Същност на Виртуализацията

Виртуални мрежи
Видове мрежови връзки на ВМ
Виртуални комутатори и др.
Виртуални firewall и port-forwarding

доц. д-р А. Пенев

Съдържание

1. Видове мрежови връзки на виртуалните машини;
2. Виртуални комутатори и др.;
3. Виртуални firewall и port-forwarding;

Видове Мрежови Връзки на ВМ

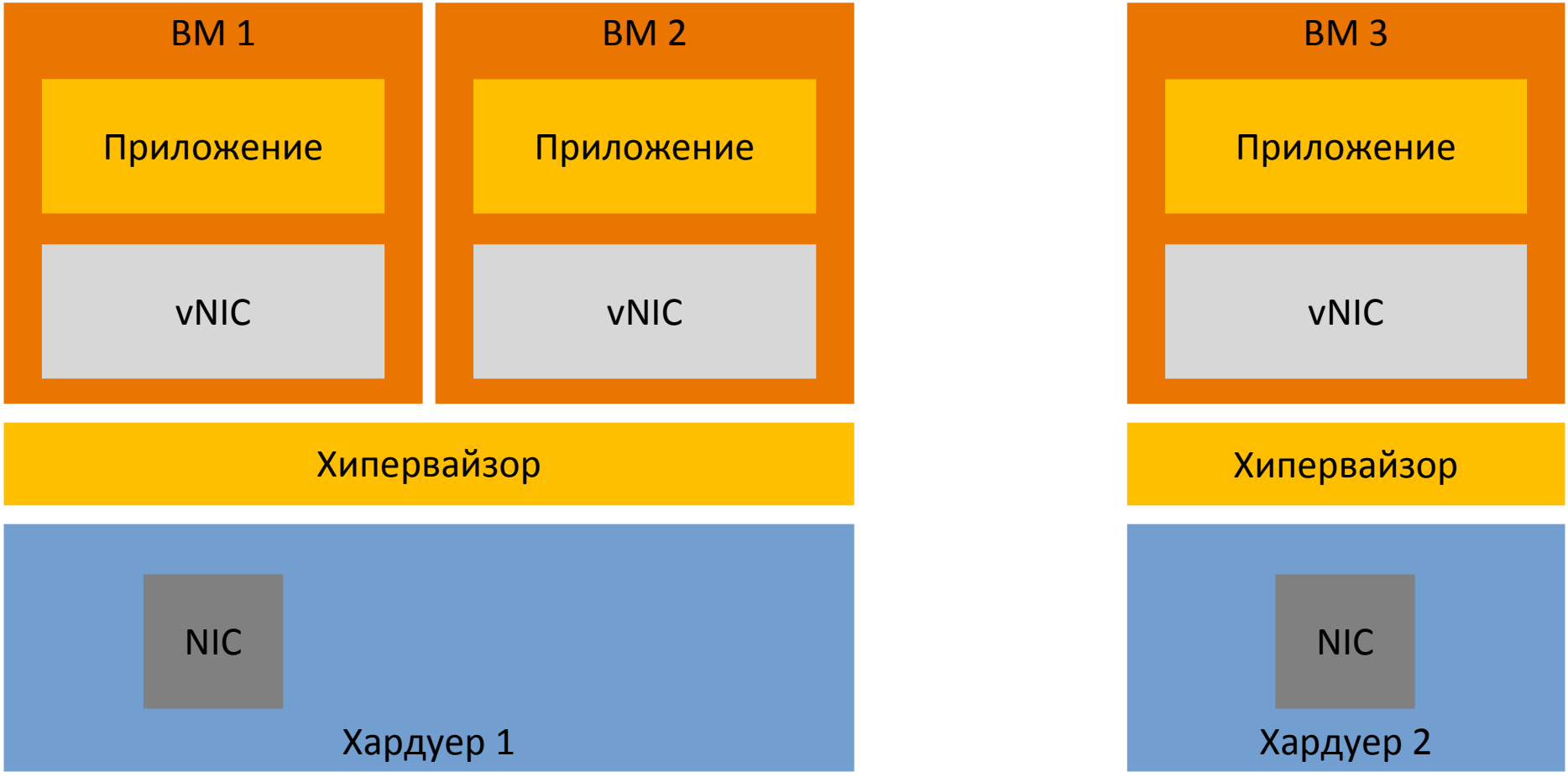
Видове връзки на vNIC с хост машината

- **Без връзка (No connection)** – ВМ (нейната vNIC) е напълно изолирана и няма никаква връзка навън т.е. нито с хоста, нито с неговите външни мрежи, нито с други виртуални машини;
- **Вътрешна (Internal)** – ВМ е изолирана от външната среда (вкл. от Host), но има връзка с другите ВМ;
- **Само хост (Host-Only)** – ВМ има възможни комуникации само в рамките на Host-а, но не и с LAN, Internet и др. извън него;
- **NAT** – ВМ има изходящи връзки (през NAT) към хоста, както и към неговите външни мрежи (LAN, Интернет и др.). Входящите връзки от хоста и неговите външни мрежи сатава само изрично през Port Forwarding;
- **NAT мрежа (NAT network)** – предлага възможностите на NAT, като в допълнение различните виртуални машини с този тип мрежа имат двупосочна връзка помежду си;
- **Мостов адаптер (Bridge)** – vNIC е директно свързан (bridged) с NIC на хоста и има същите възможности за връзка както него т.е. навсякъде (Host, LAN, Internet, VMs, и др.);

