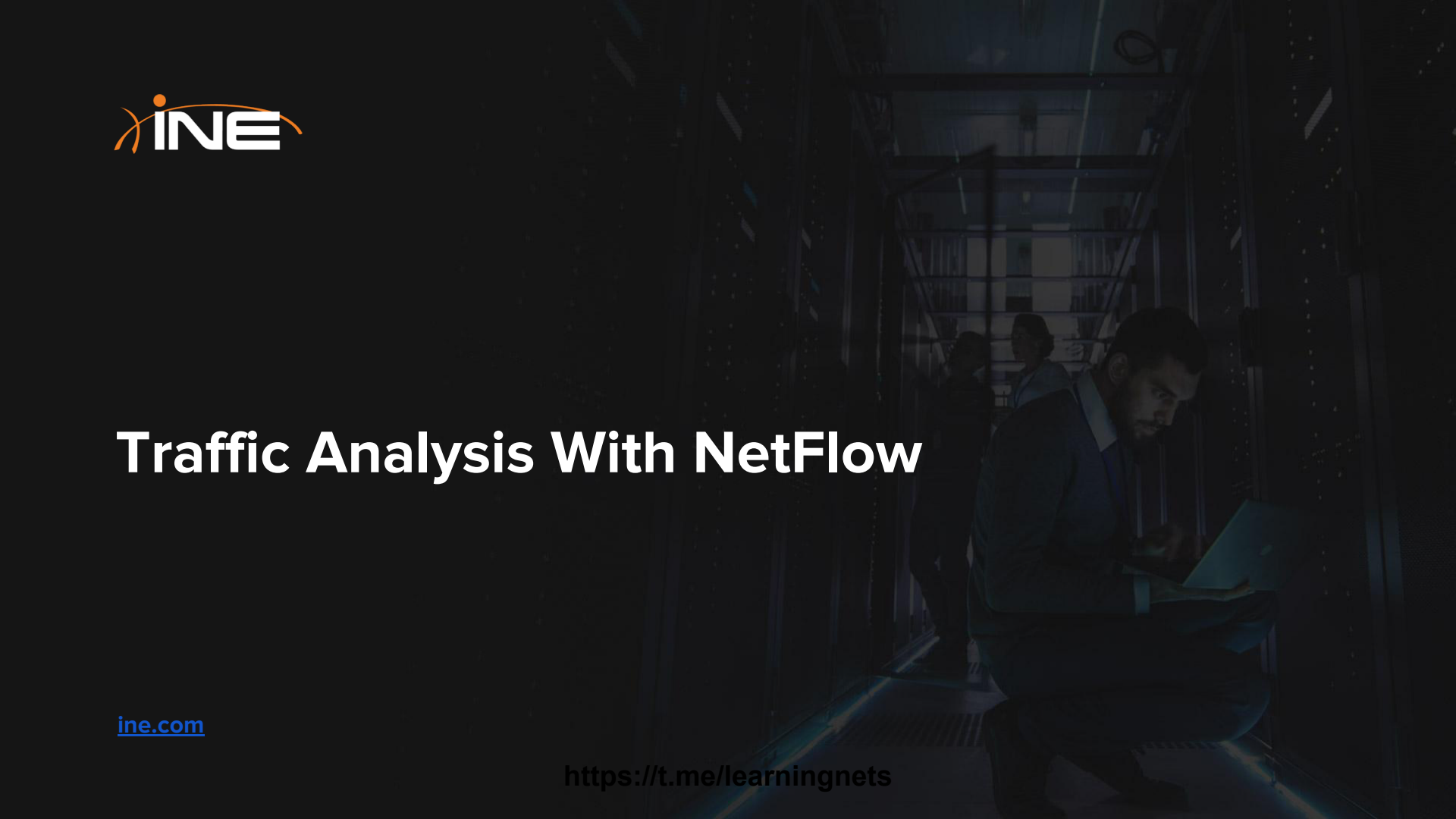


Traffic Analysis With NetFlow

ine.com

Keith Bogart

CCIE #4923

kbogart@ine.com

@keithbogart1

linkedin.com/in/keith-bogart-2a75042

CCIE Routing & Switching

Course Objectives

- To introduce you to why NetFlow exists and how it operates
- Provide an overview of the different versions of NetFlow
- Identify the configuration and operational differences between Original NetFlow and Flexible NetFlow
- Demonstrate how NetFlow data export can be reduced by using Random Samplers and Input Filters

Course Prerequisites

- Understanding of IP Packet Header fields
- Familiarity with Cisco IOS CLI

NetFlow Overview

ine.com

Topic Overview

+ Defining The Problem
+ What Is NetFlow?
+ Flows & The Flow Cache
+ Exporting Flows

Defining The Problem

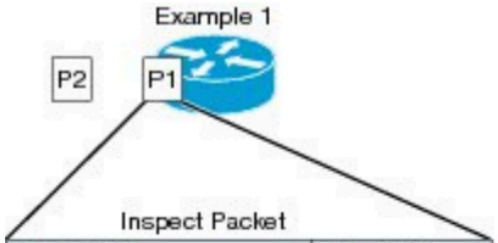
- Network Managers require visibility into traffic flowing into, and out of, their network
- SNMP provides only counters (bytes in, bytes out, etc) but no granularity
- A need exists to be able to classify, monitor, and gather statistics on individual flows of traffic....hence the need for NetFlow

What Is NetFlow?

- Embedded instrumentation within Cisco IOS to characterize network operation
- NetFlow Generator & Collector
- When enabled on an interface it:
  - Sorts all packets into “flows”
  - Collects flow data and places it into a NetFlow Cache
  - Information from NetFlow cache can be viewed with IOS CLI commands, or by exporting it to a NetFlow Collector

What Is A Flow?

- Source IP Address
- Destination IP Address
- Source & Destination Port Number
- Layer-3 Protocol Type
- ToS Byte
- Input Interface



Key Fields	Packet 1
Source IP	10.3.3.3
Destination IP	10.2.7.2
Source port	23
Destination port	22078
Layer 3 Protocol	TCP-6
TOS Byte	0
Input Interface	Ethernet 0

Create Flow record in the Cache

Source IP	Dest. IP	Dest. I/F	Protocol	TOS	...	Pkts
10.3.3.3	10.2.7.2	E1	6	0	...	11000

The Flow Cache

- Every ingress packet is inspected to determine if it belongs to an existing flow, or should be considered the first packet in a new flow
- Each new flow creates an entry in the NetFlow Cache
- NetFlow Cache can contain thousands or even millions of entries at any given time
- Once a flow expires, information about that flow is pushed to a NetFlow Collector (if configured to do so)

Exporting Flows

- NetFlow cache entries are exported once various timers expire or triggers occur:
  - Flow has been idle for a specified period of time (15-seconds default)
  - Flow is classified as “long-lived” (i.e. 30-minutes). In this case information about the flow is exported and (if traffic from this flow is still ongoing) a new Flow Cache entry is built
  - TCP connections in which the FIN or RST flags are seen.
  - If the cache becomes full, heuristics are applied to aggressively age groups of flows
- Expired flows are grouped together into NetFlow Export datagrams (UDP port 2055) and sent to Collector

Thanks for Watching!

