Bhaukaal Baba Technologies Pvt. Ltd.

www.bhaukaalbaba.com

About Bhaukaal Baba

- ITIL certified
- IT Resources and Network management and monitoring solutions
- Integrated Services and Solutions Provider
- Network designing and deployment for ISPs and Enterprise
- Also some Bhaukaal stuffs (Not flying in air with a broom)

Bhaukaal Baba Presence

- New Delhi (Corporate H.Q.)
- Mumbai (Network Control Centre)
- Pune
- Nagpur
- Chennai
- Kolkata
- Lucknow
- Patna
- Ranchi
- Ambikapur
- Bhubaneshwar
- Bangalore
- Jaipur
- Chandigarh

Bhaukaal Baba Area of Operations

- Bhaukaal Baba has served a wide range of clients from Government institutions, NGOs, SMEs, Enterprise and a few retail clients too.
- Bhaukaal Baba has provided IT and Network solutions and services to the clients.
- Bhaukaal Baba has presence in prominent Datacenters in India including but not limited to Tata Communications Datacenter, Netmagic, Nxtra, CtrlS, RicohDC, Sify, GPX Global and Webwerks.

Objectives

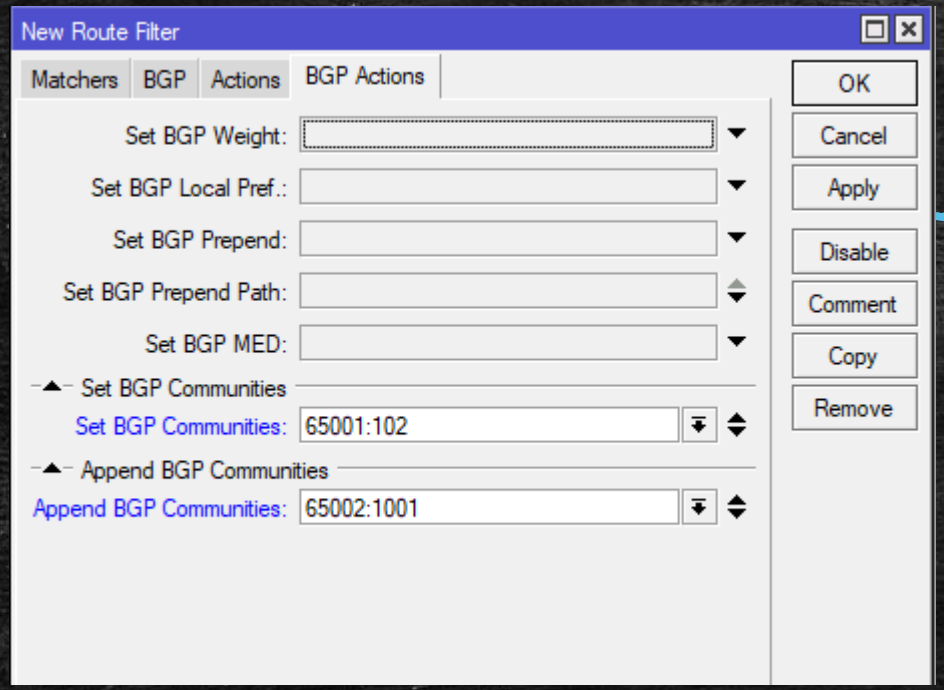
- Usage of BGP communities
- Common mistakes with BGP re-advertisement
- Simplified access management
- Setup VPN on a CHR for remote access
- Using radius to control who can access the device

