Visualizing Traffic on Network Topology

NTT Communications, Kazunori Kamiya
NTT Laboratories, Hiroshi Kurakami

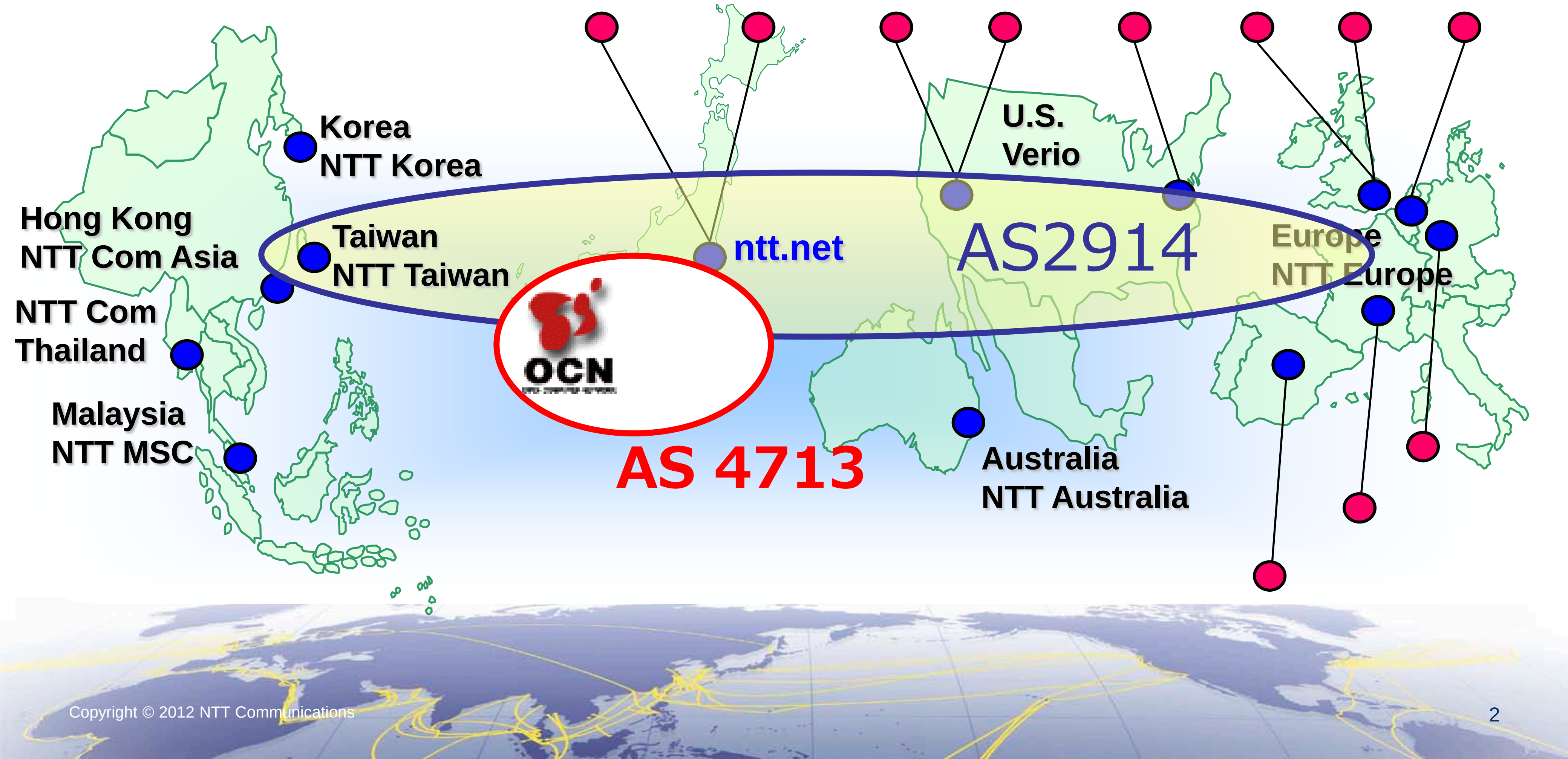
Agenda

- Company Introduction
- Motivation and Goals
- Things to consider
- Method of visualizing Traffic and Topology
- Visualizing Example and Use Cases
- Future Work
- Conclusion

NTT Communications' two large networks

AS2914 : ntt.net Global Tier-1 backbone

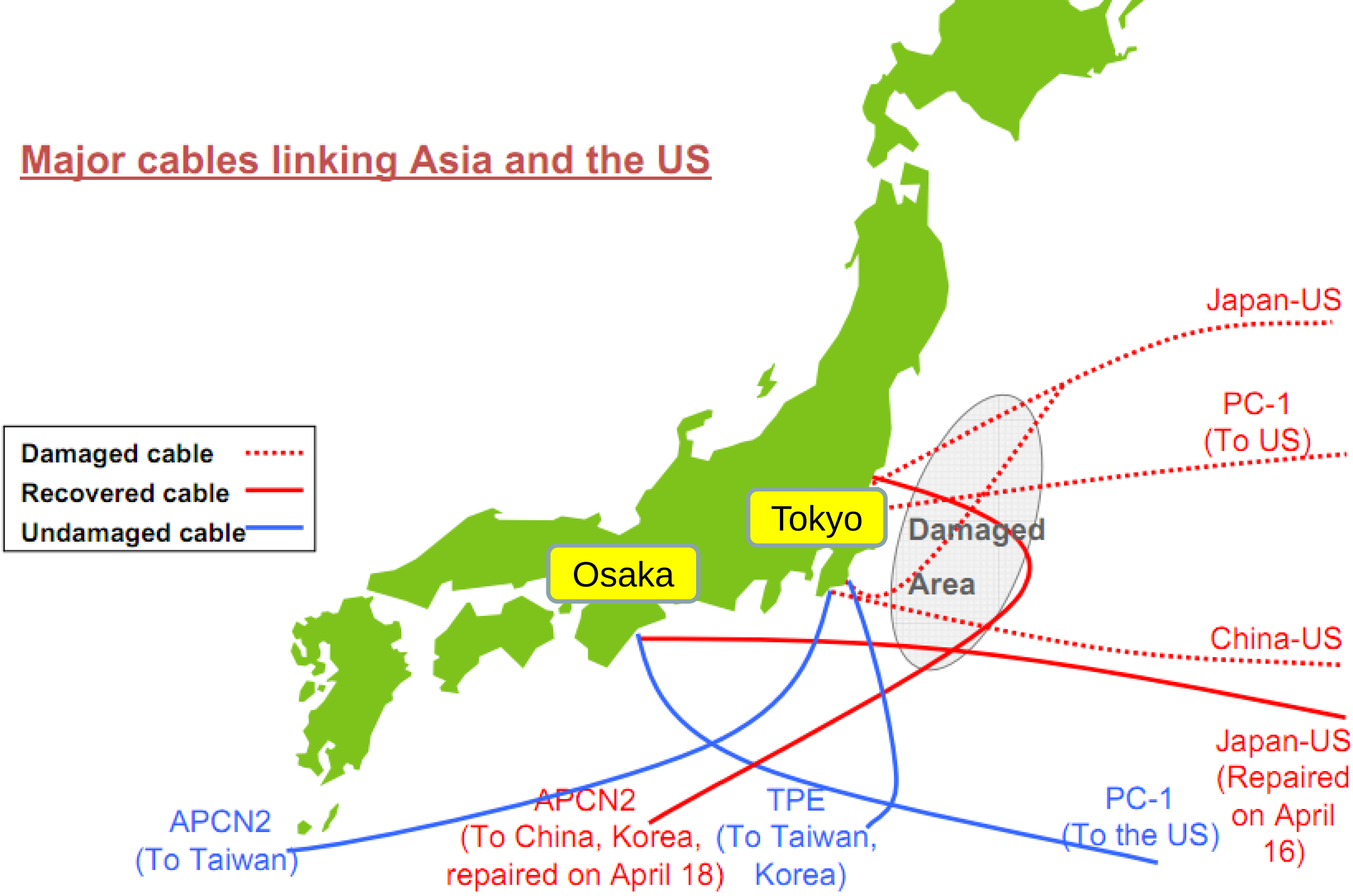
AS4713 : OCN (for Japanese domestic)



East Japan Earthquake – damage in submarine cables

- Damaged Japan-US, APCN2, China-US and PC-1 are gradually being repaired.

