Global Networking Migration to IPv6 Using MikroTik ROS

By : Ali Sami & Haidar Fadeel

March-2013 Zagreb

About :

Ali Sami : 12 years active in Data networking , Mikrotik Authorize trainer sine April 2011(MTCNA-MTCTCE-MTCWE-MTCRE-MTCINE Certified)
Specialist : Firewalling , Wireless , Routing , Network Management , QoS

Haider Fadeel : 5 years active in Data Networking Mikrotik Certified trainer since August 2012 (MTCNA – MTCTCE – MTCRE certified)
Specialist : Routing , Firewalling , Network Management

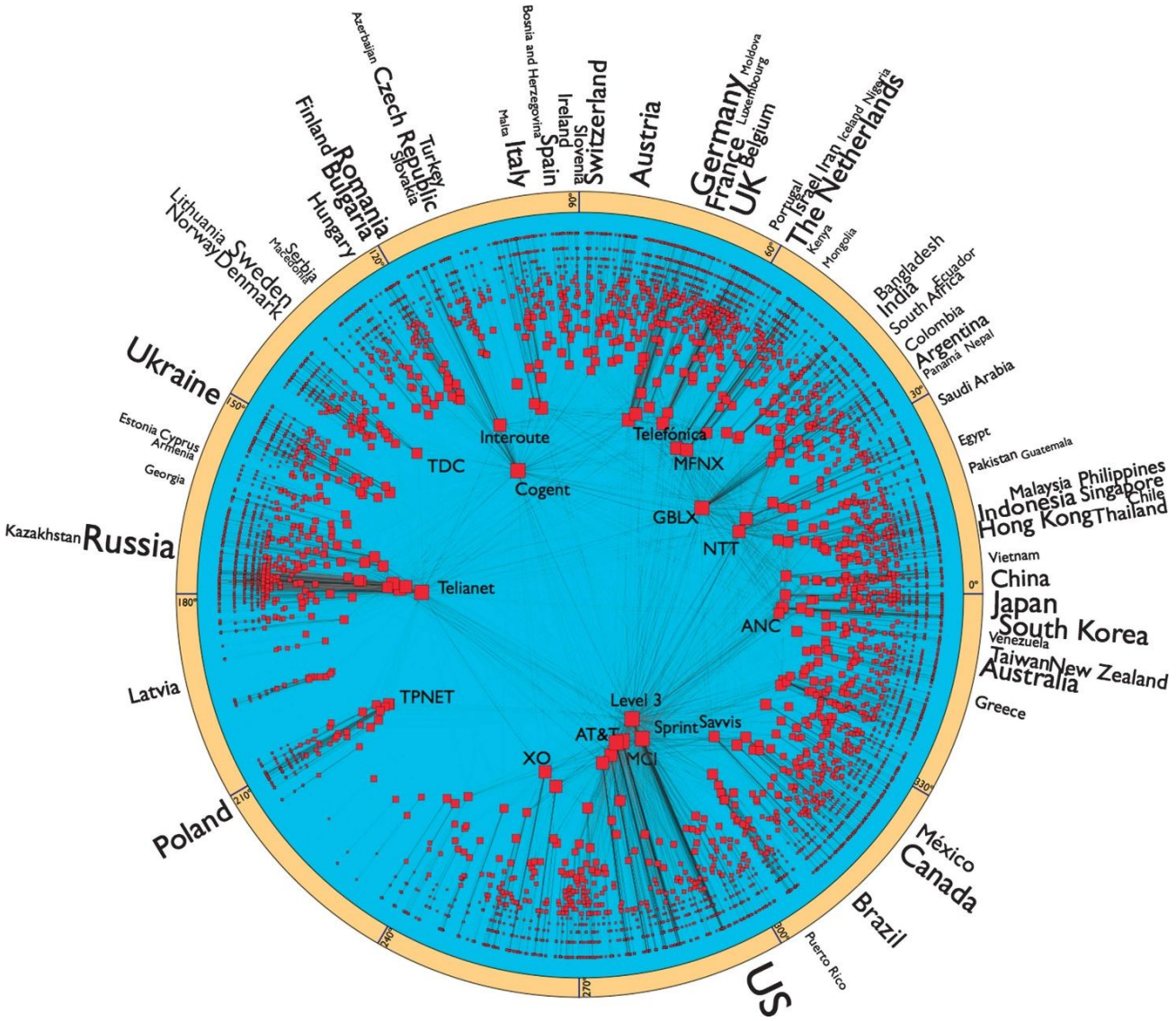
Objectives

- Autonomous systems & Connectivity design.
- Global connectivity scenario and solution over view.
- Implementation Enterprise Networking using MikroTik ROS.
- OSPF / MPLS / iBGP / eBGP in action.
- Testing the connectivity using traceRoute and ping tool.

Objectives (cont.)

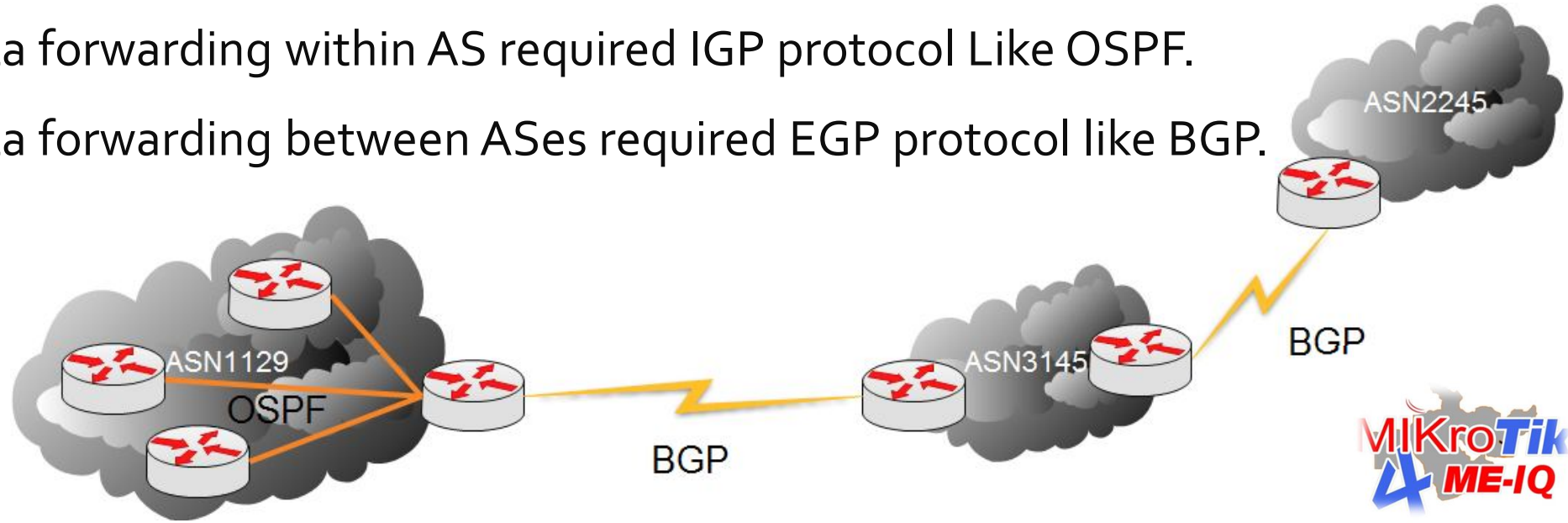
- IPv6 Global subnet distribution.
- Migration method
- Dual stack addressing.
- PtP addressing.
- OSPFv3 over view and configuration.
- BGP-MP over view configuration.

Autonomous system (AS)

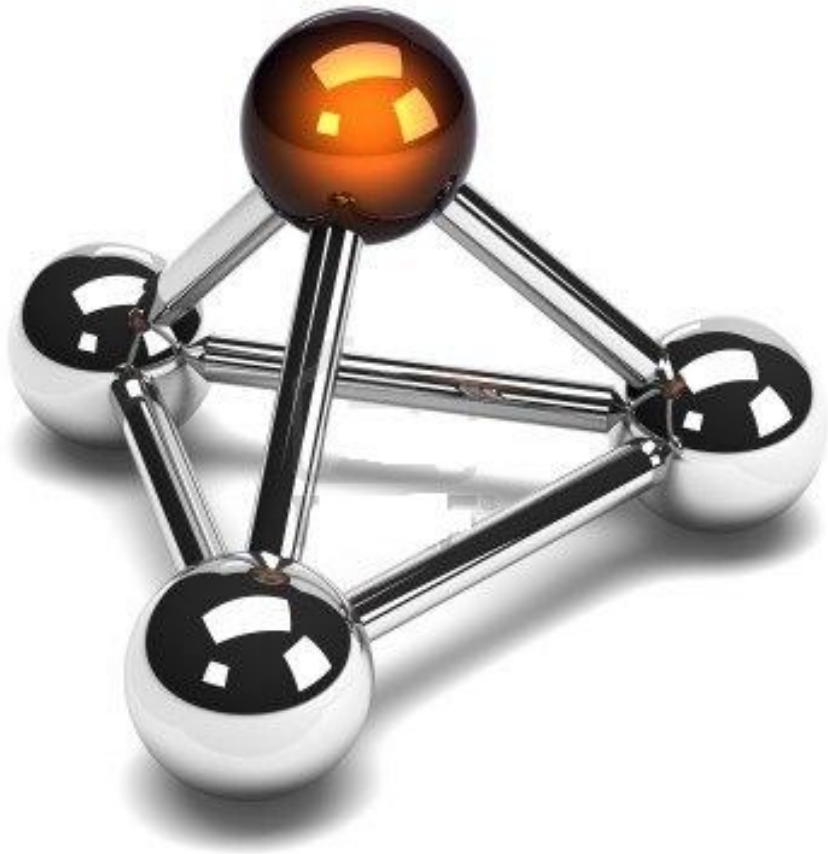


Autonomous System.

- Is a collection of networks that are controlled by single entity like ISP or very large organization.
- Identified by Number 1- 65535. (16 bits until 2007)
- 32 bit AS number has been Introduced.
- Data forwarding within AS required IGP protocol Like OSPF.
- Data forwarding between ASes required EGP protocol like BGP.

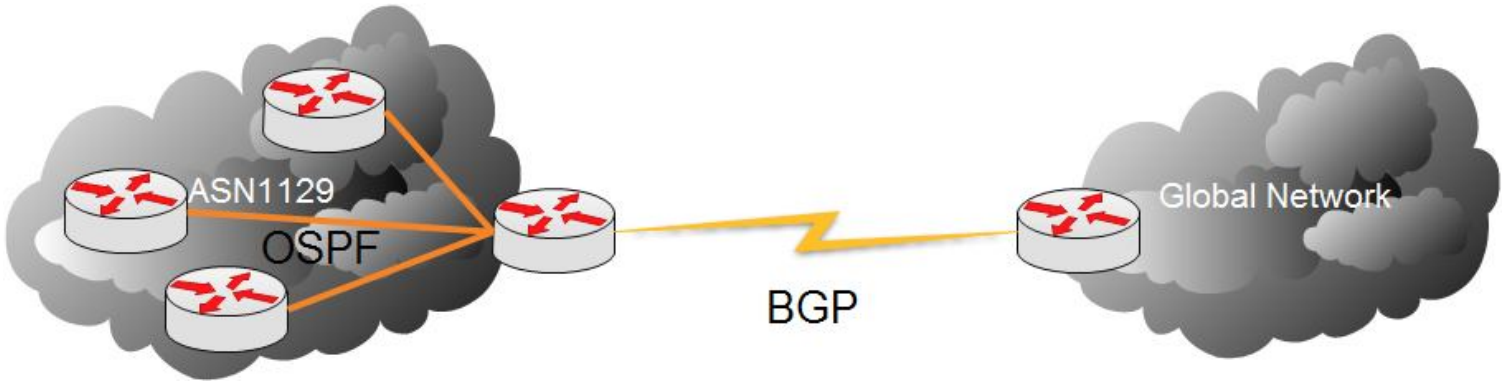


Autonomous Systems
&
Connectivity



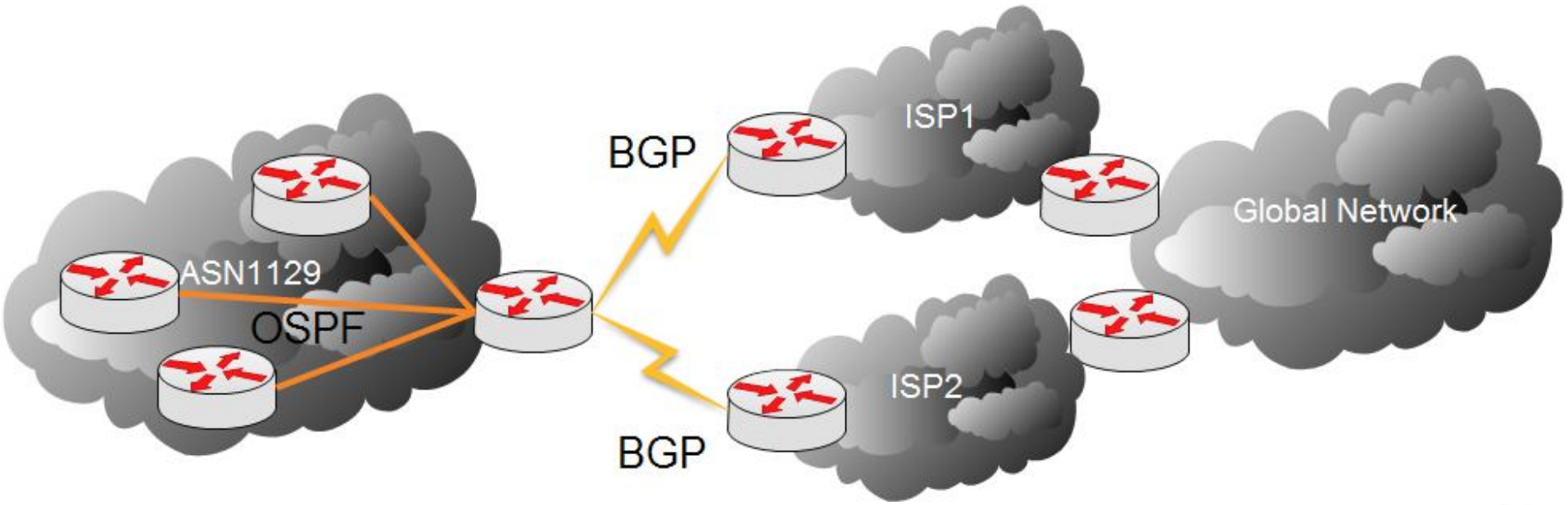
Single Homed

- Single link between ISP and enterprise.
- Only one possible next-hop router, used as Default route.



