Utmaningen för Operatörerna

Janne Östling
Systems Engineer, CCIE #11450

21 Oktober 2011

The 5th Wave By Rich Tennant

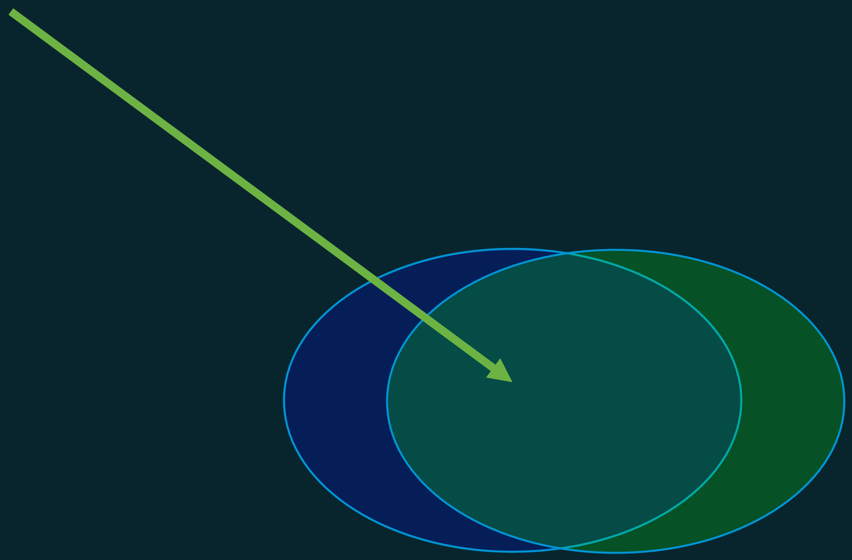
Agenda

- Adresstilldelning
- Säkerhet
- Övergångsmekanismträsket…

Which prefix size to customers?

- /48? -> 65536 subnets
- /53? -> 2048 subnets
- /56? -> 256 subnets
- /64? -> 1 subnet
- /128? -> WTF?

Shared Security Issues ?



IPv4 Vulnerabilities

IPv6 Vulnerabilities

IPv6 Attacks with Strong IPv4 Similarities

- Sniffing

  IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4

- Application layer attacks

  The majority of vulnerabilities on the Internet today are at the application layer, something that IPSec will do nothing to prevent

- Rogue devices

  Rogue devices will be as easy to insert into an IPv6 network as in IPv4

- Man-in-the-Middle Attacks (MITM)

  Without strong mutual authentication, any attacks utilizing MITM will have the same likelihood in IPv6 as in IPv4

- Flooding

  Flooding attacks are identical between IPv4 and IPv6

The IPsec Myth: IPsec End-to-End will Save the World

- IPv6 mandates the implementation of IPsec
- IPv6 does not require the use of IPsec
- Some organizations believe that IPsec should be used to secure all flows...
  - Interesting **scalability** issue (n^2 issue with IPsec)
  - Need to **trust endpoints and end-users** because the network cannot secure the traffic: no IPS, no ACL, no firewall
    - IOS 12.4(20)T can parse the AH
  - Network **telemetry is blinded**: NetFlow of little use
  - Network **services hindered**: what about QoS?

Recommendation: do not use IPsec end to end within an administrative domain.
Suggestion: Reserve IPsec for residential or hostile environment or high profile targets.

Preventing IPv6 Routing Attacks Protocol Authentication

- BGP, ISIS, EIGRP no change:
  - An MD5 authentication of the routing update
- OSPFv3 has changed and pulled MD5 authentication from the protocol and instead is supposed to rely on transport mode IPSec
- RIPng, PIM also rely on IPSec
- IPv6 routing attack best practices
  - Use traditional authentication mechanisms on BGP and IS-IS
  - Use IPSec to secure protocols such as OSPFv3 and RIPng

Reconnaissance in IPv6? Easy with Multicast!

