WHITE PAPER

Enterprise Survivability in the Age of All-IP Telephony

The new age of All-IP networking has arrived. Yet many business subscribers will ***not*** switch to IP-based telephony unless your service offering provides full confidence their phones will work—**no matter what!**

PATTON®
Let's Connect!™

Contents

Authored by

W. Glendon Flowers
Product Marketing Manager
Patton Electronics Co.

Marc Aeberhard
Product Line Manager,
Patton Electronics Co.

Printed in the USA.

Introduction

The new age of All-IP networking has arrived. Yet many business subscribers will ***not*** switch to IP-based Telephony unless your service offering provides full confidence their phones will work—**no matter what**!

Now that session initiation protocol (SIP)-based telephony is well established, enabling broad adoption of unified communications (UC), the traditional Public Switched Telephone Network (PSTN) seems a bit clunky and old-fashioned. Yet that old PSTN was—and still is—highly reliable. As carrier-providers—and their subscribers—plunge head-first in to the sea of IP Telephony, the good old PSTN remains good solid ground—a trustworthy *Plan B*—for those inevitable times when your subscriber's **Internet connection fails…** *for whatever reason.*

Another way (in addition to PSTN backup) to solve the uptime problem with Internet-based phone systems is for the subscriber maintain dual access links with separate Internet service providers (ISPs)—ideally over different physical cabling plants with varied networking providers (fiber-optic Ethernet, coaxial cable-modem, copper DSL). This multi-provider approach is highly resilient. In addition to providing a backup plan for the broken WAN access link, it covers potential hardware or software failures in the service-provider cloud. As another layer of redundancy for added resilience, a second Internet Telephony Service Provider (ITSP) may be added to the mix.

Proposed Survivability Solution

This paper proposes a flexible solution for enterprise-telephony survivability and business continuity that employs an intelligent enterprise session border controller (eSBC)—equipped with the necessary features and functions—installed on the subscriber premise.

The Crux of the Problem

Whether your subscriber is operating a business, hotel, school, church or hospital, the problem is the same. How are you going to keep your customer's phone system working—no matter what?

Cloud PBX

In this age where the PBX is often in the cloud, the unfortunate reality is that a loss of connection to the cloud service, for any reason, breaks station-to-station calls within the enterprise, kills 911 emergency services and wipes out inbound and outbound call capability.