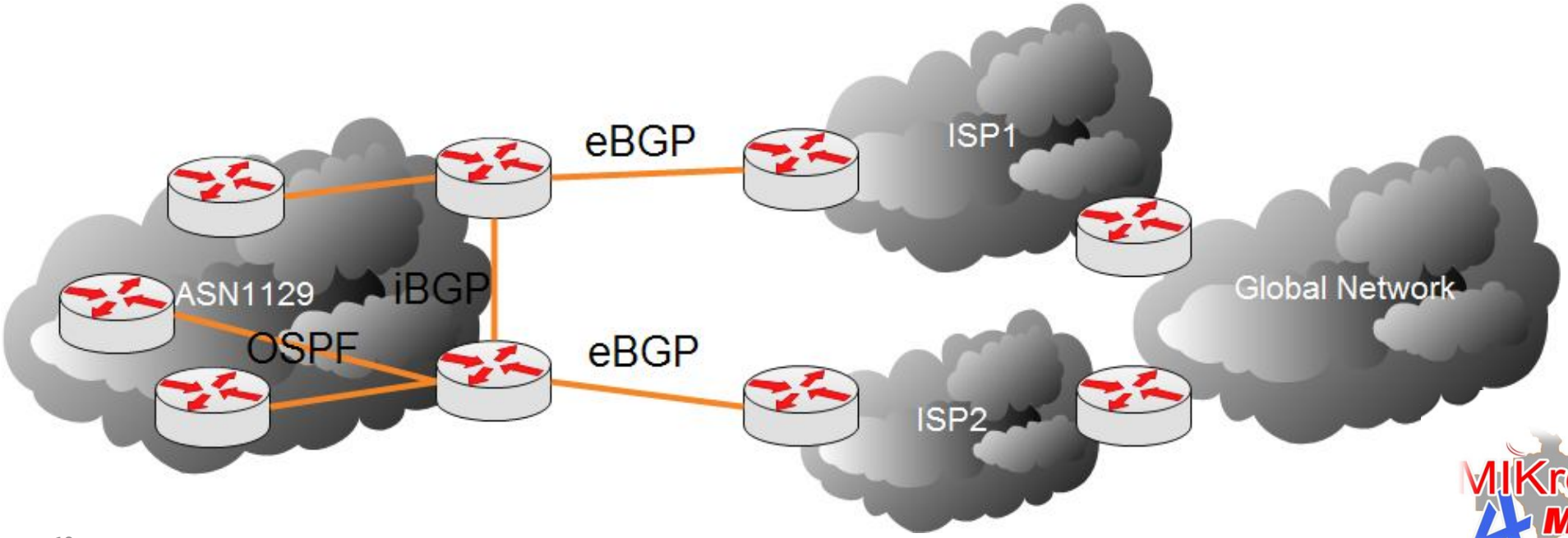
Single Multi Homed

- Required, When there is two ore more connections to Global Network.
- Single link per each ISP.



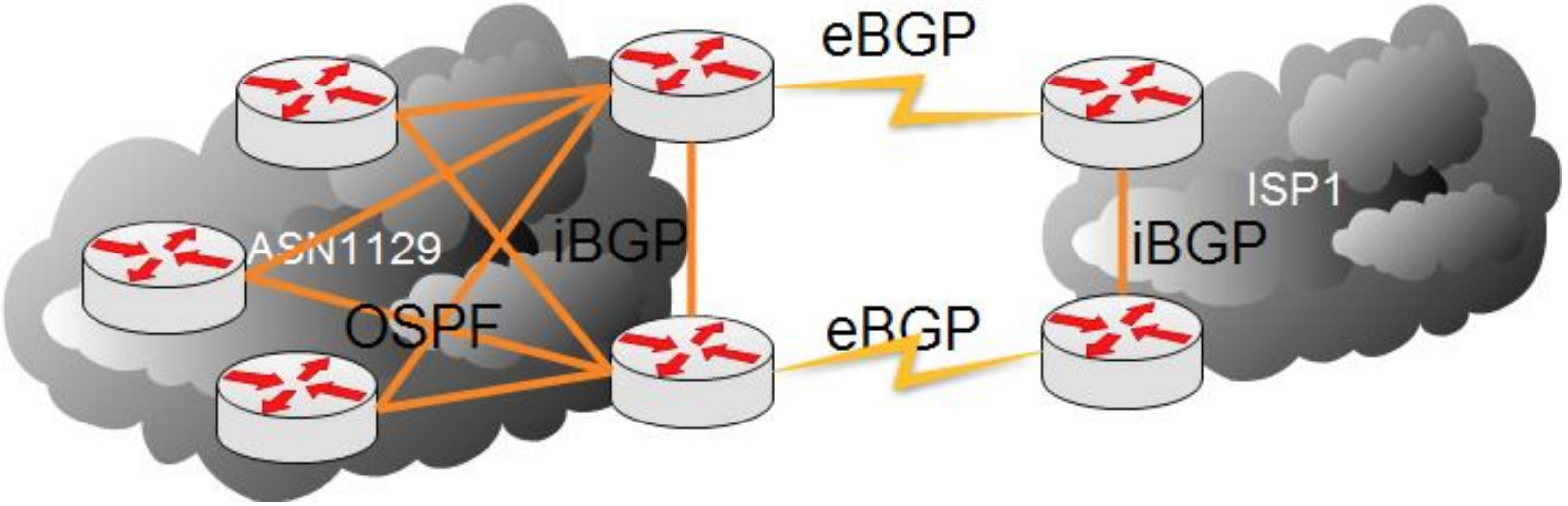
Single Multi Homed (cont.)

- Can use multi routers at ISP to connect to other ISPs.
- Redundancy for up stream and down stream.
- load balancing Per connection for up stream and down stream



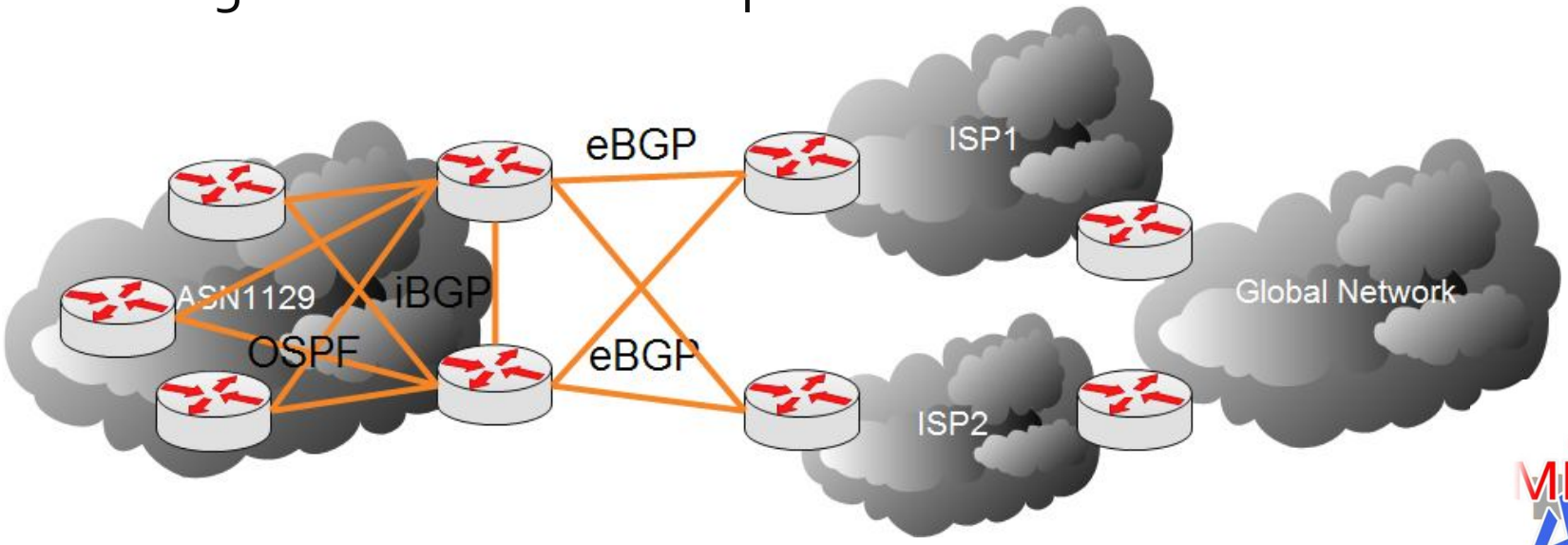
Dual homed.

- Connection to Global Network via single ISP.
- Multiple link to remote ISP.
- Can use a pair of routers.
- Redundancy and load balancing per Link.

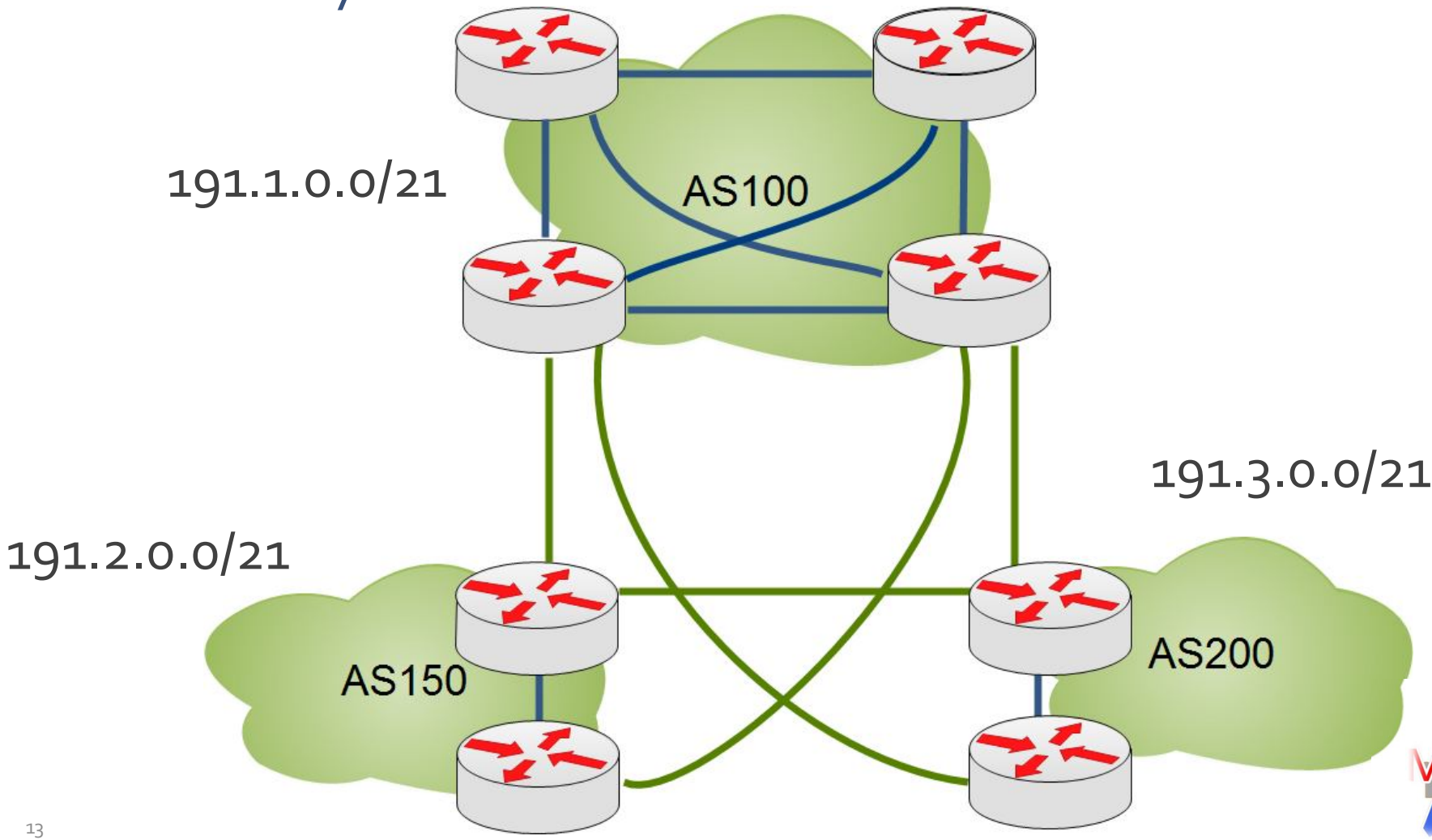


Dual Multihomed

- Required, when there is two or more connections to Global Network.
- Multiple link to each ISP.
- Can use multi routers.
- load balancing Per connection for up stream and down stream



Connectivity Scenario



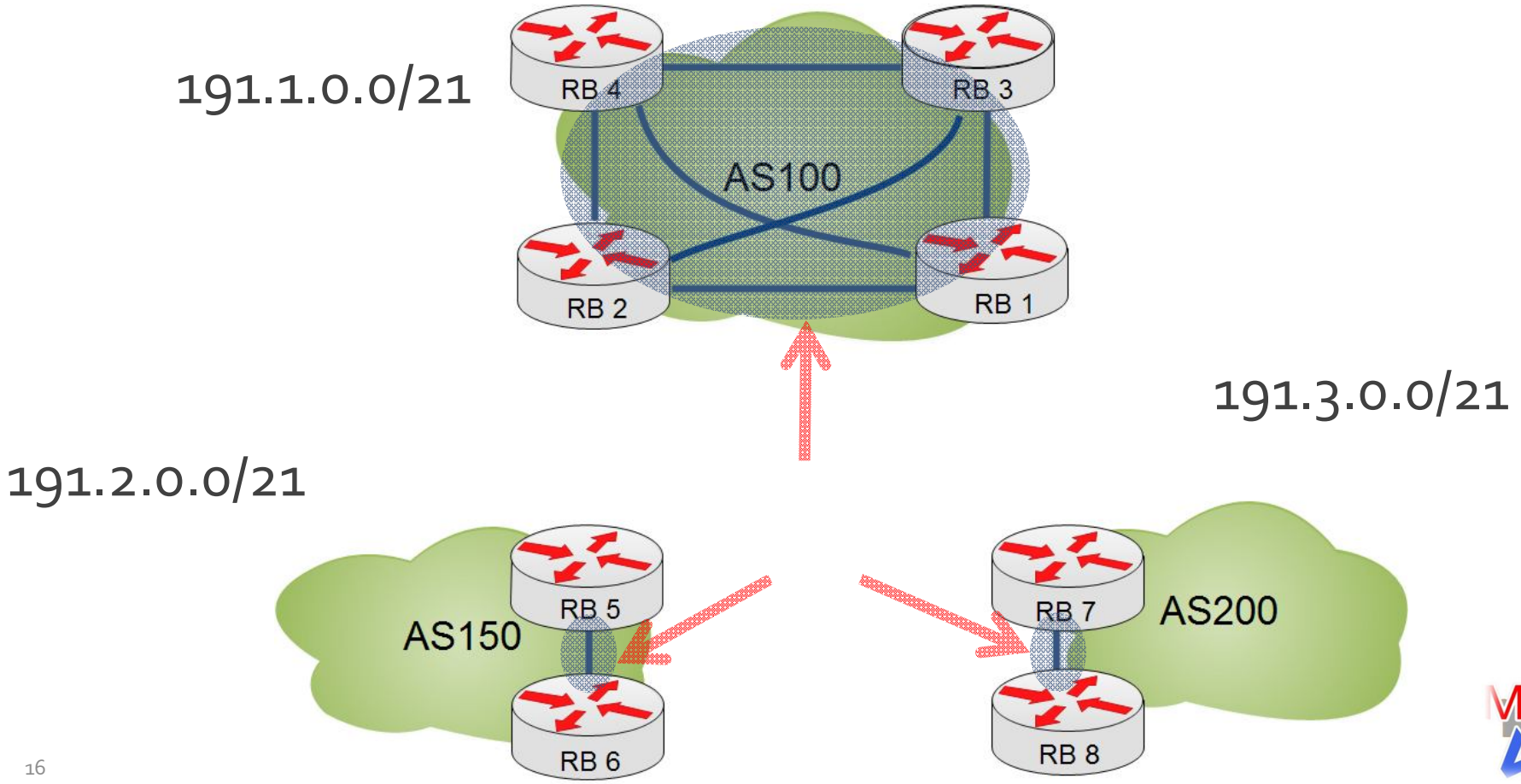
Scenario Design

- Full Mesh connectivity between Core routers.
- Data carrier between network within AS will be OSPFv2.
- Core level forwarding using MPLS.
- iBGP and eBGP for global data forwarding.
- Dual multi homed connectivity between ASes.

