

Cisco IOS NetFlow 101

Chris Smithee
Senior Systems Engineer

Quote from the Yankee Group:

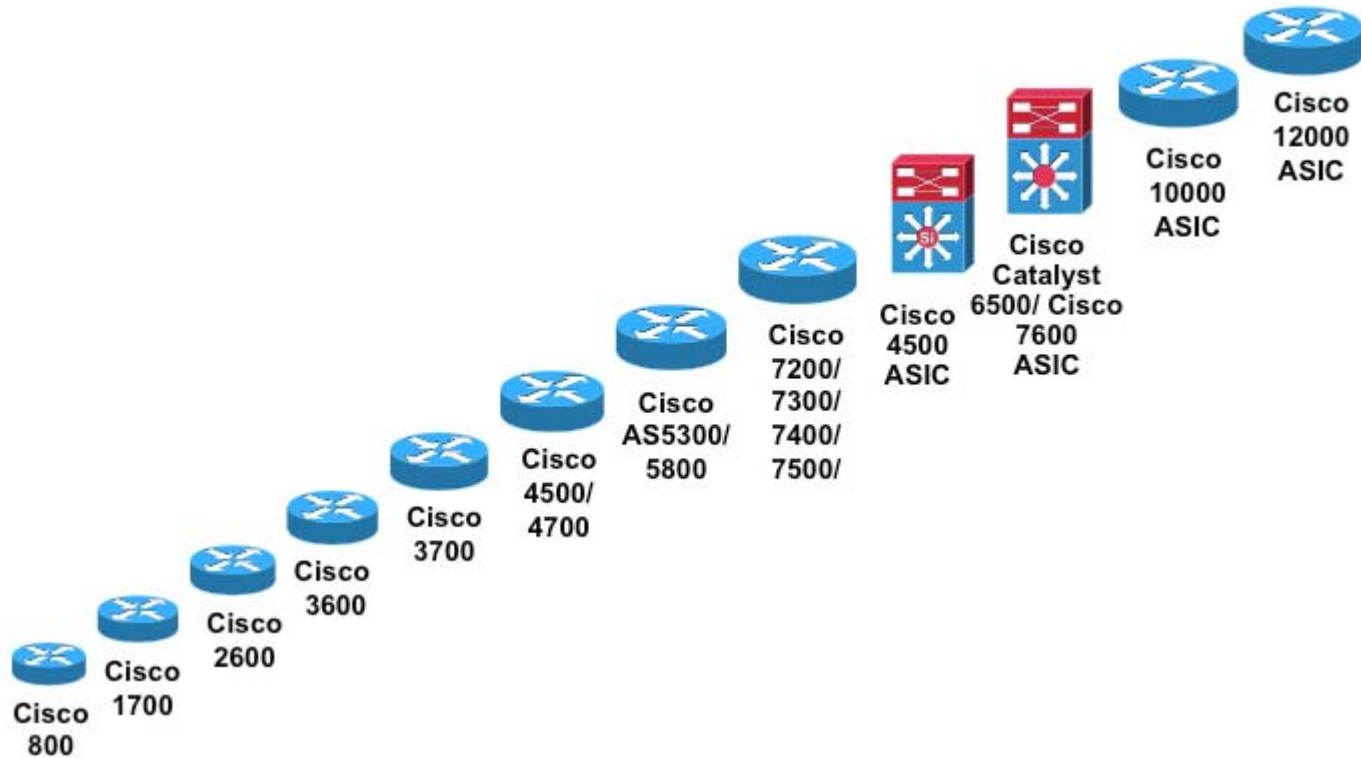
“Network and security administrators have already discovered the value that behavioral analysis has beyond security threat detection. Behavioral analysis provides visibility into all the network activity to optimize the end-user experience, understand and monitor for meaningful change, troubleshoot performance issues faster, and deliver value to both network and security operations.”

- George Hamilton, Yankee Group

A little background...

