Large Scale WiFi Deployment using MPLS/VPLS

Robert Patrick Harris, April 2015
Introduction

• Pat Harris
• Sr. Network Eng. for United States Sugar Corp.
• About U. S. Sugar Corp.
• Built around Mikrotik
• Our wireless system
A brief summary of U. S. Sugar Corp.

- Headquartered in Clewiston, Florida, the Company farms over 180,000 acres and operates a state-of-the-art citrus nursery on 80 acres in Northern Florida.
- U.S. Sugar is the USA’s largest vertically integrated producer of sugarcane and refined cane sugar.
- Our subsidiary, Southern Gardens Citrus, is one of Florida’s major growers of oranges and processors of orange juice products.
- In season, we process up to 42,000 tons of sugarcane per day and produce ~750,000 tons of refined sugar per year.
Due to the size of our land holdings and the real-time, requirements of Opx, an innovative solution was required. Cellular connectivity was ruled out due to cost availability and reliability. Other technologies considered, such as WiMax, were also deemed too costly to deliver an expected ROI.

The chosen solution was to build a private wireless WAN based upon the 802.11 standard. A combination of 120 to 140 foot towers, 50 foot towers, leased towers and sites on suitable tall structures within our plant facilities were used.
Design Considerations and requirements

- Direct client access.
- System wide roaming.
- Scalability
- Redundancy
- Enterprise security options compatible with a diverse array of client systems.
- Performance
- Cost
- Ease of Maintenance
- Ease of installation
- Availability of components

The solution to these requirements were met by Mikrotik
Building an MPLS/VPLS System

• When reviewing and selecting hardware consider interface MTU capability. Referencing Mikrotik documentation regarding maximum transmission unit on RouterBoards it will be understood the requirements imposed when implementing VLAN's, MPLS, VPLS etc.

-Example of normal frame.

• Example of frame with additional bytes supporting MPLS and VPLS.

Reference Material drawn from:
Building an MPLS/VPLS System

Normalize ROS and firmware releases.

It is much easier to configure and troubleshoot systems when working on a common release. We are currently on release 6.27 with no problems.

Configure the system building blocks, loopback’s, interfaces, logging, alerting, monitoring, dhcp, authentication methods, clock etc.

We can reference a small model system with some example output from a real production system.
Building an MPLS/VPLS System

A model to build upon.

Routerboard Material used in this example
4 – RB800
9 – R52Hn
# Building an MPLS/VPLS System

# on router X

```
/interf ace bridge
   add name=Loopback0 protocol-mode=rstp
   add name=Bridge_E2
/interf ace bridge port add interface=ether2 disabled=no
```

# on routers 1, 2 and 3

```
/interf ace bridge
   add name=Loopback0 protocol-mode=rstp
   add name=VPLS_Bridge  ← Note no stp mode for this configuration
/interf ace bridge port add interface=AP1 horizon=1 disabled=no
/interf ace bridge port add interface=AP2 horizon=1 disabled=no
/interf ace bridge port add interface=AP3 horizon=1 disabled=no
```

Note: repeat configuration for each identical site, modify as required.
Establish IP connectivity, configure and address interfaces. RouterX

/ip address
  add address=1.0.0.1/32 disabled=no interface=Loopback0
  add address=172.16.1.2/30 disabled=no interface=ether1 network=172.16.1.0
  add address=172.16.2.1/30 disabled=no interface=ether2 network=172.16.2.0
  add address=10.5.5.1/24 disabled=no interface=Bridge_E2 network=10.5.5.0

# our example is small so we will issue DHCP from RouterX
/ip pool add name=pool1 ranges=10.5.5.10-10.5.5.250
/ip dhcp-server add name=vpls_dhcp interface=Bridge_E2 lease-time=3d \
  address-pool=pool1 add-arp=yes authoratative=after-2sec-delay
/ip dhcp network set address=10.5.5.0/24 gateway=10.5.5.1 netmask=24\
  dns-server=10.x.x.3,10.x.x.4

Output from a production tower.

