Cisco Live!
January 29 - February 2, 2018 · Barcelona
Enterprise IPv6 Deployment

Tim Martin
CCIE #2020
@bckcntryskr
Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

cs.co/ciscolivebot#BRKIP6-2301
Agenda

- General Design
- Host Configuration
- Access Layer
- Data Center
- WAN Deployment
- Internet Edge
- Conclusion
Enterprise IPv6 Guidance

- RFC 7381 enterprise IPv6 guidelines
- White paper – Cisco.com
- Cisco Press Live Lesson

IPv6 for the Enterprise in 2015

Over 83 percent of the world’s population no longer has access to the legacy variant of the commodity we have become familiar with as “public Internet address.” Put another way, in North America, Latin America, Asia, and Europe, the IPv4 address pool is already entirely depleted.
Where Do We Start?

• Core-to-Access – Gain experience with IPv6
• Turn up your servers – Enable the experience
• Access-to-Core – Securing and monitoring
• Internet Edge – Business continuity
Dual Stack Mode

• Preferred Method, Versatile, Scalable and Highest Performance
• No Dependency on IPv4, runs in parallel on the same HW
• No tunnelling, MTU, NAT or performance degrading technologies
• Does require IPv6 support on all devices
What about IPv6 only?

- Is everything ready?
  - Network services
  - Applications
  - Operations and Management
- Connectivity to non-IPv6 resources
  - NAT64/DNS64

- RFCs are out there
  - RFC 6586 - Experiences from an IPv6-Only Network
  - RFC 7755 - SIIT-DC: Stateless IP/ICMP Translation for IPv6 Data Center Environments
  - RFC 7756 - Explicit Address Mappings for Stateless IP/ICMP Translation
Global Address Assignment

- Provider Allocated (PA)
  - From your ISP, single homed
  - /48 - /60

- Provider Independent (PI)
  - Multi home, Multi provider
  - /32 - /48

- Local Internet Registry (LIR)
  - Regional registry member
  - Acquire & manage space
  - /29 - /32
Multinational Model

- PA or PI from each region you operate in
- Coordination of advertised space within each RIR
- Most run PI from primary region as an LIR
Prefix Length Considerations

- **Point to Point /127**
  - RFC 6164, cache exhaustion
  - Reserve a /64, configure a /127

- **Loopback or Anycast /128**

- **Anywhere a host exists /64**
  - RFC 7421, rational for /64
Explaining BIG Numbers With Math

- The LAN size standard has been set at a /64
  - 18,446,744,073,709,600,000 IPv6 addresses

- Let’s attempt to exhaust all of the available addresses
  - We will allocate 10,000,000 addresses per second
  - Hint: there are 31,536,000 seconds per year
  - 10,000,000 x 31,536,000 = 315,360,000,000,000

\[
\frac{18,446,744,073,709,600,000}{315,360,000,000,000} = 58,494 \text{ years}
\]

Attribution: Ed Horley
Building the IPv6 Address Plan

• Location-based Plan (/48)
  • 4 bits = (16) Locations (states, counties, agencies, etc.)
  • 4 bits = (16) Buildings or sub levels within a location
  • 4 bits = (16) Floors or directional pointers
  • 4 bits = (16) Traffic Types (Admin, Guest, Telephony, etc.)

2001:db8:4646:xxxxx::

0001 1000 0011 0110

2001:db8:4646:1836::
Building the IPv6 Address Plan

• Function-based Plan (/48)
  • 4 bits = (16) Traffic Types (Admin, Guest, Telephony, etc.)
  • 4 bits = (16) Locations (states, counties, agencies, etc.)
  • 4 bits = (16) Buildings or sub levels within a location
  • 4 bits = (16) Floors or directional pointers

2001:db8:4646:xxxx::

0110 0001 1000 0011

2001:db8:4646:6183::
Unique Local Address (ULA)

- Automatic Prefix Generation (RFC 4193) non sequential /48
- Some may find it attractive (home net, Sec Ops)
- Multiple policies to maintain (ACL, QoS, Routing)
- Caution - source address selection using ULA & IPv4

Corporate Backbone

ULA - fd9c:58ed:7d73::/48
Global – 2001:db8:cafe::/48

fc00::/7
fc00::/8 – reserved
fd00::/8 - private
Infrastructure Link Local Addressing

