Secure EVPN MAC Signaling

draft-thubert-bess-secure-evpn-mac-signaling

Pascal Thubert, Tony Przygienda, and Jeff Tantsura

IETF 112

Virtual

Snooping IPv6 SLAAC for eVPN: Building on Sand

- As opposed to DHCP, SLAAC is not stateful / deterministic

Þ Nodes may remain silent, or move silently, or unreliable multicast: missing state

Þ May leave, drop addresses and form new ones unbeknownst: wasted/stale state

Þ Device identification and location through movement uncertain and insecure

- Major hassles on large networks / wireless / overlays

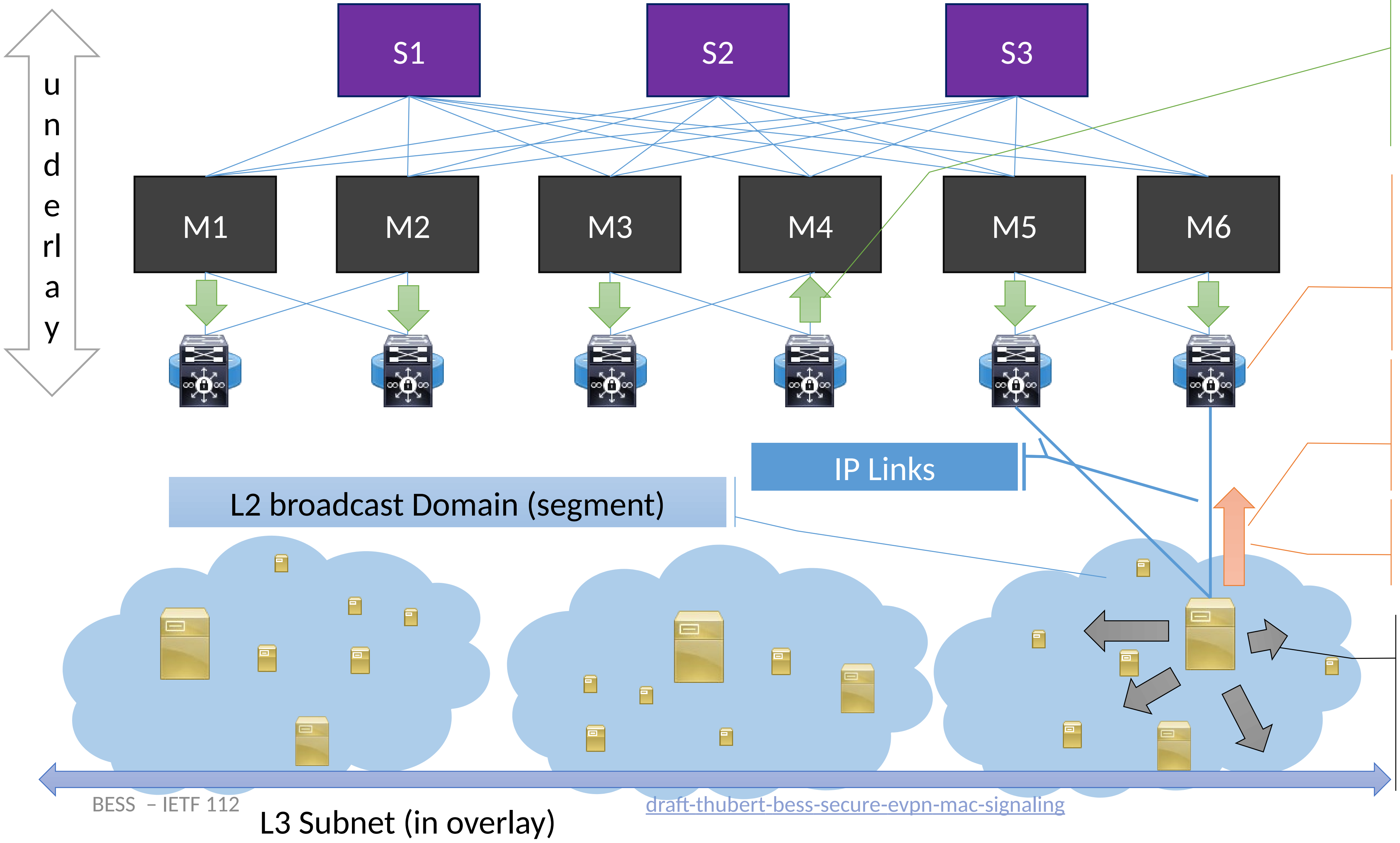
Þ Onlink model forces L3 Subnet and L2 Broadcast Domain Congruence