[admin@USSC-VAUGHN-800] > ip dhcp-server print detail
Flags: X - disabled, I - invalid
0   name="dhcp1" interface=VAUGHN_LANtoREF_LAN lease-time=1d
  address-pool=dhcp_pool1 bootp-support=static add-arp=yes
  authoritative=after-2sec-delay use-radius=yes lease-script=""
Building an MPLS/VPLS System

Establish IP connectivity, configure wireless security profiles and address interfaces. Router1

```
/interface wireless security-profiles
    add authentication-types=wpa2-psk group-ciphers=aes-ccm name=Profile1
    unicast-ciphers=aes-ccm  wpa2-pre-shared-key=K3y0fy0urC401c33
    add authentication-types=wpa2-psk group-ciphers=aes-ccm name=Profile2
    unicast-ciphers=aes-ccm wpa2-pre-shared-key= K3y0fy0urC401c34
```

Note: If radius authentication and accounting are used, the following commands are added to your wireless security profile.

```
radius-mac-authentication=yes radius-mac-accounting=yes interim-update=2m
```

```
/ip address
    add address=1.1.1.1/32 disabled=no interface=Loopback0
    add address=172.16.2.2/30 interface=ether2 network=172.16.2.0 disabled=no
    add address=10.1.1.1/30 interface=wlan1 network=10.1.1.0 disabled=no
    add address=10.1.1.5/30 interface=wlan2 network=10.1.1.0 disabled=no
    add address=10.5.5.5/24 interface=VPLS_Bridge network=10.5.5.0 disabled=no
```
Building an MPLS/VPLS System

Establish IP connectivity, configure wireless security profiles and address interfaces. Router2

/iface wireless security-profiles

[Example]

add authentication-types=wpa2-psk group-ciphers=aes-ccm name=Profile1
unicast-ciphers=aes-ccm wpa2-pre-shared-key=K3y0fy0urC401c33
add authentication-types=wpa2-psk group-ciphers=aes-ccm name=Profile2
unicast-ciphers=aes-ccm wpa2-pre-shared-key=K3y0fy0urC401c34

Note: If radius authentication and accounting are used, the following commands are added to the security profile.
radius-mac-authentication=yes radius-mac-accounting=yes interim-update=2m

/ip address

add address=1.1.1.2/32 disabled=no interface=Loopback0
add address=10.1.1.2/30 interface=wlan1 network=10.1.1.0 disabled=no
add address=10.1.1.9/30 interface=wlan2 network=10.1.1.0 disabled=no
add address=10.5.5.6/24 interface=VPLS_Bridge network=10.5.5.0 disabled=no
Building an MPLS/VPLS System

Establish IP connectivity, configure wireless security profiles and address interfaces. Router3

/interface wireless security-profiles  [Example]
  add authentication-types=wpa2-psk group-ciphers=aes-ccm name=Profile1
  unicast-ciphers=aes-ccm  wpa2-pre-shared-key=K3y0fy0urC401c33
  add authentication-types=wpa2-psk group-ciphers=aes-ccm name=Profile2
  unicast-ciphers=aes-ccm  wpa2-pre-shared-key= K3y0fy0urC401c34

Note: If radius authentication and accounting are used, the following commands are added to the security profile.

  radius-mac-authentication=yes  radius-mac-accounting=yes  interim-update=2m

/ip address
  add address=1.1.1.3/32 disabled=no interface=Loopback0
  add address=10.1.1.10/30 interface=wlan1 network=10.1.1.0 disabled=no
  add address=10.1.1.6/30 interface=wlan2 network=10.1.1.0 disabled=no
  add address=10.5.5.7/24 interface=VPLS_Bridge network=10.5.5.0 disabled=no
Building an MPLS/VPLS System

Establish IP connectivity, ensure devices see their neighbors, Links Up! Router1

/interface wireless

set interface=wlan1 band=5ghz or 2ghz channel-width=choose bandwidth
frequency=5XXX or 2XXX ht-txchains=0,1 if supported name=NameYourIF
mode=ap-bridge ssid=link1 nv2-cell-radius=SET as required
nv2-preshared-key="K3y0fy0urC401c33" nv2-qos=default nv2-queue-count=4
nv2-security=enabled security-profile=Profile1 tdma-period-size=2
wireless-protocol=nv2 wmm-support=enabled default-forwarding=no disabled=no

set interface=wlan2 band=5ghz or 2ghz channel-width=choose bandwidth
frequency=5XXX or 2XXX ht-txchains=0,1 if supported name=NameYourIF
mode=station ssid=link2 nv2-cell-radius=SET as required
nv2-preshared-key="K3y0fy0urC401c33" nv2-qos=default nv2-queue-count=4
nv2-security=enabled security-profile=Profile1 tdma-period-size=2
wireless-protocol=nv2 wmm-support=enabled default-forwarding=no disabled=no
Establish IP connectivity, ensure devices see their neighbors. Router1

set interface=wlan3 band=5ghz or 2ghz channel-width=choose bandwidth
frequency=5XXX or 2XXX ht-txchains=0,1 if supported name=NameYourIF
security-profile=Profile2 mode=ap-bridge ssid=AP1 disabled=no
wireless-protocol=802.11 wmm-support=enabled default-forwarding=no