- Topology hiding, Interfaces cannot be seen by off link devices
- Reduces routing table prefix count, less configuration
- Need to use GUA for generating ICMPv6 messages
- What about DNS?, Traceroute, WAN Connections, etc..
- RFC 7404 – Details pros and cons
Agenda

- General Design
- Host Configuration
- Access Layer
- Data Center
- WAN Deployment
- Internet Edge
- Conclusion
IPv6 Host Portion Address Assignment

<table>
<thead>
<tr>
<th>Similar to IPv4</th>
<th>New in IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manually configured</td>
<td>Stateless Address Auto Configuration</td>
</tr>
<tr>
<td>Assigned via DHCPv6</td>
<td>SLAAC EUI64</td>
</tr>
<tr>
<td></td>
<td>SLAAC Privacy Addressing</td>
</tr>
</tbody>
</table>

* Secure Neighbor Discovery (SeND)
Router Advertisement Provisioning

- **M-Flag** – Stateful DHCPv6 to acquire IPv6 address
- **O-Flag** – Stateless DHCPv6 in addition to SLAAC
- **Preference Bits** – low, med, high
- **Router Lifetime** – Must be >0 for default
- **Options** - Prefix Information, Length, Flags
- **L bit** – Host installs the prefix as on link
- **A bit** – Instructs hosts to auto configure an address

Class: 134 (RA)  
Code: 0
Checksum: 0xff78 [correct]
Cur hop limit: 64
∞ Flags: 0x84  
1… …. = Managed (M flag)
.0.. …. = Not other (O flag)
..0. …. = Not Home (H flag)
…0 1… = Router pref: High

Router lifetime: (s) **1800**  
Reachable time: (ms) 3000000  
Retrans timer: (ms) 1000  
ICMPv6 Option 3 (Prefix Info)  
Prefix length: 64
∞ Flags: 0x84  
1… …. = On link (L Bit)
.... 1… = Autonomous (A Bit)
Prefix: 2001:db8:4646:234::/64
Host Address Acquisition

C:\Documents and Settings\>netsh
netsh>interface ipv6
netsh interface ipv6>show address
Querying active state...
Interface 5: Local Area Connection

<table>
<thead>
<tr>
<th>Addr Type</th>
<th>DAD State</th>
<th>Valid Life</th>
<th>Pref. Life</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Preferred</td>
<td>29d23h58m25s</td>
<td>6d23h58m25s</td>
<td>2001:db8:4646:1:4f02:8a49:41ad:a136</td>
</tr>
<tr>
<td>Temporary</td>
<td>Preferred</td>
<td>6d21h48m47s</td>
<td>21h46m</td>
<td>2001:db8:4646:1:bd86:eac2:f5f1:39c1</td>
</tr>
<tr>
<td>Link</td>
<td>Preferred</td>
<td>infinite</td>
<td>infinite</td>
<td>fe80::4f02:8a49:41ad:a136</td>
</tr>
</tbody>
</table>

netsh interface ipv6>show route
Querying active state...

<table>
<thead>
<tr>
<th>Publish</th>
<th>Type</th>
<th>Met</th>
<th>Prefix</th>
<th>Idx</th>
<th>Gateway/Interface Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Autoconf</td>
<td>8</td>
<td>2001:db8:4646:1::/64</td>
<td>5</td>
<td>Local Area Connection</td>
</tr>
<tr>
<td>no</td>
<td>Autoconf</td>
<td>256</td>
<td>::/0</td>
<td>5</td>
<td>fe80::20d:bdff:fe87:f6f9</td>
</tr>
</tbody>
</table>
Client Provisioning DHCPv6 & SLAAC

- SLAAC address tracking
  - Radius accounting, CAM table scrapes
  - Older OS’s (MSFT) lack support RDNSS

- DHCPv6 challenges
  - MAC address for reservations, inventory, tracking
  - Android doesn't support DHCPv6

- Understand the implications of switching methods
  - Inconsistent amongst the OS’s

DHCPv6 Server

Internet

Username=joe@example.org Acct-Session-Id=xyz
Acct-Status-Type=Start Framed-IP-Address=192.0.2.1
Framed-IPv6-Address=fe80::d00d

Username=joe@example.org Acct-Session-Id=xyz
Acct-Status-Type=Alive Framed-IP-Address=192.0.2.1
Framed-IPv6-Address=fe80::d00d Framed-IPv6-Address=2001:db8::d00d Framed-IPv6-Address=2001:db8::d00d

