Virtualization of Wireless LAN Infrastructures

IDAACS 2011

IEEE 6th International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications

15-17 September 2011, Prague – Czech Republic
http://www.idaacs.net/

Fachhochschule Dortmund
University of Applied Sciences and Arts

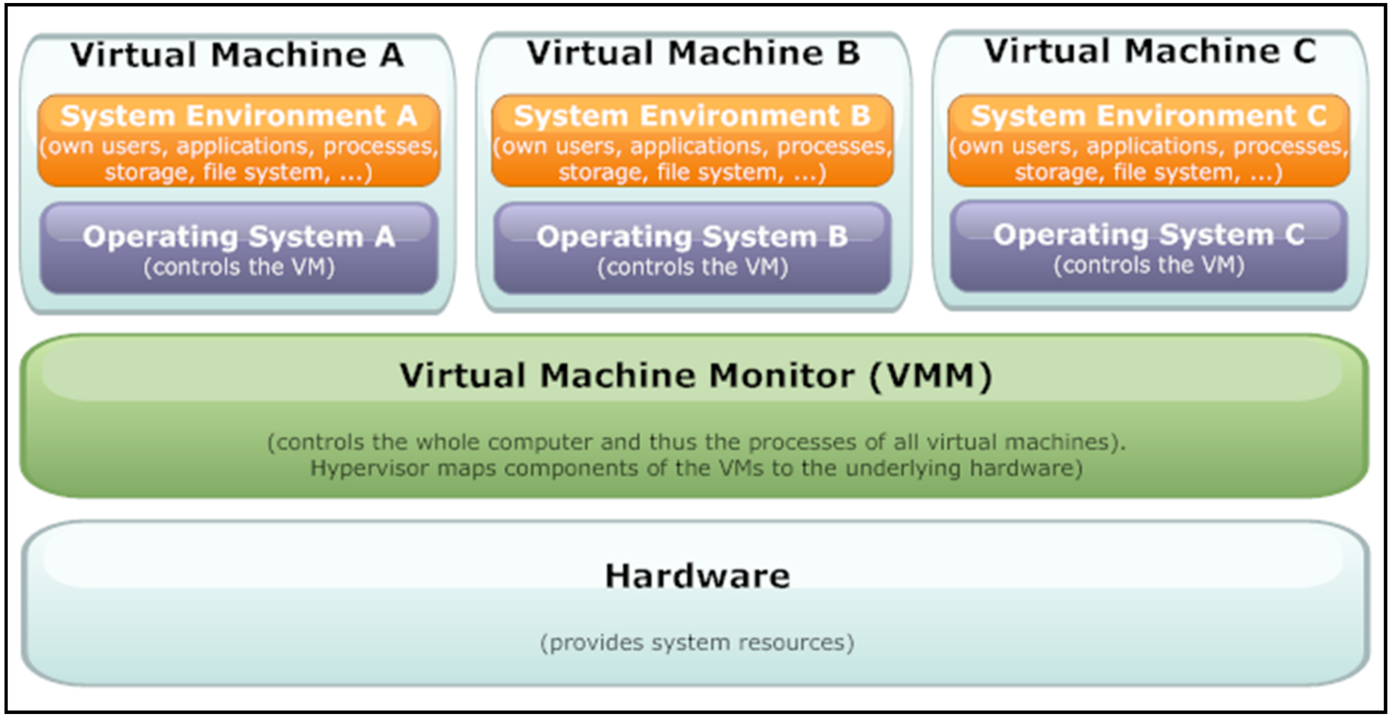
Prof. Dr. -Ing. Evren Eren
University of Applied Sciences and Arts
Emil-Figge-Str. 42
44227 Dortmund – Germany
Fon: +49-(0)231-755-6776
Fax: +49-(0)231-755-6710
E-Mail: eren@fh-dortmund.de
Web: www.fh-dortmund.de/eren

LISA
Laboratory for IT-Security Architectures
www.lisa.fh-dortmund.de

Ghannam Aljabari
Palestine Polytechnic University
Hebron, Palestine
P.O.Box 198
Tel: +970-(0)2-223-1921
Fax: +970-(0)2-223-5505
Email: galjabari@ppu.edu
Web: staff.ppu.edu/galjabari