NetFlow Versions

ine.com

Topic Overview

+ Differentiating NetFlow Versions
+ NetFlow Version 5 & Export Records
+ NetFlow Version 9 & Export Records

NetFlow Versions

- Version 1: Released in 1996 by Cisco, an export format that is rarely used today
- Versions 2 – 4: Never released
- Version 5: Added several new fields to the flow-cache and flow-record including BGP ASN, flow sequence numbers and IP mask information
- Version 6: No longer supported by Cisco
- Version 7: Old version that supported Hybrid and Native IOS Switches
- Version 8: Supports router-based Flow Aggregation
- Version 9: Template-based, also supports IPv6

NetFlow Version 5

- Limited to IPv4 (no IPv6 support)
- Packet format fixed, predictable and unchanging
- Collector software is hardcoded to know what to expect in a received NetFlow packet

NetFlow v5 Export Record

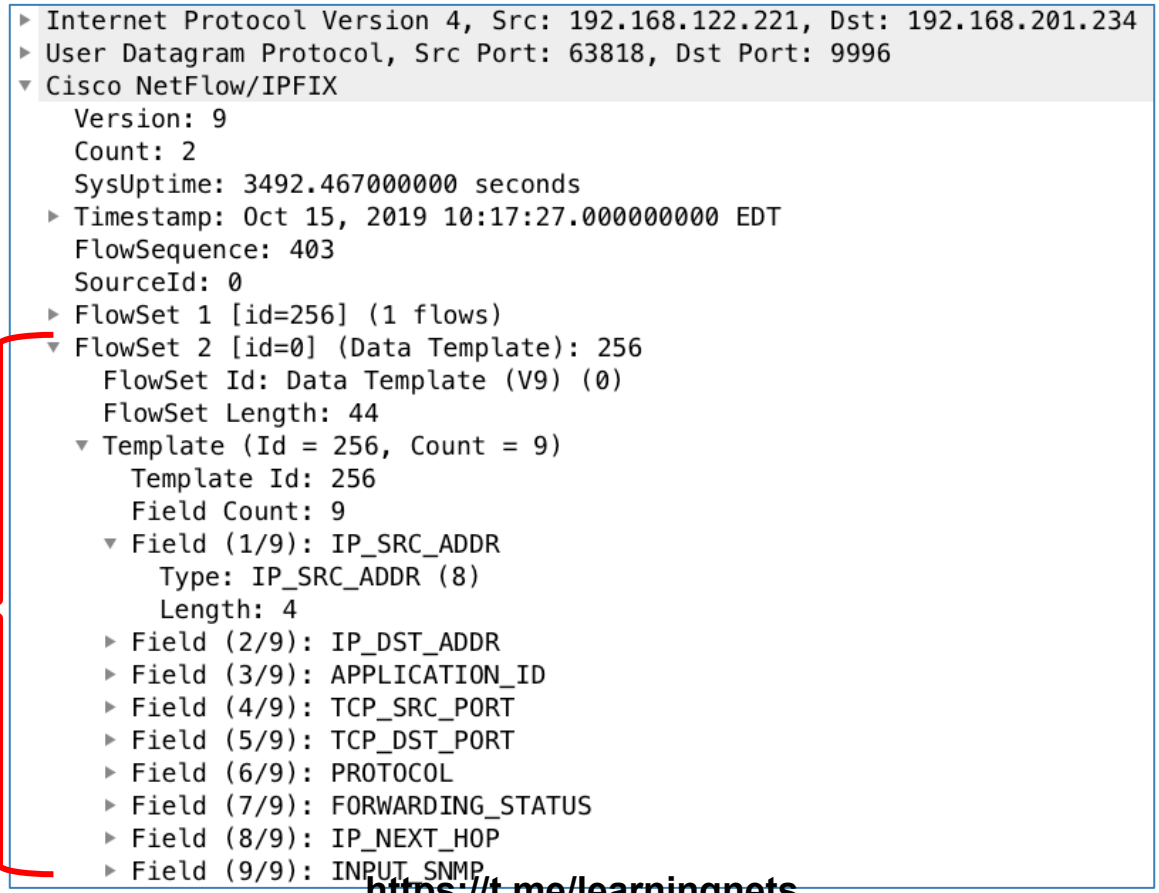
```
└     3 241.975780    2.3.2.2               2.3.2.3               CFLOW     114 total: 1 (v5) flow

▶ Frame 3: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
▶ Ethernet II, Src: c2:02:1c:4f:00:01 (c2:02:1c:4f:00:01), Dst: c2:03:1c:50:00:00 (c2:03:1c:50:00:00)
▶ Internet Protocol Version 4, Src: 2.3.2.2, Dst: 2.3.2.3
▶ User Datagram Protocol, Src Port: 61922, Dst Port: 2055
▼ Cisco NetFlow/IPFIX
    Version: 5
    Count: 1
    SysUptime: 586.344000000 seconds
  ▶ Timestamp: Feb 28, 2002 19:09:46.343930578 EST
    FlowSequence: 4
    EngineType: RP (0)
    EngineId: 0
    00.. .... .... .... = SamplingMode: No sampling mode configured (0)
    ..00 0000 0000 0000 = SampleRate: 0
  ▼ pdu 1/1
      SrcAddr: 1.2.1.1
      DstAddr: 2.3.2.3
      NextHop: 2.3.2.3
      InputInt: 2
      OutputInt: 4
      Packets: 5
      Octets: 500
    ▶ [Duration: 8.012000000 seconds]
      SrcPort: 0
      DstPort: 2048
      Padding: 00
      TCP Flags: 0x10
      Protocol: ICMP (1)
      IP ToS: 0x00
      SrcAS: 0
      DstAS: 0
      SrcMask: 24 (prefix: 1.2.1.0/24)
      DstMask: 24 (prefix: 2.3.2.0/24)
      Padding: 0000
```

NetFlow Version 9

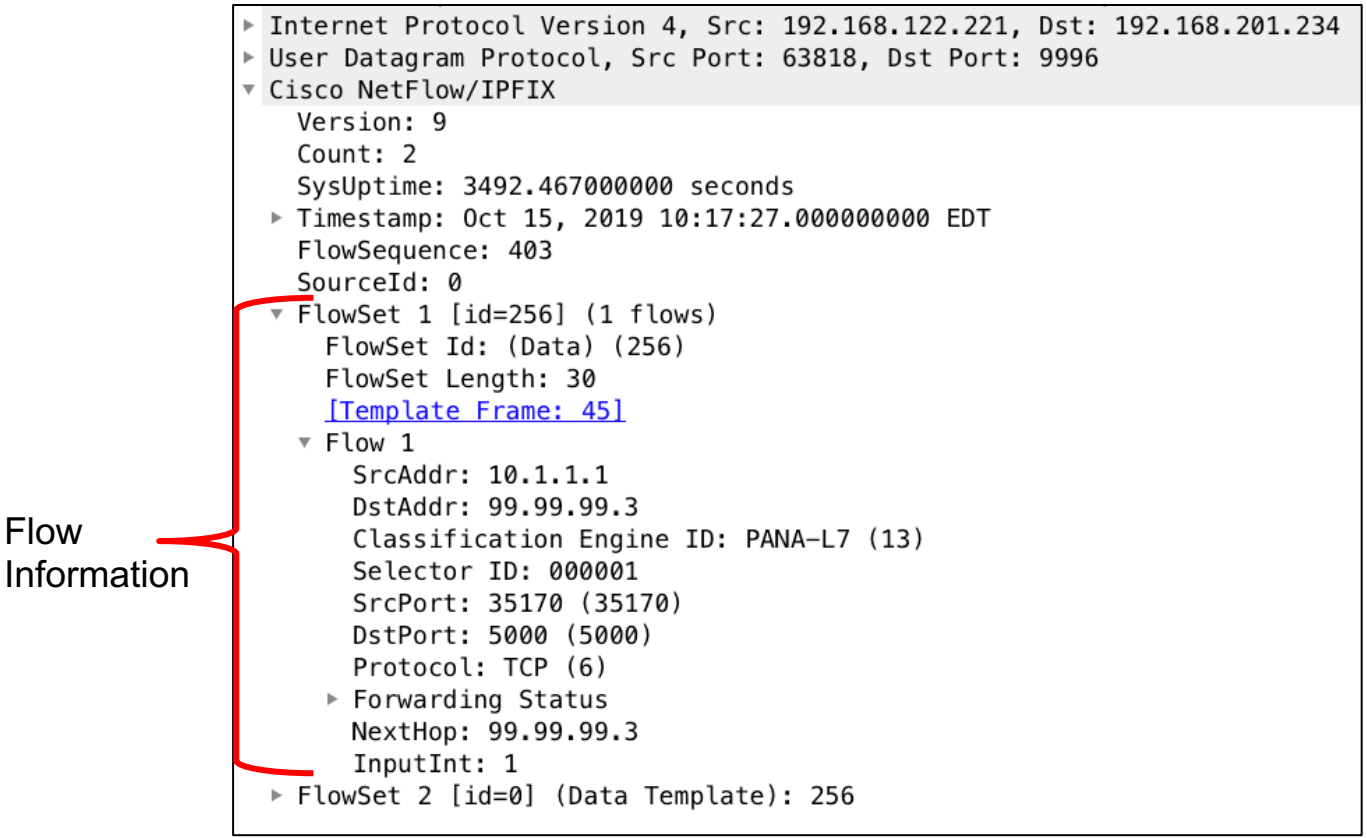
- Current industry standard
- Supports both IPv4 and IPv6
- Template-based
  - A Template defines exactly what information you want exported to the Collector
  - YOU define the Template
  - Template definitions periodically sent to the Collector
  - You may configure/utilize more than one Template

