SESSION BORDER CONTROLLERS PRODUCT LINE

SANGOMA

CONNECT WITH SANGOMA

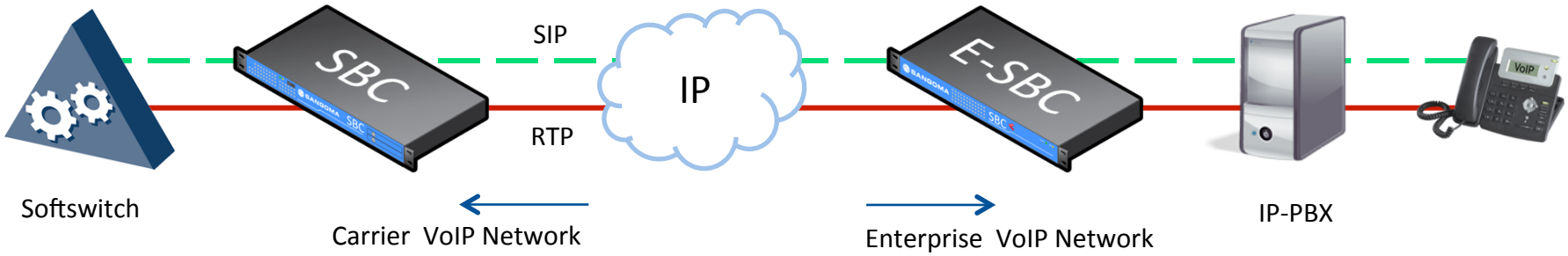
SBC Defined

- To ensure VoIP interop end to end, you need SBC functionality to:
  - Solve firewall and NAT issues (ALG)
  - Normalize sip messaging / Fix errors in the sip messaging stream
  - Register sip trunks with ITSP
  - Secure SIP & voice (TLC, SRTP, IPSEC)
  - Codec conversion / Protocol Translation – UDP/TCP
  - Manage QoS settings and SLA
  - Usage policies
  - Provide access to remote users without complicated VPN account management

Traditional Firewalls or ALG do not cover this range of functions;
SBCs are Natural Extensions to Firewalls / UTM devices

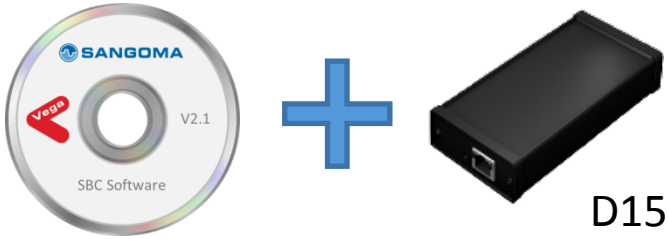
Rule of thumb / Best Practices

- Everywhere a VoIP Network needs to interface to another VoIP Network, you need and SBC
- Same rule with IP Network and Firewalls
- SBC are required in both Carriers and Enterprise Networks



Enterprise SBC

- Appliance
  - 25-250 Sessions
  - H/W DSP acceleration
  - 1U / 2 x 1 GE ports
- Software Version
  - 25-250 Sessions / Self-Contained ISO
  - VM requirements
    - 1 Core / 1 GB RAM / Bridged
- Software / Hybrid Version - UNIQUE
  - 25-400 Sessions / Self-Contained ISO
  - VM requirements
    - 1 Core / 1 GB RAM / Bridged
  - H/W DSP acceleration