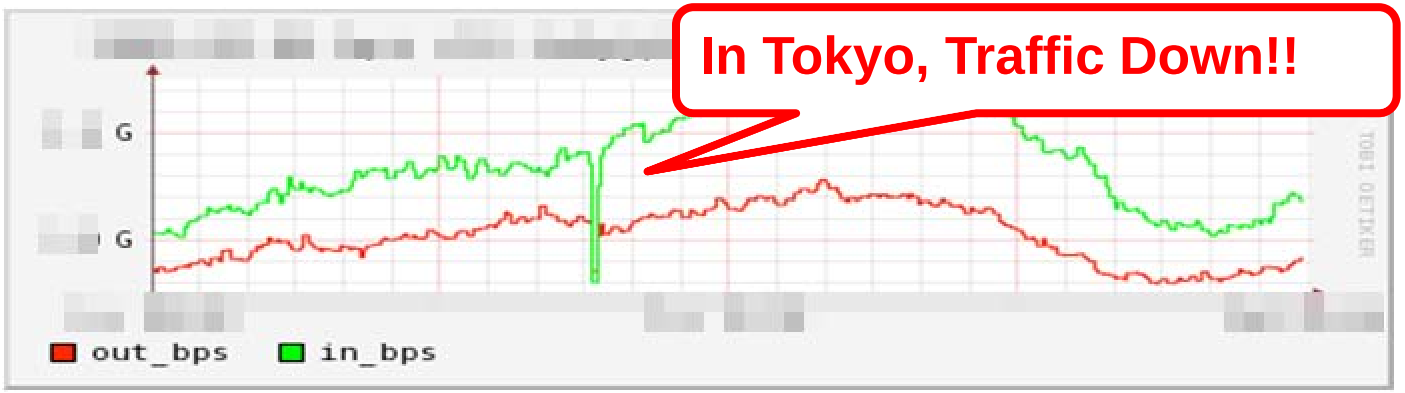
Major cables linking Asia and the US



http://www.ntt.co.jp/ir/library_e/presentation/2011/1105e_2.pdf

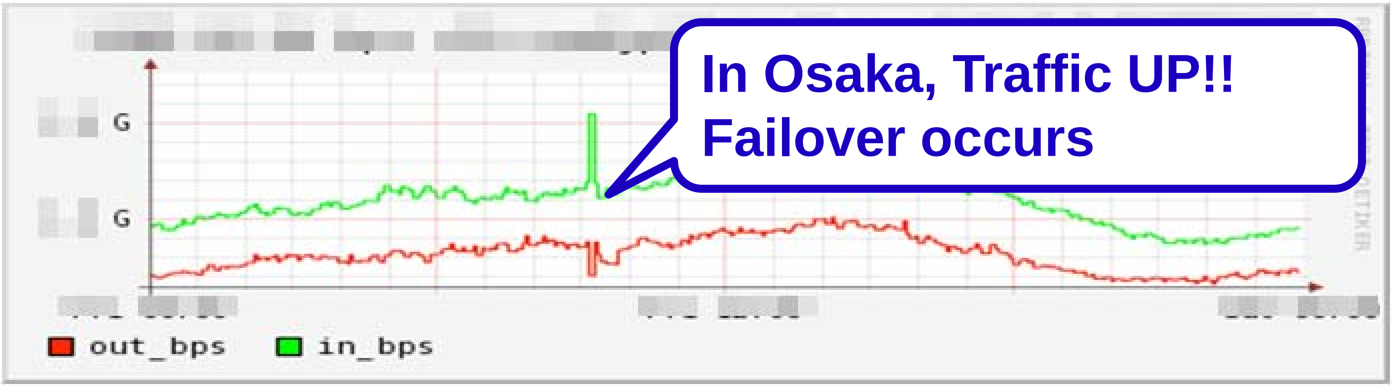
Our Motivation 1

- Visualizing Traffic on Single Point
  - When traffic increases or decreases, we would like to know what is happening on Network



In Tokyo, Traffic Down!!

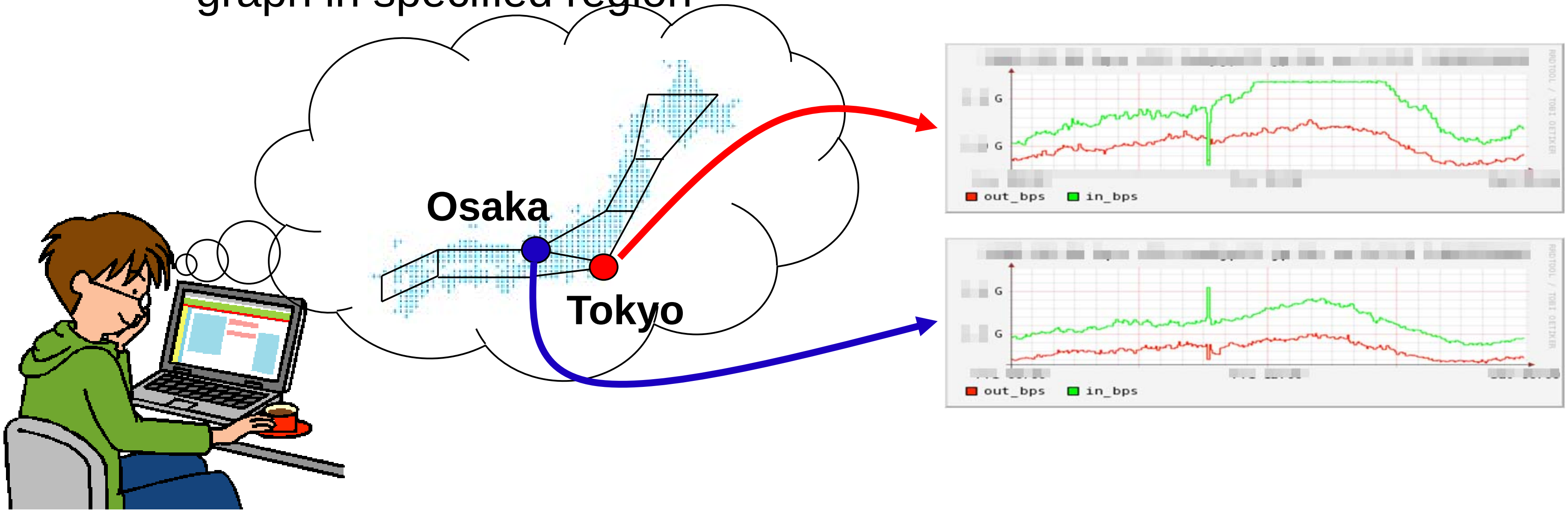
- Looking at Multi Point Traffic leads to understanding



