



Big Monitoring Fabric

Out-of-band

INFO@BIGSWITCH.COM

MENU BAR OPTIONS



DIRECTIONS

HANDS-ON LAB

REFERENCE CONFIGURATION

Guide (PDF) with
instructions for this
module

Lab Topology &
options to access the
Big Monitoring Fabric
Controller

Reference
Configuration

INTRODUCTION



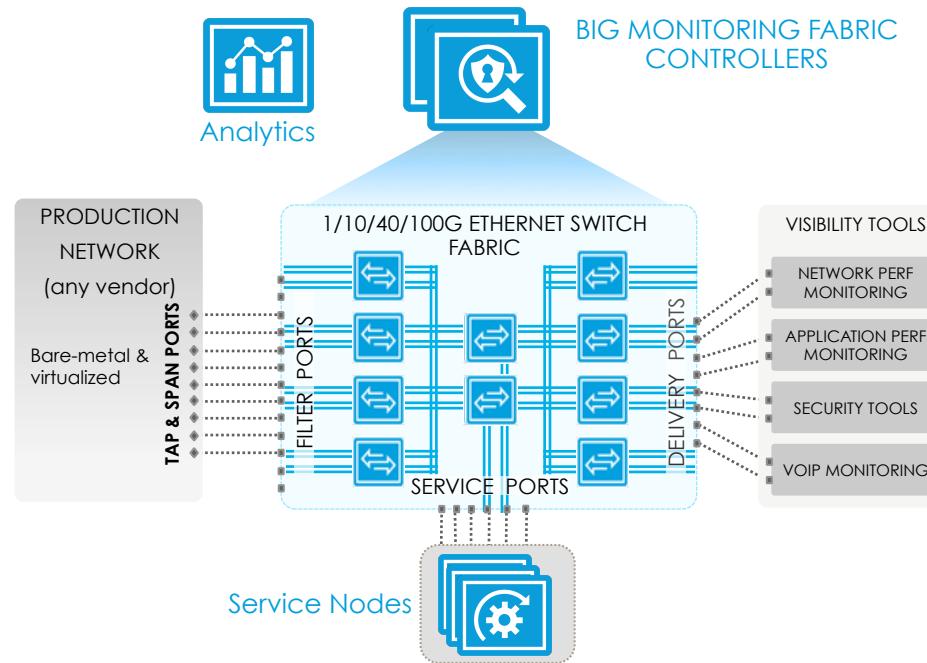
This Hands-on lab introduces Big Monitoring Fabric's out-of-band mode

- Use Big Mon's Graphical User Interface (GUI) client to
 - On-board fabric switches
 - Assign filter and delivery roles to fabric interfaces
 - Create policies to aggregate, filter and deliver traffic from SPAN/TAPs to monitoring tools
- Big Monitoring Fabric can be configured using the Controller's REST API. Internally, both the CLI and the GUI clients use the same REST API calls to configure Big Monitoring Fabric

You will be using actual software in a sandbox environment. Feel free to experiment

BIG MONITORING FABRIC INTRODUCTION

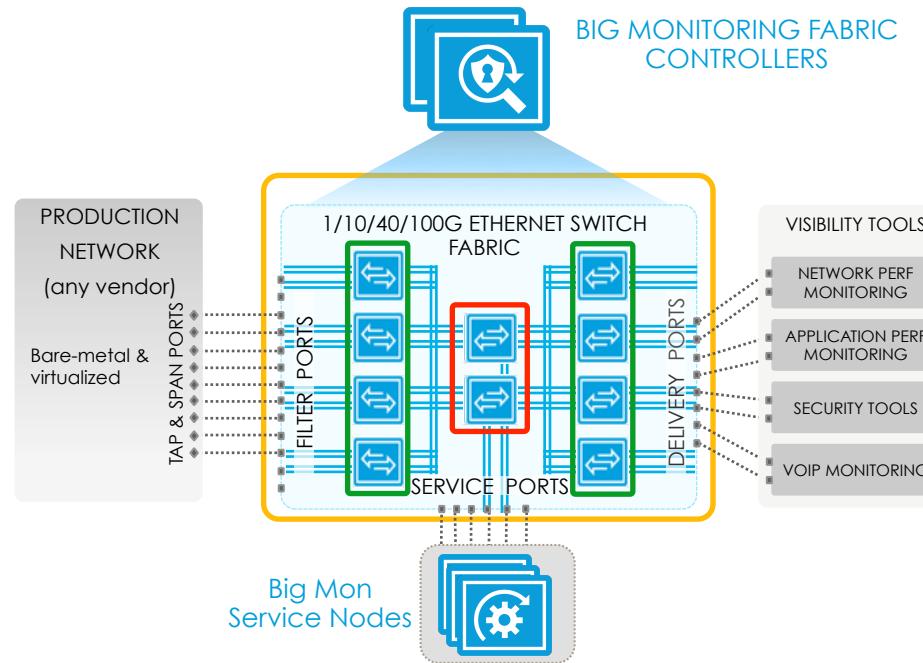
Big Monitoring Fabric out-of-band allows you to monitor all of your bare-metal and virtualized workloads, east-west traffic included, selectively delivering mirrored traffic to security, monitoring, and performance measurement tools in centralized tool farms



BIG MONITORING FABRIC BUILDING BLOCKS

Fabric scales out to admit additional SPAN/TAP & tool ports

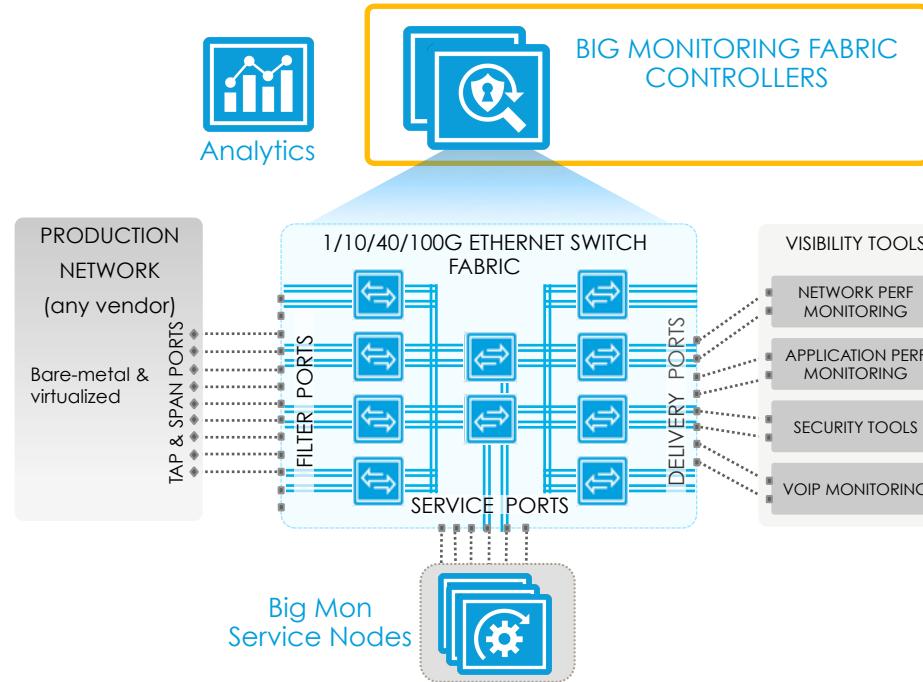
Big Mon is based on a centrally-managed **leaf-spine** fabric built out of high-performance 1/10/40/100G **Open Networking** data center switches.



