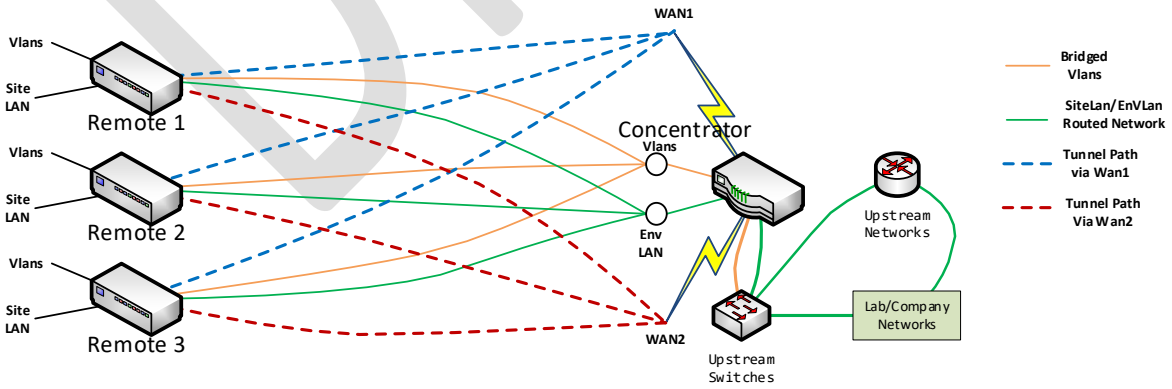
Remote Lab Environment
LabRmt

RingCentral Custom Engineering (CE) has some unique networking requirements. Most of the engineers work remotely across the globe. These engineers need access to a complex laboratory network that includes shared VLANs to work most efficiently, even to the extent of extending public WAN subnets to remote users. The LabRmt platform described in this document has been developed to provide this environment in a secure and inexpensive manner.

Overview

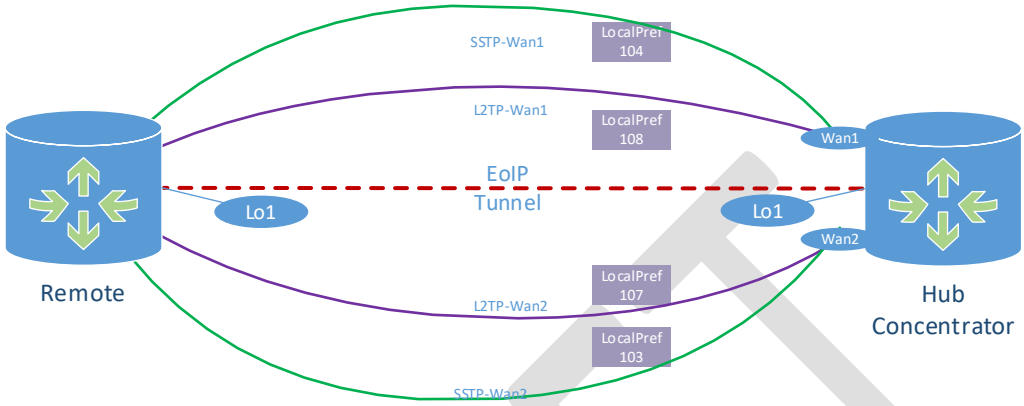
The LabRmt platform uses consumer network devices in a hub and spoke configuration to deliver a /16 routed laboratory network (EnvLanNet) and bridge multiple laboratory VLANs securely to remote sites across the public internet. It consists of a central network concentrator device (concentrator) and multiple (up to 239) remote site network devices (remotes). The concentrator provides completely automated and transparent failover between dual WAN links at the central site. It supports full 1500-byte packets for all network traffic, regardless of intervening network limitations.

The LabRmt platform supports multiple parallel Environments. Each LabRmt Environment consists of a single concentrator and up to 239 possible remotes. Any number of LabRmt Environments may be run in parallel so long as there are no IP or MAC address conflicts, for instance a company's development and production environments. Similarly, systems for IT and Engineering may be run in parallel. The following diagram shows the relationship between the remote sites and the central concentrator. The dashed lines show the encrypted tunnels between devices while the solid lines show the logical data flow between devices.



LabRemote General Layout

There is currently no automated coordination between the concentrator configuration and the remotes. Scripts to add vlans, map vlans to remote units, etc. must be run on both the concentrator and remote units individually.



Hub ⇔ Remote Logical Connection Diagram

Hardware

LabRmt is based upon hardware from Mikrotik. This hardware is inexpensive and quite robust. The Mikrotik ***hEX S*** (RB760iGS), current MSRP of US$79.00, functions well as a development platform; it has 5 Gigabit copper ports and 1 Gigabit fiber SFP port, supports AES256-CBC hardware encryption, and can be used as a concentrator for smaller production environments. Mikrotik has many different device models that can be utilized as remotes, the choice depends on which physical features (port count, SFP slots, WiFi radios, hardware encryption support, and/or LTE) are desired.

All device configurations are currently based upon Mikrotik ROS Version V6.49.x.

Concentrator Appliance

The concentrator appliance acts as the central hub for a LabRmt Environment. It supports 2 WAN connections for tunnel termination and 1 LAN connection for Layer-3 IP routing to/from the upstream lab network. It also accepts multiple VLAN appearances for Layer-2 bridging.