NetFlow Version 9 Export Record

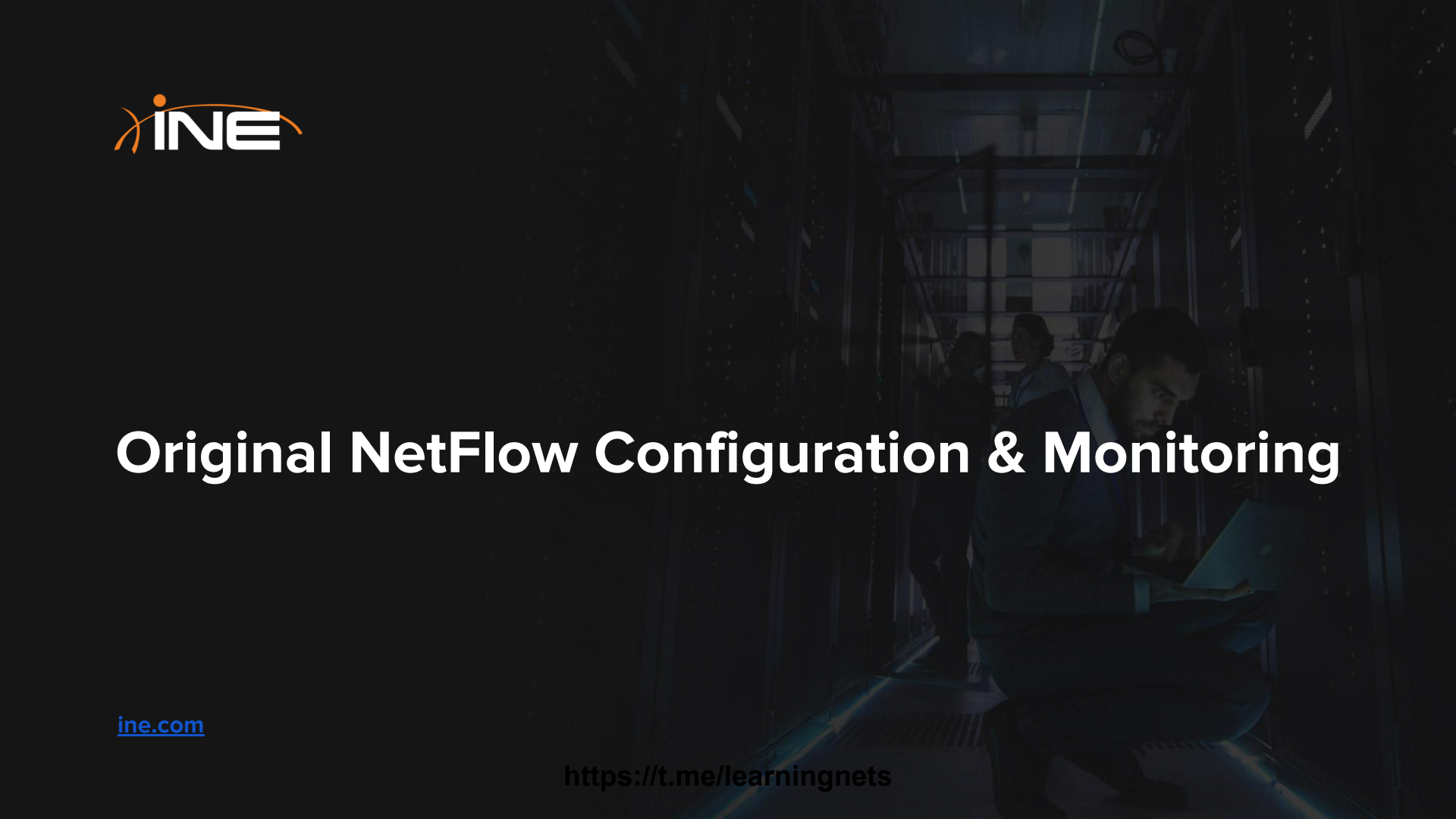


Template Information

NetFlow Version 9 Export Record



Thanks for Watching!



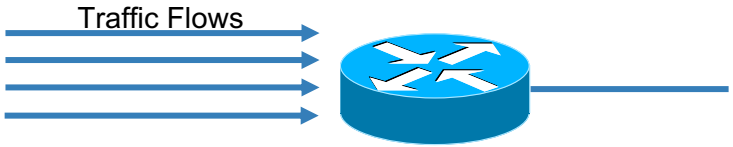
Original NetFlow Configuration & Monitoring

ine.com

Topic Overview

+ Enabling Original NetFlow
+ Viewing The Flow Cache
+ Monitoring Original NetFlow

Enabling Original NetFlow



- Enable Cisco Express Forwarding
  - Device(config)#ip cef
- Enable NetFlow on one-or-more interfaces
  - Device(config-if)#ip flow <ingress | egress>
- Modify timeout values for flows (*optional*)
  - Device(config)#ip flow-cache timeout <active | inactive> <1-60>

Viewing The Flow Cache

- Show ip flow interface
  - Verifies that NetFlow has been configured
- Show ip cache flow
  - Provides flow statistics and summarized flow information
- Show ip cache verbose flow
  - Same as above but provides more granular details of each flow

Monitoring Original NetFlow

```
R2#show ip flow interface
GigabitEthernet0/1
  ip flow egress
```

```
R2#show ip cache flow
IP packet size distribution (17 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .588 .352 .058 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  6 active, 4090 inactive, 6 added
  42 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
```

Monitoring Original NetFlow

```
R2#show ip cache flow
```

<output omitted>

```
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-BGP              6      0.0         2    54       0.0       3.8      15.3
TCP-other           20      0.0         4    41       0.1       0.0       1.6
UDP-NTP             16      0.0         2    76       0.0       2.0      15.1

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
UDP-other           19      0.0         1    80       0.0       0.0      15.6
Total:              61      0.1         2    55       0.3       0.9      10.9

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         10.1.1.1        Gi0/1         99.99.99.3      01 0000 0800    30
Gi0/0         10.1.1.1        Gi0/1         99.99.99.3      11 1E61 07AF   152
Gi0/0         10.1.1.1        Null          224.0.0.10      58 0000 0000    66
```

