Mikrotik in real life, full scale and low budget ISP

wima.sy@gmail.com

additional presentation

How do the youngest country in the world ISPs run their bussiness more efficient, and more reliable with Mikrotik

about me

- Working in ISP industries since 1994
- Currently working as consultant engineer for asia pacific oceania countries company & organization

Definition

- Real life
  - Not in simulation, or lab scale
  - In bussiness, operational, still operational
- Full Scale
  - Have ASN, buy transit, peering
  - Connect to IX
- Low Budget
  - Is low budget

Disclaimer

- This presentation will not talk in depth about BGP, OSPF & Traffic Engineering
- I just share simple example, and how to do it with Mikrotik
- It is real case, some IP/AS is fake, for security

Before

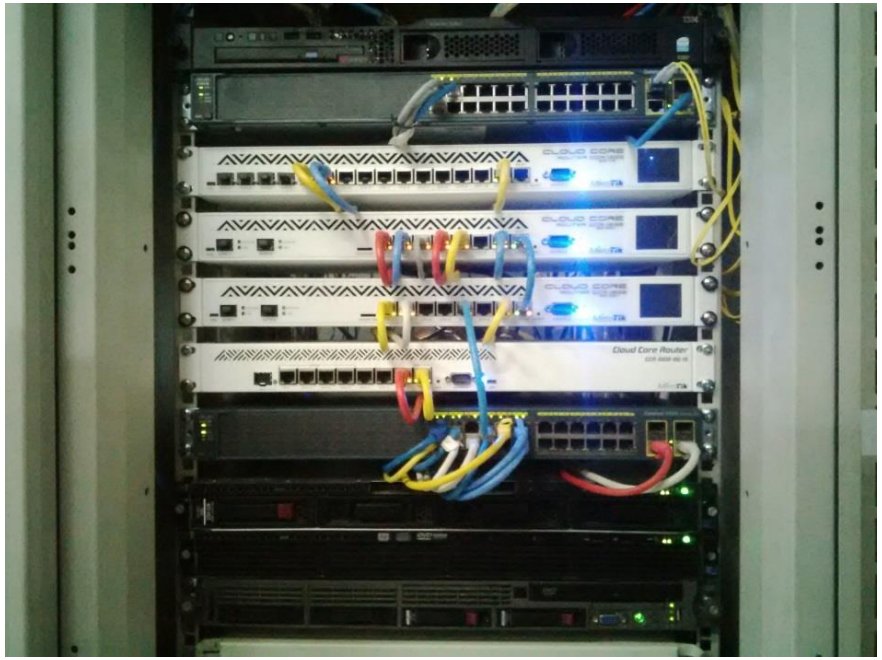
- Cisco 7200 VXR
  - Border Router
  - BGP Peering to Transit Provider
  - BGP Peering to Local IXP
  - Customer Access Router
- IBM e Series
  - FreeBSD / Quagga
  - BGP Peering to Local IXP
  - BGP Peering to IP Transit Customer
- Problem
  - Expensive Router
  - Difficult to Maintain

Reason to Upgrade

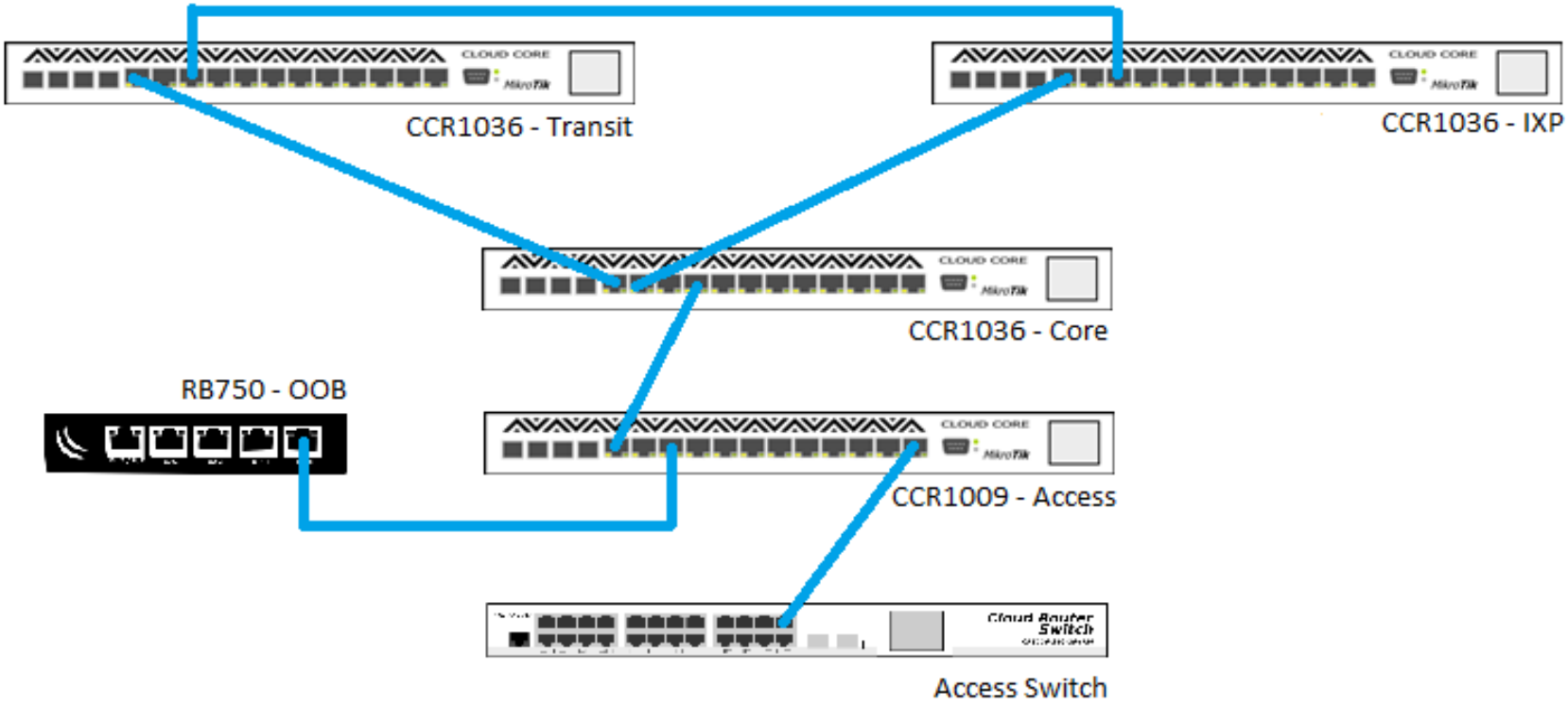
- Efficiency
- Performance
- Maintenance
- Cost
- Growth

After

- CCR 1036-8 – Transit
  - OSPF
  - BGP Peering to Transit Provider
- CCR 1036-8 – IXP
  - OSPF
  - BGP Peering to IXP
- CCR 1036-12 – Core
  - OSPF
  - BGP Route collector
- CCR 1009 – Access
  - Static Routing, VLAN, Trunk
  - Management Router
- RB750 – OOB
  - VPN



