

# IO Visor-based Packet Tracing and Collection over Distributed SmartX Server-Switch Boxes

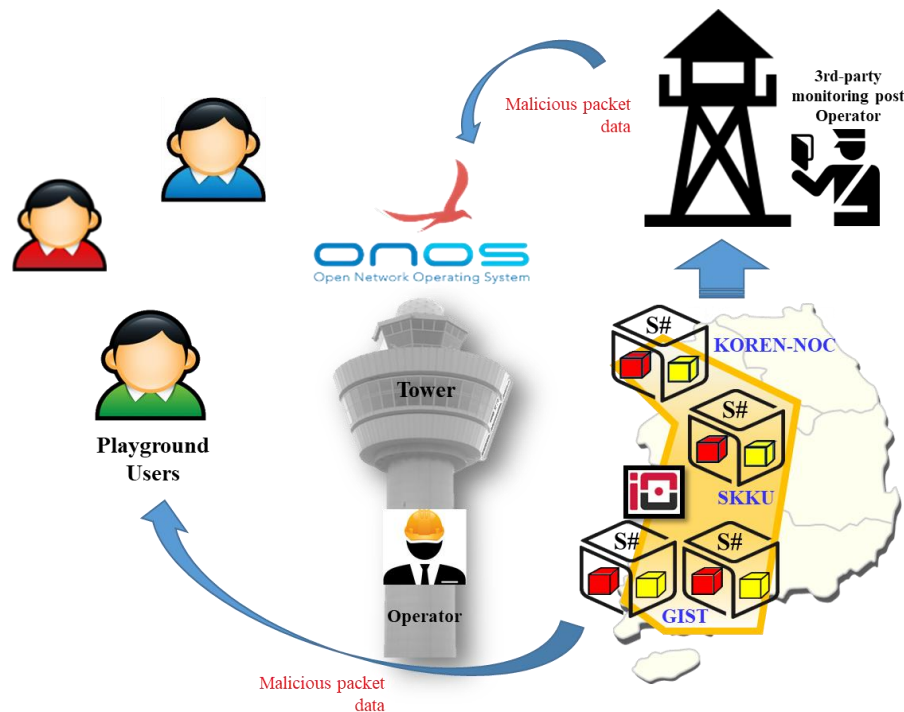
Jungi Lee, Taekho Nam,  
Aris Cahyadi Risdianto, and JongWon Kim  
thnam@nm.gist.ac.kr

Networked Computing Systems Lab.,  
School of Electrical Engineering and Computer Science,  
Gwangju Institute of Science and Technology (GIST)

# Contents

- Introduction: Background and Motivation
- Playground with Distributed Cloud-ready Boxes
- Layer 2 and Layer 3 Inter-Connections  
for distributed Cloud-ready Boxes
- IO Visor-based Packet Tracing and Collection
- Conclusion

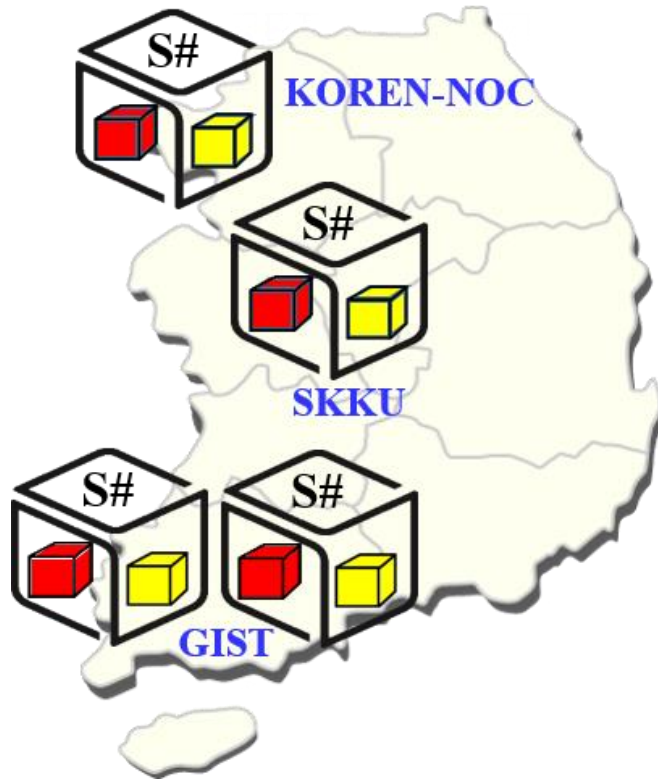
# Introduction: Background and Motivation



- Multiple cloud-ready SmartX Server-Switch boxes (i.e., SmartX Box Type S#) are deployed over KOREN (Korea Advanced Research Network).
- How to inter-connect distributed resource boxes to provide an environment for running application and/or services?
- How to provide flexible provisioning of L2/L3 Inter-connection between boxes?
- How to control and secure the distributed resource boxes at the center?