- NetFlow was developed at Cisco in 1996
- NetFlow is built into most Cisco routers and layer 3 switches
- In 2003 NetFlow Version 9 was chosen for a proposed IETF standard called IP Flow Information Export (IPFIX).
- IPFIX defines the format by which IP flow information can be transferred from an exporter, such as a Cisco router, to a collector application that analyzes the data.
- NetFlow is a form of telemetry pushed from routers and Layer 3 switches

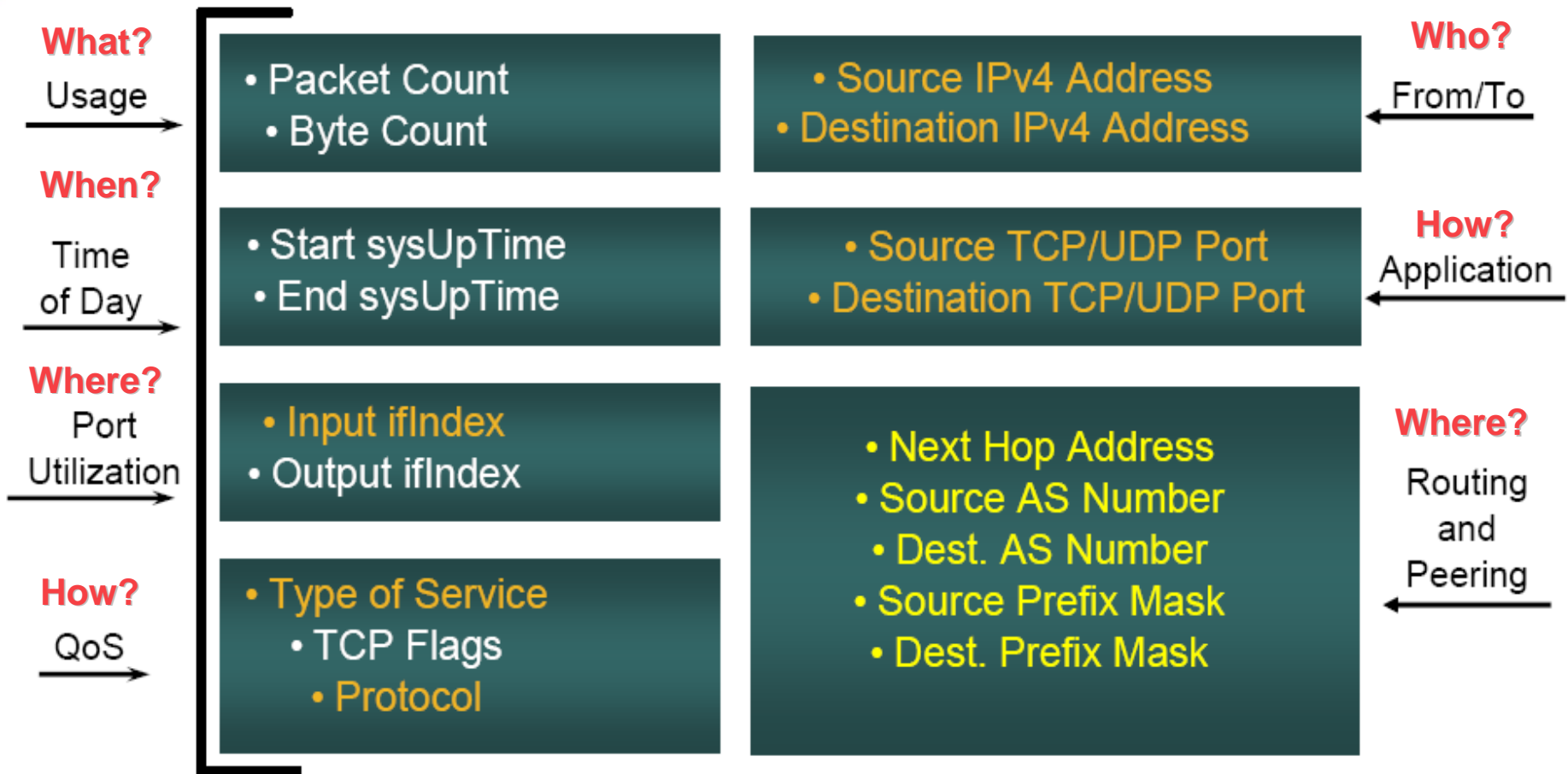
NETFLOW SUPPORT AND AVAILABILITY



The ability to characterize IP traffic and account for how and where it flows is critical for network availability and performance

- Monitoring IP traffic flow facilitates more accurate capacity planning
- Ensure resources are used appropriately in support of business goals
- Helps determine where to apply quality of service (QoS) so that vital traffic receives priority.
- Network security by continuously monitoring traffic to detect undesirable network traffic

NetFlow Version 5 Field Types



NetFlow provides the data to answer the Questions:

Who? What? When? Where? and How?

