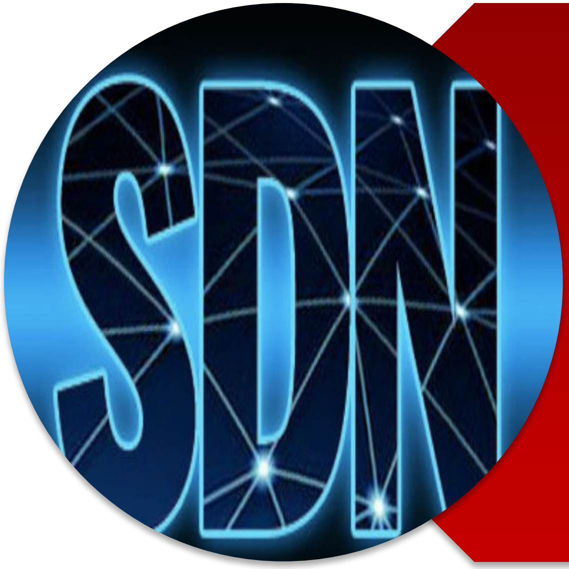
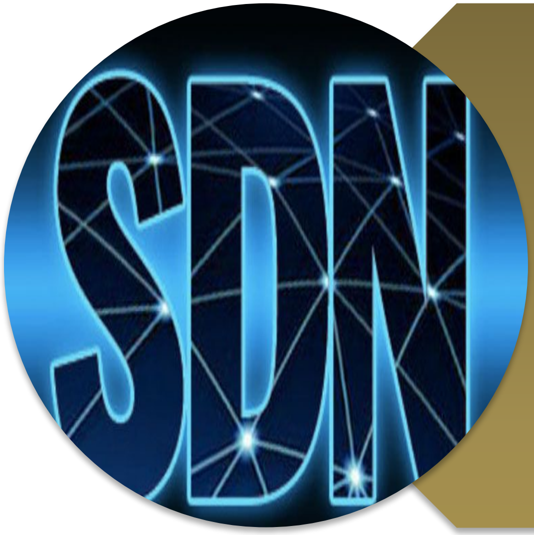
Lecture 4



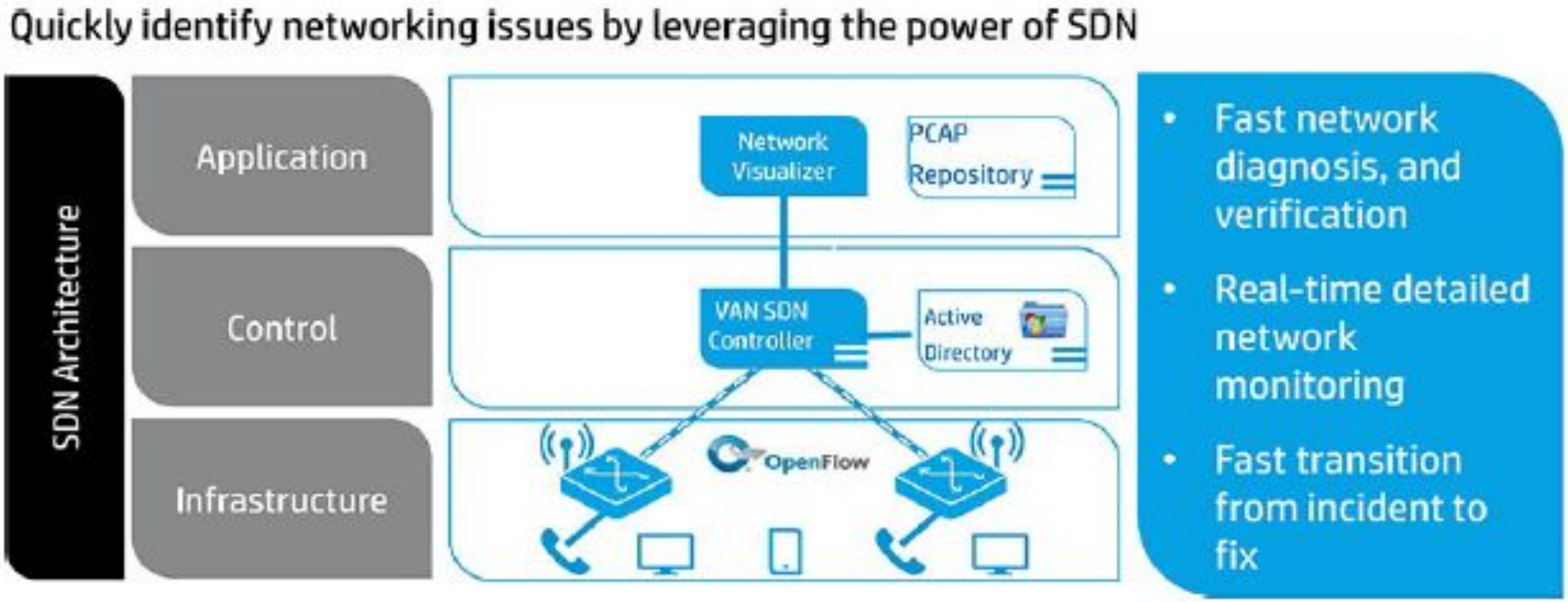
HP Network Visualizer SDN

Objectives



HP Network Visualizer SDN

Introduction to the lecture



Quickly identify networking issues by leveraging the power of SDN

- Fast network diagnosis, and verification
- Real-time detailed network monitoring
- Fast transition from incident to fix

Introduction to the lecture

Introduction to the lecture

- Users
- User devices
- Location
- Application
- Status of network
- Time

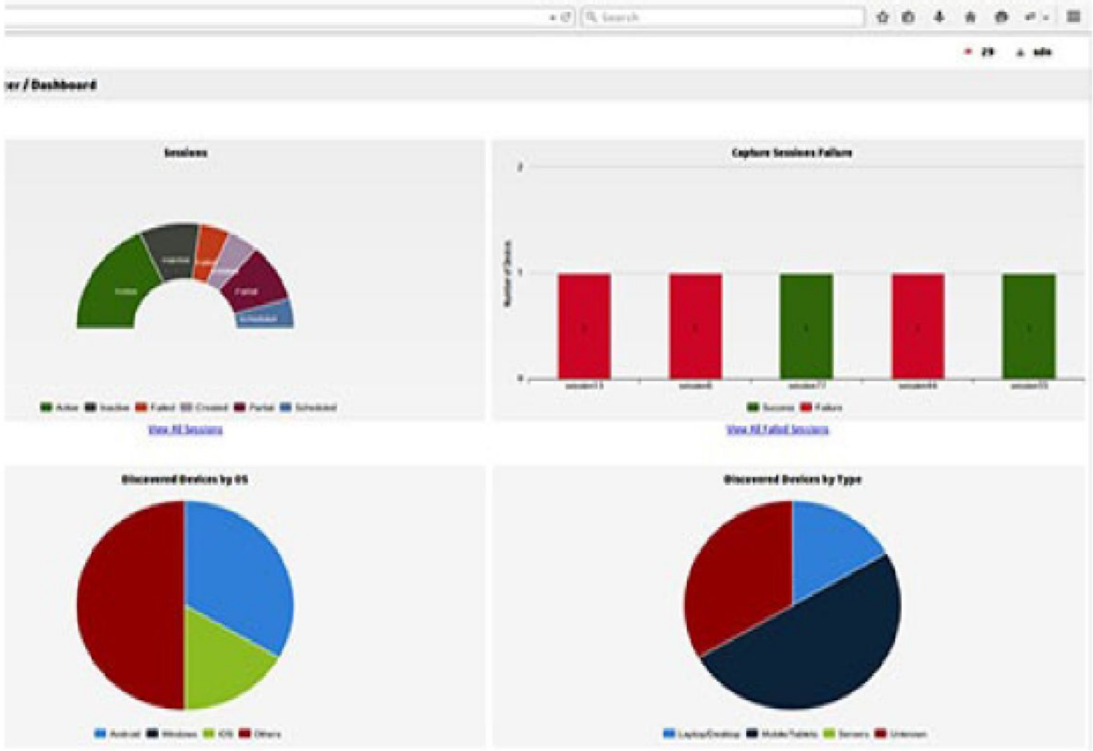
HP Network Visualizer key features

Monitor and analyze the network;

Visibility;

Event Logs;

Create Capture Session wizard.



HP Network Visualizer key features

Monitor and analyze the network: You can narrow down the source of network problems, know the traffic peaks from any network device, and validate network connectivity

Visibility:

- Client address identification
- GUI-based real-time monitoring of captured packets
- Dashboard charts
- Detailed capture session view

pcap

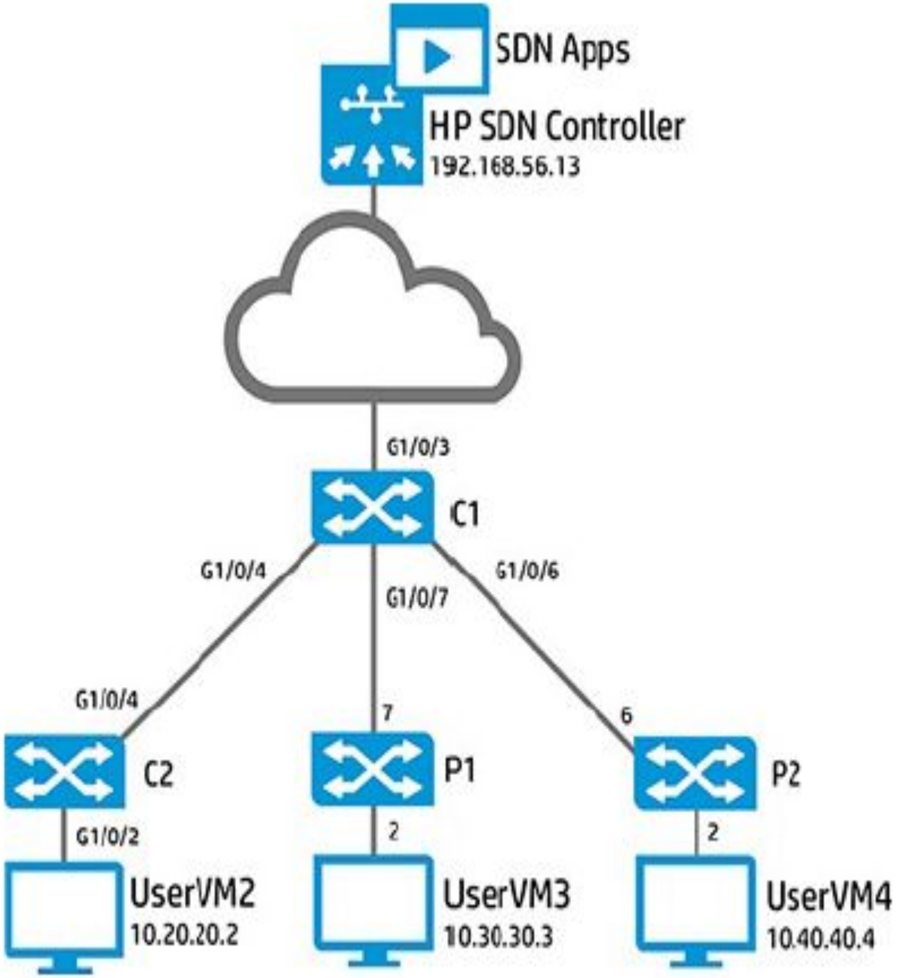
Event Logs:

Create Capture Session wizard:

- Custom — Configure the source/destination IP address, source/destination MAC address, port, and protocol for a capture session.
- User — Configure the user, user group, device(s), and application for a capture session.

HP Network Visualizer SDN

Network Visualizer installation instructions



Install the HP Network Visualizer Application

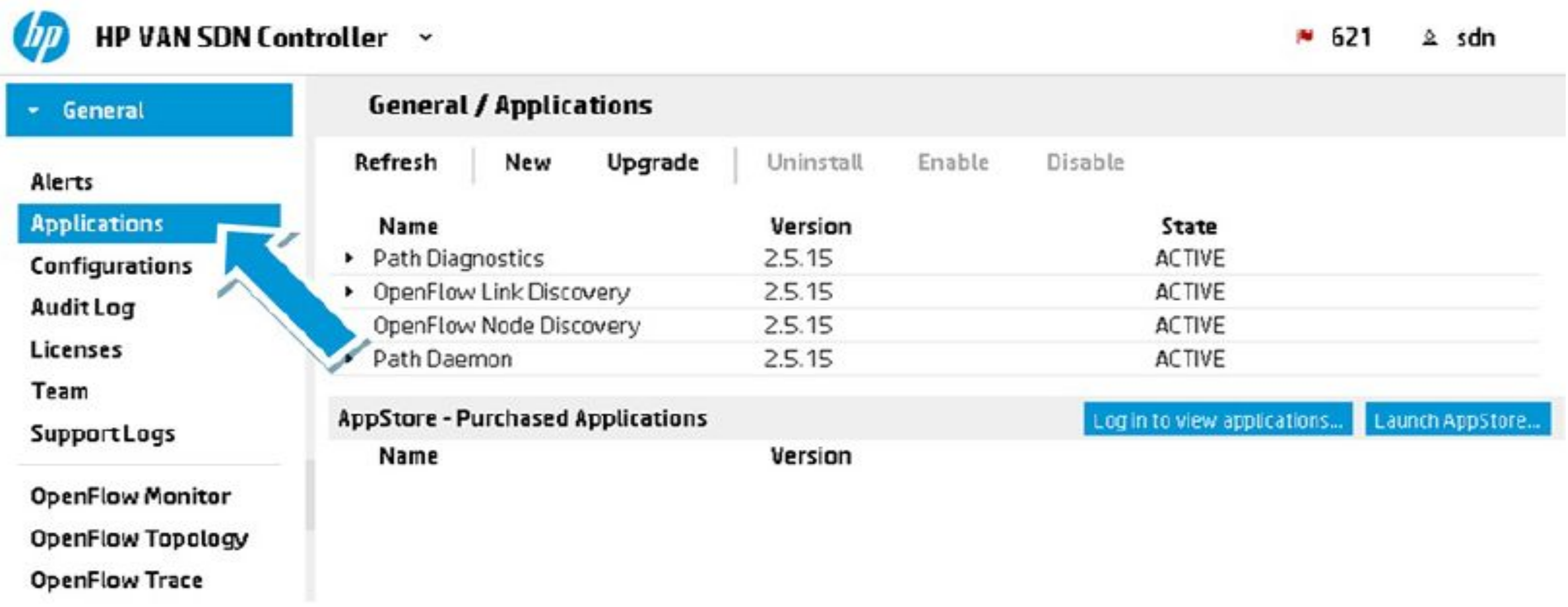
192.168.56.13

http://192.168.56.13:8443/sdn/ui.

- **Username: sdn**
- **Password: skyline**

Install the HP Network Visualizer Application

Applications



HP VAN SDN Controller

621 sdn

General / Applications

Name	Version	State
Path Diagnostics	2.5.15	ACTIVE
OpenFlow Link Discovery	2.5.15	ACTIVE
OpenFlow Node Discovery	2.5.15	ACTIVE
Path Daemon	2.5.15	ACTIVE

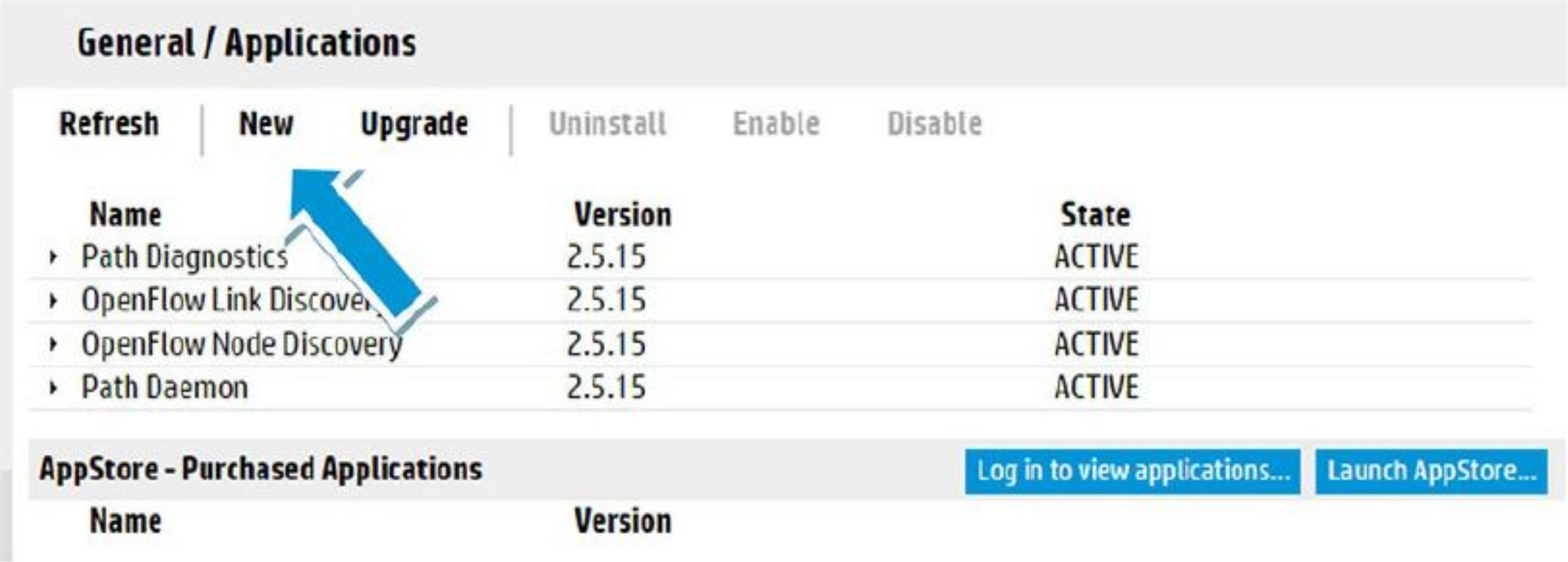
AppStore - Purchased Applications

Name	Version

WARNING!

Install the HP Network Visualizer Application

New



Name	Version	State
Path Diagnostics	2.5.15	ACTIVE
OpenFlow Link Discover	2.5.15	ACTIVE
OpenFlow Node Discovery	2.5.15	ACTIVE
Path Daemon	2.5.15	ACTIVE

AppStore - Purchased Applications
Log in to view applications...
Launch AppStore...
Name
Version

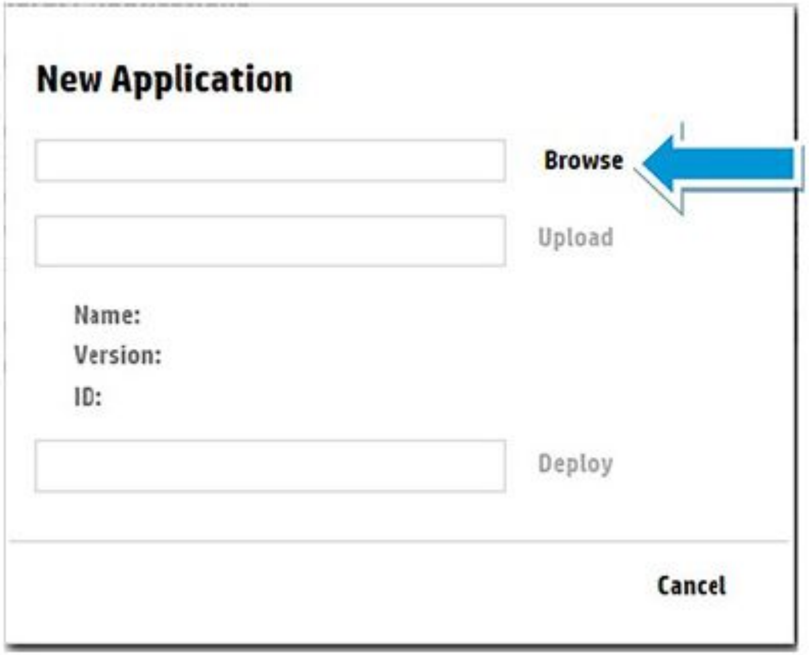
Install the HP Network Visualizer Application

Browse

Desktop

SDN Lab Files

Software



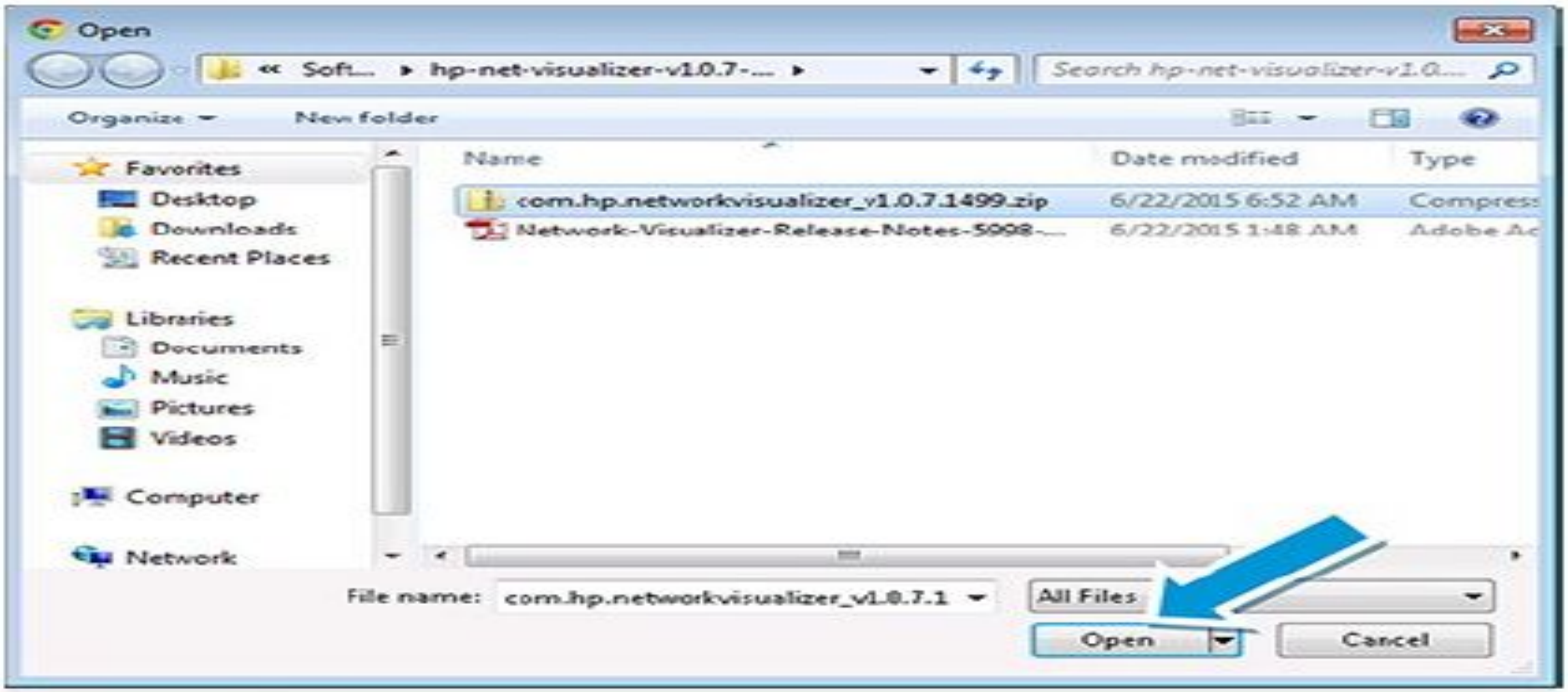
New Application

WARNING!

Install the HP Network Visualizer Application

hp-net-visualizer-v1.0.7-x64

com.hp.networkvisualizer_v1.0.7.1499.zip



Name	Date modified	Type
com.hp.networkvisualizer_v1.0.7.1499.zip	6/22/2015 6:52 AM	Compress
Network-Visualizer-Release-Notes-5998-...	6/22/2015 1:48 AM	Adobe Ac

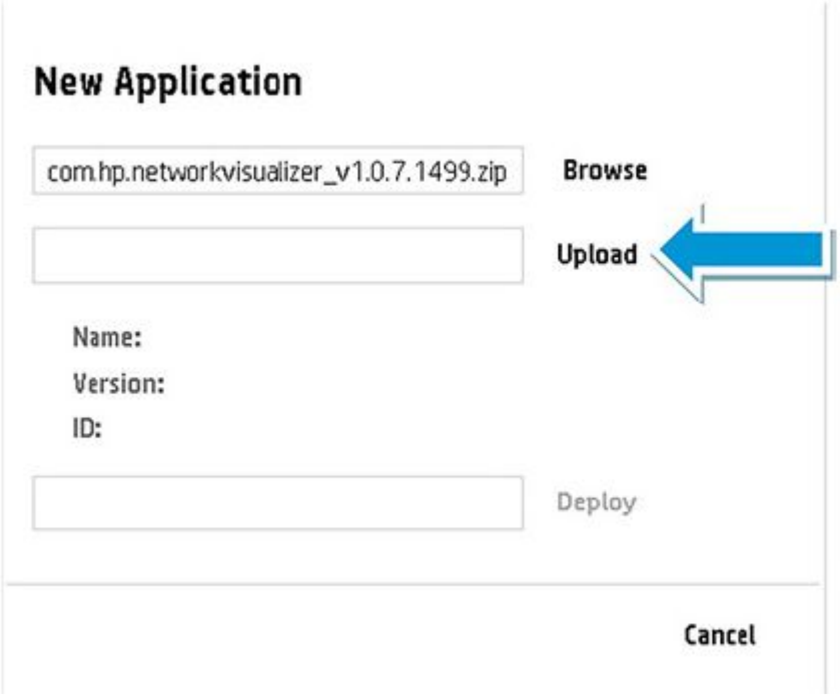
File name: com.hp.networkvisualizer_v1.0.7.1

All Files

Install the HP Network Visualizer Application

Upload

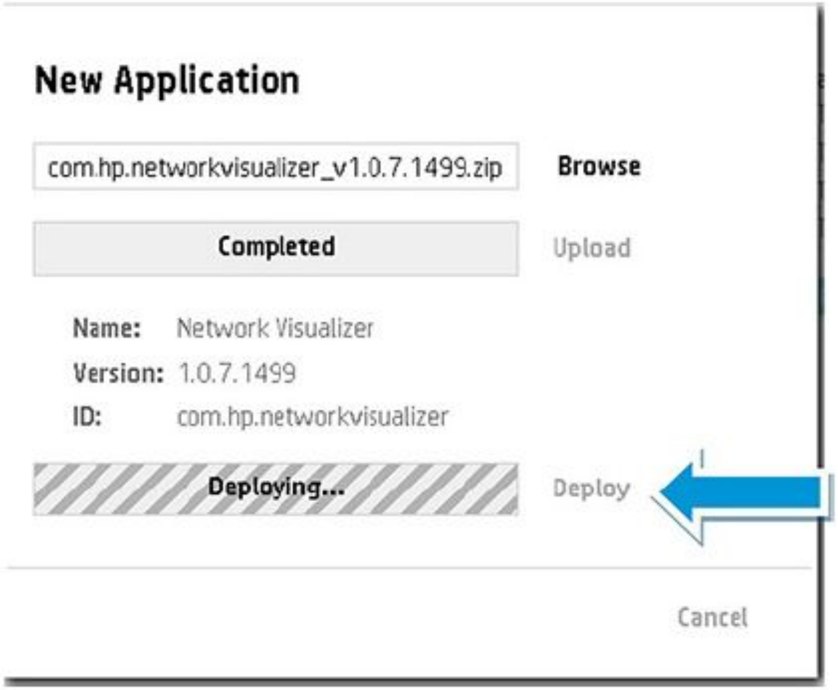
Deploy



New Application

com.hp.networkvisualizer_v1.0.7.1499.zip

Name:
Version:
ID:



New Application

com.hp.networkvisualizer_v1.0.7.1499.zip

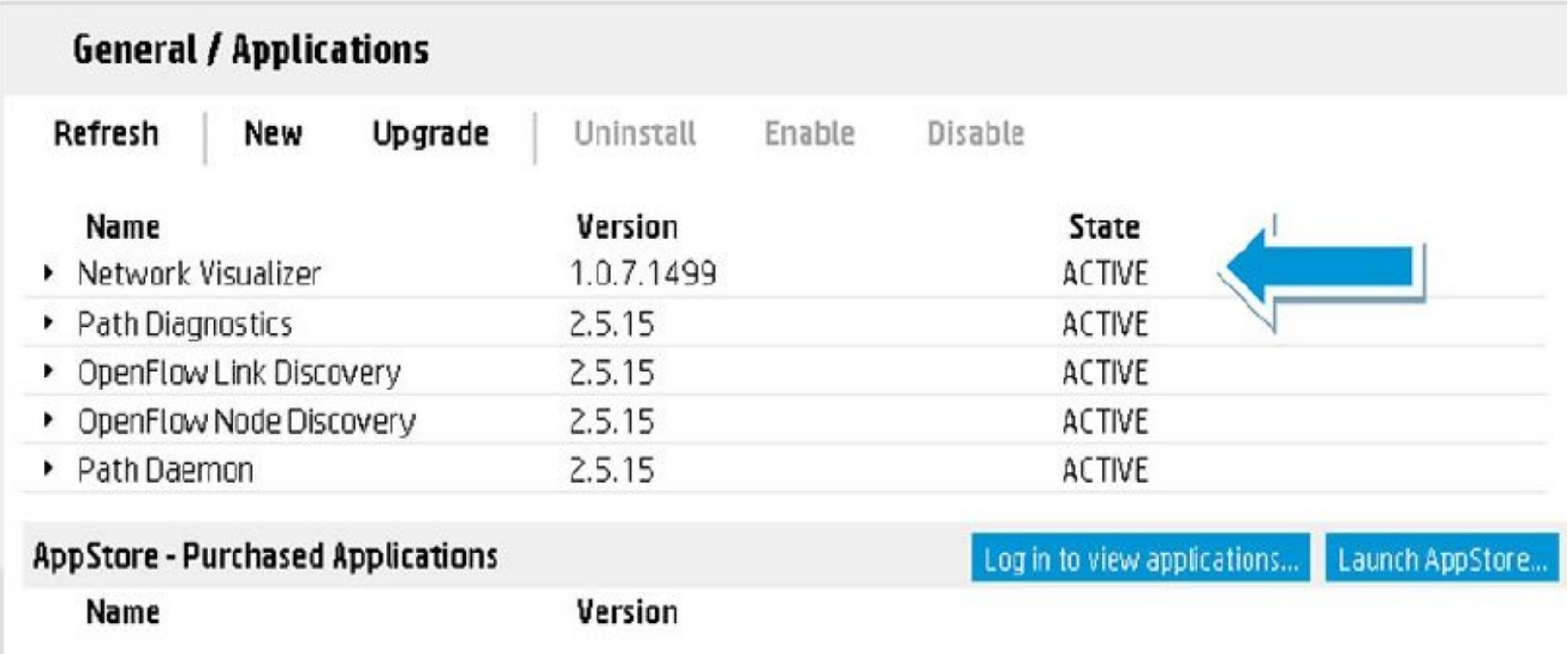
Completed

Name: Network Visualizer
Version: 1.0.7.1499
ID: com.hp.networkvisualizer

Deploying...

Install the HP Network Visualizer Application

ACTIVE



General / Applications

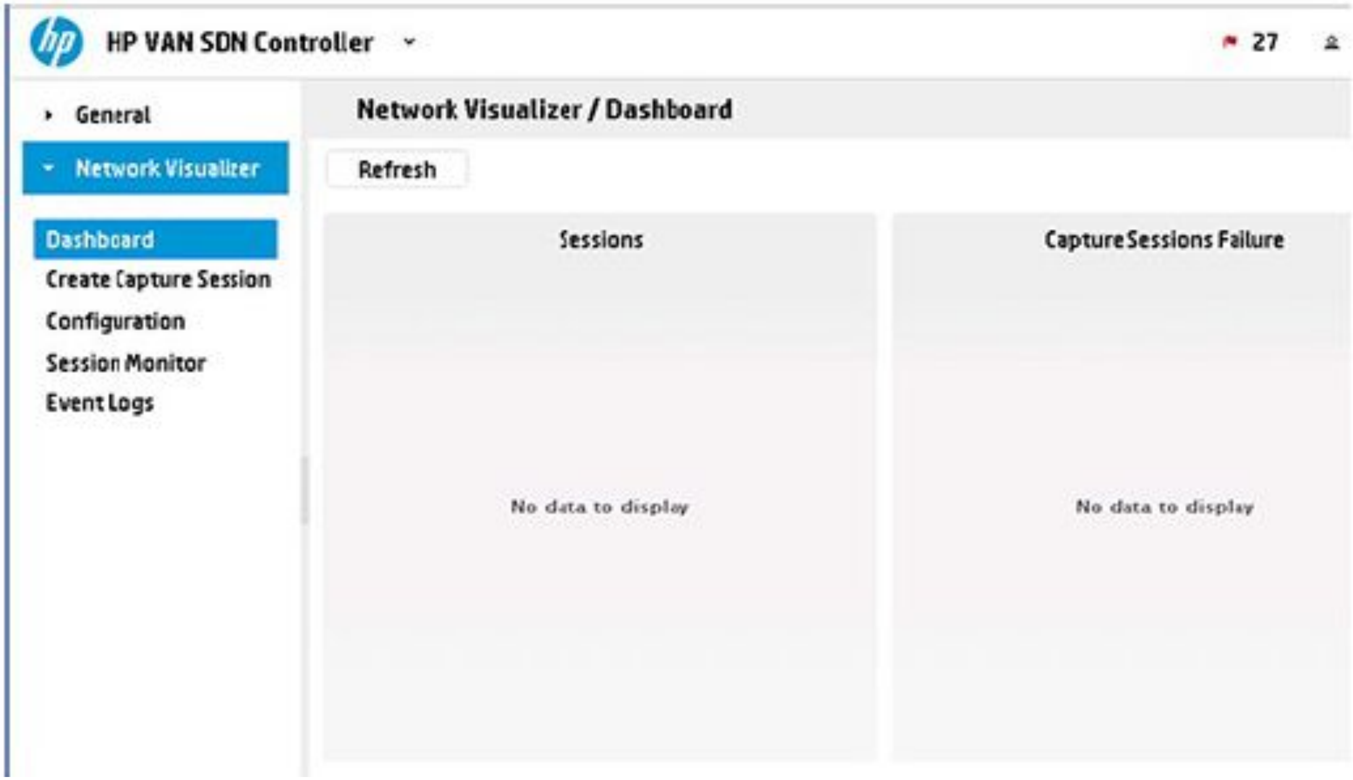
Name	Version	State
Network Visualizer	1.0.7.1499	ACTIVE
Path Diagnostics	2.5.15	ACTIVE
OpenFlow Link Discovery	2.5.15	ACTIVE
OpenFlow Node Discovery	2.5.15	ACTIVE
Path Daemon	2.5.15	ACTIVE

AppStore - Purchased Applications

Name	Version

Install the HP Network Visualizer Application

Network Visualizer



Network Visualizer / Dashboard

Sessions

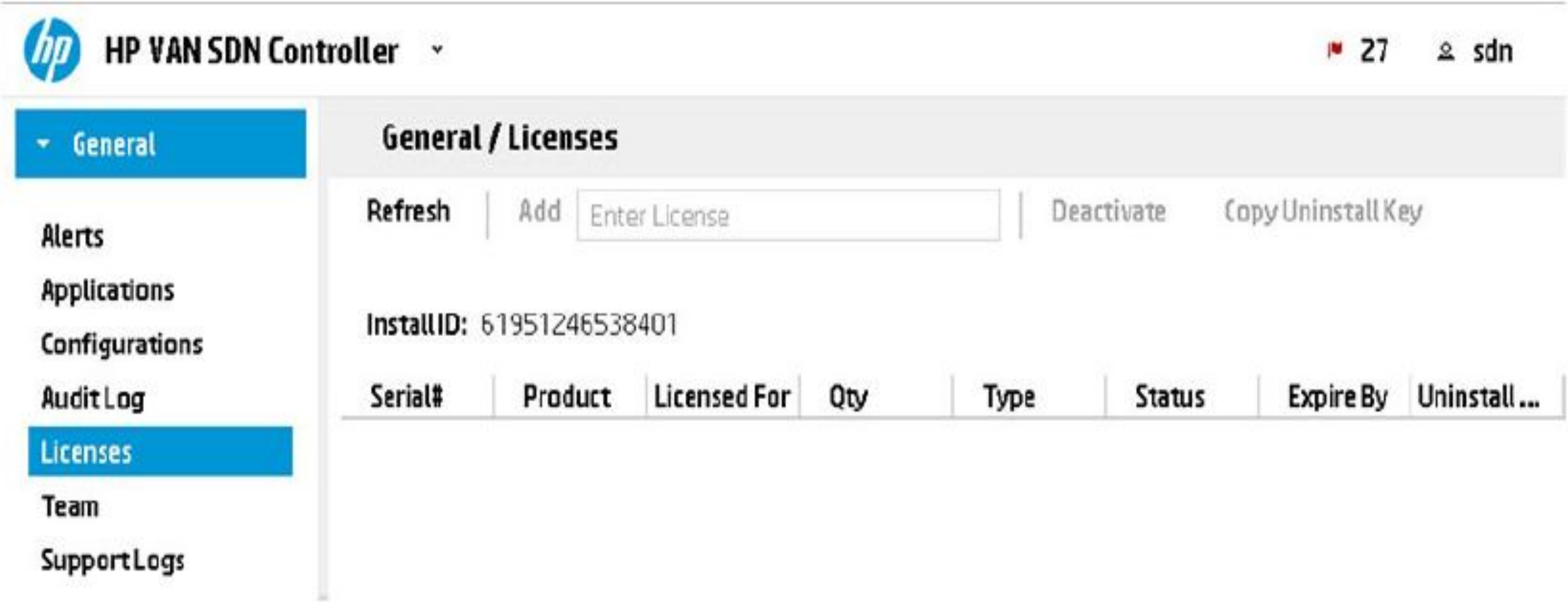
No data to display

Capture Sessions Failure

No data to display

Install the HP Network Visualizer Application

General Licenses



InstallID: 619512465384O1

Serial#	Product	Licensed For	Qty	Type	Status	Expire By	Uninstall ...

Network Visualizer licensing

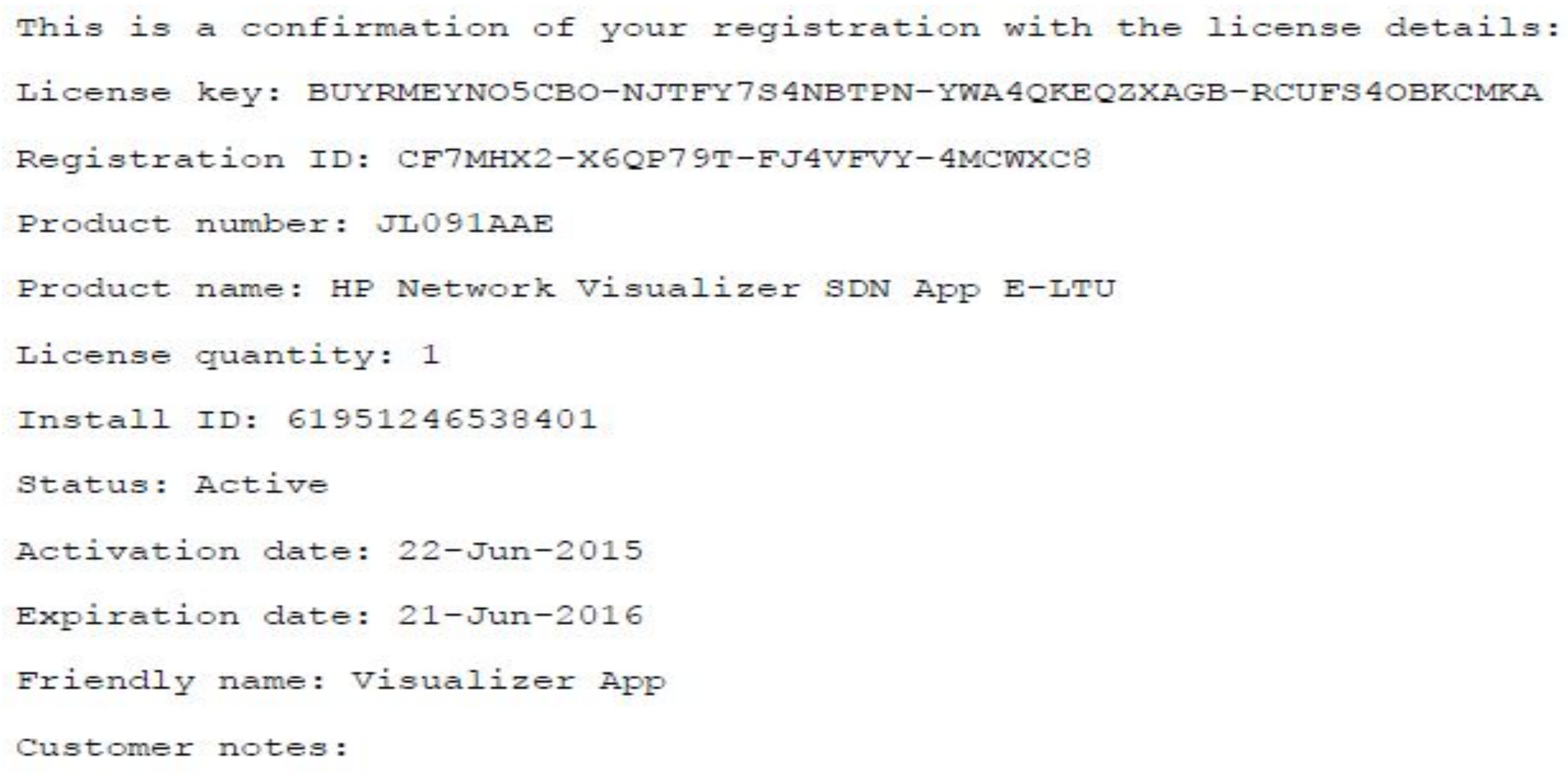
- A VAN SDN Controller Base license
- A Network Visualizer license

- JL091AAE HP Network Visualizer SDN App E-LTU
- J9863AAE HP VAN SDN Controller Base Software with 50-node License E-LTU

Network Visualizer licensing

- Install the HP VAN SDN Controller.
- Install the SDN Applications that you would like to evaluate. If you are using the AppStore, install the Trial Mode SDN applications.
- Go to the My Networking Portal http://www.hp.com/networking/mynetworking and select SDN Evaluation Licenses.
- Enter your install id. MNP generates every evaluation license possible for this install id.
- Apply the relevant licenses to the controller and applications.