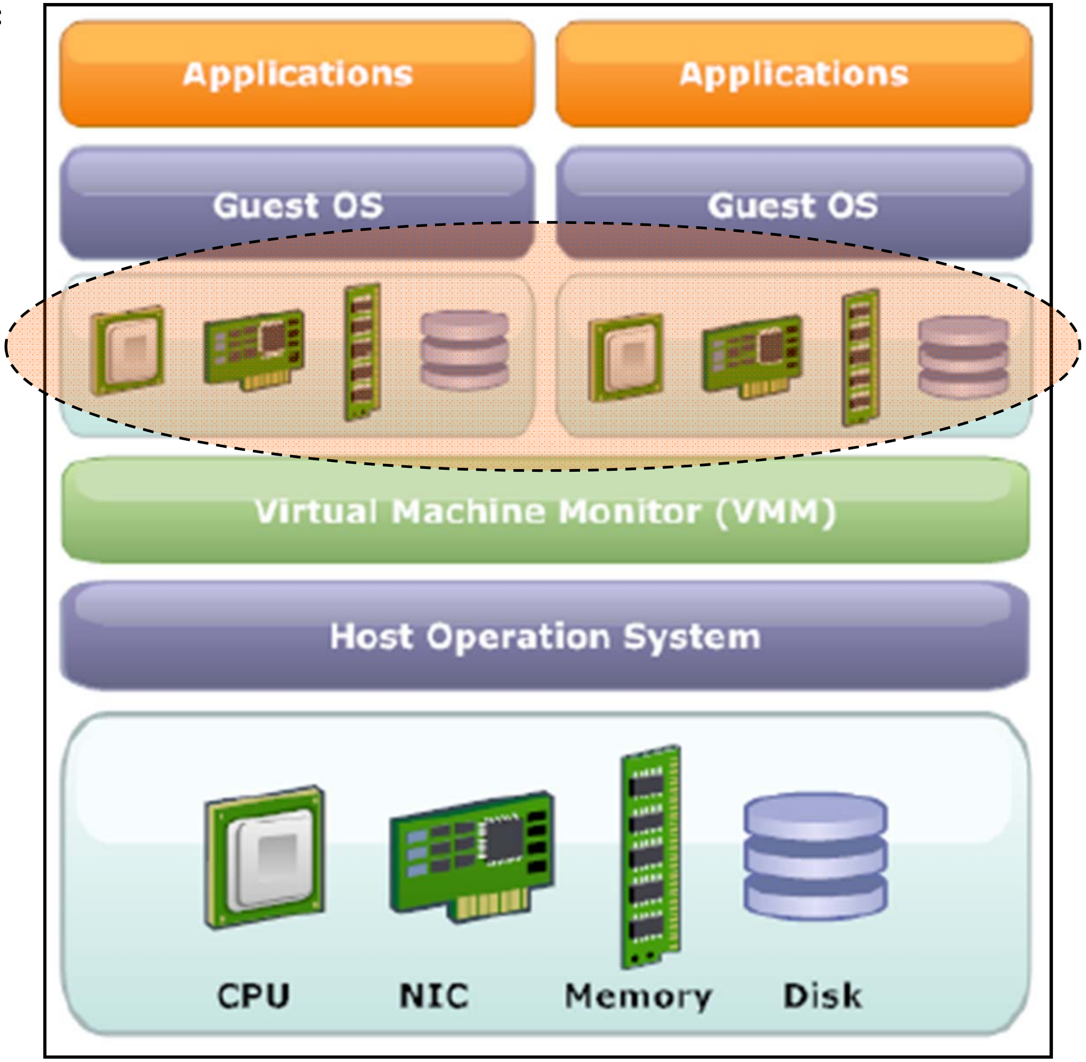
Conventional Virtualization

- Conventional virtualization techniques enable running multiple OS and multiple applications concurrently on the same physical machine.
- Each VM has its own OS and application(s) such as the physical machine.
- The VMs share physical resources such as memory, disk space, and network devices of the host machine.



Conventional Virtualization

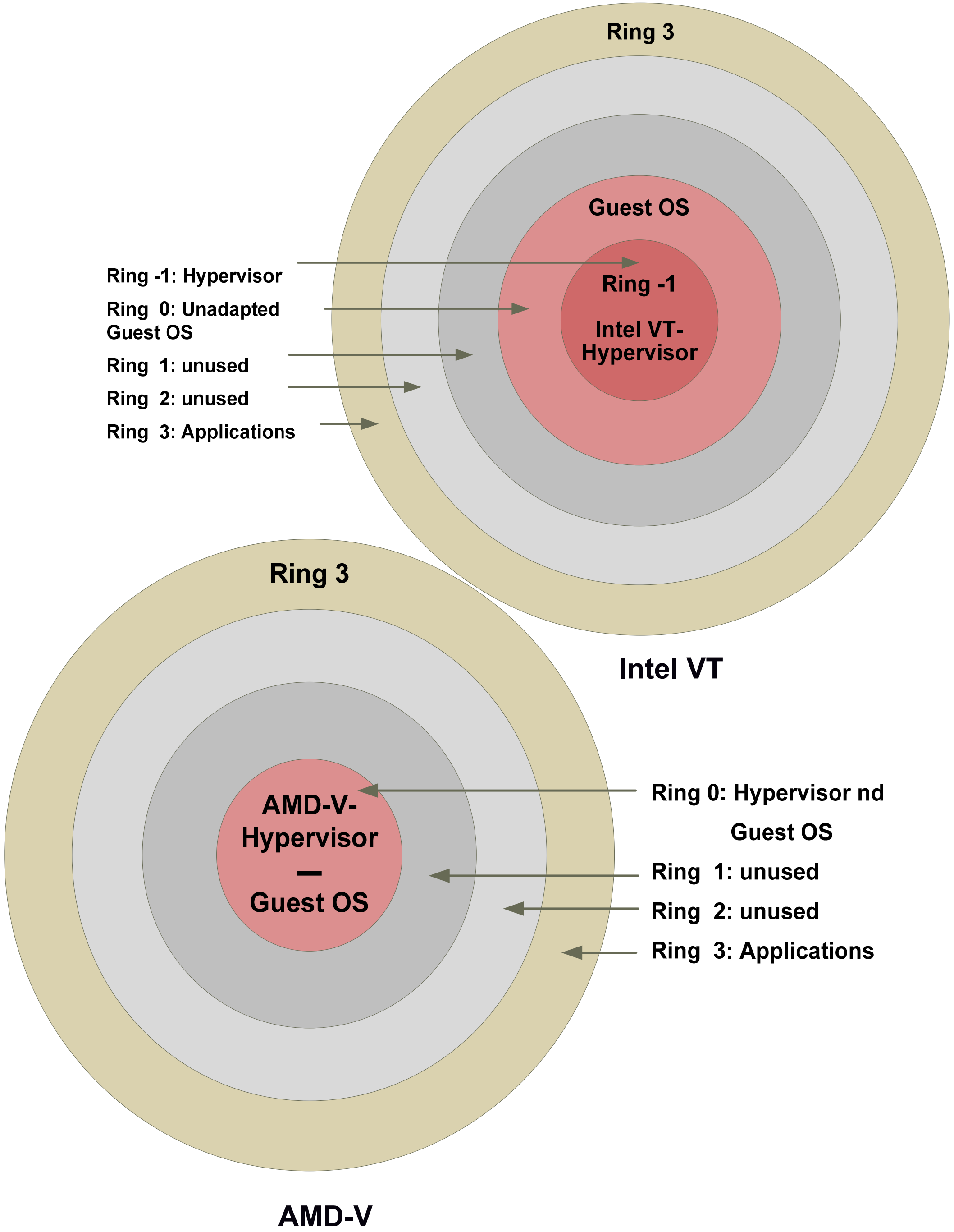
- VMs and guest OS run on top of virtual hardware provided by the VMM.
- Generally, the VMM (Hypervisor) runs on top of the host OS acting as a user space program.



