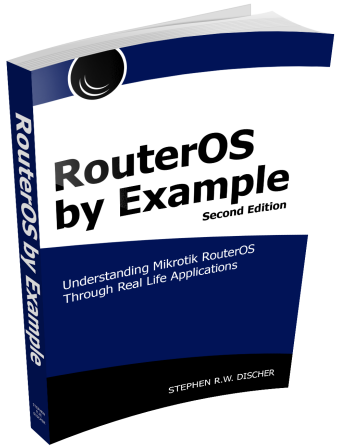
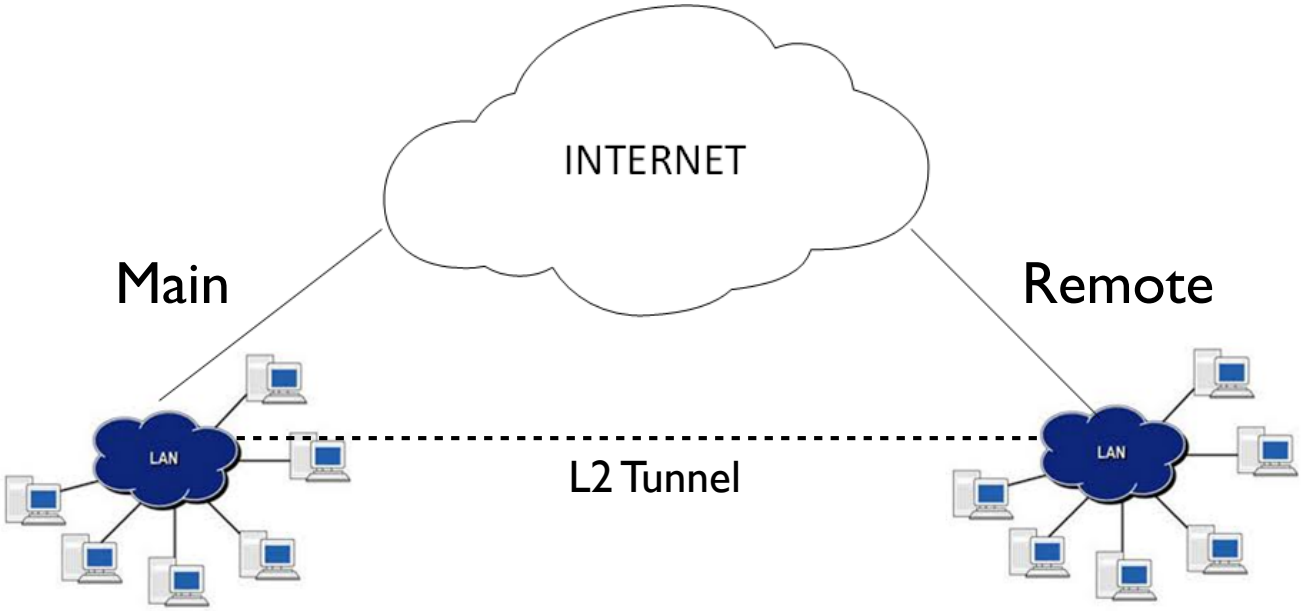
Using BCP to Create Layer 2 Networks Over the Internet

About Me

- Steve Discher, from College Station, Texas, USA
- MikroTik Certified Trainer since 2008 and teach RouterOS classes, LearnMikroTik.com and blog at SteveDischer.com
- Operate a wireless distribution company, ISP Supplies
- Author of RouterOS by Example, 1st and 2nd Editions



The Problem



L2 because we want DHCP, Romon and other Layer 2 services like VOIP Discovery over the WAN

Site to Site VPN Differences L2 vs L3

Site-to-site Layer 2 VPN	Site-to-site Layer 3 VPN
All sites share same LAN IP subnet	Each site has different LAN IP subnet
Broadcast domain is end-to-end everywhere	Broadcast is not possible between sites
Centralized DHCP Server	Independent DHCP Server in each site
Centralized Internet Gateway	Possible individual Internet Gateway in each site
Based on bridging No routing required	Static Route or Dynamic Routing Protocol required

- Site = Location = Office

Or More Important: a Specific Application that requires L2 functionality

* Reference: Lay Minh (Makito) April 24th, 2017 MikroTik User Meeting, Phnom Penh, Cambodia

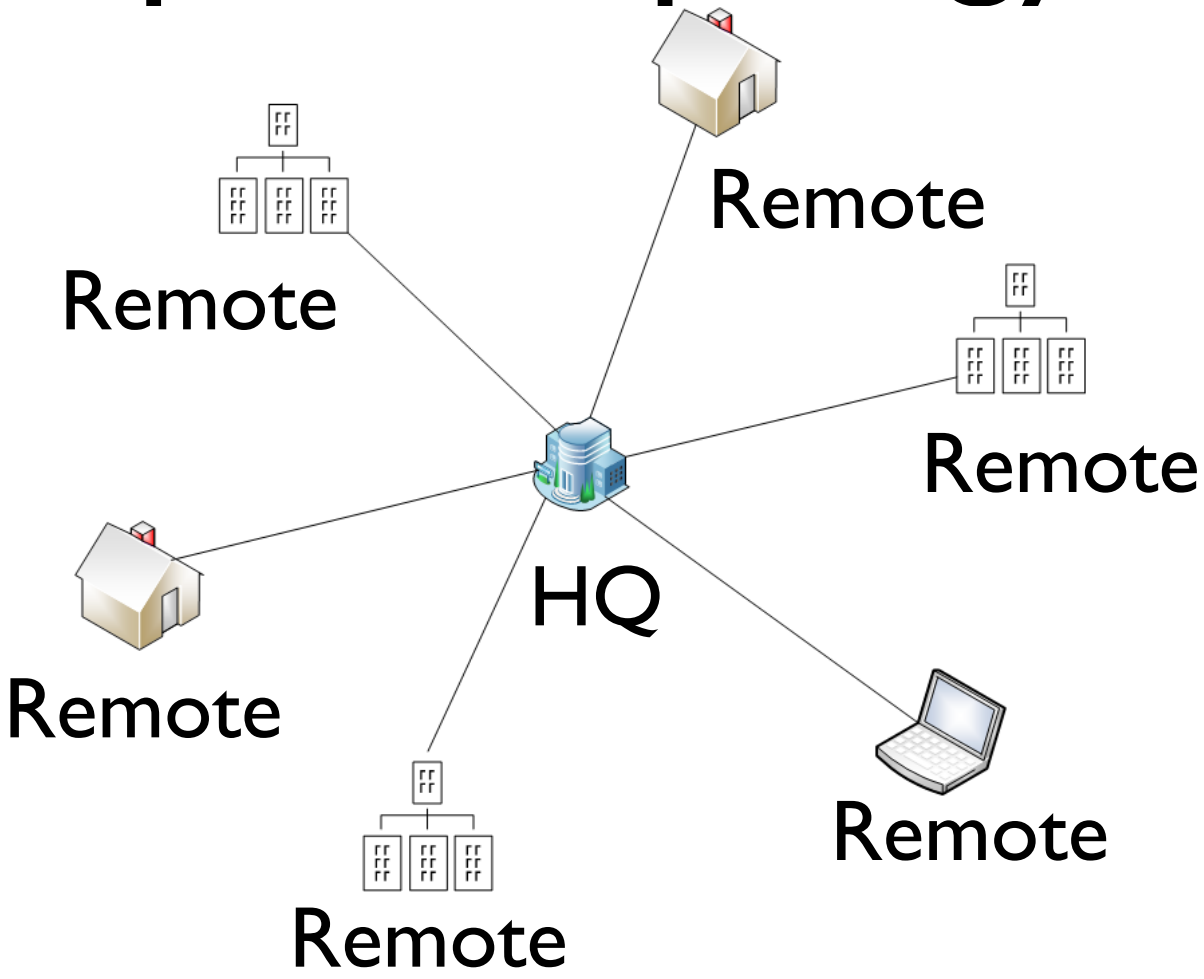
L2 Tunnel Options

"Goto" Option in RouterOS:

EOIP

- IPSec encryption but no authentication mechanism
- Typically requires both ends to be directly connected to the internet or you build the tunnel over another tunnel protocol like L2TP, PPTP, etc.
- Additional packet overhead, additional configuration steps
- Easy to configure, harder to maintain. Must create one static tunnel per client.

