EXHIBIT E


dynamicsoft®

SIP Proxies

Jonathan Rosenberg

Chief Scientist

Presentation Agenda

- **SIP Overview**
- **Definition of Proxy Roles**
- **Features for each role**
- **Generally useful capabilities**

Session Initiation Protocol (SIP)

- **Developed in mmusic Group in IETF**
  - Proposed standard RFC2543, February 1999
  - Work began 1995
  - Part of *Internet Multimedia Conferencing Suite*
- **Main Functions**
  - Invite users to sessions
    - Find the user's current location, match with their capabilities and preferences in order to deliver invitation
    - Carry opaque session descriptions
  - Modification of sessions
  - Termination of sessions

Session Initiation Protocol (SIP) cont.

- **Main Features**
  - Personal mobility services
  - Wide area operation
  - Session flexibility
    - Voice; video; games; chat; virtual reality; etc.
  - Leverages other Internet protocols

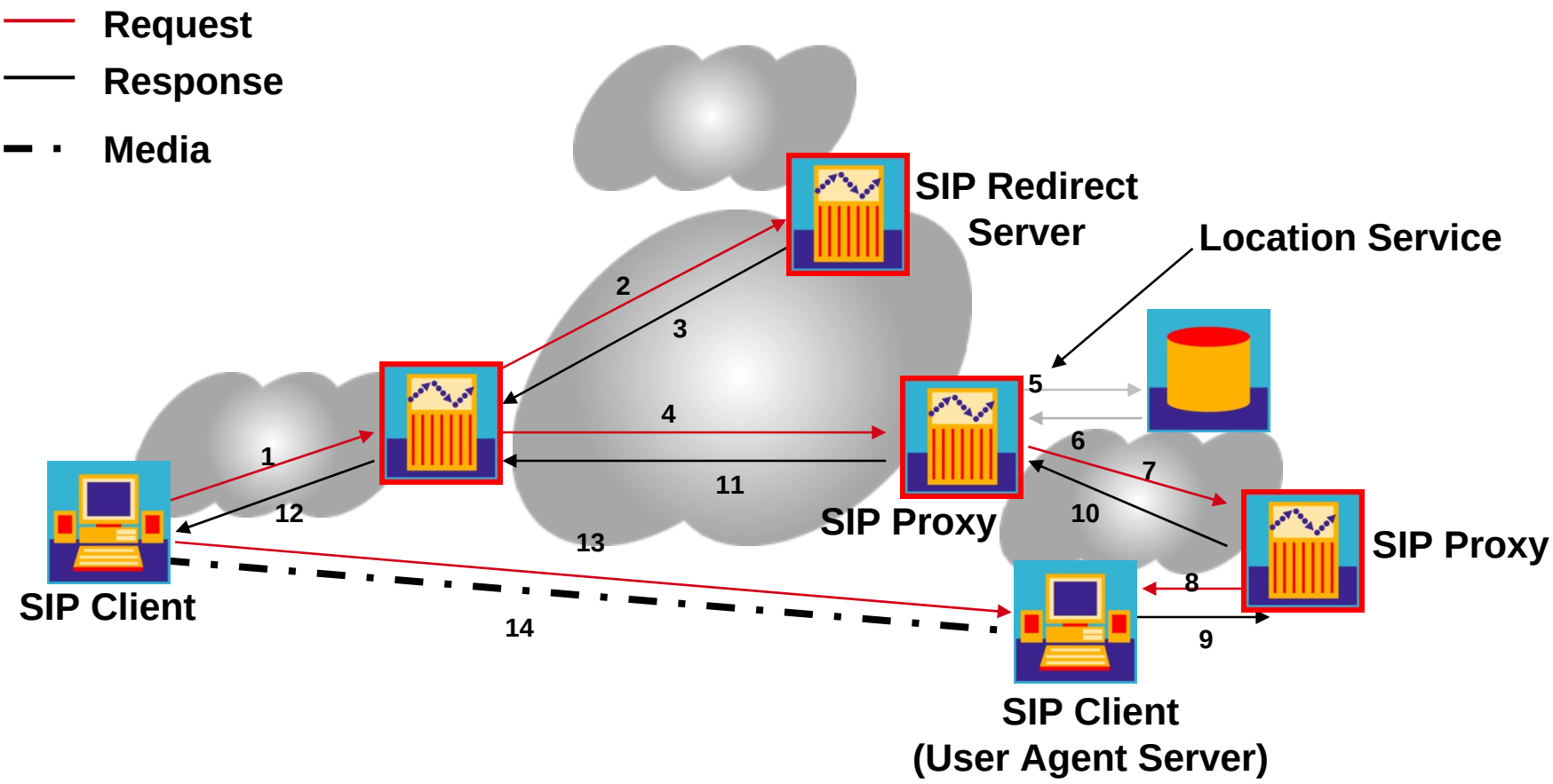
Protocol Components

- **User Agent Client (UAC)**
  - End systems
  - Send SIP requests
- **User Agent Server (UAS)**
  - Listens for call requests
  - Prompts user or executes program to determine response
- **User Agent**
  - UAC plus UAS