BIG MONITORING FABRIC BUILDING BLOCKS

SDN-style management for unprecedented operational simplicity

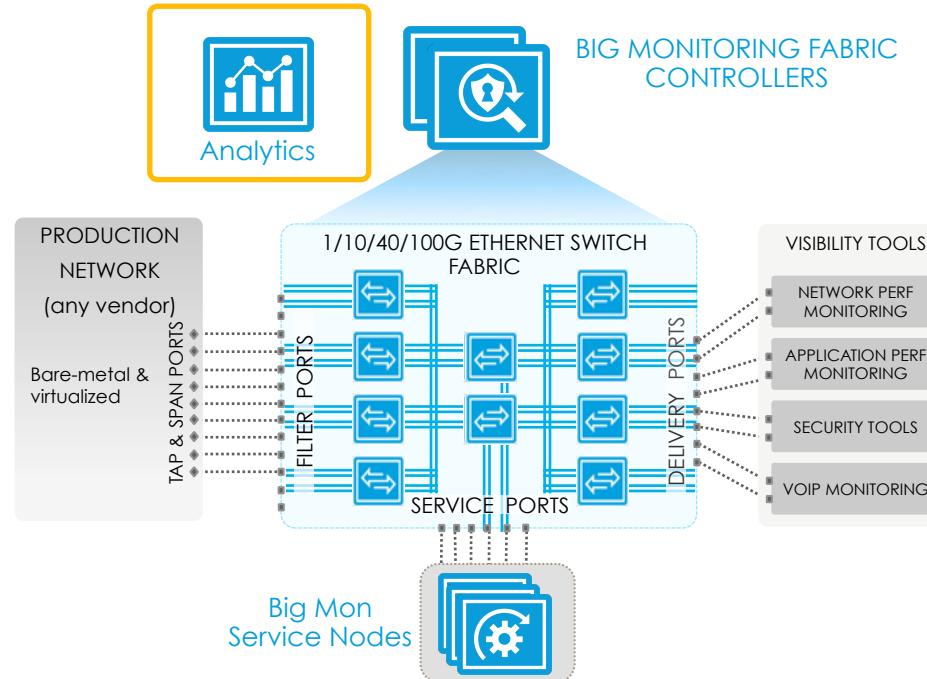
HA cluster of Big Mon controllers enables single pane of glass configuration, monitoring and troubleshooting



BIG MONITORING FABRIC BUILDING BLOCKS

Big Monitoring Fabric Analytics

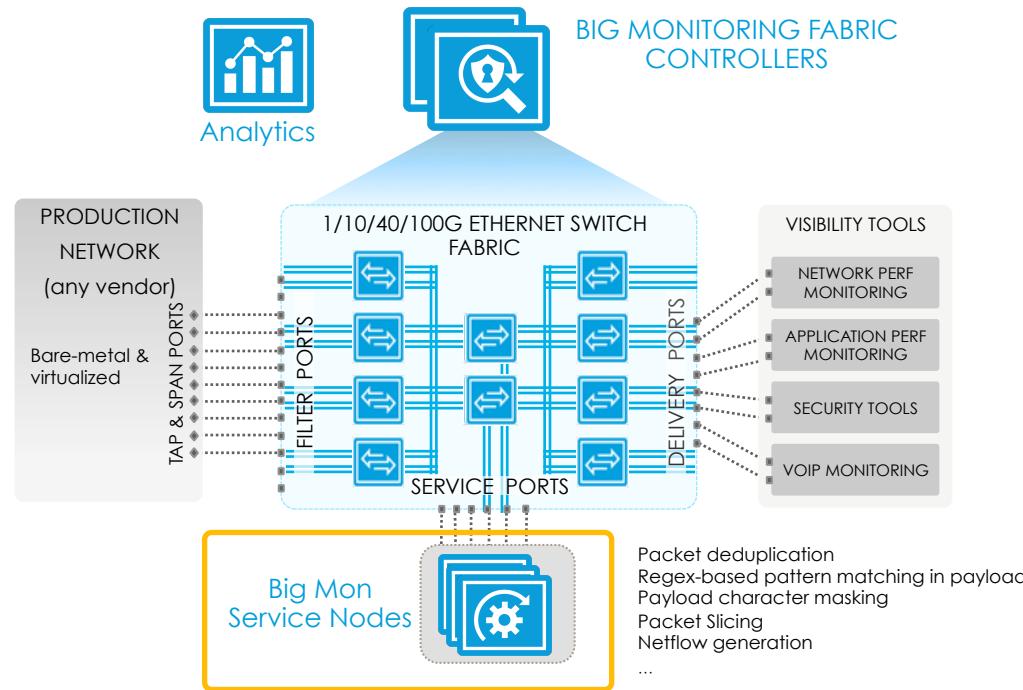
Big Monitoring Fabric Analytics



BIG MONITORING FABRIC BUILDING BLOCKS

Big Mon Managed Service Nodes for advanced packet functions *

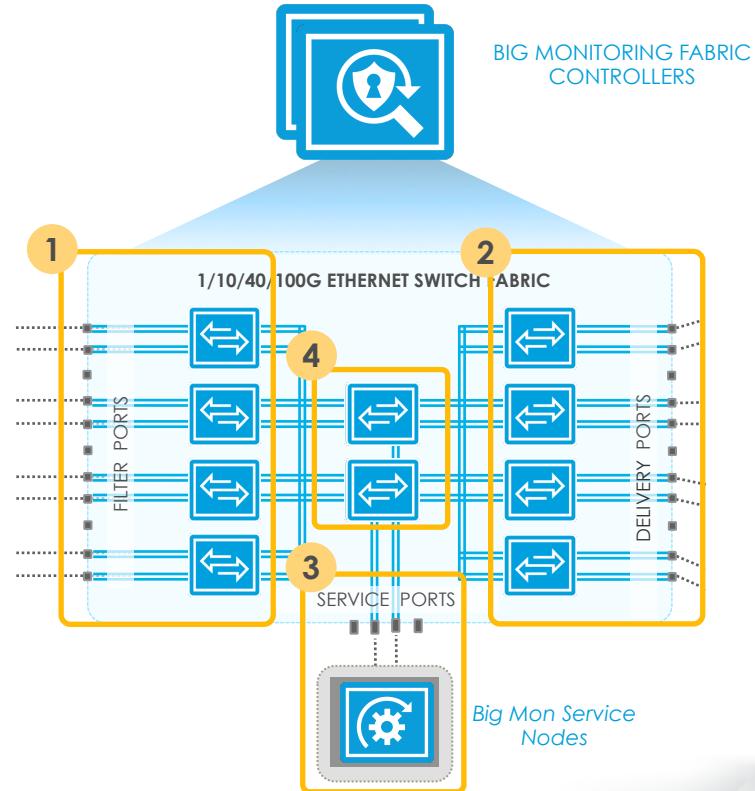
Big Monitoring Fabric's Managed Service Nodes allow the insertion of advanced packet services within policies that you define over the monitoring fabric