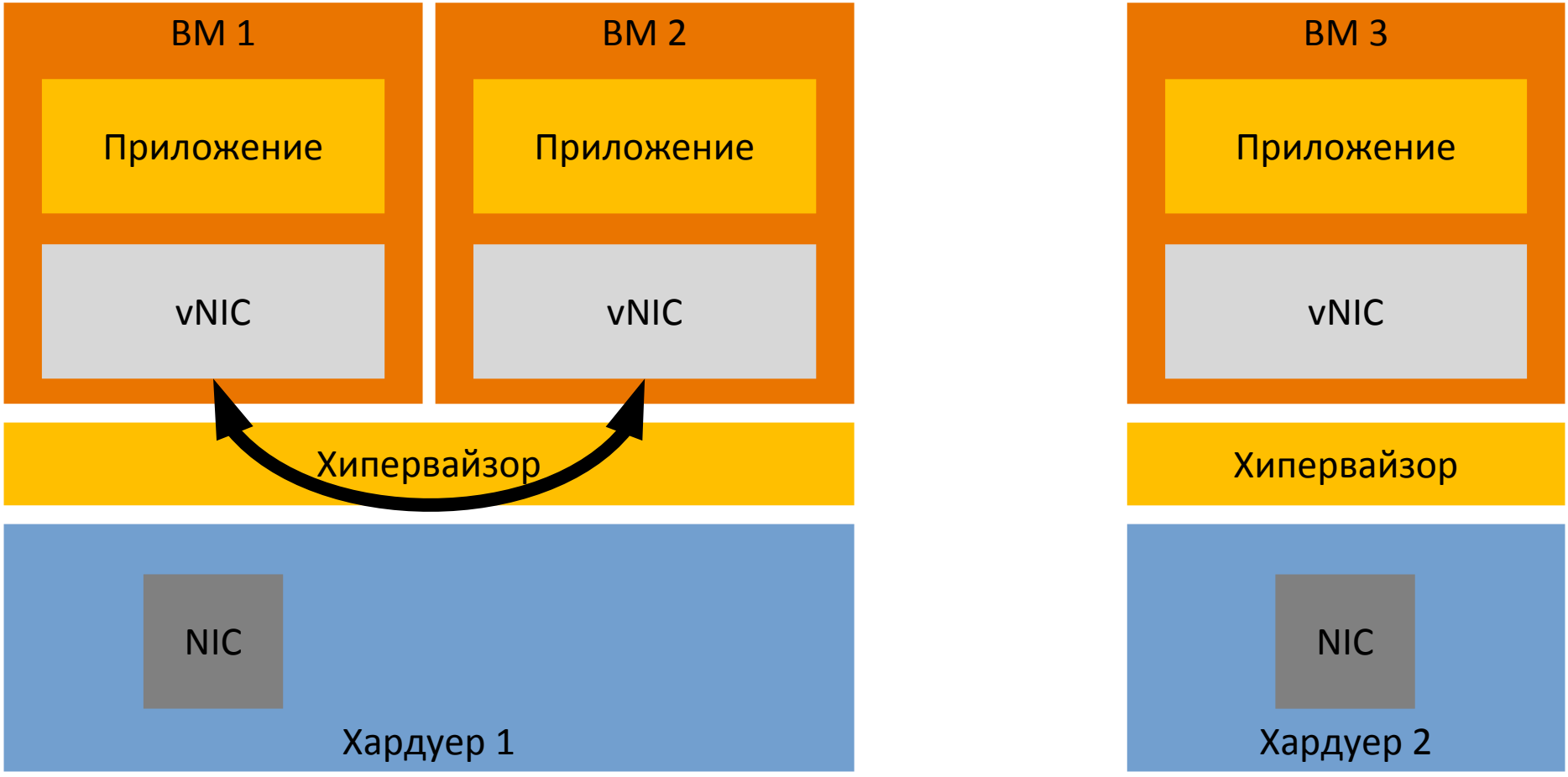
Видове връзки на vNIC с хост машината

Режим	VM → Host	VM ← Host	VM1 ↔ VM2	VM → Net/LAN	VM ← Net/LAN
Disconnect	–	–	–	–	–
Internal	–	–	+	–	–
Host-only	+	+	+	–	–
NAT	+	Port forward	–	+	Port forward
NAT network	+	Port forward	+	+	Port forward
Bridged	+	+	+	+	+

