APNIC Training

SANOG

IPv6 Tunnel Transit Service Tutorial

28 January 2010 – Dhaka, Bangladesh

15 South Asian Network Operators Group (SANOG) Conference

In conjunction with ISPAB

Introduction

- Presenters
  - Nurul Islam Roman
    - Technical Training Officer
    - nurul@apnic.net
  - Jeffrey Tosco
    - Training Office
    - jeffrey@apnic.net

Overview

- **IPv6 Tunnel Transit Service Tutorial**
  - IPv4 to IPv6 Transition technologies
  - IPv6 Host Configuration
  - Case study- IXP Configuration
  - Case study- ISP Tunnel Transit Service

Overview

- IPv6 Tunnel Transit Service Tutorial
  - **IPv4 to IPv6 Transition technologies**
  - IPv6 Host Configuration
  - Case study- IXP Configuration
  - Case study- ISP Tunnel Transit Service

Acknowledgements

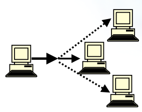
The material used in this course was created in collaboration with the Japan IPv6 Promotional Council, Jordi Palet Martinez of Consulintel, Merike Kaeo of Double Shot Security, Philip Smith of Cisco, Randy Bush (IIJ), Paul Wilson (APNIC), and Geoff Huston (APNIC) and includes material provided by them.

APNIC acknowledges with thanks and appreciation the contribution and support of the above.

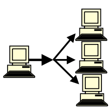
IPv6 addressing model

- **IPv6 Address type** RFC 4291
  - Unicast
    - An identifier for a single interface

  - Anycast
    - An identifier for a set of interfaces

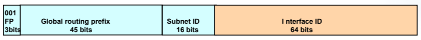


  - Multicast
    - An identifier for a group of nodes

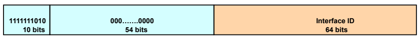


Unicast address

- Address given to interface for communication between host and router
  - Global unicast address currently delegated by IANA



  - Local use unicast address
    - Link-local address (starting with FE80::)



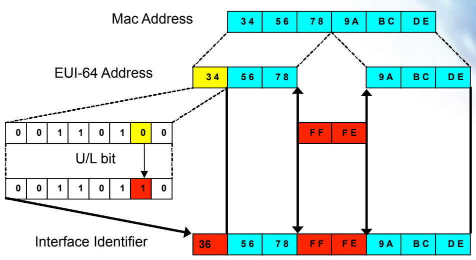
Special addresses

- The unspecified address
  - A value of 0:0:0:0:0:0:0:0 (::)
  - It is comparable to 0.0.0.0 in IPv4
- The loopback address
  - It is represented as 0:0:0:0:0:0:0:1 (::1)
  - Similar to 127.0.0.1 in IPv4

Interface ID

- The lowest-order 64-bit field addresses may be assigned in several different ways:
  - auto-configured from a 48-bit MAC address expanded into a 64-bit EUI-64
  - assigned via DHCP
  - manually configured
  - auto-generated pseudo-random number
  - possibly other methods in the future

EUI-64



Zone IDs for local-use addresses

- In Windows XP for example:
- Host A:
  - fe80::2abc:d0ff:fee9:4121%4
- Host B:
  - fe80::3123:e0ff:fe12:3001%3
- Ping from Host A to Host B
  - ping fe80::3123:e0ff:fe12:3001%4 (not %3)
    - identifies the interface zone ID on the host which is connected to that segment.

Transition overview

- How to get connectivity from an IPv6 host to the global IPv6 Internet?
  - Via a native connectivity
  - Via IPv6-in-IPv4 tunnelling techniques
- IPv6-only deployments are rare
- Practical reality
  - Sites deploying IPv6 will not transit to IPv6 -only, but transit to a state where they support both IPv4 and IPv6 (dual-stack)

http://www.6net.org/book/deployment-guide.pdf p59

IPv4 to IPv6 transition

- Implementation rather than transition
  - No fixed day to convert
- The key to successful IPv6 transition
  - Maintaining compatibility with IPv4 hosts and routers while deploying IPv6
    - Millions of IPv4 nodes already exist
    - Upgrading every IPv4 nodes to IPv6 is not feasible
      - No need to convert all at once
    - Transition process will be gradual

Transition overview

- Three basic ways of transition
  - Dual stack
  - Deploying IPv6 and then implementing IPv6 -in-IPv4 tunnelling
  - IPv6 only networking
- Different demands of hosts and networks to be connected to IPv6 networks will determine the best way of transition