- No need for reconnaissance anymore
- 3 site-local multicast addresses

  FF05::2 all-routers, FF05::FB mDNSv6, FF05::1:3 all DHCP servers

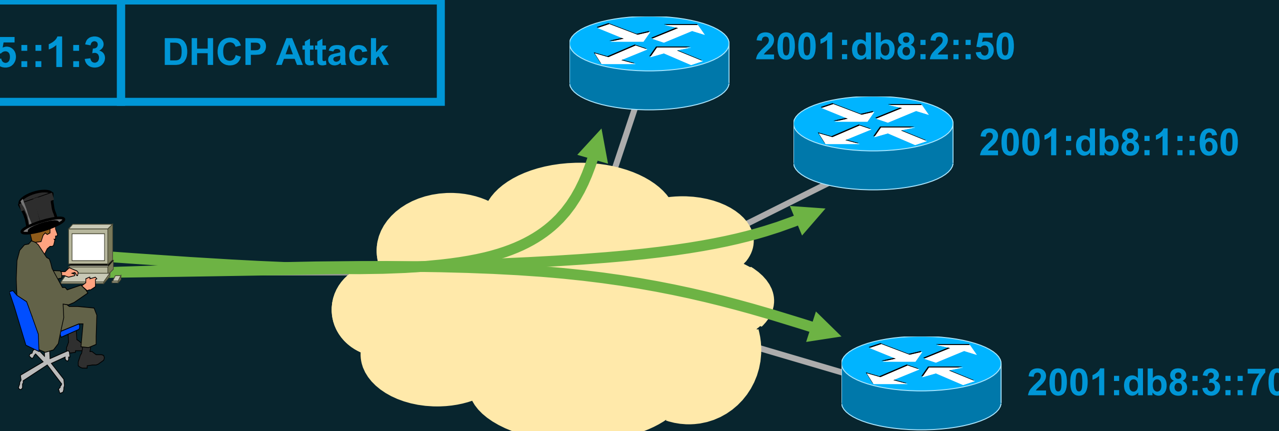
- Several link-local multicast addresses

  FF02::1 all nodes, FF02::2 all routers, FF02::F all UPnP, ...

- Some deprecated (RFC 3879) site-local addresses but still used

  FEC0:0:0:FFFF::1 DNS server

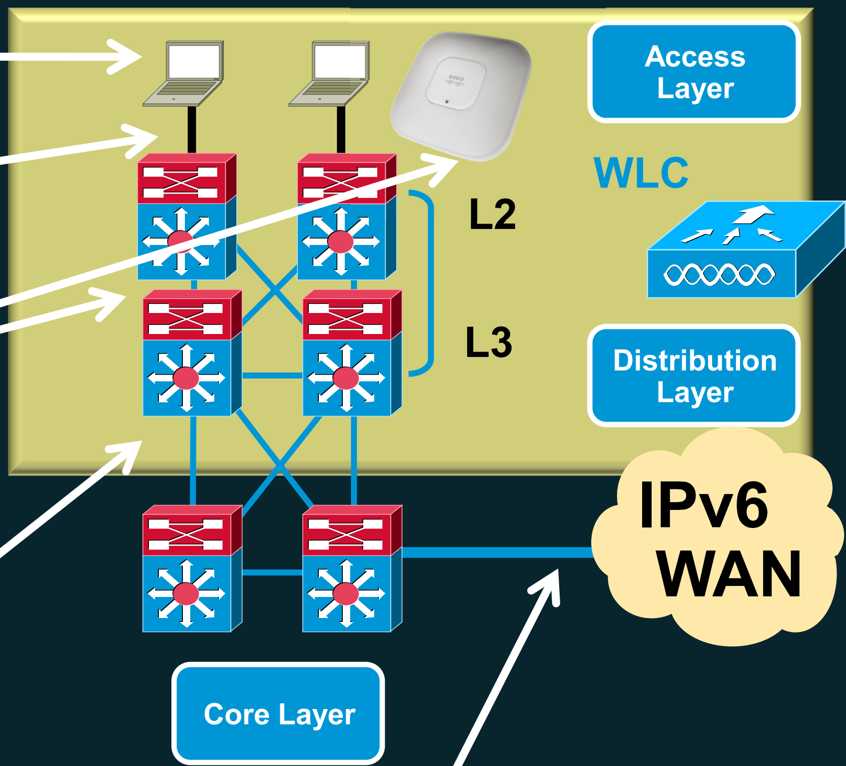
Source	Destination	Payload
Attacker	FF05::1:3	DHCP Attack