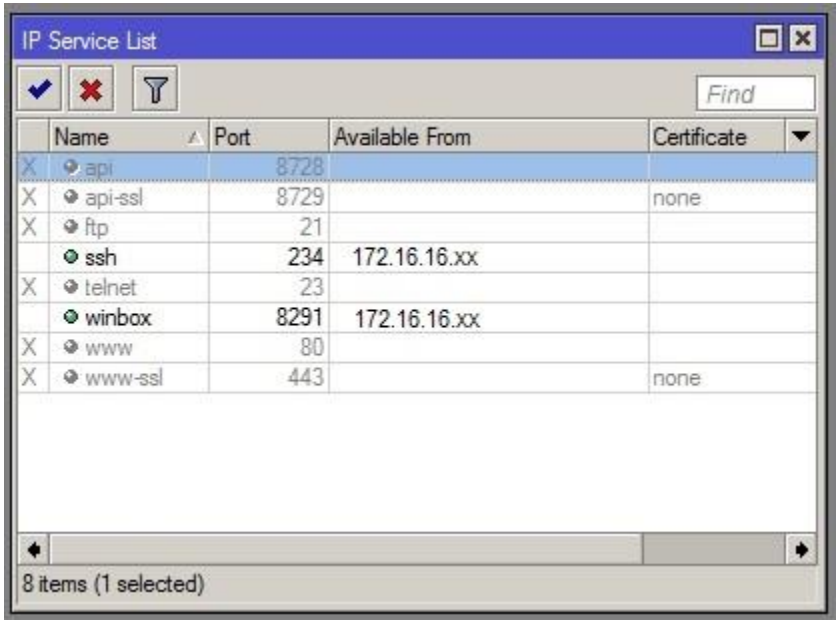
Physical Network Diagram



Configuration

Pre-config

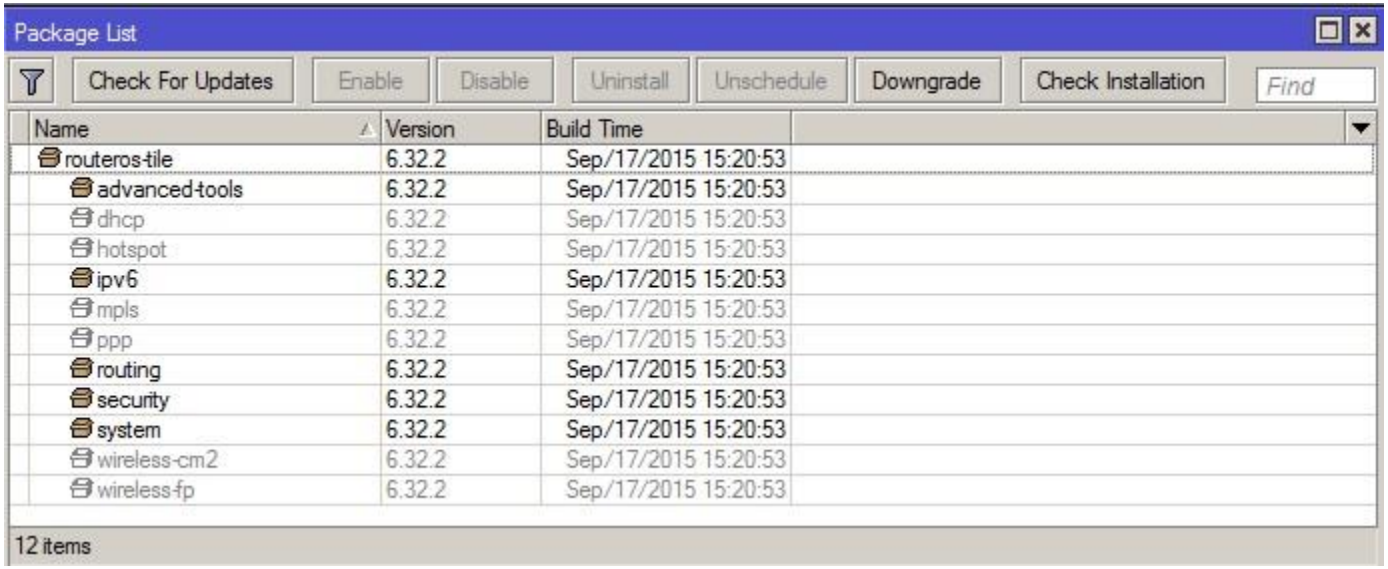
- Turn off unused service features
  - Web,telnet,ftp,etc
- Winbox / SSH only available from Remote Access IP
- Change default port



Configuration

Turn off unused packages features

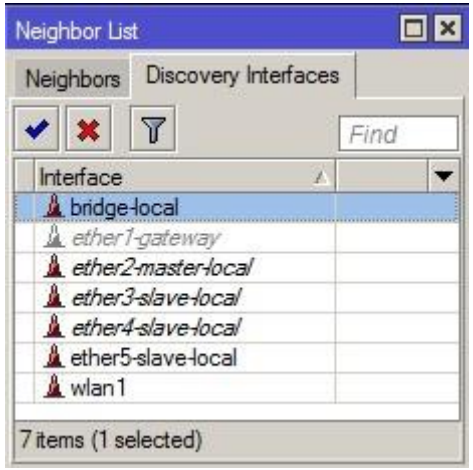
- Disable features/packages



Configuration

Neighbour discovery

- Disable interface



- ✓ Disable MNDP on interface to IXP/Transit, some of them will handle this as a threat
- ✓ Some IX/Transit require you to turn off Proxy ARP,ICMP redirects,Directed broadcast,IEEE802 Spanning Tree,Interior routing protocol broadcast,Mac layer broadcast
- ✓ Read peering agreement

