GregSowell.com
MikrotikUniversity.com

Greg Sowell Consulting

Rogue Access Point Detectoin and Mitigation
MUM 2011

GregSowell.com
MikrotikUniversity.com

Define Rogue Access Point

- A rogue in this instance is any access point connected to your network without permission.

GregSowell.com
MikrotikUniversity.com

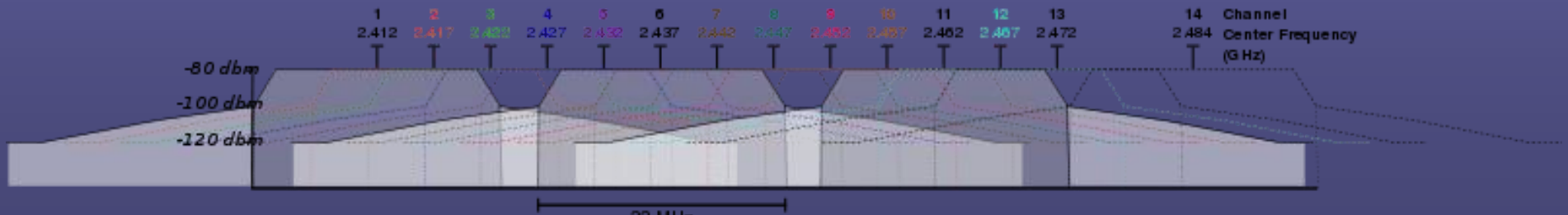
Why Should I Care?

- Limited 802.11spectrum.
- Man in the middle attacks/information theft.
- Because they didn’t say please.

GregSowell.com
MikrotikUniversity.com

Limited Spectrum

- 802.11b has only 3 non-overlapping channels.
- 2400Mhz – 2483Mhz
  - 22Mhz channels
  - 22 * 3 = 66Mhz for transmissions
  - 4Mhz separation * 2 = 8Mhz
  - 66 + 8 = 74Mhz of the available 83Mhz



GregSowell.com
MikrotikUniversity.com

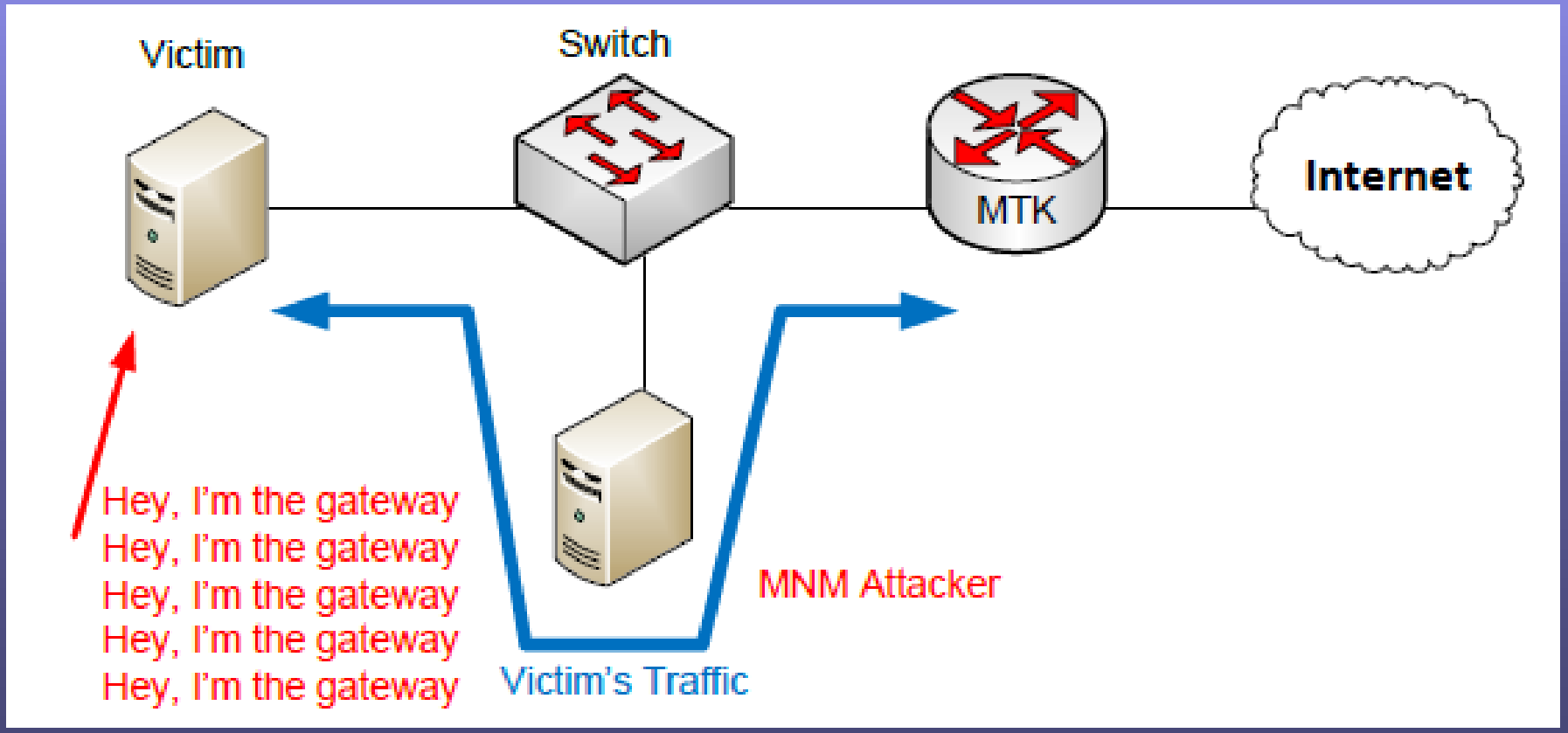
Man In The Middle Attack

- MITM happens when an attacker convinces you to proxy your traffic through him. He then steals information or directs you to false resources.

