Configuring ISA Layer 3 Access

The Intelligent Service Architecture (ISA) is a core set of Cisco IOS components that provide 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). This module contains information on how to configure ISA to bring up IP interface sessions, IP sessions based on source IP address, and IP subnet sessions. This module also describes how to configure policies for identifying and authorizing IP sessions; specifically, Layer 4 redirection for unauthenticated subscribers, port-bundle host key functionality, and transparent autologon.

Module History

This module was first published on April 11, 2005, and was last updated April 11, 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 Configuring ISA Layer 3 Access" section on page 69.

Contents

CISCO SYSTEMS

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

Restrictions for Configuring Layer 3 Access

Overlapping static IP subscribers are not supported.

Overlapping IP subscribers in different virtual routing and forwarding instances (VRFs) are not supported on the same interface.

IP interface sessions can be created only through static command-line interface (CLI) provisioning.

Information About ISA Layer 3 Access

Before you configure ISA Layer 3 access, you should understand the following concepts:

- Supported Types of Layer 3 Sessions, page 48
- IP Session Creation, page 49
- IP Session Termination, page 49
- Default Services for IP Sessions, page 50

Supported Types of Layer 3 Sessions

ISA supports three types of layer 3 sessions:

- IP interface sessions
- IP sessions
- IP subnet sessions

IP Interface Sessions

An IP interface session includes all IP traffic received on a specific physical or virtual interface. IP interface sessions are provisioned through the CLI; that is, a session is created when the IP interface session commands are entered.

IP interface sessions might be used in situations in which a subscriber is represented by an interface (with the exception of PPP) and communicates using more than one IP address. For example, a subscriber using routed bridge encapsulation (RBE) access might have a dedicated ATM virtual circuit (VC) to home customer premises equipment (CPE) that is hosting multiple PCs.

IP Sessions

An IP session includes all the traffic that is associated with a single subscriber IP address. If the IP address is not unique to the system, other distinguishing characteristics such as VRF or MAC address form part of the identity of the session. An ISG can be configured to create IP sessions upon receipt of Dynamic Host Configuration Protocol (DHCP) packets and unknown IP source addresses. See the "IP Session Creation" section on page 49 for more information.

IP sessions may be hosted for a connected subscriber device (one routing hop from the ISG) or one that is multiple hops from the gateway.

IP Subnet Sessions

An IP subnet session represents all the traffic that is associated with a single IP subnet. IP subnet sessions are used to apply uniform edge processing to packets associated with a particular IP subnet.

Like an IP session, an IP subnet session may be hosted whether it is directly connected or it is multiple hops from the gateway.

IP subnet sessions are created the same way as IP sessions, except that when a subscriber is authorized or authenticated and the Framed-IP-Netmask attribute is present in the user or service profile, the ISG converts the source-IP-based session into a subnet session with the subnet value in the Framed-IP-Netmask attribute.

Note Where an ingress interface maps to a single subnet, the subnet might be accommodated with an IP interface session. However, if the ISG is more than one hop away from a subscriber, and there is the possibility that multiple subnets are accessible through the same interface, IP subnet sessions may be defined to distinguish the traffic and apply appropriate edge functionality to each subnet.

IP Session Creation

The following events may be used to signal the start of an IP session or IP subnet session:

- DHCP Discover packet

  If the following conditions are met, receipt of a DHCP Discover packet will trigger the creation of an IP session:

  - The ISG serves as a DHCP relay or server for new IP address assignments.
  - Subscribers are configured for DHCP.
  - The DHCP Discover packet is the first DHCP request received from the subscriber.

- Unrecognized source IP address

  In the absence of a DHCP DISCOVER packet, a new IP session is triggered by the appearance of an IP packet with an unrecognized source IP address.

IP Session Termination

An IP session may be terminated in one of the following ways:

- DHCP Lease Expiry or DHCP Release from client

  If DHCP is used to detect a new session, its departure may also be signaled by a DHCP event.

- Application stop

  An application command that is used to terminate the session. The application stop command is typically used to terminate the session when a subscriber initiates an account logoff from a Web portal. An application stop may also result from the actions of an administrator, such as action taken in response to rogue behaviour from a subscriber.

- Idle timeout and session timeout

  Idle timeouts and session timeouts can be used to detect or impose termination of an IP session.