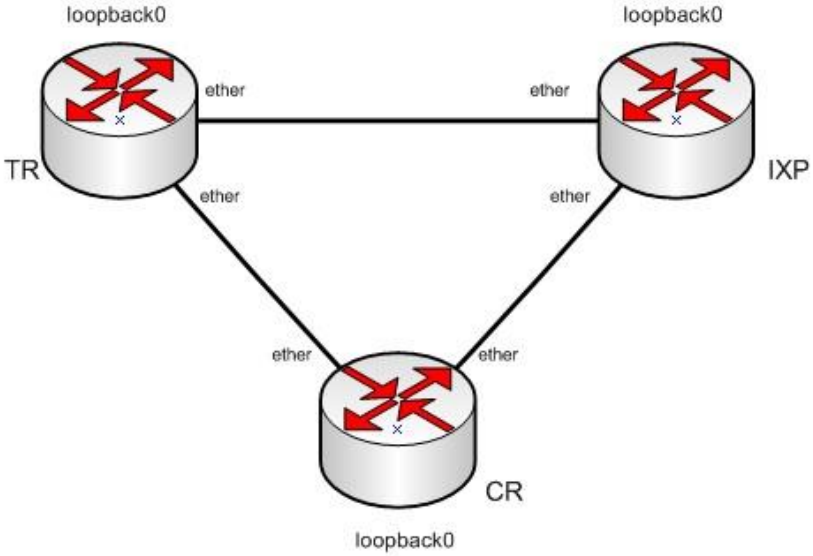
Configuration

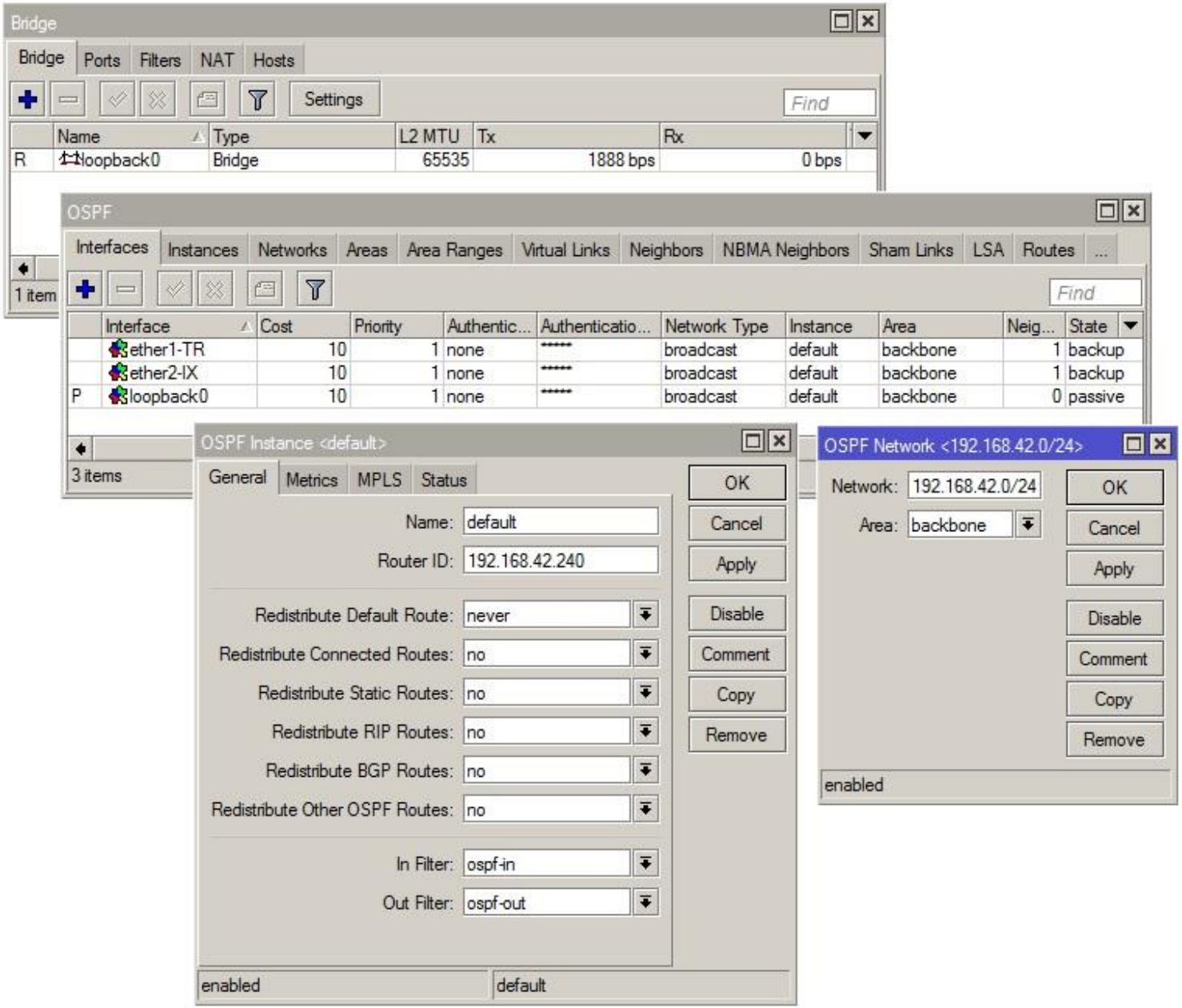
- Disable unused physical interface
- Device name
- User / Password
  - Proper credentials
- NTP Client
  - Make sure your router time is synchronized
- Latest stable OS
- Disable LCD / Minimal information

Configuration

OSPF between devices for IGP

- for infrastructure
- loopback interface, for adjacency, not only router id

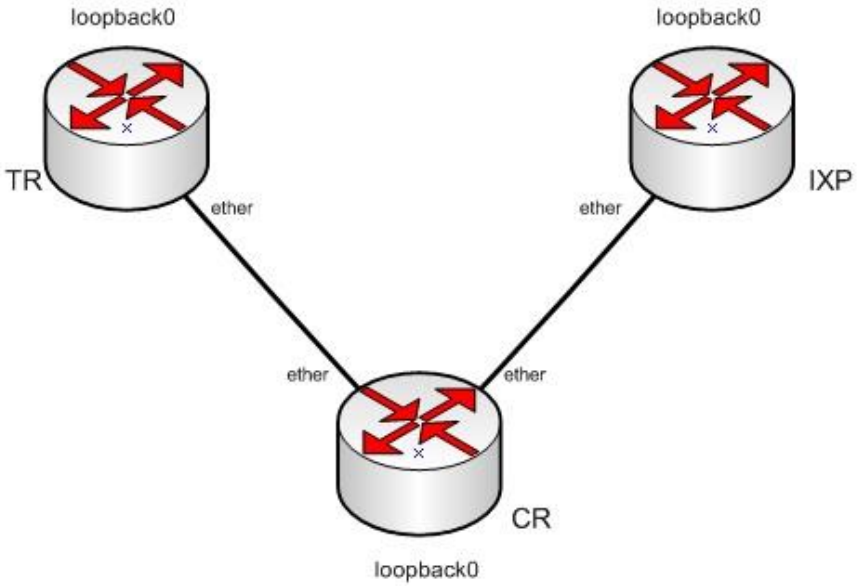



Bridge
Bridge Ports Filters NAT Hosts
Settings
Find
Name Type L2 MTU Tx Rx
R loopback0 Bridge 65535 1888 bps 0 bps
1 item
OSPF
Interfaces Instances Networks Areas Area Ranges Virtual Links Neighbors NBMA Neighbors Sham Links LSA Routes ...
Find
Interface Cost Priority Authentic... Authenticatio... Network Type Instance Area Neig... State
ether1-TR 10 1 none ***** broadcast default backbone 1 backup
ether2-IX 10 1 none ***** broadcast default backbone 1 backup
P loopback0 10 1 none ***** broadcast default backbone 0 passive
3 items
OSPF Instance <default>
General Metrics MPLS Status
Name: default
Router ID: 192.168.42.240
Redistribute Default Route: never
Redistribute Connected Routes: no
Redistribute Static Routes: no
Redistribute RIP Routes: no
Redistribute BGP Routes: no
Redistribute Other OSPF Routes: no
In Filter: ospf-in
Out Filter: ospf-out
OK
Cancel
Apply
Disable
Comment
Copy
Remove
enabled
default
OSPF Network <192.168.42.0/24>
Network: 192.168.42.0/24
Area: backbone
OK
Cancel
Apply
Disable
Comment
Copy
Remove
enabled

Configuration

iBGP between devices

- TR – CR – IXP
- Loopback interface peering
- For carry prefixes across backbone



iBGP instance

BGP Instance <default>

Name: default

AS: 65530

Router ID: 192.168.42.240

Loopback peering

BGP Peer <IX>

General | Advanced | Status

Name: IX

Instance: default

Remote Address: 192.168.42.242

Remote Port:

