



CRANNOG SOFTWARE



# Utilizing NetFlow

## for

# Detailed Network Traffic Visibility



CRANNOG SOFTWARE

## Agenda



- Introduction to NetFlow – the Hidden Gem in Cisco IOS
  - NetFlow Past, Present, Future
  - NetFlow in Network Management – Usage and Reporting
- Turning NetFlow “Data” into Information
  - Enabling NetFlow on Devices
  - NetFlow Data Collection
  - NetFlow Scalability/Performance
  - Real-Time Traffic Investigation
  - Network Forensics
  - Detailed Reporting
- Demonstration
- User Experiences
- Questions



CRANNOG SOFTWARE

## Crannog Software



- Founded 1998 HQ Dublin, Ireland
- CTO was the first CCIE in Ireland – Career in Network Management
- Crannog Founders started LAN Communications
  - Became the largest Gold Reseller in Ireland
  - LANCOMM created and ran NOC/MSP business
  - Purchased By Eircom, Ireland's Telephone Company

**CISCO SYSTEMS**



Technology  
Developer  
Partner

**About Crannog:** “simple yet effective point solutions that have outpaced all our larger NMS products in both usage and effectiveness.”

**From Network World - Reader's Choice, Network Management**



CRANNOG SOFTWARE

## NetFlow – Past, Present, Future...



Cisco IOS® NetFlow technology is an integral part of Cisco IOS Software (mature, since 1996) that collects and measures data as it enters specific routers or switch interfaces. NetFlow provides input for performance, security, billing and accounting applications.

- Past
  - Overhead on devices/network
  - Treacherous to turn “data” into information (collection/presentation)
- Present
  - Improved memory management
  - V5, V7(Catalyst), V9 (“templates”), Almost all Routers and CAT 45XX, 55XX, 6XXX.
  - Availability of NetFlow Analysis Tools
  - Emerging Industry Adoption – Peribit, Juniper (J-flow), Enterasys, Alcatel...
  - Network World/EMA
- Future
  - IPFIX (IP Flow Information Export) V9 Chosen as basis for IPFIX by IETF (Internet Engineering Task Force)
  - Increased vendor adoption
  - Continued improvement in tools

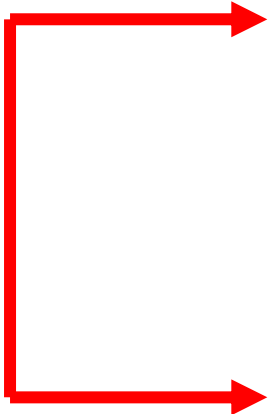


CRANNOG SOFTWARE

# LEVELS OF NETWORK MANAGEMENT



N  
E  
T  
F  
L  
O  
W



SECURITY

RESPONSE

USAGE

UTILISATION

STATUS

EVENTS

IP/SLA (SAA)

SYSTEM /APP  
MANAGEMENT

QOS

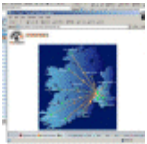
Visualisation  
URL Portal

SEARCH



ELEMENT  
MANAGEMENT

TROUBLE  
TICKETING





CRANNOG SOFTWARE

## NetFlow: The Power of Usage Information



- **Network Forensics**
  - Who is doing what, where, when, with what applications and using how much bandwidth (or who did what, when....)
- **Troubleshooting**
  - Visibility beyond utilization numbers
  - Who and what is causing a problem
- **Spot Security Threats**
  - Suspicious behavior
  - Packets/Origination/Destination
- **Detailed Reporting**
  - Database of Network Traffic/Transactions
- **Other**
  - Anomaly Detection



CRANNOG SOFTWARE

## Advantages of a NetFlow Implementation



- NetFlow in Cisco IOS
- Window Based Server Application (Linux, Solaris...)
- No Probes
- No Appliances
- Non Intrusive (Traffic Described v. NetFlow Traffic)
- Scaleable – Ease of Deployment
- No Formal Training – Intuitive
  
- Real-time visibility AND Archive/Reporting



CRANNOG SOFTWARE

## Turning NetFlow "Data" into Information



- Key Elements
  - Enable NetFlow on key/core devices
  - Collect NetFlow Data
  - Store NetFlow Data - DataBase
  - Present Useful Information



CRANNOG SOFTWARE

## Enabling NetFlow on Devices



### Configuration:-

```
ip flow-export destination 10.1.1.1 2055
ip flow-export version 5
ip flow-export source loopback 0
ip flow-cache timeout active 1
                    (mins)
ip flow-cache timeout inactive 30 (secs)
int type interface number
ip route-cache flow      (Put on all
WAN and LAN interfaces)
```

