Bridged to Routed - How?

Link Technologies, Inc.

3/15/2011

Dennis Burgess

- **Mikrotik Certified Trainer / Engineer**
- **MikroTik Certified Dude Consultant**
- **Consulting Since 1997**
  - *Enterprise Class Networks*
  - *WAN Connectivity*
- **Certifications**
  - *Cisco, Microsoft, MikroTik*
- **BGP/OSPF Experience**
  - *Deployed many BGP and OSPF networks based on MikroTik, Cisco and Juniper*
- **What I do Currently**
  - *Work with WISPs and CLECs all over the world, designing, and assisting in network configurations including wireless, OSPF, BGP, Traffic Management, Firewalling, and other Network Engineering*

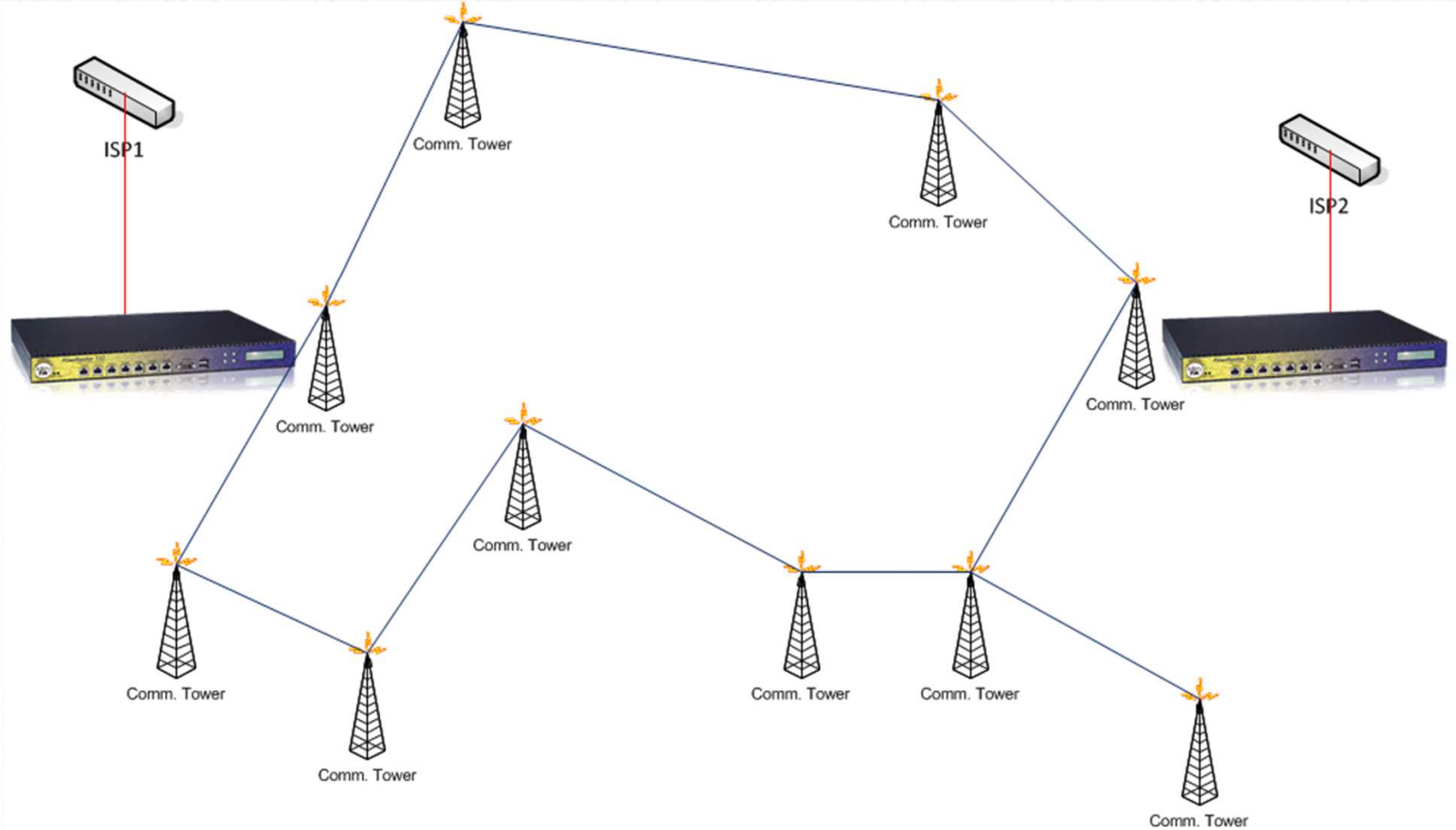
What are we going to Cover?

- Why Bridged Networks Typically Fail
- Why Routed Networks Work
- Is there a “happy medium” between the two
- Conversion Options
- Conversion Techniques

A Bridged Network

- Large geographically diverse network
  - Bridged Backhauls
  - Bridged Client Radios
  - Bridged Access Points

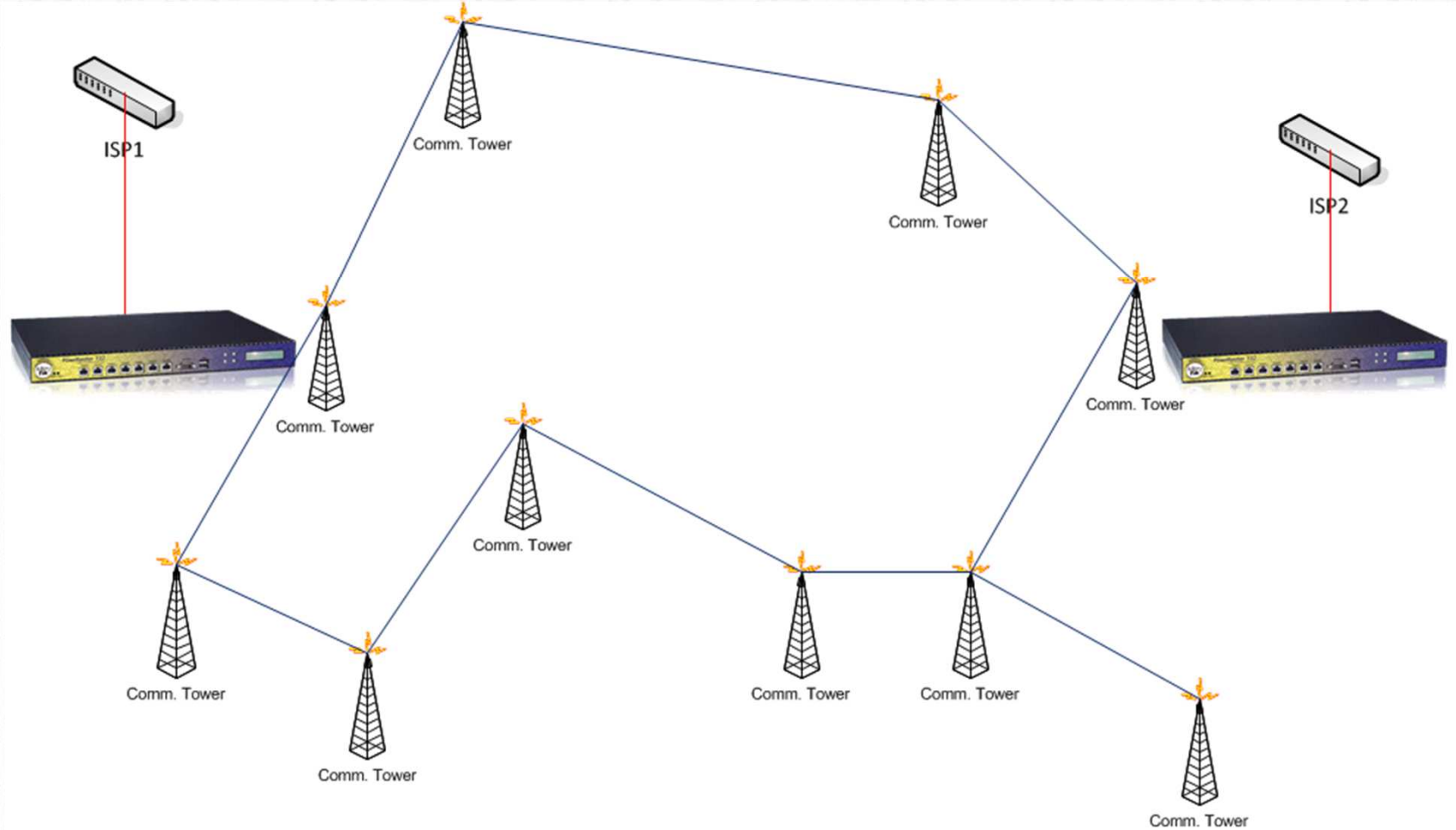
A Bridged Network



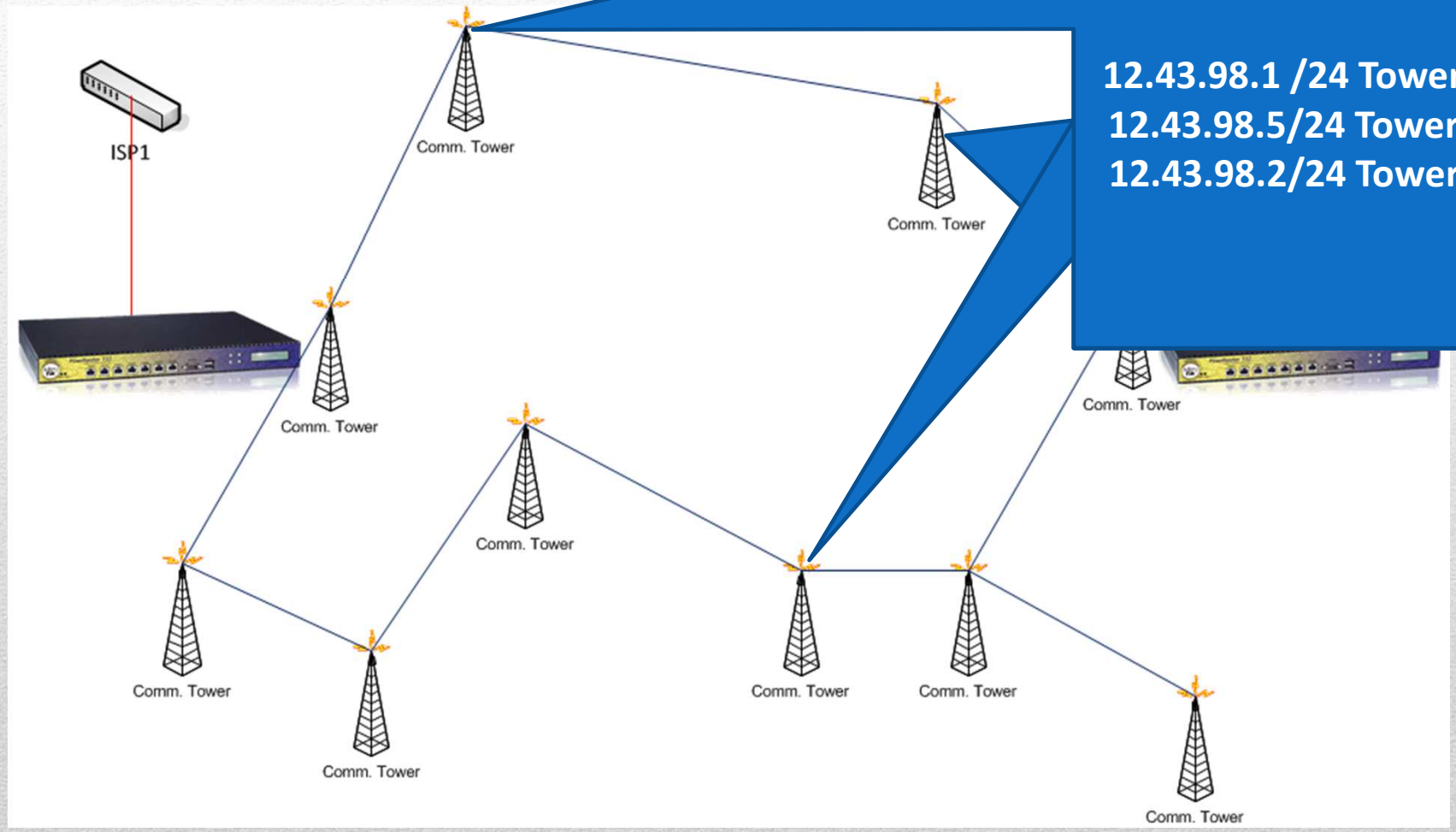
A Bridged Network

- **Positives of a bridged network**
  - **No lost IP addresses due to Subnetting**
  - **Easy IP Scheme**
  - **Easy IP moves**
  - **IP scheme super simple**
  - **No subnetting knowledge needed**
    - *Lower Cost or non-existent engineering*
  - **Switches at towers vs. routers**
    - *Lower Cost hardware*
    - *Faster ping times – switching faster than routing*
  - **Single DHCP server for entire network!**

A Bridged Network



A Bridged Network



Same Subnet.