Remote AS: 65530

Advertise Networks

BGP

Instances | VRFs | Peers | Networks | Aggregat

Network	Synchroni...
172.16.16.0/20	no
192.168.0.0/16	no

Loopback interface as source

BGP Peer <TR>

General | Advanced | Status

Address Families: ☑ ip ☐ ipv6

Update Source: loopback0

Checking

BGP

Instances | VRFs | Peers | Networks | Aggregates | VPN4 Routes | Advertisements

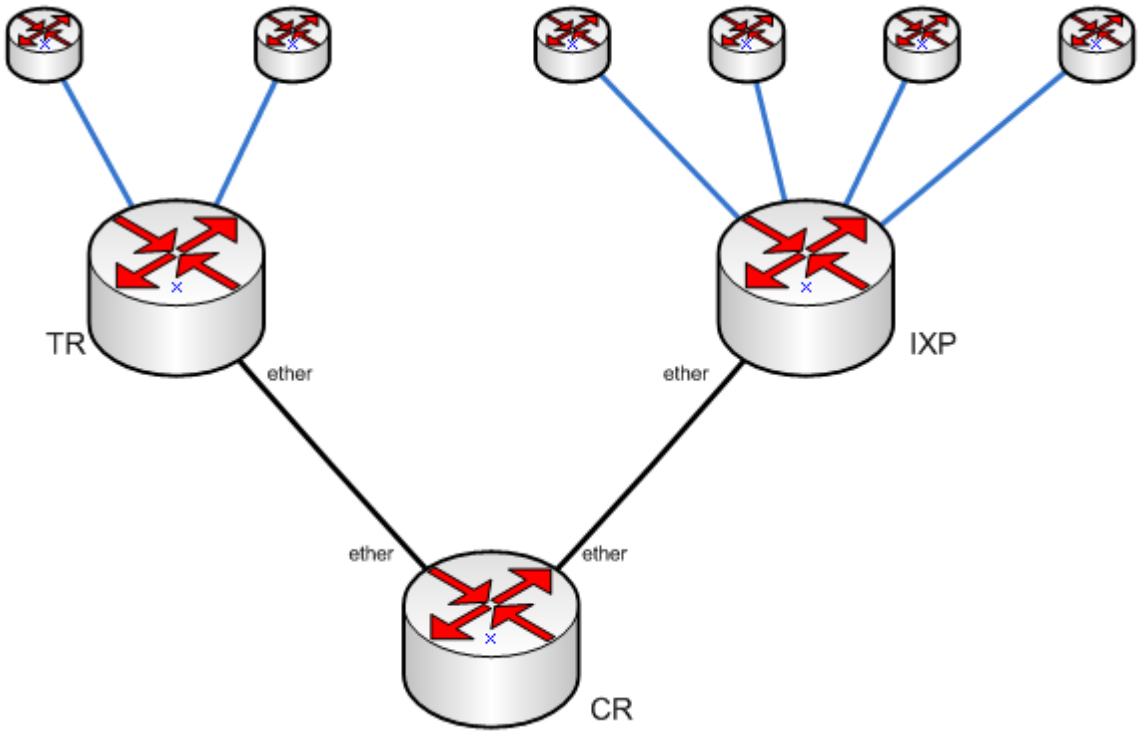
Refresh | Refresh All | Resend | Resend All

Name	Instance	Remote Address	Remote AS	M...	R...	TTL	Remote ID	Uptime	Prefix Co...	State
IX	default	192.168.42.242	65530	no	no	d...	192.168.42.242	00:11:58	1	established
TR	default	192.168.42.241	65530	no	no	d...	192.168.42.241	10:40:38		established

Configuration

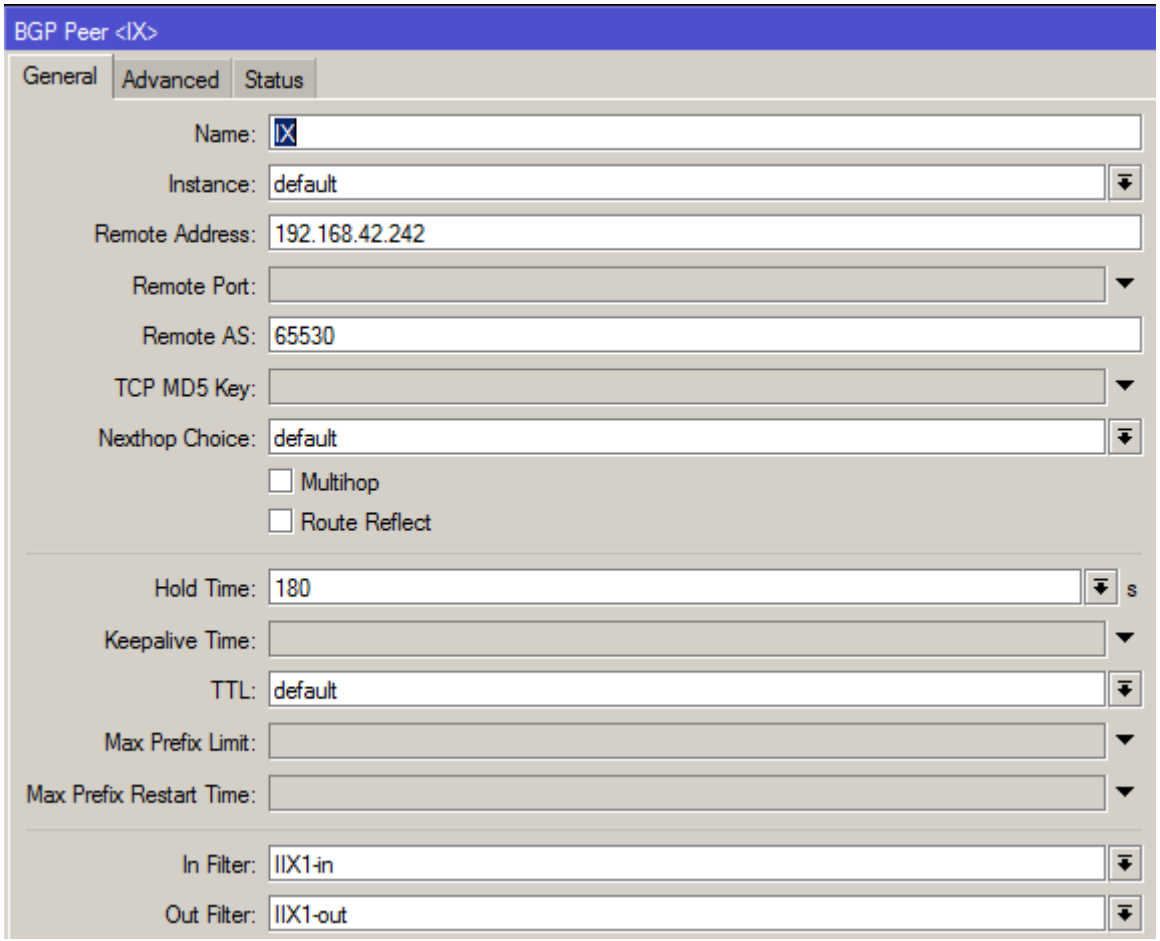
eBGP between peer / other AS

- Peering
- Advertise your prefixes
- Filtering
  - In Filter -> how we send the traffic
  - Out filter -> how they will send the traffic
  - Standard regexp
  - Use template for filter
  - Organize filter using jump
- Traffic engineering, routing policy, follow BGP BCP


