
Beholder
Thotcon 0x1 – Chicago - 2010

Who I am

A security researcher since 1992

Author of some papers and security book

Security tools author, including one to detect rootkit/malware signs called ***chkrootkit*** tool for Unix environmnet.

Agenda

Motivation

Concepts

Tool structrure

Detection

What it doesn't do

Scenarios

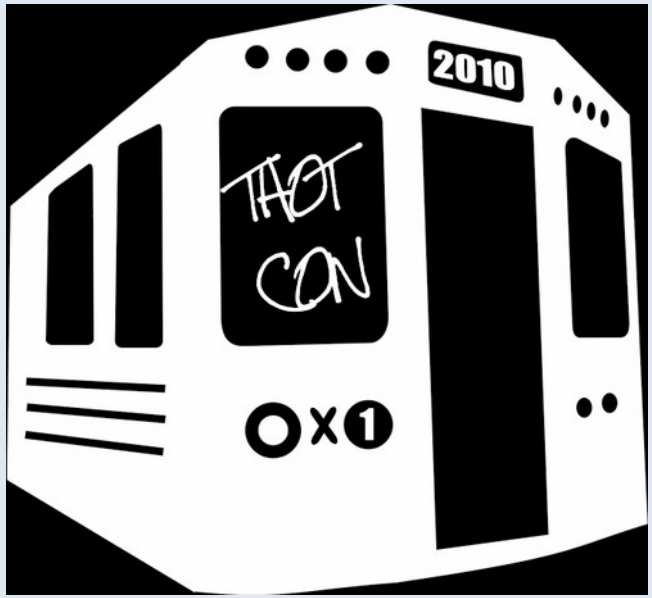
Demo

Motivation

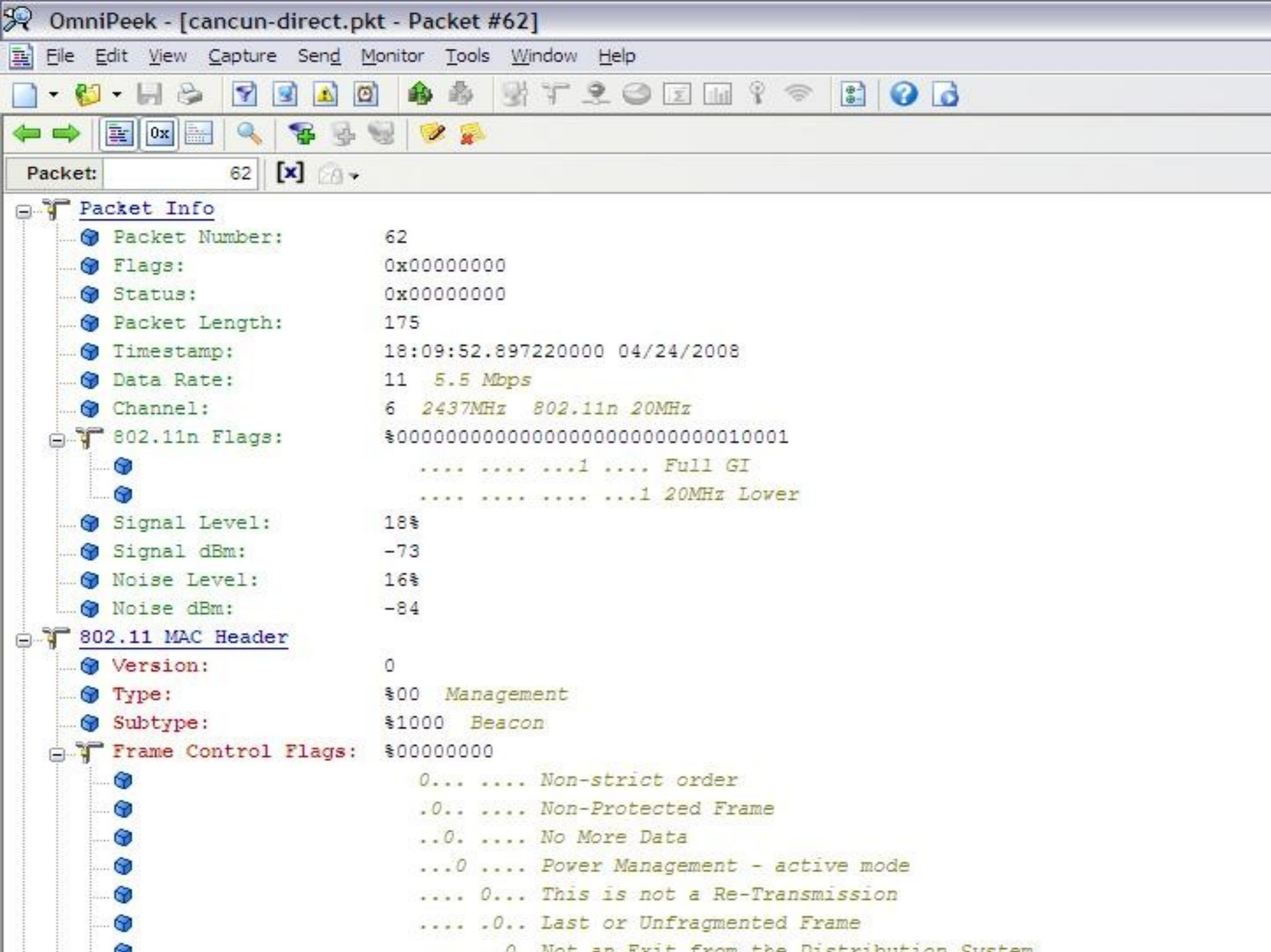
Because sometimes the current WIDSs fail?