GregSowell.com
MikrotikUniversity.com

Man In The Middle Attack

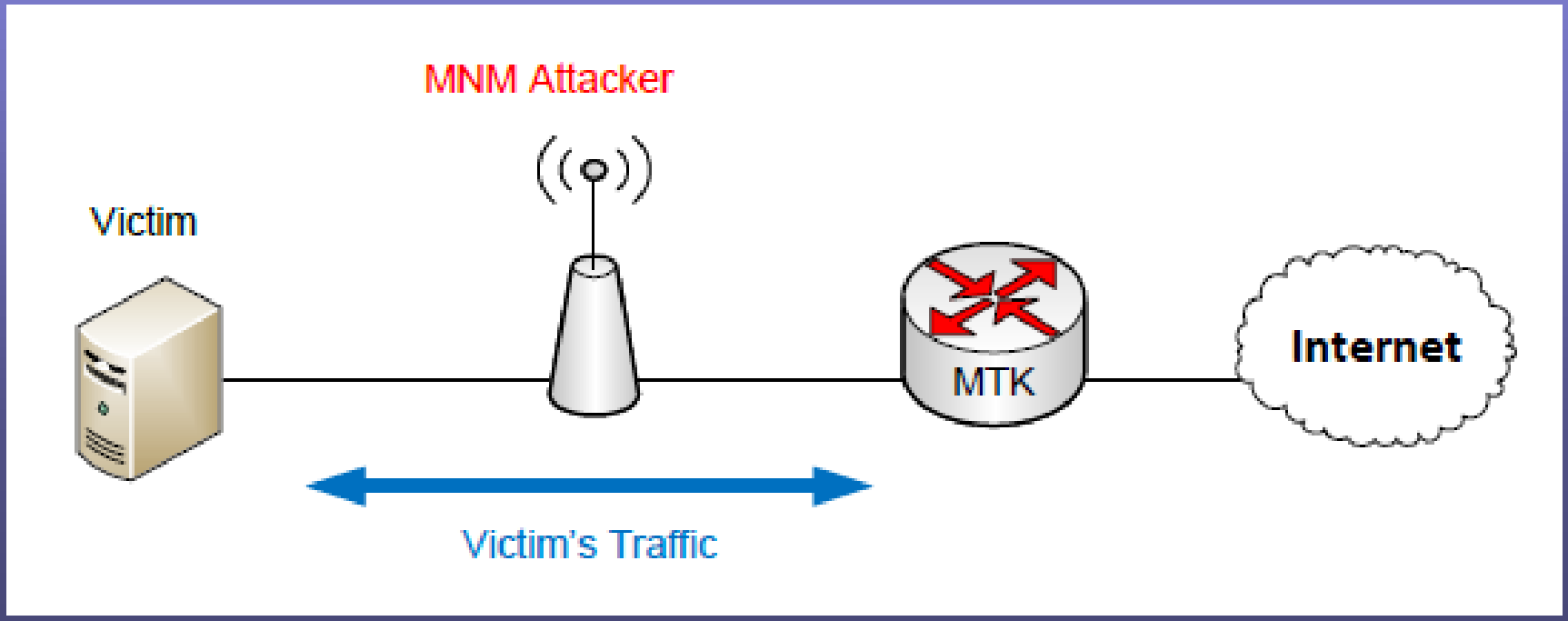
- A MITM attack usually happens when an attacker uses ARP poisoning on a network.



GregSowell.com
MikrotikUniversity.com

Man In The Middle Attack

- If you are performing MITM via an attackers access point, no poisoning is necessary… you are willingly sending all of your traffic. How nice of you ☺



