genua
Soviel ist sicher.

IT Security
Made in Germany

IP-Switch: network security by SDN

BMBF project vmFire

Andreas Brinner <andreas_brinner@genua.de>

November 15, 2013

genua

The vmFire project

vmFire: a BMBF funded research project
startet July 2012 until June 2014

b-tu Brandenburgische Technische Universität Cottbus - Senftenberg

genua Soviel ist sicher.

Radoslaw Cwalinski
Rene Rietz

Andreas Brinner

vmFire: Firewalling in virtualized environments

genua

Security threats

Are there any new security threats induced by virtualization?

genua

Security threats

Are there any new security threats induced by virtualization?

⇒ Yes, of course!

genua

Security threats

Are there any new security threats induced by virtualization?
⇒ Yes, of course!

Which of these threats are exploitable by network and can be prevented by a firewall?

genua

Security threats

Are there any new security threats induced by virtualization?
⇒ Yes, of course!

Which of these threats are exploitable by network and can be prevented by a firewall?
⇒ Basically none!

genua

Relevant threats

1. MAC spoofing
2. ARP spoofing
3. ARP flooding
4. Rogue DHCP server
5. Insecure system services

genua

Relevant threats

1. MAC spoofing
2. ARP spoofing
3. ARP flooding
4. Rogue DHCP server
5. Insecure system services

⇒ standard network flaws

genua

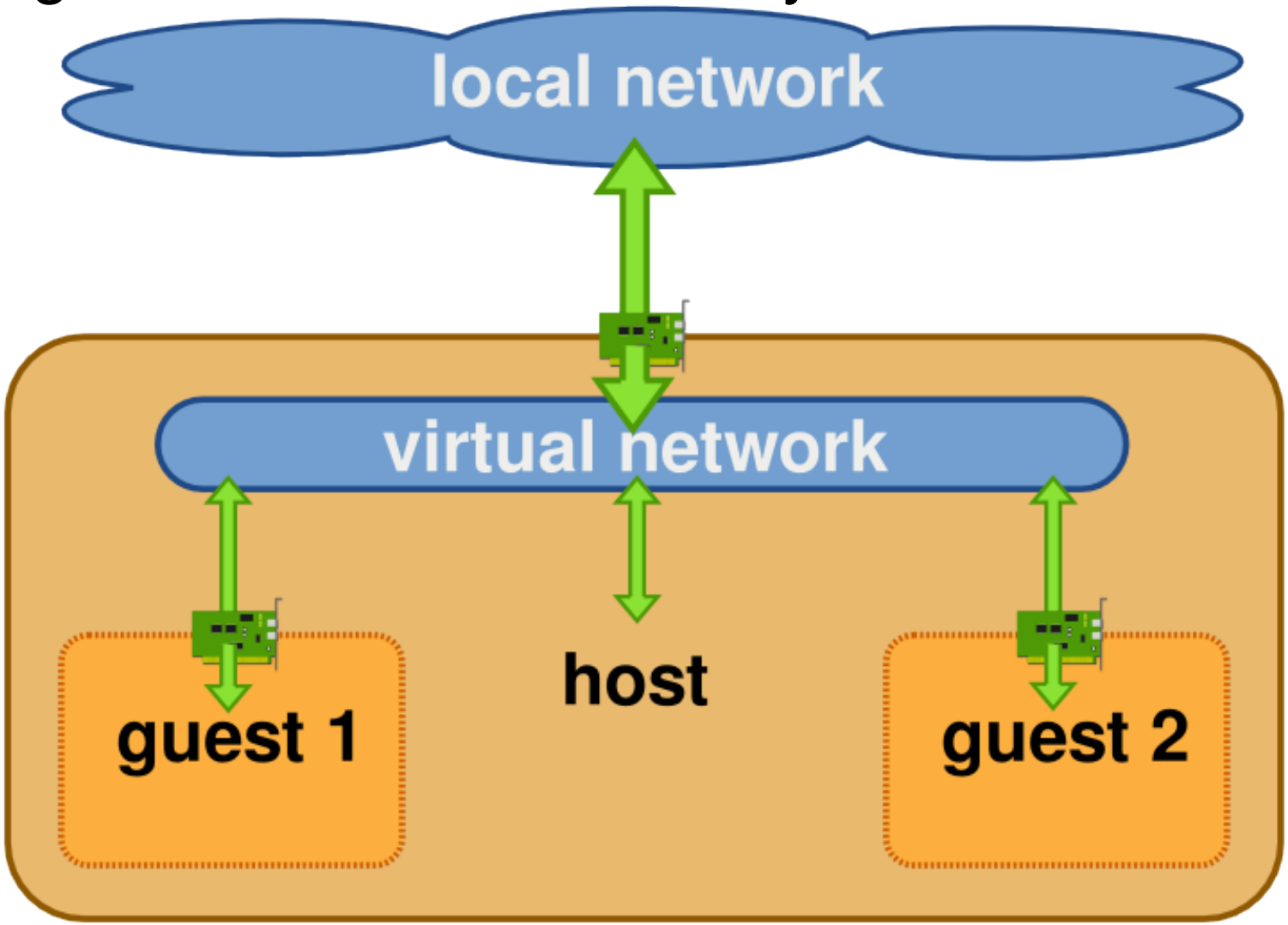
Solutions in physical systems

dividing the network in smaller chunks by using:

