SIP Trunking & Security

Dan York, CISSP
VOIPSA Best Practices Chair

VOIPSA

September 2, 2009

VOIPSA

Blue Box

The VoIP Security Podcast
www.blueboxpodcast.com

voxeo

VOIPSA

Privacy **Availability**

Compliance **Confidence**

Mobility **Cost Avoidance**

Business Continuity

VOIPSA


VoIP | Wireless | Mobile | Networks

The Register » Comms » VoIP »

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 - Whe

With VoIP rapidly
barcode scanners,
shaped - a predicti

VIPER reckons tha
start to become se
Communications

LIGHT READING

NEWS ANALYSIS

Go to a section GO

Home > News Analysis > VOIP

Discuss Print Email License content Reprint Article

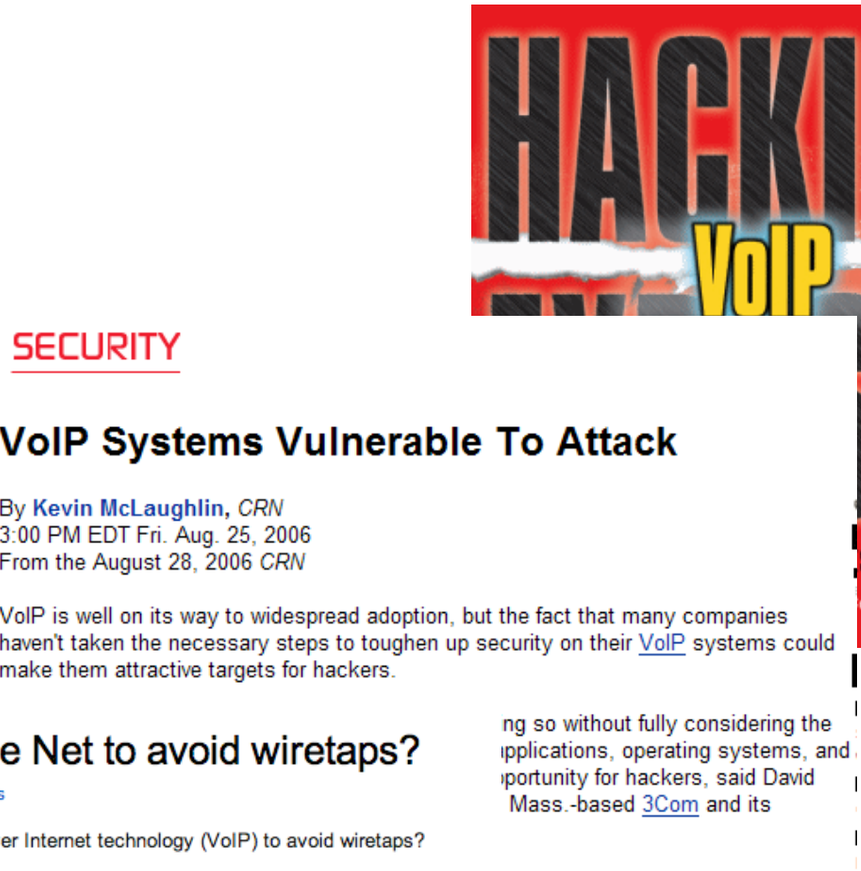
Two Charged in VOIP Hacking Scandal

JUNE 09, 2006

Discuss >

Fede
whol

Rob
had


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.

ng so without fully considering the
pplications, operating systems, and
portunity for hackers, said David
Mass.-based 3Com and its

HACKING
VoIP
SED
s & Solutions
ollier

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.

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Security Considerations for Voice Over IP Systems

Recommendations of the National Institute of Standards and Technology


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.

VOIPSA

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

Done

VOIPSA

WIRESHARK

Intelligent Wardialer [IWar]

Nessus Vulnerability Scanner

PROTOS - Security Testing of Protocol Implementations

SiVuS

SIPv6 Analyzer
An Analyzer for SIP and IPv6

Scapy

sipsak

SIPp

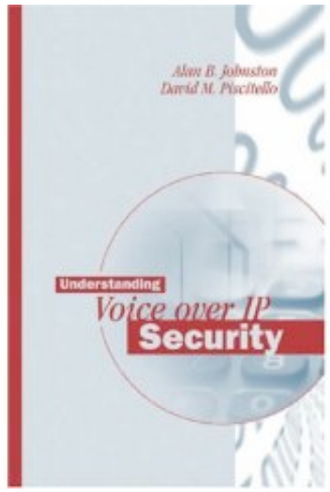
SIPcrack - SIP login dumper/cracker

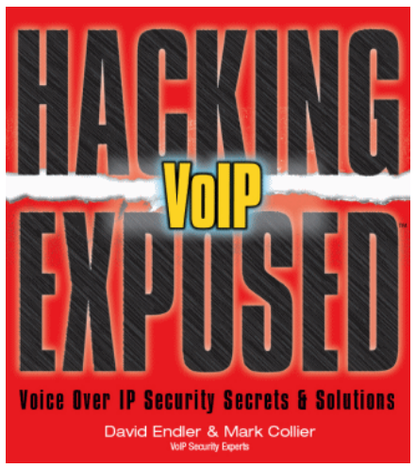
CODENOMICON

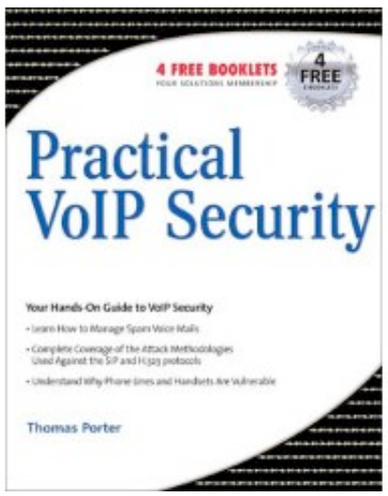
vomit - voice over misconfigured[1] internet telephones

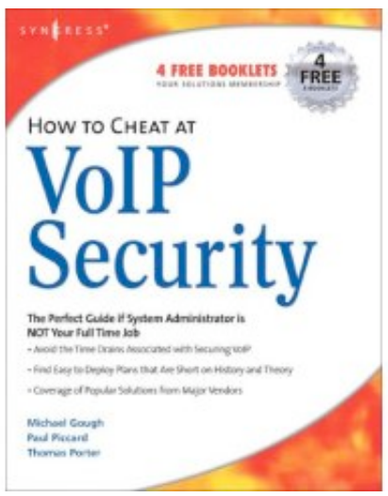
ASTEROID SIP Denial of Service Tool

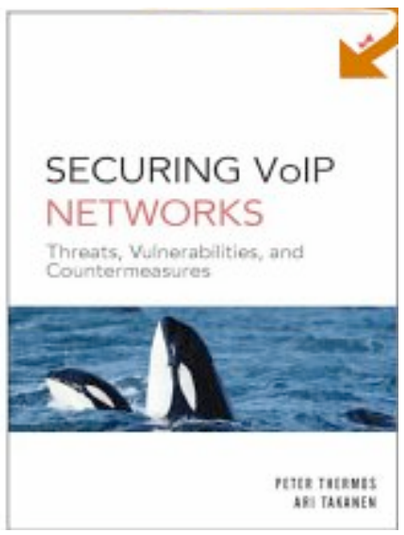
VOIPSA

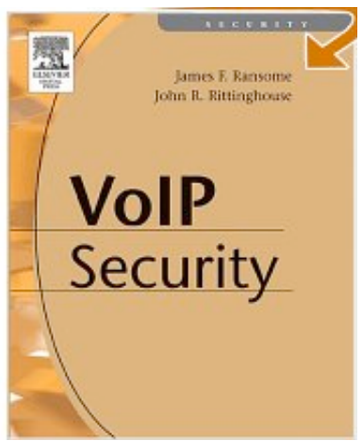












VOIPSA

TDM security is relatively simple...