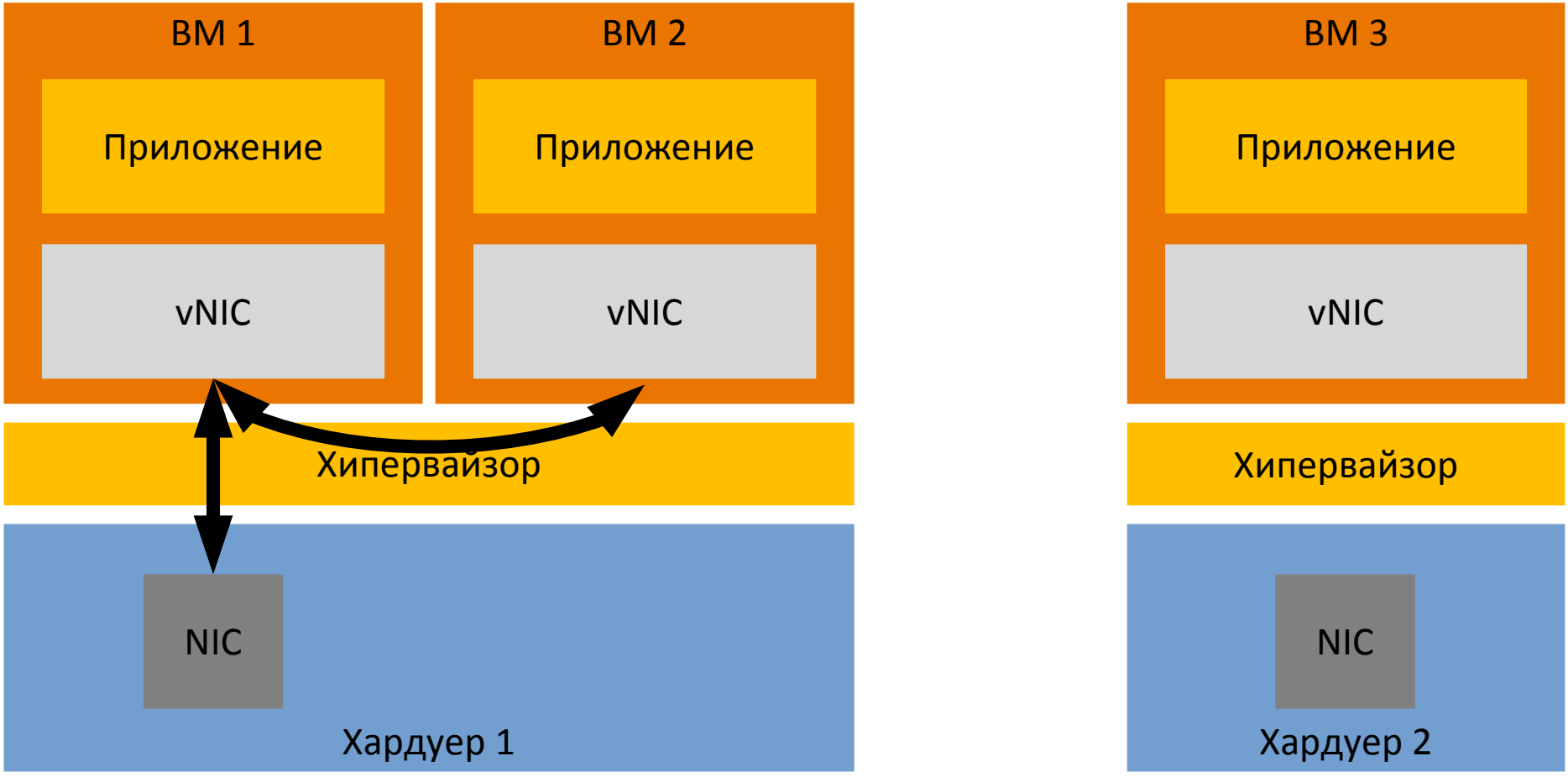
Без връзка


ВМ 1
Приложение
vNIC
ВМ 2
Приложение
vNIC
ВМ 3
Приложение
vNIC
Хипервайзор
Хипервайзор
NIC
Хардуер 1
NIC
Хардуер 2

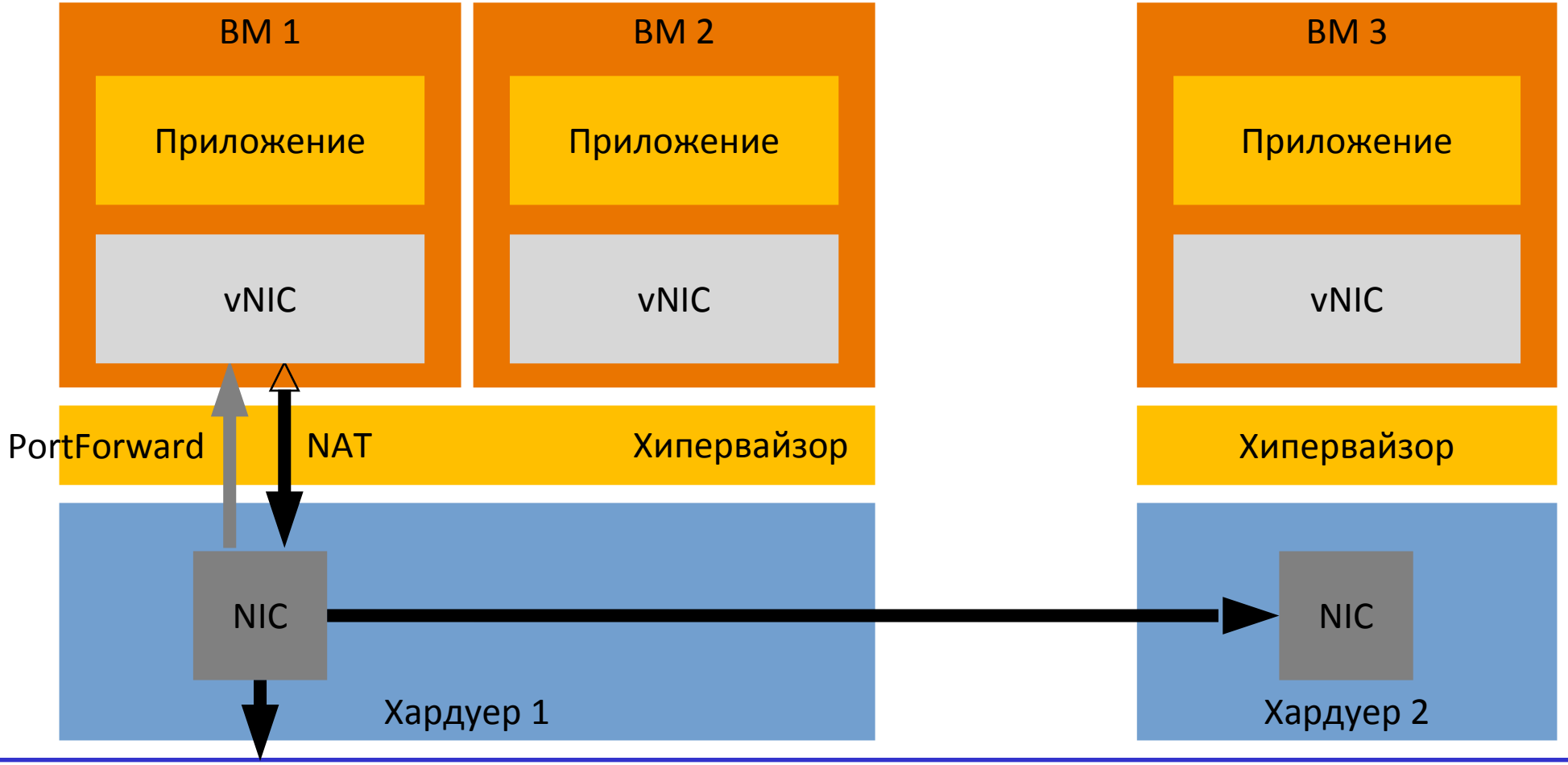
Вътрешна (Internal)