GregSowell.com
MikrotikUniversity.com

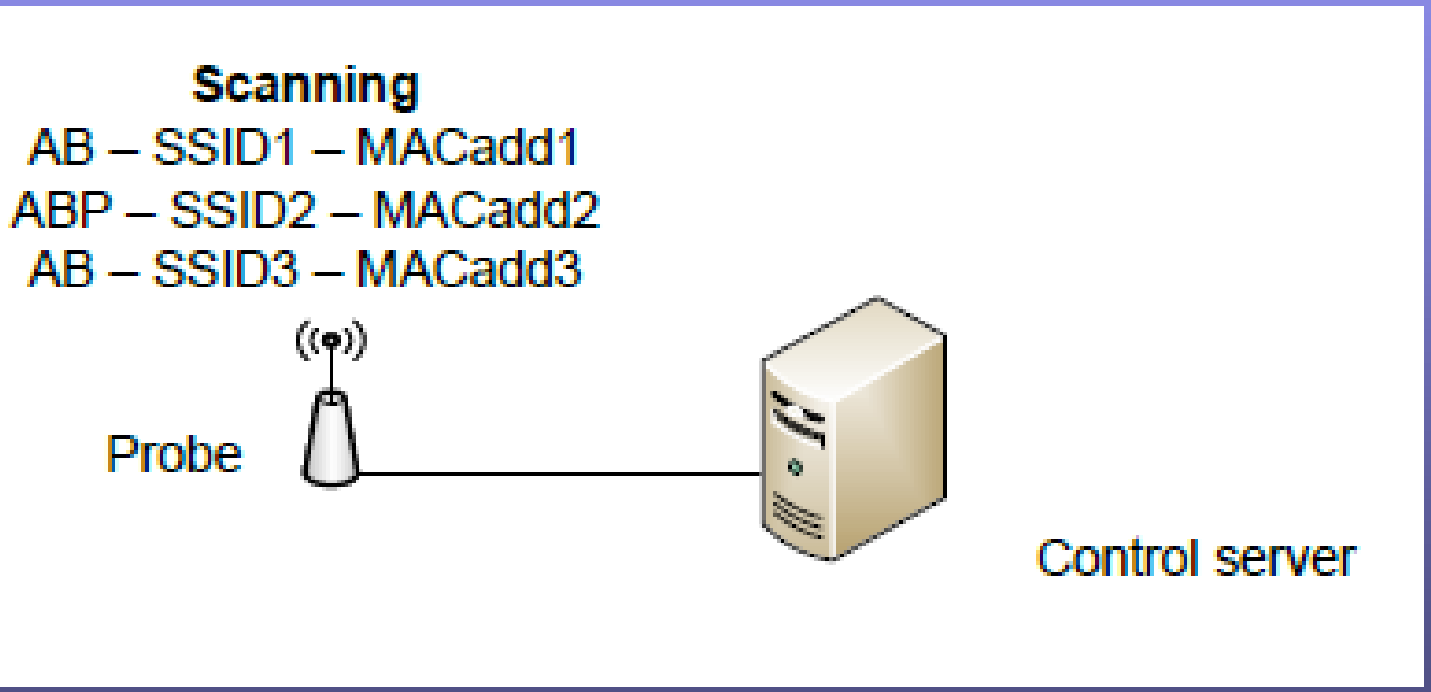
Commercial Methods

- Keep a list of MAC addresses and alert when a new address appears.
- Monitor MAC addresses looking for those that are of a wireless manufacturer.

GregSowell.com
MikrotikUniversity.com

Detect Rogues – Basic Flow

- Connect to probe and run wireless scan.



GregSowell.com
MikrotikUniversity.com

Detect Rogues – Basic Flow

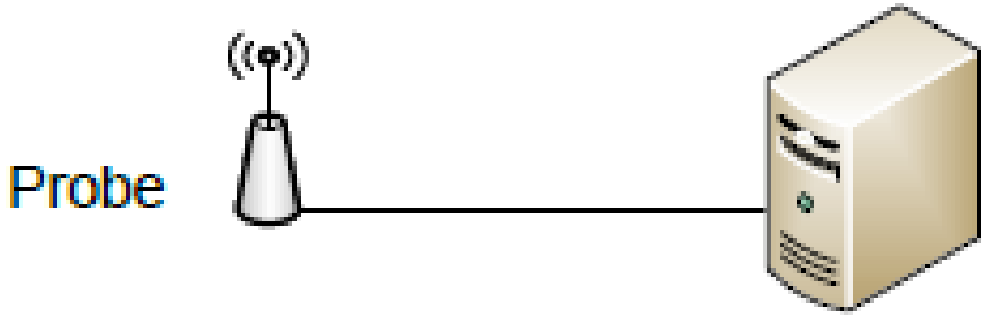
- Parse scan for open AP's not in ignore list.