PSTN Gateways

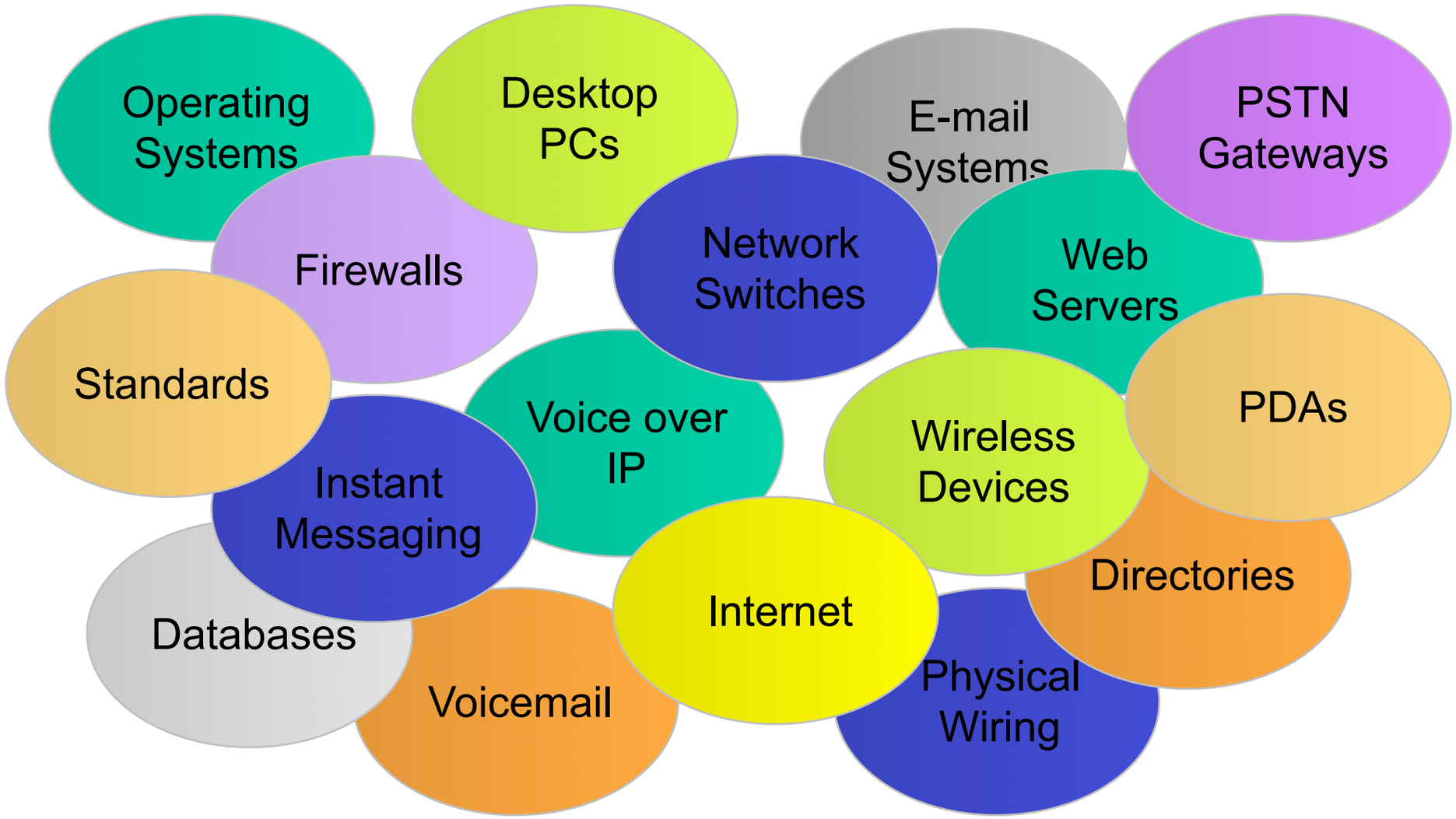
TDM Switch

Voicemail

Physical Wiring

VOIPSA

VoIP security is more complex



VOIPSA

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

VOIPSA

VoIP Security Concerns

VOIPSA

Security concerns in telephony are not new…

Image courtesy of the Computer History Museum

VOIPSA

Nor are our attempts to protect against threats…

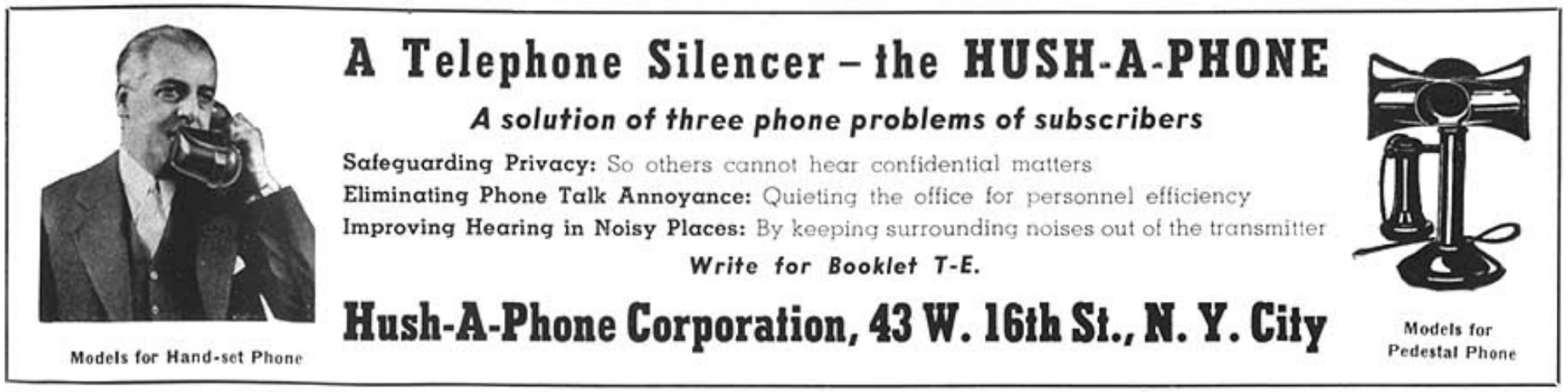
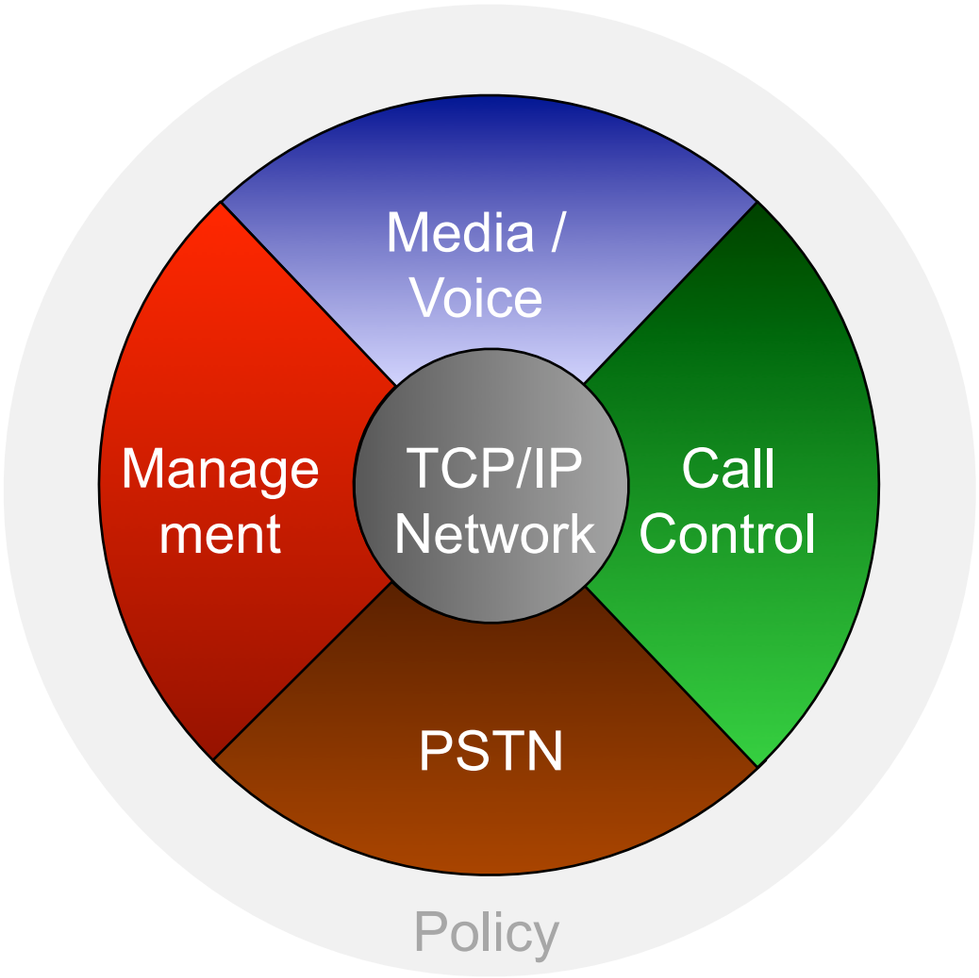
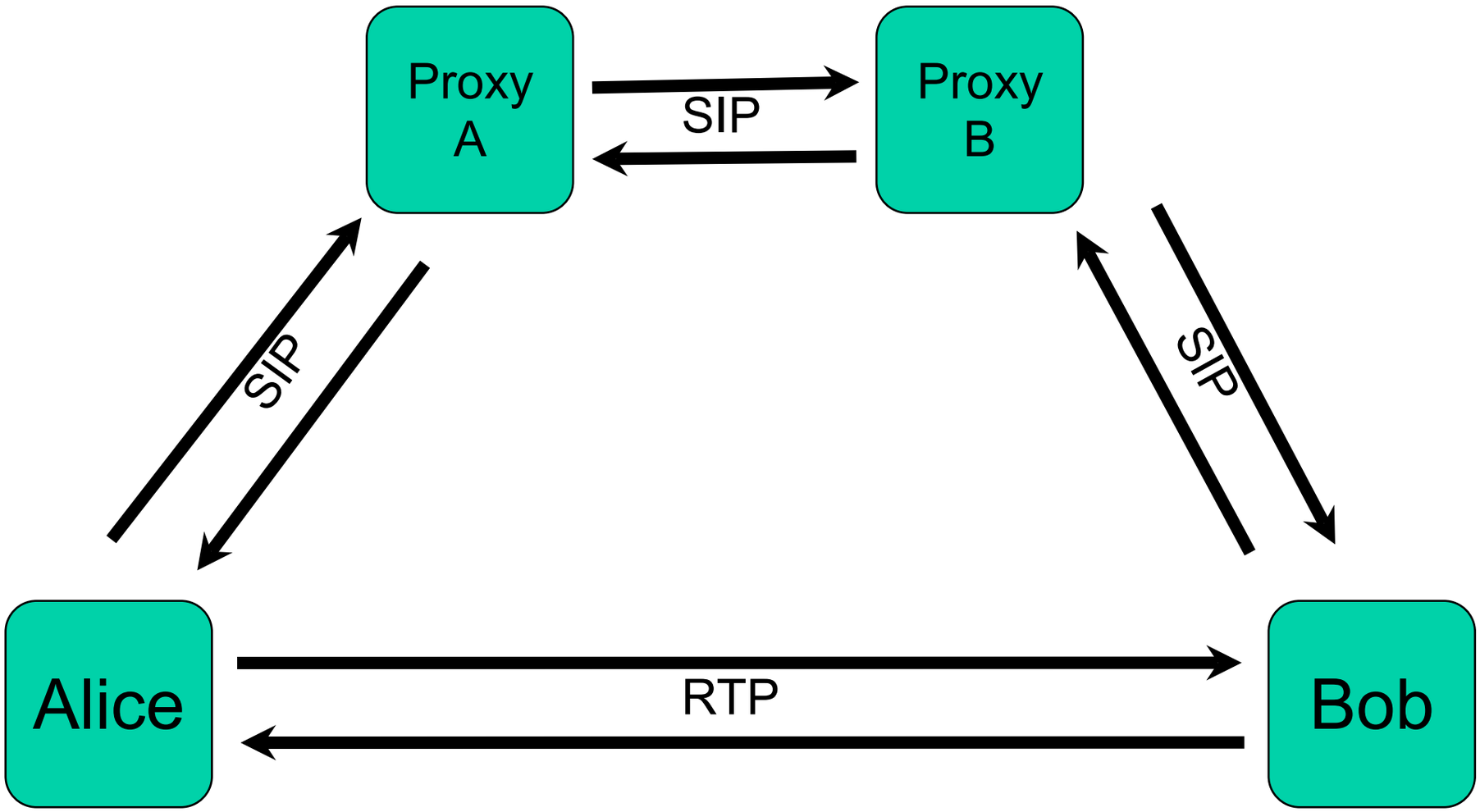


