

# Myth: VoIP is not secure



Dan York, CISSP  
VOIPSA Best Practices Chair

VOIPSA

January 24, 2008



**Privacy**

**Availability**

**Compliance**

**Confidence**

**Mobility**

**Cost Avoidance**

**Business Continuity**

**VQIPSA**

## 2008 - the year VoIP gets hacked?

The drawbacks of IP everywhere

By [Bill Ray](#) → [More by this author](#)

Published Thursday 17th January 2008 12:49 GMT  
[Green Computing - Where](#)

With VoIP rapidly replacing  
barcode scanners, the  
shaped - a prediction

VIPER reckons that  
start to become serious  
Communications



### NEWS ANALYSIS

Go to a section

[Home](#) > [News Analysis](#) > [VOIP](#)

Discuss Print Email License content Reprint Article

## Two Charged in VOIP Hacking Scandal

JUNE 09, 2008

[Discuss >](#)

Feder  
whol  
Rob  
had



### Security Considerations for Voice Over IP Systems

Recommendations of the National Institute of Standards and Technology

January 16, 2008 8:53 AM PST

## Can terrorists use the Net to avoid wiretaps?

Posted by [Chris Soghoian](#) | 6 comments

Can members of Al Qaeda use voice over Internet technology (VoIP) to avoid wiretaps?

Recent comments by Michael McConnell, Director of National Intelligence, seem to suggest that terrorists could create significant roadblocks for the National Security Agency by simply routing their traffic through the U.S.

[perimeter](#)

### VoIP Security Still Falling Short

Posted by Carl Weinschenk on January 18, 2008 at 6:18 pm

It may be a bit late in the month to still be posting "year ahead"-type stories, but the content of this [Help Net Security piece](#) on the security threats facing VoIP makes it worthwhile. The bottom line of this commentary is that VoIP security is not yet where it should be.

## SECURITY

## VoIP Systems Vulnerable To Attack

By [Kevin McLaughlin](#), *CRN*  
3:00 PM EDT Fri. Aug. 25, 2006  
From the August 28, 2006 *CRN*

VoIP is well on its way to widespread adoption, but the fact that many companies haven't taken the necessary steps to toughen up security on their [VoIP](#) systems could make them attractive targets for hackers.



ing so without fully considering the applications, operating systems, and opportunity for hackers, said David Mass.-based [3Com](#) and its

[why SANS?](#)[pick a course](#)[why certify?](#)[register now](#)

The most trusted source for computer security training, certi

[training](#) [certification](#) [resources](#) [vendor](#) [portal](#) [storm center](#) [colleges](#)

## SANS Top-20 2007 Security Risks (2007 Annual Update)

7 Security Risks (2007 Annual Update)

http://www.sans.org/top20/#n1

Google

top

### N1. VoIP Servers and Phones

#### N1.1 Description

Use of VoIP technologies has continued to expand during the past year. Rapid adoption to garner the economic advantages of VoIP has led many to overlook, or even set aside, security concerns. Vulnerabilities can exist throughout a VoIP network, from mismanaged and unpatched call proxy and media servers to the VoIP phones themselves. Vulnerabilities have been found in products such as [Cisco Unified Call Manager](#) and [Asterisk](#), along with VoIP phones from multiple vendors. By leveraging those vulnerabilities, attackers can carry out VoIP phishing scams, eavesdropping, toll fraud, or denial-of-service attacks. Poorly designed implementations can provide inroads to data networks and researchers are continuing to uncover additional areas for potential attack, such as cross site scripting through VoIP clients.

As many VoIP servers -- especially the ones at VoIP service providers -- are an interface between SS7 (traditional phone signaling) and IP networks, an attacker capable of compromising a vulnerable VoIP server could potentially manipulate the SS7 signaling interconnection to disrupt services on the Public Switched Telephone Network (PSTN).

#### N1.2 CVE Entries

Asterisk

[CVE-2007-1594](#), [CVE-2007-1561](#)

Cisco Call Manager

[CVE-2006-5277](#)

VoIP Phones

[CVE-2007-4459](#), [CVE-2007-2512](#), [CVE-2007-3047](#), [CVE-2007-2270](#), [CVE-2006-7121](#), [CVE-2007-0431](#), [CVE-2006-6411](#), [CVE-2006-5233](#), [CVE-2006-5231](#), [CVE-2006-5038](#)

Avaya

[CVE-2007-5556](#)

Cisco IOS

[CVE-2007-4291](#)

