Transparent Bridging Support for Authentication Proxy

Last Updated: January 18, 2012

The Transparent Bridging Support for Authentication Proxy feature allows network administrators to configure transparent authentication proxy on existing networks without having to reconfigure the statically defined IP addresses of their network-connected devices. The result is that security policies are dynamically authenticated and authorized on a per user basis, which eliminates the tedious and costly overhead required to renumber devices on the trusted network.

Authentication proxy rules on bridged interfaces can coexist with router interfaces on the same device, whenever applicable, which allows administrators to deploy different authentication proxy rules on bridged and routed domains.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

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

Restrictions for Transparent Bridging Support for Authentication Proxy

Authentication Proxy is not supported on vLAN trunk interfaces that are configured in a bridge group.

Information About Transparent Bridging Support for Authentication Proxy

Authentication proxy provides dynamic, per-user authentication and authorization of network access connections to enforce security policies. Typically, authentication proxy is a Layer 3 functionality that is configured on routed interfaces with different networks and IP subnets on each interface.

Integrating authentication proxy with transparent bridging enables network administrators to deploy authentication proxy on an existing network without impacting the existing network configuration and IP address assignments of the hosts on the network.

- Transparent Bridging Overview, page 2

Transparent Bridging Overview

If configured for bridging, a Cisco IOS device can bridge any number of interfaces. The device can complete basic bridging tasks such as learning MAC addresses on ports to restrict collision domains and running Spanning Tree Protocol (STP) to prevent looping in the topology.

Within bridging, a user can configure Integrated Routed Bridging (IRB), which allows a device to bridge on some interfaces while a Layer 3 Bridged Virtual Interface (BVI) is presented for routing. The bridge can determine whether the packet is to be bridged or routed on the basis of the destination of the Layer 2 or Layer 3 IP address in the packet. Configured with an IP address, the BVI can manage the device even if no interface is configured for routing.

How to Configure Transparent Authentication Proxy

To configure authentication proxy on bridged interfaces, you must configure the interface in a bridge group and apply an authentication proxy rule on the interface. You must also set up and configure the authentication, authorization, and accounting (AAA) server (Cisco ACS) for authentication proxy. For examples on how to configure authentication proxy on a bridged interface, see the section, Configuration Examples for Transparent Authentication Proxy.

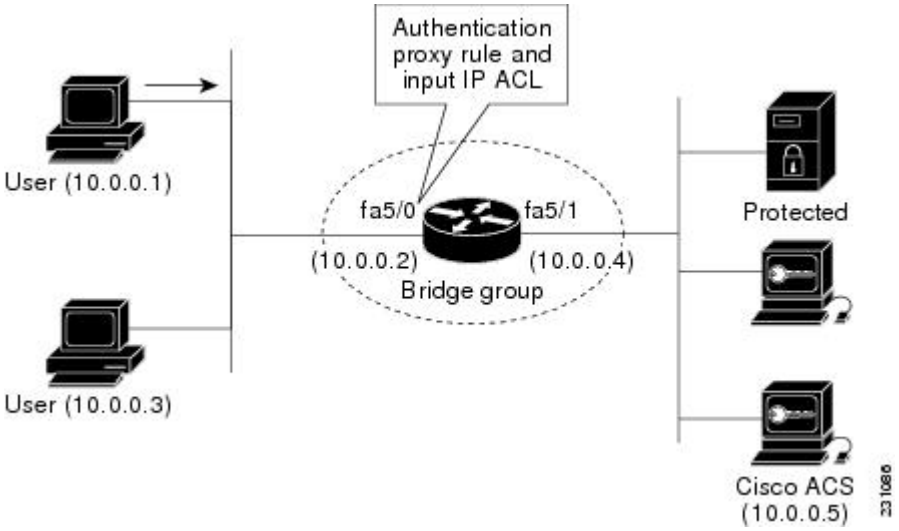
Configuration Examples for Transparent Authentication Proxy

- Authentication Proxy in Transparent Bridge Mode Example, page 3
- Authentication Proxy in Concurrent Route Bridge Mode Example, page 4
- Authentication Proxy in Integrated Route Bridge Mode Example, page 5

Authentication Proxy in Transparent Bridge Mode Example

The following example (see the figure below) shows how to configure authentication proxy in a transparent bridged environment in which network users (that is, hosts on the bridged interface FastEthernet 5/0) are challenged for user credentials before being given access to protected resources.

