Hotspot, VLAN and User Manager

Presenter: Sunday A. Idajili
ITClick Networx Limited
sonny@itclick.net
Established since 2002 and is a subsidiary of ITClick Solutions Ltd.

Briefly and simply put, we:
- provide broadband internet service using
  (i) 802.11 wireless.
  (ii) C & KU iDirect VSAT
- carry out Data & Voice Network Design and Integration
- provide consulting Services
1999 - Started out with Dialup ISP.
2001 – Wireless experience with Breezecom products. Acquired Breezecom certifications
2004 – Purchased first set of Routerboards and RouterOS. Started with RouterOS 2.8.13 and RB200.
2004 – Attended RouterOS 2.8 Training in Ibadan Organised by Skannet.
Our Transition towards Mikrotik

- 2004 – Backend Solution for QoS, Firewall 100% changed to Mikrotik. Changed Authentication method to Mikrotik hotspot
- 2006 – Attended Advanced RouterOS 2.9 Training in Singapore MUM organised by Mikrotik. Acquired Mikrotik Certifications
- 2007 – Adopted use of Mikrotik User Manager for Hosted Hotspot service for hotels, malls and Cybercafés
- 2007, March – 14 ISP base station sites with over 20 Routerboard 532s total. In all, we have deployed over 200 RouterBoards in consulting projects and client premise links
Why Transition to Mikrotik?

- Reliability - We find RouterBoards the most powerful and reliable outdoor solution ever deployed. With over 200 deployment of routerboard between 2004 and 2007, we've only RMA'd 2 units.
- Performance - ability to handle high traffic. Low power consumption (about 350mA on RB532 with two 400mW cards. Very solar friendly!)
- Features: Unlimited options for system integrators and users. Your solutions and designs are limited only by how far you can imagine...
- Cost: Everybody wants reliability and performance at low price...
Why Transition to Mikrotik?

- Ease of use: Most users’ reason for using RouterOS. Winbox is love at first sight!
- Control: Network Admins first love. All the power you can imagine to enforce resource control with just a few key strokes.
Wireless Network

- All Sites RB532
- Longest link 30.89km with -68dBm Signal (R52+32dBi Ant.)

Note:
Blue lines – completed and active links
Brown lines - proposed links
Backend Diagram (Simple)

Sat Antenna + ODU

Cisco Router RT1

Tx/Rx Modem

Serial

Bridge

DNS, Email & Web

Billing, CRM & DUDE

Satellite

Satellite

Cisco Router RT1

Serial

Ethernet

S1

BR2

S2

BR1

RT2

S3

BR2

DISTRIBUTION NETWORK

VLANS 71 - 80

RouterOS x86

Services:
- Multiple VLAN Hotspot
- Multiple PPPoE Servers
- Simple Queues
- Firewall (against attacks from users)
- NAT

RouterOS x86

Services:
- Multiple VLAN Hotspot
- Multiple PPPoE Servers
- Simple Queues
- Firewall (against attacks from users)
- NAT

RouterOS x86

Services:
- QoS with Queue Tree
- Firewall (against attacks from Internet)
- User Manager
- RSTP for high path availability (VRRP is IP, layer 3)
Design objectives:

- Centralized Firewall and QoS, Radius Authentication and Access Gateway (Hotspot & PPPoE) for simplified administration and single point of failure. **Layer 2 a must for Central PPPoE. Optional for Hotspot and Firewall. Central Hotspot is also possible at layer 3 (routing). Use VLAN.**
Centralized Hotspot type login with different login pages and different classes of service (hosted service for Virtual ISP reseller model) Possible in two ways:

1. Multiple ‘real’ interfaces on gateway. You need install as many interface as hotspot servers required
2. Virtual interfaces on single interface (VLANs). Cost effective and most reasonable option is VLAN
- Hotspot Trial Feature enabled; e.g. 5 minutes trial per day
Layer 2 link required between users and hotspot server.
With Trial enabled, Hotspot allows users’ mac free browsing as configured by the administrator. Routers replace users’ mac with own mac. Use VLAN.
- Control PPPoE & Hotspot Login based on Radius ‘Caller-id’ and ‘Called-id’ attributes. Layer 2 required, use VLAN
- Prevent user to user packet forwarding. Disable ‘default forwarding’ in all APs
- Provide hosted billing service for resellers (Hotels, Cafes, Virtual ISPs. Different login pages and called-id for resellers. Again we need layer 2, use VLAN
- Peering, Co-lo and backup transport Services for Network Operators. ISP-A is peered to ISP-B’s network. Both use Mikrotik. ISP-A wishes to sell hotspot or PPPoE type 128k Internet service where ISP-B has coverage. ISP-B offers ISP-A 128k data only transport at a fee. ISP-A is now able to offer service to customer. This peering and service type is provided at layer 2, while separating the networks. Use VLAN
- Ability to provide Private layer 2 Network Services. **Customer needs to network two sites in one broadcast domain. ISP has service covering both sites. ISP offers customer cheaper networking alternative at layer 2. Use VLAN**
Things you must know:

-A LAN is a local area network and can be defined as all devices in the same broadcast domain.
- Routers stop broadcasts, switches forward them.
- A VLAN is a virtual LAN. In technical terms, a VLAN is a broadcast domain created by switches.
- Administrators must create the VLAN’s then assign what port goes in what VLAN, manually.
- VLAN’s provide better performance for medium and large LAN’s.
- For devices in different VLAN’s to communicate, you must use a router (Layer 3.)
Reference the network diagram above, create multiple hotspot with different login pages on RT2