Advantage of Design

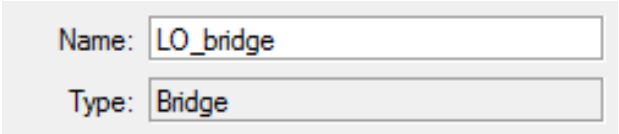
- Mesh will provide full redundant connectivity at core level.
- IGP will provide full IP level connectivity between Networks within AS.
- MPLS will increase forwarding performance between core routers.
- iBGP to select best path to access Global network through multi connections.
- IGP will help to keep iBGP peers away of network change.?
- Dual multi homed for eBGP will provide full redundant connectivity between ASes.

Configuration steps :
IP level connectivity & Internal routing protocol

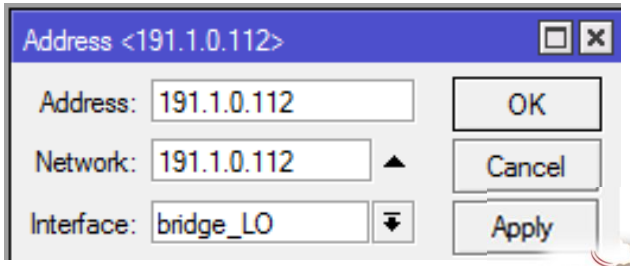


Configuration steps :
IP level connectivity & Internal routing protocol (cont.)

- Adding IP address on each connected interface
  - ✓ recommended /30 for P2P connectivity
- Add loopback (Lo) Interfaces on routers by using bridge interface as logical interface.



- Adding IP address on loopback interface.
  - ✓ This IP will be use for MPLS and iBGP peers

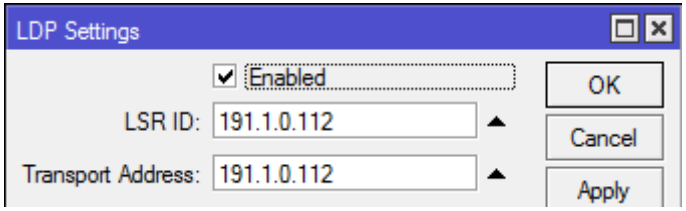


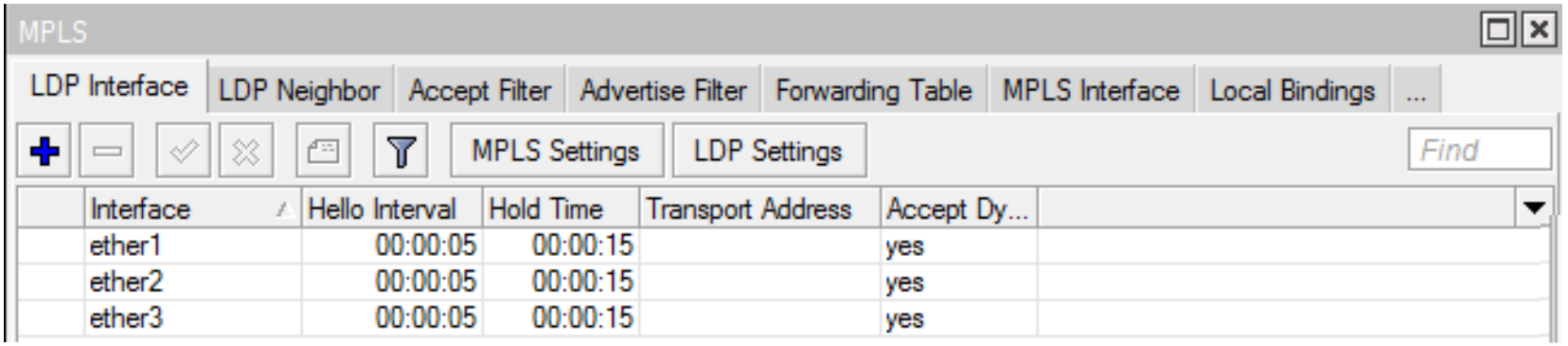
Configuration steps :
IP level connectivity & Internal routing protocol (cont.)

- Enable OSPF routing protocol to achieve IP level connectivity between Networks within AS.
  - ✓ Router ID will be IP of Loopback interface.
  - ✓ All internal router join under backbone area.
  - ✓ add proper network in the OSPF network .

Configuration steps :
IP level connectivity & Internal routing protocol (cont.)

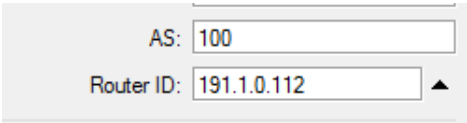
- Enable MPSL to increase forwarding performance at core level.
  - ✓ Use loopback IP address at LSR-ID and transport address.
  - ✓ connected interface to the internal network added as LDP interface.





Configuration steps :
IP level connectivity & BGP routing protocol

- Configure BGP instances



- Establish multi iBGP peering between internal routers
  - ✓ Multi peer will achieve mesh connectivity between internal router.

Name	Instance	Remote Address	Remote AS	Multihop	R...	TTL	Remote ID	Uptime	Prefix Co...	State
peer-RB1	default	191.1.0.111	100	yes	no	d...	0.0.0.1	01:40:11	3	established
peer-RB3	default	191.1.0.113	100	yes	no	d...	0.0.0.3	01:40:11		established
peer-RB4	default	191.1.0.114	100	yes	no	d...	0.0.0.4	01:40:12		established

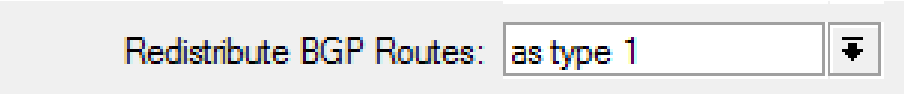
Configuration steps :
IP level connectivity & BGP routing protocol (cont.)

- Establish eBGP peers between AS Border routers (ASBRs).

Name	Instance	Remote Address	Remote AS	Multihop	R...	TTL	Remote ID	Uptime	Prefix Co...	State
peer-RB5	default	10.4.1.2	150	no	no	d...	5.5.5.5	01:42:19	2	established
peer-RB8	default	10.3.1.2	200	no	no	d...	8.8.8.8	01:42:19	2	established

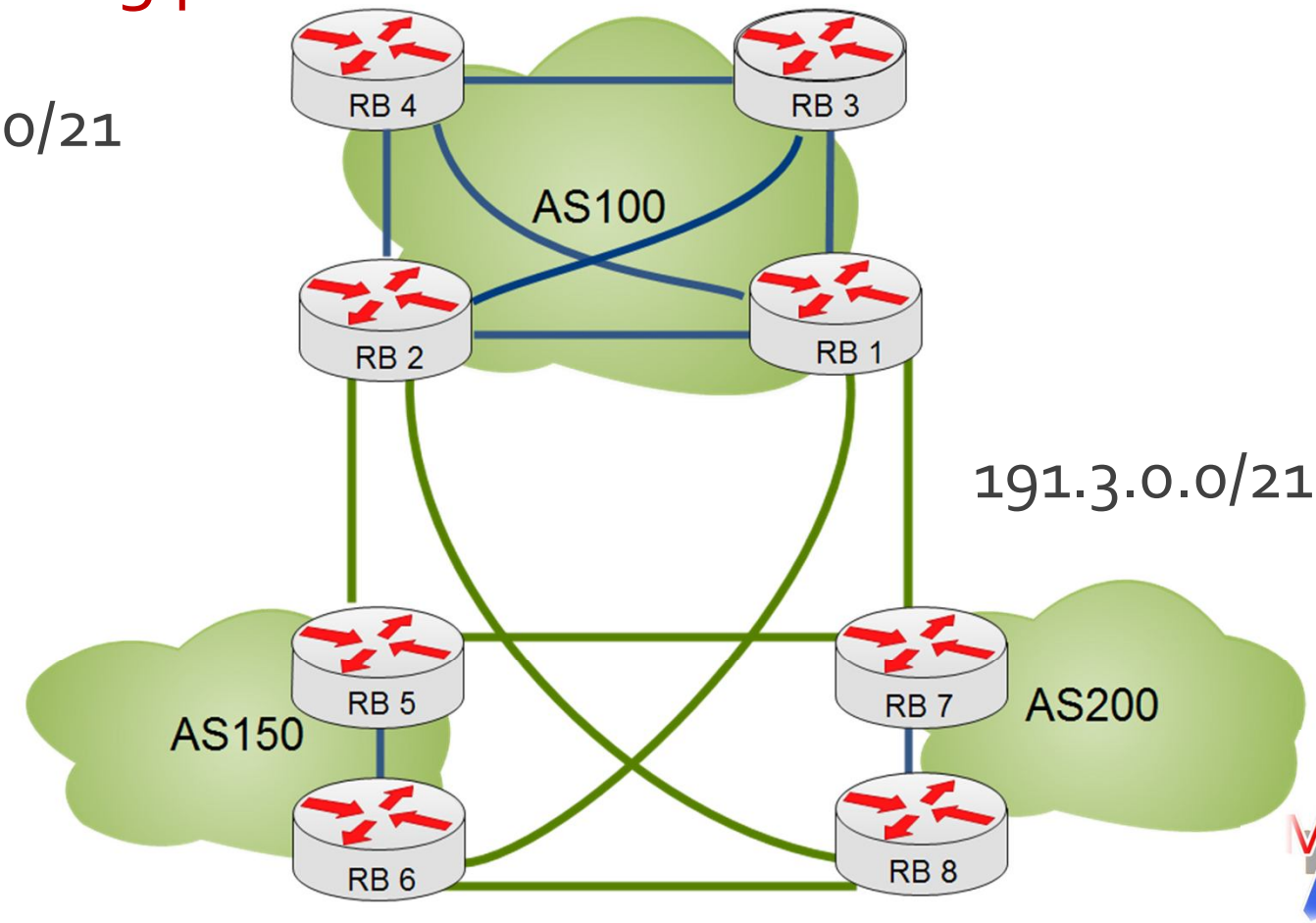
- Adding proper Networks that need to be advertised through eBGP peers.

- Enable received eBGP updates to redistribute into OSPF data base.
  - ✓ This will provide possibility for internal networks to connect to external networks.



Configuration steps :
External routing protocol

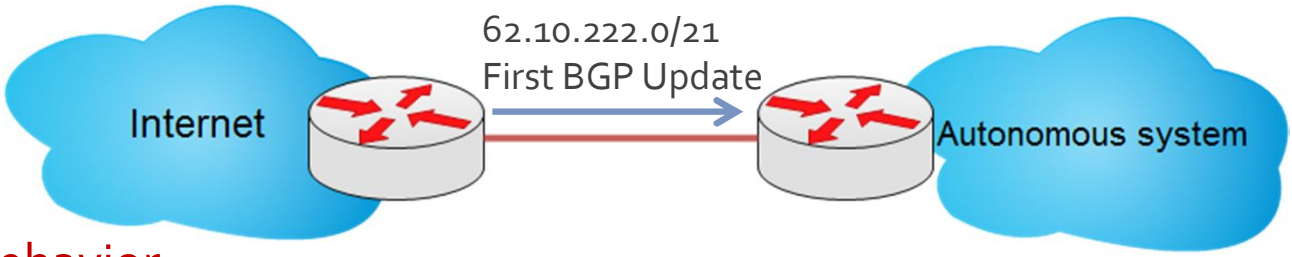
191.1.0.0/21



Information about External routing protocol need to know:

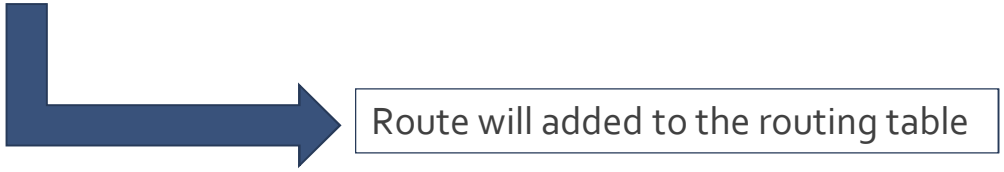
- ✓ Network Advertisement to external peers can be controlled by:
  - ✓ Outgoing traffic.
  - ✓ Incoming traffic (return traffic).
- ✓ **Outgoing traffic** (forwarding traffic) is the easiest part, because you have control over what your own routers do.
- ✓ **Incoming traffic** It's harder to control the coming traffic from Global network.
- ✓ Traffic can be controlled by BGP Path attribute.

How The BGP best path selection work

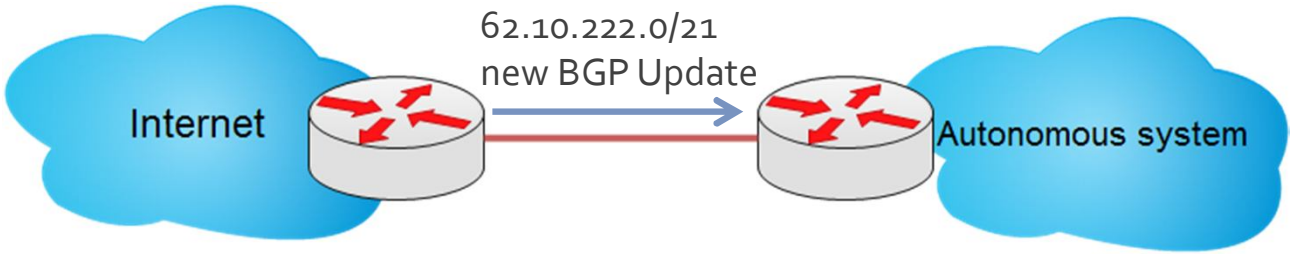


BGP behavior

- Router will ignoring received update if the route is not **valid**.
- Validity of route is:
  - NEXT-HOP of router should valid and reachable.
  - AS-PATH received from External peer does not contain the local ASN.
  - Route should not rejected by routing filter.



How The BGP best path selection work (cont.)



