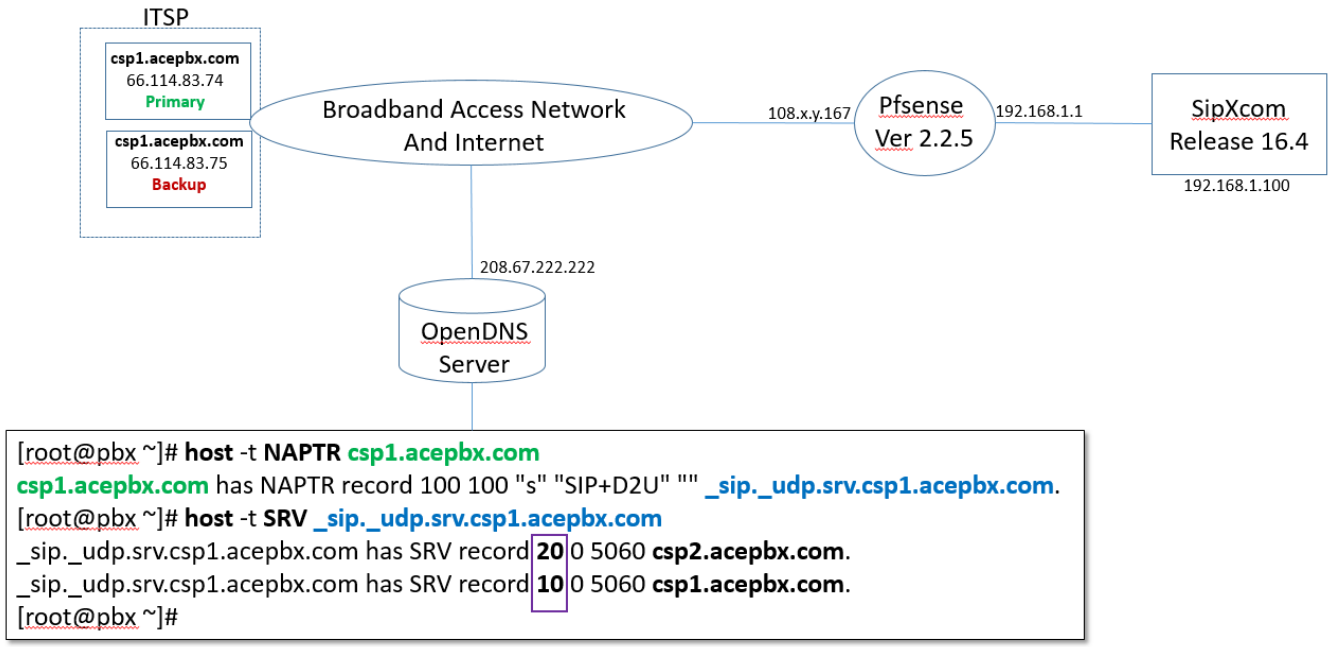
SipXbridge and Interoperating with High Availability ITSP Nodes

This document describes the issues and workaround of connecting to a high availability ITSP node using the SipXcom SipXbridge pseudo-SBC capabilities. The high-availability ITSP node configuration provided by Ace Innovative will be used to describe the situation - the network configuration is as follows:



Ace Innovative has recently introduced a high availability service and has begun migrating most of their clients to this ITSP node named **csp1.acepbx.com** . There are actually two target nodes behind **csp1.acepbx.com** - **csp1.acepbx.com** (66.114.83.74) and **csp2.acepbx.com** (66.114.83.75). **csp1.acepbx.com** is provisioned in the address field (PSTN gateway address in the **Devices->Gateways->SIP trunk** menu) when the SIP trunk is defined. The way Ace has defined the service is that all traffic goes through the primary **csp1** node and the backup **csp2** node is used only when **csp1** is unavailable. In the above diagram, Ace Innovative has defined a NAPTR record for **csp1.acepbx.com** called _sip._udp.srv.csp1.acepbx.com. That NAPTR record is then used to query the SRV records - two are returned. The target node **csp1.acepbx.com** is the record with the lower priority (10) and Sipxbridge should register to this node. Sipxbridge queries for the NAPTR and SRV records correctly - the issue is that Sipxbridge prior to 17.10 does not process the SRV records correctly, and registers the trunk to **csp2.acepbx.com** about 50 percent of the time. sipXbridge in 17.10 and later now handles ITSP connections with SRV records.

The good news is that on a busy Sipxcom system, there is no impact when the SIP trunk registers to **csp2.acepbx.com**. Sipxbridge always sends a keep-alive UDP packet every 20 seconds to **csp1.acepbx.com** regardless of whether the SIP trunks registers to **csp1** or **csp2**. If there are incoming PSTN calls that arrive within the 10 minute SIP trunk registration window, then the invites will continue to be delivered from the primary **csp1** node. The firewall state for **csp1** is maintained by the 20-second Sipx keep-alive packet, so the incoming call successfully traverses the firewall to the Sipxcom server.

If there are no incoming calls within the 10-minute interval when the SIP trunk is registered to **csp2**, and the subsequent registration also registers to **csp2**, then invites for incoming PSTN calls on the SIP trunk will be sent from **csp2**. This presents a firewall state issue - when the SIP trunk registers to **csp2**, firewall states are created for **csp2** and the 20 second keep-alive maintains the firewall states for **csp1.** However firewall state information for **csp2** ages out in 60 seconds when default firewall parameters are used.

Diagnostics: Show States

States | Reset States

Firewall state immediately after SIP trunk Registers

Current total state count: 128

Filter expression: 66.114.83.7 Filter Ki

Int	Proto	Source -> Router -> Destination	State
LAN2	udp	66.114.83.75:5060 <- 192.168.1.100:5080	MULTIPLE:MULTIPLE
WAN	udp	108.[redacted].167:5080 (192.168.1.100:5080) -> 66.114.83.75:5060	MULTIPLE:MULTIPLE
LAN2	udp	66.114.83.74:5060 <- 192.168.1.100:5080	MULTIPLE:MULTIPLE
WAN	udp	108.[redacted].167:5080 (192.168.1.100:5080) -> 66.114.83.74:5060	MULTIPLE:MULTIPLE

States matching current filter: 4

Diagnostics: Show States

States | Reset States

Firewall state 60 seconds after SIP trunk Registers

Current total state count: 101

Filter expression: 66.114.83.7 Filter Ki

Int	Proto	Source -> Router -> Destination	State
LAN2	udp	66.114.83.74:5060 <- 192.168.1.100:5080	MULTIPLE:MULTIPLE
WAN	udp	108.[redacted].167:5080 (192.168.1.100:5080) -> 66.114.83.74:5060	MULTIPLE:MULTIPLE

States matching current filter: 2

The workaround is to replace the **csp1.acepbx.com** address in the SIP trunk definition with the actual IP address (64.114.83.74) in the Sipxcom gateway configuration definition - this forces all registrations to **csp1** but bypasses the high availability capability.