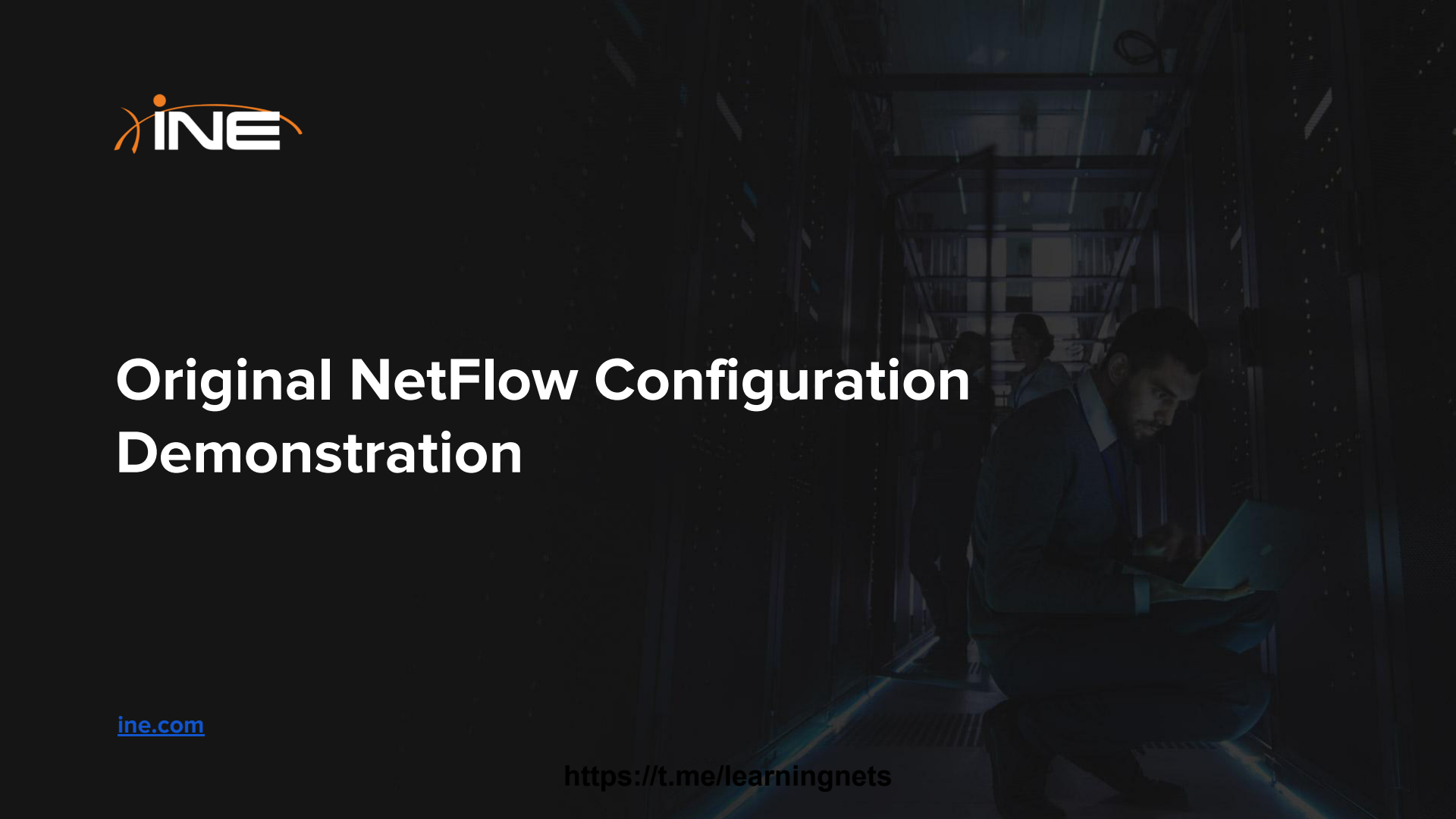
Show IP Cache Verbose Flow

```
R2#show ip cache verbose flow
```

<output omitted>

```
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                   Port Msk AS   NextHop              B/Pk  Active
Gi0/0         10.1.1.1        Gi0/1         99.99.99.3      11 00  10        1
FF5C /0   0                   07AF /0   0   0.0.0.0                80      0.0
```

Thanks for Watching!



Original NetFlow Configuration Demonstration

ine.com

Topic Overview

+ Demonstration Of Original NetFlow Configuration

Thanks for Watching!

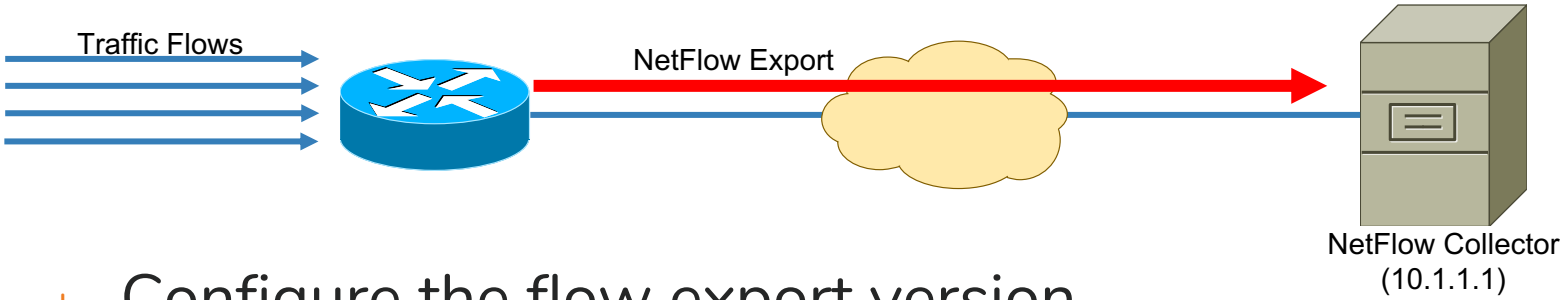
Original NetFlow Export & Monitoring

ine.com

Topic Overview

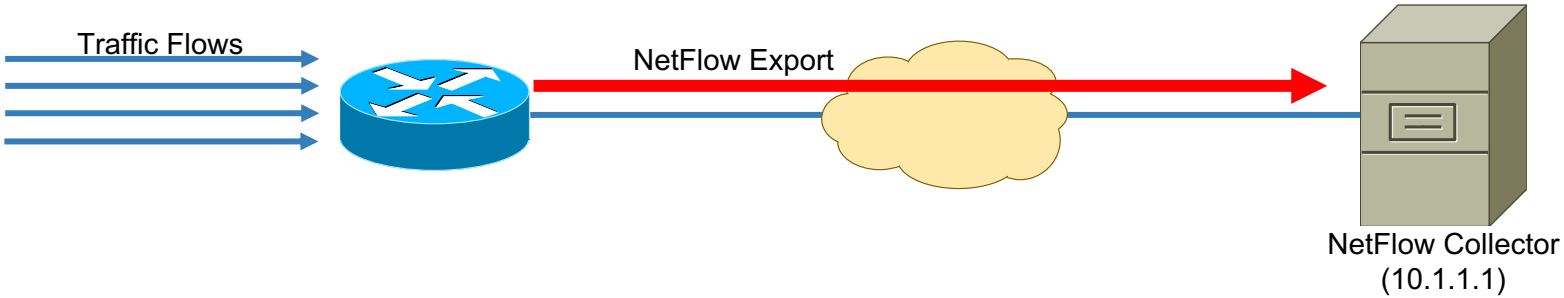
- Enabling Original NetFlow Data Export
- Monitoring Data Export

Enabling Original NetFlow Export



- Configure the flow export version
  - Device(config)#ip flow-export version <1 | 5 | 9>
- Specify the address of (up to two) NetFlow Collectors
  - Device(config)# ip flow-export destination {hostname | ip-address} port [udp | sctp] [vrf vrf-name]
- Allow additional statistics to be exported for v.9 (optional)
  - Device(config)# ip flow-capture <fragment-offset | icmp | ip-id | mac-addresses | packet-length | ttl | vlan-id>