Scanning

AB – SSID1 – MACadd1
ABP – SSID2 – MACadd2
AB – SSID3 – MACadd3

Ignore List

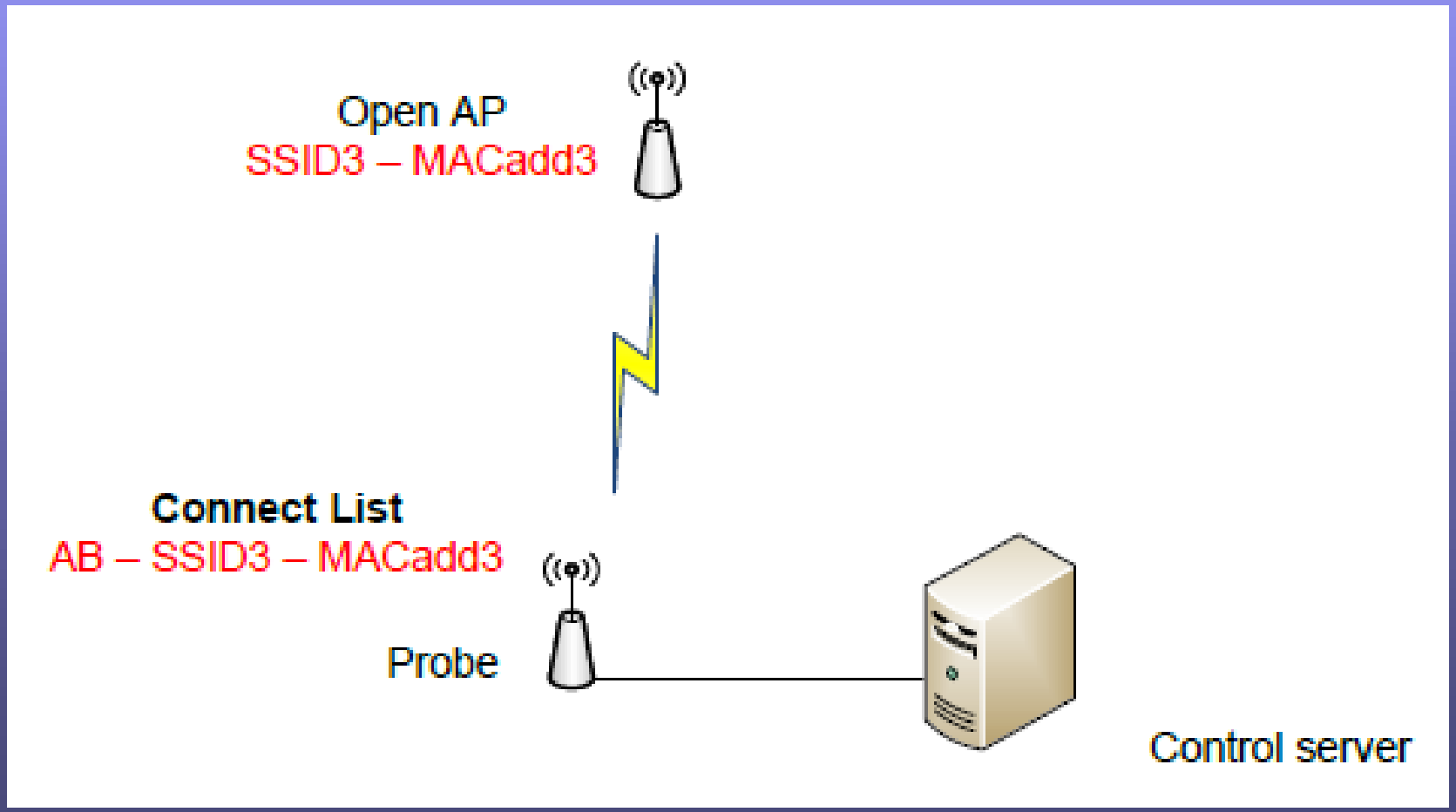
AB – SSID1 – MACadd1



GregSowell.com
MikrotikUniversity.com

Detect Rogues – Basic Flow

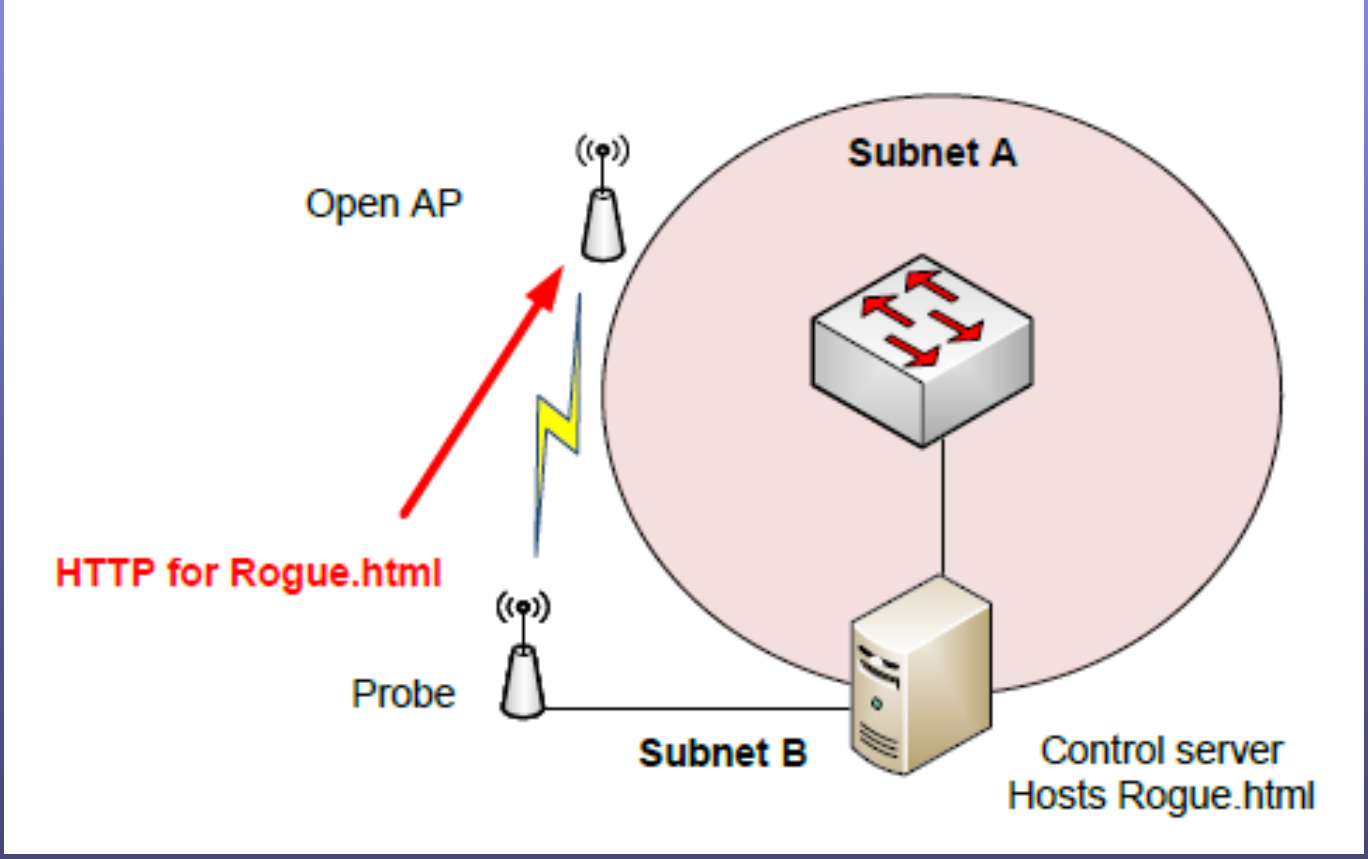
- Connect to open AP's.



