IPv4/IPv6 Routing and Deployment Workshop

July 10-14, 2012, Karachi, Pakistan

In conjunction with

APNIC

Presenter

- Champika Wijayatunga
  - Training Unit Manager, APNIC
  - champika@apnic.net

- GZ Kabir
  - Systems Integrator
  - gzkabir@bdcom.com

- Vivek Nigam
  - Internet Resource Analyst, APNIC
  - vivek@apnic.net

Agenda

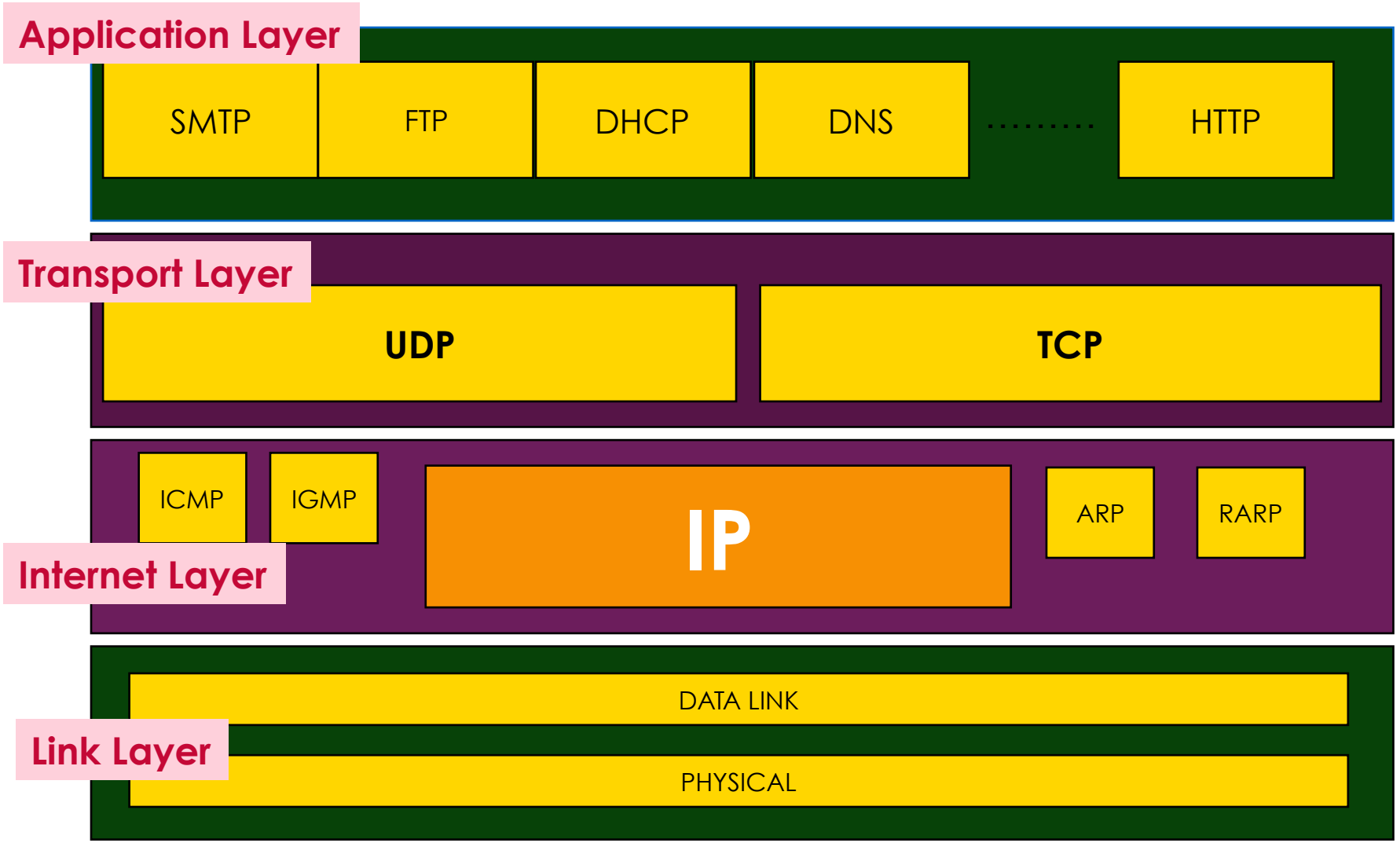
- Internet Fundamentals
- Internet Resource Management
- IP addressing and IP routing basics
- Introduction to IPv6 and Protocol Architecture
- IPv6 Addressing and Sub-netting
- IPv6 Host Configuration
- IPv4/IPv6 Deployment Plan – Case Study
- IPv4/IPv6 Deployment in IGP – Case Study
- IPv4 to IPv6 Transition Technologies
- IPv4/IPv6 Deployment in EGP – Case Study
- IPv6 DNS

IPv6 Overview

What is IPv6?

- IP stands for Internet Protocol which is one of the main pillars that supports the Internet today
- Current version of IP protocol is IPv4
- The new version of IP protocol is IPv6
- There is a version of IPv5 but it was assigned for experimental use [RFC1190]
- IPv6 was also called IPng in the early days of IPv6 protocol development stage

TCP/IP Protocol Structure



Background Of IPv6 Protocol

- During the late 1980s (88-89), the Internet has started to grow exponentially
- The ability to scale the Internet for future demand requires a limitless supply of IP addresses and improved mobility
- In 1991, IETF decided that the current version of IP (IPv4) had outlived its design and need to develop a new protocol for Internet
- In 1994, IETF gave a clear direction of IPng or IPv6 after a long process of discussion

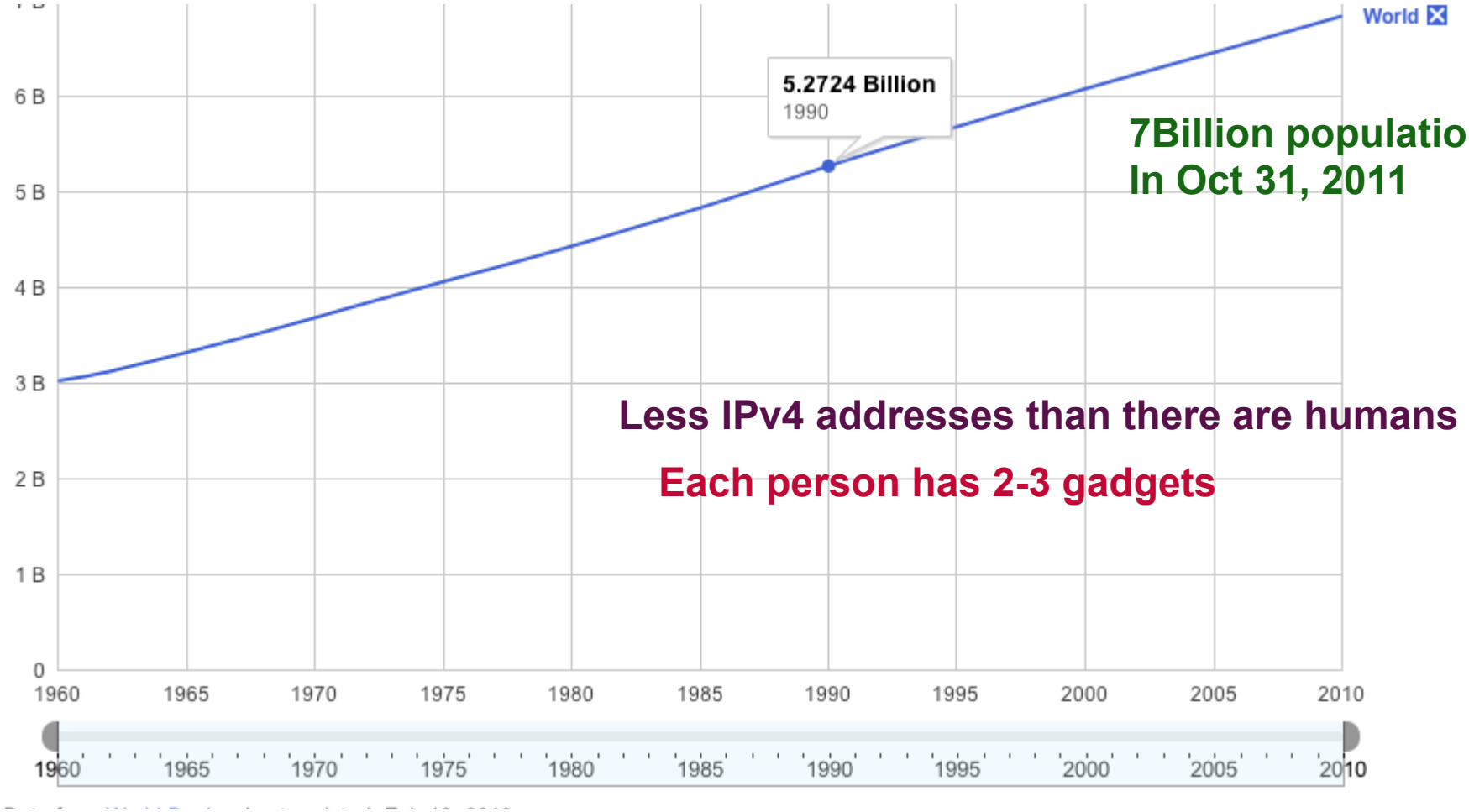
Background Of IPv6 Protocol

- August 1990
  - First wakeup call by Solensky in IETF on IPv4 address exhaustion
- December 1994
  - IPng area were formed within IETF to manage IPng effort [RFC1719]
- December 1994
  - List of technical criteria was defined to choose IPng [RFC1726]
- January 1995
  - IPng director recommendation to use 128 bit address [RFC1752]
- December 1995
  - First version of IPv6 address specification [RFC1883]
- December 1998
  - Updated version changing header format from 1st version [RFC2460]

Motivation Behind IPv6 Protocol

- New generation Internet need:
  - Plenty of address space (PDA, Mobile Phones, Tablet PC, Car, TV etc etc ☺)
  - Solution of very complex hierarchical addressing need, which IPv4 is unable to provide
  - End to end communication without the need of NAT for some real time application (i.e online transaction)
  - Ensure security, reliability of data and faster processing of protocol overhead
  - Stable service for mobile network (i.e Internet in airline)

Human Population



7Billion population
In Oct 31, 2011

Less IPv4 addresses than there are humans

Each person has 2-3 gadgets

New Functional Improvement

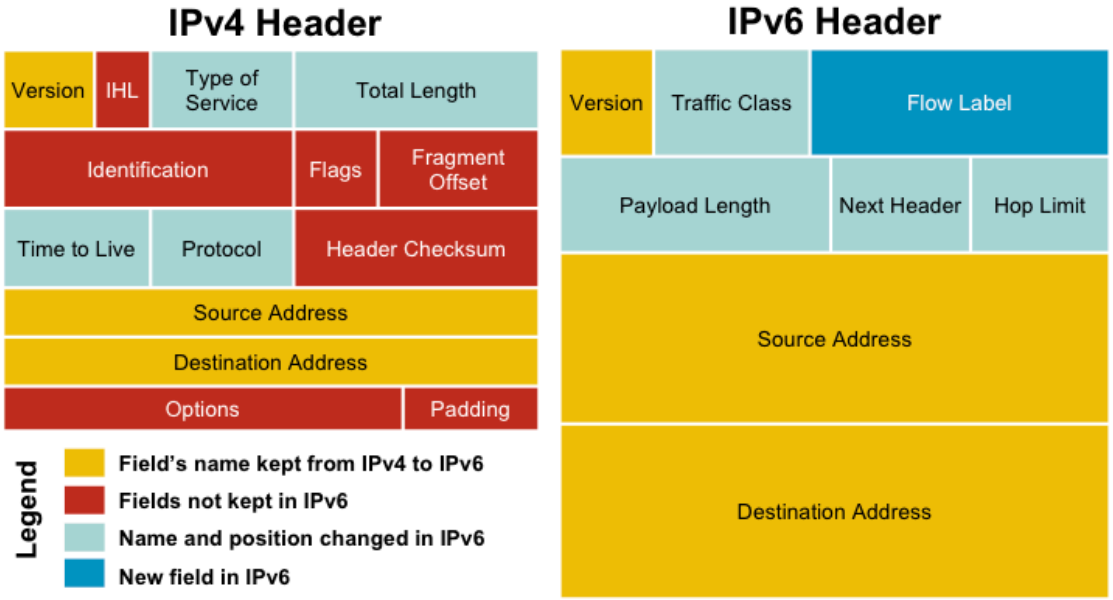
- Address Space
  - Increase from 32-bit to 128-bit address space
- Management
  - Stateless autoconfiguration means no more need to configure IP addresses for end systems, even via DHCP
- Performance
  - Fixed header size (40 bytes) and 64-bit header alignment mean better performance from routers and bridges/switches