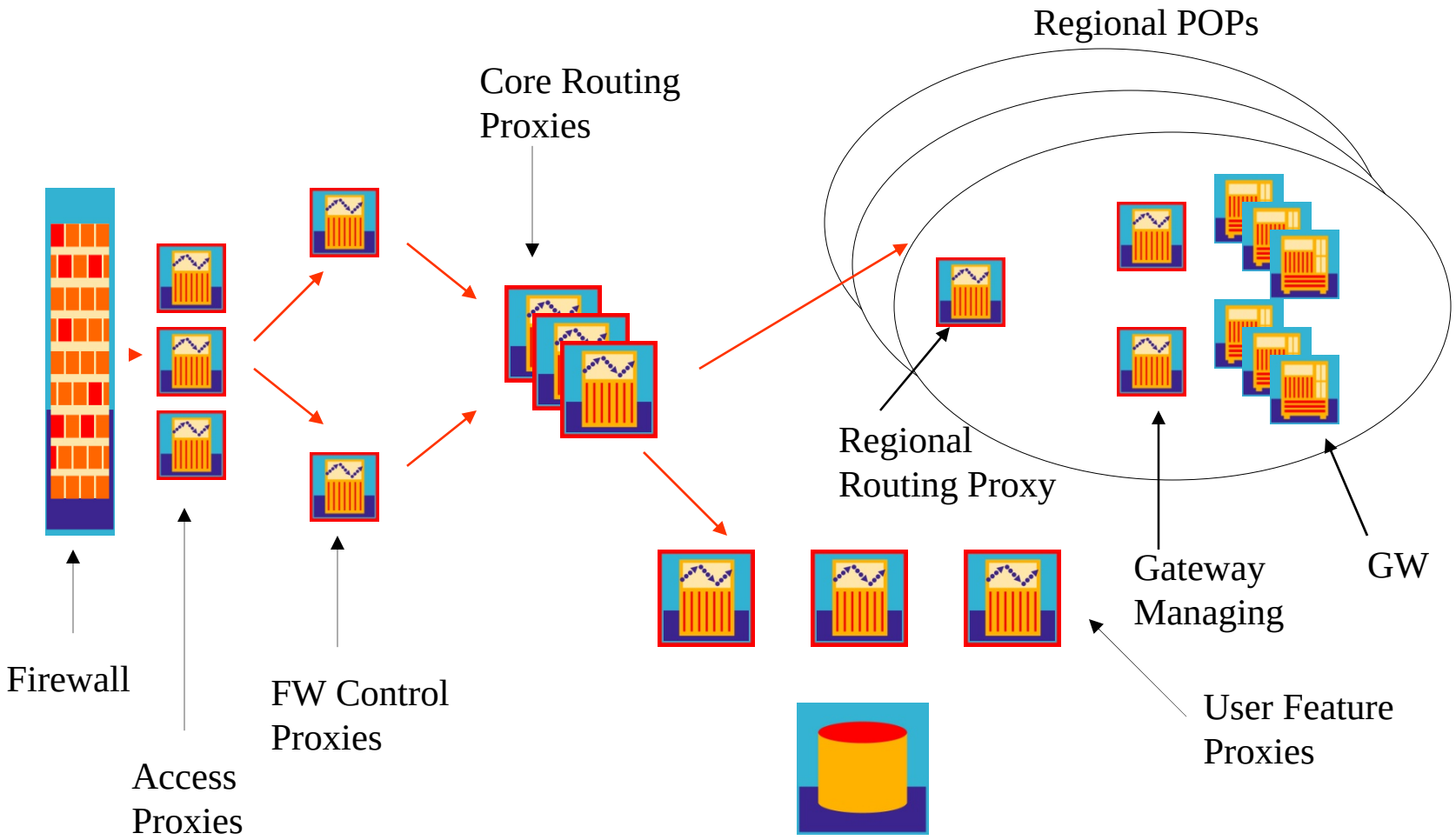
Protocol Components cont.

- **Redirect Server**
  - Network server - redirects users to try other server
- **Proxy Server**
  - Network server - a proxy request to another server can “fork” request to multiple servers, creating a search tree
- **Registrar**
  - Receives registrations regarding current user locations

SIP Architecture



A Real ITSP Network



Proxy Servers have Roles

- **Proxy is just a SIP defined logical function**
  - Not useful in and of itself
  - Critical piece is value add features built on top of SIP proxy function
  - Which features you need depends on roles
- **Real VoIP networks have multiple signaling points, each with specific roles and functions**
  - Access Proxies
  - Firewall Control Proxies
  - Core Routing Proxies
  - Regional Routing Proxies
  - Gateway Managing Proxies
  - User Feature Proxies

Access Proxies

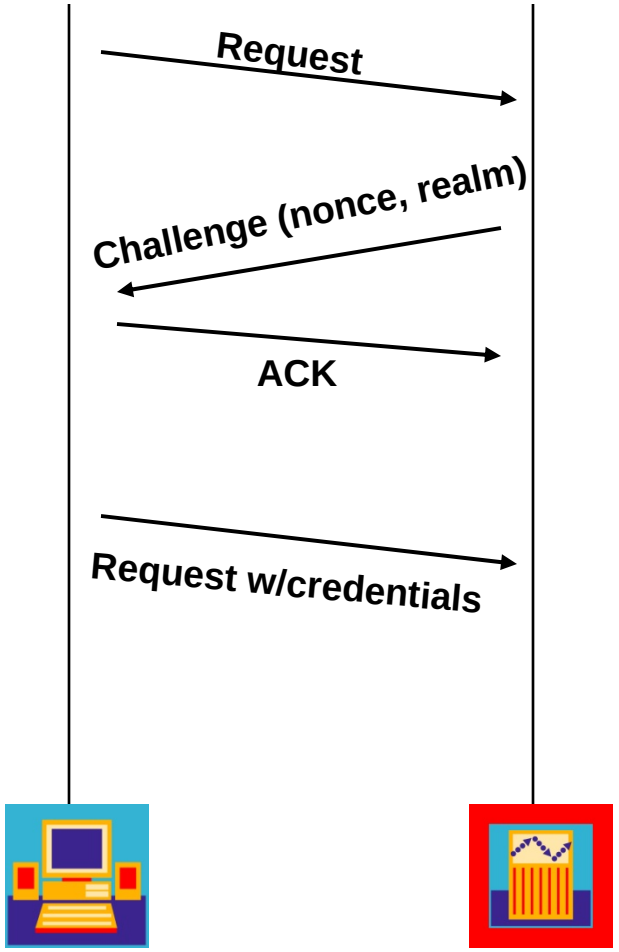
- **Serve as access point into network**
- **What needs to be done at access point?**
  - Authentication
  - Accounting
  - DoS Attack Prevention
- **Authentication only need be done once at ingress point**
  - From there, secure TLS based connections between elements
  - Critical for DOS prevention
- **How is authentication done?**
  - Wholesale, bulk traffic – TLS
  - Individual consumers – SIP proxy authentication mechanisms
- **Why is accounting needed here?**
  - For wholesale customers
    - Only place in network where all traffic from/to customer arrives
    - Ideal point for troubleshooting customer interface
    - Customer traffic profiling and usage metrics
    - Customer care
  - Intrusion detection
  - DoS attack detection
- **Useful to dedicate proxies to specific customers**
  - No resource contention
  - High availability
  - Common model in web server market as well

