Virtual Host Identity and Address Resolution for Cloud Computing Service

Problem Statements

Linda Dunbar (ldunbar@huawei.com)
Sue Hares (shares@huawei.com)
Ning So (ning.so@verizonbusiness.com)
Infrastructure As A Service
- Service Model

Client can request a Virtual Subnet (with a group of VMs) to run their applications.
Client can also request multiple Virtual Subnets. They can define policy among Virtual Subnets.

Another client may request a Virtual Network with multiple virtual Subnets. The Client defines policy among their Virtual Subnets.

Application

Virtual Subnet (Closed User Group)

Network Infrastructure

Service Provider owns the Network Infrastructure and Physical Data Center Infrastructure
Most likely, it is IP/MPLS networks which interconnect multiple data center sites.
Virtual Subnet

- Cloud Computing service needs Network to provide Virtual Subnets and Virtual hosts
  - Virtual hosts within one virtual subnet can span across different sites due to customer requirement or resource allocation
  - Some virtual subnets can only be connected by Private Networks (layer 2 or/and layer 3)
Identity to physical IP/MAC address resolution

- Virtual hosts come and go. But each service provider’s IP/MAC address space is no unlimited.
- Therefore, it is important to have a scalable Address Resolution protocol to map virtual host’s identity to physical IP/MAC addresses.
Virtual Host’s identity

- Virtual host identity has be associated with its Virtual Network
- Similar to IP to Ethernet MAC ARP (RFC826), Cloud Computing service needs “Virtual Host Identity” to IP/MAC address resolution
Proposal to IETF

  - To develop scalable address resolution protocols (IPv4 ARP & IPv6’s ND) for Cloud Computing Service with large amount of virtual subnets & virtual hosts, and for data center with large amount of virtual hosts, including
    - Proper identity for virtual subnets and virtual hosts
    - Address resolution protocols to resolve physical IP/MAC addresses from virtual hosts identities.
    - Duplicated address detection, make sure solutions don’t break IGMP redirect and various components of IPv6 ND
  - Security to detect/prevent gratuitous ARPs from malicious hosts.
  - To develop network solutions to allow virtual hosts see other virtual hosts as if they are on one subnet, but the network interconnect them can be anything (Layer 2 or/and Layer 3).
  - To develop solutions to scope the broadcast messages, including ARP and DHCP, so that broadcast storm are confined to smaller zones.
  - To develop solutions of handling of multicast messages among virtual hosts in one Virtual Subnet which spans across multiple locations.

- **List address:** arp222@ietf.org
  - Archive: [http://www.ietf.org/mail-archive/web/arp222/](http://www.ietf.org/mail-archive/web/arp222/)
  - To subscribe: [https://www.ietf.org/mailman/listinfo/arp222](https://www.ietf.org/mailman/listinfo/arp222)