D150

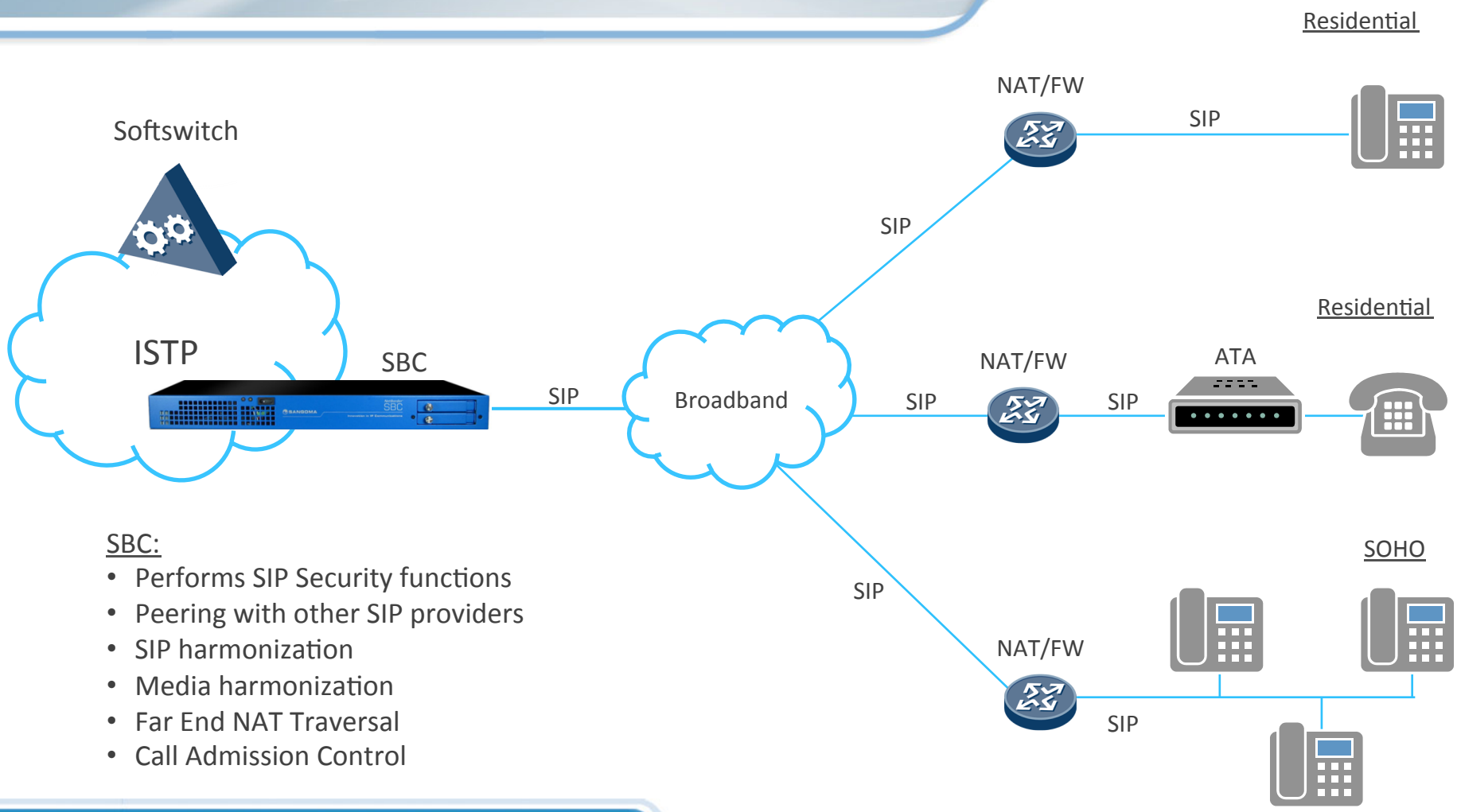
NetBorder Carrier SBC

- Appliance
  - 400-4000 Sessions
  - H/W DSP acceleration
  - 1U / 2 x 1 GE ports

Product Highlights – All SBCs

- Web GUI for ease of Configuration and Deployment
- Efficient Scaling from 25 to 4000 Sessions
- Session-based licensing, not hidden costs or fees
- Cost-Effective Carrier-Class Features and Performance
- Network Interconnect Point for SIP Trunking
- Certified for Microsoft Lync 2013
- QOS & QOE (Quality of Experience) for Enterprise Networks
- Encryption and Security
- Topology Hiding for Fraud Protection
- DOS/DDOS Attack Protection
- Advanced Routing
- Hosted NAT traversal
- Voice, Video, Fax, IM and Presence Support
- SIP-SIP Interworking & protocol normalization

USE CASE : Carrier SBC for SIP 'dial tone'

