



ArchiTechs

MANAGED SERVICES

www.iparchitech.com 1-855-MIKROTIK

Effective Virtual Route Forwarding

PRESENTED BY:

SCOTT HAMMERSLEY, NETWORK ARCHITECT

IP ARCHITECHS MANAGED SERVICES



ArchiTechs
MANAGED SERVICES

1-855-MIKROTIK
www.iparchitech.com

Background

Scott Hammersley

- Working in the industry for over 15 years.
- Thorough knowledge of industry standards, protocols and best practices
- Complete background of high level routing and switching; BGP, OSPF, MPLS etc
- Mainly focused on Cisco, Adtran, Lucent and ZyXEL, etc. then;
- Introduced to MikroTik products and RouterOS a few years ago.
- Certifications: MTCNA, MTCRE, MTCWE, MTCTCE, ATSA-IN, ATSA-wLAN



ArchiTechs
MANAGED SERVICES

1-855-MIKROTIK
www.iparchitech.com

IP ArchiTechs Managed Services

- The first Carrier-Grade 24/7/365 MikroTik TAC (Technical Assistance Center)
 - Three tiers of engineering support
 - Monthly and on-demand pricing available
 - 1-855-MIKROTIK or support.iparchitech.com
- Private Nationwide 4G LTE MPLS backbone
 - Partnership with Verizon Wireless - available anywhere in the Verizon service area
 - Not Internet facing – privately routed over our MPLS infrastructure
 - Point-to-Point or Point-to-MultiPoint
- Proactive Monitoring / Ticketing / Change Control / IPAM
- Carrier-Grade Network Engineering / Design in large (10,000+ nodes) environments
- Training

24/7/365 MikroTik TAC | Nationwide Private 4G LTE MPLS | Proactive Network Monitoring | Design / Engineering / Operations



What is 'Virtual Route Forwarding'

- Virtual Route Forwarding, or VRF for short, is a mechanism to virtually segregate your L3 traffic.
- This allows you to have many instances of routing tables that co-exist on the same router.
- A routing table uses a FIB (forwarding information base), so, each VRF uses its own FIB.
- These are not accessible to other routing tables present without special configuration.
- When implemented properly, becomes a very effective tool to segregate traffic without the need to use multiple routers.



ArchiTechs
MANAGED SERVICES

1-855-MIKROTIK
www.iparchitech.com

How can VRF's benefit you!

- Triple play designs – Voice is critical, Video is intensive, Data is just data.
- Management Segregation – Why would you want your customers managing your core!
- Customer Segregation – Customer 'A' doesn't need to know about Customer 'B', EVER!

