About Me

- Steve Discher, from College Station, Texas, USA
- Class of '87 Texas A&M University, home of Heisman winner Johnny Football
- MikroTik Certified Trainer and teach RouterOS classes, LearnMikroTIk.com and MyWISPTraining.com
- Operate a wireless distribution company, ISPSupplies.com

Common Mistakes

RouterOS - Common Mistakes and Simple Solutions

RouterOS Configuration Tool Update And First Release

Common Errors

1. New router, fresh out of the box, can't connect to the router on ether1.
2. Changes made with MAC Winbox are lost, constant disconnects.
3. Accidentally creating an open DNS server.
4. Accidentally creating an open web proxy.
5. Not disabling default forwarding on wireless interface.
6. Leaving "wireless protocol" set to "any" or "unsupported" on an AP.

Can't Connect on Ether1

PROBLEM: New router, POE input is typically on ether1 connect a laptop and you can't connect through MAC Winbox or through the default IP address.

Can't Connect on Ether1

SOLUTION: Since the default firewall blocks access to ether1 and disables discovery by Winbox, use a different port to connect, ether2, ether3 etc.

① Can't Connect on Ether1

Default Firewall Rules

```
/ip firewall filter
add chain=input comment="default configuration" protocol=icmp
add chain=input comment="default configuration" connection-state=established
add chain=input comment="default configuration" connection-state=related
add action=drop chain=input comment="default configuration" in-interface=\
    ether1-gateway
add chain=forward comment="default configuration" connection-state=\
    established
add chain=forward comment="default configuration" connection-state=related
add action=drop chain=forward comment="default configuration" \
    connection-state=invalid
```

① Can't Connect on Ether1

Default - IP Neighbors Disabled on ether1

```
[admin@MikroTik] /ip neighbor discovery> pr
Flags: X - disabled
 #    NAME
 0 X  ether1-gateway
 1    ether2-master-local
 2    ether3-slave-local
 3    ether4-slave-local
 4    ether5-slave-local
```

Can't Connect on Ether1

Learn more about the default configurations for each model at http://wiki.mikrotik.com/wiki/Manual:Default_Configurations

② Changes made with MAC Winbox are lost, constant disconnects

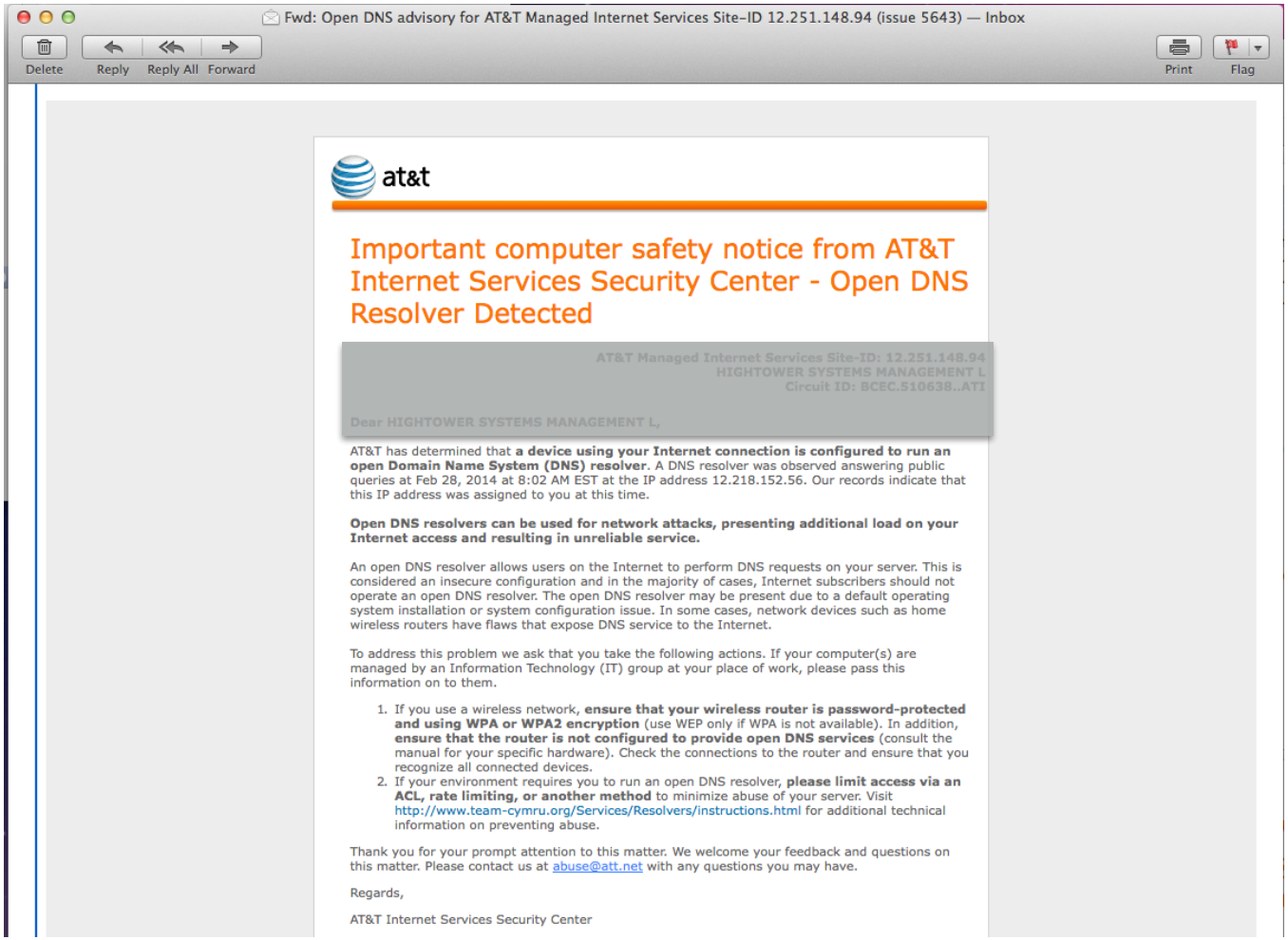
PROBLEM: Connect with MAC Winbox, make change to configuration and you get disconnected or changes don't seem to save.