In Osaka, Traffic UP!!
Failover occurs

Our Motivation 2

- Visualizing Traffic on Multi-Point
  - Operators imagine topology in their brain, then search for traffic graph in specified region

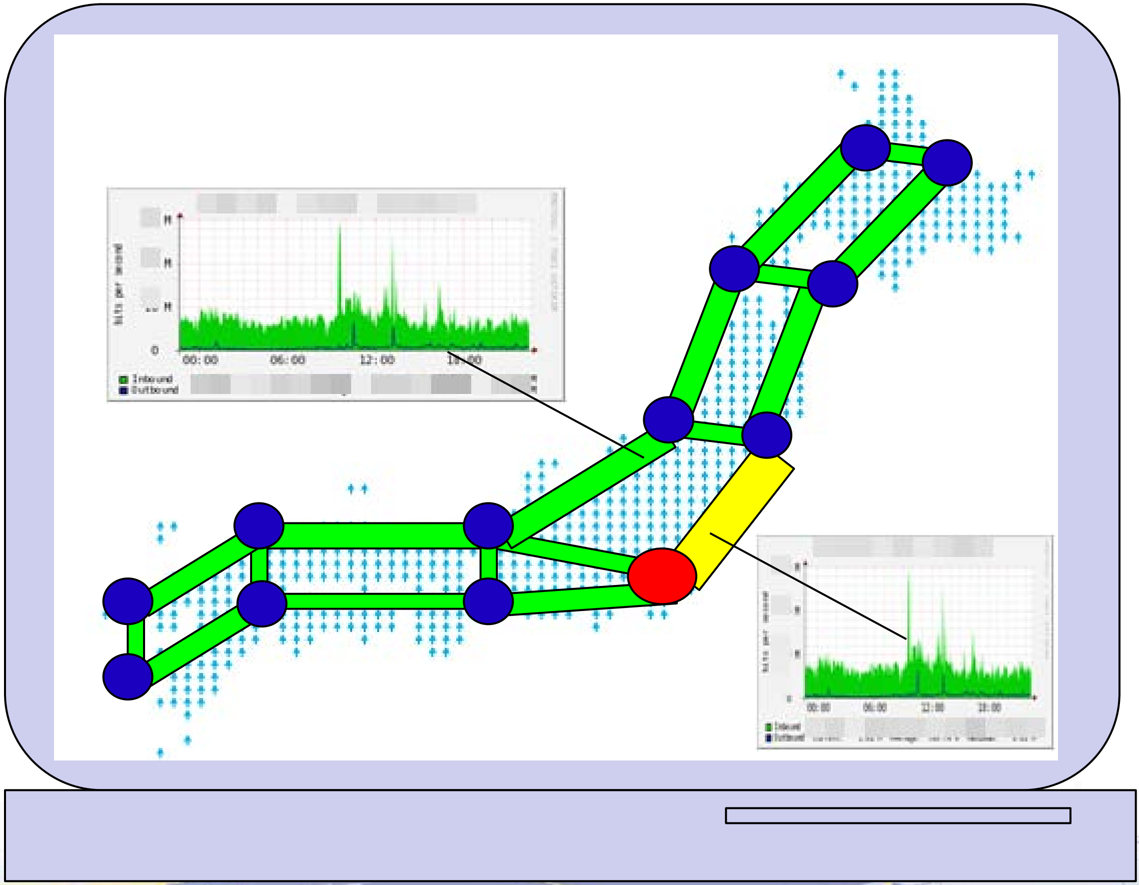


Looking at Traffic on Routing Topology leads to far better/fast understanding.

Our Goal

Our Goal:

Monitoring Traffic on Routing Topology



Better View

Easy Operation

Fast Trouble Shooting

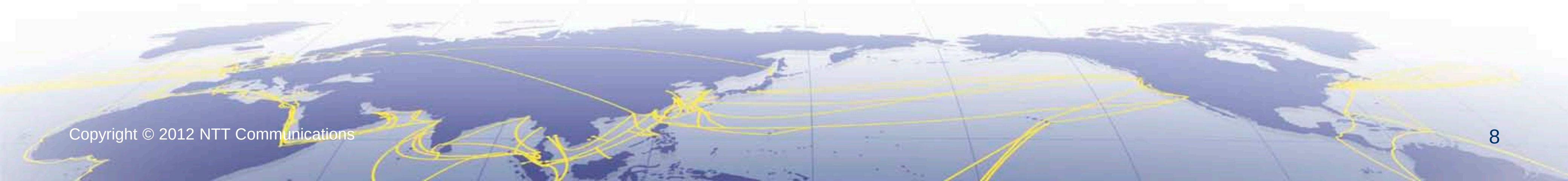
Things to Consider

- Routing Topology changes dynamically
- Routing Topology may differ between internal network and external network
- Routing Topology may differ between IPv4 and IPv6

- Monitor routing protocol continuously as well as Monitor Flow Traffic
- Monitor separate routing protocol for internal/external network
- Monitor separate routing protocol for IPv4/IPv6 network

Routing Protocol to be Monitored

	IPv4	IPv6
Internal	OSPFv2	OSPFv3
	IS-IS	
External	BGP4	BGP4+



Monitoring Internal Routing Protocol(OSPFv2/OSPFv3)

Method	Pros and Cons
(1)Login to Router	Good: Comparably fast Little load to router Bad: Different output format by vendor, need many parser Comparably difficult to get login permission Protocol message is not possible to be monitored OSPFv3
(2)SNMP	Good: Standardized output format (Except OSPFv3) Comparably easy to get SNMP access (read-only) Bad: Load given to router Comparably slow Protocol message is not possible to be monitored OSPFv2
(3)Join Network	Good: Comparably fast A little load to router Protocol message is monitored Bad: Need protocol stack (difficult implementation) Difficult management, Topology may change by joining network

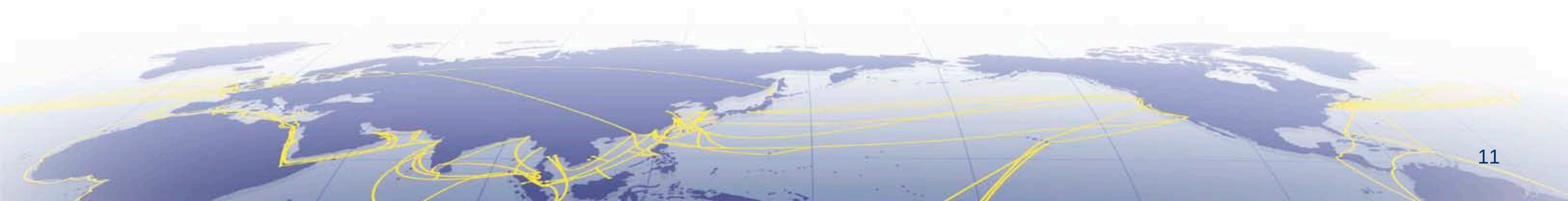
Monitoring External Routing Protocol(BGP/BGP4+)

Method	Pros and Cons
(1)Login to Router	Good: Comparably fast Little load to router Bad: Different output format by vendor, need many parser Comparably difficult to get login permission Protocol message is not possible to be monitored
(2)SNMP	Good: Comparably easy to get SNMP access Bad: Vendor-specific MIB Load given to router Comparably slow Protocol message is not possible to be monitored
(3)Join Network	Good: Comparably fast A little load to router Protocol message is monitored Easy management Bad: Need protocol stack (difficult implementation) BGP BGP4+

