IP ArchiTechs

MANAGED SERVICES

www.iparchitechs.com

ISP Design – Using MikroTik CHR For highly avaliable SSTP Aggregation

PRESENTED BY:

SAŠA BLAGOJEVIĆ,
NETWORK ENGINEER

Profile: **About Saša Blagojević**

Background:

- 14+ years in Networking
- Worked mainly in WISP industry
- Designed/Built several WISP networks
- MikroTik Certified Trainer
- MikroTik Academy Trainer
- MikroTik Certifications: MTCNA, MTCRE, MTCWE, MTCTCE, MTCUME, MTCIPv6, MTCINE, MTCSE

Profile: About IP ArchiTechs

IP ArchiTechs
MANAGED SERVICES

Expert Networking

Whitebox | ISP | Data Center | Enterprise

- ✓ Global Consulting
- ✓ Managed Networks
- ✓ Monitoring
- ✓ Load Testing
- ✓ Development

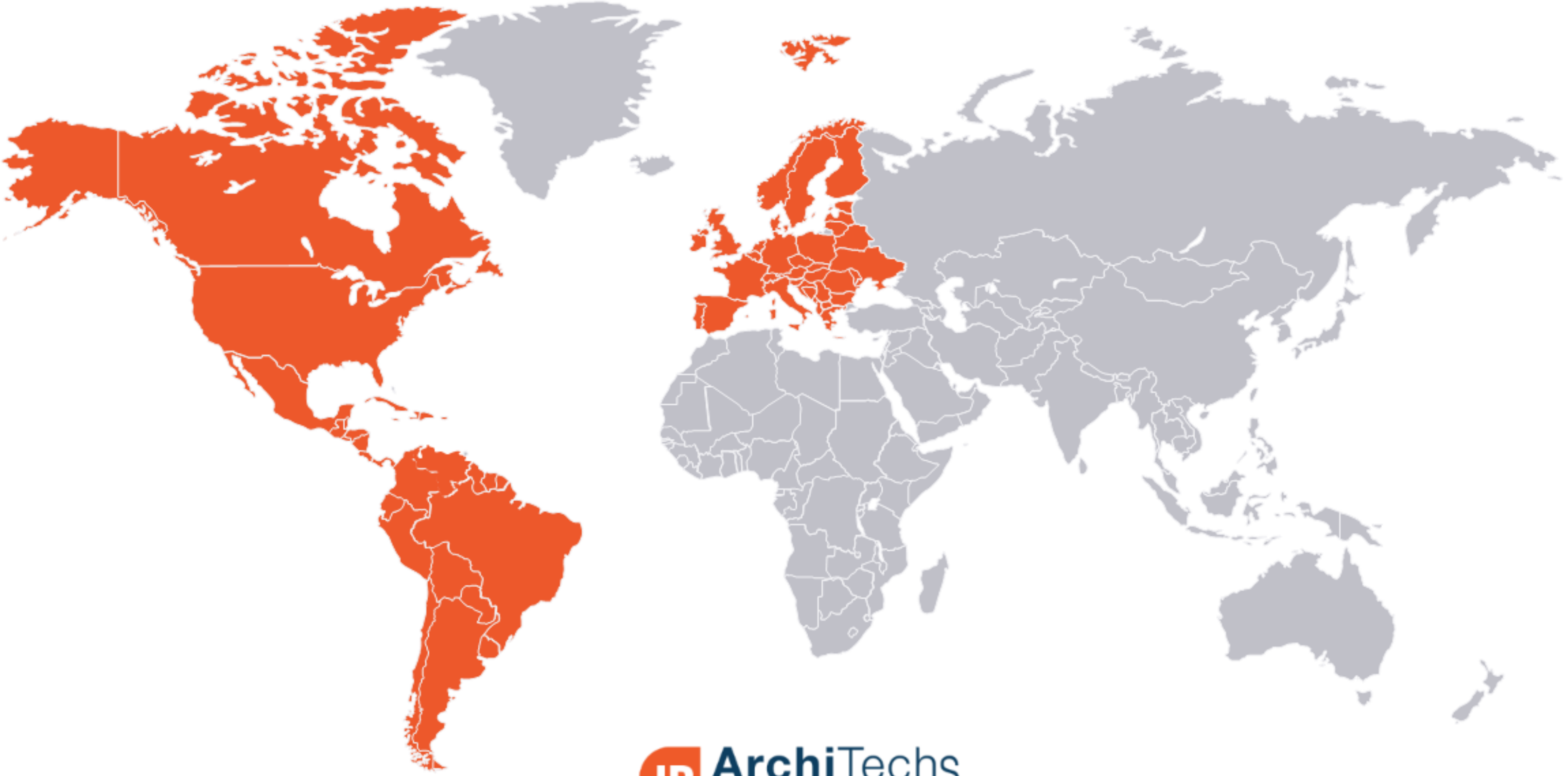
Locations in: US | Canada | South America