② Changes made with MAC Winbox are lost, constant disconnects

SOLUTION: Only use MAC Winbox to get an IP configured on the device, then connect via the IP address for all extended configurations.

Disconnects? Check your PC's MTU size.

③Accidentally Create an Open DNS Server



Fwd: Open DNS advisory for AT&T Managed Internet Services Site-ID 12.251.148.94 (issue 5643) — Inbox

Delete Reply Reply All Forward Print Flag

at&t

Important computer safety notice from AT&T Internet Services Security Center - Open DNS Resolver Detected

AT&T Managed Internet Services Site-ID: 12.251.148.94
HIGHTOWER SYSTEMS MANAGEMENT L
Circuit ID: BCEC.510638..ATI

Dear HIGHTOWER SYSTEMS MANAGEMENT L,

AT&T has determined that **a device using your Internet connection is configured to run an open Domain Name System (DNS) resolver**. A DNS resolver was observed answering public queries at Feb 28, 2014 at 8:02 AM EST at the IP address 12.218.152.56. Our records indicate that this IP address was assigned to you at this time.

Open DNS resolvers can be used for network attacks, presenting additional load on your Internet access and resulting in unreliable service.

An open DNS resolver allows users on the Internet to perform DNS requests on your server. This is considered an insecure configuration and in the majority of cases, Internet subscribers should not operate an open DNS resolver. The open DNS resolver may be present due to a default operating system installation or system configuration issue. In some cases, network devices such as home wireless routers have flaws that expose DNS service to the Internet.

To address this problem we ask that you take the following actions. If your computer(s) are managed by an Information Technology (IT) group at your place of work, please pass this information on to them.

1. If you use a wireless network, **ensure that your wireless router is password-protected and using WPA or WPA2 encryption** (use WEP only if WPA is not available). In addition, **ensure that the router is not configured to provide open DNS services** (consult the manual for your specific hardware). Check the connections to the router and ensure that you recognize all connected devices.
2. If your environment requires you to run an open DNS resolver, **please limit access via an ACL, rate limiting, or another method** to minimize abuse of your server. Visit http://www.team-cymru.org/Services/Resolvers/instructions.html for additional technical information on preventing abuse.

