Be your own telephone company...

...with Asterisk!

Presented by
Strom Carlson and Black Ratchet
DEFCON 13
July 2005

Brief history of telephone switching

- Manual cordboards
  - Labor-intensive
- Step / Panel / Crossbar
  - Electromechanical
  - Simple and effective, but limited in function
  - Expensive to maintain
- No. 1 / 1AESS
  - Electronically-controlled analog switching
  - Much wider array of services available
  - More flexibility than electromechanical switches
  - Some still in use today in North America

Brief history of telephone switching

- 4 ESS / 5 ESS / DMS
  - Digital time-division switching
  - Greatly increased flexibility and array of services
  - Much cheaper to maintain than previous systems
  - Huge and expensive

Part I:
Asterisk Overview
(or... what the &$#%@ is this thing?)

What is Asterisk?

- Free, open-source PBX that runs on Linux
  - Best thing since sliced bread
- Originally written by Mark Spencer
  - Now has a large number of contributors

Why Asterisk?

- It's FREEEEEEEEEEEEEEEEEEEEEE!!!!!!!
  - How much are you paying your PBX vendor now?
- Runs on commodity PC hardware
- Broad support for VoIP protocols and hardware
- Easy to interconnect with other boxes
  - Form your own VoIP network
- Configurable to do (almost) whatever you want
  - Tweak it to your needs
  - Write your own code
  - It will still not do your dishes, unfortunately

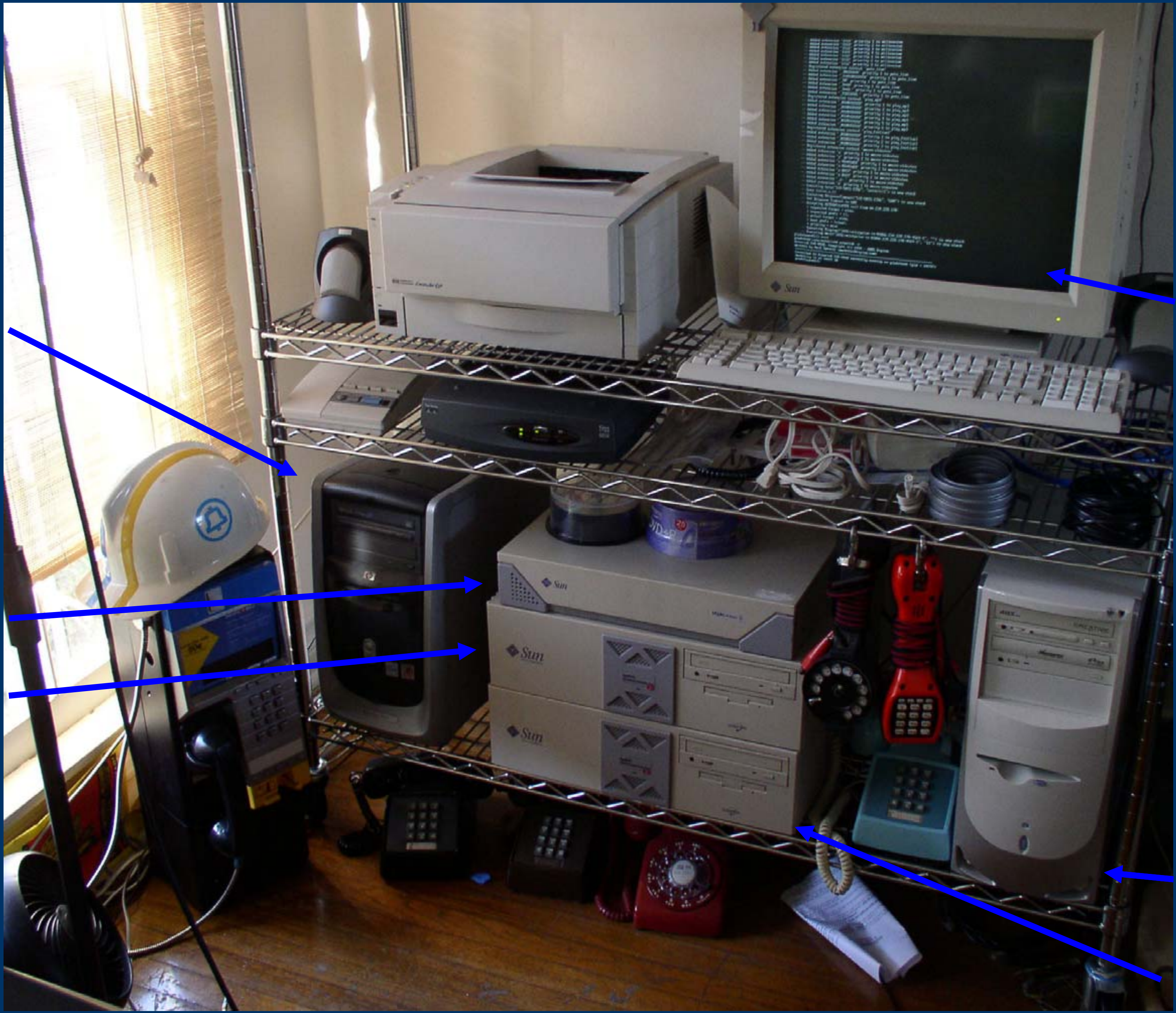
Asterisk and Hardware

Asterisk Hardware Requirements

- Will run on surprisingly out-of-date hardware
  - 133MHz Pentium I w/16MB RAM
    - supports 3 concurrent SIP calls before quality degrades
- Any PC you have lying around will work
  - 2.4 GHz P4 w/512 MB RAM
    - 790 simultaneous calls

http://www.voip-info.org/wiki-Asterisk+dimensioning

Sample Asterisk Installation



Asterisk

Catsex

Mail

Asterisk Console

NAS

Web

Popular VoIP Telephones

Cisco 7960
$250-$300

Polycom IP600
$250-$300

Grandstream
BudgeTone 100
$40-$75

Snom 190
$175-$250

Popular VoIP Terminal Adapters

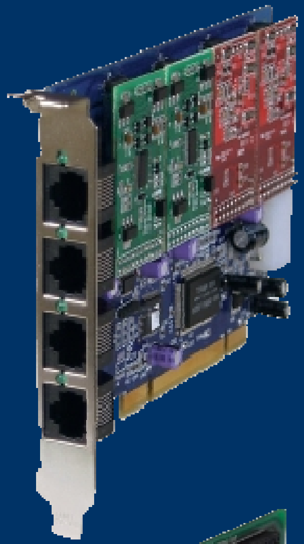
Digium IAXy
$100

Sipura SPA-2002
$70

Grandstream
HandyTone 286
$65

Cisco ATA-186
$50-$125

Digium Zaptel Cards



- TDM400P
  - Connect analog telephones to asterisk box
  - Connect analog telephone lines to asterisk box

- TE405P / TE410P
  - Connect four T1 / E1 circuits to asterisk box
  - Connect channel banks to asterisk box

Interconnecting Asterisk: Signaling Protocols

Session Initiation Protocol (SIP)

- Signaling protocol only
  - Actual media transport handled by RTP
- Protocol developed by IETF, not ITU-T
  - Uses URLs instead of telephone numbers
    - sip:strom@stromcarlson.com
- Intended to be a peer-to-peer protocol
- Fairly ubiquitous
  - Most VoIP phones, terminal adapters, etc speak SIP
  - Used by Vonage, Packet8, Broadvoice, etc
- Does not play well with NAT