* Service Node Covered in the Big Monitoring Fabric Service Node lab

BIG MONITORING FABRIC TERMINOLOGY

- 1. Filter Ports:** Mirrored traffic comes into the monitoring fabric on interfaces that you configure as *filter ports*
- 2. Delivery Ports:** Tools connect to interfaces configured as *delivery ports*. In this module we use Wireshark and Snort as delivery tools
- 3. Service Ports (optional):** Big Mon's Managed Service Nodes can be connected to fabric interfaces which then become service ports. Alternatively, fabric interfaces may be assigned the service role allowing third party services to be attached to the fabric
- 4. Core Switches & Ports (optional):** In scale-out designs, core switches are typically attached to aggregate traffic from multiple leaf switches



MODULE OUTLINE

INTRODUCTION

- * Demo Setup & Terminology

HANDS-ON LAB SECTIONS

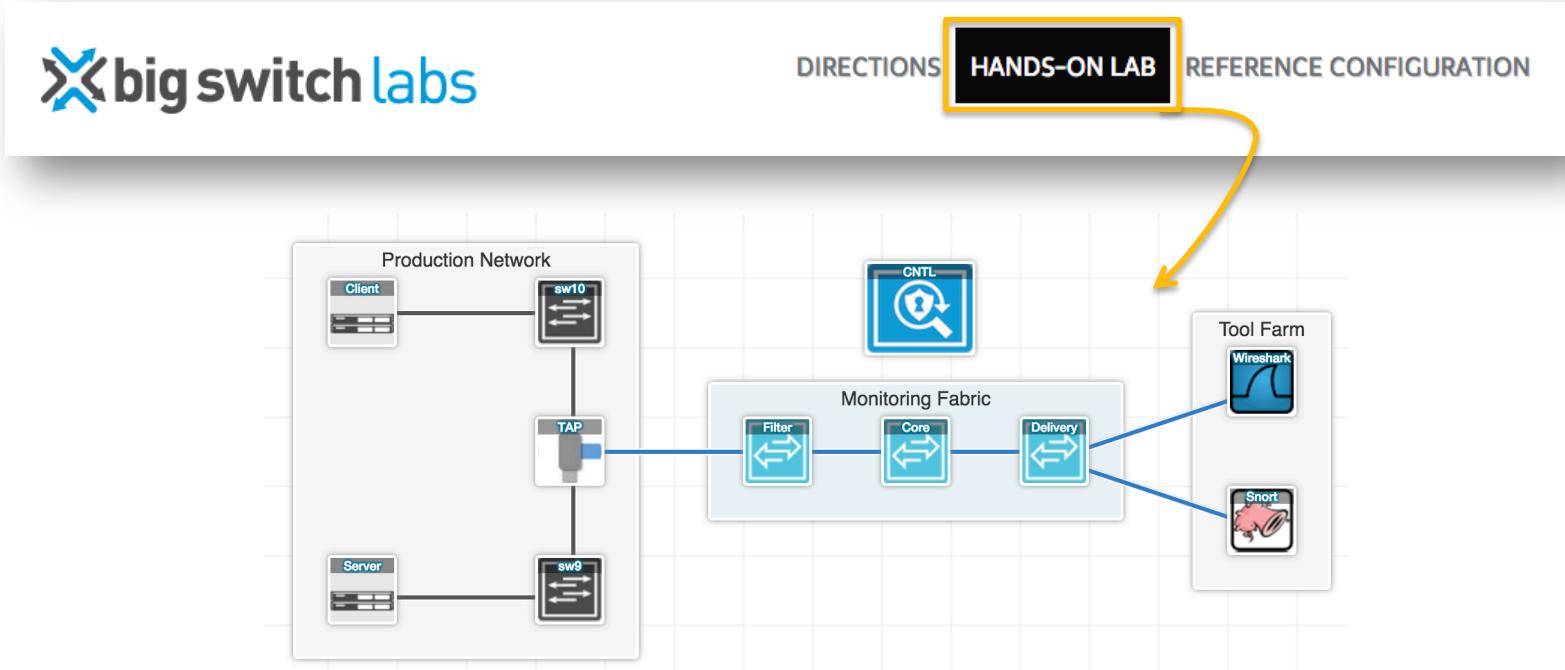
1. Fabric Configuration
2. Create a First Policy
3. Create a Second Policy



Demo Setup & Terminology

LAB TOPOLOGY

Click Hands-on Lab on the menu bar to view the topology and access the controller



LAB TOPOLOGY: BIG TAP CONTROLLER

The Big Monitoring Fabric Controller is the single pane of glass for configuring and troubleshooting the monitoring fabric

- You will only need access to the Big Monitoring Fabric controller
- Right click on the controller icon and select Controller GUI

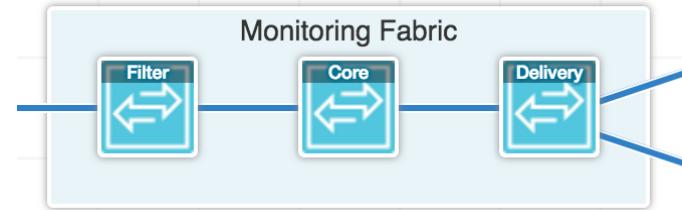


Tip: Default controller username/password for initial access is: **admin/bsn123**

LAB TOPOLOGY: ETHERNET SWITCH FABRIC

In this module, the Fabric topology consists of 3 switches running Switch Light™ OS:

- Filter Switch – **Filter**
- Core Switch – **Core**
- Delivery Switch – **Delivery**

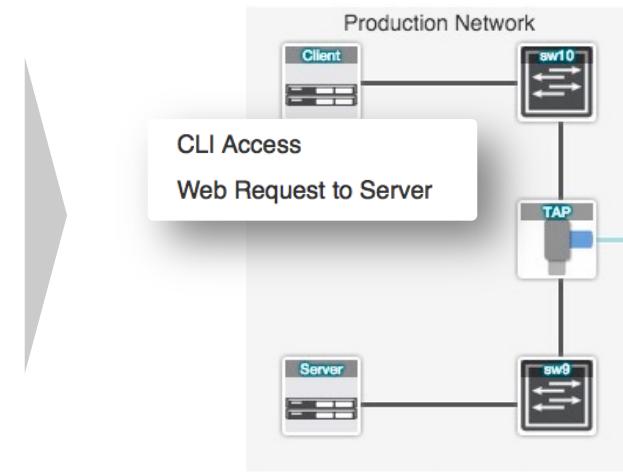


Note on the Design of Fabric Topologies:

- To highlight the scale-out fabric design, the topology used in this module depicts Filter Ports to be configured on the Filter Switch, Delivery Ports to be configured on the Delivery Switch and Service Ports on the Core Switch. This is not a design requirement.
- For smaller deployments, a single Ethernet switch can have Filter, Delivery and Service ports. For very large deployments, a multi-tier topology with Filter, Core and Delivery Switches is recommended.