Enabling Original NetFlow Export

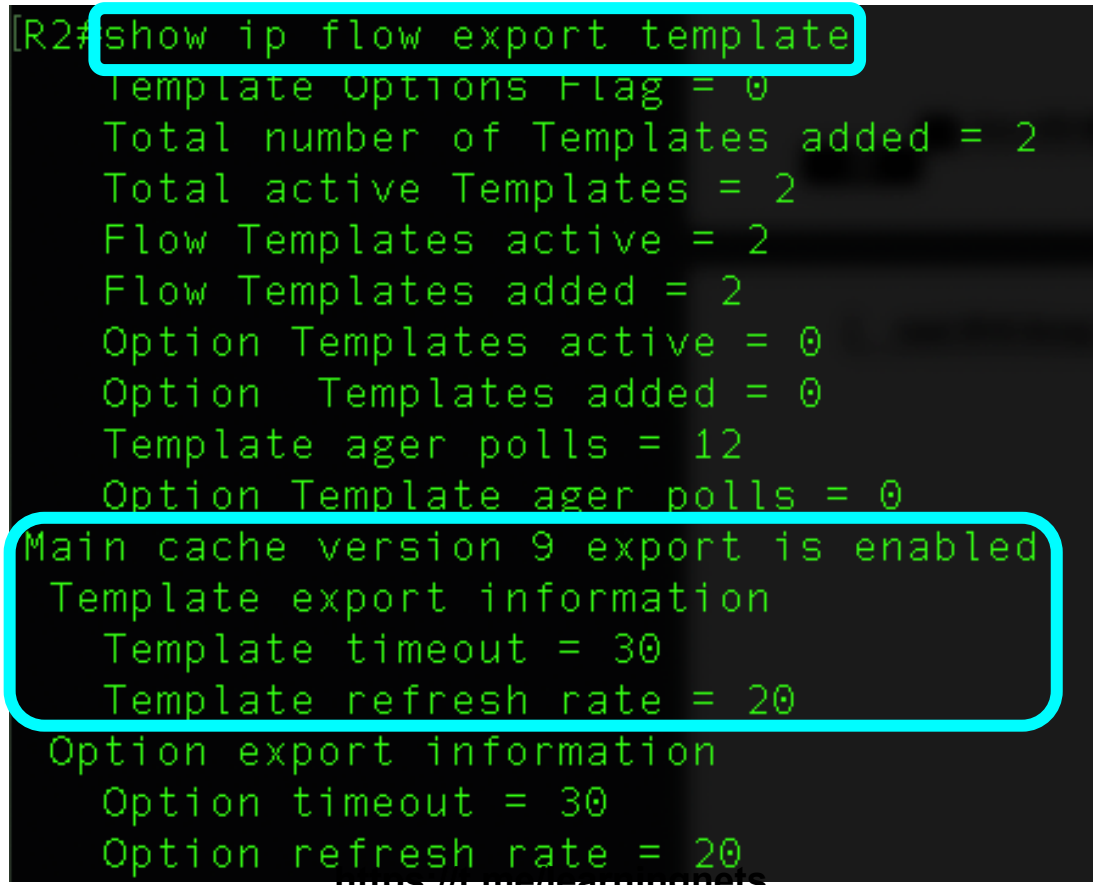


- Specify the source IP address for exported packets (optional)
  - Device(config)# ip flow-export source <interface name/number>

Monitoring Original NetFlow Export

```
R2#show ip flow export
Flow export v9 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Destination(1)  192.168.201.207 (9996)
  Version 9 flow records
  485 flows exported in 136 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
```

Monitoring Original NetFlow Export



Thanks for Watching!

Introducing Flexible NetFlow

ine.com

Topic Overview

+ Original vs. Flexible NetFlow
+ General Concepts Of Flexible NetFlow

Original vs Flexible NetFlow

- On Cisco IOS devices, NetFlow can be configured in one-of-two ways:
  - Original NetFlow
  - Flexible NetFlow
- Most original NetFlow commands start with "ip flow-xxx"
  - Primarily designed for NetFlow v.5
  - Can be utilized with NetFlow v.9 but severely limits the type of data that can be captured/exported
- Flexible NetFlow utilizes modularity when configuring NetFlow

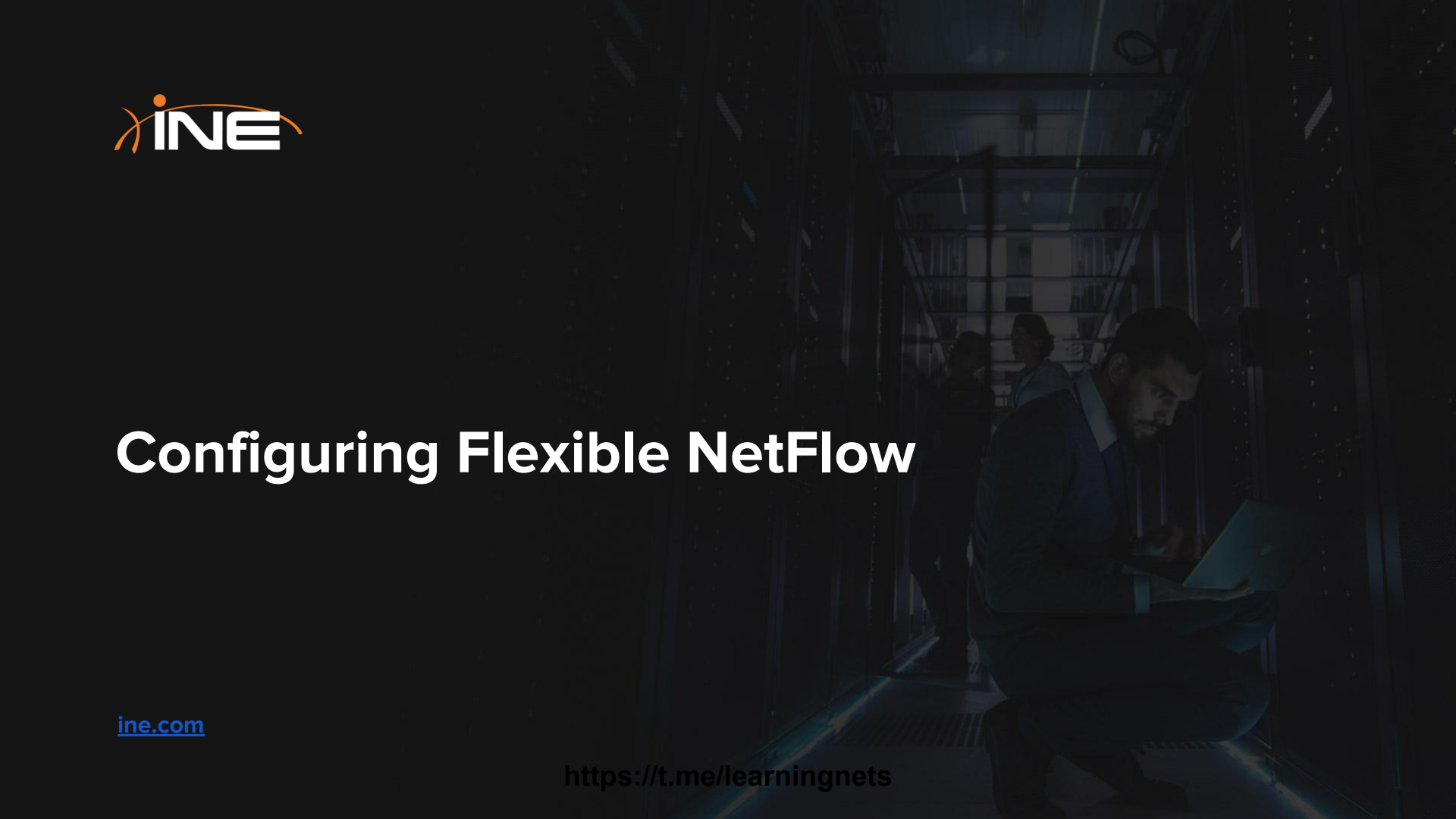
Original vs Flexible NetFlow

- Some platforms allow both styles, some allow only Flexible NetFlow configuration
- Configuration of additional NetFlow features (such as Random Sampling) will vary depending on whether original or Flexible NetFlow has been utilized
  - Some features are only available in one mode or the other

Flexible NetFlow General Concepts

- Flow Exporters
  - Original NetFlow only supports two (2) exporters
  - Flexible NetFlow supports up to ten (10) exporters
- Flow Records
  - NetFlow export version-9 with original NetFlow limited in quantity of descriptive fields that were available
  - Flexible NetFlow allows collection of greater quantity of granular data
- Flow Monitors
  - Provides flexibility with pairing of Exporters to Records

Thanks for Watching!