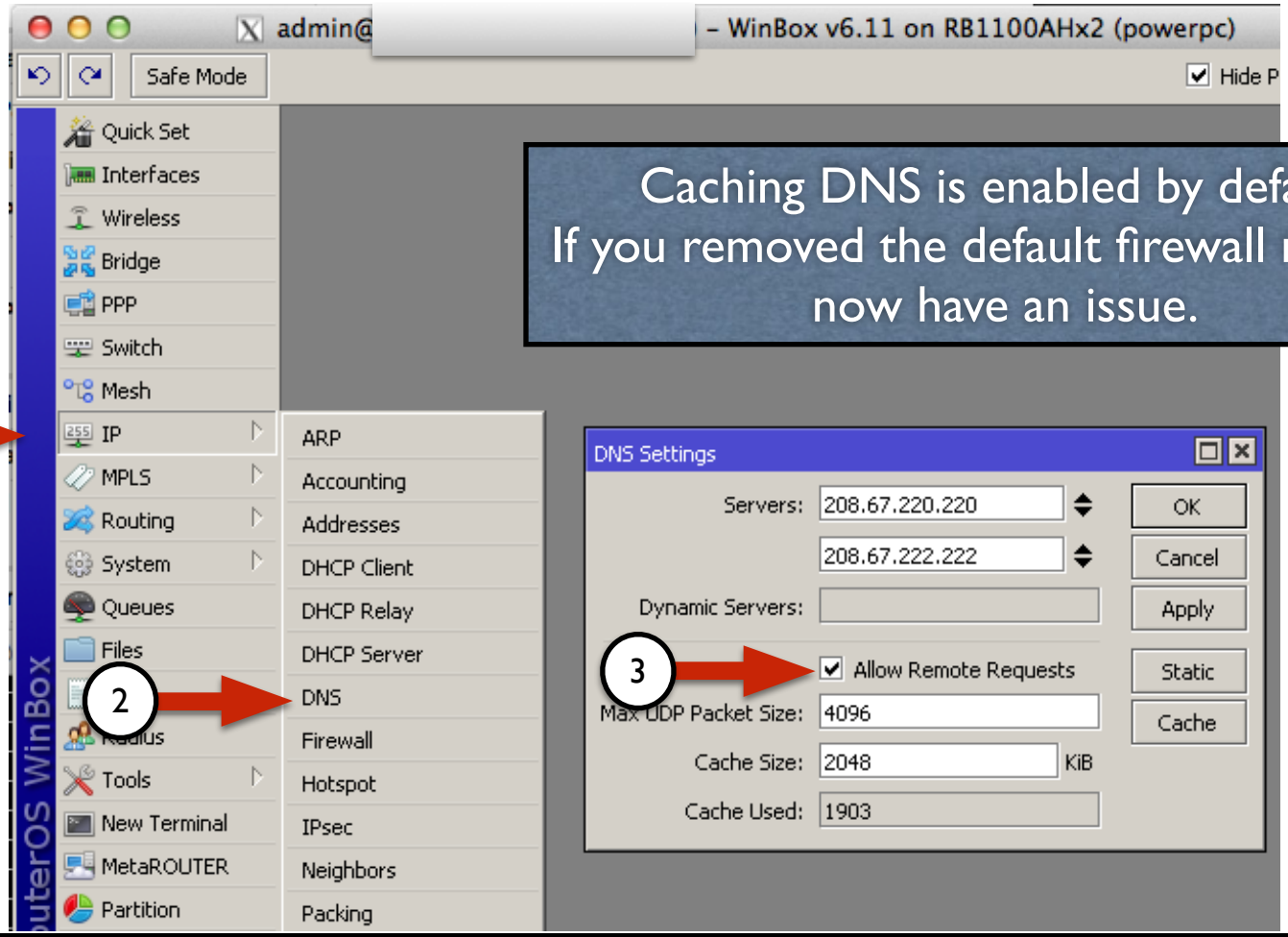
Thank you for your prompt attention to this matter. We welcome your feedback and questions on this matter. Please contact us at abuse@att.net with any questions you may have.

Regards,

AT&T Internet Services Security Center

3

Caching DNS in RouterOS



③ Threat of Open DNS Servers

- Open DNS servers can be used to launch Distributed Denial of Service (DDoS) attacks
- Using spoofed DNS requests a malicious attacker sends several thousand spoofed requests to a DNS server.
- The DNS server processes these requests as valid and then returns the DNS replies to the spoofed recipient (i.e., the victim). When the number of requests is in the thousands, the attacker could potentially generate a multi-gigabit flood of DNS replies.

3

Caching DNS in RouterOS

Less Specific

SOLUTION: Create a firewall rule to block everything on the WAN port or specifically to block port 53 UDP and TCP

```
/ip firewall filter

add action=drop chain=input comment="default configuration" in-interface=\
    ether1-gateway
```

