VoIP SECURITY

Dan Wing

dwing@cisco.com

Agenda

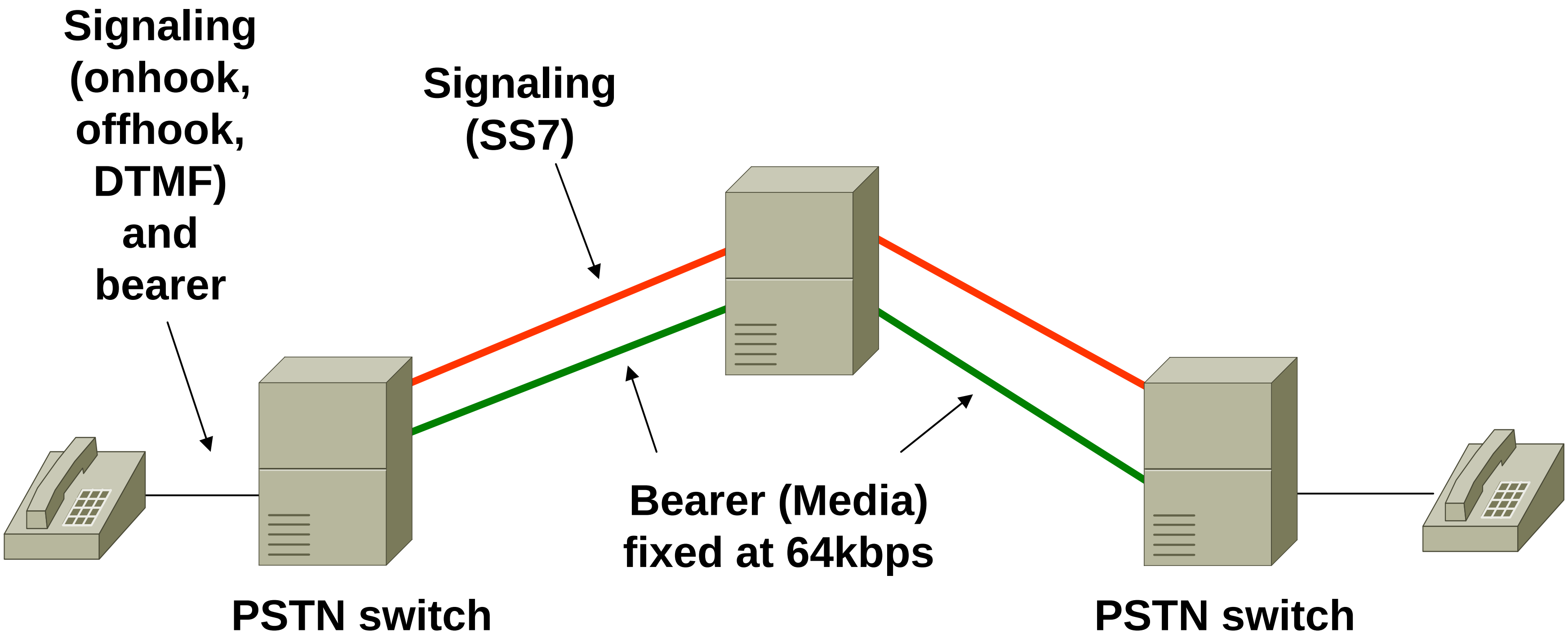
- Overviews

  PSTN

  VoIP

- VoIP Threats
- SIP Security Overview

Background: Basic PSTN Architecture


Signaling (onhook, offhook, DTMF) and bearer
Signaling (SS7)
Bearer (Media) fixed at 64kbps
PSTN switch
PSTN switch

- Transitive trust of signaling (and bearer)
- Active call reserves one bearer channel (DS0)
- Per-switch overload protection

