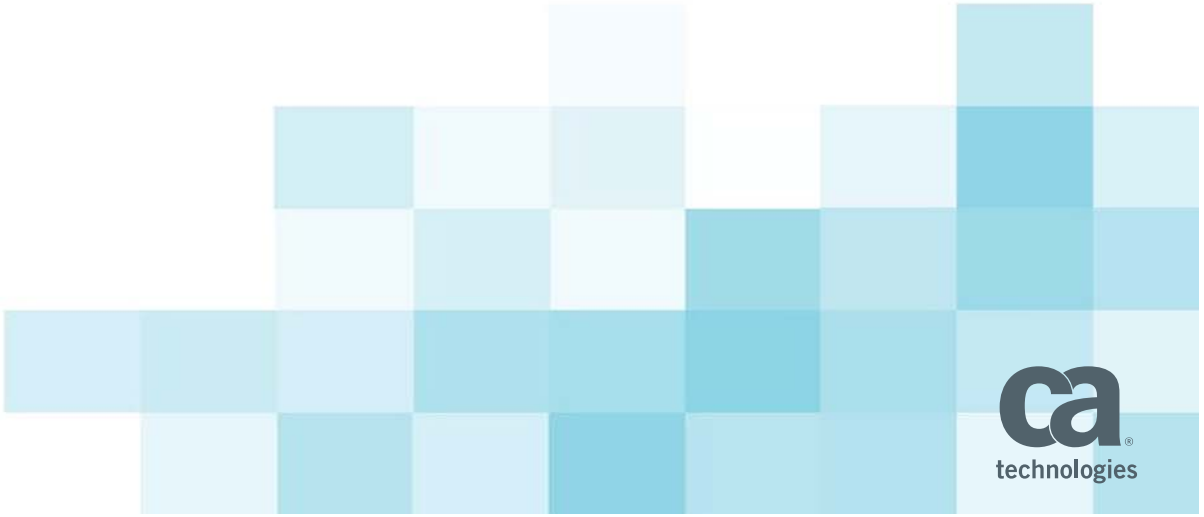
EM DevXchange 11 & 12th May 2016
NFA Best Practices
Infrastructure Management

Todor Kardjiev
Principal Consultant Technical Sales - EMEA

14 May 2016



Disclaimer

Certain information in this presentation may outline CA's general product direction. This presentation shall not serve to (i) affect the rights and/or obligations of CA or its licensees under any existing or future license agreement or services agreement relating to any CA software product; or (ii) amend any product documentation or specifications for any CA software product. This presentation is based on current information and resource allocations as of January 5, 2016 and **is subject to change or withdrawal by CA at any time without notice**. **The development, release and timing of any features or functionality described in this presentation remain at CA's sole discretion**.

Notwithstanding anything in this presentation to the contrary, upon the general availability of any future CA product release referenced in this presentation, CA may make such release available to new licensees in the form of a regularly scheduled major product release. Such release may be made available to licensees of the product who are active subscribers to CA maintenance and support, on a when and if-available basis. The information in this presentation is not deemed to be incorporated into any contract.

THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY. CA assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. **In n**o event will CA be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if CA is expressly advised in advance of the possibility of such damages.

Agenda

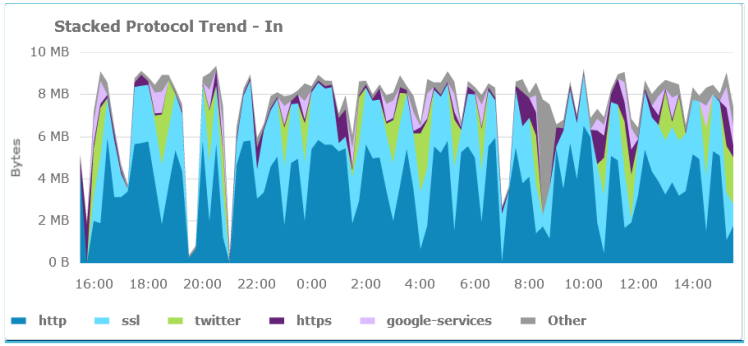
1. NFA BACK TO BASICS
2. ARCHITECTURE
3. PLACEMENT/FLOW CONFIGURATION – WHERE AND WHY
4. CONFIGURATION
5. DATA ANALYSIS
6. Q & A

ca technologies

NFA Back to basics

CA Network Flow Analysis

100% visibility into network traffic and behavior



- Visibility into how the network is being used – users, destinations, prioritization
- Single, data center-based collection point
- Accurate historical, real-time and projective capacity account
- Cisco IVT certified for AVC (Application Visibility and Control) enabled devices for rich accounting, classification and reporting of applications

ca technologies

CA Network Flow Analysis – Benefits

Reduce WAN Costs	• Visibility into utilization levels in order to optimize network capacity • Make sure bandwidth is not the root cause for performance issues before investing in costly upgrades
Detect, isolate and resolve network problems faster	• Reduces false positives and wasted efforts through patented anomaly detection that dynamically adapts the network profile to ensure detection accuracy. • Gain an enterprise-wide view of infrastructure availability and performance, and, when needed, drill down to flow components for detailed analysis and guided workflows that enable faster problem remediation.
Understand, predict and meet changing network capacity demands	• Reality-based capacity planning with access to 13 months of enterprise-wide historical data. • Intelligent, fact-based decisions regarding capacity investments and resource optimization to address and anticipate evolving technical and business requirements.
Align to business priorities	• Cisco NBAR2 support enables rich application accounting, classification and reporting to enhance visibility into applications running on the network. • With enhanced visibility - Intelligently prioritize, control, route, load-balance and optimize application traffic to maximize user experience, optimize bandwidth and reduce costs.

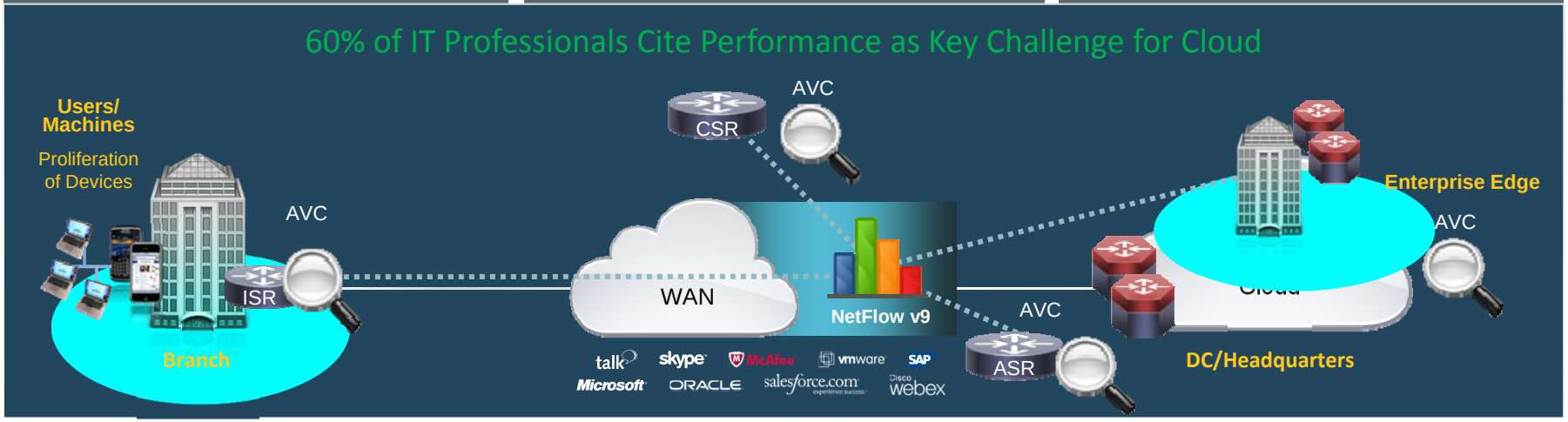
IP-Flow Technology Support

- Flexible NetFlow
- sFlow
- JFlow
- Cflowd
- NetFlow v5
- NetFlow v9
- IPFIX
- NetStream

