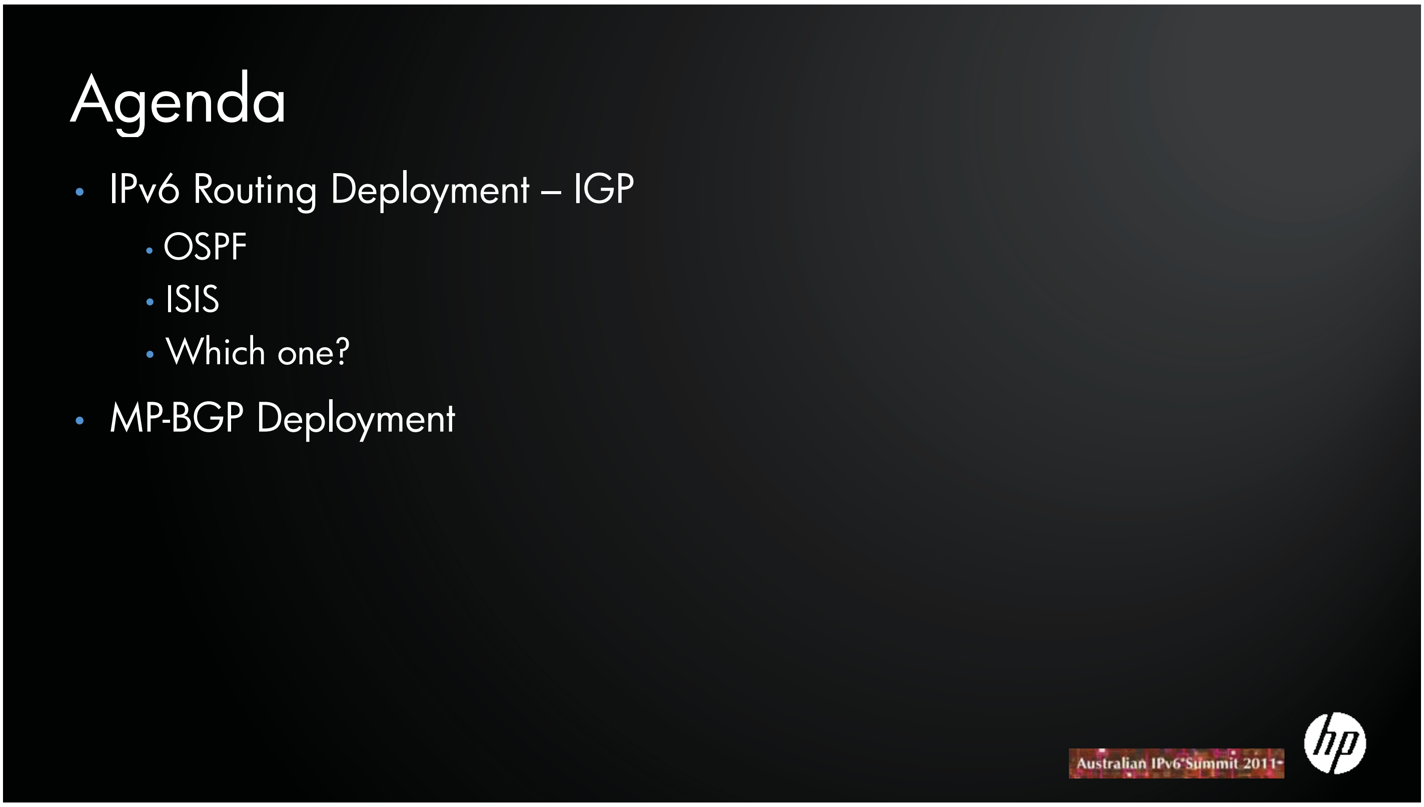
DUAL STACK DEPLOYMENT

Alvaro Retana (alvaro.retana@hp.com)
Distinguished Technologist

Australian IPv6 Summit 2011

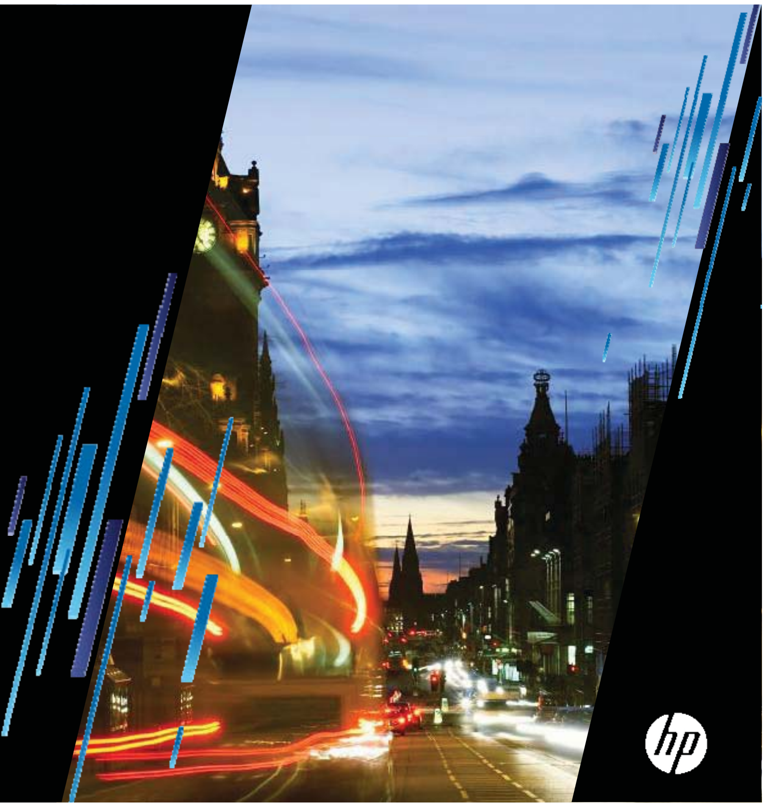


Agenda

- IPv6 Routing Deployment – IGP
  - OSPF
  - ISIS
  - Which one?
- MP-BGP Deployment

Australian IPv6 Summit 2011

OSPF



OSPFv3 and v2 Differences

- Changes made to OSPFv2 to accommodate increased address size of IPv6
- OSPF now runs on per-link, not per-subnet
- Removal of addressing semantics from OSPF packets and LSAs making it network-protocol-independent
- New LSAs created to carry IPv6 addresses and prefixes
- Addition of Flooding scope (similar to RFC2370)
- Explicit support for multiple instances per link
- Use of IPv6 link-local addresses for protocol processing and providing next hop information during packet forwarding
- Authentication method changes
- Packet format & LSA's header format changes
- Handling of unknown LSA types

OSPFv3 and v2 Similarities

packet type	Description
1	Hello
2	Database Description
3	Link State Request
4	Link State Update
5	Link State Acknowledgment

- OSPFv3 has the same 5 packet type but some fields have been changed
- Mechanisms for neighbor discovery and adjacency formation
- Interface types
  - P2P, P2MP, Broadcast, NBMA, Virtual
- LSA flooding and aging
- DR, BDR election, area support, SPF
- Nearly identical LSA types

OSPFv3 Flooding Scope

LS age	Options	LS type

LS age	U	S2	S1	LSA Function Code

- The high-order three bits of LS type {1 bit (U) for handling unrecognized LSA and two bits (S2, S1) for flooding scope} encode generic properties of the LSA, while the remainder, (called LSA function code) indicate the LSA's specific functionality
- OSPFv2 had two flooding scope, AS wide and area wide
- OSPFv3 has three flooding scope:
  - AS scope - LSA is flooded throughout the AS
  - Area scope - LSA is flooded only within an area
  - Link-local scope - LSA is flooded only on the local link

OSPFv3 Flooding Scope

- U (unrecognized) bit is used to indicate a router how to handle an LSA if it is unrecognized

U-bit	LSA Handling
0	Treat this LSA as if it has link-local Scope
1	Store and flood this LSA as if type understood

- S2 / S1 bit indicates the three flooding scopes

S2	S1	Flooding scope
0	0	Link-Local flooding scope
0	1	Area flodding scope
1	0	AS flooding scope
1	1	Reserved