Deep look at Wireless-tools source code

Talks at DefCon and others nice Cons



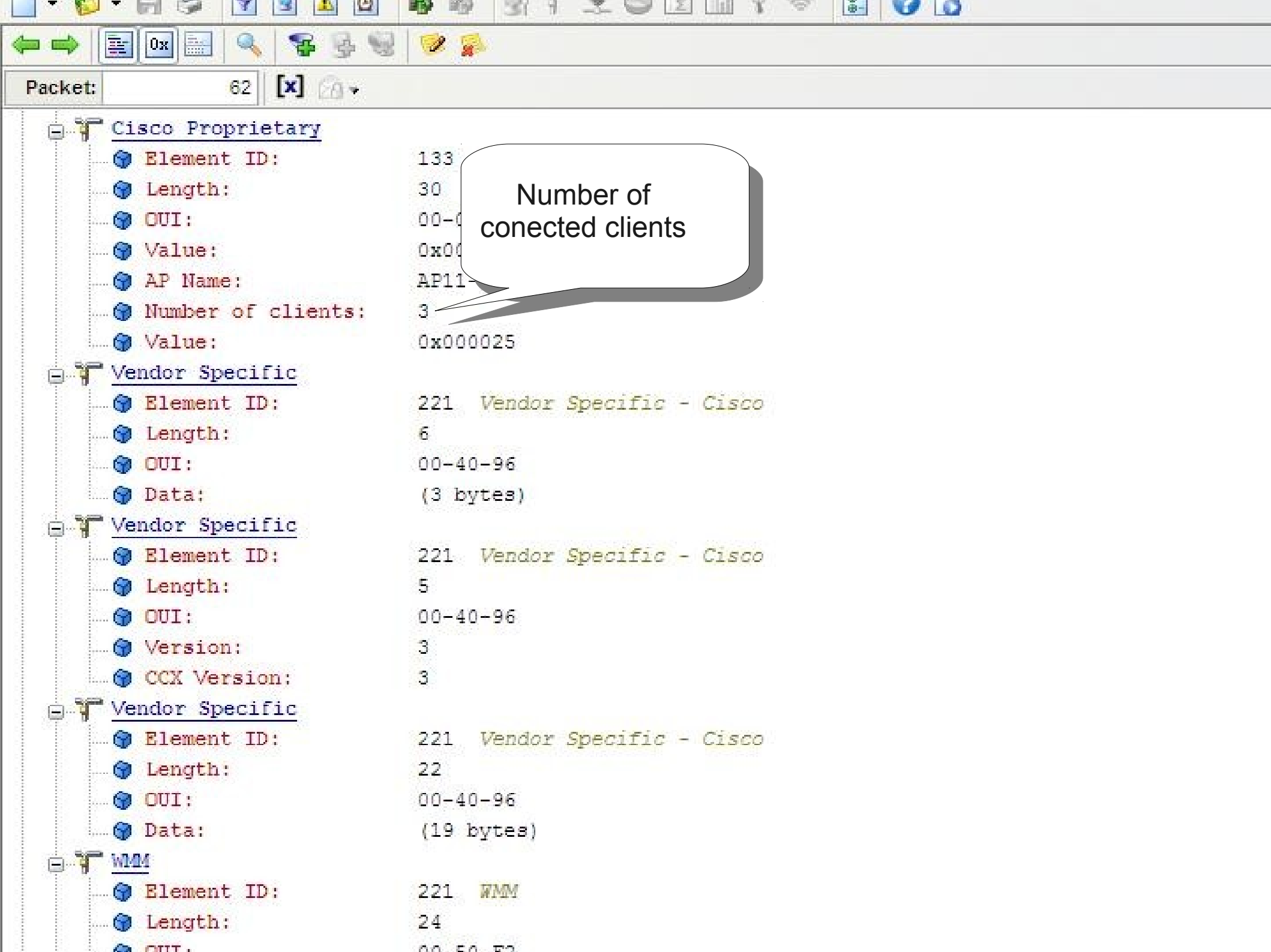
BEACONS


OmniPeek - [cancun-direct.pkt - Packet #62]
File Edit View Capture Send Monitor Tools Window Help
Packet: 62
Packet Info
Packet Number: 62
Flags: 0x00000000
Status: 0x00000000
Packet Length: 175
Timestamp: 18:09:52.897220000 04/24/2008
Data Rate: 11 5.5 Mbps
Channel: 6 2437MHz 802.11n 20MHz
802.11n Flags: %00000000000000000000000000010001
....1 .... Full GI
....1 20MHz Lower
Signal Level: 18%
Signal dBm: -73
Noise Level: 16%
Noise dBm: -84
802.11 MAC Header
Version: 0
Type: %00 Management
Subtype: %1000 Beacon
Frame Control Flags: %00000000
0... .... Non-strict order
.0.. .... Non-Protected Frame
..0. .... No More Data
...0 .... Power Management - active mode
.... 0... This is not a Re-Transmission
.... .0.. Last or Unfragmented Frame

```
▽ IEEE 802.11 wireless LAN management frame
  ▽ Fixed parameters (12 bytes)
      Timestamp: 0x0000000DB42DC18D
      Beacon Interval: 0.102400 [Seconds]
    ▽ Capability Information: 0x0411
        .... .... .... ...1 = ESS capabilities: Transmitter is an AP
        .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
        .... ..0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x0000)
        .... .... ...1 .... = Privacy: AP/STA can support WEP
        .... .... ..0. .... = Short Preamble: Short preamble not allowed
        .... .... .0.. .... = PBCC: PBCC modulation not allowed
        .... .... 0... .... = Channel Agility: Channel agility not in use
        .... ...0 .... .... = Spectrum Management: dot11SpectrumManagementRequired FALSE
        .... .1.. .... .... = Short Slot Time: Short slot time in use
        .... 0... .... .... = Automatic Power Save Delivery: apsd not implemented
        ..0. .... .... .... = DSSS-OFDM: DSSS-OFDM modulation not allowed
        .0.. .... .... .... = Delayed Block Ack: delayed block ack not implemented
        0... .... .... .... = Immediate Block Ack: immediate block ack not implemented
  ▽ Tagged parameters (73 bytes)
    ▷ SSID parameter set
    ▷ Supported Rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B)
    ▷ DS Parameter set: Current Channel: 1
    ▷ Traffic Indication Map (TIM): DTIM 0 of 1 bitmap empty
    ▷ ERP Information: no Non-ERP STAs, do not use protection, short or long preambles
    ▷ ERP Information: no Non-ERP STAs, do not use protection, short or long preambles
    ▷ Extended Supported Rates: 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
    ▷ Vendor Specific: Broadcom
    ▷ Vendor Specific: Microsof: WPA
```

802.11 Beacons

Can hide important stuff


Packet: 62
Cisco Proprietary
Element ID: 133
Length: 30
OUI: 00-0
Value: 0x00
AP Name: AP11-
Number of clients: 3
Value: 0x000025
Vendor Specific
Element ID: 221 Vendor Specific - Cisco
Length: 6
OUI: 00-40-96
Data: (3 bytes)
Vendor Specific
Element ID: 221 Vendor Specific - Cisco
Length: 5
OUI: 00-40-96
Version: 3
CCX Version: 3
Vendor Specific
Element ID: 221 Vendor Specific - Cisco
Length: 22
OUI: 00-40-96
Data: (19 bytes)
WMM
Element ID: 221 WMM
Length: 24
Number of conected clients

Hidden ESSID

File Edit Settings Help

scan
channel 6

Network device ath0 Refresh
Driver type Other

40 bit crack breadth: 3
128 bit crack breadth: 2

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	Unique	PW: Hex	PW: ASCII
	00:07:40:4D:1A:5C	Homenet54		Fri Apr 21 20:23:39 2006	00:00:00	3	542	0	0	0		
	00:09:5B:66:3D:0E	NETGEAR	Y	Fri Apr 21 20:23:23 2006	00:00:00	11	2	0	0	0		

Enable bridging to wired LAN

Enable SSID broadcast

Apply Cancel

File Edit Settings

scan
channel 6

Network device ath0 Refresh
Driver type Other

40 bit crack breadth: 3
128 bit crack breadth: 2

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	Unique	PW: Hex	PW: ASCII
	00:07:40:4D:1A:5C	Homenet54		Fri Apr 21 20:14:18 2006	00:00:00	3	266	0	0	0		
	00:09:5B:66:3D:0E	.....	Y	Fri Apr 21 20:13:58 2006	00:00:00	11	1	0	0	0		

Hidden SSID

```
23:05:16.386193 Beacon () [1.0 2.0 5.5 11.0 6.0 12.0 24.0 36.0
Mbit] ESS CH: 11

23:05:16.488612 Beacon () [1.0 2.0 5.5 11.0 6.0 12.0 24.0 36.0
Mbit] ESS CH: 11

23:05:17.321039 Beacon (Homenet54) [1.0 2.0 5.5 11.0 Mbit] ESS
CH: 3

23:05:17.629271 Beacon (Homenet54) [1.0 2.0 5.5 11.0 Mbit] ESS
CH: 3
```

Features

Beholder facts

Written in C Ansi and based on IWLIST (Linux wireless tools)

Changes on AP (SSID, MAC, Mode)

Channel and encryption proto changes

Meaningful signal level variations

Syslog support to large networks (many sensors)

Not just another network scanner

Features

Karma


Adventure
Love
Fortune
ADVENTURE
LOVE
FORTUNE
$
Pick Your Karma
Booster Juice

Karma

KARMA includes patches for the Linux MADWifi driver to allow the creation of an 802.11 Access Point that responds to any probed SSID. So if a client looks for 'linksys', it is 'linksys' to them (even while it may be 'tmobile' to someone else). Operating in this fashion has revealed vulnerabilities in how Windows XP and MacOS X look for networks, so clients may join even if their preferred networks list is empty.

DHCP Offer
POP3/FTP password sniffing
Redirect HTTP traffic to malicious server

Karma with steroids

```
KARMA + MetaSploit3 + Aircrack-ng == KarmaSploit
```

- Karma re-burn
- MadWifi patch changed by Aircrack-ng tools
- Easy to write new xploits
- New power with DNS D. Kaminsky vulnerability
- New xploits are imediately available to add in Metasploit.


```
/h[a4@](([c<]((k)|(\|<)))|((k)|(\|<))|(x))\s+\
((d)|([t\+]h))[3ea4@]\s+p[l1][a4@]n[3e][t\+]/i
```