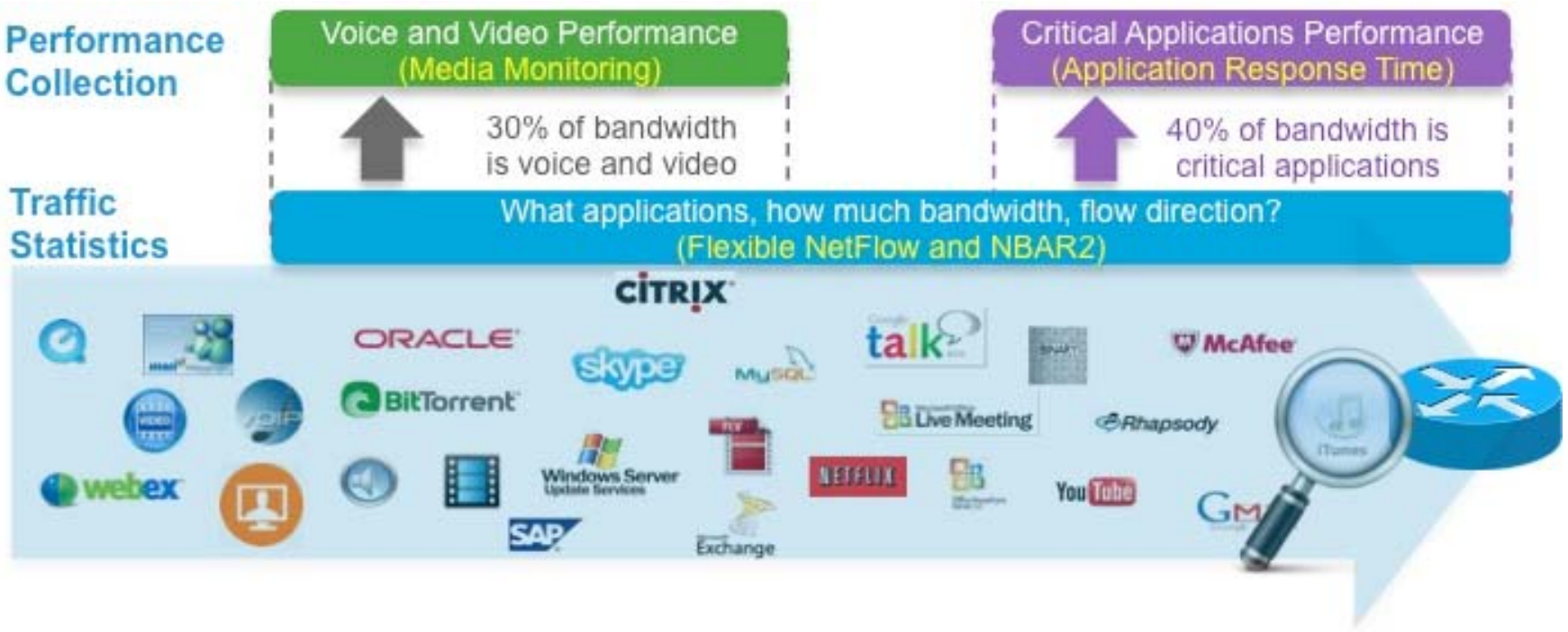
Application Awareness

Cisco Application Visibility and Control (AVC)

NO PROBES	VISIBILITY TO 1000+ APPS	SMART CAPACITY PLANNING
Pervasive App Visibility • No additional hardware • Rich data collection using NetFlow v9/IPFIX • Easy to integrate into many reporting tools	**Business Policy-based Rules** • No need for complex IP and port ACLs • See inside HTTP flows to identify specific Cloud applications	**Comprehensive Reporting** • Better use of costly bandwidth • Per-branch and per-application level reporting



AVC Operation - Performance Collection and Exporting



ca technologies

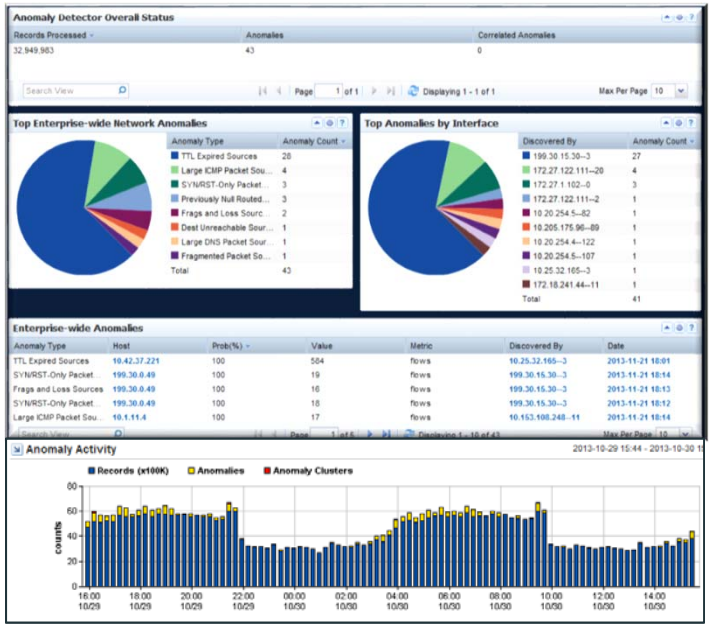
Cisco AVC

- With Cisco AVC, customers can…
  - Discover network traffic with application-level insight with deep packet visibility into web traffic
  - Analyze and report on application usage
  - Classify and manage application sessions (including web browsing, multimedia streaming, and peer-to-peer applications)
  - Build reporting for capacity planning and compliance
  - Enforce quality-of-service (QoS) policies and service guarantees for latency-sensitive applications (such as voice over IP [VoIP] and interactive gaming)
  - Implement fair-use policies and manage network congestion by optimizing application-level traffic

Patented Anomaly Detection

Proactively detect security risks that impact performance

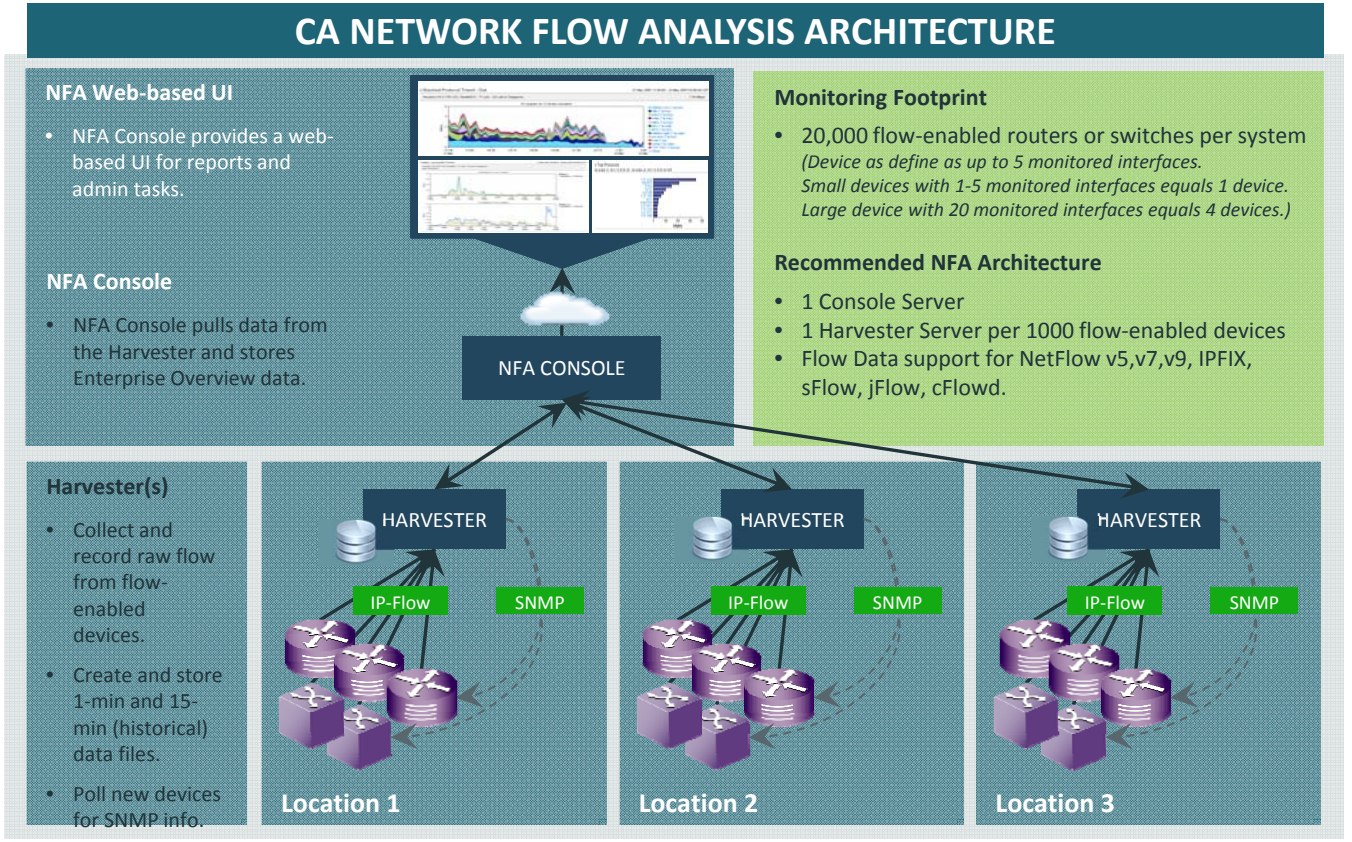
- Visibility into network use – users, destinations, prioritization
- Single collection point
- Accurate historical, real-time and projective capacity account
- Cisco IVT certified for AVC (Application Visibility and Control) enabled devices