3

Caching DNS in RouterOS

More Specific

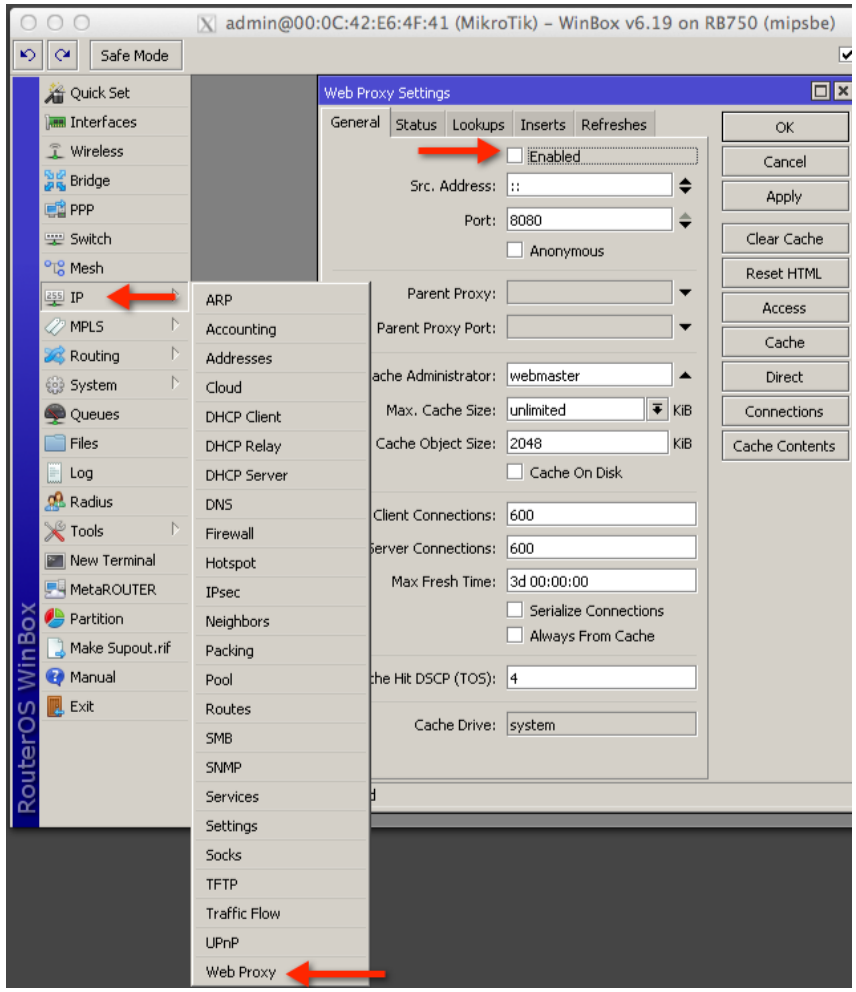
SOLUTION: Create a firewall rule to block everything on the WAN port or specifically to block port 53 UDP and TCP.

```
/ip firewall filter

add chain=input protocol=tcp dst-port=53 in-interface=ether1-gateway
action=drop

add chain=input protocol=udp dst-port=53 in-interface=ether1-gateway
action=drop
```

④ Forgetting a Firewall Rule for Web Proxy

- Web proxy can speed up web browsing by caching pages in the router's memory or on disk
- Subsequent requests to the same URL can be served from cache instead of using the internet connection
- Also provides http firewalling, blocking or redirecting certain sites based on regex rules

④ Forgetting a Firewall Rule for Web Proxy



PROBLEM: Open proxy.

- Enabling is simple, one check box
- Once enabled, the proxy is available from all interfaces
- Can AND WILL be used for many illegal activities to conceal the hacker's identity

④ Forgetting a Firewall Rule for Web Proxy

- SOLUTION: Create a firewall rule to protect your proxy. This can be less specific or more specific depending on the application.

4

Forgetting a Firewall Rule for Web Proxy

Less Specific

SOLUTION: Create a firewall rule to protect your proxy. This can be less specific or more specific depending on the application.

```
/ip firewall filter

add action=drop chain=input comment="default configuration" in-interface=\
    ether1-gateway
```

4

Forgetting a Firewall Rule for Web Proxy

More Specific

SOLUTION: Create a firewall rule to protect your proxy. This can be less specific or more specific depending on the application.

```
/ip firewall filter

add action=drop chain=input protocol=tcp dst-port=8080 in-interface=\
    ether1-gateway
```