Example: Typical Hub and Spoke Topology



Components Required

To complete the hub and spoke configuration we will need these technologies:

- A tunnel protocol
- Bridging
- BCP
- Multilink PPP

Concepts Used

Bridging

- Bridging is simply the ability to join together two dissimilar interfaces into one logical interface
- Bridges behave much like switches, and after 6.41 they offload to onboard switches
- Bridging over a Layer 3 network is useful for extending Layer 2 services from Point A to Point B when you do not control the network in between. (The Internet)

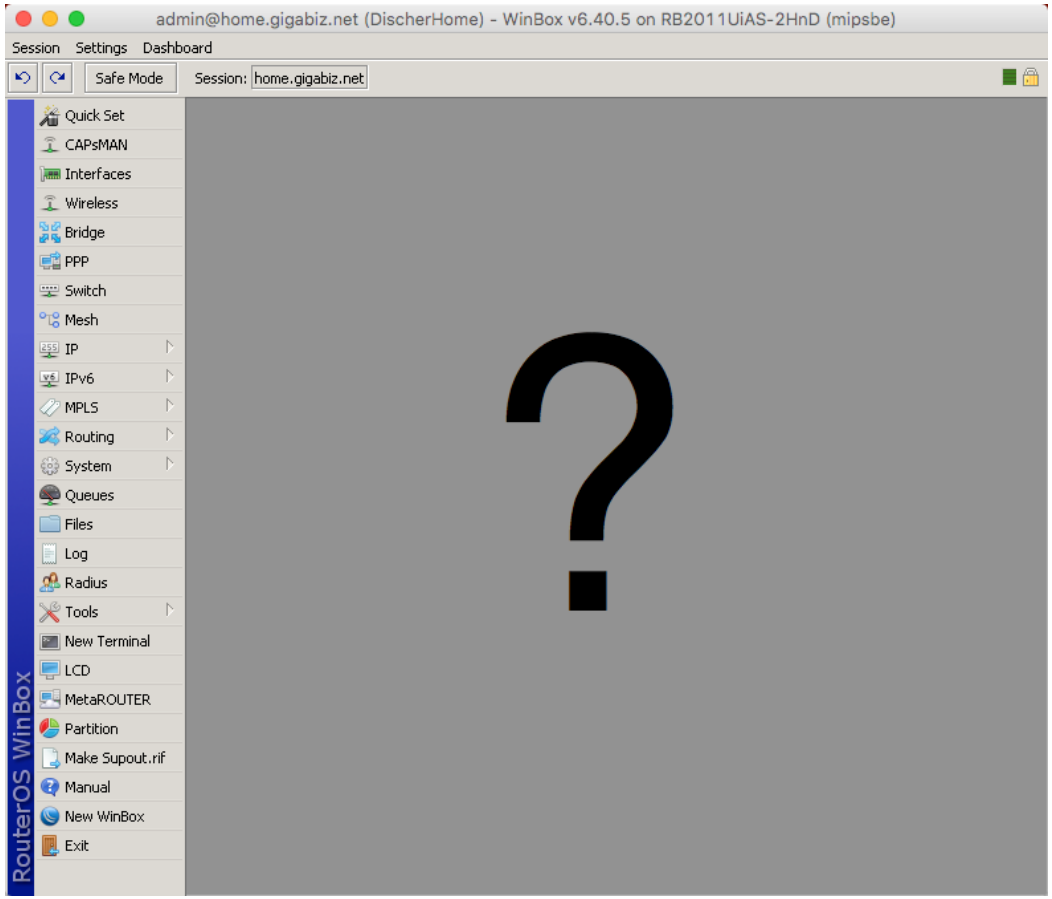
BCP

- Point to Point Protocol (PPP) + BCP
- Hub and spoke network is easily built
- Only a single directly connected border router is required (or dst-nat)

BCP

- Clients can be static or dynamic IP's
- Tunnels can be created by remote devices on the fly
- Single step configuration, not tunnel over a tunnel
- Provides authentication and encryption in a single step

I Don't see BCP!



automagical

RouterOS does the heavy lifting in the background through PPP profile

Multilink PPP

- RFC 1990, published by the Internet Engineering Task Force (IETF) Network Working Group
- Originally intended for systems using the Integrated Services Digital Network (ISDN)

Multilink PPP

- Multi-Link Point to Point Protocol (MP, Multi-Link PPP, MultiPPP or MLPPP) is a method of splitting, recombining, and sequencing data across multiple logical data links or over a single PPP link.

  Source: https://wiki.mikrotik.com/wiki/Manual:MLPPP_over_single_and_multiple_links

Multilink PPP

Why do we need MLPPP?

- L2 tunnels over L3 networks require transmitting Ethernet through VPN tunnels
- Tunnel MTU's + tunnel overhead can't pass the whole frame so we have to have a way to get the whole data through the tunnel in pieces and reassemble

Multilink PPP

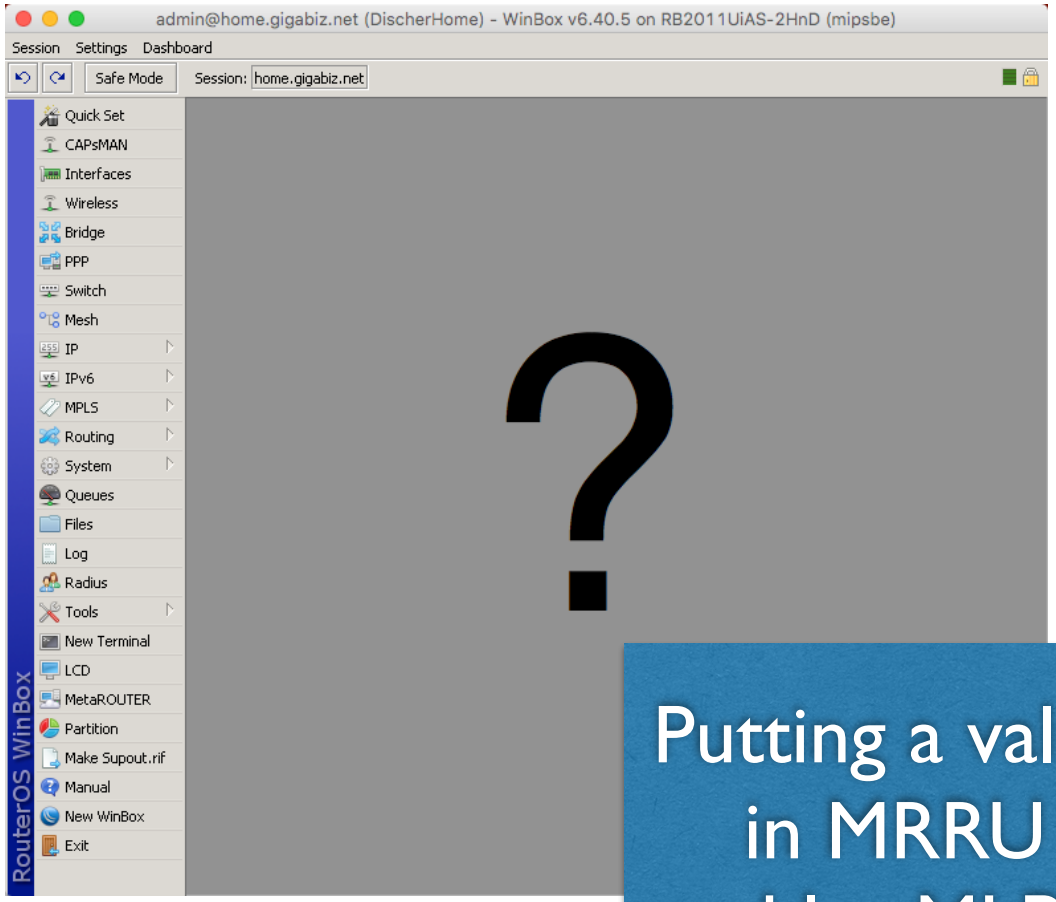
Why do we need MLPPP?

- Fragmenting and then reassembling packets can break some applications, example VOIP via UDP and DHCP to name a few.

Multilink PPP

In our case, we can configure RouterOS to split the tunnels into multiple logical tunnels over a single PPP link and then combine them back together on the other end. This allows us to transmit the full Ethernet frame.