ca technologies

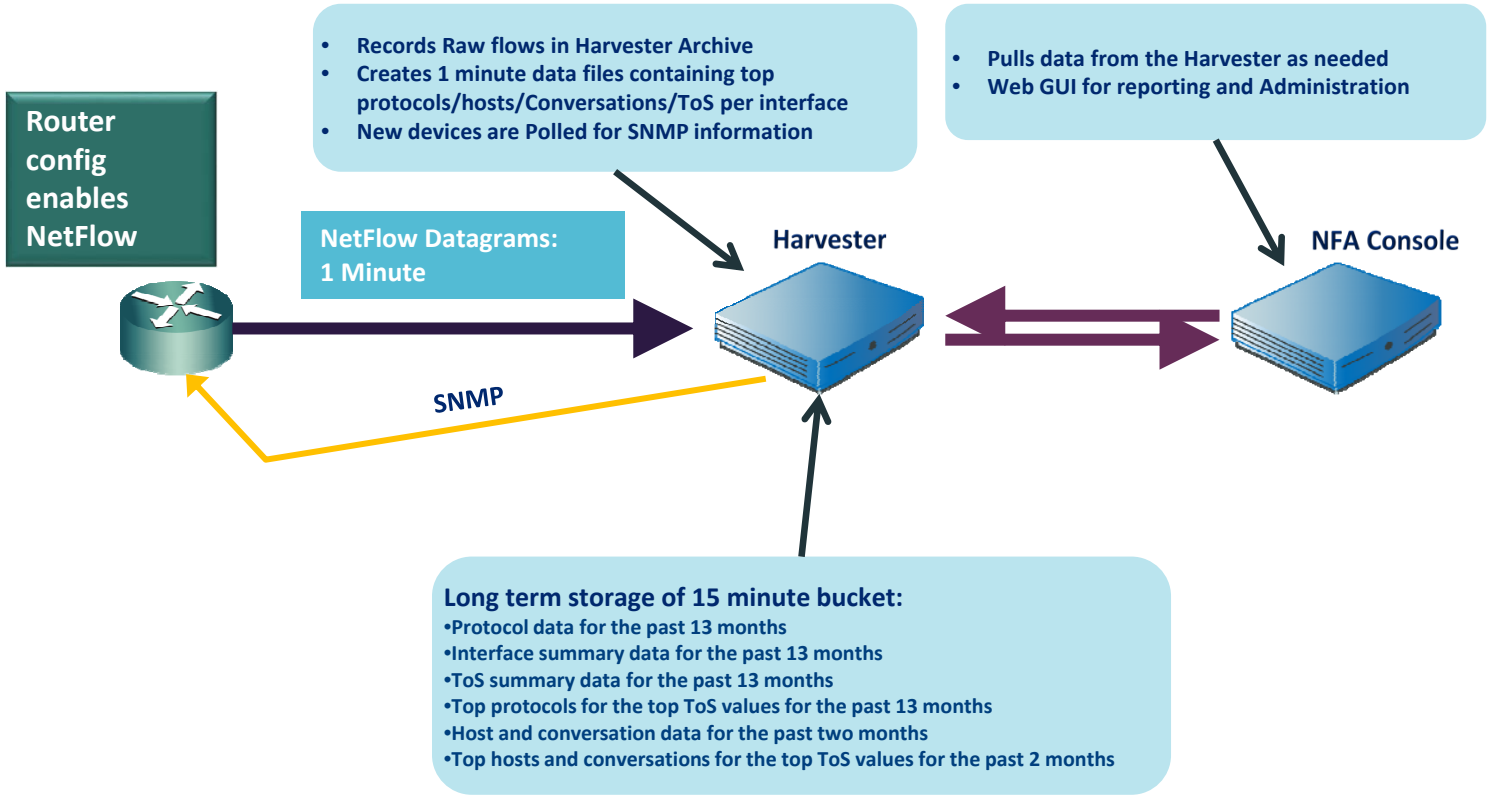
Architecture

CA Network Flow Analysis (NFA) – 2-Tier Architecture



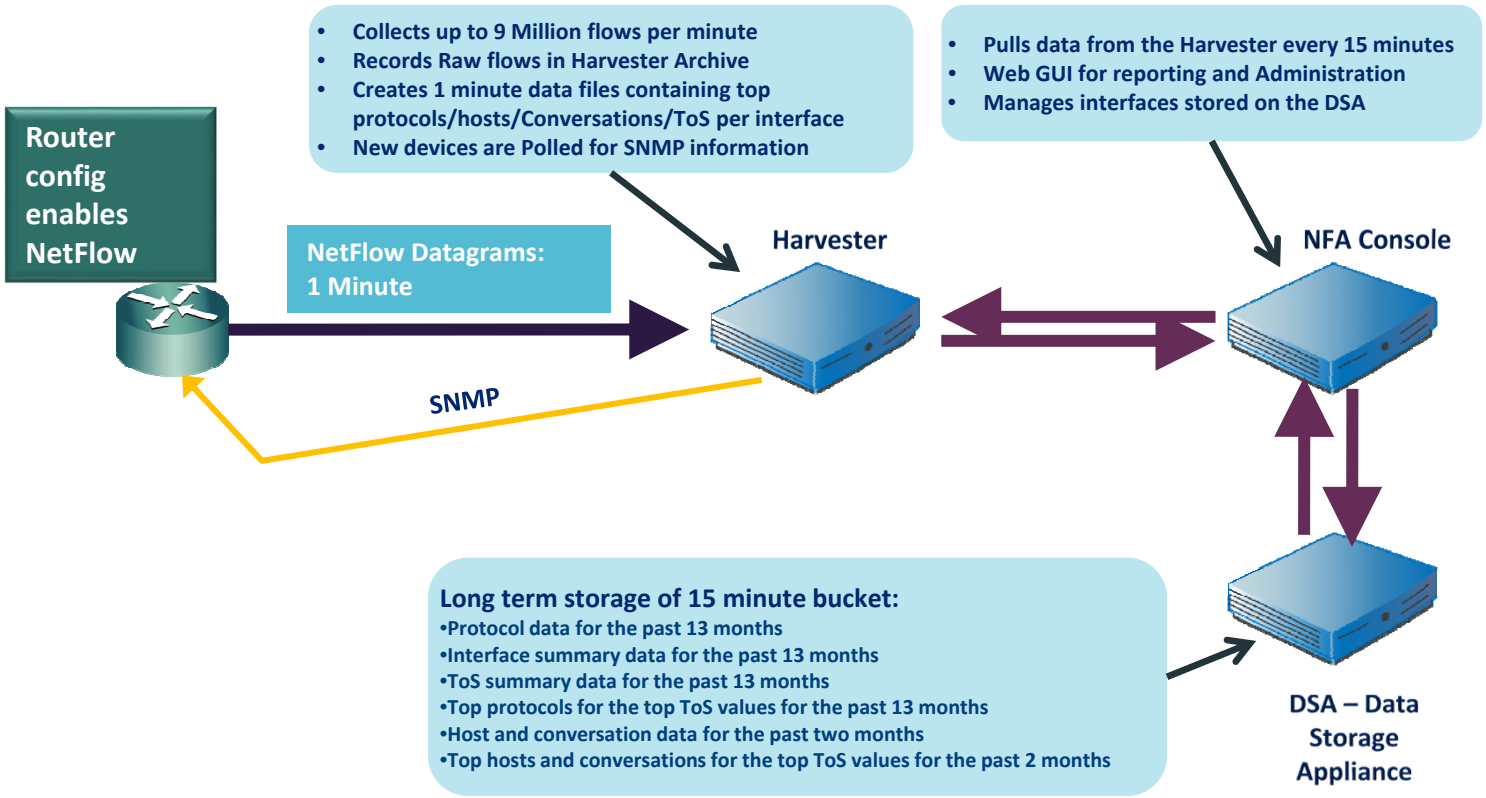
ca technologies

Deployment Architecture 2-Tier

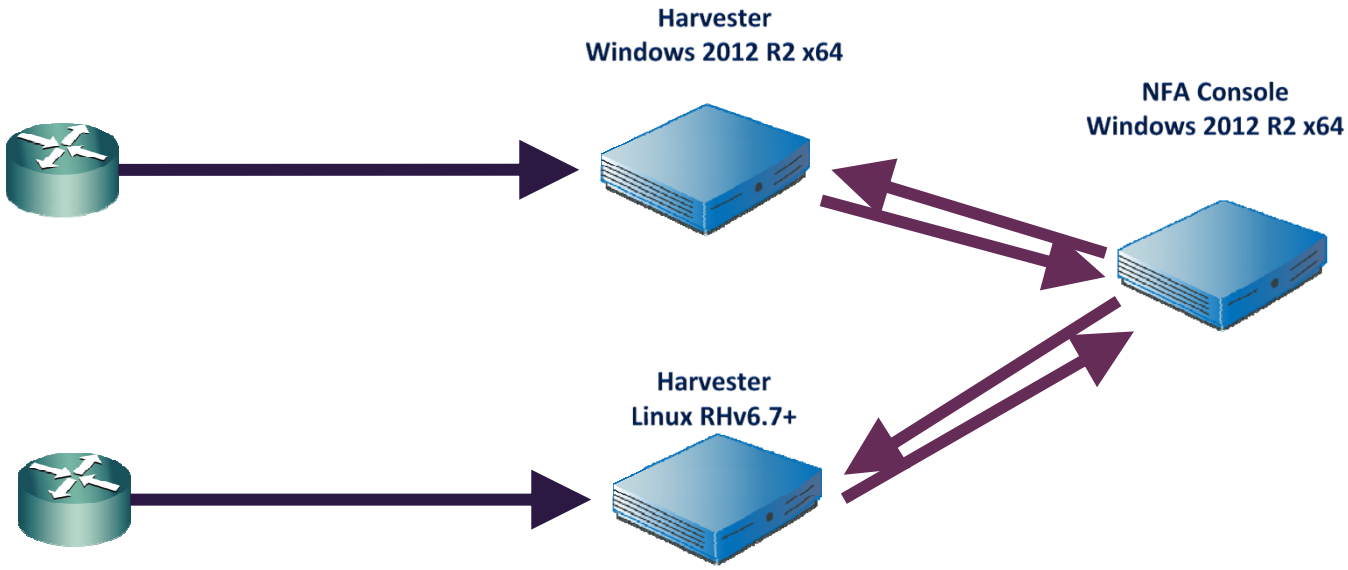


ca technologies

Deployment Architecture 3-Tier *



Deployment Architecture - Multi-Platform Harvester



Placement/Flow Configuration – where and why

Placement/Flow Configuration Best Practices

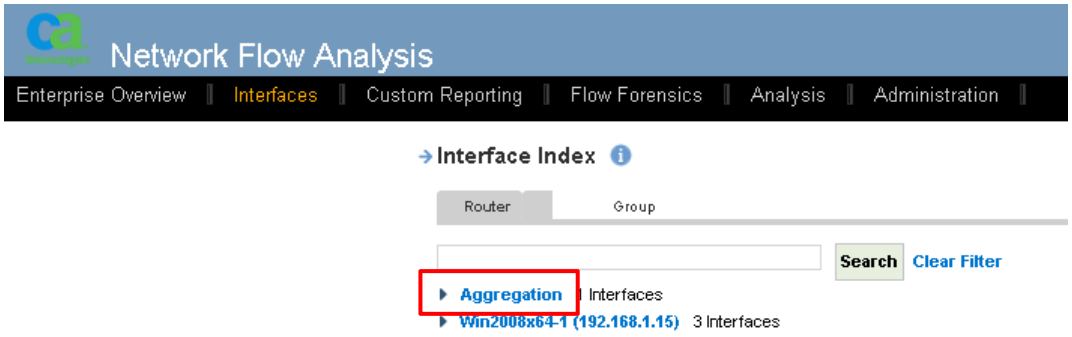
- Keep Flow Exports localized
- Console in DC (close to PM/UMP)
- DSAs close to the Console
- Configure Bidirectional exports on interfaces of interest if possible
- Configure Unidirectional flow exports on all Layer 3 interfaces
- Make sure cache exports happen at least once a minute

Configuration

Interface Aggregation

— An interface aggregation combines traffic from two or more interfaces so the traffic is reported together.

— Aggregations let you report on the interfaces as a single unit without requiring you to create a custom report for that purpose.



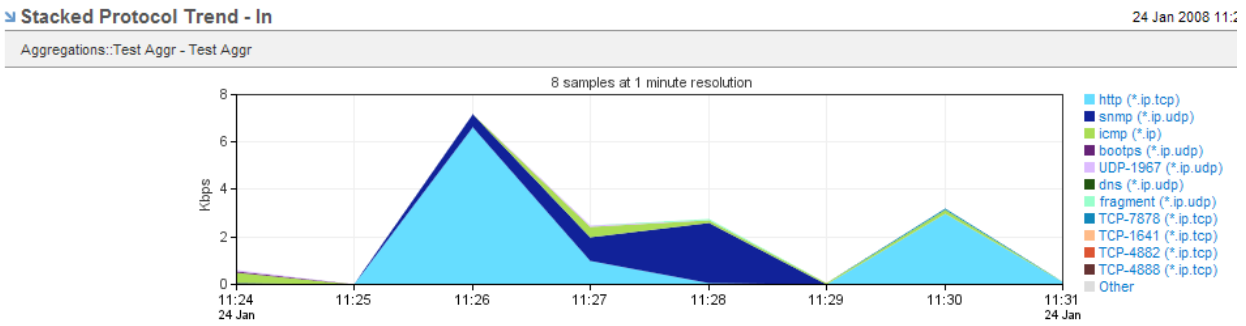
Interface Aggregation

— Act as a real interface