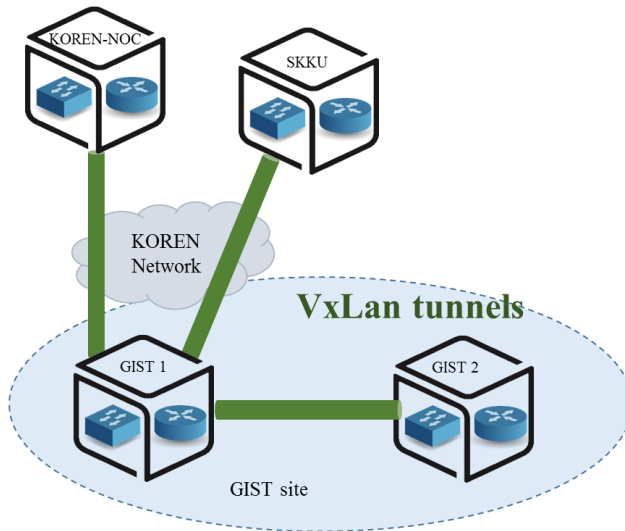
# Playground with Distributed SmartX Server-Switch Boxes

- Znyx B1 Server-Switch: Specification



Switch Environment	Znyx B1
Processor Family	Intel® Xeon® E5-2600v2
Switch Fabric	Up to 480Gbps throughput
External Interfaces	(24) 1G/10G supporting copper and fiber (SFP/SFP+)
Software Support	OpenArchitect® 4.0 - Ubuntu LTS with KVM
Protocol Support	Quagga L3 Protocol Suite & etc...

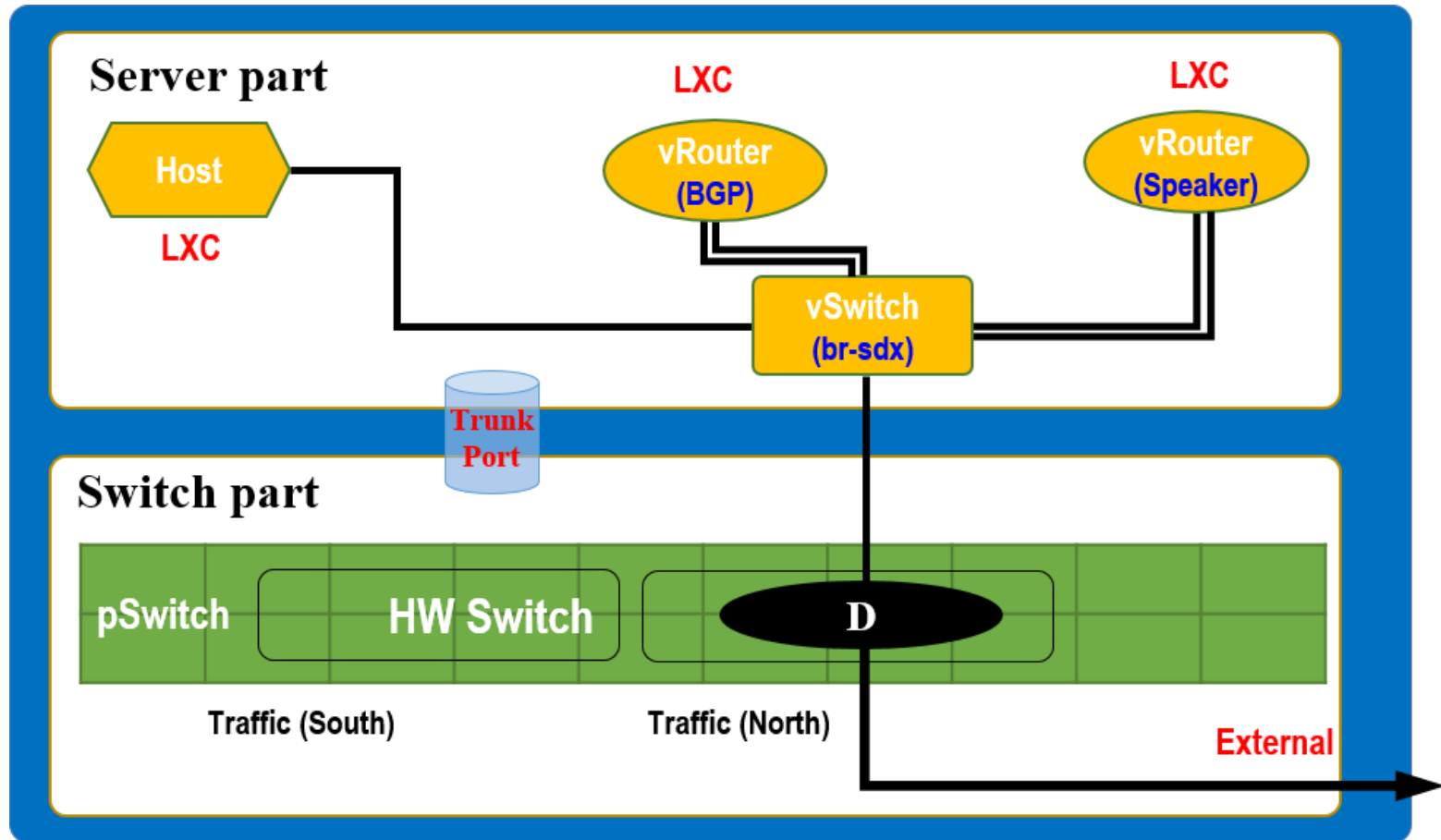
# Layer 2 and Layer 3 Inter-Connections for distributed Cloud-ready Boxes



