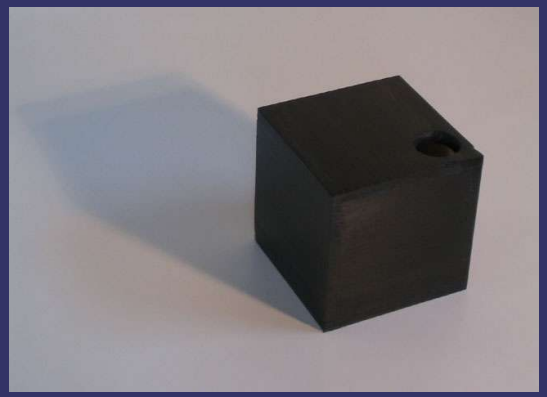
Attacks of Nortel VoIP Implementations
ySt S v.1.0



Eldon Sprickerhoff, CISSP CISA

e•sentire
Critical Security Solutions

Nortel Networks

- Nortel is Canadian (so am I).
- Large presence in Brazil
- Since its establishment in Brazil in 1991, Nortel Networks secured a significant share in the data and transmission markets. The company has closely followed and participated in the whole Brazilian telephony market growth, deregulation and digitalization processes, not only by supplying but also by producing equipment in Brazil, using local labor.
- The results of this activity are gauged in numbers. In the first year, equipment sales in Brazil were US$ 25 million and in 1999 reached US$ 700 million. This result comes from a growing market share that has reached 70% in some cases.

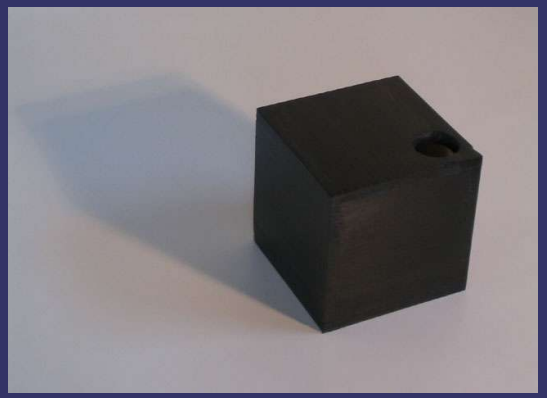
Nortel Networks

- Practically non-existent public security attack tree
- Nortel always seemed to get off easy (ugly stepsister to Cisco and Avaya?)
- We have clients that use Nortel IP Telephony (and were willing to let us play)

Overview

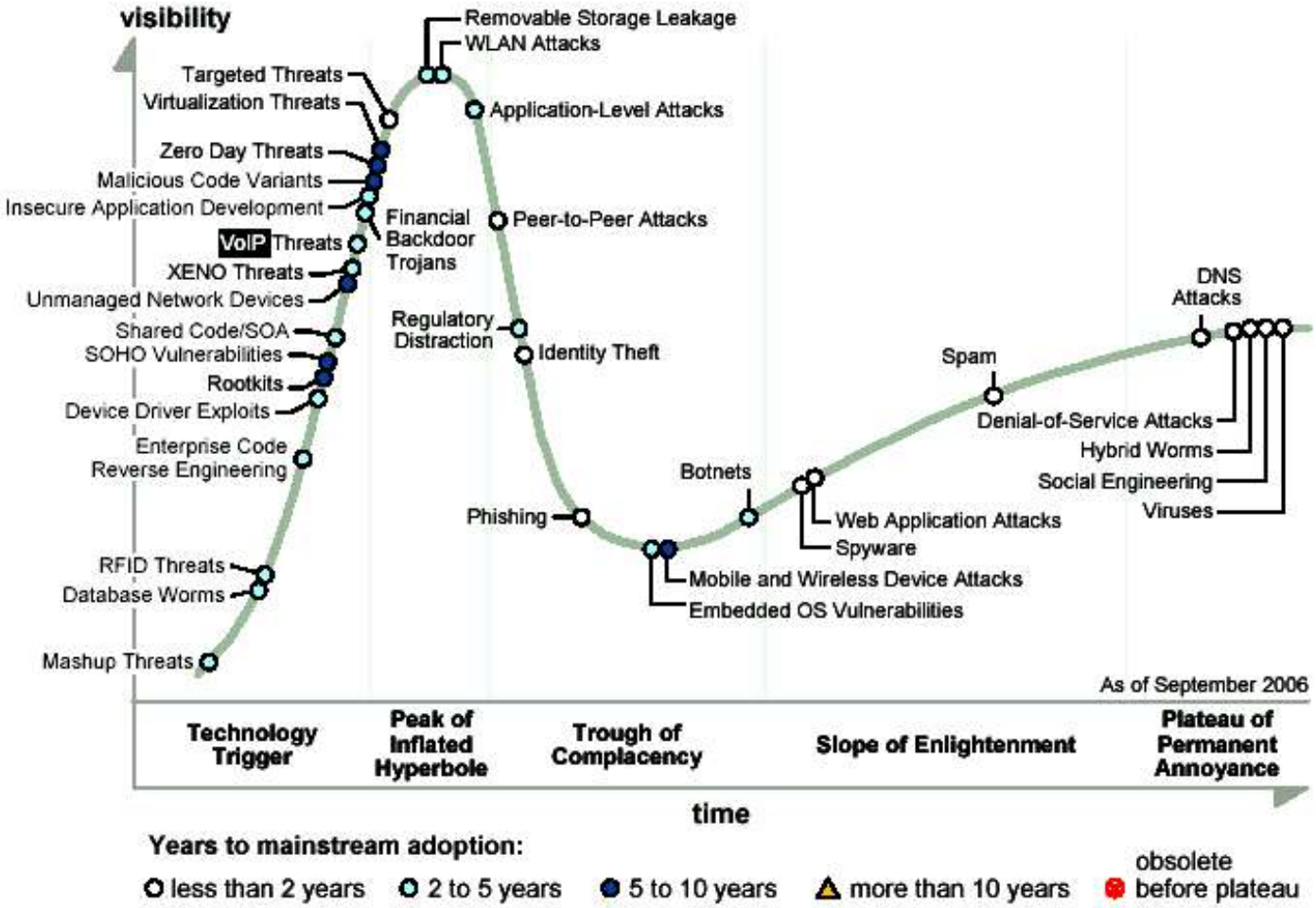
- Misconceptions about Nortel IP Telephony
- Physical Traffic Capture Configuration
- Protocols
- Attack Tree
- Implementation Weaknesses
- Remedies Against Attacks
- Nortel's Responses
- Tidbits