— View through historical reports, real time reports, custom reports, analysis, and flow forensics

— Consumes 1 device license per 5 aggregations (standard license rules apply)

Do not attempt to aggregate interfaces from multiple Harvesters.



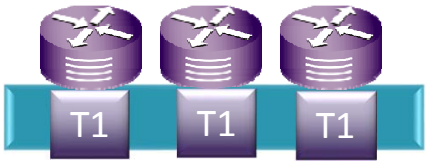
ca technologies

Interface Groups

— Used when defining custom reports, analysis, and flow forensics

— Facilitate adding or removing many interfaces to reports without having to do each one individually

— Interface Groups can be applied to Roles so that users can only see specific interfaces



Interface Groups

— Build Interface groups for users you want to give limited access to

— Build interface groups for any links that are commonly reported together

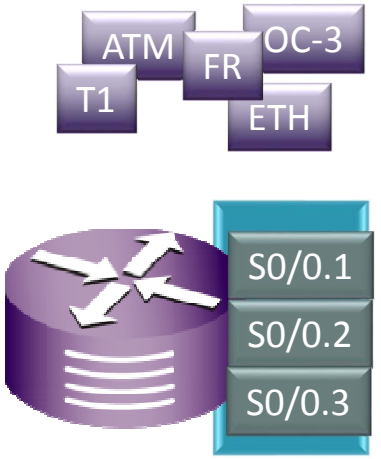
Group by geographic location

Group by network layer

Group by Interface Type or Access Rate

Interface Aggregations

— Aggregate links with asymmetric traffic
  - Prevents you from having to look in two places to look at in/out data
  - See both sides of TCP conversations on one link
— Aggregate load balanced links
— Aggregate sub-interfaces into a single interface