H.323

- Developed in 1996 by ITU-T
- Far more similar to traditional telephony signaling protocols than SIP
- Uses RTP for media transport
- Used internally by interexchange carriers
- Fairly unpopular in the do-it-yourself VoIP world
  - Difficult to implement in software
  - Major pain in the ass to get working correctly

“Just don't use H.323 and all your problems will be solved”
- JerJer on #asterisk

Inter-Asterisk EXchange (IAX)

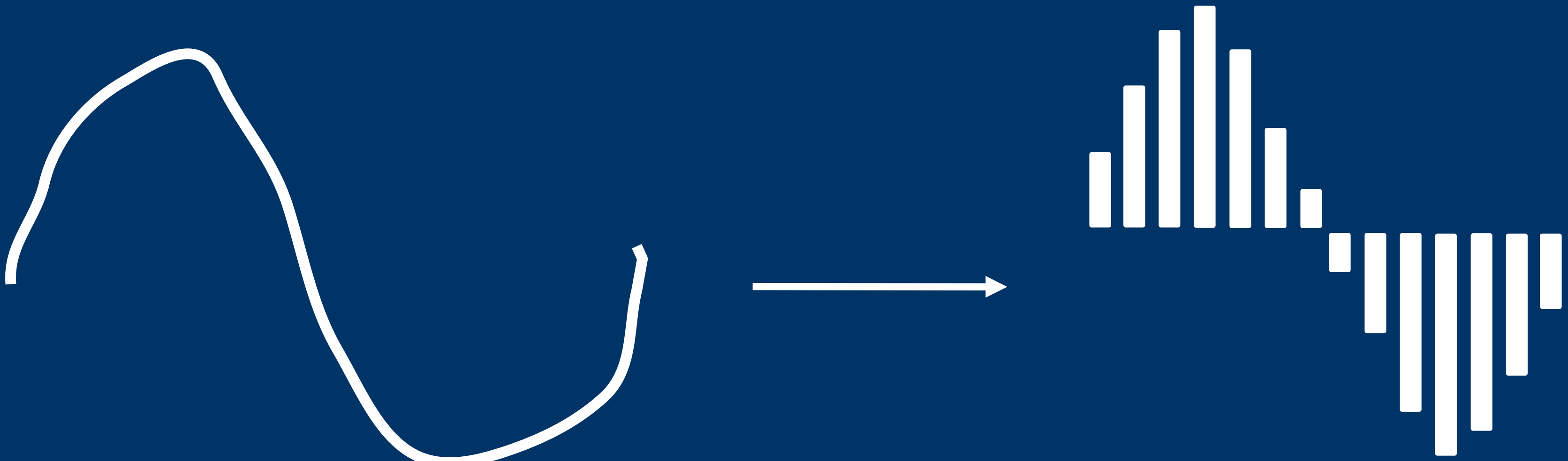
- Developed by Mark Spencer of Digium
- Covers both signaling and media transport
  - Streamlined, simple protocol
- Does not suffer from NAT traversal issues
  - Data and signaling happen via UDP on port 4569
- Well-supported by Asterisk
- Support in terminal equipment is rare
  - Digium IAXy terminal adapter speaks IAX
- Preferred protocol for many PSTN termination providers

Other protocols

- Media Gateway Control Protocol (MGCP)
- Cisco's Skinny Client Control Protocol (SCCP)

Interconnecting Asterisk: Codecs

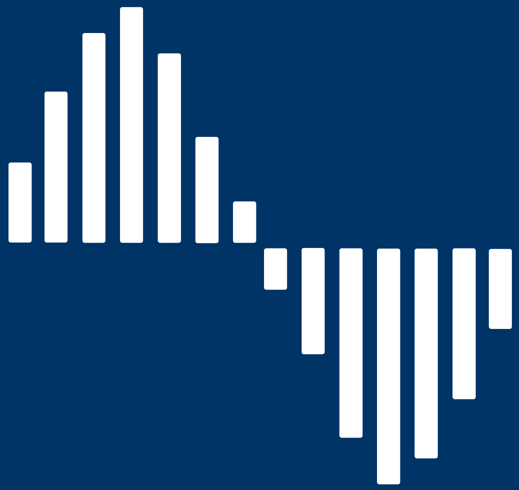
Digital Audio Basics – PAM



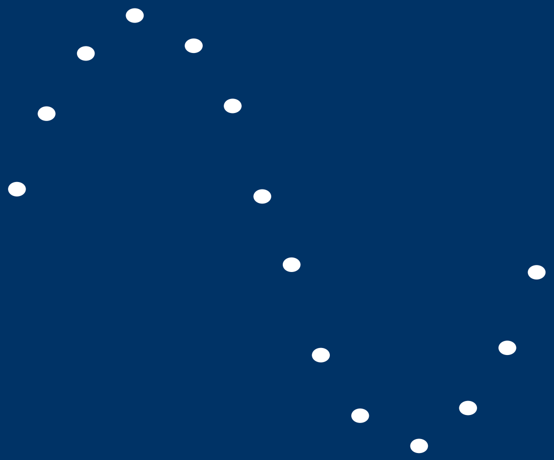
Analog Waveform

Pulse Amplitude
Modulation (PAM)