Misconceptions About IP Telephony



- Voodoo/Scary
- Implemented by external consultants
- Not fully understood by Voice group
- Not fully understood by Network group
- Security == Chicken Little

Figure 1. Hype Cycle for Cyberthreats, 2006



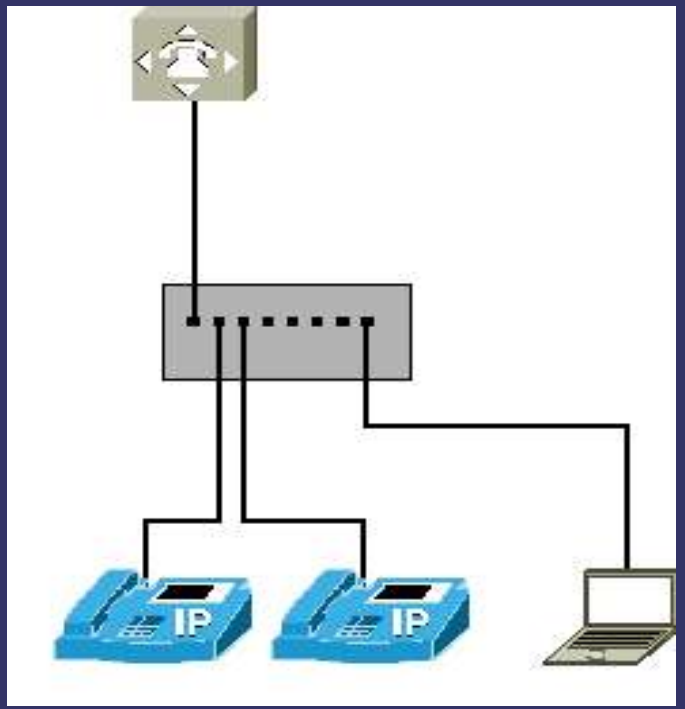
Source: Gartner (September 2006)

Misconceptions

- “Nortel uses a proprietary protocol and it's impossible to eavesdrop or extract the conversation.”
- “I did a packet capture and only got VLAN tagged data.”
- “I did a packet capture with WireShark and couldn't extract a .MP3 file.”
- “We're OK - it's segregated from the data network.”
- “Haven't seen any tools on the Net.”
- “Nessus didn't find anything.”
- “We're getting a SIP firewall.”

On The Wire

- Need to get in-line to reverse-engineer protocol
- Hub/Bridge combination
- VLAN if necessary
- We used OpenBSD's bridge/vlan combo.



e•sentire
Critical Security Solutions

Decode All Possible Traffic Combinations

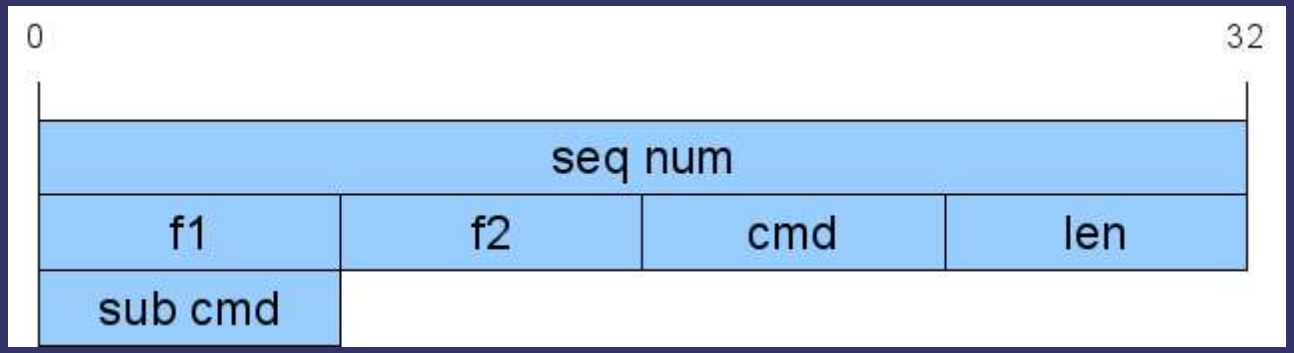
- reboot_phone
- offhook_and_hangup
- offhook_onedigit_hangup
- call_internal_no_answer
- call_internal_answer
- internal_call_us
- internal_call_no_pickup
- internal_call_us_answer
- speakerphone_nocall
- speakerphone_call
- speakerphone_call_answer
- redial
- redial_answer
- change_volume
- disconnect_server_cable
- disconnect_server_cable_in_conversation
- disconnect_client_cable_in_conversation
- nmap_client
- external_call_in
- call_external
- And so on....

