Lecture 4



HP Network Visualizer SDN





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



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

pcap





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





			Applica	tions
🍺 HP VAN SDN CO	ontroller 🗸			≈ 621 ≙ sdn
- General	General / Applications			
Alerts	Refresh New Upgrad	e Uninstall Enable	Disable	
Applications	Name	Version	State	
Configurations	 Path Diagnostics 	2.5.15	ACTIVE	
Audit lag	 OpenFlow Link Discovery 	2.5.15	ACTIVE	
kuantog	OpenFlow Node Discovery	2.5.15	ACTIVE	
Licenses	Path Daemon	2.5.15	ACTIVE	
Team Support Logs	AppStore - Purchased Application	ns	Login to view applic	ations Launch AppStore
OpenFlow Monitor OpenFlow Topology OpenFlow Trace	Name	Version		

WARNING!

New

General / Applications					
Refresh New Upgrade	Uninstall	Enable	Disable		
Name	Version			State	
 Path Diagnostics 	2.5.15			ACTIVE	
OpenFlow Link Discove	2.5.15			ACTIVE	
 OpenFlow Node Discovery 	2.5.15			ACTIVE	
Path Daemon	2.5.15			ACTIVE	
AppStore - Purchased Applications			Lo	g in to view applications	Launch AppStore
Name	Version				

Browse	New Application	240
		Browse
		Upload
Desktop	Name: Version:	
		Deploy
SDN Lab Files Software		Cancel



hp-net-visualizer-v1.0.7-x64

com.hp.networkvisualizer_v1.0.7.1499.zip

Organize - New	folder					811 - {	•
🔆 Favorites	á	Name	-			Date modified	Type
Desktop		tom.hp.r	etworkvisualiz	er_v1.0.7.1499	9.zip	6/22/2015 6:52 AM	Compre
Downloads		Di Network-	Visualizer-Rele	ase-Notes-56		6/22/2015 1:48 AM	Adobe A
Documents	1 11						
Music							
Pictures							
Videos							
Computer							
Network		0		1010			
🙀 Network		G		-			

Upload



New Application com.hp.networkvisualizer_v1.0.7.1499.zip Browse Upload Name: Version: ID: Deploy



ACTIVE

General / Applications						
Refresh New Upgrade	Uninstall	Enable	Disable			
Name Naturali Visualiana	Version			State	1	
Network Visualizer 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			Logi	n to view app	lications	Launch AppStore
Name	Version					

Network Visualizer

e Sessions Failure
data to display
e

	General		Li	cens	es			
🍻 HP VAN SDN C	ontroller 🔹						# 27	≗ sdn
✓ General	General	/Licenses						
Alerts Applications Configurations	Refresh Install ID:	Add Ent	er License 3401		De	activate Co	opy Uninstall K	εy
AuditLog	Serial#	Product	Licensed For	Qty	Туре	Status	Expire By	Uninstall
Licenses Team SupportLogs								



- 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.

This is a confirmation of your registration with the license details: License key: BUYRMEYNO5CBO-NJTFY7S4NBTPN-YWA4QKEQZXAGB-RCUFS40BKCMKA 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:

General	General	/ Licenses						
Alerts Applications Configurations	Refresh Install ID:	Add Entr	ar License		Dea	activate Co	py Uninstall Ko	2y
AuditLog	Serial#	Product	Licensed For	Qty	Туре	Status	Expire By	Uninstall
Team SupportLogs								

Genera	l/Licenses						
Refresh	Add -yv	VA4QKEQZXAGB	RCUFS40B	KCMKA De	activate	Copy Uninstall Ke	ey.
Install ID:	6195124653	8401					
Serial#	Product	Licensed For	Qty	Туре	Status	Expire By	Uninstall

General / Licenses

Refresh

Add EnterLicense

Deactivate

Copy Uninstall Key

Install ID: 61951246538401

Serial#	- Product	Licensed For	Qty	Туре	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
- LOAP Profile
 Capture Sessions
- · Destinations

Configure destinations to capture or redirect the packets.

8	Destination Name	IP Address		State		Managed	Deli	ete
8	localAgent	192.168.56.13	3 dep	oloyed	Yes		Dep	loy
	n store blomme - 10 A	Mare	Manual	Elective (MD)	Che Caur			

	Session	Create Capture
IP VAN SDN Cont	roller ~	~ 27 s
• General	Network Visualizer / Dashboard	
Network Visualiter	Refresh	
Dashboard Create Capture Session Configuration Session Monitor Event Logs	Sessions	Capture Sessions Failure
	No data to display	No data to display

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

Relet	
SessionName	This wizard walks you through the steps for configuring the capture session. You can navigate to different steps by clicking
	on theleft panel.
technition	Session Name User VM4
aneste.	Session Mode O User * Custom
	Custom Mode : Select Protocol, Source and Destination Ports, IP/MAC Addresses
itatus	



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

sea for the Cus	tom filter criteria.
SwitchP Bidnetto	10.1.1.254
Source P Destinati	l0.40.40.4 kmP rp.1.1.1.1
Source N Destinet	MC (gr-anton minet) (mMAC (gr-anton minet)
rmany Protocal Source Pr	ALL •
itur Destinat	en Port
rtur Destinati File Nam	ion Port e /tmg

• 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

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.