VoIP Signaling and Media

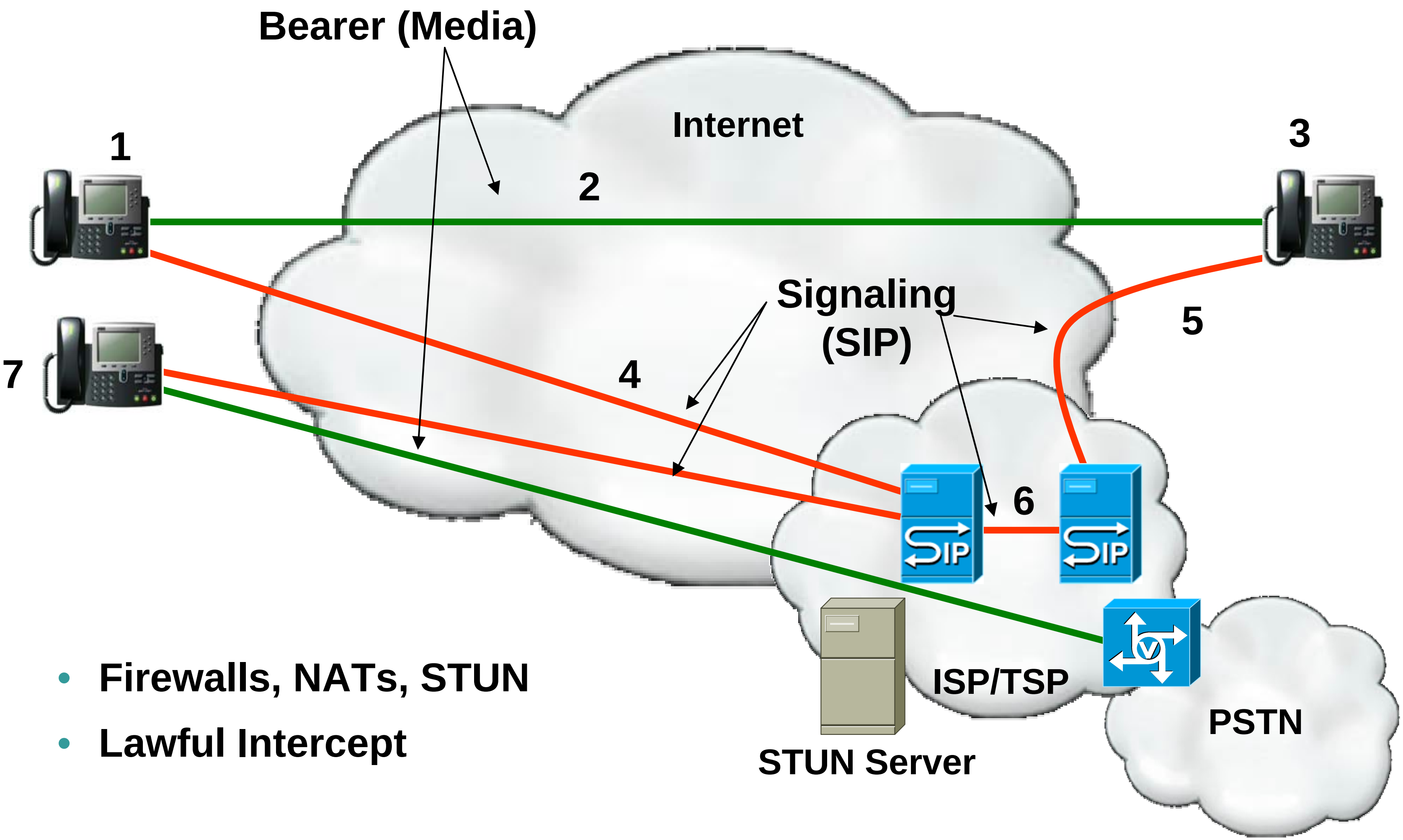
Signaling

- Dumb endpoints
  - MGCP, SGCP, TGCP (PacketCable)
  - H.248 (ITU), MEGACO (IETF)
  - SCCP (Cisco proprietary)
- Smart endpoints
  - SIP
  - H.323

Media

- RTP, RTCP (RFC3550)
  - Both run over UDP
  - Dynamic port numbers (signaled)
  - May carry fax, modem, DTMF, and TDD/TTY

Basic VoIP Architecture (Vonage-like model), STUN



- Firewalls, NATs, STUN
- Lawful Intercept

NAT & Firewall Traversal

- **ALGs - Application Layer Gateways**
  - **Easy to fool (on purpose or accidentally)**
  - **Require unencrypted signaling**
- **UDP Bindings**
  - **Combined with STUN (RFC 3489) allows voice through most NATs and firewalls**

How STUN (RFC 3489) Works

- **Bob pings the STUN server to discover the NAT’s public IP address and creates a mapping in the NAT**
- **Bob then tells this address to Alice**

Bob sends packet to stun server

NAT maps packet to be from 1.2.3.4:5555

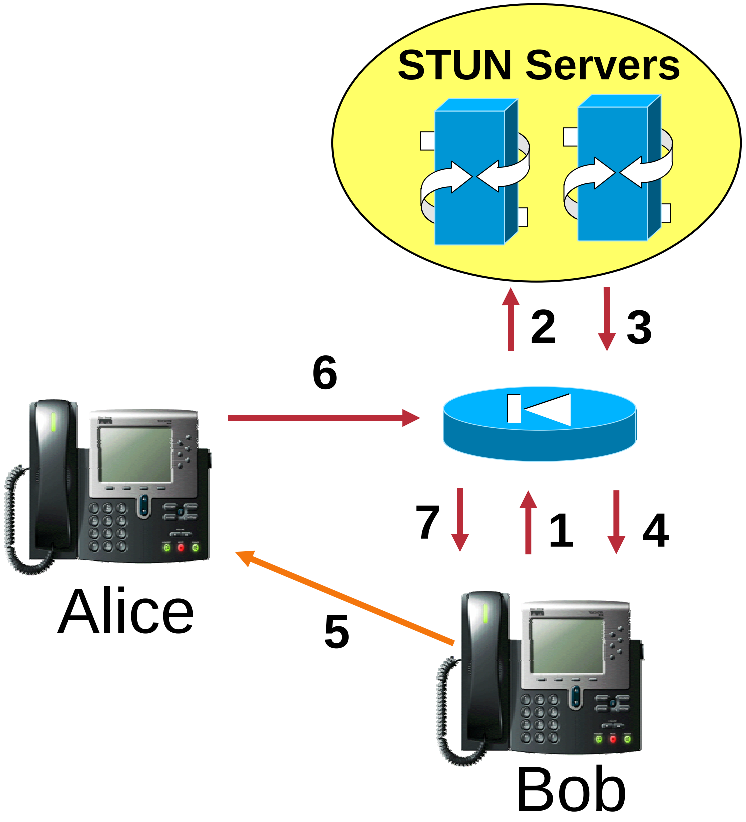
STUN replies and says address packet came from is 1.2.3.4:5555