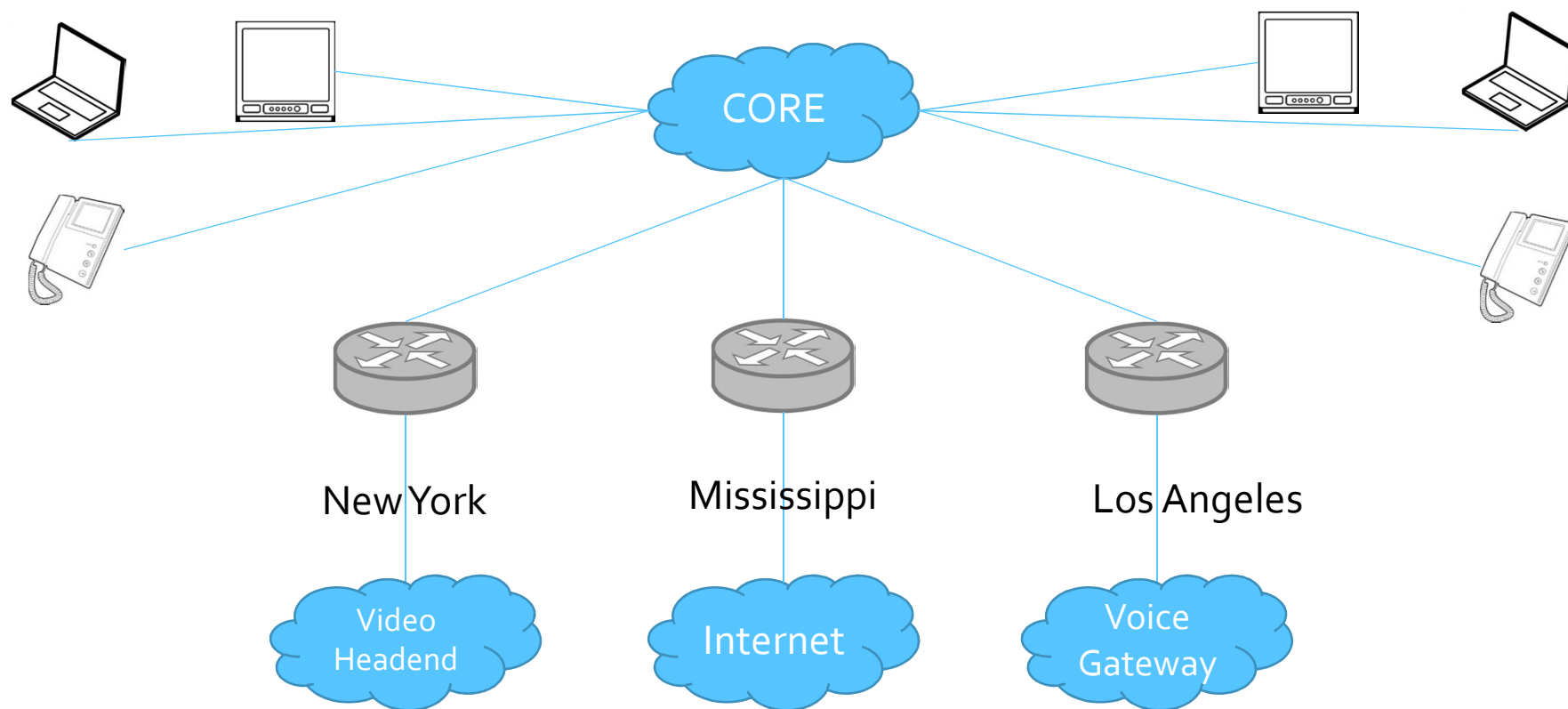
These are just a few reasons/benefits to use VRF's when available to you.



ArchiTechs
MANAGED SERVICES

1-855-MIKROTIK
www.iparchitech.com

Contemplate This...



24/7/365 MikroTik TAC | Nationwide Private 4G LTE MPLS | Proactive Network Monitoring | Design / Engineering / Operations



ArchiTechs
MANAGED SERVICES

1-855-MIKROTIK
www.iparchitech.com

Design Consideration Questions

Below are some of the most common design considerations when implementing VRF's in your network:

- How do I cross VRF's if needed?
- Where do I allow the entry and exit points for each VRF?
- How do I tell other nodes in my network about routes for a certain VRF that exist on another node?
- What type of security do I need to protect my VRF's?



ArchiTechs
MANAGED SERVICES

1-855-MIKROTIK
www.iparchitech.com

Design Consideration Answers

- How do I cross VRF's if needed?

This is where a dedicated router/firewall comes in handy. This way, traffic crossing the VRF's is tightly monitored and security can be applied easily. Something a Meta-Router in MikroTik can come in handy for!!!

- Where do I allow the entry and exit points for each VRF?

You see we have our Internet gateway in Mississippi, Voice gateway located in Los Angeles, and our Video headend in New York, guess where you would allow the exit points??!! The entry points are the customers that need access to the different services.

Simple Right!



Design Consideration Answers

- How do I tell other nodes in my network about routes for a certain VRF that exist on another node?

While VRF's on their own are neat, using BGP to advertise each VRF's table to other nodes is neater. This way, all nodes know about each others routes, for each VRF routing instance!!!