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

Cneate

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"

Network Visualizer /	Create Capture Session		
neate New			
Secure Here	Swccesshilt/Configured the Session I		
Titler Parks			
Destruction	Activate -> Activates the oranized seption and navigates to Session Monitor Dane -> Navigates to Deshifts and		
Steki			
Security			
200			
		atteste	Dow

Session Monitor

Session Operational Status

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

Network Visualizer / Session Monitor Deactivate Refresh Filter Export All Create Delete Activate Session Name State Session Type Source Status **Destination Status** 1 1 ItterVMd ACTIVE UNSCHEDULED Session Name: UserVM4 Overall Status : 🕑 Bidirectional:Yes File Name Jimp/UserVM4--TIMESTAMP-.pcap Custom filter information Source P 10.48.40.4 Destination IP : 192,168,56,51 Protocol. : tcp Destination Name Latest Captur IP Address Status View lumphost 192,16856.5 Unmanaged Flow Entries Device Sic IP /Port Dst IP /Port Src Mac Dst Mac Protocol Status Time 10.1.1.254 10.40.40.4/-192.168.56.51/- top 4 2015-07-02-00... Υ. 10.1.1.254 192.168.55.51/- 10.40.40.4/top 4 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

	1	Network Visuali	zer/Session Me	nitor			
• KVissolier	ViewLates	Capture					
od	Number	Time	Source	Destination	Protocol	Leigh	anto
prove Sessi	445	2.119573	192,168,10,118	192.158.10.117	TCP	91	e-mdu = 2465 *
10	445	2.139439	192.168.10.118	192.158.10.117	TCP	893	e-mdu = 2465 =
Stat.	447	2.140419	192.168.10.117	192.158.10.118	TCP	64	24567 + e-md.
	448	2.159457	192.168.10.118	192.158.10.117	TCP	103	e-mdu > 2465
2	-649	2.159510	192.168.10.118	192.158.10.117	TCP	211	e-mdu × 2465
	450	2.160343	192,168.10.117	192.158.10.118	TCP	64	24667 > e-md
	451	2.539422	192,168,10.118	192.168.10.117	TCP	426	e-mdu > 2455
	452	2,739350	192,168,10.117	192.158.10.118	TCP	64	24667 + e-md
	453	2,945198	192,168,10,118	192.168.10.117	TCP	1289	e-mdu ≻ 2466
	454	2.945294	192,168,10.118	192.168.10.117	TCP	1289	e-mdu > 2466
	455	2.945361	192.168.10.118	192.168.10.117	TCP	1283	e-mdu > 2455
	455	2.945487	192.168.10.118	192.168.10.117	TCP	1285	e-mdu > 2466_
	457	2.945528	192,168,10.118	192.158.10.117	TCP	1283	e-mdu > 2466
	458	2.945602	192.168.10.118	192.158.10.117	TCP	1283	e-mdu = 2455
	45.9	2.905672	192.168.10.118	192.158.10.117	TCP	1283	e-mdu > 2455 *



Network Visualizer Dashboard

		Network Visualizer
HP VAN SDN Controller	r •	~ 27
> General N	letwork Visualizer / Dashboard	
 Network Visualizer 	tefresh	
Dashboard Create Capture Session Configuration Session Monitor Event Logs	Sessions	Capture Sessions Failure
	No data to display	No data to display

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



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

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

Network Visualizer

Configuration

General	Network Visualizer / Configuration
Network Visualizer	
ashboard	Configurable Feature Anonymous Mode
reate Capture Session	 SNMP Profiles
onfiguration	 LDAP Profile
ession Monitor	 Capture Sessions
ventlogs	 Destinations
venteogs	 Applications
	 Users
	 Event Logs
	 Export Support Logs



Network Visualizer / Configuration

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

	Desc	ription		Туре			Delete		
	Defaul	t SNMP key		SNMP					
							<mark>Resu</mark> Profi	<mark>lt:</mark> SNMP le is added	
Name			Туре	User Na	ame				
SNMF	Pv3Pro	ofile	snmpv3 •	sdn					1
Auth T	уре	Authenticatio	n Password - F	Privacy Ty	/pe	Privacy Password			
MD5	•			DES	•		A	td (lear

IP address: 192.168.56.13
Port number: 22
Protocol: SSH

sdn@sdnct13:~\$	ping	192.168.56.251
sdn@sdnct13:~\$	ping	10.1.1.252
sdn@sdnct13:~\$	ping	10.1.1.253
sdn@sdnct13:~\$	ping	10.1.1.254

Result:

All pings should succeed.