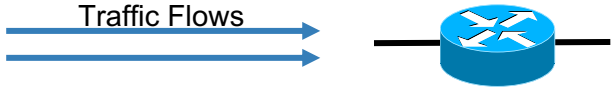
Configuring Flexible NetFlow

ine.com

Topic Overview

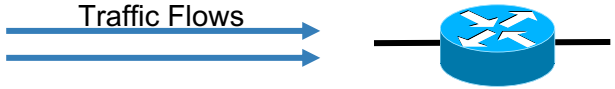
+ Enabling Flexible NetFlow

Enabling Basic Flexible NetFlow



- Enable Cisco Express Forwarding
  - Device(config)#ip cef
- Create one or more Flow Monitors
  - Device(config)#flow monitor <name>
- Define the record format within the Flow Monitor
  - Device(config-flow-monitor)# record {record-name | netflow-original | netflow {ipv4 | ipv6 } record [peer]}

Enabling Flexible NetFlow



- Modify characteristics of the NetFlow Cache (optional)
  - Device(config-flow-monitor)#
    cache {entries number | timeout {active | inactive | update } seconds |
    {immediate | normal | permanent }}
- Enable NetFlow on the desired interface
  - Device(config-if)#ip flow monitor <name> <input | output>

Example Configuration

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#flow monitor INE
R2(config-flow-monitor)#record netflow-original
R2(config-flow-monitor)#exit
R2(config)#interface gig0/0
R2(config-if)#ip flow monitor INE input
R2(config-if)#end
```

Thanks for Watching!

Monitoring Flexible NetFlow

ine.com

Topic Overview

+ Various Commands To Monitor Flexible NetFlow

Monitoring Flexible NetFlow

```
R2#show flow monitor
Flow Monitor Test:
  Description:        User defined
  Flow Record:        netflow-original
  Cache:
    Type:                 normal
    Status:               allocated
    Size:                 4096 entries / 344088 bytes
    Inactive Timeout:     15 secs
    Active Timeout:       1800 secs

Flow Monitor IP:
  Description:        User defined
  Flow Record:        netflow ipv6 original-input
  Cache:
    Type:                 normal
    Status:               not allocated
    Size:                 4096 entries / 0 bytes
    Inactive Timeout:     15 secs
    Active Timeout:       1800 secs
```

Monitoring Flexible NetFlow

```
R1#show flow record netflow-original
flow record netflow-original:
  Description:        Traditional IPv4 input NetFlow with origin ASs
  No. of users:       1
  Total field space:  53 bytes
  Fields:
    match ipv4 tos
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    match interface input
    match flow sampler
    collect routing source as
    collect routing destination as
    collect routing next-hop address ipv4
    collect ipv4 source mask
    collect ipv4 destination mask
    collect transport tcp flags
    collect interface output
    collect counter bytes
    collect counter packets
    collect timestamp sys-uptime first
    collect timestamp sys-uptime last
```

Monitoring Flexible NetFlow

```
R2#show flow interface gig0/0
Interface GigabitEthernet0/0
  FNF:   monitor:                Test
         direction:              Input
         traffic(ip):            on
```

Monitoring Flexible NetFlow

```
R2#show flow monitor Test cache
  Cache type:                                   Normal
  Cache size:                                     4096
  Current entries:                                   6
  High Watermark:                                   10

  Flows added:                                     231
  Flows aged:                                      225
    - Active timeout      (  1800 secs)              0
    - Inactive timeout    (    15 secs)            225
    - Event aged                                     0
    - Watermark aged                                 0
    - Emergency aged                                 0

IPV4 SOURCE ADDRESS:        10.1.1.1
IPV4 DESTINATION ADDRESS:   99.99.99.3
TRNS SOURCE PORT:           7777
TRNS DESTINATION PORT:      1967
INTERFACE INPUT:            Gi0/0
FLOW SAMPLER ID:            0
IP TOS:                     0x00
IP PROTOCOL:                17
ip source as:               0
ip destination as:          0
ipv4 next hop address:      99.99.99.3
ipv4 source mask:           /24
ipv4 destination mask:      /24
 --More--
```

Thanks for Watching!

Flexible NetFlow Records

ine.com

Topic Overview

- Defining Flow Records
- Creating Custom Flow Records
- Adding Flow Records To Flow Monitors
- Monitoring Flow Records & The Flow Cache

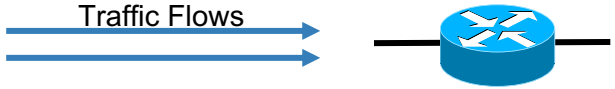
Flexible NetFlow Records

- Like original NetFlow, Flexible NetFlow constructs a flow cache
- The structure of entries within the flow cache is defined by a NetFlow Record
- Each Flow Monitor maintains its own NetFlow cache
- A NetFlow Record is a required component of a Flow Monitor
- One can utilize pre-defined NetFlow records or construct your own

Flow Record Components

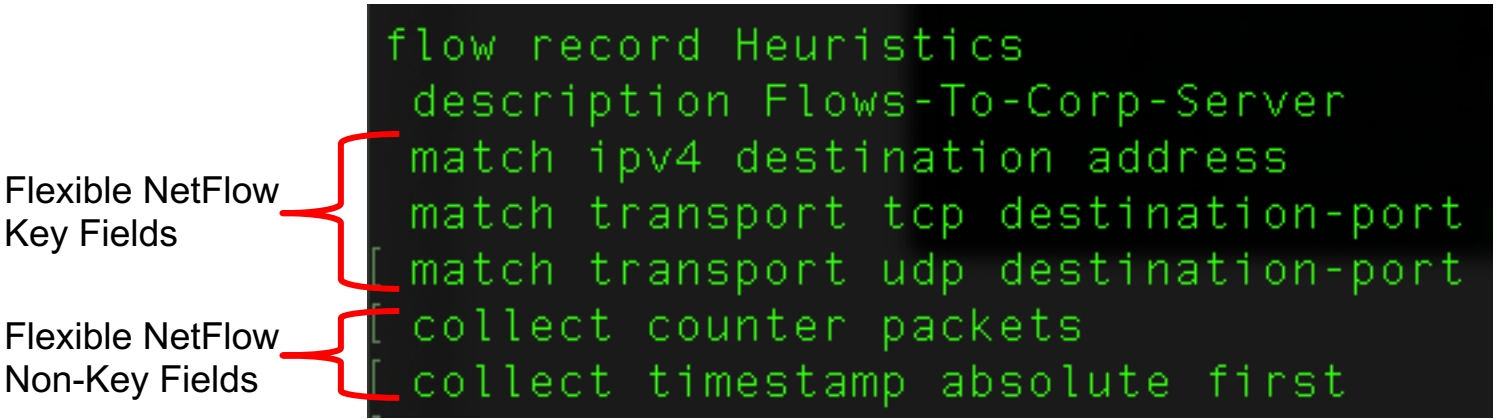
- Flow records contain two components:
  - “match” statements
  - “collect” statements
- Match statements
  - Are required
  - Match on key fields for flow identification
  - Components identified in “match” statements are included in NetFlow export records
- Collect statements
  - Are optional
  - Match on non-key fields for additional visibility about flow details
  - Are included in NetFlow export records

Flexible NetFlow Custom Records

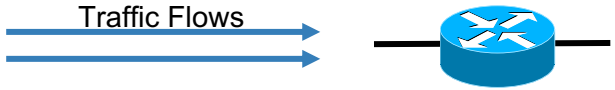


- Create one or more Flow Records
  - Device(config)#flow record <name>
- Provide an (optional) description for the Flow Record
  - Device(config-flow-record)#description Data-to-web-server
- Specify match criteria for flow identification
  - Device(config-if)#match ipv4 destination address
- Specify (optional) non-key fields to be exported to Collector
  - Device(config-if)#collect counter packets

Flexible NetFlow Records



Associate Records To Monitors



- Associate NetFlow records to monitors
  - Device(config)#flow monitor <name>
- Provide an (optional) description for the Flow Record
  - Device(config-flow-monitor)#record <name>

Sample Configuration