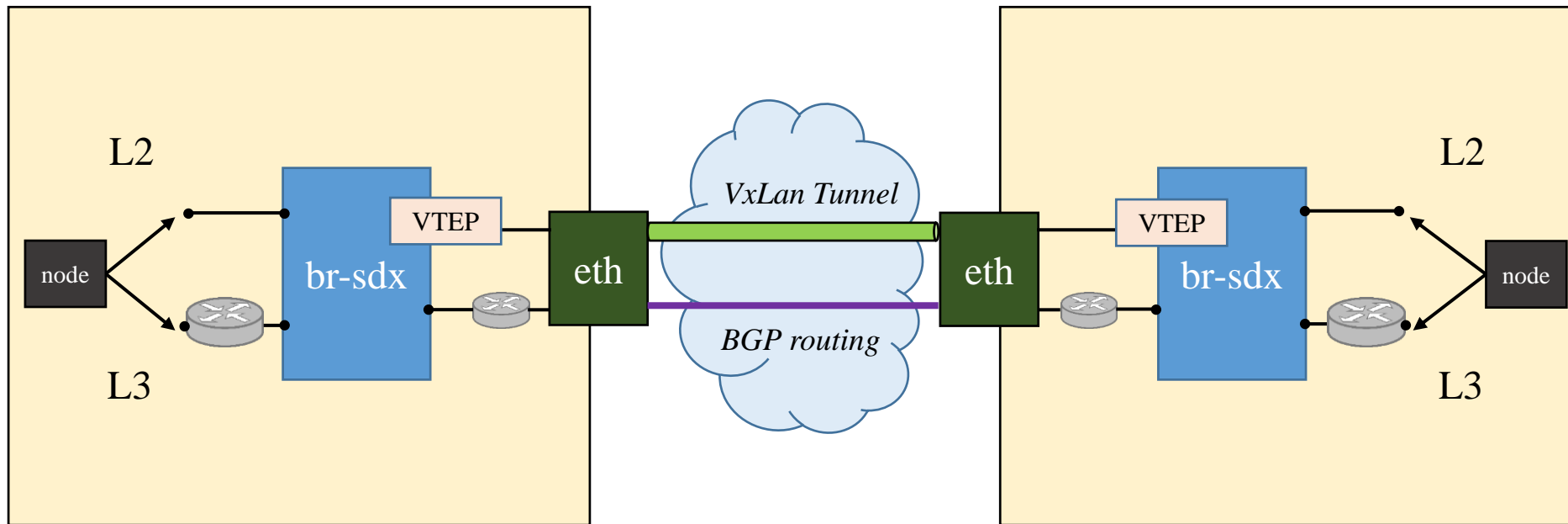
	How to find the path	How to use
L2 (VXLAN)	Multi-cast between VTEPs (Vxlan Tunnel End Points)	Connect VM/Container with <b>vSwitch</b>
L3 (BGP)	BGP routing	Connect VM/Container with <b>vRouter</b>

- In case of L2 inter-connection, VXLAN tunneling can be used to implement inter-connection between boxes in the form of overlay networking regardless of the actual physical network environment.
- In the case of L3 inter-connect, virtual router and virtual switch are used inside the cloud-ready box to support L3 routing of nodes inside the box.

# L3 Inter-Connection: Design and Implementation inside Server-switch Box

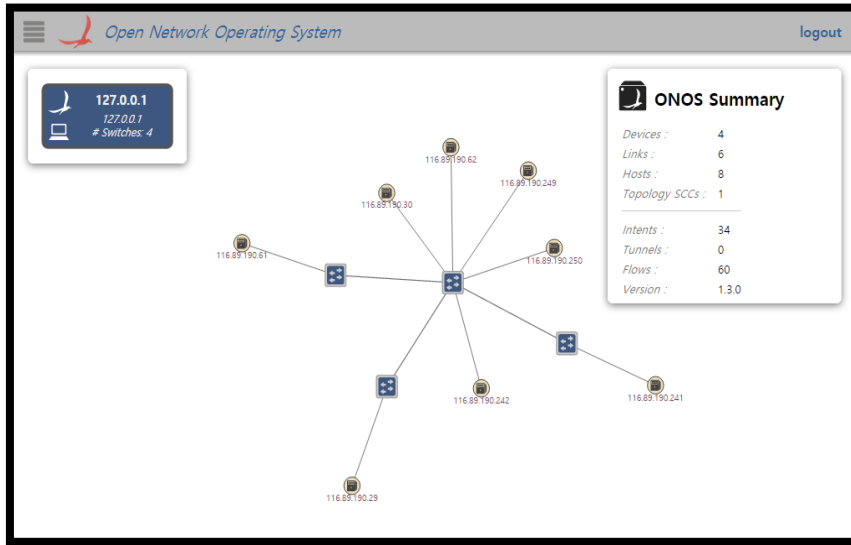


# Flexible L2/L3 Inter-Connections Over Distributed Server-Switch Boxes



- VxLan allows L2 connections between nodes with overlay network
- BGP L3 connection allows BGP routing between nodes

