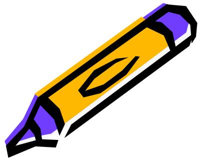
ARP vulnerability issues in migration

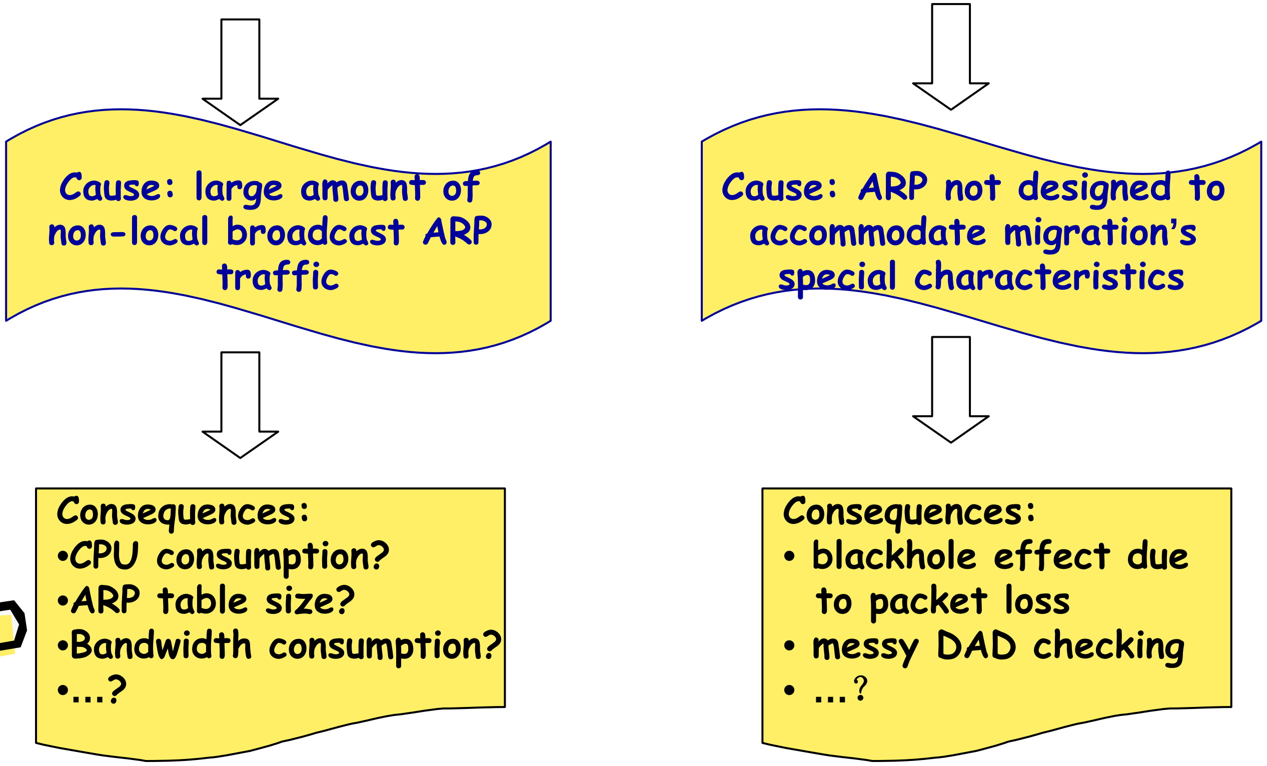


liyizhou@huawei.com

Scope of ARMD?

Scalibility issues ✓

Vulnerability issues ?