**STEPS:**

1. Create VLANs on RT2

   ```
   [admin@RT2] > interface ethernet print
   Flags: X - disabled, R - running
   #   NAME            MTU   MAC-ADDRESS     ARP
   0   R ;;; Internet  1500  00:05:5D:2E:2F:75 enabled
       ether1

   1   R ;;; Internal  1500  00:04:76:C9:CB:0D enabled
       ether2
   ```

   ```
   [admin@RT2] > interface vlan add name=ether2-vlan71 vlan-id=71 interface=ether2 disabled=no
   [admin@RT2] > interface vlan add name=ether2-vlan72 vlan-id=72 interface=ether2 disabled=no
   [admin@RT2] > interface vlan add name=ether2-vlan73 vlan-id=73 interface=ether2 disabled=no
   [admin@RT2] > interface vlan add name=ether2-vlan74 vlan-id=74 interface=ether2 disabled=no
   ```

   Add comments as appropriate

   ```
   [admin@Peacock] > interface vlan print
   Flags: X - disabled, R - running
   #   NAME                        MTU   ARP   VLAN-ID INTERFACE
   0   R ;;; visp hotspot service 1500 enabled 71 ether2
       ether2-vlan71

   1   R ;;; v72 clickspot service 1500 enabled 72 ether2
       ether2-vlan72

   2   R ;;; clickspot – Seaview hotels 1500 enabled 73 ether2
       ether2-vlan73

   3   R ;;; clickspot – Parkview estate 1500 enabled 74 ether2
       ether2-vlan74
   ```
- Add IP addresses to the VLAN interfaces
- Create DHCP server on each VLAN interface

```
[admin@RT2] > ip dhcp-server print
Flags: X - disabled, I - invalid
#   NAME   INTERFACE   RELAY   ADDRESS-POOL   LEASE-TIME   ADD-ARP
0   dhcp-v71 ether2-vlan71 v71-dhcp 6h
1   dhcp-v72 ether2-vlan72 v72-dhcp 6h
2   dhcp-v73 ether2-vlan73 v73-dhcp 6h
3   dhcp-v74 ether2-vlan74 v74-dhcp 6h
```

- Create hotspot server on each VLAN interface

```
[admin@RT2] > ip hotspot print
Flags: X - disabled, I - invalid, S - HTTPS
#   NAME   INTERFACE   ADDRESS-POOL   PROFILE   IDLE-TIMEOUT
0   v71-clickspot ether2-vlan71 v71-clickspot none
1   v72-clickspot ether2-vlan72 v72-clickspot none
2   v73-clickspot ether2-vlan73 v73-clickspot none
3   v74-clickspot ether2-vlan74 v74-clickspot none
```
- Modify server profiles as necessary
  [admin@RT2] > ip hotspot profile print
  Flags: * - default
  0 * name="default" hotspot-address=0.0.0.0 dns-name="" html-directory="" rate-limit="" http-proxy=0.0.0.0:0 smtp-server=0.0.0.0
    login-by=http-chap,http-pap split-user-domain=no use-radius=no

  1 name="v71-clickspot" hotspot-address=192.168.0.1 dns-name=""
    html-directory=hotzone rate-limit="" http-proxy=0.0.0.0:0
    smtp-server=0.0.0.0 login-by=http-chap,http-pap split-user-domain=no
    use-radius=yes radius-accounting=yes radius-interim-update=received
    nas-port-type=wireless-802.11 radius-default-domain=""
    radius-location-id="" radius-location-name=""

  2 name="v72-clickspot" hotspot-address=192.168.1.1 dns-name=""
    html-directory=clickspot rate-limit="" http-proxy=0.0.0.0:0
    smtp-server=0.0.0.0 login-by=http-chap,http-pap split-user-domain=no
    use-radius=yes radius-accounting=yes radius-interim-update=received
    nas-port-type=wireless-802.11 radius-default-domain=""
    radius-location-id="" radius-location-name=""
- Create user Profiles
- Add Radius Servers
**Example:**
- Seaview hotel is buying 256/128kbps Internet from ITClick to resell using own branded login page to guests. Vouchers from seaview CANNOT be used elsewhere. Authentication and Vouchers are hosted at ITClick. Seaview will login to Mikrotik user manager hosted at ITClick to manage users and generate vouchers. Seaview is paying ITClick for both internet and voucher services.
  - Other customers must NOT see the Seaview login page
- RB2 is at the NOC and has wlan1, wlan2 and ether1
- RB7 is located at seaview hotel and has wlan1, wlan2 and ether1
- RB7 wlan1 is backhaul to RB2 wlan1 in 'station-wds' mode
- RB7 wlan2 is AP and repeater for remote customers
- Ether1 of RB7 will connect to hotel’s ‘VLAN dumb’ wireless APs.
- Ether1 of RB7 will be bridged to vlan73 on wireless
Thank you!

Sunday A. Idajili
sonny@itclick.net

Head Office:
ITClick Networx Limited
Suites B180/181
Ikota Shopping Complex, VGC,
Lekki, Lagos, Nigeria
Tel: +234-1-4616126, +234-1-8980156, +234-1-4722950

Branch Office:
ITClick Networx Limited
AP-B18, AMAC Commercial Complex
Kabale Close, Off Sultan Abubakar way,
Wuse Zone 3, Abuja, Nigeria.
Tel: +234-9-6726070, +234-9-5250044