Network Visualizer licensing



This is a confirmation of your registration with the license details:

License key: BUYRMEYNO5CBO-NJTFY7S4NBTPN-YWA4QKEQZXAGB-RCUFS4OBKCMKA

Registration ID: CF7MHX2-X6QP79T-FJ4VFVY-4MCWXC8

Product number: JL091AAE

Product name: HP Network Visualizer SDN App E-LTU

License quantity: 1

Install ID: 61951246538401

Status: Active

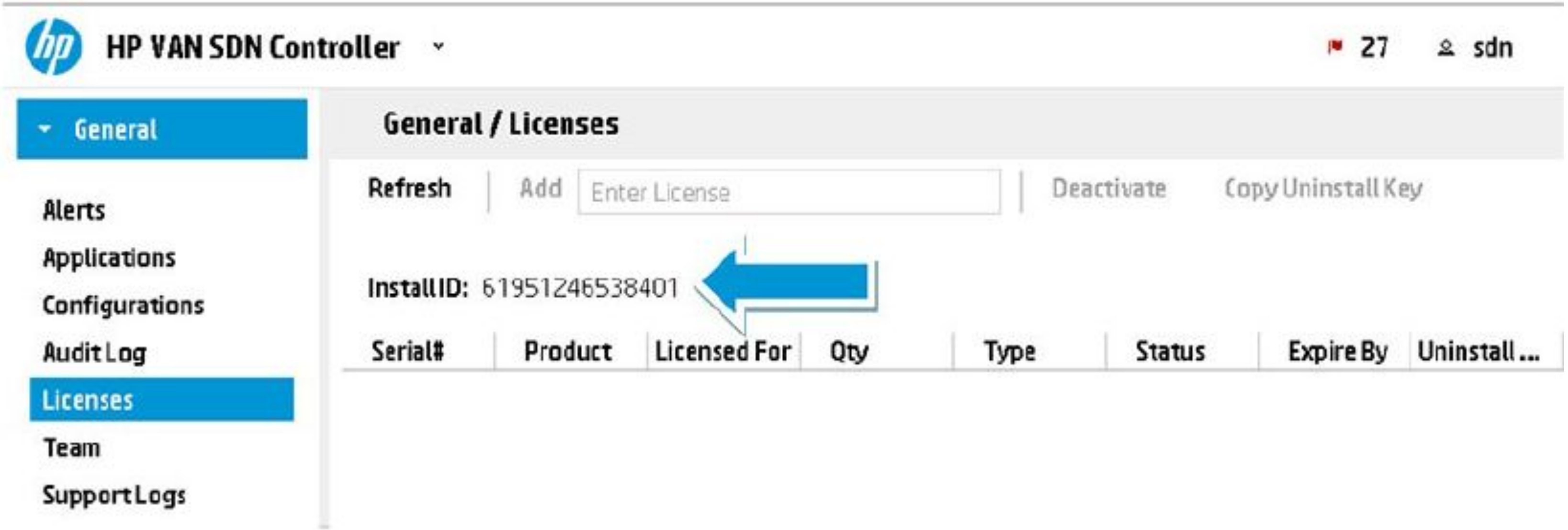
Activation date: 22-Jun-2015

Expiration date: 21-Jun-2016

Friendly name: Visualizer App

Customer notes:

Network Visualizer licensing

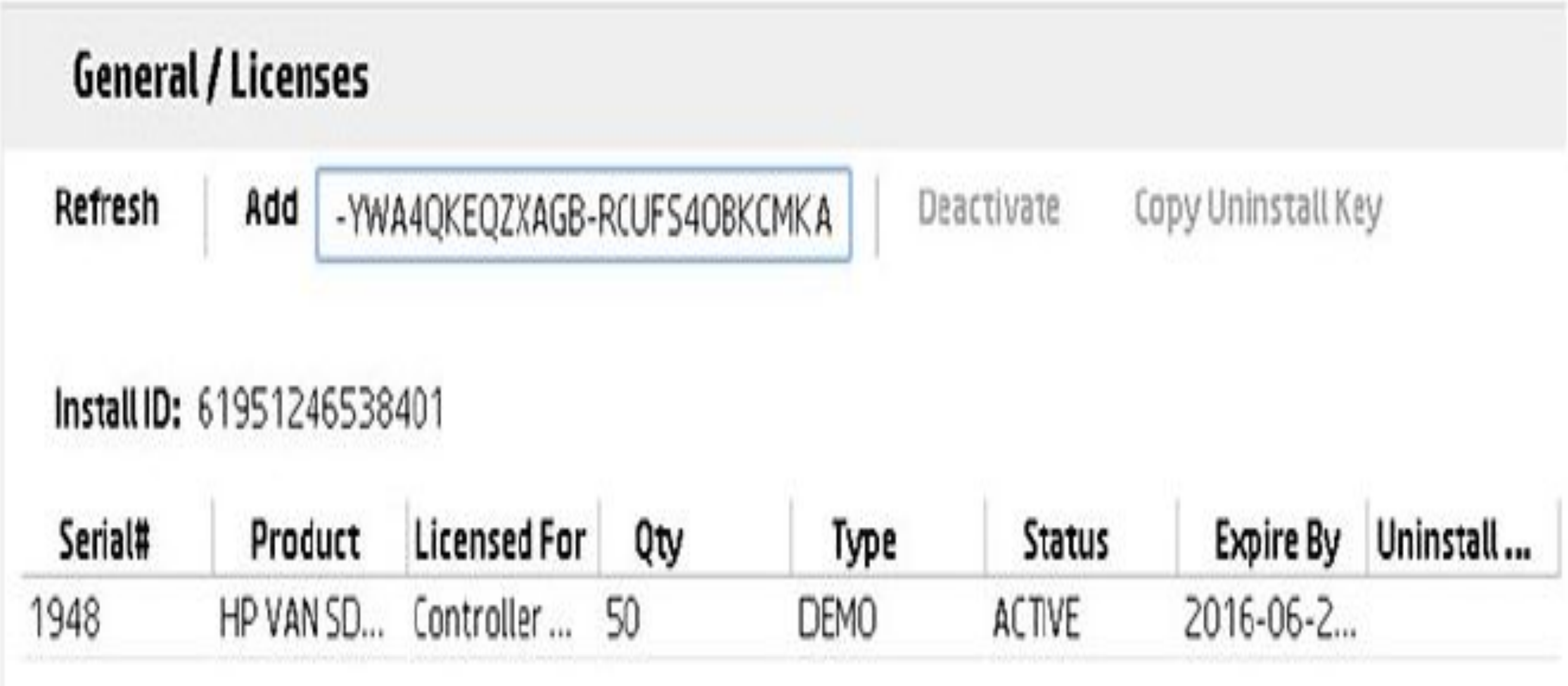


InstallID: 61951246538401

Serial#	Product	Licensed For	Qty	Type	Status	Expire By	Uninstall ...

Desktop\SDN Lab Files\Software\Network Visualizer license Key.txt

Network Visualizer licensing

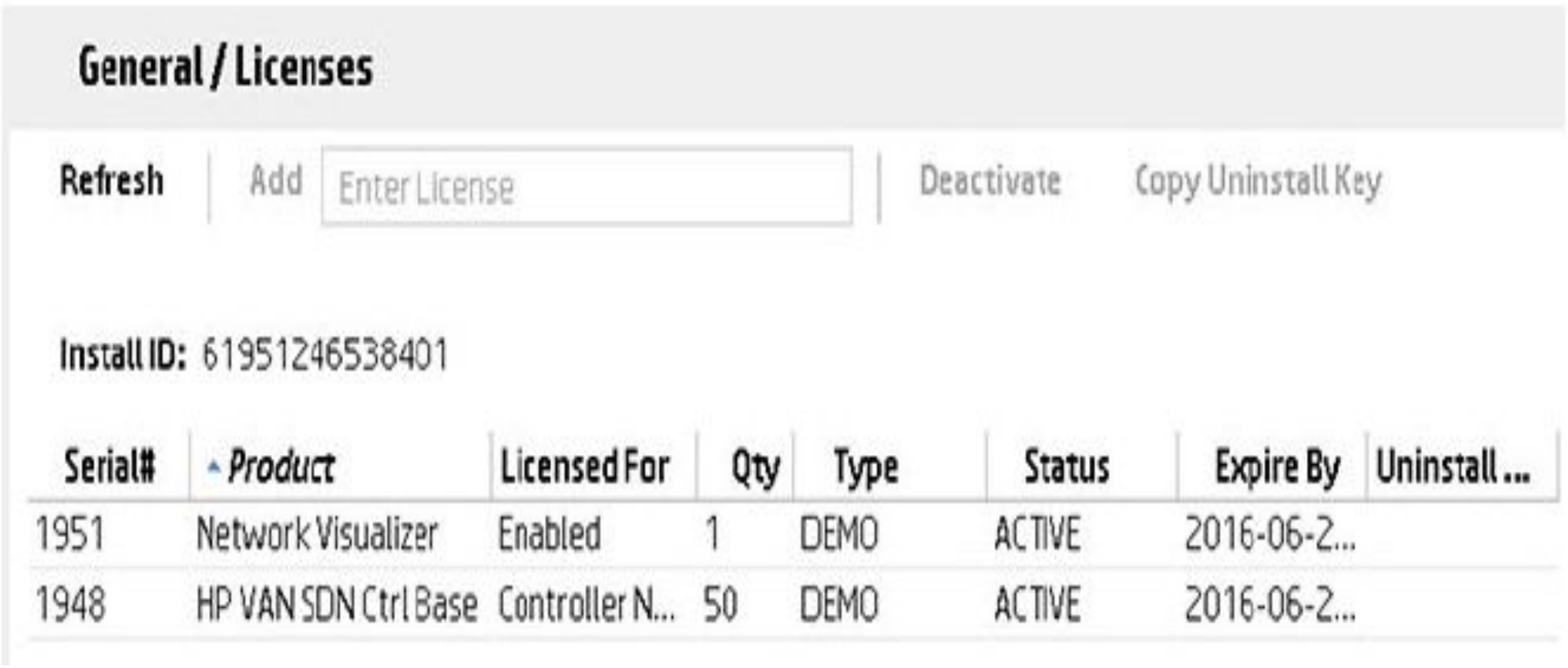


-YWA4QKEQZXAGB-RCUFS4OBKCMKA

Install ID: 61951246538401

Serial#	Product	Licensed For	Qty	Type	Status	Expire By	Uninstall...
1948	HP VAN SD...	Controller ...	50	DEMO	ACTIVE	2016-06-2...	

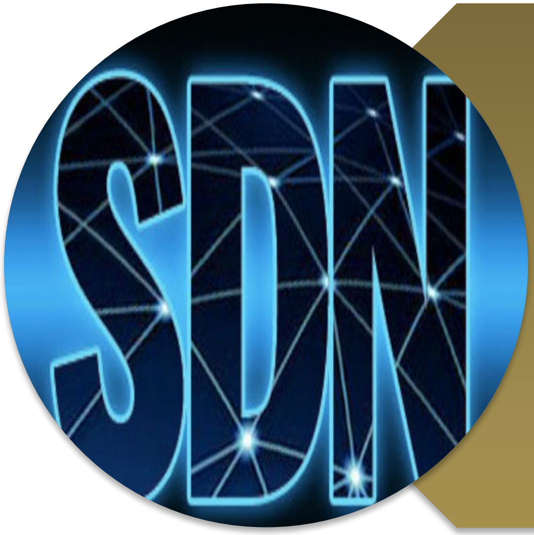
Network Visualizer licensing



General / Licenses

Install ID: 61951246538401

Serial#	▴ *Product*	Licensed For	Qty	Type	Status	Expire By	Uninstall ...
1951	Network Visualizer	Enabled	1	DEMO	ACTIVE	2016-06-2...	
1948	HP VAN SDN Ctrl Base	Controller N...	50	DEMO	ACTIVE	2016-06-2...	



HP Network Visualizer SDN

Capture destinations

Managed destination:

- Runs as a daemon service that receives capture packets and persists them in pcap format. A local managed destination is installed when you install Network Visualizer. You must configure and deploy remote destinations from Network Visualizer.

Unmanaged destination:

- You can run a program or solution to process the incoming copy traffic from the network device.

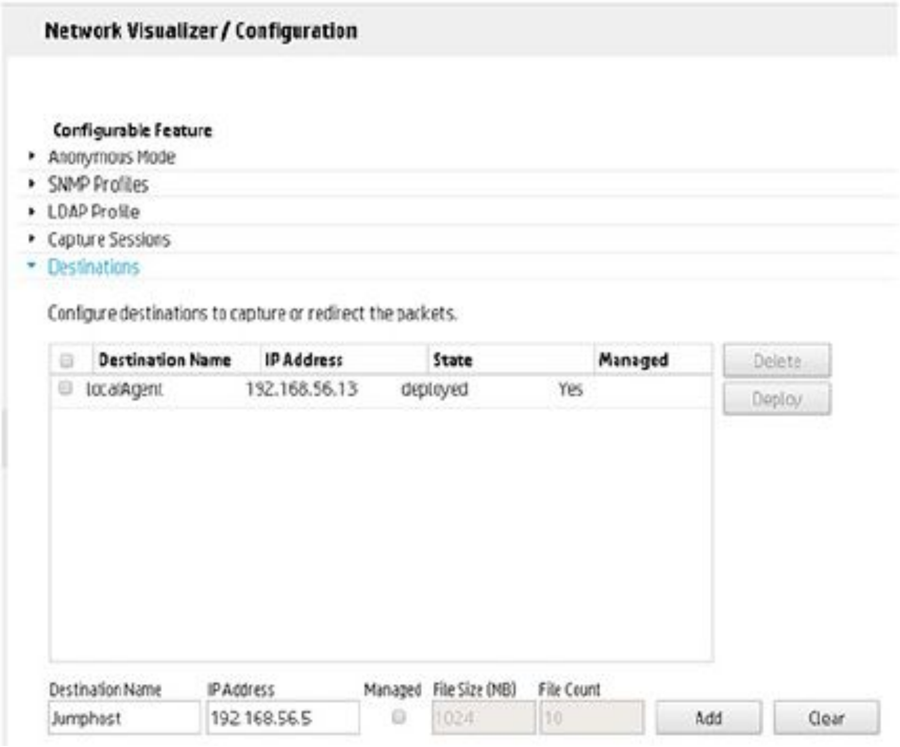
Capture destinations

State

Destinations

Receiver for copied traffic

- Local Destination installed by default
- Managed destination
  - Local or remote service
  - PCAP capture format
- Unmanaged destination
  - Application to capture incoming packets



Network Visualizer / Configuration

Configurable Feature

- Anonymous Mode
- SNMP Profiles
- LDAP Profile
- Capture Sessions
- Destinations

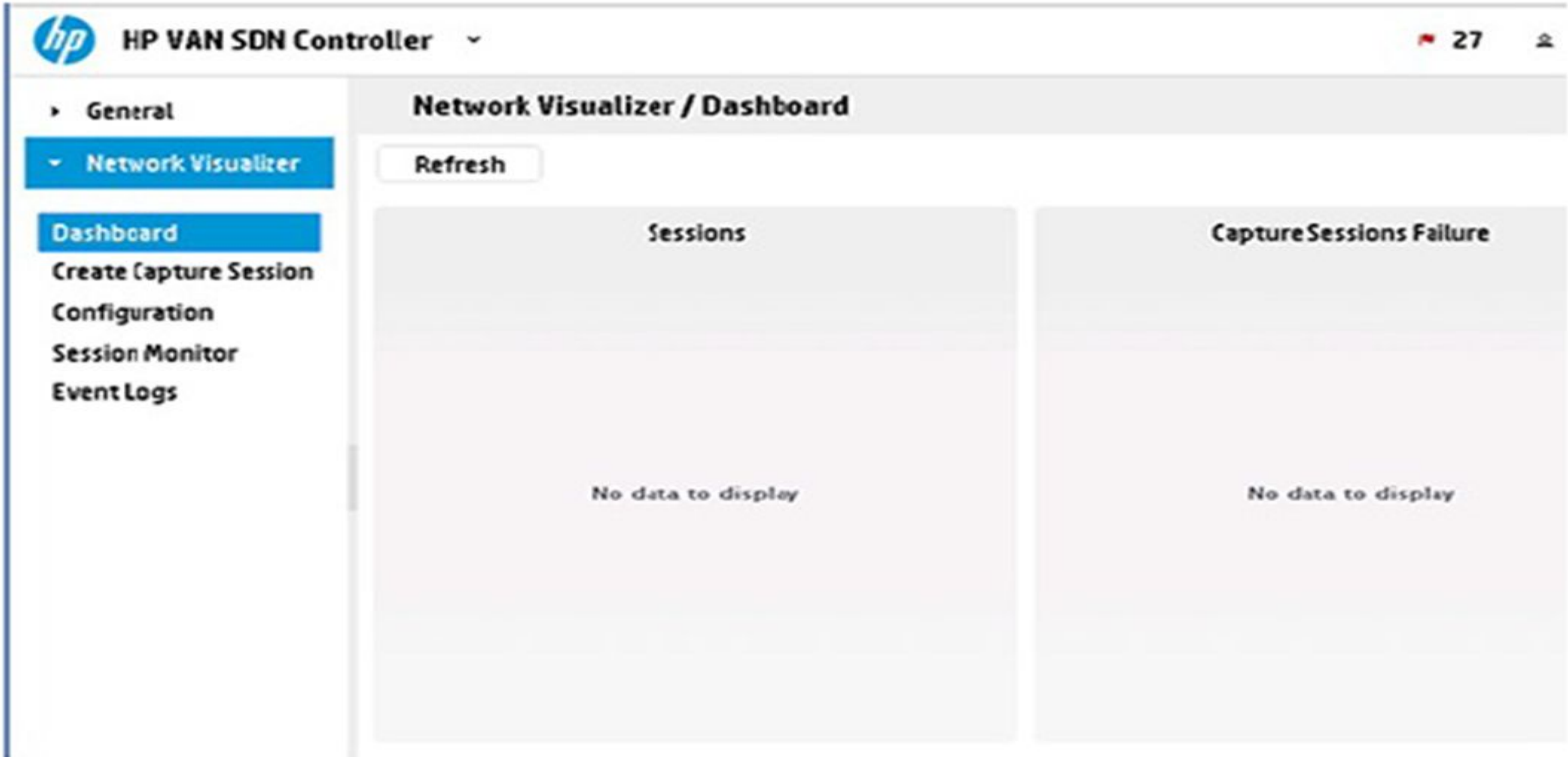
Configure destinations to capture or redirect the packets.

☐	Destination Name	IP Address	State	Managed
☐	localAgent	192.168.56.13	deployed	Yes

Destination Name	IP Address	Managed	File Size (MB)	File Count
Jumphost	192.168.56.5	☐	1024	10

Custom mode capture

Create Capture
Session



No data to display

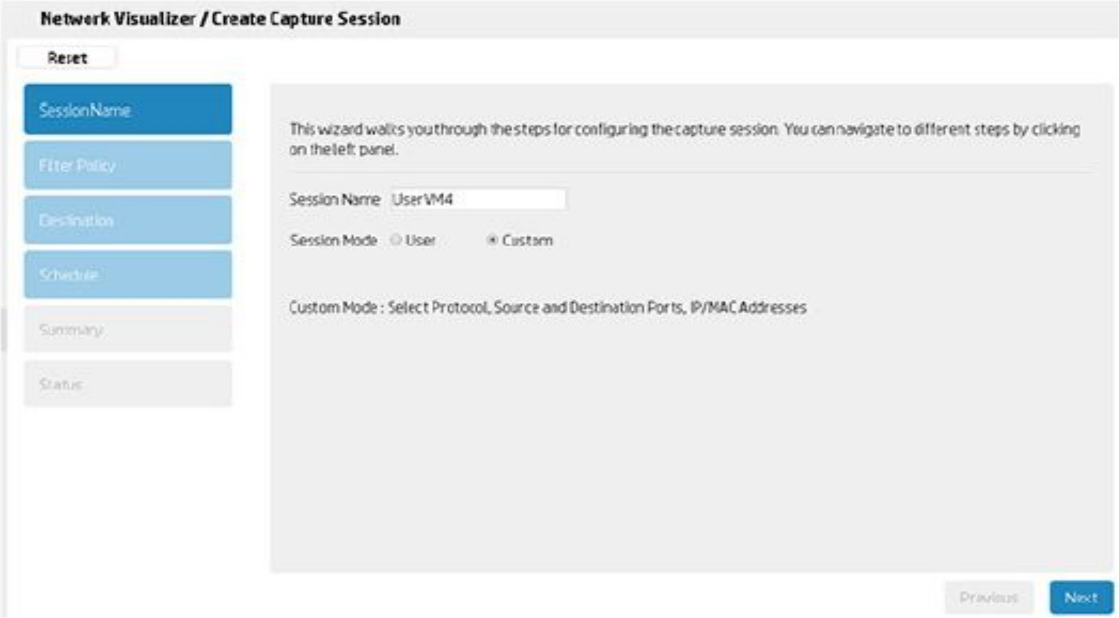
No data to display

Custom mode capture

Custom:	• **Configure the source/destination IP address, source/destination MAC address, port, and protocol for a capture session.**
User:	• **Configure the user, user group, device(s), and application for a capture session.**

Filter Policy – Custom Mode

- Legacy ACL-like match conditions
- Supports scheduled capture
- Supports local or remote destination
- Supports activate/deactivate



Network Visualizer / Create Capture Session

This wizard walks you through the steps for configuring the capture session. You can navigate to different steps by clicking on the left panel.

Session Name: UserVM4

Session Mode: ○ User ● Custom

Custom Mode : Select Protocol, Source and Destination Ports, IP/MAC Addresses

Custom mode capture

In the first step,

- User
- Custom

Custom mode capture

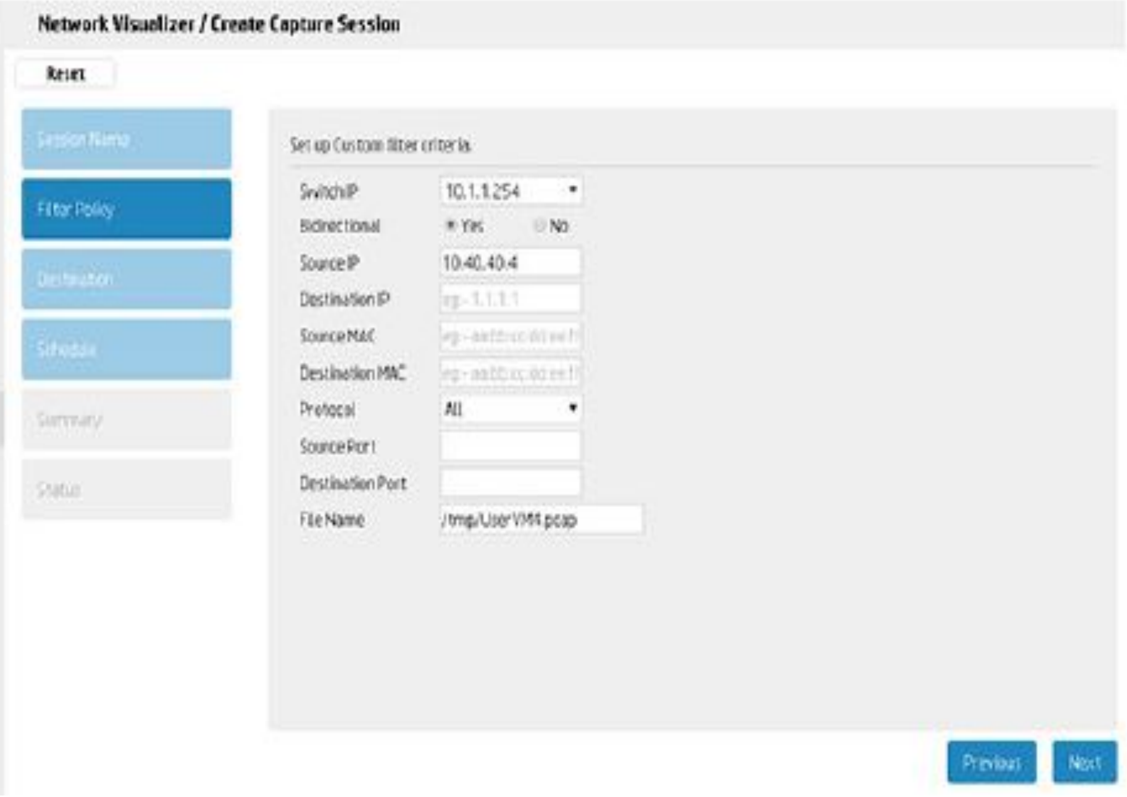
In the second step

Filter Criteria

- Select Switch by IP address
- Choose traffic direction to monitor
- IP address: source, destination
- MAC address: source, destination
- Protocol
- L4 Port: source, destination
- Configure capture file name

Note

- All fields are optional, but at least one must to be configured



Set up Custom filter criteria

Switch IP	10.1.1.254 ▾
Bidirectional	● Yes ○ No
Source IP	10.40.40.4
Destination IP	eg - 1.1.1.1
Source MAC	eg - aa:bb:cc:dd:ee:ff
Destination MAC	eg - aa:bb:cc:dd:ee:ff
Protocol	All ▾
Source Port	
Destination Port	
File Name	/tmp/UserVM4.pcap

Custom mode capture

- IP address of the network device
- Select the traffic capture direction by clicking one of the following: Yes: Captures packets sent and received by the user. No: Captures packets sent by the user
- IP address of the source (for example, 10.40.40.4)
- IP address of the destination (for example, 192.168.56.51)
- MAC address of the source (for example, aa:bb:cc:dd:ee:ff)
- MAC address of the destination (for example, aa:bb:cc:dd:ee:ff)
- Network protocol. By default, protocol is All
- Layer 4 port for the source
- Layer 4 port for the destination
- Name of the pcap file in which to save the packets

Custom mode capture

third step

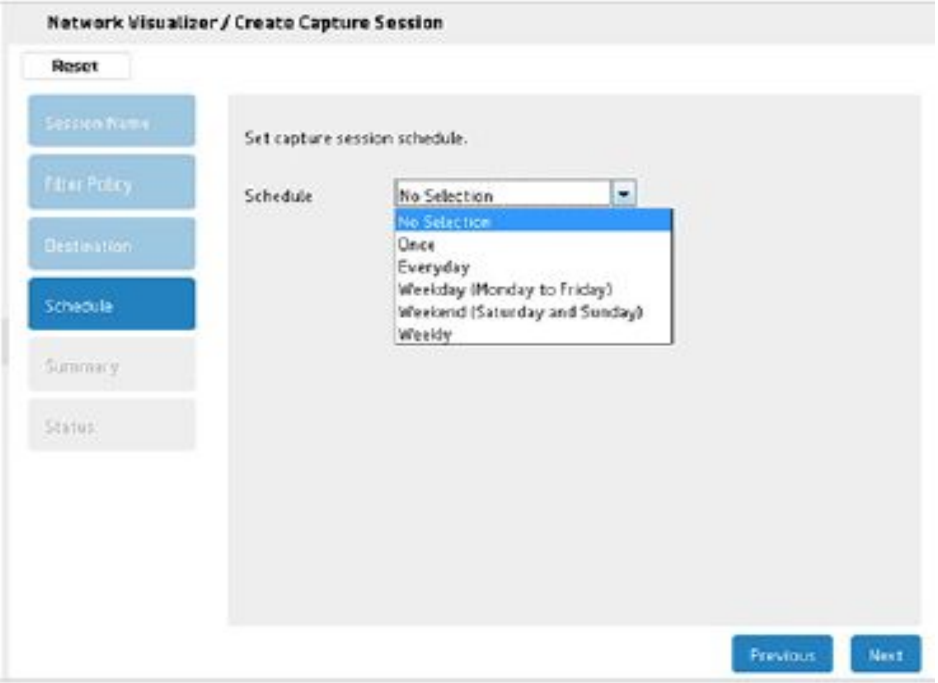
fourth step

Schedule

- Select one schedule type

Note

- No selection results in activated session running immediately, and only stops when session is deactivated.



Network Visualizer / Create Capture Session

Set capture session schedule.

Schedule: No Selection

Custom mode capture

	• Monitoring of a capture session is not scheduled.
	• Monitor the capture session once. Specify the Start Time and Stop Time.
	• Monitor the capture session everyday. Specify the repeat interval in Repeat every (days), Start Time, Stop Time, and End Date.
	• Monitor the capture session on weekdays. Specify the Start Time, Stop Time, and End Date.
	• Monitor the capture session on weekends. Specify the Start Time, Stop Time, and End Date.
	• Monitor the capture session on a weekly basis. Select the days of the week to capture the sessions with Repeat on check boxes. Specify the Start Time, Stop Time, and End Date.

Custom mode capture

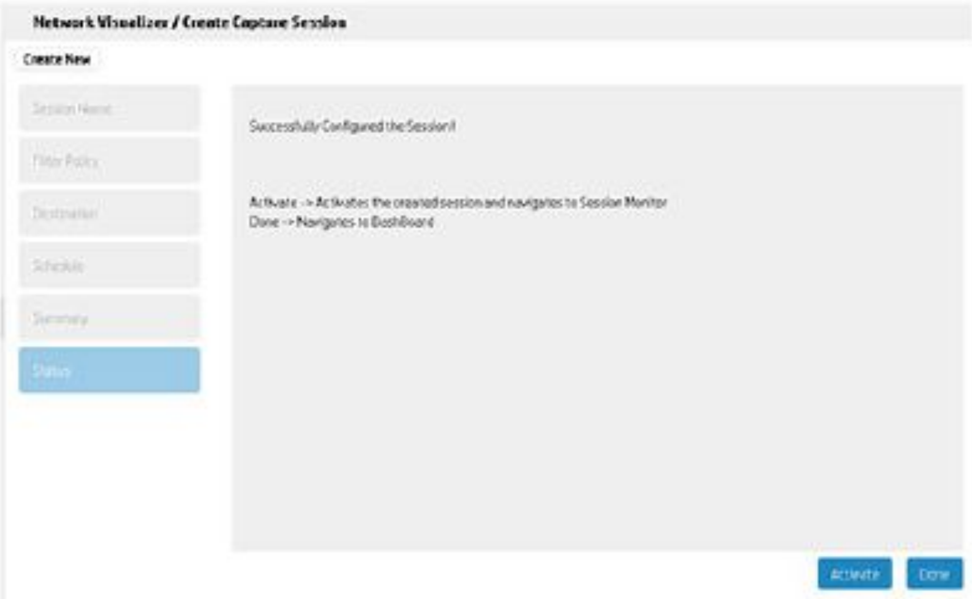
The last step

Behavior after Activation

- Non-scheduled session: capture rule is installed immediately if devices are discovered
- Scheduled session: scheduled session is saved, and once time range is reached, capture rule is installed if devices are discovered
- In both case, system updates number of runs

How to Activate

- At the end of wizard, click "Activate" button to activate session.
- Configuration → Capture Session, click "Activate" to activate selected session
- Session Monitor → Select session and click "Activate"



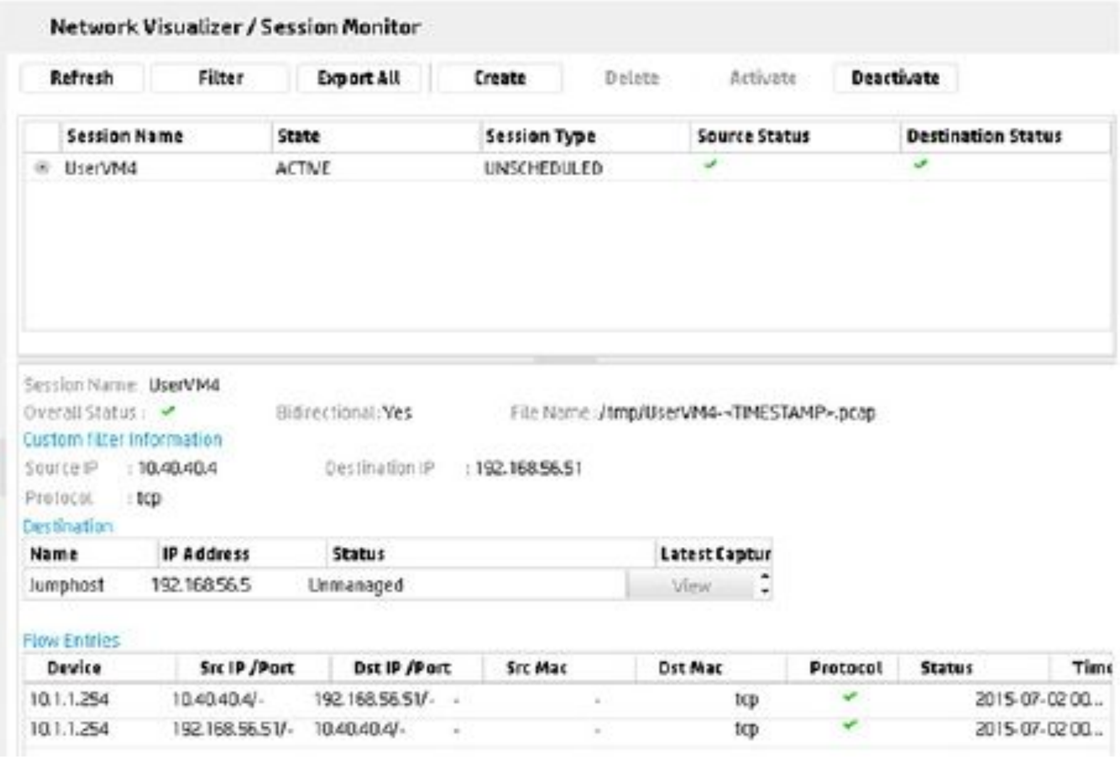
Successfully Configured the Session!

Activate -> Activates the created session and navigates to Session Monitor
Done -> Navigates to DashBoard

Session Monitor

Session Operational Status

- Session failure reason
- Flows installed for activated session
- Number of runs



	Session Name	State	Session Type	Source Status	Destination Status
○	UserVM4	ACTIVE	UNSCHEDULED	✓	✓

Session Name: UserVM4

Overall Status : ✓ Bidirectional: Yes File Name : /tmp/UserVM4-<TIMESTAMP>.pcap

Custom filter information

Source IP : 10.40.40.4 Destination IP : 192.168.56.51

Protocol : tcp

Destination

Name	IP Address	Status	Latest Captur
Jumphost	192.168.56.5	Unmanaged	View

Flow Entries

Device	Src IP /Port	Dst IP /Port	Src Mac	Dst Mac	Protocol	Status	Time
10.1.1.254	10.40.40.4/-	192.168.56.51/-	-	-	tcp	✓	2015-07-02 00...
10.1.1.254	192.168.56.51/-	10.40.40.4/-	-	-	tcp	✓	2015-07-02 00...

Session Monitor

View

Refresh

Filter

Export All

Create

Delete

Activate Deactivate

Enable Disable

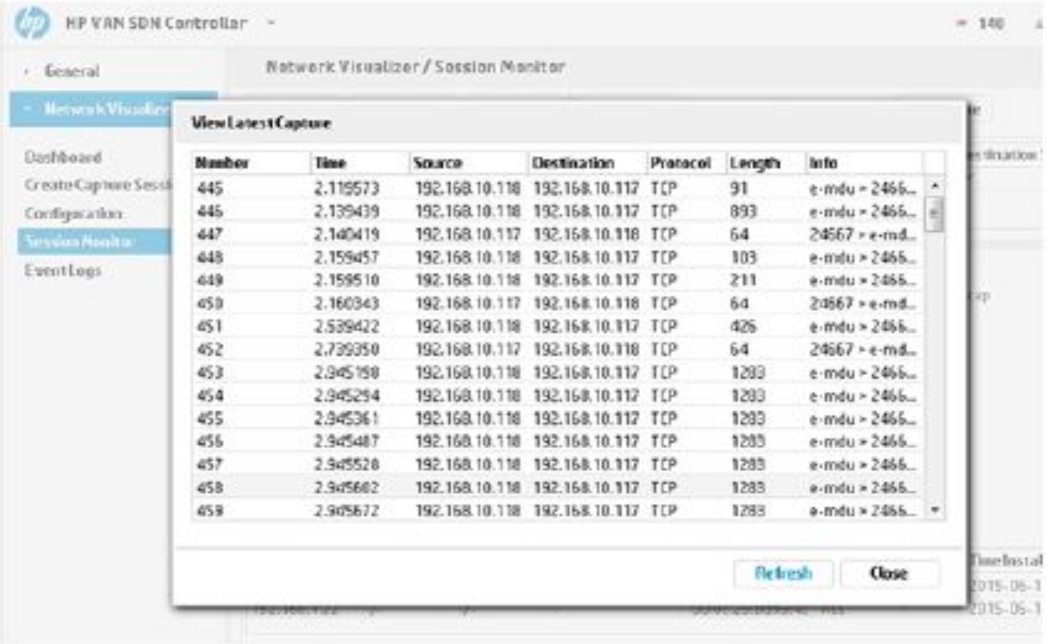
Session Monitor

Session Monitor

- Activated session
- Click “View” Button

Configuration → Capture Session

- Activated session
- Click “View” Button



View Latest Capture

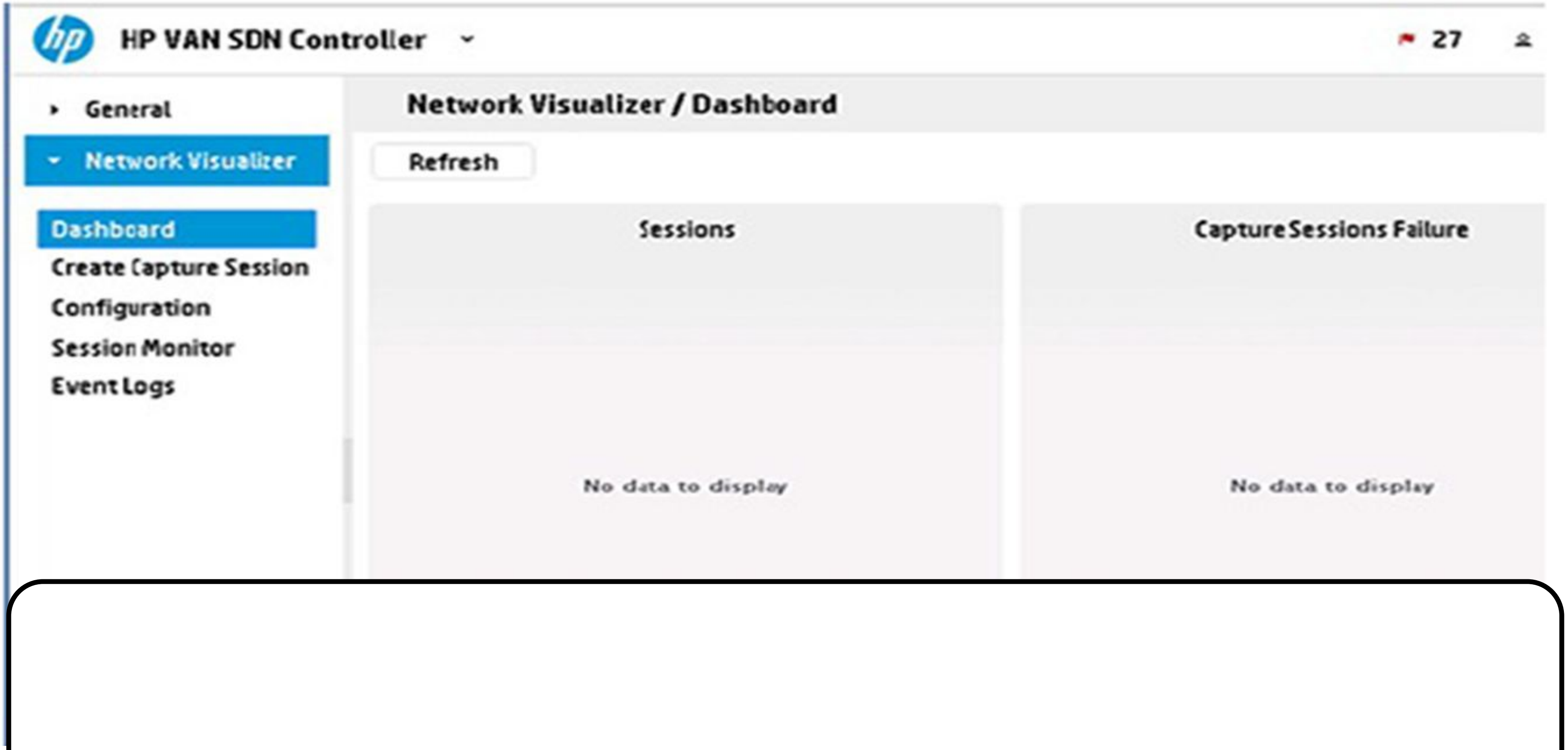
Number	Time	Source	Destination	Protocol	Length	Info
445	2.119573	192.168.10.118	192.168.10.117	TCP	91	e-mdu > 2466...
446	2.139439	192.168.10.118	192.168.10.117	TCP	893	e-mdu > 2466...
447	2.140419	192.168.10.117	192.168.10.118	TCP	64	24667 > e-md...
448	2.159457	192.168.10.118	192.168.10.117	TCP	103	e-mdu > 2466...
449	2.159510	192.168.10.118	192.168.10.117	TCP	211	e-mdu > 2466...
450	2.160343	192.168.10.117	192.168.10.118	TCP	64	24667 > e-md...
451	2.539422	192.168.10.118	192.168.10.117	TCP	426	e-mdu > 2466...
452	2.739350	192.168.10.117	192.168.10.118	TCP	64	24667 > e-md...
453	2.945198	192.168.10.118	192.168.10.117	TCP	1283	e-mdu > 2466...
454	2.945294	192.168.10.118	192.168.10.117	TCP	1283	e-mdu > 2466...
455	2.945361	192.168.10.118	192.168.10.117	TCP	1283	e-mdu > 2466...
456	2.945487	192.168.10.118	192.168.10.117	TCP	1283	e-mdu > 2466...
457	2.945528	192.168.10.118	192.168.10.117	TCP	1283	e-mdu > 2466...
458	2.945602	192.168.10.118	192.168.10.117	TCP	1283	e-mdu > 2466...
459	2.945672	192.168.10.118	192.168.10.117	TCP	1283	e-mdu > 2466...

