Service Provider NAT44 Overview

NANOG

October 2010

Jason Weil

your friend in the digital age®

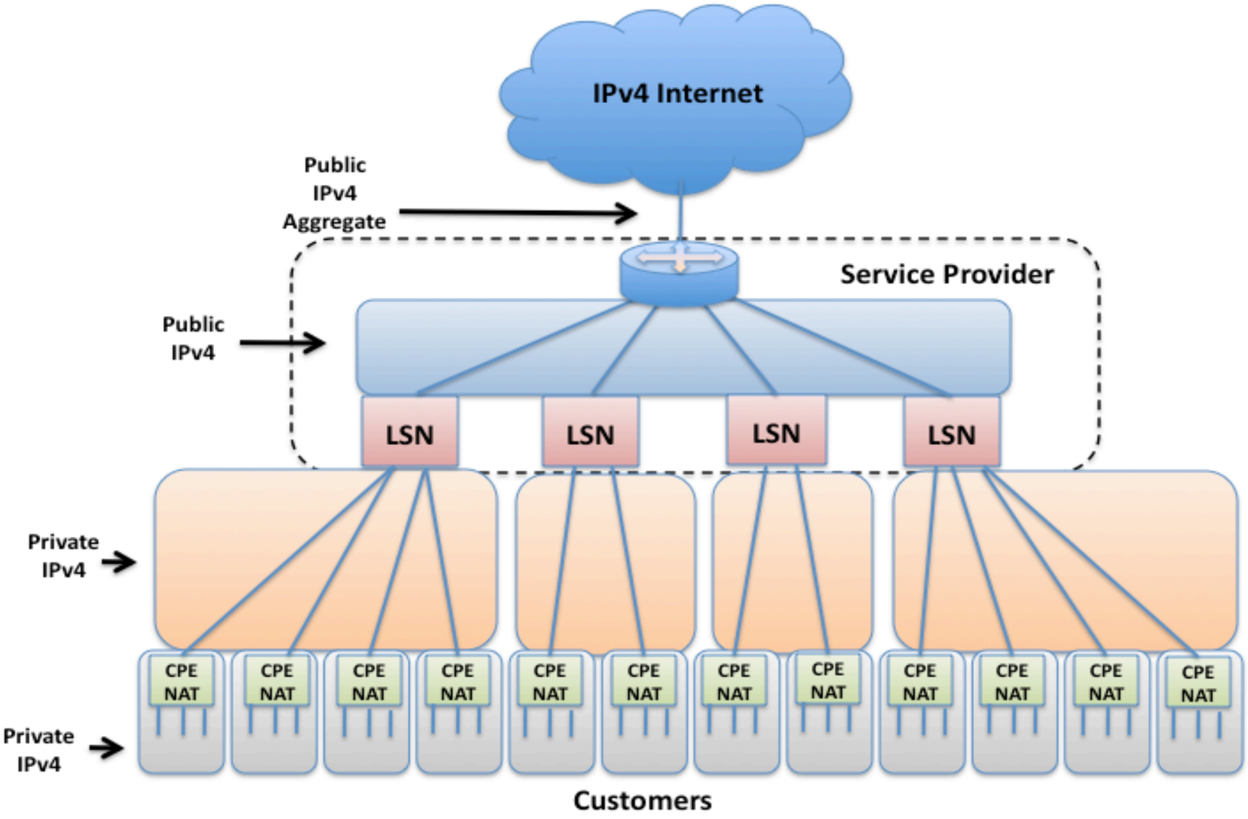
COX®

Service Provider NAT44

- Service Provider NAT44 goes by many names
  - CGN - Carrier Grade NAT
  - LSN - Large Scale NAT
  - NAT444 – three fours implies the existence of two layers of NAT44
- Comparisons to Residential NAT44
  - Residential NAT44
    - NAT44 address realm bounded by Home Gateway and CE devices
    - Single Public IPv4 address represents one household
      - Full 16 bit Layer 4 Port availability
    - Utilizes RC1918 space – 192.168/16 or 10/8
  - Service Provider NAT44
    - SP NAT44 address realm bounded by SP NAT device and the customer's Home Gateway
    - Single Public IPv4 address shared across multiple households
      - Limited Layer 4 Port Availability
    - Preferred implementation employs Shared Provider Space to avoid address overlap in two layered NAT scenarios

SP NAT44 Diagram

- Service Provider NAT Realm – between LSN and CPE NAT
- Residential NAT Realm: South of CPE NAT



SP NAT44 Deployment Considerations

- Two Primary Deployment Options
  - In-line Model
    - Common Enterprise Deployment Model
    - Creates a single point of failure for all traffic forced to traverse this path
  - NAT-on-a-stick Model
    - Source-IP based routing to SP NAT44
    - Removes NAT from primary data path
- Deployment Considerations
  - Logging infrastructure
  - Operational overhead associated with SP NAT44 challenges
- Benefits of SP NAT44
  - Well-understood technology with many years experience
  - Residential NAT44 device does not require replacement
  - Enforces Accepted Use Policies

Challenges with Service Provider NAT44

- Identifying users by IP address no longer possible
  - Now: Customer=Public IP Address
  - SP NAT44: Customer=Public IP+Port+Time Stamp
- SP NAT44 breaks current UPnP deployments
  - Solutions currently being studied
- Address conflicts between the residential private realm and service provider private realm
  - Potential Solution: Shared Provider Space
    - https://tools.ietf.org/html/draft-weil-opsawg-provider-address-space-02
    - http://tools.ietf.org/html/draft-shirasaki-nat444-isp-shared-addr-04
- Security issues
  - Blacklisting/Whitelisting
    - Many household/users behind a single IPv4 address
  - IP Rate-limiting
    - Impacts applications that set max transactions per second by IP
  - NAT device becomes an attractive attack target
- Reduction in resiliency
  - SP NAT44 device is a single point of failure for all users

Use Cases

- Assumptions:
  - RIR Address pool exhausted
  - Provider is no longer able to provision customer with public IPv4
  - Provider is actively deploying IPv6
  - No IPv6 support in some percentage of deployed retail gateways
  - No IPv6 support in some percentage of consumer CE devices
- Use Case 1: Single Stack IPv4
  - Scenario 1: Provider Network Segment unable to support IPv6
  - Scenario 2: Customer Home Gateway unable to support IPv6
  - Solution allows extension of current IPv4 address…at a price
  - Solution assumes reduced functionality for IPv4 access
- Use Case 2: Dual-stack Native IPv6 + SP NAT IPv4
  - Scenario: Consumer Electronic devices require IPv4-only connectivity
  - Solution allows continued access to the IPv4 Internet
  - Solution assumes reduced functionality for IPv4 access

Conclusions

- SP NAT will be deployed
  - Only question is to what extent
- Preferred topology is standalone NAT–on-a-stick model
  - Limits impact on primary data stream
  - Dedicated box allows for separation of function
- Many challenges with implementing any Shared Addressing model
- Service will be limited in functionality
- Users will benefit by upgrading the residential network to IPv6