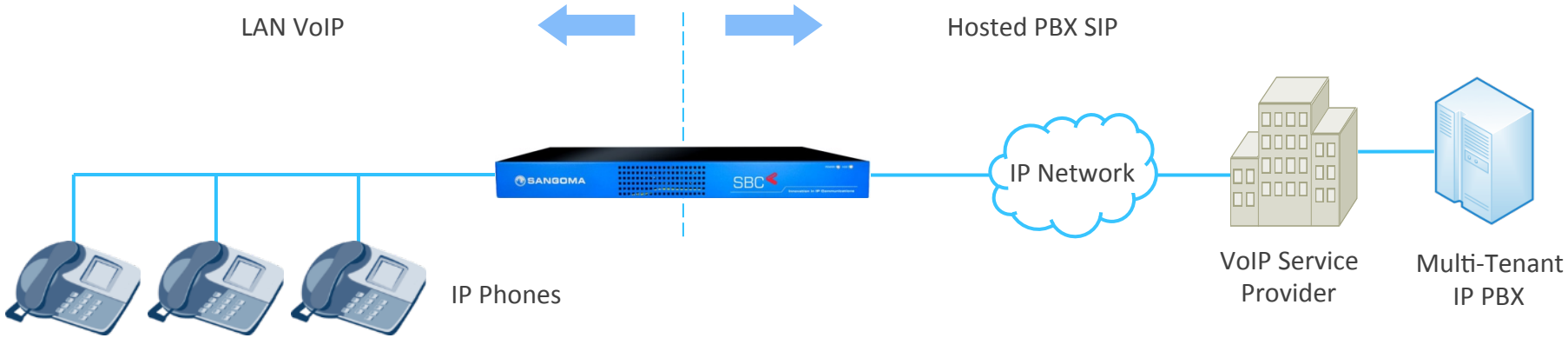


SBC:

- Performs SIP Security functions
- Peering with other SIP providers
- SIP harmonization
- Media harmonization
- Far End NAT Traversal
- Call Admission Control

USE CASE : Enterprise SBC For Hosted PBX / Remote User

- Advantages
  - Known demarcation point
  - Reduces interoperability issues/resource with core
  - Transcoding if required
  - No need for VPN to secure traffic