View

Refresh

Network Visualizer Dashboard

Dashboard Network Visualizer



Network Visualizer Dashboard

Sessions

- Sessions chart displays the current state of all the capture sessions

Capture Sessions Failure

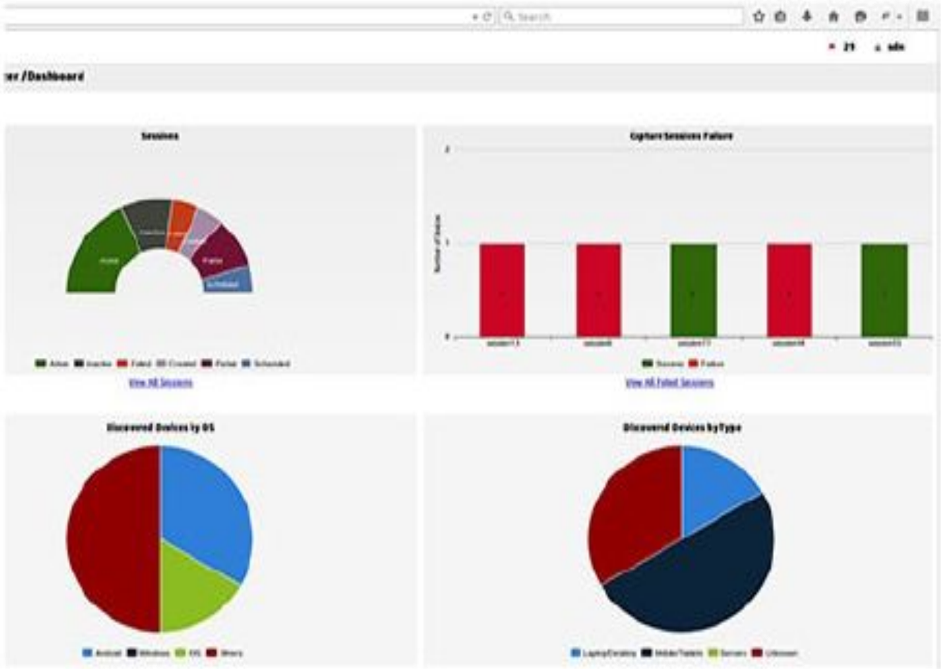
- The information about the deployment of monitoring policies across configured network devices for the most recent five unique sessions

Discovered Devices by OS

- Discovered devices by operating systems

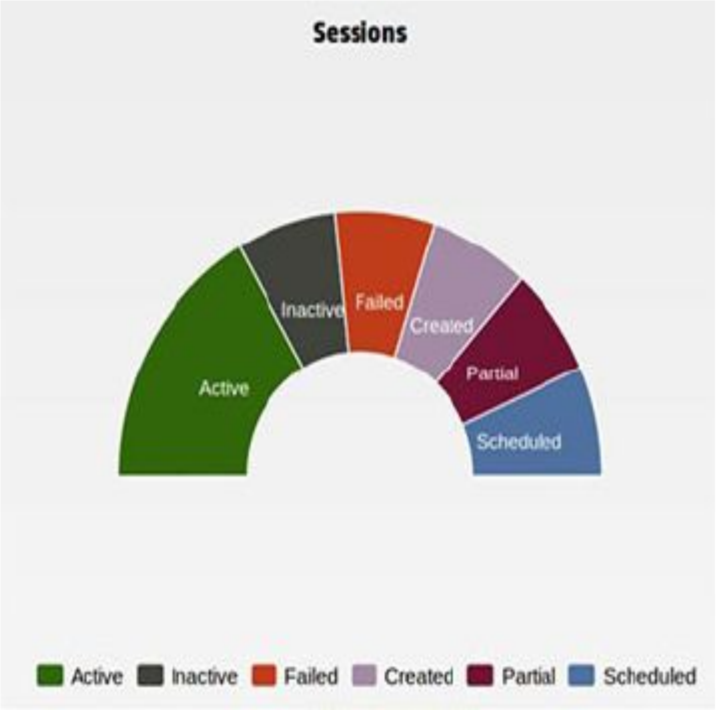
Discovered Devices by Type

- Discovered devices by device types

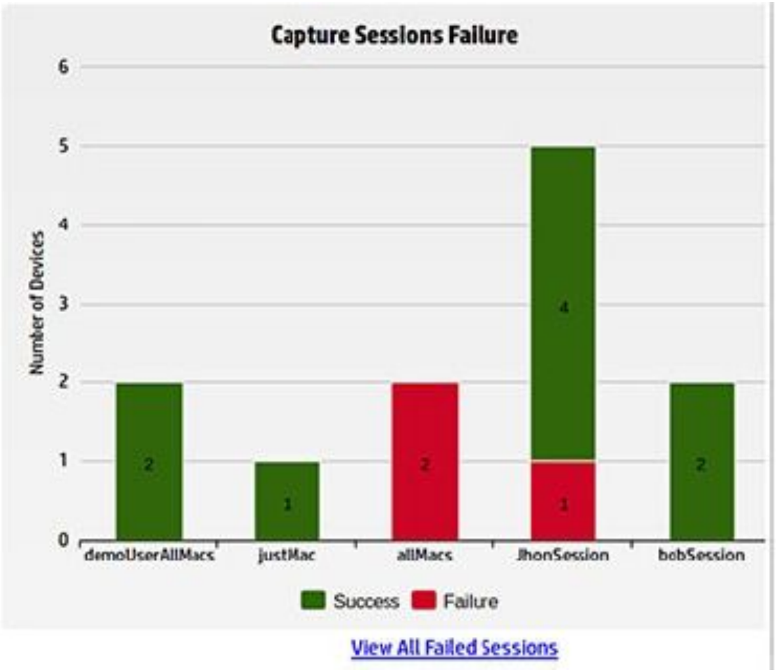

Search
/Dashboard
Sessions
Active
Active Inactive Failed Created Partial Scheduled
View All Sessions
Capture Sessions Failure
2
1
0
Success Failure
View All Failed Sessions
Discovered Devices by OS
Android Windows iOS Others
Discovered Devices by Type
Laptop/Desktop Mobile/Tablets Servers Unknown

Sessions chart

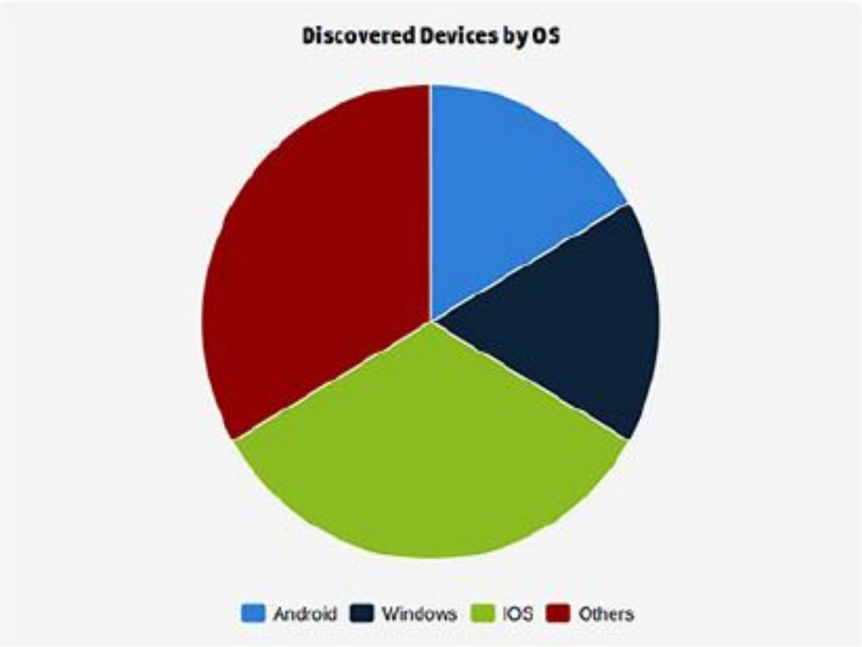
Created — **Number of created capture sessions**
Active — **Number of active capture sessions**
Inactive — **Number of inactive capture sessions**
Partial — **Number of sessions for which the network traffic capture failed on a few devices**
Failed — **Number of sessions for which the network traffic capture failed**
Scheduled — **Number of sessions for which network traffic capture is scheduled**

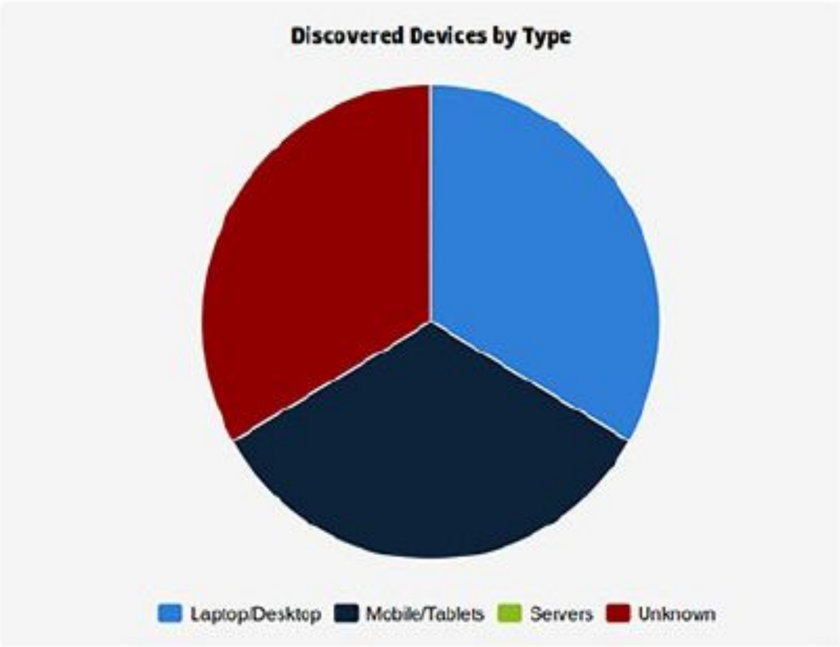


Capture Sessions Failure chart



Discovered devices

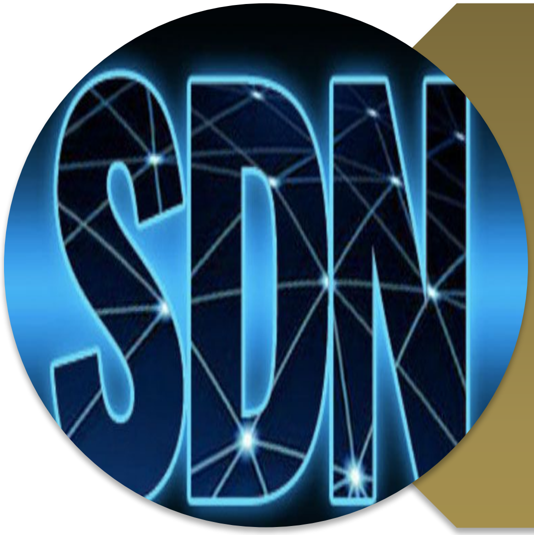




Discovered devices

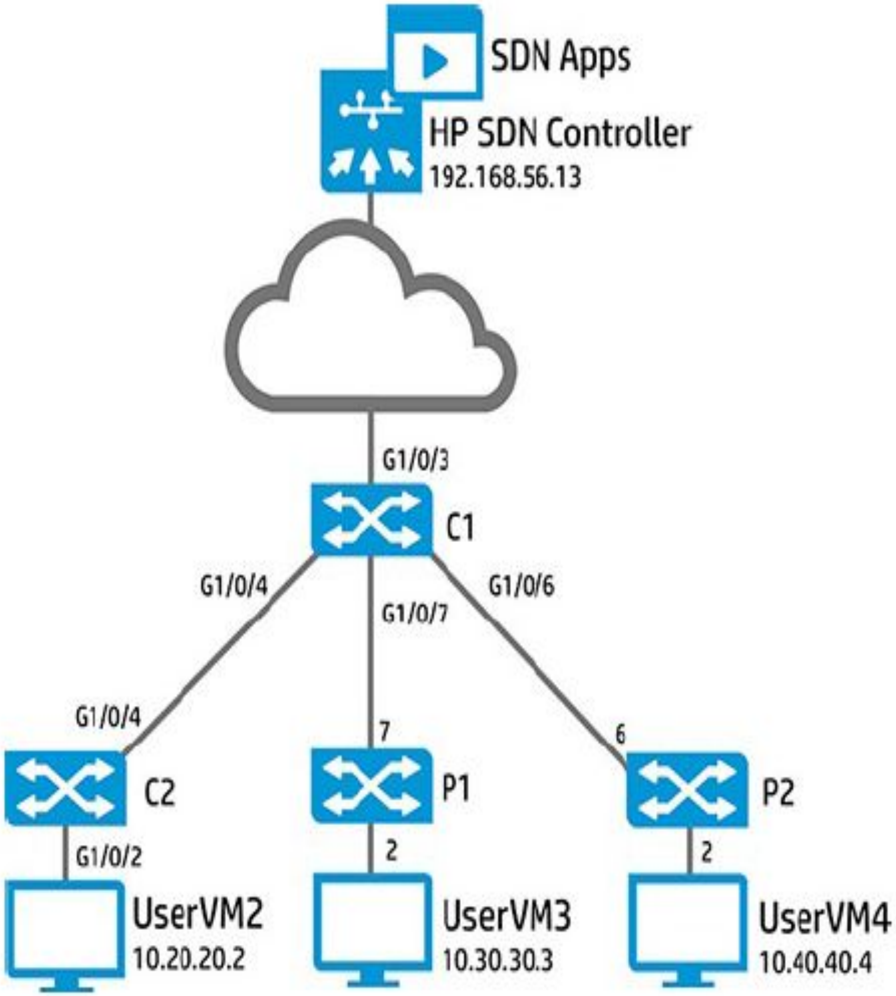
- Android: Indicates the number of devices with Android operating system.
- Windows: Indicates the number of devices with Windows operating system.
- IOS: Indicates the number of devices with iOS operating system.
- Others: Indicates the number of devices with any other operating system.

- Laptop/Desktop: Indicates the number of discovered laptops and desktops.
- Mobiles/Tablets: Indicates the number of discovered mobile devices and tablets.
- Servers: Indicates the number of discovered servers.
- Unknown: Indicates the number of discovered unknown devices.

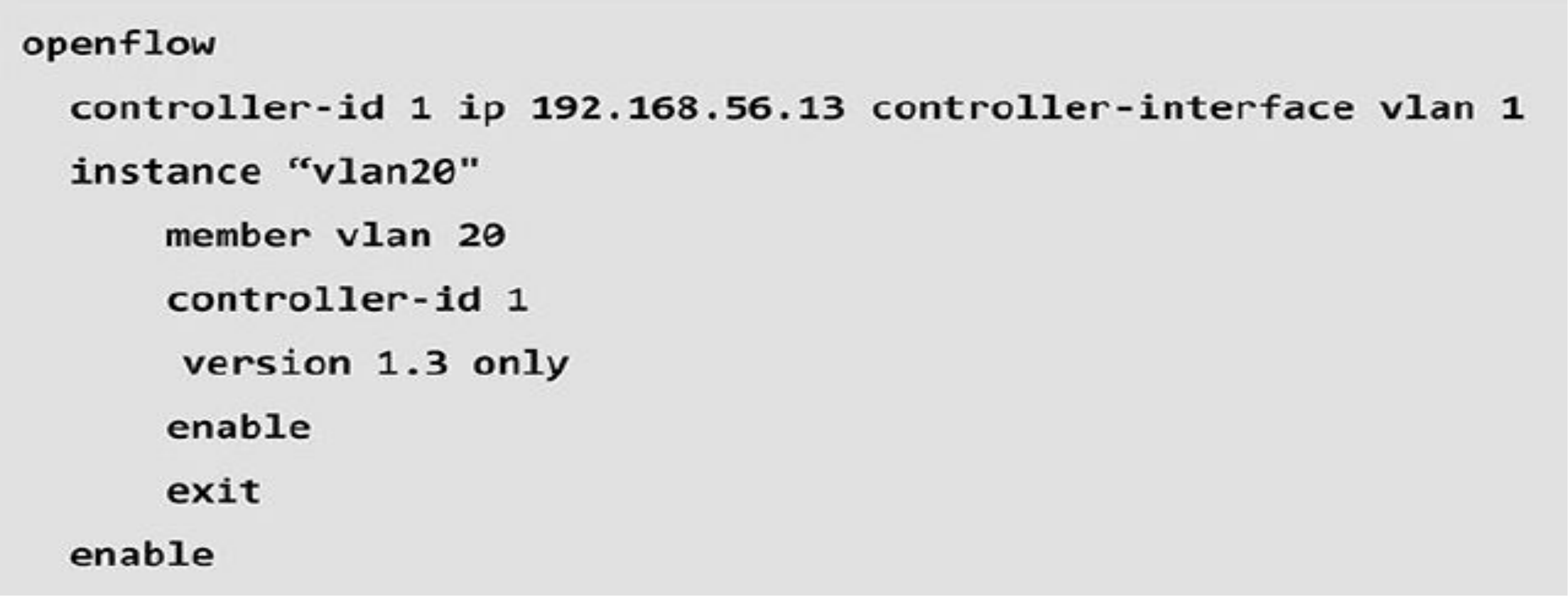


HP Network Visualizer SDN

Example topology for instructions

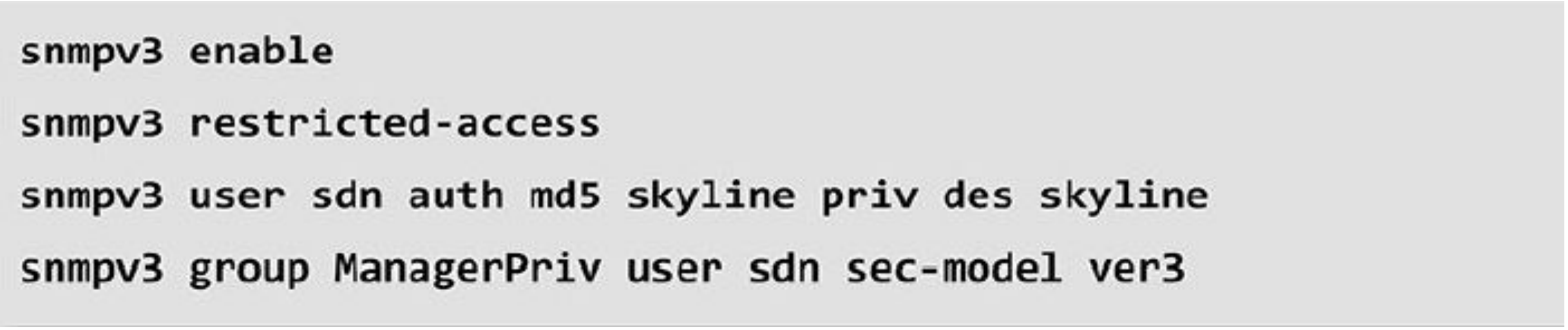


Switch configuration



```
openflow
   controller-id 1 ip 192.168.56.13 controller-interface vlan 1
   instance “vlan20"
         member vlan 20
         controller-id 1
          version 1.3 only
         enable
         exit
   enable
```

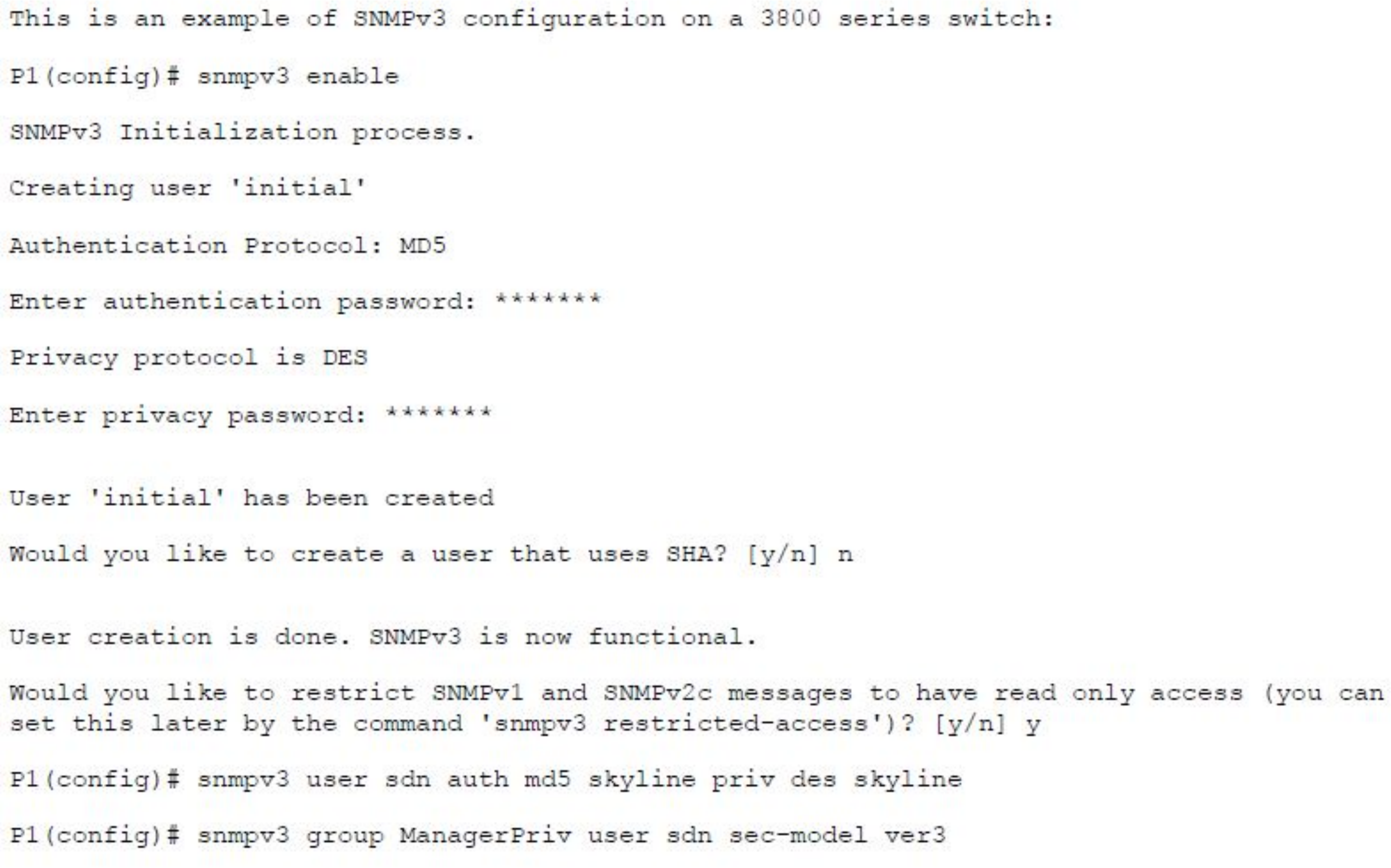
Switch configuration



```
snmpv3 enable
snmpv3 restricted-access
snmpv3 user sdn auth md5 skyline priv des skyline
snmpv3 group ManagerPriv user sdn sec-model ver3
```

WARNING!

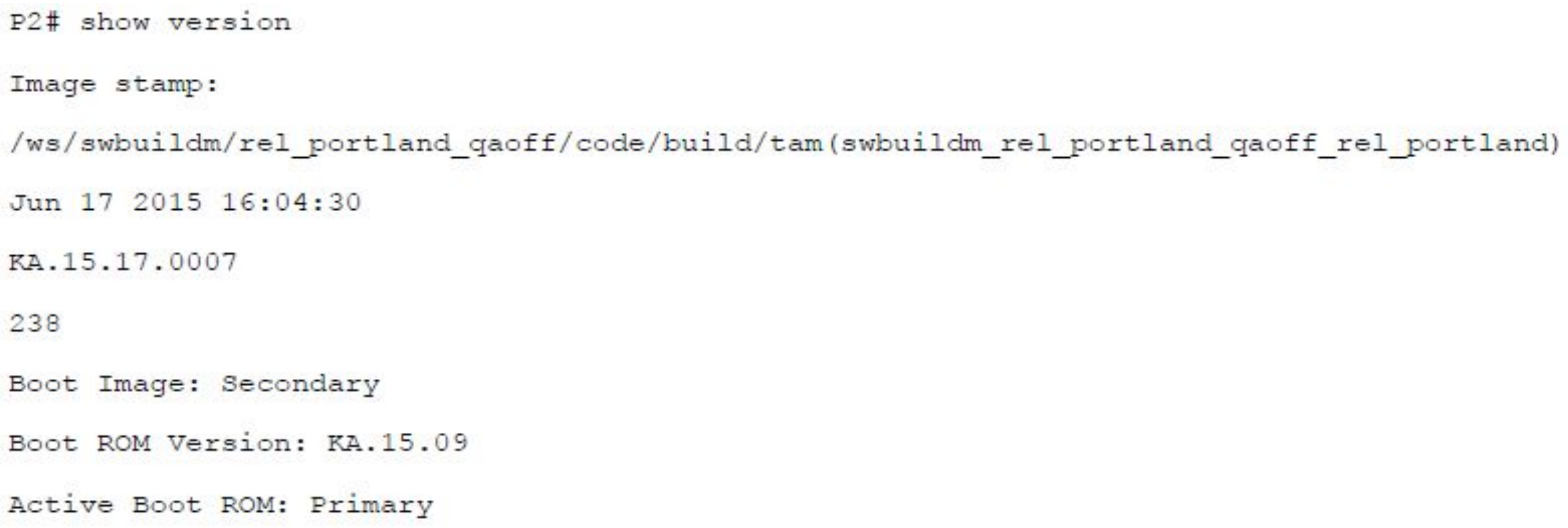
Switch configuration



This is an example of SNMPv3 configuration on a 3800 series switch:

```
P1(config)# snmpv3 enable

SNMPv3 Initialization process.

Creating user 'initial'

Authentication Protocol: MD5

Enter authentication password: *******

Privacy protocol is DES

Enter privacy password: *******


User 'initial' has been created

Would you like to create a user that uses SHA? [y/n] n


User creation is done. SNMPv3 is now functional.

Would you like to restrict SNMPv1 and SNMPv2c messages to have read only access (you can
set this later by the command 'snmpv3 restricted-access')? [y/n] y

P1(config)# snmpv3 user sdn auth md5 skyline priv des skyline

P1(config)# snmpv3 group ManagerPriv user sdn sec-model ver3
```

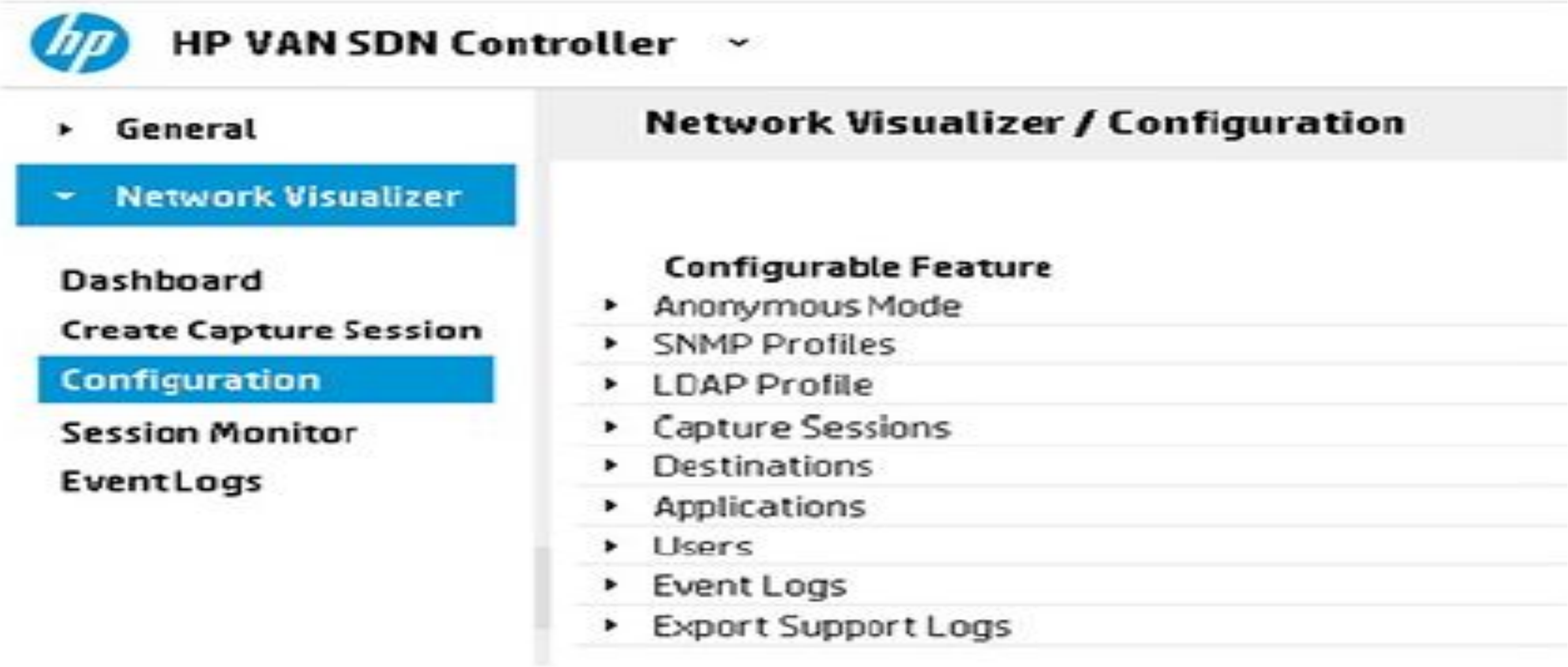
Instructions



```
P2# show version

Image stamp:

/ws/swbuildm/rel_portland_qaoff/code/build/tam(swbuildm_rel_portland_qaoff_rel_portland)

Jun 17 2015 16:04:30

KA.15.17.0007

238

Boot Image: Secondary

Boot ROM Version: KA.15.09

Active Boot ROM: Primary
```

Instructions

Network Visualizer Configuration



HP VAN SDN Controller

- General
- Network Visualizer
  - Dashboard
  - Create Capture Session
  - Configuration
  - Session Monitor
  - EventLogs

Network Visualizer / Configuration

Configurable Feature

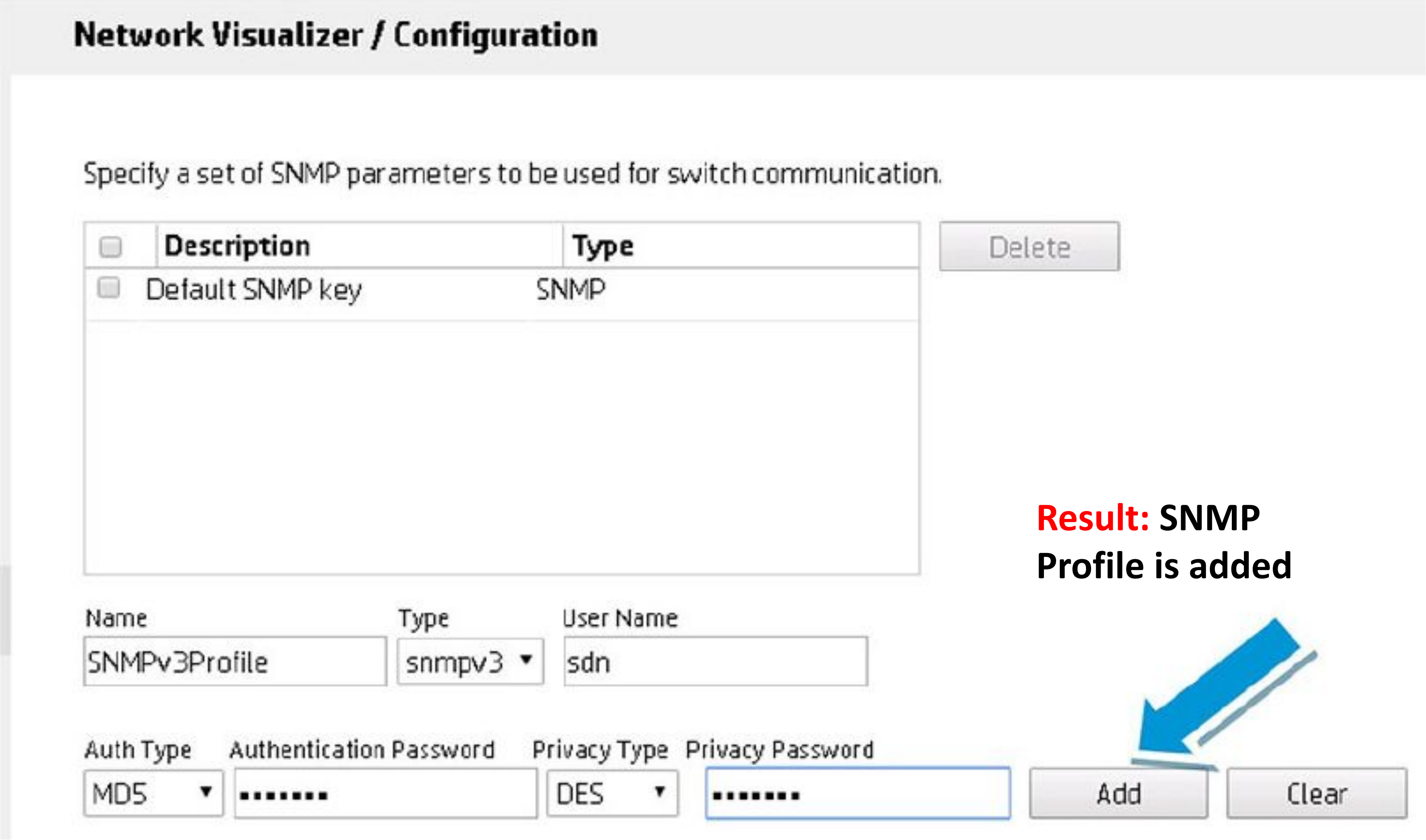
- Anonymous Mode
- SNMP Profiles
- LDAP Profile
- Capture Sessions
- Destinations
- Applications
- Users
- Event Logs
- Export Support Logs

Instructions

SNMP Profiles

- **Name:** SNMPv3Profile
- **Type:** snmpv3
- **Username:** sdn
- **Auth Type:** MD5
- **Authentication Password:** skyline
- **Privacy Type:** DES
- **Privacy Password:** skyline

Instructions



Network Visualizer / Configuration

Specify a set of SNMP parameters to be used for switch communication.