```
R2(config)#flow record Payroll-Server
R2(config-flow-record)#match ipv4 destination address
R2(config-flow-record)#match ipv4 protocol
R2(config-flow-record)#collect counter packets
R2(config-flow-record)#exit
R2(config)#flow monitor INE
R2(config-flow-monitor)#record Payroll-Server
R2(config-flow-monitor)#exit
R2(config)#interface gig0/0
R2(config-if)#ip flow monitor INE input
R2(config-if)#end
R2#
```

Monitoring Flow Records

```
R2#show flow record ?
  Payroll-Server    User defined
  name              Show the configuration for a specific Flow Record
  netflow           Traditional NetFlow collection schemes
  netflow-original  Traditional IPv4 input NetFlow with origin ASs
  type              Type of the Flow Record
  |                 Output modifiers
  <cr>

R2#show flow record Payroll-Server
flow record Payroll-Server:
  Description:         User defined
  No. of users:        1
  Total field space:   9 bytes
  Fields:
    match ipv4 protocol
    match ipv4 destination address
    collect counter packets
```

Confirming The Flow Cache

```
R2#show flow monitor INE cache
  Cache type:                                 Normal
  Cache size:                                   4096
  Current entries:                                 4
  High Watermark:                                  4

  Flows added:                                     4
  Flows aged:                                      0
    - Active timeout      (  1800 secs)            0
    - Inactive timeout    (    15 secs)            0
    - Event aged                                   0
    - Watermark aged                               0
    - Emergency aged                               0

IPV4 DST ADDR    IP PROT         pkts
---------------- ------- ------------
224.0.0.10            88           73
99.99.99.3            17          394
99.99.99.3             1           34
99.99.99.3             6          100
```

Thanks for Watching!

Flexible NetFlow Data Export

ine.com

Topic Overview

+ Data Export For Flexible NetFlow
+ Data Export Configuration
+ Optional Export Features
+ Monitoring Data Export

Data Export For Flexible NetFlow

- NetFlow is typically activated so that flow information can be exported to an external collector
- The flow exporter:
  - Identifies the destination of the flow collector
  - Specifies the NetFlow export version
  - Allows you to specify the UDP port number
  - Provides other optional capabilities
- Original NetFlow configuration is limited to two (2) exporters
- Flexible NetFlow allows up to ten (10) flow exporters per flow monitor

Data Export Configuration

- Create and name your flow exporter
  - Device(config)#flow exporter <name>
- Provide the IP address and UDP port numbers for communicating with the collector
  - Device(config-flow-exporter)#destination <ip-address>
  - Device(config-flow-exporter)#transport udp <1-65535>
- (Optional) Specify the NetFlow export version
  - Device(config-flow-exporter)#export-protocol <ipfix | netflow-v5 | netflow-v9>
  - NetFlow version-9 is the default if left unspecified

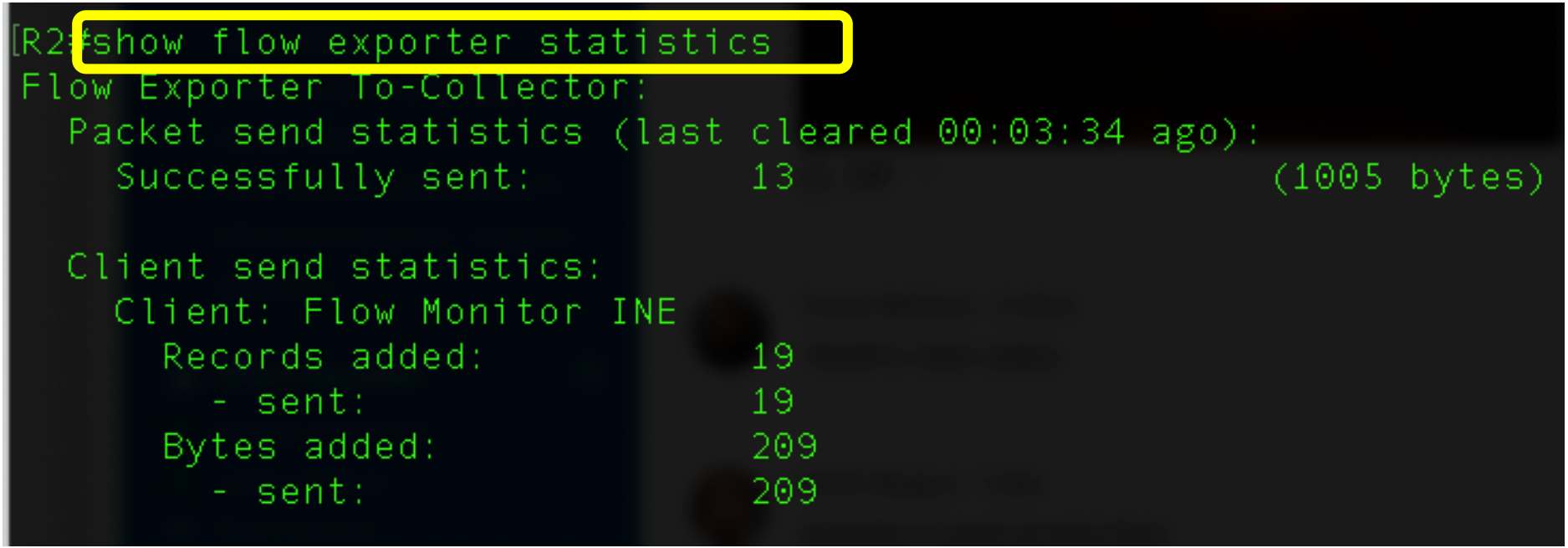
Optional Export Configuration

- Specify the source IP address of exported packets
  - Device(config-flow-exporter)#source <interface name/number>
- Modify the timeout value for sending NetFlow v.9 Template definitions
  - Device(config-flow-exporter)#template data timeout <1-86400>

Monitoring NetFlow Data Export