set interface=wlan4 band=5ghz or 2ghz channel-width=choose bandwidth
frequency=5XXX or 2XXX ht-txchains=0,1 if supported name=NameYourIF
security-profile=Profile2 mode=ap-bridge ssid=AP2 disabled=no
wireless-protocol=802.11 wmm-support=enabled default-forwarding=no

set interface=wlan5 band=5ghz or 2ghz channel-width=choose bandwidth
frequency=5XXX or 2XXX ht-txchains=0,1 if supported name=NameYourIF
security-profile=Profile2 mode=ap-bridge ssid=AP3 disabled=no
wireless-protocol=802.11 wmm-support=enabled default-forwarding=no
Building an MPLS/VPLS System

Establish IP connectivity, ensure devices see their neighbors, Links Up! Router2

```
/interface wireless
   set interface=wlan1 band=5ghz or 2ghz channel-width=choose bandwidth
   frequency=5XXX or 2XXX ht-txchains=0,1 if supported name=NameYourIF
   mode=station ssid=link1 nv2-cell-radius=SET as required
   nv2-preshared-key=" K3y0fy0urC401c33 " nv2-qos=default nv2-queue-count=4
   nv2-security=enabled security-profile=Profile1 tdma-period-size=2
   wireless-protocol=nv2 wmm-support=enabled default-forwarding=no disabled=no
set interface=wlan2 band=5ghz or 2ghz channel-width=choose bandwidth
   frequency=5XXX or 2XXX ht-txchains=0,1 if supported name=NameYourIF
   mode=ap-bridge ssid=link2 nv2-cell-radius=SET as required
   nv2-preshared-key=" K3y0fy0urC401c33 " nv2-qos=default nv2-queue-count=4
   nv2-security=enabled security-profile=Profile1 tdma-period-size=2
   wireless-protocol=nv2 wmm-support=enabled default-forwarding=no disabled=no
```
Establish IP connectivity, ensure devices see their neighbors. Router2

```
set interface=wlan3 band=5ghz or 2ghz channel-width=choose bandwidth
frequency=5XXX or 2XXX ht-txchains=0,1 if supported name=NameYourIF
security-profile=Profile2 mode=ap-bridge ssid=AP1 disabled=no
wireless-protocol=802.11 wmm-support=enabled default-forwarding=no

set interface=wlan4 band=5ghz or 2ghz channel-width=choose bandwidth
frequency=5XXX or 2XXX ht-txchains=0,1 if supported name=NameYourIF
security-profile=Profile2 mode=ap-bridge ssid=AP2 disabled=no
wireless-protocol=802.11 wmm-support=enabled default-forwarding=no

set interface=wlan5 band=5ghz or 2ghz channel-width=choose bandwidth
frequency=5XXX or 2XXX ht-txchains=0,1 if supported name=NameYourIF
security-profile=Profile2 mode=ap-bridge ssid=AP3 disabled=no
wireless-protocol=802.11 wmm-support=enabled default-forwarding=no
```
Establish IP connectivity, ensure devices see their neighbors, Links Up! Router3

```
set interface=wlan1 band=5ghz or 2ghz channel-width=choose bandwidth
  frequency=5XXX or 2XXX ht-txchains=0,1 if supported name=NameYourIF
mode=station ssid=link1 nv2-cell-radius=SET as required
  nv2-preshared-key="K3y0fy0urC401c33" nv2-qos=default nv2-queue-count=4
nv2-security=enabled security-profile=Profile1 tdma-period-size=2
  wireless-protocol=nv2 wmm-support=enabled default-forwarding=no disabled=no
set interface=wlan2 band=5ghz or 2ghz channel-width=choose bandwidth
  frequency=5XXX or 2XXX ht-txchains=0,1 if supported name=NameYourIF
mode=ap-bridge ssid=link2 nv2-cell-radius=SET as required
  nv2-preshared-key="K3y0fy0urC401c33" nv2-qos=default nv2-queue-count=4
nv2-security=enabled security-profile=Profile1 tdma-period-size=2
  wireless-protocol=nv2 wmm-support=enabled default-forwarding=no disabled=no
```
Establish IP connectivity, ensure devices see their neighbors. Router3

```
set interface=wlan3 band=5ghz or 2ghz channel-width=choose bandwidth
frequency=5XXX or 2XXX ht-txchains=0,1 if supported name=NameYourIF
security-profile=Profile2 mode=ap-bridge ssid=AP1 disabled=no
wireless-protocol=802.11 wmm-support=enabled default-forwarding=no
```

```
set interface=wlan4 band=5ghz or 2ghz channel-width=choose bandwidth
frequency=5XXX or 2XXX ht-txchains=0,1 if supported name=NameYourIF
security-profile=Profile2 mode=ap-bridge ssid=AP2 disabled=no
wireless-protocol=802.11 wmm-support=enabled default-forwarding=no
```

```
set interface=wlan5 band=5ghz or 2ghz channel-width=choose bandwidth
frequency=5XXX or 2XXX ht-txchains=0,1 if supported name=NameYourIF
security-profile=Profile2 mode=ap-bridge ssid=AP3 disabled=no
wireless-protocol=802.11 wmm-support=enabled default-forwarding=no
```
Building an MPLS/VPLS System