### Diagnostic:-

```
Show ip flow export
Show ip cache flow verbose
```



**netflow**tracker

### Configuration:-

**ip flow-export destination 10.1.1.1 2055**

**ip flow-export version 5**

**ip flow-export source loopback 0**

**ip flow-cache timeout active 1**

**(mins)**

**ip flow-cache timeout inactive 30 (secs)**

**int *type interface number***

**ip route-cache flow (Put on all  
WAN and LAN interfaces)**

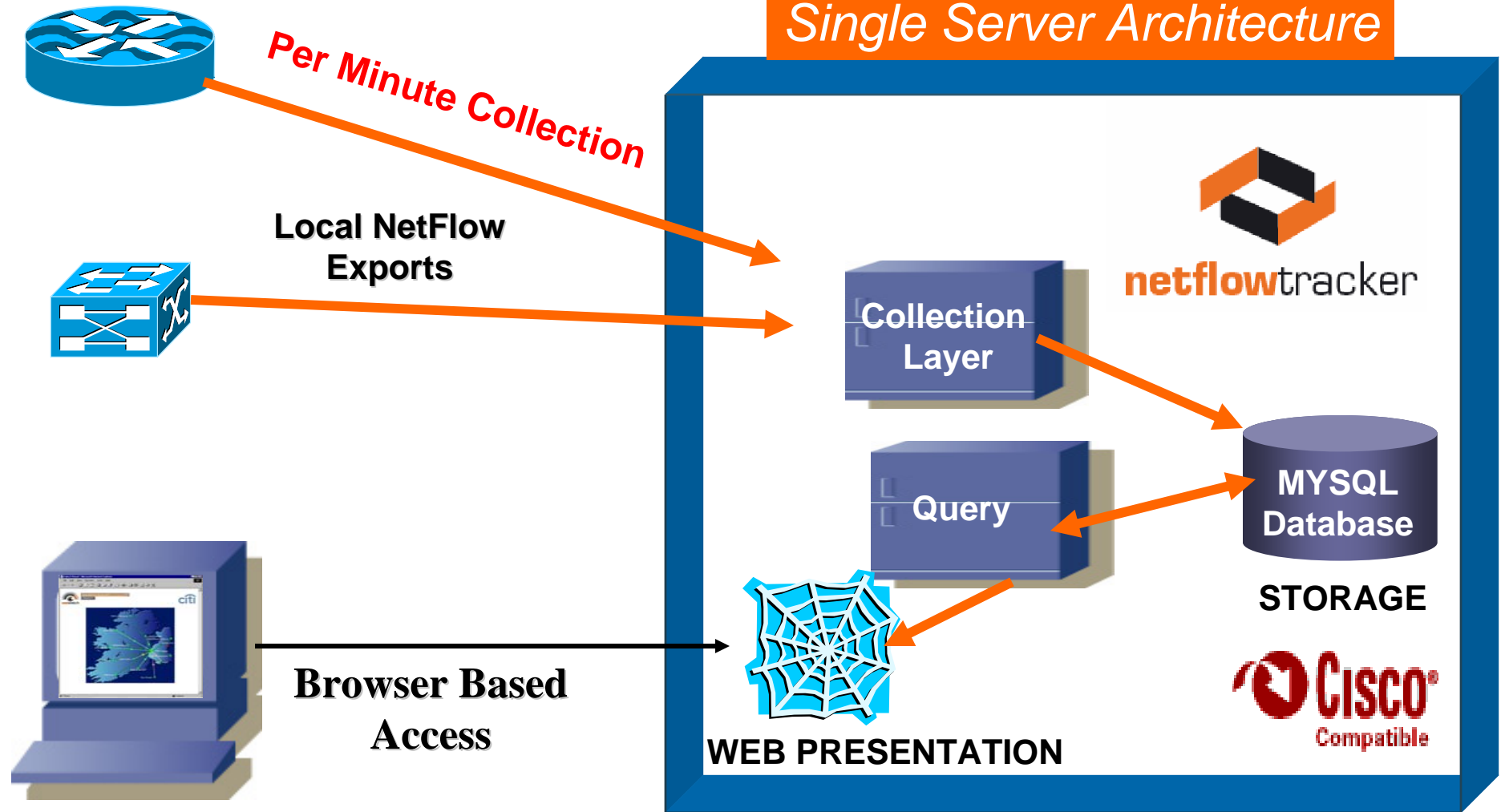
### Dagnostic:-

**Show ip flow export**

**Show ip cache flow verbose**



### Single Server Architecture





CRANNOG SOFTWARE

## Information...



- Source Addresses
- Destination Addresses
- Address Pairs
- Protocols
- Source Ports
- Destination Ports
- Source Applications
- Destination Applications
- Source Endpoints
- Destination Endpoints
- Server-Client Sessions
- Client-Server Sessions
- Conversations
- Type of Service TOS
- Differentiated Services DiffServ
- AS Pairs
- Source Networks
- Destination Networks
- Network Pairs
- In Interfaces
- Out Interfaces
- Next Hops
- Source Address Dissemination
- Destination Address Popularity



CRANNOG SOFTWARE

## Common Implementation



Core Network

Great Tool for MPLS Networks!