# Preliminary Implementation and Verifications



- Network Topology

Open Network Operating System

Intents (34 total)

Application ID	Key	Type	Priority	State
13 : org.onosproject.sdnip	116.89.190.244/30	MultiPointToSinglePointIntent	250	Withdrawn
(No resources for this intent)				
Details: Selector: [ETH_TYPE(ethType=ipv4), IPV4_DST(ip=116.89.190.244/30)]Treatment: [ETH_DST(mac=00:16:3E:49:86:81)]Constraints: [org.onosproject.net.intent.constraint.PartialFailureConstraint@78a1b2d] Ingress=of:0000000000000002/1 of:0000000000000003/1 of:0000000000000004/1 of:0000000000000001/5 of:0000000000000002/3, Egress=of:0000000000000001/4				
13 : org.onosproject.sdnip	116.89.190.24/30	MultiPointToSinglePointIntent	250	Withdrawn
(No resources for this intent)				
Details: Selector: [ETH_TYPE(ethType=ipv4), IPV4_DST(ip=116.89.190.24/30)]Treatment: [ETH_DST(mac=00:16:3E:49:86:81)]Constraints: [org.onosproject.net.intent.constraint.PartialFailureConstraint@78a1b2d] Ingress=of:0000000000000002/1 of:0000000000000003/1 of:0000000000000004/1 of:0000000000000001/5 of:0000000000000002/3, Egress=of:0000000000000001/4				
13 : org.onosproject.sdnip	116.89.190.56/30	MultiPointToSinglePointIntent	250	Withdrawn
(No resources for this intent)				
Details: Selector: [ETH_TYPE(ethType=ipv4), IPV4_DST(ip=116.89.190.56/30)]Treatment: [ETH_DST(mac=00:16:3E:C2:64:00)]Constraints: [org.onosproject.net.intent.constraint.PartialFailureConstraint@78a1b2d] Ingress=of:0000000000000002/1 of:0000000000000003/1 of:0000000000000004/1 of:0000000000000001/5 of:0000000000000002/3, Egress=of:0000000000000001/4				
13 : org.onosproject.sdnip	116.89.190.236/30	MultiPointToSinglePointIntent	250	Withdrawn
(No resources for this intent)				
Details: Selector: [ETH_TYPE(ethType=ipv4), IPV4_DST(ip=116.89.190.236/30)]Treatment: [ETH_DST(mac=00:16:3E:C0:8D:20)]Constraints: [org.onosproject.net.intent.constraint.PartialFailureConstraint@78a1b2d] Ingress=of:0000000000000002/1 of:0000000000000003/1 of:0000000000000004/1 of:0000000000000001/5 of:0000000000000002/3, Egress=of:0000000000000001/4				
13 : org.onosproject.sdnip	0x600011	PointToPointIntent	1000	Installed
(No resources for this intent)				
Details: Selector: [ETH_TYPE(ethType=ipv4), IP_PROTOCOL(protocol=1), IPV4_DST(ip=116.89.190.62/32), IPV4_SRC(ip=116.89.190.61/32)] Ingress: of:0000000000000004/1, Egress: of:0000000000000001/10				
13 : org.onosproject.sdnip	0x600002	PointToPointIntent	1000	Installed
(No resources for this intent)				
Details: Selector: [TCP_DST(tcpPort=179), ETH_TYPE(ethType=ipv4), IP_PROTOCOL(protocol=6), IPV4_DST(ip=116.89.190.253/32), IPV4_SRC(ip=116.89.190.254/32)] Ingress: of:0000000000000001/5, Egress: of:0000000000000001/2				

- L3 Routing rules

Open Network Operating System

Devices (4 total)

Device ID	Master Instance	Ports	Vendor	W/P Version
of:0000000000000001	127.0.0.1	11	Nicira, Inc	Open vSwitch
of:0000000000000002	127.0.0.1	8	Nicira, Inc	Open vSwitch
of:0000000000000003	127.0.0.1	8	Nicira, Inc	Open vSwitch
of:0000000000000004	127.0.0.1	8	Nicira, Inc	Open vSwitch

of:0000000000000001

Type: Switch Vendor: Nicira, Inc  
Master ID: 127.0.0.1 W/P Version: Open vSwitch  
Channel ID: 1 W/P Version: 2.4.0  
Protocol: DP\_13  
Serial #: None

Ports

Enabled	ID	Speed	Type	Egress Links	Name
false	Local	0	Copper		br-nd1
true	1	10	Copper		speaker1.1
true	2	10	Copper		speaker1.2
true	3	10	Copper		speaker1.3
true	4	10	Copper		router1.1
true	5	10	Copper		gateway1.1
true	6	10	Copper	of:0000000000000002/2	eth2
true	7	0	Copper	of:0000000000000003/2	VOLAN_GIG725KIU
true	8	0	Copper	of:0000000000000004/2	VOLAN_GIG72XORE
true	9	10	Copper		speaker1.4
true	10	10	Copper		speaker1.5

- The port information inside each box.