Disclaimer

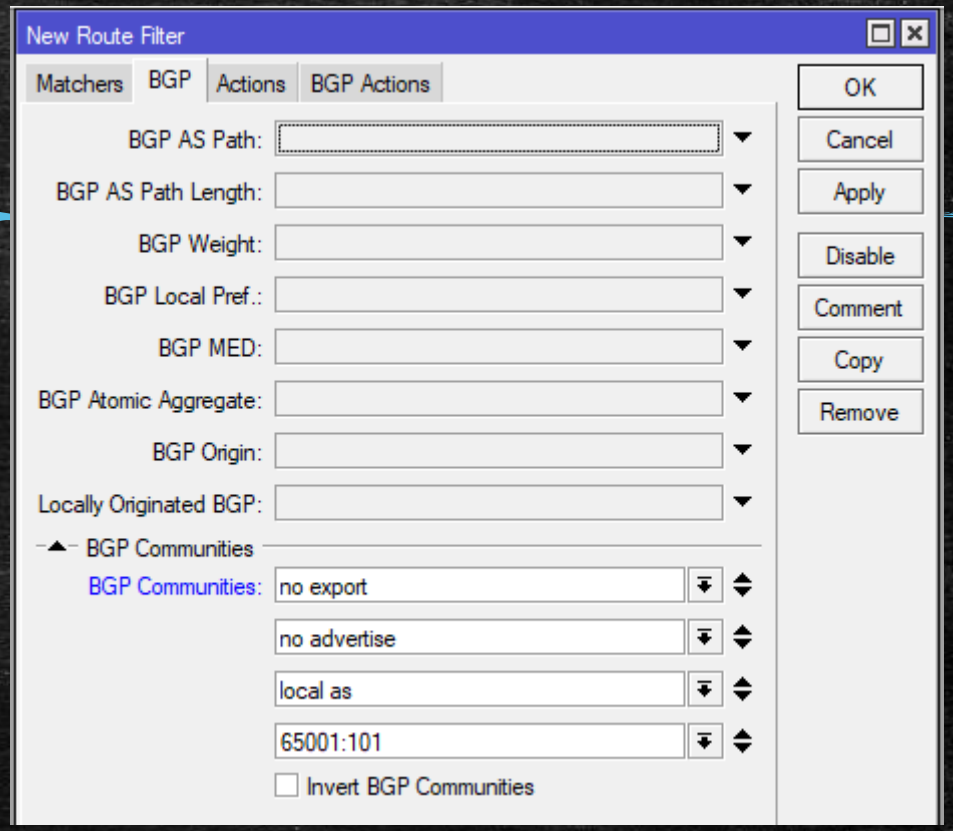
- You are free to reproduce, distribute, interpret, misinterpret, distort, garble, do whatever you like, even claim authorship, without my consent or the permission of anybody.
- I am doing all as mentioned in the presentation according to requirement of the situation and as per my experience with things related. This may require changing parameters as per your environment.
- Always keep a backup before proceeding to try this in a production environment
- The work represented here is only used to share my knowledge. For professional training, contact Mikrotik Certified trainers.

What are BGP Communities

- The BGP community attribute is a numerical value that can be assigned to a specific prefix and advertised to other neighbours. When the neighbour receives the prefix it will examine the community value and take proper action whether it is filtering or modifying other attributes.
- Four commonly found communities
  - Internet - Advertise these routes to all neighbours.
  - Local-AS - Prevent sending routes outside the local As within the confederation.
  - No-Advertise - Do not advertise this route to any peer, internal or external.
  - No-Export - Do not advertise this route to external BGP peers.
  - Bonus – 666 – Black-hole



Used while exporting routes



Used while importing routes

Why use BGP communities

- Communities can be used to mark a set of prefixes that share a common property. Upstream providers can use these marks to apply a common routing policy such as filtering or assigning a specific local preference. You can use it to make changes and policies of your own.

- As a service provider you can make an agreement with your customers on a specific policy to be applied to their prefixes using communities; this gives your customers the freedom to change the policy of a prefix just by changing the community attribute value with no support from your side.
  Ask your service provider for supported BGP communities

Example of implementation

- Discarding a route and not announcing our routes to an ASN

#Setting a community to an outbound advertisement
/routing filter add action=accept chain=extreme-out prefix=103.210.220.0/22 \
prefix-length=22-24 set-bgp-communities=49378:65013

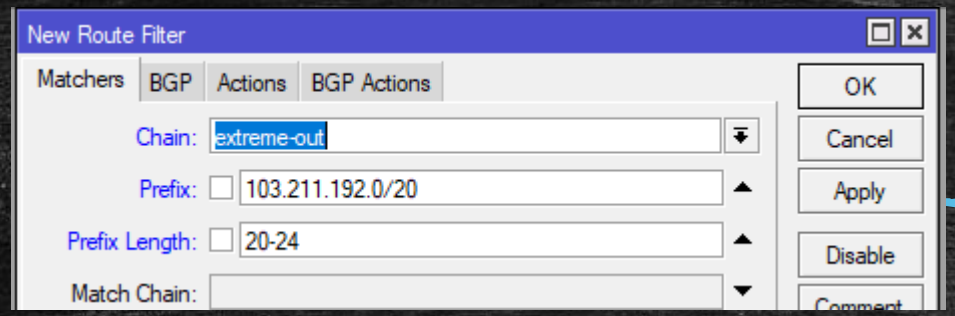
#Discarding inbound reception
/ routing filter add action=discard bgp-communities=49378:65013 chain=extreme-ix-in