The concentrator is connected to an upstream switch or switch stack using an IEEE 803.3ad Link Aggregation Control Protocol (LACP) bonded port group. All laboratory network connections are delivered using VLANs trunked over this LACP bonded port group. Splitting LACP ports across the members of a 'virtual switch stack' is highly recommended. This practice provides protection from failure of a single upstream switch. Switch stacks are supported by several switch manufacturers, among the vendors are Cisco, Extreme, Dell, Huawei, and Juniper.

Two WAN VLANs have a statically addressed Layer-3 presence on the concentrator and are used to terminate tunnels from the remotes. One LAN VLAN has a statically addressed Layer-3 presence on the concentrator and is used to route internal IP traffic between this LabRmt Environment and the

remainder of the upstream network. These three VLANs are predefined on the concentrator and can be bridged to remotes if needed for Layer-2 purposes.

Two encrypted tunnel servers are created on each WAN link, one based on L2TP/IPSEC and one based on SSTP. The SSTP tunnel is normally disabled on the remote side as the L2TP/IPSEC tunnel is much more efficient but can be enabled when the remote is unable to pass L2TP traffic - such as when used in hotels and public locations. The L2TP/IPSEC encryption parameters may be altered in the build configuration file to support differing encryption hardware capabilities of different concentrator models.

Remote Appliances

A remote provides connectivity to the LabRmt Environment defined by its associated concentrator. Access to the Layer-3 network and Layer-2 VLANs located at the central site is provided using this remote.

The remote connects to a local ISP using DHCP on a specified port. Once the connection is established, the remote will establish L2TP/IPSEC and, optionally, SSTP tunnels back to each of the two WAN addresses on the associated concentrator.

The iBGP routing protocol is used in conjunction with BFD to support tunnel prioritization and rapid failure detection/failover. Failover times are under 1.5 seconds, which nears those of some relatively expensive SD-Wan solutions.

Dual WAN support on the remote has not been implemented at this time as most remote sites have access to only one ISP link. Hooks to implement it in a future release have been reserved.

Internals

Encryption

The default encryption settings are SHA-256/AES256-CBC/ecp521, the maximum security level supported by the hardware encryption accelerator in the Mikrotik ***hEX S*** (RB760iGS) device. There are some Mikrotik models with different hardware that support the CTR and GCM encryption algorithms.

The settings are global for the entire LabRmt Environment. The settings may be altered in the environment build configuration file initially used to establish the system to conform with the hardware supported by the selected concentrator device.

Layer-3 Traffic Routing

A single /16 CIDR network block is allocated for each environment using configuration file parameter ***EnvLanNet***. The first /24 block (3rd octet value of 0) is reserved and is used to allocate loopback identification addresses (Loopback1) for each appliance. The fourth octet in the Loopback1 address is the remote unit number or 254 for the concentrator. The remainder of ***EnvLanNet*** is allocated to the remotes in /24 blocks (third octet is the remote unit number) and will be used as a ***SiteLan***. The ***SiteLan*** network block and the Loopback1 interface address are advertised by iBgp. All unused ports on the remote default to access mode ports on ***SiteLan***.

EnvLanNet had 8 reserved /24 blocks that are used for tunnel addressing. Four of these are in current use and four are reserved for a future redundant WAN link on remote nodes as shown in this table:

Network Block	Purpose
EnvLanNet.0.x/24	Used for Loopback addresses
EnvLanNet.240.x/24	L2TP from Remote WAN1 to Concentrator WAN1
EnvLanNet.241.x/24	L2TP from Remote WAN1 to Concentrator WAN2
EnvLanNet.242.x/24	L2TP from Remote WAN2 to Concentrator WAN1 *(Reserved for future use.)*
EnvLanNet.243.x/24	L2TP from Remote WAN2 to Concentrator WAN2 *(Reserved for future use.)*
EnvLanNet.244.x/24	SSTP from Remote WAN1 to Concentrator WAN1
EnvLanNet.245.x/24	SSTP from Remote WAN1 to Concentrator WAN2
EnvLanNet.246.x/24	SSTP from Remote WAN2 to Concentrator WAN1 *(Reserved for future use.)*
EnvLanNet.247.x/24	SSTP from Remote WAN2 to Concentrator WAN2 *(Reserved for future use.)*

Grayed out entries are reserved for future use.

A mesh of logical tunnels is used to carry Layer-3 IP traffic between the concentrator and the remotes. These tunnels are established diversely using the two different WAN links on the concentrator and two different connectivity technologies, L2TP/IPSEC (Preferred) and SSTP. Note that SSTP tunnels must be manually enabled. All Layer-3 tunnels are configured to support Multilink-PPP so that 1500 byte packets are automatically and transparently fragmented and reassembled as needed. Bidirectional Forwarding Detection (BFD) is utilized on the tunnel interfaces to provide extremely rapid link failure detection.

The iBGP protocol runs across all active tunnels. Precedence of the four tunnels is established using iBGP LocalPref values shown in ***Table 1*** below. Note that in iBGP higher LocalPref values are the most preferred. ***There is no load balancing in this system, all traffic flows exclusively on the most preferred active tunnel.***

	L2TP/Ipsec		SSTP	
	Rmt Wan1	Rmt Wan2	**Rmt Wan1**	Rmt Wan2
Wan1 Provider	108	106	104	102
Wan2 Provider	107	105	103	101

Table 1 *- iBGP LocalPref (Grayed out is for future feature)*

Use of iBGP is local to the concentrator and associated remotes. There is no provision in the code for dynamic routing between the concentrator and the upstream network using any routing protocol. The upstream lab network must have a static route delivering the ***EnvLanNet*** /16 block to the concentrator's LAN interface IP address.