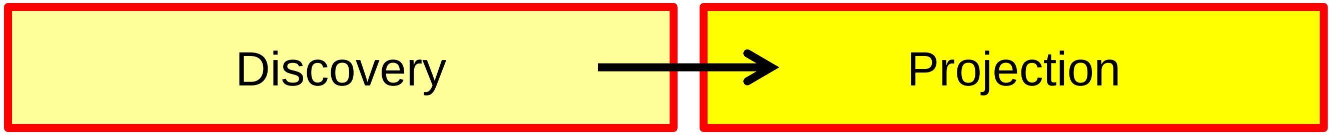
Flow Technology for Traffic Monitoring

		IPv4	IPv6
Netflow	Version 5	OK	NG
	Version 9	OK	OK
sFlow	Version 2	OK	OK
	Version 4	OK	OK
	Version 5	OK	OK
IPFIX		OK	OK

Recent Flow technologies can handle IPv6 traffic information.

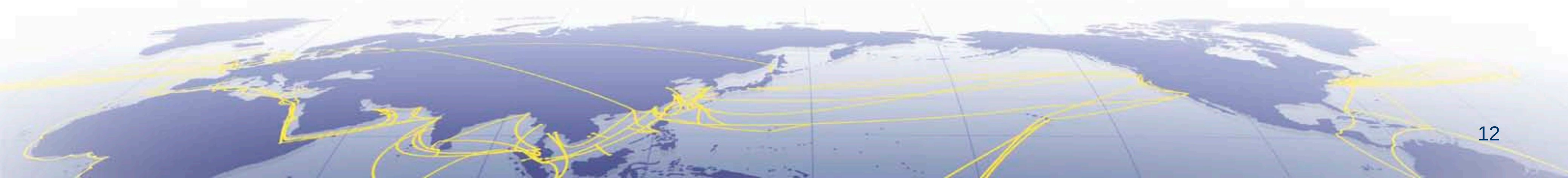


Visualizing Process

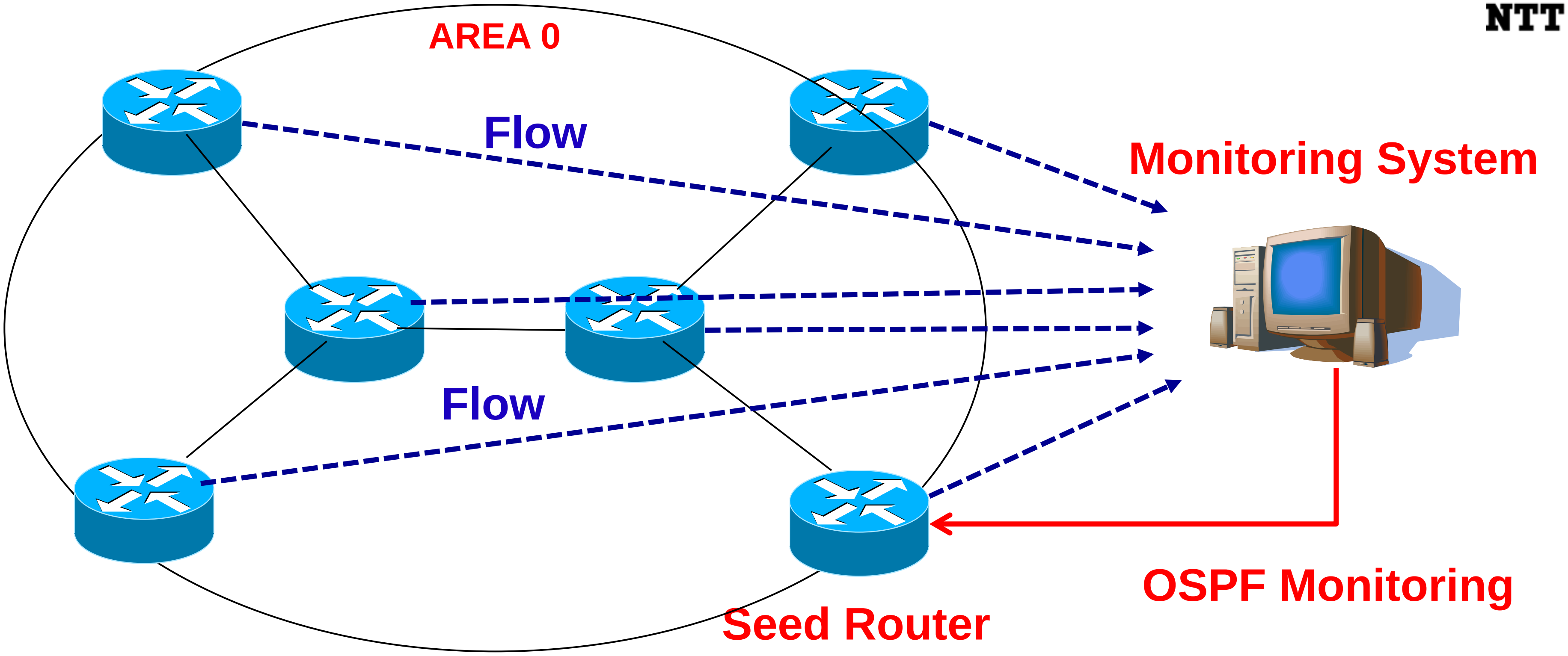

Discovery

Projection

		Discovery	Projection
		Monitor **Routing Protocol**	Monitor **Flow**
Internal	**IPv4** **IPv6**	- Analyze OSPF/OSPFv3 Link State Database - Enumerate all interfaces of Network Links	- Extract Flow of specified interface - Calculate Interface Traffic, then map onto links
External	**IPv4** **IPv6**	- Analyze BGP/BGP4+ Routing Table and Attributes - Enumerate all AS Path by Origin AS	- Extract Origin AS for each flow - Calculate Traffic for each origin AS, then map onto AS Path