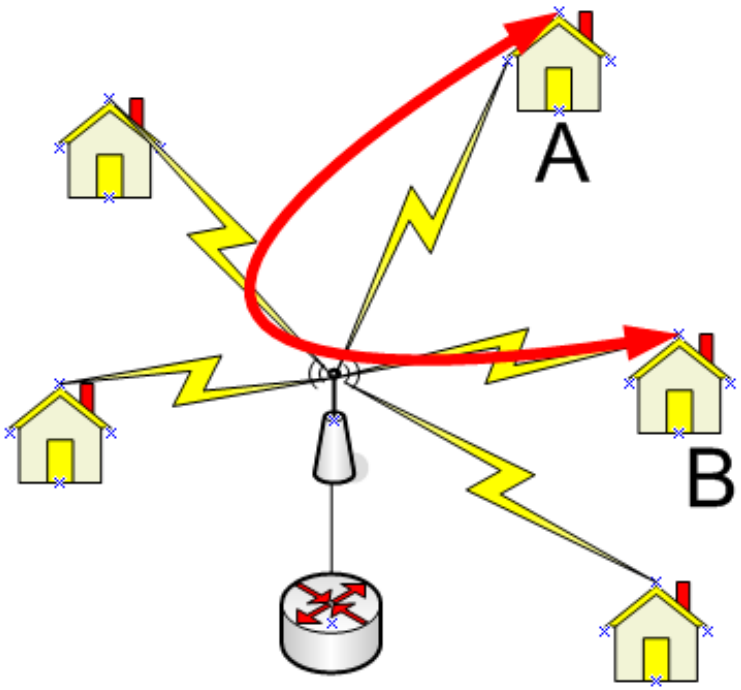
5

Not Disabling "Default Forwarding" on Wireless Interface

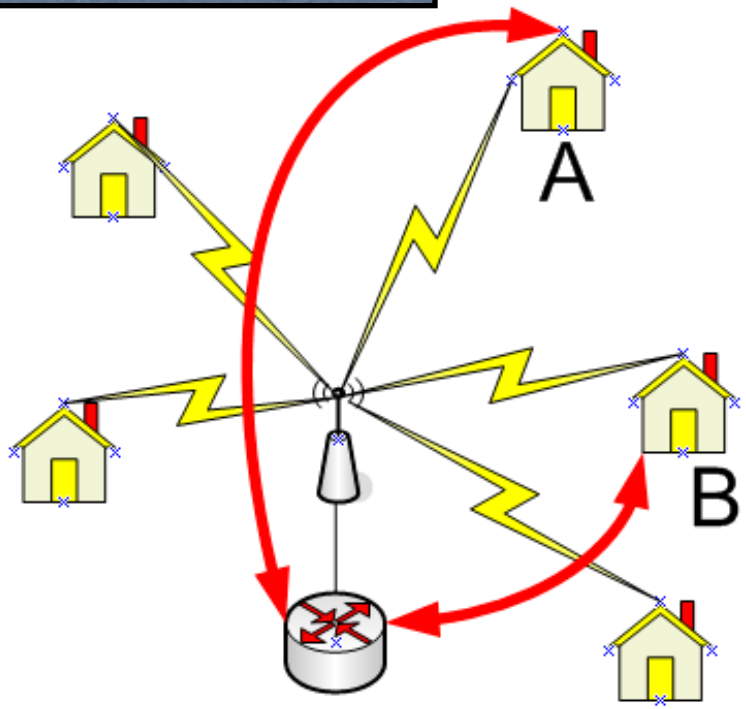
PROBLEM: By default, "Default Forwarding" is enabled on all wireless interfaces. In a WISP scenario this can allow subscribers on one AP (same wlan) to pass traffic freely between themselves and consume all your resources.

Not Disabling "Default Forwarding" on Wireless Interface

With Default Forwarding disabled, traffic passes through router and Firewall/NAT



Default: Forwarding Enabled



Forwarding Disabled

5

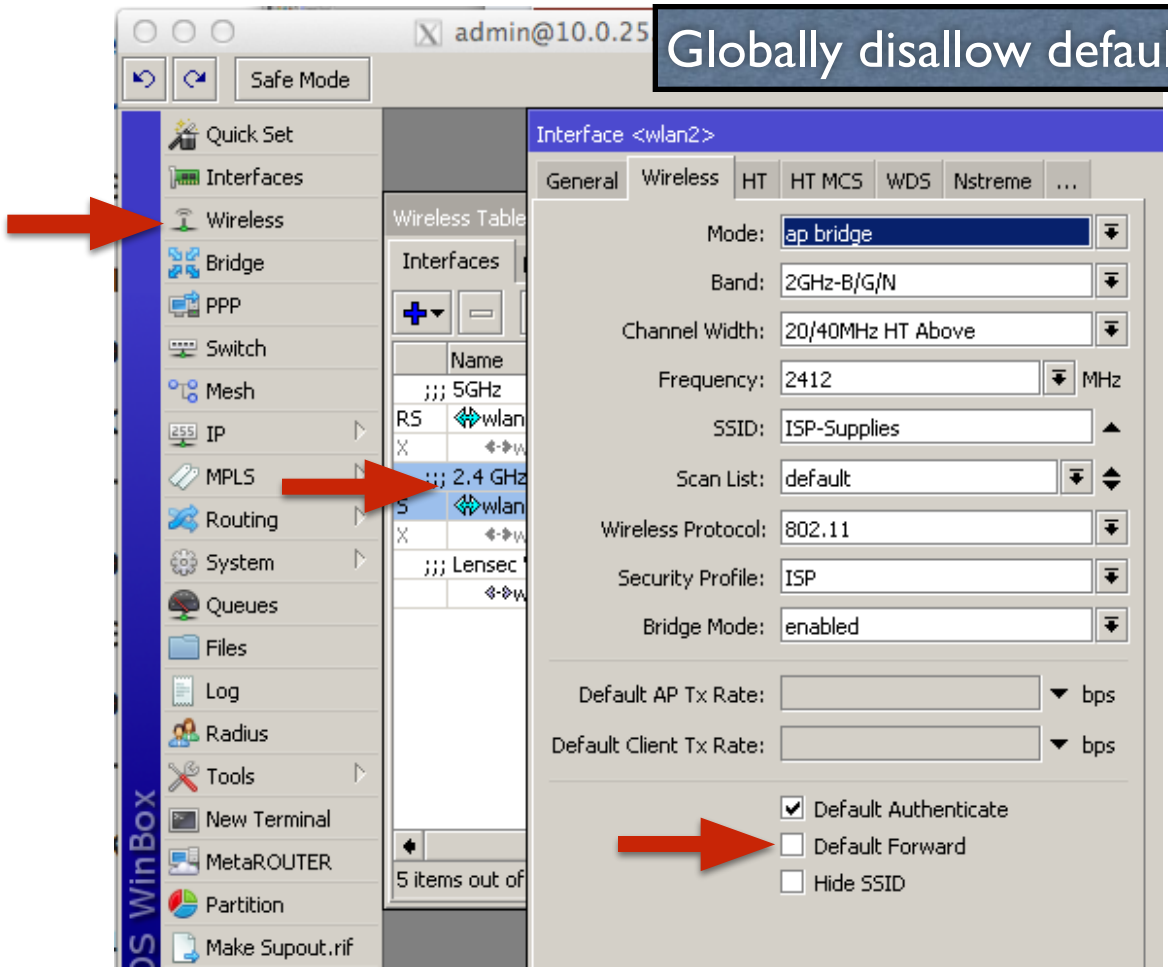
Not Disabling "Default Forwarding" on Wireless Interface