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#

```
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

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:

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#

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

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:

			Event Logs	
p HP VAN SDN Con	troller 🗸			≈ 2
▶ General	Network	Visualiz	er / Event Logs	
- Network Visualizer	Refresh	Fil	ter Delete	
Dashboard	Time	Level	Message	Area
Create Capture Session	today 04:46:	INFO	Network Visualizer license is installed	CONFIGURATION
	today 05:44:	INFO	Device IP 10.1.1.253 is discovered	CONFIGURATION
Configuration	today 05:46:	INFO	Device IP 10.1.1.254 is discovered	CONFIGURATION
Session Monitor				

Result:

Con	figuration	Destinations.
	 Destination Na IP address: 192 Jumphost PC) Managed = Und Click Add (see F 	me: Jumphost 168.56.5 (this is the IP address of the checked (off) Figure):



HP VAN SDN Controller ~

Network Visualizer / Configuration

Configurable Feature

Capture Sessions

Destinations

Network Visualizer

Dashboard

General

Create Capture Session

Configuration

Session Monitor

EventLogs

Configure destinations to capture or redirect the packets.

	Destination Name	IP Address		State		Managed	Dele	ete
	localAgent	192.168.56.13	dep	loyed	Yes		Dep	loy
PCI	nation Name IP &	Idress	Manamed	File Size (MR)	File Cour	1		



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

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

sion Name	Set up Custom lilter	criteria
	Switch IP	10.1.1.254
ter Policy	Bidirectional	* Yes O No
	Source IP	10.40.40.4
stination	Destination P	192 168.56.51
102.02	Source MAC	eg-aabbiceiddigeill
redute	Destination MAC	eg-aatbroddeell
non and	Protocol	TCP ·
r nin di y	Source Port	
tus.	Destination Port	
177	File Name	/tmp/UserVM4.pcap

Next

Next

Previous

- 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

The third step Destination	Jumphost
Next	



Network Visualizer / Create Capture Session

Reset					
SessionName	Select a conligured de	stination to capt	ure the packets.		
Filter Policy	Destination Jumpho	ust			
Destination					
Schedule					
Summary					
Status					
				Previous	Next

Reset				
Session Name	Set capture set	ssion schedule.		
Fiter Parcy	Schedule	No Selection		
Distriction				
Schedule				
Summery				
Status				
			Previous	Next

- 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.

Finish




Statistics Tel

Ctrl+I

Ctrl+K

Ctrl+E

Ctrl+E

Ctrl+R

Lab Network

Options

📃 📂 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	Detai



A							C			<i>c</i>	
Capture DO NOT TO	interface		Link	(-layer	headerp	rom, Mode	suspien [B] B	brute [web]		Capt	tureFilter
5000.15mm.16da 93.433.33	2010/0710		Eth	emat		disabled	262144	2			
Lab Networ	k		***	- A.S	·	· · · ·	N/500				1.
Capture on all int	erfaces mode on all	linter	laces	1							Manage Interfac
Canture Filtes	t tco port 33	12									Compile selected BPI
Table a superior		-								Second Second	
apture Files									Displa	y Options	
npture Files File							B	rowse	Display	y Options Ipdate list o	of pickets in rial time
apture Files File:			Use po	cap-ng	a format) (B	rowse	Display	y Options Ipdate list o Automatical	of pickets in stal time By scroll during live capt
npture Files File: Use <u>multiple</u> files 2 Next file every	[1	1	Use po	cap-ng	ş format) (R	rowse	Display	y Options Ipdate list o Sutomatical Side captur	of pickets in real time Ily scroll during live capt re into dialog
apture Files File Use <u>multiple</u> files Next file every Next file every	1	ar ar	V Use po megabyte minute(s)	cap-ng e(1)	g format		R	rowse]	Display	y Options Ipdate list o Sutomatical Side captur Resolution	of packets in real time By scroll during live capt re into dialog
apture Files File Use multiple files Next file every Next file every Ring buffer with	1		Use po megabyt minute(s) file:	cap-ng e(1))	g format v			rowse]	Displa 20 5 20 6 20 5 Name	y Options Ipdate list o Jutomatical gide captur Resolution Resolution	of pickets in real time illy scroll during live capt re inlo dialog .C addresses
apture Files File: Use multiple files Use tile every Next file every Ring buffer with op Capture Automat	1 1 2 ically After	an an	Vie p megabyt minute(s) file:	cap-rig e(t)	g format v		. (R	rowse	Display V S V S Name V S Name	y Options Ipdate list o Sutomatical Side captur Resolution Resolve <u>M</u> A Resolve <u>M</u> A	of pickets in real time illy scroll during live capt re into dialog C addresses work-layer names
aptuse Files File Use multiple files Use multiple files Next file every Ring buffer with top Capture Automat 1	1 1 2 ically After packet(s)		Use p megabyt minute(s) file:	cap-ng e(s))	g format v v (megaby	yte(s) =		rowse	Display	y Options Ipdate list o Automatical Side captur Resolution Resolve <u>M</u> A Resolve <u>p</u> eto Resolve <u>p</u> eto	of packets in stal time illy scroll during live capt re inlo dialog C addresses work-layer names hsport-layer name



Session Name Successfully Configured the Session I Filter Policy Activate -> Activates the created session and navigates to Session Monitor Done -> Navigates to DashBoard Schedule Summary Activate

Network Visualizer / Create Capture Session

Create New

		A HOUSE / Je	salen nomeo					
	Refresh	Fitter	Export All	Create	elete Activat	e Deact	ivate	
	Sessio	n Name S	tate	Session Type	Source Stat	tus	Destination Stat	
	BiserVM	14 A	CTIVE	UNSCHEDULED	2		~	
Session Ionitor	Session Nam Overall State Custom filter Source IP	ie: UserVM4 us : B Istormation : 10.40.40.4 : 10p	idirectional: Ves Destination IP	File Name :/ tm : 192.168.56.51	rp/UserVM4. «TIMEST	ам₽≈рсар		
	PTODOCOL							
	Destination							
	Destination	IP Address	Status		Latert Captur			
	Destination Name Jumphost	IP Address 192.168.56.5	Status Unmanaged		Latest Captur View			
	Destination Name Jumphost	IP Address 192.168.56.5	Status Unminäged		View 3			