Transition overview

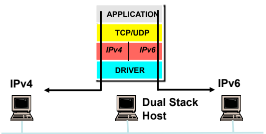
- Dual stack
  - Allow IPv4 and IPv6 to coexist in the same devices and networks
- Tunnelling
  - Allow the transport of IPv6 traffic over the existing IPv4 infrastructure
- Translation
  - Allow IPv6 only nodes to communicate with IPv4 only nodes

IPv6 essentials by Silvia Hagen, p255

Dual stack transition

RFC 4213

- Dual stack = TCP/IP protocol stack running both IPv4 and IPv6 protocol stacks simultaneously
  - Application can talk to both
- Useful at the early phase of transition



Dual stack

- A host or a router runs both IPv4 and IPv6 in the protocol TCP/IP stack.
- Each dual stack node is configured with both IPv4 and IPv6 addresses
- Therefore it can both send and receive datagrams belonging to both protocols
- The simplest and the most desirable way for IPv4 and IPv6 to coexist

http://www.6net.org/book/deployment-guide.pdf p60

Dual stack

- Challenges
  - Compatible software
    - Eg. If you use OSPFv2 for your IPv4 network you need to run OSPFv3 in addition to OPSFv2
  - Transparent availability of services
    - Deployment of servers and services
    - Content provision
    - Business processes
    - Traffic monitoring
    - End user deployment

Dual stack and DNS

- DNS is used with both protocol versions to resolve names and IP addresses
  - An dual stack node needs a DNS resolver that is capable of resolving both types of DNS address records
    - DSN A record to resolve IPv4 addresses
    - DNS AAAA record to resolve IPv6 addresses
- Dual stack network
  - Is an infrastructure in which both IPv4 and Ipv6 forwarding is enabled on routers

IPv6 essentials by Silvia Hagen, p256

APNIC Asia Pacific Network Information Centre

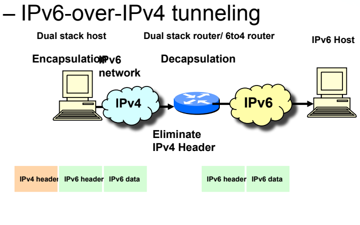
Tunnels

- Part of a network is IPv6 enabled
  - Tunnelling techniques are used on top of an existing IPv4 infrastructure and uses IPv4 to route the IPv6 packets between IPv6 networks by transporting these encapsulated in IPv4
  - Tunnelling is used by networks not yet capable of offering native IPv6 functionality
  - It is the main mechanism currently being deployed to create global IPv6 connectivity
- Manual, automatic tunnel configuration are available

APNIC Asia Pacific Network Information Centre

Tunneling – general concept

- Tunneling can be used by routers and hosts
  - IPv6-over-IPv4 tunneling



APNIC Asia Pacific Network Information Centre

Tunnelling – general concept

- A tunnel can be configured in four different ways:
  - Router to router
    - Spans one hop of the end-to-end path between two hosts. Probably the most common method
  - Host to router
    - Spans the first hop of the end-to-end path between two hosts. Found in the tunnel broker model
  - Host to host
    - Spans the entire end-to-end path between two hosts
  - Router to host
    - Spans the last hop of the end-to-end path between two hosts

Tunnel encapsulation

- The steps for the encapsulation of the IPv6 packet
  - The entry point of the tunnel decrements the IPv6 hop limit by one
  - Encapsulates the packet in an IPv4 header
  - Transmits the encapsulated packet through the tunnel
  - The exit point of tunnel receives the encapsulated packet
    - If necessary, the IPv4 packet is fragmented

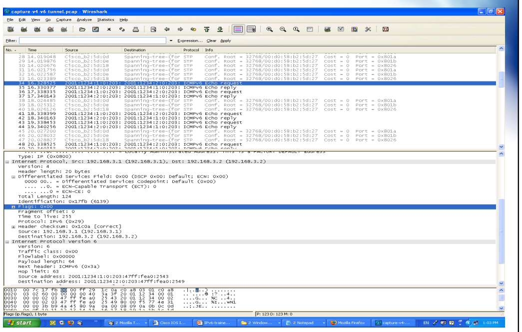
IPv6 essentials by Silvia Hagen, p258

Tunnel encapsulation (Cont)

