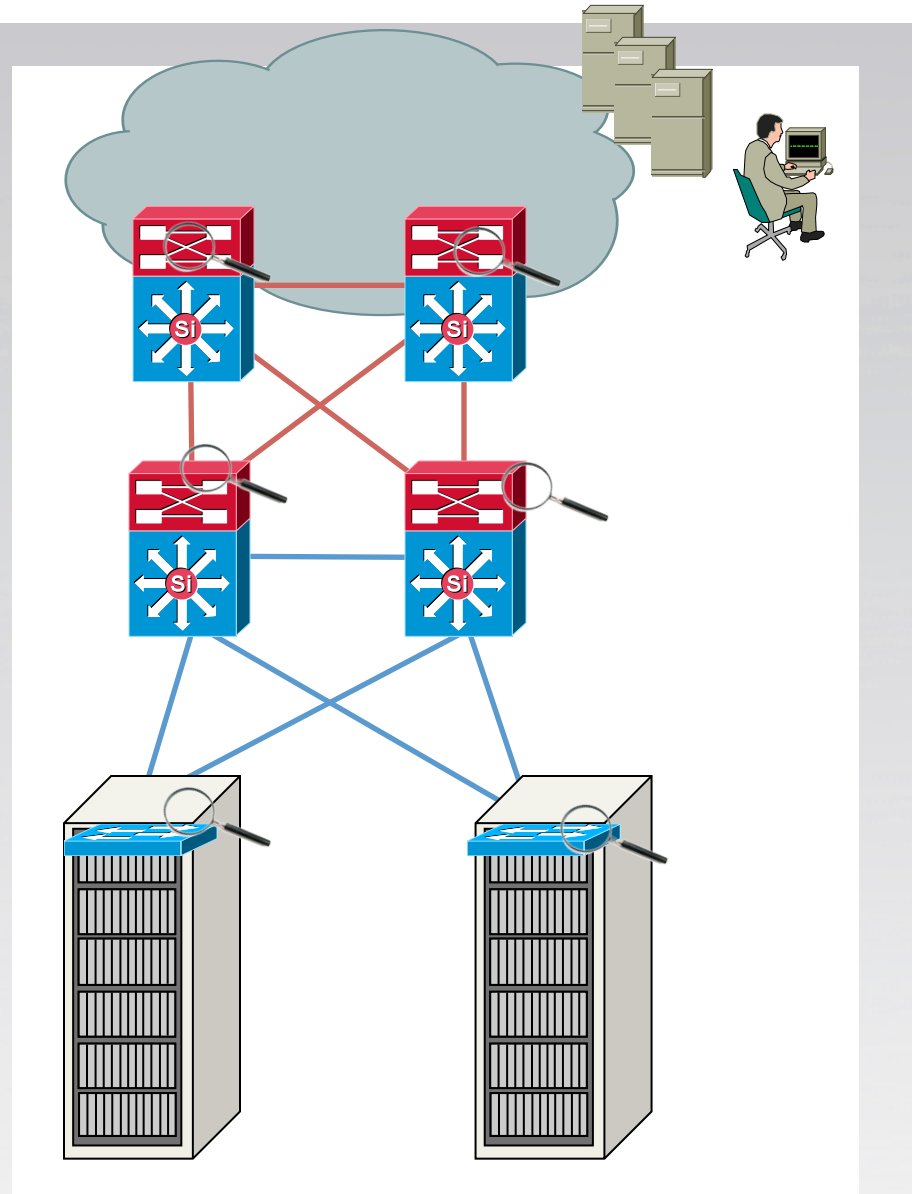# Cisco Catalyst 4948E NetFlow-lite

Application Visibility in Data Center

Why Application Visibility in Data Center

- **Efficient Operation**
  - What applications are consuming bandwidth
  - Who is using them
  - When they are being used
  - What activities are prevalent
- **Visibility** into the network & control
- End-user experience management
- Network and capacity planning
- Troubleshooting
- Network forensics