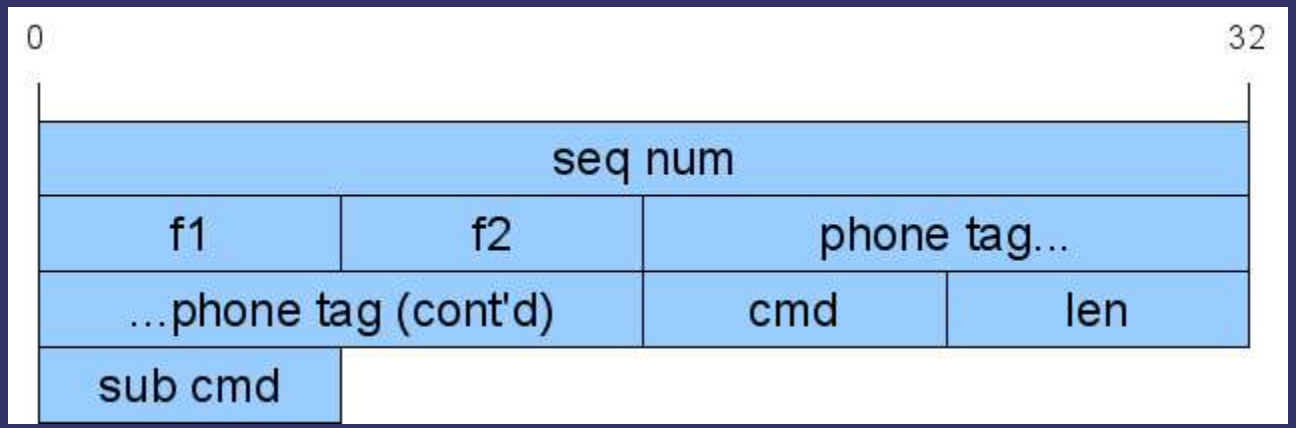
Protocol is known as UNIStim

- NOT SIP.
- Unified Networks IP Stimulus (UNIStim)
- US Patent 7068641
- Canadian Patent 2273657
- Some (outdated/incorrect) details may be found in Asterix documentation

UNIStim

- UDP protocol
- Contains a sequence number, a few flags, and commands/parameters





UNIStim Sequence Number

- Sequence number increments by 1 for each packet.
- Very simple to brute force (will get back to this later)
- Both client and server appear to ignore packets with incorrect sequence number (although they still reply with an ACK)

UNIStim Flags

- Flag1: 0x00 – Error, 0x01 – ACK, 0x02 - PUSH
- Flag2: 0x00 – ServerACK/Irrelevant, 0x01 – server (to client), 0x02 – client (to server)
- Tag: (Client only) 4 bytes that the server will instruct the client to use
- cmd/sub cmd: These fields are combined to give the instruction to the client/server.

Conversation - Network Capture

- Headset boots up (DHCP)
- Initial setup conversation with Call Manager/PBX (UNIStim)
- Voice packets sent directly between two phones (RTP)

UNIStim

- Nortel Marketing will tell you that they support SIP and H.323
- IP sets themselves only speak UNIStim.
- SIP functionality “available” through UNIStim Terminal Proxy Server
- Not “Open Source”
- Partial UNIStim channel driver exists for Asterix (not built up to actually use Nortel phones though).

CIA: Confidentiality

- For Phone Calls
  - Easy to sniff and reassemble phone conversations. (Ethereal/Wireshark can do it right out of the box for any RTP stream.)
- For Control Stream
  - Also easy to sniff UNISTim packets, so you can see exactly who the phone is calling.

CIA: Integrity

- For Phone Call
  - RTP also has a sequence number, so must sniff it before being able to inject.
  - Nothing prevents you from modifying packets as they pass through.
- For Control Stream
  - Seq number (in theory!) means that you must sniff an RTP packet first, and then can take over the stream.
  - Again, nothing prevents you from modifying the packets in transit.

CIA: Availability

- For Phone Call
  - Determine seq number and spoof some packets. The other end now hears what you want (which could be nothing at all.)
- For Control Stream
  - Determine seq number and tell the phone to do whatever you want it to do (including hanging up.)

CIA: Availability (2)

- For Phone
  - Start sending it packets (with a valid sequence number.) If you don't do everything properly, you'll confuse the phone and cause it to reboot (which takes a few minutes.)
- For Call Manager
  - Of course, nothing works if you can take down the Call Manager. (More on this later... :)

Recon and Attacks

- SYN Floods
- Network Mapping
- Fuzzing
- Brute Force Pass
- UNISTim seq num brute force
- Pickup/Hangup
- Media Card
- RTP injection
- ChangeDisplay
- Dial
- Terminate Conn
- Force Conn Open

NMAP

- tcp/21, 23, 80, 111, 513, 1313, 7734, 15000, 15080
- udp/161, 5060, 15000
- icmp
- There is a LOT to play with here!