BGP behavior

Route is valid then:

New update Compared with the first route by using BGP path attribute

Default path attribute is shortest AS-Path

First update dst-Net=62.10.222.0/21 AS100 AS120 AS150 AS200 (4 hops)

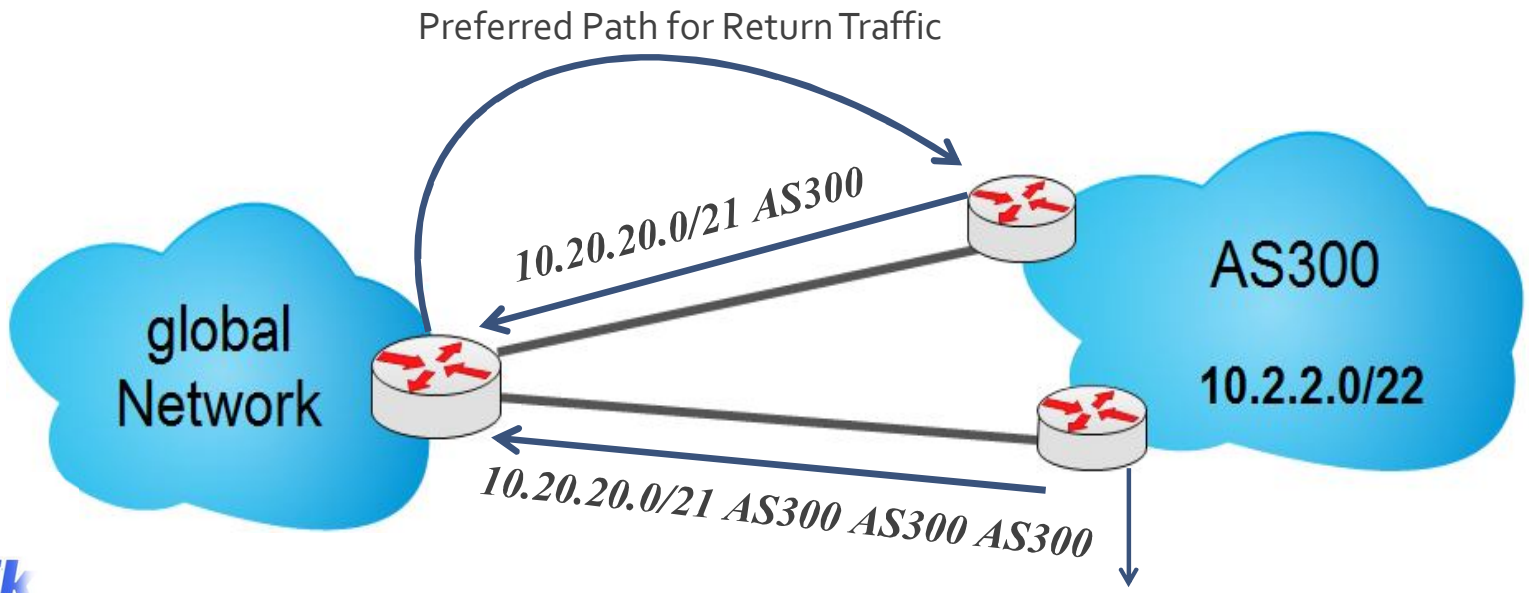
Next update dst-Net=62.10.222.0/21 AS100 AS120 AS150 (3 Hops)

BGP Path attribute

- MikroTik ROS supported path attribute to select best path between received BGP routes.
  - ✓ Prefer the path with the highest **WEIGHT**.
  - ✓ Prefer the path with the highest **LOCAL_PREF**. It is used only within an AS.
  - ✓ Prefer the path with the shortest **AS_PATH.**
  - ✓ Prefer the path that was locally originated via aggregate or BGP network
  - ✓ Prefer the path with the lowest **ORIGIN** type.
  - ✓ Prefer the path with the lowest **multi-exit discriminator** (MED).
  - ✓ Prefer **eBGP** over **iBGP** paths.
  - ✓ Prefer BGP router with the lowest **router ID**.
  - ✓ BGP router with the lowest **neighbor address**.

BGP action on out-going update

- To influencing BGP route selection in the Global network is the extension of AS_PATH attribute , route with the shorts AS_PATH preferred.
- Prepend is a BGP action to create Multi copies of own AS number added in front of AS_PATH



BGP action on out-going update with Mikrotik RoS

- Frist adding routing filter with the respected info:
  - Filter name "Out_going_peer1"
  - Match parameter like network and subnet.. etc
  - BGP-action (set New BGP attribute)..!
- Select the filter name on Out-going-filter for the required peer

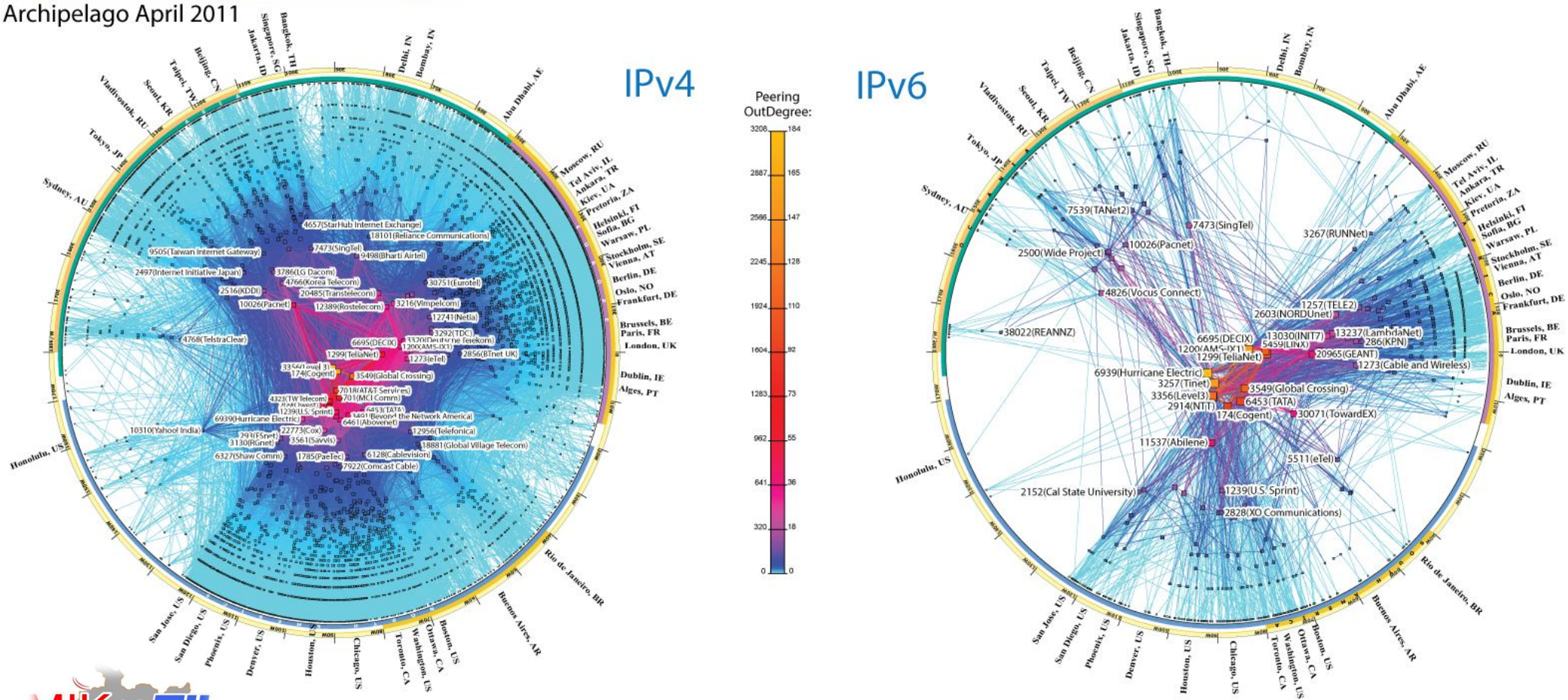
Note :

- One filter can be used for all peers or multi peers or only for one peer
- Its possible to have multi filter for one peer to set specific BGP action on specific networks, but should all have same name..!!
- Its possible to set deferent outing policy for each peer, by create specific filter for each peer

IPv6

CAIDA'S IPv4 & IPv6 AS Core
AS-level INTERNET GRAPH

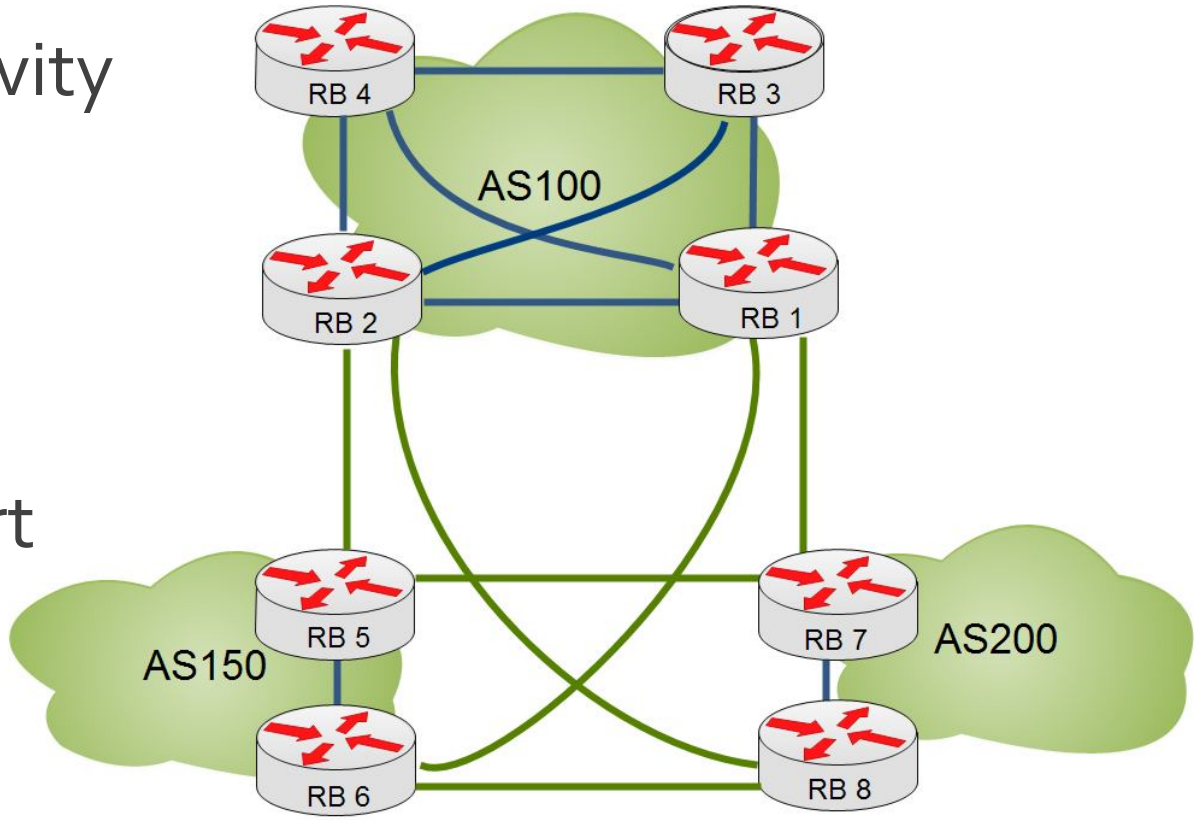
Archipelago April 2011



IPv6 Global Networking

Current IP level connectivity based on IPv4

Let's make its support the IPv6



Unicast IPv6 Addresses

IPv6 supports three main types of unicast addresses:

- Global (Same as Public IPv4 address).
- Unique local (Same as IPv4 private address).
- link local:
  - ✓ For sending and receiving IPv6 packets on a single subnet.
  - ✓ Used by Neighbor discovery (the equivalent of ARP for IPv6).
  - ✓ Used as the next-hop for IP routes.
  - ✓ Link-local Traffic never forwards beyond the network.

Global IPv6 distribution (RFC 2374)

- Hierarchy address structure format.
- Design criteria is to facilitate scalable Internet routing.
- Support provider and exchange based routes aggregation.
- Separation of public and site topology.
- Aggregatable addresses are organized into a three level hierarchy:
  - ✓ Public Topology.
  - ✓ Site Topology.
  - ✓ Interface Identifier.

Global IPv6 distribution (cont.)

- Aggregatable Global Unicast address format structure

24 bit	24 bit	16 bit	64 bit
TLA ID	NLA ID	SLA ID	Interface ID

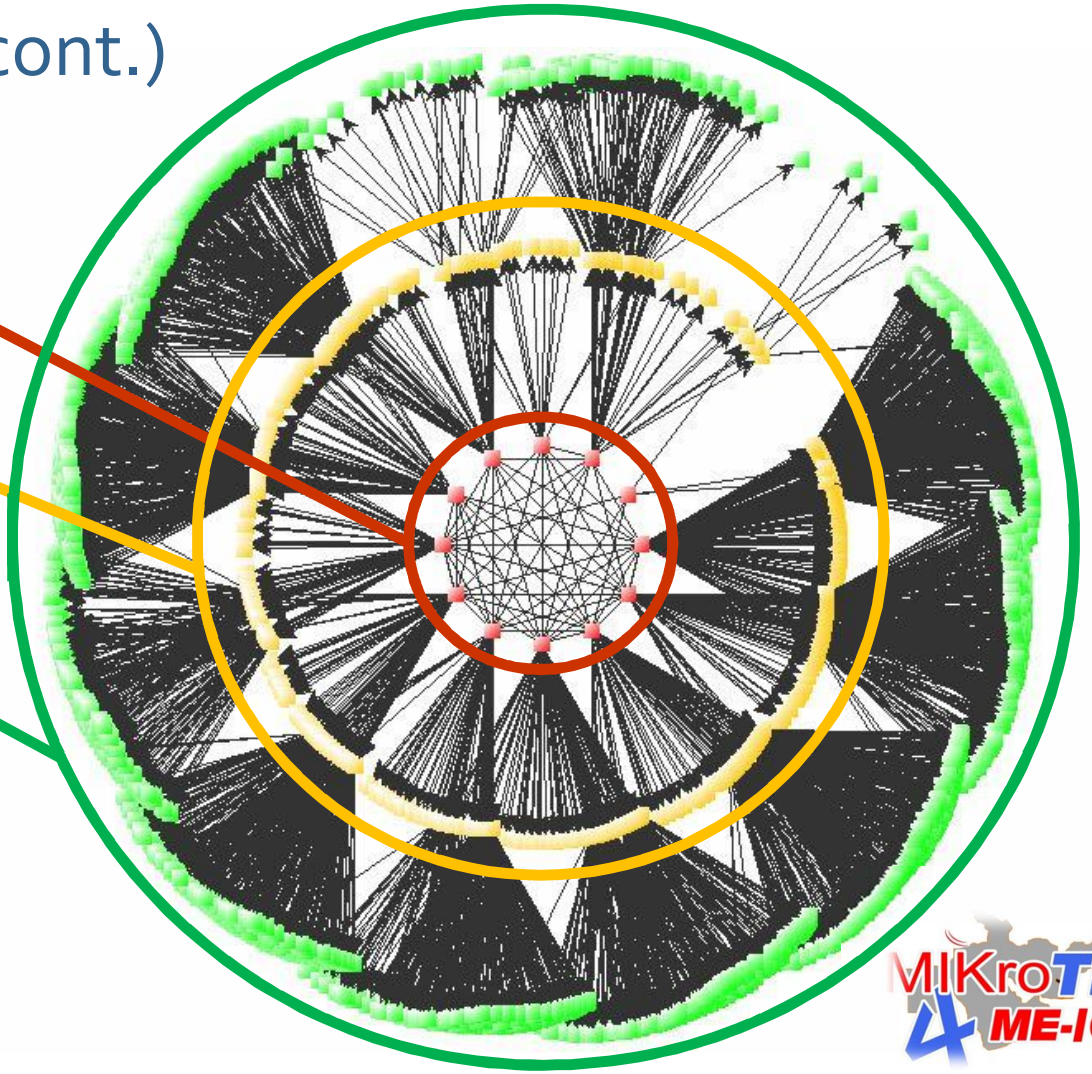
- Where :
  - ✓ TLA (Top Level Aggregation)
  - ✓ NLA (Next Level Aggregation)
  - ✓ SLA (Site Level Aggregation)

Global IPv6 distribution (cont.)