Call us at: +1 855-645-7684
E-mail: consulting@iparchitechs.com
Web: www.iparchitechs.com

Profile: About IP ArchiTechs

Now in Europe!

IPA Opened an office in Nis, Serbia in 2018



ArchiTechs
MANAGED SERVICES

North America - South America - Europe

Design: **Presentation goals**

Goal of this presentation: When the presentation is finished, hopefully you will have walked away with a few key concepts:

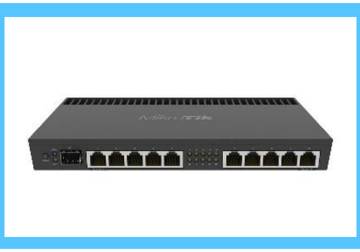
- Benefits of using virtualized platform for endpoint aggregation
- How to create a redundant system for SSTP aggregation
- You will able to choose right routing protocol
- Use scripting to automate processes

Design: **CHR vs. Hardware for MPLS?**

- Which platform is better?
- Throughput capabilities?
- x86 CPU vs. ARM/Tilera?
- MTU/Throughput concerns on different Hypervisors

vs.

Design: CHR vs. Tilera/ARM for MPLS?

Platform	MikroTik CHR		
CPU MPLS router CPU requirements depend on load and explicit/implicit null	**x86** Better for heavy computational work. Higher power draw.	**Tilera** Optimized for packet transfer. Designed to be low power draw.	**ARM** In between x86 and Tilera for performance.
Throughput At 1530 bytes (L2), and 8970 bytes (L2)	**x86** More CPU and power is required to move data at the same speed as a CCR	**Tilera** Handles throughput at different frame sizes slightly better than x86	**ARM** Handles throughput at different frame sizes similar to Tilera
MTU Handling	**x86** x86 hardware and HV can typically support up to 9000 MTU.	**Tilera** Supports up to 10222	**ARM** Supports up to 9982

Design: **Why CHR?**

Here at IPA we have performed extensive testing in our lab between physical hardware such as the CCR1036 and CCR1072, Cisco 7600's etc. We have found that virtualizing functions such as PPPoE, SSTP, (Hotspot etc) significantly improves the performance and handling RouterOS specifically.

So with that, we recommend the CHR. This also benefits when implementing HA requirements as virtual resources can be spun up with the need for physical intervention.

There are plethora of options available for x86 hardware to run CHR. If you want to build a LAB, eBay is a resource for used servers. However, if you are building for production, we recommend the Maxxwave Venegeance from Baltic Networks…

Design: **Choose right VPN protocol?**

Plenty of options

- PPTP
  - Considered obsolete
  - Has many well known security issues
- SSTP
  - SSL/TLS encryption
  - Uses TCP port 443 (pass through virtually all firewalls)
- L2TP
  - Does not provide encryption by itself
  - With IPsec can provide encryption and uses UDP 500,1701,4500
- OpenVPN
  - Very strong encryption
  - Uses port TCP 1194

Design: **What is SSTP?**

- Secure Socket Tunneling Protocol, also known as SSTP, is one of the most secure protocols used in VPN tunneling.
- The protocol, though owned by Microsoft, is available to both Linux and Mac users.
- SSTP uses SSL/TLS (Secure Socket Layer/Transport Layer Security) channel over TCP 443 port same as HTTPS traffic.
- SSTP is often compared to OpenVPN thanks to the high level of security it offers, and the fact that it can bypass NAT firewalls.
- SSTP offers good speeds if you have enough bandwidth.