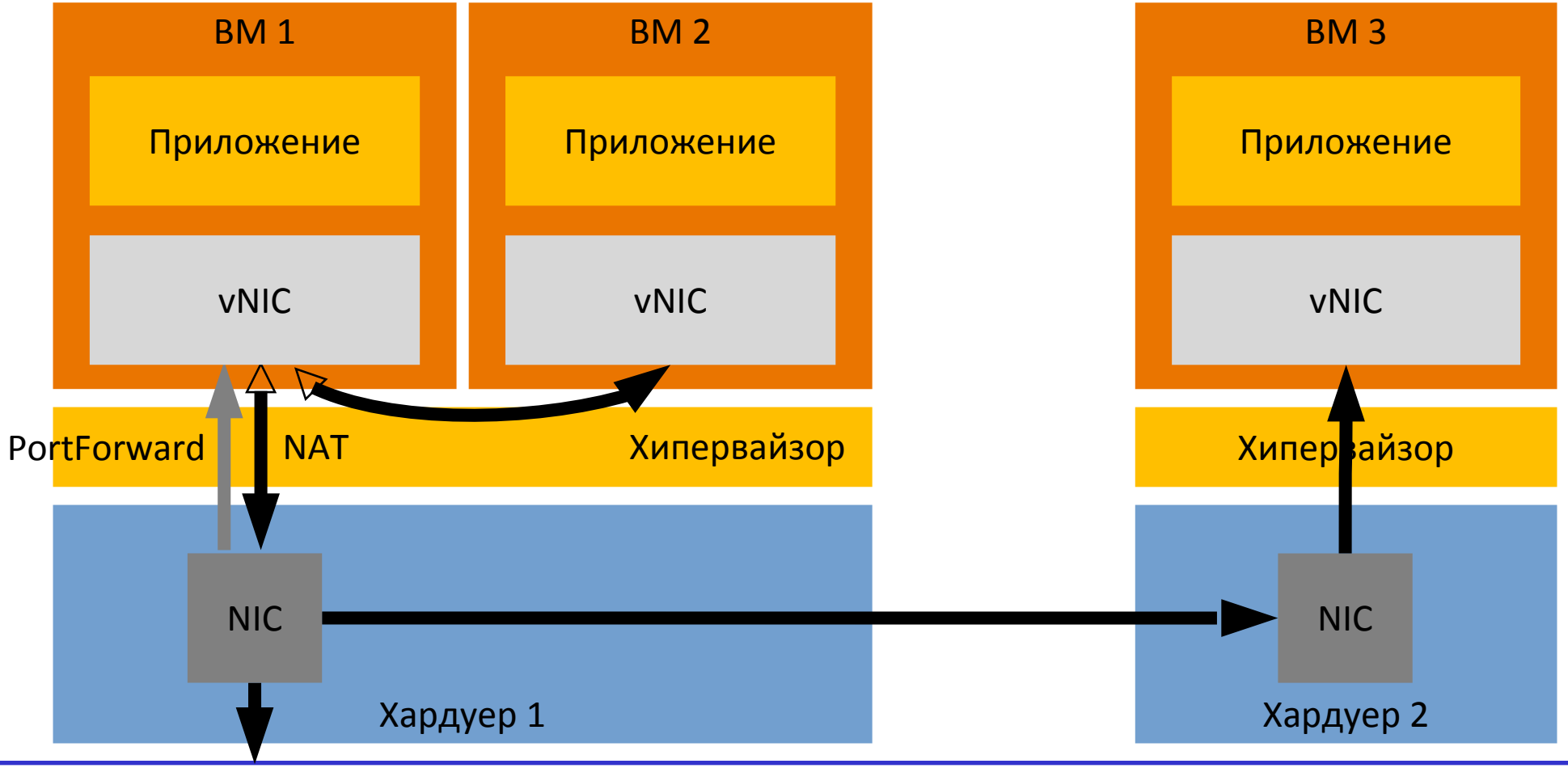
Само хост (Host-Only)



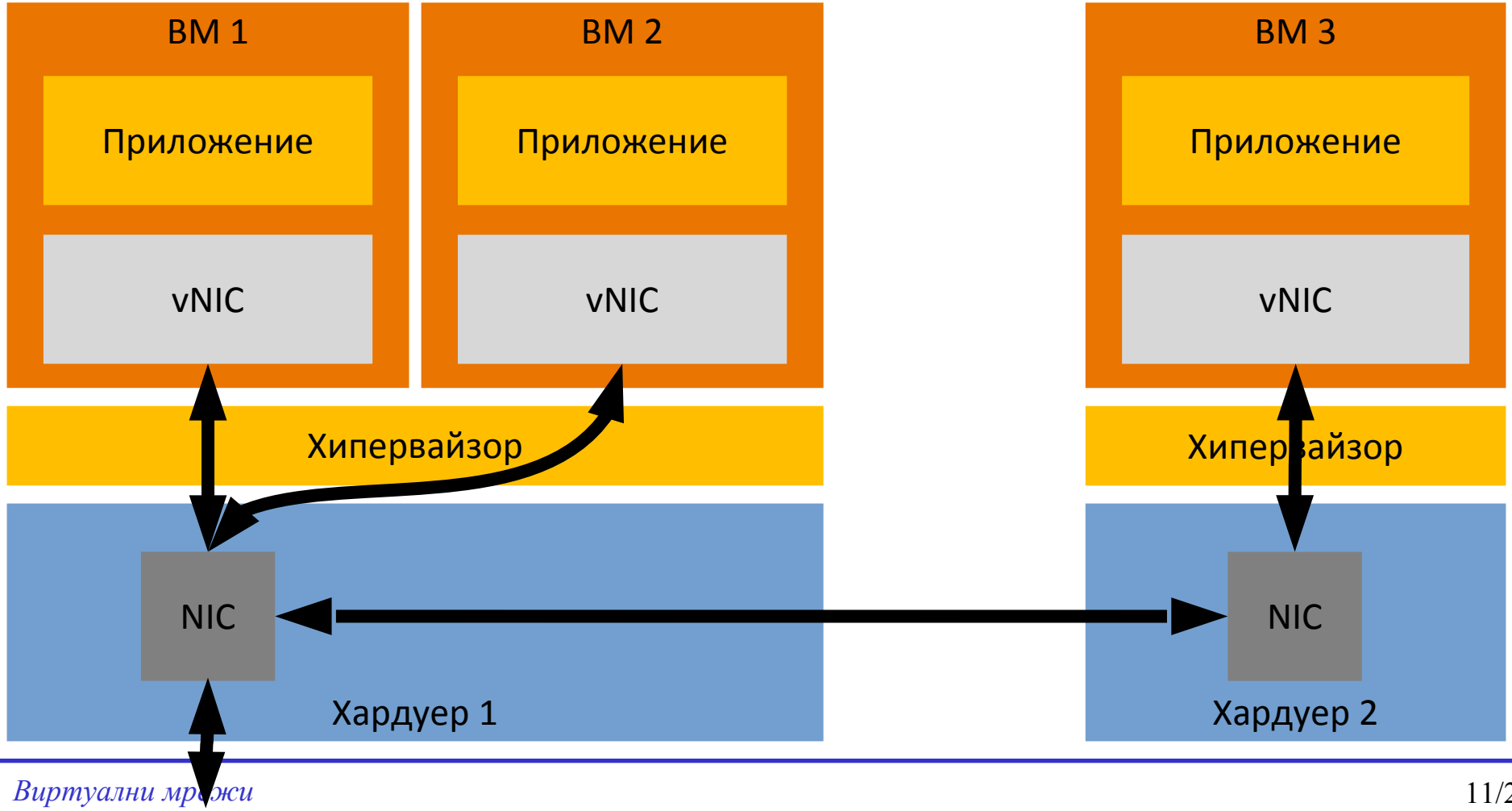
NAT


ВМ 1
Приложение
vNIC
ВМ 2
Приложение
vNIC
ВМ 3
Приложение
vNIC
PortForward
NAT
Хипервайзор
Хипервайзор
NIC
NIC
Хардуер 1
Хардуер 2