What else?

- SNMP: OID 1.3.6.1.2.1.1.1 (sysDescr, sysUptime, Software Release)
- SNMP community name: public
- FTP, HTTP: VxWorks
- ICMP: Timestamp

SYN Floods

- Server well-defended against flood of half-open packets.
- But the protocol appears to be weakly defended against fuzzing attacks.
- **EXTREMELY WEAK**
- How bad?

"Atemi" Denial of Service

- amapcrap by THC
- Send random crap to ports
- Create a broadfisted DoS (works especially well against TCP).
- amapcrap -w0 -e -m0ab IP.x.x.x port
- Be generous with your usage.
- Takes about 5-10 seconds to take down the Primary
- Keep sniffing; you can quickly find Secondary and Tertiary servers.

Pickup/Hangup

- Send many (100k) Pickup/Hangup packets rapidly.
- Generally, servers not well defended against this (fall down, go boom).
- Some firmware appears to defend against this attack.

RTP Packet Injection

- Inject tone (square waveform)
- Ouch!
- Works both in-band and out-of-band (caveat about sequence numbers).

UNISTim Seq Num Brute Force

- Sequence number for UNISTim packets appears to be 32bits in size. Unless you can sniff a packet, you must guess and 32bits is too large (due to hardware limitations on the phones themselves.)
- However, from observation, the first 16 bits always seem to be 0. This makes a brute force attack on the sequence number very feasible. (About a minute or so.)
- Don't need to be “in-line”.

Dial

- Cause any phone to dial any number you want.
- Want to get that annoying co-worker fired?
- Keep initiating calls from your boss to the CEO (or their spouse – marital discord).
- Leaves no trace!

Terminate Connection

- Causes a connection to be closed.
- Inject one packet towards server saying client has hung up.
- Also inject one packet towards client saying other side has hung up.

Surveillance/Eavesdropping Mode

- Force Connection Open
- Initiate a phone call without recipient knowing.
- Enable Remote Speaker Phone
- Setup call to Local phone
- Why wait for a phone call in order to listen in to your victim?
- **ILLEGAL! FOR EDUCATIONAL PURPOSES ONLY!**

Brute Force Passwords

- tcp/23, 80 ADMIN1/1111
- tcp/1313 dba/dba

Media Card Tidbits

- Tertiary IP telephony provisioning
- 32 phones per card
- Doesn't require a separate PBX.
- Only has UDP ports open (and not particularly susceptible to AMAPcrap).
- But appears to be particularly susceptible to protocol-sensitive fuzzing attacks.
- Do you notice a trend here?

Media Card One-Packet DoS Example

- UDP src: 5000, dst: 5100
- Send an null-data packet to the media card.
- One UDP packet takes down whole card.

Nortel's Response

- Please send Packet Captures.
- Please send System Revision information.
  - "The more details you can provide, the quicker we will be able to reproduce and resolve any issues. Information such as the packet captures you have already sent, platform configuration, software load info, test tools used, location of sets and attackers (E-LAN, T-LAN etc.) are always very helpful."
- "The test tools were written specifically to test UNIStim."
- Secunia: SA25409
- Nortel Patch: MPLR 23899

Official Nortel Position

- Securing Multimedia & IP Telephony
- “Instant” Secure Multimedia Zone Secure Multimedia Controller 2450 (SMC)
- Virtual “moat” around servers
- Stateful filters (SIP, H.323, etc.)
- Denial of Service defence engine
- Secure UNIStim encryption proxy
- 802.1X with EAP
- SRTP
- Gratuitous ARP Denial, Switch Lockdown

Unofficial Nortel Position

- Blame the implementers, we gave you/them all the tools you need to secure your system.
- “Does your SQL Server offer you the security granularity that we do?”
- “The vendor recommends that customers restrict direct access to the ELAN from unknown devices.”
- ELAN = Embedded LAN

“We're Isolated From the Data Network”

Security is a PITA

- Easy to ignore (Just get it working!)
- Can add overhead
- Can limit debugging capability
- Compatibility issues (conference calls, etc.)
- Can be difficult to add after-the-fact
- Difficult to justify (politically) after-the-fact