Interface Groups Versus Aggregations

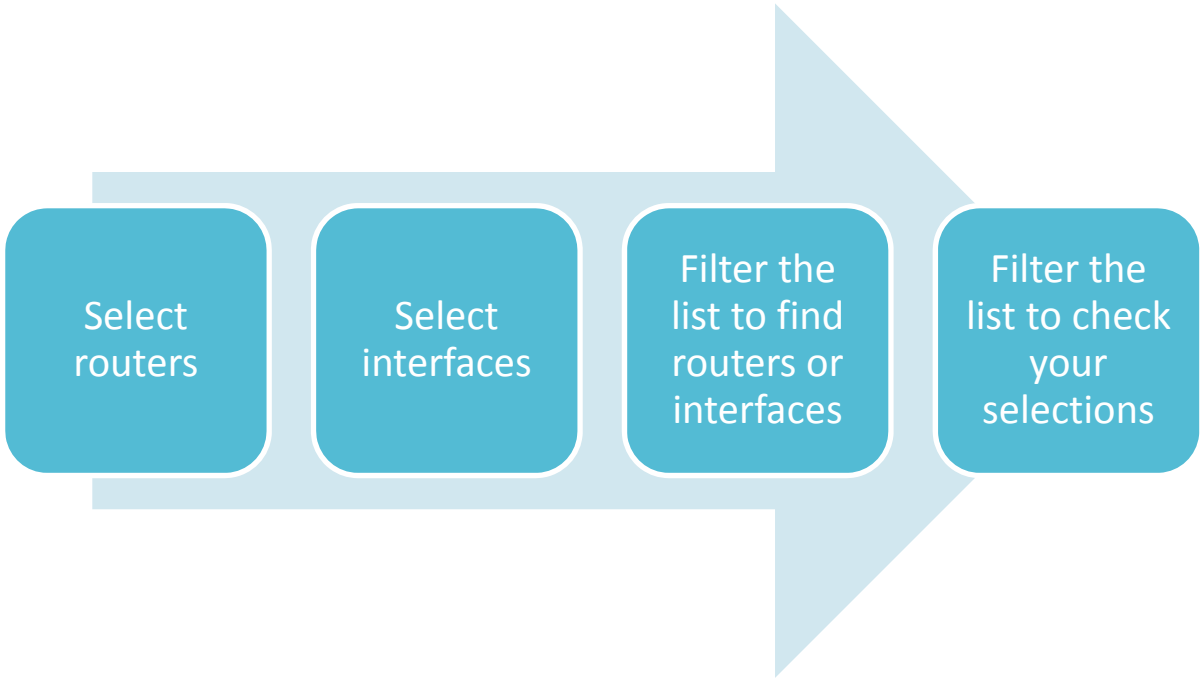
Interface Groups

- Logical grouping of interfaces
- Does not impact license count
- Used for reporting and user administration
- Configured in CA Performance Center

Interface Aggregations

- Behave as an actual interface with all the traffic from the aggregated interfaces added together
- Consumes one device license per 5 aggregations
- Interfaces must be on routers exporting flows to the same harvester

Create Interface Aggregations



Interface Templates

— Create custom templates to standardize the way interface names appear in the NFA console and in related CA products.

— A template consists of text and properties, with the properties enclosed in square brackets. Any text that is not enclosed in square brackets is displayed as text.

When you select a new interface template, by default the template takes effect at the next synchronization. The display reflects the new interface names within 5 minutes.

Interface Templates

Template Property	Description
[DeviceAlias]	Device name that is displayed in the NFA console.
[DeviceName]	DNS name or IP address of the device (router).
[ifDescr]	Interface description as defined in the SNMP ifEntry table.
[ifAlias]	Interface alias.
[ifName]	Name of the interface.
[portName]	Port name, which may be the port number.
[ifIndex]	Index of the interface SNMP ifEntry table.
[ifType]	Interface type as defined in the ifType field of the SNMP ifEntry.

Protocol Groups

— Protocol groups act as filters for report data.

— Administrator can set up custom protocol groups that contain the protocols for particular types of network traffic.

— Each protocol group includes all the protocol values that are used in the enterprise for the target applications.

In a multi-domain environment, the contents of protocol groups are displayed with any domain-specific custom protocol names groups that administrators have created.

ToS Groups

— Administrator can create ToS groups that act as filters for report data.

— Operators can use the ToS group as a filter in reports instead of adding filters for each ToS value.

ToS groups are available in all domains as filters for Analysis reports and Custom reports. The ToS labels that you see displayed for the contents of a ToS group are domain-specific.

Protocol Versus ToS Groups

Protocols groups

- Logical grouping of protocols
- Always group protocols that will be reported on together
  - Applications that use multiple ports or tiers
  - Application types

ToS groups

- Logical grouping of ToS values
- Group ToS values by their respective treatment in your network

When to Map Applications?

— Differentiate common protocols that are based on the application type.

— Aggregate VoIP traffic that uses several different ports into one port.

— Aggregate all mail traffic for mail systems that use multiple protocols, such as IMAP and POP.

— Identify all Microsoft Exchange Server traffic that uses a broad range of port numbers.

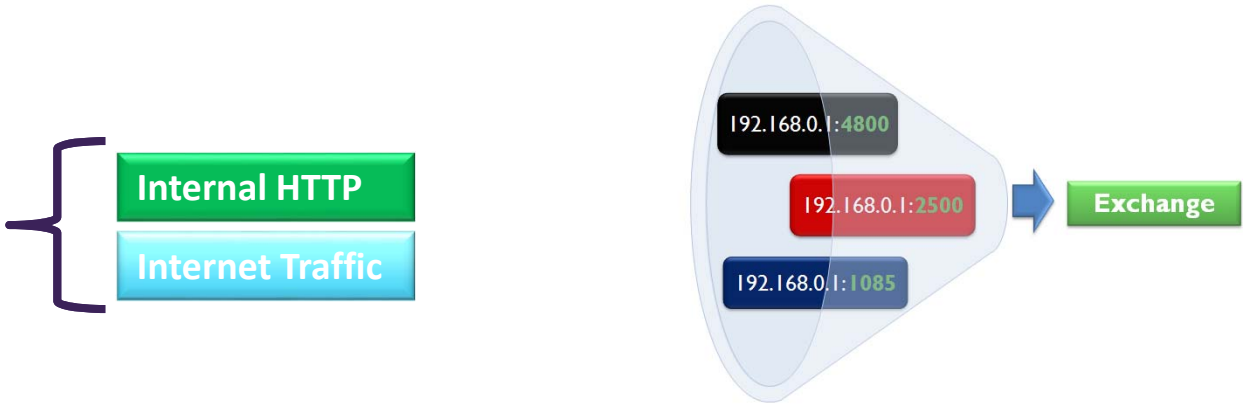
Before you start the application mapping you should show the Protocol Names and ToS Names and how to edit and change the port/tos number to your own defined name.
Once you've created an application mapping you will want to rename the created application port to your own custom defined name.

Map Applications

You can combine traffic from an application that uses several ports into one port.

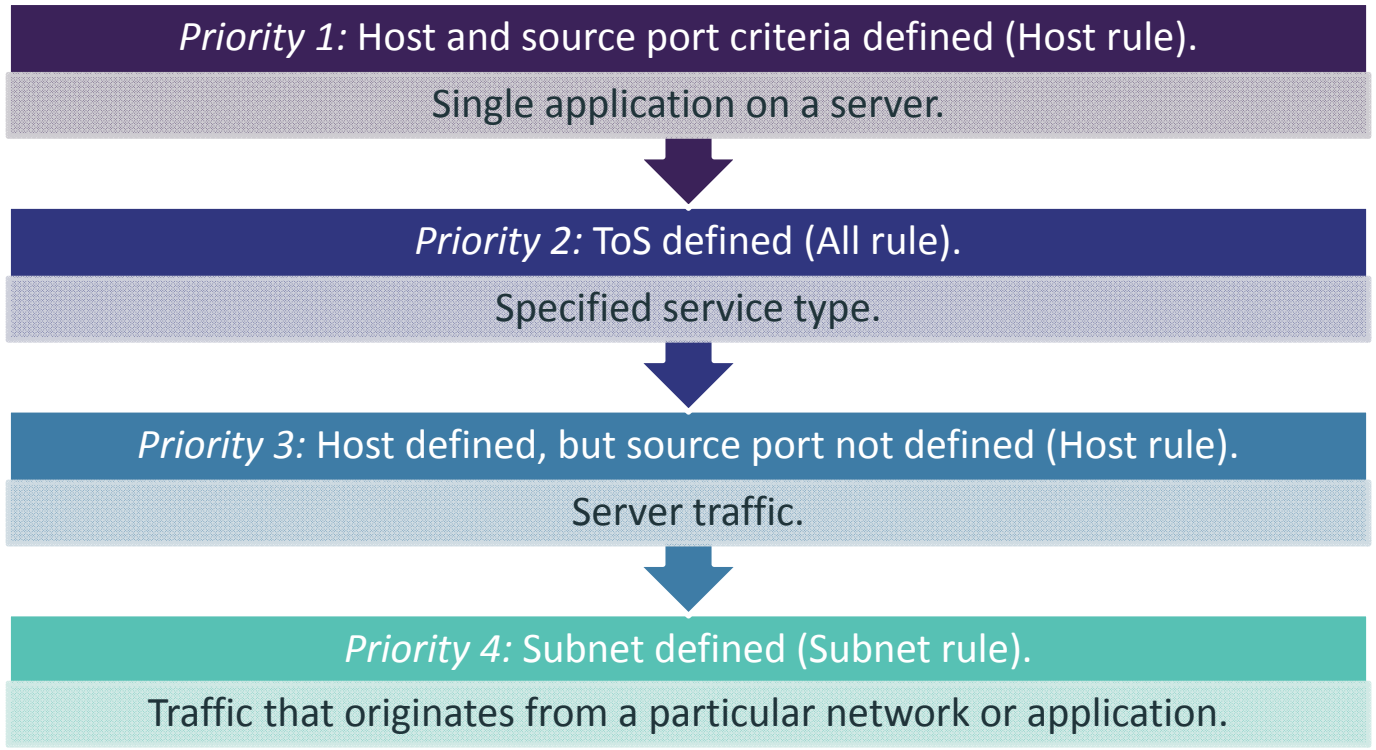
To create application mappings, use the Administration functions to:

- Set up mapping rules to aggregate or segregate data by port number.
- Configure global settings to support mapping rules in reports.



ca technologies

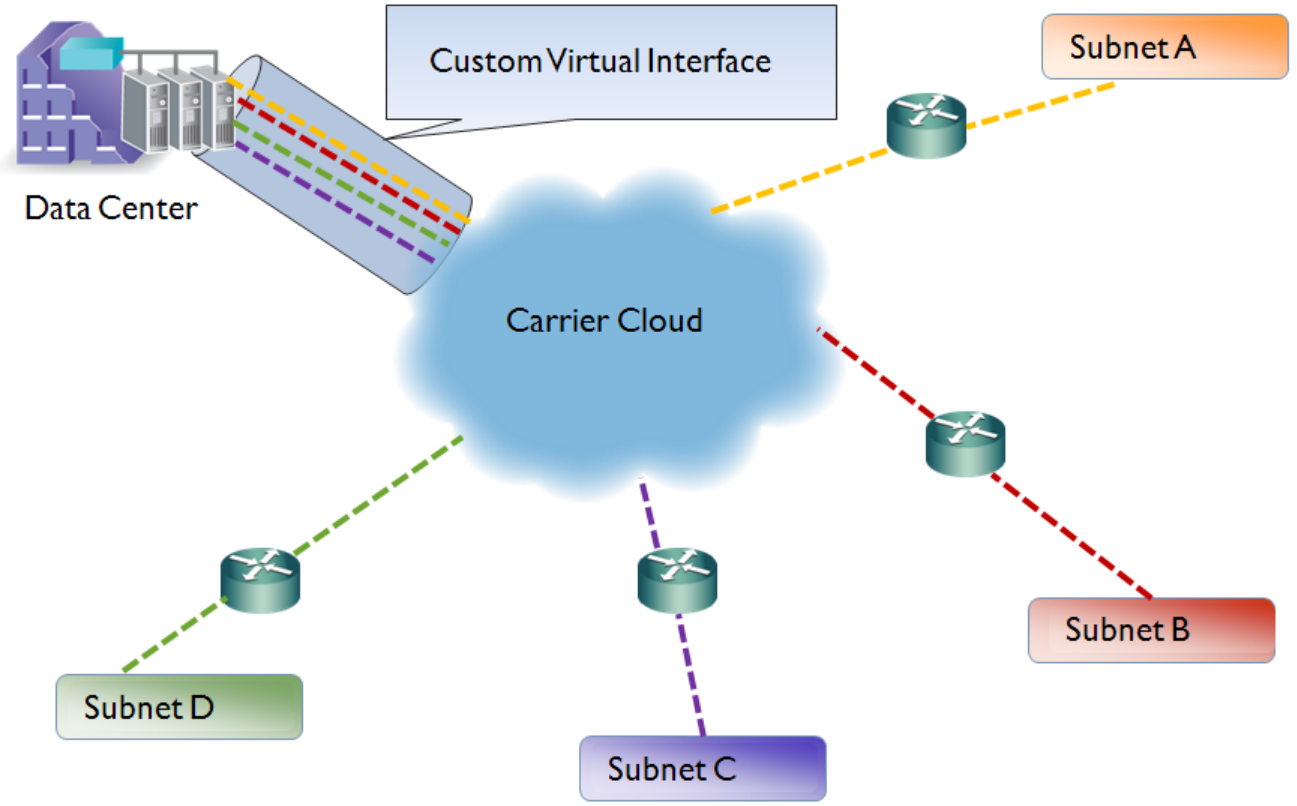
Mapping Priorities



Work With Interfaces

- **Abstract representation of a network interface, which corresponds to one or more subnets of actual physical interfaces.**
- **You can create CVIs to report on subnet traffic.**

Work With Interfaces

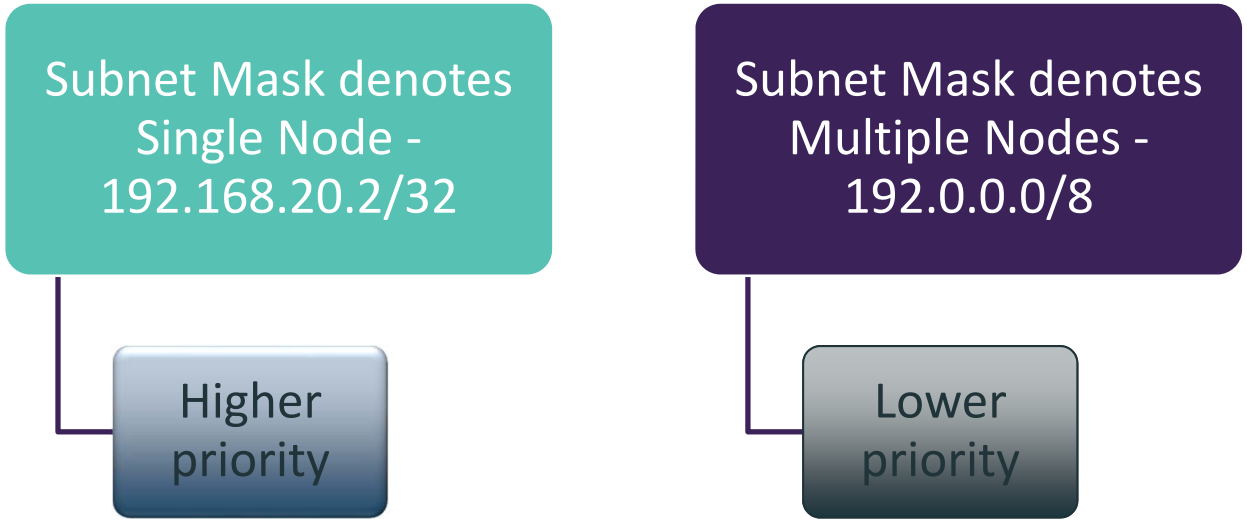


Work With Interfaces

- **Create CVIs for a network that is designed in the following way:**
  - Traffic from a data center is transferred to subnets through an MPLS carrier cloud, and
  - Flow is enabled on the routers in the data center rather than on the routers on the edge of the cloud.

Work With Interfaces

CVI priorities are set according to the degree of specificity of the subnet mask



Reports that are generated for traffic between two CVIs with the same priority can be inconsistent.