Full (Bare Metal) Virtualization

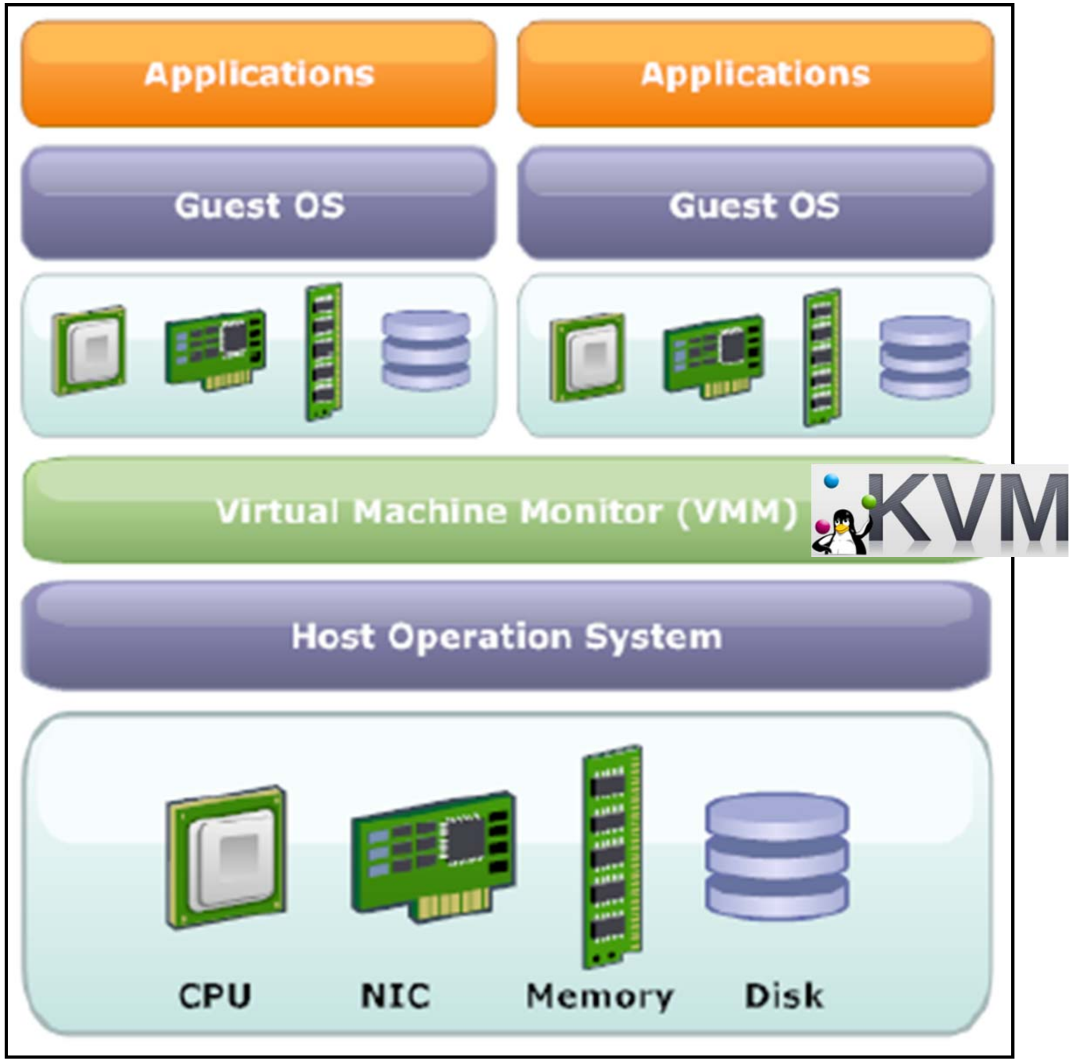
- Guest OS
  - do not have to be operated in unprivileged rings; their kernel can run in ring 0.
  - do not have to be adapted/modified since they are in their usual environment.
  - can use the processor directly.