Digital Audio Basics – PCM

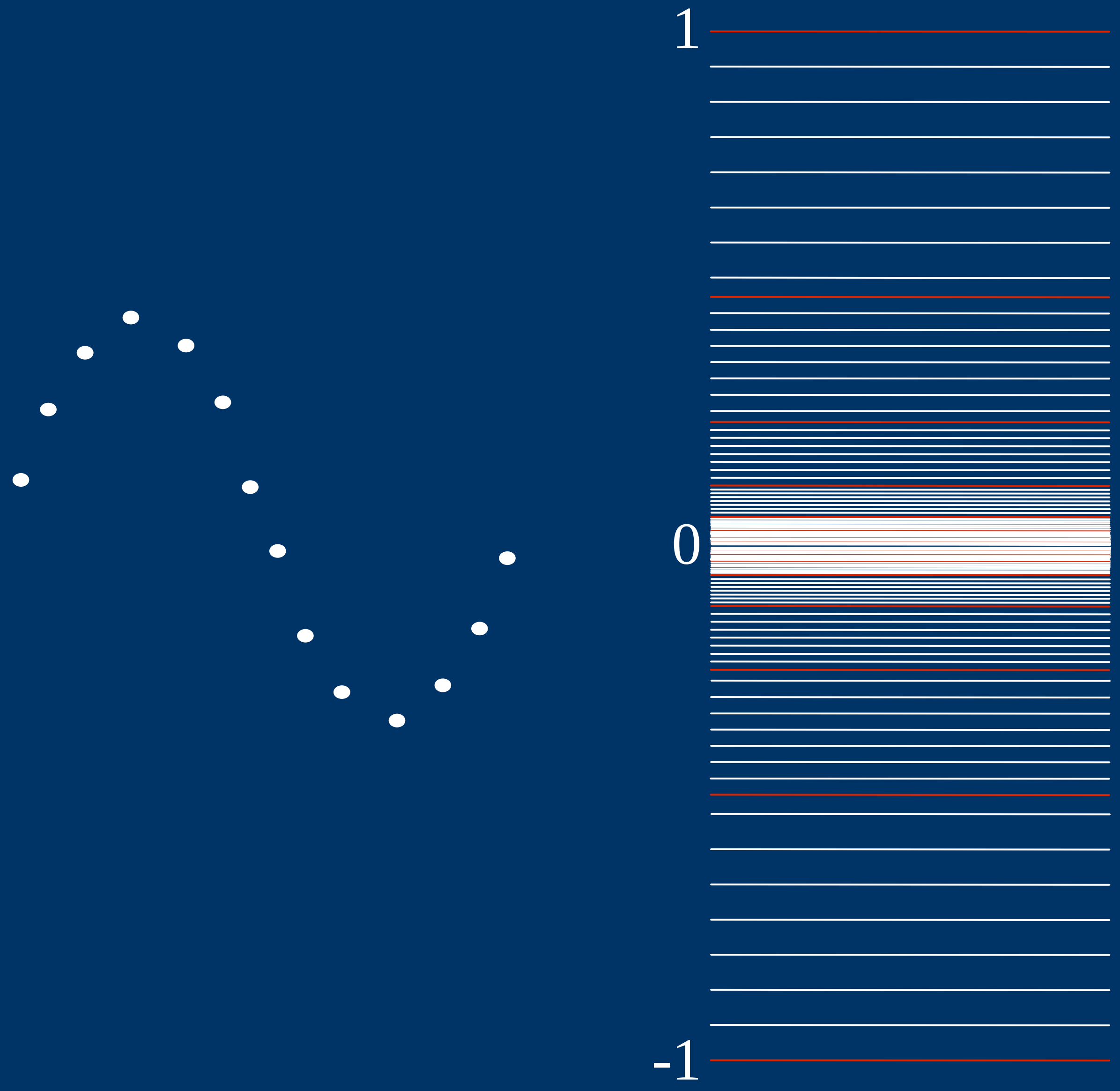


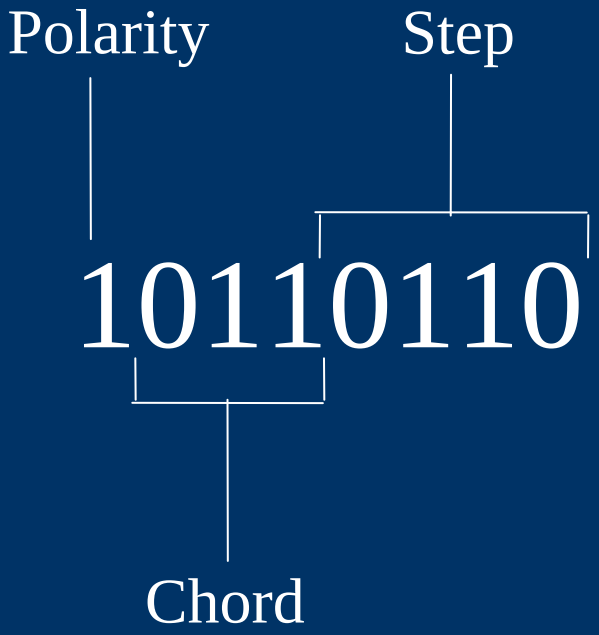
Pulse Amplitude
Modulation (PAM)



Pulse Code Modulation
(PCM)

Digital Audio Basics – μ-law





Polarity

Step

10110110

Chord

Digital Audio Basics – (A)DPCM

- Differential Pulse Code Modulation
  - Uses four bits to describe the change from the last sample, regardless of original source resolution
- Adaptive Differential PCM
  - Uses a varying number of bits depending on the complexity of the sample

Digital Audio Basics – LPC

- Linear Predictive Coding
- Uses vocoders to compress speech
  - Vocoders are also used to create the “singing synthesizer” effect in some modern music

Voice on the PSTN

- 64 kilobit per second synchronous bandwidth for wireline telephones
  - µ-law companding in North America
  - a-law companding in the rest of the world
  - 56 kilobits per second if doing in-band supervision signaling on a DS0 (i.e. bit-robbing)
- 4 to 13 kilobit per second synchronous bandwidth for mobile phones
  - All sorts of crazy audio codecs
  - Sounds like crap

Costs of speech compression

- Increased CPU power required for transcoding
- No guarantee that two pieces of equipment will speak the same codecs
  - Especially true if using nonstandard bitrates
- Some codecs require LICEN$ING
- Codecs do not handle all kinds of sounds well
  - People will have trouble understanding certain words
  - Difficult to understand anyone who has poor diction
  - Music on hold in codec land is pure torture
    - Be like Oedipus! Gouge your eyes out!

Benefits of speech compression

- Each call uses less bandwidth

Codecs supported by Asterisk

- G.711
  - 64kbps μ-law or a-law companding
- G.726
  - 32kbps Adaptive Differential Pulse Code Modulation
- G.729
  - 8kbps Conjugate-Structure Algebraic Code-Excited Linear Prediction
  - Requires a license
- GSM
  - 13kbps Regular Pulse Excitation Long-Term Prediction

Codecs supported by Asterisk

- Internet Low Bandwidth Codec (iLBC)
  - 13.3kbps Linear Predictive Coding
  - This is the codec used by Skype
- Speex
  - 13.3kbps Code-Excited Linear Prediction
  - Open Source codec
- LPC10
  - 2.4kbps Linear Predictive Coding
  - Sounds more ghastly than you can possibly imagine

Codec Comparison Audio Demo

Music:
Redeye Flight - “Natalie”
(band from Los Angeles – they're cool – go see their shows)
redeyeflight_band@yahoo.com

Codec Comparison Audio Demo

5

Music:
Redeye Flight - “Natalie”
(band from Los Angeles – they're cool – go see their shows)
redeyeflight_band@yahoo.com

Codec Comparison Audio Demo

4

Music:
Redeye Flight - “Natalie”
(band from Los Angeles – they're cool – go see their shows)
redeyeflight_band@yahoo.com

Codec Comparison Audio Demo

3

Music:
Redeye Flight - “Natalie”
(band from Los Angeles – they're cool – go see their shows)
redeyeflight_band@yahoo.com

Codec Comparison Audio Demo

2

Music:
Redeye Flight - “Natalie”
(band from Los Angeles – they're cool – go see their shows)
redeyeflight_band@yahoo.com

Codec Comparison Audio Demo

1

Music:
Redeye Flight - “Natalie”
(band from Los Angeles – they're cool – go see their shows)
redeyeflight_band@yahoo.com

G.711

64kbps μlaw companding

G.729

8kbps

Conjugate-Structure Algebraic Code-Excited Linear Prediction

G.726

32kbps Adaptive Differential Pulse Code Modulation

GSM

13kbps Regular Pulse Excitation Long-Term Prediction

G.711

64kbps µlaw companding

iLBC

13.3kbps Linear Predictive Coding

LPC-10

2.4kbps Linear Predictive Coding

Speex

13.3kbps Code-Excited Linear Prediction

Interconnecting Asterisk: PSTN Termination

NuFone

- Pros
  - Cheap rates
  - Geared for Asterisk
  - Spoofable CallerID
  - Insanely easy to provision 800 numbers
  - Very easy going
  - Calling Party Number delivery
  - Proper call completion progress
- Cons
  - Michigan DIDs only
  - Not too phreak friendly
    - Disabled Caller ID spoofing during DC12 (Geee, think he doesn't trust us?)