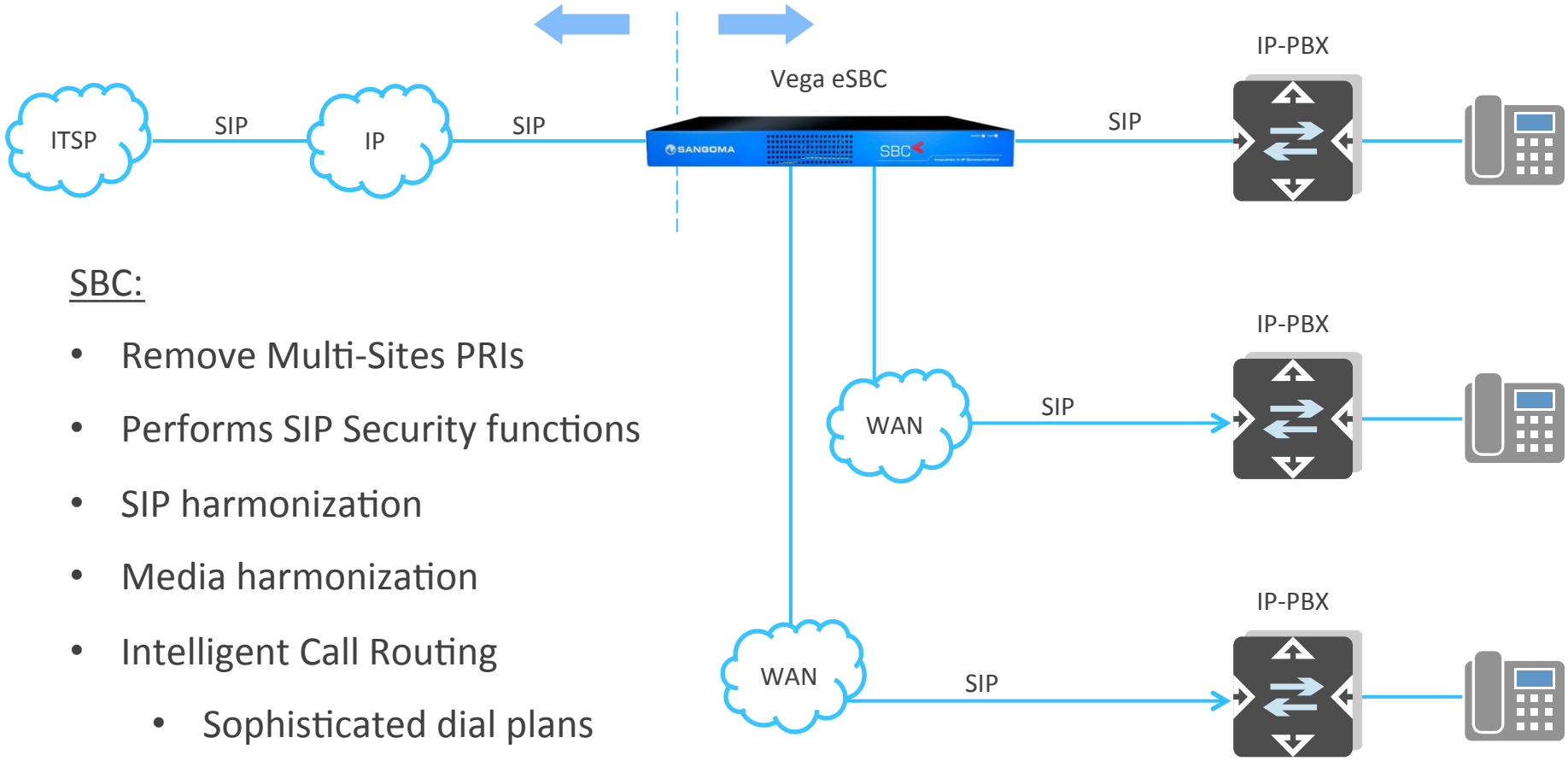


Use Case: Enterprise SIP Trunking

DMZ Deployment

Direct Deployment on Public IP address

Use Case: Multi-Site Consolidation



SBC:

- Remove Multi-Sites PRIs
- Performs SIP Security functions
- SIP harmonization
- Media harmonization
- Intelligent Call Routing
  - Sophisticated dial plans

High Availability Scenarios

Sangoma Session Border Controllers

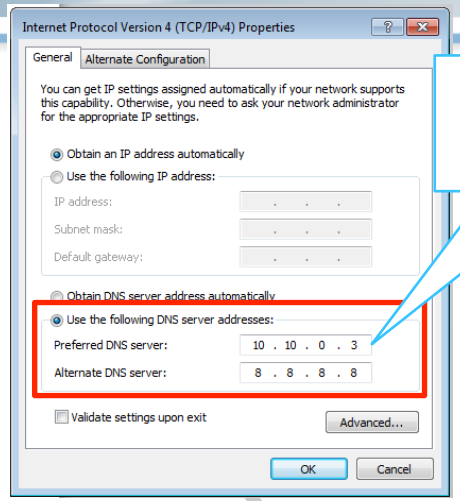
SANGOMA

CONNECT WITH SANGOMA

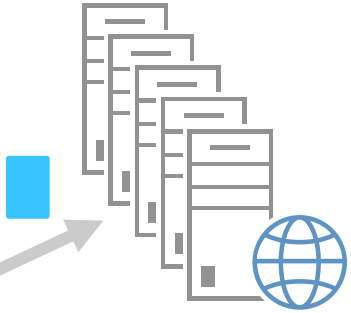
DNS Technology

- DNS = Domain Name System
- Used as ‘phonebook’ for the Internet
- Internet all works on IP addresses
- DNS infrastructure allows you to remember something like www.google.com instead of 173.194.43.71 (Google’s IP address)
- DNS infrastructure is a hierarchy of databases distributed across the Internet
  - See http://en.wikipedia.org/wiki/Domain_Name_System

DNS Illustrated



PC is configured to use ISP's DNS Servers



www.google.com
173.194.43.71

Internet

I need directions to www.google.com

DNS Server
10.10.0.3

Thanks for the directions. I will send my request to 173.194.43.71

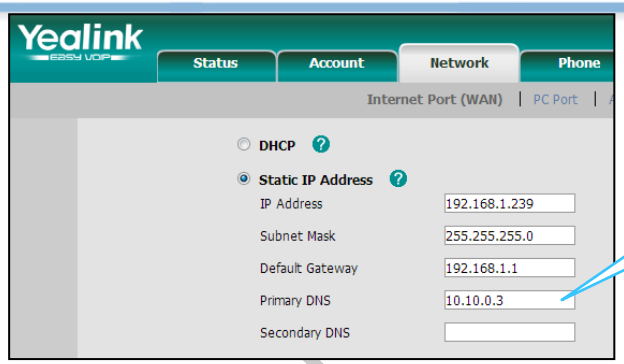
The domain name www.google.com maps to IP address 173.194.43.71

I am doing SIP Telephony, not Web!