L2TP/IPSEC is the preferred tunnel protocol as the tunnel encryption is hardware assisted and thus has much higher throughput and less processing overhead. The SSTP tunnels are disabled by default on the remote unit – a script must be executed on the remote unit to enable them. There is no need to enable the SSTP tunnels unless the remote needs to operate in a restrictive environment where L2TP/IPsec is not allowed, such as a hotel or conference center. They may be left enabled if desired as there is no issue other than some additional processing overhead for tunnel maintenance and routing.

Wan1 has arbitrarily been chosen as the primary link. As shown in '*Table 1 - iBGP LocalPref*', for each tunnel type the Wan1 link has the higher LocalPref value.

An environment build configuration parameter introduced in Version 7.0, ***DefRouteType***, provides the following selections for routing non-local Layer-3 IP traffic.

DefRouteType **Value**	**Routing Action**
viaLocalOnly	Only RFC1918 (private) address space is sent to the concentrator for routing/distribution. All other traffic sent out the WAN link after having overload NAT applied.
viaHubOnly	All traffic is sent to the concentrator for routing/distribution. (Allows for enforced central firewall/policy decisions.)
viaHubPreferred	Same as 'viaHubOnly', except when all tunnels are down non-RFC1918 traffic will be sent out the WAN link after having overload NAT applied.

Layer-2 Traffic Bridging

Layer-2 VLAN bridging is based upon a Mikrotik proprietary Ethernet over IP (EoIP) tunnel with a 1500 byte MTU. A single EoIP tunnel is created between each remote appliance and the concentrator appliance. It will always be carried over the currently preferred tunnel. The EoIP tunnel route will shift between tunnels transparently.

EoIP tunnels are established between the Loopback1 interface on the concentrator appliance and the Loopback1 interface on the remote appliances. The Loopback1 interface addresses are part of the iBGP routing tables and, as a result, layer-3 and EoIP traffic will flow over the best currently active tunnel between the Loopback interfaces. Each Layer-2 VLAN bridge is created as a logical subinterface of the EoIP tunnel and becomes part of a bridge group named for the VLAN.

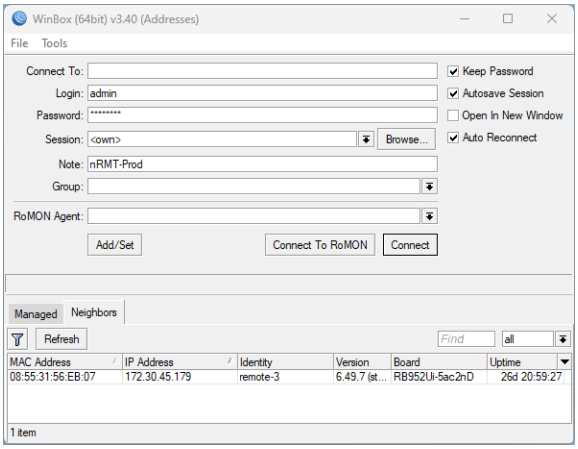
Layer-2 VLANs may be presented as access mode ports or as trunked VLANs on the remote unit. This is configured on a per-remote basis using scripts on the remote unit.

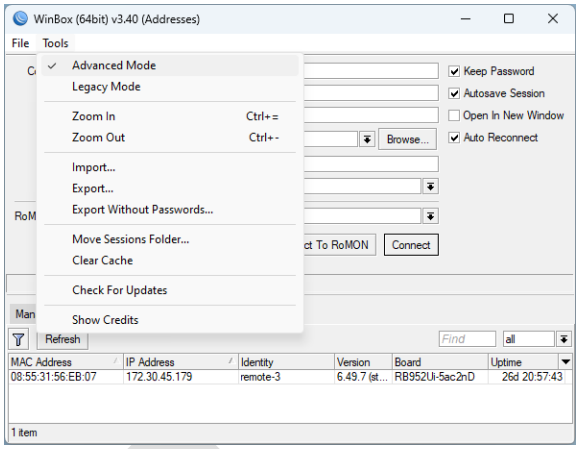
Installation

There are two installation scripts, one for the concentrator and one for the remote. Installation requires a computer running Windows and the Mikrotik 'Winbox' GUI. These scripts use an environment build configuration file which may be edited to change the default information used in parallel setups.

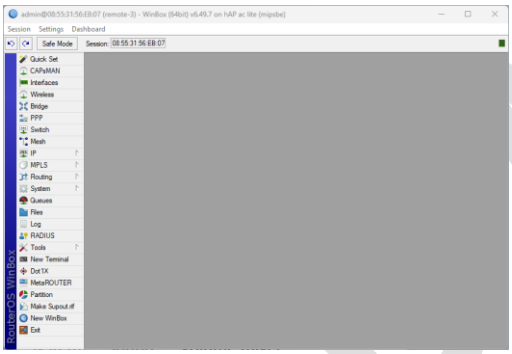
Beware, edit ONLY the relevant information and be careful of punctuation – the Mikrotik scripting language has very complex punctuation rules and an errant keypress can be all but impossible to troubleshoot!

The Mikrotik 'Winbox' GUI can be downloaded from ***https://mikrotik.com/download***. Ensure that you download the version appropriate for your version of Windows, 32-bit or 64-bit. (Note that if you encounter any issues getting to that website there is a 64-bit version of winbox available on the CELab website alongside the scripts. It is not guaranteed to be the latest version, but it should work.) The Mikrotik 'Winbox' GUI allows you to connect to a Mikrotik device by either IP address OR, more importantly, by using its layer-2 MAC address. It provides drag-n-drop file copy functionality and console access on the Windows desktop.