#### N1.3 How to Mitigate These VoIP Vulnerabilities

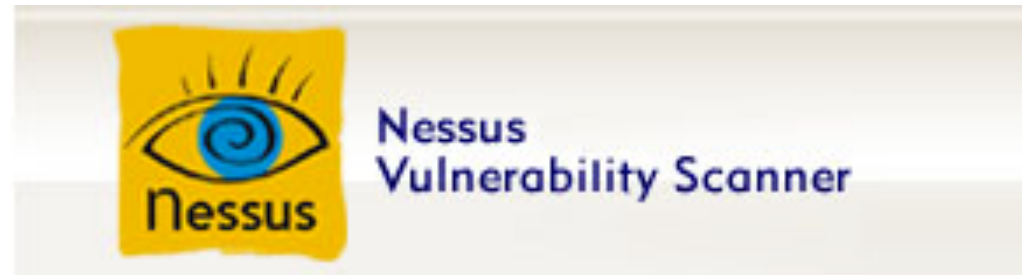
VOIPSA

Done

**WIRESHARK**



**Intelligent Wardialer [IWar]**



*PROTOS - Security Testing of Protocol Implementations*

**Scapy**

SiVuS

**sipsak**

**SIPv6 Analyzer**  
An Analyzer for SIP and IPv6

**SIPp**

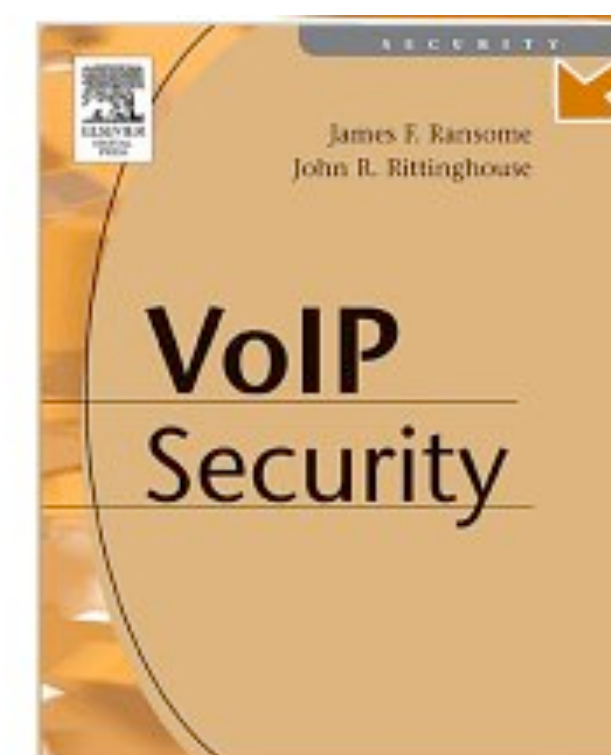
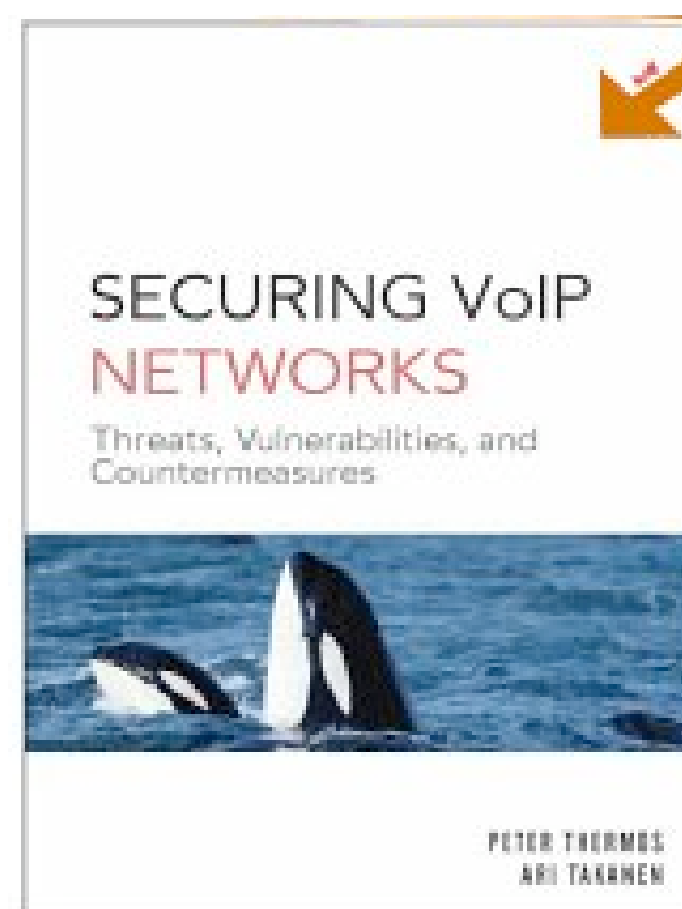
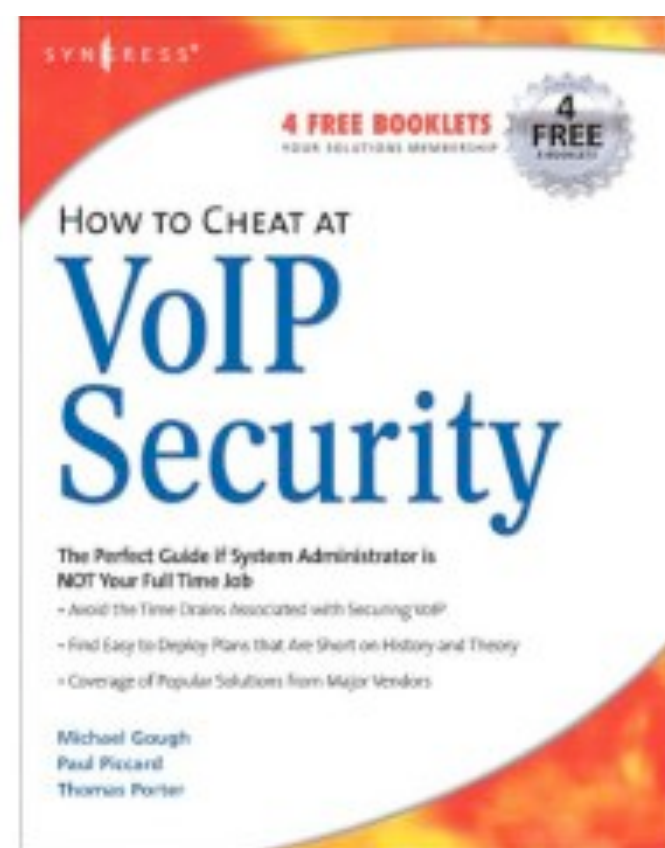
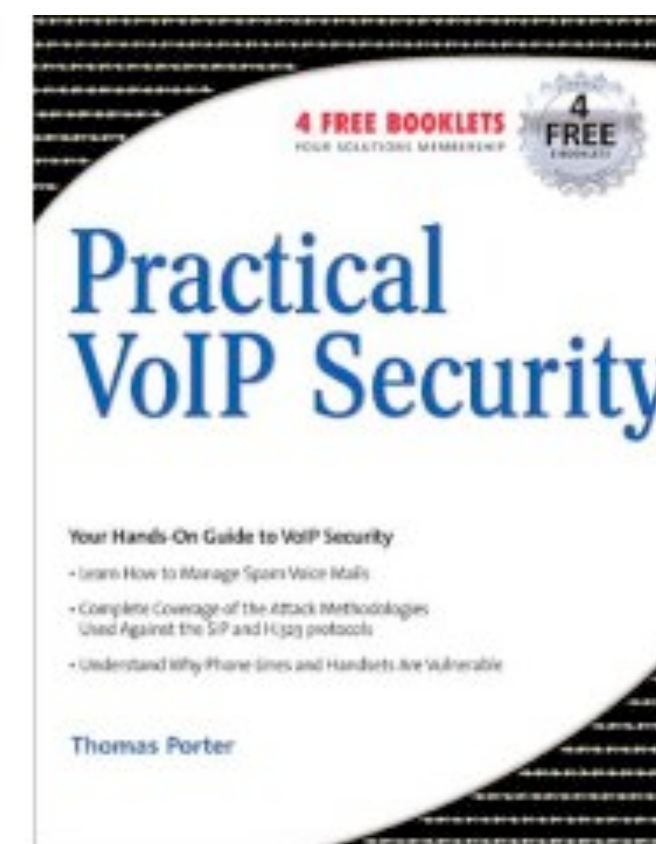
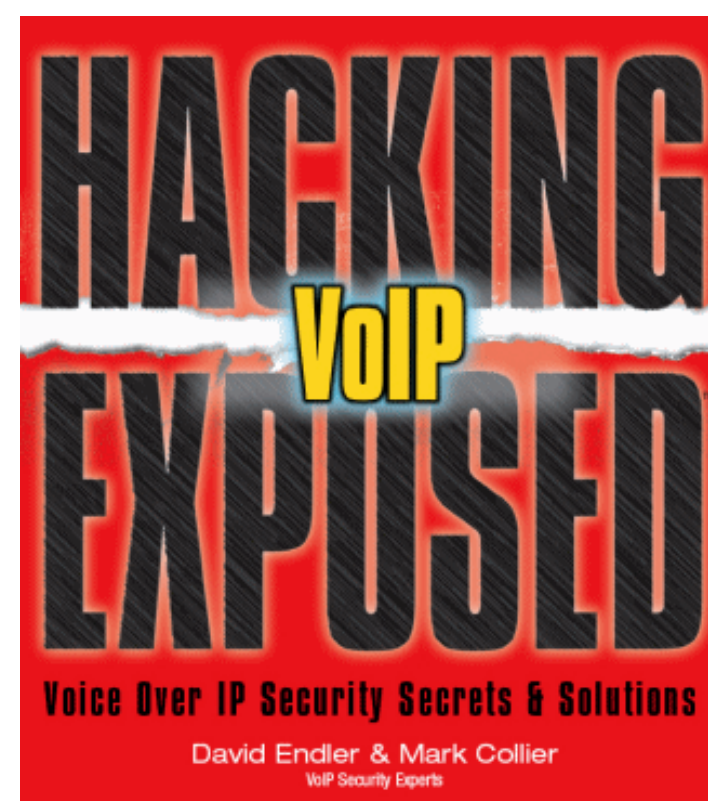
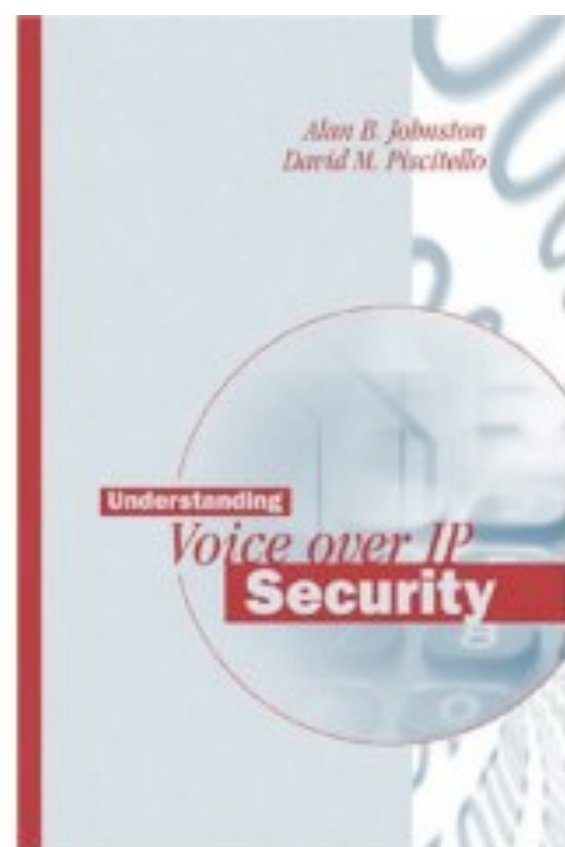
SIPcrack - SIP login dumper/cracker