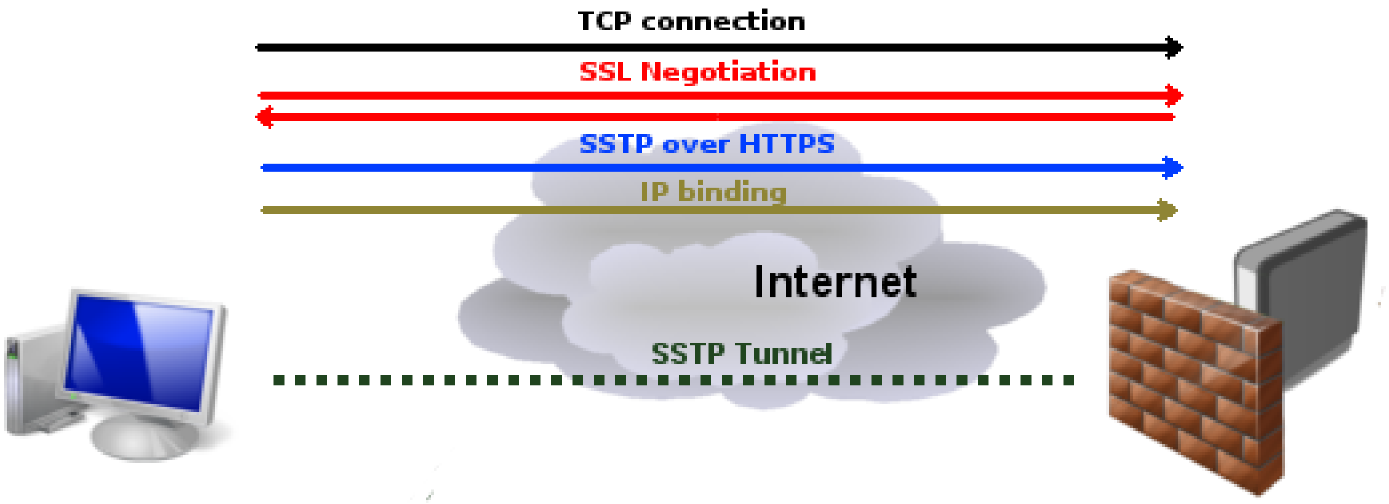
Design: **Some benefits of using SSTP**

- SSTP encryption offers a decent level of security, almost on par with OpenVPN (SSL 3.0 + 256-bit encryption).
- SSTP is easy to configure on platforms it is built into.
- The SSTP VPN protocol is very difficult to block because it uses TCP port 443 (the same one HTTPS uses).
- Unlike the OpenVPN, this protocol won't slow down your connections even though it uses more advanced techniques of protection.
- Despite SSTP was developed by Microsoft, SSTP remains compatible with other operating systems as well
- In Mikrotik to Mikrotik site to site connections you don't need certificates to establish VPN tunnel

Design: **Some drawbacks of using SSTP**

- SSTP is closed-source and solely owned by Microsoft
- It is possible for your username and password to be intercepted at public places (unsecured hotspots)

Design: **Basic operation of SSTP**



- TCP connection is established from client to server (by default on port 443)
- SSL validates server certificate. If certificate is valid connection is established otherwise connection is torn down. (But see note below)
- The client sends SSTP control packets within the HTTPS session which establishes the SSTP state machine on both sides.
- PPP negotiation over SSTP. Client authenticates to the server and binds IP addresses to SSTP interface
- SSTP tunnel is now established and packet encapsulation can begin.

Design: **What problem are we trying to solve?**

- Designing the network to support redundancy means we are tasked with making sure there are backup systems in place should our primary fail.
- Choose as much as possible secured VPN protocol while maintaining flexibility and easy configuration
- Support massive amount of the VPN clients
- Use dynamic routing protocol for sending endpoint prefixes to SSTP concentrators
- Automate processes as much as possible using scripting

Design: Choosing right routing protocol?

