MikroTikSA

BGP vs OSPF vs RIP vs MME

Battle of the Dynamic Protocols

Presentation Outline

- Introduction
  - Who am I?
  - What is this presentation all about
  - What will I learn from this
- What are dynamic routing protocols?
  - Basics of RIP
  - Basics of OSPF
  - Basics of BGP
  - Basics of MME
- When should I be using these protocols
  - Application of RIP
  - Application of OSPF
  - Application of BGP
  - Application of MME

MikroTik SA

Outline Continued

- Best Practices
  - How do I combine these protocols together?
  - What do I need to support larger networks
    - E.g. MPLS, VPLS, Traffic Engineering, VRF's
- Conclusion

About MikroTik SA

- Independent Wireless Specialist company
- Not owned by / affiliated to MikroTik Latvia
- Official training and support partner for MikroTik
- Specialist in all forms of wireless and wired networking technologies
- Offers high speed PTP links, carrier independent backbone services, high availability SLA's, ad-hoc consultation, retainer based consultation

MikroTik SA

David Savage

- Is a MikroTik Certified Trainer and consultant – 11+ years
- Installs and manages and wireless networks
- Has over 30 years experience in the IT field
- Teaches general networking and MikroTik RouterOS
- Provides high level support for many companies around the world
- More recently partnering with Teraco to present Teraco Tech Days featuring MikroTik RouterOS

MikroTik SA

What is this all about?

- MikroTik provides a number of dynamic routing protocols that can be deployed to build robust, fault tolerant layer 3 networks
- It is often confusing as to which protocol is suitable for which network application
- This presentation will explore the fundamental differences between these protocols
- I will provide guidelines on when to deploy them, where to deploy them and why.

Protocol Fundamentals

RIP

OSPF

MME

BGP

RIP

- Routing Information Protocol
- Distance Vector Protocol
- V1
- V2
- RIPng

MikroTik SA

RIP V1	RIP V2	RIPNG
Sends update as broadcast	Sends update as multicast	Sends update as multicast
Broadcast at 255.255.255.255	Multicast at 224.0.0.9	Multicast at FF02::9 (RIPng can only run on IPv6 networks)
Doesn’t support authentication of update messages	Supports authentication of RIPv2 update messages	–
Classful routing protocol	Classless protocol, supports classful	Classless updates are sent

MikroTik SA

RIPv1

- RIPv1 defined in RFC 1058.
- Routes are specified by IP destination network and hop count.
- The routing table is broadcast to all stations on the attached network
- Does not support CIDR – only the destination network is sent, not the subnet prefix
- Deprecated since the introduction of RIPv2

MikroTik SA

RIPv2

- RIPv2 defined in RFC 1723.
- Route specification also includes subnet mask and gateway.
- The routing table is sent to a multicast address, reducing network traffic.
- Authentication may be used for security.

MikroTik SA

RIPng

- RIPng defined in RFC 2080.
- Extension of RIPv2 designed for IPv6.
- The routing table is sent to a multicast address, reducing network traffic.
- While RIPv2 supports updates authentication, RIPng does not
  - IPv6 routers were, at the time, supposed to use IPsec for authentication.

MikroTik SA

RIP Operation

- RIP is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network
- It is a distance vector routing protocol which has AD value 120 (distance value installed in the routing table)
- Distance vector calculates only based on hop count and has no means for defining individual link metrics

MikroTik SA

Hop Count

- Hop count is the number of routers occurring in between the source and destination network.
- The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table.
- RIP prevents routing loops by limiting the number of hops allowed in a path from source and destination.
- The maximum hop count allowed for RIP is 15 and hop count of 16 is considered as network unreachable

MikroTik SA

Features of RIP

- Updates of the network are exchanged periodically.
- Updates (routing information) are always broadcast.
- Full routing tables are sent in updates.
- Routers always trust on routing information received from neighbor routers (Routing on Rumours)
- Convergence (calculation of best path) is slow

MikroTik SA

OSPF

- Open Shortest Path First protocol
- Uses a link state routing algorithm
- V2 and V3 in current operation
  - V3 is defined for IPv6
- Can use broadcast, multicast, PTP to reduce network traffic
- Can define a Designated Router for broadcast nodes to reduce traffic between peers