http://www.iana.org/assignments/ipv6-multicast-addresses/

IPv6 First Hop Security

IPv6/IPv4 Dual Stack Hosts



IPv6 Device Tracking
Revoke network access for inactive devices

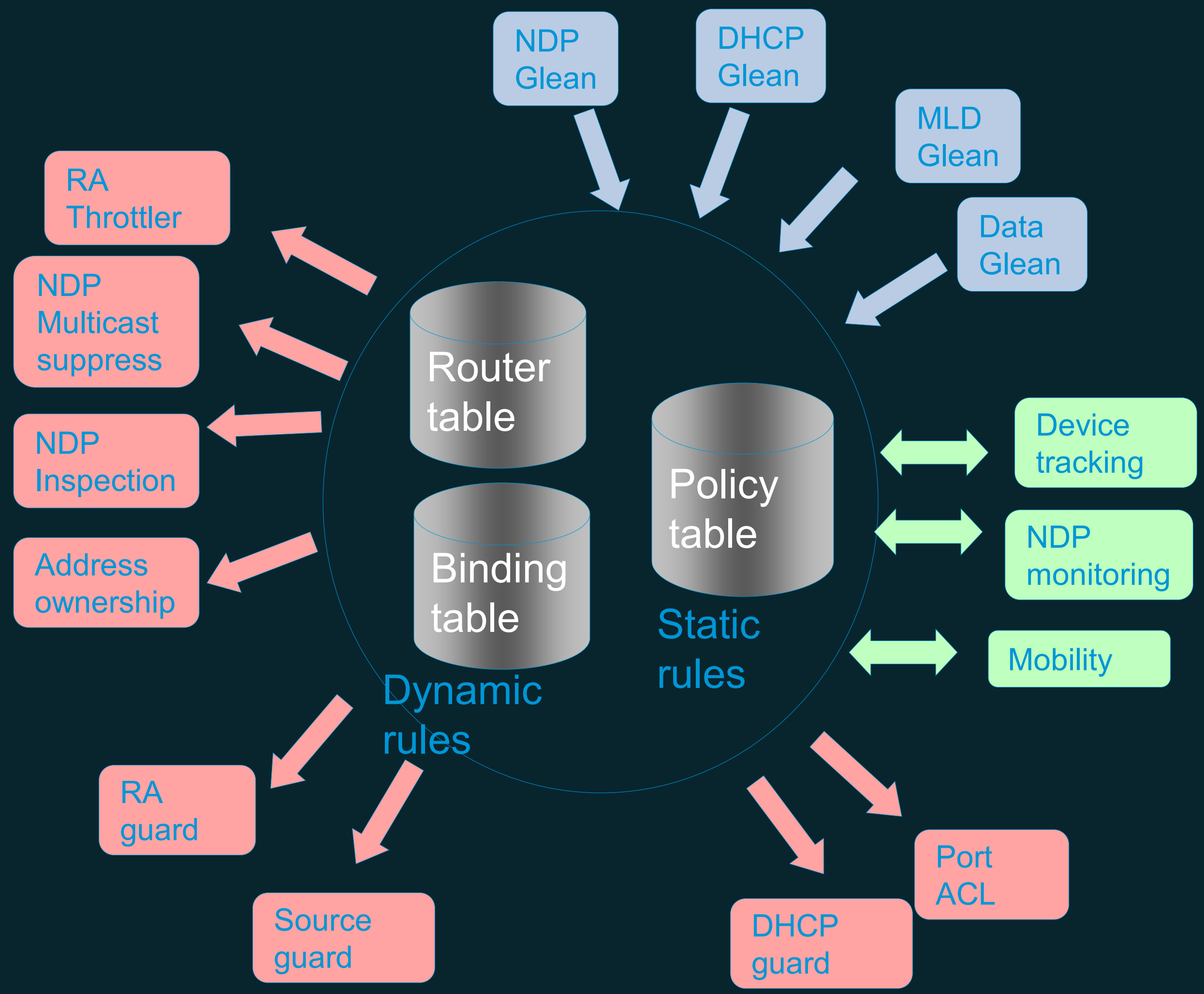
IPv6 PACL
Filter traffic on Layer 2 ports