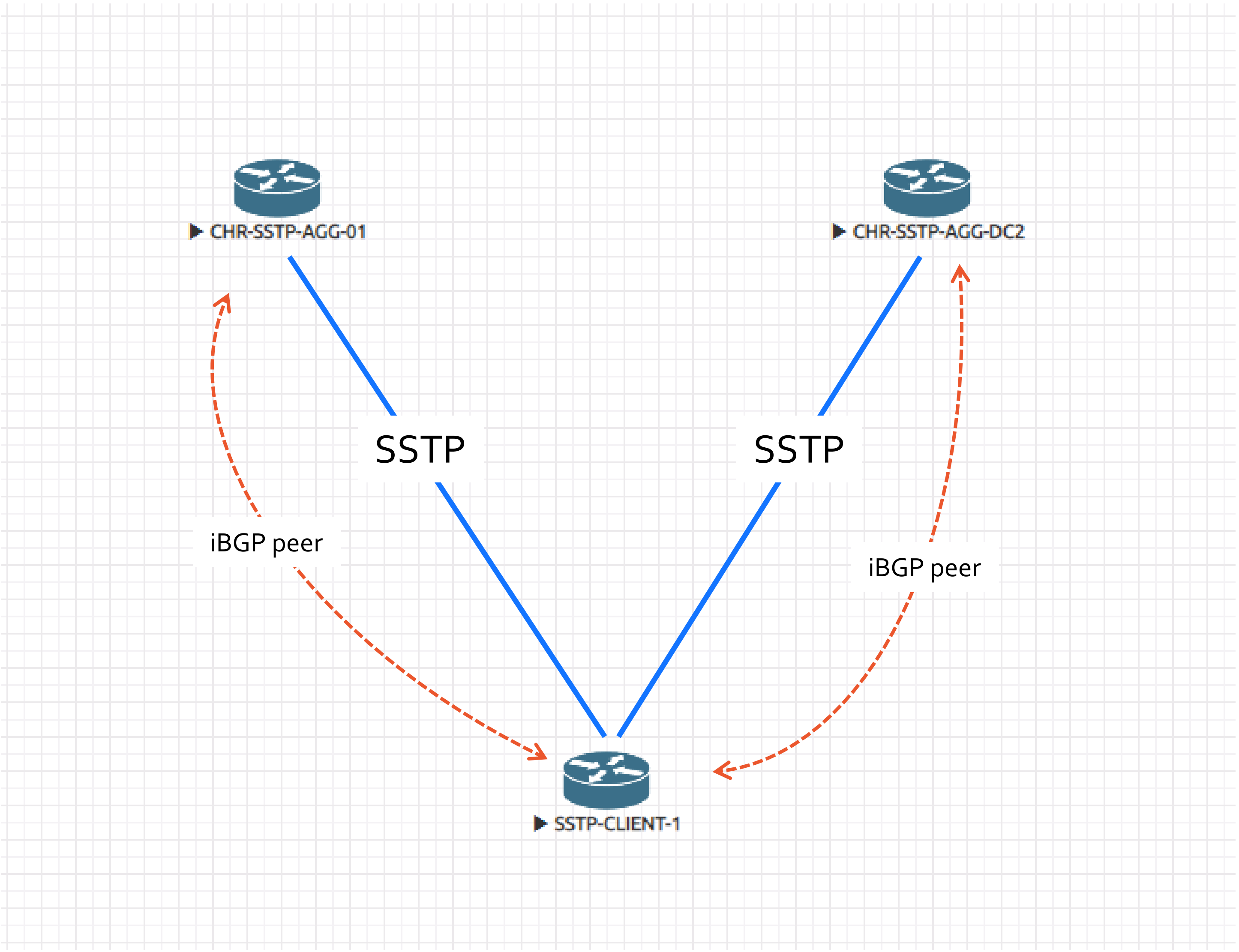
Protocol	OSPF	iBGP
Scalability	In VPN scenario like we have, ospf is not scalable cause changing on one endpoint will affect all endpoints	With routing filters we can easily manipulate what routes we are sending to endpoints
Easy to configure	Ospf is easy to configure	iBGP is harder to configure

Design: **Decisions…**

Design decisions:

- Use SSTP for VPN protocol
- Use CHR as platform for SSTP concentrators
- Using iBGP as IGP
- Use scripting to automate processes for iBGP peering and any other processes
- Simplify installation process of the endpoint