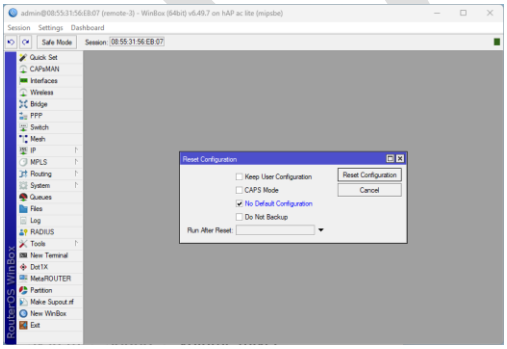




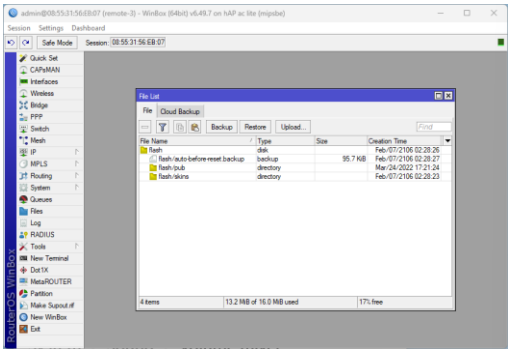
You must start with a completely blank configuration. Once you see the node show up in the 'Neighbors' tab, click on the MAC Address of the node, then click on the 'Connect' button. Note that if you have an existing configuration on the device you will need to supply the correct username and password to connect.



Click on 'System', then select 'Reset Configuration'. You should check the 'No Default Configuration' and 'Do Not Backup' checkboxes. If you want to keep your existing usernames and passwords you should check the 'Keep User Configuration' checkbox, otherwise you will end up with a single username of 'admin' and a blank password. (Note – You will be required to set the password upon initial login!)



Use the Winbox GUI to log in using the MAC Address once again, then click on 'Files'.



Now you are ready to proceed with the LabRmt configuration.

Note that you will need a PKCS12 certificate signed with the private key. Wild-card domain certificates are acceptable for this purpose. There is a dummy self-signed certificate with a dummy CA certificate available within the LabRmt system generation scripts which will be downloaded in the next step. The procedure for generating self-signed certificates using OpenSSL is provided in Appendix A. Note that these certificates are ONLY used locally in the LabRmt Environment.

Download the LabRmt system generation scripts zipfile from the repository located at https://www.celab.ringcentral.com/LabRmt. Edit the build configuration script, *build-defs.rsc*, to set the local information to the desired values for this LabRmt Environment. ***Carefully save this build configuration script file as you will need to use it for EACH remote node you wish to add to this LabRmt Environment now and in the future.***

Concentrator

Use file manager to drag the *MasterConcBuild-Vx-x.rsc* script file, the *build-defs.rsc* build configuration script file, and the PKCS12 (*.pfx*) certificate file to the 'Files' window in the Winbox GUI. This copies the files to the concentrator device.

Using the Winbox GUI click on 'New Terminal'. A terminal screen will open on the GUI. Hit the Enter key several times to make sure you have a working prompt. On the terminal screen enter the command '`import MasterConcBuild.rsc`' and press Enter. When prompted to continue, press Enter.

Once the import is completed, the concentrator device will reboot. Make the proper ethernet connections to the upstream switch(es) and you are done with the central concentrator device. These are the port assignments in the default configuration supplied. Sample upstream switch configurations for Cisco Catalyst and Juniper switches is provided in Appendix B. Regardless of switch vendor you should, if supported, employ a multi-chassis (virtual switch stack) LACP port group (port-channel in Cisco parlance).

Port	Function
sfp1	Unused
ether1	Unused
ether2	LACP member
ether3	LACP member
ether4	Unused
ether5	Local last-ditch management.

Central Concentrator Port Assignments

Remote

Use file manager to drag the *MasterRemoteBuild-Vx.x.rsc* script file, the *build-defs.rsc* build configuration script file, and the (*.pem*) CA certificate file to the 'Files' window in the Winbox GUI. This copies the file to the device. ***Make SURE you use the build configuration script file that was used to build the concentrator with NO CHANGES!!!***

Using the Winbox GUI click on 'New Terminal'. A terminal screen will open on the GUI. Hit the enter key several times to make sure you have a working prompt. On that terminal screen enter the command '`import MasterRemoteBuild.rsc`' and press Enter. You will be asked for the remote number that you wish to create. Each remote must have a unique node number between 1 and 239. Press Enter once again to proceed. The remote will reboot when the import is completed.

Note that you must run the **AddRemote** script on the concentrator to register the remote to its internal database. This adds the tunnel endpoints and the iBGP peers to the concentrator configuration. You must also run the **AttachVlanToRemote** script to map any desired Layer-2 VLANs to this remote.

Port	Function
ether1	WAN Link (DHCP Client)
ether2	Access or Trunk mode port
ether3	Access or Trunk mode port
ether4	Access or Trunk mode port
ether5	Local Management Port

Default Remote Node Port Assignments

Management

GUI (WinBox)

The Mikrotik WinBox program can be utilized for device management. Whilst I am not generally a fan of GUI based management, I find this one to be quite good and extremely usable. It offers the option of creating a local terminal session which is needed to run the interactive LabRmt scripts and can connect using Layer-2 MAC addressing as well as Layer-3 IP addressing. ***DO NOT ATTEMPT TO CHANGE ANYTHING IN THE CONFIGURATION MANUALLY AS EVERYTHING IS DEEPLY INTERRELATED.***

SSH

Connections may be made using SSH clients to create a terminal session. The firewall system will detect repeated SSH breach attempts and automatically block the source IP address for 3 days.