Introducing NetFlow-lite

NetFlow-lite Aggregator

Any NetFlow Collector

NetFlow-lite 1:N packet sampling

NetFlow v9 or IPFIX export
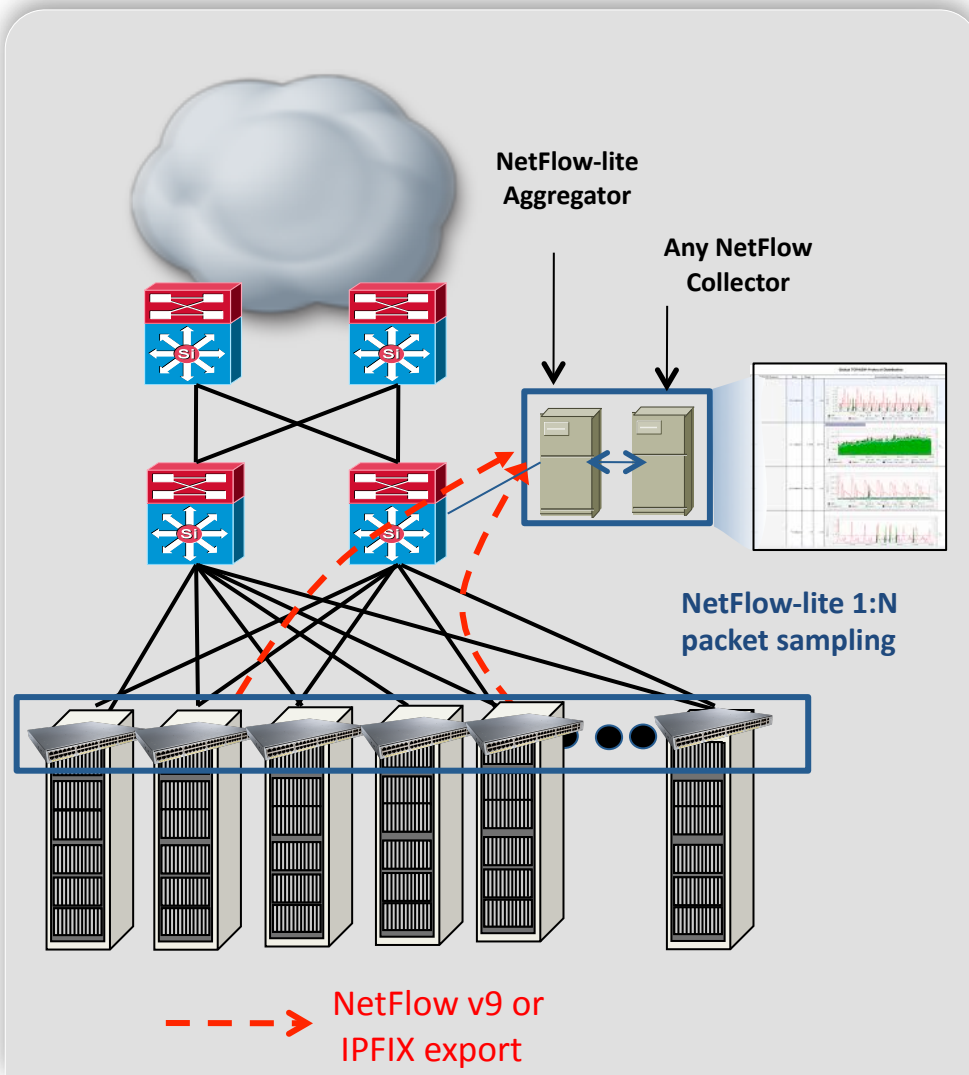
What is NetFlow-lite for?

- Traffic monitoring capability for east-west & north-south L2/L3 traffic.

- Identify top talkers (applications, servers, hosts)

- Capacity planning thru insights of link/network utilization

What does NetFlow-lite Provide?

- Up to 1:32 sampling on all 1G downlink & 10G uplink ports

- 1:1 sampling on up to 2 downlink ports for troubleshooting

- Supported on L2/L3 ports, EtherChannel

- NetFlow v9 and IPFIX format

- Optional packet section

NetFlow-lite:

Building upon the flexibility of Flexible NetFlow

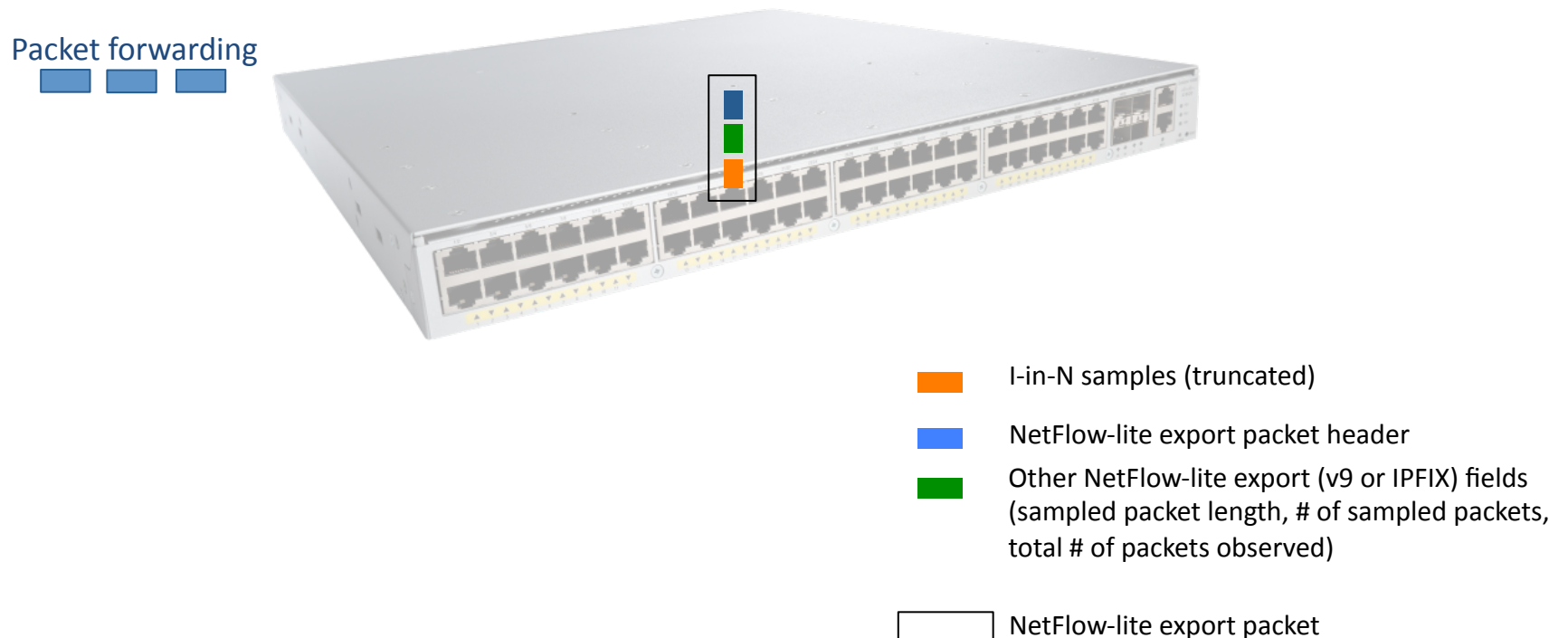|	Flexible NetFlow	NetFlow-lite
Metering Process	More selection of flow keys* User selection of flow keys User definition of flow records	Packet sampling + More selection of flow keys* Packet length | packet section | Sampling rate
Flow Cache	Permanent cache Normal cache Immediate cache	Immediate cache
Exporting Process	NetFlow version 9 or IPFIX	NetFlow version 9 or IPFIX

•NetFlow-lite exports new keys such as raw packet section & sampling rate

NetFlow-lite: Metering Process

Packet forwarding

■ 1-in-N samples (truncated)

■ NetFlow-lite export packet header

■ Other NetFlow-lite export (v9 or IPFIX) fields (sampled packet length, # of sampled packets, total # of packets observed)
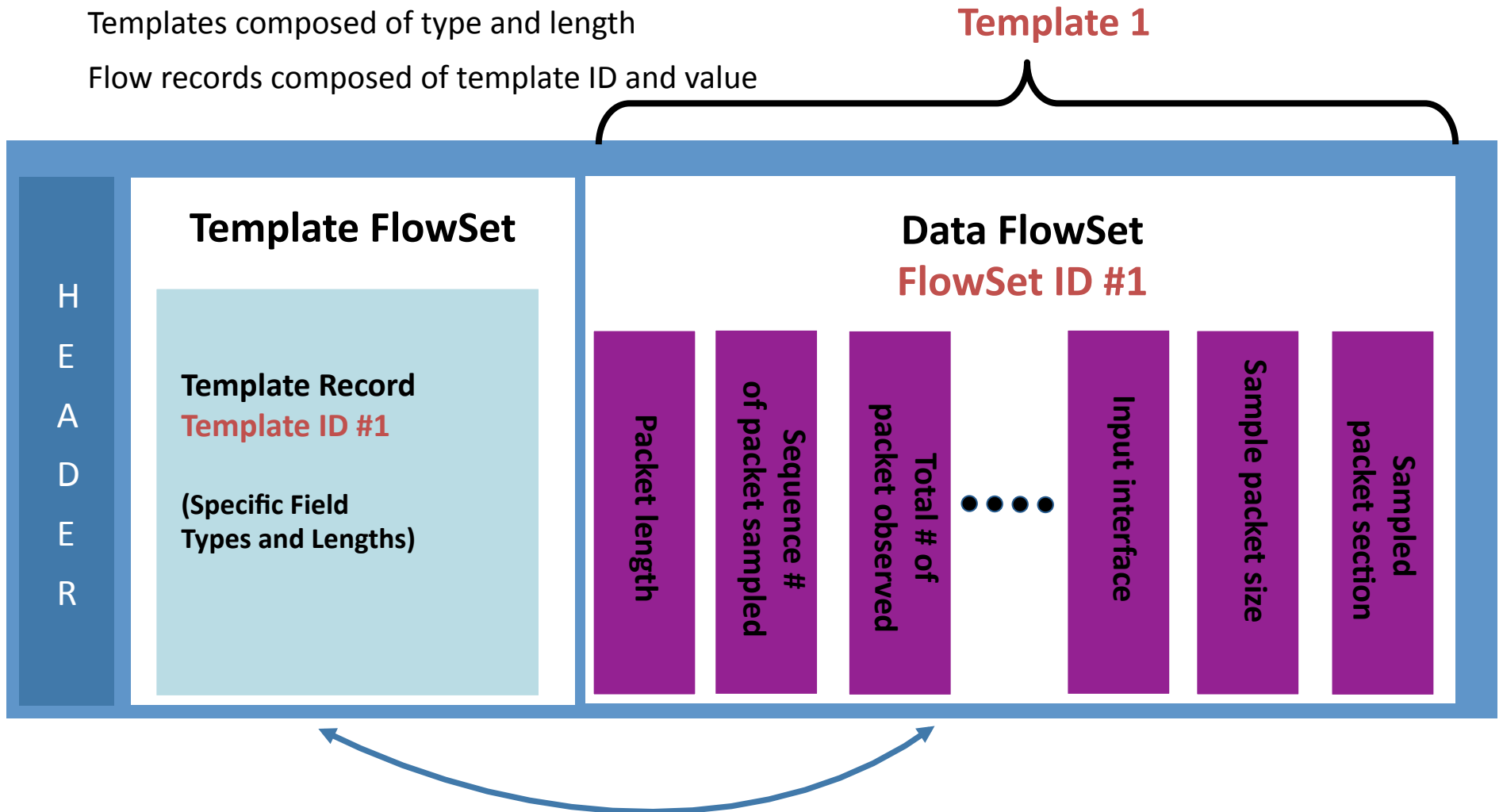
☐ NetFlow-lite export packet