Common Applications for NetFlow

Service Provider

Network Infrastructure Optimization
and Planning

Peering Arrangements

Traffic Engineering

Policy Enforcement

Security Monitoring and Incident
(DDoS) Detection

Enterprise

Internet Access Monitoring

User Monitoring/Profiling

Application Monitoring

Policy Enforcement

Security Monitoring and Incident
(DDoS) Detection

Provides for Network *and* Security Operations

Lancope[®]

Optimizing Security and Network Operations[™]

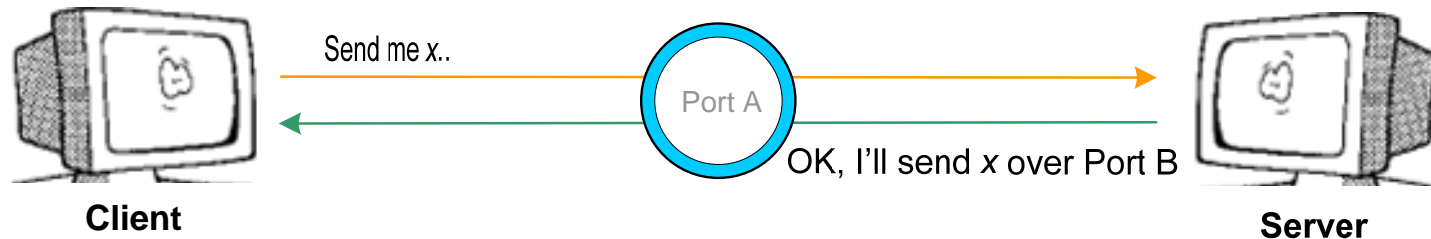
NetFlow Benefits

- Provides end-to-end Visibility into all Host Communications
 - Host-to-Host, User-to-Application, User/Host-to-Internet
- Allows for complete Behavioral Analysis of the Network
 - Hosts, Applications, and Infrastructure
 - Establish Baselines, Profiles and Thresholds
- Capabilities on 10Gig+ Networks
- Rich Dataset for Real-time or Forensic Analysis
 - Network/Interface Utilization
 - Trending and Capacity Planning

What is a flow?

- Flow

- A “conversation” between two hosts that consists of a client, a server, and a service port



What is NetFlow?

google.com

10.1.1.1

router

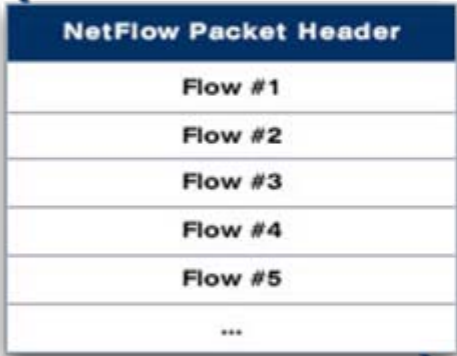


Start Time	Interface	Src IP	Src Port	Dest IP	Dest Port	Proto	Pkts Sent	Bytes Sent	TCP Flags
10:20:12.221	eth0/1	10.1.1.1	1024	google.com	80	TCP	5	1029	SYN, ACK, PSH
10:20:12.871	eth0/2	google.com	80	10.1.1.1	1024	TCP	17	28712	SYN, ACK, FIN

Lancopé[®]