I Don't see MLPPP!



automagical

Putting a value in MRRU enables MLPPP

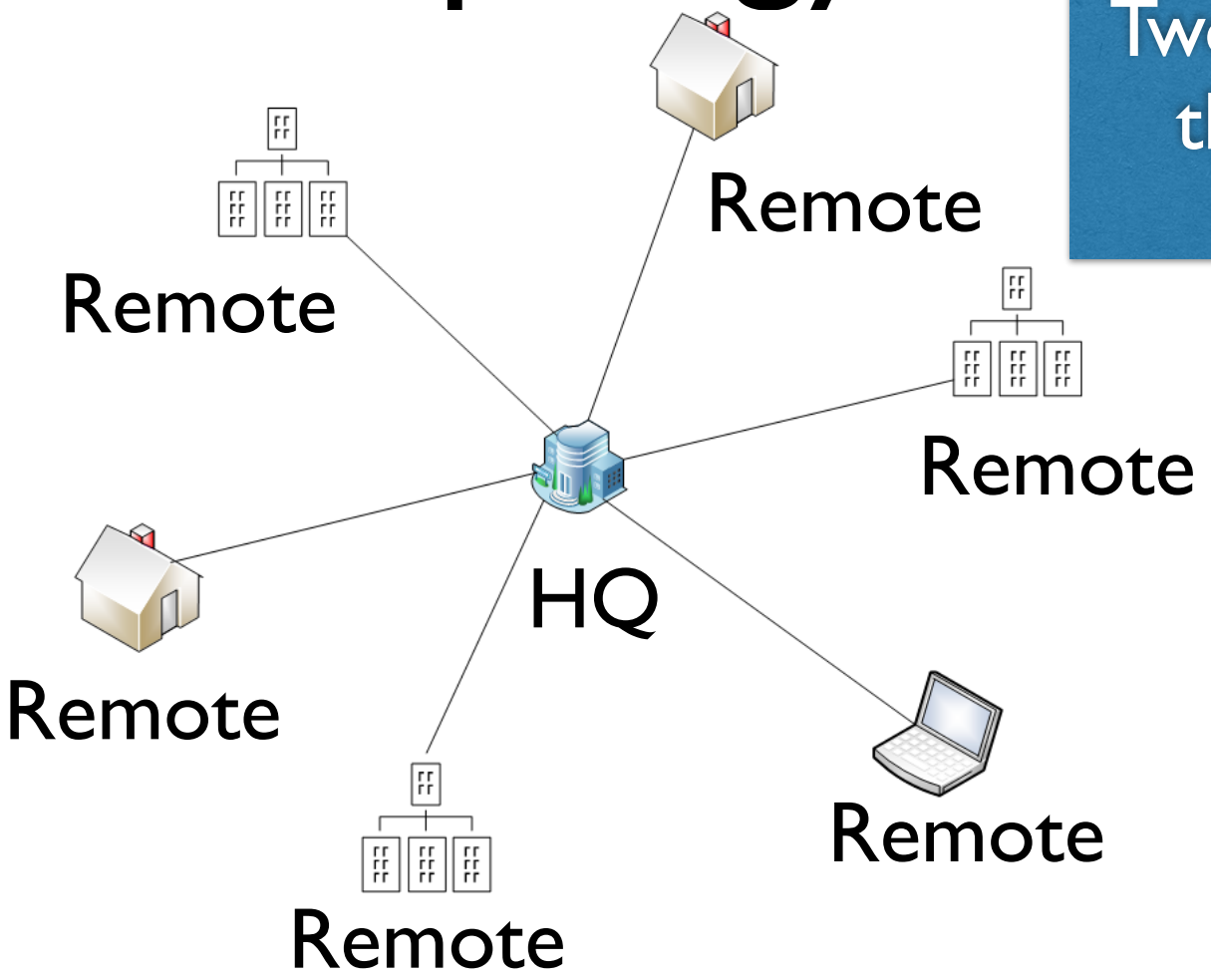
RouterOS does the heavy lifting in the background through the L2TP server MRRU setting

MRRU

The maximum received reconstructed unit (MRRU) is similar to a maximum transmission unit (MTU), but applies only to multilink bundles; it is the maximum packet size that the multilink interface can process. Default is 1600 which is optimal.

Typical Hub and Spoke Topology

Two pieces to the config



HQ Configuration

5 steps to complete

1. Create the Bridge Interface
2. Add the LAN interfaces to the Bridge
3. Create a PPP Profile by assigning the Bridge in the profile
4. Create the PPP Secrets using the PPP Profile you created in Step 3
5. Enable the L2TP VPN Server with Multi-Link PPP

Remote Configuration

4 steps to complete

1. Create the Bridge Interface
2. Add the LAN interfaces to the Bridge
3. Create a PPP Profile by assigning the Bridge in a profile
4. Create the L2TP client interface with Multi-Link PPP

WHY?

Case Study

ISP Supplies deploying a Grandstream UCM6208 PBX and Grandstream phones.

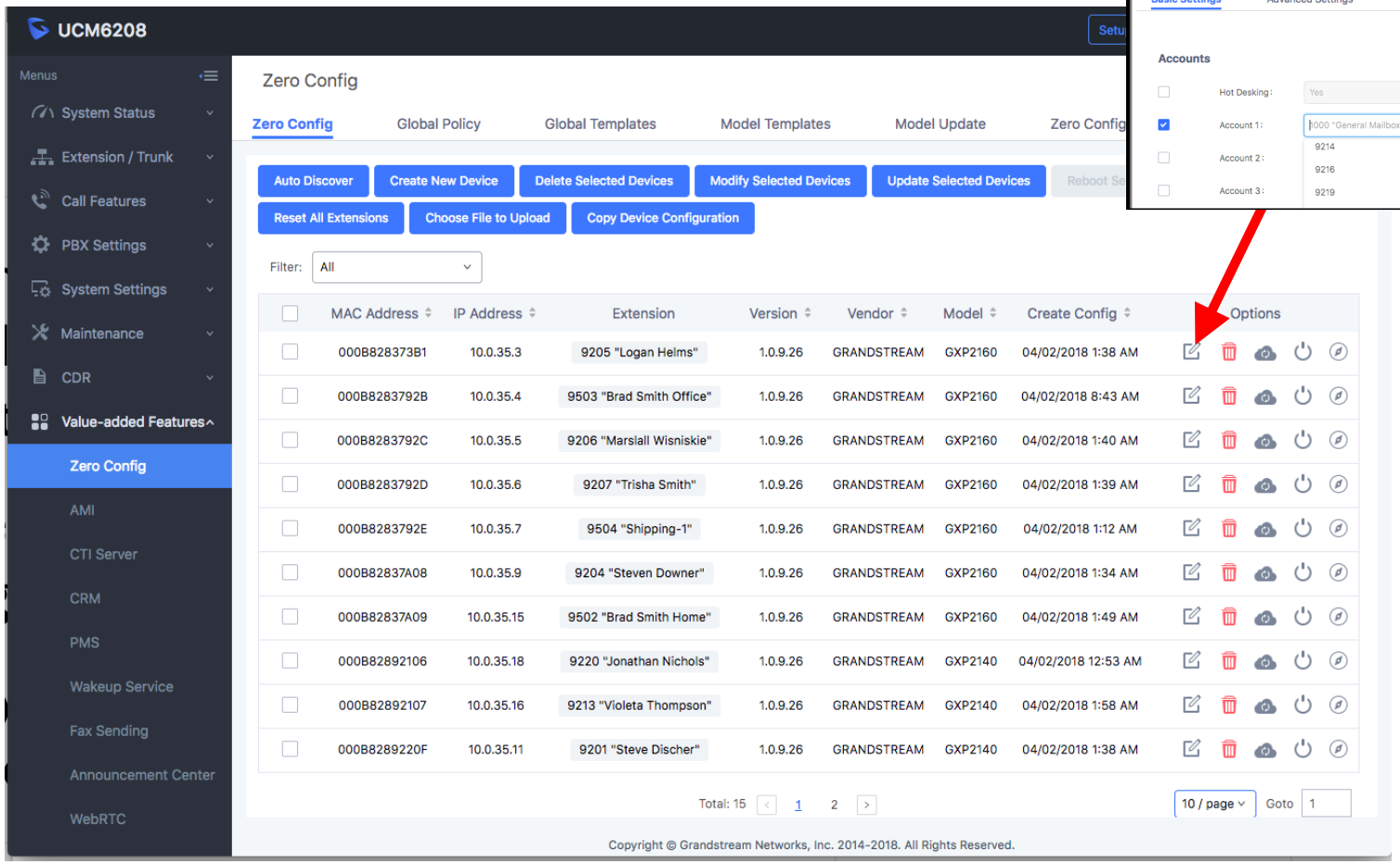
Requirements:

- PBX located behind MikroTik Router/Firewall
- Some phones on same LAN as the Router
- Some phones in remote locations
- Ability to use the "Zero Configuration" option, thereby necessitating L2 functionality