Top Level Aggregation

Next Level Aggregation

Site Level Aggregation



Global IPv6 distribution (cont.)

- Top Level Aggregation Nodes:
  - ✓ Top level in the global routing hierarchy.
  - ✓ Default-free routers.
  - ✓ Must have routing information of all active TLD IDs.
  - ✓ This addressing format supports 8,192 (2^13) TLA ID's
  - ✓ 8 bits from "24 bits" reserved for future use..!!!!

Site Level Aggregation scenario

- Assigned subnet from ISP is 2013:1234:CF01::/48.
- There is 3 Autonomous system.
- At least 3 Global prefix required.
- Each (AS) contain multi sub networks .
- Each sub network represent complex.
- In each complex there are Campus, Business Center or Government Institution..etc

IPv6 subnet distribution design

- Using Hierarchy structure addressing.
- Assigned subnet will considered as TLA.
- These three AS consider as NLA 1 (first level subnet)
- Each complex consider as NLA2 (second level subnet).
- Campus , Business Center and Government Institution will be considered as Site Level.

IPv6 subnet distribution design (cont.)

Top Level Aggregation
2013:1234:CF01::/48

NLA 1

AS 100

AS 200

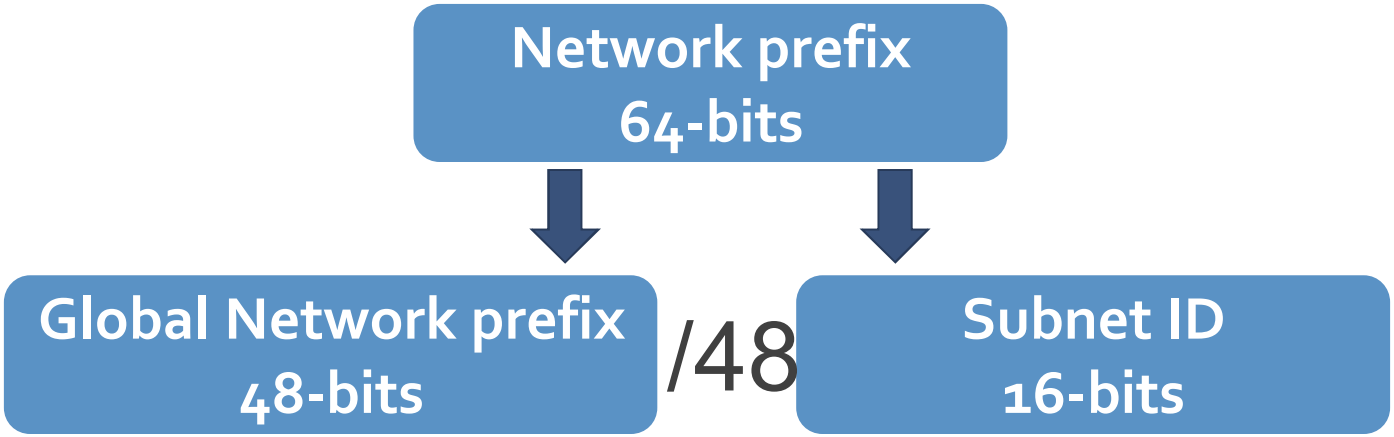
AS 150

IPv6 subnet distribution

- Each IPv6 address represent 128 bit instead of 32 bit in IPv4.
- Contain tow portion Network prefix / Interface identifier .
- Each of network prefix portion and Interface ID represent 64bit.

IPv6 subnet distribution (cont.)

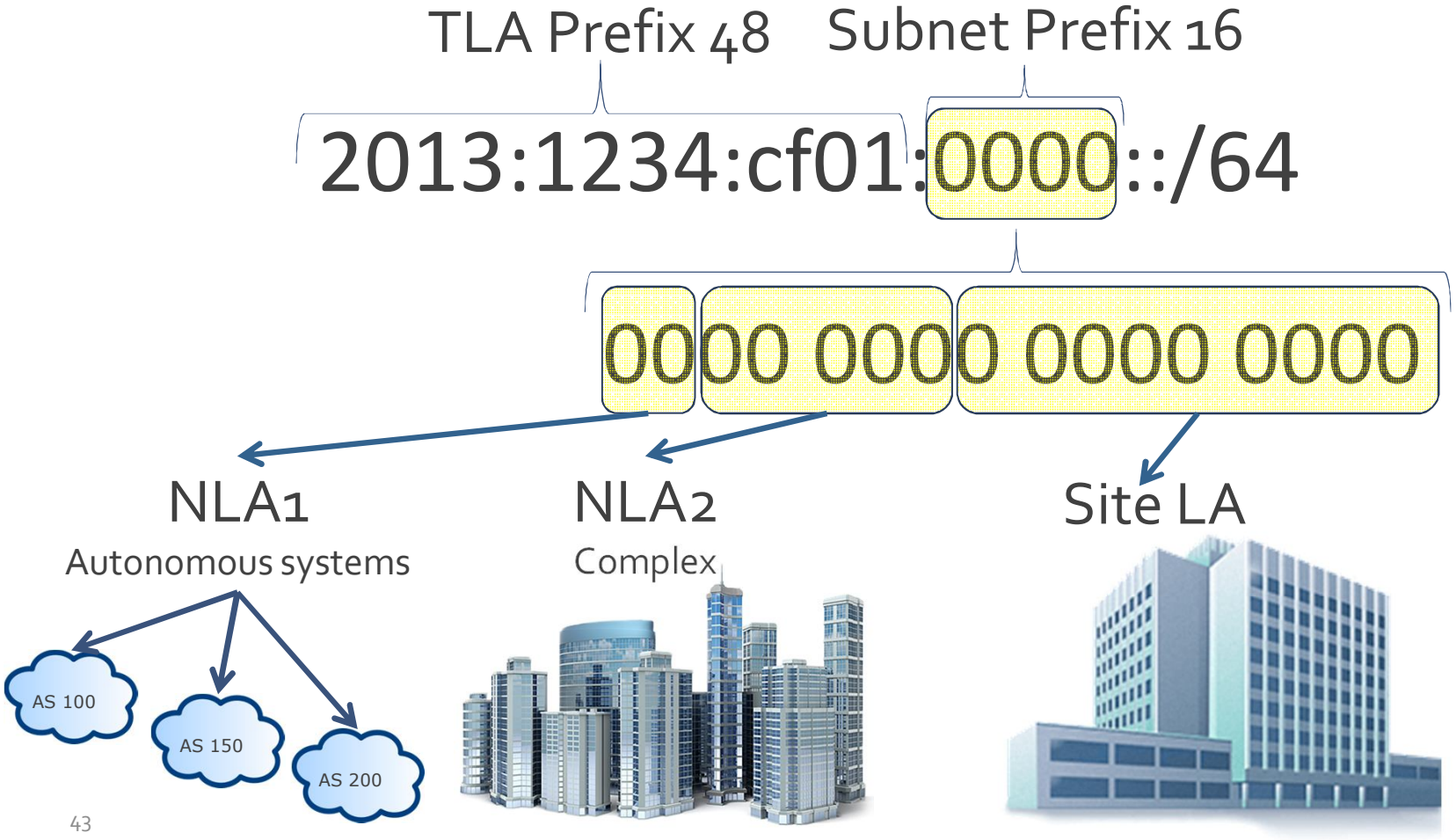
- For Global IPv6 subnetting usually work on network prefix portion.
- 64 (network prefix) – 48 (Prefix of assigned subnet) = 16 bits.
- This16 bits called Subnet ID
- Will be used to create subnet distribution plan



IPv6 subnet distribution (cont.)

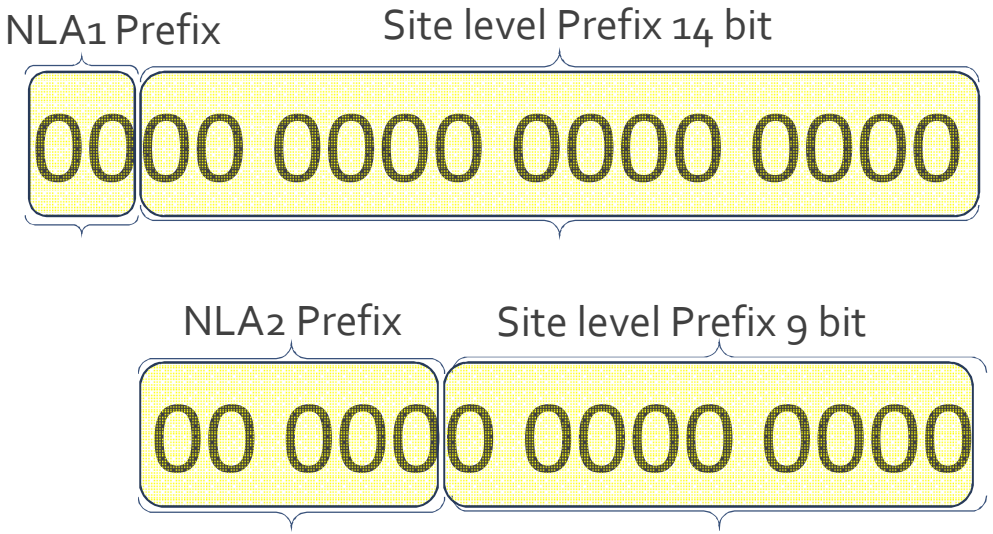
- First 2 bits of 16 bits will be used for NLA1 (/50)
- Next 5 bits will be used for NLA2
- And reset bits will be used for Site level.
- 64 bit at Interface ID will be used for Host assignment.

IPv6 subnet distribution (cont.)



Next Level Aggregation

Hierarchy point of view to lower prefix



IPv6 subnet distribution

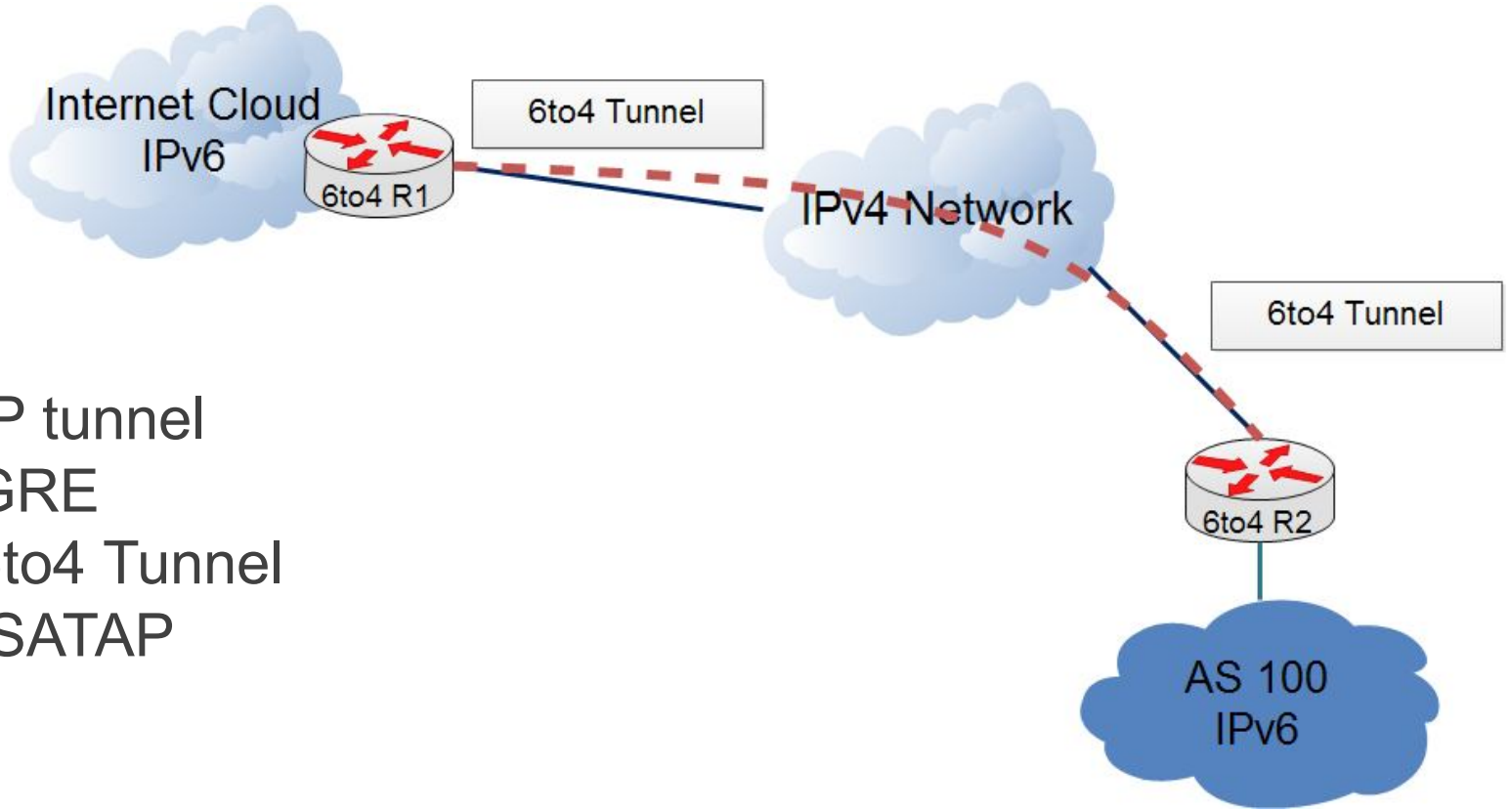
- 2 bit will provide 4 /50 subnet as show in below:
  - ✓ 00 = first subnet
  - ✓ 01 = second subnet
  - ✓ 10: third subnet
  - ✓ 11= 4th subnet
- 5 bit will provide 32 /55 subnet
- 9 bit will provide 512 /64 subnet
- At the end each AS can contain 16384 /64 subnet
- Visit www.subnetonline.com

Migration to IPv6

IPv4 to IPv6 Migration

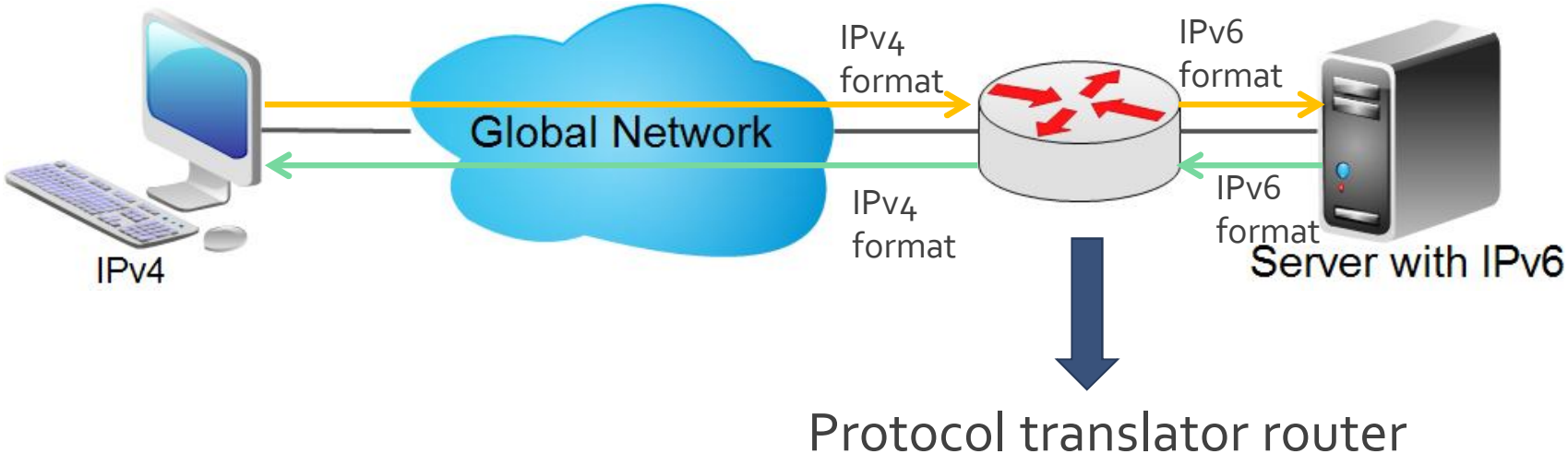
- Most Enterprises do not move from having no formal IPv6 support to creating a full native IPv6 implementation on all routers and other devices.
- In the real world, some Enterprise networks will begin with several locations that need consistent and working IPv6 support.
- During this possibly long migration, three main classes of tools may be used to allow IPv4 to continue to work well, while supporting IPv6:
  - ✓ Tunneling.
  - ✓ NAT Protocol Translator (NAT-PT).
  - ✓ Dual IPv4/IPv6 stacks (dual stacks).

