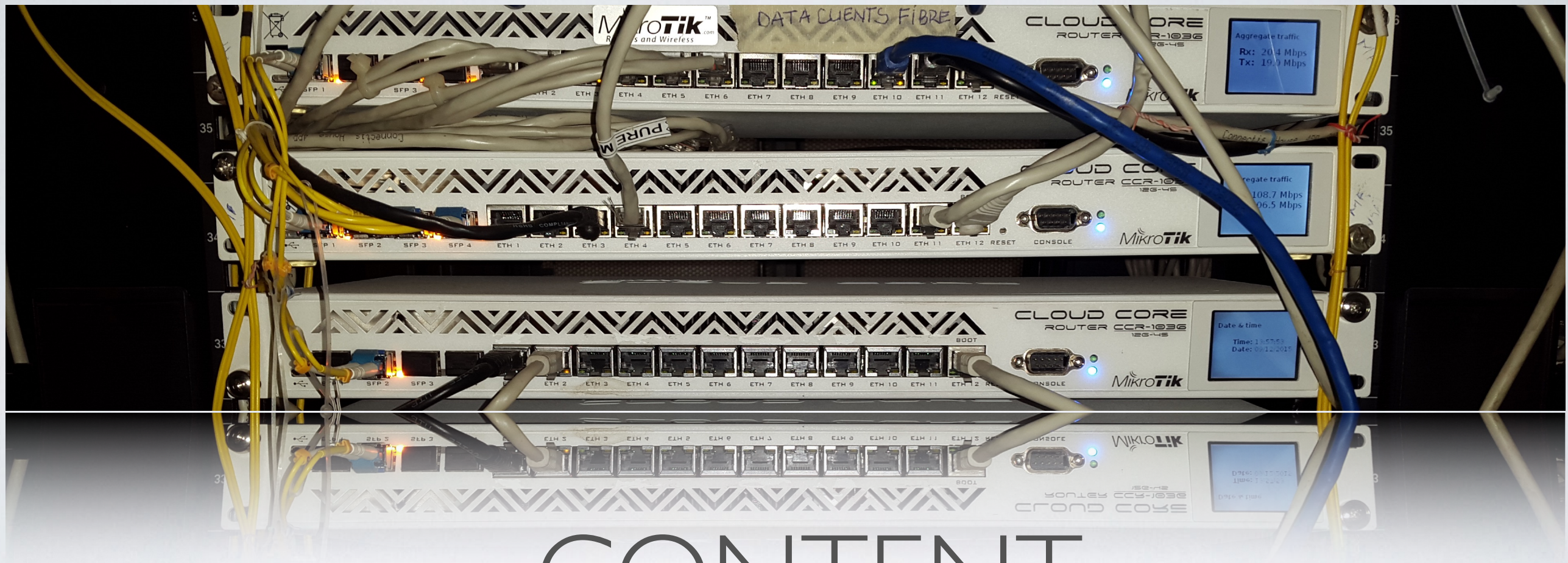




NETWORK DESIGN & SECURITY

using EoIP Encryption



CONTENT

- A three 3 layered network (extended star)
- Network masts of 252
- EoIP encrypted (IPSec) tunnels over IP links - RouterOS 6.35 min
- Redundant connectivity & VPN for remote access



START-UP POINT

- No server room, racks, earth
- Flat network design
- Cabling was a huge web
- No IT security measure
- Diguim, IP PBX, RB2011, Ceragon₃, Fiber

- 3 layered design
- Extended Start Topology
- Physical & EoIP link with masts of 252
- Redundant 3G/VSAT & VPN for remote
- All traffic via EoIPs
- Ext Firewall in Edge

4

LI COUNTRY EDGE

- EoIP enabled links between countries
- External firewall and mangle rules are managed
- Remote access VPN
- Global monitoring