Default Services for IP Sessions

Newly created IP sessions may require a default service to allow subsequent subscriber packets to be processed appropriately; for example, to permit or force TCP packets to a captive portal where menu-driven authentication and service selection can be performed. A default service policy map or service profile may be configured for IP sessions to redirect traffic, enable port-bundle host-key functionality for session identification, or enable transparent autologon. A default service would also likely include a network service, typically a VRF, so that subscriber packets may be routed or forwarded.

How to Configure ISA Layer 3 Access

The first task is required to configure ISA Layer 3 access. The last three tasks are optional and configure policies for the identification and authorization of IP sessions.

- Bringing Up Layer 3 Sessions, page 50
- Configuring Layer 4 Redirect for Unauthenticated Subscribers, page 53
- Configuring ISA Port-Bundle Host Key, page 56
- Configuring ISA Transparent Autologon, page 63

Bringing Up Layer 3 Sessions

An ISG creates IP sessions for IP traffic on subscriber-side interfaces. The following tasks enable IP sessions on the interface and indicate how a session will be identified. Perform one or both of the following tasks to bring up Layer 3 ISA sessions:

- Creating an IP Interface Session, page 50
- Creating IP Subscriber Sessions, page 51

Creating an IP Interface Session

An ISA IP interface session encompasses all IP packets that cross the specified interface or subinterface. Perform this task to create an ISA IP interface session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip subscriber**
5. **identifier interface**
6. **end**
7. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** interface-*type* *interface-number*[**.***subinterface-number*] **Example:** `Router(config)#`	Specifies an interface or subinterface and enters interface configuration mode.
Step 4	**ip subscriber** **Example:** `Router(config-if)# ip subscriber`	Enables ISA IP subscriber configuration mode.
Step 5	**identifier interface** **Example:** `Router(config-subscriber)# identifier interface`	Creates an ISA IP interface session.
Step 6	**end** **Example:** `Router(config-subscriber)# exit`	(Optional) Returns to privileged EXEC mode.
Step 7	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*] **Example:** `Router# show subscriber session detailed`	Displays ISA subscriber session information. • Use this command to verify session creation.

Creating IP Subscriber Sessions

Perform this task to enable ISA to create an IP session or IP subnet session when it receives a DHCP DISCOVER packet or an IP packet from an unrecognized source IP address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip subscriber**
5. **identifier ip src-addr** [**match** *access-list-number*]

6. **initiator dhcp** [**class-aware**]
7. **end**
8. Add the Framed-IP-Netmask attribute to the service or user profile.
9. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*]
10. **show ip subscriber** [**vrf** {*vrf-name* | **global**}]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)#`	Specifies an interface and enters interface configuration mode.
Step 4	**ip subscriber** **Example:** `Router(config-if)# ip subscriber`	Enables ISA IP subscriber configuration mode.
Step 5	**identifier ip src-address** [**match** *access-list-number*] **Example:** `Router(config-subscriber)# identifier ip src-address`	Configures ISA to create an IP session upon detection of the first IP packet from an unidentified subscriber. • The **match** *access-list-number* option causes IP sessions to be created only for subscriber traffic matching the access list.
Step 6	**initiator dhcp** [**class-aware**] **Example:** `Router(config-subscriber)# initiator dhcp`	Configures ISA to create IP sessions upon receipt of DHCP DISCOVER packets. • The **class-aware** keyword allows ISA to influence the IP address assigned by DHCP by providing DHCP with a class name. • IP subnet sessions cannot be created for DHCP-initiated sessions.
Step 7	**end** **Example:** `Router(config-subscriber)# end`	(Optional) Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 8	Add the Framed-IP-Netmask attribute to the service or user profile.	(Optional) Enables an IP subnet session for the subscriber. • When a subscriber is authorized or authenticated and the Framed-IP-Netmask attribute is present in the user or service profile, ISA converts the source-IP-based session into a subnet session with the subnet value in the Framed-IP-Netmask attribute.
Step 9	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*] **Example:** `Router# show subscriber session detailed`	(Optional) Displays ISA subscriber session information. • Use this command to verify session creation.
Step 10	**show ip subscriber** [**vrf** {*vrf-name* | **global**}] **Example:** `Router# show ip subscriber vrf global`	(Optional) Displays information about ISA subscriber IP sessions. • Use this command to display the IP sessions on the ISG.