What we have as an example. Three linked sites each with two backhauls and three access points for broadcast.
Building an MPLS/VPLS System

Configure and secure your routing protocols on your routers. For R1, R2 and R3

/routing ospf instance
set [ find default=yes ] redistribute-connected=as-type-1 \ 
    redistribute-static=as-type-1 router-id="Loopback0"
/routing ospf interface
add authentication=md5 authentication-key=ospfkey interface=Wlan1 \ 
    network-type=point-to-point
add interface=Loopback0 network-type=broadcast passive=yes
add authentication=md5 authentication-key=ospfkey interface=Wlan2 \ 
    network-type=point-to-point
/routing ospf network
add area=backbone network=10.1.1.0/24
add area=backbone network=Loopback0/32
For R1 include the following config.
add authentication=md5 authentication-key=ospfkey interface=ether1 \ 
    network-type=point-to-point
Add area=backbone network=172.16.2.0/24
Configure and secure your routing protocols on your router X.

/routing ospf instance
set [ find default=yes ] redistribute-connected=as-type-1 \redistribute-static=as-type-1 router-id="Loopback0"

/routing ospf interface
add authentication=md5 authentication-key=ospfkey interface=ether1 \network-type=point-to-point
add interface=Loopback0 network-type=broadcast passive=yes
add authentication=md5 authentication-key=ospfkey interface=ether2 \network-type=point-to-point

/routing ospf network
add area=backbone network=10.1.1.0/24
add area=backbone network=172.16.1.0/30
add area=backbone network=172.16.2.0/30
add area=backbone network=Loopback0/32
[admin@Ref_800] > routing ospf neighbor print
0 instance=default router-id=10.X.X.105 address=172.X.X.129 interface=Interface1
    priority=1 dr-address=0.0.0.0 backup-dr-address=0.0.0.0 state="Full"
    state-changes=4 ls-retransmits=0 ls-requests=0 db-summaries=0
    adjacency=8w4d20h11m10s

1 instance=default router-id=10.X.X.70 address=192.X.X.2 interface=Interface2
    priority=1 dr-address=0.0.0.0 backup-dr-address=0.0.0.0 state="Full"
    state-changes=4 ls-retransmits=0 ls-requests=0 db-summaries=0
    adjacency=2w5d10h18m13s
Now we will add MPLS to our network, all interfaces forwarding traffic up to PE should be included in this configuration.

# on all routers

```
/mls
set dynamic-label-range=16000-1048575 <- Consider leaving an open range for future options
```

```
/mls ldp
set enabled=yes lsr-id=Loopback0 transport-address=Loopback0
```

# on router X

```
/mls interface
set [ find default=yes ] mpls-mtu=1526 <- As required and supported
add interface=ether2 mpls-mtu=1526 <- As required and supported
```

```
/mls ldp interface
add interface=ether2
```
Building an MPLS/VPLS System

# on router R1

/mpls
set dynamic-label-range=16000-1048575 <- Consider leaving an open range for future options

/mls ldp
set enabled=yes lsr-id=Loopback0 transport-address=Loopback0

/mls interface
set [ find default=yes ] mpls-mtu=1526 <- As required and supported
add interface=ether1 mpls-mtu=1526 <- As required and supported
add interface=wlan1 mpls-mtu=1526<- As required and supported
add interface=wlan2 mpls-mtu=1526 <- As required and supported

/mls ldp interface
add interface=ether1
add interface=wlan1
add interface=wlan2
Building an MPLS/VPLS System

# on router R2 and R3

/mpls
set dynamic-label-range=16000-1048575 <- Consider leaving an open range for future options

/mpls ldp
set enabled=yes lsr-id=Loopback0 transport-address=Loopback0

/mpls interface
set [ find default=yes ] mpls-mtu=1526 <- As required and supported
add interface=wlan1 mpls-mtu=1526 <- As required and supported
add interface=wlan2 mpls-mtu=1526 <- As required and supported

/mpls ldp interface
add interface=wlan1
add interface=wlan2
Now we have added MPLS to our system.
Building an MPLS/VPLS System

An example from a production Tower.