- It checks whether the source of the packet (tunnel entry point) is an acceptable source (according to its configuration)
  - If the packet is fragmented, the exit point reassembles it
- The exit point removes the IPv4 header
- Then it forwards the IPv6 packet to its original destination

IPv6 essentials by Silvia Hagen, p258

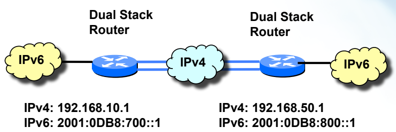
Encapsulated IPv6 packets in IPv4



Asia Pacific Network Information Centre
APNIC

Manual configuration

RFC 4213



Manually configured tunnels require:

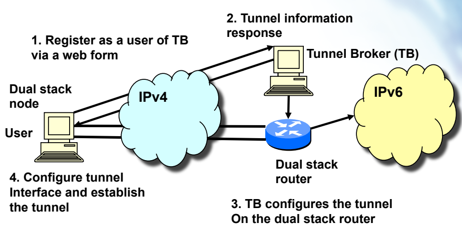
- Dual stack end points
- Explicit configuration with both IPv4 and IPv6 addresses at each end

Concept is borrowed from Cisco. Training material "Ipv6 Seminar" delivered at South Asian IPv6 Summit, Jan 2004

Asia Pacific Network Information Centre
APNIC

Tunnel broker

RFC 3053



Questions?

APNIC Asia Pacific Network Information Centre

Overview

- IPv6 Tunnel Transit Service Tutorial
  - IPv4 to IPv6 Transition technologies
  - **IPv6 Host Configuration**
  - Case study- IXP Configuration
  - Case study- ISP Tunnel Transit Service

APNIC Asia Pacific Network Information Centre

Exercise 1: IPv6 Host Configuration

- Windows XP SP2
- **netsh interface ipv6 install**

- Windows XP
- **ipv6 install**

APNIC Asia Pacific Network Information Centre

Exercise 1: IPv6 Host Configuration

Verify your Configuration

- c:\>ipconfig

Exercise 1: IPv6 Host Configuration

Testing your configuration

- **ping fe80::260:97ff:fe02:6ea5%4**

- **Note: the Zone id is YOUR interface index**

Questions?

Overview

- **IPv6 Tunnel Transit Service Tutorial**
  - IPv4 to IPv6 Transition technologies
  - IPv6 Host Configuration
  - **Case study- IXP Configuration**
  - Case study- ISP Tunnel Transit Service

Case study- IXP Configuration

IOS version support basic IPv6
- 12.2(2)T

IOS version support OSPF3 (IPv6)
- 12.2(15)T

IOS version support BGP(IPv6)
- 12.2(2)T

IOS version support BGP(4 byte AS Path)
- 12.4(24)T

APNIC Asia Pacific Network Information Centre

Case study- IXP Configuration

Required **global & interface** commands to enable IPv6

Router(Config)#ipv6 unicast-routing
Router(Config)#ipv6 cef (optional)

- Configure IPv6 address on interface

Router(Config-if)#ipv6 address *2001:0df0:00aa::1/64*
Router(Config-if)#ipv6 enable

- Verify IPv6 configuration

Router#sh ipv6 interface fa0/0

- Verify connectivity

Router#ping *2001:0df0:00aa::1*

APNIC Asia Pacific Network Information Centre

Case study- IXP Configuration

- Required **BGP** commands to enable IPv6 routing

Router(config)# router bgp 1
Router2(config-router)#bgp router-id 10.0.0.1 (if no 32 bit address on any interface)

Router(config-router)# address-family ipv6
Router(config-router-af)# no synchronization
Router(config-router-af)# neighbor 2001:0df0:00aa::1 remote-as 2 (EBGP)
Router(config-router-af)#neighbor 2001:0df0:00aa::1 activate
Router(config-router-af)# network 2001:0df0:00aa::/48

- Verify BGP IPv6 configuration

Router#sh bgp ipv6 unicast summary (summarized neighbor list)
Router#sh bgp ipv6 unicast (BGP database)
Router#sh ipv6 route bgp (BGP routing table)

APNIC Asia Pacific Network Information Centre

Case study- IXP Configuration

Required command to add IX prefix filter

- Create prefix filter in global mode

Router(config)#ipv6 prefix-list AS1 seq 2 permit 2001:0df0:aa::/48

- Apply prefix filter in BGP router configuration mode

Router(config-router)# address-family ipv6
Router(config-router-af)#neighbor 2001:0df0:aa::1 prefix-list AS1 in
Router(config-router-af)#neighbor 2001:0df0:aa::1 prefix-list AS1 out