Þ Makes broadcast storms several time worse per address (MLD + DAD + Lookup)

Þ Forces permanent address presence (address defense by the host)

Þ Requires MLD which causes more state than stateful AAC if deployed

Issues with IPv6 ND SLAAC (Non-Deterministic snooping)



NS Lookup for Silent node causes broadcast ND in overlay (BUM)

Snooping SLAAC is unreliable, causes silent nodes and stale state

SLAAC prone to attacks (DDOS, address theft, SAVI)

SLAAC lacks mobility signaling

L2 broadcast domain must remain congruent with L3 constructs

SFAAC: Deterministic and Secured Presence

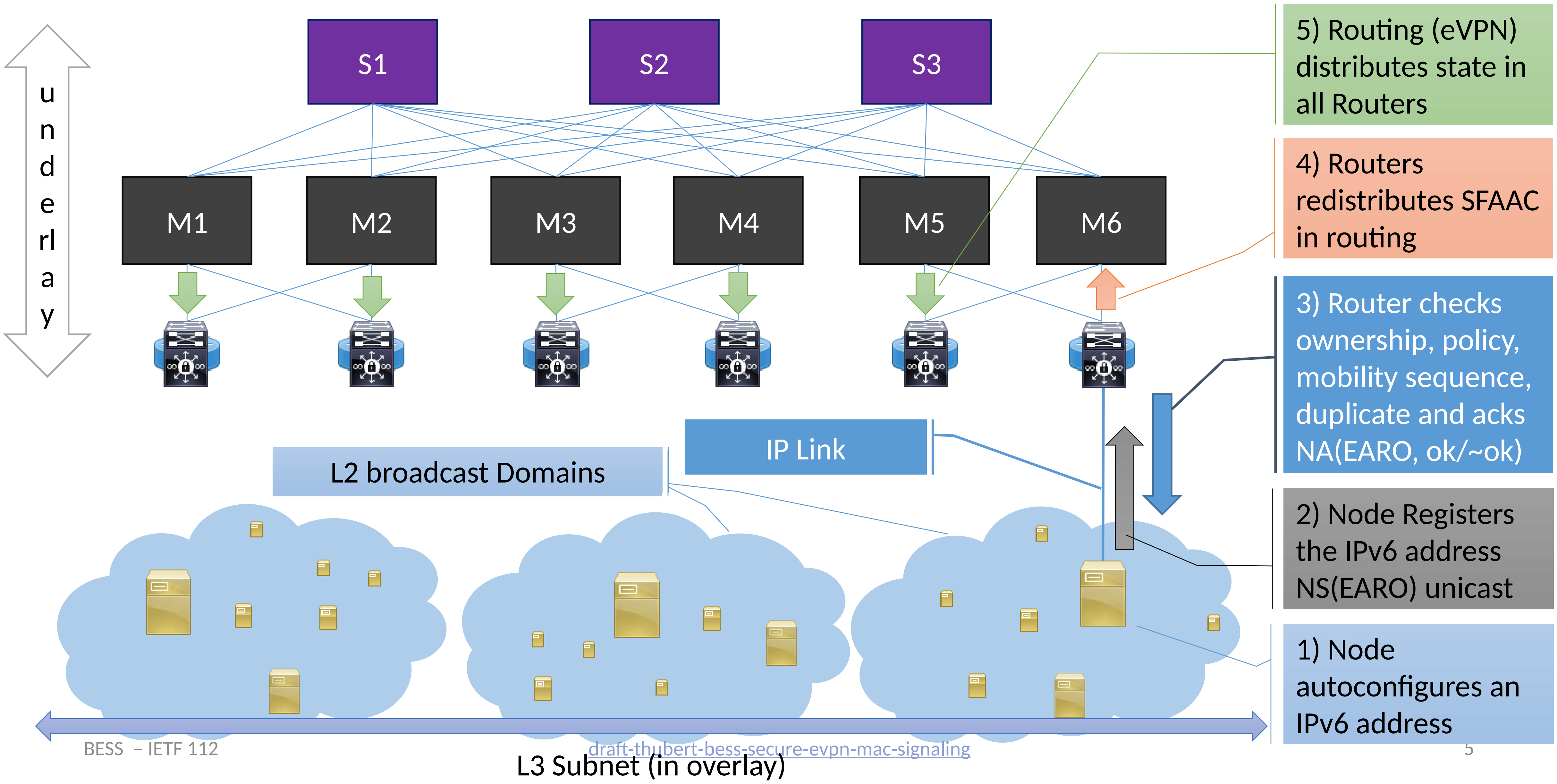
- RFC 8505 StateFul (Proactive) Address AutoConfiguration
  - Address Registration + meta, allow instant DAD and overlay setup
  - Lifetime, Unique ID, <u>sequencing to manage mobility</u>
  - Exposes IPv6 address + MAC + Location
  - Avoids broadcast, silent node and scanning DDOS
  - Simpler – no MLD, no async broadcast, no block/pun