□	Description	Type
□	Default SNMP key	SNMP

Name	Type	User Name
SNMPv3Profile	snmpv3 ▾	sdn

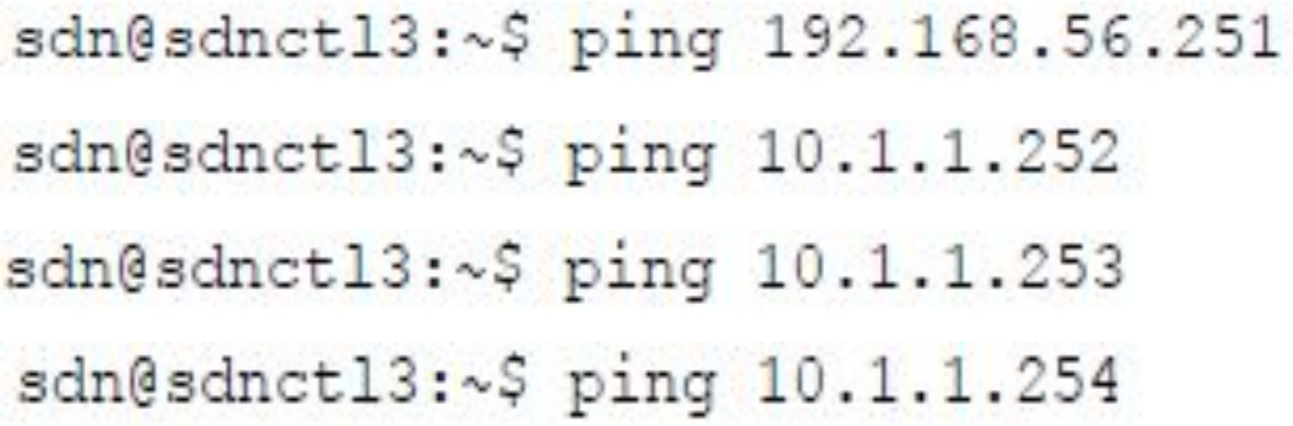
Auth Type	Authentication Password	Privacy Type	Privacy Password
MD5 ▾	●●●●●●●●	DES ▾	●●●●●●●●

Result: **SNMP Profile is added**

Instructions

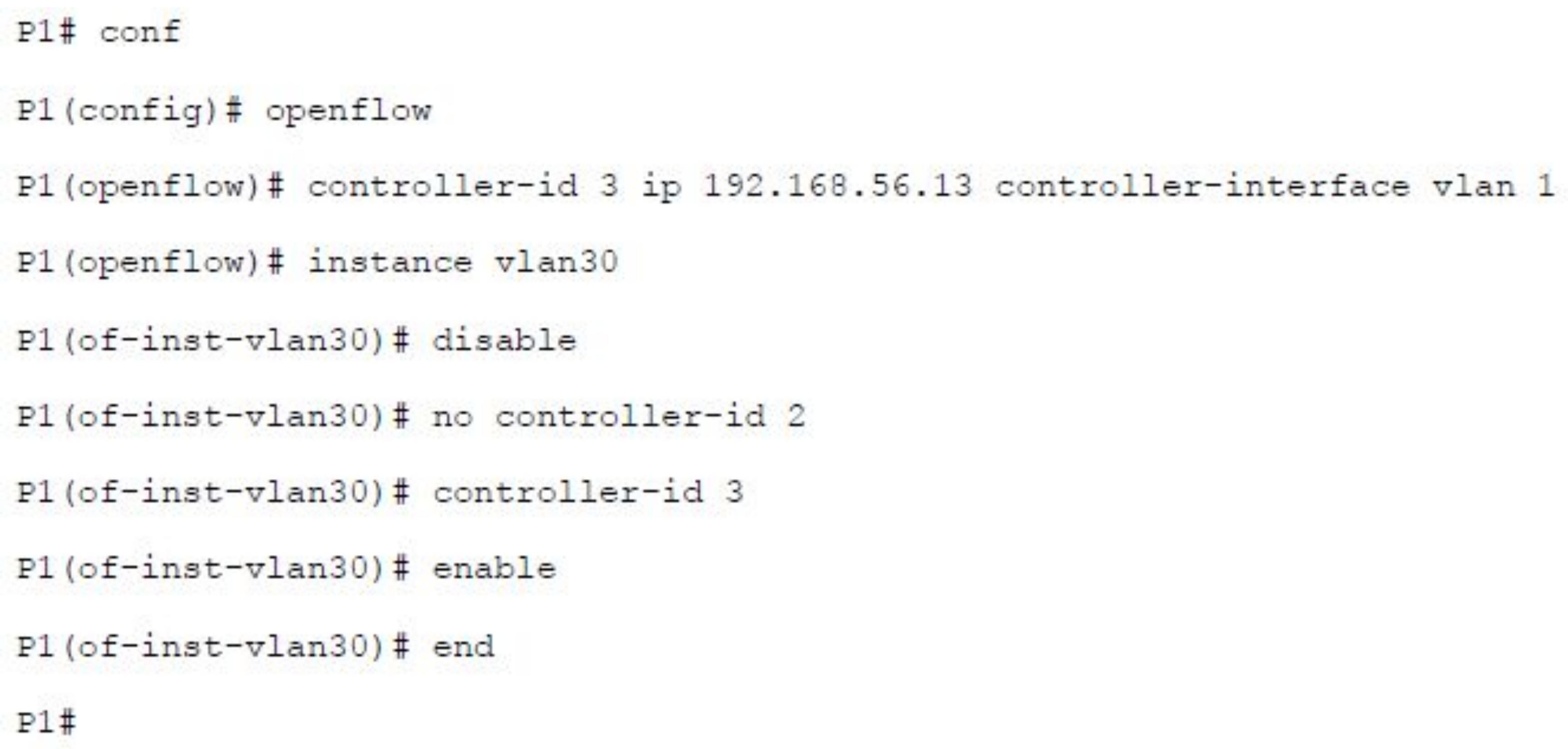
- **IP address: 192.168.56.13**
- **Port number: 22**
- **Protocol: SSH**

Result:
All pings should succeed.



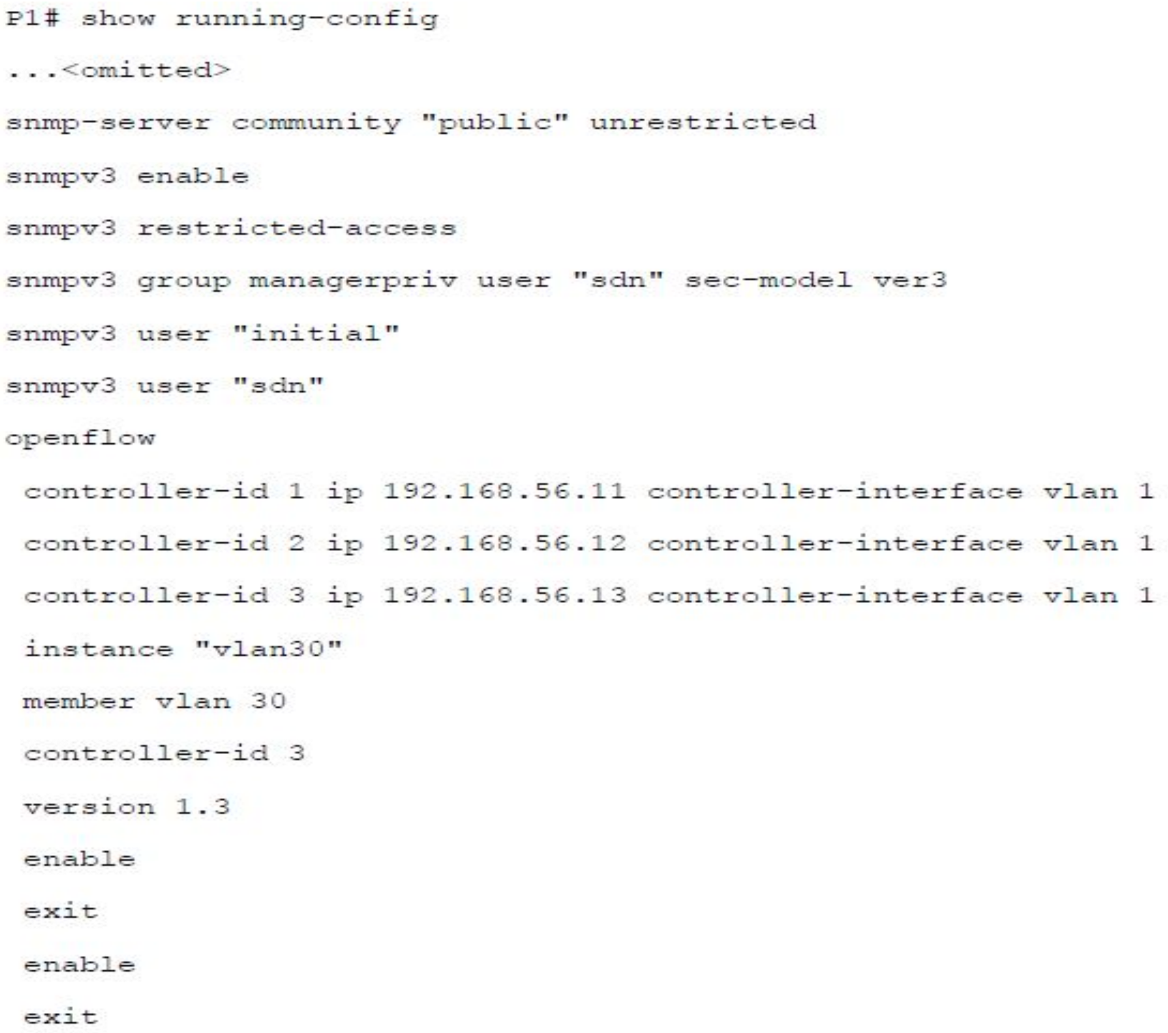
```
sdn@sdnctl3:~$ ping 192.168.56.251
sdn@sdnctl3:~$ ping 10.1.1.252
sdn@sdnctl3:~$ ping 10.1.1.253
sdn@sdnctl3:~$ ping 10.1.1.254
```

Instructions



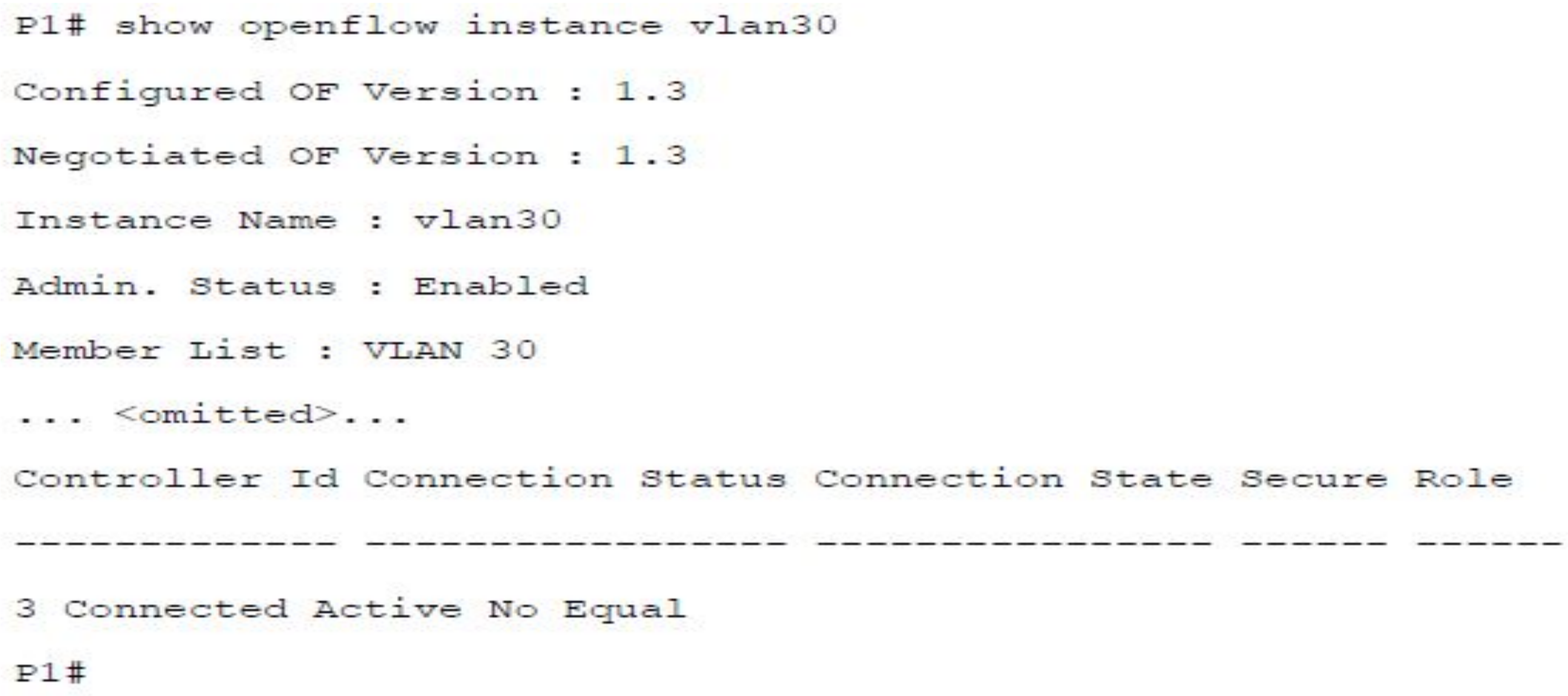
```
P1# conf

P1(config)# openflow

P1(openflow)# controller-id 3 ip 192.168.56.13 controller-interface vlan 1

P1(openflow)# instance vlan30

P1(of-inst-vlan30)# disable

P1(of-inst-vlan30)# no controller-id 2

P1(of-inst-vlan30)# controller-id 3

P1(of-inst-vlan30)# enable

P1(of-inst-vlan30)# end

P1#
```

Instructions



```
P1# show running-config
...<omitted>
snmp-server community "public" unrestricted
snmpv3 enable
snmpv3 restricted-access
snmpv3 group managerpriv user "sdn" sec-model ver3
snmpv3 user "initial"
snmpv3 user "sdn"
openflow
 controller-id 1 ip 192.168.56.11 controller-interface vlan 1
 controller-id 2 ip 192.168.56.12 controller-interface vlan 1
 controller-id 3 ip 192.168.56.13 controller-interface vlan 1
 instance "vlan30"
 member vlan 30
 controller-id 3
 version 1.3
 enable
 exit
 enable
 exit
```

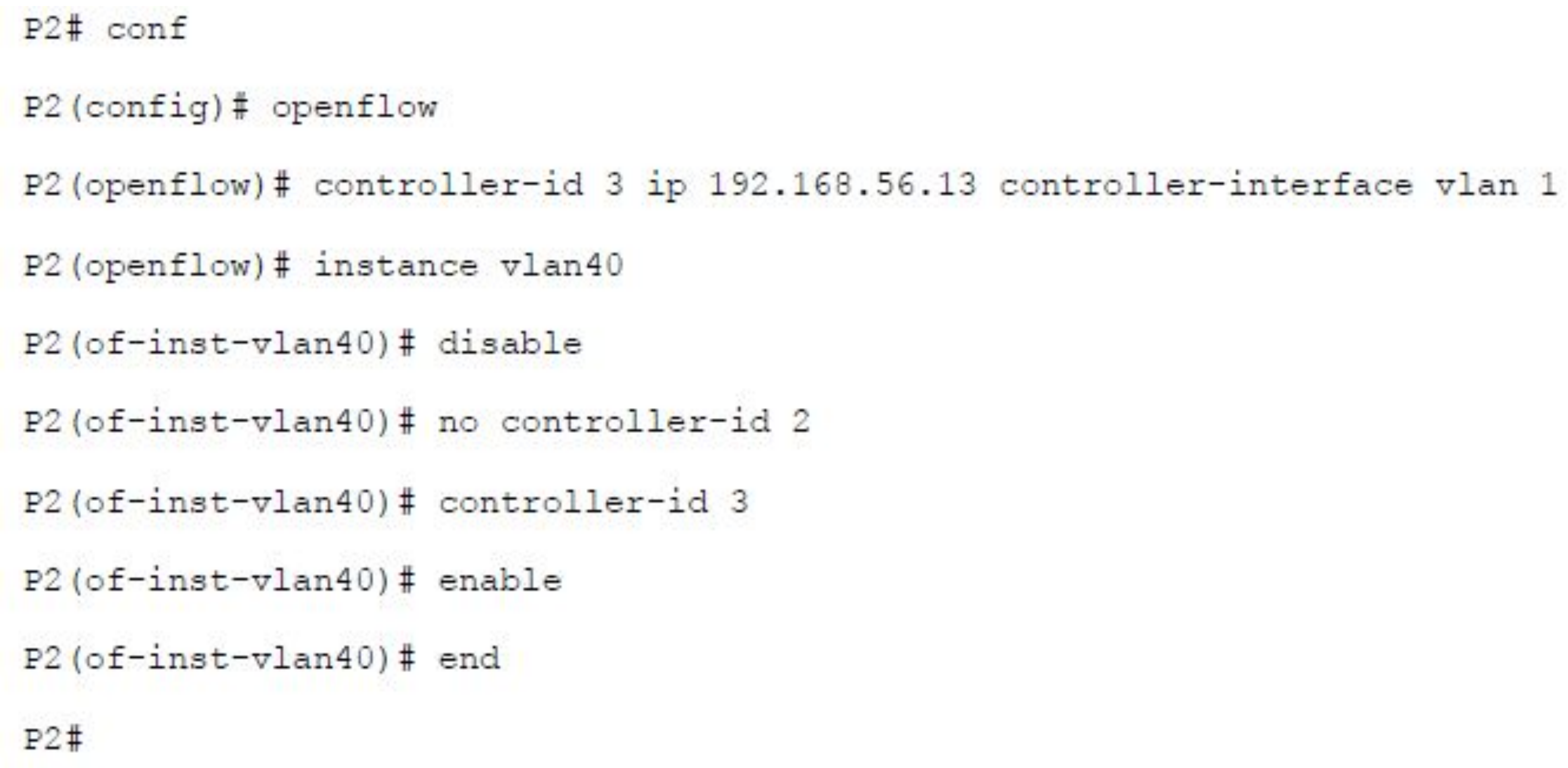
Instructions



```
P1# show openflow instance vlan30
Configured OF Version : 1.3
Negotiated OF Version : 1.3
Instance Name : vlan30
Admin. Status : Enabled
Member List : VLAN 30
... <omitted>...
Controller Id Connection Status Connection State Secure Role
------------- ------------------ ----------------- ------ ------
3 Connected Active No Equal
P1#
```

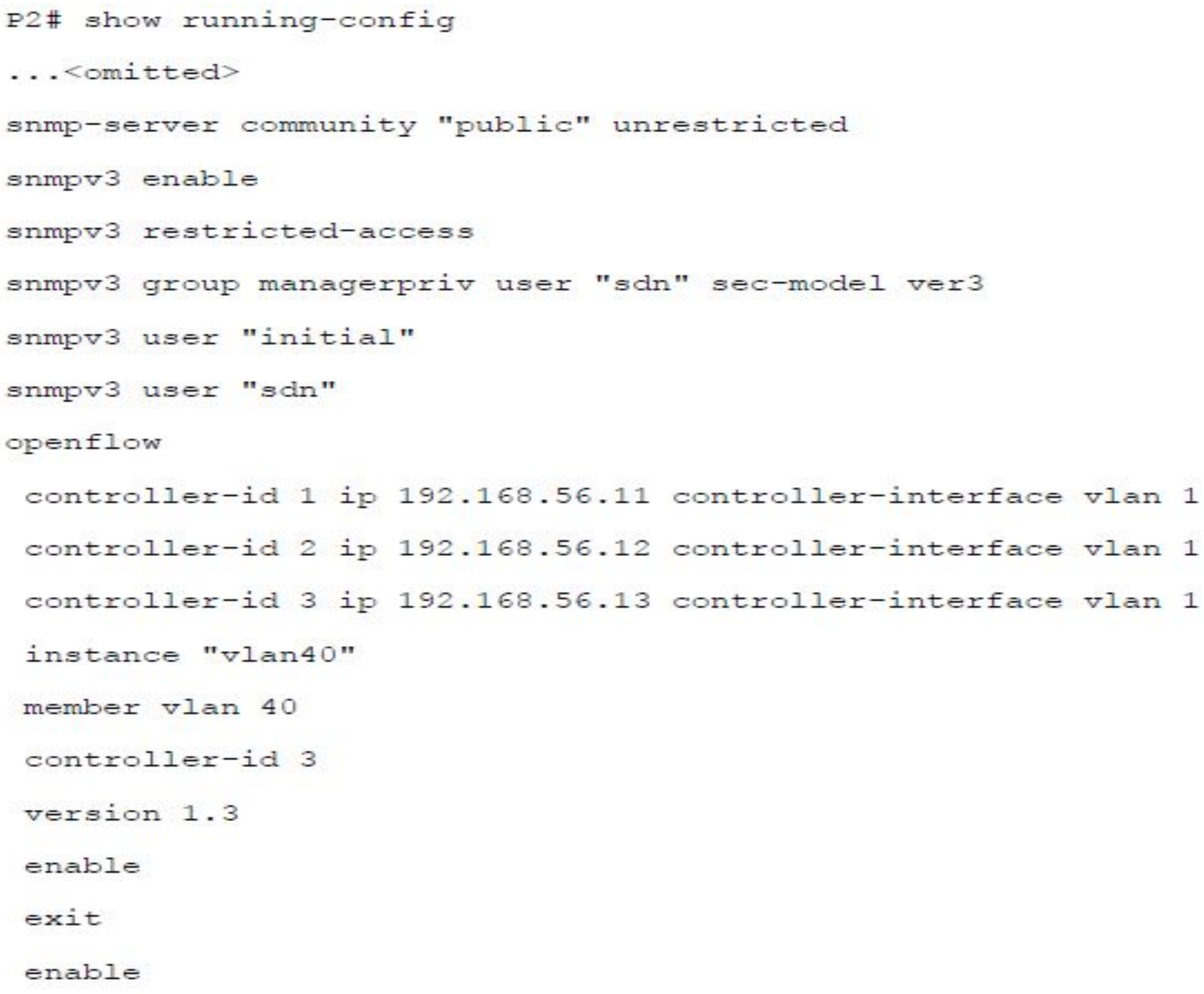
Result:

Instructions



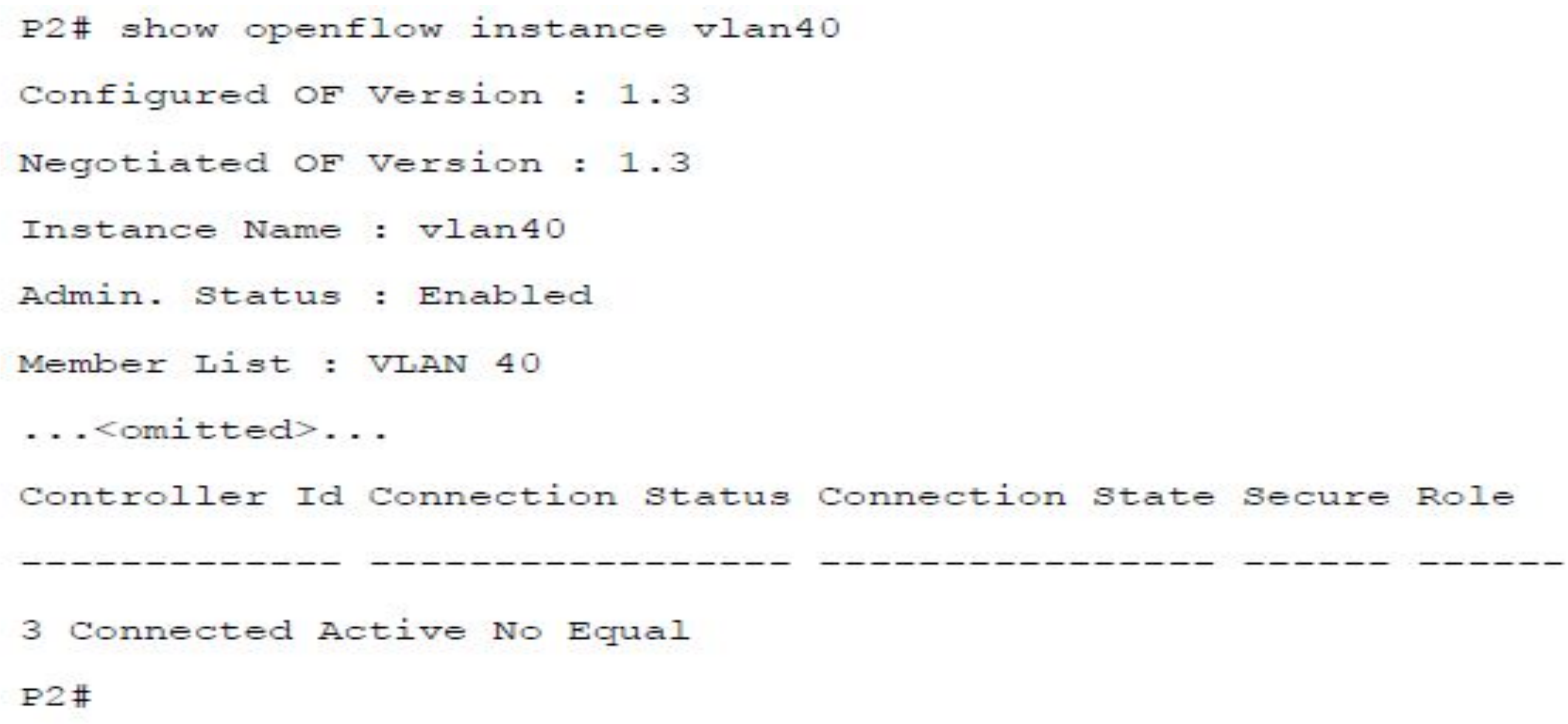
```
P2# conf

P2(config)# openflow

P2(openflow)# controller-id 3 ip 192.168.56.13 controller-interface vlan 1

P2(openflow)# instance vlan40

P2(of-inst-vlan40)# disable

P2(of-inst-vlan40)# no controller-id 2

P2(of-inst-vlan40)# controller-id 3

P2(of-inst-vlan40)# enable

P2(of-inst-vlan40)# end

P2#
```

Instructions



```
P2# show running-config
...<omitted>
snmp-server community "public" unrestricted
snmpv3 enable
snmpv3 restricted-access
snmpv3 group managerpriv user "sdn" sec-model ver3
snmpv3 user "initial"
snmpv3 user "sdn"
openflow
 controller-id 1 ip 192.168.56.11 controller-interface vlan 1
 controller-id 2 ip 192.168.56.12 controller-interface vlan 1
 controller-id 3 ip 192.168.56.13 controller-interface vlan 1
 instance "vlan40"
 member vlan 40
 controller-id 3
 version 1.3
 enable
 exit
 enable
```

Instructions

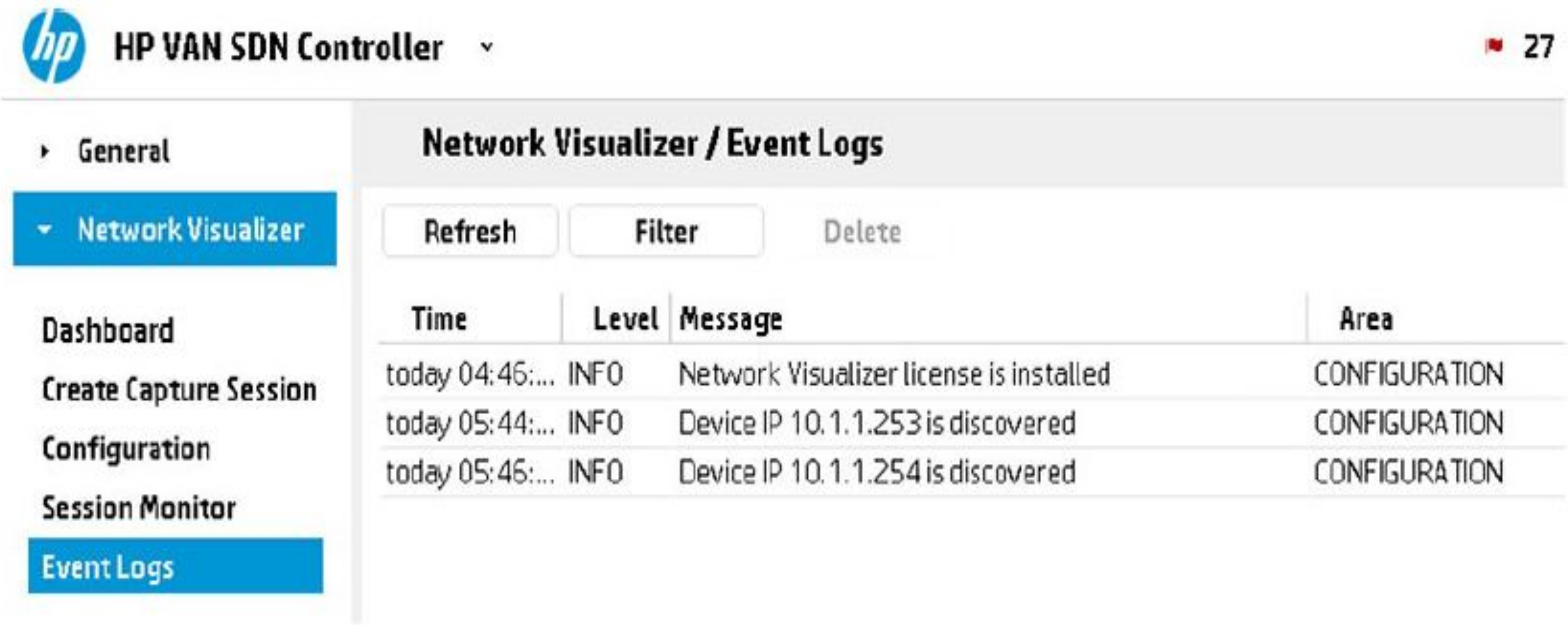


```
P2# show openflow instance vlan40

Configured OF Version : 1.3

Negotiated OF Version : 1.3

Instance Name : vlan40

Admin. Status : Enabled

Member List : VLAN 40

...<omitted>...

Controller Id Connection Status Connection State Secure Role

------------- ----------------- ---------------- ------ ------

3 Connected Active No Equal

P2#
```

Result:

Instructions

Event Logs



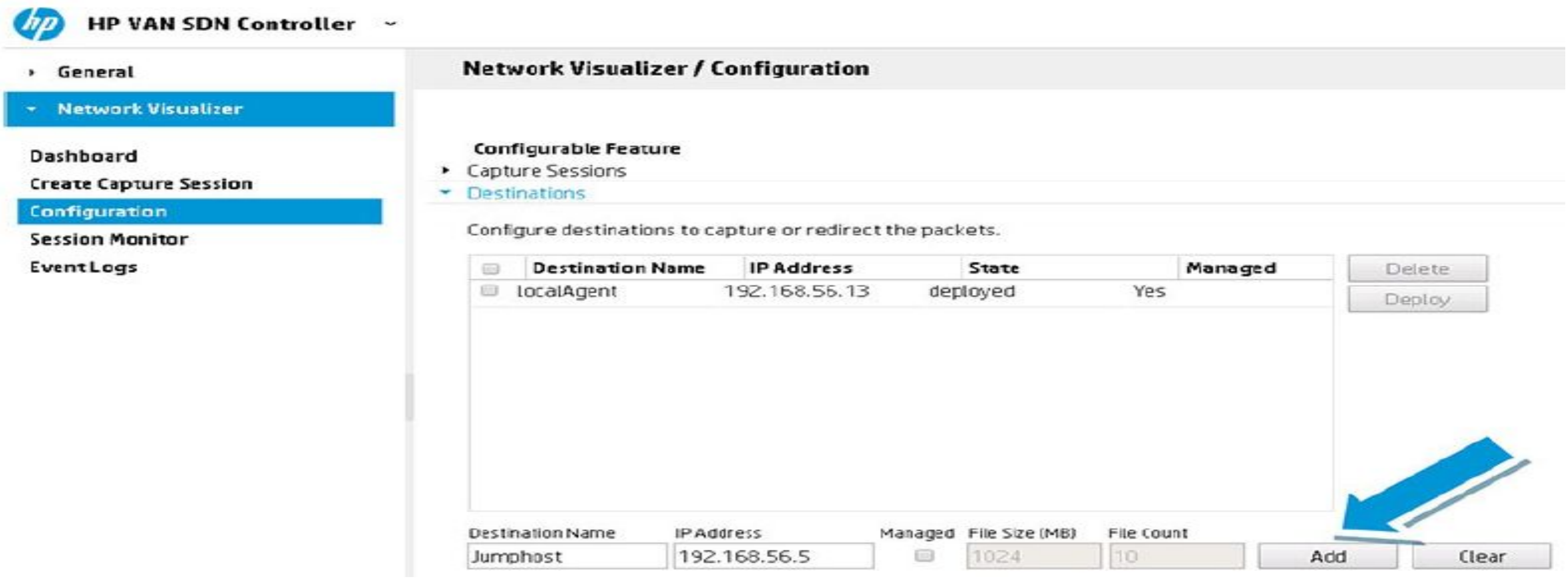
Time	Level	Message	Area
today 04:46:...	INFO	Network Visualizer license is installed	CONFIGURATION
today 05:44:...	INFO	Device IP 10.1.1.253 is discovered	CONFIGURATION
today 05:46:...	INFO	Device IP 10.1.1.254 is discovered	CONFIGURATION

Result:

Instructions

Configuration Destinations.

- **Destination Name:** Jumphost
- **IP address:** 192.168.56.5 (this is the IP address of the Jumphost PC)
- Managed = Unchecked (off)
- Click Add (see Figure):



Configure destinations to capture or redirect the packets.

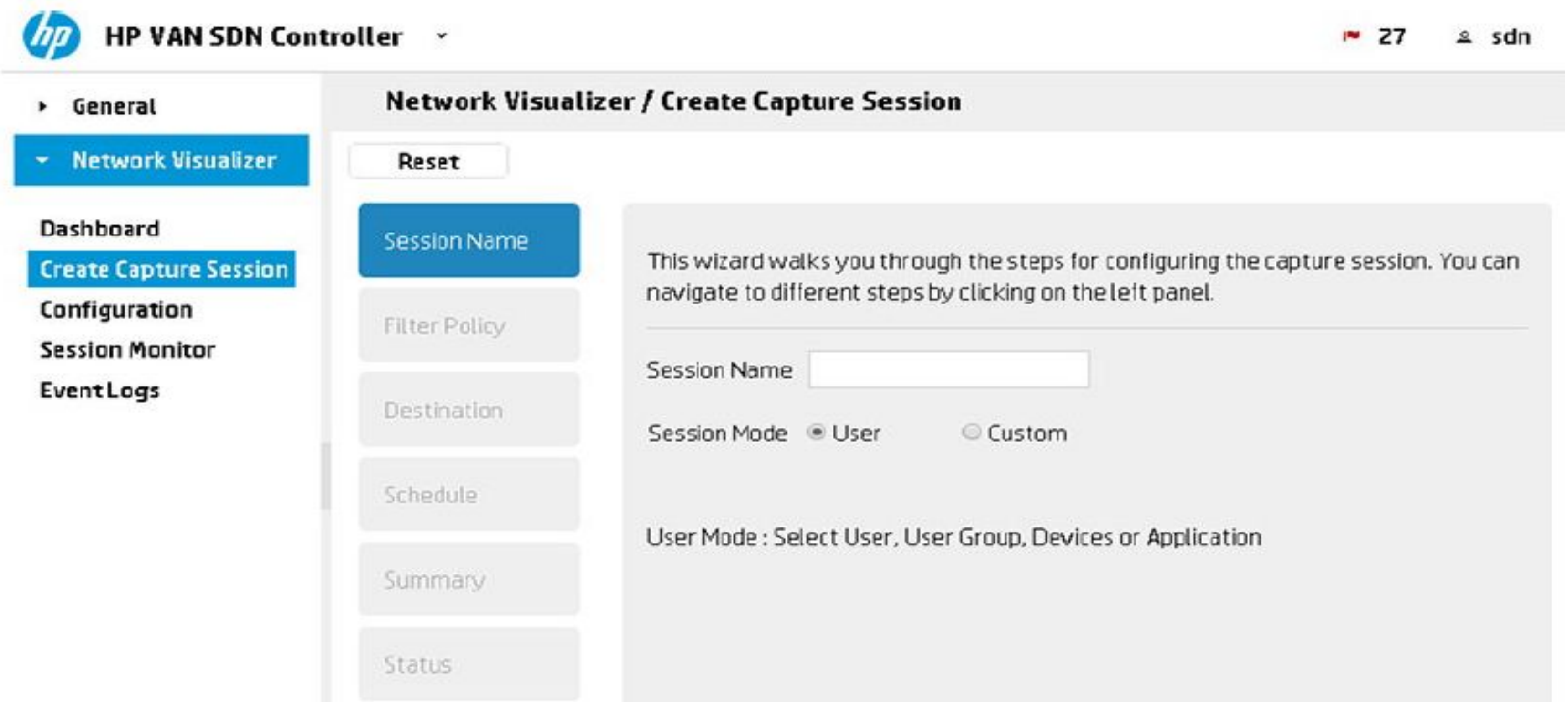
□	Destination Name	IP Address	State	Managed
□	localAgent	192.168.56.13	deployed	Yes

Destination Name	IP Address	Managed	File Size (MB)	File Count
Jumphost	192.168.56.5	□	1024	10

Instructions

Create Capture Session

Create Capture Session



This wizard walks you through the steps for configuring the capture session. You can navigate to different steps by clicking on the left panel.

Session Name

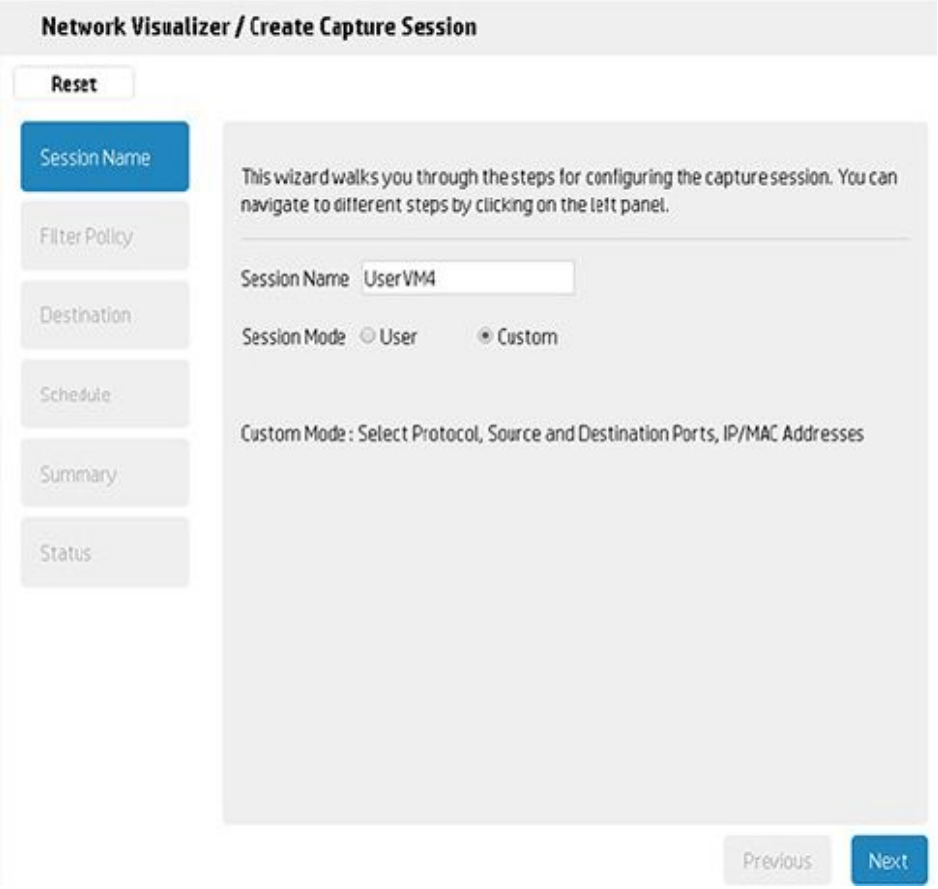
Session Mode ● User ○ Custom

User Mode : Select User, User Group, Devices or Application

Instructions

In the first step

- **User:** You can configure the user, user group, device, and application for capture session monitoring.
- **Custom:** You can configure the source/destination IP address, source/destination MAC address, port, and protocol for capture session monitoring.



Network Visualizer / Create Capture Session

This wizard walks you through the steps for configuring the capture session. You can navigate to different steps by clicking on the left panel.