APNIC Asia Pacific Network Information Centre

Case study- IXP Configuration

Controlling routing update traffic (Not data traffic)

1. Incoming routing update (Will control outgoing data traffic)
2. Outgoing routing update (Will control incoming data traffic)

APNIC Asia Pacific Network Information Centre

Case study- IXP Configuration

Two type of traffic exchange between ISPs

- Transit
  - Where ISP will pay to send/receive traffic
  - Downstream ISP will pay upstream ISP for transit service
- Peering
  - ISPs will not pay each other to interchange traffic
  - Works well if win win for both
  - Reduce cost on expensive transit link

IX Peering Model

- **BLPA (Bi-Lateral Peering Agreement)**
  - IX will only provide layer two connection/switch port to ISPs
  - Every ISPs will arrange necessary peering arrangement with others by their mutual business understanding.
- **MLPA (Multi-Lateral Peering Agreement)**
  - IX will provide layer two connection/switch port to ISPs
  - Each ISP will peer with a **route server** on the IX.
  - Route server will collect and distribute directly connected routes to every peers.

IXP Peering Policy

- BLPA is applicable where different categories of ISPs are connected in an IX
  - Large ISPs can choose to peer with large ISPs (base on their traffic volume)
  - Small ISPs will arrange peering with small ISPs
- Would be preferable for large ISPs
  - They will peer with selected large ISPs (Equal traffic interchange)
  - Will not loose business by peering with small ISP

IX Peering Policy

- MLPA model works well to widen the IX scope of operation (i.e national IX).
- Easy to manage peering
  - Peer with the **route server** and get all available local routes.
  - Do not need to arrange peering with every ISPs connected to the IX.
- Unequal traffic condition can create not intersected situation to peer with route server

IX peering Policy

- Both peering model can be available in an IX.
- Member will select peering model i.e either BLPA or MLPA (Route Server Peering)
- IX will provide switch port
- **Mandatory MLPA** model some time not preferred by large ISP (Business Interest)
  - Can create not interested situation to connect to an IX

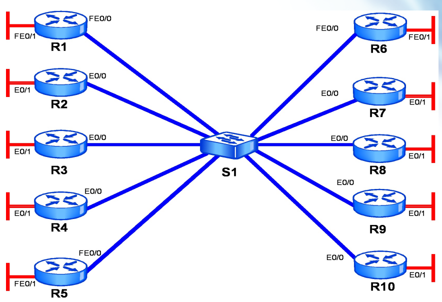
IX Operating Cost

- Access link
- Link maintenance
- Utility
- Administration

Cost Model

- Not for profit
- Cost sharing
- Membership based
- Commercial IX

IX Network Diagram



Steps to be done

- Determine the IP addressing scheme for the IX and for your ISP LAN network
- Configure the external interfaces of the Routers connecting your ISP to the IX
- Configure an internal LAN for your ISP
- Configure BGP on the Router
- Test this connectivity

IPv6 addressing plan

IX Subnet: 2001:AA::/48

Routers interface IPv6 Address (IX side)

Router 1: 2001:00AA::1/64
Router 2: 2001:00AA::2/64
Router 3: 2001:00AA::3/64
Router 4: 2001:00AA::4/64
Router 5: 2001:00AA::5/64
Router 6: 2001:00AA::6/64
Router 7: 2001:00AA::7/64
Router 8: 2001:00AA::8/64
Router 9: 2001:00AA::9/64
Router 10: 2001:00AA::10/64

IPv6 addressing plan

ISP's Global routing prefix

Router 1: 2001:abc1::/32
Router 2: 2001:abc2::/32
Router 3: 2001:abc3::/32
Router 4: 2001:abc4::/32
Router 5: 2001:abc5::/32
Router 6: 2001:abc6::/32
Router 7: 2001:abc7::/32
Router 8: 2001:abc8::/32
Router 9: 2001:abc9::/32
Router 10: 2001:abca::/32

Configuration steps

•Configure Router Interface Connected to IX (0/0)
•Configure Router Interface Connected to LAN (0/1)
•Try ping others

•Create EBGP Peering
•Announce LAN/ISP prefix

Step of IOS command line

Interface mode command:

- ***Router(config-if) # ipv6 address 2001:ABC1::1/64***

Enable IPv6 on the interface selected.