Configuring Layer 4 Redirect for Unauthenticated Subscribers

Before you configure Layer 4 redirect for unauthenticated subscribers, you should understand the following concept:

- Unauthenticated Layer 4 Redirect, page 53

Note The following sections show one way to redirect the Layer 4 traffic of unauthenticated subscribers. For more information about ISA Layer 4 redirect functionality, see the module "Redirecting Subscriber Traffic Using ISA Layer 4 Redirect".

Perform the following tasks to configure Layer 4 redirect for unauthenticated subscribers:

- Configuring L4 Redirection in a Service Policy Map, page 53
- Configuring a Control Policy for Unauthenticated Layer 4 Redirect, page 55

Unauthenticated Layer 4 Redirect

The ISA Layer 4 Redirect feature redirects specified TCP or User Datagram Protocol (UDP) packets to servers that have been configured to handle the packets in a specific manner. Unauthenticated Layer 4 redirect is one application of the ISA Layer 4 Redirect feature. Typically, unauthenticated Layer 4 redirect is configured to redirect the TCP traffic of unauthenicated subscribers to a web portal where subscribers can log in and the authentication process can begin.

Configuring L4 Redirection in a Service Policy Map

Perform this task to configure ISA Layer 4 redirection in a service policy map on the router.

The ISA Layer 4 Redirect feature can also be configured in a service profile on a AAA server. For more information about redirecting Layer 4 subscriber traffic, see the module "Redirecting Subscriber Traffic Using ISA Layer 4 Redirect."

Prerequisites

The ISA Layer 4 Redirect feature is configured under a traffic class within the service policy map. This task assumes that you have defined the traffic class map. See the module "Configuring ISA Subscriber Services" for more information.

Traffic can be redirected to a server or server group. If you are redirecting traffic to a server group, this task assumes that the server group has been configured. See the module "Redirecting ISA Subscriber Traffic" for more information about configuring server groups.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **class type traffic** *class-name*
5. **redirect to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]} [**duration** *seconds*] [**frequency** *seconds*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service web_portal_redirect`	Creates or defines a service policy map, which is used to define an ISA service.
Step 4	**class type traffic** *class-name* **Example:** `Router(config-service-policymap)# class type traffic TCP_redirect`	(Optional) Associates a previously configured traffic class to the policy map.
Step 5	**redirect to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]} [**duration** *seconds*] [**frequency** *seconds*] **Example:** `Router(config-service-policymap-class-traffic)# redirect to group web_portal`	Redirects Layer 4 traffic to a specified server or server group.

Configuring a Control Policy for Unauthenticated Layer 4 Redirect

Perform this task to configure a control policy that will apply a service configured with Layer 4 redirect at the start of every session. The service is unapplied once the subscriber has been authenticated and account logon has occurred.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-name*
4. **class type control always event session-start**
5. *action-number* **service-policy type service** *policy-map-name*
6. **exit**
7. **class type control always event account-logon**
8. *action-number* **service-policy type service unapply** *policy-map-name*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control** *policy-name* **Example:** `Router(config)# policy-map type control unauth_rdt`	Creates or modifies a control policy map, which is used to define a control policy.
Step 4	**class type control always event session-start** **Example:** `Router(config-control-policymap)# class type control always event session-start`	Specifies a control class that will always evaluate true and be activated at session start.
Step 5	*action-number* **service-policy type service** *policy-map-name* **Example:** `Router(config-control-policymap-class-control)# 1 service-policy type service web_portal_redirect`	Applies the specified service policy map. • The *policy-map-name* should reference the service policy map configured with Layer 4 redirect. • This action redirects the Layer 4 traffic of unauthenticated subscribers.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-control-policymap-class-control)# exit`	Returns to control policy map configuration mode.
Step 7	**class type control always event account-logon** **Example:** `Router(config-control-policymap)# class type control always event account-logon`	Specifies a control class that will always evaluate true and will be activated at account logon.
Step 8	*action-number* **service-policy type service unapply** *policy-map-name* **Example:** `Router#(config-control-policymap-class-control) # 1 service-policy type service unapply web_portal_redirect`	Removes the specified service policy map. • The *policy-map-name* should reference the service policy map that was configured with Layer 4 redirect. • This action removes the Layer 4 redirection once the subscriber has been authenticated.
Step 9	**end** **Example:** `Router#(config-control-policymap-class-control) end`	(Optional) Returns to privileged EXEC mode.