IPv6 Tunneling

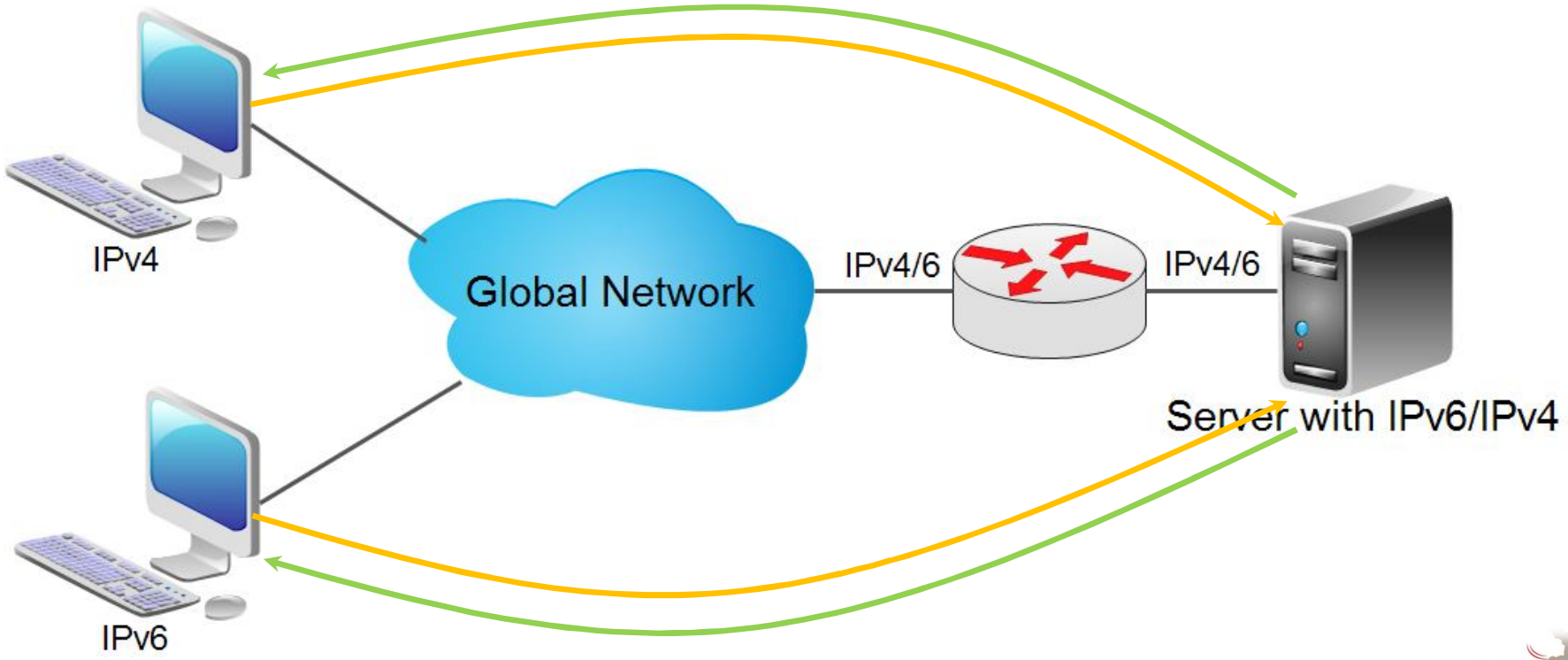


- ✓ IP tunnel
- ✓ GRE
- ✓ 6to4 Tunnel
- ✓ ISATAP

IPv6 Protocol Translation

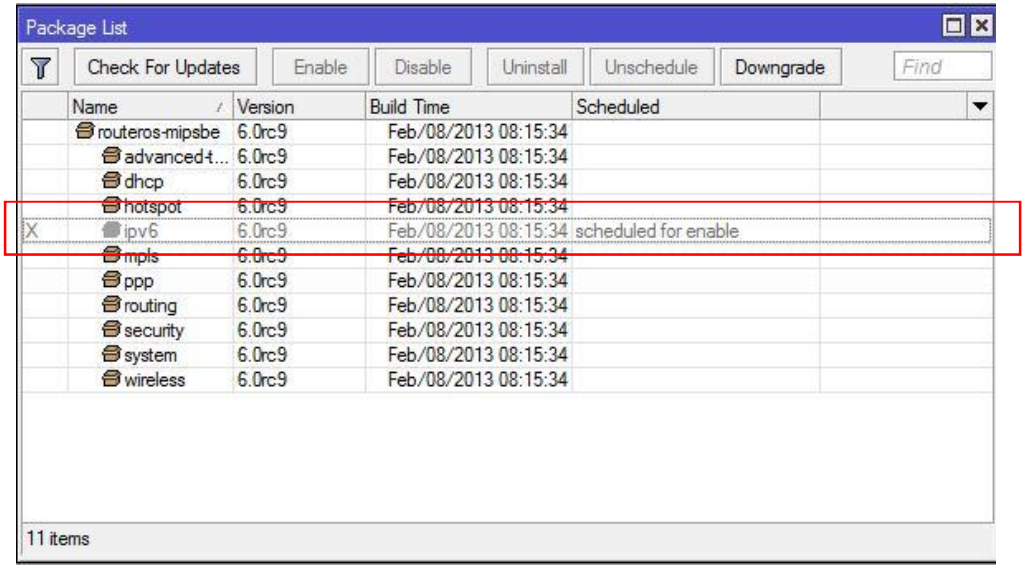


Dual Stacks addressing

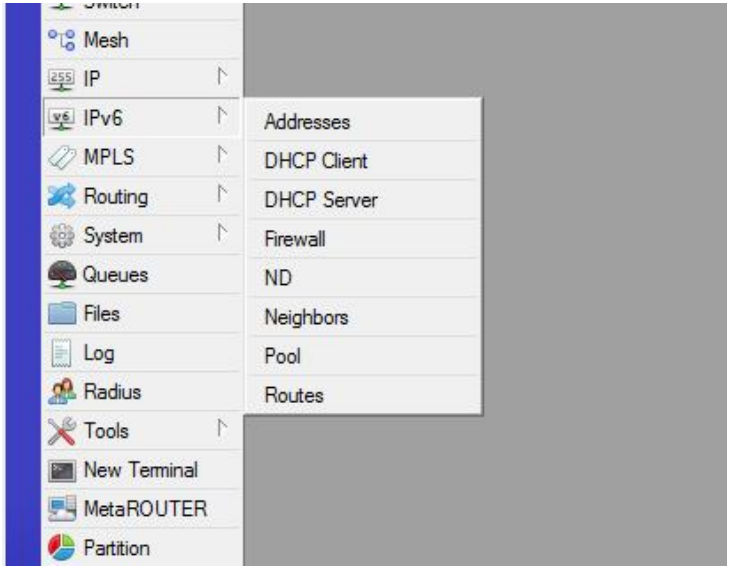


IPv6 addressing on MikroTik RoS

- Enable IPv6 Package



- IPv6 Menu

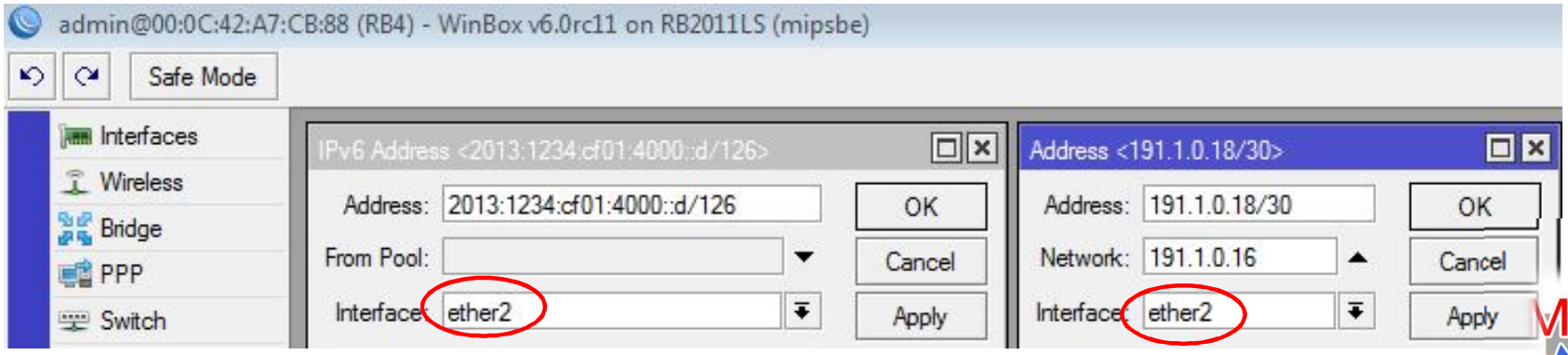


Dual Stacks addressing

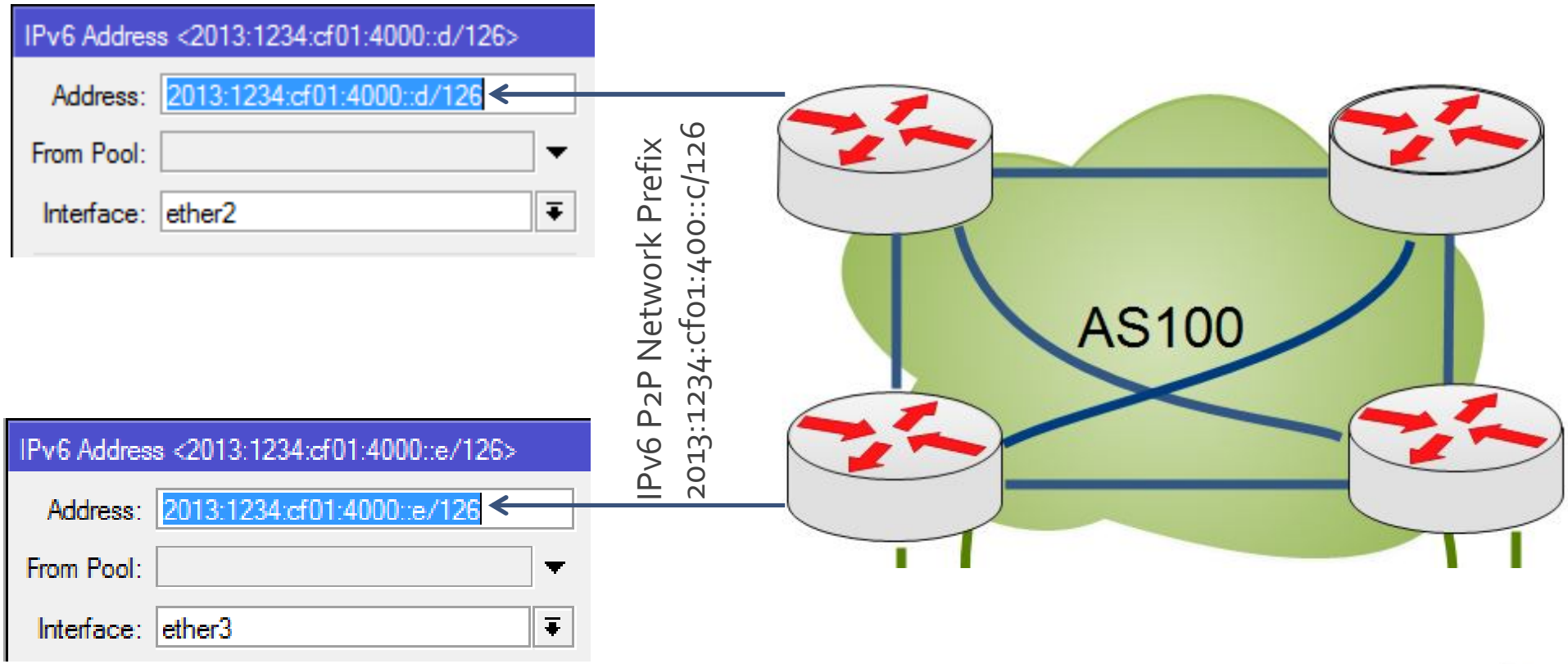
- The term *dual stacks* means that the host or router uses both IPv4 and IPv6 at the same time.
- Means that both an IPv4 and IPv6 address associated with each NIC.
- Host can send IPv4 packets to other IPv4 hosts, and at same time host can send IPv6 packets to other IPv6 hosts.
- For routers, it means that in addition to the usual IPv4 IP addresses and routing protocols, the routers would also have IPv6 addresses and routing protocols configured.

Why Dual Stacks?

- Possible to giving each interface one or more IPv6 addresses, enabling IPv6 routing protocols, and so on.
- Assuming an IPv4 network already exists, the engineer could build and execute and implementation plan to configure native IPv6 by enabling IPv6 on the same interfaces as IPv4.
- configuring an IPv6 routing protocol, and the routers would be ready to forward both types of packets.



IPv6 P2P addressing



IPv6 Routing Protocols

- To support IPv6, all the IPv4 routing protocols had to go through varying degrees of changes.
- Each had to be changed to support longer addresses and prefixes.
- The actual messages used to send and receive routing information using IPv6 headers instead of IPv4 headers, and using IPv6 addresses in those headers.

IPv6 Routing Protocols (cont.)

- In particular, like their IPv4 versions, each IPv6 IGP uses IPv6 multicast addresses.
- each IPv6 IGP has more similarities than differences compared to their respective IPv4.
- For example: RIPng, based on RIP-2, is still a Distance Vector protocol, with hop count as the metric and 15 hops as the longest valid route (16 is infinity).