LAB TOPOLOGY: PRODUCTION NETWORK

Production network traffic is simulated by sending requests from the Client to the Server.



Use Case – Tap Every Rack or Location

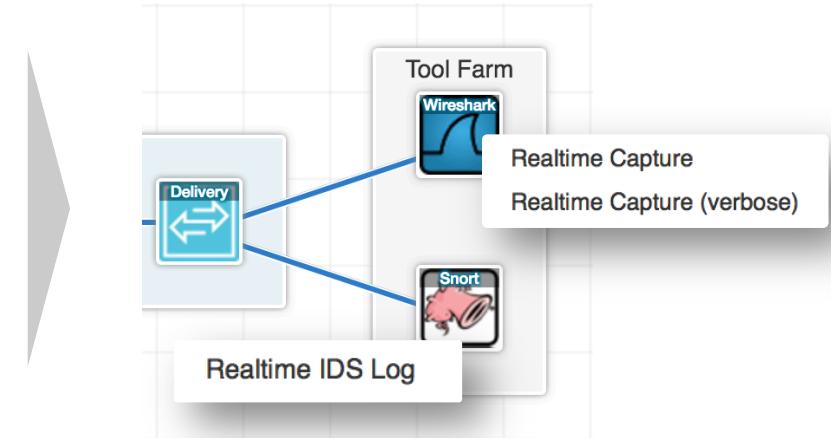
In a large data center, enterprise or campus network, SPAN and TAP traffic from multiple physical or virtual switches can be fed to the monitoring fabric.

Tip: Right click a topology icon (e.g. Client) to open shell access to that node.

LAB TOPOLOGY: CENTRALIZED TOOLS

Two tools are used in this module:

- **Wireshark** as a network traffic analyzer (packet capture)
- **Snort** as the intrusion detection and prevention system (IDS/IPS)



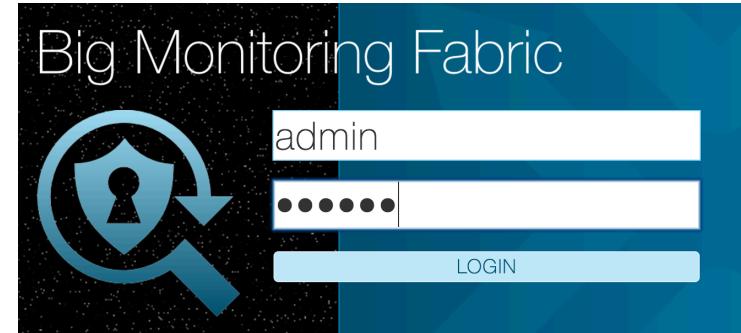
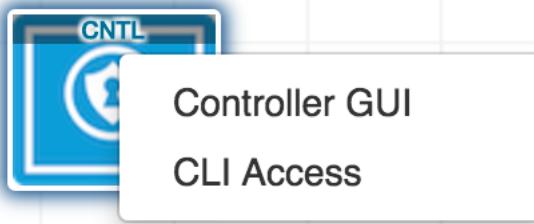
Hyperscale Design – Centralized Tool Farms

Big Monitoring Fabric selectively filters and optimally replicates traffic to a pool of shared services. Which traffic flows are sent to which tools is determined by the policies configured via the Controller

1. Fabric Configuration

1.1 ACCESS BIG MONITORING FABRIC CONTROLLER

Right click the Big Mon controller icon and select the **Controller GUI** and **CLI Access**



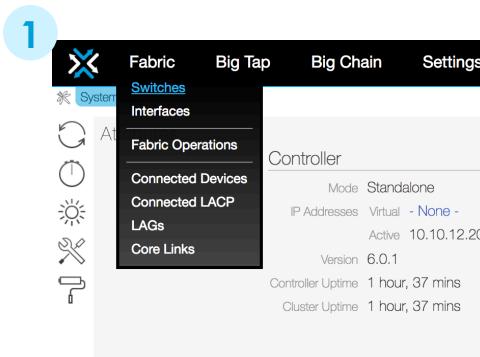
The image shows a terminal window titled 'Shell In A Box' with the IP address '54.224.132.62:8000'. The window displays a log of a successful SSH login:

```
54 login: admin
admin@54.144.8.142's password:
Controller: 127.0.0.1:8000, Big Tap Controller 4.0.0 (2014.08.04.1943-m.bsc.bi
gdb) Logged in as admin, authenticated 2015-01-19 05:42:28 UTC, auth request f
rom ec2-54-224-132-62.compute-1.amazonaws.com
ip-10-60-86-80> enable
ip-10-60-86-80#
```

Tip: Default Controller username/password for initial access is **admin/bsn123**

1.2 ADD FABRIC SWITCHES

1. Navigate to Fabric > Switches
2. Click + to provision a switch
3. Configure the Filter-Switch using MAC address 00:00:00:00:00:0A & Save



The screenshot shows the 'Provision switch' dialog with the following fields:

- Name: Filter-Switch
- DPID: (empty)
- MAC Address: 00:00:00:00:00:0A
- Description: (empty)
- Admin Status: Down (green toggle switch)
- Role: Big Tap (radio button selected)

1.3 ADD CORE AND DELIVERY SWITCHES TO THE FABRIC

- Under Fabric > Switches, repeat the same steps to add Core-Switch 00:00:00:00:00:0B & Delivery-Switch 00:00:00:00:00:0C

Name *
Core-Switch

DPID

MAC Address
00:00:00:00:00:0B

Description

Admin Status *
Down Role *
 Big Tap
 Big Chain
 Service



Name *
Delivery-Switch

DPID

MAC Address
00:00:00:00:00:0C

Description

Admin Status *
Down Role *
 Big Tap
 Big Chain
 Service



Note: To highlight the scale-out fabric design, the topology used in this module depicts Filter Ports to be configured on the Filter Switch, Delivery Ports to be configured on the Delivery Switch. This is not a design requirement. A leaf switch of the fabric can be configured with a mix of filter & delivery ports

1.4 VERIFY FABRIC TOPOLOGY

Click Fabric to show a graphical summary of your fabric

The screenshot shows the 'Fabric' tab selected in a navigation bar. On the left, there's a sidebar with various configuration options like Policies, Settings, and Legend. The main area displays a grid-based network topology with three blue square nodes representing switches. A tooltip for one node provides specific details:

DRID	00:00:00:00:00:00:00:00
Name	Core-Switch
Connected	✓
Interface Count	64
Core Link Interfaces	2

Below the grid, a coordinate indicator shows [494,000; 303,000].