MikroTik SA

Theory of OSPF

- OSPF is a link-state routing protocol which is used to find the best path between the source and the destination router using its own Shortest Path First (Djikstra) algorithm.
- OSPF was developed as one of the Interior Gateway Protocol (IGP), i.e, the protocol which aims at moving the packet within a large autonomous system or routing domain.
- It is a network layer protocol which works on the protocol number 89 and uses AD value 110.
- OSPF uses multicast address 224.0.0.5 for normal communication

MikroTik SA

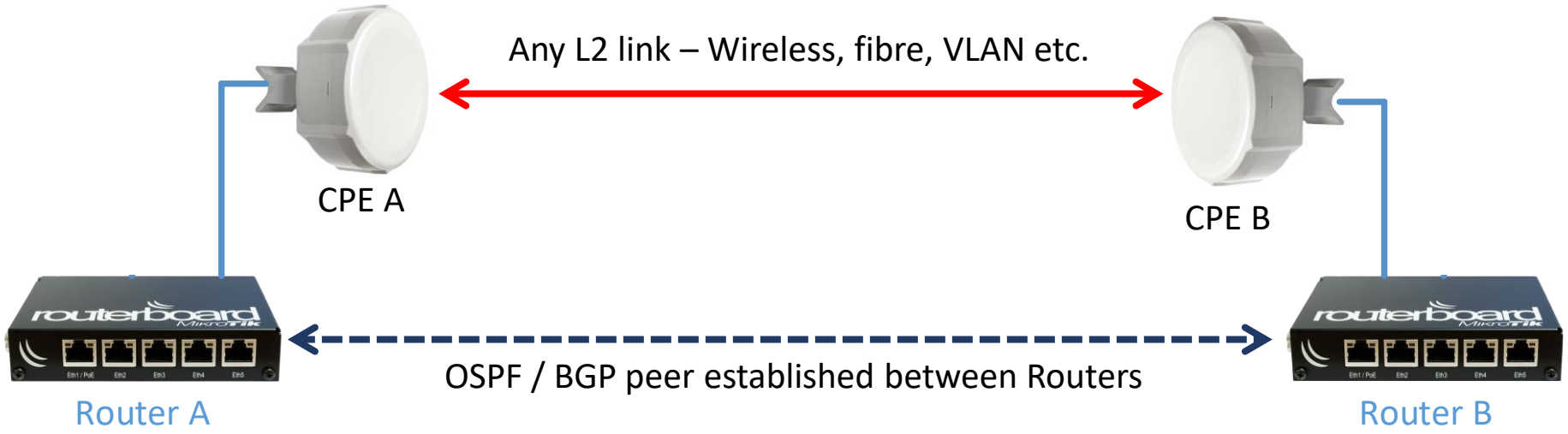
Link State Routing

- The basic concept is that every node constructs a map of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes.
- Each node then independently calculates the next best logical path from it to every possible destination in the network.
- Each collection of best paths will then form each node's routing table.
- Calculations can take into account individual costs per link in either direction
- Costs can be based on default value, administrative value, bandwidth constraints, load on the link etc.