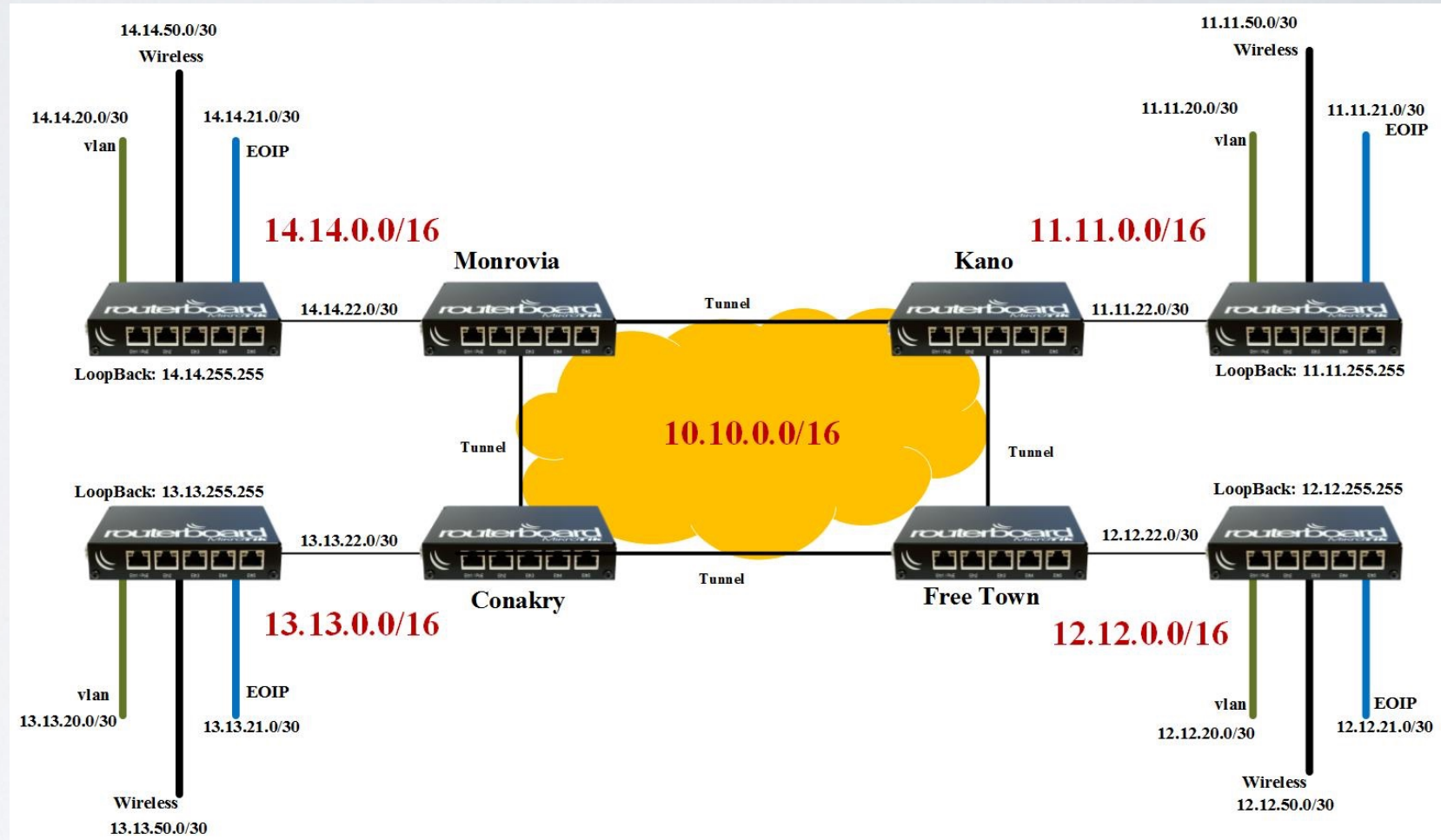
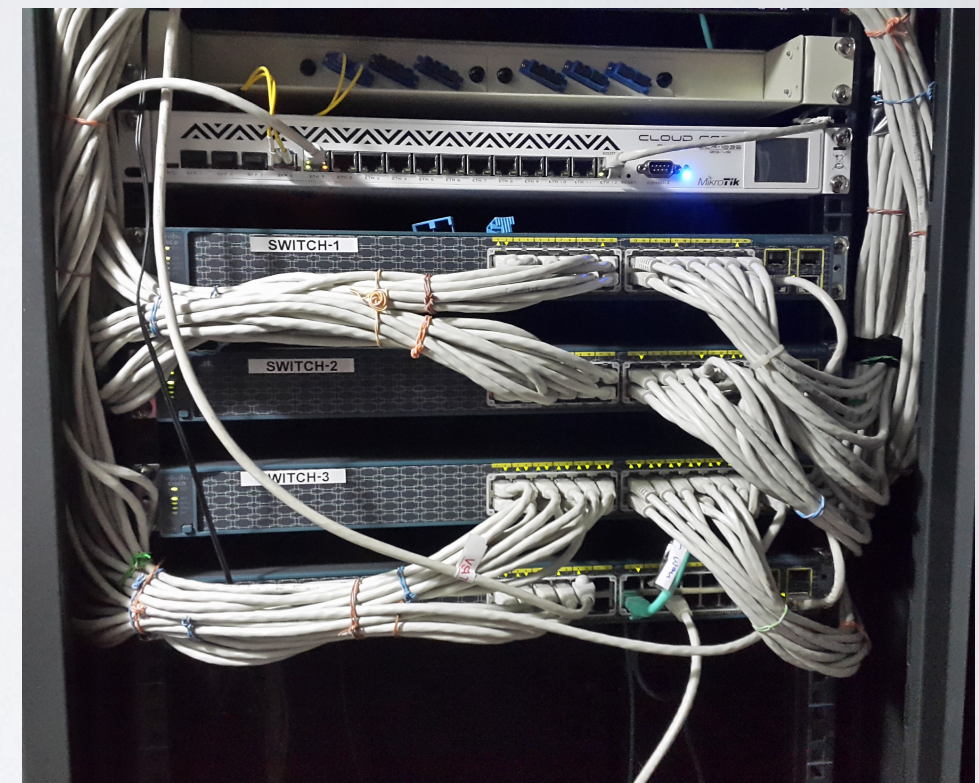