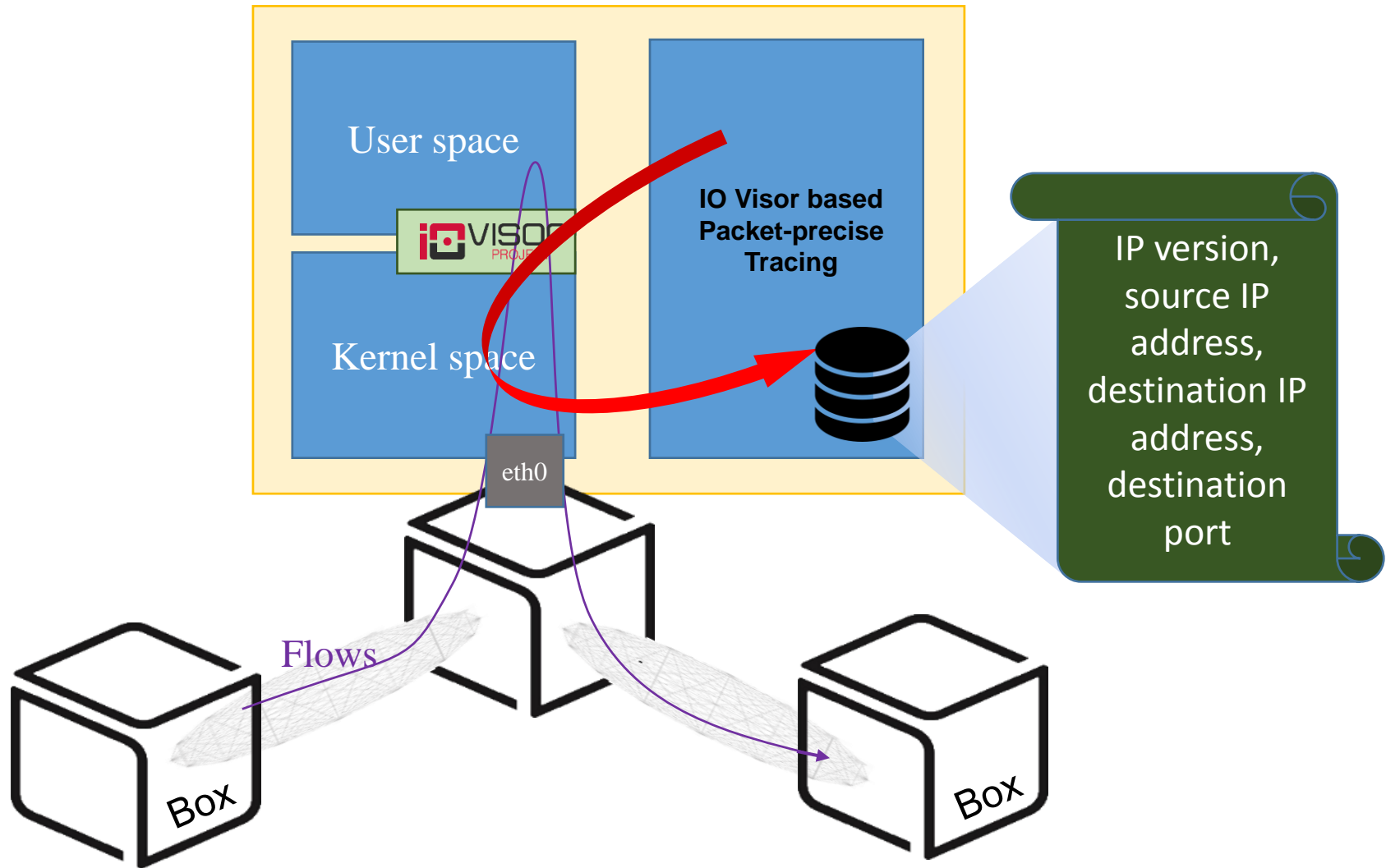


# Packet Tracing/Collection with IO Visor for Secured Inter-Connection

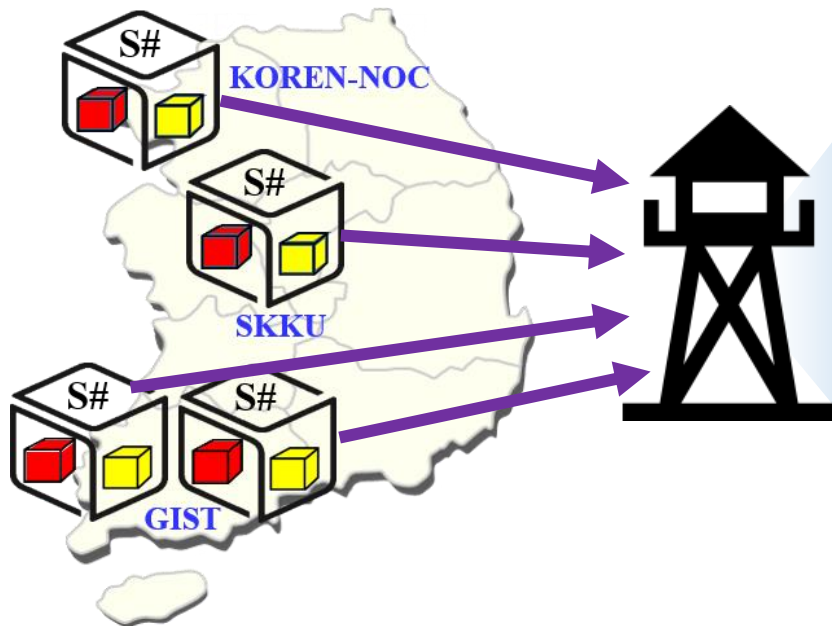
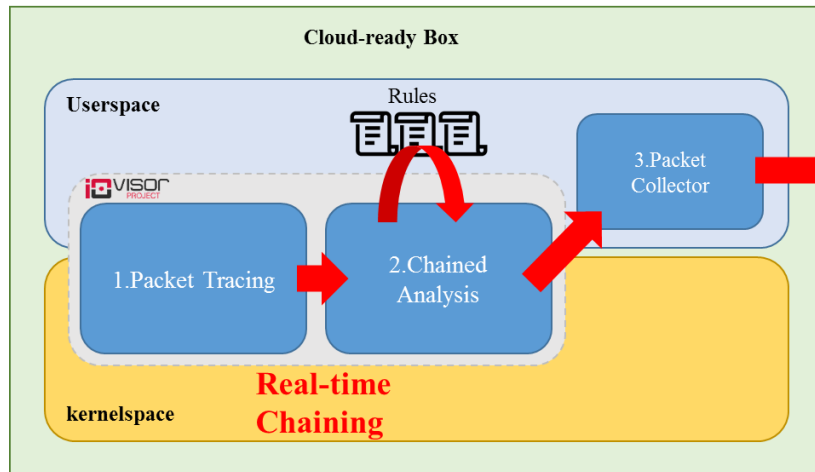
- IO Visor?
  - IO Visor is an open-source collaborative project designed to accelerate the innovation, development and sharing of virtualized kernel I/O services for many networking-related functions.
  - IO Visor can be effectively exploited in many areas that include networking, security, and tracing. Specifically for packet tracing functionality, it utilizes a BCC (BPF Compiler Collection) to implement IO Visor-based I/O-level packet tracing.



# Design: IO Visor-based Packet Tracing and Collection



# Implementation and Verifications of IO Visor-based Packet Tracing/Collection



3rd-Party  
Monitoring Post

```
GNU nano 2.2.6 File: gist1.txt
Suspicious Packets on SmartX Box Type S - GIST 1
2017-06-21 10:40:52.874497 4 116.89.190.193 203.237.53.71 192
2017-06-21 10:40:53.989903 4 203.237.53.71 116.89.190.193 22
2017-06-21 10:40:54.386266 4 116.89.190.193 37.218.240.68 80
2017-06-21 10:42:17.213728 4 116.89.190.193 140.205.94.189 80
2017-06-21 10:43:02.714445 4 116.89.190.193 37.218.240.68 80
2017-06-21 10:47:57.844628 4 116.89.190.193 37.218.240.68 80
2017-06-21 10:47:59.258018 4 37.218.240.68 116.89.190.193 156
2017-06-21 10:48:09.393483 4 116.89.190.193 140.205.94.189 80
2017-06-21 10:48:09.795307 4 140.205.94.189 116.89.190.193 212
2017-06-21 10:48:28.658305 4 116.89.190.193 125.209.222.142 80