A B C

RA
Disabling SLAAC/Privacy Addresses

- Enable DHCPv6 via the M flag
- Disable prefix auto configuration
- Enable router preference to high
- Enable DHCPv6 relay destination

```
interface fastEthernet 0/0
  ipv6 address 2001:db8:4646:acc1::1/64
  ipv6 nd managed-config-flag
  ipv6 nd prefix default no-autoconfig
  ipv6 nd router-preference high
  ipv6 dhcp relay destination 2001:db8:4646::café
```
Agenda

- General Design
- Host Configuration
- Access Layer
- Data Center
- WAN Deployment
- Internet Edge
- Conclusion
IPv6 First Hop Redundancy Protocols

• FHRPs provide resilient default gateway
  • First hop address to end-stations

• IPv6 has a “built in” FHRP mechanism
  • Neighbor Unreachable Detection (NUD)

• HSRP, GLBP, and VRRP alternatives
  • Millisecond timers for fast convergence

• Preempt timers need to be tuned
  • To avoid black-holed traffic
IPv6 FHS

RA Guard
Protection:
- Rogue or malicious RA
- MiM attacks

DHCPv6 Guard
Protection:
- Invalid DHCP Offers
- DoS attacks
- MiM attacks

Source/Prefix Guard
Protection:
- Invalid source address
- Invalid prefix
- Source address spoofing

Destination Guard
Protection:
- DoS attacks
- Scanning
- Invalid destination address

RA Throttle
Facilitates:
- Scale converting multicast traffic to unicast

ND Multicast Suppress
Reduces:
- Control traffic necessary for proper link operations to improve performance

Core Features
Advance Features
Scalability & Performance
IPv6 Snooping
IPv6 Wi-Fi & RA Throttler

- Scaling the 802.11 multicast reliability issues
- Controller response (proxy) to RS with unicast RA
- Controller rate limits the period RAs, while allowing RS to flow
- Proxy services reduce the amount of processing on end devices
IPv6 Wi-Fi & ND Multicast Suppression

• Uses a binding table similar to RFC 6620

• Binding table keeps track of “associated” MAC addresses
  • Purges MAC addresses from device when they “disassociate”

• Caching allows the Controller to “proxy” the NA, based on gleaning

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IPv6 Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:24:56:75:44:33</td>
<td>2001:db8:0:20::2</td>
</tr>
<tr>
<td>00:24:56:11:93:28</td>
<td>2001:db8:0:20::4</td>
</tr>
</tbody>
</table>
Cisco is Rewriting the Network Playbook

Traditional Network

Hardware Centric
Manual
Fragmented Security
Network Data

The New Network

Software Driven
Automated
Built-In Security
Business Insights

Powered by Cisco DNA-Center
Software Defined Access (SDA)

- Host Mobility without stretching VLANs
- Layer 3 VPN Segmentation without implementing MPLS
- Policy based Access Control with ‘End-to-End’ TrustSec
- Real time network monitoring, analytics and user/device assurance
IPv6 Support in Software Defined Access (SDA)

Edge Node Routing Table
- 2001:db8:46:1::/64 – Local
- 2001:db8:46:1::ac/128 – Local

Map Register
Endpoint 2001:db8:46:1::ac
Edge Node: 10.0.255.1

Control-Plane Node Database
- 2001:db8:46:1::/64 – 10.0.255.1
- 2001:db8:46:3::/64 – 10.0.255.3
- 2001:db8:46:1::ac – 10.0.255.1
- 2001:db8:46:1::ac – 10.0.255.3

Anycast Gateway
fe80::1

10.0.255.1

10.0.255.3
Agenda

• General Design
• Host Configuration
• Access Layer
• **Routing Protocols**
• Data Center
• WAN Deployment
• Internet Edge
• Conclusion
Static Routing

- IGPs use Link Local Addresses
- Redistribution needs GUA or ULA
- Direct (interface)
- Recursive (next hop)
- Fully qualified (interface) (next hop)
- Default route ::/0

```
ipv6 unicast-routing
!direct
ipv6 route 2001:db8:1::/48 ethernet1/0
!recursive
ipv6 route 2001:db8:5::/48 2001:db8:4::1
!fully qualified
ipv6 route 2001:46::/32 ethernet0/0 fe80::9
!default
ipv6 route ::/0 ethernet0/2 fe80:2
```
Classic EIGRP or EIGRPv6