TR
IXP
CR
ether
ether
ether
ether

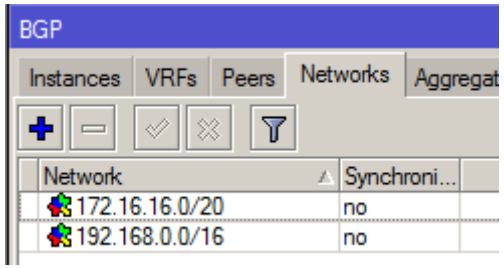
Peering

- Use your AS, peering IP, peer AS
- Prepare your in/out filter

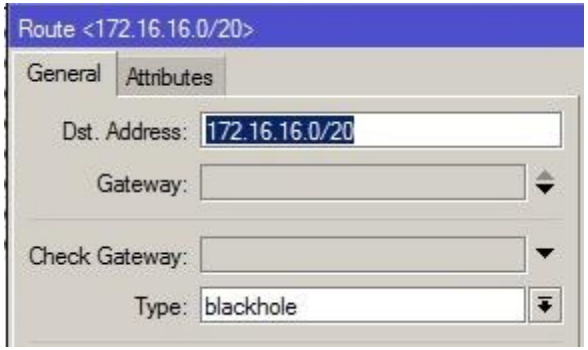


Advertise your prefix

- Announce your aggregate from registry



- Use blackhole type route for pull-up route
- Put on core router, not border



Announce your aggregate, for internet stability

Routing Filters

- In Filter -> how we send the traffic -> our routing table
- Out filter -> how they will send the traffic -> their route to our AS
- Template
  - In Filter
    - Discard prefix from other peering AS
    - Accept prefix from peering AS
    - Discard our own prefixes
    - Discard RFC5735 prefixes
    - Discard prefix longer than 24
  - Out Filter
    - Allow only our prefixes to be announce
  - Use jump for organize your rule
- Regexp
  - . - any single character
  - ^ - start of the as-path
  - $ - end of the as-path
  - _ - matches comma, space, start and end of as-path

Route Filters

#	Chain	Prefix	Prefix Length	BGP AS Path	Action	Jump Target
;;; Discard prefix from other peering AS						
0	IIX1-in			_17451	discard	
1	IIX1-in			_38060	discard	
2	IIX1-in			_56258	discard	
;;; Accept prefix from peering AS						
3	IIX1-in			^7597_	accept	
;;; Discard our own prefixes						
4	IIX1-in				jump	Our-Discard
;;; Discard RFC5735 prefixes						
5	IIX1-in				jump	RFC5735
;;; Discard prefix longer than 24						
6	IIX1-in	0.0.0.0/25	25-32		discard	
7	IIX1-in				discard	
;;; Allow only our prefixes to be announce						
8	IIX1-out				jump	Our-Allow
9	IIX1-out				discard	
10	Our-Allow	192.168.40.0/21	21-24		accept	
11	Our-Allow				return	
12	Our-Discard	192.168.40.0/21	21-24		discard	
13	Our-Discard				return	
14	RFC5735	0.0.0.0/8	8-32		discard	
15	RFC5735	10.0.0.0/8	8-32		discard	
16	RFC5735	127.0.0.0/8	8-32		discard	
17	RFC5735	169.254.0.0/16	16-32		discard	
18	RFC5735	192.0.0.0/24	24-32		discard	
19	RFC5735	192.0.2.0/24	24-32		discard	
20	RFC5735	192.88.99.0/24	24-32		discard	
21	RFC5735	192.18.0.0/15	15-32		discard	
22	RFC5735	198.51.100.0/24	24-32		discard	
23	RFC5735	203.0.113.0/24	24-32		discard	
24	RFC5735	224.0.0.0/4	4-32		discard	
25	RFC5735	255.255.255.255			discard	
26	RFC5735				return	
27	def-discard	0.0.0.0/0			discard	
28	def-discard				return	

Traffic Engineering, Policy Routing

- BGP Attribute
  - http://wiki.mikrotik.com/wiki/Manual:BGP_Best_Path_Selection_Algorithm
- Routing scenario, multihomed
  - Redudancy
  - Load sharing
  - Local traffic goes to and from local peer

References

- NANOG / APNIC BGP Tutorial
- BGP Filtering with Router OS – 2013 MUM Croatia by W. Maia
- Routing Security – 2011 MUM Hungary by W. Maia
- BGP and OSPF Implementations – 2011 MUM Hungary by D. Burgess

Configuration

Access Router

- Plain Static Routing for customer
- Bandwidht Manager
- Controlled by Management Server

Remote Access Server (RB750)

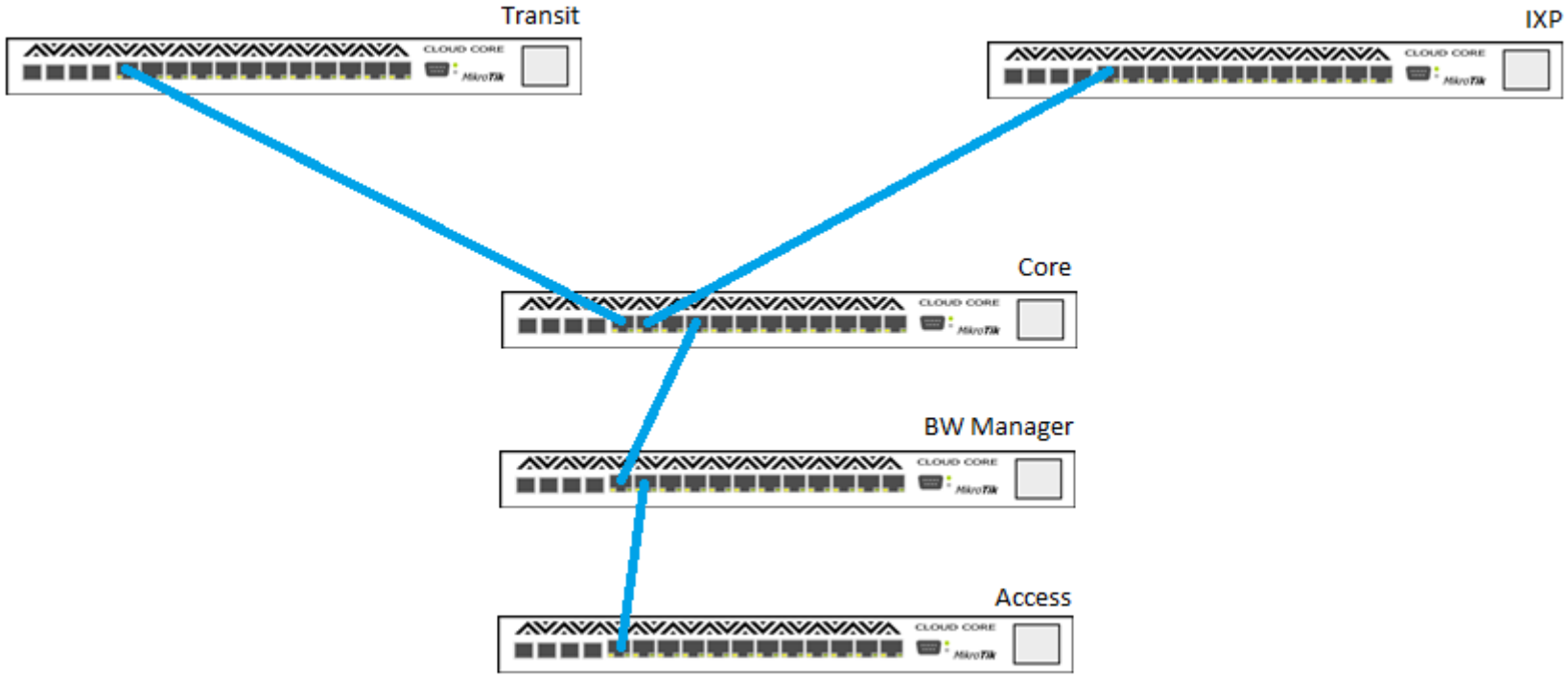
- Secure VPN PPTP/L2TP
- OOB - Connection from other ISP

