SOFT inBOX

vDiff User Guide

Versioning

- Document version: v6.0.0-pre06.
- For software version v6.0.x.

SOFT inBOX

Basic Applications

- Switching.
- Routing.
- L4 filtering (firewall).
- L4 routing.

SOFT inBOX

Advanced Applications

- L4 switching (i.e., load balancing and fault tolerance) for AP servers.
- L4 switching for WAN routers, i.e., outbound WAN load balancing.

vDiff Models

Model	VDA100	VDA200	VDA300	VDA400
Max connections	1M	2M	4M	8M
Max targets	5	20	100	1000
RAM requirement	2G	4G	8G	16G
Compatible hypervisors	VMware ESXi, MS Hyper-V, Xen.			

SOFT inBOX

User Interfaces

- Web UI
  - https://192.168.1.99/
  - http://192.168.1.99/
- CLI
  - telnet 192.168.1.99
  - ssh 192.168.1.99
  - virtual machine console

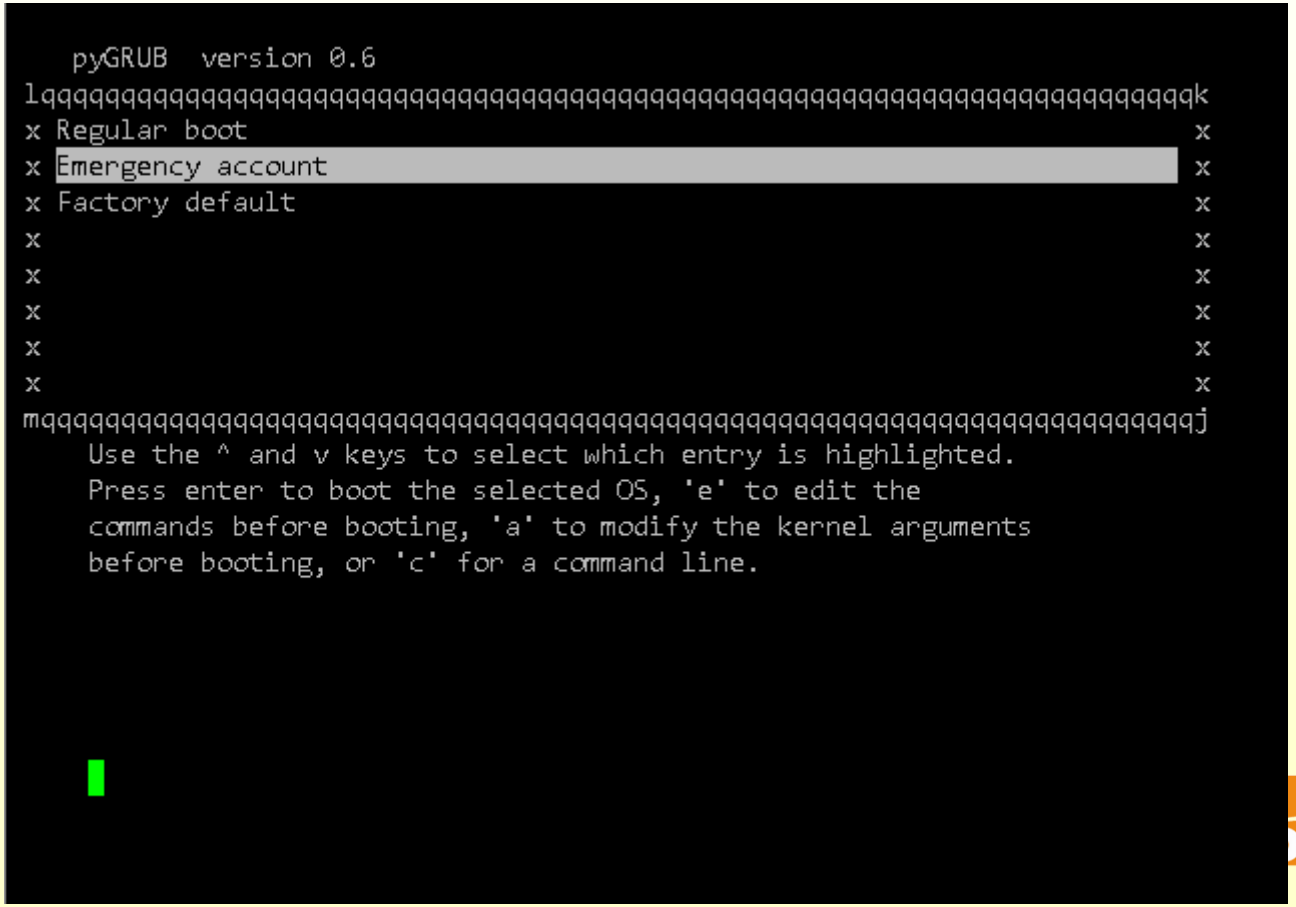
SOFT inBOX

Defaults

- Management IP：192.168.1.99/24,
- One bridge, bridge_1. The first Ethernet port, e1, is on bridge_1.
- Console is always on, https and ssh are on, http and telnet are off
- One account with username/password = admin/admin.

Emergency Account

- Select “Emergency account” on the boot menu on the console.



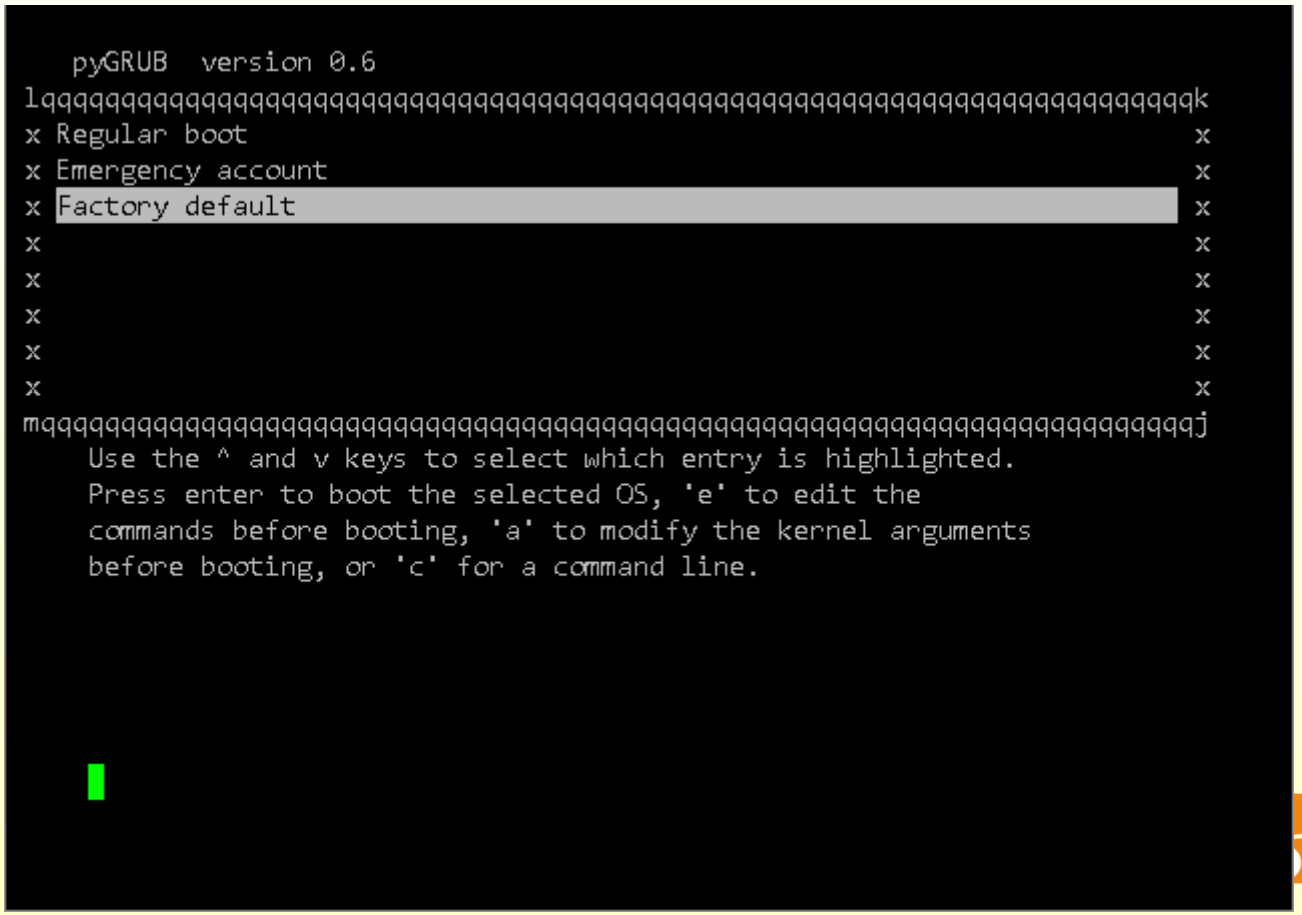
Emergency Account

- Login with username = emergency and password = emergency during the initial 30 seconds the system is booted.
- Useful commands:
  - get all (show the current configuration)
  - save config from default to system (restore the default configuration)
  - get ip
  - get route
  - get dns
  - get account

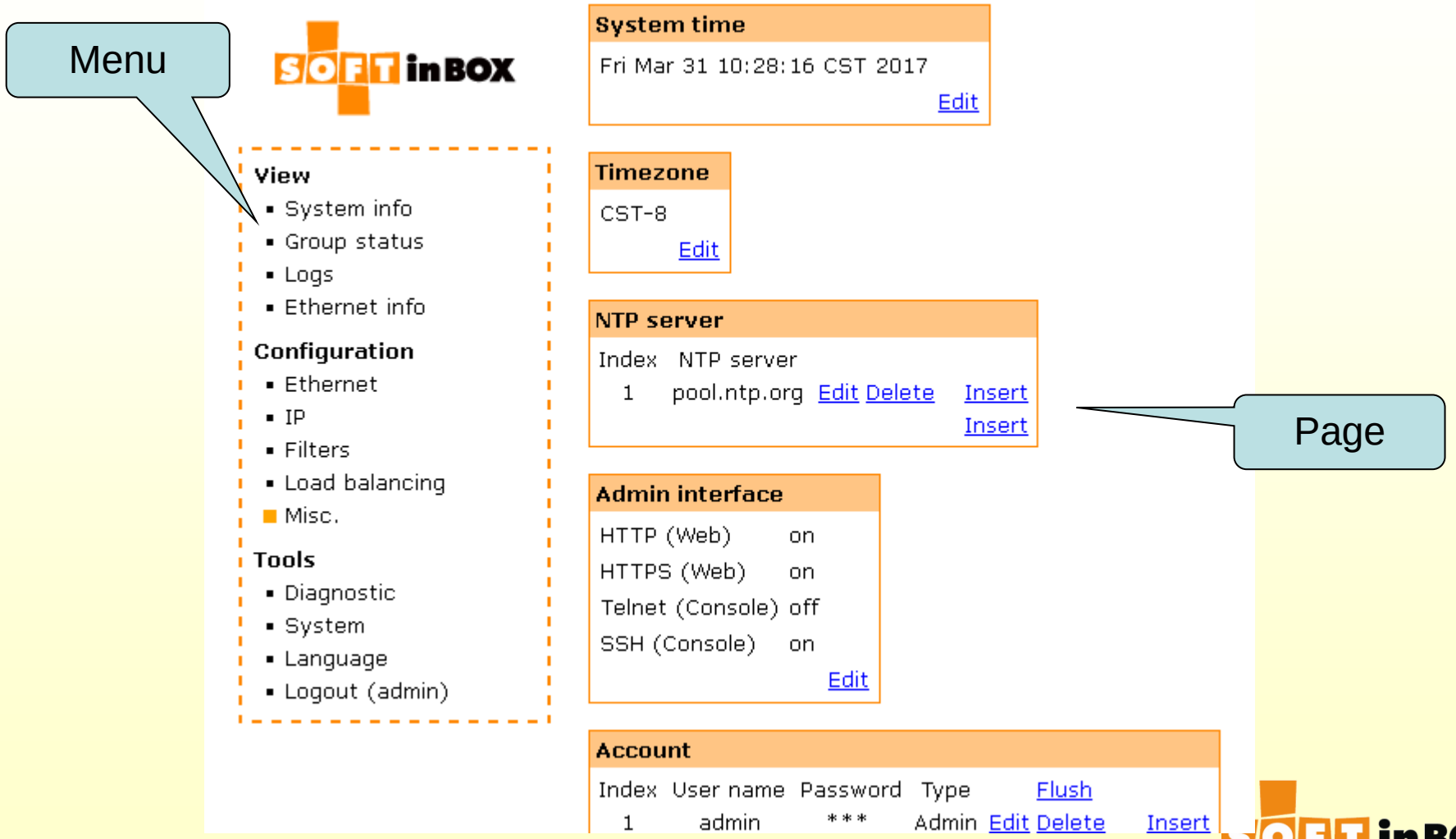
SOFT inBOX

Restore Factory Defaults

- Select “Factory default” on the boot menu.



Web UI Layout



Command Line Interface (CLI)

SOFT inBOX

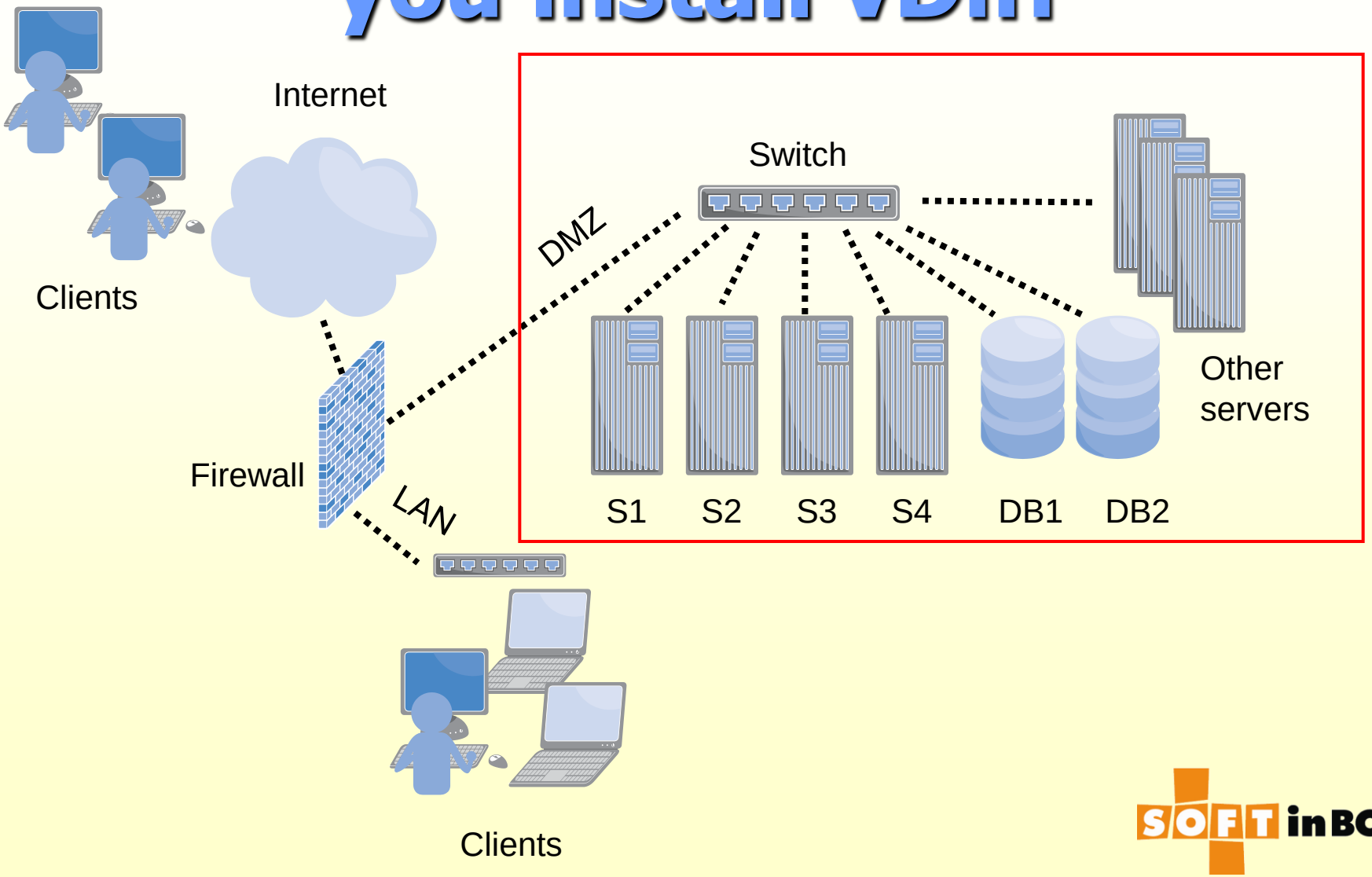
CLI Editing Keys

Key name	Function
Control-A	Jump to the front of the command.
Control-B or LEFT	Move the cursor backward one character.
Control-C	Cancel the command.
Control-D or DELETE	Delete the character on the cursor.
Control-E	Jump to the end of the command.
Control-F or RIGHT	Move forward one character.
Control-H or Backspace	Delete the character on the left of the cursor.
Control-P or UP	Browse the previous command in the history buffer.
Control-N or DOWN	Browse the next command in the history buffer.
Control-R	Clear the screen.
TAB	Help.
Enter	Execute the command.

CLI Usage

- get ip
- set ip append ipmask 192.168.1.99/24 bridge bridge_1
- If you see error messages, the command failed. Correct the command and try again.
- Otherwise (no error message), the command is applied successfully, and new configuration is saved.

Network topology before you install vDiff



SOFT inBOX

Basic Networking models for AP load balancing

- Transparent bridge mode
- VIP bridge mode
- Single-arm mode
- VIP router mode
- FW mode