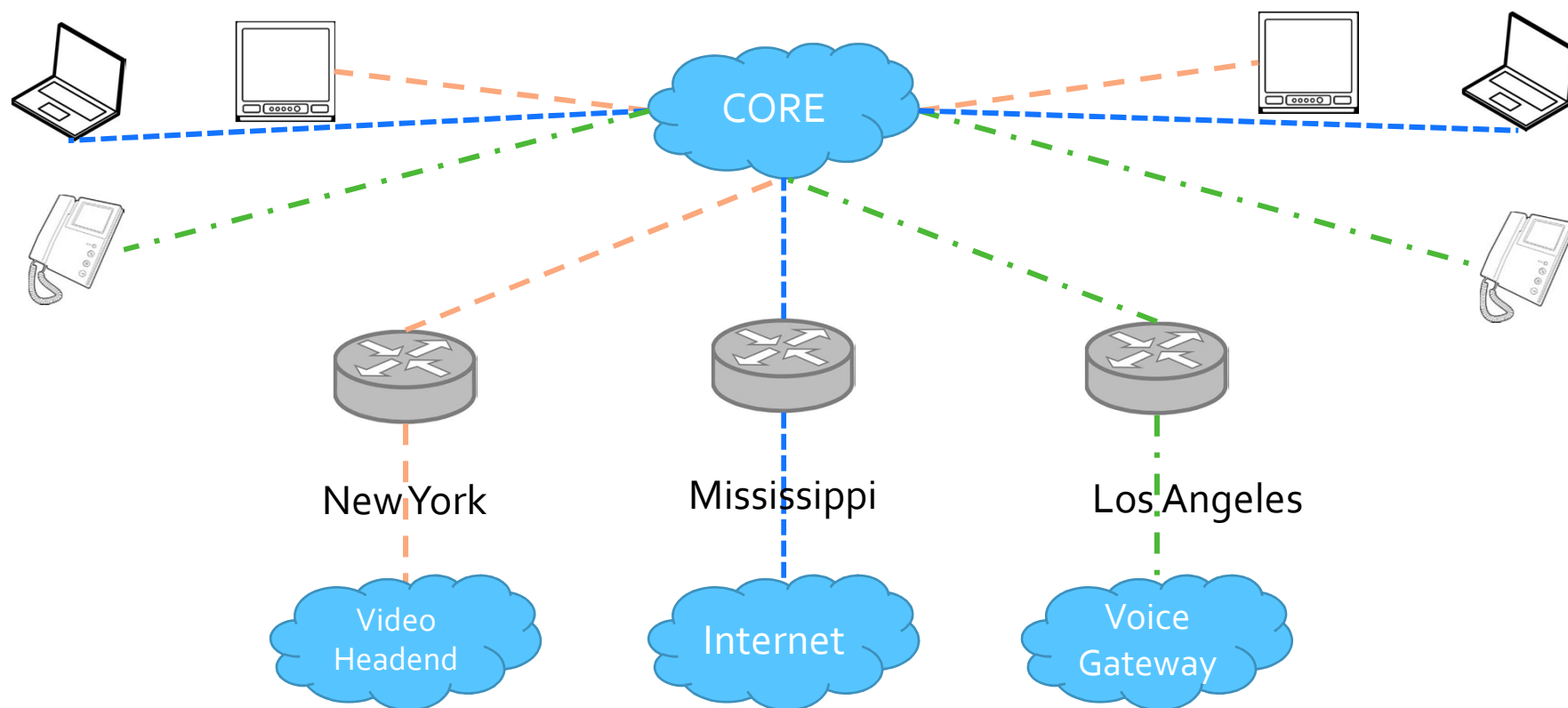
- What type of security do I need to protect my VRF's?

Again, we would handle this at the firewall. A rule of thumb is; try not to allow routes to cross tables by route leaking. This is what firewalls are good at. While it is perfectly legal and technically possible, we do not advocate route leaking unless absolutely necessary. It ends up becoming a nightmare to manage and possibly (while inadvertently) cause a security loop hole.



Becomes This...

- Video_VRF
- Internet_VRF
- Voice_VRF





ArchiTechs
MANAGED SERVICES

1-855-MIKROTIK
www.iparchitech.com

Lets Build It!!!

- The next slide depicts a network that was built in GNS3 using MikroTik RouterOS.
- Video Headend and Voice Gateway nodes are Cisco 7200 IOS acting as plain vanilla nodes.

FYI, we build all test and deployment networks in GNS3 before ever touching a production network.

Why???

