Overview of ISA

The Intelligent Service Architecture (ISA) is a core set of Cisco IOS components that combines access, forwarding, and feature-processing capabilities to facilitate a flexible and scalable solution for the management of subscriber sessions at the network edge. A Cisco device running a Cisco IOS image that includes ISA is called an Intelligent Service Gateway (ISG). This document provides information about what ISA is, the benefits of ISA, and how to begin implementing it.

Module History

This module was first published on April 28, 2005, and last updated on April 28, 2005.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all features. To find information about feature support and configuration, use the "Feature Information for the Overview of ISA" section on page 15.

Contents

Information About ISA

This section contains the following concepts:

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

What Is ISA?

ISA is a structured framework in which edge access devices can deliver flexible and scalable services to subscribers. A Cisco device that is running a Cisco IOS image with ISA is called an Intelligent Service Gateway (ISG).

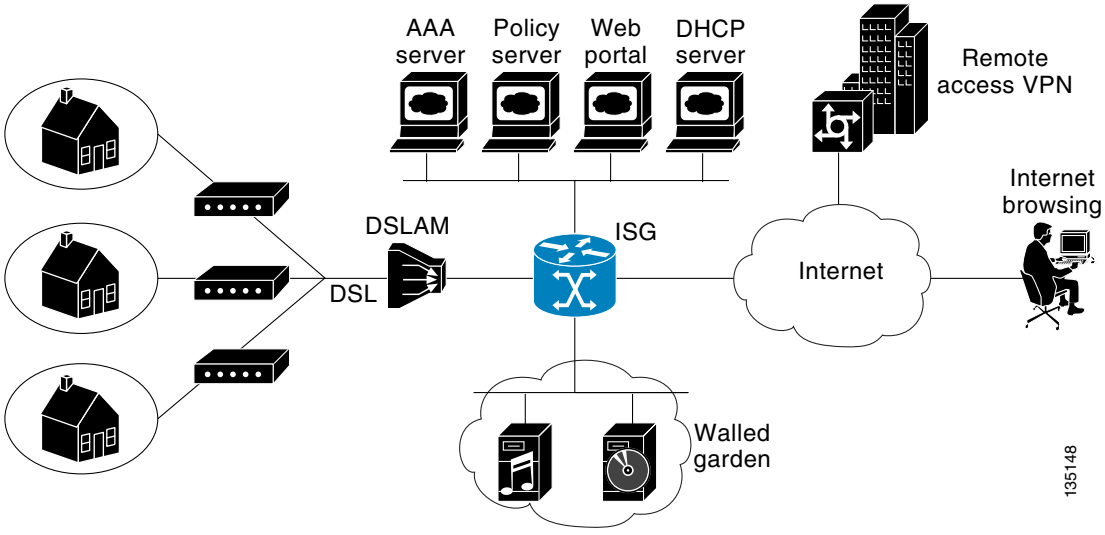
An ISG handles the following key aspects of subscriber management:

- Subscriber identification
- Service and policy determination
- Session policy enforcement
- Session life-cycle management
- Accounting for access and service usage
- Session state monitoring

In addition, ISA introduces a dynamic element to the provisioning and activation of services through control policies and Change of Authorization (CoA) extensions to the RADIUS protocol.

An ISG may be deployed at the access edge and service edge of a network and is applicable to a range of subscriber network environments, such as digital subscriber line (DSL), public wireless LAN (PWLAN), and mobile wireless. Moreover, ISA has been designed to accommodate a flexible distribution of subscriber and service information within a given solution. Figure 1 illustrates a typical DSL deployment for which service profile data may be stored in an authentication, authorization, and accounting (AAA) database and retrieved and cached on demand.

Figure 1 Sample Topology for a DSL Deployment



It is also possible to define services directly on an ISG. In all cases, service activation may be triggered as a result of a locally defined control policy, user profile associations, or CoA commands from an external policy server or portal application.

ISA Principles

Fundamental to the ISA architecture is the provisioning of a common session layer at which the management of generic subscriber sessions is decoupled from the technology that is used to provide access to the edge device.

Within this session management layer, common methods are provided for the extraction of subscriber identity information and the determination and activation of services. These methods are described in the following sections:

Subscriber Sessions

An ISA subscriber session is a generic system context that is created for every subscriber who interacts with the edge device. A subscriber session is created on first interaction so that policies may be applied as early as possible. Such policies may facilitate the retrieval of subscriber identity information. All subscriber sessions are assigned a locally unique identifier that may subsequently be used to reference the session.