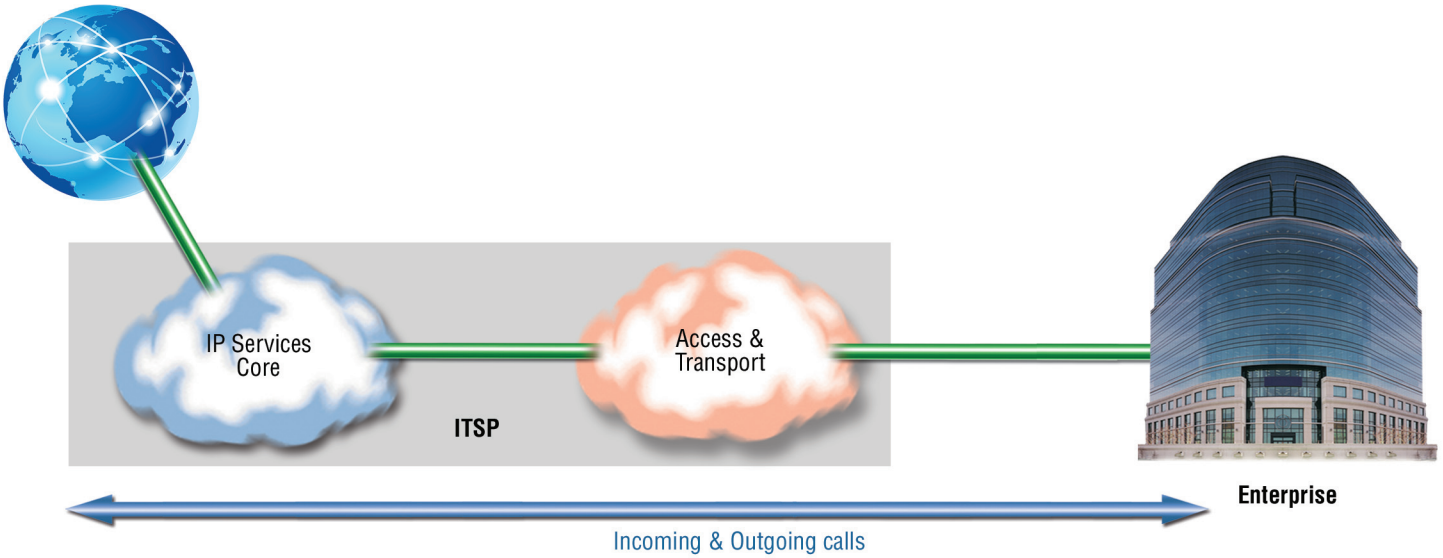


Figure 1: Proposed Survivability Solution

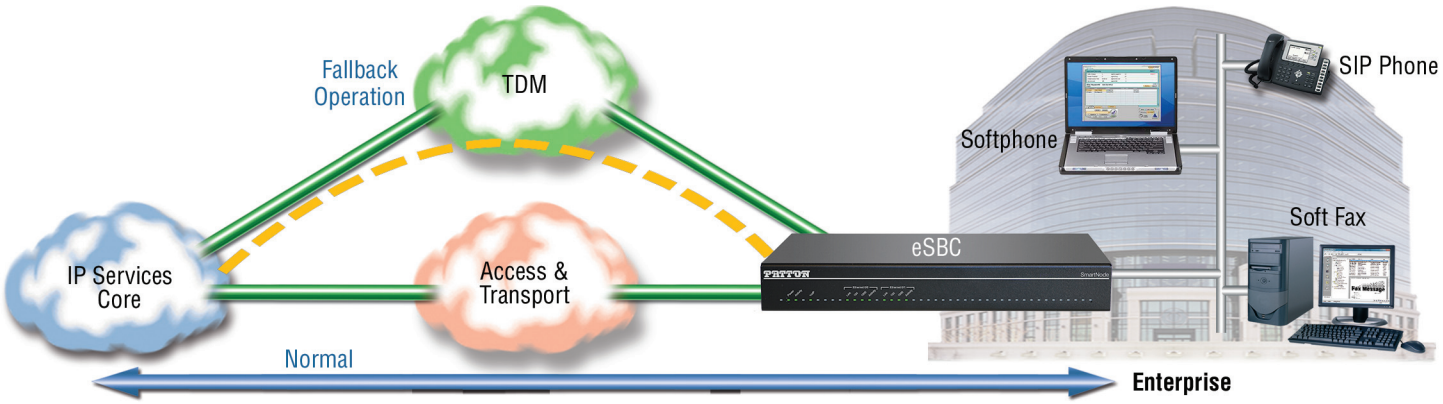


Figure 2: Option A: Survivable PSTN Access

SIP Trunks

In SIP trunking implementations, where the IP-PBX resides on-premise, a broken Internet access link kills inbound and outbound calling. However the PBX can still support station-to-station calls between SIP terminals within the local area network).

Redundancy

Redundancy—rather the absence of it—is the heart of the reliability problem: the lack of redundant connections for Internet and wide area network (WAN) services. Whichever backup plan we choose, PTSN or dual ITSP service, the question remains: *how will the service provider manage and control redundant network-access connections to ensure continuity of operations for the business subscriber?* What are you going to do if the WAN link works, but something else disrupts access to trunk or cloud services?

The Answer

Many organizations that chose to move forward with adopting an All-IP communications system will demand a comprehensive and innovative solution for the survivability problem. Such technology should combine intelligent self-learning capability with automated monitoring, switching and notification mechanisms—all embedded in a customer-premise enterprise session border controller (eSBC).

How to Do it

1) **Redundant WAN connections**—The eSBC should provide multiple on-board interfaces that support WAN connections to the ISP, ITSP, and PSTN. Connectivity options may include:

   - Dual Ethernet ports
   - Wired cable/fiber/DSL
   - Wireless LTE/WiFi

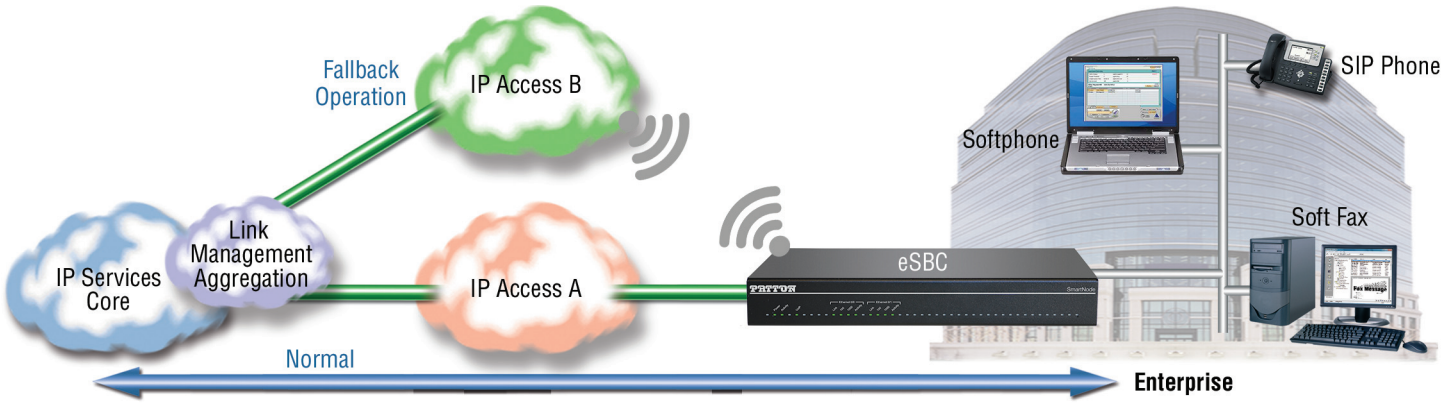


Figure 3: Option B: Redundant IP Access

2) **Intelligent Self-learning**—The eSBC should include a SIP registrar function. The intelligent CPE engages in discovery operations to learn and record the fully qualified domain name (FQDN) of SIP servers residing in the provider networks. Further, the eSBC discovers and records the FQDN of each local IP endpoint (hardware SIP phones, IP softphones) located within the subscriber LAN environment.

   Local Keep-Alive. By automatically registering SIP endpoints that reside on the enterprise LAN, the local eSBC can keep the intra-office (internal) phone system alive for station-to-station calls by handling internal intra-office calls even when there is no live out-route to BroadCloud, BroadWorks or the PSTN.

3) **Real-Time Monitoring**—The eSBC should provide IP-Link supervision. The *SIP Options ping* message (specified in the SIP protocol) is leveraged to monitor the up/down state of SIP servers. If no response is received from a server, a WAN failure is indicated and link switchover is initiated.

4) **Automatic Path Switching (re-Routing)**—When the eSBC must be able to detect a WAN failure, and redirect all SIP traffic over the alternate WAN link—which may be a PSTN connection, secondary WAN, or wireless Internet-access link. Failover notifications should be sent to the enterprise as well as the IP telephony service provider, while inbound and outbound phone calls are re-routed end-to-end over the alternate (backup) path.

5) **Configurable notifications**—Notification can be accomplished via syslog, SNMP, SMS, or eMail. Any or all of the above notification methods may be turned on or off as required by the system administrator.

6) **Other Pluses**—Of course any high-quality CPE should provide all the other value-added benefits available with modern eSBC technology:

   - SIP normalization for interoperability assurance
   - Codec transcoding for bandwidth management and WAN optimization
   - Security mechanisms against tool fraud and denial of service attacks, including call admission control, accesses control lists, and TLS/SRTP encryption
   - Quality of Service (QoS) for the upstream and downstream paths
   - Link Quality monitoring and reporting
   - Cloud support for touchless provisioning, configuration, and management

Alternatives

Various vendors offer an array of redundancy and failover solutions. Most if not all such solutions *require human intervention* to configure IP end-points, edge devices and/or cloud services. Here we will present a summary of the four most popular survivability approaches (other than the Patton solution) currently available in the market, with pros and cons for each:

- Dual Registration (survivability node)
- Back-to-Back User Agent (B2BUA)
- SIP Proxy Server
- Mobile Re-Direct

Dual Registration

PROs: Dual registration is likely the simplest way to *implement* a basic survivability solution.

CONs: Activation may be delayed and inconsistent. Maintenance is complex and requires human intervention.

How it works

A *survivability node* is installed within the enterprise LAN, which does not participate in the normal SIP signaling or call flow. Each SIP endpoint is configured with the address of the survivability node as a secondary (backup) SIP registrar. If the WAN connection goes down, or if the SIP server within the primary