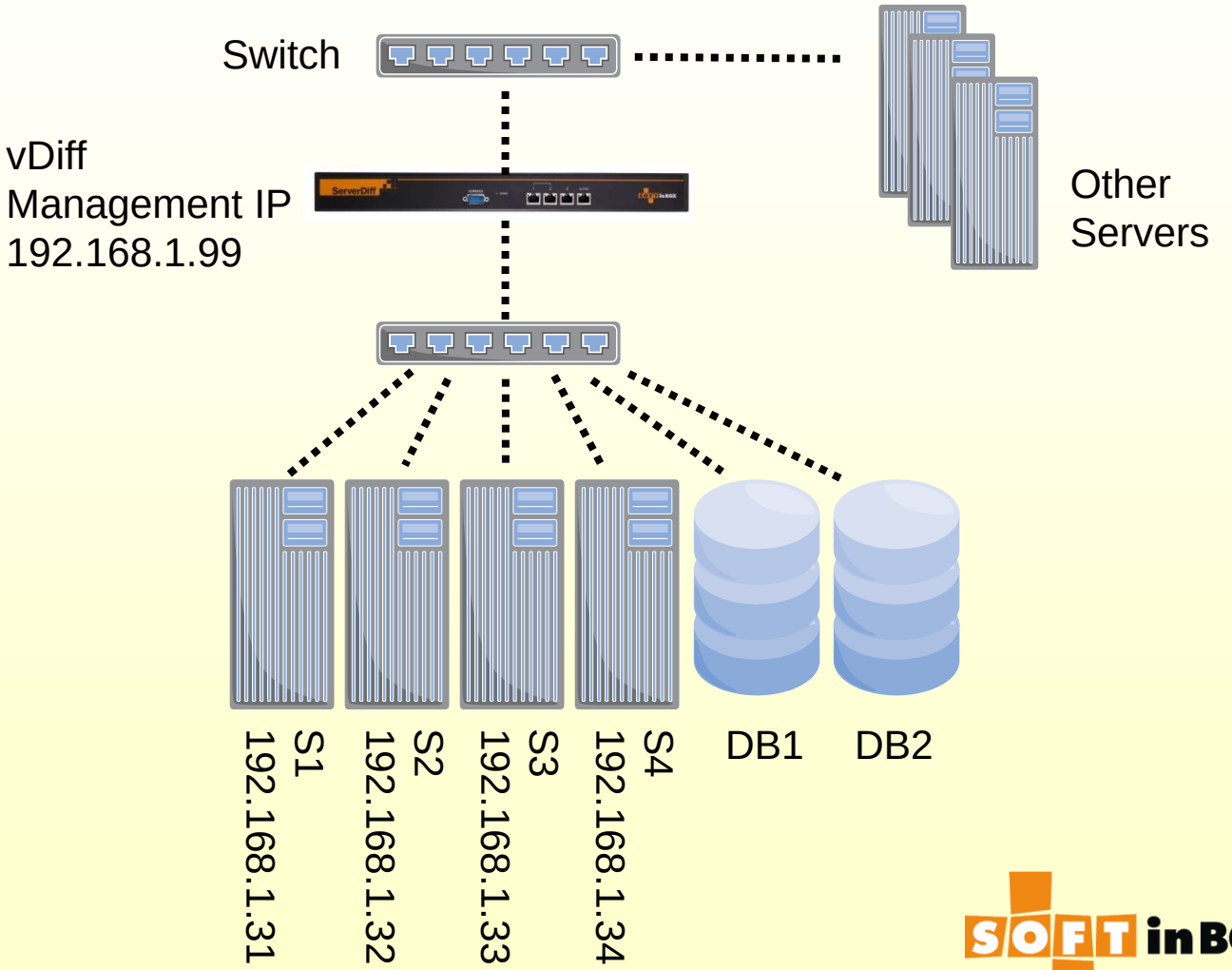
SOFT inBOX

Mode 1: Transparent Bridge Mode

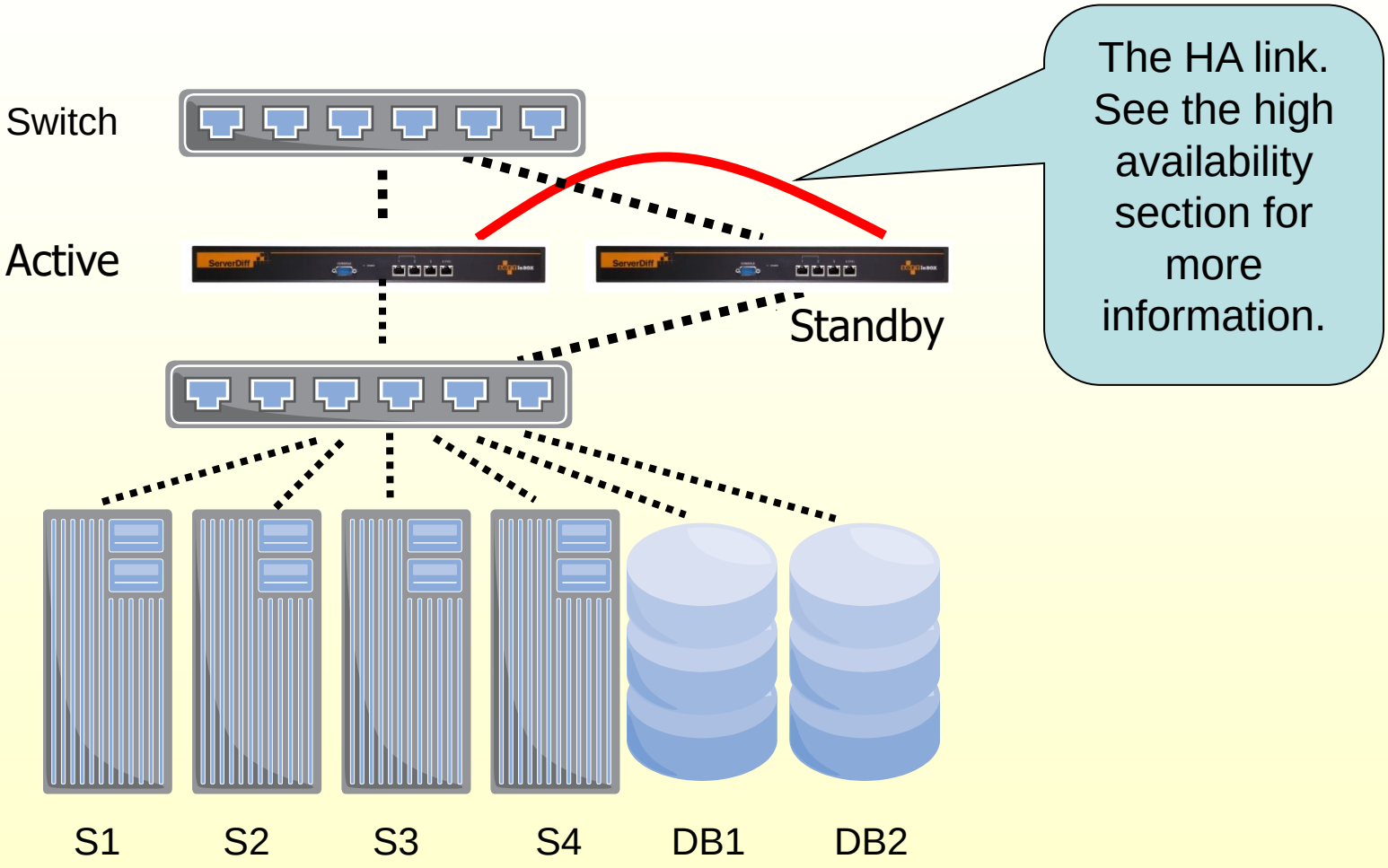
SOFT inBOX

Transparent Bridge (TB) Mode

- ✓Configure vDiff as a bridge (i.e., L2 switch) and place it in front of the AP servers.
- ✓Clients connects as before to the AP servers (with IP or domain name to the AP servers), with the added benefits of load balancing and fault tolerance.
- ✓Servers see the real source IP of the clients.



High Availability in TB mode



Configuration in TB mode (1/4)

Ethernet port setting

Ethernet	Speed	Watch	Mode	
e1	all-auto	off	on	Edit
e2	all-auto	off	on	Edit

Ethernet bonding

Ethernet	Mode	
e1	active-backup	Edit
e2	active-backup	Edit

VLAN and bridge binding

Index	Ethernet	VLAN tag	bridge	path cost	port priority	
1	e1	none	bridge_1	100	32	Ec
2	e2	none	bridge_1	100	32	Ec

Bridge list

Index	Name			
1	bridge_1	Edit	Delete	Insert
				Insert

SOFT inBOX

(2/4)

IPv4 address

Index	IP/mask	Bridge			
1	192.168.1.99/24	bridge_1	Edit	Delete	Insert
					Insert

IPv4 route

Index	Destination subnet	Gateway			
1	default	192.168.1.1	Edit	Delete	Insert
					Insert

IPv4 ARP watch

Index	IP	Bridge	Flush			
1	192.168.1.31	bridge_1	Edit	Delete		Insert
2	192.168.1.32	bridge_1	Edit	Delete	Up	Insert
3	192.168.1.33	bridge_1	Edit	Delete	Up	Insert
4	192.168.1.34	bridge_1	Edit	Delete	Up	Insert
						Insert

Notice this.

SOFT inBOX

(3/4)

Group list

Index	Name				
1	G_web_sample	VIP 192.168.1.31, tcp 80,443, 4 targets. Detail	Edit	Delete	Insert
					Insert

Group G_web_sample health check

Health check method: HTTP
Health check port: 80
HTTP URL to check: /
HTTP text to match: 200 OK
Health check interval (in sec): 10
Health check target:
Health check counts: 1:1:0:1:1:0
One target down action: CONTINUE

Edit

Group G_web_sample parameter

Virtual IP: 192.168.1.31
Virtual IP6:
TCP ports: 80,443
UDP ports:
==========
Load balancing algorithm: RANDOM
Session help: S
Session timeout: 600
Connection limit per session:1000000
==========
SNAT IP:
SNAT IP6:
DNAT: on
All targets down action: CONTINUE

Edit

Group G_web_sample target list

Index	Name	IP	IP6	Weight	Misc.	Flush		
1	AP_31	192.168.1.31		1		Edit	Delete	
2	AP_32	192.168.1.32		1		Edit	Delete	Up
3	AP_33	192.168.1.33		1		Edit	Delete	Up
4	AP_34	192.168.1.34		1		Edit	Delete	Up

SOFT inBOX

(4/4)

Table

Index	Name		Flush			
1	Root	(root table)	Edit	Delete		Insert
2	admin_accept		Edit	Delete	Up	Insert
3	group_tweak		Edit	Delete	Up	Insert
						Insert

Filter Root (root table)

Index	Bridge	Source IP	Destination IP	Misc.	Action	Flush			
1					CALL#admin_accept	Edit	Delete		Insert
2					CALL#group_tweak	Edit	Delete	Up	Insert
									Insert

Filter admin_accept

Index	Bridge	Source IP	Destination IP	Misc.	Action			
1		10.10.10.123			ACCEPT	Edit	Delete	Insert
								Insert

Filter group_tweak

Index	Bridge	Source IP	Destination IP	Misc.	Action	
1			192.168.1.32-192.168.1.34	TCP dstport=80	L4SW#G_web_sample	Edi
2			192.168.1.32-192.168.1.34	TCP dstport=443	L4SW#G_web_sample	Edi

Do not load balance connections from the administrator (you, 10.10.10.123). So when you connect to say 192.168.1.32 you are not load balanced. This helps debugging.

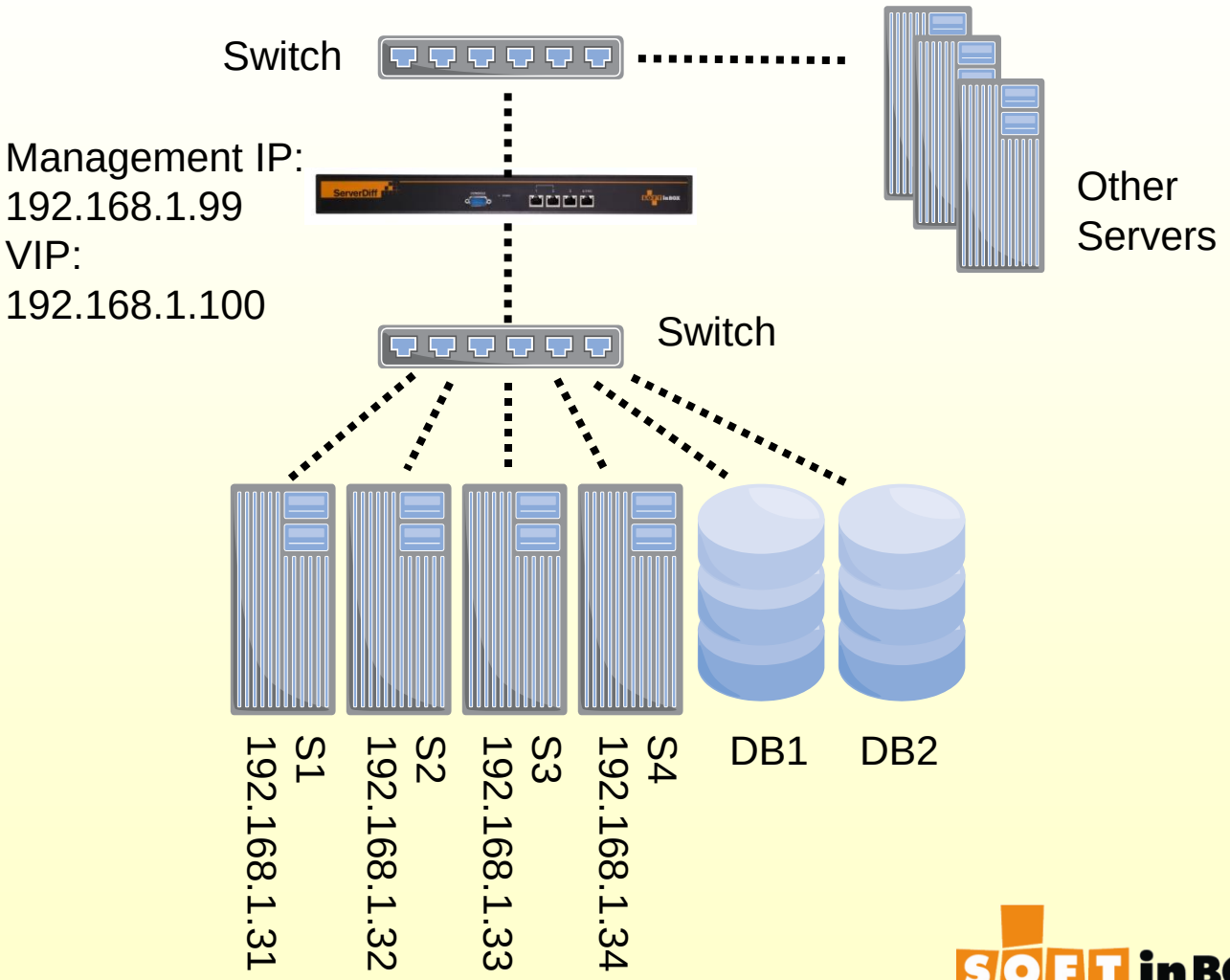
SOFT inBOX

Mode 2: VIP Bridge Mode

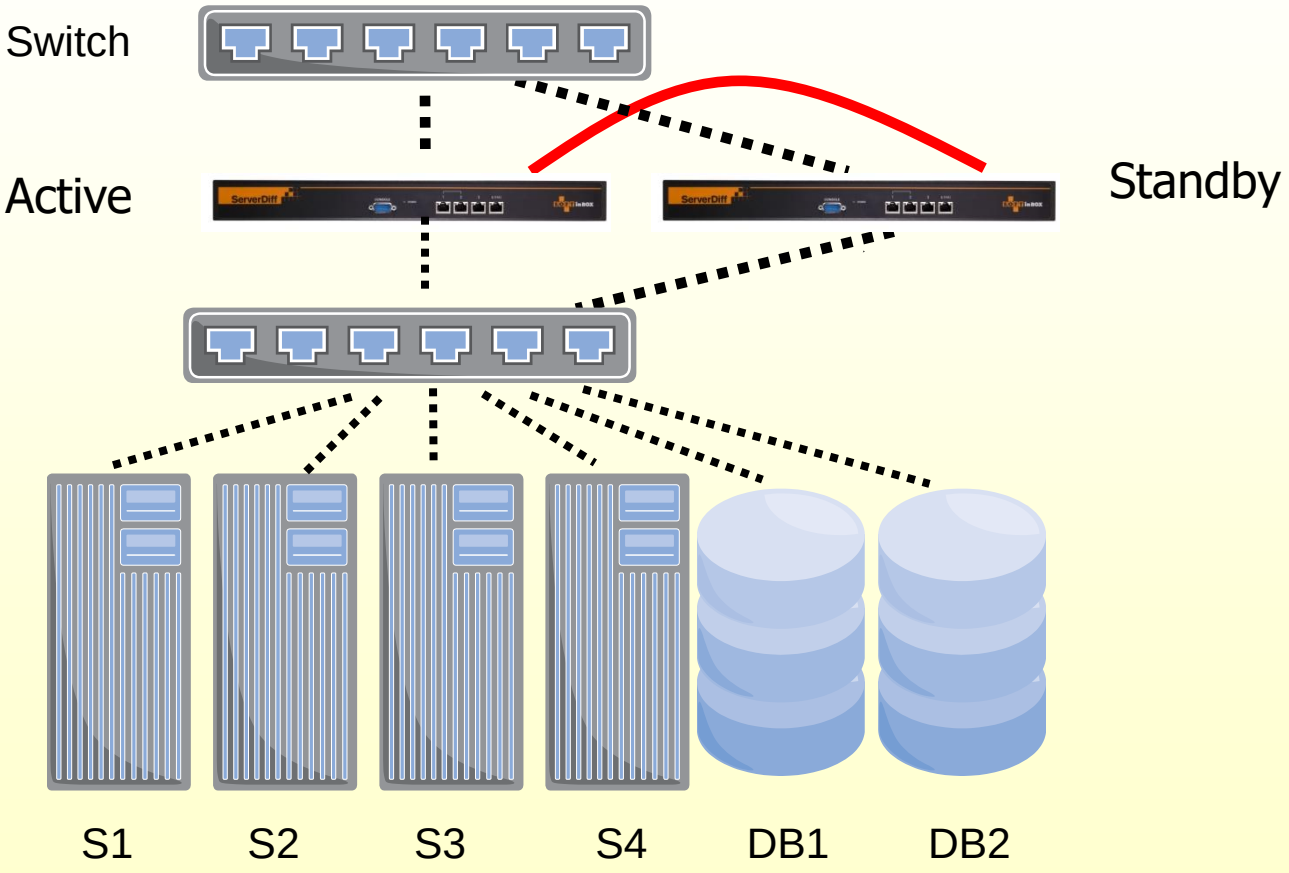
SOFT inBOX

VIP Bridge Mode

- ✓vDiff is configured as a bridge (L2 switch) and with an additional IP called the VIP (192.168.1.100 here).
- ✓Connect to the VIP and you get the load balancing.
- ✓The AP servers see the original client IP(s).



HA in VIP bridge mode



SOFT inBOX

VIP bridge mode config (1/3)

Ethernet port setting

Ethernet	Speed	Watch	Mode	
e1	all-auto	off	on	Edit
e2	all-auto	off	on	Edit

Ethernet bonding

Ethernet	Mode	
e1	active-backup	Edit
e2	active-backup	Edit

VLAN and bridge binding

Index	Ethernet	VLAN tag	bridge	path cost	port priority	
1	e1	none	bridge_1	100	32	Ed
2	e2	none	bridge_1	100	32	Ed

Bridge list

Index	Name			
1	bridge_1	Edit	Delete	Insert
				Insert

SOFT inBOX

Config (2/3)

Add the VIP 192.168.1.100.

IPv4 address

Index	IP/mask	Bridge				
			Flush			
1	192.168.1.99/24	bridge_1	Edit	Delete		Insert
2	192.168.1.100/24	bridge_1	Edit	Delete	Up	Insert
						Insert

IPv4 route

Index	Destination subnet	Gateway			
1	default	192.168.1.1	Edit	Delete	Insert
					Insert

SOFT inBOX

Config (3/3)

Group list

Index	Name				
1	G_web_sample	VIP 192.168.1.100, tcp 80,443, 4 targets. Detail	Edit	Delete	Insert
					Insert

Group G_web_sample health check

Health check method: HTTP
Health check port: 80
HTTP URL to check: /
HTTP text to match: 200 OK
Health check interval (in sec): 10
Health check target:
Health check counts: 1:1:0:1:1:0
One target down action: CONTINUE

Edit

Group G_web_sample parameter

Virtual IP: 192.168.1.100
Virtual IP6:
TCP ports: 80,443
UDP ports:
==========
Load balancing algorithm: RANDOM
Session help: S
Session timeout: 600
Connection limit per session:1000000
==========
SNAT IP:
SNAT IP6:
DNAT: on
All targets down action: CONTINUE

Edit

Group G_web_sample target list

Index	Name	IP	IP6	Weight	Misc.	Flush		
1	AP_31	192.168.1.31		1		Edit	Delete	
2	AP_32	192.168.1.32		1		Edit	Delete	Up
3	AP_33	192.168.1.33		1		Edit	Delete	Up
4	AP_34	192.168.1.34		1		Edit	Delete	Up

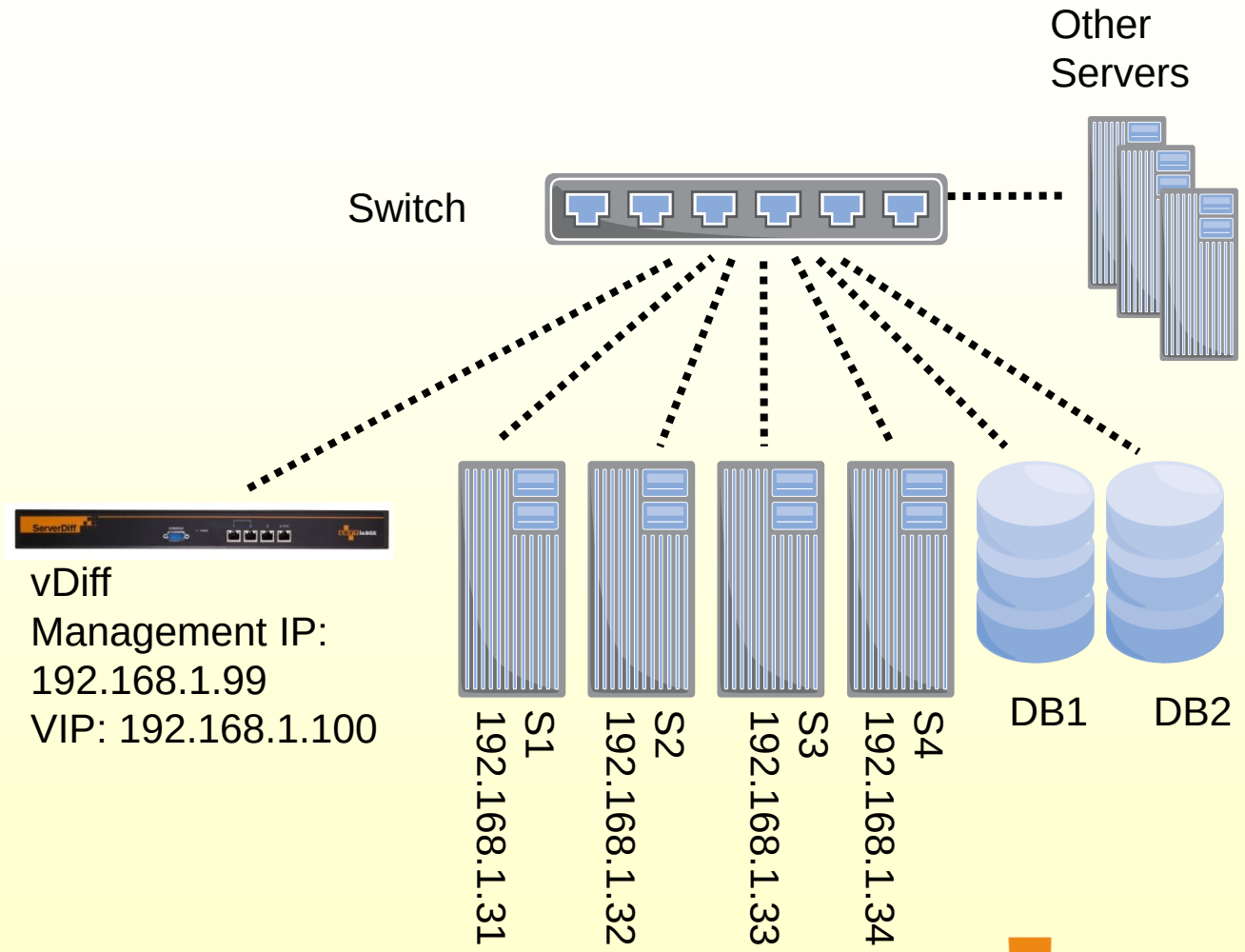
SOFT inBOX

Mode 3: VIP One-Arm Mode

SOFT inBOX

Mode 3: VIP One-Arm Mode

- ✓A Client connects to the VIP (192.168.1.100).
- ✓vDiff connects to the selected server, with VIP as the source IP.
- ✓The server processes the request and reply to VIP (which is vDiff).
- ✓vDiff reply to the client.