Source: http://www.opus1.com/ipv6/whatisipv6.html

New Functional Improvement

- Multicast/Multimedia
  - Built-in features for multicast groups,management, and new "anycast" groups
- Mobile IP
  - Eliminate triangular routing and simplify deployment of mobile IP-based systems
- Virtual Private Networks
  - Built-in support for ESP/AH encrypted/ authenticated virtual private network protocols;
- No more broadcast

Protocol Header Comparison



- IPv4 contains 10 basic header field
- IPv6 contains 6 basic header field
- IPv6 header has 40 octets in contrast to the 20 octets in IPv4
- So a smaller number of header fields and the header is 64-bit aligned to enable fast processing by current processors

Diagram Source: www.cisco.com

IPv6 Protocol Header Fields

- Version
  - A 4-bit field, same as in IPv4. It contains the number 6 instead of the number 4 for IPv4
- Traffic class
  - An 8-bit field similar to the type of service (ToS) field in IPv4. It tags packet with a traffic class that it uses in differentiated services (DiffServ). These functionalities are the same for IPv6 and IPv4.
- Flow label
  - A completely new 20-bit field. It tags a flow for the IP packets. It can be used for multilayer switching techniques and faster packet-switching performance

IPv6 Protocol Header Format

- Payload length
  - 16-bit field is similar to the IPv4 Total Length Field
  - the length of the data carried after the header, (whereas with IPv4 the Total Length Field included the header). 2^{16} = 65536 Octets.
- Next header
  - The 8-bit value of this field determines the type of information that follows the basic IPv6 header. It can be a transport-layer packet, such as TCP or UDP, or it can be an extension header. The next header field is similar to the protocol field of IPv4.
- Hop limit
  - This 8-bit field defined by a number which count the maximum hops that a packet can remain in the network before it is destroyed. With the IPv4 TTL field this was expressed in seconds and was typically a theoretical value and not very easy to estimate.

IPv6 Extension Header

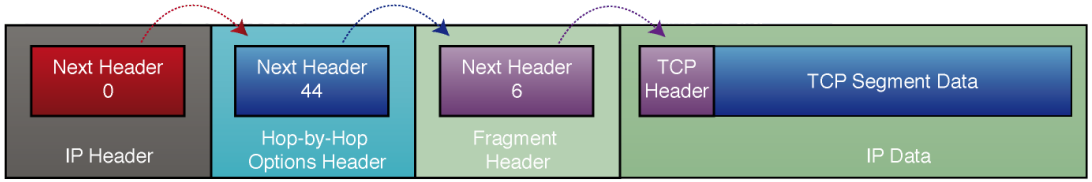
- Adding an optional Extension Header in IPv6 makes it simple to add new features in IP protocol in future without a major re-engineering of IP routers everywhere
- The number of extension headers are not fixed, so the total length of the extension header chain is variable
- The extension header will be placed in between main header and payload in an IPv6 packet

IPv6 Extension Header

- If the Next Header field value (code) is 6, it determines that there is no extension header and the next header field is pointing to TCP header which is the payload of this IPv6 packet
- Code values of Next Header field:
  - 0 Hop-by-hop option
  - 2 ICMP
  - 6 TCP
  - 17 UDP
  - 43 Source routing
  - 44 Fragmentation
  - 50 Encrypted security payload
  - 51 Authentication
  - 59 Null (No next header)
  - 60 Destination option

Link listed Extension Header

IPv6 Datagram With No Extension Headers Carrying TCP Segment



IPv6 Datagram With Two Extension Headers Carrying TCP Segment

- Link listed extension header can be used by simply using next header code value
- Above example use multiple extension header creating link list by using next header code value i.e 0 44 6
- The link list will end when the next header point to transport header i.e next header code 6

MTU Size Guideline

- MTU for IPv4 and IPv6
  - MTU is the largest size datagram that a given link layer technology can support [i.e HDLC]
  - Minimum MTU 68 Octet [IPv4] 1280 Octet [IPV6]
  - Most efficient MTU 576 [IPv4] 1500 [IPv6]
- Important things to remember:
  - Minimum MTU for IPv6 is 1280
  - Most efficient MTU is 1500
  - Maximum datagram size 64k

Size of The IPv6 Datagram

- The maximum size of IPv6 datagram will be determined by two factor:
  - Maximum Transmission Unit (MTU) of intermediate nodes [L2 link technology can support i.e HDLC]
  - Payload length of IPv6 header which is 16 bit so normal payload can not be larger then 64k octets.
- Jumbogram can increase IPv6 datagram size larger then 64k octets. But they need special processing on each hop since they are oversize.
  - One of two uses of hop-by-hop option header is Jumbogram

IPv6 Security Features

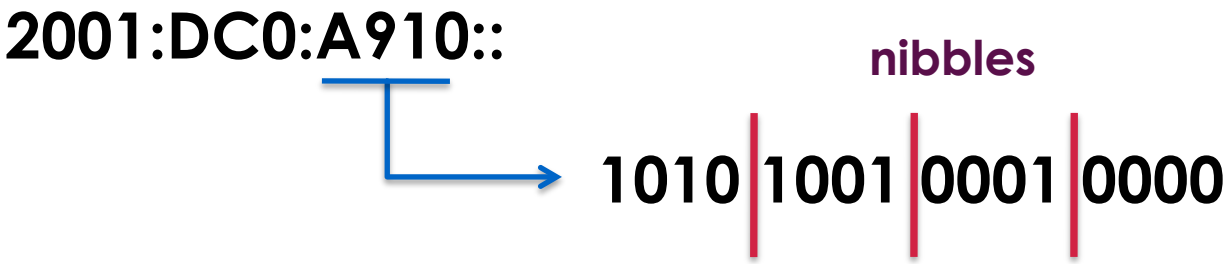
- IPsec is mandatory in IPv6
- Since IPsec become part of the IPv6 protocol all node can secure their IP traffic if they have required keying infrastructure
- In build IPsec does not replace standard network security requirement but introduce added layer of security with existing IP network

IP Address Mobility

- IP address mobility is a mechanism that will sustain the IP connection even when the IP address change if the device move from one location to other location (subnet)
- IP address mobility is achieved by using Mobile IP
- Mobile IP is designed to work with both IPv4 [RFC3344] and IPv6 [RFC3775]
- Mobile IP operation is optimized for IPv6

IPv6 Addressing

- An IPv6 address is 128 bits long
- So the number of addresses are **2^128** = 340282366920938463463374607431768211455
- In hex, 4 bits (also called a ‘nibble’) is represented by a hex digit
- So 128 bits is reduced down to 32 hex digits



IPv6 Addressing

- Hexadecimal values of eight 16 bit fields
  - X:X:X:X:X:X:X:X (X=16 bit number, ex: A2FE)
  - 16 bit number is converted to a 4 digit hexadecimal number
- Example:
  - FE38:DCE3:124C:C1A2:BA03:6735:EF1C:683D
  - Abbreviated form of address

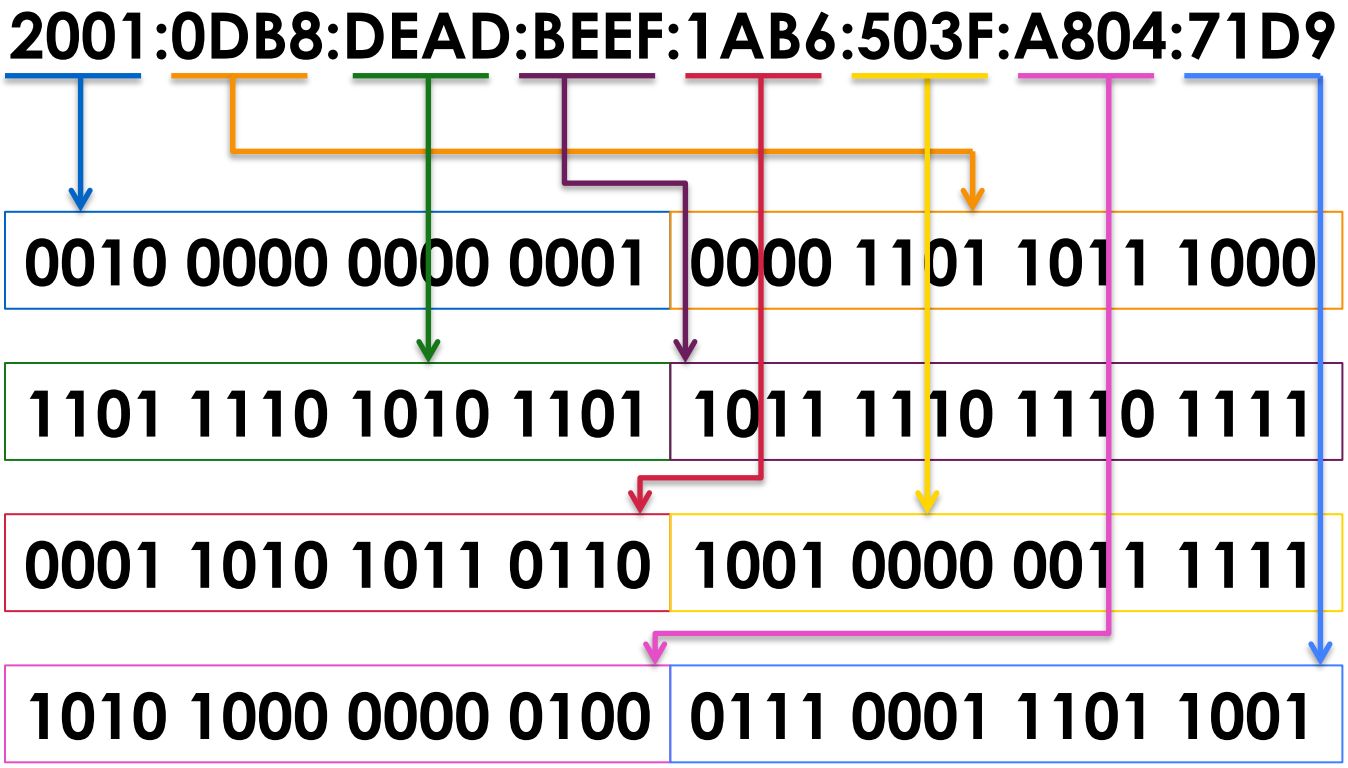
4EED:0023:**0000:0000:0000**:036E:1250:2B00 **Leading zeroes**

→4EED:23:**0:0:0**:36E:1250:2B00 **Groups of zeroes**

→4EED:23**::**36E:1250:2B00 **Double colons**

(Null value can be used only once)

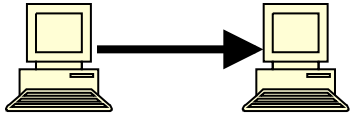
IPv6 Addressing



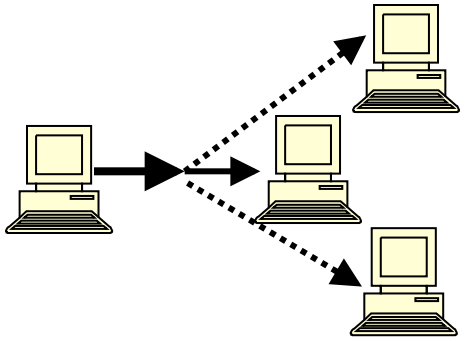
IPv6 Addressing Model

RFC 4291

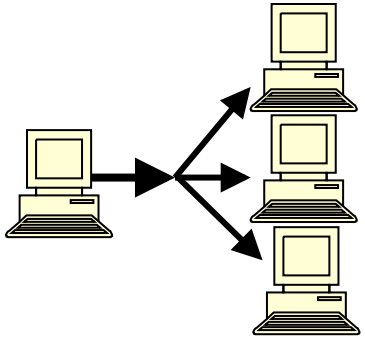
- Unicast
  - An identifier for a single interface



- Anycast
  - An identifier for a set of interfaces



- Multicast
  - An identifier for a group of nodes



Local Addresses With Network Prefix

- Link Local Address
  - A special address used to communicate within the local link of an interface
  - i.e. anyone on the link as host or router
  - This address in packet destination that packet would never pass through a router
  - **fe80::/10**