The session context is the basis for common handling at the session management layer, but the type of traffic that is encompassed in a session context may vary. Broadly, session types may be categorized as Layer 2 or Layer 3, depending on the packet types that are being handled by the session. For instance, a PPP session is a Layer 2 session in that it includes all packets transferred over a link that was established using PPP negotiation. An IP session is Layer 3 because it includes all IP packets exchanged with a subscriber device at a single IP address. Whether a session is Layer 2 or Layer 3 will, to some extent, influence the type of polices that may be activated for the session.

ISA also provides flexibility in terms of how an IP session is defined for an interface. For example, on a particular interface, ISA can be provisioned to classify IP sessions on the basis of a single address (an IP session), a subnet (an IP subnet session), or the interface itself (an IP interface session), wherein all IP packets transferred over the interface are encompassed by the same session.

In a network deployment, ISA session types should be provisioned to represent individual subscriber entities. For example, a particular ISG interface may be directly connected to a subscriber household in which multiple subscriber devices with individual IP addresses are attached to a household LAN. If the plan is to model each LAN-attached device as a separate subscriber and apply different policies and services to each, the interface should be provisioned to expect IP sessions. However, if the household represents a single subscriber account and common handling is required for all packets exchanged, the interface should be provisioned as an IP interface or subnet session.

Subscriber Access

Under ISA, the provisioning and handling of specific access media and protocols is decoupled as far as possible from the functionality that is applicable to all session types. This model has the following benefits:

- A common set of subscriber services may be used on an ISG at which heterogeneous subscriber networks are aggregated.
- A common set of subscriber services may be used for multiple ISGs, even when the access technology differs.
- For a given subscriber, the access method may be altered (through provisioning or roaming) without any need to change the service provisioning.
- As new access protocols become available, they can be leveraged by existing edge deployments without requiring changes to the service content; new access protocols "plug in" to the ISA framework.

Subscriber Identification

A subscriber session is created when the first control protocol packet is received from the subscriber device. The control protocol will vary depending on the session type. If there is no control protocol, the session is signaled by the first data packet from the subscriber.

At session start, certain identity information is available, although typically not enough to completely identify the subscriber. Through the use of control policies, the identity information available at session start can be used to drive the extraction of further identity from the subscriber and determine new policy for the session. The following examples illustrate how an ISG might handle subscriber identity:

- When the subscriber access protocol is PPPoA, the ATM virtual connection on which the call request arrived is available at session start. A control policy could be defined to forward all sessions on virtual path identifier (VPI) 1 over the tunnel defined by service "ISP-A" but to request a username from all subscribers attempting to access the network via VPI 2.
- For an IP session, where session start is signaled by a DHCP protocol event, a TCP redirection policy could be activated. This policy would facilitate the collection of a username and credential at an external web portal.

Subscriber Services

An ISA service is a collection of policies applicable to a subscriber session. When a service is activated on a session, all policies contained within that service are activated on the session. Likewise, when a service is deactivated, all policies that are contained within the service are deactivated or removed from a session.

Services are useful for handling fixed policy combinations that are applicable to multiple subscribers. This application reduces duplication of persistent data and allows a group of policies to be activated with a single action and a single reference.

A service may be defined on the edge device directly, through the command-line interface (CLI), or in an external repository and downloaded as required. A downloaded service definition is cached on the device for as long as it is active on one or more sessions.

A service may be activated in one of the following ways:

- As a result of control policy execution
- When a CoA service-logon command is received

- By reference in a user profile, where the service is flagged for automatic activation

Services primarily contain traffic policies. There are some restrictions regarding the policies that may be combined in a given service; for example, a service may not contain two traffic policies that specify a different nondefault traffic class unless they apply to different traffic directions (inbound versus outbound).

Where a service contains a network-forwarding policy, it is known as a *primary service*. Only one primary service may be active for a given session at any point in time; that is, primary services are mutually exclusive.

Policies

ISA introduces support for two basic policy types:

- Traffic policies
- Control policies

Traffic policies define the handling of data packets and consist of a traffic class, which defines the packet-based criteria for which the policy is applicable, and one or more traffic actions, which are functional instances that perform specific operations on a data stream and are often referred to as *features*. The traffic actions configured within a traffic policy are invoked for data packets that meet the criteria defined by the traffic class.

