

# NetFlow and Flexible NetFlow

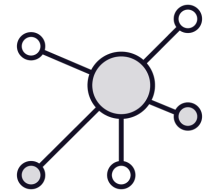


**Stephen Wenn**

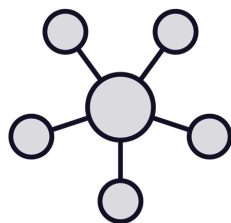
Network Engineer



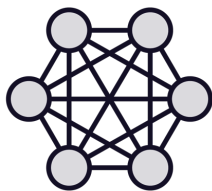
# Cisco NetFlow History



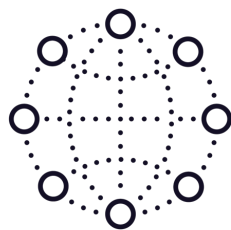
**NetFlow v1: Basic IP traffic monitoring, limited features, no support for IPv6 or MPLS. Early 1990s. (Obsolete)**



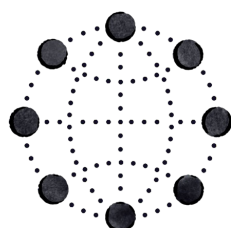
**NetFlow v5: Widely used, 20-field records, scalable, lacks IPv6 and MPLS support. Mid 1990s.**



**NetFlow v8: Aggregates flow records, reducing data export overhead, efficient for large networks. Early 2000s. (Obsolete)**



**NetFlow v9: Template-based, supports IPv6, MPLS, and BGP; highly extensible and flexible. Mid 2000s.**



**Flexible NetFlow: Fully customizable, advanced monitoring for modern traffic types, highly flexible. Derived from NetFlow v9. 2010s.**