12.43.98.1 /24 Tower A
12.43.98.5/24 Tower B
12.43.98.2/24 Tower C

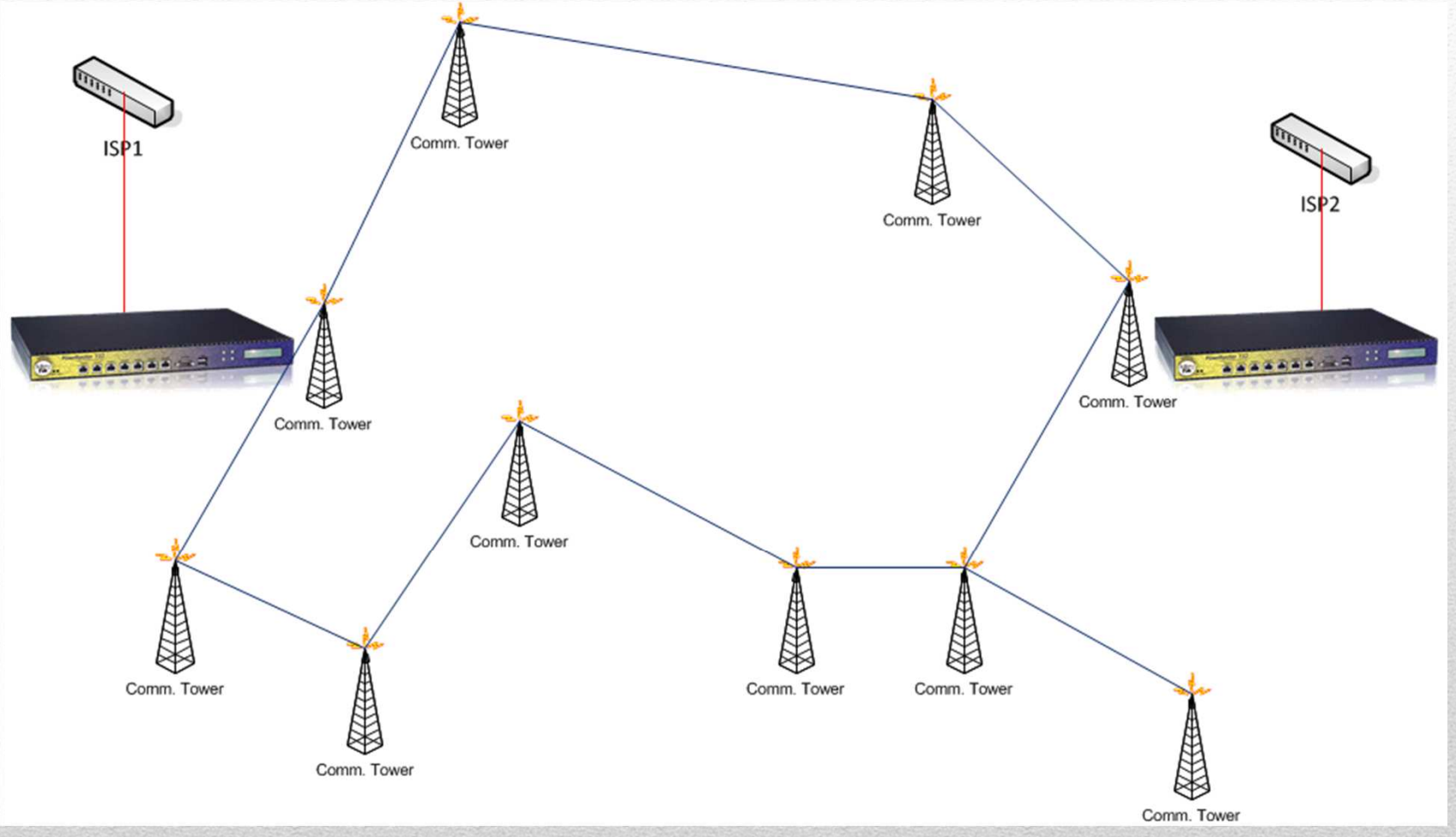
A Bridged Network

- **Negatives of a bridged network**
  - **Automatic routing of network done at bridge levels**
    - *Great for simple "ring" networks*
    - *Not Great for Complex interconnected networks*
    - *Customer has CPE in business plugged into network switch. Runs cable to another switch. Everything works for months! One day customer comes in and computers on second switch does not work. Customer plugs second cable from primary to secondary switch! Loop occurs! Looped data goes out CPE, to AP, to other APs to Other Towers!*

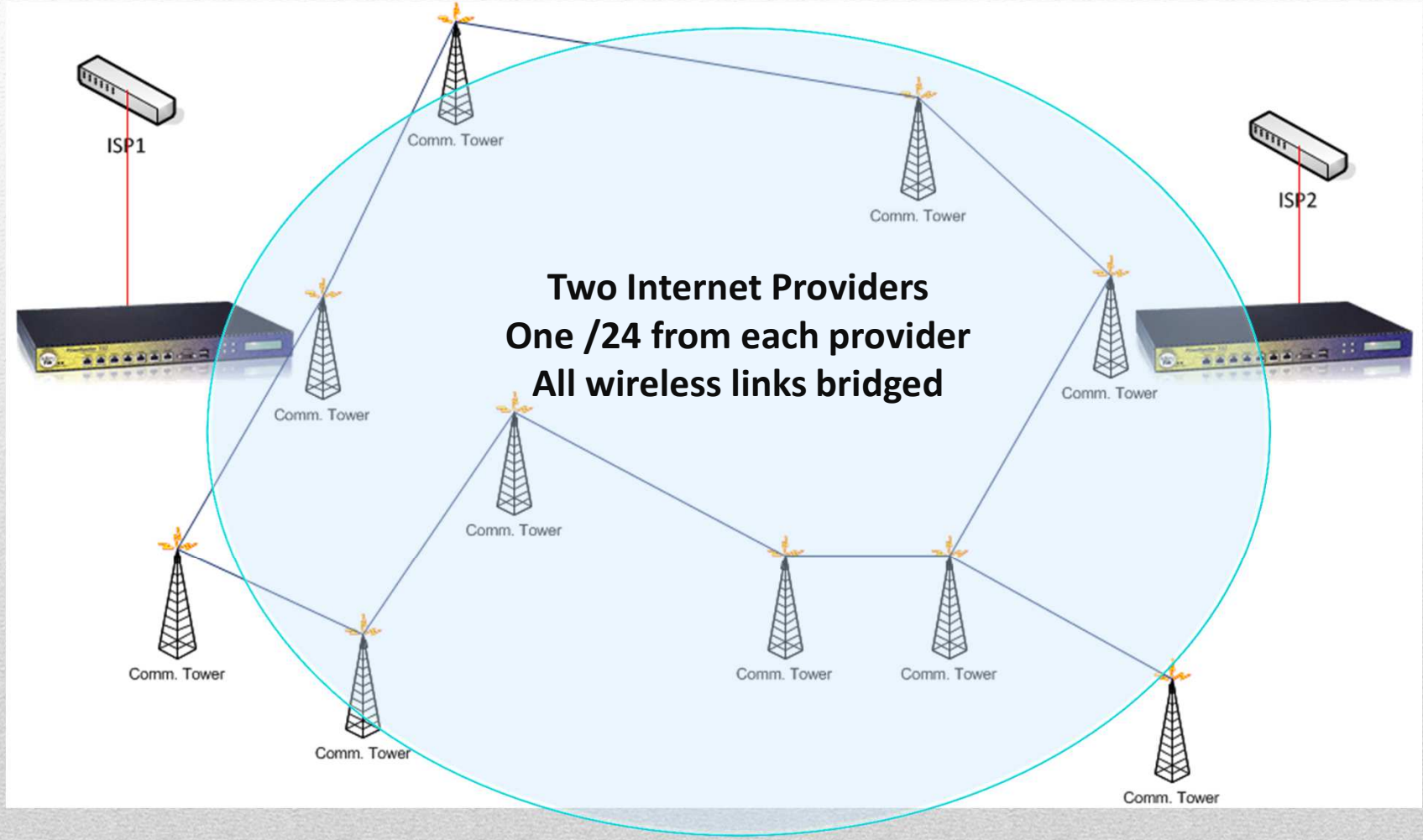
Bridge Loops

- **Bridge LOOPS!**
  - *Create network wide issues*
    - Customers can create issues for ISP
    - Not to mention some tech plugging in something wrong at a tower!
    - Tower Installers programming AP connects it to another AP on same tower.
    - Things happen!
  - *(r)STP will assist with this, but not a solution for large networks*