BECAUSE IT MAKES SENSE



ArchiTechs

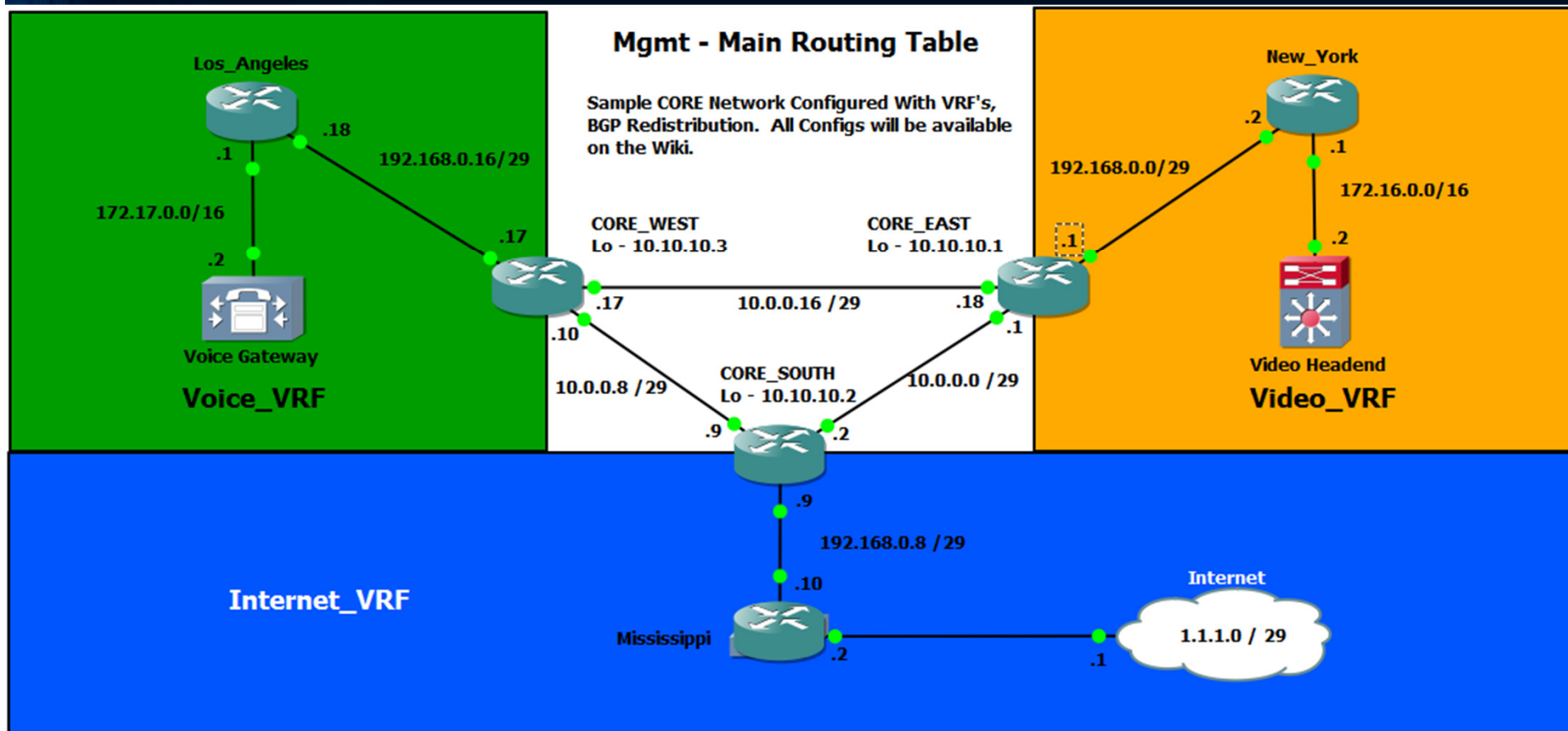
MANAGED SERVICES

1-855-MIKROTIK

www.iparchitech.com

Router VRF Configuration Examples:

Built Using MikroTik Router OS In A Virtual Lab Environment





Router VRF Configuration

- Using these VRF's allows transit communication to be separated. No application knows about each other.
- The CORE handles all L2/L3, uses BGP for its IGP and advertises all VRF information to each node participating in the BGP advertisement. At any entry point in the CORE you are able to leverage the known VRF's. Again, each VRF's routing instance is advertised AUTOMAGICALLY to each other using address-families.
- One immediate noticeable security plus is MGMT of the CORE is totally isolated.

Though the advertisement of the VRF's using BGP will be shown, because this presentation is focused on VRF's, we assume that all other ancillary configuration is already there (such as IP's, Other BGP etc.)

Now we will drill the config down. I am going to use just one node from the CORE to reference:



Router VRF Configuration

IP Address List:

Standard IP addresses used per the design of the LAB.