Configuration Tips

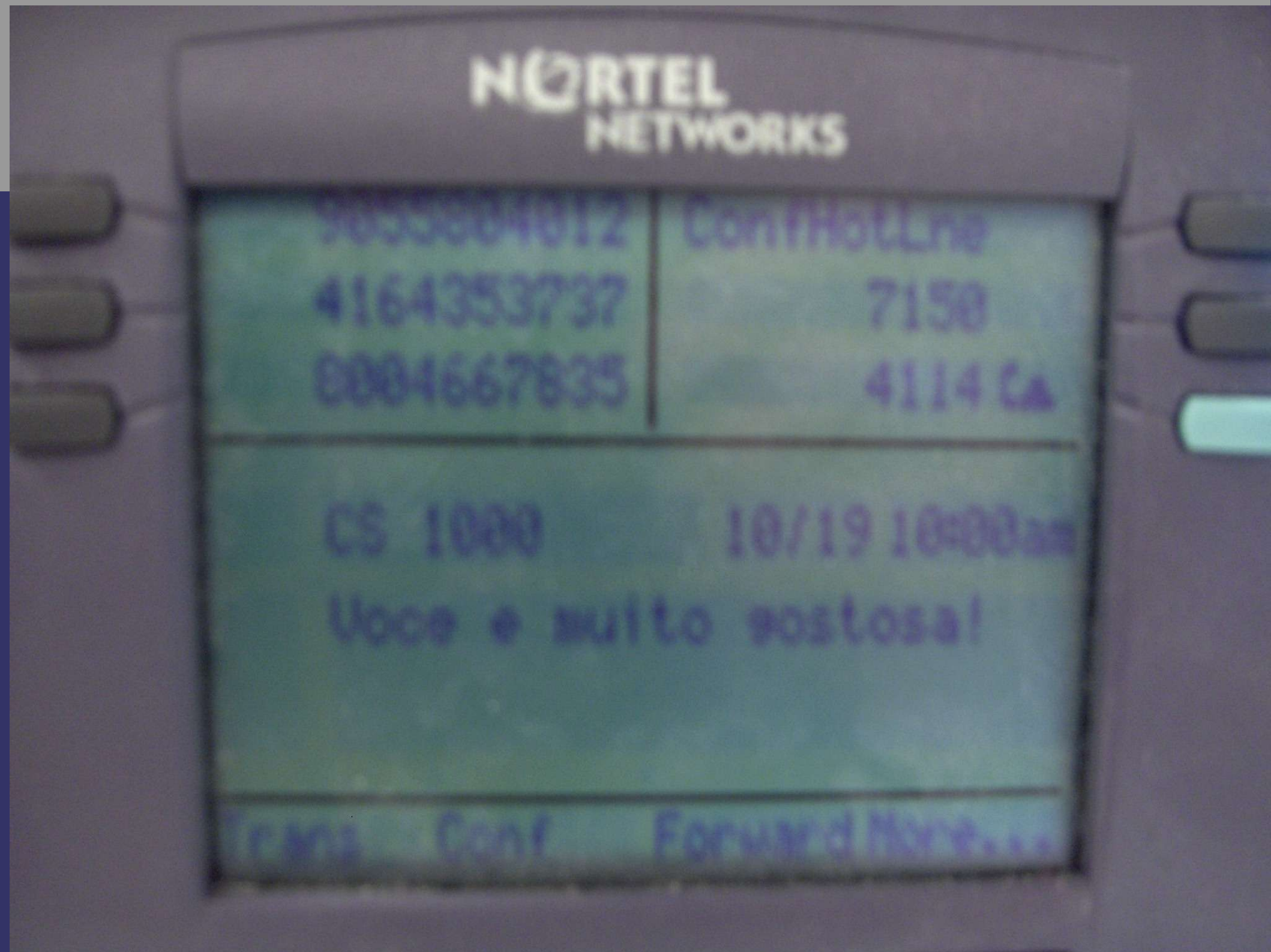
- Limit administrative access.
- Lock down protocols (some firewall functionality exists in the product itself).
- Investigate what's available in the product.
- Lock down switches.