Image credit: Mani

L2 ACCESS

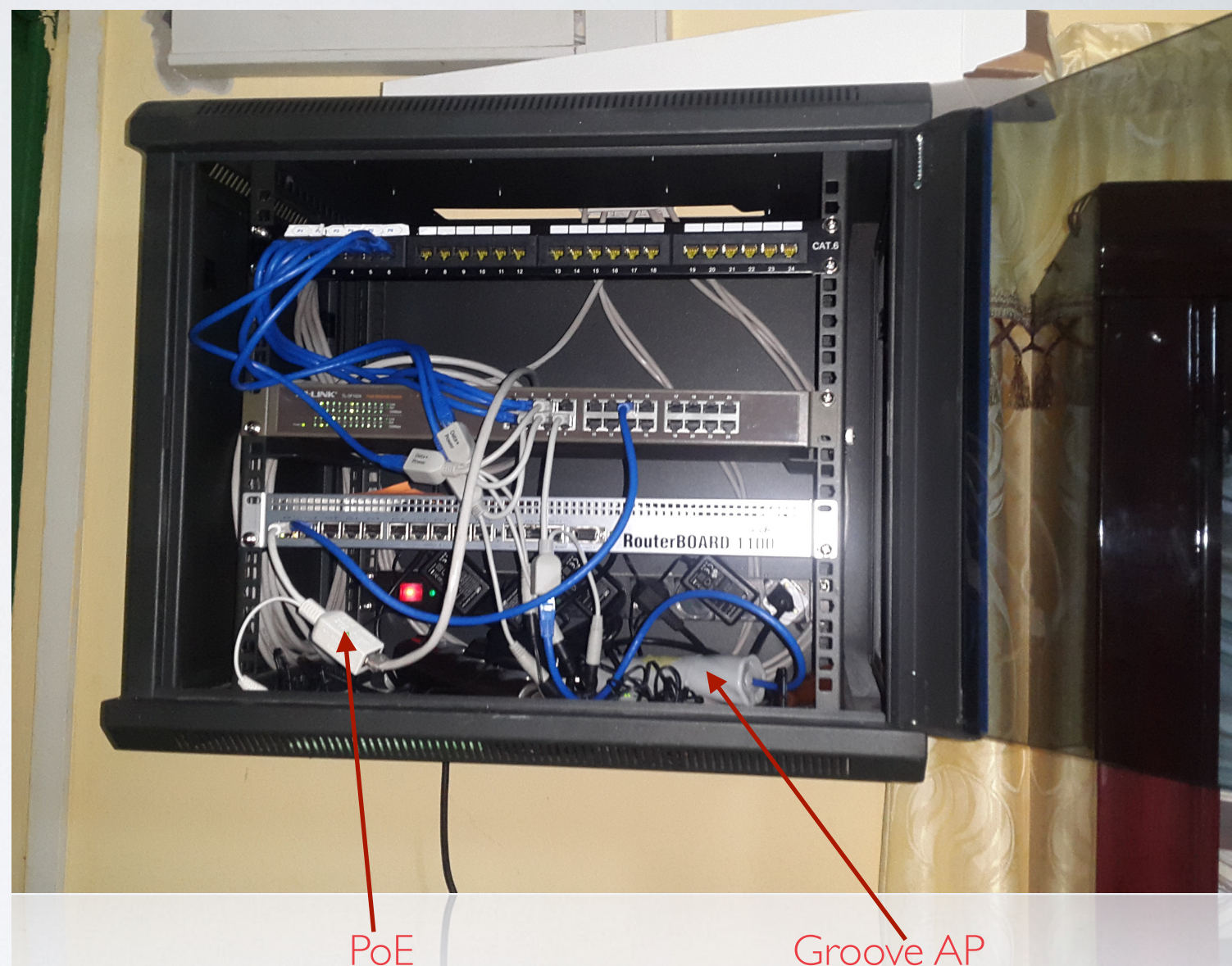
- Define Interfaces with IP & 252 masks
- Define logical interface EoIP with name, IP & 252 masks, remote IP, physical interface assigned to, MTU and ID. Repeat (MTU & ID).
- Tunnel is encrypted and 2 IPs allowed
- Routing is conducted here.
- Internal firewall rules.
- All traffic via the EoIPs.