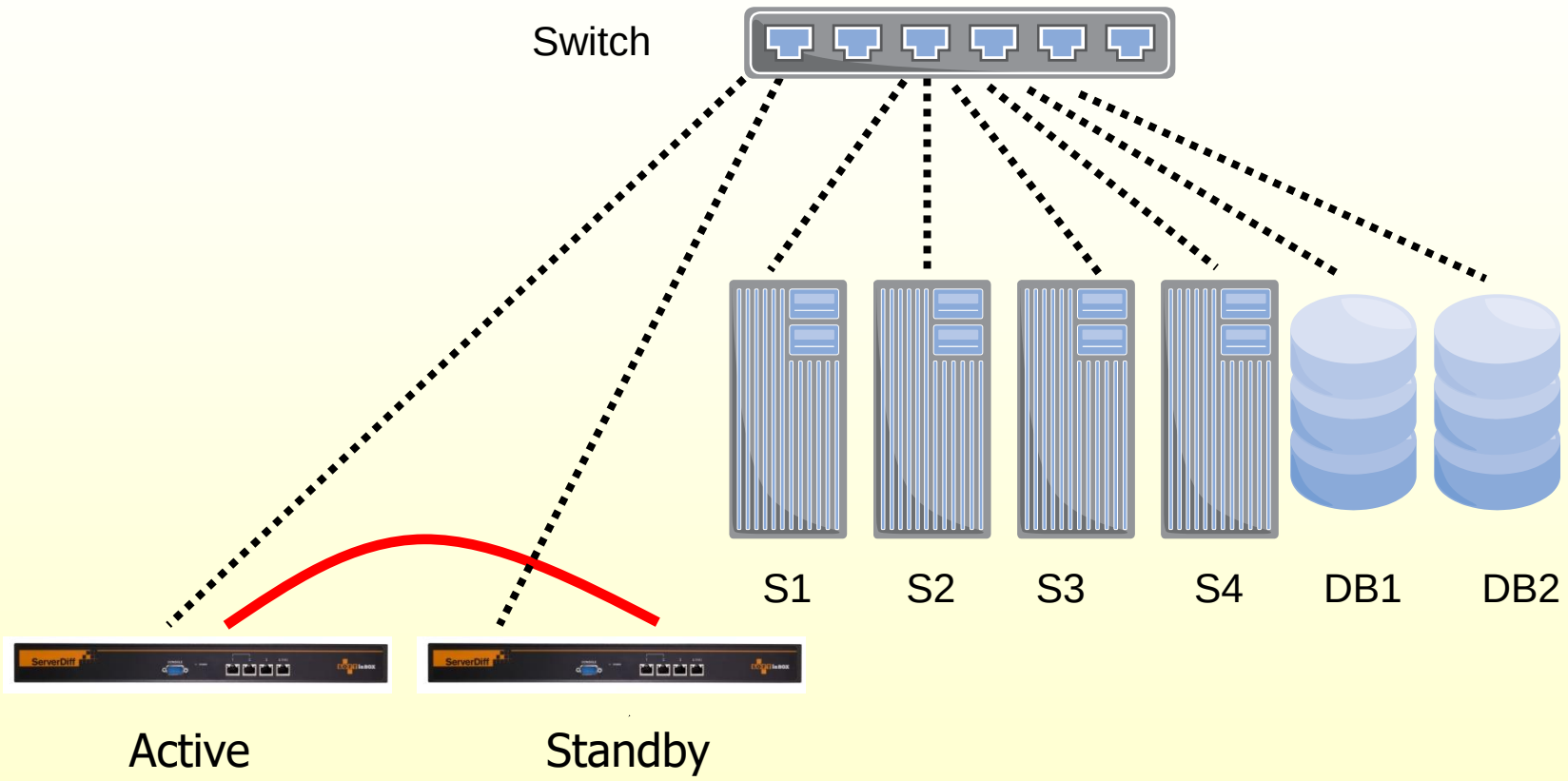
SOFT inBOX

Characteristics

- vDiff is acting just like a host, with one cable to the switch.
- The AP server does not see the IP(s) of the clients. All the connections comes from the VIP.

SOFT inBOX

HA in one-arm mode



Config (1/3)

VLAN and bridge binding

Index	Ethernet	VLAN tag	bridge	path cost	port priority			
1	e1	none	bridge_1	100	32	Edit	Delete	Insert
								Insert

Bridge list

Index	Name			
1	bridge_1	Edit	Delete	Insert
				Insert

SOFT inBOX

Config (2/3)

Add the VIP 192.168.1.100.

IPv4 address

Index	IP/mask	Bridge				
			Flush			
1	192.168.1.99/24	bridge_1	Edit	Delete		Insert
2	192.168.1.100/24	bridge_1	Edit	Delete	Up	Insert
						Insert

IPv4 route

Index	Destination subnet	Gateway			
1	default	192.168.1.1	Edit	Delete	Insert
					Insert

SOFT inBOX

Config (3/3)

Group list

Index	Name				
1	G_web_sample	VIP 192.168.1.100, tcp 80,443, 4 targets. Detail	Edit	Delete	Insert
					Insert

Group G_web_sample health check

Health check method: HTTP
Health check port: 80
HTTP URL to check: /
HTTP text to match: 200 OK
Health check interval (in sec): 10
Health check target:
Health check counts: 1:1:0:1:1:0
One target down action: CONTINUE

Edit

Group G_web_sample parameter

Virtual IP: 192.168.1.100
Virtual IP6:
TCP ports: 80,443
UDP ports:
==========
Load balancing algorithm: RANDOM
Session help: S
Session timeout: 600
Connection limit per session:1000000
==========
SNAT IP: 192.168.1.100
SNAT IP6:
DNAT: on
All targets down action: CONTINUE

Edit

Group G_web_sample target list

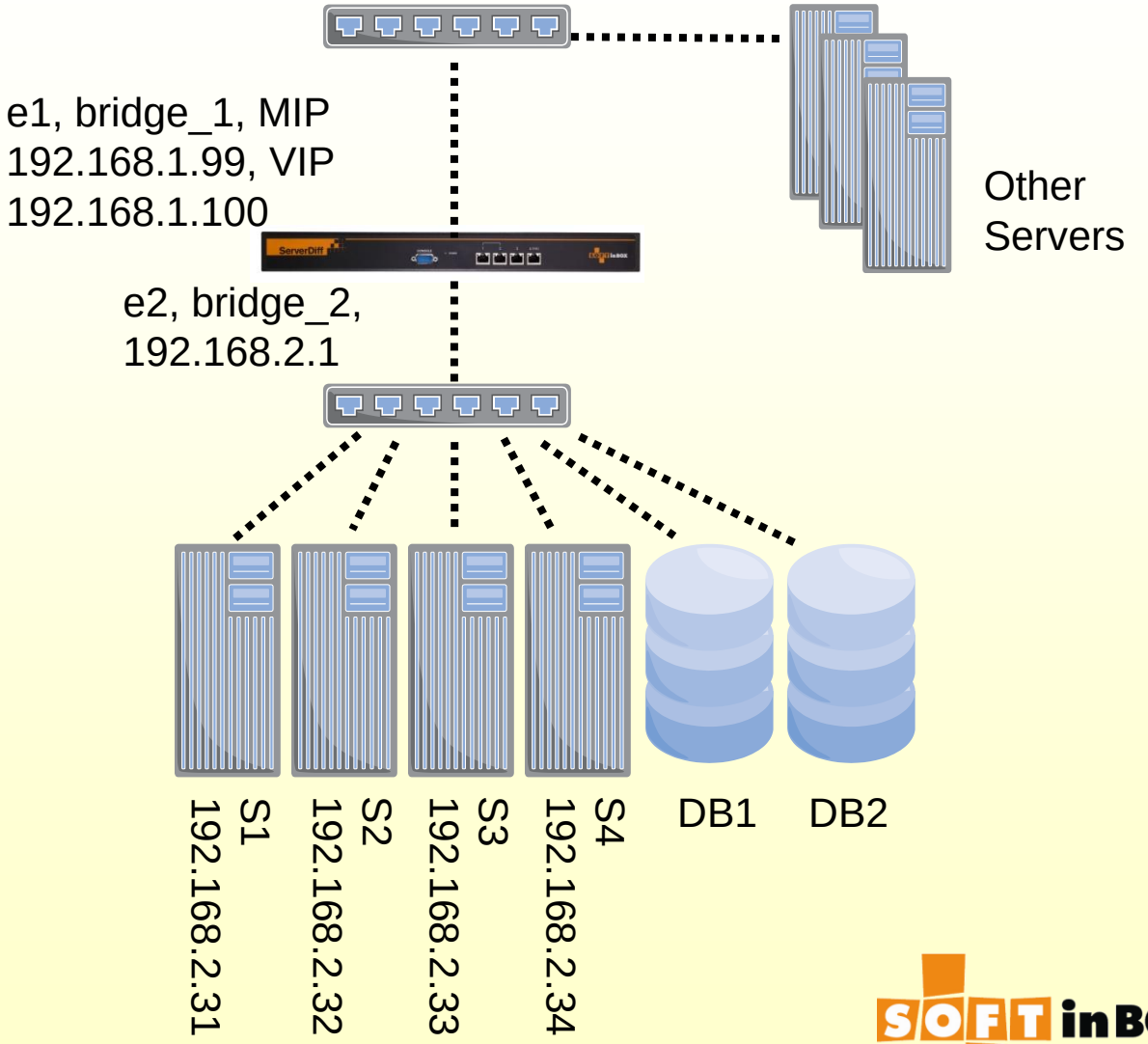
Index	Name	IP	IP6	Weight	Misc.	Flush
1	AP_31	192.168.1.31		1		Edit Delete
2	AP_32	192.168.1.32		1		Edit Delete Up
3	AP_33	192.168.1.33		1		Edit Delete Up
4	AP_34	192.168.1.34		1		Edit Delete Up

Notice!

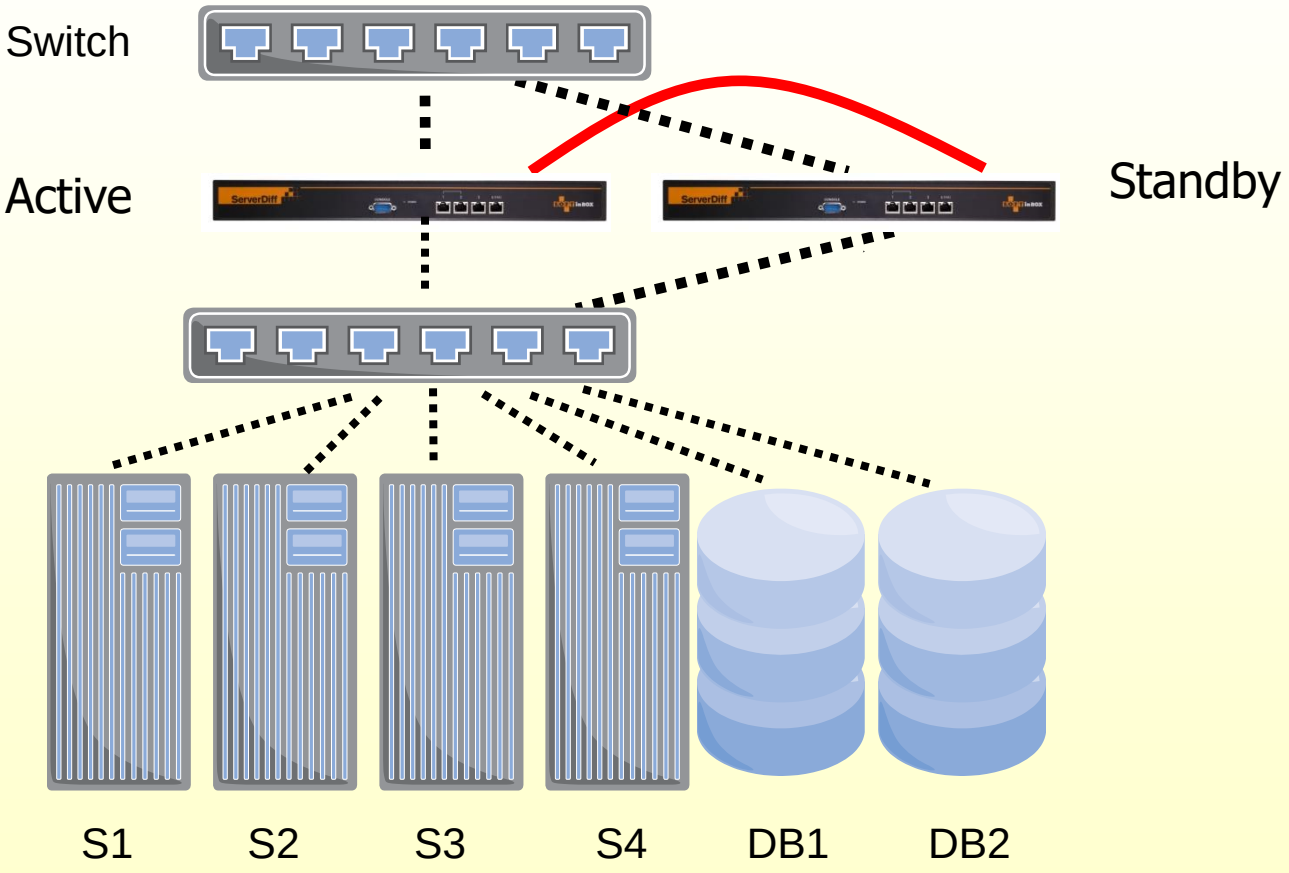
SOFT inBOX

Mode 4: VIP Router Mode

- ✓vDiff is configured as a router and with an additional IP called the VIP (192.168.1.100 here).
- ✓192.168.2.1 is the gateway for the hosts in 192.168.2.0/24
- ✓The clients Connect to the VIP and get load balanced.
- ✓The AP servers see the original client IP(s).



HA in VIP router mode



SOFT inBOX

Config (1/3)

VLAN and bridge binding

Index	Ethernet	VLAN tag	bridge	path cost	port priority	Flush			
1	e1	none	bridge_1	100	32	Edit	Delete		Insert
2	e2	none	bridge_2	100	32	Edit	Delete	Up	Insert
									Insert

Bridge list

Index	Name	Flush			
1	bridge_1	Edit	Delete		Insert
2	bridge_2	Edit	Delete	Up	Insert
					Insert

SOFT inBOX

Config (2/3)

IPv4 address

Index	IP/mask	Bridge		Flush		
1	192.168.1.99/24	bridge_1	Edit	Delete		Insert
2	192.168.1.100/24	bridge_1	Edit	Delete	Up	Insert
3	192.168.2.1/24	bridge_2	Edit	Delete	Up	Insert
						Insert

IPv4 route

Index	Destination subnet	Gateway			
1	default	192.168.1.1	Edit	Delete	Insert
					Insert

SOFT inBOX

Config (3/3)

Group list

Index	Name				
1	G_web_sample	VIP 192.168.1.100, tcp 80,443, 4 targets. Detail	Edit	Delete	Insert
					Insert

Group G_web_sample health check

Health check method: HTTP
Health check port: 80
HTTP URL to check: /
HTTP text to match: 200 OK
Health check interval (in sec): 10
Health check target:
Health check counts: 1:1:0:1:1:0
One target down action: CONTINUE

Edit

Group G_web_sample parameter

Virtual IP: 192.168.1.100
Virtual IP6:
TCP ports: 80,443
UDP ports:
==========
Load balancing algorithm: RANDOM
Session help: S
Session timeout: 600
Connection limit per session:1000000
==========
SNAT IP:
SNAT IP6:
DNAT: on
All targets down action: CONTINUE

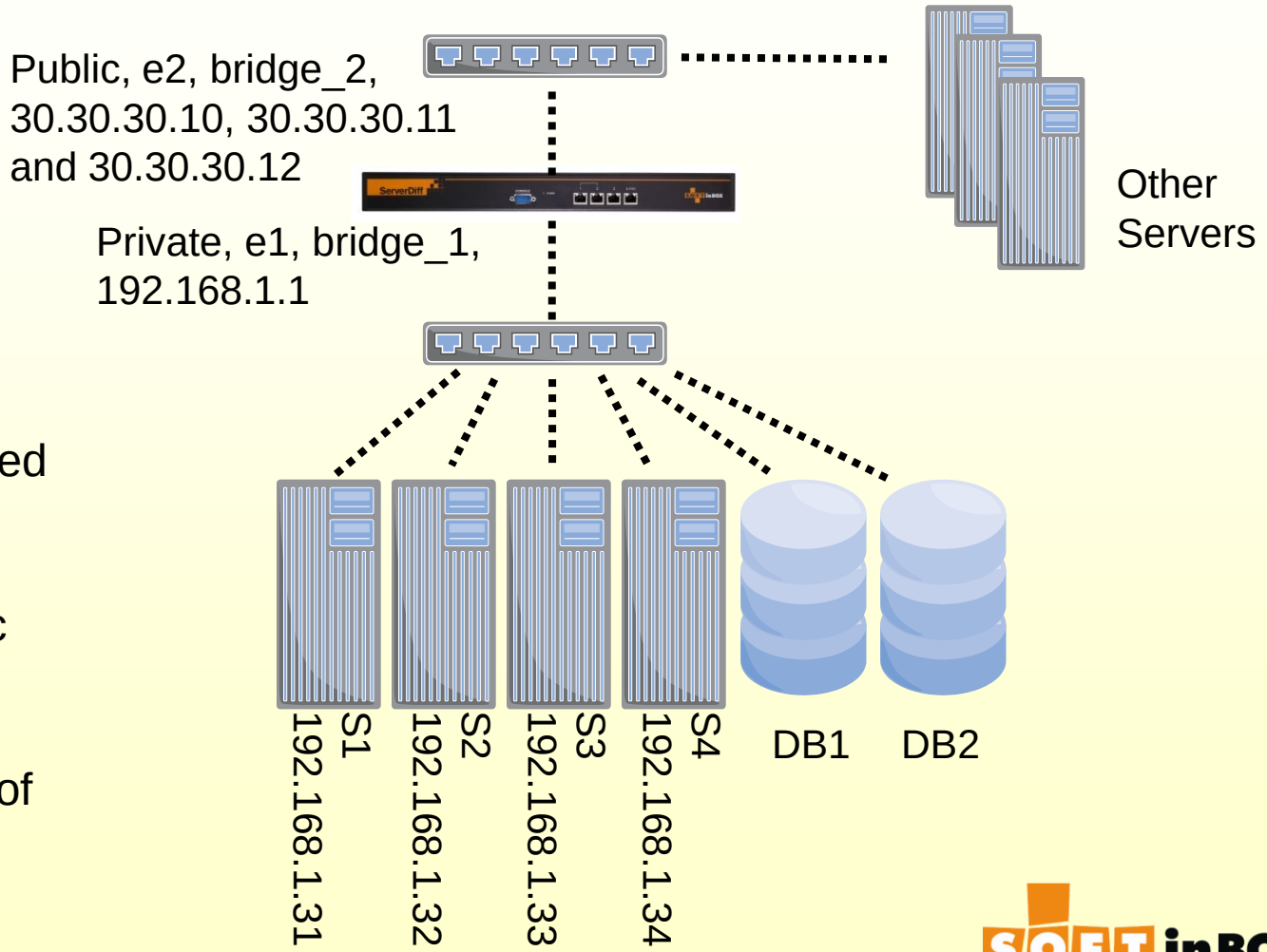
Edit

Group G_web_sample target list

Index	Name	IP	IP6	Weight	Misc.	Flush		
1	AP_31	192.168.2.31		1		Edit	Delete	
2	AP_32	192.168.2.32		1		Edit	Delete	Up
3	AP_33	192.168.2.33		1		Edit	Delete	Up
4	AP_34	192.168.2.34		1		Edit	Delete	Up

SOFT inBOX

5: VIP FW mode

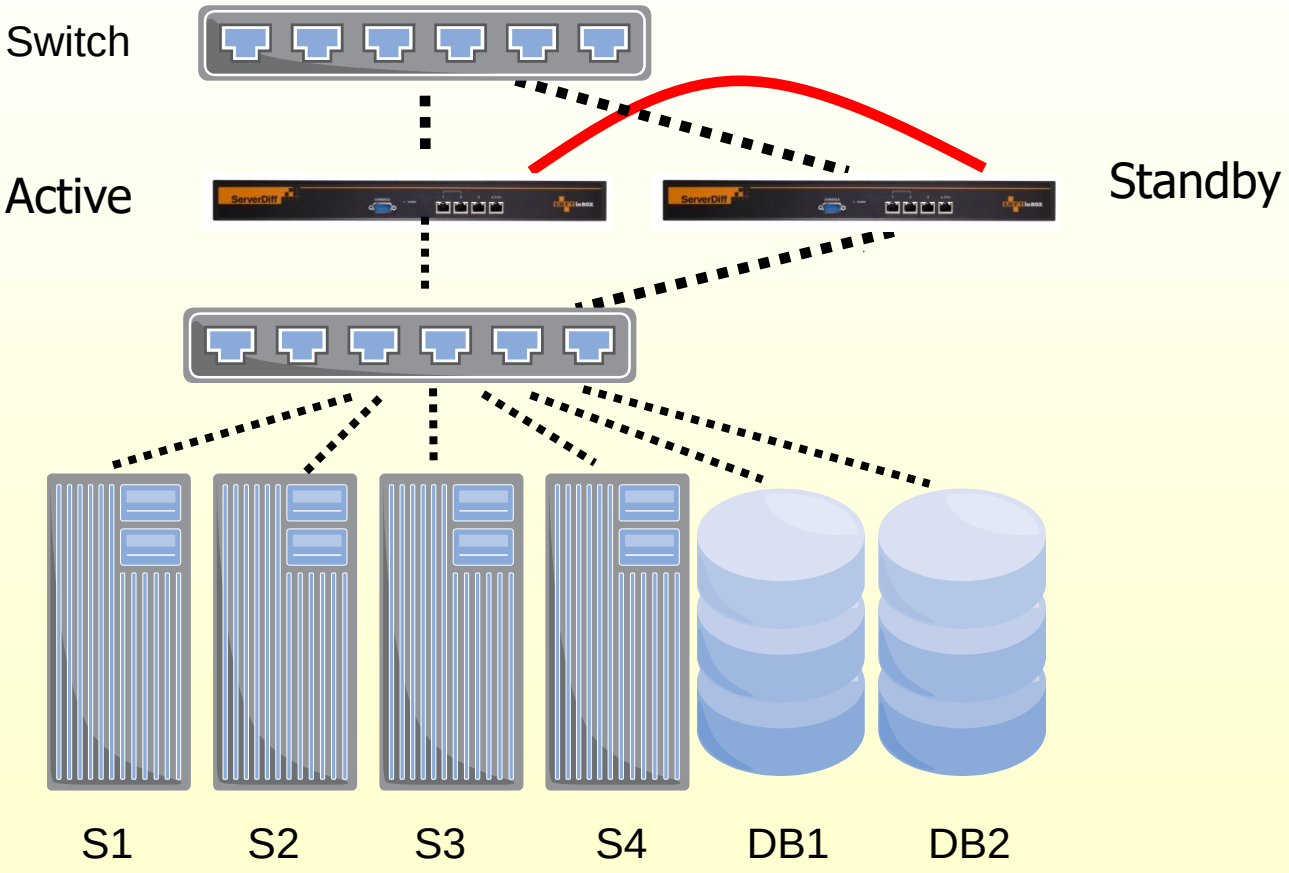


- ✓vDiff is configured as a router that separates the private and public networks.
- ✓AP servers see the original IP(s) of clients.