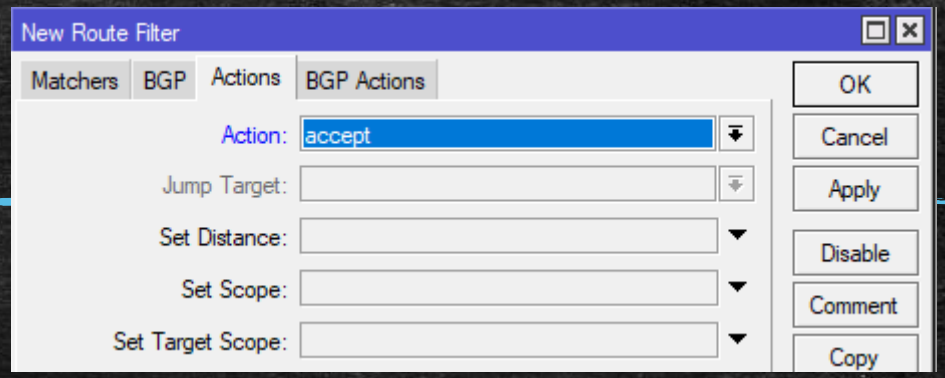
- Prepending “n” number of times

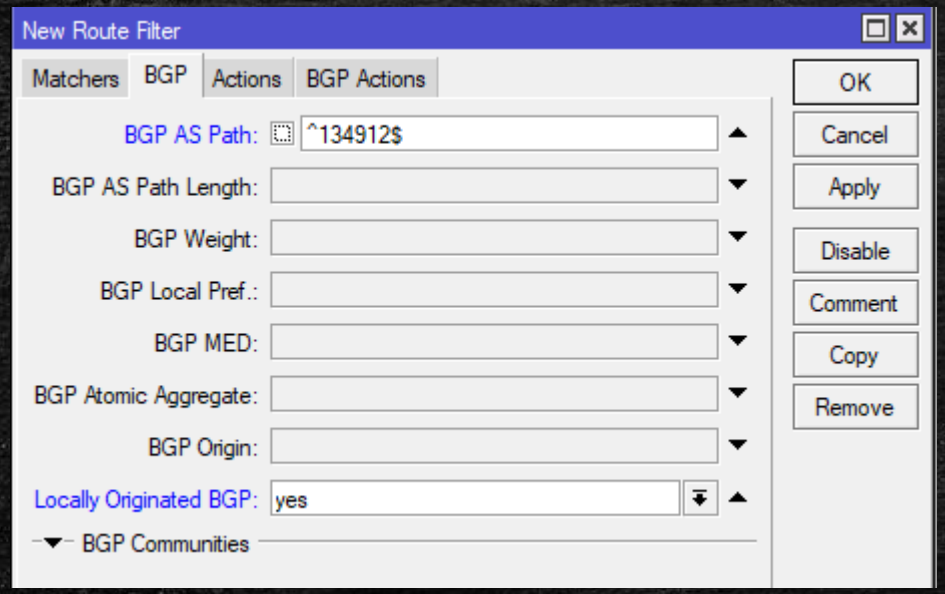
/routing filter add action=accept set-bgp-prepend=3 bgp-communities=65001:1003
chain=upstream1