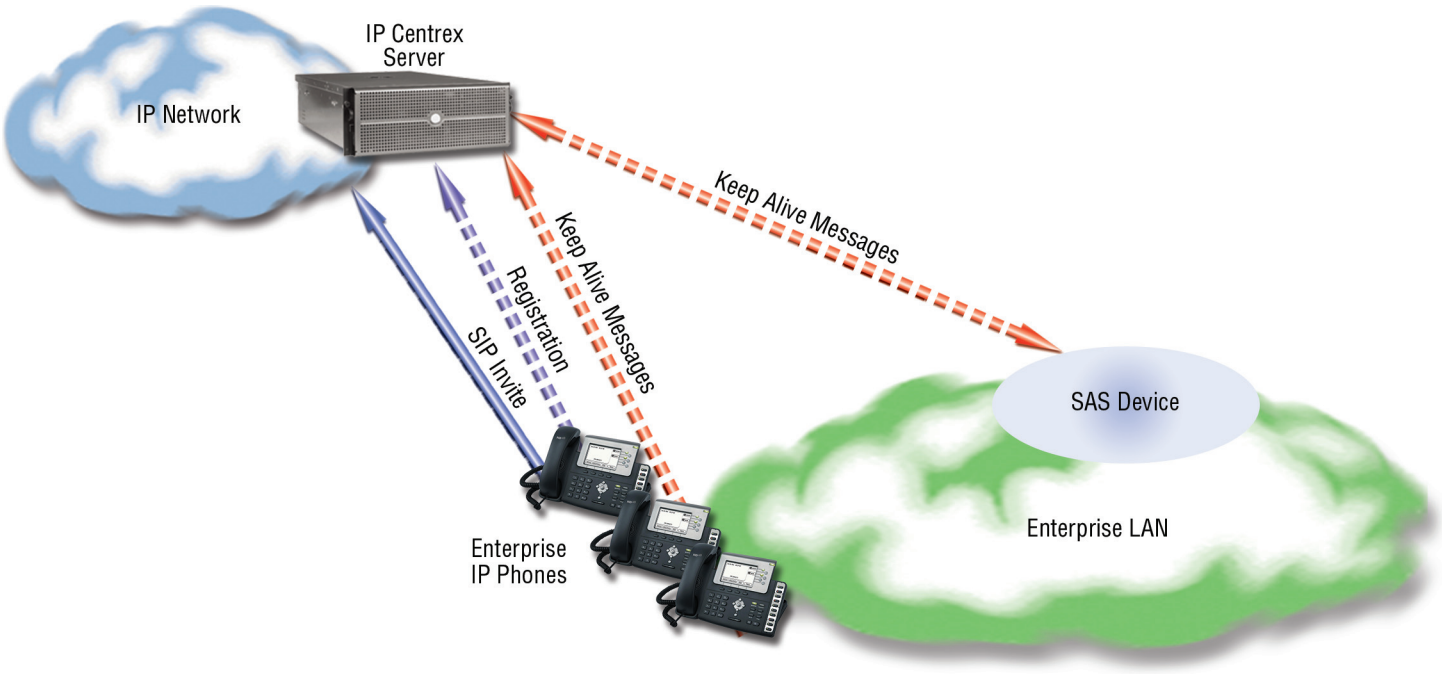


Figure 4: Dual Registration Normal Operation

ITSP becomes unreachable for any reason, local SIP endpoints (hard or soft SIP phones) target the local survivability node for SIP registration and call control.

Normal Operation

The survivability node does not participate in the SIP call-control stream during normal operation. SIP endpoints (phones) register over the WAN-access link to the primary ITSP, which provides all call-control processing. During normal operation status information for the SIP phones is NOT available to the survivability node.

Survivable operation

When the SIP phones cannot reach their primary SIP server, they fail-over to the pre-configured backup server (survivability node). Redirecting SIP registration and call control to the to the local server preserves station-to-station calling within the enterprise, as well as E911 emergency calls to the PSTN over an E1/T1, FXO or BRI connection.

Installation and maintenance

SIP phone configuration. For the dual-registration solution to work, each and every SIP phone must be pre-configured with the address of the fallback SIP registrar (survivability node). Phones that don't support such fallback configuration won't work during an outage of the Internet-access link.

Delayed activation. Failover does not happen instantaneously. It can take several minutes for all the phones to detect WAN-access failure and redirect registration and call flows through the local survivability node.

Inconsistent operation. Since each phone must separately detect the failed WAN link, internal extensions may not all be reachable immediately because each phone must independently switch to the survivability node.

Back To Back User Agent (B2BUA)

PROs: Powerful—Going well beyond the basics of survivable station-to-station and E911 calling the back-to-back user agent (B2BUA) continues to provide SIP-service demarcation, QoS, SIP-header manipulation, and SIP security when the ITSP service is down or un-reachable.