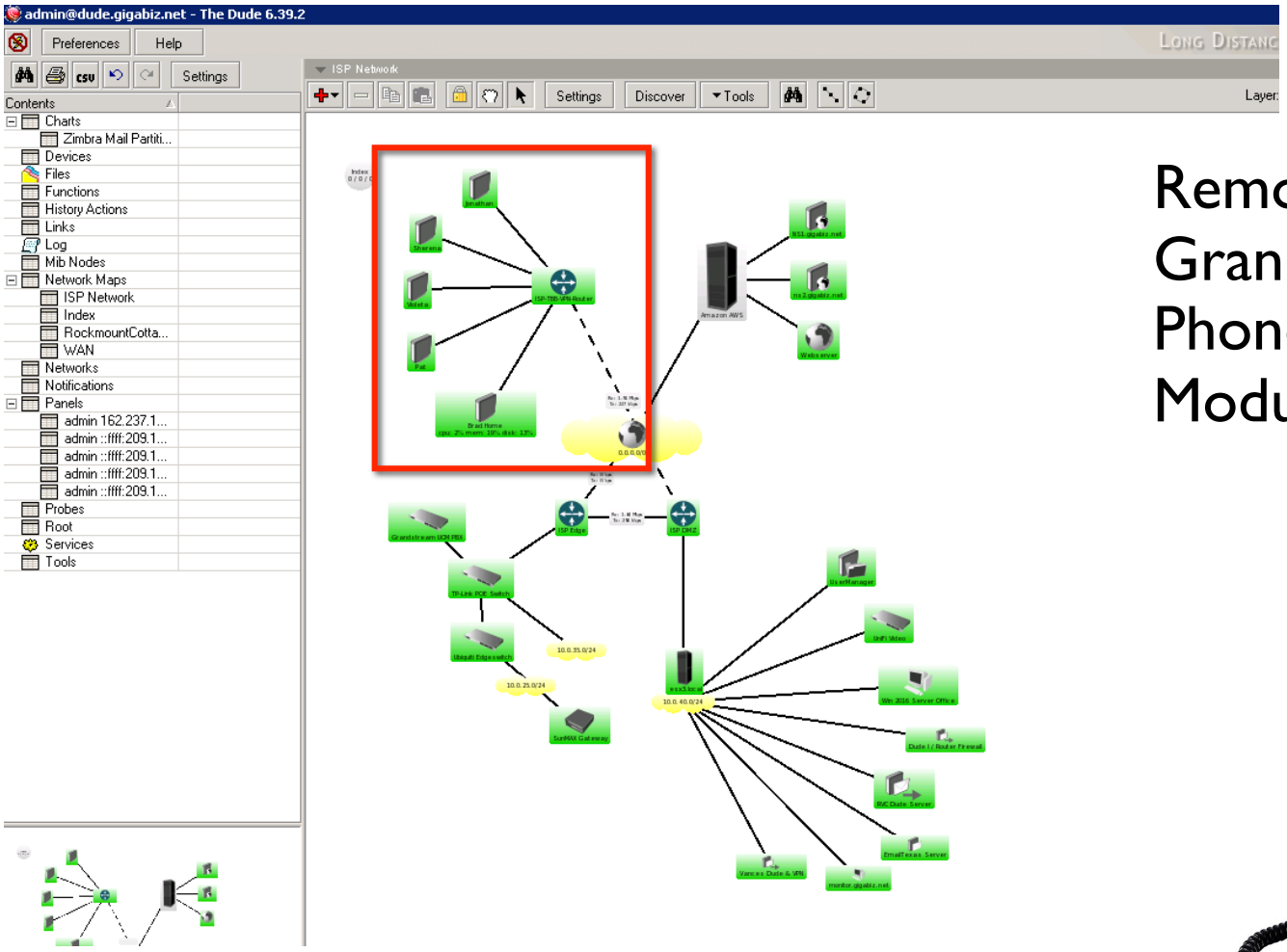
Take Advantage of Grandstream Zero Config

- Automatic provisioning of new phones added to the network by simply assigning an extension
- Pushes model specific or global templated configs to phone
- Ability to push config updates or firmware updates to the phone

Grandstream Zero Config

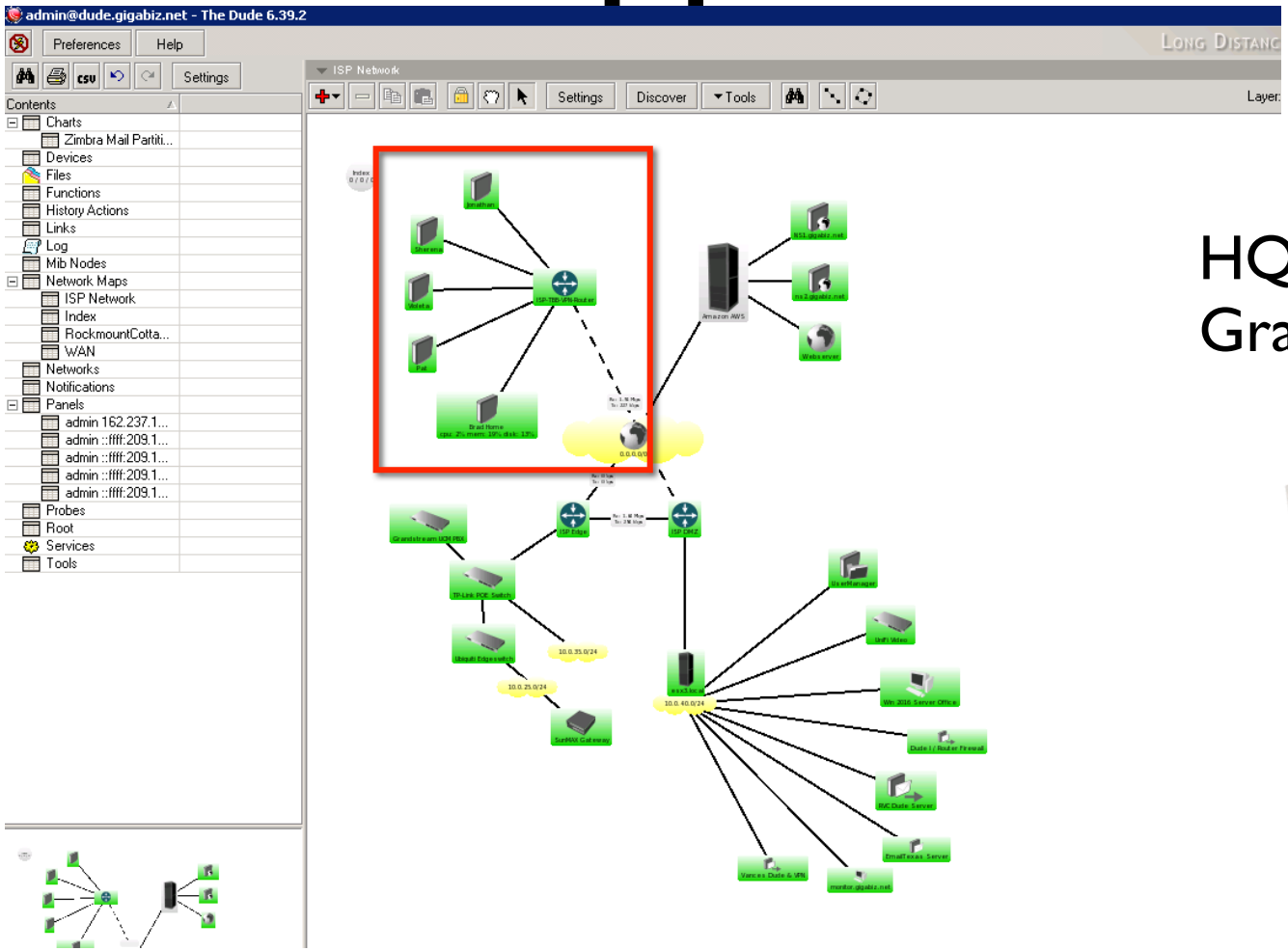


ISP Supplies Network



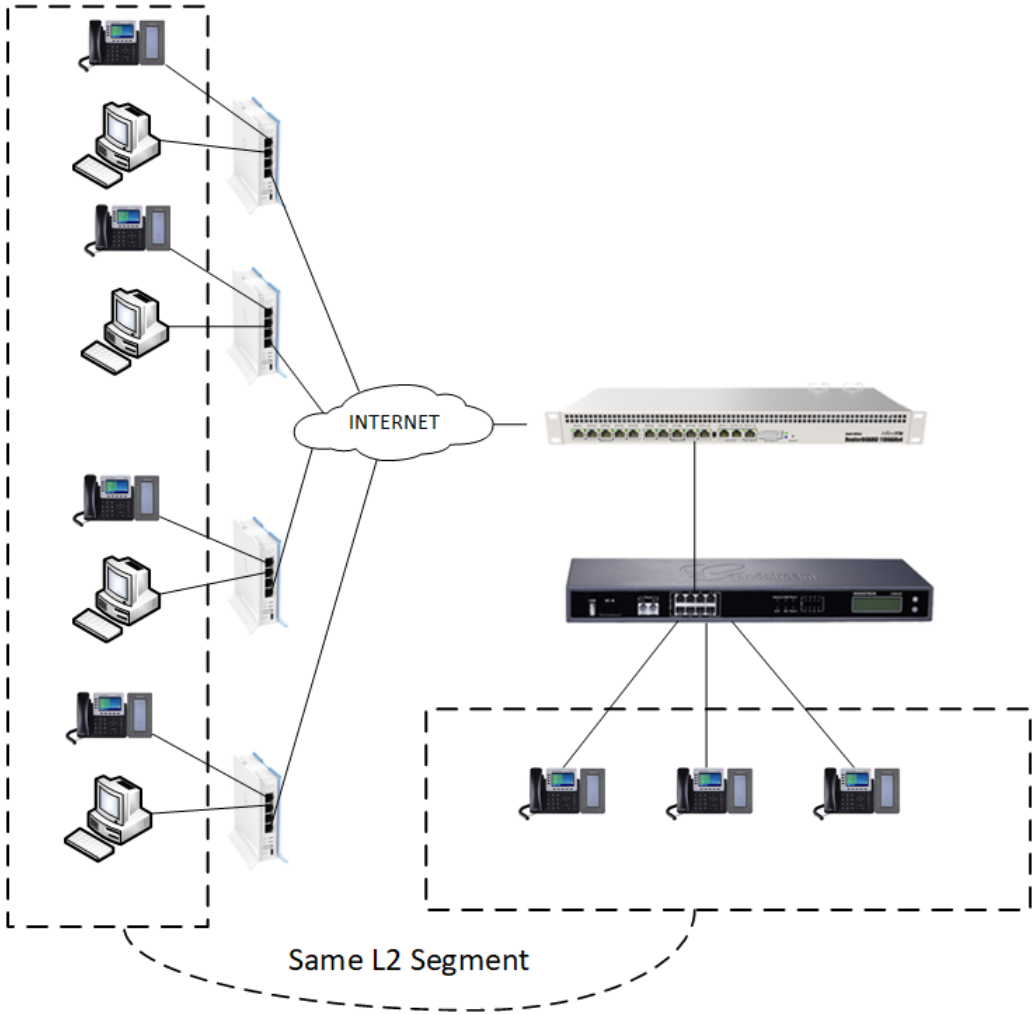
Remotes: HAP Lite and Grandstream GXP2140 Phone with Extension Module

