Cisco Service Advertisement Framework Fundamentals

What You Will Learn

Cisco[®] Service Advertisement Framework (SAF) is a network-based, scalable, bandwidth-efficient approach to service advertisement and discovery. Unlike traditional service discovery mechanisms, Cisco SAF provides a dynamic, network-integrated, real-time messaging mechanism that allows host applications the ability to discover the existence, location, and configuration of networked resources through a local area network (LAN) or across a wide area network (WAN) based on industry-proven Cisco IP routing technology.

This whitepaper is targeted for technical decision makers as well as anyone interested in learning more about the functional components and protocols of SAF.

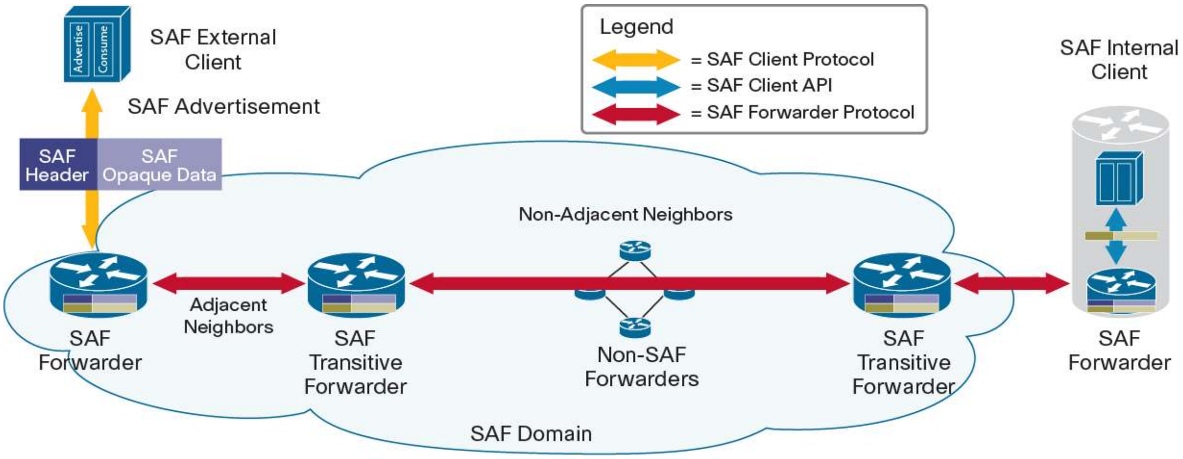
To learn more about applications and benefits of Cisco IOS[®] SAF, refer to *Service Advertisement: Application Service Advertisement on Your Networks*, available at http://www.cisco.com/go/saf.

This technical whitepaper covers the following topics:

- SAF Terminology
- The Role of SAF Forwarders
- The SAF Forwarder Protocol
- SAF Neighbor Relationships
- Connecting SAF Forwarders
- The Role of SAF Clients
- The SAF Client Protocol
- How Services Are Advertised and Propagated
- SAF Service Identifier
- SAF Domains

SAF Terminology

Figure 1. SAF Components and Protocols



SAF consists of the following functional components, protocols and concepts (Figure 1):

- SAF Service: Any information that a SAF Client wishes to advertise (publish) or consume (subscribe to)
- SAF Client: Advertises and/or consumes information about services
- SAF Forwarder: Distributes and maintains SAF service availability information
- SAF Transitive Forwarder: Router that distributes and maintains SAF service availability information but does not have SAF Clients connected
- Non-SAF Forwarder: Router that does not understand SAF, but forwards SAF information as IP packets
- SAF Domain: Administrative boundary and policies that are common to a group of SAF Forwarders
- Non-SAF Network: Collection of non-SAF Forwarders (for example, an IP VPN service provider network)
- SAF Forwarder Protocol: Used to communicate between SAF Forwarders
- SAF Client Protocol: Used to communicate between SAF Clients and SAF Forwarders
- SAF Client API: Used by SAF internal client to establish relationship with SAF Forwarder
- SAF Advertisement: Carries service information; consists of SAF header and SAF opaque data
- SAF Header: Used by network to identify and forward service advertisements; identifies service type and instance
- SAF Opaque Data: Contains service-specific information; meaningful to SAF Clients but ignored by SAF Forwarders
- SAF Database: Maintained by SAF Forwarders; stores SAF advertisements

The Role of SAF Forwarders

SAF Forwarders run on Cisco IOS routers and switches and are responsible for *receiving services* published by SAF Clients, *distributing the services* reliably throughout the SAF network, and *making the services available* for other interested SAF Clients to use.