IPv6 RA Guard
Stops false router advertisement threats

IPv6 NDP inspection
Prevents neighbor discovery spoofing attacks

IPv6 uRPF
Blocks spoofed traffic in hardware

IPv6 Snooping Software Architecture



ARP Spoofing is now NDP Spoofing: Mitigation

- **BAD NEWS**: nothing like dynamic ARP inspection for IPv6
  - Will require new hardware on some platforms
- **GOOD NEWS**: Secure Neighbor Discovery
  - SEND = NDP + crypto
  - IOS 12.4(24)T
  - **More BAD NEWS**:
    - But not in Windows Vista, 2008 and 7
    - Crypto means slower...
- Other **GOOD NEWS**:
  - Private VLAN works with IPv6
  - Port security works with IPv6
  - 801.x works with IPv6

First Hop Security Features Plans

Released in Phase I

- Port ACL
- ACL Based RA Guard
- ACL based DHCP Guard
- RA Guard
- NDP Inspection
- Device Tracking
- Per port address limit

Phase II

- DHCPv6 inspection
- DHCPv6 Guard
- Source Guard
- DAD Proxy

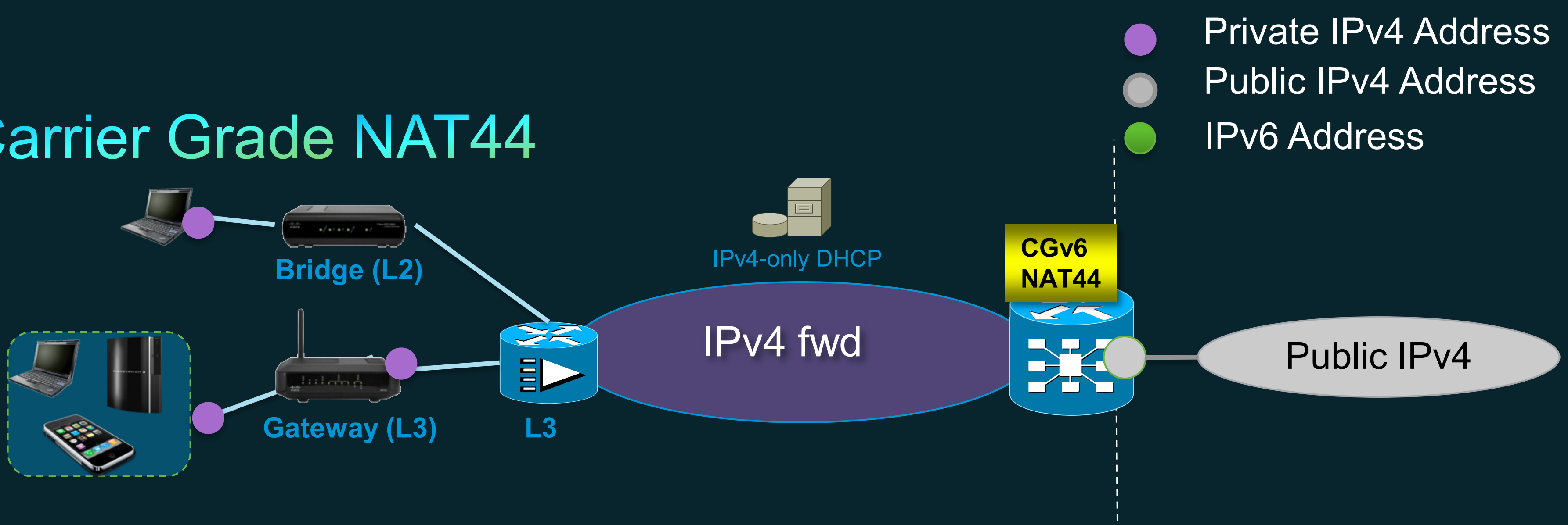
Phase III

- Destination Guard
- Prefix Guard
- Binding table recovery
- DHCPv6 Relay L2 (LDRA)