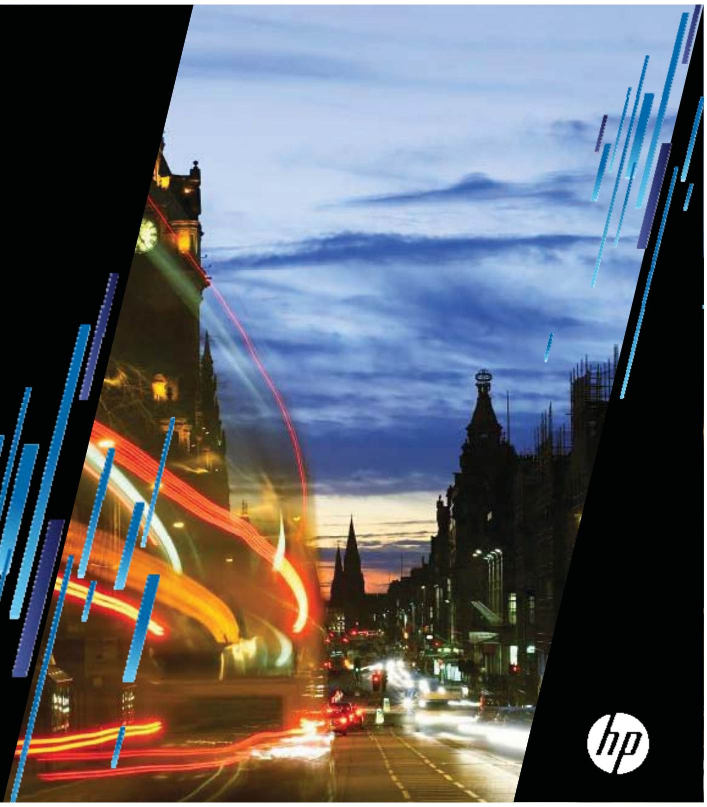
- Unrecognized LS type with flooding scope set to link local or area local can be flooded into stub area or NSSA with U bit set to 1

OSPFv3 LSA Types

- List of LSA in OSPFv3:

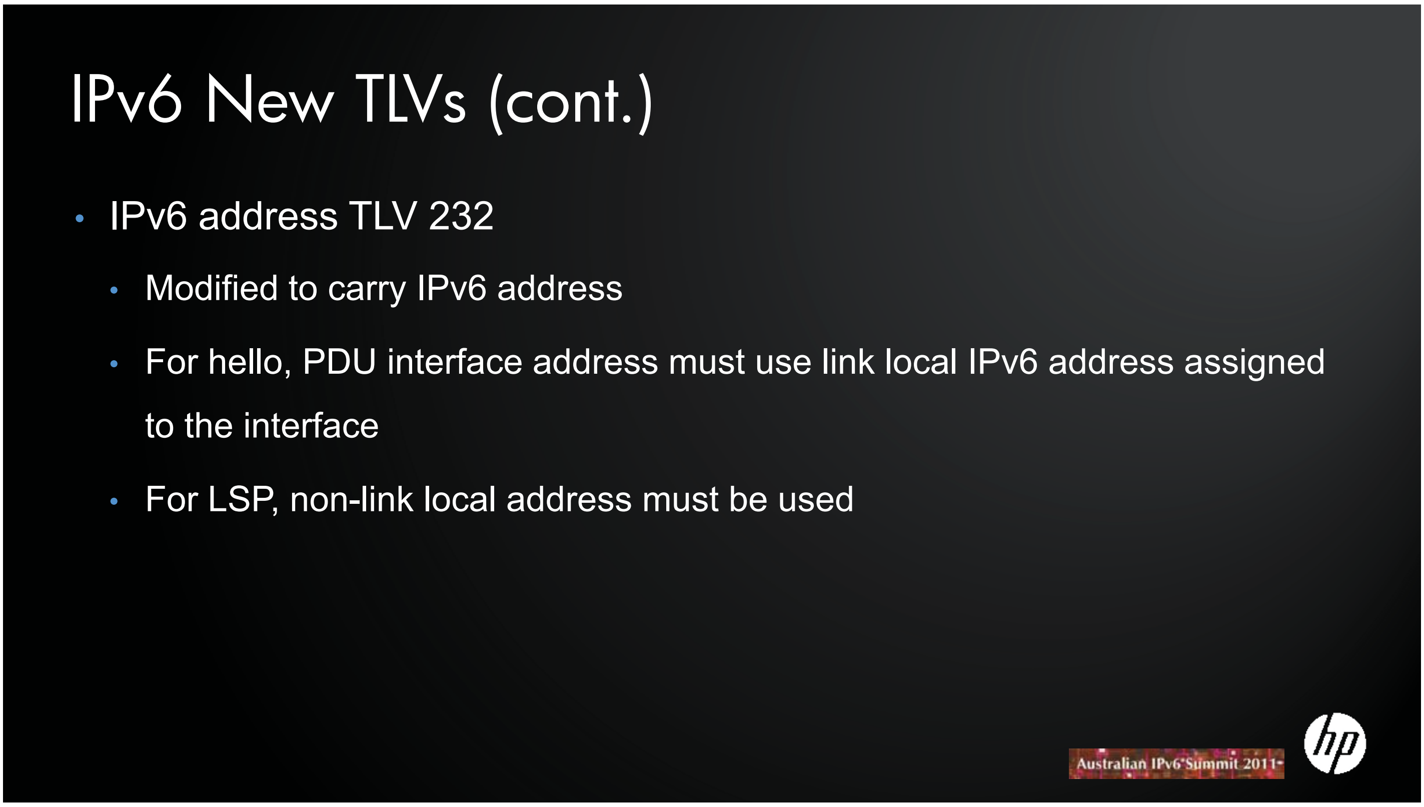
LSA Name	LS Type code	Flooding scope	LSA Function code
Router LSA	0x2001	Area scope	1
Network LSA	0x2002	Area scope	2
Inter-Area-Prefix-LSA	0x2003	Area scope	3
Inter-Area-Router-LSA	0x2004	Area scope	4
AS-External-LSA	0x4005	AS scope	5
Group-membership-LSA	0x2006	Area scope	6
Type-7-LSA	0x2007	Area scope	7
Link-LSA	0x0008	Link-local scope	8
Intra-Area-Prefix-LSA	0x2009	Area scope	9