13.13.20.0/30 for IP link & 13.13.21.0/30 for EoIP tunnels

L3 DISTRIBUTION

- Router & Groove APs (PoE)
- EoIP tunnel connects to the Access
- Tunnel is encrypted and 2 IPs allowed
- Internal firewall rules
- All traffic via the EoIP



Interface <eoip-hotspot-server>

General Status Traffic

Name:

Type:

MTU:

Actual MTU:

L2 MTU:

MAC Address:

ARP:

Local Address:

Remote Address:

Tunnel ID:

IPsec Secret:

Keepalive:

DSCP:

Dont Fragment:

☒ Clamp TCP MSS

☒ Allow Fast Path

enabled running slave

Quick Set

Interfaces

Wireless

Bridge

PPP

Switch

Mesh

IP

MPLS

Routing

Interface List

Interface Ethernet EoIP Tunnel IP

EoIP Tunnel

IP Tunnel

GRE Tunnel

VLAN

VRRP

Bonding

Interface Ethernet EoIP Tunnel IP Tunnel GRE Tunnel VLAN VRRP Bonding LTE

Find

Name	Type	Actual ...	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
To Norfolk	EoIP Tunnel	1458	65535	648 bps	0 bps	0	1

1 item out of 5

Interface <To Norfolk>

General Status Traffic

Tx/Rx Rate: /

Tx/Rx Packet Rate: /

Tx/Rx Bytes: /

Tx/Rx Packets: /

Tx/Rx Drops: /

Tx/Rx Errors: /

Tx: 648 bps

Rx: 0 bps

Tx Packet: 1 p/s

Rx Packet: 0 p/s

Profiles Active Hosts IP Bindings Service Ports Walled Garden Walled Garden

New Interface

General Loop Protect Status Traffic

Name: eoip-test

Type: EoIP Tunnel

MTU: 1500

Actual MTU:

L2 MTU:

MAC Address: 02:ED:0B:CF:37:43

ARP: enabled

ARP Timeout:

Local Address:

Remote Address: 10.10.10.1

Tunnel ID: 12

IPsec Secret: *****

Keepalive:

DSCP: inherit

Dont Fragment: no

☒ Clamp TCP MSS

☐ Allow Fast Path

enabled running slave

Quick Set

Interfaces

Wireless

Bridge

PPP

Switch

Mesh

IP

MPLS

Routing

Interface List

Interface Ethernet EoIP Tunnel IP

+ - ✓ ✗ [icon] [icon]

EoIP Tunnel

IP Tunnel

GRE Tunnel

VLAN

VRRP

Bonding

Interface Ethernet EoIP Tunnel IP Tunnel GRE Tunnel VLAN VRRP Bonding LTE

+ - ✓ ✗ [icon] [icon]

Name	Type	Actual ...	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
RS To Norfolk	EoIP Tunnel	1458	65535	648 bps	0 bps	1	

1 item out of 5

Interface <To Norfolk>

General Status Traffic

Tx/Rx Rate: 648 bps / 0 bps

Tx/Rx Packet Rate: 1 p/s / 0 p/s

Tx/Rx Bytes: 2223.9 MiB / 330.0 KiB

Tx/Rx Packets: 3 424 134 / 4 850

Tx/Rx Drops: 3 / 0

Tx/Rx Errors: 0 / 0

Tx: 648 bps

Rx: 0 bps

Tx Packet: 1 p/s

Rx Packet: 0 p/s

OK Cancel Apply Disable Comment Copy Remove Torch

“Notes to remember”

- A user with viewing rights was created for the NOC.
- Edge Routers cannot be accessed from outside the network, a VPN was used for remote access.
- Only specified Mac addresses were permitted to ping & access routers from within the network. Generally, pings were dropped.
- Thanks to the 3-layered architecture, visibility, scalability and debuggability were improved.
- Thanks to 2 IPs per subnet and EoIP tunnel, and all traffic routed via the EoIP tunnels, network security is improved.

SERVERROOM

- Secured room
- Racks, cooling, earth, & Gen
- Improved cabling
- UPSs in series
- Upgraded servers and network devices
- Video surveillance
- Global monitoring



“Thanks for the your kind attention, comments and questions are welcomed”

–Narcisse Opu