IPv4-IPv6 Transition/Coexistence

- A wide range of techniques have been identified and implemented, basically falling into three categories:
  1. Dual-stack techniques, to allow IPv4 and IPv6 to co-exist in the same devices and networks
  2. Tunneling techniques, to avoid order dependencies when upgrading hosts, routers, or regions
  3. Translation techniques, to allow IPv6-only devices to communicate with IPv4-only devices
- Expect all of these to be used, in combination

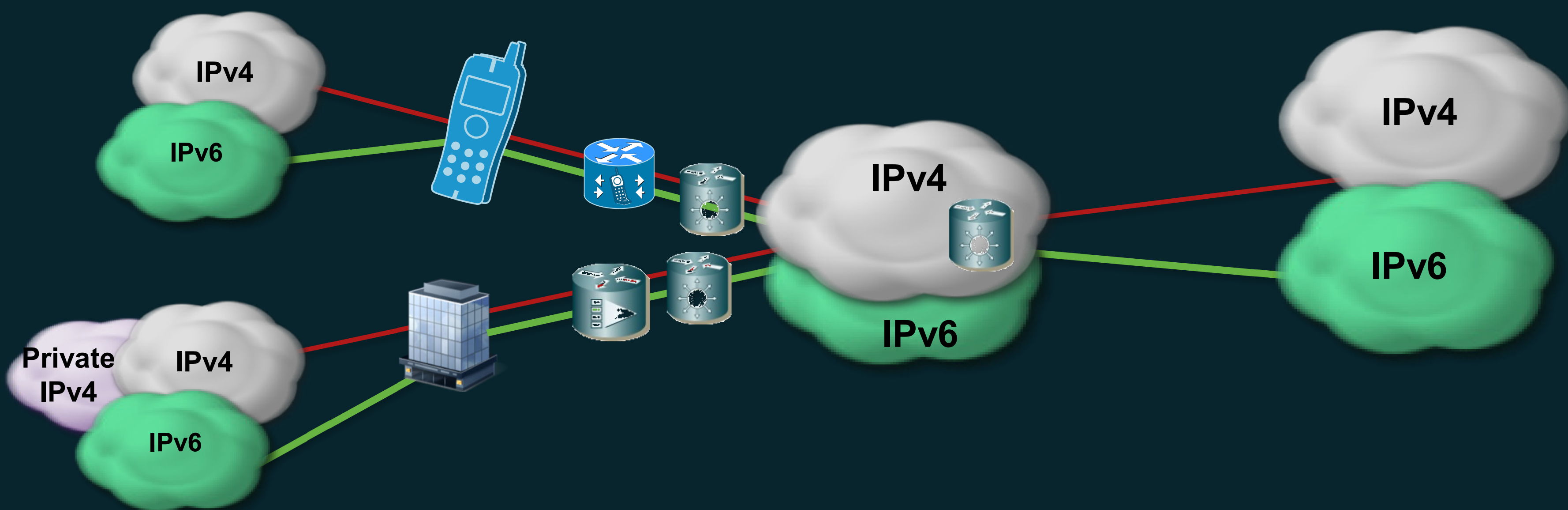
Carrier Grade NAT44



- Preserves public IPv4 address space
  - Ports become shared, managed resource
  - Compliant with standard NAT behaviors (RFC4787, 5382, 5508)
- Stateful NAT44
  - Translator state built via outgoing session
  - TCP/UDP timers
  - Port limit per subscriber

