# IPv6 Best Practices

**co.example. SOA ns1 root 2012020300 1h 15m 30d 1h**

|  | NS | ns1.co.example. |
|---|---|---|
|  | NS | ns2.co.example. |
|  | A | 192.0.2.4 |
|  | AAAA | 2001:db8:ff00:1::4 |
|  | MX | 0 mail.co.example. |
|  | MX | 10 mail.isp.net. |
| ns1 | A | 192.0.2.2 |
|  | AAAA | 2001:db8:ff00:1::2 |
| ns2 | A | 192.168.2.2 |
|  | AAAA | 2001:db8:ff00:2::2 |
| mail | A | 192.0.2.3 |
|  | AAAA | 2001:db8:ff00:1::3 |
| www | A | 192.0.2.4 |
|  | AAAA | 2001:db8:ff00:1::4 |

**Internet**

2ff0:1500:ab::2/127
300a:12:ff00::2/127

**DMZ subnets:**
192.0.2/24 (IPv4)
2001:db8:ff00:1::/64 (IPv6)

mail   DNS   web
**DMZ**

**Firewall**

2001:db8:ff00::2/127

Site network: 2001:db8:ff01::/48
Infrastructure subnets: 2001:db8:ff01:0000::/56
Data subnets: 2001:db8:ff01:0100::/56
First data subnet: 2001:db8:ff01:0100::/64
Wireless subnets: 2001:db8:ff01:0200::/56
VoIP subnets: 2001:db8:ff01:0300::/56

**Site 1**

Site network: 2001:db8:ff02::/48
Infrastructure subnets: 2001:db8:ff02:0000::/56
Data subnets: 2001:db8:ff02:0100::/56
Wireless subnets: 2001:db8:ff02:0200::/56
VoIP subnets: 2001:db8:ff02:0300::/56

**Site 2**

Site network: 2001:db8:ff03::/48
Infrastructure subnets: 2001:db8:ff03:0000::/56
Data subnets: 2001:db8:ff03:0100::/56
Wireless subnets: 2001:db8:ff03:0200::/56
VoIP subnets: 2001:db8:ff03:0300::/56

**Site 3**

2001:db8:ff00::4/127
2001:db8:ff00::6/127

**1** Company decides to participate in World IPv6 Launch and begin deployment of IPv6

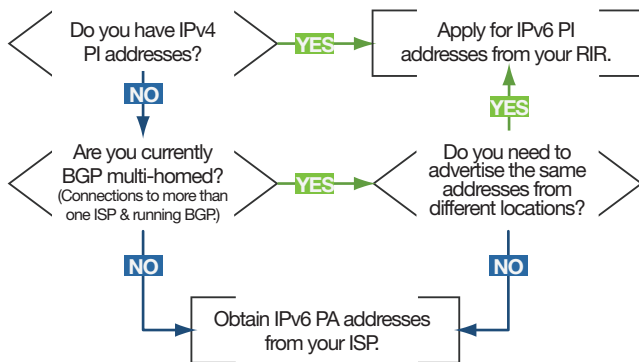**2** Company conducts a census of sites, counts three. Sites are interconnected using MPLS.

Company validates MPLS provider and internal routing protocol can support IPv6. (Only necessary if considering internal IPv6 deployment.)

**Scan QR code**
(video on IPv6 IGP selection.)

| if your internal routing protocol is… | Then for IPv6 use… |
|---|---|
| OSPF | OSPFv3 |
| EIGRP | EIGRP for IPv6 |
| RIP | Anything else |

**3** Company has two ISPs for redundancy, and has Provider Independent (PI) IPv4 address space, so opts for PI IPv6 address space

Do you have IPv4 PI addresses? — **YES** → Apply for IPv6 PI addresses from your RIR.

**NO**

Are you currently BGP multi-homed?
(Connections to more than one ISP & running BGP.) — **YES** → Do you need to advertise the same addresses from different locations? — **YES** ↑

**NO**          **NO**

Obtain IPv6 PA addresses from your ISP.

**4** Company approaches Regional Internet Registry (RIRs by region listed below) to get PI IPv6 address space.
RIR offers it a /48. Company makes case for a /44 based on planned expansion to eight sites, which the RIR approves. Company is assigned 2001:db8:ff00::/44.