	Protocol Destination Name Jumphost Flow Entries Device	IP Address 192.168.56.5 Src IP /Per	Status Unmanaged t Dst IP /Port	Src Mac	Latert Captur View	Protocol	Status	Tir
	Protocol Destination Name Jumphost Flow Entries Device 10.1.1.254	IP Address 192.168.56.5 Src IP /Por 10.40.40.4/-	Status Unmanaged t Dst IP /Port 192.168.56.51/-	Src Mac	Latert Captur View 3	Protocol	Status 2015-07-	Tir 0200.





Capturing from Lab Network [Wireshark 1.12.6 (v1.1	12.6-0-gee1fce6 from master-1.12)]	[
Eile Edit View Go Capture Analyze Statistics	Telephony Iools Internals Help		
• • 1 1 1 1 1 1 1 1 1 1	/ 🖗 🥥 7 👱 🗐 🗐 Q	ର୍ ଦ୍ 🖆 🖉 🕵 % 🙀	
Filter: ip.src == 10.40.40.4 ip.dst == 10.40.40.4	 Expression 	Clear Apply Save	
No. Time Source [Destination Protocol L	ength Info 112 49314-80 [SYN] Seg=0 win=8192 Lon=0 MSS=1460 WS=4	
8839 448.082423 192.168.56.5 8840 448.082573 192.168.56.51	10.1.1.254 ICMP 10.40.40.4 TCP	140 Destination unreachable (Protocol unreachable) 112 80-49314 [SYN, ACK] Seq-0 Ack-1 Win-14600 Len-0 M	MSS-1460 S.
8841 448.082593 192.168.56.5 8842 448.083375 10.40.40.4	10.1.1.254 ICMP 192.168.56.51 TCP	140 Destination unreachable (Protocol unreachable) 106 49314+80 [ACK] Seq=1 Ack=1 win=65700 Len=0	-
 Frame 8838: 112 bytes on wire (896) Ethernet II, Src: HewlettP_37:a4:97 Internet Protocol Version 4, Src: 1 	bits), 112 bytes captured ((78:48:59:37:a4:97), Dst: 0.1.1.254 (10.1.1.254), Dst	(896 bits) on interface 0 Vmware_97:28:03 (00:50:56:97:28:03) t: 192.168.56.5 (192.168.56.5)	î
■ Generic Routing Encapsulation (Tran ■ Flags and Version: 0x2000 Protocol Type: Transparent Ethern Key: 0x0000138d	sparent Ethernet bridging) et bridging (0x6558)		
Ethernet II, Src: Vmware_97:26:77 (00:50:56:97:26:77), Dst: He	ewlettP_37:a4:9f (78:48:59:37:a4:9f)	
E Internet Protocol version 4. src: 1	0.40.40.4 (10.40.40.4), DST	1: 192.168.56.51 (192.168.56.51)	
E Transmission Control Protocol, Src 1	Port: 49314 (49314), Dst Po	ort: 80 (80), seq: 0, Len: 0	
Source Port: 49314 (49314)			
Destination Port: 80 (80)			
[TCP Segment Len: 0]			
Sequence number: 0 (relative se	equence number)		10
Acknowledgment number: 0			
0000 0000 0010 = Flags: 0x00.	2 (SYN)		
window size value: 8192	an addressed b		
[Calculated window size: 8192]			
Urgent pointer: 0	piedl		

Capturing fr	om Lab Network Vireshark 1.	12.6 (v1.12.6-0-geelfce6 from n	naster-1.12)]			
<u>File Edit Vie</u>	ew 🦻 🚽 analyze 🔅	Statistics Telephony Tools	Internals <u>H</u> elp			
• • 1		् 🗢 🔿 🐼 👱		ର୍ ପ୍ 🖭 🛛 🖉	(🗹 🕵 %	H
Filter: ip.src =	= 10.40.40.4 ip.dst == 10.40.40	.4	Expression	Clear Apply Sav	e	
No. Time	Source	Destination	Protocol Le	ngth Info		
8838 448	.08237010.40.40.4	192.168.56.51	TCP	112 49314+80	[SYN] Seq=0	Win=8192 Lt
8839 448	.082423192.168.56.5	10.1.1.254	ICMP	140 Destinati	ion unreacha	ble (Protoco
		* * * * *			F	- ^ . ! ^
🖪 Frame 88	38: 112 bytes on wire	(896 bits), 112 byte	s captured (896 bits) on i	interface 0	
🕀 Ethernet	II, Src: HewlettP_37	:a4:97 (78:48:59:37:a	4:97), Dst: 4	Vmware_97:28:0	3 (00:50:56	:97:28:03)
🗄 Internet	Protocol version 4, :	Src: 10.1.1.254 (10.1	.1.254), DST	: 192.168.56.5	(192.168.5	6.5)
⊕ Generic I	Routing Encapsulation	(Transparent Etherne	t bridging)			
🕀 Ethernet	II, Src: Vmware_97:20	6:77 (00:50:56:97:26:	77), Dst: He	wlettP_37:a4:9	f (78:48:59	:37:a4:9f)
€ 802.1Q V	irtual LAN, PRI: 0, CI	FI: 0, ID: 40				
Internet	Protocol Version 4,	5rc: 10.40.40.4 (10.4	0.40.4), Dst	: 192.168.56.5	1 (192.168.	56.51)
⊕ Transmiss	sion Control Protocol	, Src Port: 49314 (49	314), Dst Po	rt: 80 (80), s	Seq: 0, Len:	0

- 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

2								
1	*Lab Network	[Wireshark1.12.6	(v1.12.6-0-geelfce	from master-1.12)]				
Elle	<u>E</u> dit <u>V</u> iew	<u>G</u> o <u>C</u> apture	Analyze Statistics	Telephony <u>T</u> oo	is Internais <u>H</u> elp			
0	0 🥻 🔳	1 1 1 1 1	X 2 🔍	Þ 🔿 🖗 🕯		ର୍ ପ୍ 🗹	🖗 🗹 🕵 %	
Filt	er: ip.src ==	10.40.40.4 ip.dst	== 10.40.40.4		Expression	. Clear Apply	Save	
No.	Time	Source		Destination	Protocol I	ength Info		
	8838 448.0	08237010.40.	40.4	192.168.56.51	TCP	112 49314	+80 [SYN] Seq=	0 win=8192 Len=0
	8839 448.(082423 192.10	58.56.5	10.1.1.254	ICMP	140 Desti	nation unreach	able (Protocol u
				** ** ** *		*** ** **		
Ð.	Frame 8838	3: 112 bytes	on wire (896	bits), 112 by	tes captured	(896 bits)	on interface 0	
1	Ethernet I	I, Src: Hew	lettP_37:a4:97	(78:48:59:37	:a4:97), Dst:	Vmware_97:	28:03 (00:50:5	6:97:28:03)
Đ.	Internet P	Protocol Ver	sion 4, Src: 1	0.1.1.254 (10	.1.1.254), DS	t: 192.168.	56.5 (192.168.	56.5)
) (II	Seneric Ro	outing Encap	sulation (Tra	sparent Ether	net bridaina)		•	
E I	Thernet I	T. Src: Vmw	are 97:26:77	00:50:56:97:2	6:77). Dst: H	ewlettp 37:	a4:9f (78:48:5	9:37:a4:9f)
	802 10 vir	TUALION P	DT: 0 CET: 0	TD: 40	•••••			
	Jos connet	cuar LAN, P	rion (cree (0 10 10 1 (1/	10 10 10 00	. 103 160	56 51 (100 160	56 51)
±.	internet F	rotocol ver	sion 4, Src: .	.0.40.40.4 (10	.40.40.4), DS	t: 192.108.	50.51 (192.108	. 30. 31)
•	Fransmissi	ion Control	Protocol, Src	Port: 49314 (49314), Dst P	ort: 80 (80), Seq: 0, Len	: 0

Op	OpenFlow Monitor						General			
HP VAN SDN Co	ntroller • General /	OpenFlow	w Monitor				* 3	¶ ≗ sdn		
denerov	Refresh	Summary	Ports	Flows	Groups					
Alerts	New York	Seminary	Ports	1.045	aloups					
Applications	Data Path ID		Address	Negotiate	Manufacturer	H/W Version	S/W Version	Serial #		
Configurations	00:1e:14:58:d0):f0:db:80	10.1.1.253	1.3.0	HP	3800-24G-25F	KA.15.17.0007	SG49G0V430		
AuditLog	00:28:14:58:d0	0:f0:bc:80	10.1.1.254	1.3.0	HP	3800-246-25F	KA. 15. 17.0007	SG49G0V437		
Licenses										
Team										

OpenFlow Monitor

Flows

	Flows for Data Path ID: 00:28:14:58:d0:f0:bc:80								
						Summary	Ports	Flows	
,	Table ID O	Priority O	Packets 0	Bytes O	Match	Actions/Instructions goto_table: 100	Flow Class com.hp.sdn	ID .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:

Normal

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 TP 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
```