Tasks

- vDiff is a simple firewall that separates the public and the private subnets.
- 30.30.30.10 is the source IP for outbound connections.
- Connections to 30.30.30.11 (which is called the VIP) is load balanced to the AP servers.
- Connections to 30.30.30.12 is redirected to some internal server.
- See the configuration in the following for details.

HA in FW mode



SOFT inBOX

Config (1/5)

VLAN and bridge binding

Index	Ethernet	VLAN tag	bridge	path cost	port priority	Flush			
1	e1	none	bridge_lan	100	32	Edit	Delete		Insert
2	e2	none	bridge_wan	100	32	Edit	Delete	Up	Insert
									Insert

Bridge list

Index	Name	Flush			
1	bridge_lan	Edit	Delete		Insert
2	bridge_wan	Edit	Delete	Up	Insert
					Insert

SOFT inBOX

Config (2/5)

IPv4 address

Index	IP/mask	Bridge			Flush	
1	192.168.1.1/24	bridge_lan	Edit	Delete		Insert
2	30.30.30.10/24	bridge_wan	Edit	Delete	Up	Insert
3	30.30.30.11/24	bridge_wan	Edit	Delete	Up	Insert
4	30.30.30.12/24	bridge_wan	Edit	Delete	Up	Insert
						Insert

IPv4 route

Index	Destination subnet	Gateway				Flush
[redacted]						
2	default	30.30.30.1	Edit	Delete	Up	Insert
						Insert

Ignore it.

SOFT inBOX

Config (3/5)

Group list

Index	Name				
1	G_web_sample	VIP 30.30.30.11, tcp 80,443, 4 targets. Detail	Edit	Delete	Insert
					Insert

Group G_web_sample health check

Health check method: HTTP
Health check port: 80
HTTP URL to check: /
HTTP text to match: 200 OK
Health check interval (in sec): 10
Health check target:
Health check counts: 1:1:0:1:1:0
One target down action: CONTINUE

Edit

Group G_web_sample parameter

Virtual IP: 30.30.30.11
Virtual IP6:
TCP ports: 80,443
UDP ports:
==========
Load balancing algorithm: RANDOM
Session help: S
Session timeout: 600
Connection limit per session:1000000
==========
SNAT IP:
SNAT IP6:
DNAT: on
All targets down action: CONTINUE

Edit

Group G_web_sample target list

Index	Name	IP	IP6	Weight	Misc.	Flush		
1	AP_31	192.168.1.31		1		Edit	Delete	
2	AP_32	192.168.1.32		1		Edit	Delete	Up
3	AP_33	192.168.1.33		1		Edit	Delete	Up
4	AP_34	192.168.1.34		1		Edit	Delete	Up

SOFT inBOX

Config (4/5)

Table

Index	Name		Flush			
1	Root	(root table)	Edit	Delete		Insert
2	local_accept		Edit	Delete	Up	Insert
3	out_snat		Edit	Delete	Up	Insert
4	in_dnat		Edit	Delete	Up	Insert
						Insert

SOFT inBOX

Config (5/5)

Filter local_accept

Index	Bridge	Source IP	Destination IP	Misc.	Action			
1	bridge_lan	192.168.1.0/24	192.168.1.0/24		ACCEPT	Edit	Delete	Insert
								Insert

Filter out_snat

Index	Bridge	Source IP	Destination IP	Misc.	Action			
1	bridge_lan	192.168.1.0/24			SNAT#30.30.30.10	Edit	Delete	Insert
								Insert

Filter in_dnat

Index	Bridge	Source IP	Destination IP	Misc.	Action			
1	bridge_wan		30.30.30.12	TCP dstport=1022	DNAT#192.168.1.33#22	Edit	Delete	Insert
								Insert

Filter Root (root table)

Index	Bridge	Source IP	Destination IP	Misc.	Action				Flush
1					CALL#local_accept	Edit	Delete		Insert
2					CALL#out_snat	Edit	Delete	Up	Insert
3					CALL#in_dnat	Edit	Delete	Up	Insert
									Insert

SOFT inBOX

High Availability

SOFT inBOX

HA operations (1/2)

- With HA in operation, one of the vDiff is the “master” and the other is the “slave.” The master is responsible for the processing of all traffic, and the slave works in standby mode and monitors the status of the master via the HA links.
- When the master fails, the slave will take over and become the new master.

(2/2)

- When you log into the UI (web or CLI), you are connecting to the master. When the configuration changes, it is transferred to the slave automatically.
- The master and the slave shares all configurations and IP(s). There is no IP configured specifically for the slave.
- You can check the status of the slave in the UI. With console, use “show hainfo”. With Web UI, check “View>System” and watch the “HA peer information” block.

SOFT inBOX

HA config

- You can configure vDiff with zero, one or two Ethernet ports as the HA ports.
- Use it in CLI (console, SSH, telnet)
- tool halink 0
- tool halink 1 e1 all-auto
- tool halink 2 e1 all-auto e2 all-auto
- Then reboot.
- The involving two vDiff(s) should be configured separately with exactly the same halink config.
- You can give the two vDiff(s) different hostnames to distinguish them easily. Use “tool hostname <name>” in the console.

SOFT inBOX

HA requirements

- Two vDiff(s) should have same hardware (CPU, RAM, Ethernet ports, etc), same software version, and same halink config.
- Save the configuration file in case something went wrong.
- Link the HA port(s) of the two vDiff(s) BEFORE you power on the second vDiff.

SOFT inBOX

Verification of HA

- Ping continuously an IP on vDiff. Usually you pick the IP used to connect to the web UI.
- Power off the master.
- The ping will continue after a few drops.
- Log in the web UI and see that the old slave is now the new master. You may distinguish them by the serial numbers or the hostnames.

SOFT inBOX

Load Balancing Algorithms

SOFT inBOX

LBA: Randomized

- Choose a target randomly.
- Example: 3 targets A, B, and C, with weights 1, 3, and 2, respectively. Then the probability to target A, B, or C is 1/6, 3/6, and 2/6, respectively.

LBA: Round Robin

- Choose a target in round robin.
- Example: 3 targets A, B, and C, with weights 1, 1, and 2. Then connections to this group will be delivered to A, B, C, C, A, B, C, C, and so on.

LBA: Connection Rate

- Choose a target that has minimum connection rate.
- Connection rates are measured in connections per second, in the last few seconds.

LBA: Bandwidth

- Choose a target with minimum bandwidth consumptions.
- Bandwidth consumption is measured in bytes per second, in both directions, in the last few seconds.

LBA: Active Connections

- Choose a target with the least number of active connections.
- An active connection is an connection that is in vDiff's connection table.

LBA: Session Rate

- Choose a target with minimum session rate.
- Session rate is measured in sessions per second, in the last few seconds.

LBA: Active Sessions

- Choose a target with the least active sessions.
- A active session is a session that is in vDiff's session table.

LBA: Response Time

- Choose a target with probability reciprocal to the response time in its last health check.

LBA: Hash

- Choose a target with a static hash function.
- The hash function takes as arguments the source and destination addresses of the connection and the weight of a target. Connections whose source and destination addresses are the same will be dispatched to the same target.

Session Helper

SOFT inBOX

SH: None

- This means that every connection get the opportunity to be load balanced.

SH: By source and destination IP

- The session table in vDiff keeps track of which target to use for a (src, dst) pair. When a new connection arrived, the session table is looked up. If an entry is found, use the stored target. Otherwise, do load balance and choose a target and new an entry in the session table about it.

SH: By source IP

- Ignore the destination IP in the session table described in the previous page. Use the source IP only.

Health Check Method

SOFT inBOX

HCM: Ping

- Use ping (IPv4 echo request) to check if a target is alive or dead (faulty).

HCM: TCP connection establishment

- Try to establish a TCP connection (the SYN, SYN-ACK, ACK handshake) to a target at the specified port.

HCM: SMTP server 220 response

- Try TCP connection to a target at the specified port (usually 25) and wait for the SMTP 220 response (the hello response).
- Useful for SMTP (sendmail) servers.

HCM: HTTP page test (1/2)

- Do health check by connecting to the specified TCP port (usually 80) and try to grab a HTTP page.
- Example: If you provide a page /aux/health.php on the web server, set the “HTTP URL to check” as “/aux/health.php”, “HTTP text to match” as “200 OK” (this is usually the first line of text you see in the HTTP response) or a string that can be found on the page.

SOFT inBOX

(2/2)

- HTTP host to check: The domain name of the web server, for example www.abc.com. Usually you can leave it blank.
- HTTP additional header 1/2/3: supply additional HTTP header lines here. Usually they can be left blank.

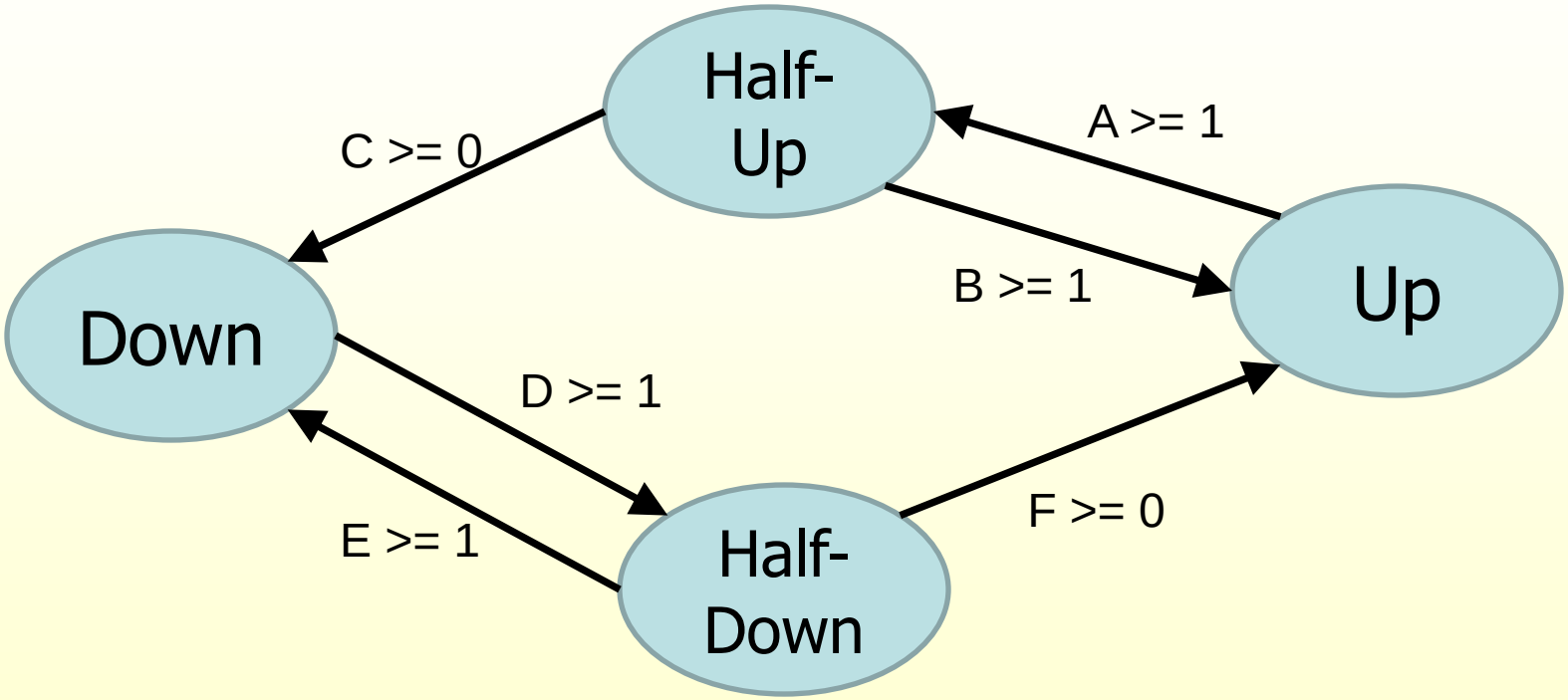
Target State Transition

SOFT inBOX

Target states

- A target can be in one of the four states.
- Up: The target accepts new connections.
- Half-Up or Half-Down: The target accepts new connections that match some entry in the session table.
- Down: The target is unable to accept new connections.

State transition diagram



SOFT inBOX

Moving in the state transition diagram

- A: Number of consecutive health check failures to move from Up to Half_Up.
- B: Number of consecutive health check successes to move from Half_Up to Up.
- C: Number of consecutive failures to move from Half_Up to Down.
- D: Number of consecutive successes to move from Down to Half_Down.
- E: Number of consecutive failures to move from Half_Down to Down.
- F: Number of consecutive successes to move from Half_Down to Up

Aggressive default configuration

- The default configuration for the state transition counters, which is 1:1:0:1:1:0, is pretty aggressive. It catches the up/down events fast.
- However, if you find unusually many up/donw logs in the "target health check log," consider change the counters to something milder, for example, 2:2:1:2:2:1.

Action when one target is down

- When a target is down, what to do to the packets of the existing connections to the target. The options are:
- Continue: flow of the packets continues.
- Drop: drop the packets.
- Reject: drop the packets and send REJECT packets back to the senders.

Action when all targets are down (1/2)

- When all the targets in a group is unable to accept new connections, what to do to new connections. (This may due to that a target is down, the connection/session limit of the a target is reached, or the connection per session count is reached.)
- This config is in “group parameter.”
- The options are:

(2/2)

- Continue: forwarding the connection without load balancing. This is usually useful only to the transparent bridge mode. With other networking models, the connection may hit vDiff and show the management UI or be simply rejected.
- Drop: the connection is dropped.
- Reject: the connection is dropped and a reject packet is returned to the sender.

Some measures to protect the targets

- Connection limit (target configuration): The number of active connections a target can have.
- Session limit (target configuration): The number of active sessions a target can have.
- Connections per session limit (group parameter): The limit of the number of active connections of a session.

Configuration examples for some popular services

SOFT inBOX

Example for the web service

- TCP ports: “80,443”
- Session help: S or SD
- Health check method: HTTP

Example for the SMTP service

- TCP ports: “25”
- Session help: None
- Health check method: SMTP

SOFT inBOX

Example for the MS terminal service

- TCP ports: “3389”
- Session help: S or SD
- Health check method: SYNACK at port 3389

Gracefully off-line a target for maintenance (1/5)

- Four AP servers run smoothly.

Group G_web_sample status

Index	Name	IP	Status	Weight	Active connections	Active sessions	Mode
1	AP_31	192.168.1.31	Up	1	3,009	4,428	On Edit
2	AP_32	192.168.1.32	Up	1	3,000	4,424	On Edit
3	AP_33	192.168.1.33	Up	1	2,995	4,433	On Edit
4	AP_34	192.168.1.34	Up	1	2,996	4,426	On Edit

SOFT inBOX

(2/5)

- AP_32 is scheduled to upgrade the RAM, for example. So we change its mode to “half.”
- New connections to old sessions on AP_32 still go to AP_32, but new sessions are not to be created on AP_32. The active connections/sessions counters decrease.

(3/5)

- Like this.

Group G_web_sample status

Index	Name	IP	Status	Weight	Active connections	Active sessions	Mode
1	AP_31	192.168.1.31	Up	1	3,339	4,765	On Edit
2	AP_32	192.168.1.32	Up	0	2,015	3,443	Half Edit
3	AP_33	192.168.1.33	Up	1	3,325	4,733	On Edit
4	AP_34	192.168.1.34	Up	1	3,321	4,760	On Edit

SOFT inBOX

(4/5)

- Eventually the counters are zeros (or close to zeros). It is time to off-line AP_32 and do your maintenance.

Group G_web_sample status

Index	Name	IP	Status	Weight	Active connections	Active sessions	Mode
1	AP_31	192.168.1.31	Up	1	4,073	6,005	On Edit
2	AP_32	192.168.1.32	Up	0	0	0	Half Edit
3	AP_33	192.168.1.33	Up	1	3,972	5,859	On Edit
4	AP_34	192.168.1.34	Up	1	3,955	5,840	On Edit

SOFT inBOX

(5/5)

- After the maintenance. Change its mode back to “on.”
- The counters of AP_32 increase and back to normal gradually.

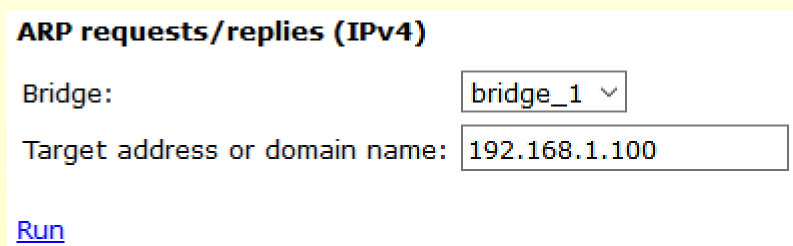
Group G_web_sample status

Index	Name	IP	Status	Weight	Active connections	Active sessions	Mode
1	AP_31	192.168.1.31	Up	1	3,805	5,761	On Edit
2	AP_32	192.168.1.32	Up	1	750	750	On Edit
3	AP_33	192.168.1.33	Up	1	3,729	5,614	On Edit
4	AP_34	192.168.1.34	Up	1	3,716	5,606	On Edit

SOFT inBOX

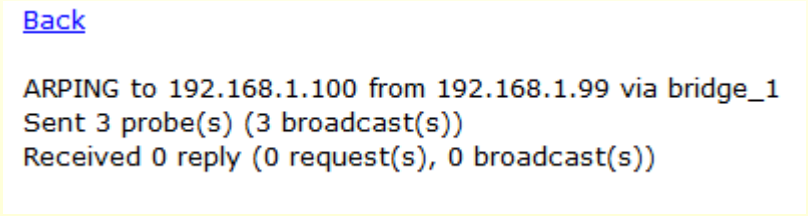
ARP request/reply test (1/3)

- This is useful to detect duplicate IP(s) on the network. For example to test if there are duplicate IP(s) of the VIP 192.168.1.100 on the network, do the following in web UI > Tools > Diagnostic.



(2/3)

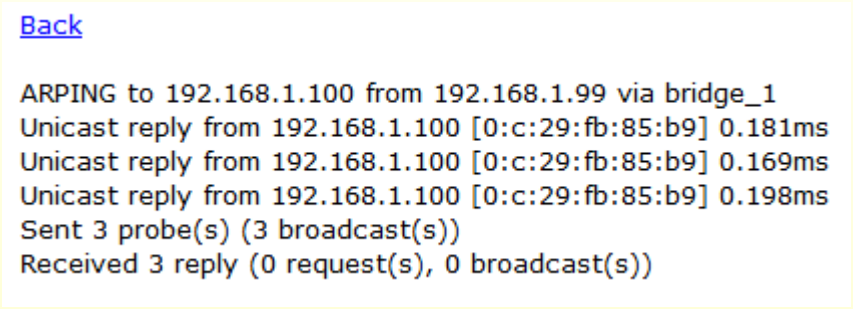
- Normally, there should not be other hosts on the network that have the IP, so the result look like this:



SOFT inBOX

(3/3)

- Otherwise, you will see something like this, indicating some duplicate IP.