Image courtesy of Mike Sandman – http://www.sandman.com/

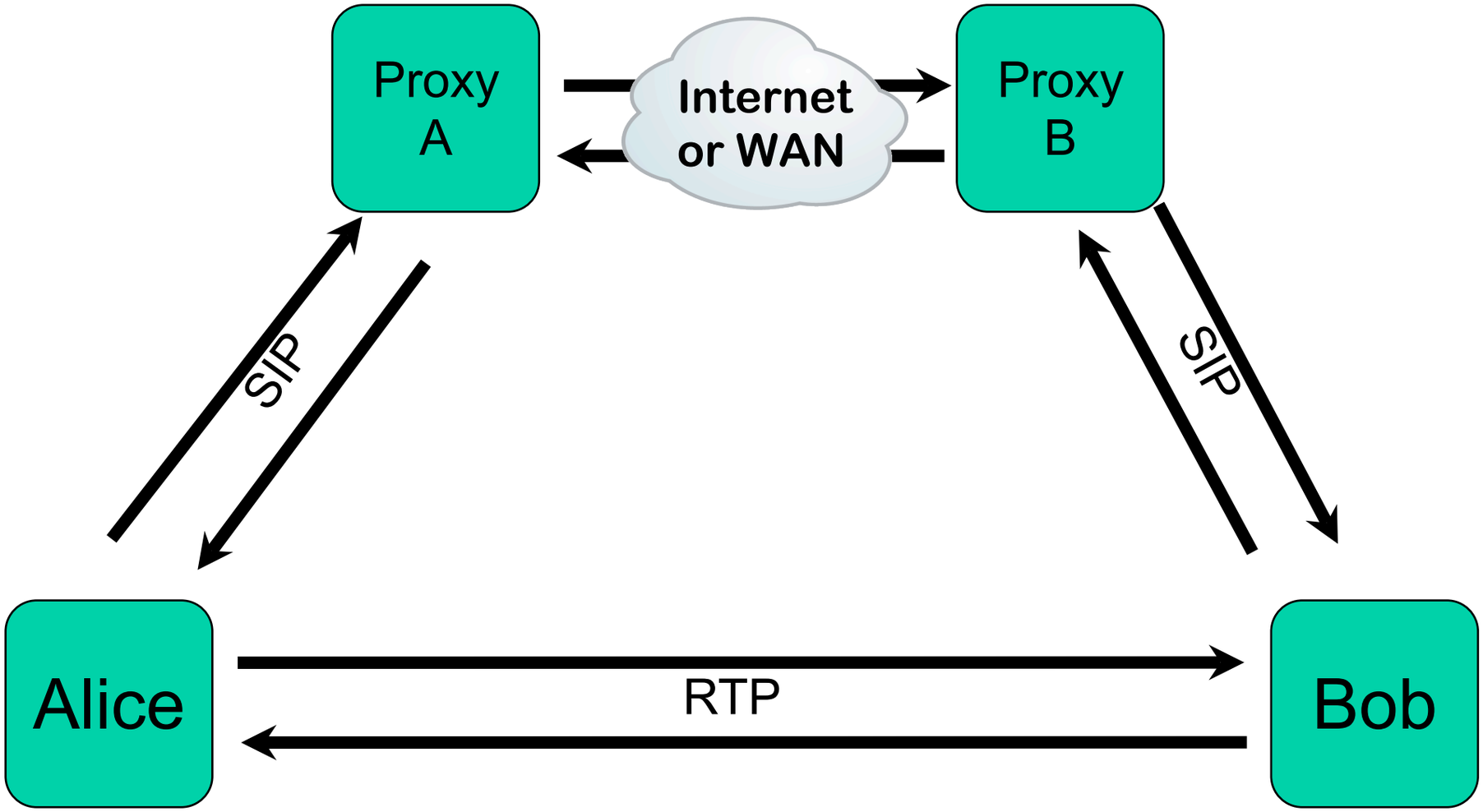
Security Aspects of IP Telephony



The SIP Call Flow



The SIP Call Flow



Media

Eavesdropping

Degraded Voice Quality

Encryption

Virtual LANs (VLANs)

Packet Filtering

VOIPSA

Signaling

Denial of Service

Impersonation

Toll Fraud

Encryption

Encrypted Phone Software

Proper Programming

VOIPSA

Management

Web Interfaces

APIs!

Phones!