Design: **Logical design…**

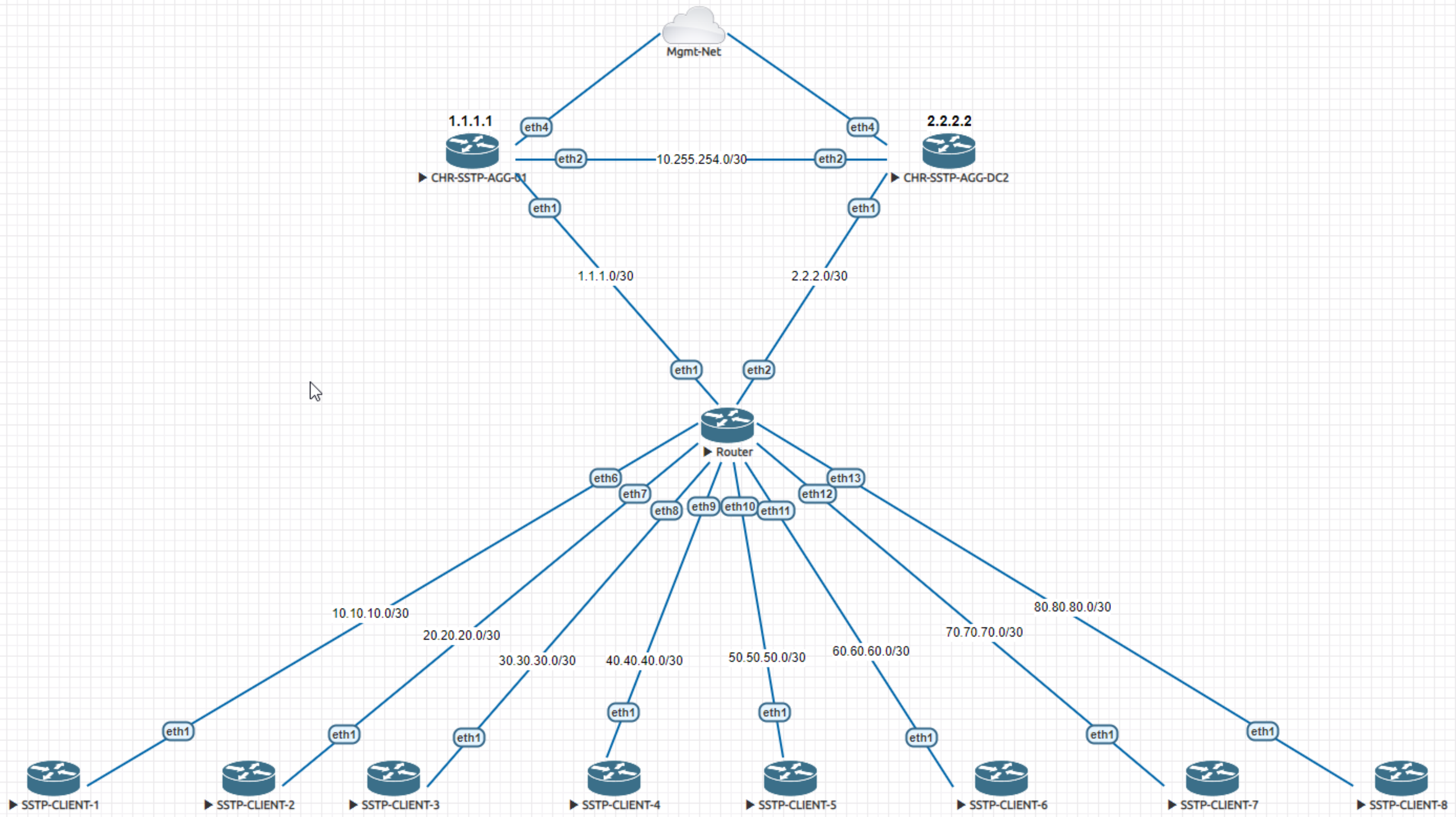


The Example Setup:

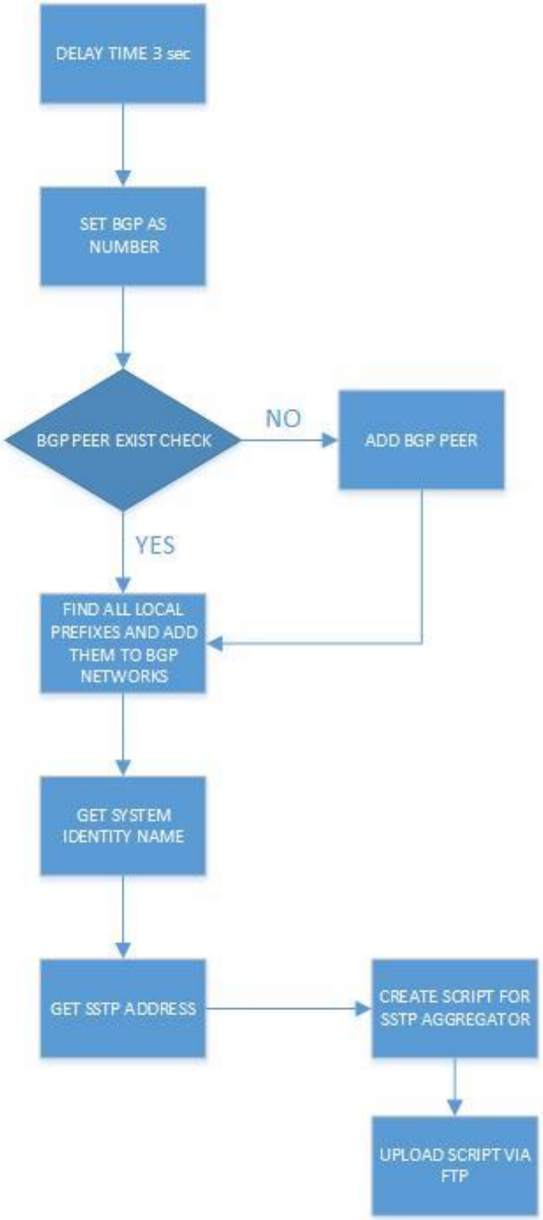
This lab was all built using EVE-NG..

2 MikroTik CHR’s configured as the SSTP concentrators, local authentication and IP assignments.
1 MikroTik CHR configured as a router, to have ip connectivity between SSTP clients and servers.
8 MikroTik CHR’s configured as SSTP Clients with a script to automatically connect to ftp and send bgp peer data to CHR aggregation routers
All CHR’s configured with one (1) CPU and 256M RAM on MikroTik free license level.