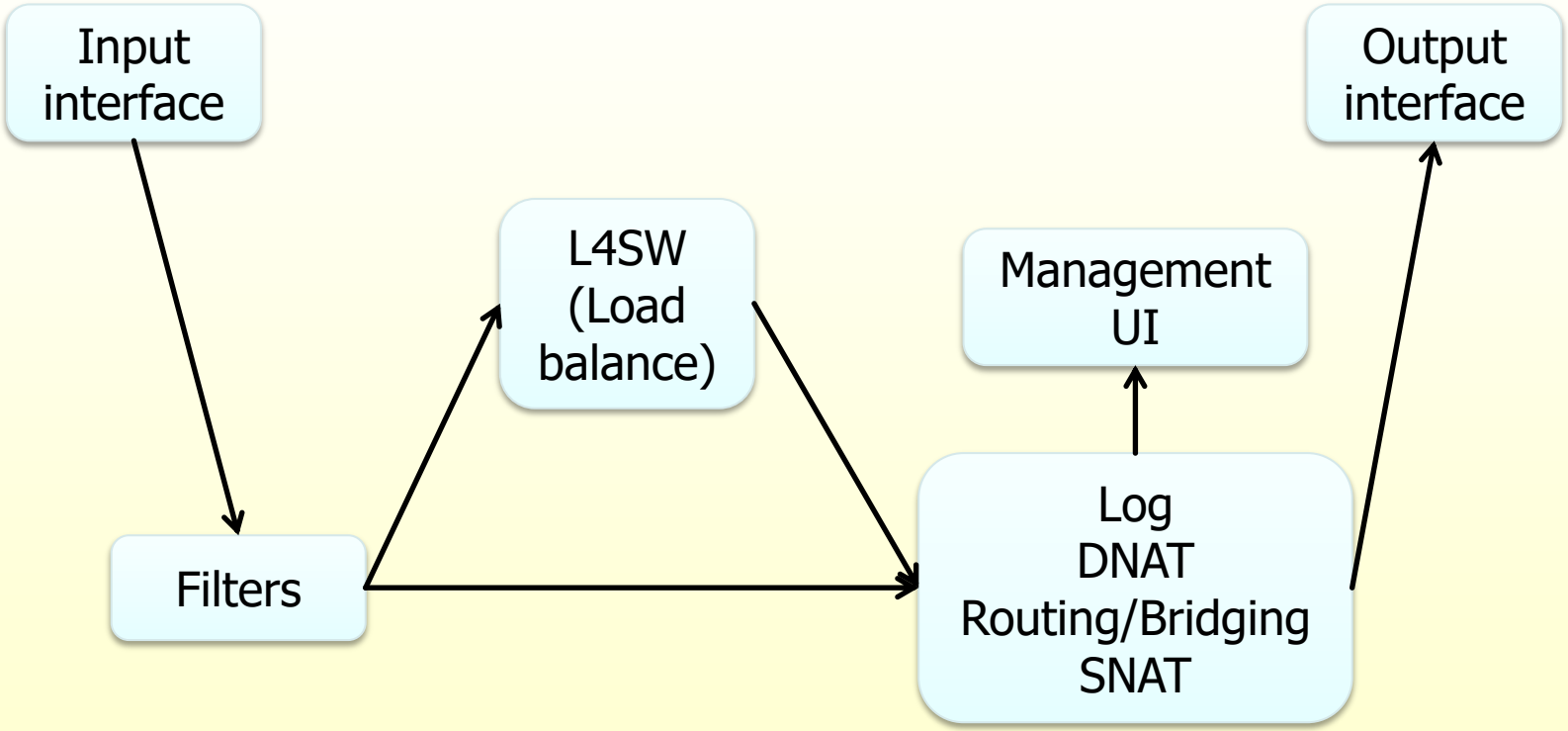


SOFT inBOX

Filters and the processing of connections

SOFT inBOX

Processing of connections



Basics (1/2)

- Every new connection travelling through vDiff is processes by the filters.
- Start from the first rule of the table marked as “root table” and “flow” through the rules one by one.
- The connection is matched against the rule. If it matches, the action is taken.
- Depending on the action it takes, the connection may (1) leave the filters all together, (2) be dropped, or (3) “flow” the following rules.

SOFT inBOX

(2/2)

- At the end of a non-root table. The flow resumes at the calling rule.
- At the end of the root table, the connection will be given to the L4 switching module, which matches the connection against the groups.

The matches

- Input interface.
- Source IP.
- Destination IP.
- Protocol: None, TCP, UDP, or ICMP.
- TCP/UDP source and destination port.
- Forwarded from <ip>. Match if the source MAC address of the connection is equal to the MAC of <ip>. Useful to see if the connection is from some gateway (router) specified by <ip>.

The actions (1/6)

- CONTINUE. A dummy action that does nothing. Flow the next rule.
- LOG <text>. Emit a entry to the "connection log" along with the <text>. Flow the next rule.
- ACCEPT. Leave the filters all together. The connection will be processed by the L2/L3 modules of vDiff. It goes to the management UI if appropriate. But it will NOT be processed by the L4 switching module.

SOFT inBOX

(2/6)

- DROP. Drop the connection. It is fed to “the blackhole.”
- REJECT. The same to “DROP” and a reject packet is returned to the sender.
- CALL <table>. Jump to <table> (and flow the first rule).
- RETURN. The flow of the connection resumes at the calling rule.

(3/6)

- L4SW log on. Turn on the “L4SW log flag.” The flow continues.
- L4SW log off. Turn off the “L4SW log flag”. The flow continues.
- Admin allow. Turn on the “admin allow flag.” The flow continues.
- Admin deny. Turn off the “admin allow flag.” The flow continues.

(4/6)

- SNAT <ip>. Replace the “SNAT mark” with <ip>. The flow continues.
- DNAT <ip>. Replace the “DNAT mark” with <ip>. The flow continues.
- DNAT <ip> <port>. Replace the “DNAT mark” with <ip> and <port>. The flow continues.

(5/6)

- L4SW <group>. Feed the connection to the load balance <group>. If it is not processed by <group>, the flow continues, otherwise, leave the filters all together.
- Session help with source IP override <ip>. Replace the “session help source ip mark” with <ip>. The flow continues.

(6/6)

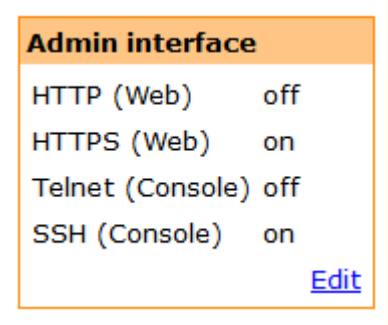
- Session help with source IP mask <mask>. Replace the “session help source ip mask” with <mask>. The flow continues.
- REPLY_GW <ip>. Replace the “reply gateway mark” with <ip>. The flow continues.

Admin UI access

SOFT inBOX

(1/2)

- There are several administrative user interfaces: http, https, telnet, and ssh. They can be activated/deactivated individually by:



SOFT inBOX

(2/2)

- By default, admin UI is allowed from all IP(s). You can allow connections only from hosts in 10.0.0.0/8, as follows.

Table

Index	Name		Flush			
1	Root	(root table)	Edit	Delete		Insert
2	Admin_control		Edit	Delete	Up	Insert
						Insert

Filter Admin_control

Index	Bridge	Source IP	Destination IP	Misc.	Action	Flush			
1					ADMIN_DENY	Edit	Delete		Insert
2		10.0.0.0/8			ADMIN_ALLOW	Edit	Delete	Up	Insert
									Insert

Filter Root (root table)

Index	Bridge	Source IP	Destination IP	Misc.	Action			
1					CALL#Admin_control	Edit	Delete	Insert
								Insert

SOFT inBOX

L4SW (load balancing) logs

SOFT inBOX

(1/2)

- By default, the L4SW log is off. You can enable it as follows.

Table

Index	Name		Flush			
1	Root	(root table)	Edit	Delete		Insert
2	L4SW_log		Edit	Delete	Up	Insert
						Insert

Filter Root (root table)

Index	Bridge	Source IP	Destination IP	Misc.	Action			
1					CALL#L4SW_log	Edit	Delete	Insert
								Insert

Filter L4SW_log

Index	Bridge	Source IP	Destination IP	Misc.	Action			
1					L4SW_LOG_ON	Edit	Delete	Insert
								Insert

SOFT inBOX

(2/2)

- And you can fine tune it, for example log only connections from 192.168.2.0/24, like this:

Table

Index	Name				Flush	
1	Root	(root table)	Edit	Delete		Insert
2	L4SW_log		Edit	Delete	Up	Insert
						Insert

Filter Root (root table)

Index	Bridge	Source IP	Destination IP	Misc.	Action			
1					CALL#L4SW_log	Edit	Delete	Insert
								Insert

Filter L4SW_log

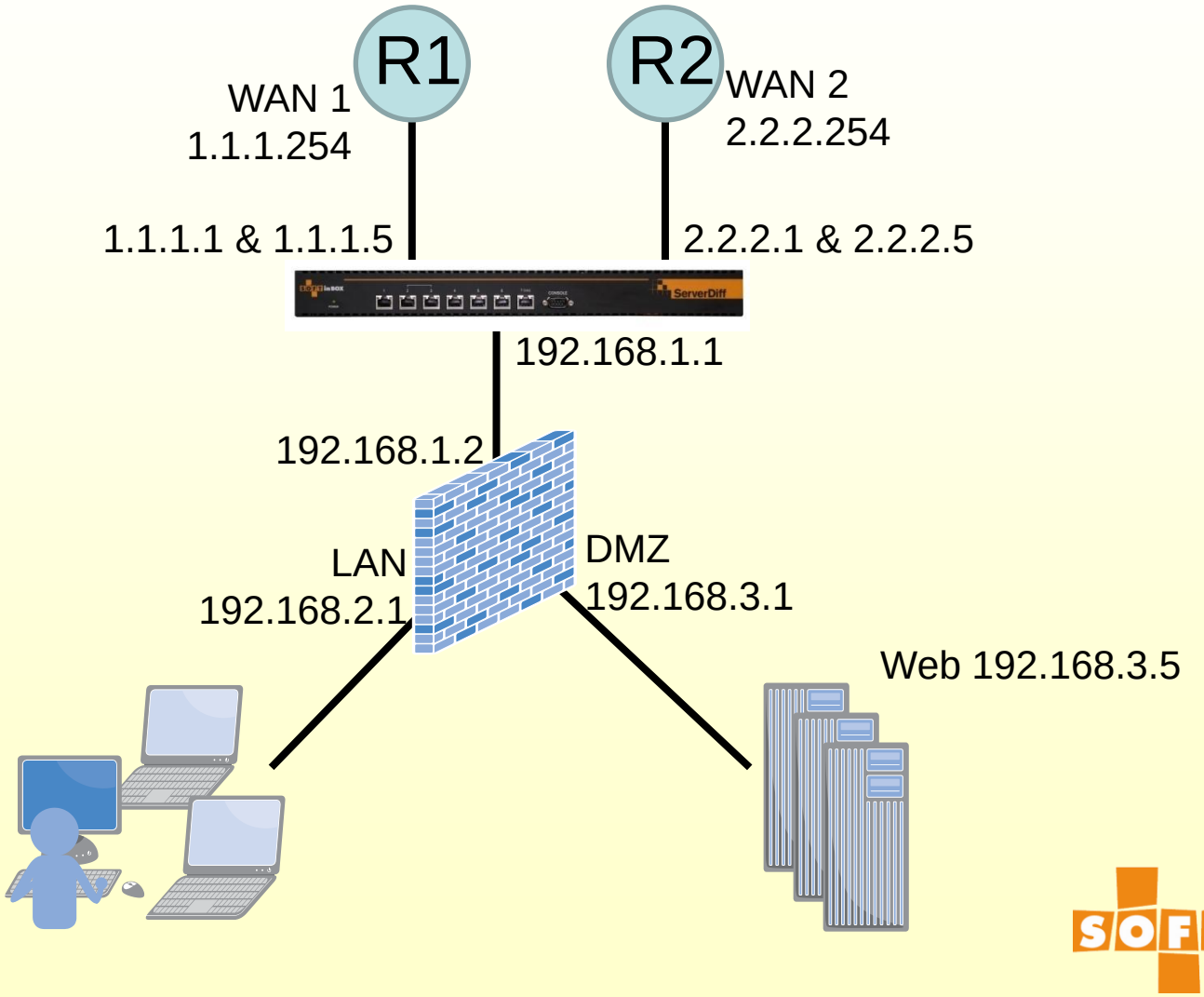
Index	Bridge	Source IP	Destination IP	Misc.	Action			
1		192.168.2.0/24			L4SW_LOG_ON	Edit	Delete	Insert
								Insert

SOFT inBOX

WAN load balance

SOFT inBOX

Network topology



Tasks (1/2)

- Outbound load balancing. For connections from 192.168.x.x to Internet, load balance on WAN 1 and WAN 2, by doing so, SNAT to 1.1.1.1 for WAN 1 and 2.2.2.1 for WAN 2, respectively.

Tasks (2/2)

- Map public IP(s) to internal services. In this example, map 1.1.1.5 and 2.2.2.5 to the internal web server at 192.168.3.5.

Config (1/5)

VLAN and bridge binding

Index	Ethernet	VLAN tag	bridge	path cost	port priority	Flush			
1	e1	none	b_lan	100	32	Edit	Delete		Insert
2	e2	none	b_wan_1	100	32	Edit	Delete	Up	Insert
3	e3	none	b_wan_2	100	32	Edit	Delete	Up	Insert
									Insert

Bridge list

Index	Name	Flush			
1	b_lan	Edit	Delete		Insert
2	b_wan_1	Edit	Delete	Up	Insert
3	b_wan_2	Edit	Delete	Up	Insert
					Insert

SOFT inBOX

(2/5)

IPv4 address

Index	IP/mask	Bridge		Flush		
1	192.168.1.1/24	b_lan	Edit	Delete		Insert
2	1.1.1.1/24	b_wan_1	Edit	Delete	Up	Insert
3	2.2.2.1/24	b_wan_2	Edit	Delete	Up	Insert
						Insert

IPv4 route

Index	Destination subnet	Gateway			
1	default	192.168.1.2	Edit	Delete	Insert
					Insert

SOFT inBOX

(3/5)

Group WAN_LB parameter

Virtual IP:
Virtual IP6:
TCP ports:
UDP ports:
==========
Load balancing algorithm: CONN_RATE
Session help: SD
  Session timeout: 600
  Connection limit per session:1000000
==========
SNAT IP:
SNAT IP6:
DNAT: off
All targets down action: CONTINUE

Group WAN_LB health check

Health check method: PING
  Ping TTL: 4
Health check interval (in sec): 10
Health check target: 8.8.8.8
Health check counts: 1:1:0:1:1:0
One target down action: CONTINUE

Edit

Group WAN_LB target list

Index	Name	IP	IP6	Weight	Misc.	Flush			
1	WAN_1	1.1.1.254		1	SNAT IP: 1.1.1.1	Edit	Delete		Insert
2	WAN_2	2.2.2.254		1	SNAT IP: 2.2.2.1	Edit	Delete	Up	Insert
									Insert

(4/5)

Table

Index	Name		Flush			
1	Root	(root table)	Edit	Delete		Insert
2	admin_control		Edit	Delete	Up	Insert
3	reply		Edit	Delete	Up	Insert
4	inbound		Edit	Delete	Up	Insert
5	outbound		Edit	Delete	Up	Insert
						Insert

Filter admin_control

Index	Bridge	Source IP	Destination IP	Misc.	Action	Flush			
1					ADMIN_DENY	Edit	Delete		Insert
2			192.168.1.1		ADMIN_ALLOW	Edit	Delete	Up	Insert
3			192.168.1.1		ACCEPT	Edit	Delete	Up	Insert
									Insert

Filter reply

Index	Bridge	Source IP	Destination IP	Misc.	Action	Flush			
1	b_wan_1			forwarded_from=1.1.1.254	REPLY_GW#1.1.1.254	Edit	Delete		Insert
2	b_wan_2			forwarded_from=2.2.2.254	REPLY_GW#2.2.2.254	Edit	Delete	Up	Insert
									Insert

SOFT inBOX

(5/5)

Filter inbound

Index	Bridge	Source IP	Destination IP	Misc.	Action	Flush			
1	b_wan_1		1.1.1.5	TCP dstport=80	DNAT#192.168.3.5	Edit	Delete		Insert
2	b_wan_2		2.2.2.5	TCP dstport=80	DNAT#192.168.3.5	Edit	Delete	Up	Insert
									Insert

Filter outbound

Index	Bridge	Source IP	Destination IP	Misc.	Action			
1	b_lan				L4SW#WAN_LB	Edit	Delete	Insert
								Insert

Filter Root (root table)

Index	Bridge	Source IP	Destination IP	Misc.	Action	Flush			
1					CALL#admin_control	Edit	Delete		Insert
2					CALL#reply	Edit	Delete	Up	Insert
3					CALL#inbound	Edit	Delete	Up	Insert
4					CALL#outbound	Edit	Delete	Up	Insert
									Insert

SOFT inBOX

vDiff installation

SOFT inBOX

install.zip

- You are supplied with an install file install.zip, with the following contents:

install
install/00readme.txt
install/install_hyperv
install/install_hyperv/disk.vhd
install/install_vmware
install/install_vmware/disk.vmdk
install/install_vmware/vdiff.ovf
install/install_xen
install/install_xen/config_sample.1
install/install_xen/config_sample.2
install/install_xen/disk.bin

SOFT inBOX

VMWare installation

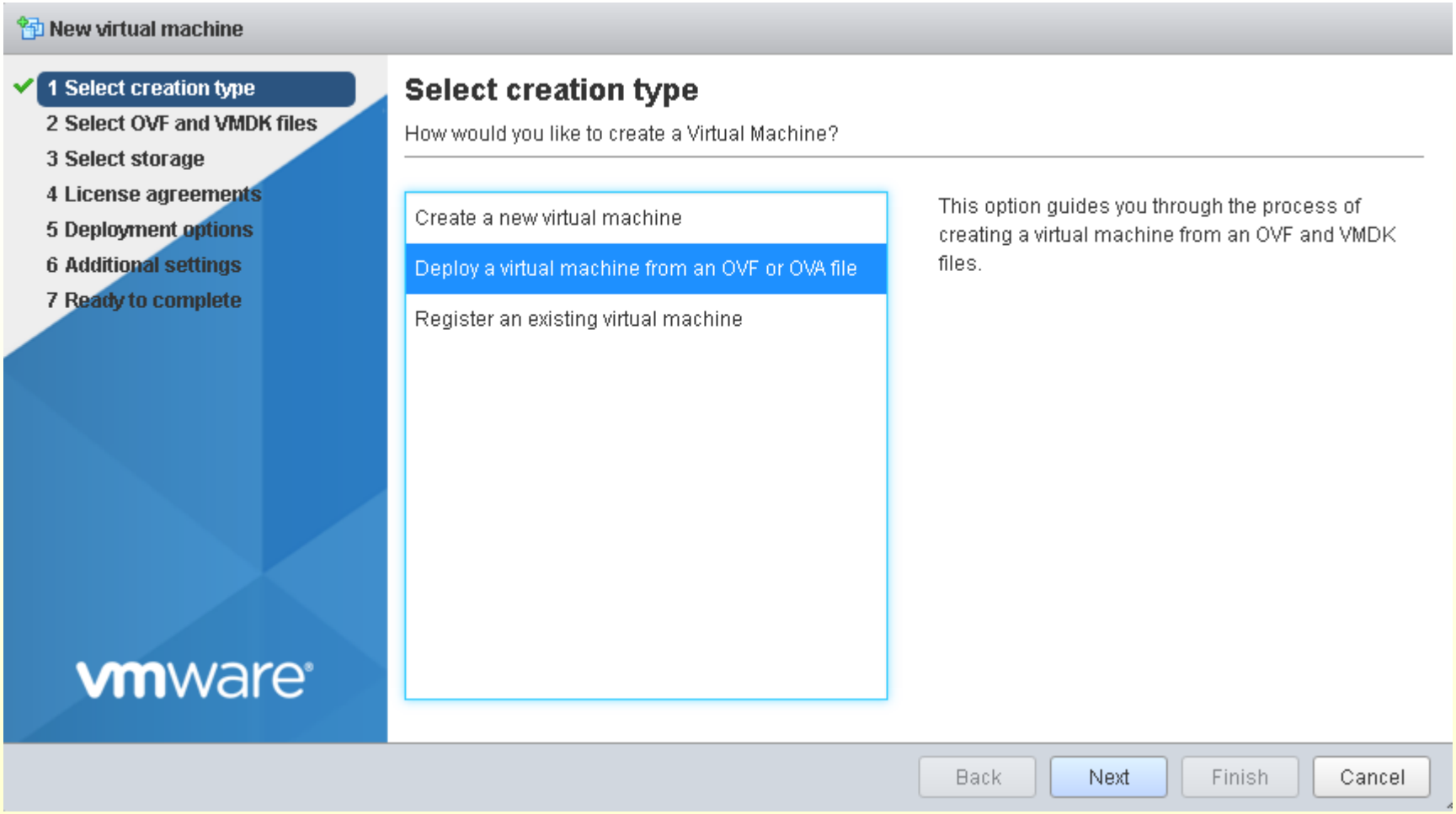
SOFT inBOX

Sample environment

- This document is prepared with Vmware ESXi-6.5.0 Host Client web UI.
- Extract install.zip and look into the install_vmware directory.