6LoWPAN

IPv6-based Low-power
Wireless Personal Area Networks

- RFC 8928 Proof of Ownership
  - Associates a token to the address registration
  - Based on auto-configured key pair
  - Only the owner of the private key can modify the address and source packets
  - Enables SAVI protection, trusted injection in routing protocols

Stateful IPv6 ND: Creates a deterministic state for routing



5) Routing (eVPN) distributes state in all Routers

4) Routers redistributes SFAAC in routing

3) Router checks ownership, policy, mobility sequence, duplicate and acks NA(EARO, ok/~ok)

2) Node Registers the IPv6 address NS(EARO) unicast

1) Node autoconfigures an IPv6 address

StateFul Address AutoConfiguration: Principles

- Stateful Like DHCPv6, autoconfiguration like SLAAC

Þ Deterministic address presence through ins and outs, with maintained state (not a cache)

- Interaction with local router (UNI) as opposed to with a remote server

Þ Unicast and immediate (no DAD), meant to populate routing / lookup state on backend

- Abstract to router to router (NNI): supports RIFT, eVPN, RPL, ND proxy…
- Abstract registrar: can be centralized (e.g., LISP) and distributed (e.g., BGP)
- Advertises Lifetime, mobility sequence (TID), and Proof of Ownership

Redistributing RFC 8505/8928 in eVPN

- RFC 8929 IPv6 ND Proxy, can be leveraged in eVPN fabric
  - Proxies RFC 8505 in a mixed network, can reply to legacy ND or unicast NS
  - Routing Proxy: Router / L3 switch / L3 AP replies with its MAC address
  - Switching Proxy: L3 switch / L3 AP replies with its MAC address
  - Enables multilink subnet with L2 isolation
- In eVPN: draft-thubert-bess-secure-evpn-mac-signaling
  - Distributes the registrar (6LBR) across PEs, datastore is BGP table
  - Modifies interaction with the host (ROVR challenge)
  - Mobility validation (EDAR over the datapath)
  - Modified MAC Mobility Extended Community (ROVR Hash + TID)