NAT forwards to Bob

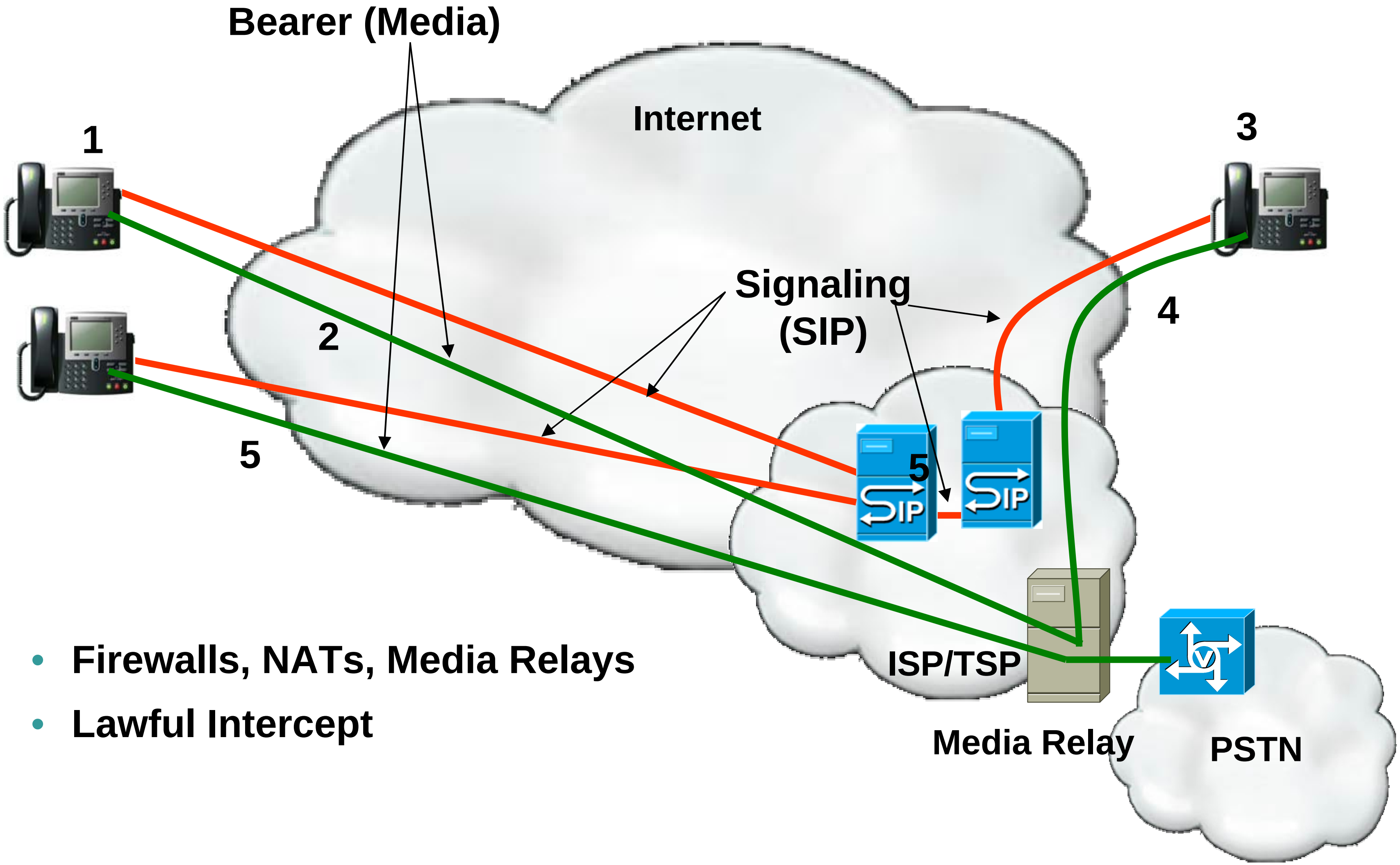
Bob tells Alice to send to 1.2.3.4:5555 and sends a packet to where Alice will send from