- The VMM acts passively.



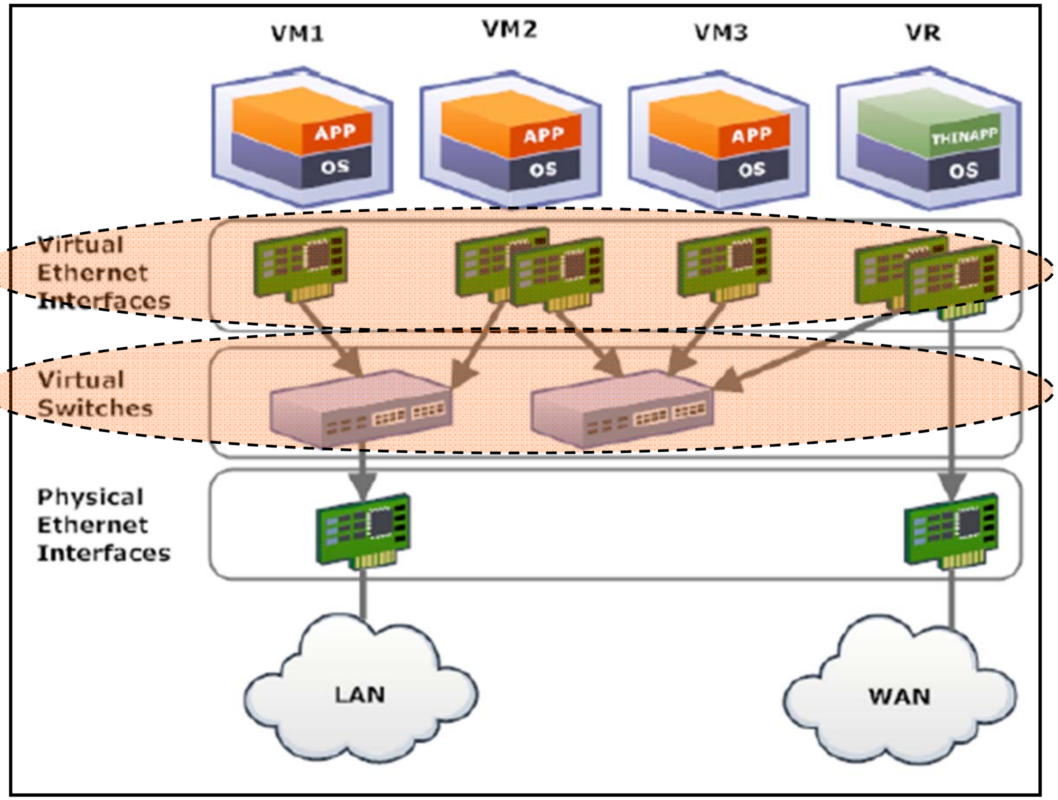
KVM

- KVM (Kernel-based Virtual Machine) is a full (bare metal) virtualization solution which adds VMM capability to Linux OS.
- With KVM multiple VMs can be operated with unmodified OS, since it benefits from CPU hardware virtualization extensions such as Intel VT and AMD-V.