2017-06-21 10:48:29.087982 4 125.209.222.142 116.89.190.193 216
2017-06-21 10:48:30.248496 4 116.89.190.193 104.74.171.196 80
2017-06-21 10:48:30.863159 4 104.74.171.196 116.89.190.193 130
2017-06-21 10:49:54.473272 4 116.89.190.193 162.125.32.14 80
2017-06-21 10:49:54.887103 4 162.125.32.14 116.89.190.193 118
2017-06-21 10:51:25.710384 4 116.89.190.193 140.205.94.189 80
```

```
GNU nano 2.2.6 File: GIST2.txt
Suspicious Packets on SmartX Box Type S - GIST 2
2017-06-22 17:17:44.506792 4 116.89.190.195 140.205.94.189 80
2017-06-22 17:17:45.020335 4 116.89.190.195 140.205.94.189 80
2017-06-22 17:17:54.238907 4 203.237.53.71 116.89.190.195 22
2017-06-22 17:18:35.821581 4 116.89.190.195 140.205.220.96 80
2017-06-22 17:18:39.038757 4 116.89.190.195 140.205.220.96 80
2017-06-22 17:18:45.172829 4 116.89.190.195 140.205.94.189 80
```

```
GNU nano 2.2.6 File: koren.txt
Suspicious Packets on SmartX Type S - KOREN
2017-06-22 17:22:42.003652 4 140.205.220.96 116.89.190.50 216
2017-06-22 17:22:48.436376 4 140.205.94.189 116.89.190.50 4
2017-06-22 17:23:48.763336 4 140.205.94.189 116.89.190.50 30
2017-06-22 17:24:01.455707 4 37.157.196.97 116.89.190.50 156
2017-06-22 17:24:24.703698 4 140.205.220.96 116.89.190.50 24
```

```
GNU nano 2.2.6 File: SKKU.txt
Suspicious Packets on SmartX Box Type S - SKKU
2017-06-22 17:25:53.294443 4 116.89.190.18 140.205.94.189 80
2017-06-22 17:25:53.503372 4 140.205.94.189 116.89.190.18 0
2017-06-22 17:26:05.329115 4 116.89.190.18 140.205.94.189 80
2017-06-22 17:26:05.519436 4 140.205.94.189 116.89.190.18 14
```