What to Do Next

You must apply the control policy to a context by using the **service-policy type control** command. For information about applying control policies, see the module "Configuring ISA Control Policies."

Configuring ISA Port-Bundle Host Key

Before you configure the ISA Port-Bundle Host Key feature, you should understand the following concepts:

- Overview of ISA Port-Bundle Host Key, page 57
- Port Bundle Host Key Mechanism, page 57
- Benefits of ISA Port-Bundle Host Key, page 58
- Prerequisites for the ISA Port-Bundle Host Key Feature, page 58
- Restrictions for the ISA Port-Bundle Host Key Feature, page 59

Perform the following tasks to configure the ISA Port-Bundle Host Key feature:

- Enabling the ISA Port-Bundle Host Key Feature in a User or Service Profile on the AAA Server, page 60
- Enabling the ISA Port-Bundle Host Key Feature in a Service Policy Map, page 59
- Configuring Port-Bundle Host Key Parameters, page 61
- Verifying ISA Port-Bundle Host Key Configuration, page 62

Overview of ISA Port-Bundle Host Key

The ISA Port-Bundle Host Key feature serves as an in-band signaling mechanism for session identification at external portals. TCP packets from subscribers are mapped to a local IP address for the ISA gateway and a range of ports. This mapping allows the portal to identify the ISA gateway from which the session originated. The mapping also identifies sessions uniquely even when subscribers have overlapping IP addresses. The ISA Port-Bundle Host Key feature enables a single portal to be deployed for multiple VRFs even when there are subscribers with overlapping IP addresses.

Port Bundle Host Key Mechanism

With the ISA Port-Bundle Host Key feature, an ISG performs Port-Address Translation (PAT) and Network Address Translation (NAT) on the TCP traffic between the subscriber and the portal. When a subscriber TCP connection is set up, the ISG creates a port mapping that changes the source IP address to a configured ISA IP address and changes the source TCP port to a port allocated by the ISG. The ISG assigns a bundle of ports to each subscriber because one subscriber can have several simultaneous TCP sessions when accessing a web page. The assigned *port-bundle host key*, or combination of port bundle and ISA source IP address, uniquely identifies each subscriber. The host key is carried in RADIUS packets sent between the portal server and the ISG in the Subscriber IP vendor-specific attribute (VSA). Table 5 describes the Subscriber IP VSA. When the portal server sends a reply to the subscriber, the ISG reverse translates the destination IP address and destination TCP port according to the translation tables.

Table 5 Subscriber IP VSA Description

Attribute ID	Vendor ID	Subattribute ID and Type	Attribute Name	Attribute Data
26	9	250 Account-Info	Subscriber IP	S<subscriber-ip-address>[:<port-bundle-number>] • S—Account-Info code for subscriber IP. • <subscriber IP address>:<port-bundle number>—The port-bundle number is used only if the ISA Port-Bundle Host Key feature is configured.

For each TCP session between a subscriber and the portal, the ISG uses one port from the port bundle as the port map. Individual port mappings are flagged as eligible for reuse on the basis of inactivity timers, but are not explicitly removed once assigned. The number of port bundles is limited per ISA address, but , but there is no limit to the number of ISA IP addresses that can be configured for port bundle usage.

Port-Bundle Length

The port-bundle length is used to determine the number of ports in one bundle. By default, the port-bundle length is four bits. The maximum port-bundle length is ten bits. See Table 2 for available port-bundle length values and the resulting port-per-bundle and bundle-per-group values. You may want to increase the port-bundle length when you see frequent error messages about running out of ports in a port bundle.

Table 6 Port-Bundle Lengths and Resulting Port-per-Bundle and Bundle-per-Group Values

Port-Bundle Length (in bits)	Number of Ports per Bundle	Number of Bundles per Group (and per ISA Source IP Address)
0	1	64512
1	2	32256
2	4	16128
3	8	8064
4 (default)	16	4032
5	32	2016
6	64	1008
7	128	504
8	256	252
9	512	126
10	1024	63

Note For each portal server, all connected ISAs must have the same port-bundle length, which must correspond to the configured value given in the portal server's BUNDLE_LENGTH argument. If you change the port-bundle length on an ISA, be sure to make the corresponding change in the configuration on the portal.