[admin@USSC-VAUGHN-800] > mpls ldp neighbor print
Flags: X - disabled, D - dynamic, O - operational, T - sending-targeted-hello, V - vpls

<table>
<thead>
<tr>
<th>#</th>
<th>TRANSPORT</th>
<th>LOCAL-TRANSPORT</th>
<th>PEER</th>
<th>SEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>10.x.x.128</td>
<td>10.x.x.119</td>
<td>10.x.x.128:0</td>
<td>no</td>
</tr>
<tr>
<td>1</td>
<td>10.x.x.116</td>
<td>10.x.x.119</td>
<td>10.x.x.116:0</td>
<td>no</td>
</tr>
</tbody>
</table>

[admin@USSC-VAUGHN-800] > mpls remote-bindings print
Flags: X - disabled, A - active, D - dynamic

<table>
<thead>
<tr>
<th>#</th>
<th>DST-ADDRESS</th>
<th>NEXTHOP</th>
<th>LABEL</th>
<th>PEER</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>10.x.x.105/32</td>
<td>172.x.x.197</td>
<td>23897</td>
<td>10.x.x.128:0</td>
</tr>
<tr>
<td>1</td>
<td>10.x.x.0/24</td>
<td>172.x.x.197</td>
<td>23134</td>
<td>10.x.x.128:0</td>
</tr>
<tr>
<td>2</td>
<td>172.x.x.184/30</td>
<td>172.x.x.197</td>
<td>23136</td>
<td>10.x.x.128:0</td>
</tr>
<tr>
<td>3</td>
<td>10.x.x.0/24</td>
<td>172.x.x.197</td>
<td>23137</td>
<td>10.x.x.128:0</td>
</tr>
<tr>
<td>4</td>
<td>172.x.x.0/24</td>
<td>172.x.x.197</td>
<td>23139</td>
<td>10.x.x.128:0</td>
</tr>
<tr>
<td>5</td>
<td>10.x.x.0/24</td>
<td>172.x.x.197</td>
<td>23140</td>
<td>10.x.x.128:0</td>
</tr>
<tr>
<td>6</td>
<td>10.x.x.0/24</td>
<td>172.x.x.197</td>
<td>23141</td>
<td>10.x.x.128:0</td>
</tr>
<tr>
<td>7</td>
<td>10.x.x.115/32</td>
<td>172.x.x.98</td>
<td>16348</td>
<td>10.x.x.116:0</td>
</tr>
</tbody>
</table>
Building an MPLS/VPLS System

[admin@USSC-VAUGHN-800] > mpls local-bindings print


<table>
<thead>
<tr>
<th>#</th>
<th>DST-ADDRESS</th>
<th>LABEL</th>
<th>PEERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>ADLe 10.X.X.119/32</td>
<td>impl-null</td>
<td>10.X.X.116:0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10.X.X.128:0</td>
</tr>
<tr>
<td>1</td>
<td>ADG 172.X.X.44/30</td>
<td>43353</td>
<td>10.X.X.116:0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10.X.X.128:0</td>
</tr>
<tr>
<td>2</td>
<td>ADG 10.X.X.109/32</td>
<td>43354</td>
<td>10.X.X.116:0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10.X.X.128:0</td>
</tr>
<tr>
<td>3</td>
<td>ADG 10.X.X.107/32</td>
<td>43355</td>
<td>10.X.X.116:0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10.X.X.128:0</td>
</tr>
</tbody>
</table>

4/25/2015 29
Building an MPLS/VPLS System

We will use BGP to signal reach ability for our VPLS tunnels.

On a tower router (R2) we will use the default instance.
/routing bgp instance set router-id=1.1.1.2 client-to-client-reflection=yes
/routing bgp peer set address-families=l2vpn name=R2_R1peer remote-address=1.1.1.1\remote-as=65530 tcp-md5-key=bgpkey update-source=Loopback0

On a tower router (R3) we will also use the default instance.
/routing bgp instance set router-id=1.1.1.3 client-to-client-reflection=yes
/routing bgp peer set address-families=l2vpn name=R3_R1peer remote-address=1.1.1.1\remote-as=65530 tcp-md5-key=bgpkey update-source=Loopback0

On router (RX) we will use the default instance.
/routing bgp instance set router-id=1.0.0.1 client-to-client-reflection=yes
/routing bgp peer set address-families=l2vpn name=RX_R1peer remote-address=1.1.1.1\remote-as=65530 tcp-md5-key=bgpkey update-source=Loopback0
Building an MPLS/VPLS System

Even though our example system is quite small we will use route reflection.