Design: **Setup-Physical connections…**



Design: **Setup-Scripting Algorithm…**



DELAY TIME 3 sec

SET BGP AS NUMBER

BGP PEER EXIST CHECK

NO

ADD BGP PEER

YES

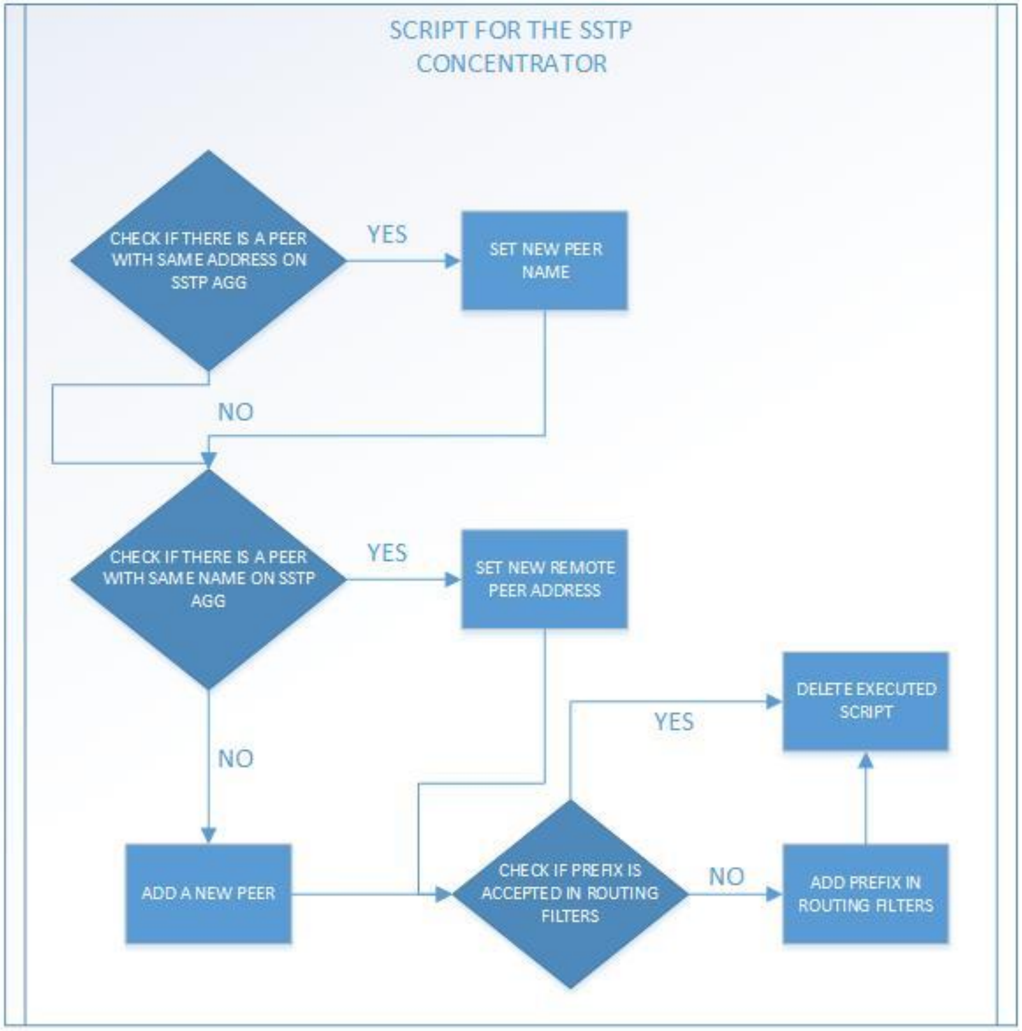
FIND ALL LOCAL PREFIXES AND ADD THEM TO BGP NETWORKS