Benefits of ISA Port-Bundle Host Key

Support for Overlapped Subscriber IP Addresses Extended to Include External Portal Usage

The ISA Port-Bundle Host Key feature enables external portal access regardless of subscriber IP address or VRF membership. Without the use of port-bundle host keys, all subscribers accessing a single external portal must have unique IP addresses. Furthermore, since port-bundle host keys isolate VRF-specific addresses from the domain in which the portal resides, routing considerations are simplified.

Portal Provisioning for Subscriber and ISA IP Addresses No Longer Required

Without the ISA Port-Bundle Host Key feature, a portal must be provisioned for subscriber and ISA IP addresses before the portal is able to send RADIUS packets to the ISG or send HTTP packets to subscribers. The ISA Port-Bundle Host Key feature eliminates the need to provision a portal in order to allow one portal server to serve multiple ISGs and to allow one ISG to be served by multiple portal servers.

Prerequisites for the ISA Port-Bundle Host Key Feature

The external portal must support port-bundle host keys and must be configured with the same port-bundle host key parameters.

Restrictions for the ISA Port-Bundle Host Key Feature

The following restrictions apply to the ISA Port-Bundle Host Key feature:

- The ISA Port-Bundle Host Key feature must be separately enabled at the portal and at all connected ISAs.
- All ISA source IP addresses configured with the **source** command must be routable in the management network where the portal resides.
- For each portal server, all connected ISAs must have the same port-bundle length.
- The ISA Port-Bundle Host Key feature uses TCP. Packets will not be mapped for asubscriber who is not sending TCP traffic.
- Specifying the Port-Bundle Host Key feature in a user profile will work only when the user profile is available prior to the arrival of IP packets; for example, for PPP sessions or for DHCP-initiated IP sessions with transparent autologon.

Enabling the ISA Port-Bundle Host Key Feature in a Service Policy Map

Perform this task to enable the ISA Port-Bundle Host Key feature in a service policy map. The ISA Port-Bundle Host Key feature will be applied to any subscriber whos uses this service policy map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-name*
4. **ip portbundle**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-name* **Example:** `Router(config)# policy-map type service service1`	Creates or defines a service policy map, which is used to define an ISA service.
Step 4	**ip portbundle** **Example:** `Router(config-service-policymap)# ip portbundle`	Enables the ISA Port-Bundle Host Key feature for the service.
Step 5	**end** **Example:** `Router(config-service-policymap)# end`	(Optional) Returns to privileged EXEC mode.

What to Do Next

You may want to configure a method of activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISA Subscriber Services."

Enabling the ISA Port-Bundle Host Key Feature in a User or Service Profile on the AAA Server

Perform this task to enable the ISA Port-Bundle Host Key feature in a user profile or service profile on the AAA server.

SUMMARY STEPS

1. Add the Port-Bundle Host Key attribute to the user or service profile.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Add the Port-Bundle Host Key attribute to the user or service profile. 26,9,1 = "ip:portbundle=enable"	Enables the ISA Port-Bundle Host Key feature in the user or service profile.

What to Do Next

If you enabled the ISA Port Bundle Host Key feature in a service profile, you may want to configure a method of activating the service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISA Subscriber Services."

Configuring Port-Bundle Host Key Parameters

Perform this task to configure ISA Port-Bundle Host Key parameters and specify the interface for which ISA will reverse translate the IP address and port number for downstream traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip portbundle**
4. **match access-list** *access-list-number*
5. **length** *bits*
6. **source** *interface-type interface-number*
7. **exit**
8. **interface** *type number*
9. **ip portbundle outside**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip portbundle** **Example:** `Router(config)# ip portbundle`	Enters IP portbundle configuration mode.
Step 4	**match access-list** *access-list-number* **Example:** `Router(config-portbundle)# match access-list 101`	Specifies packets for port-mapping by specifying an access list to compare against the subscriber traffic.