So on a tower router (R1) we will again use the default instance.

```
/routing bgp instance set router-id=1.1.1.1 client-to-client-reflection=yes
/routing bgp peer set address-families=l2vpn name=R1_R2peer remote-address=1.1.1.2
remote-as=65530 route-reflect=yes tcp-md5-key=bgpkey update-source=Loopback0
/routing bgp peer set address-families=l2vpn name=R1_R3peer remote-address=1.1.1.3
remote-as=65530 route-reflect=yes tcp-md5-key=bgpkey update-source=Loopback0
/routing bgp peer set address-families=l2vpn name=R1_RXpeer remote-address=1.0.0.1
remote-as=65530 route-reflect=yes tcp-md5-key=bgpkey update-source=Loopback0
```

Output from a route reflector.

[admin@USSC600-433] > routing bgp peer print

Flags: X - disabled, E - established

<table>
<thead>
<tr>
<th>#</th>
<th>INSTANCE</th>
<th>REMOTE-ADDRESS</th>
<th>REMOTE-AS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>E default</td>
<td>10.x.x.103</td>
<td>65530</td>
</tr>
<tr>
<td>1</td>
<td>E default</td>
<td>10.x.x.107</td>
<td>65530</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>E default</td>
<td>10.x.x.109</td>
<td>65530</td>
</tr>
<tr>
<td>3</td>
<td>E default</td>
<td>10.x.x.115</td>
<td>65530</td>
</tr>
<tr>
<td>4</td>
<td>E default</td>
<td>10.x.x.111</td>
<td>65530</td>
</tr>
<tr>
<td>5</td>
<td>E default</td>
<td>10.x.x.120</td>
<td>65530</td>
</tr>
<tr>
<td>6</td>
<td>E default</td>
<td>10.x.x.114</td>
<td>65530</td>
</tr>
</tbody>
</table>

etc.

Output from a tower.

[admin@USSC-VAUGHN-800] > routing bgp peer print

Flags: X - disabled, E - established

<table>
<thead>
<tr>
<th>#</th>
<th>INSTANCE</th>
<th>REMOTE-ADDRESS</th>
<th>REMOTE-AS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>E default</td>
<td>10.x.x.107</td>
<td>65530</td>
</tr>
<tr>
<td>1</td>
<td>E default</td>
<td>10.x.x.105</td>
<td>65530</td>
</tr>
</tbody>
</table>

<- peered with route reflectors

4/25/2015
[admin@USSC-VAUGHN-800] > routing bgp peer print detail
Flags: X - disabled, E - established
0 E name="VA-LH433peer" instance=default remote-address=10.X.X.107
    remote-as=65530 tcp-md5-key="bgpkey" nexthop-choice=default
    multihop=no route-reflect=no hold-time=3m ttl=255 in-filter=""
    out-filter="" address-families=l2vpn update-source=Loopback0
    default-originate=never remove-private-as=no as-override=no passive=no
    use-bfd=no

1 E name="VA-600_433peer" instance=default remote-address=10.X.X.105
    remote-as=65530 tcp-md5-key="bgpkey" nexthop-choice=default
    multihop=no route-reflect=no hold-time=3m ttl=255 in-filter=""
    out-filter="" address-families=l2vpn update-source=Loopback0
    default-originate=never remove-private-as=no as-override=no passive=no
    use-bfd=no
Set up your vpls tunnels

```
/interface vpls bgp-vpls <- Egress Bridge
# on router RX
add bridge=Bridge_E2 bridge-cost=0 bridge-horizon=3 export-route-targets=1:1 \import-route-targets=1:1 site-id=4 name=VPLS_RX>R1 route-distinguisher=1:1
add bridge=Bridge_E2 bridge-cost=0 bridge-horizon=3 export-route-targets=2:2 \import-route-targets=2:2 site-id=4 name=VPLS_RX>R2 route-distinguisher=2:2
add bridge=Bridge_E2 bridge-cost=0 bridge-horizon=3 export-route-targets=3:3 \import-route-targets=2:2 site-id=4 name=VPLS_RX>R3 route-distinguisher=3:3

/interface vpls bgp-vpls <- Tower Bridge R1
add name="VPLS_R1>RX" route-distinguisher=1:1 import-route-targets=1:1 export-route-targets=1:1 site-id=1 bridge=VPLS_Bridge bridge-cost=0 bridge-horizon=2 use-control-word=yes
```
Set up your vpls tunnels