Configuration

Bandwidht Manager

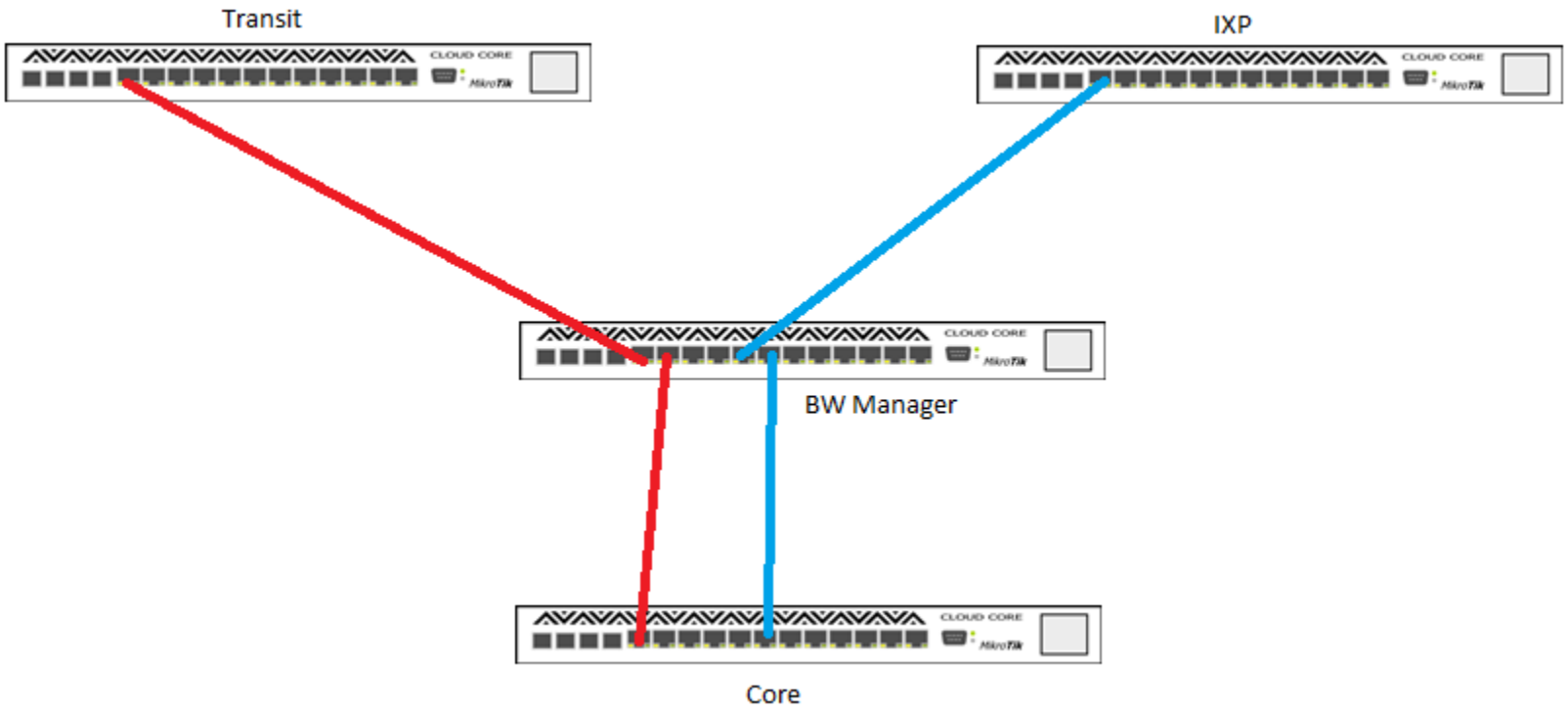
- Strategy
  - Mark packet came from AC router for Upload
  - Mark packet came from TR/IX router for Download
  - Done at Core Router
- International / Local Simple Queue / Queue Tree
- You can use transparent traffic limiter
  - http://wiki.mikrotik.com/wiki/TransparentTrafficShaper

Configuration



- Bridge / Routing Configuration
- International / Local Management
  - Routing List, ref : http://mikrotik.co.id/artikel_lihat.php?id=23
  - Custom Scripting -> export routing from bgp router