TLS Authentication

- **Transport Layer Security (TLS) is newer version of Secure Sockets Layer (SSL)**
- **TLS/SSL is basis for web security**
- **HTTPS = HTTP over TLS/SSL**
- **Functions**
  - Server to client and optionally client to server authentication using public keys
  - Negotiation of shared private session key
  - Encryption of all messages once connection established
- **Applications to SIP**
  - Functions as a “Secure VoIP Trunk”
  - All signaling traffic between pair of providers can run over TLS
- **Benefits to provider**
  - Prove that all traffic is from actual customer
  - Very efficient – public key operations only at beginning of connection

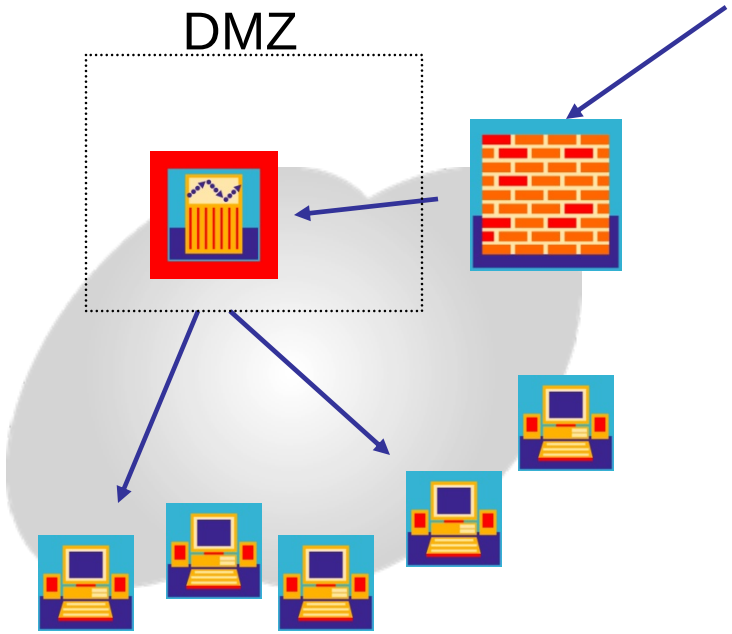
SIP Authentication

- **Authentication Mechanisms**
  - Basic
  - Digest
  - PGP (to be deprecated – S/MIME and PGP/MIME to replace)
- **Basic and Digest Are Shared Secret - Assume Trust Relationship Between UA and Proxy**
  - Only for outgoing requests
- **SIP Can Also Authenticate Responses**
  - Not used – will be deprecated



DoS Attack Protection

- **DoS Attacks**
  - Flooding of packets
  - Malicious content
- **Access Proxy Acts as DMZ Machine**
  - Sole point of entry for calls to network
- **Filtering Functions**
  - Absorbs bursts
  - Blocks large messages
  - Removes content with viruses
  - String parsing checks and validations



Firewall Control Proxies

- **Responsible for allowing SIP and media traffic to traverse firewalls and NATs at periphery of network**
- **Ideally isolated from access proxies**
  - Security risk in directly making these accessible
  - Scalability
  - Authenticate and authorize at periphery, freeing internal boxes from performing the function again
- **Logging to record firewall usage**
- **How do they allow SIP and media to traverse firewalls?**

Getting SIP Through Firewalls

- **Firewalls Typically Statically Configured to Let Traffic in/out of Specific Ports/Addresses**
- **SIP Itself Can Easily Be Let in/out**
  - Static port 5060 opened
- **But SIP Signals Media Sessions, Usually RTP**
- **RTP Difficult to Isolate**
  - Uses dynamic UDP ports
  - Not its own protocol
  - No way to statelessly identify
- **Therefore, Media Sessions Will Not Flow Through Firewall**

Getting SIP Through NATs

- **Network Address Translation (NAT)**
- **Modifies IP Addresses/Ports in Packets**
- **Benefits**
  - Avoids network renumbering on change of provider
  - Allows multiplexing of multiple private addresses into a single public address ($$ savings)
  - Maintains privacy of internal addresses

Getting SIP Through NATs cont.