	Command or Action	Purpose
Step 5	**length** *bits* **Example:** `Router(config-portbundle)# length 5`	Specifies the ISA port-bundle length, which determines the number of ports per bundle and bundles per group. • The default is 4.
Step 6	**source** *interface-type interface-number* **Example:** `Router(config-portbundle)# source ethernet 0/0`	Specifies the interface for which the main IP address will be mapped by ISA to the destination IP addresses in subscriber traffic.
Step 7	**exit** **Example:** `Router(config-portbundle)# exit`	Returns to privileged EXEC mode.
Step 8	**interface** *type number* **Example:** `Router(config)# interface ethernet 0/0`	Specifies an interface for configuration.
Step 9	**ip portbundle outside** **Example:** `Router(config-if)# ip portbundle outside`	Configures ISA to reverse translate the destination IP address and TCP port to the actual subscriber IP address and TCP port for traffic going from the portal to the subscriber for the interface being configured.

Verifying ISA Port-Bundle Host Key Configuration

Perform this task to display information about ISA port-bundle host key configuration.

SUMMARY STEPSh

1. **enable**
2. **show ip portbundle status** [**free** | **inuse**]
3. **show ip portbundle ip** *portbundle-ip-address* **bundle** *port-bundle-number*
4. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip portbundle status** [**free** | **inuse**] **Example:** `Router# show ip portbundle status free`	Displays information about ISA port-bundle groups.
Step 3	**show ip portbundle ip** *portbundle-ip-address* **bundle** *port-bundle-number* **Example:** `Router# show ip portbundle ip 10.10.10.10 bundle 65`	Displays information about a specific ISA port bundle.
Step 4	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*] **Example:** `Router# show subscriber session detailed`	Displays ISA subscriber session information.

Configuring ISA Transparent Autologon

The following prerequisites apply to ISA Transparent Autologon:

- Prerequisites for ISA Transparent Autologon

Before you configure ISA Transparent Autologon, you should understand the following concept:

- ISA Transparent Autologon, page 63

To configure ISA Transparent Autologon, perform the following tasks:

- Identifying Traffic for ISA Transparent Autologon in a Control Policy Class Map, page 64
- Configuring a Control Policy for ISA Transparent Autologon, page 65

Prerequisites for ISA Transparent Autologon

Depending on your AAA implementation, you may need to configure the IP source address or MAC address in the username field and a global address in the password field of the user profile.

ISA Transparent Autologon

Service providers commonly implement a policy at the start of IP sessions that redirects all subscriber packets to a logon portal for authenticatoin. Following successful authentication, per-subscriber authorization data is typically returned from a AAA server. For some deployments, usually in subscriber networks that are well protected against spoofing and denial-of-service (DoS) attacks, service providers

are willing to forgo authentication and trust subscriber identity. The ISA Transparent Logon feature allows service providers to grant certain subscribers access to services without requiring the subscribers to log on.

ISA transparent autologon enables an IP address or MAC address to be used in place of the username in authorization requests. Enabling the AAA server to authorize subscribers on the basis of their source IP address or MAC address allows subscriber profiles to be downloaded from the AAA server as soon as packets are received from subscribers.

The event that triggers transparent autologon is session-start. For IP sessions, session-start occurs when a DHCP DISCOVER request is received or when an unrecognized source IP address is detected.

Identifying Traffic for ISA Transparent Autologon in a Control Policy Class Map

Perform this task to configure a control policy class map that specifies the traffic to which ISA transparent autologon will apply.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type control match-all** *class-map-name*
4. **match source-ip-address** *ip-address subnet-mask*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map type control match-all** *class-map-name* **Example:** `Router(config)# class-map type control match-all TAL-subscribers`	Creates a control class map, which defines the conditions under which the actions of a control policy map will be executed.

	Command or Action	Purpose
Step 4	**match source-ip-address** *ip-address subnet-mask* **Example:** `Router(config-control-classmap)# match source-ip-address 1.1.1.0 255.255.255.0`	Creates a condition that will evaluate true if a subscriber's source IP address matches the specified IP address.
Step 5	**end** **Example:** `Router(config-control-classmap)# end`	(Optional) Returns to privileged EXEC mode.

Configuring a Control Policy for ISA Transparent Autologon

ISA transparent autologon allows subscribers to be authorized on the basis of their source IP address or MAC address. Perform this task to configure ISA transparent autologon in a control policy.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*class-map-name* | **always**} **event session-start**
5. **1 authorize** [**aaa list** {*list-name* | **default**}] [**password** *password*] **identifier** {**source-ip-address** | **mac-address**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control TAL`	Creates or modifies a control policy map, which is used to define a control policy.