Network Virtualization

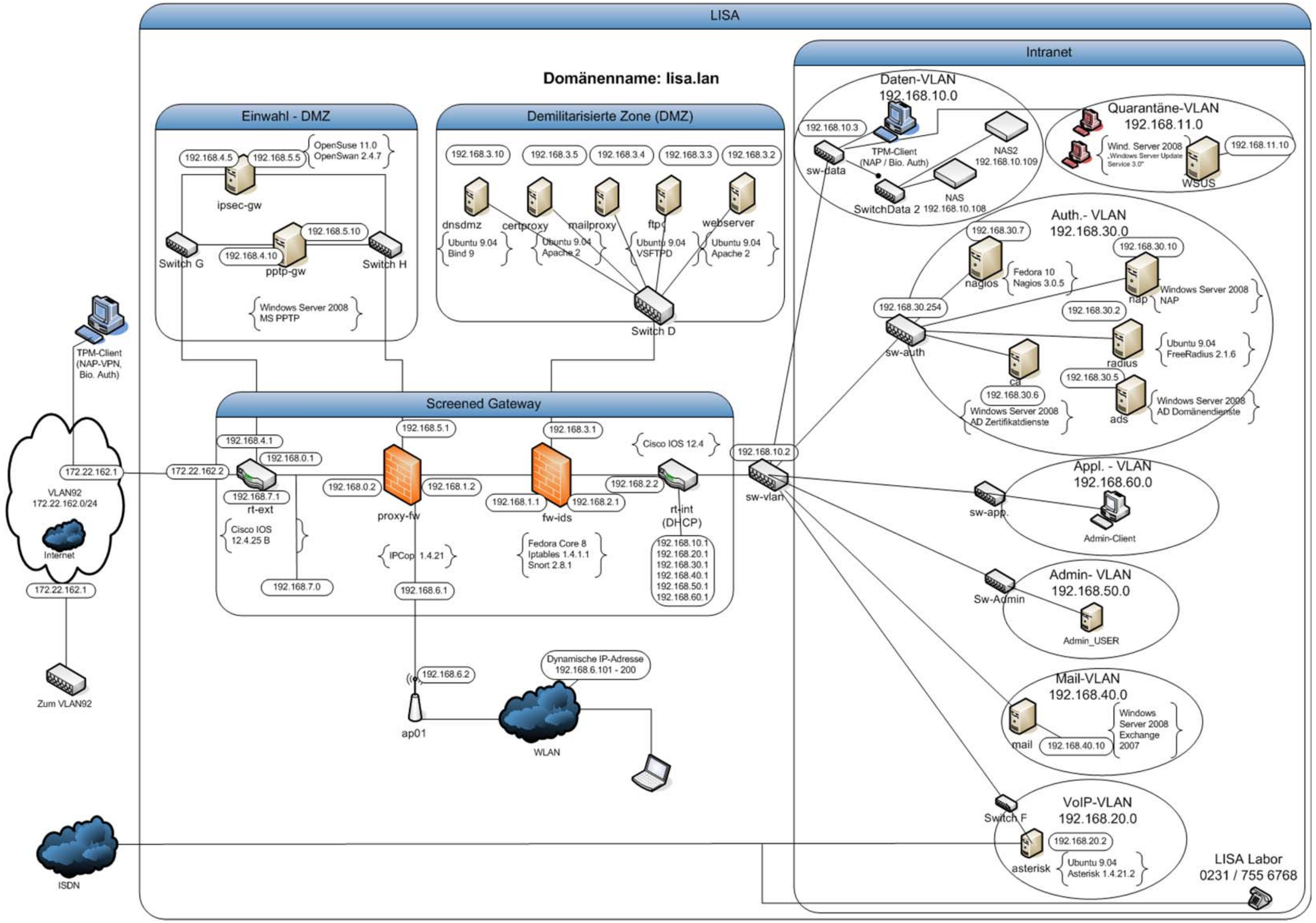
- Network virtualization (ISO OSI Layer 1-3) combines network functionality into a common virtualized environment.
- Multiple logical networks can operate on the same underlying physical infrastructure.
- For the time being, network virtualization techniques can realize
  - virtual Ethernet interfaces,
  - virtual switches (VDE, OpenvSwitch) and
  - virtual routers (Vyatta).