Alice sends to 1.2.3.4:5555

NAT forwards to Bob

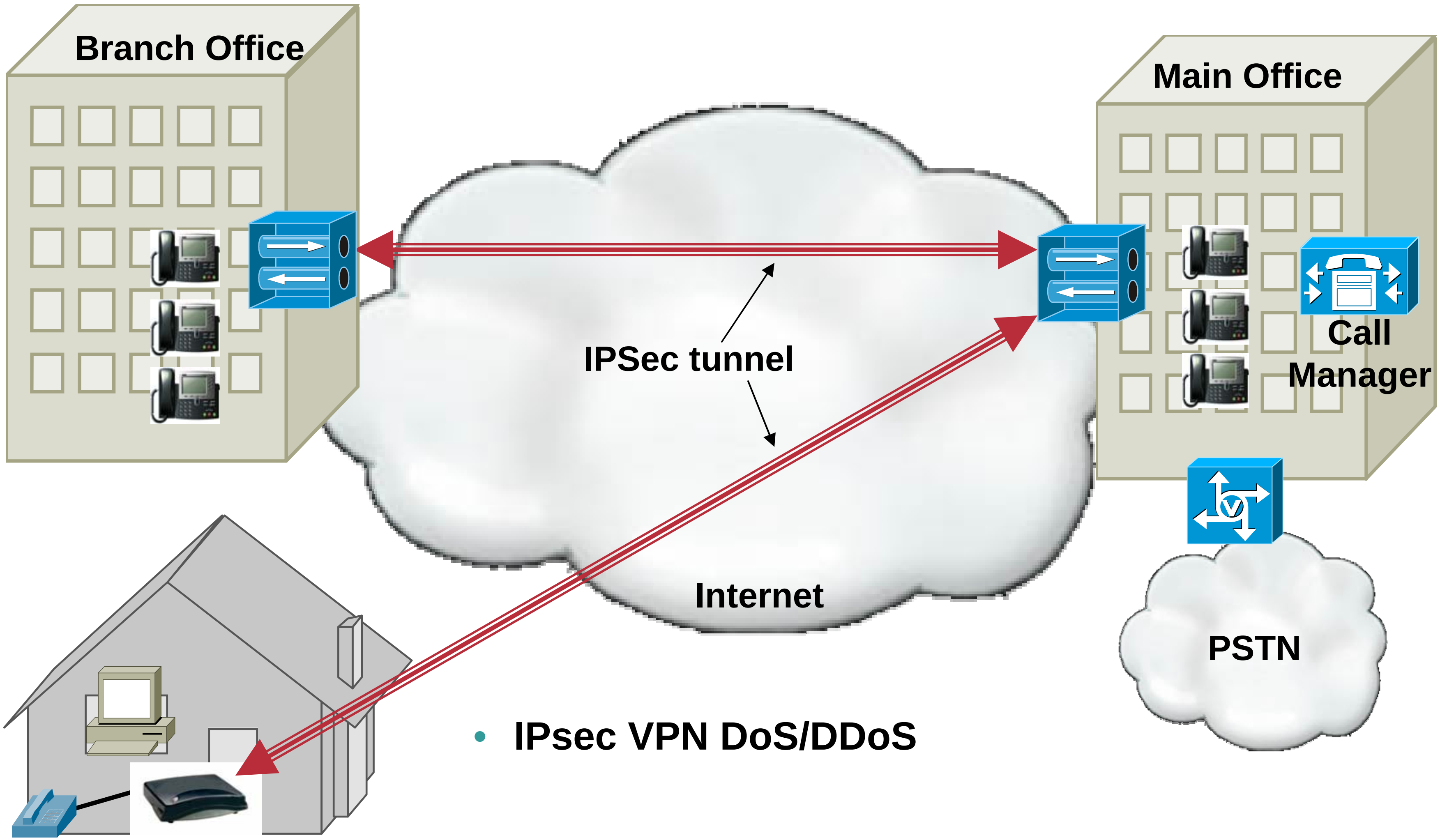


Basic VoIP Architecture (Vonage-like model), Media Relay



- Firewalls, NATs, Media Relays
- Lawful Intercept

Typical Enterprise Deployment

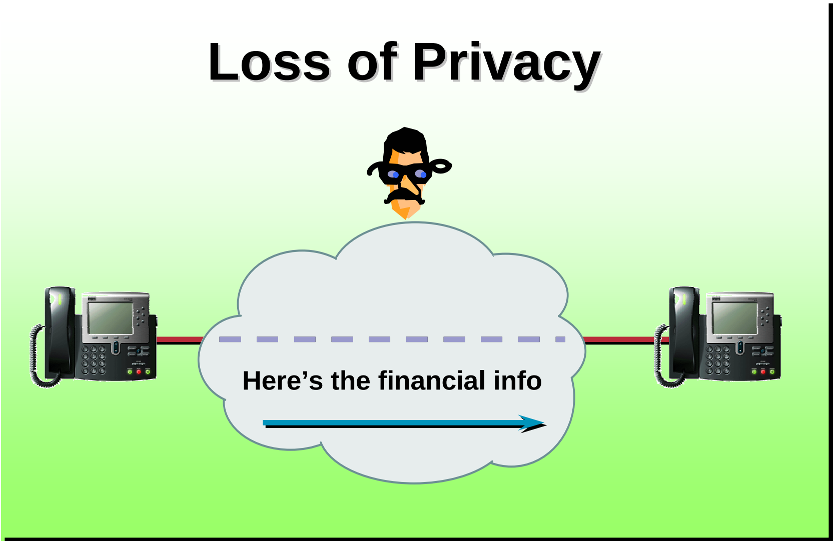


- **IPsec VPN DoS/DDoS**

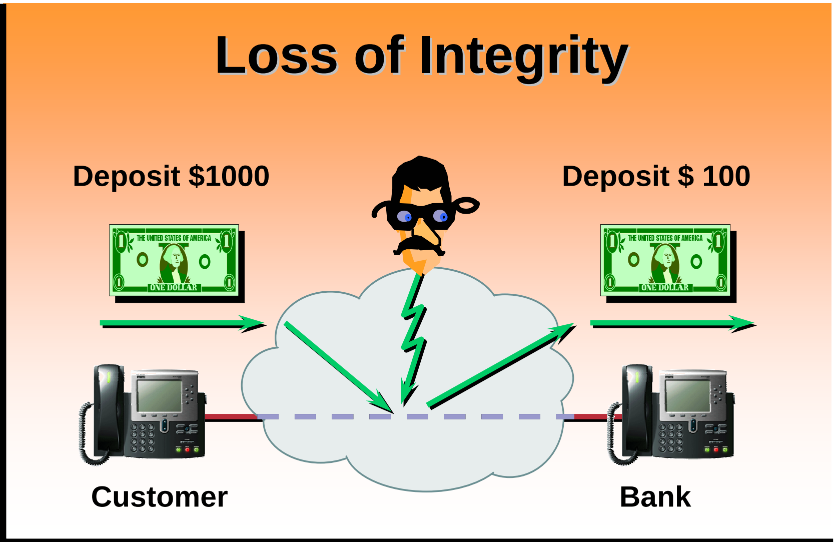
VoIP THREATS

Threats to IP Communications Consistent with IP Network Threats

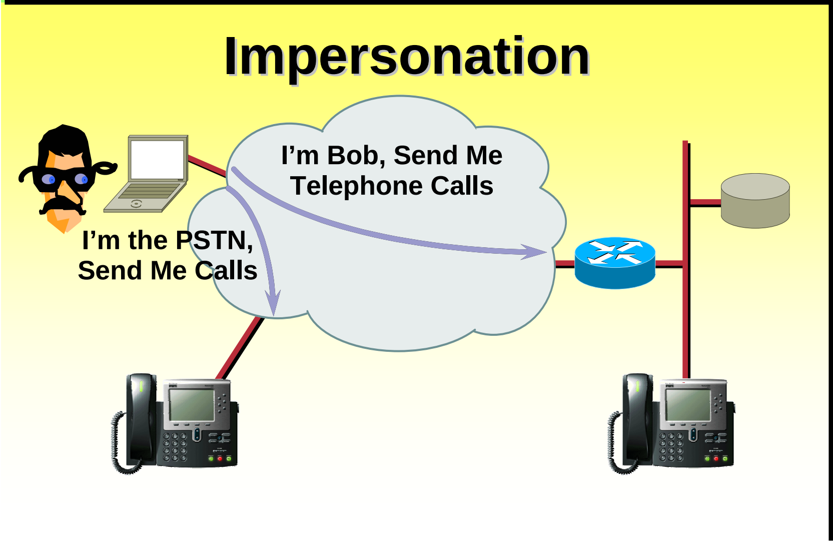
Loss of Privacy