Node Numbering

- The concentrator is considered to be node number 254 (0xfe).
- The remotes start at node number 1 and are numbered in ascending order (1-239). *<The actual number of remote units supported concurrently depends upon the processing capability and hardware composition of the concentrator and the traffic levels to/from the remotes.>*
- Node numbers 0 and 240-254 are reserved for system use.

- The node number is encoded into many of the IP Addresses and MAC addresses used by the overall system.

Addresses Used (Distribution Default Values)

Each environment must utilize a different set of IP addresses. The addresses used in the following section are the **distribution's default values** and may be overridden in the Environment configuration file.

Parameter	Default Value	Description
EnvLanNet	172.25	Environment IP Allocation. (/16) Note: First two octets with no trailing period. The first /24 block (third octet 0) is used for Loopback1 addresses and the last 16 /24 blocks (third octet 240-254) are used internally The remaining /24 blocks are SiteLans. The third octet is the decimal remote number)
CncMgmtPort	ether5	Concentrator port to use as local management port. This port will act as a DHCP server. It is used strictly as a last-ditch device access mechanism. It should not be used for any other reason.
RmtMgmtPort	ether5	Remote Site port to use as local management port. This port will act as a DHCP server. It is used strictly as a last-ditch device access mechanism. It should not be used for any other reason.
RmtMgmtNet	192.168.255	A /24 used for local management port. Not advertised, same on each remote.

Allocation of MAC addresses

Each environment must utilize a unique set of logical MAC addresses which do not conflict with any other MAC addresses present on the customer networks. IEEE 802c standards for their Structured Local Address Plan (SLAP) has reserved the x2:xx:xx:xx:xx:xx MAC address space as reserved for Random / Arbitrary Local Administrative Assignments (MAC analog to IPv4 RFC1918 address space). Use of the A2:xx:xx:xx:xx:xx sequence will prevent overlap with any vendor assignments.

EoIP interfaces, Loopback interfaces, and Bridge interfaces must have non-conflicting MAC addresses assigned. The following MAC address blocks are the **distribution's default values**.

Parameter	Default Value	Description
MacPfxBr	A2:BB:00	Bridge Mac Address Prefix • A2:BB:00:{nn}:{va}:{vb} • {nn} = 2 digit hexadecimal form of this remote number • {va}:{vb} = 4 digit hexadecimal form of vlan number with colon in middle

MacPfxLoop	A2:BB:01:FE	Loopback Interface Mac Address Prefix A loopback is essentially a bridge with no member interfaces. • A2:BB:01:FE:{nn}:{ll} • {nn} = 2 digit hexadecimal of this router remote number • {ll} = 2 digit hexadecimal of loopback number
MacPfxEoip	A2:BB:01:FF	EoIP Tunnel Interface Mac Address Prefix • A2:BB:01:FF:{oo}:{dd} • {oo} = 2 digit hexadecimal of this router remote number • {dd} = 2 digit hexadecimal of termination remote number

Management Scripts

Scripts on Central Concentrator

- **AddVlan** – Defines a new Vlan that is delivered on the trunk port and available for delivery to remotes.
- **RemoveVlan** – Remove an unused Vlan from the concentrator.
- **ShowVlan** – Show Vlans and associated remotes from the concentrator neighborhood.

- **AddRemote** – Add a remote unit to the concentrator neighborhood.
- **RemoveRemote** – Remove a remote unit from the concentrator neighborhood.

- **AttachVlanToRemote** – Deliver an already defined Vlan to a remote unit in the concentrator neighborhood.
- **DetachVlanFromRemote** – Cease delivery of a Vlan to a remote unit in the concentrator neighborhood.
- **ListVlansOnRemote** – List Vlans attached to a specific remote unit in the concentrator neighborhood.

- **ZZ-MasterDefinitions** – **Do not use or edit this script.** It is called internally by all other scripts to set up background information specific to this LabRmt Environment. It is created dynamically by the system at build time.

Scripts on Remote Units

- **EnableSSTP** – Enable the SSTP tunnel functionality. (Use for highly restricted environments such as hotels and conference centers where L2TP / IPSEC tunnels are not allowed.)
- **DisableSSTP** – Disable the SSTP tunnel functionality.

- **AddVlan** – Defines a new Vlan that is delivered via the concentrator node. (Note, this does NOT provide access to the Vlan on any port(s). Access must be defined using other scripts or it will not be present on any port.) Also, the **AttachVlanToRemote** script must be executed on the concentrator to deliver it.
- **RemoveVlan** – Remove an unused Vlan.
- **ShowVlan** – Show the defined Vlans and port memberships.

- **EnableWifi** – Enable Wifi. Set up WAN and Local Lan SSIDs.
- **RemoveWifiAll** – Remove all Wifi configuration.

- **AddWifiSSID** – Add an SSID connected to a specific Vlan to the Wifi System.
- **RemoveWifiSSID** – Remove a specific Vlan / SSID from the Wifi system.

- **SetModeToAccess** – Change a port from Trunk mode to Access mode.
- **SetAccessPortVlan** – Set an access mode port to carry a specific Vlan.