MikroTik SA

Peer State Monitoring

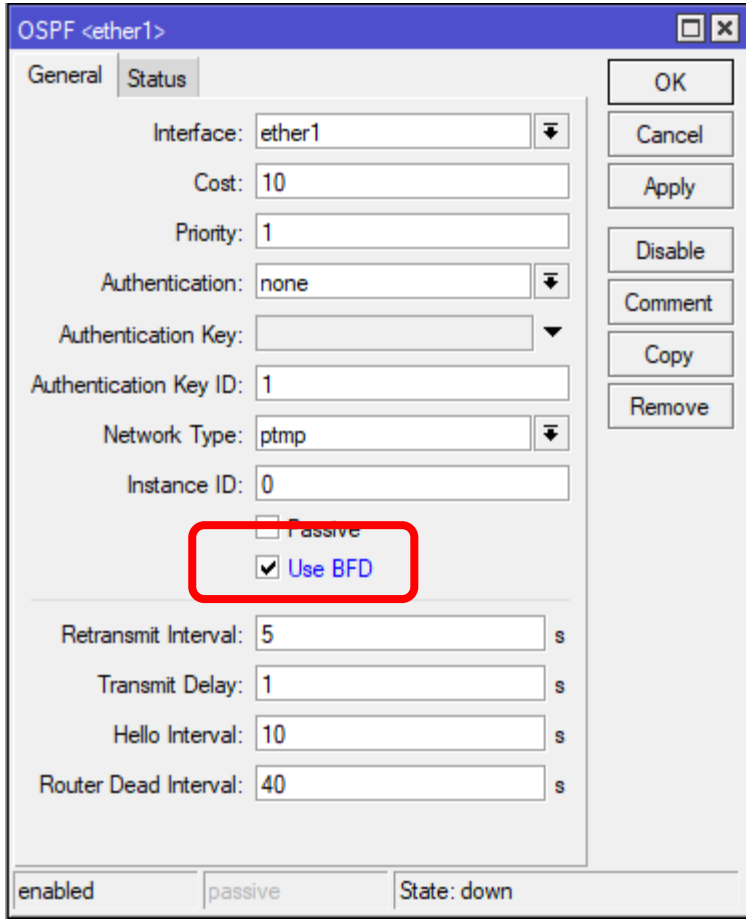
- Routers may have L2 connections to each other via a 3rd party device or provider
- In this case the router cannot directly detect the state of the link, since the ether port will always be running irrespective of the link state