- cabling
- configuring subnets
- intelligent switches
- router
- packet filter
- statefull firewalls
- application level gateways
- intrusion prevention systems

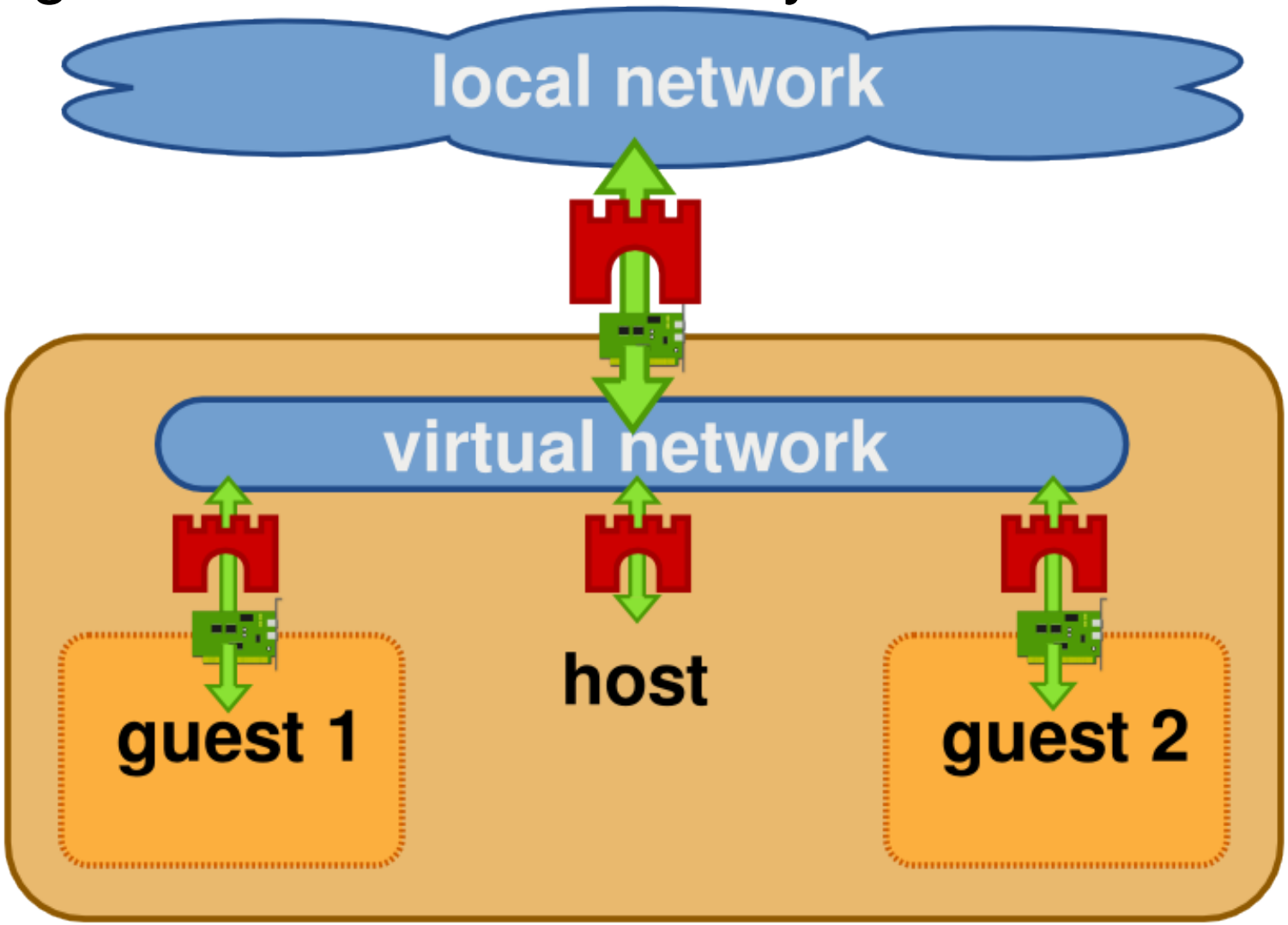
genua

Using firewalls in virtualized systems



genua