Session Name: UserVM4

Session Mode ○ User ● Custom

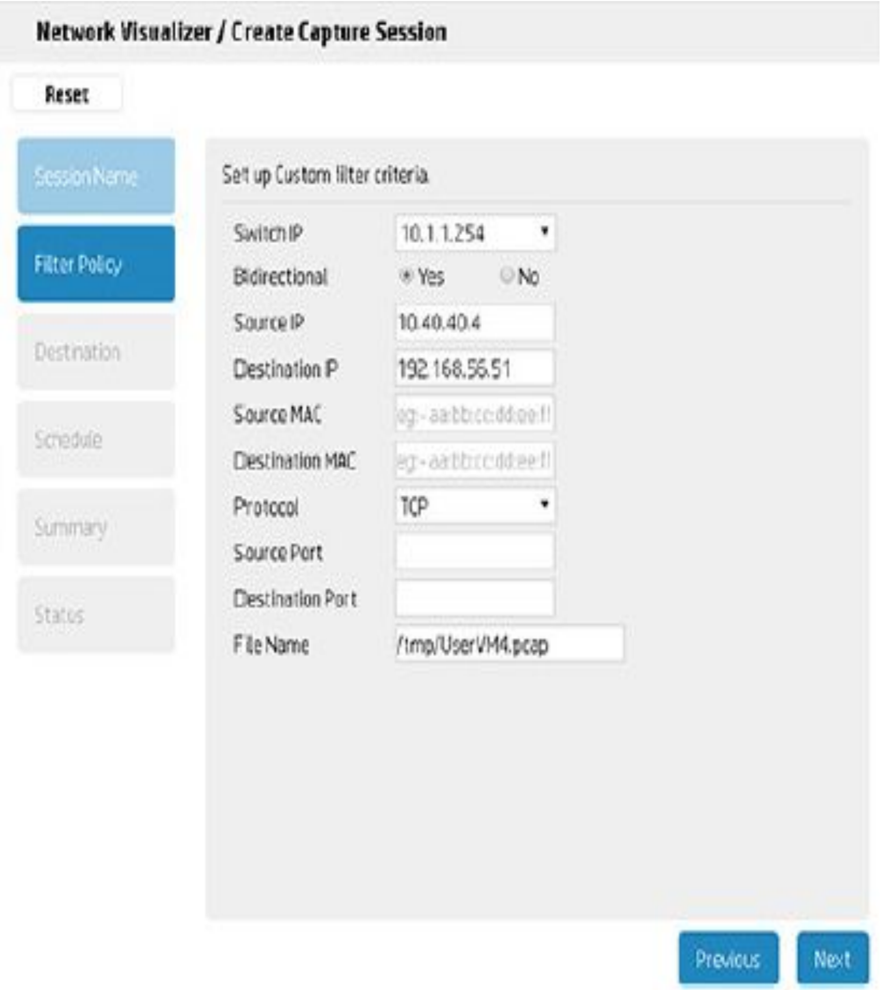
Custom Mode : Select Protocol, Source and Destination Ports, IP/MAC Addresses

Instructions

In the second step Filter Policy

- Switch IP: 10.1.1.254
- Bidirectional: Yes
- Source IP: 10.40.40.4
- Destination IP: 192.168.56.51
- Protocol: TCP

Next



Set up Custom filter criteria

Switch IP	10.1.1.254 ▾
Bidirectional	● Yes ○ No
Source IP	10.40.40.4
Destination IP	192.168.56.51
Source MAC	eg:-aa:bb:cc:dd:ee:ff
Destination MAC	eg:-aa:bb:cc:dd:ee:ff
Protocol	TCP ▾
Source Port	
Destination Port	
File Name	/tmp/UserVM4.pcap

Instructions

- Switch IP: IP address of the network device
- Bidirectional: Select the traffic capture direction by clicking one of the following:
- Yes – Captures packets sent and received by the user
- No – Captures packets sent by the user
- Source IP: IP address of the source (for example, 10.40.40.4)
- Destination IP: IP address of the destination (for example, 192.168.56.51)
- Source MAC: MAC address of the source (for example, aa:bb:cc:dd:ee:ff)
- Destination MAC: MAC address of the destination (for example, aa:bb:cc:dd:ee:ff)
- Protocol: Network protocol; by default, protocol is All
- Source Port: Layer 4 port for the source
- Destination Port: Layer 4 port for the destination
- File Name: Name of the pcap file to save the packets

Instructions

The third step

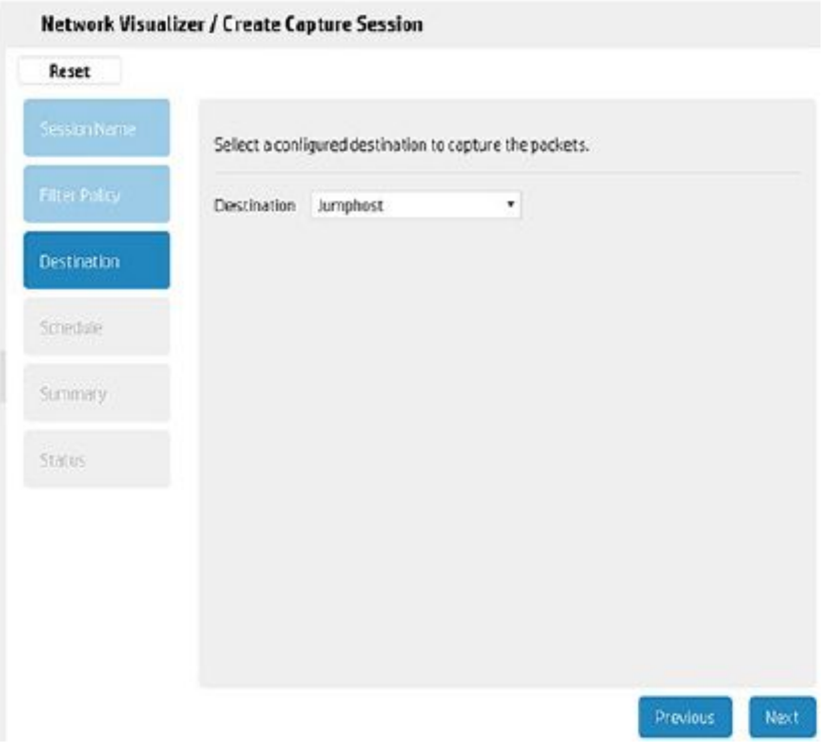
Destination Jumphost

Next

. The fourth step Schedule

No

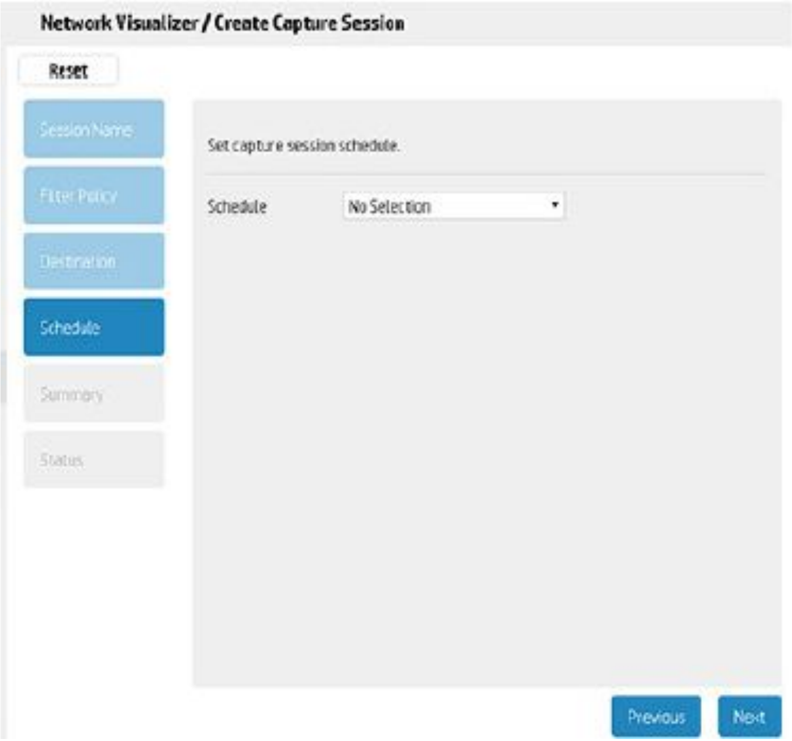
Selection Next



Network Visualizer / Create Capture Session

Select a configured destination to capture the packets.

Destination: Jumphost



Network Visualizer / Create Capture Session

Set capture session schedule.

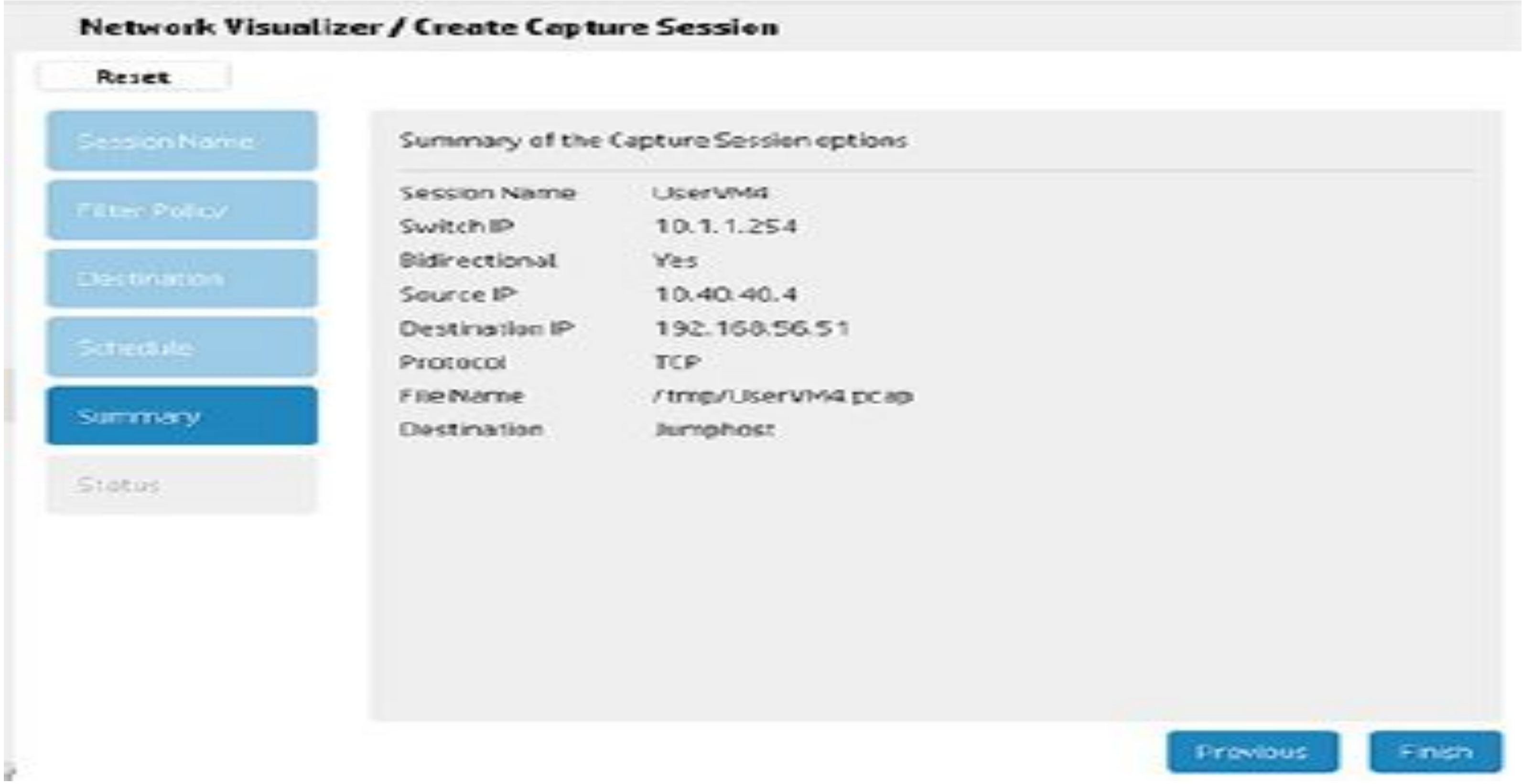
Schedule: No Selection

Instructions

- **No Selection:** Monitoring of capture session is not scheduled.
- **Once:** Monitor the capture session once. Specify the Start Time and Stop Time.
- **Everyday:** Monitor the capture session without day restrictions. Specify the repeat interval in Repeat every (days), Start Time, Stop Time, and End Date.
- **Weekday (Monday to Friday):** Monitor the capture session on weekdays. Specify the Start Time, Stop Time, and End Date.
- **Weekend (Saturday and Sunday):** Monitor the capture session on weekends. Specify the Start Time, Stop Time, and End Date.
- **Weekly:** Monitor the capture session on a weekly basis. Select the days of the week to capture the sessions with Repeat on check boxes. Specify the Start Time, Stop Time, and End Date.

Instructions

Finish



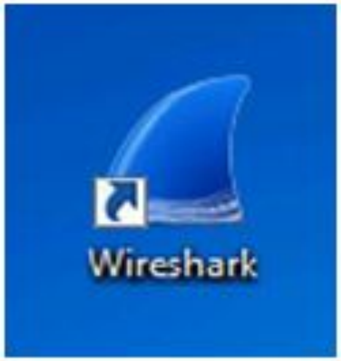
Network Visualizer / Create Capture Session

Summary of the Capture Session options

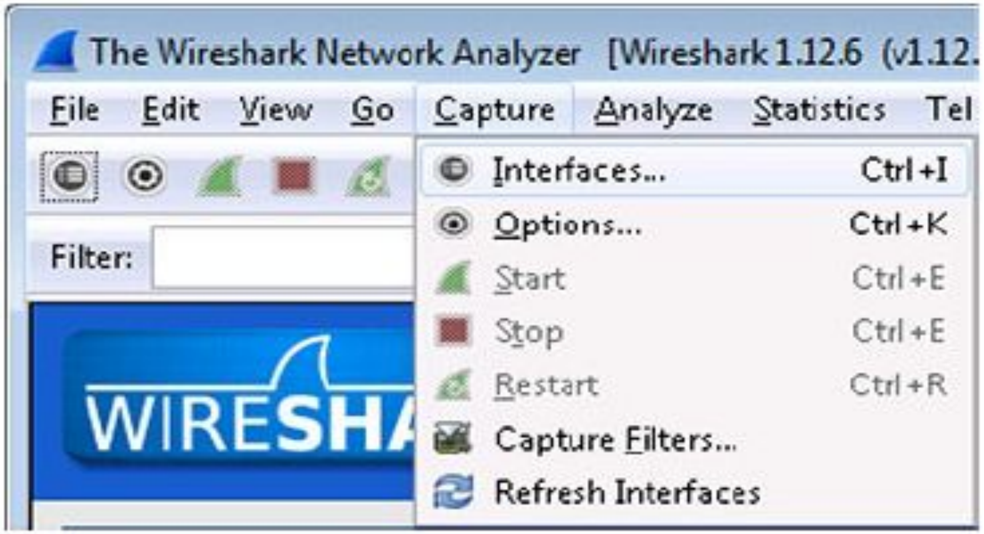
Session Name	UserVM4
Switch IP	10.1.1.254
Bidirectional	Yes
Source IP	10.40.40.4
Destination IP	192.168.56.51
Protocol	TCP
File Name	/tmp/UserVM4.pcap
Destination	Jumphost

Activate the session

Wireshark

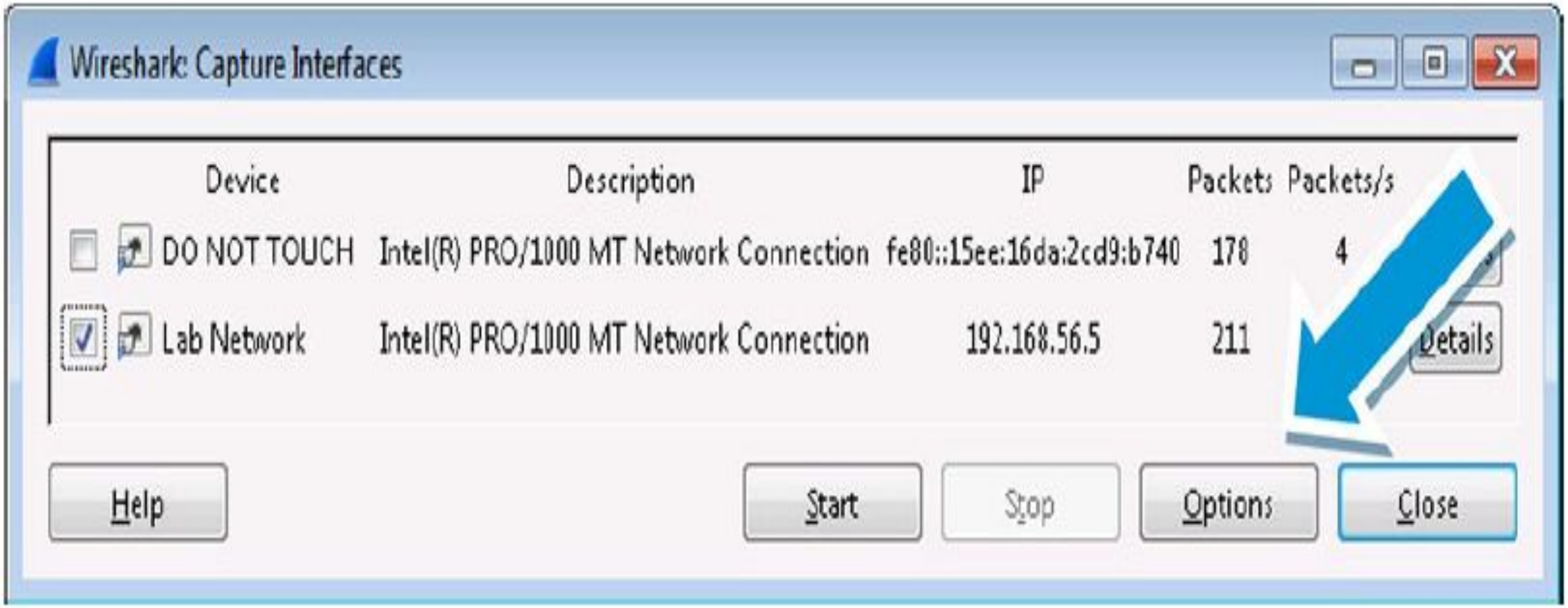


Capture Interfaces



Activate the session

Lab Network **Options**

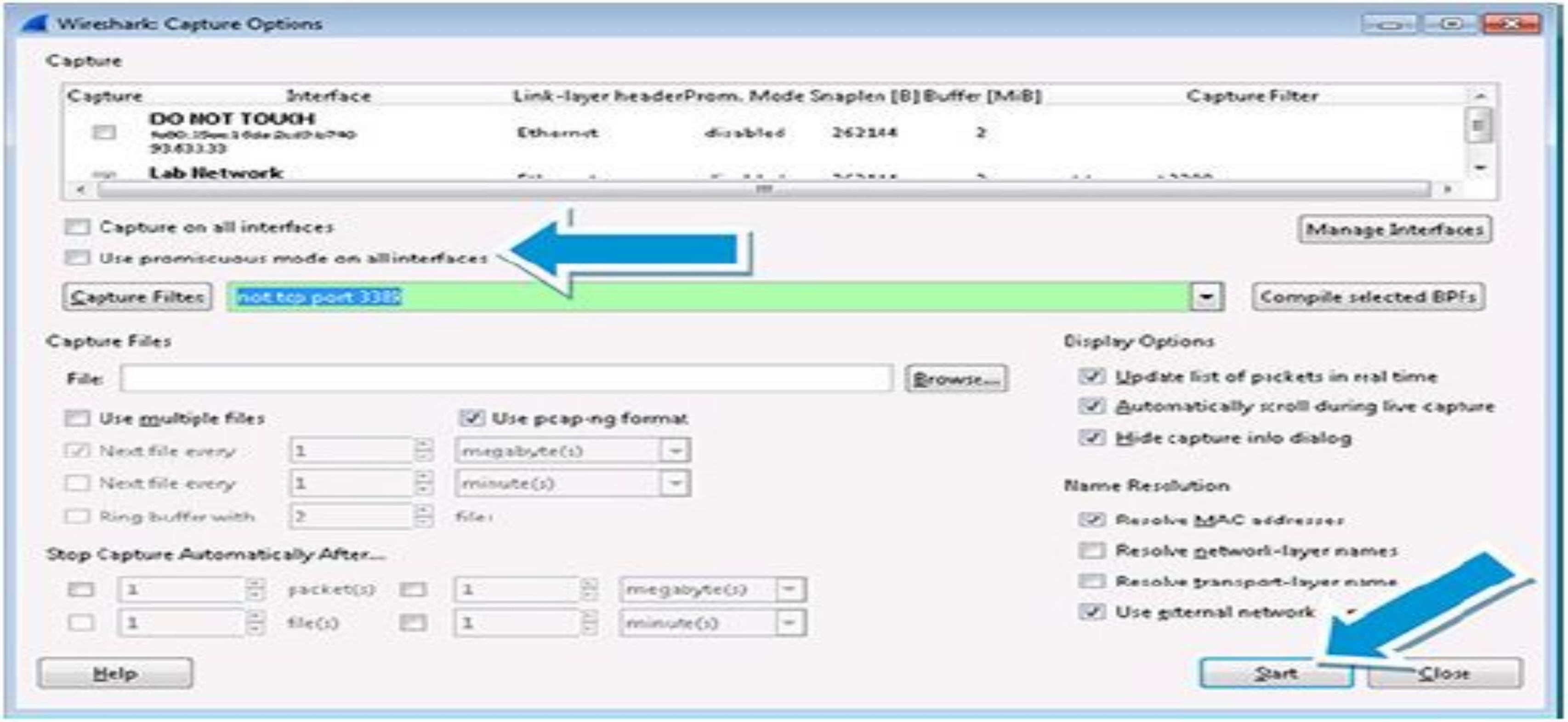


	Device	Description	IP	Packets	Packets/s	
□	DO NOT TOUCH	Intel(R) PRO/1000 MT Network Connection	fe80::15ee:16da:2cd9:b740	178	4	
☑	Lab Network	Intel(R) PRO/1000 MT Network Connection	192.168.56.5	211		Details

Activate the session

Use promiscuous mode

Start



Wireshark: Capture Options

Capture

Capture	Interface	Link-layer header	Prom. Mode	Snaplen [B]	Buffer [MiB]	Capture Filter
□	DO NOT TOUKH [illegible] 93.63.3.33	Ethernet	disabled	262144	2	
	Lab Network					

□ Capture on all interfaces

□ Use promiscuous mode on allinterfaces

Capture Filtes: not tcp port 3389

Capture Files

File:

□ Use multiple files

☑ Use pcap-ng format

☑ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

□ Ring buffer with 2 files

Stop Capture Automatically After...

□ 1 packet(s) □ 1 megabyte(s)

□ 1 file(s) □ 1 minute(s)

Display Options

☑ Update list of pickets in real time

☑ Automatically scroll during live capture

☑ Hide capture inlo dialog

Name Resolution

☑ Resolve MAC addresses

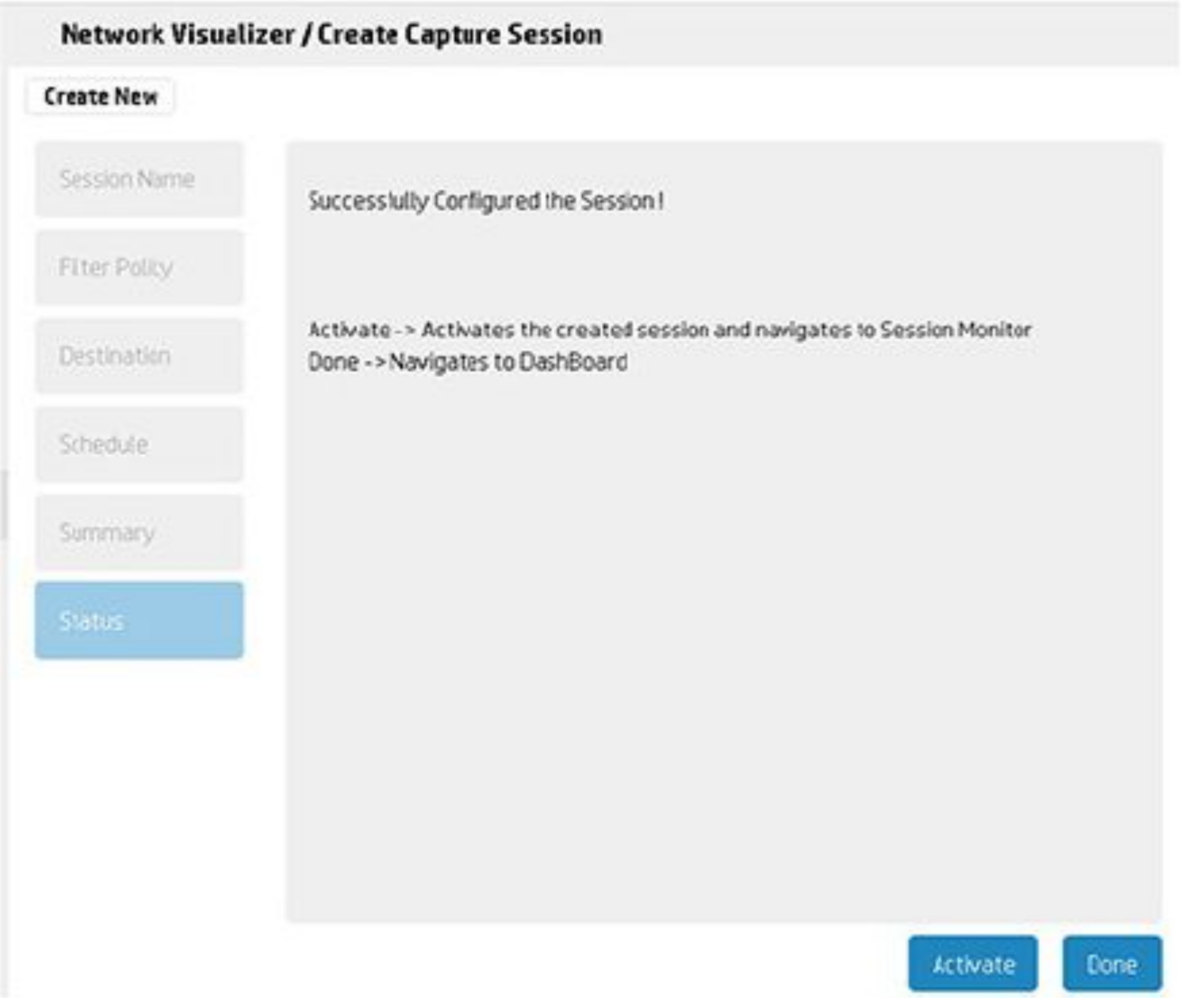
□ Resolve network-layer names

□ Resolve transport-layer name

☑ Use external network

Activate the session

Activate

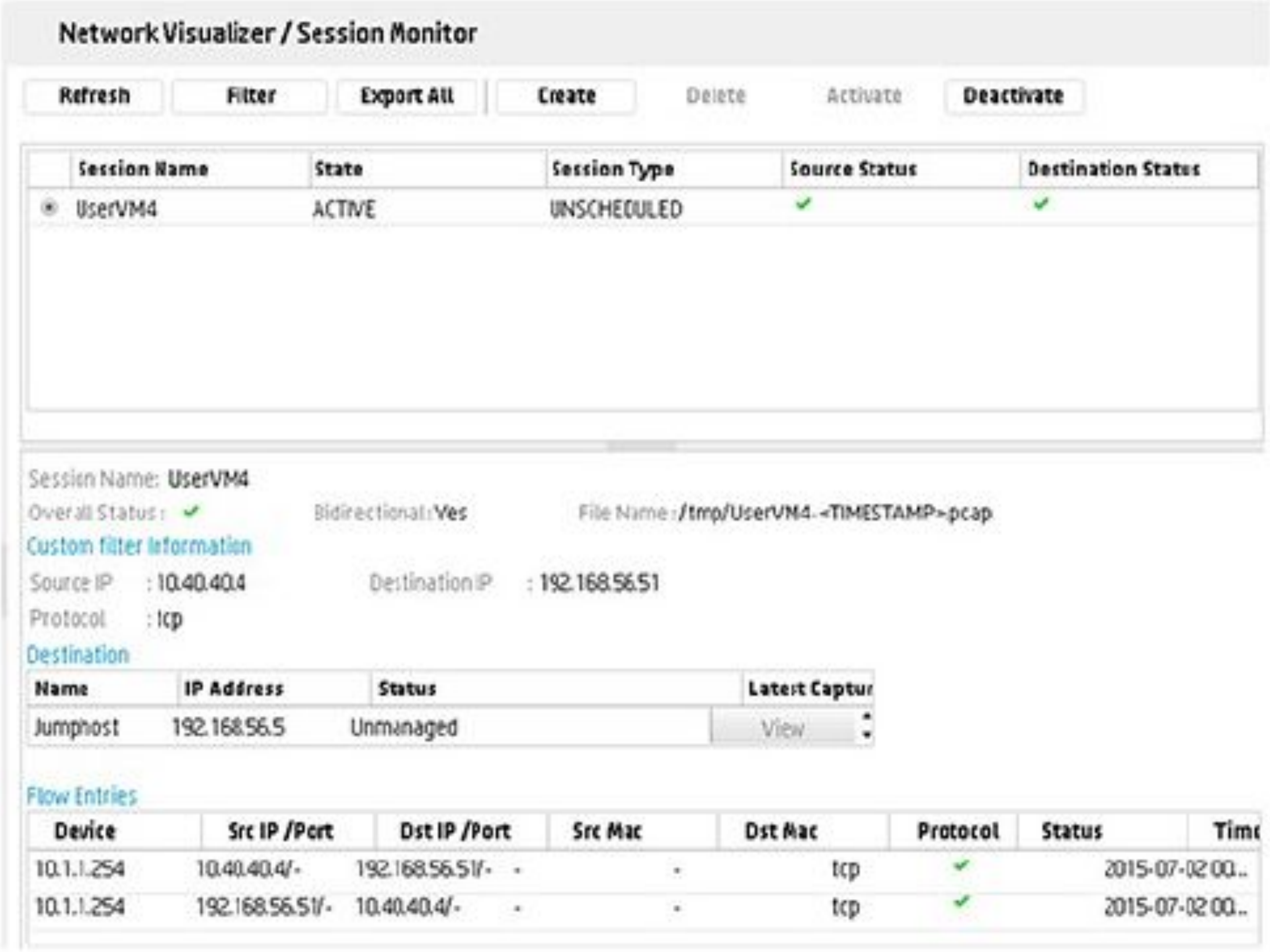


Successfully Configured the Session !

Activate -> Activates the created session and navigates to Session Monitor
Done -> Navigates to DashBoard

Activate the session

Session Monitor



Network Visualizer / Session Monitor

	Session Name	State	Session Type	Source Status	Destination Status
●	UserVM4	ACTIVE	UNSCHEDULED	✓	✓

Session Name: UserVM4

Overall Status: ✓ Bidirectional: Yes File Name: /tmp/UserVM4-<TIMESTAMP>-pcap

Custom filter information

Source IP : 10.40.40.4 Destination IP : 192.168.56.51

Protocol : tcp

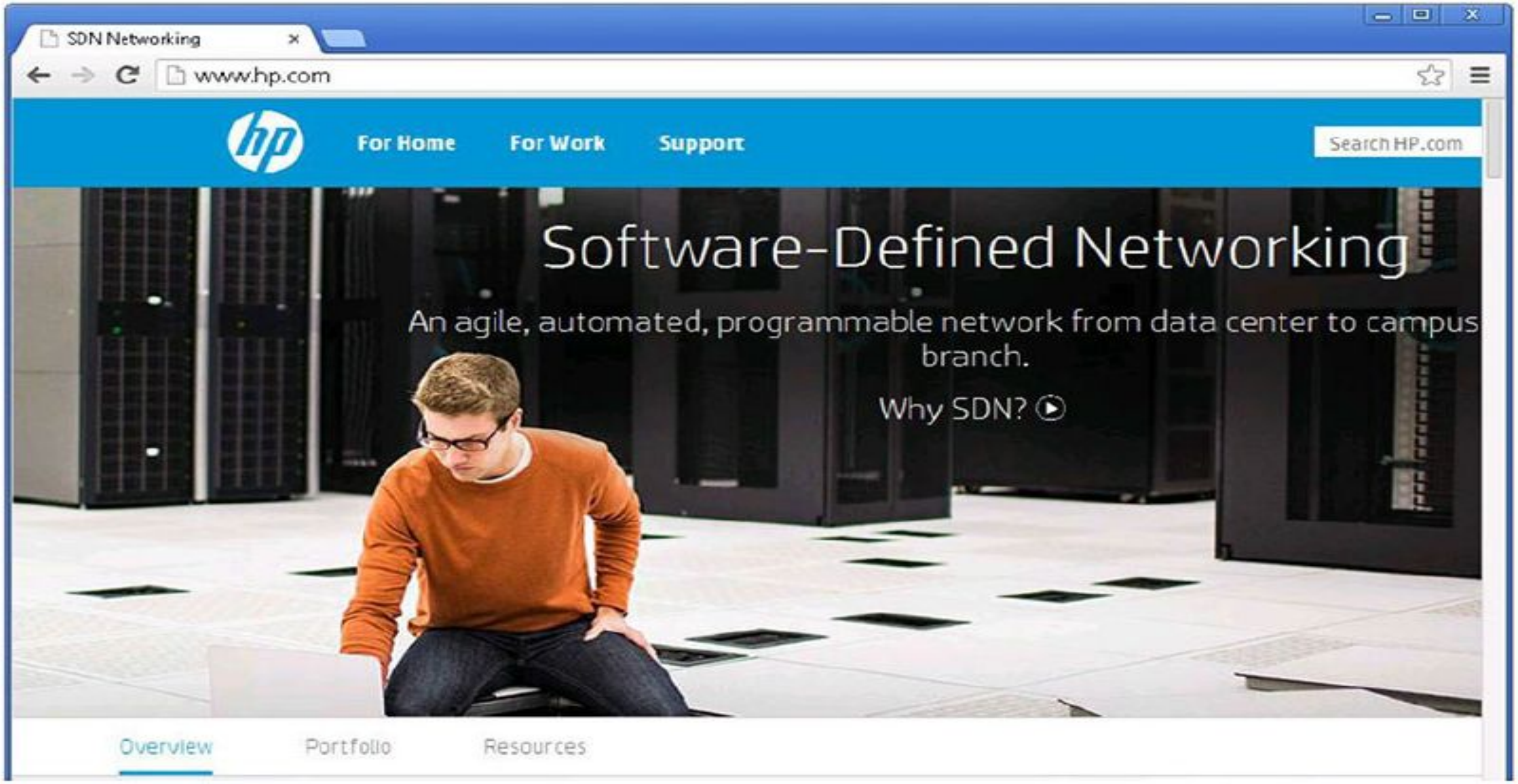
Destination

Name	IP Address	Status	Latest Captur
Jumphost	192.168.56.5	Unmanaged	View

Flow Entries

Device	Src IP /Port	Dst IP /Port	Src Mac	Dst Mac	Protocol	Status	Time
10.1.1.254	10.40.40.4/-	192.168.56.51/-	-	-	tcp	✓	2015-07-02 00..
10.1.1.254	192.168.56.51/-	10.40.40.4/-	-	-	tcp	✓	2015-07-02 00..

Activate the session

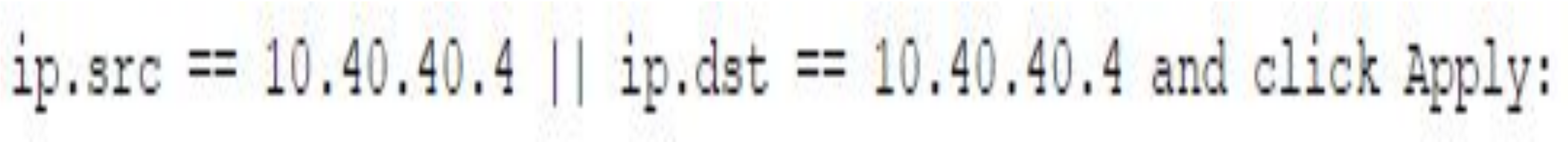


Software-Defined Networking

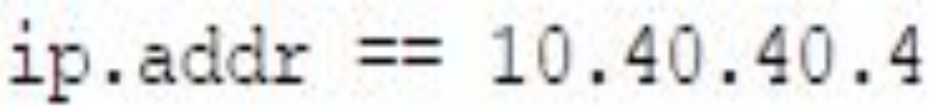
An agile, automated, programmable network from data center to campus branch.

Why SDN?

Activate the session

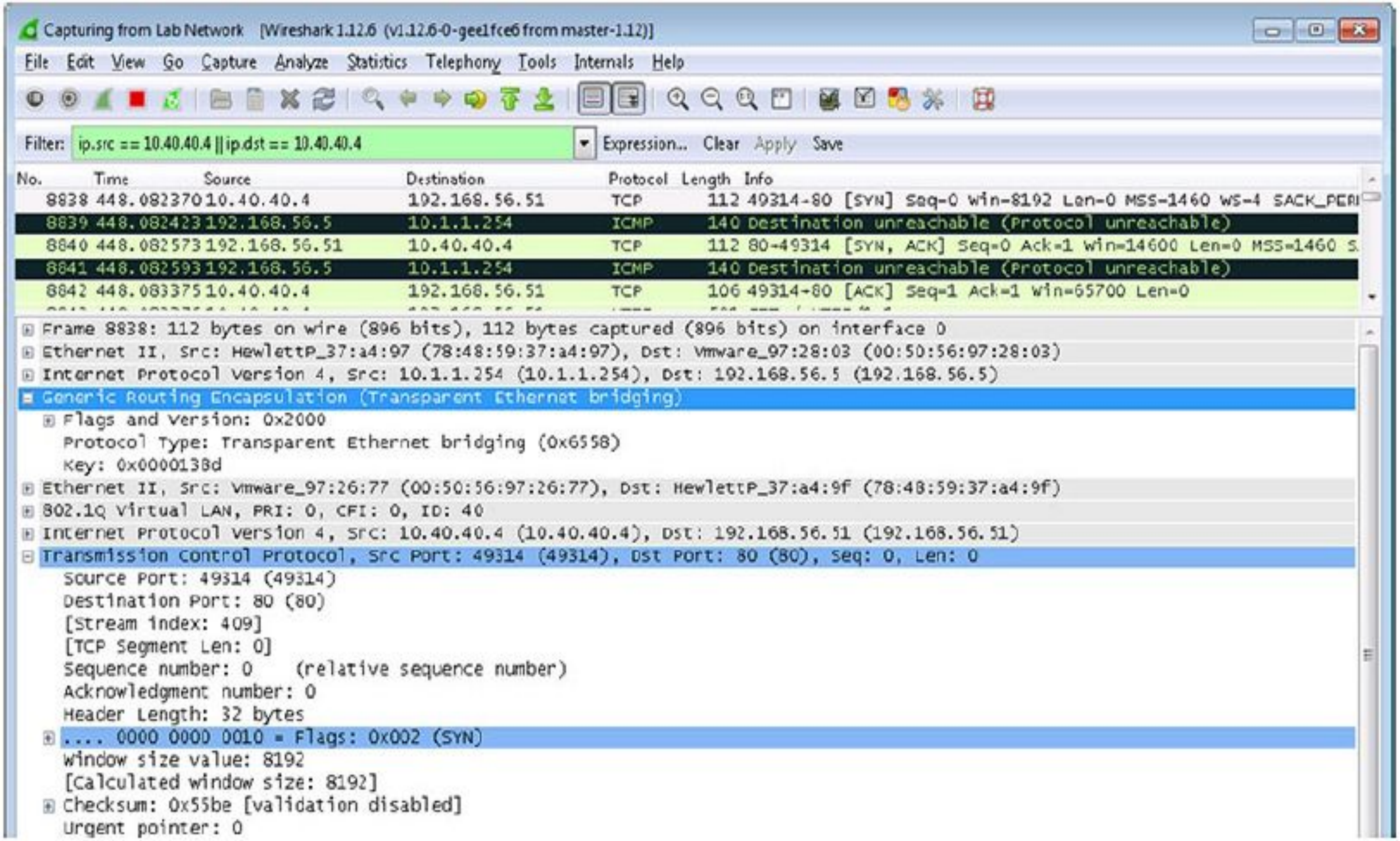


```
ip.src == 10.40.40.4 || ip.dst == 10.40.40.4 and click Apply:
```



```
ip.addr == 10.40.40.4
```

Activate the session

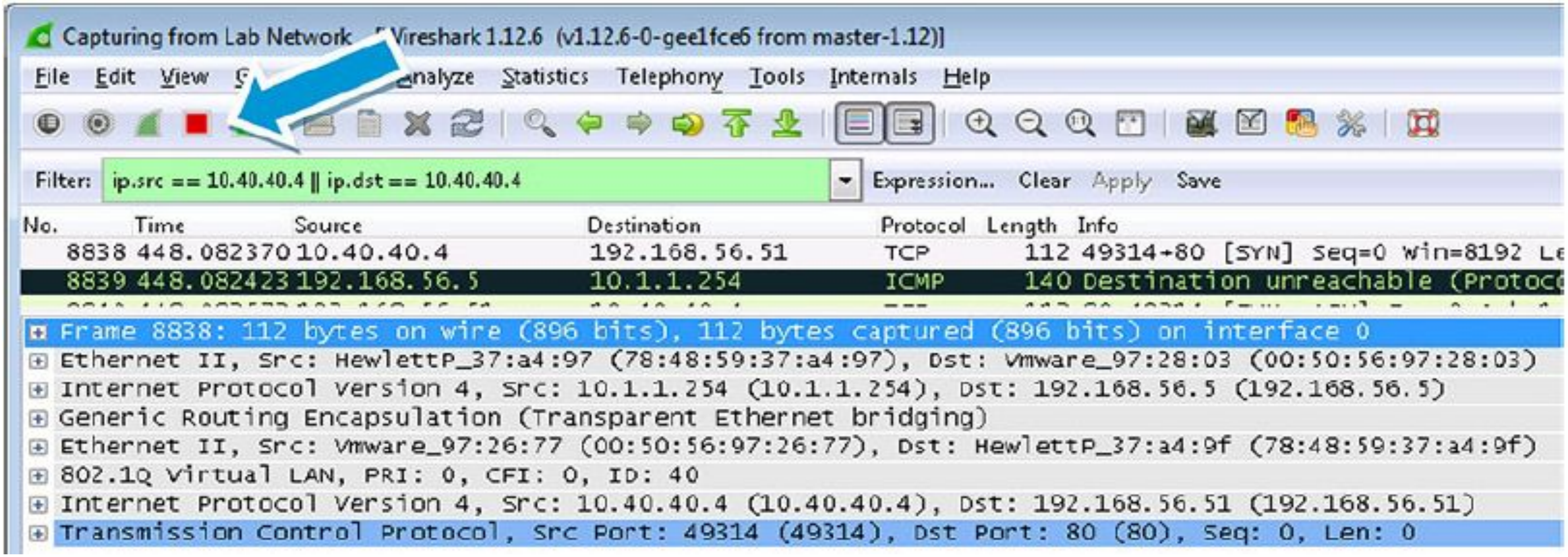

Capturing from Lab Network [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: ip.src == 10.40.40.4 || ip.dst == 10.40.40.4

```
No.   Time       Source         Destination     Protocol Length Info
 8838 448.082370 10.40.40.4     192.168.56.51   TCP      112 49314-80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERI
 8839 448.082423 192.168.56.5   10.1.1.254      ICMP     140 Destination unreachable (Protocol unreachable)
 8840 448.082573 192.168.56.51  10.40.40.4      TCP      112 80-49314 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 S
 8841 448.082593 192.168.56.5   10.1.1.254      ICMP     140 Destination unreachable (Protocol unreachable)
 8842 448.083375 10.40.40.4     192.168.56.51   TCP      106 49314-80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
```

```
⊞ Frame 8838: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface 0
⊞ Ethernet II, Src: HewlettP_37:a4:97 (78:48:59:37:a4:97), Dst: Vmware_97:28:03 (00:50:56:97:28:03)
⊞ Internet Protocol Version 4, Src: 10.1.1.254 (10.1.1.254), Dst: 192.168.56.5 (192.168.56.5)
⊟ Generic Routing Encapsulation (Transparent Ethernet bridging)
   ⊞ Flags and Version: 0x2000
     Protocol Type: Transparent Ethernet bridging (0x6558)
     Key: 0x0000138d
⊞ Ethernet II, Src: Vmware_97:26:77 (00:50:56:97:26:77), Dst: HewlettP_37:a4:9f (78:48:59:37:a4:9f)
⊞ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 40
⊞ Internet Protocol Version 4, Src: 10.40.40.4 (10.40.40.4), Dst: 192.168.56.51 (192.168.56.51)
⊟ Transmission Control Protocol, Src Port: 49314 (49314), Dst Port: 80 (80), Seq: 0, Len: 0
     Source Port: 49314 (49314)
     Destination Port: 80 (80)
     [Stream index: 409]
     [TCP Segment Len: 0]
     Sequence number: 0    (relative sequence number)
     Acknowledgment number: 0
     Header Length: 32 bytes
   ⊞ .... 0000 0000 0010 = Flags: 0x002 (SYN)
     Window size value: 8192
     [Calculated window size: 8192]
   ⊞ Checksum: 0x55be [validation disabled]
     Urgent pointer: 0
```