NAT мрежа (NAT network)

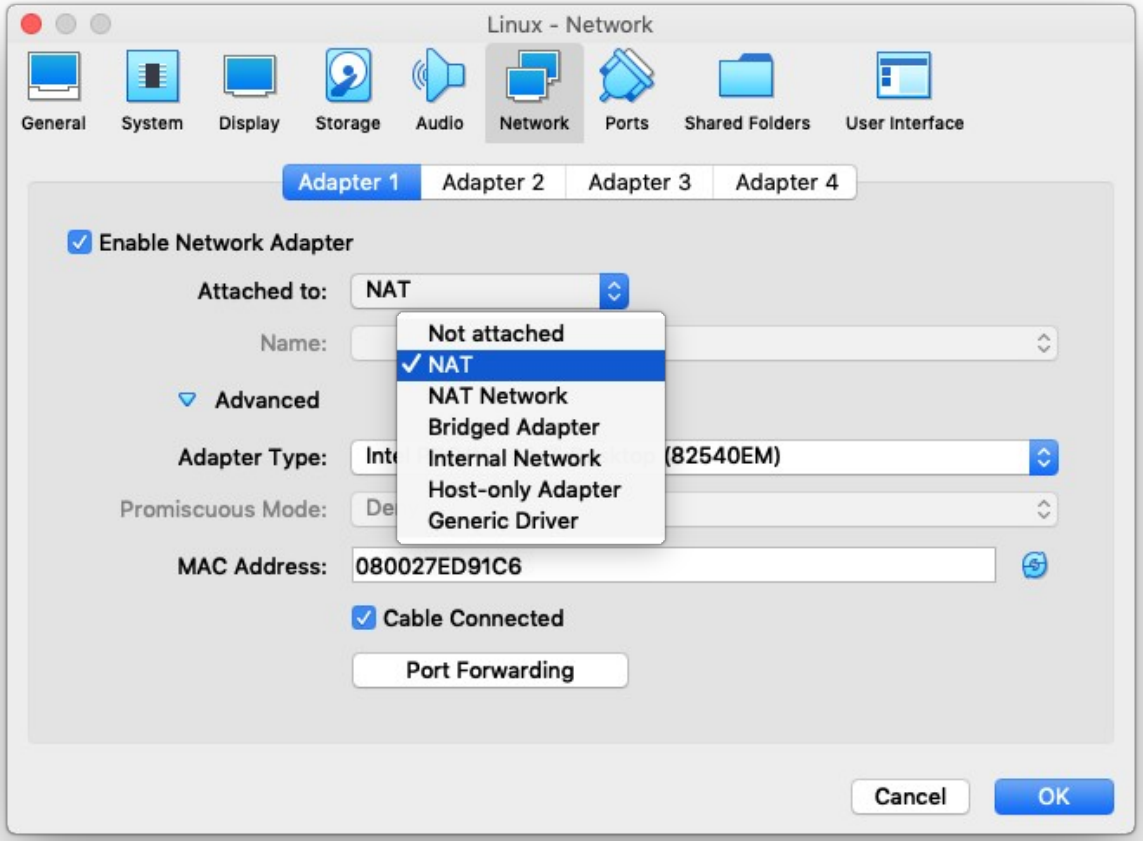


Мостов адаптер (Bridge)