Encryption

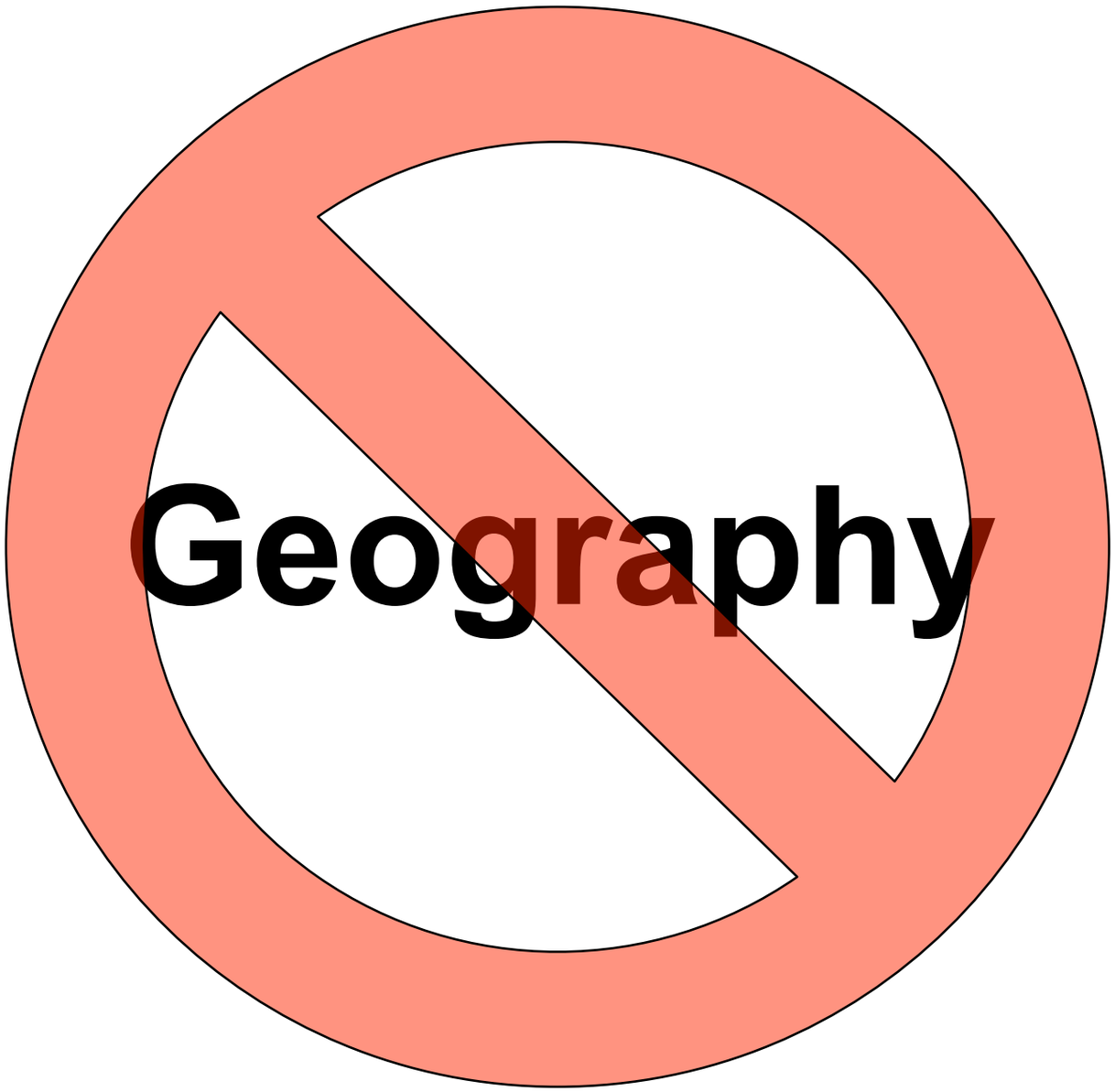
Change Default Passwords!

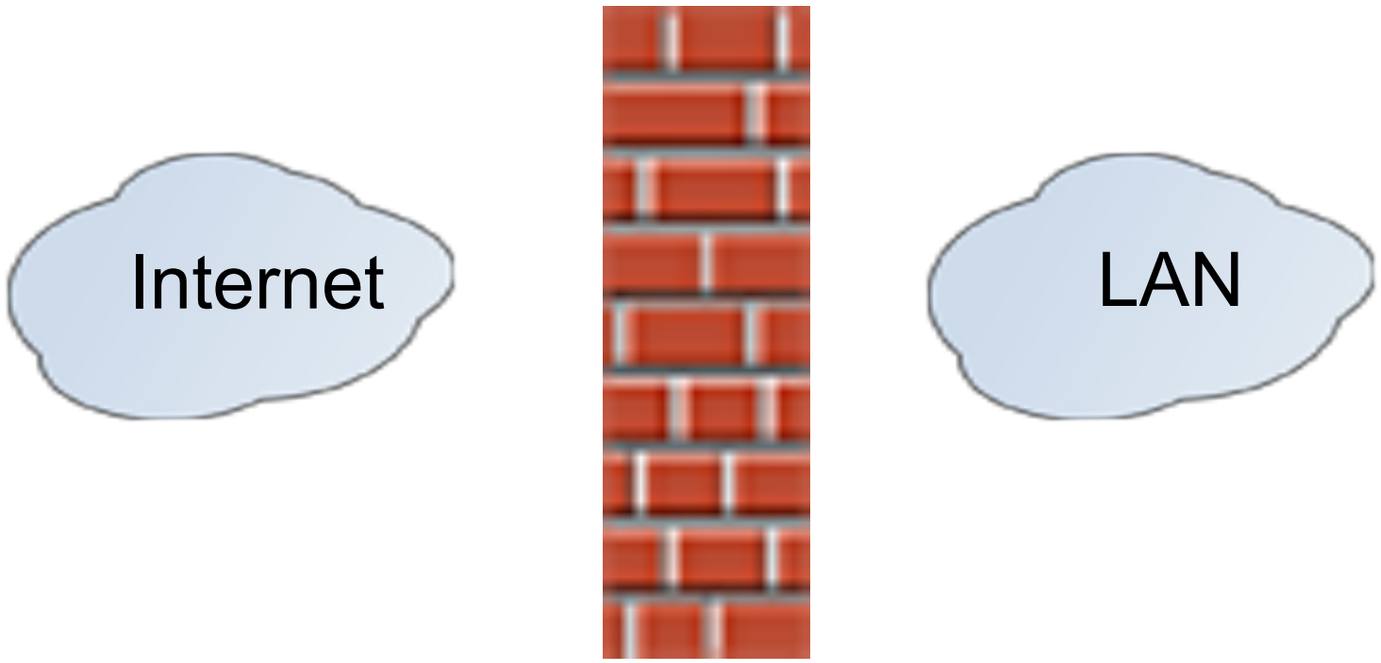
Patches? We don't need...