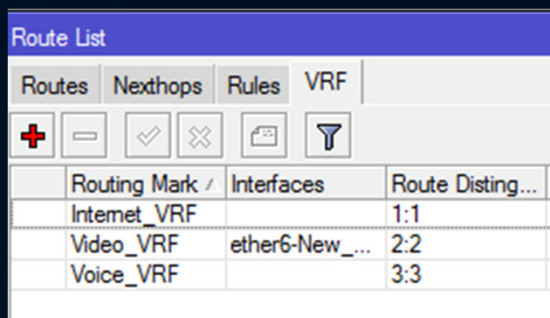
NOTE: Ether1 is used by GNS3 for mgmt connection to the RouterOS.

Address	Network	Interface
10.0.0.1/29	10.0.0.0	ether4-CORE_SOUTH
10.0.0.18/29	10.0.0.16	ether2-CORE_WEST
10.0.1.3/24	10.0.1.0	ether1
10.10.10.1	10.10.10.1	Lo0
192.168.0.1/29	192.168.0.0	ether6-New_York



Router VRF Configuration

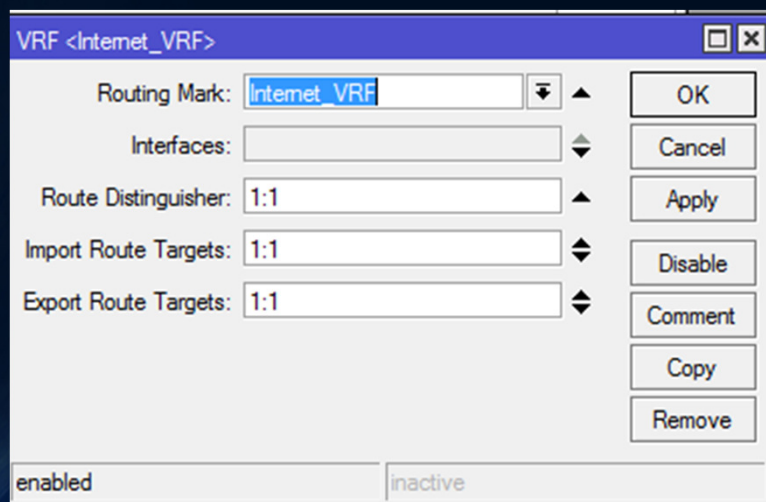
VRF Config In the Route List:



Routes	Nexthops	Rules	VRF
+	-	✓	✗
Routing Mark /	Interfaces	Route Disting...	
Internet_VRF		1:1	
Video_VRF	ether6-New_...	2:2	
Voice_VRF		3:3	

Here we define the VRF's.

For each VRF you want define the name and interfaces to belong to that VRF



VRF <Internet_VRF>

Routing Mark: Internet_VRF

Interfaces:

Route Distinguisher: 1:1

Import Route Targets: 1:1

Export Route Targets: 1:1

enabled inactive

The route distinguishers are used to identify the VRF throughout the routing tables and allow the likes of BGP to advertise out the instances to other nodes.



Router VRF Configuration

BGP VRF Configuration Screen:

Quick view of the BGP VRF config.

This tells BGP what to advertise to other nodes.

The screenshot shows the 'BGP' configuration window with the 'VRFs' tab selected. It contains a table with columns: Instance, Routing Mark, and Out Filter. The table lists three VRFs: 'default' with 'Internet_VRF', 'default' with 'Video_VRF', and 'default' with 'Voice_VRF'.

Instance	Routing Mark	Out Filter
default	Internet_VRF	
default	Video_VRF	
default	Voice_VRF	

The screenshot shows the 'BGP VRF <default>' configuration dialog box. It has fields for 'Instance' (set to 'default') and 'Routing Mark' (set to 'Internet_VRF'). There are checkboxes for 'Redistribute Connected' (checked), 'Redistribute Static' (checked), 'Redistribute RIP' (unchecked), 'Redistribute OSPF' (unchecked), and 'Redistribute Other BGP' (unchecked). There is also an 'Out Filter' dropdown menu. At the bottom, there is an 'enabled' checkbox. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'.

For each VRF advertisement, what do you want to actually advertise.