ISIS



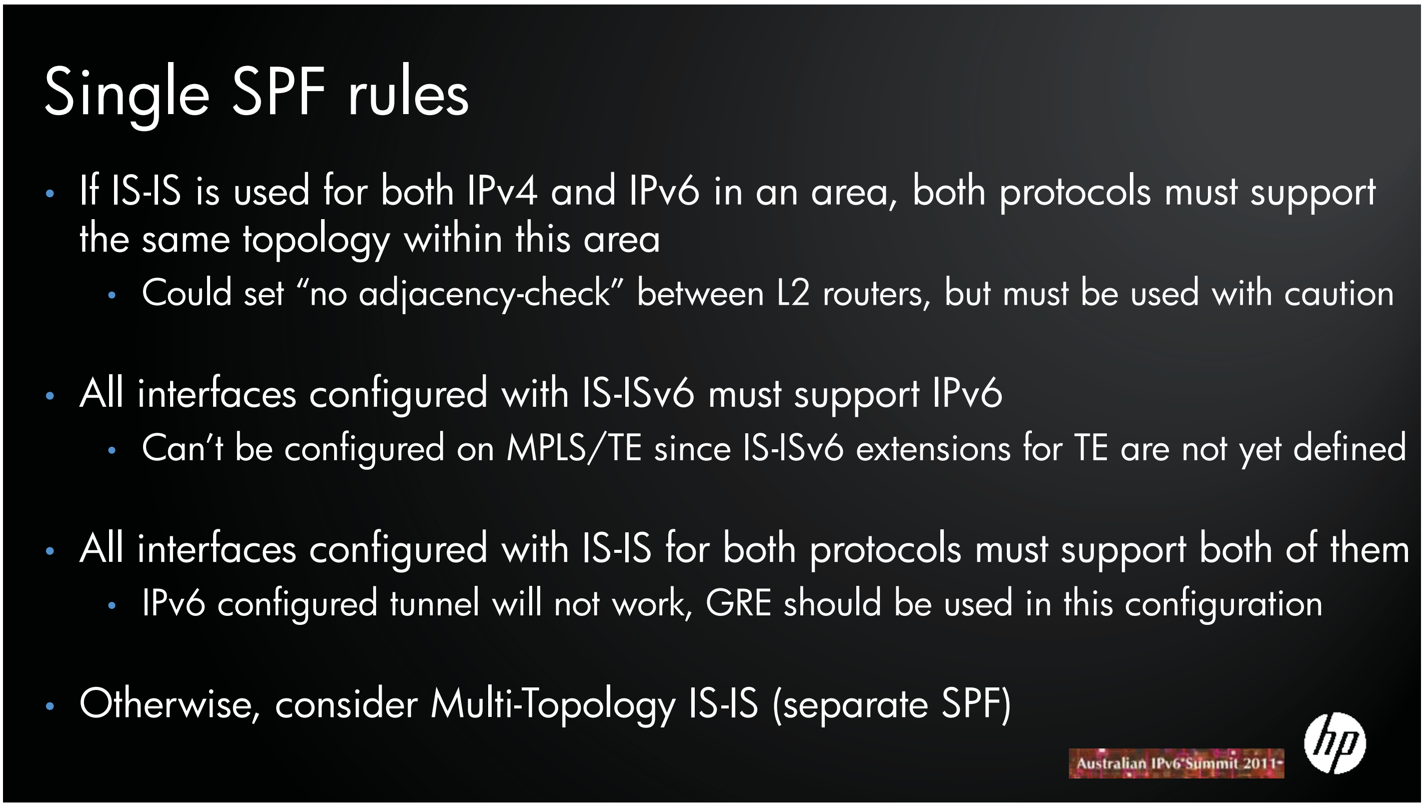
IPv6 New TLVs

- Defines both IPv6 Internal and External reachability information
  - Metric is still 32 bits
  - U: Up/Down
  - X: External origin bit
  - S: Sub-TLV present
  - Prefix length: Length of prefix 8 bits
  - Prefix: Number of octet is calculated depending on the prefix length



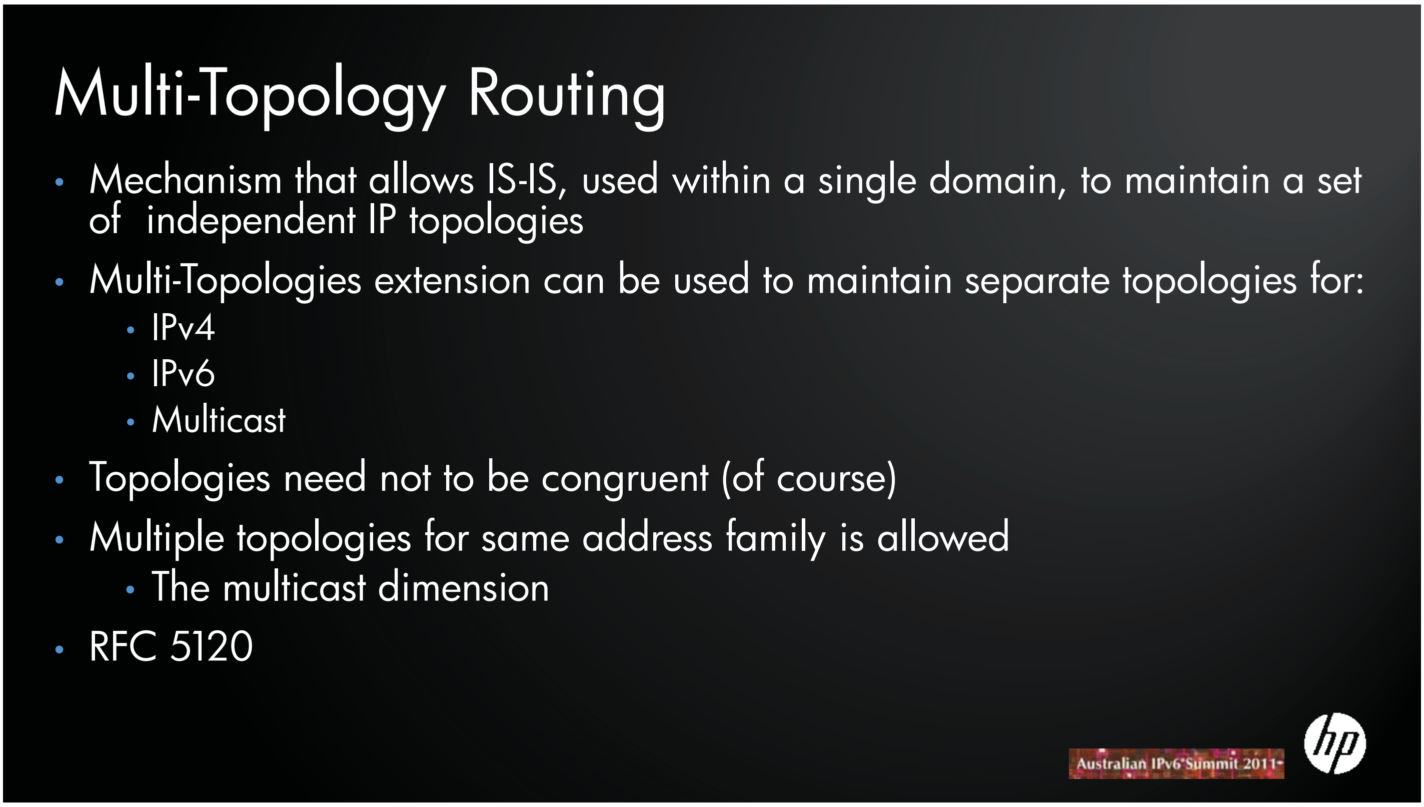
IPv6 New TLVs (cont.)

- IPv6 address TLV 232
  - Modified to carry IPv6 address
  - For hello, PDU interface address must use link local IPv6 address assigned to the interface
  - For LSP, non-link local address must be used