	Command or Action	Purpose
Step 4	**class type control** {*class-map-name* | **always**} **event session-start** **Example:** `Router(config-control-policymap)# class type control TAL-subscribers event session-start`	Specifies a control class, which defines the conditions that must be met in order for an associated set of actions to be executed. • Specify the control class-map that was configured in the task Identifying Traffic for ISA Transparent Autologon in a Control Policy Class Map.
Step 5	*action-number* **authorize** [**aaa list** {*list-name* | **default**}] [**password** *password*] **identifier** {**source-ip-address** | **mac-address**} **Example:** `Router(config-control-policymap-class-control)# 1 authorize aaa list TAL_LIST password cisco identifier source-ip-address`	Inserts the source IP address or MAC address into the username field of authorization requests. • For sessions triggered by an unrecognized IP address, the MAC address should be used only when the subscriber is one hop away.

What to Do Next

You must apply the control policy to a context by using the **service-policy type control** command. For information about applying control policies, see the module "Configuring ISA Control Policies."

You may want to configure policies to determine what should happen for transparent autologon subscribers whose IP address or MAC address authorization fails; for example, you may want to redirect the subscriber to the policy server for authentication.

Configuration Examples for ISA Layer 3 Access

This section contains the following examples:

ISA IP Interface Session Configuration: Example

The following example shows an IP interface session configured on Ethernet interface 0/0:

```
interface ethernet0/0
 ip subscriber
  identifier interface
```

ISA IP Subscriber Session Configuration: Example

The followin example shows how to configure ISA to create IP sessions upon receipt of DHCP DISCOVER packets:

```
interface ethernet0/0
 ip subscriber
  initiator dhcp
```

Unauthenticated Layer 4 Redirect: Example

In the following example, Layer 4 redirect is configured in the service policy map “BLIND-RDT”. This policy is applied to all sessions at session start and redirects subsribers TCP traffic to the server group called “PORTAL”. At account logon the subscriber is authenticated and the redirection is unapplied.

```
Service-policy type control DEFAULT-IP-POLICY

policy-map type control DEFAULT-IP-POLICY
 class type control always event session-start
  1 service-policy type service BLIND-RDT
!
 class type control always event account-logon
  1 authenticate aaa list AUTH-LIST
  2 service-policy type service unapply BLIND-RDT

policy-map type service BLIND-RDT
 class type traffic CLASS-ALL
  redirect to group PORTAL
!
redirect server-group PORTAL
 server ip 10.2.36.253 port 80
```

ISA Port-Bundle Host Key Configuration: Example

The following example shows how to configure the ISA Port-Bundle Host Key feature to apply to all sessions:

```
policy-map type service ISGPBHKService
 ip portbundle
!
policy-map type control PBHKRule
 class type control always event session-start
  1 service-policy type service ISGPBHKService
!
service-policy type control PBHKRule

interface ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip portbundle outside
!
ip portbundle
 match access-list 101
 length 5
 source ethernet0/0
```

ISA Transparent Autologon Configuration: Example

In the following example, if the client is from the 1.1.1.0 subnet, ISA transparent autologon is applied and an authorization request is sent to the list "TAL_LIST" with the subscriber's source IP address as the username. If the authorization request is successful, any automatic-activation services specified in the returned user profile are activated for the session and the execution of rules within the control-policy stops. If the authorization is not successful, the rule execution proceeds and the subscriber is redirected to the policy server to login. If the subscriber does not log in within five minutes, the session is disconnected.