- ***Router(config-if) # ipv6 enable***

Bring the interface up

Router(config-if) no shutdown

Step of IOS command line

Exit from the interface configuration and enable IPv6 unicast datagram forwarding by typing the command below in the global mode.

- ***Router(config) # ipv6 unicast-routing***
  - ***Router(config) # ipv6 cef***

Configure BGP with the IPv6 address

Type "Router bgp" with the AS number in the command prompt of the Router global mode to configure the BGP protocol.

- ***Router#configure terminal***
- ***Router(config)#router bgp*** *<ASN>*
- ***Router(config-router)#no auto summary***
- ***Router(config-router)#no synchronization***
- ***Router (config-router-af)#no synchronization (IPv6 address-family mode)***

Where the AS number is the number of your Router

Configure BGP with the IPv6 address

Configure the peering address of the neighboring AS. Use the point to-point interface IP address for each Router connected to the IX.

NOTE: Each Router will have 9 neighbours

```
– Router(config-router)# neighbor <other ASN
  interface IP> remote-as <other ASN>
```

• Example for Router1:

```
Router#configure terminal
Router(config)#router bgp 1
Router(config-router)#no auto-summary
Router(config-router)#no synchronization Route
 r(config-router)#neighbor 2001:00AA::2 remote-as
  2 (for peering with Router2)
```

Asia Pacific Network Information Centre

APNIC

Configure BGP with the IPv6 address

```
Router(config-router)#address-family ipv6
Router(config-router-af)#neighbor 2001:00AA::2 activate
Router(config-router-af)#network 2001:00AA::/64
```

Asia Pacific Network Information Centre

APNIC

Configure BGP with the IPv6 address

Configure BGP router-id (optional). BGP protocol might ask for “router id” if there’s no IPv4 address configured aside from IPv6 address. Each eBGP speaker needs to have a 32 bit integer router ID.

The highest IP address configured on the router will become the router ID.

If a loopback interface address is configured, it will be use as the router ID.

If no IPv4 address is configured, watch out for such error message below.

- *% BGP cannot run because the Router-id is not configured*
- *BGP Router identifier 0.0.0.0, local AS number 1*

Asia Pacific Network Information Centre

APNIC

Verifying the BGP process

show bgp ipv6 unicast summary (to check the bgp summary table)

Expected output:

– Router6#sh bgp ipv6 unicast summary

– BGP router identifier 192.169.8.1, local AS number 6
– BGP table version is 4, main routing table version 4
– 3 network entries using 447 bytes of memory
– 3 path entries using 228 bytes of memory

– 0 BGP filter-list cache entries using 0 bytes of memory
– BGP using 1787 total bytes of memory
– BGP activity 8/1 prefixes, 14/4 paths, scan interval 60 secs

```
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
– 2001:ABC6::2 4      7    4252       4259      4            0    0     2d22h         0
– 2001:ABC6:0:1::2 4 8  5515       5513      4            0    0     3d19h
```

Verifying the BGP process

sh bgp ipv6 (to check the routing table for the BGP announcement)

– Expected Output:

```
– Router6#sh bgp ipv6 unicast
– BGP table version is 4, local router ID is 192.169.8.1
– Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
–              r RIB-failure, S Stale
– Origin codes: i - IGP, e - EGP, ? - incomplete

–    Network          Next Hop            Metric LocPrf Weight Path
– *> 2001:ABC6::/32   ::                   0        32768 i
– *> 2001:ABC8::/32   2001:ABC6:0:1::2
–                              0           0 8 i
– *> 2001:ABC9::/32   2001:ABC6:0:1::2
–                                            0 8 9 i
```

Verifying the BGP process

sh ipv6 route (to check the IPv6 routing table)

- Expected Output:

```
• Routerouter#sh ipv6 route
• IPv6 Routing Table - 9 entries
• Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
               U - Per-user Static route
•       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
•       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
•       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
• S   ::/0 [1/0]
•      via ::, Null0
• C   2001:AA::/64 [0/0]
•      via ::, Ethernet0/0
• L   2001:AA::2/128 [0/0]
•      via ::, Ethernet0/0
• C   2001:ABC1::/64 [0/0]
•      via ::, Ethernet0/0
• L   2001:ABC1::2/128 [0/0]
•      via ::, Ethernet0/0
```

Verifying the BGP process

sh ipv6 route (to check the IPv6 routing table)

Expected Output continue…….