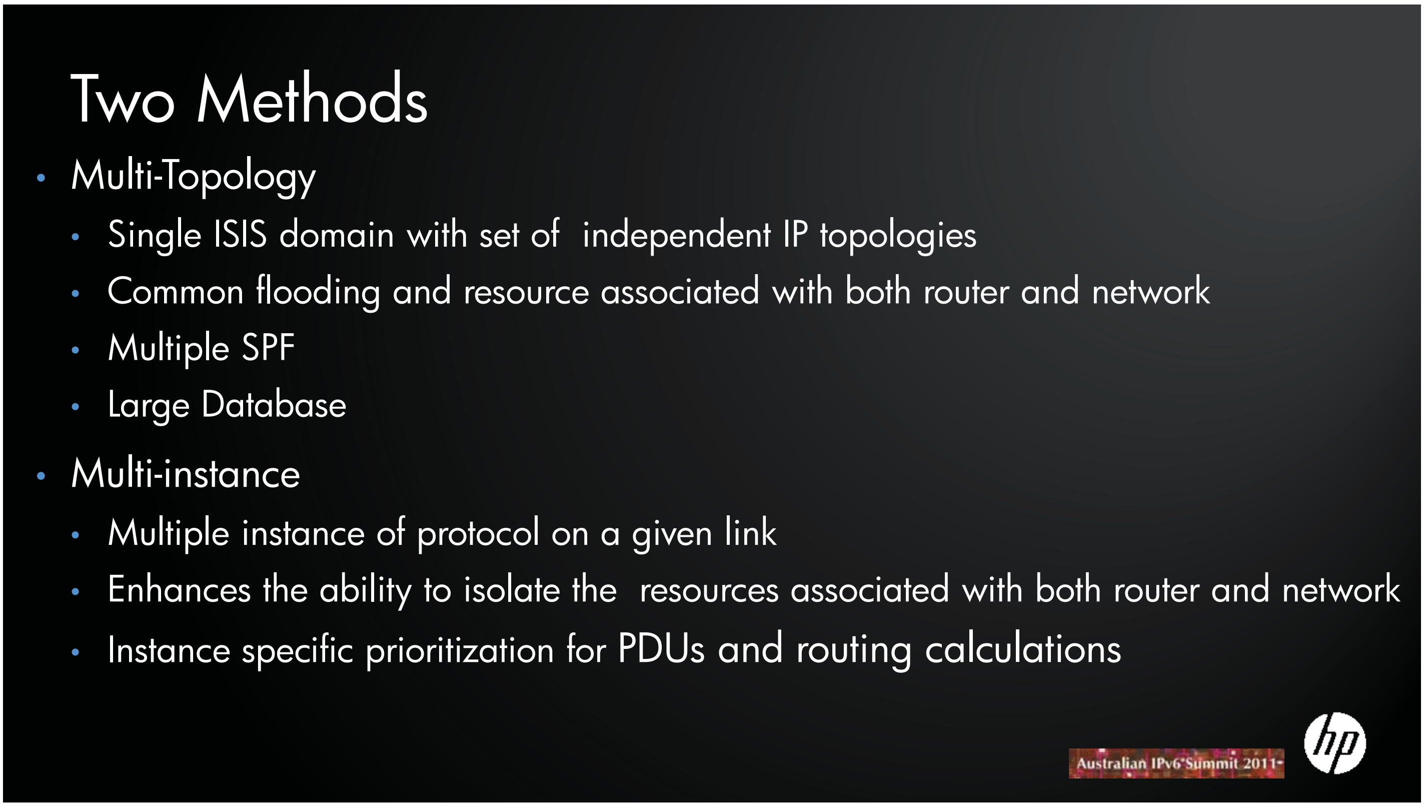
Single SPF rules

- If IS-IS is used for both IPv4 and IPv6 in an area, both protocols must support the same topology within this area
  - Could set “no adjacency-check” between L2 routers, but must be used with caution
- All interfaces configured with IS-ISv6 must support IPv6
  - Can’t be configured on MPLS/TE since IS-ISv6 extensions for TE are not yet defined
- All interfaces configured with IS-IS for both protocols must support both of them
  - IPv6 configured tunnel will not work, GRE should be used in this configuration
- Otherwise, consider Multi-Topology IS-IS (separate SPF)



Multi-Topology Routing

- Mechanism that allows IS-IS, used within a single domain, to maintain a set of independent IP topologies
- Multi-Topologies extension can be used to maintain separate topologies for:
  - IPv4
  - IPv6
  - Multicast
- Topologies need not to be congruent (of course)
- Multiple topologies for same address family is allowed
  - The multicast dimension
- RFC 5120



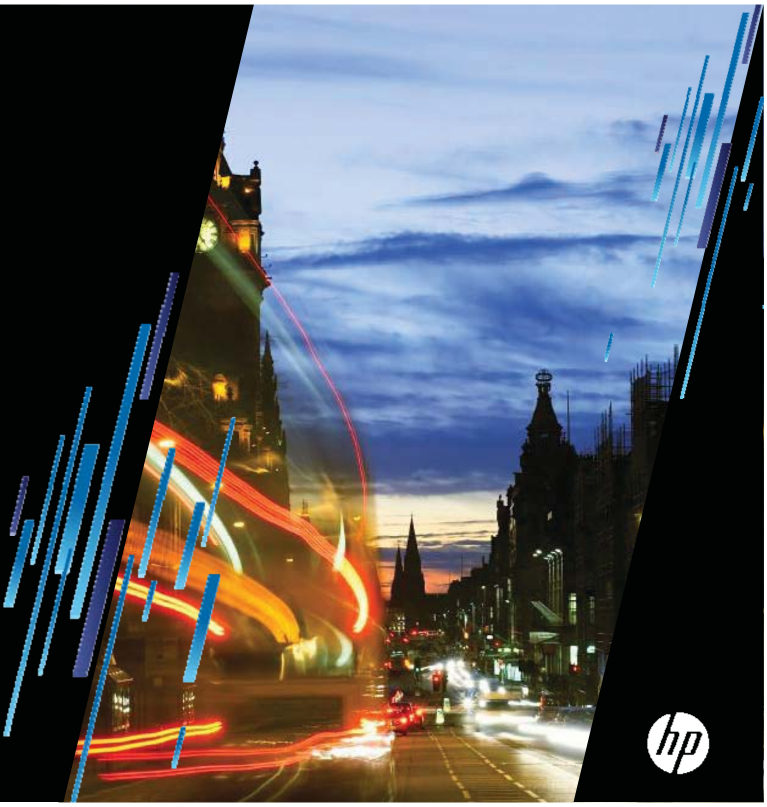
Two Methods

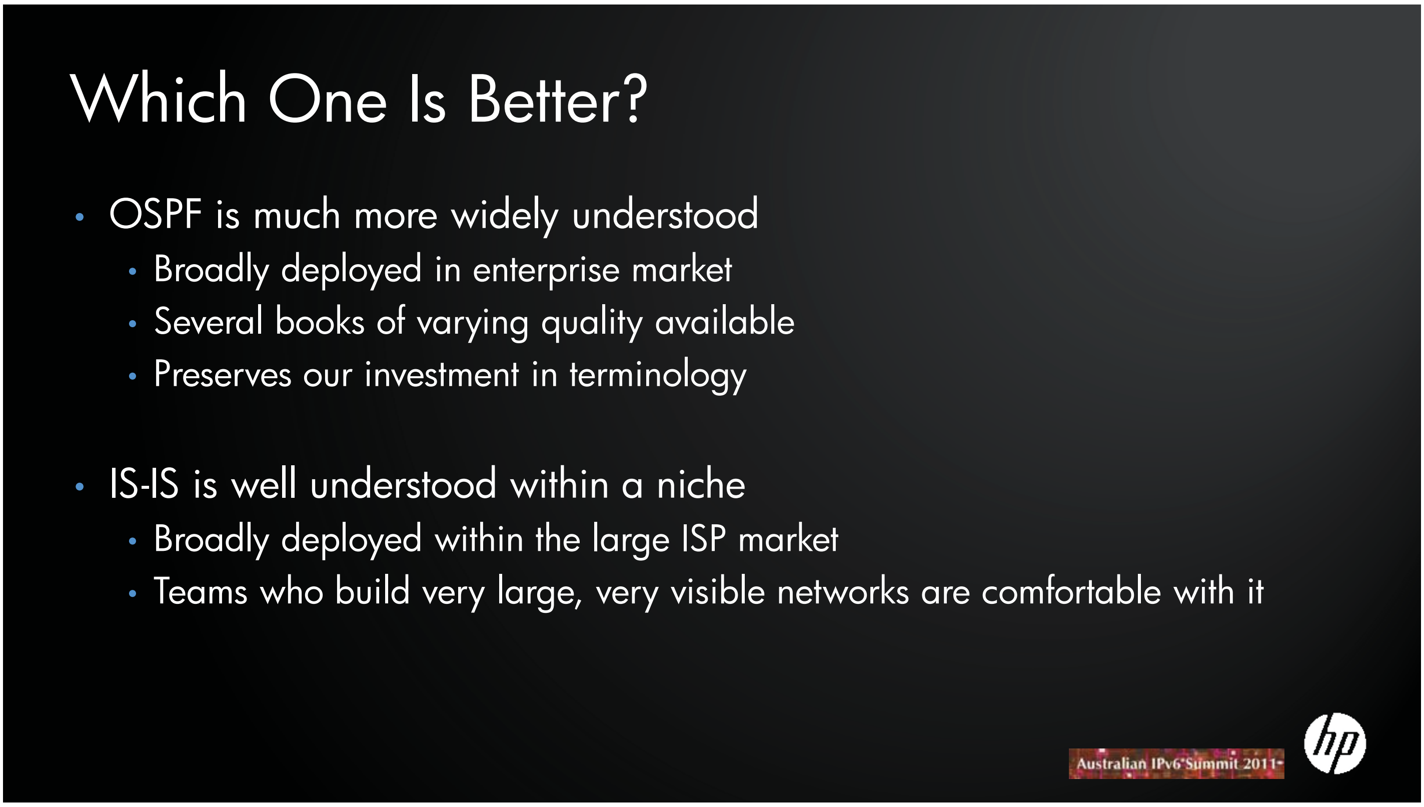
- Multi-Topology
  - Single ISIS domain with set of independent IP topologies
  - Common flooding and resource associated with both router and network
  - Multiple SPF
  - Large Database
- Multi-instance
  - Multiple instance of protocol on a given link
  - Enhances the ability to isolate the resources associated with both router and network
  - Instance specific prioritization for PDUs and routing calculations

Two Methods (cont.)