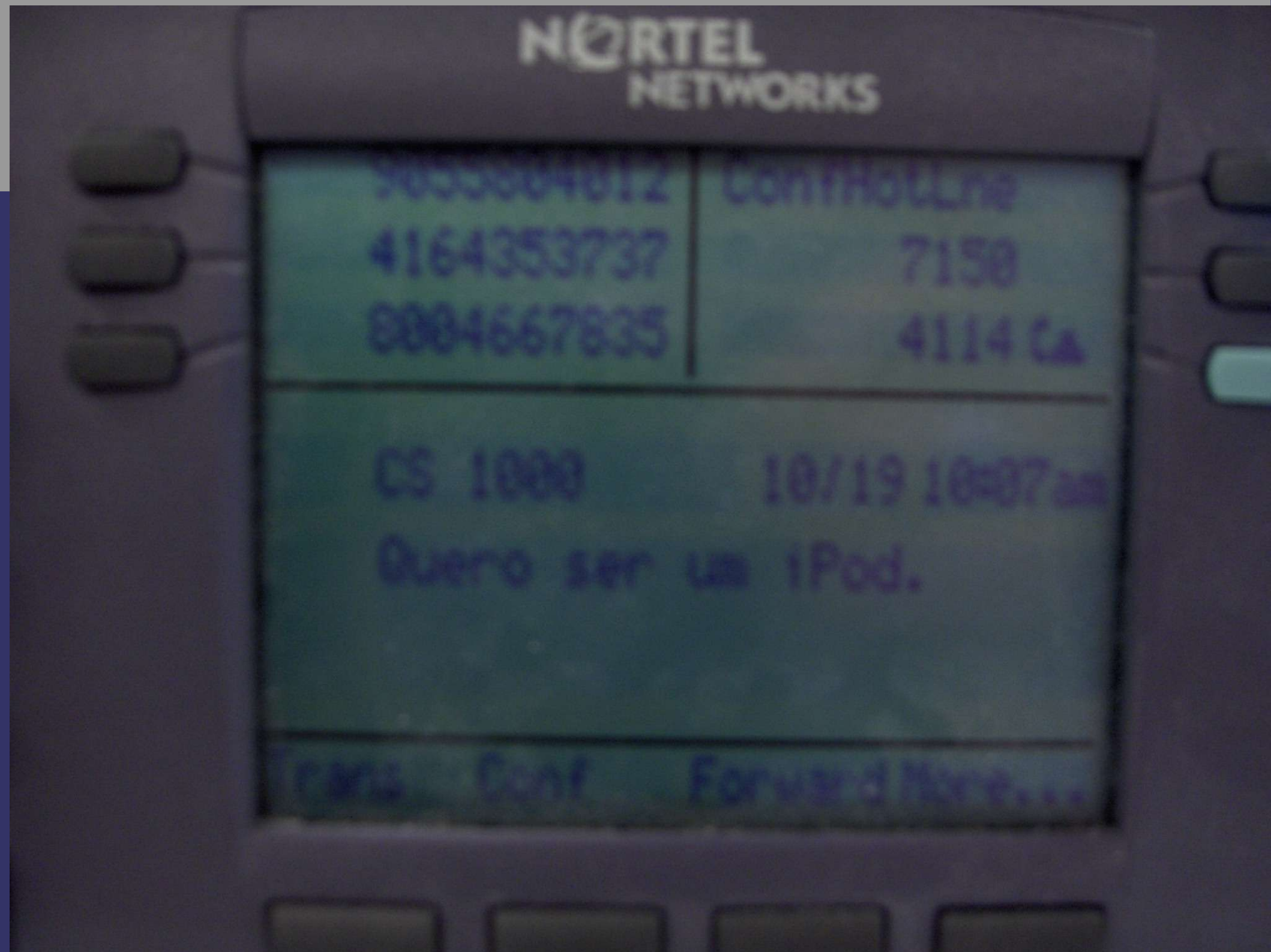
Misconceptions Revisited

- “Nortel uses a proprietary protocol and it's impossible to eavesdrop or extract the conversation.”
- “I did a packet capture and only got VLAN tagged data.”
- “I did a packet capture with WireShark and couldn't extract an .AU file.”
- “Haven't seen any tools on the Net.”
- “nCircle/Nessus didn't find anything.”
- “We're getting a SIP firewall.”