GregSowell.com
MikrotikUniversity.com

Detect Rogues – Basic Flow

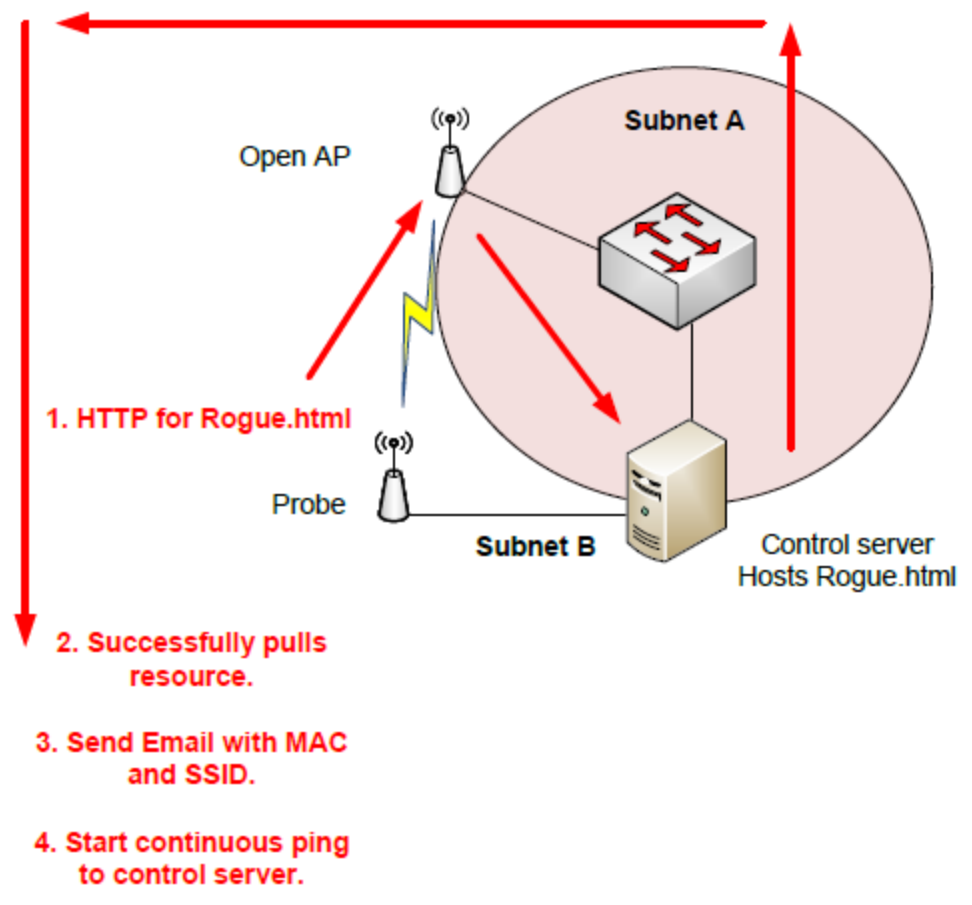
- Attempt to pull a resource that only exists internally to my network.
  - If it fails to, move to the next AP.



GregSowell.com
MikrotikUniversity.com

Detect Rogues – Basic Flow

- Attempt to pull a resource that only exists internally to my network.
- If it successfully pulls internal resource, we have a rogue.
  - Send email alert listing what probe it came from and rogue info.
  - Start a continuous ping from probe to internal resource.



GregSowell.com
MikrotikUniversity.com

Detect Rogues - Supplies

- Mikrotik Access Point. Preferably with a centrally located omni antenna.
- Windows machine. (Try to keep your booing to a minimum.)
- Putty. Windows SSH client.
- SMTP relay. Allows us to send alert emails.
- HTTP server. Hosts a basic html page.
- Rogue Detect program. Newest version will be on my blog along with source code. Written in AutoIT.