- OSPF currently is based on multi-instance
  - Adding multi topology is very easy for OSPFv3
  - Multiple address family support is in place, minor extension for multi-topology needs to be added
- ISIS
  - Multi-topology support has been there for a while
  - Multi-instance draft is there for ISIS now
- Which one is better
  - Depends who you talk to
    - Operation (Multi-instance is better)
    - Development (Multi-Topology is better)

COMPARISON

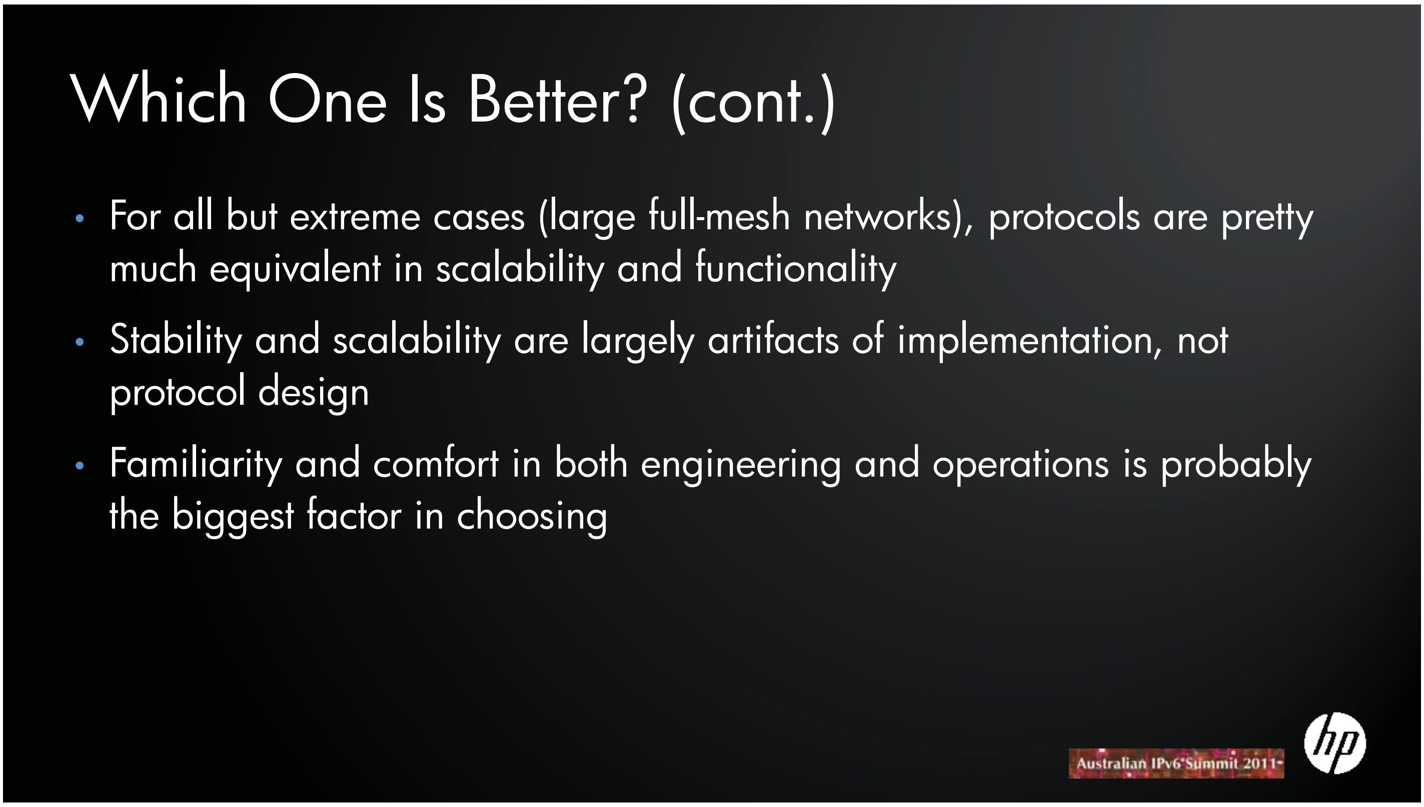




Which One Is Better?

- OSPF is much more widely understood
  - Broadly deployed in enterprise market
  - Several books of varying quality available
  - Preserves our investment in terminology
- IS-IS is well understood within a niche
  - Broadly deployed within the large ISP market
  - Teams who build very large, very visible networks are comfortable with it

Australian IPv6 Summit 2011

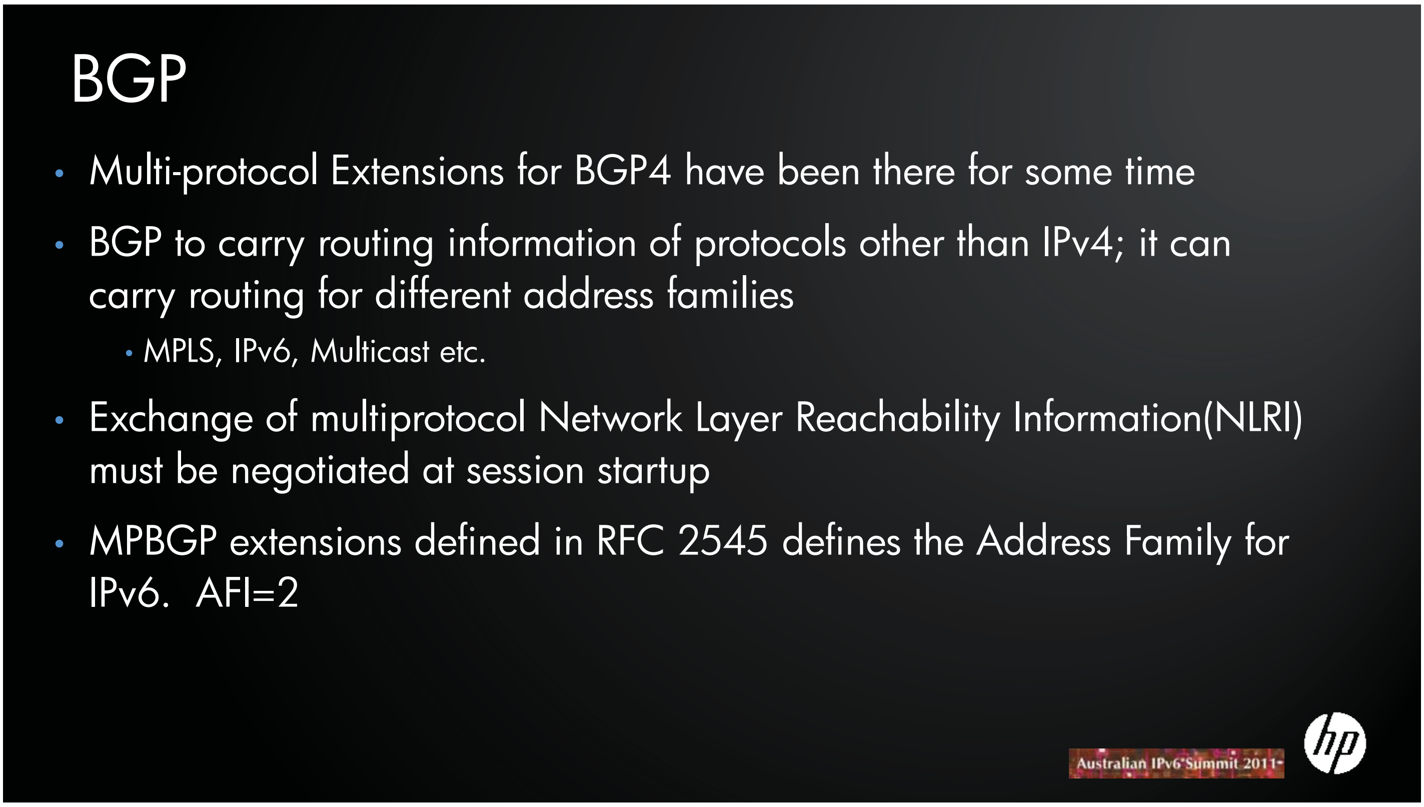


Which One Is Better? (cont.)