Backup

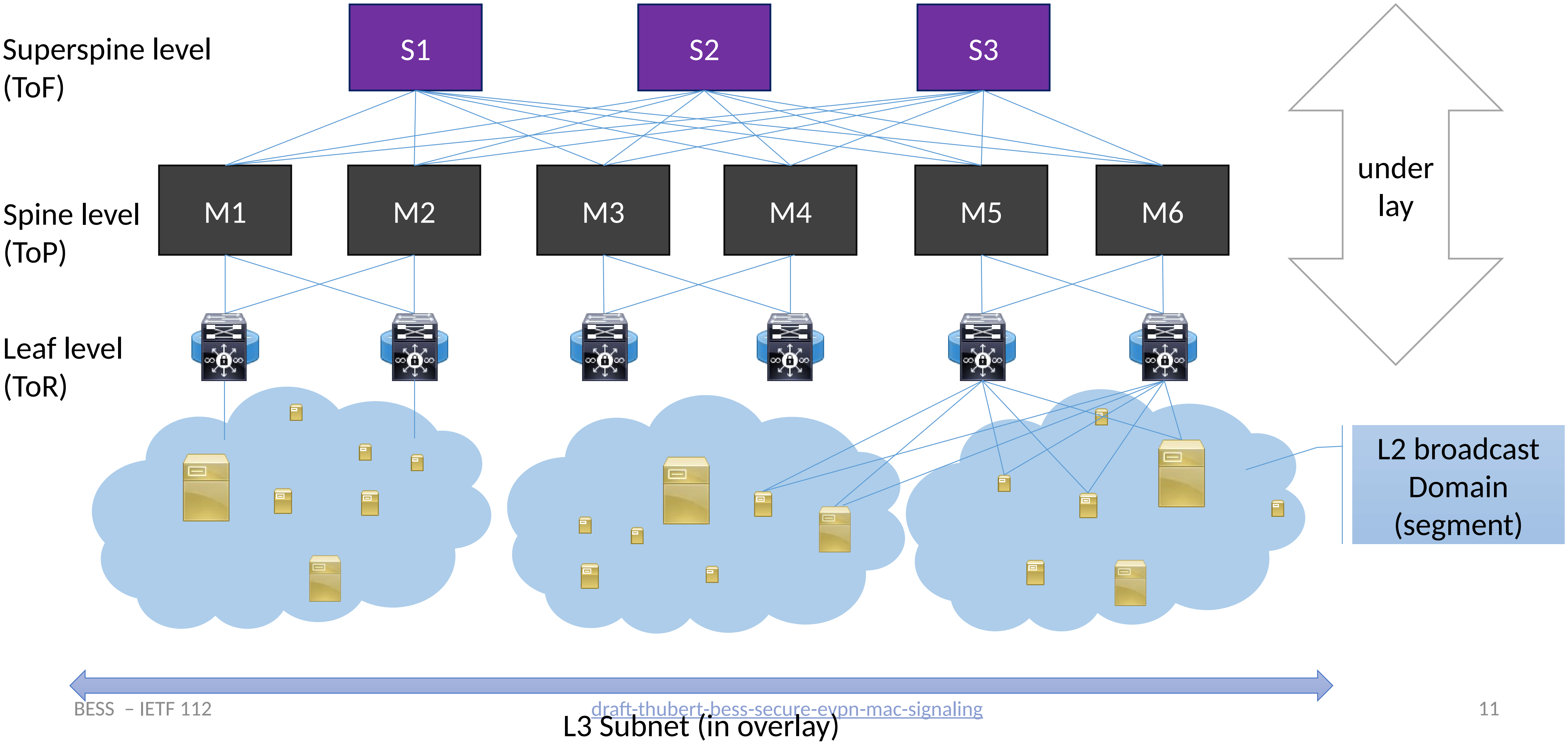
IPv6 of Y2K: Largely derived from IPv4 of 198

- RFC 4861/2 (IPv6 ND) adds SLAAC, mcast, and L3 abstraction
  - but is still reactive, broadcast-heavy, same mechanics as IPv4
- Link model still P2P and Transit
  - Bad match for wireless and distributed cloud / overlays
- IPv6 security / ACL model / IPSec
  - nothing new, quasi same impersonation and DDOS attacks
- IPv6 has128 bits addresses, Extension Hdr and flow label
  - But largely unexploited (except SRv6), e.g., /64 to host
- DHCPv6 IA-NA provides same deterministic addressing
  - No address protection, no sense of mobility

New Expectations in Cloud and overlays

- Deterministic Address Presence/Location
  - BUM: Optimize B&M, no U. Neither L2 Broadcast nor silent nodes
- Automated DevOps => NetOps importation
  - As opposed to passing excel spreadsheets around
- Simplification (flat network)
  - As opposed to overlay definitions and induced latencies
  - Decouple IP Link, IP Subnet and L2 broadcast domain
- Micro-segmentation (policies applied within and between tenants)
  - As opposed to 1 tenant / server + VRF
- Better use of ECMP, instant steering around breakages
  - e.g., flow label switching, network coding at ingress

Generic eVPN Topology



Not-Onlink Model (aka Multi-Link Subnet)