- **EIGRP** – IP 88
  - fe80::/64 Source → ff02::a Destination
- No shutdown for older versions
- Apply the route process to interfaces
- Auto Summary disabled
- Transport & peering over IPv6

```plaintext
ipv6 unicast-routing
!
Interface ethernet 0/0
ipv6 address 2001:db8:1000::1/128
ipv6 eigrp 11
!
interface ethernet 0/1
ipv6 address 2001:db8:50:31::1/64
ipv6 eigrp 11
!
ipv6 router eigrp 11
no shutdown
eigrp router-id 4.4.4.4
```
EIGRP Named Mode

- Name creates a virtual instance
  - Does not need to be common in domain

- Address family configures protocol instance
  - AS number must common within domain

- Auto Applied to all IPv6 enabled interfaces

- EIGRP can perform better
  - Large-scale hub and spoke environments

```
router eigrp IPv6rocks !
address-family ipv6 unicast autonomous-system 11 !
af-interface Loopback0 passive-interface exit-af-interface !
af-interface Ethernet0/0 summary-address ::/0 exit-af-topology eigrp router-id 4.6.4.6 exit-address-family
```
OSPFv3

• OSPFv3 – IP 89
  • fe80::/64 Source → ff02::5, ff02::6 (DR’s)
  • Link-LSA (8) – Local Scope, NH
  • Intra-Area-Prefix-LSA (9) – Routers’ Prefixes
  • Use Inter-Area-Prefix-LSA (3) – Between ABRs

• Can converge quickly to a point of scale
  • Initial database build takes time

• LSPs generally perform better in full mesh

ipv6 unicast-routing

interface loopback0
ipv6 address 2001:db8:1000::1/128
ipv6 ospf 8 area 0

interface ethernet 0/0
ipv6 address 2001:db8:50:31::1/64
ipv6 ospf 8 area 0

ipv6 router ospf 8
router-id 8.8.8.8
passive-interface loopback0
Agenda

• General Design
• Host Configuration
• Access Layer
• Routing Protocols
• Data Center
• WAN Deployment
• Internet Edge
• Conclusion
IPv6 Only Data Center

- Dual stack front end
- Translation via NAT/Proxy/SLB
- Forces developers to use IPv6
- Reduces operational costs
- Eliminates complexity within the DC
Stateless IP/ICMP Translation

- RFC 7757
  - IPv6-only Internet Data Center (IDC)
  - Primarily RFC 6144, scenario’s 2, 4, 6
- IPv4 to IPv6 header
  - Operator configured mapping between IPv4 & IPv6
  - Fragmentation converts to EH 44
  - No other options in extension headers
- ICMP to ICMPv6 header
  - Pseudo Checksum for IPv6
  - Type Translated (IPv4 8, 0 to IPv6 128, 129)
  - Fragmented ICMP packets not translated
Static Server Addressing

- Predictable & deterministic
  - Address, default gateway, DNS

- Requires disabling key IPv6 components
  - RA’s, DHCPv6

- Should still configure FHS

- Readdressing will take time

- Operationally intensive
Dynamic Server Addressing

• Aligns well with SDN
• DHCPv6
  • Converting lease to reservation
  • Reservation mechanisms (RFC6939)
  • Dynamic DNS update for critical services
• Prefix Delegation
  • A /64 per host
  • Application or content addressing
Agenda

• General Design
• Host Configuration
• Access Layer
• Routing Protocols
• Data Center
• WAN Deployment
• Internet Edge
• Conclusion
Point-to-Point Routed Links

- Use a prefix length of /127
  - Reserve the /64, configure the /127
  - Nodes 1 & 2 are NOT in the same subnet
- Suppress RAs for global assigned addressing
- Disable ICMPv6 redirects
- Don’t send ICMPv6 unreachable

```
interface FastEthernet0/1
ipv6 address 2001:db8:46:67::a/127
ipv6 nd ra suppress
no ipv6 redirects
no ipv6 unreachables
```
IPv6 & MPLS

- 6PE (RFC 4798)
  - MP-BGP next hop ::ffff:A.B.C.D/96
- 6VPE (RFC 4659)
  - Utilizes address family (AF) in VRF context
AnyConnect & IPv6

- A dual-stacked host can connect via IPv4 or IPv6
- Tries IPv6 address first, then IPv4 address
- No DHCPv6 or SLAAC, uses pool from ASA
  - Also defined on client side

```
ipv6 local pool pool6 2001:db8:46:37::/64
```
Agenda

- General Design
- Host Configuration
- Access Layer
- Routing Protocols
- Data Center
- WAN Deployment
- Internet Edge
- Conclusion
Internet Edge Design Characteristics

- How will your enterprise use the Internet?
  - Does the Enterprise host content?
  - Does the Enterprise access content?