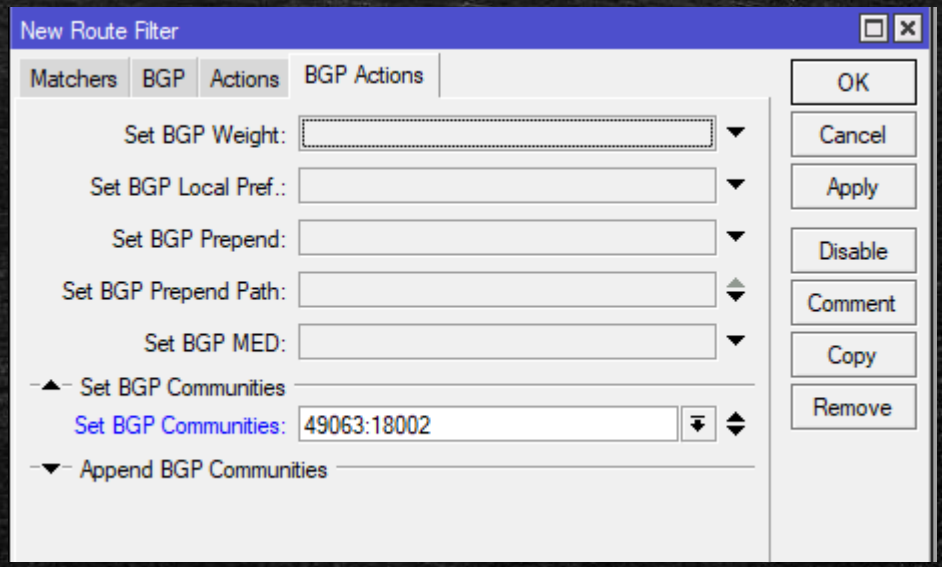
Common mistakes in re-advertisement

- Not using filters at all.
- Using only prefix based filters and ignoring the AS-PATH
- Specific prefix length
- Fix
  /routing filters add action=accept bgp-as-path="^135914\$" chain=ggc-out bgp-communities=65001:102 set-bgp-communities=15169:13300,11344:11300 prefix=103.211.212.0/22 prefix-length=22-24
- /routing filters add action=accept bgp-as-path="^ 135914\$ " chain=extreme-ix-in set-bgp-communities=65001:102 prefix=103.211.212.0/22 prefix-length=22-24


New Route Filter
Matchers
BGP
Actions
BGP Actions
Chain: extreme-out
Prefix: 103.211.192.0/20
Prefix Length: 20-24
Match Chain:
OK
Cancel
Apply
Disable


New Route Filter
Matchers
BGP
Actions
BGP Actions
Action: accept
Jump Target:
Set Distance:
Set Scope:
Set Target Scope:
OK
Cancel
Apply
Disable
Comment
Copy


New Route Filter
Matchers
BGP
Actions
BGP Actions
BGP AS Path: ^134912$
BGP AS Path Length:
BGP Weight:
BGP Local Pref.:
BGP MED:
BGP Atomic Aggregate:
BGP Origin:
Locally Originated BGP: yes
BGP Communities
OK
Cancel
Apply
Disable
Comment
Copy
Remove


New Route Filter
Matchers
BGP
Actions
BGP Actions
Set BGP Weight:
Set BGP Local Pref.:
Set BGP Prepend:
Set BGP Prepend Path:
Set BGP MED:
Set BGP Communities
Set BGP Communities: 49063:18002
Append BGP Communities
OK
Cancel
Apply
Disable
Comment
Copy
Remove

Simplified access management #NoMercy

- Most effective way to control access on network level to the router is via IP > Firewall > Filter
- /ip firewall filter

```
add action=accept chain=input comment="Allow Management Pools" src-address-list=mgmnt
add action=accept chain=input comment="Allow ICMP Monitoring" protocol=icmp
add action=add-dst-to-address-list address-list=bgp-peers chain=output comment="Export BGP Peer IPs to address list"
dst-port=179 protocol=tcp
add action=accept chain=input comment="Allow BGP from peers only" dst-port=179 protocol=tcp src-address-list=bgp-
peers
add action=drop chain=input comment="DROP INPUT FROM OTHER IPS" dst-port=21,22,23,80,161,8291 protocol=tcp
add action=drop chain=input comment="DROP INPUT FROM OTHER IPS" dst-port=21,22,23,80,161,8291 protocol=udp
add action=drop chain=input comment="DROP OTHER INPUTS"
```

Make changes and add rules for other interconnect protocols.