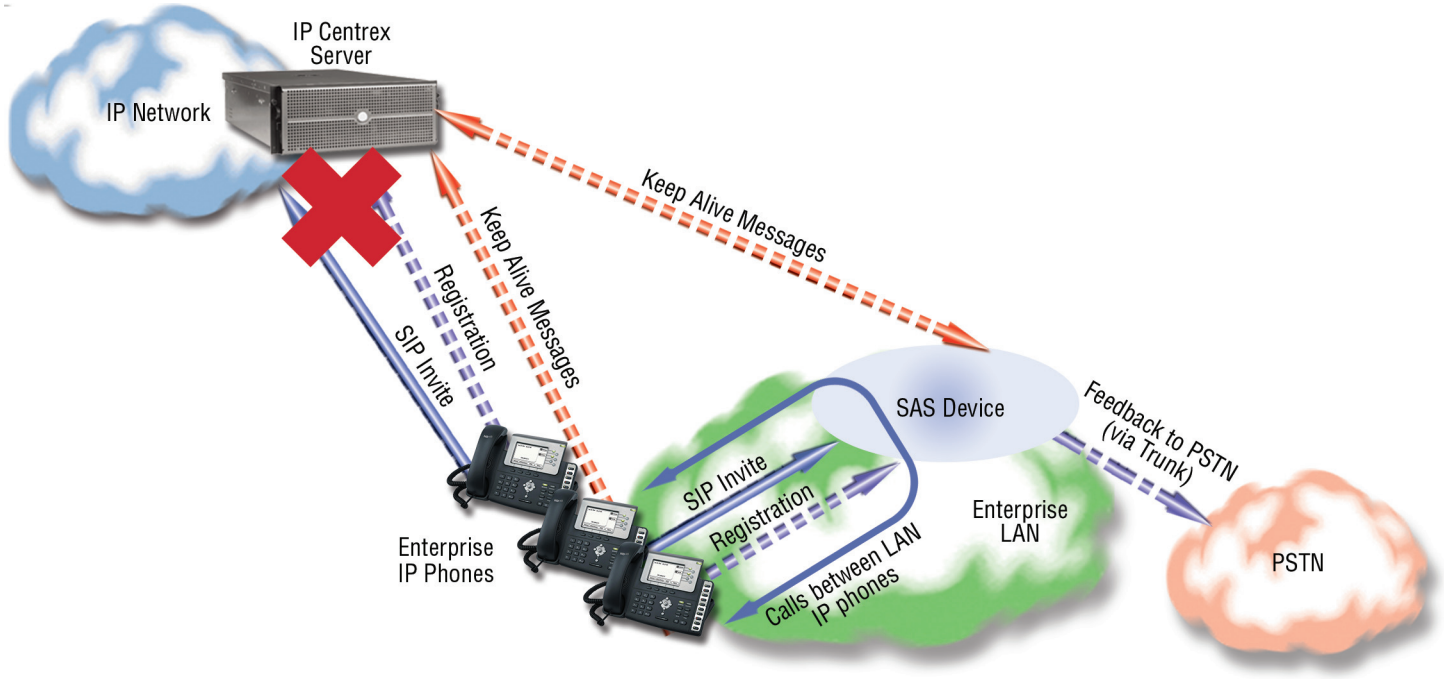


Figure 5: Dual Registration Survivable Operation

CONs: Labor-intensive—For moves, adds, and changes (MACs) the B2BUA must be configured (or RE-configured) with registration credentials for every SIP endpoint. Another consideration: for certain enterprises, especially when the VoIP service is hosted, the added functions this approach provides might be overkill (i.e. unnecessary).

Overview

The B2BUA is set up as the primary registrar for all local SIP endpoints (phones). Credentials for all endpoints are managed and processed by the B2BUA device. Typically a central location provisions and manages the endpoint configurations over a remote connection to the B2BUA. Each new SIP endpoint must be configured in the B2BUA in order to provide survivability functions.

Normal operation

The B2BUA provides secure network separation between the enterprise LAN and the service-provider WAN. The B2BUA receives (terminates) and re-sends (re-initiates) SIP messages from local SIP phones and remote entities (SIP servers, SIP endpoints) accessed via the WAN.