Asterlink

- Pros
  - Reliable
  - Inbound via tollfree numbers
  - Delivers ANI II if you want it
  - Proper call progress
- Cons
  - Kludgy account management interface

Voicepulse Connect

- Pros
  - Unlimited incoming minutes on inbound IAX calls
  - Inbound numbers in a large number of rate centers
  - Proper call progress
- Cons
  - One of the most expensive IAX providers for outbound PSTN call termination

VoipJet

- Pros
  - Cheap! (1.3 cents per minute)
- Cons
  - Caller ID delivery unreliable
  - No incoming service
  - No proper call completion
    - Instead of hearing an intercept message, you'll just hear ringing

BroadVoice

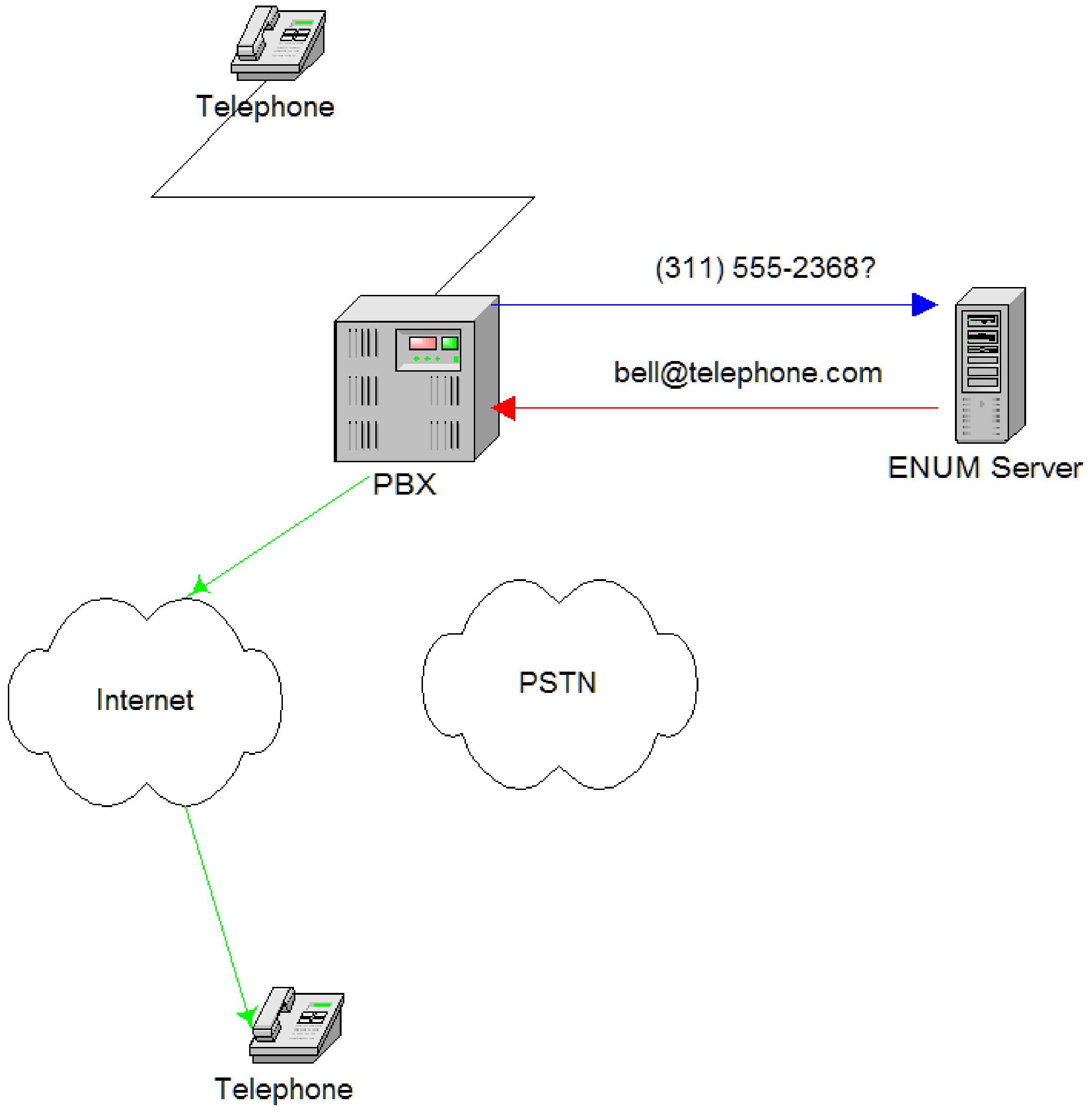
- Pros
  - Cheap DIDs in most ratecenters
  - Run by phone phreaks
  - 24/7 Phone Support
  - Caller ID with name
- Cons
  - SIP Only
  - Prone to service outages
  - Phone support is slow at best
  - Will CNAM work today?

Interconnecting Asterisk: Network Design

ENUM / E.164

- Based on DNS
- Allows any number to be queried
  - If it exists, you can bypass the PSTN saving money.
- Designed by the ITU
- Officially 'supposed' to be used by Telcos
  - e164.org – Free DIY solution
    - Over 350,000 Numbers on record
    - 78,000,000 Special PSTN services (800 numbers, etc)

How ENUM Works



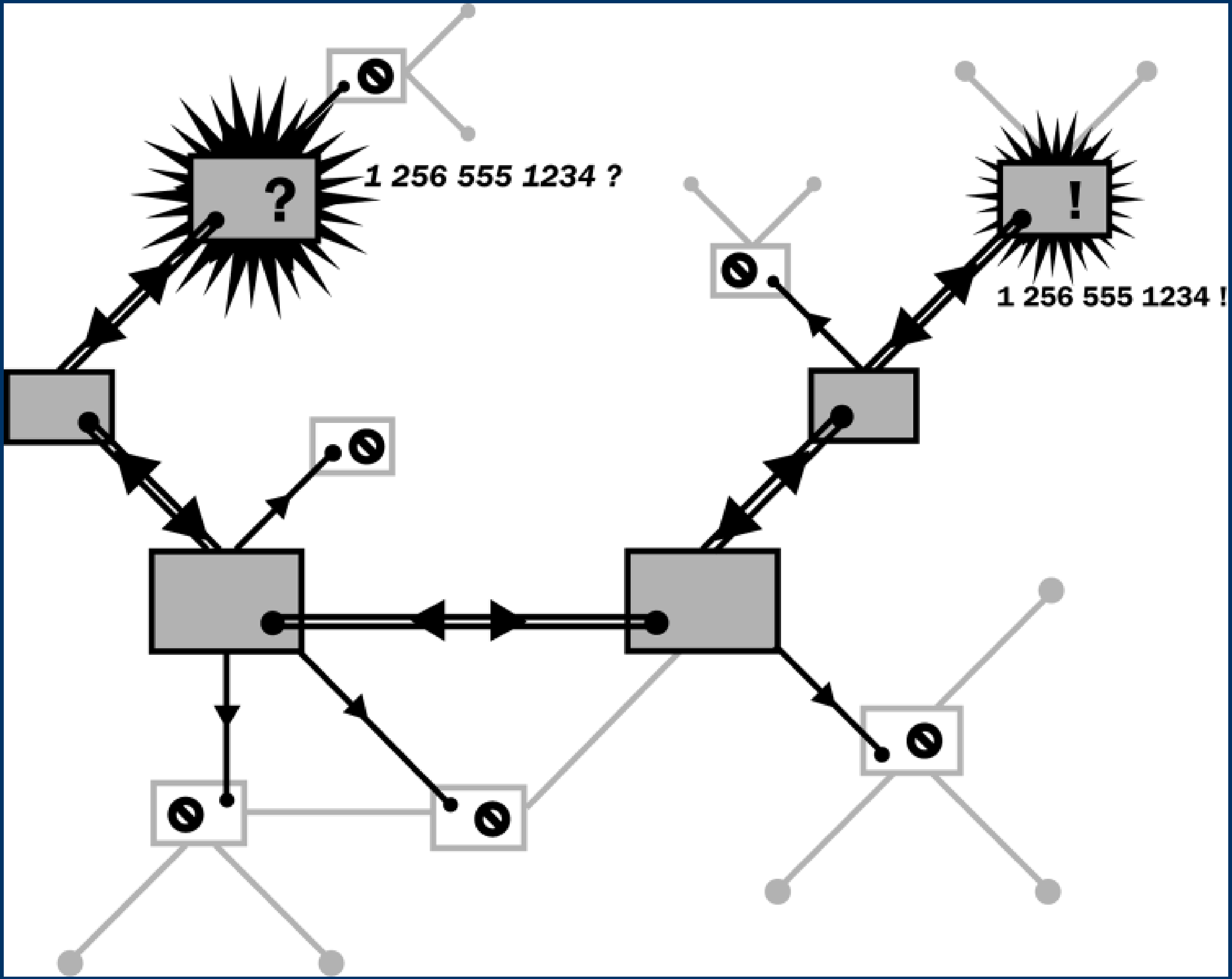
ENUM problems

- A very 'top-down' way of doing lookup
  - Centrally managed
  - Centrally served
  - Centrally centralized
- Not in use by any(?) PSTN providers
  - Why should they save YOU money?
- Nowhere near critical mass yet