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

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

*Lab Network [Wireshark 1.12.6 (v1.12.6-0-geelfce6 from master-1.12)]	
Eile Edit View Go Capture Analyze Statistics Telephony Tools	internals Help
● ● ◢ ■ ◢ ⊨ ≧ ೫ ₴ < ↔ ⇔ ∞ 7 높	■ 🕞 🍳 Q, Q, 🖸 🚆 🗹 🥵 🔆 🚆
Filter: http && ip.src == 10.40.40.4 ip.dst == 10.40.40.4	Expression Clear Apply Save
No. Time Source Destination 8843 448.083376 10.40.40.4 192.168.56.51 8845 448.083410 192.168.56.51 10.1.1.254	Protocol Length Info HTTP 501 GET / HTTP/1.1
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 8850 448.102100 10.40.40.4 192.168.56.51	ICMP \$77 Destination unreachable (Protocol unreachable) HTTP 524 GET /images/sdn.png HTTP/1.1
 Ethernet II, Src: HewlettP_37:a4:97 (78:48:59:37:a Internet Protocol Version 4, Src: 10.1.1.254 (10.1 Generic Routing Encapsulation (Transparent Etherne Ethernet II, Src: Vmware_97:26:77 (00:50:56:97:26: 802.10 Virtual LAN, PRI: 0, CFI: 0, ID: 40 Internet Protocol Version 4, Src: 10.40.40.4 (10.4 Transmission Control Protocol. Src Port: 49314 (49 Hypertext Transfer Protocol GET / HTTP/1.1\r\n 	4:97), Dst: Vmware_97:28:03 (00:50:56:97:28:03) .1.254), Dst: 192.168.56.5 (192.168.56.5) t bridging) 77), Dst: HewlettP_37:a4:9f (78:48:59:37:a4:9f) 0.40.4), Dst: 192.168.56.51 (192.168.56.51) 314), Dst Port: 80 (80), Seq: 1. Ack: 1. Len: 401
Accept: image/jpeg, application/x-ms-application Accept-Language: en-us\r\n User-Agent: Nozilla/4.0 (compatible; MSIE 8.0; W Accept-Encoding: gzip, deflate\r\n Host: hp.com\r\n Connection: Keep-Alive\r\n \r\n <u>[Full request URI: http://hp.com/]</u> [HTTP request 1/8] <u>[Next request in frame: 8845]</u>	i, image/gif, application/xaml+xml, image/pjpeg, application/x-ms-xbap, */*\r\r