OSPFv3 VS OSPFv2

- Size of the message header is reduced from 24 bytes to 16.
- Protocol processing per-link, not per-subnet.
- Explicit support for multiple instances per link (using instance ID new field).
- Using IPv6 link-local addresses as next hop.
- Authentication method changes, was on header now its on based IPSec.
- Packet format, LSA header format changes.
- Handling of new LSA types 8,9.
  - ✓ Type 8 " Link-Local Scope"
  - ✓ Intra-Area-Perfix-LSA Area Scope

• Note: Router ID and Area ID is still use 32 bit

OSPFv3 and v2 similarities

Packet Type

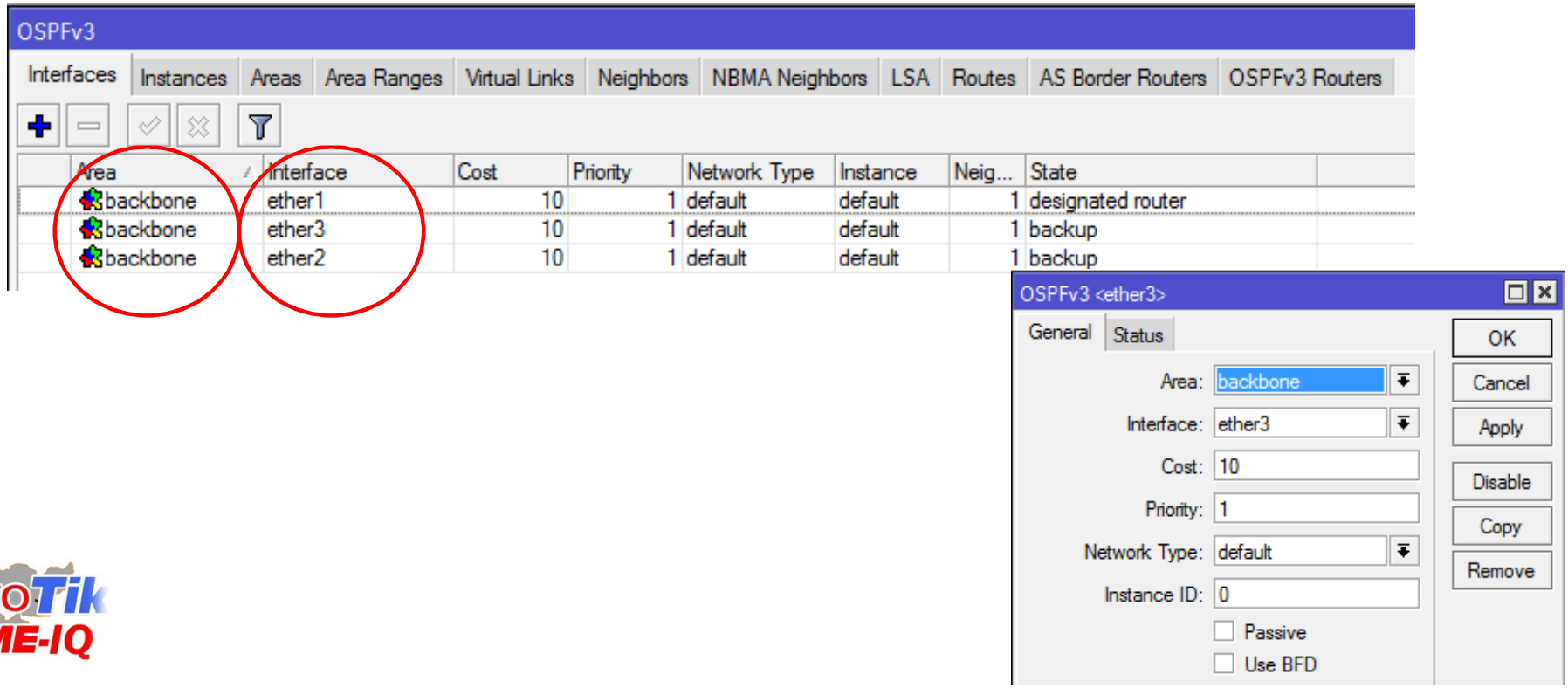
OSPFv3 Packet Type
Type 1 - Hello
Type 2 - Database Description
Type 3 - Link State Request
Type 4 - Link State Update
Type 5 - Link State Acknowledgement

Interface Type

OSPFv3 Interface Type
P2P
P2MP
Broadcast
NBMA
Virtual

OSPF v3 Implementation

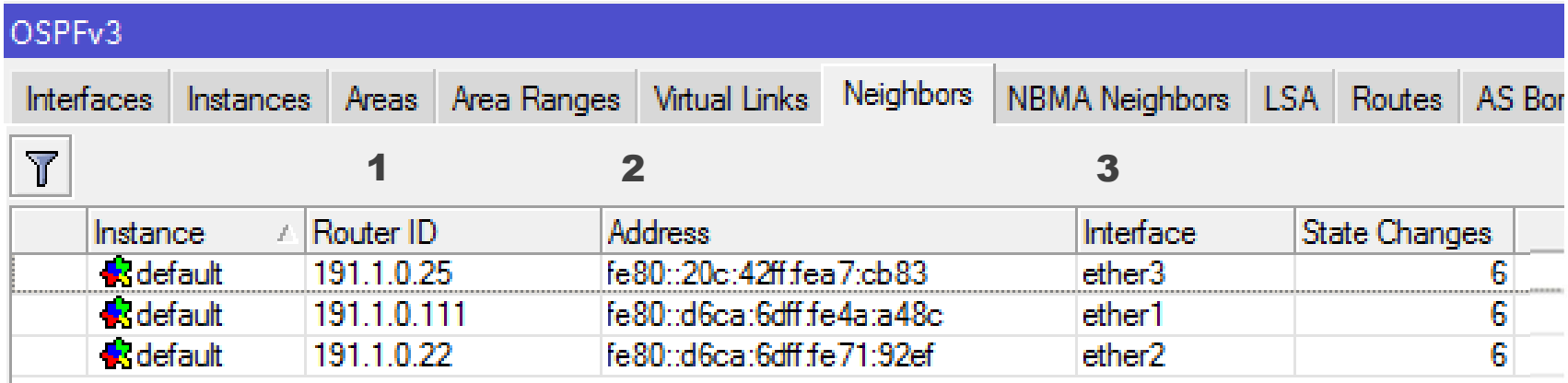
- Just Add connected interfaces with proper area.



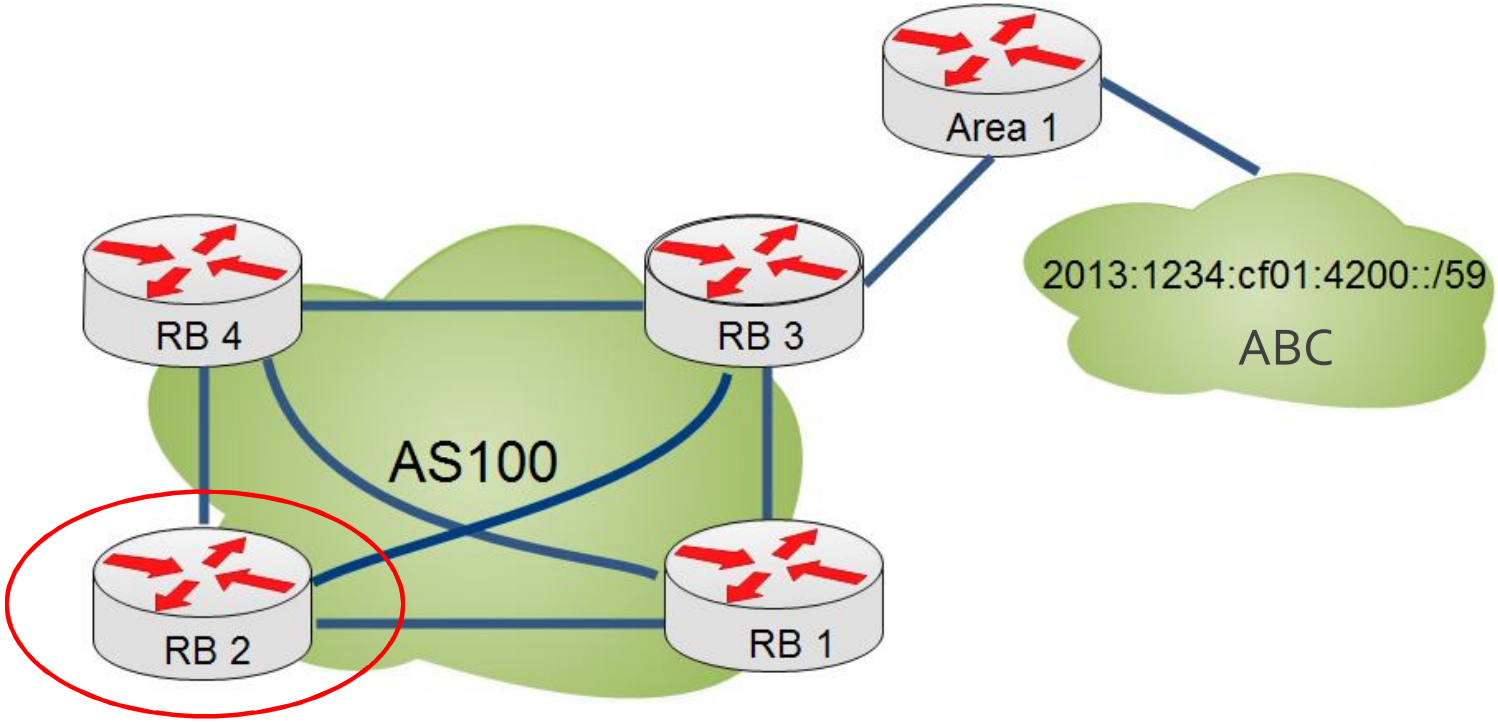
OSPF v3 Implementation (cont.)

Neighbor details:

1. Router ID: its same as OSPFv2 use the 32 bit address with the same election.
2. Address: IPv6 address (link-local) which belong neighbor direct connected interface.
3. Interface: local interface that connected to the neighbor router.



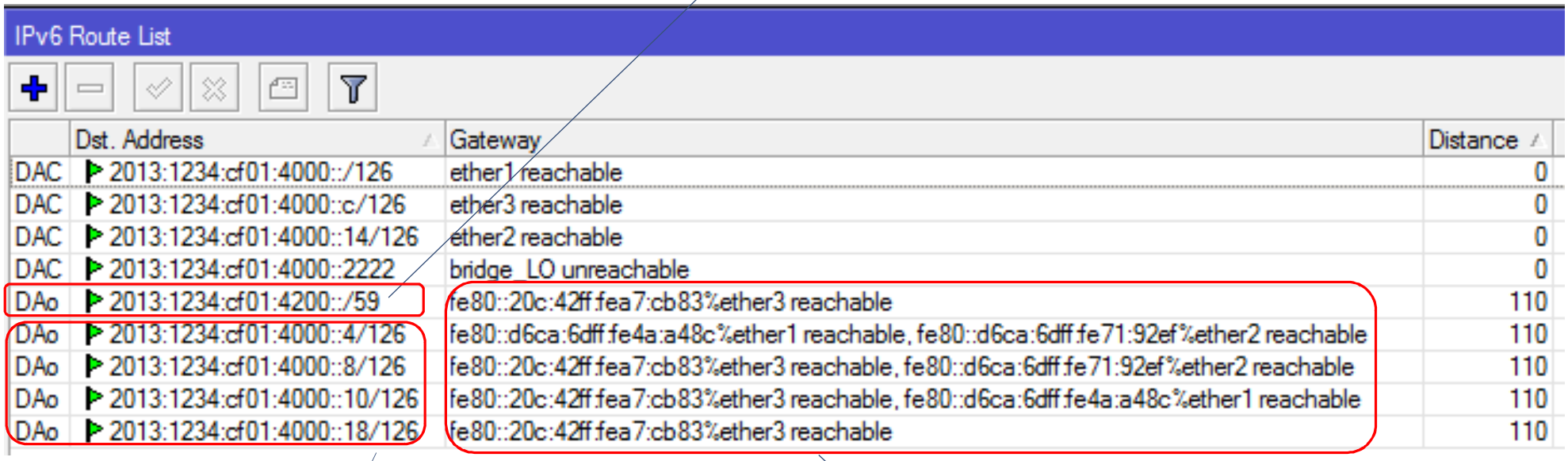
OSPF v3 Implementation (cont.)



Showing routing table of RB2 at next slide

OSPF v3 Implementation (cont.)

Network advertised from ABC Network via OSPFv3



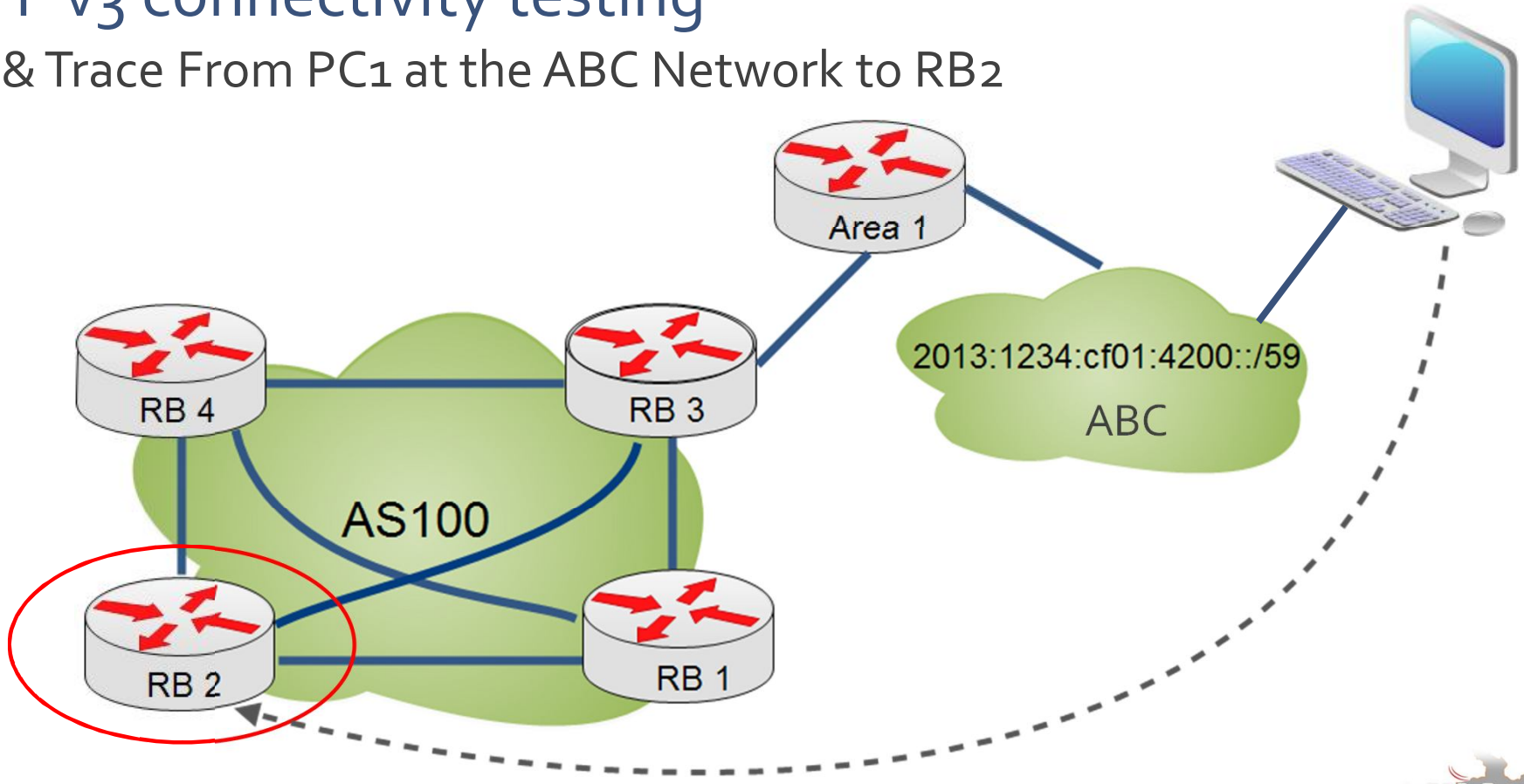
	Dst. Address	Gateway	Distance
DAC	2013:1234:cf01:4000::/126	ether1 reachable	0
DAC	2013:1234:cf01:4000::c/126	ether3 reachable	0
DAC	2013:1234:cf01:4000::14/126	ether2 reachable	0
DAC	2013:1234:cf01:4000::2222	bridge_LO unreachable	0
DAo	2013:1234:cf01:4200::/59	fe80::20c:42ff:fea7:cb83%ether3 reachable	110
DAo	2013:1234:cf01:4000::4/126	fe80::d6ca:6dff:fe4a:a48c%ether1 reachable, fe80::d6ca:6dff:fe71:92ef%ether2 reachable	110
DAo	2013:1234:cf01:4000::8/126	fe80::20c:42ff:fea7:cb83%ether3 reachable, fe80::d6ca:6dff:fe71:92ef%ether2 reachable	110
DAo	2013:1234:cf01:4000::10/126	fe80::20c:42ff:fea7:cb83%ether3 reachable, fe80::d6ca:6dff:fe4a:a48c%ether1 reachable	110
DAo	2013:1234:cf01:4000::18/126	fe80::20c:42ff:fea7:cb83%ether3 reachable	110