Activate the session


Capturing from Lab Network [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View G Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: ip.src == 10.40.40.4 || ip.dst == 10.40.40.4

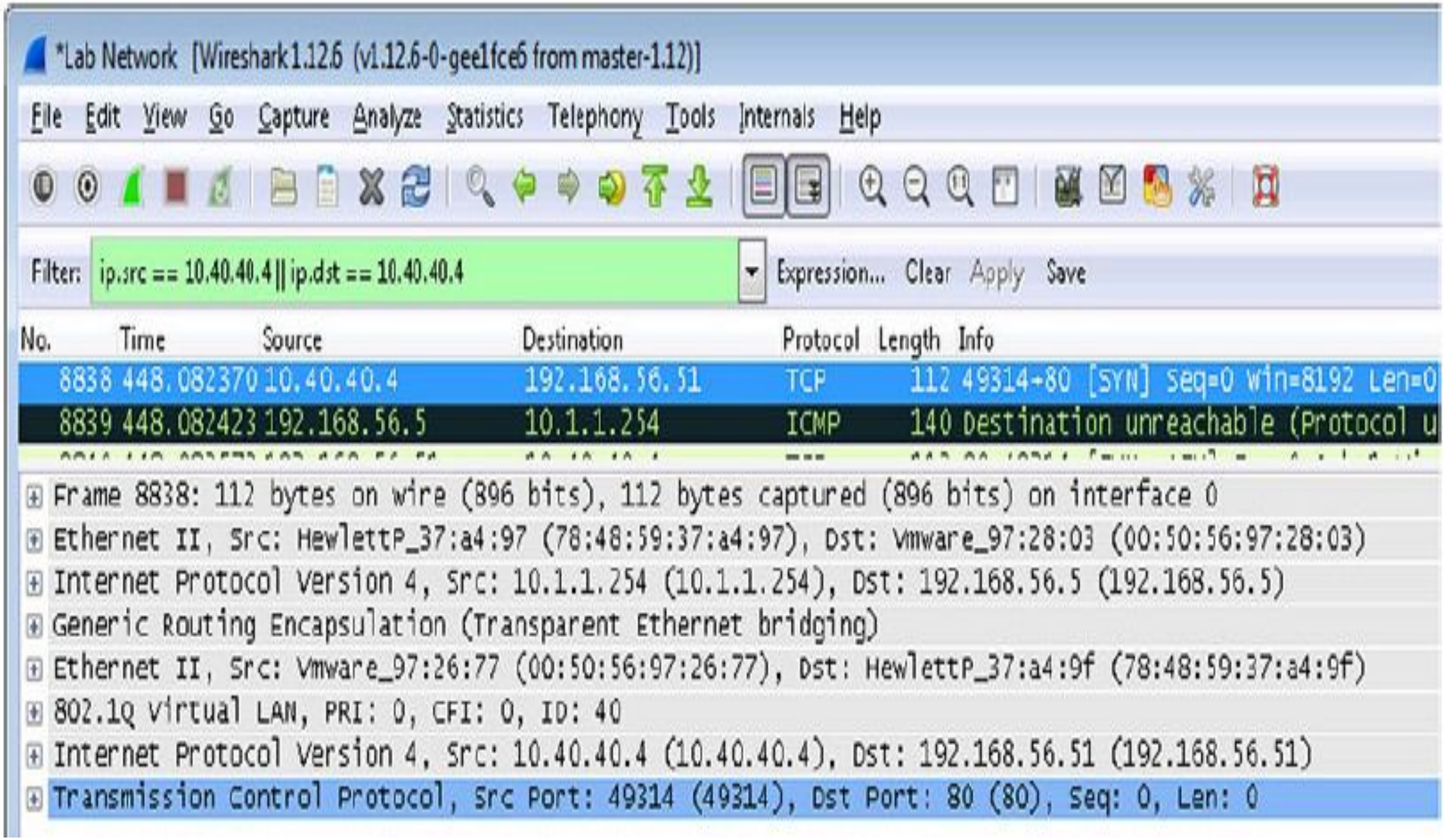
```
No.    Time        Source          Destination       Protocol  Length  Info
  8838 448.082370 10.40.40.4       192.168.56.51     TCP          112 49314→80 [SYN] Seq=0 Win=8192 Le
  8839 448.082423 192.168.56.5     10.1.1.254        ICMP         140 Destination unreachable (Protoco
```

```
⊞ Frame 8838: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface 0
⊞ Ethernet II, Src: HewlettP_37:a4:97 (78:48:59:37:a4:97), Dst: Vmware_97:28:03 (00:50:56:97:28:03)
⊞ Internet Protocol Version 4, Src: 10.1.1.254 (10.1.1.254), Dst: 192.168.56.5 (192.168.56.5)
⊞ Generic Routing Encapsulation (Transparent Ethernet bridging)
⊞ Ethernet II, Src: Vmware_97:26:77 (00:50:56:97:26:77), Dst: HewlettP_37:a4:9f (78:48:59:37:a4:9f)
⊞ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 40
⊞ Internet Protocol Version 4, Src: 10.40.40.4 (10.40.40.4), Dst: 192.168.56.51 (192.168.56.51)
⊞ Transmission Control Protocol, Src Port: 49314 (49314), Dst Port: 80 (80), Seq: 0, Len: 0
```

Activate the session

- Layer 2: Ethernet Frame with source MAC address of an HP switch and the destination a VMware virtual machine (Jumphost)
- Layer 3: IP source of 10.1.1.254 (ProVision P2) and IP destination of 192.168.56.5 (Jumphost)
- Layer 4: GRE tunnel
- Encapsulated Layer 2: Source MAC address of VMware host (UserVM4) and destination MAC address of an HP switch (Comware switch C1)
- Encapsulated 802.1Q VLAN information
- Encapsulated Layer 3: Source IP address of 10.40.40.4 (UserVM4) and destination IP address of 192.168.56.51 (hp.com test website)
- Encapsulated Layer 4: TCP destination port 80

Activate the session


*Lab Network [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: ip.src == 10.40.40.4 || ip.dst == 10.40.40.4

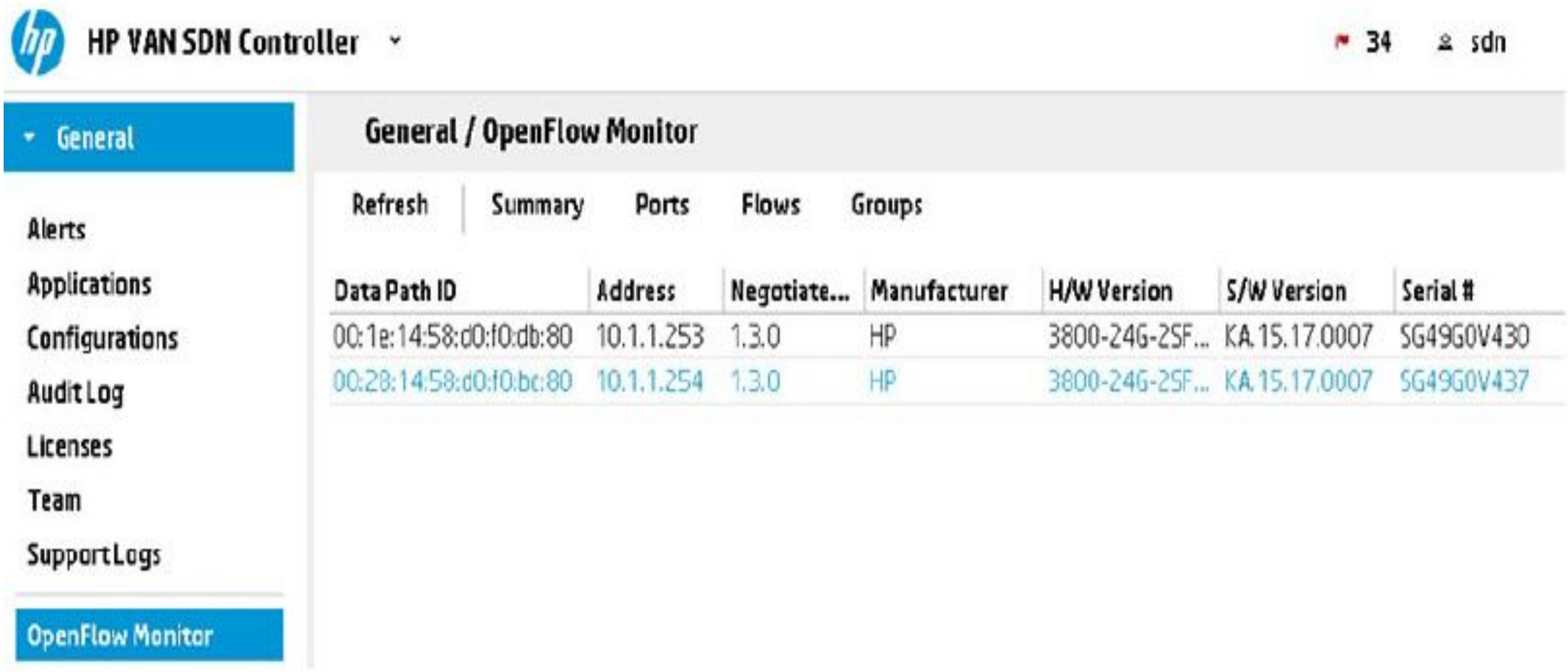
```
No.   Time        Source        Destination    Protocol Length Info
8838 448.082370 10.40.40.4     192.168.56.51  TCP       112 49314→80 [SYN] Seq=0 Win=8192 Len=0
8839 448.082423 192.168.56.5   10.1.1.254     ICMP      140 Destination unreachable (Protocol u
```

```
⊞ Frame 8838: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface 0
⊞ Ethernet II, Src: HewlettP_37:a4:97 (78:48:59:37:a4:97), Dst: Vmware_97:28:03 (00:50:56:97:28:03)
⊞ Internet Protocol Version 4, Src: 10.1.1.254 (10.1.1.254), Dst: 192.168.56.5 (192.168.56.5)
⊞ Generic Routing Encapsulation (Transparent Ethernet bridging)
⊞ Ethernet II, Src: Vmware_97:26:77 (00:50:56:97:26:77), Dst: HewlettP_37:a4:9f (78:48:59:37:a4:9f)
⊞ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 40
⊞ Internet Protocol Version 4, Src: 10.40.40.4 (10.40.40.4), Dst: 192.168.56.51 (192.168.56.51)
⊞ Transmission Control Protocol, Src Port: 49314 (49314), Dst Port: 80 (80), Seq: 0, Len: 0
```

Activate the session

General

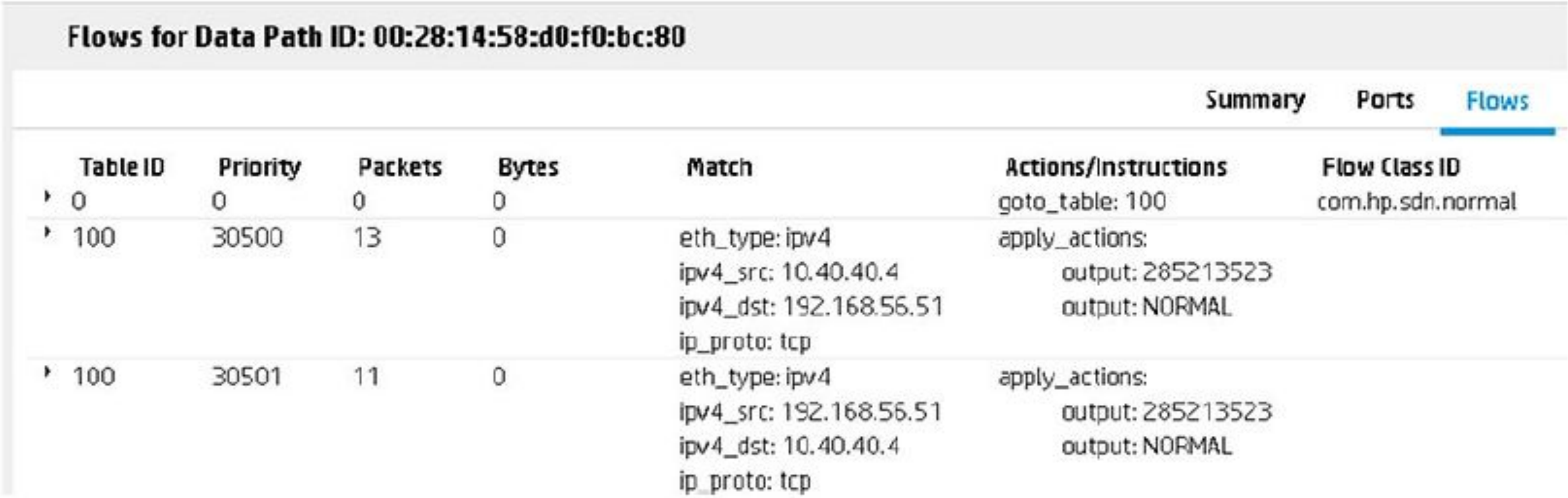
OpenFlow Monitor



Data Path ID	Address	Negotiate...	Manufacturer	H/W Version	S/W Version	Serial #
00:1e:14:58:d0:f0:db:80	10.1.1.253	1.3.0	HP	3800-24G-2SF...	KA.15.17.0007	SG49G0V430
00:28:14:58:d0:f0:bc:80	10.1.1.254	1.3.0	HP	3800-24G-2SF...	KA.15.17.0007	SG49G0V437

Activate the session

Flows

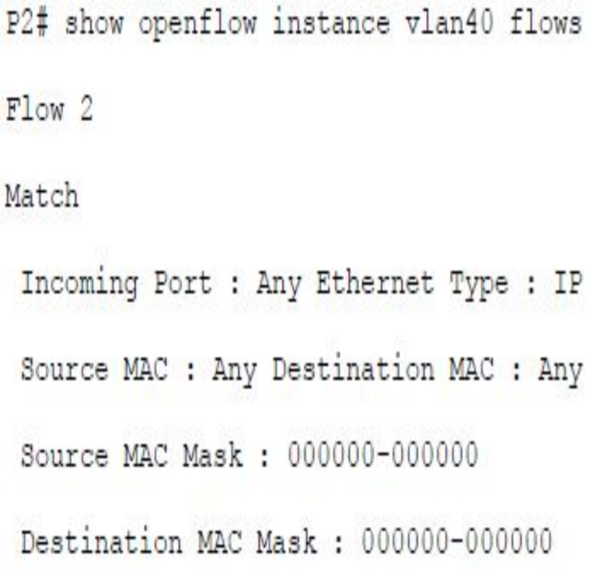


Flows for Data Path ID: 00:28:14:58:d0:f0:bc:80

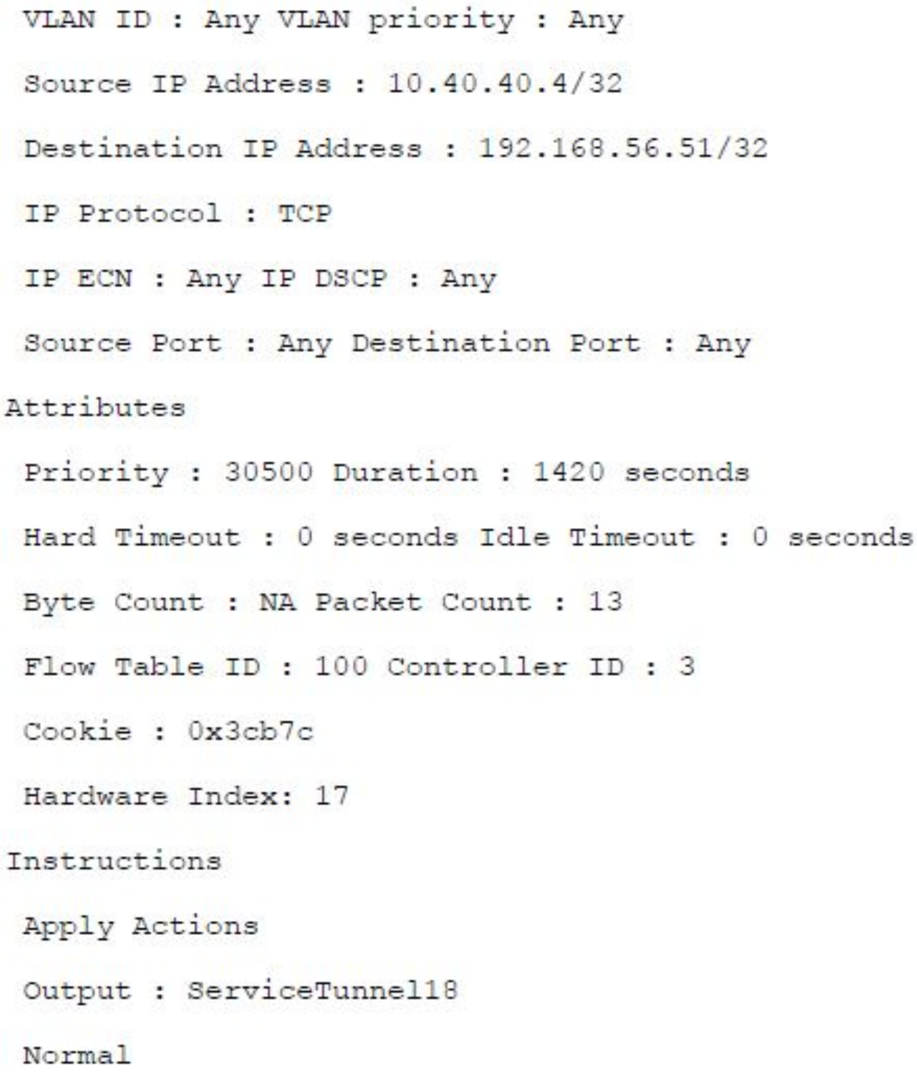
Table ID	Priority	Packets	Bytes	Match	Actions/Instructions	Flow Class ID
0	0	0	0		goto_table: 100	com.hp.sdn.normal
100	30500	13	0	eth_type: ipv4 ipv4_src: 10.40.40.4 ipv4_dst: 192.168.56.51 ip_proto: tcp	apply_actions: output: 285213523 output: NORMAL	
100	30501	11	0	eth_type: ipv4 ipv4_src: 192.168.56.51 ipv4_dst: 10.40.40.4 ip_proto: tcp	apply_actions: output: 285213523 output: NORMAL	

Result:

Activate the session

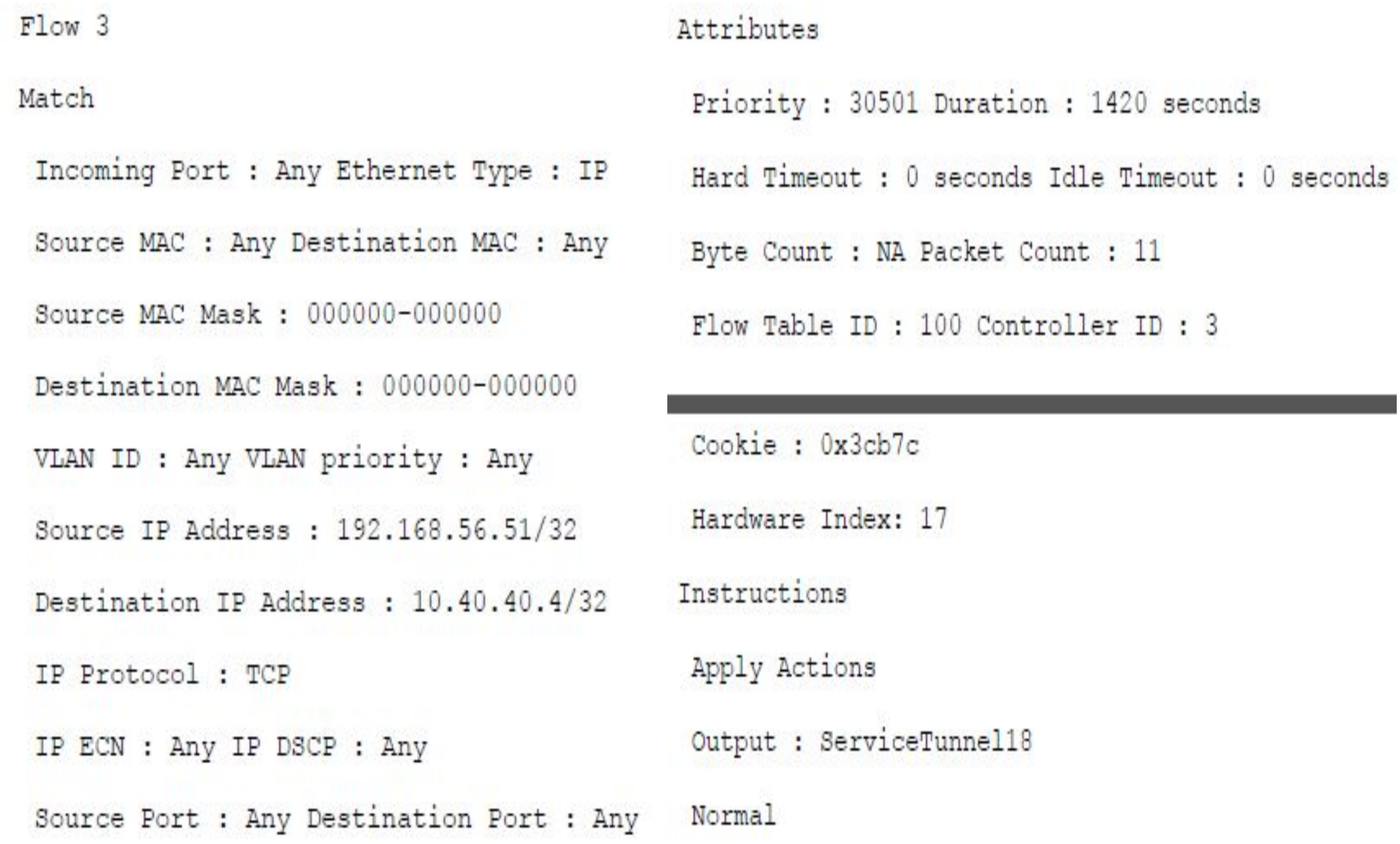


```
P2# show openflow instance vlan40 flows

Flow 2

Match

 Incoming Port : Any Ethernet Type : IP

 Source MAC : Any Destination MAC : Any

 Source MAC Mask : 000000-000000

 Destination MAC Mask : 000000-000000
```



```
 VLAN ID : Any VLAN priority : Any

 Source IP Address : 10.40.40.4/32

 Destination IP Address : 192.168.56.51/32

 IP Protocol : TCP

 IP ECN : Any IP DSCP : Any

 Source Port : Any Destination Port : Any

Attributes

 Priority : 30500 Duration : 1420 seconds

 Hard Timeout : 0 seconds Idle Timeout : 0 seconds

 Byte Count : NA Packet Count : 13

 Flow Table ID : 100 Controller ID : 3

 Cookie : 0x3cb7c

 Hardware Index: 17

Instructions

 Apply Actions

 Output : ServiceTunnel18

 Normal
```

Activate the session

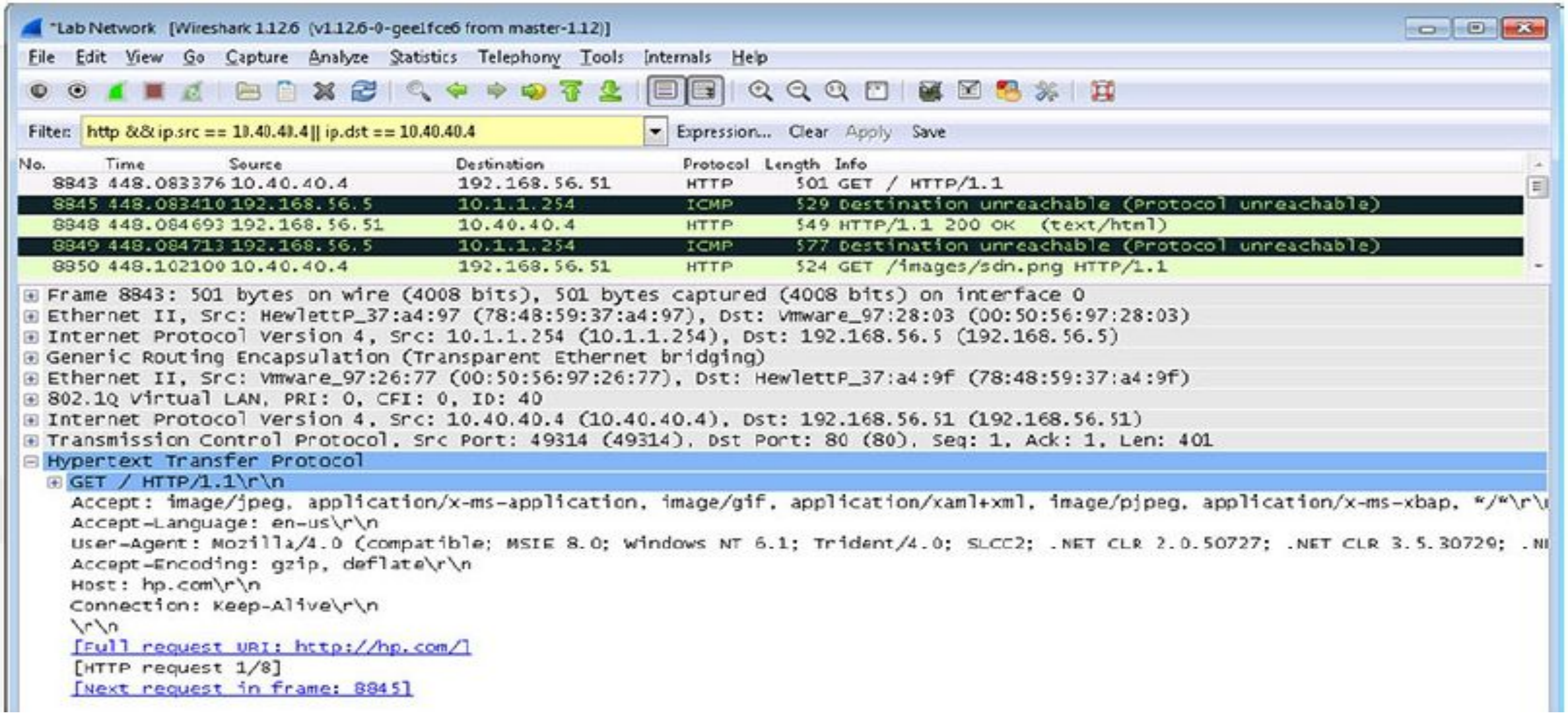


```
Flow 3

Match

 Incoming Port : Any Ethernet Type : IP

 Source MAC : Any Destination MAC : Any

 Source MAC Mask : 000000-000000

 Destination MAC Mask : 000000-000000

 VLAN ID : Any VLAN priority : Any

 Source IP Address : 192.168.56.51/32

 Destination IP Address : 10.40.40.4/32

 IP Protocol : TCP

 IP ECN : Any IP DSCP : Any

 Source Port : Any Destination Port : Any
```

```
Attributes

 Priority : 30501 Duration : 1420 seconds

 Hard Timeout : 0 seconds Idle Timeout : 0 seconds

 Byte Count : NA Packet Count : 11

 Flow Table ID : 100 Controller ID : 3

 Cookie : 0x3cb7c

 Hardware Index: 17

Instructions

 Apply Actions

 Output : ServiceTunnel18

 Normal
```

Activate the session

```
Filter: http && ip.src == 10.40.40.4 || ip.dst == 10.40.40.4
```

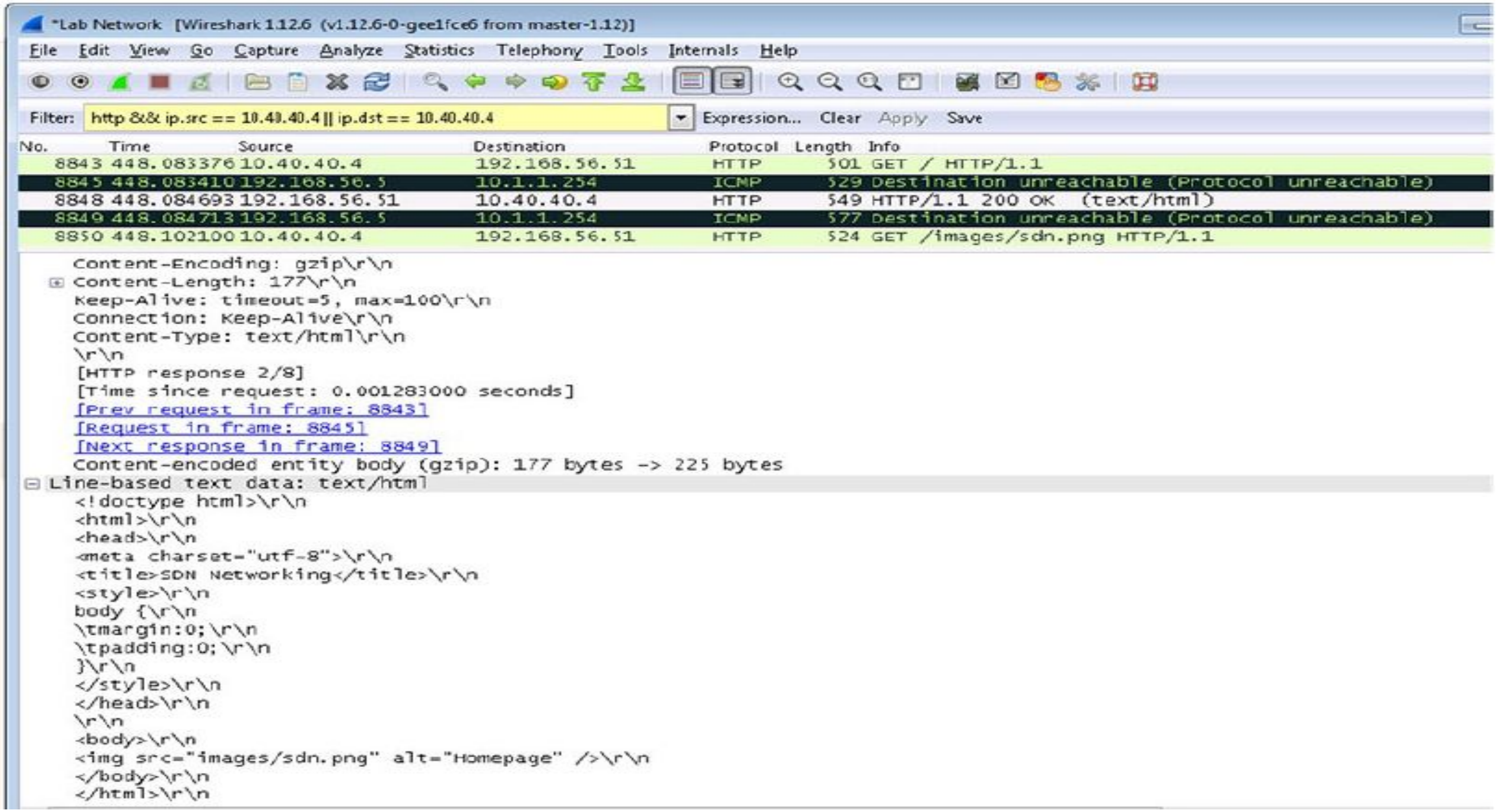


*Lab Network [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http && ip.src == 10.40.40.4 || ip.dst == 10.40.40.4
Expression... Clear Apply Save

```
No.   Time        Source          Destination     Protocol Length Info
 8843 448.083376  10.40.40.4      192.168.56.51   HTTP     501 GET / HTTP/1.1
 8845 448.083410  192.168.56.5    10.1.1.254      ICMP     529 Destination unreachable (Protocol unreachable)
 8848 448.084693  192.168.56.51   10.40.40.4      HTTP     549 HTTP/1.1 200 OK  (text/html)
 8849 448.084713  192.168.56.5    10.1.1.254      ICMP     577 Destination unreachable (Protocol unreachable)
 8850 448.102100  10.40.40.4      192.168.56.51   HTTP     524 GET /images/sdn.png HTTP/1.1
```

```
⊞ Frame 8843: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface 0
⊞ Ethernet II, Src: HewlettP_37:a4:97 (78:48:59:37:a4:97), Dst: Vmware_97:28:03 (00:50:56:97:28:03)
⊞ Internet Protocol Version 4, Src: 10.1.1.254 (10.1.1.254), Dst: 192.168.56.5 (192.168.56.5)
⊞ Generic Routing Encapsulation (Transparent Ethernet bridging)
⊞ Ethernet II, Src: Vmware_97:26:77 (00:50:56:97:26:77), Dst: HewlettP_37:a4:9f (78:48:59:37:a4:9f)
⊞ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 40
⊞ Internet Protocol Version 4, Src: 10.40.40.4 (10.40.40.4), Dst: 192.168.56.51 (192.168.56.51)
⊞ Transmission Control Protocol, Src Port: 49314 (49314), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 401
⊟ Hypertext Transfer Protocol
  ⊞ GET / HTTP/1.1\r\n
    Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg, application/x-ms-xbap, */*\r\
    Accept-Language: en-us\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .N
    Accept-Encoding: gzip, deflate\r\n
    Host: hp.com\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://hp.com/]
    [HTTP request 1/8]
    [Next request in frame: 8845]
```

Activate the session


*Lab Network [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

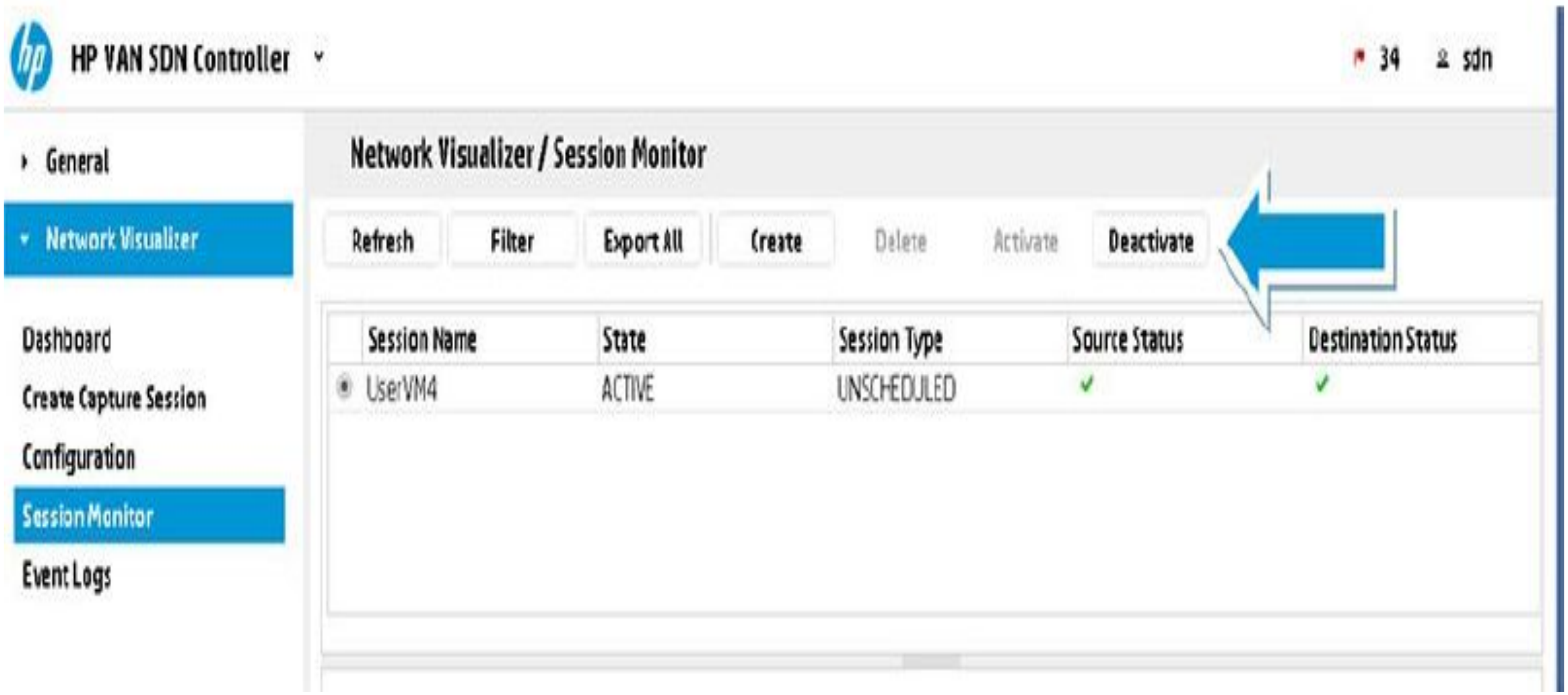
Filter: http && ip.src == 10.40.40.4 || ip.dst == 10.40.40.4

```
No.   Time        Source          Destination     Protocol Length Info
 8843 448.083376 10.40.40.4      192.168.56.51   HTTP     501 GET / HTTP/1.1
 8845 448.083410 192.168.56.5    10.1.1.254      ICMP     529 Destination unreachable (Protocol unreachable)
 8848 448.084693 192.168.56.51   10.40.40.4      HTTP     549 HTTP/1.1 200 OK  (text/html)
 8849 448.084713 192.168.56.5    10.1.1.254      ICMP     577 Destination unreachable (Protocol unreachable)
 8850 448.102100 10.40.40.4      192.168.56.51   HTTP     524 GET /images/sdn.png HTTP/1.1
```

```
    Content-Encoding: gzip\r\n
 ⊞  Content-Length: 177\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html\r\n
    \r\n
    [HTTP response 2/8]
    [Time since request: 0.001283000 seconds]
    [Prev request in frame: 8843]
    [Request in frame: 8845]
    [Next response in frame: 8849]
    Content-encoded entity body (gzip): 177 bytes -> 225 bytes
⊟ Line-based text data: text/html
    <!doctype html>\r\n
    <html>\r\n
    <head>\r\n
    <meta charset="utf-8">\r\n
    <title>SDN Networking</title>\r\n
    <style>\r\n
    body {\r\n
    \tmargin:0;\r\n
    \tpadding:0;\r\n
    }\r\n
    </style>\r\n
    </head>\r\n
    \r\n
    <body>\r\n
    <img src="images/sdn.png" alt="Homepage" />\r\n
    </body>\r\n
    </html>\r\n
```

Activate the session

Deactivate

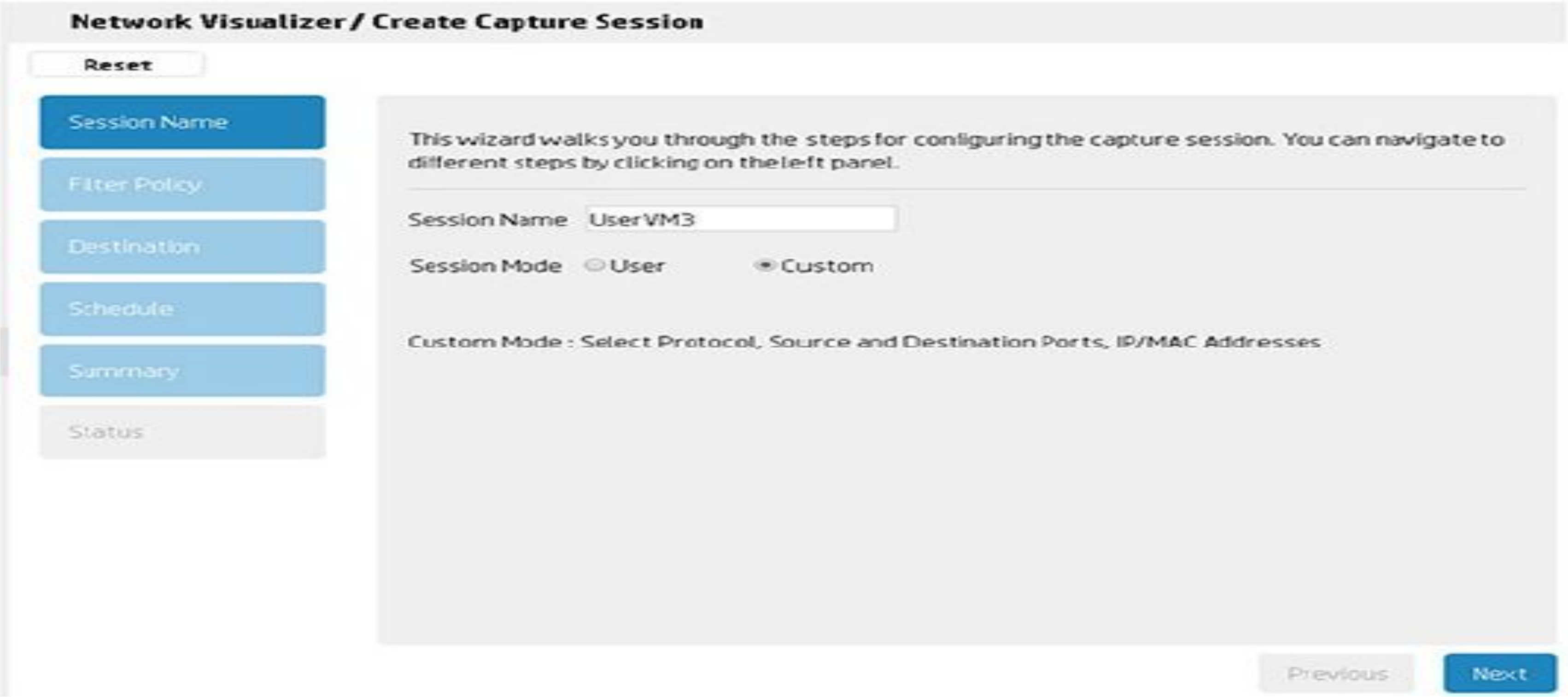


	Session Name	State	Session Type	Source Status	Destination Status
●	UserVM4	ACTIVE	UNSCHEDULED	✓	✓

Activate the session

Create Capture Session
Session Name UserVM3

Session Mode Next



Network Visualizer / Create Capture Session

This wizard walks you through the steps for configuring the capture session. You can navigate to different steps by clicking on the left panel.