- For all but extreme cases (large full-mesh networks), protocols are pretty much equivalent in scalability and functionality
- Stability and scalability are largely artifacts of implementation, not protocol design
- Familiarity and comfort in both engineering and operations is probably the biggest factor in choosing

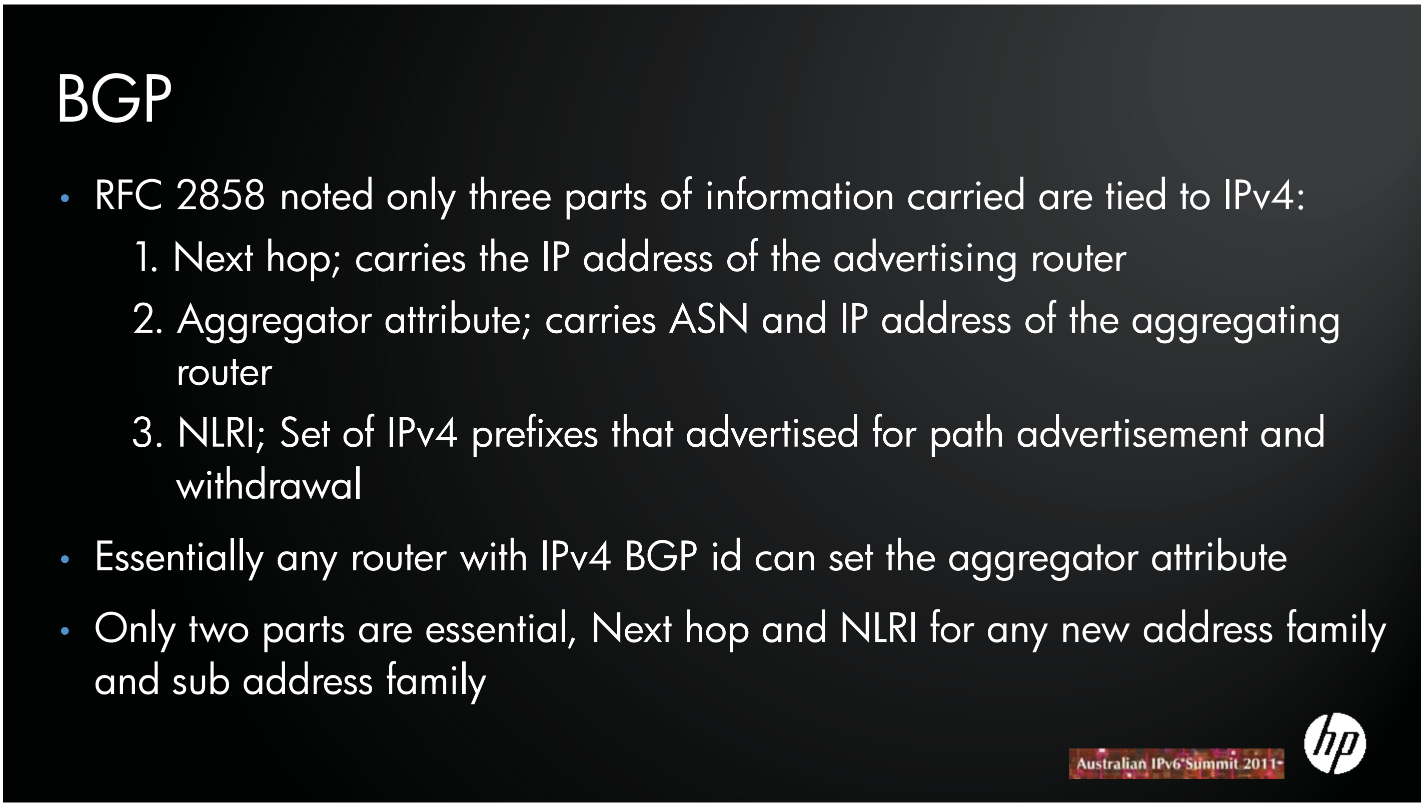
Australian IPv6 Summit 2011

BGP



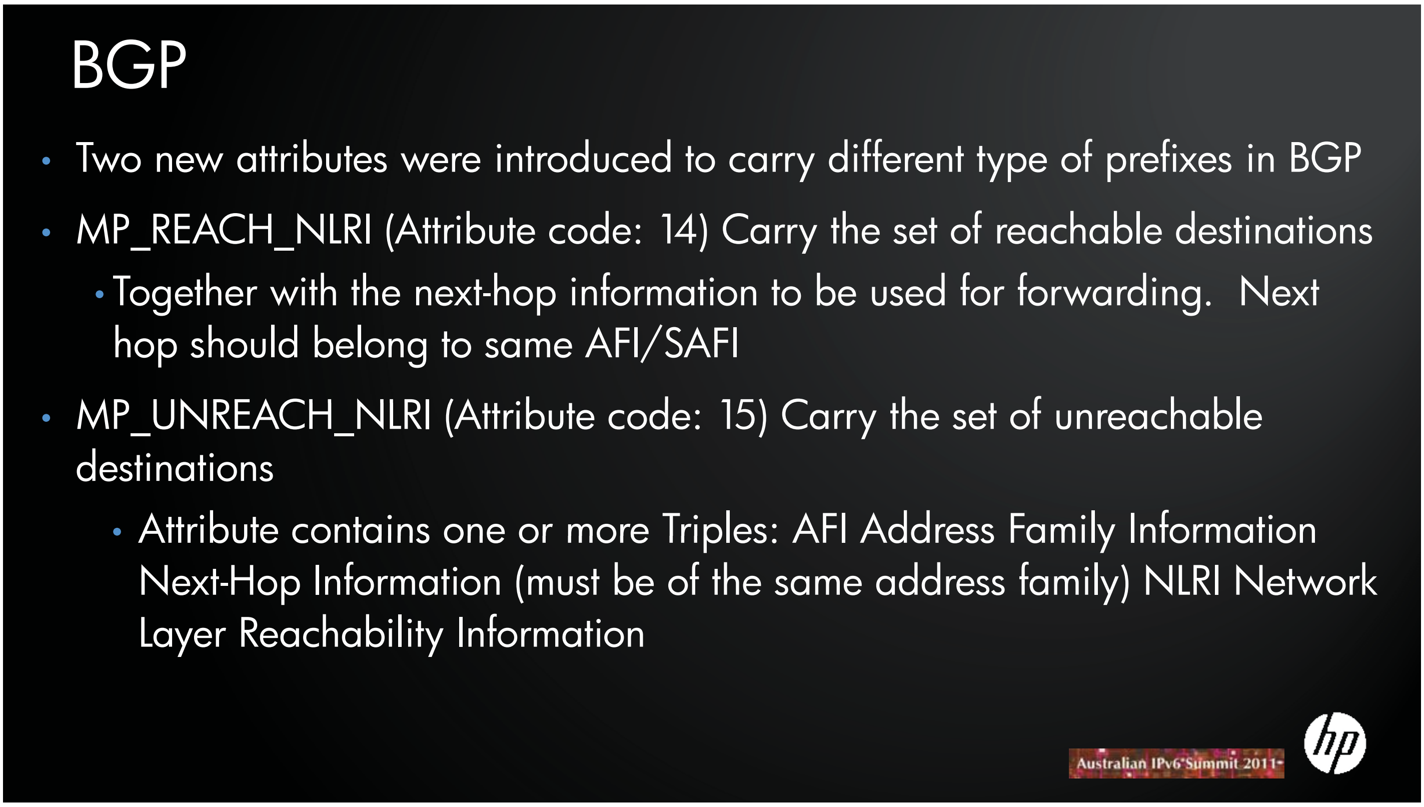
BGP

- Multi-protocol Extensions for BGP4 have been there for some time
- BGP to carry routing information of protocols other than IPv4; it can carry routing for different address families
  - MPLS, IPv6, Multicast etc.
- Exchange of multiprotocol Network Layer Reachability Information(NLRI) must be negotiated at session startup
- MPBGP extensions defined in RFC 2545 defines the Address Family for IPv6. AFI=2