DUNDi - Distributed Universal Number Discovery

- Designed by the good folks at Digium
  - Therefore, it has to be good
- A fully peer-to-peer E.164 solution
- Easily set up your own telephone network with friends
- DIY alternative to waiting for your telephone company to implement E.164

How DUNDi works



http://www.dundi.com/dundi-e164-big.png

DUNDi Problems

- Requires everyone to be honest
  - Hey Hey! I'm the white house!
- Scalability
- Not officially a standard (yet)
- Only in CVS HEAD version of asterisk
- The 'i' looks silly at the end.

Quality of Service

- Ensure that calls receive enough bandwidth and low latency
  - Priority Queueing
  - Bandwidth Shaping
- Many residential routers are now VoIP-aware and will do a decent job out-of-the-box
- Tweak a Cisco router to do this on a large scale or if you're a control freak

Part II:
Extending Asterisk

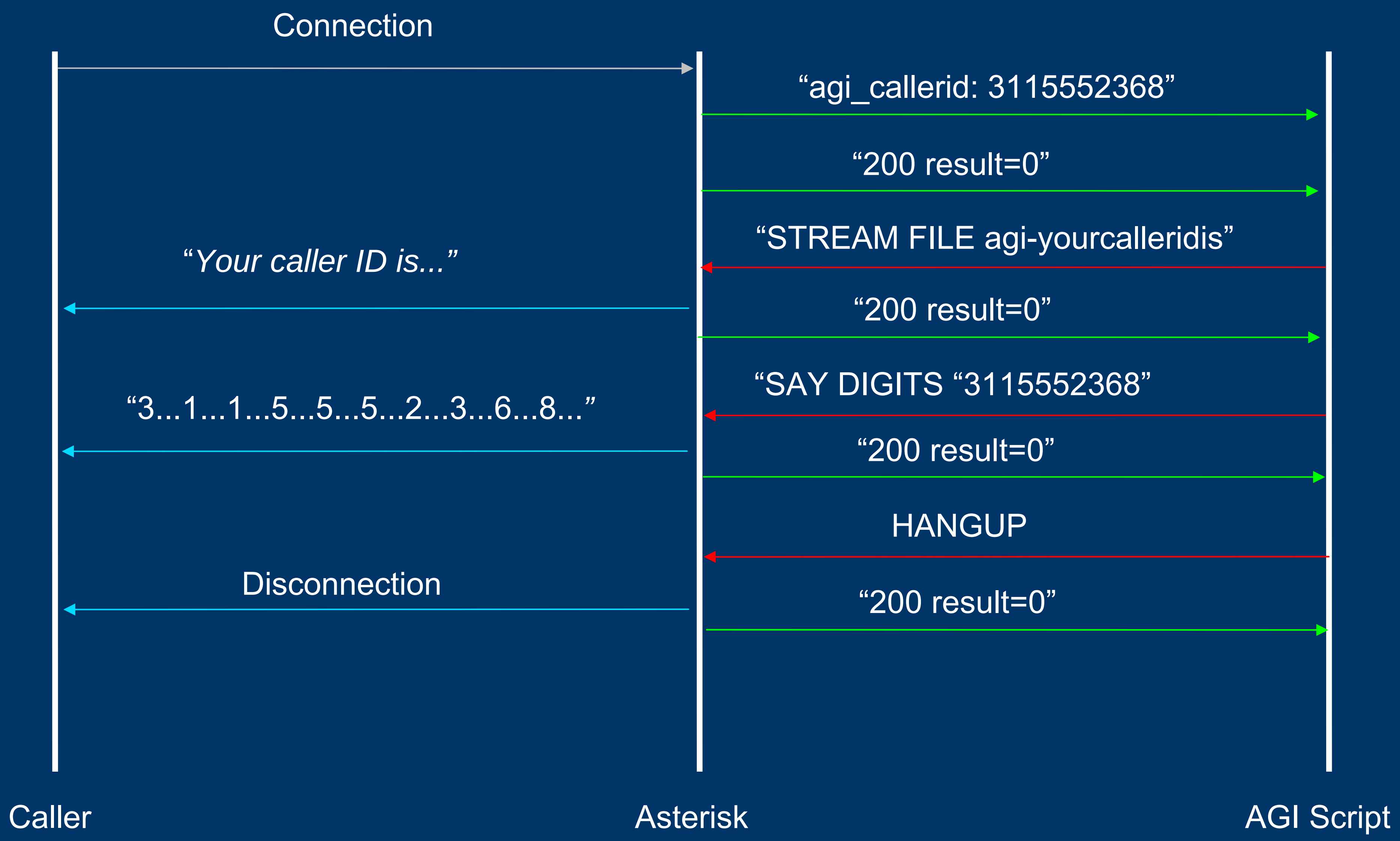
AGI – Asterisk Gateway Interface

- Interface for adding functionality to Asterisk
- Cross-Language
  - Perl
  - C
  - PHP
  - Whatever you want...
- Allows programs to communicate to asterisk via STDIN and STDOUT
- Second-best thing since sliced bread

A simple AGI program

```
#!/bin/bash
#
# Simple agi example reads back Caller ID
#
# Written by: Black Ratchet <blackratchet@blackratchet.org>
#

# Suck in the variables from asterisk
declare -a array
while read -e ARG && [ "$ARG" ] ; do
    array=(` echo $ARG | sed -e 's/://'`)
    export ${array[0]}=${array[1]}
done

checkresults() {
    while read line
    do
    case ${line:0:4} in
    "200 " ) echo $line >&2
             return;;
    "510 " ) echo $line >&2
             return;;
    "520 " ) echo $line >&2
             return;;
    *      ) echo $line >&2;;   #keep on reading those Invalid command
                    #command syntax until "520 End ..."
    esac
    done
}

# Say the user's Caller ID
echo "STREAM FILE yourcalleridis \"\""
checkresults

echo "SAY DIGITS " $agi_callerid  "\"\""
checkresults
```

How it works...


Connection
“agi_callerid: 3115552368”
“200 result=0”
“STREAM FILE agi-yourcalleridis”
“Your caller ID is...”
“200 result=0”
“SAY DIGITS “3115552368”
“3...1...1...5...5...5...2...3...6...8...”
“200 result=0”
HANGUP
Disconnection
“200 result=0”
Caller
Asterisk
AGI Script

Asterisk::AGI

- Perl module that simplifies AGI programming
  - Takes care a lot of the 'dirty work'
  - “Doing the work so you don't have to”
- Allows the AGI interface to be controlled via an object interface
- Rather old; not very well maintained
- Allows AGI to easily integrate with Perl, which easily integrates with almost everything in the known universe.
- http://asterisk.gnuinter.net/

A simple AGI program w/Asterisk:AGI

```
#!/usr/bin/perl
#
# Simple AGI example that says the Caller ID w/Asterisk::AGI
#
# Written by: Black Ratchet <blackratchet@blackratchet.org>
#


use Asterisk::AGI;

$AGI = new Asterisk::AGI;

# Suck in the variables from asterisk
my %input = $AGI->ReadParse();

# Speak the user's caller ID (If they have one)
if ($input{'callerid'}) {
        $AGI->stream_file('yourcalleridis');
        $AGI->say_digits($input{'callerid'});
}
```

Wow... That was easier...