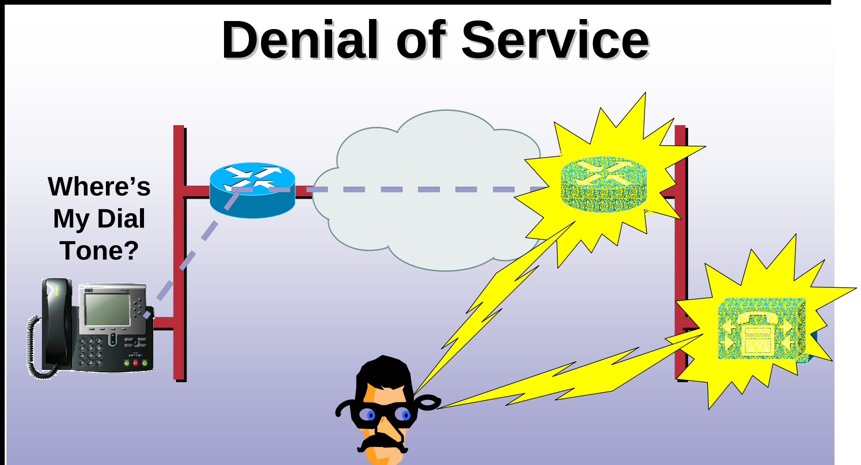
Loss of Integrity



Impersonation



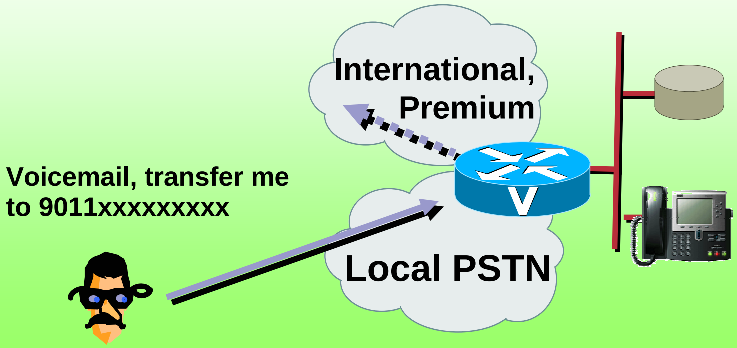
Denial of Service



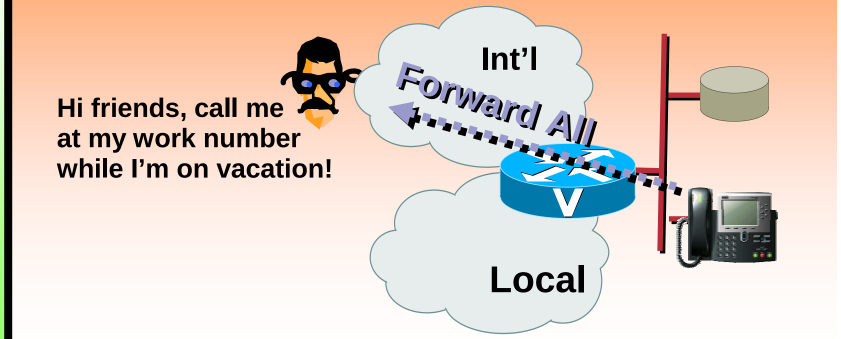
Voice Attack Points:
Servers, GWs, Delay, Jitter, Packet Loss, BW

Threats to IP Communications Also Consistent with *Some* PBX Threats

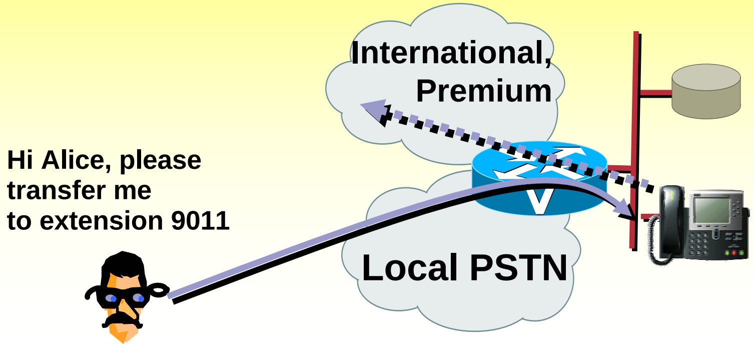
Toll Fraud 1: Transfer from Voicemail



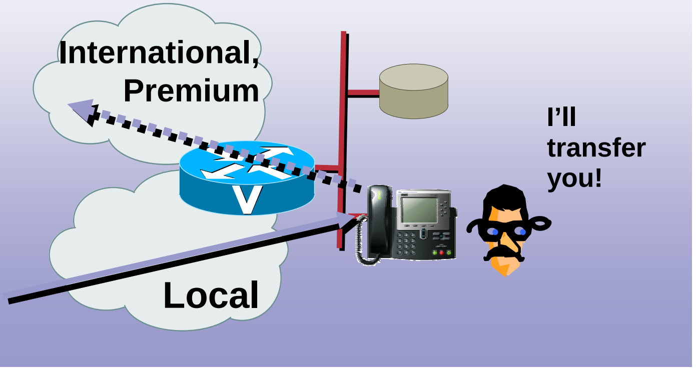
Toll Fraud 2: Call Forward All