`/interface vpls bgp-vpls  <- Tower Bridge R2`
  `add name="VPLS_R2>RX" route-distinguisher=2:2 import-route-targets=2:2`
  `export-route-targets=2:2 site-id=2 bridge=VPLS_Bridge`
  `bridge-cost=0 bridge-horizon=2 use-control-word=yes`

`/interface vpls bgp-vpls  <- Tower Bridge R3`
  `add name="VPLS_R3>RX" route-distinguisher=3:3 import-route-targets=3:3`
  `export-route-targets=3:3 site-id=3 bridge=VPLS_Bridge`
  `bridge-cost=0 bridge-horizon=2 use-control-word=yes`
Output from an egress bridge.

[admin@REF-RB1200] > interface vpls print brief

Flags: X - disabled, R - running, D - dynamic, B - bgp-signaled, C - cisco-bgp-signaled

<table>
<thead>
<tr>
<th>#</th>
<th>NAME</th>
<th>REMOTE-PEER</th>
<th>VPLS-ID</th>
<th>VPLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>RDB vpls328</td>
<td>10.X.X.104</td>
<td></td>
<td>VPLS_5n</td>
</tr>
<tr>
<td>1</td>
<td>RDB vpls329</td>
<td>10.X.X.123</td>
<td></td>
<td>REF1200-</td>
</tr>
<tr>
<td>2</td>
<td>RDB vpls330</td>
<td>10.X.X.122</td>
<td></td>
<td>REF1200-</td>
</tr>
<tr>
<td>3</td>
<td>RDB vpls343</td>
<td>10.X.X.104</td>
<td></td>
<td>REF1200-</td>
</tr>
<tr>
<td>4</td>
<td>RDB vpls380</td>
<td>10.X.X.126</td>
<td></td>
<td>REF1200-</td>
</tr>
<tr>
<td>5</td>
<td>RDB vpls382</td>
<td>10.X.X.118</td>
<td></td>
<td>VPLS_5n</td>
</tr>
<tr>
<td>6</td>
<td>RDB vpls387</td>
<td>10.X.X.118</td>
<td></td>
<td>REF1200-</td>
</tr>
</tbody>
</table>

ETC.

Output from a tower bridge.

[admin@USSC-VAUGHN-800] > interface vpls bgp-vpls print

Flags: X - disabled, I - inactive

<table>
<thead>
<tr>
<th>#</th>
<th>NAME</th>
<th>ROUTE-DISTINGUISHER</th>
<th>SITE-ID BRIDGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>VA-REF1200</td>
<td>8:8</td>
<td>14 VAUGHN_LANto...</td>
</tr>
</tbody>
</table>
What we have built.

How has our system evolved. Our tower LANs can forward data.
A few tips.

Disable services not required for operations, Set ACL’s for access to management protocols and consider disabling unsecure services.

/ip service set address=10.10.10.10 port=8291 disabled=no
/ip service set address=10.10.10.10 port=22 disabled=no
/ip service disable 0
/ip service disable 1

Output from a production router.

[admin@RB2011-H] > ip service print

Flags: X - disabled, I - invalid

<table>
<thead>
<tr>
<th>#</th>
<th>NAME</th>
<th>PORT</th>
<th>ADDRESS</th>
<th>CERTIFICATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 X</td>
<td>telnet</td>
<td>23</td>
<td>10.X.X.0/24</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>172.X.X.0/24</td>
<td></td>
</tr>
<tr>
<td>1 X</td>
<td>ftp</td>
<td>21</td>
<td>10.X.X.0/24</td>
<td></td>
</tr>
</tbody>
</table>

Time is an important component to coordinate system functions, scheduling, logging etc.

/system ntp client set enabled=yes primary-ntp=10.x.x.1 secondary-ntp=10.x.x.2
/system clock set time-zone-name=est5edt
Additional Tips.

- Alerting can be considered and configured in various ways. We use the Dude and Solar Winds NPM, there are many options both commercial and open source to choose from. Also consider configuring an alert upon login to critical devices.
- tool e-mail set address=Mail Xchanger n.n.n.n from=YourDevice@yourco.com
- system logging action set name=action1 target=email email-to=netadmin@yourco.com
- system logging set topics=account action=action1
- Authentication to your device may be managed in various ways. Mikrotik supports various options. Consider limiting access to your device by subnet, user group with reduced privilege. Radius authentication offers more centralized control of access and accountability for logged in users.
  