Leaf switches (filter & delivery) are not directly connected to each other. On the other hand, a spine switch (core) is a switch that is physically connected to every leaf switch, and core switches do not connect to each other

1.5 ASSIGN FILTER ROLE TO INTERFACE

- In this lab's topology `ethernet2` of the *Filter-Switch* is connected to a TAP in the production network
- Navigate to Big Tap > Interfaces, click + to add an interface
- Choose Filter-Switch & `ethernet2`, then hit next, select Filter and name the interface FILTER1. Save to apply the configuration

1 Create Interface

1. Interface

The following settings may affect the availability of some configuration options.

Auto VLAN Mode push-per-policy
Auto Strip VLAN ✓ Enabled

Big Tap Switch
Filter-Switch (00:00:00:00:00:00:0a) ▾ Show Connector

Optional: use to filter interface choices below

Interface *

ethernet1
✓ ethernet2
✗ ethernet3
✗ ethernet4
✗ ethernet5

2 1. Interface ✓
2. Configure ✓

The following settings may affect the availability of some configuration options.

Auto VLAN Mode push-per-policy
Auto Strip VLAN ✓ Enabled

Filter

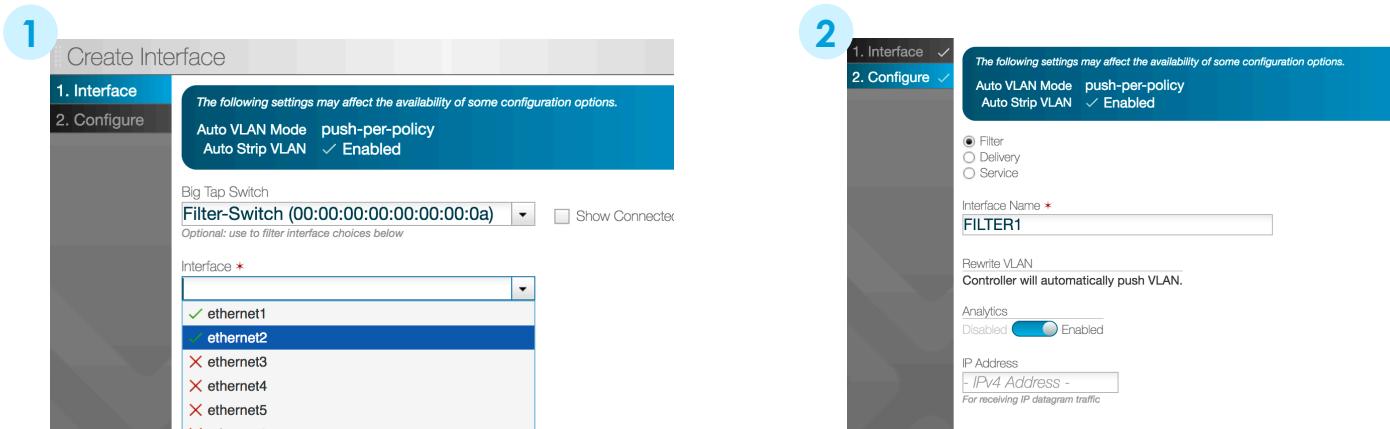
Interface Name *

FILTER1

Rewrite VLAN
Controller will automatically push VLAN.

Analytics
Disabled Enabled

IP Address
- IPv4 Address -
For receiving IP datagram traffic



1.6 ASSIGN DELIVERY ROLE TO INTERFACES

- ethernet2 of Delivery-Switch is physically connected to a Wireshark tool, and ethernet3 of the same switch is connected to the Snort IDS
- Repeat the same steps to add two delivery interfaces as shown below, making sure you set the role of the interfaces to Delivery

Create Interface

1. Interface ✓
2. Configure ✓

The following settings may affect the availability of some configuration options:
Auto VLAN Mode push-per-policy
Auto Strip VLAN ✓ Enabled

Big Tap Switch
Delivery-Switch (00:00:00:00:00:00:0c) ▾ S

Interface *
ethernet2

Edit Interface

1. Interface ✓
2. Configure ✓

The following settings may affect the availability of some configuration options:
Auto VLAN Mode push-per-policy
Auto Strip VLAN ✓ Enabled

Interface Name *
WIRESHARK1

Filter
 Delivery
 Service

Strip VLAN at Interface
VLANs will be stripped automatically by controller.

Next Hop IP
- IPv4 Address - / - Prefix - ▾
- IPv4 Mask -
Next hop IP that's reachable via delivery interface with local mask

Create Interface

1. Interface ✓
2. Configure ✓

The following settings may affect the availability of some configuration options:
Auto VLAN Mode push-per-policy
Auto Strip VLAN ✓ Enabled

Big Tap Switch
Delivery-Switch (00:00:00:00:00:00:0c) ▾ S

Interface *
ethernet3

Create Interface

1. Interface ✓
2. Configure ✓

The following settings may affect the availability of some configuration options:
Auto VLAN Mode push-per-policy
Auto Strip VLAN ✓ Enabled

Interface Name *
IDS1

Filter
 Delivery
 Service

Strip VLAN at Interface
VLANs will be stripped automatically by controller.

Next Hop IP
- IPv4 Address - / - Prefix - ▾
- IPv4 Mask -
Next hop IP that's reachable via delivery interface with local mask

1.7 VERIFY FABRIC INTERFACE ROLES

Review the **roles** (filter or delivery) assigned to the interfaces of the Fabric under *Big Tap > Interfaces*

The screenshot shows a table titled "Big Tap Interfaces" with a header row containing columns for Name, Type, Switch DPID, Switch Name, Interface, Groups, Analytics, IP Address, Rewrite VLAN, Strip VLAN, Next Hop IP, Next Hop Mask, Service, State, Speed, Direction, and Device Name. There are three rows of data:

	Name	Type	Switch DPID	Switch Name	Interface	Groups	Analytics	IP Address	Rewrite VLAN	Strip VLAN	Next Hop IP	Next Hop Mask	Service	State	Speed	Direction	Device Name
<input type="checkbox"/>	FILTER1	Filter	00:00:00:00:00:00:0a	Filter-Switch	ethernet2	—	✓	—	NA	NA	NA	NA	NA	✓ Up	10 Gbit/s	rx	—
<input type="checkbox"/>	IDS1	Delivery	00:00:00:00:00:00:0c	Delivery-Switch	ethernet3	—	NA	NA	NA	✓	—	—	NA	✓ Up	10 Gbit/s	tx	—
<input type="checkbox"/>	WIRESHARK1	Delivery	00:00:00:00:00:00:0c	Delivery-Switch	ethernet2	—	NA	NA	NA	✓	—	—	NA	✓ Up	10 Gbit/s	tx	—

2. Create a First Policy

2.1 GENERATE PRODUCTION TRAFFIC

1. Generate production network traffic by sending Ping traffic from the Client to the Server.

- Go to HANDS-ON LAB tab and right click on the Client icon in the topology
- Select CLI Access and start a ping to the Server

```
ping -c 100 10.0.0.2
```

2. Verify that Big Monitoring Fabric is not capturing any traffic. This is the default drop behavior for packets not matching any policies.