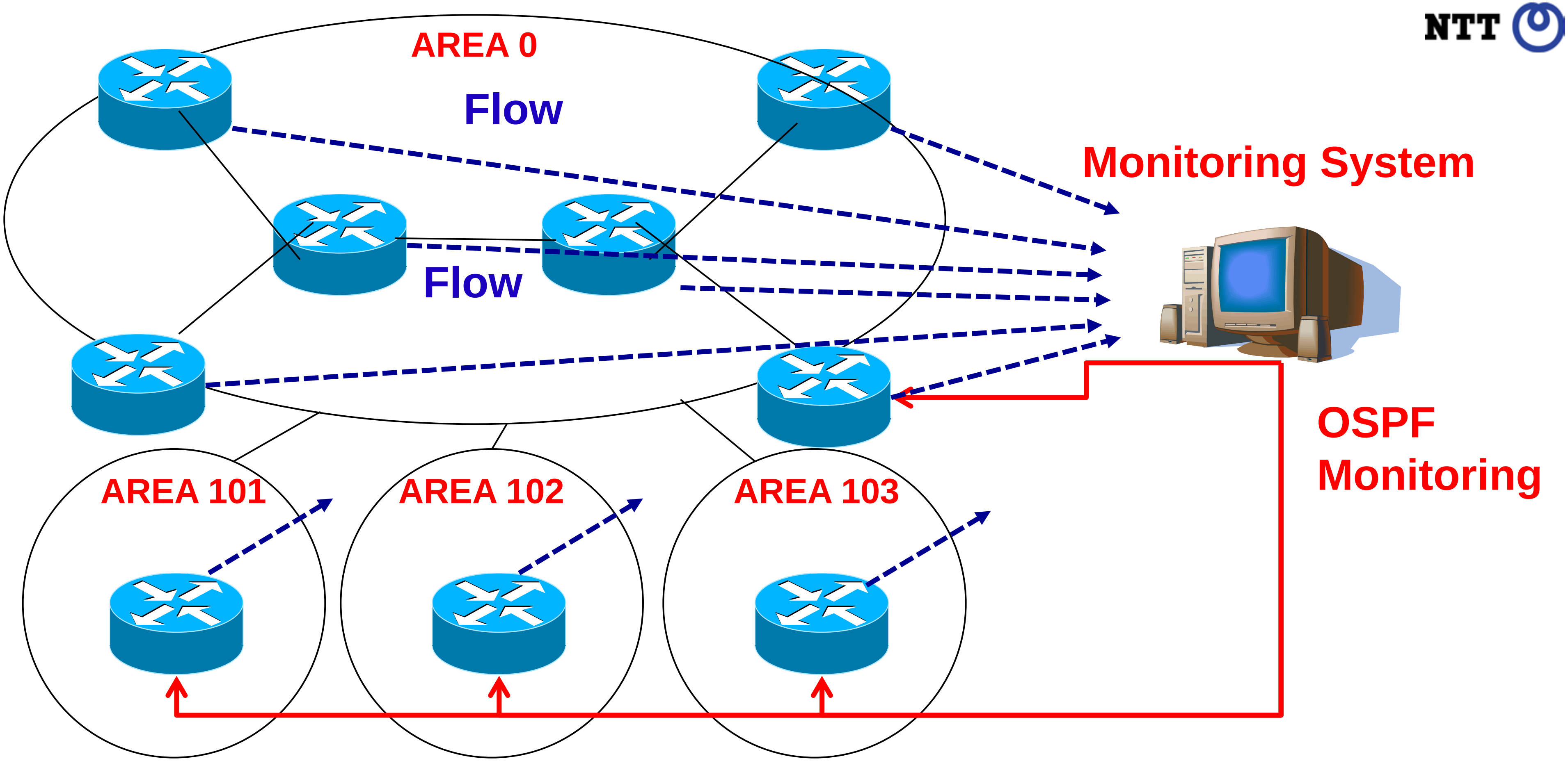


Monitoring System (Internal Topology)



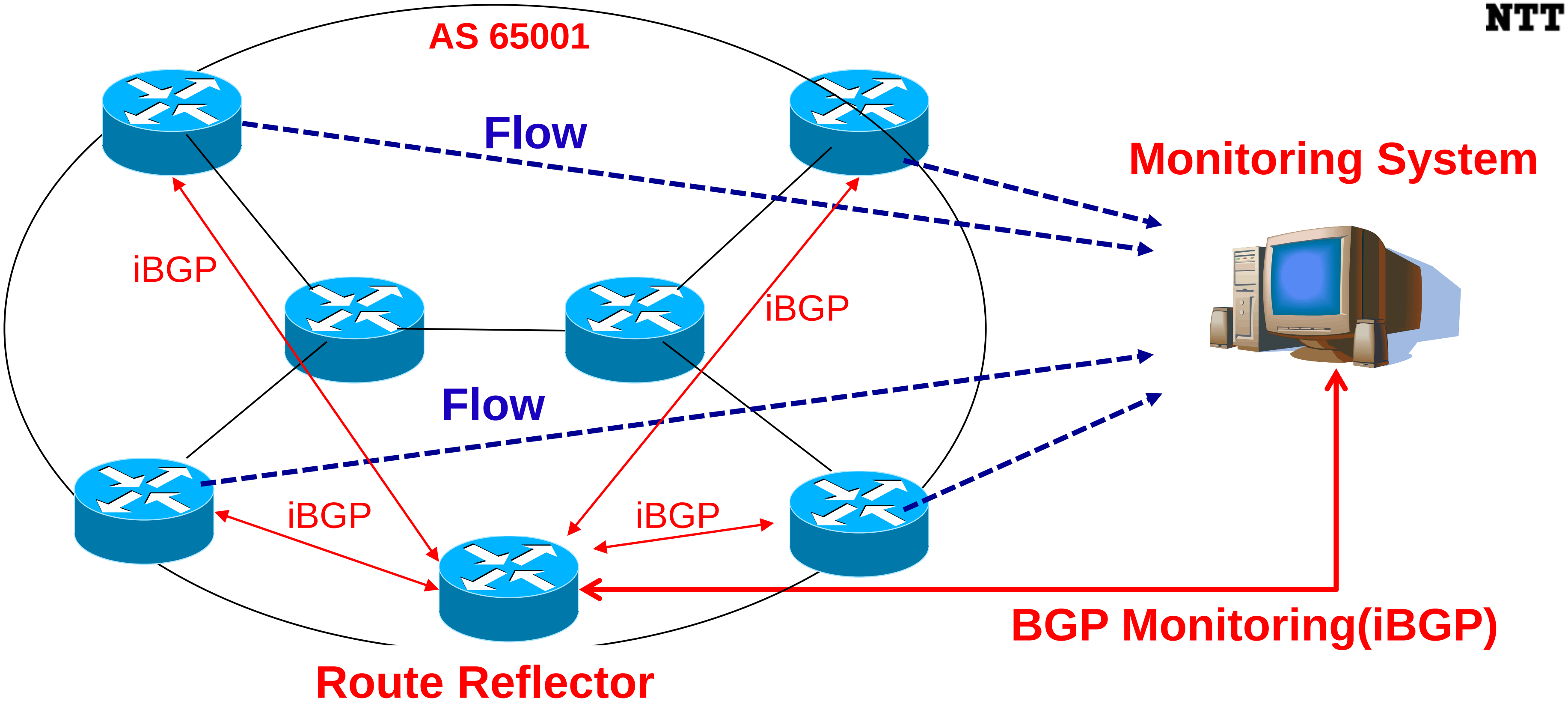
- All routers send Flow to Monitoring System
- System monitors OSPF link state database on one of the routers