- Prefix is advertised as not being onlink

Þ Host passes all packets to their routers, IP routing within the subnet

Þ Possibility to redirect inside shared L2 links

- Improves IPv6 Operation

Þ Separates the L2 Broadcast domains from L3 constructs

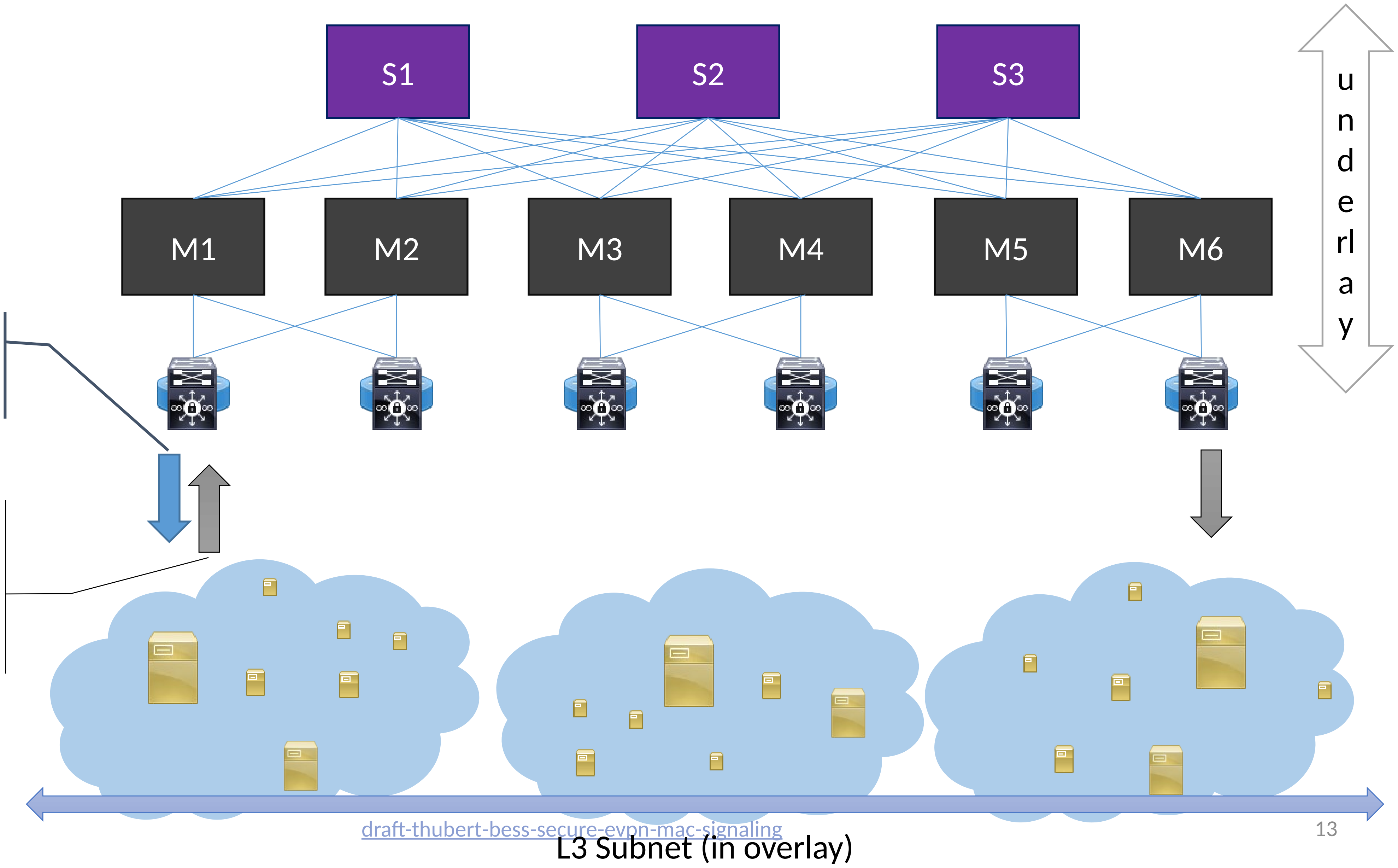
Þ Scalability and simplification

- But does not change SLAAC

Þ Same non-deterministic discovery, same unknowns and stale state

Þ Same address theft, impersonation and DDOS attacks

IPv6 ND with prefix not onlink: Forces traffic via the router



1) RA advertising Prefix not onlink

2) Nodes pass all traffic to routers (no address lookup)