- Configurable sampling rate up to 1-in-32 on all 48 downlinks (1G) ad 4 uplinks (10G), AND 1-in-1 sampling on up to 2 ports (1G only)
- Configurable packet sample length (export truncated packet section to conserve bandwidth)

NetFlow-lite: Export Format

- Example: NetFlow-lite in NetFlow version 9 export Format
- Version 9 is based on template and separate flow records

    Templates composed of type and length

    Flow records composed of template ID and value

Template 1

HEADER

Template FlowSet

Template Record
Template ID #1

(Specific Field Types and Lengths)

Data FlowSet
FlowSet ID #1

Packet length

Sequence # of packet sampled

Total # of packet observed

• • • •

Input interface

Sample packet size

Sampled packet section

NetFlow-lite: Flow Cache

- There are 3 type of flow caches in Flexible NetFlow
    - Normal Cache (traditional NetFlow)
    - Permanent Cache
    - Immediate Cache

- NetFlow-lite uses immediate cache
    - Every packet creates a new flow
    - Good for packet section export in version 9/IPFIX format

- Additional Reference:
  Cisco IOS Flexible NetFlow Technology White Paper (http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/ps6965/prod_white_paper0900aecd804be1cc.html)

NetFlow-lite vs. NetFlow

Catalyst 4500/4900 Switches NetFlow-lite vs NetFlow Support:

	NetFlow-lite (4948E, 4948E-F)	NetFlow (SupIV/V, SupV-10GE, Sup7-E)
Technology	Packet-based	Flow-based
Hardware	FPGA-assist	NetFlow ASIC
Metering Method	Sampling (configurable, up to 1-in-32*)	Every packet accounted for
Export format	v5, v9, IPFIX**	v5, v8, v9, IPFIX
Flow Cache	Immediate Cache	Norman cache/immediate cache/permanent cache
Ecosystem	Easily integrate with any NetFlow collector with NetFlow-lite Aggregator	NetFlow collector
Platform Support	4948E, 4948E-F	SupIV/V (with daughter card) SupV-10GE Sup7-E (Flexible NetFlow)