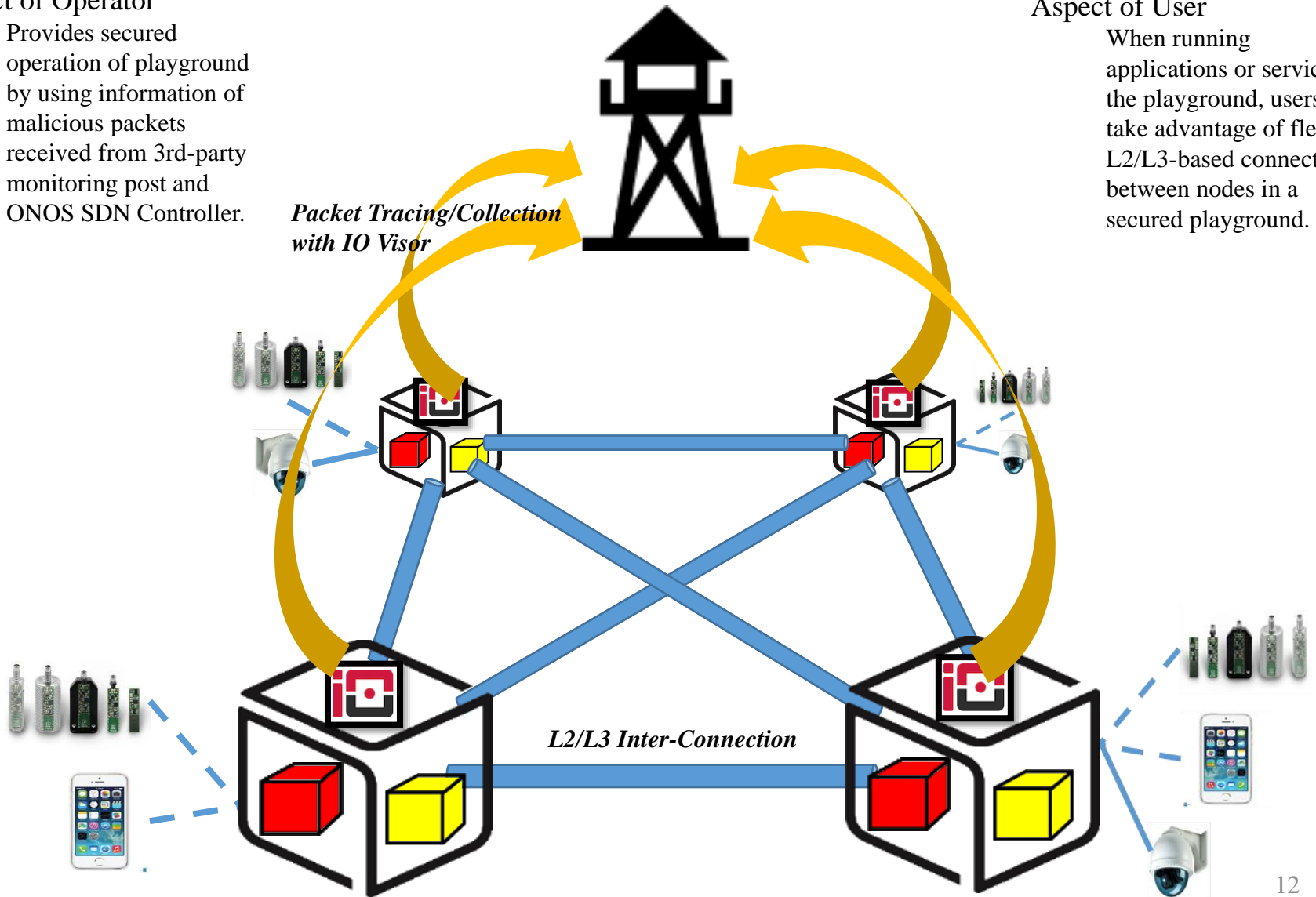
# Conclusion: IO Visor-based Packet Tracing/Collection over Distributed SmartX Server-Switch Boxes.