Using firewalls in virtualized systems



IP-Switch

Security by using SDN

a special OpenFlow controller which implements

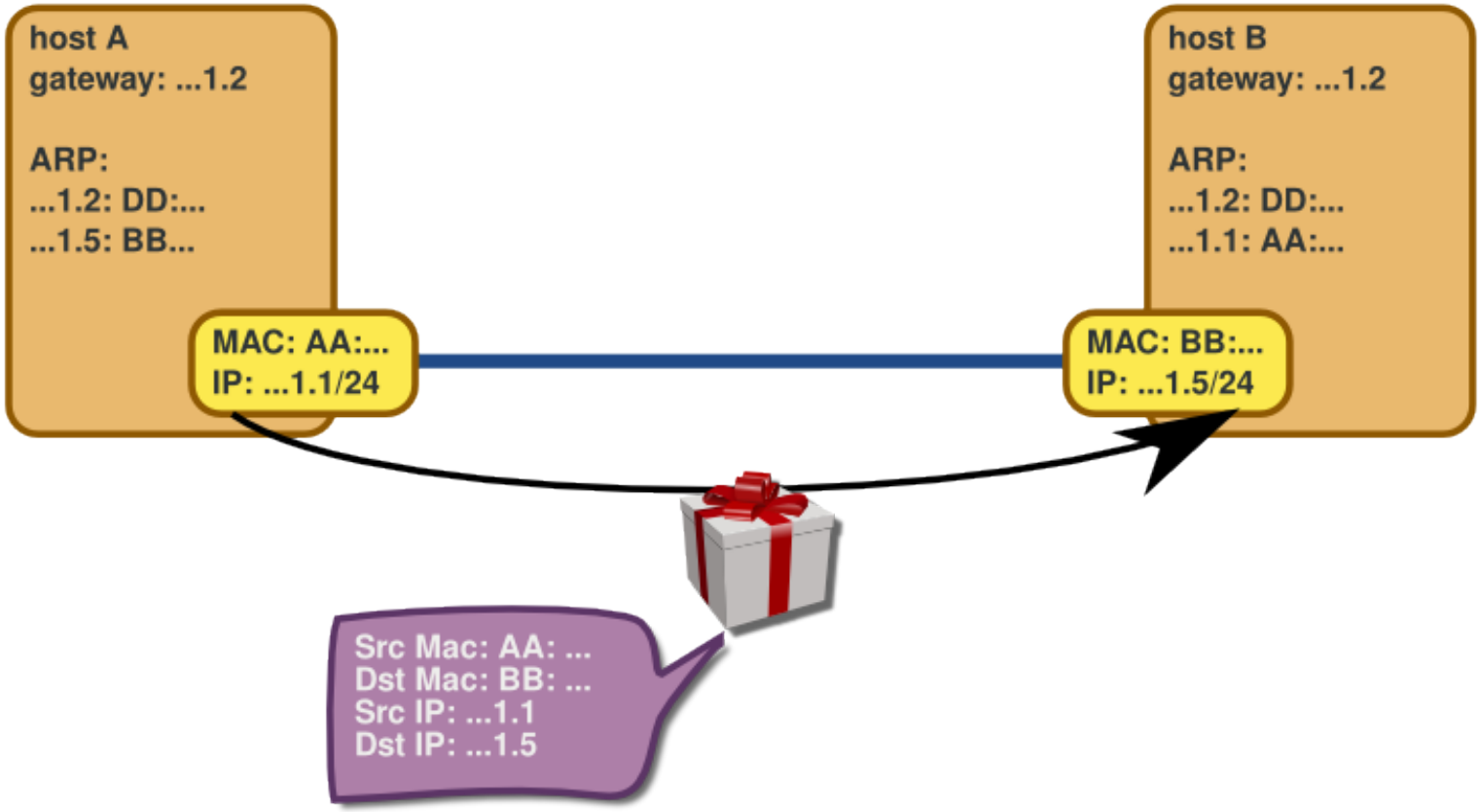
- ARP server
- DHCP server
- topology detection
- shortest path routing
- authorisation

OpenFlow switches act as gateways.

