How Guestnet is Magic

Tim Clark (eclipse)

February 24, 2011

What is Guestnet

- Lets you connect to the SUCS network
- SUCS has a theoretical 1Gbps link to the internet
- Wired guestnet gets this link
- Wireless guestnet gets however much you can squeeze out of the wireless

Old guestnet

- A wired switch
- Some iptables rules
- Some weird dhcp stuff
- Some scripts

New Guestnet

- A wired switch
- A wireless card in gateway
- Some iptables rules
- Some ebtables rules
- Freeradius
- hostapd
- Some scripts

Wireless Basics

- LDAP stores who is who and who can log in
- Freeradius is a RADIUS server for authentication some glue
- hostapd can turn some wireless cards into an access points
- hostapd can talk to a radius server for EAP authentication

RADIUS and EAP basics

- RADIUS = Remote Authentication Dial In User Service
- EAP = Extensible Authentication Protocol
- RADIUS talks EAP and talks to LDAP
- Client a.k.a. the users computer talks EAP to RADIUS via the access point(hostapd)
- There are different EAP types that work in a different way

EAP

- Need to pick an EAP type
- Need an EAP type thata allows freeradius to get plaintext passwords out of its end
- Needed so RADIUS can talk to LDAP as you need to tell LDAP plaintext for it to check if its correct
- EAP-TTLS is an EAP type that is something like a TLS tunnel in a TSL tunnel
- TTLS stands for Tunneled Transport Layer Security
- EAP-TTLS is a tunnel that you use another authentication type down
- We use PAP in the tunnel which is Password Authentication Protocol a.k.a. plaintext passwords

Basics

- Switch like before
- Bridge with the wireless interface
- Mark packets useing ebtables that are from the wireless or from the wired and with an authorised mac address
- Use iptables as before, but instead of useing ip address use if its marked tod ecide if its allowed.
- Give IP address to everyone but only let allowed mac addresses connect to anyware

Bridge

- A brige links multiple interfaces a.k.a. network ports
- Shows up on the computer as a new interface
- Appears to things on each side of the bridge as if they are on the same bit of network
- Works as the mac address level
- Has ebtables, which is like iptables but for the mac level
- ebtables can filter or mark packets based on a mac address list out of a file

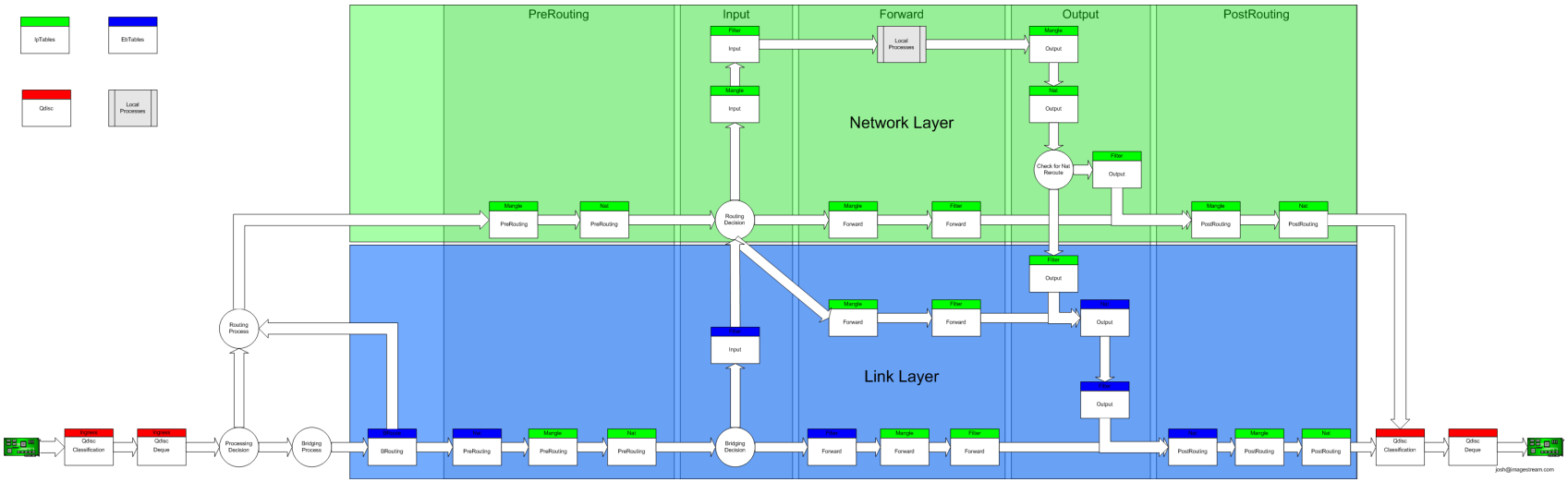
ebtables

```
ebtables -t nat -F PREROUTING
ebtables -t nat -A PREROUTING -i wlan0 -j mark
--mark-set 1
ebtables -t nat -A PREROUTING --among-src-file
/root/auth-mac -j mark --mark-set 1
ebtables -t nat -A PREROUTING -j mark --mark-set 0
```

IPtables

- iptables rules do different thigns depending on if the packets are marked
- If they are marked corrently, then let them talk to the outside world
- Authenticated mac addressed can't do everything, we arent stupid
- If http packets arent marked they get redirected to a thing that says how to register

Network Path



Scripts

- Scripts on silver update the file of allowed mac addresses from the database
- Scripts also reload the ebtables rules to apply the new mac address list

Broken bits

- Bounce/registration page doesnt work
- TTLS with PAP isnt very well supported by clients
- hostapd seems to have problems with people connecting
- hostapd seems to do weird things if lots of people try to connect
- There seems to be something up with DHCP

The Internet

Slides Available at `http://sucs.org/~eclipse`

Questions?

Any Questions?