The SAF Forwarder Protocol

The SAF Forwarder Protocol (SAF-FP) is used between SAF Forwarders and is responsible for *advertising information about services over IP networks*.

SAF-FP is a "service" advertisement protocol, not an IP routing protocol. It is completely separate and distinct from the underlying IP routing protocol. Networks of SAF Forwarders can run any IP routing protocol they wish (Enhanced Interior Gateway Routing Protocol [EIGRP], Open Shortest Path First [OSPF], Border Gateway Protocol [BGP], and so on).

SAF-FP:

- Uses the EIGRP transport layer for *service advertisement* (does *not* require or rely on EIGRP for IP routing)
- Uses split-horizon and the Diffusing Update Algorithm (DUAL) to prevent service advertisement loops
- Uses link local multicast on LAN and Layer 2 segments for neighbor discovery (IPv4: 224.0.0.10; IPv6: FF02::a)
- Uses IP protocol 88
- Utilizes incremental updates when advertisement changes occur. Does not periodically broadcast/flood service advertisements.

Advertisement changes include service publication, service withdrawal, service updates, connectivity loss or when a new SAF Forwarder comes online.

SAF Neighbor Relationships

SAF Forwarders periodically send hello packets to each other to dynamically discover who their neighbors are and to learn when their neighbors become unreachable or inoperative. SAF Forwarders use link local IP multicast to discover and communicate with other SAF Forwarders on a LAN and can use multicast peer- group or unicast point-to-point peering statements across networks that do not support SAF such as Multiprotocol Label Switching (MPLS) service provider networks or where configuring SAF Transitive Forwarders is prohibitive.

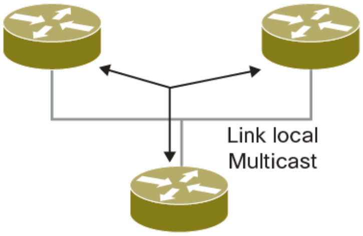
SAF neighbor relationships can be classified further under two categories:

- Layer 2 Adjacent Neighbors
- Nonadjacent Remote Neighbors

Layer 2 Adjacent Neighbors

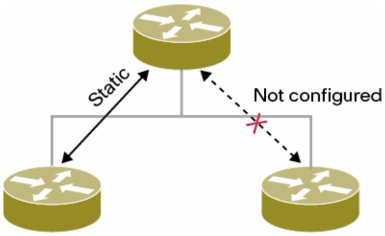
Layer 2 adjacent *dynamic neighbor discovery* relies on link local multicast and occurs automatically on all SAF-enabled interfaces. The link local multicast address is the same used by EIGRP (IPv4: 224.0.0.10, IPv6: FF02::a). (See Figure 2.)

Figure 2. Layer 2 Adjacent Dynamic Neighbor Discovery



Layer 2 adjacent *static configuration* relies on unicast and may be used to prevent dynamic discovery on the same interface. (Figure 3).

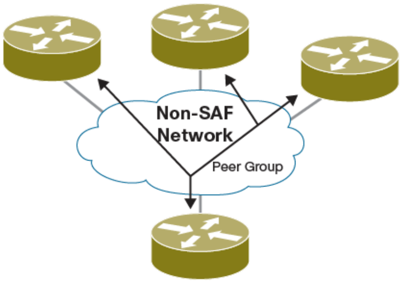
Figure 3. Layer 2 Adjacent Static Configuration



Layer 3 Adjacent Neighbors

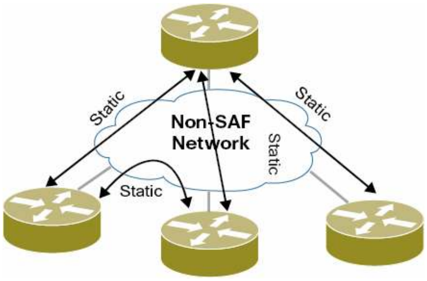
Layer 3 adjacent dynamic discovery requires multicast routing. SAF Forwarders join a common peer group. (Figure 4).