- S 2001:ABC2::/32 [1/0]
- via ::, Null0
- B 2001:ABC3::/32 [20/0]
- via FE80::2E0:1EFF:FE63:2901, Ethernet0/0
- L FE80::/10 [0/0]
- via ::, Null0
- L FF00::/8 [0/0]
- via ::, Null0

Apply IX peering policy

- BLPA
  - Get an IX switch port
  - Arrange separate peering with other participating member
  - Routing updates can be controlled based on individual peer
  - Configuration example:

```
Router(config)#ipv6 prefix-list AS2-IN seq 2 permit 2001:0df0:abc2::/32
Router(config)#ipv6 prefix-list AS3-IN seq 2 permit 2001:0df0:abc3::/32
Router(config)#ipv6 prefix-list MYAS-PREFIX seq 2 permit 2001:0df0:abc1::/32

Router(config-router)# neighbor 2001:0df0:00aa::2 remote-as 2 (EBGP)
Router(config-router)# neighbor 2001:0df0:00aa::3 remote-as 3 (EBGP)

Router(config-router-af)#neighbor 2001:0df0:aa::2 prefix-list AS2-IN in
Router(config-router-af)#neighbor 2001:0df0:aa::2 prefix-list MYAS-PREFIX out

Router(config-router-af)#neighbor 2001:0df0:aa::3 prefix-list AS3-IN in
Router(config-router-af)#neighbor 2001:0df0:aa::3 prefix-list MYAS-PREFIX out
```

Apply IX peering policy

- MLPA
  - Get an IX switch port
  - Arrange a single peering with route server
  - Routing updates can be controlled on individual prefix
  - Configuration example:

```
Router(config)#ipv6 prefix-list RS-IN seq 2 permit 2001:0df0:abc2::/32
Router(config)#ipv6 prefix-list RS-IN seq 3 permit 2001:0df0:abc3::/32
Router(config)#ipv6 prefix-list RS-OUT seq 2 permit 2001:0df0:abc1::/32

Router(config-router-af)# neighbor 2001:0df0:00aa::e remote-as 100 (EBGP)

Router(config-router-af)# neighbor 2001:0df0:aa::e prefix-list RS-IN in
Router(config-router-af)# neighbor 2001:0df0:aa::2 prefix-list RS-OUT out
```

Questions?

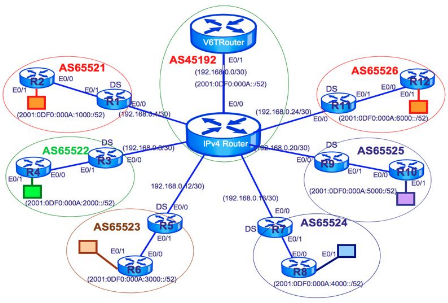
APNIC
Asia Pacific Network Information Centre

Overview

- **IPv6 Tunnel Transit Service Tutorial**
  - IPv4 to IPv6 Transition technologies
  - IPv6 Host Configuration
  - Case study- IXP Configuration
  - **Case study- ISP Tunnel Transit Service**

APNIC
Asia Pacific Network Information Centre

Case study- ISP Tunnel Transit Service



APNIC
Asia Pacific Network Information Centre

Case study- ISP Tunnel Transit Service

Steps to be done

- Determine the IP addressing scheme for your ISP LAN network
- Determine the IP addressing scheme for the tunnel interface
- Configure the interfaces of the Routers with IPv6 address
- Configure EBGP on Dual Stack (DS) router
- Configure Tunnel in DS router with IPV6 address
- Configure EBGP Peering with IPv6 router
- Configure iBGP peering with ISP router
- Test this connectivity

Case study- ISP Tunnel Transit Service

- Global prefix received: 2001:0df0:000a::/48

2001:0DF0:000A:0000::/52 (AS45192)
2001:0DF0:000A:1000::/52 (AS65521)
2001:0DF0:000A:2000::/52 (AS65522)
2001:0DF0:000A:3000::/52 (AS65523)
2001:0DF0:000A:4000::/52 (AS65524)
2001:0DF0:000A:5000::/52 (AS65525)
2001:0DF0:000A:6000::/52 (AS65526)