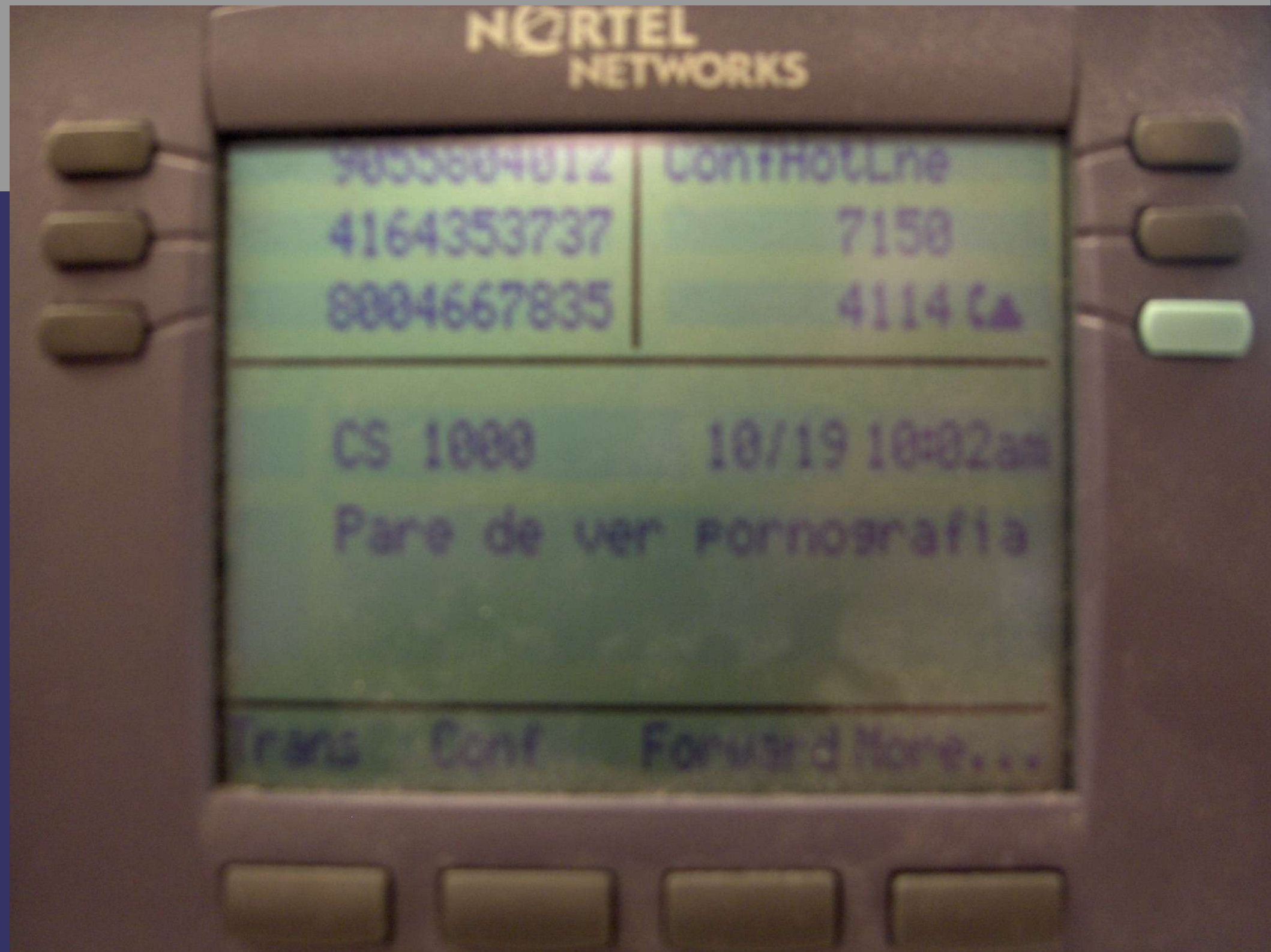
Finally... ChangeDisplay

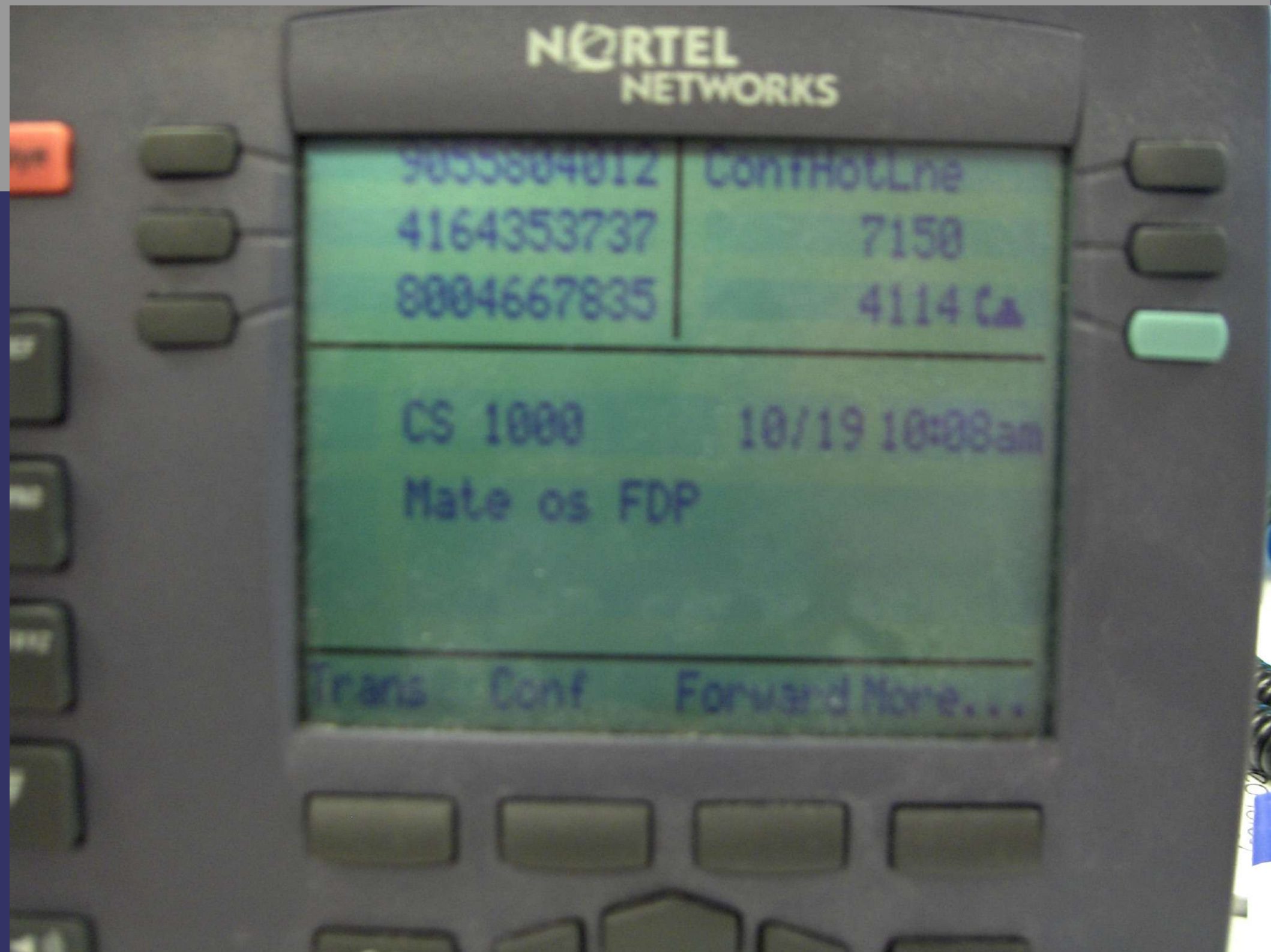
- Tells the phone what to display
  - Change caller-id information (name/number)
  - Or just for fun...