**CODENOMICON**

**vomit - voice over misconfigured[1] internet telephones**

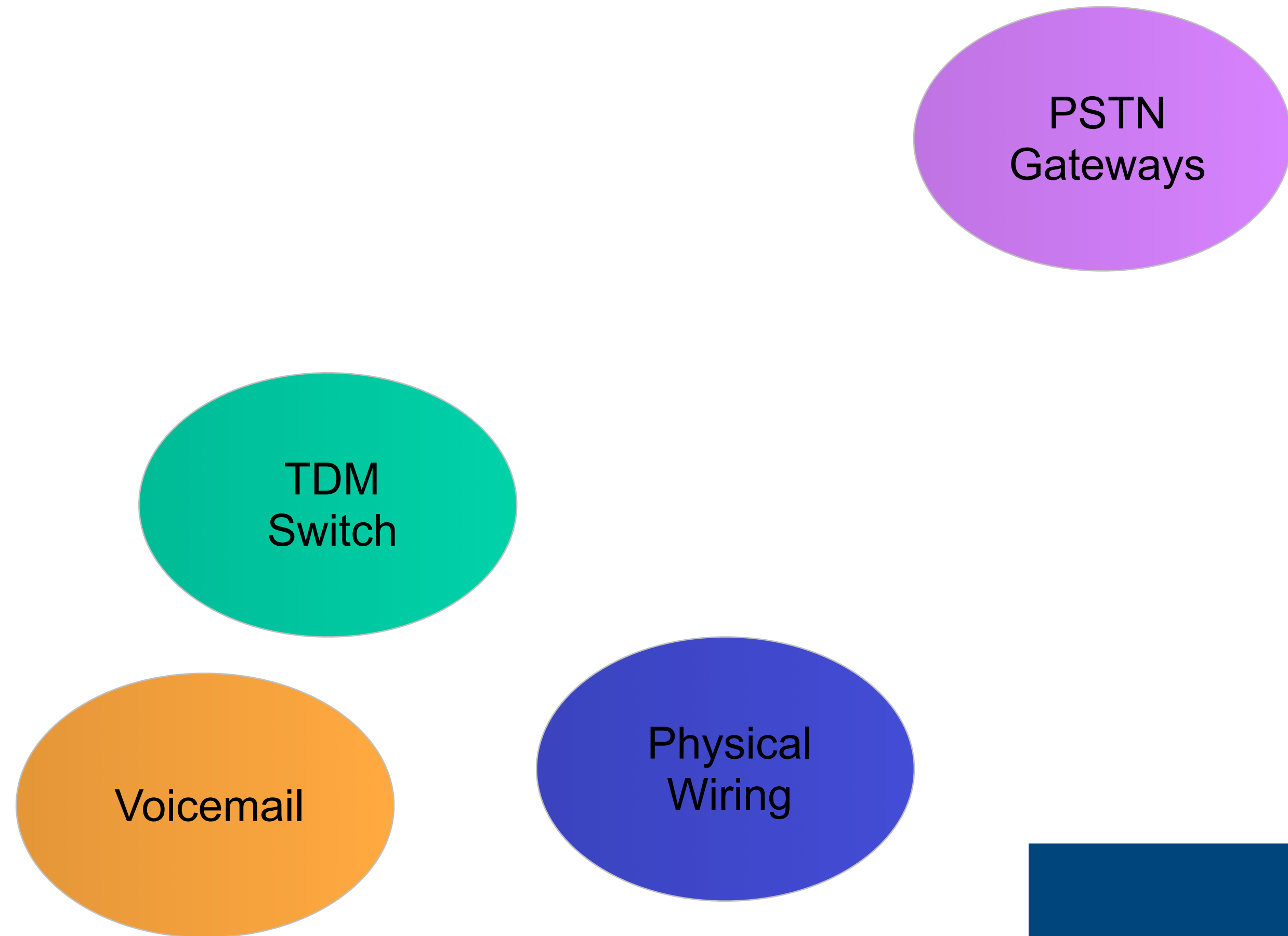
**ASTEROID SIP Denial of Service Tool**

**VOIPSA**



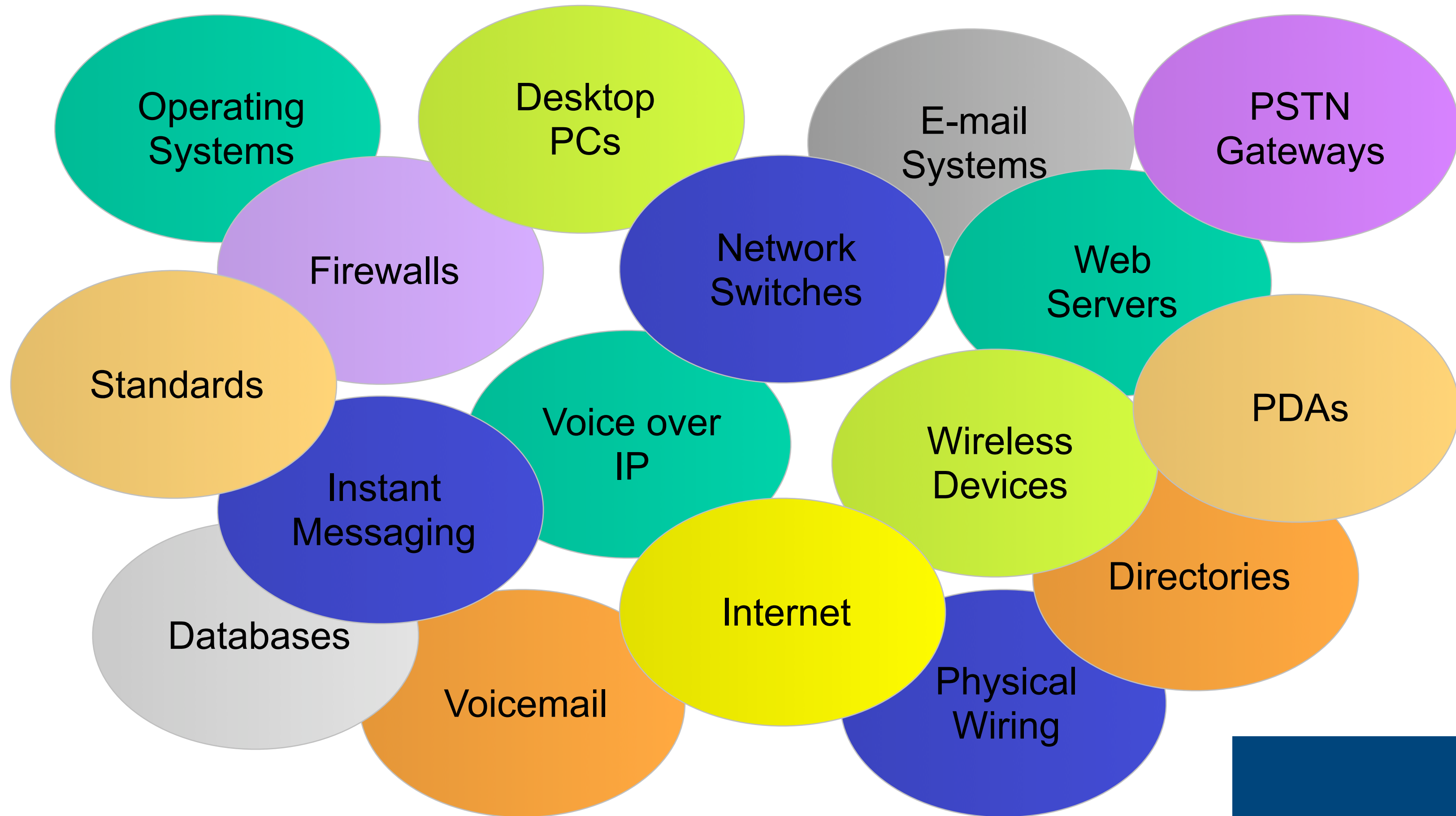
VOIPSA

# TDM security is relatively simple...





# VoIP security is more complex



**VoIP is NOT secure!**

VOIPSA



**VoIP can be *more* secure  
than the PSTN...**

VOIPSA

IF

VOIPSA

**... it is properly deployed.**

VOIPSA

**VoIP can be *more* secure  
than the PSTN *if* it is  
properly deployed.**

# Security concerns in telephony are not new...



Image courtesy of the Computer History Museum

VOIPSA



# Nor are our attempts to protect against threats...



**A Telephone Silencer – the HUSH-A-PHONE**  
*A solution of three phone problems of subscribers*

**Safeguarding Privacy:** So others cannot hear confidential matters  
**Eliminating Phone Talk Annoyance:** Quieting the office for personnel efficiency  
**Improving Hearing in Noisy Places:** By keeping surrounding noises out of the transmitter