- Right click on any of the delivery tool icons (Wireshark, Snort) and access their Realtime logs. You should find them empty.

Tip: Client IP Address: 10.0.0.3 Server IP Address: 10.0.0.2

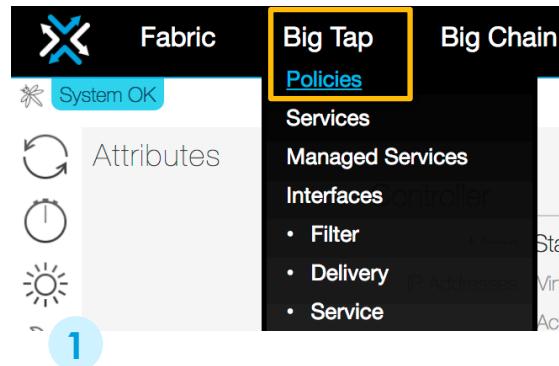


```
bsn@client: ~ - Shell In A Box
$ 54.147.86.229:8080/Clientshell/
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

bsn@client:~$ ping -c 100 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.085 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.097 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.081 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.095 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=0.092 ms
64 bytes from 10.0.0.2: icmp_seq=6 ttl=64 time=0.098 ms
64 bytes from 10.0.0.2: icmp_seq=7 ttl=64 time=0.096 ms
64 bytes from 10.0.0.2: icmp_seq=8 ttl=64 time=0.093 ms
64 bytes from 10.0.0.2: icmp_seq=9 ttl=64 time=0.073 ms
64 bytes from 10.0.0.2: icmp_seq=10 ttl=64 time=0.096 ms
```

2.2 DELIVER PRODUCTION TRAFFIC TO TOOLS

Create the 1st Policy



Click on “Policies” under Big Tap



Click on + to add a new policy

A screenshot of a form for creating a new policy. The "Name" field is filled with "POLICY1" and has a yellow border. Below it is a "Description" field with an empty text area. At the bottom, there is a toggle switch set to "Active".

Name *	POLICY1
Description	
Inactive	<input checked="" type="button"/> Active

3

In the 1. Info menu name your policy “POLICY1”, and set the Action field to value “Forward”

2.3 DELIVER PRODUCTION TRAFFIC TO TOOLS

Create the 1st Policy

The screenshot shows the policy configuration interface with three main panels:

- Left Panel (Step 4):** Shows a list of steps: 1. Info, 2. Rules (selected), 3. Filter Interfaces, 4. Delivery Interfaces, 5. Services, 6. Managed Services, 7. Summary. A tooltip "The following settings apply to all rules in this policy" is shown above the "Switching Mode" dropdown, which is set to "L3-L4 M". The "Rules" section contains a button "Add rule ...".
- Middle Panel (Step 5):** Shows the "Traffic" configuration screen. It includes fields for Sequence (set to 1), Source, Destination, and Offset Match. The "Ethertype" field is set to "IPv4 - 0x800 (2048)" and the "IP Protocol" field is set to "ICMP (1)".
- Right Panel (Step 6):** Shows the "Filter Interfaces" configuration screen. It includes a checkbox "All Filter Interfaces" (unchecked) and a "Filter Interfaces" section with a "Add interface ..." button. The "Switching Mode" is set to "L3-L4 M".

4

Click on the + symbol to add a rule for your policy

5

Select **IPv4** as Etheretype and **ICMP (1)** as the IP Protocol

Leave all other fields set to their default values

Skip Source, Destination and Offset match settings, then **Append** the rule

6

Under Filter Interfaces, click to add an interface and **select FILTER1**, submit with **Append Selected**

2.4 DELIVER PRODUCTION TRAFFIC TO TOOLS

Create the 1st Policy

3. Filter Interfaces ✓
4. Delivery Interfaces ✓
5. Services ✓
6. Managed Services ✓
7. Summary ✓

Add Delivery Interfaces

Name	Switch
<input checked="" type="checkbox"/> IDS1	00:00:00:00:0
<input checked="" type="checkbox"/> WIRESHARK1	00:00:00:00:0

Back Next Reset Cancel Save

- 7 Under **Delivery Interfaces** click the + symbol and **select both IDS1 and WIRESHARK1** then click **Append Selected**

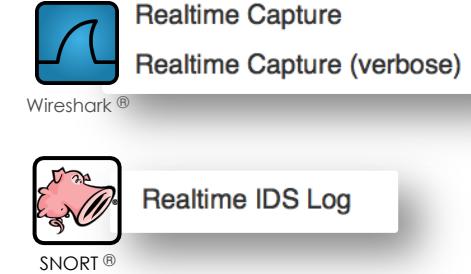
- 8 Leave the fields under Services, Managed Services and Summary set to their default value
Then click **Save** to install to the policy

Name	Description	Runtime Status	Config Status	Type	Action	Active	Priority	Push VLAN
POLICY1	-	✓ installed	✓ active - forward	Configured	→ Forward	✓ Yes	100	1

2.5 DELIVER PRODUCTION TRAFFIC TO TOOLS

Test the 1st Policy

1. Right click on the “Wireshark” icon and select “**Realtime Capture**”.
 - A real-time capture CLI window should appear.
2. Right click on the “SNORT®” icon, and select “**Realtime IDS Log**”.
 - A real-time IDS log window should appear.
3. Right click on the “Client” icon, and select “**CLI Access**”.
 - In the CLI issue the command “ping 10.0.0.2”.
 - This command will send ICMP traffic to Server. Press CTRL-C after a few seconds to stop the test.