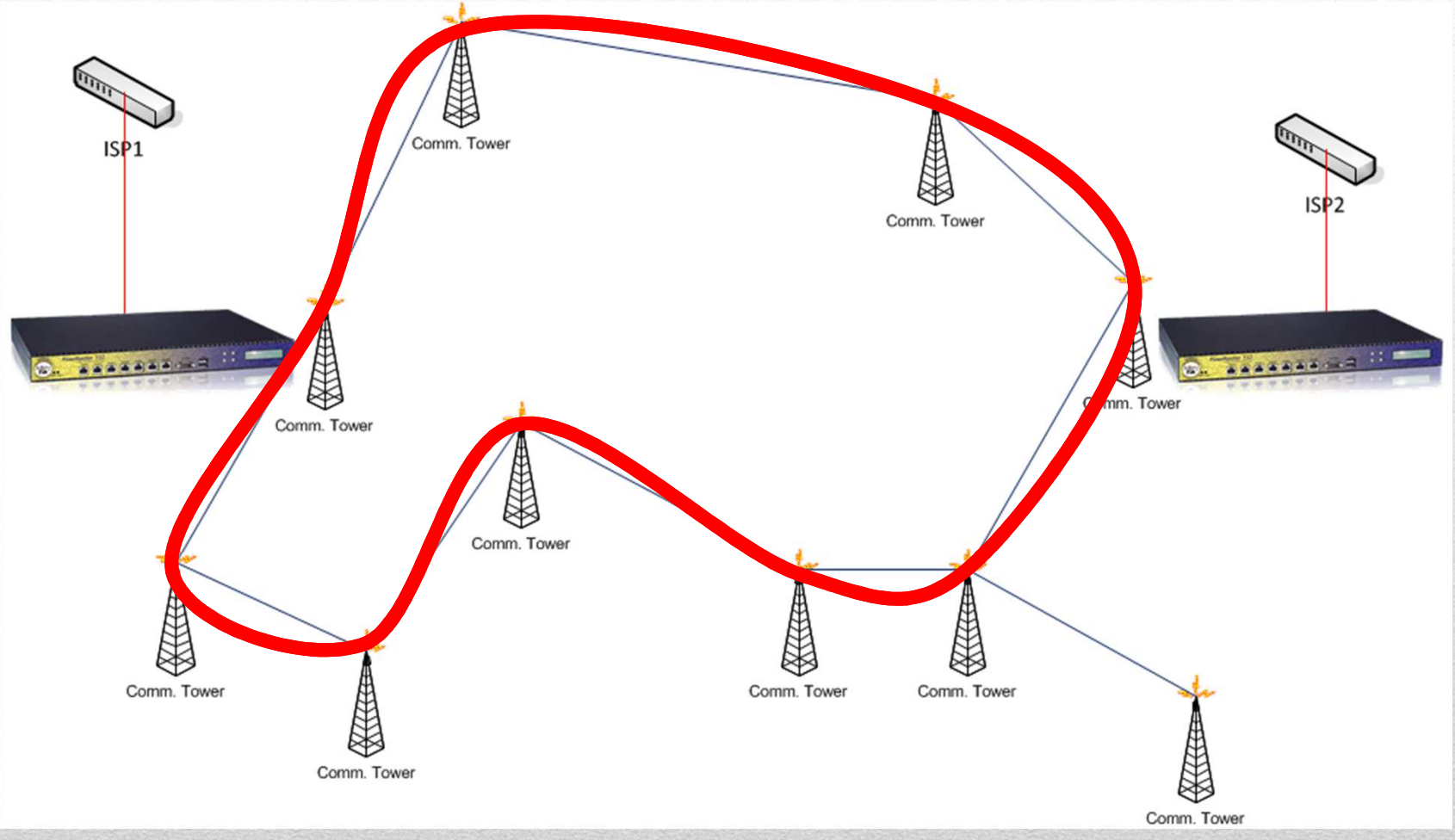
Bridge Loop



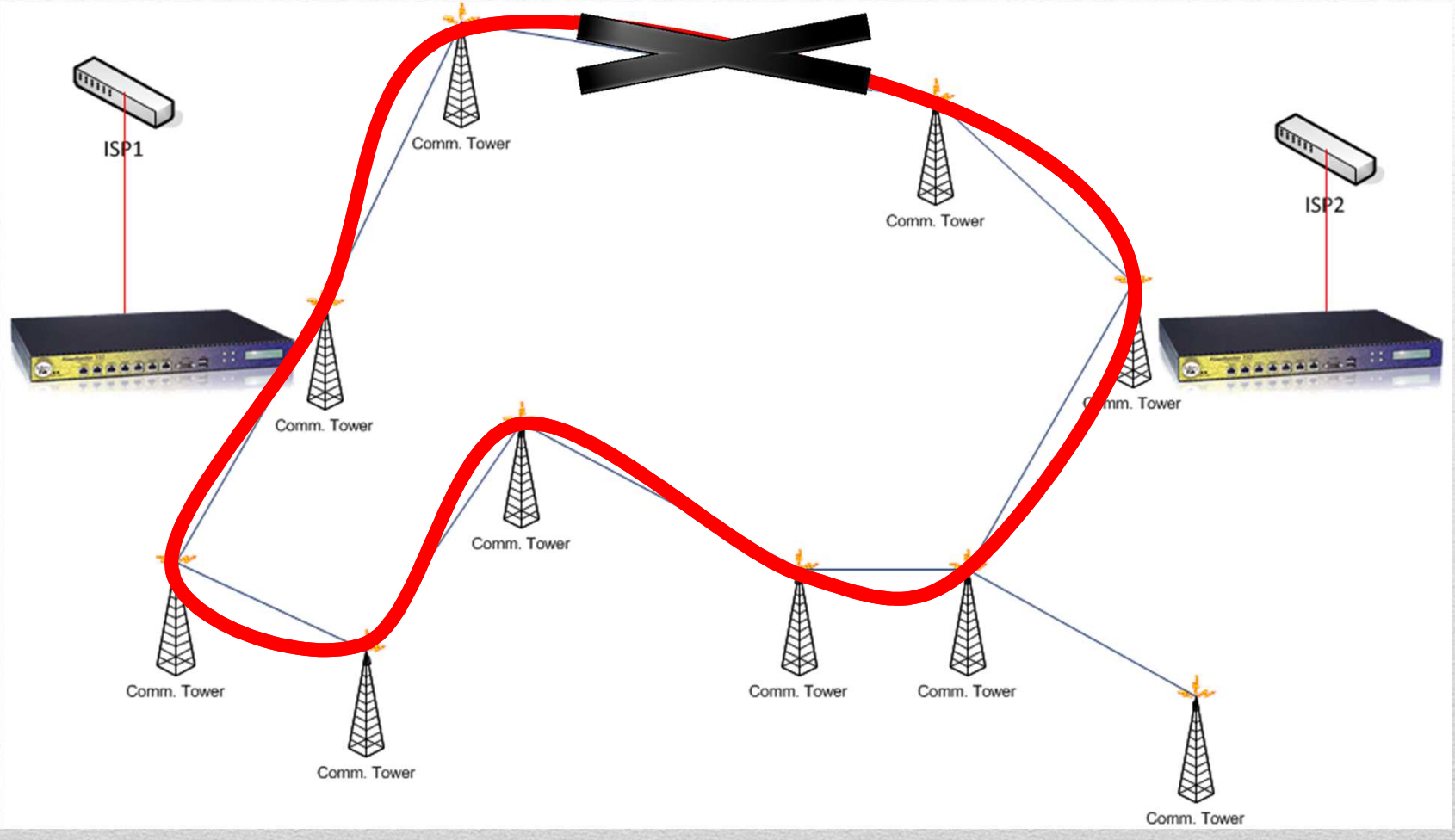
Bridge Loop



A BIG ULGY Bridging Loop!



Use (r)STP to block the loop and give us a “redundant” path using Bridging.

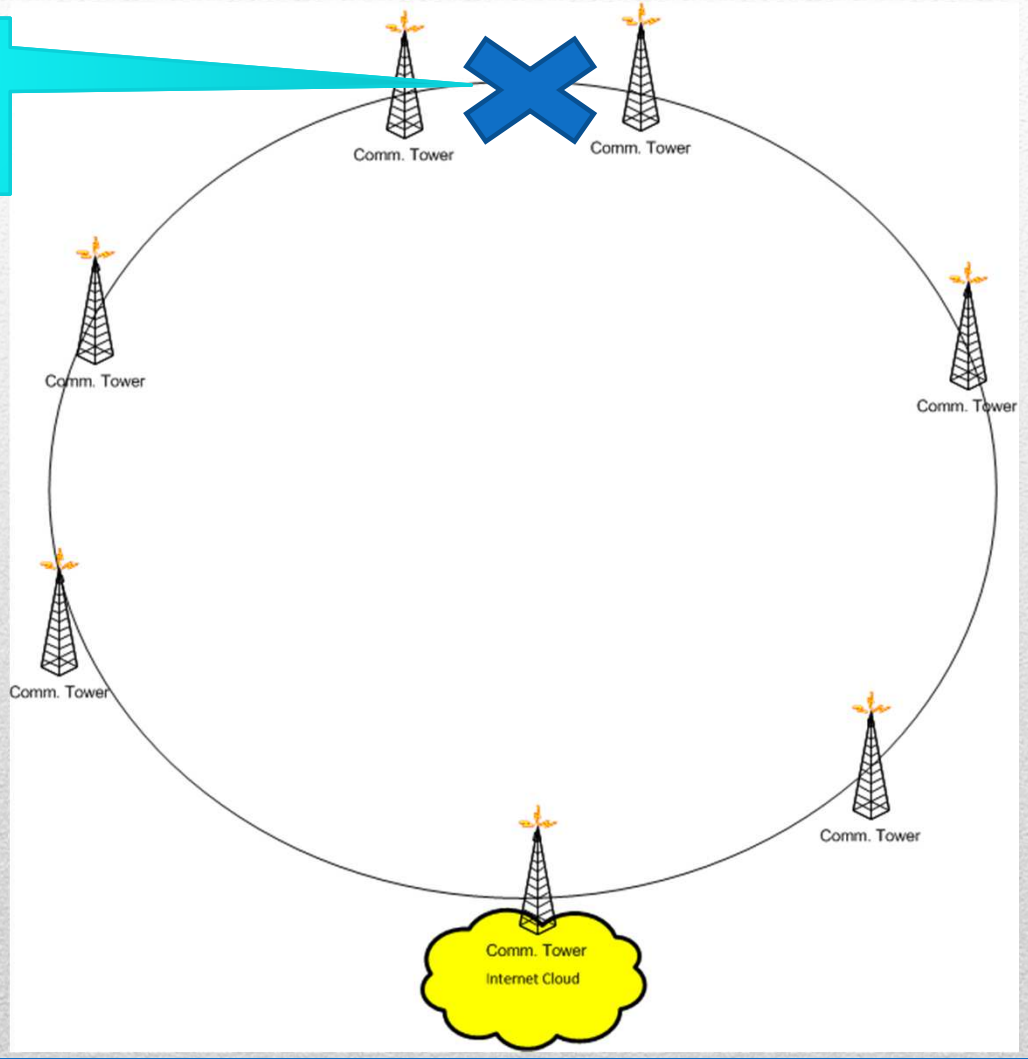


A Bridged Network

- **Negatives of a bridged network**
  - **Automatic routing of network done at bridge levels**
    - *Great for simple "ring" networks*
    - *Not Great for Complex interconnected networks*
    - *Complicated setups for failover connections, and redundancies*
    - *RSTP turns off links! Backup links are NOT used at all!*

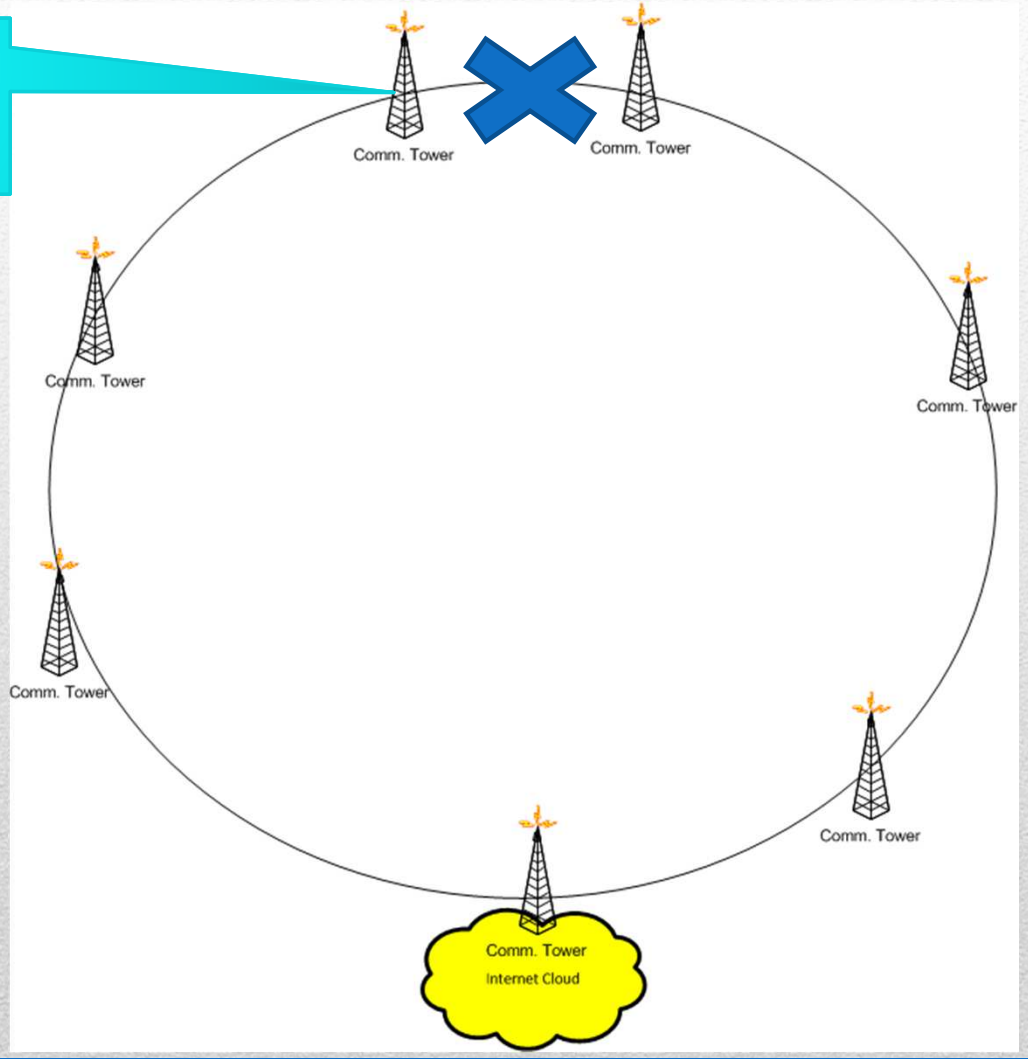
A Bridged Network

Bridge Breaks Link



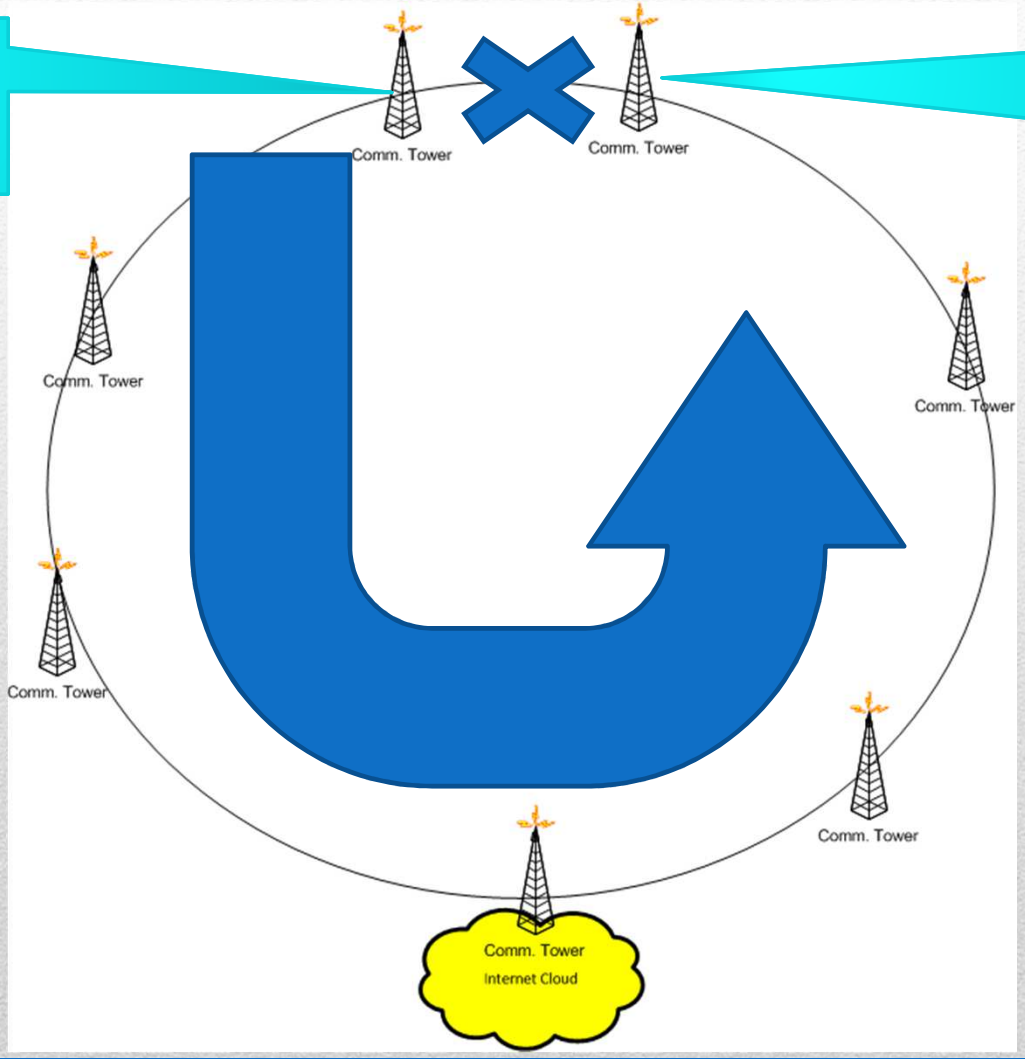
A Bridged Network

Traffic from here



A Bridged Network

Traffic from here



Must go completely AROUND the network

A Bridged Network

- **Negatives of a bridged network**
  - **Issues Harder to track down**
    - *Lost ARPs*
    - *Devices sending out Thousands of PPS due to bad NIC driver?*
    - *Pseudo Bridging faults/issues*
      - MAC NATing creates other issues on network
    - *Ever Try to trace a problem IP?*
      - If you have an IP that is not working what do you do?
        - Can't traceroute it!
      - Ping it from the CPE, Ping it from the AP, then Ping it from the BH, then From the other side of the backhaul, um, how many more backhauls do we have?
        - Where does it stop
    - *Unless you are actively monitoring all network devices, its harder to identify where a break in network connectivity is.*