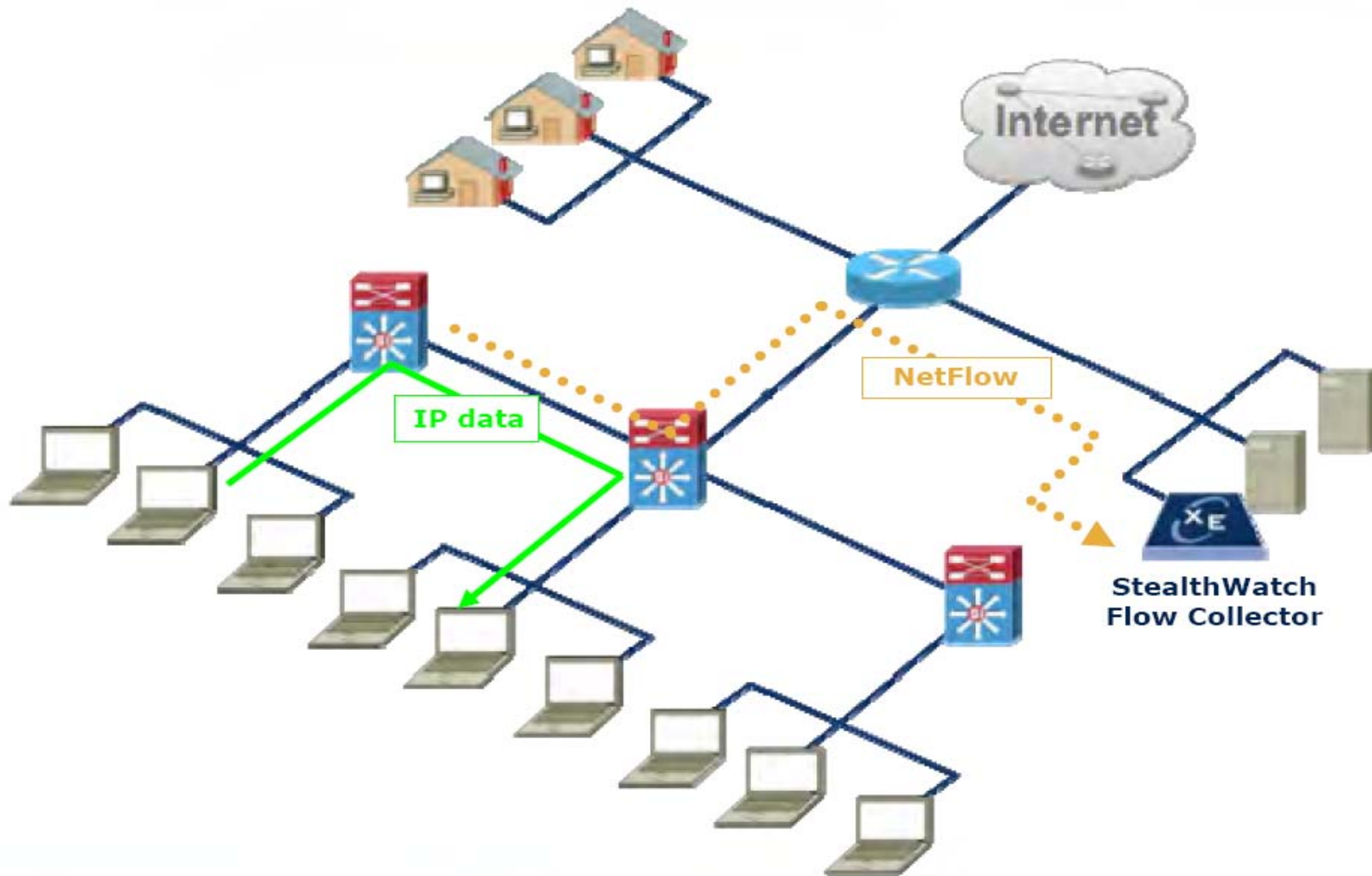
Optimizing Security and Network Operations[™]

NetFlow Export



NetFlow Collector

NetFlow Data Export (NDE)



Netflow, why use it?

- Easy to deploy
 - Taking once multiple sensors down to a single collector
- Cost effective
 - 1 collector vs numerous → *Network constantly changing grow / consolidate*

(EXAMPLE CONFIG)

Business Value: Reduce...

man hours, on-the-fly changes for sniffing, hardware cost, and maintenance thus save money and reduce network down time

Netflow optimal configuration for Flow monitoring

```
ip flow-export destination <netflow collector IP> 2055
```

```
ip flow-export source loopback 0
```

```
ip flow-export version 9
```

```
ip flow-cache timeout active 1
```

```
ip flow-cache timeout inactive 15
```

```
snmp-server ifindex persist
```