Case study- ISP Tunnel Transit Service

AS45192 IP distribution

192.168.0.0/30 [IPv6Router(1) -IPv4Router(2)]
2001:0DF0:000A:0000::/52 (AS45192)
2001:0DF0:000A:0000::/64 (IPv6Router-R1 Tunnel0)
2001:0DF0:000A:0001::/64 (IPv6Router-R3 Tunnel0)
2001:0DF0:000A:0002::/64 (IPv6Router-R5 Tunnel0)
2001:0DF0:000A:0003::/64 (IPv6Router-R7 Tunnel0)
2001:0DF0:000A:0004::/64 (IPv6Router-R9 Tunnel0)
2001:0DF0:000A:0005::/64 (IPv6Router-R11 Tunnel0)

Case study- ISP Tunnel Transit Service

Allocated IPv6 address for different AS

192.168.0.4/30 [R1(6) -IPv4Router(5)]
2001:0DF0:000A:1000::/52 (AS65521)
2001:0DF0:000A:1000::/64 (R1-R2)
2001:0DF0:000A:1001::/64 (R1 LAN)
2001:0DF0:000A:0000::2/64 (R1 Tunnel 0)

AS65521

192.168.0.8/30 [R3(10) -IPv4Router(9)]
2001:0DF0:000A:2000::/52 (AS65522)
2001:0DF0:000A:2000::/64 (R3-R4)
2001:0DF0:000A:2001::/64 (R4 LAN)
2001:0DF0:000A:0001::2/64 (R3 Tunnel 0)

AS65522

192.168.0.12/30 [R5(14) -IPv4Router(13)]
2001:0DF0:000A:3000::/52 (AS65523)
2001:0DF0:000A:3000::/64 (R5-R6)
2001:0DF0:000A:3001::/64 (R6 LAN)
2001:0DF0:000A:0002::2/64 (R5 Tunnel 0)

AS65523

Case study- ISP Tunnel Transit Service

Allocated IPv6 address for different AS

192.168.0.16/30 [R7(18) -IPv4Router(17)]
2001:0DF0:000A:4000::/52 (AS65524)
2001:0DF0:000A:4000::/64 (R7-R8)
2001:0DF0:000A:4001::/64 (R8 LAN)
2001:0DF0:000A:0003::2/64 (R7 Tunnel 0)

AS65524

192.168.0.20/30 [R9(22) -IPv4Router(21)]
2001:0DF0:000A:5000::/52 (AS65525)
2001:0DF0:000A:5000::/64 (R9-R10)
2001:0DF0:000A:5001::/64 (R10 LAN)
2001:0DF0:000A:0004::2/64 (R9 Tunnel 0)

AS65525

192.168.0.24/30 [R11(26) -IPv4Router(25)]
2001:0DF0:000A:6000::/52 (AS65526)
2001:0DF0:000A:6000::/64 (R11-R12)
2001:0DF0:000A:6001::/64 (R12 LAN)
2001:0DF0:000A:0005::2/64 (R11 Tunnel 0)

AS65526

Case study- ISP Tunnel Transit Service

Configuration steps in every AS

- DSRouter(Config)#ipv6 unicast-routing
- DSRouter(Config)#ipv6 cef
- DSRouter(Config-if)#IPv4 address with IPv4Router
- DSRouter(Config)# EBGP with IPv4Router
- DSRouter(Config-if)#6 to 4 Tunnel with IPv6Router
- DSRouter(Config)#EBGP with IPv6 router
- DSRouter(Config-if)#IPv6 address with IPv6 only router
- DSRouter(Config-if)#iBGP peering with IPv6 only router

- IPv6OnlyRouter(Config)#ipv6 unicast-routing
- IPv6OnlyRouter(Config)#ipv6 cef
- IPv6OnlyRouter(Config)#IPv6 address with DSRouter
- IPv6OnlyRouter(Config)#IPv6 address with LAN
- IPv6OnlyRouter(Config)#iBGP Peering with DS router

Case study- ISP Tunnel Transit Service

Verification steps in every AS

- DSRouter#sh bgp ipv6 (unicast) summary
- DSRouter#sh bgp ipv6 (unicast)
- DSRouter#sh ipv6 route (bgp)

- IPv6OnlyRouter#sh bgp ipv6 (unicast) summary
- IPv6OnlyRouterRouter#sh bgp ipv6 (unicast)
- IPv6OnlyRouterRouter#sh ipv6 route (bgp)

Questions?

Thank you!