Network-forwarding policies are a specific type of traffic policy, for which the action is a network-forwarding action, such as to route packets using a specific virtual routing and forwarding instance (VRF) or forward packets over a Layer 2 connection. Network-forwarding policies are "classless" in that it is not possible to refine the criteria for which the forwarding action is applicable.

Control policies define the handling of system events and consist of one or more control policy rules and a decision strategy that governs how the constituent policy rules are evaluated. A control policy rule consists of a control class (a flexible condition clause), an event for which the condition is evaluated, and one or more control actions. Control actions are general system functions, such as "authenticate" or "activate a service."

Control policies may be activated on various targets, such as interfaces or ATM virtual circuits (VCs), and typically control the extraction and authentication of subscriber identity and the activation of services on sessions. Traffic policies may be activated only on sessions and are typically (though not always) applied through service activation.

Control policies are a structured replacement for feature-specific configuration commands and allow configurable functionality to be expressed in terms of an event, a condition, and an action. Control policies represent an intuitive and extensible framework for specifying system behavior. As additional functionality is added to the system, an administrator just has to learn what new events and actions can be included in a control policy, not a completely new set of configuration commands.

Dynamic Policy Updates

Traditionally, subscriber policy has been determined at one point only, at session establishment time, once the principal identity of a subscriber has been authenticated. ISA introduces a dynamic policy model in which session policy may be altered at any time.

Session policy is evaluated at session start and may be reassessed whenever additional identity or service selection information is gleaned from the subscriber via the access protocol. In addition, policy may be updated for a session through the activation of control policies or by means of CoA commands from an

external application. In the latter case, the external application may update policy as a result of administrator activity, back-end processing, or subscriber activity (such as service selection at a web portal).

Benefits of ISA

ISA provides the following benefits:

- A common system for session management across Cisco products and access technologies. New access protocols, forwarding protocols, and features may be "plugged in" with minimal impact and maximum potential for reuse.
- Separation of the concerns of subscriber identification, service application, and subscriber access and session type.
- Flexible session definitions.
- Flexible session detection.
- Flexible, iterative approach to identification and service and policy activation.
- Different trust levels. Session authorization is not contingent on authentication.
- Control policies. Control policies facilitate distributed policy decision-making, reducing round-trip latency between the edge device and policy server, and allow system event handling to be described in a consistent and intuitive manner.
- Common policy model and language for control and traffic policy.
- Provision for dynamic policy updates via CoA (through service activation or "policy push").
- Use of existing Cisco IOS infrastructure to provide session functionality.
- Use of existing Cisco IOS infrastructure to track session state and life cycle.
- Creation of a session context at first instance of subscriber interaction, thereby facilitating the immediate application of policy to subscriber traffic.
- Flexible distribution of service data.
- Range of accounting options, including prepaid accounting, postpaid accounting, tariff-switching for prepaid and postpaid accounting, interim accounting, event-based accounting, and flow-based accounting.
- Single sign-on services to an external application.
- Flexible infrastructure in support of "equal-access" deployments, such as service-based Dynamic Host Configuration Protocol (DHCP) pool and DHCP server determination, dynamic readdressing through DHCP, and VRF transfer.
- Support for standard external interfaces, such as RADIUS and CoA.

Planning for ISA Implementation

ISA is very flexible and supports a wide variety of functionality. Before you begin to configure ISA, you should plan your system carefully. The following sections describe some of the important aspects of your system that you should consider:

- Trust Model, page 13
- Subscriber Access Model, page 13

Trust Model

Trust levels are determined by the security needs of a particular application domain and the inherent security afforded by the subscriber network. In the following situations, it may not be necessary to authenticate subscriber identity:

- When security is not considered paramount
- When end-to-end security is provided in-band
- When the subscriber network is intrinsically secure

Whether or not subscribers must be authenticated will influence the choice of access protocol. When authentication is not required, control policies may be used to determine authorization and other session policy on the basis of subscriber identity.

Where authentication is considered necessary, the authenticated identity may be trusted:

- For the duration of the session
- Until a periodic reauthentication is instigated
- Beyond the duration of a session; for example, for the lifetime of a subscription

For complete security, cryptographic methods may be used to secure the session (to the edge) following authentication, obviating the need for reauthentication. However, there are administrative and performance overheads associated with this practice.

Subscriber Access Model

The trust model will, to a large extent, influence the choice of access protocol. However, the access model will also depend on other factors such as the underlying media (for example, ATM versus Ethernet), type of endpoint (for example, PC, cell phone, PDA), mobility requirements, ability to influence the software installed on a subscriber device, and scalability requirements.