A screenshot of a terminal window titled "bsn@client: ~ - Shell in A Box". The window shows the output of a ping command to 10.0.0.2, displaying nine ICMP echo requests sent at approximately 0.085 ms intervals.

```
bsn@client:~$ ping -c 100 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.085 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.097 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.081 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.089 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=0.092 ms
64 bytes from 10.0.0.2: icmp_seq=6 ttl=64 time=0.098 ms
64 bytes from 10.0.0.2: icmp_seq=7 ttl=64 time=0.096 ms
64 bytes from 10.0.0.2: icmp_seq=8 ttl=64 time=0.093 ms
64 bytes from 10.0.0.2: icmp_seq=9 ttl=64 time=0.073 ms
64 bytes from 10.0.0.2: icmp_seq=10 ttl=64 time=0.086 ms
```

2.6 DELIVER PRODUCTION TRAFFIC TO TOOLS

Test the 1st Policy

Verify that Ping traffic from the Client to the Server is mirrored onto the Monitoring Fabric. After configuring POLICY1, the traffic should be forwarded from the filter ports to the delivery ports where the tools (Wireshark & Snort) are connected.

Note: Big Mon replicates traffic on the common switch closest to the delivery ports to optimize fabric resource utilization



Wireshark®

Realtime Capture

Realtime Capture (verbose)



SNORT®

Realtime IDS Log

The diagram illustrates the traffic flow and its capture. On the left, a client sends a ping to a server. This traffic is mirrored onto the monitoring fabric. On the right, two windows show the captured traffic: a Wireshark window titled "Realtime Capture (verbose)" and a Snort window titled "Realtime IDS Log". Both windows display the same ICMP traffic, showing requests and replies between the client and server, along with classification information.

```
seq=6/1536, ttl=64          ICMP 98 Echo (ping) request  id
6.000166      10.0.0.1 -> 10.0.0.2
seq=7/1792, ttl=64          ICMP 98 Echo (ping) reply    id
6.000117      10.0.0.2 -> 10.0.0.1
seq=7/1792, ttl=64          ICMP 98 Echo (ping) request  id
7.000118      10.0.0.1 -> 10.0.0.2
seq=8/2048, ttl=64          ICMP 98 Echo (ping) request  id
7.000131      10.0.0.2 ->
8.000140      10.0.0.1 ->
seq=9/2304, ttl=64          ICMP PING *NIX [**] [Classification: M activity] [Priority: 3] {ICMP} 10.0.0.1 -> 10.0.0.2
8.000156      10.0.0.2 ->
seq=9/2304, ttl=64          ICMP PING [*] [Classification: M activity] [Priority: 3] {ICMP} 10.0.0.1 -> 10.0.0.2
9.000105      10.0.0.1 ->
seq=10/2560, ttl=64         ICMP Echo Reply [**] [Classification: M activity] [Priority: 3] {ICMP} 10.0.0.2 -> 10.0.0.1
9.000119      10.0.0.2 ->
seq=10/2560, ttl=64         ICMP PING *NIX [**] [Classification: M activity] [Priority: 3] {ICMP} 10.0.0.1 -> 10.0.0.2
01/15-01:37:02.454203  [**] [1:366:7] ICMP PING *NIX [**] [Classification: M activity] [Priority: 3] {ICMP} 10.0.0.1 -> 10.0.0.2
01/15-01:37:02.454203  [**] [1:384:5] ICMP PING [*] [Classification: M activity] [Priority: 3] {ICMP} 10.0.0.1 -> 10.0.0.2
01/15-01:37:02.454213  [**] [1:408:5] ICMP Echo Reply [**] [Classification: M activity] [Priority: 3] {ICMP} 10.0.0.2 -> 10.0.0.1
01/15-01:37:03.454216  [**] [1:366:7] ICMP PING *NIX [**] [Classification: M activity] [Priority: 3] {ICMP} 10.0.0.1 -> 10.0.0.2
01/15-01:37:03.454216  [**] [1:384:5] ICMP PING [*] [Classification: M activity] [Priority: 3] {ICMP} 10.0.0.1 -> 10.0.0.2
01/15-01:37:03.454227  [**] [1:408:5] ICMP Echo Reply [**] [Classification: M activity] [Priority: 3] {ICMP} 10.0.0.2 -> 10.0.0.1
01/15-01:37:03.454227  [**] [1:366:7] ICMP PING *NIX [**] [Classification: M activity] [Priority: 3] {ICMP} 10.0.0.1 -> 10.0.0.2
01/15-01:37:04.454238  [**] [1:366:7] ICMP PING *NIX [**] [Classification: M activity] [Priority: 3] {ICMP} 10.0.0.1 -> 10.0.0.2
01/15-01:37:04.454238  [**] [1:384:5] ICMP PING [*] [Classification: M activity] [Priority: 3] {ICMP} 10.0.0.1 -> 10.0.0.2
```

3. Create a Second Policy

3.1 CREATE THE 2ND POLICY

Create the 2nd Policy

Goal: Add a second policy for one tool (Wireshark) to monitor TCP traffic in addition to the ICMP*



1

Go to Interfaces under Big Tap

Big Tap Interfaces	
Filter table rows	
Name	Type
<input checked="" type="checkbox"/> FILTER1	Filter 00:00:0
<input type="checkbox"/> IDS1	Delivery 00:00:0
<input checked="" type="checkbox"/> WIRESHARK1	Delivery 00:00:0

2

Select FILTER1 and WIRESHARK1

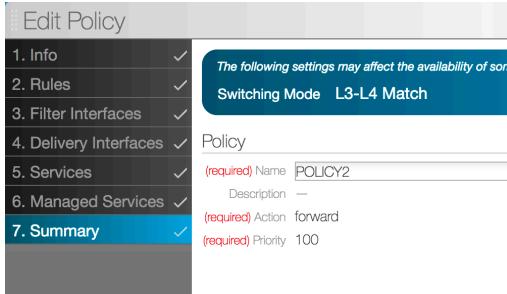
Big Tap Interfaces	
Filter table rows	
Show/Hide Columns	Switch DPID
Monitor Selected Stats	0:00:00:00
Group Selected Interfaces	0:00:00:00
Start Policy From Selected Interfaces	0:00:00:00
<input checked="" type="checkbox"/> WIRESHARK1	Delivery 00:00:00:00:00:00

3

Click on the drop-down icon and choose Start Policy From Selected Interfaces. A policy menu gets automatically created and populated

* Note this time we use a slightly different workflow for creating a policy, starting from Big Tap interfaces

3.2 CREATE THE 2ND POLICY



4

Set policy name to POLICY2

The screenshot shows the 'Edit Policy' interface with the 'Rules' tab selected. A modal window titled 'Rules' is open, showing a table with one row. The row has sequence 1 and is labeled 'Any Traffic'. There is a 'Remove selected rules' button with a yellow box around it.

5

Under Rules, select & remove the default All Traffic rule

The screenshot shows the 'Edit Policy' interface with the 'Traffic' tab selected. The 'Ethertype' field is set to 'IPv4 - 0x800 (2048)' and the 'IP Protocol' field is set to 'TCP (6)'. Both fields are highlighted with a yellow box.

6

Add a new rules to match on IPv4 TCP traffic. Click Append, then Save to create the policy.