ARIN: https://www.arin.net/resources/request/ipv6_initial_assign.html
RIPE:http://www.ripe.net/lir-services/resource-management/number-resources/ipv6
APNIC:http://www.apnic.net/services/apply-for-resources/kickstart-your-ipv6
LACNIC: http://lacnic.net/templates/eu-v6-template-en.txt
AFRINIC: http://www.afrinic.net/forms/affrm-v6fst200501.htm

**5** Company develops IPv6 subnetting plan.

Allocation from RIR: 2001:db8:ff00::/44

Infrastructure: 2001:db8:ff00::/48
/64 for point-to-point links: 2001:db8:ff00::/64
Border router -> Site 2 router: 2001:db8:ff00::2/127
Site 2 router -> Site 1 router: 2001:db8:ff00::4/127
Site 2 router -> Site 3 router: 2001:db8:ff00::6/127
DMZ hosts: 2001:db8:ff00:1::/64
/64 for loopback addresses: 2001:db8:ff00:2::/64

Site 1: 2001:db8:ff01::/48
Infrastructure: 2001:db8:ff01::/56
Wired data: 2001:db8:ff01:100::/56
Wireless data: 2001:db8:ff01:200::/56
VoIP: 2001:db8:ff01:300::/56

Site 2: 2001:db8:ff02::/48
Infrastructure: 2001:db8:ff02::/56
Wired data: 2001:db8:ff02:100::/56
Wireless data: 2001:db8:ff02:200::/56
VoIP: 2001:db8:ff02:300::/56

Site 3: 2001:db8:ff03::/48
Infrastructure: 2001:db8:ff03::/56
Wired data: 2001:db8:ff03:100::/56
Wireless data: 2001:db8:ff03:200::/56
VoIP: 2001:db8:ff03:300::/56

Future use:     2001:db8::ff04::/46
                2001:db8::ff08::/45

IPv6 subnets used for eBGP connections to ISPs:
ISP1: 2ff0:1500:ab::2/127
ISP2: 300a:12:ff00::2/127

ARIN   RIPE   APNIC   AFRINIC   LACNIC
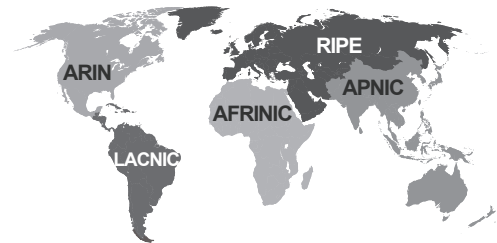
**6** Company approaches existing ISPs to "order IPv6." One ISP has IPv6 connectivity available, the other doesn't. Order successfully placed with one ISP (after customer provides required information represented by the following typical questions):

• Will you be configuring IPv6 on an existing IPv4 connection (dual-stack)?
• If not, what is the desired connection type and speed of the IPv6-only connection?
• Are you single-homed or multi-homed?
• If multi-homed, what is your AS number?
• Will you need an address allocation from the ISP?
• If not, what PI space will you be announcing?

**7** Company approaches alternate ISP to order IPv6. Order successfully placed. Major IP transit providers that support IPv6: Global Crossing, Hurricane Electric, Level3, NTT Communications, Tata, eliaSonera, Inteliquent (Tinet)

Additional IP transit providers that currently support IPv6 can be found here:
http://en.wikipedia.org/wiki/Comparison_of_IPv6_support_by_major_transit_providers

Make sure the ISP provides the necessary IPv6 routes.
You can research an ISP's IPv6 routes at these sites:

IPv6 CIDR REPORT
　　http://www.cidr-report.org/v6/as2.0/
BGPMon - IPv6 BGP Weathermap
　　http://bgpmon.net/weathermap.php?inet=6
Hurricane Electric's BGP Toolkit
　　http://bgp.he.net

**8** Company conducts audit of existing DMZ-based hardware and software to determine what supports IPv6, what must be upgraded, and what must be replaced. Determines OSes of DNS, web and mail servers and border router will support IPv6, while external firewall and IDS must be upgraded.

**9** Company upgrades/replaces DMZ-based hardware and software as needed.

**10** ISPs inform company that IPv6 connectivity is ready, give company/127s to configure on uplinks.
　　ISP1: 2ff0:1500:ab::2/127
　　ISP2: 300a:12:ff00::2/127

**11** Company configures external firewall to ensure neither native IPv6 nor tunneled IPv6 is passed.

| Source | Destination | Protocol | Action | Comment |
|---|---|---|---|---|
| Any | Any | IPv4 proto 41 | Deny | ISATAP, 6to4 |
| Any | 192.88.99.1 | IPv4 | Deny | 6to4 anycast relay |
| Any | Any | Port 3544 UDP | Deny | Teredo |

**12** Company secures border router against access (e.g., SSH, SNMP) via IPv6, configures border router to exchange routing information with ISPs' routers using BGP.