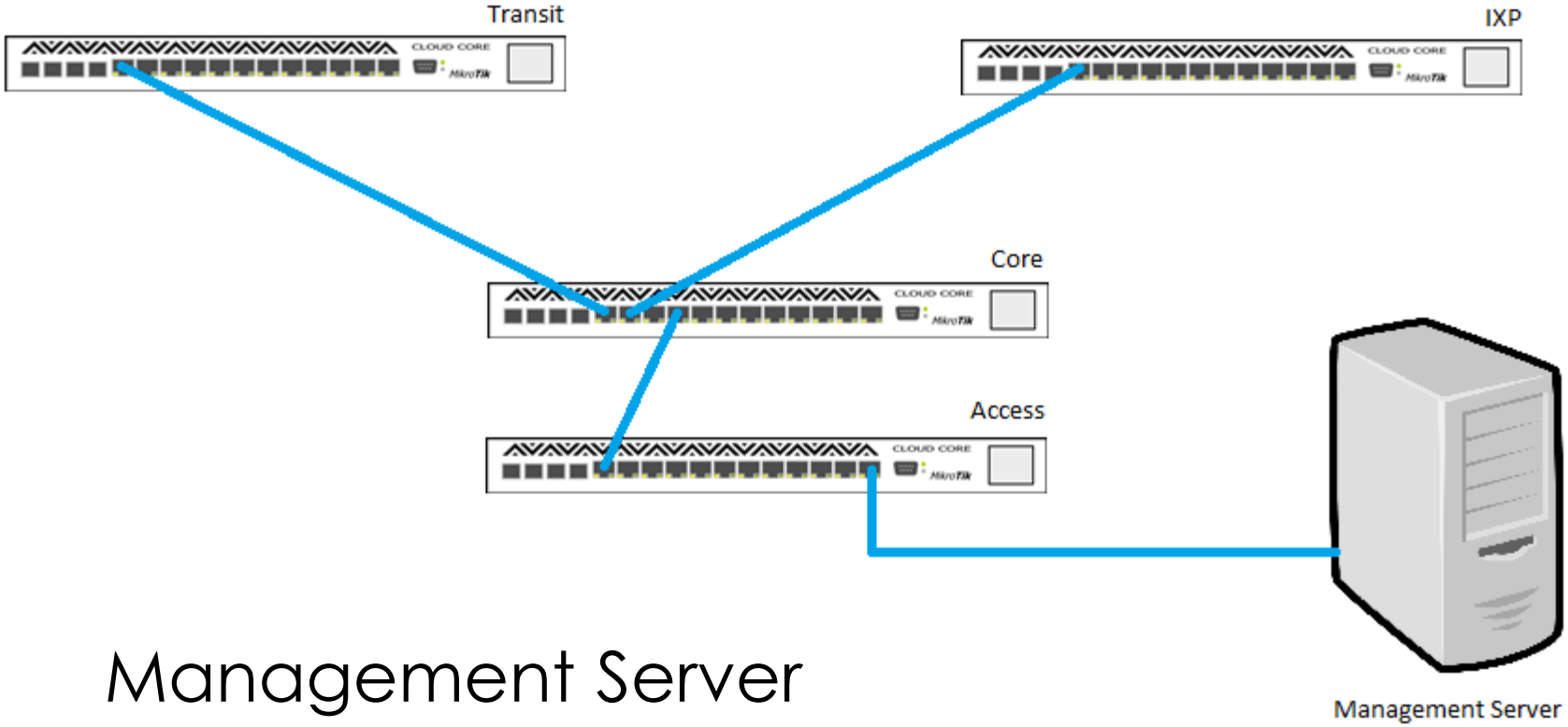
Configuration



Transparent

- Create Bridge Interface
- Marking, check packet flow diagram

Configuration



Management Server

- Don't touch my router
- Simple Mikrotik ROS API Call
- Automatic IP / VLAN / BW Allocation
- Automatic client activation / cut-off

Screenshot

Transit Router

BGP

Instances | VRFs | Peers | Networks | Aggregates | VPN4 Routes | Advertisements

Refresh | Refresh All | Resend | Resend All

Name	Instance	Remote Address	Remote AS	Multihop	Route Reflect	TTL	Remote ID	Uptime	Prefix C...	State
CORE	default	[redacted]	[redacted]	no	no	default	[redacted]	152d 11:14:03	1	established
SDI	default	[redacted]	[redacted]	no	no	default	[redacted]	27d 11:23:58	579226	established
BIZNET	default	[redacted]	[redacted]	no	no	default	[redacted]	86d 02:28:20	597666	established

IX Router

BGP

Instances | VRFs | Peers | Networks | Aggregates | VPN4 Routes | Advertisements

Refresh | Refresh All | Resend | Resend All

Name	Instance	Remote Address	Remote AS	Multi...	R...	TTL	In Filter	Out Filter	Remote ID	Uptime	Prefix ...	State
CORE	default	[redacted]	[redacted]	no	no	default	CORE-in	CORE-out	[redacted]	145d 01:48:02	1	established
BIX	default	[redacted]	[redacted]	no	no	default	BIX-in	BIX-out	[redacted]	4d 02:39:30	435	established
IIX1	default	[redacted]	[redacted]	no	no	default	IIX1-in	IIX1-out	[redacted]	85d 17:02:05	9881	established
IIX2	default	[redacted]	[redacted]	no	no	default	IIX2-in	IIX2-out	[redacted]	03:49:59	9984	established
IIX3	default	[redacted]	[redacted]	no	no	default	IIX3-in	IIX3-out	[redacted]	03:49:43	10049	established
OIXP	default	[redacted]	[redacted]	no	no	default	OIXP-in	OIXP-out	[redacted]	4d 11:08:20	11622	established
SDIIX	default	[redacted]	[redacted]	no	no	default	SDIIX-in	SDIIX-out	[redacted]	66d 13:51:53	52057	established

Maintenance

ROS upgrade strategy

- Use stable/current only
  - RouterOS current release 6.XX
  - RouterOS bugfix release 6.XX.Y
- Read Changelog
  - Upgrade wisely
- Improving system stability

Config backup

- Simple script

Documentation

- Everything
- Log / Syslog ex: syslog-ng

additional presentation

How do the youngest country in the world ISPs run their bussiness more efficient, and more reliable with Mikrotik

History of iNet Timor

- 1999 – Referendum for Freedom
- 2000 – Telstra start cellular telephone
- 2003 – Timor Telecom : Voice (GSM/PSTN)
  Telstra iNet : Data Internet
  (ADSL/Dialup/Wireless)

Before Mikrotik

Network scale

- 30Mbps Upstream
- One main hub
- Dialup / ADSL Services
- 3 Wireless BTS around Dili
- VSAT Backbone
- 20 Client

Using well known product

- Cisco Router
- Cisco Switch
- Nortel/Paradyne DSLAM
- Avaya / Cisco / Breezecom
- Cisco 800 / 2500 CP Router
- Airlive CPE

Past


NEW SAT
PARADYNE
NEW SAT
COMTECH
Cisco 4000
MAX
MAXBOX2
MAX
MAXBOX3
MAX
MAXBOX5

Problem

- Power line quality are bad, devices easy to damage
- Time to deliver replacement devices
  - From HQ (2 weeks)
  - From order to deliver, 15 day minimum
- High down time
- Expensive, almost impossible to have spare
- High cost CPE

Mikrotik

- **2006 – 2007**
  - RB230, RB132, RB133, RB532 (RouterOS v2) as Wireless Infrastructure
- **2008**
  - RB1000 (RouterOS v3), as experimental access router
- **2009**
  - RB750 as CPE router, replace Cisco 700,800,2500
- **2010**
  - RB1100 as Edge Router – Cisco replacement
    - ✓ BGP/OSPF (One default route only, One Full Routing Table)
  - RB1100 as Bandwidht Manager
    - ✓ HTB, good but complicated
    - ✓ Simple Filter Rule
  - RB1100 – As Distribution Router
    - ✓ Plain static routing
- **2013**
  - Next step with CCR1036
    - ✓ Using Simple Queue as RouterOS 6, lot easier than HTB and faster