GET SYSTEM IDENTITY NAME

GET SSTP ADDRESS

CREATE SCRIPT FOR SSTP AGGREGATOR

UPLOAD SCRIPT VIA FTP



SCRIPT FOR THE SSTP CONCENTRATOR

CHECK IF THERE IS A PEER WITH SAME ADDRESS ON SSTP AGG

YES

SET NEW PEER NAME

NO

CHECK IF THERE IS A PEER WITH SAME NAME ON SSTP AGG

YES

SET NEW REMOTE PEER ADDRESS

NO

ADD A NEW PEER

CHECK IF PREFIX IS ACCEPTED IN ROUTING FILTERS

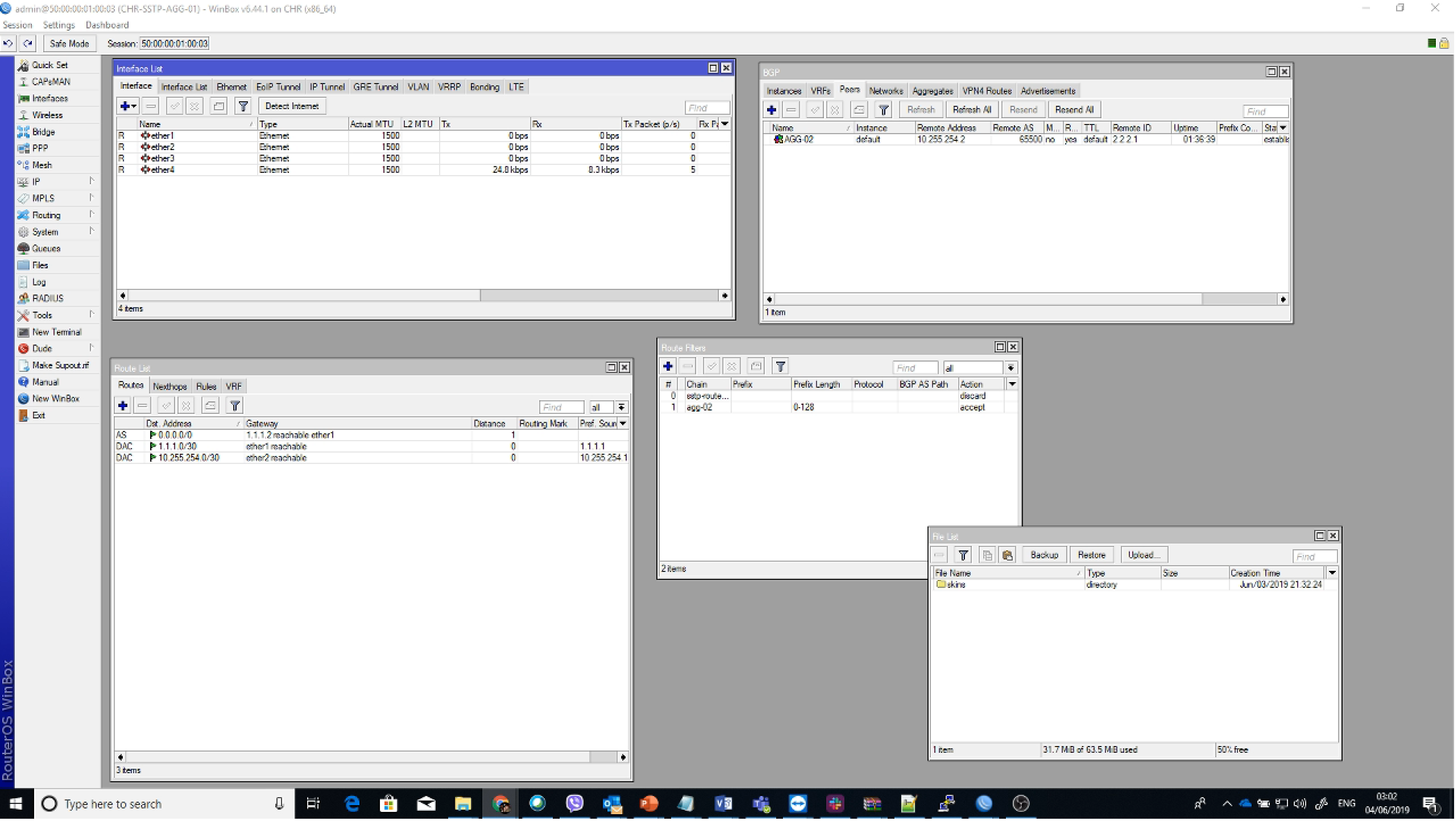
YES

DELETE EXECUTED SCRIPT

NO

ADD PREFIX IN ROUTING FILTERS

Design: **Setup-Scripting Algorithm…**



Interface List

	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx P
R	ether1	Ethernet	1500		0 bps	0 bps	0	
R	ether2	Ethernet	1500		0 bps	0 bps	0	
R	ether3	Ethernet	1500		0 bps	0 bps	0	
R	ether4	Ethernet	1500		24.8 kbps	8.3 kbps	5	

4 items

BGP

Name	Instance	Remote Address	Remote AS	M...	R...	TTL	Remote ID	Uptime	Prefix Co...	Sta
AGG-02	default	10.255.254.2	65500	no	yes	default	2.2.2.1	01:36:39		establis

1 item

Route List

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Sour
AS	0.0.0.0/0	1.1.1.2 reachable ether1	1		
DAC	1.1.1.0/30	ether1 reachable	0		1.1.1.1
DAC	10.255.254.0/30	ether2 reachable	0		10.255.254.1

3 items

Route Filters

#		Chain	Prefix	Prefix Length	Protocol	BGP AS Path	Action
0		sstp-route...					discard
1		agg-02		0-128			accept

2 items

File List

File Name	Type	Size	Creation Time
skins	directory		Jun/03/2019 21:32:24

1 item 31.7 MiB of 63.5 MiB used 50% free

Design: **Conclusion…**

This as we have discussed is due to several reasons. To be able to easily add high availability, load balancing system using virtual resources and CHR we can deploy effective solutions that meet the needs of clients.

Design: Questions?

Questions??