- **SetModeToTrunk** – Change a port from Access mode to Trunk mode.
- **AddVlanToTrunkPort** – Add a tagged Vlan to a trunk mode port.
- **RemoveVlanFromTrunkPort** – Remove a tagged Vlan from a trunk mode port.

- **ZZ-MasterDefinitions** – **Do not use or edit this script.** It is called internally by all other scripts to set up background information specific to this implementation. It is created dynamically by the system at build time.

Example Setup - Concentrator

All Vlans must be added to the concentrator, delivered over the LACP bonded trunk, and then attached to each remote unit that needs bridged access to that Vlan.

This example will register remote unit 5 to the concentrator, then add vlan 399 to the concentrator, then attach vlan 399 to remote unit 5.

1. On concentrator: Add remote unit 5.

```
[admin@LabRmt-Beta] /system script> run AddRemote
===> Adding Remote Unit to concentrator.
Enter Remote Unit number:
value: 5
---> Adding ppp secrets
---> Adding eoip tunnel
---> Adding L2TP Server bindings
---> Adding SSTP Server bindings
---> Adding BGP Peers
----> Adding BGP Peer Wan1-L2TP
----> Adding BGP Peer Wan2-L2TP
----> Adding BGP Peer Wan1-SSTP
----> Adding BGP Peer Wan2-SSTP
Concentrator action completed
```

2. On concentrator: add Vlan 399 using script **AddVlan**.

```
[admin@LabRmt-Beta] /system script> run AddVlan
===> Adding Vlan to concentrator.
Enter vlan number:
value: 399
Concentrator creating Uplink vlan Uplink.399
Concentrator creating Vlan399 bridge MAC Address = A2:BB:00:FE:01:8F
Concentrator action completed
```

3. On concentrator: Attach Vlan 399 to remote unit 5 using script **AttachVlanToRemote**. Note that the remote unit must also be configured to know about and accept Vlan 399.

```
[admin@LabRmt-Beta] /system script> run AttachVlanToRemote
===> Associate Vlan with Remote Node.
Enter Remote Node number:
value: 5
===> Vlan to connect with remote node 5..
Enter vlan number:
value: 399
   > creating eoip vlan eoip5
   > adding eoip5 to vlan399 bridge
Concentrator action completed
```

4. On concentrator: Show Vlans

```
[admin@LabRmt-Beta] /system script> run ShowVlan
===> List Remotes Attached to Vlan.

    VLAN
    -----------
    Vlan3
    Vlan301
    Vlan307
    Vlan399
        Remote 5
```

5. On concentrator: List Vlans attached to a particular remote

```
[admin@LabRmt-Beta] /system script> run ListVlansOnRemotes
===> Show Vlans Attached to Remote Node.
Enter Remote Node number:
value: 5
    Vlan399

Concentrator remote 5 action completed
```

Example Setup – Remote

The Vlan must have been added to the concentrator and attached to this remote before these operations are attempted. If not, you will spend hours or days troubleshooting an issue that is not an issue!!!

All Vlans must be added to the remote site network device and then attached to an access mode port or a trunk mode port.

1. On remote 5: Add Vlan to the remote using script **AddVlan**.

```
[admin@LabRmt-Beta-remote-5] /system script> run AddVlan
Enter vlan number:
value: 399
Remote 5 creating eoip vlan eoip5.399
Remote 5 creating Vlan399 bridge MAC Address = A2:BB:00:05:01:8F
Remote 5 action completed
```

2. On remote 5: Set remote to deliver Vlan 399 as untagged traffic on access mode port ether3.

```
[admin@LabRmt-Beta-remote-5] /system script> run SetAccessPortVlan
Set a port's access/native vlan.
Enter ethernet port number (2, 3, or 4)
value: 3
Enter vlan number (enter 'L' for the SiteLan network):
value: 399
Remote 5 - Switching ether3 to untagged Vlan399
Remote 5 action complete
```

3. On remote 5: Set remote port ether4 as a vlan trunk port.

```
[admin@LabRmt-Beta-remote-5] /system script> run SetModeToTrunk
Convert port from Access mode to Trunk mode.
Enter ethernet port number (2, 3, or 4)
value: 4
Remote 5 port ether4 will be converted into a trunk port.
Remember to attach tagged vlans to it.

Remote 5 action completed
```

4. On remote 5: Set remote to deliver Vlan 399 as tagged traffic on trunk mode port ether4.

```
[admin@LabRmt-Beta-remote-5] /system script> run AddVlanToTrunkPort
Add tagged vlan to trunk port.
Enter ethernet trunk number (2, 3, or 4)
value: 4
Enter vlan number:
value: 399
Remote  trunk port ether4 adding tagged vlan number 399
Remote  action complete.
```

5. On remote 5: Show final Vlan/port assignments. (Trunk ports show as a port name dot vlan – ether4.3)

```
[admin@LabRmt-Beta-remote-5] /system script> run ShowVlan
Remote 5 bridge ports listing

  Vlan399
  - ether3
  - ether4.399

Remote 5 action completed.
```

Appendix A - OpenSSL Self-Signed Certificate Generation

Creating a Dummy Certificate Chain using OpenSSL

This shows the creation of two certificates, a dummy self-signed CA certificate with a password of 'abc123' and a PKCS12 (PFX) certificate with the same 'abc123' password. Save ALL the files used in this example as they may be needed in the future. Safeguard the .key files.