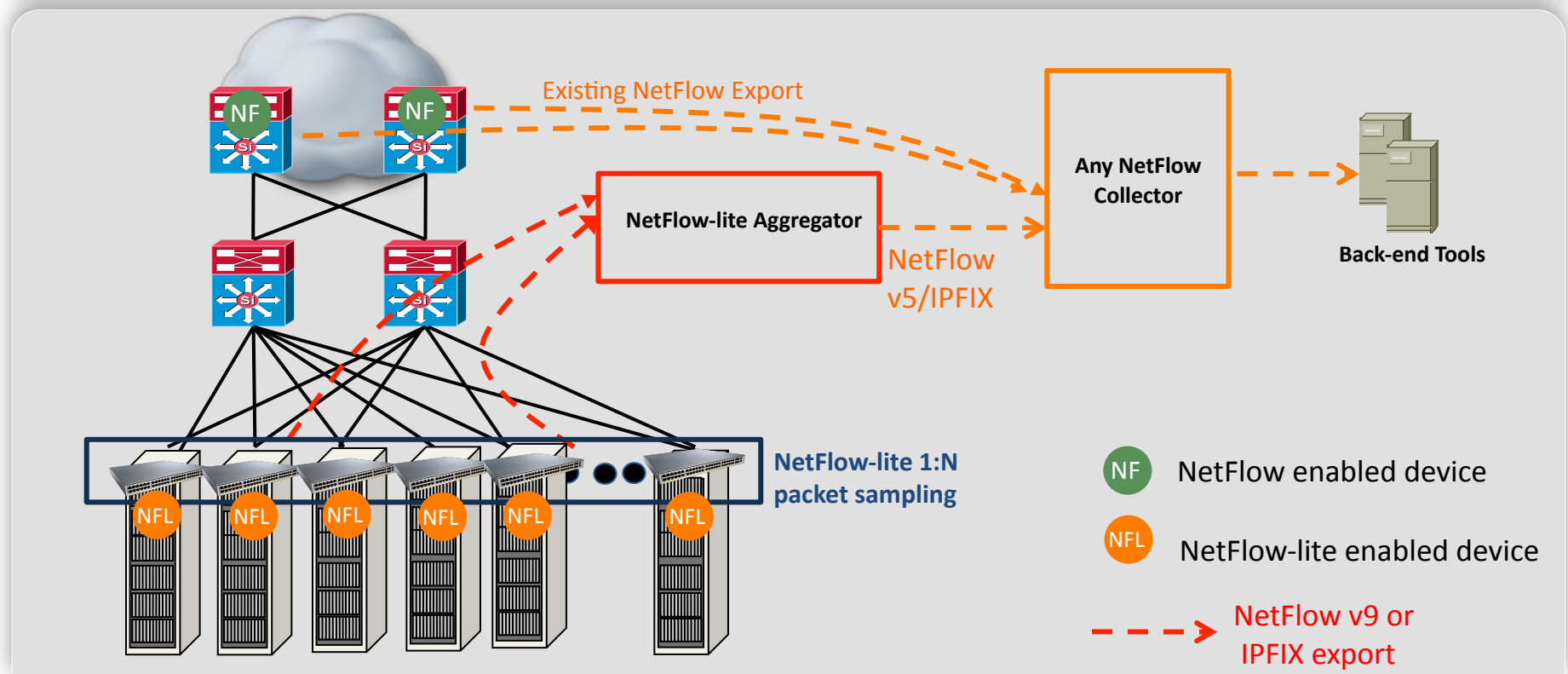* Supports 1-in-1 sampling for up to 2 ports for troubleshooting
**Catalyst 4948E/4948E-F is the first Cisco products supporting IPFIX

Data Center-wide Monitoring

Integrating NetFlow-lite into Your Network

Integrating NetFlow-lite into existing NetFlow architecture is easy:
- Work with existing collectors & back-end tools through NetFlow-lite Aggregators
- NetFlow-lite Aggregators and collectors can sit anywhere in the network, as long as L3 reachable
- NetFlow-lite Aggregators are transparent to NetFlow collector (NetFlow collectors receive aggregated flow data as if it's coming directly from the switch)
- NetFlow collector analyzes & correlates both NetFow and aggregated NetFlow-lite data

Existing NetFlow Export

NetFlow-lite Aggregator

NetFlow v5/IPFIX

Any NetFlow Collector

Back-end Tools

NetFlow-lite 1:N packet sampling

NF — NetFlow enabled device

NFL — NetFlow-lite enabled device

NetFlow v9 or IPFIX export

Why do I Need a NetFlow-lite Aggregator?

NetFlow-lite Aggregator serves the following purposes:

- Parse NetFlow-lite data to extract information such as src/dst IP address, TCP/UDP port, packet length, etc.

- Construct temporary flow cache

- Extrapolate flow statistics by correlating sampling rate w/ sampled packets

- Export aggregated and extrapolated data to NetFlow collectors in standard IPFIX or NetFlow v5/v9 format

- Conserve valuable forwarding bandwidth by aggregating NetFlow-lite data to more bandwidth efficient NetFlow export

NetFlow-lite Aggregator – Using nProbe

What is it?

nProbe is an open source NetFlow collector/ probe/NetFlow-lite Aggregator and can be obtained from ntop.org

How

- nProbe can run on any linux server by issuing the following command:

```
# ./nprobe -i eth2 -b 1 -s 5 -t 60 -w 1000000
--nflite 2055:16 -n 5.5.5.10:2055 -O 2 -e 0
```

NetFlow-lite aggregator (nProbe)

Any NetFlow Collector

5.5.5.10:5000

The command Indicates that nProbe will be collecting NetFlow-lite info over eth2, on port 2055~2070, extract & aggregate info using 1MB of cache size, flow expiration time is 60 seconds, into NetFlow v5/v9/IPFIX format, send to NetFlow collector located at 5.5.5.10, port 2055, whether on the same server or other L3 reachable servers/appliances