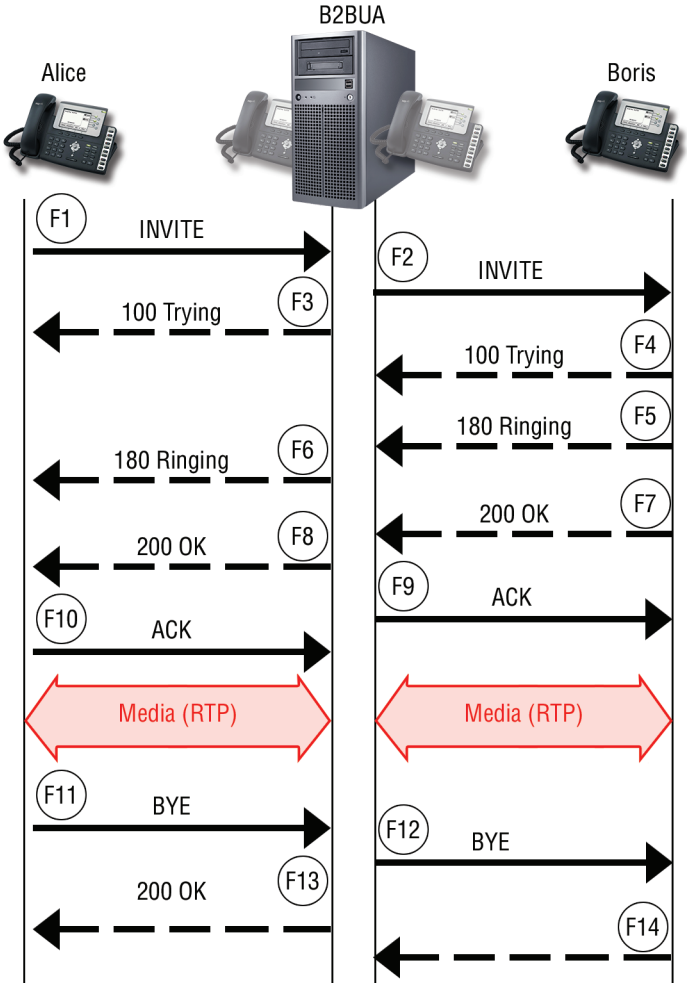


Figure 6: B2BUA Normal Operation

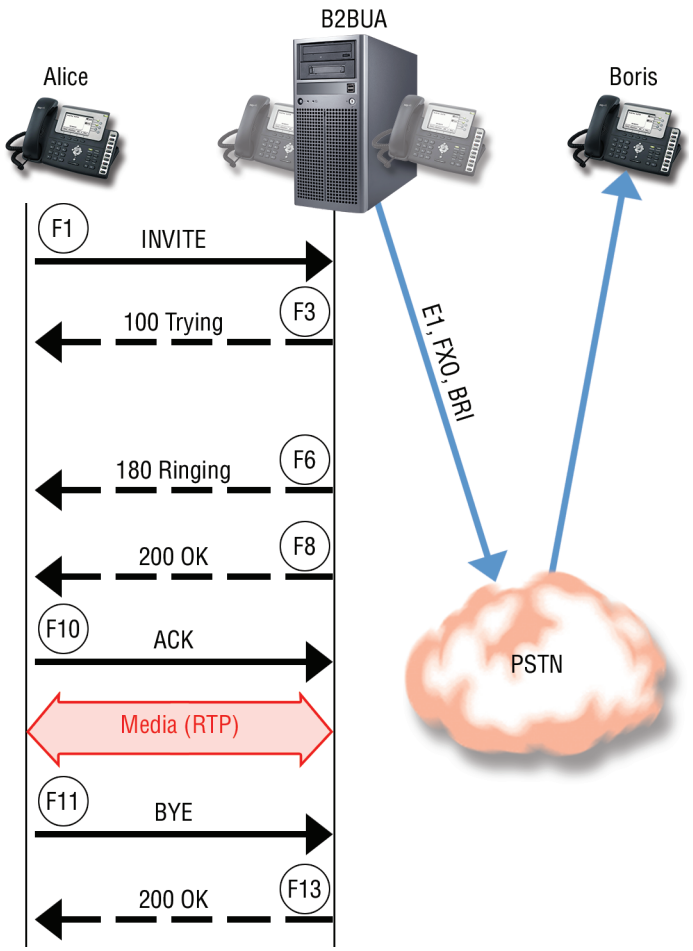


Figure 7: B2BUA Survivable Operation

Survivable operation

The B2BUA monitors the WAN link at all times, regardless of whether the ITSP service is available. If a ping response is not received from the ITSP after a configurable timeout threshold, the B2BUA reroutes calls to an alternative connection (E1/T1, FXO, wireless, or althernet Ethernet line).

In survivability/fallback mode, the B2BUA is able to preserve station-to-station calling because it knows the previously registered addresses of all the SIP phones. The B2BUA solution can also support inbound calls—but only if failover call routing is be pre-configured within the ITSP.