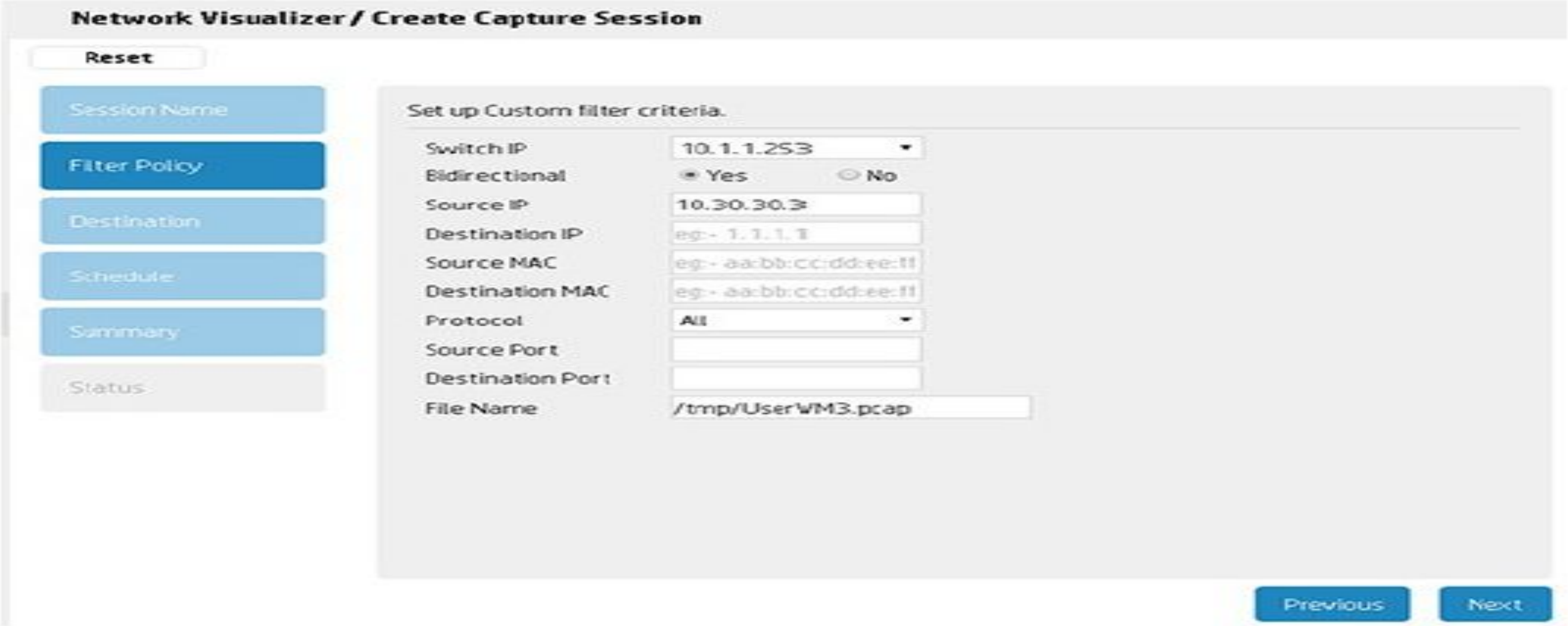
Session Name: UserVM3

Session Mode: ○ User ● Custom

Custom Mode : Select Protocol, Source and Destination Ports, IP/MAC Addresses

Activate the session

- Switch IP: 10.1.1.253
- Bidirectional: Yes
- Source IP: 10.30.30.3
- Leave other options and default values and click Next:



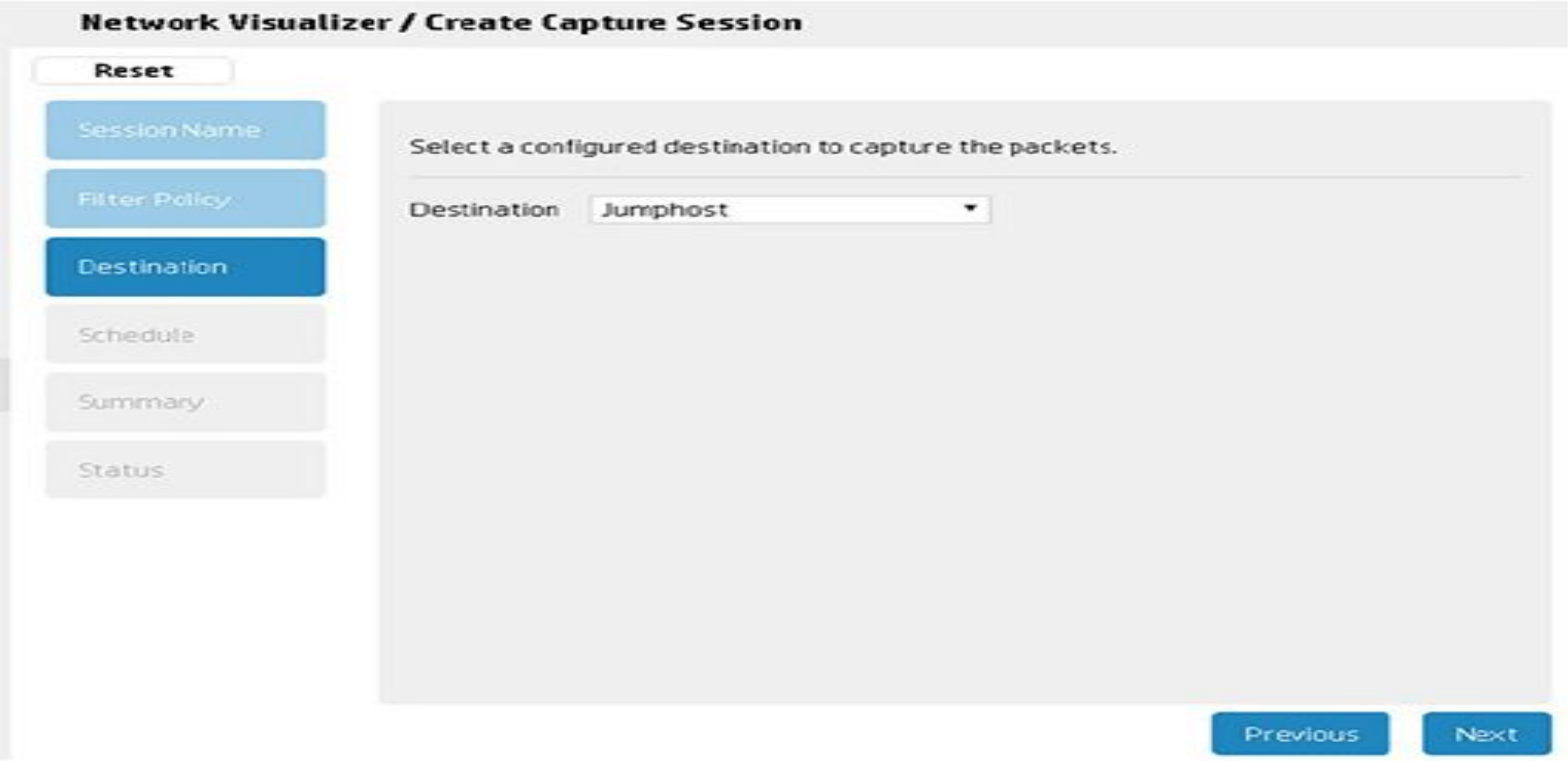
Network Visualizer / Create Capture Session

Set up Custom filter criteria.

Switch IP	10.1.1.253
Bidirectional	● Yes ○ No
Source IP	10.30.30.3
Destination IP	eg:- 1.1.1.1
Source MAC	eg:- aa:bb:cc:dd:ee:ff
Destination MAC	eg:- aa:bb:cc:dd:ee:ff
Protocol	All
Source Port	
Destination Port	
File Name	/tmp/UserVM3.pcap

Activate the session

Destination Jumphost Next



Network Visualizer / Create Capture Session

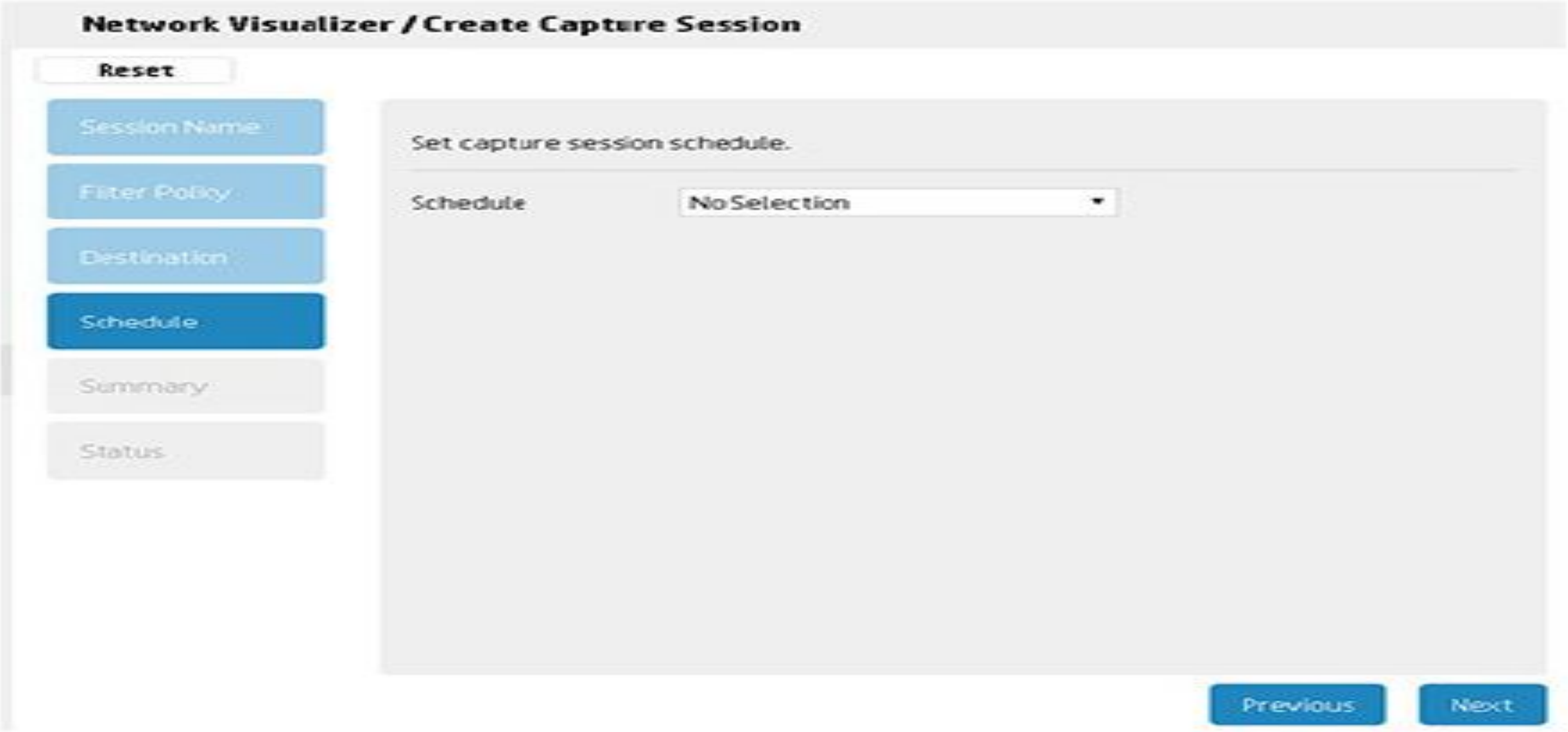
Select a configured destination to capture the packets.

Destination: Jumphost

Activate the session

No Selection

Next



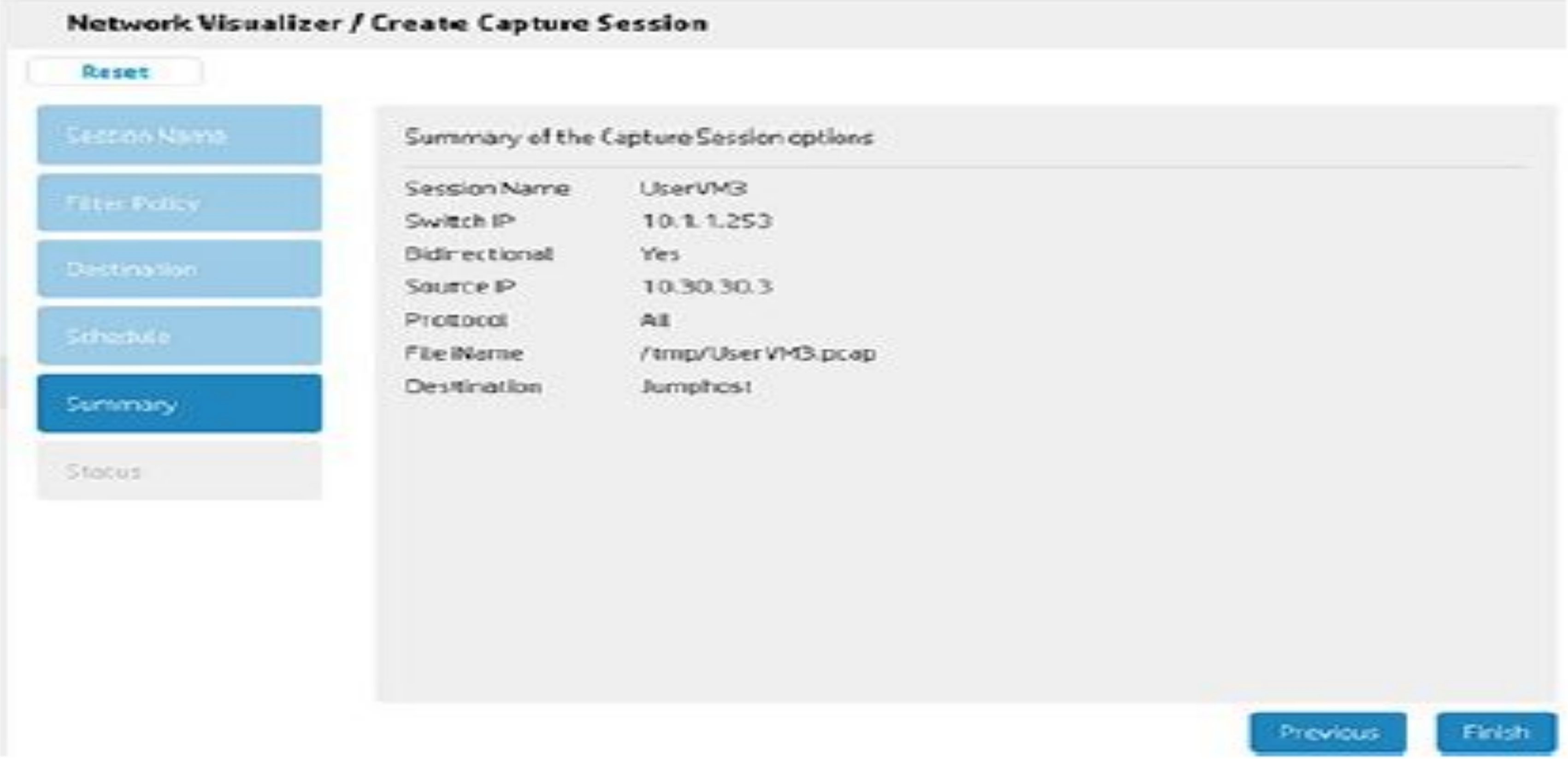
Network Visualizer / Create Capture Session

Set capture session schedule.

Schedule: No Selection

Activate the session

Finish



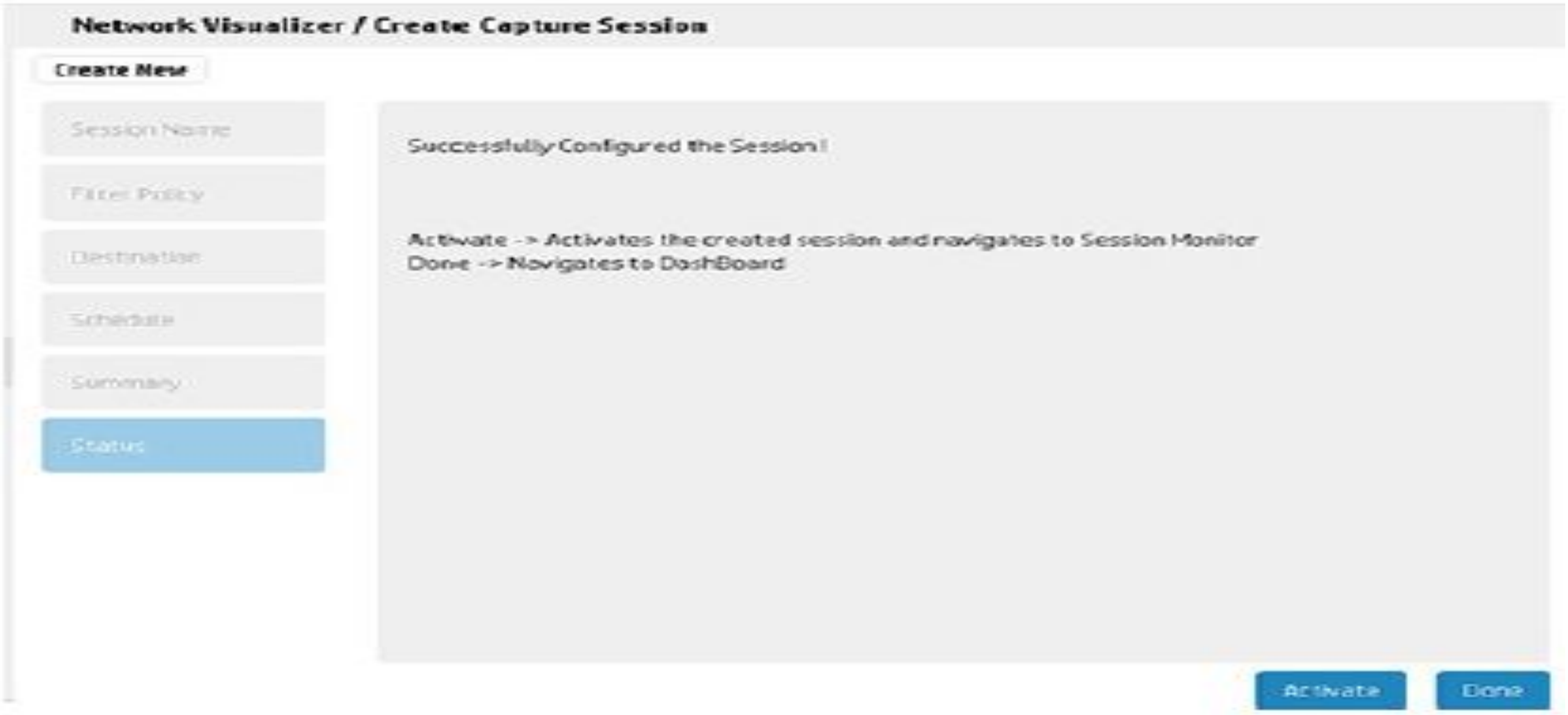
Network Visualizer / Create Capture Session

Summary of the Capture Session options

Session Name	UserVM3
Switch IP	10.1.1.253
Bidirectional	Yes
Source IP	10.30.30.3
Protocol	All
File Name	/tmp/UserVM3.pcap
Destination	Jumphost

Activate the session

Activate

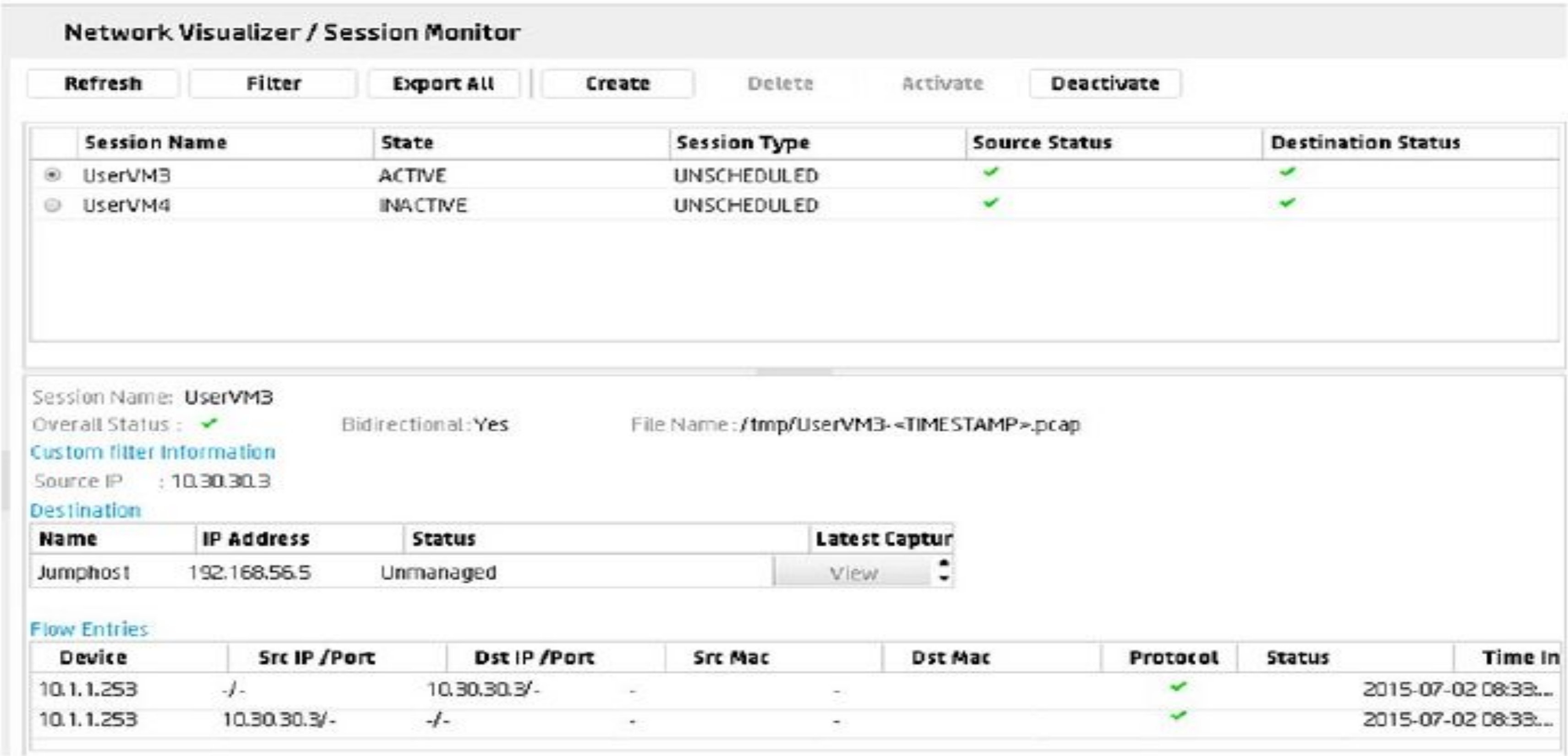


Successfully Configured the Session !

Activate -> Activates the created session and navigates to Session Monitor
Done -> Navigates to DashBoard

Activate the session

Session Monitor



Network Visualizer / Session Monitor

	Session Name	State	Session Type	Source Status	Destination Status
●	UserVM3	ACTIVE	UNSCHEDULED	✓	✓
○	UserVM4	INACTIVE	UNSCHEDULED	✓	✓

Session Name: UserVM3

Overall Status : ✓ Bidirectional : Yes File Name : /tmp/UserVM3-<TIMESTAMP>.pcap

Custom filter Information

Source IP : 10.30.30.3

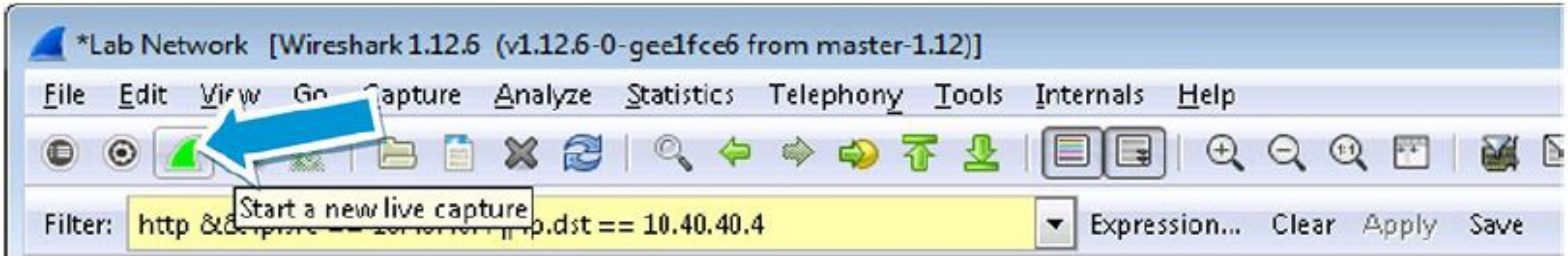
Destination

Name	IP Address	Status	Latest Captur
Jumphost	192.168.56.5	Unmanaged	View

Flow Entries

Device	Src IP /Port	Dst IP /Port	Src Mac	Dst Mac	Protocol	Status	Time In
10.1.1.253	-/-	10.30.30.3/-	-	-	✓		2015-07-02 08:33:...
10.1.1.253	10.30.30.3/-	-/-	-	-	✓		2015-07-02 08:33:...

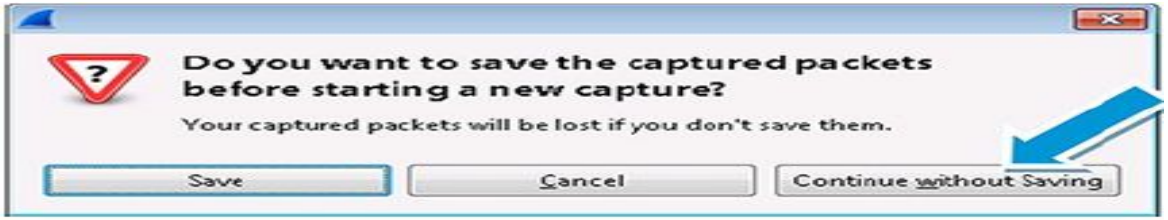
Activate the session



*Lab Network [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]

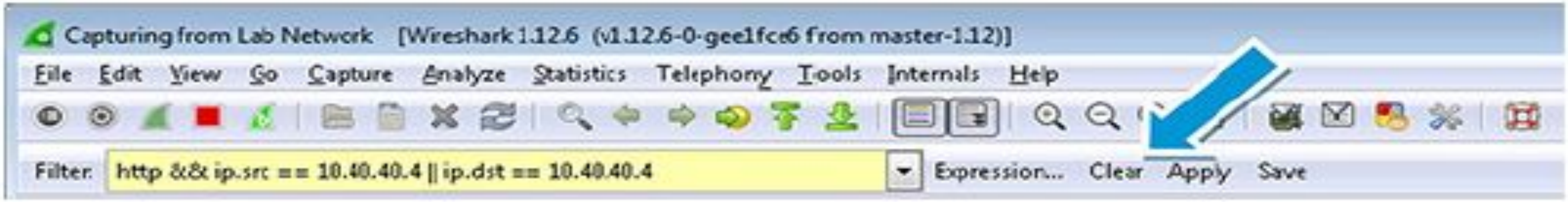
Filter: http &&... p.dst == 10.40.40.4

Continue without Saving



Do you want to save the captured packets before starting a new capture?

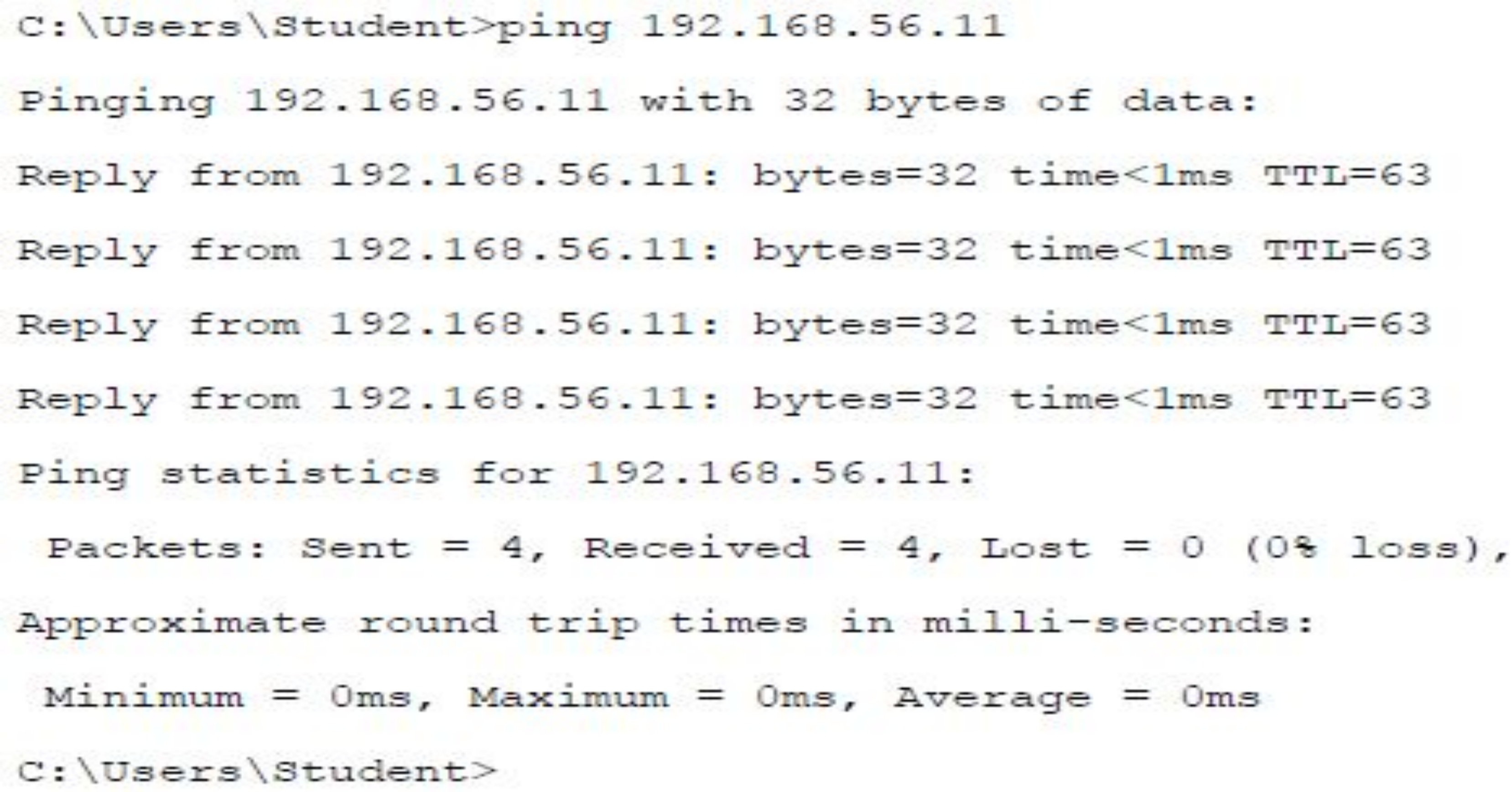
Your captured packets will be lost if you don't save them.