A Bridged Network

- **Negatives of a bridged network**
  - **Broadcast Domains**
    - *A single Client can directly talk to any other client, AP, CPE.*
    - *Due to this, figure every device on a 1000 device network, will have to hear ARPs.*
    - *ARP Process*
      - Client wants to talk to gateway IP. SEND BROADCAST ARP
        - "What MAC responds to x.x.x.x IP Address?"
        - This is sent to EVERY DEVICE ON THE BRIDGED NETWORK!
      - Gateway gets broadcast and then does a directed reply.
        - "I am responsible for x.x.x.x IP, here is my MAC"
      - **EVERY DEVICE GOES THOUGH THIS!**

A Bridged Network

- **Negatives of a bridged network**
  - **Broadcast Domains**
    - ***IP Takeover – ARP spoofing – ARP Poisoning***
      - **Customer puts your gateway IP as their IP!**
      - **Customers ARPs start going to their PC or device!**
    - ***Broadcasts and Wireless Links***
      - **Broadcasts are typically the lowest priority on many networks and wireless networks**
      - **Broadcasts can be dropped on loaded connections**
    - ***Customer Access to backbone***

ARP Spoofing

ARP Spoofing / Takeover

- **Customer with completely bridged network**
  - **Irate client on network – "Network Admin"**
  - **Took the gateway IP, and added it to his internal Router**
    - *Customers traffic was going though his router*
    - *Created overall network slowdown (slow Wireless link)*
    - *Most traffic appeared to come from client of customer*
  - **Had to disconnect clients RADIO from AP to recover**
    - *Shows what damage a client can do with access to your backbone!*

Customer Router Issue

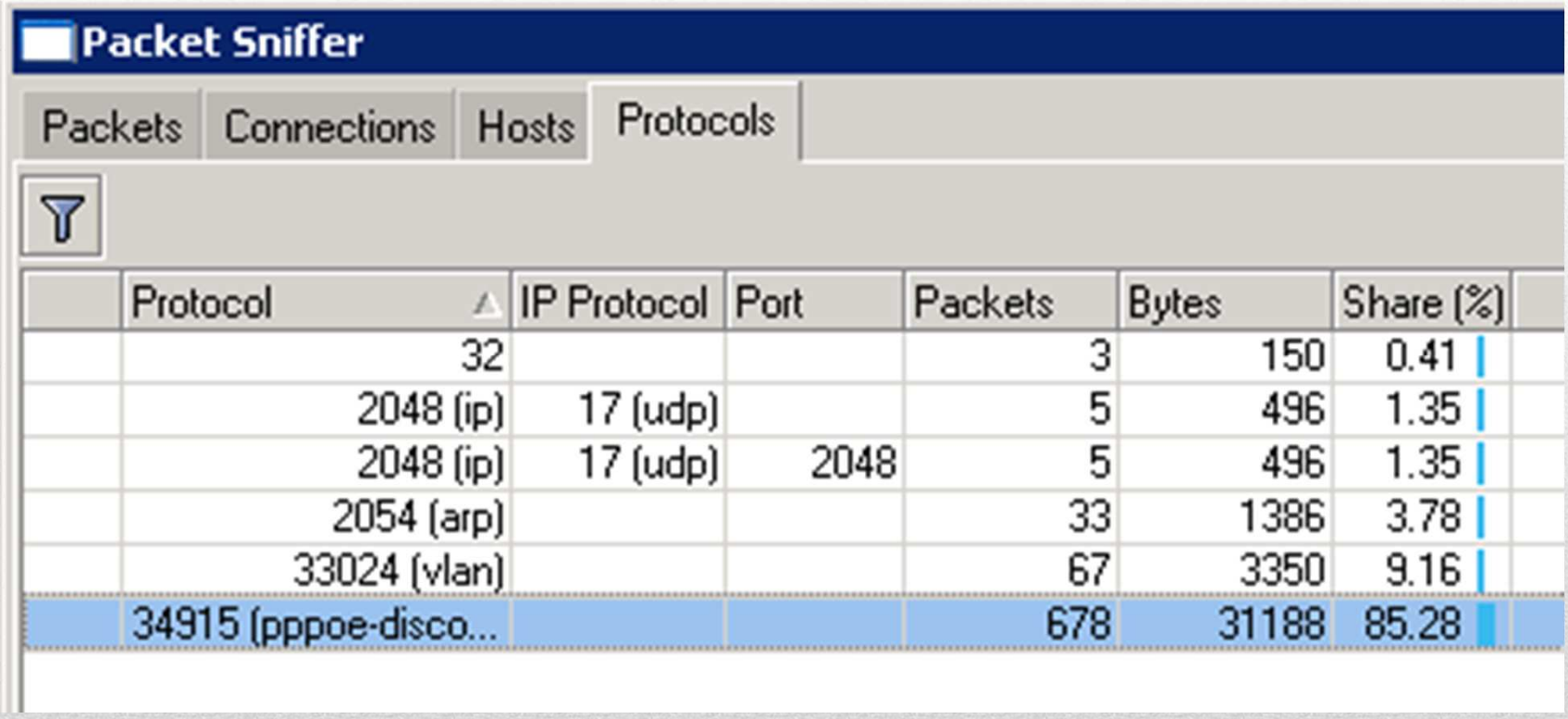
Bridged Network

- **Bad Router Issues**
  - **Example – Customer Controlled Router FLOODING network with PPPoE Discovery Requests!**
  - **5000+ Packets Per Second**
  - **Small Packets**
    - *Created High Loading on Backhauls and other devices*
    - *Devices with low CPU caused network slowdown*
    - *Actual network bandwidth usage was around 500k.*
      - Due to the High PPS, it caused network wide issues!

Bad Customer Router

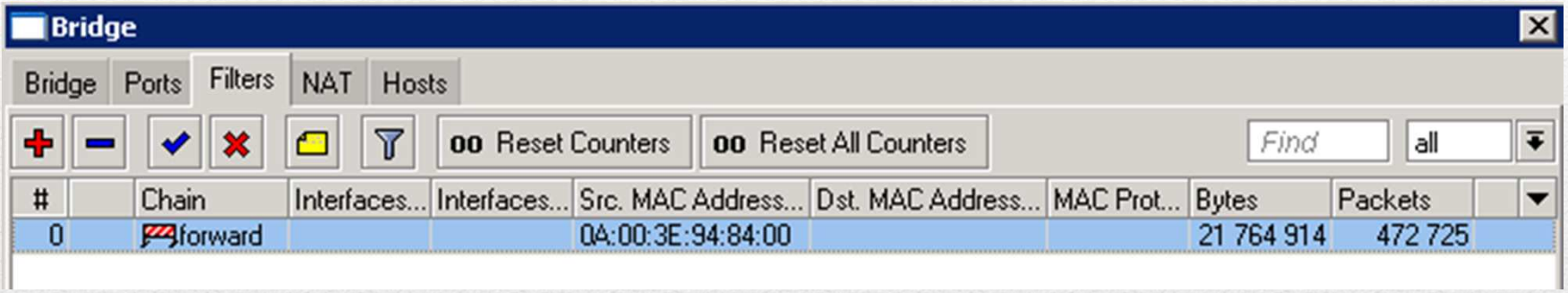
	0.913	cpe-32.52-vl50	00:15:17:24:A3:7D			2054 (arp)	42
	0.920	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	0.922	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	0.923	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	0.925	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	0.927	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	0.935	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	0.937	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	0.944	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	0.945	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	0.951	cpe-32.52-vl50	00:15:17:24:A3:7D			2054 (arp)	42
	0.969	cpe-32.52-vl50	00:15:17:24:A3:7D			2054 (arp)	42
	0.972	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	0.973	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	0.975	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	0.976	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	0.978	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	0.979	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	0.980	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	0.982	cpe-32.52-vl50	00:15:17:24:A3:7D			2054 (arp)	42
	0.986	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	0.988	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	0.995	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	0.996	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	1.003	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	1.004	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	1.011	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	1.012	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	1.022	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	1.024	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	1.037	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	1.039	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	1.040	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	1.059	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	1.060	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46
	1.062	cpe-32.52-vl50	0A:00:3E:94:84:00			34915 (pppoe-discovery)	46

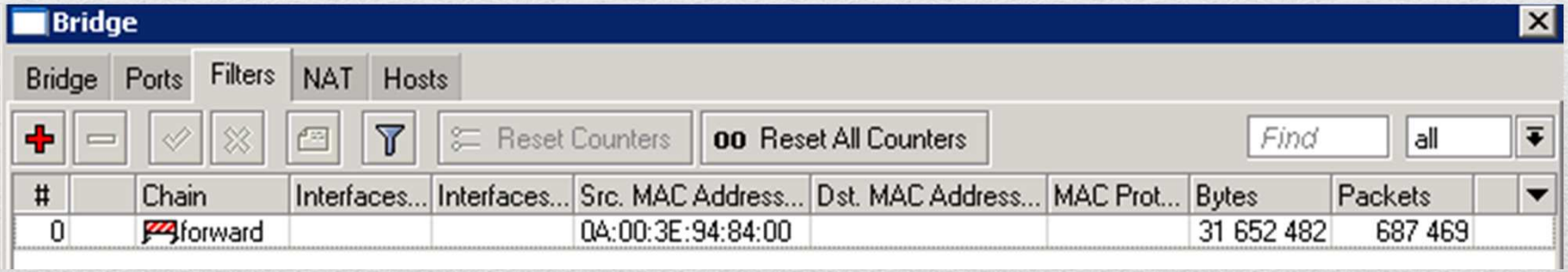
Bad Customer Router



Protocol	IP Protocol	Port	Packets	Bytes	Share (%)
32			3	150	0.41
2048 (ip)	17 (udp)		5	496	1.35
2048 (ip)	17 (udp)	2048	5	496	1.35
2054 (arp)			33	1386	3.78
33024 (vlan)			67	3350	9.16
34915 (pppoe-disco...			678	31188	85.28

Bad Customer Router





Screenshots about 10-15 seconds apart!

Want to go Routed?

So you want to go routed!

- **Positives with a Routed Network**
  - **Automatic Rerouting**
    - *With Dynamic Routing Protocols*
  - **Usage of backup links for data that can use it**
    - *Backup links are not disconnected and not usable*
  - **Limited Broadcast domains**
    - *If you route customers CPE (recommended)*
      - Customers never have direct access to your AP
      - Bridge Loops or other “internal” issues are stopped at the CPE!
      - Customers can’t type in a wrong IP and cause network issues
    - *If your Route at the APs*
      - A issue on one wireless AP will not affect others

So you want to go routed!