- **Issues**
  - If a host includes its IP address inside of an application packet, it is wrong to the outside
  - SIP fundamentally does this
  - Addresses inside of SIP must be rewritten

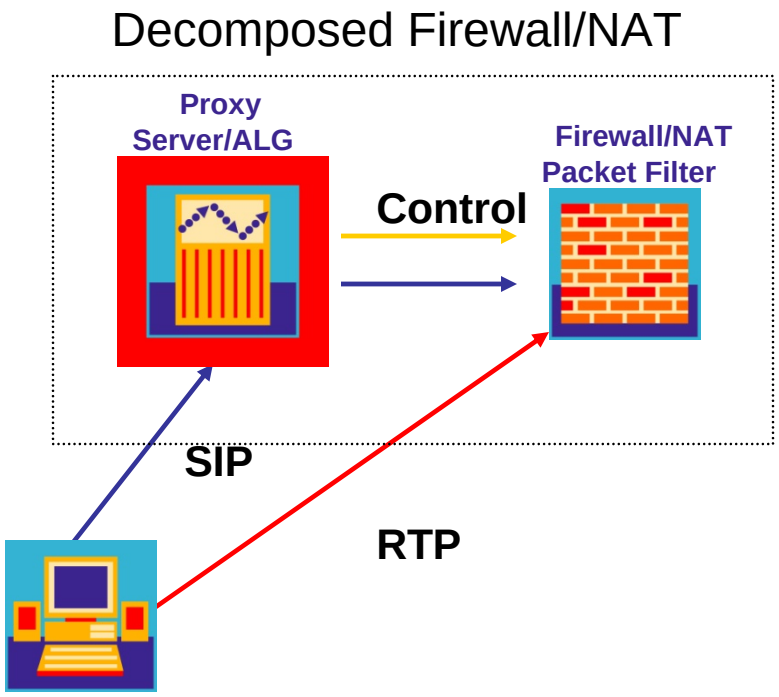
- **Where Can IP Addresses Be?**
  - SDP
  - From field
  - To field
  - Contact
  - Record-route
  - Via

Continuing Challenges

- **Other Application Protocols Have Trouble With Firewalls and NAT**
  - ftp
  - H.323
- **Solution is to Embed Application Layer Gateway (ALG) into Firewall/NAT**
  - Actually goes into packet and modifies addresses
  - Requires understanding of protocol
- **Embedding ALG in NAT is Not Ideal Solution**
  - Scaling
  - Separation of function
  - Expertise issue

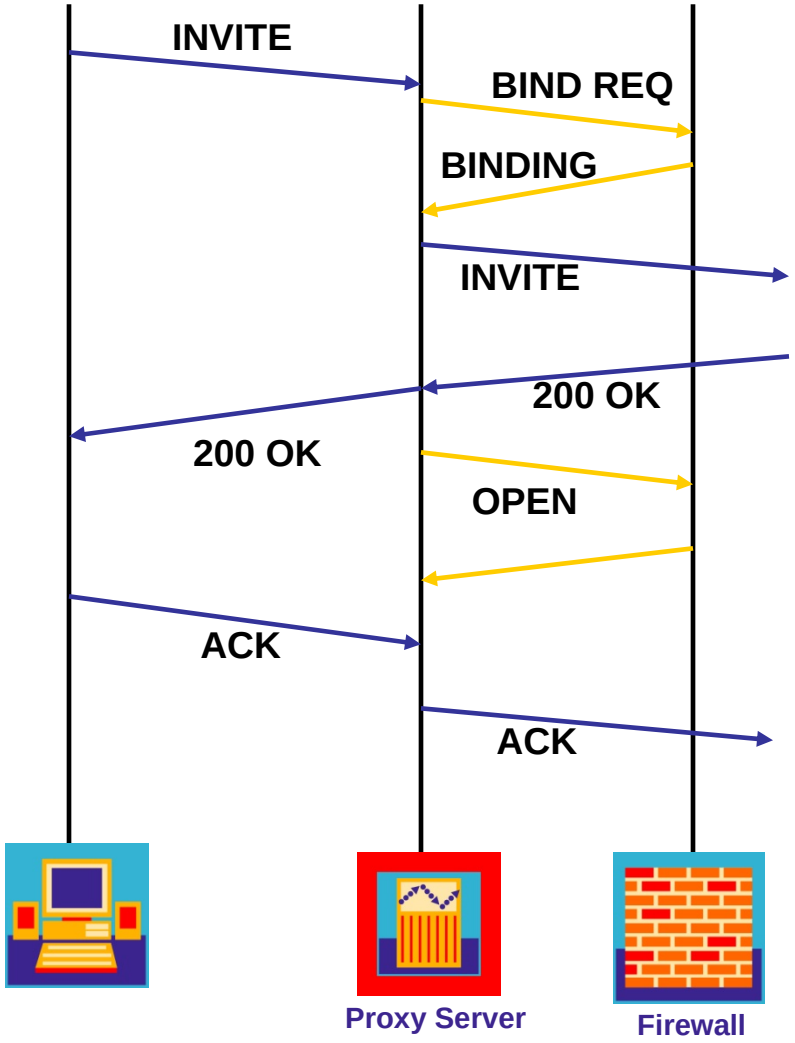
Proposed Solution

- **Separate Application Layer NAT/Firewall from IP Layer NAT/Firewall**
  - Similar to megaco decomposition
  - MG analagous to packet filter
  - MGC analagous to ALG (proxy)
  - Same benefits
    - Better scaling
    - Faster
    - Lower Cost
    - Expertise problem solved
    - Deployment paths for new apps
    - Load balancing



The Missing Piece

- **Control Protocol Between SIP ALG and IP NAT/Firewall**
- **Main Requirements**
  - Binding request: give a private address, obtain a public address
  - Binding release
  - Open hole (firewall)
  - Close hole (firewall)
  - Group bindings