Figure 1 Authentication Proxy in Transparent Bridging Mode: Sample Topology




```
aaa new-model
!
aaa authentication login default group radius
aaa authorization auth-proxy default group radius
aaa accounting auth-proxy default start-stop group radius
!
no ip routing
!
!
no ip cef
!
ip auth-proxy name AuthRule http inactivity-time 60
!
interface FastEthernet5/0
 ip address 10.0.0.2 255.255.255.0
 ip auth-proxy AuthRule
 ip access-group 100 in
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
!
interface FastEthernet5/1
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
!
ip http server
ip http secure-server
!
radius-server host 10.0.0.5 auth-port 1645 acct-port 1646
radius-server key cisco
!
```

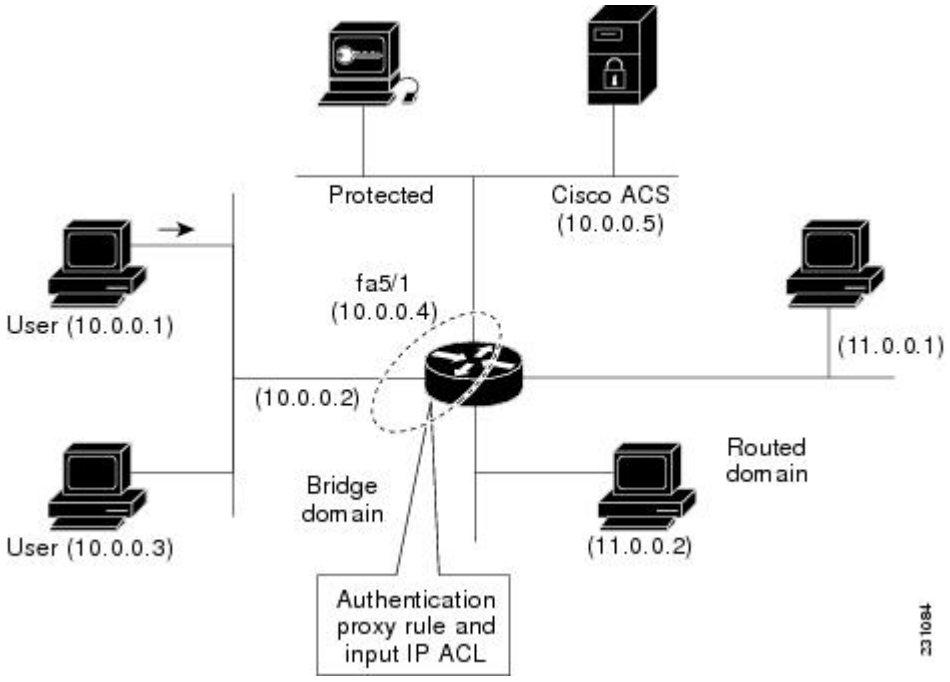
```
bridge 1 protocol ieee
!
Router# show ip auth-proxy cache
Authentication Proxy Cache
Client Name AuthRule, Client IP 10.0.0.1, Port 1100,
                timeout 60, Time Remaining 60, state ESTAB
```

Authentication Proxy in Concurrent Route Bridge Mode Example

Concurrent routing and bridging configuration mode allows routing and bridging to occur in the same router; however, the given protocol is not switched between the two domains. Instead, routed traffic is confined to the routed interfaces and bridged traffic is confined to the bridged interfaces.

The following example (see the figure below) shows how to configure authentication proxy in a concurrent routing and bridging environment in which network users (that is, hosts on the bridged interface FastEthernet 5/0) are challenged for user credentials before being given access to protected resources.

Figure 2 Authentication Proxy in Concurrent Route Bridge Mode: Sample Topology




```
aaa new-model
!
aaa authentication login default group radius
aaa authorization auth-proxy default group radius
aaa accounting auth-proxy default start-stop group radiusb
!
ip cef
!
bridge crb
!
ip auth-proxy name AuthRule http inactivity-time 60
!
interface FastEthernet5/0
 ip address 10.0.0.2 255.255.255.0
 ip auth-proxy AuthRule
 ip access-group 100 in
 no ip route-cache
```