Virtual Square · Open vSwitch An Open Virtual Switch · VYATTA Open Networking

Wireless LAN Virtualization

- This has been demonstrated in the LISA Laboratory



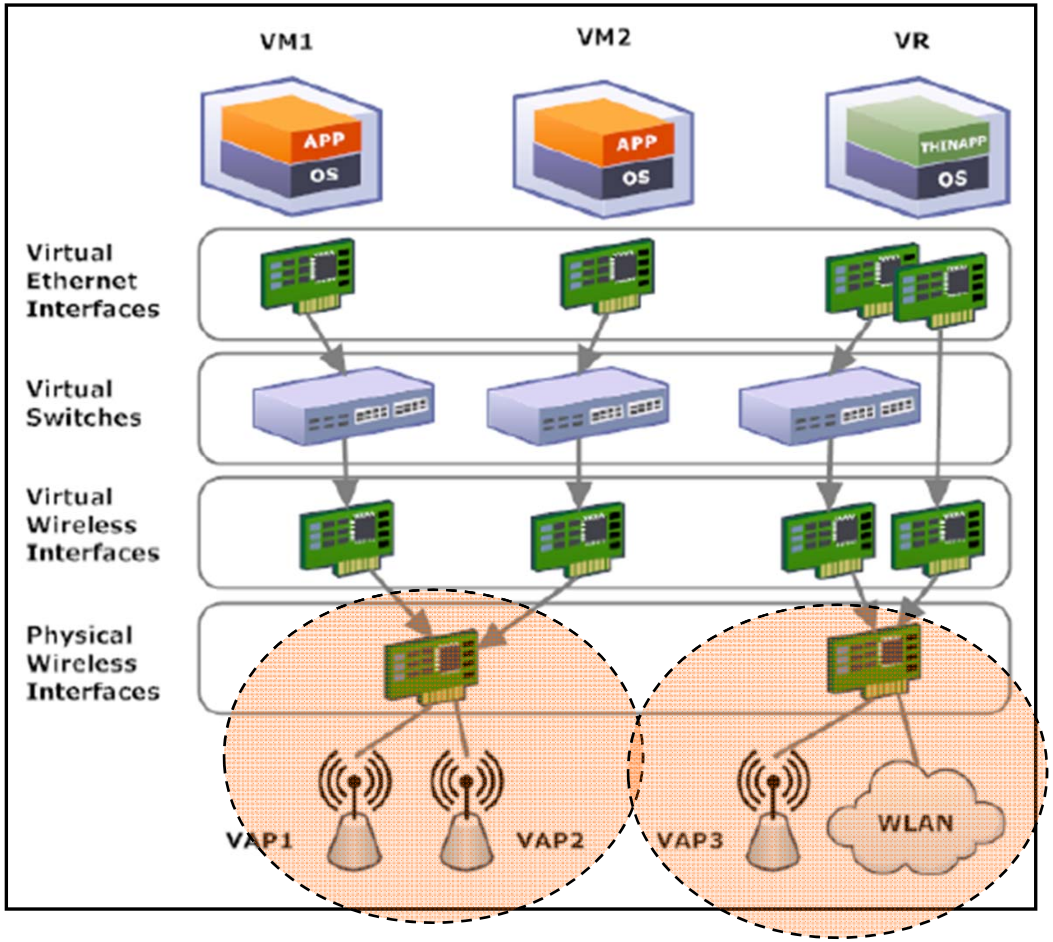
Wireless LAN Virtualization

- However, virtualization of Wireless LAN is different, since existing virtualization approaches require a separate and dedicated physical wireless LAN network interface for each VM.
- But, this is possible using open source virtualization. Multiple wireless networks can be deployed through a single physical wireless LAN network interface → each VM can have its own wireless network.
- This technique is a form of resource virtualization – logical resources are created by partitioning hardware resources into virtual interfaces or ports.

Wireless LAN Virtualization

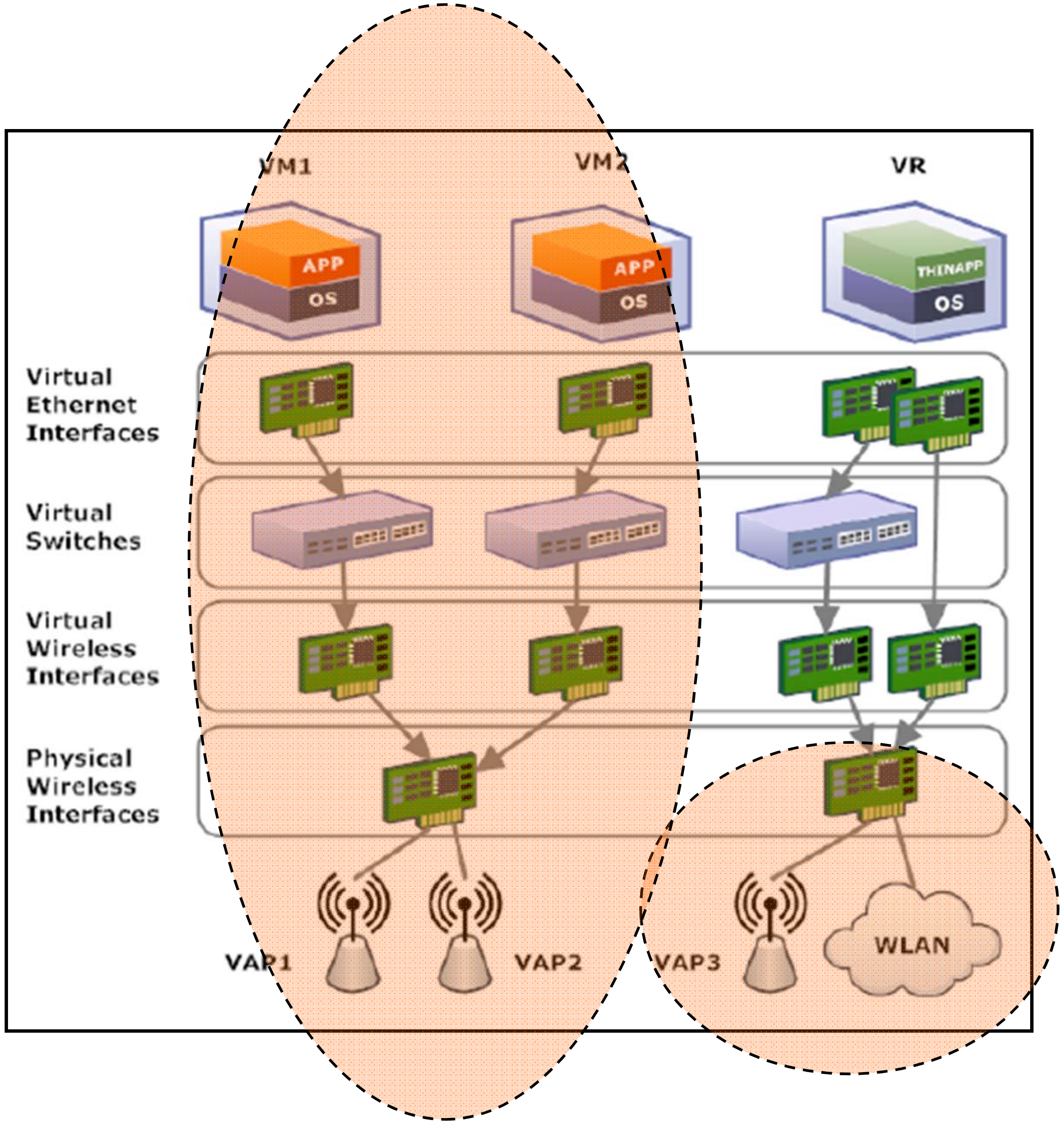
- Virtual wireless interfaces operate concurrently without considering the physical nature of the wireless medium and management.
- A virtual wireless interface can be configured to operate as
  - access point (AP) or
  - client station device.