IETF Efforts on Firewall Traversal

- **SIP Working Group**
  - Informational RFC will be developed
    - Summarizes SIP operations needed in firewall controlling proxy
    - Defines SIP ALG function for NAT
- **MIDCOM Working Group**
  - Recently approved
  - Will develop framework and requirements
  - Initial draft:
    - J. Kuthan, J. Rosenberg, “Firewall Control Protocol Framework and Requirements”, draft-kuthan-fcp-01.txt

Routing

- **Routing is one of the primary functions of a proxy**
- **Routing is one of the core services of a service provider**
- **Most general definition:**
  - Connecting users to the network services required for the session by selecting a next hop server to process the request
  - Network Services
    - Gateways
    - POPs
    - Application Platforms
    - Media Servers
- **Routing is best performed in a hierarchical fashion**
  - Scalability
  - Ease of management
    - Delegation
    - Upgradability
    - Isolation
- **Many inputs to routing process**
  - Registration database
  - Telephone routing prefixes
  - TRIP and TRIP-GW
  - Caller preferences
  - External databases

Core Routing Proxy

- **How does a proxy route? Depends on roles.**
- **Core Routing Proxy**
  - Job is to take calls from all access points and figure out high level next hop service to handle call
  - Can recreate Class 4 Features
  - Next hop service is typically
    - Regional POP for PSTN termination
    - User Feature Proxies for local subscribers
    - FCP for calls out to peer networks
  - Routing generally based
    - Telephone prefixes
    - TRIP
    - Databases for domain lookups
  - Why use a core?
    - Avoids need for each service to know about each other
    - Example: CPL in user feature proxy forwards call to PSTN termination

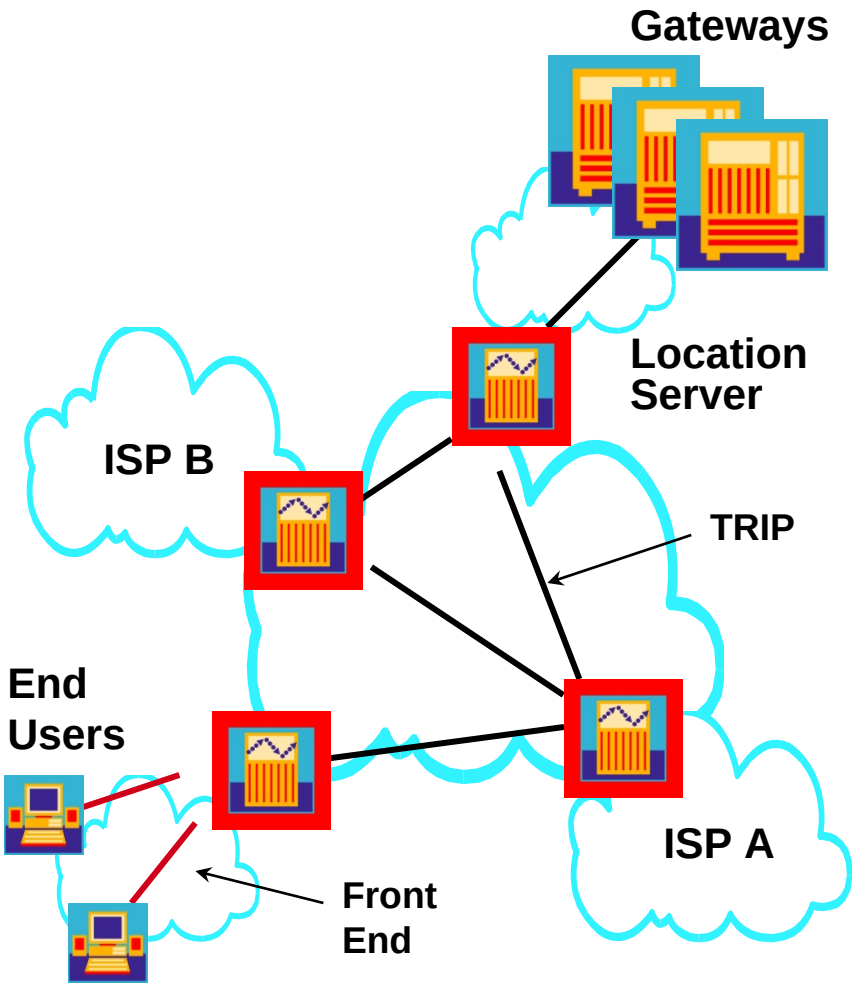
Telephone Routing Prefixes

- **SIP INVITE Can Contain Phone Numbers**
  - sip:17325551212@domain.com
  - tel:17325551212
- **Do Not Correspond to Users on IP Network, but PSTN Terminals**
- **Call Must Be Routed to Gateway**
- **Gateways Often Arranged Through Peering**
- **Which One to Use Based on Prefixes (Domestic = gw1, Europe = gw2)**
- **Route Table is Mapping From Prefixes to Next Hop IP address/port/transport Plus URL Rewrite Rules**

1-732	regional.com
1	longdistance.com
	international.com

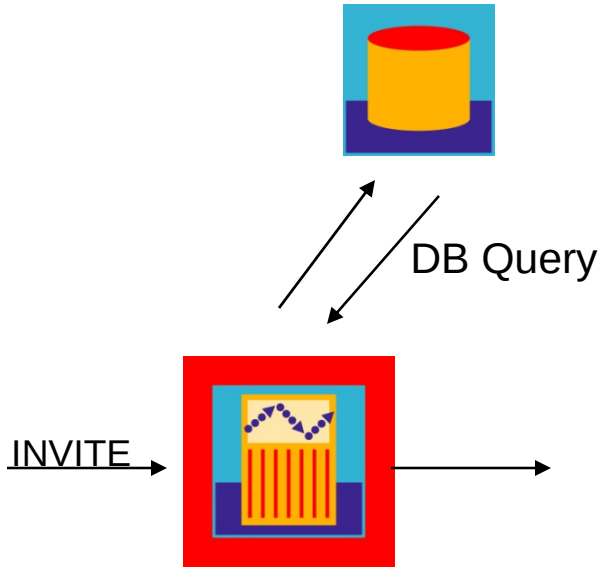
Telephony Routing Over IP (TRIP)