SOLUTION: Disable "Default Forwarding" globally on the interface or specifically on a per station basis using Access List entries.

5

Not Disabling "Default Forwarding" on Wireless Interface

Less Specific

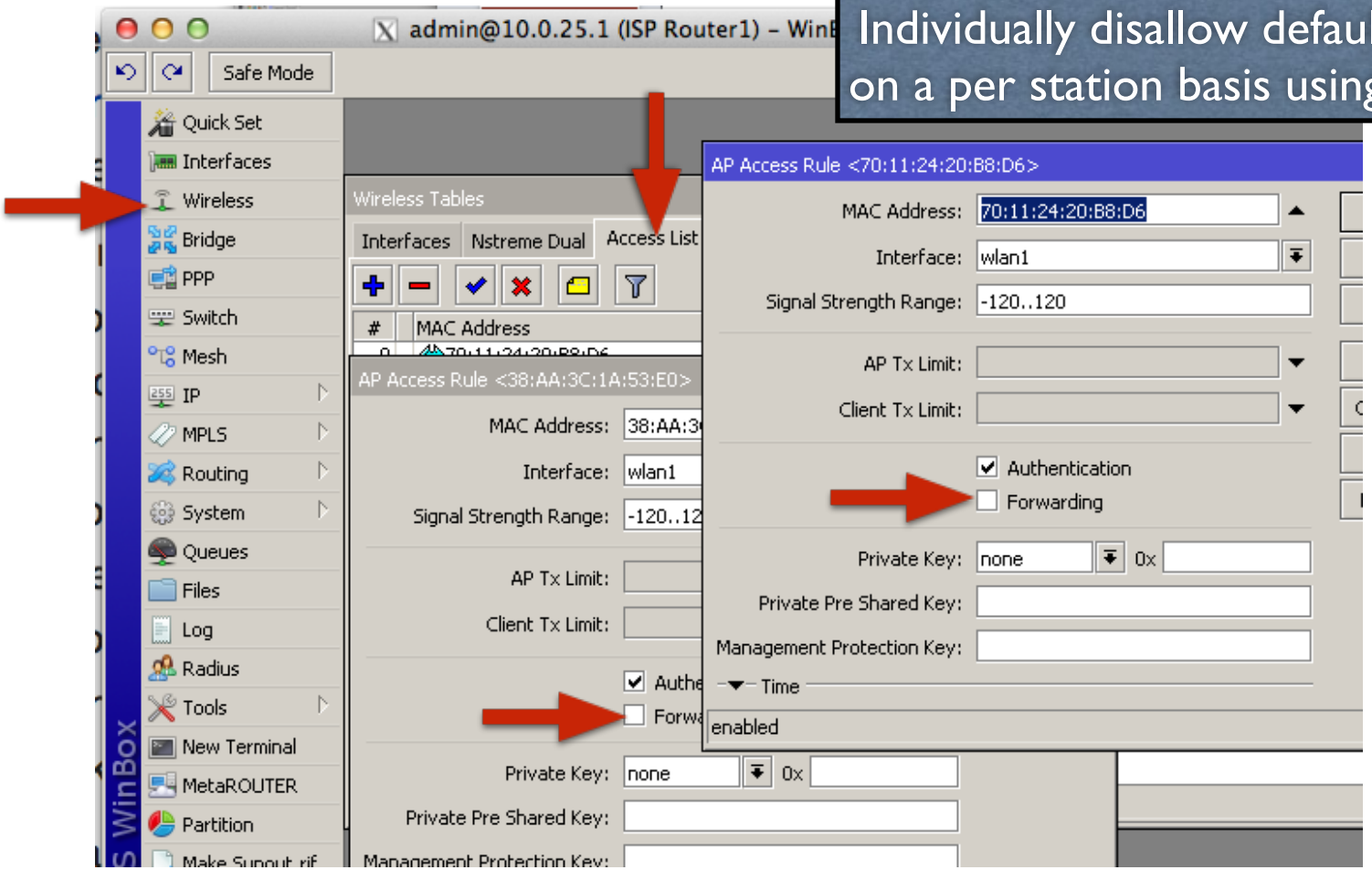


5

More Specific

Not Disabling "Default Forwarding" on Wireless Interface

Individually disallow default forwarding on a per station basis using Access Lists