VOIPSA

PSTN

VOIPSA

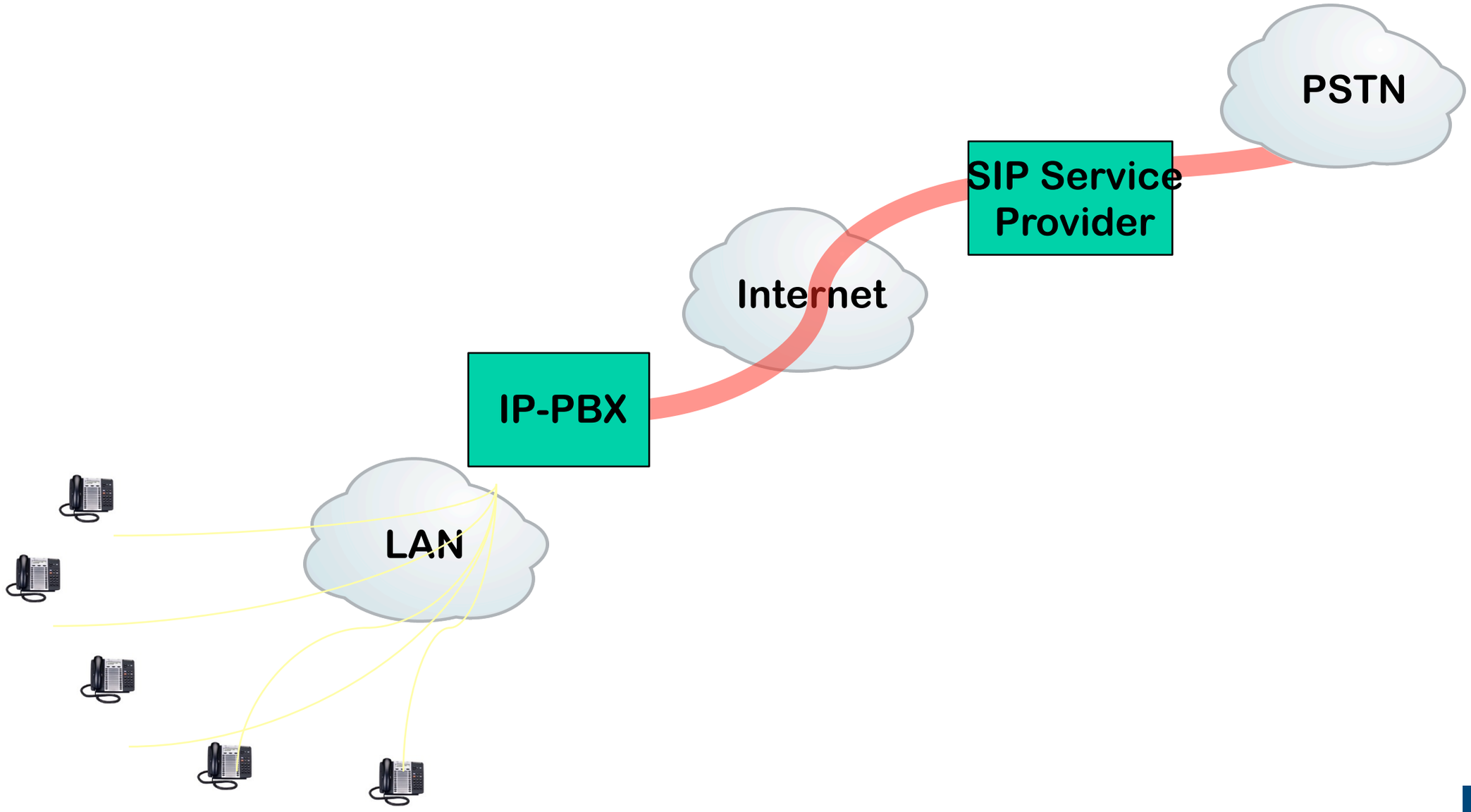




SIP Trunking

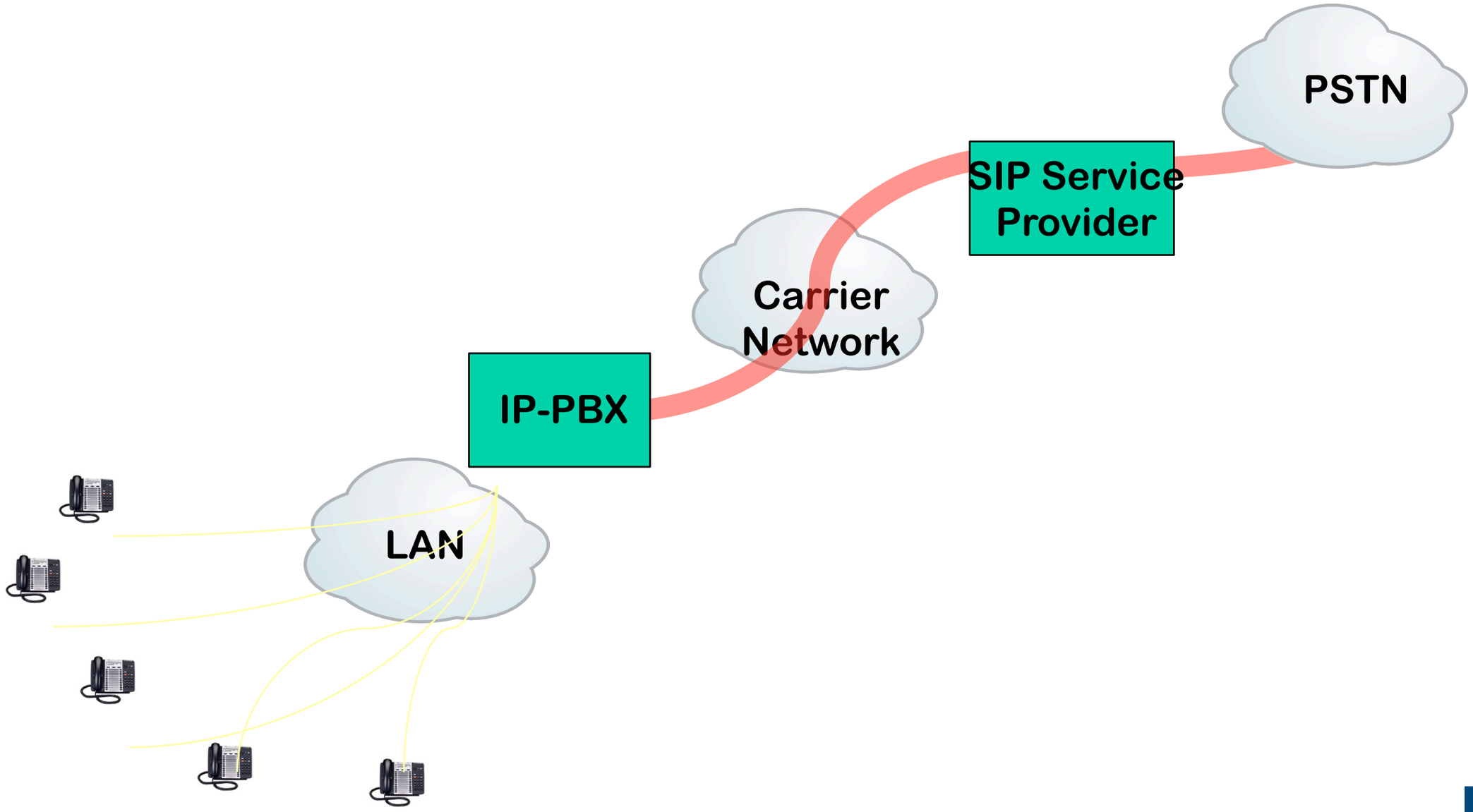
VOIPSA

The Challenge of SIP Trunking

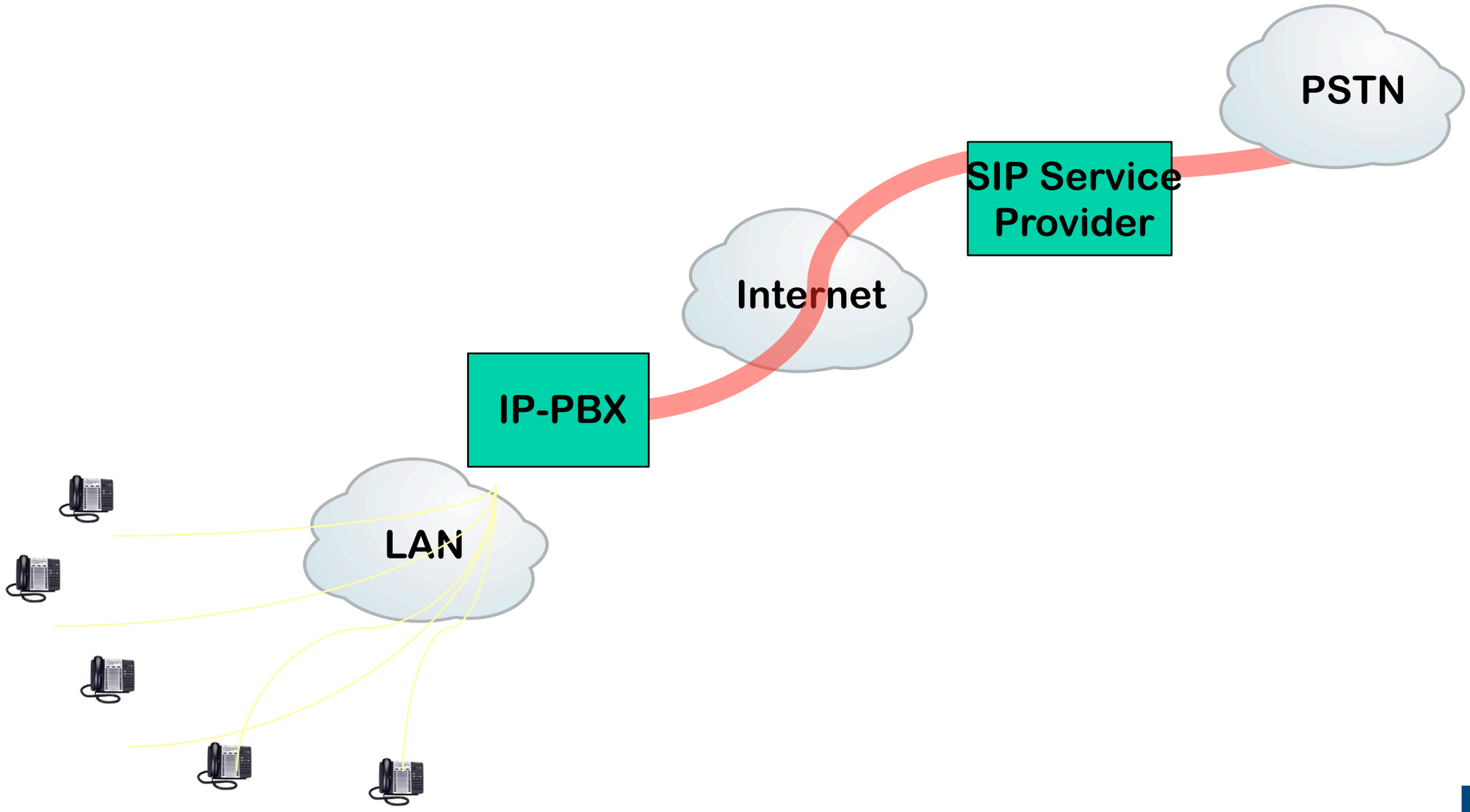


VOIPSA

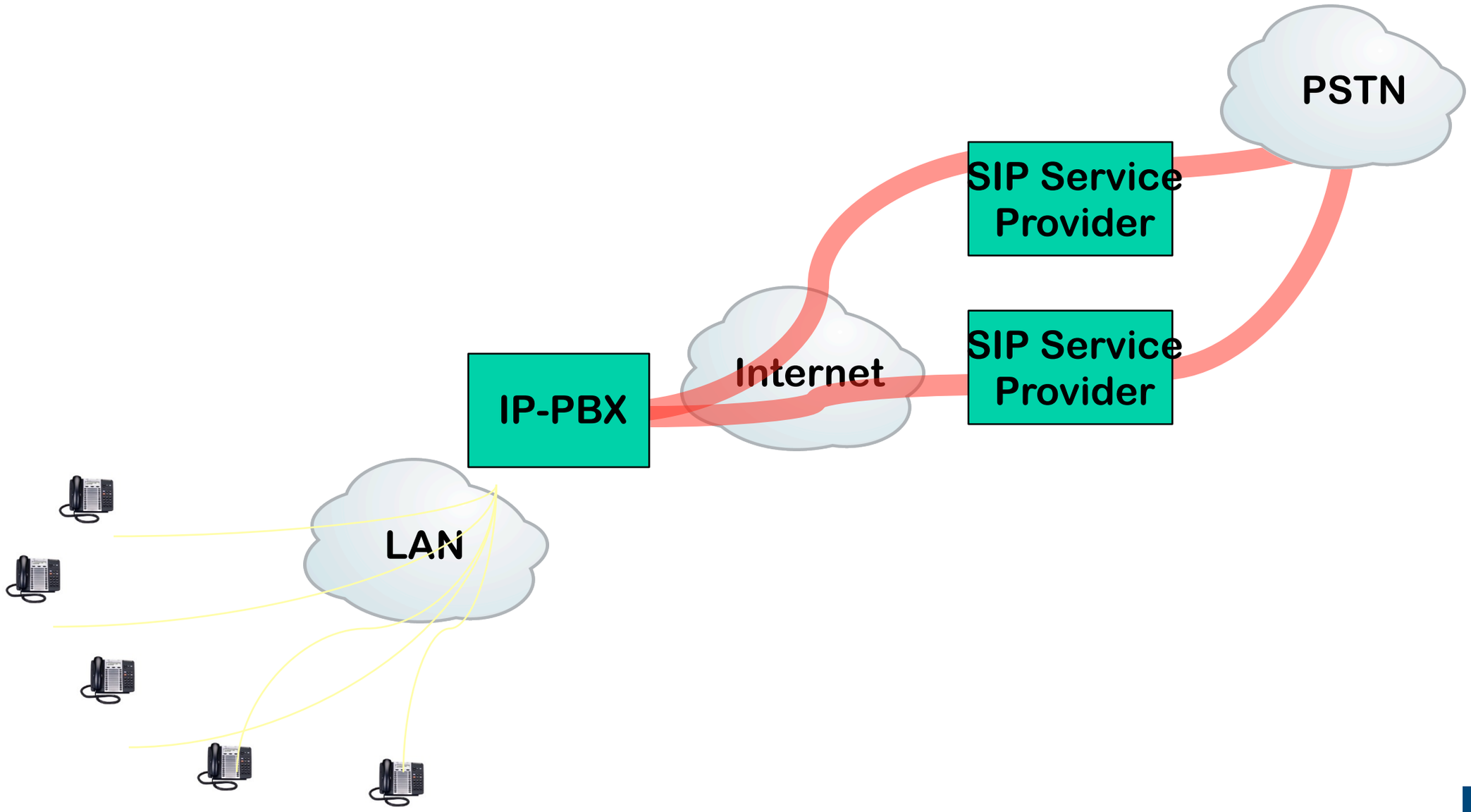
SIP Trunking



The Challenge of SIP Trunking

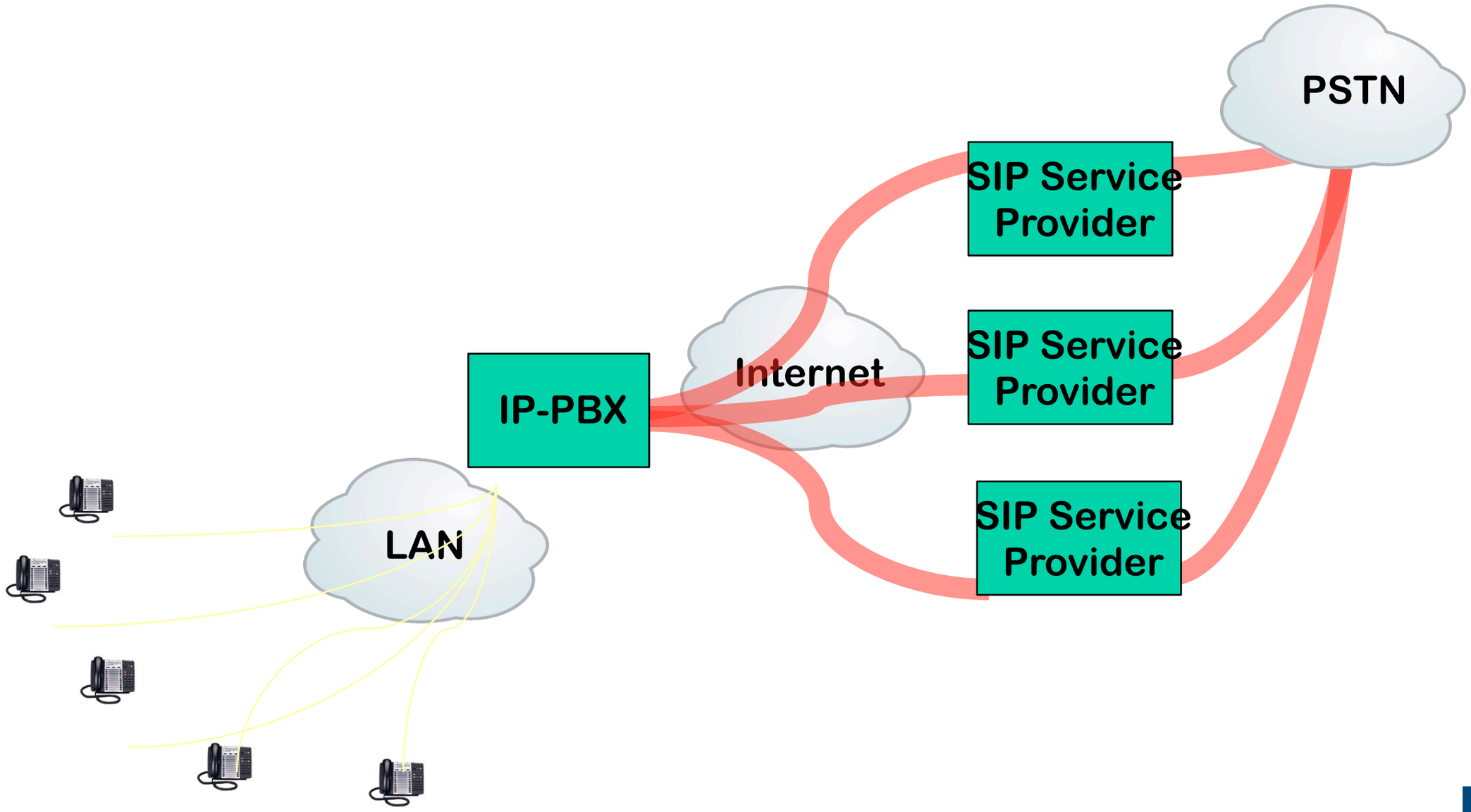


SIP Trunking - Business Continuity



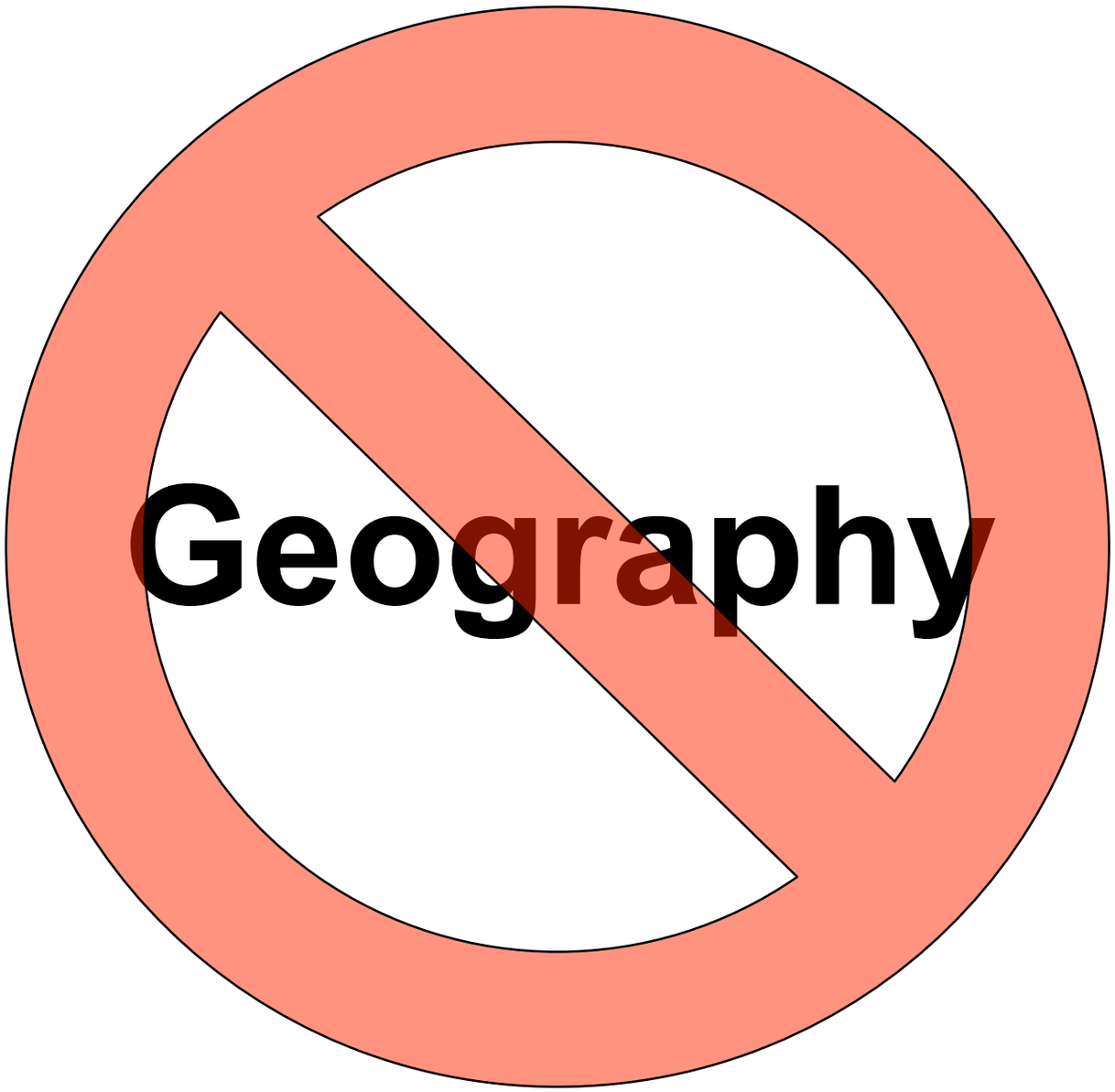
VOIPSA

SIP Trunking - Business Continuity

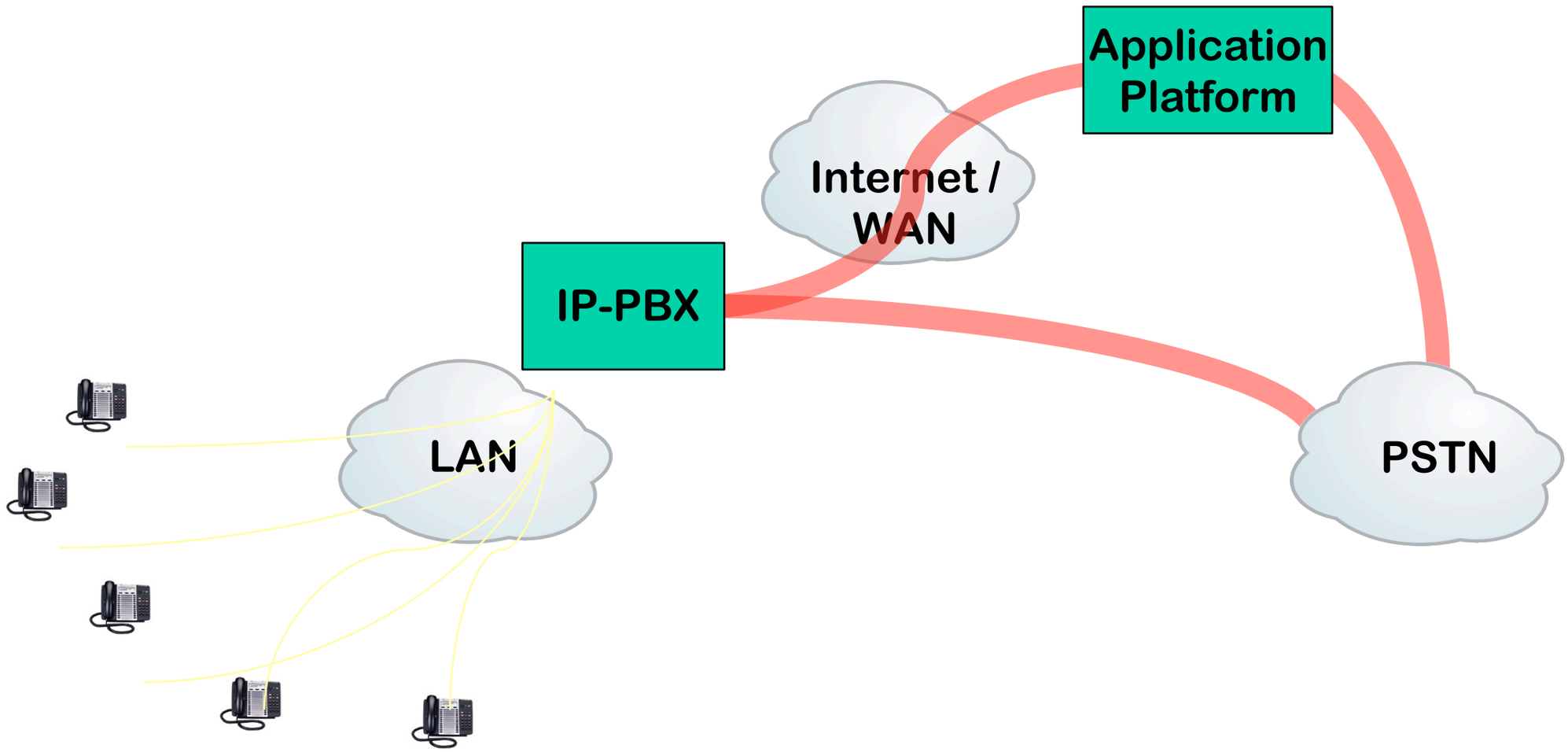


Cloud Computing

VOIPSA

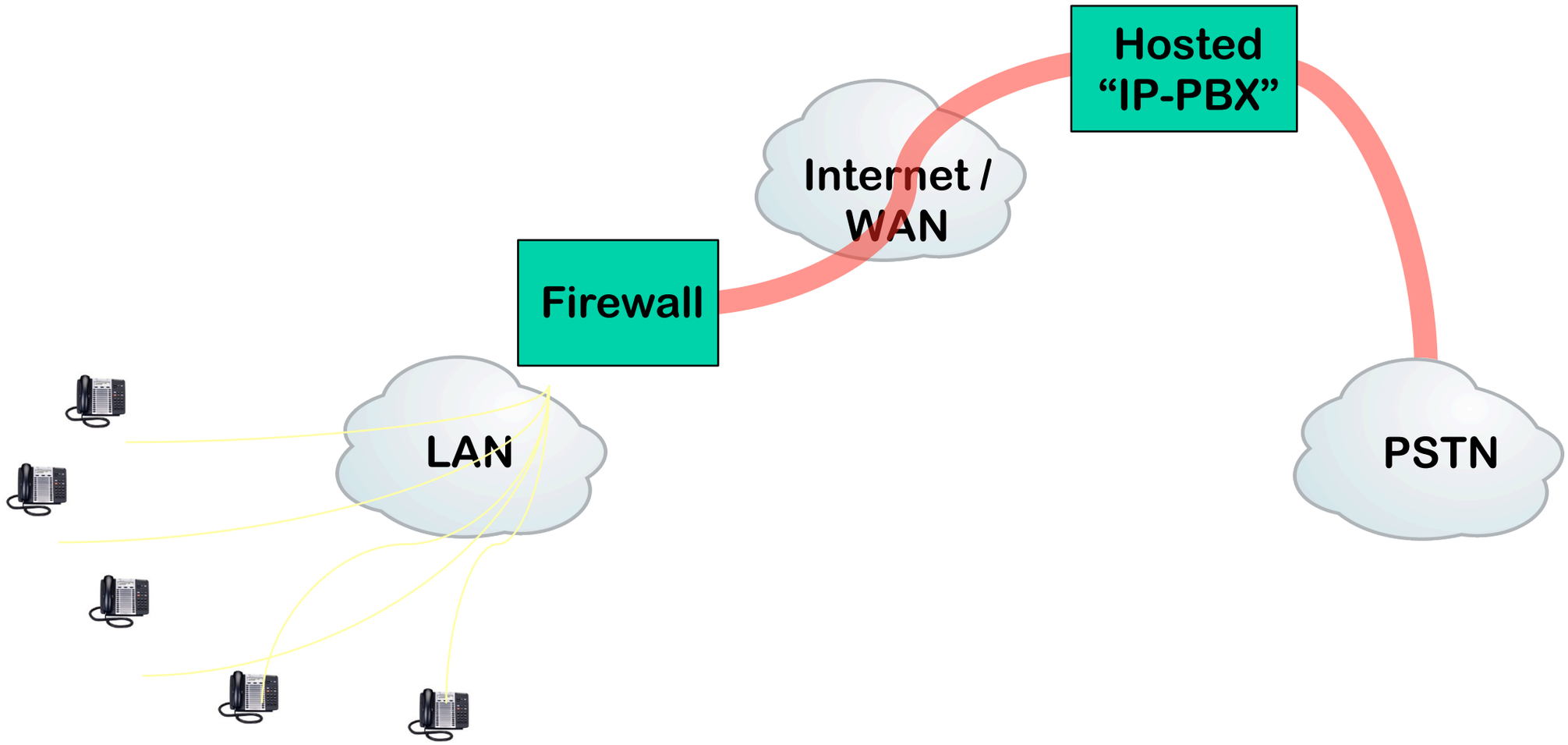