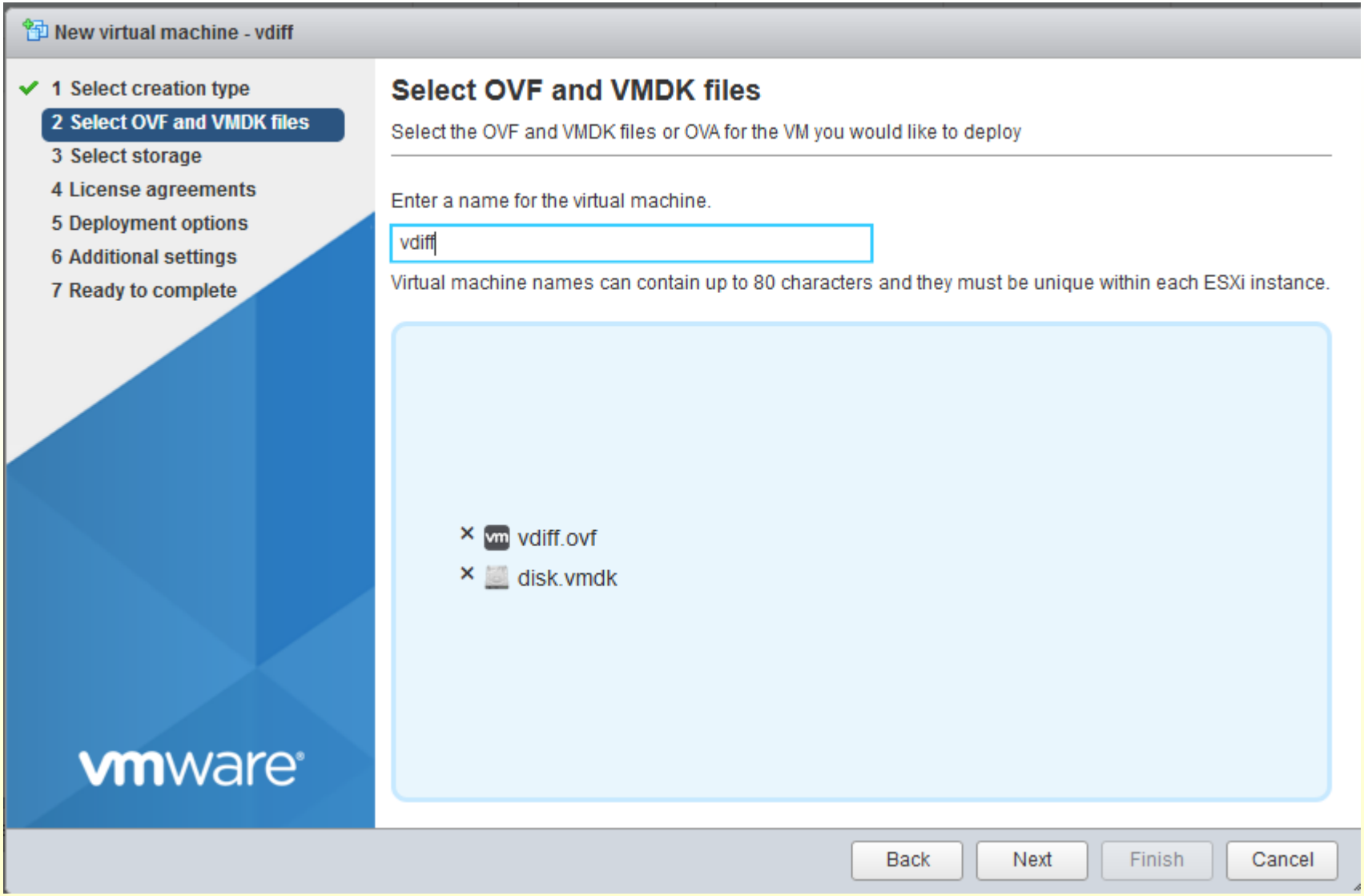
Create a VMWare ESXi VM from OVF and VMDK files

SOFT inBOX



Select “Deploy a virtual machine from an OVF or OVA file.”

SOFT inBOX

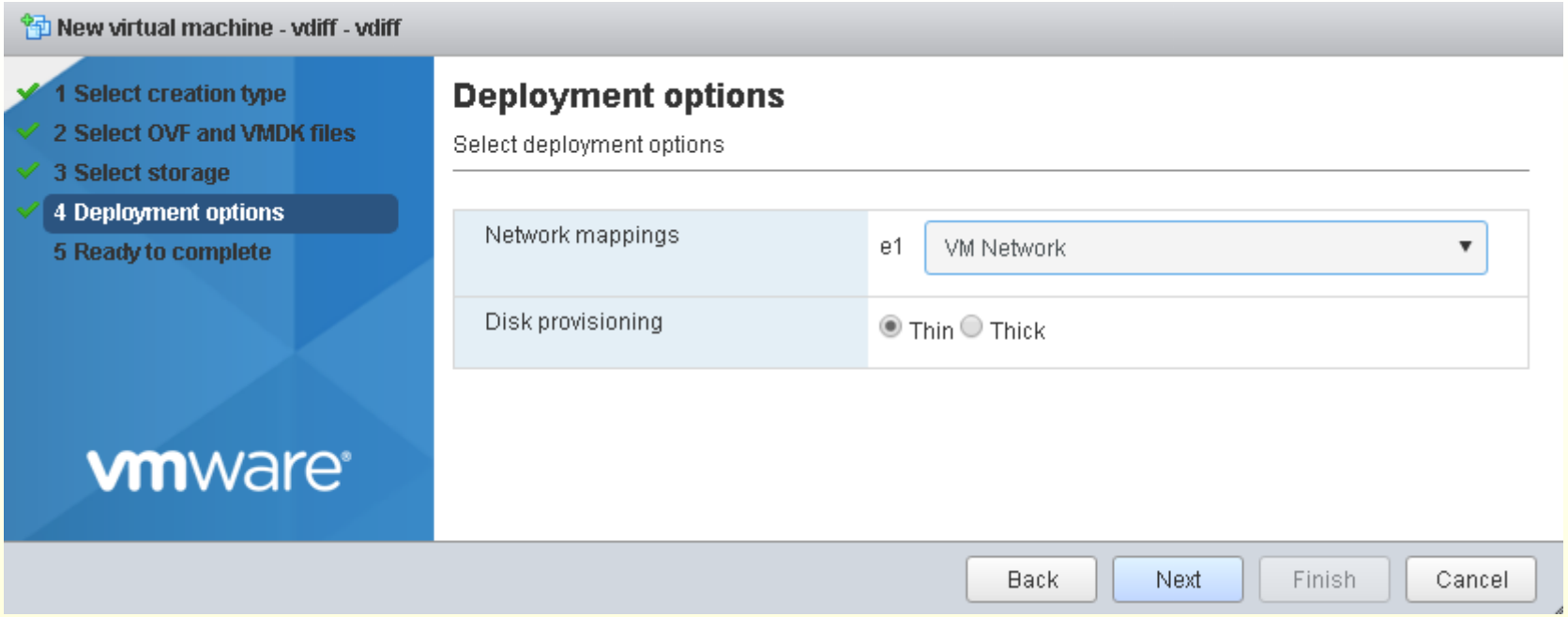


Give a name to the new VM and upload the ovf and vmdk files.

SOFT inBOX

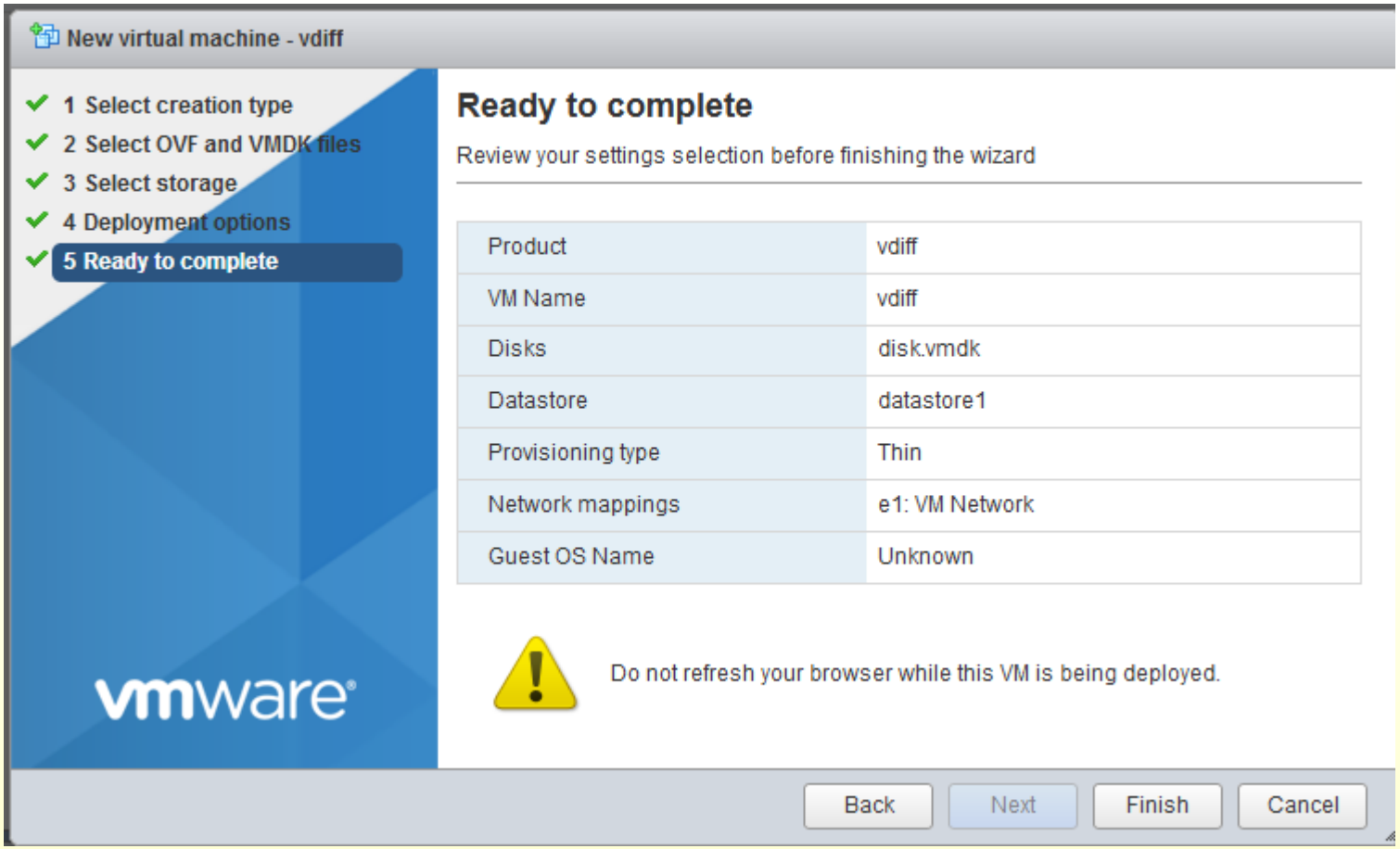
Select a storage you prefer.

SOFT inBOX



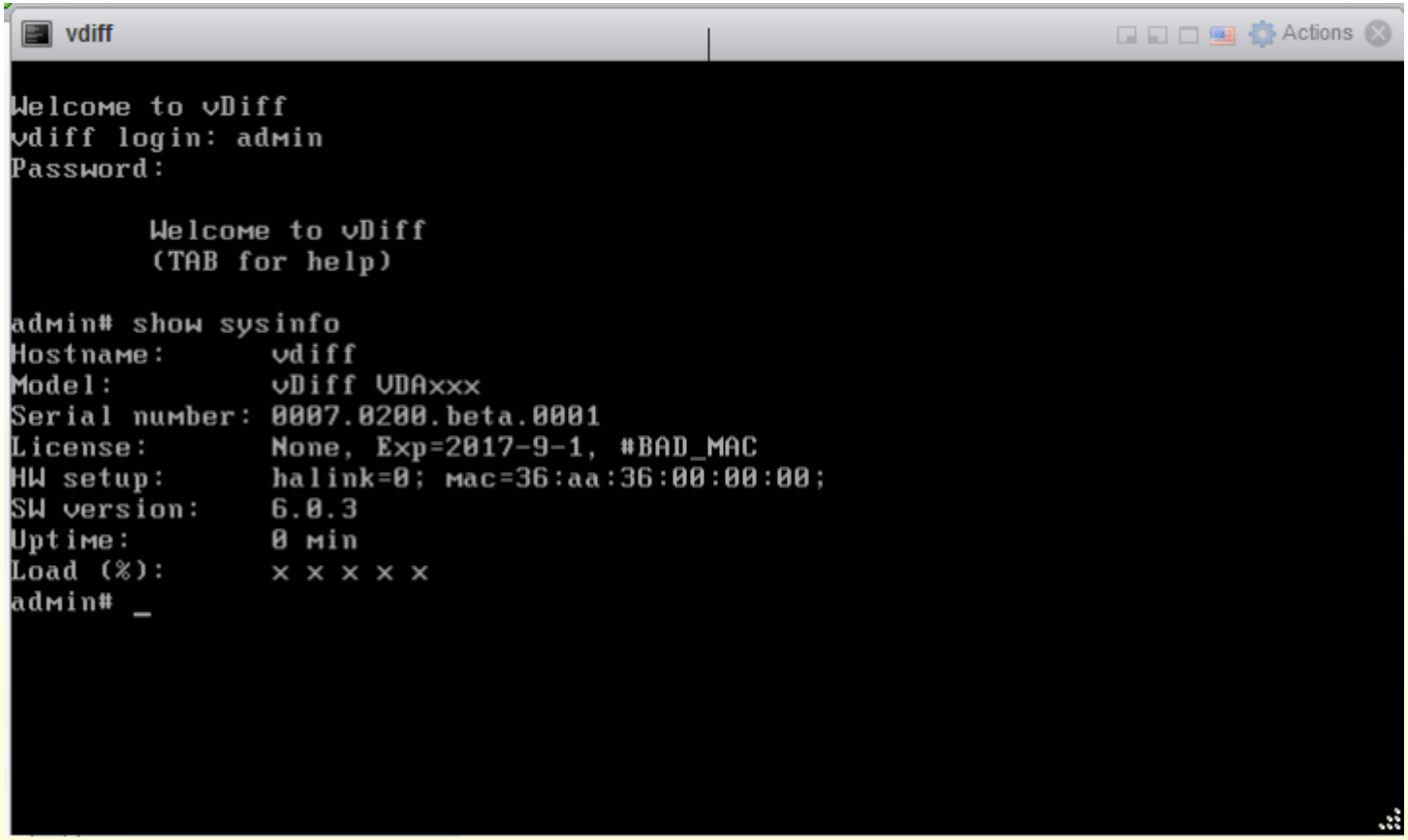
Attach e1 to the default port group “VM Network” or whatever port group you like.

SOFT inBOX



Click “Finish” and wait for the vmdk file to upload.

SOFT inBOX



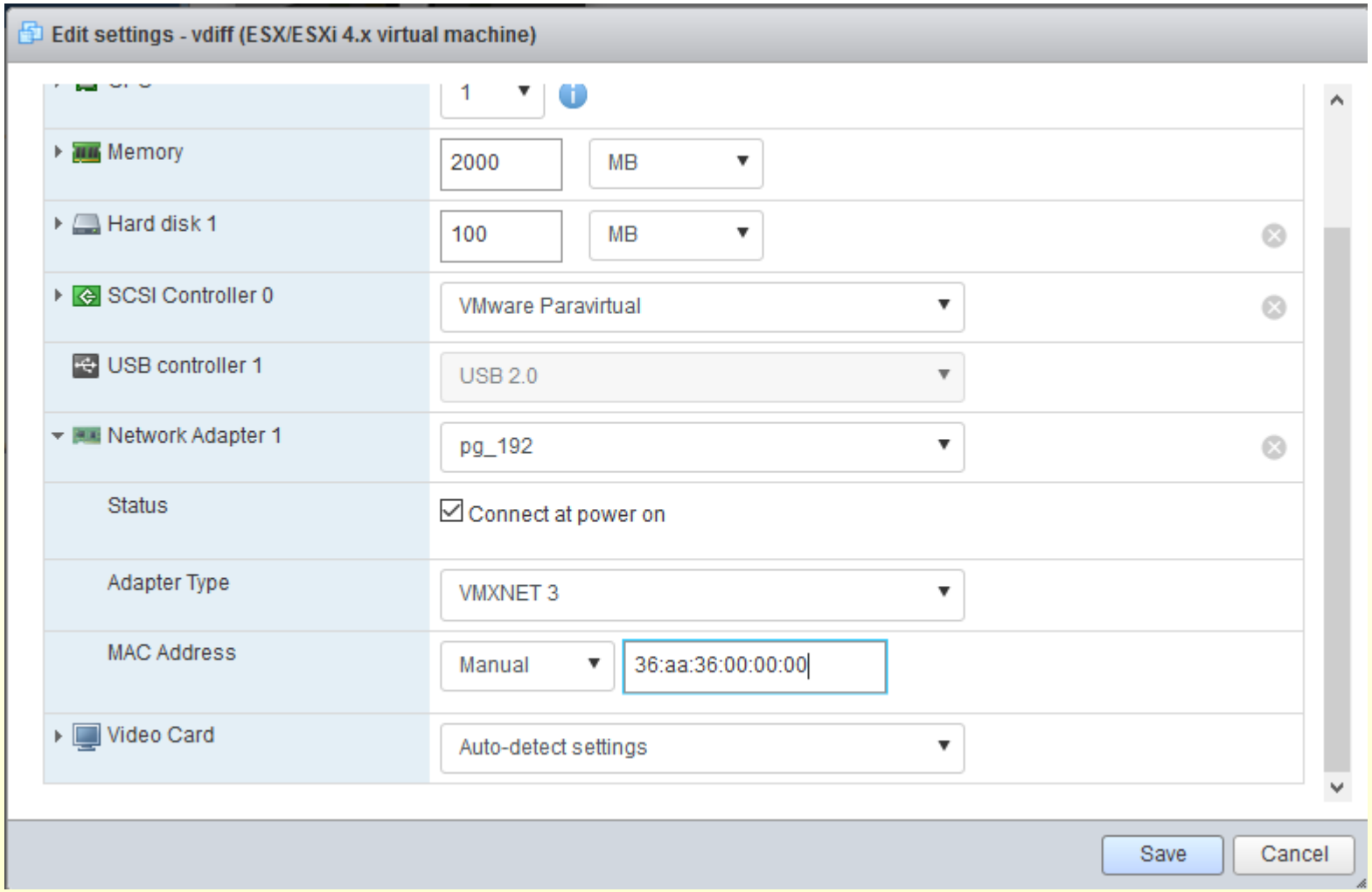
You can log into the console with username/password = admin/admin. Enter the command “show sysinfo”.

SOFT inBOX

Assign MAC address

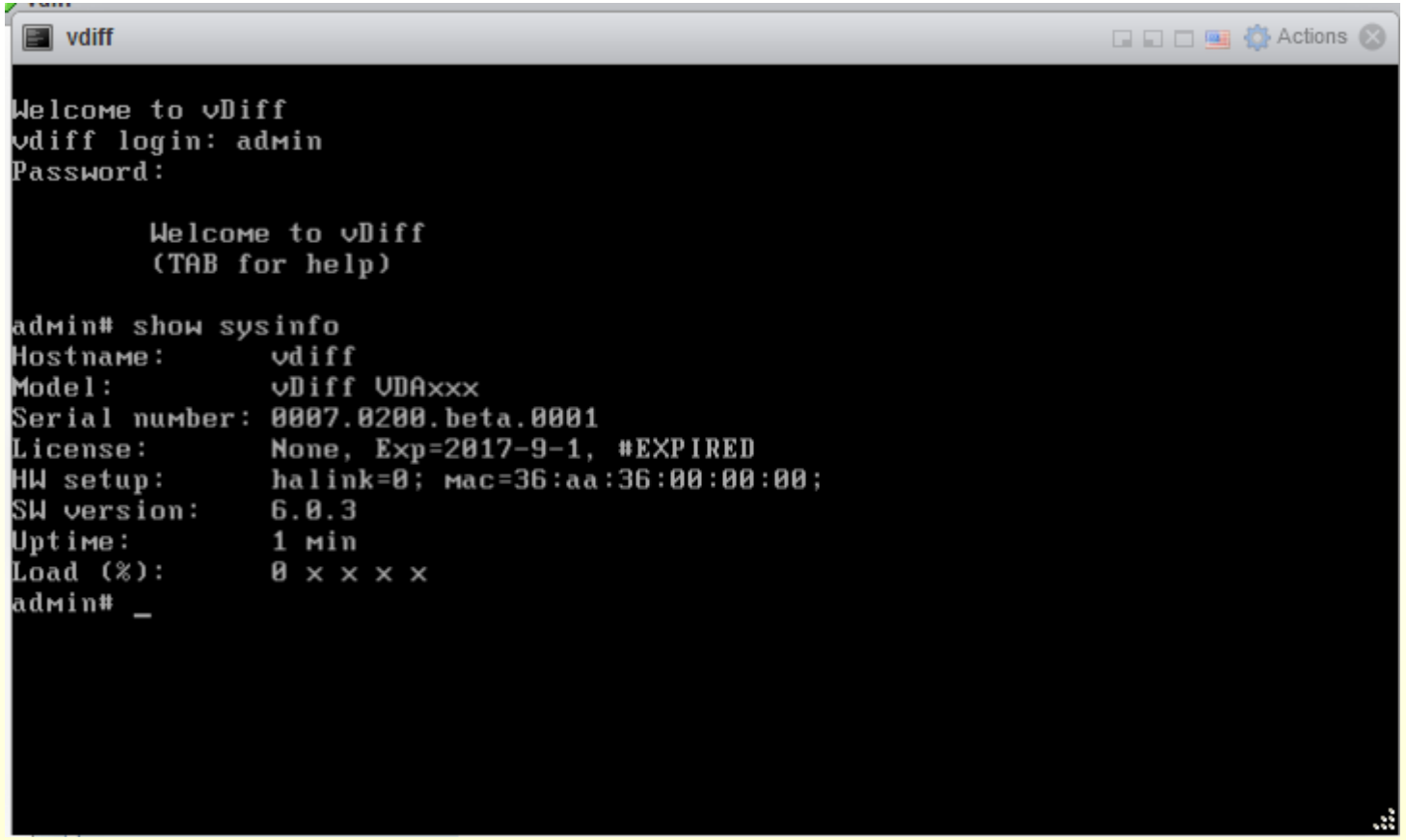
- Note the MAC address shown in the “HW setup” line. In this sample, its 36:aa:36:00:00:00.
- “Power off” the VM and “Edit” its settins.
- Expand “Network Adapter 1”, select the “MAC address” line and change it from “Automatic” to “Manual” and enter “36:aa:36:00:00:00” in the next field.
- (Cont at the following page.)

