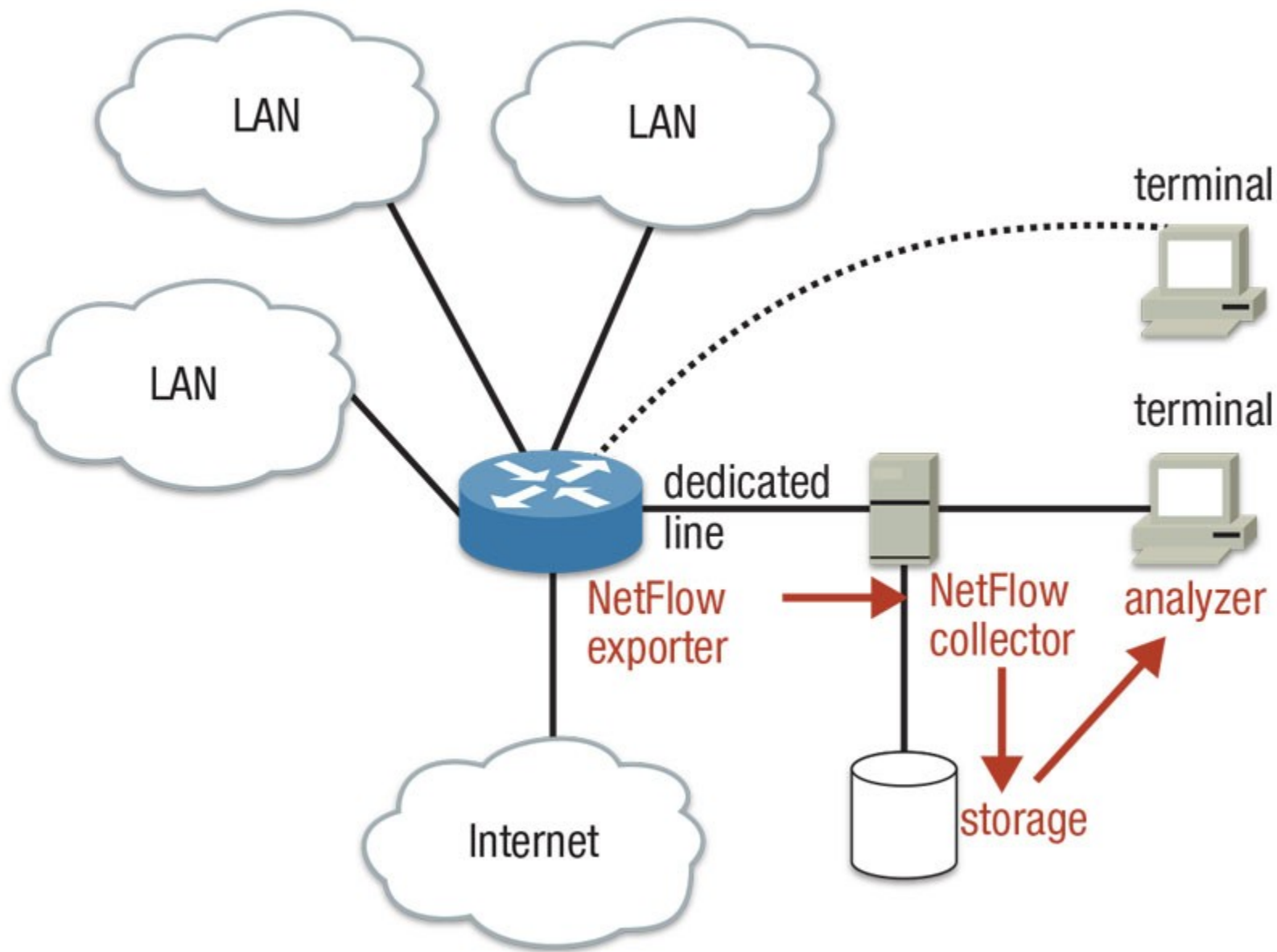


# LAB



## Laboratory - NetFlow

- Processing of NetFlow records
- Collection of data
- Structure of data
- Processing of sample data
  - Search for particular patterns



# Flow data generation

## YAF

- <https://tools.netsa.cert.org/yaf/>
- Yet Another Flowmeter
- Generates IPFIX, large set of features

## Softflowd

- <https://github.com/irino/softflowd>
- Easy to use simple flow generator
- NetFlow v9

## Fprobe

- <http://man.cx/fprobe>
- NetFlow v5, no IPv6 support

# Collection of data

## Nfcapd

- <http://man.cx/nfcapd>
- NetFlow collector

## IPFIXcol

- <https://github.com/cesnet/ipfixcol>
- Flexible IPFIX collector

## SiLK

- <https://tools.netsa.cert.org/silk/>
- Flow data analysis suite

## Collection of data

- Setup a collector and capture the data send from probe
  - nfcapd
  - use port 1[last 4 digits of UČO] based on you user account (i.e. 987654 => port 17654)
  - export flows every 300 s
  - export flows to your home directory

## Structure of data

- Start Time, End Time, Duration
- Protocol
- Flows, Bytes, Packets
- Source Address, Destination Address
- Source Port, Destination Port
- TCP Flags
- Packets per second, Bits per second, Bytes per packet
- Source AS, Destination AS, Input Interface, Output Interface

# Processing of sample data

## Nfdump

- <http://man.cx/nfdump>
- Netflow display and analyzing program
- Filtering, aggregation, top N statistics



## Processing of sample data

```
nfdump [options] ["filter"]
```

- options

- r <input file>

- A <aggregation fields>

- s <statistics>

- n <number of top n>

- filter

- not** src ip 83.187.4.5 **and** (src port 80 **or** src port 443)

## Additional Information

Connect to 10.16.71.143

- Username: UČO
- Password: sha1 hash of UČO
- The flow data has been anonymized
- The university IP range in anonymized data is **83.187.0.0/16**
- To interpret port numbers you can use IANA.org

# Exercises

1. Compute the ratio of UDP packets and flows in the traffic
2. Count the hosts actively communicating from MU network
3. Find most the web server most visited by users from MU network
4. Find how many hosts from MU network has accessed the web on 60.182.41.219:80
5. Find a horizontal scan
6. Find a vertical scan
7. Form groups and find some interesting information in the data

# Homework

Work with the flow data hw.nfcapd in study materials.

1. What is an IP address of the most used DNS server in MU network?

During capture period, a SSH brute force attack was captured.

2. What is the IP address of the attacker?

3. How many victims has the attack?

4. How many ports have been used by attacker to launch the attack?

# Homework

The prefix of MU in data is 147.250.0.0/16

Submit the homework in a format:

- 1.IP of the dns server
- 2.IP of the attacker
- 3.Number of attacked hosts
- 4.Number of port used

Describe briefly for each task the steps you took.