Figure 4. Layer 3 Adjacent Dynamic Neighbor Discovery



Layer 3 adjacent *static configuration* is unicast and configured between each pair of forwarders. (Figure 5).

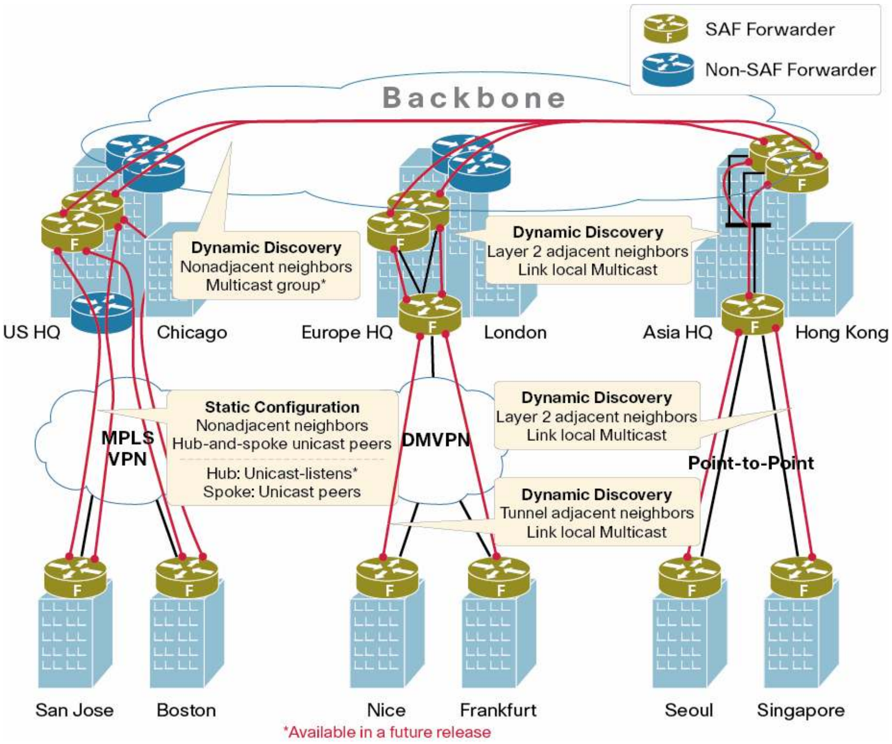
Figure 5. Layer 3 Adjacent Static Configuration



Connecting SAF Forwarders

SAF Forwarders can *dynamically discover other forwarders or be statically configured as neighbors* to exchange service advertisements. (Figure 6).

Figure 6. Connecting SAF Forwarders—Dynamic and Static Neighbor Relationships



Dynamic neighbor discovery is automatically performed over the directly connected interfaces or can be accomplished over a common IP multicast peer group. Dynamic neighbor discovery is the preferred method of connecting SAF Forwarders.

Statically defined neighbors can be used for security purposes or when IP multicast is not available.

In future releases, statically defined neighbors may be defined in such a way that allows for spoke SAF Forwarders to statically establish unicast peerings with hub SAF Forwarders that are configured to “listen” for unicast peerings initiated by spoke SAF Forwarders. This improves overall scalability and simplifies static neighbor configurations for large numbers of nonadjacent SAF neighbors in hub-and-spoke topologies.