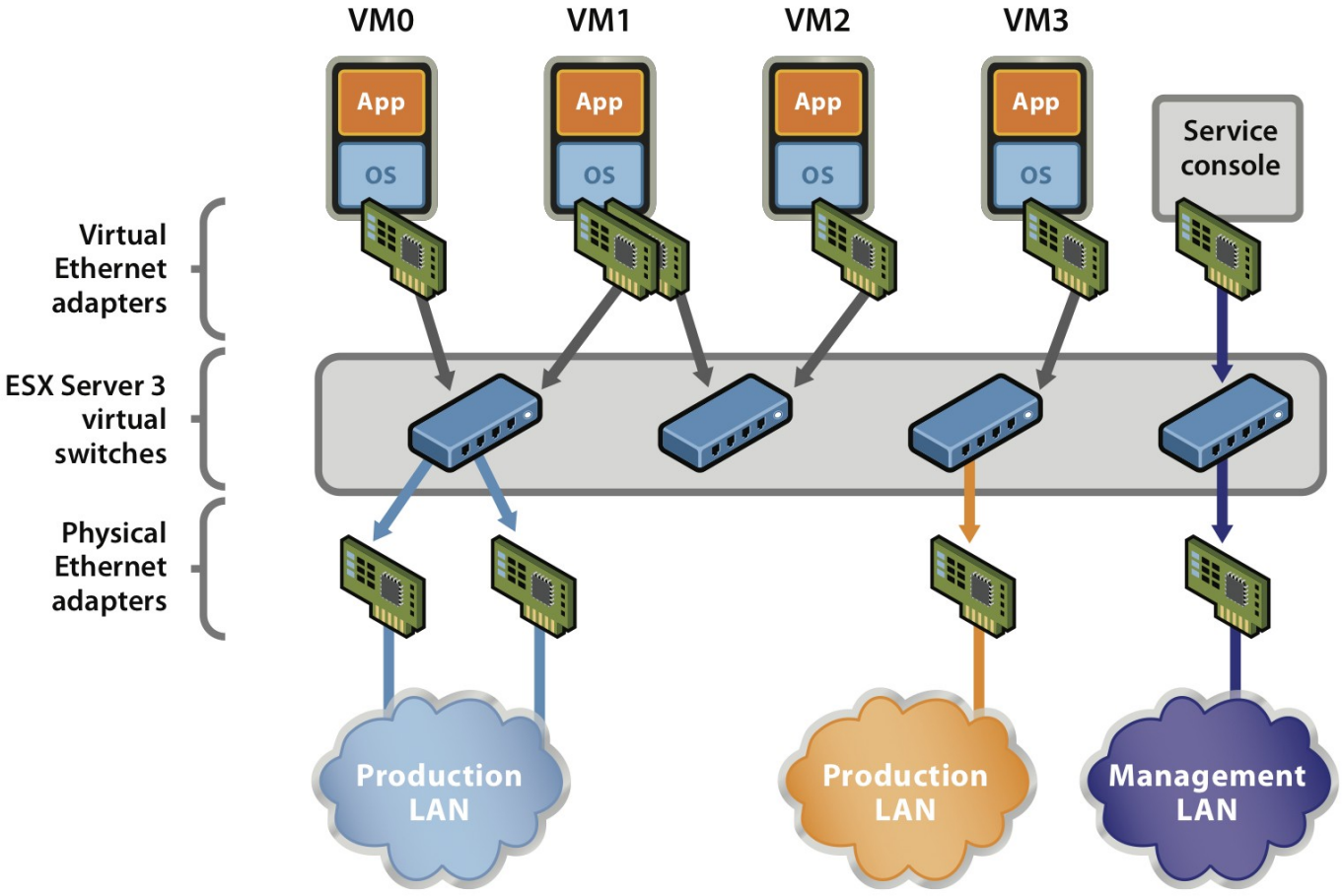
Видове мрежови връзки във VirtualBox

- За всеки мрежов адаптер може да се избере вида на връзката;
- В допълнителните (advanced) параметрите може да изберем вида на емулираната мрежова карта, MAC адреса и, както и дали в момента искаме да има връзка или не;
- За някои видове връзки може да зададем Port Forward параметрите;