Local Addresses With Network Prefix

- Site Local Address
  - Addresses similar to the RFC 1918 / private address like in IPv4
  - **fec0::/10**
- This address type is now deprecated by RFC 3879 because of lack of uniqueness
- Still used in test lab

Global Addresses With Network Prefix

- IPV6 Global Unicast Address
  - Global Unicast Range: 0010 2000::/3
    0011 3000::/3
  - All five RIRs are given a /12 from the /3 to further distribute within the RIR region

APNIC	2400:0000::/12
ARIN	2600:0000::/12
AfriNIC	2C00:0000::/12
LACNIC	2800:0000::/12
Ripe NCC	2A00:0000::/12

Global Addresses With Network Prefix

- 6to4 Addresses
  - **2002::/16**
  - Designed for a special tunneling mechanism [RFC 3056] to connect IPv6 Domains via IPv4 Clouds
  - Automatic tunnel transition Mechanisms for IPv6 Hosts and Routers
  - Need 6to4 relay routers in ISP network

Examples and Documentation Prefix

- Two address ranges are reserved for examples and documentation purpose by RFC 3849
  - For example 3fff:ffff::/32
  - For documentation 2001:0DB8::/32

IPv6 Address Range

- Unspecified Address ::/128
- Loopback ::1/128
- Global Unicast `0010` 2000::/3
- Link Local `1111 1110 10` FE80::/10
- Multicast Address `1111 1111` FF00::/8

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::)

Exercise

1. 2001:0db8:0000:0000:0000:0000:0000:0000
2. 2001:0db8:0000:0000:d170:0000:1000:0ba8
3. 2001:0db8:00a0:0000:0000:00f6:0000:00aa
4. 2001:0db8:0fc5:007b:ab70:0210:0000:00bb

Exercise 1.1: IPv6 subnetting

1. Identify the first four /64 address blocks out of 2001:AA:2000::/48
    1. _____
    2. _____
    3. _____
    4. _____

Exercise 1.2: IPv6 subnetting

2. Identify the first four /36 address blocks out of 2001:ABC::/32
    1. _____
    2. _____
    3. _____
    4. _____

Exercise 1.3: IPv6 subnetting

3. Identify the first six /37 address blocks out of 2001:AA::/32

    1. _____
    2. _____
    3. _____
    4. _____
    5. _____
    6. _____

IPv6 Address Management

Allocation and Assignment

APNIC
Allocates
to APNIC Member

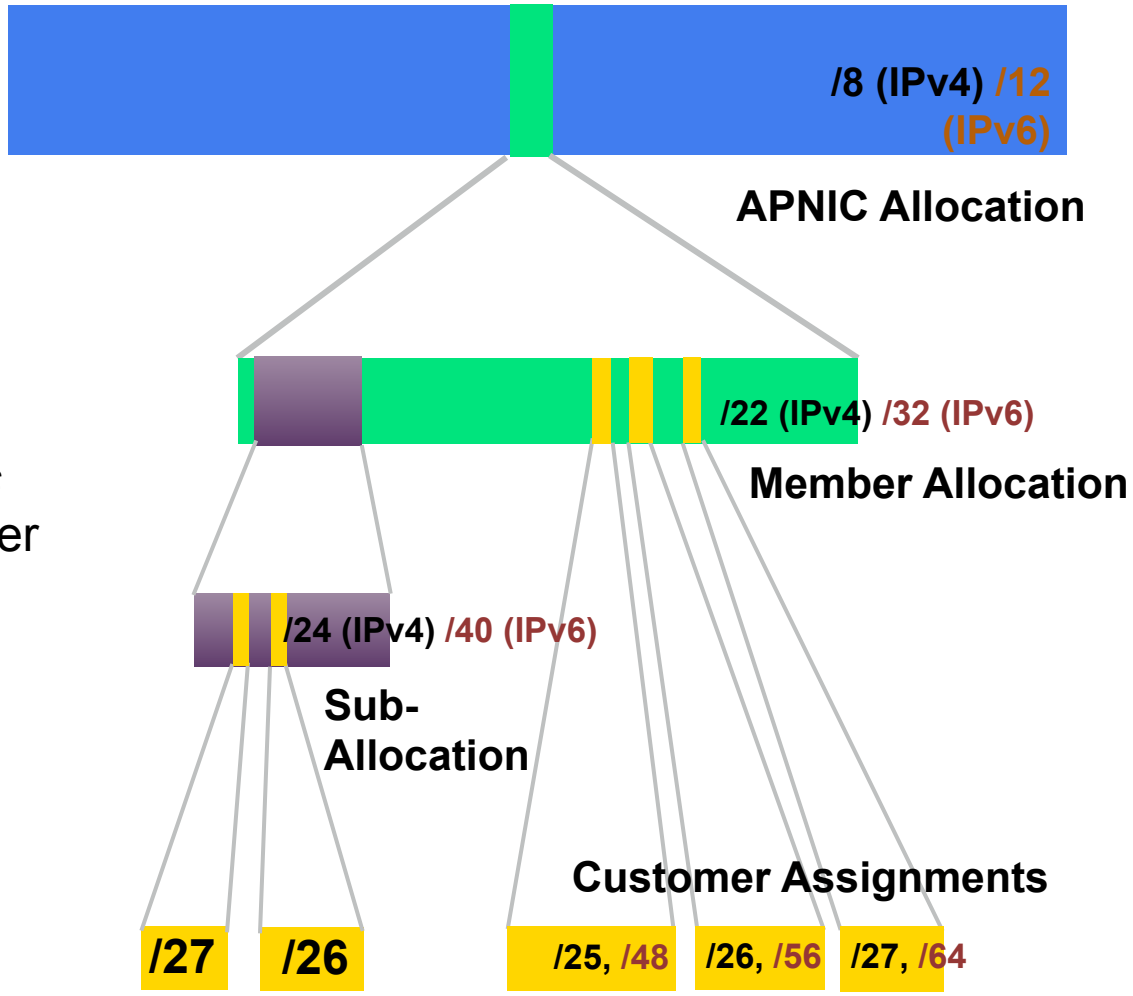
APNIC Member

Allocates
to downstream

Downstream
Assigns
to end-user

Assigns
to end-user

Customer / End User



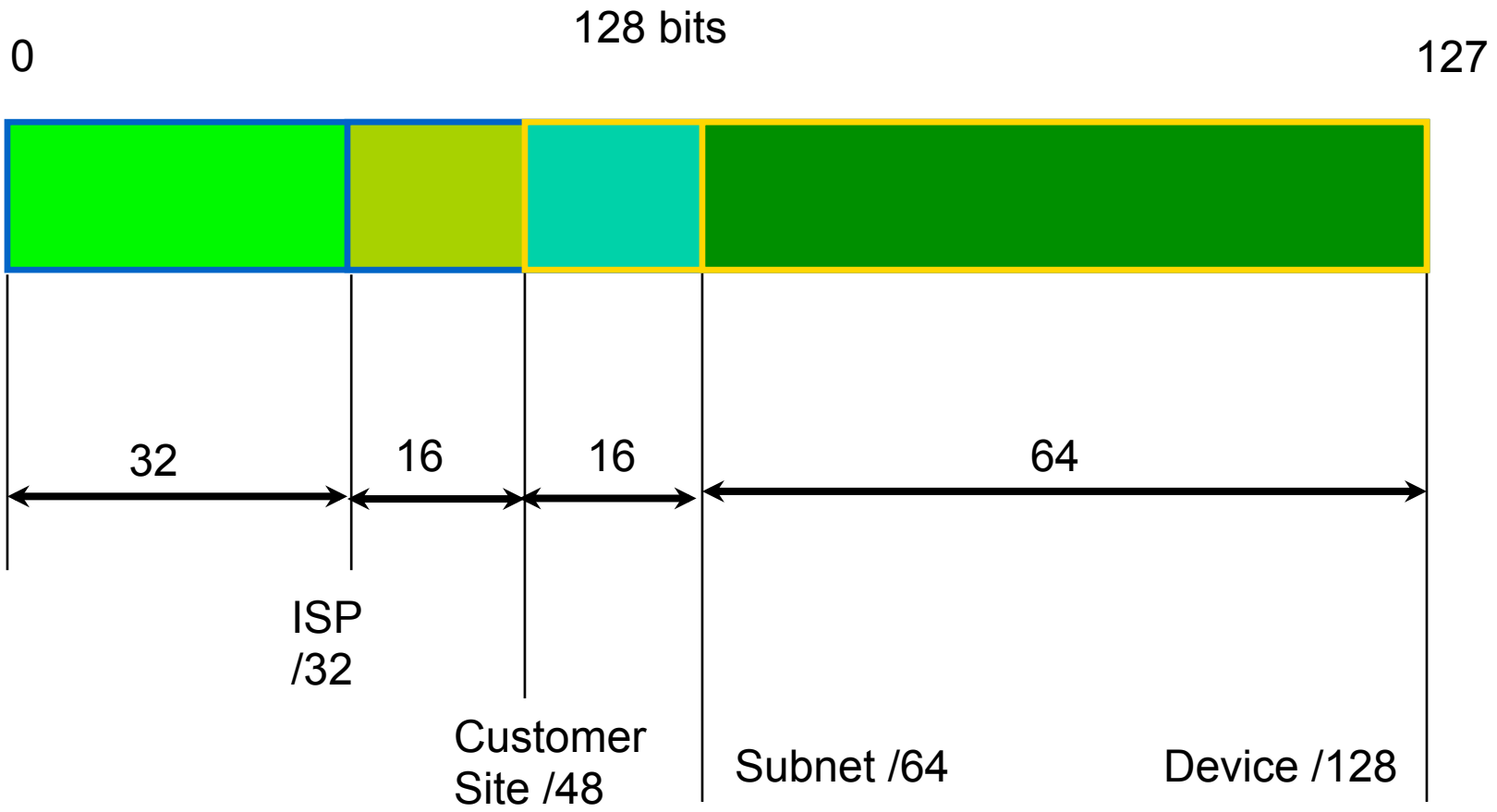
Initial IPv6 Allocation

- To qualify for an initial allocation of IPv6 address space, an organization must:
  - Not be an end site (must provide downstream services)
  - Plan to provide IPv6 connectivity to organizations to which it will make assignments
- Meet one of the two following criteria:
  - Have a plan for making at least 200 assignments to other organizations within two years OR
  - Be an existing ISP with IPv4 allocations from an APNIC or an NIR, which will make IPv6 assignments or sub-allocations to other organizations and announce the allocation in the inter-domain routing system within two years

