

APPLICATION NOTE

Don't Drown in the Registration Flood

*The transient nature of VoIP means that the VoIP device must identify itself on the network and the network must in turn grant access to the device - a process known as **Registration**.*

IMS networks build on basic SIP registration mechanisms, adding several additional layers of complexity.



Registration traffic was once an afterthought in designing VoIP networks. But today's network registration messages generate an overwhelming amount of network traffic. As a result, poorly designed and tested networks can succumb to outages caused by the dreaded Registration Flood.

This application note reviews registration in SIP and IMS networks, describes what occurs during a registration flood, and introduces testing and monitoring strategies for preventing these outages.

Registration Background

Unlike traditional wireline networks, today's VoIP devices are not permanently connected to the network. With many VoIP services, a user can take an IP phone with a unique number and plug it in anywhere on the IP network, or even anywhere on the internet. The transient nature of VoIP means that the VoIP device must identify itself on the network and the network must in turn grant access to the device—a process known as *Registration*.

The SIP protocol enables this process by sending several messages that contain basic information such as "From," "To," and authentication codes. Registration messages are also used as a "keep-alive" mechanism, helping the network react if the device status changes—i.e. "do-not-call" or the device is turned off. The timing between these keep-alive registrations can vary greatly. For example, the network may require re-registration once every hour, but NAT devices may need to see a registration attempt every 30 seconds or less to keep firewall pinholes open.

IMS networks build on basic SIP registration mechanisms, adding several additional layers of complexity. For example, in an IMS network, registration messages must pass between a minimum of five to six network entities as opposed to a minimum of two to three for a basic SIP network. IMS messages also contain more information fields than standard SIP networks. In addition, IMS networks typically require authentication for additional security.

This process requires a second registration message to be propagated through the network, doubling traffic (see Figure 1 and Figure 2). As a result, IMS registration consumes more network bandwidth and computing time — often by a factor of ten or more.

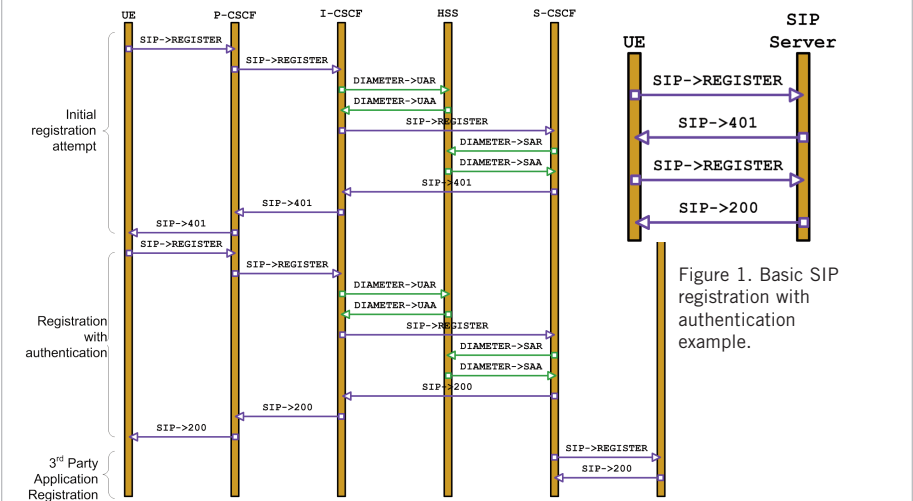


Figure 2. Registration of a single endpoint in an IMS network, including authentication and third party application registration.

The Registration Flood

A registration flood occurs when many VoIP devices try to register simultaneously. Registration servers have finite processing power and can therefore handle a limited amount of traffic. If the volume of registration messages exceeds the device's capacity some messages will be lost, meaning some users will not be able to make or receive calls. These devices may then attempt the registration again, adding more congestion. Depending on the design of the network, the performance of network devices, and severity of the registration flood users may be unable to access the network for several minutes to several hours.

One million subscribers re-registering every hour is equivalent to the signaling for about 159 calls per second (CPS), assuming a seven-message call. The same population re-registering every half minute, which is common for NAT traversal, is equivalent to the signaling for 19,000 CPS. At these rates, it is easy to imagine how a burst of 10,000 subscribers coming online within a small window of time can overwhelm a system.

Calculating Registration Traffic												
messages / subscriber	÷	expiration (seconds)	=	messages / second / subscriber	x	subscribers	=	messages / second	÷	average messages / call	=	equivalent calls / second
4	÷	3600	=	0.0011	x	1,000,000	=	1111	÷	7	=	159

Figure 3. Calculations showing the number of SIP registrations for a million subscribers and the equivalent number of calls per second.

Common causes of a registration flood include:

- **Power outages** — when an electric company returns power to a region all at once, the IP phones all turn-on and attempt to register.
- **Downed infrastructure** —if a proxy or edge device goes down, it may cause many users to retransmit their registration, increasing the message rate.
- **Malfunctioning software and devices** — software bugs or mis-configured devices can cause end-user devices or network devices to send too many registration attempts.
- **Network attacks** — hackers attempting to down a network may intentionally flood a network.

Session Border Controllers (SBC) are typically used to protect the core network (including registration processing servers) from these floods. However, configuring these devices can be a complex undertaking, particularly in large-scale networks with numerous NAT points. Mis-configured SBCs can prevent users from registering altogether, leave security holes open, allow a registration flood to occur, or even cause a registration flood.