Optional: Navigate to Big Tap > Policies to verify policy creation

∅ Big Tap Policies

	Name	Description	Runtime Status	Config Status	Type	Action	Active
<input type="checkbox"/>	POLICY1	-	✓ installed	✓ active - forward	Configured	→ Forward	✓ Yes
<input type="checkbox"/>	POLICY2	-	✓ installed	✓ active - forward	Configured	→ Forward	✓ Yes

3.3 TEST THE 2ND POLICY

To verify the policy perform the following steps

- Right click on the “Wireshark” icon, and select “**Realtime Capture**”.
A real-time capture CLI window should appear.
- Right click on the “Client” icon, and select “**Web Request to Server**”.
This should open the website on the Server in a new browser window. The request for this website by the browser is proxied via Client to the Server.



```
① 54.147.86.229:8080/capturelog/
Capturing on 'Wireshark-eth0'
1 0.000000 10.0.0.3 -> 10.0.0.2 TCP 74 37870 > http [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSeqval=18556697 TSecr=0 WS=512
2 0.048955 10.0.0.2 -> 10.0.0.3 TCP 74 37870 > http [SYN ACK] Seq=1 Ack=1 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSeqval=18556697 TSecr=18556697 WS=512
3 0.097910 10.0.0.3 -> 10.0.0.2 TCP 74 37871 > http [ACK] Seq=1 Ack=0 Win=29208 Len=0 TSeqval=18556697 TSecr=18556697 WS=512
4 0.171108 10.0.0.3 -> 10.0.0.2 TCP 74 37871 > http [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSeqval=18556732 TSecr=0 WS=512
5 0.251074 10.0.0.2 -> 10.0.0.3 TCP 74 http > 37871 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSeqval=18556732 WS=512
6 0.312185 10.0.0.3 -> 10.0.0.2 TCP 66 37873 > http [ACK] Seq=1 Ack=1 Win=28966 Len=0 TSeqval=18556732 TSecr=18556732 WS=512
7 0.360250 10.0.0.2 -> 10.0.0.3 TCP 66 37873 > http [SYN] Seq=0 Ack=1 Win=28966 Len=0 MSS=1460 SACK_PERM=1 TSeqval=18556732 TSecr=0 WS=512
8 0.436749 10.0.0.2 -> 10.0.0.3 TCP 4 37872 > http [SYN, ACK] Seq=0 Ack=1 Win=28966 Len=0 MSS=1460 SACK_PERM=1 TSeqval=18556761 TSecr=18556761 WS=512
9 0.459334 10.0.0.3 -> 10.0.0.2 TCP 66 37872 > http [ACK] Seq=1 Ack=1 Win=28966 Len=0 TSeqval=18556761 TSecr=18556761 WS=512
10 0.551952 10.0.0.3 -> 10.0.0.2 TCP 74 37873 > http [SYN] Seq=0 Win=29208 Len=0 MSS=1460 SACK_PERM=1 TSeqval=18556807 TSecr=0 WS=512
11 0.610020 10.0.0.2 -> 10.0.0.3 TCP 66 37873 > http [ACK] Seq=0 Ack=1 Win=28966 Len=0 MSS=1460 SACK_PERM=1 TSeqval=18556807 TSecr=18556807 WS=512
12 0.557554 10.0.0.3 -> 10.0.0.2 TCP 66 37873 > http [ACK] Seq=1 Ack=1 Win=28966 Len=0 TSeqval=18556807 TSecr=18556807 WS=512
13 0.573192 10.0.0.3 -> 10.0.0.2 HTTP 1034 GET / HTTP/1.1
13 14 0.5756843 10.0.0.2 -> 10.0.0.3 TCP 66 http > 37873 [ACK] Seq=1 Ack=969 Win=31232 Len=0 TSeqval=18556810 TSecr=18556810
14 0.632280 10.0.0.2 -> 10.0.0.3 HTTP 1034 GET / HTTP/1.1
15 0.689891 10.0.0.3 -> 10.0.0.2 TCP 66 37873 > http [ACK] Seq=969 Ack=198 Win=30728 Len=0 TSeqval=18556810 TSecr=18556810
16 0.748569 10.0.0.2 -> 10.0.0.3 TCP 66 37873 > http [ACK] Seq=969 Ack=198 Win=30728 Len=0 TSeqval=18556810 TSecr=18556810
16 17 0.8064287 10.0.0.3 -> 10.0.0.2 TCP 66 37870 > http [FIN, ACK] Seq=1 Ack=1 Win=29696 Len=0 TSeqval=18559258 TSecr=18556697
17 18 0.812228 10.0.0.2 -> 10.0.0.3 TCP 66 37870 > http [FIN, ACK] Seq=2 Ack=2 Win=29184 Len=0 TSeqval=18559258 TSecr=18559258
19 0.825288 10.0.0.3 -> 10.0.0.2 TCP 37870 > http [ACK] Seq=2 Ack=2 Win=29184 Len=0 TSeqval=18559258 TSecr=18559258
20 0.843239 10.0.0.2 -> 10.0.0.3 TCP 66 37873 > http [ACK] Seq=1 Ack=1 Win=28966 Len=0 TSeqval=18556732 TSecr=18556732
21 0.878518 10.0.0.2 -> 10.0.0.3 TCP 66 http > 37871 [FIN, ACK] Seq=1 Ack=2 Win=29184 Len=0 TSeqval=18559258 TSecr=18559258
22 0.91873 10.0.0.3 -> 10.0.0.2 TCP 66 37871 > http [ACK] Seq=2 Ack=2 Win=29696 Len=0 TSeqval=18559258 TSecr=18559258
23 0.982211 10.0.0.3 -> 10.0.0.2 TCP 66 37872 > http [FIN, ACK] Seq=1 Ack=1 Win=28956 Len=0 TSeqval=18559258 TSecr=18556761
24 1.000269 10.0.0.2 -> 10.0.0.3 TCP 66 37872 > http [ACK] Seq=2 Ack=2 Win=28956 Len=0 TSeqval=18559258 TSecr=18556761
25 1.045860 10.0.0.3 -> 10.0.0.2 TCP 66 37872 > http [ACK] Seq=199 Ack=969 Win=31232 Len=0 TSeqval=18559260 TSecr=18559260
26 27 65.519987 10.0.0.3 -> 10.0.0.2 TCP 66 37873 > http [ACK] Seq=969 Ack=191 Win=30728 Len=0 TSeqval=18573084 TSecr=18573074
27 66.011596 10.0.0.3 -> 10.0.0.2 TCP 66 37873 > http [ACK] Seq=969 Ack=191 Win=30728 Len=0 TSeqval=18573199 TSecr=18573087
28 66.014915 10.0.0.2 -> 10.0.0.3 TCP 66 http > 37873 [ACK] Seq=191 Ack=978 Win=31232 Len=0 TSeqval=18573199 TSecr=18573199
```



Thank You

FOR MORE INFORMATION, PLEASE CONTACT INFO@BIGSWITCH.COM.