“One Click” IPv6 Policy

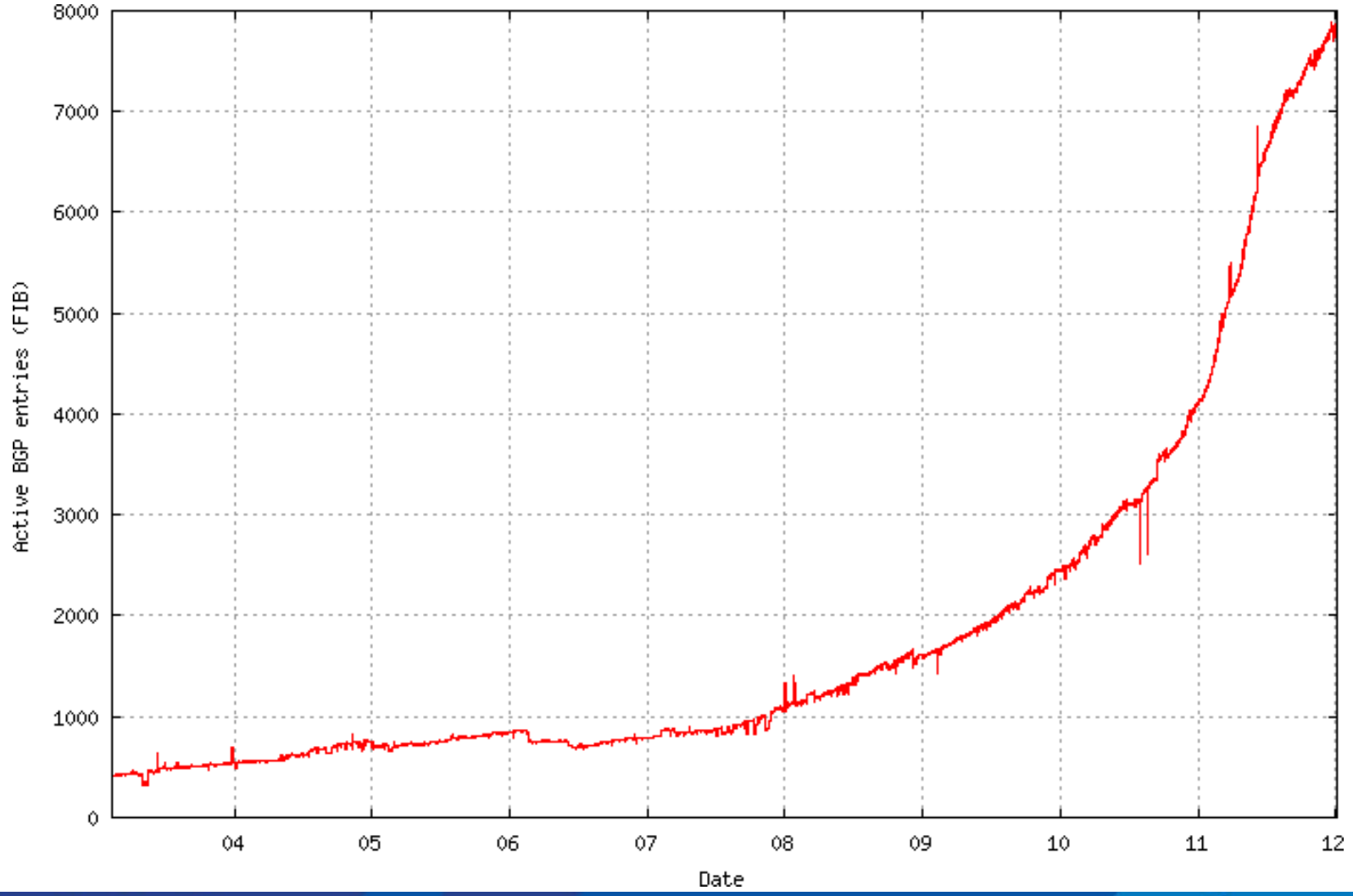
- Members with IPv4 holdings can click the button in MyAPNIC to instantly receive their IPv6 block
  - No forms to fill out!
  - “Get your IPv6 addresses” icon in the main landing page at MyAPNIC
- A Member that has an IPv4 allocation is eligible for a /32
- A Member that has an IPv4 assignment is eligible for a /48

IPv6 addressing structure

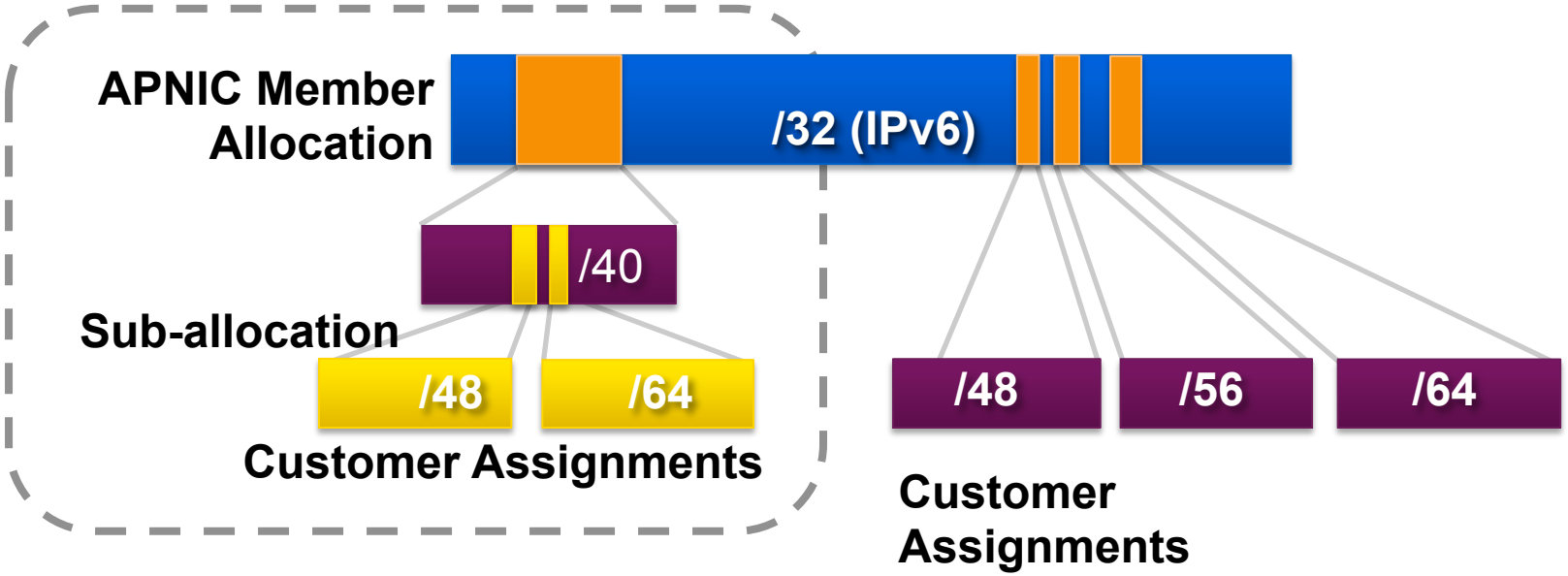


IPv6 BGP Routing Table

Source: CIDR Report



Sub-allocations



- No specific policy for LIRs to allocate space to subordinate ISPs
- All /48 assignments to end sites must be registered
- Second Opinion applies
  - Must submit a second opinion request for assignments more than /48

Sub-allocation Guidelines

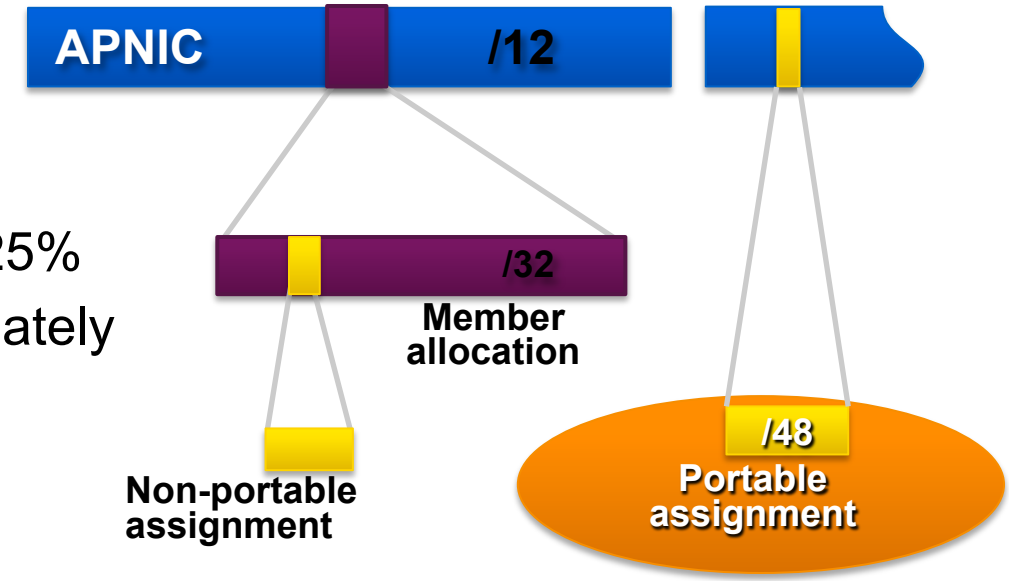
- Sub-allocate cautiously
  - Only allocate or assign what the customer has demonstrated a need for
  - Seek APNIC advice if in doubt
- Efficient assignments
  - Member is responsible for overall utilisation
- Database registration (WHOIS Db)
  - Sub-allocations & assignments must be registered in the whois db

IPv6 Assignment Policy

- Assignment address space size
  - Minimum of /64 (only 1 subnet), Normal maximum of /48, Larger end-site assignment can be justified
- In typical deployments today
  - Several ISPs gives small customers a /56 or a /60 and Single LAN end sites a /64, e.g.,
    - /64 if end-site will ever only be a LAN
    - /60 for small end-sites (e.g. consumer)
    - /56 for medium end-sites (e.g. small business)
    - /48 for large end-sites
- Assignment of multiple /48s to a single end site
  - Documentation must be provided
  - Will be reviewed at the RIR/NIR level
- Assignment to operator's infrastructure
  - /48 per PoP as the service infrastructure of an IPv6 service operator

Portable Assignments for IPv6

- For (small) organisations who require a portable assignment for multi-homing purposes
  - The current policy allows for IPv6 portable assignment to end-sites
  - Size: /48, or a shorter prefix if the end site can justify it
  - To be multihomed within 1 month
  - Demonstrate need to use 25% of requested space immediately and 50% within a year



IXP IPv6 Assignment Policy

- Criteria
  - Demonstrate ‘open peering policy’
  - 3 or more peers
- Portable assignment size: /48
  - All other needs should be met through normal processes
  - /64 holders can “upgrade” to /48
    - Through NIRs/ APNIC
    - Need to return /64

Portable Critical Infrastructure Assignments

- What is Critical Internet Infrastructure?
  - Domain Registry Infrastructure
    - Operators of Root DNS, gTLD, and ccTLD
  - Address Registry Infrastructure
    - IANA, RIRs & NIRs
- Why a specific policy ?
  - Protect stability of core Internet function
- Assignment sizes:
  - IPv6: /32

IPv6 Utilisation

- Utilisation determined from end site assignments
  - ISP responsible for registration of all /48 assignments
  - Intermediate allocation hierarchy not considered
- Utilisation of IPv6 address space is measured differently from IPv4
  - Use HD ratio to measure
- Subsequent allocation may be requested when IPv6 utilisation requirement is met

Subsequent Allocation

- Must meet **HD = 0.94** utilisation requirement of previous allocation (subject to change)
- Other criteria to be met
  - Correct registrations (all /48s registered)
  - Correct assignment practices etc
- Subsequent allocation results in a doubling of the address space allocated to it
  - Resulting in total IPv6 prefix is 1 bit shorter
  - Or sufficient for 2 years requirement

HD Ratio

- The HD ratio threshold is
  - HD = log (/56 units assigned) / log (16,777,216)
  - 0.94 = 6,183,533 x /56 units
- Calculation of the HD ratio
  - Convert the assignment size into equivalent /56 units
    - Each /48 end site = 256 x /56 units
    - Each /52 end site = 16 x /56 units
    - Each /56 end site = 1 x /56 units
    - Each /60 end site = 1/16 x /56 units
    - Each /64 end site = 1/256 x /56 units

IPv6 utilisation (HD = 0.94)

- Percentage utilisation calculation

IPv6 Prefix	Site Address Bits	Total site address in /56s	Threshold (HD ratio 0.94)	Utilisation %
/42	14	16,384	9,153	55.9%
/36	20	1,048,576	456,419	43.5%
/35	21	2,097,152	875,653	41.8 %
/32	**24**	**16,777,216**	**6,185,533**	**36.9%**
/29	27	134,217,728	43,665,787	32.5 %
/24	32	4,294,967,296	1,134,964,479	26.4 %
/16	40	1,099,511,627,776	208,318,498,661	18.9 %

RFC 3194: “In a hierarchical address plan, as the size of the allocation increases, the density of assignments will decrease.”