*Write for Booklet T-E.*

**Hush-A-Phone Corporation, 43 W. 16th St., N. Y. City**

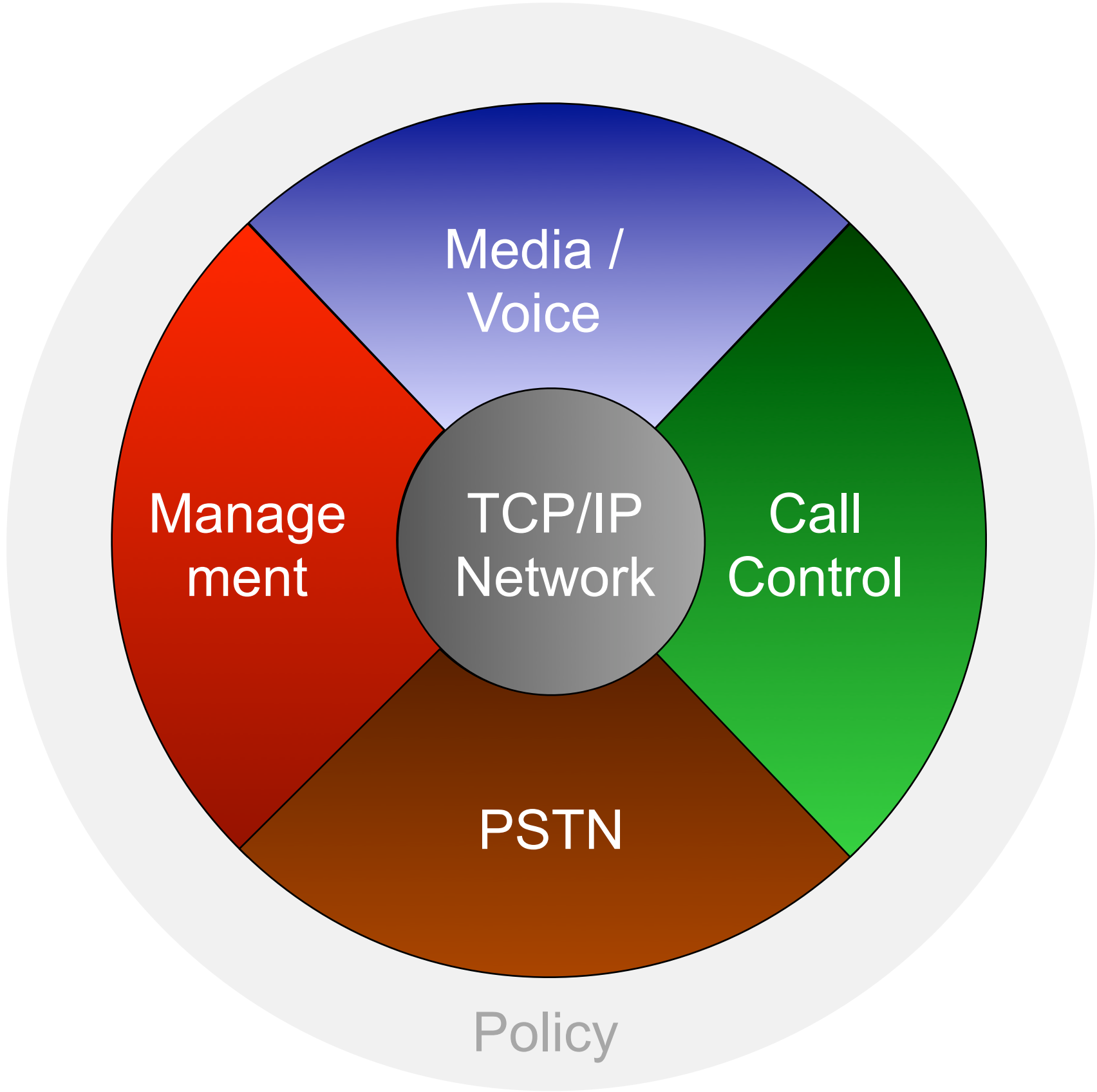
Models for Hand-set Phone

Models for Pedestal Phone

Image courtesy of Mike Sandman – <http://www.sandman.com/>

VOIPSA

# Security Aspects of IP Telephony



Eavesdropping

Degraded Voice Quality

Encryption

Virtual LANs (VLANs)

Packet Filtering

Denial of Service

Impersonation

Toll Fraud

Encryption

Encrypted Phone Software

Proper Programming

Web Interfaces

APIs!

Phones!

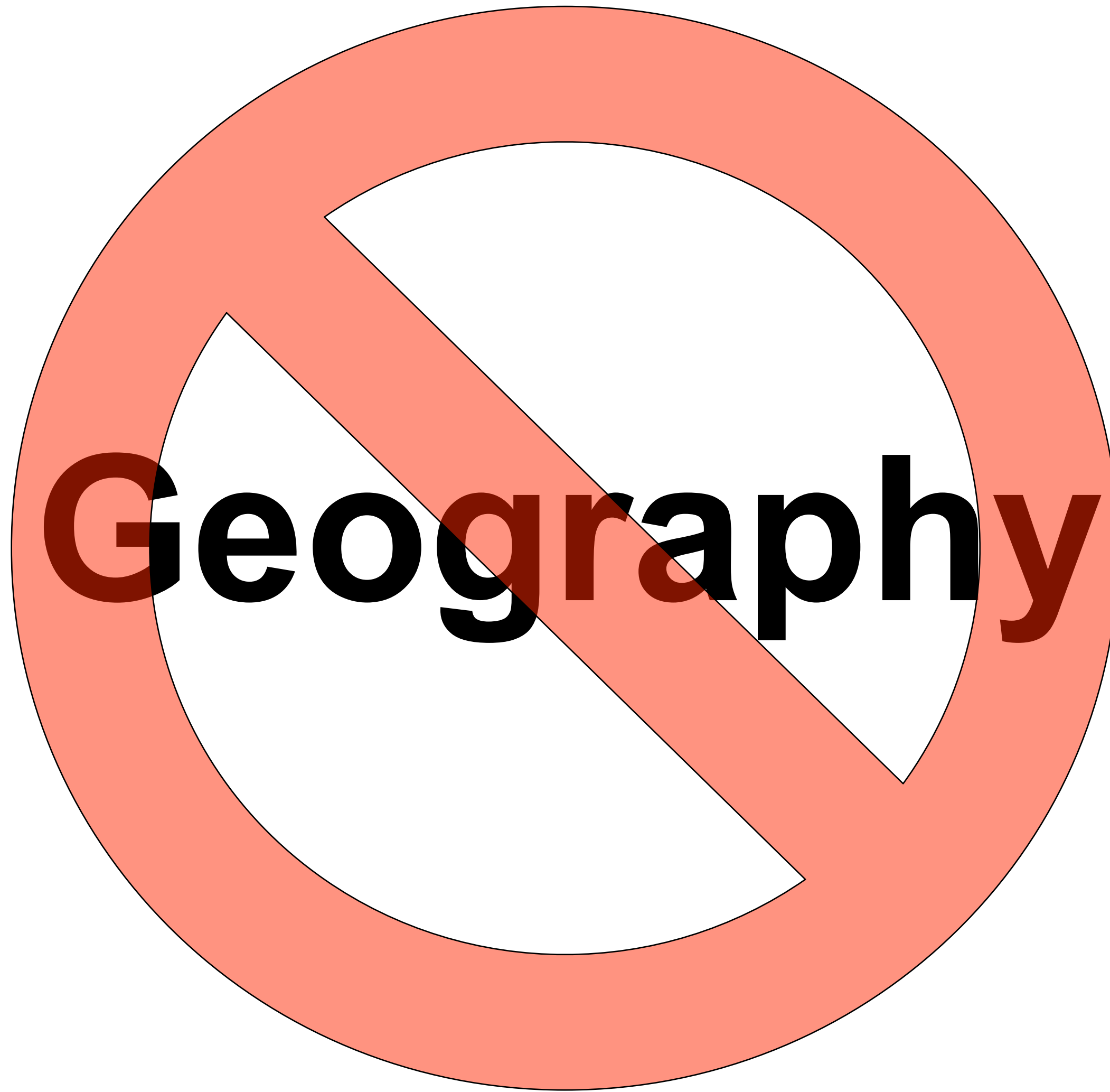
Encryption

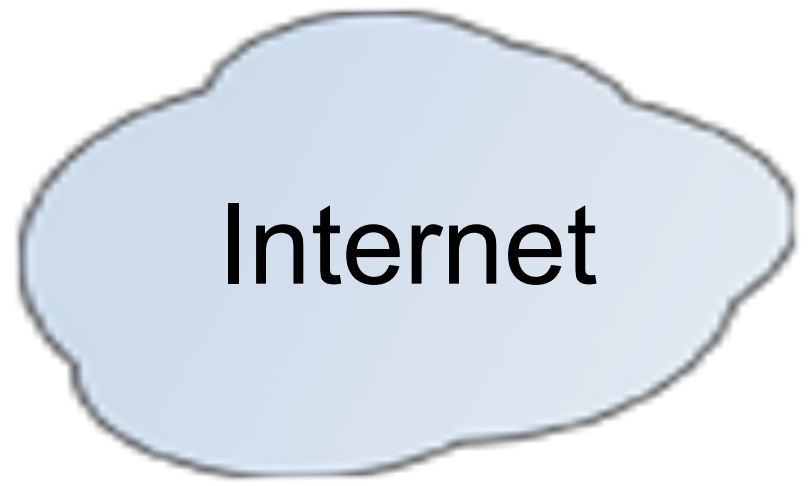
Change Default Passwords!

Patches? We don't need...