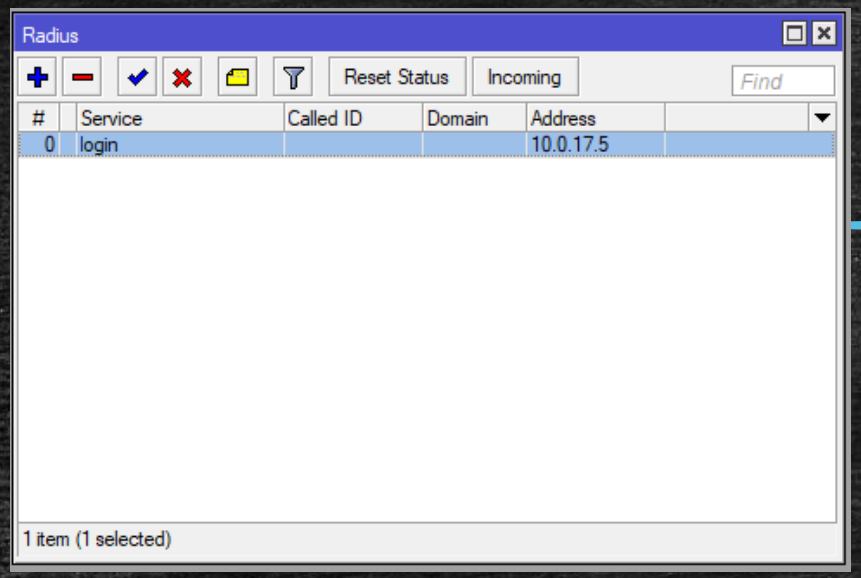
Warning – Do add your IP to the address list "mgmnt" before adding these rules. If locked out, mac-telnet or console is the only way to get in.

Setup VPN on a CHR for remote access

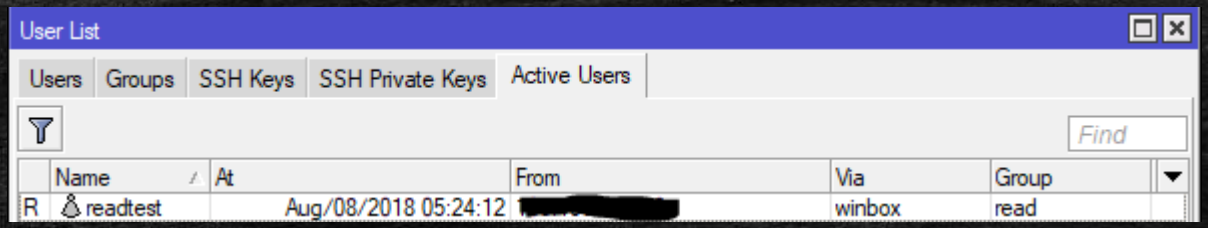
- How to manage your resources in case you are not connected to your network or are in a restricted zone?
- How to connect to your network when you are using Mobile Data or on someone else's network?
- VPN is the answer!
- The ones I use are PPTP(I am so sorry) and L2TP. You can try other protocols on your own. Implementation remains same.

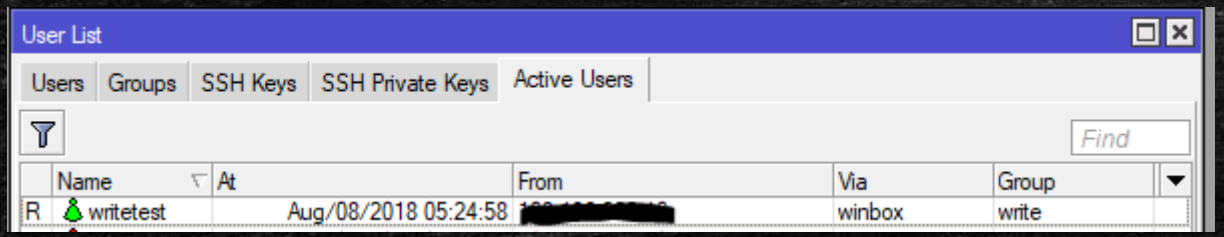
Radius Authentication

- You can also use radius server for local user authentication. Multiple groups and exclude groups are supported.
- You can also define which users can login into which group of devices
- With a syslog server, you can also keep a log record of all settings changed.



You can centrally manage admin users for all your Mikrotik devices once you set up Radius.