- With SIP, it is actually pretty similar!
- A call in SIP might start like this:

  ‘19054741990@sangoma.com’
- For the call to proceed, your phone needs to find sangoma.com
- It will of course use DNS to do this
- Sangoma.com could be an IP-PBX, a softswitch, a proxy server

SIP Call Illustrated



Telephone is configured to use ISP's DNS Servers

SIP Server
www.sangoma.com
50.56.194.118

Internet

I need directions to sangoma.com

DNS Server
10.10.0.3

Thanks for the directions. I will send my request to 50.56.194.118

The domain name www.sangoma.com maps to IP address 50.56.194.118

DNS is a massively distributed database

- Database entries are called Records
- Database look ups and IP resolution takes just a few msec
- It is very reliable – it is the foundation of the internet
- Several types of DNS records exist:
  - A type: Map a single domain name to an IP address (1:1)
  - SRV Records: Service Records. Useful for locating specific services (such as SIP) and multiple servers
  - Many others (MX, AAAA, etc.)

DNS SVR Records Structure

_Service.Proto.Name TTL Class SVR Priority Weight Port Target

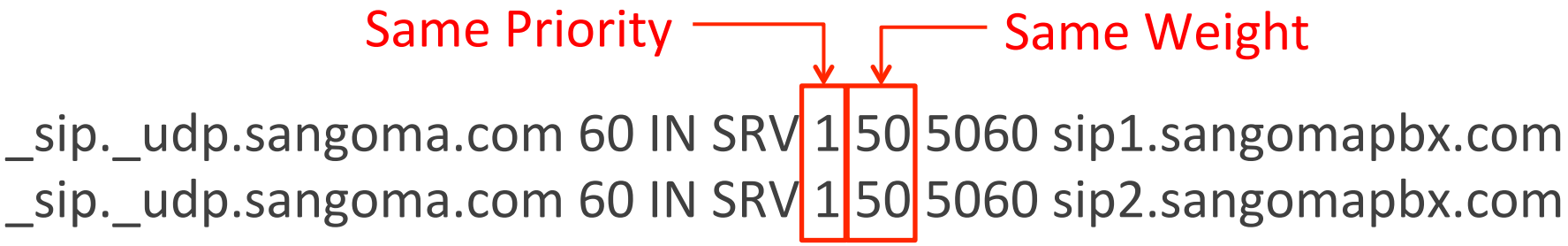
- Service: the symbolic name of the desired service.
- Proto: the protocol of the desired service; this is usually either TCP or UDP.
- Name: the domain name for which this record is valid.
- TTL: standard DNS time to live field.
- Class: standard DNS class field (this is always IN).
- Priority: the priority of the target host, lower value means more preferred.
- Weight: A relative weight for records with the same priority.
- Port: the TCP or UDP port on which the service is to be found.
- Target: the canonical hostname of the machine providing the service.

- Example: A query to sangomapbx.com would yield

  _sip._udp.sangoma.com 60 IN SRV 1 50 5060 sip1.sangomapbx.com
  _sip._udp.sangoma.com 60 IN SRV 1 50 5060 sip2.sangomapbx.com

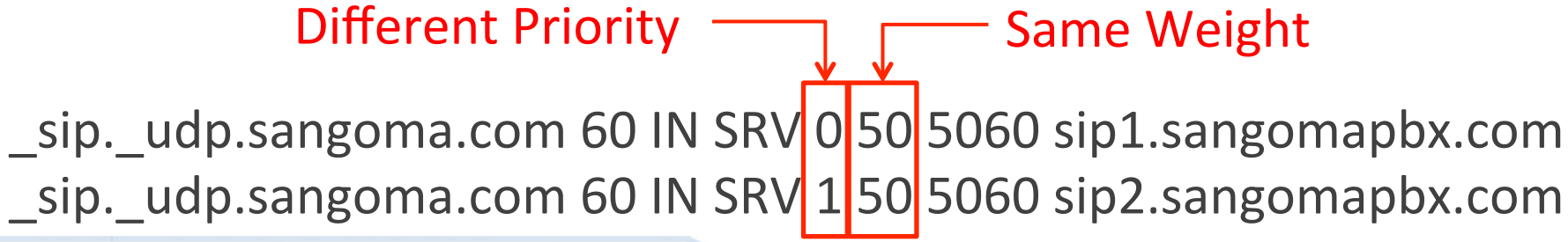
Load Balancing with DNS SRV

- All SRV records with the same Priority form a load balancing group
- Weight allows for distribution
- Example: Even Distribution between 2 servers