The certificates will be generated with a validity period of 9999 days (over 27 years). This is not a good idea for a production environment, but great for a lab/test environment where you don't want sudden unexpected certificate failure in the middle of testing. Adjust to your preferences/policy requirements.

User typed input is highlighted in yellow.

Create CA Certificate

Create a CA CSR for the CA Certificate

```
PS> openssl req -new -newkey rsa:2048 -nodes -out ca.csr -keyout ca.key
====pictogram===
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:South Carolina
Locality Name (eg, city) []:SomeCity
Organization Name (eg, company) [Internet Widgits Pty Ltd]:RingCentral, Inc
Organizational Unit Name (eg, section) []:Custom Engineering
Common Name (e.g. server FQDN or YOUR name) []:Tim.McKee
Email Address []:tim.mckee@ringcentral.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:abc123
An optional company name []:
```

Use the Resultant CA CSR to Create the CA Certificate

```
PS> openssl x509 -trustout -signkey ca.key -days 9999 -req -in ca.csr -out ca.pem
Certificate request self-signature ok
subject=C = US, ST = South Carolina, L = Some City, O = "RingCentral, Inc", OU = Custom
Engineering, CN = Tim.McKee, emailAddress = tim.mckee@ringcentral.com
```

Use CA to Create Certificate for Concentrator (client)

Create a CSR to for the Concentrator Certificate

```
PS> openssl req -new -newkey rsa:2048 -out client.csr -keyout client.key
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
```

```
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:South Carolina
Locality Name (eg, city) []:Some City
Organization Name (eg, company) [Internet Widgits Pty Ltd]:RingCentral, Inc
Organizational Unit Name (eg, section) []:Custom Engineering
Common Name (e.g. server FQDN or YOUR name) []:concentrator
Email Address []:tim.mckee@ringcentral.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:abc123
An optional company name []:
```

Use the Resultant CSR to Create the Concentrator Certificate

```
PS> openssl x509 -req -days 9999 -in client.csr -CA ca.pem -CAkey ca.key -out client.cer
Certificate request self-signature ok
subject=C = US, ST = South Carolina, L = Some City, O = "RingCentral, Inc", OU = Custom
Engineering, CN = concentrator, emailAddress = tim.mckee@ringcentral.com
```

Create a combined signed PKCS12 Certificate

```
PS> openssl pkcs12 -export -in client.cer -certfile ca.pem -inkey client.key -out client.pfx
Enter Export Password:abc123
Verifying - Enter Export Password:abc123
```

Resultant Files

The files ca.pem and client.pfx must be used on the LabRmt hardware, they are referenced in the build configuration file.

Appendix B - LACP Bonded Port Group Setup

The configuration assumes that if you are using a 'stacked switch' it has already been configured. The first digit of the interface number is the virtual chassis number.

It is highly recommended that you split the ports used in an LACP group between chassis members. Failure of one chassis will not render the LabRmt system inoperative when this is configured.

Cisco

LACP bonded port groups are referred to as Port-channels in the Cisco world and may be either single chassis or multi-chassis in scope. This example is from a 2 chassis Catalyst 3750X switch stack. It passes vlans 3, 301, 307, and 350-354 to the concentrator.

```
interface GigabitEthernet1/0/2
 description CELAB-LabRmt-beta-ether2
 priority-queue out
 mls qos trust dscp
 storm-control broadcast level bps 2m 1.5m
 channel-group 1 mode active
exit
!
interface GigabitEthernet2/0/2
 description CELAB-LabRmt-beta-ether3
 priority-queue out
 mls qos trust dscp
 storm-control broadcast level bps 2m 1.5m
 channel-group 1 mode active
exit
!
interface Port-channel1
 description CELAB-LabRmt-beta
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 3,301,307,350-354
 storm-control broadcast level bps 2m 1.5m
exit
!
! Add vlan 399 to the Port Channel
interface Port-channel1
 switchport trunk allowed vlan add 399
exit
```

Juniper

LACP bonded port groups are referred to as aggregated ethernet interfaces in the Juniper world may be either single chassis or multi-chassis in scope. This example is from a 2 chassis Juniper ES switch stack. It passes vlans 3, 301, 307, and 350-354 to the concentrator.

```
set chassis aggregated-devices ethernet device-count 1

set interfaces ge-0/0/2 ether-options 802.3ad ae0
delete interfaces ge-0/0/2.0

set interfaces ge-1/0/2 ether-options 802.3ad ae0
delete interfaces ge-1/0/2.0

set interfaces ae0 aggregated-ether-options lacp active
```

```
edit interfaces ae0 unit 0 family ethernet-switching
set port-mode trunk
set vlan members [ Vlan3, Vlan301, Vlan307, Vlan350, Vlan351, Vlan352, Vlan353, Vlan354 ]

top
commit
```

Appendix C - LabRmt Environment Configuration File

Yellow highlighted elements should be changed to match your environment as needed.