NetFlow v9 or IPFIX export
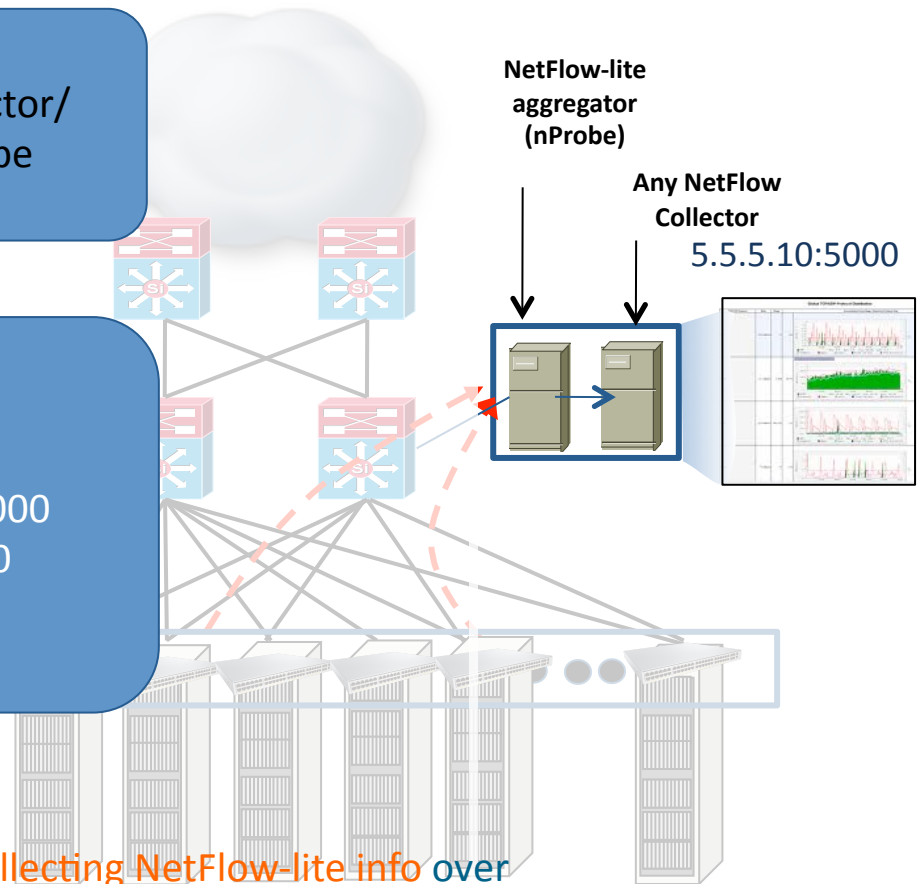
# Designing NetFlow-lite in Large-scale DC

A Tiered Approach
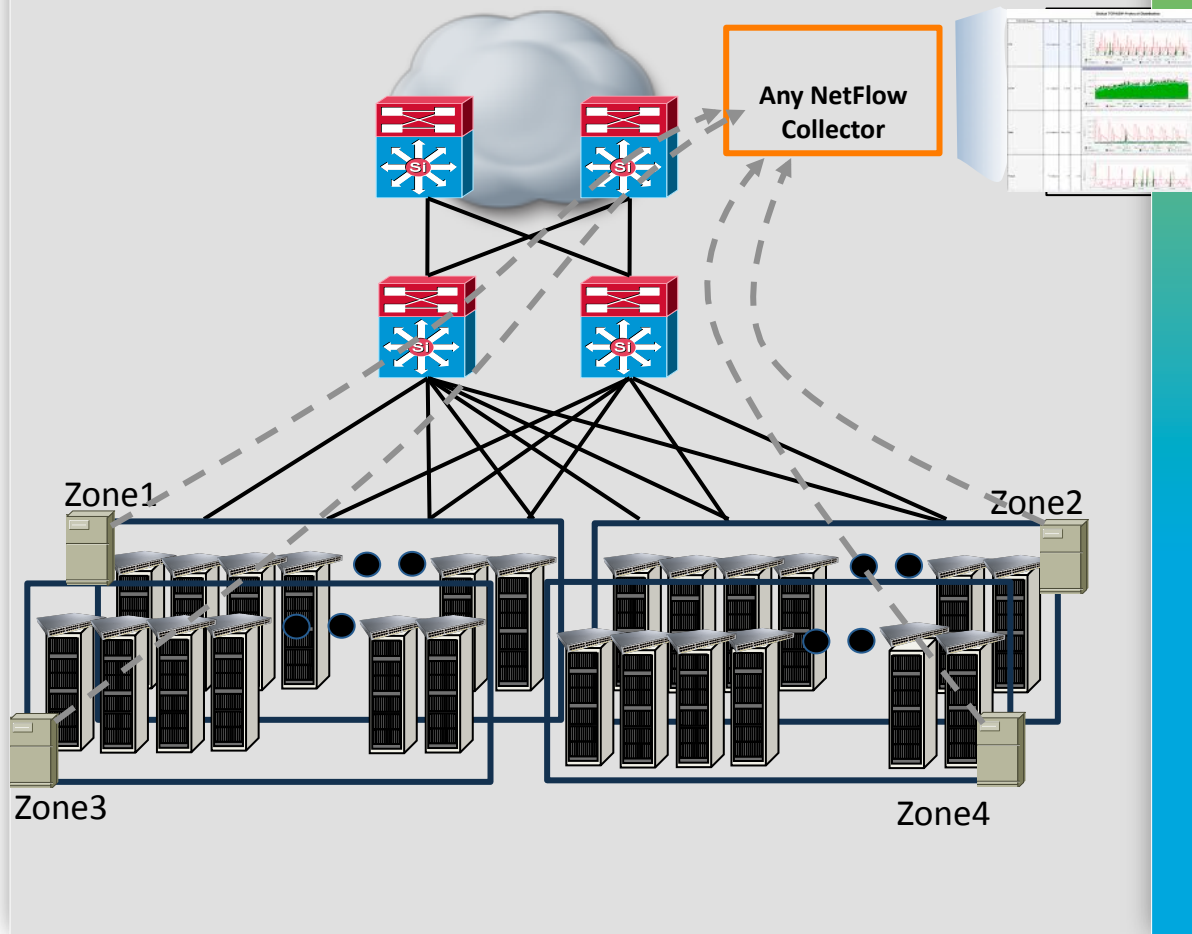
- Deploy an nProbe per zone to scale