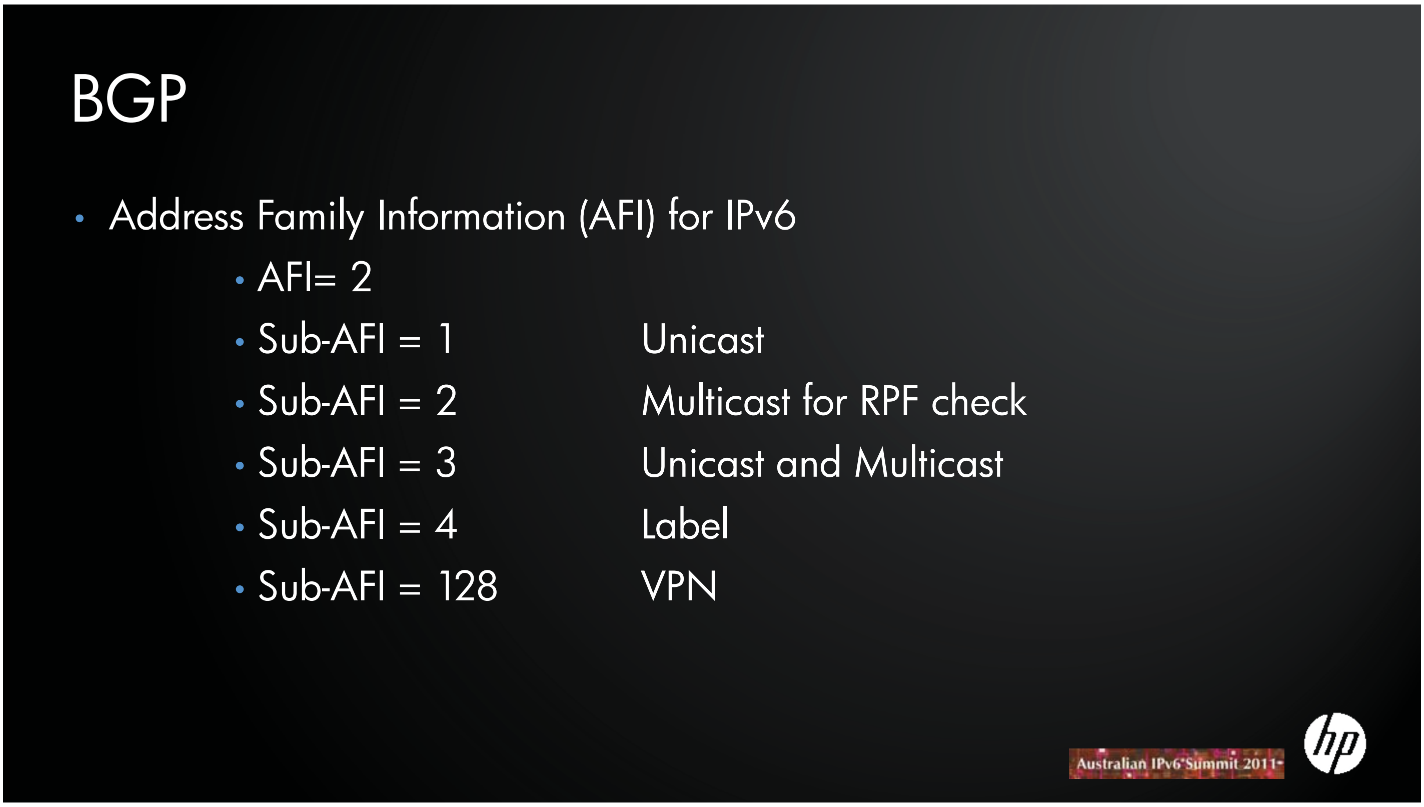
BGP

- RFC 2858 noted only three parts of information carried are tied to IPv4:
  1. Next hop; carries the IP address of the advertising router
  2. Aggregator attribute; carries ASN and IP address of the aggregating router
  3. NLRI; Set of IPv4 prefixes that advertised for path advertisement and withdrawal
- Essentially any router with IPv4 BGP id can set the aggregator attribute
- Only two parts are essential, Next hop and NLRI for any new address family and sub address family