Avoid Registration Floods by Testing and Monitoring Your Network

Early VoIP networks had relatively simple call flows and low numbers of subscribers, so registration-related traffic was relatively insignificant. Today's VoIP networks have hundreds of thousands or even millions of subscribers. These networks are also more complex, with messages traversing numerous network domains, proxies, and NAT devices across numerous peering-configurations. Future IMS networks will be even more complex, adding more registration steps, network infrastructure devices and security mechanisms.

The only way to ensure your network will properly deal with registration flood attempts is to conduct specific tests using a variety of scenarios. These tests help to characterize the network, including optimum configurations for changing traffic mixes.

Test equipment should be able to provide the speeds required to adequately stress the network. The traffic mix should include several different profiles:

- Legitimate registrations—attempts from a variety of IP addresses and ports up to line-rate speeds, including flood scenarios.
- Malformed/corrupted registration messages—incomplete or non-standard registration information.
- Illegitimate registrations—attempts from external users that should not have access.

Even the best tested networks can become susceptible to problems over time. Unfortunately, service providers often do not have complete control of the end-to-end connections between their users and VoIP infrastructure. Changes in one carrier's network can lead to problems in another. To prevent these potential issues, real-time monitoring tools that evaluate registration and user quality should be used to identify new issues and analyze the situations that cause them.

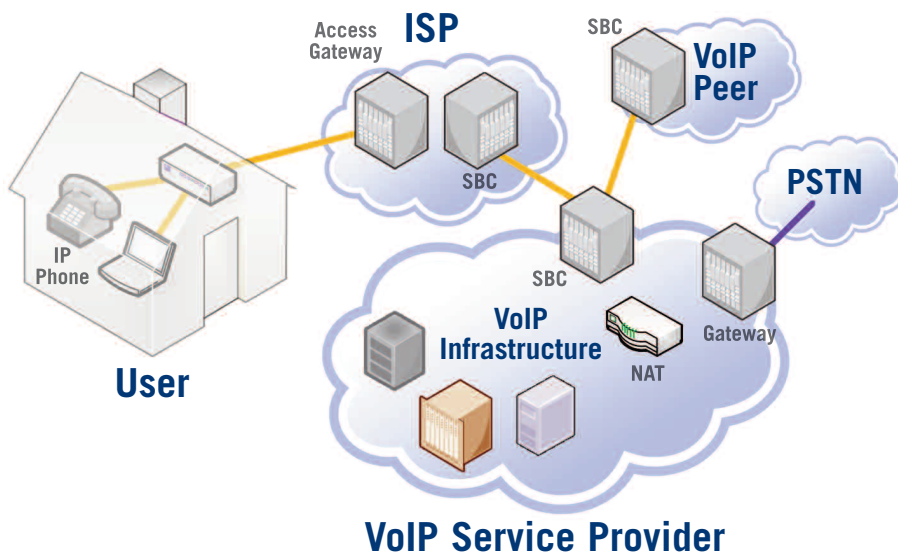


Figure 4. Example of VoIP network showing multiple network peer interconnection points.

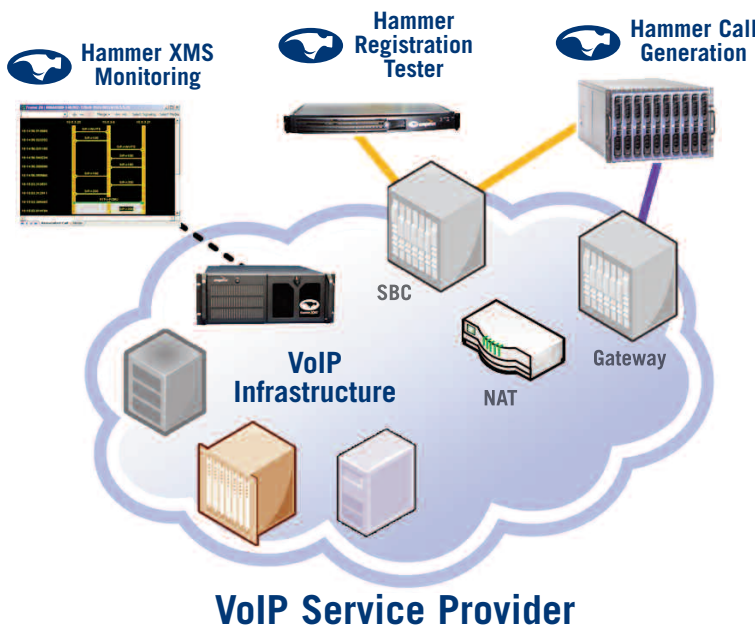


Figure 5. Testing and monitoring a VoIP Service Provider using a registration tester, call generator, and monitoring probe.

Conclusion

The Hammer Registration Tester simulates SIP and IMS endpoints registering to the network. Able to scale from 250 registrations per second and emulating 250,000 end points, the Hammer Registration Tester is useful for feature, functional, and load testing of registration call flows and associated network devices. In addition, the Hammer Registration Tester is based on a flexible signaling engine that is both extensible and editable by the end user, enabling simulation of different implementations of SIP and IMS protocols and advanced negative and malicious-attack testing.