SOFT inBOX



Click “Save” when you are done.

SOFT inBOX



Power on the VM and login the console and “show sysinfo”. Check that the “#BAD_MAC” is gone in the License line.

SOFT inBOX

At this stage, you should be able to connect to the web management UI at https://192.168.1.99. Username/password is the same admin/admin.

Request for up-to-date license

- See the chapter “Request for up-to-date license” to complete the installation process.

SOFT inBOX

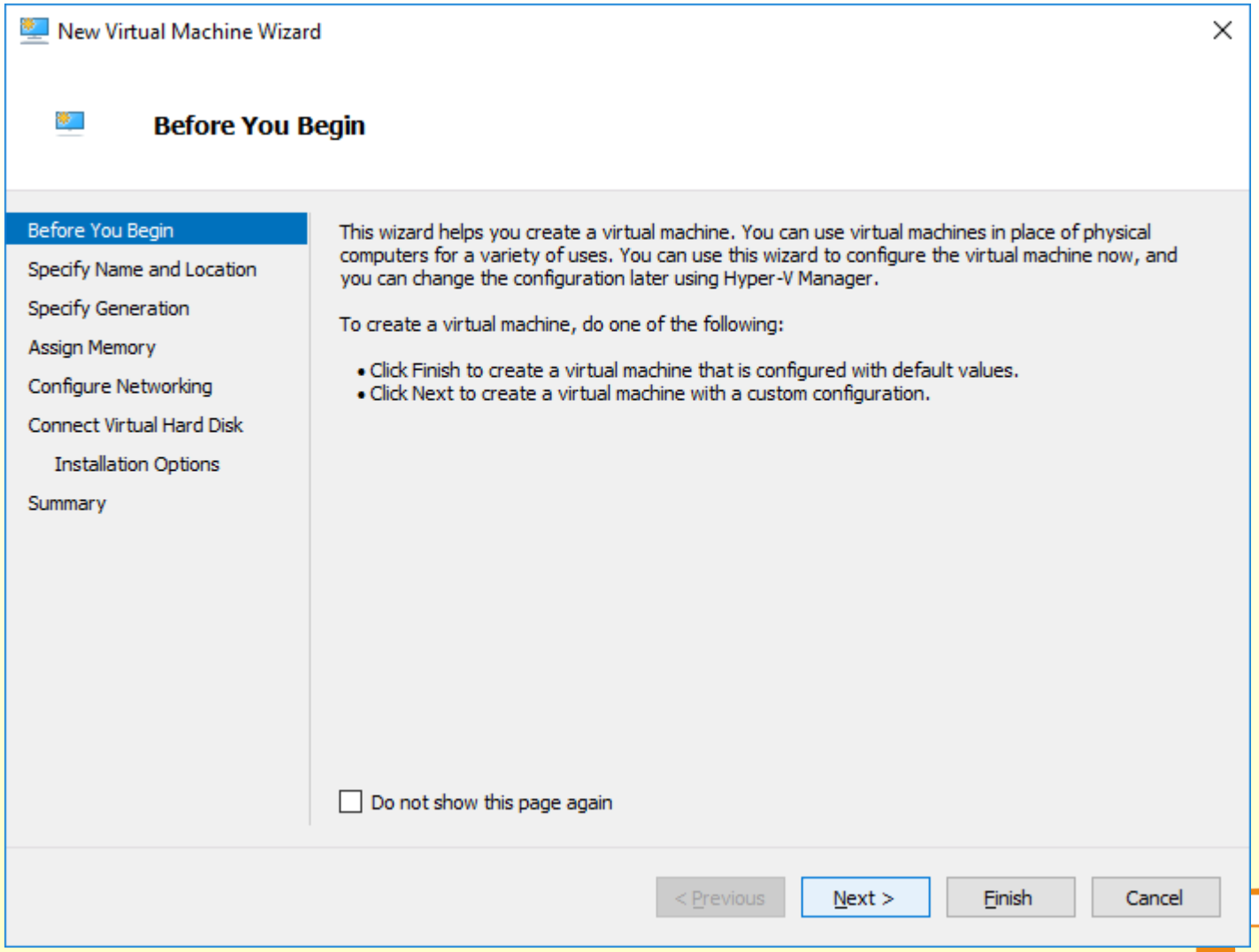
Creating a Hyper-V VM

SOFT inBOX

Extract disk.vhd

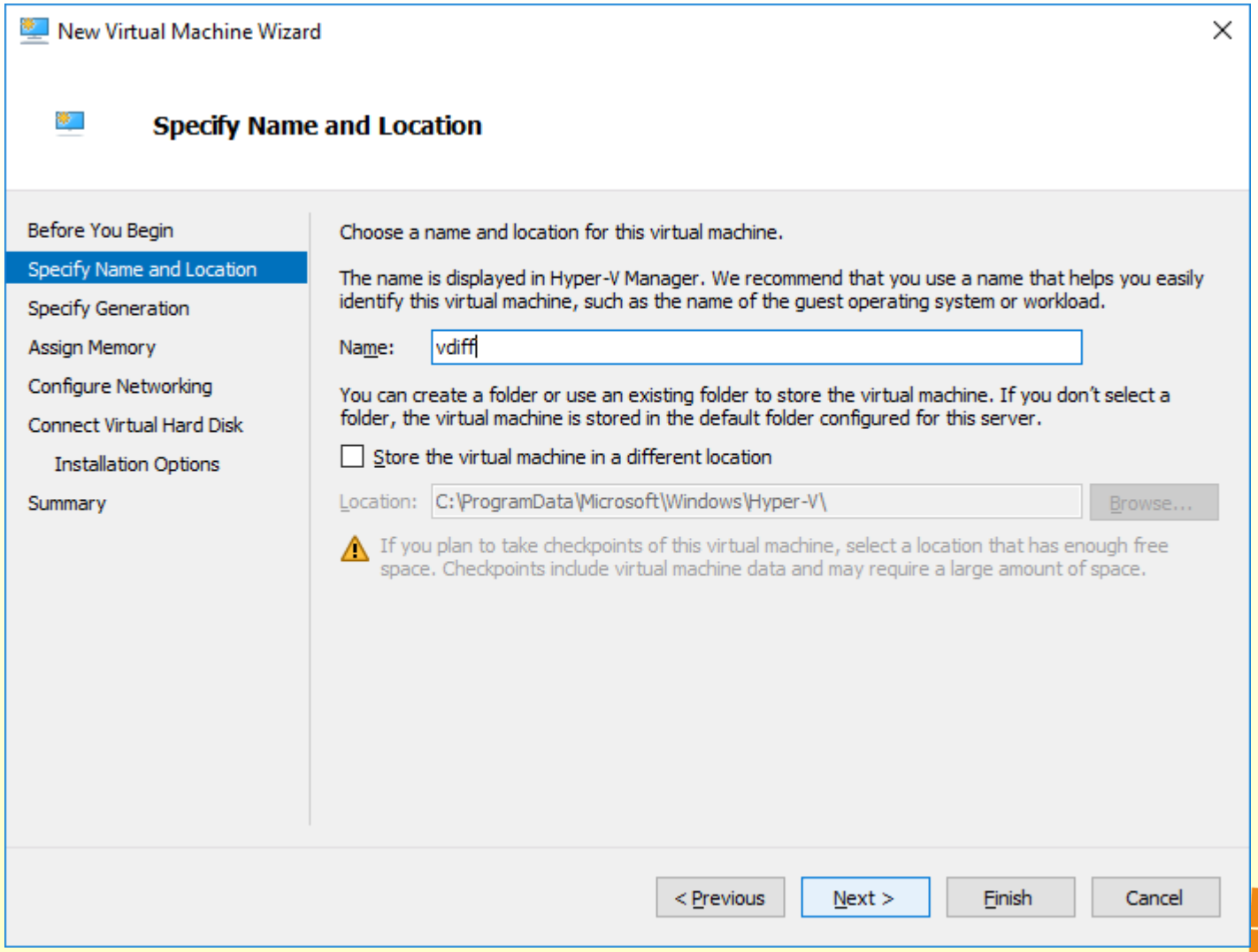
- Extract install.zip and locate disk.vhd (install/install_hyperv/disk.vhd)
- Save disk.vhd somewhere in the Hyper-V host.

“New” a “Virtual Machine” in “Hyper-V Manager.”



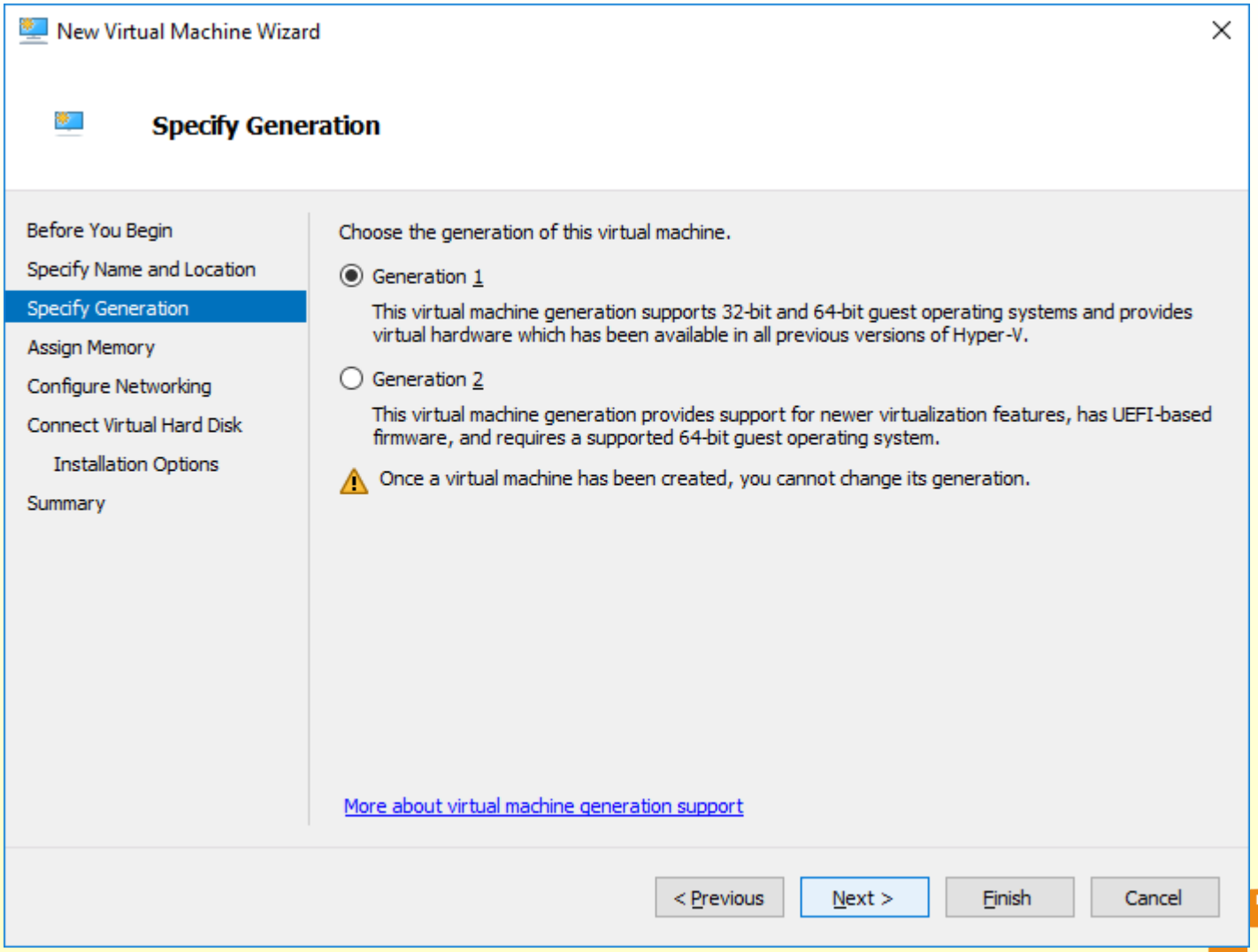
inBOX

Give it a name.

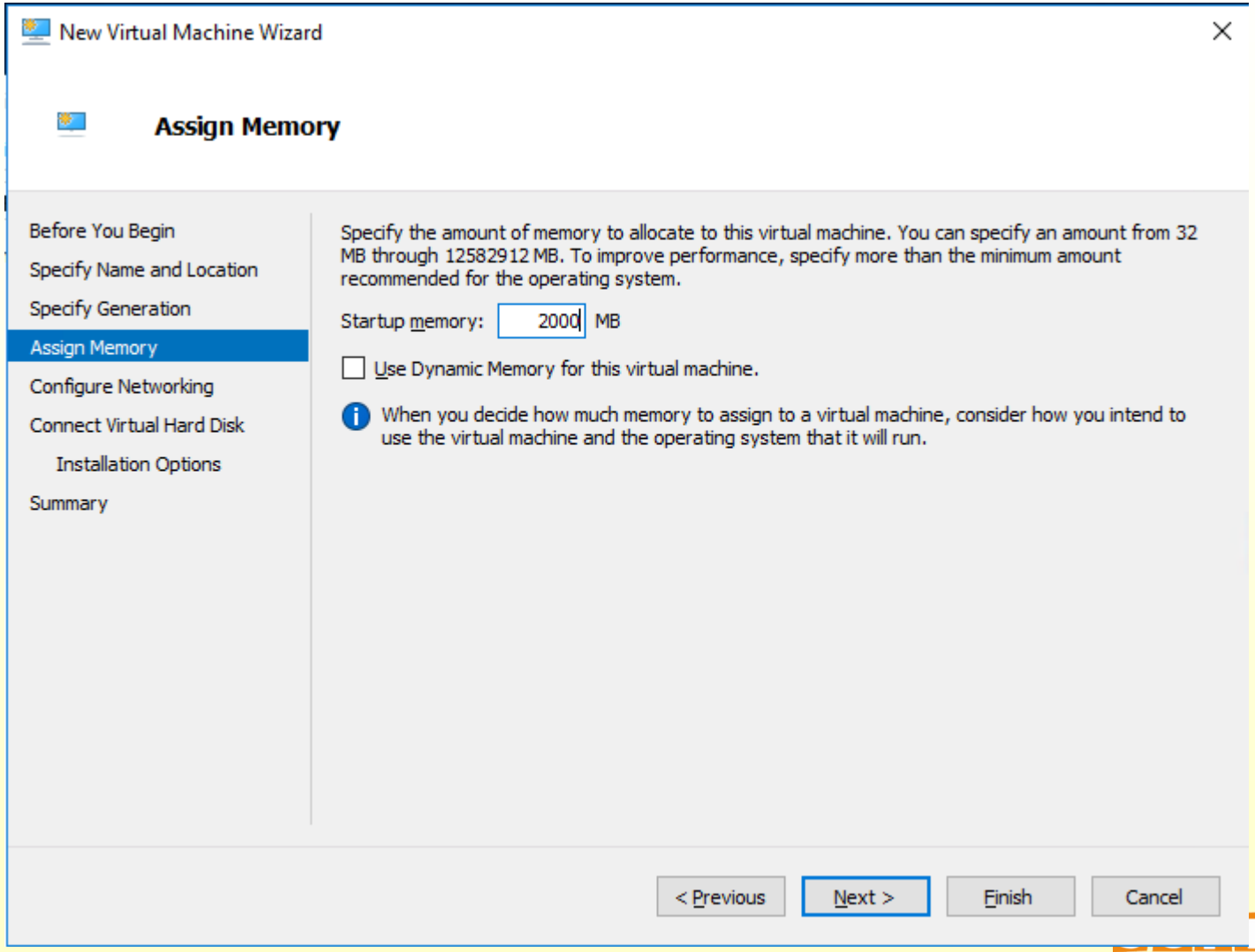


FT inBOX

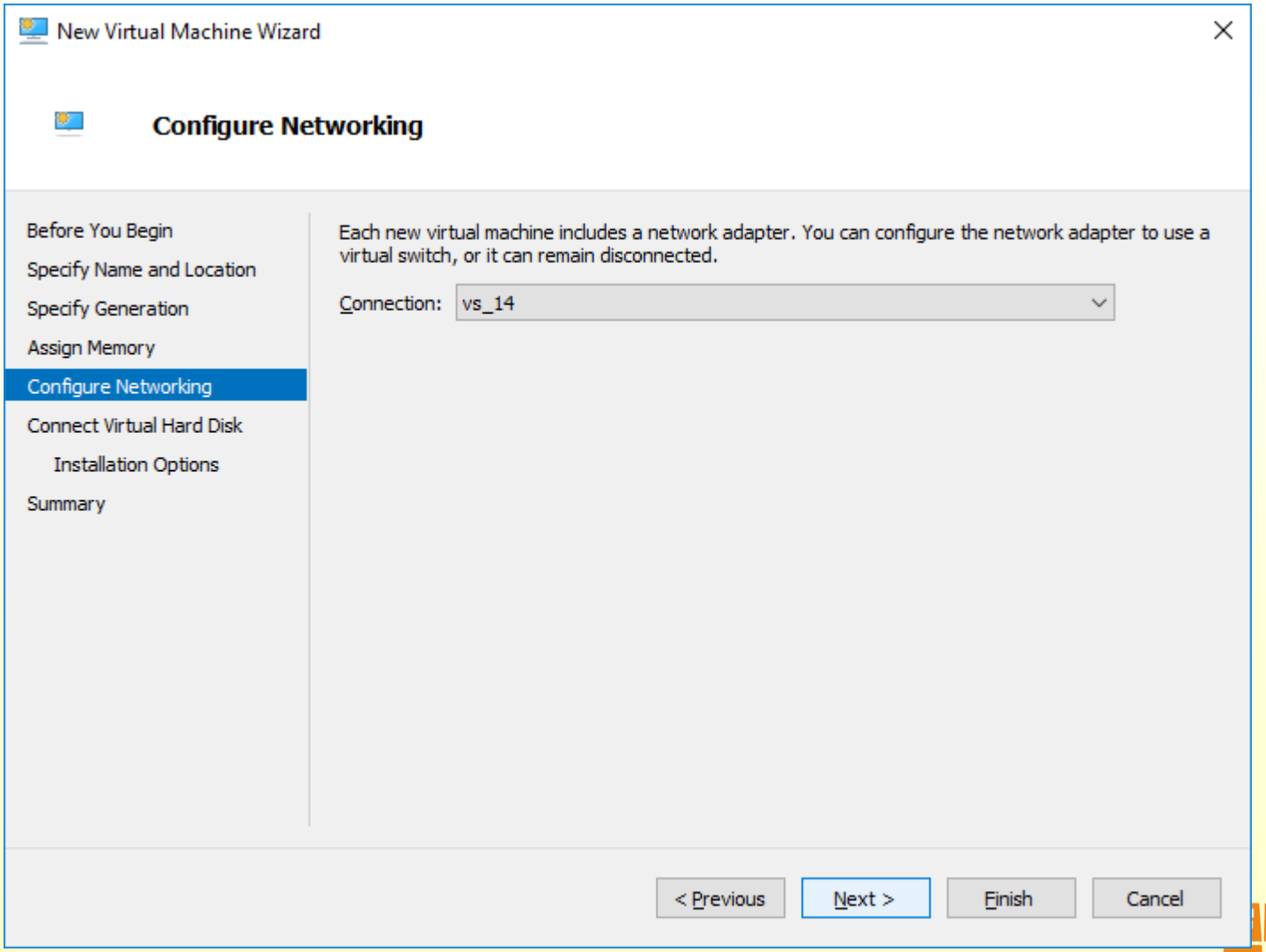
Specify “Generation 1.”