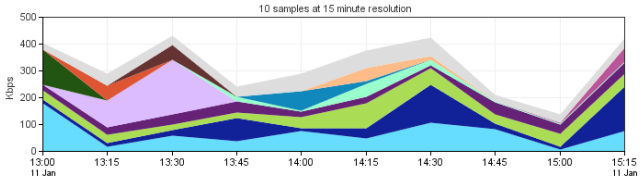
ca technologies

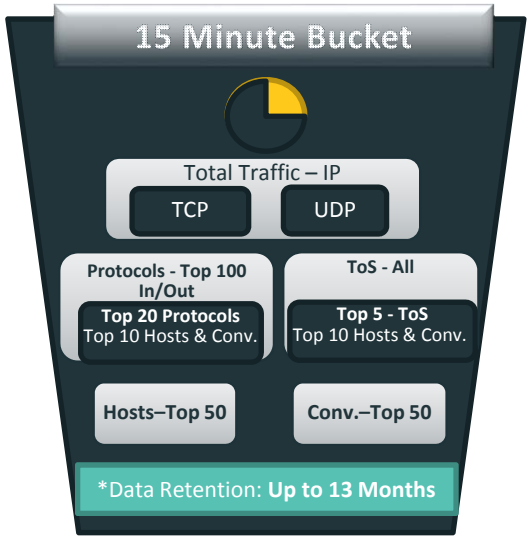
Data Analysis

1 15 Minute Trend Data

Interface Trending

- Greater than 2 Hour Time interval
- For individual breakouts: data must pass a threshold
- Ideal for trending and capacity planning

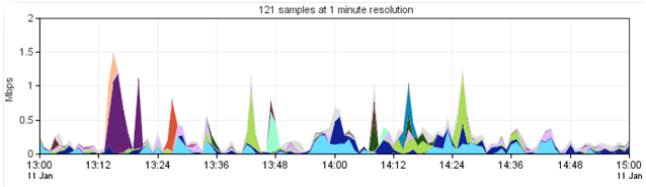


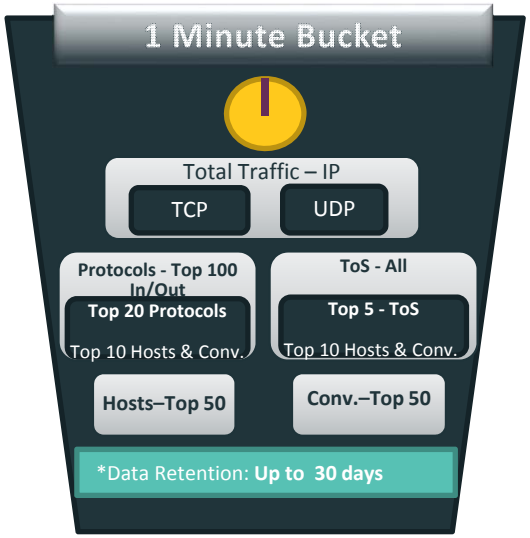


2 1 Minute Trend Data

Interface Reports

- Less than 2 Hour Time Interval
- No Thresholds
- Ideal for troubleshooting and capacity planning





3 Raw Flow Data

Record of the raw flow files received from the routers

- Flow Forensics Reports
- Can filter and search for key fields in NetFlow data
- Up to 24 hours of data

Report Results

Src Addr	Dest Addr	Bytes ▼	Rate (Bits)	% Total (Bytes)	Flows	Pkts	Rate (Pkts)	% Total (Pkts)
nqfs.netqos.local (192.168.0.2)	192.168.9.55	1.29 MBytes	11.46 Kbps	29.59 %	4	1,867	2.07 pkts/s	25.13 %
nqfs.netqos.local (192.168.0.2)	ddev277-devra81.netqos.local (192.168.9.232)	863.04 KBytes	7.67 Kbps	19.81 %	13	1,682	1.87 pkts/s	22.64 %
nqfs.netqos.local (192.168.0.2)	ddev324-dev2003.netqos.local (192.168.9.241)	745.41 KBytes	6.63 Kbps	17.11 %	9	1,780	1.98 pkts/s	23.96 %
nqfs.netqos.local (192.168.0.2)	ddev218-dev2003.netqos.local (192.168.8.57)	737.52 KBytes	6.56 Kbps	16.93 %	4	1,095	1.22 pkts/s	14.74 %
nqfs.netqos.local (192.168.0.2)	APSSERVER (10.0.12.2)	303.81 KBytes	2.70 Kbps	6.97 %	1	208	0.23 pkts/s	2.80 %
nqfs.netqos.local (192.168.0.2)	ddev57-npc4.netqos.local (192.168.9.33)	262.44 KBytes	2.33 Kbps	6.02 %	2	396	0.44 pkts/s	5.33 %
nqfs.netqos.local (192.168.0.2)	ddev90-dev.netqos.local (192.168.9.45)	121.59 KBytes	1.08 Kbps	2.79 %	3	196	0.22 pkts/s	2.64 %
nqfs.netqos.local (192.168.0.2)	d-030.netqos.local (192.168.2.42)	17.64 KBytes	157 bps	0.40 %	6	95	0.11 pkts/s	1.28 %
nqfs.netqos.local (192.168.0.2)	192.168.8.210	9.81 KBytes	87 bps	0.23 %	1	58	0.06 pkts/s	0.78 %
nqfs.netqos.local (192.168.0.2)	192.168.6.28	2.25 KBytes	20 bps	0.05 %	2	8	0.01 pkts/s	0.11 %

Duration to Store Data

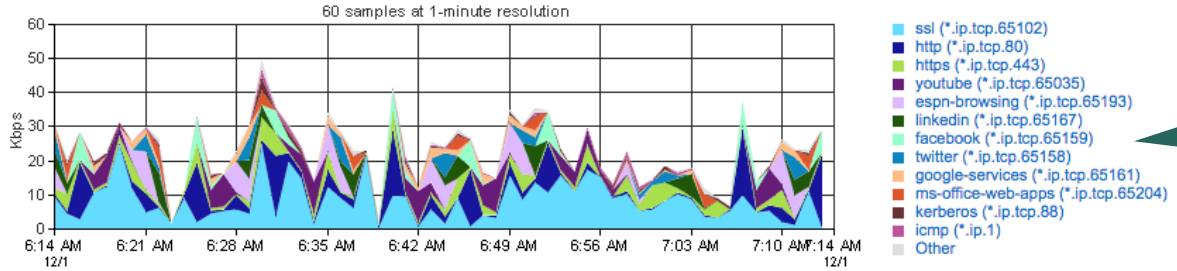
Data Type	By default stored for….	
1 minute data	30 days (but viewable by interface within a 2 hour window)	
15-minute data	Protocol data	13 months
	Interface summary data	
	ToS summary data	
	Top protocols for top ToS values	
	Host and conversation data	2 months
	Top hosts and conversations for top ToS values	
Raw flow data	1 day (24 hours)	

Stacked Protocol Trend

Stacked Protocol Trend - In

December 01, 2014 6:14:00 AM - December 01, 2014 7:14:00 AM MST

BRANCH3 (10.0.4.240)::Gi2 - Connection to BRANCH3 LAN

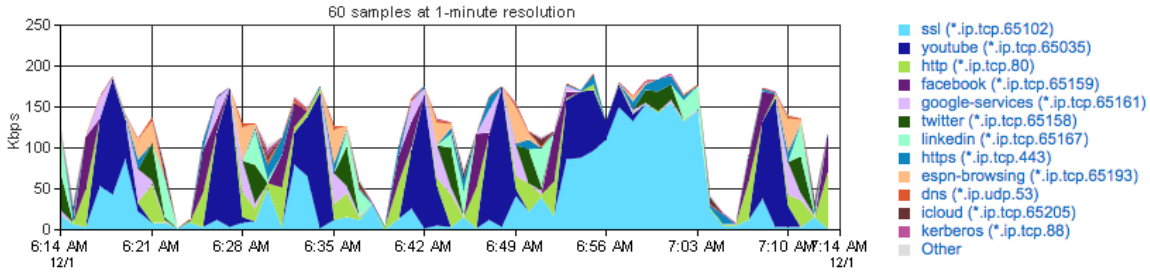


Applications broken out by NBAR2 Classification….