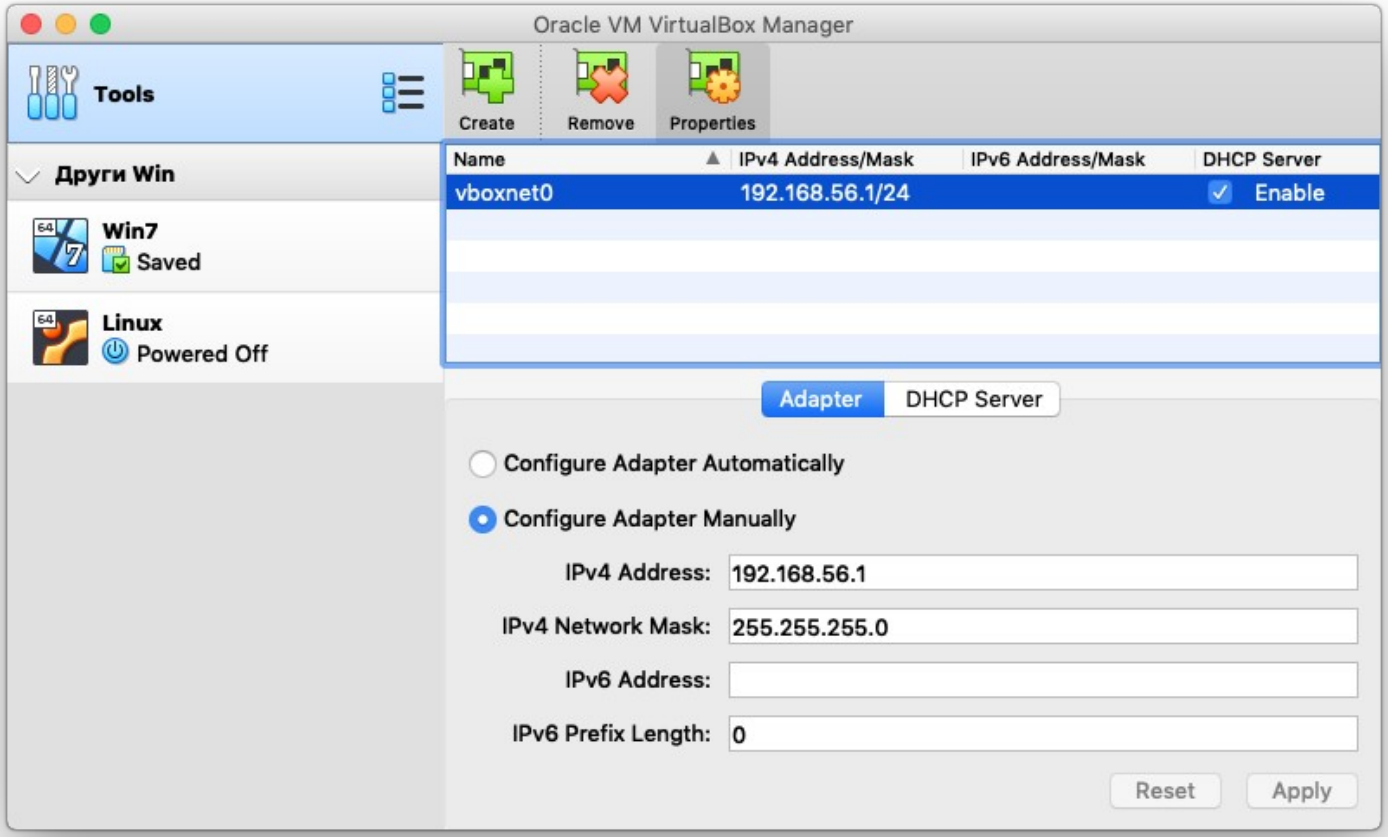
Виртуални Комутатори

Настройки на виртуални мрежови комутатори



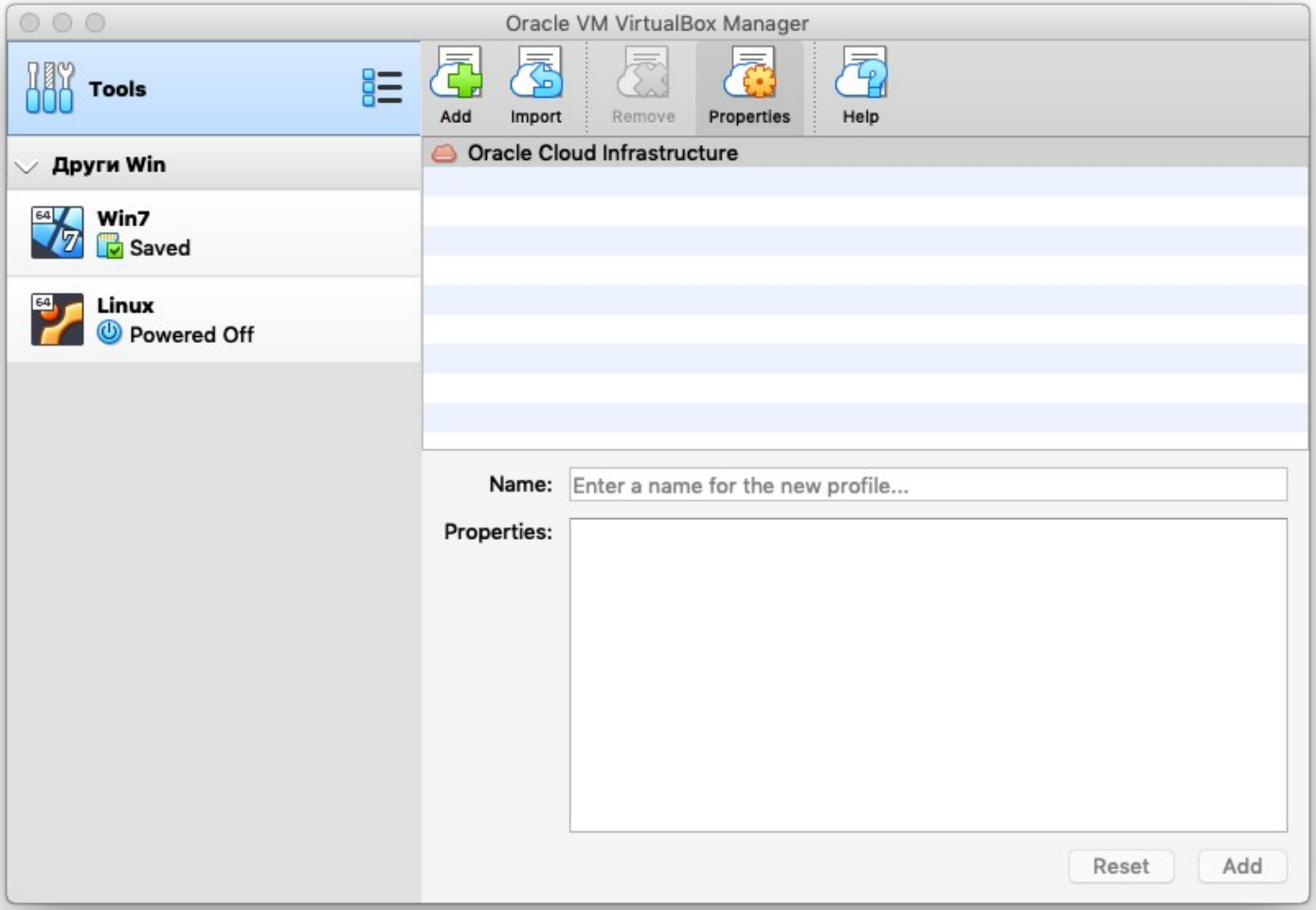
Създаване на виртуални комутатори във VirtualBox

- Помагат за създаване на vLAN и включването на различни ВМ към тях;
- Възможности за настройка на основните параметри;
- Поддръжката на DHCP сървър и др.