6 Leaving Wireless Protocol set to Unspecified or Any on an AP

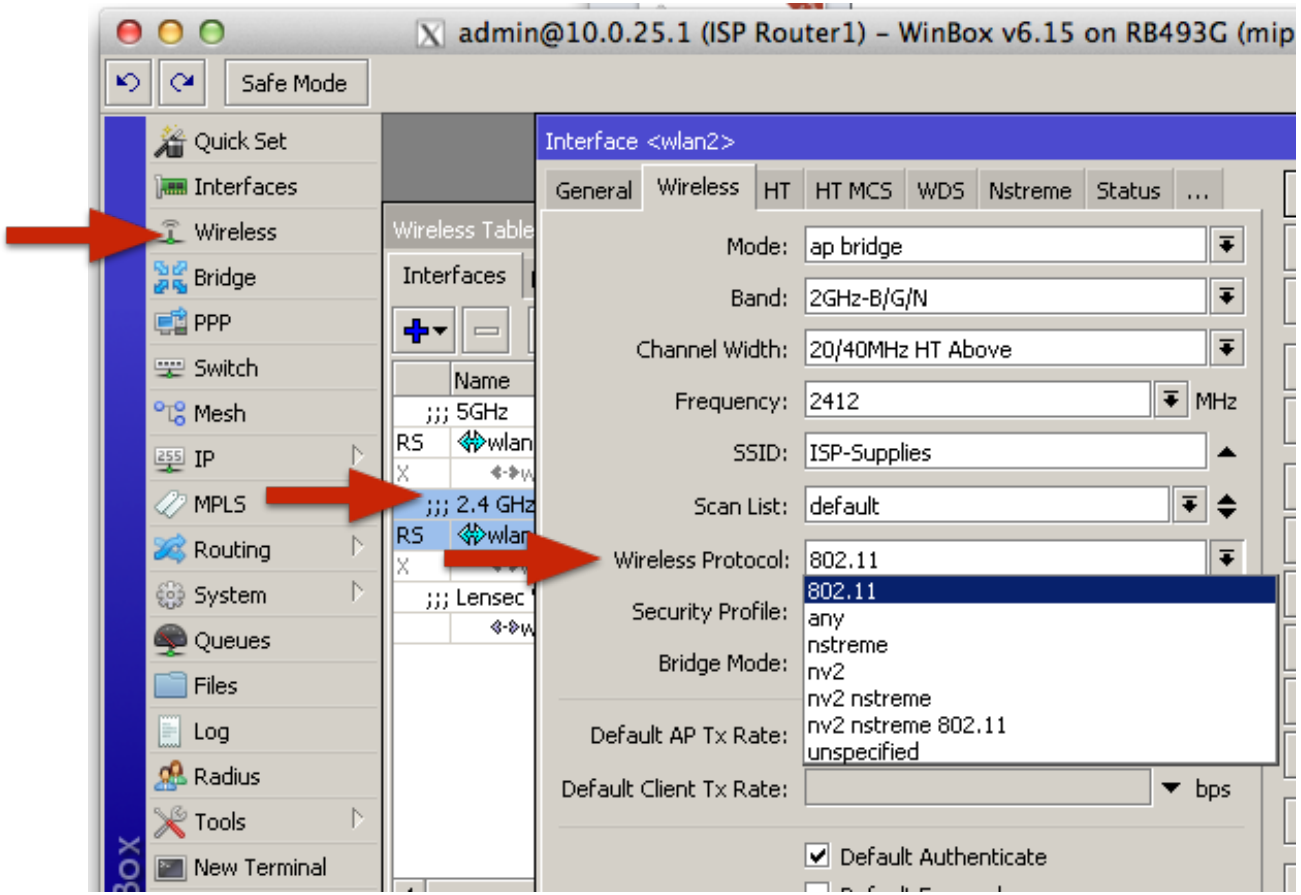
PROBLEM: Default setting for "Wireless Protocol" on a wireless interface is "unspecified". Many users believe this means AP will support any client, 802.11, NV2, etc.

Leaving Wireless Protocol to "Unspecified" or "Any" on an AP

SOLUTION: Always select a wireless protocol on the AP since the AP determines the protocol.

6

Leaving Wireless Protocol to "Unspecified" or "Any" on an AP



Leaving Wireless Protocol to Unspecified or Any on an AP

- unspecified - protocol mode used on previous RouterOS versions (v3.x, v4.x). Nstreme is enabled by old enable-nstreme setting, Nv2 configuration is not possible.
- any : on AP - regular 802.11 Access Point
- nstreme - enables Nstreme protocol (the same as old enable-nstreme setting).
- nv2 - enables Nv2 protocol.
- nv2 nstreme : on AP - uses first wireless-protocol setting, always Nv2
- nv2 nstreme 802.11 - on AP - uses first wireless-protocol setting, always Nv2