POWER
CHARGE
GNXT

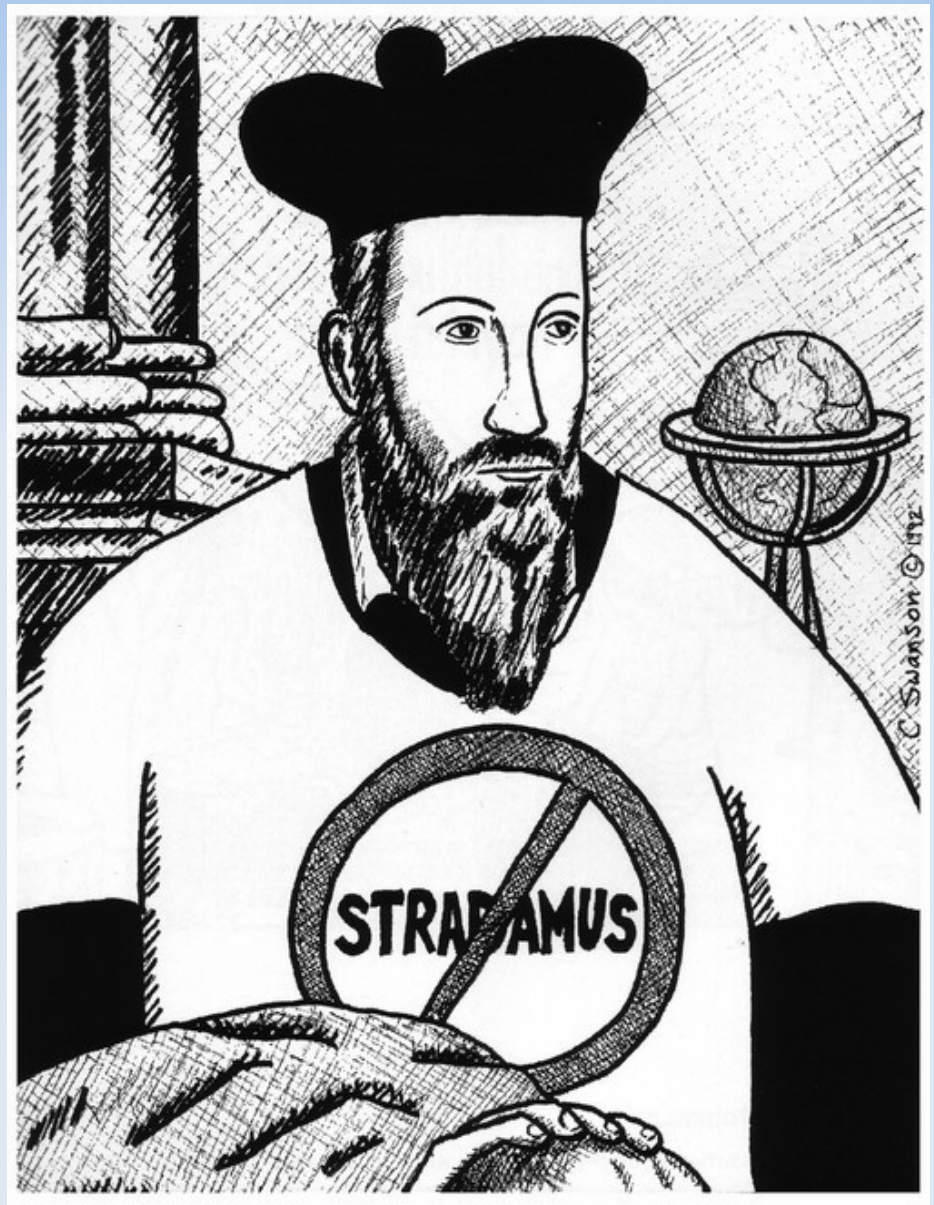
What beholder doesn't do

- Put interface in promisc mode
- Put interface in monitor mode
- WPA/WEP stuff
- Access Point or client weakness

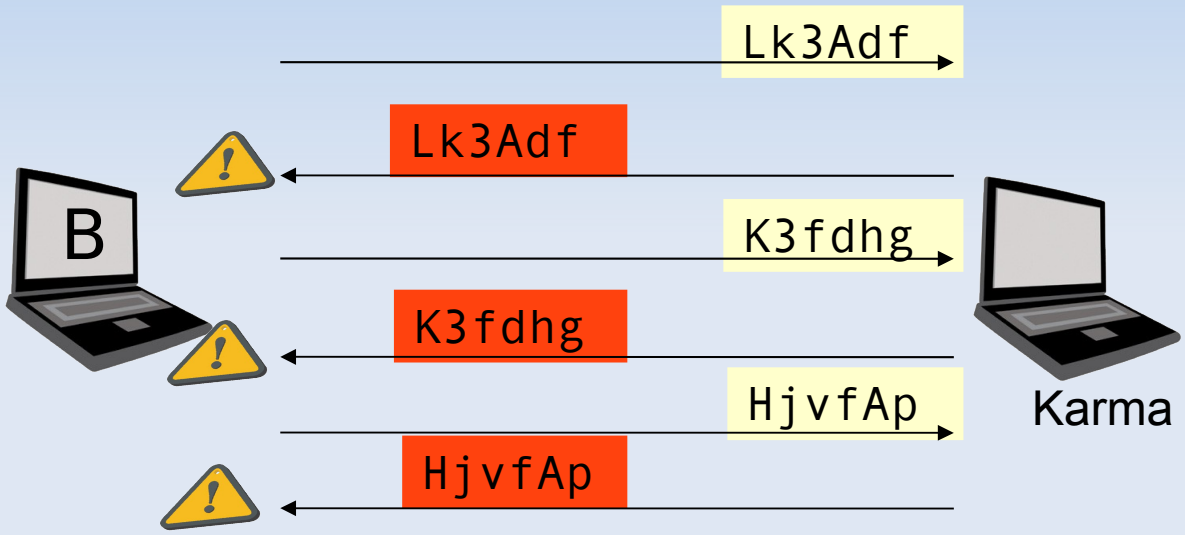
Availability

For while...

Future?



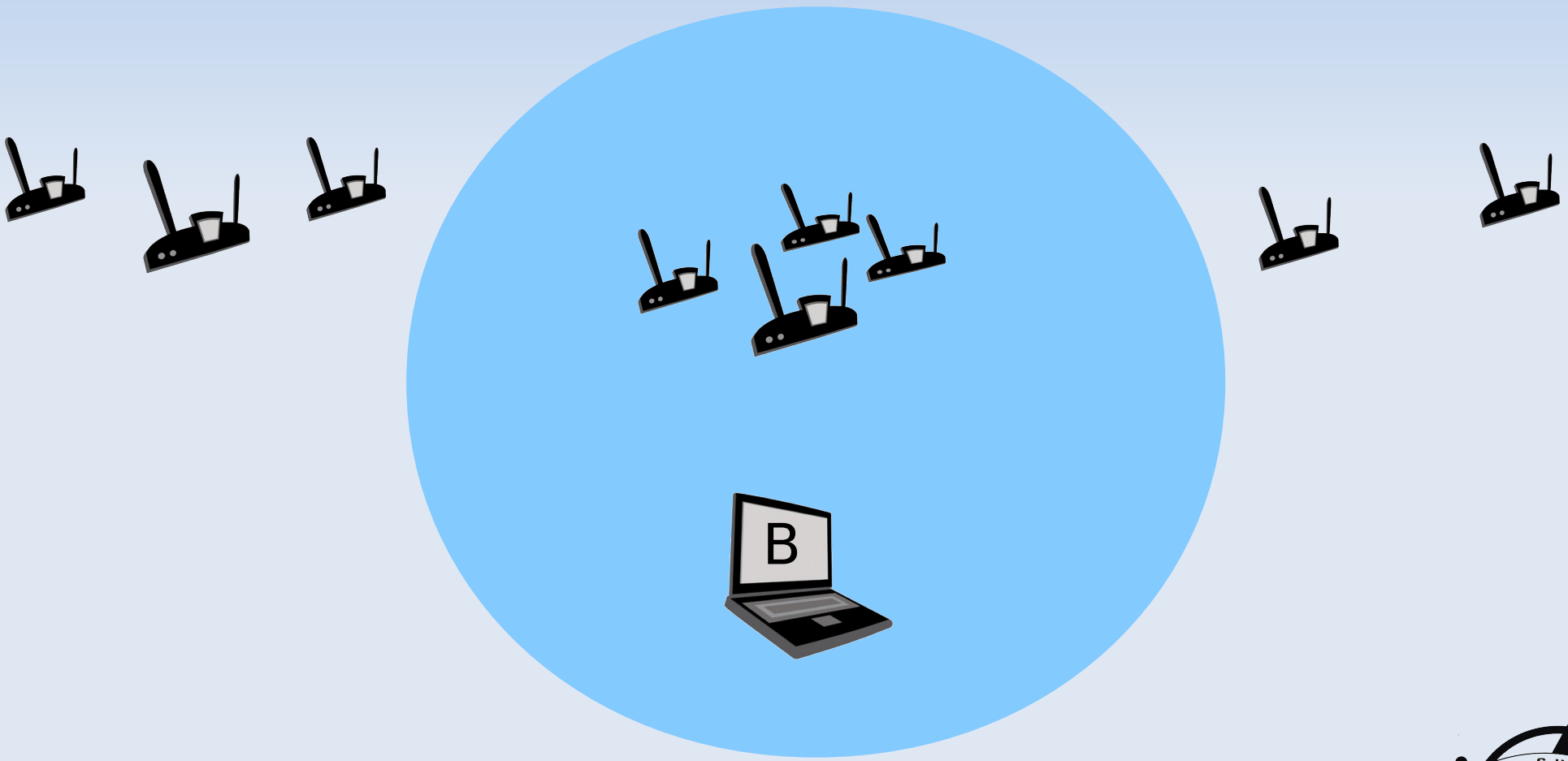
Karma detecion



Scenarios

Alert for missing APs(RegEx)