Toll Fraud 3: Social Engineering



Toll Fraud 4: Inside Facilitators



Best Practices

- Separate voice and non-voice equipment (VLANs, IP address space)
- ACL signaling traffic
- RPF - Reverse Path Forwarding
- Rate Limit at network edges
- Endpoint security
  - Authenticate endpoints
  - Signed software loads on endpoints

IP Telephony Security: Build it in Layers

CallManager

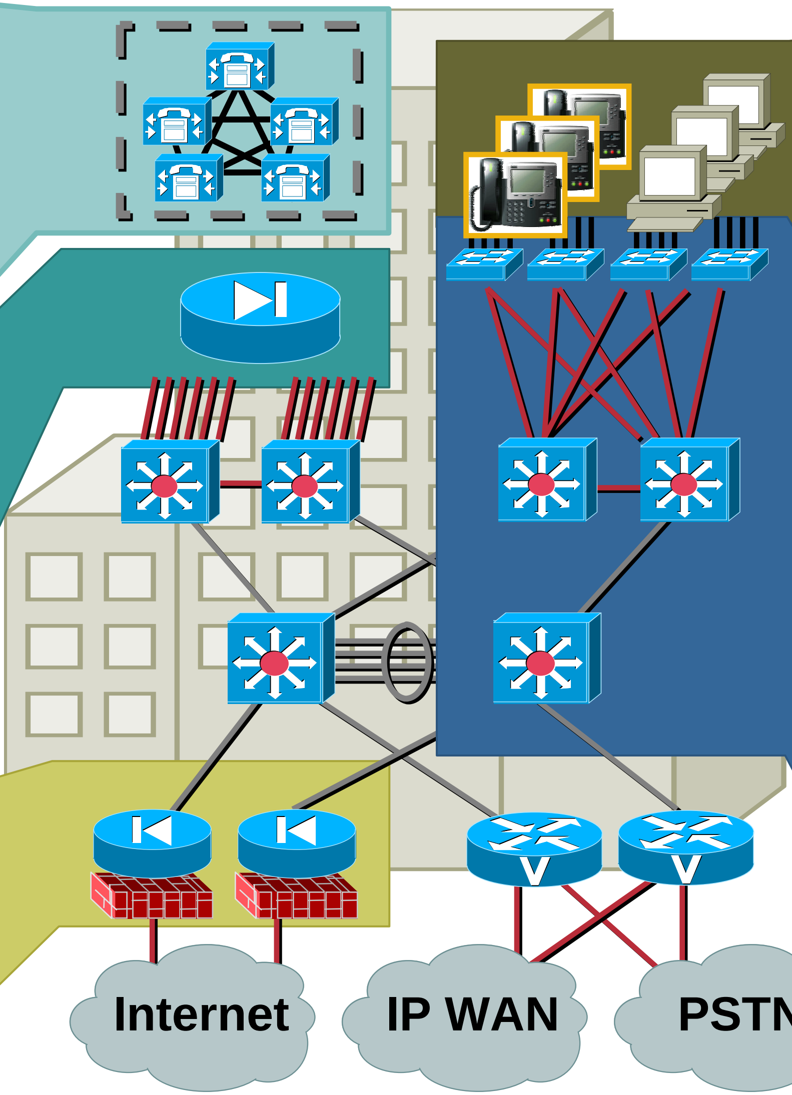
- Minimize Win2K services
- NTFS
- Secure IIS
- Lock down SQL
- IDS/virus