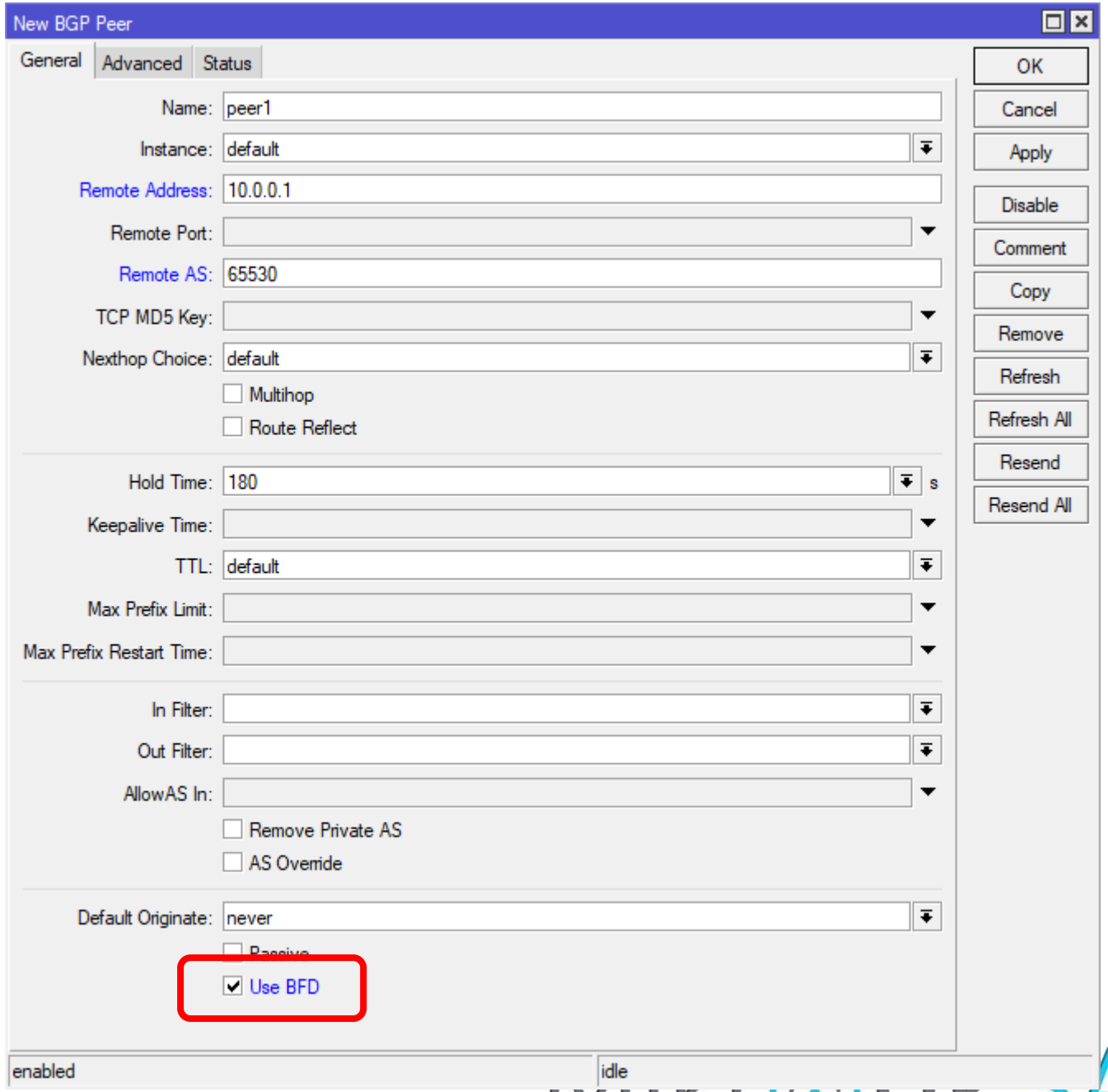


MikroTik SA

BFD

- Protocols like BGP and OSPF will use peer state monitoring to detect peer down state – this could take some time
  - OSPF Dead Interval is 40s, BGP standard peer Hold Time is 180s
- Both OSPF and BGP support Bidirectional Forwarding Detection
- This allows rapid signalling to the upper level protocols in the event of intermediate link failure that could not normally be detected i.e. physical interface is not in the down state
- BFD should be set on both sides of the link


OSPF <ether1>
General
Status
Interface: ether1
Cost: 10
Priority: 1
Authentication: none
Authentication Key:
Authentication Key ID: 1
Network Type: ptmp
Instance ID: 0
Passive
Use BFD
Retransmit Interval: 5 s
Transmit Delay: 1 s
Hello Interval: 10 s
Router Dead Interval: 40 s
OK
Cancel
Apply
Disable
Comment
Copy
Remove
enabled
passive
State: down


New BGP Peer
General
Advanced
Status
Name: peer1
Instance: default
Remote Address: 10.0.0.1
Remote Port:
Remote AS: 65530
TCP MD5 Key:
Nexthop Choice: default
Multihop
Route Reflect
Hold Time: 180 s
Keepalive Time:
TTL: default
Max Prefix Limit:
Max Prefix Restart Time:
In Filter:
Out Filter:
AllowAS In:
Remove Private AS
AS Override
Default Originate: never
Passive
Use BFD
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Refresh
Refresh All
Resend
Resend All
enabled
idle

Traffic Engineering

- OSPF-TE is an extension to OSPF that allows for traffic engineering
- MPLS networks can be built on top of OSPF, and along with OSPF-TE, more information about the topology can be exchanged such as bandwidth limitations and reservations on specific interfaces
- In the Resource Reservation Protocol (RSVP), OSPF-TE is used for recording and flooding RSVP signaled bandwidth reservations for label switched paths within the link-state database.

MikroTik SA

BGP

- Border Gateway Protocol
- Uses Path Vector implementation
- Exterior BGP (eBGP) for routing across the Internet
- Interior BGP (iBGP) for carrying information between eBGP routers
- Native support for IPv4 and IPv6
- Only protocol that can handle an Internet sized network

MikroTik SA

BGP Theory

- Border Gateway Protocol is used to Exchange routing information for the internet and is the protocol used between ISP's which are different Autonomous Systems.
- The protocol can connect any internetwork of AS using an arbitrary topology.
- The only requirement is that each AS have at least one router that is able to run BGP and that is router connect to at least one other AS's BGP router.
- BGP's main function is to exchange network layer reachability information (NLRI) with other BGP systems. BGP constructs an autonomous systems' graph based on the information exchanged between BGP routers.