Failover with DNS SRV

- SRV Records with a lower priority value are tried first
- Records with higher priority values are only tried if all records with a lower priority are considered unreachable
- Example: Failover between 2 servers



DNS and SBC deployments

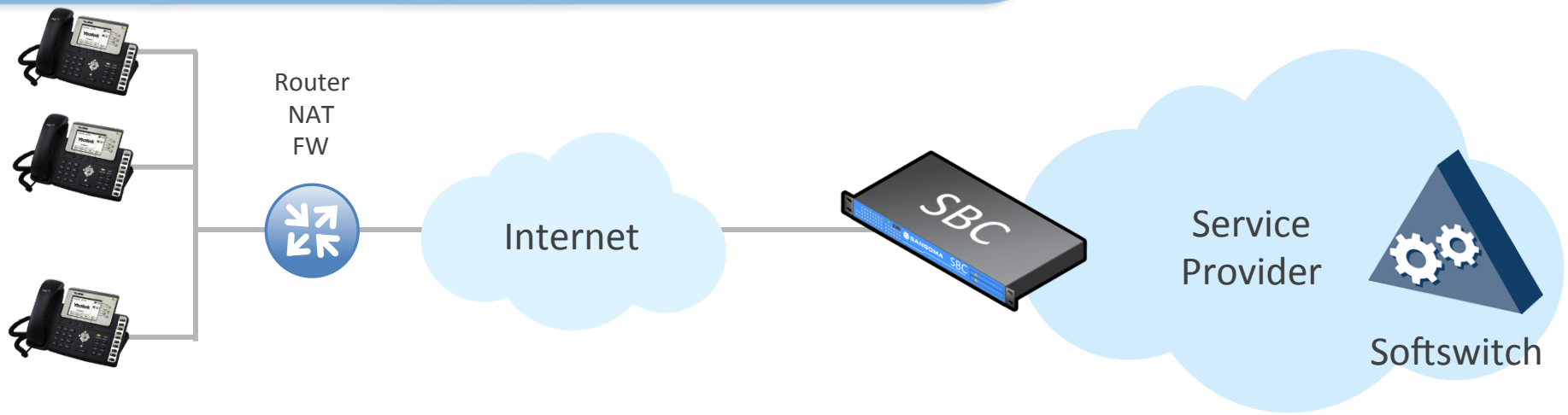
SANGOMA

CONNECT WITH SANGOMA

Session Border Controllers

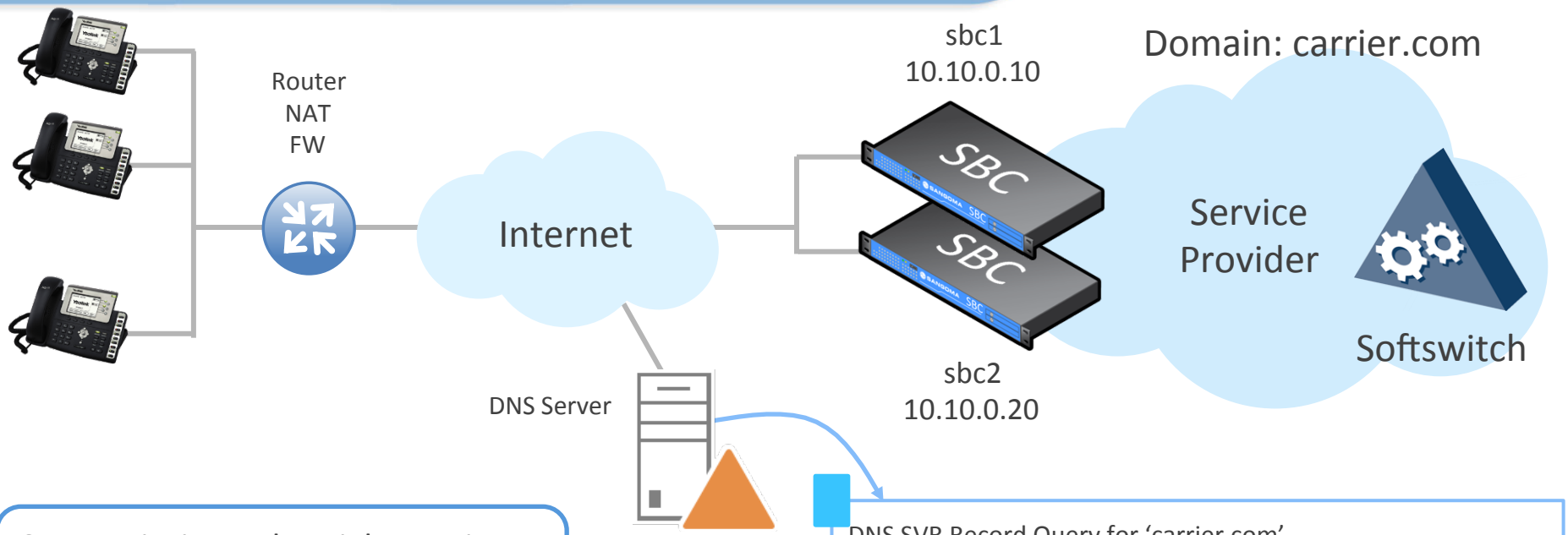
- Installed at the border of VoIP networks for:
  - VoIP Security
    - NAT Traversal, Ddos, Call Admission Control, topology hiding, etc.
  - SIP Mediation
    - SIP header differences, port remapping, etc.
  - Media (RTP) Mediation
    - Transcoding, DTMF, Fax Relay, port remapping, etc.
  - Secure Remote Access of VoIP users