```
R2#show flow exporter To-Collector
Flow Exporter To-Collector:
  Description:                  User defined
  Export protocol:              NetFlow Version 9
  Transport Configuration:
    Destination IP address:     88.88.88.8
    Source IP address:          192.168.122.221
    Transport Protocol:         UDP
    Destination Port:           9995
    Source Port:                57699
    DSCP:                       0x0
    TTL:                        255
    Output Features:            Not Used
```

Monitoring NetFlow Data Export



Thanks for Watching!

NetFlow Data Sampling

ine.com

Topic Overview

+ The Problem Defined
+ Introducing NetFlow Samplers
+ NetFlow Input Filters

Problems With NetFlow Data Export

- Depending on the quantity of exporters, a NetFlow Collector might need to capture and save thousands (if not hundreds of thousands) of flows per second
- This can consume:
  - Tremendous network bandwidth
  - Great quantities of memory on the router to store large NetFlow caches
  - Tremendous resources on the Collector
- This quantity of data may not be necessary for your objectives

NetFlow Samplers

- Reducing the sampling rate for NetFlow can save bandwidth and resources
- NetFlow samplers can be created to support:
  - Random sampling of flows (original and Flexible NetFlow)
  - Deterministic sampling of flows (Flexible NetFlow only)
- Samplers configure NetFlow to process only one randomly/deterministically selected packet out of “n” sequential packets
  - “n” is a user-configurable parameter

NetFlow Random Samplers

- NetFlow Random Sampling (NetFlow Original Mode) can be configured in two different ways:
  - Randomly sample one-out-of-every-n collected packets on an interface
  - Create a NetFlow Input Filter and subsequently randomly sample one-out-of-every-n-packets that match that input filter
- You can use full NetFlow or Random Sampled NetFlow on an interface…but not both (Full NetFlow overrides Random Sampled NetFlow)

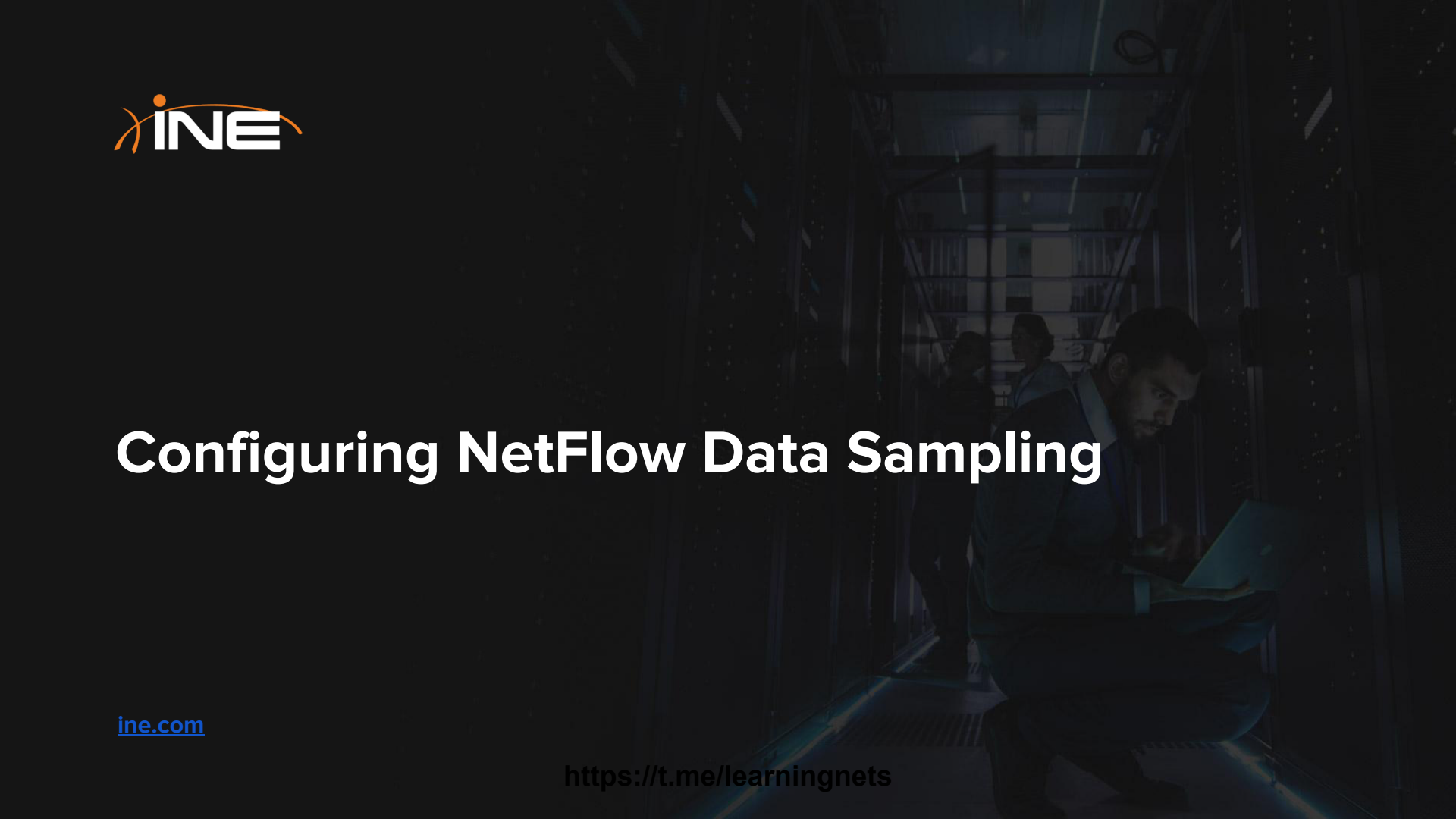
Original NetFlow Input Filters

- Input filters can be created on any of the following criteria:
  - IP source and destination addresses
  - Layer 4 protocol and port numbers
  - Incoming interface
  - MAC address
  - IP Precedence or DSCP value
  - Layer 2 information (such as Frame-Relay DE bits or Ethernet 802.1p bits)
  - Network-Based Application Recognition (NBAR) information
- Flow accounting information is then created for matched flows

Original NetFlow Input Filters

- The NetFlow input filters feature uses the Modular QoS Command-Line Interface (MQC) to classify flows
  - Simply configure a class-map and match on your desired criteria
- Two types of filters are available for matching
  - ACL-based flow-mask filters
  - Fields of filter (done within Class-Map statements)

Thanks for Watching!



Configuring NetFlow Data Sampling

ine.com

Topic Overview

+ Configuring NetFlow Random Sampling

Original NetFlow Random Samplers

- Uses an algorithm that selects a subset of traffic for NetFlow processing
- Requires configuration of a named NetFlow Sampler Map
- Packets are randomly sampled so that one out of each “n” sequential packets is selected on average

Configuring Original NetFlow Random Samplers

```
ip cef
!
flow-sampler-map <name>
 mode random one-out-of <1-65535>
 exit
!
interface gigabitethernet0/0
 flow-sampler <name>
 End
```

Monitoring Original NetFlow Random Samplers

- Flow-cache prior to adding the random-sampler:

```
R2#show ip cache flow
IP packet size distribution (123 total packets):
IP Flow Switching Cache, 278544 bytes
  8 active, 4088 inactive, 19 added
  395 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
```

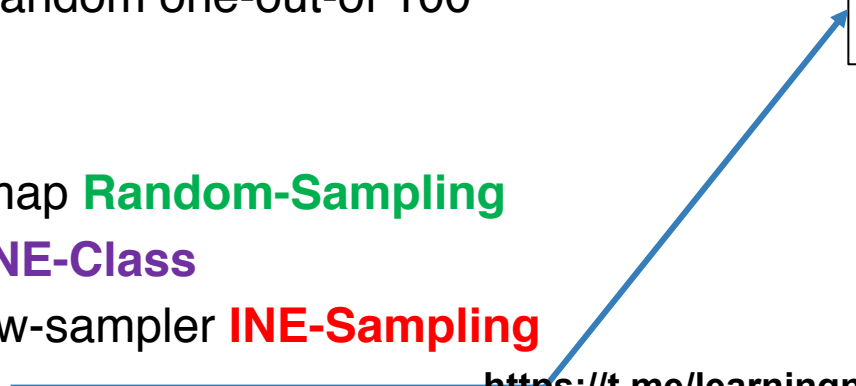
- Flow-cache after adding a random-sampler:

```
R2#show ip cache flow
IP packet size distribution (30 total packets):
IP Flow Switching Cache, 278544 bytes
  1 active, 4095 inactive, 2 added
  33 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
```

Random Sampling With Input Filtering

```
Access-list 101 permit xxxxxxxxxx
!
class-map INE-Class
 match access-group 101
 exit
!
flow-sampler-map INE-Sampling
 mode random one-out-of 100
 exit
!
policy-map Random-Sampling
 class INE-Class
   netflow-sampler INE-Sampling
   exit
```

```
!
Interface GigabitEthernet0/0
 service-policy input Random-Sampling
!
```



Configuring NetFlow Sampled Mode (Flexible NetFlow)

```
ip cef
!
sampler <sampler-name>
  mode {deterministic | random } 1 out-of <2-32768 window-size>
  exit
!
interface <type number>
  {ip | ipv6 } flow monitor <monitor-name> [[sampler ] sampler-name ]
      {input | output }
  end
!
```

Thanks for Watching!

Course Conclusion

ine.com

Topics Covered

- Introduced NetFlow technology and the problems it solved
- Discussed the relevant components of NetFlow such as flow records, the flow cache and flow export
- Covered the differences between the various (current) NetFlow versions
- Demonstrated the differences between Original & Flexible NetFlow
- Identified how flow export could be reduced by utilizing flow samplers and input filters