Partial IPv6 BGP configuration example:

```
router bgp 64511
    bgp router-id 1.1.1.1
    no bgp default ipv4-unicast
    [other global configuration parameters]
!
    neighbor 2ff0:1500:ab::2 remote-as 64496
    neighbor 2ff0:1500:ab::2 soft-reconfiguration inbound
    neighbor 2ff0:1500:ab::2 description eBGP with ISP
    neighbor 2ff0:1500:ab::2 password bgpwith64496
    neighbor 2ff0:1500:ab::2 maximum-prefix [1|5000]
    neighbor 2ff0:1500:ab::2 ttl-security hops 2
!
    neighbor 300a:12:ff00::2 remote-as 64499
    neighbor 300a:12:ff00::2 soft-reconfiguration inbound
    neighbor 300a:12:ff00::2 description eBGP with ISP64499
    neighbor 300a:12:ff00::2 password bgpwith64499
    neighbor 300a:12:ff00::2 maximum-prefix [1|5000]
    neighbor 300a:12:ff00::2 ttl-security hops 2
!
address-family ipv6 unicast
    network 2001:db8:ff00::/48
    neighbor 2ff0:1500:ab::2 activate
    neighbor 2ff0:1500:ab::2 remove-private-as
    neighbor 2ff0:1500:ab::2 prefix-list bogons in
    neighbor 2ff0:1500:ab::2 preflx-list announce out
    neighbor 300a:12:ff00::2 activate
    neighbor 300a:12:ff00::2 remove-private-as
    neighbor 300a:12:ff00::2 prefix-list bogons in
    neighbor 300a:12:ff00::2 prefix-list announce out
```

**13** Company configures external firewall to allow native IPv6 traffic to DNS server, mail server and web server.

| Source | Destination | Protocol | Action | Comment |
|---|---|---|---|---|
| Any port any | 2001:db8:ff00:1::2 port 53 | UDP | Allow | Inbound DNS queries (UDP) |
| 2001:db8:ff00:1::2 port 53 | Any port any | UDP | Allow | Outbound DNS queries (UDP) |
| Any port any | 2001:db8:ff00:1::2 port 53 | TCP + connect | Allow | Inbound DNS queries (TCP) |
| 2001:db8:ff00:1::2 port 53 | Any port any | TCP | Allow | Outbound DNS queries (TCP) |
| Any port any | 2001:db8:ff00:1::3 port 25 | TCP + connect | Allow | Inbound SMTP |
| 2001:db8:ff00:1::3 port 25 | Any port any | TCP | Allow | Inbound SMTP (TCP return) |
| 2001:db8:ff00:1::3p ort any | Any port 25 | TCP | Allow | Outbound SMTP |
| Any port 25 | 2001:db8:ff00:1::3 port any | TCP | Allow | Outbound SMTP (TCP return) |
| Any port any | 2001:db8:ff00:1::4 port 80 | TCP | Allow | Inbound HTTP |
| 2001:db8:ff00:1::4 port 80 | Any port any | TCP | Allow | Inbound HTTP (TCP return) |

You may also want to permit ICMPv6 error messages (type 1 through 4) to and from each server.

**14** Company configures IPv6 addresses on DMZ-based DNS, mail and web servers.

*Some recursive DNS and mail servers will automatically identify newly configured IPv6 addresses and require special options (e.g., BIND's -4 command-line option) to prevent them from trying to use IPv6 for outbound transactions (e.g., querying Internet name servers using IPv6) and causing unnecessary delays.

**15** Company configures DNS, mail and web servers to listen on IPv6 addresses. Company adds AAAA resource records pointing to the DNS, mail and web servers, but from domain names other than their production names, e.g., www.v6.company.example.
*Most DNS, mail and web servers require explicit configuration to listen on an IPv6 address. For example, BIND uses the listen-on-v6 substatement, Postfix uses the inet_protocols parameter in main.cf, and Apache uses the Listen directive.

**16** Company tests, tests, tests inbound and outbound DNS and SMTP, and inbound HTTP/S over IPv6.

Testing your host's IPv6 connectivty:
　　http://test-ipv6.com
　　http://ipv6-test.com
　　http://ipv6test.google.com

Looking glass site with excellent IPv6 visibility:
　　http://lg.he.net

**17** Company registers IPv6 addresses of external DNS servers through registrar.

**18** Before, on or after World IPv6 Launch, company begins advertising AAAA records for production domain names of DNS, mail and web servers.

**For more information go to www.infoblox.com/ipv6**