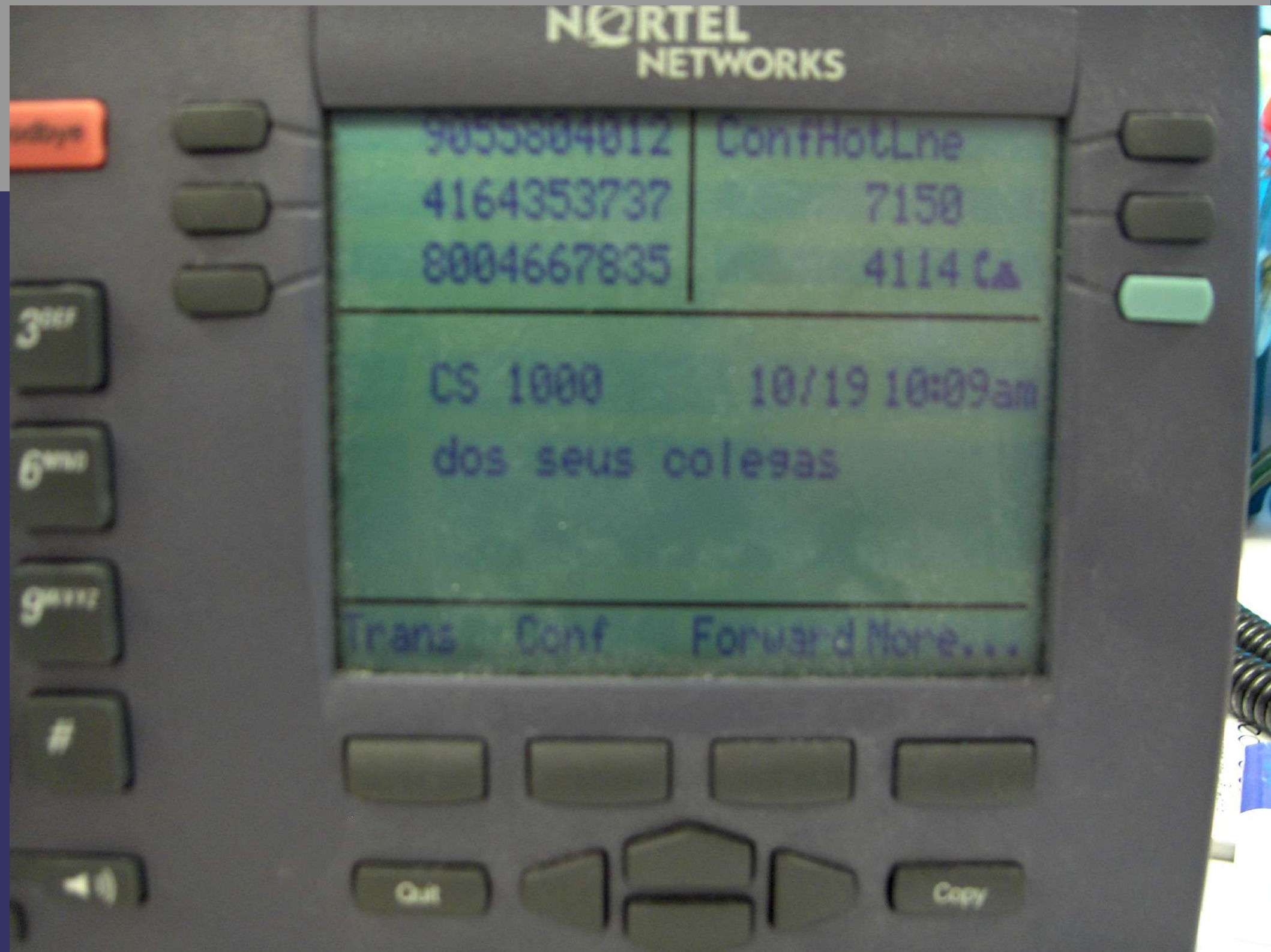

NORTEL
NETWORKS
4164353737
7158
CS 1000
Voce e molto costosa!
Conf
Forward More...


NORTEL
NETWORKS
4164353737
7158
CS 1000
Quero ser um iPod.


NORTEL
NETWORKS
9055604012 ConfHotLne
41643537737 7150
8004667835 4114
CS 1000 10/19 10:14am
Eu ouco as suas conversa
Trans Conf Forward More...


NORTEL
NETWORKS
4164353737
7150
CS 1000
10/19 10:02
Pare de ver pornografia


NORTEL
NETWORKS
9055804012
4164353737
8004667835
ContHotLine
7150
4114
CS 1000
10/19 10:08am
Mate os FDP
Trans
Conf
Forward
More...


NORTEL
NETWORKS
9055804012
ConfHotLne
4164353737
7150
8004667835
4114
CS 1000
10/19 10:09am
dos seus colegas
Trans
Conf
Forward
More...
Quit
Copy

Slides and Code - UNIStimpy!

- http://www.esentire.com/unistimpy
- Requirements: libpcap, libnet, gcc, linux
- UNISTIMpy NG released shortly, including UNIStim fuzzer and eavesdropping code.
- These attacks work against Nortel's wired, wireless and software clients.

e•sentire
Critical Security Solutions

Obrigado!

- Luiz, Nelson, Willian
- eSentire staff (for their support)
- eSentire clients (that let us play on their gear)
- Nortel (for giving us something to play with)
- Thank you for your time!
- Questions, comments to: eldons@esentire.com