Monitoring System (Internal Topology) cont’d



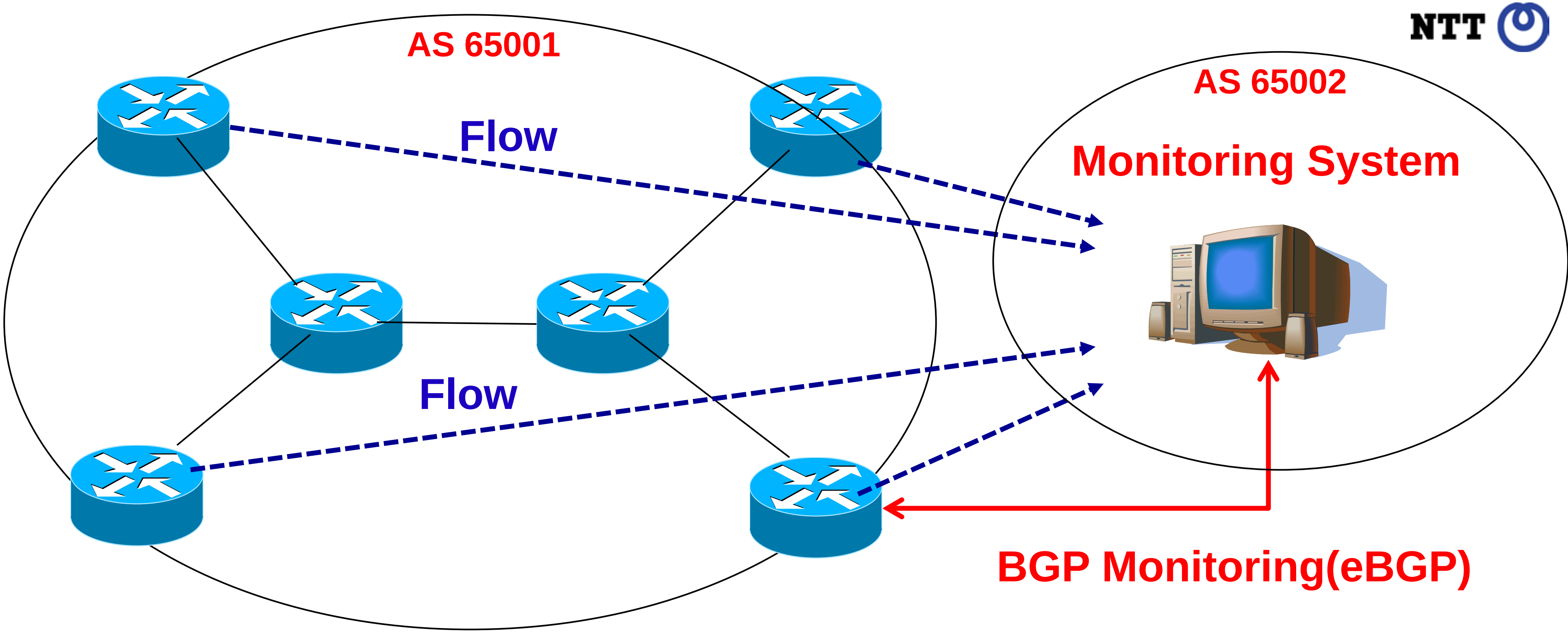
- All routers send Flow to Monitoring System
- System monitors OSPF link state database on one of the **routers in Each AREA**

Monitoring System (External Topology)



- Edge routers send Flow to Monitoring System
- System monitors BGP routing table by iBGP peer with Route Reflector

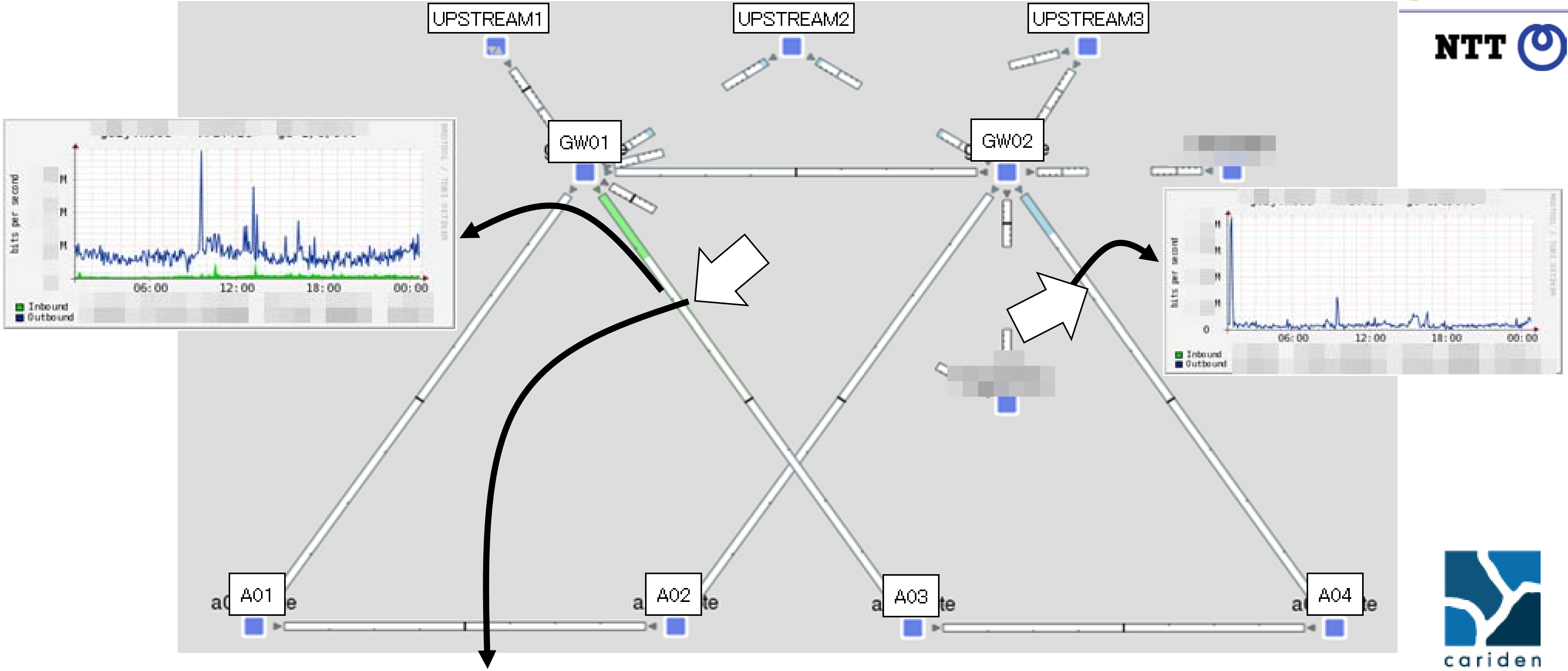
Monitoring System (External Topology) cont'd