Dual-Stack

Private IPv4 Address
Public IPv4 Address
IPv6 Address

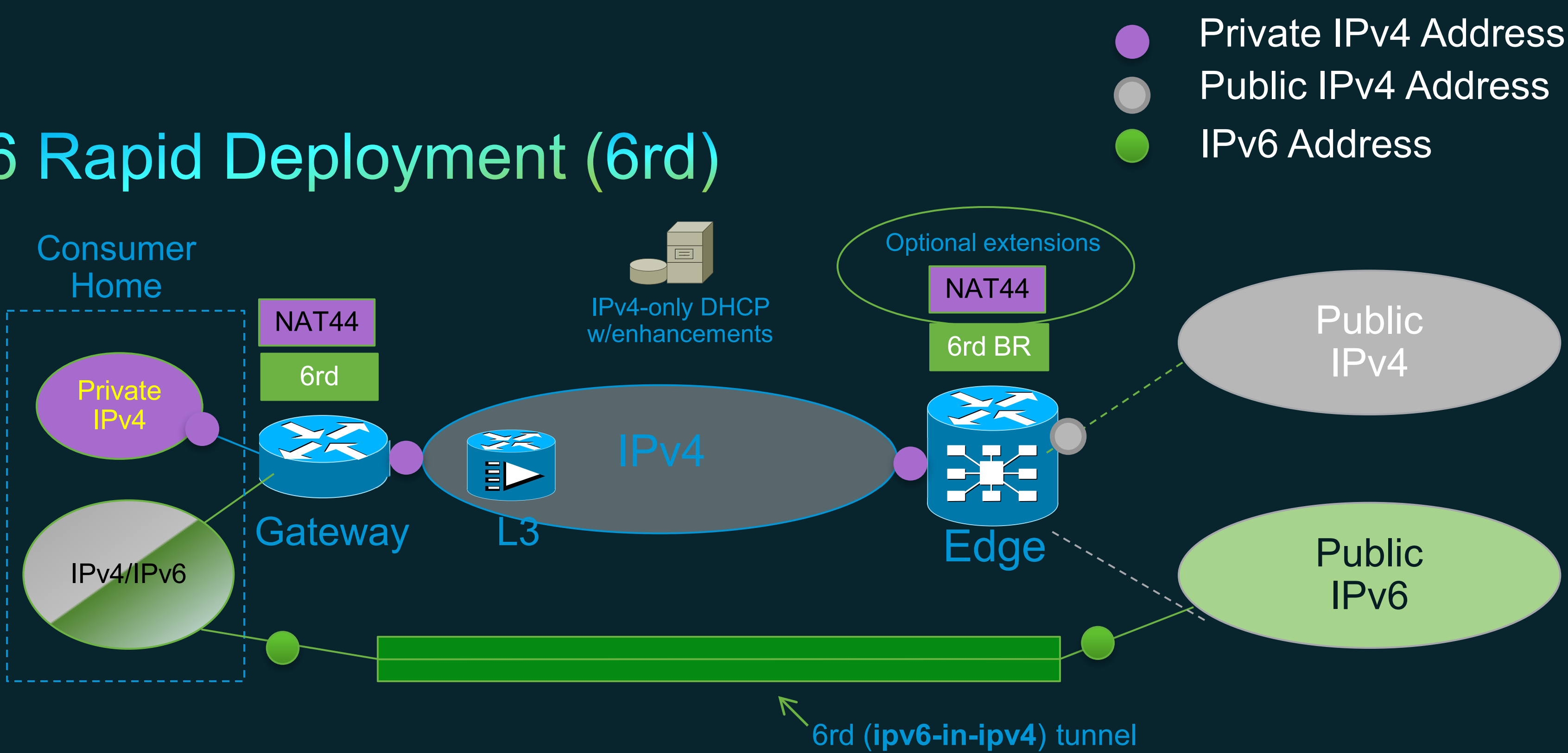


- Classic RFC 4213 solution
  - Logical deployment choice when one has little control over end-point
- *In the short term deploying IPv6 in dual stack does not solve IPv4 exhaust*; IPv4 shortage is expected before full deployment
  - Can be easily combined with NAT44 solution, while allowing IPv6 deployment ramp-up