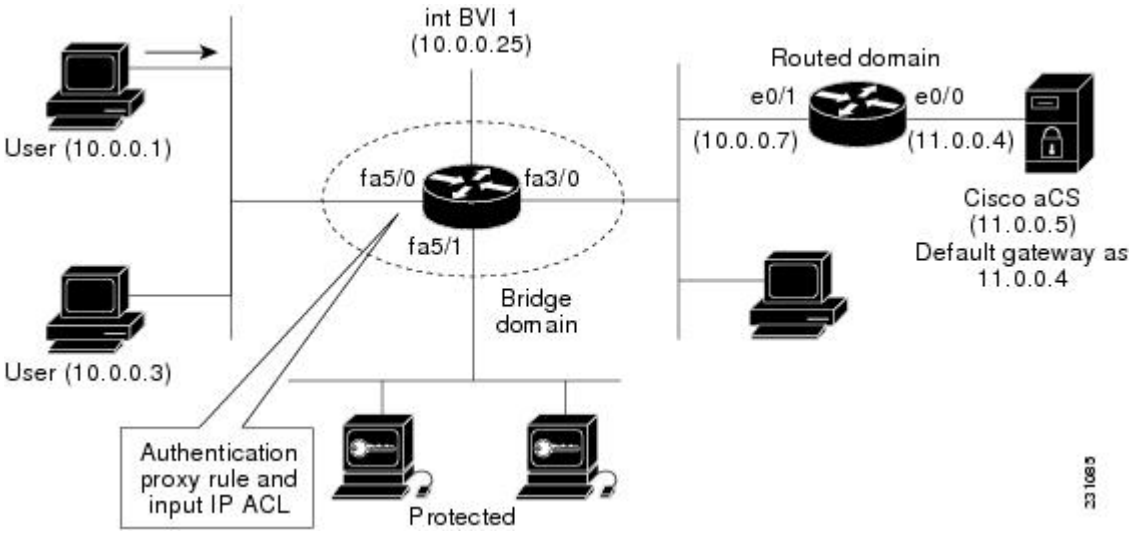
```
 duplex auto
 speed auto
 bridge-group 1
!
interface FastEthernet5/1
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
!
ip http server
ip http secure-server
!
radius-server host 10.0.0.5 auth-port 1645 acct-port 1646
radius-server key cisco
!
bridge 1 protocol ieee
!
Router# show ip auth-proxy cache
Authentication Proxy Cache
Client Name AuthRule, Client IP 10.0.0.1, Port 1145,
               timeout 60, Time Remaining 60, state ESTAB
```

Authentication Proxy in Integrated Route Bridge Mode Example

In an integrated routing and bridging environment, a bridged network is interconnected with a router network. Both routing and bridging can occur in the same router with connectivity between routed and bridged domains.

The following example (see the figure below) shows how to configure authentication proxy in an integrated routing and bridging environment in which network users (that is, hosts on the bridged interface FastEthernet 5/0) are challenged for user credentials before being given access to protected resources.

Figure 3 Authentication Proxy in Integrated Route Bridge Mode: Sample Topology




```
!
aaa new-model
!
aaa authentication login default group radius
aaa authorization auth-proxy default group radius
aaa accounting auth-proxy default start-stop group radius
```

```
!
ip cef
!
ip auth-proxy name AuthRule http inactivity-time 60
!
bridge irb
!
interface FastEthernet3/0
 no ip address
 duplex half
 bridge-group 1
!
interface FastEthernet5/0
 no ip address
 ip auth-proxy AuthRule
 ip access-group 100 in
 duplex auto
 speed auto
 bridge-group 1
!
interface FastEthernet5/1
 no ip address
 duplex auto
 speed auto
 bridge-group 1
!
interface BVI1
 ip address 10.0.0.25 255.255.255.0
!
!
ip route 11.0.0.0 255.255.255.0 10.0.0.7
!
ip http server
ip http secure-server
!
radius-server host 11.0.0.5 auth-port 1645 acct-port 1646
radius-server key cisco
!
bridge 1 protocol ieee
bridge 1 route ip
!
Router# show ip auth-proxy cache
Authentication Proxy Cache
Client Name AuthRule, Client IP 10.0.0.1, Port 1100,
                timeout 60, Time Remaining 60, state ESTAB
```

Additional References

The following sections provide references related to the Transparent Bridging Support for Authentication Proxy feature.

Related Documents

Related Topic	Document Title
Authentication proxy commands	*Cisco IOS Security Command Reference*
Bridging commands	*Cisco IOS Bridging Command Reference*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Transparent Authentication Proxy

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for Transparent Authentication Proxy

Feature Name	Releases	Feature Information
Transparent Bridging Support for Authentication Proxy	12.4(15)T	The Transparent Bridging Support for Authentication Proxy feature allows network administrators to configure transparent authentication proxy on existing networks without having to reconfigure the statically defined IP addresses of their network-connected devices. The result is that security policies are dynamically authenticated and authorized on a per user basis, which eliminates the tedious and costly overhead required to renumber devices on the trusted network. Authentication proxy rules on bridged interfaces can coexist with router interfaces on the same device, whenever applicable, which allows administrators to deploy different authentication proxy rules on bridged and routed domains. This feature was introduced in Cisco IOS Release 12.4(15)T.