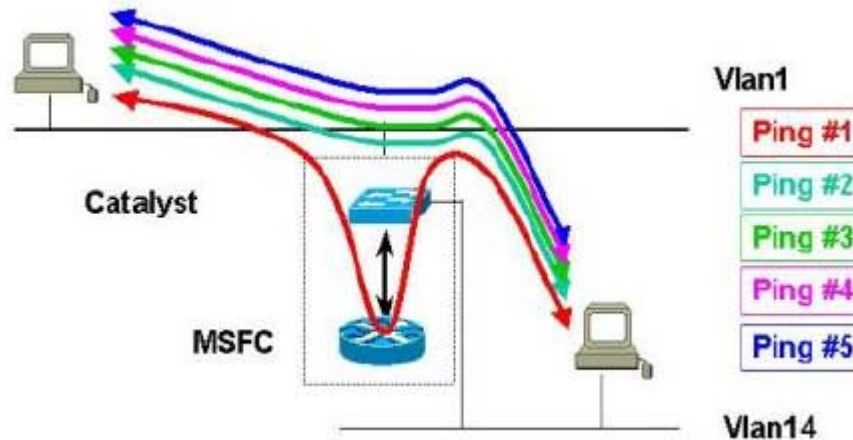
Enable Netflow on all interfaces you are interested in recording traffic on, either physical interface or logical interface (typically logical on Catalyst switches):

```
interface <interface>
```

```
ip flow ingress (newer command) or ip route-cache flow
```

NetFlow Accounting with MLS on Catalyst 6500/7600

In practical terms, if five pings are sent from host1 in VLAN1 to host14 in VLAN14, only the first one is routed through the MSFC. The four remaining are switched on the Supervisor. The five pings are considered a single flow because the characteristics (such as source address, destination address, and source port) of the packets does not change.



In a more general statement, only the first packet of a flow reaches the MSFC, while all subsequent packet of the same flow are switched locally on the Supervisor.

Netflow Data Engine (NDE) on Native IOS Catalyst 6500 Native Mode

In configuration mode on the Supervisor Engine, follow the instructions for an IOS device above, and then issue the following to enable NDE:

```
mls nde sender version 7
```

```
mls aging long 64
```

```
mls aging normal 32
```

```
mls nde interface
```

```
mls flow ip interface-full
```

```
ip flow ingress layer2-switched vlan {vlanlist}
```

```
ip flow export layer2-switched vlan {vlanlist}
```

Enables NDE for all traffic within the specified VLANs rather than just inter-VLAN traffic.

Netflow in Action: Business Challenge *Compliance*

- Compliance – SOX, PCI, HIPPA, etc
 - Lack of visibility into behaviors across the network
 - User accountability for employees, partners, consultants, customers

NetFlow Solutions supply organizations with the means to:

- Continuously but passively monitoring host behaviors looking for deviations from normal processes
- Tie individual users to internal network performance problems
- Tie individual users to the introduction of security risks inside the internal network
- Implement appropriate Network Controls and Policies
- Provide for Internal Audit and Risk Assessment

Netflow in Action: Business Challenge *Compliance*

- Michelle Stewart, Manager of Data Security, AirTran Airways

“During testing, StealthWatch demonstrated the ability to detect unauthorized remote access, worm activity and root cause analysis of increases in WAN activity. All of these functions have aided our efforts to demonstrate compliance with the PCI Data Security Standard.”

http://www.loveyourtool.com/blog/2008/05/airtran_lancope.html

Netflow in Action: Business Challenge *Lack of Internal Security*

- Lack of Internal security
 - Gaps left by traditional security technologies
 - High-speed, highly segmented networks
- Anomaly Detection: Quickly pinpoint zero-day and unknown threats that bypass perimeter security
- Identify policy violations, unauthorized activity/applications, misconfigured hosts, and other rogue devices
- Faster Incident Resolution & detailed Forensic data
- Detection of DoS/DDoS attacks, Worms, Viruses and Botnets
- Track and Audit network behavior and access by Individual Hosts

Example: RinBot missed by signature. Only picking up where tapped in.