📕 "La	b Network	[Wireshark 1.12.6 (v1.12.6-0-g	ee1fce6 from master-1.12)]			
Eile	Edit View	w <u>Go C</u> apture <u>A</u> nalyze <u>S</u>	tatistics Telephony <u>T</u> ools	Internals <u>H</u> elp	o	
•	• 🧉 🗖	I 🙇 🗁 🛅 💥 😂 🛛	् 🗢 🗢 😜 🔆 🕹		Q Q 🖸 📓 🖻 🧏 % 📴	
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	
88	\$43 448.	08337610.40.40.4	192.168.56.51	HTTP	501 GET / HTTP/1.1	
88	45 448.	083410192.168.56.5	10.1.1.254	ICNP	S49 HTTP /1 1 300 OK (text/html)	nreachable)
88	40 440.	084713192.168.56.5	10 1 1 254	TENP	577 Destination unreachable (Protocol u	preachable)
88	350 448.	102100 10.40.40.4	192.168.56.51	HTTP	524 GET /images/sdn.png HTTP/1.1	
	Content Keep-Al Content Content (r\n [HTTP ro [Time s [Prev ro [Request [Next ro Content ne-base	-Length: 177\r\n ive: timeout=5, max=1 ion: Keep-Alive\r\n -Type: text/html\r\n esponse 2/8] ince request: 0.00128 equest in frame: 88431 esponse in frame: 884 -encoded entity body d text data: text/htm	00\r\n 3000 seconds]] 9] (gzip): 177 bytes ->	225 bytes		
	docty</td <td>pe html>\r\n</td> <td></td> <td></td> <td></td> <td></td>	pe html>\r\n				
	<ntml>\</ntml>	r\n				
	-meta cl	harset="utf-8">\r\n				
	<title>:</title>	SDN Networking <td>>/r/n</td> <td></td> <td></td> <td></td>	>/r/n			
	<style></style>					

Deactivate

General	Network V	sualizer / S	ession Monitor					1
Network Visualiter	Refresh	Filter	Export All	(reate	Delete	Activate	Deactivate	
Jashboard	Session Na	me	State		Session Type		Source Status	Destination Status
reate Capture Session onfiguration	UserVM4		ACTIVE		UNSCHEDULED		V	~
ession Manitor								
event Logs								

	Session Name	Create Capture Session UserVM3
	Session Mode	Next
Network Visualize	er/Create Capture Session	
Reset		
Session Name	This wizard walks you through the steps for	conliguring the capture session. You can navigate to
Session Name	This wizard walks you through the steps for different steps by clicking on the left panel.	configuring the capture session. You can navigate to
Session Name Fiter Policy Destination	This wizard walks you through the steps for different steps by clicking on the left panel. Session Name User VM3 Session Mode OUser Custom	conliguring the capture session. You can navigate to
Session Name Fiter Policy Destination Schedule	This wizard walks you through the steps for different steps by clicking on the left panel. Session Name User VM3 Session Mode OUser Oustom	configuring the capture session. You can navigate to
Session Name Fiter Policy Destination Schedule Summary	This wizard walks you through the steps for different steps by clicking on the left panel. Session Name User VM3 Session Mode © User ® Custom Custom Mode : Select Protocol, Source and R	conliguring the capture session. You can navigate to Destination Ports, IP/MAC Addresses

- 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

	Switch IP	10.1.1.253	•	
Iter Policy	Bidirectional	Yes	O No	
concerne:	Source IP	10.30.30.3		
Destination	Destination IP	eg- 1.1.1.1		
and the second second	Source MAC	egaarbb:c	cidd:ee:tt	
suiconie	Destination MAC	eg - aa:bb:c	c:dd:ee:ff	
	Protocol	ALL	-)	
sammery	Source Port			
Status	Destination Port			
	File Name	/tmp/UserW	M3.pcap	

Destination Jumphost

Peret				
SessionName				
	Select a conf	igured destination to	capture the packets.	
Filter Policy	Destination	Jumphost	•	
Destination				
Schedule				
Summary				
Status				

Next

No Selection

Next

Reset				
Session Name	Set capture se	ssion schedule.		
Fater Policy	Schedule	NoSelection	•	
Destination				
Schedule				
Summary				
Status				

Finish



Activate

Network V	isualizer / Create Capture Session
Create New	
Session North	Successfully Configured the Session I
Filter Policy	
Destination	Activate -> Activates the created session and navigates to Session Monitor Done -> Novigates to DoshBoard
Schedule	
Summary	
Searce	
	Activate Done

Session Monitor

Session Na			creace D	elete Acti	vate D	eactivate		
	me	State	Session	Type	Source St	atus	Destination S	itatus
UserVM3		ACTIVE	UNSCHED	ULED	~		~	
UserVM4		INACTIVE	UNSCHED	ULED	*		*	
Session Name: U Overall Status : Custom filter Info Source IP : 10	JserVM3 Bormation 130.30.3	idirectional: Yes	File Name : / tr	np/UserVM3- <tim< th=""><th>STAMP>.pca</th><th>p</th><th></th><th></th></tim<>	STAMP>.pca	p		
restination		Status		Latest Captu	r			
Name	IP Address	200002						
Name Jumphost 1	IP Address 92.168.56.5	Unmanaged		View				
Name Jumphost 1	IP Address 92.168.56.5	Unmanaged		View				