- Ingress – How traffic will enter your domain
  - High availability, congestion
  - Balanced across multiple providers

- Egress – How traffic will leave your domain
  - High availability, congestion, cost
  - Firewall’s holding state
Multihomed, Multiprefix (BGP)

- **Peer over IPv6** for IPv6 prefixes
- **Use GUA for neighbor peering**
- **Controlling hop limit**, accepting ~254 only
- **MD5 shared secrets**, IPsec possible

```
router bgp 200
bgp router-id 4.6.4.6
no bgp default ipv4-unicast
neighbor 2001:db8:460:102::2 remote-as 2014
neighbor 2001:db8:460:102::2 ttl-security hops 1
neighbor 2001:db8:460:102::2 password cisco4646
```
Translation Techniques
IPv6 Translation Definitions

• Translation algorithms
  • RFC 6052 (implementation details)

• Framework for Translation
  • RFC 6144 (implementation scenarios)

• Stateless NAT64 (inbound)
  • RFC 6145 → 7915 (IP/ICMP translation algorithm)

• Stateful NAT64 (outbound)
  • RFC 6146 (state table for IPv4/IPv6 translation)
  • IPv6-only clients need to access IPv4 services

• DNS64
  • RFC 6147 (IPv6 client to IPv4 server)
DNS64 Operation

**Step 1** IPv6 client queries AAAA record for IPv4 server

**Step 2** DNS responds “empty” AAAA record

**Step 3** Translator asks for A record of IPv4 server

**Step 4** DNS server responds A record for IPv4 server

**Step 5** Translates it to a AAAA record
NAT64 Operation

Source IPv6 3001::c000:221 Dest. IPv6 2001:db8:122:344::6

Source IPv4 192.0.2.33 Dest. IPv4 192.0.2.1

Source IPv6 2001:db8:122:344::6 Dest. IPv6 3001::c000:221

Source IPv4 192.0.2.1 Dest. IPv4 192.0.2.33
SLB64 Translation Technique

• Almost every network has some load balancing
• Create Virtual IP (VIP)
  • Tie the VIP to R-servers (WWW)
  • Publish VIP AAAA record in DNS
• Establish a source NAT pool
  • Use as IPv4 source after translation
• Citrix NetScaler or F5 BIG-IP
• Very quick to deploy
  • Hard to move forward
  • Native IPv6 is the end goal
X-Forwarded-For (XFF)

- Web Server Logging for Geo Location, Analytics, Security
- Source IP of client requests will be logged as SNAT address
- Use XFF field of the HTTP header

```
GET / HTTP/1.1
Host: www.foo.org
User-Agent: Mozilla Firefox/3.0.3
Accept: text/html,application/xhtml+xml,application/xml
Accept-Language: en-us,en
Keep-Alive: 300
x-forward-for: 2001:db8:ea5e:1:49fa:b11a:aaf8:91a5
Connection: keep-alive
```
Network Prefix Translation IPv6

- RFC 6296 - NPTv6
  - Unique Local Addressing (ULA) inside
  - Provider allocated addressing outside

- Small-to-Medium Enterprise

- Swaps Left Most Bits of Address
  - Equal length Prefixes

interface GigabitEthernet0/0/0
nat66 inside
interface GigabitEthernet0/0/1
nat66 outside

! nat66 prefix inside fd07:18:4c::/48 outside 2001:db8:46::/48
Securing The Internet Edge
IPv6 ACL Implicit Rules