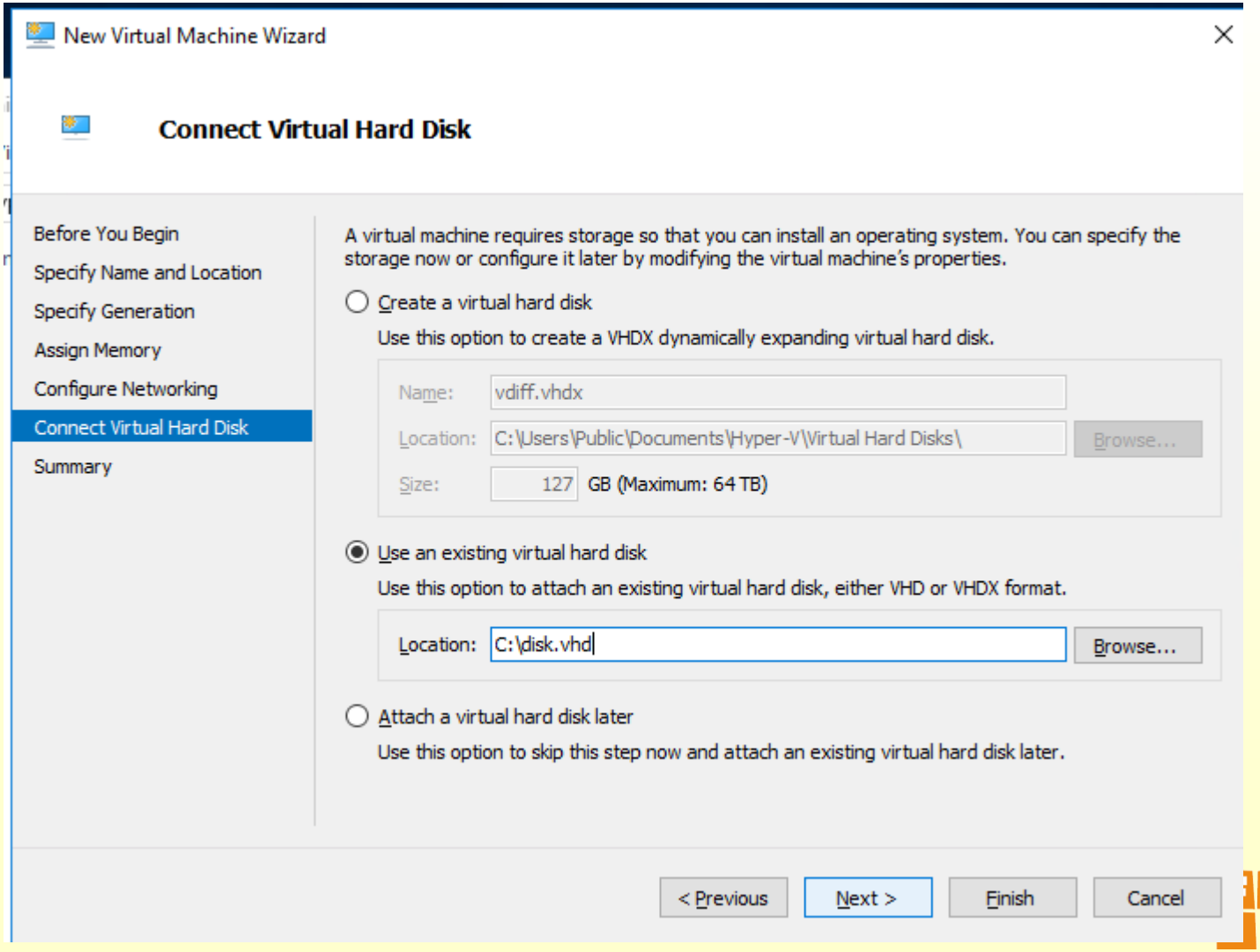
- Give it 2000MB of memory for VDA100. (Check the spec page for other models.)



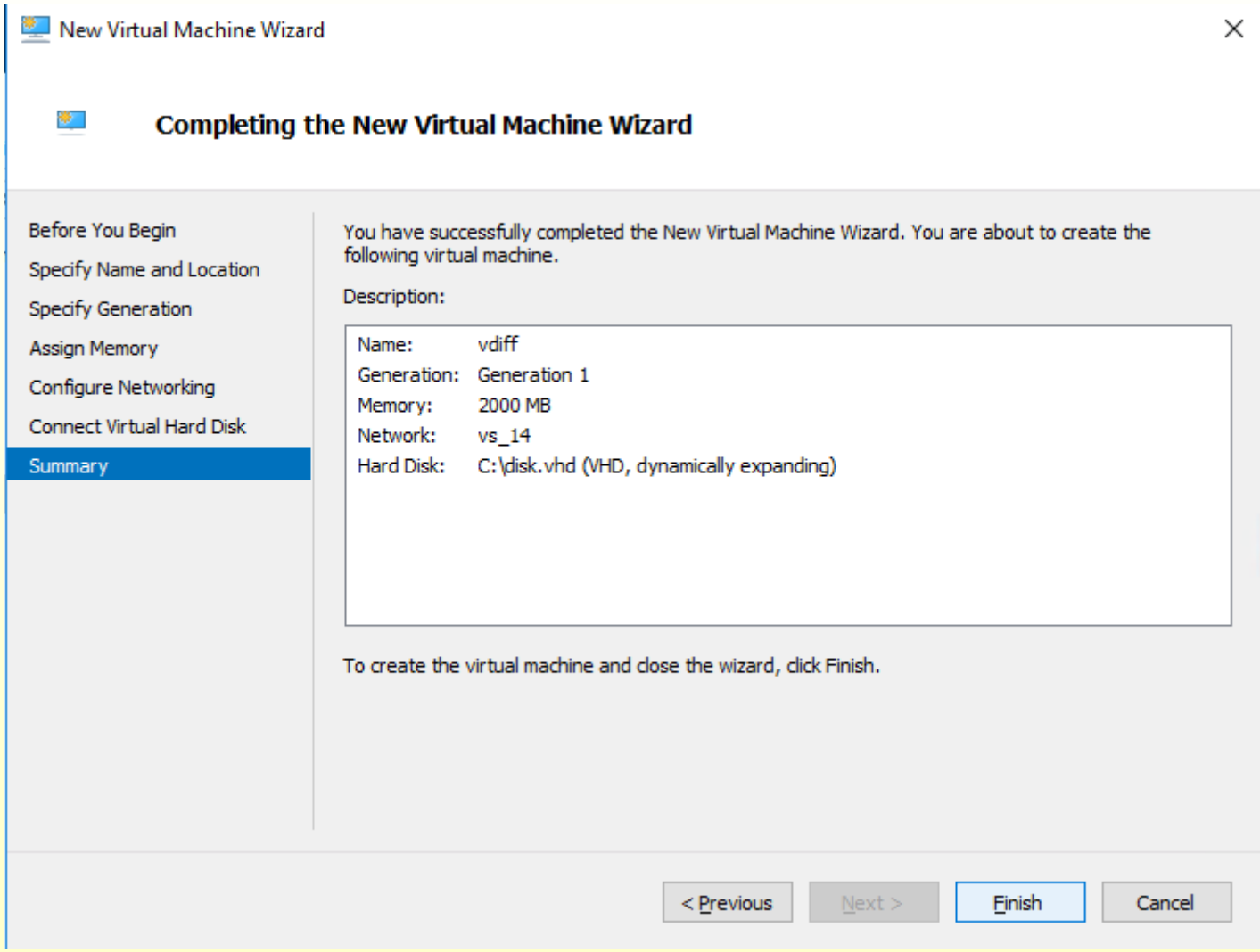
- Connect to some virtual switch.



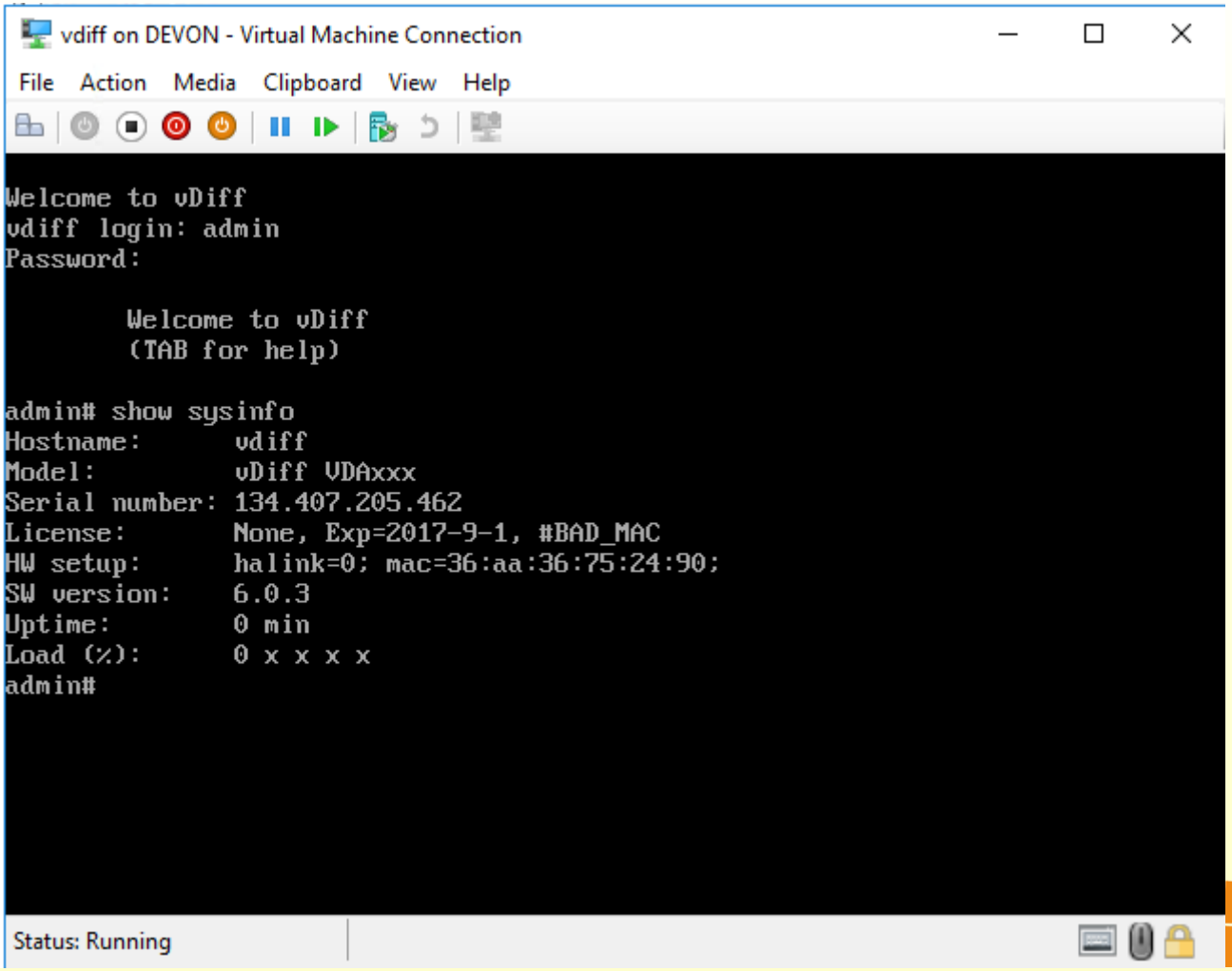
- “Use an existing virtual hard disk” and specifly the extracted disk.vhd.



- “Finish” the creation of the new virtual machine.



- Start (power on) the new VM and login with username/password = admin/admin.
- Enter the command “show sysinfo”.



Assign MAC address

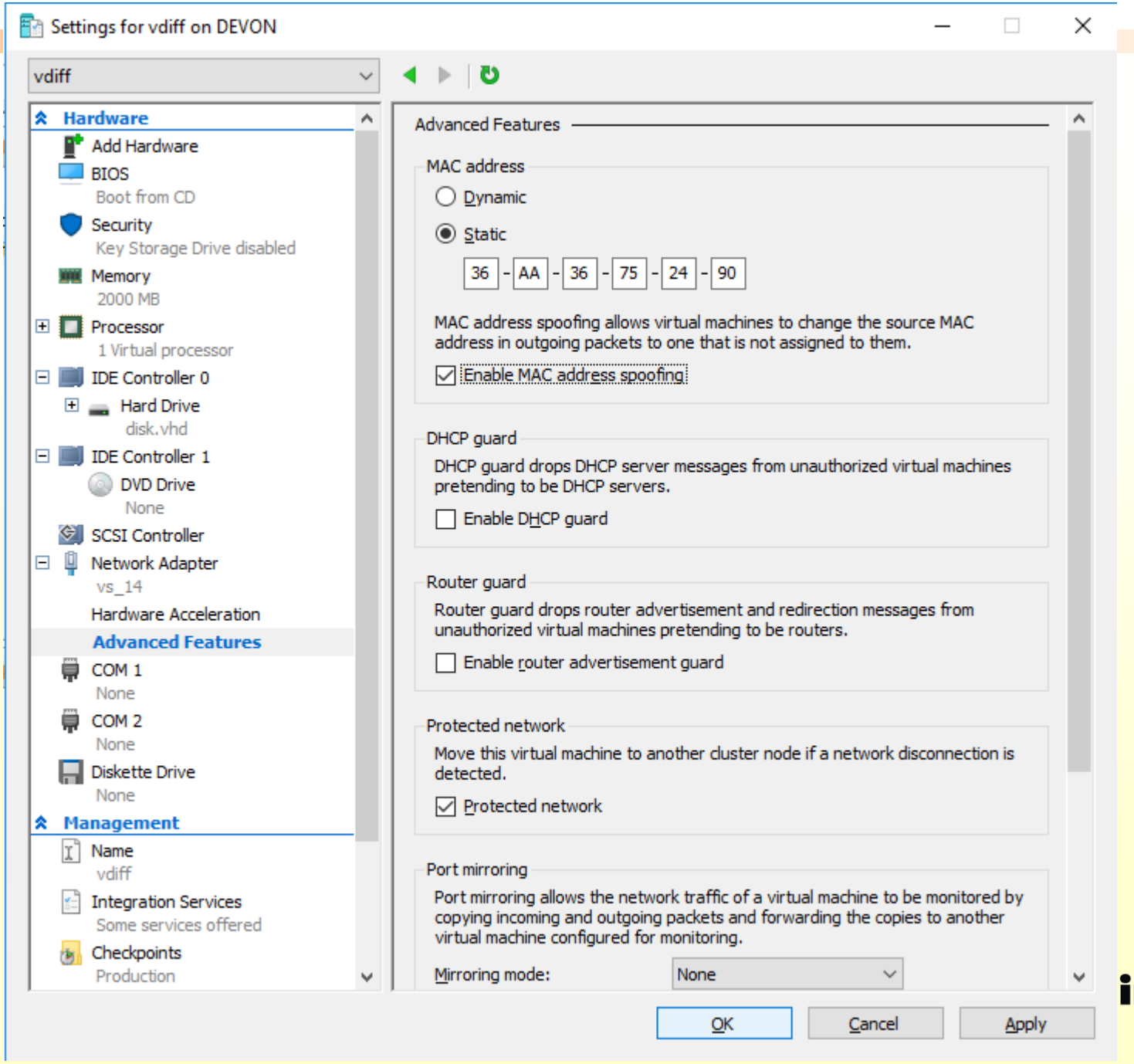
- First we must resolve the "#BAD_MAC" in the "License" line.
- Record the MAC address given in the "HW setup" line. In this example, it is 36:aa:36:75:24:90.
- "Turn off" the VM and edit its "Settings".
- Expand "Network Adapter" and click "Advanced features".

SOFT inBOX

Cont.

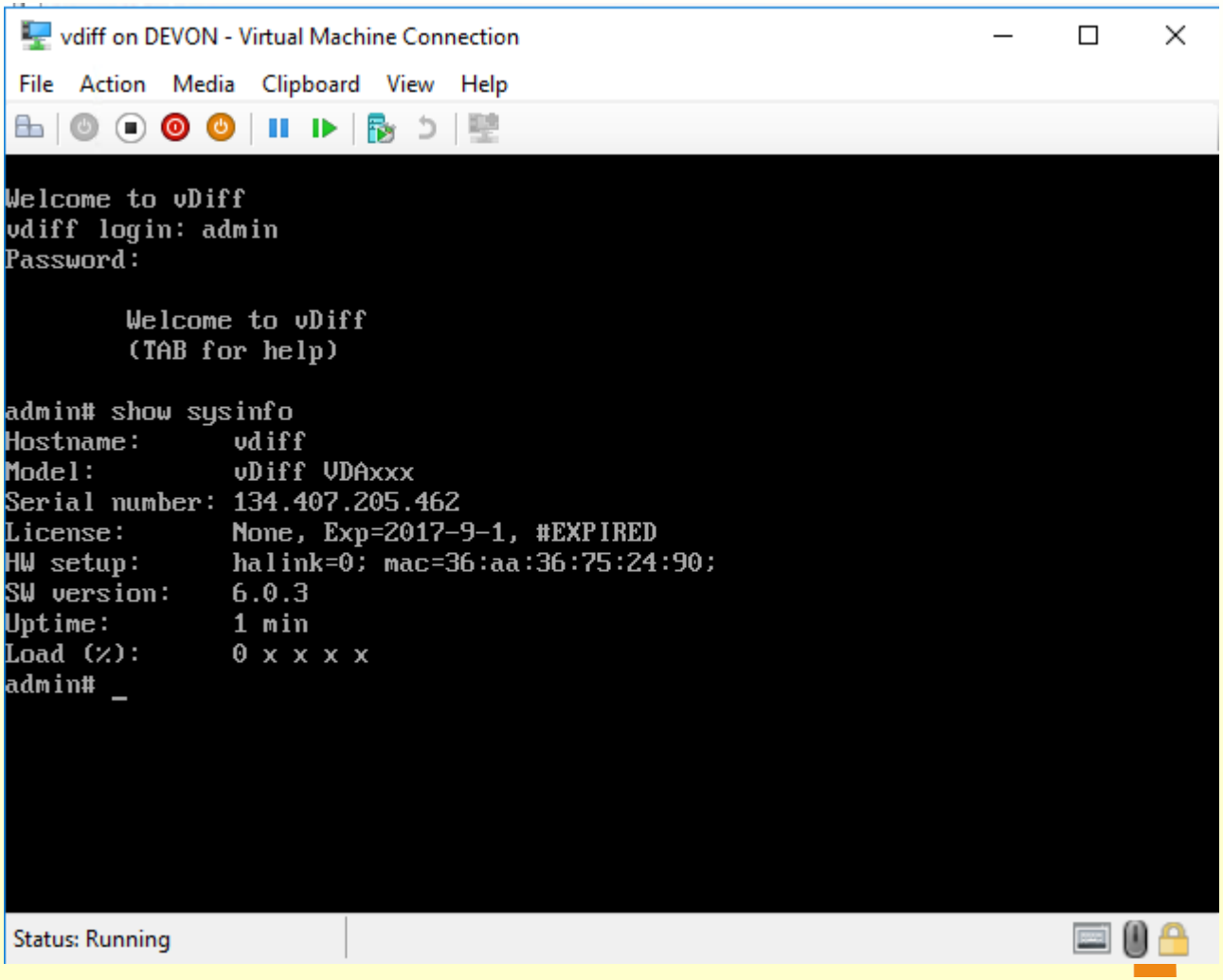
- Click “Static” and enter the MAC supplied in the previous step.
- Check “Enable MAC address spoofing”.
- Click “OK”.
- See the figure in the following page.

SOFT inBOX


Settings for vdiff on DEVON
vdiff
Hardware
Add Hardware
BIOS
Boot from CD
Security
Key Storage Drive disabled
Memory
2000 MB
Processor
1 Virtual processor
IDE Controller 0
Hard Drive
disk.vhd
IDE Controller 1
DVD Drive
None
SCSI Controller
Network Adapter
vs_14
Hardware Acceleration
Advanced Features
COM 1
None
COM 2
None
Diskette Drive
None
Management
Name
vdiff
Integration Services
Some services offered
Checkpoints
Production
Advanced Features
MAC address
Dynamic
Static
36 - AA - 36 - 75 - 24 - 90
MAC address spoofing allows virtual machines to change the source MAC address in outgoing packets to one that is not assigned to them.
Enable MAC address spoofing
DHCP guard
DHCP guard drops DHCP server messages from unauthorized virtual machines pretending to be DHCP servers.
Enable DHCP guard
Router guard
Router guard drops router advertisement and redirection messages from unauthorized virtual machines pretending to be routers.
Enable router advertisement guard
Protected network
Move this virtual machine to another cluster node if a network disconnection is detected.
Protected network
Port mirroring
Port mirroring allows the network traffic of a virtual machine to be monitored by copying incoming and outgoing packets and forwarding the copies to another virtual machine configured for monitoring.
Mirroring mode:
None
OK
Cancel
Apply

inBOX

- Start the VM again and login the console.
- “show sysinfo” and verify that “#BAD_MAC” is gone.



Request for new license

- However, this time, it show “#EXPIRED” which means that the license is expired.
- Please see the chapter “Request for new license” to resolve it.

SOFT inBOX

Creating a Xen DomU

SOFT inBOX

Install files

- Related files in install.zip are:

  install/install_xen/disk.bin

  install/install_xen/config_sample.1

  install/install_xen/config_sample.2

- Use config_sample.1 as the starting point. Edit it with the following notes:
- Memory size: it is 2000 in the sample. Change it to your model.
- vif bridge name: bridge0 in the sample.
- Disk file location: /home/xen/vdiff/disk.bin in the sample.
- Boot vdiff with something like “xl create -c config_sample”.
- Check config_sample.2 for additional Ethernet ports.

Request for new license

SOFT inBOX

- Log in the web management UI.
- Go to the “Tools > System” page.
- Click “Request for up-to-date license”.
- You will see “200 Operation completed successfully. Please check email.”
- Check you email. and download “upgrade_license.bin”
- Upload the file in “Upload kernel/license” block in “Tools > System” page
- Reboot

SOFT inBOX

- Log in the system and check “System information” block in “View > System info” page.
- Check that “#EXPIRED” is gone in the “License” line.
- Also check that your model name is correct in the “Model” line.

SOFT inBOX