# What is Flexible NetFlow (Part 1)?

Advanced network monitoring developed by Cisco

Define custom flow records using a template-based system

Enables the collection of specific traffic data based on network needs



# What is Flexible NetFlow (Part 2)?

Support for IPv4,  
IPv6, MPLS, VLANs  
and much more

Real-time monitoring  
by exporting  
collected flow data  
to a flow collector

Highly flexible;  
perfect for both  
small and large  
networks



# Flexible NetFlow Building Blocks



# Flexible NetFlow Building Blocks



Flow Record



# Flexible NetFlow Building Blocks



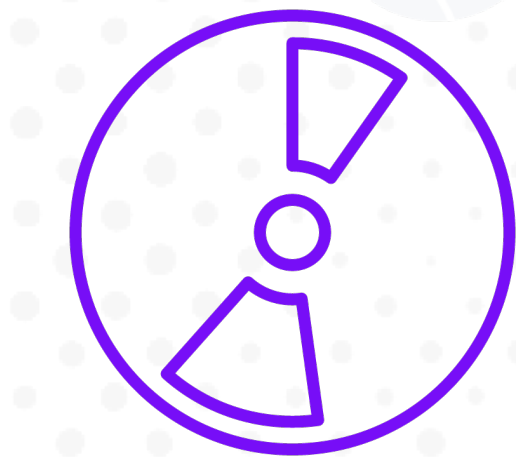
Flow Record



Flow Monitor

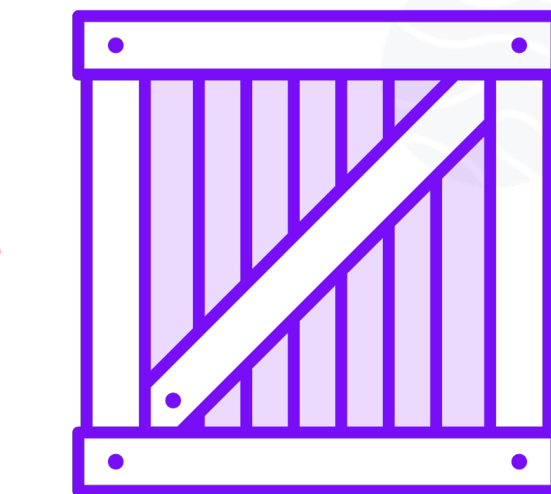


# Flexible NetFlow Building Blocks

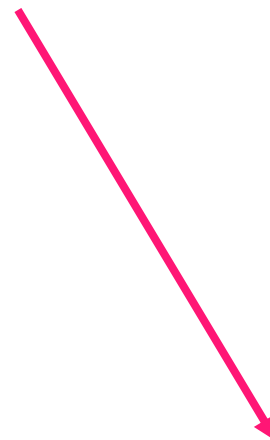


Flow Record

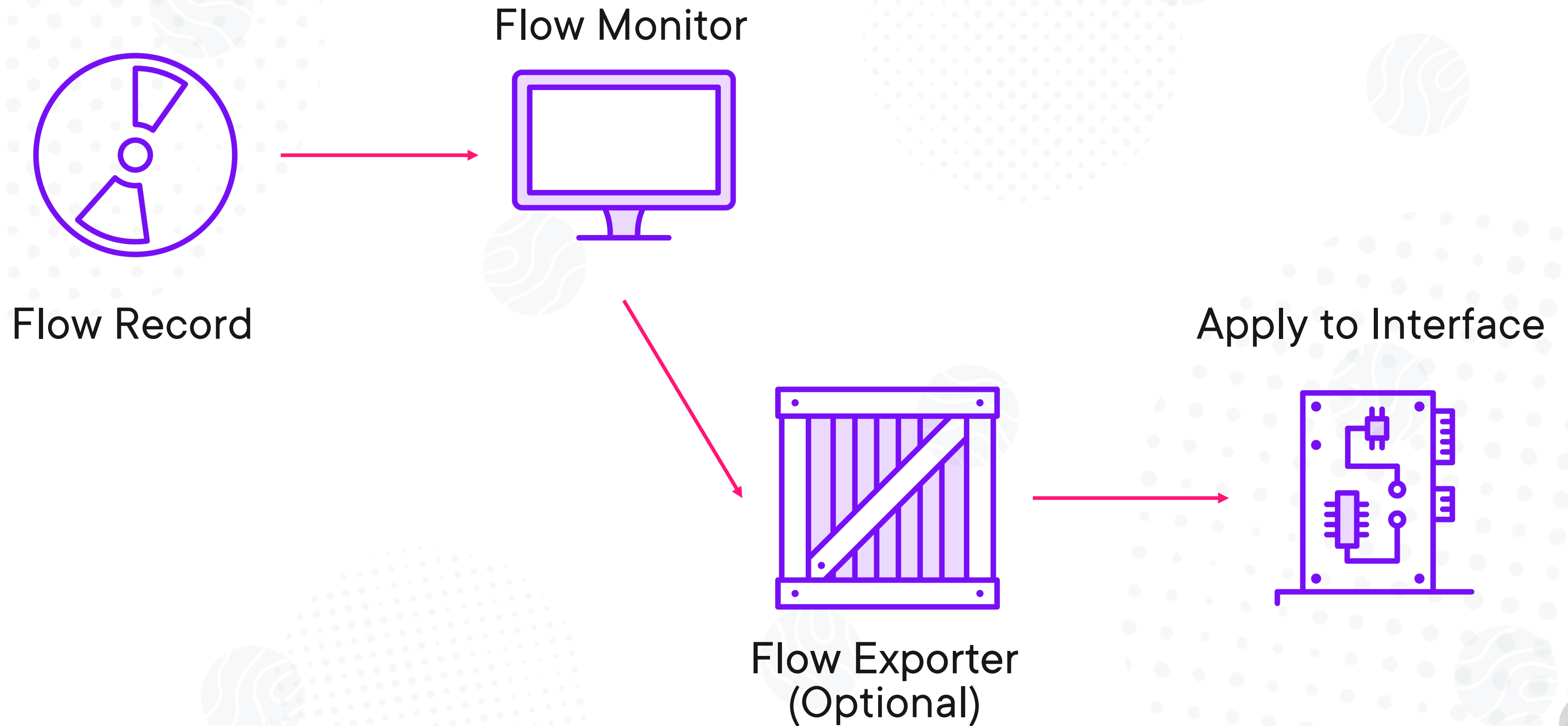
Flow Monitor



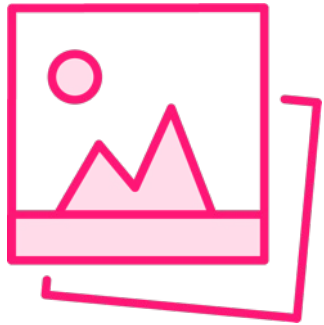
Flow Exporter  
(Optional)



# Flexible NetFlow Building Blocks



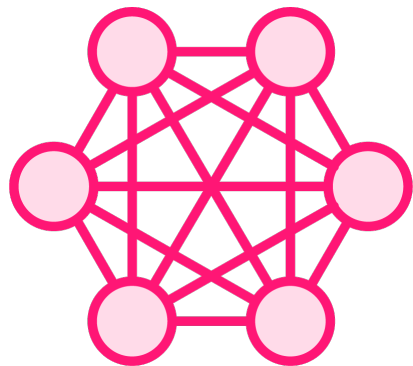
# What Is Network Based Application Recognition (NBAR)?



A Cisco DPI technology that classifies applications by Layer 7 protocol signatures.



Primarily identifies and manages application traffic on networks, enabling devices to detect applications beyond port or protocol.



Enhances NetFlow by improving application visibility, supporting QoS, and optimizing bandwidth.



# Key Features of NBAR



**Detects applications by protocol signatures rather than ports, allowing more accurate identification.**



**Supports a broad range of applications, including HTTP, VoIP, P2P, and custom apps.**



**Regularly updated by Cisco to recognize new applications.**



**Enables QoS policies by application type, prioritizing critical traffic like VoIP and video.**



**NBAR2: The latest version analyzes SSL/TLS metadata to identify applications, even with encrypted payloads.**



# NBAR and NetFlow



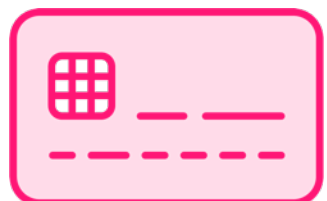
**NetFlow captures flow data, while NBAR adds application-layer visibility for deeper traffic insights.**



**NBAR enriches NetFlow records with application-level data.**



**Helps admins identify bandwidth-consuming apps (e.g., streaming) and apply policies.**



**Without NBAR, Netflix traffic appears as HTTP/HTTPS; with NBAR, it's recognized as Netflix, allowing better management.**



# Configuring and Verifying Detected Applications with NBAR2

```
interface GigabitEthernet1
 ip nbar protocol-discovery
```

```
show ip nbar protocol-discovery
```

	Input	Output
	-----	-----
Protocol	Packet Count	Packet Count
	Byte Count	Byte Count
-----	-----	-----
ping	57	57
	4446	4446
	0	0