  - NetFlow-lite data aggregated per zone to conserve bandwidth usage in data center core/distribution

  - Recommended to deploy nProbe as close to the switches as possible

- How many switches can be in a zone?

  - Depending on the sampling rate, link utilization, # of flows, the horsepower of server running nProbe

Use Case Example:

Network Visibility with NetFlow-lite

Screenshot taken from Plixer Scrutinizer
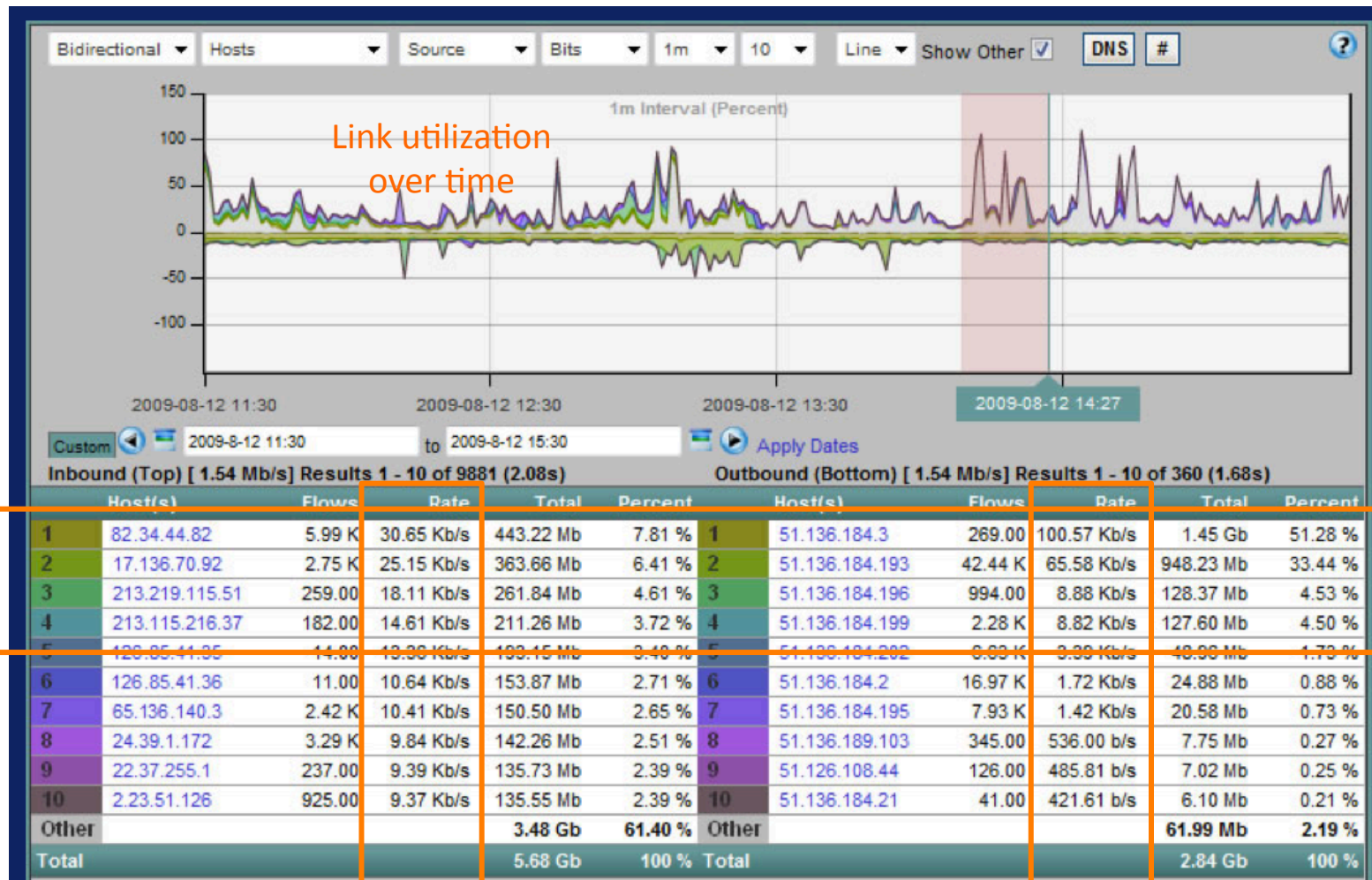
NetFlow-lite Configuration