Typical Service Provider SBC deployment



- Hosted PBX Service
- SBC Protects SP's Network ; performs far end NAT traversal, etc.
- Each VoIP Phone sends all SIP protocol messages to SP'S Softswitch via SBC (phone's outbound proxy settings)
- SBC is critical; if it fails no service for 1000's of users

Load Balancing SBCs with DNS SRV



Same priority and Weight entries:

- sbc1 and sbc2 would each get 50% of the traffic load
- If one SBC becomes unavailable, remaining machine takes the load

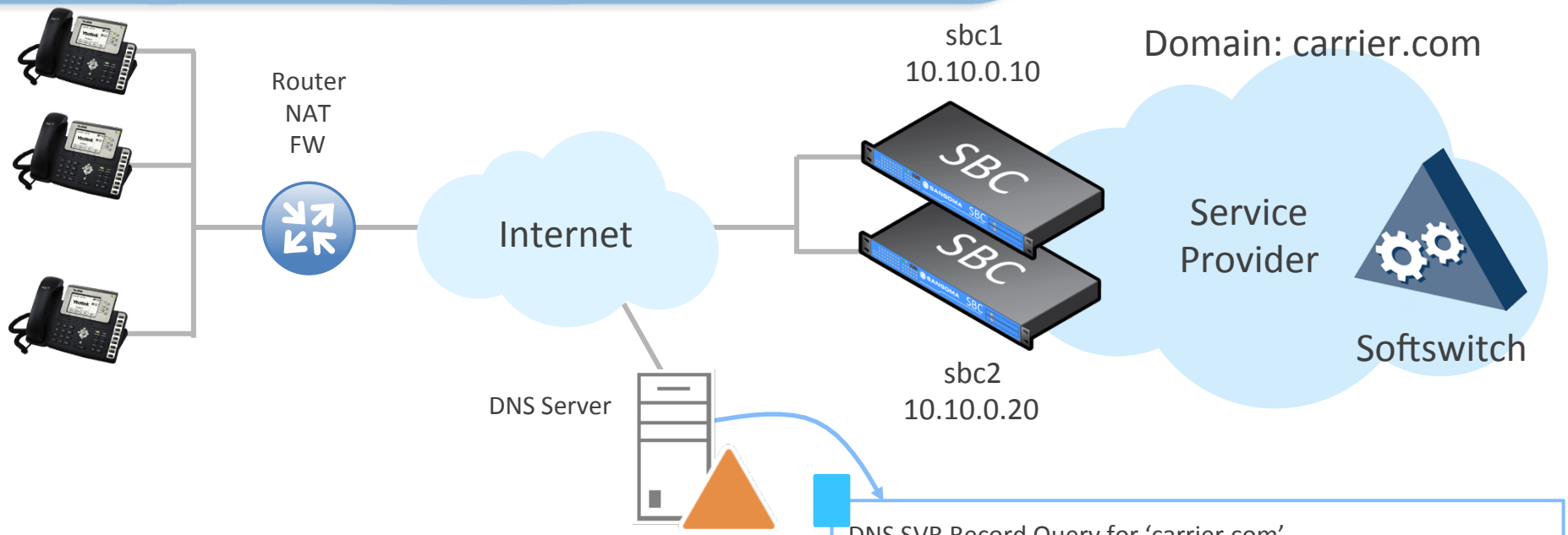
DNS SVR Record Query for 'carrier.com'