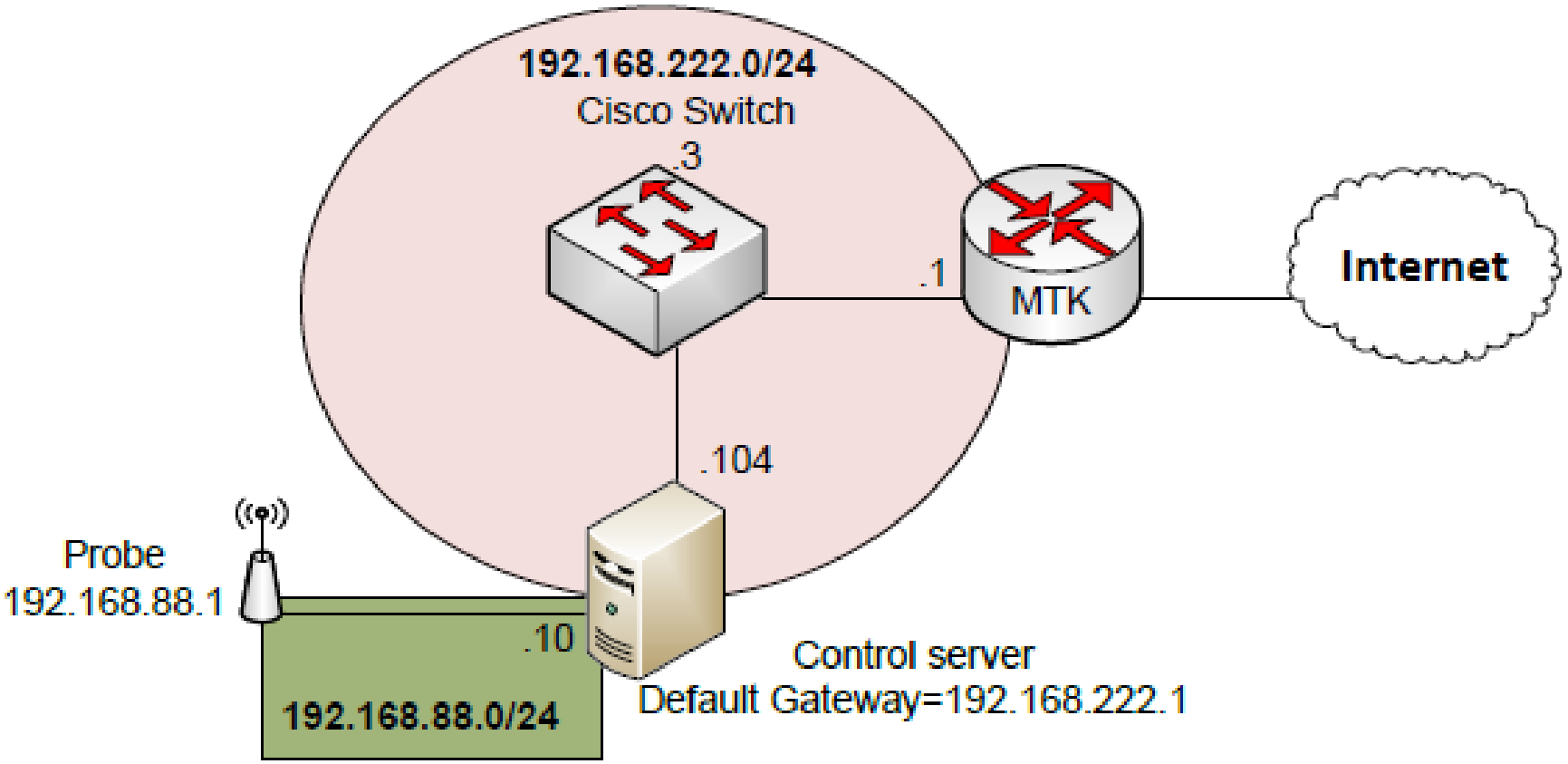
GregSowell.com
MikrotikUniversity.com

Rogue Detect Configuration

- Edit config files:
  - Ignore-list.txt
    - Any open AP's to ignore should be in this file. Format of MAC address~SSID
  - Probes.txt
    - This is the list of MTK probes to connect to. Format of IPaddress~username~password.
  - Settings.txt
    - This has all of the program settings. Format of: scan interval, internal server addressing and email settings.

GregSowell.com
MikrotikUniversity.com

Diagram



GregSowell.com
MikrotikUniversity.com

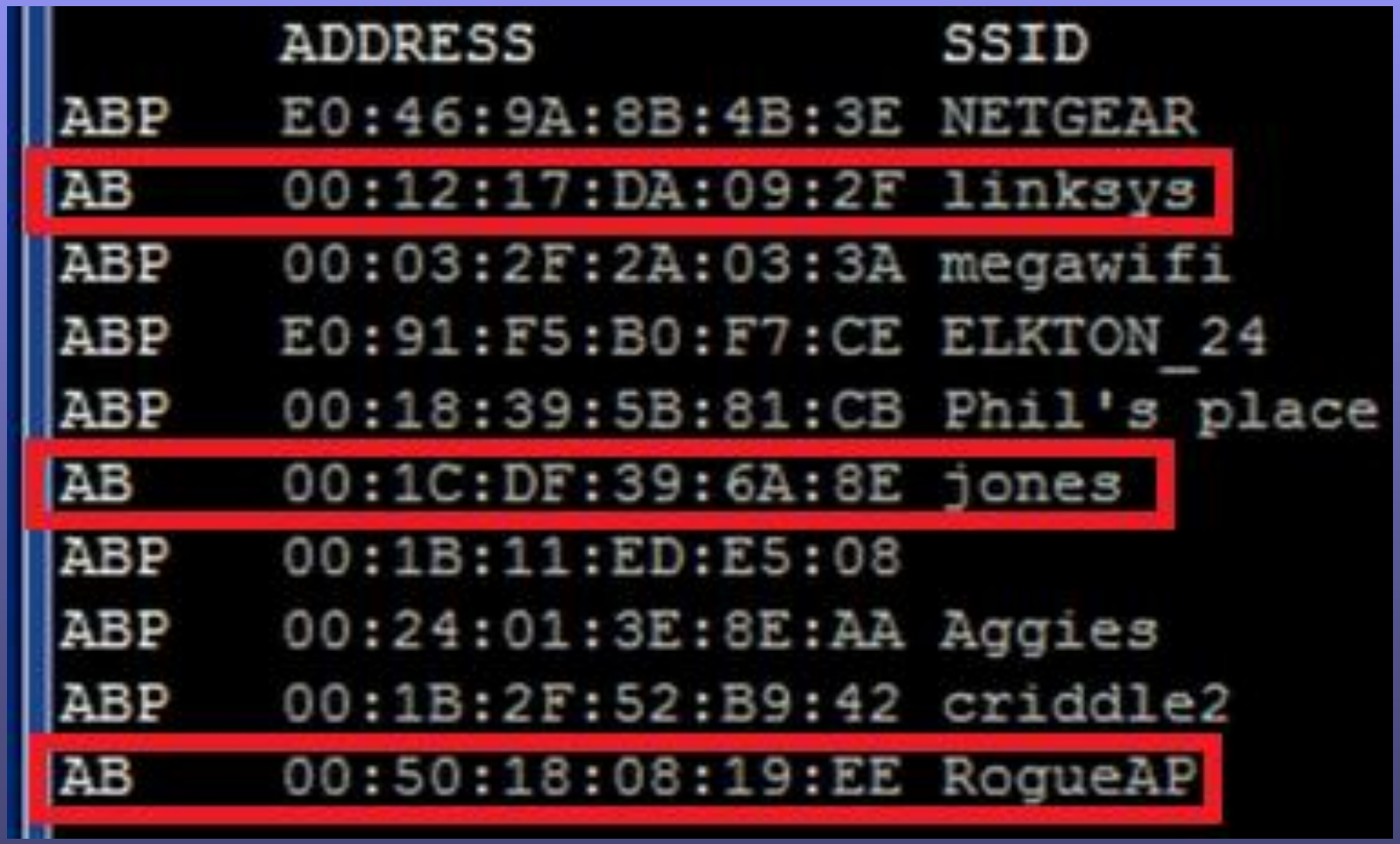
Step 1

- Program starts.
- Connects to first probe.
- Scans for available APs.