- **Inter-domain Protocol for Gateway Route Exchange**
  - Currently in working group last call in IETF
- **TRIP Supports Various Models**
  - Bilateral agreements
  - Centralized settlements provider
  - Wholesaler service
- **TRIP Based on Scalable IP Routing Technology**
  - Uses BGP4 as a basis
  - Supports aggregation
  - Uses proven algorithms
- **Proxy = TRIP LS**
  - Allows proxy to build routing table dynamically
- **Core Proxy would use TRIP to determine whether to route call to a peer provider**



External Databases

- **Routing Information Can Also Be Located in External Databases**
  - LDAP
  - SQL
  - whois++
- **Static or Dynamic**
- **Several Standards**

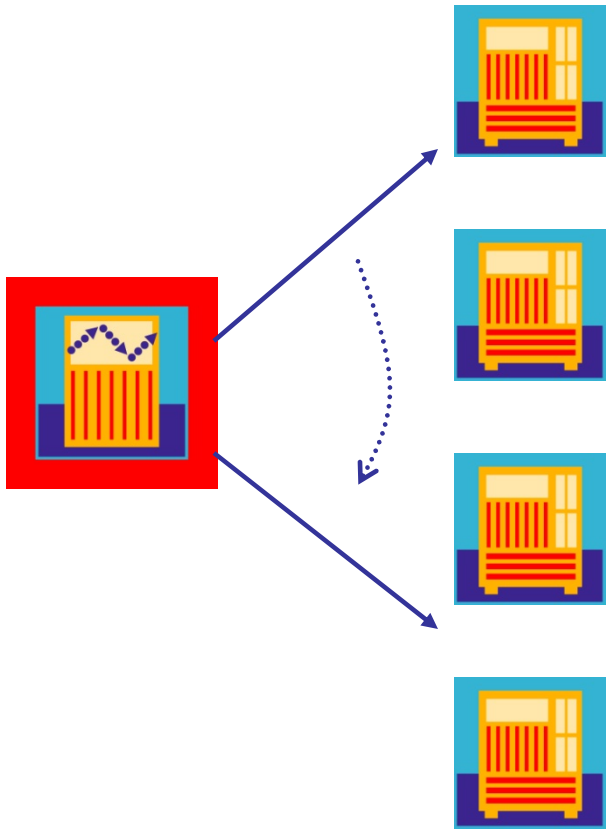


Regional Proxy

- **Manages all gateways in a geographical region**
  - Country, state, province
  - Depends on size
- **Why separate from Core proxy?**
  - Separate administrators for POPs
  - Information on optimal routing not known globally
- **May be additional sub-regions depending on size**
- **Generally you want regional proxy when there are more than one heterogeneous gateways in a POP**

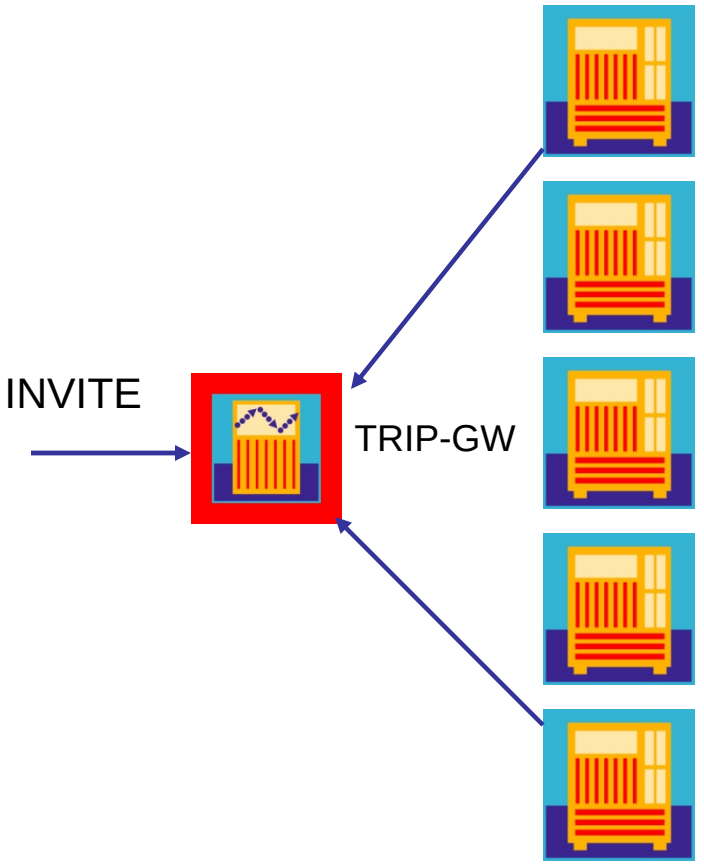
Gateway Managing Proxies

- **Responsible for managing routing of calls to sets of gateways**
- **Routing decisions based on**
  - Gateway availability (up/down)
  - Available gateway capacity
  - Codecs and other features
  - Possibly cost
- **May want to handle temporary overload cases**
  - Gateway responds with 503; should try another one
- **Generation of CDRs for calls**
- **Ideally should utilize full capacity of gateways**
- **Question: how does proxy know available capacity of gateways?**