*Enable NetFlow*  
*Look at Data Per Interface*  
*Look at Traffic In and Out*

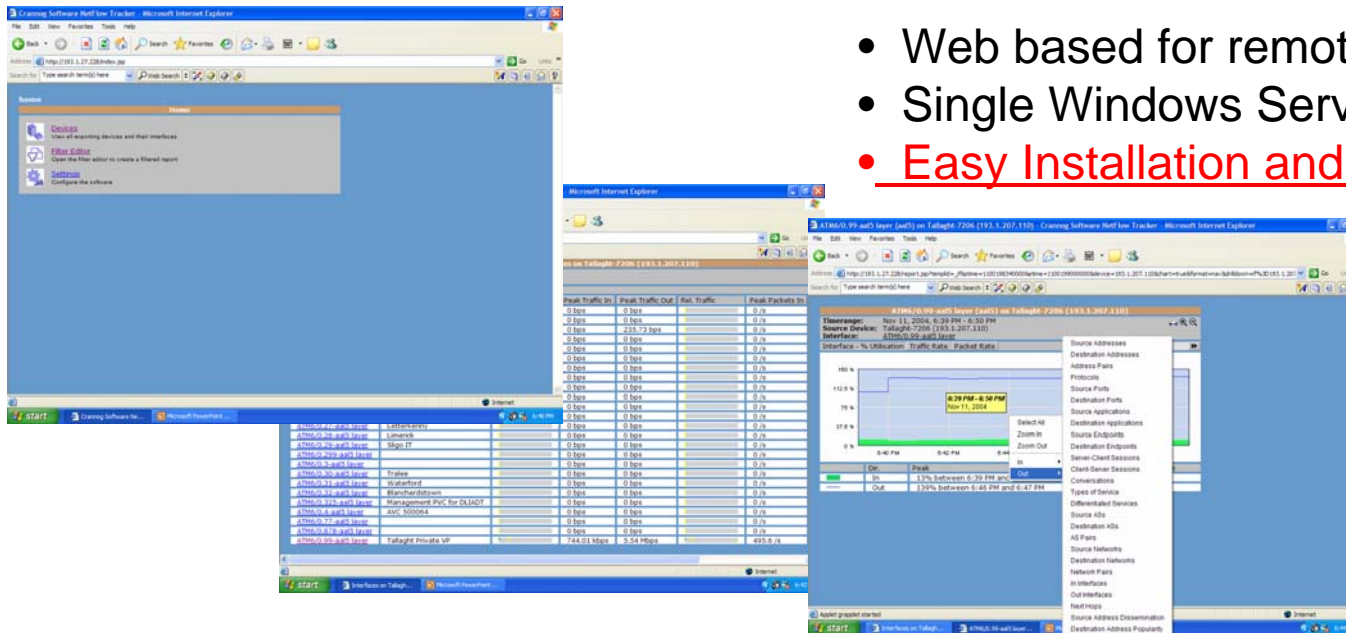
UDP NetFlow  
Export  
Packets



Single Server Collects and Presents  
Web Based Interface



# Tracker turns NetFlow Data into *Information*



- Web based for remote access
- Single Windows Server (C/S/P)
- Easy Installation and Set up (10 Minutes)

- Real-time information – every minute
- Archives Information – granular network forensics and detailed reporting
- Output .csv
- Each report or view is a unique URL

Full Functioning Software – Extended Evaluation [www.crannog-software.com](http://www.crannog-software.com)



CRANNOG SOFTWARE

## Sample List of Customers



- CitiCorp
- Intel
- LSI Logic
- Emulex
- Westinghouse
- Nintendo of America
- Johns Hopkins
- Merchants Bank
- Campus USA Credit Union
- St. Paul Travelers
- GE Financial Assurance
- Quicken Loans
- Banta
- EDS ATKearney
- Hub Group
- CH Robinson
- Guardian
- IBM
- HP
- Pfizer
- Trimble Navigation
- Education Networks of America
- EMC
- Connoco-Phillips
- Duke Energy
- Cinergy
- El Paso Energy
- Constellation Energy
- Parsons
- Amerisource Bergen
- Northrop
- US Department of Transportation
- Missouri DOT
- Ohio DOT
- State of Delaware
- University of New Hampshire
- Lee County Schools
- Jefferson County Schools
- Calvert County Public Schools
- Hillsborough Courts
- Government Agencies
- NOAA – National Oceanic and Atmosphere
- USA Today