genua

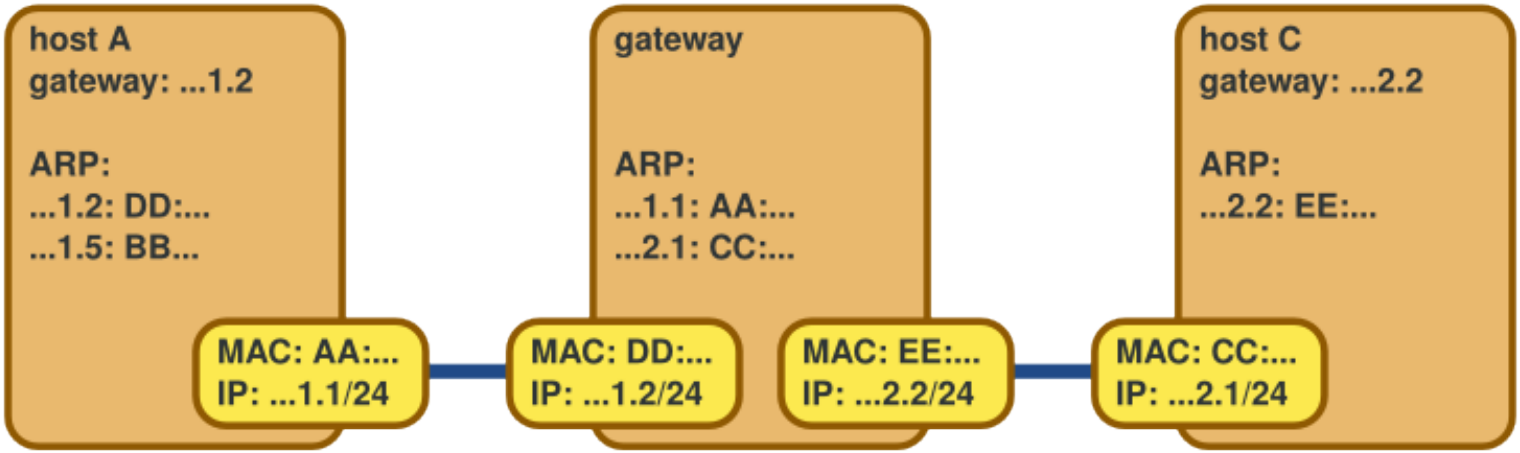
Same subnet

Same subnet


host A
gateway: ...1.2
ARP:
...1.2: DD:...
...1.5: BB...
MAC: AA:...
IP: ...1.1/24
host B
gateway: ...1.2
ARP:
...1.2: DD:...
...1.1: AA:...
MAC: BB:...
IP: ...1.5/24
Src Mac: AA: ...
Dst Mac: BB: ...
Src IP: ...1.1
Dst IP: ...1.5