Stacked Protocol Trend - Out

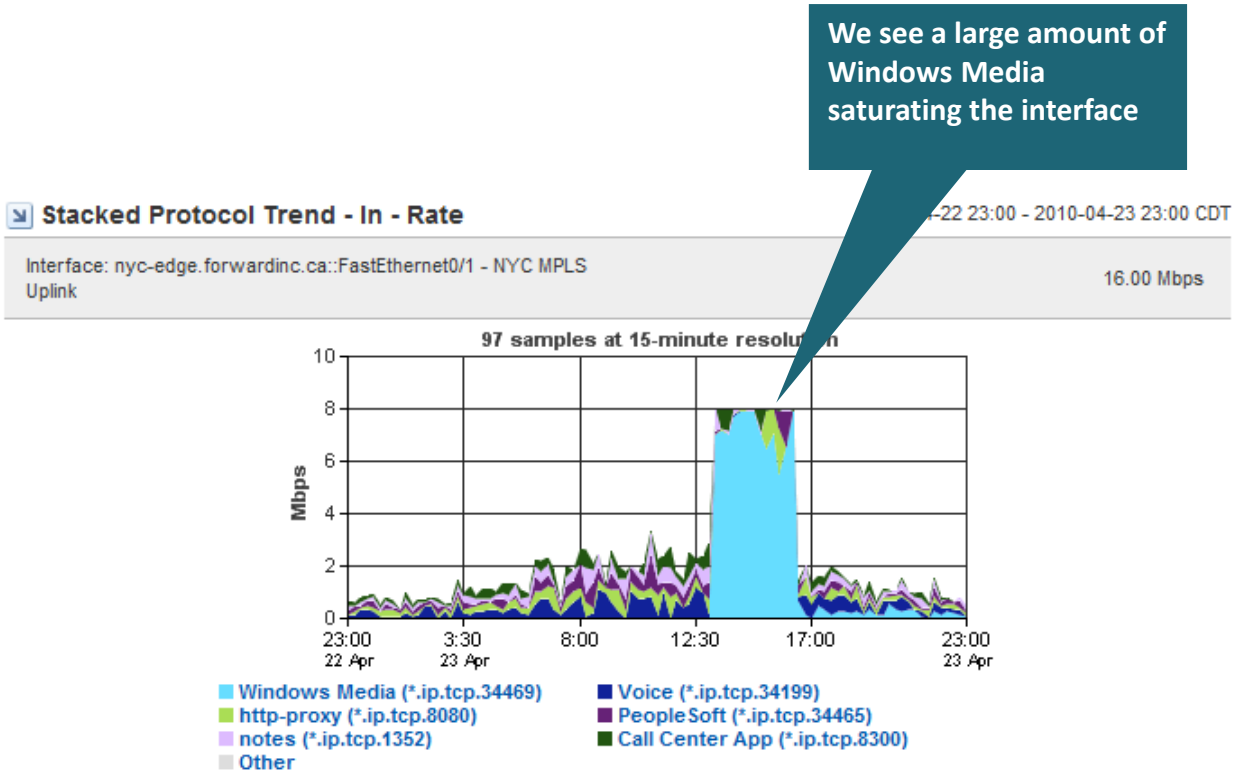
December 01, 2014 6:14:00 AM - December 01, 2014 7:14:00 AM MST

BRANCH3 (10.0.4.240)::Gi2 - Connection to BRANCH3 LAN

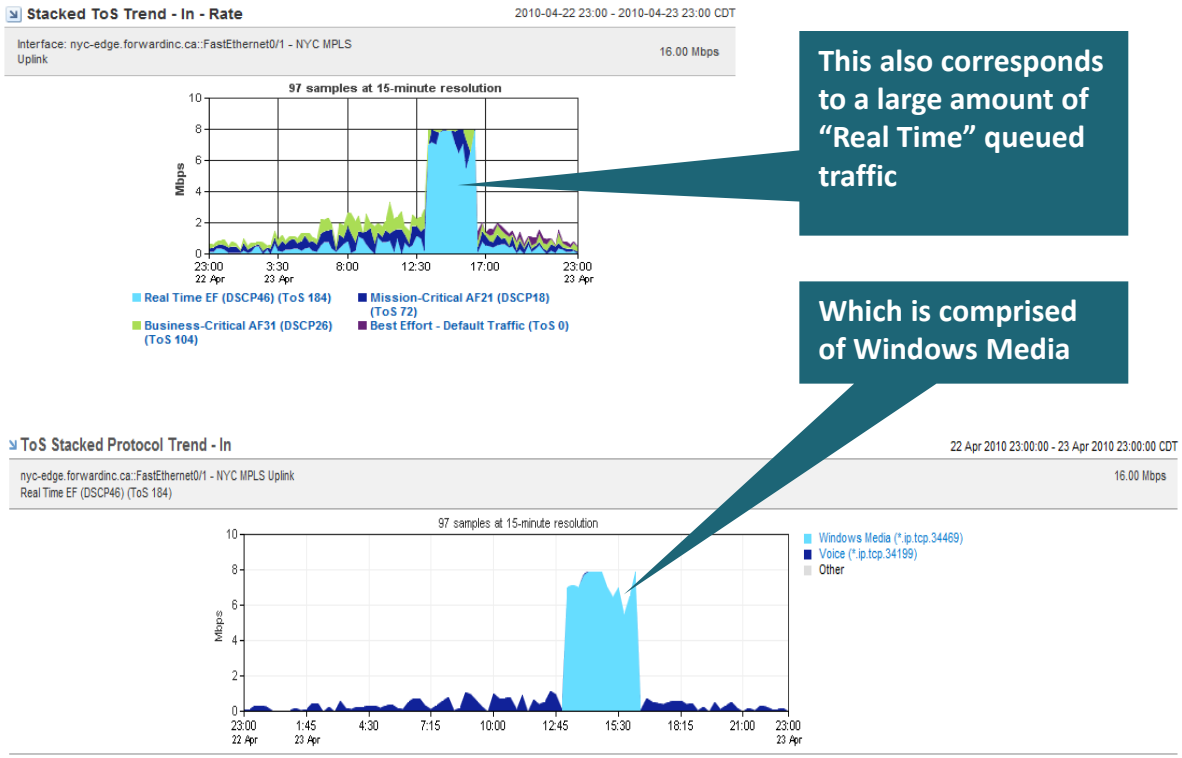


ca technologies

Network Congestion



QoS Validation



Root Cause: Non-Business Critical Traffic

Which is caused by streaming games from NBA.com

Protocol Hosts Summary - From 23 Apr 2010 12:30:00 - 23 Apr 2010 17:00:00 CDT

nyc-edge.forwardinc.ca::FastEthernet0/1 - NYC MPLS Uplink
Windows Media (*.ip.tcp.34469) 16.00 Mbps

nba.com (63.240.105.1)	1.98 GBytes	18.73 %
research98.nyc.forwardinc.ca (10.1.1.4)	1.86 GBytes	17.58 %
mfg22.nyc.forwardinc.ca (10.1.1.10)	1.79 GBytes	16.89 %
support21.nyc.forwardinc.ca (10.1.1.6)	1.07 GBytes	10.06 %
support40.nyc.forwardinc.ca (10.1.1.9)	1.05 GBytes	9.95 %
sales13.nyc.forwardinc.ca (10.1.1.8)	1.04 GBytes	9.83 %
sales87.nyc.forwardinc.ca (10.1.1.7)	699.50 MBytes	6.60 %

Deeper Network Flow Details When Needed

- Drill-down to raw data with flow forensics

Report Results

Router Addr	Application	Transactions	Avg Total Transaction Time	Late Responses	Retransmissions
10.0.9.243	udplite (136)	180	27 secs 973 ms	49995	0
10.0.9.243	custom-10 (244)	990	51 ms	0	18000
10.0.9.243	oracle-ebsuite-unsecured (516)	0	0 ms	1500000	165000
10.0.9.243	google-accounts (528)	6300	4 ms	990	30
10.0.9.243	facetime (535)	285000	18 ms	1160475	150
10.0.9.243	bittorrent-networking (543)	2250	600 ms	7500	1485

1 / 1 Size: 10

Delay between router and client

Report Results

Router Addr	Application	New Connections	Avg Server Network Delay	Avg Response Time	Avg Application Delay
10.0.9.243	udplite (136)	315	5 secs 714 ms	2 mins 38 secs 762 ms	470 ms
10.0.9.243	custom-10 (244)	150	2 secs	5 secs 600 ms	23 secs 457 ms
10.0.9.243	oracle-ebsuite-unsecured (516)	0	0 ms	0 ms	0 ms
10.0.9.243	google-accounts (528)	12840	117 ms	11 ms	40 ms
10.0.9.243	facetime (535)	241845	28 ms	8 ms	10 ms
10.0.9.243	bittorrent-networking (543)	85155	2 ms	2 ms	1 ms

1 / 1 Size: 10

Server Response

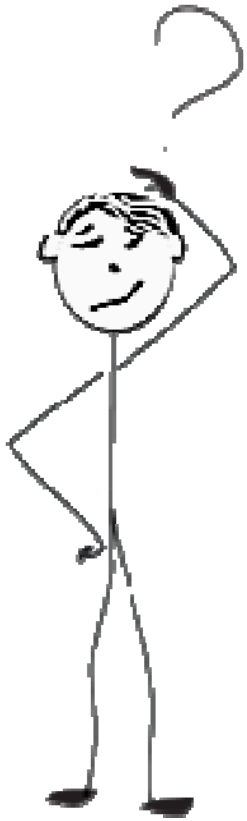
Client Experience

- Report on all of the flow data that is collected in your environment & analyze every protocol, host, and conversation on your network.
- Browse raw flow data & drill down to jump to detailed information about any of the fields in a data packet for any monitored interface.

ca technologies

Q & A

Questions?



ca technologies

Todor Kardjiev
Principal Consultant Technical Sales - EMEA
Todor.Kardjiev@ca.com