Netflow in Action: Security Operations

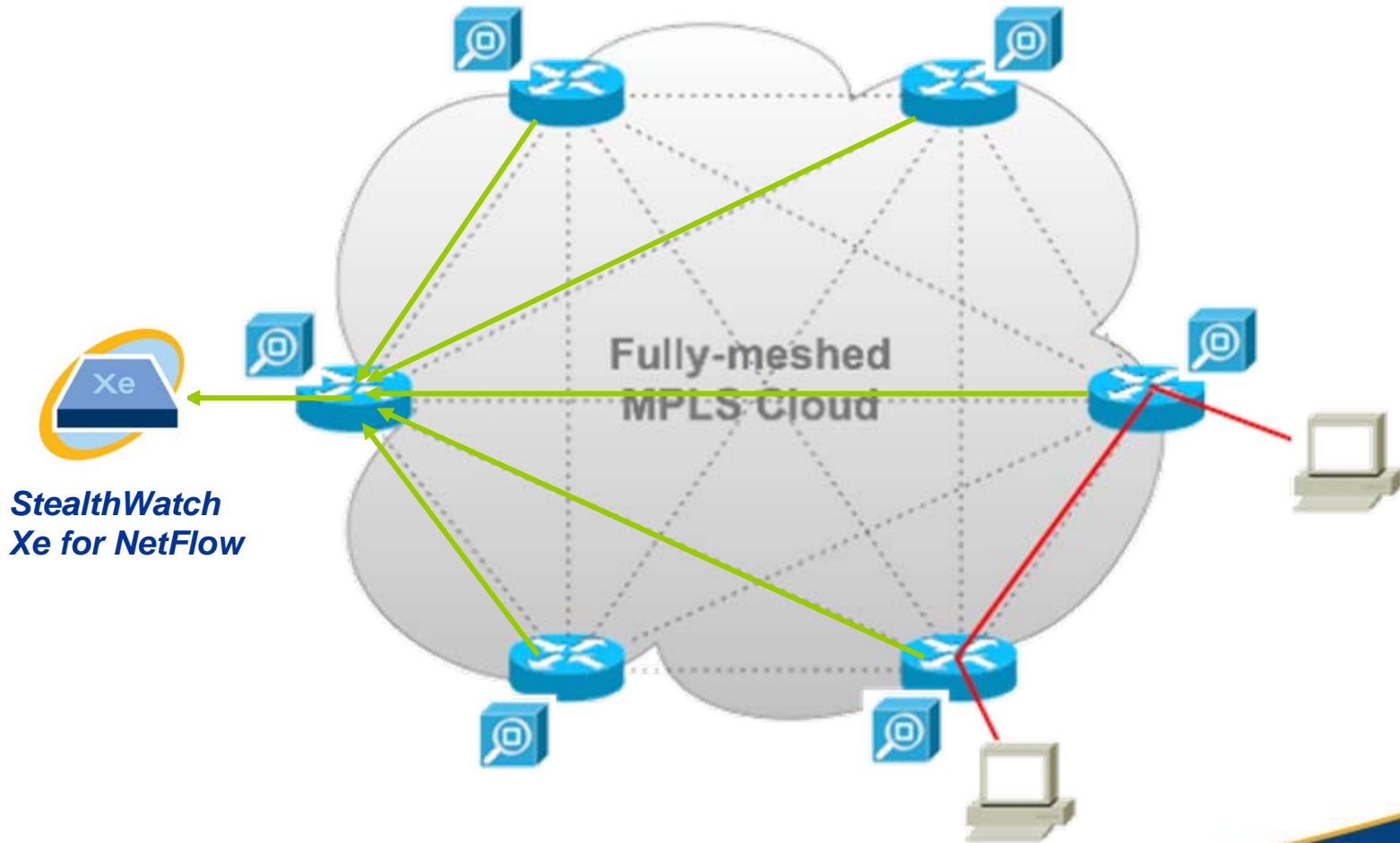
- Todd Ferris: Stanford University's School of Medicine

“We were quickly able to get [bot-infected] machines off the network that had been sitting there and scanning for months,”

http://www.darkreading.com/document.asp?doc_id=155191&WT.svl=news2_1

Netflow in Action: Managing changing networks MPLS Networks

Traditional probe-based approaches require many hardware installations and are often reactive in nature...



Lancope™

Optimizing Security and Network Operations™

Netflow in Action: Network Operations

- Fully integrated view of network usage, performance, host integrity and user behavior
- Diagnose Network congestion and provide root cause analysis of the problem causing response time delays
- Visibility and Metrics for WAN Optimization
- Real-time and Historical data to facilitate network performance monitoring, capacity planning and resource management
- Monitor Quality of Service on a per-hop basis throughout the Network

Netflow in Action: Network Operations

- Eric Michael, manager of IS Infrastructure for Gibraltar Industries

“StealthWatch not only provides basic details about the ‘who, what, when and where’ of network traffic, but it also enables us to focus on the all-important ‘why’ behind many network problems. Our team’s productivity has increased significantly because we now have time to focus on other projects instead of spending hours manually diagnosing network-related traffic problems.”