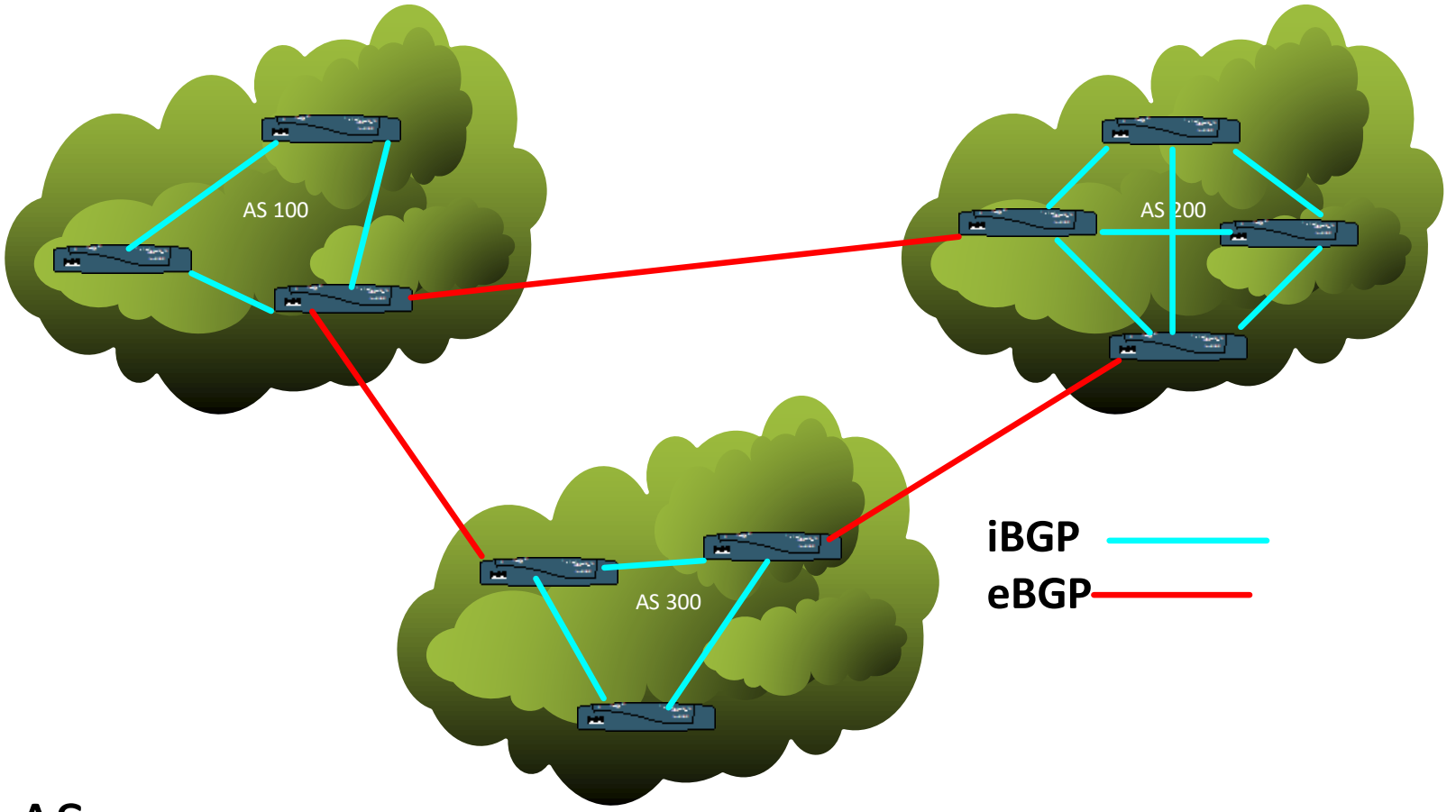
MikroTik SA

eBGP and iBGP

- Aside from building peering relationships and transporting data between two BGP speakers, two types of peering relationships exist within BGP: *interior peering* and *exterior peering*
- BGP sessions between peers within a single autonomous system are referred to as interior BGP, or iBGP
- BGP running between peers in different autonomous system are referred to as exterior BGP, or eBGP sessions
- iBGP is essentially required to carry information between eBGP peers across an Autonomous System

MikroTik SA

eBGP and iBGP



eBGP Between AS

iBGP internal to an AS

MikroTik SA

Path Vector Protocol

- BGP is primarily designed as a method to route between networks
- It cares only about the shortest path between networks, and not about the individual networks internal structure
- Thus it is the only protocol capable of handling networks the size of the Internet