Configuration of IPv6 Node Address

- There are 3 ways to configure IPv6 address on an IPv6 node:
  - Static address configuration
  - DHCPv6 assigned node address
  - Auto-configuration [New feature in IPv6]

IPv6 autoconfiguration

- Stateless mechanism
  - For a site not concerned with the exact addresses
  - No manual configuration required
  - Minimal configuration of routers
  - No additional servers
- Stateful mechanism
  - For a site that requires tighter control over exact address assignments
  - Needs a DHCP server
    - DHCPv6

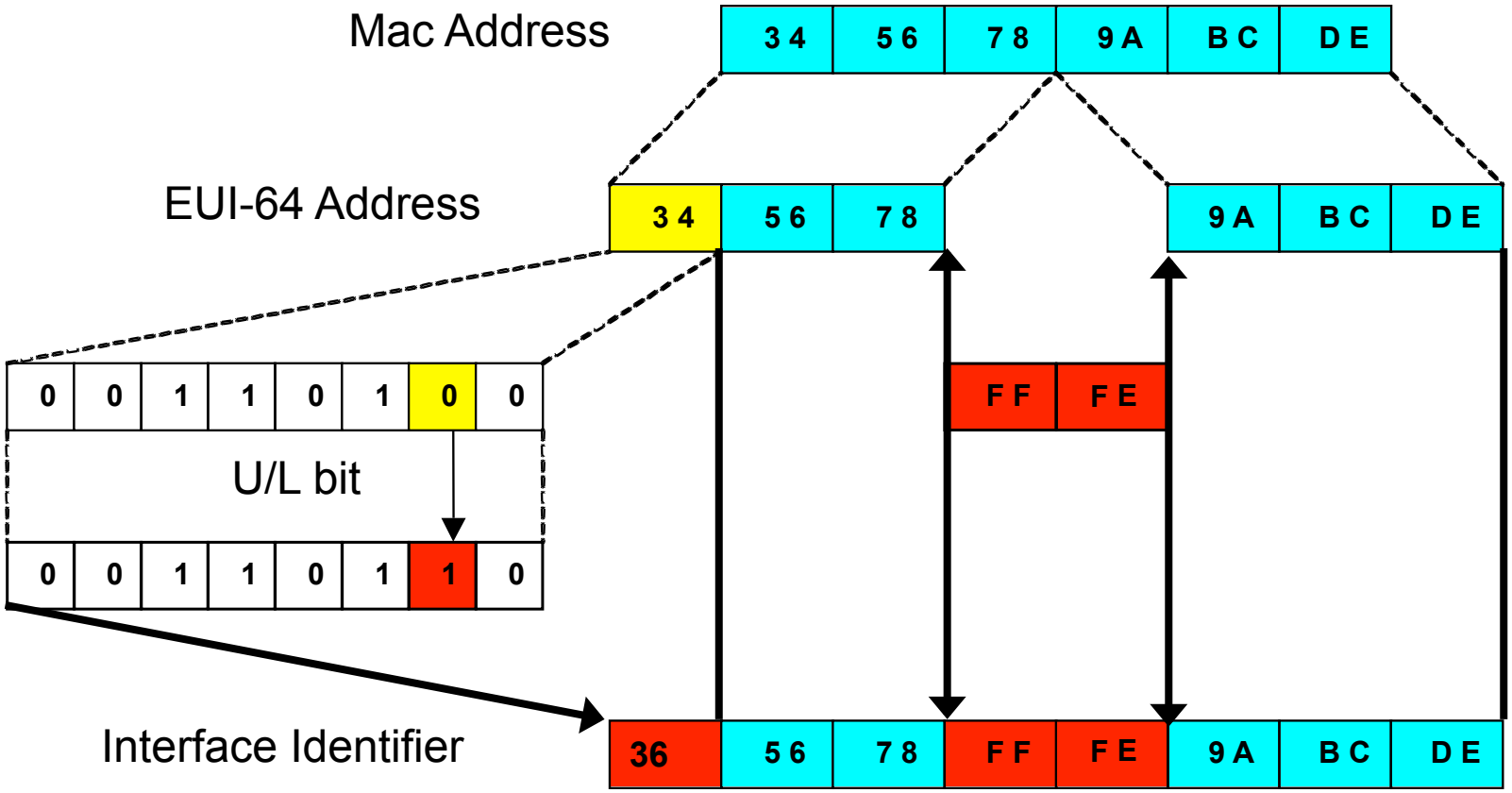
IPv6 Plug and Play

- IPv6 link local address
  - Even if no servers/routers exist to assign an IP address to a device, the device can still auto-generate an IP address
    - Allows interfaces on the same link to communicate with each other
- Stateless mechanism
  - For a site not concerned with the exact addresses
  - No manual configuration required
  - Minimal configuration of routers
  - No additional servers

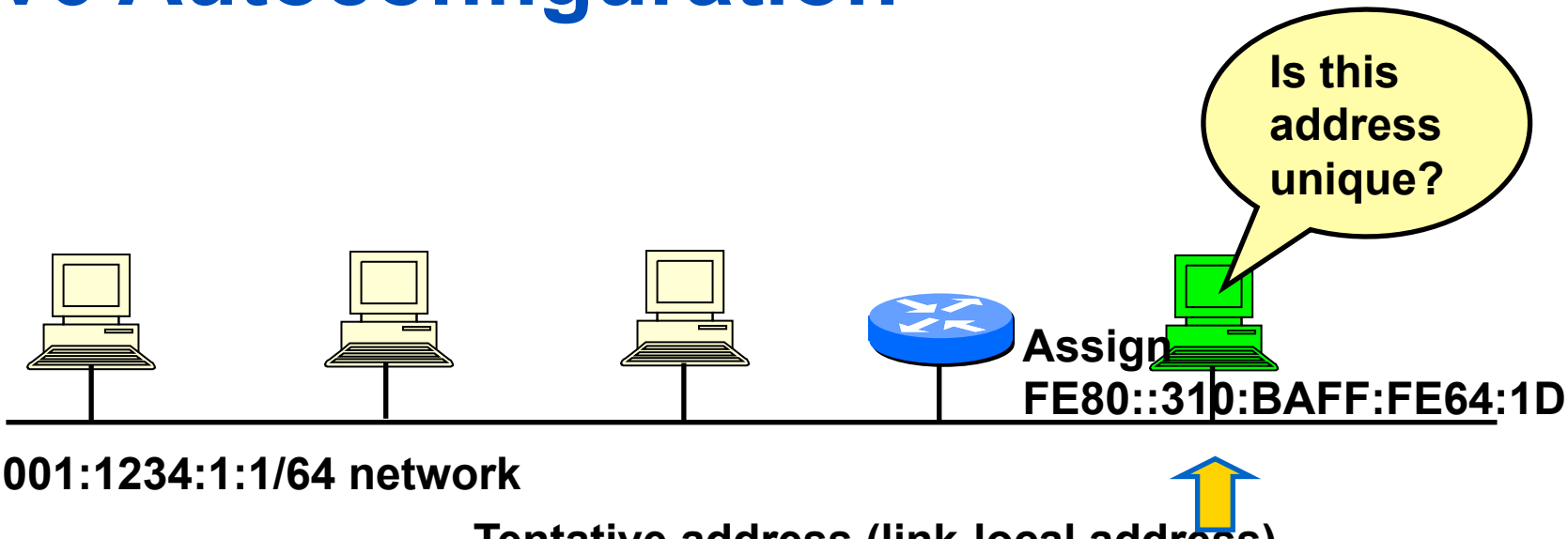
Interface ID

- 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

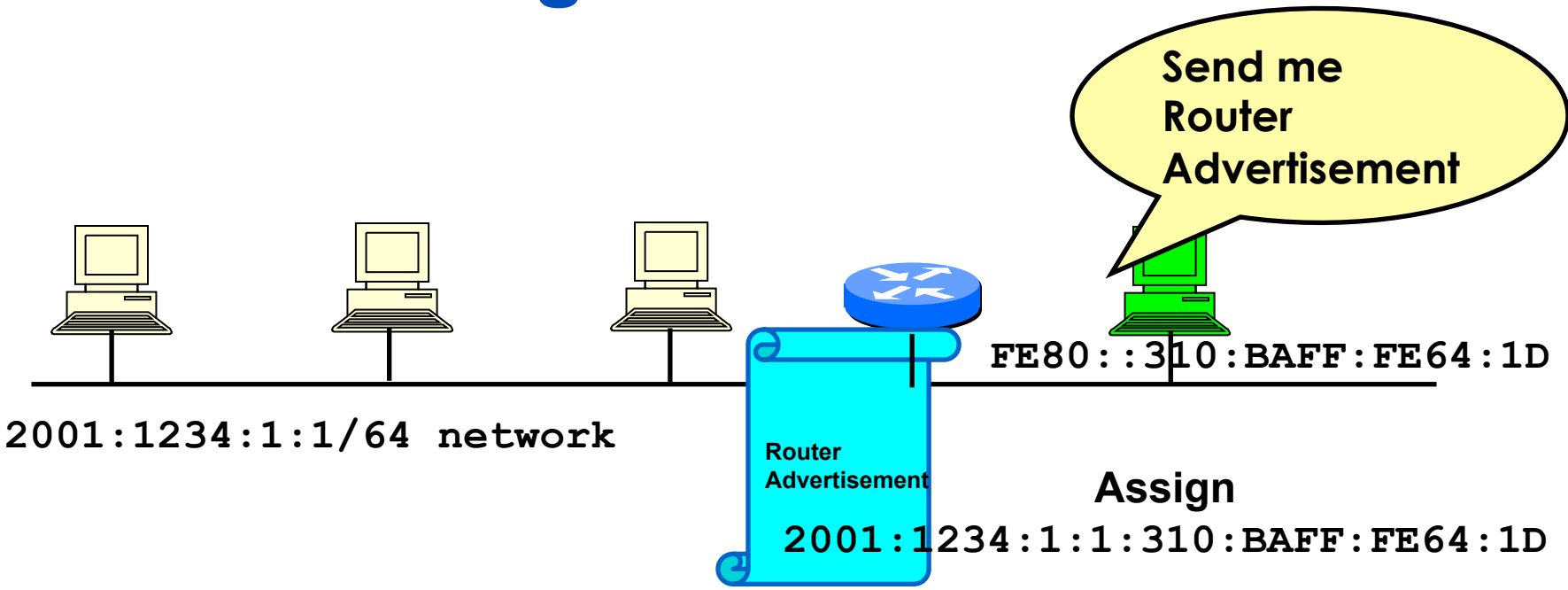

Mac Address
3 4
5 6
7 8
9 A
B C
D E
EUI-64 Address
3 4
5 6
7 8
9 A
B C
D E
0 0 1 1 0 1 0 0
U/L bit
0 0 1 1 0 1 1 0
F F
F E
Interface Identifier
36
5 6
7 8
F F
F E
9 A
B C
D E

IPv6 Autoconfiguration



1. A new host is turned on.
2. Tentative address will be assigned to the new host.
3. Duplicate Address Detection (DAD) is performed. First the host transmit
- a Neighbor Solicitation (NS) message to all-nodes multicast address (FF02::1)
5. If no Neighbor Advertisement (NA) message comes back then the address is unique.
6. FE80::310:BAFF:FE64:1D will be assigned to the new host.

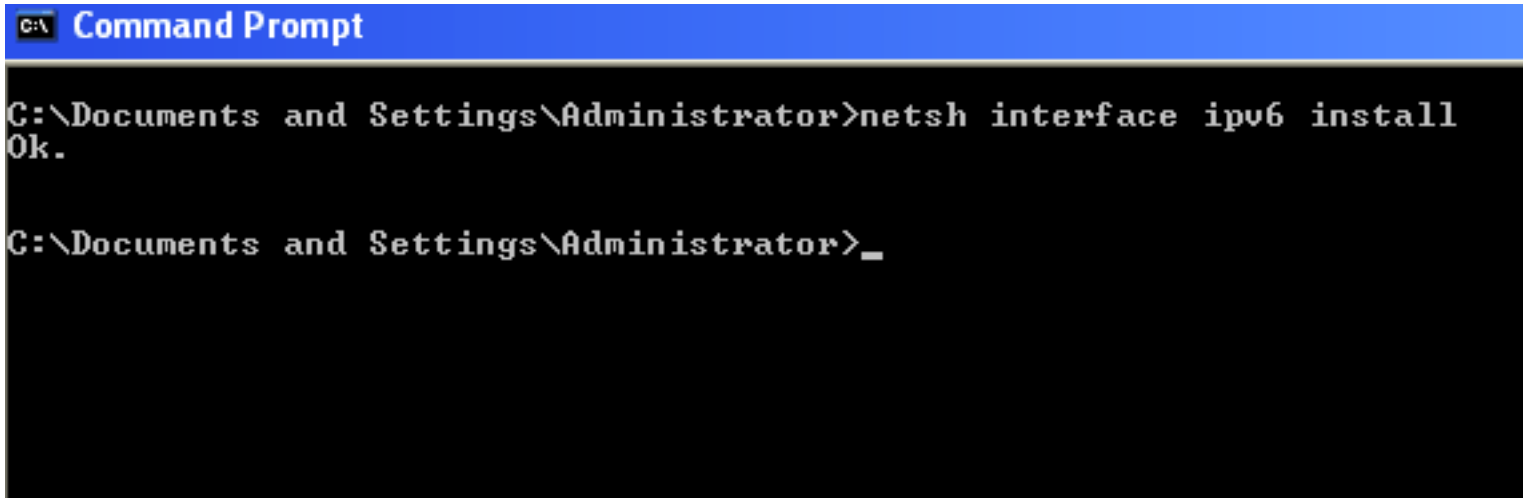
IPv6 Autoconfiguration



1. The new host will send Router Solicitation (RS) request to the all-routers multicast group (FF02::2).
2. The router will reply Routing Advertisement (RA).
3. The new host will learn the network prefix. E.g, 2001:1234:1:1/64
4. The new host will assigned a new address Network prefix+Interface ID E.g, 2001:1234:1:1:310:BAFF:FE64:1D