Interacting with your script - Input

- Touch Tone
  - Basic
  - Ubiquitous
  - Easy
  - Limited
- VXML
  - eXtensible
  - No native support
  - SIPxPBX
  - Numerous Commerical offerings

Interacting with your script - Output

- Text to Speech
  - Festival
    - Native Support
    - Free
    - Sounds like crap
  - Cepstral
    - Can easy be integrated
    - Sounds great
    - Not free, but cheap

Interacting with your script - Output

- Recordings
    - Do it yourself
        - Free
    - Allison Smith
        - For pay
        - Lots of canned sayings

A slightly more complex script...

```
#!/usr/bin/perl
#
# Simple agi example that demonstrates input and output
#
# Written by: Black Ratchet <blackratchet@blackratchet.org>
#


use Asterisk::AGI;

$AGI = new Asterisk::AGI;

while (1){
        $input = chr($AGI->stream_file('seeandsay/menu','123'));
        if ($input eq "1"){
                $AGI->stream_file('seeandsay/ratchet');
        }elsif($input eq "2"){
                $AGI-> stream_file('seeandsay/cepstralsays');
                $AGI-> stream_file('seeandsay/cepstral');
        }elsif($input eq "3"){
                $AGI-> stream_file('seeandsay/allisonsays');
                $AGI-> stream_file('seeandsay/allisonhello');
        }

}
```

(intermission)

Part II(a):
Cool Applications
(or... what can I do with this thing?)

Caller ID Spoofing

- Asterisk allows you to set your own Caller ID, much like a PRI
- Certain PSTN termination providers will also set your Calling Party Number of your SS7 IAM to this number as well
- Most switches blindly accept this information, some more then others
  - 5ESS – Caller ID
  - DMS-100 – Caller ID
  - GTD-5 – Caller ID with Name

Caller ID & CPN Spoofing uses...

- Confuse and Amuse your friends
  - How many times have you received a call from “Simpson, Homer J” ?
- Activate your neighbor's credit card
- Charge calls to people you don't like
  - Slightly more complex
  - Requires certain phone equipment to be misconfigured
  - Easiest way to do this is via a certain company's calling card

Caller ID & CPN Spoofing uses...

- Own Paris Hilton's voice mail
  - T-Mobile upgraded their system, but is still vulnerable
- Social Engineering
  - Because hey... Caller ID is always right... right?

Simple Caller ID Spoofing Scripts

- Nick84
  - http://www.rootsecure.net/
- NotTheory
  - http://www.bellsmind.net/

Backspoofing

- Related to Caller ID Spoofing
- Relatively new concept
  - NotTheory - http://www.bellsmind.net/
  - Natas - http://www.oldskoolphreak.com/
  - Vox - http://xscans.united.net.kg/
- Fools the phone company into providing the name associated with a telephone number
  - Listed and Unlisted

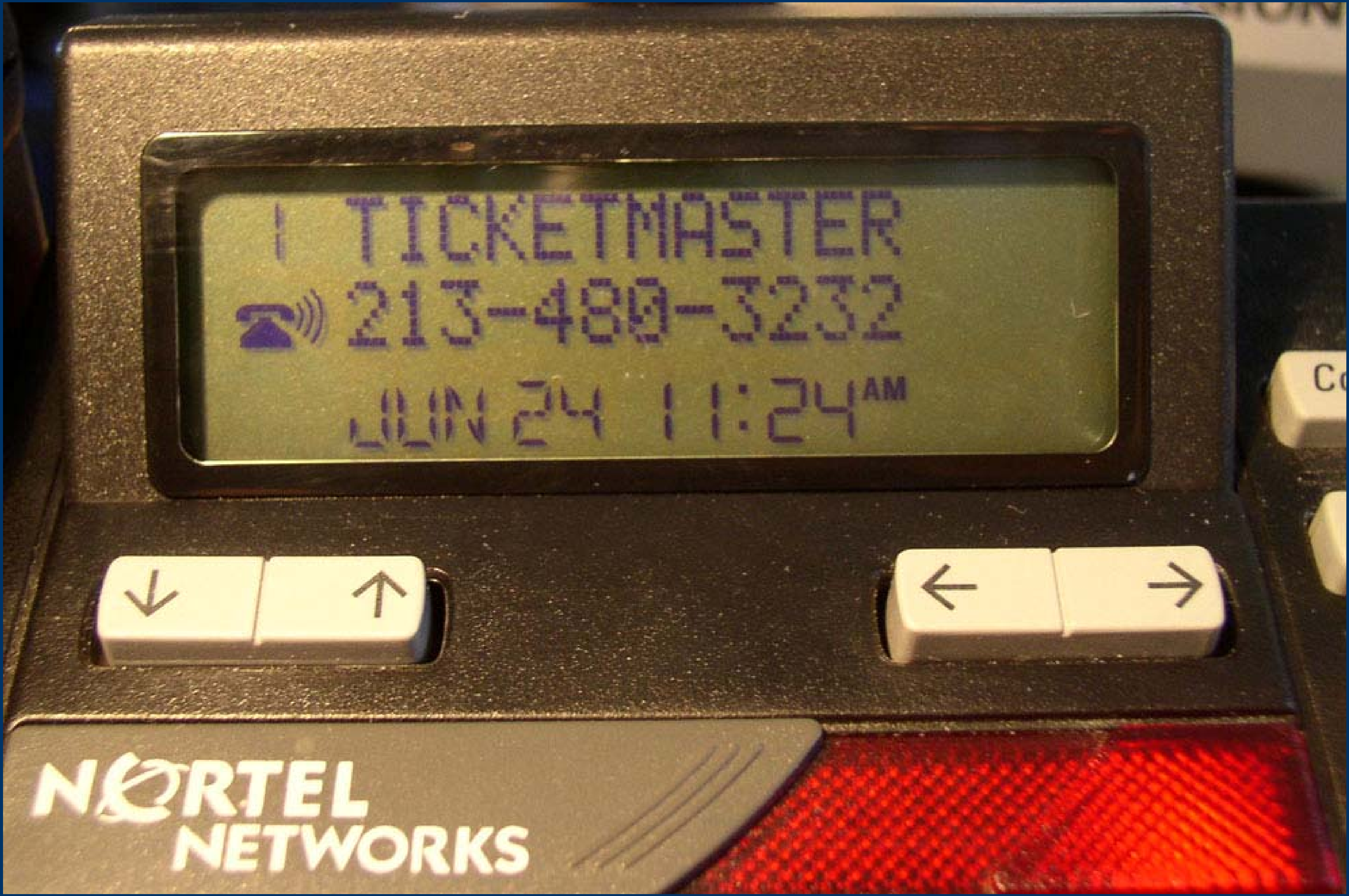
Backspoofing

- How it works
  - Spoof Caller ID to yourself
  - Your LEC looks up the number in its Caller ID database (CNAM)
  - You get the name associated with that number