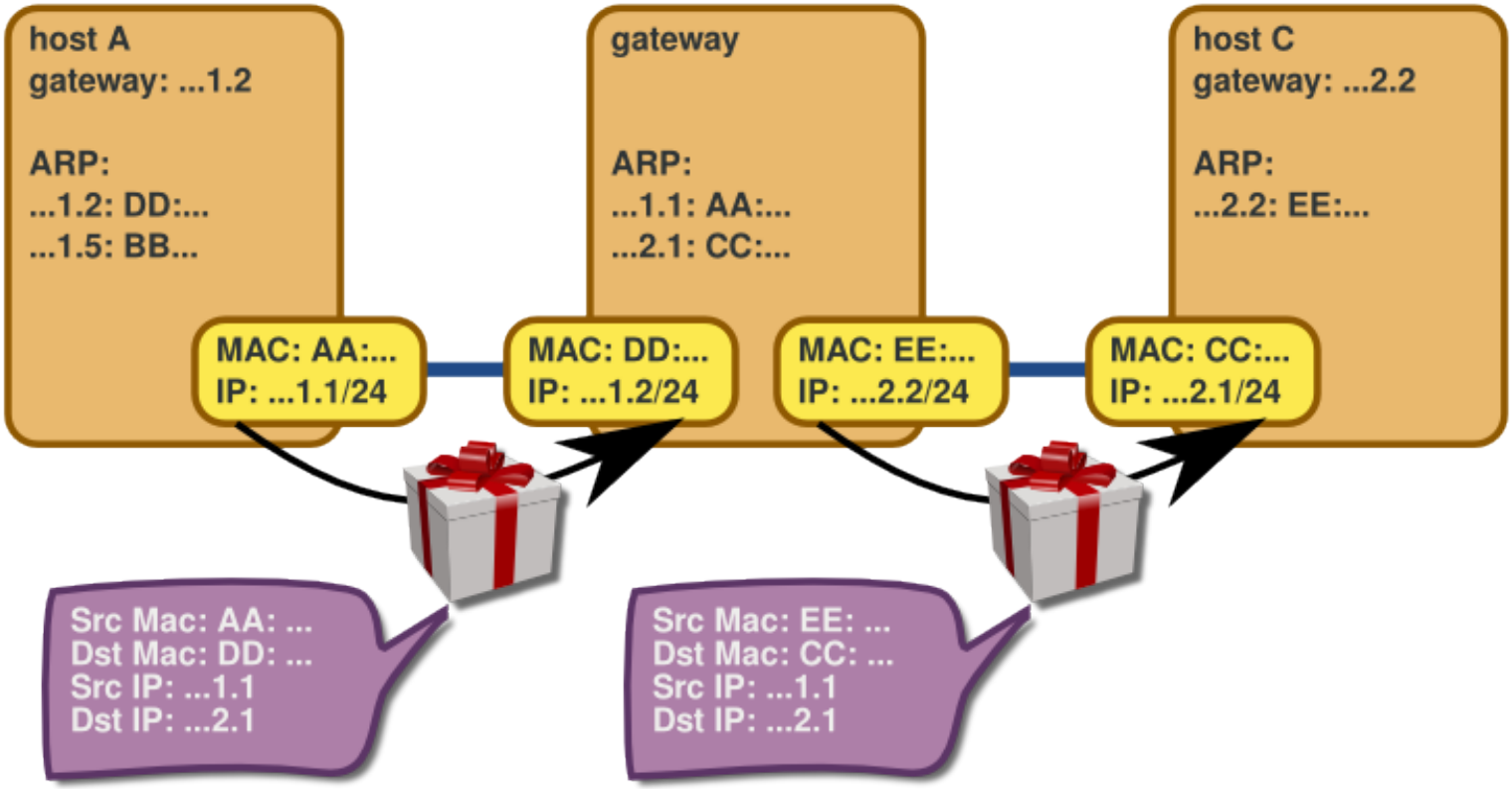
genua

Different subnets connected by a gateway



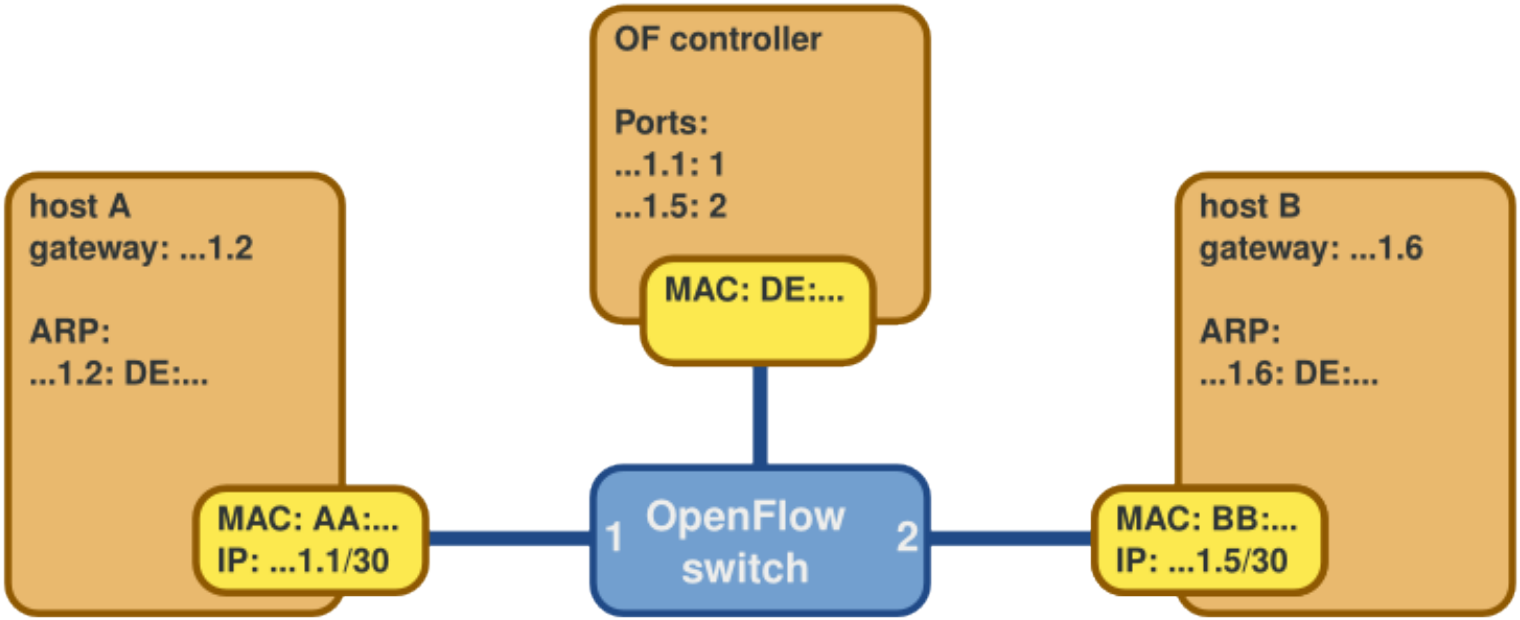
genua

Different subnets connected by a gateway

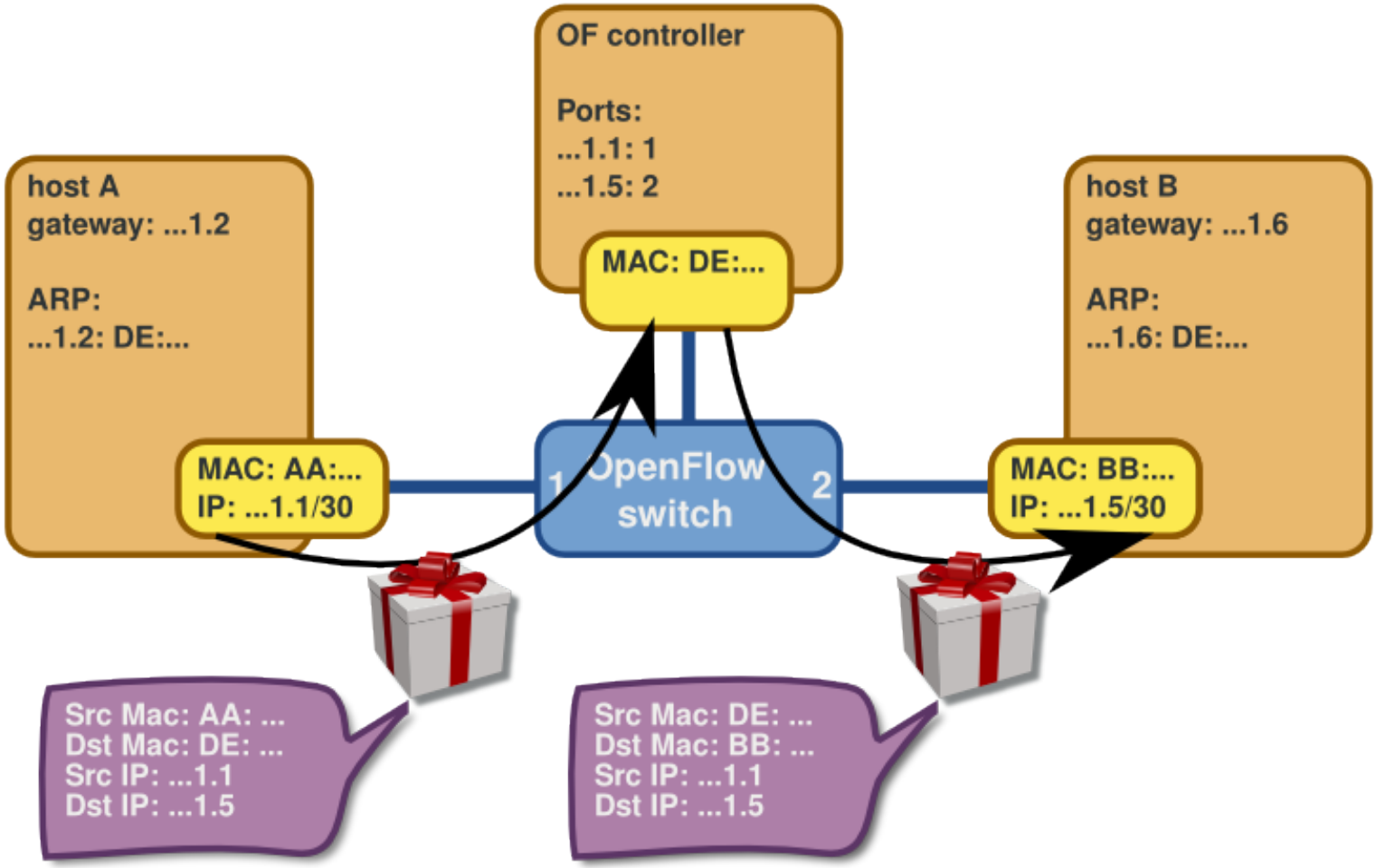


genua

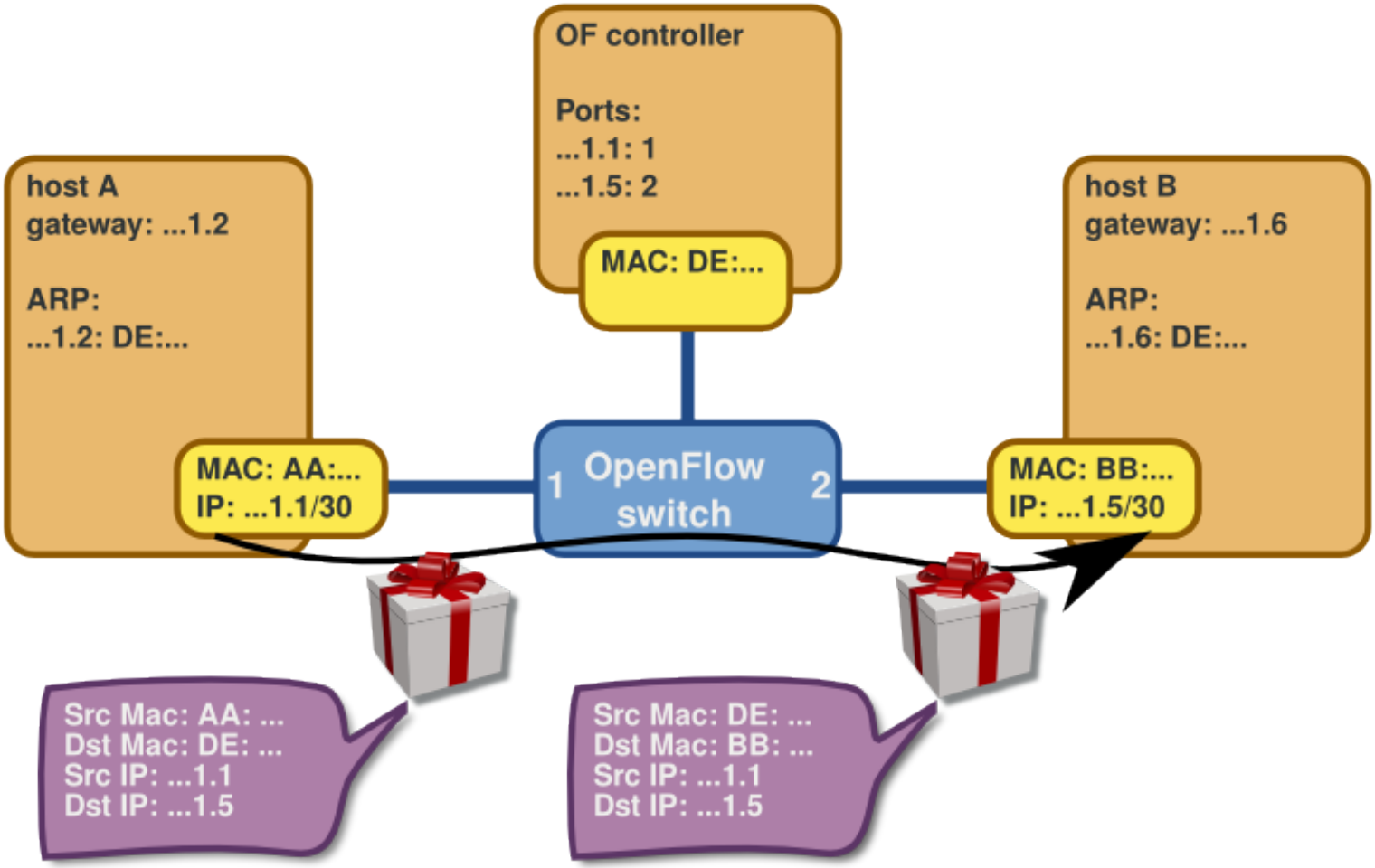
IP Switching



IP Switching



IP Switching



genua

Evaluation: goals achieved?

dividing the network in smaller chunks by using:

- cabling
- configuring subnets
- intelligent switches

- router
- packet filter

- statefull firewalls

- application level gateways

- intrusion prevention systems

Evaluation: goals achieved?

dividing the network in smaller chunks by using:

- cabling ⇒ setting up connections with Open vSwitch
- configuring subnets
- intelligent switches

- router
- packet filter

- statefull firewalls