Installation and maintenance

All SIP endpoints must be configured for a single registrar: the local B2BUA. This solution is easier to set up for new installations. When an existing hosted implementation needs to be changed, every SIP endpoints has to be touched and reconfigured to register with the B2BUA.

From a maintenance perspective, this setup requires more effort than a SIP proxy solution (covered below) because the B2BUA must manage and maintain all the local SIP user identities and credentials.

SIP Proxy

PROs: The SIP Proxy approach is less complex than the B2BUA method, with fewer parameters to configure and maintain. Multiple alternate paths (if accessible) can be configured and supported.

CONs: All the SIP phones must be pre-configured to re-direct call flows to a proxy server when the primary SIP server fails. While it can reroute SIP calls over any alternate access link that is available and operating, the SIP proxy does not provide any WAN-link failover mechanism. Further the SIP proxy does not provide the added security features, header manipulation or other feature/benefits the B2BUA offers.

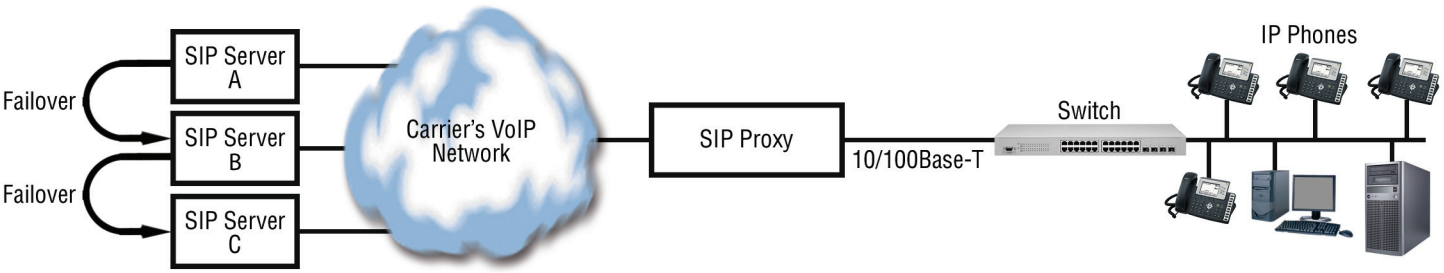


Figure 8: SIP Proxy

Overview

The SIP proxy server (RFC 3261) is essentially a router, examining headers only, and does examine or process the payload of deeper protocol units such as RTP. While is similar to the B2BUA solution, it is a bit simpler to implement and maintain. A SIP proxy can provide local authentication and maintain a user database, **yet the SIP phones must also authenticate with a SIP server within the ITSP network**.

Normal operation

Local SIP phones are configured to send registration requests and call data to the SIP proxy. The proxy server *forwards (does NOT retransmit)* the call-signaling information to the SIP server within the ITSP. The SIP proxy adds a route header that tells the SIP server how to reach the local SIP endpoints—using the proxy as a hop.

Survivable operation

When the primary SIP server becomes unreachable, the SIP proxy re-reroutes SIP calls to the SIP server in an alternate ITSP (this must be pre-configured in the proxy server). In this case, the SIP Proxy only addresses ITSP-related problems—not a WAN link outage. However, if the local network architecture offers alternate outbound WAN connections, the SIP server will re-route call traffic to an available uplink when the primary WAN link fails.

Installation and maintenance

The SIP proxy, if not doing authentication, is quite straight-forward to set up and configure. Still, all the phones must be pre-configured with the proxy address configured for the application to work.

Mobile Re-Direct

PROs: The SIP proxy, if not doing authentication, is quite straight-forward to set up and configure. Still, all the phones must be pre-configured with the proxy address configured for the application to work.

CONs: Partial solution for survivable phone service. Inadequate for most businesses.

Some ITSPs offer a mobile re-direct service, which provides a partial survivability solution for enterprises. When the WAN-access link fails, the ITSP can re-route incoming calls to a mobile phone. This solution only applies to inbound (downstream) calls. In some cases all the numbers handled by a SIP trunk are routed to a single mobile phone. While this mechanism ensures very basic reachability, it severely restricts the level of service for an organization. Of course workers can always use their mobile phones to make outbound calls. However, such business-class features as conferencing and forwarding are missing. And, obviously, personal mobile phone numbers (instead of business numbers) are presented to the called party.