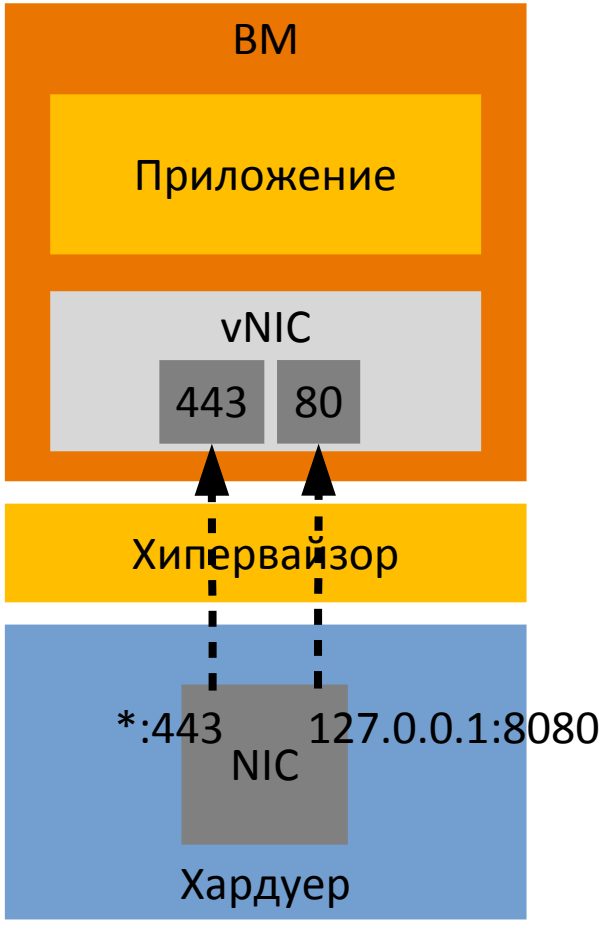
Хибридни системи

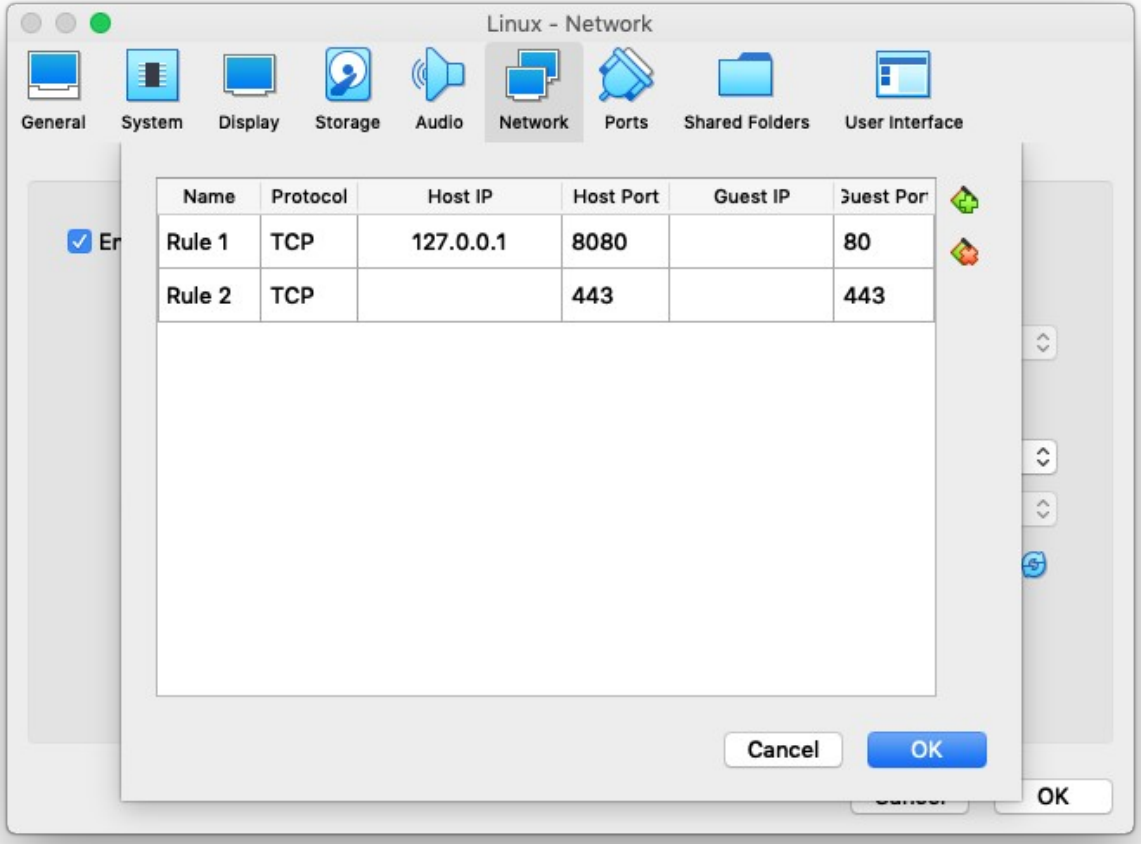
- Повечето съвременни системи за виртуализация предлагат и възможности за създаване на хибридни системи;
- Те включват както локани ВМ, така и ВМ във системите на доставчиците на Cloud услуги;



Виртуални Firewall и Port-forwarding;

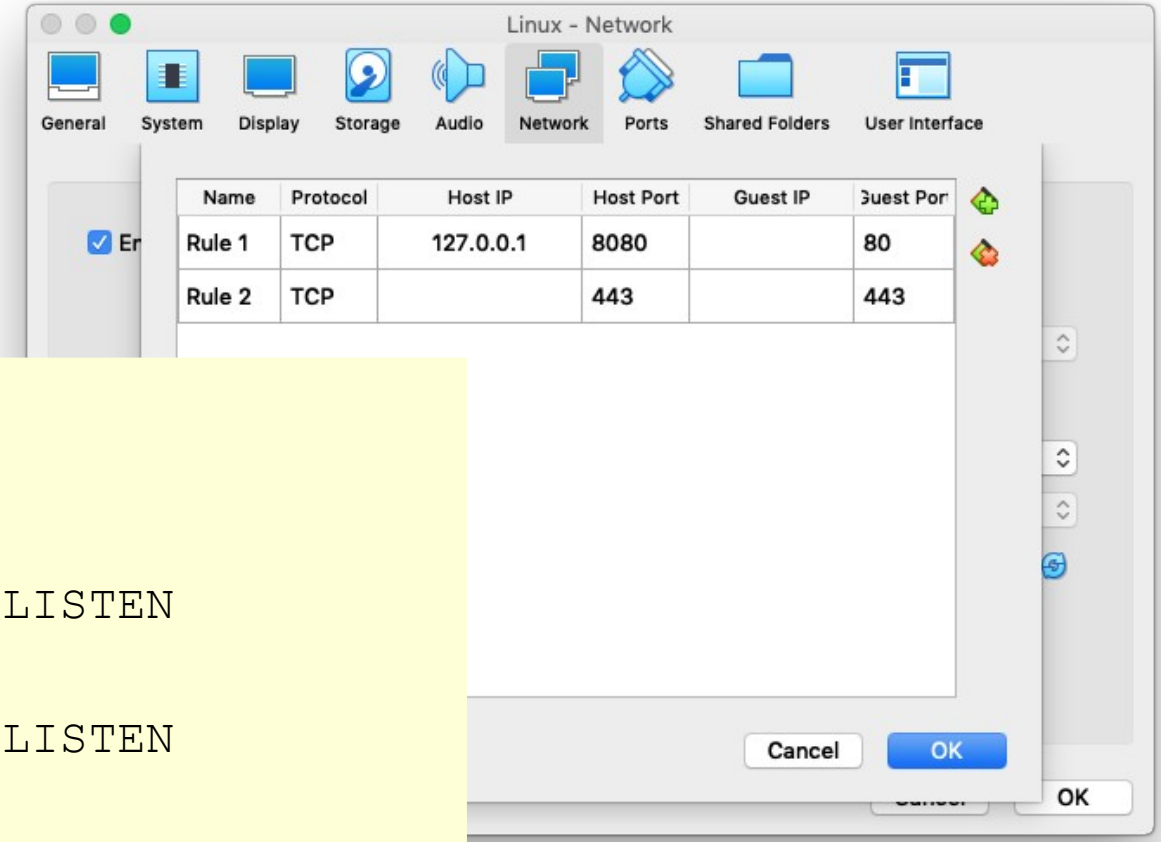
Port-forwarding във VirtualBox





Port-forwarding във VirtualBox

При стартиране на ВМ, VirtualBox прихваща и препраща комуникацията от Host портовете към портовете на съответната vNIC на ВМ.




```
$ netstat -an | grep LISTEN

tcp4  0  0  *:443              *.*  LISTEN
...
tcp4  0  0  127.0.0.1:8080     *.*  LISTEN
...
```

Firewall, Маршрутизация и др.

- Голяма част от сървеменните системи за виртуализация предоставят възможности за настройка на виртуални firewall под една или друга форма. Единия вариант е системата да има визможност за настройка на филтирането и други, обработки на входящите и изходящите пакети в/от ВМ (включително Port-frowarding, NAT и др.). Друг вариант е, ако системата не предоставя директно тези възможности за параметризация на ВМ, да се изгради по-сложна мрежа от няколко ВМ, една или повече, от които да са инсталирани със специализирани ОС (или ОС с общо предназначение), настроени за работа като маршрутизатори, firewall и др.;
- Изграждането на мрежи от такъв вид, може да е свързано с експериментиране на различни сценарии и настройки, но може да е част от Production система;



Въпроси?

apenev@uni-plovdiv.bg