<http://www.lancope.com/news/05122008.aspx>

Lancope™

Optimizing Security and Network Operations™

NetFlow in Action : Network Visibility

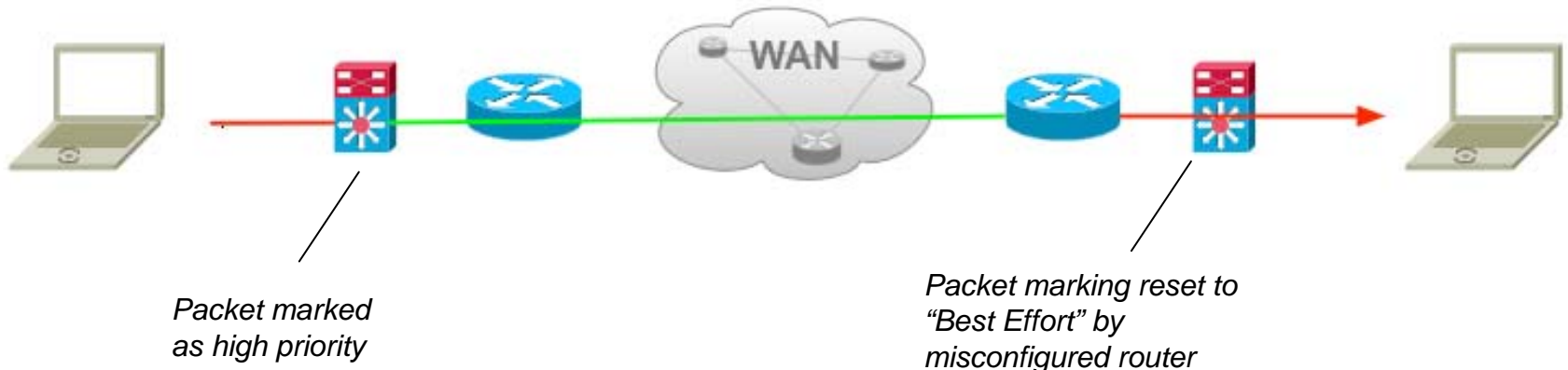
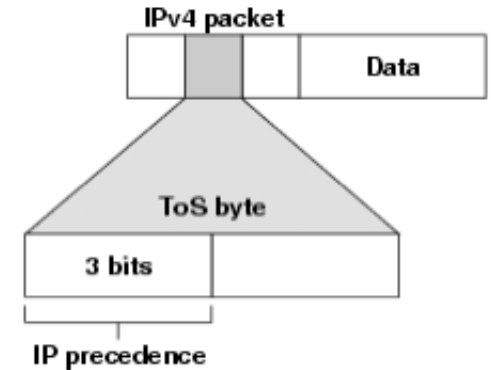
- Supply real-time visibility and awareness of network and host-based behaviors
- Track, measure and prioritize network and host-based risk
- Monitor and investigate individual host and broad network communications
- Maintain network availability, integrity and performance of crucial business processes
- Discover and inventory the underlying assets of the corporate network