IPv6 Host Configuration (Windows)

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



IPv6 Host Configuration (Windows)

- Configuring an interface

```
netsh interface ipv6 add address "Local Area
Connection" 2406:6400::1
```

- Note: Prefix length is not specified with address which will force a /64 on the interface
- Verify your Configuration

```
c:\>ipconfig
```

- Verify your neighbour table
  - `C:\> netsh interface ipv6 show neighbors`

IPv6 Host Configuration (Windows)

- Disable privacy state variable

```
C:\> netsh interface ipv6 set privacy state=disable

OR

C:\> netsh interface ipv6 set global
randomizeidentifiers=disabled
```

IPv6 Host Configuration (Windows)

- Testing your configuration
  - `ping fe80::260:97ff:fe02:6ea5%4`

- Note: the Zone id is YOUR interface index

IPv6 Host Configuration (Linux)

- Enabling IPv6 on Linux
  - Set the NETWORKING_IPV6 variable to yes in /etc/sysconfig/network

```
# vi /etc/sysconfig/network
NETWORKING_IPV6=yes
# service network restart
```

- Adding IPv6 address on an interface

```
# ifconfig eth0 add inet6 2406:6400::1/64
```

IPv6 Host Configuration (Linux)

- Configuring Router Advertisement (RA) on Linux
  - Set IPv6 address forwarding on

    `# echo "1" /proc/sys/net/ipv6/conf/all/forward`
  - Need radvd-0.7.1-3.i386.rpm installed
  - On the demon conf file /etc/radvd.conf

    `# vi /etc/radvd.conf`

```
Interface eth1 {
        advSendAdvert on;
        prefix 2406:6400::/64 {
        AdvOnLink on;
        };
        };
```

IPv6 Host Configuration (FreeBSD)

- Enabling IPv6 on FreeBSD
  - Set the ipv6_enable variable to yes in the /etc/rc.conf

```
# vi /etc/rc.conf
ipv6_enable=yes
```

- Adding IPv6 address on an interface

```
# ifconfig fxp0 inet6 2406:6400::1/64
```

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.

Network Planning Essentials

APNIC

Hierarchical Network Design

- A network with different layers
  - Each level of the network has it own function
- Minimise costs
  - Avoid spending money to buy unnecessary features on equipment for each layer's requirements
  - Save bandwidth due to modularity of design
- Scalability is the major goal
  - Fast convergence
  - Route summarisation

Disadvantages of a Flat Network

- Designed for small networks
  - Easy to design and maintain as long the network stays small
- No hierarchy
- All networking devices have the same jobs
- No layer divisions

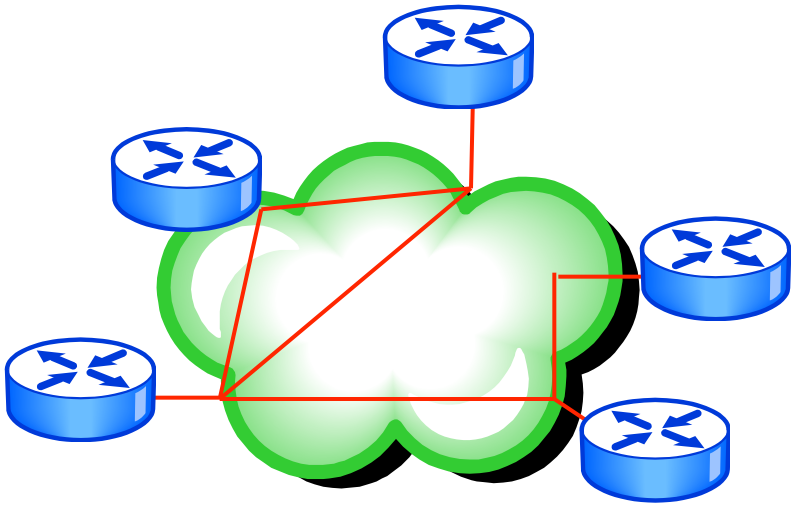
Partial Mesh vs Full-mesh Topology

- Network designers recommend mesh topology

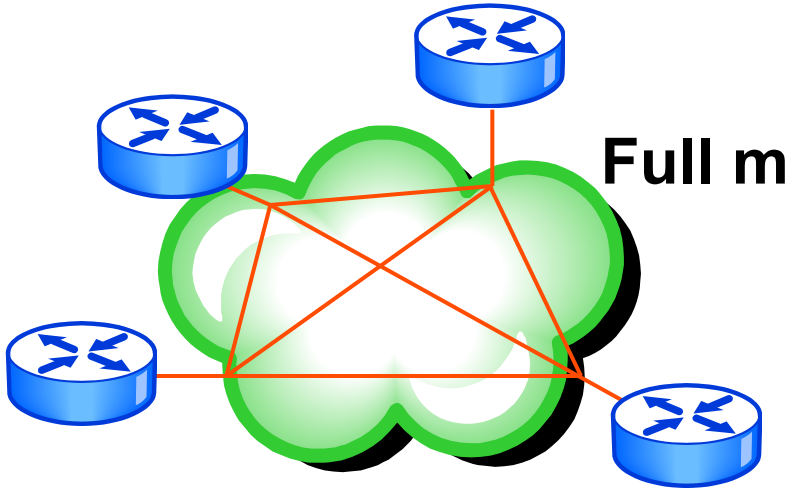
- Good performance and provides redundancy
  - Partial mesh topology
    - Has fewer connections
    - Each router may require direct connection from an intermediate link to get to another device
  - Full-mesh topology
    - All routers are connected to each other to offer good performance

Formula for full-mesh = (N x (N – 1))/2

Mesh versus Full-mesh Topology

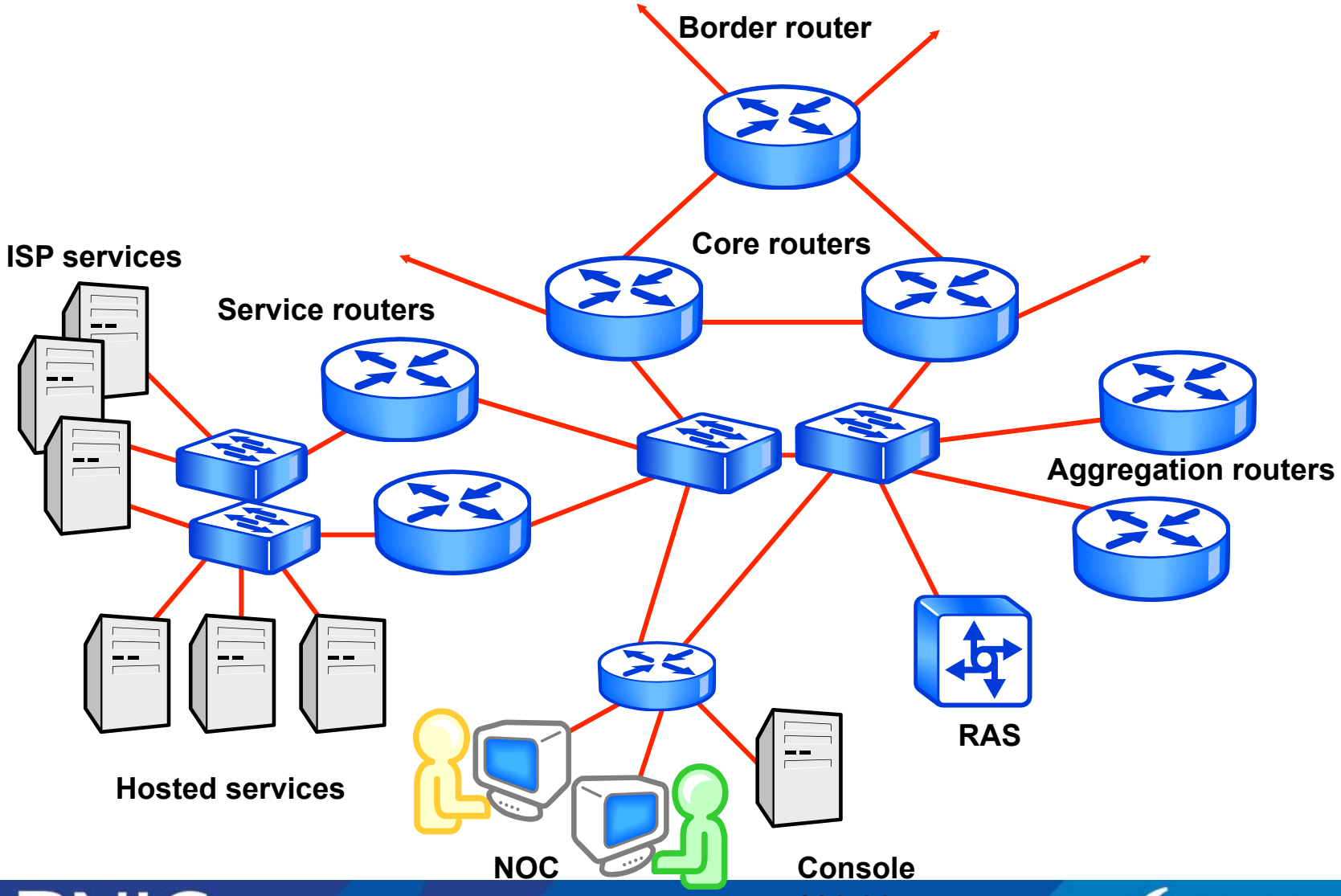


Partial mesh



Full mesh

Simple Network Plan



Border Router

- Provides connectivity to the rest of the Internet service providers in the world
- Protects the ISP network and the customers networks from the Internet
- Critical and should be correct because this is the main reason for the business connection

Core Router

- Critical for connectivity; it should be designed to have a redundant component

- When configurating this router:
  - Enable routing feature for optimised packet throughput
  - Avoid using filtering which will slow down manipulation of packets
  - Avoid usage of routing policy for filtering purposes

- Should be high-speed to switch packets easily and faster

Aggregation Router

- Aggregation or gateway router for connecting fixed line customers
- Improves routing protocol performance
- Allows summarisation of routes from an aggregated address
- Allows configuration of routing policy for customers network announcements

Services Router

- Used for services provided to customers
  - DNS, email, news
  - Hosted services (content provided)
    - Web, email, DNS
- Configured by default to have filters to allow only authorised users
- Routers with firewall features are often used as a firewall itself
- Protect the core services provided by the ISP

NOC Router

- Connects ISP essential services
  - Syslog, TACACS+, RADIUS, primary DNS

- Operations engineer network
  - Trouble isolations
  - Network monitoring
  - Research network testing
  - Staging area (option)

Access Router

- Routers designed to provide access services
  - Cable services (on demand)
  - DSL on demand service
  - Wireless services (Wifi) etc.