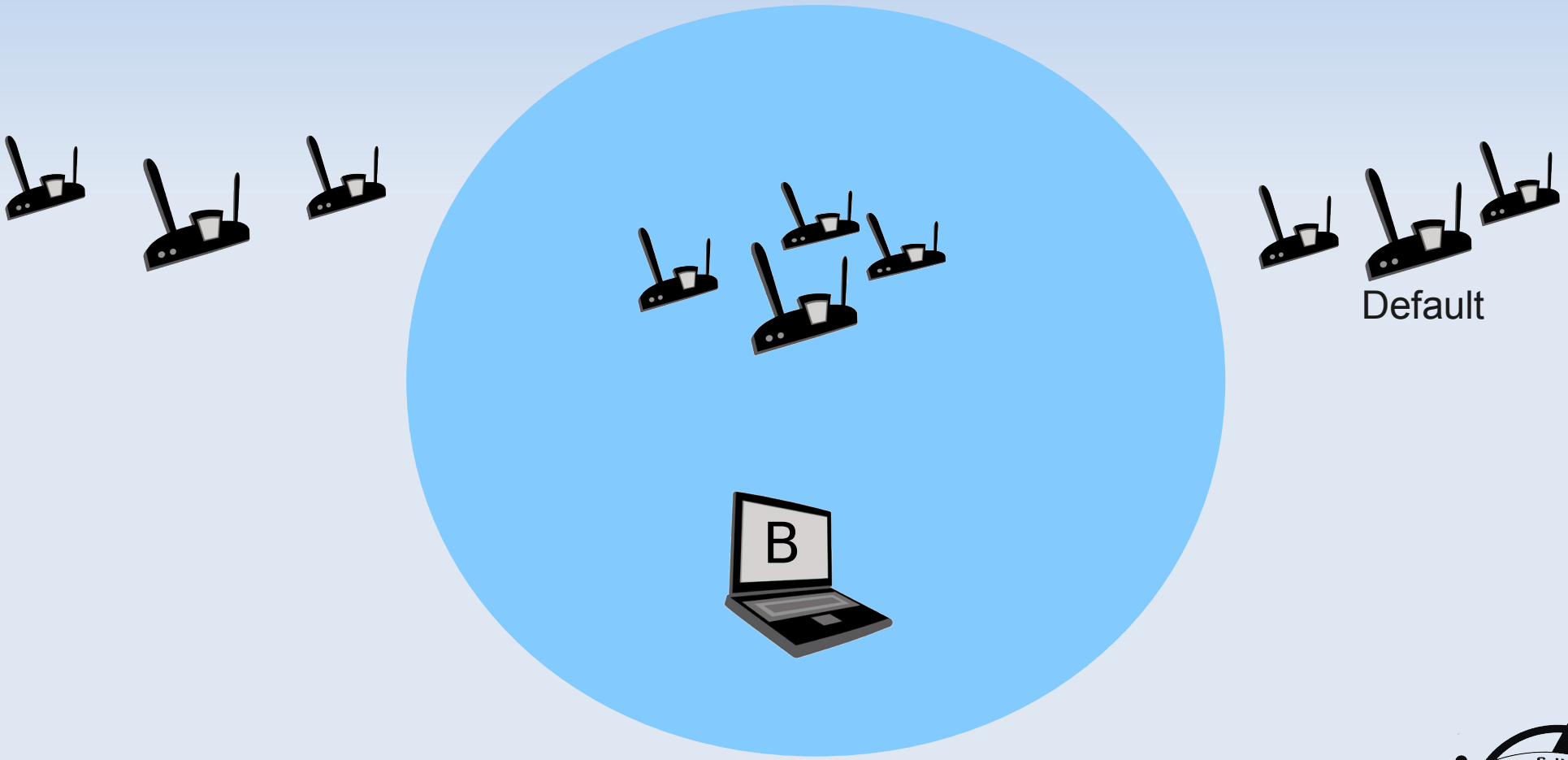
```
beholder -m “mynets” wifidev
```



Scenarios

Alert for missing APs(RegEx)

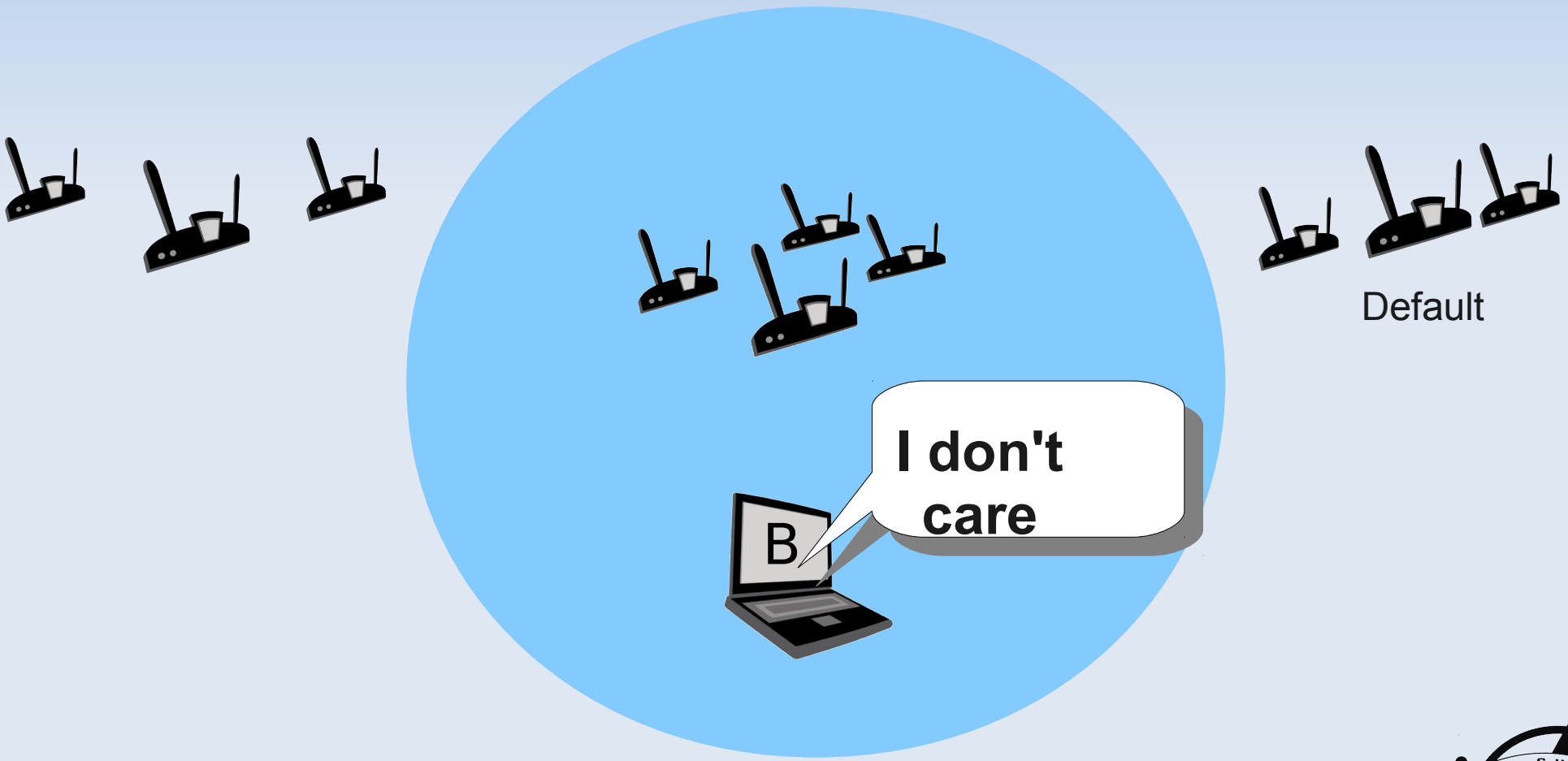
```
beholder -m “mynets” wifidev
```



Scenarios

Alert for missing APs(RegEx)

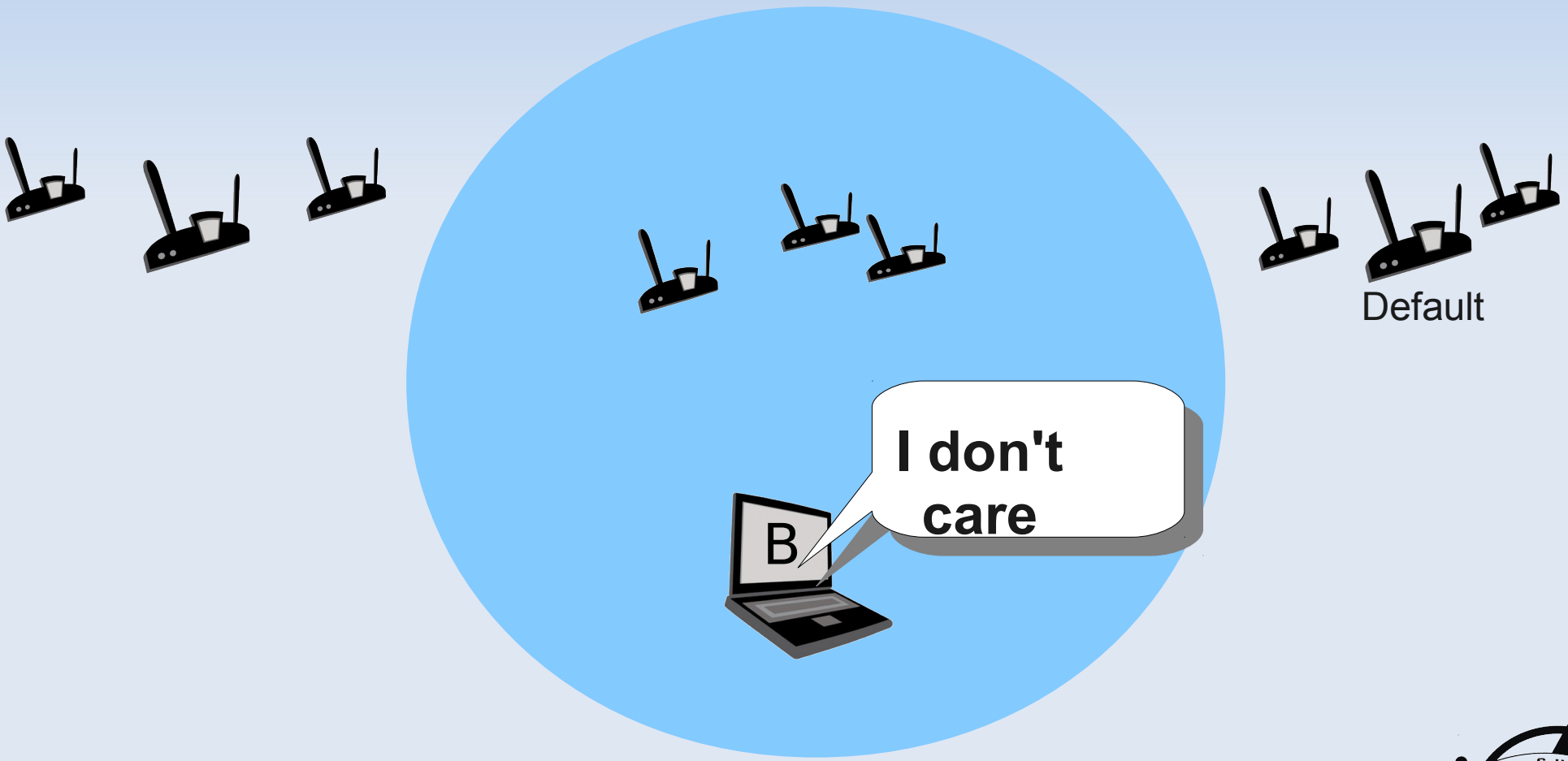
```
beholder -m “mynets” wifidev
```



Scenarios

Alert for missing APs(RegEx)