After Mikrotik

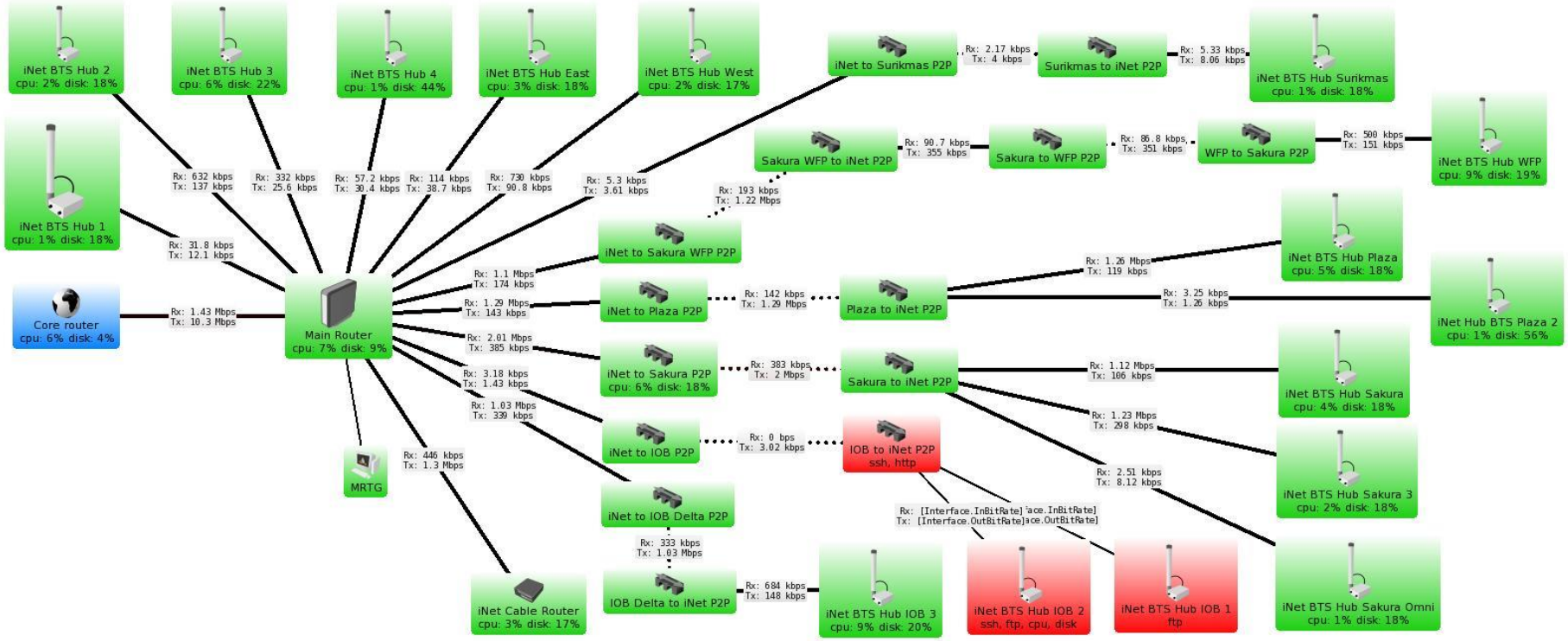
Network scale

- 150Mbps Upstream
  - VSAT & Fiber Multihoming
- Wireless & GPON Services
- 16 Wireless BTS around Dili, 5 remote BTS
- > 400 Client

Expansion

- 3G/4G LTE Access Point (Canceled 2013)
- GPON FTTH, Mikrotik ONT/ONU only
- Solar Powered remote BTS
  - 100W Solar panel + Battery
  - GSM remote switch
  - RB750UP / hEX POE Lite for controller
  - RB433, RB911, Metal

The Dude


iNet BTS Hub 2
cpu: 2% disk: 18%
iNet BTS Hub 3
cpu: 6% disk: 22%
iNet BTS Hub 4
cpu: 1% disk: 44%
iNet BTS Hub East
cpu: 3% disk: 18%
iNet BTS Hub West
cpu: 2% disk: 17%
iNet to Surikmas P2P
Rx: 2.17 kbps
Tx: 4 kbps
Surikmas to iNet P2P
Rx: 5.33 kbps
Tx: 8.06 kbps
iNet BTS Hub Surikmas
cpu: 1% disk: 18%
iNet BTS Hub 1
cpu: 1% disk: 18%
Rx: 632 kbps
Tx: 137 kbps
Rx: 332 kbps
Tx: 25.6 kbps
Rx: 57.2 kbps
Tx: 30.4 kbps
Rx: 114 kbps
Tx: 38.7 kbps
Rx: 730 kbps
Tx: 90.8 kbps
Rx: 5.3 kbps
Tx: 3.61 kbps
Sakura WFP to iNet P2P
Rx: 90.7 kbps
Tx: 355 kbps
Sakura to WFP P2P
Rx: 86.8 kbps
Tx: 351 kbps
WFP to Sakura P2P
Rx: 500 kbps
Tx: 151 kbps
iNet BTS Hub WFP
cpu: 9% disk: 19%
Rx: 193 kbps
Tx: 1.22 Mbps
Rx: 31.8 kbps
Tx: 12.1 kbps
iNet to Sakura WFP P2P
iNet BTS Hub Plaza
cpu: 5% disk: 18%
Rx: 1.26 Mbps
Tx: 119 kbps
Rx: 1.1 Mbps
Tx: 174 kbps
Rx: 1.29 Mbps
Tx: 143 kbps
iNet to Plaza P2P
Rx: 142 kbps
Tx: 1.29 Mbps
Plaza to iNet P2P
Rx: 3.25 kbps
Tx: 1.26 kbps
iNet Hub BTS Plaza 2
cpu: 1% disk: 56%
Core router
cpu: 6% disk: 4%
Rx: 1.43 Mbps
Tx: 10.3 Mbps
Main Router
cpu: 7% disk: 9%
Rx: 2.01 Mbps
Tx: 385 kbps
iNet to Sakura P2P
cpu: 6% disk: 18%
Rx: 383 kbps
Tx: 2 Mbps
Sakura to iNet P2P
Rx: 1.12 Mbps
Tx: 106 kbps
iNet BTS Hub Sakura
cpu: 4% disk: 18%
Rx: 3.18 kbps
Tx: 1.43 kbps
Rx: 1.03 Mbps
Tx: 339 kbps
Rx: 1.23 Mbps
Tx: 298 kbps
iNet to IOB P2P
Rx: 0 bps
Tx: 3.02 kbps
IOB to iNet P2P
ssh, http
iNet BTS Hub Sakura 3
cpu: 2% disk: 18%
MRTG
Rx: 446 kbps
Tx: 1.3 Mbps
Rx: 2.51 kbps
Tx: 8.12 kbps
iNet to IOB Delta P2P
Rx: [Interface.InBitRate] ace.InBitRate]
Tx: [Interface.OutBitRate]ace.OutBitRate]
Rx: 333 kbps
Tx: 1.03 Mbps
iNet Cable Router
cpu: 3% disk: 17%
IOB Delta to iNet P2P
Rx: 684 kbps
Tx: 148 kbps
iNet BTS Hub IOB 3
cpu: 9% disk: 20%
iNet BTS Hub IOB 2
ssh, ftp, cpu, disk
iNet BTS Hub IOB 1
ftp
iNet BTS Hub Sakura Omni
cpu: 1% disk: 18%

CCR1036

400 client simple queues ?

No Problem, we did that

39	California Hotel	1500k	2M
29	City Auto	1M	1M
57	Cooyadygs	256k	256k
41	Covec Compound	2M	2M
24	Covec Engineering	1M	1M
109	Covec Group	3M	3M
1	Covec House1	768k	768k
44	Covec House2	768k	768k
111	Covec Office1	2M	2M
22	Covec Office2	2M	2M
60	DN Movers	384k	384k
55	Dai Nippon Lda	768k	768k
16	Dili Beach	2M	2M
95	Dive Center	512k	512k
2	EDTL	768k	768k
18	ETT Groups	5M	5M
15	BK ANZ	1M	1M
93	BK Airport	1M	1M
43	BK Dili Port	1M	1M
101	Discovery Hotel	2M	2M
98	ETT	4M	4M
92	Gloria Jeans	2M	2M
9	Sakib House	1M	1M
82	Eastern Burger	1M	1M
83	Eugenia Compound	384k	384k
70	Fernanda House	768k	768k
58	Fundasaun Mahein	1M	1M
4	GFA-Lahane	512k	512k
79	GMP-TL Group	3M	3M
421 items 1 selected)		0 B queued	

Result

- Reducing Expenses
  - Reducing capex
  - Reducing customer cost
- Fast to deliver, Fast to replace, Low down time
  - We have cold spare devices
  - If we dont, we can get it less than 12 hours
- Easy to operate and maintain
  - Winbox easy to use
- Open lot of possibilities,
  - Exploit all of technology available on ROS

Last Update

iNet start using O3b

- Medium orbit Satellite, not geo stationer
- 360 minutes contact per satellite
- 300ms latency, not 500ms anymore
- Required two autotracking dish
- Using Mikrotik to do VRRP

Last..

- Don’t be affraid to use RouterOS on your ISP
- Don’t be embarassed if you already use ROS
- Router OS have complete features for ISP

Thank You