ISP Supplies Network



HQ: RB1100AHx2 and Grandstream UCM6208

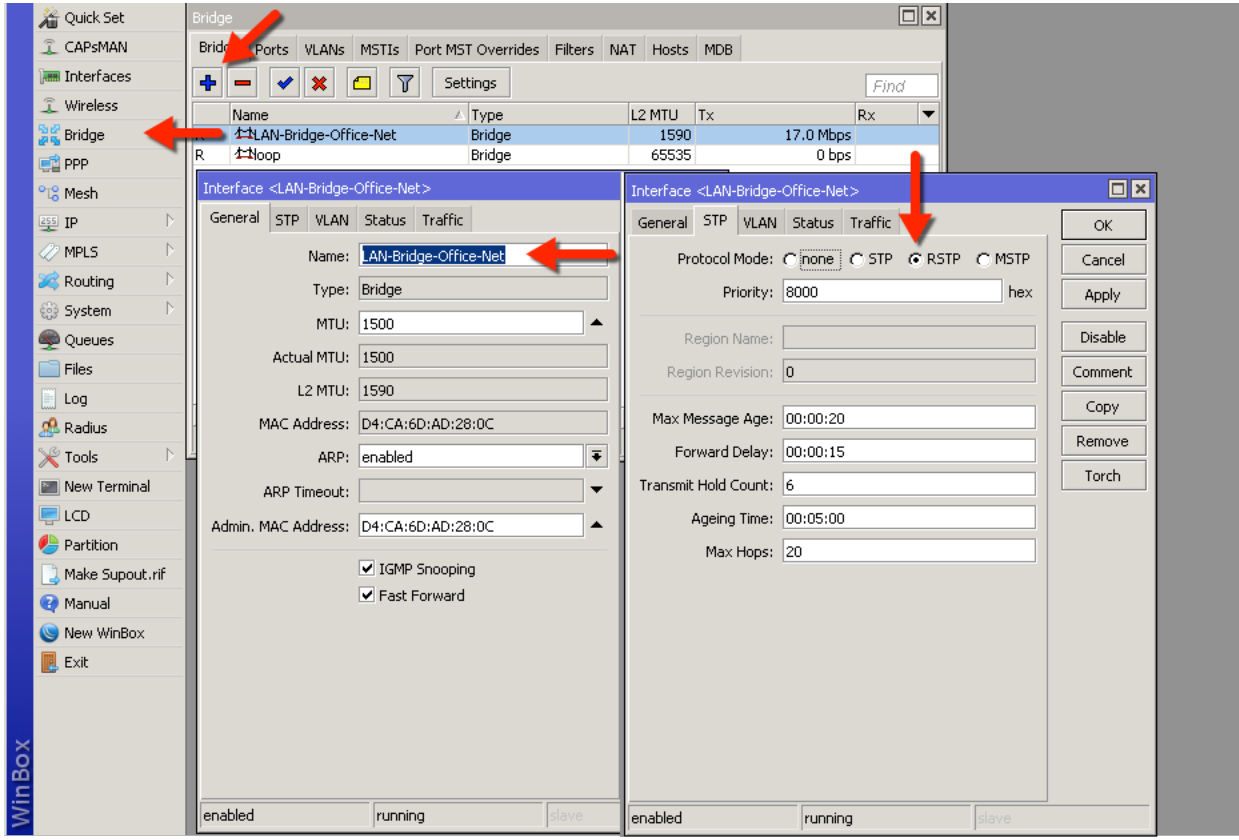
ISP Supplies Network



Configure HQ End

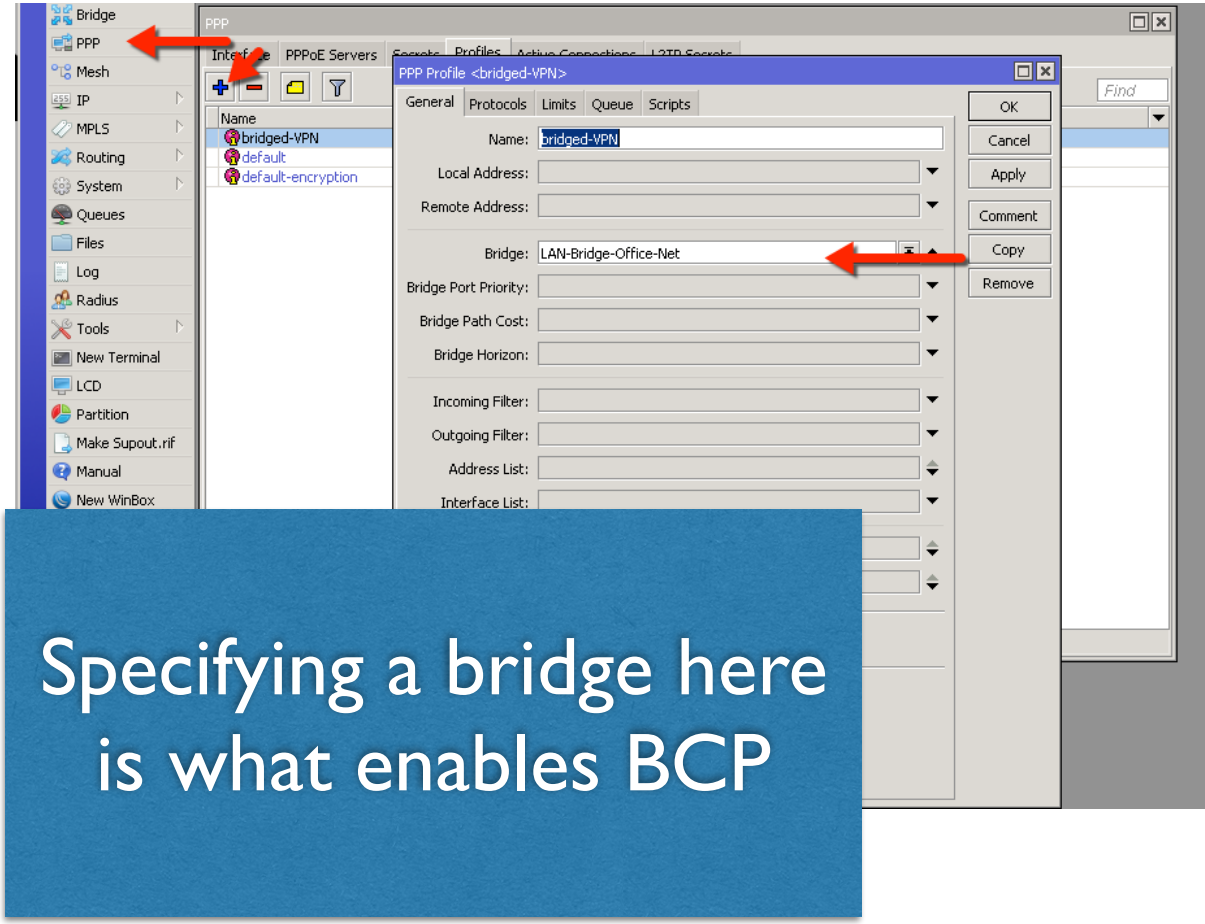
1. Create a bridge for the LAN. The PBX will connect to this bridge as well as any phones at HQ.