NetFlow in Action : Security Operations

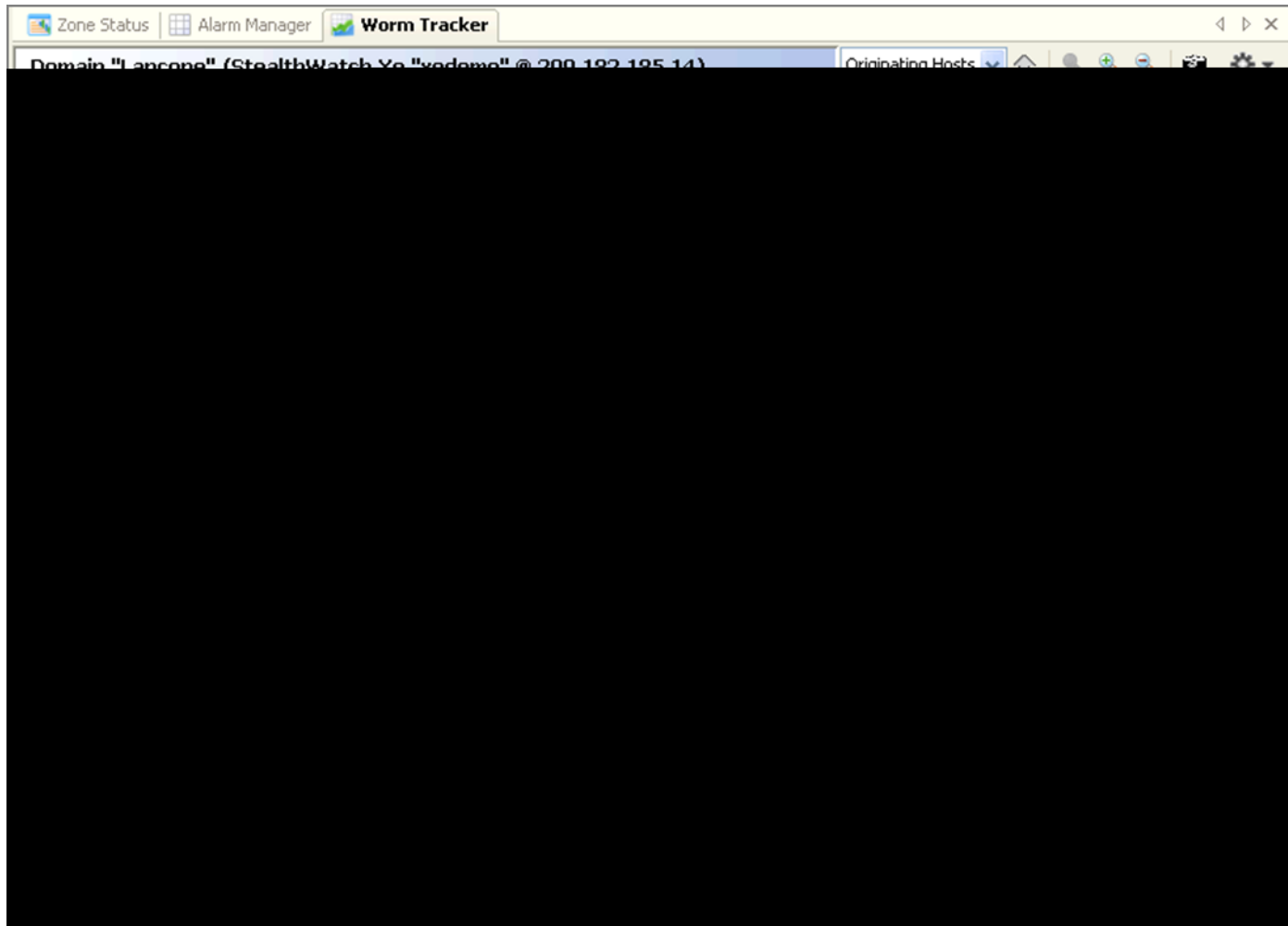
- Anomaly Detection: Quickly pinpoint zero-day and unknown threats that bypass perimeter security
- Identify policy violations, unauthorized activity/applications, misconfigured hosts, and other rogue devices
- Faster Incident Resolution & detailed Forensic data
- Detection of DoS/DDoS attacks, Worms, Viruses and Botnets
- Track and Audit network behavior and access by Individual Hosts

QoS Per-Hop-Behavior Monitoring and Reporting

- DSCP (Differentiated Services Code Point)
- Uses ToS byte in the IP header
- Backwards compatible with older ToS/IP Precedence solution
- 64 different classifications
- A packet's per-hop behavior and classification can change as the packet moves through the network



NetFlow in Action : Flow Visualization



Visualization of a Worm Outbreak

Lancope™

Optimizing Security and Network Operations™

- Inherent Network and Security Data
- Provides Visibility into behaviors across the Network
- Traffic/Application monitoring and Problem diagnosis
- Restores visibility in WAN Optimized network environments
- Applications for Security and Compliance
- Scalable monitoring of QoS and MPLS environments

Can you give the CIO the Facts ?

- **What impact did this have on the corporation?**
- **Was customer data compromised?**
- **How did this happen?**
- **When did you first detect the problem?**
- **Were network services impacted?**
- **What users were impacted?**
- **How long was this occurring?**
- **Do we have proper controls in place to guard against this?**

NetFlow Can....

Lancope™

Optimizing Security and Network Operations™

Questions?

Questions?

Lancope™

Optimizing Security and Network Operations™