Firewall or ACLs

- Allow only call control, LDAP, management
- Control source addresses

Outside World

- Voice over I-Net using V3PN
- IOS DoS tools
- Network IDS



Endpoints

- Separate voice and data VLANS
- Disable GARP and voice VLAN on PC port

Campus Network

- High availability design
- Use VLANs
- Use IP filters between voice and data network
- Avoid NAT
- Secure access (TACACS+, SSH, Permit Lists)

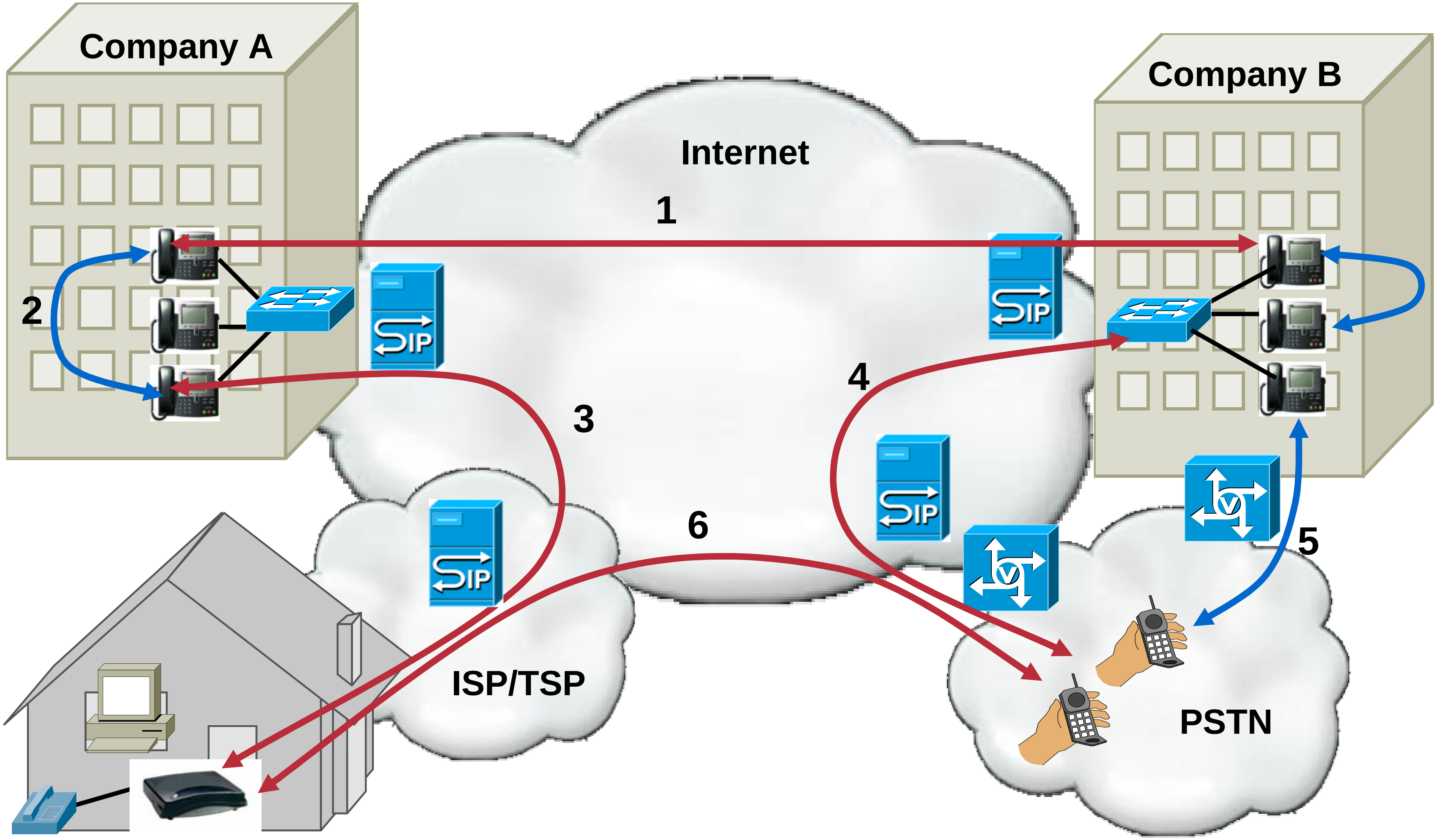
SIP SECURITY

SIP Introduction

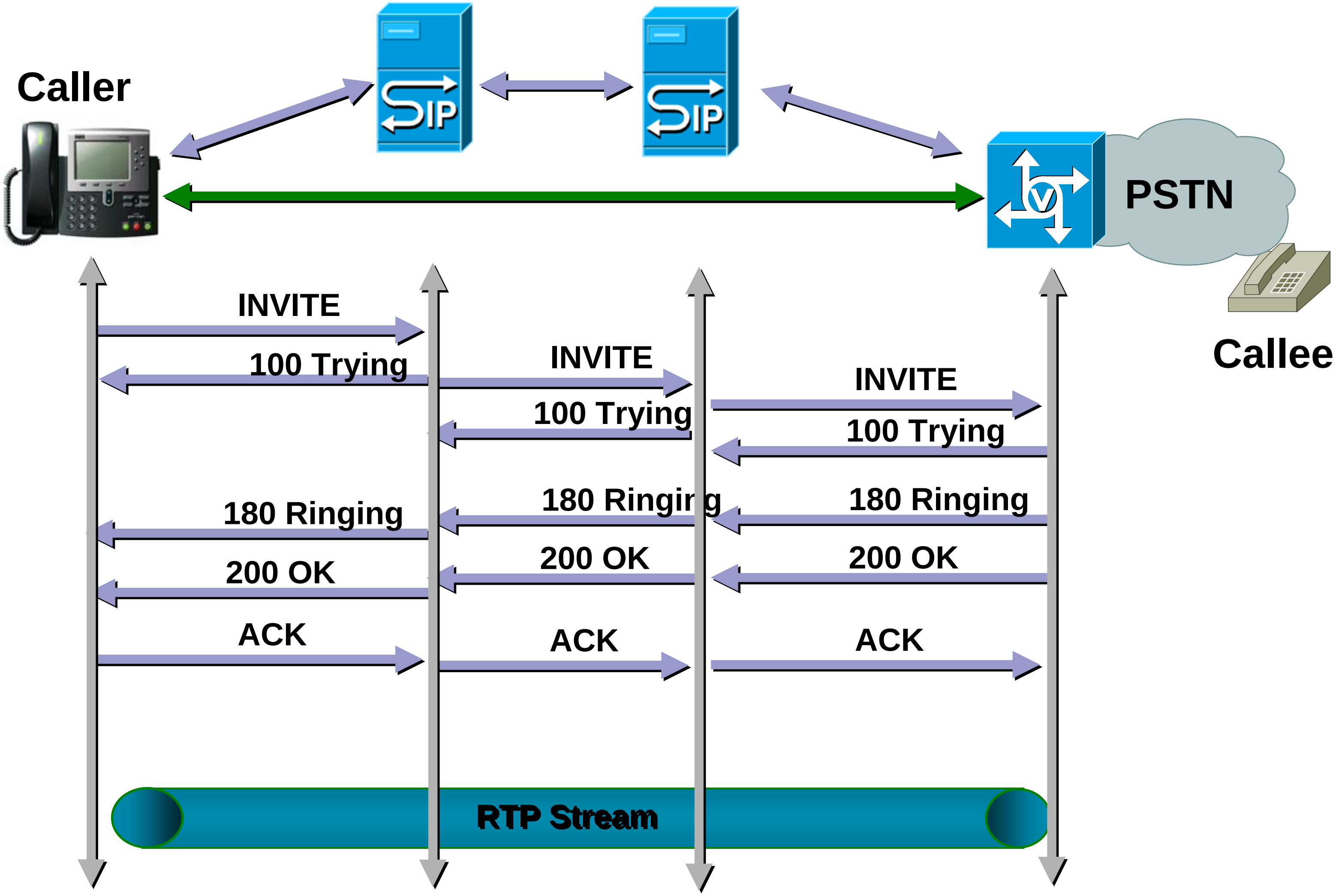
- Used for Voice and Video over IP
  - Toll Arbitrage
  - Residential / IP Centrex
  - Enterprise / IP PBX
- SIP/SIMPLE for Instant Messaging
- Used for Application, Whiteboard, and Web sharing

- How SIP works
  - Peer to Peer System
  - Rendezvous points to find others
  - Separation of media and signaling
  - Negotiation of rich media

SIP Architectures



Logical Architecture



Threats

- Toll fraud

  unauthorized or unbillable resource utilization

- Impersonating others
- Hijacking calls
- Learning private information

  (ex: voice, IM, caller ID, DTMF password/accounts, calling patterns)

- Eavesdropping
- Session Replay

- Fake identity
- Media tampering
- Denial of Service

  Hanging up other people's conversations

  Contributing to other DOS attacks

- SPAM (Both IM and Voice)

  more spam

    spam

      spam

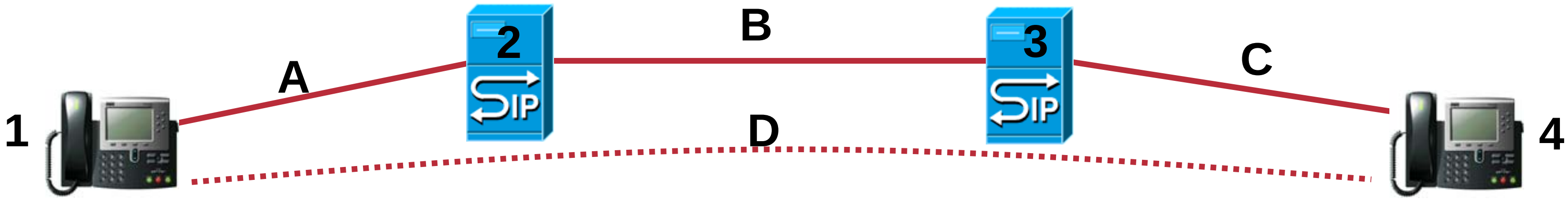
Why It’s Hard

- SIP is a rendezvous protocol, communicates with peers in any domain with no previous security relationship
- Deals with multiple intermediaries and endpoints with different trust for each (need both channel and object security)
- Multiple endpoints can be involved (ex: forwarding, forking, conferencing, transfer)
- Supports anonymity, call trace, legal intercept, and privacy (simultaneously)
- Complicated by: NATs, firewalls, high reliability, large scale, choice of transport protocol (ex: TCP, UDP, TLS, SCTP, DCCP)