netflow-lite exporter check
transport udp 2055
 transport udp load-share 16
 template data timeout 60
 options sampler-table timeout 60
 source 9.9.9.10
 destination 9.9.9.1
 export-protocol ipfix
!

netflow-lite sampler check
 packet-rate 32
 packet-section size 64
 packet-offset 0
!

interface GigabitEthernet1/1
 no switchport
 ip address 40.40.40.1 255.255.255.0
 netflow-lite monitor 1
  sampler check
  exporter check

Configure exporter setting

Configure sampler setting

Apply sampler and exporter to
Netflow-lite monitor on the
interface

NetFlow-lite to
NetFlow
Converter

Any NetFlow
Collector
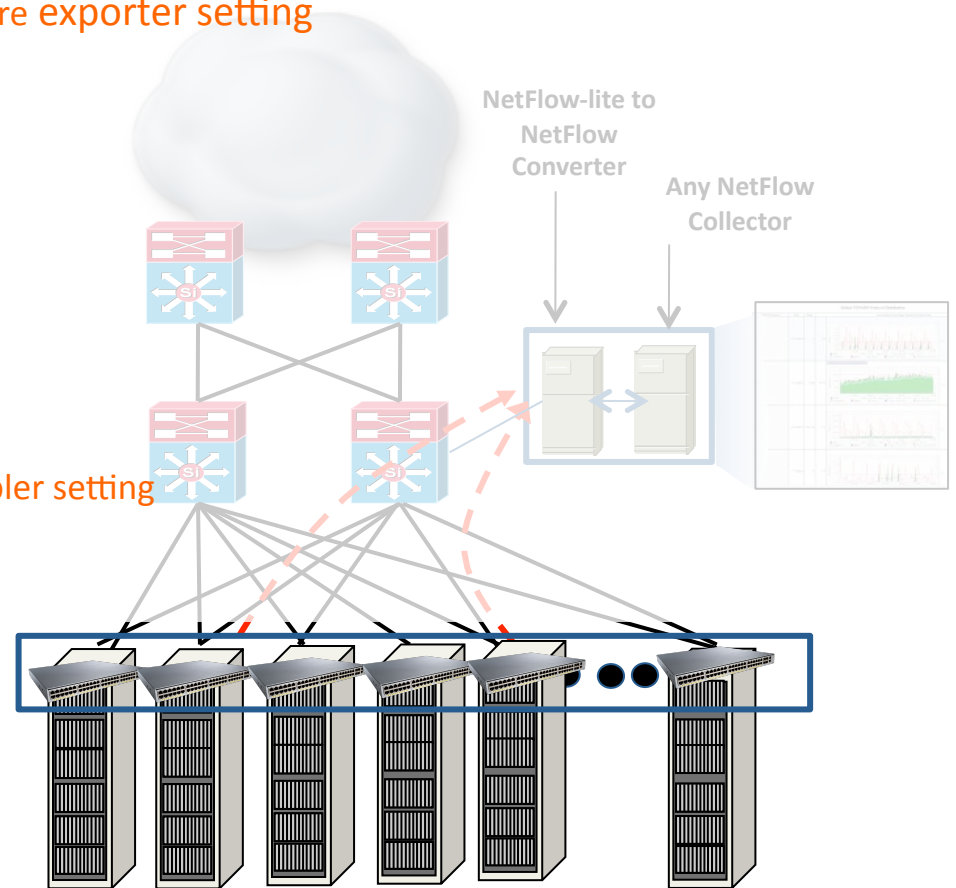
NetFlow v9 or
IPFIX export

Other Resources

- Catalyst 4948E NetFlow-lite configuration guide
  - http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/15.02SG/configuration/guide/nswich_l.html
- Ntop.org
  - http://www.ntop.org/nProbe.html
- Flexible NetFlow Technology White Paper
  - http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/ps6965/prod_white_paper0900aecd804be1cc.html