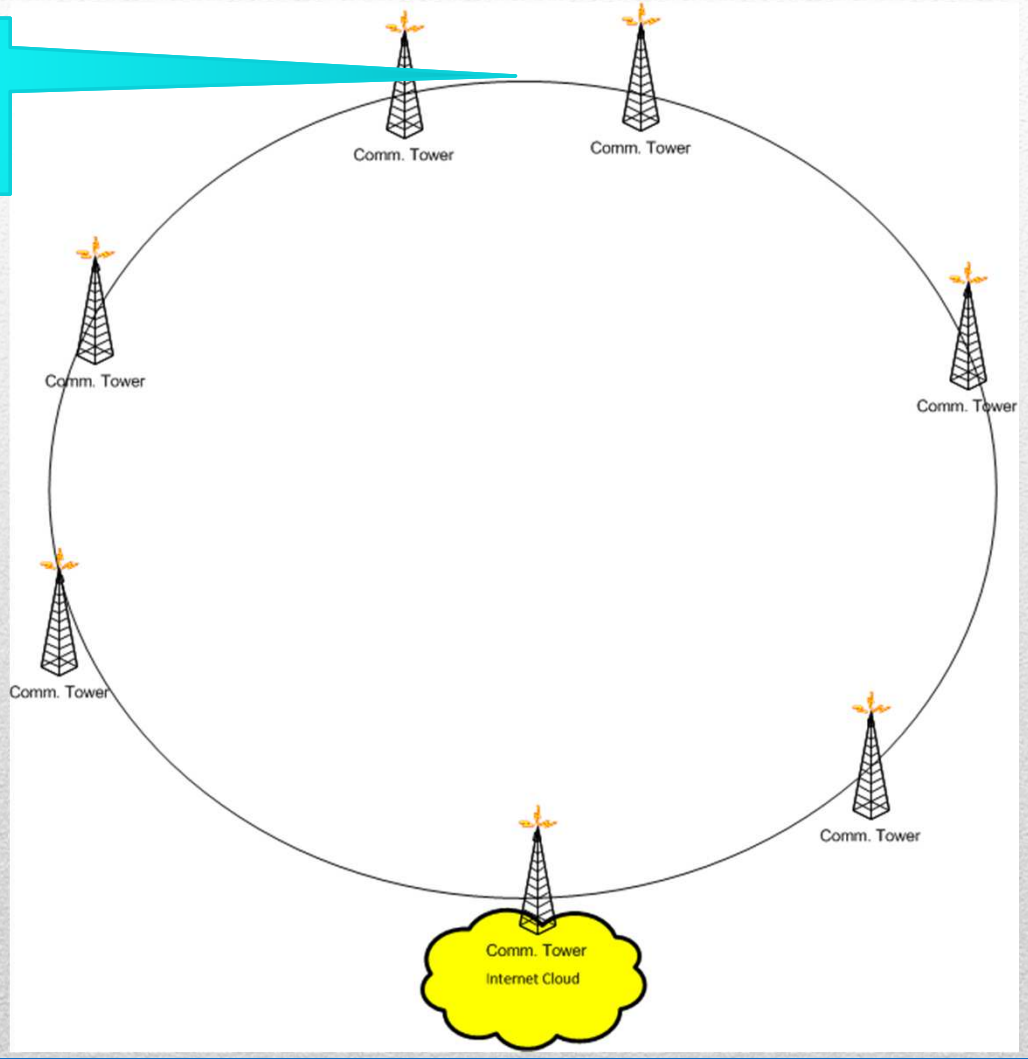
- **Positives with a Routed Network**
  - **Automatic Rerouting**
    - *With Dynamic Routing Protocols*
  - **Limited Broadcast domains**
    - *If you Route your backbone*
      - Automatic rerouting of traffic
      - Only traffic that needs to leave your tower will!
      - You control what ARPs go across your backhauls
      - Greater efficiency
  - **TraceRoute Assistance**
    - *You can use traceroutes to spot slow links or other issues.*

So you want to go routed!

- **Positives with a Routed Network**
  - **Usage of backup links for data that can use it**
    - *Backup links are not disconnected and not usable*

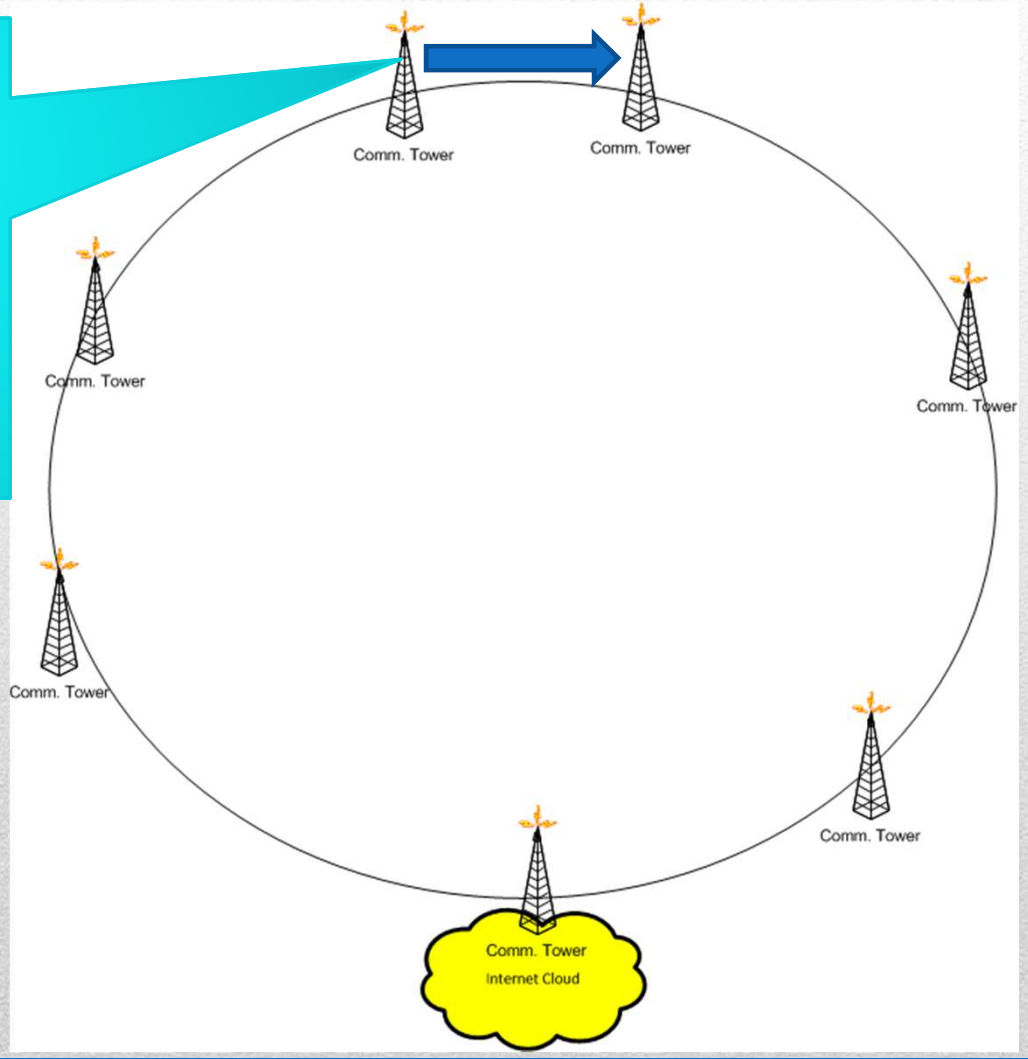
So you want to go routed!

This link is not used for internet



So you want to go routed!

Traffic from tower to tower uses the most cost effective path. The link does not go completely unused.



So you want to go routed!

- **Negatives of Routed Networks**
  - **Yes there are some!**
  - **Subnetting**
    - *Subnetting requires knowledge of TCP/IP*
    - *No more /24s!*
    - *More experienced engineer to do subnetting*
    - *Tracking used subnets is more complicated*
  - **Loss of public IPs due to subnetting**
    - *Network/broadcast addressing*
  - **Shows hops on traceroutes**
  - **Have to have Multiple DCHP Servers and/or DHCP Relays**
  - **Customers that move in-network**
    - *Public IP addresses may not be moved in some cases.*

Routing and Bridging

- **Before we PLAN it ----**
  - **Am I recommending all networks to go fully routed.**
    - *NO.*
  - **Am I telling you that if you have a bridged network it WILL FAIL**
    - *Not Necessary! There are many bridged networks that work!*
  - **Do I think you will have more issues with a bridged network vs. Routed?**
    - *Depending on the network, and what management practices you do. Yep!*
  - **Is there a number of customers before a fully bridged network will start to have issues?**
    - *There is nothing set in stone, but with no management, figure 300-500, with some management, I have seen networks go upwards of 1700+.*
  - **Is there a happy median between the two?**
    - *OF COURSE!*

THE PLAN

THE PLAN

1. Plan IP Addressing / Subnetting
2. Get the Right Hardware In the Field
3. Keep Network Running
4. Setup Routed Network
5. Plan Cutovers with Customers
6. Break Bridges

IP Planning

Bridged to Routed

- IP Addressing / Subnetting
  - What Addresses are going to go where on the network.
  - How are you going to hand out IP addresses?
  - How many IP addresses do you need per Tower? AP?
  - Create Subnet Plan
  - Create method for tracking Assigned Subnets and Assigned Ips

Bridged to Routed

- **PLAN**
  - **IP Addressing / Subnetting**
    - ***HOW TO SUBNET***

Subnetting Suggestions

- **PLAN**
  - **IP Addressing / Subnetting**
    - ***HOW TO SUBNET -*** *Subnet Per Access Point*
      - Limits broadcast domain to each Access Point
      - Complicated if there are many access points
        - One of our towers has 10 Access Points
        - 10 Subnets = 30 *Lost Public* IPs due to Subnetting!
        - 10 Subnets = 10 DHCP Servers
        - 10 Subnets = 10 routes in your Routing Table
        - Plus at least one more subnet for “routing” between Access Points

Subnetting Suggestions

- **PLAN**
  - **IP Addressing / Subnetting**
    - ***HOW TO SUBNET -*** *Subnet Per Tower*
      - Limits broadcast domain to each Tower
        - Broadcast domain still across All access points!
          - *Ability with MikroTik to Limit Broadcasts – Discussed later!*
      - Backhaul Data stays off backhauls unless needed
      - One larger subnet for all customers off tower
      - One DHCP / PPPoE Server
      - One Route for entire tower in routing table
      - Only loose 3 Ips for entire network

Subnetting Suggestions

- **PLAN**
  - **IP Addressing / Subnetting**
    - ***HOW TO SUBNET -*** *Subnet Per Tower*
      - Recommended this method along with separate VLANs for Access Points
        - *You will also need proper filtering to limit the size of your broadcast domain!*
      - APs will be bridged, out to CPE (but CPE Should be Routed/NATed)
      - Aps will be responsible for only the connections on them, routing not needed
      - Limits routing table to make it simpler
      - Simpler subnetting

The Right Hardware

The Right Hardware

- **PLAN**
  - **Get the Right Hardware in the Field**
    - *Ensure you have hardware at the sites to be able to do routed*
    - *Need Routers! Not Switches!*
      - RB493AH, other MTs
        - Bridge All interfaces, to make it into a smart switch
        - Label each interface based on what you plug into it
        - Backhauls should go directly into MT
        - APs should also if you have enough ports
          - If not, run VLANs to manageable switch. Each AP should be separated on its own VLAN

Example.. VLANs

Name	Type
bridge1	Bridge
ether1_BH	Ethernet
ether2_Ap1	Ethernet
ap1.vlan100 - mangement	VLAN
ap1.vlan101 - 2.4gig	VLAN
ap1.vlan102 - 5gig	VLAN
ap1.vlan103 - 900mhz	VLAN
ether3_Ap2	Ethernet
ap2.vlan100 - mangement	VLAN
ap2.vlan101 - 2.4 gig	VLAN
ap2.vlan102 - 5gig	VLAN
ap2.vlan103 -- 900mhz	VLAN

Keep the Network Running!

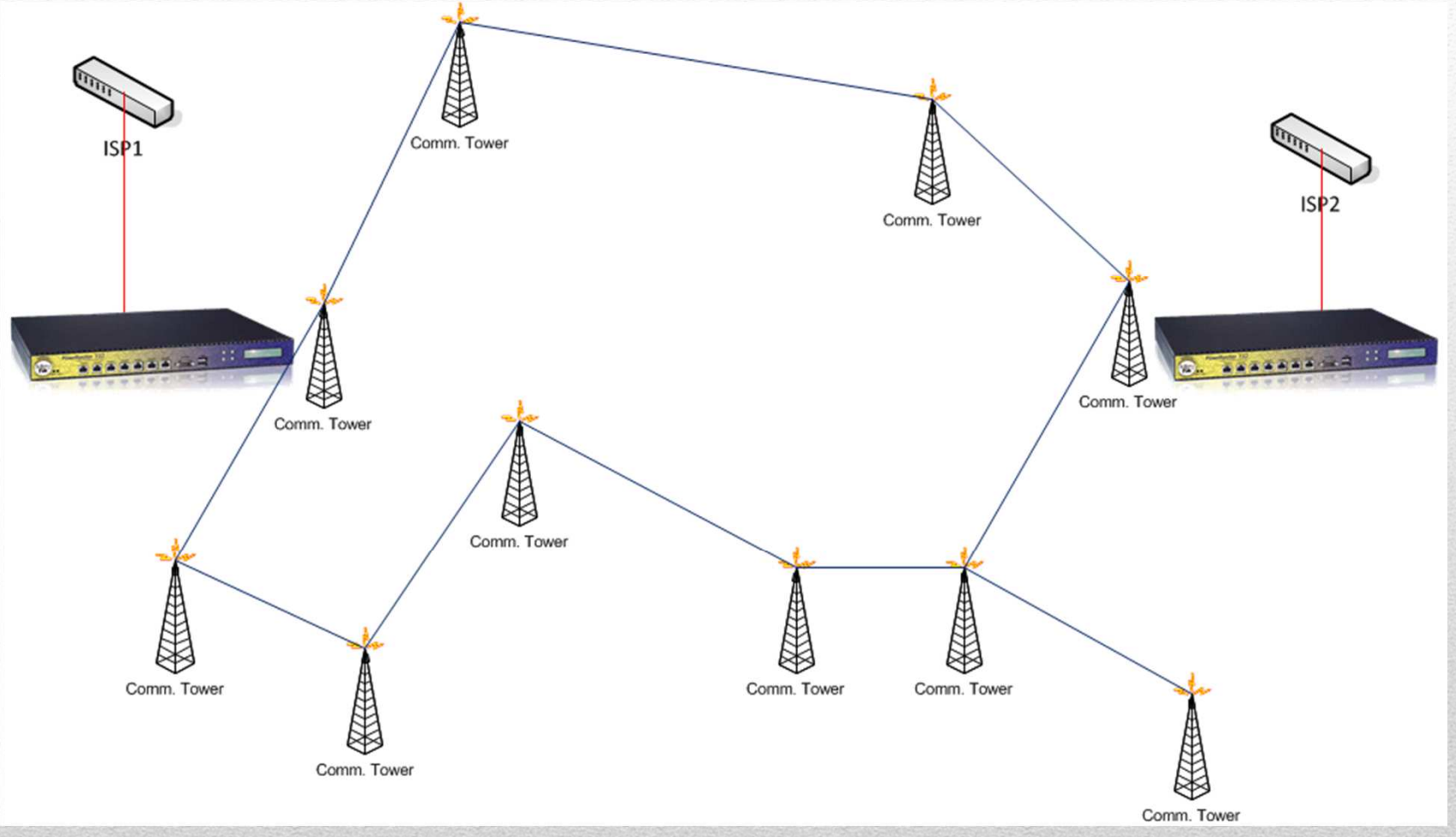
Keep the Network Running

- **Use your In-Place hardware to BLOCK data to and from unnecessary parts of your network.**
  - **AP -2- AP communications**
    - *If Traffic comes in vLAN100 (AP1) it should go out our backhaul!*
    - *We don't need to send ARP and Broadcast data to VLAN200 (AP2)*
    - *Use Bridging Filters to BLOCK traffic between VLANS*
      - This would include broadcasts and ARPs