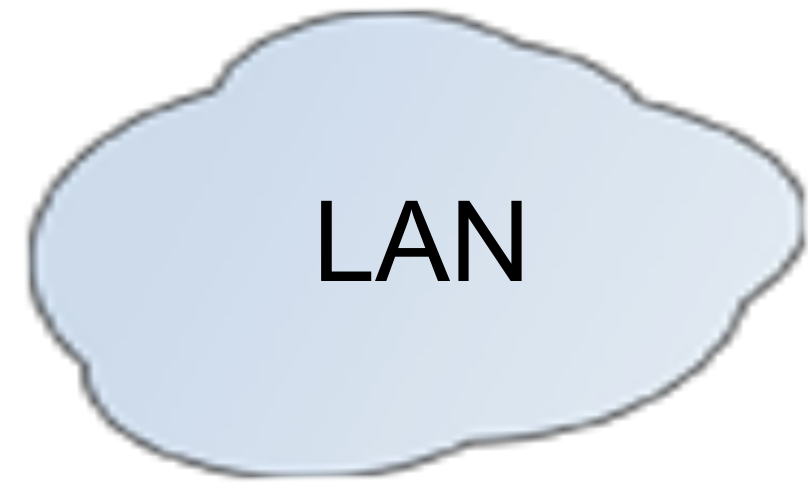
PSSTNN

VOIPSA





Internet



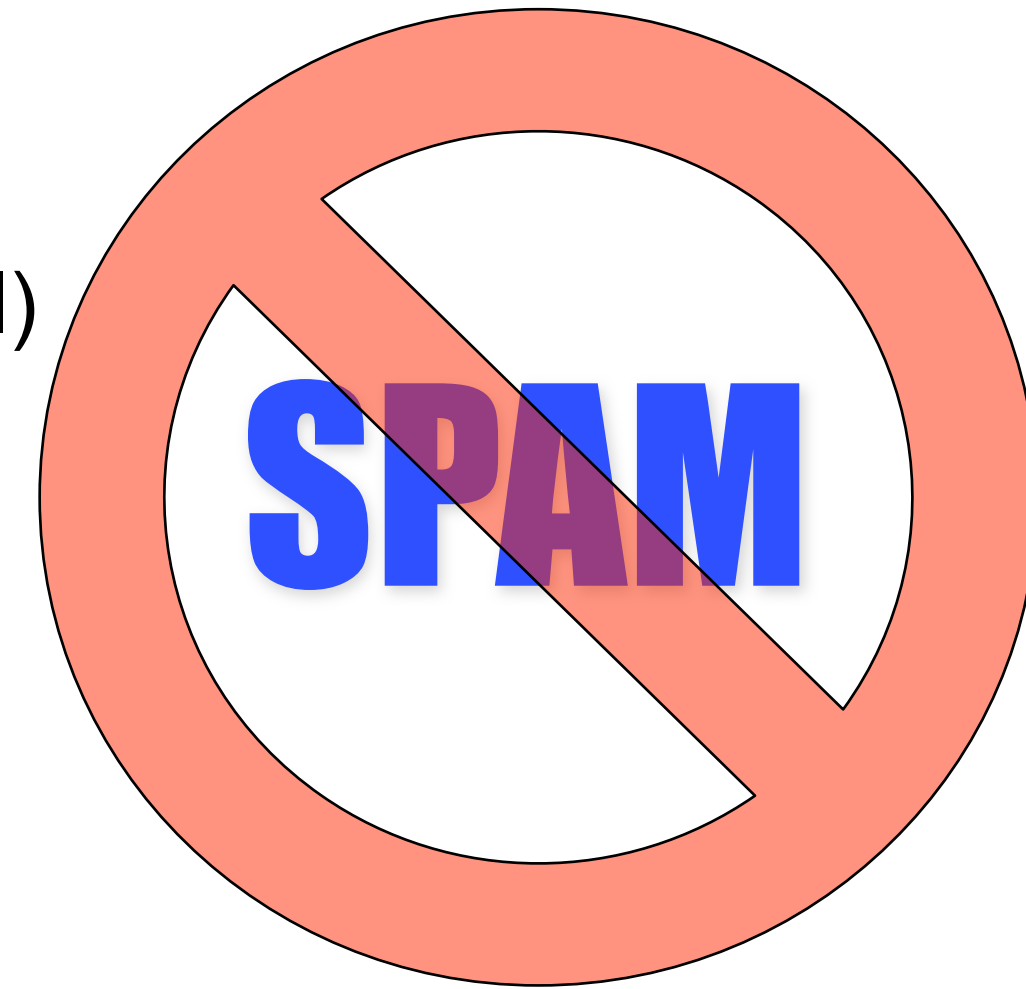
LAN





# What about SPIT? (“SPam over Internet Telephony”)

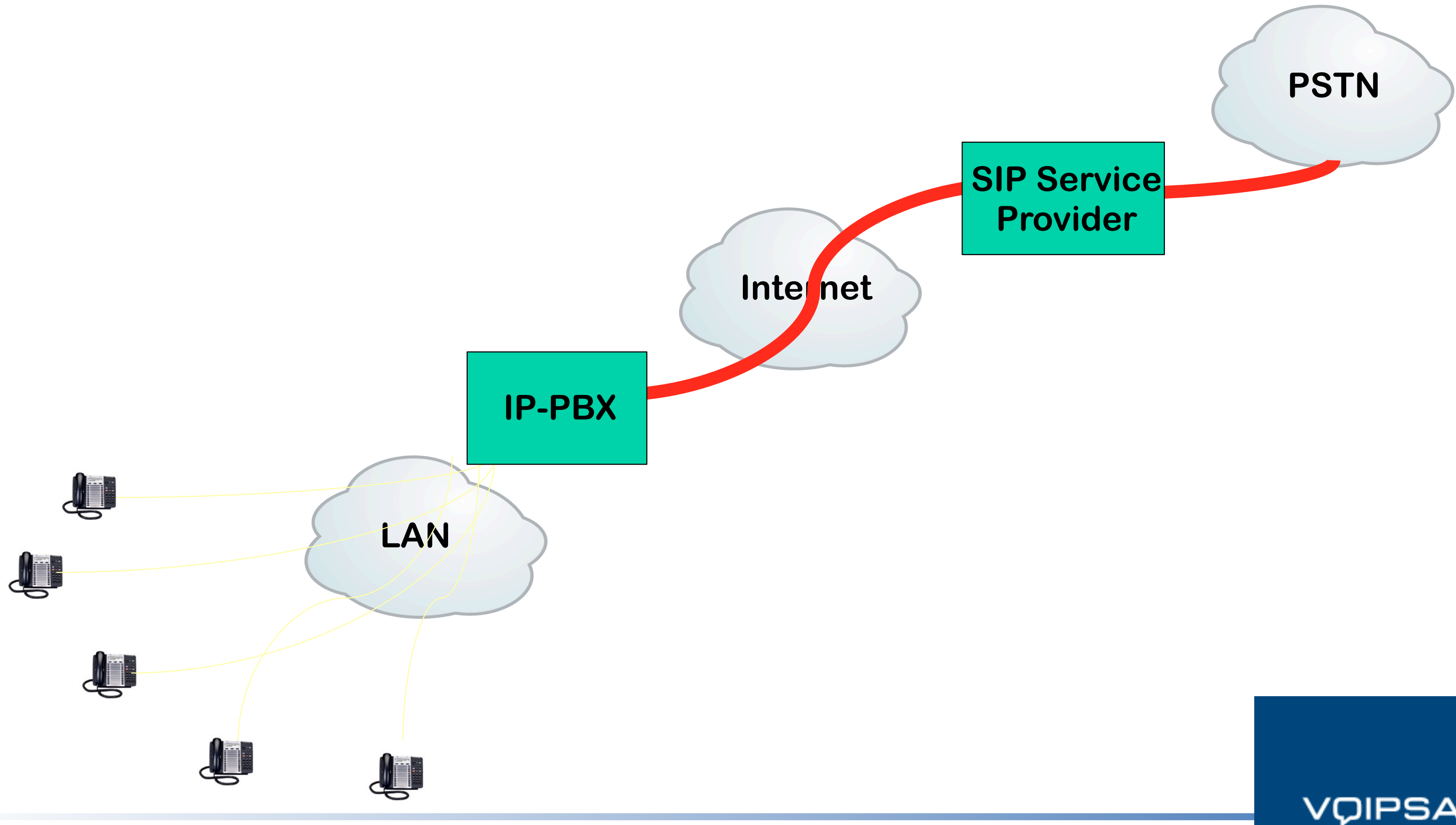
- What does a traditional telemarketer need?
- Makes for great headlines, but not yet a significant threat
- Fear is script/tool that:
  - Iterates through calling SIP addresses:
    - 111@sip.company.com, 112@sip.company.com, ...
    - Opens an audio stream if call is answered (by person or voicemail)
  - Steals VoIP credentials and uses account to make calls
- Reality is that today such direct connections are generally not allowed
- This will change as companies make greater use of SIP trunking and/or directly connect IP-PBX systems to the Internet (and allow incoming calls from any other IP endpoint)
- Until that time, Telemarketers have to initiate unsolicited calls through the PSTN to reach their primary market: slows them down and adds cost