## Aspect of Operator

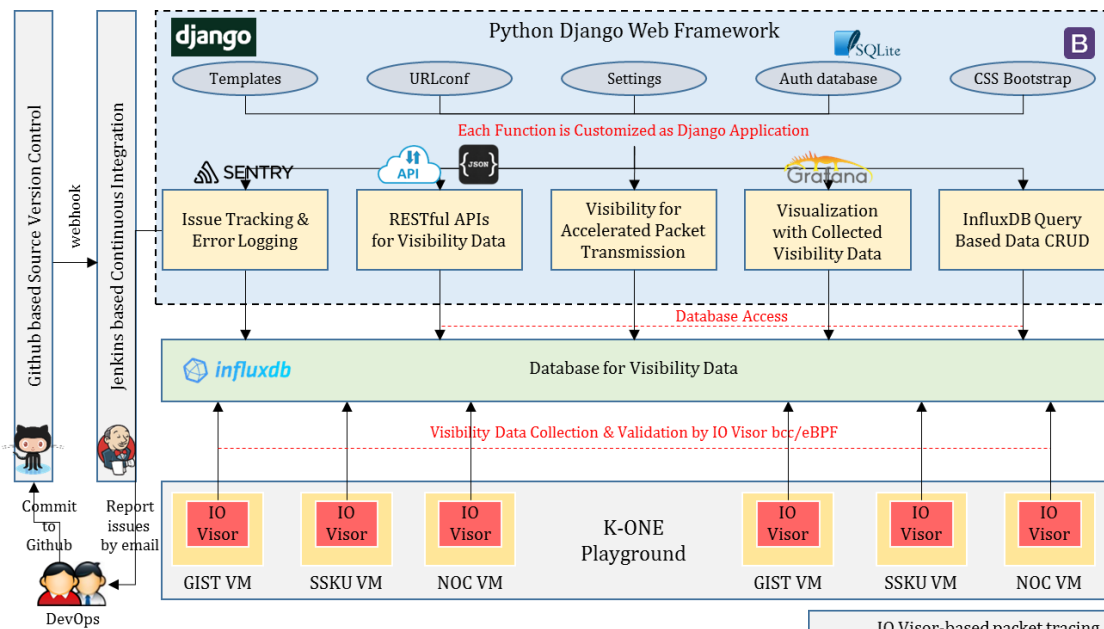
Provides secured operation of playground by using information of malicious packets received from 3rd-party monitoring post and ONOS SDN Controller.

## Aspect of User

When running applications or services in the playground, users can take advantage of flexible L2/L3-based connections between nodes in a secured playground.



# Future Works: IO Visor for Site Visibility Framework



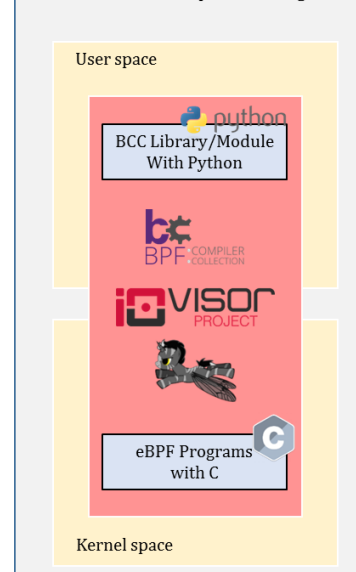
By extending the basic functionality of IO Visor-based packet tracing and collection over distributed server-switch boxes,

We re-design and develop a prototype-level site visibility framework with DevOps concept to inspect all packets passing through multiple network interfaces at the same time.

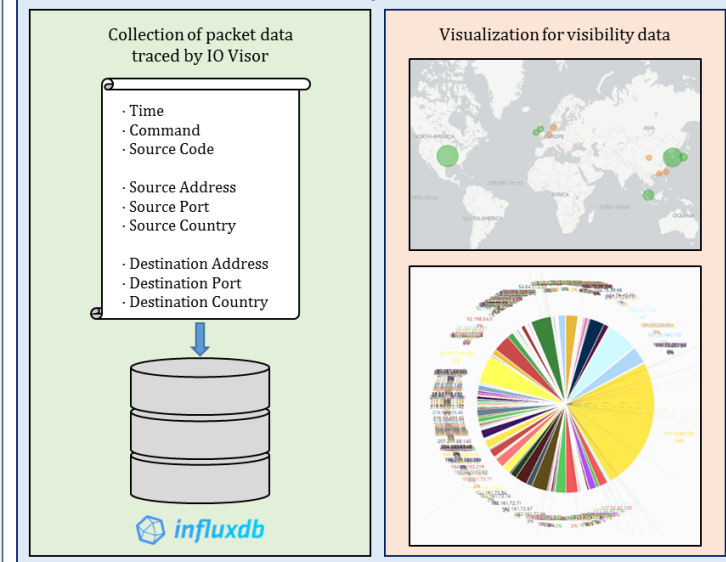
Site visibility framework is Django-based software framework that leveraging IO Visor-based packet tracing and collection.

It can support the visibility visualization of traced packets and provide associated APIs.

## IO Visor-based packet tracing



## Site Visibility Framework



**Thank You**