  - user group add name=limitpriv
    policy=local,telnet,ssh,read,winbox,!ftp,!reboot,!write,!policy,!test,!password,!web,!sniff,!sensitive,!api
  - user aaa set use-radius=yes accounting=yes default-group=limitpriv
  - radius add service=login address=1.1.1.1 secret=secret

Note: If radius authentication and accounting are used, the following commands are added to your wireless security profile.

radius-mac-authentication=YES radius-mac-accounting=YES interim-update=(n)m <- your call
Some log output from the radius server

Passed Authentication examples:

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Message-Type</th>
<th>User-Name</th>
<th>Group-Name</th>
<th>NAS-Port</th>
<th>NAS-IP-Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/5/2015</td>
<td>0:54:28</td>
<td>Authen OK</td>
<td>00:17:47:12:34:56</td>
<td>Group 3</td>
<td>2202046826</td>
<td>172.X.X.34</td>
</tr>
<tr>
<td>4/5/2015</td>
<td>0:58:30</td>
<td>Authen OK</td>
<td>00:20:4A:12:34:56</td>
<td>Group 3</td>
<td>2202046827</td>
<td>172.X.X.34</td>
</tr>
<tr>
<td>4/5/2015</td>
<td>4:27:29</td>
<td>Authen OK</td>
<td>00:17:47:12:34:56</td>
<td>Group 3</td>
<td>2202046832</td>
<td>172.X.X.34</td>
</tr>
</tbody>
</table>

Failed Authentication examples:

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Message-Type</th>
<th>User-Name</th>
<th>Group-Name</th>
<th>Caller-ID</th>
<th>Authen-Failure-Code</th>
<th>NAS-IP-Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/5/2015</td>
<td>16:37:45</td>
<td>Authen failed</td>
<td>00:1C:58:57:40:8B</td>
<td>Default Group</td>
<td>1:01c:58:57:40:8b</td>
<td>External DB user invalid or bad password</td>
<td>10.X.X.119</td>
</tr>
<tr>
<td>4/5/2015</td>
<td>16:37:45</td>
<td>Authen failed</td>
<td>00:1C:58:57:40:8B</td>
<td>Default Group</td>
<td>1:01c:58:57:40:8b</td>
<td>External DB user invalid or bad password</td>
<td>10.X.X.119</td>
</tr>
<tr>
<td>4/5/2015</td>
<td>16:44:35</td>
<td>Authen failed</td>
<td>00:1C:58:57:40:8B</td>
<td>Default Group</td>
<td>1:01c:58:57:40:8b</td>
<td>External DB user invalid or bad password</td>
<td>10.X.X.119</td>
</tr>
<tr>
<td>4/5/2015</td>
<td>16:44:35</td>
<td>Authen failed</td>
<td>00:1C:58:57:40:8B</td>
<td>Default Group</td>
<td>1:01c:58:57:40:8b</td>
<td>External DB user invalid or bad password</td>
<td>10.X.X.119</td>
</tr>
</tbody>
</table>
Additional notes:

• You may enhance your system with traffic engineering, packet marking and prioritization, consider scripting to automate desired functions.

One of the scripts we run collect registration stats from the towers that are uploaded via FTP and combined with GPS location data that is fed to an application that displays. Client signal level and quality in relation to location from tower.

```
:for fileCount from=1 to=1440 do=
  interface wireless registration-table print stats file="/Stats/WiFistats$fileCount";
  :delay 1m;
```

How is this data used?

An application developed in house renders the data collected from the towers into a format that permits the overall observation of client performance. Over time this data can reveal a dynamic coverage map and output can be compared against baseline performance to identify and address any possible issues.
How is this data used?

Additional output. Hovering a data point with some statistical detail.
How is this data used?

Additional output. Zoomed in reveals more activity.
How is this data used?

Additional output. Zoomed in views. The daily progress may be followed.
Our System

A 300~ square mile (77,600 hectare) network.
Our System

Putting a perspective on things.
Our System
Configurations

- We will display two different form factors as applied in the field.
- One design employs separate Routerboards for the point to point and broadcast duties.
Configurations

- We will display two different form factors as applied in the field.
- The other combines point to point and broadcast duties.
Reference Material


**MUM US09: MPLS by Janis Megis**

- Routerboard MTU
- MPLS TE
Conclusion

Thank You for your time…

Questions?
United States Sugar Corporation