File: build-defs.rsc

```
##############################################
# Beta Development system definitions go here #
##############################################
#########################################################################
# Identify the build configuration environment name and allow the user
# to abort by using Control-C if this is in error.
#
# ** BETA ** environment
#
:put "Utilizing BETA environment definitions.";
:global getInput;
:local temp [$getInput "Press return to continue or ^C to abort."];
#
# Device name should reflect the Environment name
:global systemId "RingLab-Beta";
#
# BGP Autonomous System Number (private RFC1930/RFC6996 number)
#   Rarely needs to be changed as iBGP is internal to this environment only.
:global bgpAsNo 65530;
#
# LAN network (/16) to use in the environment to local layer-3 traffic
:global EnvLanNet "172.23";
#
# Identify LACP interface members as a comma separated list
#   These interfaces are used on the hub concentratgor to form a bonded LACP
#   interface to the upstream network switch(es).
#   You may specify any number of interfaces.
:global BondingInterfaces "ether2,ether3";
#
# Set LACP interface name to this value.  Used internally to create
#   Vlan interface names.
:global TrunkName "Uplink";
#
##################
# ** Wan1 ** Data (Must be a static address)
# Wan1 is the preferred interface for traffic
#
# IP Address with trailing /netmask
:global Wan1IpAddr "12.31.117.19/27";
#
# IP Address of gateway
:global Wan1IpGw "12.31.117.1";
#
# Vlan ID number on which Wan1 is delivered across Trunk
:global Wan1VlanId "307";
#
# Carrier Identification for comments
:global Wan1Provider "ISP#1";
#
##################
# ** Wan2 ** Data (Must be a static address)
#
# IP Address with trailing /netmask
:global Wan2IpAddr "173.95.76.210/27";
#
```

```
# IP Address of gateway
:global Wan2IpGw "173.95.76.193";
#
# Vlan ID number on which Wan2 is delivered across Trunk
:global Wan2VlanId "301";
#
# Carrier Identification for comments
:global Wan2Provider "ISP#2";
#
###################
# ** Link to main network **
# Note: route to $EnvLanNet through this link must be added to upstream router
# Reminder instructions are generated at the end of concentrator build.
#
# Vlan ID number on which Upstream Network is connected across Trunk
:global UpstreamNtwkVlanId "3";
#
# IP Address with trailing /netmask
:global UpstreamNtwkIpAddr "192.168.0.10/24";
#
# IP Address of gateway
:global UpstreamNtwkGw "192.168.0.1";
#
# Upstream DNS servers as a comma separated list
:global UpstreamNtwkDns "172.16.240.6,172.16.240.7,172.16.240.8";
#
# Networks to route via upstream link as comma separated list
#   of "network/netmask:gateway" elements
:global UpstreamNtwkRoutes "192.168.0.0/16:192.168.0.1,172.16.0.0/12:192.168.0.3";
#
###################
# Encryption Algorithm to use for IPSEC traffic.
# Make sure the concentrator hardware supports these algorithms
# CBC is good, GCM is better if and only if supported in hardware.
#
:global IpsecAlgAuth "sha256";
:global IpsecAlgEnc "aes-256-cbc";
:global IpsecPfsGroup "ecp521";
#
# Preshared key to use for IPSEC
:global L2tpSecret "Ui@dy7f38d$je83";
#
# L2TP preshared keys for tunnels
:global L2tpWan1Secret "Kdkldjf79ekv897";
:global L2tpWan2Secret "Mklfjglifgu87fg";
:global SstpWan1Secret "Vjkd7f6fd78gekl";
:global SstpWan2Secret "Okdlyuitfbk737f";#
###################
# MAC address prefixes for Bridges, EoIP tunnels, and Loopbacks
:global MacPfxBr "A2:BB:00";
:global MacPfxEoip "A2:BB:01:FF";
:global MacPfxLoop "A2:BB:01:FE";
#
###################
# Optional SNMP information, leave blank if not desired
:global SnmpContact "user@domain.name";
:global SnmpLocation "Location Information";
:global SnmpCmtyRw "qwerty911";
:global SnmpCmtyRwAllow "172.16.255.0/24,172.16.242.12";
:global SnmpCmtyRo "abcdef811";
:global SnmpCmtyRoAllow "172.16.242.0/24,172.16.243.24/31";
```

```
:global SnmpTrapTarget "172.16.255.110,172.16.255.112";
#
##################
# Certificates
#
# ConcCert must be signed PKCS12 (PFX) certificate.  password will be prompted
:global ConcCertFname "client.pfx";
:global ConcCertCname "Conc_Certificate";
:global ConcCertPwd "abc123";
#
# RemoteCaCert is optional.  password will be prompted
:global RemoteCaCertFname "ca.pem";
:global RemoteCaCertCname "Conc_CA_Certificate";
:global RemoteCaCertPwd "abc123";
#
##################
# REMOTE UNIT port definitions
#
# Wan/ISP port
:global RmtWanPort "ether1";
#
# Default Route Type
#   viaHubOnly - Out tunnels ONLY
#   viaHubPreferred - Out tunnels, fail to local
#   viaLocalOnly - Out local Wan Link
#
:global DefRouteType "viaHubPreferred";
#
# Define array of potential LAN/Access/Trunk Ports on Remote Units
# All will be initially set to access the local LAN.
# Must be semicolon separated list in braces
:global SiteLanPorts {"ether2";"ether3";"ether4"};
#
# DNS Server list
:global RmtDnsServers "172.16.240.6,172.16.240.7,172.16.240.8";
#
# Local Management port (Concentrator)
:global CncMgmtPort "ether5";
#
# Local Management port (Remotes)
:global RmtMgmtPort "ether5";
#
# Define Local Management Subnet
:global RmtMgmtNet "192.168.255";
#
# Define wireless security profile name, password, and ssid names
:global wifiSecProfile "LabRmtSecProfile";
:global wifiPassword "LabRmtSitePwd";
:global wifiSsidLocal "LabRmt-Beta-SiteLan";
:global wifiSsidWan "LabRmt-Beta-Home";
#
```