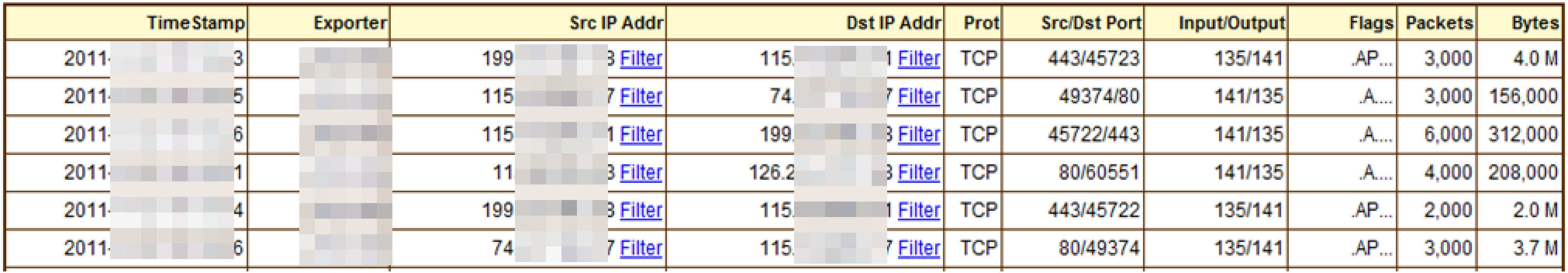


- Edge routers send Flow to Monitoring System

-System monitors BGP routing table by eBGP peer with one of the Edge router

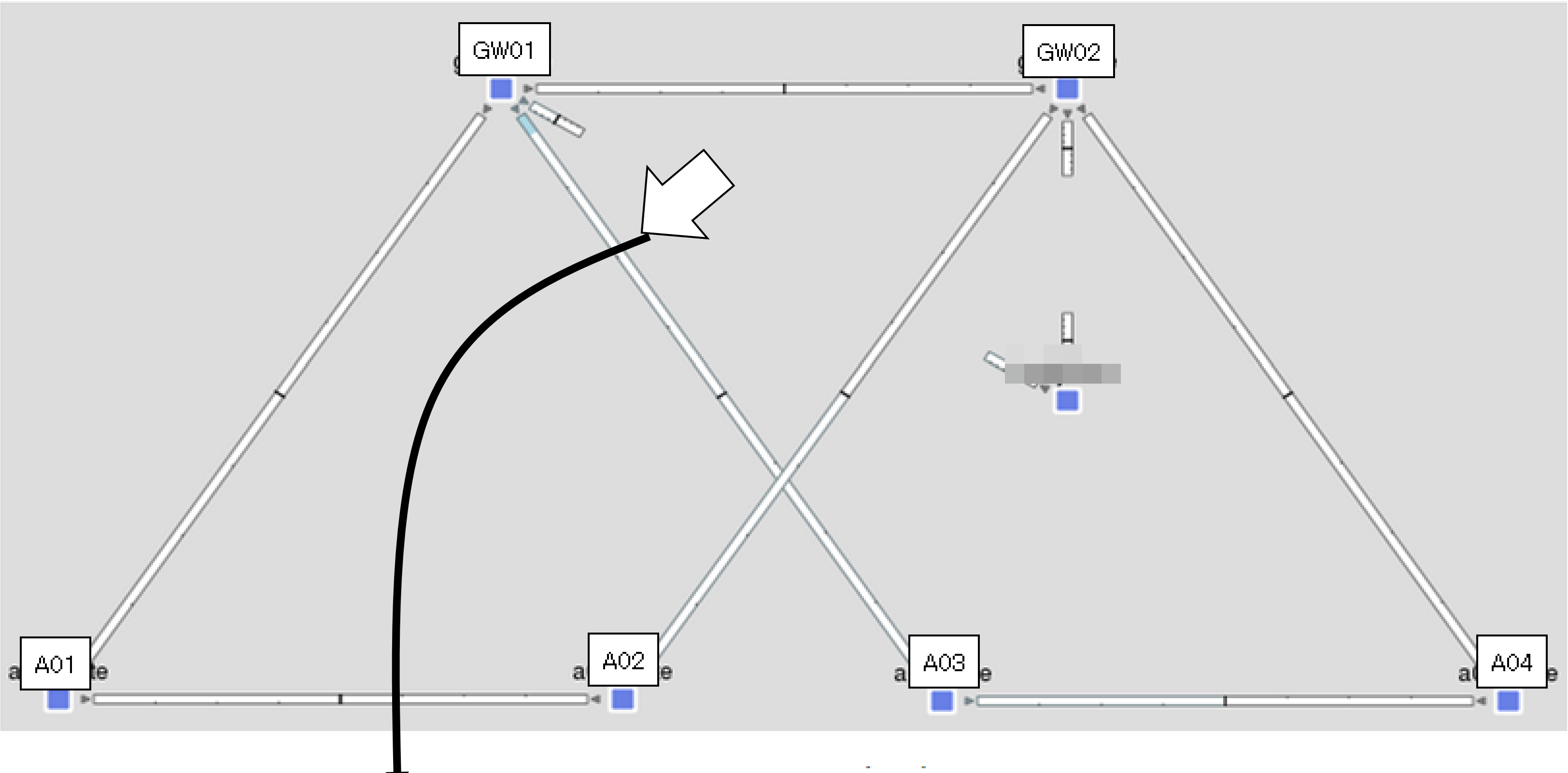
Visualization Example – Internal IPv4

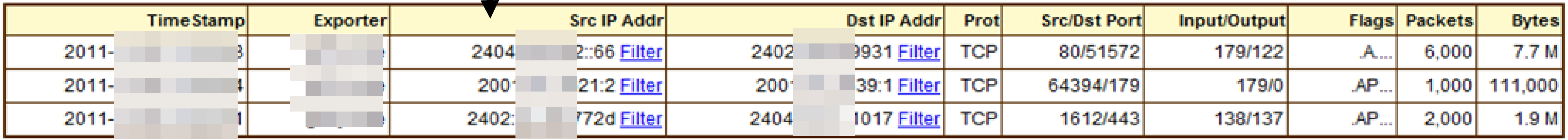




Time Stamp	Exporter	Src IP Addr	Dst IP Addr	Prot	Src/Dst Port	Input/Output	Flags	Packets	Bytes
2011[redacted]3	[redacted]	199[redacted]3 Filter	115[redacted]1 Filter	TCP	443/45723	135/141	.AP...	3,000	4.0 M
2011[redacted]5	[redacted]	115[redacted]7 Filter	74[redacted]7 Filter	TCP	49374/80	141/135	.A....	3,000	156,000
2011[redacted]6	[redacted]	115[redacted]1 Filter	199[redacted]3 Filter	TCP	45722/443	141/135	.A....	6,000	312,000
2011[redacted]1	[redacted]	11[redacted]3 Filter	126.2[redacted]3 Filter	TCP	80/60551	141/135	.A....	4,000	208,000
2011[redacted]4	[redacted]	199[redacted]3 Filter	115[redacted]1 Filter	TCP	443/45722	135/141	.AP...	2,000	2.0 M
2011[redacted]6	[redacted]	74[redacted]7 Filter	115[redacted]7 Filter	TCP	80/49374	135/141	.AP...	3,000	3.7 M