- Connections to this network requires proper authentication credentials

Out-of-band Console Server

- Can be typical router that has Async port configured for out-band access
- Allows remote access of routers without using the in-band network
- Access to routers through its console port
- Utilises a different network
  - Not affected if the in-band network is down
  - Only small bandwidth usage is required

Principles of Addressing

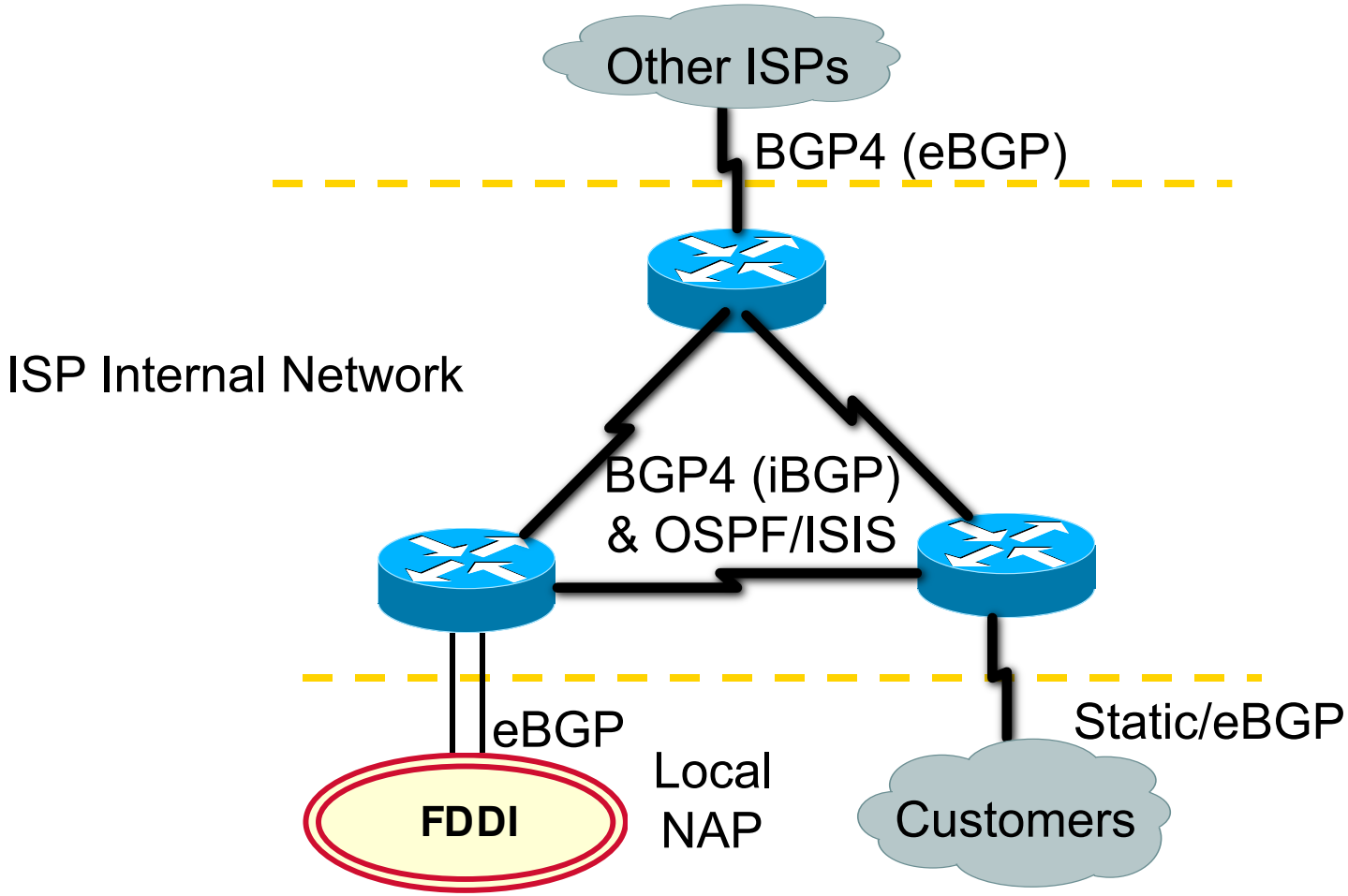
Separate customer & infrastructure address pools:

- Manageability
  - Different personnel manage infrastructure and assignments to customers
- Scalability
  - Easier renumbering
    - customers are difficult
    - infrastructure is relatively easy

Principles of Addressing

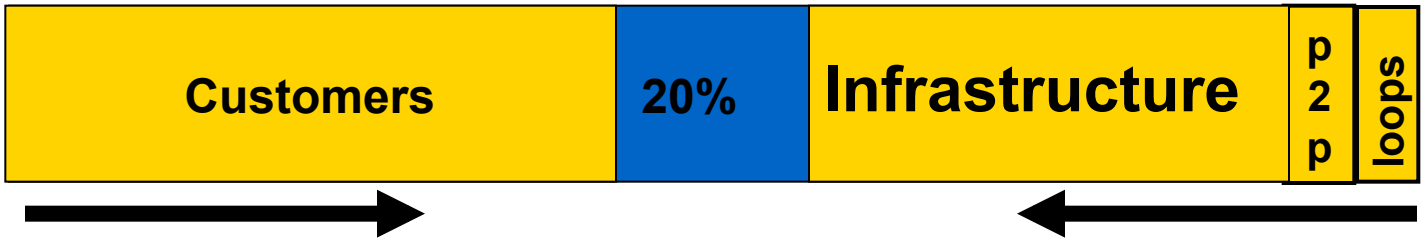
- Further separate infrastructure
  - ‘Static’ infrastructure examples
    - RAS server address pools, CMTS
    - Virtual web and content hosting LANs
    - Anything where there is no dynamic route calculation
- Customer networks
  - Carry in iBGP , do not put in IGP
    - No need to aggregate address space carried in iBGP
    - Can carry in excess of 100K prefixes

Hierarchy of Routing Protocols



Management – Simple Networks

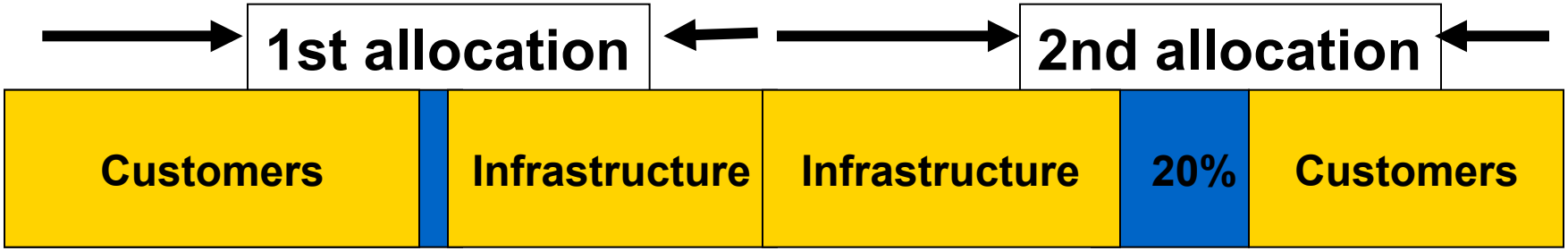
- First allocation from APNIC
  - Infrastructure is known, customers are not
  - 20% free is trigger for next request



  - Grow usage of blocks from edges
  - Assign customers sequentially

Management - Simple Network

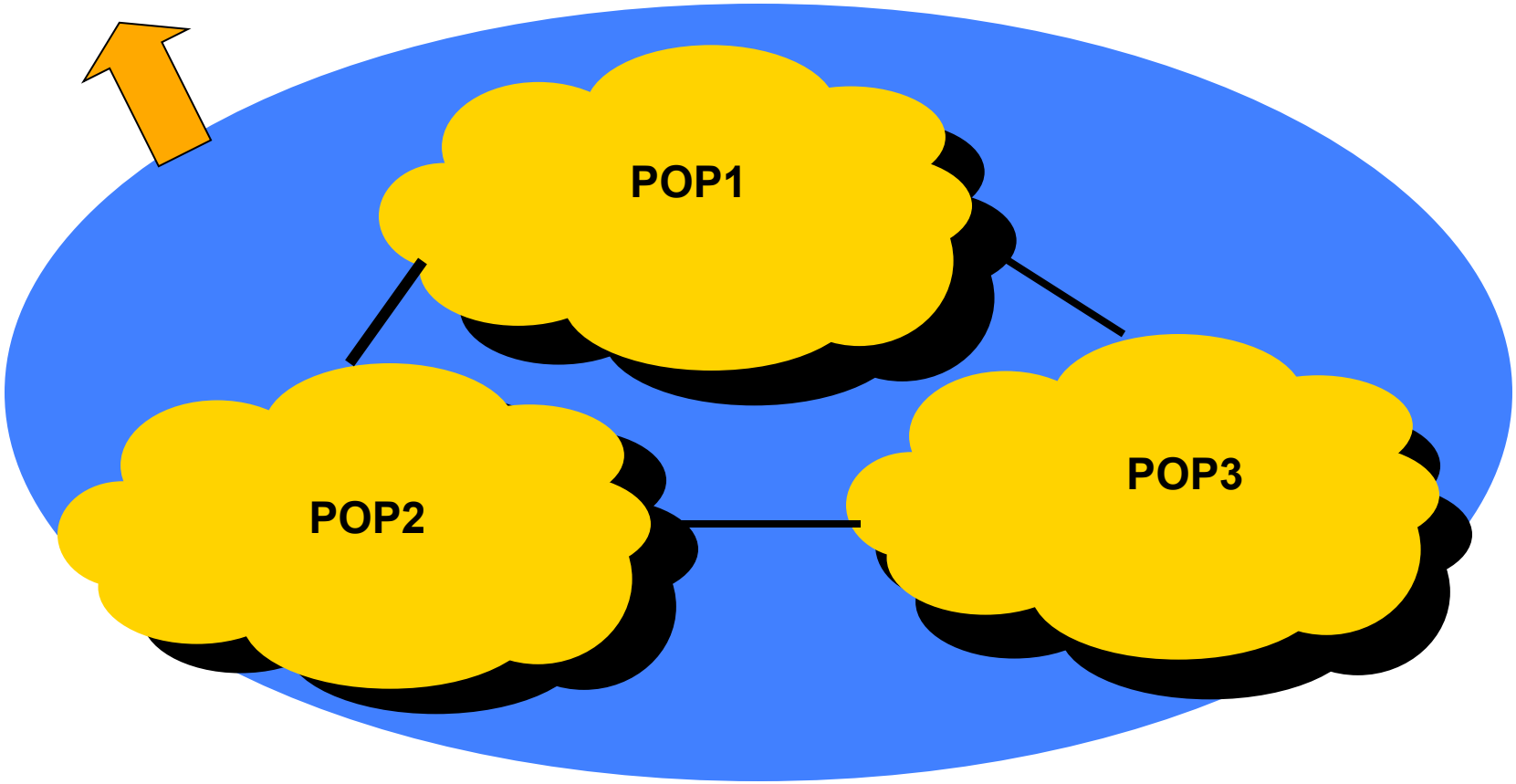
- If second allocation is contiguous



  - Reverse order of division of first block
  - Maximise contiguous space for infrastructure
    - Easier for debugging
  - Customer networks can be discontiguous

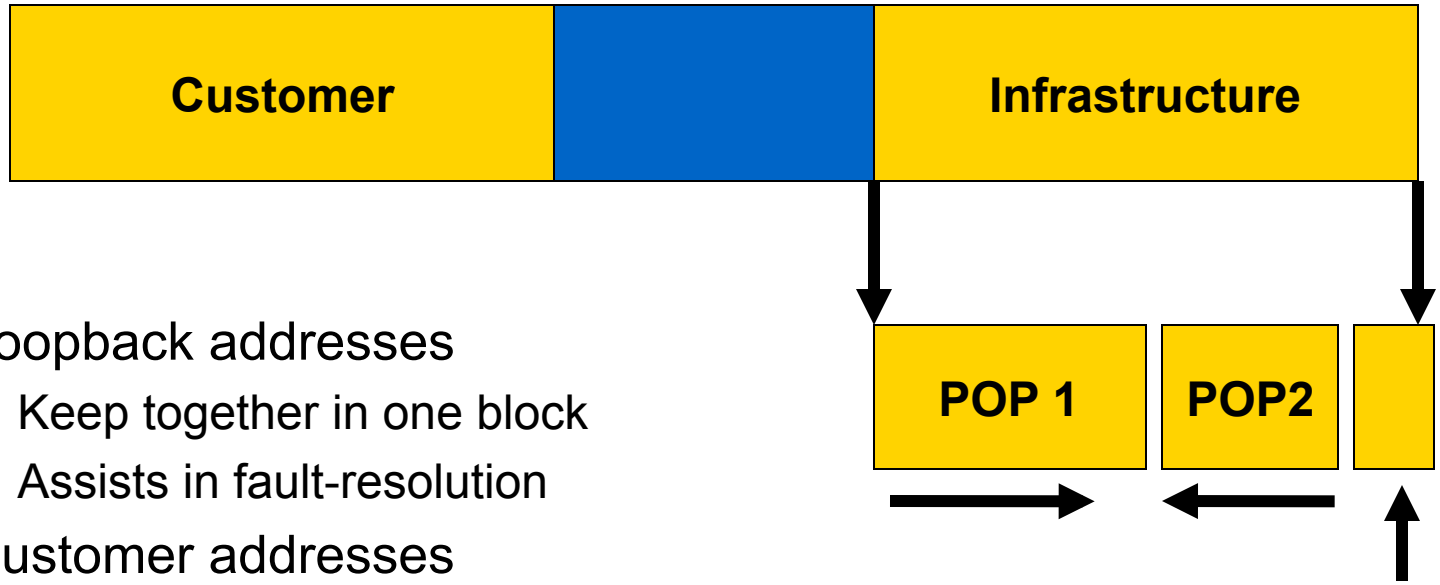
Management - Many POPs

- WAN link to single transit ISP



Management - Many POPs

- POP sizes
  - Choose address pools for each POP according to need



  - Loopback addresses
    - Keep together in one block
    - Assists in fault-resolution
  - Customer addresses
    - Assign sequentially