- application level gateways

- intrusion prevention systems

Evaluation: goals achieved?

dividing the network in smaller chunks by using:

- cabling ⇒ setting up connections with Open vSwitch
- configuring subnets ⇒ not applicable
- intelligent switches

- router
- packet filter

- statefull firewalls

- application level gateways

- intrusion prevention systems

Evaluation: goals achieved?

dividing the network in smaller chunks by using:

- cabling ⇒ setting up connections with Open vSwitch
- configuring subnets ⇒ not applicable
- intelligent switches ⇒ implemented by the OpenFlow controller
- router
- packet filter

- statefull firewalls

- application level gateways

- intrusion prevention systems

Evaluation: goals achieved?

dividing the network in smaller chunks by using:

- cabling ⇒ setting up connections with Open vSwitch
- configuring subnets ⇒ not applicable
- intelligent switches ⇒ implemented by the OpenFlow controller
- router ⇒ implemented by the OpenFlow controller
- packet filter
- statefull firewalls
- application level gateways
- intrusion prevention systems

Evaluation: goals achieved?

dividing the network in smaller chunks by using:

- cabling ⇒ setting up connections with Open vSwitch
- configuring subnets ⇒ not applicable
- intelligent switches ⇒ implemented by the OpenFlow controller
- router ⇒ implemented by the OpenFlow controller
- packet filter ⇒ easy to implement with special flow entries in the OF switches
- statefull firewalls
- application level gateways
- intrusion prevention systems

Evaluation: goals achieved?

dividing the network in smaller chunks by using:

- cabling ⇒ setting up connections with Open vSwitch
- configuring subnets ⇒ not applicable
- intelligent switches ⇒ implemented by the OpenFlow controller
- router ⇒ implemented by the OpenFlow controller
- packet filter ⇒ easy to implement with special flow entries in the OF switches
- statefull firewalls ⇒ can be implemented by the OpenFlow controller
- application level gateways ⇒ can be implemented by the OpenFlow controller
- intrusion prevention systems ⇒ can be implemented by the OpenFlow controller

genua

Feasability studies

- performance measurements
- testing the counteractions
- simulation with Mininet
- real world tests with a physical WiFi

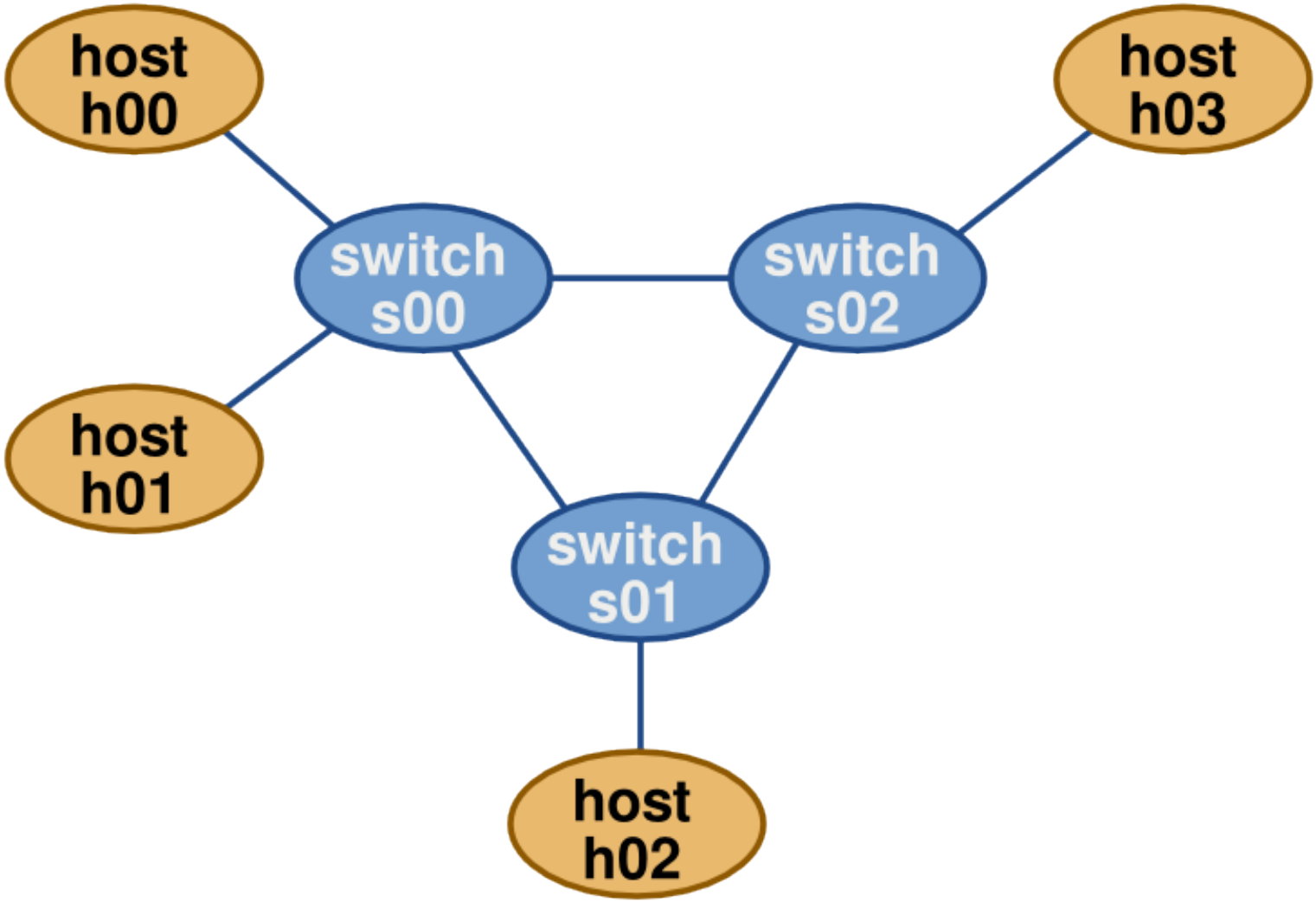
genua

Testing with Mininet

- rapid prototyping for Software Defined Networks
- network emulation with hosts, switches and links
- Python based
- uses process based virtualization and network namespaces

genua

Demonstration OpenFlow Controller



genua

Questions?