Single Sign-On Requirements

Where a subscriber will have access to services provided by other devices in the administrative domain of the access or service provider, is an additional authentication required, or should the identity of the subscriber be trusted? It may be necessary for the latter device to query the access device to collect additional subscriber identity information and ascertain whether the subscriber has already been authenticated by the access device. The single sign-on facility is provided through the “session query” capability of CoA.

Network Forwarding

How should subscribers be given access to network services? Network forwarding options include the following:

- Layer 2 connections; for example, a Layer 2 Tunneling Protocol (L2TP) tunnel to an L2TP network server (LNS)
- Layer 3 connections, by associating all session packets with a particular VRF or routing domain

Service Packaging

How should subscriber policies be organized into services, if at all? Some considerations for service packaging include the following:

- Are certain policy combinations common to multiple subscribers?
- Are shared policy combinations dependent on a particular forwarding domain?
- Is it necessary for a subscriber to move between service domains?
- Should services be defined on the device or in a remote repository? Externally defined services will be cached locally for as long as they are activated for one or more sessions.

Billing Model

How should subscribers be billed for service usage? Billing options include the following:

- Billing by usage of time or volume
- Billing in advance (prepaid) or at regular intervals (traditional postpaid)
- Billing according to policies provisioned for the session
- Billing according to the time of day (tariff switching)

Where to Go Next

To configure ISA, see the following modules:

- Configuring ISA Control Policies—Provides information about how to configure ISA control policies, which define the actions the system will take in response to specific condition and events.
- Configuring ISA Layer 2 Access—Provides information about how to configure policies for ISA Layer 2 session handling.
- Configuring ISA Layer 3 Access—Provides information about how to configure ISA to bring up IP sessions and policies for identifying and authorizing IP sessions; specifically, Layer 4 redirection for unauthenticated subscribers, port-bundle host key functionality, and transparent autologon.
- Managing ISA Subscriber IP Addresses—Provides information about how to manage the assignment of ISA subscriber IP addresses.
- Enabling ISA to Interact with External Policy Servers—Provides information about configuring ISA to retrieve policies from an external policy server or for a policy server to dynamically update session policies.
- Configuring ISA Subscriber Services—Provides information about how ISA subscriber services work, how to configure services and traffic classes that can be applied to services, and how to activate services.
- Configuring ISA Network Forwarding Policies—Provides information about how to configure network policies, which allow packets to be routed or forwarded to and from an upstream network.

- Configuring ISA Accounting—Provides information about how to configure ISA accounting, including per-session and per-service accounting, broadcast accounting, and postpaid tariff switching.
- Configuring ISA Support for Prepaid Billing—provides information about how to configure ISA support for prepaid billing, including prepaid idle timeout and prepaid tariff switching.
- Configuring Policies for Session Maintenance—Provides information about how to configure ISA session and idle timeouts.
- Redirecting Subscriber Traffic Using ISA Layer 4 Redirect—Provides information about how to redirect subscribers' Layer 4 traffic to facilitate subscriber authentication, initial and periodic advertising captivation, redirection of application traffic, and DNS redirection.
- Configuring ISA Policies for Regulating Network Access—Provides information about the following methods of regulating session bandwidth and network access: Modular quality of service (QoS) CLI policies, Dynamic Subscriber Bandwidth Selection (DBS), per-subscriber firewalls, and ISA policing.
- Configuring ISA VRF Transfer—Provides information about how to configure VRF transfer, which enables an ISA subscriber session to move from one virtual routing or forwarding instance (VRF) to another following selection of a new primary service.
- Troubleshooting ISA with Session Monitoring and Distributed Conditional Debugging—Provides information about how to use conditional debugging to facilitate debug filtering for ISA.

Additional References

The following sections provide references related to ISA.

Related Documents

Related Topic	Document Title
ISA commands	*Cisco IOS Intelligent Service Architecture Command Reference*

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for the Overview of ISA

Table 2 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(27)SBA or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation.

For information on a feature in this technology that is not documented here, see the "Intelligent Service Architecture Features Roadmap."

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2 Feature Information for the Overview of ISA

Feature Name	Releases	Feature Configuration Information
ISA:Session: Auth: Single Sign-on	12.2(27)SBA	Single sign-on eliminates the need to authenticate a session more than once when a subscriber has access to services provided by other devices in the administrative domain of the access or service provider. The following sections provide information about this feature: • Planning for ISA Implementation, page 12

This module first published April 28, 2005. Last updated April 28, 2005.