2. Add any local ethernet ports to the bridge.



Configure HQ End

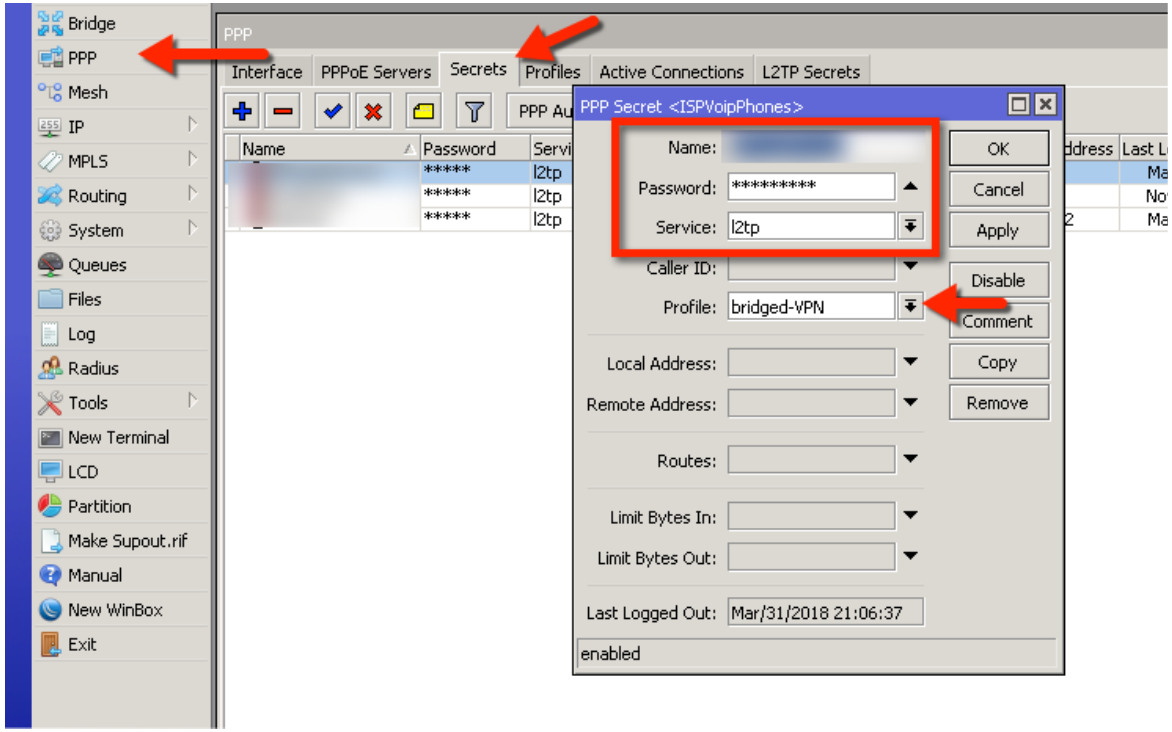
3. Create a PPP profile for inbound remotes. No IP's are required.



Specifying a bridge here is what enables BCP

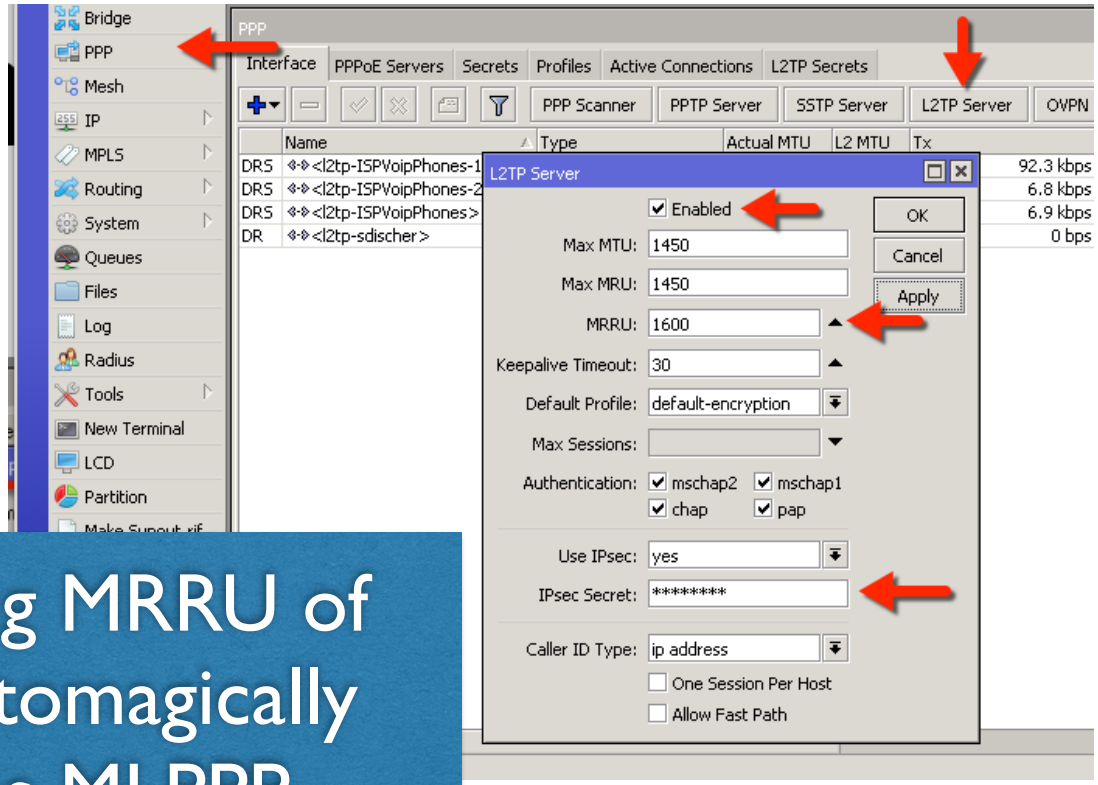
Configure HQ End

4. Create a PPP secret, one for all remote users or one for each (easier to identify them for troubleshooting later).



Configure HQ End

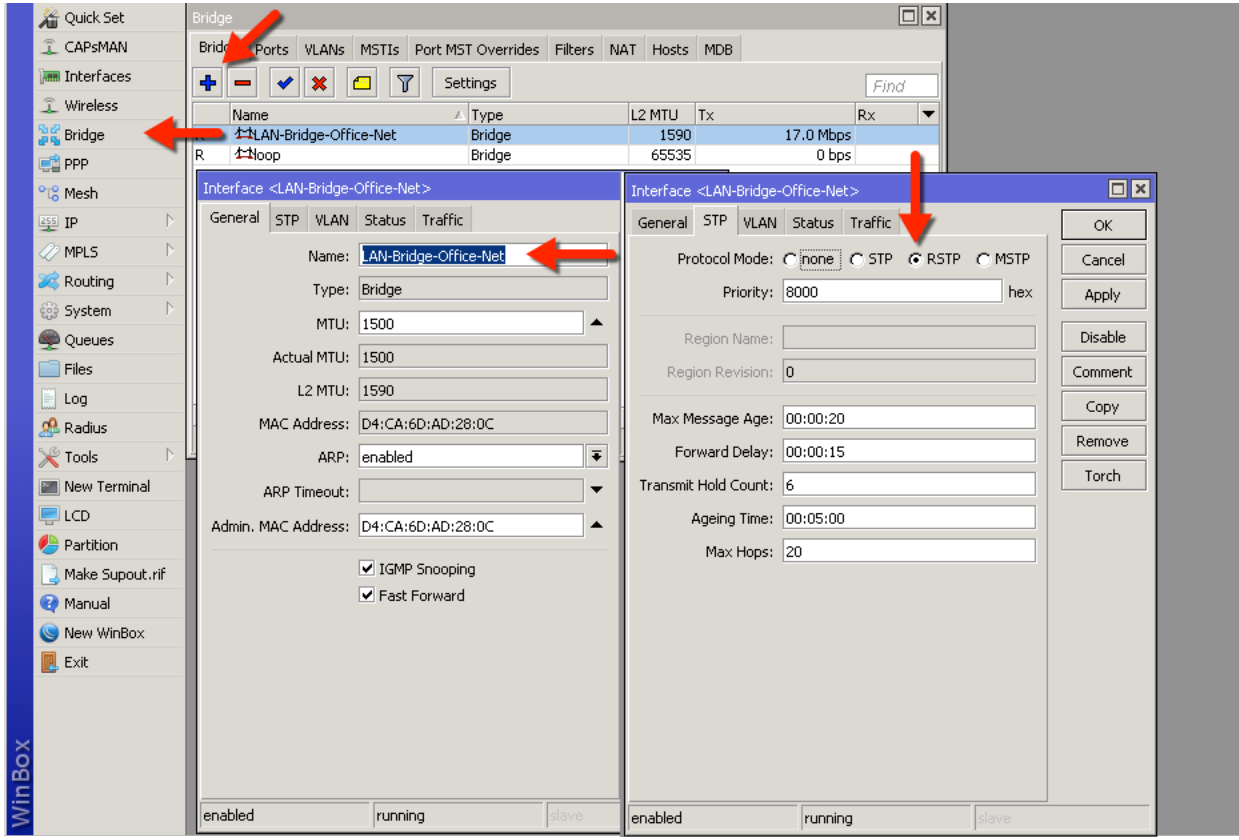
5. Enable L2TP server. Add IPSec secret for encryption.