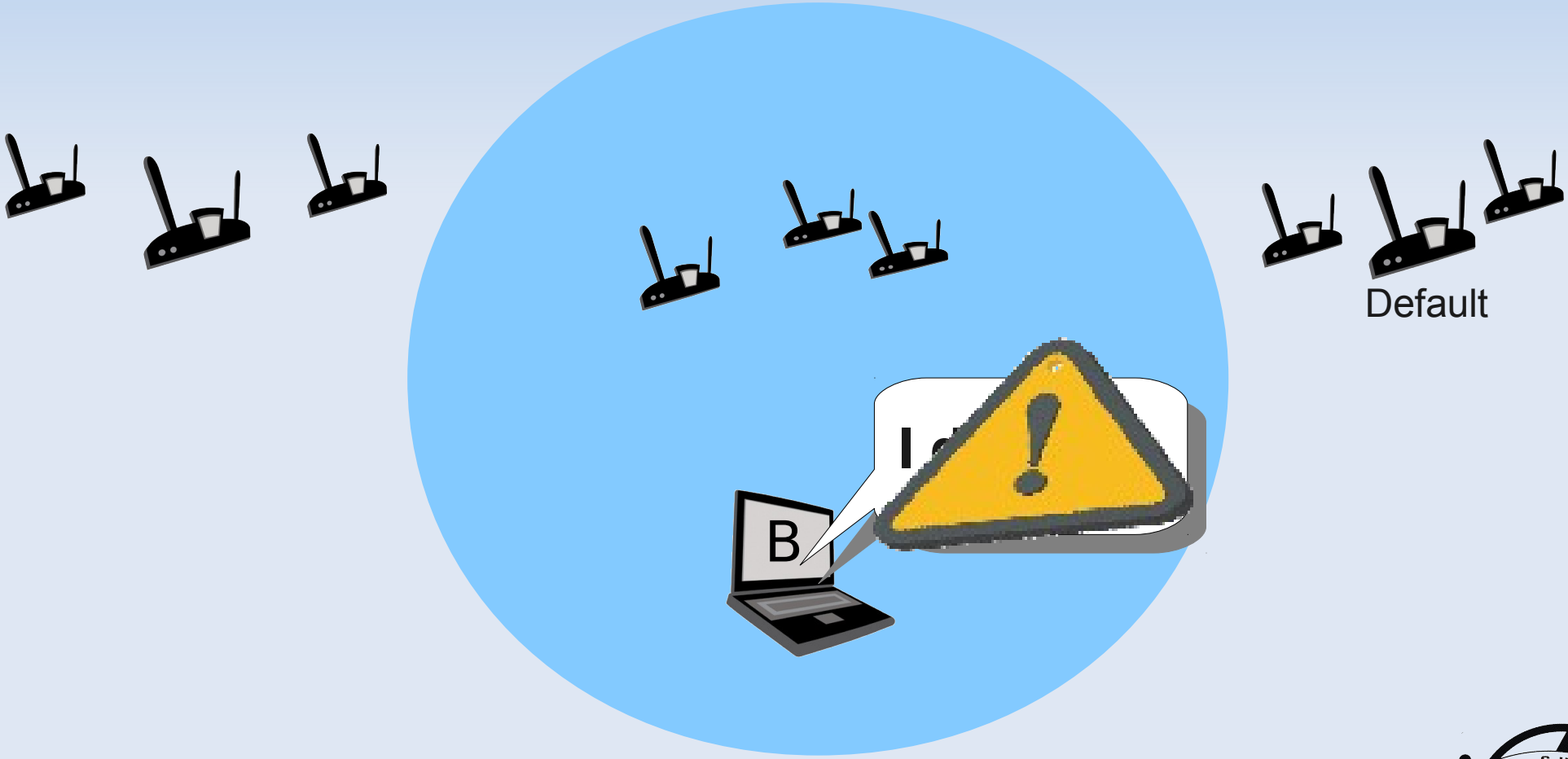
```
beholder -m “mynets” wifidev
```



Scenarios

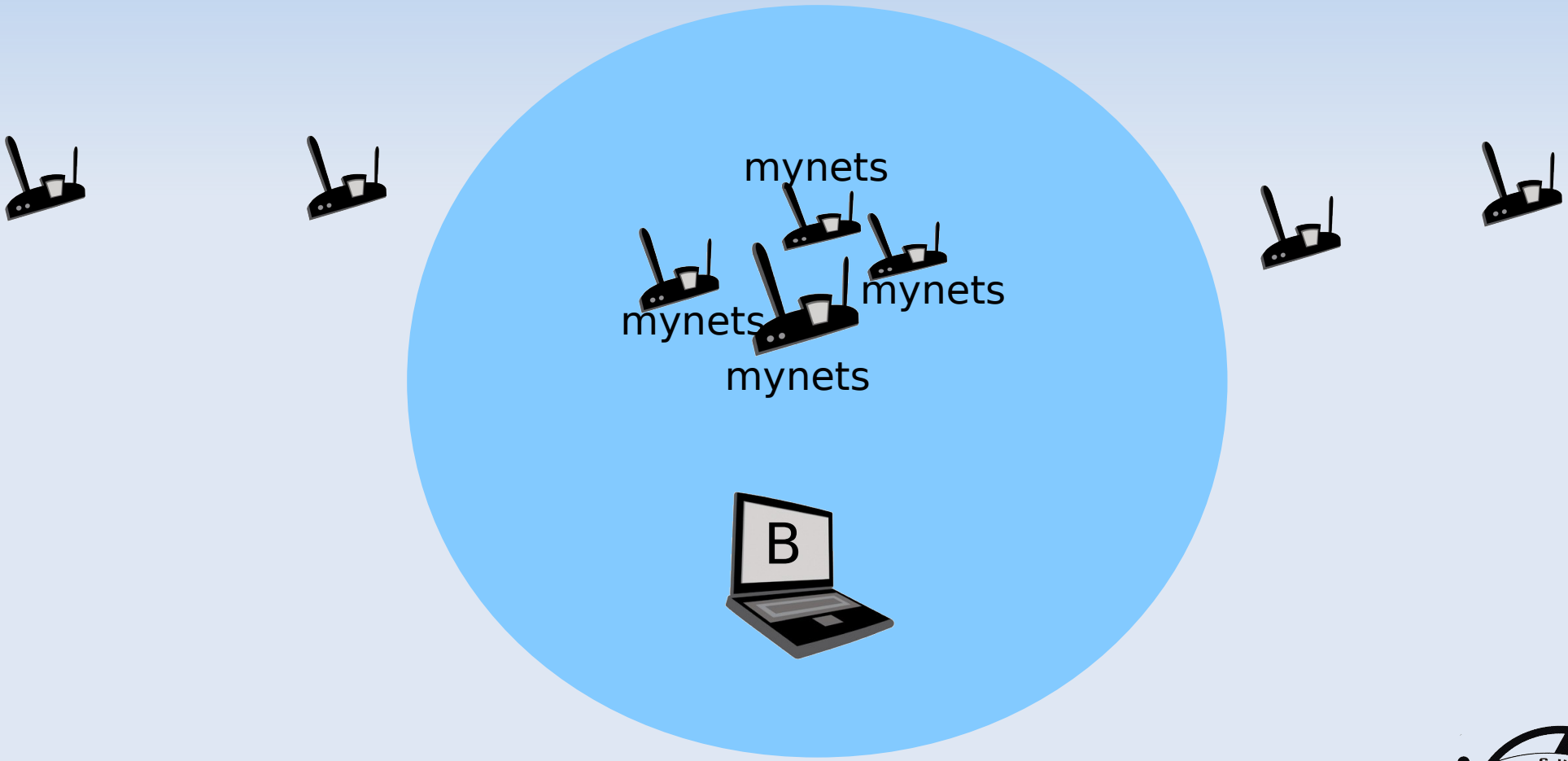
Alert for missing APs(RegEx)

```
beholder -m “mynets” wifidev
```