Be like Mr. X

- ✓ Keeping your network secure also helps you, your peers and your clients to stay safe.
- ✓ Keep checking for news updates for latest vulnerabilities and apply security patches
- ✓ Always participate in community discussions

Sources to references

- http://www.networkers-online.com/blog/2008/09/understanding-bgp-communities/
- https://www.noction.com/blog/understanding_bgp_communities
- https://mikrotik.com/testdocs/ros/2.8/appex/user_rad.php
- https://wiki.mikrotik.com/wiki/How_to_setup_up_RADIUS_for_use_with_MikroTik_-_By_Ramona

Questions?

Special vote of thanks to

Powernet Communications Pvt. Ltd.

Tara Consultants Pvt. Ltd.

Mikrotikls, Sabiedriba ar ierobezotu atbildibu

Do भौकाल Be भौकाल ------ In consortium with Powernet Communications and Tara Constltants

Tara
(An ISO 9001 : 2015 Certified Company)

Tara Consultants Pvt. Ltd.

Our Strength

★ Manufacturing EPON OLT/ONU.★
★ Triple Play/Quad Play Solutions.★
★ WISP infrastructure.★
★ ISP Solutions.★
★Point to Point Solutions.★
★Point to Multi Point Solutions.★
★Routing Solutions.★
★Surveillance Solutions.★
★ FTTx Solutions.★
★★*After Sale Support* ★★

Fiber Accessories

Fast Connector

Fiber Adapters

Face Plate TY-GOM-A

FTTH Drop Cable Stripper

Fiber Stripper

Fiber Cutter

PLC Splitter Cassette 1x4

PLC Splitter Cassette 1x8

PLC Splitter Cassette 1x16

PLC Splitter Cassette 1x32

Splitter with steel Tube type 1x2/1x4/1x8/1x16/1x32

Ty-GF14-6J

Ty-GF16-8E

Ty-GF06-16P

Ty-GF21-16P

SIP Products
(Session Initiation Protocol)

SIP Server UCM6202/6204

Video Door Phone GDS 3710

SIP Server UCM6510

VOIP Phone GXP1610/1615

Tara EPON Products

1GE ONU

1GE+WiFi ONU

2 Ports OLT

4 Ports OLT

8 Ports OLT

16 Ports OLT

Tara GPON Products

1GE+1FE+1POTS+ICATV+WiFi

1GE+IFE+1POTS+WiFi

GPON PON Module

Tara 1GE GPON ONT

Tara 8 Port GPON OLT

Switches

1GE XPON ONU

Tara Reverse PoE Switch

Tara Reverse PoE Switc 1G input

N1-9802w

N1-9208W

Edgecore ECS2110-26T

Edgecore ECS2100-10T

Edgecore ECS4120-28F

Edgecore ECS2100-28T

Edgecore ECS4120-28FV2

Brands which we deal

TARA FIBER
HUAWEI
NPort Networks
Edge-corE NETWORKS
GRANDSTREAM CONNECTING THE WORLD
ZTE
MikroTik
UBIQUITI NETWORKS
cisco
D-Link Building Networks for People
Tenda
TP-LINK The Reliable Choice

MAKE IN INDIA

Contact Details:

307,08,09 Osian Building-12, Nehru Place, New Delhi-110019
Tel : 011-65170029, 46570272, 46570273, Mob : +91-9811686026, 9205137250, 9210898452
E-mail: sales@tcplonline.com, gamma@tcplonline.com, bharat@tcplonline.com
Web: www.ispmart.com/www.tarafiber.com

Do भौकाल Be भौकाल ------ In consortium with Powernet Communications and Tara Constltants

Useful Links

- Powernet Communications - http://getpowernet.com
- TCPL ISP Mart - http://www.ispmart.com/ ; http://www.tcplonline.com/
- Krauss International Mikrotik Training - http://www.kc-india.com/
- Vajra Telecom - http://vajratelecom.net/
- Extreme-IX - https://extreme-ix.org/
- Freeradius - https://freeradius.org/
- Ubuntu Server - https://www.ubuntu.com/server
- Centos Server - http://isoredirect.centos.org/centos/7/isos/x86_64/

Thank you for your attention

Bhaukaal Baba Technologies Pvt. Ltd.
Office No.-3, TOP Floor, Plot No.-7 Vardhmaan JayPee Plaza, MLU Sec.-4, Dwarka
Dwarka South West Delhi - 110078 IN

sampark@bhaukaalbaba.com http://www.bhaukaalbaba.com

Do भौकाल Be भौकाल ------ In consortium with Powernet Communications and Tara Constltants