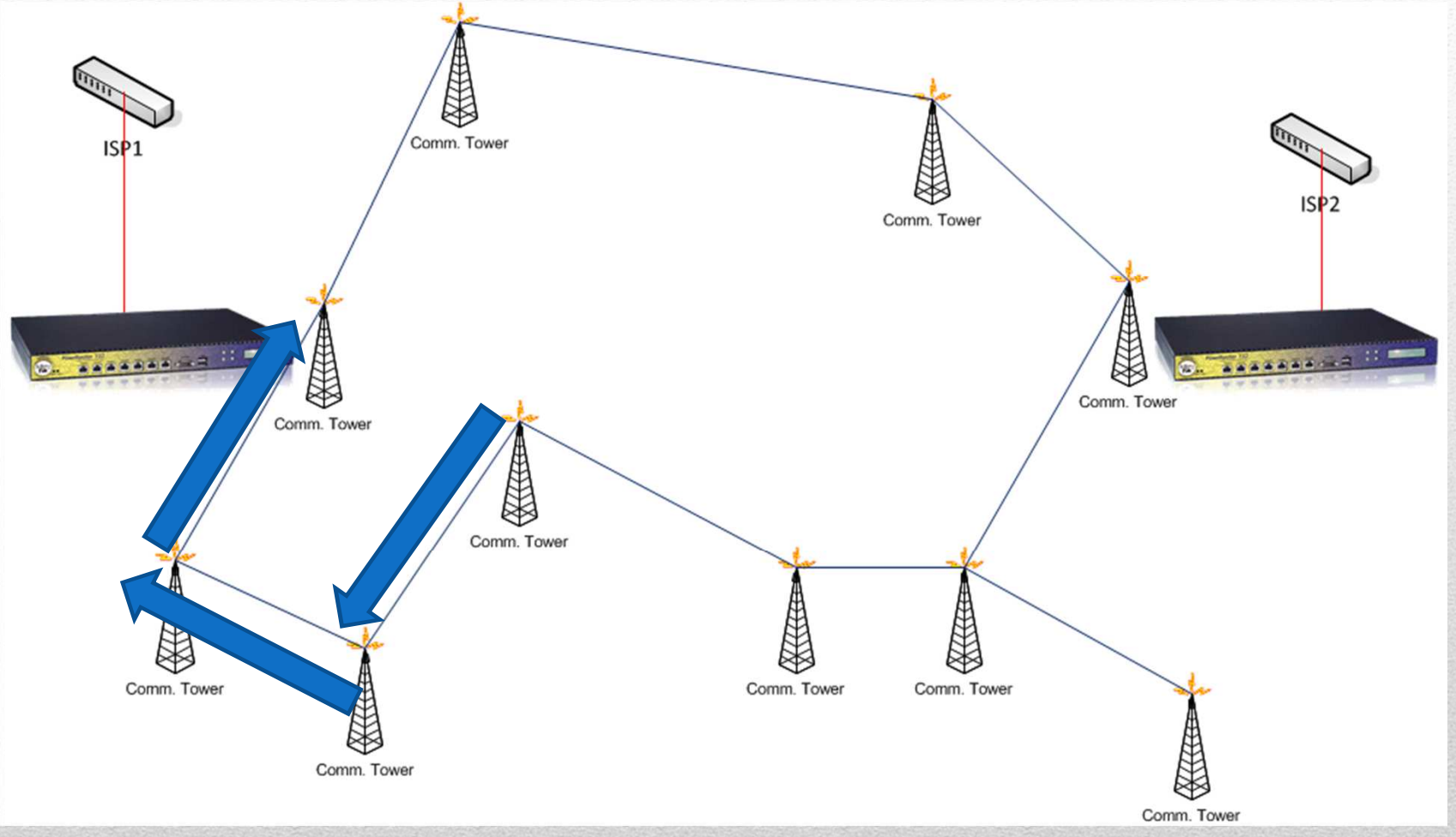
Keep the Network Running

- **Use your In-Place hardware to BLOCK data to and from unnecessary parts of your network.**
  - **AP -2- AP communications**
    - *Use filters to block traffic between multiple network SEGMENTS*
      - If you have 5 backhauls that go out from your main site, block traffic between each backhaul.
      - Most of your traffic should be going out your internet connection, not across your network
        - There are some cases where you can allow traffic across your network.