Moving Voice Applications into “the Cloud”



VOIPSA

Moving Telephony into “the Cloud”



Can you trust “the Cloud” to be there?

Questions for SIP Trunk Providers or Cloud Computing Platforms?

- What kind of **availability** guarantees / Service Level Agreements (SLAs) does the platform vendor provide?
- What kind of **geographic redundancy** is built into the underlying network?
- What kind of **network redundancy** is built into the underlying network?
- What kind of **physical redundancy** is built into the data centers?
- What kind of **monitoring** does the vendor perform?
- What kind of **scalability** is in the cloud computing platform?
- What kind of **security**, both network and physical, is part of the computing platform?
- Finally, what will the vendor do if there is downtime? Will the downtime be reflected in your bill?

VOIPSA

Spam / SPIT

VOIPSA

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, PSTN is de facto firewall

VOIPSA

Resources

VQIPSA

What is the Industry Doing to Help?

Security Vendors

"The Sky Is Falling!"
(Buy our products!)

VOIPSA

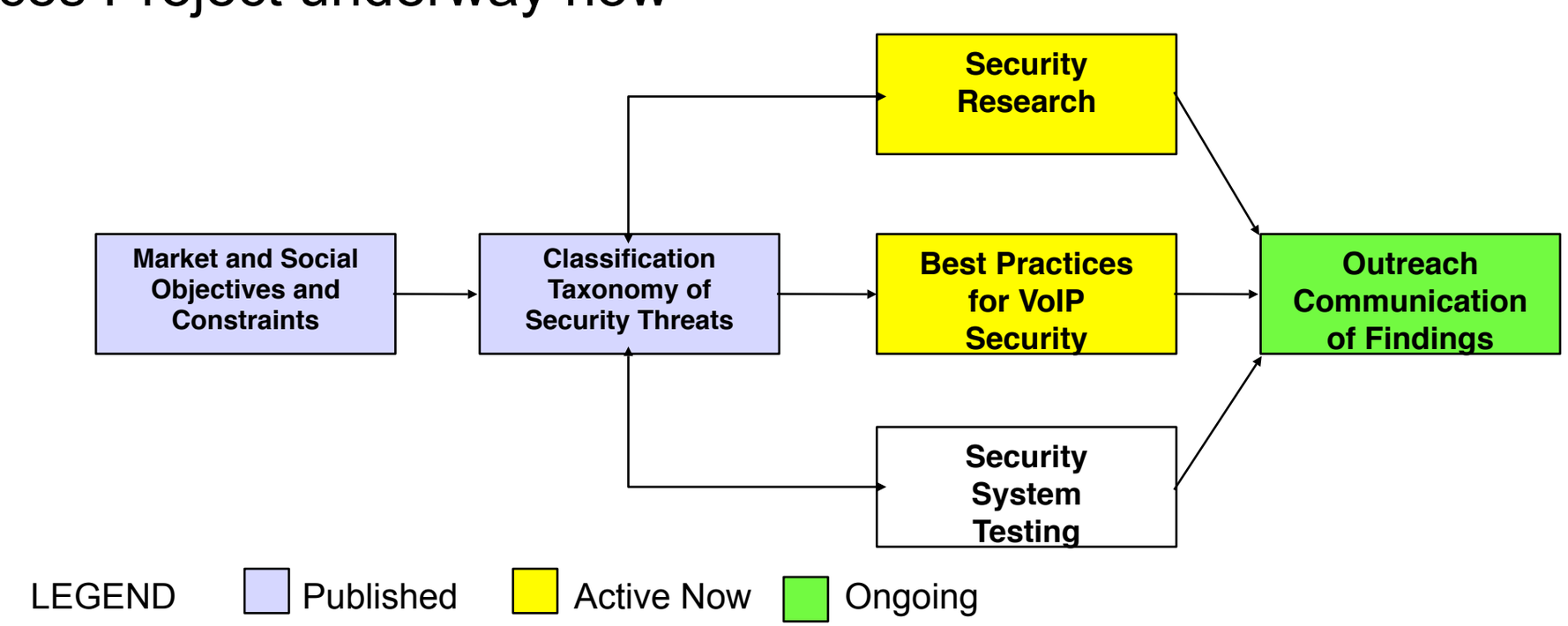
VoIP Vendors

"Don't Worry, Trust Us!"
(Buy our products!)

VOIPSA

Voice Over IP Security Alliance (VOIPSA)

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



www.voipsa.org/Resources/tools.php

WIRESHARK

Intelligent Wardialer [IWar]

Nessus Vulnerability Scanner

PROTOS - Security Testing of Protocol Implementations

SiVuS

SIPv6 Analyzer
An Analyzer for SIP and IPv6

Scapy

sipsak

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

VOIPSA

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.

VOIPSA

Q&eh?

www.voipsa.org

VOIPSA

Dan York - dan.york@voipsa.org