ISA Configuration

```
interface Ethernet0/0
 service-policy type control RULEA

aaa authentication login TAL_LIST group radius
aaa authentication login LOCAL local
access-list 100 permit ip any any


class-map type traffic match-any all-traffic
 match access-group input 100
 match access-group output 100

policy-map type service redirectprofile
 class type traffic all-traffic
  redirect to ip 10.0.0.148 port 8080

class-map type control match-all CONDA
 match source-ip-address 1.1.1.0 255.255.255.0

!
class-map type control match-all CONDF
 match timer TIMERB
 match authen-status unauthenticated

policy-map type control RULEA
 class type control CONDA event session-start
  1 authorize aaa list TAL_LIST password cisco identifier source-ip-address
  2 apply aaa list LOCAL service redirectprofile
  3 set-timer TIMERB 5 minutes
!
 class type control CONDF event timed-policy-expiry
  1 service disconnect
```

User Profile Configuration

```
9.0.0.48 Password = "cisco"
 Service-Type = Outbound,
 Cisco:Account-Info = "AAuto-Internet;proxy-user;cisco"
```

Service Profile Configuration

```
Auto-Internet Password = "cisco"
 Cisco:Service-Info = "IAuto-Internet",
 Cisco-Avpair = "traffic-class=input access-group 100"

proxy-user Password = "cisco"
 Idle-Timeout = 5
```

Additional References

The following sections provide references related to ISA Layer 3 access.

Related Documents

Related Topic	Document Title
DHCP configuration	The "Configuring DHCP" chapter of the *Cisco IOS IP Configuration Guide*, Release 12.2.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 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/public/support/tac/home.shtml

Feature Information for Configuring ISA Layer 3 Access

Table 7 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 later appear in the table.

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

If you are looking 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 7 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 7 Feature Information for ISA Layer 3 Access

Feature Name	Releases	Feature Configuration Information
ISA:Session: Creation: IP Session: Protocol Event (DHCP)	12.2(27)SBA	Most ISA sessions are created upon detection of a data flow that cannot be affiliated with an already active session. An ISG can be configured to create an IP session upon receipt of the first DHCP DISCOVER packet received from a subscriber. The following sections provide information about this feature: • Information About ISA Layer 3 Access, page 48 • Bringing Up Layer 3 Sessions, page 50
ISA:Session: Creation: IP Session: Subnet and Source IP: L2	12.2(27)SBA	The ISA session is the primary component used for associating services and policies across specific data flows. An IP subnet session is an ISA session that includes any IP traffic from a single IP subnet . A source-IP-based session includes traffic from a single source IP address. The following sections provide information about this feature: • Information About ISA Layer 3 Access, page 48 • How to Configure ISA Layer 3 Access, page 50
ISA:Session: Creation: IP Session: Subnet and Source IP: L3	12.2(27)SBA	The ISA session is the primary component used for associating services and policies across specific data flows. An IP subnet session is an ISA session that includes any IP traffic from a single IP subnet . A source-IP-based session includes traffic from a single source IP address. The following sections provide information about this feature: • Information About ISA Layer 3 Access, page 48 • How to Configure ISA Layer 3 Access, page 50
ISA:Session: Creation: Interface IP Session: L2	12.2(27)SBA	ISA IP interface sessions include all IP traffic received on a specific physical or virtual interface. IP interface sessions are provisioned through the CLI; that is, a session is created when the IP interface session commands are entered. The following sections provide information about this feature: • Information About ISA Layer 3 Access, page 48 • Creating an IP Interface Session, page 50

Table 7 Feature Information for ISA Layer 3 Access

Feature Name	Releases	Feature Configuration Information
ISA:Session: Creation: Interface IP Session: L3	12.2(27)SBA	ISA IP interface sessions include all IP traffic received on a specific physical or virtual interface. IP interface sessions are provisioned through the CLI; that is, a session is created when the IP interface session commands are entered. The following sections provide information about this feature: • Information About ISA Layer 3 Access, page 48 • Creating an IP Interface Session, page 50
ISA:Session: Authorization (MAC, IP)	12.2(27)SBA	ISA transparent autologon enables an IP address or MAC address to be used in place of the username in authorization requests. Enabling the AAA server to authorize subscribers on the basis of their source IP address or MAC address allows subscriber profiles to be downloaded from the AAA server as soon as packets are received from subscribers. The following section provides information about this feature: • ISA Transparent Autologon Configuration: Example, page 68
ISA:Session: Auth: PBHK	12.2(27)SBA	The ISA Port-Bundle Host Key feature serves as an in-band signaling mechanism for session identification at external portals. TCP packets from subscribers are mapped to a local IP address for the ISA gateway and a range of ports. This mapping allows the portal to identify the ISA gateway from which the session originated. The following section provides information about this feature: • Configuring ISA Port-Bundle Host Key, page 56