GregSowell.com
MikrotikUniversity.com

Step 1

- AP list pulled:



	ADDRESS	SSID
ABP	E0:46:9A:8B:4B:3E	NETGEAR
AB	00:12:17:DA:09:2F	linksys
ABP	00:03:2F:2A:03:3A	megawifi
ABP	E0:91:F5:B0:F7:CE	ELKTON_24
ABP	00:18:39:5B:81:CB	Phil's place
AB	00:1C:DF:39:6A:8E	jones
ABP	00:1B:11:ED:E5:08	
ABP	00:24:01:3E:8E:AA	Aggies
ABP	00:1B:2F:52:B9:42	criddle2
AB	00:50:18:08:19:EE	RogueAP

GregSowell.com
MikrotikUniversity.com

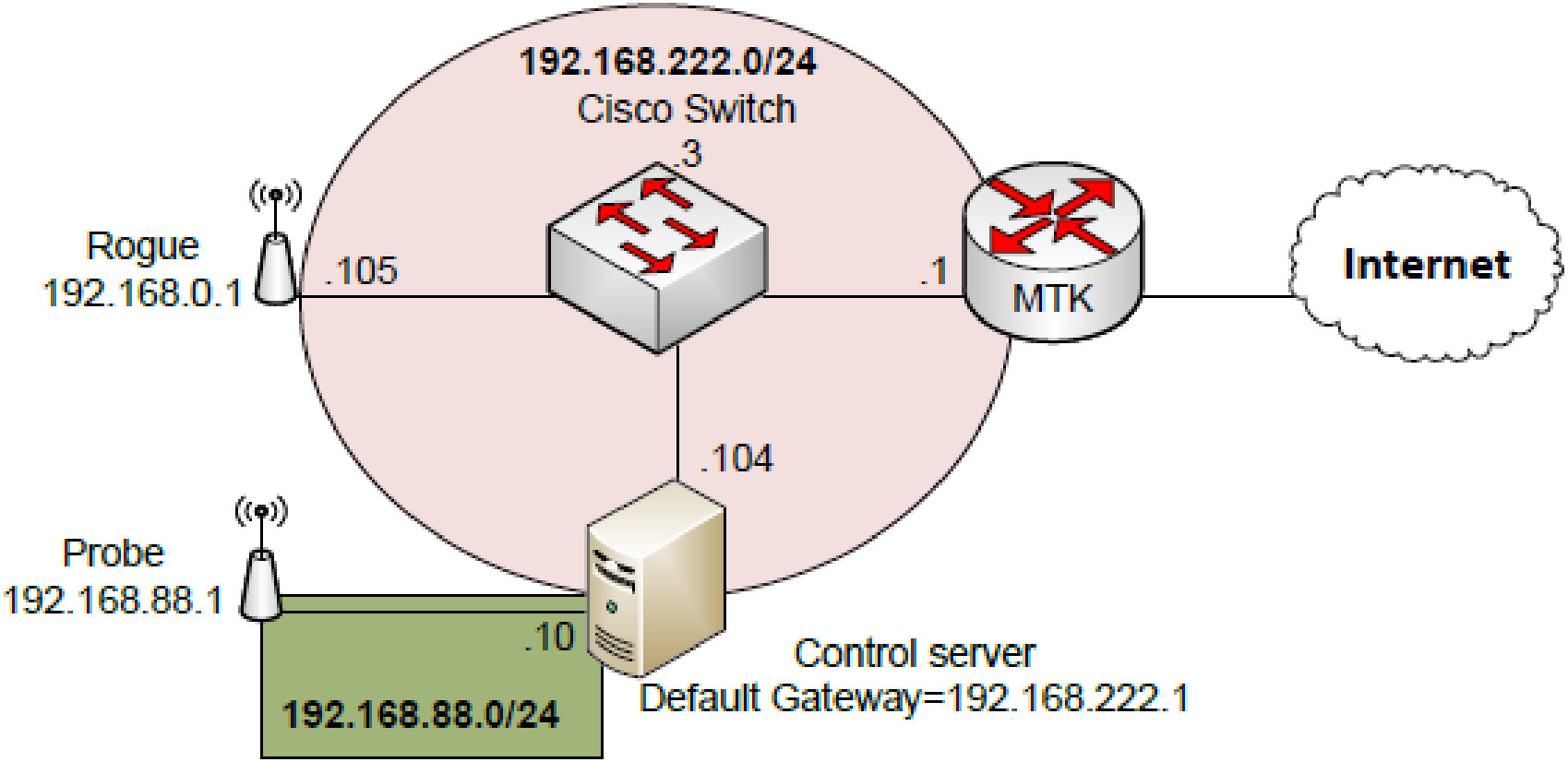
Step 2

- Grab list of APs.
- Scan through for open APs.
- Ensure the open APs aren’t on ignore list.
- Connect to AP.
- Release/renew DHCP address.
- Try and fetch rogue html page from server.