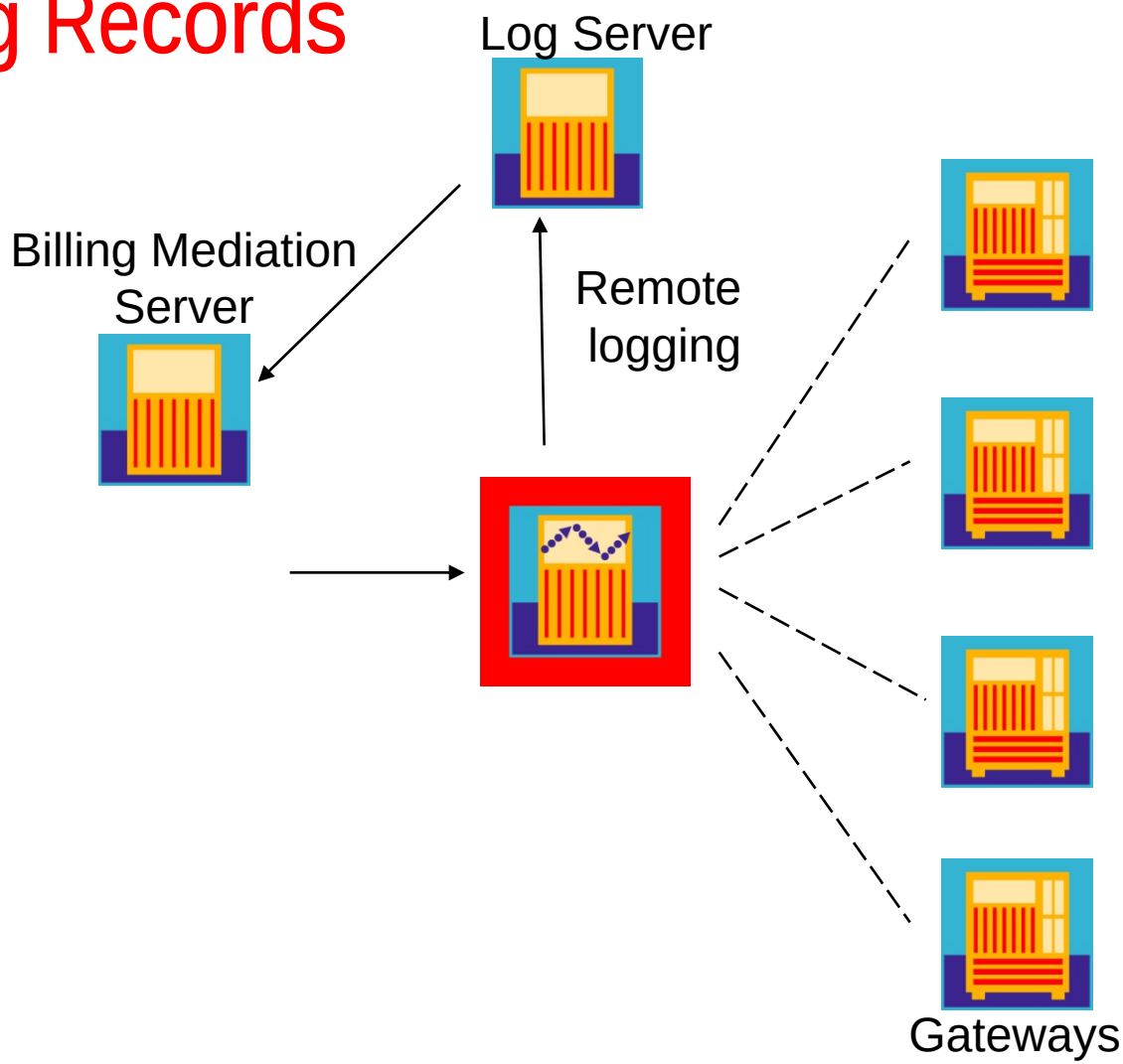
TRIP and Gateways

- **Normal TRIP Runs Interdomain**
- **TRIP-GW: Lightweight Version That Runs Between LS and Local Gateways**
- **Provides Gateway Information Exported to Other Domains Via TRIP**
- **Provides Gateway Management Capabilities**
  - Load balancing based on available ports/codecs
  - Liveness detection
  - Failover



Generating Billing Records

- **Billing Issues**
  - Must bill for a real service
    - Gateways
    - MCUs
  - Proxy “fronts” gateway
  - Need secure association to gateway
  - Session timer
- **Logging to Remote Logging Server is Key Benefit**
- **Real time not needed**