Capturing from Lab Network [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]

Filter: http && ip.src == 10.40.40.4 || ip.dst == 10.40.40.4

Activate the session

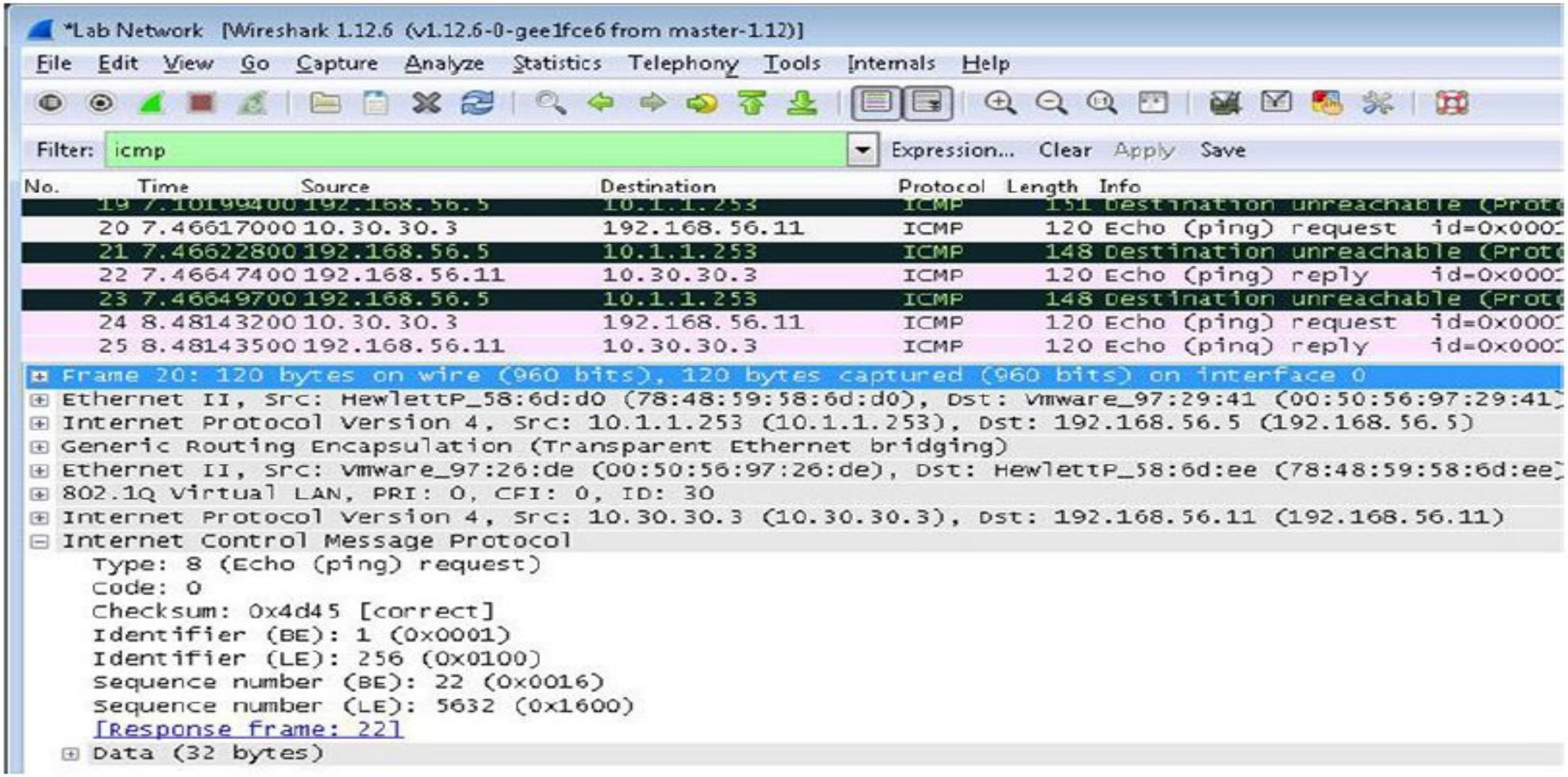


```
C:\Users\Student>ping 192.168.56.11
Pinging 192.168.56.11 with 32 bytes of data:
Reply from 192.168.56.11: bytes=32 time<1ms TTL=63
Reply from 192.168.56.11: bytes=32 time<1ms TTL=63
Reply from 192.168.56.11: bytes=32 time<1ms TTL=63
Reply from 192.168.56.11: bytes=32 time<1ms TTL=63
Ping statistics for 192.168.56.11:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\Student>
```

Activate the session

Stop

icmp


*Lab Network [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

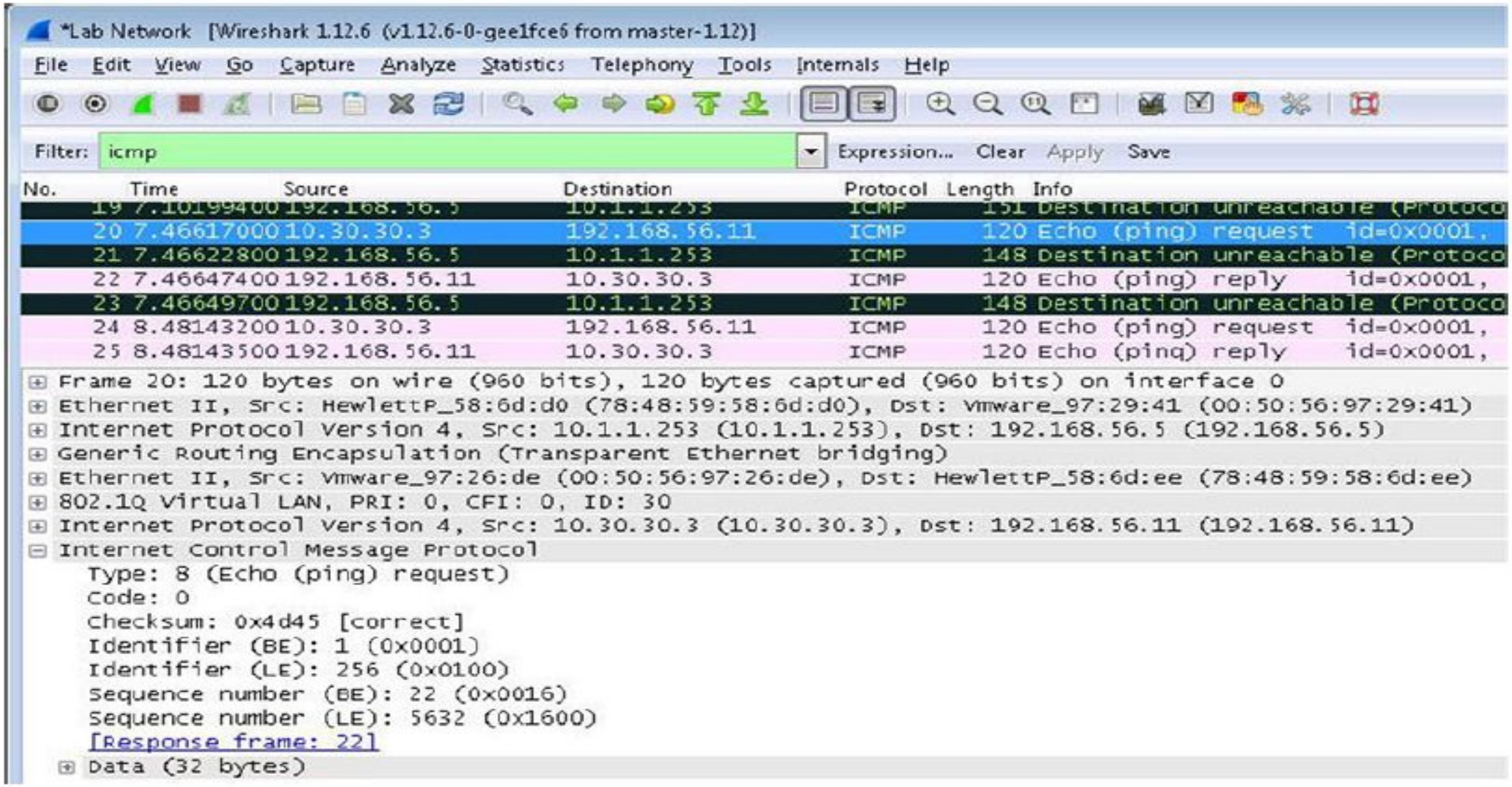
Filter: icmp

```
No.    Time          Source           Destination      Protocol  Length  Info
  19 7.10199400 192.168.56.5          10.1.1.253       ICMP      151 Destination unreachable (Prot
  20 7.46617000 10.30.30.3            192.168.56.11    ICMP      120 Echo (ping) request   id=0x000
  21 7.46622800 192.168.56.5          10.1.1.253       ICMP      148 Destination unreachable (Prot
  22 7.46647400 192.168.56.11         10.30.30.3       ICMP      120 Echo (ping) reply     id=0x000
  23 7.46649700 192.168.56.5          10.1.1.253       ICMP      148 Destination unreachable (Prot
  24 8.48143200 10.30.30.3            192.168.56.11    ICMP      120 Echo (ping) request   id=0x000
  25 8.48143500 192.168.56.11         10.30.30.3       ICMP      120 Echo (ping) reply     id=0x000
```

```
⊞ Frame 20: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface 0
⊞ Ethernet II, Src: HewlettP_58:6d:d0 (78:48:59:58:6d:d0), Dst: Vmware_97:29:41 (00:50:56:97:29:41)
⊞ Internet Protocol Version 4, Src: 10.1.1.253 (10.1.1.253), Dst: 192.168.56.5 (192.168.56.5)
⊞ Generic Routing Encapsulation (Transparent Ethernet bridging)
⊞ Ethernet II, Src: Vmware_97:26:de (00:50:56:97:26:de), Dst: HewlettP_58:6d:ee (78:48:59:58:6d:ee)
⊞ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 30
⊞ Internet Protocol Version 4, Src: 10.30.30.3 (10.30.30.3), Dst: 192.168.56.11 (192.168.56.11)
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d45 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 22 (0x0016)
    Sequence number (LE): 5632 (0x1600)
    [Response frame: 22]
  ⊞ Data (32 bytes)
```

Activate the session

ICMP message



Filter: icmp

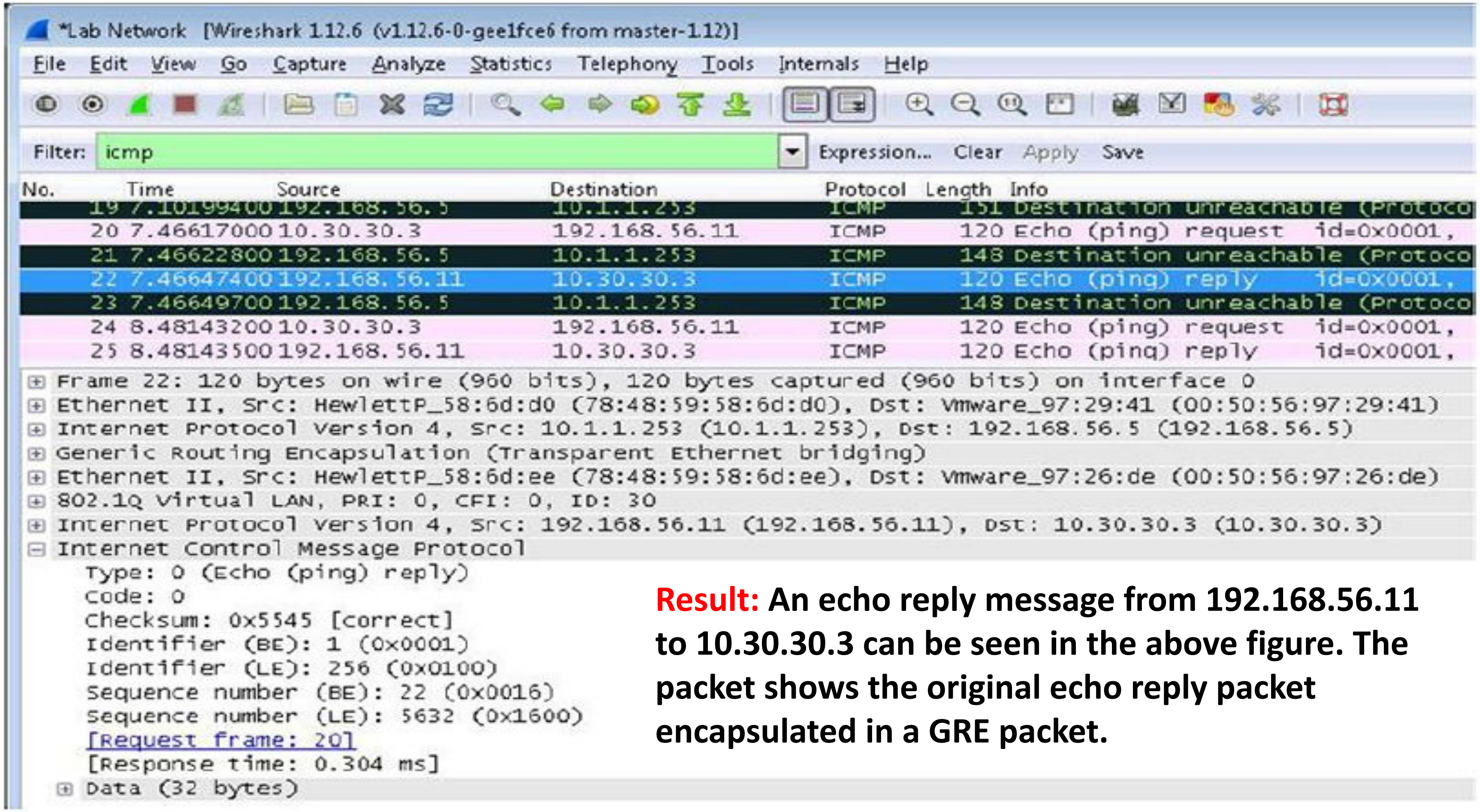
```
No.   Time          Source          Destination      Protocol  Length  Info
   19 7.10199400 192.168.56.5    10.1.1.253       ICMP      151 Destination unreachable (Protoco
   20 7.46617000 10.30.30.3      192.168.56.11    ICMP      120 Echo (ping) request  id=0x0001,
   21 7.46622800 192.168.56.5    10.1.1.253       ICMP      148 Destination unreachable (Protoco
   22 7.46647400 192.168.56.11   10.30.30.3       ICMP      120 Echo (ping) reply    id=0x0001,
   23 7.46649700 192.168.56.5    10.1.1.253       ICMP      148 Destination unreachable (Protoco
   24 8.48143200 10.30.30.3      192.168.56.11    ICMP      120 Echo (ping) request  id=0x0001,
   25 8.48143500 192.168.56.11   10.30.30.3       ICMP      120 Echo (ping) reply    id=0x0001,
```

```
⊞ Frame 20: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface 0
⊞ Ethernet II, Src: HewlettP_58:6d:d0 (78:48:59:58:6d:d0), Dst: Vmware_97:29:41 (00:50:56:97:29:41)
⊞ Internet Protocol Version 4, Src: 10.1.1.253 (10.1.1.253), Dst: 192.168.56.5 (192.168.56.5)
⊞ Generic Routing Encapsulation (Transparent Ethernet bridging)
⊞ Ethernet II, Src: Vmware_97:26:de (00:50:56:97:26:de), Dst: HewlettP_58:6d:ee (78:48:59:58:6d:ee)
⊞ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 30
⊞ Internet Protocol Version 4, Src: 10.30.30.3 (10.30.30.3), Dst: 192.168.56.11 (192.168.56.11)
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d45 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 22 (0x0016)
    Sequence number (LE): 5632 (0x1600)
    [Response frame: 22]
  ⊞ Data (32 bytes)
```

Activate the session

- **Layer 2:** Ethernet Frame with source MAC address of an HP switch and the destination a Vmware virtual machine (Jumphost)
- **Layer 3: IP** source of 10.1.1.253 (ProVision S1) and IP destination of 192.168.56.5 (Jumphost)
- **Layer 4:** GRE tunnel
- **Encapsulated Layer 2:** Source MAC address of VMware host (UserVM3) and destination MAC address of an HP switch (Comware switch 1)
- **Encapsulated 802.1Q** VLAN information
- **Encapsulated Layer 3:** Source IP address of 10.30.30.3 (UserVM4) and destination IP address of 192.168.56.11 (HP VAN SDN Controller)
- **Encapsulated Layer 4:** ICMP echo request message

Activate the session



*Lab Network [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: icmp

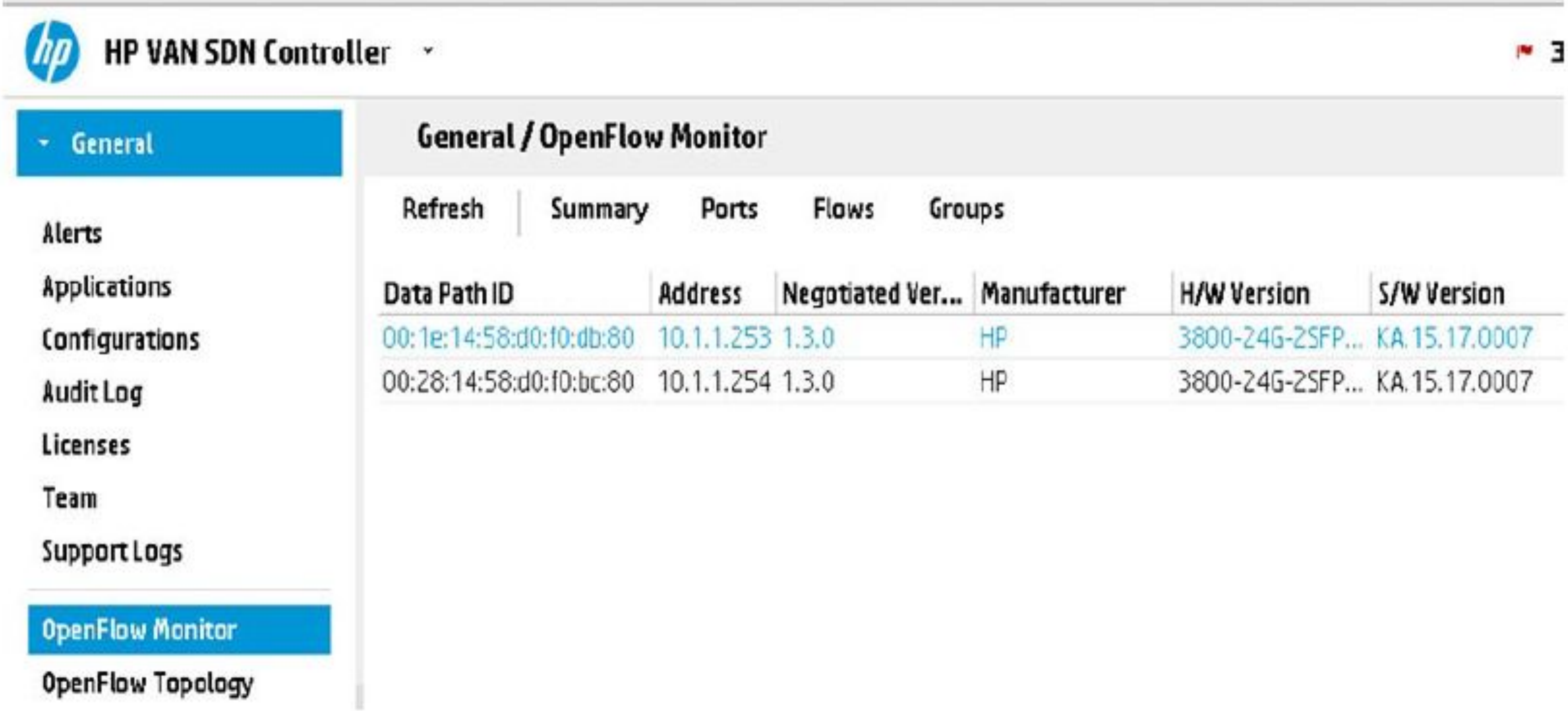
```
No.  Time        Source          Destination     Protocol Length Info
 19 7.10199400 192.168.56.5    10.1.1.253      ICMP     151 Destination unreachable (Protoco
 20 7.46617000 10.30.30.3      192.168.56.11   ICMP     120 Echo (ping) request  id=0x0001,
 21 7.46622800 192.168.56.5    10.1.1.253      ICMP     148 Destination unreachable (Protoco
 22 7.46647400 192.168.56.11   10.30.30.3      ICMP     120 Echo (ping) reply    id=0x0001,
 23 7.46649700 192.168.56.5    10.1.1.253      ICMP     148 Destination unreachable (Protoco
 24 8.48143200 10.30.30.3      192.168.56.11   ICMP     120 Echo (ping) request  id=0x0001,
 25 8.48143500 192.168.56.11   10.30.30.3      ICMP     120 Echo (ping) reply    id=0x0001,

⊞ Frame 22: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface 0
⊞ Ethernet II, Src: HewlettP_58:6d:d0 (78:48:59:58:6d:d0), Dst: Vmware_97:29:41 (00:50:56:97:29:41)
⊞ Internet Protocol Version 4, Src: 10.1.1.253 (10.1.1.253), Dst: 192.168.56.5 (192.168.56.5)
⊞ Generic Routing Encapsulation (Transparent Ethernet bridging)
⊞ Ethernet II, Src: HewlettP_58:6d:ee (78:48:59:58:6d:ee), Dst: Vmware_97:26:de (00:50:56:97:26:de)
⊞ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 30
⊞ Internet Protocol Version 4, Src: 192.168.56.11 (192.168.56.11), Dst: 10.30.30.3 (10.30.30.3)
⊟ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x5545 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 22 (0x0016)
    Sequence number (LE): 5632 (0x1600)
    [Request frame: 20]
    [Response time: 0.304 ms]
  ⊞ Data (32 bytes)
```

Result: An echo reply message from 192.168.56.11 to 10.30.30.3 can be seen in the above figure. The packet shows the original echo reply packet encapsulated in a GRE packet.

Activate the session

General OpenFlow

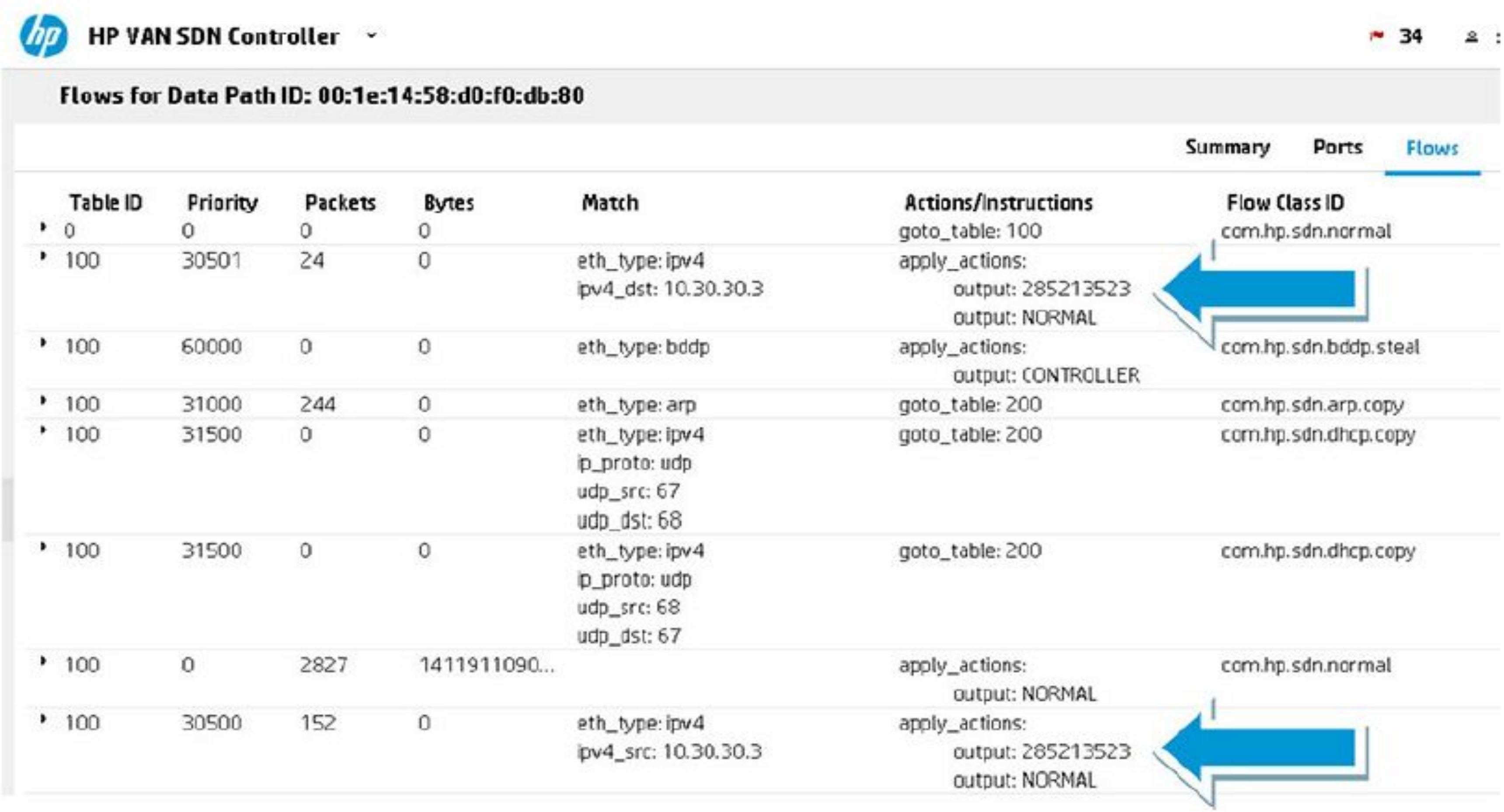
Monitor



Data Path ID	Address	Negotiated Ver...	Manufacturer	H/W Version	S/W Version
00:1e:14:58:d0:f0:db:80	10.1.1.253	1.3.0	HP	3800-24G-2SFP...	KA.15.17.0007
00:28:14:58:d0:f0:bc:80	10.1.1.254	1.3.0	HP	3800-24G-2SFP...	KA.15.17.0007

Activate the session

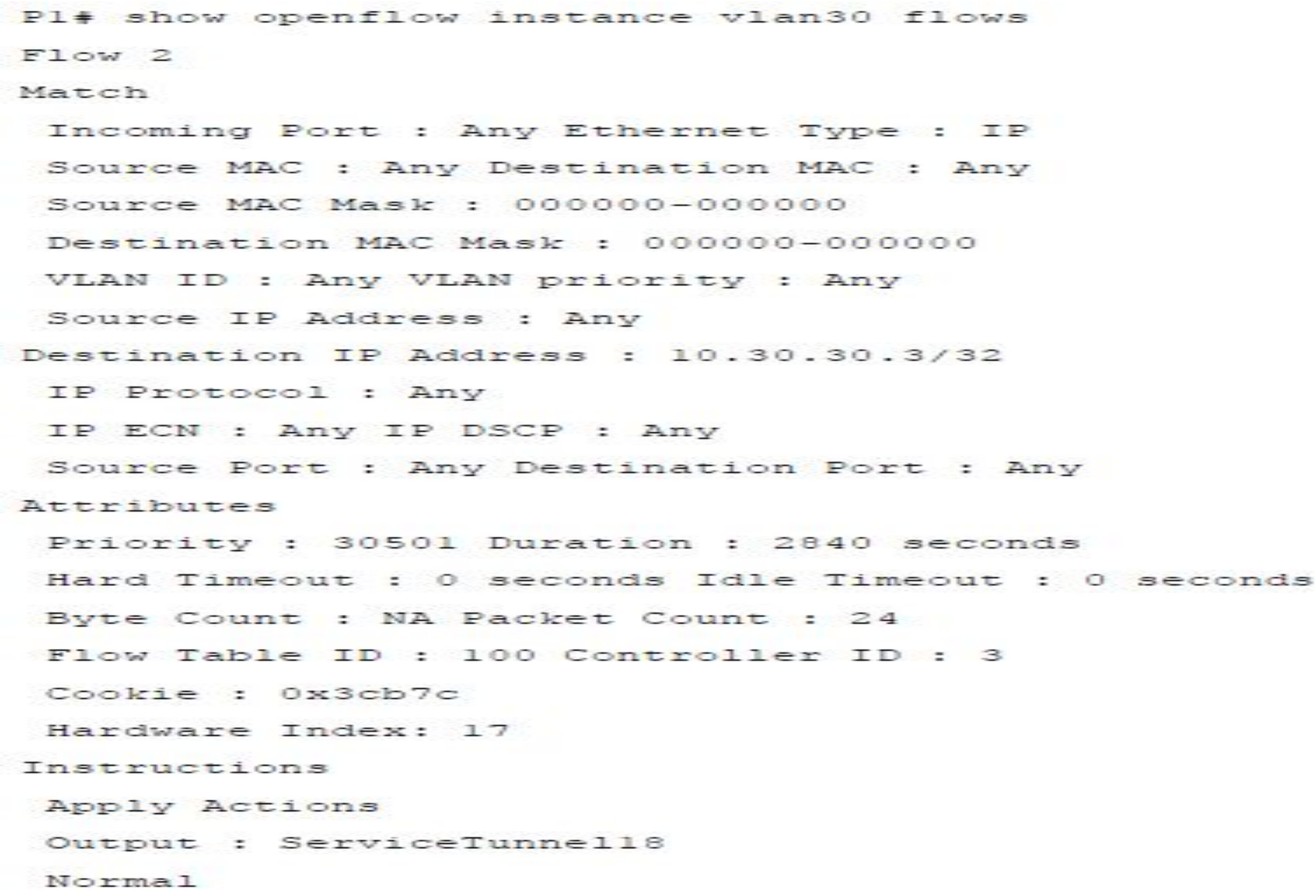
Flows



Flows for Data Path ID: 00:1e:14:58:d0:f0:db:80

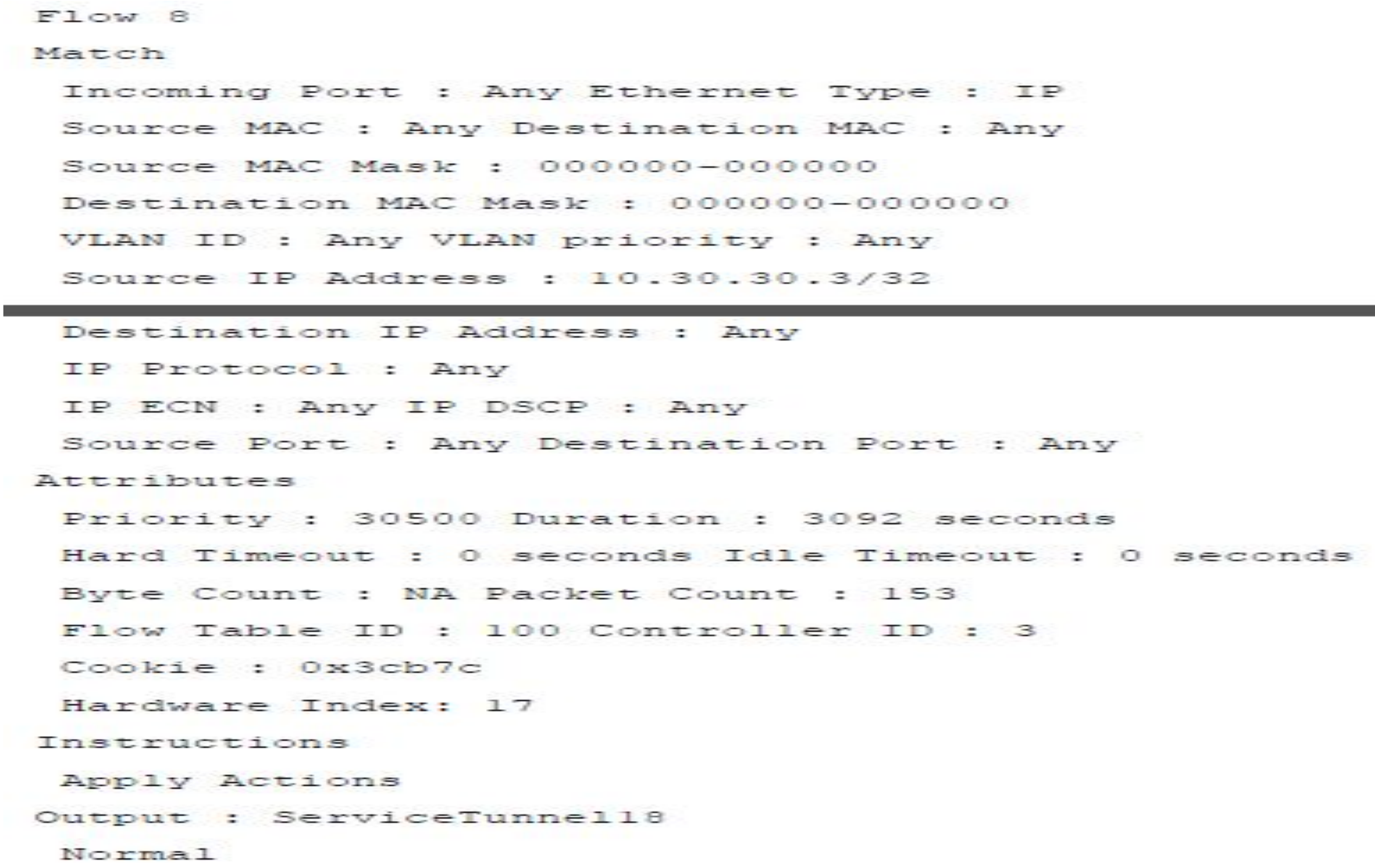
Table ID	Priority	Packets	Bytes	Match	Actions/Instructions	Flow Class ID
0	0	0	0		goto_table: 100	com.hp.sdn.normal
100	30501	24	0	eth_type: ipv4 ipv4_dst: 10.30.30.3	apply_actions: output: 285213523 output: NORMAL	
100	60000	0	0	eth_type: bddp	apply_actions: output: CONTROLLER	com.hp.sdn.bddp.steal
100	31000	244	0	eth_type: arp	goto_table: 200	com.hp.sdn.arp.copy
100	31500	0	0	eth_type: ipv4 ip_proto: udp udp_src: 67 udp_dst: 68	goto_table: 200	com.hp.sdn.dhcp.copy
100	31500	0	0	eth_type: ipv4 ip_proto: udp udp_src: 68 udp_dst: 67	goto_table: 200	com.hp.sdn.dhcp.copy
100	0	2827	1411911090...		apply_actions: output: NORMAL	com.hp.sdn.normal
100	30500	152	0	eth_type: ipv4 ipv4_src: 10.30.30.3	apply_actions: output: 285213523 output: NORMAL	

Activate the session



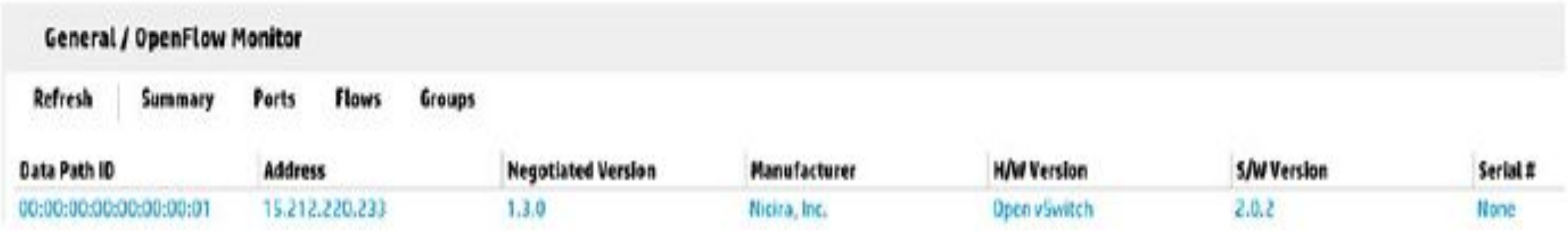
```
P1# show openflow instance vlan30 flows
Flow 2
Match
 Incoming Port : Any Ethernet Type : IP
 Source MAC : Any Destination MAC : Any
 Source MAC Mask : 000000-000000
 Destination MAC Mask : 000000-000000
 VLAN ID : Any VLAN priority : Any
 Source IP Address : Any
Destination IP Address : 10.30.30.3/32
 IP Protocol : Any
 IP ECN : Any IP DSCP : Any
 Source Port : Any Destination Port : Any
Attributes
 Priority : 30501 Duration : 2840 seconds
 Hard Timeout : 0 seconds Idle Timeout : 0 seconds
 Byte Count : NA Packet Count : 24
 Flow Table ID : 100 Controller ID : 3
 Cookie : 0x3cb7c
 Hardware Index: 17
Instructions
 Apply Actions
 Output : ServiceTunnel18
 Normal
```

Activate the session



```
Flow 8
Match
 Incoming Port : Any Ethernet Type : IP
 Source MAC : Any Destination MAC : Any
 Source MAC Mask : 000000-000000
 Destination MAC Mask : 000000-000000
 VLAN ID : Any VLAN priority : Any
 Source IP Address : 10.30.30.3/32
 Destination IP Address : Any
 IP Protocol : Any
 IP ECN : Any IP DSCP : Any
 Source Port : Any Destination Port : Any
Attributes
 Priority : 30500 Duration : 3092 seconds
 Hard Timeout : 0 seconds Idle Timeout : 0 seconds
 Byte Count : NA Packet Count : 153
 Flow Table ID : 100 Controller ID : 3
 Cookie : 0x3cb7c
 Hardware Index: 17
Instructions
 Apply Actions
Output : ServiceTunnel18
 Normal
```

Open vSwitch

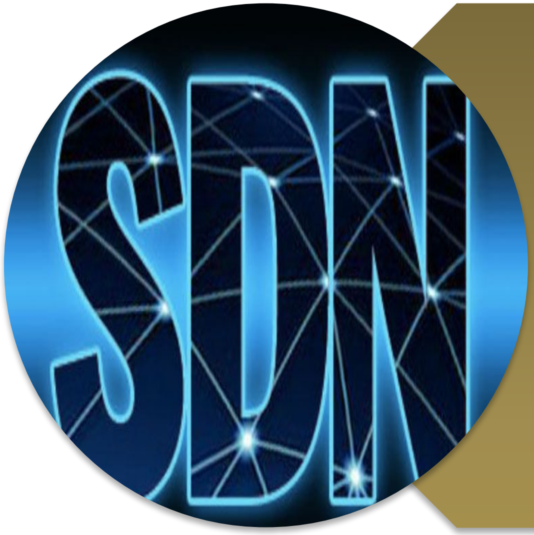


General / OpenFlow Monitor

Data Path ID	Address	Negotiated Version	Manufacturer	H/W Version	S/W Version	Serial #
00:00:00:00:00:00:00:01	15.212.220.233	1.3.0	Nicira, Inc.	Open vSwitch	2.0.2	None

OVS as a Network Device

- OpenFlow v1.3 only
- Tunnel type: GRE



HP Network Visualizer SDN

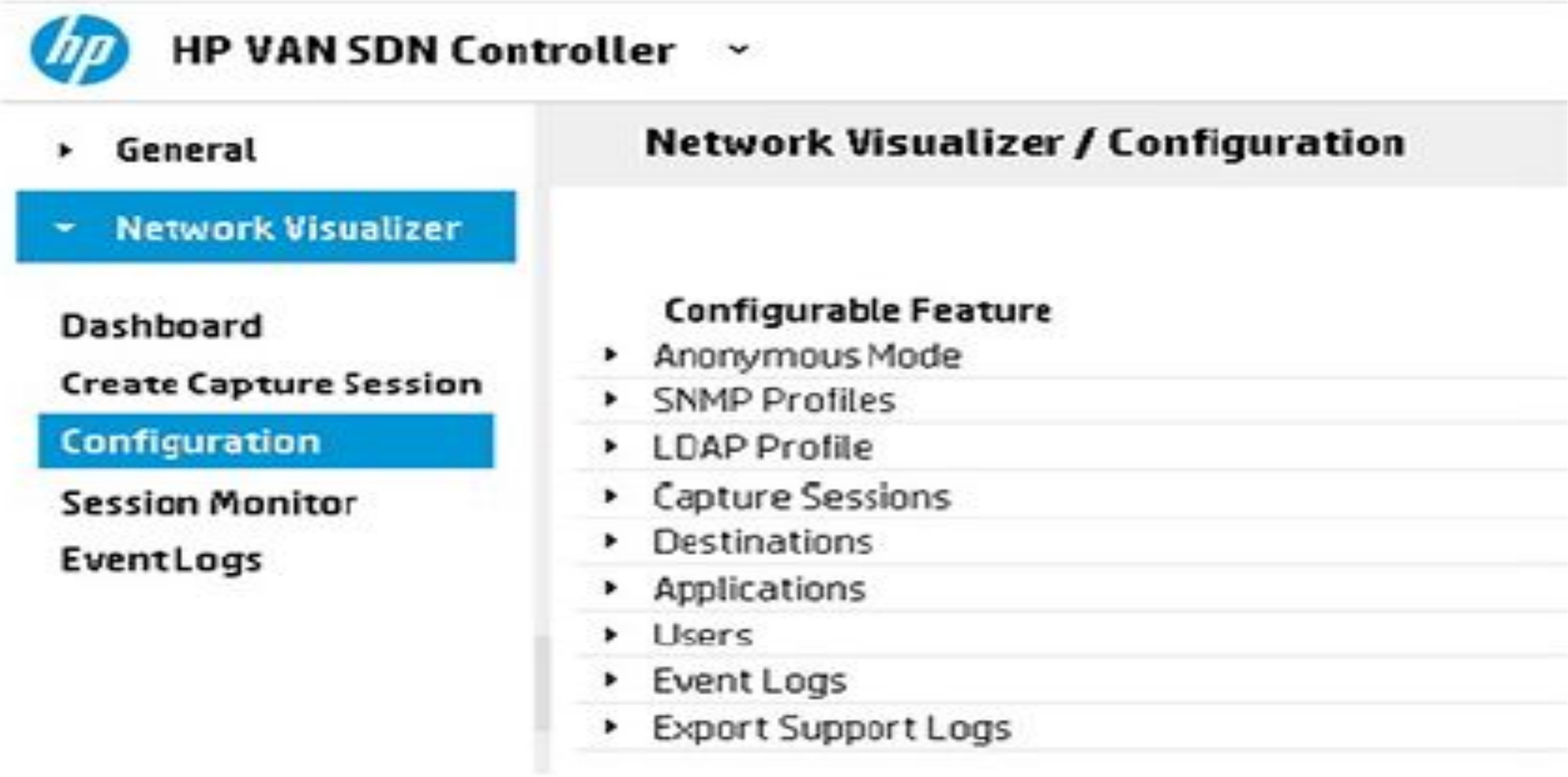
Active Directory integration

Active Directory integration

Active Directory integration

Configurations

LDAP Profile



HP VAN SDN Controller

Network Visualizer / Configuration

Configurable Feature

- Anonymous Mode
- SNMP Profiles
- LDAP Profile
- Capture Sessions
- Destinations
- Applications
- Users
- Event Logs
- Export Support Logs

Active Directory integration

LDAP Profile

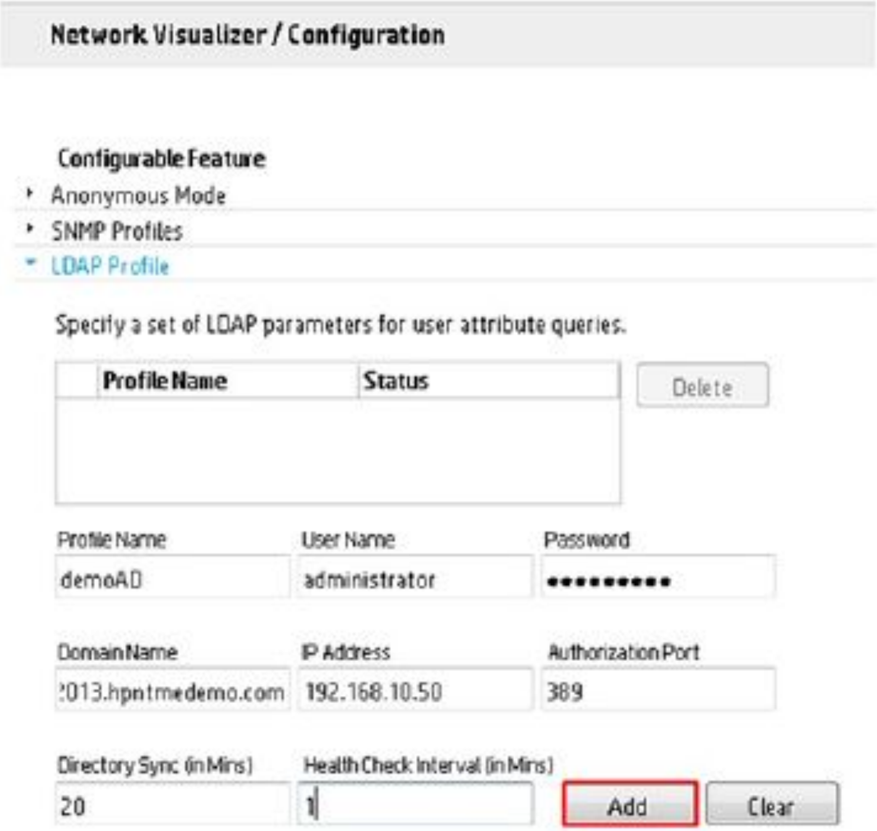
- Configuration → LDAP Profile
- Enter all fields

Enable SSH Server

- Install SSH server on Windows Server running Active Directory
- Openssh or Winssh or others

Support

- Support Windows 2008 R2, 2012, 2012 R2
- Ensure Windows Management Framework 4.0 is installed on the system



Specify a set of LDAP parameters for user attribute queries.

Profile Name	Status

Profile Name	User Name	Password
demoAD	administrator	••••••••••

Domain Name	IP Address	Authorization Port
:013.hpntmedemo.com	192.168.10.50	389

Directory Sync (in Mins)	Health Check Interval (in Mins)
20	1

Active Directory integration

- **Profile Name**: Name of the profile
- **User Name:** Active Directory account name; user must have read access to Active Directory event logs
- **Password:** Active Directory system password
- **Domain Name**: Active Directory system domain name
- **IP Address**: Active Directory system IP address
- **Authorization Port**: Port on which Active Directory is configured; default port is 389
- **Directory Sync (in Minutes):** The sync up interval to fetch user records from Active Directory
- **Health Check Interval (in Minutes):** The interval to check the health of SSH connection between Network Visualizer and Active Directory

Summary