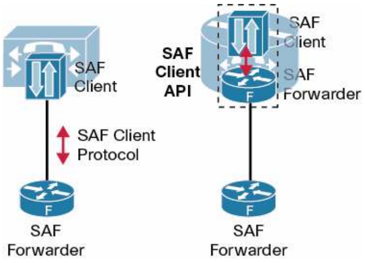
The Role of SAF Clients

A SAF Client can be a *producer of services* (advertises services to the SAF network), a *consumer of services* (requests one or more services from the SAF network), or *both*. SAF Clients perform three basic functions:

- Registering with the SAF network
- Publishing services
- Subscribing to services

SAF Clients take two forms (see Figure 7):

Figure 7. External and Internal SAF Clients



External SAF Clients

External SAF Clients do not reside within the SAF Forwarder. External SAF Clients use the SAF Client Protocol (SAF-CP) to communicate with a SAF Forwarder.

Internal SAF Clients

An internal SAF Client resides on the same platform as the SAF Forwarder. The client/forwarder connection is established through an internal Cisco IOS application programming interface (API).

The SAF Client Protocol

SAF-CP is used between external SAF Clients and SAF Forwarders. SAF Clients initiate a TCP connection to SAF Forwarders. (Figure 8).

Figure 8. SAF Client/Forwarder Connection

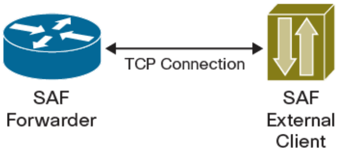
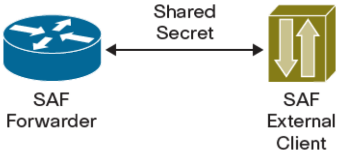
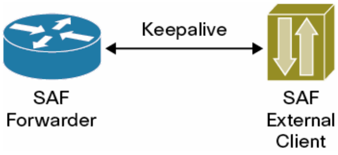


Figure 9. Client/Forwarder Authentication



During the establishment of the TCP connection between an external SAF Client and SAF Forwarder, a shared secret consisting of a username and a password is used for authentication (Figure 9). The username is used as an index to determine which password to use as the shared secret. When a SAF Client sends a request, it sends attributes that include its username, the actual message contents, and an HMAC-SHA1 hash of the username and password with the message contents. When a SAF Forwarder receives a request, it locates the username attribute and uses it to access its local copy of the password. It then computes the HMAC-SHA1 hash using its locally stored password. If the hashes match, the SAF Client is authenticated and the connection proceeds; otherwise, the forwarder will reject the request.

Figure 10. Client/Forwarder Keepalive

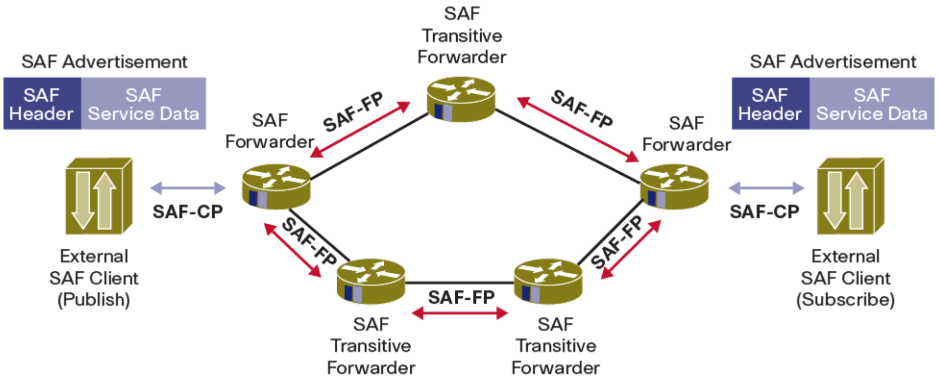


Once a SAF Client has published its services to the SAF network, the SAF Forwarder uses a keepalive mechanism to track the status of the SAF Client (Figure 10). A SAF Forwarder and a SAF Client exchange a keepalive timer value at the time of registration. A SAF Forwarder considers a SAF Client to have failed if it has not seen a request from the SAF Client in a time period equal to the keepalive timer value. A SAF Client ensures that the interval between requests never exceeds this value. If a SAF Client has no data to send, it generates a register message to refresh the timer.