- Each VM can be assigned to one or even more virtual wireless interfaces.
- Multiple virtual APs can be configured on top of solely one physical wireless device.



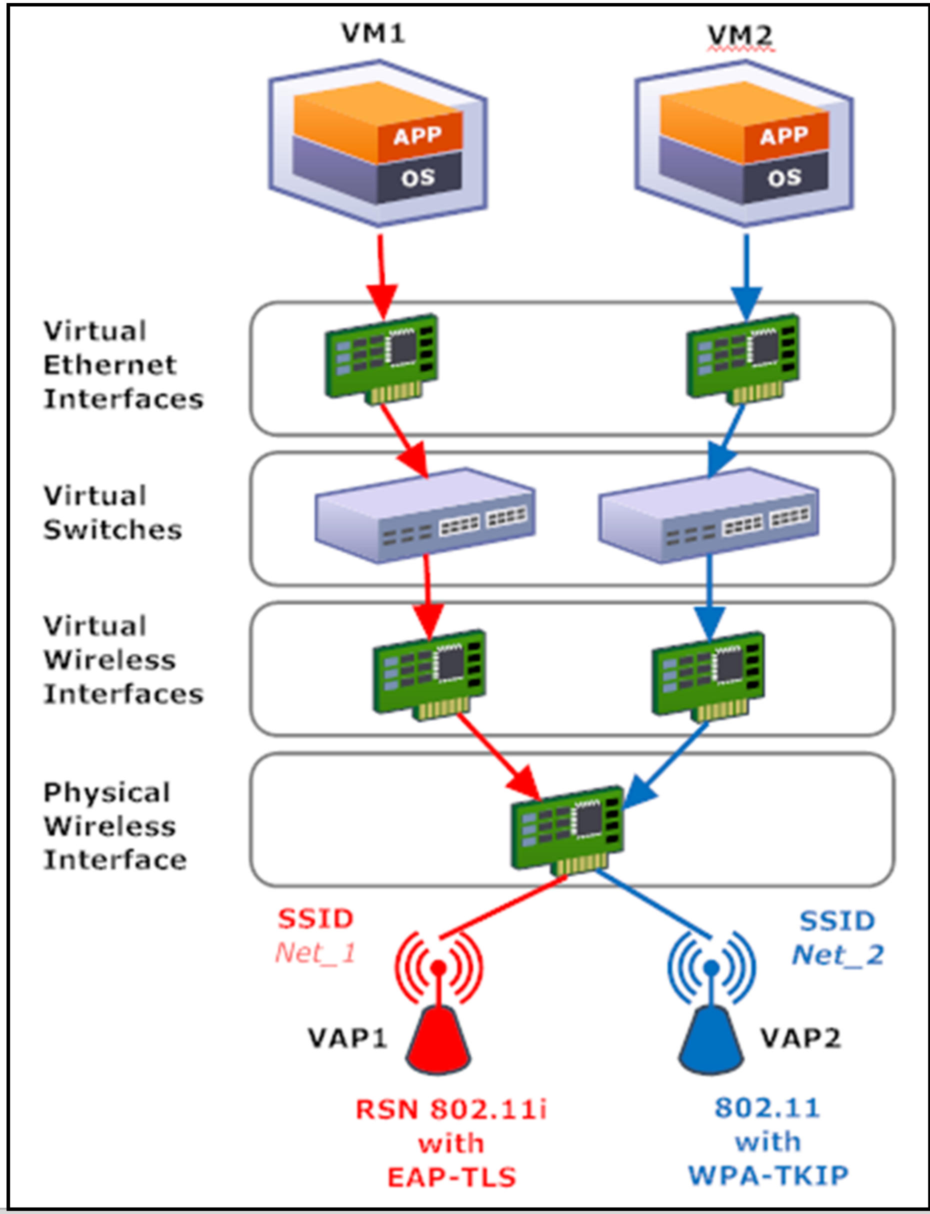
Wireless LAN Virtualization

- A wireless device can be connected to multiple wireless networks simultaneously; e.g. one virtual interface to an AP, while another virtual interface operates as an AP itself.
- Concurrent wireless connections can be established sharing the same physical layer of the wireless LAN device.
- To the layers above (VMs) each virtual AP appears as an independent physical one.



Wireless LAN Virtualization

- Multiple services (respectively different security policies – authentication, encryption, etc.) can be offered on the same physical infrastructure.
- Radio resources can be shared and thus virtualized in different ways.
- The same radio frequency or channel can be used for multiple virtual wireless interfaces, each with its own Service Set Identifier (SSID).