MikroTik SA

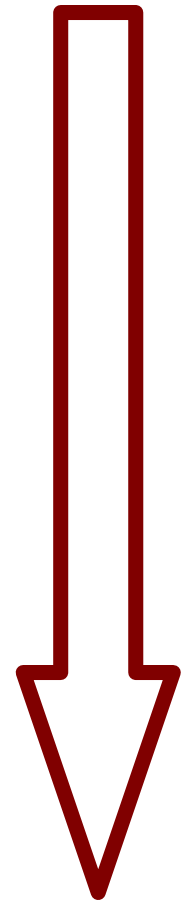
BGP as IGP

- iBGP can be configured as an interior protocol by distributing connected and static routes
- However there may be a few disadvantages as compared to a dedicated IGP (such as OSPF)
  - No dynamic neighbour discovery
  - Complex path selection process
  - Full mesh requirement or route reflector setup
  - Slow convergence compared to other IGP’s
  - No detection of link state when configured between loopbacks (recommended setup)

MikroTik SA

Best path selection

1. Next-hop validation --
2. Highest WEIGHT (default 0)
3. Highest LOCAL-PREF – iBGP Attribute
4. Shortest AS-PATH – eBGP Attribute
5. Prefer locally sourced route (via aggregate or BGP network)
6. Lowest origin type (EGP, IGP, Incomplete in that order)
7. Lowest MED – eBGP Attribute
8. Prefer eBGP over iBGP
9. Prefer the route with lowest router ID or ORIGINATOR_ID
10. Shortest route reflection cluster (default 0)
11. Prefer the path that comes from the lowest neighbour address



MikroTik SA

MME

- MME (Mesh Made Easy) is a MikroTik routing protocol suited for IP level routing in wireless mesh networks
- It is based on ideas from B.A.T.M.A.N. (Better Approach To Mobile Ad-hoc Networking) routing protocol.
  - See https://www.open-mesh.net for more information about B.A.T.M.A.N.
- MME works by periodically broadcasting so called originator messages
- Routing information contained in a message consists of IP address of it's originator and optional list of IP prefixes.
- If a node receives an originator message it hasn't seen before, it rebroadcasts that message.

MikroTik SA

MME

- Unlike OLSR or other "traditional" proactive routing protocols, MME does not maintain network topology information.
- Consequently, MME is not able to calculate a routing table, and does not need to.
- Instead, it keeps tracks of packets received and their sequence numbers - to tell how many packets were lost.
- This way, from message loss statistics for all combinations of originators and single-hop neighbors, MME is able to find the best gateway to a particular destination.

MikroTik SA

MME

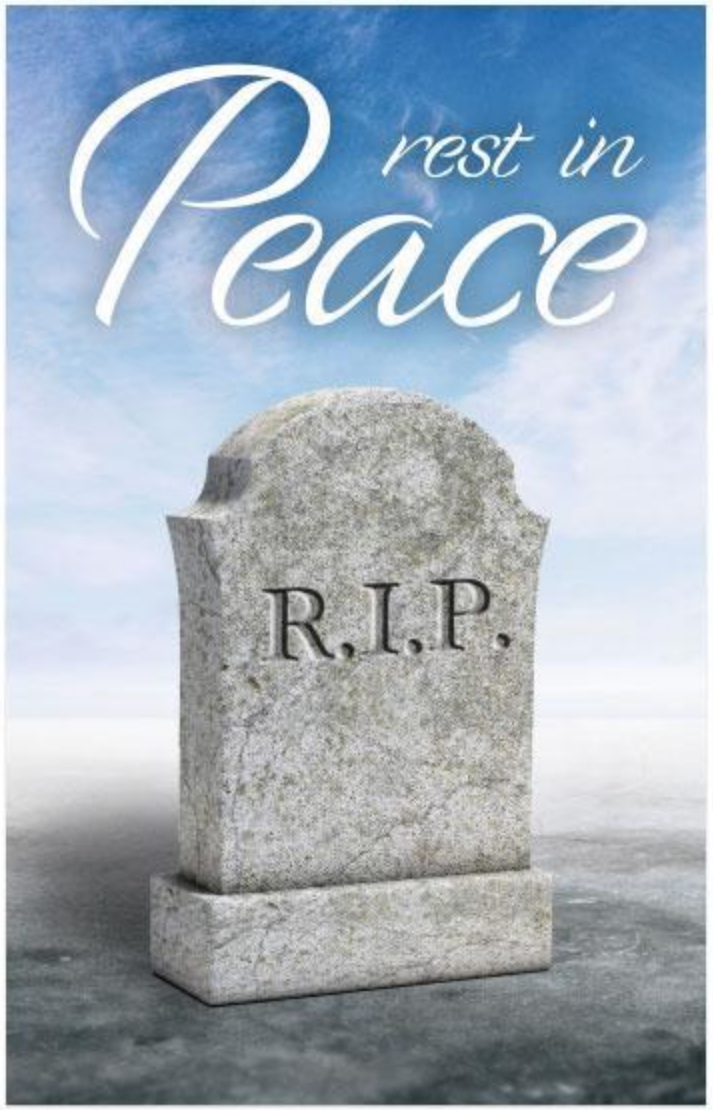
- The main ideas behind Mesh Made Easy are based on these observations made in mobile mesh networks:
  - it may be impossible to know the exact topology of all networks, as it is rapidly changing
  - if topology changes trigger routing table recalculation for all nodes in the network; and for embedded systems, the routing table calculation CPU overhead can be significant.
- To avoid these problems, an MME node:
  - cares only about the best single-hop neighbor in path to a particular destination;
  - avoids routing table calculations.
- Secondary functions of the MME protocol are:
  - to carry information about gateways to the Internet,
  - to dynamically setup default routes.