- IPv6 ACLs match IPv6, extension & Layer 4 headers
- IPv6 ACLs have multiple implicit rules
  - Similar to `deny ip any any`
- IOS has 3 implicit IPv6 ACL rules
- NXOS has 5 implicit IPv6 ACL rules
- IOS-XE has no implicit IPv6 ACL rules

```
ipv6 access-list IOS
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any

deny ipv6 any any log undetermined-transport
```

```
ipv6 access-list NXOS
permit icmp any any nd-na
permit icmp any any nd-ns
permit icmp any any router-advertisement
permit icmp any any router-solicitation
deny ipv6 any any
```
IPv6 Bogon Filtering & Anti-Spoofing

- Use perimeter router to reduce firewall log entries
- Anti-spoofing (RFC2827, BCP38)
- Multihomed filtering (RFC3704, BCP 84)
- uRPF – Unicast Reverse Path Forwarding
- Bogon filtering (data plane & BGP route-map)

```
ipv6 access-list BOGONS
permit ip 2001::/16 any
permit ip 2002::/16 any
permit ip 2003::/18 any
permit ip 2400::/12 any
permit ip 2600::/10 any
permit ip 2800::/12 any
permit ip 2a00::/12 any
permit ip 2c00::/12 any
```

```
ipv6 verify unicast reverse-path
```
Perimeter Firewall Best Practices

- Control address range of permit statements
  - Source of 2000::/3 at minimum vs. “any”
  - Watch for link local (fe80) to the firewall
- Allow ICMPv6 messages RFC4890
  - Error (types 1-4), ping (types 128-129)
  - NDP (type 135-136) to the firewall
- Extension Headers
  - Allow Fragmentation, others as needed
  - Block HBH & RH type 0
IPv6 Route to Black Hole

• BGP peers have static route to null0
  • Using IPv6 discard prefix (100::/64)
  • No unreachablees, prevents DOSing yourself

• BGP allows route announcement to/from

• NOC sees bad actor (2001:db8::bad1)

• NOC pushes route to network choke point

```
interface Null0
  no ipv6 unreachables
!
ipv6 route 100::/64 Null0

router bgp 65666
  !
  address-family IPv6
  redistribute static route-map RTBH
  !
  route-map RTBH permit 10
  match tag 66
  set ipv6 next-hop 100::1

ipv6 route 2001:db8::bad1/128 100::1 tag 66
```
Securing Email over IPv6

- Email relies on DNS PTR records to mitigate bad actors
  - DNSSEC preserves integrity of DNS records
- Sender Policy Framework (SPF)
  - Validates the IP address of the sender
- Domain Keys Identified Mail (DKIM)
  - Validates the domain name of the sender
- Receiving email servers use reputation (DNSBL)
  - Most reputation servers block IPv6 at /64
Agenda

• General Design
• Host Configuration
• Access Layer
• Routing Protocols
• Data Center
• WAN Deployment
• Internet Edge
• Conclusion
Key Take Away

• Gain **Operational Experience** now
• IPv6, the time is now.
• Control IPv6 traffic as you would IPv4
• “Poke” your Provider’s
• Lead your OT/LOB’s into the Internet
Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

cs.co/ciscolivebot#BRKIP6-2301
• Please complete your Online Session Evaluations after each session

• Complete 4 Session Evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt

• All surveys can be completed via the Cisco Live Mobile App or the Communication Stations

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at www.ciscolive.com/global/on-demand-library/.
Continue Your Education

• Demos in the Cisco campus
• Walk-in Self-Paced Labs
• Tech Circle
• Meet the Engineer 1:1 meetings
• Related sessions
Future IPv6 this week in Barcelona

- BRKIP6-2616 - Beyond Dual-Stack: Using IPv6 like you’ve never imagined – 30 Jan. 16:45
- BRKRST-3304 - Hitchhiker’s Guide to Troubleshooting IPv6 - Advanced – 31 Jan. 9:00
- BRKSPG-2602 - IPv4 Exhaustion: NAT and Transition to IPv6 for Service Providers – 31 Jan. 9:00
- BRKIP6-2301 - Enterprise IPv6 Deployment – 31 Jan. 11:30
- LABSPG-3122 - Advanced IPv6 Routing and services lab – 31 Jan 14:00 & 1 Feb. 14:00
- BRKCOL-2020 - IPv6 in Enterprise Unified Communications Networks – 31 Jan. 16:30
- BRKCOC-2388 - Inside Cisco IT: A Tale of Two Protocols – 2 Feb. 9:00
- BRKIP6-2002 - IPv6 for the World of IoT – 2 Feb. 11:30
Thank you