Backspoofing Uses

- Prescanning
  - Allows you to prioritize the more interesting phone numbers.
    - “NET - 5ESS”
    - “OFC# 897 TEST L”
    - “VERIZON INFORMA”
    - “CIA, INTERNATION”
    - “BOOZE”
    - “UNCLAIMED MONEY”
- Uber-cheap reverse lookup
- Figure out celebrities' cell phone numbers
  - Lindsay Lohan
  - Nikki Hilton

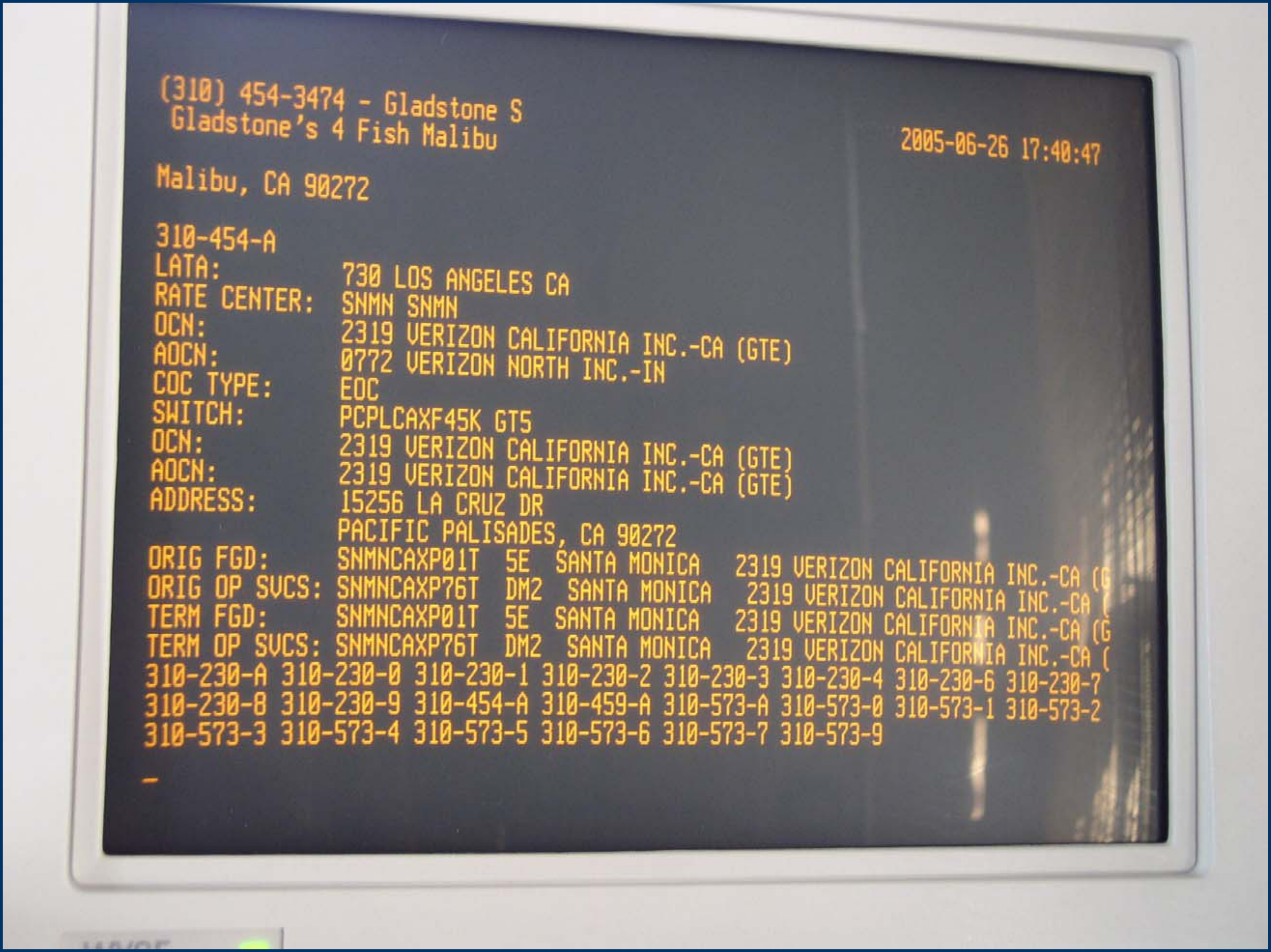
Backspoofing



Super Caller ID

- Extrapolates tons of useless data from a telephone number
  - Name and address from whitepages.com
  - Switch information from LERG
- Runs on its own dedicated WYSE 150
- Hacked up in an hour by Strom Carlson
- A less customized version (non-LERG) available at http://www.oldskoolphreak.com/

Super Caller ID



```
(310) 454-3474 - Gladstone S
 Gladstone's 4 Fish Malibu
                                                              2005-06-26 17:40:47
Malibu, CA 90272

310-454-A
LATA:          730 LOS ANGELES CA
RATE CENTER:   SNMN SNMN
OCN:           2319 VERIZON CALIFORNIA INC.-CA (GTE)
AOCN:          0772 VERIZON NORTH INC.-IN
COC TYPE:      EOC
SWITCH:        PCPLCAXF45K GT5
OCN:           2319 VERIZON CALIFORNIA INC.-CA (GTE)
AOCN:          2319 VERIZON CALIFORNIA INC.-CA (GTE)
ADDRESS:       15256 LA CRUZ DR
               PACIFIC PALISADES, CA 90272
ORIG FGD:      SNMNCAXP01T  5E  SANTA MONICA  2319 VERIZON CALIFORNIA INC.-CA (G
ORIG OP SVCS: SNMNCAXP76T  DM2  SANTA MONICA  2319 VERIZON CALIFORNIA INC.-CA (
TERM FGD:      SNMNCAXP01T  5E  SANTA MONICA  2319 VERIZON CALIFORNIA INC.-CA (G
TERM OP SVCS: SNMNCAXP76T  DM2  SANTA MONICA  2319 VERIZON CALIFORNIA INC.-CA (
310-230-A 310-230-0 310-230-1 310-230-2 310-230-3 310-230-4 310-230-6 310-230-7
310-230-8 310-230-9 310-454-A 310-459-A 310-573-A 310-573-0 310-573-1 310-573-2
310-573-3 310-573-4 310-573-5 310-573-6 310-573-7 310-573-9

_
```