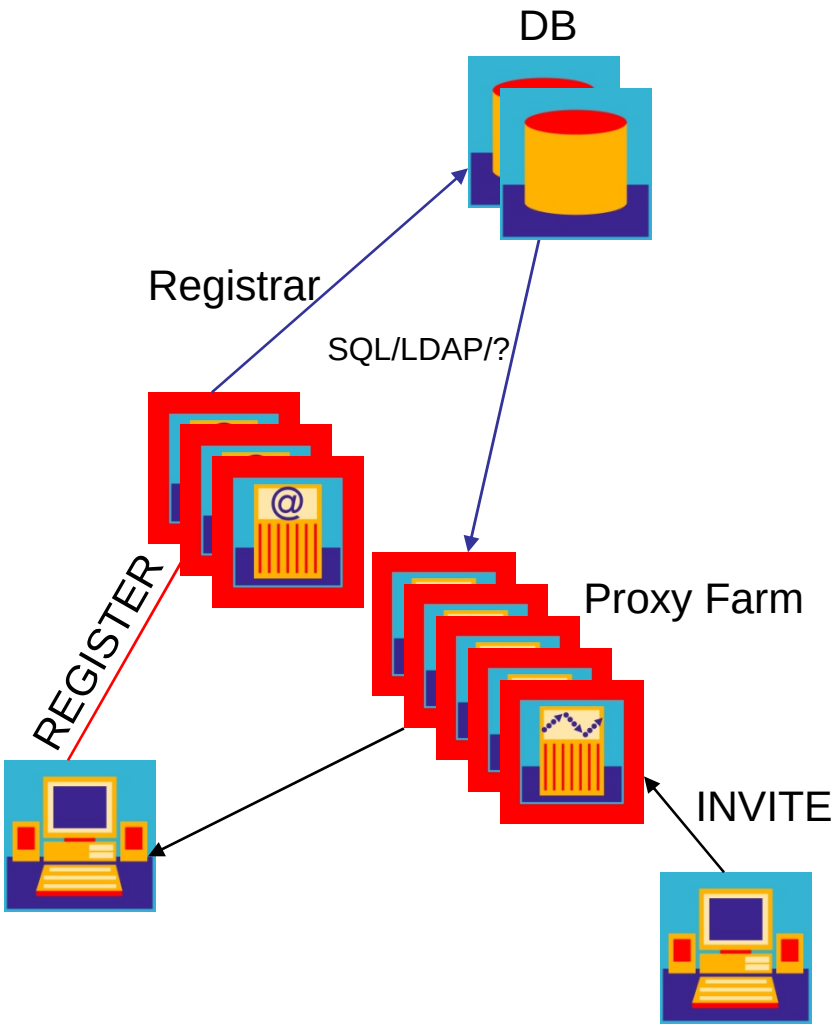


User Feature Proxies

- **Proxies “closest” to users**
- **Responsible for routing calls based on**
  - User Location
  - User preferences
- **Execution of user services**
- **Accounting for billing of user services**
- **Authentication and Authorization of end users**
- **Back end DB for location and feature data**
- **Can recreate Class 5 Features**

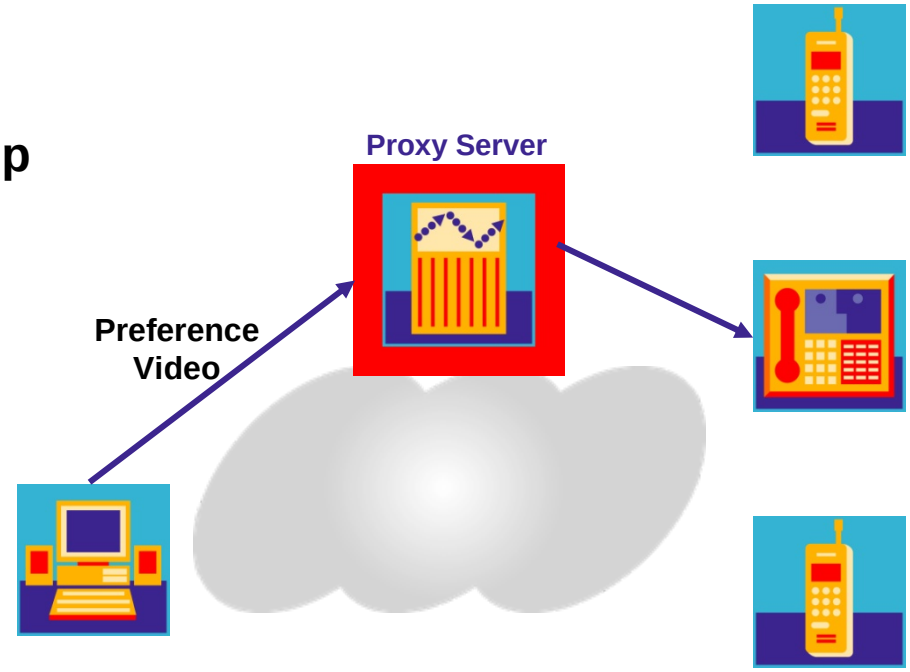
Registration Database

- **On Startup, SIP UA Sends REGISTER to Registrar**
- **Registration Data Provides Addresses to Reach User**
- **Registration Database Forms a Dynamic Routing Database of Users**
- **Centralized Store is Desired for Scalability**



SIP Caller Preferences

- **SIP Extensions for Specifying Caller Preferences and Callee State**
  - Presence
- **Preferences Carried in INVITE Setup Message**
- **Preferences for**
  - Reaching callee at home or work
  - Fax, video, audio call
  - Mobile or landline
  - Secretary or voicemail
  - Priority locations
- **Caller Can Specify Proxy Routing**



Checklist of Other Desired Features

- **Configuration and Management**
  - Command line interface
  - web
  - SNMP
- **Fault tolerance**
  - No single point of failure
    - Its not for free with SIP
  - Alarms to report device failures
  - Many approaches to handle backups
- **Scale**
  - $$/Call or $$/Transaction is the key
  - Linear scalability in performance is ideal

Checklist of Other Desired Features cont.

- **Subscriber Management**
  - Add users to system
  - Define services and capabilities
    - CPL or not?
  - Authorize services against subscriber lists
- **Dynamic Reconfiguration**
  - Change parameters/routing table entries on the fly
- **Customized Logging Outputs**
  - XML, apache, etc.

Information Resource

- **Jonathan Rosenberg**
  - jdrosen@dynamicsoft.com
  - +1 973.952.5000