http://wiki.mikrotik.com/wiki/Manual:Interface/Wireless

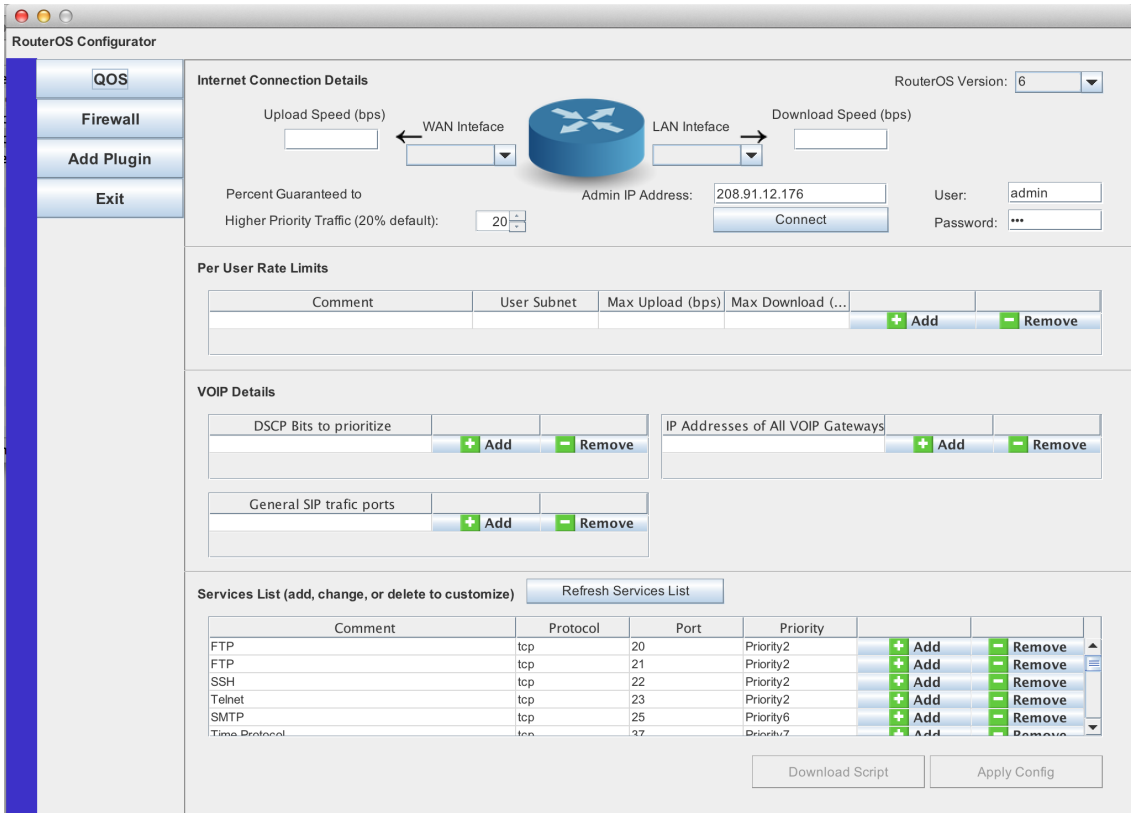
Common Errors

1. New router, fresh out of the box, can't connect to the router on ether1.
2. Changes made with MAC Winbox are lost, constant disconnects.
3. Accidentally creating an open DNS server.
4. Accidentally creating an open web proxy.
5. Not disabling default forwarding on the wireless interface.
6. Leaving "wireless protocol" set to "any" or "unsupported".

RouterOS Configuration Tool Update And First Release

MikroTik Configuration Tool

- First showed this at the 2013 MUM in St. Louis
- First version in Java and, test group
- Feedback:
  - Wanted it to be free
  - Free
  - No charge
  - Wanted it to be web based



MikroTik Configuration Tool

- So far we have developed three apps, all web based
  - Address list tool
  - Firewall tool
  - QOS tool

Address List Tool

- Allow you to create an address list based on IP blocks assigned to countries
- With the tool, you select the countries you want to include in your list and then download the list
- With the list you can write firewall rules to block these countries, only allow these countries, etc.

Firewall Tool

- Creates a basic state-full firewall
- Assumes the LAN interface is secure and the WAN interface is insecure
- Not a "one size fits all" solution but adequate for most internet routers for home, office, etc.
- Two flavors:
  - Masqueraded firewall (Private IP's on LAN, Public on WAN)
  - Public IP firewall (Public on LAN and WAN)
  - Both have the ability to block countries from the Country IP Block address tool

QOS Tool

- Again, not a one size fits all approach
- Basic QOS setup for common services like VOIP
- Ability to add your own protocols/ports or alter the default priorities

Demo

Questions?

Thank You!

- MyWISPTraining.com
- LearnMikroTik.com
- ISPSupplies.com
- Blog.ISPSupplies.com
- "RouterOS by Example" available from distributors, Amazon.com, Kindle, iTunes
- http://MikroTikConfig.com

Next training is MTCNA/MTCRE October 6-9 Columbus, Ohio