Solutions to Threats

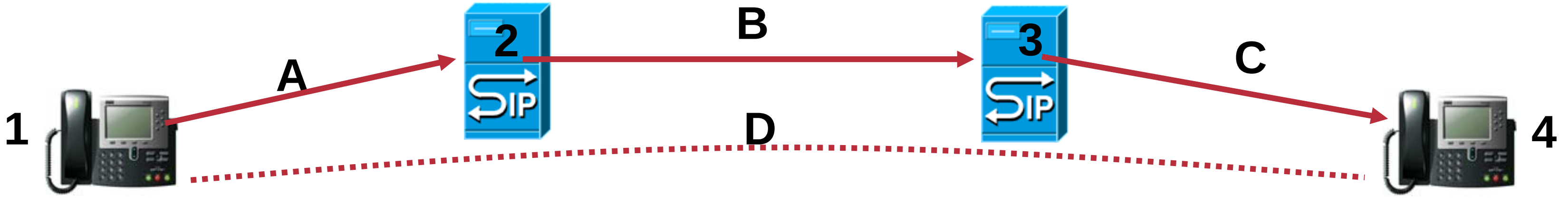
- Authentication/Authorization from:
  - client to server
  - server to server
  - server to client
- Privacy and integrity hop by hop (Channel Security)
- Privacy and integrity end to end (Object Security)
- Client and server assertion of identity (can be different)
- Server removal of identity for anonymous calls
- End to end assertion of identity
- Media integrity and privacy

Channel (Hop by Hop) Privacy & Integrity



- **Follows the HTTP web model and uses TLS on a Hop by Hop basis**
- **Can’t protect everything end to end because proxies need to change parts of the message (Request URIs, Via’s, ..)**
- **TLS creates an authenticated, encrypted, integrity-checked channel**
- **Crypto generally: RSA, 3DES or AES, SHA-1**

Channel (Hop by Hop) Authentication & Authorization



- **Authentication - Who sent me this?**

  over link A: Proxy checks the user (Digest or mutual TLS)

  over link B: Proxies check each other (mutual TLS)

  over link C: UA may verify request came from “its” proxy (TLS)

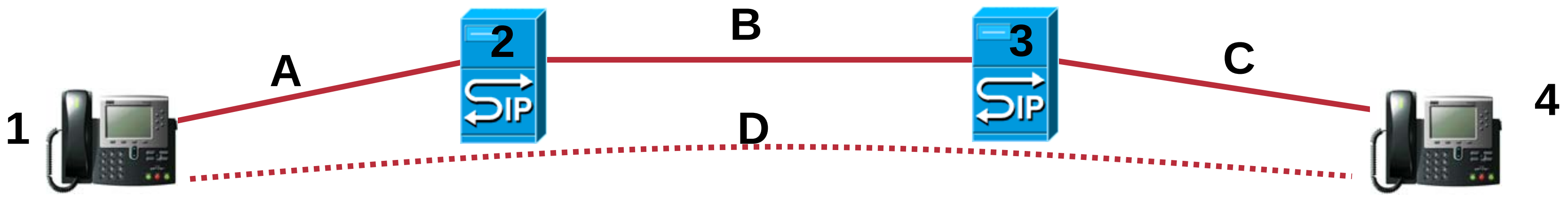
  end to end (D): UAS may verify UAC (SMIME)

- **Authorization is policy, can you: register, call a phone in this domain, use a resource like a conference system or gateway to PSTN**

- **Trust is not transitive: even if 1 trusts 2 and 2 trusts 3, it does not follow that 1 trusts 3**

  MCI might carry Vonage calls, Cullen has account with Vonage, but MCI does not have any trust relationship with Cullen

Object (End to End) Security



- Use S/MIME to sign and encrypt portions of the SIP message
- Protect private information from intermediaries
- Assertion of far end identity in a certificate

  Know who you end up communicating with

- Before saying S/MIME was a failure ….

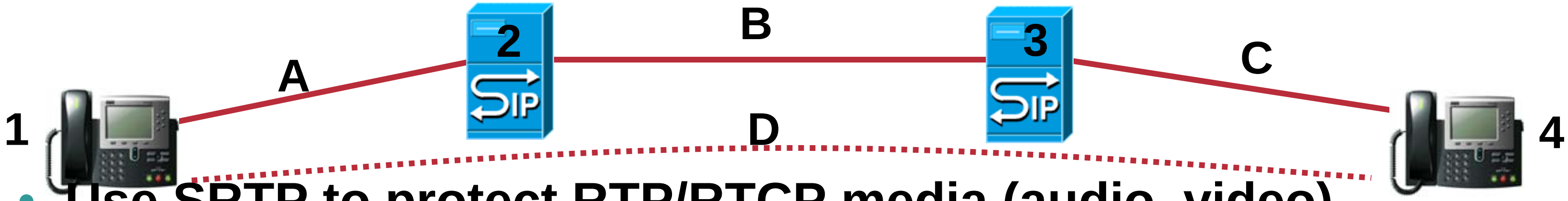
  It has been widely implemented, it works, security is good. Technically works well. Deployment is sparse but this relates to the difficulty and cost of an end user getting a certificate.

- Crypto generally: RSA, 3DES (want to move to AES), SHA-1

Identity Privacy

- Some folks want to make anonymous calls
  - Residents at women’s shelters
- Some organizations want calls to be traceable by trusted parties
  - Most countries on the public phone system
  - Financial companies may have certain regulatory obligations
- SIP has a “User Asserted Identity” (From) and a “Network Asserted Identity”
  - The AI is only valid in a particular Trust Domain and is removed as the signaling leaves that Trust Domain
- Things to anonymize
  - SIP URIs, Vias, contacts, IP addresses in session descriptions

Media Encryption



- Use SRTP to protect RTP/RTCP media (audio, video)
  - Keying material is passed in SIP signaling
  - AES Counter Mode
    - counter derived from 16 bit RTP sequence number
    - 32 bit roll over counter provided in RTCP
  - Crypto generally: AES-CM, SHA1
- Protect Instant Messaging with S/MIME
  - Crypto generally: RSA, AES, SHA1

VoIP Security Check List

- How does the system authenticate users?

  Digest and Mutual TLS are good answers

- How does the system protect privacy of signaling?

  TLS is a good answer

- How does the system do media privacy?

  SRTP and S/MIME are good answers

- Can devices be enrolled easily?

Cisco Systems®