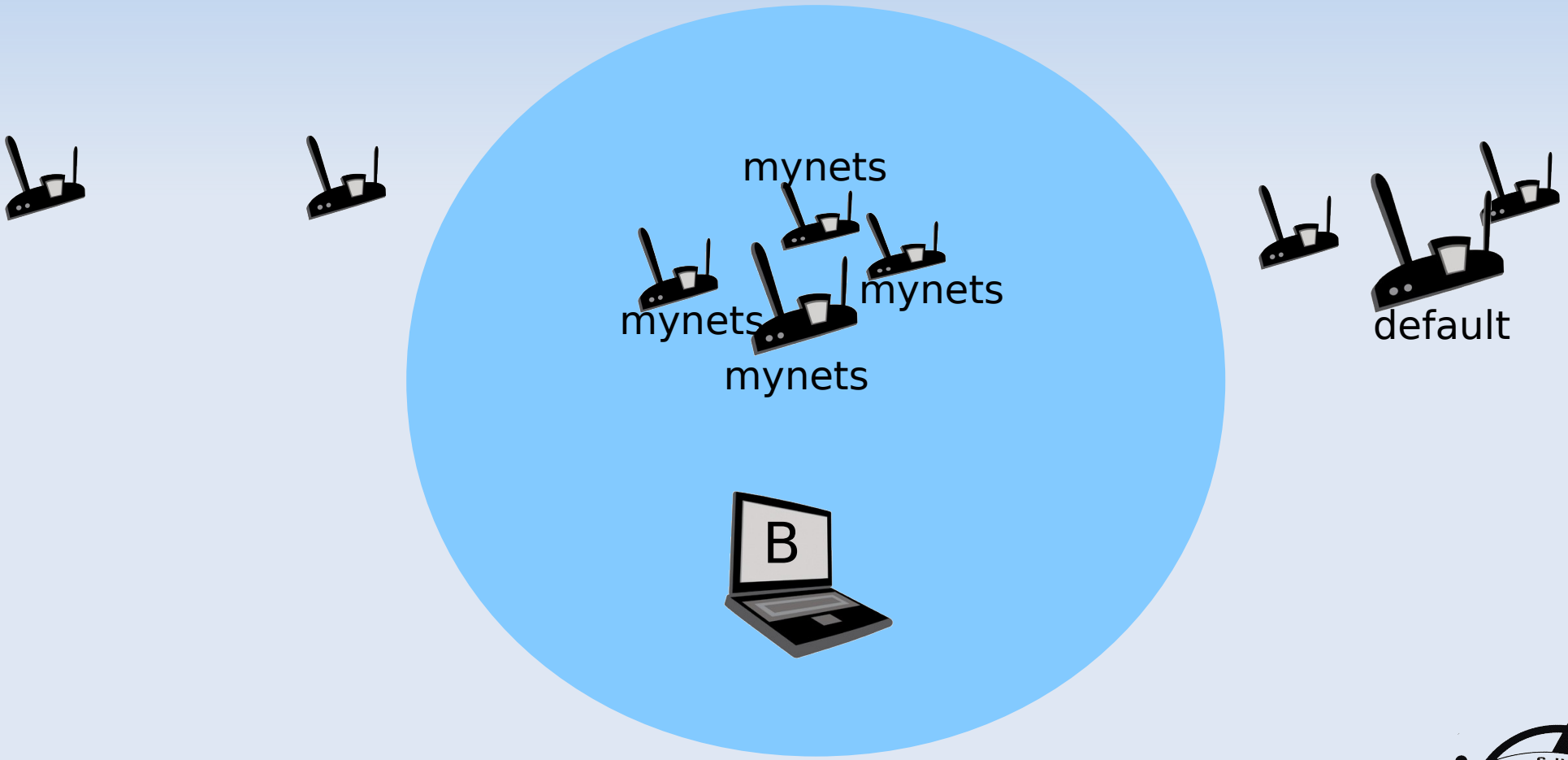
Scenarios
checking for similar essids via RegEX

beholder **-r “myne[t7]s.*”** wifidev



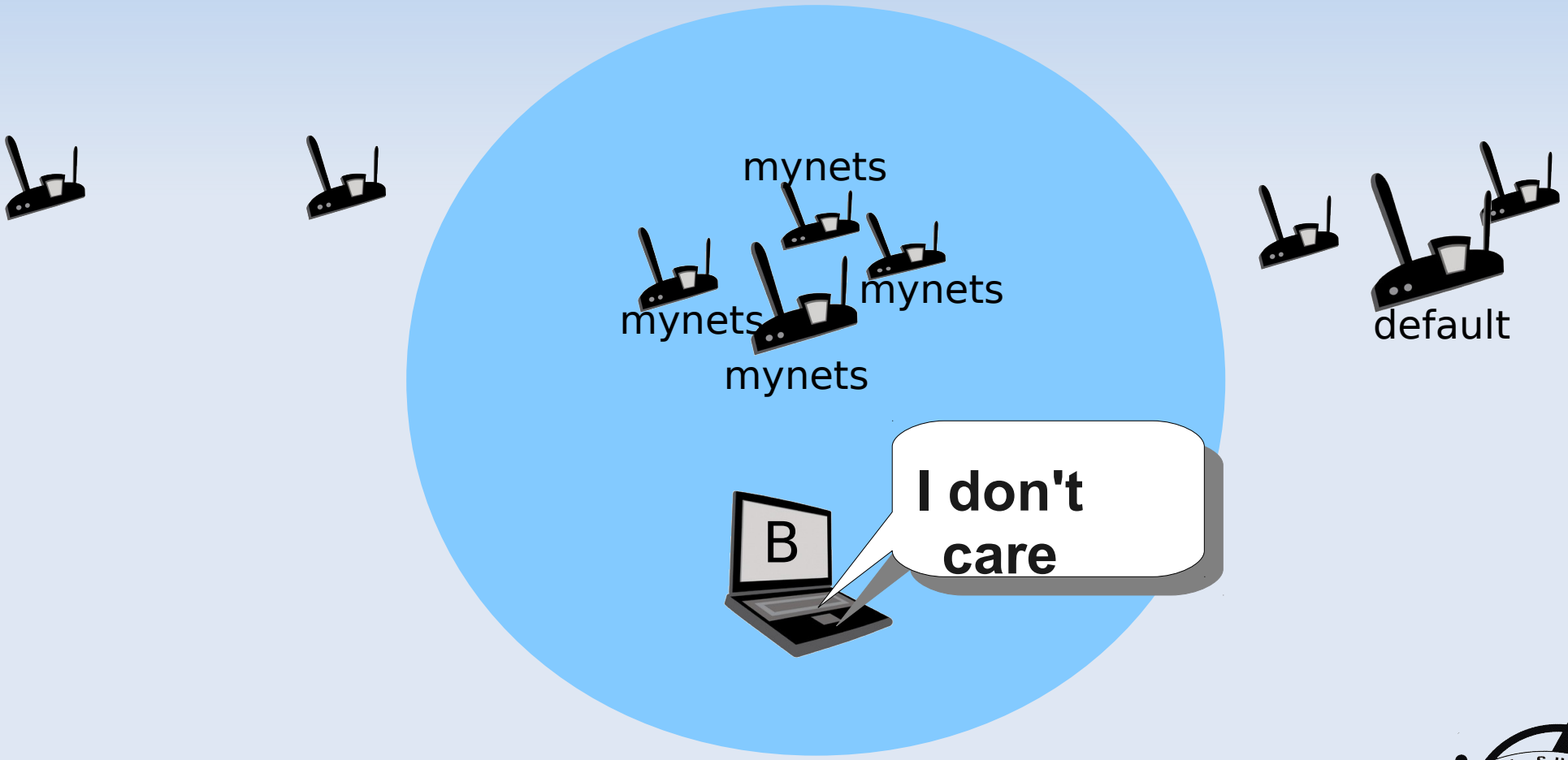
Scenarios
checking for similar essids via RegEX