Specifying MRRU of 1600 automagically enables MLPPP

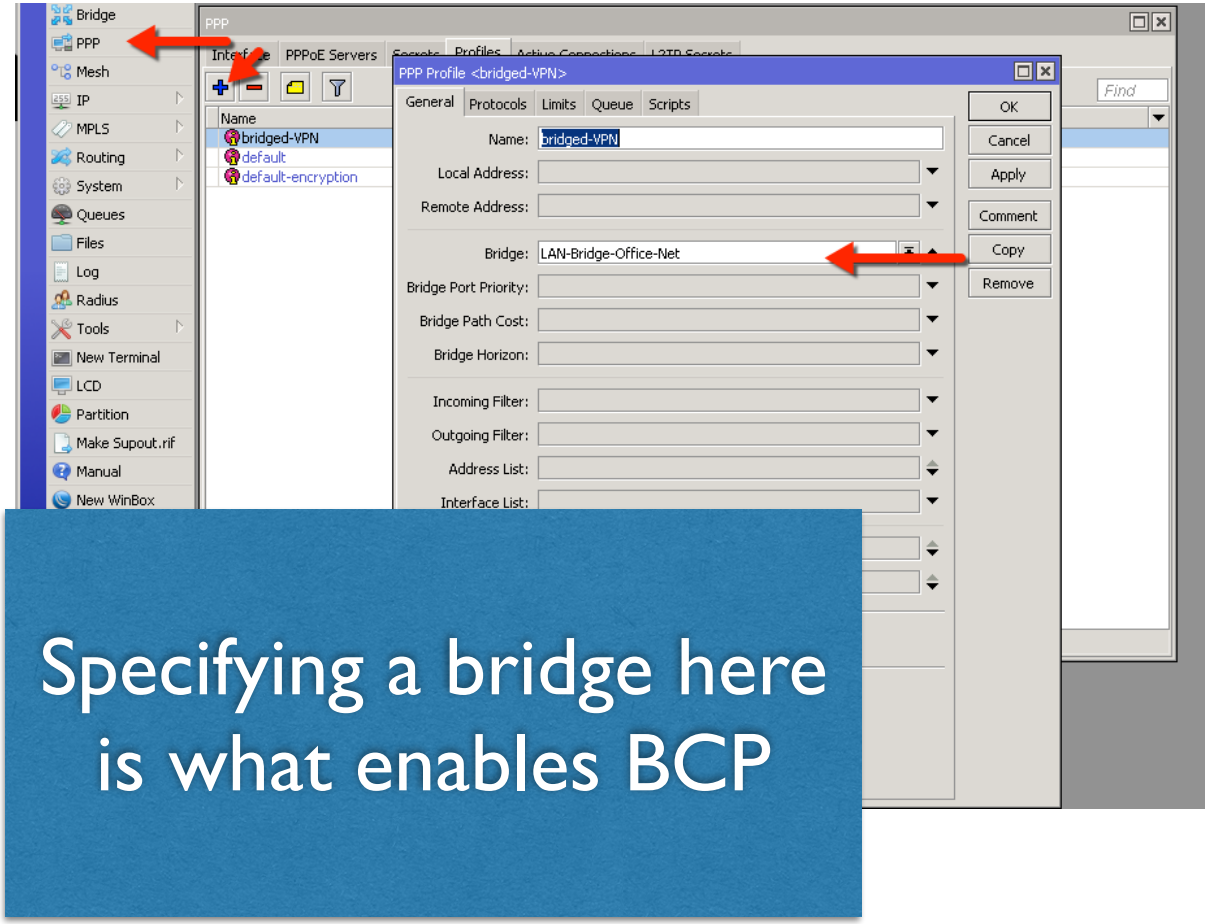
Configure Remote End

1. Create a bridge for the LAN. The phone and tunnel will connect to this bridge.
2. Add one local ethernet ports to the bridge for the phone.



Configure Remote End

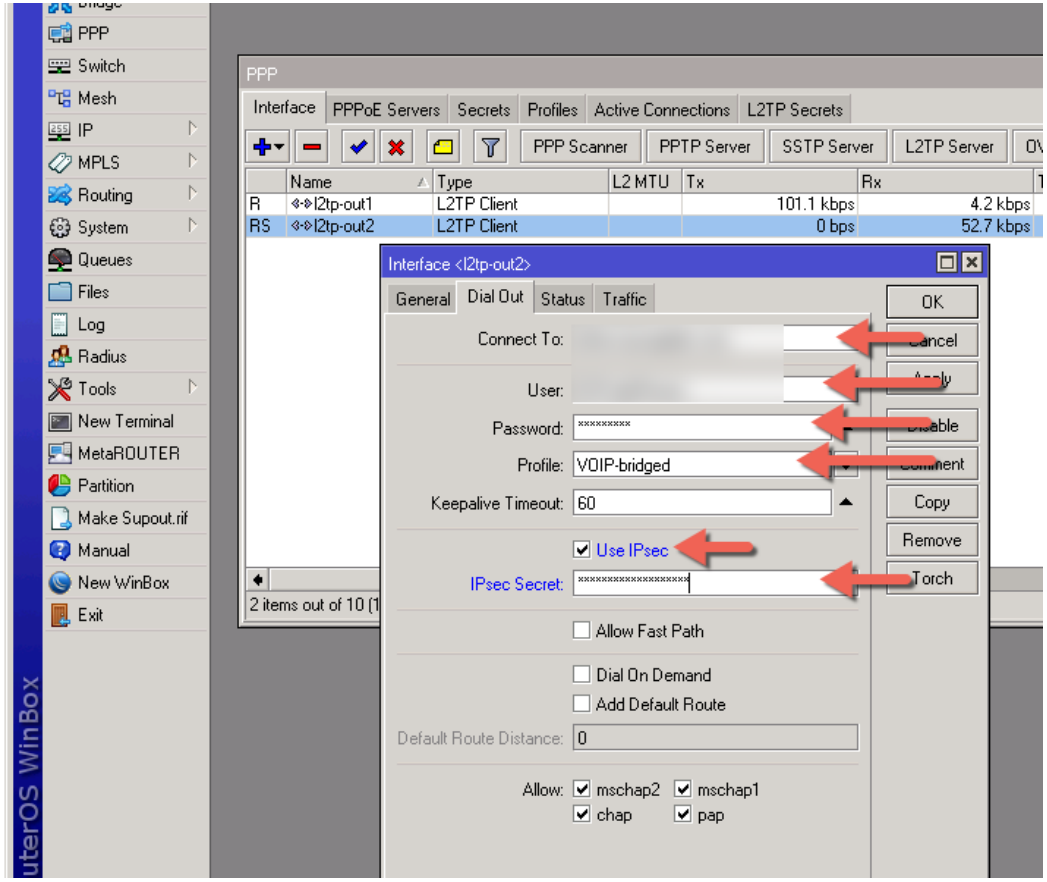
3. Create a PPP profile for the outbound tunnel.



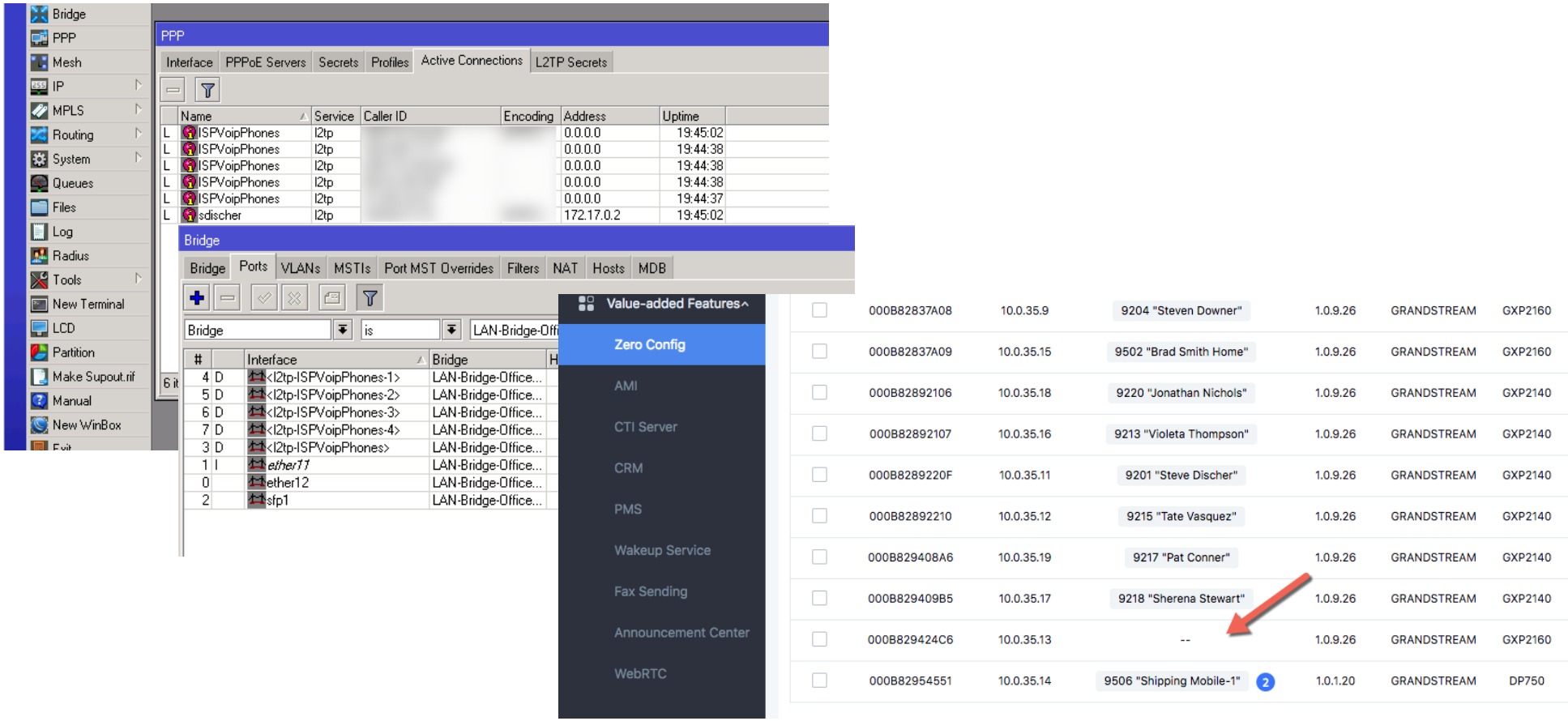
Specifying a bridge here is what enables BCP