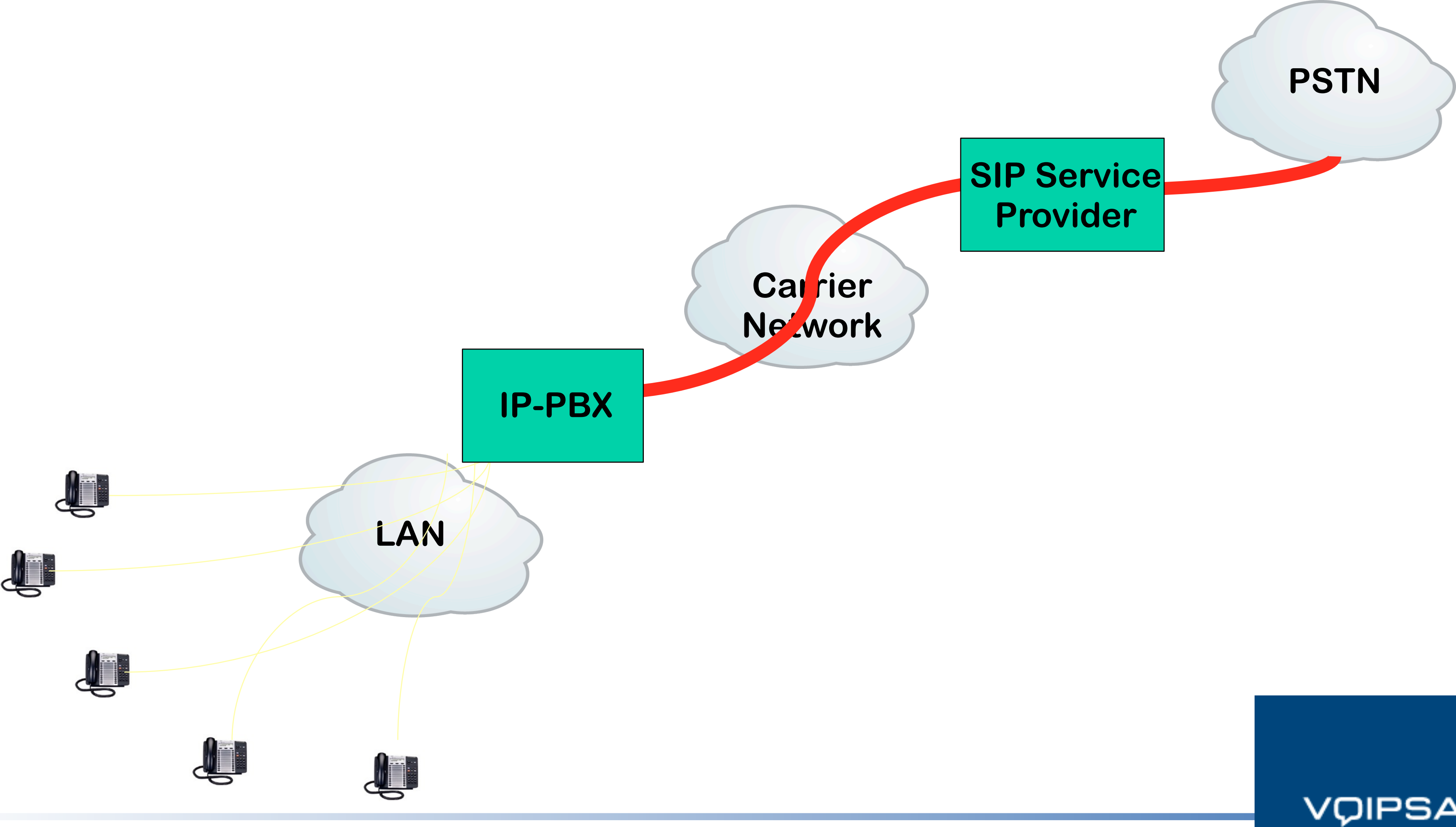
# SIP Trunking



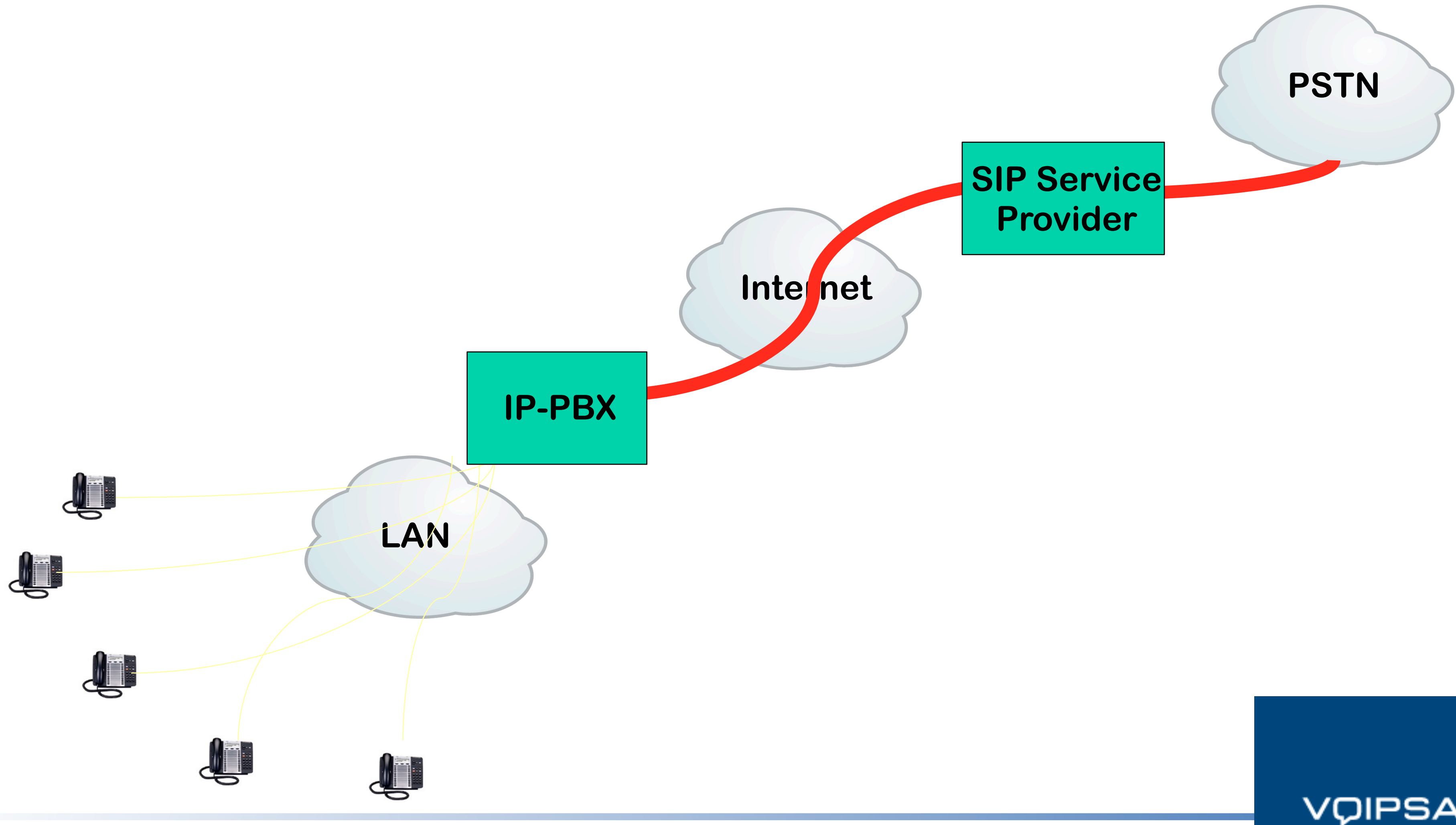
# The Challenge of SIP Trunking



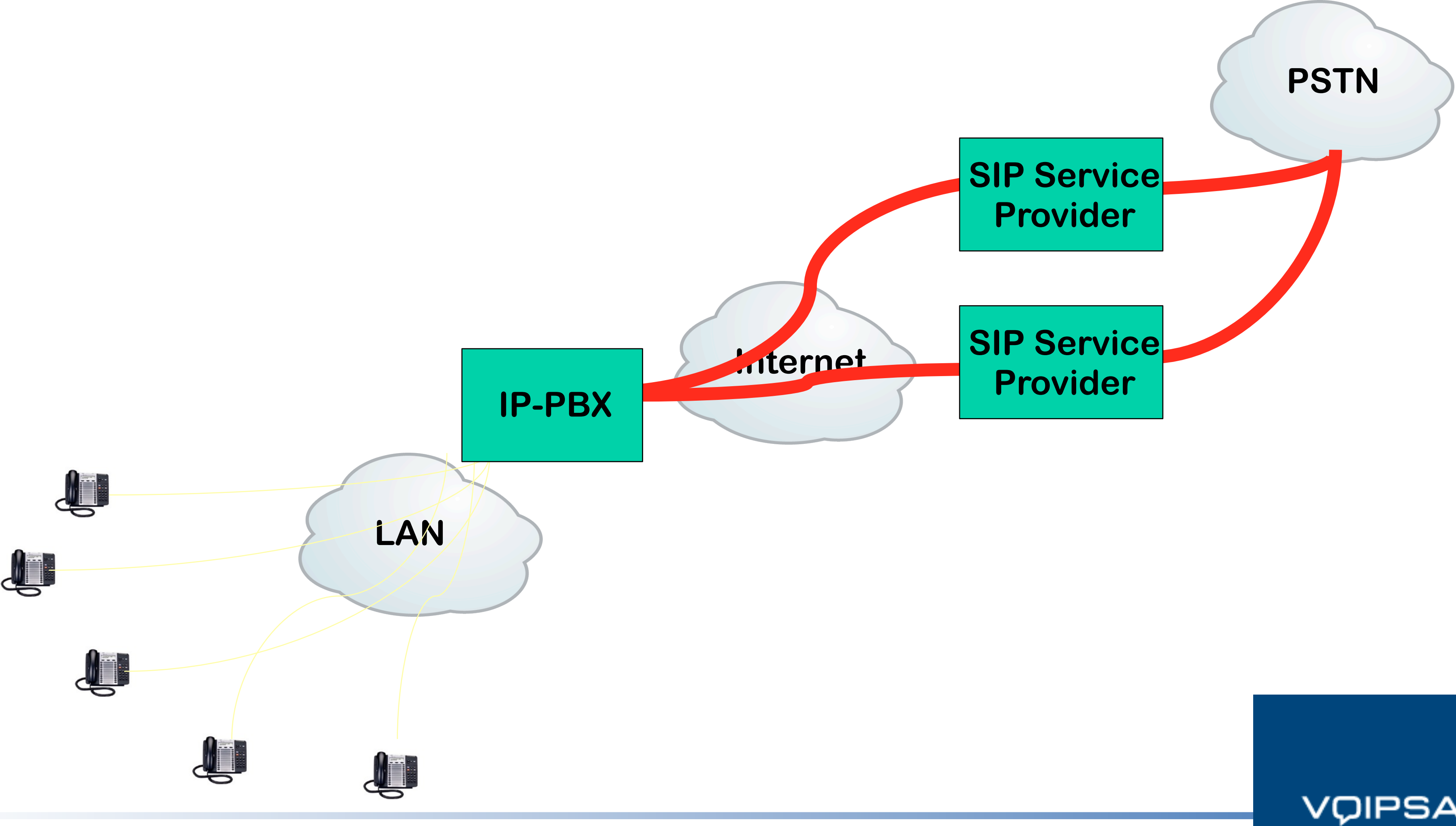
# SIP Trunking



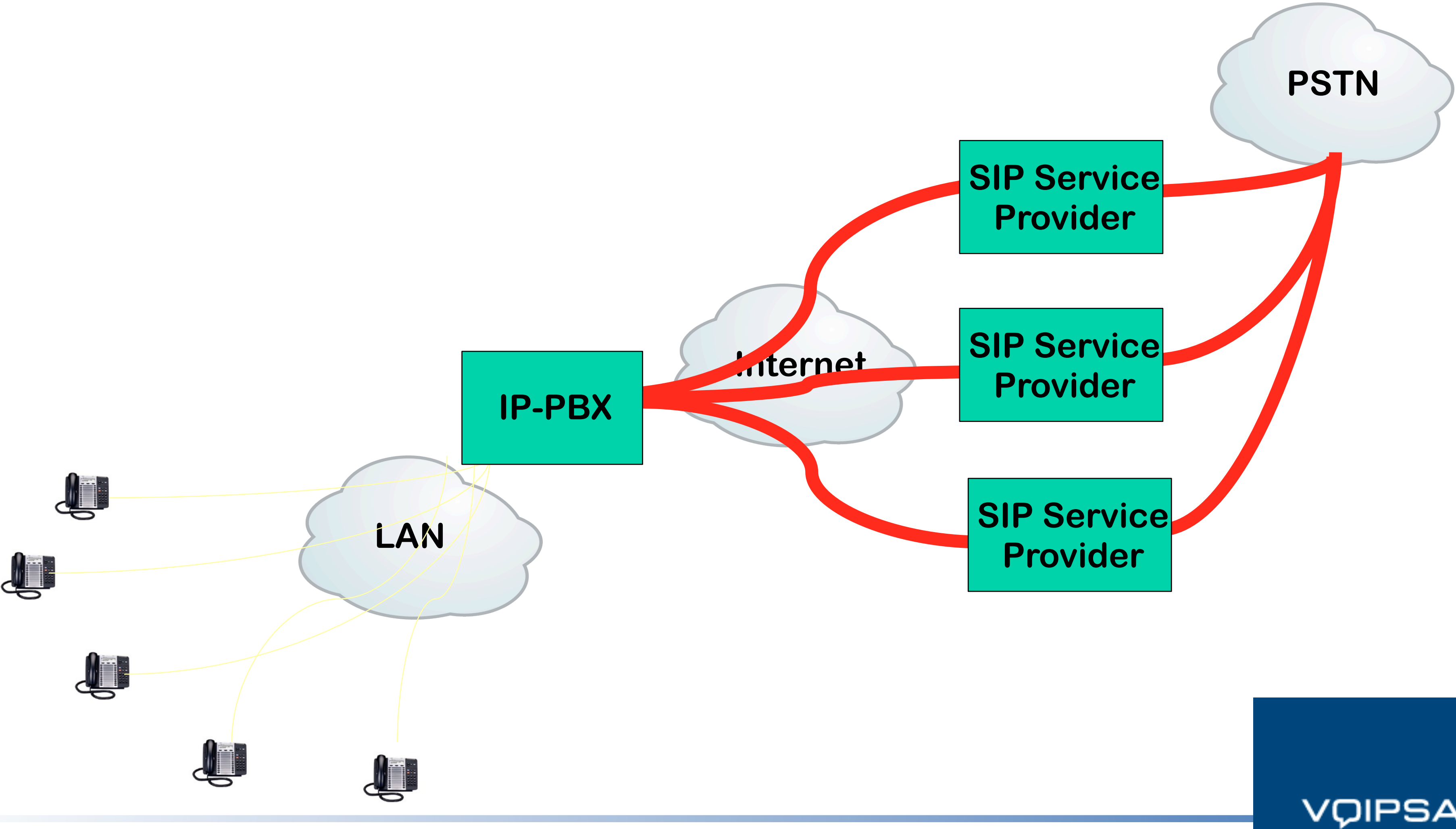
# The Challenge of SIP Trunking



# SIP Trunking - Business Continuity



# SIP Trunking - Business Continuity

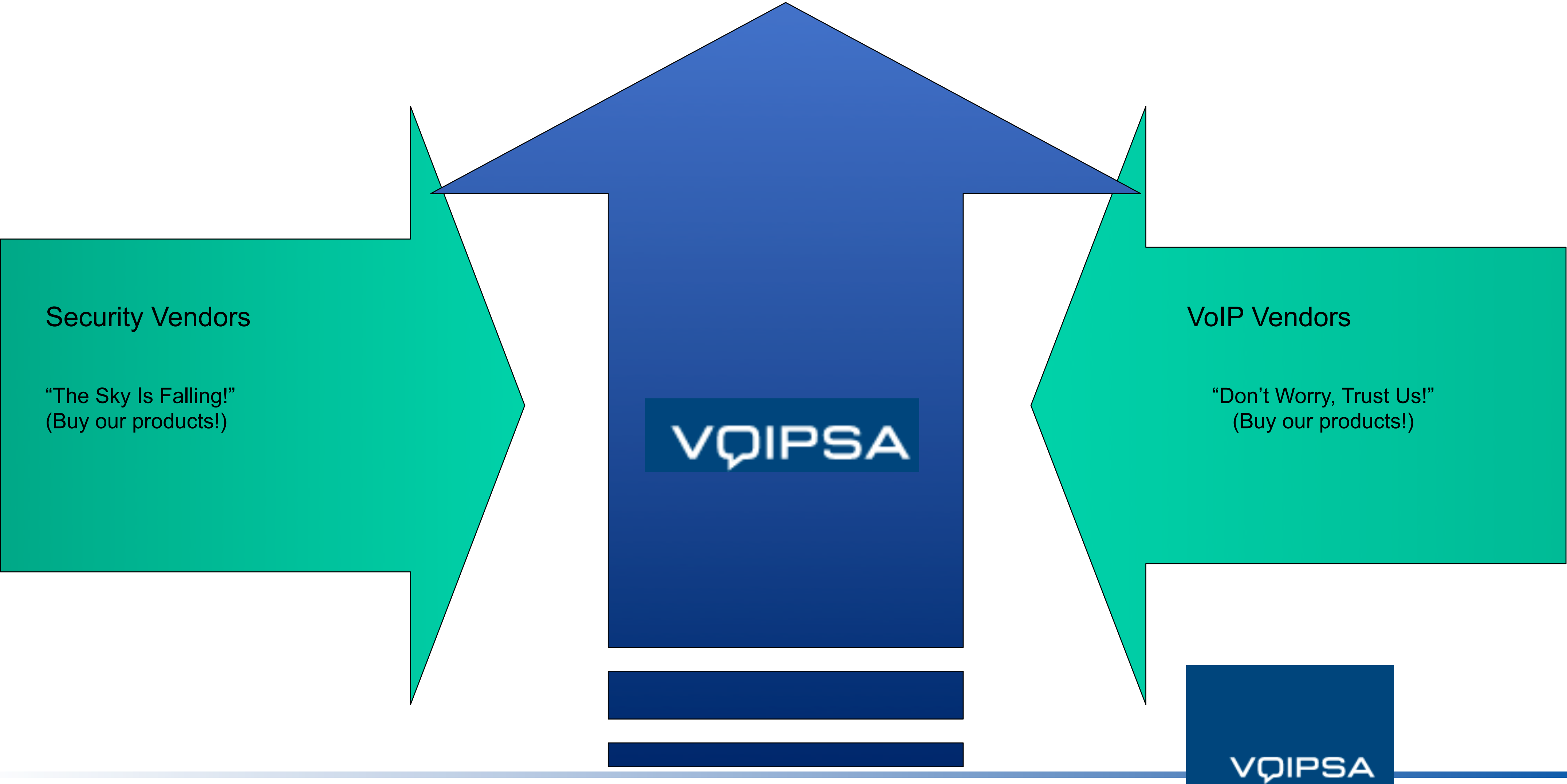


# Resources



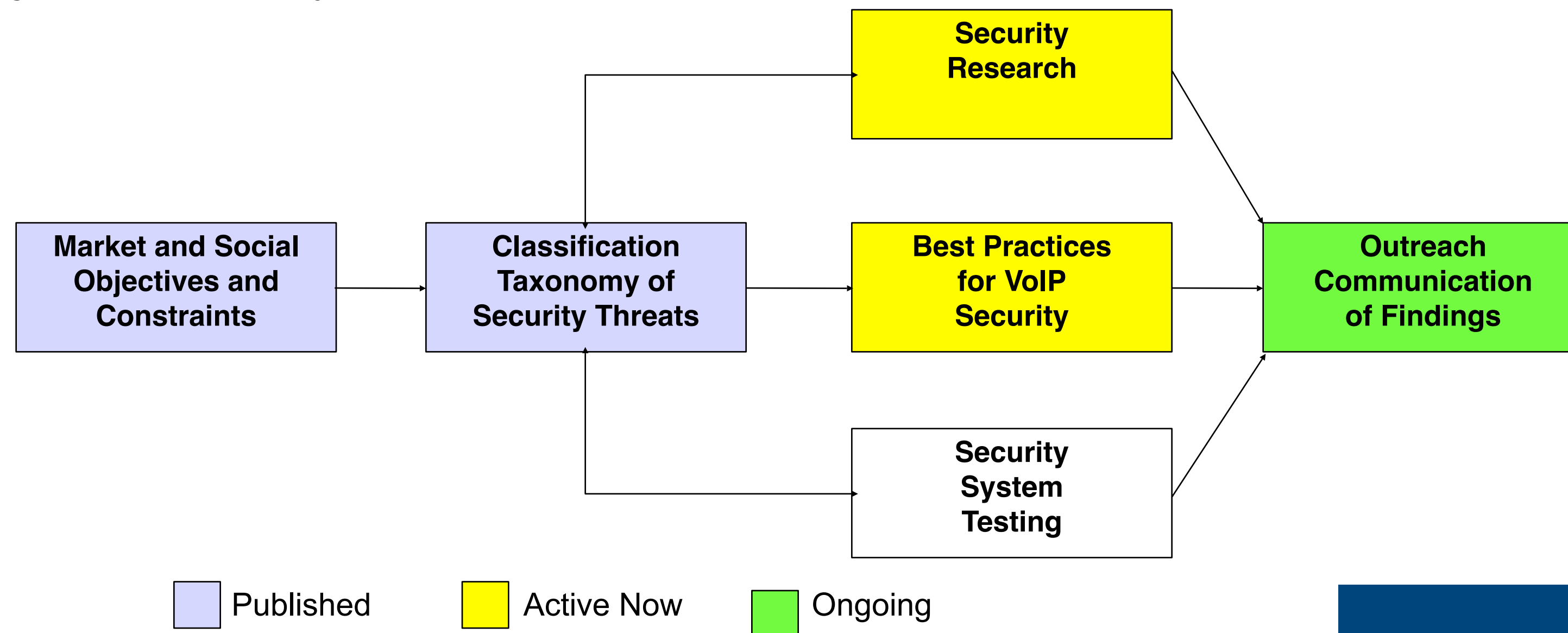


# What is the Industry Doing to Help?



# Voice Over IP Security Alliance (VOIPSA)

- [www.voipsa.org](http://www.voipsa.org) – 100 members from VoIP and security industries
- VOIPSEC mailing list – [www.voipsa.org/VOIPSEC/](http://www.voipsa.org/VOIPSEC/)
- “Voice of VOIPSA” Blog – [www.voipsa.org/blog](http://www.voipsa.org/blog)
- Blue Box: The VoIP Security Podcast – [www.blueboxpodcast.com](http://www.blueboxpodcast.com)
- VoIP Security Threat Taxonomy
- Best Practices Project underway now

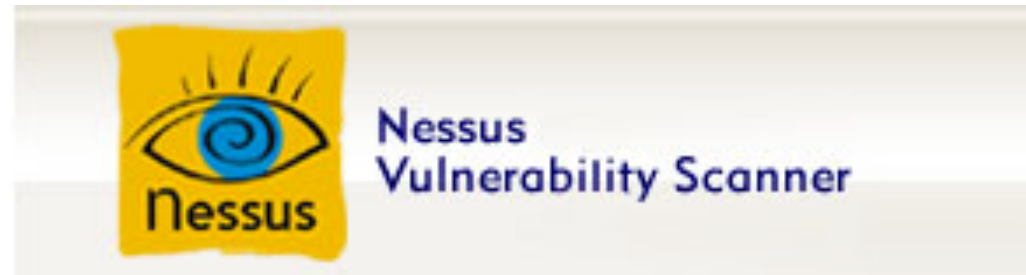


[www.voipsa.org/Resources/tools.php](http://www.voipsa.org/Resources/tools.php)

VOIPSA



**Intelligent Wardialer [IWar]**



*PROTOS - Security Testing of Protocol Implementations*

**Scapy**

SiVuS

**sipsak**

**SIPv6 Analyzer**  
An Analyzer for SIP and IPv6

**SIPp**

SIPcrack - SIP login dumper/cracker

**CODENOMICON**

**vomit - voice over misconfigured[1] internet telephones**

**ASTEROID SIP Denial of Service Tool**

**VOIPSA**

# Tools, tools, tools...

- UDP Flooder
- IAX Flooder
- IAX Enumerator
- ohrwurm RTP Fuzzer
- RTP Flooder
- INVITE Flooder
- AuthTool
- BYE Teardown
- Redirect Poison
- Registration Hijacker
- Registration Eraser
- RTP InsertSound
- RTP MixSound
- SPITTER
- Asteroid
- enumIAX
- iWar
- StegRTP
- VoiPong
- Web Interface for SIP Trace