GregSowell.com
MikrotikUniversity.com

Step 3

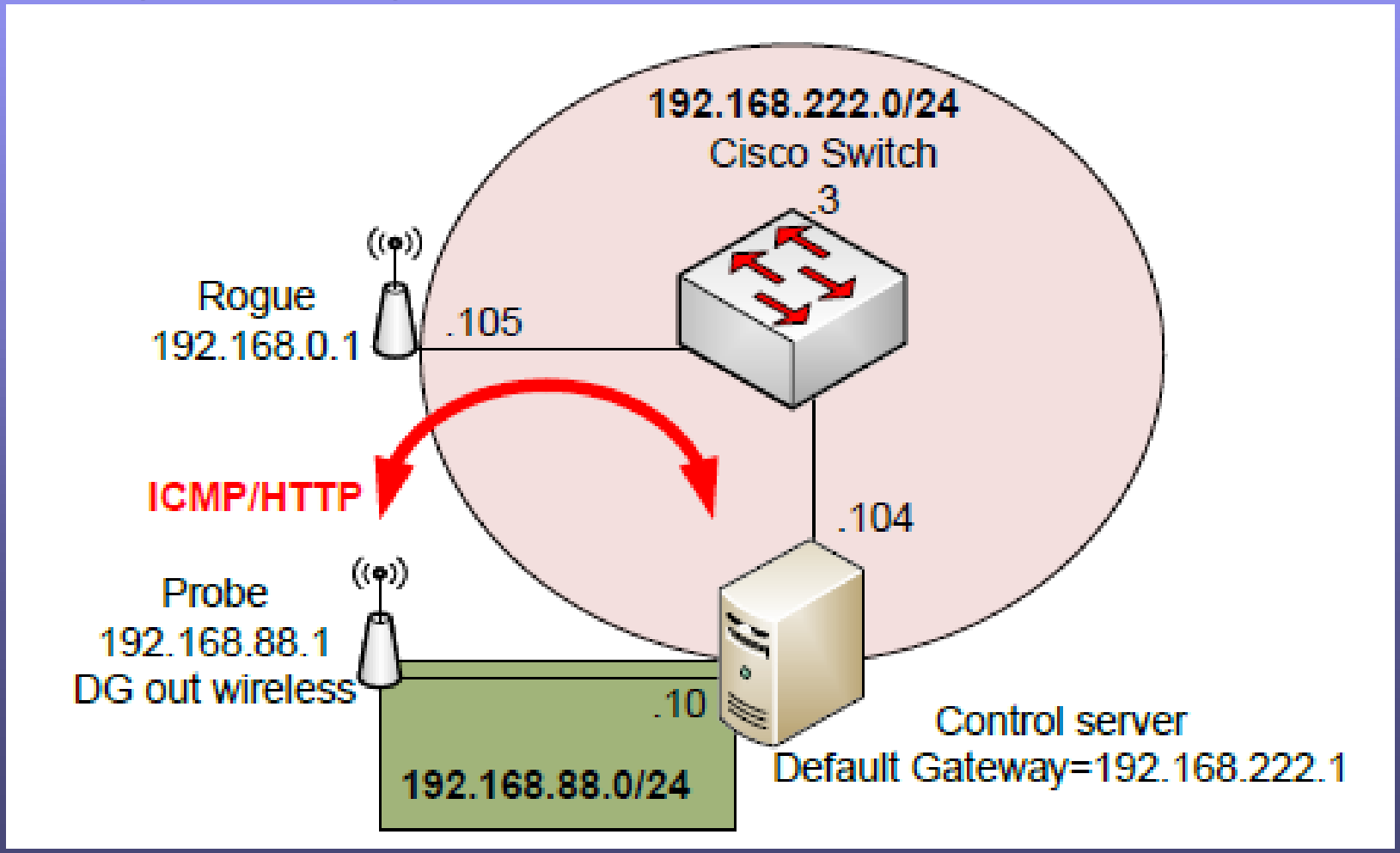
- Rogue Diagram:



GregSowell.com
MikrotikUniversity.com

Step 3

- Rogue Diagram Traffic Flow:



GregSowell.com
MikrotikUniversity.com

Step 3

- Open packet sniffer.
- Determine IP address of sending ICMP.
- If on same subnet, find MAC address.

GregSowell.com
MikrotikUniversity.com

Step 3

- IP in same subnet.
- Make note of MAC address.

GregSowell.com
MikrotikUniversity.com

Step 4

- Track down MAC address.
- “show mac-address-table”.
- Shut down port with offending device.
- Pay visit to owner of AP.

GregSowell.com
MikrotikUniversity.com

Possible Extensions

- Track all APs, open and encrypted.
- Try company encryption on protected APs.
- Rewrite in portable format.
- Rewrite completely CLI version.

GregSowell.com
MikrotikUniversity.com

Completely Theoretical Extensions

- Get pan/tilt mount

GregSowell.com
MikrotikUniversity.com

Completely Theoretical Extensions

- Mount outdoor AP to PT.

GregSowell.com
MikrotikUniversity.com

Completely Theoretical Extensions

- Mount outdoors.

GregSowell.com
MikrotikUniversity.com

Completely Theoretical Extensions

- Connect serially controlled relays from PC to PT.

GregSowell.com
MikrotikUniversity.com

Completely Theoretical Extensions

- Create algorithm that scans for open APs and connects to each for connectivity test.
- Keep track of signal strength/speed test of all and connect to best.
- If connectivity is lost or signal degrades, automatically switch to backup APs.

GregSowell.com
MikrotikUniversity.com

Thanks and happy routing!

GregSowell.com
MikrotikUniversity.com

Resources

- Link To Article (Contains files)
  - http://gregsowell.com/?p=3228
- Greg's Blog
  - http://GregSowell.com
- Training
  - http://MikrotikUniversity.com
- Wikipedia
  - http://en.wikipedia.org/wiki/Rogue_access_point
  - http://en.wikipedia.org/wiki/IEEE_802.11
- Wireshark
  - http://www.wireshark.org/
- Putty
  - http://www.chiark.greenend.org.uk/~sgtatham/putty/