

STANDARDS

As The IP World Converges, Signaling Protocols Continue To Diverge

Nir Zvulun

IP-telephony components frequently fail to interoperate. Why doesn't protocol standardization solve the problem of interoperability failure?

Signaling protocols—programmed into IP-telephony network components to initiate, direct and terminate traffic—are immature, disparate and divergent. The Session Initiation Protocol (SIP), for example, is used mostly in the residential and enterprise markets. H.248/Megaco is favored by carriers to control trunking gateways mediating between the PSTN and the IP network.

In contrast to the incipient IP signaling protocols, PSTN protocols, developed over the past 100 years, are fully mature. Implemented around the world, PSTN systems are generally interoperable.

When VOIP network components fail to interoperate, signaling protocols per se are not exclusively responsible. The failure can often be related to how IP network infrastructure vendors implement them in their products.

Vendors Implement Protocols Differently

Even if two gateway vendors both implement SIP (for example), their gateways may fail to interoperate because software engineers program the protocol differently. The reasons for programming variations are manifold:

- Some vendors deliberately introduce proprietary data (e.g., unique headers) into their protocol programming, forcing customers to remain loyal to them in the future and shutting out competition.
- Within a single protocol, there are multiple sub-standards, packages, versions and updates. Both closed and open protocols are continuously evolving. Vendor development timetables are never in sync. Vendor times to market vary. Many past

deployments still use an interim draft version of a protocol.

- Vendor software engineers program the hundreds of features, capabilities and packages in a protocol according to different roadmaps, in a sequence different than the one specified in the standard, and in a sequence different from other vendors.

- Engineers understand and interpret protocol standards differently.

- Vendors develop customer-specific applications to meet customer requirements. Some customers prefer a simple application, trading off feature-richness for quicker time to market and lower development cost. Others prefer complexity. The result is that often a feature implemented at one end of a connection is unsupported at the other, and the negotiation fails.

Diagnosing Interoperability Failure

Interoperability engineers use debugging logs (for example, Syslog) and network captures (for example, Ethereal) to analyze and diagnose precisely what it is in the implementation of the signaling protocol that is causing interoperability failure. The reason can often be banal. For example: Vendor A software engineer inserted a single space when programming a component's protocol syntax, whereas B implemented a double space.

After diagnosis, these scenarios (among others) can unfold:

- Vendor B can decide to instruct its engineers to modify their implementation and delete a space; new firmware can then be released.

- The vendor implements the above scenario only in products deployed in the customer network in which the interoperability failure was found.

- The initial scenario is implemented in all products shipped to all deployments from now on.

- Vendor B can notify Vendor A that the standard dictates a double space and that A should implement the modification.

Nir Zvulun is a senior interoperability engineer at AudioCodes, and directs the AudioCodes Interoperability Laboratory.

■ It may be against the interests of Vendor A to cooperate, especially if Vendor A enjoys a bigger share of the VOIP market. The rule of thumb is that smaller vendors must perform the adaptation.

■ Or, vendor A agrees to modify its firmware, but only in those products deployed in the customer network in which the interoperability failure was found.

■ Or, the above step is implemented in all products that Vendor A will ship to all deployments from now on.

■ In another type of scenario, sometimes a third-party component connecting Vendor A and Vendor B—for example, a softswitch or a proxy (SIP)/gatekeeper (H.323), etc.—can cause an interoperability failure.

Corporate policy tells the decision-makers working for Vendors A and B what decision to take. Astute decision-makers know that their interoperability team's power increases significantly when their R&D division is given resources for fixes, adaptations and improvements. By correctly integrating the efforts of the interoperability team with the R&D division's, a vendor's VOIP products mature quicker and achieve greater robustness and flexibility.

Interoperability teams may distill the results obtained from such interoperability scenarios into "adaptation packs" (optimal parameter configurations for specific interworking) that can quickly and easily be implemented by customers in future deployments. The larger your bank of packs and the more operator-friendly it is, the greater the likelihood that customers will prefer your products over competitors'.

Smaller vendors usually ask the big players for permission to perform interoperability tests with their products and to exchange critical, non-proprietary information to resolve interoperability issues quickly and inexpensively.

Bigger players often refuse to cooperate with the small fry, forcing the latter to go out and acquire the product and run interoperability tests unilaterally. If a vendor cannot get another vendor's cooperation agreement, and cannot purchase the product for interoperability testing, the arena in which they'll ultimately meet will inevitably be the customer's premises. It's therefore advantageous for a smaller vendor to employ a skilled interoperability team that goes out to the various arenas in the market and finds the incompatibilities between the network components in the field for its R&D division to rectify.

Mixing and Matching On The Basis Of Path-Dependency

More often than not, customers wind up mixing and matching components from different vendors, which are best in their class, to migrate or build their VOIP network. Thus they face the challenge of making the components interoperate.

Customer choice of vendor is widely informed

by path-dependency, i.e., based on an assessment of a vendor's specialization and history. Customers who opt to purchase a vendor's end-to-end solution and later want to add equipment from another vendor may be unable to introduce the new vendor's gear, and are instead forced to stick with the first vendor due to interoperability issues.

Inter-network Interoperability

VOIP networks are vastly more complex than the PSTN. VOIP equipment must interoperate with dozens of different kinds of VOIP network components and services, including: softswitches, call agents, call managers, proxies, gatekeepers, media servers, IP-PBXs, gateways, softphones, VOIP phones, VOIP application servers (such as voice mail, unified messaging, media servers/IVR), multipoint conferencing units, multimedia terminal adapters, cable modem termination systems, broadband telephone systems, multimedia communications servers, session border controllers, firewalls and network address translators (NATs).

Moreover, VOIP equipment must interoperate with PSTN equipment for the hybrid network of the future.

Currently, most enterprise customers are still bound to PSTN equipment. Installing VOIP can require a prohibitively expensive investment in an IP-PBX, IP telephones, integrated access devices (IADs), IP switching equipment and media gateways. This solution may be suitable for a green-field (start-up) scenario, but for an enterprise with an existing telecommunications infrastructure, it unfortunately means scrapping the installed base of legacy PSTN equipment. Therefore, in many cases, enterprises will opt for a hybrid solution.

To achieve a hybrid solution, it is not enough for the equipment to be technologically superior, cost-effective or feature-rich. The equipment must interoperate.

Conclusion

The ideal way to synchronize and ensure reliable communications between VOIP components/applications is to implement one single protocol standard to be followed identically by vendor software engineers around the world.

But of course this is totally unrealistic.

In the best of all possible worlds, vendors ought to be conscious of other vendors in the market; customers should know that interoperability issues can arise; and each vendor, small and large, should employ a team of interoperability engineers to produce interoperability-rich products in cooperation with their R&D software engineers.

Although standardization may be achievable when the technology matures and the stacks are closed, field deployments are currently the battleground of competing infrastructure vendors and standards bodies, all vying for control of the VOIP market□

Interoperability battles are being fought in field deployments