- SIPScan
- SIPCrack
- SiVuS
- SIPVicious Tool Suite
- SIPBomber
- SIPsak
- SIP bot

# Security Links

- VoIP Security Alliance - <http://www.voipsa.org/>
  - Threat Taxonomy - <http://www.voipsa.org/Activities/taxonomy.php>
  - VOIPSEC email list - <http://www.voipsa.org/VOIPSEC/>
  - Weblog - <http://www.voipsa.org/blog/>
  - Security Tools list - <http://www.voipsa.org/Resources/tools.php>
  - Blue Box: The VoIP Security Podcast - <http://www.blueboxpodcast.com>
- NIST SP800-58, “Security Considerations for VoIP Systems”
  - <http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>
- Network Security Tools
  - <http://sectools.org/>
- Hacking Exposed VoIP site and tools
  - <http://www.hackingvoip.com/>

**VoIP can be *more* secure  
than the PSTN *if* it is  
properly deployed.**

**Please  
Practice  
Safe  
VoIP!**

**VOIPSA**



# Q&eh?



[www.voipsa.org](http://www.voipsa.org)



# Speaker Introduction – Dan York

Dan York, CISSP, is the Best Practices Chair for the VOIP Security Alliance where he leads the project to develop and document a concise set of industry-wide best practices for security VoIP systems. He is also heading up VOIPSA's move into "social media" with the launch of the "Voice of VOIPSA" group weblog. Additionally, York is the producer of "Blue Box: The VoIP Security Podcast" ([www.blueboxpodcast.com](http://www.blueboxpodcast.com)) where each week he and co-host Jonathan Zar discuss VoIP security news and interview people involved in the field.

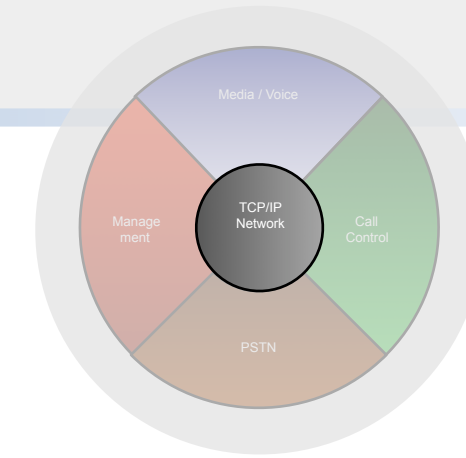
Dan currently serves as the Director of Emerging Communication Technology for the CTO of Voxeo Corporation focused on analyzing and evaluating new technologies to understand their potential impact on the ways in which we communicate. He participates in industry standards organizations on behalf of Voxeo and also assists in ensuring Voxeo's voice application services are secure.