When a SAF Forwarder detects that the SAF Client has gone away, it immediately withdraws the services advertised on behalf of that SAF Client from the network and removes any subscriptions that the SAF Client had established. A SAF Client can be unregistered manually to cause a SAF Forwarder to withdraw all services and subscriptions gracefully.

How Services Are Advertised and Propagated

Figure 11. Advertising and Propagating Services



SAF Clients must register with a SAF Forwarder before publishing, subscribing, withdrawing, or updating service data. When a SAF Forwarder receives a service advertisement published by a SAF Client, the SAF Forwarder stores it in memory then advertises it out all other SAF-enabled interfaces. When a SAF Transitive Forwarder receives the advertisement from the SAF Forwarder, the transitive forwarder advertises a copy to all its other SAF neighbors. Split-horizon and DUAL are used hop by hop to avoid loops and to provide fast convergence. The SAF-FP uses a reliable transport protocol to provide guaranteed, ordered packet delivery. See Figure 11.

The client/forwarder relationship is used to maintain the state of each advertised service. If a client removes a service or disconnects from the SAF Forwarder, the SAF Forwarder informs the rest of the SAF network about the services that are no longer available.

At all times, the nature of the advertised service is “opaque” to the network of SAF Forwarders and only meaningful to SAF Clients.

SAF Service Identifiers

SAF service identifier numbers (service IDs) are used by clients and forwarders to identify and distinguish different services (and their subservices) from one another. This will allow, for example, Unified Communications (UC) clients to send and receive only UC type advertisements. Service IDs must be globally unique within a SAF domain. The service ID takes the following format:

service:sub-service:instance

The *service* field is represented by an integer value in the range 1–65534.

The *sub-service* field is represented by an integer value in the range 1–65534.

The *instance* field is represented by four hexadecimal values each in the range 0x0–0xFFFFFFFF.

An example SAF service is Call Control Discovery (CCD) for Cisco Unified Communications. CCD for Unified Communications uses a SAF Service ID of 101:2:x.x.x.x, where:

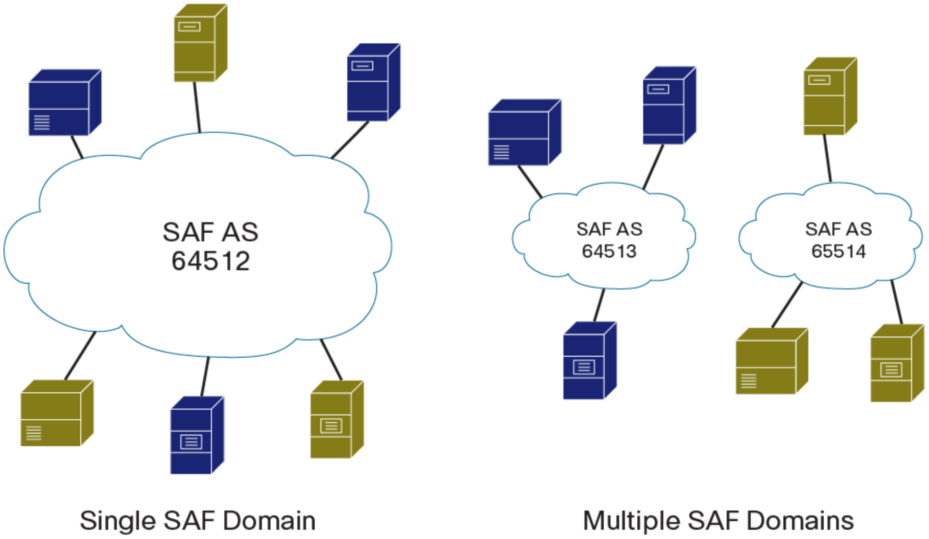
- Service ID 101 = Unified Communications
- Sub-Service ID 2 = CCD
- Instance ID x.x.x.x = ID of Cisco Unified Call Manager cluster (PKID) or Cisco IOS device

SAF Domains

A SAF domain represents the administrative boundary for policies that are common to a group of SAF Forwarders. All SAF Forwarders in the same administrative domain have complete knowledge of the entire domain. SAF domains can be defined for IPv4 or IPv6 transport and are also supported within VPN Routing and Forwarding contexts (VRFs). The terms SAF “domain” and “Autonomous System” (AS) are often used interchangeably.