<u>File Edit Virw</u>	Go Gapture	Analyze Statistics	Telephony Tools	Internals <u>H</u> elp	
• • •		× 2 9, ¢	• 🔿 🖓 🛃		ର୍ ଭ୍ 🖭 🛛 🖉
	tart a new live cap	ture			

Continue without Saving

~	before starting a new capture?
	Your captured packets will be lost if you don't save them.
	Save <u>Cancel</u> Continue without Saving



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

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>

Stop

icmp

🚄 *Lab Network	[Wireshark 1.12.6 (v1.12.6	0-gee1fce6 from master-1.12)]				
<u>File Edit View</u>	<u>Go</u> <u>C</u> apture <u>A</u> nalyze	Statistics Telephony Tools	Internals <u>H</u> elp			
• • 4 =	1 * 2	1		Q Q 🗹	🙀 🗹 🐔	* 🖬
Filter: icmp			Expression	Clear Apply	Save	
No. Time	Source	Destination	Protocol L	ength Info		
19 7.101	99400 192.168.56.5	10.1.1.253	ICMP	151 Desti	ination unrea	achable (Prote
20 7.466	1/00010.30.30.3	192.168.56.11	ICMP	120 ECN0	(ping) reque	est 1d=0x0001
21 7.400	22800 192.108.50.5	1 10.20.20.3	ICMP	130 Echo	(ning) conly	achable (Proce
22 7.400	47400 192.108.50.1	10.1.1.253	ICMP	1/8 Dest	(ping) repis	
23 7.400	4320010 30 30 3	192 168 56 11	TCMP	120 Echo	(ning) ceque	st id-0x0001
25 8,481	43500 192,168,56,1	1 10.30.30.3	TCMP	120 Echo	(ping) reque	/ id=0x0001
		(060 bits) 270 b tos	constructed (06		Cpingy repri	
 Ethernet II Internet Pi Generic Roi Ethernet II 802.1Q Viri Internet Pi Internet Control Type: 8 Code: 0 Checksum Identificities Sequence Sequence Fresponse Data (32) 	I, Src: HewlettP_1 rotocol Version 4 uting Encapsulatio I, Src: Vmware_97 tual LAN, PRI: 0, rotocol Version 4 ontrol Message Pro (Echo (ping) reque : 0x4d45 [correct] er (BE): 1 (0x000 er (LE): 256 (0x00 number (BE): 22 o number (BE): 22 o number (LE): 5632 e frame: 221 bytes)	58:6d:d0 (78:48:59:58: , src: 10.1.1.253 (10.7 on (Transparent Ethern :26:de (00:50:56:97:26 CFI: 0, ID: 30 , src: 10.30.30.3 (10. otocol est) [L) L00) (0×0016) 2 (0×1600)	6d:d0), Dst: 1.1.253), Dst et bridging) :de), Dst: He 30.30.3), Dst	vmware_97: : 192.168. wlettP_58: : 192.168.	29:41 (00:50 56.5 (192.10 6d:ee (78:48 56.11 (192.1	0:56:97:29:41 58.56.5) 3:59:58:6d:ee 168.56.11)

ICMP message

🚄 *Lab Network	[Wireshark 1.12.6 (v1.12.6-0-ge	eelfce6 from master-1.12)]					
Eile Edit View	<u>Go</u> <u>C</u> apture <u>Analyze</u> <u>S</u> t	atistics Telephony <u>T</u> ools [nternals <u>H</u> elp)			
004		् 🗢 🗢 🕹 😨 🗌			1 🏼 🖻	0 🍢 🐝	
Filter: icmp			Expression	. Clear Apply	Save		
No. Time	Source	Destination	Protocol	Length Info			
20 7 466	1700010 20 20 2	107 168 56 11	TCMP	131 Desti	(ning)	unreacha	id-0x0001
21.7.466	22800 192, 168, 56, 5	10.1.1.253	TCMP	148 Desti	nation	unreacha	able (Protoco
22 7.466	47400 192.168.56.11	10.30.30.3	ICMP	120 Echo	(ping)	reply	id=0x0001,
23 7.466	49700 192.168.56.5	10.1.1.253	ICMP	148 Desti	nation	unreacha	able (Protoco
24 8.481	4320010.30.30.3	192.168.56.11	ICMP	120 Echo	(ping)	request	id=0x0001,
25 8.481	43500 192.168.56.11	10.30.30.3	ICMP	120 Echo	(pinq)	reply	id=0x0001,
 Ethernet I Internet P Generic Ro Ethernet I 802.1Q Vir Internet P Internet P Internet C Type: 8 Code: 0 Checksum Identific Identific Sequence Sequence <u>Frespons</u> Data (32) 	I, Src: HewlettP_58:0 rotocol Version 4, Sr uting Encapsulation 0 I, Src: Vmware_97:26 tual LAN, PRI: 0, CF rotocol Version 4, Sr ontrol Message Protoc (Echo (ping) request) : 0x4d45 [correct] er (BE): 1 (0x0001) er (LE): 256 (0x0100) number (BE): 22 (0x0 number (BE): 22 (0x0 number (LE): 5632 (0 e frame: 221 bytes)	6d:d0 (78:48:59:58:6d c: 10.1.1.253 (10.1. (Transparent Ethernet :de (00:50:56:97:26:d I: 0, ID: 30 c: 10.30.30.3 (10.30 col) 0016) 0x1600)	:d0), Dst: 1.253), Ds bridging) e), Dst: H .30.3), Ds	Vinware_97: t: 192.168. ewlettP_58: t: 192.168.	29:41 56.5 (: 6d:ee 56.11	(00:50:56 192.168.5 (78:48:59 (192.168.	56.11)