Implementation

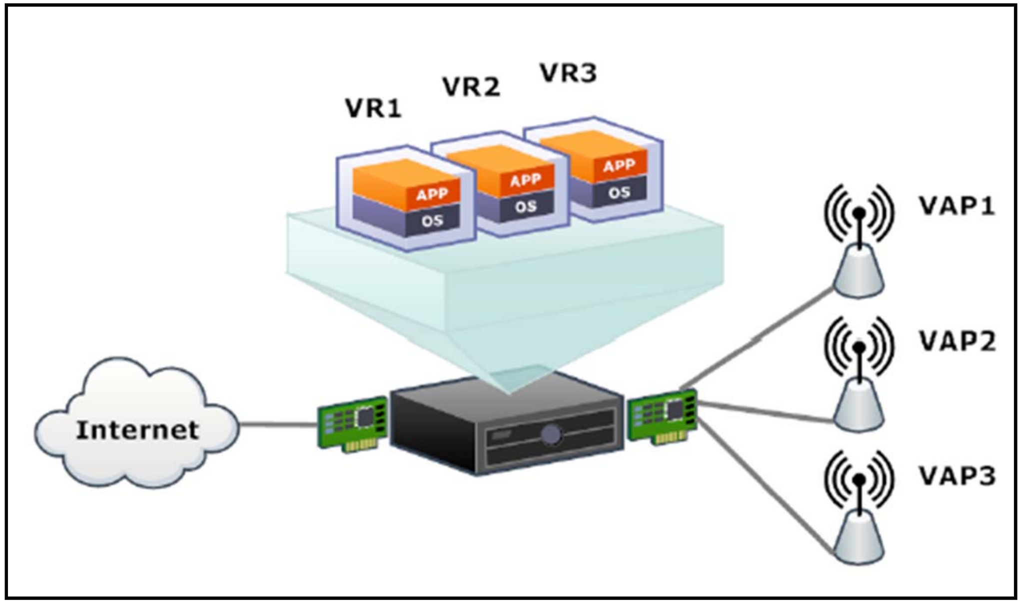
- Used system components:
  - **Conventional PC** with a wireless card based on the Atheros IEEE 802.11n chipset.
  - The **Atheros chipset** allows implementing multiple IEEE 802.11 networks on a single physical wireless card with Linux since it includes a wireless driver supporting multiple virtual interface configurations.
  - **Ubuntu** as host OS
  - **KVM** for virtualization (VMM/Hypervisor)
  - **libvirt** as frontend to manage VMs
  - ***iw*** (Linux CLI configuration utility) to create virtual wireless interfaces
  - **hostapd** for implementing a virtual AP
    - hostapd is an IEEE 802.11 access point, IEEE 802.1X/WPA/WPA2/EAP/RADIUS authenticator, RADIUS client and server, and EAP server.

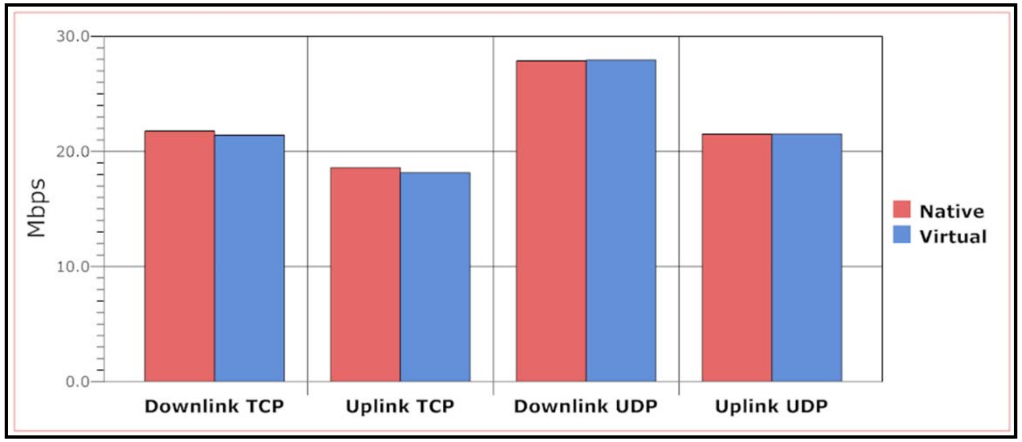
Implementation

- For testing purposes, several virtual wireless routers (Vyatta) have been hosted on the PC with a shared Internet connection.

- In order to validate the impact of virtualization we made some performance measures (TCP/UDP) and compared both worlds (real AP vs. VAP).

- Our tests focussed two metrics:
  - throughput and
  - response time





- The results showed that our proposed solution achieves performance values comparable to native hardware environments.

Conclusion & Outlook

- Our approach combined WLAN + conventional virtualization so that WLAN interfaces can be shared among several VMs.
- We deployed multiple WLANs on a single shared physical infrastructure with different security policies.
- At the same time, these WLANs could be isolated from each other at a satisfactory performance level comparable to native hardware environments.

- Virtualization of WLANs has become one of the important issues in network virtualization.
- It is useful in many scenarios:
  - hosting multiple wireless networks and services (providers) on a single shared physical infrastructure,
  - providing wireless services with different authentication/security mechanisms, and
  - for virtual testbed environments.

Thank you for your attention

Q&A