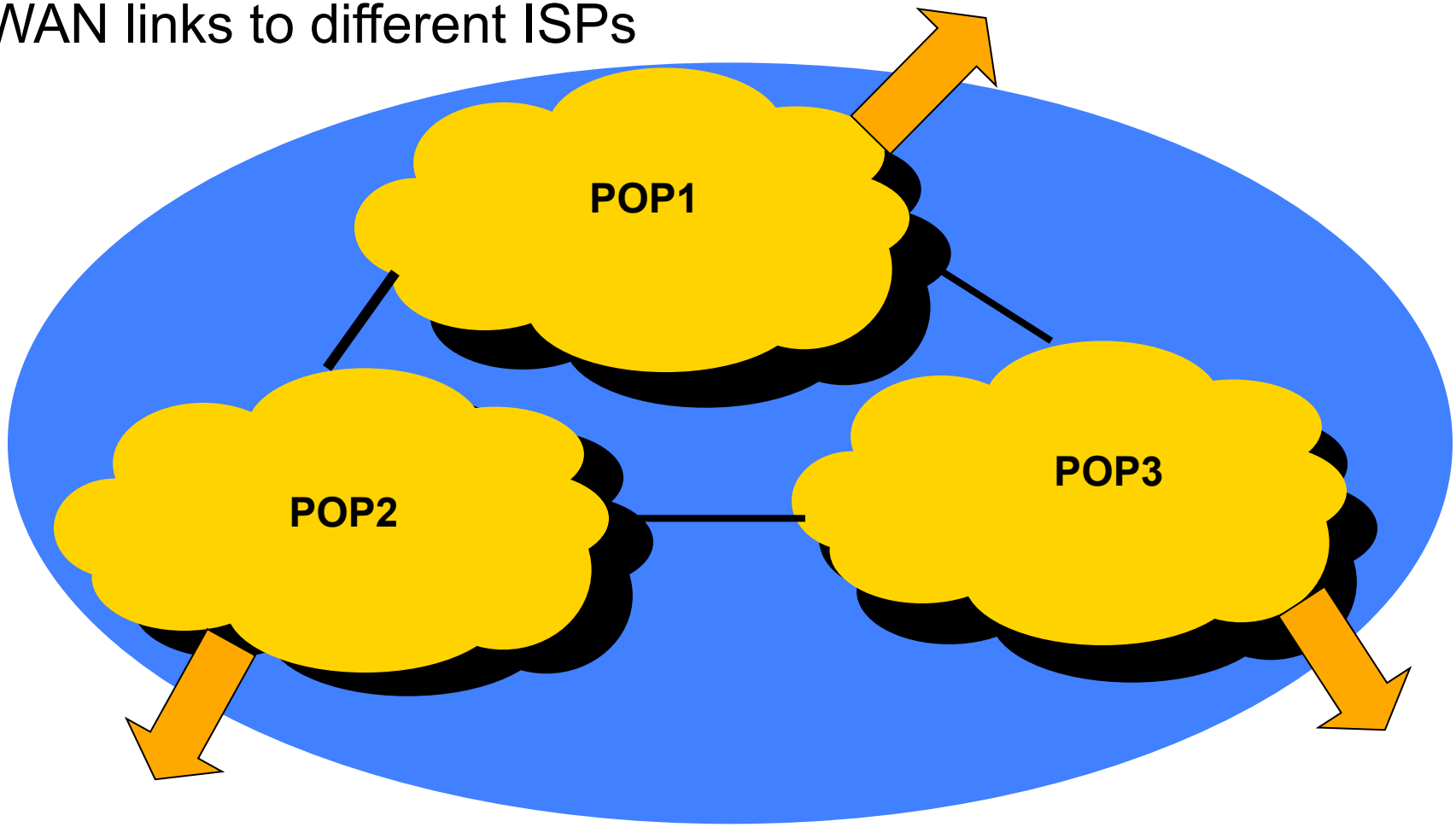
loopbacks

Management - Many POPs

- Minimum allocation not enough for all your POPs?
  - Deploy addresses on infrastructure first
- Common mistake:
  - Reserving customer addresses on a per POP basis

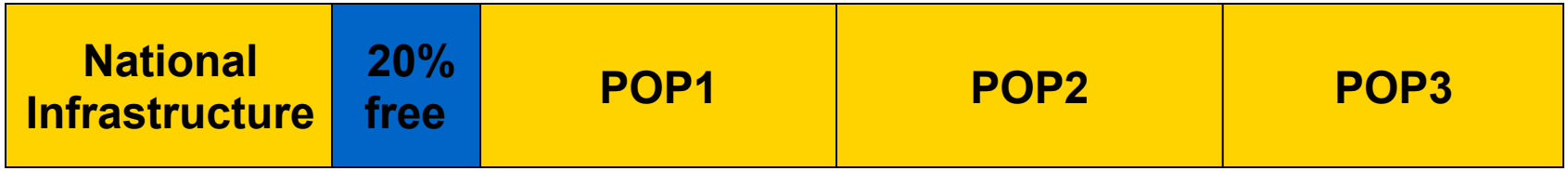
Management – Multiple Exits

- WAN links to different ISPs



Management – Multiple Exits

- Create a ‘national’ infrastructure pool



  - Carry in IGP
    - Eg. loopbacks, p2p links, infrastructure connecting routers and hosts which are multiply connected
  - On a per POP basis
    - Consider separate memberships if requirement for each POP is very large from day one.

Router Overview

APNIC

What is a Router?

- A device in the network that processes and routes data between two points
- A device that routes data between networks using IP addressing
- A layer 3 device
- Hardware or software used to connect two or more networks

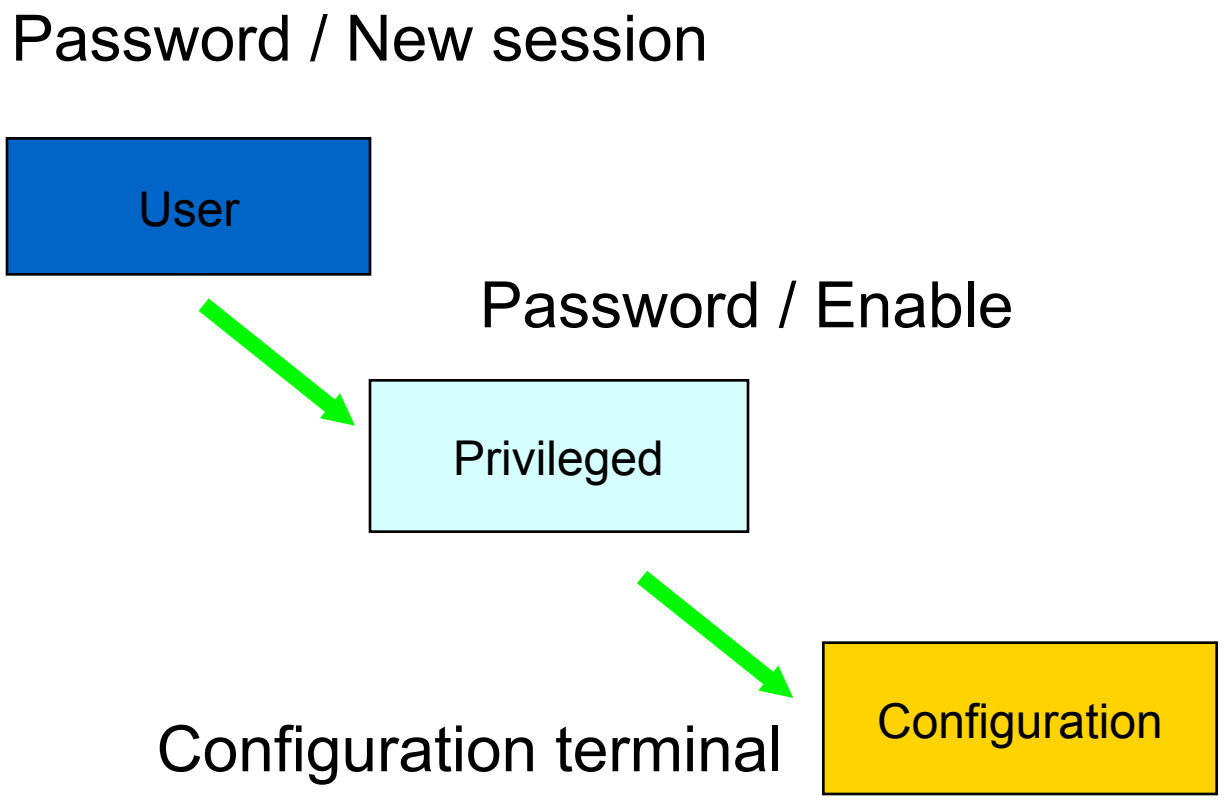
Router Basics

- Operating systems
  - IOS (Cisco)
  - Free BSD base (Juniper)
  - Quagga / Quagga (UNIX or LINUX)

- Several interfaces
  - Ethernet/Fast Ethernet, Serial, Gigabit port, Management port

- Management Interfaces
  - GUI based (web)
  - Command line interface (CLI)

Router Modes



Router Modes

- User mode
  - Check the router status and operation
  - Configuration is not visible
  - Prompt = ***router>***

- Privileged mode
  - Allows complete control to the router
  - Does not allow alteration of configuration
  - Prompt = **router#**

- Configuration mode
  - Mode to change configuration settings
  - Full control of the router configuration
  - Prompt = **router(config)#**

Router Configuration Mode

- Configuration
  - Active configuration
    - ***show running-config***
  - Startup configuration
    - ***show startup-config***

Router Components

Read Only Memory (ROM) chips:

- ROM Monitor (bootstrap program)
  - Firmware that runs when the router is boot up or reset
- Certain tasks can be done using the ROM monitor
  - Password recovery option
  - Downloading the software image using the management port
- Runs if there are no software images available on the router (with early model routers)

Router Components

Flash Memory

- Stores the software image of the router
- Usually built into the router
- Some vendors also provide external flash memory card or disk

- Allows update of router software image with less interruption of service
  - Image can be upgraded without affecting the existing image running in the router
  - Install the software then instruct the router to boot the new image after the next boot

- Allows the router to load other information
  - Router logs
    - Crash information of the router
    - Debug information

Router Component

Non-Volatile RAM (NVRAM)

- Stores the existing running configuration
- Router start-up boot configuration

- Tiny memory size

- Stored configuration is very important
  - Upon router reboot / shutdown
  - Because RAM information is lost during reboot and shutdown

Router Component

Random Access Memory (RAM)

- Stores the current working configuration
- Handles the tables and buffers
- Non-permanent memory

- Broken down into two main areas
  - Main processor memory
    - Stores entry for the routing table, ARP table, and current running configuration
  - Shared processor memory
    - Buffer location for temporary stored packets for process

Router Configuration Requirements

- In configuring a router we need to address the following requirements.
  - Security
  - Manageability
  - Accessibility

Security Requirements

- To secure the router, the setup should enable the following:
  - Provide names to your router
  - Banner information
  - Configure password for the router
  - Access with privilege per user
  - Authentication and Authorisation
    - Locally configured
    - Remote server access (TACACS/RADIUS)
  - Access filters policy
  - Enable logging for auditing
  - Disable unnecessary services running

Disable Unused Access and Services

- Disable http servers running if not in use
  - http and secure http server
- Disable discovery protocol
  - CDP (Cisco)
- Disable services which can be used for reconnaissance attempts
  - Ip source-route, finger, boot server, domain-lookup, service pad

Accessibility Requirements

- Be able to manage the routers properly
  - Enable console and VTY line to
    - Allow access to the router
      - With specific host only (using filters)
    - Enable the use of privileges access
  - Provide the use of out-of-band management (console access)
  - Setup a centralised management console to control all devices