B-10: Wireshark vs. “The Cloud”
Thursday June 17, 2010. 10:45am -12:15pm

Jasper Bongertz
Senior Technical Consultant  |  Synerity Systems / Fast Lane GmbH

SHARKFEST ‘10
Stanford University
June 14-17, 2010
- Physical vs. Virtual
- Cluster Basics
- VMs on the Move
- Capture Methods
- New Capture Methods
Physical vs. Virtual

From what we know to “Virtual Environments”
Physical Environments

• Applications and services running on “real” servers
• Often multiple servers per application/service
  – Mail servers, Web server farms
  – Often difficult to capture: clustered servers
• Multiple applications/services per server
  – Web service, database service
Capture Strategies

• Common capture strategies:
  – HUB (for single clients or when really really desperate)
  – SPAN (quick, no disconnects)
  – TAP (most exact)

• Less common:
  – Inline/Pass Thru capture
  – With locally installed Wireshark (bad idea)
  – Using hacking techniques (really bad idea)
Typical physical setup example
Let’s go virtual...
Virtual Environments

- Virtual Environments usually consolidate multiple servers on one or multiple virtualization hosts.
- Physical hardware runs a virtualization layer with virtual servers on top.
- Shared Resources:
  - CPU cycles and memory
  - Storage
  - Of course: network adapters!
Enterprise Virtualization

• Common virtualization solutions found in datacenters today are:
  – Citrix XenServer
  – Microsoft Hyper-V
  – Red Hat Enterprise Virtualization
  – VMware vSphere

• Basically all enterprise virtualization solutions have the same basic features
  – or will have them sooner or later
Host Virtualization Example #1

- Virtualization host runs multiple Virtual Machines on a single NIC
- The host may use the NIC for its own data communication, too
- Potentially dozens of virtual servers showing up with their own virtual MAC address on the physical NIC
Capturing virtual servers

- Virtual servers running on a physical host share one or multiple network cards
- Capturing possible using HUB/SPAN/TAB method at the physical uplink to the host
- Challenges:
  - Capture at the correct NIC in case of multiple cards (and there will be, trust me)
  - Isolate traffic for the virtual server you want
  - Server Blade Centers with 10GBit or faster uplinks
Host Virtualization Example #2

• There may also be "internal only" switches making things complicated
• Data on internal switches never leaves the host
• No physical pickup possible
• Watch out for teamed NICs!
Common NIC Teaming Strategies

- Port ID based
- Source MAC hash
- Source/Destination IP hash
Virtual Cluster Basics

Trouble Brewing
Virtualization Cluster Example

• Group of virtualization hosts combined into a cluster
Cluster Basics

- Server clusters are always difficult to capture
  - Even without virtualization you usually don’t know where the connection will end up
- Possible solutions include
  - Forcing specific connections to certain cluster members that can be captured
  - Capturing a common cluster uplink if available
  - Las Vegas style: capture somewhere and hope that you’ll catch the relevant frames 😊
Virtualization clusters

- Virtualization clusters are even more complex than clusters of physical servers
  - Load Balancing of virtual machines
  - High Availability / Failover
- Virtual machines may move from host to host without warning, at any given time!
- Requires shared storage
  - Fibre Channel, iSCSI, NFS
  - Lets better hope you never have to capture those... 😊
VMs on the move
Live Moving of Virtual Machines

- Virtual Machines may move between virtualization hosts while they continue to run
Cluster Movement Features

- High Availability (sort of)
  - Restart virtual machines on other hosts if there is a host crash
- Real High Availability
  - Running an “invisible” hot standby VM on a secondary host that is kept in sync
- Fully automatic live VM moving
  - Load Balancing virtual machines across virtualization hosts
Capture Strategies
Capture Strategy #1

- Install Wireshark on the virtual system of interest

  **Advantages:**
  - Can capture, even on VMs with internal only NICs
  - Easy to do

  **Disadvantage:**
  - Changes the environment
  - Gets funny results (way too often)
  - May crash the VM
Capture Strategy #2

- Capture at virtualization host uplink (TAP/SPAN)
- Maybe your only option when you have no better access to the virtual infrastructure
- Advantages:
  - Easy to do in simple setups
  - Usually gets good data
  - Most familiar way to get data since it's similar to physical captures
Capture Strategy #2

- Disadvantages:
  - May get you tons and tons of data to sort
  - Server uplink may be too fast for your capture device
  - VM may be live-moved off the server, interrupting the capture
  - Worst case: you don’t even know where to capture!
Real World Example
„Too much data“

• Ways to handle „too much data“ (a.k.a „dropped frames“) on physical captures:
  – use frame slicing if possible
  – SPAN only as few affected ports or VLANs as possible
  – use a filtering TAP
  – Capture Filters on the Wireshark itself may help, too
New Capture Strategies

Virtual captures for a virtual environment
New Capture Strategies

• Virtualization technologies may or may not offer additional capture strategies
• The big question usually is „what can you do with that virtual switch thingy?“ 😊
• Worst case: the vSwitch behaves like a dumb switch (a.k.a. Desktop Switch) – out of luck 😞
New Capture Strategies

- Promiscuous vSwitch Mode (a.k.a „let’s play hub...“)
- Virtual SPAN sessions
- Virtual TAPs
No more slides, so... lets go!
Questions?