The Ideal

Whether a TDM failover or dual-WAN approach is selected, a fully-automated survivability solution ***must NOT require human intervention*** for link switching or re-configuration of network elements. It must employ intelligent technology to be self-learning. The flexible eSBC might be installed as a stand-alone survivability appliance, yet ideally it should also provide the security, routing, gateway and other eSBC functions enumerated above, as well as the standard survivability mechanisms discussed in this white paper, including:

- **Dual registration**
- **B2BUA**
- **Mobile re-direct**

Conclusion

A flexible eSBC can function as a stand-alone survivability appliance for enterprise IP-telephony to provide all functions cited above. It must employ intelligent technology for self-learning of local SIP endpoint credentials. Further, WAN-link failover must be handled automatically by customer premise equipment. Ideally the eSBC should provide all the other functions enumerated above: gateway, routing, security, and so on.

The solution described above is available from Patton Electronics in the SmartNode eSBC product line.

Because it is *automated*, the Patton survivability solution is unique in the telephony market today.

In addition to the common industry-standard survivability techniques, Patton's-survivability solution includes the following differentiating features and functions:

- **Automatic path switching** (WAN-link failover and call re-routing)
- **Redundant WAN connections** -- All WAN connection types are supported (Ethernet, PSTN, Wireless)
- **Intelligent self-learning** of FQDNs for remote SIP servers and local SIP-endpoints. This means *no configuration or reconfiguration is required for any network elements*.
- **Real-Time Monitoring** of Internet access links and SIP service entities (softswitches, servers, registrars)
- **Configurable Notifications** for state/status changes

Additional benefits that come with the Patton SmartNode brand include:

- **Interoperability**—SmartNode eSBC devices interoperate seamlessly with standard SIP-based telephony service offerings and are certified with all the well-known SIP-based service providers, softswitch vendors, and telephony devices.
- **Automated Provisioning**—SmartNode devices work with the Patton Cloud to support automated provision from remote locations
- **Split Management Domain**—Also known as *split configuration domain*, this feature clarifies and enforces the secure demarc by separating the customer-facing configuration from the carrier-facing configuration. This feature allows the service provider to manage the WAN-facing configuration while only the customer (and/or the integration partner that provides installation services) can manage the LAN/iPBX-facing configuration. The carrier-provider defines which SmartNode parameters may be configured by the customer/installer and which parameters are accessible only to the service-provider.
- **Patton Cloud**—The Patton Cloud service supports SmartNode eSBCs by providing edge orchestration functions that include feature license management, provisioning, configuration, and other element management services all the way to the customer premise—along with failover notifications.

Manufactured in the USA, SmartNode eSBCs provides all the features and functions cited above, combined in a **single customer-premise device**.

About Patton

Patton is all about connections. It is our joy and mission to connect real-world customer challenges with high-quality, right-priced solutions—complemented by unrivaled customer service and technical support. Incorporated 1984, Patton has built everything from micro-sized widgets that connect "this-with-that," to carrier-grade Telecom gear that connects subscribers to service-providers. Patton's specialty is interconnecting legacy TDM and serial systems with new-generation IP-based voice, data, and multimedia technologies.

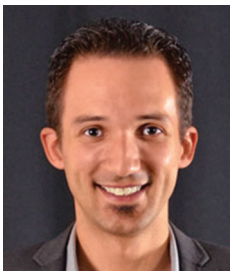
Headquartered in Gaithersburg, MD, USA, Patton equipment—including VoIP, Ethernet extension, and wireless router technologies—is up-and-running in carrier, enterprise and industrial networks worldwide. Patton works in connection with a growing network of technology, business, and sales-channel partners. To connect with local-market requirements, Patton operates training and support centers in Switzerland, Hungary, Lebanon, Australia and the USA.

Patton… Let's Connect!

About the authors

W. Glendon Flowers
Product Marketing Manager,
Patton Electronics Co.

Glendon is responsible for creating corporate marketing and technical content including press releases, web copy, white papers, case studies, educational and tutorial pieces as well as other publications. He serves as editor in chief for Patton's email newsletter and other outbound communications. He holds a Bachelor of Science in Computer Science from UMUC and a Bachelor of Music in percussion performance from UMCP.



Marc Aeberhard
Product Line Manager,
Patton Electronics Co.

Marc Aeberhard is SmartNode Product Line Manager at Patton, based in Switzerland. He is a specialist in Business administration and technical management and holds a Swiss federal diploma. He is involved in Telecommunication technology for close to 20 years and is with the company for more than 10 years where he previously was leading the technical support team in Western Europe.

PATTON®
let's Connect!™

7622 Rickenbacker Drive
Gaithersburg, MD 20879 USA
tel: **+1.301.975.1007**
fax: **+1.301.869.9293**
web: **www.patton.com**
email: **marketing@patton.com**
Document: 07M-ENTSURVALLIP-WP