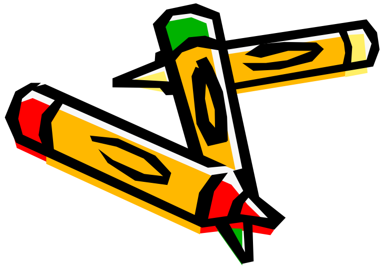


Cause: large amount of non-local broadcast ARP traffic

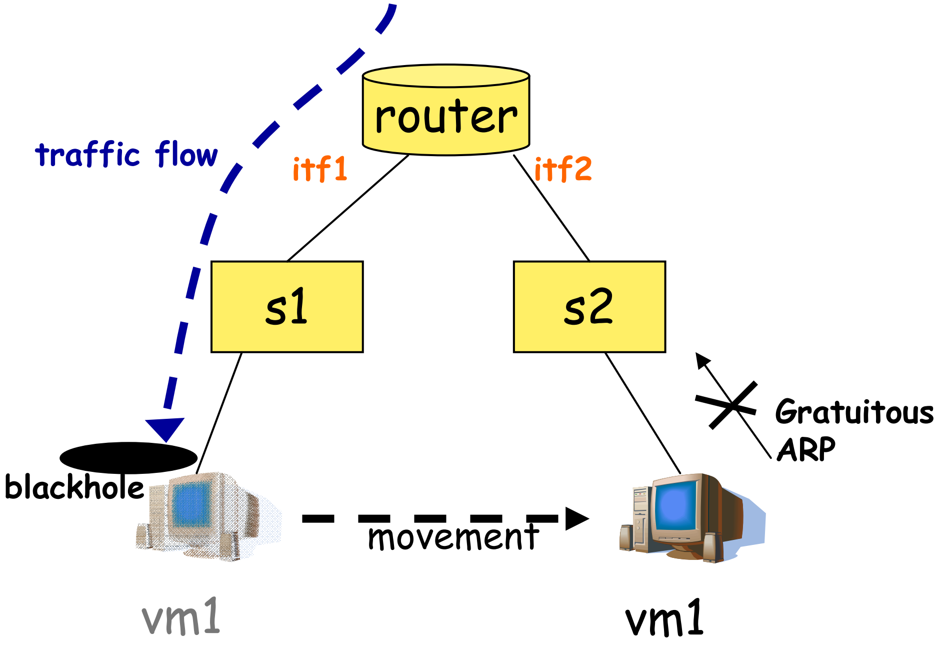
Consequences:
- •CPU consumption?
- •ARP table size?
- •Bandwidth consumption?
- •…?

Cause: ARP not designed to accommodate migration's special characteristics

Consequences:
- blackhole effect due to packet loss
- messy DAD checking
- …?



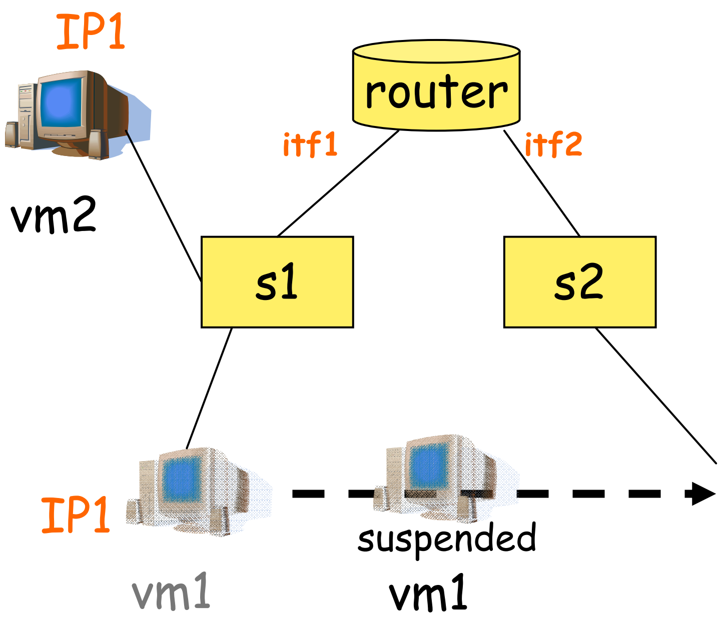
Vulnerability Issues (1) – ARP packet loss



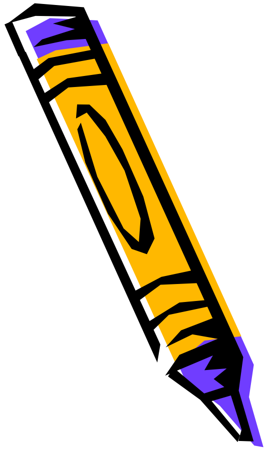
- Address resolution:

  IP + MAC + Interface
- Blackhole issue: gratuitous ARP lost due to congestion
- Severe consequence, esp when traffic is uni-directional
- Normal congestion control mechanisms (re-trans, reducing sending rate) do not help
- Recovered by next successful gratuitous ARP or ARP reply

Vulnerability Issues (2) – DAD (duplicate address detection)



- Suspension time always exists when vm moves
- Suspension time = vm's non-responding time
- Not able to respond to DAD
- Late comer (vm2) may take over IP (vm'1 IP) legally
- Mess up the address allocation



Solicit the feedback

- ARMD covers “vulnerability issues” too?
- Suggestions?

Scalibility issues ✓

Vulnerability issues ✓