Visualization Example – Internal IPv6





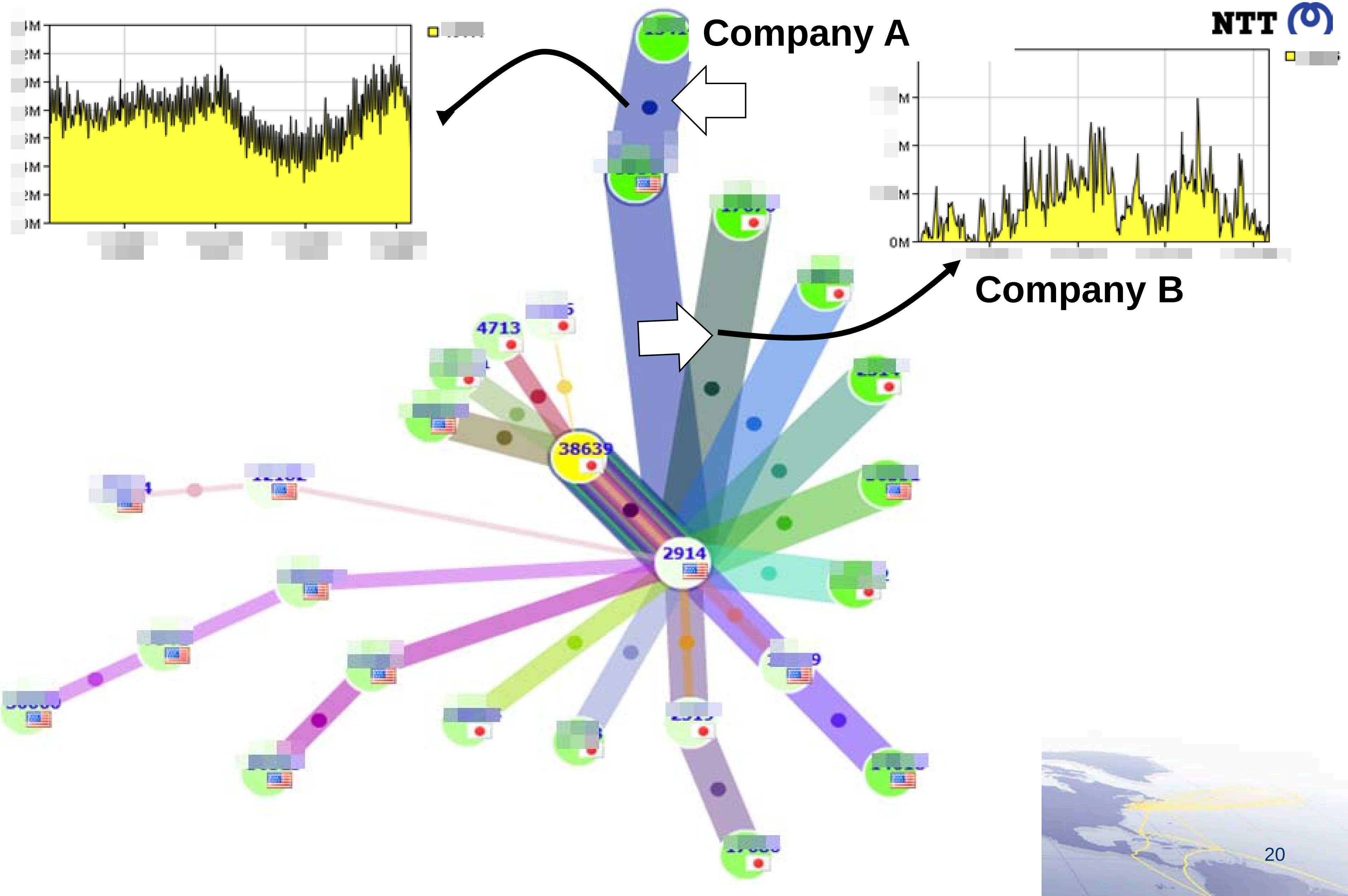
Time Stamp	Exporter	Src IP Addr	Dst IP Addr	Prot	Src/Dst Port	Input/Output	Flags	Packets	Bytes
2011-[redacted]3	[redacted]	2404[redacted]2::66 Filter	2402[redacted]9931 Filter	TCP	80/51572	179/122	.A....	6,000	7.7 M
2011-[redacted]4	[redacted]	200[redacted]21:2 Filter	200[redacted]39:1 Filter	TCP	64394/179	179/0	.AP...	1,000	111,000
2011-[redacted]1	[redacted]	2402:[redacted]72d Filter	2404[redacted]1017 Filter	TCP	1612/443	138/137	.AP...	2,000	1.9 M

Same Topology as IPv4, Far less traffic

Use Case – Failover Detection

Demonstration Onsite

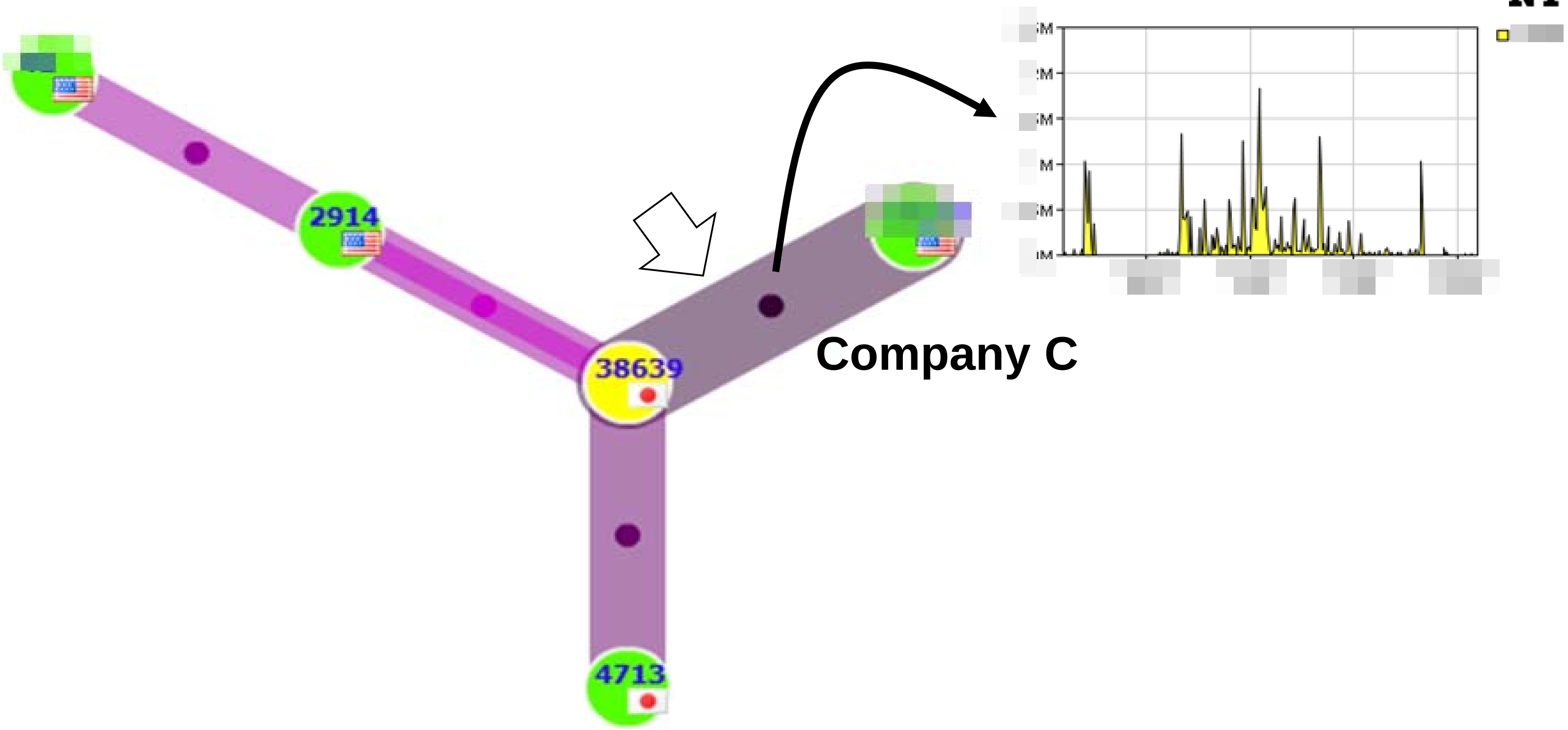
Visualization Example – External IPv4



Company A

Company B

Visualization Example – External IPv6



Company C

Far less traffic than IPv4

Use Case – AS Path Change Detection

Demonstration Onsite

Future Work

- Automation
  - Detect Interface Failover
  - Detect AS-Path Change,,,etc
  - Detect Asymmetric Routing
- Monitor other IP routing protocols
  - IS-IS
  - Static
- Monitor other layers
  - MPLS
  - L2, VLAN, Static Network
  - L1

Conclusion

- Successful in visualizing traffic on routing topology
  - Monitor routing protocol as well as flow
- Different routing protocol must be monitored depending on what kind of network to visualize (internal/external, ipv4/ipv6)
- Topology visualization is useful for
  - Better view
  - Easy operation
  - Fast trouble shooting