_sip._udp.carrier.com 60 IN SRV 10 50 5060 sbc1.carrier.com
_sip._udp.carrier.com 60 IN SRV 10 50 5060 sbc2.carrier.com

DNS A Record Query

sbc1.carrier.com = 10.10.0.10
sbc2.carrier.com = 10.10.0.20

Failover SBCs with DNS SRV



- Different Priorities
- Lower Priority tried first:
  - sbc1.carrier.com
- If sbc1.carrier.com unavailable:
  - sbc2.carrier.com

DNS SRV: Countless other scenarios

- DNS SRV records not limited to 2 lines
- Could implement several scenarios:
  - M-ways load balancing
  - M-ways load balancing ; N-way failover
- Example:

```
_sip._udp.carrier.com 60 IN SRV 10 60 5060 sbc1.carrier.com
_sip._udp.carrier.com 60 IN SRV 10 20 5060 sbc2.carrier.com
_sip._udp.carrier.com 60 IN SRV 10 10 5060 sbc3.carrier.com
_sip._udp.carrier.com 60 IN SRV 10 10 5060 sbc4.carrier.com
_sip._udp.carrier.com 60 IN SRV 20 0  5060 sbc5.carrier.com
```

- The first 4 SBC would share the load at 60%, 20%, 10% and 10% respectively
- If the fist 4 SBC should become unavailable, sbc5 would take the load

Q & A

[Q] You only showed an example with Hosted PBX service. Can I implement this with IP-PBX and SIP Trunks?

[A] Yes. The same principles apply. Instead of SIP phones configured to respond to DNS SRV answers, it would be an IP-PBX

[Q] You only showed an example with Hosted PBX service. Can I implement this with VoIP Gateways and SIP Trunks?

[A] Yes. The same principles apply. Instead of SIP phones configured to respond to DNS SRV answers, it would be a VoIP GW. Note that Vega gateways can support DNS SRV responses.

[Q] You only showed an example with carrier SBCs. Can I implement DNS SRV with Enterprise-SBCs?

[A] Yes. In this case the DNS infrastructure will be internal to the enterprise, instead of reaching out to public DNS Servers. This is very common in the enterprise.

[Q] Can most VoIP endpoint support DNS SRV look-ups?

[A] Yes. It is advisable to verify with your supplier however. Sangoma e-SBCs and Vega VoIP Gateways support DNS SRV look-ups and responses.

[Q] With DNS SRV, if an SBC goes down, what happens to the active calls on it?

[A] Call are dropped, new calls are taken care of by the remaining SBCs.

[Q] Do I need to set a low Time to Live (TTL)?

[A] It is advisable, to make sure SIP endpoints (phones, PBX, Gateways) refresh their DNS cache often; make new queries and obtain the IP address of active server quickly in case of a failover. 30 seconds is typical.

[Q] This seems theoretical and esoteric.

[A] No. DNS SRV is inherently embedded in the fabric of the internet and TCP/IP Networking. Several references to DNS SRV in SIP Networking:

- RFC 2782: DNS SRV
- RFC 3263: Locating SIP Servers
- www.cs.columbia.edu/techreports/cucs-011-04.pdf
  - » Failover and Load Sharing in SIP Telephony

Load Balancing vs Failover

- Both scenarios are quite valid to offer HA
- Load Balancing brings in a few more advantages:
  - All equipment is active
  - Allows to double the call rate and accommodate for traffic bursts
  - Sometimes referred to as Active-Active Scenario
- Fail-over
  - Only 1 unit active
  - Traffic limited to the capacity of that 1 device
  - Sometimes referred to as Active-Standby Scenario

THANK YOU!
QUESTIONS?

SANGOMA

CONNECT WITH SANGOMA