PtP addressing at core level network

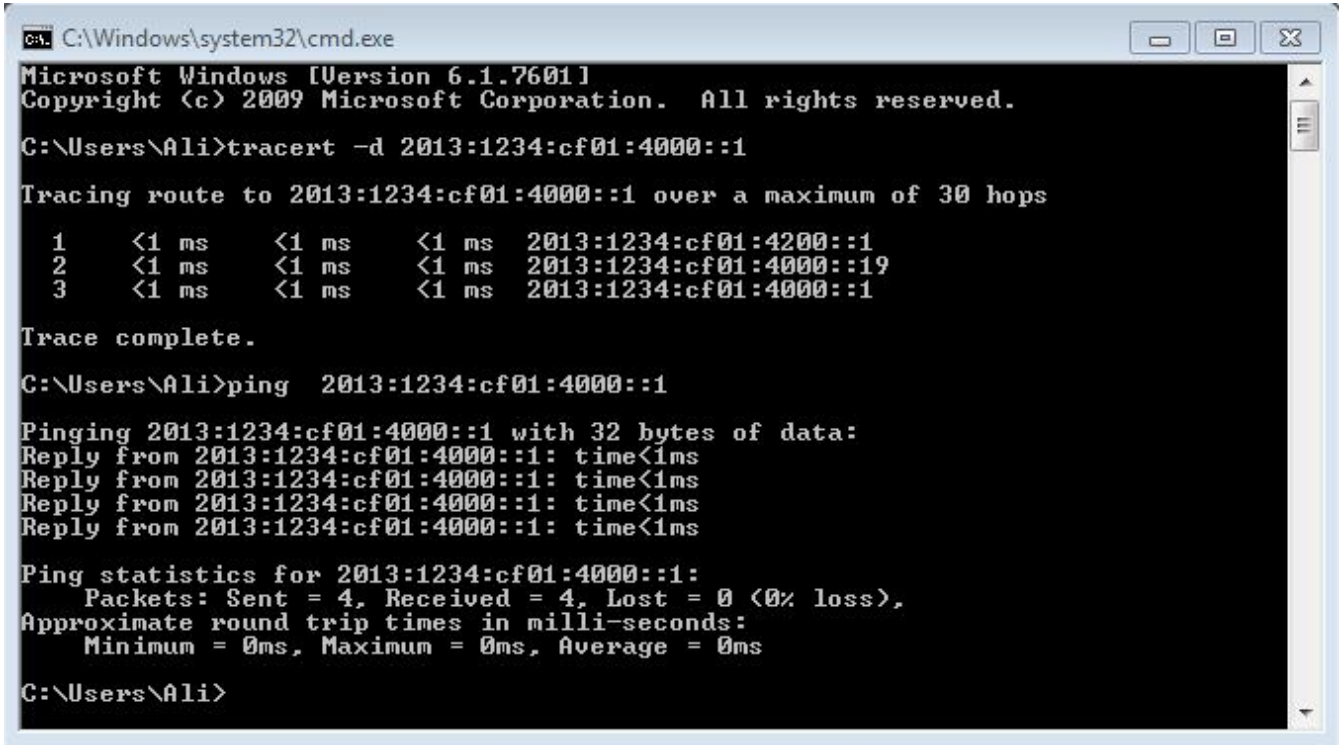
All next hop are used Link-Local addresses

OSPF v3 connectivity testing

Ping & Trace From PC1 at the ABC Network to RB2



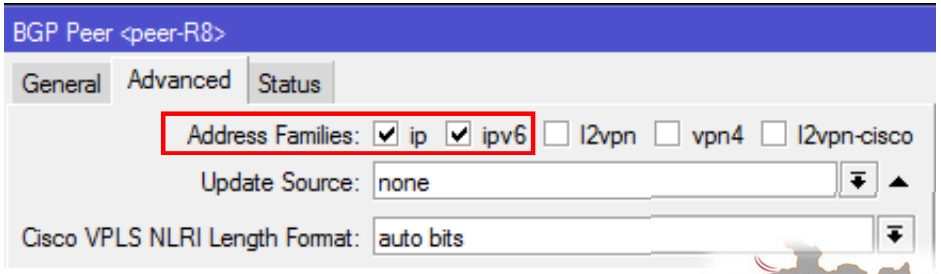
Check network reachability by simple network tools



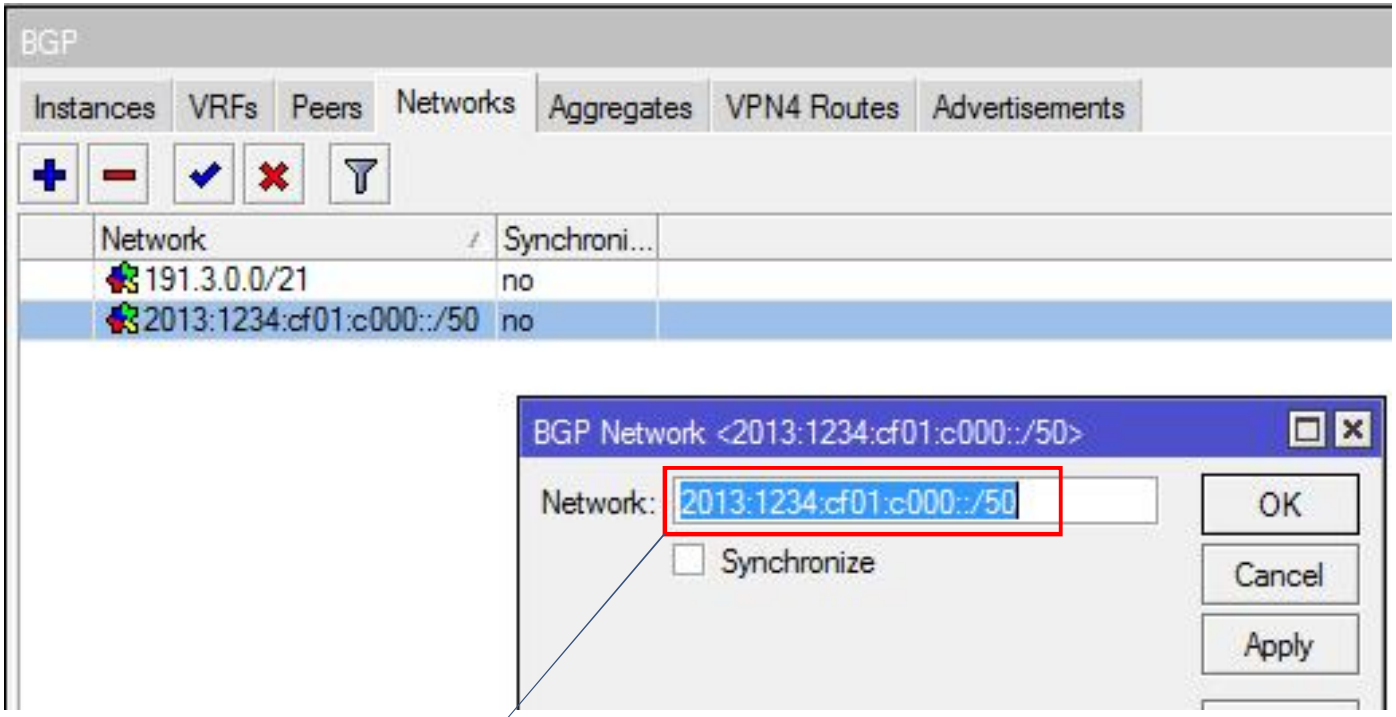
By using ping and trace route we approve the IPv6 and OSPFv3 working successfully according to the routing table in the previous slide .

Global IPv6 connectivity

- Migration within AS had been done..!
- Migration based on Native IPv6 Dual stacks.
- To make IPv6 Internal network connect to External network need to enable this feature on BGP protocol
- BGP by default does not support IPv6 protocol… In MikroTik RoS
- By select IPv6 from "address-families" BGP will start advertised IPv6 Prefix:
  - ✓ Listed in the Networks
  - ✓ Received update from other external peers.



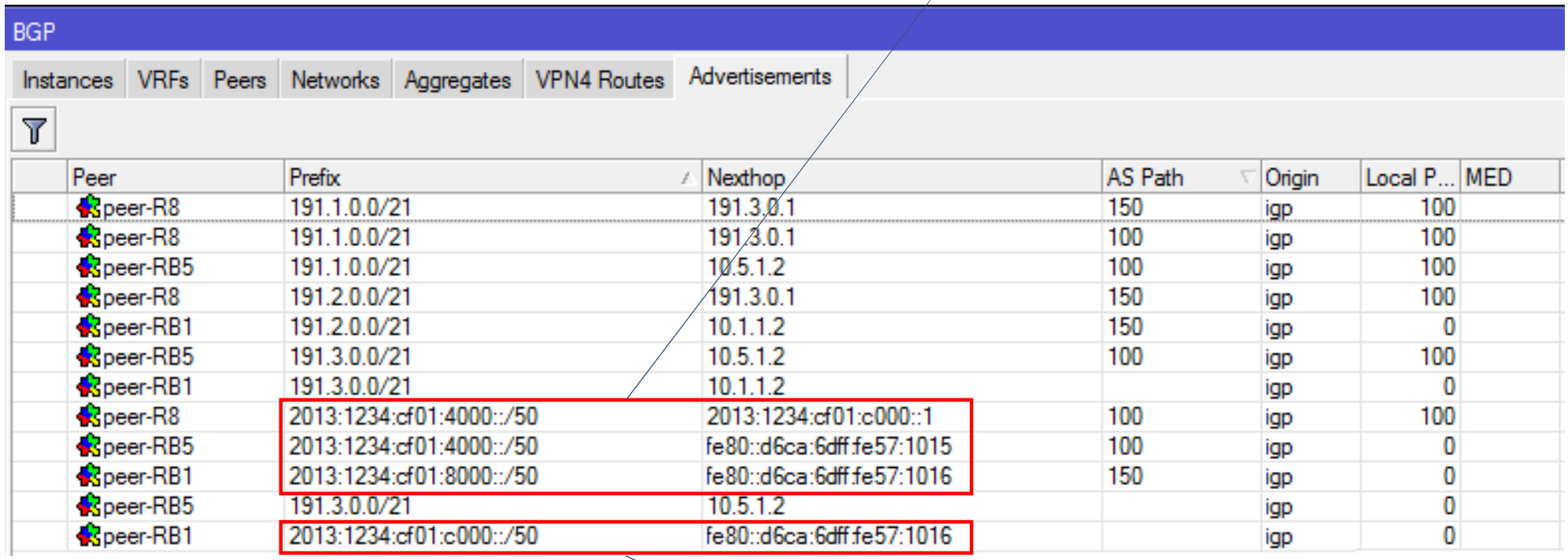
Global IPv6 connectivity (Cont.)



Adding local prefix to advertise to external peers

Global IPv6 connectivity (Prefix updates)

Re-advertised Prefix to another iBGP and eBGP peers



Peer	Prefix	Nexthop	AS Path	Origin	Local P...	MED
peer-R8	191.1.0.0/21	191.3.0.1	150	igp	100	
peer-R8	191.1.0.0/21	191.3.0.1	100	igp	100	
peer-RB5	191.1.0.0/21	10.5.1.2	100	igp	100	
peer-R8	191.2.0.0/21	191.3.0.1	150	igp	100	
peer-RB1	191.2.0.0/21	10.1.1.2	150	igp	0	
peer-RB5	191.3.0.0/21	10.5.1.2	100	igp	100	
peer-RB1	191.3.0.0/21	10.1.1.2		igp	0	
peer-R8	2013:1234:cf01:4000::/50	2013:1234:cf01:c000::1	100	igp	100	
peer-RB5	2013:1234:cf01:4000::/50	fe80::d6ca:6dff:fe57:1015	100	igp	0	
peer-RB1	2013:1234:cf01:8000::/50	fe80::d6ca:6dff:fe57:1016	150	igp	0	
peer-RB5	191.3.0.0/21	10.5.1.2		igp	0	
peer-RB1	2013:1234:cf01:c000::/50	fe80::d6ca:6dff:fe57:1016		igp	0	

Advertised local prefix after added to the network tab

Global IPv6 connectivity (Routing Table)

IPv6 Route List

	Dst. Address	Gateway	Distance
DAb	2013:1234:cf01:4000::/50	fe80::d6ca:6dff:fe4a:a495%ether10 reachable	20
Db	2013:1234:cf01:4000::/50	fe80::d6ca:6dff:fe71:91ee%ether9 reachable	20
Db	2013:1234:cf01:4000::/50	fe80::d6ca:6dff:fe2e:b6ff%ether1 reachable	200
DAb	2013:1234:cf01:8000::/50	fe80::d6ca:6dff:fe71:91ee%ether9 reachable	20
Db	2013:1234:cf01:8000::/50	fe80::d6ca:6dff:fe4a:a495%ether10 reachable	20
Db	2013:1234:cf01:8000::/50	fe80::d6ca:6dff:fe2e:b6ff%ether1 reachable	200
DAb	2013:1234:cf01:c000::/50	fe80::d6ca:6dff:fe2e:b6ff%ether1 reachable	200
DAC	2013:1234:cf01:c000::/126	ether1 reachable	0

D = Dynamic
A = Active
b = iBGP (Distance 200)
b = eBGP (Distance 20)
C = Direct Connected
Note: Blue color entry is mean this is back up route to destination

Thanks for Attention!!

www.mikrotik4me.com
ali@mikrotik4me.com
009647800075000