beholder **-r “myne[t7]s.*”** wifidev



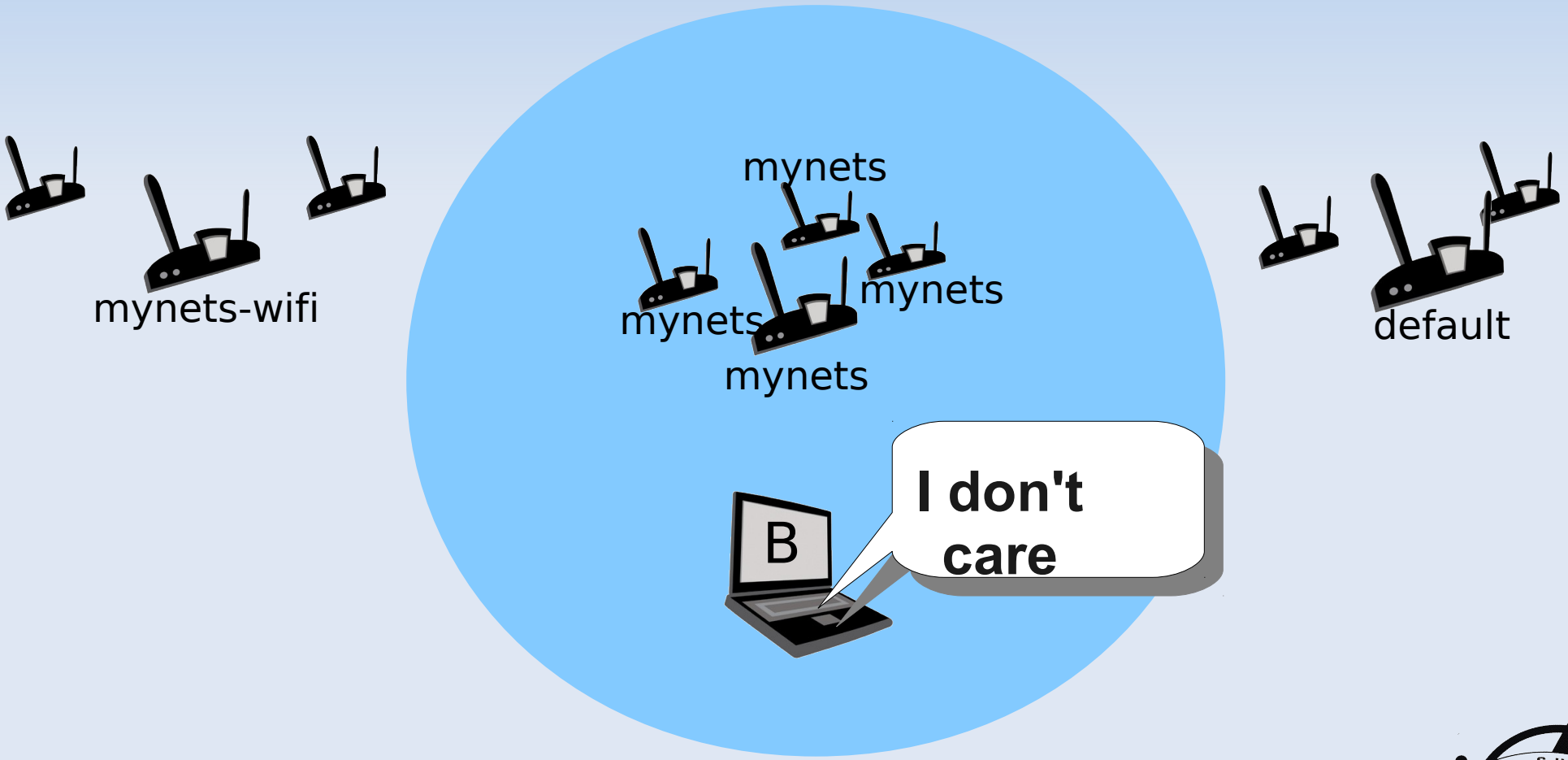
Scenarios
checking for similar essids via RegEX

beholder **-r “myne[t7]s.*”** wifidev



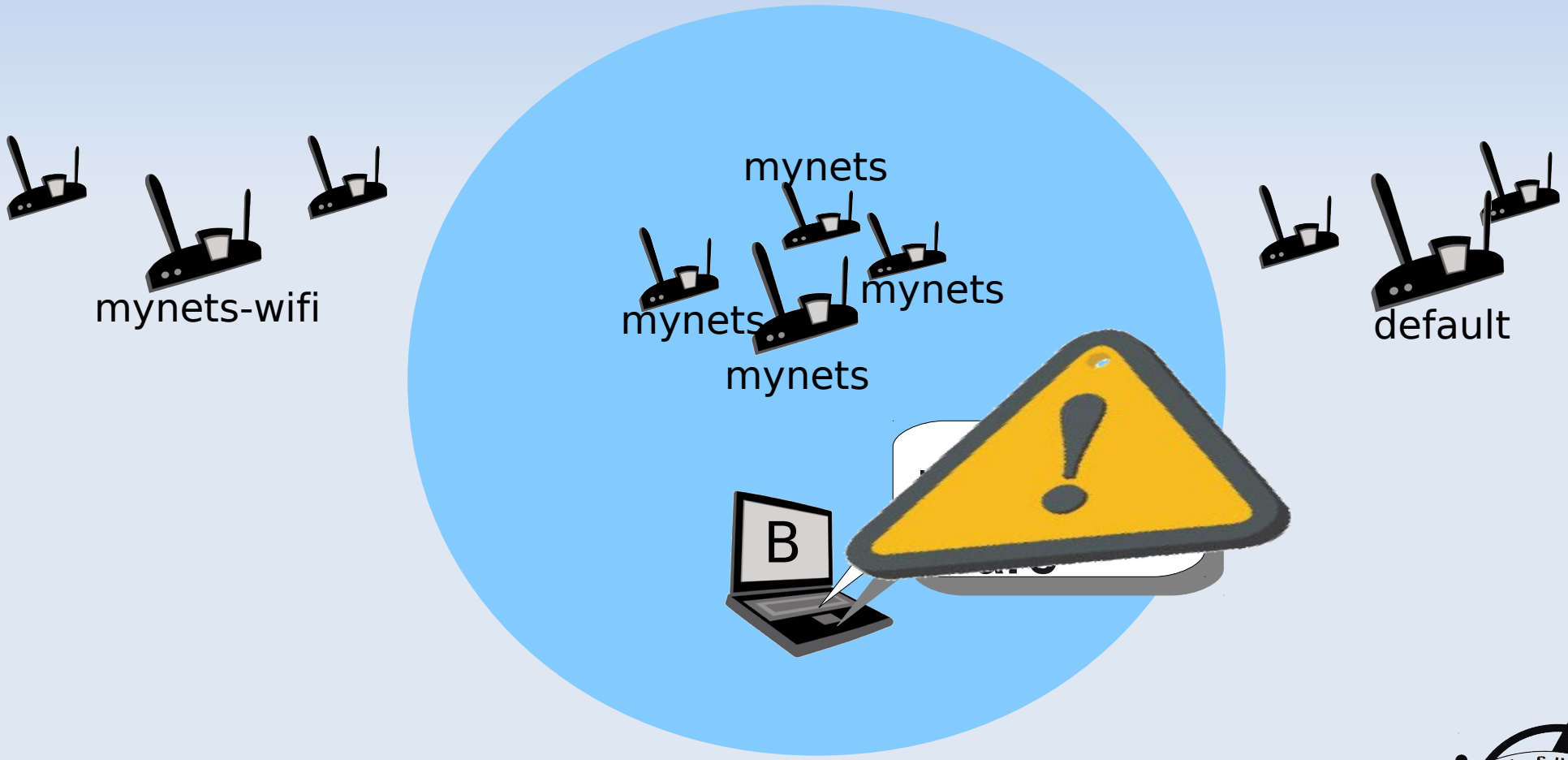
Scenarios
checking for similar essids via RegEX

beholder **-r “myne[t7]s.*”** wifidev



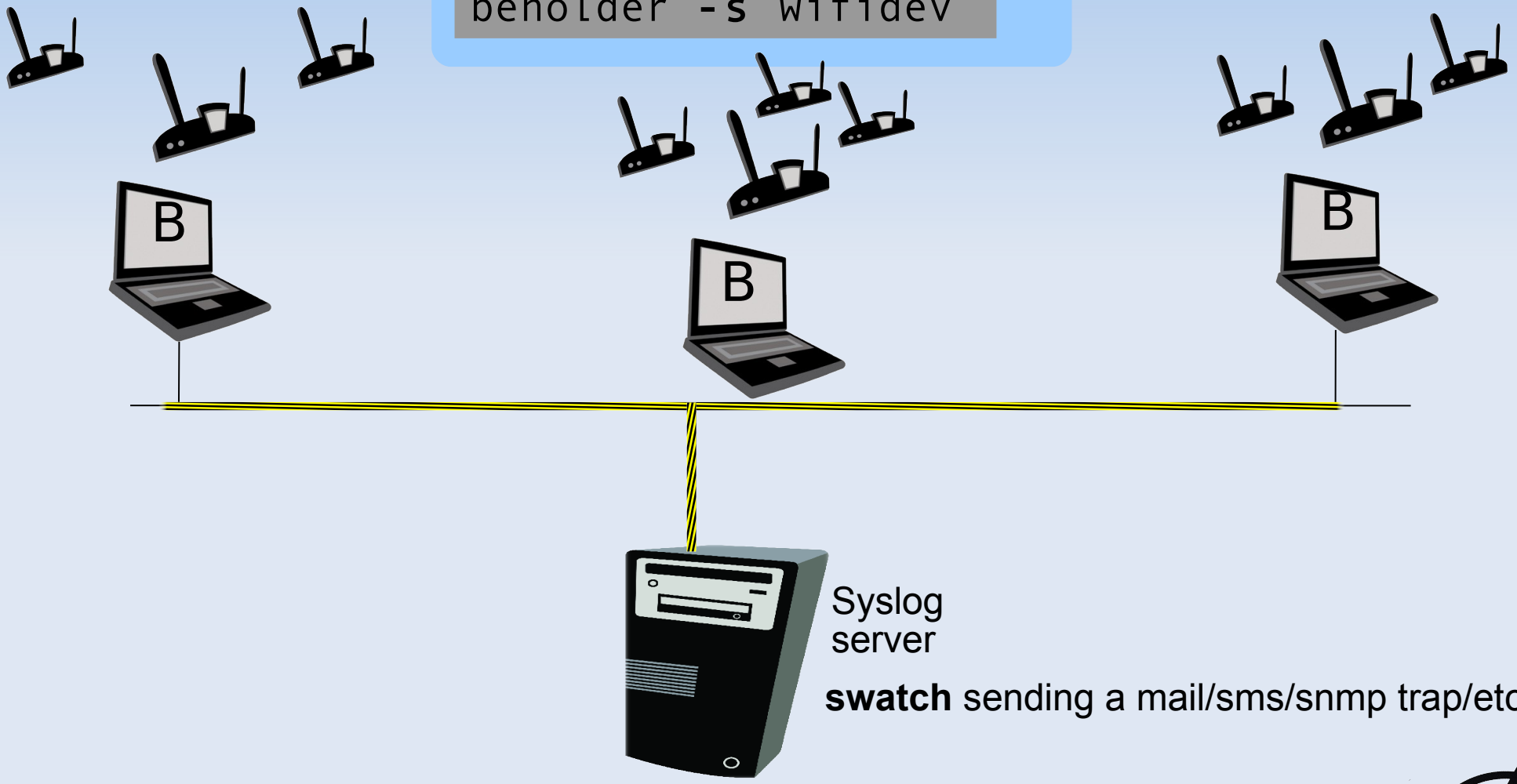
Scenarios
checking for similar essids via RegEX

```
beholder -r “myne[t7]s.*” wifidev
```