Using Tunnels for IPv6 Deployment

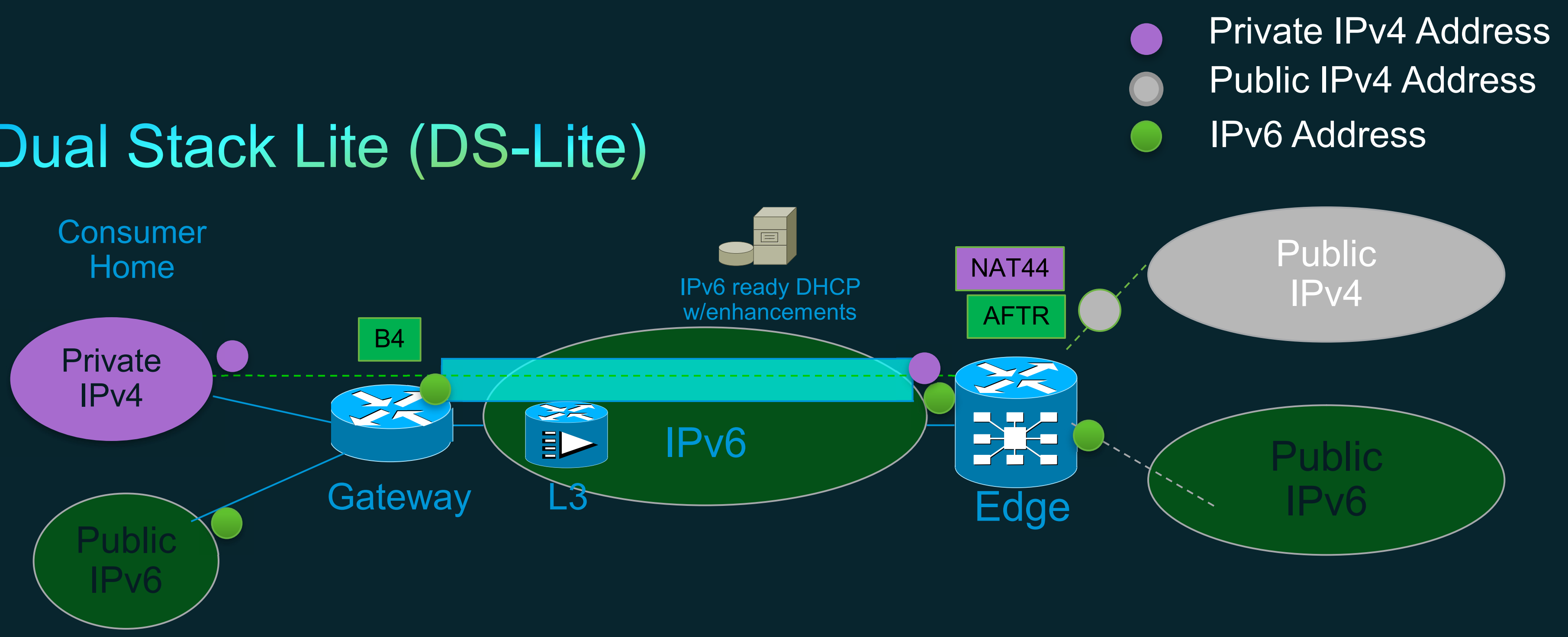
- Many techniques are available to establish a tunnel:
  - Manually configured
    - Manual Tunnel (RFC 2893)
    - GRE (RFC 2473)
    - (MPLS)
  - Automatic
    - 6 over 4
      - Compatible IPv4 (RFC 2893): Deprecated
      - 6to4 (RFC 3056)
      - 6over4: Deprecated
      - ISATAP (RFC 4214)
      - Teredo (RFC 4380)
      - 6rd
    - 4 over 6
      - DS-Lite
      - 4rd
      - dIVI
      - A+P

IPv6 Rapid Deployment (6rd)



- Native IPv4 forwarding and IPv6 tunneling
- 6rd aware devices: RG and Border Relay
- Simple: Stateless, automatic encaps/decaps
- Standard: rfc5969
- Optional CGN(NAT44). IPv6 will offload NAT44.