MikroTik SA

Practical Application

RIP

- Not much of an argument can be made to use RIP
- 15 hop limitation combined with constant resending of the full routing table and slow convergence of routes means it’s not very scalable and limited to small network setups
- However: it is very easy to setup and can be implemented in a few steps
- Maybe we should call it Rest In Peace protocol and leave it there…



MikroTik SA

MME

- From the MikroTik Wiki: *MME is not a replacement for OSPF or RIP. It is meant to be used in mesh networks, and is best suited for wireless nodes with one logical interface. When used in traditional networks, the protocol overhead will be greater than even that of RIP*
- Only recommended in wireless mesh networks where network conditions are changing rapidly
  - Latency increases/decreases
  - Link flaps / disconnects / reconnects
  - Roaming mesh devices

MikroTik SA

OSPF

- Widely deployed routing protocol
- Can converge a network in a few seconds and guarantee loop-free paths
- Rapid topology updates based on state of links (interfaces)
- Many features that allow the imposition of policies about the propagation of routes that it may be appropriate to keep local, for load sharing, and for selective route importing
- Hierarchical structure by using OSPF Areas
- Different network types (Broadcast, NBMA, PTP, PTMP) allow for different network setups
- Compatible with BFD for rapid detection of link failures when the intermediate L2 network is not controlled directly

MikroTik SA

Vote for OSPF?

- Well established Interior Gateway Protocol
- Easily deployed in any routed network
- Open standard compatible with a wide range of vendors
- Support for IPv4 and IPv6
- Offers rapid convergence, great performance
- Useful for carrying iBGP messages between eBGP routers when loopback addressing is used (recommended for iBGP)
- Allows for additional services such as MPLS, VPLS Pseudowires, Traffic Engineering to be rapidly deployed on existing networks

MikroTik SA

Vote for BGP?

- Only real choice for an Exterior Gateway Protocol
- Uses complex decision algorithms to determine best path (Weight, Local-pref, AS-path, MED etc.)
- Can be used as an IGP with some additional configuration (but was never really designed as such
- Compatible with BFD for rapid detection of link failures when the intermediate L2 network is not controlled directly
- iBGP can be combined with OSPF and MPLS to provide BGP signaled VPLS tunnels and VRF's that can be rapidly deployed in enterprise networks

Hybrid Network Setup

- Possibility to combine OSPF as core network protocol and BGP as edge network (client facing) protocol
- i.e. use OSPF to manage routing within you core, providing rapid convergence and fast link state updates;
- While using BGP to carry client ranges across your core network, thus isolating core routes from client routes

MikroTik SA

Conclusion

- There is no 1 best protocol for all
- Each protocol has advantages and disadvantages
- Use the best protocol for your current network setup, or combine them if required

More Information

- Questions / comments – it will all be fixed in ROS7

Contact me

http://trainwireless.com for latest training dates and information

training@mikrotiksa.com for any queries

david@mikrotiksa.com – my personal email

083 456 2002 – my number, although I don't have the best record of answering calls…

MikroTik SA