Scenarios
Large environments

```
beholder -s wifidev
```



Syslog server

swatch sending a mail/sms/snmp trap/etc

Let me see the code

BEHOLDER Code

Detect, Regex, Etc.

IWLIST Code

Beacons, WiFI interface

Hardware

Let me see the code

Struture

- Initial scanning
- Infinite loop
  - Jamming detection
  - AP/AD-Doc detection
  - Anommalies detection
    - Changes on Mac, Channel, mode, etc.
    - Similar names (essid) detection
    - Missing APs detection
  - Random requests (karma detecion)
  - Look for karma responses

Let me see the code

REGEX implementation:

Two functions

Compile:

```
int regcomp(regex_t *preg, const char *regex, int cflags);
```

Compare:

```
int regexec(regex_t *preg, const char *strings, size_t nmatch,,
regmatch_ pmatch[], int eflags);
```

Let me see the code

Karma detection

```
char *karma_trap(int skfd, const char *dev){
   struct iwreq wrq;
   [...]
   char essid[KARMA_TRAP_LEN] = "XXXXXX";
   [...]
   // Create a random ESSID
   mktemp(essid);
   wrq.u.essid.pointer = (caddr_t) essid;
   [...]
// Set random ESSID
   if(iw_set_ext(skfd, dev, SIOCSIWESSID, &wrq) < 0)
   [...]
  // Get random ESSID
   if(iw_get_ext(skfd, dev, SIOCSIWESSID, &wrq) < 0)
```

Let me see the code

Jamming detection

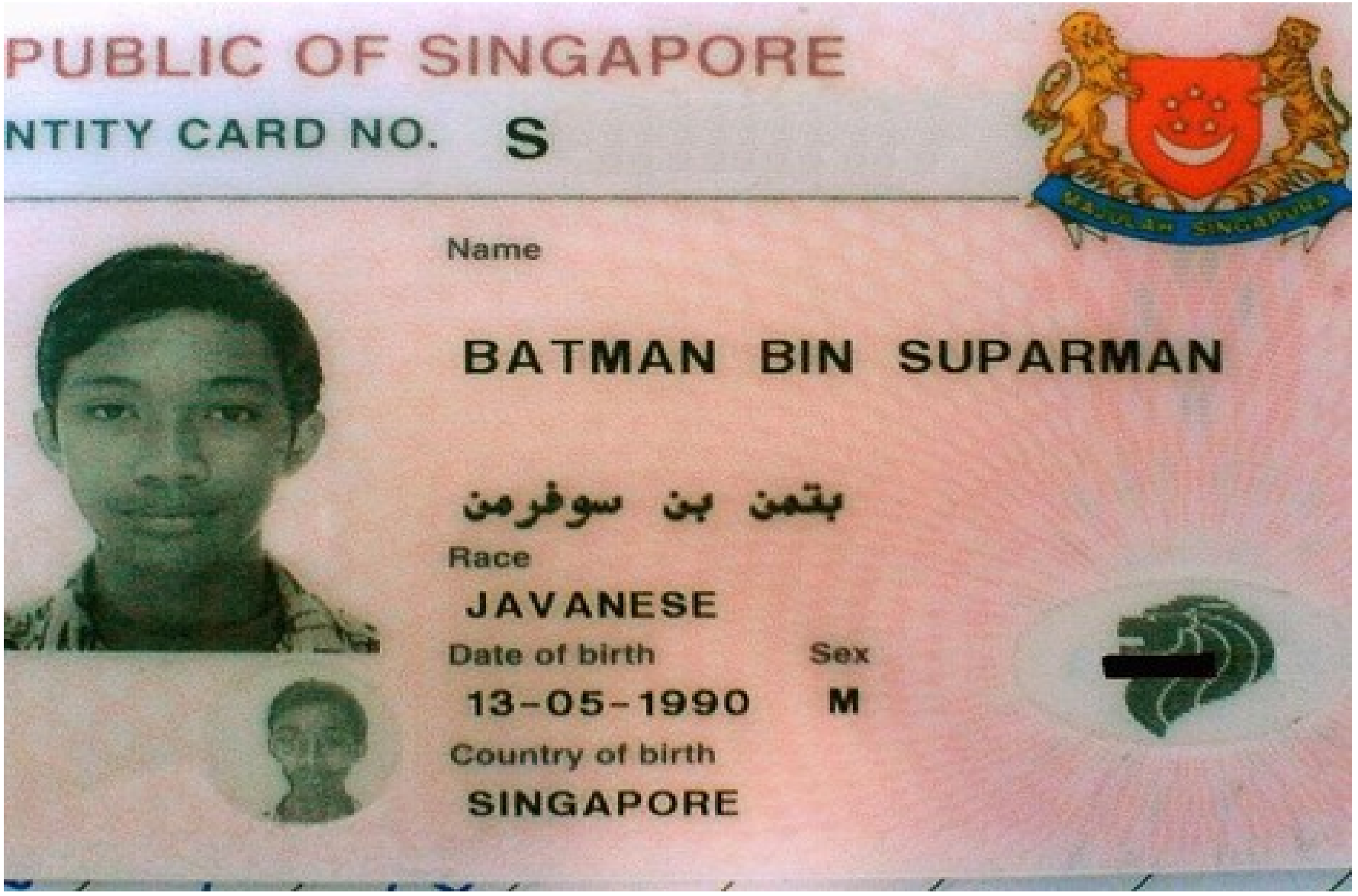
```
while (ap_temp)
 {
        if (!wscan_init) /* AP table empty */
        {
           jam++;

           if (jam == 3) // if table empty after 3 seq scanning
           {
              print_out(slog, "ALERT: Danger, Will Robinson!
Jamming device detected\n");
              break;
           }
        }
  }
```

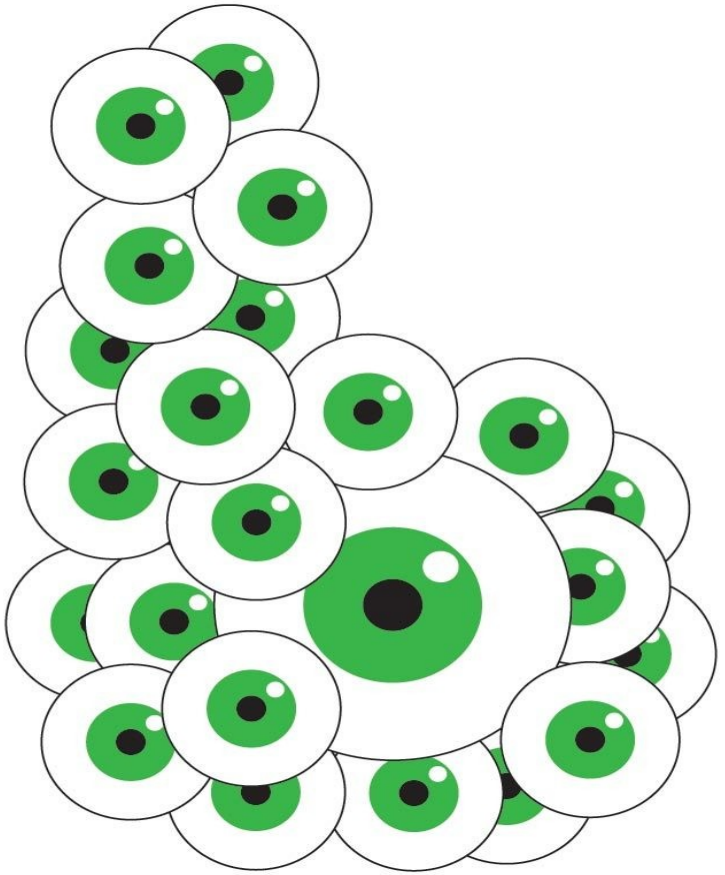
Demo?

Rembember:

Help doesn't always come from where you expect



Pick one free



http://www.beholderwireless.org


12