Dual Stack Lite (DS-Lite)



- Introduction of two functional components: B4 and AFTR

  B4 elements responsible for encap/decap of IPv4 into IPv6

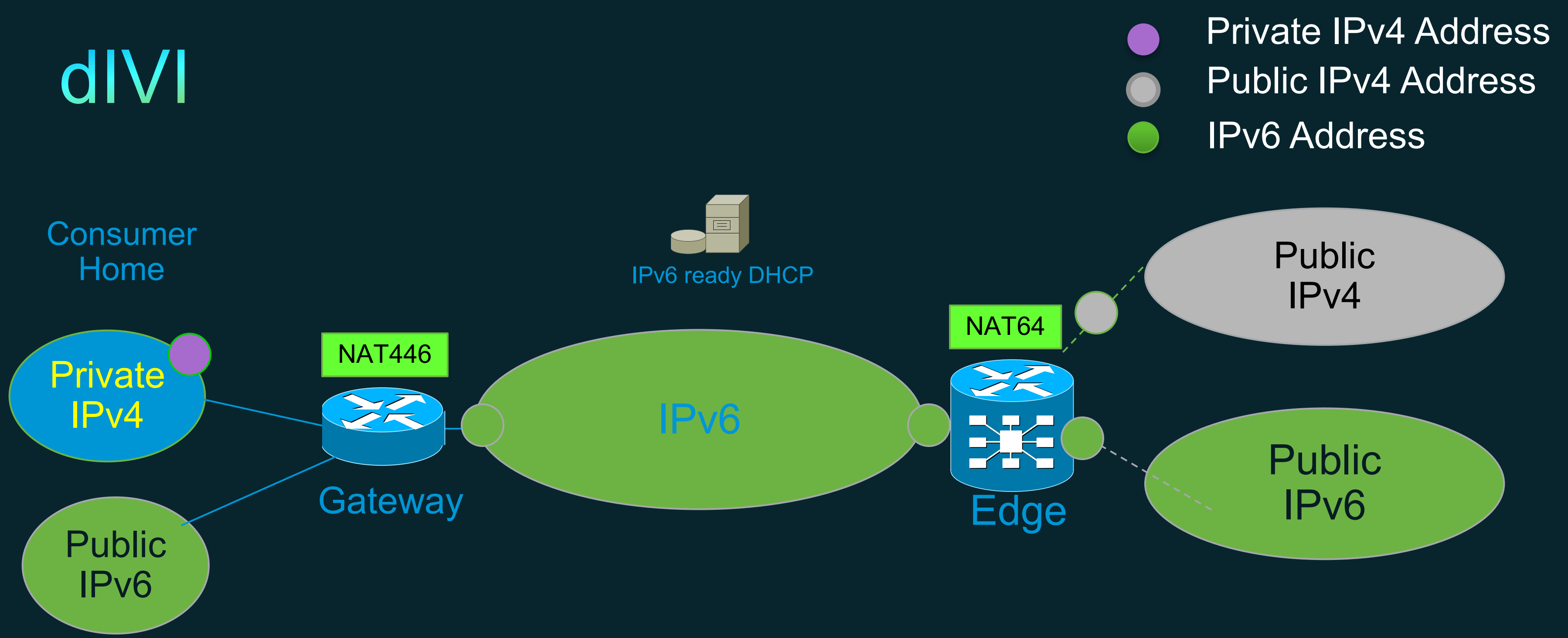
  NAT44 is disabled in B4

  Private IPv4 LAN address common on all gateways (e.g. 192.168.0/24)

  AFTR Node responsible for aggregated encap/decap of IPv4 into IPv6

  AFTR Node performs NAT44 translation indexed with IPv6 tunnel src

dIVI



- Introduction of two functional components: NAT446 and NAT64
  - NAT446 = Stateful port restricted NAT44 + Stateless NAT46
  - Stateless NAT64 (can be reused for IPv6-only ⬄ IPv4 Internet)
- How it works? (IETF draft-xli-divi)
  - CPE derives public IPv4 address and port range schema from IPv6 addr
  - NAT is done on the gateway (no CGN)
  - Algorithmic mapping for IPv4/IPv6 translation

Summering

- Adresstilldelning – Det löser sig om man har hjärnan påslagen!
- Säkerhet – Finns hål kvar att upptäcka/utnyttja.
- Övergångsmekanismträsket… - Den som lever får se…

IPv4 to IPv6 transition and the stages of grief

Thank you.