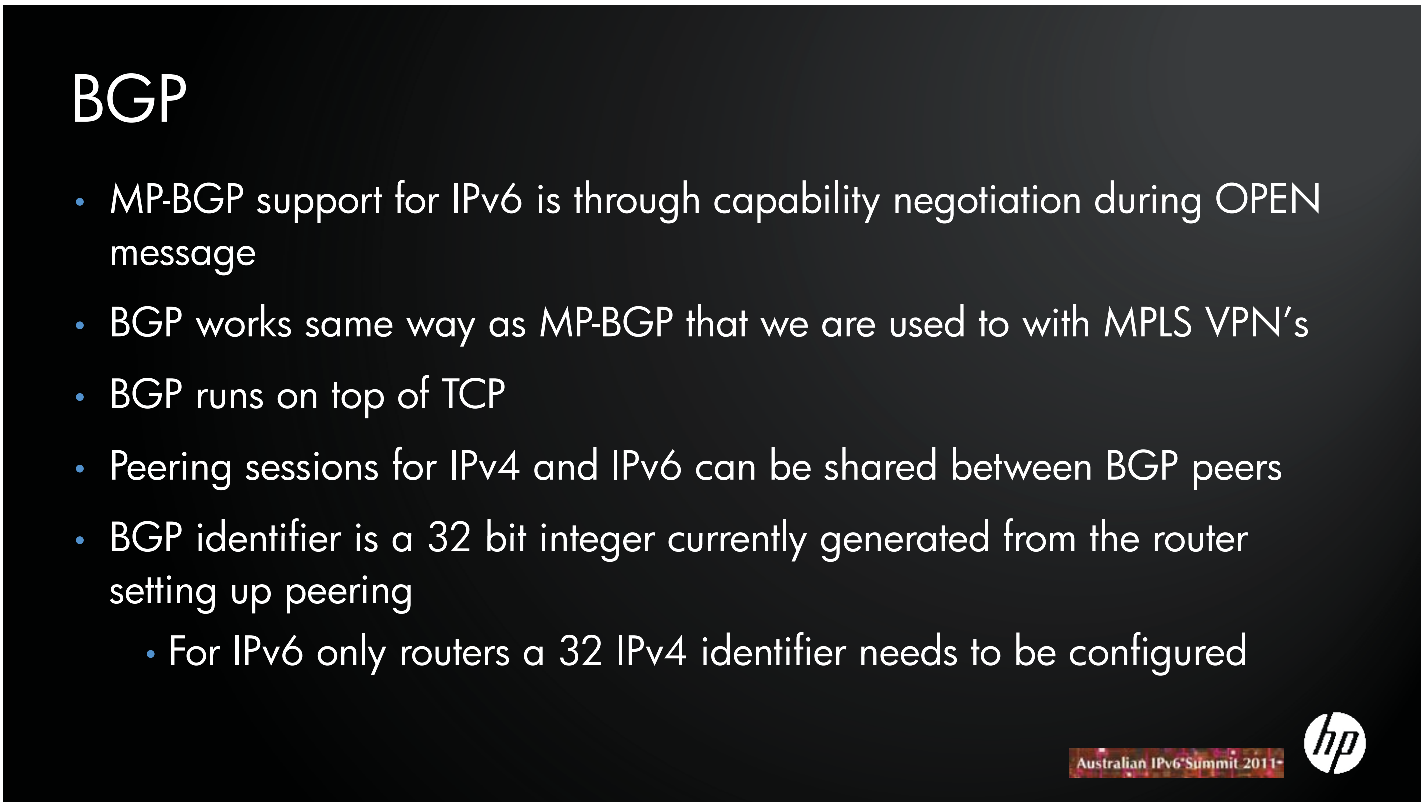
BGP

- Two new attributes were introduced to carry different type of prefixes in BGP
- MP_REACH_NLRI (Attribute code: 14) Carry the set of reachable destinations
  - Together with the next-hop information to be used for forwarding. Next hop should belong to same AFI/SAFI
- MP_UNREACH_NLRI (Attribute code: 15) Carry the set of unreachable destinations
  - Attribute contains one or more Triples: AFI Address Family Information Next-Hop Information (must be of the same address family) NLRI Network Layer Reachability Information



BGP

- Address Family Information (AFI) for IPv6
  - AFI= 2
  - Sub-AFI = 1 Unicast
  - Sub-AFI = 2 Multicast for RPF check
  - Sub-AFI = 3 Unicast and Multicast
  - Sub-AFI = 4 Label
  - Sub-AFI = 128 VPN



BGP

- MP-BGP support for IPv6 is through capability negotiation during OPEN message
- BGP works same way as MP-BGP that we are used to with MPLS VPN's
- BGP runs on top of TCP
- Peering sessions for IPv4 and IPv6 can be shared between BGP peers
- BGP identifier is a 32 bit integer currently generated from the router setting up peering
  - For IPv6 only routers a 32 IPv4 identifier needs to be configured

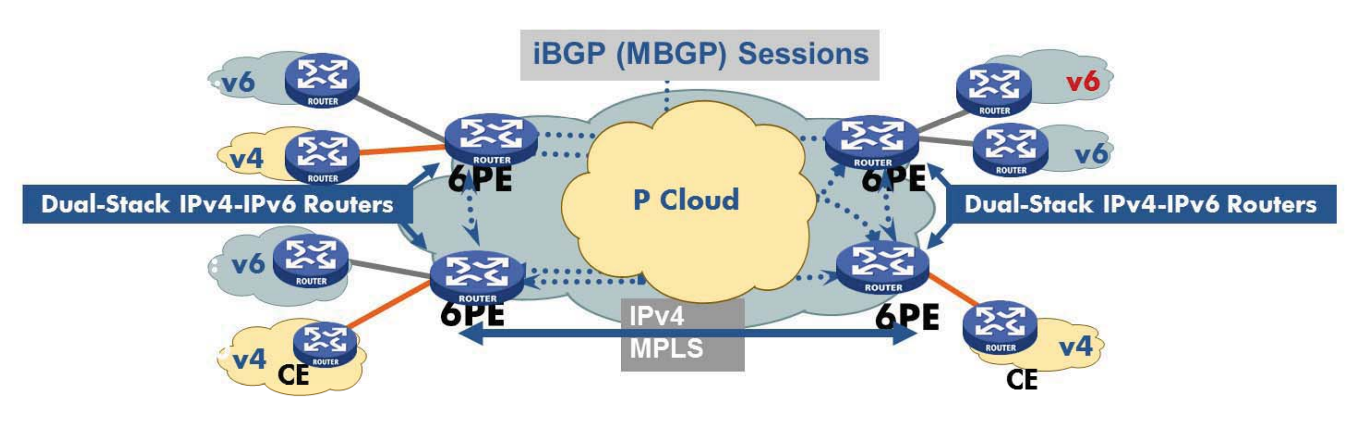
MPLS Network

- Two options are available:
  1. 6PE
  2. 6VPE

Provider Edge Router MPLS 6PE

- Non VPN routing service
- Routes are installed global table
- Used for providing IPv6 service for internet connectivity
- Scaling will become a huge issue since the only place summarization can be done is at the PE (no other router can aggregate due to FEC change)
- Simple solutions for enterprise to turn on IPv6 in their network if they are already running MPLS
- Do not run OSPF as CE-PE protocol, OSPFv3 currently does not have loop avoidance plus route comes in the global table

Provider Edge Router (6PE) over MPLS

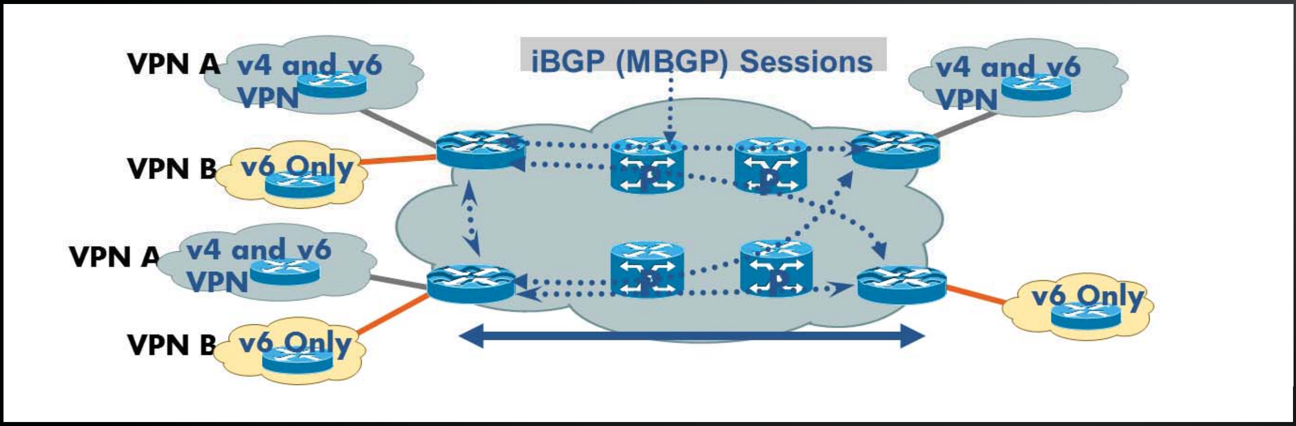


- IPv4 or MPLS core infrastructure is IPv6-unaware
- PEs are updated to support dual stack/6PE
- IPv6 reachability exchanged among 6PEs via iBGP (MBGP)
- IPv6 packets transported from 6PE to 6PE inside MPLS

VPN Provider Edge (6VPE)?

- Makes more sense as a long term solution
- Routing is within VPN context
- Summarization is based on VPN addressing
- IPv6 VPN service is exactly the same as IPv4 VPN service
- Current 6PE is a short term solution due to global reachability
- You can enable IPv6 segmentation in your network with:
  - No modification on the MPLS core
  - Support both IPv4 and IPv6 VPNs concurrently on the same interfaces
  - Configuration and operations of IPv6 VPNs are exactly like IPv4 VPNs

6VPE Deployment



- IPv6 VPN can coexist with IPv4 VPN—same coverage
- 6VPE is added only when and where the service is required
- 6VPE—an implementation over MPLS/IPv4

BGP design considerations (RR)

- Off path route reflector are better for MPLS VPN environment
- No route aggregation any where in the network except at the edge (FEC is defined at the edge only)
- Due to a large number of existing VPN IPv4 customers providers have built multi-planer route reflection designs
- Introducing 6VPE will add more burden on existing IPv4-VPN RRs
- Better to build different IPv6 RRs that are off path - this will protect existing VPN-v4 service

Conclusion

- Remember IPv6 is still IP
- Design considerations for both carrier and enterprise do not change
- Routing protocol design fundamentals still remain the same
- Scaling would require more planning but basics do not change
- If you know your routing protocols, operating them for IPv6 will require little but of learning

Australian IPv6 Summit 2011

THANK YOU

Australian IPv6 Summit