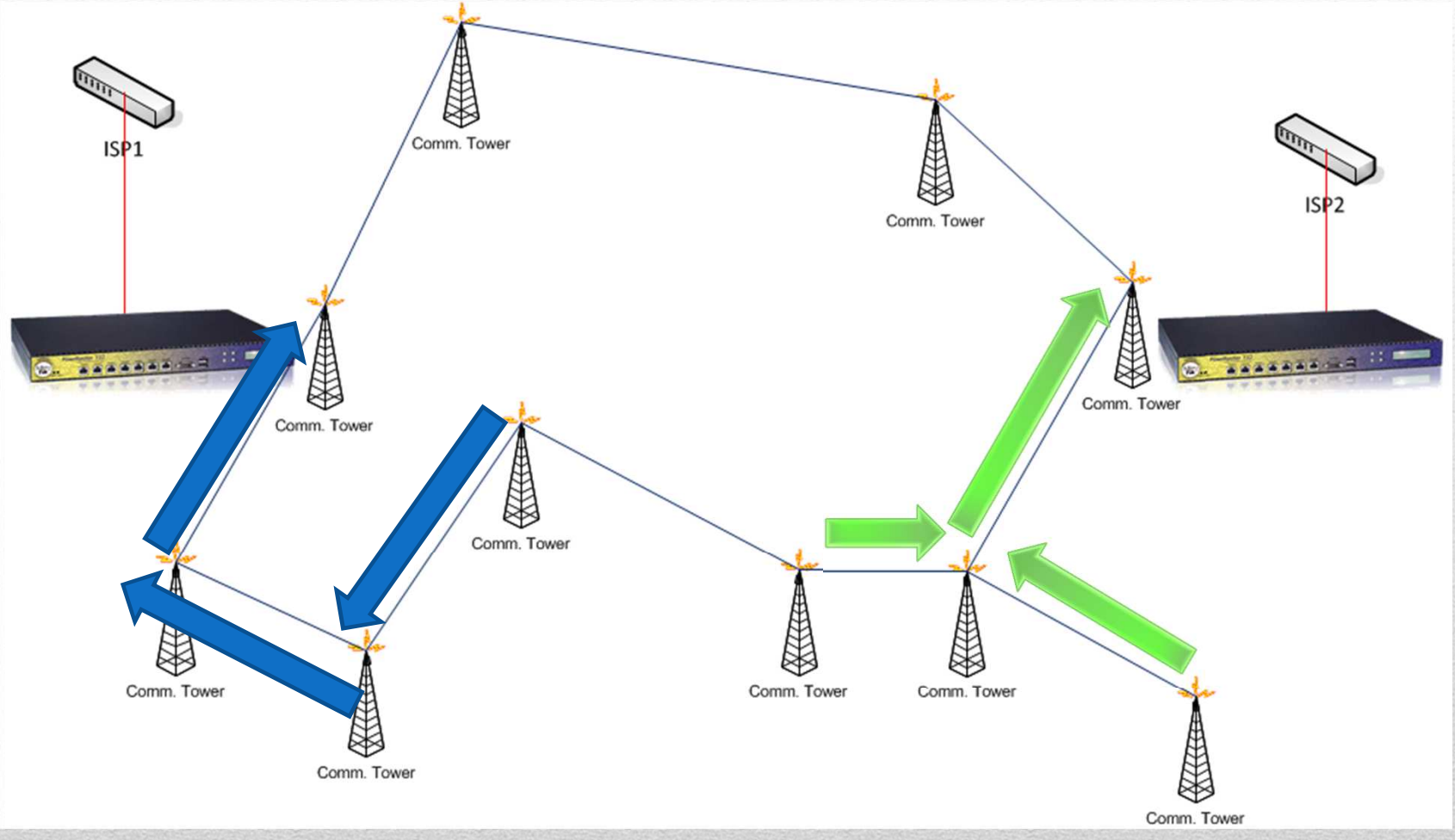
Limit the Broadcast Domain



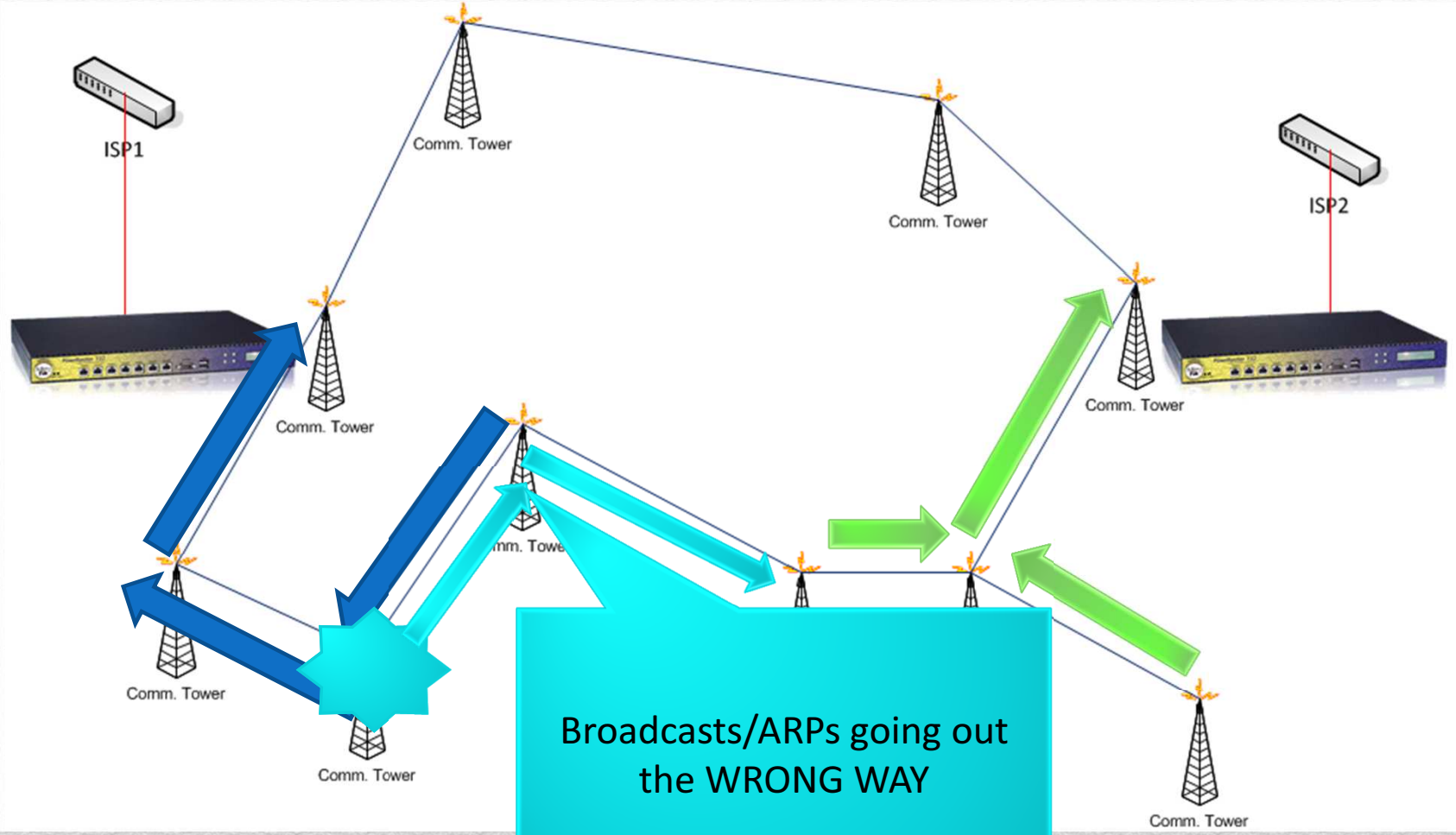
Limit the Broadcast Domain



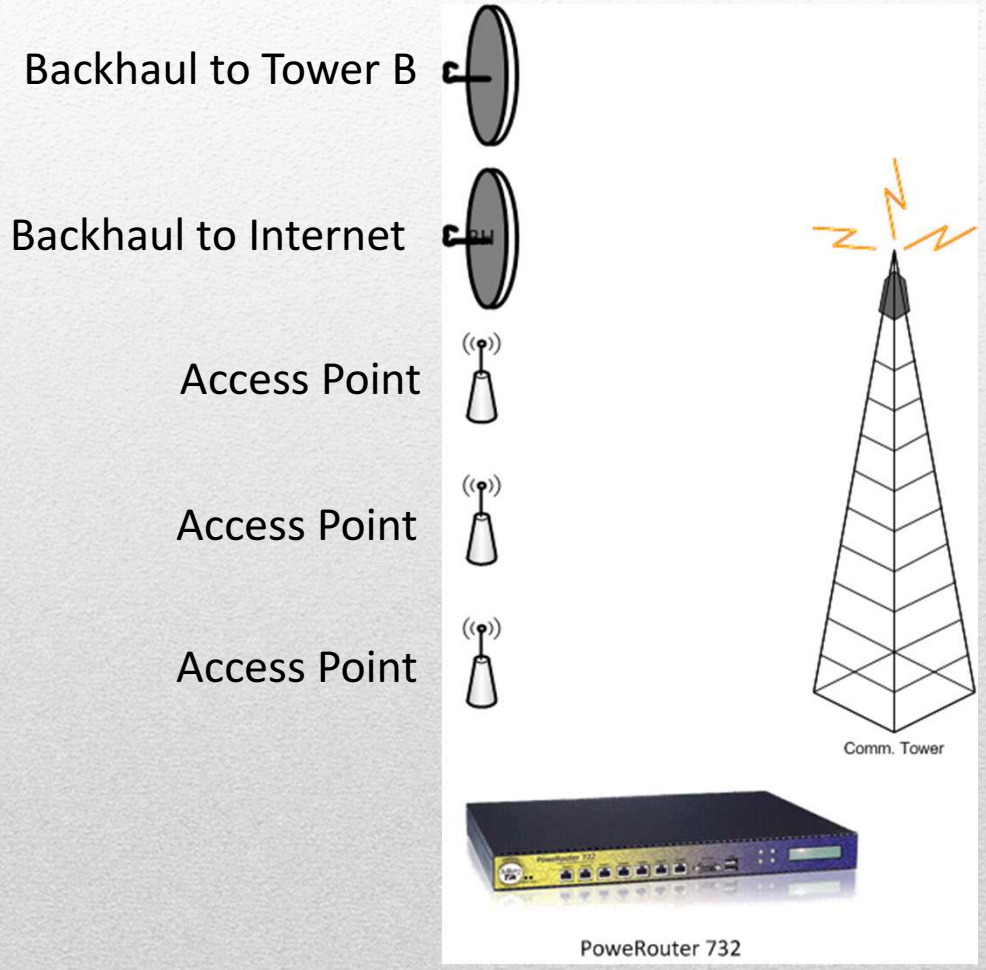
Limit the Broadcast Domain



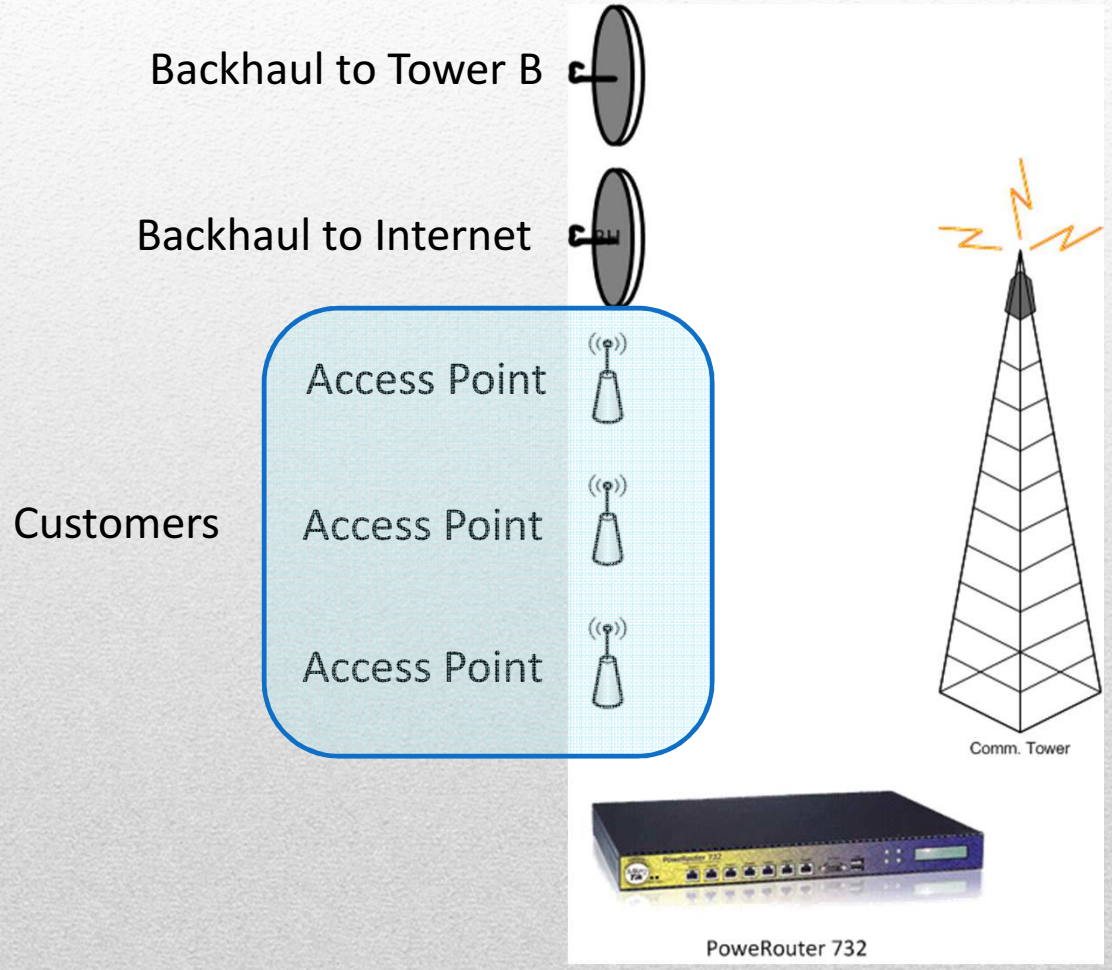
What We Do Not Want



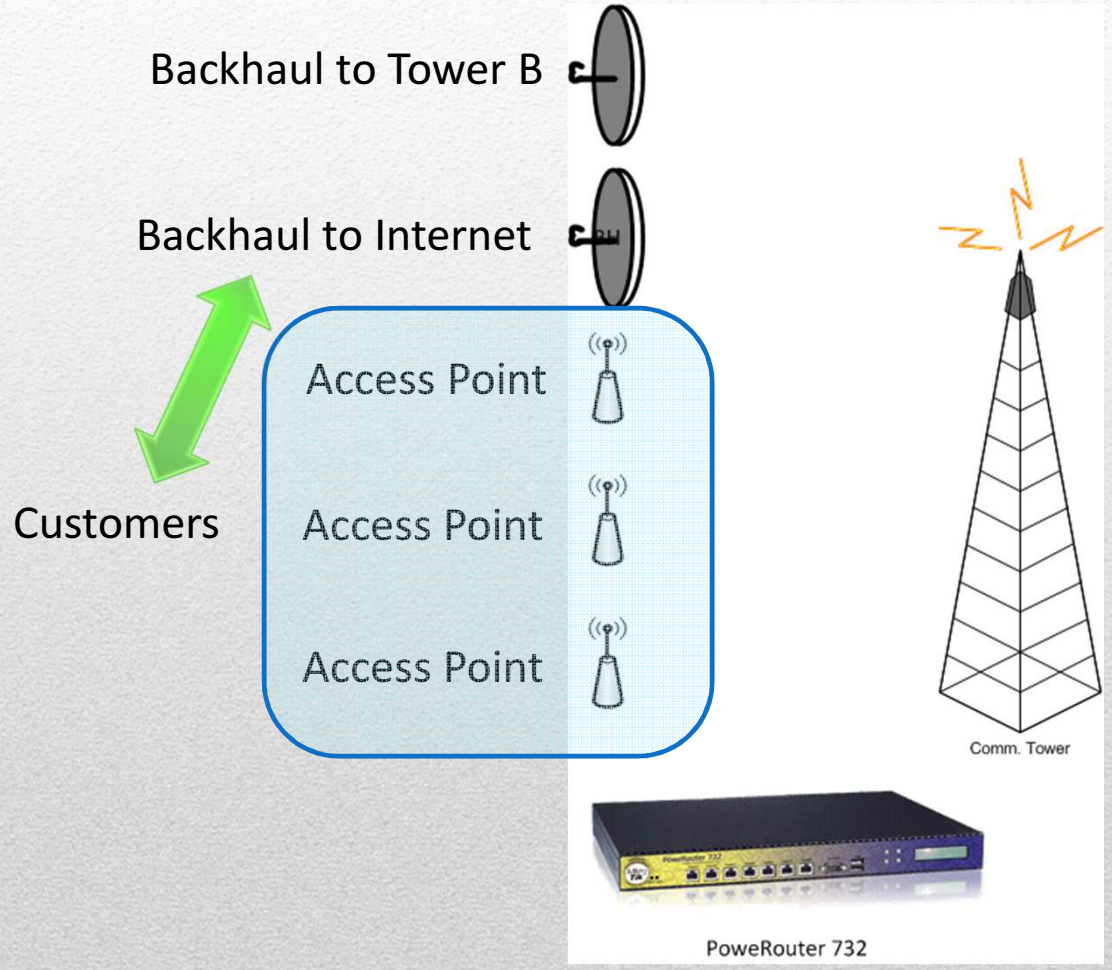
Tower View



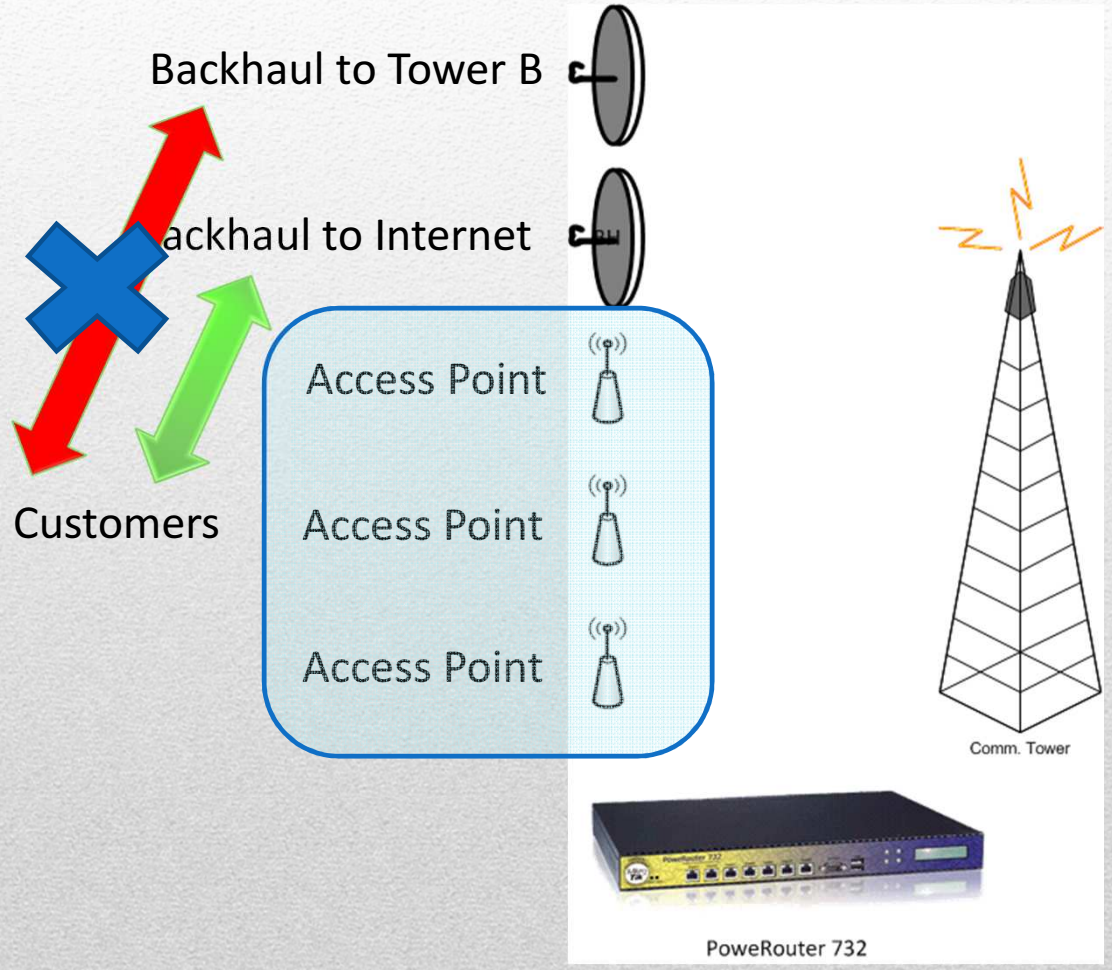
Tower View



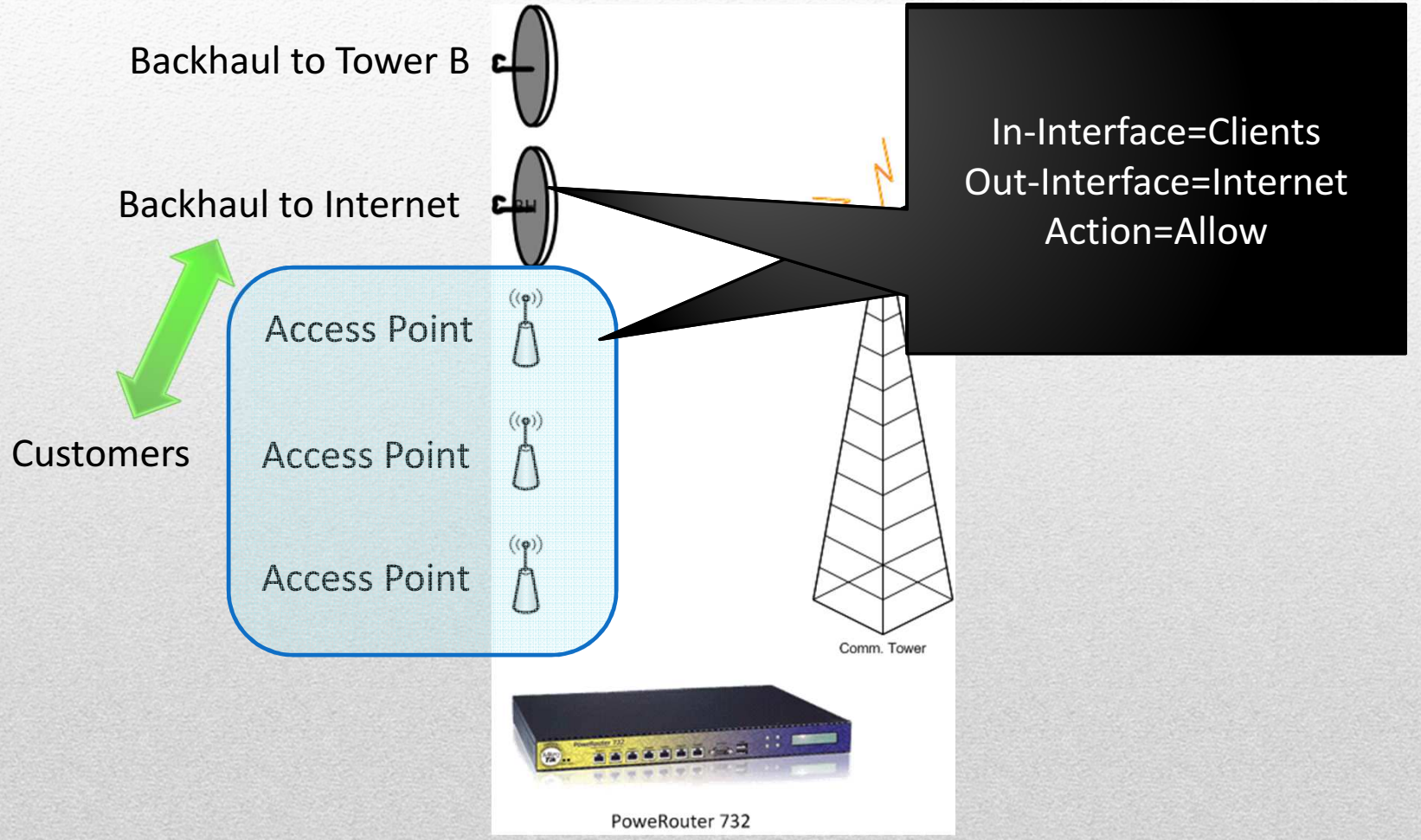
Tower View



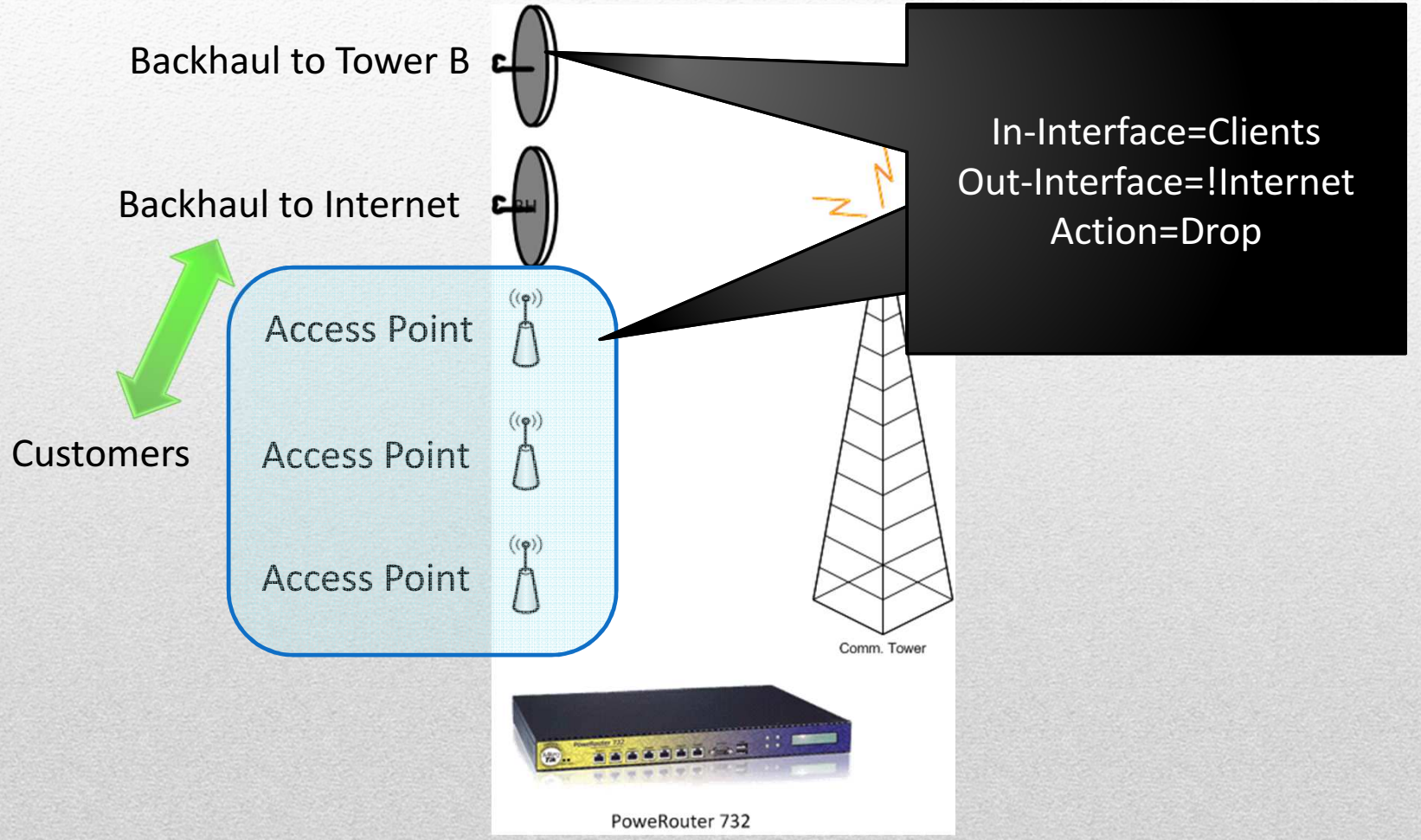
Tower View



Tower View



Tower View



Bridged to Routed

#		Chain	Interfaces/In. Interface	Interfaces/Out. Interface				Action
0		forward	ap1.vlan100 - mangement					accept
1		forward	ap2.vlan100 - mangement					accept
2		forward	ether1_BH					accept
3		forward		ether1_BH				accept
4		forward		ap1.vlan100 - mangement				accept
5		forward		ap2.vlan100 - mangement				accept
6		forward	ap1.vlan101 - 2.4gig					drop
7		forward	ap1.vlan102 - 5gig					drop
8		forward	ap1.vlan103 - 900mhz					drop
9		forward	ap2.vlan101 - 2.4 gig					drop
10		forward	ap2.vlan102 - 5gig					drop
11		forward	ap2.vlan103 -- 900mhz					drop

Bridged to Routed

#		Chain	Interfaces/In. Interface	Interfaces/Out. Interface				Action
0		forward	ap1.vlan100 - mangement					accept
1		forward	ap2.vlan100 - mangement					accept
2		forward	ether1_BH					accept
3		forward		ether1_BH				accept
4		forward		ap1.vlan100 - mangement				accept
5		forward		ap2.vlan100 - mangement				accept
6		forward	ap1.vlan101 - 2.4gig					drop
7		forward	ap1.vlan102 - 5gig					drop
8		forward	ap1.vlan103 - 900mhz					drop
9		forward	ap2.vlan101 - 2.4 gig					drop
10		forward	ap2.vlan102 - 5gig					drop
11		forward	ap2.vlan103 -- 900mhz					drop

Accept data to and from our Management & Internet
Drop data that is not going to or from our Management & Internet

Bridged to Routed

#		Chain	Interfaces/In. Interface	Interfaces/Out. Interface				Action
0		forward	ap1.vlan100 - mangement					accept
1		forward	ap2.vlan100 - mangement					accept
2		forward	ether1_BH					accept
3		forward		ether1_BH				accept
4		forward		ap1.vlan100 - mangement				accept
5		forward		ap2.vlan100 - mangement				accept
6		forward	ap1.vlan101 - 2.4gig					drop
7		forward	ap1.vlan102 - 5gig					drop
8		forward	ap1.vlan103 - 900mhz					drop
9		forward	ap2.vlan101 - 2.4 gig					drop
10		forward	ap2.vlan102 - 5gig					drop
11		forward	ap2.vlan103 -- 900mhz					drop

There are multiple ways of filtering! This is just one example.

Setup the Routed Network

Setting up the Routed Network

- **IP Addressing Informational Requirements**
  - **What IPs ARE currently used**
    - *Do we have enough subnets to "route" or all they all used?*
  - **Who is using them**
    - *This should already be known, as a IP spreadsheet or other IP Tracking application should be used.*
  - **WHERE are they at!**
    - *Knowing where your customer base is at is important.*
    - *We need to know how many IP addresses per tower, or AP, we will need in the new routed network*

Setting up the Routed Network

- **Currently in this network**
  - **Using two /24s, one from each provider.**