Prior to joining Voxeo in 2007 he served as Director of IP Technology reporting to the CTO of Mitel Corporation and focused on emerging VoIP technology and VoIP security. As chair of Mitel's Product Security Team, he coordinates the efforts of a cross-functional group to communicate both externally and internally on VoIP security issues, respond to customer inquiries related to security, investigate security vulnerability reports, and monitor security standards and trends. Previously, York served in Mitel Product Management bringing multiple products to market including Mitel's secure VoIP Teleworker Solution in 2003.

His writing can also be found online at his weblog, Disruptive Telephony at [www.disruptivetelephony.com](http://www.disruptivetelephony.com).

The logo for VOIPSA, consisting of the letters "VOIPSA" in a white, sans-serif font, centered within a dark blue square.

# Other Best Practices



- Network

- Networks should be evaluated for readiness to carry VoIP traffic.
- Secure mechanisms should be used for traversal of firewalls.

- Phone Sets

- Set software loads should be encrypted and tamper-proof.
- Sets should run the minimum of services required.
- Connection of a set to the system must require an initial authentication and authorization.

- Servers

- Servers should be incorporated into appropriate patch management and anti-virus systems.
- Sufficient backup power should be available to maintain operation of telephony devices (and necessary network infrastructure) in the event of a power failure.

- Wireless

- All wireless devices should implement WPA and/or WPA2 versus WEP.