Here I just wanted any connected routes and static routes to be known by other nodes participating in the address-family advertisements in the CORE.



Router VRF Configuration

BGP Peers Throughout The CORE:

Quick look at the Peers in BGP.

admin@10.0.1.3 (CORE_EAST) - WinBox v5.19 on x86 (x86)

Safe Mode

Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
ISDN Channels

BGP

Instances VRFs Peers Networks Aggregates VPN4 Routes Advertisements

+ - ✓ ✕ [icon] Refresh Refresh All Resend Resend All Find

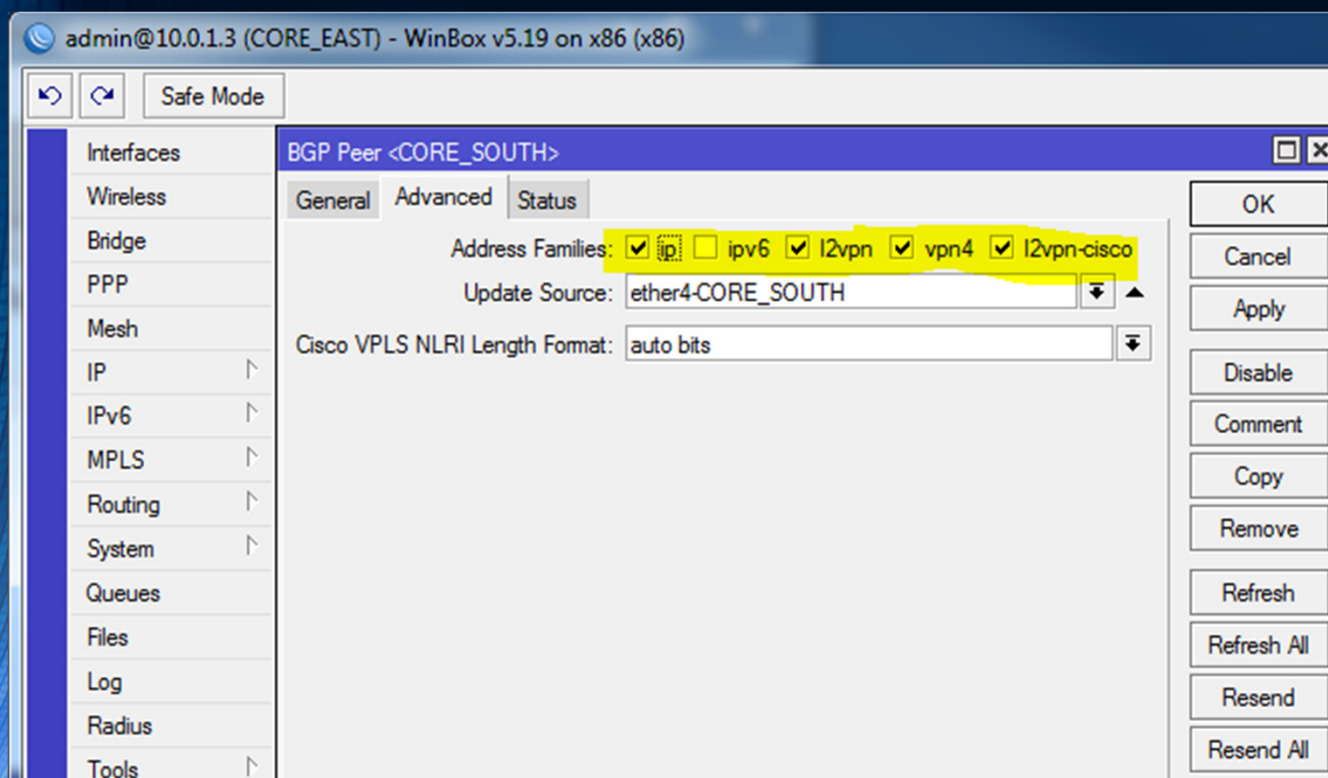
Name	Instance	Remote Address	Remote AS	M...	R...	TTL	Remote ID
CORE_S...	default	10.0.0.2	65530	no	no	d...	10.10.10.2
CORE_W...	default	10.0.0.17	65530	no	no	d...	10.10.10.3

2 items



Router VRF Configuration

BGP Peers Throughout The CORE:



In order for BGP to actually advertise the VRF's, vpnv4 must be selected.