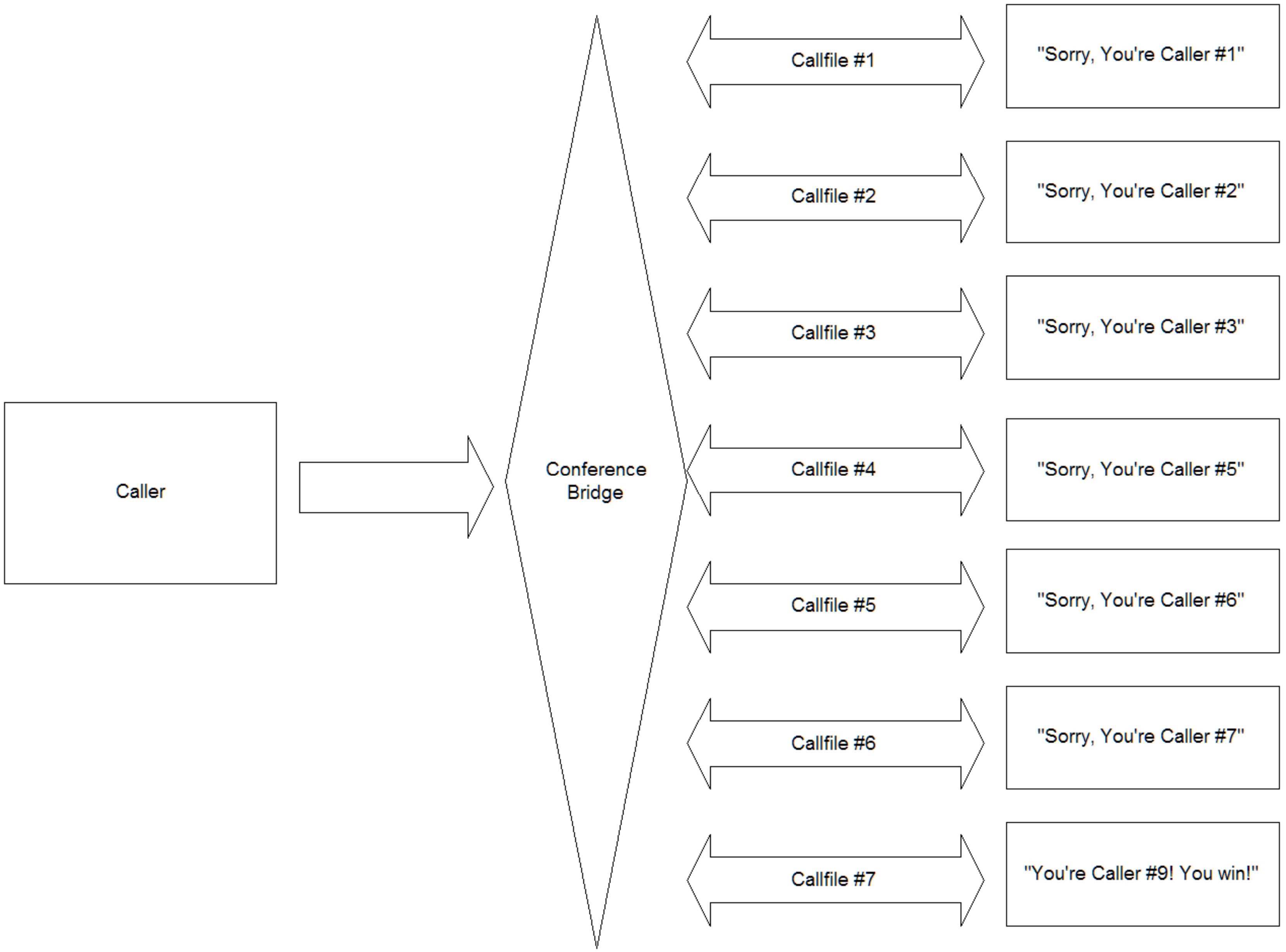
Rigging Radio Contests...

- Radio stations have a 'hunt group' for their contest lines
  - Hunt group – A single telephone number that 'hunts' for free wire pairs on a switch.
  - Back in the day, crackers would busy out hunt line at the switch, disallowing the public to call it, while calling the individual lines directly
  - Result: They win, public loses, line is re-enabled back after the contest, everyone is none the wiser.
  - Dark Dante (Kevin Poulsen) used this method to win a Porsche

Tipping the scales in your favor...

- Shouts to Natas & NotTheory
- Certain providers allow numerous simultaneous outbound calls (hundreds in some cases)
  - DS1 = 24 calls
  - DS3 = 672 calls
- Radio station hunt groups can have around 20 lines on their hunt group
- What happens if they are suddenly inundated with 300 calls?
  - Won't guarantee a win, but will definitely increase your chances

How it works


Caller
Conference Bridge
Callfile #1
Callfile #2
Callfile #3
Callfile #4
Callfile #5
Callfile #6
Callfile #7
"Sorry, You're Caller #1"
"Sorry, You're Caller #2"
"Sorry, You're Caller #3"
"Sorry, You're Caller #5"
"Sorry, You're Caller #6"
"Sorry, You're Caller #7"
"You're Caller #9! You win!"

Still some problems

- After you win, calls that are still in the queue will connect to the bridge if answered.
  - Radio Station Guy 1: “Hey! You win”
  - You: “Phonetastic!”
  - Radio Station Guy 2: “Hey, we already have a winner!”
  - Radio Station Guy 1: “Whaaaa?!”
- No easy way to fix this (?)

Other possible uses

- Rigging telephone voting contests
- Telephone DoS
- Telling PBS to wrap up their pledge break and get back to Red Dwarf
- Busying out lines
- Racking up 800 number charges

Nmap-by-phone

- Simple script that allows you to port scan from your phone
- Scan a computer from any payphone in the world
- Impress your friends
- Own microsoft.com while driving to work
- Almost but not entirely useless beyond the coolness factor

Your own personal assistant

- Read your e-mail over the phone
  - Can't dictate messages (Yet)
- Not as cool as WildFire or Webley
  - http://www.wildfire.com/
  - http://www.webley.com/
- Insanely cheaper than wildfire or Webley
- VXML would make this much much cooler

Part II(b) DEFCON by phone

DEFCON by Phone

- Problem: Massive Def Con Schedule
  - Hard to memorize
  - Times and locations change
  - “Was that presentation on Friday or Saturday?”
  - “Crap! I missed So-and-So's presentation!”
  - This is 2005! Who really wants to carry around a schedule made of dead trees?

DEFCON by Phone (cont.)

- Solution: Def Con By Phone!
  - Allows searching of Def Con schedule
  - Reminds users when presentations start
    - Reminders can be set for up to one hour before a presentation, allowing the user to get in line.
  - Alerts users to when a presentation changes
  - Allows users to keep “in touch” with the con despite their location (IE: Blackjack Tables!)
  - Allows users to get their *very own* phone call from Strom Carlson, phone phreak extrodanaire!

DEFCON by Phone (cont.)

- Features
  - Search available to anyone that calls
  - Quick reminder (Tells user what is coming in the next hour)
  - User Registration
  - Registered users can:
    - Add reminders
    - Delete reminders
    - Be notified if event venues or times change
    - Be notified if events are cancelled

DEFCON by Phone (cont.)

- How it works
  - Database driven (Duh)
  - Over 250 audio clips
  - AGI handles user registration, searching, and reminders.
  - Daemon checks for reminders every 10 seconds and generates callfiles for reminders
    - Limited only by bandwith (100Mbps) and the PSTN termination provider (hundreds of calls)
  - Web interface controls the addition of events and changing times of presentation.

Defcon By Phone Demo

Code and assorted info available at

http://www.blackratchet.org/
http://www.stromcarlson.com/

Part III:
Caveats
(or, why asterisk sucks)

TDM Card Flakiness

- Connecting an FXS module to a real telephone line can be dangerous
  - If the phone line rings, the FXS module is toast
- Cards sometimes go crazy for no apparent reason
- Drivers are not entirely bug-free

Code Restrictions

- Asterisk ***is*** GPL
- All code contributed to Asterisk is owned by Digium
  - You waive your rights
  - You don't own your code
  - They need to have your wavier on record to contribute
- Digium does have commericial options (?)

Termination Issues

- Proper call progression
  - Supported in protocols
  - Some providers (notably VoipJet) don't support it
  - Tough luck if you want to hear intercepts
- Most providers have nowhere near 99.999% uptime
  - Broadvoice had a large outage both inbound and outbound
- Some providers 'lose' your registration, requiring a kick to Asterisk

Part IV:
Q&A

Q&A by phone!

Call on in!
Harass us from your hotel room!
1-800-4-CATSEX

Further Reading and Resources

- http://www.asterisk.org/
- http://www.blackratchet.org/
- http://www.digium.com/
- http://www.stromcarlson.com/
- http://www.voip-info.org/
- http://www.voipsupply.com/