- 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

4 *La	b Network	(Wireshark 1.12	.6 (v1.12.6-0	0-geelfceó f	rom master-1	12)]						
Eile	Edit View	Go Capture	Analyze	Statistics	Telephony	Tools Inter	nals <u>H</u> e	elp				
•	• 🔺 🔳	Ø 🖻 🕻		Q @	🔿 🔕 🗿	· 👱 🔳		€ Q (Q 🗹		2 🥵 %	
Filter:	icmp					-	xpressio	n Clear	Apply	/ Save		
No.	Time	Source		D	estination		Protocol	I Length	Info			
	19 7.101	99400 192.1	108.56.5	1	0.1.1.253		ICMP	151	Dest	ination	unreacr	hable (Protoc
	20 7.466	1700010.30	0.30.3	1	92.168.56	. 11	ICMP	120	Echo	(ping)	request	: 1d=0x0001,
	21 7.466	22800 192.1	60 66 11	4	0.20.20.2		TCMP	148	Dest	That ton	unreach	able (Protoc
	23 7 466	49700 192.1	68 56 5		0 1 1 253		TCMP	148	Dest	ination	upreach	hable (Proto
	24 8,481	4320010.30	0.30.3	1	92,168,56	.11	TCMP	120	Echo	(ping)	request	id=0x0001.
	25 8.481	43500 192.1	68, 56, 11	1 1	0.30.30.3		TCMP	120	Echo	(ping)	reply	id=0x0001
 € Ge € Et € 80 € In 	neric Ro hernet I 2.10 Vir ternet P	uting Encap I, Src: Hew tual LAN, P rotocol Ver	psulatio wlettP_5 PRI: 0, o rsion 4,	n (Trans 8:6d:ee CFI: 0, Src: 19	parent Et (78:48:59 ID: 30 2.168.56.	hernet br :58:6d:ea 11 (192.1	idging), Ds1 68.56	g) t: Vmwar .11), Ds	e_97	:26:de 0.30.30	(00:50:5 .3 (10.3	6:97:26:de)
🖃 In	ternet C	ontrol Mess	sage Pro	tocol								
	Type: 0 Code: 0 Checksum Identifi Identifi Sequence Sequence	(Echo (ping er (BE): 1 er (LE): 2 number (BE number (LE	g) reply correct] (0x0001 56 (0x01 E): 22 (E): 5632) 00) 0×0016) (0×1600	Res to 1 pac	sult: An 10.30.30 cket sho	echo .3 car ws the	reply m n be seo e origin	nessa en in nal eo	nge fro 1 the al 2 cho rej	m 192.1 bove fig oly pack	168.56.11 jure. The cet

Monitor			Gen	eral	Ор	enFlow
p HP VAN SDN Contr	oller -					~
- General	General / OpenFlo	w Monitor				
Alerts	Refresh Summary	Ports	Flows Grou	ups		
Applications	Data Path ID	Address	Negotiated Ver	Manufacturer	H/W Version	S/W Version
Configurations	00:1e:14:58:d0:f0:db:80	10.1.1.253	1.3.0	HP	3800-24G-25FP	KA.15.17.0007
Audit Log	00:28:14:58:d0:f0:bc:80	10.1.1.254	1.3.0	HP	3800-24G-25FP	KA.15.17.0007
Licenses						
Support Logs						
OpenFlow Monitor						
OpenFlow Topology						

Flows



HP VAN SDN Controller

■ 34 ≗:

Flows

Summarv

Ports

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

							-
,	Table ID 0	Priority 0	Packets 0	Bytes 0	Match	Actions/Instructions goto_table: 100	Flow Class ID 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	

Pl# 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 : Anv 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

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													
Refresh	Summary	Ports	Flows	Groups									
Data Path ID		Address			Negotiated Version	Manufacturer	H/W Version	S/W Version	Serial #				
00:00:00:00:	00:00:00:01	15.212	1220.233		1.3.0	Nicira, Inc.	Open vSwitch	5.0.5	None				

OVS as a Network Device

- OpenFlow v1.3 only
- Tunnel type: GRE


HP Network Visualizer SDN







Configurations LDAP Profile



HP VAN SDN Controller ~

General

Network Visualizer / Configuration

Network Visualizer

Dashboard

Create Capture Session

Configuration

Session Monitor

EventLogs

Configurable Feature

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

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

Network Visualizer / Configuration

Configurable Feature

- Anonymous Mode
- SNMP Profiles
- LDAP Profile

Specify a set of LOAP parameters for user attribute queries.

Profile Name	Status		Delete
Profile Name	User Name	Password	
demoAD	administrator		
DomainName	IP Address	Authorization Port	
013.hpntmedemo.com	192.168.10.50	389	
Directory Sync (in Mins)	Health Check Interval (in Mins)	
20	1	Add	Clear

- 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