We just like to make sure we allow l2vpn and l2vpn-cisco also. Especially when using MPLS/VPLS etc.



Router VRF Configuration

VPNv4 Routes In BGP, Advertising VRF's

BGP doing its thing!

You can see the route-distinguishers we set earlier under 'IP Routes, VRF'.

admin@10.0.1.3 (CORE_EAST) - WinBox v5.19 on x86 (x86)

Safe Mode

Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
ISDN Channels

BGP

Instances VRFs Peers Networks Aggregates VPN4 Routes Advertisements

Find

	Route Dist...	Dst. Address	Gateway	Interface	In Label	Out Label	
1:1		192.168.0.8/29	10.0.0.2	ether4-CORE...	16	16	
2:2		192.168.0.0/29		ether6-New_...	16	0	
2:2		172.16.0.0/16	192.168.0.2	ether6-New_...	17	0	
3:3		192.168.0.16...	10.0.0.17	ether2-CORE...	16	16	
3:3		172.17.0.0/16	10.0.0.17	ether2-CORE...	17	17	

5 items



Router VRF Configuration

End Result Of VRF Routes In The Routing Table:

And Finally, the route table showing the learned VRF routes from the other nodes.

Pretty isn't it!!! It's a Kinda Magic!

Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAC 10.0.0.0/29	ether4-CORE_SOUTH reachable	0		10.0.0.1
Db 10.0.0.0/29	10.0.0.2 reachable ether4-CORE_SOUTH	200		
DAb 10.0.0.8/29	10.0.0.2 reachable ether4-CORE_SOUTH	200		
Db 10.0.0.8/29	10.0.0.17 reachable ether2-CORE_WEST	200		
DAC 10.0.0.16/29	ether2-CORE_WEST reachable	0		10.0.0.18
Db 10.0.0.16/29	10.0.0.17 reachable ether2-CORE_WEST	200		
DAC 10.0.1.0/24	ether1 reachable	0		10.0.1.3
Db 10.0.1.0/24	10.0.0.2 reachable ether4-CORE_SOUTH	200		
Db 10.0.1.0/24	10.0.0.17 reachable ether2-CORE_WEST	200		
DAC 10.10.10.1	Lo0 reachable	0		10.10.10.1
DAb 10.10.10.2	10.0.0.2 reachable ether4-CORE_SOUTH	200		
DAb 10.10.10.3	10.0.0.17 reachable ether2-CORE_WEST	200		
AS 172.16.0.0/16	192.168.0.2 on Video_VRF reachable ether6-New_York	1	Video_VRF	
DAb 172.17.0.0/16	10.0.0.17 reachable ether2-CORE_WEST	200	Voice_VRF	
DAC 192.168.0.0/29	ether6-New_York reachable	0	Video_VRF	192.168.0.1
DAb 192.168.0.8/29	10.0.0.2 reachable ether4-CORE_SOUTH	200	Internet_VRF	
DAb 192.168.0.16/...	10.0.0.17 reachable ether2-CORE_WEST	200	Voice_VRF	



ArchiTechs
MANAGED SERVICES

1-855-MIKROTIK
www.iparchitech.com

Final Take Away's

- VRF's greatly enhance the usefulness of your network and can increase your selling point to customers looking for a 'Private Virtual Network' throughout a geographically disperse provider.
- If you want all your nodes to be 'AWARE' of the other VRF's instances in your network, BGP is required to populate those tables.
- If you need to cross VRF's, we suggest using a separate firewall (again, you could leverage a Meta Router for this!!!).



ArchiTechs
MANAGED SERVICES

1-855-MIKROTIK
www.iparchitech.com

Thank You!

The following will be available on the Wiki!!!

- This presentation (obviously).
- All config's that I created for this presentation.
- GNS3 topology (Although, for the Voice and Video Gateway nodes a Cisco image will be required. We can not legally provide that).

Thank you for listening,

Questions??

Don't Go Anywhere, There's MORE!!!!!!



ArchiTechs
MANAGED SERVICES

1-855-MIKROTIK
www.iparchitech.com

2013 St Louis MUM –Tablet Giveaway !!

- One 7" Android .TAB Nero will be given away on Sep 19th and one on Sep 20th
- Stop by the IP ArchiTechs exhibition booth, guess the right number and WIN!