Typically, a SAF network will utilize a single domain for advertising all services. However, multiple SAF domains may be used if, for example, closed SAF groups are needed to prevent clients from browsing services they are not allowed to access or the number of services within a domain need to be limited for scalability. (Figure 12).

Figure 12. Examples of Single and Multiple SAF Domains



Summary

Cisco® Service Advertisement Framework is a network-based, scalable, bandwidth-efficient approach to service advertisement and discovery. SAF provides a dynamic, network-integrated, real-time messaging mechanism that allows host applications the ability to discover the existence, location, and configuration of networked resources through a local area network (LAN) or across a wide area network (WAN) based on industry-proven Cisco IP routing technology.

Figure 13. SAF Architecture with Unified Communications Call Control Discovery Service

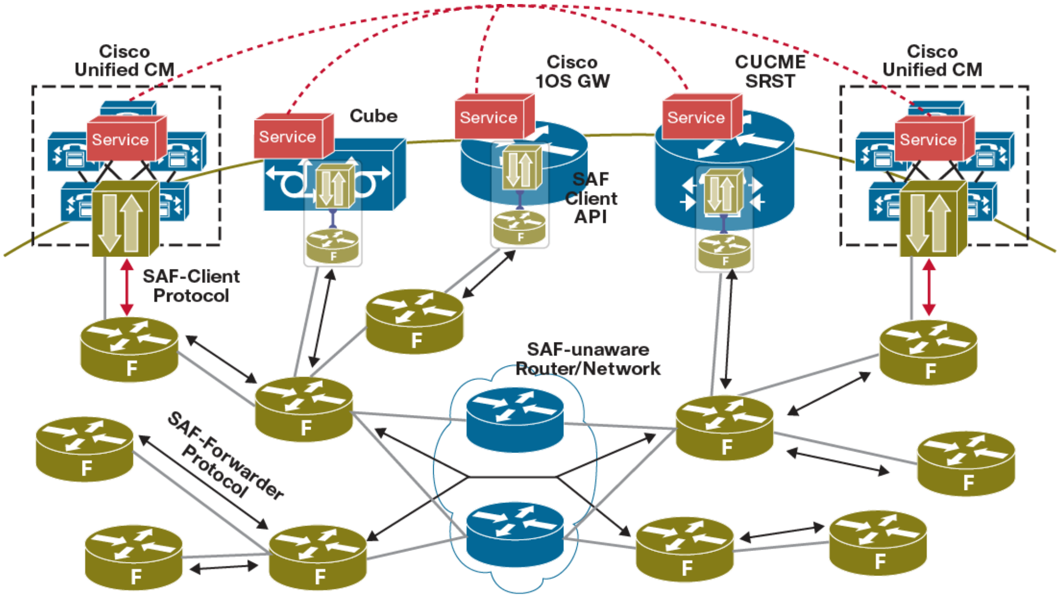


Figure 13 demonstrates how SAF can be used with Unified Communications Call Control Discovery CCD as a service where:

- Cisco Unified Communications Managers are external SAF Clients using SAF-CP to advertise call control information to the SAF network.

- CUBE, Cisco IOS Gateway, and Cisco Unified Communications Manager Express with Survivable Remote Site Telephony are running as internal SAF Clients using the SAF Client API to advertise call control information to the SAF network.

For More Information

For more information on Cisco IOS SAF, refer to http://www.cisco.com/go/saf.

For more information on Cisco IOS SAF configuration, refer to the *Cisco IOS Service Advertisement Framework Configuration Guide*, available at http://www.cisco.com/en/US/docs/ios/saf/configuration/guide/15_0/saf_15_0_book.html.

For more information on Cisco IOS SAF configuration examples on DocWiki, refer to the *Router Configuration Examples*, available at http://docwiki.cisco.com/wiki/Category:Router_Configuration_Examples.

For information on the use of CCD with Cisco SAF, refer to the *Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 8.x* available at http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns818/landing_uc_mgr.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA

C11-622512-00 09/10