    - *These subnets can't be used for our conversion!*
  - **Contact Providers**
    - *Can we get two new /24s ROUTED to us. One from each provider.*
      - This means that the providers router, has a subnet, say 12.1.1.0/24 ROUTED to our routers IP.
      - Not a /24 on providers router!
    - *It is common to use MORE IP space than before.*
      - Ex. If you are currently using up most of two /24s, its possible that you will need 3 or even 4 /24s to subnet out.
      - IP addresses will be on towers that will be unused. Its possible for you to have 10-20 IPs, if not more, on each tower unused.

Setup Routed Network

- Setup Proper IP subnets on bridged Interfaces
- Setup Proper IP Subnets on backhauls
- Reprogram backhaul and Access Points to new subnets
- Setup proper IP Dynamic Routing Protocols.
- Setup DHCP on interfaces – if you are using DHCP

Customer Cutovers

Customer Cutovers

- **Plan Cutovers if necessary with Customers**
  - **Since you are running both Bridged and routing**
    - *Most customers can simply change their IP and it will work*
  - **Are there customers with public services?**
    - *EX. Web Servers, Mail Servers*
    - *These typically will take priority.*
    - *Changes in IP addressing may require them to change DNS information!*
    - *Prior to breaking the bridges!*

Customer Cutovers

- **Plan Cutovers if necessary with Customers**
  - **Since you are running both Bridged and routing**
    - *DHCP Customers*
      - Setup original DHCP Server to a small lease time, say 1 hour
      - Setup new DHCP Server on bridge group. Leave off
      - At night, break bridge between towers and backhauls, enable DHCP Server. Clients will be offline at most 1 hour before they get their new IP!
        - Depending on Your CPE, you may be able to force a new IP.
    - *Once all customers are off the old IP addresses, remove backhauls from bridge group!*
    - *Start at furthest from internet access.*

Break Bridges

Bridge Breaking

- **DHCP**
  - **Don’t forget DHCP does NOT work until you break your bridges!**
- **Start removing bridges**
  - **Verify access to the new subnet**
  - **Keep moving forward**
- **Verify / Repeat**
  - **Once you verify your new subnet is working repeat the process on your network**
  - **Eventually you won’t have any bridged network segments**
  - **Some customers want the lower latency for their backhauls, so they leave their bridges in for the backhaul network**
    - *All customer Access Points are routed though*
    - *No Direct access to backbone*

Recap

Recap

- **My Recommendations**
  - **Keep Customers off your backbone!**
  - **Keep Customers off your Access Points!**
  - **Route Backbone for best path**
  - **Remember VLANs do not break up Broadcast domains!**
    - *Only VLANS with proper firewalling will!*
    - *VLANs running across entire network does not help*

Your Presenter

- Dennis Burgess

Link Technologies, Inc.

- Contact Information
  - http://www.linktechs.net
  - support@linktechs.net
  - Office: 314-735-0270

- "Learn RouterOS" Book
  - www.routerosbook.com