Configure Remote End

4. Create L2TP Client. Add IPSec secret for encryption.

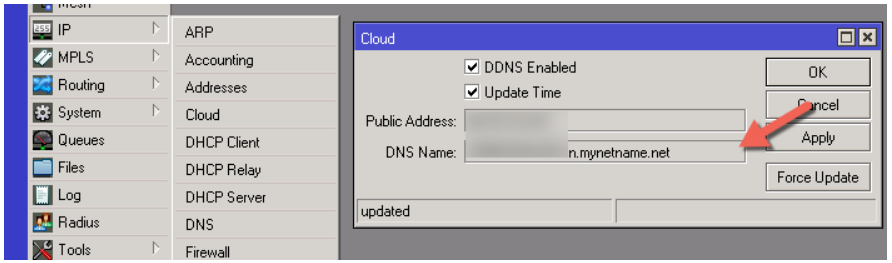


HQ Status

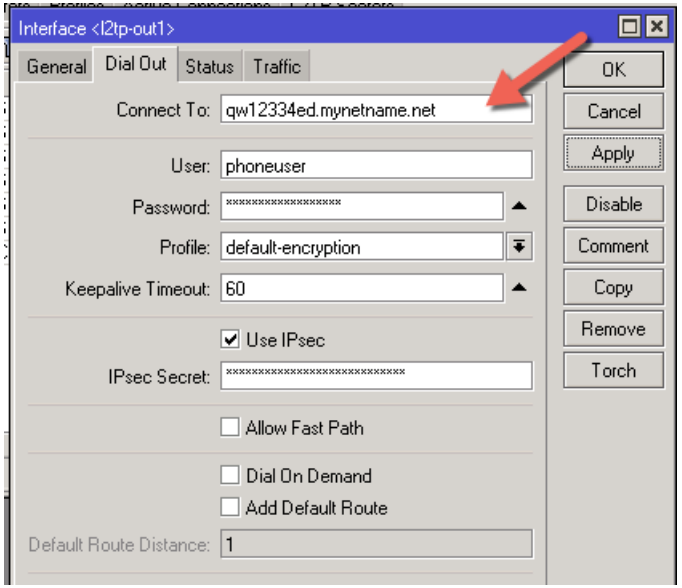

Bridge
PPP
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
LCD
Partition
Make Supout.rif
Manual
New WinBox
PPP
Interface
PPPoE Servers
Secrets
Profiles
Active Connections
L2TP Secrets
Name
Service
Caller ID
Encoding
Address
Uptime
ISPVoipPhones l2tp 0.0.0.0 19:45:02
ISPVoipPhones l2tp 0.0.0.0 19:44:38
ISPVoipPhones l2tp 0.0.0.0 19:44:38
ISPVoipPhones l2tp 0.0.0.0 19:44:38
ISPVoipPhones l2tp 0.0.0.0 19:44:37
sdischer l2tp 172.17.0.2 19:45:02
Bridge
Bridge
Ports
VLANs
MSTIs
Port MST Overrides
Filters
NAT
Hosts
MDB
Bridge
is
LAN-Bridge-Off
Interface
Bridge
4 D <l2tp-ISPVoipPhones-1> LAN-Bridge-Office...
5 D <l2tp-ISPVoipPhones-2> LAN-Bridge-Office...
6 D <l2tp-ISPVoipPhones-3> LAN-Bridge-Office...
7 D <l2tp-ISPVoipPhones-4> LAN-Bridge-Office...
3 D <l2tp-ISPVoipPhones> LAN-Bridge-Office...
1 I ether11 LAN-Bridge-Office...
0 ether12 LAN-Bridge-Office...
2 sfp1 LAN-Bridge-Office...
Value-added Features
Zero Config
AMI
CTI Server
CRM
PMS
Wakeup Service
Fax Sending
Announcement Center
WebRTC
000B82837A08 10.0.35.9 9204 "Steven Downer" 1.0.9.26 GRANDSTREAM GXP2160
000B82837A09 10.0.35.15 9502 "Brad Smith Home" 1.0.9.26 GRANDSTREAM GXP2160
000B82892106 10.0.35.18 9220 "Jonathan Nichols" 1.0.9.26 GRANDSTREAM GXP2140
000B82892107 10.0.35.16 9213 "Violeta Thompson" 1.0.9.26 GRANDSTREAM GXP2140
000B8289220F 10.0.35.11 9201 "Steve Discher" 1.0.9.26 GRANDSTREAM GXP2140
000B82892210 10.0.35.12 9215 "Tate Vasquez" 1.0.9.26 GRANDSTREAM GXP2140
000B829408A6 10.0.35.19 9217 "Pat Conner" 1.0.9.26 GRANDSTREAM GXP2140
000B829409B5 10.0.35.17 9218 "Sherena Stewart" 1.0.9.26 GRANDSTREAM GXP2140
000B829424C6 10.0.35.13 -- 1.0.9.26 GRANDSTREAM GXP2160
000B82954551 10.0.35.14 9506 "Shipping Mobile-1" 2 1.0.1.20 GRANDSTREAM DP750

FAQ: HQ Config

What if my HQ device has a dynamic IP?

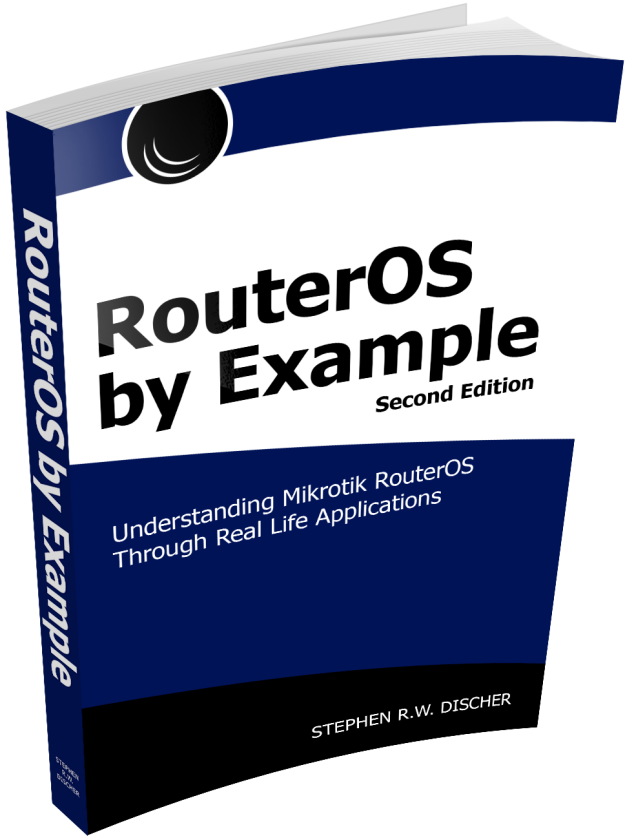


No problem. Use IP Cloud, MikroTik's dynamic DNS. Set the HQ DDNS name as "Connect To" address on remote routers



Second Edition

- Everything is updated to version 6.40
- Examples are expanded
- Significant content for CRS switches was added including hw-offload
- AVAILABLE on Amazon and ISPSupplies.com



Thank you

- Training: MyWISPTraining.com & LearnMikroTik.com
- Store: ISPSupplies.com
- Blog: SteveDischer.com
- "RouterOS by Example" available from ISP Supplies, Amazon
- Configurator: MikroTikConfig.com